

# HP Network Automation ソフトウェア

Windows<sup>®</sup>、Linux、Solarisオペレーティングシステム向け

ソフトウェアバージョン: 9.20

---

## ユーザガイド



## ご注意

### 保証

HP製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載で追加保証を意図するものは一切ありません。ここに含まれる技術的、編集上の誤り、または欠如について、HPはいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

### 権利の制限

機密性のあるコンピュータソフトウェアです。これらを所有、使用、または複製するには、HPからの有効な使用許諾が必要です。商用コンピュータソフトウェア、コンピュータソフトウェアに関する文書類、および商用アイテムの技術データは、FAR12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

### 著作権

© Copyright 20012012 Hewlett-Packard Development Company, L.P.

### 商標について

Adobe®は、Adobe Systems Incorporated (アドビシステムズ社) の商標です。

AMDは Advanced Micro Devices, Inc. の商標です。

IntelおよびIntel Itaniumは、Intel Coporationの米国およびその他の国の登録商標です。

Microsoft®およびWindows®は、米国におけるMicrosoft Corporationの登録商標です。

JavaおよびJavaは、Oracle Corporationおよびその関連会社の登録商標です。

UNIX®は、The Open Groupの登録商標です。

### Oracle Technology Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Oracleの完全なライセンステキストについては、製品のインストール後、NAアプリケーションサーバの\$NA\_HOME/server/licenseディレクトリ（またはWindowsシステムの%NA\_HOME%\server\licenseディレクトリ）を参照してください。

### 謝辞

本製品には、Apache Software Foundation (<http://www.apache.org> (英語サイト)) によって開発されたソフトウェアが含まれています。

本ソフトウェアの一部 : Copyright © 2003-2008 Enterprise Distributed Technologies Ltd. All Rights Reserved.  
(<http://www.enterprisedt.com> (英語サイト))

## ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

- ソフトウェアのバージョン番号は、ソフトウェアのバージョンを示します。
- ドキュメントリリース日は、ドキュメントが更新されるたびに変更されます。
- ソフトウェアリリース日は、このバージョンのソフトウェアのリリース期日を表します。

最新の更新のチェック、またはご使用のドキュメントが最新版かどうかの確認には、次のサイトをご利用ください。

**<http://support.openview.hp.com/selfsolve/manuals>**

このサイトを利用するには、HP Passport への登録とサインインが必要です。HP Passport ID の取得登録は、次の Web サイトから行なうことができます。

**<http://h20229.www2.hp.com/passport-registration.html>** (英語サイト)

または、HP Passport のログインページの **[New users - please register]** リンクをクリックします。

適切な製品サポートサービスをお申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、HP の営業担当にお問い合わせください。

## サポート

HP ソフトウェアサポートオンライン Web サイトを参照してください。

**<http://support.openview.hp.com>**

HP ソフトウェアが提供する製品、サービス、サポートに関する詳細情報をご覧ください。

HP ソフトウェアオンラインではセルフソルブ機能を提供しています。お客様の業務の管理に必要な対話型の技術支援ツールに素早く効率的にアクセスいただけます。HP ソフトウェアサポート Web サイトのサポート範囲は次のとおりです。

- 関心のある技術情報の検索
- サポートケースとエンハンスメント要求の登録とトラッキング
- ソフトウェアパッチのダウンロード
- サポート契約の管理
- HP サポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部を除き、サポートのご利用には、HP Passport ユーザとしてご登録の上、ログインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。

アクセスレベルに関する詳細は、以下の Web サイトにアクセスしてください。

**[http://support.openview.hp.com/access\\_level.jsp](http://support.openview.hp.com/access_level.jsp)**

HP Passport ID の登録は、次の場所で行います。

**<http://h20229.www2.hp.com/passport-registration.html>** (英語サイト)

# 目次

<b>第1章：はじめに</b>	17
製品の概要	18
NA 7.50の機能	19
NA 7.60の機能	20
NA 9.00の機能	21
NA 9.10の機能	22
NA 9.20の機能	23
ヘルプメニューオプション	24
NA ホームページ	25
コマンドウィンドウを開く	26
ドキュメントへのアクセス	26
HP Network Automation ユーザガイド	27
このドキュメントでの表記規則	28
[トラブルシューティングの送信]ページのフィールド	29
最新ソフトウェアバージョンの表示	30
ライセンス情報の表示	30
[システム構成を表示]ページ	31
<b>第2章：管理設定の構成</b>	33
はじめに	34
構成管理	35
[構成管理]ページのフィールド	36
変更の検出	41
Syslog メッセージ	42
[ユーザ属性の詳細]ページのフィールド	42
タスク前とタスク後のスナップショットの構成	43
デバイスアクセス	44
[デバイスアクセス]ページのフィールド	45
タスク単位の資格情報	50
サーバ	52
[サーバ]ページのフィールド	52
ワークフロー	59
[ワークフロー]ページのフィールド	59
ユーザインターフェイス	61
[ユーザインターフェイス]ページのフィールド	61
NA ログインページをカスタマイズする	64
Telnet/SSH	65
[Telnet/SSH]ページのフィールド	65
レポート作成	68

[レポート作成]ページのフィールド	69
ユーザ認証	73
認証フェイルオーバー	73
LDAP認証	74
SecurID認証	74
TACACS+認証	75
RADIUS認証	75
HP Server Automation (HP SA)	76
HP Operations Orchestration (HP OO)	76
[ユーザ認証]ページのフィールド	77
LDAP外部認証の設定	80
LDAP SSL 構成	81
サーバ監視	83
[サーバ監視]ページのフィールド	83
サードパーティ統合	87
[サードパーティ統合]ページのフィールド	87
監視結果の表示	89
[システムステータス]ページのフィールド	89
監視のメッセージ	90
サービスの開始および停止	94
[サービスの開始/停止]ページのフィールド	94
ログ記録	96
ログのレベル	96
ログ名	97
セッションログ	98
タスクログ	98
サーバログ	99
ログ管理	99
[トラブルシューティング]ページのフィールド	100
ドライバのレビュー	101
[ドライバ]ページのフィールド	101
<b>第3章：デバイスとデバイスグループの追加</b>	103
はじめに	104
デバイスグループの命名規則	105
デバイスの追加	106
[デバイスの新規作成]ページのフィールド	106
[デバイスの編集]ページのフィールド	111
ベアメタルプロビジョニング	116
デバイステンプレート	118
[デバイステンプレート]ページのフィールド	118
[デバイステンプレートの詳細]ページのフィールド	119
[テンプレート構成を編集]ページ	120
新しいデバイステンプレートの追加	122
[デバイステンプレートの新規作成]ページのフィールド	122
デバイス固有のテンプレート	124
デバイスの新規作成ウィザードの使用	125

[デバイスの新規作成ウィザード]ページのフィールド	125
デバイスのインポート	126
デバイスデータのインポートのためのCSVファイルの作成	126
デバイスデータのインポートファイル	127
デバイスグループデータのインポートファイル	130
デバイス固有パスワードデータのインポートファイル	131
デバイスパスワードルールの作成	132
[デバイスパスワードルール]ページのフィールド	132
[デバイスパスワードルール]ページのフィールド	134
デバイスグループの追加	136
[グループの新規作成]ページのフィールド	137
親グループの追加	138
[親グループの新規作成]ページのフィールド	138
[親グループ]ページのフィールド	139
動的デバイスグループ	140
動的デバイスグループの作成	140
動的デバイスグループの計算	141
デバイスセクタ	142
デバイスの選択	142
デバイスグループの選択	143
デバイスセクタボタン	143
デバイスグループの表示	144
[デバイスグループ]ページのフィールド	145
[デバイスグループの詳細]ページのフィールド	146
デバイスとユーザのセグメント化	148
ローカル領域	150
ローカル領域とNATアクセス	150
ローカル領域とコンソールアクセス	150
ローカル領域と要塞ホストアクセス	150
ローカル領域の追加	151
重複IPネットワーク	151
HP Gatewayの設定	152
[ゲートウェイリスト]ページのフィールド	153
[ゲートウェイの編集]ページのフィールド	155
パーティション	156
[パーティション]ページのフィールド	156
[パーティションの新規作成]ページ	157
[パーティションの編集]ページのフィールド	157
パーティションにデバイスを追加	158
パーティション詳細の表示	159
デバイスグループの編集	160
[グループを編集]ページのフィールド	160
デバイスの一括編集	161
[デバイスを一括編集]ページのフィールド	161
デバイスドライバの検出	163
Telnetを使用したデバイスへのアクセス	164

SSHを使用したデバイスへのアクセス .....	165
Telnet/SSHセッションのリスト表示 .....	166
[Telnet/SSHセッションリスト]ページのフィールド .....	166
Telnet/SSHプロキシを使用した構成の変更 .....	168
要塞ホストの使用 .....	169
<b>第4章：デバイス構成の管理</b> .....	171
はじめに .....	172
デバイス構成変更の表示 .....	172
[デバイス構成]ページのフィールド .....	173
[デバイス構成の詳細]ページのフィールド .....	175
デバイス構成データの編集 .....	178
デバイス構成の比較 .....	179
[デバイス構成の比較]ページのフィールド .....	179
デバイス構成の展開 .....	180
[構成を配布]タスクページのフィールド .....	181
<b>第5章：デバイスの表示</b> .....	185
デバイスの表示 .....	186
[インベントリ]ページのフィールド .....	186
デバイスグループの表示 .....	188
[デバイスグループ]ページのフィールド .....	188
デバイスの予約 .....	190
アクティビティカレンダー .....	191
デバイス詳細の表示 .....	193
[デバイス詳細]ページのフィールド .....	193
NA/SA統合 .....	196
NA/SA権限 .....	196
デバイスハードウェア情報 .....	197
ファイアウォールを介したNAへの接続 .....	197
ポートの変更 .....	199
ポート数が正しくない .....	200
表示メニューオプション .....	201
[デバイスイベント]ページのフィールド .....	204
[デバイスインターフェイス]ページのフィールド .....	205
[インターフェイスの詳細]ページのフィールド .....	206
[インターフェイスの詳細を編集]ページのフィールド .....	208
[サブネット内のインターフェイス]ページのフィールド .....	210
[デバイスIPアドレス]ページのフィールド .....	211
[デバイスMACアドレス]ページのフィールド .....	212
仮想ローカルエリアネットワーク（VLAN） .....	213
[デバイスVLAN]ページのフィールド .....	215
VLANの作成と編集 .....	216
[VLAN詳細]ページのフィールド .....	217
[VTP詳細]ページのフィールド .....	218
[VTPドメイン]ページのフィールド .....	219
[VTPドメイン]ページ .....	220



[デバイスブレード/モジュール]ページのフィールド	220
[デバイスポリシー]ページのフィールド	221
[サーバ]ページのフィールド	222
[デバイスソフトウェアイメージ推奨]ページのフィールド	223
[デバイスタスク]ページのフィールド	225
[デバイス関係]ページのフィールド	226
[デバイスソフトウェア履歴]ページのフィールド	228
[デバイスセッション]ページのフィールド	229
編集メニューオプション	230
[デバイス管理対象IPアドレス]ページのフィールド	232
[IPアドレスの新規作成]ページ（要塞ホスト）	234
[IPアドレスの新規作成]ページ（カスタムIPアドレス）	235
[IPアドレスの新規作成]ページ（コンソールサーバ）	236
[IPアドレスの新規作成]ページ（ホップボックス）	237
[IPアドレスの新規作成]ページ（新規接続スルー）	238
プロビジョニングメニューオプション	239
接続メニューオプション	241
<b>第6章：ユーザの管理</b>	243
ユーザの追加	244
[全ユーザ]ページのフィールド	244
[ログオンしているユーザ]ページのフィールド	246
電子メール通知	246
[ユーザの新規作成]ページのフィールド	247
ユーザパスワードの構成	250
ユーザシナリオ1	250
ユーザシナリオ2	251
ユーザシナリオ3	251
パスワードの有効期限	252
パスワードの再使用	252
ユーザグループの追加	253
[ユーザグループ]ページのフィールド	253
[ユーザグループの新規作成]ページのフィールド	254
ユーザロールの追加	257
[ユーザのロールと権限]ページのフィールド	257
[ユーザロールの新規作成]ページのフィールド	259
ユーザ設定の編集	260
自分の設定	260
[自分のプロフィール]ページのフィールド	260
[自分のワークスペース]ページのフィールド	262
[自分の環境設定]ページのフィールド	262
[自分の権限]ページのフィールド	264
[パスワードの変更]ページのフィールド	265
クイック起動とは	265
クイック起動の構成方法	266
クイック起動の管理	266
クイック起動の使用方法	267

サンプルのクイック起動の表示 .....	267
NA ホームページのカスタマイズ .....	269
[自分のホームページ] タブのフィールド .....	270
[統計ダッシュボード] タブのフィールド .....	272
検索/接続機能 .....	273
<b>第7章：タスクの予定</b> .....	275
タスクとは .....	277
アドホックデバイスグループへのタスクの実行 .....	277
タスクの予定 .....	278
用語 .....	278
ラウンドロビングループタスク .....	279
タスクテンプレート .....	280
NA タスク .....	282
[Syslog の構成] タスクページのフィールド .....	284
[パスワードの配布] タスクページのフィールド .....	288
[ドライバの検出] タスクページのフィールド .....	293
[デバイスのリポート] タスクページのフィールド .....	296
[ICMP テストの実行] タスクページのフィールド .....	299
[コマンドスクリプトの実行] タスクページのフィールド .....	304
[診断の実行] タスクページのフィールド .....	310
[スナップショットの取得] タスクページのフィールド .....	315
[スタートアップとランニングの同期] タスクページのフィールド .....	319
[デバイスソフトウェアの更新] タスクページのフィールド .....	323
配布表 .....	327
[デバイスのインポート] タスクページのフィールド .....	329
[ユーザのインポート] タスクページのフィールド .....	334
ユーザデータのインポートのための CSV ファイルの作成 .....	337
[ネットワークデバイスの検出] タスクページのフィールド .....	341
スキャン方法 .....	342
IP アドレス範囲の定義 .....	343
[重複の削除] タスクページのフィールド .....	347
[OS 分析] タスクページのフィールド .....	350
[ポートスキャン] ページのフィールド .....	353
[デバイスのプロビジョニング] タスクページのフィールド .....	356
[デバイスコンテキストを追加] タスクページのフィールド .....	359
[VLAN タスク] ページのフィールド .....	363
トランクポートの構成 .....	366
[Cisco.com からイメージをダウンロード] タスクページ .....	367
[デバイスソフトウェアのバックアップ] タスクページのフィールド .....	369
[ポリシー準拠の確認] タスクページのフィールド .....	372
[サマリレポートの生成] タスクページのフィールド .....	375
[電子メールレポート] タスクページのフィールド .....	377
[リモートエージェントを配布] タスクページのフィールド .....	380
[FQDN の解決] タスクページのフィールド .....	382
[データの整理] タスクページのフィールド .....	385
[外部アプリケーションの実行] タスクページのフィールド .....	388

マルチタスクプロジェクトの予定	391
サブタスク警告ステータス	391
[マルチタスクプロジェクト]ページのフィールド	393
マルチタスクプロジェクトの構成方法	395
[自分のタスク]の表示	397
[自分のタスク]ページのフィールド	397
予定されたタスクの表示	400
[予定タスク]ページのフィールド	400
実行中のタスクの表示	402
[実行中のタスク]ページのフィールド	402
最近のタスクの表示	404
[最近のタスク]ページのフィールド	404
[タスク情報]ページのフィールド	406
タスク負荷の表示	409
[タスク負荷]ページ	409
<b>第8章：ポリシー保証の管理</b>	411
はじめに	412
NA Policy Managerの動作方法	413
ポリシーの作成	414
[ポリシー]ページのフィールド	415
[ポリシーの新規作成]ページのフィールド	417
[ルールの新規作成]ページのフィールド	420
ポリシーのインポート/エクスポート	424
[ポリシーのインポート/エクスポート]ページのフィールド	424
ポリシーを編集	425
[ポリシーを編集]ページのフィールド	425
ルール例外の追加	428
[ルール例外の新規作成]ページのフィールド	428
適用されるポリシーの表示	429
ポリシーアクティビティの表示	430
[ポリシーアクティビティ]ページのフィールド	430
ポリシー準拠の表示	431
[ポリシー準拠]ページのフィールド	431
[デバイスに適用される構成ポリシー]ページのフィールド	432
新規ソフトウェアレベルの追加	433
[ソフトウェアレベルを追加]ページのフィールド	433
[ソフトウェアレベル]ページのフィールド	435
ソフトウェアレベルの編集	437
[ソフトウェアレベルの編集]ページのフィールド	437
ポリシー準拠のテスト	439
[ポリシー準拠のテスト]ページのフィールド	439
[ポリシーをテスト]ページのフィールド	439
<b>第9章：ソフトウェアの配布</b>	441
はじめに	442
ソフトウェアイメージ	444

[ソフトウェアイメージ]ページのフィールド .....	444
イメージセットの追加 .....	445
[ソフトウェアイメージセットを追加]ページのフィールド .....	445
[ソフトウェアイメージの編集]ページのフィールド .....	447
ソフトウェアの配布 .....	448
新規ソフトウェアレベルの追加 .....	449
[ソフトウェアレベルを追加]ページのフィールド .....	449
デバイスソフトウェアのバージョンの表示 .....	451
<b>第10章：イベント通知ルール</b> .....	453
はじめに .....	454
イベントルールの追加 .....	459
[イベント通知とレスポンスルール]ページのフィールド .....	459
[イベント通知とレスポンスルールの新規作成]ページのフィールド .....	460
イベントルール変数 .....	464
デバイスイベントの変数 .....	464
デバイス構成イベントの変数 .....	465
デバイス診断イベントの変数 .....	465
タスクイベントの変数 .....	466
すべてのイベントの変数 .....	467
<b>第11章：検索の実行</b> .....	469
全文検索機能の使用 .....	470
デバイスの検索 .....	472
[デバイスを検索]ページのフィールド .....	473
[デバイスの検索結果]ページのフィールド .....	478
インターフェイスの検索 .....	480
[インターフェイスを検索]ページのフィールド .....	480
[インターフェイスの検索結果]ページのフィールド .....	482
モジュールの検索 .....	483
[モジュールを検索]ページのフィールド .....	483
[モジュールの検索結果]ページのフィールド .....	485
ポリシーの検索 .....	486
[ポリシーの検索]ページのフィールド .....	486
[ポリシーの検索結果]ページのフィールド .....	488
ポリシー、ルール、および準拠の検索 .....	489
[ポリシー、ルール、および準拠を検索]ページのフィールド .....	490
[ポリシー、ルール、および準拠の検索結果]ページのフィールド .....	492
構成の検索 .....	494
[構成を検索]ページのフィールド .....	494
[構成の検索結果]ページのフィールド .....	497
診断の検索 .....	498
[診断を検索]ページのフィールド .....	499
[診断の検索結果]ページのフィールド .....	501
タスクの検索 .....	502
[タスクを検索]ページのフィールド .....	502
[タスクの検索結果]ページのフィールド .....	506

セッションの検索 .....	508
[セッションを検索]ページのフィールド .....	508
[セッションの検索結果]ページのフィールド .....	511
イベントの検索 .....	512
[イベントを検索]ページのフィールド .....	512
[イベントの検索結果]ページのフィールド .....	514
イベントの説明 .....	515
ユーザの検索 .....	520
[ユーザを検索]ページ .....	520
[ユーザの検索結果]ページ .....	521
ACLの検索 .....	522
[ACLを検索]ページのフィールド .....	523
[ACLの検索結果]ページのフィールド .....	525
MACアドレスの検索 .....	526
[MACアドレスを検索]ページのフィールド .....	527
[MACアドレスの検索結果]ページのフィールド .....	529
IPアドレスの検索 .....	530
[IPアドレスを検索]ページのフィールド .....	530
[IPアドレスの検索結果]ページのフィールド .....	532
VLANの検索 .....	533
[VLANを検索]ページのフィールド .....	533
[VLANの検索結果]ページのフィールド .....	535
デバイステンプレートの検索 .....	536
[DeviceTemplateを検索]ページのフィールド .....	536
[DeviceTemplateの検索結果]ページのフィールド .....	538
シングルサーチ .....	539
[シングルサーチを検索]ページのフィールド .....	539
[シングルサーチの検索結果]ページのフィールド .....	541
詳細検索 .....	542
[詳細検索]ページのフィールド .....	542
詳細検索の例 .....	544
<b>第12章：イベントおよび診断の管理</b> .....	545
イベントの連結ビュー（シングルビュー） .....	546
[シングルビュー]ページのフィールド .....	547
診断 .....	549
[診断]ページのフィールド .....	549
[診断の新規作成]ページのフィールド .....	551
カスタム診断の追加および編集 .....	552
<b>第13章：カスタムデータの設定</b> .....	553
はじめに .....	554
[カスタムデータの設定]ページのフィールド .....	554
拡張カスタムフィールド設定 .....	558
[カスタムデータフィールドの新規作成]ページ .....	559
<b>第14章：構成テンプレートの作成</b> .....	561
はじめに .....	562

構成テンプレートの表示 .....	563
[構成テンプレート]ページのフィールド .....	563
新規構成テンプレートの作成 .....	565
[テンプレートの新規作成]ページのフィールド .....	565
[テンプレートを表示]ページのフィールド .....	567
<b>第15章 : コマンドスクリプトの管理</b> .....	569
はじめに .....	570
HP Operations Orchestration (HP OO) のフロー .....	570
ベアメタルプロビジョニングスクリプト .....	571
コマンドスクリプトの表示 .....	573
[コマンドスクリプト]ページのフィールド .....	573
スクリプト/診断のインポート/エクスポート .....	575
コマンドスクリプトの追加 .....	576
[コマンドスクリプトの新規作成]ページのフィールド .....	578
自動修正スクリプトの作成 .....	581
自動修正スクリプトのシンタックス .....	581
自動修正スクリプト変数の命名規則 .....	582
自動修正スクリプトの例 .....	583
コマンドスクリプトの実行 .....	590
構成テンプレートからのスクリプトの作成 .....	590
<b>第16章 : レポート</b> .....	591
はじめに .....	592
ユーザレポートとシステムレポート .....	593
ユーザレポートとシステムレポートのフィールド .....	595
ネットワークステータスレポート .....	596
ネットワークステータスレポートのフィールド .....	596
ベストプラクティスレポート .....	599
ベストプラクティスレポートのフィールド .....	600
デバイスステータスレポート .....	601
デバイスステータスレポートのフィールド .....	601
統計ダッシュボード .....	602
ダイアグラム .....	603
[ダイアグラム]ページのフィールド .....	608
appserver.rcx ファイルの編集 .....	611
デバイスソフトウェアレポート .....	612
デバイスソフトウェアレポートのフィールド .....	612
ソフトウェアレベルレポート .....	614
ソフトウェアレベルレポートのフィールド .....	614
ソフトウェアの脆弱性レポート .....	616
ソフトウェアの脆弱性レポートのフィールド .....	616
イメージ同期レポート .....	618
イメージ同期レポートのフィールド .....	618
システム/ネットワークイベントレポート .....	619
システム/ネットワークイベントレポートのフィールド .....	619
ソフトウェアの脆弱性イベントの詳細レポート .....	620

サマリレポート .....	621
サマリレポートの説明 .....	622
電子メールレポート .....	624
<b>第17章 : SecurIDの使用</b> .....	625
はじめに .....	626
インストールの前提条件 .....	627
RSA Server Authentication Manager .....	627
ユーザ認証 .....	627
ネットワークデバイスへのアクセス .....	628
SecurID ソフトウェアトークンの追加 .....	630
[SecurID トークンの新規作成] ページ .....	630
SecurIDを使用したログイン .....	631
ログイン方法1 : システムPINの使用 .....	632
ログイン方法2 : 新しいPINの使用 .....	632
SecurIDのトラブルシューティング .....	633
<b>第18章 : コンプライアンスセンター</b> .....	635
はじめに .....	636
コンプライアンスセンターのホームページ .....	637
COBIT 準拠のステータスレポート .....	638
[COBIT 準拠のステータス] ページのフィールド .....	639
COSO 準拠のステータスレポート .....	646
COSO 準拠のステータスページのフィールド .....	646
ITIL 準拠のステータスレポート .....	649
ITIL 準拠のステータスページのフィールド .....	649
GLBA 準拠のステータスレポート .....	652
GLBA 準拠のステータスページのフィールド .....	653
HIPAA 準拠のステータスレポート .....	655
HIPAA 準拠のステータスページのフィールド .....	655
PCI データセキュリティ標準準拠のステータスレポート .....	662
[PCI データセキュリティ標準準拠のステータス] ページ .....	662
<b>第19章 : ワークフローの作成</b> .....	663
はじめに .....	664
ワークフローウィザード .....	665
自分のタスク .....	667
[自分のタスク] ページのフィールド .....	667
承認の要求 .....	670
[承認の要求] ページのフィールド .....	670
タスクの承認 .....	672
[タスク情報] ページのフィールド .....	672
電子メール通知 .....	675
<b>第20章 : ACLの扱い方</b> .....	677
はじめに .....	678
ACLの表示 .....	679
[デバイスACL] ページのフィールド .....	679

[ACLの表示]ページのフィールド .....	681
コマンドスクリプトの実行 .....	683
ACLの作成 .....	684
ACLアプリケーションの変更 .....	685
ACL行の一括挿入 .....	686
ACL行の一括削除 .....	686
ACLへのコメント追加とACLハンドルの作成 .....	688
ACLテンプレートの作成 .....	689
ACLの編集 .....	690
ACLの削除 .....	691
ACLの削除タスクページ .....	692
<b>第21章：トラブルシューティング</b> .....	695
ドライバ検出の失敗 .....	696
デバイスのスナップショット取得の失敗 .....	697
syslogによるリアルタイム変更検出機能なし .....	698
セッションログ .....	699
SWIMエラーメッセージ .....	700
<b>付録A：コマンドラインリファレンス</b> .....	711
<b>付録B：コマンド権限</b> .....	713
コマンド権限の付与 .....	713
コマンドのリスト .....	714
コマンド権限の定義 .....	715
<b>付録C：サンプルスクリプト</b> .....	723
PERLスクリプトのサンプル#1 .....	723
PERLスクリプトのサンプル#2 .....	724
Expectスクリプトのサンプル .....	725
<b>用語集</b> .....	727
<b>ご意見、ご感想について</b> .....	731



# 第1章：はじめに

**注意：** このドキュメントは、新しい情報が加わり次第、更新されます。最近更新のチェック、またはご使用のドキュメントが最新版かどうかのご確認には、次のサイトをご利用ください。

<http://support.openview.hp.com/selfsolve/manuals>

詳細については、「[ドキュメントの更新情報](#)」(3ページ)を参照してください。

## トピックの参照先リスト

トピック	参照先：
製品の概要	<a href="#">「製品の概要」</a> (18 ページ)
NA 7.50の機能	<a href="#">「NA 7.50の機能」</a> (19 ページ)
NA 7.60の機能	<a href="#">「NA 7.60の機能」</a> (20 ページ)
NA 9.00の機能	<a href="#">「NA 9.00の機能」</a> (21 ページ)
NA 9.10の機能	<a href="#">「NA 9.10の機能」</a> (22 ページ)
NA 9.20の機能	<a href="#">「NA 9.20の機能」</a> (23 ページ)
メニューバーのオプション	<a href="#">「ヘルプメニューオプション」</a> (24 ページ)
NA ホームページ	<a href="#">「NA ホームページ」</a> (25 ページ)
コマンドウィンドウを開く	<a href="#">「コマンドウィンドウを開く」</a> (26 ページ)
ドキュメントへのアクセス	<a href="#">「ドキュメントへのアクセス」</a> (26 ページ)
最新ソフトウェアバージョンの表示	<a href="#">「最新ソフトウェアバージョンの表示」</a> (30 ページ)
ライセンス情報の表示	<a href="#">「ライセンス情報の表示」</a> (30 ページ)
[システム構成を表示] ページ	<a href="#">「[システム構成を表示] ページ」</a> (31 ページ)

## 製品の概要

ネットワーク規模の拡大に伴い、ネットワークのトポロジーも複雑化してきています。さらに多くのネットワークは、規制やセキュリティのベストプラクティスに準拠する必要に迫られています。その結果、サポートする複数のプロトコル、テクノロジー、およびベンダーで構成された複合インフラストラクチャが登場してきました。

セキュリティの脆弱化から完全な機能停止に至るまでのパフォーマンスへの影響に対処するには、ネットワークのインフラストラクチャをセキュリティで保護し、一元的な方法で集中管理することが重要です。パフォーマンスへの影響があると、債務の増大、収益の減少、および生産性の低下につながるからです。

HP Network Automation (NA) は、ルータ、スイッチ、ファイアウォール、負荷分散機能、およびワイヤレスアクセスポイントの全体にわたり、これらの構成やソフトウェアの変更を追跡規定するエンタープライズクラスのソリューションです。NAは、ネットワークの変更情報を視覚的に提供して、問題となる可能性のある傾向をITスタッフが特定し、修正できるようにします。同時に、コンプライアンスに関する問題、セキュリティの危険、および災害復旧リスクを軽減させます。さらに、それぞれのデバイス変更についての監査証跡情報をすべてキャプチャします。

ネットワークエンジニアは、NAを使用して以下を特定できます。

- 変更されたデバイスの構成
- 構成に実際に加えられた変更項目
- 変更を行ったユーザ
- 変更が行われた理由

さらに、NAを使用して、構成を定義済みの標準に確実に準拠させることにより、ネットワークレベルでセキュリティポリシーや規制ポリシーを適用できます。結果として、標準や規定に準拠し、回復性と、保守性に優れたネットワークが構築されます。

NAは、HP、Cisco、Nortel、F5 Networks、Extremeなどの大手ベンダー製のデバイス群をサポートしており、ネットワークの変更プロセスを自動化することでネットワーク全体の管理性を高めます。NAのアーキテクチャは拡張性に優れており、大手のベンダー製のデバイスを組み込むことができるため、NAを使用してすべてのデバイスをサポートできます。

**注意：** NAのインストールまたはアップグレード方法については、『NA インストールおよびアップグレードガイド』を参照してください。

## NA 7.50の機能

NA 7.50には次の新機能が導入されました。

- **ベアメタルプロビジョニング**：デバイスを設置します。「ベアメタル」ドライバを使用することで、ベアメタルデバイスに対しスクリプトを実行して、本番ネットワークに完全構成されたデバイスを導入できます。
- **ネットワークデバイステンプレート**：実際のデバイスが存在しない場合でも、構成テンプレートを作成します。ネットワークデバイステンプレートを使用することで、本番ネットワークにデバイスを追加する前に、コンプライアンスの確認、ポリシールールの作成、構成の表示と比較（テンプレートと実際のデバイス間も可能）、パスワードルールの設定などを行えます。
- **セキュリティパーティション**：パーティションあたりのNAオブジェクトのセットを作成して、より細かな権限を指定します。NAのオブジェクトとしては、デバイス、ユーザ、コマンドスクリプト、デバイスパスワードルール、ポリシー、ソフトウェアイメージなどがあります。セキュリティパーティションは、権限モデル、グループ階層、複数のNAコアに渡るデバイスの配布、ネットワークのダイアグラムと組み合わせで使用できます。
- **自動修正スクリプト**：違反されたポリシールール内の正規表現パターングループからのデータを参照する、スクリプト内の変数を定義します。自動修正ポップアップウィンドウは、[ポリシールール]ページのデータにアクセスして、変数マッピングを表示し、サンプルコードを生成し、保存前にスクリプトを検証します。標準コマンドスクリプトとは異なり、自動修正スクリプトは新しい言語シンタックスを使用して一致を繰り返します。自動修正スクリプトは、処理され、ネットワークデバイス上で実行されるコマンドスクリプトへと変換されます。
- **NNMi統合**：NNMiとNAを統合することで、単一サーバ上に配置します。これにより、次のことを実行できます。
  - － NNMiからのデバイスポリシー準拠レポートの起動
  - － NNMiからのコマンドスクリプトと診断の起動
  - － NNMiのアウトオブザボックスのコマンドスクリプトと診断へのリンク
  - － 変更中のデバイスに対する非稼動中状態の指定
  - － NNMiへの変更されたコミュニティ文字列の自動プロパゲート
  - － 必須NNMi管理設定向けの新規デバイスの自動構成
  - － 通信モードおよび速度の不一致状態への警告
- **VoIPサポート**：VoIP管理の重要な要素には、以下があります。
  - － ネットワークデバイス内でのVoIP、MPLS、PoE、およびBGP構成要素の自動検出
  - － インターフェイスQoSとACL構成セクションは、自動的に解析され、特定インターフェイスのインターフェイス構成サマリに表示されます。
  - － 構成準拠チェックと基本的なデバイス診断を実行できるCisco CallManager用のデバイスドライバが用意されています。

- ゲートウェイサーバ上の Software Image Management (SWIM) プロセス : リモートデバイスの SWIM 中心データを表示します。ただし、リモートデバイスは、NA ゲートウェイ経由でのみ到達可能なデバイスとして定義されます。
- HP Operations Orchestration (OO) 統合 : NA とサードパーティベンダーのホストとの相互運用を可能にします。

## NA 7.60 の機能

NA 7.60 には次の新機能が導入されました。

- Solaris 64 ビットサポート : Solaris プラットフォームに NA をインストールすると、NA は 64 ビットの Java Virtual Machine (JVM) を使用します。その結果、NA はより多くのメモリを活用できます。
- 拡張されたタスクスケジューリング : タスクの作成または更新時に、他のタスクより高い優先順位で実行するようにタスクの優先順位を設定できるようになりました。タスクの優先度レベルは 1 ~ 5 であり、1 が最も高いタスク優先度レベルです。優先度の高いタスクは優先度の低いタスクより前に実行されます。また、グループタスクに新しいラウンドロビンアルゴリズムを使用することができます。たとえば、ラウンドロビンアルゴリズムを使用して、午前 10 時に 10,000 個のデバイスに対してグループタスクを開始し、午前 10 時 5 分に 10 個のデバイスに対してグループタスクを開始した場合、最初のタスクグループの完了を待たずに、2 番目のグループタスクを開始することができます。
- 拡張されたデバイス選択とデバイスグループ探索 : 拡張されたデバイス選択とデバイスグループ探索機能を使用すると、グループツリー内を容易に移動して各種アプリケーションのデバイスおよびデバイスグループを選択できます。
- 1 ポートでの複数 VLAN サポート : NA で x は、ネットワークスイッチ上の VLAN を表示およびプロビジョニングすることができます。NA を使用することにより、次のことが可能になります。
  - デバイスの VLAN の完全リストの表示
  - 特定の VLAN 詳細情報の表示
  - VLAN に割り当てられたポートリストの表示
  - トランクポートの表示
  - トランクポート上の VLAN リストの表示
  - トランクポートのネガティブ VLAN の表示 (トランクポート上にトラフィックを持つ VLAN にはタグが付きません)
  - ネットワークスイッチの VTP 設定の表示
  - ネットワークスイッチでの新規 VLAN の作成
  - VLAN に割り当てられたポートの変更 (ポートの追加/整理)
  - VLAN の削除
  - トランクポートとしてのポートの構成 (タグ付けされた複数の VLAN)
  - トランクポート VLAN の変更 (VLAN メンバーシップ)
  - トランクポートのネガティブ VLAN の変更
  - 非トランクとしてのトランクポートの構成
- 仮想デバイスと仮想コンテキストサポート : NA では、VMware のインフラストラクチャ (ESX) と Cisco Nexus 1000V シリーズスイッチを介して使用可能な VMware の仮想スイッチ (vSwitch) 技術などの仮想デ

バースに対応できるようになりました。これらの新しい仮想デバイスをレガシーデバイスとともに管理し、一元管理されたサポートを提供します。Cisco Firewall Services モジュール (FWSM) や Cisco ACE Application Control Engine モジュールなどの、仮想コンテキストをサポートするデバイスと同様に、仮想デバイスは、実際のハードウェアと仮想コンテキストの間の基本的な関係の表示ばかりでなく、非 IP アドレスコンテキストの管理も提供するデバイス関係の拡張機能によってさらに充実しました。

- デバイス関係：デバイス関係は親デバイス、ピアデバイス、および子デバイスのデータを保持します。新しい Device Relationships API によってデバイスの依存関係を定義できます。
- リンクアグリゲーションのサポート：リンクアグリゲーションのサポートにより、NA ではデバイス上の特定のポートに関連付けられたすべてのリンク（または接続）を一覧できます。この情報は、拡張された診断または新規デバイスコンテキスト情報から収集されます。リンクアグリゲーションを使用することによって、1 個の物理ポートに複数の接続を割り当てる仮想コンテキストを持つデバイスを管理できます。
- 接続パスの拡張：プライマリ IP アドレスを介したデバイスアクセスを有効または無効にできるようになりました。
- プロビジョニングおよびスクリプティング API の拡張：Device Relationships API を使用してデバイステンプレートの一覧、デバイステンプレート構成の表示、デバイステンプレート構成の変更、およびデバイスのプロビジョニングが可能になりました。

## NA 9.00 の機能

NA 9.00 には次の機能が導入されました。

- クイック起動：現在のページから移動しなくても、タスクをカスタマイズし、事前入力されたデータを使用してこれらのタスクを迅速に起動できるようになりました。
- タスクテンプレート：タスクテンプレートを使用することで、タスク定義を保存できるようになり、いちから作業を始めなくても、新しいタスクまたは既存のタスクを迅速に構成および実行できるようになりました。
- 合理化されたポリシーマネージャ：デバイスに適用するポリシーを表示できるようになりました。これにより、次のことを実行できます。
  - デバイスに適切なポリシーが適用されたことの確認
  - ポリシーが成功したか失敗したかの表示
  - NA にデバイスを追加した際にデバイスに適用されるポリシーの表示
  - デバイスに適用されたポリシーに対して適切に指定されている例外の表示
- Nmap ポートのスキャン：Nmap を使用してネットワークデバイスの検出ができるようになりました。また、Nmap を使用して、デバイスのポートをスキャンして、開いているポート、およびポートが提供するサービスの内容についての詳細を返すことも可能です。ポートスキャンタスクを実行すると、次のことを実行できます。
  - デバイス上のポートが開いているか閉じているかを容易に確認できます。
  - TCP スタック、OS 検出、および Nmap によって提供されるその他のサービスに基づいて、デバイスの脆弱性を確認できます。
- 構成ファイルの解析：ナビゲーションを簡単に行うために、構成ファイルのセクションを迅速に解析できるようにするためのリンクが備わりました。このリンクは、構成テキストの直前に配置されます。たとえば、構成ファイル内に [アクセスリスト] セクションが含まれている場合、構成ファイル上で [アクセスリスト] リンクをクリックすると、当該セクションに直接ナビゲートできます。ただし、現時点では、セクション解析をサポートしているのは Cisco IOS のジェネリックドライバのみです。

- SecurID ユーザデバイス認証：NA インストーラは、インストール時に `NA_DIRECTORY/jre` ディレクトリの `rsa_api.properties` をインストールします。NA がインストールされているサーバの IP アドレスと、RSA Server Authentication Manager によって生成される RSA 構成ファイルの場所を含めるように、このファイルを編集できます。
- FTP サーバのサポート：NA には統合 FTP サーバが備えられ、これにより NA はこのデバイスとの送受信を設定するために、デバイスへの通常のアクセスを CLI 経由で実行できるようになります。
- デバイスのアップタイム情報：デバイスのアップタイムの検索、およびデバイスに対してデバイスのブート検出診断の最後の実行日時を検索ができるようになりました。
- NA ユーザパスワードの有効期限 - ユーザプロファイルの新規作成時または既存のユーザプロファイルの編集時に、NA システム管理者の[ユーザを編集]ページと[ユーザの新規作成]ページに、次のオプションが表示されるようになりました。
  - － ユーザは次回ログイン時にパスワードを変更する必要あり
  - － ユーザによるパスワードの変更を禁止
  - － パスワードの有効期限なし
  - － アカウントをロックアウト
- NA 9.00 には、ナビゲーションを簡単に行うための新しいメインメニューのドロップダウンメニューや、更新された[自分のワークスペース]領域などの、より直観的なユーザインターフェイスが備えられています。
- CLI/API 内のカスタムデータフィールドの設定：これまでは、いくつかの CLI コマンドに、コマンドの「customname」と「customvalue」オプションを使用してカスタムフィールドを変更する機能がありましたが、一度に1つのフィールドしか処理できませんでした。これは、複数のフィールドを変更する必要がある場合面倒な作業でした。今回のバージョンでは、「customnames」と「customvalues」の新しい値を使用して、複数のフィールドを指定して同時に変更できるようになりました。
- 新しい検索とレポート作成アーキテクチャ：新しい検索とレポート作成アーキテクチャを使用すると、NA で検索結果をより迅速に表示できます。また、新しいデータタイプフィールドの追加、削除、変更を容易に実行できるようになりました。
- 改良されたログ記録とトラブルシューティング：トラブルシューティング情報をレポートする際にサーバログ、タスクログ、およびラッパーログについての詳細情報を提供できるようになりました。

## NA 9.10 の機能

NA 9.10 には次の機能が導入されました。

- オートパス：NA には2種類のライセンスがあります。
  - － インスタントオン：NA のインスタントオンライセンスは製品に付属しています。各インスタントオンライセンスには、デバイス250台、製品インストール後の試用期間60日間という制限があります。
  - － 永久：NA の永久ライセンスは、HP License Key Delivery Service から取得する必要があります。永久ライセンスには有効期限がなく、NA のいずれかのアドオン機能（Horizontal Scalability、Multimaster Distributed System など）と併せて使用できます。NA ライセンスの詳細については、『NA インストールおよびアップグレードガイド』を参照してください。

- デバイスグループの表示：その系統の親グループを基準にデバイスリストを表示できるようになりました。これによって、任意の親グループの視点からデバイスを一括編集できます。また、[デバイスグループ]ページをツリー表示できます。これは、複数のページによって構成されていたドリルダウンメニューに代わる新しいナビゲーションデザインです。
- 電子メール通知：ログインしているNAユーザとの間で電子メールを送受信できるようになりました。
- Policy Manager API：NA APIを使用してポリシーを作成できるようになりました。ポリシーの作成、ポリシー内のルール作成、ルールの修正スクリプトの作成、既存のポリシーの修正などのためのCLIコマンドがあります。詳細については、『NA CLI/API Command Reference』を参照してください。
- NNMiとNAの統合：NNMiとNAの統合コネクタは、NAでは使用していません。NNMiとNAの統合は、2つの製品間のWebサービスコールを通じて行います。NNMiとNAの新たな統合には、次の利点があります。
  - － 配布の簡易化
  - － トポロジ同期の信頼性の向上
  - － NNMiとNAの間での同期速度の向上
  - － NAとNNMiの間でのシングルサインオンのサポート（ログインし直さなくても2つの製品間の移動が可能）

HP NNMi と HP NA の統合を有効化するには、『HP Network Node Manager i Software - HP Network Automation Integration Guide (HP Network Node Manager iソフトウェア - HP Network Automation統合ガイド)』の手順に従います。

- SNMP v3のサポート：デバイス検出にSNMPv3を使用しているネットワークデバイスの検出が可能になりました。SNMPv3 プロトコルを使用すると、安全性の低いネットワークデバイス検出方法を回避でき、最新のSNMPのセキュリティメカニズムの使用が可能になります。

## NA 9.20の機能

NA 9.20には次の機能が導入されました。

- HP NNMiとHP NAの統合による改善
  - － 統合により、NAとNNMiの間でSSL接続がサポートされるようになりました。
  - － NNMi ノード、インターフェイス、インシデントフォームに、分析ペインのNA データ（現在のデバイス構成、構成履歴、インターフェイス構成）を含むタブが新しく加われました。

HP NNMi と HP NA の統合の詳細については、『HP Network Node Manager i Software - HP Network Automation Integration Guide (HP Network Node Manager iソフトウェア - HP Network Automation統合ガイド)』を参照してください。

- ユーザーデータのインポート：CSV ファイルからユーザおよびユーザグループ定義をインポートできるようになりました。
- デバイスデータのインポートに関する改善：CSV ファイルからデバイスおよびデバイスグループのカスタム属性をインポートできるようになりました。
- タスク完了時の通知：完了時に電子メールメッセージを送信するようにタスクを構成できるようになりました。
- Oracle RACのサポート

- 検索の向上
  - Oracle データベースのほとんどのフィールドで大文字小文字を区別しない検索が可能になりました (Microsoft® SQL Server および MySQL データベースサーバでは、検索時にデフォルトで大文字と小文字が区別されます)。
  - 「含む (全文)」 演算子により、デバイス構成の検索が高速になりました。
- データベースの整理の改善によって、NA データベースのサイズが徐々に小さくなります。
- PCI (旧 Visa CISP) 準拠レポートを更新しました。
- 必要なデータストレージの削減など、パフォーマンスが向上しました。
- Oracle GoldenGate を使用した災害復旧のための配布アーキテクチャが新たに加わりました。詳細については、『NA Disaster Recovery Configuration Guide』を参照してください。
- ドライバの改善
  - サポート対象の仮想デバイスが増えました。
  - IPv6 のサポートを追加しました。
  - JavaScript ドライバのため、PERL API をサポートしました。
  - SFTP クライアントをサポートしました。
  - タスク単位で強制的に構成を保存できるようになりました。
  - ファイルシステム診断およびソフトウェアセンターのため、ディレクトリ構造をサポートしました。
  - DSD\_Feature\_Index.html (各ドライバの機能一覧表と各ドライバの個別 DSD へのリンクを含むドライバの全リスト) が加わりました。
  - DSD\_SYSOID\_Mapping\_Index.html (ドライバパッケージ/ドライバ名/ドライバ説明ごとに、サポート対象/テスト済みのすべての sysOID が記載されたマスターリスト) が加わりました。

## ヘルプメニューオプション

[ヘルプ] ドロップダウンメニューには、次のオプションがあります。

- [ドキュメント]: [HP Network Automation ドキュメント] ページが開きます。ただし、コンテキスト依存のオンラインヘルプ情報は各 NA ページにある [ヘルプ] リンクから利用できます。
- [サポート]: [HP ソフトウェアサポート] ページが開きます。このサイトでは、HP の顧客に対して最新のパッチリリースとドキュメントが提供されます。また、問題の解決とトラブルシューティングのためにファイルをアップロードすることもできます。
- [HP Live Network]: [HP Live Network] ページが開きます。このページでは、セキュリティアラートサービスデータと他の NA コンテンツサービスの資料をダウンロードできます。HP Live Network とは、HP Network Automation に統合され、定期的なネットワークセキュリティとコンプライアンスコンテンツの更新を配信可能な、補完的なコンテンツ配信サービスです。



また、HP Live Networkのポータルでは、以下をホストしています。

- － ドライバパック
- － 特殊なNDSドライバ開発フォーラム
- － 一般的なNAコミュニティフォーラム

HP Live Networkのセキュリティとコンプライアンスサービスにより、ネットワークセキュリティとポリシー違反の即時評価、および自動化された修復オプションが利用できます。HP Live Networkには、無料コンテンツやサブスクリプションサービスが含まれています。詳細については、「[ソフトウェアの脆弱性レポート](#)」(616ページ)を参照してください。

**注意：** HP Live Network Serviceのインストール方法については、『NA インストールおよびアップグレードガイド』を参照してください。

- HP Network Automationについて - [HP Network Automationについて]ページを開きます。ここでは、HP Network Automationについての情報を表示できます。[HP Network Automationについて]ページの詳細については、「[最新ソフトウェアバージョンの表示](#)」(30ページ)を参照してください。

## NAホームページ

ユーザがNAにログインすると、常にNAホームページが開きます。各ページの左上隅にある[ホーム]リンクをクリックして、NAホームページに戻ることもできます。

NAホームページには2つのフレームが含まれます。左側のフレームには以下が含まれます。

- 検索：検索オプションを使用すると、ホスト名またはIPアドレスによってデバイスを検索し、それらのデバイスにTelnetまたはSSH経由で接続できます。詳細については、「[検索/接続機能](#)」(273ページ)を参照してください。
- 自分のワークスペース：[自分のワークスペース]領域には、次のセクションが含まれます。
  - － 現在のデバイス/現在のデバイスグループ ([インベントリ]がデフォルトです)
  - － 自分のお気に入り
  - － クイック起動
  - － 自分の設定

[自分のワークスペース]領域のオプション設定の詳細については、「[ユーザ設定の編集](#)」(260ページ)を参照してください。

右側のフレームは、過去24時間以内に発生した最近の構成変更のスナップショット、さまざまなシステムイベント、承認が必要なタスクなどを含めるようにカスタマイズできます。詳細については、「[NA ホームページのカスタマイズ](#)」(269ページ)を参照してください。

## コマンドウィンドウを開く

コマンドウィンドウを開くには、ディスプレイの左側の[検索]タブでデバイスのIPアドレスかホスト名を入力し、[接続]ボタンをクリックします。また、[接続]メニューを使用して[デバイス詳細]ページからもコマンドウィンドウを開くことができます。コマンドウィンドウ内では、コピーするテキストを選択し、[Return]キーを押します。強調表示されたテキストがコピーバッファに格納されます。次にそのテキストを別のアプリケーションに貼り付けます。作業が終了したら、「exit」と入力してウィンドウを閉じます。

**注意：** Telnet/SSH プロキシを使用して直接デバイスに接続している場合は、デバイスを終了しても Telnet/SSH プロキシ内に留まったままになります。「exit」ともう一度入力するまでは、CLI コマンドを入力して他のデバイスに接続できます。

CLI コマンドのヘルプを参照するには、「help」と入力してすべてのコマンドリストを参照してください。特定のコマンドの詳細なヘルプを表示するには、「help <コマンド名>」と入力します。

## ドキュメントへのアクセス

コアとなる NA ドキュメントセットの内容は以下のとおりです。

- 『NA ユーザガイド』: PDF バージョンを表示するには、ログイン後に、[ヘルプ] ドロップダウンメニューで [ドキュメント] をクリックします。[HP Network Automation ドキュメント] ページが開きます。リストから [HP Network Automation ユーザガイド] を選択します。
- NA ヘルプファイル: オンラインヘルプファイルを表示するには、ログイン後に、任意のページの先頭にある [ヘルプ] リンクをクリックします。
- 『NA インストールおよびアップグレードガイド』: PDF バージョンを表示するには、ログイン後に、[ヘルプ] ドロップダウンメニューで [ドキュメント] をクリックします。[HP Network Automation ドキュメント] ページが開きます。リストから [HP Network Automation インストールおよびアップグレードガイド] を選択します。
- 『NA Release Notes』: PDF バージョンを表示するには、ログイン後に、[ヘルプ] ドロップダウンメニューで [ドキュメント] をクリックします。[HP Network Automation ドキュメント] ページが開きます。リストから [HP Network Automation Release Notes] を選択します。

以下にリストしたドキュメントを含む追加の NA 出版物を入手するには、NA サポートサイトにアクセスしてください。

- 『NA Multimaster Distributed System on Oracle Guide』
- 『NA Multimaster Distributed System on SQL Server Guide』
- 『NA Horizontal Scalability Guide』
- 『NA Satellite Guide』

# HP Network Automation ユーザガイド

このガイドでは、次について説明します。

- システムの設定と構成
- デバイスおよびデバイスグループの追加と設定
- ユーザ、グループ、およびロールの追加
- ワークフローの作成
- SecurID、TACACS+、およびRADIUSによるネットワークデバイスへのアクセス
- LDAPからのユーザおよびユーザグループのインポート
- アクセス制御リスト（ACL）の管理
- コンプライアンスセンターの使用
- 情報の検索、カスタムレポートの作成、およびサマリレポートの実行
- 構成の配布
- VLANの表示およびプロビジョニング
- デバイス関係の構成
- イベントルールとイベント通知の作成
- デフォルトの診断の表示
- 診断およびコマンドスクリプトの作成および実行
- 不整合を防止する企業全体のポリシールールの作成
- 中央リポジトリからのデバイスソフトウェアの配布
- TelnetおよびSSH経由でのデバイスへの接続
- コマンドラインインターフェイス（CLI）の実行
- JavaおよびPERL APIを使用した他のITアプリケーションとのデータ交換
- オンラインヘルプの使用、顧客サポートへの問い合わせ、およびソフトウェアライセンスの更新

**注意：**『NA ユーザガイド』には、NA システム管理者が使用可能なすべてのオプションについての情報が記載されています。ユーザに与えられている権限に応じて、一部のNAメニューオプションはグレー表示されます。

## このドキュメントでの表記規則

次の表は、このガイドで使用している表記規則を示します。

規則	説明/アクション
斜体	システムメッセージ、パス、ファイル名、およびWeb URLなどに使用します。たとえば、 <i>C:\hp\sdk\docs</i> 。
<u>リンク</u>	これをクリックすると、ドキュメント内の別の場所に移動したり、Web ページを開いたり、新しい電子メールメッセージを開いたりします。このガイドでは、相互参照先とページ数をそれぞれ鍵かっこで囲んで示し、URL および電子メールアドレスへのリンクを下線付きテキストで表記します。
Enter	テキストまたは後続のコマンドを入力してからキーボードのEnterキーを押すことを示します。
< >	ユーザが入力する必要があるフォルダ名などの変数情報を示します。プレースホルダを置き換える場合は、山かっこを含めないように注意してください。

## [トラブルシューティングの送信]ページのフィールド

顧客サポートにトラブルシューティング情報を送信するには：

1. [管理]のメニューバーで、[トラブルシューティング]をクリックします。[トラブルシューティング]ページが開きます。
2. ページの先頭にある[トラブルシューティング情報の送信]へのリンクをクリックします。[トラブルシューティング情報の送信]ページが開きます。

**注意：** ログファイルにアクセスするには、管理権限を持つ必要があります。

フィールド	説明/アクション
宛先	表示されていない場合に、自分の電子メールアドレスを入力します。
件名	件名には、「HP Network Automation Info」と表示されます。
問題番号	オープンチケットに関する問題番号がある場合は入力します。
コメント	問題についてのコメントを入力します。返信先の電子メールアドレスと直通の電話番号（または携帯電話の番号）は、必ず入力してください。ファイルにある連絡先情報が正確でない、または問題がユーザに固有でない場合もあります。
対象	<p>次の中からオプションを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• [過去&lt;&gt;時間のサーバログ]：送信するログの記録期間を時間単位で入力します。デフォルト値は4です。</li> <li>• [システム管理設定]：NAサーバの管理設定とオプションが集められています。</li> <li>• [システムステータスファイル]：システムステータス情報を提供するために作成されたファイルです。</li> <li>• [ラッパログ]：要求された場合は、これによりJboss_Wrapperログファイルを送信します。</li> <li>• タスクログ：利用できるタスクログファイルのリストです。各ファイルには、タスクのタイプ、タスクID、デバイス（存在する場合）、およびタスクの完了時刻が表示されます。</li> </ul>

入力したら、[送信]をクリックします。

**注意：** [トラブルシューティング情報のダウンロード]ページでは、トラブルシューティング情報をダウンロードできます。このページは、[トラブルシューティング情報の送信]ページと同じですが、[宛先]、[件名]、[問題番号]、または[コメント]フィールドがありません。また、[送信]ボタンは[ダウンロード]ボタンとなります。

## 最新ソフトウェアバージョンの表示

[HP Network Automation について] ページを表示するには、[ヘルプ] ドロップダウンメニューで、[HP Network Automation について] をクリックします。[HP Network Automation について] ページが開きます。

現在のNAソフトウェアバージョンについての詳細情報が表示されます。また、次のリンクもあります。

- ドライバ更新パッケージのダウンロード：HP BSA Essentials Network Webサイトを表示します。
- 最新のリリースノートを表示：HP パスポートへのサインインページを表示します。
- ライセンス情報を表示：詳細については、[「ライセンス情報の表示」\(30 ページ\)](#) を参照してください。
- 顧客サポートに連絡：ソフトウェアサポートオンラインWebサイトを表示します。
- システム構成を表示：詳細については、[「\[システム構成を表示\] ページ」\(31 ページ\)](#) を参照してください。

システムにインストールされているデバイスドライバのリストもあります。サポートされるデバイスの詳細については、Driver Release Service (DRS) ドキュメントを参照してください。DRSは、ドライバの自動リリースおよび配信システムです。

## ライセンス情報の表示

[ライセンス情報] ページでは、次の情報を確認できます。

- 製品のライセンス先
- ライセンスされているノード数
- 使用中のノード数
- ライセンスの期限切れ

このページからライセンスを更新することもできます。

[ライセンス情報]ページを表示するには、次の手順に従います。

1. [ヘルプ]ドロップダウンメニューで、[HP Network Automationについて]をクリックします。[HP Network Automationについて]ページが開きます。
2. [ライセンス情報を表示]へのリンクをクリックします。[ライセンス情報]ページが開きます。

フィールド	説明/アクション
製品	使用ライセンスを与えられているソフトウェアバージョンが表示されます。
ライセンス先	ユーザの企業または部署の名前が表示されます。
ライセンスされているノード数	ソフトウェアが認識できるノード数が表示されます。Cisco 6500などの一部のデバイスには、別々のノードとして動作するカードが搭載されています。
使用中のノード数	NAでアクティブ化されているノードの数が表示されます。
ライセンスの期限切れ	ソフトウェアの有効期限が表示されます。
[ライセンスを更新]ボタン	ソフトウェアライセンスの更新時期になると、HPから新しいライセンステキストが送信されます。テキストをボックスに貼り付けてから、[ライセンスを更新]をクリックして新規ライセンスをインストールします。

## [システム構成を表示]ページ

分散システムが有効で、NAコアを設定している場合は、[システム構成を表示]ページで次の情報を確認できます。

- 構成されているNAコアの数
- 構成されているパーティションの数

IPネットワークの重複、および制限されるデバイスとユーザビューの詳細については、「**デバイスとユーザのセグメント化**」(148 ページ) を参照してください。Multimaster Distributed System のインストール方法と構成方法の詳細については、『NA Multimaster Distributed System on Oracle Guide』、または『NA Multimaster Distributed System on SQL Server Guide』を参照してください。





## 第2章：管理設定の構成

### トピックの参照先リスト

トピック	参照先：
はじめに	<a href="#">「はじめに」</a> （34 ページ）
構成管理	<a href="#">「構成管理」</a> （35 ページ）
デバイスアクセス	<a href="#">「[デバイスアクセス]ページのフィールド」</a> （45 ページ）
サーバ	<a href="#">「サーバ」</a> （52 ページ）
ワークフロー	<a href="#">「ワークフロー」</a> （59 ページ）
ユーザインターフェイス	<a href="#">「ユーザインターフェイス」</a> （61 ページ）
Telnet/SSH	<a href="#">「Telnet/SSH」</a> （65 ページ）
レポート作成	<a href="#">「レポート作成」</a> （68 ページ）
ユーザ認証	<a href="#">「ユーザ認証」</a> （73 ページ）
LDAP 認証の設定	<a href="#">「LDAP 外部認証の設定」</a> （80 ページ）
サーバ監視	<a href="#">「サーバ監視」</a> （83 ページ）
サードパーティ統合	<a href="#">「サードパーティ統合」</a> （87 ページ）
監視結果の表示	<a href="#">「監視結果の表示」</a> （89 ページ）
サービスの開始および停止	<a href="#">「サービスの開始および停止」</a> （94 ページ）
ログ記録	<a href="#">「ログ記録」</a> （96 ページ）
デバイスドライバのレビュー	<a href="#">「ドライバのレビュー」</a> （101 ページ）

## はじめに

システム管理者として、NAの操作に影響する構成可能な設定値を定義できます。これらの設定はインストール中に初期値のまま構成されますが、値を変更して機能をカスタマイズすることも可能です。たとえば、さまざまな操作に関連付けられている間隔のデフォルト値を変更する、あるいはスクリプト言語のサポートなどを構成できます。また、特定のページの外観や内容のカスタマイズも可能です。

構成オプションを確認して変更を行うには、[管理]のメニューバーから[システム管理設定]を選択します。次のオプションを選択できます。

- 構成管理
- デバイスアクセス
- サーバ
- ワークフロー
- ユーザインターフェイス
- Telnet/SSH
- レポート作成
- ユーザ認証
- サーバ監視
- サードパーティ統合

## 構成管理

[構成管理]ページでは、次の構成が可能です。

- 構成変更の検出
- ユーザID
- スタートアップとランニング構成
- ACL解析と編集
- 構成ポリシーの検証
- タスク前とタスク後のスナップショット
- 診断
- フラッシュ記憶域容量
- ブートの検出
- カスタムサービスタイプ

[構成管理]ページを表示するには、[管理]メニューバーから[システム管理設定]を選択し、[構成管理]をクリックします。[構成管理]ページが開きます。変更を保存するには、必ず[保存]をクリックしてください。

## [構成管理]ページのフィールド

フィールド	説明/アクション
変更の検出	
変更の検出	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>有効：変更が検出されたときは常にスナップショットが作成されます（デフォルト）。</li> <li>ポーリングのみ：デバイス グループのスナップショット時にはスナップショットが作成されますが、変更の検出時には作成されません。</li> <li>無効：変更の検出に応じて、またはデバイス グループのスナップショット時に構成のスナップショットが作成されません。</li> </ul> <p>変更の検出の詳細については、「<a href="#">変更の検出</a>」（41ページ）を参照してください。</p>
変更検出間隔	<p>変更の検出とスナップショット作成の間の待ち時間を入力します。デフォルトでは10分です。NAにより変更が検出されると、ここで指定する間隔で、デバイスのスナップショット作成に遅延が生じます。以降のスナップショット作成でも、この間隔で送信されるすべての変更の通知が反映されます。</p>
Syslogの検出パターン	<p>NAで指定されているデフォルトのパターンに新しいパターンを追加したい場合、右側のボックスに追加したいパターンを入力して[パターンを追加&lt;&lt;]をクリックします。パターンを削除するには、左側のボックスからパターンを選択して[パターンを削除]をクリックします。NAは、Syslogサーバを検索してこれらのパターンとの一致を探します。上記のオプションが有効な場合、一致が見つかったと、構成が変更されていてデバイス構成のスナップショットが作成されていることを示します。（<b>注意</b>：HPにはSyslogサーバが搭載されています。NAのインストール時に現在のSyslogサーバがそのまま維持されている場合、NA Syslogサーバをインストールして、NA SyslogサーバへのSyslogメッセージを中継します。）</p> <p>Syslogメッセージパターンの詳細については、「<a href="#">Syslogメッセージ</a>」（42ページ）を参照してください。</p>
無視するSyslogパターン	<p>パターンを無視する場合、右側のボックスにそのパターンを入力して[パターンを追加&lt;&lt;]をクリックします。パターンを削除するには、左側のボックスからパターンを選択して[パターンを削除]をクリックします。</p>
セカンダリIPタイプ	<p>セカンダリIPタイプを選択します。デフォルトでは、「プライマリ」と「代替」が選択されています。セカンダリIPタイプは、セカンダリIPアドレスの変更検出Syslogイベント処理に使用されます。ただし、すべてのセカンダリIPアドレスがSyslogイベント処理に含まれる訳ではないので注意してください。次のオプションから選択できます。</p> <ul style="list-style-type: none"> <li>プライマリ</li> <li>代替</li> <li>コンソール</li> <li>ホップボックス</li> <li>NAT</li> <li>接続スルー</li> <li>内部スルー</li> <li>内部ダイレクト</li> </ul> <p>IPアドレス管理の詳細については、「<a href="#">[デバイス管理対象IPアドレス]ページのフィールド</a>」（232ページ）を参照してください。</p>

フィールド	説明/アクション
Syslogメッセージの送信者のIPアドレスを使用	オンにすると、Syslogメッセージの送信者のIPアドレスが使用されます。
変更検出時に無視するユーザ	SyslogまたはAAA変更イベントを処理する場合に無視するユーザを示します。ユーザを追加するには、ユーザ名を右側のボックスに入力して[ユーザ名を追加<<]をクリックします。ユーザを削除するには、左側のボックスからユーザ名を選択して[ユーザ名を削除]をクリックします。
<b>ユーザIDの変更</b>	
ユーザを自動作成	オンにすると、構成変更の実行者が存在しない場合に新しいユーザが作成されます。
自動作成ユーザのサフィックス	自動作成機能により追加された新しいユーザに付くサフィックスを入力します。デフォルトでは「_auto」です。
Syslogユーザの特定	オンにすると、Syslogメッセージからユーザの特定を試みます。
syslogユーザパターン	<p>SyslogユーザパターンはJava正規表現です。キャプチャグループを正規表現に追加し、ユーザ名の存在箇所を示します。例：</p> <ul style="list-style-type: none"> <li>• 認証されたユーザ(\S+)</li> <li>• ユーザ(\S+)の開いたセッション</li> <li>• ユーザ(\S+)の成功したログイン</li> </ul>
	NAはこれらのパターンを使用して、構成変更を担当するユーザを判断します。
	右側のボックスにパターンを入力して[パターンを追加<<]をクリックします。パターンを削除するには、左側のボックスからパターンを選択して[パターンを削除]をクリックします。NAでは、Syslogサーバを検索してこれらの正規表現との一致を探します。一致が見つかったら、ユーザとしてそのテキストをキャプチャします。通常、デバイスドライバがこれらのパターンを入力します。
SyslogからワークステーションのIPアドレスを解決	オンにすると、SyslogメッセージからIPアドレスが解決され、関連する構成の変更を行ったユーザ名としてドメイン名が扱われます。この方法は、Syslogメッセージから他の方法でユーザ名が判断できない場合にのみ使用されます。
未解決のIPアドレスを格納	オンにすると、DNSを使用するホスト名が解決されない場合に、そのIPアドレスがユーザ名として扱われます。ピリオドはダッシュ(-)記号に置き換えられます。たとえば、ユーザ10.10.1.1を10-10-1-1となります。
Syslogからユーザを自動作成	このオプションと[ユーザを自動作成]オプションが両方オンになっている場合、Syslogメッセージから識別したユーザと既存のユーザの一致を試みます。既存のユーザが存在しない場合、新しいユーザが作成されます。

フィールド	説明/アクション
<b>スタートアップとランニング構成</b>	
スタートアップ構成をキャプチャ	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• オフ：スタートアップ構成をキャプチャしません。</li> <li>• 検出のみ：比較のためにスタートアップ構成をキャプチャしますが、保存しません。</li> <li>• オン（デフォルト）：スタートアップ構成をキャプチャ、比較、格納します。すべてのベンダーおよびデバイスがスタートアップ構成の概念に対応しているわけではありません。</li> </ul>
<b>ACL解析</b>	
各スナップショットでACLデータを解析	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 有効：各スナップショットでACLデータを解析して格納します。</li> <li>• 無効：各スナップショットでACLデータを解析しません。</li> </ul> <p>このオプションにより、新しいデバイスを追加したときに、この機能のデフォルトの状態が設定されます。一括編集を使用して、デバイスグループに対するACL解析のオンとオフを切り替えることができます。（<b>注意</b>：このオプションよりも、デバイスごとの設定の方が優先されます。）</p>
<b>ACL編集</b>	
編集前のアプリケーションスクリプトの表示	オンにすると、ACLの編集または作成時に編集前のACLアプリケーションスクリプトが表示されます。編集前のアプリケーションスクリプトでは、デバイスにあるACLの既存のアプリケーションが無視されます。新規または更新済みのACLスクリプトにより、編集済みのACLがデバイスに追加されます。
準備スクリプトの編集の表示	オンにすると、ACLの編集または作成時に準備スクリプトの編集が表示されます。準備スクリプトは、編集済みACLを承認するデバイスの準備に必要なスクリプト処理を実行します。
アプリケーションスクリプトを表示	オンにすると、ACLの編集または作成時にアプリケーションスクリプトが表示されます。アプリケーションスクリプトは、VTY接続などのACLの適用に使用するスクリプトです。アプリケーションスクリプトにより、ACLが再適用されます。
<b>構成ポリシーの検証</b>	
デフォルトで配布する前に検証	オンにすると、配布前に定義済みの構成ポリシーに対して編集済みの構成がチェックされます。
パターンのタイムアウト	構成のパターンマッチングの最大許容秒数を入力します。デフォルト値は30秒です。
自動修正スクリプトの実行	オンの場合、ルールが非準拠と判断された後に、自動修正スクリプトを自動的に実行するかどうかを制御します。自動修正スクリプトの詳細については、「 <b>自動修正スクリプトの作成</b> 」（581 ページ）を参照してください。
インベントリグループにインポートされるポリシーを自動的に適用	オンの場合、インポートされるすべてのポリシーがインベントリグループに適用されます。

フィールド	説明/アクション
<b>タスク前とタスク後のスナップショット</b>	
ユーザによるタスク前/後のスナップショットの無効化	<p>オンにすると、ユーザが個々のタスクを実行するときに、デフォルトのタスク前後のスナップショット設定よりもユーザ設定のスナップショットを優先できます。優先が許可されると、適用可能な場合は、[タスクの新規作成]ページにタスク前後のスナップショットオプションが表示されます。優先が許可されていない場合、デフォルトの設定が使用されます（詳細については、「<a href="#">タスク前とタスク後のスナップショットの構成</a>」(43ページ)を参照してください）。</p>
スクリプトごとにタスク前/後のスナップショット設定のヒントを許可	<p>オンにすると、個々のスクリプトでタスク前後のスナップショット設定を優先できます。</p> <p><b>注意：</b>タスク前のスナップショット設定よりも優先させる場合、タスク前のスナップショットを要求するにはスクリプトに "tc_pre_snapshot=true" というテキストのコメントを含めます。タスク前のスナップショットを要求しない場合、"tc_pre_snapshot=false" を含めます。タスク後のスナップショット設定よりも優先させる場合、タスクの一部としてタスク後のスナップショットを要求するにはスクリプトに "tc_post_snapshot=true" というテキストのコメントを含めます。別のタスクとしてタスク後のスナップショットを要求するには "tc_post_snapshot=task" を、タスク後のスナップショットを要求しない場合、"tc_post_snapshot=false" を含めます。</p> <p>詳細については、「<a href="#">タスク前とタスク後のスナップショットの構成</a>」(43ページ)を参照してください。</p>
コマンドスクリプト実行前のスナップショット	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>なし（デフォルト）</li> <li>タスクの一部として</li> </ul>
コマンドスクリプト実行後のスナップショット	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>なし</li> <li>タスクの一部として（デフォルト）</li> <li>個別のタスクとしてスケジュール</li> </ul>
構成配布前のスナップショット	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>なし</li> <li>タスクの一部として（デフォルト）</li> </ul>
構成配布後のスナップショット	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>なし</li> <li>タスクの一部として（デフォルト）</li> <li>個別のタスクとしてスケジュール</li> </ul>
デバイスのプロビジョニング後のスナップショット	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>なし</li> <li>タスクの一部として（デフォルト）</li> <li>個別のタスクとしてスケジュール</li> </ul>
診断実行前のスナップショット	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>なし（デフォルト）</li> <li>タスクの一部として</li> </ul>

フィールド	説明/アクション
診断実行後の スナップショット	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>なし（デフォルト）</li> <li>タスクの一部として</li> <li>個別のタスクとしてスケジュール</li> </ul>
ACL削除前の スナップショット	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>なし</li> <li>タスクの一部として（デフォルト）</li> </ul>
ACL削除後の スナップショット	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>なし</li> <li>タスクの一部として（デフォルト）</li> <li>個別のタスクとしてスケジュール</li> </ul>
スタートアップと ランニング構成の同期後の スナップショット	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>なし（デフォルト）</li> <li>タスクの一部として</li> <li>個別のタスクとしてスケジュール</li> </ul>
タスク後スナップショット の待ち時間	個別のスナップショットタスクとして実行されるタスク後のスナップショット（ある場合）の遅延を入力します。デフォルト値は30秒です。
<b>診断</b>	
トポロジデータの 収集頻度	トポロジデータは、ネットワークパフォーマンスを維持するために調整が必要な診断の新しいクラスに追加されます。トポロジデータは、ネットワーク図のレンダリングに使用します。トポロジデータの収集は、NAサーバに大きな負荷がかかるため、できるだけ頻度を少なくする必要があります。トポロジデータの収集を許可する最小間隔を時間単位で入力します。デフォルトでは168時間です。
格納された トポロジデータ	現在データベースに格納されているトポロジデータの許容期限を時間単位で入力します。格納データがこの値より古い場合、データはデバイスから直接取得されます。それ以外の場合、格納データが使用されます。デフォルトでは72時間です。
通信モードデータの 収集頻度	通信モードの不一致は、ネットワークパフォーマンスを維持するために調整が必要な診断の新しいクラスに追加されます。通信モードの不一致データは、一般的なエンドツーエンドのパフォーマンスの問題の識別に使用します。あるマシンが全二重で別のマシンが半二重に設定されていると、多くの場合重複の不一致が複数回発生します。重複の不一致データの収集は、NAサーバに大きな負荷がかかるため、できるだけ頻度を少なくする必要があります。通信モードデータを収集する最小間隔を時間単位で入力します。デフォルトでは168時間です。
格納されている 通信モードデータ	現在データベースに格納されている通信モードデータの許容期間を時間単位で入力します。格納データがこの値より古い場合、データはデバイスから直接取得されます。それ以外の場合、格納データが使用されます。デフォルトでは72時間です。
<b>フラッシュ記憶域容量</b>	
フラッシュ低容量イベント	オンにすると、検出された使用可能なフラッシュ記憶域容量が低いと検出された場合にイベントが生成されます。
フラッシュ低容量の しきい値	低容量イベントが生成される条件となるフラッシュ記憶域容量の使用割合を入力します。デフォルトは90%です。



フィールド	説明/アクション
<b>ブートの検出</b>	
エラーマージン係数	デバイスのブートが検出された場合に許可するクロックドリフト数（6時間ごとの秒単位）を入力します。デバイスの確認を行う最小頻度は、6時間ごととすることをお勧めします。
<b>カスタムサービスタイプ</b>	
カスタムサービスタイプ	サービスタイプを追加したり削除します。サービスタイプは、デバイスにVoIP、BGP、MPLSなどを指定できます。この値により、デバイスの用途を判断できます。サービスタイプの詳細については、「 <a href="#">デバイス詳細の表示</a> 」（193 ページ）を参照してください。

## 変更の検出

NAは、デバイス構成の変更を検出するため、次の示す複数の方法を使用します。

- Syslog メッセージ
- AAA ログの読み出し
- 内部プロキシ

NAでは、これらの方法によりさまざまな情報を入手して、実際にデバイスの変更を行ったユーザを特定します。この情報により、変更を行った可能性が最も高いユーザを特定できます。優先順位に応じて、次の情報を利用します。

- デバイスで実行されたパスワード変更をスケジュールしたユーザ
- デバイスで実行されたソフトウェア更新をスケジュールしたユーザ
- デバイスに構成を配布したユーザ
- デバイスでスクリプトを実行したユーザ
- NA プロキシ経由でデバイスに接続したユーザ
- AAA ログから収集されたユーザ情報
- syslog メッセージから分析されたユーザ情報

NAは、優先度リストの上位にあるデバイス対話に対して変更属性を割り当てます。たとえば、あるユーザがパスワード変更をスケジュールリングし、同じ期間に別のユーザがデバイスにプロキシした場合、変更が検出されると、その変更はパスワード変更をスケジュールリングしたユーザに割り当てられます。

デバイスの構成の変更を表示するには：

1. [デバイス]メニューで、[インベントリ]をクリックします。現在管理されているデバイスのリストがすべて開きます。
2. 構成の変更を表示したいデバイスをクリックします。[デバイス詳細]ページが開きます。
3. [表示]ドロップダウンメニューから[構成変更]をクリックします。
4. [変更者]列で詳細リンクをクリックします。[ユーザ属性の詳細]ページが開きます。

## Syslog メッセージ

NA コア Syslog サーバは、システムで使用中のドライバの Syslog パターンリストに一致する NA コアに Syslog メッセージを転送します。ドライバの検出タスクを実行すると、このタスクが、検出した Syslog メッセージパターンリストを更新し、NA Syslog サーバに対してその Syslog メッセージパターンリストを更新するよう指示を出します。

NA サテライト Syslog サーバも同様の処理を実行します。NA サテライト Syslog サーバには、使用中のデバイスの Syslog メッセージパターンリストが格納されていますが、NA サテライト Syslog サーバはこれらのパターンの1つに一致する NA コアにのみこのメッセージを転送します。その結果、リモートエージェントの配布タスクを実行すると、次のメッセージが表示されます。Initialized Satellite with *N* syslog change detection patterns from Core.

最初の NA サテライトは、現在の Syslog メッセージパターンリストを受け取ります。後続するドライバの検出タスクは、新しいデバイスを検出しそれに新しい Syslog パターンが必要な場合、NA コア Syslog サーバと NA サテライト Syslog サーバの両方に通知します。

## [ユーザ属性の詳細] ページのフィールド

**注意：**一部の構成変更は「ユーザ」に割り当てることができず、「N/A」とすることができます。

フィールド	説明/アクション
<b>イベントの詳細を変更</b>	
ユーザ	変更を行ったユーザの名前が表示されます。
日付	変更が行われた日付が表示されます。
デバイス対話	Syslog など、変更の検出に使用する方法が表示されます。
追加詳細	変更がコンソールから行われたかどうかなど、変更に関する追加詳細が表示されます。

## タスク前とタスク後のスナップショットの構成

タスク前後のスナップショットを構成すると、次のことが可能になります。

- さまざまな種類のタスクに対して、タスク前後のスナップショットの動作を定義する
- タスク後のスナップショットを個別のタスクとして実行する
- 特定のタスクを実行する場合に、デフォルトのタスク前後のスナップショットの動作を優先する

次のタスクに対してタスク前後のスナップショットオプションを表示できます。

- 構成を配布（「[\[構成を配布\]タスクページのフィールド](#)」（181ページ）を参照）
- 診断の実行（「[\[診断の実行\]タスクページのフィールド](#)」（310ページ）を参照）
- ACLの削除（「[\[ACLの削除タスクページ\]](#)」（708ページ）を参照）
- スタートアップとランニングの同期（「[\[スタートアップとランニングの同期\]タスクページのフィールド](#)」（319ページ）を参照）
- コマンドスクリプトの実行（「[\[コマンドスクリプトの実行\]タスクページのフィールド](#)」（304ページ）を参照）
- ACL行の一括挿入（「[\[ACL行の一括挿入\]](#)」（702ページ）を参照）
- ACL行の一括削除（「[\[ACL行の一括削除\]](#)」（702ページ）を参照）

コマンドスクリプトにスナップショットのヒントを提供すると、スクリプトの実行時に、タスク前後のスナップショットの動作を指定する特別なタグをコマンドスクリプトに追加できます。たとえば、実際にはデバイスに接続されていない、またはデバイスを変更しない高度なスクリプトがあるとします。このような高度なスクリプトでは、デバイスに関する情報を抽出してレポート生成するためだけにNA APIを使用することができます。その場合、タスクの実行後にスナップショットを作成する必要がないため、高度なスクリプトにタスク後のスナップショットが不要であることを示すタグを追加できます。

デバイスグループに対して複数のスクリプトが実行されるように選択されており、ヒントが含まれているスクリプトが複数ある場合、指定した動作の中で最も無難な動作が実行されます。

## デバイスアクセス

[デバイスアクセス]ページでは、次のことが可能です。

- デバイスの接続方法を指定する
- ネットワークデバイスの検出のタスク設定を構成する
- 要塞ホスト設定を構成する
- SecurID デバイスアクセスを構成する
- SSH デバイスアクセスを構成する
- タスク単位でデバイスアクセスに使用する資格情報を指定する
- Nortel BayRS MIB/OS のバージョンを指定する
- ゲートウェイメッシュ情報を入力する

ネットワーク環境は、多くの場合ネットワークファイアウォールで保護されています。NA では、次の4つの方法によりファイアウォール経由でデバイスにアクセスします。

- ファイアウォール経由でダイレクトアクセスを開く。
- ファイアウォールでネットワークアドレス変換 (NAT) を作成し、NAT を使用してデバイスにアクセスするよう NA を構成します。NAT を使用するデバイスの構成に NAT アドレスは表示されません。
- ファイアウォールの対極で既存の要塞ホストを使用して管理要求をプロキシするよう NA を構成します。要塞ホストは既にファイアウォール経由でのアクセスが許可されているため、要塞ホストを設定すると、その要塞ホストのプロキシ接続経由でデバイスを管理できるようになります。
- ゲートウェイメッシュを使用します。(詳細については、『NA Satellite Guide』を参照してください)。

コンソールサーバでは、シリアル接続を使用した物理接続が維持されます。これらの接続はTelnet経由で行われ、コンソールサーバでホストされる IP ポート番号を指定します。コンソールサーバ接続は、ネットワークデバイスがネットワークから切断されても使用可能です。

[デバイスアクセス]ページを表示するには、[管理]メニューバーから[システム管理設定]を選択し、[デバイスアクセス]をクリックします。[デバイスアクセス]ページが表示されます。

## [デバイスアクセス]ページのフィールド

フィールド	説明/アクション
デバイス接続方法	
パスワードの選択	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>常に最後に成功したパスワードから試行する。：このフィールドのチェックボックスをオンにすると、前のデバイスアクセスから、最終成功パスワードを常に最初に試行します。タスクの途中で最終成功パスワードを変更しても、そのタスクのそれ以降での新しい最終成功パスワードの使用は保証されません。さらに、「最後に使用したルールの変更」イベントがそのまま生成されます。以降、デバイスで目的のパスワードルールを使用しない場合を判断できます。</li> <li>常に定義順でパスワードを試行する。：オンにすると、常に定義順でパスワードを試行します。最近使用した認証の資格情報は次のデバイスとの通信時に追跡されます。これにより、デバイスパスワードルールを利用して、各デバイスへの接続の試行回数を最小限に抑えることができます。詳細については、「<a href="#">デバイスパスワードルールの作成</a>」(132ページ)を参照してください。</li> </ul>
デフォルトの接続方法	<p>デバイスの接続には、次の方法を使用します。[デバイスの新規作成]ページと[デバイスの追加]ウィザードでは、これらはデフォルトでオンになった状態で表示されます。次のいずれかのオプション（複数の場合あり）にチェックを付けます。</p> <ul style="list-style-type: none"> <li>• Telnet</li> <li>• SSH</li> <li>• RLogin</li> <li>• SNMP</li> <li>• SCP</li> <li>• FTP</li> <li>• TFTP</li> </ul> <p><b>注意：</b>NAには統合TFTPサーバがあり、このデバイスとの送受信の設定は、一般的にSNMP経由またはCLIによりデバイスにアクセスして行います。独自のTFTPサーバを持つデバイスの場合、NAはTFTPクライアントとして動作します。通常SCPはCLIで使用する必要があります。SCPでは、SSHを使ってデバイスを有効にする必要があります。デバイスでSSHサーバが実行されていない場合、SCPを実行できません。また、NAには統合FTPサーバがあり、このデバイスとの送受信の設定は、一般的にCLI経由によりデバイスにアクセスして行います。</p>
ログインミス後の待ち時間	ログイン操作を誤った後に、デバイスが回復するまでの秒数を入力します。デフォルトは5秒です。
SNMPタイムアウト	デバイスがSNMPコマンド群（構成のロードなど）を処理するときに待機する秒数を入力します。デフォルト値は40秒です。
パスワード試行の最大回数	許容されるパスワードの最大試行回数を入力します。ゼロ（0）は無制限を意味します。10個のパスワードルールがある状態で「3」を入力すると、NAは最初の3個のパスワードルールを試行した後に試行を停止します。TACACSサーバがログイン試行に3回失敗した後にユーザ名をロックする場合、この設定が役立ちます。パスワードルールを1個のみ試行する場合、「1」を入力します。パスワードルールが1個のみ機能する場合、この設定が役立ちます。
最大アーカイブルール回数	試行するアーカイブパスワードルールの最大数を入力します。デフォルトは3です。このオプションを無効にするには、「0」を入力します。

フィールド	説明/アクション
<b>ネットワークデバイスタスク設定とポートスキャンタスク設定の検出</b>	
Nmapユーティリティのパス	ネットワークデバイスのスキャンに使用するNmapユーティリティのパスを入力します（ <b>注意</b> ：Nmapユーティリティを使用すると、ネットワークをスキャンして、稼働中のポートと提供されているサービスを把握できます。Nmapの詳細については、 <a href="http://www.Insecure.Org">www.Insecure.Org</a> を参照してください。）Nmapのインストールの詳細については、『NA インストールおよびアップグレードガイド』を参照してください。
Nmapポートスキャンの許可	オンにすると、適切な権限を持つユーザはNmapを使用してネットワークデバイスをスキャンできます。Nmapの使用方法的詳細については、『 <a href="#">[ポートスキャン]ページのフィールド</a> 』（353ページ）を参照してください。
Nmapポートスキャンオプション	Nmapを使用してネットワークデバイスをスキャンする際のデフォルトオプションを表示します。Nmapは、デバイススキャンの実行方法を制御します。デフォルトで、NAはNmapに-POを渡して、UDPではなくIPで動作することをNmapに指示します。オプションの詳細リストについては、Nmapマニュアルを参照してください。Nmapの使用方法的詳細については、『 <a href="#">[ポートスキャン]ページのフィールド</a> 』（353ページ）を参照してください。
タスクごとに検出する最大アドレス数	検出するIPアドレスの最大数を入力します。ネットワークデバイスの検出のタスクは、ネットワークトラフィックを抑えるために、スキャンするアドレスの最大数（デフォルトは1024）を超えないようにしてください。
最高SNMPスキャナスレッド	SNMPスキャン方法によるデバイスの検出中にネットワークデバイスの検出のタスクで保持するSNMPスキャナスレッドの最大数を入力します。デフォルトは79です。理論的には、SNMPスキャナスレッドの最大数を大きくすると、タスクの実行速度が向上します。ただし、SNMPスキャナスレッド数を大きくしすぎると、SNMPスキャナスレッドごとに必要なCPUの負荷およびネットワークトラフィックにより、システムのパフォーマンスが低下する場合があります。（ <b>注意</b> ：ネットワークデバイスの検出のタスクを設定する場合、ネットワークデバイスの検出のタスクでSNMPによりデバイスを検出することも可能です。その結果、SNMP経由でデバイスと通信するSNMPスキャナスレッドをタスクに多く保存できます。その他のスキャン方法については、『 <a href="#">[ネットワークデバイスの検出]タスクページのフィールド</a> 』（341ページ）を参照してください。）
ネットワーク検出IPまたはCIDR範囲の除外	右側のボックスにIPアドレスまたはCIDR（Classless Inter-Domain Routing）の範囲の除外（例：192.168.1.0-192.168.2.0または192.168.31.0/24）を入力し、[パターンを追加<<]ボタンをクリックします。アドレスの範囲は両端を含みます。パターンを削除するには、左側のボックスからパターンを選択して[パターンを削除]ボタンをクリックします。
SNMPタイムアウト	各SNMP SysOID調査のタイムアウトをミリ秒単位で入力します。デフォルトは500ミリ秒です。
<b>要塞ホストの設定</b>	
デフォルトで要塞ホストを使用	オンにすると、TelnetおよびSSHでアクセスするときに、新規デバイスで要塞ホストが使用されます。（ <b>注意</b> ：この要塞ホスト設定は、デバイス単位で無効化できます。）
デフォルトの要塞ホスト	TelnetまたはSSHアクセスに使用する要塞ホストのホスト名またはIPアドレスを入力します。
デフォルトの要塞ホストのユーザ名	TelnetまたはSSHアクセスに使用する要塞ホストのユーザ名を入力します。
デフォルトの要塞ホストのパスワード	TelnetまたはSSHアクセスに使用する要塞ホストのパスワードを入力します。

フィールド	説明/アクション
<b>SecurIDのデバイスアクセス</b>	
SecurIDのライセンス使用	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• ユーザごとに固有のトークンを使用：オンにすると（デフォルト）、各デバイスアクセスで、タスクまたは Telnet/SSH プロキシ接続を開始したユーザに対応するシードのみが使用されます。</li> <li>• ソフトウェアトークンプールを使用：オンにすると、一般的に使用するソフトウェアトークンシードのプールが提供され、パフォーマンスを最大限に引き出すために、できるだけ効率的に使用されます。SecurID ソフトウェアトークンプールに関連付けられているユーザ名を入力します。</li> </ul> <p>ユーザ単位で独自のソフトウェアトークンを使用するには、より多くのトークンが必要となるため、トークンのメンテナンスが増えます。プールされているソフトウェアトークンを使用すると、必要なトークン数が減少し、タスクのスループットを強化できる場合があります。</p>
ソフトウェアトークンの最大数	NAを実行しているマシンにインポートされるソフトウェアトークンライセンスの最大数を入力します。デフォルトでは1024です。
パスコードの有効期間	ソフトウェアトークンのパスコードの有効期間を入力します。デフォルト値は60秒です。
<b>FTPとSSHデバイスアクセス</b>	
FTP/SSHユーザ	<p>FTPまたはSSHユーザを入力します。デバイス接続を経由してFTPまたはSSHサーバにアクセスするときに、FTPまたはSSHユーザ名が使用されます。このユーザ名がシステムFTPまたはSSHサーバに存在しない場合、自動的に作成されます。</p> <p><b>注意：</b> Linux または Solaris プラットフォーム上でSCPを使用する場合、システムのSSHデーモン（SSHD）を変更して別のポートで動作するようにし、SSHDサービスを再起動する必要があります。ポート8022を推奨します。SCPとSSHが正しく機能するようにデバイス固有の設定を構成する必要があります。さらに、デバイスとデバイスドライバが、SCP用にNA SSHサーバを使用するためにSCPをサポートする必要があります。</p>
FTP/SSHパスワード	FTPまたはSSHパスワードを入力します。デバイス接続を経由してFTPまたはSSHサーバにアクセスするときに、FTPまたはSSHパスワードが使用されます。

フィールド	説明/アクション
<b>タスク単位のパスワード</b>	
標準デバイスの資格情報を許可	<p>次のいずれかのタスク（複数の場合あり）を選択します。デフォルトでは、すべてのタスクが選択されています。</p> <ul style="list-style-type: none"> <li>• Syslog の構成</li> <li>• ACL の削除</li> <li>• 構成ファイルを配布</li> <li>• パスワードの配布</li> <li>• ドライバの検出</li> <li>• デバイスのリブート</li> <li>• コマンドスクリプトの実行</li> <li>• 診断の実行</li> <li>• ICMP テストの実行</li> <li>• スタートアップとランニングの同期</li> <li>• スナップショットの取得</li> <li>• デバイスソフトウェアの更新</li> </ul> <p>上記のタスクにより、ユーザは、デバイス固有パスワード、またはネットワーク全体のパスワードルールの両方または一方について、標準の処理を選択できます。タスク単位の資格情報についての詳細については、「<a href="#">タスク単位の資格情報</a>」（50 ページ）を参照してください。パスワードルールの詳細については、「<a href="#">[デバイスパスワードルール] ページのフィールド</a>」（134 ページ）を参照してください。</p>
タスクごとのデバイスの資格情報を許可	<p>次のいずれかのタスク（複数の場合あり）を選択します。</p> <ul style="list-style-type: none"> <li>• Syslog の構成</li> <li>• ACL の削除</li> <li>• 構成ファイルを配布</li> <li>• ドライバの検出</li> <li>• パスワードの配布</li> <li>• デバイスのリブート</li> <li>• コマンドスクリプトの実行</li> <li>• 診断の実行</li> <li>• ICMP テストの実行</li> <li>• スタートアップとランニングの同期</li> <li>• スナップショットの取得</li> <li>• デバイスソフトウェアの更新</li> </ul> <p>オンにすると、ユーザはそのタスクに固有の、1 回のみ使用するデバイスの資格情報を入力するよう求められます。タスク単位の資格情報についての詳細については、「<a href="#">タスク単位の資格情報</a>」（50 ページ）を参照してください。</p>



フィールド	説明/アクション
ユーザのAAA資格情報を許可	<p>次のいずれかのタスク（複数の場合あり）を選択します。</p> <ul style="list-style-type: none"> <li>• Syslog の構成</li> <li>• ACL の削除</li> <li>• 構成ファイルを配布</li> <li>• ドライバの検出</li> <li>• パスワードの配布</li> <li>• デバイスのリブート</li> <li>• コマンドスクリプトの実行</li> <li>• 診断の実行</li> <li>• ICMP テストの実行</li> <li>• スタートアップとランニングの同期</li> <li>• スナップショットの取得</li> <li>• デバイスソフトウェアの更新</li> </ul> <p>オンにすると、上記のタスクにより、ユーザがタスク実行時にタスク所有者のAAA資格情報を選択できるようになります。（<b>注意</b>：ユーザは有効なAAA資格情報を定義する必要があります。）タスク単位の資格情報についての詳細については、「<a href="#">タスク単位の資格情報</a>」（50ページ）を参照してください。</p>
フォールバック管理ユーザ	不明のユーザのタスクに使用されるAAA資格情報の管理ユーザを入力します。
<b>Nortelの検出</b>	
Nortel BayRS MIB/OSバージョン	BayRS ドライバを検出する追加のBayRS MIBバージョン/更新バージョンのリストが表示されます。<MIBのバージョン>、パーティカルバーで区切った<更新番号>の順に表記します（例：14.00/1D12 14.20/）。
<b>ゲートウェイメッシュ</b>	
ローカルゲートウェイのホスト	NAコアと同じ領域にあるゲートウェイシステム（例：gw-vlan10:3001）のホスト名またはIPアドレスとポートを入力します。ゲートウェイメッシュの詳細については、「 <a href="#">重複IPネットワーク</a> 」（151ページ）を参照してください。
ローカルゲートウェイのプロキシポート	NAコアと同じ領域にあるゲートウェイシステム（例：gw-vlan10:3001）のポート名を入力します。デフォルト値は 3002 です。ゲートウェイメッシュの詳細については、「 <a href="#">重複IPネットワーク</a> 」（151ページ）を参照してください。
ローカルゲートウェイの管理ポート	ローカル領域のゲートウェイの管理ポート番号を入力します。メッシュから領域名をフェッチするときに使用されます。デフォルト値は9090です。

フィールド	説明/アクション
ゲートウェイ管理の 秘密鍵ファイル名	<p>管理ポートへの接続が必要なゲートウェイの秘密鍵のファイル名を入力します。ファイル名は相対パスの場合と絶対パス場合があります。相対パスは、NAインストールツリーのルートから見た相対的なパスのことで、通常 C:\WA のように表記されます。ゲートウェイの秘密鍵はゲートウェイのインストール時に作成されます。</p> <p>NA スタンドアロンゲートウェイの場合、秘密鍵のファイル名は <code>opswgw-mngt-server.pkcs8</code> です。このファイルは、NA ゲートウェイがインストールされている <code>saOPSWgw\certificates</code> ディレクトリからコピーします。このファイルは、NA インストールのルート（通常 <code>C:\Rendition</code>）からコピーする必要があります。HP SA と NA を統合する場合、NA では HP SA ゲートウェイメッシュが使用されます。この場合、<code>spog.pkcs</code> ファイルを HP SA のホストから NA インストールのルートディレクトリ（通常 <code>C:\Rendition</code>）へコピーします。[システム管理設定] でファイル名を <code>spog.pkcs8</code> に変更してください。</p> <p><b>注意：</b> <code>.pkcs8</code> ファイルは PKCS#8 形式のファイルで、公開鍵暗号化方式で使用する秘密鍵が含まれています。ゲートウェイメッシュを保護するには、秘密鍵を使用してゲートウェイメッシュを管理する必要があります。NA では、ゲートウェイメッシュ管理機能を使用して、ゲートウェイメッシュでサポートされる領域名のリストを表示します。</p> <p>ゲートウェイ管理設定をテストするには、[デバイスの新規作成] ページを開き、[接続情報] セクションまでスクロールして領域名のリストを表示します。</p>
ゲートウェイの メッシュ接続の待ち時間	<p>ゲートウェイメッシュからリモート領域に到達するまでの遅延時間を秒数で入力します。デフォルトでは 5 秒です。この数値は、リモートデバイスとの通信に使用するタイムアウトに追加されます。</p>

変更を保存するには、必ず[保存]をクリックしてください。

## タスク単位の資格情報

タスク単位の資格情報を設定すると、デバイスにアクセスするタスクの処理に一意的資格情報を指定することで、デバイスへのアクセスに使用する資格情報を指定できます。次のことが可能です。

- タスク所有者の AAA 資格情報を使用してタスクを実行する
- タスクの作成時に指定したワンタイム資格情報を使用してタスクを実行する
- 必要なタスクと資格情報の種類を構成する

保護された環境の場合、通常は CiscoSecure ACS TACACS+ などの AAA サーバが実装されています。このようなサーバでは、各デバイスで個々のユーザが実行できるコマンドが制限されています。

たとえば、ユーザ A とユーザ B の両方が特定のコマンドを使用して、権限を持っているコマンドスクリプトを実行するとします。この場合、NA を一度実装すると、ユーザ A とユーザ B の両方がコマンドスクリプトを実行できなければなりません。ただし、ユーザ A とユーザ B の両方に、権限のあるコマンドのみを実行する資格情報を持たせたい場合もあります。

そのため、タスク単位の資格情報を使用すれば、ユーザ A とユーザ B の両方にコマンドスクリプトの実行権限を持たせるために、NA の静的アカウントを新たに設定する必要がありません。各ユーザは、現在の権限でコマンドスクリプトを実行できます。ユーザ A とユーザ B のどちらかが権限のないコマンドを実行すると、エラーが表示されます。

AAA資格情報を使用すると、NAでは次のことを実行できます。

- 最後に成功した資格情報、デバイス固有の資格情報、パスワードルール、デバイスアーカイブパスワードなど、標準的な資格情報の処理をすべて試行します。
- 各試行で、NAはユーザ名とパスワードをタスク所有者のAAAユーザ名とパスワードに置き換えます。試行に失敗すると、NAはユーザのAAAパスワードを実行パスワードと有効パスワードの両方として使い、再試行します。すべてのAAAログイン試行に失敗すると、タスクは失敗に終わります。

**注意：** .RCX ファイルで設定できる、proxy/auth\_fallback\_for\_aaa\_task という非表示の設定があります。この設定を true にすると、フォールバックにより標準的なパスワード処理が試行されます。

1回限りの資格情報を設定すると、指定した種類の資格情報の処理がタスクの種類に応じて使用されます。たとえば、AAA 資格情報のみがスナップショットのタスクに許可されている場合、すべてのスナップショットタスクで AAA 資格情報が使用されます。所定のタスクの種類で複数の種類の資格情報が許可されている場合、ユーザは使用する資格情報を選択できます。

所定のタスクに1回限りの資格情報を使用する場合、タスクの作成時にユーザが指定した資格情報のみが使用されます。1回限りの資格情報に失敗すると、そのタスクは失敗に終わります。

**注意：** 1回限りの資格情報に成功した場合、そのデバイスで最後に成功した資格情報は更新されません。

## サーバ

[サーバ]ページでは、次のことが可能です。

- TFTPサーバ、FTPサーバ、SMTPサーバを指定する
- NAタスクの制限を設定する
- Syslog の構成
- デバイスのインポート間隔を構成する
- プライマリIPアドレスの再割り当てと重複の解除を構成する
- ドメイン名の解決を構成する
- 監査ログを有効にする
- データベースの整理を構成する
- 高度なスクリプト機能を構成する
- HTTPプロキシサーバを構成する
- 動的デバイスグループの再計算を構成する
- ソフトウェアイメージ管理を構成する
- 拡張ドライバのディレクトリへの絶対パスを指定する
- サーバのパフォーマンス調整を構成する
- イベント差異サイズのしきい値を構成する
- 非管理NAコア上のSyslog変更検出を無視する

[サーバ]ページを表示するには、[管理]メニューバーから[システム管理設定]を選択し、[サーバ]をクリックします。[サーバ]ページが開きます。

## [サーバ]ページのフィールド

フィールド	説明/アクション
<b>サーバ</b>	
FTPまたはTFTPサーバのIPv4アドレス	NAが使用するFTPまたはTFTPサーバのIPv4アドレスを入力します（デフォルトではNAサーバ自身に設定されています）。
FTPまたはTFTPサーバのIPv6アドレス	NAが使用するFTPまたはTFTPサーバのIPv6アドレスを入力します（デフォルトではNAサーバ自身に設定されています）。IPv6サポートの詳細については、『NA インストールおよびアップグレードガイド』を参照してください。
FTP/TFTPファイルパス	FTP/TFTPサーバによる構成ファイルの書き込み先となるパスとフォルダを入力します。NAでは、このフォルダに読み取りと書き込みの権限が必要となります。デフォルトのフォルダは、C:\<インストールディレクトリ>\server\ext\tftp\tftpdrootです。
SyslogサーバのIPv4アドレス	NAが使用するSyslogサーバのIPv4アドレスを入力します（ <b>注意</b> ：指定しないと、NAサーバの最初の非ルーバックIPv4アドレスが使用されます）。

フィールド	説明/アクション
Syslog サーバの IPv6 アドレス	NA が使用する Syslog サーバの IPv6 アドレスを入力します（ <b>注意</b> ：指定しないと、NA サーバの最初の非ルーバック IPv6 アドレスが使用されます）。
SMTP サーバ	NA が電子メール通知に使用する SMTP サーバのホスト名または IP アドレスを入力します。
SMTP 送信元 アドレス	NA が電子メールの送信元に使用するアドレスを入力します。
<b>タスク</b>	
最大同時タスク	<p>同時に実行できるタスクの最大数を入力します。この設定により、同時に実行できる非グループタスク数が制限されます。NA では、システムおよびネットワークのパフォーマンスを損なわないようにするために、同時に実行可能な非グループタスク数が制限されています。同時に実行可能なグループ外のタスクの数は、デフォルトでは 20 です。データベース接続プール内でのデータベース接続数には制限があります。そのため、同時に実行できるタスクの最大数は 50 以内に制限されています。</p> <p><b>注意</b>：使用可能なメモリが不十分な場合、NA は最大同時タスクを実行しません。その結果、[最大同時タスク] が 200 に設定されている場合、NA は 200 個の同時タスクすべてを実行できないこともあります。</p>
最大同時グループタスク	<p>同時に実行できるグループタスクの最大数を入力します。デバイススイントリに対して実行するスナップショットなどのグループタスクでは、子タスクがスケジュールされます（グループ内のデバイスあたり 1 タスク）。</p> <p><b>注意</b>：[最大同時グループタスク] の値を [最大同時タスク] の値よりも小さく設定すると、大規模なグループの操作中に、時間に依存するタスクを個別に実行できます。たとえば、グループ全体の大規模なパスワード変更タスクを実行している間でも、NA はリアルタイムでタイムリーに変更を検出し、スナップショットタスクを実行します。</p>
最長タスク時間	タスクが停止して [失敗] 状態になるまでの、タスクの実行可能な最大時間を入力します。デフォルトでは 3,600 秒（1 時間）です。指定したタスクが [最長タスク時間] に達すると、NA はタスクの停止を試みます。ただし、タスクは、安全に停止できるポイントに達するまで実際には処理を停止しません。タスクによってはタスクの停止までに長い時間がかかるものもあるので注意してください。
<b>Syslog の設定</b>	
デフォルトで syslog を構成	オンにすると、新規デバイスでの Syslog 変更検出が自動的に構成されます。
デフォルトの syslog リレー	新規デバイスのリレーホストの、デフォルトのホスト名または IP アドレスを入力します。
<b>デバイスのインポート</b>	
既存デバイスを上書き	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• はい：NA データベースに保存された既存のデバイスデータをインポートするデータで上書きします（デフォルト）。インポートに含まれないデバイスには影響ありません。</li> <li>• いいえ：NA データベースに保存された既存のデバイスデータをインポートするデータで上書きしません。</li> </ul>
不明デバイスの期間	この期間よりも長い間、インポートソースに見つからないデバイスは、[不明またはアクセス不能なデバイスアクション] 設定に従って、削除、非アクティブ化、またはそのままにされます。デフォルトでは 45 日です。

フィールド	説明/アクション
アクセス不能デバイスの期間	この期間にNAがアクセスできないデバイスは、[不明またはアクセス不能なデバイスアクション]設定に従って、削除、非アクティブ化、またはそのままにされます。デフォルトでは45日です。
不明またはアクセス不能なデバイスアクション	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• デバイスを削除：不明またはアクセス不能なデバイスがデータベースから削除されます。</li> <li>• デバイスを非アクティブ化：不明またはアクセス不能なデバイスが非アクティブ化されます（デフォルト）。一般的に、設定の履歴を維持するために、デバイスをデータベースから削除するのではなく非アクティブ化することをお勧めします。</li> <li>• アクションなし：不明またはアクセス不能なデバイスをそのままにしておきます。</li> </ul>
<b>ユーザのインポート</b>	
既存のユーザまたはユーザグループの上書き	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• はい：NA データベースに保存された既存のユーザアカウントおよびユーザグループデータをインポートするデータで上書きします。インポートに含まれないユーザアカウントおよびユーザグループには影響しません。</li> <li>• いいえ：NA データベースに保存された既存のユーザアカウントまたはユーザグループデータをインポートするデータで上書きしません。</li> </ul>
<b>プライマリIPの再割り当てと重複の削除の設定</b>	
プライマリIPアドレスの再割り当て	オンにすると、プライマリIPアドレスを含むデバイスに関連付けられたIPアドレス（およびデバイスに関連付けられたその他すべてのインターフェイス）を検索し、正規表現またはその他のルールと一致するプライマリIPアドレスがあれば、そのアドレスを設定します。
インターフェイス名再割り当ての正規表現	右側のボックスに正規表現のパターンを入力して[パターンを追加<<]をクリックします。正規表現は、インターフェイス名を指定するための特殊なテキスト文字列（例：Loopback.*）で、IPアドレスはこの文字列と一致している必要があります。パターンを削除するには、左側のボックスからパターンを選択して[パターンを削除]ボタンをクリックします。
IPアドレス再割り当ての正規表現	右側のボックスに正規表現のパターンを入力して[パターンを追加<<]ボタンをクリックします。正規表現は、使用可能なインターフェイスのIPアドレスと一致させるための特殊なテキスト文字列です（例：10\1\.*）。10\1\.*。パターンを削除するには、左側のボックスからパターンを選択して[パターンを削除]ボタンをクリックします。
IPの再割り当ての順番	<p>複数のIPアドレスがインターフェイス名またはIPアドレスのパターンと一致する場合、どちらか一方を選択します。</p> <ul style="list-style-type: none"> <li>• 最低のアドレスをプライマリIPアドレスとして割り当てる（デフォルト）</li> <li>• 最高のアドレスをプライマリIPアドレスとして割り当てる</li> </ul>
重複の検出	<p>重複が検出された場合、次のデバイスオプションのいずれかを選択します。<b>注意</b>：インターフェイスとIPアドレスの情報が同一である場合、デバイスが重複していると見なされます。</p> <ul style="list-style-type: none"> <li>• 重複を無視</li> <li>• 重複を非アクティブ化（デフォルト）</li> <li>• 重複を削除</li> </ul>

フィールド	説明/アクション
<b>ドメイン名の解決</b>	
既存のドメイン名を上書き	オンにして[FQDNの解決]タスクを実行すると、手動入力したFQDNエントリがDNSが解決されたエントリで上書きされます。タスクの実行により、デバイスドメイン名とデバイスホスト名が置き換えられます。
<b>監査ログ</b>	
監査ログ	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>有効：ユーザ操作の監査ログを保存します。ログを確認するには、[監査ログを表示]をクリックします。</li> <li>無効：ユーザ操作の監査ログを保存しません（デフォルト）。</li> </ul>
<b>データベースの整理</b>	
構成	データベースに構成を保存する日数を入力します。デフォルトでは365日です。
診断	データベースに診断を保存する日数を入力します。デフォルトでは45日です。
イベント	データベースにイベントを保存する日数を入力します。デフォルトでは45日です。
タスク	データベースにタスクを保存する日数を入力します。デフォルトでは365日です。
セッション	データベースにTelnet/SSHプロキシセッションを保存する日数を入力します。デフォルトでは45日です。
ログファイル	サーバのログファイルを保存する日数を入力します。デフォルトでは30日です。ログファイルは極めて大きくなることもあるため、サーバのディスク容量を確保するのにログファイルの整理は不可欠です。
一時ドライバファイル	一時ドライバファイルを保存する日数を入力します。デフォルトでは30日です。
タスクログファイル	タスクのログファイルを保持する日数を入力します。デフォルトでは7日です。
トポロジーデータ	トポロジーデータを保存する日数を入力します。デフォルトでは45日です。
ダイアグラムファイル	ダイアグラムファイルを保存する日数を入力します。デフォルトでは1日です。
ACL データ	ACL データを保存する日数を入力します。デフォルトでは365日です。
デバイス認証データ	デバイス認証データを保存する日数を入力します。デフォルトでは45日です。

フィールド	説明/アクション
<b>高度なスクリプティング</b>	
スクリプト言語 1	<p>[高度なスクリプティング]により、ネットワークで使用するスクリプト言語で書かれたカスタムスクリプトを実行できます。そのためには、インストールされている各言語のインタープリタが必要です。また、[高度なスクリプティング]設定から言語オプションとパスを関連付ける必要があります。</p> <p>[高度なスクリプティング]を有効にすると、ここで指定するスクリプト言語が[コマンドスクリプトの新規作成]ページの選択リストに表示されます。デフォルトでは、この設定は「Expect」に構成されています。このページの[インタープリタのパス[#]]設定に対応する言語のインタープリタへのパスを指定する必要があります。</p> <p>[高度なスクリプティング]機能では、最大5つの言語を構成できます。また、それらの言語を使用しない場合、事前に構成されたデフォルト値を上書きすることも可能です。コマンドラインから実行可能な言語のみがサポートされています（JScript、Python など）。</p> <p><b>注意：</b>スロット1と2は、あらかじめExpectとPerlに構成されています。ただし、NAではExpectのインタープリタのみがインストールされています。これらの言語で書かれたスクリプトを実行するには、ここで指定する各言語のインタープリタをインストールしてパスを構成する必要があります。</p>
インタープリタのパス 1	[スクリプト言語 1]で指定する言語のインタープリタへのパスを入力します。
スクリプト言語 [2-5]	<p>[高度なスクリプティング]を有効にすると、ここで指定する言語が[コマンドスクリプトの新規作成]ページの言語選択リストに表示されます。[インタープリタのパス[#]]設定に対応する言語のインタープリタへのパスを指定する必要があります。</p> <p><b>注意：</b>デフォルトでは、[スクリプト言語 2]はあらかじめPerlに構成されていますが、この設定を有効にするには、Perlのインタープリタをインストールする必要があります。</p>
インタープリタのパス [2-5]	<p>関連付けられた[スクリプト言語[#]]ボックスで指定する言語のインタープリタへのパスを入力します。</p> <p><b>注意：</b>Windows 環境の場合、[インタープリタのパス 2]のデフォルトがあらかじめPerlに構成されていますが、Perlのインタープリタはインストールされていません。この設定を有効にするには、Perl をインストールしてパスを指定する必要があります。</p>
<b>動的グループ</b>	
動的グループの自動再計算	<p>すべての動的グループのメンバーデバイスを再計算する頻度を入力します。デフォルトでは60分です。自動計算を無効にするには、「0」を入力してください。（<b>注意：</b>動的グループメンバーを再計算すると、NAは多数のクエリを実行し、グループのルール、フィルタのいずれかまたは両方を基にして動的グループに属すデバイスを判断します）。</p>
イベント主導の再計算	オンにすると、デバイス変更イベントが発生するたびに、動的グループのメンバーが再計算されます。



フィールド	説明/アクション
デバイス変更イベント	<p>動的グループのメンバーの再計算を開始するデバイス変更イベントを選択します。この設定は、[イベント主導の再計算]オプションがオンの場合のみ機能します。デバイス変更イベントには、次のような例があります。</p> <ul style="list-style-type: none"> <li>• デバイスが追加されました</li> <li>• デバイス構成の変更</li> <li>• デバイスが削除されました</li> <li>• デバイスが編集されました</li> <li>• デバイスソフトウェアの変更</li> <li>• デバイスが管理解除されました</li> </ul>
<b>ソフトウェアイメージ管理</b>	
SNMP再試行	最初の試行を失敗した後に試行を実行する回数を入力します。最大値は5です。
SNMPタイムアウト	SNMPパケットのタイムアウトを秒数で入力します。デフォルトは5です。
Telnetタイムアウト	ソケットタイムアウトの値を秒数で入力します。デフォルト値は10です。
HTTP プロキシサーバ	HTTP プロキシサーバを入力します。プロキシサーバが、直接アクセスが機能しないときにHTTP を介してCisco.comにアクセスするのに使用します。
HTTP プロキシサーバポート	HTTP プロキシポートを入力します。
ソフトウェアイメージ管理サービスホスト	ソフトウェアイメージ管理サービスを実行するシステムのホスト名またはIPアドレスを入力します。
ソフトウェアイメージ管理サービスポート	ソフトウェアイメージ管理サービスポートを入力します。これは、ソフトウェアイメージ管理サービスがリスニングするポートです。通常6099です。
<b>ドライバ</b>	
ドライバ拡張ディレクトリ	NA が追加ドライバを検索するディレクトリを入力します。ドライバの開発の詳細については、『Driver Development Kit (DDK)』マニュアルを参照してください。
<b>パフォーマンスの調整</b>	
イベントのリストについては、「はじめに」(454 ページ)を参照してください。	フィルタするイベントのチェックボックスをオンにします。これにより、システムのパフォーマンスを調整できます。大規模な構成でのイベント差異の制限、大規模な構成での行ごとのマスクの制限、大きなセッションログの格納と表示の制限なども実行できます。
<b>特殊なパフォーマンス設定</b>	
大きな構成のイベント差異の制限	大規模な構成の場合、イベント電子メールで構成差異レポートを作成するプロセスが大量のシステムリソースを消費する場合があります。このオプションをオンに設定し、サイズ制限を設定（以下を参照）すると、構成サイズが指定したしきい値を超えたイベントに対する構成差異レポートがスキップされます。
イベント差異サイズのしきい値	サイズ制限を設定すると、構成サイズが指定したしきい値を超えたイベントに対する構成差異レポートがスキップされます。

フィールド	説明/アクション
大きな構成の1行ごとのマスキングの制限	大規模な構成の場合、2つの構成間の1行ごとの差異を表示するプロセスが大量のシステムリソースを消費する場合があります。このオプションをオンに設定し、サイズ制限（以下を参照）を設定すると、構成差異ページに、指定したしきい値を超えたサイズのこれら2つの構成が、追加の強調表示や行番号がない状態で並んで表示されます。
1行ごとのマスキングサイズのしきい値	サイズのしきい値を設定すると、構成差異ページに、指定したしきい値を超えたサイズの2つの構成が、追加の強調表示や行番号がない状態で並んで表示されます。
大きなタスクセッションログのストレージと表示の制限	タスク結果の一部としてタスクセッションログが保存されます。デバイスによってはセッションログに膨大なデータがダンプされ、これによりデータベース内のタスクテーブルのサイズが大幅に増大する場合があります。このオプションをオンに設定し、サイズ制限を設定（以下を参照）すると、セッションログは指定したしきい値に達したところで切り捨てられ、セッションログのサイズが極端に大きくなることはありません。
タスクセッションログサイズのしきい値	サイズのしきい値を設定すると、セッションログは指定したしきい値に達したところで切り捨てられ、セッションログのサイズが極端に大きくなることはありません。
非管理コア上のsyslog変更検出を無視	分散システムで、Syslogメッセージを複数のNAコアに送信するようにデバイスをセットアップすると、2つのNAコアが同時に同じデバイスのスナップショットタスクをスケジュールしようとしてデータベースレプリケーションの競合が発生する場合があります。このオプションをオンに設定すると、NAコアに対して、Syslogメッセージを無視して、スナップショットタスクをスケジュールしないように指示されます。分散システムの詳細については、『NA Multimaster Distributed System on Oracle Guide』を参照してください。
メッシュ内コア上にローカルに作成された全タスクをコアが実行できるようにする	このオプションは、指定したデバイスのタスクが任意のNAコア上で実行可能になるようにローカルNAコアに指示し、1つのデバイス上で一度に1つのタスクしか実行しないようにします。実行中のタスクの内容を確認するために、このNAコアは他のNAコアと通信する必要があります。分散システムの詳細については、『NA Multimaster Distributed System on Oracle Guide』を参照してください。
このコア上にローカルに作成された全タスクをコアが実行できるようにする	このオプションを設定すると、このNAコアにログインするユーザによって作成されたすべてのタスクが、現在のNAコアにタスクを割り当てることになります。これにより、デバイスが属するサイトの管理NAコアは無視されます。分散システムの詳細については、『NA Multimaster Distributed System on Oracle Guide』を参照してください。

変更を保存するには、必ず[保存]をクリックしてください。

## ワークフロー

[ワークフロー] ページでは、次のことが可能です。

- ワークフローを有効にする
- イベント通知とレスポンスルールを構成する
- デバイス予約システムを構成する
- Telnet/SSH プロキシのデバイスの予約を構成する

[ワークフロー] ページを表示するには、[管理] メニューバーから [システム管理設定] を選択し、[ワークフロー] をクリックします。[ワークフロー] ページが開きます。

## [ワークフロー] ページのフィールド

フィールド	説明/アクション
<b>ワークフロー</b>	
ワークフローを有効にする	オンにすると、承認ルールが定義されている場合、タスクの承認が必要になります。
優先値	<p>承認を要求するタスクに設定できる優先度の値を定義します。デフォルトでは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 低</li> <li>• 中</li> <li>• 高</li> </ul> <p>[緊急] や [通常] などの異なる値を入力し、[値を追加 &lt;&lt;] ボタンをクリックすると、それらの値を追加できます。値を削除するには、値を選択して [値を削除] ボタンをクリックします。</p> <p><b>注意：</b> NA Scheduler では、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。</p>
<b>イベント通知とレスポンスルール</b>	
タスクを実行	このフィールドのチェックボックスをオンにすると（デフォルト）、イベントのルールを承認しなければならないため、すべてのタスクがスケジュールされます。たとえば、設定ポリシーに準拠しないイベントの発生を受けて対応策のタスクを実行する場合、そのタスクを承認してから配布する必要があります。
<b>デバイス予約システム</b>	
デバイス予約システム	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 有効：[デバイス予約システム] が有効になります（デフォルト）。デバイス予約システムの詳細については、<a href="#">「デバイスの予約」</a>（190 ページ）を参照してください。</li> <li>• 無効：[デバイス予約システム] が無効になります。</li> </ul>
デフォルトの継続時間	デバイスグループの予約を保存できる時間（分）を入力します。デフォルトでは60分です。
アクティビティカレンダーの最大列数	アクティビティカレンダーの最大列数を設定します。デフォルトでは1024です。アクティビティカレンダーの詳細については、 <a href="#">「アクティビティカレンダー」</a> （191 ページ）を参照してください。

フィールド	説明/アクション
30分間の延長を決定する時間（分）	予約を延長する最短分数。最長 30 分間です。30 分間の予約としてアクティビティカレンダーに表示されます。デフォルトでは 5 分です。
<b>Telnet/SSH プロキシの予約</b>	
Telnet/SSH プロキシのデバイス予約	<p>NA Telnet/SSH プロキシは、デバイスのアクセスおよび構成に使用できます。アクセス制御、セッションログ記録のキーストローク、インラインコメントなどの機能を構成できます。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 無視：Telnet/SSH プロキシ経由でデバイスにアクセスするとき、デバイス予約を無視（デフォルト）デバイス予約システムの詳細については、「<a href="#">デバイスの予約</a>」（190 ページ）を参照してください。</li> <li>• 警告：Telnet/SSH プロキシ経由でデバイスに接続する際に、承認済みのデバイス予約が存在しない場合にユーザに警告</li> <li>• 回避：承認されたデバイス予約が存在しない場合、ユーザがTelnet/SSH プロキシ経由でデバイスにアクセスしないユーザが無効化権限を持っている場合、そのユーザに、デバイスへの非アクセスを無効化するかどうか確認するためのプロンプトが表示されます。</li> </ul> <p>「警告」または「回避」を選択した場合、承認済みであれば、ユーザ、デバイス、デバイスグループ、およびマルチタスクプロジェクトの予約時間など、デバイス予約の一致を検索します。</p>
デバイス予約なしの警告メッセージ	承認されたデバイス予約が存在しない場合に表示する警告メッセージを入力します。デフォルトの警告メッセージは次のとおりです。 <b>警告：現在、このデバイスの承認された予約がありません。</b> デフォルトの警告メッセージを削除することもできます。

## ユーザインターフェイス

[ユーザインターフェイス]ページでは、次のことが可能です。

- ログインのセキュリティを構成する
- すべてのページで表示する日付の形式を設定する
- NAメニューをカスタマイズする
- [モジュールの表示]/[モジュールの編集]ページのスロットを追加する
- [テンプレートの新規作成]/[テンプレートの編集]ページから役割を追加または削除する
- [コマンドスクリプトの編集]/[診断編集]ページのテキストボックスのサイズをカスタマイズする
- デバイスセレクトの表示をカスタマイズする
- 拡張カスタムフィールドを有効にする
- クイック起動タスクを構成する

[ユーザインターフェイス]ページを表示するには、[管理]メニューバーから[システム管理設定]を選択し、[ユーザインターフェイス]をクリックします。[ユーザインターフェイス]ページが開きます。終了する場合は、必ず[保存]をクリックしてください。

## [ユーザインターフェイス]ページのフィールド

フィールド	説明/アクション
<b>セキュリティ</b>	
セッションタイムアウト	非アクティブなWebセッションが終了するまでの時間数を秒単位で入力します。デフォルト値は1800秒です。この変更は、次のログインから有効となります。
[デバイス構成の表示]でデバイスのアクセス許可を確認	オンにすると、ユーザに適切なデバイスのアクセス許可がある場合のみデバイス設定を表示できます。この設定を有効にするには、NAを再起動してください。
ユーザ名とパスワードの自動入力	オンにすると、NAのログインページで、ブラウザの自動入力機能が有効になります。
スタックトレースの表示	オンにすると、例外スタックトレースがWeb UIエラーページで確認できるようになります。
クロスサイトスクリプティングの確認	オンにするとユーザ入力が確認され、<script>、<object>、<img>、<input>など、クロスサイトスクリプティングの可能性がある要素を除去します。つまり、このオプションをオンにすると使用中のスクリプトから潜在的に悪質なJavascriptコードを削除できます。悪質なJavascriptコードが見つかったら、エラーが返されます。
<b>日付/時刻の表示</b>	
日付書式	この設定は、Webインターフェイス全体で表示される日付の書式を制御します。デフォルトの形式はMMM-dd-yy HH:mm:ssです。日付/時刻要素の順序を変更する、日付/時刻を入れ替える、4桁の年（yyyy）を入力する、月を2桁の数値（MM）に変更するなどの操作が可能です。要素には大文字と小文字の区別があります。たとえば、HHは1-24時の時間を表し、hhは午前/午後1-12時までの時間を表します。

フィールド	説明/アクション
<b>メニューのカスタマイズ</b>	
カスタムメニューリンクの表示	オンにすると、[概要]オプションの上にユーザ定義の名前が表示されます。メニューのタイトルと、チケットアプリケーションのホームページなど、HTML ページへのリンクが表示されます。
カスタムメニュータイトル	表示する名前を入力します。
カスタムメニューページ	[カスタムメニューリンクの表示]を選択する場合、ユーザがメニュータイトルをクリックした時に表示する HTML ページの URL を入力します。このページは、別の HTML アプリケーション内のページでもかまいません。
<b>構成の比較</b>	
画面比較時の行数	2つの設定を画面上で比較する際に表示する、各変更の上下の行数を入力します。デフォルト値は3です。
電子メール比較時の行数	電子メールのテキストとして2つの設定を比較する際に表示する、各変更の上下の行数を入力します。デフォルト値は3です。
<b>ソフトウェアセンター</b>	
スロット	[モジュールを表示]/[モジュールを編集] ページでユーザの画面に表示されるスロット（カード/ブレード/モジュール用のシャーシスロット）を追加または削除します。スロットを追加するには、スロット名を右側のボックスに入力して[スロットを追加<<]をクリックします。スロットを削除するには、左側のボックスからスロット名を選択して[スロットを削除]をクリックします。
ファイル準拠レベルの表示	イメージセット内の各イメージファイルの準拠レベルを表示するには、チェックボックスをオンにします。
デバイスモデル	デバイスモデルを入力し、[モデルを追加] ボタンをクリックします。[モジュールを削除] ボタンをクリックすると、デバイスモジュールを削除できます。
プロセッサタイプ	プロセッサタイプを入力し、[プロセッサを追加] ボタンをクリックします。[プロセッサを削除] ボタンをクリックすると、プロセッサタイプを削除できます。
デバイス BootROM	デバイス BootROM を入力し、[デバイス BootROM を追加] ボタンをクリックします。[デバイス BootROM を削除] ボタンをクリックすると、デバイス BootROM を削除できます。
<b>テンプレート</b>	
テンプレートのロール	[テンプレートの新規作成]/[テンプレートを編集] ページから、テンプレートの作成者が選択するロールを追加または削除します。ロールは、[境界]または[コア]など、ネットワークでデバイスが果たす役割を説明するものです。ロールを追加するには、ロール名を右側のボックスに入力して[ロールを追加<<]をクリックします。ロールを削除するには、左側のボックスからロール名を選択して[ロールを削除]をクリックします。
<b>スクリプト</b>	
スクリプトテキストの高さ	[コマンドスクリプトを編集]/[診断を編集] ページのテキストボックスのサイズ（高さ）を入力します。デフォルトでは12行です。
スクリプトテキストの幅	[コマンドスクリプトを編集]/[診断を編集] ページのテキストボックスのサイズ（幅）を入力します。デフォルトでは60文字です。
<b>拡張カスタムフィールド</b>	
拡張カスタムフィールドを有効にする	オンにすると、一部のデータセットに拡張カスタムフィールドを構成できます。カスタムデータフィールドでは、特定のデバイス、設定、ユーザなどに有効なデータを割り当てることができます。詳細については、 <a href="#">「拡張カスタムフィールド設定」(558 ページ)</a> を参照してください。

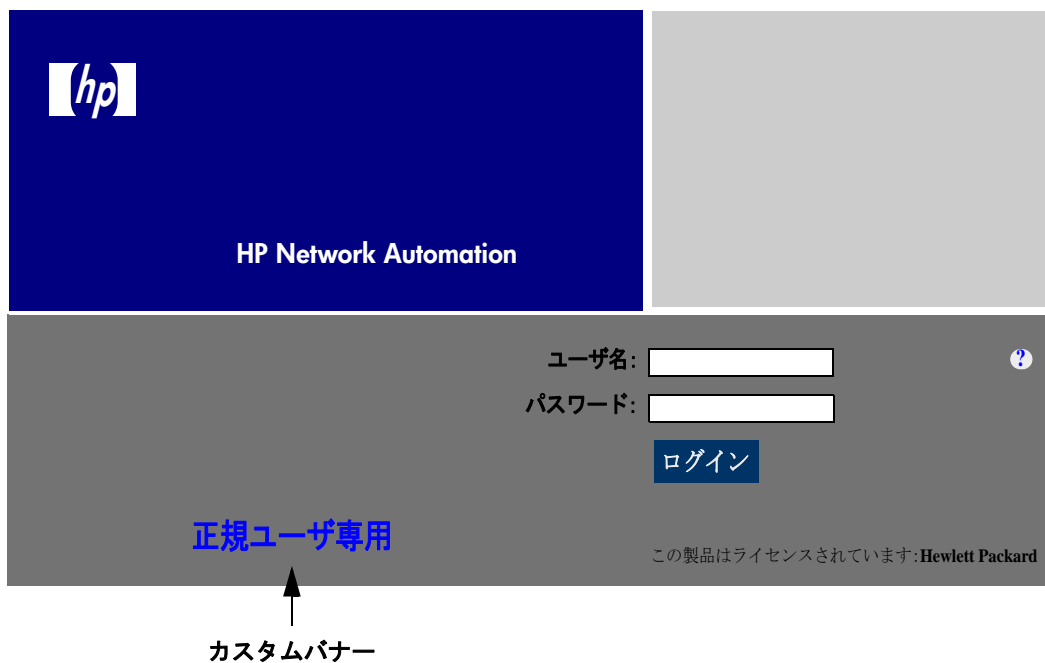
フィールド	説明/アクション
<b>プロキシウィンドウ</b>	
プロキシウィンドウの寸法	プロキシウィンドウに使用するサイズを選択します。
<b>その他</b>	
タスクページの リフレッシュ間隔	[タスクリスト]ページのリフレッシュ間隔を秒数で入力します。デフォルト値は60秒です。
プレーンテキストとして表示する場合のサイズのしきい値を設定	プレーンテキストとして表示する場合のサイズのしきい値を入力します。デフォルトでは200,000バイトです。容量の大きな一部の設定では、サーバやブラウザのリソースを大量に消費する行番号指定などの特別な処理ができない場合もあります。設定値がデフォルト値を超えると、その値は<pre></pre>タグで囲まれた状態でプレーンテキストとして表示されます。
コミュニティ文字列を隠す	オンにすると、コミュニティ文字列がWeb UIに平文で表示されなくなります。このオプションは、NAが表示するコミュニティ文字列専用のオプションです。構成に埋め込まれたコミュニティ文字列は、ドライバ固有の機密情報データのマスキング実装に基づいてマスクされます。
隠し文字のスタックトレース出力を無効にする	オンにすると、隠し文字のスタックトレース出力が無効になります。オフにすると、サーバエラーが発生したときに、サーバログの他に、HTMLページに隠し文字としてスタックトレースを出力します。 (注意：デフォルトでは、サポートコールを支援する目的で、完全なJavaスタックトレースが隠し文字としてHTML表示されます。このオプションをオフにするとセキュリティの脆弱性につながる可能性があると考えられる場合は、このオプションをオンにしてください。
詳細例外メッセージ出力の無効化	オンにすると、詳細例外メッセージの出力が無効になります。オフにすると、サーバエラーが発生したときに、HTMLページにサーバログに加え詳細例外メッセージが出力されます。

## NA ログインページをカスタマイズする

HP Network Automation (NA) のログインページでは、警告メッセージや企業固有の情報など、情報の表示に関するカスタマイズが可能です。

HP ログインページをカスタマイズするには：

1. 「\$NA\_HOME/resource」ディレクトリで、「customer\_banner.html」ファイルを開きます。このファイルが存在しない場合は、上記の名前でファイルを作成します。（注意：「resource」ディレクトリも同様に作成する必要があります。）
2. HTML をサポートしているテキストエディタでファイルを開き、NA のログインページに表示するテキストを入力します。
3. ファイルを保存し、NA にログインします。[ログイン] ボタンの下にテキストが表示されます。表示する語数に制限はありません。ただし、表示が正しくページ内に収まっているかどうかを確認する必要があります。次にログインページのサンプルを示します。





# Telnet/SSH

[Telnet/SSH] ページでは、次の構成が可能です。

- Telnet/SSHのログ記録
- Telnet/SSH プロキシ
- デバイスのシングルサインオン
- Telnetクライアント
- Telnetサーバ
- SSHサーバ

[Telnet/SSH] ページを表示するには、[管理]メニューバーから[システム管理設定]を選択し、[Telnet/SSH]をクリックします。[Telnet/SSH] ページが開きます。

セッションのログ記録を有効にした状態で、デバイスと対話するすべてのタスクが実行できます。タスク実行中のデバイスとの対話に関する詳細なログが記録されます。デバイス固有の問題をデバッグする場合、最初にセッションログを表示する必要があります。セッションログでは、CLI、SNMP およびタスクで実行されるすべての転送プロトコルアクションの詳細がわかります。

## [Telnet/SSH] ページのフィールド

フィールド	説明/アクション
<b>Telnet/SSH セッションのログ記録</b>	
コマンドをログに記録	オンにすると、TelnetまたはSSHセッション実行時のコマンドが保存されます。コマンドを表示するには、[デバイス情報] ページで[Telnet/SSHセッションを表示]と[コマンドのみ表示]をクリックします。このページで[スクリプトに変換]というリンクを使用すると、次回以降セッションのコマンドをスクリプトからすばやくキャプチャできます。詳細については、「 <a href="#">コマンドスクリプトの追加</a> 」(576 ページ) を参照してください。
レスポンスをログに記録	オンにすると、TelnetまたはSSHセッション実行時の完全なセッションログが保存されます。ログを表示するには、[デバイス情報] ページで[Telnet/SSHセッションを表示]と[全セッションを表示]をクリックします。このページで[スクリプトに変換]というリンクを使用すると、次回以降セッションのコマンドをスクリプトからすばやくキャプチャできます。詳細については、「 <a href="#">コマンドスクリプトの追加</a> 」(576 ページ) を参照してください。
強制的にログ記録	オンにすると、API使用時にTelnet/SSHの各セッションについて、デバイスのコマンド/レスポンスを強制的にログに記録します。
<b>Telnet/SSH プロキシ</b>	
Telnet/SSHサーバを有効にする	Telnet/SSH プロキシは、デバイスのアクセスおよび構成に使用できます。アクセス制御、セッションログ記録のキーストロック、インラインコメントなどの機能を構成できます。オンにすると（デフォルト）、NAがTelnet/SSHサーバとして動作します。
非アクティブなサーバ接続のタイムアウト	アイドル状態にあるTelnetセッションまたはSSHセッションがNA Telnet/SSHサーバから切断されるまでの最長接続時間を入力します。ここで指定した時間、NAに接続されているTelnet/SSHクライアントが非アクティブである場合、セッションはタイムアウトになります。デフォルトでは30分です。

フィールド	説明/アクション
デフォルトの接続方法	<p>シングルサインオンなしでデバイスに接続するときに使用する方法（TelnetまたはSSH）を選択します。ここで選択する接続方法は、<code>-method</code>オプションが追加されていない場合、Telnet/SSH プロキシの接続コマンドで使用する接続方法となります。[シングルサインオンを使用]が選択されておらず、[デバイスの編集]ページのサポートリストに同じ接続方法が含まれていない場合、この方法は無視されます。</p> <p><b>注意：</b> 外部認証としてSecurIDを使用するようにNAを構成している場合は、NA プロキシに接続するときのシングルサインオン機能が無効になります。SecurIDのパスコードは再利用できないため、お使いのSecurIDの資格情報を使用して再認証する必要があります。</p>
非アクティブなデバイスのタイムアウト	<p>接続を終了する前に、アイドル状態にあるデバイスセッションを開いておくことのできる最長時間を分単位で入力します。デフォルトでは30分です。</p>
SSHログインのタイムアウト	<p>NA プロキシに「-login」スイッチを使用してSSHログインする際のタイムアウトを秒単位で入力します。デフォルト値は15秒です。</p>
同時セッション時にアラート	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 同時セッションを警告：オンにすると（デフォルト）、別のユーザがデバイスに接続しようとした場合に警告が生成されます。あるユーザが誤って別のユーザの行った変更を無効化することを防ぎます。警告を無効にできるのは、管理権限のあるユーザのみです。</li> <li>• 同時セッションを回避：オンにすると、すべてのユーザが同時セッションを使用できなくなります。</li> <li>• アクションなし：オンにすると、同時セッションが無視されます。</li> </ul>
分散システムの同時セッション処理	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 非ローカルデバイスのセッションを許可（[同時セッションを警告]（上記を参照）と[非ローカルデバイスのセッションを許可]の両方をオンにすると、警告が発行されないので注意してください）。</li> <li>• 非ローカルデバイスのセッションを拒否</li> </ul> <p>分散システムの詳細については、『NA Multimaster Distributed System on Oracle Guide』を参照してください。</p>
不明デバイスに接続	<p>オンにすると（デフォルト）、ユーザは管理対象でないデバイスに接続できます。</p>
最大デバイス接続リスト	<p>ワイルドカード検索に基づいてデバイスに接続する場合、複数の一致デバイスが見つかったときに表示されるデバイス数の最大数を入力します。デフォルトは20です。この数値を超えるデバイス数が返された場合、ワイルドカードの正規表現に条件を付けるよう要求されます。</p>
<b>デバイスのシングルサインオン</b>	
シングルサインオンを使用	<p>オンにすると（デフォルト）、自動的にユーザを一度認証すると、以降はデバイス変更権限を持つデバイスにログインできます。</p> <p><b>注意：</b> 外部認証としてSecurIDを使用するようにNAを構成している場合は、NA プロキシに接続するときのシングルサインオン機能が無効になります。SecurIDのパスコードは再利用できないため、お使いのSecurIDの資格情報を使用して再認証する必要があります。</p>

フィールド	説明/アクション
デバイスのアクセス許可を 変更しない場合の サインオンモード	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• ログインのプロンプトを表示</li> <li>• 制限付きアクセスモードでサインオン</li> <li>• ログインを拒否</li> </ul>
サインオンのバナーを表示	オンにすると（デフォルト）、デバイスにログオンした時点でサインオンのバナーが表示されます。
シングルサインオンにAAA ログインを使用	オンにすると、AAA ログイン情報が使用されます。このオプションは、[新規/ユーザの編集]ページの[プロキシインターフェイスでのAAAログインの使用]のことです。
AAA ログインの失敗時に HP Network Automation ログインを使用	オンにしている（デフォルト）AAAのユーザ名とパスワード情報を使用できない場合、NAのログイン情報が使用されます。
<b>Telnetクライアント</b>	
Telnetクライアント	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• NAの統合Telnetクライアントを使用（デフォルト）（<b>注意</b>：これは、シングルサインオンをサポートする唯一のオプションです）。</li> <li>• NAのtelnetプロキシに接続するときに標準のブラウザでTelnet:// URLを使用</li> <li>• 指定したデバイスに接続するときに標準のブラウザでTelnet:// URLを直接使用</li> </ul>
<b>Telnetサーバ（この設定を変更するとTelnet/SSHサーバが再起動します）</b>	
Telnetを有効にする	オンにすると（デフォルト）、NAがTelnetサーバとして動作します。
Telnetサーバのポート	NAがクライアント接続を許可するポートを入力します。Windowsの場合のデフォルト値は23です。UNIX®の場合のデフォルト値は8023です。
最大Telnet接続数	NAが同時に許可するTelnetクライアントの最大接続数を入力します。デフォルト値は50です。
<b>SSHサーバ（この設定を変更するとTelnet/SSHサーバが再起動します）</b>	
SSHを有効にする	オンにすると（デフォルト）、NAがSSHサーバとして動作します。
SSHサーバのポート	NAがクライアント接続を許可するポートを入力します。デフォルト値は22です。
最大SSH接続数	NAが同時に許可するSSHクライアントの最大接続数を入力します。デフォルト値は50です。

変更を保存するには、必ず[保存]をクリックしてください。

## レポート作成

[レポート作成]ページでは、以下の点についての組織内の[ネットワークステータスレポート]をカスタマイズできます。

- ポリシールール違反
- ソフトウェア準拠違反
- スタートアップとランニング構成の不一致
- デバイスアクセスエラー
- 構成の変更
- 電子メールレポート
- ダイアグラム
- イメージ同期レポート

レポートの各カテゴリで、リスクレベルを示すカラーコードと、各層で準拠していないデバイスの割合のしきい値を指定するパラメータを組み合わせ、個々のデバイス（およびデバイスグループ）のステータスのインジケータを設定できます。たとえば、ボーダールータグループにはより高いスコアが割り当てられます。ボーダールータは、外部ネットワークやリモートオフィスへのアクセスを制御するものです。一方、LAN デバイスにはデフォルト値がそのまま割り当てられています。

ネットワーク内の各イベントの重要性を最も反映する設定を行うことで、問題の識別や確立されたポリシー慣行に対するネットワークの準拠の確保に役立ちます。

また、[レポート作成]ページには、ユーザ定義の電子メール通知タスク経由で送信される電子メールレポートの形式や内容のオプション、およびレポートの保存場所を指定するオプションもあります。さらに、ダイアグラムを有効にして、ダイアグラムパラメータを設定することもできます。ダイアグラムの詳細については、[「\[ダイアグラム\]ページのフィールド」](#)（608 ページ）を参照してください。

**注意：** 準拠していないデバイスのステータス（リスクレベル）により、グループのステータスが決定されます。たとえば、単一の非準拠デバイスのリスクレベルを黄色に設定し、グループ内のあるデバイスが違反の状態にある場合、そのデバイスグループは、違反デバイス数のしきい値に達すると黄色でステータスを反映します。

[レポート作成]ページを表示するには、[管理]メニューバーから[システム管理設定]を選択し、[レポート作成]をクリックします。[レポート作成]ページが開きます。

## [レポート作成]ページのフィールド

フィールド	説明/アクション
<b>ポリシールール違反</b>	
デバイスステータスの色	<p>デバイスグループ内のあるデバイスが準拠ポリシーのルールに違反している場合に表示する色を選択します。オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 赤色（デフォルト）</li> <li>• 黄色</li> <li>• 緑色</li> </ul>
カテゴリステータスの色	<p>次のデバイスステータスの色に対する設定ポリシー違反のデバイスの割合に対するしきい値を入力します。</p> <ul style="list-style-type: none"> <li>• 黄色：デフォルト値は1%です。</li> <li>• 赤色：デフォルト値は2%です。</li> </ul>
<b>ソフトウェア準拠違反</b>	
デバイスステータスの色	<p>デバイスグループ内のあるデバイスのソフトウェアが準拠していない場合に表示する色を選択します。オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 赤色（デフォルト）</li> <li>• 黄色</li> <li>• 緑色</li> </ul> <p>次の準拠レベルは違反と見なされます。</p> <ul style="list-style-type: none"> <li>• セキュリティリスク</li> <li>• 実稼動前</li> <li>• 廃止</li> <li>• ブロンズ</li> <li>• シルバー</li> <li>• ゴールド</li> <li>• プラチナ</li> </ul>
カテゴリステータスの色	<p>ソフトウェアレベル違反のデバイスの割合に対するしきい値を入力します。オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 黄色：デフォルト値は1%です。</li> <li>• 赤色：デフォルト値は2%です。</li> </ul>
<b>スタートアップとランニング構成の不一致</b>	
デバイスステータスの色	<p>デバイスグループ内のあるデバイスのスタートアップ設定が実行中の設定と一致しない場合に表示する色を選択します。オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 赤色</li> <li>• 黄色（デフォルト）</li> <li>• 緑色</li> </ul>

フィールド	説明/アクション
カテゴリステータスの色	<p>スタートアップ設定と実行中の設定が一致しないデバイスの割合に対するしきい値を入力します。オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 黄色：デフォルト値は1%です。</li> <li>• 赤色：デフォルト値は2%です。</li> </ul>
<b>デバイスアクセスエラー</b>	
デバイスステータスの色	<p>デバイスグループ内のあるデバイスがデバイスアクセスの失敗をレポートした場合に表示する色を選択します。オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 赤色</li> <li>• 黄色（デフォルト）</li> <li>• 緑色</li> </ul>
カテゴリステータスの色	<p>デバイスアクセスの失敗を示すデバイスの割合に対するしきい値を入力します。オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 黄色：デフォルト値は1%です。</li> <li>• 赤色：デフォルト値は2%です。</li> </ul>
<b>構成の変更</b>	
デバイスステータスの色	<p>デバイスグループ内のあるデバイスの設定が変更された場合に表示する色を選択します。オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 赤色</li> <li>• 黄色（デフォルト）</li> <li>• 緑色</li> </ul>
カテゴリステータスの色	<p>設定変更が行われたデバイスの割合に対するしきい値を入力します。オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 黄色：デフォルト値は1%です。</li> <li>• 赤色：デフォルト値は2%です。</li> </ul>
<b>電子メールレポート</b>	
電子メールレポート形式	<p>検索結果を電子メールレポートで送信するときに使用する電子メール形式を選択します。ネットワークステータスレポートにはこの設定が適用されません。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• HTMLメール（デフォルト）</li> <li>• CSV ファイルの添付</li> <li>• プレーンテキスト</li> <li>• HTMLメール（リンクなし）</li> </ul>
テキストの詳細を電子メールに含める	<p>オンにすると、タスク検索の結果を含むタスクの詳細が、CSV（カンマ区切り値）ファイル形式で電子メールレポートに含まれます。ネットワークステータスレポートにはこの設定が適用されません。</p>

フィールド	説明/アクション
電子メールリンク	<p>電子メールレポートのHTMLリンクのアドレス形式を選択します。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• ホスト名（解決できる場合）</li> <li>• IPアドレス</li> <li>• 標準名（解決できる場合はFQDN）（デフォルト）</li> <li>• ユーザ定義：電子メールリンクで使用するユーザ定義のサーバアドレスを入力します。</li> </ul>
<b>シングルビュー</b>	
追跡するデバイス 変更イベント	<p>追跡するデバイス変更イベントを選択します。この設定により、[シングルビュー]ページに表示するイベントのデフォルトセットが決まります。「<a href="#">[シングルビュー]ページのフィールド</a>」(547 ページ) を参照してください。イベントは次のとおりです。</p> <ul style="list-style-type: none"> <li>• デバイス構成の変更</li> <li>• デバイスがブートしました</li> <li>• デバイス診断が変化しました</li> <li>• デバイスパスワードの変更</li> <li>• モジュールが追加されました</li> <li>• モジュールが変更されました</li> <li>• モジュールが削除されました</li> <li>• ソフトウェアの変更</li> <li>• ユーザメッセージ</li> </ul>
追跡する診断	<p>追跡する診断を選択します。この設定により、[デバイス診断の変更]イベントの種類が[シングルビュー]ページで選択されている場合に、表示する[デバイス診断の変更]イベントが決まります。「<a href="#">[シングルビュー]ページのフィールド</a>」(547 ページ) を参照してください。デフォルトの診断の種類は次のとおりです。</p> <ul style="list-style-type: none"> <li>• ハードウェア情報</li> <li>• メモリトラブルシューティング</li> <li>• NAがデバイスのブートを検出</li> <li>• NAデバイスファイルシステム</li> <li>• NAフラッシュ記憶域容量</li> <li>• NAインターフェイス</li> <li>• NAモジュールのステータス</li> <li>• NA OSPF ネイバー</li> <li>• NAルーティングテーブル</li> </ul> <p><b>注意：</b> 診断の詳細については、「<a href="#">表示メニューオプション</a>」(201 ページ) を参照してください。</p>
<b>ダイアグラム</b>	
ダイアグラムを有効にする	<p>オンにすると、ダイアグラム機能が有効になります。</p>

フィールド	説明/アクション
最大ノード	図に表示するノードの最大数を入力します。デフォルトでは250ノードです。図の生成により「メモリ不足」エラーが発生する場合、この値を下げることも可能です。ノードが多数含まれる図の場合、画像の容量が大きくなります。画像は、圧縮されていない状態でメモリに生成されてからJPEG形式で出力されます。より多くのノードを図に含める場合、値を増やすことができますが、メモリ不足が発生する可能性もあります。
ラベルのフォントサイズ	図のラベルに使用するフォントのポイントサイズを入力します。デフォルトは8ポイントです。この値を増やすと、ノードのサイズに比例してラベルのサイズも大きくなるため、ラベルが読みやすくなります。
最長レイアウト時間	実行するレイアウトのアルゴリズムの最長時間を入力します。デフォルト値は30秒です。この最大時間が経過すると、レイアウトのアルゴリズムが停止します。正確な図は、この制限値に達した後も引き続き生成されます。ただし、図のレイアウトが最適に生成されない場合もあります。
ダイアグラムの圧縮	ノード間のスペースを0から100の値で入力します。デフォルトは95です。この値はダイアグラムの広がり制御します。圧縮率の低い図のノードは読みやすくなります。圧縮率の高い図の場合、使用する空間は小さいですが、読みづらくなります。圧縮率の高い図は、レイアウトの表示に時間がかかるため、実行にも多少時間がかかります。
品質と時間の比率	希望するレイアウト比率を0から100の値で入力します。デフォルトは100です。値を高くすると、ダイアグラムはきれいに表示されますが、レイアウトに時間がかかり、CPUサイクルも増えます。
優先するエッジの長さ	0から100までの間で、優先するエッジの長さの値を入力します。デフォルトは100です。一般的に、エッジを長くすると図のノードの空間は大きくなりますが、必要に応じてレイアウトのアルゴリズムを優先させることができます。値を大きくすると、図が拡大されるため、メモリの消費が増大します。値を高くすると、ノードとラベルのエッジの重なりが少なくなるため、図が読みやすくなります。
優先最小ノード距離	0から100までの間で、優先するノードの最小距離の値を入力します。デフォルト値は20です。この値は、接続されていないクローズノードの空間を制御します。値を小さくすると、図の圧縮率が高まります。
<b>イメージ同期レポート</b>	
イメージ同期レポートのファイル	イメージ同期レポートのファイルを入力して、[ファイルを追加]ボタンをクリックします。[ファイルを削除]ボタンをクリックすると、イメージ同期レポートファイルを削除できます。イメージ同期レポートでは、デバイスやデバイスのグループ上においてNAソフトウェアイメージリポジトリにはない、現在実行中のソフトウェアイメージ、またはバックアップソフトウェアイメージを表示できます。イメージ同期レポートの詳細については、「 <a href="#">イメージ同期レポートのフィールド</a> 」(618ページ)を参照してください。
<b>その他</b>	
ExcelのCSV形式を使用	オンにすると（デフォルト）、検索結果をCSVファイルにエクスポートするときに、Microsoft ExcelのCSV形式を使用します。
レポートを保存するファイルの場所	レポートファイルの保存先となるNAサーバの保存場所のパスを入力します。ユーザが電子メールレポート作成タスクの定義時に[レポートを保存するファイルの場所]オプションを選択すると、レポートは自動的にこの場所に保存されます。デフォルトの場所はC:\インストールディレクトリ>laddinsです。



## ユーザ認証

ユーザ認証により、ユーザの認証が集中管理され、複数のデータベースの保守が不要になります。次のユーザ認証オプションを利用できます。

- LDAP (Lightweight Directory Access Protocol)
- SecurID
- TACACS+
- RADIUS
- HP Server Automation (HP SA)
- HP Operations Orchestration (HP OO)

外部認証に失敗すると、次の条件で、NAはフォールバックによりローカルユーザの資格情報を試行します。

- 外部認証サービスが停止したりアクセス不能になったりした場合。
- 外部認証方法で一度も正常にログインしたことのない静的ユーザアカウントの場合。
- 組み込み管理ユーザアカウントの場合。

**注意：** NAがローカル認証にフェイルオーバーを行うようにするには、ユーザのアカウントでこの機能を有効にする必要があります。デフォルトでは、NAはローカル認証にフェイルオーバーしません。詳細については、「[認証フェイルオーバー](#)」(73 ページ) および「[\[ユーザの新規作成\]ページのフィールド](#)」(247 ページ) を参照してください。

また、ユーザ認証により、NA内の組み込みユーザに対して次のセキュリティポリシーを構成できます。

- パスワードの最小文字数を定義する
- パスワードの複雑さのルールを定義する
- ログイン試行の連続失敗回数が構成された回数に達すると、そのユーザはロックアウトされる

[ユーザ認証] ページを表示するには、[管理] メニューバーから[システム管理設定]を選択し、[ユーザ認証]をクリックします。[ユーザ認証] ページが開きます。詳細については、「[\[ユーザ認証\]ページのフィールド](#)」(77 ページ) を参照してください。

## 認証フェイルオーバー

NAがユーザ認証に外部アプリケーションを使用するように構成されている場合、NAは特定の状況でローカル(NAアプリケーションサーバ) 認証にフェイルオーバーできます。

NAは次のユーザについて、認証フェイルオーバーを試みます。

- NAのインストール時に作成された管理者ユーザアカウント (UID = 1)
- フェイルオーバー用に構成された任意のユーザアカウント ([ユーザの新規作成]または[ユーザを編集] ページで[外部認証フェイルオーバー] チェックボックスがオンになっている)

外部認証が成功しない場合、NAは次のアルゴリズムを使用します。

- NAが外部認証アプリケーションに接続できない場合、NA consoleにログインしようとしているユーザがUID = 1か、認証フェイルオーバー用に構成されているユーザであるとき、NAはローカル認証を試みます。ユーザが認証フェイルオーバー用に構成されていない場合、NAはローカル認証を試みず、通常の認証エラーを返します。
- NAが外部認証アプリケーションに接続したものの、エラーが返された場合、NA consoleにログインしようとしているユーザがUID = 1であるとき、NAはローカル認証を試みます。その他のユーザの場合、NAはローカル認証を試みず、通常の認証エラーを返します。
- LDAP認証の場合のみ、NA consoleにログインしようとしているユーザがディレクトリサービスに存在しないとき、NAはローカル認証を試みます。

## LDAP 認証

組織でMicrosoft Active DirectoryまたはLDAP（Lightweight Directory Access Protocol）を使用している場合、グループとユーザを同時にNAへインポートできます。NAでは、LDAPデータベースとのアクティブな連携が維持されているため、アプリケーションのログインが許可されているユーザとそうでないユーザに関する情報を最新の状態に保つことができます。

外部ユーザ認証が有効な場合でも、ネットワークの問題によりLDAPサーバへ到達できない場合、NAにログインできます。NAを指定したLDAPサーバへ接続できない場合、これまでNAにログインしたことのあるユーザであれば、NAユーザのパスワードを使用してNAへログインできます。NAのパスワードは、[自分のプロファイル]ページで設定できます。詳細については、「[\[自分のプロファイル\]ページのフィールド](#)」（260ページ）を参照してください。

LDAPユーザがNAのシステム管理者と同じユーザ名でないことを確認する必要があります。デフォルトのシステム管理者のユーザ名は「admin」ですが、変更も可能です。デフォルトの管理者と別のLDAPユーザの名前が競合する場合、デフォルトの管理者がNAにログインできなくなります。

あるユーザをNAで作成してLDAPで削除した場合、そのユーザは（LDAPのパスワードではなく）NAのパスワードを使用して再度NAにログインできます。

LDAPの外部認証の設定方法の詳細については、「[LDAP外部認証の設定](#)」（80ページ）を参照してください。

## SecurID 認証

RSA SecurID ソリューションは、認証されたユーザにのみネットワーク構成されたリソースへのアクセス権を与えることで確実に組織を保護するように設計されています。一般的に、SecurIDは2要素認証方式の一種で、パスワードとPIN、そしてトークンが必要となります。トークンは60秒ごとに変更されます。詳細については、「[SecurIDソフトウェアトークンの追加](#)」（630ページ）を参照してください。

## TACACS+ 認証

Cisco IOS ソフトウェアでは、TACACS+ など、いくつかのバージョンの TACACS セキュリティ プロトコルが現在サポートされています。TACACS+ は、詳細なアカウント情報が提供され、認証および認可のプロセスを柔軟に管理できます。

お使いの TACACS+ サーバ（通常 CiscoSecure ACS）を使用してユーザを認証すると、次のような利点があります。

- NA ユーザはユーザ名とパスワードを1つ記憶していればよい
- NA ユーザの管理を ACS サーバに集中化できる
- TACACS+ パスワードの制限事項を容易に実行できる

TACACS+ サーバを使って NA ユーザを認証すると、次のようなことが可能になります。

- TACACS+ サーバを使ってユーザのログインを認証するよう NA を構成する（例：ユーザが正しいユーザ名とパスワードの組み合わせを入力したかどうかを確認する）。
- Telnet/SSH プロキシでの TACACS+ 認証をサポートする。
- 個々のユーザに NA のフォールバックパスワードを割り当てる。
- TACACS+ サーバにアクセスできない場合以外はフォールバックパスワードを使用しないよう、TACACS+ ユーザを識別する（ただし、Admin 以外のユーザが不正な TACACS+ パスワードを入力した場合は、この限りではない）。
- フォールバックのために複数の TACACS+ サーバを構成する。

他のルータと同様、TACACS+ でも NA を特定のユーザ名を持つ認証デバイスとして定義しなければなりません。これにより、ユーザが NA にログインでき、NA がネットワークデバイスにログインできるようになります。

**注意：** TACACS+ は、認可/権限には使用されません。つまり、TACACS+ 経由でユーザを認証するには、そのユーザを手動で NA に追加し、正しい権限を割り当てる必要があるということです。いったん NA でユーザを TACACS+ ユーザとして識別すれば、この指定を削除することはできません。

## RADIUS 認証

RADIUS（Remote Authentication Dial-In User Service）では、次のようなことができます。

- ネットワークアクセス・サーバを RADIUS クライアントとして動作させる。RADIUS クライアントは、情報を指定した RADIUS サーバへ送信し、返された応答を処理します。
- RADIUS サーバで接続要求を受け付け、ユーザを認証し、正しい接続に必要なクライアント構成情報をすべて返す。
- RADIUS サーバを他の RADIUS サーバまたは認証サーバのプロキシクライアントとして動作させる。

**注意：** RADIUS は、認可/権限には使用されません。つまり、RADIUS 経由でユーザを認証するには、そのユーザを手動で NA に追加し、正しい権限を割り当てる必要があるということです。いったん NA でユーザを RADIUS ユーザとして識別すれば、この指定を削除することはできません。

TACACS+ 認証またはRADIUS 認証を有効にするには、[管理]メニューバーから[システム管理設定]を選択し、[ユーザ認証]タブをクリックします。[ユーザ認証]ページが開きます。終了する場合は、必ず[保存]をクリックしてください。

## HP Server Automation (HP SA)

HP Server Automation オプションにより、NA システムで HP SA システムをユーザ認証に使用できます。その結果、HP SA ユーザは自分の HP SA 資格情報を NA へのログインに使用できます。また、このオプションでは、ネットワーク図の HP SA サーバや MAC アドレスから HP SA サーバへのリンクを表示できます。詳細については、「[NA/SA 統合](#)」(196 ページ) を参照してください。

## HP Operations Orchestration (HP OO)

IT 組織は、実行するアクションの監査証跡を行わない旧来のトラブルシューティングガイドを使用して、手動でトラブルシューティングタスクを実行することがよくあります。IT 組織が自動化ソリューションとしてスクリプトを配布する場合でも、スクリプトは維持が容易ではなく、スクリプトは監査証跡を行いません。

HP OO オプションにより、NA の Web UI からガイドモードで HP OO フローを直接起動できます。無人 HP OO フローを実行するには、言語「Flow」のコマンドスクリプトを作成する必要があります。無人フローの起動方法の詳細については、「[HP Operations Orchestration \(HP OO\) のフロー](#)」(570 ページ) を参照してください。

一般的に、HP OO を使用することで、日常業務の順位付け、トラブルシューティング、保守のタスクのすべてを NA 内で集中管理できます。どの HP OO フローが利用可能であるかを定義し、起動できます。

- 1 つまたは複数の IP アドレスが指定されているサードパーティシステムからデータを収集して表示する、無人 HP OO フロー。詳細については、「[HP Operations Orchestration \(HP OO\) のフロー](#)」(570 ページ) を参照してください。
- 事前定義された管理ソフトウェアアップグレードフロー。この HP OO フローは、監視システムからのルータの削除、OSPF メッシュからのルータの削除、IOS イメージのアップグレード、および OSPF メッシュへのデバイスの再挿入と、デバイスの監視システムへの再追加を実行します。プロセス自動化オプションの詳細については、「[編集メニューオプション](#)」(230 ページ) を参照してください。

HP OO の詳細については、『HP Operations Orchestration ユーザガイド』および『HP Operations Orchestration Software Development Kit Guide (HP Operations Orchestration ソフトウェア開発キットガイド)』を参照してください。

## [ユーザ認証]ページのフィールド

フィールド	説明/アクション
<b>ユーザパスワードのセキュリティ</b>	
ユーザパスワードの最短長さ	パスワードに含める最小文字数を入力します。パスワードの文字数がこの文字数よりも少ない場合、そのパスワードは無効とみなされます。
ユーザパスワードに大文字と小文字を含める	オンにすると、ユーザはアルファベットの大文字と小文字の両方を含むパスワードを指定する必要があります。
その他のユーザパスワード制限	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• その他の制限なし（デフォルト）</li> <li>• 英字以外に1文字以上の数字と特殊文字を含める</li> <li>• 1文字以上の数字と1文字以上の特殊文字の両方を含める</li> </ul>
最大連続ログインエラー	連続するユーザ認証エラーの最大許容回数を入力します。この回数を超えるとそのユーザは無効になります。0（ゼロ）を指定すると、この確認はスキップされます。（ <b>注意</b> ：この設定は、組み込みユーザ認証のみに適用され、外部認証方式には適用されません）。
<b>外部認証の種類</b>	
外部認証の種類	使用する外部認証の種類を選択します。次のオプションが用意されています。 <ul style="list-style-type: none"> <li>• なし（ローカル認証）</li> <li>• HP Server Automation</li> <li>• HP Server Automation &amp; TACACS+</li> <li>• TACACS+</li> <li>• RADIUS</li> <li>• SecurID</li> <li>• LDAP</li> </ul> <p>[TACACS+]または[RADIUS]を選択した場合、次のセクションの構成が可能となります。[LDAP]を選択した場合、[LDAP設定]リンクをクリックします。詳細については、「<a href="#">LDAP外部認証の設定</a>（80ページ）」を参照してください。[SecurID]にはその他の外部認証オプションはありません。</p>
<b>TACACS+ 認証/RADIUS 認証</b>	
プライマリ TACACS+ サーバまたはプライマリ RADIUS サーバ	プライマリ TACACS+ サーバまたはプライマリ RADIUS サーバのホスト名またはIPアドレスを入力します。
セカンダリ TACACS+ サーバまたはセカンダリ RADIUS サーバ	セカンダリ TACACS+ サーバまたはセカンダリ RADIUS サーバのホスト名またはIPアドレスを入力します。このフィールドは省略可能です。
TACACS+ または RADIUS の秘密情報	TACACS+ サーバまたはRADIUS サーバで構成されるNAホストの秘密鍵を入力します。TACACS+またはRADIUSの共通鍵は、TACACS+またはRADIUSクライアント（NA）でTACACS+またはRADIUSサーバとの通信の暗号化に使用する鍵（パスワード）です。クライアントとサーバは、サーバが通信を復号化できるように、この鍵の情報について合意する必要があります。

フィールド	説明/アクション
TACACS+ または RADIUS の認証方法	<p>NA と TACACS+ または RADIUS サーバとの通信の暗号化に使用する認証方法を、次の中から選択します。</p> <ul style="list-style-type: none"> <li>• PAP (パスワード認証プロトコル)</li> <li>• CHAP (チャレンジハンドシェイク認証プロトコル)</li> <li>• MCHAP (Microsoft チャレンジハンドシェイク認証プロトコル)</li> <li>• ARAP (TACACS+ のみ)</li> <li>• ASCII (TACACS+ のみ)</li> </ul>
デフォルト NA-ID の代わりに RADIUS NA-IP を使用	<p>このオプションを選択すると、デフォルトの NA-ID フィールドの代わりに NA コア情報を使用して RADIUS NA-IP フィールドが送信されます。最初に見つかった NA コアの非ループバック IP アドレスが送信されます。<b>(注意: この設定の「NA」は、NA 製品用ではありません。RADIUS 認証固有のものです。)</b></p>
固定 RADIUS NA-IP 文字列	<p>[RADIUS NA-IP] フィールドとして、見つかったデフォルト IP アドレスの代わりに固定文字列を使用します。このオプションを使用して、デフォルト値の代わりとして [NA-IP] フィールドに使用する IP アドレスを NA に通知します。これは、複数のネットワークインターフェイスカードシステムがある場合、またはフィールドをサーバにバインドされていない IP アドレスに設定する場合のみ使用してください。<b>(注意: この設定の「NA」は、NA 製品用ではありません。RADIUS 認証固有のものです。)</b></p>
<b>HP Server Automation の認証</b>	
Twist サーバ	HP Twist サーバのホスト名または IP アドレスを入力します。詳細については、『HP Server Automation UserOs Guide』を参照してください。
Twist ポート番号	HP Twist サーバへの接続に使用する Twist ポート番号 (通常 1032) を入力します。詳細については、『HP Server Automation User's Guide』を参照してください。
Twist ユーザ名	Twist Web サービス API (wsapi) ユーザ名 (通常は <i>wsapiReadUser</i> ) を入力してください。
Twist パスワード	Twist Web サービス API (wsapi) パスワードを入力してください。
OCC サーバ	<p>接続先サーバに接続するための、OCC (HP Command Center) のホスト名を入力します。OCC サーバは、HP サーバ自動システム (HP SA) の Web UI クライアントです。NA では、HP SA へのハイパーリンクを作成できます。その結果、[NA サーバ] ページから [HP SA サーバ] ページへジャンプできます。詳細については、<b>「[サーバ] ページのフィールド」 (222 ページ)</b> を参照してください。</p>
デフォルトのユーザグループ	<p>HP SA の認証済みユーザをドロップダウンメニューから追加するための、追加先となるユーザグループの名前を選択します。このグループでは、デフォルトの HP SA ユーザ権限を設定できます。詳細については、<b>「NA/SA 統合」 (196 ページ)</b> を参照してください。</p>
<b>HP Operations Orchestration の認証</b>	
HP OO ホスト名	HP OO サーバのホスト名、または IP アドレスを入力します。
HP OO ポート	HP OO サーバに接続するための HP OO ポート番号を入力します。
HP OO サービス	<p>HP OO サービスに接続するオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• https://</li> <li>• http://</li> </ul> <p>HP OO サービスは SSL、またはプレーンテキストを使用します。</p>

フィールド	説明/アクション
HP OOユーザ名	HP OOユーザ名を入力します。
HP OOパスワード	HP OOパスワードを入力します。
ガイド付きフロー名	<p>右側のボックスにガイド付きフロー名を入力して[フローを追加&lt;&lt;]をクリックします。フローはすべてのデバイスファミリに適用されます。ガイド付きフローの名前に「Cisco IOS:flow 1」という接頭辞を付けると、ガイド付きフローはCisco IOSデバイスファミリに属すすべてのデバイスに適用されます。ガイド付きフローを削除するには、左側のボックスからガイド付きフローを選択して[フローを削除]をクリックします。</p> <p>フローの構成の詳細については、『HP Operations Orchestration ユーザガイド』を参照してください。HP OOへのログインの詳細については、「<a href="#">編集メニューオプション</a>」(230ページ)を参照してください。</p>

## LDAP 外部認証の設定

LDAP 外部認証を有効にするには：

1. [管理]メニューバーから[システム管理設定]を選択し、[ユーザ認証]をクリックします。[システム管理設定-ユーザ認証]ページが開きます。
2. [外部認証の種類]フィールドまでスクロールします。
3. [外部認証の種類]フィールドで[LDAP]を選択して[保存]をクリックします。
4. [LDAP 設定]リンクをクリックします。LDAP 設定ウィザードが開きます。これまでにLDAP 認証を設定したことがある場合、次の情報が表示されます。
  - LDAP 認証ステータス
  - LDAP 認証サーバホスト
  - ポート
  - 接続ユーザ名
  - 接続ユーザパスワード
  - 検索ベース
  - セキュア接続を使用
  - サーバタイムアウト

**注意：**NAはユーザがログインするたびにフィールドが同じであるかどうかを確認します。必要に応じて、NAは[ユーザ]フィールド情報を対応するLDAP 情報で更新します。たとえば、NA 管理者がNA のユーザA を手動で更新してユーザA の電子メールアドレスを変更すると、次回ユーザA がログインしたときに、ユーザA の電子メールアドレスがLDAP 内の値に自動的に変更されます。

次の表で、設定のプロセスについて説明します。

手順	アクション
1	<p>[LDAP 設定ウィザードへようこそ]ページで[次へ]をクリックします。次の情報を入力して[次へ]をクリックします。</p> <ul style="list-style-type: none"><li>• サーバタイプ：サーバタイプを[Active Directory]（デフォルト値）、または[通常のLDAP]から選択します。</li><li>• サーバ名：LDAP、またはActive Directoryサーバのホスト名、つまり、AD/ドメインコントローラのホスト名、またはIPアドレスを入力します。</li><li>• ポート：LDAP要求ポート番号を入力します。単一ドメイン構成の場合、ポート389または636（SSLを使用している場合）を使用します。</li><li>• 接続タイプ：[通常の接続]（デフォルト）または[セキュア接続（SSL）]を選択します。ディレクトリサーバへ接続する場合、[セキュア接続]を選択してください。（<b>注意：</b>このオプションを有効にして、お使いのディレクトリサーバ/ドメインコントローラサーバの証明書が既知のCAにより署名されていない場合、NA を実行するサーバへ証明書を手動でインポートする必要があります。）LDAPのSSL構成の詳細については、「<a href="#">LDAP SSL 構成</a>」（81 ページ）を参照してください。</li><li>• サーバタイムアウト：LDAP操作のタイムアウトをミリ秒単位で入力します。この値よりも長いLDAP操作は中断されます。</li></ul>



手順	アクション
2	<p>次の情報を入力して[次へ]をクリックします。</p> <ul style="list-style-type: none"><li>• 接続ユーザ名：接続ユーザ名を入力します。ADサーバからユーザ情報をクエリする場合、ドメインのユーザアカウント（DN）でADサーバとNAをバインドする必要があります。DNは、Windows 2000 LDAP形式とWindows 2000 ユーザプリンシパル名（UPN）形式のいずれかです。Windows 2000 UPN形式は、LDAP ツリー内のDNを一意に特定します。ユーザアカウントとそれぞれのドメインの両方が、UPNに含まれます。<i>jsmith@hp.com</i>は、Windows 2000 UPNのDNの例です。</li><li>• 接続ユーザパスワード：接続ユーザパスワードを入力します。</li><li>• 検索ベース：検索ベースを入力します。検索ベースは、LDAP 検索のためのLDAPディレクトリ内の開始点です。検索ベースは、AD フォレスト全体のルートドメインに設定するのが理想的です。これにより、NAからWindows 2000 AD フォレスト全体をクエリできます。検索ベースを特定のOUレベルに設定した場合、そのOUの子オブジェクトのみをクエリできます。検索ベースを特定のドメインレベルに設定した場合、そのドメインの子オブジェクトのみをクエリできます。そのため、検索ベースはできるだけ一般的なものに設定する必要があります。</li></ul>
3	<p>NAにアクセス可能なセキュリティグループを示します。[検索]オプションを使用して、LDAPのユーザグループを指定して[次へ]をクリックします。</p>
4	<p>ユーザ名とパスワードを入力して[ログインのテスト]ボタンをクリックすると、[外部認証]設定を確認できます。設定情報を保存するには、[保存]ボタンをクリックしてください。エラーがなければ、次のようなメッセージが表示され、[外部認証設定の概要]ページが更新されます。</p> <p>これで外部認証の設定は更新されます。</p>

## LDAP SSL 構成

LDAP SSL 構成では：

1. Windows 2000またはWindows 2003 Serverにエンタープライズ証明機関をインストールします。フォレスト内にあるすべてのドメインコントローラが自動的に登録され、適切な証明書がインストールされます。
2. グループポリシーエディタを使用してデフォルトのドメインコントローラポリシーを開きます。
3. [コンピュータの構成]で[Windowsの設定]をクリックします。
4. [セキュリティの設定]、[パブリックキーポリシー]の順にクリックします。
5. [自動証明書要求の設定]をクリックします。
6. ウィザードを使ってドメインコントローラにポリシーを追加します。

詳細については、Microsoft サポート技術情報（Q247078）を参照してください。

証明書をインポートするには：

1. （通常LDAPサーバ上）で、[スタート]→[プログラム]→[管理ツール]→[証明機関]の順にクリックして、[証明機関]管理コンソールを起動します。
2. [証明書 - ローカル コンピュータ]の中から、お使いのドメインコントローラの証明書を発行する証明機関を探します。
3. 証明機関を右クリックして[プロパティ]を選択します。
4. [全般]タブで[証明書の表示]をクリックします。

5. [詳細]タブで[ファイルにコピー]を選択します。
6. ウィザードを使って証明書をBase64 Encodedファイルにエクスポートします。
7. このファイルをNAサーバへコピーします。
8. Windowsのコマンドプロンプトで次のディレクトリに移動します。  
<インストールディレクトリ>\jre\bin
9. 次のように入力します。keytool -import -file PATH\_TO\_THE\_CERT\_FILE -alias ADSCert -keystore ../../server/ext/jboss/server/default/conf/truecontrol.keystore

キーストアパスワードは「sentinel」です。

PATH\_TO\_THE\_CERT\_FILEの部分を手順7で作成したファイルの絶対パスに置き換えます。

10. NAをサービスアプレット（または、SolarisまたはLinuxの/etc/init.d/truecontrolスクリプト）により再起動します。UIからNAを再起動すると、キーストアの変更は読み込まれません。

## サーバ監視

サーバ監視により、NAサーバ全体の状態を確認できます。エラーが発見されると、アラートの通知およびイベントのログ記録が開始されます。サーバ監視は、NAに事前に組み込まれて出荷されています。

エラーを受信すると、NA監視エラーイベントがトリガされ、エラーの通知がシステム管理者に送信されます。システムが確認された後でもエラー状態が継続している場合は、その監視の監視エラーイベントは引き続き送信されません。監視がエラー状態になって影響を及ぼすイベントがいったんトリガされれば、システムは状態の正常時に、「監視の正常動作」イベントのみを送信します。

**注意：** システムを再起動してもエラー状態が改善されない場合、新たに監視エラーイベントがトリガされます。データベースにアクセスできない場合、システムはその事実を電子メールで管理者に送信しようとしています。

[サーバ監視] ページでは、サーバ監視を構成できます。また、すべてのサーバ監視または特定のサーバ監視を有効にするオプションもあります。最近の監視の実行結果は、その監視のログファイルに保存され、[システムステータス] ページで表示できます。[システムステータス] ページの詳細については、「[\[サーバ監視\] ページのフィールド](#)」(83 ページ) を参照してください。

**注意：** 監視タスクの設定を変更できるのは、管理者のみです。結果の表示はすべてのユーザが可能です。

[サーバ監視] ページを表示するには、[管理] メニューバーから [システム管理設定] を選択し、[サーバ監視] をクリックします。[サーバ監視] ページが開きます。

## [サーバ監視] ページのフィールド

フィールド	説明/アクション
<b>サーバ監視</b>	
サーバの監視を有効にする	オンにすると（デフォルト）、サーバ監視が有効になります。NAエラーが発生すると電子メールが生成されます。最近の結果は監視ログファイルに保存され、[システムステータス] ページで表示できます。オフにすると、スケジュールされた監視による確認は実行されなくなります。ただし、サーバ監視は手動で実行できます。
スタートアップ時に監視を開始するまでの待ち時間	スタートアップ時にサーバ監視を開始するまでの待ち時間を分単位で入力します。デフォルトでは2分です。
監視の実行間隔	監視の実行間隔（分単位）を入力します。デフォルトでは360分です。
ConfigMonitor を有効にする	オンにすると、ConfigMonitor が有効になります。この監視は、インストール済みの .rcx ファイルとその他の設定ファイルの状態を確認します。この監視は、インストール時の初期の .rcx ファイルをバックアップし、最新のエラーがない状態のインストール済み .rcx ファイルのバックアップを保存します。

フィールド	説明/アクション
DatabaseDataMonitor を有効にする	オンにすると、DatabaseDataMonitor が有効になります。この監視は、すべての主要なシステムコンポーネントがデータベースにあるかどうかを確認します。たとえば、admin ユーザが存在するかどうか、暗号化キーが複数存在していないかどうか、一時停止または保留の状態にあるインベントリのスナップショットタスクがあるかどうかなどです。この監視では、(データベースサーバがダウンした場合に備えて) 暗号化キーおよび admin の電子メールアドレスのバックアップを作成します。
DatabaseMonitor を有効にする	オンにすると、DatabaseMonitor が有効になります。この監視では、無効な資格情報がないかどうか、接続の数が多すぎないかどうかなど、データベース接続の状態を確認します。
DiskMonitor を有効にする	オンにすると、DiskMonitor が有効になります。この監視では、ディスク空き容量が不足していないかどうかを確認します。
DynamicDeviceGroupMonitor を有効にする	オンにすると、DynamicDeviceGroupMonitor が有効になります。このモニタは動的デバイスグループ数をカウントします。
FTPMonitor を有効にする	オンにすると、FTPMonitor が有効になります。この監視では、タイムスタンプ付きの FTP ファイルがローカルマシンへ転送し、正しく書き込まれているかどうかファイルシステムを確認します。
HTTPMonitor を有効にする	オンにすると、HTTPMonitor が有効になります。この監視では、NA Web サーバが正しく実行されているかどうかを確認します。
LDAPMonitor を有効にする	オンにすると、LDAPMonitor が有効になります。この監視では、LDAP サーバを利用できるかどうかを確認します。
LicenseMonitor を有効にする	オンにすると、LicenseMonitor が有効になります。この監視では、利用可能であるライセンスが管理対象デバイスのパーセントを下回るかどうか、指定期間中に次のライセンスが期限切れになるかどうかのいずれか、または両方を確認します。詳細については、以下の「監視の構成」を参照してください。
LogMonitor を有効にする	オンにすると、LogMonitor が有効になります。LogMonitor は、ログ設定の管理を担当します。ログレベルが長時間にわたってトレースやデバッグのままであると、システムの性能に影響する場合があります。LogMonitor はこれらの低レベルのままになっているログを定期的に確認し、エラーレベルに再設定します。
MemoryMonitor を有効にする	オンにすると、MemoryMonitor が有効になります。この監視では、メモリが不足していないかどうかを確認します。
RMIMonitor を有効にする	オンにすると、RMIMonitor が有効になります。この監視では、NA EJB への RMI アクセスが機能しているかどうかを確認します。また、その他一部の EJB コンテナ (Java アプリケーションサーバ) が RMI ポートを独占していないかどうかを確認します。
RunExternalTaskMonitor を有効にする	オンにすると、RunExternalTaskMonitor が有効になります。この監視では、NA サーバが外部 .bat ファイルまたは .sh ファイルを実行できるかどうかを確認します。
SatelliteMonitor を有効にする	オンにすると、SatelliteMonitor が有効になります。このモニタは Syslog と TFTP が実行中であること、およびサテライトが NA コアと同じバージョンであることを確認します。NA サテライト構成については、『NA Satellite Guide』を参照してください。
SMTPMonitor を有効にする	オンにすると、SMTPMonitor が有効になります。この監視では、構成済みメールサーバ上で Telnet 接続のポートを 23 に構成し、SMTP の QUIT コマンドを送信し、適切な応答コード 221 が送信されるまで待機します。

フィールド	説明/アクション
SSHMonitorを有効にする	オンにすると、SSHMonitorが有効になります。この監視では、NAに組み込まれたSSHサーバへの接続をテストします。
SoftwareImage Management Monitorを有効にする	オンにすると、SoftwareImageManagementモニタが有効になります。SWIMが有効である場合、このモニタはSWIMサーバと通信ができることを確認します。
SyslogMonitorを有効にする	オンにすると、SyslogMonitorが有効になります。この監視では、NAへSyslogメッセージを送信し、NA管理エンジンで正しく受信されているかどうか確認します。
TelnetMonitorを有効にする	オンにすると、TelnetMonitorが有効になります。この監視では、NAに組み込まれたTelnetサーバが正しく動作しているかどうかを確認します。
TFTPMonitorを有効にする	オンにすると、TFTPMonitorが有効になります。この監視では、タイムスタンプ付きのファイルがローカルマシンへTFTP転送し、正しく書き込まれているかどうかファイルシステムを確認します。
<b>監視の構成</b>	
DatabaseDataMonitor に保存されているスナップショットを確認	オンにすると、DatabaseDataMonitorに保存されているインベントリのスナップショットを確認します。
警告のしきい値（ディスク空き容量）	ディスク空き容量の警告メッセージのトリガとなるしきい値を入力します。デフォルトは20 MBです。
エラーのしきい値（ディスク空き容量）	ディスク空き容量のエラーメッセージのトリガとなるしきい値を入力します。デフォルト値は10MBです。
ディスク容量を監視するドライブ	右側のボックスにドライブ名を入力して[ドライブの追加<<]をクリックします。ドライブを削除するには、左側のボックスからドライブ名を選択して[ドライブの削除]をクリックします。
警告のしきい値（管理対象デバイス数）	合計ライセンスのパーセントを入力します。利用できるライセンス数がこのパーセントを下回ると、警告が発行されます。デバイス数しきい値はデフォルトで10%になります。
警告のしきい値（ライセンス期限切れ）	日数を入力します。次のライセンスが指定した日数のうちに期限切れになる場合、警告が発行されます。期限切れ日のしきい値はデフォルトで30日です。
ログ監視が問題を検出すると、自動的にログをERRORにリセットし、タスクログを閉じます。	このオプションは、デフォルトでオンです。このオプションをオンにした場合、ログが長時間にわたって低レベルに設定されていることをログ監視が検出すると、ログ監視はログのレベルをERRORに再設定します。
TRACE レベルに設定されたログのオープン時間がそれより長くなると、長すぎるとレポートされるしきい値	デフォルトは48時間（2,880分間）です。ログが長時間低いレベルに設定されているとログ監視が判断しない状態で、ログをTRACEレベルに留められる時間です。
DEBUG レベルに設定されたログのオープン時間がそれより長くなると、長すぎるとレポートされるしきい値	デフォルトでは48時間です。ログが長時間低いレベルに設定されているとログ監視が判断しない状態で、ログをDEBUGレベルに留められる時間です。
アクティブタスクのログオープン時間がそれより長くなると、長すぎるとレポートされるしきい値	デフォルトは6時間（360分間）です。アクティブタスクログのオープン時間がそれより長くなると、長すぎるとレポートされるしきい値

フィールド	説明/アクション
警告のしきい値（RAMの空き容量）	RAM 空き容量の警告メッセージの発生条件となるしきい値を入力します。デフォルトでは20MBです。
エラーのしきい値（RAMの空き容量）	RAM 空き容量のエラーメッセージの発生条件となるしきい値を入力します。デフォルト値は10MBです。
SSHスレッド確認の待ち時間	SSHスレッドチェックの待ち時間を入力します。デフォルトは15000ミリ秒です。
TFTPファイル確認の待ち時間	TFTPファイルチェックの待ち時間を入力します。デフォルトは5000ミリ秒です。
FTPファイル確認の待ち時間	FTPファイル確認の待ち時間を入力します。デフォルトでは5000ミリ秒です。
syslog メッセージを表示するまでの待ち時間	Syslog メッセージを表示するまでの待ち時間を入力します。デフォルトは45000ミリ秒です。

変更を保存するには、必ず[保存]をクリックしてください。

## サードパーティ統合

HP Network Node Manager i ソフトウェア（NNMi）を使用した統合により、HP NNMi および NA の両方を実行するシステムに次の機能と利点がもたらされます。

- アラームの統合
- NNMiからのNA構成履歴へのアクセス
- 運用の効率性

HP NNMi と HP NA の統合を有効化するには、『HP Network Node Manager i Software - HP Network Automation Integration Guide（HP Network Node Manager i ソフトウェア - HP Network Automation 統合ガイド）』の手順に従います。この手順では、NNMi コンソールの HP NNMi - HP NA 統合構成フォームで NA と NNMi の通信を構成します。統合により、NA コンソールの [サードパーティ統合] ページの対応するフィールドが設定されます。

NNMi デバイスの再検出、非稼働の開始、SNMP コミュニティ文字列の送信で開始される HP NNMi - HP NA 統合の動作を変更するには、NA コンソールの [サードパーティ統合] ページで構成を更新します。

**注意：** NA console のこのページから NA と NNMi の統合を有効化または無効化することはできません。このページでは、NNMi デバイス再検出のトリガ、非稼働のトリガ、SNMP コミュニティ文字列の送信の統合動作を変更のみ行います。

HP NNMi と HP NA の統合の詳細については、『HP Network Node Manager i Software - HP Network Automation Integration Guide（HP Network Node Manager i ソフトウェア - HP Network Automation 統合ガイド）』を参照してください。

[サードパーティ統合] ページを表示するには、[管理] メニューバーから [システム管理設定] を選択し、[サードパーティ統合] をクリックします。[サードパーティ統合] ページが開きます。

## [サードパーティ統合] ページのフィールド

フィールド	説明/アクション
<b>サードパーティ統合</b>	
サードパーティ統合	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• 有効</li> <li>• 無効（デフォルト）</li> </ul> <p>この設定は変更不要です。次の点に注意してください。</p> <ul style="list-style-type: none"> <li>• NNMi コンソールから HP NNMi と HP NA の統合を有効化すると、このフィールドが有効になります。</li> <li>• このフィールドを無効に設定しても、HP NNMi と HP NA の統合は無効化されません。</li> </ul>
<b>NNMi 統合</b>	
NA ユーザ	NA-NNMi 統合ユーザ名を入力します。
NA パーティション	NA-NNMi 統合パーティション名を入力します。NA パーティションの作成方法の詳細については、「 <b>パーティション</b> 」(156 ページ) を参照してください。

フィールド	説明/アクション
NNMi ホスト	NNMi サーバのホスト名またはIPアドレスを入力します。
NNMi プロトコル	NNMi Web サービスに接続するプロトコルを選択します。
NNMi ポート	NNMi 管理サーバのWeb サービスのポート番号を入力します。HTTP 接続の場合、デフォルトポートは80です。HTTPS 接続の場合、デフォルトポートは443です。
NNMi ユーザ	NNMi ログインユーザ名を入力します。
NNMi パスワード	NNMi ログインパスワードを入力します。
タスク後のホストの再検出	<p>リストからタスクを選択します。選択したタスクが正常に実行されると、NNMi でデバイスが再検出されます。デフォルトのタスクを以下に挙げます。</p> <ul style="list-style-type: none"> <li>• デバイスソフトウェアの更新</li> <li>• パスワードの配布</li> <li>• デバイスのリブート</li> <li>• ドライバの検出</li> </ul>
非稼働イベント	<p>リストからタスクを選択します。タスク開始時には、NAはNNMi Web サービスを呼び出し、デバイスを「非稼働中」に指定します。これにより、NNMiは一時的にデバイスを管理しなくなります。このタスクの完了後、NAはNNMi Web サービスを呼び出し、デバイスを管理中として指定します。デフォルトのタスクを以下に挙げます。</p> <ul style="list-style-type: none"> <li>• デバイスソフトウェアの更新</li> <li>• パスワードの配布</li> <li>• デバイスのリブート</li> </ul>
デバイスタスクが失敗する場合	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• デバイスを稼働状態に設定する（デフォルト）。</li> <li>• デバイスを稼働状態に設定しない。</li> </ul>
タスク完了後にデバイス準備の確認に失敗する場合	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• デバイスを稼働状態に設定する（デフォルト）。</li> <li>• デバイスを稼働状態に設定しない。</li> </ul>
SNMP コミュニティ文字列の送信	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 有効</li> <li>• 無効（デフォルト）</li> </ul>



## 監視結果の表示

[システムステータス]ページでは、最近の監視の実行結果が表示されます。[システムステータス]ページを表示するには、[管理]メニューバーから[システムステータス]をクリックします。[システムステータス]ページが開きます。

### [システムステータス]ページのフィールド

フィールド	説明/アクション
すべて実行	リストにある監視をすべて実行します。
サーバ監視を構成	[サーバ監視]ページを開きます。詳細については、「 <a href="#">[サーバ監視]ページのフィールド</a> 」(83ページ)を参照してください。
監視名	監視名が表示されます。各監視から、監視対象サブシステムに関するさまざまなメッセージが返されます。 <a href="#">「監視のメッセージ」</a> (90ページ)を参照してください。
ステータス	次のような監視のステータスが表示されます。 <ul style="list-style-type: none"><li>• OK</li><li>• 警告</li><li>• エラー</li><li>• 無効</li></ul>
最終確認	監視を最後に実行した日付と時刻が表示されます。
結果	結果に関する情報が表示されます。
アクション	次のオプションを選択できます。 <ul style="list-style-type: none"><li>• 直ちに実行：監視が直ちに実行されます。</li><li>• 詳細を表示：[監視の詳細]ページが開きます。このページでは、監視の説明、ステータス、結果、追加の診断情報など、監視に関する詳細情報が表示されます。</li><li>• サービスの開始/停止：[サービスの開始/停止]ページが開きます。詳細については、「<a href="#">サービスの開始および停止</a>」(94ページ)を参照してください。</li></ul>

## 監視のメッセージ

各監視から、監視対象サブシステムに関するさまざまなメッセージが返されます。このセクションでは、次のいくつかのメッセージと、考えられる対応策について詳細に説明します。

監視	説明/対応策
BaseServerMonitor	<p>&lt;スレッド名&gt;が実行されていません。: NAが正しく動作するのに必要なスレッドが何らかの理由で実行されていません。NA管理エンジンを再起動する必要があります。</p>
ConfigMonitor	<ul style="list-style-type: none"> <li>• &lt;ファイル名&gt;.rcxが見つかりません。: NAに必要な構成ファイルの一つが見つかりません。サポートに問い合わせてください。</li> <li>• &lt;ファイル名&gt;.rcxから必要な構成を取得しようとしてエラーが発生しました。: NA構成ファイルの一つが破損しています。サポートに問い合わせてください。</li> <li>• 次の.rcxファイルの解析で例外が発生しました:&lt;ファイル名&gt;:NA構成ファイルの一つが破損しています。サポートに問い合わせてください。</li> </ul>
MySQLのDatabaseMonitor	<ul style="list-style-type: none"> <li>• &lt;サーバ名&gt;:3306でMySQLサーバに接続できません:NAが接続を試みている場所でMySQLサーバが実行されていません。MySQLサービスを再起動するか、またはNA接続情報が正しいかどうかを確認する必要があります。</li> <li>• 通信リンクの失敗: java.io.IOException: MySQLサーバへの接続が失われました。NA管理エンジンを再起動するか、またはMySQLサービスを再起動する必要があります。</li> <li>• &lt;ユーザ名&gt;ユーザのログインに失敗しました。&lt;データベース名&gt;: NAが無効なデータベースに接続しようとしているか、または既存データベースへの権限に何らかの問題があります。NAの接続情報が正しいかどうかを確認する必要があります。</li> <li>• 無効な認証指定: 次のユーザのアクセスが拒否されました:&lt;ユーザ名&gt;(パスワードの使用:あり): NAが不正なユーザ名またはパスワードを使用して接続を試みています。NAデータベースのユーザ名とパスワードを正しい値にリセットする必要があります。</li> <li>• 一般エラー: NA.RN_CRYPT0_KEYテーブルが存在しません: NAは所定の資格情報を使ってデータベースに接続できますが、そのデータベースがNAデータベースではないか、または(RN_CRYPT0_KEYテーブルがないために)破損しています。NAの接続情報が正しいかどうかを確認する必要があります。</li> </ul>
OracleのDatabaseMonitor	<ul style="list-style-type: none"> <li>• ソケットの確立エラー。次の接続が拒否されました: 接続名: NAが接続しようとしている場所でOracleが実行されていません。Oracleサービスを再起動するか、またはNA接続情報が正しいかどうかを確認する必要があります。</li> <li>• ピアにより接続がリセットされました: ソケット書き込みエラー。: Oracleサーバへの接続が失われました。NA管理エンジンまたはOracleを再起動する必要があります。</li> <li>• ORA-12505接続が拒否されました。指定したSID(&lt;データベース名&gt;)がOracleサーバで認識されていません。: NAが無効なデータベース名に接続しようとしています。NAの接続情報が正しいかどうかを確認する必要があります。</li> <li>• ORA-01017: 無効なユーザ名/パスワード; ログインが拒否されました: NAが無効なユーザ名またはパスワードを使って接続を試みています。NAデータベースのユーザ名とパスワードを正しい値にリセットする必要があります。</li> <li>• ORA-00942: テーブルまたはビューが存在しません: NAは所定の資格情報を使ってデータベースに接続できますが、そのデータベースがNAデータベースではないか、または(RN_CRYPT0_KEYテーブルがないために)破損しています。NAの接続情報が正しいかどうかを確認する必要があります。</li> </ul>

監視	説明/対応策
SQLServerの DatabaseMonitor	<ul style="list-style-type: none"> <li>• ソケットの確立エラー。: NAが接続しようとしている場所でSQLServerが実行されていません。SQLServerサービスを再起動するか、またはNA接続情報が正しいかどうかを確認する必要があります。</li> <li>• ピアにより接続がリセットされました: ソケット書き込みエラー。: SQLServerへの接続が失われました。NA管理エンジンまたはSQLServerを再起動する必要があります。</li> <li>• ログインに必要な次のデータベースを開くことができません: &lt;データベース名&gt;。ログインに失敗しました。: NAが無効なデータベース名に接続しようとしているか、または既存データベースへの権限に何らかの問題があります。NAの接続情報が正しいかどうかを確認する必要があります。</li> <li>• &lt;ユーザ名&gt;ユーザのログインに失敗しました。: NAが無効なユーザ名またはパスワードを使って接続しようとしています。NAデータベースのユーザ名とパスワードを正しい値にリセットする必要があります。</li> <li>• RN_CRYPTOKEYは無効なオブジェクト名です。: NAは所定の資格情報を使ってデータベースに接続できますが、そのデータベースがNAデータベースではないか、または(RN_CRYPTOKEYテーブルがないために)破損しています。NAの接続情報が正しいかどうかを確認する必要があります。</li> </ul>
DatabaseData 監視	<ul style="list-style-type: none"> <li>• 管理ユーザが見つかりませんでした。: NAで管理者ユーザが構成されていません。サポートに問い合わせてください。</li> <li>• 複数の暗号化キーが存在します。: NAのデータベースに複数の暗号化キーがあります。サポートに問い合わせてください。</li> <li>• 現在のキーは保存されているキーと一致しません。: NAで使用中の暗号化キーが異なります。サポートに問い合わせてください。</li> <li>• 複数の暗号化キーがあります。: NAで使用中の暗号化キーが異なります。サポートに問い合わせてください。</li> <li>• インベントリグループスナップショットが見つかりませんでした。: システムの全デバイスから構成を収集するためのタスクがNAにありません。インベントリグループのスナップショットタスクを作成する必要があります。</li> <li>• レポート作成タスクが見つかりませんでした。: サマリレポートを生成するためのタスクがNAにありません。[サマリレポートの生成]タスクを作成する必要があります。</li> <li>• プルーフタスクが見つかりませんでした。: データベースの古いデータを整理するためのタスクがNAにありません。[データベースの整理]タスクを作成する必要があります。</li> </ul>
DiskMonitor	<p>&lt;ファイルシステム名&gt;ディスク/ファイルシステムの空き容量が&lt;数値&gt;バイトしかありません。エラーのしきい値は&lt;制限値&gt;バイトです。: NAサーバのディスクドライブの空き容量が少なくなっています。不要なファイルをディスクドライブから削除する必要があります。</p>
HTTPMonitor	<p>NAログインページを開けません。: アプリケーションは構成済みのHTTP/HTTPSポートで実行されていますが、NA Webサーバではないようです。NAサーバで実行中の他のWebサーバ(IISなど)を停止し、NA管理エンジンを再起動する必要があります。</p>

監視	説明/対応策
LDAPMonitor	<ul style="list-style-type: none"> <li>• Active Directoryが使用されていません。: これは、NAサーバでActive Directoryを使用するよう構成されていないことを示す情報メッセージです。</li> <li>• LDAPMonitorの例外: javax.naming。通信の例外: &lt;ホスト名&gt;: 389: &lt;ホスト名&gt;ホストが存在しません。外部認証のサーバ名の設定を変更する必要があります。</li> <li>• LDAPMonitorの例外: javax.naming。通信の例外: &lt;ホスト名&gt;: 389: &lt;ホスト名&gt;ホストは存在しますが、LDAPポート(389)の接続が許可されていません。サーバ名の設定が正しいかどうかを確認する必要があります。正しければ、LDAPサーバがそのホストで実行されているかどうかを確認します。</li> <li>• LDAPMonitorの例外: javax.naming。認証の例外: 外部認証の[接続ユーザ名]または[接続ユーザパスワード]の設定が間違っています。これらの設定を修正する必要があります。</li> </ul>
LicenseMonitor	<p>「License about to expire(期限切れが間近のライセンス)」や「Device count exceeds the current threshold of available licenses(デバイス数が、現在の利用可能なライセンスのしきい値を超過)」などの警告は、[結果]列に表示されます。警告が表示されない場合、利用可能なデバイスライセンス数(「3600 デバイスライセンスのうち3454が残っています。」など)が表示されます。[詳細を表示]リンクをクリックして、使用中のライセンス、未使用のライセンス、およびライセンス失効日などのライセンスの詳細を表示できます。(注意: 複数のライセンスが使用されている場合、失効日は次に失効するライセンスの失効日です。)</p>
MemoryMonitor	<p>空き容量が&lt;バイト数&gt;バイトしかありません。: システムでのメモリの空き容量を示します。[エラー]状態が発生すると、システムが正しく動作するのに必要なメモリの空き容量が不足しています。サポートに問い合わせてください。</p>
RMIMonitor	<p>RMIポート1099に接続できません。: 別のアプリケーションがポート1099を使用しています。このポートは、NAでクライアントやAPIが正しく動作するのに必要なポートです。ポート1099を使用中のアプリケーションを停止し、NA管理エンジンを再起動する必要があります。この操作が不可能な場合は、サポートに問い合わせてください。</p>
RunExternalTask 監視	<ul style="list-style-type: none"> <li>• CreateProcess: &lt;パス名&gt;\tc_test.bat error=5: NAにテストスクリプト(およびその他のスクリプト)へのアクセス権がありません。NAディレクトリのファイルシステムの権限を確認する必要があります。</li> <li>• CreateProcess: &lt;パス名&gt;\tc_test.bat error=2: NAにテストスクリプトがありません。サポートに問い合わせてください。</li> <li>• &lt;パス名&gt;ディレクトリから&lt;パス名&gt;\tc_test.batを実行しています。結果コード: 0 Got output&lt;テキスト&gt;を取得しました。: テストスクリプトが破損しています。サポートに問い合わせてください。</li> </ul>
SMTPMonitor	<ul style="list-style-type: none"> <li>• SMTPサーバ名が空白です。: NAのSMTPサーバ名の管理設定が空白になっています。[システム管理設定]ページでメールサーバが設定されているかどうか確認する必要があります。</li> <li>• &lt;ホスト名&gt;25へのTelnet接続を開けません。: NAから&lt;ホスト名&gt;に接続できないか、またはホストでSMTPポート(25)の接続が許可されていません。[システム管理設定]ページでメールサーバが正しく設定されているかどうか確認する必要があります。NAサーバがこのサーバのポート25にアクセスできるかどうかを確認する必要があります。</li> <li>• タイムアウトの待機予想: 220が返されました。: アプリケーションは構成済みメールサーバのポート23で実行されていますが、正しいSMTPコードで応答していないため、SMTPアプリケーションではないようです。[システム管理設定]ページでメールサーバが正しく設定されているかどうか確認する必要があります。</li> </ul>
SSHMonitor	<p>SSHサーバへの接続に不明な問題があります。: NAのSSHサーバが正しく動作していません。他のアプリケーションがNAで使用するSSHポートをリスニングしていないかどうかを確認する必要があります。NA管理エンジンを再起動します。</p>

監視	説明/対応策
SyslogMonitor	<p>テスト syslog メッセージは処理されませんでした。：NA に組み込まれた Syslog サーバが実行されていないか、または何らかの問題があります。サポートに問い合わせてください。</p>
TelnetMonitor	<ul style="list-style-type: none"> <li>• &lt;ホスト名&gt; 23 への Telnet 接続を開けません。：NA の Telnet サーバが正しく動作していません。NA 管理エンジンを再起動します。それでも問題が解決されない場合は、サポートにお問い合わせください。</li> <li>• タイムアウトの待機予想：HP Login が返されました。：アプリケーションは構成済みの Telnet ポートで実行されていますが、NA Telnet サーバではないようです。NA Telnet サーバがリスンするポートを変更する必要があります。</li> </ul>
FTPMonitor	<ul style="list-style-type: none"> <li>• FTP サーバへの接続がタイムアウト。：FTP サーバが実行されていないか、接続が許可されていません。FTP サーバを再起動してください。</li> <li>• FTP ファイルは書き込まれましたが、正常に読み取られませんでした。FTP パス設定を確認してください。：FTP ファイルが FTP サーバへ正しく書き込まれましたが、その後ファイルシステムから読み取ることができません。NA 管理エンジンの FTP パスが正しいかどうか、設定を確認してください。</li> <li>• チェックポイントファイルは見つかりましたが、タイムスタンプが古くなっています。：最近のファイル書き込みの試行に失敗していて、システムで古いチェックポイントの試行が見つかりました。これは、FTP サーバが過去のある時点で動作していましたが、現在は動作していないことを示します。FTP サーバを再起動してください。</li> </ul>
TFTPMonitor	<ul style="list-style-type: none"> <li>• TFTP サーバへの接続がタイムアウト。：TFTP サーバが実行されていないか、接続が許可されていません。TFTP サーバを再起動してください。</li> <li>• TFTP ファイルは書き込まれましたが、正常に読み取られませんでした。TFTP パス設定を確認してください。：TFTP ファイルが TFTP サーバへ正しく書き込まれましたが、その後ファイルシステムから読み取ることができません。NA 管理エンジンの TFTP パスが正しいかどうか、設定を確認してください。</li> <li>• チェックポイントファイルは見つかりましたが、タイムスタンプが古くなっています。：最近のファイル書き込みの試行に失敗していて、システムで古いチェックポイントの試行が見つかりました。これは、TFTP サーバが過去のある時点で動作していましたが、現在は動作していないことを示します。TFTP サーバを再起動してください。</li> </ul>

## サービスの開始および停止

NA内には以下の4つの主な機能単位があります。

- NA 管理エンジン
- HP Live Network
- TFTP、FTP、およびSyslogサーバ
- ソフトウェアイメージ管理サーバ

通常、顧客サポートとの作業中にできるのは、サービスの停止、開始、または再起動のみです。

サービスを開始/停止する、またはドライバをリロードするには、[管理]メニューバーから[サービスの開始/停止]をクリックします。[サービスの開始/停止]ページが開きます。

**注意：** Webユーザインターフェイスを使用してNAサービスを開始/停止する場合、前のページに移動することができなくなる場合があります。[戻る]ボタンをクリックすると、「null」というテキストが書かれたページが表示されます。代わりにブラウザの[戻る]ボタンをクリックします。

## [サービスの開始/停止]ページのフィールド

フィールド	説明/アクション
管理エンジン	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 停止：管理エンジン（NAサーバのことです）を停止します。これは、NAのメインサービスです。</li> <li>• 再開：管理エンジンを再起動します。</li> </ul>
HP Live Network	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• ドライバをリロード：新規デバイスの追加時にNAドライバを使用できるよう、NAドライバをリロードできます。[リロード]ボタンを押してもドライバは検出されません。</li> <li>• 内容をリロード：コンテンツは、HPで利用できるNAの一連の強化および拡張機能で、製品のアップグレードは不要です。ただし、一部のコンテンツサービスへの加入は必要です。たとえばNAでは、[HPセキュリティサービス]経由によるソフトウェアレベルポリシーのコンテンツのインポートがサポートされています。[HPセキュリティサービス]の一環として、ソフトウェアレベルポリシーをHPからダウンロードし、ネットワークの完全性を管理できます。詳細については、「<a href="#">[ソフトウェアレベル]ページのフィールド</a>」(435ページ)を参照してください。</li> </ul>
TFTPサーバ	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 開始：TFTPサーバを開始します。NAでは、主に設定の取得と配布に使用します。（<b>注意：</b> TFTPでは、最適なパフォーマンスを実現します。TFTPを利用できない場合、NAではTelnetまたはSSHを使用して構成を処理します。）</li> <li>• 停止：TFTPサーバを停止します。</li> <li>• 再開：TFTPサーバを再起動します。</li> </ul>

フィールド	説明/アクション
FTPサーバ	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"><li>• 開始：FTPサーバを開始します。NAでは、主に設定の取得と配布に使用します。（<b>注意</b>：FTPを利用できない場合、NAではTFTP、TelnetまたはSSHを使用して構成を処理します。）</li><li>• 停止：FTPサーバを停止します。</li><li>• 再開：FTPサーバを再起動します。</li></ul>
Syslogサーバ	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"><li>• 開始：Syslogサーバを開始します。NAを唯一のSyslogサーバとするか、または他のSyslogサーバからメッセージをNAに転送することが可能です。NAでは、Syslogメッセージを使用して、リアルタイム変更イベントを検出し、ユーザと関連付けます。</li><li>• 停止：Syslogサーバを停止します。</li><li>• 再開：Syslogサーバを再起動します。</li></ul>
ソフトウェアイメージ管理サーバ	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"><li>• 開始：ソフトウェアイメージ管理サーバを開始します。ソフトウェアイメージ管理サーバは、Cisco.comから入手可能な優先推奨に沿ったソフトウェアイメージを提供します。[デバイスソフトウェアイメージ推奨]ページの詳細については、<a href="#">「[デバイスソフトウェアイメージ推奨]ページのフィールド」</a>（223ページ）を参照してください。</li><li>• 停止：ソフトウェアイメージ管理サーバを停止します。</li><li>• 再開：ソフトウェアイメージ管理サーバを再起動します。</li></ul>

## ログ記録

ログ記録とは、NAが機能を実行する際、行った事象に関する情報を取得するための手段です。システムエラーでは、ログ記録は問題点を明確にするための主要な手段であり、問題のトラブルシューティングの手段です。

## ログのレベル

ログは、システム内で発生するイベントを記録する一連のメッセージ形式で作成されます。デフォルトで、これらのメッセージにはエラー、予期しない状況、または潜在的にエラーを含むデータの場合などの、重大なイベントのみが記録されます。これは、「エラー」ログレベルと呼ばれます。ログレベルとは、システムの状況について記録される情報の量を示す方法です。レベルがより低くなると、記録されるメッセージが増大します。

NA ログレベルには次のレベルがあります。

- 致命的：致命的なエラーが発生した場合のみメッセージが記録されます。これは、最高位のログレベルです。
- エラー：主にエラーの状況を示すメッセージが記録されます。これが、デフォルトのログレベルです。
- デバッグ：特定のエラーが発生する理由を特定するためのメッセージが記録されます。これは、中位のログレベルです。
- トレース：システムの一般機能に関するメッセージが記録されます。これは、最低位のログレベルです。

**注意：** ログの量を増やす設定にすると、システムパフォーマンスを著しく低下させます。カスタマサポートによる指示がある場合のみログレベルを調整してください。



## ログ名

ログには、ログが関連するシステムの部分を示す名前が与えられます。ログ名は階層的であり、1つのログに多数のサブログを含められます。NAには、以下のトップレベルのログが備わっています。

- API : 標準Webインターフェイス以外の手段による、NAとの対話に関連するログ。
- キャッシュプロバイダ : データベースキャッシュパフォーマンスの改善の追跡に関連するログ。
- DDK : DDKに関連するログ
- デバイス : 主にデバイスとの対話に関連するログ。
- 外部 : TFTP、FTP、Syslogサーバ、およびサードパーティアプリケーションへのコネクタなどの外部ユーティリティに関連するログ。
- 機能 : 特定NA機能に関連するログ。
- Flex UI : Flex ユーザインターフェイスコンポーネント（デバイスセレクタなど）固有の問題の追跡に関連するログ。
- システム : NA システムおよびサーバの内部機能に関連するログ。
- Web UI : NAのWebインターフェイス経由でのNAとの対話に関連するログ。

これらの広範なカテゴリのそれぞれの配下に、多数のサブログが存在します。たとえば、デバイスログの配下には、アクセス、セッション、およびデータの各サブログが存在します。これらのサブログには、それぞれデバイスへのアクセス、デバイスとの対話、および受信したデータに特化した、より専門的なログが含まれます。これらのサブログはそれぞれ、必要に応じてより特化した独自のサブログを持ちます。

サブログは、そのサブログを含むログの名前を前に付け、スラッシュで区切ることで命名します。以下に例を挙げます。

- デバイス
- Device/Access
- Device/Access/AuthenticationRules
- Device/Session
- Device/Session/SSH
- Device/Session/SNMP

あらゆるログのレベルは、そのログ、またはそのログを含む任意のログに設定されている最低位のレベルと等しくなります。結果、Device/Session/SNMP ログが「エラー」レベルに設定されていても、Device/Session ログが「デバッグ」レベルに設定されていれば、Device/Session/SNMP ログも「デバッグ」レベルに設定されているとして扱われます。

低レベルで数の多いログを有効にすると、システムのパフォーマンスが低下する場合があります。広範コンテナログを低レベルに設定する際には、注意が必要です。含まれるログのすべてが同じレベルに自動的に設定されてしまいます。

**注意：** ログ名は関連するシステムの部分を示すヒントにはなりませんが、ログ設定を操作する前には必ずカスタマサポートまでお問い合わせください。

## セッションログ

セッションログとは、タスクの処理中にNAがデバイスとどのように対話しているかを示すタイプの異なるログです。セッションログは、デバイスと実際に対話するタスクにのみ利用できます。このログの出力は、タスクの結果に自動的に挿入されます。

セッションログは、各デバイス固有のタスク作成ページにあるチェックボックスで有効にします。通常、タスクを最初に実行したときに有効でない場合でも、タスクを再実行するとセッションログが自動的に有効になります。詳細については、「[第7章：タスクの予定](#)」(275 ページ) を参照してください。

セッションログは、接続エラー、認証エラー、スクリプトのエラーなど、一般的なデバイスとの対話で発生する問題を識別することを目的としています。セッションログは、ある結果を得るためのNAの作業内容を示し、その作業が正しいことを確認する目的にも使用できます。

セッションログは、以下の項目に関する情報を表示します。

- タスクプロセスステップ（これはNA固有の情報です。ログを整理するのに使用します）。
- さまざまなプロトコルを経由した接続の試行
- 接続解除と接続のエラー
- デバイスに送信したコマンド
- デバイスから受信した結果
- デバイスから期待される結果（存在する場合）

**注意：** エラーの多くは、特定の結果が予想できるコマンドを送信した場合に発生します。デバイスの応答が異なる結果であった場合、タスクは失敗したことになります。

セッションログを確認する際、NAは可能な限りタスクを完了しようとすることに留意してください。このため、タスクが正常に完了した場合でも、セッションログにエラーが表示される場合があります。たとえば、TFTPアップロード試行が失敗した、とセッションログに記載されていても、構成スナップショットは成功している場合があります。エラーではデバイスへのTFTP接続に問題があったと記載されますが、この失敗によりNAは他の手段で構成を取得しようとするからです。このように他の手段により成功すれば、TFTPエラーがある場合でもタスクは成功します。

## タスクログ

タスクログは、1つの固有タスクに関連するシステムアクティビティを追跡するために作成される汎用ログです。タスクログは、1回のみ実行されるタスクに限定（反復が予定されているタスクは対象外）して記録されます。さらに、タスクがデバイス関連である場合、タスクログは単一デバイスに対して実行される場合にのみ有効です。NAのタスクのなかには、タスクログをサポートしないものもあります。たとえば、タスクの新規イベント通知とレスポンスルールを作成しても、タスクログは利用できません。

**注意：** NAユーザ全員がタスク固有のログを作成できますが、これらのログを表示およびダウンロードできるのは管理者権限を持つユーザのみです。ログを表示およびダウンロードするための適切な権限がない場合は、NAシステム管理者に問い合わせ、必要に応じてログ情報をサポートに提供することを依頼してください。

タスクログが利用できる場合、タスク作成ページに[タスクログ]セクションが表示されます。作成しているタスクにタスクログが適用されない場合（デバイスのグループに対して実行されるタスクや、反復が予定されているタスクなど）、タスクログインターフェイスは反応しません。

タスクログを有効にするには、1つのチェックボックスをオンにして、1つまたは複数のログ名を選択します。すべての利用可能なログの名前のリストが表示されます。このリストは、作成しているタスクに合うログのデフォルトセットのエントリを含みます。必要なログだけを作成したり、エントリのデフォルトセットを除くこともできます。リストから選択したログ名は、タスクログのTRACEレベルに自動的に設定されます。

タスクを実行すると、そのタスクに固有のログがファイルとして生成され、NAサーバログと一緒に格納されます。何らかの理由でタスクログファイルが作成できない場合は、ただちにエラーメッセージが表示され、タスクは異常終了します。タスク結果ページにタスクログに関する情報は表示されません。

## サーバログ

サーバログは、NAシステム全体のログです。サーバログには、あるロケーションにおけるすべてのタスクとその他すべてのプロセスのアクティビティを記録するメッセージを含みます。サーバログは[トラブルシューティング]ページで有効にします。詳細については、「[\[トラブルシューティング\]ページのフィールド](#)」（100ページ）を参照してください。

**注意：**サーバログは、カスタマサポートの指示がある場合のみ使用してください。

## ログ管理

NAは、さまざまな種類のログの有効、無効を切り替えることに加え、ログファイルの保持期間を管理し、一定期間の経過後にログレベルをリセットするための性能管理技術を備えています。ログファイルの保持期間の管理については、「[\[サーバ\]ページのフィールド](#)」（52ページ）を参照してください。NAが自動的にログレベルをリセットし、ユーザがその設定を変更するための性能管理技術については、「[サーバ監視](#)」（83ページ）を参照してください。

## [トラブルシューティング]ページのフィールド

[トラブルシューティング]ページを表示するには、[管理]のメニューバーで[トラブルシューティング]をクリックします。[トラブルシューティング]ページが開きます。

フィールド	説明/アクション
トラブルシューティング情報の送信	[トラブルシューティング情報の送信]ページが開きます。ここでは、電子メールの構成、システム情報の送信、顧客サポートのログなどが可能です。詳細については、「 <a href="#">[トラブルシューティングの送信]ページのフィールド</a> 」(29ページ)を参照してください。
トラブルシューティング情報のダウンロード	トラブルシューティング情報をダウンロードできます。詳細については、「 <a href="#">[トラブルシューティングの送信]ページのフィールド</a> 」(29ページ)を参照してください。
テスト電子メールを管理ユーザに送信	電子メールをシステム管理者に送信します。NA 電子メールシステムが適切に構成されていることを確認し、電子メールが正しく機能しない場合（電子メールのトラブルシューティングを行う場合）に使用します。
ログを有効にする対象	ログ記録を有効にするコンポーネント（単独または複数）を選択します。ログの詳細については、「 <a href="#">ログ記録</a> 」(96ページ)を参照してください。
追加	リストにない追加のソフトウェアコンポーネントを入力します。
レベル<>以上	<p>ログ記録のレベルを選択します。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• 致命的（メッセージ数が最少）</li> <li>• エラー（デフォルト）</li> <li>• デバッグ</li> <li>• トレース（メッセージ数が最多）</li> </ul> <p>詳細については、「<a href="#">ログのレベル</a>」(96ページ)を参照してください。</p>
ログの保持期間	ログデータを保存する日数を入力します。デフォルトでは2日です。（ <b>注意</b> ：ログデータの保存には大量のディスク容量が必要となります。）
リセット	オンにすると、[送信]ボタンをクリックしたときに、すべてのログがデフォルトのログレベル（エラー）にリセットされます。

## ドライバのレビュー

[ドライバ]ページには、システムにインストールされているドライバのリストと、現在使用されているドライバの個数が表示されます。[ドライバ]ページでは、どのNAドライバがHP社製であり、HP社公認であって、HPがサポートするかを判断できます。

[ドライバ]ページを表示するには、[管理]のメニューバーで[ドライバ]をクリックします。[ドライバ]ページが開きます。

## [ドライバ]ページのフィールド

フィールド	説明/アクション
ドライバをリロード	NAのドライバを追加、削除、または更新した場合に、ドライバをリロードできます。
説明	ドライバ名を表示します。
内部名	ドライバを識別するのに使用する、一意のドライバ名を表示します。サポートが使用します。
パッケージ名	ドライバパッケージ名を表示します。
バージョン	ドライバのバージョンを表示します。
ビルド番号	現在のNAのビルド番号を表示します。
作者	ドライバを作成した人員の名前を表示します。指定されていない場合、ドライバはHP社製であることを表します。
認証済み	ドライバが認証済みであれば表示されます。認証済みドライバとは、HP社製、またはサードパーティが作成したHP社公認のNAドライバのことです。
使用中	ドライバが現在使用中であれば表示されます。



## 第3章：デバイスとデバイスグループの追加

### トピックの参照先リスト

トピック	参照先：
はじめに	<a href="#">「はじめに」</a> （104 ページ）
デバイスの追加	<a href="#">「デバイスの追加」</a> （106 ページ）
デバイスの編集	<a href="#">「[デバイスの編集] ページのフィールド」</a> （111 ページ）
ベアメタルプロビジョニング	<a href="#">「ベアメタルプロビジョニング」</a> （116 ページ）
新規デバイステンプレートの追加	<a href="#">「新しいデバイステンプレートの追加」</a> （122 ページ）
デバイスの追加ウィザードの使用	<a href="#">「デバイスの新規作成ウィザードの使用」</a> （125 ページ）
デバイスのインポート	<a href="#">「デバイスのインポート」</a> （126 ページ）
デバイスパスワードルールの作成	<a href="#">「デバイスパスワードルールの作成」</a> （132 ページ）
デバイスグループの追加	<a href="#">「デバイスグループの追加」</a> （136 ページ）
動的グループ	<a href="#">「動的デバイスグループ」</a> （140 ページ）
デバイスセクタ	<a href="#">「デバイスセクタ」</a> （142 ページ）
デバイスグループの表示	<a href="#">「デバイスグループの表示」</a> （144 ページ）
デバイスとユーザのセグメント化	<a href="#">「デバイスとユーザのセグメント化」</a> （148 ページ）
HP Gateway の設定	<a href="#">「HP Gateway の設定」</a> （152 ページ）
デバイスグループの編集	<a href="#">「デバイスグループの編集」</a> （160 ページ）
デバイスの一括編集	<a href="#">「デバイスの一括編集」</a> （161 ページ）
デバイスドライバの検出	<a href="#">「デバイスドライバの検出」</a> （163 ページ）
Telnet/SSH セッションのリスト表示	<a href="#">「Telnet/SSH セッションのリスト表示」</a> （166 ページ）
要塞ホストの使用	<a href="#">「要塞ホストの使用」</a> （169 ページ）

## はじめに

デバイスを追加すると、HP Network Automation Software (NA) は次の作業を実行します。

1. 適切なデバイスドライバを自動検出して割り当て、デバイスとの通信を可能にする。このプロセスを「ドライバ検出」といいます。
2. デバイスのスナップショットを取得し、システム情報と初期設定を収集する。
3. 「NA インターフェイス」および「NA ルーティングテーブル」などのコア診断のセットを実行します（すべての診断の一覧については、「[表示メニューオプション](#)」(201 ページ) を参照してください)。

デバイスを検出してスナップショットを取得するには、NA がそのデバイスにフルアクセスでき、デバイスに対する SNMP 読み取りアクセスがあることが必須です。

IP ネットワークに現在到達できていないデバイスへのアクセスには、コンソールサーバが使用されます。また保護されたネットワーク内において、デバイスにハードウェアエラーがある場合、または IP プロトコル (IPX、ATM など) を実行していない場合などは、デバイスのコンソールポートを介したシリアル接続経由でのみ IP ネットワークへ到達できます。

SSH 認証を使用する Cisco AS5xxx などの標準的なコンソールサーバを使用する場合、適切なポート番号でコンソールサーバのループバックアドレスに telnet を行うことで、コンソールサーバから対象デバイスに接続できます。これには、以下の操作を実行する必要があります。

- SSH 接続方法を使用するように目的のデバイスを構成します。
- 要塞ホストアドレスを使用するように目的のデバイスを構成します。要塞ホストであるコンソールサーバにアドレスと資格情報を確実に付与します。
- デバイス固有の資格情報を使用するようにデバイスを設定します（この場合、各デバイスは異なる対象ポートを使用します）。
- 各影響を受けるデバイス上で、適切なアクセス変数を構成します。これらの変数の例を以下に挙げます。
  - `hop_prompt =>` (Cisco コンソールサーバプロンプト)
  - `hop_target_connect_protocol = telnet` (コンソールサーバから対象デバイスに接続するのに telnet を使用)
  - `hop_telnet_cmd_host = <ループバック IP>` (コンソールサーバのループバック IP アドレス)
  - `hop_telnet_cmd_port = <デバイスポート>` (コンソールサーバでのターゲットデバイスのポート番号)

**注意：** 対象デバイスをポートで指定する単純認証の Telnet コンソールサーバは、アクセス変数 `console_xxx` の使用をサポートできます。より複雑な Telnet コンソールサーバ構成では、カスタマイズした要塞ホストアクセスの使用が必要になります。

要塞ホストは、他のホストではアクセス不可能な保護されたネットワークの部分にアクセスできる、上位特権を持つホストです。これにより、管理システムでは、要塞ホストが権限を持つ保護されたネットワークで要素を管理する際に、要塞ホストを「ホップ」として使用できます。通常、要塞ホストは、インターネットおよび DMZ ルータ/スイッチ、エクストラネットのパートナー、保護されたネットワークまたはプライベートネットワークで使用されます。



いずれの場合も、NAでは、Telnet、SSH、FTP/TFTP、SNMPなどの他のアクセス方法が利用できない場合に、コンソールサーバと要塞ホストを（通常CLI経由の）デバイスアクセスの手段として使用し、通常の管理機能を実行します。

**注意：**すべてのアクセス方法が有効な場合、NAではSSH、Telnet、SNMP、コンソールの順にデバイスにアクセスします。また、SSH+SCP、SSH+TFTP、SSH+スクリーンスクレイプ、Telnet+SCP、Telnet+TFTP、Telnet+スクリーンスクレイプ、SNMP+TFTP、コンソール+スクリーンスクレイプなど、スクリーンスクレイプの前にファイル転送を行います。

## デバイスグループの命名規則

ポリシーと関連付けられている、システムで生成されたデバイスグループを参照すると、デバイスグループの命名規則が更新されています。たとえば、以前のリリースでは、DynamicCfgPolicyxxxx（ここで、xxxxはポリシー適用先デバイスグループを作成するために使用するデバイスグループの名前）という名前だったデバイスグループは、構成ポリシーグループ - CONFIGPOLICYNAME - TIMESTAMP（ここで、CONFIGPOLICYNAMEはデバイスグループ作成元の構成ポリシーの名前、TIMESTAMPはデバイスグループの作成時刻）になっています。

## デバイスの追加

新規デバイスを追加するには、[デバイス]メニューバーから[新規作成]を選択し[デバイス]をクリックします。[デバイスの新規作成]ページが開きます。終了したら[保存]ボタンをクリックするか、または[保存してさらに追加]ボタンをクリックします。

**注意：** [ネットワークデバイスの検出]タスクを使用すると、NAの管理下に置きたいデバイスの位置をネットワーク上で特定できます。IPアドレスの範囲をいったん指定すると、NAがネットワークをスキャンしてデバイスを検索します。詳細については、「[\[ネットワークデバイスの検出\]タスクページのフィールド](#)」(341 ページ) を参照してください。

## [デバイスの新規作成]ページのフィールド

フィールド	説明/アクション
ウィザードを使用	[デバイスを追加]ウィザードが開きます。(注意：[デバイスを追加]ウィザードは、デバイスがない場合に自動的に表示されます。) デバイスの新規作成ウィザードの使用の詳細については、「 <a href="#">デバイスの新規作成ウィザードの使用</a> 」(125 ページ) を参照してください。
IPアドレス (またはDNS名)	デバイスのIPアドレスまたはDNSホスト名を入力します。
ホスト名	該当する場合、デバイスのホスト名を入力します。
サイト<名>	<p>ドロップダウンメニューからパーティションを選択します。このフィールドは1つ以上のセキュリティパーティションを構成した場合にのみ表示されます。また、フィールド名は[パーティション]ページで変更できます。(詳細については、「<a href="#">[パーティション]ページのフィールド</a>」(156 ページ) を参照してください。)</p> <p>一般的に、セキュリティパーティションとは一意のIPアドレスを持つデバイスのグループです。単一のNAコアで複数のセキュリティパーティションを管理できます。NAコアはNAサーバのインストールコンポーネントの1つで、単一の管理エンジン、関連サービス、および単一のデータベースからなります。</p> <p><b>注意：</b> セキュリティパーティションがデバイス/デバイスグループに適用されている場合、各セキュリティパーティションに追加のドロップダウンメニューが存在する場合があります。(セキュリティパーティションの詳細については、「<a href="#">デバイスとユーザのセグメント化</a>」(148 ページ) を参照してください。)</p>
所属するグループ	デバイスがメンバーとして属するグループを表示します。デバイスセクタを使用してグループを選択します。デバイスセクタの使用の詳細については、「 <a href="#">デバイスセクタ</a> 」(142 ページ) を参照してください。
変更の検出とポーリング	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>有効：オンにすると(デフォルト)、通常のポーリングタスクの一環として、あるいは変更イベントが検出された場合に、デバイスの変更がポーリングされます。</li> <li>ポーリングのみ：オンにすると、通常のポーリングタスクの一環として、デバイスの変更がポーリングされます。</li> <li>無効：オンにすると、デバイス関連の変更イベントが無視されます。さらに、通常のポーリングタスクの一環としてデバイスの変更が確認されません。通常のポーリングタスクからこのデバイスを除外したい場合に、日常のメンテナンス時にこのオプションを選択するのが有効です。</li> </ul>

フィールド	説明/アクション
管理ステータス	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• アクティブ：オンにすると（デフォルト）、デバイスの変更が記録されます。</li> <li>• 実稼働前：オンにすると、デバイスは実稼働前デバイスとして指定されます。実稼働前デバイスとは、運用ネットワーク内でまだ動作していないデバイスのことです。実稼働前デバイスは、検索に含まれず（明示的に含むように選択した場合を除く）、ネットワークステータスのレポートに含まれない点に注意してください。（<b>注意</b>：ベアメタルデバイスは、実稼働前ステータスを使用する必要があります）。</li> <li>• 非アクティブ：オンにすると、デバイスの変更が記録されません。デバイスがサポートされていない、またはアクティブでない場合にこのオプションを選択するのが有効です。デバイスを非アクティブにすると、ネットワークトラフィックが減少してリソースが解放されます。</li> </ul>
デバイスドライバ	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• ドライバを自動検出：オンにすると（デフォルト）、SNMPまたはTelnetを使用してデバイスのクエリを実行し、最適なデバイスドライバを割り当てます。（<b>注意</b>：既存デバイスを編集する場合、オプションは[ドライバを再検出]に変化します。）</li> <li>• ドライバを指定：オンにすると、現在デバイスに割り当てられているドライバが表示されるか、または使用可能なドライバのドロップダウンメニューのリストからドライバを選択できます。</li> </ul>
コメント	<p>デバイスに関するコメントを入力します。</p>
<b>パスワード情報</b>	
ネットワーク全体のパスワードルールの使用	<p>オンにすると（デフォルト）、ネットワーク全体のデバイスパスワードルールがデバイスに適用されます。ネットワーク全体のパスワードルールの使用は、デバイス資格情報を設定するための拡張性の高い方法です。</p> <p><b>注意</b>：デバイスグループで同じ資格情報を共有する大規模ネットワークの場合、[デバイスパスワードルール]の設定が使用されます。これにより、デバイスの資格情報を1つの場所に整理統合できるため、管理が容易になります。デバイスパスワードルールの作成の詳細については、「<a href="#">デバイスパスワードルールの作成</a>」(132 ページ) を参照してください。</p>
このパスワードルールを最初に使用	<p>オンにすると、NAはユーザがドロップダウンメニューから選択したパスワードルールを最初に使用します。</p>

フィールド	説明/アクション
デバイス固有パスワード情報の使用	<p>オンにすると、デバイス固有の認証の資格情報が使用されます。次の情報を入力して、デバイス固有パスワードルールを実装します。</p> <ul style="list-style-type: none"> <li>• ユーザ名：必要に応じて、デバイスアクセスに使用するユーザ名を入力します。デバイスが TACACS+ や RADIUS などの AAA ソリューションを使用する場合、AAA ユーザアカウントを作成し、それらの AAA 資格情報をデバイスの資格情報として使用します。</li> <li>• パスワード：NA でデバイスアクセスに使用するパスワードを入力します。</li> <li>• パスワードの確認：パスワードを再度入力します。</li> <li>• イネーブルパスワード：NA から特権モードへのアクセスに使用するイネーブルパスワードを入力します。ほとんどの構成変更でイネーブルパスワードが必要です。<b>(注意：Nortel ASN/ARN など、一部のデバイスでは、パスワードがなくても特権モードにアクセスできる場合があります。一部のデバイスでは、特権モードのパスワードを無効に構成できます。サイト固有の構成については、ネットワーク管理者にお問い合わせください。)</b></li> <li>• イネーブルパスワードの確認：イネーブルパスワードを再度入力します。</li> <li>• SNMP 読み取り専用コミュニティ文字列：NA で SNMP 値の読み取りに使用する SNMP パスワードを入力します。</li> <li>• SNMP 読み取り/書き込みコミュニティ文字列：NA で SNMP 値の読み取り/書き込みに使用する SNMP パスワードを入力します。</li> <li>• SNMPv3 ユーザ名：デバイスにアクセスするのに使用する SNMPv3 ユーザ名を入力します。</li> <li>• SNMPv3 認証パスワード：NA がデバイスにアクセスするのに使用する SNMPv3 パスワードを入力します。</li> <li>• SNMPv3 認証パスワードの確認：SNMPv3 認証パスワードを再度入力します。</li> <li>• SNMPv3 暗号化パスワード：SNMPv3 暗号化パスワードを入力します。</li> <li>• SNMPv3 暗号化パスワードの確認：SNMPv3 暗号化パスワードを再度入力します。</li> </ul>
<b>デバイスアクセス設定</b>  デバイスアクセス設定	<p>NA は、ほとんどのネットワークおよびネットワークデバイスで動作するよう設計されています。ただし、独自のデバイス構成の場合、NA で特定のデバイスを管理する能力に影響する場合があります。デバイスアクセス設定により、NA をお使いのネットワーク構成に合わせてカスタマイズできます。デバイスアクセス設定は、デバイスのパスワード情報に関連付けられています。ここで入力するデバイス固有の設定は、デバイス固有パスワードを使用する場合のみ適用されます。ネットワーク全体のデバイス設定をパスワードルールに追加することもできます。TACACS+ 認証の詳細については、「<a href="#">TACACS+ 認証</a>」(75 ページ)を参照してください。SecurID の使用方法の詳細については、「<a href="#">SecurID を使用したログイン</a>」(631 ページ)を参照してください。</p> <p><b>注意：</b>デバイスアクセス設定の使用の詳細については、[デバイスアクセス設定の使用] リンクをクリックしてください。新しいブラウザのウィンドウにアクセス変数のヘルプファイルが開きます。</p>
<b>NAT 情報</b>  NAT IP アドレス	<p>デバイスの内部構成済み IP アドレスが NA でデバイスアクセスに使用するプライマリ IP アドレスと異なる場合、デバイスの内部構成済み IP アドレスを入力します。<b>(注意：NAT を使用する場合、ページ最上部の [デバイス IP] ボックスに、NA でデバイスアクセスに使用する IP アドレスを必ず入力してください。)</b></p>

フィールド	説明/アクション
TFTPサーバのIPアドレス	デバイスに固有のNAサーバのNAT IPアドレスを入力します。
FTPサーバのIPアドレス	デバイスに固有のNAサーバのNAT IPアドレスを入力します。
<b>接続情報</b>	
接続方法	<p>NAでは、次のプロトコルを組み合わせお使いのネットワークデバイスと通信できます。使用するプロトコルを1つ以上選択します。NAでは、プロトコルを選択した時点から任意の時点で最も効率的なプロトコルが選択されます。</p> <ul style="list-style-type: none"> <li>• SNMP</li> <li>• SNMPv1またはSNMPv2c（コミュニティ文字列認証）</li> <li>• SNMPv3（ユーザ認証）：SNMPv3では、以下のオプションがあります。noAuthNoPriv（ユーザ名のみ）、authNoPriv（ユーザ名、認証パスワード）、およびauthPriv（ユーザ名、認証用と暗号化パスワード）。認証方法には、SHA（Secure Hash Algorithm）とMD5（Message Digest Algorithm）があります。暗号化方法には、DES（Data Encryption Standard）、3DES（Triple DES）、AES（Advanced Encryption Standard）、AES128、AES192、およびAES256があります。</li> <li>• RLogin</li> <li>• Telnet</li> <li>• SSH（SSH1またはSSH2（デフォルト）、SSH1のみ、SSH2のみのいずれかを選択できます。）</li> <li>• [コンソールサーバ（Telnet経由）]チェックボックス：標準ネットワーク接続以外にも、NAではコンソールサーバ経由でデバイスに接続できます。また、標準接続にエラーが発生した場合、Telnet/SSHプロキシがユーザからデバイスへの接続時に、コンソール設定に自動的にフェイルオーバーするようになっています。オンにすると、コンソールサーバのIPアドレスまたはホスト名と、ポート番号が入力されます。</li> <li>• [コンソールサーバのみを使用する]チェックボックス：デフォルトで、少なくとも1つの接続方法を選択する必要があります。デフォルトでTelnetが使用されます。オンにすると、このオプションでは上記の接続方法のいずれも確認できません。</li> </ul>
転送プロトコル	<p>次のいずれかの転送プロトコルを選択します（複数可）。</p> <ul style="list-style-type: none"> <li>• SCP</li> <li>• SFTP</li> <li>• FTP</li> <li>• TFTP</li> </ul>
要塞ホスト	<p>[TelnetおよびSSHアクセスにUnixまたはLinux要塞ホストを使用]チェックボックスをオンにして、次の情報を入力します。</p> <ul style="list-style-type: none"> <li>• 要塞ホストのIPアドレスまたはホスト名</li> <li>• 要塞ホストへのアクセスに使用するユーザ名（通常はroot）</li> <li>• 要塞ホストへのアクセスに使用するパスワード</li> <li>• パスワード確認のための再入力</li> </ul> <p><b>(注意：)</b> 要塞ホスト情報を変更するには、<b>[「デバイス管理対象IPアドレス」ページのフィールド]（232ページ）</b>を参照してください。</p>

## フィールド

## 説明/アクション

## Syslogの設定

構成変更の検出のための  
デバイスのSyslogの構成

オンにして（デフォルト）、ドライバ検出または各デバイスへのドライバの割り当てにより、各デバイスで次の手順が実行されます。

1. 構成のスナップショットを取得します。
2. NAにSyslogメッセージを送信するように構成を更新します。
3. デバイスが変更検出を有効にするように自動構成されていることを示すコメントを、構成に書き込みます。
4. 最終的なスナップショットを取得します。

次のオプションからいずれか1つを選択できます。

- syslogサーバでログを取得するようにデバイスを設定する：[構成変更の検出のためのデバイスのSyslogの構成]チェックボックスがオンの場合、デフォルトでこのチェックボックスがオンになっています。
- デバイスはsyslogリレーにログ出力し、正しいログレベルに設定する：リレーホストのIPアドレスまたはホスト名を入力します。リレーホストが入力済みの場合、そのリレーホストがデフォルトで表示されます。

## ACL解析

次のオプションのいずれかを選択します。

- 有効：オンにすると（デフォルト）、デバイスのACLデータがスナップショットごとに保存されます。スナップショットが取得されるまでACLはロードされません。
- 無効：オンにすると、スナップショットごとにデバイスのACLデータが保存されません。

## 追加情報

NAでは、デバイスのスナップショット取得プロセスで、次のフィールドの一部が自動的に入力されます。手動でこれらのフィールドを入力する場合、デバイスをポーリングするたびにデータが上書きされます。

デバイスの説明	デバイスの識別に使用する説明を入力します。
モデル	デバイスのメーカーのモデル番号を入力します。
FQDN	デバイスが属するドメインを入力します。このドメインは、[FQDN 管理の解決]オプションがオンの場合に検出されます。
シリアル番号	デバイスのメーカーのシリアル番号を入力します。
ベンダー	CiscoやNortelなど、デバイスのベンダーを入力します。
資産タグ	デバイスの企業資産タグ番号を表示します。
場所	ネットワーク内のデバイスの物理的または論理的な場所を入力します。

フィールド	説明/アクション
階層レイヤ	<p>階層レイヤはデバイス属性です。デバイスの階層レイヤは、デバイスを追加または編集するときに設定できます。その結果、ネットワークダイアグラムの構成時にフィルタする階層レイヤを選択できます。たとえば、ネットワーク全体（インベントリ）をダイアグラムで表示し、「コア」でフィルタリングを行ってコアデバイス（階層レイヤが「コア」に設定されたデバイス）のみを取得することもできます。ネットワークダイアグラムの詳細については、「<a href="#">ダイアグラム</a>」（603ページ）を参照してください。</p> <p><b>注意：</b>以下のオプションは、デフォルトの階層レイヤです。カスタム階層レイヤの追加の詳細については、「<a href="#">appserver.rcx ファイルの編集</a>」（611ページ）を参照してください。</p> <p>ドロップダウンメニューから階層レイヤを選択します。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• 未設定レイヤ</li> <li>• コア</li> <li>• 分散</li> <li>• アクセス</li> <li>• エッジ</li> </ul>
カスタムサービスタイプ	<p>サービスタイプを入力します。サービスタイプは、VoIP、BGP、MPLSなどを指定できます。この値により、デバイスの用途を判断できます。これらの値を使用してデバイスサービスにタグ付けすることで、デバイスサービスを容易に検索したり、グループ内のデバイスグループを表示できます（静的または動的）。</p>

## [デバイスの編集]ページのフィールド

フィールド	説明/アクション
IPアドレス (またはDNS名)	<p>デバイスのIPアドレスまたはDNSホスト名を表示します。</p>
ホスト名	<p>該当する場合、デバイスのホスト名を表示します。</p>
サイト<名>	<p>サイト名を表示します。フィールド名は[パーティション]ページで変更できます。（詳細については、「<a href="#">[パーティション]ページのフィールド</a>」（156ページ）を参照してください。）一般的に、セキュリティパーティションとは一意のIPアドレスを持つデバイスのグループです。単一のNAコアで複数のセキュリティパーティションを管理できます。NAコアはNAサーバのインストールコンポーネントの1つで、単一の管理エンジン、関連サービス、および単一のデータベースからなります。</p> <p><b>注意：</b>セキュリティパーティションがデバイス/デバイスグループに適用されている場合、各セキュリティパーティションに追加のドロップダウンメニューが存在する場合があります。（セキュリティパーティションの詳細については、「<a href="#">デバイスとユーザのセグメント化</a>」（148ページ）を参照してください。）</p>
所属するグループ	<p>デバイスがメンバーとして属するグループを表示します。デバイスセレクトアを使用してグループを選択します。デバイスセレクトアの使用方法的詳細については、「<a href="#">デバイスセレクトア</a>」（142ページ）を参照してください。</p>

フィールド	説明/アクション
変更の検出とポーリング	<p>次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• 有効：オンにすると（デフォルト）、通常のポーリングタスクの一環として、あるいは変更イベントが検出された場合に、デバイスの変更がポーリングされます。</li> <li>• ポーリングのみ：オンにすると、通常のポーリングタスクの一環として、デバイスの変更がポーリングされます。</li> <li>• 無効：オンにすると、デバイス関連の変更イベントが無視されます。さらに、通常のポーリングタスクの一環としてデバイスの変更が確認されません。通常のポーリングタスクからこのデバイスを除外したい場合に、日常のメンテナンス時にこのオプションを選択するのが有効です。</li> </ul>
管理ステータス	<p>次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• アクティブ：オンにすると（デフォルト）、デバイスの変更が記録されます。</li> <li>• 実稼働前：オンにすると、デバイスは実稼働前デバイスとして指定されます。実稼働前デバイスとは、運用ネットワーク内でまだ動作していないデバイスのことです。実稼働前デバイスは、検索に含まれず（明示的に含むように選択した場合を除く）、ネットワークステータスのレポートに含まれない点に注意してください。<b>注意</b>：ベアメタルデバイスは、実稼働前ステータスを使用する必要があります。</li> <li>• 非アクティブ：オンにすると、デバイスの変更が記録されません。デバイスがサポートされていない、またはアクティブでない場合にこのオプションを選択するのが有効です。デバイスを非アクティブにすると、ネットワークトラフィックが減少してリソースが解放されます。</li> </ul>
デバイスドライバ	<p>次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• ドライバを再検出：オンにすると（デフォルト）、SNMPまたはTelnetを使用してデバイスのクエリを実行し、最適なデバイスドライバを割り当てます。</li> <li>• ドライバを指定：オンにすると、現在デバイスに割り当てられているドライバが表示されるか、または使用可能なドライバのドロップダウンメニューのリストからドライバを選択できます。</li> </ul>
コメント	<p>デバイスについてのコメントを表示します。</p>
<b>パスワード情報</b>	
ネットワーク全体のパスワードルールの使用	<p>オンにすると（デフォルト）、ネットワーク全体のデバイスパスワードルールがデバイスに適用されます。ネットワーク全体のパスワードルールの使用は、デバイス資格情報を設定するための拡張性の高い方法です。</p> <p><b>注意</b>：デバイスグループで同じ資格情報を共有する大規模ネットワークの場合、[デバイスパスワードルール]の設定が使用されます。これにより、デバイスの資格情報を1つの場所に整理統合できるため、管理が容易になります。デバイスパスワードルールの作成の詳細については、「<a href="#">デバイスパスワードルールの作成</a>」(132 ページ) を参照してください。</p>
このパスワードルールを最初に使用	<p>オンにすると、NAはユーザがドロップダウンメニューから選択したパスワードルールを最初に使用します。</p>



フィールド	説明/アクション
デバイス固有パスワード情報の使用	<p>オンにすると、デバイス固有の認証の資格情報が使用されます。次の情報を入力して、デバイス固有パスワードルールを実装します。</p> <ul style="list-style-type: none"> <li>• ユーザ名：必要に応じて、デバイスアクセスに使用するユーザ名を入力します。デバイスが TACACS+ や RADIUS などの AAA ソリューションを使用する場合、AAA ユーザアカウントを作成し、それらの AAA 資格情報をデバイスの資格情報として使用します。</li> <li>• パスワード：NA でデバイスアクセスに使用するパスワードを入力します。</li> <li>• パスワードの確認：パスワードを再度入力します。</li> <li>• イネーブルパスワード：NA から特権モードへのアクセスに使用するイネーブルパスワードを入力します。ほとんどの構成変更でイネーブルパスワードが必要です。<b>(注意：Nortel ASN/ARN など、一部のデバイスでは、パスワードがなくても特権モードにアクセスできる場合があります。一部のデバイスでは、特権モードのパスワードを無効に構成できます。サイト固有の構成については、ネットワーク管理者にお問い合わせください。)</b></li> <li>• イネーブルパスワードの確認：イネーブルパスワードを再度入力します。</li> <li>• SNMP 読み取り専用コミュニティ文字列：NA で SNMP 値の読み取りに使用する SNMP パスワードを入力します。</li> <li>• SNMP 読み取り/書き込みコミュニティ文字列：NA で SNMP 値の読み取り/書き込みに使用する SNMP パスワードを入力します。</li> <li>• SNMPv3 ユーザ名：デバイスにアクセスするのに使用する SNMPv3 ユーザ名を入力します。</li> <li>• SNMPv3 認証パスワード：NA がデバイスにアクセスするのに使用する SNMPv3 パスワードを入力します。</li> <li>• SNMPv3 認証パスワードの確認：SNMPv3 認証パスワードを再度入力します。</li> <li>• SNMPv3 暗号化パスワード：SNMPv3 暗号化パスワードを入力します。</li> <li>• SNMPv3 暗号化パスワードの確認：SNMPv3 暗号化パスワードを再度入力します。</li> </ul>
最後に使用したパスワードルールのリセット	<p>オンにすると、最後に使用されたパスワードがリセットされます。</p>
<b>デバイスアクセス設定</b>	
デバイスアクセス設定	<p>NA は、ほとんどのネットワークおよびネットワークデバイスで動作するよう設計されています。ただし、独自のデバイス構成の場合、NA で特定のデバイスを管理する能力に影響する場合があります。デバイスアクセス設定により、NA をお使いのネットワーク構成に合わせてカスタマイズできます。デバイスアクセス設定は、デバイスのパスワード情報に関連付けられています。ここで入力するデバイス固有の設定は、デバイス固有パスワードを使用する場合のみ適用されます。ネットワーク全体のデバイス設定をパスワードルールに追加することもできます。TACACS+ 認証の詳細については、<a href="#">「TACACS+ 認証」(75 ページ)</a> を参照してください。SecurID の使用方法の詳細については、<a href="#">「SecurID を使用したログイン」(631 ページ)</a> を参照してください。</p> <p><b>注意：</b>デバイスアクセス設定の使用の詳細については、[デバイスアクセス設定の使用] リンクをクリックしてください。新しいブラウザのウィンドウにアクセス変数のヘルプファイルが開きます。</p>

フィールド	説明/アクション
<b>NAT 情報</b>	
NAT IP アドレス	デバイスの内部構成済み IP アドレスが NA でデバイスアクセスに使用するプライマリ IP アドレスと異なる場合、デバイスの内部構成済み IP アドレスが表示されます。(注意: NAT を使用する場合、ページ最上部の[デバイス IP]ボックスに、NA でデバイスアクセスに使用する IP アドレスを必ず入力してください)。
TFTP サーバの IP アドレス	デバイスに固有の NA サーバの NAT IP アドレスを表示します。
<b>接続情報</b>	
接続方法	<p>NA では、次のプロトコルを組み合わせしてお使いのネットワークデバイスと通信できます。使用中のプロトコルが 1 つ以上表示されます。NA では、プロトコルを選択した時点から任意の時点で最も効率的なプロトコルが選択されます。</p> <ul style="list-style-type: none"> <li>• SNMP</li> <li>• SNMPv1 または SNMPv2c (コミュニティ文字列認証)</li> <li>• SNMPv3 (ユーザ認証): SNMPv3 では、以下のオプションがあります。noAuthNoPriv (ユーザ名のみ)、authNoPriv (ユーザ名、認証パスワード)、および authPriv (ユーザ名、認証用と暗号化パスワード)。認証方法には、SHA (Secure Hash Algorithm) と MD5 (Message Digest Algorithm) があります。暗号化方法には、DES (Data Encryption Standard)、3DES (Triple DES)、AES (Advanced Encryption Standard)、AES128、AES192、および AES256 があります。</li> <li>• RLogin</li> <li>• Telnet</li> <li>• SSH (SSH1 または SSH2 (デフォルト)、SSH1 のみ、SSH2 のみのいずれかを選択できます。)</li> <li>• [コンソールサーバ (Telnet 経由)] チェックボックス: 標準ネットワーク接続以外にも、NA ではコンソールサーバ経由でデバイスに接続できます。また、標準接続にエラーが発生した場合、Telnet/SSH プロキシがユーザからデバイスへの接続時に、コンソール設定に自動的にフェイルオーバーするようになっています。オンにすると、コンソールサーバの IP アドレスまたはホスト名と、ポート番号が入力されます。(既存デバイスの編集時にコンソールサーバ情報を変更するには、<a href="#">「[デバイス管理対象 IP アドレス] ページのフィールド」(232 ページ)</a> を参照してください。</li> </ul> <p><b>注意:</b> Cisco ASA 子デバイスへの接続は、親デバイスを介して行うことができます。ただし、Cisco ASA 子デバイスへの Telnet および SSH 接続方法が親デバイスの接続方法と一致しない場合、子デバイスの接続方法の設定が親デバイスの接続方法の設定より優先されることはないので、通信によっては失敗する場合があります。</p>
転送プロトコル	<p>転送プロトコルには、以下があります。</p> <ul style="list-style-type: none"> <li>• SCP</li> <li>• SFTP</li> <li>• FTP</li> <li>• TFTP</li> </ul>
要塞ホスト	要塞ホスト情報を変更するには、 <a href="#">「[デバイス管理対象 IP アドレス] ページのフィールド」(232 ページ)</a> を参照してください。

フィールド	説明/アクション
<b>ACL 解析</b>	
	<p>次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• 有効：オンにすると（デフォルト）、デバイスのACLデータがスナップショットごとに保存されます。スナップショットが取得されるまでACLはロードされません。</li> <li>• 無効：オンにすると、スナップショットごとにデバイスのACLデータが保存されません。</li> </ul>
<b>追加情報</b>	
NAでは、デバイスのスナップショット取得プロセスで、次のフィールドの一部が自動的に入力されます。手動でこれらのフィールドを入力する場合、デバイスをポーリングするたびにデータが上書きされます。	
デバイスの説明	デバイスの説明を表示します。
モデル	デバイスのメーカーのモデル番号を表示します。
FQDN	デバイスが属する完全修飾ドメイン名（FQDN）を入力します。このドメインは、[FQDN 管理の解決]オプションがオンの場合に検出されます。
シリアル番号	デバイスのメーカーのシリアル番号を表示します。
ベンダー	CiscoやNortelなど、デバイスのベンダーを表示します。
資産タグ	デバイスの企業資産タグ番号を表示します。
場所	ネットワーク内のデバイスの物理的または論理的な場所を表示します。
階層レイヤ	<p>階層レイヤはデバイス属性です。デバイスの階層レイヤは、デバイスを追加または編集するときに設定できますその結果、ネットワークダイアグラムの構成時にフィルタする階層レイヤを選択できます。たとえば、ネットワーク全体（インベントリ）をダイアグラムで表示し、「コア」でフィルタリングを行ってコアデバイス（階層レイヤが「コア」に設定されたデバイス）のみを取得することもできます。ネットワークダイアグラムの詳細については、<a href="#">「ダイアグラム」</a>（603ページ）を参照してください。</p> <p><b>注意：</b>以下のオプションは、デフォルトの階層レイヤです。カスタム階層レイヤの追加の詳細については、<a href="#">「appserver.rcx ファイルの編集」</a>（611ページ）を参照してください。</p> <p>ドロップダウンメニューから階層レイヤを選択します。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• 未設定レイヤ</li> <li>• コア</li> <li>• 分散</li> <li>• アクセス</li> <li>• エッジ</li> </ul>
カスタムサービスタイプ	サービスタイプは、VoIP、BGP、MPLSなどを指定できます。この値により、デバイスの用途を判断できます。これらの値を使用してデバイスサービスにタグ付けすることで、デバイスサービスを容易に検索したり、グループ内のデバイスグループを表示できます（静的または動的）。

## ベアメタルプロビジョニング

ベアメタルプロビジョニングとは、デバイスを設置し、そのデバイスが運用ネットワーク内で機能するステータスにまで移行するためのプロセスのことです。ベアメタルデバイスは、NAと適切に通信が行える状態にまでセットアップされていません。ベアメタルデバイスに関する最も一般的なシナリオは、初期化手続きが未済のシナリオです。たとえば、デバイスを標準的なNA通信に適切に応答できるポイントに構成する、対話型CLIセッションが未済の場合です。

**注意：** ベアメタルデバイスは、初めて起動するデバイスのことであり、通常は「ブートストラップ」OSの類を実行します。ベアメタルドライバ使用時には、NAはごく限られた方法でのみデバイスと通信できます。

一般的にベアメタルプロビジョニングプロセスには、以下の項目があります。

- **準備：** 準備の段階で、デバイスはシステムに組み込まれ、構成、ファームウェア、OSなどを受信できる状態にまでセットアップされます。これらのデバイスはネットワーク上の一時的な場所に配置できますが、ネットワーク内の所定の場所に一致するIP情報ではセットアップされません。準備段階の最終目標は、NAがプロビジョニングで設定するデータのタイプを受信できるように、既知の良好なステータスにデバイスを移行することです。これにより、デバイスは構成の配布、OSの配布、およびカスタムスクリプトを処理できるようになります。
- **プロトタイピング：** プロトタイピングとは、デバイステンプレートを定義して維持するためのプロセスです。デバイステンプレートは、NAのその他のデバイスに対する同様の方法で操作されますが、デバイステンプレートに関連付けられた実際のデバイスは存在しません。プロトタイピング段階の最終目標は、実際に操作するデバイスを必要としないで、デバイス構成、およびその他のプロビジョニング情報を定義できるようにすることです。2つ目の目標は、情報の定義、保守、および再使用するための手段を提供することです。

**注意：** デバイステンプレートにより、構成、OS/ファイルの仕様、および既存のデバイスに適用可能なその他のデバイス固有情報を定義できます。デバイステンプレートには、実際にテストするデバイスを必要としないで、ポリシー確認などのある種のデバイス操作をサポートする機能も備わっています。詳細については、「[新しいデバイステンプレートの追加](#)」(122ページ)を参照してください。

- **プロビジョニング：** プロビジョニングの段階で、抽象デバイステンプレートが実際のデバイス（通常、実稼動前デバイス）に適用されます。この適用は、デバイステンプレートの情報のプロビジョニング、およびその情報のデバイスへの適切な適用から構成されます。デバイステンプレート構成の場合、これは構成を展開する処理です。プロビジョニングでは、デバイステンプレートのプロビジョニング情報をそのデバイス向けにカスタマイズする、特定情報も提供することができます。この情報は、カスタムスクリプトの場合の可変値の入力にあたります。プロビジョニング段階の最終目標は、デバイス構成、およびその他のデバイステンプレートのプロビジョニング情報を実際のデバイスに適用できるようにすることです。

ここで、ベアメタルプロビジョニングの手順を簡単に説明します。

1. NAに実稼働前デバイスを追加します。「**デバイスの追加**」(106 ページ) を参照してください。実稼働前デバイスとは、運用ネットワーク内でまだ動作していないデバイスのことです。実稼働前デバイスは、検索に含まれず(明示的に含むように選択した場合を除く)、ネットワークステータスのレポートに含まれない点に注意してください。

**注意：** デバイステンプレートを構成する前に、NAに実稼働前デバイスを追加する必要はありません。ただし、実稼働前デバイスにデバイステンプレートを配布するには、デバイスがNAで管理されている必要があります。

2. デバイステンプレートを構成します。デバイステンプレートとは、OS/ファイルシステム、およびその他のデバイスにプロビジョニングできる構成情報を含む、抽象デバイス構成のことです。「**新しいデバイステンプレートの追加**」(122 ページ) を参照してください。
3. ベアメタルデバイスに接続します。ベアメタルデバイスは、実稼働前デバイスの一種です。機能は、Telnet やSSH プロキシ接続の作成、デバイスに対するスクリプトの実行、ドライバの検出、およびデバイス設定の編集までに限定されます。「**ベアメタルプロビジョニングスクリプト**」(571 ページ) を参照してください。
4. デバイステンプレートからデバイスをプロビジョニングします。「**[ デバイスのプロビジョニング ] タスク ページのフィールド**」(356 ページ) を参照してください。デバイステンプレートを検索できます。「**デバイステンプレートの検索**」(536 ページ) を参照してください。

## デバイステンプレート

デバイステンプレートにより、構成、および既存のデバイスに適用可能なその他デバイス固有情報を定義できます。デバイステンプレートには、実際にテストするデバイスを必要としないで、ポリシー確認などのある種のデバイス操作をサポートする機能も備わっています。ベアメタルプロビジョニングプロセスの詳細については、「[ベアメタルプロビジョニング](#)」(116ページ)を参照してください。

**注意:** デバイステンプレートは、デバイスに配布可能な完全構成ファイルであり、あらゆる既存データを完全に上書きします。

[デバイステンプレート]ページにアクセスするには、[デバイス]のメニューバーにある[デバイスツール]を選択し、[デバイステンプレート]をクリックします。[デバイステンプレート]ページが開きます。

## [デバイステンプレート]ページのフィールド

フィールド	説明/アクション
デバイステンプレートの新規作成	[デバイステンプレートの新規作成]ページが開きます。「 <a href="#">新しいデバイステンプレートの追加</a> 」(122ページ)を参照してください。
チェックボックス	左側のチェックボックスをオンにすると、デバイステンプレートを削除できます。デバイステンプレートを選択したら、[アクション]ドロップダウンメニューをクリックし、[削除]をクリックします。隣接の[選択]ドロップダウンメニューを使用すると、デバイステンプレートを全選択または全選択解除できます。
ホスト名	デバイステンプレートのホスト名を表示します。デバイスのホスト名をクリックすると[デバイステンプレートの詳細]ページが開きます。このページでは、テンプレートの詳細な情報を確認できます。詳細については、「 <a href="#">[デバイステンプレートの詳細]ページのフィールド</a> 」(119ページ)を参照してください。
デバイスのベンダー	CiscoやNortelなど、デバイスのベンダーを表示します。
デバイスモデル	デバイスのメーカーのモデル番号を表示します。
パーティション	セキュリティや業務上の理由でパーティションを作成した場合、特定パーティションの各デバイスについてデバイスパスワードルールをパーティションできます。パーティションの作成の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」(148ページ)を参照してください。
アクション	次のアクションを選択できます。 <ul style="list-style-type: none"> <li>編集: [デバイステンプレートの編集]ページが開きます。「<a href="#">[デバイステンプレート]ページのフィールド</a>」(118ページ)を参照してください。</li> <li>構成を表示: [構成を表示]ページが開きます。「<a href="#">[デバイス構成の詳細]ページのフィールド</a>」(175ページ)を参照してください。</li> <li>ポリシー準拠のテスト: [ポリシー準拠のテスト]ページが開きます。詳細については、「<a href="#">[ポリシー準拠のテスト]ページのフィールド</a>」(439ページ)を参照してください。</li> </ul>

## [デバイステンプレートの詳細]ページのフィールド

[デバイステンプレートの詳細]ページでデバイスを選択すると、そのデバイスの[デバイステンプレートの詳細]ページが開きます。

メニューオプション	説明/アクション
表示メニュー	<p>次のオプションを選択できます。</p> <ul style="list-style-type: none"> <li>• デバイステンプレート ホーム: [デバイステンプレート]ページが開きます。<a href="#">「[デバイステンプレート]ページのフィールド」(118ページ)</a>を参照してください。</li> <li>• デバイステンプレートの詳細: 詳細を表示する特定のデバイステンプレートを選択できます。</li> <li>• 現在の構成: [デバイス構成の詳細]ページが開きます。このページでは、このテンプレートに現在設定されている構成を表示してコメントを追加できます。[デバイスに配布]オプションをクリックすると、構成配布をスケジュールリングできます。また、構成配布をすぐに開始することもできます。</li> <li>• 構成履歴: [デバイス構成]ページが開きます。そのページで構成の変更を表示できます。<a href="#">「[デバイス構成]ページのフィールド」(173ページ)</a>を参照してください。</li> <li>• ACL: [デバイスACL]ページが開きます。このページでは、アクセス制御リスト (ACL) の情報を表示できます。詳細については、<a href="#">「ACLの表示」(695ページ)</a>を参照してください。</li> <li>• インターフェイス: [デバイスインターフェイス]ページが開きます。このページでは、デバイスのインターフェイス情報を表示できます。詳細については、<a href="#">「[デバイスインターフェイス]ページのフィールド」(205ページ)</a>を参照してください。</li> </ul>
編集メニュー	<p>次のオプションを選択できます。</p> <ul style="list-style-type: none"> <li>• 構成を編集: 現在の構成で、[構成を編集]ページを開きます。構成の編集と配布を行います。詳細については、<a href="#">「[テンプレート構成を編集]ページ」(120ページ)</a>を参照してください。</li> <li>• デバイステンプレートの編集: [デバイステンプレートの編集]ページが開きます。<a href="#">「[デバイステンプレートの新規作成]ページのフィールド」(122ページ)</a>を参照してください。</li> <li>• デバイステンプレートの削除: デバイステンプレートを削除できます。</li> <li>• 新規テンプレートとして保存: 現在のデバイステンプレートをデバイスの新規テンプレートとして保存できます。<a href="#">「[デバイステンプレート]ページのフィールド」(118ページ)</a>を参照してください。</li> <li>• プロセス自動化: [HP Operations Orchestration ログイン]ページが開きます。このページでは、HP Operations Orchestrationにログインしたり、HP Operations Orchestrationフローをガイドモードで起動します。HP Operations Orchestrationの詳細については、『HP Operation Orchestration User's Guide』を参照してください。</li> </ul>
プロビジョニングメニュー	<p>次のオプションを選択できます。</p> <ul style="list-style-type: none"> <li>• テンプレートからデバイスをプロビジョニング: [デバイステンプレート]ページが開きます。このページでは、現在のデバイステンプレートを使用して、別のデバイスをプロビジョニングできます。<a href="#">「デバイス固有のテンプレート」(124ページ)</a>を参照してください。</li> </ul>
コメント	デバイスの説明文が表示されます。
ベンダー	デバイスのメーカー名を表示します。
モデル	デバイスモデル名を表示します。
ドライバ名	デバイスに割り当てられているドライバを表示します。
デバイスタイプ	ルータ、スイッチ、ファイアウォールなど、デバイスのタイプを表示します。



メニューオプション	説明/アクション
デバイスのインポート元	デバイスがNAにインポートされており、インポートソースに名前が付けられている場合は、その名前を表示します。インポートソースに名前が付けられていない場合は、「<日付>に追加」と表示されます。デバイスが手動で追加された場合は、「<日付>に、<user name>が手動で追加」と表示されます。
最終構成変更	デバイスの構成を最後に変更した日付と時刻が表示されます。
管理ステータス	デバイステンプレートは実際のデバイスではなく、アクティブや非アクティブに指定できないことから、デバイステンプレートが表示されます。

## [テンプレート構成を編集]ページ

デバイステンプレートの構成は、本質的にはデバイスの構成ファイル全体を置き換えるスクリプトファイルです。このため構成は、デバイスのブート時に使用可能な完全に動作する構成ファイルである必要があります。

はじめから構成を作成せずに、「新規テンプレートとして保存」コマンドを使用して、ネットワークに既に存在するデバイスの構成をコピーできます。詳細については、「[編集メニューオプション](#)」(230ページ)を参照してください。

変数を使用して、構成をカスタマイズできます。文字「\$」は、変数名用に予約されています。デバイステンプレート中にリテラルの「\$」を入力する必要がある場合、エスケープシーケンス `\x24` を使用してください。

**注意：**「tc\_」で始まる変数は、特別な用途のために予約されています。この文字で始まる任意の変数を定義することはできません。

\$MyVar\$ などのカスタム変数には、[変数をプル]ボタンを使用して定義されるプロンプトを付加できます。[変数をプル]ボタンを更新します。これにより、ページ下部にデバイステンプレートで使用される各変数の入力フィールドが追加されます。これらのフィールドを使用して、変数のカスタムプロンプトを定義したり、各プロンプトの許容値を制限したりします。

- 値に複数行を許可します。
- 値を限定：(先頭、最後、最後の1つ前)
- パスワード（オンにすると、NAは[コマンドスクリプトを実行]タスクページで値の入力を求める際、パスワードをエコーしません）

\$tc\_device\_hostname\$ などの予約変数には、プロビジョニング対象のデバイスからの値が自動的に入力されます。デバイステンプレートからの値自体は、これらの変数には使用されません。

**注意：**CSV ファイルにカスタム変数を入力するのであれば、既存の scriptField1、scriptField2 などのヘッダーを、デバイステンプレートによるカスタム変数の名前で置換できます。CSV ファイルを使用することで、デバイステンプレートは複数のデバイスを1回でプロビジョニングできます。デバイステンプレートでプロビジョニングを行う各デバイスに対し、変数の値を入力してください。



## デバイスのプライマリIPアドレスの変更

デバイステンプレートのプロビジョニングプロセスの一環としてデバイスのプライマリIPアドレスを変更する場合、このための特殊な予約変数 `$tc_device_primary_ip$` が存在します。これはデバイステンプレートにのみ使用します。その他の予約変数とは異なり、デバイスのプロビジョニングタスク実行時にユーザが値を入力するか、CSVファイルに入力します。CSVデータファイルには、この変数は列として含まれます。

デバイステンプレートの構成に `$tc_device_primary_ip$` を含めると、デバイスのプロビジョニングタスク完了後、デバイスへのアクセスに使用されるプライマリIPアドレスがこの新しい値に更新されます。すべてのレポートと検索でデバイスを区別するため、新しいプライマリIPアドレスが表示されます。

## 新しいデバイステンプレートの追加

[デバイステンプレートの新規作成]ページでは、新しいデバイステンプレートを追加できます。

新しいデバイステンプレートを追加するには、[デバイス]メニューバーから[新規作成]を選択し[デバイステンプレート]をクリックします。[デバイステンプレート]ページにある[デバイステンプレートの新規作成]リンクからも、このページにアクセスできます。[デバイステンプレートの新規作成]ページが開きます。

## [デバイステンプレートの新規作成]ページのフィールド

[デバイステンプレートの新規作成]ページでは、デバイステンプレートを構成できます。

**注意：** [デバイステンプレートの編集]ページは、フィールドが入力されている点を除いて[デバイステンプレートの新規作成]ページと同じです。

フィールド	説明/アクション
名前	デバイスのメーカー名を表示します。
パーティション	ドロップダウンメニューからパーティションを選択します（可能な場合）。新しいデバイステンプレートは、パーティション内のデバイスにのみ適用されます。パーティションの作成の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」（148ページ）を参照してください。
デバイスドライバ	ドロップダウンメニューで利用できるドライバのリストからドライバを選択します。
コメント	デバイスに関するコメントを入力します。
<b>接続情報（デバイステンプレートが実際のデバイスではなく、デバイステンプレートをそれ自体に接続することはできないものの、デバイステンプレートからプロビジョニングされるデバイスは、これらの接続情報を引き継ぐ点に注意してください。詳細については、「<a href="#">デバイステンプレート</a>」（118ページ）を参照してください。）</b>	
接続方法	<p>NAでは、次のプロトコルを組み合わせさせてお使いのネットワークデバイスと通信できます。使用するプロトコルを1つ以上選択します。NAでは、プロトコルを選択した時点から任意の時点で最も効率的なプロトコルが選択されます。</p> <ul style="list-style-type: none"> <li>• SNMP</li> <li>• SNMPv1またはSNMPv2c（コミュニティ文字列認証）</li> <li>• SNMPv3（ユーザ認証）：SNMPv3では、以下のオプションがあります。noAuthNoPriv（ユーザ名のみ）、authNoPriv（ユーザ名、認証パスワード）、およびauthPriv（ユーザ名、認証用と暗号化パスワード）。認証方法には、SHA（Secure Hash Algorithm）とMD5（Message Digest Algorithm）があります。暗号化方法には、DES（Data Encryption Standard）、AES（Advanced Encryption Standard）、AES192、およびAES256があります。</li> <li>• RLogin</li> <li>• Telnet</li> <li>• SSH（SSH1またはSSH2（デフォルト）、SSH1のみ、SSH2のみのいずれかを選択できます。）</li> </ul>
転送プロトコル	<p>次のいずれかの転送プロトコルを選択します（複数可）。</p> <ul style="list-style-type: none"> <li>• SCP</li> <li>• FTP</li> <li>• TFTP</li> </ul>

フィールド	説明/アクション
-------	----------

## ACL 解析

次のオプションのいずれかを選択します。

- 有効：オンにすると（デフォルト）、デバイスのACLデータがスナップショットごとに保存されます。スナップショットが取得されるまでACLはロードされません。
- 無効：オンにすると、スナップショットごとにデバイスのACLデータが保存されません。

## 追加情報

NAでは、デバイスのスナップショット取得プロセスで、次のフィールドの一部が自動的に入力されます。手動でこれらのフィールドを入力する場合、デバイスをポーリングするたびにデータが上書きされます。

デバイスの説明	デバイスの識別に使用する説明を入力します。
モデル	デバイスのメーカーのモデル番号を入力します。FQDNの解決タスクでは、デバイスのプライマリIPアドレスに対してリバースDNS検索を実行することで、システム内の各デバイスにFQDN（Fully Qualified Domain Name）を設定できます。
ベンダー	CiscoやNortelなど、デバイスのベンダーを入力します。
階層レイヤ	<p>階層レイヤはデバイス属性です。デバイスの階層レイヤは、デバイスを追加または編集するときに設定できますその結果、ネットワークダイアグラムの構成時にフィルタする階層レイヤを選択できます。たとえば、ネットワーク全体（インベントリ）をダイアグラムで表示し、「コア」でフィルタリングを行ってコアデバイス（階層レイヤが「コア」に設定されたデバイス）のみを取得することもできます。ネットワークダイアグラムの詳細については、「<a href="#">ダイアグラム</a>」（603ページ）を参照してください。</p> <p><b>注意：</b>以下のオプションは、デフォルトの階層レイヤです。カスタム階層レイヤの追加の詳細については、「<a href="#">appserver.rcx ファイルの編集</a>」（611ページ）を参照してください。</p> <p>ドロップダウンメニューから階層レイヤを選択します。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• 未設定レイヤ</li> <li>• コア</li> <li>• 分散</li> <li>• アクセス</li> <li>• エッジ</li> </ul>
カスタムサービスタイプ	サービスタイプを入力します。サービスタイプは、VoIP、BGP、MPLSなどを指定できます。この値により、デバイスの用途を判断できます。これらの値を使用してデバイスサービスにタグ付けすることで、デバイスサービスを容易に検索したり、グループ内のデバイスグループを表示できます（静的または動的）。

完了したら[保存]ボタンをクリックするか、別のデバイステンプレートを追加する場合には[保存してさらに追加]ボタンをクリックしてください。

## デバイス固有のテンプレート

[デバイステンプレート]ページの[プロビジョニング]メニューで[テンプレートからデバイスをプロビジョニング]オプションを選択すると、そのデバイスの[デバイステンプレート]ページが開きます。このページには、デバイステンプレートからプロビジョニング可能で、デバイステンプレートに割り当てられているデバイスに一致するデバイスのリストが表示されます。

フィールド	説明/アクション
デバイスの表示	<p>プルダウンメニューから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• すべて</li> <li>• アクティブ</li> <li>• 実稼動前</li> </ul>
ホスト名	<p>デバイスのホスト名が表示されます。ホスト名をクリックすると、[デバイス詳細]ページが開きます。このページでは、デバイスとその構成履歴に関する情報を表示できます。</p>
デバイスIP	<p>デバイスのIPアドレスを表示します。赤で表示されるデバイスは、最新のスナップショットの取得に失敗しています。非アクティブなデバイスは、IPアドレスの横のアイコンでマーキングされています。IPアドレスをクリックすると、[デバイス詳細]ページが開きます。このページでは、デバイスとその構成履歴に関する情報を表示できます。</p>
デバイスのベンダー	<p>デバイスのメーカー名が表示されます。</p>
デバイスモデル	<p>デバイスのモデル名が表示されます。</p>
パーティション	<p>ドロップダウンメニューからパーティションを選択します（可能な場合）。新しいデバイステンプレートは、パーティション内のデバイスにのみ適用されます。パーティションの作成の詳細については、「<a href="#">デバイスとユーザのセグメント化</a>」（148ページ）を参照してください。</p>
アクション	<p>次のオプションを選択できます。</p> <ul style="list-style-type: none"> <li>• デバイスのプロビジョニング: [タスクの新規作成 - デバイスのプロビジョニング]ページが開きます。そのページで、デバイスをプロビジョニングできます。「<a href="#">[デバイスのプロビジョニング]タスクページのフィールド</a>」（356ページ）を参照してください。</li> <li>• 構成の比較: [デバイス構成の比較]ページが開きます。「<a href="#">[デバイス構成の比較]ページのフィールド</a>」（179ページ）を参照してください。</li> </ul>

## デバイスの新規作成ウィザードの使用

デバイスの新規作成ウィザードを使ってデバイスを追加するには、[デバイス]メニューバーから[デバイスの新規作成ウィザード]をクリックします。[デバイスの新規作成ウィザード]ページが開きます。

### [デバイスの新規作成ウィザード]ページのフィールド

手順	説明/アクション
手順1：デバイスを作成	<p>次の情報を入力します。</p> <ul style="list-style-type: none"><li>• ホスト名またはIPアドレス：デバイスのホスト名またはIPアドレスを入力します。</li><li>• コメント：デバイスに関するコメントを入力します。</li><li>• 管理ステータス：アクティブ、または非アクティブのいずれかを選択します。（<b>注意</b>：実稼動前デバイスは、デバイスの新規作成ウィザードから追加することはできません）。</li></ul> <p>終了したら、次のいずれかをクリックします。</p> <ul style="list-style-type: none"><li>• 次へ：[認証]ページが開きます（以下参照）。</li><li>• 終了：デバイスの追加が完了したら、[デバイスの新規作成ウィザードの完了]ページが開きます。このページには、検出の問題に関する情報が表示されます。</li></ul>
手順2：デバイスを認証	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"><li>• ネットワーク全体のパスワードルールを使用：オンにすると（デフォルト）、ネットワーク全体のデバイスパスワードルールがデバイスに適用されます。[作成]リンクをクリックしてネットワーク全体のパスワードルールを作成することができます。<b>「デバイスパスワードルールの作成」（132 ページ）</b>を参照してください。</li><li>• デバイス固有のパスワードを使用：オンにして、デバイスに次の情報を入力します。ユーザ名、パスワード、イネーブルパスワード（該当する場合）、SNMP読み取りコミュニティ文字列、SNMP読み取りコミュニティ文字列。SNMPv3では、認証および暗号情報を入力します。</li></ul> <p>終了したら、次のいずれかをクリックします。</p> <ul style="list-style-type: none"><li>• 戻る：[デバイスを作成]手順に戻ります。</li><li>• 次へ：[構成]ページが開きます（以下参照）。</li><li>• 終了：デバイスの追加が完了したら、[デバイスの新規作成ウィザードの完了]ページが開きます。このページには、検出した問題が表示されます。</li></ul>
手順3：デバイスを構成	<p>デバイスのベンダーとモデルの検出を試みます。検出が完了すると、そのデバイスの構成を取得および保存します。次に、変更を検出するようデバイスが構成されます。デバイスで変更検出の設定を行わない場合、[デバイスのSyslog設定を更新]チェックボックスをオフにします。このチェックボックスをオンする場合は、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"><li>• HP Network AutomationのSyslogサーバにログ：[デバイスのSyslog設定を更新]チェックボックスをオンにすると、デフォルトでこのチェックボックスもオンになります。</li><li>• 既存のsyslogリレーホストにログ出力：リレーホストのホスト名またはIPアドレスを入力します。（<b>注意</b>：変更検出の正しいログレベルが設定されます。）</li></ul> <p>[終了]をクリックします。デバイスの追加が完了したら、[デバイスを追加ウィザードの完了]ページが開きます。このページには、検出の問題に関する情報が表示されます。</p>

## デバイスのインポート

次のように、CSV（カンマ区切り値）ファイルからデバイスをインポートする方法もあります。

- デバイスパスワードルール（通常はグループに割り当てられる）とCSVファイルを使用します。
- あるCSVファイルのデバイスデータと別のCSVファイルのデバイスパスワード情報をインポートします。

CSVファイルを使ってデバイスをインポートするには、[デバイス]メニューから[デバイスタスク]を選択して、[インポート]をクリックします。[タスクの作成 - インポート]ページが開きます。「[\[デバイスのインポート\]タスクページのフィールド](#)」（329 ページ）を参照してください。

NAでは、デバイスを定期的にCSVファイルからインポートするよう構成できます。デバイスを初めてインポートする場合、次の手順を実行します。

- [デバイスパスワードルール]を設定し、インベントリグループ（すべてのデバイス）に適用します。「[デバイスパスワードルールの作成](#)」（132 ページ）を参照してください。
- デフォルトの接続方法を構成します。「[\[デバイスアクセス\]ページのフィールド](#)」（45 ページ）を参照してください。
- デバイスのインポートファイル（Device.csv）を準備します。Device.csv ファイルを編集するか、またはExcelなどのアプリケーションにロードすることができます。「[デバイスデータのインポートのためのCSVファイルの作成](#)」（126 ページ）を参照してください。

**注意：** [ネットワークデバイスの検出]タスクを使用すると、NAの管理下に置きたいデバイスの位置をネットワーク上で特定できます。IPアドレスの範囲をいったん指定すると、NAがネットワークをスキャンしてデバイスを検索します。詳細については、「[\[ネットワークデバイスの検出\]タスクページのフィールド](#)」（341 ページ）を参照してください。

グループおよびデバイスパスワードルールを使用してデバイスをインポートするには、次のデータが必要となります。

1. インポート対象デバイスの定義済みグループ。「[デバイスグループの追加](#)」（136 ページ）を参照してください。
2. 各グループに対する定義済みのネットワーク全体のパスワードルール。「[デバイスパスワードルールの作成](#)」（132 ページ）を参照してください。
3. 各デバイスが属するグループを含む、作成済みの device.csv ファイル。「[デバイスデータのインポートのためのCSVファイルの作成](#)」（126 ページ）を参照してください。
4. インポート済みデバイスの検出済みドライバ。「[デバイスドライバの検出](#)」（163 ページ）を参照してください。サポートされるデバイスの詳細については、Driver Release Service（DRS）ドキュメントを参照してください。DRSは、自動化されたドライバのリリースと配信システムです。

## デバイスデータのインポートのためのCSVファイルの作成

デバイス、デバイスグループ、デバイスパスワードの情報をCSVファイルからNAにインポートするには、デバイスデータのインポートタスクを使用します。CSVファイルの1行目にインポート対象データのNAデータベースの列名があります。その他の行は、それぞれデバイス、デバイスグループ、デバイス固有パスワードを表しています。

NAにはCSVファイル用のテンプレートがあります。次の点に注意してください。

- 空白の列には列を入力しないでください。既存のデバイスがある場合、空白の値が既存のデータを上書きします。
- 列名はデータベースの列名と一致している必要があります。NAで設定されているデータベースの列名を変更しないでください。
- データフィールドはカンマで区切られているため、フィールドには空白は使用できますが、カンマ (,) は使用できません。フィールド内の値を区切るには、コロン (:) を使用します。
- 列の順序は重要ではありません。

#### インポート用CSVファイルを作成するには：

1. [タスク/テンプレートの新規作成 - デバイスをインポート] ページに移動します。
2. [タスクオプション]、[データ型] で、適切なCSVテンプレートのリンクをクリックします。
3. 編集ツールで、次の操作を実行します。
  - － データテーブルに情報を追加します。
  - － 既存データを上書きしないように、未使用の列を削除します。
  - － CSVファイルの列の詳細については、関連するセクションを参照してください。
    - 「デバイスデータのインポートファイル」(127 ページ)
    - 「デバイスグループデータのインポートファイル」(130 ページ)
    - 「デバイス固有パスワードデータのインポートファイル」(131 ページ)

**注意：** CSV ファイルに英語以外の文字が含まれている場合、Microsoft Office Excel ではなくテキストエディタでファイルを編集します。CSV ファイルの保存にはUTF-8エンコーディングを使用します。

4. ファイルタイプをCSVとしてローカルシステムに保存します。

## デバイスデータのインポートファイル

device.csvテンプレートファイルには、デバイスデータ用のNAデータベース列名が入っています。NAはインポートでデータベース内のデバイスを一意に識別するために、primaryIPAddressおよびhostName列の値とオプションのsiteName列の値を組み合わせ使用します。primaryIPAddressまたはhostName列を1つ以上入力してください。

#### デバイスのインポートファイルのフィールド

列名	説明/アクション
primaryIPAddress	<p>デバイスのプライマリIPアドレスです。</p> <p>各デバイスデータインポートファイルに、primaryIPAddressまたはhostName列が含まれている必要があります。</p> <p>(注意：NAT環境では、NAがデバイスにアクセスするために使用するIPアドレスを指定します)。</p> <p>注意：この値を設定できるのはデバイス作成時のみです。</p>

## デバイスのインポートファイルのフィールド (続き)

列名	説明/アクション
hostName	<p>デバイスのホスト名です。 各デバイスデータインポートファイルに、primaryIPAddressまたはhostName列が含まれている必要があります。 <b>注意：</b>この値を設定できるのはデバイス作成時のみです。</p>
siteName	<p>デバイスが属するサイトの名前（パーティション）です。 <b>注意：</b>この値を設定できるのはデバイス作成時のみです。これは、[デバイスをインポート]タスクページで選択したサイトよりも優先されます。</p>
deviceGroupName	<p>デバイスを含むデバイスグループのコロン区切りのリストです。 デバイスグループ名が存在しない場合、NAによってデフォルトのプロパティを持つデバイスグループが作成されます。</p>
deviceDriver	<p>デバイスドライバの名前です。 <b>ヒント：</b>デバイスドライバを指定せず、使用するドライバをNAに決定させることをお勧めします。</p>
excludeFromPoll	<p>デバイスのポーリング設定です。次の数値のいずれかを指定します。</p> <ul style="list-style-type: none"> <li>• 1：無効（デバイスを自動的にポーリングしない）</li> <li>• 2：ポーリングのみ（通常のポーリングタスクの一環として、デバイスの変更をポーリングする）</li> </ul>
managementStatus	<p>管理ステータスのホスト名です。次の数値のいずれかを指定します。</p> <ul style="list-style-type: none"> <li>• 0：アクティブ（管理対象）</li> <li>• 1：非アクティブ（管理対象ではない）</li> <li>• 3：実稼動前（構成が未完了）</li> </ul>
nATIPAddress	<p>デバイスの内部構成済みIPアドレス。プライマリIPアドレスと異なる場合、NAはこのアドレスでデバイスにアクセスします。</p>
tFTPServerIPAddress	<p>デバイスに対してローカルのTFTPサーバのIPアドレスです。</p>
accessMethods	<p>デバイスの接続方法です。この値は次のように構成されます。 access_methods[+connect_methods[+console]]</p> <ul style="list-style-type: none"> <li>• CLI:TFTP+ssh+console</li> <li>• CLI:FTP+ssh:telnet</li> <li>• SNMP:TFTP</li> </ul> <p>accessMethodsに使用できる値は、CLI、SNMP、TFTP、またはFTPで、複数のアクセス方法をサポートする場合にはコロンで区切ります。 (<b>注意：</b>「connect_methods」はCLIがサポートされている場合にかぎり適用できます。使用可能な値は「SSH」または「Telnet」で、複数の方法をサポートする場合はコロンで区切ります。) 詳細については、「接続方法」（122ページ）を参照してください。</p>
consoleIPAddress	<p>デバイスに関連付けられているコンソールのIPアドレスです。</p>
consolePort	<p>コンソールのポート番号です。 (<b>注意：</b>コンソールサーバへのアクセスに使用できるのはTelnetのみです。)</p>



## デバイスのインポートファイルのフィールド (続き)

列名	説明/アクション
deviceName	デバイスを識別する説明です。 <b>注意</b> ：この値はデバイスのポーリングごとに更新されます。
model	デバイスのメーカーのモデル番号です。 <b>注意</b> ：この値はデバイスのポーリングごとに更新されます。
primaryFQDN	デバイスが属するドメインです。
serialNumber	デバイスのメーカーのシリアル番号です。
vendor	CiscoやNortelなど、デバイスのベンダーです。 <b>注意</b> ：この値はデバイスのポーリングごとに更新されます。
assetTag	デバイスの企業資産タグ番号です。
geographicalLocation	ネットワーク内のデバイスの物理的または論理的な場所です。
performACLParsing	デバイスのACL解析設定です。次の数値のいずれかを指定します。 <ul style="list-style-type: none"> <li>• 0：有効（各スナップショットでACLデータを解析して格納）</li> <li>• 1：無効（各スナップショットでACLデータを解析しない）</li> </ul>
hierarchyLayer	デバイスの階層レイヤです。次の数値のいずれかを指定します。 <ul style="list-style-type: none"> <li>• 1：コア</li> <li>• 2：分散</li> <li>• 3：アクセス</li> <li>• 4：エッジ</li> </ul> <b>注意</b> ：その他の階層レイヤが構成されている場合、他の値も使用できます。詳細については、 <a href="#">「appserver.rcx ファイルの編集」</a> （611ページ）を参照してください。 <b>注意</b> ：この値はデバイスのポーリングごとに更新されます。
comments	デバイスに関する追加情報です。これには、カンマ（,）を含めないでください。
deviceCustom[1-6]	[カスタムデータの設定]ページでその他のデバイスフィールドが定義されている場合、それらのフィールドのデータをインポートできます。テンプレートファイルに定義されている列見出しを使用してください。
<enhanced custom field name>	拡張カスタムフィールドが有効で、デバイスに対して定義されている場合、それらのフィールドのデータをインポートできます。データをインポートするフィールドごとに1つの列を追加します。NAデータベースの拡張カスタムフィールドの実際の名前に合わせて列見出しを設定してください。

## デバイスグループデータのインポートファイル

device\_group.csvテンプレートファイルには、デバイスグループデータ用のNAデータベース列名が入っています。NAはインポートでデータベース内のデバイスグループを一意に識別するために、deviceGroupName列の値を使用します。

### デバイスグループのインポートファイルのフィールド

列名	説明/アクション
deviceGroupName	デバイスグループの名前です（最大255文字）。 この列は、デバイスグループデータのインポートファイルそれぞれに必要です。 <b>注意：</b> この値を設定できるのはデバイスグループ作成時のみです。
siteName	デバイスグループが属するサイトの名前（パーティション）です。
comments	デバイスグループの説明です（最大255文字）。これには、カンマ（,）を含めないでください。
isParent	デバイスグループの親かどうかの指定です。次の数値のいずれかを指定します。 <ul style="list-style-type: none"><li>• 0：親ではない（他のデバイスグループを含まない）</li><li>• 1：親である（他のデバイスグループを含む）</li></ul>
shared	デバイスグループの表示設定です。次の数値のいずれかを指定します。 <ul style="list-style-type: none"><li>• 0：専用（グループの所有者とNA管理者のみ表示できる）</li><li>• 1：公開（すべてのユーザが表示できる）</li></ul>
parentDeviceGroupName	デバイスグループが属する親デバイスグループの名前です。 <b>注意：</b> この値は公開デバイスグループである必要があります。
deviceGroupCustom[1-6]	[カスタムデータの設定] ページでその他のデバイスグループフィールドが定義されている場合、それらのフィールドのデータをインポートできます。テンプレートファイルに定義されている列見出しを使用してください。

## デバイス固有パスワードデータのインポートファイル

`device_auth.csv` テンプレートファイルには、デバイス固有パスワード用のNA データベース列名が入っています。NAはインポートでデータベース内のデバイスを一意に識別するために、`deviceIPAddress` 列の値を使用します。

### デバイス固有パスワードデータのインポートファイルのフィールド

列名	説明/アクション
<code>deviceIPAddress</code>	デバイスのプライマリIPアドレスです。 この列は、デバイスパスワードデータのインポートファイルそれぞれに必要です。
<code>readCommunityString</code>	SNMP 読み取り専用コミュニティ文字列です。
<code>writeCommunityString</code>	SNMP 読み取り/書き込みコミュニティ文字列です。
<code>localUserName</code>	デバイスアクセスに使用するユーザ名です。デバイスがTACACS+などのAAAソリューションを使用するよう構成されている場合、NAのAAAユーザアカウントを作成し、それらのAAA資格情報をデバイスの資格情報として使用します。
<code>localPassword</code>	デバイスアクセスに使用するパスワードです。
<code>enablePassword</code>	NAから特権モードへのアクセスに使用するイネーブルパスワードです。

## デバイスパスワードルールの作成

デバイスパスワードルールを使用すると、同じユーザ名、パスワード、およびSNMPコミュニティ文字列がデバイスグループ、IPアドレスの範囲、またはホスト名に適用されます。

**注意：** デバイスパスワードルールは、「パブリック」デバイスグループにのみ適用可能です。「プライベート」デバイスグループにパスワードルールを適用することはできません。

デバイスにログインしようとする、ログインが成功するまで適用可能な[デバイスパスワードルール]リストが順次適用され、ログインに成功すると、そのルールがデバイスのログイン情報として設定されます。以降のログイン試行でルールを適用できない場合、再度新しい有効なログインが見つかるまで、適用可能なルールを順次試行します。これは[デバイスアクセス]ページで構成できます。詳細については、[「\[デバイスアクセス\]ページのフィールド」\(45ページ\)](#)を参照してください。

**注意：** デバイスパスワード作成時に、[常に最終成功パスワードから試行します]、および[常に定義順でパスワードを試行します]オプションを設定できます。詳細については、[「\[デバイスアクセス\]ページのフィールド」\(45ページ\)](#)を参照してください。

[デバイスパスワードルール]を作成するには、[デバイス]メニューバーから[デバイスツール]を選択して、[デバイスパスワードルール]をクリックします。[デバイスパスワードルール]ページが表示されます。

**注意：** ルールの順序は重要です。NAでは、[デバイスパスワードルール]ページに表示される順でルールが適用されます。スナップショット取得時にパフォーマンスの問題が残っている場合、最も一般的に使用するルールが最上位に来るよう、ルールの順序を変更することを検討してください。また、ルールの適用先グループまたはIP範囲を制限してください。

## [デバイスパスワードルール]ページのフィールド

フィールド	説明/アクション
パスワードルールの新規作成	[デバイスパスワードルール]ページが開きます。このページでは、デバイスパスワードルールを作成および編集できます。詳細については、 <a href="#">「[デバイスパスワードルール]ページのフィールド」(134ページ)</a> を参照してください。
チェックボックス	左側のチェックボックスで、デバイスパスワードルールを削除します。ルールを選択して、[アクション]ドロップダウンメニューから[削除]をクリックします。その隣にある[選択]ドロップダウンメニューを使用して、すべてのルールを選択または選択を解除できます。
変更日	ルールを最後に変更した日付と時刻が表示されます。
ルール名	ルールの名前が表示されます。
タイプ	次のいずれかのルールの種類が表示されます。 <ul style="list-style-type: none"> <li>• IP範囲</li> <li>• ホスト名</li> <li>• デバイスグループ</li> </ul>

フィールド	説明/アクション
パーティション	<p>セキュリティや業務上の理由でパーティションを作成した場合、特定パーティションの各デバイスについてデバイスパスワードルールをパーティションできます。デバイスパスワードルールを、特定のパーティション内の特定デバイスに加え、すべてのパーティション内のすべてのデバイスで共有するように構成できます。デバイスパスワードルールがすべてのパーティションで利用できる場合、[共有]と表示されます。パーティションの作成の詳細については、「<a href="#">デバイスとユーザのセグメント化</a>」(148ページ)を参照してください。</p> <p><b>注意：</b> デバイスパスワードルールを作成する際、ドロップダウンメニューからパーティションを選択できません。詳細については、「<a href="#">[デバイスパスワードルール]ページのフィールド</a>」(134ページ)を参照してください。</p>
デバイス	ルールのホスト名、IPアドレス、またはグループ名が表示されます。
作成者	ルールを変更したユーザのログイン名が表示されます。NAは、名前が使用不可であることを示します。
アクション	<p>各ルールで次のアクションを選択できます。</p> <ul style="list-style-type: none"><li>編集：[デバイスパスワードルール]ページを開いてルールを編集できます。詳細については、「<a href="#">[デバイスパスワードルール]ページのフィールド</a>」(134ページ)を参照してください。（<b>注意：</b> [デバイスパスワードルール]は優先度の高い順に表示されます。リスト内でルールの優先順位を変更するには、矢印を使用します。）</li></ul>

## [デバイスパスワードルール]ページのフィールド

**注意：** パスワードとSNMPコミュニティ文字列は暗号化され、NAデータベースに格納されます。

フィールド	説明/アクション
<b>ルール定義</b>	
ネットワーク全体のパスワードルール	オンにすると（デフォルト）、ネットワーク全体のデバイスパスワードルールがルール内のすべてのデバイスに適用されます。ネットワーク全体のパスワードルールの使用は、デバイス資格情報を設定するための拡張性の高い方法です。
ルール名	ルール名を入力します。
パーティション	ドロップダウンメニューからパーティションを選択します（可能な場合）。デバイスパスワードルールは、パーティション内のデバイスにのみ適用されます。パーティションの作成の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」（148ページ）を参照してください。
挿入位置	ドロップダウンメニューから既存のルール名を選択します。この既存のルールの上に、対象のルールが挿入されます。
IP範囲	オンにして、ルールの適用先となるIPアドレスの範囲の、先頭と末尾を入力します。ワイルドカード（*または?）を使用すると、関連する一連のデバイスにこのルールを適用できます。
ホスト名	オンにして、このルールの適用先となるホスト名を入力します。ワイルドカード（*または?）を使用すると、関連する一連のデバイスにこのルールを適用できます。
デバイスグループ	オンにして、このルールの適用先となる1つのグループの名前をデバイスセクタを使用して選択します。ルールをすべてのデバイスに適用するには、[インベントリ]を選択します。デバイスパスワードルールは、1つのデバイスグループにしか割り当てできないので注意してください。
デバイス固有パスワード情報	オンにして、デバイスのIPアドレスを入力します。[保存]ボタンをクリックしたときに、このページにある現在の認証情報が読み取られ、特定デバイスにコピーされます。
<b>パスワード情報</b>	
ユーザ名	デバイスアクセスに使用するユーザ名を入力します。デバイスがTACACS+などのAAAソリューションを使用するよう構成されている場合、NAのAAAユーザアカウントを作成し、それらのAAA資格情報をデバイスの資格情報として使用します。
パスワード	デバイスアクセスに使用するパスワードを入力します。
パスワードの確認	確認用にパスワードを再入力します。
イネーブルパスワード	NAから特権モードへのアクセスに使用するイネーブルパスワードを入力します。ほとんどの構成変更でイネーブルパスワードが必要です。（ <b>注意：</b> Nortel ASN/ARNなど、一部のデバイスでは、パスワードがなくても特権モードにアクセスできる場合があります。一部のデバイスでは、特権モードのパスワードを無効に構成できます。サイト固有の構成については、ネットワーク管理者にお問い合わせください。）
イネーブルパスワードの確認	確認用にイネーブルパスワードを再入力します。
SNMP読み取り専用コミュニティ文字列	SNMP読み取り専用コミュニティ文字列を入力します。

フィールド	説明/アクション
SNMP 読み取り / 書き込み コミュニティ文字列	SNMP読み取り/書き込みコミュニティ文字列を入力します。
SNMPv3ユーザ名	デバイスアクセスに使用するSNMPv3ユーザ名を入力します。
SNMPv3認証パスワード	NAがデバイスにアクセスするのに使用するSNMPv3認証パスワードを入力します。
SNMPv3認証パスワードを 確認	確認用にSNMPv3認証パスワードを再入力します。
SNMPv3暗号化パスワード	SNMPv3暗号化パスワードを入力します。
SNMPv3暗号化パスワード を確認	確認用にSNMPv3暗号化パスワードを再入力します。
デバイスアクセス設定の 表示	<p>NAは、ほとんどのネットワークおよびネットワークデバイスで動作するよう設計されています。ただし、独自のデバイス構成の場合、NAで特定のデバイスを管理する能力に影響する場合があります。デバイスアクセス設定により、NAをお使いのネットワーク構成に合わせてカスタマイズできます。デバイスアクセス設定は、デバイスのパスワード情報に関連付けられています。ここで入力するデバイス固有の設定は、デバイス固有パスワード情報を使用する場合のみ適用されます。ネットワーク全体のデバイス設定をパスワードルールに追加することもできます。次のような例があります。</p> <ul style="list-style-type: none"> <li>• 実行モードプロンプト</li> <li>• 構成モードプロンプト</li> <li>• システム管理プロンプト</li> </ul> <p><b>注意:</b> デバイスパASSWORDルールを定義する際には、各デバイスアクセス設定に複数の値を定義できますが、デバイスアクセス設定ごとに1つの値のみを指定すべきです。デバイスアクセス設定を2つ以上指定した場合、指定した値のうちの1つだけが使用されますが、使用される値を確認する方法はありません。デバイスアクセス設定の使用の詳細については、<a href="#">[デバイスアクセス設定の使用]</a>リンクをクリックしてください。</p>

終了時に、必ず[保存]をクリックしてください。[デバイスパスワードルール]リストに新規ルールが表示されます。

## デバイスグループの追加

デバイスグループを作成すると、組織固有の方法でデバイスを分類できます。次のいずれかでデバイスが分類されているケースがほとんどです。

- 地理的に実在する場所（シアトル、ニューヨークなど）
- 事業単位/部門（販売、調達、製造など）
- ネットワークアーキテクチャ内での役割（コア、エッジ、分散、アクセスなど）

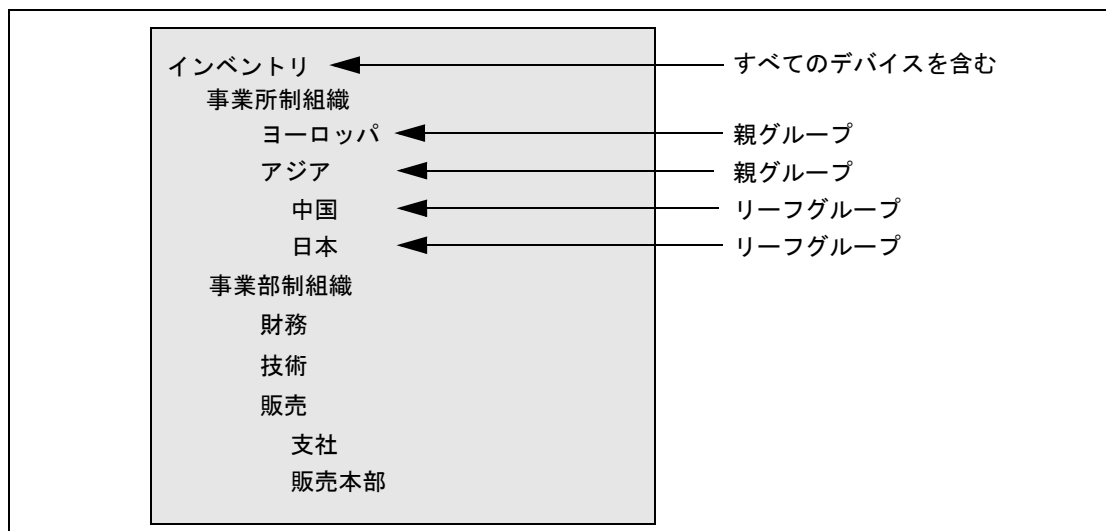
[デバイスグループ]ページには、初期設定でインベントリグループというシステムグループが含まれています。インベントリグループには、NAに追加されるすべてのデバイスが含まれます。ただし、ユーザ定義のグループを作成すると、そのグループもこのページに表示されます。

NAにおけるデバイスグループの階層は、親グループとリーフグループからなります。

- 親グループに指定できる親は1つのみです。新しい親グループの子グループとして親グループを追加した場合、これまでの関連付けは上書きされます。また、親グループにデバイスグループを含めることはできませんが、デバイスを含めることはできません。
- リーフグループにはデバイスのみを含めることができます。他のデバイスグループを含めることはできません。

デフォルトのインベントリグループは、親グループとリーフグループの両方という特殊な扱いとなっていて、システム内のすべてのデバイスが含まれています。親グループに属さないリーフグループは、インベントリグループに属します。

デバイスグループの階層を作成すると、タスクやレポートを簡単に一連のデバイスグループに対して実行できます。デバイスグループの階層例を次に示します。



たとえば、このようなデバイスグループ階層の場合、日本のデバイスまたはアジアのデバイス（中国および日本のデバイスをすべて含む）に対して、タスクとレポートを実行できます。



## [グループの新規作成]ページのフィールド

新規デバイスグループを追加するには、[デバイス]メニューバーから[新規作成]を選択し[デバイスグループ]をクリックします。[グループの新規作成]ページが開きます。

**注意：** NA管理者でなければ、「ビューの管理」または「パーティションの管理」権限をユーザグループに付与することはできません。

フィールド	説明/アクション
グループ名	グループ名を入力します。
説明	グループの説明を入力します。
サイト<名>	ドロップダウンメニューからパーティションを選択します（可能な場合）。フィールド名は[パーティション]ページで変更できます。（詳細については、「 <a href="#">[パーティション]ページのフィールド</a> 」（156ページ）を参照してください）。
所有者	ドロップダウンメニューから名前を選択します。デフォルトの設定は[naadmin]です。
共有	[公開]または[専用]を選択します。[公開]グループはすべてのユーザが表示できますが、[専用]グループを表示できるのは、グループの所有者とシステム管理者のみです。  <b>注意：</b> 専用デバイスグループの場合、複数のユーザが独自のデバイスグループを設定できます。NAにログインすると、そのユーザのデバイスグループと公開デバイスグループのみが表示されます。そのため、ユーザはNAをカスタマイズすることができ、使いやすさと拡張性が向上します。
親デバイスグループ	インベントリグループはドロップダウンメニューに表示されますが、別のグループを選択することもできます。グループを専用にすると、ここで選択したグループは無視されます。専用グループをグループ階層の一部にすることはできません。
デバイス	次のオプションのいずれかを選択します。  <ul style="list-style-type: none"> <li>デバイスセクタを使用して固定デバイスセット（静的グループ）を選択する：デバイスセクタの使用方法の詳細については、「<a href="#">デバイスセクタ</a>」（142ページ）を参照してください。</li> <li>フィルタを使用して動的デバイスセット（動的グループ）を定義する：詳細については、「<a href="#">動的デバイスグループ</a>」（140ページ）を参照してください。</li> </ul>

## 親グループの追加

親グループを追加するには:

1. [デバイス]メニューで、[グループ]をクリックします。[デバイスグループ]ページが表示されます。「[\[デバイスグループ\]ページのフィールド](#)」(145ページ)を参照してください。
2. ページの上部にある[親グループの新規作成]リンクをクリックします。[親グループの新規作成]ページが開きます。

**注意:** 親グループを作成するには、適切な権限が必要です。また、デバイスグループの階層は共有され、親グループはすべて公開にする必要があります。

### [親グループの新規作成]ページのフィールド

フィールド	説明/アクション
グループ名	親グループの名前を入力します。
説明	親グループの説明を入力します。通常この説明によって他のグループと区別されます。
サイト<名>	ドロップダウンメニューからパーティションを選択します。フィールド名は[パーティション]ページで変更できます。(詳細については、「 <a href="#">[パーティション]ページのフィールド</a> 」(156ページ)を参照してください)。
共有	親グループは常に公開です。
親デバイスグループ	インベントリは、デフォルトでドロップダウンメニューに表示されます。
子デバイスグループ	<ul style="list-style-type: none"><li>• 全デバイスグループ: 現在のデバイスグループのリストがすべて表示されます。親グループの子グループとして含めるデバイスグループを選択し、[コピー&gt;&gt;]をクリックします。グループを複数の親グループの子グループにすることはできません。追加するグループが既にいずれかの親グループに属している場合、そのグループは前の親グループから削除されます。</li><li>• このグループの子グループ: 子グループとして親グループに割り当てられたデバイスグループのリストが表示されます。この親グループから削除する子グループを選択して[&lt;&lt;削除]をクリックします。</li></ul>

終了したら、[保存]ボタンをクリックします。[親グループ]ページが開きます。

## [親グループ]ページのフィールド

フィールド	説明/アクション
グループの新規作成	[グループの新規作成]ページが開きます。このページでは、新しいデバイスグループを作成できます。詳細については、「 <a href="#">デバイスグループの追加</a> 」(136ページ)を参照してください。
親グループの新規作成	[親グループの新規作成]ページが開きます。このページで、新しい親グループを追加できます。詳細については、「 <a href="#">親グループの新規作成</a> ページのフィールド」(138ページ)を参照してください。
グループ名	デバイスグループのユーザ定義名が表示されます。グループ名をクリックすると、[デバイスグループの詳細]ページが開きます。詳細については、「 <a href="#">デバイスグループの詳細</a> ページのフィールド」(146ページ)を参照してください。
説明	グループの説明が表示されます。通常この説明によって他のグループと区別されます。
デバイス数	グループ内のデバイス数が表示されます。
所有者	デバイスグループを作成したユーザ名が表示されます。
共有	グループが[公開]か[専用]かを表示します。[公開]グループはすべてのユーザが表示できますが、[専用]グループを表示できるのは、グループの所有者とシステム管理者のみです。
アクション	<p>次のオプションを選択できます。</p> <ul style="list-style-type: none"> <li>表示：選択したデバイスグループに入っているデバイスを表示します。デバイスはこのデバイスグループの直接の子（リーフデバイスグループの場合）か、子グループの子（親デバイスグループの場合）です。[表示]オプションの詳細については、「<a href="#">デバイスグループの表示</a>」(144ページ)を参照してください。</li> <li>グループを編集：[グループを編集]ページが開きます。このページでは、ユーザ定義グループの名前とコメントを変更できます。また、グループからデバイスを追加または削除できます。詳細については、「<a href="#">グループを編集</a>ページのフィールド」(160ページ)を参照してください。</li> <li>削除：グループを完全に削除します。</li> <li>ダイアグラム：[ダイアグラム]ページが開きます。「<a href="#">ダイアグラム</a>」(603ページ)を参照してください。</li> <li>公開/専用に変更：デバイスグループのモードを公開/専用の間で切り替えます。</li> </ul>

## 動的デバイスグループ

動的デバイスグループは、動的デバイスグループに属するデバイスが固定されていない点以外は、静的デバイスグループと同じです。どのデバイスを動的デバイスグループに含めるかは、グループに関連付けられた事前定義の基準を使用したクエリを実行して決定します。

静的デバイスグループの場合と同様、動的デバイスグループは、すべての[Run Device tasks(デバイスタスクの実行)]ページ、[検索]ページ、[ダイアグラム]、[デバイスソフトウェア]レポートなど、すべてのグループリストに表示されます。以下の表に、静的デバイスグループと動的デバイスグループの違いをまとめます。

静的デバイスグループ	動的デバイスグループ
<p>デバイスを選択して作成します。「[グループの新規作成]ページのフィールド」(137ページ)を参照してください。</p> <p>手動で追加、または削除しない限り、デバイスは固定されたままです。</p> <p>グループからデバイスを手動で削除できます。</p>	<p>検索基準のセット、ルールセットのいずれか、または両方を定義することで作成します。検索基準の最大数は10個です。動的デバイスグループを作成する手順を以下に示します。</p> <p>ネットワーク構成イベント、デバイス構成イベントのいずれか、または両方が発生すると、デバイスは変化することがあります。</p> <p>グループからデバイスを手動で削除できません。</p>

**注意：** 動的グループは、グループ階層内の子グループのみにすることができます。さらに、動的グループは、デバイスの所属先となるグループを指定する[デバイスを編集]ページ、[デバイスのインポート]タスクページには表示されません。

## 動的デバイスグループの作成

動的デバイスグループを作成するには、次の2つの方法があります。

- [デバイス検索結果]ページを使用する
- [グループの新規作成]ページを使用する

[デバイス検索]ページを使って動的グループを作成するには：

1. [レポート]メニューバーから[検索]を選択して[デバイス]をクリックします。[デバイスを検索]ページが開きます。
2. 検索基準を入力します。たとえば、[デバイスのベンダー]フィールドをオンにして[Cisco]と入力します。
3. [検索]ボタンをクリックします。[デバイス検索結果]ページが開き、Cisco デバイスがすべて表示されます。
4. ページの一番下までスクロールすると、[検索条件]セクションが黄色で表示されています。
5. 動的グループの名前を入力し、[動的グループとして作成]オプションをオンにして[グループを作成]ボタンをクリックします。
6. [デバイス検索結果]ページの一番上に、「新規デバイスグループ：＜名前＞が正常に作成されました」というメッセージが表示されます。

[グループの新規作成]ページを使って動的グループを作成するには:

1. [デバイス]メニューバーで、[新規作成]を選択し[デバイスグループ]をクリックします。[グループの新規作成]ページが開きます。
2. [グループ名]フィールドに動的グループの名前を入力します。
3. [説明]、[パーティション名]（該当する場合）、[所有者]、[共有]、[親デバイスグループ]、[デバイス]の各フィールドを必要に応じて入力します。これらのフィールドの詳細については、「[\[グループの新規作成\]ページのフィールド](#)」（137 ページ）を参照してください。
4. [デバイス]フィールドまでスクロールします。
5. [フィルタを使用して動的デバイスセット（動的グループ）を定義する]オプションをクリックします。表示を変更すると、次のことができます。
  - ー 1つまたは複数の検索基準（例：[デバイスIP]、[ドメイン名]、[ポリシー準拠]など）を使用して検索を構成する。（**注意**：動的デバイスグループを作成するには、少なくとも1つの検索フィルタ、ルールのいずれかまたは両方を指定する必要があります。）
  - ー 必要に応じて、ANDおよびOR演算子を使用したブール式を作成して検索をフィルタする。

**注意**：このツールでは、正規表現は使用できません。

  - ー デバイスグループ別での検索の制限。このオプションを使用すると、他のグループを基に動的グループを作成できる。
6. 動的デバイスグループを定義したら、[保存]ボタンをクリックします。新しい動的デバイスグループが表示されます。

動的デバイスグループを静的デバイスグループに変更するには、[グループを編集]ページを開き、[デバイス]フィールドまでスクロールします。[デバイスセレクタを使用して固定デバイスセット（静的グループ）を選択する]オプションをクリックします。動的デバイスグループから静的デバイスグループに変更すると、現在のデバイスが新しい静的デバイスグループのメンバーになります。

## 動的デバイスグループの計算

動的デバイスグループのメンバーは、次のタイミングで計算されます。

- 動的デバイスグループをはじめて構成するとき。
- [動的デバイスグループ]ページで、[デバイスリストを更新]をクリックしたとき。
- バックグラウンドプロセスは、すべての動的デバイスグループを定期的に再計算します。
- 事前定義されたデバイス変更イベントが発生したとき。

動的グループの自動再計算、およびイベント主導の再計算パラメータの詳細については、「[サーバ](#)」（52 ページ）を参照してください。

## デバイスセレクト

デバイスセレクトには次の2つのオプションがあります。

- デバイス選択：このオプションを選択すると、たとえばデバイス上でタスクをスケジュールする際に、各種アプリケーションのデバイスを選択するためにグループツリー内を容易に移動できます。
- デバイスグループ選択：このオプションを選択すると、たとえばデバイスグループを編集する際に、各種アプリケーションのデバイスグループを選択するためにグループツリー内を容易に移動できます。

これらの2つのセレクトによって、デバイスおよびデバイスグループ内を移動可能なウィンドウが開きます。

## デバイスの選択

デフォルトで、デバイスセレクトは閉じています。固定デバイスまたは固定デバイスグループをすばやく参照するには、IPアドレス、ホスト名、またはデバイスグループ名の最初の数文字を入力してください。最初の文字を入力した直後に検索結果が表示されます。

自動入力リストから選択するには：

- 1つの項目の場合：項目をクリックするか、下矢印を押して項目を強調表示して、[Enter] キーを押します。
- 複数の項目の場合：[Ctrl] キーを押しながら目的の項目を選択し、[Enter] キーを押します。

自動入力リストから選択解除するには：

- 1つの項目の場合：項目の右側に表示されている赤のXアイコンをクリックします。
- 複数の項目の場合：[Ctrl] キーを押しながら目的の項目を選択し、項目の右側に表示されている赤のXアイコンをクリックします。

たとえば「Default Site:10.255.1.10」というパーティション名を接頭辞として指定して検索する場合、名前全部を入力するまでは自動入力リストにはパーティション名のみが表示されます。たとえば「Def」と入力すると、完全なパーティション名「Default Site:10.255.1.10」は、パーティション名をすべて入力するまでは表示されません。

## デバイスグループの選択

デバイスグループを参照するには、拡大鏡アイコンをクリックします。[デバイスグループセクタ]ウィンドウが開き、インベントリデバイスグループから始まるデバイスグループ階層が表示されます。

デバイスグループ階層はデフォルトで折り畳まれています。プラス記号（+）をクリックすると階層を展開できます。デバイスグループを1回クリックすると、そのグループのすべてのデバイスが表示されます。表示できるエントリ数を超えるエントリが存在する場合は、垂直スクロールバーが表示されます。

デバイスグループ内のすべてのデバイスのリストを表示するには、デバイスグループ名をクリックします。次の情報が表示されます。

フィールド	説明/アクション
フィルタ	デバイスグループをすばやく参照できます。
ホスト名	デバイスのホスト名が表示されます。
デバイスIP	デバイスのIPアドレスを表示します。
デバイスのベンダー	デバイスのメーカー名が表示されます。
デバイスモデル	デバイスのモデル名が表示されます。
パーティション	デバイスグループが属するパーティションを表示します。パーティションとは、NAオブジェクトのセットです。パーティションは、アクセス権限モデルやグループ階層を併用して、NAコア全体のデバイスの配布やネットワークのダイアグラムに使用できます。詳細については、「 <a href="#">パーティション</a> 」（156 ページ）を参照してください。

## デバイスセクタボタン

次のデバイスセクタボタンを使用します。

- [適用]ボタン: デバイスまたはデバイスグループを1つまたは複数選択するには、画面内の目的のエントリをクリックし（クリックしたエントリは強調表示される）、[適用]ボタンをクリックします。選択した項目が追加されます。[デバイスセクタ]ウィンドウまたは[デバイスグループセクタ]ウィンドウは開いたままです。選択したデバイスまたはデバイスグループのいずれかが許可されないと、[適用]ボタンはグレー表示されます。
- [OK]ボタン: 現在選択されている項目を追加し、[デバイスセクタ]ウィンドウまたは[デバイスグループセクタ]ウィンドウを閉じます。選択したデバイスまたはデバイスグループのいずれかが許可されないと、[OK]ボタンはグレー表示されます。
- [キャンセル]ボタン: 変更を保存しないで、[デバイスセクタ]ウィンドウまたは[デバイスグループセクタ]ウィンドウを閉じます。

**注意:** [デバイスセクタ]ウィンドウまたは[デバイスグループセクタ]ウィンドウの右上隅にはリサイズアイコンがあります。最大化表示したり、元のサイズに戻すことができます。

## デバイスグループの表示

[デバイスグループ]ページには、初期設定でインベントリグループというシステムグループが含まれています。インベントリグループには、すべてのデバイスが含まれます。ただし、ユーザ定義のグループを作成すると、そのグループもこのページに表示されます。

[表示]アクションのリンクでは、選択したデバイスグループに入っているデバイスが表示されます。デバイスはデバイスグループの直接の子（リーフデバイスグループの場合）か、子グループの子（親デバイスグループの場合）です。

以前のリリースのNAでは、デバイスグループの名前をクリックしても、リーフグループのデバイスしか表示できませんでした。現在、[表示]アクションリンクをクリックすると、その系統の親グループの視点からデバイスリストを表示できるようになりました。これによって、任意の親グループの視点からデバイスを一括編集できます。

たとえば、州別、郡別、市区町村別にデバイスグループを整理した場合、州レベルですべてのデバイスにバッチ編集を実行できます。以前は、デバイスのバッチ編集は市区町村レベルでしかできませんでした。デバイスグループの追加の詳細については、「[デバイスグループの追加](#)」（136ページ）を参照してください。

デバイスグループを表示するには、[デバイス]メニューバーから[グループ]をクリックします。[デバイスグループ]ページが表示されます。[公開]デバイスグループは、すべてのユーザに表示されます。[専用]デバイスグループを表示できるのは、グループの所有者とNA管理者のみです。



## [デバイスグループ]ページのフィールド

フィールド	説明/アクション
グループの新規作成	[グループの新規作成]ページが開きます。このページでは、新しいデバイスグループを作成できます。詳細については、「 <a href="#">デバイスグループの追加</a> 」(136ページ)を参照してください。
親グループの新規作成	[親グループの新規作成]ページが開きます。このページで、新しい親グループを追加できます。詳細については、「 <a href="#">親グループの新規作成</a> 」ページのフィールド」(138ページ)を参照してください。
グループ名	デバイスグループのユーザ定義名が表示されます。親グループは、他の親グループの子グループになっていない場合はインデント表示されません。親グループに属するグループは、親グループの下にインデント表示されます。グループ名をクリックすると、[デバイスグループ]ページが開きます。このページでは、デバイスグループに関する詳細情報を表示できます。詳細については、「 <a href="#">デバイスグループの詳細</a> 」ページのフィールド」(146ページ)を参照してください。
説明	グループの説明が表示されます。
デバイス数	グループ内のデバイス数が表示されます。
所有者	デバイスグループを作成したユーザ名が表示されます。
共有	グループが[公開]か[専用]かを表示します。[公開]デバイスグループはすべてのユーザが表示できますが、[専用]デバイスグループを表示できるのは、グループの所有者とNA管理者のみです。
アクション	<p>インベントリグループの[アクション]フィールドは、グループ名を選択するまで空白です。ユーザ定義グループでは、次のアクションが表示されます。</p> <ul style="list-style-type: none"> <li>表示: 選択したデバイスグループに入っているデバイスを表示します。デバイスはこのデバイスグループの直接の子（リーフデバイスグループの場合）か、子グループの子（親デバイスグループの場合）です。</li> <li>編集: [グループを編集]ページが開きます。このページでは、ユーザ定義グループの名前とコメントを変更できます。また、グループからデバイスを追加または削除できます。詳細については、「<a href="#">グループを編集</a>」ページのフィールド」(160ページ)を参照してください。</li> <li>削除: グループを完全に削除します。</li> <li>ダイアグラム: [ダイアグラム]ページが開きます。「<a href="#">ダイアグラム</a>」(603ページ)を参照してください。</li> <li>公開/専用に変更: デバイスグループのモードを公開/専用の間で切り替えます。</li> </ul>

デバイスグループのツリーに、デバイスグループのパーティションメンバーシップを示すツールヒントがあります。この情報を使用して、重複するデバイスグループ名を区別したり、デバイスグループのパーティションを設定したりすることができます。

たとえば、複数のパーティションや、表示権限がこれらのパーティションに設定された複数のユーザグループを作成すると、[デバイスグループ]ページで2つのデバイスグループが同じ名前を持つ可能性があります。ツールヒントにより、デバイスグループが属するパーティションの名前を確認できます（例:「Partition1: エッジルータ」、「Partition2: エッジルータ」）。パーティションの構成の詳細については、「[パーティション](#)」(156ページ)を参照してください。

デバイスグループの詳細情報を表示するには、次の手順に従います。

1. [デバイス]メニューで、[グループ]をクリックします。[デバイスグループ]ページが表示されます。
2. 詳細情報を表示するグループ名をクリックします。[デバイスグループの詳細]ページが表示されます。

## [デバイスグループの詳細]ページのフィールド

フィールド	説明/アクション
グループ	[デバイスグループ]ページが開きます。このページでは、すべてのデバイスグループを表示できます。詳細については、「 <a href="#">[デバイスグループ]ページのフィールド</a> 」(145ページ)を参照してください。
デバイスの新規作成	[デバイスの新規作成]ページが開きます。このページでは、新しいデバイスを追加できます。詳細については、「 <a href="#">デバイスの追加</a> 」(106ページ)を参照してください。
デバイスグループの新規作成	[グループの新規作成]ページが開きます。このページでは、新しいグループを追加できます。詳細については、「 <a href="#">デバイスグループの追加</a> 」(136ページ)を参照してください。
親グループの新規作成	[親グループの新規作成]ページが開きます。このページで、新しい親グループを追加できます。詳細については、「 <a href="#">親グループの追加</a> 」(138ページ)を参照してください。
グループを編集	[グループの編集]ページが開きます。このページでは、デバイスグループを編集できます。詳細については、「 <a href="#">[グループを編集]ページのフィールド</a> 」(160ページ)を参照してください。
デバイスリストの更新	ページを更新して、デバイスのグループメンバーシップを再計算します。
現在の作業グループ	現在の作業グループがドロップダウンメニューに表示されます。ドロップダウンメニューから別のグループを選択することもできます。
[アクティブなデバイスのみをリスト表示]チェックボックス	オンにすると、デバイスのリストがアクティブに管理されているデバイスに制限されます。
このグループでタスクを実行	ドロップダウンメニューからタスクを選択して、このグループを実行できます。タスクの実行の詳細については、「 <a href="#">タスクとは</a> 」(277ページ)を参照してください。
チェックボックス	<p>左側のチェックボックスをオンにすると、デバイスを管理できます。デバイスを選択して、[アクション]ドロップダウンメニューをクリックします。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• アクティブ化：選択したデバイスを管理するようにNAに指示します。</li> <li>• 非アクティブ化：選択したデバイスを管理しないようにNAに指示します。</li> <li>• 一括編集：[デバイスを一括編集]ページが開きます。そのページでは、選択したすべてのデバイスに対して、一度にドライバを割り当てて接続方法を設定できます。詳細については、「<a href="#">[デバイスを一括編集]ページのフィールド</a>」(161ページ)を参照してください。</li> <li>• ダイアグラム：[ダイアグラム]ページが開きます。「<a href="#">ダイアグラム</a>」(603ページ)を参照してください。</li> <li>• 削除：選択したデバイスが削除されます。</li> <li>• デバイスグループに対して実行するタスクを選択します。</li> </ul> <p>左側にある[選択]ドロップダウンメニューを使用すると、デバイスを全選択または全選択解除できます。</p>
ホスト名	デバイスのホスト名が表示されます。ホスト名をクリックすると、[デバイス詳細]ページが開きます。このページでは、デバイスとその構成履歴に関する情報を表示できます。
デバイスIP	デバイスのIPアドレスを表示します。赤で表示されるデバイスは、最新のスナップショットの取得に失敗しています。非アクティブなデバイスは、IPアドレスの横のアイコンでマーキングされています。IPアドレスをクリックすると、[デバイス詳細]ページが開きます。このページでは、デバイスとその構成履歴に関する情報を表示できます。
デバイスのベンダー	デバイスのメーカー名が表示されます。
デバイスモデル	デバイスのモデル名が表示されます。

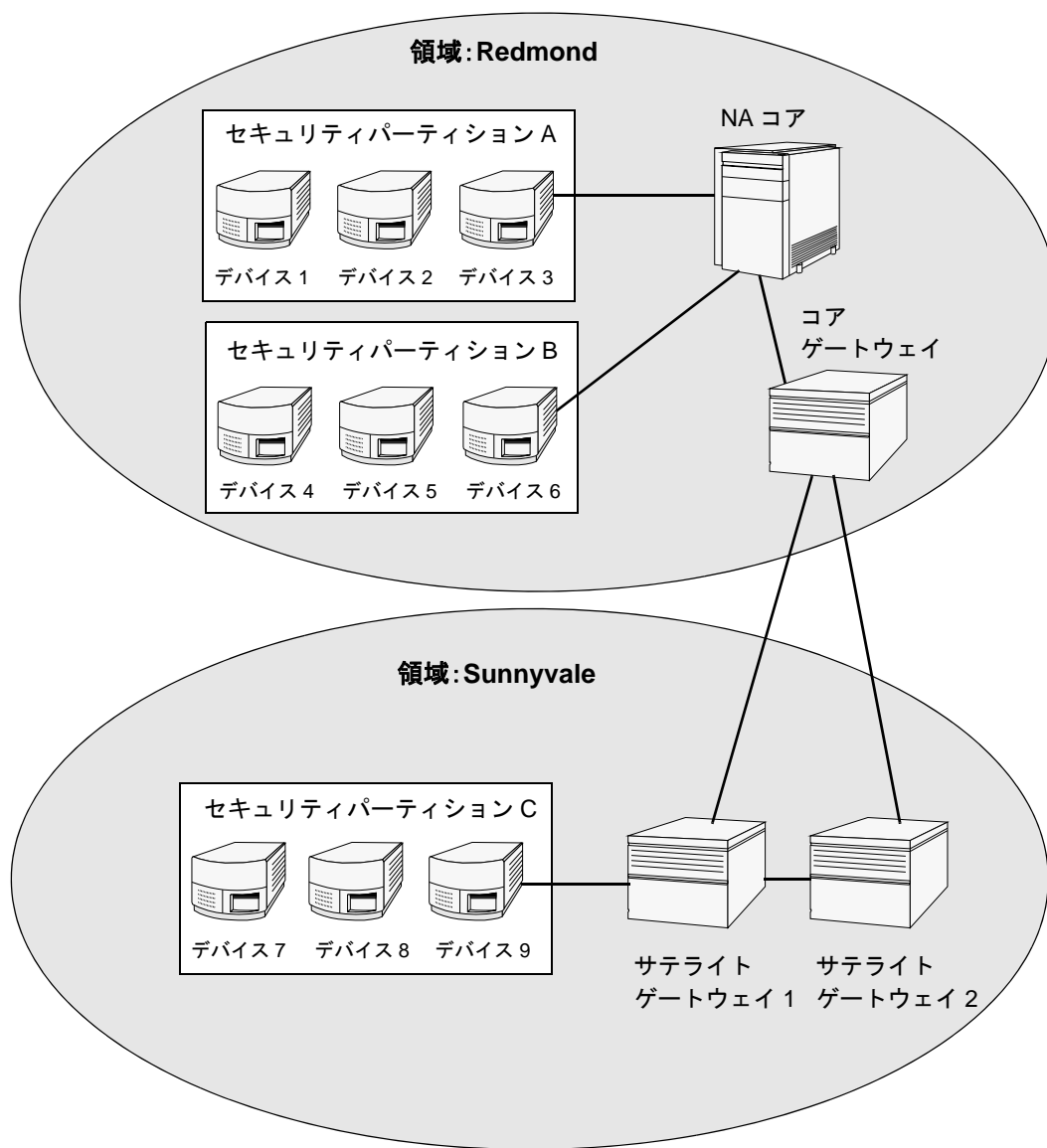
フィールド	説明/アクション
パーティション	デバイスが属するパーティションを表示します。(注意：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。)
最終変更時間	デバイスの構成を最後に変更した日付と時刻が表示されます。
アクション	次のアクションを選択できます。 <ul style="list-style-type: none"><li>編集：[デバイスを編集] ページが開きます。そのページでデバイスの情報を編集できます。詳細については、「<a href="#">[デバイスの編集] ページのフィールド</a>」(111 ページ) を参照してください。</li><li>Telnet：[Telnet] ウィンドウが開きます。</li><li>SSH：[SSH] ウィンドウを開きます。</li><li>構成を表示：[現在の構成] ページが開きます。このページでは、最新の構成を表示してコメントを追加できます。</li></ul>

## デバイスとユーザのセグメント化

NAは、重複IPネットワークを管理し、デバイス（とデバイスグループ）、およびユーザ（とユーザグループ）の両方を分割する機能を備えています。このセクションでは、次の用語を使用します。

- **NAコア**：単一のNA管理エンジン、関連サービス（SyslogおよびTFTP）、および単一のデータベースからなります。NAコアでは、複数のパーティション（デバイスセット）を管理できます。複数のNAコアを分散システム構成に接続できます。（分散システムのインストール方法と構成方法の詳細については、『NA Multimaster Distributed System on Oracle Guide』、または『NA Multimaster Distributed System on SQL Server Guide』を参照してください。）
- **セキュリティパーティション**：ビューの一部となるNAオブジェクトのセットです。NAオブジェクトには、デバイス、ユーザ、コマンドスクリプト、デバイスパスワードルール、ポリシー、ソフトウェアイメージなどを含めることができます。パーティションは、アクセス権限モデルやグループ階層を併用して、NAコア全体のデバイスの配布やネットワークのダイアグラムに使用できます。
- **デフォルトサイトパーティション**：デフォルトのパーティション（名前は「デフォルトサイト」）です。初めてNAを使用する場合、デフォルトパーティションのみが利用できる唯一のパーティションです。デフォルトのサイトパーティションは、ゲートウェイメッシュ経由でシステムからデバイスに接続する際に必要となります。NAが現在管理しているすべてのデバイスがリストされます。デフォルトサイトパーティションの名前は変更できますが、プロパティは変更できません。（**注意**：NAの旧バージョンで複数のパーティションを構成していた場合には、これらのパーティションを編集することができます。ただし、パーティションを追加したり削除することはできません。）
- **領域**：ネットワークセグメントの1つです。一般的に、領域は一意のIPアドレスの集合で識別されます。たとえば、1つの領域に10.255.111.128という番号の2つのデバイスを含めることはできません。その場合は、デバイスを個別の領域に分割する必要があります。パーティションをNAコアの管理と同じ領域に含める必要はありません。領域には多くのパーティションを含めることができます。領域にNAコアを含める必要はありませんが、通常NAコアでは、ローカル領域のデバイスを管理します。NAコアでは、リモート領域のデバイスをゲートウェイメッシュ経由で管理できます。ゲートウェイメッシュを使用して、領域間のIPトラフィックのプロキシを行います。

次の図は、マルチセキュリティパーティションのさまざまなコンポーネントを示したものです。図に示すとおり、領域やパーティションを重複させることはできません。また、デバイスを複数の領域に配置することもできません。ただし、複数のパーティションとNAコアを1つの領域に含めることは可能です。また、複数のゲートウェイを1つの領域に含めることも可能です。



## ローカル領域

デバイスがローカル領域に存在する場合、NAはNAゲートウェイメッシュを介さず、デバイスに直接接続します。

NAがデバイスに接続する際、デバイスがローカルコアと同じ領域に存在する場合は、NAはデバイスに直接的に接続します。それ以外の場合、NAはローカルコアゲートウェイに接続し、コアゲートウェイに指定された領域に存在するデバイスに接続するように要求することで、ゲートウェイメッシュを経由してデバイスに接続します。

**注意：** ローカル領域は、コア領域の別名です。デバイスがコア領域、またはローカル領域に存在する場合、NAはデバイスに直接的に接続します。

## ローカル領域とNATアクセス

NAT IPアドレスがNAのデバイスに割り当てられている場合、NAはNAT IPアドレスを使用してそのデバイスに接続します。NAT IPアドレスには関連付けられている領域があるため、同じルールが適用されます。NAT IPアドレス領域がローカル（コアの領域、または定義されたローカル領域のいずれか）である場合、アクセスは直接行われます。それ以外の場合、アクセスはゲートウェイメッシュを介して行われます。

すべてのNATアクセスがローカルであると想定される場合、領域をNAT IPアドレスに関連に関連付けることで、NA L3ネットワークダイアグラムに、デバイス上の1インターフェイスが別のL3クラウドに存在することを正しく反映させることができます。

## ローカル領域とコンソールアクセス

NAでコンソールサーバがデバイス用に定義されている場合、NAはコンソールサーバを使用して接続します。コンソールサーバのIPアドレスにも、関連付けられた領域名があります。コンソールサーバは、上記のNATアクセスと同様に処理されます。

## ローカル領域と要塞ホストアクセス

要塞ホストがデバイス用に定義されている場合、NAは要塞ホストを使用します。要塞ホストのIPアドレスに領域は割り当てられません。NAは常に要塞ホストにローカルにアクセスします。これにより、リモートデバイスに対する要塞ホストアクセスが存在すれば、ゲートウェイメッシュを使用することなく、ローカル領域を使用して異なるリモート領域に存在するデバイスを制御できます。要塞ホストアクセスでは、CLIのみがデバイスにアクセスできます。このため、SNMPおよびTFTPは使用できません。TFTPが使用できないため、要塞ホストアクセスを使用するソフトウェアの更新は機能しません。

## ローカル領域の追加

ローカル領域を追加するには

1. 「\$HPNA/jre/adjustable\_options.rcx」 ファイルを編集します。ここで \$HPNA は NA インストール（通常は Windows の「C:\Rendition」）のルートです。
2. gateway/mesh/local\_realms のコメントを削除し、ローカル領域名を追加します。

```
<!-- ゲートウェイメッシュ：ゲートウェイメッシュを使用しない領域を定義 -->
<array name="gateway/mesh/local_realms">
  <value>Local Realm 1</value>
  <value>Local Realm 2</value>
</array>
```

3. NA を再起動します。

## 重複IPネットワーク

各パーティションに管理用の NA コアが必要です。ただし、前の図に示したように、管理用の NA コアを、そのコアが管理するパーティションと同じ領域に含める必要はありません。

デバイスにアクセスする際に、NA コアが同じ領域（例：デバイス3）にある場合、NA は管理するデバイスに直接接続されます。NA コアが管理用デバイスと異なる領域（例：デバイス9）にある場合、NA からその領域のサテライトゲートウェイ1に接続され、そこから他のゲートウェイ経由でデバイス9と通信します。

ゲートウェイの集合を「ゲートウェイメッシュ」と呼びます。NA コアと同じ領域にあるゲートウェイを「コアゲートウェイ」と呼びます。NA コアのない領域にあるゲートウェイを「サテライトゲートウェイ」と呼びます。ゲートウェイメッシュを使用すると、NA コアで異なる領域のデバイスを管理できます。（ゲートウェイメッシュの構成方法の詳細については、[「\[デバイスアクセス\] ページのフィールド」](#)（45 ページ）を参照してください）。

重複する IP アドレスを使用するデバイスとネットワークを管理する場合のみ、HP Gateway のインストールおよび構成が必要です。HP Gateway は単独製品のため、NA にはバンドルされていません。

次の複数のコンポーネントを構成できます。

- 領域：重複する IP アドレスを使用できます。つまり、同じ IP アドレスで複数のデバイスを使用できます。
- セキュリティパーティション（同じ領域）：同じ領域にあるデバイスへの表示アクセスを制限できます。パーティションが削除されると、すべてのオブジェクトは自動的にデフォルトパーティションに配置されます（名前は「デフォルトサイト」）。
- ゲートウェイ（同じ領域）：ゲートウェイに障害が発生した場合の稼働時間を改善できます。
- NA コア（同じ領域）：NA システム内のデバイス情報へのアクセスを共有できます。NA Distributed System on Oracle は、マルチマスタシステムで、ゲートウェイメッシュにある各 NA コアのデータからその他すべての NA コアにアクセスできます。これにより、NA コアがクラッシュした場合の冗長データとフェイルオーバーが可能となります。（詳細については、『NA Multimaster Distributed System on Oracle Guide』を参照してください。）

## HP Gatewayの設定

このセクションでは、次の用語を使用します。

- **ゲートウェイ**：他のゲートウェイへのIPトラフィックを振り分けるアプリケーションです。
- **ゲートウェイメッシュ**：自身の間でトラフィックを振り分けるゲートウェイの集合です。
- **コアゲートウェイ**：NAコアと同一領域で動作するゲートウェイです。
- **サテライトゲートウェイ**：NAコアが存在しない領域で動作するゲートウェイです。
- **IP空間**：重複IPアドレスが存在しない1つまたは複数の領域です。

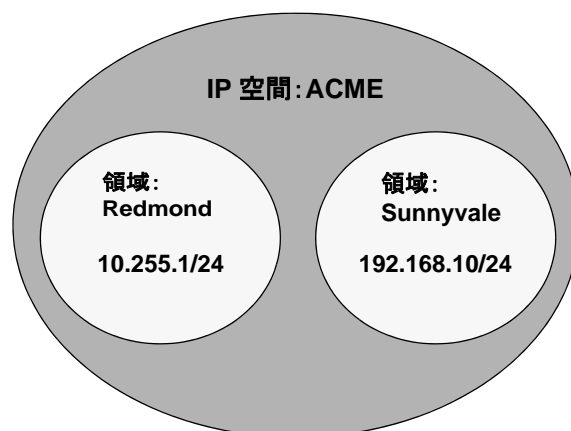
HP GatewayをNAと併用することで、重複IPアドレス（同一IPアドレスを持つ複数のデバイス）のサポートが得られます。さらに、管理対象とするデバイスと同一のLAN上にNAリモートエージェントをインストールすることで、SyslogおよびTFTPをローカルで使用してデバイスを管理できます。詳細については、[「\[リモートエージェントを配布\]タスクページのフィールド」](#)（380ページ）を参照してください。

**注意**：同一LAN内に複数のNAユーザが存在する場合、NAコア（NAマルチマスタ分散システム）の方が、そのLAN上のNAリモートエージェントよりも望ましい場合があります。（詳細については、『NA Multimaster Distributed System on Oracle Guide』を参照してください。）

通常、HP Gatewayを使用すると、1つ以上のNAT変換デバイスまたはファイアウォールで保護されたサーバをNAコアで管理できます。そのためには、Gatewayのインスタンス間に、SSHトンネルと同様の永続的なTCPトンネルを作成する必要があります。さらに、HP Gatewayでは帯域幅の管理もできます。トンネルから低帯域幅のリンクを転送し、帯域幅の使用をリンク速度の範囲内で一定量に制限する必要がある場合には、この機能が重要となります。

**注意**：NAサテライト構成については、『NA Satellite Guide』を参照してください。

HP Server Automation（HP SA）では、ゲートウェイメッシュを各インストールで使います。ただし、NAでは、重複するIPアドレスを処理する必要がある場合のみ、ゲートウェイメッシュを使います。NA/HP SA統合により、領域を重複IPアドレスのないネットワークの集合にすることができます。結果として、IP空間を、重複するIPアドレスがない1つまたは複数の領域として定義できます。



NAT変換環境では、NAコアを異なるIPアドレス空間に配置できます。同じIPアドレス空間のNAコアがある場合、NAコアが管理対象デバイスにトポロジ的に近くなければ、ゲートウェイメッシュ経由ではなくNAコアからデバイスに直接通信する場合の効率性が向上します。WANの稼働率を低減するには、管理対象デバイスからトポロジ的に近い位置にNAサテライトを配置すると、効果的である場合があります。



HP Gatewayを設定するには、次の項目をインストールする必要があります。

1. 各NAコアのコアゲートウェイ
2. 各リモート領域のサテライトゲートウェイ

**注意：** HP SAとHP NA間でゲートウェイを共有する場合、HP SAインストーラを使用する必要があります。NAゲートウェイインストーラは、HP SAが使用するゲートウェイをインストールできません。NAゲートウェイインストーラは、NA専用ゲートウェイメッシュ向けです。

コアゲートウェイのインストール方法、サテライトゲートウェイのインストール方法、およびゲートウェイメッシュを使用するようにNAを構成する方法の手順については、『NA Satellite Guide』を参照してください。ゲートウェイメッシュの構成方法の詳細については、『[\[デバイスアクセス\]ページのフィールド](#)』（45ページ）を参照してください。

## [ゲートウェイリスト]ページのフィールド

[ゲートウェイリスト]ページでは、現在構成されているゲートウェイが表示され、ゲートウェイ情報を編集できます。詳細については、『[\[ゲートウェイの編集\]ページのフィールド](#)』（155ページ）を参照してください。

[ゲートウェイリスト]ページを表示するには、[管理]メニューバーから[ゲートウェイ]をクリックします。[ゲートウェイリスト]ページが開きます。

**注意：** ゲートウェイメッシュをインストールしたら、各サテライトゲートウェイホスト上にNAリモートエージェントをインストールする必要があります。コアゲートウェイのあるホストにはNAリモートエージェントをインストールしないでください。

フィールド	説明/アクション
リモートエージェントを配布	[リモートエージェントを配布]ページを開きます。このページでは、NAリモートエージェントを配布できます。詳細については、『 <a href="#">[リモートエージェントを配布]タスクページのフィールド</a> 』（380ページ）を参照してください。
監視サテライト	[監視の詳細]ページが開きます。このページでは、監視ステータスを表示します。
IP空間	IP空間名を表示します。IP空間とは、重複IPアドレスが存在しない1つまたは複数の領域です。
領域	領域名を表示します。領域名は、ゲートウェイから返されます。領域名は、ゲートウェイのインストール時に設定され、NAでは変更できません。領域名を変更するには、ゲートウェイを再インストールする必要があります（詳細については、『NA Satellite Guide』を参照してください）。
ゲートウェイ	ゲートウェイ名を表示します。ゲートウェイ名は、ゲートウェイのインストール時に設定され、NAでは変更できません（詳細については、『NA Satellite Guide』を参照してください）。
Host	ゲートウェイのインストール先システムのホスト名またはIPアドレスを表示します。ゲートウェイホストが複数のIPアドレスを持つ場合、これはゲートウェイホストが使用するIPアドレスです。ホストIPアドレスが重要となるのは、同一領域内に、複数のゲートウェイが存在する場合のみです。 <b>注意：</b> 冗長性のため、同一領域内に複数のサテライトゲートウェイをインストールできます。
パーティション	領域名に関連付けられているパーティション名を表示します（該当する場合）。詳細については、『 <a href="#">[パーティション]</a> 』（156ページ）を参照してください。

フィールド	説明/アクション
コア	マルチマスタ分散システム環境では、コア名は[コアを編集]ページで設定します。[コアを編集]ページの領域名が、ゲートウェイの領域名と一致する場合、[ゲートウェイリスト]ページにコアのコア名が表示されます。[コアを編集]ページの詳細については、『NA Multimaster Distributed System on Oracle Guide』を参照してください。
エージェント	サテライトゲートウェイのNAリモートエージェントの名前を表示します。NAリモートエージェント名は、[ゲートウェイリスト]ページで変更できます。ゲートウェイメッシュをインストールしたら、各サテライトゲートウェイホスト上にNAリモートエージェントをインストールする必要があります。NAリモートエージェントがインストールされていない場合、[エージェント]列は空欄です。詳細については、「 <a href="#">[リモートエージェントを配布]タスクページのフィールド</a> 」(380ページ)を参照してください。
アクション	次の1つのオプションがあります。 <ul style="list-style-type: none"><li>編集 : [ゲートウェイリスト]ページが開きます。詳細については、「<a href="#">[ゲートウェイの編集]ページのフィールド</a>」(155ページ)を参照してください。</li></ul>

## [ゲートウェイの編集]ページのフィールド

IP 空間名は、領域名を基に自動的に設定されます。ただし、同一 IP 空間内に 2 つの領域が存在し、L3 ダイアグラムで領域を正しく図に示す場合、ゲートウェイを編集して IP 空間名を設定できます。

[ゲートウェイの編集]ページを開くには、[ゲートウェイリスト]ページで[アクション]列の[編集]オプションをクリックします。

フィールド	説明/アクション
ゲートウェイ	ゲートウェイ名を表示します。ゲートウェイ名は、ゲートウェイのインストール時に設定され、NA では変更できません
領域	領域名を表示します。領域名は、ゲートウェイから返されます。領域名は、ゲートウェイのインストール時に設定され、NA では変更できません。
IP 空間	IP 空間名を表示します。IP 空間とは、重複 IP アドレスが存在しない 1 つまたは複数の領域です。新規の IP 空間名を入力します。
Host	ゲートウェイのインストール先システムのホスト名または IP アドレスを表示します。ホスト名または IP アドレスを入力します。
サテライト	NA コアが存在しない領域で動作するサテライトゲートウェイを表示します。該当する場合、サテライトゲートウェイ名を入力します。

## パーティション

パーティションとは、NAオブジェクトのセットです。NAオブジェクトには、デバイス、ユーザ、コマンドスクリプト、デバイスパスワードルール、ポリシー、ソフトウェアイメージなどを含めることができます。パーティションは、アクセス権限モデルやグループ階層を併用して、NAコア全体のデバイスの配布やネットワークのダイアグラムに使用することもできます。

パーティションは、常に公開グループです。これらはデバイスグループの階層内に配置できます。オブジェクト（デバイス、デバイスグループ、ユーザ、またはユーザグループ）がパーティションに追加されると、それまで属していたパーティションから自動的に削除されます。

パーティションが削除されると、すべてのオブジェクトは自動的にデフォルトパーティションに配置されます（名前は「デフォルトサイト」）。これにより、あらゆるデバイスが1パーティションにのみ存在することが保証されます。パーティションが明示されていないIPアドレスを参照する場合、デフォルトのパーティションが使用されます。（パーティションの詳細については、「[デバイスとユーザのセグメント化](#)」（148ページ）を参照してください）。

NAには、ユーザに対して他ユーザの表示を制限する機能があります。このため、NAシステム内のユーザとユーザグループをパーティション化できます。たとえば、管理対象サービスプロバイダが大規模な銀行組織を管理している場合、銀行ユーザに対し、管理サービスプロバイダで作業するユーザを不可視にできます。パスワードルールなどのユーザオブジェクトをパーティション化する場合、すべてのパーティションに対するアクセス権限を持つユーザのみが、グローバル（または共有）オブジェクトの作成、編集のいずれかまたは両方を実行できます。

## [パーティション]ページのフィールド

[パーティション]ページを表示するには、[管理]メニューバーから[セキュリティパーティション]をクリックします。[パーティション]ページが開きます。

フィールド	説明/アクション
パーティション基準	ドロップダウンメニューからパーティションを選択します（可能な場合）。デフォルトのパーティション名は、「サイト」です。デフォルトのサイトパーティションは、ゲートウェイメッシュ経由でシステムからデバイスに接続する際に必要となります。パーティションが明示されていないIPアドレスを参照する場合、デフォルトのサイトパーティションが使用されます。
名前を変更	パーティションの名前を変更できます。この名前は、[デバイスの新規作成]、[デバイスグループの新規作成]、[親デバイスグループの新規作成]の各ページに表示されます。詳細については、「 <a href="#">[デバイスの新規作成]ページのフィールド</a> 」（106ページ）を参照してください。
新規パーティション	[パーティションの新規作成]ページが開きます。このページでは、新規パーティションを作成できます。詳細については、「 <a href="#">[パーティションの新規作成]ページ</a> 」（157ページ）を参照してください。
パーティション名	デフォルトのサイトパーティションとユーザが作成したその他のパーティションが表示されます。
コア	分散NAインストールの場合、これにより、このパーティションでデバイスの管理に使用するNAコアが指定されます。 <b>注意</b> ：NAコアが1つしかない場合、このオプションは表示されません。（詳細については、『NA Horizontal Scalability Guide』、『NA Multimaster Distributed System on Oracle Guide』または『NA Multimaster Distributed System on SQL Server Guide』を参照してください。）
領域名	ドロップダウンメニューから領域を選択します。これは、このパーティションのデバイス、ユーザのいずれかまたは両方が配置される領域が指定されます。 <b>注意</b> ：領域が1つしかない場合（HPゲートウェイメッシュがない場合など）、このオプションは表示されません。NAコアが同じ領域内にない場合、HPゲートウェイメッシュを使用してこのパーティションのデバイスに接続します。

フィールド	説明/アクション
説明	パーティションの説明を入力します。
デバイス数	パーティション内のデバイス数が表示されます。
アクション	次のアクションを選択できます。 <ul style="list-style-type: none"> <li>編集：[パーティションの編集] ページが開きます。詳細については、「<a href="#">[パーティションの編集] ページのフィールド</a>」(157 ページ) を参照してください。</li> <li>削除：パーティションを削除できます。デフォルトのサイトパーティションは削除できません。</li> </ul>

## [パーティションの新規作成] ページ

パーティションを追加するには：

1. [管理]メニューで[セキュリティパーティション]をクリックします。[パーティション]ページが開きます。
2. ページの上部にある[パーティションの新規作成]リンクをクリックします。[パーティションの新規作成]ページが開きます。
3. パーティション名と説明を入力します。
4. [デバイス]フィールドで、デバイスセレクトアを使用して、パーティションに含めるデバイスを選択します。デバイスセレクトアの使用方法的詳細については、「[デバイスセレクトア](#)」(142 ページ) を参照してください。

**注意：**パーティションはデバイスとユーザの両方に適用できます。パーティションがユーザに適用されていると、[ユーザを編集]ページに、パーティションを編集するオプションが表示されます。

5. [保存]ボタンをクリックします。[パーティション]ページが開き、現在のパーティションが表示されます。パーティションという名前のデフォルトパーティションが存在します。このパーティションには、ネットワークで検出されたデバイスがすべて含まれています。

## [パーティションの編集] ページのフィールド

パーティションを編集するには：

1. [管理]メニューで[セキュリティパーティション]をクリックします。[パーティション]ページが開きます。
2. 編集するパーティションの[アクション]列で[編集]オプションをクリックします。[パーティション<パーティションの名>の編集]ページが開きます。次の表に、デフォルトのサイトパーティションを編集する場合のフィールドを示します。

フィールド	説明/アクション
パーティション名	パーティション名を表示します。
説明	パーティションの説明を入力します。
コア	このフィールドはデフォルトのパーティションのパーティションの場合のみ表示されます。分散NAインストールの場合、これにより、このパーティションでデバイスの管理に使用するNAコアが指定されます。(NA コアの詳細については、「 <a href="#">重複IPネットワーク</a> 」(151 ページ) を参照してください)。

フィールド	説明/アクション
領域名	このフィールドは、デフォルトサイトパーティションのパーティションの場合のみ表示されます。ドロップダウンメニューから領域を選択します。この結果、このパーティションのデバイスを配置する領域が指定されます。NAコアが同じ領域内にない場合、NAはゲートウェイメッシュを使用してこのパーティションのデバイスに接続します。
デバイス	デバイスセクタの[デバイス]ボックスにデバイスのリストが表示されます。デバイスセクタの使用方法的詳細については、「 <a href="#">デバイスセクタ</a> 」(142 ページ) を参照してください。パーティションにデバイスを追加すると、追加されたデバイスは、前のパーティションから自動的に削除されます。また、パーティションを削除する場合、システムから削除する前に、すべてのデバイスを別のパーティションに移す必要があります。

終了時に、必ず[保存]ボタンをクリックしてください。

## パーティションにデバイスを追加

パーティションにデバイスを追加するには：

1. [管理]メニューで[セキュリティパーティション]をクリックします。[パーティション]ページが開きます。
2. [パーティション名]列で、編集するサイトをクリックします。[パーティション]ページが開きます。このページでは、[インベントリ]ページと同様、パーティション内の管理対象デバイスのリストを表示できます。ただし、このページの上部には、[グループを編集]と[パーティション]という2つのリンクが追加されています。[パーティション]リンクをクリックすると、[パーティション]ページに戻ります。(詳細については、「[\[インベントリ\]ページのフィールド](#)」(186 ページ) を参照してください)。
3. [グループを編集]リンクをクリックすると、[パーティションの編集]ページが開きます。このページでは、パーティション内のデバイスを編集できます。終了時に、必ず[保存]をクリックしてください。(パーティションの詳細については、「[デバイスとユーザのセグメント化](#)」(148 ページ) を参照してください)。

フィールド	説明/アクション
パーティション名	パーティションの名前が表示されます。
説明	パーティションの説明が表示されます。
デバイス	該当する場合は、デバイスのリストを表示します。デバイスセクタの使用方法的詳細については、「 <a href="#">デバイスセクタ</a> 」(142 ページ) を参照してください。

終了時に、必ず[保存]ボタンをクリックしてください。

## パーティション詳細の表示

パーティションはデバイス、ユーザのいずれかまたは両方に設定できます。デバイス、ユーザのいずれかまたは両方は、1つのパーティションにのみ配置できます。複数のパーティションが存在する場合、各デバイス、ユーザのいずれかまたは両方は、1つの（唯一の）パーティションに配置されます。

パーティション情報を表示または編集するには、次の手順に従います。

1. [管理]メニューで[セキュリティパーティション]をクリックします。
2. 必要な情報があるパーティションをクリックします。詳細については、[「\[インベントリ\]ページのフィールド」](#)（186 ページ）を参照してください。

## デバイスグループの編集

既存のデバイスグループを編集するには：

1. [デバイス]メニューで[グループ]をクリックします。[デバイスグループ]ページが表示されます。
2. 編集するデバイスグループの[アクション]列で[編集]をクリックします。[グループの編集]ページが開きます。入力が完了したら、必ず[保存]をクリックします。

### [グループを編集]ページのフィールド

フィールド	説明/アクション
グループ名	デバイスグループ名が表示されます。
説明	デバイスグループの説明が表示されます。
パーティション	ドロップダウンメニューからパーティションを選択します。(注意：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。) 一般的に、パーティションとは一意のIPアドレスを持つデバイスのグループです。単一のNA コアで複数のパーティションを管理できます。NA コアはNA サーバのインストールコンポーネントの1つで、単一の管理エンジン、関連サービス、および単一のデータベースからなります。
共有	編集中のデバイスグループが公開または専用であること、またはデバイスグループが親グループであることを通知します。リーフグループを編集している場合、そのデバイスグループに親グループがあることがユーザに通知されます。
親デバイスグループ	親デバイスグループの名前がドロップダウンメニューに表示されます。
デバイス	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• デバイスセクタを使用して固定デバイスグループ（静的グループ）を選択する：デバイスセクタの使用方法的詳細については、「<a href="#">デバイスセクタ</a>」(142 ページ) を参照してください。</li> <li>• フィルタを使用して動的デバイスセット（動的グループ）を定義する：表示を変更すると、1つ以上の検索基準を使用して検索を構成する、AND および OR 演算子を使用したブール式を作成して検索をフィルタする、またはデバイスグループごとに検索を制限することができます。 注意：このツールでは、正規表現は使用できません。</li> </ul>
子デバイスグループ	<ul style="list-style-type: none"> <li>• 全デバイスグループ：現在のデバイスグループのリストがすべて表示されます。親グループの子グループとして含めるデバイスグループを選択し、[コピー &gt;&gt;] をクリックします。</li> <li>• このグループの子グループ：子グループとして親グループに割り当てられたデバイスグループのリストが表示されます。この親グループから削除する子グループを選択して[&lt;&lt;削除] をクリックします。</li> </ul>



## デバイスの一括編集

一括編集機能を使用してデバイスの設定を変更できます。以下のことが可能です。

- ドライバの割り当て
  - 接続方法（SNMP、SNMPv3、Telnet、SSH）の設定
  - 転送プロトコル（SCP、TFTP、FTP）の設定
  - 要塞ホスト情報の設定
  - 最後に使用したパスワードのリセット
  - ACL解析の設定
1. [デバイス]メニューで、[インベントリ]をクリックします。現在管理されているデバイスのリストがすべて開きます。
  2. 一括処理で編集するデバイスのチェックボックスをオンにします。
  3. [アクション]ドロップダウンメニューから[一括編集]をクリックします。[デバイスの一括編集]ページが表示されます。終了時に、必ず[保存]をクリックしてください。

## [デバイスを一括編集]ページのフィールド

フィールド	説明/アクション
デバイス	選択されたデバイスのリストが表示されます。
ドライバを割り当て	オンにして、デバイスに一括して割り当てるドライバを選択します。
接続方法を設定	<p>オンにして、次の接続方法および転送プロトコルから一括編集のアクセス方法を選択します。</p> <p>接続方法：</p> <ul style="list-style-type: none"> <li>• SNMP</li> <li>• SNMPv3（ユーザ認証）：SNMPv3では、以下のオプションがあります。noAuthNoPriv（ユーザ名のみ）、authNoPriv（ユーザ名、認証パスワード）、およびauthPriv（ユーザ名、認証用と暗号化パスワード）。認証方法には、SHA（Secure Hash Algorithm）とMD5（Message Digest Algorithm）があります。暗号化方法には、DES（Data Encryption Standard）、AES（Advanced Encryption Standard）、AES192、およびAES256があります。</li> <li>• SNMPv1またはSNMPv2c（デフォルト）</li> <li>• Telnet</li> <li>• SSH：SSH1またはSSH2（デフォルト）、SSH1のみ、SSH2のみのいずれかを選択します。</li> </ul> <p>転送プロトコル（デフォルト）</p> <ul style="list-style-type: none"> <li>• SCP</li> <li>• SFTP</li> <li>• FTP</li> <li>• TFTP</li> </ul>

フィールド	説明/アクション
要塞ホスト情報を設定	<p>オンにして、次の情報を入力します。</p> <ul style="list-style-type: none"> <li>• 必要に応じて、[TelnetおよびSSHアクセスにUnixまたはLinux要塞ホストを使用]を使用します。</li> <li>• IPアドレスまたはホスト名</li> <li>• ユーザ名</li> <li>• パスワード</li> <li>• パスワードの確認</li> </ul>
最後に使用されたパスワードのリセット	<p>オンにすると、最後に使用されたパスワードがリセットされます。</p>
ACL解析を設定	<p>オンにして、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 有効（各スナップショットでACLを解析して格納）</li> <li>• 無効（各スナップショットでACLを解析しない）</li> </ul>
階層レイヤを設定	<p>ドロップダウンメニューから階層レイヤを選択します。</p>
カスタムサービスタイプの設定	<p>オンにすると、サービスタイプを選択できます。サービスタイプは、VoIP、BGP、MPLSなどを指定できます。この値により、デバイスの用途を判断できます。これらの値を使用してデバイスサービスにタグ付けすることで、デバイスサービスを容易に検索したり、グループ内のデバイスグループを表示できます（静的または動的）。</p>
カスタムデータフィールドを設定	<p>オンにすると、デバイスに割り当てたカスタムデータを編集できます。詳細については、「<a href="#">拡張カスタムフィールド設定</a>」（558 ページ）を参照してください。</p>

## デバイスドライバの検出

検出機能を利用して、適切なデバイスドライバとデバイスを一致させます。デバイスドライバは、デバイス固有のコマンドを、NAで異機種混在環境の管理に使用するための統一された形式に変換します。

検出では、SNMPまたはTelnet/SSHを使用して新規デバイスごとにクエリを実行し、適切なデバイスドライバを割り当てます。このプロセスに失敗すると、結果が[最近のタスク]ページに表示されます。NAでは、適切なドライバが割り当てられるまで、デバイス構成をアクティブに管理できません。ドライバの検出に失敗した場合、ドライバを手動で割り当てられます。サポートされるデバイスの詳細については、Driver Release Service (DRS) ドキュメントを参照してください。DRSは、自動化されたドライバのリリースと配信システムです。

デバイスドライバの検出プロセスを開始するには、[デバイス]メニューバーから[デバイスタスク]を選択して、[ドライバの検出]をクリックします。[タスクの新規作成 - ドライバの検出]ページが開きます。「**[ドライバの検出]タスクページのフィールド**」(293 ページ) を参照してください。ソフトウェアの配布タスクからデバイスドライバの検出を開始することもできます。ソフトウェアのアップロードが完了してデバイスを再起動すると、このオプションをオンにしている場合、デバイスドライバの検出タスクが開始されます。

## Telnetを使用したデバイスへのアクセス

NAからTelnetセッションおよびSSHセッションを開始する利点がいくつかあります。

- ログインの簡略化：ユーザはNAアカウントを使用してログインできます。NAは、ユーザの権限を検証します。ユーザは、NAのCLIコマンドを入力するか、または直接デバイスに接続します。たとえば、ユーザは1つのセッションでデバイスを終了して、別のデバイスに接続できます。ユーザが記憶する必要のあるログイン情報は、デバイスのベンダーやタイプなどに関係なく、1つのみです。要求したログイン方法が機能しない場合でも、NAにより自動的にバックアップのログイン方法が試行されます。
- グループや権限ごとに編成する：デバイスをグループごとに編成し、権限をグループ単位で割り当てることで、ユーザは権限のある目的のデバイスへ確実にアクセスできます。
- AAA資格情報がなくても構成を保存できる：Telnet/SSHプロキシを使用すると、変更した構成、インラインコメント、変更したユーザなどの情報を保存できます。Telnet/SSHプロキシでは、自動的にセッションの監査ログと構成を関連付けます。
- ACLの削減：デバイスごとに1つずつアクセス制御リスト（ACL）を用意する必要はなく、NAサーバ用に1つあれば大丈夫です。
- セキュリティの強化：ネットワーク上でデバイスを変更したユーザを識別することにより権限のないユーザの検出や権限外の変更の追跡などが容易になります。また、NAでは、権限外の変更が行われる前に保存された安定した構成を簡単に配布し、想定される障害を修正し、ネットワークサービスを迅速に復元します。

さらに、Telnet/SSHクライアントからNA経由でデバイスに接続できるため、セッションを追跡できます。NAは、次のクライアントからの接続によってテストされています（これ以外のクライアントからの接続も機能する場合があります）。

- SecureCRT
- Windows Telnet
- Putty

Telnet/SSHプロキシインターフェイスに関連するシステム管理設定は多数あります。詳細については、「[Telnet/SSH](#)」（65 ページ）を参照してください。

NAを使用してTelnetセッションを開始するには、[デバイス]メニューバーから[インベントリ]をクリックします。現在管理されているデバイスのリストがすべて開きます。デバイスの[アクション]列で[Telnet]オプションを選択します。デバイスにログインすると、[Telnet]ウィンドウにデバイスプロンプトが表示されます。

**注意：** お使いのシステムにJava Runtime Environment（JRE）がインストールされていない場合、TelnetまたはSSHを初めて使用する場合に、ブラウザ経由でSunのWebサイトからダウンロードが開始されます。この場合、JREのダウンロードとインストールを許可してください。

NAから初めてTelnetまたはSSHセッションを実行する場合、HPから証明書をダウンロードするよう要求するセキュリティウィンドウが表示される場合があります。[常に許可する]をクリックして続行します。これにより、HPコンテンツの信頼性が検証されます。

これで任意のデバイスコマンドを入力できます。終了時に、*quit*と入力します。これでTelnetセッションからログアウトしますが、NAのTelnetプロキシセッションは続行しています。プロキシセッションでは、NA> プロンプトが使用されます。

Telnet/SSH プロキシセッションでは、別のデバイスに接続するか、またはNA CLIコマンドを入力できます。任意のページで上部の[接続]をクリックすると、プロキシセッションを直接開始できます。

**注意：** NAは、セッションからのすべてのコマンド/応答シーケンスの分割を試みますが、確実ではありません。デバイスがコマンドを自動的に実行するとき、またはデバイスが次のコマンドパラメータを求めるとき、必ずしも明瞭なコマンド/応答の分割になるとは限りません。さらに、これらの対話型ショートカットが使用されているセッションは、高度なスクリプトを生成するには不向きである場合があります。

## SSHを使用したデバイスへのアクセス

SSHセッションを開始するには、[デバイス]メニューバーから[インベントリ]をクリックします。現在管理されているデバイスのリストがすべて開きます。デバイスの[アクション]列で[SSH]オプションを選択します。これで任意のデバイスコマンドを入力できます。終了時に、*quit*と入力します。

**注意：** 任意のページで上部の[接続]をクリックすると、プロキシセッションを直接開始できます。SSHプロキシセッションでは、別のデバイスに接続するか、またはNA CLIコマンドを入力できます。

## Telnet/SSHセッションのリスト表示

TelnetセッションおよびSSHセッションのリストを表示するには、[デバイス]メニューバーから[インベントリ]をクリックします。現在管理されているデバイスのリストがすべて開きます。デバイスをクリックします。そのデバイスの[デバイス詳細]ページが開きます。[表示]ドロップダウンメニューから[Telnet/SSHセッション]をクリックします。[Telnet/SSHセッション]ページが開き、デバイスのホスト名またはIPアドレスが上部に表示されます。

### [Telnet/SSHセッションリスト]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスを使用してセッションを削除できます。セッションを選択して、[アクション]ドロップダウンメニューから[削除]をクリックします。横の[選択]ドロップダウンメニューにより、すべてのセッションを選択または削除できます。
開始日	セッションが開始された日付と時刻が表示されます。
ステータス	セッションの状態（[オープン]または[クローズ]）が表示されます。
タイプ	セッションのタイプ（TelnetまたはSSH）が表示されます。
終了日	セッションが終了した日付と時刻が表示されます。
作成者	セッションを作成したユーザの名前を表示します。
<カスタムフィールド>	このページには、Telnet/SSHセッションに定義したカスタムフィールドがすべて表示されます。
アクション	次のオプションから選択できます。 <ul style="list-style-type: none"><li>• 全Telnet/SSHセッションを表示：[Telnet/SSHセッション]ページが開きます。このページでは、このセッション中に入力したコマンドとデバイスからの応答が表示されます。</li><li>• コマンドのみ表示：[Telnet/SSHセッション]ページが開きます。このページでは、このセッション中に入力したコマンドのみ表示されます。このデバイスまたは他のデバイスで再生用にスクリプトを記述する場合に便利です。任意のコマンドをクリックすると、そのコマンドに対するデバイスからの応答が表示されます。</li></ul>

**注意：** マウスを左クリックした状態でテキストを選択すると、テキストが強調表示されます。次に、[Enter] キーを押してテキストをクリップボードに貼り付けます。Telnet/SSHアプレット内でマウスの右ボタンをクリックすると、クリップボードのテキストがアプレットに貼り付けられます。

connectコマンドを使用する場合のショートカットは、connect dev\*のように、ワイルドカードをホスト名またはIPアドレスに追加します。これで、デバイスのリスト（または検索の絞り込みを要求するメッセージ）が返されます。接続するデバイス数を入力します。シェルインターフェイスでは、次の制御文字がサポートされています。

制御文字	説明
^A	カーソルを入力行の先頭に移動します。
^B、左矢印	カーソルを1文字前へ戻します。
^C	入力行をキャンセルして新しいプロンプトに戻ります。
^D	カーソル上の文字を消去します。
^F、右矢印	カーソルを1文字先に進めます。
^H、Backspace、Delete	カーソル上の文字を消去して1文字前に戻ります。
^J、^M	CRLF（改行）を行います。
^K	カーソル上の文字から行末までを削除し、テキストをキルバッファに移動します。
^L、^R	新たなコマンドラインでコマンドをエコーします（画面の再描画をシミュレートします）。
^N、下矢印	コマンド履歴の中で次のコマンドに移動します。
^P、上矢印	コマンド履歴の中で前のコマンドに移動します。
^T	カーソル上の文字を前の文字と入れ替えます。
^U、^X	行頭からカーソル上の文字までを削除し、削除した文字列をキルバッファに移動します。
^W	単語の先頭からカーソル上の文字までを削除し、削除した文字列をキルバッファに移動します。
^Y	キルバッファの文字列を現在の場所に戻します。
^\	現在のデバイス接続を終了します（コンソールサーバ経由のアクセスで便利です）。
ESC-b	カーソルを1単語分前に戻します。
ESC-f	カーソルを1単語分先に進めます。

## Telnet/SSH プロキシを使用した構成の変更

Telnet/SSH プロキシ経由で構成を変更するには、次の手順に従います。

1. NA サーバへ Telnet または SSH 経由で接続し、NA 資格情報を使ってログインします。
2. `connect` コマンドを使ってデバイスに接続します。`connect *` を入力すると、NA 経由の接続に使用できるデバイスが表示されます。表示されるデバイス数が多すぎる場合、ホスト名の最初の数文字（または IP アドレスの最初の数桁）を入力し、その後ろにアスタリスク（\*）を付けると（例：`connect bor*`）、このフィールドを絞り込むことができます。
3. 接続先のデバイスの Telnet/SSH プロキシに表示される数値のリストから、数値を選んで入力します。アクセスの資格情報を確認後、自動的にデバイスにログインします。
4. たとえば、Cisco IOS デバイスの場合、デバイスの `Config T` モードに入力すると、関連するコメントを変更または追加できます。
5. `Configure Terminal` モードを終了して `Exit` と入力します。
6. NA の Telnet/SSH プロキシを終了するには、プロンプトで `Exit` と入力します。

Telnet/SSH プロキシを使用する場合、デバイスにログインすると同時にインラインコメントが表示されます。



## 要塞ホストの使用

要塞ホストは、専用ネットワークと公開ネットワークのゲートウェイです。セキュリティ対策として要塞ホストを使用すると、専用ネットワークと公開ネットワークの障壁の役割を果たし、悪意のあるユーザからの攻撃を回避できます。

NAで要塞ホストを使用すると、TelnetまたはSSHアクセスの機能をロックダウンできます。以下のことが可能です。

- デバイス単位で要塞ホストを指定します。
- ユーザ名（任意）およびパスワードを要塞ホストのログインの資格情報として指定します。
- 要塞ホストにTelnetまたはSSH経由で接続し、次にTelnetまたはSSH経由でターゲットデバイスに接続します。

**注意：** 要塞ホストを使用する場合、すべてのCLIアクセスがデバイスへ直接ルーティングされずに、要塞ホスト経由でルーティングされます。Telnet/SSHプロキシ経由で要塞ホストを使用するよう構成されたデバイスに接続する場合、NAから要塞ホスト経由で接続されます。ユーザのAAA資格情報が提示されている場合は、その資格情報が要塞ホストとターゲットデバイスの両方に適用されます。

要塞ホストへのアクセスでは、通常のNAパスワードルールの処理が行われません。要塞ホストの資格情報が無効な場合、フォールバックは実行されません。要塞ホストへログイン後、そこからデバイスへのアクセスは、NAの通常のパスワード処理に従って行われます。

**注意：** 複数の要塞ホストを特定のデバイスに指定できません。ただし、DNS名を共有する複数の要塞ホスト間で負荷分散を行うと、この状態をシミュレートできます。

Telnet/SSHアクセスにUNIXまたはLinuxの要塞ホストを指定するには、次の手順に従います。

1. [デバイス]メニューで、[インベントリ]をクリックします。現在管理されているデバイスのリストがすべて開きます。
2. ページの上部にある[デバイスの新規作成]リンクをクリックします。[デバイスの新規作成]ページが開きます。
3. ページ中段あたりまでスクロールし、[接続情報]セクションを探します。詳細については、「[\[デバイスの新規作成\]ページのフィールド](#)」（106ページ）を参照してください。

新規デバイスのデフォルトでTelnetおよびSSHアクセスに要塞ホストを使用するよう指定するには、[管理]メニューバーから[システム管理設定]を選択して、[デバイスアクセス]をクリックします。詳細については、「[\[デバイスアクセス\]ページのフィールド](#)」（45ページ）を参照してください。



## 第4章：デバイス構成の管理

### トピックの参照先リスト

トピック	参照先：
はじめに	<a href="#">「はじめに」</a> （172ページ）
デバイス構成変更の表示	<a href="#">「デバイス構成変更の表示」</a> （172ページ）
デバイス構成の比較	<a href="#">「デバイス構成の比較」</a> （179ページ）
デバイス構成の配布	<a href="#">「デバイス構成の展開」</a> （180ページ）

## はじめに

HP Network Automation (NA) は、デバイス構成の変更を検出して記録します。デバイス構成の変更があると、NAはその構成を中央リポジトリにダウンロードします。NAは複数のリアルタイム変更検出および警告システムをサポートしており、変更内容と変更者を即座に特定できます。

Syslogを通じてユーザ属性をサポートしているCisco IOSなどのデバイスでは、NAがユーザ名を抽出して、構成変更とそのユーザ名との関連付けをします。そのユーザ名とNAユーザとの間で関連付けができない場合には、ランダムに生成されたパスワードを持つユーザアカウントを新たに作成します。デフォルトでは、新規ユーザが自動生成されたことを示す、「\_auto」の文字がユーザ名の末尾に付けられます。これにより、未登録ユーザによるものを含むすべての変更について、その変更者を記録できます。AAAアカウントングログ、Syslogメッセージ、プロキシログなど複数のメソッドを用いて、NAは構成変更の作成を検出します。

アクセス制御リスト (ACL) とは、数多くあるデバイスの構成の1つです。ACLにより、ルータのインターフェイスでフォワードされたパケットを受け入れるのか、ブロックするのかを制御して、ネットワークトラフィックをフィルタリングします。

一般にACLは、構成ステートメントの集合と定義されます。これらのステートメントでは許可または拒否をするアドレス、プロトコル、およびパターンを定義します。ルーティング更新内容の制限やネットワークセキュリティの確保を目的に、ACLを使用することができます。

NAは、デバイスから構成情報を取得し、構成からACLステートメント、およびアプリケーションを抽出します。さらに、NAは、構成に依存しないACLを保存します。ACLの作成の詳細については、「[ACLの作成](#)」(700 ページ)を参照してください。

## デバイス構成変更の表示

[構成変更] ページでは変更した構成を表示することができます。赤い文字で表示されているデバイスは、最近のタスクに失敗しています。非アクティブなデバイスは、IPアドレスの隣にアイコンが表示されます。

構成変更された個所は別の色で示されているので、2つの構成を簡単に調べて、変更があった場所をただちに特定することができます。誤った構成のデバイスをNAを使用せず手動で特定するには、デバイスに接続して構成を呼び出し、構成に異常がないかを確認する必要があります。

最近実行されたすべての構成変更について、そのリストを表示するには、[デバイス]の下にあるメニューバーの[構成変更]をクリックしてください。[構成変更] ページが開きます。デバイスをクリックすると、そのデバイスの構成情報を表示できます。

特定のデバイスの構成変更を表示するには、次の手順に従います。

1. [デバイス]の下にあるメニューバーの[インベントリ]をクリックします。現在管理されているデバイスのリストがすべて開きます。
2. 構成の変更を表示したいデバイスをクリックします。そのデバイスの[デバイス詳細]ページが開きます。
3. [表示] ドロップダウンメニューから[構成変更]をクリックします。[デバイス構成] ページが開きます。[デバイス構成の詳細] ページの詳細については、「[\[デバイス構成の詳細\] ページのフィールド](#)」(175 ページ)を参照してください。

## [デバイス構成]ページのフィールド

フィールド	説明/アクション
ホスト名	デバイスのホスト名を表示します。デバイスのホスト名をクリックすると[デバイス詳細]ページが開きます。このページでは、デバイスについての詳細な情報を確認できます。
デバイスIP	デバイスのIPアドレスを表示します。デバイスのIPアドレスをクリックすると[デバイス詳細]ページが開きます。このページでは、デバイスについての詳細な情報を確認できます。
最後のスナップショットの試行	デバイスへの最後のアクセス日時を表示します。
最後のスナップショットの結果	たとえば「構成変更の検出」など、最後のスナップショットの結果を表示します。
表示メニュー	詳細については、「 <a href="#">表示メニューオプション</a> 」(201 ページ) を参照してください。
編集メニュー	詳細については、「 <a href="#">編集メニューオプション</a> 」(230 ページ) を参照してください。
プロビジョニングメニュー	詳細については、「 <a href="#">プロビジョニングメニューオプション</a> 」(239 ページ) を参照してください。
接続メニュー	詳細については、「 <a href="#">接続メニューオプション</a> 」(241 ページ) を参照してください。
デバイスに予定された配布	[タスク検索結果]ページが開きます。そのページで、デバイスに予定されている展開の有無を表示できます。
編集された構成	[編集された構成検索結果]ページが開きます。詳細については、「 <a href="#">[構成の検索結果]ページのフィールド</a> 」(497 ページ) を参照してください。
チェックボックス	<p>左側のチェックボックスを使用して、2つのデバイス構成を比較したり、デバイス構成を削除したりできます。デバイスを選択したら、[アクション]ドロップダウンメニューをクリックし、次のいずれかをクリックします。</p> <ul style="list-style-type: none"> <li>• 比較:[<a href="#">デバイス構成の比較</a>]ページが開きます。そのページで、選択した2つの構成を並べて比較できます。差異は、分かりやすいように異なる色で強調表示されます。</li> <li>• 削除: オンにしたデバイス構成を削除します。</li> </ul> <p>横の[選択]ドロップダウンメニューにより、すべてのデバイス構成を選択または選択解除できます。</p>
日付	構成の追加や変更が行われた日時を表示します。
変更者	構成、デバイス、またはタスクを変更した実行者のログイン名を表示します。N/Aは未対応であることを意味します。
コメント	構成についてのコメントを表示します。

フィールド	説明/アクション
アクション	<p>次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>• 前と比較: [デバイス構成の比較] ページが開きます。そのページで、選択した構成とその直前の構成を並べて表示できます。差異は、分かりやすいように異なる色で強調表示されます。</li> <li>• 構成を表示: [デバイス構成の詳細] ページが開きます。そのページでは、構成全体の表示、構成のこのバージョンのデバイスランニング構成への配布、または可能な場合はスタートアップ構成への配布とリブートなどができます。また、構成の編集、構成のテキストバージョンのダウンロード、電子メールによる構成の送信、前回の構成または次回の構成との比較も可能です。詳細については、「<a href="#">[デバイス構成の詳細] ページのフィールド</a>」(175 ページ) を参照してください。</li> <li>• 診断: [診断] ページが開きます。このページには、当該構成の診断情報が表示されます。診断には、基本 IP、デバイス情報、NA デバイスのブートの検出、NA インターフェイス、NA モジュールのステータス、NA OSPF ネイバー、NA ルーティングテーブルがあります。診断の詳細については、「<a href="#">表示メニューオプション</a>」(201 ページ) を参照してください。</li> </ul>

スタートアップとランニング構成が異なる場合は、[デバイス構成] ページの最上部に次のリンクが表示されます。

- スタートアップを表示: [デバイス構成] ページが開きます。そのページで、現在のスタートアップ構成を表示できます。詳細については、「[\[デバイス構成の詳細\] ページのフィールド](#)」(175 ページ) を参照してください。
- スタートアップとランニング構成を比較: [デバイス構成の比較] ページが開きます。そのページで、スタートアップとランニング構成の比較ができます。詳細については、「[\[デバイス構成の比較\] ページのフィールド](#)」(179 ページ) を参照してください。
- 同期化: [タスクの新規作成] - [スタートアップとランニングの同期] ページが開きます。そのページで、スタートアップとランニング構成を同期化できます。詳細については、「[\[スタートアップとランニングの同期\] タスクページのフィールド](#)」(319 ページ) を参照してください。

## [デバイス構成の詳細]ページのフィールド

[デバイス構成の詳細]ページでは次のことができます。

- 特定の構成についての詳細調査
- 構成についてのコメント入力
- この構成のバージョンをデバイスへ展開。たとえば、安定している構成を展開して、デバイスへの誤った変更を取り消すことができます。

**注意：**ナビゲーションを簡単に行うために、構成ファイルのセクションを迅速に解析できるようにするためのリンクが備わっています。このリンクは、構成テキストの直前に配置されます。たとえば、構成ファイル内に[アクセスリスト]セクションがある場合、構成ファイル上で[アクセスリスト]リンクをクリックすると、当該セクションに直接ナビゲートできます。ただし、現時点では、セクション解析をサポートしているのはCisco IOSのジェネリックドライバのみです。

特定のデバイスの[デバイス構成の詳細]ページを表示するには、次の手順に従います。

1. [デバイス詳細]ページにある[表示]ドロップダウンメニューをクリックして、次に[構成変更]をクリックします。[デバイス構成]ページが開きます。
2. [アクション]列の[構成の表示]リンクオプションをクリックします。[デバイス構成の詳細]ページが開きます。

フィールド	説明/アクション
ホスト名	デバイスのホスト名を表示します。デバイスのホスト名をクリックすると[デバイス詳細]ページが開きます。このページでは、デバイスについての詳細な情報を確認できます。
デバイスIP	デバイスのIPアドレスを表示します。デバイスのIPアドレスをクリックすると[デバイス詳細]ページが開きます。このページでは、デバイスについての詳細な情報を確認できます。
最後のスナップショットの試行	デバイスへの最後のアクセス日時を表示します。
最後のスナップショットの結果	たとえば「構成変更の検出」など、最後のスナップショットの結果を表示します。

フィールド	説明/アクション
デバイスを監視	<p>[デバイスを監視]オプションを初めてクリックすると、デバイス監視のイベントルールとともにそのデバイスを含むウォッチグループが作成されます。デバイスに変更があると、デバイスを監視しているユーザに電子メール通知が発行されます。[デバイスを監視]のイベントルールによって、次に示すさまざまなイベントの電子メール通知が送信されます。</p> <ul style="list-style-type: none"> <li>• デバイスアクセスエラー</li> <li>• デバイスがブートしました</li> <li>• デバイス構成の変更</li> <li>• デバイスが削除されました</li> <li>• デバイス診断の変更</li> <li>• デバイスが編集されました</li> <li>• デバイスソフトウェアの変更</li> <li>• ソフトウェアの脆弱性が検出されました</li> </ul> <p><b>注意：</b> [デバイスを監視]のイベントルールを編集してイベントを変更できます。今後監視するすべてのデバイスは、同じイベントルール名を使用します。<a href="#">「[イベント通知とレスポンスルールの新規作成]ページのフィールド」(460ページ)</a>を参照してください。</p> <p>ウォッチグループからデバイスを削除するには、[デバイス監視を停止]をクリックしてください。</p>
表示メニュー	詳細については、 <a href="#">「表示メニューオプション」(201ページ)</a> を参照してください。
編集メニュー	詳細については、 <a href="#">「編集メニューオプション」(230ページ)</a> を参照してください。
プロビジョニングメニュー	詳細については、 <a href="#">「プロビジョニングメニューオプション」(239ページ)</a> を参照してください。
接続メニュー	詳細については、 <a href="#">「接続メニューオプション」(241ページ)</a> を参照してください。
ランニング構成に配布	[タスクの新規作成]-[構成を配布]ページが開きます。そのページで、ランニング構成に構成を配布できます。 <b>(注意：</b> このアクションはすべてのデバイスで利用できるわけではありません <b>)</b> 。詳細については、 <a href="#">「[構成を配布]タスクページのフィールド」(181ページ)</a> を参照してください。
スタートアップ構成に配布してリブート	[タスクの新規作成]-[構成を配布]ページが開きます。そのページで、スタートアップ構成への配布とデバイスのリブートを実行できます(スタートアップとランニング構成は同期化されたままの状態です)。 <b>(注意：</b> このアクションはすべてのデバイスで利用できるわけではありません <b>)</b> 。詳細については、 <a href="#">「[構成を配布]タスクページのフィールド」(181ページ)</a> を参照してください。
バイナリ構成を配布してリブート	バイナリ構成をデバイスに配布してデバイスをリブートします。
テキスト構成を表示	ブラウザの新規ウィンドウにプレーンテキストで構成を表示します。これにより、その構成をクリップボードにコピーして別のアプリケーションに貼り付けることができます。
テキスト構成をダウンロード	構成はテキストフォーマットでダウンロードされるため、他のシステムにコピーできます。
バイナリ構成をダウンロード	構成はバイナリフォーマットでダウンロードされるため、他のシステムにコピーできます。
テキスト構成を電子メール送信	構成を電子メールで送信できます。



フィールド	説明/アクション
前と比較	[デバイス構成の比較]ページが開きます。そのページで、古い構成と新しい構成を並べて表示できます。差異は、分かりやすいように異なる色で強調表示されます。 <b>注意</b> ：これが最初の構成の場合、「これは最初の構成です」と表示されます。これが最後の構成の場合、「これは現在の構成です」と表示されます。
変更者	スナップショットをトリガした変更の所有者のログイン名、およびユーザの詳細を表示するための[詳細]リンクを表示します。
作成日	構成の変更をキャプチャしたスナップショットの日付と時刻を表示します。
<カスタムフィールド>	デバイスのスナップショットと診断用に定義された、カスタムフィールドを表示します。
構成コメント	現在の構成と、別の構成（特に以前の構成）を区別するためのコメントを入力します。[コメントの編集]をクリックします。[コメントの編集]オプションを使用して、構成のカスタムフィールドやコメントを編集できます。デバイス構成データの編集の詳細については、「 <a href="#">デバイス構成データの編集</a> 」(178ページ)を参照してください。
行/構成テキスト	構成ファイルを表示します。

## デバイス構成データの編集

[編集]メニューから[インライン構成コメントを編集]をクリックして、構成コメントの追加や編集を行えます。カスタムデータの追加の詳細については、「[\[カスタムデータの設定\]ページのフィールド](#)」(554ページ)を参照してください。

インラインコメントを編集する場合は、次のことに注意してください。

- 構成内の行に変更があるたびに、その行のコメントが削除されます。コマンドの変更後にコメントが有効のままであるかNAは判断できません。そのため、たとえばホスト名を変更する場合には、NAはホスト名コマンドの上にあるコメントの削除も同時に行います。
- 空白行を追加または削除する場合には注意が必要です。デバイスによっては空白行が意味を持つことがあるので、NAでは空白行の追加や削除を構成変更として取り扱います。なお、空白のコメント行は追加できません。コメント行とは2文字のコメント文字から始まる行のことで、通常は、「!!」または「##」を使用します。
- インラインコメントは構成ファイルと同じようにバージョン管理されているわけではありません。コメントブロックは、構成内の次のコマンドに適用されます。展開しても次のコマンド行に影響を与えない場合には、コメントは変更されません。(新規設定に上書きするために)過去の構成を展開する場合には、展開した構成に新規構成のコメントを適用することができます。ただし、コメントが誤った位置に置かれる場合もあります。
- 重要な編集が必要なファイルのコメントを失いたくない場合には、コメントが書かれている構成ファイルをコピーして保存することをお勧めします。この作業をすることで、必要なときにコメントを回復できます。

## デバイス構成の比較

[デバイス構成の比較]ページでは、同じデバイスの2つの構成を並べて表示します。追加、削除、変更については、左側に行番号がある2つの列内で強調表示されています。固有のIPアドレスと、構成のスナップショットを取得した日時を使用して、それぞれの構成を特定します。

異なるデバイスの2つの構成を比較するには、次の手順に従います。

1. [デバイス]メニューで、[構成変更]をクリックします。[構成変更]ページが開きます。
2. 左側のチェックボックスを使用して、2つのデバイスのいずれかをクリックします。
3. [アクション]ドロップダウンメニューの[比較]をクリックします。[デバイス構成の比較]ページが開きます。

## [デバイス構成の比較]ページのフィールド

フィールド	説明/アクション
行の変更	変更された行の番号を薄紫色で強調表示します。
行の挿入	挿入された行の番号を薄緑色で強調表示します。
行の削除	削除された行の番号を薄い黄色で強調表示します。
コンテキストとの 差異の表示	選択されている場合（デフォルト）には、変更された行とその前後3行のみが表示されます。
全文表示	オンになっている場合には、構成ファイル全体を表示します。
UNIX diff形式の表示	オンになっている場合には、UNIX diff形式で構成ファイルが表示されます。
ランニング構成に配布	[構成を配布]ページが開きます。そのページで、デバイスのランニング構成へこの構成を配布できます。（ <b>注意</b> ：このアクションはすべてのデバイスで利用できるわけではありません）。
スタートアップ構成に 展開してリブート	[構成を配布]ページが開きます。そのページで、スタートアップ構成への配布とデバイスのリブートを実行できます（スタートアップとランニング構成は同期化されたままの状態です）。（ <b>注意</b> ：このアクションはすべてのデバイスで利用できるわけではありません）。
構成 #1/構成 #2	[構成 #1]または[構成 #2]のリンクをクリックすると、[デバイス構成の詳細]ページが開きます。詳細については、「 <a href="#">[デバイス構成の詳細]ページのフィールド</a> 」（175ページ）を参照してください。 <b>注意</b> ：これが最初の構成の場合、「これは最初の構成です」と表示されます。これが最後の構成の場合、「これは現在の構成です」と表示されます。
デバイス	デバイスのホスト名とIPアドレスを表示します。デバイスのホスト名とIPアドレスをクリックすると、[デバイス詳細]ページが開きます。そのページで、デバイスの情報や構成履歴を表示できます。
日付	構成の変更をキャプチャしたスナップショットの日付と時刻を表示します。

## デバイス構成の展開

構成を展開するには、次の2つの方法があります。

- ランニング構成：配布時には、デバイスをリブートするまで構成ファイルがそのまま使用されます。デバイスをリブートすると、スタートアップ構成がランニング構成を上書きすることがあります。
- スタートアップ構成：配布時にデバイスがリブートされ、新規構成がランニングとスタートアップ構成になります。

構成を展開するには、次の手順に従います。

1. [デバイス]メニューで、[構成変更]をクリックします。[構成変更]ページが開きます。
2. デバイスの[アクション]列にある[構成を表示]をクリックします。[デバイス構成の詳細]ページが開きます。次のオプションのいずれかを選択します（該当する場合）。
  - ー ランニング構成に配布：[タスクの新規作成]-[構成を配布]ページが開きます。そのページで、デバイスのランニング構成へ構成を配布できます。
  - ー スタートアップ構成に配布してリブート：[タスクの新規作成]-[構成の配布]ページが開きます。そのページで、スタートアップ構成への配布とデバイスのリブートを実行できます（スタートアップとランニング構成は同期化されたままの状態です）。

## [構成を配布]タスクページのフィールド

フィールド	説明/アクション
タスク名	[構成を配布]を表示します。必要に応じて別のタスク名を入力できます。
適用先	デバイスのホスト名とIPアドレスを表示します。
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
優先度	タスクの優先度を表示します。タスクの優先度レベルは1～5であり、1が最も高いタスク優先度レベルです。詳細については、「 <a href="#">タスクの予定</a> 」(278 ページ) を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
セッションログ	完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。セッションのログ記録を有効にすると、デバイスと対話するほとんどのデバイスを実行できます。タスク実行中のデバイスとの対話に関する詳細なログが記録されます。デバイス固有の問題をデバッグする場合、最初にセッションログを表示する必要があります。セッションログでは、CLI、SNMP およびタスクで実行されるすべての転送プロトコルアクションの詳細がわかります。(注意：大量のデータが格納されることがあります。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」(96 ページ) を参照してください)。
強制的に保存	デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみに適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。 <ul style="list-style-type: none"> <li>• このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>• NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>(注意：この設定はNA 9.20 で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます。)</p>
チェックボックス	[デバイスに適用されるすべてのポリシーに変更が準備していることを検証します。]オプションは、デフォルトではオンになっています。タスクの種類によっては、「ランニング構成に配布」または「スタートアップ構成に配布してリブート」も選択できます。
構成	構成を表示します。
推定継続時間	このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。

フィールド	説明/アクション
-------	----------

**デバイス資格情報のオプション**

デバイス資格情報のオプションは、[システム管理設定]の[サーバ]ページで設定する、[標準のデバイスの資格情報を許可]、[タスクごとのデバイスの資格情報を許可]、または[ユーザのAAA資格情報を許可]オプションに応じて表示されます。[タスクごとのデバイスの資格情報を許可]を有効にすると、適切なパスワード情報を入力するよう求めるプロンプトが表示されます。また、複数のデバイス資格情報オプションを有効にすると、タスクを実行するときにオプションを選択するよう求めるプロンプトが表示されます。デバイス資格情報オプションを1つだけ有効にした場合は自動的にオプションが使用され、プロンプトは表示されません（デバイス資格情報の有効化の詳細については、[「\[サーバ\]ページのフィールド」\(52ページ\)](#)を参照してください）。

デバイス資格情報 [システム管理設定]の[サーバ]ページで有効にされるデバイス資格情報オプションに応じて、次のオプションを1つ以上選択できます。

- 標準デバイス固有の資格情報とネットワーク全体のパスワードルールの使用（デフォルト）。
- タスク固有の資格情報を使用。[ユーザ名]、[パスワード]、[パスワードの確認]、[イネーブルパスワード]、[イネーブルパスワードの確認]、[SNMP読み取り専用コミュニティ文字列]、および[SNMP読み取り/書き込みコミュニティ文字列]への入力を求めるプロンプトが表示されます。
- タスク所有者のAAA資格情報の使用。タスク所有者には、定義された有効なAAA資格情報が必要です。（**注意**：標準パスワードルールとデバイス固有パスワードを使用します。ただし、タスク所有者のAAAユーザ名とパスワードが適用されます。）

**タスク前/タスク後スナップショットオプション**

スナップショットのオプションは、[システム管理設定]の下の[構成管理]ページでユーザによる無効化がシステムで有効に構成されている場合にのみ表示されます（詳細については、[「\[構成管理\]ページのフィールド」\(36ページ\)](#)を参照してください）。

タスク前スナップショット 次のオプションのいずれかを選択します。

- なし（デフォルト）
- タスクの一部として

タスク後スナップショット 次のオプションのいずれかを選択します。

- なし
- タスクの一部として（デフォルト）
- 個別のタスクとしてスケジュール

**承認オプション**

承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。

承認要求 タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。

承認の無効化 タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。

ドラフトとして保存 オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。

フィールド	説明/アクション
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift] キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96 ページ)</b> を参照してください。</p>

終了時に、必ず[タスクを保存]をクリックしてください。





## 第5章：デバイスの表示

### トピックの参照先リスト

トピック	参照先：
デバイスの表示	<a href="#">「デバイスの表示」</a> （186ページ）
デバイスグループの表示	<a href="#">「デバイスグループの表示」</a> （188ページ）
デバイスの予約	<a href="#">「デバイスの予約」</a> （190ページ）
デバイス詳細の表示	<a href="#">「デバイス詳細の表示」</a> （193ページ）
NA/SA統合	<a href="#">「NA/SA統合」</a> （196ページ）
表示メニューオプション	<a href="#">「表示メニューオプション」</a> （201ページ）
仮想ローカルエリアネットワーク（VLAN）	<a href="#">「仮想ローカルエリアネットワーク（VLAN）」</a> （213ページ）
編集メニューオプション	<a href="#">「編集メニューオプション」</a> （230ページ）
プロビジョニングメニューオプション	<a href="#">「プロビジョニングメニューオプション」</a> （239ページ）
接続メニューオプション	<a href="#">「接続メニューオプション」</a> （241ページ）

## デバイスの表示

管理しているデバイスのリストを表示するには、[デバイス]の下にあるメニューバーの[インベントリ]をクリックします。インベントリとはデフォルトのワーキンググループです。インベントリには現在管理しているすべてのデバイスがリストされています。新しいデバイスを追加する方法の詳細については、「[デバイスの追加](#)」(106ページ)を参照してください。

### [インベントリ]ページのフィールド

フィールド	説明/アクション
グループ	[デバイスグループ]ページが開きます。現在のデバイスグループのリストが表示されます。詳細については、「 <a href="#">デバイスグループの表示</a> 」(188ページ)を参照してください。
デバイスの新規作成	[デバイスの新規作成]ページが開きます。このページで、新しいデバイスを追加できます。詳細については、「 <a href="#">デバイスの追加</a> 」(106ページ)を参照してください。
デバイスグループの新規作成	[デバイスグループの新規作成]ページが開きます。このページで、新しいデバイスグループを追加できます。詳細については、「 <a href="#">デバイスグループの追加</a> 」(136ページ)を参照してください。
親グループの新規作成	[親グループの新規作成]ページが開きます。このページで、新しい親グループを追加できます。詳細については、「 <a href="#">親グループの追加</a> 」(138ページ)を参照してください。
現在の作業グループ	デフォルトグループである[インベントリ]を表示します。該当する場合は、ドロップダウンメニューから別のグループを選択できます。
[アクティブなデバイスのみをリスト表示]チェックボックス	インベントリリストにアクティブなデバイスのみを含める場合は、このチェックボックスをオンにしてください。非アクティブなデバイスは、アクティブには管理されていません。
このグループでタスクを実行	ドロップダウンメニューからタスクを選択して、このグループを実行できます。タスクの実行の詳細については、「 <a href="#">タスクとは</a> 」(277ページ)を参照してください。
グループの説明	システムが認識しているすべてのデバイスの一覧です。
チェックボックス	<p>左側のチェックボックスをオンにすると、デバイスを管理できます。デバイスを選択して、[アクション]ドロップダウンメニューをクリックしてください。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• アクティブ化：選択したデバイスを管理するようにNAに指示します。</li> <li>• 非アクティブ化：選択したデバイスを管理しないようにNAに指示します。</li> <li>• 一括編集：[デバイスを一括編集]ページが開きます。そのページでは、選択したすべてのデバイスに対して、一度にドライバを割り当てて接続方法を設定できます。詳細については、「<a href="#">[デバイスを一括編集]ページのフィールド</a>」(161ページ)を参照してください。</li> <li>• ダイアグラム：[ダイアグラム]ページが開きます。「<a href="#">ダイアグラム</a>」(603ページ)を参照してください。</li> <li>• 削除：選択したデバイスが削除されます。</li> <li>• オンにしたデバイスに対して実行するタスクを選択。詳細については、「<a href="#">アドホックデバイスグループへのタスクの実行</a>」(277ページ)を参照してください。</li> </ul> <p>左側にある[選択]ドロップダウンメニューを使用すると、デバイスを全選択または全選択解除できます。</p>
ホスト名	デバイスのホスト名が表示されます。赤で表示されるデバイスは、最後のスナップショットの取得に失敗しています。非アクティブなデバイスは、IPアドレスの横のアイコンでマーキングされています。[ホスト名]リンクをクリックすると、[デバイス詳細]ページが開きます。そのページで、デバイスの基本情報や構成履歴を表示できます。[デバイス詳細]ページについては、「 <a href="#">表示メニューオプション</a> 」(201ページ)を参照してください。

フィールド	説明/アクション
デバイスIP	デバイスのIPアドレスを表示します。[デバイスIP]リンクをクリックすると、[デバイス詳細]ページが開きます。そのページで、デバイスの基本情報や構成履歴を表示できます。[デバイス詳細]ページについては、「 <a href="#">表示メニューオプション</a> 」(201 ページ) を参照してください。
デバイスのベンダー	デバイスのメーカー名を表示します。
デバイスモデル	デバイスモデル名を表示します。
パーティション	デバイスが属すパーティションを表示します。(注意: このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。)
アクション	<p>各デバイスに対して次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>編集: [デバイスを編集]ページが開きます。そのページでデバイスの情報を編集できます。「<a href="#">[デバイスの編集]ページのフィールド</a>」(111 ページ) を参照してください。</li> <li>Telnet: [Telnet]ウィンドウが開きます。</li> <li>SSH: [SSH]ウィンドウを開きます。</li> <li>構成を表示: [現在の構成]ページが開きます。このページでは、最新の構成の表示、ランニング構成への配布、コメントの追加ができます。</li> </ul>
1ページに表示する結果の数	ドロップダウンメニューから、ページあたりの表示項目数を設定できます。デフォルトは25です。

## デバイスグループの表示

デバイスグループとは、組織にとってわかりやすいようにデバイスを分類する方法の1つです。その例を示します。

- 実在の場所
- 事業単位/部門
- ネットワークアーキテクチャ内での役割
- アクティブ化ステータス

デバイスグループを作成すると、デバイスグループを使用して、検索、ルールの認証、パスワード更新など、さまざまな機能を管理できます。デバイスグループの追加の詳細については、「[デバイスグループの追加](#)」(136ページ)を参照してください。

[デバイスグループ]ページには、初期設定でインベントリグループというシステムグループが含まれています。インベントリグループには、すべてのデバイスが含まれます。ただし、ユーザ定義のグループを作成すると、そのグループもこのページに表示されます。

デバイスグループのリストを表示するには、[デバイス]メニューの[グループ]をクリックします。[デバイスグループ]ページが表示されます。[公開]デバイスグループは、すべてのユーザに表示されます。[専用]デバイスグループは、所有者とNA管理者にのみ表示されます。

## [デバイスグループ]ページのフィールド

フィールド	説明/アクション
[グループの新規作成]リンク	[グループの新規作成]ページが開きます。このページで、新しいデバイスグループを作成できます。新規グループの作成の詳細については、「 <a href="#">デバイスグループの追加</a> 」(136ページ)を参照してください。
親グループの新規作成	[親グループの新規作成]ページが開きます。このページで、新しい親グループを追加できます。詳細については、「 <a href="#">親グループの追加</a> 」(138ページ)を参照してください。
グループ名	デバイスグループのユーザ定義名が表示されます。親グループは、他の親グループの子グループになっていない場合はインデント表示されません。親グループに属するグループは、親グループの下にインデント表示されます。グループ名をクリックすると、[デバイスグループ]ページが開きます。このページでは、デバイスグループに関する詳細情報を表示できます。詳細については、「 <a href="#">[デバイスグループ]ページのフィールド</a> 」(188ページ)を参照してください。(注意：雲アイコンが前にあるグループ名はパーティションに含まれています。パーティションの詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」(148ページ)を参照してください)。
説明	グループの簡単な説明を表示します。
デバイス数	グループ内のデバイス数が表示されます。
所有者	デバイスグループを作成したユーザ名が表示されます。
共有	デバイスグループが公開か専用のどちらであるかを表示します。公開デバイスグループは、すべてのユーザが見ることができます。専用デバイスグループは、所有者とシステム管理者のみが見ることができます。

フィールド	説明/アクション
アクション	<p>[グループ名]を選択するまで、[インベントリ]グループの[アクション]フィールドは空です。ユーザ定義のデバイスグループでは次のアクションを表示します。</p> <ul style="list-style-type: none"><li>• 表示：選択したデバイスグループに入っているデバイスを表示します。デバイスはこのデバイスグループの直接の子（リーフデバイスグループの場合）か、子グループの子（親デバイスグループの場合）です。[表示]オプションの詳細については、「<a href="#">[デバイスグループ]ページのフィールド</a>」（145ページ）を参照してください。</li><li>• 編集：[グループを編集]ページが開きます。そのページで、デバイスグループの情報を編集できます。</li><li>• 削除：デバイスグループを削除できます。</li><li>• ダイアグラム：ダイアグラムにより、ネットワークデバイスからトポロジーデータを収集できます。詳細については、「<a href="#">ダイアグラム</a>」（603ページ）を参照してください。</li><li>• 専用に変更/公開に変更：デバイスグループを公開にするか専用にするかを指定できます。公開デバイスグループは、すべてのユーザが見ることができます。専用デバイスグループは、所有者とシステム管理者にのみ、表示されます。</li></ul>

## デバイスの予約

大規模なネットワークを持つ組織では、誰がどのデバイスでいつ作業しているかを管理することが重要です。[デバイス予約システム]では、デバイスやデバイスグループを一定期間、予約することができます。[デバイス予約]が競合しているという通知を受け取ることで、誤ってメンテナンス中のデバイスで作業することを回避できます。大規模なITグループの場合でも、管理され、組織された方法でネットワーク上でのスケジューリングや作業が行えます。([デバイス予約システム]および[アクティビティカレンダー]の構成の詳細については、「[ワークフロー](#)」(59ページ)を参照してください)。

マルチタスクプロジェクトのサブタスクによる影響があるデバイスやデバイスグループは、タスクの継続期間について自動予約されます。また、マルチタスクプロジェクトが承認されており、1つ以上の予定されたタスクに次のリードライトタスク（以下に一覧）が含まれている場合は、現在予約されているデバイスにリードライトタスクが影響を与えるかどうかを確認します。影響がある場合は、デバイス予約の競合イベントが作成されます。ただし、デバイス予約の競合は、デバイスやデバイスグループに対するタスクの実行を回避できません。

リードライトタスクには以下が含まれます。

- 構成の配布
- コマンドスクリプトの実行
- パスワードの配布
- デバイスのリブート
- スタートアップとランニングの同期
- デバイスソフトウェアの更新

マルチタスクプロジェクトでデバイスやデバイスグループを予約する場合は、いずれかのデバイスでデバイス構成変更が検出されるとユーザに通知します。

マルチタスクプロジェクトの設定の詳細については、「[マルチタスクプロジェクトの予定](#)」(391ページ)を参照してください。

## アクティビティカレンダー

アクティビティカレンダーを使用して、ネットワーク上で発生するアクティビティを表示できます。また、ある日付にスケジュールリングされているタスクおよびデバイス予約のリストを見ることができます。リストの内容は次のとおりです。

- 表示されている日に実行予定になっているすべてのタスク
- タスクの開始日時
- タスクの継続期間
- タスクを実行する予約デバイスや予約デバイスグループ
- 解除されていない「デバイス予約の競合」イベントがタスクにあるか

タスクブロックはすべて、1時間刻みまたは30分刻みで開始および終了します。そのため、タスクが×時22分に開始する場合は、×時を示す列の中にタスクが表示されます。

左側のカレンダーは今月を表示します。右側のカレンダーは翌月を表示します。選択された日付は、該当するカレンダーで強調表示されます。カレンダーに記載された日付をクリックすると、特定の日付を選択できます。ページが再表示され、該当日のイベントが示されます。

右ペインにあるカレンダーの下に、[タスクの詳細]が表示されます。そこでは、次のタスク情報が得られます。

- 開始時刻
- 継続時間
- イベントをスケジュールリングしたユーザの名前
- イベントステータス（保留、実行中、成功など）

アクティビティカレンダーを表示するには、[タスク]の下にあるメニューバーの[アクティビティカレンダー]をクリックしてください。[アクティビティカレンダー]が開きます。次の図は、[アクティビティカレンダー]の例を示します。

**アクティビティカレンダー**

お気に入り◆ 追加
ヘルプ?

Aug-14-09

3 個の合計タスク / 予約

取得

スナップ

ショット

配布

パスワード

2009年8月

? < > 今日 > >

週	日	月	火	水	木	金	土
30	31	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31

日付を選択

2009年9月

? < > 今日 > >

週	日	月	火	水	木	金	土
35	36	6	7	8	9	10	11
12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27
28	29	30					

日付を選択

タスク

スナップショットの取得

開始時間: Aug-03-09 10:45:05

継続時間: 7 時間

スケジュール作成者: Tad

ステータス: 保留

lab-1000.w1

lab-6000-sw

2 デバイスまたはグループがリスト表示されました。  
[デバイス / グループリストの変更](#)

セルに表示されているリンクをクリックすると、[タスク]パネルの情報が更新されます。マルチタスクプロジェクトに解除されていないデバイス予約の競合がある場合は、セルは黄色で強調表示されます。マルチタスクプロジェクトの構成の詳細については、「[マルチタスクプロジェクトの予定](#)」(391 ページ) を参照してください。



## デバイス詳細の表示

[デバイス詳細]ページでは、デバイス固有のタスクを実行できます。[デバイス詳細]ページを表示するには、次の手順に従います。

1. [デバイス]メニューで、[インベントリ]をクリックします。
2. [インベントリ]ページでデバイスをクリックします。そのデバイスの[デバイス詳細]ページが開きます（検索機能を使用して、ほかのほとんどのページから[デバイス詳細]ページを表示できます）。

## [デバイス詳細]ページのフィールド

フィールド	説明/アクション
ホスト名	デバイスのホスト名を表示します。デバイスのホスト名をクリックすると[デバイス詳細]ページが開きます。このページでは、デバイスについての詳細な情報を確認できます。
デバイスIP	デバイスのIPアドレスを表示します。デバイスのIPアドレスをクリックすると[デバイス詳細]ページが開きます。このページでは、デバイスについての詳細な情報を確認できます。
最後のスナップショットの試行	NA経由で、デバイスの構成のスナップショットのために最後にデバイスにアクセスした日時を表示します。
最後のスナップショットの結果	このデバイス構成の最後のスナップショットのステータスを表示します。スナップショットに失敗した場合は、[タスク結果]ページへのリンクがあります。
情報	<p>利用できる場合、詳細情報へのリンクと併せて、デバイスに関する情報が表示されます。たとえば、デバイスが1つまたは複数のポリシーに非準拠である場合、[ポリシーイベント]リンクをクリックすると、[ポリシーアクティビティ]ページが開きます。スタートアップとランニング構成に差異が存在する場合、以下のリンクが表示されます。</p> <ul style="list-style-type: none"> <li>• スタートアップを表示 : [デバイス構成]ページが開きます。</li> <li>• スタートアップとランニング構成を比較 : [デバイス構成の比較]ページが開きます。</li> <li>• 同期 : [タスクの新規作成 - スタートアップとランニングの同期]ページが開きます。</li> </ul>

フィールド	説明/アクション
[デバイスを監視]リンク	<p>[デバイスを監視]オプションを初めてクリックすると、デバイス監視のイベントルールとともにそのデバイスを含むウォッチグループが作成されます。デバイスに変更があると、デバイスを監視しているユーザに電子メール通知が発行されます。[デバイスを監視]のイベントルールによって、次に示すさまざまなイベントの電子メール通知が送信されます。</p> <ul style="list-style-type: none"> <li>• デバイスアクセスエラー</li> <li>• デバイスがブートしました</li> <li>• デバイス構成の変更</li> <li>• デバイスが削除されました</li> <li>• デバイス診断が変化しました</li> <li>• デバイスが編集されました</li> <li>• デバイスソフトウェアの変更</li> <li>• ソフトウェアの脆弱性が検出されました</li> </ul> <p><b>注意：</b> [デバイスを監視]のイベントルールを編集してイベントを変更できます。今後監視するすべてのデバイスは、同じイベントルール名を使用します。「<a href="#">[イベント通知とレスポンスルールの新規作成]ページのフィールド</a>」(460 ページ) を参照してください。</p> <p>ウォッチグループからデバイスを削除するには、[デバイスを監視を停止]をクリックしてください。</p>
表示メニュー	[表示]メニューが開きます。詳細については、「 <a href="#">表示メニューオプション</a> 」(201 ページ) を参照してください。
編集メニュー	[編集]メニューが開きます。詳細については、「 <a href="#">編集メニューオプション</a> 」(230 ページ) を参照してください。
プロビジョニングメニュー	[プロビジョニング]メニューが開きます。詳細については、「 <a href="#">プロビジョニングメニューオプション</a> 」(239 ページ) を参照してください。
接続メニュー	[接続]メニューが開きます。詳細については、「 <a href="#">接続メニューオプション</a> 」(241 ページ) を参照してください。
デバイスの説明	該当する場合は、ユーザ定義したデバイスの説明を表示します。
FQDN	該当する場合は、FQDN情報を表示します。
サービスタイプ	サービスタイプは、VoIP、BGP、MPLSなどを指定できます。この値により、デバイスの用途を判断できます。これらの値を使用してデバイスサービスにタグ付けすることで、デバイスサービスを容易に検索したり、グループ内のデバイスグループを表示できます（静的または動的）。 <b>注意：</b> システム管理設定経由で、[デバイスアクセス]の配下にカスタムサービスタイプを作成できます。「 <a href="#">[構成管理]ページのフィールド</a> 」(36 ページ) を参照してください。デバイスを編集して、これらの値を設定することもできます。
コメント	該当する場合は、コメントを表示します。
ベンダー	NortelやCiscoなど、デバイスのベンダーを表示します。
モデル	メーカーのモデル番号を表示します。
ソフトウェアバージョン	デバイスで実行されているオペレーティングシステムソフトウェアのバージョンを表示します。
ドライバ名	デバイスに割り当てられているドライバを表示します。
デバイスタイプ	ルータ、スイッチ、ファイアウォールなど、デバイスのタイプを表示します。
シリアル番号	デバイスのメーカーのシリアル番号を表示します。

フィールド	説明/アクション
資産タグ	デバイスの企業資産タグ番号を表示します。
システムメモリ	デバイスのシステムメモリを表示します。
場所	通常、場所は構成ファイルで取得されます。
デバイスのインポート元	デバイスがNAにインポートされており、インポートソースに名前が付けられている場合は、その名前を表示します。インポートソースに名前が付けられていない場合は、「<日付>に追加」と表示されます。デバイスが手動で追加された場合は、「<日付>に、<user name>が手動で追加」と表示されます。
最後に成功したスナップショット	最後のスナップショットが成功した日時を表示します。
最終構成変更	デバイスの構成を最後に変更した日付と時刻が表示されます。
最終アクセス試行	デバイスへのアクセスが試行された日時を表示します。
最終成功アクセス	デバイスへのアクセスが最後に成功した日時を表示します。
変更の検出とポーリング	次のいずれかを表示します。 <ul style="list-style-type: none"> <li>有効：NAがデバイスに定期的にポーリングして、保存されている構成をデバイスの実際の構成と比較して検証します。</li> <li>無効：NAがデバイスに対して定期的なポーリングやその他の管理をしません。</li> </ul>
管理ステータス	次のいずれかを表示します。 <ul style="list-style-type: none"> <li>アクティブ：NAはデバイスの構成変更を記録します。</li> <li>非アクティブ：NAは変更を記録しません。また、NAを使ってデバイスの変更はできません。</li> </ul>
パスワードルール	パスワードルール情報を表示します。
VTP ドメイン	該当する場合は、VLAN トランッキングプロトコル（VTP）ドメイン名を表示します。
VTP 動作モード	該当する場合は、VLAN トランッキングプロトコル（VTP）動作モードを表示します。
チケット番号	該当する場合はチケット番号を表示します。NA コネクタの1つをインストールしている場合は、[チケットの更新]ボタンをクリックしてチケットを更新できます。

## NA/SA 統合

IT 環境の変更を行うときには、ネットワーク管理者とシステム管理者間の協力が必要です。異なるオペレーティングシステムが稼働している複数のサーバがある場合や、ファイアウォール、ロードバランサ、スイッチ、ルータなどを含むネットワークデバイスが存在する場合があります。たとえば、ロードバランサやファイアウォールなど、実際にアプリケーションの一部であるネットワークデバイスへの変更が必要な環境もあります。

HP Network Automation (NA) を HP Server Automation (SA) と統合することで可能なことを次に示します。

- SA サーバと NA ネットワークデバイス間のレイヤ1 接続の表示。NA は配線位置を推測するだけです。NA では発見的方法を（できるだけ）使用して、デバイスやサーバ間の物理接続を決定します。SA の詳細については、『HP Server Automation User's Guide』を参照してください。
- SA サーバと NA ネットワークデバイス間のレイヤ2 接続の表示。NA では、デバイスとサーバのすべてまたはいずれかの間のデータリンク接続数を減らすことにより、ネットワークダイアグラムを見やすくしています。この場合は、推移する接続から推測可能な接続のみが除かれます。詳細については、「[ダイアグラム](#)」(603 ページ) を参照してください。
- 指定された NA ネットワークデバイスが認識している SA サーバの情報表示。また、それとは逆に、指定された SA サーバを認識するネットワークデバイスの情報表示。

NA/SA 統合を設定するには、[HPNA トポロジーデータ収集] 診断を実行する必要があります。この診断により、NA はすべてのスイッチの MAC アドレスを収集するように指示されます。MAC アドレスは、レイヤ2 接続やレイヤ1 接続を検出および追加するために必要です。

レイヤ2 接続 (ARP テーブル) からレイヤ1 接続 (配線) を推測する場合もあります。これにより、通信モードおよび速度設定などの構成の不一致を検出できます。

- NA/SA 統合の構成の詳細については、「[ユーザ認証](#)」(73 ページ) を参照してください。
- ネットワークダイアグラムの作成についての詳細については、「[ダイアグラム](#)」(603 ページ) を参照してください。
- 通信モードおよび速度設定などを含む、インターフェイスの詳細の表示については、「[\[インターフェイスの詳細\] ページのフィールド](#)」(206 ページ) を参照してください。
- SA サーバの表示についての詳細については、「[\[サーバ\] ページのフィールド](#)」(222 ページ) を参照してください。

## NA/SA 権限

NA と SA を統合する場合は、両システムへのログインに同一のユーザ名とパスワードを使用します。ただし、そのユーザが SA と NA の両システムで SA サーバを表示できるかどうかは、ユーザの SA 権限によって管理されます。同様に、そのユーザが NA と SA の両システムでネットワークデバイスを表示できるかどうかは、NA ユーザの権限によって管理されます。

NA の構成では、SA のユーザ名とパスワードを指定できます。詳細については、「[\[ユーザ認証\] ページのフィールド](#)」(77 ページ) を参照してください。NA が [トポロジー収集診断] を通じて MAC アドレスを読み込んだ場合に、NA によって SA サーバを検出することについては、SA ユーザ権限で管理します。ユーザは権限のある SA サーバのみを表示できるため、すべての SA サーバを表示できる SA ユーザを指定することをお勧めします。これにより、既知の SA サーバはすべて、NA 内の適切な MAC アドレスにマッピングされます。

例：

- サーバ1のMACアドレスは、0060839488A1とします。
- SAユーザAは、サーバ1を表示できます。
- SAユーザBは、サーバ1を表示できません。
- スイッチS7はサーバ1と接続しています。

NAがSAユーザAをTwistサーバのユーザ名として使用する構成では、NAは[トポロジー収集診断]の実行時に、サーバ1に0060839488A1をマッピングします。SAユーザAがNAにログインする場合は、スイッチS7の[サーバ]ページに（[デバイス詳細]ページから）、サーバ1を表示することができます。SAユーザBがNAにログインする場合は、サーバ1を表示する権限を持っていないので、[サーバ]ページにサーバ1を表示することはできません。

## デバイスハードウェア情報

管理しているSAサーバとNAネットワークデバイスの基本ハードウェア詳細に加えて、NA/SA統合では、ネットワークインターフェイスについて次の情報もレポートします。

- サーバ側では、ネットワークインターフェイスはイーサネットインターフェイス、MACアドレス、接続デバイス、VLAN名、通信モードおよび速度設定などを特定します。
- ネットワークデバイス側では、ネットワークインターフェイスはイーサネットポート、速度および通信モード設定、接続デバイスを特定します。自動ネゴシエートモードをNAのネットワークインターフェイスに設定し、SAのネットワークカードにネゴシエートします。通信モードを[全二重（自動）]に、速度を[100（自動）]に指定するポリシーなど、この構成を定義するポリシーを作成できます。

詳細については、「[\[デバイスインターフェイス\]ページのフィールド](#)」（205ページ）を参照してください。

## ファイアウォールを介したNAへの接続

NA Application Program Interface（API）では、Java Remote Method Invocation（Java RMI）を使用して、NAサーバへ接続します。Java RMIはさまざまなプロトコルで実行することができます。NAはJava RemotingでのみJava RMIをサポートしています。SAとNAを統合するときには、SAでNA APIを使用します。そのため、Java RMIとJboss Remotingは次のポートを使用します。

- Java Naming and Directory Interface（JNDI）（通常はポート1099）
- RMI（通常はダイナミック1098）
- RMIオブジェクト（通常はポート4446）

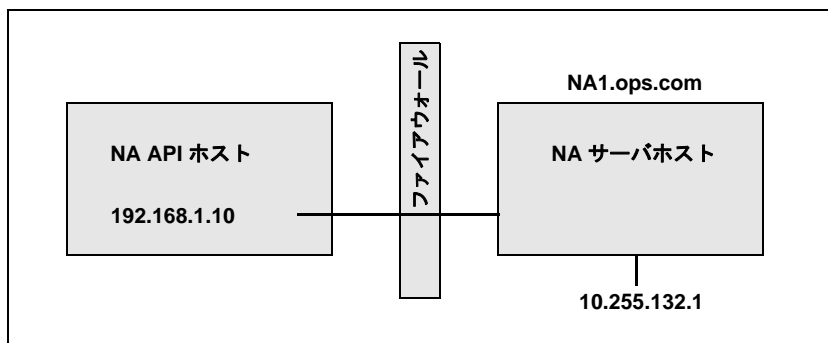
ファイアウォールを介してNA Java APIを使用するには、次の手順に従います。

1. ファイアウォール経由でポートを開きます。
  - Java Naming and Directory Interface（JNDI）（通常はポート1099）
  - RMI（通常はダイナミック1098）
  - RMIオブジェクト（通常はポート4446）

2. 次のいずれかの手順を実行します。
  - － NA アプリケーションサーバホストがファイアウォールの両側で同一の IP アドレスを持っている場合、構成は完了です。
  - － NA アプリケーションサーバホストがファイアウォールの外側で別のアドレスを持っている場合は、手順手順 3に進みます。
3. NAがRMIサーバのホスト名（IPアドレスではなく）を使用するように、次のファイルを作成します。
  - － Windows :  
`<NA_HOME>\server\ext\jboss\server\default\conf\jnp.properties`
  - － UNIX :  
`<NA_HOME>/server/ext/jboss/server/default/conf/jnp.properties`
 このファイルに次の行を含めます。
 

```
java.rmi.server.useLocalHostname=true
```
4. ファイルを保存してNAサーバを再起動します。
5. NAサーバホストおよびNA APIホスト（SAとNAを統合するときのSAサーバホスト）上で、ホスト名解決が正しいことを確認します。

次の例では、IPアドレスが10.255.132.1でNA1.ops.comという名前のホスト上で、NAが稼動しています。ファイアウォールの外側では、NA1.ops.comにアクセスするために192.168.1.10を使用します。NAサーバホスト（10.255.132.1）は、NA1.ops.comに適切に解決する必要があります。NA APIホスト上では、NA1.ops.comが10.255.132.1に適切に解決する必要があります。



高レベルでは、Java RMI/Jboss Remotingは次のように機能します。

1. クライアントは、ホスト10.255.132.1のJNDIポート（1099）に接続します。
2. クライアントのクエリ：bean Connectはどこにあるか。
3. サーバの応答：ホストna1.ops.comのポート1098。
4. クライアントは、nas1.ops.comのIPアドレスを検索します。
5. クライアントは、ホスト10.255.132.1のポート1098に接続します。
6. クライアントが新しいJava.class ファイルを必要とする場合、そのクライアントは、ホスト10.255.132.1のポート4446に接続します。

## ポートの変更

JNDIポートを変更するには、次の手順に従います。

1. 次のように、ファイルを編集して 1099 を 1199 に変更します。
  - － Windows : <NA\_HOME>\server\ext\jboss\server\default\conf\bindingservice.beans\META-INF\bindings-jboss-beans.xml
  - － UNIX : <NA\_HOME>/server/ext/jboss/server/default/conf/bindingservice.beans/META-INF/bindings-jboss-beans.xml
2. ファイルを保存して NA サーバを再起動します。(注意 : JNDIポートを変更する場合は、NA API をコールするコードも変更する必要があります。たとえば、「NA1.ops.com:1099」に接続する代わりに、NA API は「NA1.ops.com:1199」(または構成されているいずれかのポート)に接続する必要があります。)

RMIポートを変更するには、次の手順に従います。

1. 次のように、ファイルを編集して 1098 を 1198 に変更します。
  - － Windows : <NA\_HOME>\server\ext\jboss\server\default\conf\bindingservice.beans\META-INF\bindings-jboss-beans.xml
  - － UNIX : <NA\_HOME>/server/ext/jboss/server/default/conf/bindingservice.beans/META-INF/bindings-jboss-beans.xml
2. ファイルを保存して NA サーバを再起動します。(注意 : RMI ポートへの変更はクライアントには見えません。クライアント側の変更は必要ありません。)

RMIオブジェクトポートを変更するには、次の手順に従います。

1. 次のように、ファイルを編集して 4446 を 4447 に変更します。
  - － Windows : <NA\_HOME>\server\ext\jboss\server\default\conf\bindingservice.beans\META-INF\bindings-jboss-beans.xml
  - － UNIX : <NA\_HOME>/server/ext/jboss/server/default/conf/bindingservice.beans/META-INF/bindings-jboss-beans.xml
2. ファイルを保存して NA サーバを再起動します。(注意 : RMI オブジェクトポートへの変更はクライアントには見えません。クライアント側の変更は必要ありません。)

## ポート数が正しくない

ポート数が正しくない場合は、カウントするポートタイプを設定するために以下の手順を実行します。

1. NAを停止します。
2. `$NA/adjustable_options.rcx` ファイルを更新して、`<options>` タグと `</options>` タグの間のいずれかの場所に次のエントリを追加します。

```
<array name="PortCount/PortTypes">
<value>Ethernet</value>
<value>FastEthernet</value>
<value>GigEthernet</value>
<value>FDDI</value>
<value>Lex</value>
<value>TokenRing</value>
<value>VGAnyLan</value>
<value>Pos</value>
<value>Serial</value>
<value>HSSI</value>
<value>ATM</value>
<value>Dialer</value>
<value>BRI</value>
<value>DSL</value>
<value>TenGigabitEthernet</value>
<value>GigEthernetTrunk</value>
</array>
```

**注意：** カウントしたいインターフェイス/ポートタイプに合わせて上記のリストを編集します。

3. NAをインストールした場所（通常、`/opt/na/`）に`$NA`を置き換えます。
4. `$NA/adjustable_options.rcx` ファイルを更新して、`<options>` タグと `</options>` タグの間のいずれかの場所に次のエントリを追加します。

```
<option name="snapshot/force_update_model_data">true</option>
```

**注意：** このオプションを指定すると、構成変更がない場合も、NAはすべてのチェックポイントスナップショットでポート数（およびその他のデバイスデータ）を再計算します。

5. NAを再起動します。
6. インベントリに対してスナップショットタスクを実行して、ポート数を更新します。
7. [タスクの新規作成]ページの[スナップショットにチェックポイントを作成]オプションをオンにします。これにより、既存のデバイスのポート数が再計算されます。

**注意：** スナップショットタスクの実行後に、`/opt/na/adjustable_options.rcx` ファイルから`<option name="snapshot/force_update_model_data">true</option>` を削除することでパフォーマンスを向上させることができます。



# 表示メニューオプション

メニュー オプション	説明/アクション
デバイス詳細	<p>次のオプションを選択できます。</p> <ul style="list-style-type: none"> <li>• デバイスホーム：そのデバイスの[デバイス詳細]ページが開きます。</li> <li>• ACL：[デバイスACL]ページが開きます。そのページで、このデバイスに関連するすべてのACLのリストを表示できます。詳細については、「<a href="#">ACLの表示</a>」(695ページ)を参照してください。</li> <li>• インターフェイス：[デバイスインターフェイス]ページが開きます。そのページで、デバイスのインターフェイスと、各インターフェイスを介して接続している上流デバイスおよび下流デバイスのリストを表示できます。接続しているデバイスがアクティブに管理されている場合には、そのデバイスへのリンクがあります。これによって、ネットワークダイアグラムを検索する必要のないトラブルシューティングの場合は、レイヤ3トポロジを横断することができます。(注意：インターフェイス診断を実行すると、[デバイスインターフェイス]ページが更新されます。デフォルトでは、NAが構成変更を検出したときに、この診断が実行されます。) 詳細については、「<a href="#">[デバイスインターフェイス]ページのフィールド</a>」(205ページ)を参照してください。</li> <li>• IPアドレス：[デバイスIPアドレス]ページが開きます。そのページでは、デバイスに関連するすべてのIPアドレスを表示できます。このアドレスには、デバイス上のインターフェイスのIPアドレスと、デバイスに表示されるネットワーク上のIPアドレスも含まれます。詳細については、「<a href="#">[デバイスIPアドレス]ページのフィールド</a>」(211ページ)を参照してください。</li> <li>• MACアドレス：[デバイスMACアドレス]ページが開きます。そのページで、デバイスに関連し、NAで使用できるすべてのMACアドレスのリストを表示できます。詳細については、「<a href="#">[デバイスMACアドレス]ページのフィールド</a>」(212ページ)を参照してください。</li> <li>• VLAN：[デバイスVLAN]ページが開きます。そのページで、デバイスに構成されているVLAN情報を表示できます。詳細については、「<a href="#">[デバイスVLAN]ページのフィールド</a>」(215ページ)を参照してください。</li> <li>• VTP情報：[VTP詳細]ページが開きます。そのページで、VLANのVTP情報を表示できます。詳細については、「<a href="#">[VTP詳細]ページのフィールド</a>」(218ページ)を参照してください。</li> <li>• モジュール：[デバイスブレード/モジュール]ページが開きます。そのページで、デバイスにインストールされたモジュール（ブレード、カード）のリストを表示できます。デフォルトでは、モジュールデータはモジュールステータス診断によって週1回更新されます。詳細については、「<a href="#">[デバイスブレード/モジュール]ページのフィールド</a>」(220ページ)を参照してください。</li> <li>• ポリシー：[デバイスポリシー]ページを開きます。ここでは、デバイスに適切なポリシーが適用されたかの確認、ポリシーの成功または失敗の確認、デバイスをNAに追加した際にデバイスに適用されるポリシーの表示、およびデバイスに適用されるポリシーの例外の表示を行うことができます。詳細については、「<a href="#">[デバイスポリシー]ページのフィールド</a>」(221ページ)を参照してください。</li> <li>• サーバ：[サーバ]ページが開きます。そのページで、デバイスに接続しているHP Server Automation (SA) サーバのリストを表示できます。詳細については、「<a href="#">[サーバ]ページのフィールド</a>」(222ページ)を参照してください。</li> <li>• ソフトウェアイメージ推奨：[ソフトウェアイメージ推奨]ページが開きます。そのページで、[ユーザ環境設定]ページで指定したフィルタで削除したものを除いたすべてのデバイスソフトウェアイメージ推奨を表示できます。詳細については、「<a href="#">[デバイスソフトウェアイメージ推奨]ページのフィールド</a>」(223ページ)を参照してください。</li> </ul>
シングルビュー	<p>[シングルビュー]ページが開きます。そのページで、シングルデバイスまたは1つのページにあるすべてのデバイスへの変更を示すイベントを追跡できます。詳細については、「<a href="#">イベントの連結ビュー（シングルビュー）</a>」(546ページ)を参照してください。</p>
現在の構成	<p>[現在の構成]ページが開きます。そのページで、デバイスのランニング構成へこの構成を配布することができます。詳細については、「<a href="#">[デバイス構成]ページのフィールド</a>」(173ページ)を参照してください。</p>

メニュー オプション	説明/アクション
構成変更	<p>[デバイス構成]ページが開きます。そのページで、2つのデバイス構成を並べて表示できます。詳細については、<a href="#">「デバイス構成の比較」</a>（179ページ）を参照してください。</p>
診断	<p>[診断]リストからオプションを選択してください。各オプションにより、デバイス固有の診断の履歴リストが示されます。最も頻繁に使用する診断を次に示します。</p> <ul style="list-style-type: none"> <li>• <b>すべて</b>：1つのページにすべての診断を表示します。</li> <li>• <b>基本 IP</b>：デフォルトゲートウェイ、DNS サーバ、ドメインリスト、インストールしたインターフェイスに割り当てられた IP アドレスなどの基本 IP 情報を表示します。</li> <li>• <b>メモリトラブルシューティング</b>：任意のデバイスに実行するサンプルカスタム診断です。デバイス構成変更後の標準診断に含まれています。</li> <li>• <b>デバイス情報</b>：ソフトウェアやハードウェアのバージョン、デバイスのモデル名やホスト名、インターフェイスの説明などの基本デバイス情報を表示します。この情報はデフォルトの診断とともに表示されますが、デバイスで NA がスナップショットタスクを実行したときにのみ更新されます。</li> <li>• <b>NA がデバイスのブートを検出</b>：デバイスを最後にブートしたときの情報を表示します。</li> <li>• <b>NA デバイスファイルシステム</b>：デバイスのフラッシュカードまたはハードドライブ上に現在あるファイル（通常はソフトウェアイメージファイル）を記録します。このデータは、ソフトウェアの配布タスクで使用します。</li> <li>• <b>NA 通信モードデータ収集</b>：インターフェイスレポートのために、通信モード設定や現在のポートステータスなどのレイヤ 2 の接続データを収集します。ただし、すべてのデバイスがこの診断をサポートしているわけではありません。さらに、診断で表示可能な出力はありません。</li> <li>• <b>NA フラッシュ記憶域容量</b>：低容量フラッシュイベントをトリガーするために Nortel BayRS デバイスにのみ使用する、特別な目的の診断です。これによって圧縮スクリプトが実行されます。</li> <li>• <b>NA インターフェイス</b>：ステータス、IP アドレス、エラー、I/O レート、VLAN 情報など、デバイスのインターフェイス情報を表示します。</li> <li>• <b>NA モジュールのステータス</b>：このデバイスのモジュール診断を表示します。</li> <li>• <b>NA OSPF ネイバー</b>：NA データベースに格納されている OSPF ネイバーテーブルのリストを表示します。</li> <li>• <b>NA ルーティングテーブル</b>：NA データベースに格納されている、このデバイスのルーティングテーブルをすべて表示します。BGP を実行している場合で取得可能であれば、ルーティングテーブルのサマリ情報を表示します。</li> <li>• <b>HPNA トポロジーデータ収集</b>：ダイアグラム作成やトポロジーレポートに使用するテーブルを読み込む目的で使用する診断です。この診断で表示可能な出力はありません。</li> <li>• <b>NA VLAN データの収集</b>：この診断は、最新の VLAN 情報を収集するために使用します。[デバイス VLAN の新規作成]ページと[デバイス VLAN を編集]ページの情報は、デバイスから最後に収集した VLAN データに基づいています。最新の VLAN データを確実に取得するには、VLAN データ収集診断を実行して NA を最新の VLAN データで更新します。（<b>注意</b>：この診断は、データベース内のすべての診断テキストを保存しません。データベース内の特定のテーブルのみを更新します。したがって、診断は表示できません。）</li> <li>• <b>NA ポートスキャン</b>：この診断は Nmap を使用して、デバイスのポートをスキャンし、開いているポート、およびポートが提供するサービスの内容についての詳細を返します。</li> </ul>
デバイスタスク	<p>[デバイスタスク]ページが開きます。このページで、このデバイスに関連するすべてのタスクのリストを表示できます。タスクの詳細の表示やタスクの再実行も、このページからできます。[デバイスタスク]ページの詳細については、<a href="#">「[デバイスタスク]ページのフィールド」</a>（225ページ）を参照してください。</p>

メニュー オプション	説明/アクション
デバイスのイベント	[デバイスイベント]ページが開きます。このページで、[サマリ]フィールド内のリンクをクリックして、成功/失敗ステータスなど、このデバイスの最近のシステムイベントを表示したり、イベントの詳細情報にアクセスできます。[デバイスイベント]ページのフィールドの詳細については、 <a href="#">「[デバイスイベント]ページのフィールド」(204ページ)</a> を参照してください。
デバイス関係	[デバイス関係]ページが開きます。デバイス関係によって、デバイス間の関係の作成およびその関係の表示が可能になります。デバイス関係の詳細については、 <a href="#">「[デバイス関係]ページのフィールド」(226ページ)</a> を参照してください。
ソフトウェア 監査証跡	[デバイスソフトウェア履歴]ページが開きます。そのページで、デバイスにロードされたソフトウェアを表示できます。[デバイスにロードされたソフトウェア]ページのフィールドの詳細については、 <a href="#">「[デバイスソフトウェア履歴]ページのフィールド」(228ページ)</a> を参照してください。
Telnet/SSH セッション	[デバイスセッション]ページが開きます。そのページで、このデバイスに関連するTelnetおよびSSHセッションのリストを表示できます。セッションには、セッション全体にログインするコマンドまたはキーストロークのみを含むことができます。[デバイスセッション]ページのフィールドの詳細については、 <a href="#">「[デバイスセッション]ページのフィールド」(229ページ)</a> を参照してください。

NA診断の大半は、NAに標準装備されている標準診断であり、次のサンプル診断を除いて編集できません。

- メモリトラブルシューティング
- ハードウェア情報

## [デバイスイベント]ページのフィールド

[デバイスイベント]ページでは、成功/失敗ステータスなどデバイスでの最近のシステムイベントの表示や、イベントの詳細情報へのアクセスができます。

フィールド	説明/アクション
チェックボックス	左側のチェックボックスを使用して、選択したイベントを削除できます。デバイスを選択して[アクション]ドロップダウンメニューをクリックし、[削除]をクリックしてください。隣接の[選択]ドロップダウンメニューを使用すると、イベントを全選択または全選択解除できます。
イベント日時	イベントが発生した日時を表示します。
サマリ	イベントの簡単な説明を表示します。[サマリ]リンクをクリックすると、[イベントの詳細]ページが開きます。そのページで、イベントの詳細情報を表示できます。
追加ユーザ名	イベントを開始するユーザまたはプロセスを表示します。

## [デバイスインターフェイス]ページのフィールド

[デバイスインターフェイス]ページでは、デバイスのインターフェイスと、各インターフェイスを介して接続している上流デバイスおよび下流デバイスのリストを表示できます。ポートがレイヤ2で、インターフェイスがレイヤ3であっても、NAはその区別をしません。

[デバイスインターフェイス]ページを表示するには、デバイスの[表示]メニューで[デバイス詳細]を選択して[インターフェイス]をクリックします。[デバイスインターフェイス]ページが開きます。

フィールド	説明/アクション
ポート名	Ethernet0やSerial1など、ポート名を表示します。
ポートタイプ	FastEthernetなどのポートタイプの名前が表示されます。
ポートのステータス	インターフェイスが、[アップに構成]または[ダウンに管理]のどちらであるかを表示します。(注意: これはインターフェイスのプロトコルステータスには反映されず、構成ステータスのみに反映されます。)
実行ポートステータス	ポート (アップまたはダウン) のレイヤ2接続を指定します。この情報は、NAの通信モードデータ収集診断から収集されます。詳細については、「 <a href="#">[診断の実行]タスクページのフィールド</a> 」(310ページ)を参照してください。
ポートIP	インターフェイスのプライマリIPアドレスを表示します。NAはデバイス構成からIPアドレスを解析します。詳細については、「 <a href="#">[デバイス構成]ページのフィールド</a> 」(173ページ)を参照してください。
説明	インターフェイスの簡単な説明を表示します。NAはデバイス構成から説明を解析します。
ネゴシエートされた通信モード	全二重、または半二重のいずれかの通信モードを表示します。この情報は、トポロジーデータ収集診断によって収集されます。詳細については、「 <a href="#">[診断の実行]タスクページのフィールド</a> 」(310ページ)を参照してください。
アクション	<p>各インターフェイスに対して次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>• インターフェイスを編集: [インターフェイスの詳細を編集]ページが開きます。そのページで、このインターフェイスの詳細とカスタムデータフィールドを編集できます。「<a href="#">[インターフェイスの詳細を編集]ページのフィールド</a>」(208ページ)を参照してください。</li> <li>• インターフェイスを表示: [インターフェイスの詳細]ページが開きます。そのページで、このインターフェイスの詳細とカスタムデータを表示できます。また、代替IPアドレスや接続しているサーバの表示、コメントの表示や編集もできます。「<a href="#">[インターフェイスの詳細]ページのフィールド</a>」(206ページ)を参照してください。SA サーバ管理の詳細情報については、『HP Server Automation User's Guide』を参照してください。</li> <li>• サブネット内のインターフェイス: [サブネット内のインターフェイス]ページが開きます。そのページで、このインターフェイスと同一のサブネット内にある、すべてのインターフェイスを表示できます。これにより、デバイスがアクティブに管理されていれば、サブネット内でリンクされているデバイスを横断できます。「<a href="#">[サブネット内のインターフェイス]ページのフィールド</a>」(210ページ)を参照してください。</li> </ul>

## [インターフェイスの詳細]ページのフィールド

[インターフェイスの詳細]ページでは、固有のインターフェイスの詳細を表示できます。ポートがレイヤ2で、インターフェイスがレイヤ3であっても、NAはその区別をしません。

フィールド	説明/アクション
デバイス	デバイスの名前とIPアドレスを表示します。
名前	次のようにインターフェイス名を表示します：イーサネット0/1
タイプ	次のようにインターフェイスのタイプを表示します：[Ethernet]
ステータス	次のようにインターフェイスのステータスを表示します。アップに構成
接続先	インターフェイスの接続先サーバを表示します。
プライマリIP	インターフェイスのプライマリIPアドレスを表示します。[サブネット内のインターフェイス]リンクをクリックすると、[デバイスインターフェイス]ページが開きます。そのページで、このインターフェイスと同一のサブネット内にある、すべてのインターフェイスを表示できます。これにより、デバイスがアクティブに管理されていれば、サブネット内でリンクされているデバイスを横断できます。詳細については、 <a href="#">「[デバイスインターフェイス]ページのフィールド」(205 ページ)</a> を参照してください。
説明	インターフェイスの説明を表示します。
MACアドレス	次のようにインターフェイスのMACアドレスを表示します。00-50-10-F6-41
メンバー VLAN	このデバイスが属するVLANを表示します。[VLAN名]リンクをクリックすると、該当するVLANの[VLANの詳細]ページが開きます。詳細については、 <a href="#">「[VLAN詳細]ページのフィールド」(217 ページ)</a> を参照してください。VLANの詳細については、 <a href="#">「仮想ローカルエリアネットワーク (VLAN)」(213 ページ)</a> を参照してください。  <b>注意：</b> トランクポートにネイティブVLAN（タグ付けされていないVLAN）がない場合、[メンバー VLAN]リストの下部に「ネイティブVLANがありません」と表示されます。
通信モード	ネットワークインターフェイスでは、イーサネットポート設定、速度設定、通信モード設定、接続しているデバイス、VLAN名などを特定します。自動ネゴシエートモードをNAのネットワークインターフェイスに設定し、SAのネットワークカードにネゴシエートします。通信モード設定の不一致とは、管理しているサーバと接続しているネットワークデバイスについて、速度設定と通信モード設定の間で構成の不一致が起きていることを指します。
速度	ネットワークインターフェイスでは、イーサネットポート設定、速度設定、通信モード設定、接続しているデバイス、VLAN名などを特定します。自動ネゴシエートモードをNAのネットワークインターフェイスに設定し、SAのネットワークカードにネゴシエートします。速度設定の不一致とは、管理しているサーバと接続しているネットワークデバイスについて、速度設定と通信モード設定の間で構成の不一致が起きていることを指します。
構成	インターフェイスの現在の構成を表示します。[構成を表示]リンクをクリックすると、[現在の構成]ページが開きます。コンフィグレット分析により、パーサはインターフェイスに関連する構成の行を抽出できます。

フィールド	説明/アクション
VRF	<p>インターフェイスに関連付けられる仮想ルーティング/転送 (VRF) を定義するデバイス構成セクションを表示します。VRFによって、ルーティングテーブルの複数のインスタンスが同じルータ内で共存可能になります。ルーティングインスタンスは独立しているため、相互に競合することなく同一または重複IPアドレスを使用できます。</p> <p><b>注意：</b> このフィールドは、インスタンスに関連付けられたVRFがあり、デバイスドライバがVRF解析をサポートしている場合にのみ表示されます。</p>
QoS	<p>Quality of Service (QoS) 情報を表示します。NAはQoS構成文のインターフェイス構成を分析し、対応するグローバル構成情報を表示します。言い換えれば、関連するもののインターフェイス構成には含まれない構成の一部が表示されます。これには、ルートマップ、ポリシーマップ、クラスマップ、およびACLが含まれます。この情報により、デバイス構成のより広範な情報と、ネットワークの性能の理由（パケットロス、特定パケットタイプでの長時間の遅延など）が得られます。</p>
ACL	<p>インターフェイスに存在することが知られているACLが表示されます。</p>
最終変更	<p>インターフェイスが最後に変更された日時を表示します。</p>
コメント	<p>インターフェイスについてのコメントを表示します。</p>
詳細を編集	<p>[インターフェイスの詳細を編集]ページが開きます。<a href="#">「[インターフェイスの詳細を編集]ページのフィールド」(208 ページ)</a></p>

## [インターフェイスの詳細を編集]ページのフィールド

[インターフェイスの詳細を編集]ページでは、インターフェイスとカスタムデータフィールドの詳細を編集できます。

[インターフェイスの詳細を編集]ページにナビゲートするには：

1. [デバイス詳細]ページで[表示]メニューを選択します。
2. [表示]メニューで[デバイス詳細]を選択し、[インターフェイス]をクリックします。[デバイスインターフェイス]ページが開きます。
3. [アクション]フィールドで、編集するポートの[インターフェイスを編集]リンクをクリックします。[インターフェイスの詳細を編集]ページが開きます。

**注意：** [インターフェイスの詳細を編集]ページにはトランクポートの構成セクションがあります。[VLAN トランク]チェックボックスを使用すると、トランクポートをセットアップできます。このセクションは、オンにしたときに表示される折り畳み可能なフィールドセットで、表で説明するように [ネイティブVLAN ID] や [メンバー VLAN] が含まれています。

フィールド	説明/アクション
デバイス	デバイスの名前とIPアドレスを表示します。
名前	次のようにインターフェイス名を表示します：イーサネット0/1
タイプ	次のようにインターフェイスのタイプを表示します：[Ethernet]
ステータス	次のようにインターフェイスのステータスを表示します。アップに構成
接続先	インターフェイスの接続先サーバを表示します。
プライマリIP	インターフェイスのプライマリIPアドレスを表示します。[サブネット内のインターフェイス]リンクをクリックすると、[デバイスインターフェイス]ページが開きます。そのページで、このインターフェイスと同一のサブネット内にある、すべてのインターフェイスを表示できます。これにより、デバイスがアクティブに管理されていれば、サブネット内でリンクされているデバイスを横断できます。
説明	インターフェイスの説明を表示します。
MACアドレス	次のようにインターフェイスのMACアドレスを表示します。00-50-10-F6-41
メンバー VLAN	このデバイスが属するVLANを表示します。VLANの詳細については、「 <a href="#">仮想ローカルエリアネットワーク (VLAN)</a> 」(213 ページ) を参照してください。
通信モード	ネットワークインターフェイスでは、イーサネットポート設定、速度設定、通信モード設定、接続しているデバイス、VLAN名などを特定します。自動ネゴシエートモードをNAのネットワークインターフェイスに設定し、SAのネットワークカードにネゴシエートします。通信モード設定の不一致とは、管理しているサーバと接続しているネットワークデバイスについて、速度設定と通信モード設定の間で構成の不一致が起きていることを指します。
速度	ネットワークインターフェイスでは、イーサネットポート設定、速度設定、通信モード設定、接続しているデバイス、VLAN名などを特定します。自動ネゴシエートモードをNAのネットワークインターフェイスに設定し、SAのネットワークカードにネゴシエートします。速度設定の不一致とは、管理しているサーバと接続しているネットワークデバイスについて、速度設定と通信モード設定の間で構成の不一致が起きていることを指します。



フィールド	説明/アクション
VLAN トランク	<p>特定のポートをトランクポート、物理ポート、ポートチャネル（集合ポート）として構成できます。ループバックポートおよびVLANインターフェイスのポートはトランクとして構成することはできません。VLAN トランクをオフにすると、ポートは非トランクとして設定されます。これにより、ポートが[ネイティブVLAN ID]フィールドで示されているVLANに割り当てられます。VLAN トランクポート設定を変更すると、デバイスでの変更を適用する新しいVLANタスクが作成されます。詳細については、「<a href="#">[VLANタスク]ページのフィールド</a>」（363 ページ）を参照してください。</p> <p><b>注意：</b> デバイスドライバが拡張VLAN機能をサポートしていない場合、[インターフェイスの詳細を編集]ページに[VLAN トランク]フィールドが表示されません。</p>
ネイティブVLAN ID	<p>ネイティブVLAN IDは、トランクポートでタグが付かないパケットがあるVLANです。さらに、ポートで受信されたタグ付けされていないパケットはネイティブVLANのパケットと見なされます。ただし、ネイティブVLANはCiscoの用語です。たとえば、ProCurveではネイティブVLANという用語を使用しません。ProCurveではタグなしVLANメンバーシップという用語を使用します。トランクポートにはタグなしVLANメンバーシップを1つのみ設定できます。</p>
メンバー VLAN	<p>VLAN トランクポートは選択したVLANのトラフィックを転送します。選択されないVLANはすべて整理されます。</p>
VLAN ID を指定	<p>Cisco デバイスの場合、トランクポートのVLAN IDまたはVLAN IDの範囲を指定できます。Cisco デバイスのトランクポートは、デバイスで定義されないVLANのメンバーになることができます（ただし、このフィールドはCisco以外のデバイスの場合表示されません）。</p>
コメント	<p>インターフェイスについてのコメントを表示します。</p>

## [サブネット内のインターフェイス]ページのフィールド

[サブネット内のインターフェイス]ページでは、ネゴシエーションされた通信モード、およびネゴシエーションされた速度設定と一緒にサブネット内のインターフェイスが表示されます。レイヤー3インターフェイスがサブネット内のその他のインターフェイスと比較されます。不一致が存在する場合、不一致ポートが赤色の太字でその値を表示します。

フィールド	説明/アクション
ホスト名	インターフェイスのホスト名またはIPアドレスが表示されます。
ポート名	Ethernet0やSerial1など、ポート名を表示します。
ポートのステータス	インターフェイスが、[アップに構成]または[ダウンに管理]のどちらであるかを表示します。(注意: これはインターフェイスのプロトコルステータスには反映されず、構成ステータスのみに反映されます。)
ポートIP	インターフェイスのプライマリIPアドレスを表示します。NAはデバイス構成からIPアドレスを解析します。
説明	インターフェイスの簡単な説明を表示します。NAはデバイス構成から説明を解析します。
ネゴシエートされた通信モード	全二重、または半二重のいずれかの通信モードを表示します。この情報は、スイッチを経由するトラフィックが、全二重、100M、または半二重、10Mで動作するその他のスイッチにより影響を受けるかどうかを判断するのに使用されます。たとえば、パスの一部の遅延によるパケットの遅延を発生させるスイッチが存在する可能性があります。
ネゴシエートされた速度	100Mなどのネゴシエートされた速度が表示されます。
アクション	<p>各インターフェイスに対して次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>• インターフェイスを編集: [インターフェイスを編集]ページが開きます。そのページで、このインターフェイスの詳細とカスタムデータフィールドを編集できます。</li> <li>• インターフェイスを表示: [インターフェイスの詳細]ページが開きます。そのページで、このインターフェイスの詳細とカスタムデータを表示できます。また、代替IPアドレスや接続しているサーバの表示、コメントの表示や編集もできます。<a href="#">「[インターフェイスの詳細]ページのフィールド」(206 ページ)</a>を参照してください。SA サーバ管理の詳細情報については、『HP Server Automation User's Guide』を参照してください。</li> </ul>

## [デバイスIPアドレス]ページのフィールド

[デバイスのIPアドレス]ページでは、デバイスに関連するすべてのIPアドレスを表示できます。このアドレスには、デバイス上のインターフェイスのIPアドレスと、デバイスに表示されるネットワーク上のIPアドレスも含まれます。

フィールド	説明/アクション
ポート名	デバイスのIPアドレスに関連するポート名を表示します。
アドレス	IPアドレスを表示します。
アドレスタイプ	たとえば、次のようにインターフェイスのタイプを表示します。「ポートのアドレス」または「ポートから認識」。
VLAN	VLANへのリンクを提供します。タイプが[ポートのアドレス]であるIPアドレスを含みます。
説明	IPアドレスの説明を入力します。
リモート位置	タイプが[ポートから認識]であるリモート位置へのリンクを提供します。 リモート位置とは、NAが認識しているデバイスやポートのことです。NA/SA統合が可能な場合は、SAが認識しているサーバとインターフェイスを指します。
最初の認識日時	IPアドレスが最初に認識された日付および時刻が表示されます。
最終の認識日時	NAがトポロジーデータを最後に収集した時点でIPアドレスが認識されている場合は、[現在]と表示されます。[現在]でない場合は、NAがネットワーク上でIPアドレスを最後に認識した日時が表示されます。たとえば、ラップトップや他の一時的なデバイスのIPアドレスは、既にネットワーク上に存在しない可能性もあります。さらに、ルーティングトラフィックによる変更で、IPアドレスがメインフローから失われることもあります。
関連MAC	[デバイスMACアドレス]ページが開きます。そのページで、デバイスに関連し、NAで利用できるすべてのMACアドレスのリストを表示できます。
アクション	各デバイスに対して次のアクションを選択できます。 <ul style="list-style-type: none"> <li>• 詳細: [IPアドレスの詳細]ページが開きます。そのページで次の詳細を表示できます。デバイス、デバイスポート、IPアドレス、MACアドレス、タイプ、最初の認識日時、および最終更新です。</li> <li>• MACを表示: [MACアドレスの詳細]ページが開きます。そのページは、このIPアドレスで相互参照されています。相互参照とは、NAがデータを収集したときに、IPアドレスとMACアドレスのソースが同一だったことを意味します。これは、[ポートから認識]レコードでのみ使用できます。</li> </ul>

## [デバイス MAC アドレス] ページのフィールド

[デバイスの MAC アドレス] ページでは、デバイスに関連するすべての MAC アドレスのリストを表示できます。

フィールド	説明/アクション
ポート名	デバイスの IP アドレスに関連するポート名を表示します。
アドレス	MAC アドレスを表示します。
アドレスタイプ	たとえば、次のように MAC アドレスのタイプを表示します。「ポートのアドレス」または「ポートから認識」。
VLAN	VLAN へのリンクを提供します。タイプが [ポートのアドレス] である MAC アドレスを含みます。
説明	MAC アドレスの説明を表示します。
リモート位置	タイプが [ポートから認識] であるリモート位置へのリンクを提供します。リモート位置とは、NA が認識しているデバイスとポートのことです。反対に、HP Server Automation (SA) が認識するサーバやインターフェイスのこともあります。NA/SA 統合の詳細については、「 <a href="#">NA/SA 統合</a> 」(196 ページ) を参照してください。
最初の認識日時	MAC アドレスが最初に認識された日付および時刻が表示されます。
最終の認識日時	NA がトポロジーデータを最後に収集した時点で MAC アドレスが認識されている場合は、[現在] と表示されます。[現在] でない場合は、NA がネットワーク上で MAC アドレスを最後に認識した日時が表示されます。たとえば、ラップトップや他の一時的なデバイスの MAC アドレスは、既にネットワーク上に存在しない可能性もあります。さらに、ルーティングトラフィックによる変更で、MAC アドレスがメインフローから失われることもあります。
関連 IP	[デバイス IP アドレス] ページが開きます。そのページで、デバイスに関連し、NA で使用できるすべての IP アドレスのリストを表示できます。
アクション	各デバイスに対して次のアクションを選択できます。 <ul style="list-style-type: none"> <li>• 詳細を表示：[MAC アドレスの詳細] ページが開きます。そのページで次の詳細情報を表示できます。デバイス、デバイスポート、MAC アドレス、タイプ、構成スニペット、最初の認識日時、および最終更新です。</li> <li>• IP を表示：[IP アドレスの詳細] ページが開きます。そのページで、デバイス、デバイスポート、IP アドレス、MAC アドレス、タイプ、最初の認識日時、最終更新についての詳細情報を表示できます。</li> <li>• この IP アドレスで相互参照されるアクション。相互参照とは、NA がデータを収集したときに、IP アドレスと MAC アドレスのソースが同一だったことを意味します。これは、[ポートから認識] レコードでのみ使用できます。</li> </ul>

## 仮想ローカルエリアネットワーク（VLAN）

VLAN（仮想ローカルエリアネットワーク）は、単一のブロードキャストドメインとして機能するポートの集合です。VLANは、レイヤ2（データリンクレイヤ）で動作します。このレイヤでは、VLANタグを使ってイーサネットフレームを変更してブロードキャストドメインをセグメント化し、ネットワークスイッチを越えてデバイスをグループ分けします。NAは、管理デバイスに対して定義されているVLANおよび各ポートが割り当てられているVLANに関する情報を収集します。

VLANは通常、ブロードキャストドメインをセグメント化し、それらが同じネットワークスイッチ内に存在しない場合でも各端局を同じグループに属させることができます。VLANによってネットワークスイッチを仮想化することができます。つまり、1つのネットワークスイッチが、複数のレイヤ2ネットワークや複数のネットワークスイッチに及ぶ1つのLANにサービスを提供できます。

VLANはセグメントサービスを提供するので、ネットワークルータを使用せずにレイヤ2でのセキュリティ、拡張性、およびネットワーク管理の問題に対処できます。異なるブロードキャストドメインでは、ドメイン間のトラフィックを分離しているため、組織でのセキュリティが確保されます。

たとえば企業環境では、財務、人事、営業の各部門が独自のブロードキャストドメインを持つことで、各トラフィックが他の部署から見えないようにすることができます。また、財務部門では従業員が別々の場所にいる可能性があります。したがって、VLANは別々の場所にいる従業員を、同じネットワークに接続された物理的に同じ場所にいるかのようにグループ化することで、ネットワークの拡張性が向上させることができます。

また、VLANは、1つのネットワークスイッチを複数のブロードキャストドメインに分割可能にしたり、複数のネットワークスイッチを1つのブロードキャストドメインの一部にすることを可能にしたりすることで、ネットワークスイッチを仮想化します。したがって、組織内の各部門で別々のネットワークスイッチを置く代わりに、VLANを使った仮想ネットワークスイッチにネットワークスイッチを分割することで、複数の部門にサービスを提供することができます。

NAでは、ネットワークスイッチ上のVLANを表示およびプロビジョニングできます。NAを使用することにより、次のことが可能になります。

- デバイスのVLANの完全リストの表示
- 特定のVLAN詳細情報の表示
- VLANに割り当てられたポートリストの表示
- トランクポートの表示
- トランクポート上のVLANリストの表示
- トランクポートのネイティブVLAN（トランクポート上のトラフィックにタグが付かないVLAN）の表示
- ネットワークスイッチのVTP設定の表示
- ネットワークスイッチでの新規VLANの作成
- VLANに割り当てられたポートの変更（ポートの追加/整理）
- VLAN名の変更
- VLANの削除
- トランクポートとしてのポートの構成（タグ付けされた複数のVLAN）
- トランクポートVLANの変更（VLANメンバーシップ）

- トランクポートのネイティブVLANの変更
- 非トランクとしてのトランクポートの構成

## [デバイス VLAN] ページのフィールド

[デバイス VLAN] ページにはデバイスのすべての VLAN リストが表示されます。VLAN の詳細については、「[仮想ローカルエリアネットワーク \(VLAN\)](#)」(213 ページ) を参照してください。

[デバイス VLAN] ページにナビゲートするには：

1. [インベントリ] ページで VLAN 詳細を調べたいデバイスを選択します。ただし、任意のページにある [検索] オプションを使用してデバイスを特定することもできます。[デバイス詳細] ページが開きます。
2. [デバイス詳細] ページで [表示] メニューを選択します。
3. [表示] メニューで [デバイス詳細] オプションを選択し、VLAN オプションをクリックします。[デバイス VLAN] ページが開きます。

**注意：** デバイスドライバが拡張 VLAN 機能をサポートしていない場合は、プロビジョニングアクションは表示されません。

フィールド	説明/アクション
VLAN の新規作成	[デバイス VLAN の新規作成] ページが開きます。そのページで、新しい VLAN を作成できます。詳細については、「 <a href="#">VLAN の作成と編集</a> 」(216 ページ) を参照してください。
VLAN	VLAN 名を表示します。
VLAN タイプ	VLAN タイプを表示します。このフィールドはペンダー固有のフィールドです。
VLAN ID	VLAN 名を表示します。
VLAN ステータス	アクティブや一時停止などの VLAN ステータスを表示します。
最終変更	NA が最後にデバイスから VLAN を読み取った日時を表示します。(ただし、NA がこの日時以降にデバイスから VLAN を読み取っている可能性もありますが、この変更は行われません。)
説明	デバイスから引き出した VLAN の情報を表示します。
アクション	<p>VLAN ごとに、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>• 表示：[VLAN の詳細] ページが開きます。そのページで VLAN の詳細を表示できます。VLAN ポート情報は、[デバイスのインターフェイス] ページにリンクされています。詳細については、「<a href="#">[VLAN 詳細] ページのフィールド</a>」(217 ページ) を参照してください。トランクポートが VLAN のメンバーである場合、トランクポートが表示されます。</li> <li>• 編集：[VLAN 詳細を編集] ページが開きます。そのページで、VLAN 詳細の表示、および VLAN 名、説明、ポートメンバーシップの編集を行うことができます。詳細については、「<a href="#">VLAN の作成と編集</a>」(216 ページ) を参照してください。</li> <li>• 削除：VLAN の削除を確認するダイアログボックスが開きます。</li> </ul>

## VLANの作成と編集

[デバイス VLANの新規作成] ページでは、VLAN 名を入力し、その新しいVLANに割り当てるポートを確認できます。[デバイス VLANの新規作成] ページでは、VLAN 名およびポートメンバシップ情報を変更できます。VLANの詳細については、「[仮想ローカルエリアネットワーク（VLAN）](#)」（213 ページ）を参照してください。

**注意：** [デバイス VLANの新規作成] ページと [デバイス VLANを編集] ページの情報は、デバイスから最後に収集したVLANデータに基づいています。最後にVLANデータを収集した後にデバイスに変更が加えられた場合、その変更はこれらのページには反映されません。最新のVLANデータを確実に取得するには、VLANデータ収集診断を実行してNAを最新のVLANデータで更新します。詳細については、「[\[診断の実行\] タスクページのフィールド](#)」（310 ページ）を参照してください。

フィールド	説明/アクション
デバイス	デバイスのホスト名またはIPアドレス、あるいはその両方を表示します。デバイスリンクをクリックすると、[デバイス詳細] ページが開きます。「 <a href="#">デバイス詳細の表示</a> 」（193 ページ）を参照してください。
VLAN 名	新しいVLAN名を入力するか、既存のVLAN名を編集します。
VLAN ID	VLAN IDを入力します。ただし、[VLAN ID] フィールドは、VLANの新規作成操作では入力フィールドになりますが、VLANの編集操作ではテキストのみのフィールドになるので注意してください。
VLAN タイプ	VLAN タイプを表示します。このフィールドはベンダー固有のフィールドです。この情報は、デバイスから収集されたデータから自動的に入力されます。
VLAN ステータス	アクティブや一時停止などのVLANステータスを表示します。この情報は、デバイスから収集されたデータから自動的に入力されます。
VLAN MTU	VLANが使用可能なVLAN最大転送単位（パケットサイズ）を表示します。このフィールドはベンダー固有のフィールドです。この情報は、デバイスから収集されたデータから自動的に入力されます。
VLAN ポート	<p>VLAN ポートのリストを表示します。ポート名は当該ポートの[インターフェイスの詳細] ページにリンクされています。詳細については、「<a href="#">[インターフェイスの詳細] ページのフィールド</a>」（206 ページ）を参照してください。</p> <p>現在VLANに割り当てられているポートが確認されます。現在割り当てられていないが、割り当て可能な空きポートは確認されません。ポートのネイティブVLAN名が右括弧の間に指定されます。ポートがトランクポートの場合、ポートはトランクポートとして示されます。さらに、ポートがPortChannelの場合、そのポートの集合ポートがカンマ区切りリストで表示されます。</p> <p>現在VLANに割り当てられているポートは、それらのポートのチェックボックスをオフにすることでVLANから整理（削除）できます。同様に、現在VLANに割り当てられていないポートは、それらのポートのチェックボックスをオンにすることで割り当てることができます。</p>
VLANの説明	VLANの説明が表示されます。

終了時に、必ず[保存]をクリックしてください。変更を行った場合は、[VLANタスク] ページが開きます。詳細については、「[\[VLANタスク\] ページのフィールド](#)」（363 ページ）を参照してください。



## [VLAN詳細]ページのフィールド

[デバイスVLAN]ページで[アクション]フィールドの[表示]オプションをクリックすると、[VLANの詳細]ページが開きます。

フィールド	説明/アクション
デバイス	デバイスのホスト名またはIPアドレス、あるいはその両方を表示します。デバイスリンクをクリックすると、[デバイス詳細]ページが開きます。詳細については、「 <a href="#">デバイス詳細の表示</a> 」(193ページ)を参照してください。
VLAN名	VLAN名を表示します。
VLAN ID	VLAN名を表示します。
VLANタイプ	VLANタイプを表示します。このフィールドはベンダー固有のフィールドです。
VLANステータス	アクティブや一時停止などのVLANステータスを表示します。
VLAN MTU	VLANが使用可能なVLAN最大転送単位（パケットサイズ）を表示します。このフィールドはベンダー固有のフィールドです。
VLANポート	VLANポートのリストを表示します。ポートリンクをクリックすると、当該ポートの[インターフェイスの詳細]ページが開きます。トランクポートにネイティブVLAN（タグ付けされていないVLAN）がない場合、[メンバーVLAN]リストの下部に「ネイティブVLANがありません」と表示されます。「 <a href="#">[インターフェイスの詳細]ページのフィールド</a> 」(206ページ)を参照してください。  トランクポートには、[デバイスのインターフェイス]ページに一覧されているすべてのVLANがあります。詳細については、「 <a href="#">[デバイスインターフェイス]ページのフィールド</a> 」(205ページ)を参照してください。
VLANの説明	デバイスから引き出したVLANの情報を表示します。
最終変更日	NAが最後にデバイスからVLANを読み取った日時を表示します。（ただし、NAがこの日時以降にデバイスからVLANを読み取っている可能性もありますが、この変更は行われません。）
詳細を編集	[VLAN詳細を編集]ページが開きます。詳細については、「 <a href="#">VLANの作成と編集</a> 」(216ページ)を参照してください。

## [VTP 詳細] ページのフィールド

VLAN トランッキング プロトコル (VTP) は、Cisco 独自の プロトコル で Cisco の各 スイッチ 間の VLAN を管理するためのものです。VTP は、VTP ドメイン と呼ばれる 管理ドメイン を定義します。VTP ドメイン 内の 1 つまたは複数のスイッチは、ドメイン のその他の スイッチ を手動で構成する必要がないように VLAN 構成を配布するサーバとして構成されます。以下の 3 つの参加レベル (動作モード) があります。

- サーバ
- クライアント
- トランスペアレント

VTP ドメイン 内でサーバとして構成されたスイッチは、VTP ドメイン 内の他のスイッチへ VLAN 構成変更をアドバタイズします。VTP パケットは、サーバに接続されているスイッチに送信されます。クライアントモードのスイッチは VTP パケットに応答して、それに従って自分自身の VLAN 構成を変更してから、その VTP パケットを VTP ドメイン 内の他のスイッチに中継します。トランスペアレントモードのスイッチは、自分自身の VLAN 構成を変更しないで、VTP パケットを他のスイッチに中継します。

デバイスが Cisco スイッチで、VTP ドメイン に参加している場合、NA はそのデバイスの VTP 情報を表示します。VLAN の詳細については、[「仮想ローカルエリアネットワーク \(VLAN\)」\(213 ページ\)](#) を参照してください。

**注意：** NA は VTP 設定をプロビジョニングしません。NA の VTP サポート は読み取り専用です。つまり、NA は表示目的のみでデバイスから VTP 情報を収集します。

[VTP 詳細] ページにナビゲートするには：

1. [インベントリ] ページで VTP 詳細を調べたいデバイスを選択します。ただし、任意のページにある [検索] オプションを使用してデバイスを特定することもできます。[デバイスの詳細] ページが開きます。
2. [デバイス詳細] ページで [表示] メニューを選択し、[VTP 情報] オプションをクリックします。[VTP 詳細] ページが開きます。

フィールド	説明/アクション
デバイス	デバイスのホスト名または IP アドレス、あるいはその両方を表示します。デバイスリンクをクリックすると、[デバイス詳細] ページが開きます。詳細については、 <a href="#">「デバイスの詳細の表示」(193 ページ)</a> を参照してください。
VTP バージョン	VTP バージョンを表示します。
構成バージョン	構成バージョン番号を表示します。
ドメイン名	VTP ドメイン名を表示します。この名前は、[VTP ドメイン] ページにリンクされています。このページでは、当該ドメインに属するデバイスのリストを表示できます。詳細については、 <a href="#">「[VTP ドメイン] ページ」(220 ページ)</a> を参照してください。 <b>(注意：</b> 一重引用符 (') を含む VTP ドメイン名を使用すると、NA によって SQL エラーが返されます。
ローカルでサポートされる最大 VLAN 数	ローカルでサポートされる VLAN の最大数を表示します。
既存 VLAN 数	既存の VLAN 数を表示します。

フィールド	説明/アクション
VTP 動作モード	サーバ、クライアント、トランスベアレント、オフなどのVTP 動作モードを表示します。
VTP 整理モード	有効な場合、VTP 整理によって、不明なユニキャストおよびブロードキャストによって発生した不要なトラフィックを削除できます。
VTP V2モード	有効な場合、トークンリングVLANでVTP 2モードを使用できます。
VTP トラップ生成	有効な場合、トラブルシューティングのためにVTP トラップを生成できます。
MD5 ダイジェスト	有効な場合、トラブルシューティングのためにMD5 ダイジェストを使用できます。MD5 ダイジェストには、VTP パスワード（構成した場合）と VTP ドメイン名の組み合わせによって構成された 16 バイトのワード（MD5 値）が表示されます。
このドメイン内の VTP	ドメイン内のデバイスを表示します。デバイスのホスト名またはIPアドレスは、[デバイス詳細]ページにリンクされています。[デバイス詳細]ページでは、デバイスにVTP 構成がある場合にはVTP ドメイン名と動作モード情報が表示されます。詳細については、 <a href="#">「[デバイス詳細] ページのフィールド」</a> （193 ページ）を参照してください。
最終変更者	最後にVTP を変更したユーザの名前を表示します。
最終変更日	VTP を最後に変更した日付を表示します。

## [VTP ドメイン] ページのフィールド

[VLAN トランッキングプロトコル (VTP) ドメイン] ページには、NA が管理する1つまたは複数のデバイスのネットワーク内のVTP ドメインが一覧されます。VLAN の詳細については、[「仮想ローカルエリアネットワーク \(VLAN\)」](#)（213 ページ）を参照してください。

[VTP ドメイン] ページにナビゲートするには、[デバイス] メニューで[デバイスツール] を選択し、[VTP ドメイン] オプションをクリックします。[VTP ドメイン] ページが開きます。

フィールド	説明/アクション
ドメイン名	ドメイン名を表示します。
VTP バージョン	VTP バージョンを表示します。
デバイス数	NA がドメイン内で認識しているデバイス数を表示します。
アクション	[表示] リンクをクリックすると、[VTP ドメイン] ページが開きます。詳細については、 <a href="#">「[VTP ドメイン] ページ」</a> （220 ページ）を参照してください。

## [VTP ドメイン] ページ

[VTP ドメイン] ページには、特定のドメイン内のデバイスが表示されます。VLANの詳細については、「[仮想ローカルエリアネットワーク \(VLAN\)](#)」(213 ページ) を参照してください。

[VTP ドメイン (domain\_name)] ページにナビゲートするには、[VTP ドメイン] ページで、デバイスの詳細を調べたいドメインの[アクション] フィールドの[表示] オプションをクリックします。[VTP ドメイン] ページが開きます。

フィールド	説明/アクション
ホスト名	デバイスのホスト名が表示されます。[ホスト名] リンクをクリックすると、[デバイス詳細] ページが開きます。詳細については、「 <a href="#">デバイス詳細の表示</a> 」(193 ページ) を参照してください。
デバイス IP	デバイスの IP アドレスを表示します。[デバイス IP] リンクをクリックすると、[デバイス詳細] ページが開きます。詳細については、「 <a href="#">デバイス詳細の表示</a> 」(193 ページ) を参照してください。
MD5 ダイジェスト	有効な場合、トラブルシューティングのために MD5 ダイジェストを使用できます。
動作モード	サーバ、クライアント、トランスベアレント、オフなどの VTP 動作モードを表示します。
パーティション	デバイスが属するパーティションを表示します。(注意: このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。)
アクション	次のアクションを選択できます。 <ul style="list-style-type: none"> <li>VTP を表示: [VTP 詳細] ページが開きます。詳細については、「<a href="#">[VTP 詳細] ページのフィールド</a>」(218 ページ) を参照してください。</li> <li>VLAN を表示: [デバイス VLAN] ページが開きます。詳細については、「<a href="#">[デバイス VLAN] ページのフィールド</a>」(215 ページ) を参照してください。</li> </ul>

## [デバイスブレード/モジュール] ページのフィールド

[デバイスのブレード/モジュール] ページでは、デバイスにインストールされたモジュール (ブレード、カード) のリストを表示します。デフォルトでは、モジュールデータはモジュールステータス診断タスクによって週1回更新されます。

フィールド	説明/アクション
モジュールスロット	モジュールがインストールされているデバイスのスロットを表示します。
モジュールの説明	モジュールの簡単な説明を表示します。NAはデバイス構成から説明を解析します。
モジュールモデル	モデル識別子を表示します。
モジュールシリアル	モジュールのシリアル番号を表示します。
アクション	各モジュールに対して次のアクションを選択できます。 <ul style="list-style-type: none"> <li>モジュールを編集: [ブレード/モジュール詳細を編集] ページが開きます。そのページで、モジュールインベントリの詳細を表示でき、カスタムデータフィールドを編集できます。</li> <li>モジュールを表示: [ブレード/モジュール詳細] ページが開きます。そのページで、モジュールインベントリの詳細を表示でき、コメントを編集できます。</li> </ul>

## [デバイスポリシー]ページのフィールド

[デバイスポリシー]ページでは、次のことが可能です。

- デバイスに適切なポリシーが適用されたことを確認できます。
- ポリシーが成功したか失敗したかを表示できます。
- NAにデバイスを追加した際にデバイスに適用されるポリシーを表示できます。
- デバイスに適用されたポリシーの例外を表示できます。

ポリシーの作成の詳細については、「[NA Policy Managerの動作方法](#)」(413ページ)を参照してください。適用されたポリシーの表示方法の詳細については、「[適用されるポリシーの表示](#)」(429ページ)を参照してください。

フィールド	説明/アクション
ポリシー名	ポリシー名を表示します。
ルール名	該当する場合、ポリシーのルール名を表示します。詳細については、「 <a href="#">[ルールの新規作成]ページのフィールド</a> 」(420ページ)を参照してください。
説明	次のようにポリシーの説明を表示します。パスワードを確認
ポリシールールの例外	該当する場合、ポリシールールの例外を表示します。詳細については、「 <a href="#">[ルール例外の新規作成]ページのフィールド</a> 」(428ページ)を参照してください。
ステータス	次のようなポリシーのステータスが表示されます。 <ul style="list-style-type: none"> <li>• アクティブ</li> <li>• 非アクティブ</li> <li>• 合格</li> <li>• 失敗</li> </ul>
重要度	次のような違反されたルールの重要性を示します。 <ul style="list-style-type: none"> <li>• 情報：一般的に対応を必要としないイベント。</li> <li>• 低：時間的な余裕がある場合に対応を必要とするイベント。</li> <li>• 中：適時に対応を必要とするイベント（通常は72時間以内）。</li> <li>• 高：緊急の対応を必要とするイベント（通常は24時間以内）。</li> <li>• 重要：即時の対応を必要とするイベント。</li> </ul>
アクション	各ポリシーで次のアクションを選択できます。 <ul style="list-style-type: none"> <li>• ポリシーを編集：[ポリシーを編集]ページが開きます。このページでは、ポリシーを編集できます。詳細については、「<a href="#">[ポリシーを編集]ページのフィールド</a>」(425ページ)を参照してください。</li> <li>• ポリシーを編集：[ポリシールールを編集]ページが開きます。このページでは、ポリシールールを編集できます。詳細については、「<a href="#">[ルールの新規作成]ページのフィールド</a>」(420ページ)を参照してください。</li> </ul>

## [サーバ]ページのフィールド

[サーバ]ページでは、詳細を表示するデバイスに接続している各サーバの名前を表示します。サーバのホスト名をクリックすると、[サーバ詳細]ページが開きます。SAサーバの使用方法の詳細については、『HP Server Automation User's Guide』を参照してください。

NAは、レイヤ1の配線位置を推測するだけです。NAの減少アルゴリズムは、デバイスやサーバ間のすべての接続を（できるだけ）減らします。

**注意：** HP Server Automation (SA) Command Centerにログインしていない場合は、サーバのホスト名をクリックすると、ログインするように要求されます。

フィールド	説明/アクション
ネットワークデバイス インターフェイス	サーバで使用するネットワークデバイスインターフェイス。たとえば、FastEthernet1/0です。
サーバホスト名	サーバのホスト名を表示します。サーバのホスト名をクリックすると、[サーバの詳細]ページが開きます。詳細については、『HP Server Automation User's Guide』を参照してください。
サーバインターフェイス	オペレーティングシステムでレポートされるサーバインターフェイス名。
顧客	顧客名を表示します。
施設	顧客の施設を表示します。
サーバ使用	サーバ使用を表示します。詳細については、『HP Server Automation User's Guide』を参照してください。
配布の段階	配布の段階を表示します。詳細については、『HP Server Automation UserOs Guide』を参照してください。

## [デバイスソフトウェアイメージ推奨]ページのフィールド

[デバイスソフトウェアイメージ推奨]ページには、Cisco.comから入手可能な、優先推奨に沿ったソフトウェアイメージが表示されます。ソフトウェアイメージの属性も、ソフトウェアイメージの場所の情報と一緒に表示されます。ソフトウェアイメージは、Cisco.comからNAソフトウェアリポジトリへ直接ダウンロードされ、イメージセットが作成されます。

[自分の環境設定]ページで推奨フィルタを適用できます。詳細については、「[自分の環境設定]ページのフィールド」(262ページ)を参照してください。

**注意：** Ciscoのサポートするデバイスのリストを確認するには、以下のURLを参照してください。NAは、Resource Manager Essentials (RME) のデータを使用します。このため、デバイスはCiscoがサポートする必要があります。それ以外の場合、Ciscoソフトウェアイメージをダウンロードできません。

[http://cisco.com/en/US/products/sw/cscowork/ps2425/products\\_device\\_support\\_table09186a008086099b.html](http://cisco.com/en/US/products/sw/cscowork/ps2425/products_device_support_table09186a008086099b.html)

以下の図は、[デバイスソフトウェアイメージ推奨]ページのサンプルセクションを示します。例では、反転表示されているオプションが選択されています。[イメージ詳細]セクションでダウンロードするソフトウェアイメージをクリックすると、ソフトウェアイメージ（この場合では *rsp-isv56i-mz.121.bin*）がNAリポジトリにダウンロードされます。

モジュール/スロット/タイプリスト	バージョンリスト	機能リスト
BOOT_LOADER	--- 優先推奨 ---	--- 優先推奨 ---
SYSTEM_SW	12.2.46	IP/VIP IPSEC 56
	--- 一般推奨 ---	--- 一般推奨 ---
	12.4.8c	ENTERPRISE/VIP PLUS
	12.4.8b	ENTERPRISE/VIP IPSEC 56

### イメージ詳細

Schedule task to download from Cisco.com *rsp-isv56i-mz.121.bin* (Cisco.com から *rsp-isv56i-mz.121.bin* をダウンロードするタスクを予定)

ファイルサイズ: 11483336 バイト

機能: IP/VIP IPSEC 56

Flash: 16 MB

RAM: 64 MB

バージョン: 12.2..46

slot0

空き容量: 4900236 バイト Partition Size(パーティションサイズ): 1638400 バイト

警告 -SWIM10661: Image available at Cisco.com is selected for upgrade(Cisco.com から入手可能なイメージがアップグレード用に選択されています)

bootflash

空き容量: 383824 バイト Partition Size(パーティションサイズ): 7602176 バイト

警告 -SWIM10661: Image available at Cisco.com is selected for upgrade(Cisco.com から入手可能なイメージがアップグレード用に選択されています)

[デバイスソフトウェアイメージ推奨]ページを表示するには：

1. OS分析をサポートするCiscoデバイスを選択します。そのデバイスの[デバイス詳細]ページが開きます。
2. [表示]メニューで[デバイス詳細]を選択し、[ソフトウェアアップグレード推奨]をクリックします。

フィールド	説明/アクション
ホスト名	デバイスのホスト名を表示します。デバイスのホスト名をクリックすると[デバイス詳細]ページが開きます。このページでは、デバイスについての詳細な情報を確認できます。
デバイスIP	デバイスのIPアドレスを表示します。デバイスのIPアドレスをクリックすると[デバイス詳細]ページが開きます。このページでは、デバイスについての詳細な情報を確認できます。
最終アクセス時間	デバイスに最後にアクセスした日時を表示します（スナップショットの取得など）。
最後のスナップショットの結果	このデバイス構成の最後のスナップショットのステータスを表示します。スナップショットに失敗した場合は、[タスク結果]ページへのリンクがあります。
表示メニュー	[表示]メニューが開きます。詳細については、「 <a href="#">表示メニューオプション</a> 」(201 ページ) を参照してください。
編集メニュー	[編集]メニューが開きます。詳細については、「 <a href="#">編集メニューオプション</a> 」(230 ページ) を参照してください。
プロビジョニングメニュー	[プロビジョニング]メニューが開きます。詳細については、「 <a href="#">プロビジョニングメニューオプション</a> 」(239 ページ) を参照してください。
接続メニュー	[接続]メニューが開きます。詳細については、「 <a href="#">接続メニューオプション</a> 」(241 ページ) を参照してください。
ソフトウェアイメージのダウンロード	<p>以下のセクションには、選択したデータが入力されます。表示のサンプルについては、上記の図を参照してください。</p> <ul style="list-style-type: none"> <li>• モジュール/スロット/タイプリスト：BOOT_LOADER（オペレーティングシステムを起動するためのソフトウェアを読み込む小さなプログラム）およびSYSTEM_SWを表示します。</li> <li>• バージョンリスト：BOOT_LOADER、またはSYSTEM_SWのいずれかを選択すると、ソフトウェアイメージバージョンのリストが表示されます。</li> <li>• 機能リスト：ソフトウェアイメージバージョンを選択すると、ソフトウェアイメージバージョンの機能のリストが表示されます。機能を選択すると、[イメージ詳細]セクションにデータが入力されます。ソフトウェアイメージがNAソフトウェアリポジトリに存在しない場合、ソフトウェアイメージ名をクリックして、そのソフトウェアイメージをCisco.comから直接ダウンロードできます。イメージがNAソフトウェアリポジトリに存在する場合は、ソフトウェアイメージリンクをクリックしてください。[デバイスソフトウェアのアップグレードタスク]ページが開きます。このページでは、選択したソフトウェアイメージでデバイスをアップグレードできます。詳細については、「<a href="#">[デバイスソフトウェアの更新]タスクページのフィールド</a>」(323 ページ) を参照してください。</li> </ul>
イメージ詳細	ファイルサイズ、バージョンステータス、Flashなどのソフトウェアイメージの情報が表示されます。警告と一緒にデバイスのスロットとbootflashの情報も表示されます。



## [デバイスタスク]ページのフィールド

[デバイスタスク]ページでは、デバイスに関連するすべてのタスクのリストを表示します。タスクの詳細の表示やタスクの再実行も、このページからできます。

フィールド	説明/アクション
このページは60秒ごとにリフレッシュします。	表示を60秒ごとにリフレッシュさせたくない場合は、このチェックボックスをオフにします。この値の設定の詳細については、「 <a href="#">[ユーザインターフェイス]ページのフィールド</a> 」(61ページ)を参照してください。
チェックボックス	左側のチェックボックスを使用して、選択したタスクを削除できます。タスクを選択したら、[アクション]ドロップダウンメニューをクリックし、[削除]をクリックします。隣接の[選択]ドロップダウンメニューを使用すると、タスクを全選択または全選択解除できます。
予定日	タスクを実行した日時または実行予定の日時を表示します。
タスク名	タスク名をクリックすると、[タスク情報]ページが開きます。そのページでは、タスク作成者、タスク作成日時、およびタスクの影響を受けるデバイス等のタスク詳細を表示できます。また、詳細なタスク履歴情報も表示できます。
タスクのステータス	タスクのステータスを表示します。次に示すステータスがあります。 <ul style="list-style-type: none"> <li>成功：タスクは成功しました。</li> <li>失敗：タスクは失敗しました。</li> <li>重複：タスクが別のタスクと重複したため、実行されませんでした。</li> <li>スキップ：タスクを実行する時間に同一のタスクが既に実行されていたため、タスクをスキップしました。</li> <li>警告：すべてのタスクが失敗していなくても、グループタスクの一部のサブタスクが失敗しています。</li> </ul>
優先度	タスクの優先度を表示します。タスクの優先度レベルは1～5であり、1が最も高いタスク優先度レベルです。詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
スケジュール作成者	タスクをスケジュールリングしたユーザ（またはタスクを最後に変更したユーザ）のログイン名を表示します。
コメント	タスクについてのコメントを表示します。
アクション	各タスクに対して次のアクションを選択できます。 <ul style="list-style-type: none"> <li>詳細：[タスクの詳細]ページが開きます。そのページでタスクの詳細を表示できます。</li> <li>再実行：[タスクを編集]ページが開きます。そのページでタスクの編集や再実行ができます。このリンクは、タスクの再実行が可能となきのみ表示されます。</li> </ul>

## [デバイス関係]ページのフィールド

[デバイス関係]ページでは、親デバイス、ピアデバイス、子デバイスの関係を表示できます。一般にデバイス関係は、親デバイス、ピアデバイス、および子デバイスのデータを保持します。

デバイスの依存関係は、Device Relationships APIによって定義されます。たとえば、2つのデバイスがコンテキスト関係で定義される場合、その関係はコンテキスト管理機能によって保持されます。コンテキスト管理の詳細については、「[\[デバイスコンテキストを追加\]タスクページのフィールド](#)」(359 ページ)を参照してください。Device Relationship APIの詳細については、『NA CLI/API Command Reference』を参照してください。

関係する2つのデバイスはすべて、デバイス関係と呼ばれるものに参加します。たとえば、あるデバイスとの通信が別のデバイスを介してしか行うことができない場合、最初のデバイスが子となり、2番目のデバイスが親となります。したがって、親デバイスにアクセスできないと子デバイスにアクセスできません。

NAでは現在、デバイス関係という意味ではVMware ESXサーバのみをサポートしています。VMware ESXサーバへのアクセスにはCLIを使用します。ただし、サーバのシェルでは、VMware ESXサーバは他のLinuxサーバと非常に似ています。

VMware ESXサーバが特定されると、サーバ情報が[デバイス詳細]メニューの[モジュール]オプションから新しいデバイスに提供されます。「[\[デバイス詳細\]ページのフィールド](#)」(193 ページ)を参照してください。

これらの新しいデバイスは、これらのデバイスの親を介して所有する情報を使用することでこれらの新しいデバイスの情報にアクセスできるようになります。この場合、vSwitchは、それ自身がVMware ESXサーバによって実行されていることを認識します。このため、スナップショットタスクが実行されると、vSwitchにはVMware ESXサーバに関する既知の情報を使用してアクセスされます。つまり、VMware ESXサーバに直接接続される場合、またはデバイスに直接接続される場合があります。可能な限り、親に含まれるデバイスは実際のデバイスとして表示されます。

[デバイス関係]ページを開くには、[デバイス詳細]ページの[表示]メニューで[デバイス関係]をクリックします。

フィールド	説明/アクション
親デバイス	親デバイスを表示します。
ピアデバイス	ピアデバイスを表示します。
子デバイス	子デバイスを表示します。

親デバイス、ピアデバイス、または子デバイスを追加または削除するには、適切な列にある[追加]または[削除]リンクをクリックします。デバイスの追加の詳細については、「[デバイスの追加](#)」(106 ページ)を参照してください。

コンテキストをサポートしているデバイスの場合、[デバイスコンテキスト]ページに次の情報が表示されます。

- コンテキストのホスト名
- コンテキスト名
- コンテキストを削除するためのリンク
- 新しいコンテキストを追加するためのリンク詳細については、「[\[デバイスコンテキストを追加\]タスクページのフィールド](#)」(359 ページ) を参照してください。

**注意：** コンテキストを追加/削除するために必要な情報はドライバに埋め込まれています（必要な変数など）。これらの変数は追加タスクページまたは削除タスクページで提供されています。

## [デバイスソフトウェア履歴]ページのフィールド

[デバイスソフトウェア履歴]ページでは、デバイスに現在ロードされているソフトウェアを表示できます。

フィールド	説明/アクション
ホスト名	デバイスのホスト名を表示します。デバイスのホスト名をクリックすると[デバイス詳細]ページが開きます。このページでは、デバイスについての詳細な情報を確認できます。
デバイスIP	デバイスのIPアドレスを表示します。デバイスのIPアドレスをクリックすると[デバイス詳細]ページが開きます。このページでは、デバイスについての詳細な情報を確認できます。
最終アクセス時間	デバイスに最後にアクセスした日時を表示します（スナップショットの取得など）。
最後のスナップショットの結果	このデバイス構成の最後のスナップショットのステータスを表示します。スナップショットに失敗した場合は、[タスク結果]ページへのリンクがあります。
表示メニュー	[表示]メニューが開きます。詳細については、「 <a href="#">表示メニューオプション</a> 」(201 ページ) を参照してください。
編集メニュー	[編集]メニューが開きます。詳細については、「 <a href="#">編集メニューオプション</a> 」(230 ページ) を参照してください。
プロビジョニングメニュー	[プロビジョニング]メニューが開きます。詳細については、「 <a href="#">プロビジョニングメニューオプション</a> 」(239 ページ) を参照してください。
接続メニュー	[接続]メニューが開きます。詳細については、「 <a href="#">接続メニューオプション</a> 」(241 ページ) を参照してください。
変更日	ソフトウェアが最後に配布された日時を表示します。
変更者	デバイスに最後にソフトウェアを配布したユーザの名前を表示します。
変更後	デバイスで現在実行しているソフトウェアのバージョンを表示します。
デバイスソフトウェアのバージョン	デバイスで現在実行しているソフトウェアのバージョンを表示します。
変更前	ソフトウェアを配布する前にデバイスで実行されていたソフトウェアのバージョンを表示します。
ソフトウェアレベル	ソフトウェアレベルレーティングを表示します。詳細については、「 <a href="#">新規ソフトウェアレベルの追加</a> 」(433 ページ) を参照してください。
イメージセット	デバイスに最後に配布されたイメージセットの名前を表示します。イメージセットとは、デバイスに同時に配布できるイメージのグループのことです。イメージセットは1つ以上のイメージを含むことができます。

## [デバイスセッション]ページのフィールド

[デバイスセッション]ページでは、デバイスに関連する Telnet セッションおよび SSH セッションのリストを表示します。セッションには、セッション全体にロギングするコマンドまたはキーストロークのみを含むことができます。

フィールド	説明/アクション
開始日	セッションの開始日を表示します。
ステータス	セッションが開いているか閉じているかを表示します。
セッションタイプ	セッションが、Telnet経由かSSH経由かを表示します。
終了日	セッションの終了日を表示します。
作成者	セッションを開いたユーザのログイン名を表示します。
アクション	<div>各セッションに対して次のアクションを選択できます。</div> <ul style="list-style-type: none"><li>• 全 Telnet/SSH セッションを表示 : [Telnet/SSH セッション] ページが開きます。そのページには、当該セッションのコマンドおよびシステム応答が表示されます。また、当該セッションによって作成された構成がある場合は、その構成のテキスト表示も含まれます。</li><li>• コマンドのみ表示 : [Telnet/SSH セッション] ページが開きます。ただし、セッション中に入力されたコマンドのみを表示します。コマンドからスクリプトを作成する場合に便利です。</li></ul>

## 編集メニューオプション

メニューオプション	説明/アクション
スナップショットの取得	[タスクの新規作成] - [スナップショットの取得] ページが開きます。スナップショットタスクではスナップショットのスケジューリングができます。スナップショットでは、NA データベースに格納されているデバイス構成と関連データのコピーをリフレッシュします。特に、スナップショットでは、格納されている構成がデバイスのランニング構成と一致するかどうかを確認します。一致しない場合は、スナップショットタスクで、NA データベースに格納されているデバイス構成と関連データのコピーを置き換えます。詳細については、「 <a href="#">[スナップショットの取得]タスクページのフィールド</a> 」(315 ページ) を参照してください。
ドライバの検出	[タスクの新規作成] - [ドライバの検出] ページが開きます。ドライバの検出では、デバイスにドライバが割り当てられているかどうかを確認するタスクを作成します。割り当てられていない場合は、検出タスクで、NA データベースにある最も適切なドライバを現在のドライバに上書きします。(注意: NA では、各デバイスとの通信にドライバが必要です。) 詳細については、「 <a href="#">[ドライバの検出]タスクページのフィールド</a> 」(293 ページ) を参照してください。
構成を編集して配布	現在の構成で、[構成を編集] ページを開きます。そのページで、構成の編集と配布ができます。[デバイスに配布] オプションをクリックすると、構成配布をスケジューリングできます。また、構成配布をすぐに開始することもできます。NA は、構成変更をデバイスに配布して、結果の構成を取り込みます。このタスクの[タスク結果] ページは、タスク実行中に自動的にリフレッシュします。詳細については、「 <a href="#">[構成を配布]タスクページのフィールド</a> 」(181 ページ) を参照してください。
インライン構成コメントを編集	[構成を編集] ページが開きます。そのページで、コメントを入力できます。コメントには通常、2つの感嘆符 (!!) を接頭部に付けます。パーシステントコメント文字は2文字のみです。ただし、区切り文字として複数のコメント文字を使用するデバイスもあります。これにより、コメントエンジンではパーシステントコメントの解析が困難になります。
デバイスを編集	[デバイスを編集] ページが開きます。そのページでデバイスの情報を編集できます。詳細については、「 <a href="#">[デバイスの編集]ページのフィールド</a> 」(111 ページ) を参照してください。
管理対象IPアドレスを編集	[デバイス管理対象IPアドレス] ページが開きます。そのページでは、デバイスへのアクセスに使用する可能性があるすべてのIPアドレス情報について、表示および変更ができます。各デバイスを一意に特定するプライマリIPアドレスが1つ必要です。ただし、NA がそのデバイスに接続できる可能性を大きくする目的で、代替IPアドレスを追加することができます。代替IPアドレスを使用することで、管理のオーバーヘッドを減らし、デバイスデータの質が高まります。(注意: プライマリIPアドレスを使用してNA がデバイスへのアクセスに失敗した場合は、代替IPアドレスをリスト順に試行します。ネットワーク効率を確保するには、アクセスできる可能性が最も高いIPアドレスをリストの最上部に移動します)。詳細については、「 <a href="#">[デバイス管理対象IPアドレス]ページのフィールド</a> 」(232 ページ) を参照してください。
デバイスをアクティブ化/非アクティブ化	デバイスの管理または管理解除をします。
デバイスを削除	ダイアログボックスが開きます。そこで、NA データベースから完全にデバイスを削除するかどうかを確認できます。NA データベースから完全にデバイスを削除すると、そのデバイスの構成履歴は失われます。そのかわりに、デバイスを非アクティブに編集して、構成履歴を保存することができます。

メニューオプション	説明/アクション
新規デバイスとして保存	<p>既存のデバイスを使用して、次の情報を[デバイスの追加]、および[デバイステンプレートの追加]ページに事前入力できます。</p> <ul style="list-style-type: none"> <li>• グループ</li> <li>• ドライバ</li> <li>• パスワード情報</li> <li>• 接続情報</li> <li>• モデル</li> <li>• ベンダー</li> </ul> <p>詳細については、「<a href="#">[デバイスの新規作成]ページのフィールド</a>」(106ページ)を参照してください。</p>
新規テンプレートとして保存	<p>既存のデバイスを使用して、次の情報を[デバイステンプレートの追加]ページに事前入力できます。</p> <ul style="list-style-type: none"> <li>• 構成ファイル</li> <li>• ドライバ</li> <li>• 接続情報</li> <li>• モデル</li> <li>• ベンダー</li> <li>• 階層レイヤ</li> </ul> <p>詳細については、「<a href="#">[デバイステンプレート]ページのフィールド</a>」(118ページ)を参照してください。</p>
メッセージの新規作成	<p>[メッセージの新規作成]ページが開きます。デバイスを参照するすべてのNAユーザに、メッセージをポストすることができます。[シングルビュー]を使用するイベントを追跡することもできます。詳細については、「<a href="#">イベントの連結ビュー (シングルビュー)</a>」(546ページ)を参照してください。</p>
プロセス自動化	<p>[HP Operations Orchestration ログイン]ページが開きます。このページでは、HP Operations Orchestration にログインしたり、HP Operations Orchestration フローをガイドモードで起動できます。HP Operations Orchestration ユーザ認証の詳細については、「<a href="#">ユーザ認証</a>」(73ページ)を参照してください。HP Operations Orchestration の詳細については、『HP Operation Orchestration User's Guide』を参照してください。</p>

## [デバイス管理対象IPアドレス]ページのフィールド

[管理対象デバイスIPアドレス]ページでは、デバイスへのアクセスに使用する可能性があるすべてのIPアドレスについて、表示および変更ができます。各デバイスを一意に特定するプライマリIPアドレスが1つ必要です。

以下の項目使用してデバイスに接続できます。

- プライマリIPアドレス
- 任意の数のセカンダリIPアドレス（デバイスによる提供、または手動入力による）
- コンソールサーバのIPアドレスとポート
- 要塞ホスト
- ホップボックス
- 別のデバイスのIPアドレス

フィールド	説明/アクション
要塞ホストの定義	<p>デバイスに要塞ホストが定義されていない場合、[IPアドレスの新規作成]ページが開きます。詳細については、<a href="#">「[IPアドレスの新規作成]ページ（要塞ホスト）」（234ページ）</a>を参照してください。デバイスに要塞ホストが定義されていない場合、次の2つの追加リンクが表示されます。</p> <ul style="list-style-type: none"> <li>• 要塞ホストの編集</li> <li>• 要塞ホストの削除</li> </ul>
IPアドレスの新規作成	<p>[IPアドレスの新規作成]ページが開きます。詳細については、<a href="#">「[IPアドレスの新規作成]ページ（カスタムIPアドレス）」（235ページ）</a>を参照してください。NATまたはそのほかのアドレッシングスキームを使用する場合は、NAに自動検出されないIPアドレスを追加することをお勧めします。ここで追加するIPアドレスには、「custom」というラベルが付きます。</p>
コンソールサーバの新規作成	<p>[IPアドレスの新規作成]ページが開きます。詳細については、<a href="#">「[IPアドレスの新規作成]ページ（コンソールサーバ）」（236ページ）</a>を参照してください。</p>
ホップボックスの新規作成	<p>[IPアドレスの新規作成]ページが開きます。詳細については、<a href="#">「[IPアドレスの新規作成]ページ（ホップボックス）」（237ページ）</a>を参照してください。</p>
新規接続スルー	<p>[IPアドレスの新規作成]ページが開きます。詳細については、<a href="#">「[IPアドレスの新規作成]ページ（新規接続スルー）」（238ページ）</a>を参照してください。</p>
最後に使用したIPのリセット	<p>最後に使用したIPアドレスをリセットできます。</p>
ポートIP	<p>デバイスのポートIPアドレス（プライマリ、代替、またはカスタム）を表示します。（デバイス構成の分析により入力されたすべてのIPアドレスは「代替」として表示されます。）</p>
デバイスへのアクセスに使用	<p>[はい]または[いいえ]が表示されます。NASは最初にプライマリIPアドレスでデバイスへのアクセスを試みます。次に、コンソールサーバアドレス（ある場合）で、最後に、このフィールドに[はい]と表示されている代替IPアドレスでアクセスします（デフォルトは[いいえ]）。</p>
タイプ	<p>IPアドレスのタイプ（プライマリ、代替、またはカスタム）を表示します。[デバイスの新規作成]ページまたは[デバイスを編集]ページからのIPアドレスは、常にプライマリIPアドレスです。検出された追加のIPアドレスは代替アドレスです。[IPアドレスの新規作成]リンクを使用してIPアドレスを追加した場合、そのアドレスはカスタムIPアドレスとみなされます。</p>



フィールド	説明/アクション
領域名	領域名を表示します。領域名は、ゲートウェイから返されます。領域名は、ゲートウェイのインストール時に設定され、NAでは変更できません。
アクション	<p>各デバイスに対して次のアクションを選択できます。</p> <ul style="list-style-type: none"><li>• <b>編集</b>：プライマリIPアドレス用の[デバイスを編集]ページが開きます。そのページで、IPアドレスとサブネットマスクを変更できます。また、新規アクセスの順番で、新規IPアドレスをプライマリIPアドレスの前に挿入できます。さらに、変更コメントもできます。このページは、代替、NAT、TFTPサーバ、およびカスタムIPアドレスの場合に表示されます。詳細については、「<a href="#">[デバイスの編集]ページのフィールド</a>」(111ページ)を参照してください。デバイスに手動で追加されたIPアドレスのみを削除できます。その他すべてのIPアドレスでは、[IPアドレスの新規作成]ページが表示されます。「<a href="#">[IPアドレスの新規作成]ページ</a>」(235ページ)を参照してください。</li><li>• <b>上へ移動</b>：リストに複数の代替IPアドレスが表示されているときに、このオプションを使用してIPアドレスをリストの上部へ移動します。NAは、リスト順に代替アドレスを試行します。(注意：このオプションは、セカンダリIPアドレス、カスタムIPアドレス、およびホップボックスIPアドレスの場合のみ利用できます。プライマリ、およびコンソールIPアドレスはソートできません。)</li><li>• <b>下へ移動</b>：リストに複数の代替IPアドレスが表示されているときに、このオプションを使用してIPアドレスをリストの下部へ移動します。NAは、リスト順に代替アドレスを試行します。(注意：このオプションは、セカンダリIPアドレス、カスタムIPアドレス、およびホップボックスIPアドレスの場合のみ利用できます。プライマリ、およびコンソールIPアドレスはソートできません。)</li></ul>

## [IPアドレスの新規作成]ページ（要塞ホスト）

[デバイス管理対象IPアドレス]ページで、[要塞ホストの編集]リンクをクリックすると、[IPアドレスの新規作成]ページが開きます。要塞ホストはLinuxシステムまたはSolarisシステムで使用できます。

**注意：** 要塞ホストを構成すると、デバイスへのすべてのアクセス試行（コンソールサーバへのアクセスを含む）は、最初に要塞ホストと呼ばれる中間ホストにログインし、その後にデバイスへの接続を試みます。

フィールド	説明/アクション
要塞ホストIPアドレスの値	要塞ホストのIPアドレスを入力します。ホスト名を入力することもできます。この場合、NAがIPアドレスに解決します。
ユーザ名	要塞ホストへのアクセスに使用するユーザ名を入力します。
パスワード	要塞ホストへのアクセスに使用するパスワードを入力します。
パスワードの確認	確認のためのパスワードを再入力します。
デバイス接続方法	要塞ホストへのログイン後のデバイスへのアクセス方法を入力します。SSH、またはTelnetです。
接続スクリプト変数	接続スクリプトをカスタマイズするための変数のセットを入力します。NAが中間ホストに接続したことを判断するのに検索されるデフォルトのプロンプトパターン（正規表現）は、 <code>(\x23 \x24 %)</code> です。これは、 <code>'#'</code> 、 <code>'\$'</code> 、または <code>'%'</code> に変換されます。（ <b>注意：</b> フィールドを空欄にしておくと、デフォルトの変数が使用されます。ほとんどのUnix要塞ホストでデフォルトの変数が使用できます。）
コメント	必要に応じてコメントを入力します。

## [IPアドレスの新規作成]ページ（カスタムIPアドレス）

[デバイス管理対象IPアドレス]ページで、[IPアドレスの新規作成]リンクをクリックすると、[IPアドレスの新規作成]ページが開きます。

フィールド	説明/アクション
カスタムIPアドレスの値	新しいIPアドレスを入力します。ホスト名を入力することもできます。この場合、NAがIPアドレスに解決します。
デバイスアクセス	デバイスアクセスを使用すると、カスタムIPアドレスを使用してデバイスにアクセスできます。次のオプションのいずれかを選択します。 <ul style="list-style-type: none"><li>• [いいえ]：デバイスにアクセスするのにIPアドレスは使用されません。</li><li>• [はい]：デバイスにアクセスするのにIPアドレスが使用されます。</li><li>• [のみ]：デバイスにアクセスするのにこのIPアドレス（パス）のみを使用します。他のすべてのデバイスのデバイスアクセスは[いいえ]に設定されます。</li></ul>
コメント	必要に応じてコメントを入力します。

## [IP アドレスの新規作成] ページ（コンソールサーバ）

[デバイス管理対象 IP アドレス] ページで、[コンソールサーバの新規作成] リンクをクリックすると、[IP アドレスの新規作成] ページが開きます。

**注意：** Telnet が有効であるコンソールサーバがポートに基づいてデバイスへの自動パススルーを提供する場合、コンソールサーバが使用されます。このオプションは Telnet でのみ機能します。コンソールサーバを有効にすると、デバイスへの Telnet が自動的に有効になります。

フィールド	説明/アクション
Console IP アドレスの値	新しいコンソール IP アドレスを入力します。ホスト名を入力することもできます。この場合、NA が IP アドレスに解決します。
コンソールポート	コンソールサーバのコンソールポートを入力します。
デバイスアクセス	デバイスアクセスを使用すると、コンソールサーバを使用してデバイスにアクセスできます。次のオプションのいずれかを選択します。 <ul style="list-style-type: none"><li>• [いいえ]：デバイスにアクセスするのに IP アドレスは使用されません。</li><li>• [はい]：デバイスにアクセスするのに IP アドレスが使用されます。</li><li>• [のみ]：デバイスにアクセスするのにこの IP アドレス（パス）のみを使用します。他のすべてのデバイスのデバイスアクセスは [いいえ] に設定されます。</li></ul>
コメント	必要に応じてコメントを入力します。

## [IPアドレスの新規作成]ページ（ホップボックス）

[デバイス管理対象IPアドレス]ページで、[ホップボックスの新規作成]リンクをクリックすると、[IPアドレスの新規アドレス]ページが開きます。

ホップボックスは、デバイスに接続するための「要塞ホスト」スクリプトを一般的に使用します。要塞ホストとは異なり、[ホップボックス]オプションでは中間ホストへのログイン後に使用するIPアドレスを指定する必要があります。ホップボックスパスは、最初に指定された要塞ホストにはアクセスしません。

フィールド	説明/アクション
Hop Box IPアドレスの値	ホップボックスのIPアドレスを入力します。ホスト名を入力することもできます。この場合、NAがIPアドレスに解決します。
対象IP (ホップボックスから)	ホップボックスからアクセスするIPアドレスを入力します。
ユーザ名	ホップボックスへのアクセスに使用するユーザ名を入力します。
パスワード	ホップボックスへのアクセスに使用するパスワードを入力します。
パスワードの確認	確認のためのパスワードを再入力します。
デバイス接続方法	ホップボックスへのログイン後のデバイスへのアクセス方法を入力します。SSH、またはTelnetです。
接続スクリプト変数	接続スクリプトをカスタマイズするための変数のセットを入力します。NAが中間ホストに接続したことを判断するのに検索されるデフォルトのプロンプトパターン（正規表現）は、 <code>(\x23 \x24 %)</code> です。これは、'#'、'\$'、または '%' に変換されます。（ <b>注意</b> ：フィールドを空欄にしておくと、デフォルトの変数が使用されます。ほとんどのUnix要塞ホストでデフォルトの変数が使用できます。）
コメント	必要に応じてコメントを入力します。

## [IP アドレスの新規作成] ページ（新規接続スルー）

[デバイス管理対象 IP アドレス] ページで、[新規接続スルー] リンクをクリックすると、[IP アドレスの新規作成] ページが開きます。

[新規接続スルー] オプションを使用すると、あるデバイスに別のデバイス経由で接続できます。このオプションは CLI を介してのみサポートされます。SNMP はサポートされません。

**注意：** [新規接続スルー] は、NA に既に存在するデバイスにのみ使用できます。

Telnet と SSH を使用する場合、次の 4 つの組み合わせが考えられます。

- デバイス B（SSH）を介したデバイス A（SSH）へのアクセス
- デバイス B（Telnet）を介したデバイス A（SSH）へのアクセス
- デバイス B（SSH）を介したデバイス A（Telnet）へのアクセス
- デバイス B（Telnet）を介したデバイス A（Telnet）へのアクセス

したがって、デバイス B を介してデバイス A に接続する場合、新規接続スルーは自動的にデバイス B を追加します。NA モジュールステータス診断の一部として、検出されたすべてのコンテキストがデバイスとして自動的に追加され、接続パスが自動的に構成されます。デバイスコンテキストの詳細については、[「\[デバイスコンテキストを追加\] タスクページのフィールド」](#)（359 ページ）を参照してください。

フィールド	説明/アクション
接続スルー IP アドレスの値	接続スルーに使用する新規 IP アドレスを入力します。
デバイスアクセス	<p>デバイスアクセスを使用すると、IP アドレスを使用してデバイスにアクセスできます。SCP は使用できないので注意してください。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [いいえ]：デバイスにアクセスするのに IP アドレスは使用されません。</li> <li>• [はい]：デバイスにアクセスするのに IP アドレスが使用されます。</li> <li>• [のみ]：デバイスにアクセスするのにこの IP アドレス（パス）のみを使用します。他のすべてのデバイスのデバイスアクセスは [いいえ] に設定されます。</li> </ul>
コメント	必要に応じてコメントを入力します。

# プロビジョニングメニューオプション

メニューオプション	説明/アクション
テンプレートからデバイスをプロビジョニング	[デバイステンプレート] ページが開きます。このページでは、このデバイスのデバイステンプレートを表示できます。詳細については、「 <a href="#">[デバイステンプレート] ページのフィールド</a> 」(118 ページ) を参照してください。
ポリシー準拠の確認	[タスクの新規作成 - ポリシー準拠の確認] ページが開きます。そのページで、デバイスの構成とソフトウェアが現在のポリシーに準拠しているかを表示できます。「 <a href="#">[ポリシー準拠の確認] タスクページのフィールド</a> 」(372 ページ) を参照してください。
Syslog の構成	[タスクの新規作成 - Syslog の構成] ページを開きます。そのページで、リアルタイム変更検出のために、デバイス上で自動的に Syslog を構成できます。「 <a href="#">[Syslog の構成] タスクページのフィールド</a> 」(284 ページ) を参照してください。
ACL の削除	[新規タスク - ACL の削除] ページが開きます。そのページで ACL を削除できます。「 <a href="#">ACL の削除</a> 」(707 ページ) を参照してください。
パスワードの配布	[タスクの新規作成 - パスワードの配布] ページが開きます。そのページで、パスワード変更をデバイスへ配布するタスクを設定できます。「 <a href="#">[パスワードの配布] タスクページのフィールド</a> 」(288 ページ) を参照してください。
デバイスのリブート	[タスクの新規作成 - デバイスのリブート] ページが開きます。そのページで、NA データベース内のデバイスをリブートできます。「 <a href="#">[デバイスのリブート] タスクページのフィールド</a> 」(296 ページ) を参照してください。
ICMP テストの実行	[タスクの新規作成 - ICMP テストの実行] ページが開きます。あるデバイスから1台または複数のデバイスに対する ping、または traceroute テストをスケジューリングできます。「 <a href="#">[ICMP テストの実行] タスクページのフィールド</a> 」(299 ページ) を参照してください。
コマンドスクリプトの実行	[新規タスク - コマンドスクリプトの実行] ページが開きます。そのページで、デバイスのコマンドスクリプトの編集とスケジューリングができます。「 <a href="#">[コマンドスクリプトの実行] タスクページのフィールド</a> 」(304 ページ) を参照してください。
診断の実行	[新規タスク - 診断の実行] ページが開きます。そのページで、デバイスの診断をスケジューリングできます。「 <a href="#">[診断の実行] タスクページのフィールド</a> 」(310 ページ) を参照してください。
スタートアップとランニングの同期	[新規タスク - スタートアップとランニング構成の同期] ページが開きます。そのページで、デバイスのスタートアップとランニング構成を同期化できます。「 <a href="#">[スタートアップとランニングの同期] タスクページのフィールド</a> 」(319 ページ) を参照してください。
デバイスソフトウェアの更新	[新規タスク - デバイスソフトウェアの更新] ページが開きます。そのページで、1つ以上のデバイスへのソフトウェアの配布がスケジューリングできます。「 <a href="#">[デバイスソフトウェアの更新] タスクページのフィールド</a> 」(323 ページ) を参照してください。
VLAN の新規作成	[タスクの新規作成] ページが開きます。そのページで、ネットワークスイッチ上に VLAN を構成できます。詳細については、「 <a href="#">[VLAN タスク] ページのフィールド</a> 」(363 ページ) を参照してください。
OS 分析	[OS 分析] タスクページが開きます。このページは、sysoid (デバイスモデルの一意の識別子)、OS バージョン、フラッシュストレージオプション、モジュール、その他などの Cisco デバイスに関する情報を収集します。詳細については、「 <a href="#">[OS 分析] タスクページのフィールド</a> 」(350 ページ) を参照してください。
デバイスコンテキスト	[タスクの新規作成] ページが開きます。そのページで、デバイスコンテキストを作成できます。コンテキストとはデバイス内部にあるデバイスを指します。コンテキストには (モジュールやスロットがある) ハードウェアや仮想があります。NA は、デバイスコンテキストを使用して、親デバイスと子デバイスの間の関係を自動的に追加します。NA では IP アドレスを設定するためのコンテキストは必要ありません。それどころか、コンテキストへのスルーパス接続を構成することが可能で、これにより NA でコンテキストを管理することができます。詳細については、「 <a href="#">[デバイスコンテキストを追加] タスクページのフィールド</a> 」(359 ページ) を参照してください。

メニューオプション	説明/アクション
ポートスキャン	[タスクの新規作成]: [ポートスキャンタスク]ページが開きます。このページでは、Nmapでネットワークデバイスを検出できます。また、Nmapを使用して、デバイスのポートをスキャンして、開いているポート、およびポートが提供するサービスの内容についての詳細を返すことも可能です。詳細については、「 <a href="#">[ポートスキャン]ページのフィールド</a> 」(353ページ)を参照してください。



## 接続メニューオプション

NAでは、TelnetプロトコルまたはSSHプロトコルを使用するネットワークデバイスへの、シングルサインオンをサポートしています。NAサーバは、Telnet/SSHプロキシとしての役割を果たします。移動したデータは、クリアテキスト形式です。

NAサーバをTelnet/SSHプロキシとして使用しない場合は、セキュアURLを通じて、あるいは標準のTelnetコマンドを使用して、デバイスに直接ログインできます。

メニューオプション	説明/アクション
Telnetを使用する プロキシ経由	[Telnet]ウィンドウが開きます。そのウィンドウで、デバイスに対してTelnetコマンドを入力できます。
SSHを使用する プロキシ経由	[SSH]ウィンドウが開きます。そのウィンドウで、デバイスに対してSSHコマンドを入力できます。



## 第6章：ユーザの管理

### トピックの参照先リスト

トピック	参照先：
ユーザの追加	<a href="#">「ユーザの追加」(244 ページ)</a>
電子メール通知	<a href="#">「電子メール通知」(246 ページ)</a>
ユーザパスワードの構成	<a href="#">「ユーザパスワードの構成」(250 ページ)</a>
ユーザグループの追加	<a href="#">「ユーザグループの追加」(253 ページ)</a>
新規ユーザロールの追加	<a href="#">「ユーザロールの追加」(257 ページ)</a>
ユーザ設定の編集	<a href="#">「ユーザ設定の編集」(260 ページ)</a>
クイック起動	<a href="#">「クイック起動とは」(265 ページ)</a>
NA ホームページのカスタマイズ	<a href="#">「NA ホームページのカスタマイズ」(269 ページ)</a>
検索/接続機能	<a href="#">「検索/接続機能」(273 ページ)</a>

## ユーザの追加

ユーザの認証と認可の設計は難しい作業です。選択内容により、HP Network Automation（NA）の使用方法が影響を受けます。適切な認証と認可の設計を採用することで、数多くのセキュリティリスクが減少します。

情報セキュリティとIT部門の両者を考慮したベストプラクティスには、通常、「最小権限」という概念があります。「最小権限」とは、作業の実行に必要な最小限の権利を各ユーザに割り当てることを意味します。さらに、組織の性質によっては、各ユーザが実行可能なタスクを、その役割ごとに適切に分ける環境を作成することもあります。

このセクションでは、次の用語を使用します。

- 同一のセキュリティ権限を共有するグループに、ユーザ进行分类することです。ロールを割り当てられたユーザは、そのロールで定義している権限を付与されます。たとえば、デバイスの追加、構成ポリシーの管理、ソフトウェアの配布など、ある処理を実行する権限がユーザに与えられた場合、NAでは、リソースにアクセスするための固定ロールIDを使用します。開始点として既存のロールを使用するのではなく、最初から新規ユーザロールを作成して、アクションタイプごとにデフォルトの拒否権限があるテンプレートを作成します。これにより、セキュリティのベストプラクティスである「最小権限」に沿った形で、簡単にロールを作成できます。
- ユーザグループ：ユーザ管理を目的とした論理コンテナです。システム管理者はユーザにユーザグループを割り当てることができます。また、特定のロールもマッピングできます。ユーザグループには、1つ以上のロールを割り当てることができます。



新規ユーザを追加するには、[管理]メニューバーから[ユーザ]をクリックします。[全ユーザ]ページが開きます。ページの上にある[ユーザの新規作成]リンクをクリックします。[ユーザの新規作成]ページが開きます。「[\[ユーザの新規作成\]ページのフィールド](#)」（247ページ）を参照してください。

**注意：** [管理]の下にある[ユーザの新規作成]オプションをクリックして、[ユーザの新規作成]ページに移動することもできます。

**注意：** CSV ファイルから、新規のユーザや既存ユーザの変更をインポートできます。詳細については、「[\[ユーザのインポート\]タスクページのフィールド](#)」（334ページ）を参照してください。

## [全ユーザ]ページのフィールド

フィールド	説明
ユーザの新規作成	[ユーザの新規作成]ページが開きます。このページでユーザを追加できます。詳細については、「 <a href="#">[ユーザの新規作成]ページのフィールド</a> 」（247ページ）を参照してください。ユーザを追加できるのは、システム管理者のみです。
ユーザの検索	[ユーザの検索]ページが開きます。このページで、名、姓、電子メールアドレス、AAAユーザ名などでユーザを検索できます。詳細については、「 <a href="#">ユーザの検索</a> 」（520ページ）を参照してください。

フィールド	説明
ログオンしているユーザ	[ログオンしているユーザ]ページが開きます。このページで、現在ログインしているユーザのユーザ名、ユーザホスト、最終アクセス時間などを表示できます。このときに、コマンドラインインターフェイス (CLI) ではなく、Web UI を使用してログインしているユーザのみを表示します。(注意:[管理]のドロップダウンメニューから[ログオンしているユーザ]を選択して、このページを表示することもできます)。詳細については、「 <a href="#">[ログオンしているユーザ]ページのフィールド</a> 」(246 ページ) を参照してください。
ユーザグループ	[ユーザグループ]ページが開きます。このページで、ユーザグループの追加や編集ができます。詳細については、「 <a href="#">[ユーザグループ]ページのフィールド</a> 」(253 ページ) を参照してください。
[ユーザのロールと権限]リンク	[ユーザのロールと権限]ページが開きます。このページで、ユーザ権限を編集できます。詳細については、「 <a href="#">[ユーザのロールと権限]ページのフィールド</a> 」(257 ページ) を参照してください。
このグループのユーザ	次のアイコンを表示します。 <ul style="list-style-type: none"> <li> 通常のユーザアカウント</li> <li> 無効のユーザアカウント</li> </ul>
ユーザ名	ユーザの姓名を表示します。
名	ユーザの名前を表示します。
姓	ユーザの姓を表示します。
電子メール	ユーザの電子メールアドレスを表示します。
アクション	次のオプションを選択できます。 <ul style="list-style-type: none"> <li>編集:[ユーザを編集]ページが開きます。アカウントがユーザ自身のものである場合、[自分のプロフィール]ページが開きます。[自分のプロフィール]ページでパスワードオプションを表示できるのは、管理グループのユーザのみです。詳細については、「<a href="#">[自分のプロフィール]ページのフィールド</a>」(260 ページ) を参照してください。[ユーザリスト]ページには、自分のプロフィールへの変更内容が表示されます。</li> <li>削除:ユーザを削除できます (システム管理権限を使用)。</li> <li>権限:[ユーザ権限]ページが開きます。このページの最上部にある[ユーザプロフィールの編集]をクリックすると、[ユーザの編集]ページが開きます。ユーザプロフィールに変更を加え、[保存]をクリックして保存することができます。[ユーザリスト]ページに変更内容が表示されます。詳細については、「<a href="#">[ユーザの新規作成]ページのフィールド</a>」(247 ページ) を参照してください。</li> <li>構成変更:[構成検索結果]ページが開きます。ユーザによる構成変更がある場合は、このページで内容を表示します。詳細については、「<a href="#">デバイス構成変更の表示</a>」(172 ページ) を参照してください。</li> </ul>

## [ログオンしているユーザ]ページのフィールド

[ログオンしているユーザ]ページでは、現在NAにログインしているユーザのユーザ名、電子メールアドレス、ユーザのホストシステム、ホストシステムへの最終アクセス日時を表示できます。このページには、コマンドラインインターフェイス（CLI）ではなく、NA UIを使用してログインしているユーザのみが表示されます。

フィールド	説明/アクション
ユーザ名	ユーザ名を表示します。
電子メールアドレス	ユーザの電子メールアドレスを表示します。ログインしているユーザとの間で電子メールメッセージを送受信するには、「 <a href="#">電子メール通知</a> 」(246ページ)を参照してください。
ユーザホスト	ユーザがログインしているシステムのホストIPアドレスを表示します。
最終アクセス時間	ユーザがシステムに最後にアクセスした日時を表示します。

## 電子メール通知

NAにログインしているとき、ログインしている1人以上のNAユーザにメッセージを送信できます。自分のメッセージは削除できます。NAをログアウトすると、すべてのメッセージが自動的に削除されます。

**注意：**メッセージはNA UIフレームワークで通信されるため、APIを使用してこの機能を実装することはできません。データベースにはアクセスできません。

メッセージを送信するには：

1. [管理]メニューで[ログオンしているユーザ]をクリックします。[ログオンしているユーザ]ページが開きます。
2. メッセージを送信するユーザのチェックボックスをオンにします。[選択]ドロップダウンメニューからすべてのユーザを選択できます。
3. [アクション]ドロップダウンメニューから[メッセージを送信]を選択します。[メッセージの送信]ページが開きます。
4. [メッセージ]フィールドにメッセージテキストを入力します。
5. メッセージテキストを入力し終わったら、[送信]ボタンをクリックします。メッセージが正常に送信されると、[ログオンしているユーザ]ページの上部に「メッセージが送信されました。」と表示されます。

メッセージを読むには：

1. 新しいメッセージがある場合、NA UIの左側のフレーム上部の[新しいメッセージが到着しました]リンクをクリックします。メッセージが送信者と送信日時とともに表示されます。メッセージに返信するか、削除できます。

**注意：**すべてのメッセージを読み終わると、[新しいメッセージが到着しました]リンクが[メッセージを表示]に変わります。メッセージはすべて、送信された順に表示されます。

2. [返信]ボタンをクリックすると、[メッセージを送信]ページが開き、メッセージに返信できます。[削除]ボタンをクリックすると、メッセージが削除されます。

メッセージに返信する場合、NA では元のメッセージ送信者の UserID が使用されます。新しいメッセージの SenderID は自動的に自分になります。

1. メッセージの下に[返信]ボタンを選択します。[メッセージの送信]ページが開きます。
2. メッセージテキストを入力し、[送信]ボタンをクリックします。メッセージの送信先であるユーザの NA UI の左側フレームの上部に、[新しいメッセージが到着しました]リンクが表示されます。

## [ユーザの新規作成]ページのフィールド

ユーザの追加を初めて行うとき、このページは、[管理]アカウント情報以外は空白です。このページでの作業を完了し保存した後に、情報を編集したい場合は、[ユーザを編集]ページで編集できます。[ユーザを編集]ページのフィールドは、[ユーザの新規作成]ページのフィールドと同じです。

フィールド	説明/アクション
<b>ユーザ情報</b>	
ユーザ名	ユーザの NA ユーザ名を入力します。このユーザ名は、オペレータまたは管理者などで NA へログインするときに使用します。 <b>注意:</b> ユーザ名には、英数字、ピリオド (.)、アンダースコア (_)、ハイフン (-)、およびバックスラッシュ (\) のみ使用できます。
パスワード	ユーザの NA パスワードを入力します。これは、NA にログインするときに使用するパスワードです。パスワードの設定の詳細については、「 <a href="#">ユーザパスワードの構成</a> 」(250 ページ) を参照してください。
パスワードの確認	確認用にユーザの NA パスワードを入力します。
パスワードオプション	次の中からオプションを1つ以上選択します。 <ul style="list-style-type: none"> <li>• ユーザは次回ログオン時にパスワードを変更する必要あり</li> <li>• ユーザによるパスワードの変更を禁止</li> <li>• パスワードの有効期限なし</li> <li>• アカウントをロックアウト</li> </ul> <p>パスワードオプションの設定の詳細については、「<a href="#">ユーザパスワードの構成</a>」(250 ページ) を参照してください。</p>
名	ユーザの名を入力します。
姓	ユーザの姓を入力します。
電子メールアドレス	ユーザの電子メールアドレスを入力します。

フィールド	説明/アクション
ユーザが所属するグループ	<p>ユーザが属するユーザグループを、次に示すデフォルトのユーザグループから1つまたは複数を選択します。これらのグループで、ユーザのユーザロールと関連するすべての権限が付与されます。デフォルトではNAはグループを割り当てません。グループに属さないユーザは、デバイスや構成変更の表示など限られたタスクしか実行できません。(注意：新規グループを作成した場合は、リストにそのグループが表示されます)。</p> <ul style="list-style-type: none"> <li>• 制限付きアクセスユーザ：通常は、ネットワークデバイスを構成するためのパスワードを持たないオペレータのことです。デバイスを表示する権限はありますが、NA データベースの情報の大半を修正できません。また、バッチ処理やネットワークデバイスを再構成する処理も実行できません。</li> <li>• フルアクセスユーザ：通常は、ネットワーク内の複数のデバイス（全デバイスとは限りません）を構成するパスワードを持つ、信頼できるネットワークエンジニアのことです。フルアクセスユーザには、NA データベース内の大半の情報を修正できる権限があり、一括モードではなく、デバイスを1つずつ再構成することができます。多くの場合、再構成する権限を持つことができるデバイスは制限されます。</li> <li>• パワーユーザ：通常は、大半のアクションの実行を許可されているエキスパートエンジニアのことです。デバイスのグループについて再構成したり、アクションを実行したりできます。</li> <li>• 管理者：ユーザ管理、ポリシー設定、ネットワーク全体の処理の実行など、NA を管理する責任を負います。管理者には、すべてのデバイスに対するすべてのアクションを実行できる権限があります。</li> <li>• 全パーティションの表示：ユーザがすべてのパーティションを表示できるようになります。パーティションとは、NA デバイスのセットのことです。各パーティションは、1つのNA コアにのみ属します。このため、パーティションを管理するNA コアは1つのみになります。さらに、各デバイスは1つのパーティションにのみ属します。パーティションの構成の詳細については、「<a href="#">デバイスとユーザのセグメント化</a>」(148 ページ) を参照してください。</li> </ul>
サイト	<p>このユーザが属するパーティションを選択します。ユーザは、当該パーティションへの表示権限を持つ他のユーザにしか見えません。</p> <p><b>注意：</b>ユーザが1つのパーティションにしかアクセスできない場合、[サイト] ドロップダウンメニューは使用できません)。</p>
デフォルト	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 有効：アカウントは有効です（デフォルト）。</li> <li>• 無効：アカウントは無効です。このオプションを使用して、システム上にアカウントを残したまま、そのアカウントを無効にすることができます。</li> </ul>
外部認証フェイルオーバー	<p>外部認証サーバに到達できない場合に、認証をローカル認証にフェイルオーバーできます。</p>
コメント	<p>アカウントについてのコメントを入力します。</p>
<b>AAA</b>	
AAAユーザ名	<p>ユーザのAAA（TACACS+またはRADIUS）ユーザ名を入力します。これにより、NAでAAAユーザ名とNAユーザ名とを関連付けることができます。NAがローカル認証にフェイルオーバーを行うようにするには、ユーザのアカウントでこの機能を有効にする必要があります。デフォルトでは、NAはローカル認証にフェイルオーバーしません。</p>
AAAパスワード	<p>ユーザのAAAパスワードを入力します。</p>
AAAパスワードの確認	<p>確認用にAAAパスワードを再入力します。</p>



フィールド	説明/アクション
[プロキシインターフェイスでのAAAログインの使用]チェックボックス	オンにすると、ユーザがTelnet/SSH プロキシにログインするときに、NAがユーザのAAA 資格情報を確認します。

### SecurID

新規ユーザが追加されたあとでそのユーザ情報を編集するときに、[ソフトウェアトークンの管理]ページへのリンクが表示されます。ソフトウェアトークンの管理ページでは、ユーザのログインに関連付けられるソフトウェアトークンライセンスを追加することができます。詳細については、「[SecurID ソフトウェアトークンの追加](#)」(630ページ)を参照してください。

---

## ユーザパスワードの構成

次のオプションは、ユーザプロファイルの新規作成または既存のユーザプロファイルの編集を行うためのユーザパスワード設定権限を持つNAユーザの[ユーザの新規作成]ページと[ユーザを編集]ページに表示されます。

- ユーザは次回ログオン時にパスワードを変更する必要あり
- ユーザによるパスワードの変更を禁止
- パスワードの有効期限なし
- アカウントをロックアウト

ユーザが管理者グループに属している場合、これらのオプションは[自分のプロファイル]ページにも表示されます。詳細については、「[\[自分のプロファイル\]ページのフィールド](#)」(260ページ)を参照してください。

**注意：** ユーザはCLIを使用する場合、パスワードの有効期限が切れるとログインできなくなります。その場合、NA UIを使用してパスワードをリセットする必要があります。

## ユーザシナリオ1

ユーザAは別の可能性を求めて会社を退職することになり、自分のアカウントを無効にする必要がありますが、アカウントに関連する履歴データを残したままにしています。NAシステム管理者は、次の操作を実行します。

1. NAにログインします。
2. [管理]のメインメニューから、[ユーザ]オプションをクリックします。[全ユーザ]ページが開きます。
3. ユーザAの[アクション]列で[編集]オプションをクリックします。ユーザAの[ユーザを編集]ページが開きます。
4. [ユーザを編集]ページで、[ステータス]フィールドの[無効]オプションを選択し、[保存]ボタンをクリックします。

NAシステム管理者が上記の操作を実行したことにより、ユーザAがNAにログインを試みると、次のメッセージが表示されます。**アカウントは無効です**

## ユーザシナリオ2

NAシステム管理者がNAシステムのメインテナンスを行おうとしています。NAシステム管理者はシステムにログインしているNAユーザがいなかったことを確認する必要があります。全員がNAからログアウトした後、NAシステム管理者は次の操作を実行します。

1. NAにログインします。
2. [管理]のメインメニューから、[ユーザ]オプションをクリックします。[全ユーザ]ページが開きます。
3. 各ユーザの[アクション]列で[編集]オプションをクリックします。[ユーザを編集]ページが開きます。
4. [ユーザを編集]ページで、[パスワードオプション]フィールドの[アカウントをロックアウト]チェックボックスをオンにし、[保存]ボタンをクリックします。

NAシステム管理者が上記の操作を実行したことにより、ユーザがNAにログインを試みると、次のメッセージが表示されます。**アカウントをロックアウト**

NAシステム管理者は、システムのメンテナンスが完了したら、各ユーザの[ユーザを編集]ページに戻り、[アカウントをロックアウト]チェックボックスをオフにし、[保存]ボタンをクリックします。これにより、ユーザはNAにログインできるようになります。

**注意：**現時点では、ユーザアカウントを一括編集することはできません。

## ユーザシナリオ3

ユーザBは数週間の休暇をとっています。その間、NAシステム管理者は新しいコーポレートパスワードポリシーに準拠するように指示されました。従業員は自分のNAパスワードを30日間ごとに変更することが義務付けられることになりました。NAシステム管理者はこの新しいポリシーに準拠するために、次の操作を実行します。

1. NAにログインします。
2. [管理]のメインメニューから、[ユーザ]オプションをクリックします。[全ユーザ]ページが開きます。
3. ユーザBの[アクション]列で[編集]オプションをクリックします。[ユーザを編集]ページが開きます。
4. [ユーザを編集]ページで、[パスワードオプション]フィールドの[ユーザは次回ログオン時にパスワードを変更する必要あり]チェックボックスをオンにし、[保存]ボタンをクリックします。

NAシステム管理者が上記の操作を実行したことにより、ユーザBが仕事に戻りNAにログインを試みると、次のメッセージが表示されます。**「パスワードが失効しました。」「パスワードを再設定してください。」「新しいパスワードは、過去<8>個のパスワードと異なる必要があります。」**

ユーザBはユーザ名、古いパスワード、新しいパスワードを入力してから、確認のために再度新しいパスワードを入力する必要があります。

**注意：**NAシステム管理者が[ユーザの新規作成]ページまたは[ユーザを編集]ページで[ユーザによるパスワードの変更を禁止]オプションをオンにしていなければ、[パスワードの変更]ページでパスワードを変更できます。詳細については、**「[パスワードの変更]ページのフィールド」(265ページ)**を参照してください。

## パスワードの有効期限

NAシステム管理者は、[ユーザの新規作成]ページと[ユーザを編集]ページの[パスワードの有効期限なし]オプションを選択することで、NAユーザのパスワードの有効期限を有効または無効にできます。セキュリティのため、*appserver.rcx*ファイルには次の設定が含まれます。

- *security/user\_password\_expiration\_enabled* : デフォルトで、この設定はfalseです。
- *security/user\_password\_expire\_in\_days* : デフォルトで、この値は180日です。この値は、1～999を指定する必要があります。*security/user\_password\_expiration\_enabled* 設定がfalseの場合、この設定は無視されます。

デフォルト値を変更する場合、次の操作を実行します。

1. NAを停止します。
2. *\$NA/adjustable\_options.rcx* ファイルを開き、<options> タグと </options> タグの間のいずれかの場所に次のエントリを追加します。

```
<option name="security/user_password_expiration_enabled">false</option>
<option name="security/user_password_expire_in_days">180</option>
<option name="security/user_password_reuse_allowed">false</option>
<option name="security/user_password_history_size">8</option>
```

3. 必要に応じて値を変更し、ファイルを保存します。
4. すべてのNAコアで手順1、2、3を繰り返します。
5. NAを再起動します。

## パスワードの再使用

過去に指定したパスワードをユーザが使用することを防止するために、過去のパスワードはデータベースに保存されます。このために、新しくRN\_PASSWORD\_HISTORYテーブルが作成されています。

*appserver.rcx*ファイルには新しい次の2つの設定が含まれます。

- *security/user\_password\_reuse\_allowed* : デフォルト値はfalseです。
- *security/user\_password\_history\_size* : デフォルト値は8です。指定可能な値の範囲は[1, 999]です。

## ユーザグループの追加

新規ユーザグループを追加するには、[管理]メニューバーから[ユーザグループ]をクリックします。[ユーザグループ]ページが開きます。ページの上部にある[ユーザグループの新規作成]リンクをクリックします。[ユーザグループの新規作成]ページが開きます。「[\[ユーザグループの新規作成\]ページのフィールド](#)」(254 ページ)を参照してください。

**注意：** [ユーザグループ]へのリンクをクリックして、[全ユーザ]ページからこのページへナビゲートすることもできます。

**注意：** CSV ファイルから、新規のユーザグループや既存ユーザグループの変更をインポートできます。詳細については、「[\[ユーザのインポート\]タスクページのフィールド](#)」(334 ページ)を参照してください。

## [ユーザグループ]ページのフィールド

フィールド	説明/アクション
ユーザグループの新規作成	[ユーザグループの新規作成]ページが開きます。このページでユーザグループを追加できます。詳細については、「 <a href="#">[ユーザグループの新規作成]ページのフィールド</a> 」(254 ページ)を参照してください。
ユーザ	[全ユーザ]ページが開きます。このページで、ユーザグループを編集できます。詳細については、「 <a href="#">[全ユーザ]ページのフィールド</a> 」(244 ページ)を参照してください。
[ユーザのロールと権限]リンク	[ユーザのロールと権限]ページが開きます。このページで、ユーザ権限を編集できます。詳細については、「 <a href="#">[ユーザのロールと権限]ページのフィールド</a> 」(257 ページ)を参照してください。
グループ名	ユーザグループ名を表示します。[グループ名]へのリンクのいずれかをクリックすると、[ユーザ詳細]ページが開きます。このページで、グループ内の現在の全ユーザを表示できます。ユーザの追加やユーザプロフィールの編集の詳細については、「 <a href="#">[全ユーザ]ページのフィールド</a> 」(244 ページ)を参照してください。
説明	グループの簡単な説明を表示します。
ユーザロール	グループに割り当てられているユーザロールを表示します。ユーザロールをクリックすると、[ユーザロール情報]ページが開きます。このページでユーザロールの詳細を表示できます。詳細については、「 <a href="#">ユーザロールの追加</a> 」(257 ページ)を参照してください。
アクション	次のオプションを選択できます。 <ul style="list-style-type: none"><li>編集：[ユーザグループを編集]ページが開きます。詳細については、「<a href="#">[ユーザグループ]ページのフィールド</a>」(253 ページ)を参照してください。</li><li>削除：グループを削除できます（管理（Admin）権限を使用）。</li><li>権限：[表示権限]ページが開きます。詳細については、「<a href="#">[ユーザグループの新規作成]ページのフィールド</a>」(254 ページ)を参照してください。</li></ul>

## [ユーザグループの新規作成]ページのフィールド

デフォルトでは、ユーザグループに適用しているロールの集合で定義されたとおりに、ユーザグループは最も制限のないコマンド権限を使用します。権限を適切にロックダウンするには、最も制限されているロールをユーザグループに割り当てます。

フィールド	説明/アクション
<b>一般情報</b>	
グループ名	ユーザグループ名を入力します。
説明	ユーザグループの説明を入力します。
サイト	このユーザグループが属するパーティションを選択します。 <b>注意：</b> ユーザが1つのパーティションにしかアクセスできない場合、[サイト] ドロップダウンメニューは使用できません。
<b>コマンド権限</b>	
既存のコマンド権限ロール	<p>ユーザグループのユーザは、実行するすべてのアクションに対応するコマンド権限を、明示的に付与される必要があります。オンにして（デフォルト）、次の中からオプションを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• <b>管理者：</b>ユーザ管理、ポリシー設定、ネットワーク全体の処理の実行など、NA を管理する責任を負います。管理者には、すべてのデバイスに対するすべてのアクションを実行できる権限があります。</li> <li>• <b>パワー：</b>パワーユーザとは、通常、大半のアクションの実行を許可されているエキスパートエンジニアのことです。デバイスのグループについて再構成したり、アクションを実行したりできます。</li> <li>• <b>フルアクセス：</b>フルアクセスユーザとは、通常、ネットワーク内の複数のデバイス（全デバイスとは限りません）を構成するパスワードを持つ、信頼できるネットワークエンジニアのことです。フルアクセスユーザには、NA データベース内の大半の情報を修正できる権限があり、一括モードではなく、デバイスを個々に再構成することができます。多くの場合、再構成する権限を持つことができるデバイスは制限されます。</li> <li>• <b>制限付きアクセスユーザ：</b>通常は、ネットワークデバイスを構成するためのパスワードを持たないオペレータのことです。デバイスを表示する権限はありますが、NA データベースの情報の大半を修正できません。また、パッチ処理やネットワークデバイスを再構成する処理も実行できません。</li> </ul> <p><b>注意：</b>デフォルトのコマンド権限ロールとは別にコマンド権限ロールを定義した場合には、そのロールがリストに表示されます。</p>

フィールド	説明/アクション
カスタマイズされた コマンド権限ロール	<p>オンにすると、ユーザグループに特定のコマンド権限ロールをカスタマイズできます。コマンドごとにボタンをクリックして、ロールへの権限の付与と拒否を設定できます。コマンド権限の全リストについては、「<b>付録B：コマンド権限</b>」(713ページ)を参照してください。[すべて付与]をクリックすると、すべてのコマンドの権限を付与できます。これは管理ユーザにとって便利なものです。また、少数のコマンドのみについて権限を拒否したい場合にも便利です。[すべて拒否]をクリックすると、すべてのコマンドの権限を拒否できます。デフォルトでは、すべてのコマンドが拒否されています。コマンドの右側にある次のアイコンは、デバイス権限またはスクリプト権限の変更を必要とする場合があることを示します。</p> <ul style="list-style-type: none"> <li>• デバイスの修正権限が必要アイコン：NAでデバイスごとに権限を管理できます。[デバイスの修正権限]では、デバイスを変更可能かどうかを指定します。このコマンドを実行したい特定のデバイスの、[デバイスの修正権限]を持っている必要があります。以下の「デバイスの修正権限」を参照してください。</li> <li>• スクリプト権限が必要アイコン：NAでコマンドスクリプトごとに権限を管理できます。[スクリプト権限]では、コマンドスクリプトを実行可能かどうかを指定します。実行したいコマンドスクリプトの[スクリプト権限]が必要です。以下の「スクリプト権限」を参照してください。</li> </ul> <p><b>注意：</b>カスタムスクリプトはデバイス構成の変更とみなされます。そのため、ユーザの[デバイス構成の変更]権限がオンになります。</p>
<b>デバイスの修正権限</b>	
全デバイス	グループのユーザは、すべてのデバイスを修正できます。
	<p><b>注意：</b>デバイスの修正権限を持たないユーザがデバイス構成を表示すると、パスワードやSNMPコミュニティ文字列などのデバイス構成内の機密情報はマスクされています。これにより、デバイスの修正権限を持たないユーザが機密データを表示できないようにします。</p>
なし	修正できるデバイスはありません。これはデフォルトの設定です。
既存のデバイスの修正権限 ロール	グループのユーザが持つ、既存の[デバイス変更権限]ロールを選択できます。構成されている既存のロールがない場合は、次のメッセージが表示されます：既存のロールが見つかりませんでした。
カスタマイズされた デバイスの修正権限ロール	ユーザグループ固有のリストから[デバイス権限]ロールを選択できます。
<b>スクリプト権限</b>	
全スクリプト	グループのユーザは、すべてのスクリプトを修正できます。
なし	修正できるスクリプトはありません。これはデフォルトの設定です。
既存のスクリプト権限 ロール	グループのユーザが持つ、既存の[スクリプト]権限ロールを選択できます。構成されている既存のロールがない場合は、次のメッセージが表示されます：既存のロールが見つかりませんでした。
カスタマイズされた スクリプト権限ロール	ユーザグループ固有のリストから[スクリプト権限]ロールを1つ選択できます。
カスタマイズされた スクリプト権限ロール	カスタマイズされたスクリプト権限ロールをリストから選択できます。

フィールド	説明/アクション
<b>パーティションの表示権限</b>	
全オブジェクト	<p>ユーザグループのユーザは全パーティションを表示できます。(詳細については、「<b>デバイスとユーザのセグメント化</b>」(148ページ)を参照してください)。</p> <p><b>注意:</b> 表示権限を使用しない場合は、新規ユーザは全デバイスへの表示権限を与えられて、[全パーティションの表示]グループに配置されます。表示権限を作成する場合、新規ユーザにはいずれの表示権限も暗黙的に付与されません。</p>
なし	表示可能なパーティションはありません。これはデフォルトの設定です。
既存の表示権限ロール	ユーザグループのユーザが持つ、既存の表示権限ロールを選択できます。構成されている既存のロールがない場合は、「既存のロールが見つかりませんでした」というメッセージが表示されます。
表示権限ロールのカスタマイズ	表示権限ロールをリストから選択できます。[すべて] ラジオボタンが選択されている場合、すべてのパーティションが含まれます。
<b>ユーザ</b>	
グループのユーザ/ 全ユーザ	<p>ユーザを追加するには、右側のボックスからユーザを選択して、[&lt;&lt;追加]をクリックします。ユーザを削除するには、左側のボックスからユーザを選択して、[削除]をクリックします。</p>

終了時に、必ず[保存]をクリックしてください。



## ユーザロールの追加

ユーザがWeb ページの表示またはコマンドの実行などアクションを行うには、それぞれのアクションに対応するコマンド権限が明示的に付与されている必要があります。一連のコマンド権限によって、コマンド権限ロールを作成します。その後、作成したロールをユーザグループに適用して、そのユーザグループにコマンド権限を設定できます。たとえば、ネットワーク運用スタッフに、デバイスレコードへのアクセスや変更の表示の権限を持たせる一方で、デバイス上の変更のスク립ティングやデバイスの削除の権限を持たせないということも可能です。

**注意：** 表示権限を使用しない場合は、新規ユーザは全デバイスへの表示権限を与えられて、[全パーティションの表示]グループに配置されます。表示権限を作成する場合、新規ユーザにはいずれの表示権限も暗黙的に付与されません。

新規ユーザロールを追加するには：

1. [管理]の下メニューバーで、[ユーザのロールと権限]オプションをクリックします。[ユーザロールと権限]ページが開きます。
2. ページの上部にある[ユーザロールの新規作成]リンクをクリックします。[ユーザロールの新規作成]ページが開きます。**「[ユーザロールの新規作成]ページのフィールド」(259 ページ)**を参照してください。

## [ユーザのロールと権限]ページのフィールド

フィールド	説明/アクション
ユーザロールの新規作成	[ユーザロールの新規作成]ページが開きます。このページでユーザロールを選択できます。詳細については、 <b>「[ユーザロールの新規作成]ページのフィールド」(259 ページ)</b> を参照してください。
ユーザ	[全ユーザ]ページが開きます。このページで、現在のユーザの表示と新規ユーザの追加ができます。詳細については、 <b>「[全ユーザ]ページのフィールド」(244 ページ)</b> を参照してください。
ユーザグループ	[ユーザグループ]ページが開きます。このページで、現在のユーザグループの表示と新規ユーザグループの追加ができます。詳細については、 <b>「[ユーザグループ]ページのフィールド」(253 ページ)</b> を参照してください。

### システムのデフォルトのロール

ロール名	ロール名を表示します。ロールを選択して、そのロールのコマンド権限リストなどのロール情報を表示できます。
ロールタイプ	コマンド権限、デバイス修正権限、スクリプト権限、パーティションの表示権限などのロールタイプを表示します。
説明	ロールの説明を表示します。
アクション	次のオプションを選択できます。 <ul style="list-style-type: none"> <li>• 編集：[ユーザロールを編集]ページが開きます。詳細については、<b>「ユーザロールの追加」(257 ページ)</b>を参照してください。デフォルトのロールは編集できません。</li> <li>• コピーを作成：[ユーザロールを編集]ページが開きます。このページで新規ユーザロールを追加できます。詳細については、<b>「[ユーザロールの新規作成]ページのフィールド」(259 ページ)</b>を参照してください。</li> <li>• 削除：ロールを削除できます（システム管理権限のみ）。デフォルトのロールは削除できません。</li> </ul>

フィールド	説明/アクション
<b>ユーザ定義ロール</b>	
ロール名	ロール名を表示します。ロールを選択して、そのロールのコマンド権限リストなどのロール情報を表示できます。
ロールタイプ	たとえば、コマンド権限、デバイスの修正権限、パーティションの表示権限、スクリプト権限などのロールタイプを表示します。
説明	ロールの説明を表示します。
アクション	次のオプションを選択できます。 <ul style="list-style-type: none"><li>編集：[ ユーザロールを編集 ] ページが開きます。詳細については、「[ ユーザロールの新規作成 ] ページのフィールド」（259 ページ）を参照してください。</li><li>コピーを作成：[ ユーザロールを編集 ] ページが開きます。このページで新規ユーザロールを追加できます。詳細については、「[ ユーザロールの新規作成 ] ページのフィールド」（259 ページ）を参照してください。ユーザ定義ロールはコピーできません。</li><li>削除：ロールを削除できます（システム管理権限のみ）。</li></ul>

## [ユーザロールの新規作成]ページのフィールド

フィールド	説明/アクション
ユーザロールの新規作成	<p>ドロップダウンメニューからユーザロールを選択します。その選択によって表示が変わります。オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>コマンド権限</b>：ユーザロールの名前と説明を入力します。コマンドごとにボタンをクリックして、ロールへの権限の付与と拒否を設定できます。コマンド権限の全リストについては、「<a href="#">付録B：コマンド権限</a>」(713ページ)を参照してください。[すべて付与]をクリックすると、すべてのコマンドの権限を付与できます。これは管理ユーザにとって便利なものです。また、少数のコマンドのみについて権限を拒否したい場合にも便利です。[すべて拒否]をクリックすると、すべてのコマンドの権限を拒否できます。</li> <li>• <b>デバイスの修正権限</b>：ユーザロールの名前と説明を入力します。デバイスセクタを使用してデバイスグループを選択します。デバイスセクタの使用方法的詳細については、「<a href="#">デバイスセクタ</a>」(142ページ)を参照してください。このロールは、選択されたデバイスグループのメンバーである全デバイスのデバイス変更権限を持ちます。</li> <li>• <b>スクリプト権限</b>：ユーザロールの名前と説明を入力します。リストからスクリプトを選択します。このロールは、選択されたすべてのスクリプトのスクリプト権限を持ちます。</li> <li>• <b>パーティションの表示権限</b>：ユーザロールの名前と説明を入力します。リストからパーティションを選択します。このロールは、選択されたパーティションのデバイス、ユーザのいずれかまたは両方グループのメンバーである全デバイス、ユーザのいずれかまたは両方のパーティションの表示権限を持ちます。パーティションの表示権限は、個々のユーザではなく、ユーザグループに割り当てられるので注意が必要です。複数のユーザグループに属するユーザは、複数のパーティションの表示権限を取得できます。デバイスのセグメント化の詳細については、「<a href="#">デバイスとユーザのセグメント化</a>」(148ページ)を参照してください。</li> </ul>

終了時に、必ず[保存]をクリックしてください。

ユーザグループにはユーザロールが自動的に割り当てられないので、注意が必要です。ユーザグループにユーザロールを割り当てるには：

1. [管理]メニューバーで[ユーザグループ]をクリックします。[ユーザグループ]ページが開きます。
2. 新規ロールを追加するグループの[アクション]列にある[編集]をクリックします。[ユーザグループの編集]ページが開きます。詳細については、「[\[ユーザグループの新規作成\]ページのフィールド](#)」(254ページ)を参照してください。

## ユーザ設定の編集

ホームページの[ユーザワークスペース]領域に含まれているセクションは次のとおりです。

- 現在のデバイス：該当する場合は、現在のデバイスを表示します。
- 現在のデバイスグループ：現在のデバイスグループを表示します。[インベントリ]がデフォルトです。
- 自分のお気に入り：お気に入りのデバイス、URL、NA ページなどのリストを表示します。大半のNA ページの最上部にある[お気に入りに追加]へのリンクをクリックして、このリストに項目を追加できます。
- クイック起動：「[クイック起動とは](#)」（265 ページ）を参照してください。
- 自分の設定：詳細については、「[自分の設定](#)」（260 ページ）を参照してください。

## 自分の設定

[自分の設定]の下にある次のオプションを選択できます。

- 自分のプロフィール：「[\[自分のプロフィール\]ページのフィールド](#)」（260 ページ）を参照してください。
- ユーザワークスペース：「[\[自分のワークスペース\]ページのフィールド](#)」（262 ページ）を参照してください。
- 自分の環境設定：「[\[自分の環境設定\]ページのフィールド](#)」（262 ページ）を参照してください。
- 自分の権限：「[\[自分の権限\]ページのフィールド](#)」（264 ページ）を参照してください。
- パスワードの変更：「[\[パスワードの変更\]ページのフィールド](#)」（265 ページ）を参照してください。
- クイック起動：「[クイック起動とは](#)」（265 ページ）を参照してください。

## [自分のプロフィール]ページのフィールド

[自分のプロフィール]ページでは、ユーザ名、パスワード、電子メールアドレスなどのユーザ設定を変更できます。パスワードオプションを表示できるのは、管理グループのユーザのみです。詳細については、「[ユーザパスワードの構成](#)」（250 ページ）を参照してください。

NA ホームページの[自分の設定]の下にある[自分のプロフィール]をクリックします。[自分のプロフィール]ページが開きます。終了時に、必ず[保存]ボタンをクリックしてください。

フィールド	説明/アクション
ユーザ情報	
ユーザ名	新規のNA ユーザ名を入力します。
パスワード	新規のNA パスワードを入力します。
パスワードの確認	確認用に新規のNA パスワードを再入力します。

フィールド	説明/アクション
パスワードオプション	<p>次の中からオプションを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• ユーザは次回ログオン時にパスワードを変更する必要あり</li> <li>• ユーザによるパスワードの変更を禁止</li> <li>• パスワードの有効期限なし</li> <li>• アカウントをロックアウト</li> </ul> <p>パスワードオプションの設定の詳細については、「<a href="#">ユーザパスワードの構成</a>」(250 ページ) を参照してください。</p>
外部リソース資格情報	[外部リソース資格情報を変更]リンクをクリックすると、[パスワードの変更]ページが開きます。「 <a href="#">[パスワードの変更]ページのフィールド</a> 」(265 ページ) 参照してください。
名	新規の名を入力します。
姓	新規の姓を入力します。
電子メールアドレス	新規の電子メールアドレスを入力します。
ユーザが属すグループ	ユーザが属すグループを表示します。グループをクリックすると、グループに属すユーザの現在のリストが表示されます。
外部認証フェイルオーバー チェックボックス	オンにすると、外部認証に失敗した場合、認証が自動的にローカル認証にフェイルオーバーします。
コメント	ユーザアカウントについてのコメントを入力します。
<b>AAA</b>	
AAA ユーザ名	新規のAAA (TACACS+またはRADIUS) ユーザ名を入力します。
AAA パスワード	新規のAAAパスワードを入力します。
AAA パスワードの確認	確認用に新規のAAAパスワードを再入力します。
[プロキシインターフェイスでのAAAログインの使用]チェックボックス	オンにすると、AAA ログイン情報はNA TelnetおよびSSHの各セッションとともに使用されます。
<b>SecurID</b>	
ソフトウェアトークンライセンスを管理	SecurID 資格情報を使用してデバイスにログインできるように、NA を構成できます。このリンクをクリックして、[SecurID トークンの表示]ページを開きます。詳細については、「 <a href="#">SecurID ソフトウェアトークンの追加</a> 」(630 ページ) を参照してください。(注意: ソフトウェアトークンがユーザのプラットフォームでサポートされていない場合や、SecurID が適切に構成されていない場合、このリンクは表示されません)。

## [自分のワークスペース]ページのフィールド

ワークスペースを編集するには、NA ホームページの[自分の設定]の下にある[自分のワークスペース]をクリックします。[自分のワークスペース]ページが開きます。

フィールド	説明/アクション
お気に入り	お気に入りのリンクを表示します。リンクには、デバイス、NA ページ、または他の URL があります。リンクを削除するには、削除したいリンクの隣にある赤い[削除]アイコンをクリックします。新規の名前を入力して[名前変更]ボタンをクリックすると、リンクの名前変更もできます。上下矢印を使用して、お気に入りのリンクをリスト内で上下に移動することもできます。
カスタマイズされたお気に入りリンクの追加	[リンク名]フィールドにリンク名を入力します。最大文字数は25です。リンクの URL アドレスを入力することもできます。終了時に、必ず[お気に入りリンクの追加]ボタンをクリックしてください。
ワークスペース設定	ドロップダウンメニューからリンクを選択して、いずれかのリンクをデフォルトのホームページとして使用することができます。[自分のお気に入り]リストに登録できるリンク数を変更するには、ドロップダウンメニューから数値を選択します。デフォルトは10です。(注意：このオプションは、ショートカットを追加しない限り、利用できません)。

## [自分の環境設定]ページのフィールド

現在の NA ホームページ環境設定を編集するには、NA ホームページの[自分の設定]の下にある[自分の環境設定]をクリックします。[自分の環境設定]ページが開きます。このページでは、ホームページをカスタマイズし、[デバイスソフトウェアイメージ推奨]ページに表示される Cisco ソフトウェアイメージを指定できます。詳細については、[「\[デバイスソフトウェアイメージ推奨\]ページのフィールド」\(223 ページ\)](#)を参照してください。

フィールド	説明/アクション
自分のタスクおよび承認の要求（ワークフローが有効な場合）をホームページに表示	[はい](デフォルト)または[いいえ]を選択します。
最近の変更をホームページに表示	[はい](デフォルト)または[いいえ]を選択します。
最近のイベントをホームページに表示	[はい](デフォルト)または[いいえ]を選択します。
システムレポートをホームページに表示	[はい]または[いいえ](デフォルト)を選択します。
お気に入りレポートをホームページに表示	[はい](デフォルト)または[いいえ]を選択します。
自分のデバイスグループをホームページに表示	[はい](デフォルト)または[いいえ]を選択します。
<b>ソフトウェアイメージ推奨設定</b>	
現在のバージョンよりも高いバージョンのイメージのみを含みます。	[はい]または[いいえ](デフォルト)を選択します。
同一サブセット機能のイメージのみを含みます。	[はい]または[いいえ](デフォルト)を選択します。
一般配布イメージのみを含みます。	[はい]または[いいえ](デフォルト)を選択します。
最新保守リリースイメージのみを含みます。	[はい]または[いいえ](デフォルト)を選択します。
イメージ推奨の Cisco.com イメージを含みます。	[はい](デフォルト)または[いいえ]を選択します。

終了時に、必ず[保存]ボタンをクリックしてください。

## [自分の権限]ページのフィールド

[表示権限]ページでは、属すグループによってユーザが持っている権限を表示します。割り当てられたロールもあるので注意が必要です。詳細については、「[\[ユーザロールの新規作成\]ページのフィールド](#)」(259 ページ)を参照してください。

**注意：** 表示権限を使用しない場合は、新規ユーザは全デバイスへの表示権限を与えられて、[全パーティションの表示]グループに配置されます。表示権限を作成する場合、新規ユーザにはいずれの表示権限も暗黙的に付与されません。

現在の権限を表示するには、NA ホームページの[自分の設定]の下にある[自分の権限]をクリックします。[自分の権限]ページが開きます。

フィールド	説明/アクション
ユーザグループとロール	ユーザが属す全グループと、各グループに割り当てられたロールを表示します。詳細については、「 <a href="#">ユーザロールの追加</a> 」(257 ページ)を参照してください。
コマンド権限の付与	コマンドに関する所有権限を表示します。詳細については、「 <a href="#">コマンド権限の付与</a> 」(713 ページ)を参照してください。
デバイスの修正権限の付与	デバイスの修正のための所有権限を表示します。
スクリプト権限の付与	スクリプトの実行や修正のための所有権限を表示します。
パーティションの表示権限の付与	ユーザやデバイスを表示するための所有権限を表示します。詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」(148 ページ)を参照してください。



## [パスワードの変更]ページのフィールド

ローカルの認証パスワード、外部リソース資格情報のいずれかまたは両方を変更するには、NAホームページの[自分の設定]の下にある[パスワードの変更]をクリックします。[パスワードの変更]ページが開きます。

フィールド	説明/アクション
<b>ローカル認証パスワード</b>	
新しいパスワード	新しいパスワードを入力します。
新しいパスワードの確認	確認用に新しいパスワードを再入力して、[送信]ボタンをクリックします。
<b>外部リソース認証/新規外部リソース資格情報の追加</b>	
資格情報タイプ	<p>ドロップダウンメニューから資格情報タイプを選択します。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• Cisco.com 資格情報：この資格情報は、ソフトウェアイメージ推奨と Cisco デバイスへのソフトウェアイメージのダウンロードのために、Cisco.comが使用します。Cisco.comには、Cisco のインターネットワーク製品向けのシステムソフトウェアおよびドライバの公開バージョンが存在します。詳細については、<a href="#">「[Cisco.comからイメージをダウンロード]タスクページ」</a> (367 ページ) を参照してください。</li> <li>• プロキシ資格情報：この資格情報は、ユーザ名とパスワードを必要とするプロキシ経由で Cisco.com にアクセスする場合に使用します。</li> </ul>
ユーザ名	ユーザ名を入力します。プロキシは一般的なもので、Cisco.comには直接的に関連しません。ソフトウェアイメージ管理コレクタ HTTP プロキシサーバの構成の詳細については、 <a href="#">「[サーバ]ページのフィールド」</a> (52 ページ) を参照してください。
パスワード	パスワードを入力します。
パスワードの確認	確認用に新規パスワードを再入力して、[追加]ボタンをクリックします。

既存の外部リソース資格情報を変更、または削除するには、[変更]、または[削除]ボタンをクリックします。

## クイック起動とは

NAの以前のバージョンでは、スナップショットの取得や、ポリシー準拠の確認、レポートの生成などのタスクを実行する際に、現在のページから移動する必要がありました。

現在のページから移動しなくても、タスクをカスタマイズし、事前入力されたデータを使用してこれらのタスクを迅速に起動できるようになりました。たとえば、デバイスの[デバイス詳細]ページを表示しながら、スナップショットの取得などのクイック起動アクションを構成した場合は、[自分のワークスペース]領域の[クイック起動]の下に表示される[クイック起動]アクションをクリックするだけで、タスクは自動的に実行されます。

**注意：** クイック起動を作成、実行、削除できるのは、管理権限を持っているユーザのみです。

## クイック起動の構成方法

クイック起動はタスクテンプレートを使用します。タスクテンプレートを使用すると、タスク定義を保存できるようになり、いちから作業を始めなくても、新しいタスクまたは既存のタスクを迅速に構成および実行できます。

タスクをクイック起動に追加するには：

1. [タスク] の下のメインメニューバーで、[タスクテンプレート] をクリックします。[タスクテンプレート] ページが開きます。タスクテンプレートを検索することもできます。詳細については、「[タスクの検索](#)」(502 ページ) を参照してください。
2. [アクション] 列で[クイック起動への追加]リンクをクリックします。[自分のワークスペース]領域の[クイック起動]セクションに、[クイック起動]リンクが自動的に表示されます。[クイック起動]リンクでは、現在のタスクテンプレートの名前が仮に付けられます。リンク名を変更したい場合は、表示されたポップアップボックスを使用してください。ポップアップボックスが表示されるのは、重複名が存在する場合だけであることを注意してください。

タスクテンプレートの詳細については、「[タスクテンプレート](#)」(280 ページ) を参照してください。

タスクテンプレートを定義していない場合は、次の操作を実行します。

1. [タスク] の下のメインメニューバーで、[タスクの新規作成]を選択し、スナップショットの取得などのタスクをクリックします。[スナップショットの取得]ページが開きます。
2. [タスクの新規作成]または[タスクを編集]ページで、[保存オプション]フィールドの[タスクテンプレートとして保存]オプションをクリックします。タスクを保存すると、タスクはテンプレートとして保存され、[タスクテンプレート]ページに表示されます。

## クイック起動の管理

クイック起動を管理するには、NA ホームページで[自分のワークスペース]領域の[自分の設定]の下にある[クイック起動]リンクをクリックします。[クイック起動]ページが開きます。このページでは、次のことを実行できます。

- 矢印ボタンまたはドラッグアンドドロップ機能を使用して、表示されるクイック起動の順序を変更できます。
- クイック起動を削除できます。
- クイック起動の名前を変更できます。
- NA ホームページの[自分のワークスペース]領域の下にある[クイック起動]領域のサイズを決定できます。

一般的な表示については、「[サンプルのクイック起動の表示](#)」(267 ページ) を参照してください。

## クイック起動の使用方法

クイック起動を定義すると、NAホームページの[自分のワークスペース]領域にある[自分の設定]セクションの下に、クイック起動のリストが表示されます。

[クイック起動]リンクは、作業している特定のページおよびコンテンツによって異なります。たとえば、[インベントリ]ページで詳細を調べたいデバイスを選択します。そのデバイスの[デバイス詳細]ページが開きます。スナップショットの取得のクイック起動を構成した場合、NAホームページの[自分のワークスペース]領域にある[自分の設定]の下に[クイック起動]セクションの[スナップショットの取得]リンクをクリックすると、タスクは自動的に実行されます。タスクが正常に保存されましたなどの情報メッセージが表示されます。

クイック起動のタスクを構成する際は、クイック起動は常に現在のデバイスまたはデバイスグループ（これらが存在しなければ、インベントリ）に対して実行されるので注意してください。タスクテンプレートを構成する場合は、タスクのデバイス情報またはデバイスグループ情報を入力します。この情報は、実行しようとしているクイック起動の現在のデバイス情報またはデバイスグループ情報で置き換えられます。

たとえば、デバイスのリブートタスクのクイック起動を構成していて、表示中のデバイスに対してクイック起動を実行すると、元のタスクテンプレートに入力したデバイス情報またはデバイスグループ情報に関係なく、デバイスが自動的にリブートされます。リブート前にプロンプトメッセージが表示されることはありません。

## サンプルのクイック起動の表示

次の表は、サンプルの[クイック起動]ページのフィールドを説明します。クイック起動の構成方法の詳細については、「[クイック起動とは](#)」(265 ページ) を参照してください。

フィールド	説明/アクション
タスクテンプレートリストのページリンク	このリンクをクリックすると、[タスクテンプレート]ページが開きます。詳細については、「 <a href="#">タスクテンプレート</a> 」(280 ページ) を参照してください。
<b>クイック起動のアクション：デバイス</b>	
タスク名。「スナップショットの取得」など	上下矢印を使用すると、一覧されるクイック起動デバイスアクションをソートできます。
	赤のXアイコンを使用すると、クイック起動デバイスアクションを削除できます。
	クイック起動デバイスアクション名を変更する場合は、新しい名前を入力して[名前を変更]ボタンをクリックします。アクション名は25文字を超えて指定することはできません。
<b>クイック起動のアクション：ポリシー</b>	
タスク名。「ポリシーの確認」など	上下矢印を使用すると、一覧されるクイック起動ポリシーアクションをソートできます。
	赤のXアイコンを使用すると、クイック起動デバイスアクションを削除できます。
	クイック起動ポリシーアクション名を変更する場合は、新しい名前を入力して[名前を変更]ボタンをクリックします。アクション名は25文字を超えて指定することはできません。

フィールド	説明/アクション
<b>クイック起動のアクション：レポート</b>	
タスク名。「サマリレポートの生成」など	上下矢印を使用すると、一覧されるクイック起動レポートアクションをソートできます。
	赤のXアイコンを使用すると、クイック起動レポートアクションを削除できます。
	クイック起動レポートアクション名を変更する場合は、新しい名前を入力して[名前を変更]ボタンをクリックします。アクション名は25文字を超えて指定することはできません。
<b>クイック起動設定</b>	
クイック起動に表示される最大ショートカット数	プルダウンメニューから値を選択します。デフォルト値は10です。この値によって、NAホームページの自分のワークスペース]領域の下にある[クイック起動]領域のサイズが決定されます。NAホームページの詳細については、「 <a href="#">ユーザ設定の編集</a> 」(260 ページ) を参照してください。

## NA ホームページのカスタマイズ

ユーザがNAにログインすると、常にNAホームページが開きます。各ページの左上隅にある[ホーム]リンクをクリックして、NAホームページに戻ることもできます。

NAホームページには2つのフレームが含まれます。左側のフレームには以下が含まれます。

- 検索：検索オプションを使用すると、ホスト名またはIPアドレスによってデバイスを検索し、それらのデバイスにTelnetまたはSSH経由で接続できます。詳細については、「[検索/接続機能](#)」(273ページ)を参照してください。
- 自分のワークスペース：[自分のワークスペース]領域には、次のセクションが含まれます。
  - － 現在のデバイス/現在のデバイスグループ ([インベントリ]がデフォルトです)
  - － 自分のお気に入り
  - － クイック起動 (該当する場合)
  - － 自分の設定

[自分のワークスペース]領域のオプション設定の詳細については、「[ユーザ設定の編集](#)」(260ページ)を参照してください。

右側のフレームは、以下を含めるようにカスタマイズできます。

- ワークフロー承認
- タスクのリスト
- 最近の構成変更 (変更したデバイスや時間)
- 最近のシステムイベント (デバイスアクセスエラーなど)
- 選択されたデバイスグループ
- 選択されたお気に入りレポート
- 選択されたシステムレポート

詳細については、「[\[自分のホームページ\]タブのフィールド](#)」(270ページ) および 「[\[統計ダッシュボード\]タブのフィールド](#)」(272ページ)を参照してください。

## [自分のホームページ]タブのフィールド

フィールド	説明/アクション
<b>ワークフロー承認</b> （該当する場合）	
自分の承認を待機している タスク	<p>承認を待機しているタスクを表示します。タスクには次のものが含まれています。</p> <ul style="list-style-type: none"> <li>• <b>タスク名</b>：タスク名を表示します。タスク名をクリックすると、[タスク情報]ページが開きます。このページで、タスクを承認できます。[タスク情報]ページの詳細については、「<a href="#">[タスク情報]ページのフィールド</a>」(672 ページ) を参照してください。</li> <li>• <b>承認期限</b>：承認が必要なタスクについて、その承認期限の日付と時刻を表示します。タスク承認の詳細については、「<a href="#">承認の要求</a>」(670 ページ) を参照してください。</li> <li>• <b>承認</b>：承認のステータスを表示します。</li> <li>• <b>スケジュール日</b>：タスクが予定された日付を表示します。</li> <li>• <b>ステータス</b>：現在のステータスを表示します。</li> </ul> <p>[すべて表示]リンクをクリックすると、[承認の要求]ページが開きます。このページで、承認の要求のリストを表示できます。[承認の要求]ページの詳細については、「<a href="#">承認の要求</a>」(670 ページ) を参照してください。</p>
<b>自分のタスク</b>	
タスク名	タスクのリストを表示します。詳細については、「 <a href="#">タスクとは</a> 」(277 ページ) を参照してください。最初に NA を設定するときに、デフォルトのタスクのリストが表示されます。そのリストには、[スナップショットの取得]、[サマリレポートの生成]、[診断の実行]、[データの整理]などが含まれています。
予定日	タスクが予定された日付と時刻を表示します。
ステータス	現在のタスクのステータスを表示します。タスクのステータスのリストの詳細については、「 <a href="#">[タスク情報]ページのフィールド</a> 」(406 ページ) を参照してください。
すべて表示	[自分のタスク]ページが開きます。このページで、全タスクを表示できます。詳細については、「 <a href="#">タスクとは</a> 」(277 ページ) を参照してください。
<b>最近の変更</b>	
期間	<p>デフォルトの期間は、過去24時間です。次の期間を選択できます。</p> <ul style="list-style-type: none"> <li>• 過去1、2、4、8、12、24、および48時間</li> <li>• 過去1および2週間</li> <li>• 過去1ヶ月</li> <li>• 全構成</li> </ul>
日付	構成を変更した日付と時刻を表示します。
デバイス	変更したデバイスのホスト名またはIPアドレスを表示します。デバイスのリンクをクリックすると、[デバイス詳細]ページが開きます。
変更者	構成、デバイス、またはタスクを変更した実行者のログイン名を表示します。N/Aは未対応であることを意味します。
コメント	構成についてのコメントを表示します。

フィールド	説明/アクション
アクション	<p>次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>• 前と比較 : [デバイス構成の比較] ページが開きます。そのページで、選択した構成とその直前の構成を並べて表示できます。差異は、分かりやすいように異なる色で強調表示されます。</li> <li>• 構成を表示 : [デバイス構成の詳細] ページが開きます。そのページでは、構成全体の表示、構成のこのバージョンのデバイスランニング構成への配布、構成の編集、診断の取得、以前の構成との比較などができます。</li> </ul>
すべて表示	<p>[構成変更] ページが開きます。このページで、すべての構成変更を表示でき、変更を表示する期間を調整できます。詳細については、「<a href="#">デバイス構成変更の表示</a>」(172 ページ) を参照してください。</p>
<b>最近のイベント</b>	
期間	<p>デフォルトの期間は、過去24時間です。次の期間を選択できます。</p> <ul style="list-style-type: none"> <li>• 過去1、2、4、8、12、24、および48時間</li> <li>• 過去1および2週間</li> <li>• 過去1ヶ月</li> <li>• 全構成</li> </ul>
イベントサマリ	<p>イベントのタイプが表示されます。リンクをクリックして、このタイプのイベントの完全なリストを表示します。詳細については、「<a href="#">イベントの連結ビュー（シングルビュー）</a>」(546 ページ) を参照してください。</p>
カウント	<p>このタイプのイベント数を表示します。</p>
イベントリストページ	<p>[システム/ネットワークイベント] ページが開きます。このページで、イベントの長いリストを表示でき、イベントを表示する期間を調整できます。詳細については、「<a href="#">イベントの連結ビュー（シングルビュー）</a>」(546 ページ) を参照してください。</p>
<b>自分のデバイスグループ（該当する場合）</b>	
デバイスグループ	<p>[デバイスグループ] ページが開きます。このページで、現在のデバイスグループを表示できます。</p>
<b>お気に入りレポート（該当する場合）</b>	
全お気に入りレポート	<p>[ユーザーレポートとシステムレポート] ページが開きます。このページで、カスタム検索から作成したレポートとシステムレポートを表示できます。</p>

## [統計ダッシュボード]タブのフィールド

[統計ダッシュボード]タブでは、次の情報を提供しています。

- ベンダーのトップ5
- OSバージョンのトップ5
- アクティブユーザのトップ5
- 1日あたりの平均変更数
- 変更頻度
- 最もアクセスされるデバイスのトップ10
- ソフトウェアレベル
- OSインベントリ
- 構成ポリシー準拠

詳細については、「[サマリレポート](#)」(621 ページ) を参照してください。



## 検索/接続機能

ホームページ（およびすべてのページ）には、各ページの左側に[検索]タブがあります。この[検索]タブで、ホスト名またはIPアドレスを使用してデバイスを検出して、TelnetまたはSSH経由でそのデバイスに接続できます。検索機能ではワイルドカードが使用できるので、関連デバイスのグループを迅速に検出できます。または、少なくともターゲットデバイスが検出されるまで、検索範囲を絞ることができます。[デバイスの検索]ページのフィールドの詳細については、「[デバイスの検索](#)」（472ページ）を参照してください。

[検索]ドロップダウンメニューを使用して、次の対象の検索もできます。

- デバイス
- インターフェイス
- モジュール
- ポリシー
- 準拠
- 構成
- 診断
- タスク
- セッション
- イベント
- ユーザ
- シングルサーチ
- ACL
- MACアドレス
- IPアドレス
- VLAN
- デバイステンプレート
- 詳細検索



## 第7章：タスクの予定

### トピックの参照先リスト

トピック	参照先：
タスクとは	<a href="#">「タスクとは」</a> (277 ページ)
タスクの予定	<a href="#">「タスクの予定」</a> (278 ページ)
タスクテンプレート	<a href="#">「タスクテンプレート」</a> (280 ページ)
Syslogの構成タスク	<a href="#">「[Syslogの構成]タスクページのフィールド」</a> (284 ページ)
パスワードの配布タスク	<a href="#">「[パスワードの配布]タスクページのフィールド」</a> (288 ページ)
ドライバの検出タスク	<a href="#">「[ドライバの検出]タスクページのフィールド」</a> (293 ページ)
デバイスのリポートタスク	<a href="#">「[デバイスのリポート]タスクページのフィールド」</a> (296 ページ)
ICMPテストの実行タスク	<a href="#">「[ICMPテストの実行]タスクページのフィールド」</a> (299 ページ)
コマンドスクリプトの実行タスク	<a href="#">「[コマンドスクリプトの実行]タスクページのフィールド」</a> (304 ページ)
診断の実行タスク	<a href="#">「[診断の実行]タスクページのフィールド」</a> (310 ページ)
スナップショットの取得タスク	<a href="#">「[スナップショットの取得]タスクページのフィールド」</a> (315 ページ)
スタートアップとランニングの同期タスク	<a href="#">「[スタートアップとランニングの同期]タスクページのフィールド」</a> (319 ページ)
デバイスソフトウェアの更新タスク	<a href="#">「[デバイスソフトウェアの更新]タスクページのフィールド」</a> (323 ページ)
デバイスのインポートタスク	<a href="#">「[デバイスのインポート]タスクページのフィールド」</a> (329 ページ)
ユーザのインポートタスク	<a href="#">「[ユーザのインポート]タスクページのフィールド」</a> (334 ページ)
ネットワークデバイスの検出タスク	<a href="#">「[ネットワークデバイスの検出]タスクページのフィールド」</a> (341 ページ)
通信モードデータの削除タスク	<a href="#">「[重複の削除]タスクページのフィールド」</a> (347 ページ)
OS分析	<a href="#">「[OS分析]タスクページのフィールド」</a> (350 ページ)
ポートスキャン	<a href="#">「[ポートスキャン]ページのフィールド」</a> (353 ページ)
テンプレートからデバイスをプロビジョニング	<a href="#">「[デバイスのプロビジョニング]タスクページのフィールド」</a> (356 ページ)
デバイスコンテキストを追加	<a href="#">「[デバイスコンテキストを追加]タスクページのフィールド」</a> (359 ページ)
VLAN	<a href="#">「[VLANタスク]ページのフィールド」</a> (363 ページ)
Cisco.comからイメージをダウンロードタスク	<a href="#">「[Cisco.comからイメージをダウンロード]タスクページ」</a> (367 ページ)
デバイスソフトウェアのバックアップタスク	<a href="#">「[デバイスソフトウェアのバックアップ]タスクページのフィールド」</a> (369 ページ)

トピック	参照先：
ポリシー準拠の確認タスク	<a href="#">「[ポリシー準拠の確認]タスクページのフィールド」</a> （372 ページ）
サマリレポートの生成タスク	<a href="#">「[サマリレポートの生成]タスクページのフィールド」</a> （375 ページ）
電子メールレポートタスク	<a href="#">「[電子メールレポート]タスクページのフィールド」</a> （377 ページ）
リモートエージェントを配布タスク	<a href="#">「[リモートエージェントを配布]タスクページのフィールド」</a> （380 ページ）
FQDNの解決タスク	<a href="#">「[FQDNの解決]タスクページのフィールド」</a> （382 ページ）
データの整理タスク	<a href="#">「[データの整理]タスクページのフィールド」</a> （385 ページ）
外部アプリケーションの実行タスク	<a href="#">「[外部アプリケーションの実行]タスクページのフィールド」</a> （388 ページ）
マルチタスクプロジェクトの予定	<a href="#">「マルチタスクプロジェクトの予定」</a> （391 ページ）
[自分のタスク]の表示	<a href="#">「[自分のタスク]ページのフィールド」</a> （397 ページ）
予定されたタスクの表示	<a href="#">「予定されたタスクの表示」</a> （400 ページ）
実行中のタスクの表示	<a href="#">「実行中のタスクの表示」</a> （402 ページ）
最近のタスクの表示	<a href="#">「最近のタスクの表示」</a> （404 ページ）
タスク負荷の表示	<a href="#">「タスク負荷の表示」</a> （409 ページ）

## タスクとは

タスクは、HP Network Automation (NA) がユーザのネットワークとやりとりを行う手段として最も重要なメカニズムです。タスクは特定のアクションであり、スケジュールすることも、すぐに実行することもできます。[タスク情報]ページには、デバイスや構成の変更を特定するスナップショットや、準拠しているデバイスかどうかを特定するためのソフトウェアポリシー準拠など、実行されたタスクの結果が表示されます。

## アドホックデバイスグループへのタスクの実行

アドホックデバイスグループを作成することで、一時デバイスグループに対して、タスクやタスク群（マルチタスクプロジェクト）を実行できます。次のいずれかの方法で、アドホックデバイスグループを作成できます。

- [デバイスリスト]ページのチェックボックスでデバイスを選択し、[アクション]ドロップダウンメニューでデバイスに対して実行するタスクを選択します。詳細については、「[デバイスの表示](#)」(186ページ)を参照してください。
- アドホックデバイスのリストを含むCSVファイルをインポートします。たとえば、ユーザのネットワーク上に200デバイスあり、50デバイスのグループごとに1つのDNSサーバがあると仮定します。4つのデバイスグループ（50デバイスで）を作成する代わりに、DNSサーバにデバイスをマッピングするCSVファイルを生成できます。次に、そのCSVファイルをコマンドスクリプトにロードし、1つのタスクを実行して、すべてのDNSサーバを更新することができます。コマンドスクリプトの実行の詳細については、「[\[コマンドスクリプトの実行\]タスクページのフィールド](#)」(304ページ)を参照してください。

マルチタスクプロジェクトの詳細については、「[\[マルチタスクプロジェクト\]ページのフィールド](#)」(393ページ)を参照してください。

## タスクの予定

タスクの作成または更新時に、他のタスクより高い優先順位で実行するようにタスクの優先順位を設定できます。タスクの優先度レベルは1～5であり、1が最も高いタスク優先度レベルです。優先度の高いタスクは優先度の低いタスクより前に実行されます。

デフォルトで、すべてのタスクはタスク優先度レベル3で作成されます。タスクに優先度レベル1を設定するには、管理者権限がつか、NA管理者からそのための権限を付与される必要があります。この権限を持たないユーザは、タスクに優先度レベル2～5までを設定できます。コマンド権限の詳細については、[「\[ユーザロールの新規作成\] ページのフィールド」 \(259 ページ\)](#) を参照してください。

現在実行中の親タスクの優先度を変更すると、「保留中」または「待機中」状態にある既存の子タスクは、その優先度が親タスクの優先度に適切に変更されます。ただし、まだ作成されていない子タスクや、「実行中」または「一時停止」などの別の状態にある子タスクは、親タスクに元々設定されている優先度のままになります。親タスクが実行中でなく、その優先度を変更すると、親タスクが持つすべての子タスクには新しい優先度が設定されます。

**注意：** タスク関連APIには `-taskpriority` オプションがあります。詳細については、『NA CLI/API Command Reference』を参照してください。

## 用語

NA タスクスケジューラの説明では次の用語が使用されます。

- **タスク：** NA タスクスケジューラによって実行される最小単位。1つのタスクには1つ以上の子タスクを含めることができます。タスクには、独自のNAコアID、タスクID、親タスクID（省略可能）、優先度、および予定時間が設定されます。NA コアIDの詳細については、『NA Multimaster Distributed System on Oracle Guide』、または『NA Multimaster Distributed System on SQL Server Guide』を参照してください。
- **タスクキュー：** NA コアID、親タスクID、優先度がそれぞれ同じであるタスクグループ。タスクに親タスクがない場合、そのタスクIDが親タスクIDとして使用されます。
- **タスクキューグループ：** NA コアIDと優先度が同じであるタスクキューのグループ。タスクキューグループは合計5つまで設定できます。
- **タスクプール：** NA コアIDが同じである合計5つのタスクキューグループ。タスクプールはメモリにキャッシュされ、タスクのスケジューリングに使用されます。タスクプールはデータベースで定義されたタスクと同期します。データベースでタスクを作成、更新、または削除すると、NAによってタスクプールが更新されます。タスクがローカルNAコア用の場合、ローカルタスクプールが更新されます。タスクがリモートNAコア用の場合、リモートNAコア上のタスクプールが更新されます。
- **タスクプールキャッシング：** タスクプールはまだ実行されていないすべてのタスクをキャッシュします。

タスクプール以外にあるタスクをポーリングすると、NAは次の処理を行います。

1. タスクキューグループを優先度の高い順に処理します。
2. タスクの予定時間に基づいた先入れ先出しアルゴリズムを使用して各タスクキュー内のタスクを処理します。遅延が生じると、NAはそのタスクの優先度を上げます。このタスクのすべてのサブタスクは新しい優先度を使用します。タスクが反復タスクの場合、新しい優先度はこのタスクと、現在のオカレンスのサブタスクにのみ適用されます。

使用可能なメモリが不十分な場合、NAは同時タスクを最大限まで実行しません。その結果、[最大同時タスク]が200に設定されている場合、NAは200個の同時タスクすべてを実行できないこともあります。最大同時タスクの設定の詳細については、「[\[サーバ\]ページのフィールド](#)」(52ページ)を参照してください。

**注意：**(ユーザでなく)スケジューラによってタスク(予定時間とタスクの優先度)を再スケジュールする必要がある場合、新しい情報はタスクプール内でのみ更新されます。タスクはデータベースには保存されず、ユーザは使用することができません。

## ラウンドロビングループタスク

タスクが完了すると、NAはグループ1からの次のサブタスクとグループ2からの次のサブタスクを交互に実行します。たとえば、ラウンドロビンアルゴリズムを使用して、午前10時に10,000個のデバイスに対してグループタスクを開始し、午前10時5分に10個のデバイスに対してグループタスクを開始した場合、最初のタスクグループの完了を待たずに、2番目のグループタスクを開始することができます。

## タスクテンプレート

タスクテンプレートを使用すると、タスク定義を保存できるようになり、いちから作業を始めなくても、新しいタスクまたは既存のタスクを容易に構成および実行できます。NA ホームページの[自分のワークスペース]領域の下にある[自分のお気に入り]セクションに、頻繁に実行するタスクへのリンクを作成することもできます。

タスクテンプレートを作成するには次の3の方法があります。

- [タスクの新規作成]または[タスクを編集]ページで、[保存オプション]フィールドの[タスクテンプレートとして保存]オプションをクリックします。その結果、タスクはテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクの構成の詳細については、「[NA タスク](#)」(282 ページ) を参照してください。
- [予定タスク]ページの[アクション]列にある[テンプレートの作成]リンクをクリックします。詳細については、「[\[予定タスク\]ページのフィールド](#)」(400 ページ) を参照してください。
- [最近のタスク]ページの[アクション]列にある[テンプレートの作成]リンクをクリックします。詳細については、「[\[最近のタスク\]ページのフィールド](#)」(404 ページ) を参照してください。

マルチタスクプロジェクトをスケジュールし、このプロジェクトをタスクテンプレートとして保存する場合、プロジェクトのサブタスクのために、プロジェクトを適用するデバイスまたはデバイスグループ、あるいはその両方をすべて選択する必要があります。また、マルチタスクプロジェクトを実行するための適切な権限も必要です。詳細については、「[マルチタスクプロジェクトの予定](#)」(391 ページ) を参照してください。

**注意：** [タスクの検索]ページでタスクテンプレートを検索できます。詳細については、「[タスクの検索](#)」(502 ページ) を参照してください。

現在のタスクテンプレートを表示するには、メインメニューバーの[タスク]の下にある[タスクテンプレート]をクリックします。[タスクテンプレート]ページが開きます。

**注意：** [タスクテンプレート]ページには、[予定タスク]、[実行中のタスク]、および[最近のタスク]ページからも移動できます。

フィールド	説明/アクション
自分のタスク	[自分のタスク]ページが開きます。詳細については、「 <a href="#">[自分のタスク]ページのフィールド</a> 」(397 ページ) を参照してください。
自分のドラフト	[自分のドラフト]ページが開きます。詳細については、「 <a href="#">[自分のタスク]ページのフィールド</a> 」(397 ページ) を参照してください。
承認の要求	[承認の要求]ページが開きます。このページで、現在のログインユーザによる承認が必要なタスクを表示できます。詳細については、「 <a href="#">承認の要求</a> 」(670 ページ) を参照してください。
予定タスク	[予定タスク]ページが開きます。詳細については、「 <a href="#">[予定タスク]ページのフィールド</a> 」(400 ページ) を参照してください。
実行中のタスク	[実行中のタスク]ページが開きます。詳細については、「 <a href="#">[実行中のタスク]ページのフィールド</a> 」(402 ページ) を参照してください。
最近のタスク	[最近のタスク]ページが開きます。詳細については、「 <a href="#">[最近のタスク]ページのフィールド</a> 」(404 ページ) を参照してください。
チェックボックス	左側のチェックボックスを使用してテンプレートを削除できます。テンプレートを選択したら、[アクション] ドロップダウンメニューをクリックし、[削除]をクリックします。横の[選択]ドロップダウンメニューにより、すべてのテンプレートを選択または選択解除できます。



フィールド	説明/アクション
作成日	NAがタスクの実行を開始した日付と時刻を表示します。
テンプレート名	テンプレート名を表示します。
ホスト/グループ	タスクに関連するネットワークデバイスのホスト名またはグループ名を表示します。リンクをクリックすると、[デバイス情報]ページが開きます。このページで、グループ内のデバイスの詳細情報を表示できます。
優先度	タスクの優先度を表示します。タスクの優先度レベルは1～5であり、1が最も高いタスク優先度レベルです。詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
パーティション	セキュリティや業務上の理由でパーティションを作成した場合、パーティションは列に表示されます。パーティションの作成の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」(148ページ)を参照してください。
作成者	タスクをスケジューリングしたユーザ（またはタスクを最後に変更したユーザ）のログイン名を表示します。
コメント	タスクについてのコメントを表示します。
アクション	次のアクションを選択できます。 <ul style="list-style-type: none"> <li>• 削除：テンプレートを削除することを確認するダイアログボックスが開きます。テンプレートを削除すると、それに対応するお気に入りリンクも削除されます。</li> <li>• 編集：選択したタスクの[タスクを編集]ページが開きます。たとえば、[タスクを編集 - スナップショット]ページが開きます。タスクを編集し、そのタスクをテンプレートとして保存できます。（<b>注意</b>：テンプレートの名前を変更しないと、新しいテンプレートによって古いテンプレートが上書きされます。）</li> <li>• 実行：[タスクを再実行]ページが開きます。このページでは、タスクを再実行したり、タスクを編集して再度実行することができます。（<b>注意</b>：このオプションは、タスクの“スケジューリングオプション”での構成に従ってタスクを再実行できる場合にのみ表示されます。</li> <li>• お気に入りに追加：タスクページに移動しなくてもタスクを実行できるように、NAホームページの[自分のワークスペース]領域の[自分のお気に入り]セクションにタスクを追加します。</li> <li>• クイック起動への追加：NAホームページの[自分のワークスペース]タブの下にある[クイック起動]セクションに、[クイック起動]リンクを追加します。[クイック起動]リンクでは、現在のタスクテンプレートの名前が仮に付けられます。リンク名を変更したい場合は、表示されたポップアップボックスを使用してください。クイック起動の詳細については、「<a href="#">クイック起動とは</a>」(265ページ)を参照してください。</li> </ul>
1ページに表示する結果の数	ドロップダウンメニューから、ページあたりの表示項目数を設定できます。デフォルト値は25です。

## NA タスク

[タスク/テンプレートの新規作成]ページを開くには、[タスク]の下のメニューバーの[タスク]を選択して、スケジュールするタスクをクリックします。そのタスクの[タスク/テンプレートの新規作成]ページが開きます。次の表に、ユーザが選択できるタスクのリストを示します。

タスク	参照先
Syslogの構成	「[Syslogの構成]タスクページのフィールド」(284ページ)
パスワードの配布	「[パスワードの配布]タスクページのフィールド」(288ページ)
ドライバの検出	「[ドライバの検出]タスクページのフィールド」(293ページ)
デバイスのリブート	「[デバイスのリブート]タスクページのフィールド」(296ページ)
ICMPテストの実行	「[ICMPテストの実行]タスクページのフィールド」(299ページ)
コマンドスクリプトの実行	「[コマンドスクリプトの実行]タスクページのフィールド」(304ページ)
診断の実行	「[診断の実行]タスクページのフィールド」(310ページ)
スナップショットの取得	「[スナップショットの取得]タスクページのフィールド」(315ページ)
スタートアップとランニングの同期	「[スタートアップとランニングの同期]タスクページのフィールド」(319ページ)
デバイスソフトウェアの更新	「[デバイスソフトウェアの更新]タスクページのフィールド」(323ページ)
インポート	「[デバイスのインポート]タスクページのフィールド」(329ページ)
ユーザのインポート	「[ユーザのインポート]タスクページのフィールド」(334ページ)
ネットワークデバイスの検出	「[ネットワークデバイスの検出]タスクページのフィールド」(341ページ)
重複の削除	「[重複の削除]タスクページのフィールド」(347ページ)
OS 分析	「[OS分析]タスクページのフィールド」(350ページ)
ポートスキャン	「[ポートスキャン]ページのフィールド」(353ページ)
テンプレートからデバイスをプロビジョニング	「[デバイスのプロビジョニング]タスクページのフィールド」(356ページ)
デバイスコンテキスト	「[デバイスコンテキストを追加]タスクページのフィールド」(359ページ)
VLAN	「[VLANタスク]ページのフィールド」(363ページ)
Cisco.comからイメージをダウンロードタスク	「[Cisco.comからイメージをダウンロード]タスクページ」(367ページ)
テンプレートからデバイスをプロビジョニング	「[デバイスのプロビジョニング]タスクページのフィールド」(356ページ)
Cisco.comからイメージをダウンロードタスク	「[Cisco.comからイメージをダウンロード]タスクページ」(367ページ)
デバイスソフトウェアのバックアップタスク	「[デバイスソフトウェアのバックアップ]タスクページのフィールド」(369ページ)
ポリシー準拠の確認	「[ポリシー準拠の確認]タスクページのフィールド」(372ページ)
サマリレポートの生成	「[サマリレポートの生成]タスクページのフィールド」(375ページ)
電子メールレポート	「[電子メールレポート]タスクページのフィールド」(377ページ)
リモートエージェントの配布	「[リモートエージェントを配布]タスクページのフィールド」(380ページ)

タスク	参照先
FQDNの解決	<a href="#">「[FQDNの解決]タスクページのフィールド」</a> （382 ページ）
データの整理	<a href="#">「[データの整理]タスクページのフィールド」</a> （385 ページ）
外部アプリケーションの実行	<a href="#">「[外部アプリケーションの実行]タスクページのフィールド」</a> （388 ページ）

## [Syslogの構成]タスクページのフィールド

Syslogの構成タスクでは、1つ以上のデバイスの自動構成をスケジューリングして、Syslogメッセージを送信できます。NAではSyslogメッセージを使用して、リアルタイムで構成変更を検出します。

検出後（または各デバイスにドライバを割り当てるとき）、NAは次の手順を実行します。

1. 構成のスナップショットを取得します。
2. NAにSyslogメッセージを送信するように構成を更新します。
3. デバイスが変更検出を有効にするように自動構成されていることを示すコメントを、構成に書き込みます。
4. 最終的なスナップショットを取得します。

フィールド	説明/アクション
タスク名	[Syslogの構成]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセレクトタの使用方法的詳細については、「<a href="#">デバイスセレクトタ</a>」(142ページ)を参照してください。</li> <li>• CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b>（[デバイスリスト]ページのチェックボックスでグループのデバイスを選択して）アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。

フィールド	説明/アクション
<b>タスクオプション</b>	
セッションログ	<p>完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。セッションのログ記録を有効にした状態で、デバイスと対話するすべてのタスクが実行できます。タスク実行中のデバイスとの対話に関する詳細なログが記録されます。セッションログは、デバイス固有の問題をデバッグするための第一段階として表示してください。セッションログでは、CLI、SNMPおよびタスクで実行されるすべての転送プロトコルアクションの詳細がわかります。(注意: 大量のデータが格納されることがあります。ログ記録の詳細については、「<a href="#">ログ記録</a>」(96 ページ) を参照してください)。</p>
強制的に保存	<p>デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみに適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。</p> <ul style="list-style-type: none"> <li>このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>(注意: この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます)。</p>
Syslogの設定	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>NA syslogサーバでログを取得するようにデバイスを設定する (デフォルト)。</li> <li>デバイスはsyslogリレーにログ出力し、正しいログレベルに設定する。[リレーホスト]を入力します。</li> </ul>
推定継続時間	<p>このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。</p>

#### デバイス資格情報のオプション

デバイス資格情報のオプションは、[システム管理設定]の[デバイスアクセス]ページで設定されている[標準デバイスの資格情報を許可]、[タスクごとのデバイスの資格情報を許可]、[ユーザのAAA資格情報を許可]の内1つまたは複数のオプションの構成に従って表示されます。[タスクごとのデバイスの資格情報を許可]を有効にすると、適切なパスワード情報を入力するよう求めるプロンプトが表示されます。また、複数のデバイス資格情報オプションを有効にすると、タスクを実行するときにオプションを選択するよう求めるプロンプトが表示されます。デバイス資格情報オプションを1つだけ有効にした場合は自動的にオプションが使用され、プロンプトは表示されません (デバイス資格情報の有効化の詳細については、「[\[デバイスアクセス\]ページのフィールド](#)」(45 ページ) を参照してください)。

デバイス資格情報	<p>[システム管理設定]の[サーバ]ページで有効にされるデバイス資格情報オプションに応じて、次のオプションを1つ以上選択できます。</p> <ul style="list-style-type: none"> <li>標準デバイス固有の資格情報とネットワーク全体のパスワードルールの使用 (デフォルト)。</li> <li>特定のタスク単位のパスワードを使用。[ユーザ名]、[パスワード]、[パスワードの確認]、[イネーブルパスワードの確認]、[SNMP読み取り専用コミュニティ文字列]、および[SNMP読み取り/書き込みコミュニティ文字列]への入力を求めるプロンプトが表示されます。</li> <li>タスク所有者のAAA資格情報の使用。タスク所有者には、定義された有効なAAA資格情報が必要です。(注意: 標準パスワードルールとデバイス固有パスワードを使用します。ただし、タスク所有者のAAAユーザ名とパスワードが適用されます。)</li> </ul>
----------	---

フィールド	説明/アクション
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>

フィールド	説明/アクション
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールアドレスです。
<b>タスクログ</b>	
タスクログ	利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift] キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、 <a href="#">「ログ記録」(96ページ)</a> を参照してください。

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、[「\[タスク情報\]ページのフィールド」\(406ページ\)](#)を参照してください。

タスクが今後を開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、[「\[自分のタスク\]ページのフィールド」\(397ページ\)](#)を参照してください。

## [パスワードの配布]タスクページのフィールド

パスワードの配布タスクでは、複数のデバイスのパスワード設定やSNMPコミュニティ文字列を、中央の位置から変更できます。

**注意：** ネットワーク全体のパスワードルールを使用する単一デバイスにパスワードを配布すると、NA はデバイス固有のパスワード情報を使用するようにデバイスを設定します。この設定の変更は、[デバイスを編集]ページで行うことができます。単一デバイスにパスワードを配布するには、[プロビジョニング]メニューから[パスワードの配布]を選択します。「[プロビジョニングメニューオプション](#)」(239 ページ) を参照してください。

NA でユーザのネットワークがAAAを使用している場合、NAではなくAAAサーバを通じてパスワード変更をします。そうしない場合、NAがデバイスとのコンタクトを失う可能性があります。また、実際には、NAはAAAパスワードおよびデバイス保守のユーザアカウントは管理していません。NAは、単一デバイスのパスワードの配布をスケジューリングするときに要求されるものと、グループパスワードの配布をスケジューリングする場合の[意味]リンクの出力を管理します。

Nortel Baystack 450などのメニュー駆動型デバイスを含む大半のデバイスについて、NAではパスワード変更とコミュニティ文字列変更をサポートしています。サポートするデバイスの詳細については、Driver Release Service (DRS) ドキュメントを参照してください。DRSは、ドライバの自動リリースおよび配信システムです。

変更が成功すると、NAはデバイスのスナップショットを実行し、変更された構成をダウンロードします。最近のパスワード変更とコミュニティ文字列の変更をすべてすぐに表示するには、[構成変更]ページへ移動します。詳細については、「[デバイス構成変更の表示](#)」(172 ページ) を参照してください。

AAAを使用してパスワード配布機能でデバイスパスワードを変更する場合、NAは、AAAではなく新規パスワードを使用してデバイスへの接続を試行する場合があります。ただし、それでもデバイスはAAAログインを求める可能性もあります。必要に応じて、AAAを使用するようにデバイスを手動で再構成する必要があります。また、適切なAAA資格情報を使用してデバイスにログインするようにNAを再設定する必要があります。

**注意：** パスワードの配布タスクが新規資格情報のユーザ名部分を、NAがデバイスにアクセスするのに必要となる資格情報の一部として指定しない場合があります。これは、デバイスへのログインにユーザ名が必要な場合に、パスワードの配布タスクを実行して、デバイスのパスワード変更を行う場合に発生します。タスクが完了し、スナップショットが実行されると、ユーザ名が存在しない旨のエラーメッセージが表示されます。この現象が発生した場合、パスワードの配布タスクの実行後に、デバイスを編集して[デバイス固有パスワード情報を使用]セクションにユーザ名を追加します。詳細については、「[\[デバイスパスワードルール\]ページのフィールド](#)」(132 ページ) を参照してください。



フィールド	説明/アクション
タスク名	[パスワードの配布]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセクタの使用方法的詳細については、「<a href="#">デバイスセクタ</a>」(142ページ)を参照してください。</li> <li>• CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b> ([デバイスリスト]ページのチェックボックスでグループのデバイスを選択して) アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
セッションログ	完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。セッションのログ記録を有効にした状態で、デバイスと対話するすべてのタスクが実行できます。タスク実行中のデバイスとの対話に関する詳細なログが記録されます。セッションログは、デバイス固有の問題をデバッグするための第一段階として表示してください。セッションログでは、CLI、SNMPおよびタスクで実行されるすべての転送プロトコルアクションの詳細がわかります。（ <b>注意：</b> 大量のデータが格納されることがあります。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」(96ページ)を参照してください。）

フィールド	説明/アクション
強制的に保存	<p>デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみ適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。</p> <ul style="list-style-type: none"> <li>このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>(注意: この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます)。</p>
制限付きアクセスのユーザ名	<p>デバイスアクセスに必要な、制限付きアクセスのユーザ名を入力します。デバイスのベンダーやオペレーティングシステムによってユーザ名が異なります。デバイス固有の情報の[意味]リンクをクリックします。(注意: ユーザ名が空白の場合、関連するフィールドはデバイスで変更されません。)</p>
制限付きアクセスパスワード	<p>デバイスアクセスに必要な、制限付きアクセスのパスワードを入力します。デバイスのベンダーやオペレーティングシステムによってパスワードが異なります。デバイス固有の情報の[意味]リンクをクリックします。(注意: パスワードが空白の場合、関連するフィールドはデバイスで変更されません。)</p>
パスワードの確認	<p>確認用にパスワードを再入力します。</p>
フルアクセスのユーザ名	<p>デバイスアクセスに必要な、フルアクセスのユーザ名を入力します。デバイスのベンダーやオペレーティングシステムによってユーザ名が異なります。デバイス固有の情報の[意味]リンクをクリックします。(注意: ユーザ名が空白の場合、関連するフィールドはデバイスで変更されません。)</p>
フルアクセスのパスワード	<p>デバイスアクセスに必要な、フルアクセスパスワードを入力します。デバイスのベンダーやオペレーティングシステムによってパスワードが異なります。デバイス固有の情報の[意味]リンクをクリックします。(注意: パスワードが空白の場合、関連するフィールドはデバイスで変更されません。)</p>
パスワードの確認	<p>確認用にパスワードを再入力します。</p>
SNMP読み取りコミュニティ文字列	<p>SNMP読み取りコミュニティ文字列を追加するには、右側のボックスに文字列を入力して、&lt;&lt;[コミュニティ文字列の追加]をクリックします。SNMP読み取りコミュニティ文字列を削除するには、左側のボックスで名前を選択して、[コミュニティ文字列を削除]をクリックします。[デバイスの既存のコミュニティ文字列に付加。](デフォルト)または[デバイスの既存のコミュニティ文字列を置換。]を選択します。</p>
SNMP書き込みコミュニティ文字列	<p>SNMP書き込みコミュニティ文字列を追加するには、右側のボックスに文字列を入力して、&lt;&lt;[コミュニティ文字列の追加]をクリックします。SNMP書き込みコミュニティ文字列を削除するには、左側のボックスで名前を選択して、[コミュニティ文字列を削除]をクリックします。[デバイスの既存のコミュニティ文字列に付加。](デフォルト)または[デバイスの既存のコミュニティ文字列を置換。]を選択します。</p>
推定継続時間	<p>このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。</p>

フィールド	説明/アクション
<b>デバイス資格情報のオプション</b> デバイス資格情報のオプションは、[システム管理設定]の[デバイスアクセス]ページで設定されている[標準デバイスの資格情報を許可]、[タスクごとのデバイスの資格情報を許可]、[ユーザのAAA資格情報を許可]の内1つまたは複数のオプションの構成に従って表示されます。[タスクごとのデバイスの資格情報を許可]を有効にすると、適切なパスワード情報を入力するよう求めるプロンプトが表示されます。また、複数のデバイス資格情報オプションを有効にすると、タスクを実行するときにオプションを選択するよう求めるプロンプトが表示されます。デバイス資格情報オプションを1つだけ有効にした場合は自動的にオプションが使用され、プロンプトは表示されません（デバイス資格情報の有効化の詳細については、「 <a href="#">[デバイスアクセス]ページのフィールド</a> 」（45ページ）を参照してください）。	
デバイス資格情報	<p>[システム管理設定]の[サーバ]ページで有効にされるデバイス資格情報オプションに応じて、次のオプションを1つ以上選択できます。</p> <ul style="list-style-type: none"> <li>標準デバイス固有の資格情報とネットワーク全体のパスワードルールの使用（デフォルト）。</li> <li>特定のタスク単位のパスワードを使用。[ユーザ名]、[パスワード]、[パスワードの確認]、[イネーブルパスワードの確認]、[SNMP読み取り専用コミュニティ文字列]、および[SNMP読み取り/書き込みコミュニティ文字列]への入力を求めるプロンプトが表示されます。</li> <li>タスク所有者のAAA資格情報の使用。タスク所有者には、定義された有効なAAA資格情報が必要です。（<b>注意</b>：標準パスワードルールとデバイス固有パスワードを使用します。ただし、タスク所有者のAAAユーザ名とパスワードが適用されます。）</li> </ul>
<b>承認オプション</b> 承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>再試行なし（デフォルト）</li> <li>1回</li> <li>2回</li> <li>3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	使用不可

フィールド	説明/アクション
<b>タスク完了時の通知</b>	
タスク完了時の通知	NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。 ヒント：電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift] キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、 <b>「ログ記録」(96ページ)</b> を参照してください。

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、**「[タスク情報]ページのフィールド」(406ページ)**を参照してください。

タスクが今後に開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、**「[自分のタスク]ページのフィールド」(397ページ)**を参照してください。

## [ドライバの検出]タスクページのフィールド

ドライバの検出タスクでは、ドライバの検出をスケジューリングできます。

フィールド	説明/アクション
タスク名	[ドライバの検出]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセクタの使用方法の詳細については、「<a href="#">デバイスセクタ</a>」(142ページ)を参照してください。</li> <li>CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b>（[デバイスリスト]ページのチェックボックスでグループのデバイスを選択して）アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>すぐに開始（デフォルト）</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
セッションログ	完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。セッションのログ記録を有効にした状態で、デバイスと対話するすべてのタスクが実行できます。タスク実行中のデバイスとの対話に関する詳細なログが記録されます。セッションログは、デバイス固有の問題をデバッグするための第一段階として表示してください。セッションログでは、CLI、SNMPおよびタスクで実行されるすべての転送プロトコルアクションの詳細がわかります。（ <b>注意：</b> 大量のデータが格納されることがあります。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」(96ページ)を参照してください。）
オプション	ドライバが設定されていない場合は、[ドライバが設定されていない場合のみ]チェックボックスをオンにします（デフォルト）。
推定継続時間	このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。

## フィールド

## 説明/アクション

## デバイス資格情報のオプション

デバイス資格情報のオプションは、[システム管理設定]の[デバイスアクセス]ページで設定されている[標準デバイスの資格情報を許可]、[タスクごとのデバイスの資格情報を許可]、[ユーザのAAA資格情報を許可]の内1つまたは複数のオプションの構成に従って表示されます。[タスクごとのデバイスの資格情報を許可]を有効にすると、適切なパスワード情報を入力するよう求めるプロンプトが表示されます。また、複数のデバイス資格情報オプションを有効にすると、タスクを実行するときにオプションを選択するよう求めるプロンプトが表示されます。デバイス資格情報オプションを1つだけ有効にした場合は自動的にオプションが使用され、プロンプトは表示されません（デバイス資格情報の有効化の詳細については、「[\[デバイスアクセス\]ページのフィールド](#)」（45ページ）を参照してください）。

デバイス資格情報	<p>[システム管理設定]の[サーバ]ページで有効にされるデバイス資格情報オプションに応じて、次のオプションを1つ以上選択できます。</p> <ul style="list-style-type: none"> <li>• 標準デバイス固有の資格情報とネットワーク全体のパスワードルールの使用（デフォルト）。</li> <li>• 特定のタスク単位のパスワードを使用。[ユーザ名]、[パスワード]、[パスワードの確認]、[イネーブルパスワードの確認]、[SNMP読み取り専用コミュニティ文字列]、および[SNMP読み取り/書き込みコミュニティ文字列]への入力を求めるプロンプトが表示されます。</li> <li>• タスク所有者のAAA資格情報の使用。タスク所有者には、定義された有効なAAA資格情報が必要です。（<b>注意</b>：標準パスワードルールとデバイス固有パスワードを使用します。ただし、タスク所有者のAAAユーザ名とパスワードが適用されます。）</li> </ul>
----------	--

## 承認オプション

承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。

承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。

## スケジューリングオプション

再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。

フィールド	説明/アクション
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	<p>メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。</p>
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96ページ)</b>を参照してください。</p>

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。

詳細については、**「[タスク情報]ページのフィールド」(406ページ)**を参照してください。タスクが今後を開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、**「[自分のタスク]ページのフィールド」(397ページ)**を参照してください。



## [デバイスのリブート]タスクページのフィールド

デバイスのリブートタスクでは、デバイスをリブートできます。

フィールド	説明/アクション
タスク名	[デバイスのリブート]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセクタの使用方法的詳細については、「<a href="#">デバイスセクタ</a>」(142ページ)を参照してください。</li> <li>CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b>（[デバイスリスト]ページのチェックボックスでグループのデバイスを選択して）アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>すぐに開始（デフォルト）</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
セッションログ	完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。大量のデータを格納することができます。このオプションは、デバイスのトラブルシューティングにのみお勧めします。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」(96ページ)を参照してください。
強制的に保存	デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみ適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。 <ul style="list-style-type: none"> <li>このタスクの完了時に、NAで現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>NAでスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>（<b>注意：</b>この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます。）</p>



フィールド	説明/アクション
推定継続時間	このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。
<b>デバイス資格情報のオプション</b> デバイス資格情報のオプションは、[システム管理設定]の[デバイスアクセス]ページで設定されている[標準デバイスの資格情報を許可]、[タスクごとのデバイスの資格情報を許可]、[ユーザのAAA資格情報を許可]の内1つまたは複数のオプションの構成に従って表示されます。[タスクごとのデバイスの資格情報を許可]を有効にすると、適切なパスワード情報を入力するよう求めるプロンプトが表示されます。また、複数のデバイス資格情報オプションを有効にすると、タスクを実行するときにオプションを選択するよう求めるプロンプトが表示されます。デバイス資格情報オプションを1つだけ有効にした場合は自動的にオプションが使用され、プロンプトは表示されません（デバイス資格情報の有効化の詳細については、「 <a href="#">[デバイスアクセス]ページのフィールド</a> 」（45ページ）を参照してください）。	
デバイス資格情報	[システム管理設定]の[サーバ]ページで有効にされるデバイス資格情報オプションに応じて、次のオプションを1つ以上選択できます。 <ul style="list-style-type: none"> <li>標準デバイス固有の資格情報とネットワーク全体のパスワードルールの使用（デフォルト）。</li> <li>特定のタスク単位のパスワードを使用。[ユーザ名]、[パスワード]、[パスワードの確認]、[イーネブルパスワードの確認]、[SNMP読み取り専用コミュニティ文字列]、および[SNMP読み取り/書き込みコミュニティ文字列]への入力を求めるプロンプトが表示されます。</li> <li>タスク所有者のAAA資格情報の使用。タスク所有者には、定義された有効なAAA資格情報が必要です。（<b>注意</b>：標準パスワードルールとデバイス固有パスワードを使用します。ただし、タスク所有者のAAAユーザ名とパスワードが適用されます。）</li> </ul>
<b>承認オプション</b> 承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>再試行なし（デフォルト）</li> <li>1回</li> <li>2回</li> <li>3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	使用不可。

フィールド	説明/アクション
<b>タスク完了時の通知</b>	
タスク完了時の通知	NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。 ヒント：電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、 <b>「ログ記録」(96ページ)</b> を参照してください。

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、**「[タスク情報]ページのフィールド」(406ページ)**を参照してください。

タスクが今後に開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、**「[自分のタスク]ページのフィールド」(397ページ)**を参照してください。

## [ICMPテストの実行]タスクページのフィールド

ICMP (Internet Control Message Protocol) テストの実行タスクでは、あるデバイスから1つ以上のデバイスへの、pingテストまたはtracerouteテストをスケジューリングできます。

traceroute では、ネットワークを通じて、パケットがたどったパスのトレースを試行します。traceroute は、小さな TTL (Time-To-Live) 値でパケットを送信します。TTL とは、パケットを無限ループさせないための IP ヘッダフィールドのことです。また、ホップリミットとも呼ばれます。traceroute は、"ICMP Time Exceeded" メッセージを送信側に返信するデバイスによって決まります。traceroute によって、パケットの通常の配信パスにあるデバイスは、パスを特定するこの ICMP メッセージを生成します。

Ping (Packet INternet Groper) では、シングルパケットを送信し、シングルパケットの返信をリスンします。ping は、必要な ICMP Echo 機能を使用して実装されています。

通常、traceroute オプションは、1つのデバイスから、そのデバイスが認識しているルートに沿って次のデバイスへ移動することで、アクションを実行します。あるいは、それぞれのルートに沿って、各デバイスへpingを送ります。

traceroute コマンドと ping コマンドは、NA が終了させる機能ではありません。デバイスがそれらの機能を終了させます。宛先デバイスを追跡するために、NA はソースデバイスにログインして、デバイスに適切なコマンドを発行する必要があります。各デバイスは別々に機能を実装できます (まったく実装しない場合もあります)。[ICMP テスト結果] ページには、デバイスが画面上に表示する内容のダンプが表示されます。

ping と traceroute は、ネットワークのトラブルシューティングツールとしてどちらも優れています。たとえば ping を使用して、特定のデバイスにアクセスできるかどうかの確認テストを、100 デバイスに対して実行できます。また、20 デバイスで特定のデバイスへのアクセスに問題がある場合に、自動リモート traceroute を実行して、その宛先デバイスまで各デバイスがたどったパスを確認できます。

**注意：** ICMP テストは、時々または変更後に接続を確認するためだけに使用します。ソフトウェアの監視に代わるものではありません。ICMP テストは10分間に1回以上スケジュールしないようにしてください。

フィールド	説明/アクション
タスク名	[ICMPテストの実行]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280 ページ) を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセクタの使用方法的詳細については、「<a href="#">デバイスセクタ</a>」(142 ページ) を参照してください。</li> <li>CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b> ([デバイスリスト]ページのチェックボックスでグループのデバイスを選択して) アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>すぐに開始（デフォルト）</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278 ページ) を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
セッションログ	完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。セッションのログ記録を有効にした状態で、デバイスと対話するすべてのタスクが実行できます。タスク実行中のデバイスとの対話に関する詳細なログが記録されます。セッションログは、デバイス固有の問題をデバッグするための第一段階として表示してください。セッションログでは、CLI、SNMPおよびタスクで実行されるすべての転送プロトコルアクションの詳細がわかります。（ <b>注意：</b> 大量のデータが格納されることがあります。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」(96 ページ) を参照してください。）
テストタイプ	pingまたはtracerouteを選択してください。
対象ホストリスト	ホストを追加するには、右側のボックスに名前を入力して、[<<ホストの追加]をクリックします。ホストを削除するには、左側のボックスでホスト名を選択して、[ホストの削除]をクリックします。
推定継続時間	このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。

フィールド	説明/アクション
<b>デバイス資格情報のオプション</b>	
<p>デバイス資格情報のオプションは、[システム管理設定]の[デバイスアクセス]ページで設定されている[標準デバイスの資格情報を許可]、[タスクごとのデバイスの資格情報を許可]、[ユーザのAAA資格情報を許可]の内1つまたは複数のオプションの構成に従って表示されます。[タスクごとのデバイスの資格情報を許可]を有効にすると、適切なパスワード情報を入力するよう求めるプロンプトが表示されます。また、複数のデバイス資格情報オプションを有効にすると、タスクを実行するときにオプションを選択するよう求めるプロンプトが表示されます。デバイス資格情報オプションを1つだけ有効にした場合は自動的にオプションが使用され、プロンプトは表示されません（デバイス資格情報の有効化の詳細については、「<a href="#">[デバイスアクセス]ページのフィールド</a>」（45ページ）を参照してください）。</p>	
デバイス資格情報	<p>[システム管理設定]の[サーバ]ページで有効にされるデバイス資格情報オプションに応じて、次のオプションを1つ以上選択できます。</p> <ul style="list-style-type: none"> <li>• 標準デバイス固有の資格情報とネットワーク全体のパスワードルールの使用（デフォルト）。</li> <li>• 特定のタスク単位のパスワードを使用。[ユーザ名]、[パスワード]、[パスワードの確認]、[イネーブルパスワードの確認]、[SNMP読み取り専用コミュニティ文字列]、および[SNMP読み取り/書き込みコミュニティ文字列]への入力を求めるプロンプトが表示されます。</li> <li>• タスク所有者のAAA資格情報の使用。タスク所有者には、定義された有効なAAA資格情報が必要です。（<b>注意</b>：標準パスワードルールとデバイス固有パスワードを使用します。ただし、タスク所有者のAAAユーザ名とパスワードが適用されます。）</li> </ul>
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	<p>タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。</p>
承認の無効化	<p>タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。</p>
ドラフトとして保存	<p>オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。</p>
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	<p>次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。</p>

フィールド	説明/アクション
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	<p>メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。</p>
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96ページ)</b>を参照してください。</p>

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[ICMPテスト結果]ページが開きます。

**注意：** [ICMPテスト結果]ページには、デバイスが画面上に表示する内容のダンプが表示されます。

タスクが成功し、pingオプションが選択されていた場合は、デバイスと[ICMPテストの実行]タスクページに入力した情報によって、次の情報が表示されます。

- 作成日
- コマンド実行
- 結果
- コマンド出力（例：Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms)

traceroute オプションが選択されていた場合は、デバイスと [ICMP テストの実行タスク] ページに入力した情報によって、次の情報が表示されます。

- 作成日
- コマンド実行
- 結果
- コマンド出力（例：

```
1 1ms 1ms 1ms 10.255.111.2
2 4ms 4ms 4ms 10.255.111.3
3 * * * *
```

1列目はホップを表示します。次の3列では、デバイスの応答にかかった時間を表示します。デバイスの応答にかかった時間が、指定されたタイムアウト値よりも長い場合は、アスタリスクを表示します。）最終列では、応答したホストを表示します。

タスクが今後を開始するようにスケジューリングされている場合は、[自分のタスク] ページで新規タスクが強調表示されます。詳細については、「[\[自分のタスク\] ページのフィールド](#)」（397 ページ）を参照してください。

## [コマンドスクリプトの実行]タスクページのフィールド

コマンドスクリプトの実行タスクにより、コマンドスクリプトを実行できます。

フィールド	説明/アクション
コマンドスクリプトの新規作成	[コマンドスクリプトの新規作成]ページが開きます。スクリプトの作成の詳細については、「 <a href="#">[コマンドスクリプトの新規作成]ページのフィールド</a> 」(578ページ)を参照してください。
コマンドスクリプト	[コマンドスクリプト]ページが開きます。詳細については、「 <a href="#">[コマンドスクリプト]ページのフィールド</a> 」(573ページ)を参照してください。
タスク名	[コマンドスクリプトの実行]の名前を表示します。必要に応じて、別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセレクトアの使用方法的詳細については、「<a href="#">デバイスセレクトア</a>」(142ページ)を参照してください。</li> <li>CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b>（[デバイスリスト]ページのチェックボックスでグループのデバイスを選択して）アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>すぐに開始（デフォルト）</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
セッションログ	完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。大量のデータを格納することができます。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」(96ページ)を参照してください。



フィールド	説明/アクション
強制的に保存	<p>デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみ適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。</p> <ul style="list-style-type: none"> <li>• このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>• NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>(注意: この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます)。</p>
実行するコマンドスクリプト	<p>実行するコマンドスクリプトを選択します。選択するスクリプトのタイプによって、オプションが変わります。標準のコマンドスクリプトには次のものが含まれています。</p> <ul style="list-style-type: none"> <li>• Cisco IOS Initial Setup</li> <li>• Cisco IOSによるACL IDに基づいたACLへの行の挿入</li> <li>• Cisco IOSによるハンドルに基づいたACLへの行の挿入</li> <li>• Cisco IOSによるACL IDに基づいたACLからの行の削除</li> <li>• Cisco IOSによるハンドルに基づいたACLからの行の削除</li> <li>• フラッシュの圧縮</li> <li>• Contivity 1100 SNMPコミュニティ文字列の配布</li> <li>• 拡張Ping</li> <li>• 全二重通信</li> <li>• ios_7k_reboot</li> <li>• ios_generic_reboot</li> <li>• ios_l3switch_reboot</li> <li>• Passport 8xxx - コミュニティ文字列の配布</li> <li>• Passport 8xxx-SNMP-v3 コミュニティ文字列の配布</li> <li>• Passport 8xxx - ユーザパスワードの配布</li> <li>• Passport 8xxx-Radiusの有効化</li> <li>• Passport 8xxx-Web サーバの有効化</li> <li>• サンプル - FastEther インターフェイスのプロビジョニング</li> <li>• バナー設定</li> <li>• 必要なときのみバナー設定</li> <li>• 場所設定</li> <li>• NTPサーバ設定</li> <li>• ディレクティッドブロードキャストを無効にする</li> <li>• インターフェイスの更新</li> </ul>
プレビューオプション	<p>完全なスクリプトを作成できます。ただし、実行できません。これにより、実際にコマンドを実行しないで実行するコマンドを表示できます。</p>

フィールド	説明/アクション
スクリプトタイプを限定	次の項目のすべて（デフォルト）または1つを選択します。 <ul style="list-style-type: none"> <li>• 高度なACLスクリプト</li> <li>• ACLアプリケーションスクリプト</li> <li>• ACL作成スクリプト</li> <li>• ACL編集スクリプト</li> </ul>
<b>選択するコマンドスクリプトによって、次のオプションの表示が変わります。</b>	
モード	Cisco ExecやNortel Managerなどのデバイスアクセスモードを表示します。これはデバイスプラットフォームに類似しています。
変数	スクリプトに入力する変数フィールドがある場合は、値を入力します。終了したら、[スクリプトを更新]をクリックして、これらの変数で実行するスクリプトを表示できます。カスタム変数の定義方法の詳細については、 <a href="#">「[コマンドスクリプトの新規作成]ページのフィールド」(578ページ)</a> を参照してください。
デバイスファミリ	(高度なスクリプティング) スクリプトを実行するデバイスファミリの名前を表示します。デバイスファミリとは、類似する構成CLIコマンドシンタックスを共有する、デバイスの集合のことです。
パラメータ	スクリプトのパラメータを入力します。
スクリプト	実行するデバイス固有のコマンドを表示します。スクリプトのインスタンスを編集できます。ただし、インスタンス実行後の変更は保存できません。複数のモードがある場合は、スクリプトの1つのインスタンスが各モードに表示されます。 <p><b>注意：</b>スクリプトボックスの高さと幅は、[システム管理設定]ページの[ユーザインターフェイス]タブの設定で制御できます。スクリプティング機能を広範囲にわたって使用する場合、スクロールしなくてもスクリプトを確認できるように、これらの設定の調整が必要となることがあります。</p>
配布オプション	スクリプトを一括で配布するのではなく1行ずつ実行するには、[配布オプション]チェックボックスをオンにします。一括配布の方法（Cisco IOS構成スクリプトなど）でスクリプト実行できるデバイスは、可能であれば常にその方法で実行します。デフォルトでは、スクリプトのすべての内容が配布されて、1つのバッチで実行されます。エラーが発生した場合も、スクリプトを実行し続けます。このようなケースで1行ずつスクリプトを実行すると、エラーをキャプチャして実行が停止します。
待機オプション	デフォルトではオンです。このオプションをオフにすると、同一のデバイスで別のタスクが既に実行されている場合でも、タスクを実行できます。
言語	(高度なスクリプティング) スクリプトの記述に使用した言語を表示します。
推定継続時間	このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。

## フィールド

## 説明/アクション

**デバイス資格情報のオプション**

デバイス資格情報のオプションは、[システム管理設定]の[デバイスアクセス]ページで設定されている[標準デバイスの資格情報を許可]、[タスクごとのデバイスの資格情報を許可]、[ユーザのAAA資格情報を許可]の内1つまたは複数のオプションの構成に従って表示されます。[タスクごとのデバイスの資格情報を許可]を有効にすると、適切なパスワード情報を入力するよう求めるプロンプトが表示されます。また、複数のデバイス資格情報オプションを有効にすると、タスクを実行するときにオプションを選択するよう求めるプロンプトが表示されます。デバイス資格情報オプションを1つだけ有効にした場合は自動的にオプションが使用され、プロンプトは表示されません（デバイス資格情報の有効化の詳細については、「[\[デバイスアクセス\]ページのフィールド](#)」（45ページ）を参照してください）。

デバイス資格情報 [システム管理設定]の[サーバ]ページで有効にされるデバイス資格情報オプションに応じて、次のオプションを1つ以上選択できます。

- 標準デバイス固有の資格情報とネットワーク全体のパスワードルールの使用（デフォルト）。
- 特定のタスク単位のパスワードを使用。[ユーザ名]、[パスワード]、[パスワードの確認]、[イネーブルパスワードの確認]、[SNMP読み取り専用コミュニティ文字列]、および[SNMP読み取り/書き込みコミュニティ文字列]への入力を求めるプロンプトが表示されます。
- タスク所有者のAAA資格情報の使用。タスク所有者には、定義された有効なAAA資格情報が必要です。（**注意**：標準パスワードルールとデバイス固有パスワードを使用します。ただし、タスク所有者のAAAユーザ名とパスワードが適用されます。）

**タスク前/タスク後スナップショットオプション**

スナップショットのオプションは、[システム管理設定]の下の[構成管理]ページでユーザによる無効化がシステムで有効に構成されている場合にのみ表示されます（詳細については、「[\[構成管理\]ページのフィールド](#)」（36ページ）を参照してください）。

タスク前スナップショット 次のオプションのいずれかを選択します。

- なし（デフォルト）
- タスクの一部として

タスク後スナップショット 次のオプションのいずれかを選択します。

- なし
- タスクの一部として（デフォルト）
- 個別のタスクとしてスケジュール

**承認オプション**

承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。

承認要求 タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。

承認の無効化 タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。

ドラフトとして保存 オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。

フィールド	説明/アクション
<b>スケジューリングオプション</b>	
開始日	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	<p>次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。</p>
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	<p>メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。</p>
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96ページ)</b>を参照してください。</p>

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、「[\[タスク情報\]ページのフィールド](#)」(406ページ)を参照してください。

タスクが今後に開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、「[\[自分のタスク\]ページのフィールド](#)」(397ページ)を参照してください。

## [診断の実行]タスクページのフィールド

診断の実行タスクでは、診断の実行をスケジューリングできます。[タスク]の下メニューバーで[タスクの新規作成]を選択し、[診断の実行]をクリックします。[診断の実行]ページが開きます。

フィールド	説明/アクション
診断の新規作成	[診断の新規作成]ページが開きます。詳細については、「 <a href="#">[診断の新規作成]ページのフィールド</a> 」(551 ページ) を参照してください。
診断	[診断]ページが開きます。診断の管理の詳細については、「 <a href="#">[診断]ページのフィールド</a> 」(549 ページ) を参照してください。
タスク名	[診断の実行]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280 ページ) を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセクタの使用方法的詳細については、「<a href="#">デバイスセクタ</a>」(142 ページ) を参照してください。</li> <li>CSV ファイル：デバイスのリストを含む CSV ファイルの名前を入力するか、または参照します。CSV ファイルでは、CSV ファイルの各行 (IP アドレスとホスト名) に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクの CSV テンプレート]へのリンクをクリックすると、サンプルの CSV ファイルをダウンロードできます。</li> </ul> <p><b>注意：</b> ([デバイスリスト]ページのチェックボックスでグループのデバイスを選択して) アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>すぐに開始 (デフォルト)</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5 (1 が最も高い優先度) までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278 ページ) を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
セッションログ	完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。大量のデータを格納することができます。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」(96 ページ) を参照してください。

フィールド	説明/アクション
強制的に保存	<p>デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみ適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。</p> <ul style="list-style-type: none"> <li>• このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>• NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>(<b>注意</b>：この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます)。</p>
実行する診断	<p>実行する診断を選択します。[Ctrl]キーを押しながらクリックして、追加の診断を選択（または選択解除）します。診断には次の項目があります。</p> <ul style="list-style-type: none"> <li>• ハードウェア情報</li> <li>• メモリトラブルシューティング</li> <li>• NAがデバイスのブートを検出</li> <li>• NA デバイスファイルシステム</li> <li>• NA 通信モードデータ収集</li> <li>• NA フラッシュ記憶域容量</li> <li>• NA インターフェイス</li> <li>• NA モジュールのステータス</li> <li>• NA OSPF ネイバー</li> <li>• NA ルーティングテーブル</li> <li>• NA トポロジーデータ収集</li> <li>• NA VLAN データ収集</li> <li>• NA ポートスキャン</li> </ul> <p><b>注意</b>：診断の詳細については、「<b>表示メニューオプション</b>」(201 ページ)を参照してください。</p>
推定継続時間	<p>このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。</p>

## フィールド

## 説明/アクション

**デバイス資格情報のオプション**

デバイス資格情報のオプションは、[システム管理設定]の[デバイスアクセス]ページで設定されている[標準デバイスの資格情報を許可]、[タスクごとのデバイスの資格情報を許可]、[ユーザのAAA資格情報を許可]の内1つまたは複数のオプションの構成に従って表示されます。[タスクごとのデバイスの資格情報を許可]を有効にすると、適切なパスワード情報を入力するよう求めるプロンプトが表示されます。また、複数のデバイス資格情報オプションを有効にすると、タスクを実行するときにオプションを選択するよう求めるプロンプトが表示されます。デバイス資格情報オプションを1つだけ有効にした場合は自動的にオプションが使用され、プロンプトは表示されません（デバイス資格情報の有効化の詳細については、「[\[デバイスアクセス\]ページのフィールド](#)」（45ページ）を参照してください）。

デバイス資格情報 [システム管理設定]の[サーバ]ページで有効にされるデバイス資格情報オプションに応じて、次のオプションを1つ以上選択できます。

- 標準デバイス固有の資格情報とネットワーク全体のパスワードルールの使用（デフォルト）。
- 特定のタスク単位のパスワードを使用。[ユーザ名]、[パスワード]、[パスワードの確認]、[イネーブルパスワードの確認]、[SNMP読み取り専用コミュニティ文字列]、および[SNMP読み取り/書き込みコミュニティ文字列]への入力を求めるプロンプトが表示されます。
- タスク所有者のAAA資格情報の使用。タスク所有者には、定義された有効なAAA資格情報が必要です。（**注意**：標準パスワードルールとデバイス固有パスワードを使用します。ただし、タスク所有者のAAAユーザ名とパスワードが適用されます。）

**タスク前/タスク後スナップショットオプション**

スナップショットのオプションは、[システム管理設定]の下の[構成管理]ページでユーザによる無効化がシステムで有効に構成されている場合にのみ表示されます（詳細については、「[\[構成管理\]ページのフィールド](#)」（36ページ）を参照してください）。

タスク前スナップショット 次のオプションのいずれかを選択します。

- なし（デフォルト）
- タスクの一部として

タスク後スナップショット 次のオプションのいずれかを選択します。

- なし
- タスクの一部として（デフォルト）
- 個別のタスクとしてスケジュール

**承認オプション**

承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。

承認要求 タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。

承認の無効化 タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。

ドラフトとして保存 オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。



フィールド	説明/アクション
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96ページ)</b>を参照してください。</p>

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、**「[タスク情報]ページのフィールド」(406ページ)**を参照してください。

タスクが今後に開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、「[\[自分のタスク\]ページのフィールド](#)」(397 ページ) を参照してください。

## [スナップショットの取得]タスクページのフィールド

スナップショットの取得タスクでは、スナップショットのスケジューリングができます。スナップショットでは、格納されている構成がデバイスのランニング構成と一致するかどうかを確認します。一致しない場合は、そのタスクで、デバイス構成と関連データの新規コピーをNAデータベースに格納します。

[スナップショットにチェックポイントを作成]オプションを選択した場合は、NAが差異を検出しないときでもNAデータベースが更新されます。このため、スナップショットは、ホームページ、サマリレポート、構成変更検索結果などで構成変更として引き続き表示されます。

フィールド	説明/アクション
タスク名	[スナップショットの取得]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセレクトアの使用方法的詳細については、「<a href="#">デバイスセレクトア</a>」(142ページ)を参照してください。</li> <li>CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b>（[デバイスリスト]ページのチェックボックスでグループのデバイスを選択して）アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>すぐに開始（デフォルト）</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
セッションログ	[完全なデバイスセッションログを格納]ボックスをオンにしてデバッグログを格納します。セッションのログ記録を有効にした状態で、デバイスと対話するすべてのタスクが実行できます。タスク実行中のデバイスとの対話に関する詳細なログが記録されます。セッションログは、デバイス固有の問題をデバッグするための第一段階として表示してください。セッションログでは、CLI、SNMP およびタスクで実行されるすべての転送プロトコルアクションの詳細がわかります。（ <b>注意：</b> 大量のデータが格納されることがあります。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」(96ページ)を参照してください）。

フィールド	説明/アクション
強制的に保存	<p>デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみにも適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。</p> <ul style="list-style-type: none"> <li>• このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>• NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>(注意: この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます)。</p>
オプション	<p>次のオプションのいずれかまたは両方を選択します。</p> <ul style="list-style-type: none"> <li>• スナップショットにチェックポイントを作成: 格納されている構成がランニング構成と異なっているかどうかを確認しないで、NA データベースにランニング構成をコピーします。このオプションは、構成ファイルが変更されているかどうかに関係なく構成ファイルを格納します。ただし、変更がない場合、スナップショットは、ホームページ、サマリレポート、構成変更検索結果などで構成変更として引き続き表示されます。このため、構成変更数には、チェックポイント付きの構成が含まれることになり、構成変更数は正確なものでない可能性があります。</li> <li>• バイナリ構成を取得: バイナリ構成がもしあれば、テキスト情報と同様にNA データベースにコピーします。</li> </ul>
推定継続時間	<p>このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。</p>
<b>デバイス資格情報のオプション</b>	
<p>デバイス資格情報のオプションは、[システム管理設定]の[デバイスアクセス]ページで設定されている[標準デバイスの資格情報を許可]、[タスクごとのデバイスの資格情報を許可]、[ユーザのAAA資格情報を許可]の内1つまたは複数のオプションの構成に従って表示されます。[タスクごとのデバイスの資格情報を許可]を有効にすると、適切なパスワード情報を入力するよう求めるプロンプトが表示されます。また、複数のデバイス資格情報オプションを有効にすると、タスクを実行するときにオプションを選択するよう求めるプロンプトが表示されます。デバイス資格情報オプションを1つだけ有効にした場合は自動的にオプションが使用され、プロンプトは表示されません（デバイス資格情報の有効化の詳細については、「<a href="#">[デバイスアクセス]ページのフィールド</a>」(45ページ)を参照してください)。</p>	
デバイス資格情報	<p>[システム管理設定]の[サーバ]ページで有効にされるデバイス資格情報オプションに応じて、次のオプションを1つ以上選択できます。</p> <ul style="list-style-type: none"> <li>• 標準デバイス固有の資格情報とネットワーク全体のパスワードルールの使用（デフォルト）。</li> <li>• 特定のタスク単位のパスワードを使用。[ユーザ名]、[パスワード]、[パスワードの確認]、[イネーブルパスワードの確認]、[SNMP読み取り専用コミュニティ文字列]、および[SNMP読み取り/書き込みコミュニティ文字列]への入力を求めるプロンプトが表示されます。</li> <li>• タスク所有者のAAA資格情報の使用。タスク所有者には、定義された有効なAAA資格情報が必要です。(注意: 標準パスワードルールとデバイス固有パスワードを使用します。ただし、タスク所有者のAAAユーザ名とパスワードが適用されます。)</li> </ul>

フィールド	説明/アクション
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>

フィールド	説明/アクション
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクリグ</b>	
タスクリグ	利用可能である場合、特定タスクリグのタスクリグを1回実行するように予定できます。[このタスクリグで生成されたタスクリグ出力を格納]チェックボックスをオンにして、[Shift] キーを押しながら1つまたは複数のタスクリグを選択します。選択したタスクリグが強調表示されます。タスクリグの実行時にタスクリグ記録を行うように設定したときに、タスクリグを開始できない場合、タスクリグはその後の処理を行うことなく、ただちに異常終了します。タスクリグ記録の詳細については、「 <a href="#">タスクリグ記録</a> 」(96 ページ) を参照してください。

入力が完了したら、必ず[保存]をクリックします。タスクリグを直ちに実行するようにスケジューリングされている場合は、[タスクリグ情報]ページが開きます。[タスクリグ情報]ページには、タスクリグの開始日、継続期間、ステータスなど、タスクリグの詳細が表示されます。詳細については、「[\[タスクリグ情報\]ページのフィールド](#)」(406 ページ) を参照してください。

タスクリグが今後を開始するようにスケジューリングされている場合は、[自分のタスクリグ]ページで新規タスクリグが強調表示されます。詳細については、「[\[自分のタスクリグ\]ページのフィールド](#)」(397 ページ) を参照してください。

## [スタートアップとランニングの同期]タスクページのフィールド

[スタートアップとランニングの同期]タスクでは、デバイスのスタートアップとランニング構成の同期ができます。NAは、スタートアップ構成に現在のランニング構成を上書きします。このタスクにより、デバイスをリブートすると現在の構成が実行を続けます。

フィールド	説明/アクション
タスク名	[スタートアップとランニングの同期]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセレクトタの使用方法的詳細については、「<a href="#">デバイスセレクトタ</a>」(142ページ)を参照してください。</li> <li>• CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b>（[デバイスリスト]ページのチェックボックスでグループのデバイスを選択して）アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
セッションログ	[完全なデバイスセッションログを格納]ボックスをオンにしてデバッグログを格納します。このオプションは失敗したスナップショットをデバッグする場合に役立ちますが、格納されるデータのサイズが大きくなる可能性があります。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」(96ページ)を参照してください。

フィールド	説明/アクション
強制的に保存	<p>デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみに適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。</p> <ul style="list-style-type: none"> <li>このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>(注意: この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます)。</p>
オプション	構成が既に同期しているためタスクをスキップしたい場合は、[同期している場合は無視]ボックスをオンにします。
推定継続時間	このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。

#### デバイス資格情報のオプション

デバイス資格情報のオプションは、[システム管理設定]の[デバイスアクセス]ページで設定されている[標準デバイスの資格情報を許可]、[タスクごとのデバイスの資格情報を許可]、[ユーザのAAA資格情報を許可]の内1つまたは複数のオプションの構成に従って表示されます。[タスクごとのデバイスの資格情報を許可]を有効にすると、適切なパスワード情報を入力するよう求めるプロンプトが表示されます。また、複数のデバイス資格情報オプションを有効にすると、タスクを実行するときにオプションを選択するよう求めるプロンプトが表示されます。デバイス資格情報オプションを1つだけ有効にした場合は自動的にオプションが使用され、プロンプトは表示されません（デバイス資格情報の有効化の詳細については、[「\[デバイスアクセス\]ページのフィールド」\(45ページ\)](#)を参照してください）。

デバイス資格情報	<p>[システム管理設定]の[サーバ]ページで有効にされるデバイス資格情報オプションに応じて、次のオプションを1つ以上選択できます。</p> <ul style="list-style-type: none"> <li>標準デバイス固有の資格情報とネットワーク全体のパスワードルールの使用（デフォルト）。</li> <li>特定のタスク単位のパスワードを使用。[ユーザ名]、[パスワード]、[パスワードの確認]、[イネーブルパスワードの確認]、[SNMP読み取り専用コミュニティ文字列]、および[SNMP読み取り/書き込みコミュニティ文字列]への入力を求めるプロンプトが表示されます。</li> <li>タスク所有者のAAA資格情報の使用。タスク所有者には、定義された有効なAAA資格情報が必要です。(注意: 標準パスワードルールとデバイス固有パスワードを使用します。ただし、タスク所有者のAAAユーザ名とパスワードが適用されます。)</li> </ul>
----------	--

#### タスク前/タスク後スナップショットオプション

スナップショットのオプションは、[システム管理設定]の下[構成管理]ページでユーザによる無効化がシステムで有効に構成されている場合にのみ表示されます（詳細については、[「\[構成管理\]ページのフィールド」\(36ページ\)](#)を参照してください）。

タスク後スナップショット	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>なし</li> <li>タスクの一部として（デフォルト）</li> <li>個別のタスクとしてスケジュール</li> </ul>
--------------	--



フィールド	説明/アクション
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>

フィールド	説明/アクション
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクリグ</b>	
タスクリグ	利用可能である場合、特定タスクリグのタスクリグを1回実行するように予定できます。[このタスクリグで生成されたタスクリグ出力を格納]チェックボックスをオンにして、[Shift] キーを押しながら1つまたは複数のタスクリグを選択します。選択したタスクリグが強調表示されます。タスクリグの実行時にタスクリグ記録を行うように設定したときに、タスクリグを開始できない場合、タスクリグはその後の処理を行うことなく、ただちに異常終了します。タスクリグ記録の詳細については、「 <a href="#">タスクリグ記録</a> 」(96 ページ) を参照してください。

入力が完了したら、必ず[保存]をクリックします。タスクリグを直ちに実行するようにスケジューリングされている場合は、[タスクリグ情報]ページが開きます。[タスクリグ情報]ページには、タスクリグの開始日、継続期間、ステータスなど、タスクリグの詳細が表示されます。詳細については、「[\[タスクリグ情報\]ページのフィールド](#)」(406 ページ) を参照してください。

タスクリグが今後を開始するようにスケジューリングされている場合は、[自分のタスクリグ]ページで新規タスクリグが強調表示されます。詳細については、「[\[自分のタスクリグ\]ページのフィールド](#)」(397 ページ) を参照してください。

## [デバイスソフトウェアの更新]タスクページのフィールド

デバイスソフトウェアの更新タスクでは、1つ以上のデバイスに対するソフトウェアの配布をスケジューリングできます。詳細については、「[ソフトウェアイメージ](#)」(444ページ)を参照してください。次のことに注意が必要です。

- 合計メモリとは、デバイスの物理メモリの合計です。
- 空きメモリとは、最後のメモリ診断の時点で、アップロードに使用できる空きメモリのことです。
- ネットメモリとは、デバイスソフトウェアの更新タスク実行後の空きメモリの推定値です。デバイスに追加または削除されるようにマークされたファイルも考慮されています（ただし、タスク処理前後の圧縮は考慮されていません）。

フィールド	説明/アクション
タスク名	[デバイスソフトウェアの更新]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセレクトタの使用方法的詳細については、「<a href="#">デバイスセレクトタ</a>」(142ページ)を参照してください。</li> <li>• パーティションにあるデバイスに限定：パーティションを選択します。指定したパーティションのみのデバイスで、ソフトウェアのイメージがアップデートされます。デバイス設定の限定条件の詳細については、[詳細...]をクリックしてください。</li> <li>• CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b>（[デバイスリスト]ページのチェックボックスでグループのデバイスを選択して）アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。

フィールド	説明/アクション
<b>タスクオプション</b>	
セッションログ	[完全なデバイスセッションログを格納]ボックスをオンにしてデバッグログを格納します。このオプションは失敗したスナップショットをデバッグする場合に役立ちますが、格納されるデータのサイズが大きくなる可能性があります。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」(96 ページ) を参照してください。
強制的に保存	<p>デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみにも適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。</p> <ul style="list-style-type: none"> <li>このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>(<b>注意</b>：この設定は NA 9.20 で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます)。</p>
配布表	単一デバイスにソフトウェアを配布する場合、[配布表]が開きます。詳細については、「 <a href="#">配布表</a> 」(327 ページ) を参照してください。
イメージセット	配布するソフトウェアイメージの名前を選択します。
スロット	ソフトウェアを配布するスロットを選択します。NA は、現在 NA データベースにあるすべてのスロットを一覧表示します。
メモリ準備	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>なし：ソフトウェア更新前にデバイスメモリを準備しません。デバイスが新規ソフトウェアを受信するために必要なメモリを手動で確保してください。確保しない場合、タスクは失敗します。</li> <li>選択スロットのデバイスメモリを圧縮：Cisco IOS squeeze commandなどのメモリ圧縮コマンドをデバイスがサポートしている場合は、ソフトウェア配布前にNAがそのコマンドを実行してメモリを圧縮します。デバイスから削除されるファイルはありません。この場合も、更新に必要なメモリを確保してください。</li> <li>選択スロットからファイルを削除し、メモリを圧縮：デバイスが圧縮コマンドをサポートしている場合は、ソフトウェア配布前に、NAがフラッシュ上のすべてのブートイメージ（すべてに .bin、.tar、および .W ファイル）を削除してメモリを圧縮します。(注意：ソフトウェアの配布タスクに失敗し、それに引き続いてデバイスの電源異常が起きたりリポートすると、デバイスをブートできなくなる場合があります。)</li> </ul>
確認	オンにすると、[確認]オプションはデバイス上で利用できるコマンドを使用して、イメージを確認します。デバイス上でのMD5チェックサムと、データベースに格納されているMD5チェックサムとが比較されます。デバイスがこのオプションをサポートしない場合、ドライバはイメージに確認コマンドを実行します。
リポート	ソフトウェア配布後にデバイスをリポートするスクリプトを実行するには、[ソフトウェアの配布後にデバイスをリポート]ボックスをオンにします。リポートしてから構成のスナップショットを取得するまでの間に休止する秒数を、[リポート後に休止]ボックスに入力します。デフォルト値は60秒です。
推定継続時間	このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。

フィールド	説明/アクション
<b>デバイス資格情報のオプション</b>	
<p>デバイス資格情報のオプションは、[システム管理設定]の[デバイス]ページで設定されている[標準デバイスの資格情報を許可]、[タスクごとのデバイスの資格情報を許可]、[ユーザのAAA資格情報を許可]の内1つまたは複数のオプションの構成に従って表示されます。[タスクごとのデバイスの資格情報を許可]を有効にすると、適切なパスワード情報を入力するよう求めるプロンプトが表示されます。また、複数のデバイス資格情報オプションを有効にすると、タスクを実行するときにオプションを選択するよう求めるプロンプトが表示されます。デバイス資格情報オプションを1つだけ有効にした場合は自動的にオプションが使用され、プロンプトは表示されません（デバイス資格情報の有効化の詳細については、「<a href="#">[デバイスアクセス]ページのフィールド</a>」（45ページ）を参照してください）。</p>	
デバイス資格情報	<p>[システム管理設定]の[サーバ]ページで有効にされるデバイス資格情報オプションに応じて、次のオプションを1つ以上選択できます。</p> <ul style="list-style-type: none"> <li>• 標準デバイス固有の資格情報とネットワーク全体のパスワードルールの使用（デフォルト）。</li> <li>• 特定のタスク単位のパスワードを使用。[ユーザ名]、[パスワード]、[パスワードの確認]、[イネーブルパスワードの確認]、[SNMP読み取り専用コミュニティ文字列]、および[SNMP読み取り/書き込みコミュニティ文字列]への入力を求めるプロンプトが表示されます。</li> <li>• タスク所有者のAAA資格情報の使用。タスク所有者には、定義された有効なAAA資格情報が必要です。（<b>注意</b>：標準パスワードルールとデバイス固有パスワードを使用します。ただし、タスク所有者のAAAユーザ名とパスワードが適用されます。）</li> </ul>
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	<p>タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。</p>
承認の無効化	<p>タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。</p>
ドラフトとして保存	<p>オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。</p>
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	<p>次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。</p>

フィールド	説明/アクション
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	<p>メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。</p>
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96ページ)</b>を参照してください。</p>

## 配布表

配布表は、単独デバイスにソフトウェアを配布するための詳細オプションを備えています。データは最後のファイルシステム診断に基づきます。

フィールド	説明/アクション
ファイルシステム診断を実行します	[タスクの新規作成] - [診断の実行] ページが開きます。このページでは、デバイス上でのファイルシステム診断の実行を予定できます（詳細については、「 <a href="#">[診断の実行] タスクページのフィールド</a> 」（310 ページ）を参照してください）。
タスクの前処理	Cisco IOS squeeze commandなどのメモリ圧縮コマンドをデバイスがサポートしている場合は、ソフトウェア配布前にNAがそのコマンドを実行してメモリを圧縮します。デバイスから削除されるファイルはありません。この場合も、更新に必要なメモリを確保してください。
[ファイル] 領域	<p>[ファイル] 領域には次のセクションがあります。</p> <ul style="list-style-type: none"> <li>• <b>[デバイス上]</b>：デバイス上のファイルシステムのコンテンツが表示されます。NAにより、ファイルシステムごとの合計サイズ、空き領域、デバイスソフトウェアの更新後の正味空き領域が表示されます。正味空き領域が負の数値である場合、計画している更新に十分な領域がデバイスのファイルシステムにありません。</li> <li>• <b>[ソフトウェアイメージリポジトリ]</b>：NAで現在のデバイスに定義されているものの、現在はデバイス上にないソフトウェアイメージセットが表示されます。</li> </ul> <p>NAにより、ファイルごとのファイルサイズと、該当する場合は準拠に関する警告が表示されます（<b>注意</b>：準拠に関する警告はデフォルトでは表示されません。詳細については、「<a href="#">[ユーザインターフェイス] ページのフィールド</a>」（61 ページ）を参照してください）。ファイルの操作は次のように行います。</p> <ul style="list-style-type: none"> <li>• ファイルをデバイスに移動するには、ソフトウェアイメージリポジトリから適切なファイルシステムにドラッグします。移動を取り消すには、ファイルをソフトウェアイメージリポジトリにドラッグして戻します。</li> <li>• ファイルをデバイスから削除するには、ファイル名を右クリックし、<b>[削除マーク]</b>をクリックします。</li> <li>• ブートイメージを設定するには、デバイスにすでにあるファイル、またはその対象となるファイルを右クリックし、<b>[ブートイメージとしてマーク]</b>をクリックします（<b>注意</b>：ブートイメージにできるファイルは1つのみです。ブートイメージとして2番目のファイルを設定すると、最初のファイルの選択が解除されます。）</li> <li>• OSイメージを設定するには、デバイスにすでにあるファイル、またはその対象となるファイルを右クリックし、<b>[OSイメージとしてマーク]</b>をクリックします（<b>注意</b>：OSイメージにできるファイルは1つのみです。OSイメージとして2番目のファイルを設定すると、最初のファイルの選択が解除されます。）</li> <li>• ファイルの削除、ブートイメージ、OSイメージの選択を解除するには、ファイル名を右クリックし、<b>[マークを削除]</b>をクリックします。</li> </ul>
タスクの後処理	Cisco IOS squeeze commandなどのメモリ圧縮コマンドをデバイスがサポートしている場合は、ソフトウェア配布後にNAがそのコマンドを実行してメモリを圧縮します。デバイスから削除されるファイルはありません。この場合も、更新に必要なメモリを確保してください。
サマリ	行う変更を表示します。
確認	オンにすると、[確認] オプションはデバイス上で利用できるコマンドを使用して、イメージを確認します。デバイス上でのMD5チェックサムと、データベースに格納されているMD5チェックサムとが比較されます。デバイスがこのオプションをサポートしない場合、ドライバはイメージに確認コマンドを実行します。

フィールド	説明/アクション
リブート	ソフトウェア配布後にデバイスをリブートするスクリプトを実行するには、[ソフトウェアの配布後にデバイスをリブート]ボックスをオンにします。リブートしてから構成のスナップショットを取得するまでの間に休止する秒数を、[リブート後に休止]ボックスに入力します。デフォルト値は60秒です。

**注意：** 複数のイメージがインストールされているデバイス上で、どのイメージをブートイメージ、OSイメージのいずれかまたは両方にするかを指定する機能が備わっています。この機能は、Cisco IOSを実行するデバイス上でのみ利用できます。

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、「[\[タスク情報\]ページのフィールド](#)」(406ページ)を参照してください。

タスクが今後を開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、「[\[自分のタスク\]ページのフィールド](#)」(397ページ)を参照してください。

**注意：** デバイスで使用可能なディスク空き容量に、配布するために選択したイメージが収まらない場合は、エラーメッセージが表示されます。タスクに戻って変更するか、ソフトウェアを配布できます。ディスク容量の計算が誤っている可能性があります。



## [デバイスのインポート]タスクページのフィールド

デバイスをインポートタスクでは、CSV形式（カンマ区切り値）のファイルからデータを読み取ります。CSVファイルの各行に1つのデータベースオブジェクトが記述されています。デバイスデータについては、NAはオブジェクトを一意に識別するために、primaryIPAddress および hostName 列の値とオプションの siteName 列の値を組み合わせで使用します。デバイスグループデータについては、deviceGroupName 列の値を使用してオブジェクトを一意に識別します。デバイス固有パスワードについては、deviceIPAddress 列の値を使用してオブジェクトを一意に識別します。

最初にネットワーク全体のデバイスパスワードルールを作成してから、デバイスをインポートすることをお勧めします。あるファイルからデバイス固有のデータ群をインポートし、他のファイルからデバイスパスワードデータをインポートすることもできます。

CSVファイルの行ごとに、次のようにデータベースが更新されます。

- 一意的識別子が存在しない場合、ファイルで指定された値を使って新しいオブジェクトが作成されます。
  - 空のセルはNULLと同等です。
  - CSVファイルに含まれないデータベース列には、デフォルト値が使用されます。
- 一意的識別子が存在する場合、次の処理が行われます。
  - [既存デバイスを上書き]フラグが設定されている場合、CSVファイルに指定された値を使ってデータベースオブジェクトが更新されます（空のセルはNULLと同等です）。

**注意：** 既存のデバイスグループは変更されません。

- [既存デバイスを上書き]フラグが設定されていない場合、その行は無視され、データベースオブジェクトは変更されません。

1つのCSVファイルから、新規のデータベースオブジェクトや既存のデータベースオブジェクトの変更をインポートできます。CSVファイルの列を完全に入力してください。

**ヒント：** CSVファイルには、値を設定する列のみ含めます。データセットの一部のオブジェクトで他のオブジェクトには適用しない列が必要な場合、複数のCSVファイルおよび複数のインポートタスクを作成します。

## デバイスデータをインポートするには：

1. 「**デバイスデータのインポートのためのCSVファイルの作成**」(126 ページ) に従って、CSV インポートファイルを作成します。  
  
**注意：** [管理] > [システム管理設定] > [サーバ] ページで [既存デバイスを上書き] オプションが [はい] に設定されている場合、CSV ファイルのデータによって NA のデータが上書きされます。特定のフィールドが上書きされないようにするには、CSV ファイルからそれらのフィールドを削除します。
2. [タスク/テンプレートの新規作成 - デバイスをインポート] ページに移動します。
3. 任意の構成を行います (330 ページの表「**[デバイスデータのインポート] タスクページのフィールド**」を参照してください)。
4. [保存] をクリックして変更を適用します。

### [デバイスデータのインポート] タスクページのフィールド

フィールド	説明/アクション
デバイスインポート管理設定	[システム管理設定] ページが開きます ([サーバ] タブ)。このページで、NA のタスク制限の設定、ワークフローの有効化、Syslog の構成などができます。
タスク名	このタスクの名前を設定します。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート] ページに表示されます。タスクテンプレートの詳細については、「<b>タスクテンプレート</b>」(280 ページ) を参照してください。</li> </ul>
サイト	パーティションを選択するドロップダウンメニューが表示されます。このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「 <b>デバイスとユーザのセグメント化</b> 」(148 ページ) を参照してください。  <b>注意：</b> この値を設定できるのはデバイスまたはデバイスグループ作成時のみです。CSV ファイルの siteName 列の値は、ここで選択したサイトよりも優先されます。
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始 (デフォルト)</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5 (1 が最も高い優先度) までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <b>タスクの予定</b> 」(278 ページ) を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
ファイルのインポート	インポートデータを含む CSV ファイルの名前を入力します。 <ul style="list-style-type: none"> <li>• ファイルがローカルシステムにある場合は、[参照] ボタンを使用してファイルを検索できます。</li> <li>• ファイルが NA サーバにある場合、NA サーバのファイルのフルパスを含めてください。</li> </ul>

## [デバイスデータのインポート]タスクページのフィールド (続き)

フィールド	説明/アクション
データ型	<p>次のオプションから1つ選択して、インポートするデータを入力します。</p> <ul style="list-style-type: none"> <li>• デバイス: デバイスCSVテンプレートには、NAにネットワークデバイスデータをインポートするために使用可能なフィールドがすべて含まれています。</li> <li>• デバイスグループ: デバイスグループCSVテンプレートには、NAにデバイスグループデータをインポートするために使用可能なフィールドがすべて含まれています。</li> <li>• パスワード: デバイスパスワードルールを使用しない場合のみ、デバイスパスワードCSVテンプレートが必要になります。</li> </ul> <p>新規CSVファイルの作成にテンプレートを使用する場合は、リンクをクリックしてテンプレートファイルを開きます。ローカルシステム上の場所にファイルを保存し、デバイスデータに合わせてコンテンツの変更や未使用の列の削除を行います。詳細については、「<a href="#">デバイスデータのインポートのためのCSVファイルの作成</a>」(126 ページ)を参照してください。</p>
Syslogの設定	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• NA syslog サーバでログを取得するようデバイスを設定する</li> <li>• デバイスはsyslog リレーにログ出力し、正しいログレベルに設定する</li> <li>• syslogを構成しない</li> </ul> <p>インポートするCSVファイルに関連するデバイスのデバイスドライバを検出するには、[新しくインポートされたデバイスでドライバの検出タスクを実行]ボックスをオンにします。このオプションでは、有効なデバイスパスワードとコミュニティ文字列が必要です。このため、パスワードとデバイスパスワードルールを既にユーザのネットワーク用に設定してデバッグしている場合、またはデバイスパスワード情報を含む2番目のファイルをインポートする場合のみ、そのオプションを使用します。</p> <p>過去45日間にアクセスされていないまたはインポートが成功していないデバイスを非アクティブ化する場合、[非アクティブのデバイス、または存在しないデバイスを非アクティブ化する]チェックボックスをオンにします。</p>
コマンドの前処理	<p>NA内のプロセス全体を自動化してスケジューリングするには、データをインポートする前に、実行するスクリプトファイルの名前（およびパス）を入力します。このフィールドには、サーバのコマンドコンソールまたはシェルコンソールで実行される、実行可能なフルコマンドが必要です。たとえば、フィルタがWindows用のPERLスクリプトの場合、「perl」をperl c:/filter.plのように指定する必要があります。</p>
ログファイル名	<p>NAがインポートタスクの情報を書き込むファイル名を入力します。ログファイルは、インポートで起きた問題をデバッグするときに役立ちます。既存のログファイルにこのデータを付加する場合は、[ログファイルに付加]をオンにします。オンにしない場合、NAはログファイル内の既存のデータを上書きしてしまいます。</p>
デバイスのインポート元	<p>インポートファイルにつける名前を入力します。これは、データを繰り返しインポートした場合、データソースや日付の区別が必要ときに役立ちます。</p>
推定継続時間	<p>このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。</p>

## [デバイスデータのインポート]タスクページのフィールド (続き)

フィールド	説明/アクション
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。 <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。 <b>ヒント：</b> 電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。

## [デバイスデータのインポート]タスクページのフィールド (続き)

フィールド	説明/アクション
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、 <b>「ログ記録」(96ページ)</b> を参照してください。

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、**「[タスク情報]ページのフィールド」(406ページ)**を参照してください。

タスクが今後を開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、**「[自分のタスク]ページのフィールド」(397ページ)**を参照してください。

## [ユーザのインポート]タスクページのフィールド

ユーザのインポートタスクでは、CSV形式（カンマ区切り値）のファイルからデータを読み取ります。CSVファイルの各行に1つのデータベースオブジェクトが記述されています。ユーザアカウントデータについては、userName列の値を使用してオブジェクトを一意に識別します。ユーザグループデータについては、userGroupName列の値を使用してオブジェクトを一意に識別します。

CSVファイルの行ごとに、次のようにデータベースが更新されます。

- 一意の識別子が存在しない場合、ファイルで指定された値を使って新しいオブジェクトが作成されます。
  - 空のセルはNULLと同等です。
  - CSVファイルに含まれないデータベース列には、デフォルト値が使用されます。
- 一意の識別子が存在する場合、次の処理が行われます。
  - [既存のユーザまたはユーザグループの上書き]フラグが設定されている場合、CSVファイルに指定された値を使ってデータベースオブジェクトが更新されます。（空のセルはNULLと同等です）。
  - [既存のユーザまたはユーザグループの上書き]フラグが設定されていない場合、その行は無視され、データベースオブジェクトは変更されません。

1つのCSVファイルから、新規のデータベースオブジェクトや既存のデータベースオブジェクトの変更をインポートできます。CSVファイルの列を完全に入力してください。

**ヒント：**CSVファイルには、値を設定する列のみ含めます。データセットの一部のオブジェクトで他のオブジェクトには適用しない列が必要な場合、複数のCSVファイルおよび複数のインポートタスクを作成します。

**ユーザデータをインポートするには：**

1. 「**ユーザデータのインポートのためのCSVファイルの作成**」(337 ページ) に従って、CSVインポートファイルを作成します。

**注意：** [管理] > [システム管理設定] > [サーバ] ページで [既存のユーザまたはユーザグループの上書き] フラグが [はい] に設定されている場合、CSVファイルのデータによってNAデータベースのデータが上書きされます。特定のフィールドが上書きされないようにするには、CSVテーブルからそれらの列を削除します。

2. [タスク/テンプレートの新規作成 - ユーザのインポート] ページに移動します。
3. 任意の構成を行います（335 ページの表「**ユーザデータのインポート**」タスクページのフィールド」を参照してください）。
4. [保存] をクリックして変更を適用します。

## [ユーザデータのインポート]タスクページのフィールド

フィールド	説明/アクション
ユーザインポート管理設定	[システム管理設定]ページが開きます（[サーバ]タブ）。このページで、NAのタスク制限の設定、ワークフローの有効化、Syslogの構成などができます。
タスク名	このタスクの名前を設定します。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>すぐに開始（デフォルト）</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
ファイルのインポート	インポートデータを含むCSVファイルの名前を入力します。 <ul style="list-style-type: none"> <li>ファイルがローカルシステムにある場合は、[参照]ボタンを使用してファイルを検索できます。</li> <li>ファイルがNAサーバにある場合、NAサーバのファイルのフルパスを含めてください。</li> </ul>
データ型	次のオプションから1つ選択して、インポートするデータを入力します。 <ul style="list-style-type: none"> <li>ユーザ：ユーザCSVテンプレートには、NAにユーザアカウントデータをインポートするために使用可能なフィールドがすべて含まれています。</li> <li>ユーザグループ：ユーザグループCSVテンプレートには、NAにユーザグループデータをインポートするために使用可能なフィールドがすべて含まれています。</li> </ul> <p>新規CSVファイルの作成にテンプレートを使用する場合は、リンクをクリックしてテンプレートファイルを開きます。ローカルシステム上の場所にファイルを保存し、ユーザデータに合わせてコンテンツの変更や未使用の列の削除を行います。詳細については、「<a href="#">ユーザデータのインポートのためのCSVファイルの作成</a>」(337ページ)を参照してください。</p>
コマンドの前処理	NA内のプロセス全体を自動化してスケジューリングするには、データをインポートする前に、実行するスクリプトファイルの名前（およびパス）を入力します。このフィールドには、サーバのコマンドコンソールまたはシェルコンソールで実行される、実行可能なフルコマンドが必要です。たとえば、フィルタがWindows用のPERLスクリプトの場合、「perl」をperl c:/filter.plのように指定する必要があります。
ログファイル名	NAがインポートタスクの情報を書き込むファイル名を入力します。ログファイルは、インポートで起きた問題をデバッグするときに役立ちます。既存のログファイルにこのデータを付加する場合は、[ログファイルに付加]をオンにします。オンにしない場合、NAはログファイル内の既存のデータを上書きしてしまいます。

## [ユーザデータのインポート]タスクページのフィールド (続き)

フィールド	説明/アクション
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。 <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。 <b>ヒント：</b> 電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。



## [ユーザデータのインポート]タスクページのフィールド (続き)

フィールド	説明/アクション
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
タスクログ	
タスクログ	利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、 <a href="#">「ログ記録」(96ページ)</a> を参照してください。

## ユーザデータのインポートのためのCSVファイルの作成

ユーザアカウントまたはユーザグループの情報をCSVファイルからNAにインポートするには、デバイスデータのインポートタスクを使用します。CSVファイルの1行目にインポート対象データのNAデータベースの列名があります。その他の行は、それぞれユーザアカウントまたはユーザグループを表しています。

NAにはCSVファイル用のテンプレートがあります。次の点に注意してください。

- 空白の列には列を入力しないでください。既存のデバイスがある場合、空白の値が既存のデータを上書きします。
- 列名はデータベースの列名と一致している必要があります。NAで設定されているデータベースの列名を変更しないでください。
- データフィールドはカンマで区切られているため、フィールドには空白は使用できますが、カンマ(,)は使用できません。フィールド内の値を区切るには、コロン(:)を使用します。
- 列の順序は重要ではありません。

## インポート用CSVファイルを作成するには：

1. [タスク/テンプレートの新規作成 - ユーザのインポート]ページに移動します。
2. [タスクオプション]、[データ型]で、適切なCSVテンプレートのリンクをクリックします。
3. 編集ツールで、次の操作を実行します。
  - － データテーブルに情報を追加します。
  - － 既存データを上書きしないように、未使用の列を削除します。
  - － CSVファイルの列の詳細については、関連するセクションを参照してください。
    - [「ユーザアカウントデータのインポートファイル」\(338ページ\)](#)
    - [「ユーザグループのインポートファイル」\(339ページ\)](#)

**注意：** CSVファイルに英語以外の文字が含まれている場合、Microsoft Office Excelではなくテキストエディタでファイルを編集します。CSVファイルの保存にはUTF-8エンコーディングを使用します。

4. ファイルタイプをCSVとしてローカルシステムに保存します。

## ユーザアカウントデータのインポートファイル

`user.csv`テンプレートファイルには、ユーザアカウントデータ用のNAデータベース列名が入っています。NAはインポートでデータベース内のユーザアカウントを一意に識別するために、`userName`列の値を使用します。

### ユーザアカウントデータのインポートファイルのフィールド

列名	説明/アクション
<code>userName</code>	オペレータまたは管理者などがNAにログインするときに使用するユーザ名です。 この列は、ユーザアカウントデータのインポートファイルそれぞれに必要です。 <b>注意</b> ：ユーザ名には、英数字、ピリオド (.)、アンダースコア (_)、ハイフン (-)、およびバックスラッシュ (\) のみ使用できます。 <b>注意</b> ：この値を設定できるのはユーザ作成時のみです。
<code>siteName</code>	ユーザアカウントが属するサイトの名前（パーティション）です。ユーザアカウントは、当該パーティションへの表示権限を持つ他のユーザにしか見えません。 <b>注意</b> ：この値を設定できるのはユーザ作成時のみです。
<code>userGroupName</code>	ユーザアカウントを含むユーザグループのコロン区切りのリストです。
<code>firstName</code>	ユーザの名。
<code>lastName</code>	ユーザの姓。
<code>userPassword</code>	ユーザアカウントのパスワード。 新規ユーザアカウントを作成する場合、この列を含める必要があります。
<code>emailAddress</code>	ユーザの電子メールアドレス。
<code>passwordOption</code>	ユーザアカウントのパスワードオプションのコロン区切りのリストです。次の数値のいずれかを1つ以上指定します。  <ul style="list-style-type: none"> <li>• 1：ユーザは次回ログオン時にパスワードを変更する必要あり</li> <li>• 2：ユーザによるパスワードの変更を禁止</li> <li>• 4：パスワードの有効期限なし</li> <li>• 6：ユーザによるパスワードの変更を禁止、パスワードの有効期限なし</li> <li>• 8：アカウントをロックアウト</li> <li>• 9：ユーザは次回ログオン時にパスワードを変更する必要あり、アカウントをロックアウト</li> <li>• 10：ユーザによるパスワードの変更を禁止、アカウントをロックアウト</li> <li>• 12：パスワードの有効期限なし、アカウントをロックアウト</li> <li>• 14：ユーザによるパスワードの変更を禁止、パスワードの有効期限なし、アカウントをロックアウト</li> </ul> <p>パスワードオプションの設定の詳細については、「<a href="#">ユーザパスワードの構成</a>」（250 ページ）を参照してください。</p>
<code>aaaUserName</code>	ユーザのAAA（TACACS+またはRADIUS）ユーザ名。
<code>aaaPassword</code>	AAAユーザ名のAAAパスワード。

## ユーザアカウントデータのインポートファイルのフィールド (続き)

列名	説明/アクション
useAaaLoginForProxy	プロキシ設定。次の数値のいずれかを指定します。 <ul style="list-style-type: none"> <li>• 0：無効（Telnet/SSH プロキシでの認証時にこのユーザアカウントのNA資格情報を使用）</li> <li>• 1：有効（Telnet/SSH プロキシでの認証時にこのユーザアカウントのAAA資格情報を使用）</li> </ul>
status	ユーザアカウントのステータス。次の数値のいずれかを指定します。 <ul style="list-style-type: none"> <li>• 0：有効</li> <li>• 1：無効</li> </ul>
allowFailover	認証フェイルオーバーの設定。次の数値のいずれかを指定します。 <ul style="list-style-type: none"> <li>• 0：無効（外部認証サーバに到達できない場合、ユーザ認証を使用しない）</li> <li>• 1：有効（外部認証サーバに到達できない場合、ローカル認証を使用する）</li> </ul>
userCustom[1-6]	[カスタムデータの設定] ページでその他のユーザフィールドが定義されている場合、それらのフィールドのデータをインポートできます。テンプレートファイルに定義されている列見出しを使用してください。
comments	ユーザアカウントに関する追加情報（最大255文字）。これには、カンマ（,）を含めないでください。

## ユーザグループのインポートファイル

`user_group.csv` テンプレートファイルには、ユーザグループデータ用のNAデータベース列名が入っています。NAはインポートでデータベース内のユーザグループを一意に識別するために、`userGroupName` 列の値を使用します。

**ヒント：** ユーザグループにカスタマイズした権限ロールを適用するには、次のいずれかを実行します。

- [管理] > [ユーザのロールと権限] ページで新規のユーザロールを作成し、CSV ファイルでそのロールを指定します。
- CSV ファイルから権限列を削除します。新規ユーザグループをインポートした後、NA コンソールで新規の各ユーザグループにカスタマイズした権限ロールを構成します。

## ユーザグループデータのインポートファイルのフィールド

列名	説明/アクション
userGroupName	ユーザグループの名前です（最大255文字）。 この列は、ユーザグループデータのインポートファイルそれぞれに必要です。
siteName	ユーザグループが属するサイトの名前（パーティション）です。 <b>注意：</b> この値を設定できるのはユーザグループ作成時のみです。

## ユーザグループデータのインポートファイルのフィールド (続き)

列名	説明/アクション
説明	ユーザグループの説明です (最大255文字)。これには、カンマ (,) を含めないでください。
commandPermission	コマンド権限のタイプ。次の値のいずれかを指定します。 <ul style="list-style-type: none"><li>• NONE</li><li>• ユーザグループに割り当てる既存のコマンド権限ロールのコロン区切りのリスト</li></ul>
scriptPermission	スクリプト権限のタイプ。次の値のいずれかを指定します。 <ul style="list-style-type: none"><li>• ALL</li><li>• NONE</li><li>• ユーザグループに割り当てる既存のスクリプト権限ロールのコロン区切りのリスト</li></ul>
viewPermission	パーティションの表示権限のタイプ。次の値のいずれかを指定します。 <ul style="list-style-type: none"><li>• ALL</li><li>• NONE</li><li>• ユーザグループに割り当てる既存のパーティションの表示権限ロールのコロン区切りのリスト</li></ul>
deviceModificationPermission	デバイスの修正権限のタイプ。次の値のいずれかを指定します。 <ul style="list-style-type: none"><li>• ALL</li><li>• NONE</li><li>• ユーザグループに割り当てる既存のデバイスの変更権限ロールのコロン区切りのリスト</li></ul>

## [ネットワークデバイスの検出]タスクページのフィールド

ネットワークデバイスの検出によって、NAの管理下に置くネットワーク上のデバイスを検索することができます。IPアドレスの範囲をいったん指定すると、NAがネットワークをスキャンしてデバイスを検索します。新しく検出されたデバイスは、適切なデバイスドライバとともに自動的に追加されます。さらに、[システム管理設定 - サーバ]ページの[プライマリIPアドレスの再割り当て]オプションがオンで、デバイスに複数のIPアドレスやインターフェイスがある場合は、NAはデバイスに対して正しいIPアドレスを自動的に割り当てます。その結果、デバイスはシステムに1回のみ登録されます。タスク設定の詳細については、「[\[デバイスアクセス\]ページのフィールド](#)」(45ページ) および「[\[サーバ\]ページのフィールド](#)」(52ページ)を参照してください。

タスクページで[ドライバ検出]を選択した場合、NAがシステムにデバイスを追加した後で、デバイスをポーリングしてデバイスのタイプを認識します。その後で、適切なデバイスドライバを割り当ててデバイスを管理します。次にデバイスのスナップショットを取得して、デバイスの構成と資産情報をデータベースにダウンロードします。

サポートされていないホストに対しては、グループも作成してシステム（インベントリ）に追加します。サポートされていないデバイスがアクティブで追加されないように（その結果としてデバイスのライセンスに考慮されます）、およびこれらのデバイスを含むインベントリに対して実行される操作を防ぐために、サポートされていないホストのデバイスはすべて、デフォルトで非アクティブに設定されています。

これらのデバイスにタスクを実行する場合、まずそのデバイスをアクティブ化する必要があります。次のいずれかの手順でデバイスをアクティブ化できます。

- [デバイス詳細]ページの[プロビジョニング]メニュー（[デバイスをアクティブ化]オプション）を使用する。
- [グループデバイス]ページで、チェックボックスを使用してデバイスを選択し、[アクション]ドロップダウンメニューから[アクティブ化]を選択する。

ネットワークデバイスの検出タスクの実行時に、[タスク情報]ページでは次のように表示されます。

- ノードがアクティブ：アクティブノードは、SNMPスキャンまたはNmapスキャンに応答したIPアドレスです。NAでノードを管理できる場合、そのノードはアクティブであるとみなされます。サポートされるデバイスの詳細については、『HP Network Automation Device Driver Reference』を参照してください。
- ノードが非アクティブ：非アクティブノードは、SNMPスキャンまたはNmapスキャン、またはそのいずれにも応答しなかったIPアドレスです。NAがデバイス照会用に不正なコミュニティ文字列を使用している場合、デバイスがSNMPスキャンに응答しない場合があります。
- サポートされていないホスト：サポートされていないホストは、SNMPスキャンまたはNmapスキャンに응答したIPアドレスです。ただし、SNMPの場合は、NAがサポートしていないSysOIDが返されます。Nmapの場合は、オペレーティングシステムのフィンガープリントが、NAがサポートしているものは一致しない、と返します。
- 既存デバイス：デバイスのIPアドレスが既にNAに認識されており、システム内に存在していることを示します。基本IPの診断として、そのデバイスのプライマリIPアドレスまたはIPアドレスがデータベース内に表示されます。

## スキャン方法

インターネットプロトコル（IP）のトラフィックには、次の2つのタイプがあります。

- ユーザデータグラムプロトコル（UDP）：単純なメッセージベースのコネクションレスプロトコルです。UDPを使用して、まとまった量のパケットがネットワーク全体に送信できます。一般的には、UDPはやや信頼性に欠けており、到着パケットの順序が保証されません。
- トランスミッションコントロールプロトコル（TCP）：コネクション指向のプロトコルです。TCPは非常に信頼性が高く、コネクションに沿ってパケットを受信する順序が保証されています。

SNMP スキャンではUDPが使用されます。SNMPでは、既知のSYSOIDを使用してシステムへの接続を試行し、ネットワークデバイスを特定します。SNMP スキャンの方法を使用すると、各システムへの複数の接続が不要なため、ネットワークにあまり影響を与えません。なお、SNMPは高速ですが、スキャンしたすべてのIPアドレスにすべてのパスワードルールが試されるため、大量のパスワードルールがある場合はダウンすることがあります。また、SNMPが成功するには、ログイン資格情報（コミュニティ文字列）が必要です。

Nmap スキャンではTCPが使用されます。ただし、一部のタスクでUDPを使用する構成にすることも可能です。Nmapはポートスキャナなので、ユーザのネットワークをスキャンしない場合は、SNMP スキャンの方法を選択します。また、さまざまなポートをテストするために、Nmapはデバイスに対して多くの接続をします。

Nmapはデバイスにログインしないため、ログイン資格情報は必要ありません。ネットワーク構成やスキャンしたIPアドレスによって、Nmapは高速にも低速にもなります。たとえば、192.168.0.0のIPアドレスのスキャンは、非常に低速になる可能性があります。ユーザの組織内にあるIPアドレス範囲のみをスキャンすることを、強く推奨します。

**注意：**多くの組織で、実行中のネットワークスキャンを検出したときにアラームを送信する監視システムが使用されています。Nmapを使用してネットワークデバイスを検出する場合は、ITチームが予定されたアクティビティを完全に認識していることを確認してください。

## IP アドレス範囲の定義

1つ以上のIPアドレス範囲を指定する必要があります。範囲を定義するには、次の2つの方法があります。

- CIDR（Classless InterDomain Routing）表記：CIDRは、IPアドレスのブロックすなわち範囲を示します。たとえば、10.255.1.0/24である場合、IPアドレス範囲が10.255.1.0から10.255.1.255までであることを示します。合計で256のIPアドレスがあります。CIDR表記で10.255.1.0/24の「/24」は、CIDRブロックの接頭部を構成するビット数を示します。この例では24ビットです。ブロックのバランス（最後の8ビット）は、ワイルドカードとみなされます。別の例を次に示します。
  - － 192.168.100.1/32は、192.168.100.1という1つのホストのことです。（ワイルドカードのビットはなく、32ビットすべてで接頭部を構成しているので注意が必要です。）
  - － 172.16.0.0/16は、172.16.0.0から172.16.255.255までの非常に大きな範囲を示しています。このような大きな範囲の検出はしないことをお勧めします。
  - － 10.255.0.0/23は、中程度の大きさの範囲です。この範囲は10.255.0.0から10.255.1.255までで、512のIPアドレスを含みます。
- 範囲入力：10.255.1.0 - 10.255.1.255のように、最小-最大表記でIPアドレスブロックを示します。192.168.100.1のように単一のIPアドレスを入力することもできます。除外範囲を指定することもできます。これにより、ネットワークデバイスの検出から、特定のアドレスやアドレス範囲をマスクすることができます。たとえば、10.255.1.0/24の範囲をスキャンするとします。ただし、10.255.1.10から10.255.1.20までにプリンタがあり、これをスキャンしたくない場合は、対象範囲を10.255.1.0/24に、除外範囲を10.255.1.10 - 10.255.1.20にします。

フィールド	説明/アクション
タスク名	[ネットワークデバイスの検出]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」（280ページ）を参照してください。</li> </ul>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」（278ページ）を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
最大ノード数	検出するIPアドレスの数を入力します。最大数は1024です。最大許容数を超えるノードが設定されているタスクは失敗するので注意が必要です。

フィールド	説明/アクション
包含	右側のボックスに、検出するIPアドレスまたはCIDR（Classless Inter-Domain Routing）範囲を入力して（たとえば、192.168.1.0-192.168.2.0、192.168.31.0/24など）、[<<検出範囲を追加]ボタンをクリックします。アドレスの範囲は両端を含みます。[検出範囲を削除]ボタンを使用して、範囲を削除することができます。
除外	右側のボックスに、除外するIPアドレスまたはCIDR（Classless Inter-Domain Routing）範囲を入力して（たとえば、192.168.1.0-192.168.2.0、192.168.31.0/24など）、[<<除外範囲を追加]ボタンをクリックします。アドレスの範囲は両端を含みます。[除外範囲を削除]ボタンを使用して、範囲を削除することができます。
スキャン方法	<p>次のスキャン方法から、1つまたは両方を選択します。</p> <ul style="list-style-type: none"> <li>• SNMP（デフォルト）</li> <li>• Nmap（注意：スキャンをするネットワーク範囲を指定するときには十分な考慮が必要です。ネットワークポロジによっては、非常に長時間のスキャンになる場合があります。また、インターネットアドレスはスキャンしないことをお勧めします。）</li> </ul> <p>スキャン方法の詳細については、「<a href="#">スキャン方法</a>」（342ページ）を参照してください。</p>
パスワードルールのフォールバック	選択した場合（デフォルト）、SNAPは必要なコミュニティ文字列をスキャンします。パスワードルールのフォールバックは、このコミュニティ文字列に使用します。
パーティション	ドロップダウンメニューからパーティションを選択します。パーティションの詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」（148ページ）を参照してください。
デバイスグループ名	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• デフォルトのグループ名を使用します（検出されたネットワークデバイス&lt;nnn&gt;、nnnはタスクIDです）。または、ドロップダウンメニューからデバイスグループを選択します。</li> <li>• 追加するデバイスのデバイスグループ名を入力します（デフォルト）。</li> </ul> <p><b>注意：</b>ネットワークデバイスの検出タスクを使用する場合、ネットワークスキャンには応答していても既知のOSは返さないデバイスから、新規グループが作成される場合があります。</p>
ドライバ検出	オンにすると（デフォルト）、デバイスの検出後にデバイスドライバが検出されます。
<b>デバイス資格情報のオプション</b>	
デバイス資格情報	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• ネットワーク全体のパスワードルールの使用</li> <li>• タスク固有の資格情報を使用。[ユーザ名]、[パスワード]、[SNMPコミュニティ文字列情報]を入力します。</li> </ul>
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。



フィールド	説明/アクション
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift] キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96ページ)</b>を参照してください。</p>

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、検出されたノードの詳細情報が表示されます。詳細については、「[\[タスク情報\]ページのフィールド](#)」(406ページ)を参照してください。

タスクが今後を開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、「[\[自分のタスク\]ページのフィールド](#)」(397ページ)を参照してください。

## [重複の削除]タスクページのフィールド

CSV（Comma Separated Value）ファイルまたはコネクタを使用してデバイスをNAにインポートする場合、重複するデバイスがNA データベースに作成される場合があります。たとえば、HP Network Node Manager や CiscoWorksなどの別の管理システムからデバイスをインポートする場合に、同一のデバイスに対して異なる管理 IP アドレスを使用する可能性があります。

重複の削除タスクでは、デバイスの重複の問題を解決します。ネットワークデバイスの検出タスクでは、これが自動的に実行されます。詳細については、「[\[ネットワークデバイスの検出\]タスクページのフィールド](#)」(341 ページ) を参照してください。

フィールド	説明/アクション
タスク名	[重複の削除]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280 ページ) を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセクタの使用方法的詳細については、「<a href="#">デバイスセクタ</a>」(142 ページ) を参照してください。</li> <li>CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b>（[デバイスリスト]ページのチェックボックスでグループのデバイスを選択して）アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>すぐに開始（デフォルト）</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278 ページ) を参照してください。
コメント	タスクに関するコメントを入力します。

フィールド	説明/アクション
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>

フィールド	説明/アクション
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、 <b>「ログ記録」(96ページ)</b> を参照してください。

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、**「[タスク情報]ページのフィールド」(406ページ)**を参照してください。

タスクが今後を開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、**「[自分のタスク]ページのフィールド」(397ページ)**を参照してください。

## [OS分析]タスクページのフィールド

[OS分析]タスクページは、sysoid（デバイスモデルの一意の識別子）、OSバージョン、フラッシュストレージオプション、モジュール、その他などのCisco デバイスに関する情報を収集します。この情報を使用して、ソフトウェア推奨が作成されます。OS分析タスクを実行してから、[タスク情報]ページにある[このデバイスのOS推奨を表示します。]をクリックします。詳細については、「[\[デバイスソフトウェアイメージ推奨\]ページのフィールド](#)」（223ページ）を参照してください。

フィールド	説明/アクション
タスク名	OS分析を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」（280ページ）を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセレクトアの使用法の詳細については、「<a href="#">デバイスセレクトア</a>」（142ページ）を参照してください。</li> <li>CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b>（[デバイスリスト]ページのチェックボックスでグループのデバイスを選択して）アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>すぐに開始（デフォルト）</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」（278ページ）を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
セッションログ	完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。セッションのログ記録を有効にした状態で、デバイスと対話するすべてのタスクが実行できます。タスク実行中のデバイスとの対話に関する詳細なログが記録されます。セッションログは、デバイス固有の問題をデバッグするための第一段階として表示してください。セッションログでは、CLI、SNMPおよびタスクで実行されるすべての転送プロトコルアクションの詳細がわかります。（ <b>注意：</b> 大量のデータが格納されることがあります。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」（96ページ）を参照してください。）

フィールド	説明/アクション
強制的に保存	<p>デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみに適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。</p> <ul style="list-style-type: none"> <li>• このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>• NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>(注意: この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます)。</p>
推定継続時間	<p>このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。</p>
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	<p>タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。</p>
承認の無効化	<p>タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。</p>
ドラフトとして保存	<p>オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。</p>
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	<p>次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。</p>
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ: タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的: 繰り返し間隔を分単位で指定します。</li> <li>• 日次: タスクは指定した時刻に毎日実行されます。</li> <li>• 週次: 週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次: 毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>

フィールド	説明/アクション
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	<p>メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。</p>
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96ページ)</b>を参照してください。</p>

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、**「[タスク情報]ページのフィールド」(406ページ)**を参照してください。

タスクが今後を開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、**「[自分のタスク]ページのフィールド」(397ページ)**を参照してください。



## [ポートスキャン]ページのフィールド

Nmapはネットワークデバイスの検出に使用されます。また、Nmapを使用して、デバイスのポートをスキャンして、開いているポート、およびポートが提供するサービスの内容についての詳細を返すことも可能です。ポートスキャンタスクを実行すると、次のことを実行できます。

- デバイス上のポートが開いているか閉じているかを容易に確認できます。
- TCPスタック、OS検出、およびNmapによって提供されるその他のサービスに基づいて、デバイスの脆弱性を確認できます。

ポートスキャンの結果は、[デバイスの詳細]ページの[表示]メニュー（[表示] --> [診断] --> [NAポートスキャン]）から表示できます。デバイス詳細の表示の詳細については、[「\[デバイス詳細\]ページのフィールド」](#)（193 ページ）を参照してください。

ポートスキャンタスクの設定を行うには、[「デバイスアクセス」](#)（44 ページ）を参照してください。

**注意：** ポートスキャンタスクに失敗すると、Nmapが適切に構成されない可能性があります。Nmapユーティリティのパスの入力方法の詳細については、[「\[デバイスアクセス\]ページのフィールド」](#)（45 ページ）を参照してください。Nmapのインストールの詳細については、『NA インストールおよびアップグレードガイド』を参照してください。

ポートは、リスンのために開かれている実際のソフトウェアベースのソケットです。診断の詳細は、[\[診断を検索\]](#) ページで検索できます。詳細については、[「\[診断を検索\]ページのフィールド」](#)（499 ページ）を参照してください。

フィールド	説明/アクション
タスク名	「ポートスキャン」と表示されます。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、<a href="#">「タスクテンプレート」</a>（280 ページ）を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセレクトタの使用法の詳細については、<a href="#">「デバイスセレクトタ」</a>（142 ページ）を参照してください。</li> <li>• CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b>（[デバイスリスト]ページのチェックボックスでグループのデバイスを選択して）アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>

フィールド	説明/アクション
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」（278ページ）を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
セッションログ	完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。セッションのログ記録を有効にした状態で、デバイスと対話するすべてのタスクが実行できます。タスク実行中のデバイスとの対話に関する詳細なログが記録されます。セッションログは、デバイス固有の問題をデバッグするための第一段階として表示してください。セッションログでは、CLI、SNMPおよびタスクで実行されるすべての転送プロトコルアクションの詳細がわかります。（ <b>注意</b> ：大量のデータが格納されることがあります。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」（96ページ）を参照してください。）
強制的に保存	<p>デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみに適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。</p> <ul style="list-style-type: none"> <li>このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>（<b>注意</b>：この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます。）</p>
推定継続時間	このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは 60 分です。
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>再試行なし（デフォルト）</li> <li>1回</li> <li>2回</li> <li>3回</li> </ul>

フィールド	説明/アクション
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96ページ)</b>を参照してください。</p>

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、**「[タスク情報]ページのフィールド」(406ページ)**を参照してください。

タスクが今後を開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、**「[自分のタスク]ページのフィールド」(397ページ)**を参照してください。

## [デバイスのプロビジョニング]タスクページのフィールド

デバイスのプロビジョニングタスクでは、デバイステンプレートをデバイスに適用します。デバイステンプレートの作成の詳細については、「[デバイステンプレート](#)」(118ページ)を参照してください。

**注意：** デバイステンプレートと、テンプレートの適用先デバイスが一致しない場合、タスクは失敗します。

フィールド	説明/アクション
タスク名	[デバイスのプロビジョニング]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセレクトアの使用方法的詳細については、「<a href="#">デバイスセレクトア</a>」(142ページ)を参照してください。</li> <li>CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。[デバイスのプロビジョニング]タスクを複数のデバイスに対して実行できるのは、CSVファイルを使用した場合だけである点に注意してください。また、CSVファイルを使用すれば、タスクの完了後に新しいプライマリIPアドレスをデバイスに割り当てることもできます。詳細については、「<a href="#">[テンプレート構成を編集]</a>」(120ページ)を参照してください。</li> </ul>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>すぐに開始（デフォルト）</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
セッションログ	完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。セッションのログ記録を有効にした状態で、デバイスと対話するすべてのタスクが実行できます。タスク実行中のデバイスとの対話に関する詳細なログが記録されます。セッションログは、デバイス固有の問題をデバッグするための第一段階として表示してください。セッションログでは、CLI、SNMPおよびタスクで実行されるすべての転送プロトコルアクションの詳細がわかります。（ <b>注意：</b> 大量のデータが格納されることがあります。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」(96ページ)を参照してください。）

フィールド	説明/アクション
強制的に保存	<p>デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみに適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。</p> <ul style="list-style-type: none"> <li>• このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>• NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>(注意: この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます)。</p>
デバイステンプレート	ドロップダウンメニューからデバイステンプレートを選択します。
準拠オプション	オンにすると、デバイスをプロビジョニングする前にポリシー準拠をテストします。
ステータスオプション	オンにすると、デバイスステータスはプロビジョニングでアクティブになります。
データコピーオプション	オンにすると、デバイステンプレートからの追加情報がデバイスにコピーされます。
推定継続時間	このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。
<b>タスク前/タスク後スナップショットオプション</b>	
タスク前スナップショット	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• なし</li> <li>• タスクの一部として</li> </ul>
タスク後スナップショット	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• なし</li> <li>• タスクの一部として</li> <li>• 個別のタスクとしてスケジュール</li> </ul>
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。

フィールド	説明/アクション
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、「<b>ログ記録</b>」(96ページ)を参照してください。</p>

## [デバイスコンテキストを追加]タスクページのフィールド

コンテキストとはデバイス内部にあるデバイスを指します。コンテキストには（モジュールやスロットがある）ハードウェアや仮想があります。NA 7.60以降は、コンテキストにはIPアドレスが必要でなくなりました。NAは、NAモジュールステータス診断を使用して親デバイス上のコンテキストを自動的に検出します。NAモジュールステータス診断の一部として、検出されたすべてのコンテキストはデバイスとして自動的に追加され、接続パスが自動的に構成されます。接続スルーデバイスの詳細については、「[\[IPアドレスの新規作成\]ページ（新規接続スルー）](#)」（238ページ）を参照してください。

さらにNAモジュールステータス診断は自動的に内部デバイス関係を追加します。ユーザ定義のデバイス関係の追加と削除の詳細については、「[\[デバイス関係\]ページのフィールド](#)」（226ページ）を参照してください。

Cisco FWSM（Firewall Service モジュール）の場合は、Cisco FWSMはCisco Catalyst デバイス内のモジュールです。Cisco FWSMにはコンテキストを含めることができます。したがって、Cisco FWSMとそのコンテキストにはそれぞれ独自の構成があるため、Cisco FWSMとそのコンテキストはNAに対してデバイスとして表示されます。

**注意：** NA デバイスドライバは、親デバイスに接続してコンテキストにアクセスするコマンドを発行する代わりに、親デバイスに接続して必要なスクリプトを自動的に実行することでコンテキストへの接続を処理します。これにより、コンテキストは標準デバイスとして表示されます。

NA インターフェイス診断を実行すると、NAによってコンテキストが自動的に検出され、デバイスが追加されます。NA インターフェイス診断によってコンテキストの削除が検出されると、それに対応するデバイスは非アクティブとしてマークされます。NA インターフェイス診断によって後でこのデバイスが検出された場合、このデバイスが再度有効化され、デバイス履歴が保存されます。

**注意：** デバイスコンテキストの削除は、デバイスコンテキストの追加のときと同じタスクページを使用します。ただし、NAはドライバから必要な変数を動的に取り出します。



フィールド	説明/アクション
タスク名	[デバイスコンテキストを追加]ページを表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280 ページ) を参照してください。</li> </ul>
適用先	デバイス：タスクを実行するIPアドレスまたはホスト名を入力します。ただし、デバイスコンテキストタスク（追加と削除）は、単一のデバイスに対してのみ実行可能です。
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278 ページ) を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
セッションログ	完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。セッションのログ記録を有効にした状態で、デバイスと対話するすべてのタスクが実行できます。タスク実行中のデバイスとの対話に関する詳細なログが記録されます。セッションログは、デバイス固有の問題をデバッグするための第一段階として表示してください。セッションログでは、CLI、SNMPおよびタスクで実行されるすべての転送プロトコルアクションの詳細がわかります。（ <b>注意</b> ：大量のデータが格納されることがあります。ログ記録の詳細については、「 <a href="#">ログ記録</a> 」(96 ページ) を参照してください。）
強制的に保存	デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみに適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。 <ul style="list-style-type: none"> <li>• このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>• NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>（<b>注意</b>：この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます。）</p>



フィールド	説明/アクション
変数	<p>変数はデバイスドライバで定義され、実行時にNAで表示されます。したがって、変数は各デバイスで異なります。CiscoPIX FWSM デバイスでは、デバイスコンテキストを作成するために必要な3つの変数があります。</p> <ul style="list-style-type: none"> <li>• コンテキスト名：作成するデバイスコンテキストの名前を入力します。</li> <li>• 構成の場所：デバイスコンテキストの構成場所を入力します。この場合、構成場所は構成を提供する方法を指定するプロトコルセットです。たとえば、構成がローカルディスク上である場合、ドロップダウンメニューで「ディスク」を選択できます。</li> <li>• 構成ファイル名：たとえば、「default.cfg」などの構成ファイル名を入力します。</li> </ul>
推定継続時間	このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは 60 分です。
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	使用不可
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>

フィールド	説明/アクション
<b>タスク完了時の通知</b>	
タスク完了時の通知	NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。 ヒント：電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、 <b>「ログ記録」(96ページ)</b> を参照してください。

## [VLANタスク]ページのフィールド

NAでは、VLANエントリとトランクポートをプロビジョニングできます。以下のことが可能です。

- VLANの新規作成
- VLAN名の編集
- VLANポートの割り当ての編集
- VLANコメントの編集（データベース内のみで、デバイス上では編集できません）
- トランクポートの構成（詳細については、「[トランクポートの構成](#)」（366ページ）を参照）

[デバイス VLAN の新規作成]ページで新しいVLANの作成、またはVLAN名とポート割り当ての編集を行うと、デバイス上で変更を実行する新しいVLANタスクがスケジュールされます。詳細については、「[VLANの作成と編集](#)」（216ページ）を参照してください。

**注意：** NAでは、要求されたVLAN変更内容でデータベースが更新されることはありません。それよりもむしろ、NAでは、VLANの新規作成タスクの結果として変更をキャプチャするために、タスク後のスナップショットタスクとVLANデータ収集診断タスクがスケジュールされます。

フィールド	説明/アクション
タスク名	[VLANを追加]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」（280ページ）を参照してください。</li> </ul>
適用先	デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセレクトアの使用法の詳細については、「 <a href="#">デバイスセレクトア</a> 」（142ページ）を参照してください。
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジュールリングの詳細については、「 <a href="#">タスクの予定</a> 」（278ページ）を参照してください。
コメント	タスクに関するコメントを入力します。

フィールド	説明/アクション
<b>タスクオプション</b>	
セッションログ	<p>完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。セッションのログ記録を有効にした状態で、デバイスと対話するすべてのタスクが実行できます。タスク実行中のデバイスとの対話に関する詳細なログが記録されます。セッションログは、デバイス固有の問題をデバッグするための第一段階として表示してください。セッションログでは、CLI、SNMPおよびタスクで実行されるすべての転送プロトコルアクションの詳細がわかります。(注意: 大量のデータが格納されることがあります。ログ記録の詳細については、「<a href="#">ログ記録</a>」(96 ページ) を参照してください)。</p>
強制的に保存	<p>デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみに適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。</p> <ul style="list-style-type: none"> <li>このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>(注意: この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます)。</p>
VLAN を編集	編集されたVLAN名を表示します。
新しい名前	新しいVLAN名を表示します。
ポートを追加	追加するポートを表示します。
ポートを削除	削除するポートを表示します。
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	<p>タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。</p>
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>再試行なし (デフォルト)</li> <li>1回</li> <li>2回</li> <li>3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。

フィールド	説明/アクション
繰り返しオプション	使用不可
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	<p>メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。</p>
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96ページ)</b>を参照してください。</p>

## トランクポートの構成

[インターフェイスの詳細を編集]ページの[VLAN トランク]オプションを使用すると、トランクポートを構成できます。ただし、トランクポートとして構成可能なのは特定のポートのみで、これらのポートを物理ポートやポートチャンネル（集合リンク）などのトランクポートとして構成できます。ループバックポートやVLAN インターフェイスとして使用するポートは、トランクポートとして構成することはできません。

[VLAN トランク]オプションは、[インターフェイスの詳細を編集]ページの[VLAN トランク]オプションをオンにしたときに表示される折り畳み可能な行セットです。表示されるフィールドは次のとおりです。

- ネイティブVLAN ID
- メンバー VLAN

ネイティブVLANトラフィックは、トランクポート上でタグ付けされません。さらに、トランクポートで受信されたタグ付けされていないパケットはネイティブVLANのパケットと見なされます。

**注意：** ネイティブVLANはCiscoの用語です。ProCurveではネイティブVLANという用語は使用されません。代わりにメンバーVLANという用語が使用されます。つまり、トランクポートにはタグなしVLANメンバーシップを1つのみ設定できます。ネイティブVLAN IDとメンバーVLANという用語は基本的に同義語です。

[メンバーVLAN]フィールドで選択したVLANのトラフィックはトランクポートによって転送されます。選択していないVLANはすべて整理されます（トランクポートが元々VLANのメンバーであった場合は、VLANメンバーシップが削除されます）。[VLAN トランク]オプションがオフの場合、ポートは非トランクポートとして構成され、[ネイティブVLAN ID]フィールドで示されるVLANに割り当てられます。

**注意：** [トランクポート]オプションがオフの場合、ポートが現在トランクポートであると、デフォルトのVLAN IDを求めるプロンプトが表示されます。デフォルトのVLAN IDは、トランクポートが非トランクポートになるときにポートに割り当てられるVLAN IDです。VLAN IDの入力を求めるプロンプトが表示されます。VLAN IDを入力しないと、ネイティブVLAN IDが使用されます。ネイティブVLAN IDが存在しない場合、NAはデバイスにデフォルトのVLAN IDを送りません。このため、デバイスはポートをそのデフォルトVLAN（VLAN 1）に割り当てます。

詳細については、「[\[インターフェイスの詳細を編集\]ページのフィールド](#)」（208 ページ）を参照してください。VLAN トランクポート設定を変更すると、デバイスでの変更を適用する新しいVLAN タスクが作成されます。詳細については、「[\[VLAN タスク\]ページのフィールド](#)」（363 ページ）を参照してください。

## [Cisco.comからイメージをダウンロード]タスクページ

[Cisco.comからイメージをダウンロードタスク]ページでは、Cisco.com Software Center を閲覧して、ダウンロードできるイメージを決定できます。Cisco.com Software Center には、Cisco のインターネットワーク製品向けのシステムソフトウェアおよびドライバの公開バージョンが存在します。

[Cisco.comからイメージをダウンロード]ページを表示するには、[デバイス]メニューバーで[デバイスツール]を選択し、[ソフトウェアイメージ]をクリックします。[ソフトウェアイメージ]ページが開きます。ページの最上部にある[Cisco.comからイメージセットを追加]リンクをクリックします。

フィールド	説明/アクション
タスク名	[Cisco.comからイメージをダウンロード]を表示します。必要に応じて、別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280 ページ) を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセクタの使用方法的詳細については、「<a href="#">デバイスセクタ</a>」(142 ページ) を参照してください。</li> </ul>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
デバイス/グループリストを変更	<p>[デバイスリストをリフレッシュ]ボタンをクリックすると、上で選択したあらゆるデバイスが[デバイスリスト]フィールドにリストされます（Cisco がデバイスベンダーのデバイスのみ）。他のベンダーのデバイスを選択しても、そのデバイスは[デバイスリスト]フィールドには表示されません。一般的なプラットフォーム情報も一緒に表示されます。これにより、今後の使用を予定している、またはまだNAに追加していないデバイスのソフトウェアイメージを検索できます。</p> <p>[デバイスリスト]フィールドで項目を選択すると、以下のフィールド間にフローが作成されます。次のフィールドの詳細については、「<a href="#">[デバイスソフトウェアイメージ推奨]ページのフィールド</a>」(223 ページ) を参照してください。</p> <ul style="list-style-type: none"> <li>• デバイスリスト：すべての利用可能な汎用Cisco デバイスをリストします。</li> <li>• バージョンリスト：選択したデバイスのデバイスバージョン情報を表示します。</li> <li>• 機能リスト：選択したデバイスの機能情報を表示します。</li> </ul>
ダウンロード選択	ダウンロードするソフトウェアイメージを選択して、[タスクを保存]ボタンをクリックします。詳細については、「 <a href="#">[ソフトウェアイメージセットを追加]ページのフィールド</a> 」(445 ページ) を参照してください。

フィールド	説明/アクション
Apply to パーティション	ドロップダウンメニューからパーティションを選択します。(注意：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。) セキュリティや業務上の理由でパーティションを作成した場合、パーティションに沿ってソフトウェアイメージをパーティションできます。ソフトウェアイメージがすべてのパーティションで利用できる場合、構成に応じてソフトウェアイメージは[共有] (または[グローバル]) と表示されます。
<b>スケジューリングオプション</b>	
再試行回数	使用不可
繰り返しオプション	使用不可
<b>タスク完了時の通知</b>	
タスク完了時の通知	NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。 ヒント：電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift] キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、 <b>「ログ記録」(96ページ)</b> を参照してください。

終了時に、必ず[保存]をクリックしてください。[タスク情報]ページが開きます。このページには、タスクステータス、影響を受けるデバイス、継続期間、結果の詳細などの詳細なタスク情報が記載されています。



## [デバイスソフトウェアのバックアップ]タスクページのフィールド

デバイスソフトウェアのバックアップタスクで、デバイスからNAソフトウェアイメージリポジトリにソフトウェアイメージをコピーできます。すべてのコピーされたソフトウェアイメージは、各ソフトウェアイメージを独自のソフトウェアイメージセットに追加するように指定しない限り、既存のソフトウェアイメージセットに追加されます。ソフトウェアイメージセットの名前は、指定されたソフトウェアイメージセットの名前と、デバイスからコピーされたソフトウェアイメージセットの名前との組み合わせになります。次のことに注意が必要です。

- 一意の名前を指定すると、新規ソフトウェアイメージセット名が作成されます。
- ソフトウェアセット名が一意ではない場合、ソフトウェアイメージセットは既存のソフトウェアイメージセットに追加されます。
- 重複するソフトウェアイメージは、既存のソフトウェアイメージセットには追加されません。このため、デバイスソフトウェアのバックアップタスク実行時に警告メッセージが表示されます。

新規ソフトウェアイメージセットが作成されると、ソフトウェアイメージセットの属性が、ダウンロード元となったデバイスの既知の情報と照合されます。これにより、ダウンロードされたソフトウェアイメージが、そのソフトウェアイメージを実行できないデバイスに適用されることを防ぎます。詳細については、「[イメージ同期レポートのフィールド](#)」(618 ページ) を参照してください。

[デバイスソフトウェアのバックアップタスクの結果]ページには、ソフトウェアイメージセットのリストへのリンクがあり、このリストですべてのソフトウェアイメージセットの名前と要件を確認できます。

[デバイスソフトウェアのバックアップ]タスクページを開くには、[レポート]メニューバーで[イメージ同期レポート]をクリックします。[イメージ同期レポート]で、1つまたは複数のチェックボックスをオンにしてから、[アクション]ドロップダウンメニューの[イメージを同期]オプションを選択します。

フィールド	説明/アクション
タスク名	[デバイスソフトウェアのバックアップ]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280 ページ) を参照してください。</li> </ul>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278 ページ) を参照してください。
コメント	タスクに関するコメントを入力します。
カスタム1	カスタムデータを入力します。

フィールド	説明/アクション
<b>タスクオプション</b>	
セッションログ	<p>完全なデバイスセッションログを格納するには、[完全なデバイスセッションログを格納]チェックボックスをオンにします。セッションのログ記録を有効にした状態で、デバイスと対話するすべてのタスクが実行できます。タスク実行中のデバイスとの対話に関する詳細なログが記録されます。セッションログは、デバイス固有の問題をデバッグするための第一段階として表示してください。セッションログでは、CLI、SNMPおよびタスクで実行されるすべての転送プロトコルアクションの詳細がわかります。(注意: 大量のデータが格納されることがあります。ログ記録の詳細については、「ログ記録」(96 ページ) を参照してください)。</p>
強制的に保存	<p>デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみに適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。</p> <ul style="list-style-type: none"> <li>このタスクの完了時に、NA で現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>NA でスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>(注意: この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます)。</p>
ベースイメージセット名	<p>次のオプションから選択できます。</p> <ul style="list-style-type: none"> <li>ユーザ名: ベースイメージセット名を入力します。</li> <li>既存を使用: ドロップダウンメニューから既存のソフトウェアイメージセットを選択します。</li> </ul>
イメージストレージ	<p>デバイスとNA ソフトウェアリポジトリにコピーするソフトウェアイメージが表示されます。次のオプションから選択できます。</p> <ul style="list-style-type: none"> <li>グループイメージセット: コピーされるすべてのソフトウェアイメージが、新規、または既存のソフトウェアイメージセットのいずれかに追加されます。</li> <li>イメージを一意的イメージセットに分割: 上で指定 (入力、または選択) したイメージセット名を、新規イメージセットのベース名として使用します。完全名には、元の名前とデバイスからコピーされたソフトウェアイメージの名前が含まれます。</li> </ul>
推定継続時間	<p>このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルトでは60分です。</p>
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>再試行なし (デフォルト)</li> <li>1回</li> <li>2回</li> <li>3回</li> </ul>
再試行間隔	<p>次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。</p>
繰り返しオプション	<p>このタスクではこのオプションは利用できません。</p>

フィールド	説明/アクション
<b>タスク完了時の通知</b>	
タスク完了時の通知	NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。 ヒント：電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、 <b>「ログ記録」(96ページ)</b> を参照してください。

終了時に、必ず[タスクを保存]をクリックしてください。[タスク情報]ページが開きます。このページには、タスクステータス、影響を受けるデバイス、継続期間、結果の詳細などの詳細なタスク情報が記載されています。

## [ポリシー準拠の確認]タスクページのフィールド

ポリシー準拠の確認タスクにより、デバイスが、構成ポリシーまたはソフトウェア準拠ポリシーに準拠しているかどうかを判別できます。ポリシーの作成や更新のときに、ポリシー準拠の確認タスクを実行するのみです。これを行うことによって、新たに作成したポリシーにデバイスが準拠しているかどうかを直ちに判断することができます。

**注意：** デフォルトでは、構成の変更が検出されるたびに、NAはデバイスの構成に対して準拠性チェックを実行します。構成されている場合、適用したポリシーに構成変更が違反しているとユーザに通知します。また、電子メール警告、SNMPトラップなど多くの自動機能を構成でき、デバイスを強制的に準拠状態に戻すコマンドスクリプトの実行も可能です。

フィールド	説明/アクション
タスク名	[ポリシー準拠の確認]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセクタの使用方法の詳細については、「<a href="#">デバイスセクタ</a>」(142ページ)を参照してください。</li> <li>• CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b> ([デバイスリスト]ページのチェックボックスでグループのデバイスを選択して) アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。

フィールド	説明/アクション
<b>タスクオプション</b>	
アクション	<p>次のオプションの1つまたはすべてを選択します。</p> <ul style="list-style-type: none"> <li>• 構成ポリシー準拠を確認（デフォルト）：選択したデバイスが構成ポリシーに準拠しているかどうかを確認します。</li> <li>• 診断準拠を確認：選択したデバイスが診断ポリシーに準拠しているかどうかを確認します。</li> <li>• ソフトウェア準拠を確認：選択したデバイスがソフトウェアポリシーに準拠しているかどうかを確認します。</li> <li>• ソフトウェアレベルを確認：オンにすると、ソフトウェアレベルが確認され、ソフトウェアレベルおよび特定されたセキュリティの脆弱性に関する結果をテキスト出力します。</li> </ul>
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>

フィールド	説明/アクション
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	<p>メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。</p>
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96ページ)</b>を参照してください。</p>

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。

詳細については、**「[タスク情報]ページのフィールド」(406ページ)**を参照してください。タスクが今後に開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、**「[自分のタスク]ページのフィールド」(397ページ)**を参照してください。

## [サマリレポートの生成]タスクページのフィールド

サマリレポートの生成タスクでは、サマリレポートを更新できます（デフォルトでは、日曜日ごとの繰り返しタスクで更新）。サマリレポートの更新スケジュールを恒久的に変更したい場合は、既存の繰り返しタスクを編集できます。

フィールド	説明/アクション
タスク名	[サマリレポートの生成]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>すぐに開始（デフォルト）</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには拡大鏡アイコンをクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>再試行なし（デフォルト）</li> <li>1回</li> <li>2回</li> <li>3回</li> </ul>

フィールド	説明/アクション
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p>ヒント：電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、「[\[タスク情報\]ページのフィールド](#)」（406ページ）を参照してください。

タスクが今後を開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、「[\[自分のタスク\]ページのフィールド](#)」（397ページ）を参照してください。



## [電子メールレポート]タスクページのフィールド

電子メールレポートタスクでは、NA レポートを電子メールで送信できます。

フィールド	説明/アクション
タスク名	[電子メールレポート]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280 ページ)を参照してください。</li> </ul>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>すぐに開始（デフォルト）</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278 ページ)を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
実行するレポート	電子メールで送信するレポートを選択します。このタスクを実行するたびに、最後に保存されたレポートが新規の情報に上書きされます。(注意：このタスクで、サマリレポートを電子メールで送信することはできません。)
適用先	このフィールドは、ネットワークステータスのレポートのみに表示されます。レポートを実行するデバイスグループを選択します。
電子メールの受信者	電子メールアドレスを1つ以上入力します。複数のアドレスは必ずカンマで区切ります。
電子メールの件名	電子メールメッセージの件名を入力します。
電子メールの書式	ドロップダウンメニューから、次のオプションのいずれかを選択します <ul style="list-style-type: none"> <li>デフォルトの書式</li> <li>HTML メール</li> <li>CSV ファイルの添付</li> <li>プレーンテキスト</li> <li>HTML メール（リンクなし）</li> </ul>
ファイルのエクスポート	チェックボックスをクリックして、レポートのコピーをファイルに保存します。

フィールド	説明/アクション
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>

フィールド	説明/アクション
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、 <a href="#">「ログ記録」(96ページ)</a> を参照してください。

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、[「\[タスク情報\]ページのフィールド」\(406ページ\)](#)を参照してください。タスクが今後を開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、[「\[自分のタスク\]ページのフィールド」\(397ページ\)](#)を参照してください。

## [リモートエージェントを配布]タスクページのフィールド

リモートエージェントの配布タスクでは、各サテライトゲートウェイホスト上にNAリモートエージェントを配布できます。管理対象とするデバイスと同一のLAN上にNAリモートエージェントをインストールすることで、WANトラフィックを最小限に抑え、SyslogおよびTFTPをローカルで使用してデバイスを管理できます。

リモートエージェントの配布タスクを開くには、[タスク]メニューバーで[タスクの新規作成]を選択し、[リモートエージェントを配布]をクリックします。[ゲートウェイリスト]ページの[リモートエージェントを配布]リンクをクリックしても、このページに移動できます。詳細については、「[\[ゲートウェイリスト\]ページのフィールド](#)」(153ページ)を参照してください。

フィールド	説明/アクション
タスク名	[リモートエージェントを配布]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>すぐに開始（デフォルト）</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
アクション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>インストール（または再インストール）：NA リモートエージェントをインストールします。NA リモートエージェントが既にインストールされている場合、既存のNA リモートエージェントは削除され、新しいNA リモートエージェントがインストールされます。</li> <li>アンインストール：NA リモートエージェントをアンインストールします。</li> </ul>
リモートゲートウェイ	NAリモートエージェントの配布先となるゲートウェイ名をドロップダウンメニューから選択します。
ログイン	リモートエージェントの配布には、サテライトゲートウェイホストのルート権限が必要です。次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>rootとして：rootユーザ名でSSHを行い、rootパスワードを入力します。</li> <li>非rootとして：非rootユーザとしてSSHを行います。このオプションを選択した場合、suパスワード（ルートパスワード）、またはsudoパスワード（通常はユーザ名パスワードと同じですが、sudoの構成によっては変えることができます）のいずれかを選択します。</li> </ul>

フィールド	説明/アクション
管理コア	コアゲートウェイがNAコアと同じホスト上にインストールされている場合、[管理コア]は「localhost」である必要があります（デフォルト）。コアゲートウェイがNAコアとは異なるホスト上に存在する場合、[管理コア]はNAコアのホスト名、またはIPアドレスである必要があります。（ <b>注意</b> ：NAコアホストに別のIPアドレスが存在する場合、コアゲートウェイホストからNAコアに接続するためのIPアドレスを使用してください。）
対象領域	ドロップダウンメニューからコアゲートウェイの領域名を選択します。
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	使用不可
<b>タスク完了時の通知</b>	
タスク完了時の通知	NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。 <b>ヒント</b> ：電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、 <b>「ログ記録」(96ページ)</b> を参照してください。

## [FQDNの解決]タスクページのフィールド

FQDNの解決タスクでは、デバイスのプライマリIPアドレスに対してリバースDNS検索を実行することで、システム内の各デバイスにFQDN（Fully Qualified Domain Name）を設定できます。

フィールド	説明/アクション
タスク名	[FQDNの解決]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	<p>次の中からオプションを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
適用先	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセクタの使用方法的詳細については、「<a href="#">デバイスセクタ</a>」(142ページ)を参照してください。</li> <li>CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul> <p><b>注意：</b>（[デバイスリスト]ページのチェックボックスでグループのデバイスを選択して）アドホックデバイスグループに対して実行するタスクをスケジューリングするときに、このセクションではアドホックデバイスグループに含まれるデバイスが表示されます。</p>
開始日	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>すぐに開始（デフォルト）</li> <li>開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	<p>タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「<a href="#">タスクの予定</a>」(278ページ)を参照してください。</p>
コメント	タスクに関するコメントを入力します。
タスクオプション (使用不可)	
承認オプション	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	<p>タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。</p>
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。

フィールド	説明/アクション
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96ページ)</b>を参照してください。</p>

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、「[\[タスク情報\]ページのフィールド](#)」(406ページ)を参照してください。タスクが今後に開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、「[\[自分のタスク\]ページのフィールド](#)」(397ページ)を参照してください。



## [データの整理]タスクページのフィールド

データの整理は、システムを構成できるシステム管理者、またはそれに類似の権限を持つユーザが必要なシステムタスクです。データの整理により、廃止されたファイル、診断、イベントおよびタスクが削除されます。次のファイルは、[データの整理]で削除できません。

- 現在の構成
- 配布予定の構成

NAサーバを整理用に構成する場合、ファイルの保存期間を指定する必要があります。これらのファイルのデフォルト設定は、次のとおりです。

- 構成：365日
- タスク：365日
- 診断：45日
- イベント：45日
- セッション：45日
- ログファイル：30日

フィールド	説明/アクション
タスク名	[データの整理]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	タスクに関するコメントを入力します。
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。

フィールド	説明/アクション
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96 ページ)</b>を参照してください。</p>

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。

詳細については、「[\[タスク情報\]ページのフィールド](#)」(406ページ)を参照してください。タスクが今後に開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、「[\[自分のタスク\]ページのフィールド](#)」(397ページ)を参照してください。

## [外部アプリケーションの実行]タスクページのフィールド

外部アプリケーションの実行タスクでは、「ping」コマンドや外部言語インタープリタなどの、外部アプリケーションのNAからの実行をスケジューリングできます。このタスクで、外部のヘルプデスクやNMSソリューションを統合することもできます。

**注意：** Windowsプラットフォームでは、パスにWindowsファイルの区切り文字であるバックスラッシュ（\）を使用してください。ショートネーム（~<n>が付いている名前）は、ファイル名にスペースが含まれる場合のみ必要です。たとえば、C:\Rendition は問題ありませんが、C:\Program Files は不可です。ショートネームは、パラメータを渡すときにのみ必要です。たとえば、C:\Program Files\Internet Explorer\iexplore.exe は問題ありません。ただし、C:\Program Files\Internet Explorer\iexplore.exe someFilename.html は不可です。C:\Progra~1\Intern~1\iexplore.exe someFilename.html を使用する必要があります。

フィールド	説明/アクション
タスク名	[外部アプリケーションの実行]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280 ページ) を参照してください。</li> </ul>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278 ページ) を参照してください。
コメント	タスクに関するコメントを入力します。
<b>タスクオプション</b>	
実行	実行するコマンド・ライン・ユーティリティまたはスクリプトを入力します。実行ファイルに必ず完全修飾パスとファイル名を付けてください。実行するアプリケーションの名前の後にパラメータを続けることで、外部アプリケーションにパラメータを付けることができます。たとえば、外部コマンド「foo」をパラメータの「bar」および「bat」と実行するには、「foo bar bat」と入力します。
開始	外部アプリケーションのパスと、そのアプリケーションの起動ディレクトリを入力します。
タスク結果	0以外の結果コードをタスクの失敗とする場合は、[0ではない結果コードが返された場合にタスクが失敗したとみなす]ボックスをオンにします。

フィールド	説明/アクション
テキスト出力	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• <b>stdoutの結果（デフォルト）</b>：アプリケーションの実行後に、コンソールへの標準テキスト出力が[タスクの詳細]に保存されます。このテキスト出力は、コマンド・ライン・ユーティリティなどの、大半のアプリケーションで使用されます。</li> <li>• <b>ファイル結果</b>：出力結果がない場合、このオプションを選択します。ただし、ファイル名は空白にします。アプリケーションの実行後に、NAはこのファイルを読み込み、[タスクの詳細]にその内容を含めます。これは、標準出力ではなくファイルに出力を書き出すコマンドで便利です。該当する場合は、結果ファイルの完全修飾パスを必ず入力してください。</li> </ul>
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	<p>タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。</p>
承認の無効化	<p>タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。</p>
ドラフトとして保存	<p>オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。</p>
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	<p>次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。</p>
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>

フィールド	説明/アクション
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがタスク完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	<p>メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。</p>
<b>タスクログ</b>	
タスクログ	<p>利用可能である場合、特定タスクのログを1回実行するように予定できます。[このタスクで生成されたログ出力を格納]チェックボックスをオンにして、[Shift]キーを押しながら1つまたは複数のログを選択します。選択したログが強調表示されます。タスクの実行時にログ記録を行うように設定したときに、ログを開始できない場合、タスクはその後の処理を行うことなく、ただちに異常終了します。ログ記録の詳細については、<b>「ログ記録」(96ページ)</b>を参照してください。</p>

入力が完了したら、必ず[保存]をクリックします。タスクを直ちに実行するようにスケジューリングされている場合は、[タスク情報]ページが開きます。[タスク情報]ページには、タスクの開始日、継続期間、ステータスなど、タスクの詳細が表示されます。詳細については、**「[タスク情報]ページのフィールド」(406ページ)**を参照してください。

タスクが今後を開始するようにスケジューリングされている場合は、[自分のタスク]ページで新規タスクが強調表示されます。詳細については、**「[自分のタスク]ページのフィールド」(397ページ)**を参照してください。

## マルチタスクプロジェクトの予定

マルチタスクプロジェクトを構成して、単一のプロジェクトで複数の異なるタスクをまとめて順次実行できます。たとえば、ソフトウェアのアップグレードを実行してから、更新した構成をデバイスに送信するとします。1つのプロジェクトにタスクを統合すると、タスクレベルではなくプロジェクトレベルで作業を許可できるので、管理承認が単純になります。また、別々のタスク群を統合して、まとめて管理もできます。

**注意：** マルチタスクプロジェクトを実行するための適切な権限が必要です。詳細については、「[\[ユーザのロールと権限\] ページのフィールド](#)」(257 ページ) を参照してください。

マルチタスクプロジェクトに含まれる各タスクは指定された順に実行されます。たとえばデバイスグループに対して、ドライバの検出、スナップショット、カスタムスクリプトの実行などをスケジューリングできます。NA Schedulerに関する場合は、マルチタスクプロジェクトは1つのタスクとみなされます。マルチタスクプロジェクトの実行がスケジューリングされると、NA Schedulerが全タスクを指定された順に実行します。なんらかの理由で、マルチタスクプロジェクトのタスクの1つが実行されない場合、マルチタスクプロジェクトは失敗します。マルチタスクプロジェクトに承認が必要な場合、マルチタスクプロジェクトが承認されると、マルチタスクプロジェクトに含まれる全タスクが自動的に承認されます。

**注意：** [マルチタスクプロジェクト] ページで、デバイスやデバイスグループを予約することができます。

## サブタスク警告ステータス

マルチタスクプロジェクトでは、サブタスクが警告状態で完了した場合、後続するサブタスクの実行を継続するか、残りのサブタスクをすべてキャンセルするか、どちらかを選択できます。この機能を使用すると、問題が発生する可能性のあるデバイスに対して実行しているタスクをキャンセルできます。

この機能を有効にするには：

1. [管理]メニューから、[カスタムデータの設定]ページに移動します。
2. [タスク]セクションの下の方の6番目の[API名]フィールドまでスクロールします。
3. 6番目の[API名]フィールドで、次のように入力します。**[subtask\_control]**
4. [表示名]フィールドで、次のように入力します。**警告メッセージのある残りタスクを取り消す**
5. [値]フィールドで、[絞り込み]チェックボックスをオンにして、次のように入力します。**[Yes, No]**
6. [保存]ボタンをクリックします。

この機能を有効にしてマルチタスクプロジェクトのサブタスクを作成すると、すべてのマルチタスクサブタスクページの[コメント]フィールドの下に、次のフィールドが表示されます。「警告メッセージのある残りタスクを取り消す」

このフィールドには次のオプションがあります。

- 空白：残りのサブタスクの実行を継続します。
- Yes：残りのサブタスクをキャンセルします。
- No：残りのサブタスクの実行を継続します。

**注意：** この機能を無効にするには、[カスタムデータ設定]ページの[6番目のAPI名]チェックボックスをオフにして、[保存]ボタンをクリックします。

マルチタスクプロジェクトを作成するには、[タスク]メニューバーで[マルチタスクプロジェクトの新規作成]をクリックします。[タスク/テンプレートの新規作成 - マルチタスクプロジェクト]ページが開きます。



## [マルチタスクプロジェクト]ページのフィールド

フィールド	説明/アクション
タスク名	[マルチタスクプロジェクト]を表示します。必要に応じて別のタスク名を入力できます。
保存オプション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• タスクとして保存：デフォルトでこのオプションが選択されています。</li> <li>• タスクテンプレートとして保存：選択した場合、タスクはタスクテンプレートとして保存され、[タスクテンプレート]ページに表示されます。タスクテンプレートの詳細については、「<a href="#">タスクテンプレート</a>」(280ページ)を参照してください。</li> </ul>
開始日	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• すぐに開始（デフォルト）</li> <li>• 開始時刻：タスクを開始する日時を入力します。日付ボックスの隣にあるカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。</li> </ul>
タスク優先度	タスクに優先度を設定できます。1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。タスクのスケジューリングの詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	複数のタスクジョブについてのコメントを追加します。
<b>タスクオプション</b>	
サブタスク	ドロップダウンメニューからサブタスクを選択します。選択するサブタスクによって、そのタスクの[タスクの新規作成]ページが開き、タスクを構成できます。たとえば、[Syslogの構成]タスクを選択した場合は、[タスクの新規作成 - Syslogの構成]ページが開きます。タスクを追加すると、[タスクの編集 - マルチタスクプロジェクト]ページに表示されます。必要に応じて、タスクの編集と削除ができます。[タスクの保存]をクリックすると、[保留タスク]ページが開きます。「 <a href="#">[予定タスク]ページのフィールド</a> 」(400ページ)を参照してください。
予約デバイス	デバイスセクタを使用してデバイスを予約します。デバイスセクタの使用法の詳細については、「 <a href="#">デバイスセクタ</a> 」(142ページ)を参照するか、またはデバイスセクタの右上にある疑問符(?)をクリックします。
推定継続時間	タスクを実行するデバイスまたはデバイスグループの予約時間を入力します。デフォルトでは60分です。
<b>承認オプション</b>	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。

フィールド	説明/アクション
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	使用不可
<b>タスク完了時の通知</b>	
タスク完了時の通知	<p>NAがマルチタスクプロジェクトの完了時に電子メールメッセージを送信するようにするには、[電子メールを送信]チェックボックスをオンにします。</p> <p><b>注意：</b>各サブタスクの完了時には電子メールメッセージは送信されません。</p> <p><b>ヒント：</b>電子メールコンテンツのフォーマットはすべてのタスクで同じです。電子メールコンテンツの変更の詳細については、『NA Administration Guide』を参照してください。</p>
電子メールの受信者	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。デフォルト値はタスク作成者の電子メールメッセージです。

終了時に、必ず[保存]をクリックしてください。

## マルチタスクプロジェクトの構成方法

このセクションでは、マルチタスクプロジェクトの設定の過程を段階的に見ていきます。これには、プロジェクトのデバイスまたはデバイスグループの予約や、アクティビティカレンダーを使用してプロジェクトで予約したデバイスやデバイスグループを表示することなどが含まれます。

1. [タスク]メニューバーから[マルチタスクプロジェクトの新規作成]をクリックします。[タスク/テンプレートの新規作成 - マルチタスクプロジェクト]ページが開きます。
2. [タスク名]フィールドに、たとえば「Pine Valley Office」などのプロジェクト名を入力します。特定のデバイスやデバイスグループを *Pine Valley Office* という名前の親グループに既に追加していると仮定します。それ以外の詳細については、[「デバイスグループの追加」\(136ページ\)](#) を参照してください。
3. [開始日]フィールドで、[すぐに開始]（デフォルト）をオンにするか、カレンダーをクリックしてプロジェクト開始の日付と時刻を選択します。
4. 1～5（1が最も高い優先度）までのタスク優先度を選択するには下矢印をクリックします。デフォルト値は3です。優先度の高いタスクは優先度の低いタスクより前に実行されます。
5. [コメント]フィールドに、プロジェクトのコメントを入力します。
6. [タスクオプション]の[サブタスク]フィールドで、プロジェクトに含めるサブタスクをドロップダウンメニューから選択します。たとえば、[パスワードの配布]タスクを選択した場合は、[タスク/テンプレートの新規作成 - パスワードの配布]ページが開きます。
7. [パスワードの配布]ページで、[適用先]フィールドのドロップダウンメニューから Pine Valley Office を選択します。CSV ファイルの名前を入力するか、またはブラウズすることもできます。この CSV ファイルには、Pine Valley Office にあるデバイスやデバイスグループのリストが含まれています。
8. [タスクオプション]セクションを終了します。このセクションに表示されるオプションは、タスクごとに異なります。パスワードの配布タスクの詳細については、[「\[パスワードの配布\]タスクページのフィールド」\(288ページ\)](#) を参照してください。
9. [タスクを保存]をクリックします。[マルチタスクプロジェクト]ページに戻り、プロジェクトにさらにサブタスクを追加することができます。
10. Pine Valley Office のすべてのデバイスを予約するには、[予約デバイス]フィールドの[変更]をクリックします。[デバイスセクタ]が開きます。
11. [Pine Valley Office]をダブルクリックします。[Pine Valley Office]の全デバイスが表示されます。
12. Pine Valley Office の全デバイスを予約する場合は、[すべて選択]をクリックして、次に右矢印(>>>)をクリックします。[追加されたデバイス]ボックスにデバイスが一覧表示されます。特定のデバイスのみ追加するには、ホスト名やデバイスのIPアドレスの一部を入力して検索範囲を狭めるか、追加するデバイスのみ選択して、右矢印をクリックします。
13. デバイスを予約する推定継続期間を入力します。デフォルトは1時間です。
14. [タスクを保存]をクリックします。予約デバイスのリストが、[予約デバイス]フィールドに含まれます。
15. [タスクを保存]をクリックします。[自分のタスク]ページが開き、プロジェクトの編集、削除、休止、即座に実行などができます。
16. [タスク]メニューバーで、[アクティビティカレンダー]をクリックします。[アクティビティカレンダー]が開きます。

17. カレンダーで、プロジェクトの Pine Valley Office デバイスの予約日を選択します。選択したタイムスロットに、プロジェクト Pine Valley Office が表示されます。
18. [Pine Valley Office] をクリックします。[タスク情報] ページが開きます。このページに、プロジェクトの詳細情報が表示されます。

## [自分のタスク]の表示

[自分のタスク]ページでは、現在ログインしているユーザが作成したタスクを表示します。タスクが実行されていない場合、該当するものがあればタスクの承認ステータスも表示します。

[自分のタスク]ページを表示するには、[タスク]メニューバーから[自分のタスク]をクリックします。[自分のタスク]ページが開きます。

## [自分のタスク]ページのフィールド

フィールド	説明/アクション
自分のドラフト	該当する場合は、[自分のドラフト]ページが開きます。
承認の要求	<p>タスク承認を受ける必要がある場合は、[承認の要求]ページが開きます。このページでは、現在ログインしているユーザによる承認を必要とするタスクを確認できます。デフォルトでは、次のステータスのタスクを含む未完了のタスクがページに表示されます。</p> <ul style="list-style-type: none"> <li>• 未承認</li> <li>• 承認を待機中</li> <li>• 実行待ち</li> </ul> <p>詳細については、「<a href="#">承認の要求</a>」(670 ページ) を参照してください。</p>
予定タスク	[予定タスク]ページが開きます。このページでは、キュー内に存在していてまだ実行されていない予定されたタスクを確認できます。詳細については、「 <a href="#">[予定タスク]ページのフィールド</a> 」(400 ページ) を参照してください。
実行中のタスク	[実行中のタスク]ページが開きます。このページで、実行中のタスクをすべて表示できます。詳細については、「 <a href="#">[実行中のタスク]ページのフィールド</a> 」(402 ページ) を参照してください。
最近のタスク	[最近のタスク]ページが開きます。このページでは、最近のすべてのタスクを確認できます。詳細については、「 <a href="#">[最近のタスク]ページのフィールド</a> 」(404 ページ) を参照してください。
タスクの表示のチェックボックス	<p>タスクの承認を受ける必要がある場合は、表示オプションを選択できます。</p> <ul style="list-style-type: none"> <li>• 承認済み</li> <li>• 未承認</li> <li>• 承認を待機中</li> <li>• 無効化</li> <li>• ドラフト</li> <li>• 承認は不要</li> </ul>
チェックボックス	左側のチェックボックスを使用してタスクを削除できます。タスクを選択したら、[アクション]ドロップダウンメニューをクリックし、[削除]をクリックします。横の[選択]ドロップダウンメニューにより、すべてのタスクを選択または削除できます。
スケジュール日	タスクが作成された日時を表示します。
承認期限	該当する場合は、タスクの承認期限となる日時を表示します。タスクが承認期限までに承認されない場合、ステータスが「未承認」に設定されます（ <b>注意</b> ：承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます）。

フィールド	説明/アクション
タスク名	タスク名を表示します。タスクをクリックすると、[タスクの詳細]ページが開きます。詳細については、「 <a href="#">タスクとは</a> 」(277 ページ) を参照してください。
承認のステータス	<p>該当する場合は、タスクの承認ステータスを表示します。承認ステータスは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。次に示す承認のステータスがあります。</p> <ul style="list-style-type: none"> <li>承認を待機中</li> <li>承認済み</li> <li>未承認</li> <li>無効化</li> <li>承認は不要</li> </ul>
タスクのステータス	<p>タスクのステータスを表示します。次に示すステータスがあります。</p> <ul style="list-style-type: none"> <li>警告：すべてのタスクが失敗していなくても、グループタスクの一部のサブタスクが失敗しています。</li> <li>ドラフト：ドラフトステータスの場合、NAはタスクを実行せず、また承認を受けるためにタスクが送信されることはありません。</li> <li>重複：同一のタスクがすでに実行されているため、タスクは開始されませんでした。</li> <li>失敗：タスクは失敗しました。</li> <li>一時停止：他のユーザによりタスクが一時停止されました。タスクは、予定時刻になるまで実行されません。</li> <li>保留：タスクはキューに送られ、予定時刻になるまで待機します。</li> <li>実行中：タスクは開始しましたが、まだ終了していません。</li> <li>スキップ：タスクはエラー（たとえば、不正な権限や非管理デバイスなど）のためにスキップされました。</li> <li>成功：タスクは成功しました。</li> <li>待機中：予定時刻になりましたが、「最大同時タスク」制限に達したため、タスクは待機中です。</li> </ul>
優先度	タスクの優先度を表示します。タスクの優先度レベルは1～5であり、1が最も高いタスク優先度レベルです。詳細については、「 <a href="#">タスクの予定</a> 」(278 ページ) を参照してください。
タスクタイプ	<p>次のようなタスクタイプを表示します。</p> <ul style="list-style-type: none"> <li>パスワードの配布</li> <li>構成を配布</li> <li>ドライバの検出</li> <li>デバイスのリポート</li> <li>スナップショットの取得</li> <li>スタートアップとランニングの同期</li> </ul> <p>タスクの全リストについては、「<a href="#">タスクとは</a>」(277 ページ) を参照してください。（<b>注意</b>：マルチタスクプロジェクトタスクは、[自分のタスク]結果ページに表示される場合とされない場合があります。表示されるかどうかは、マルチタスクプロジェクトのタスクに上記のタスクタイプの1つがサブタスクとして含まれているかどうかによって決まります）。</p>

フィールド	説明/アクション
アクション	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"><li>• 削除：タスクを削除できます。</li><li>• 一時停止：タスクを一時停止し、その予定された時刻に実行されないようにします（<b>注意</b>：タスクを再開する場合は、[再開]を選択します）。</li><li>• 直ちに実行：できるだけすぐにタスクを実行します。同時タスクの最大数に到達していない場合は、タスクが直ちに実行されます。</li><li>• 編集：[タスクを編集]ページが開きます。</li></ul>
1ページに表示する 結果の数	ドロップダウンメニューから、ページあたりの表示項目数を設定できます。デフォルトでは25です。

## 予定されたタスクの表示

キュー内にある、まだ実行されていない予定タスクを表示するには、[タスク]メニューバーの[予定タスク]をクリックします。[予定タスク]ページが開きます。

**注意：** [タスク]ページのリフレッシュ間隔を変更するには、[管理]メニューバーから[システム管理設定]を選択して、[ユーザインターフェイス]をクリックします。[ユーザインターフェイス]ページで[その他]セクションにスクロールダウンして、[タスク]ページのリフレッシュ間隔を入力します。

## [予定タスク]ページのフィールド

フィールド	説明/アクション
自分のタスク	[自分のタスク]ページが開きます。詳細については、「 <a href="#">[自分のタスク]ページのフィールド</a> 」(397 ページ)を参照してください。
タスクテンプレート	[タスクテンプレート]ページが開きます。詳細については、「 <a href="#">タスクテンプレート</a> 」(280 ページ)を参照してください。
自分のドラフト	[自分のドラフト]ページが開きます。詳細については、「 <a href="#">[自分のタスク]ページのフィールド</a> 」(397 ページ)を参照してください。
承認の要求	タスク承認を受ける必要がある場合は、[承認の要求]ページが開きます。このページでは、現在ログインしているユーザによる承認を必要とするタスクを確認できます。詳細については、「 <a href="#">承認の要求</a> 」(670 ページ)を参照してください。
実行中のタスク	[実行中のタスク]ページが開きます。詳細については、「 <a href="#">[実行中のタスク]ページのフィールド</a> 」(402 ページ)を参照してください。
最近のタスク	[最近のタスク]ページが開きます。詳細については、「 <a href="#">[最近のタスク]ページのフィールド</a> 」(404 ページ)を参照してください。
現在の作業グループ	現在の作業グループ名を表示します。ドロップダウンメニューから別のグループを選択して、[リフレッシュ]ボタンをクリックします。
[子タスクを表示]	オンにすると、子タスクが表示されます
チェックボックス	左側のチェックボックスで、予定されたタスクを削除できます。タスクを選択したら、[アクション]ドロップダウンメニューをクリックし、[削除]をクリックします。横の[選択]ドロップダウンメニューにより、すべてのタスクを選択または削除できます。
スケジュール日	NAがタスクを実行する予定の日付と時刻を表示します。
タスク名	タスク名を表示します。
ホスト/グループ	タスクに関連するネットワークデバイスのホスト名またはグループ名を表示します。リンクをクリックすると、[デバイス情報]ページが開きます。このページで、グループ内のデバイスの基本情報を表示できます。



フィールド	説明/アクション
タスクのステータス	<p>次のようにタスクのステータスを表示します。</p> <ul style="list-style-type: none"> <li>• 保留：タスクはキューにあります。実行されていません。</li> <li>• 一時停止：ポーリングは一時停止しています。ポーリングを再開するには、「resume polling」というCLIコマンドを入力します。</li> <li>• ドラフト：タスクはドラフトモードになっており、実行されません。</li> </ul> <p>タスクのステータスの全リストについては、「<a href="#">[タスク情報] ページのフィールド</a>」(406 ページ) を参照してください。</p>
優先度	<p>タスクの優先度を表示します。タスクの優先度レベルは1～5であり、1が最も高いタスク優先度レベルです。詳細については、「<a href="#">タスクの予定</a>」(278 ページ) を参照してください。</p>
スケジュール作成者	<p>タスクをスケジューリングしたユーザ（またはタスクを最後に変更したユーザ）のログイン名を表示します。</p>
コメント	<p>保留タスクについてのコメントを表示します。</p>
アクション	<p>[保留タスク] テーブルの各エントリに対して、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>• 削除：タスクが削除されます。</li> <li>• 一時停止：タスクを一時停止し、その予定された時刻に実行されないようにします（<b>注意</b>：タスクを再開する場合は、[再開]を選択します）。</li> <li>• 直ちに実行：できるだけすぐにタスクを実行します。同時タスクの最大数に到達していない場合は、タスクが直ちに実行されます。</li> <li>• 編集：<a href="#">[タスクを編集]</a> ページが開きます。このページで、繰り返しているタスク、またはまだ実行していないタスクについて、編集や再実行ができます。</li> <li>• テンプレートの作成：<a href="#">[タスクテンプレート]</a> ページが開きます。このページでは、タスク定義を保存できるようになり、いちから作業を始めなくても、新しいタスクまたは既存のタスクを容易に構成および実行できます。詳細については、「<a href="#">タスクテンプレート</a>」(280 ページ) を参照してください。</li> </ul>
1ページに表示する結果の数	<p>ドロップダウンメニューから、ページあたりの表示項目数を設定できます。デフォルト値は25です。</p>

## 実行中のタスクの表示

実行中のタスクを表示するには、[タスク]メニューバーの[実行中のタスク]をクリックします。[実行中のタスク]ページが開きます。

**注意：** [タスク]ページのリフレッシュ間隔を変更するには、[管理]メニューバーから[システム管理設定]を選択して、[ユーザインターフェイス]をクリックします。[ユーザインターフェイス]ページで[その他]セクションにスクロールダウンして、[タスク]ページのリフレッシュ間隔を入力します。

## [実行中のタスク]ページのフィールド

フィールド	説明/アクション
自分のタスク	[自分のタスク]ページが開きます。詳細については、「 <a href="#">[自分のタスク]ページのフィールド</a> 」(397 ページ) を参照してください。
自分のドラフト	[自分のドラフト]ページが開きます。詳細については、「 <a href="#">[自分のタスク]ページのフィールド</a> 」(397 ページ) を参照してください。
承認の要求	[承認の要求]ページが開きます。このページで、現在のログインユーザによる承認が必要なタスクを表示できます。詳細については、「 <a href="#">承認の要求</a> 」(670 ページ) を参照してください。
予定タスク	[予定タスク]ページが開きます。詳細については、「 <a href="#">[予定タスク]ページのフィールド</a> 」(400 ページ) を参照してください。
最近のタスク	[最近のタスク]ページが開きます。詳細については、「 <a href="#">[最近のタスク]ページのフィールド</a> 」(404 ページ) を参照してください。
現在の作業グループ	現在の作業グループを表示します。[Ctrl]キーを押しながらグループをクリックして、複数のグループを選択または選択解除します。
子／親タスクのみを表示	オンにすると、子タスクと親タスクのみが表示されます。
このページを 60 秒ごとにリフレッシュします。	表示を 60 秒ごとにリフレッシュさせたくない場合は、このチェックボックスをオフにします。この値の設定の詳細については、「 <a href="#">[ユーザインターフェイス]ページのフィールド</a> 」(61 ページ) を参照してください。
チェックボックス	左側のチェックボックスを使用してタスクを削除できます。タスクを選択したら、[アクション]ドロップダウンメニューをクリックし、[削除]をクリックします。横の[選択]ドロップダウンメニューにより、すべてのタスクを選択または削除できます。
開始日	NAがタスクの実行を開始した日付と時刻を表示します。
タスク名	タスクタイプを表示します。
ホスト/グループ	タスクに関連するネットワークデバイスのホスト名またはグループ名を表示します。リンクをクリックすると、[デバイス情報]ページが開きます。このページで、グループ内のデバイスの基本情報を表示できます。
タスクのステータス	タスク（実行中）のステータスを表示します。同時タスクの最大数に達している場合は、タスクは別のタスクが終了するまで待機します。そのため、[実行中のタスク]ページでは、「タスクが見つかりませんでした。」を返します（ <b>注意：</b> 親タスクグループが設定に含まれていないため、タスク数が最大同時タスクの値を超える場合があります）。

フィールド	説明/アクション
優先度	タスクの優先度レベルを表示します。タスク優先度の設定の詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
スケジュール作成者	タスクをスケジュールリングしたユーザ（またはタスクを最後に変更したユーザ）のログイン名を表示します。
コメント	保留タスクについてのコメントを表示します。
アクション	<p>[実行中のタスク]テーブルの各エントリに対して、次のアクションを選択できます。</p> <ul style="list-style-type: none"><li>• 編集：[タスクを編集]ページが開き、タスクを編集できます。</li><li>• 詳細：[タスク情報]ページが開きます。このページでタスクの詳細を表示できます。</li><li>• キャンセル：タスクを削除できます。</li><li>• 優先度を上げる：タスク優先度を上げることができます。[優先度を上げる]オプションをクリックした時点で、当該タスクの優先度レベルが設定可能な権限の中で最も高い優先度レベルになっていた場合、このオプションをクリックしてもタスクの優先度レベルは変更されません。詳細については、「<a href="#">タスクの予定</a>」(278ページ)を参照してください。</li><li>• 優先度を下げる：タスク優先度レベルを下げるができます。</li></ul>

## 最近のタスクの表示

[最近のタスク]を表示するには、[タスク]メニューバーから[最近のタスク]をクリックします。[最近のタスク]ページが開きます。[最近のタスク]ページでは、タスクのステータスにかかわらず、最近のタスクをすべて表示します。

**注意：**[タスク]ページのリフレッシュ間隔を変更するには、[管理]メニューバーから[システム管理設定]を選択して、[ユーザインターフェイス]をクリックします。[ユーザインターフェイス]ページで[その他]セクションにスクロールダウンして、[タスク]ページのリフレッシュ間隔を入力します。

## [最近のタスク]ページのフィールド

フィールド	説明/アクション
自分のタスク	[自分のタスク]ページが開きます。詳細については、「 <a href="#">[自分のタスク]ページのフィールド</a> 」(397 ページ)を参照してください。
タスクテンプレート	[タスクテンプレート]ページが開きます。詳細については、「 <a href="#">タスクテンプレート</a> 」(280 ページ)を参照してください。
自分のドラフト	[自分のドラフト]ページが開きます。詳細については、「 <a href="#">[自分のタスク]ページのフィールド</a> 」(397 ページ)を参照してください。
承認の要求	[承認の要求]ページが開きます。このページで、現在のログインユーザによる承認が必要なタスクを表示できます。詳細については、「 <a href="#">承認の要求</a> 」(670 ページ)を参照してください。
予定タスク	[予定タスク]ページが開きます。詳細については、「 <a href="#">[予定タスク]ページのフィールド</a> 」(400 ページ)を参照してください。
実行中のタスク	[実行中のタスク]ページが開きます。詳細については、「 <a href="#">[実行中のタスク]ページのフィールド</a> 」(402 ページ)を参照してください。
現在の作業グループ	タスクに関連するネットワークデバイスのグループ名を表示します。[Ctrl] キーを押しながらグループをクリックして、複数のグループを選択または選択解除します。
フィルタの表示	<p>[フィルタを表示]オプションをクリックして、次のフィルタを表示します。</p> <ul style="list-style-type: none"> <li>次の期間のタスクを表示：最近のタスクを表示する期間を選択します。</li> <li>詳細を表示：[詳細を表示]ボックスをクリックして、次に[リフレッシュ]をクリックすると、[最近のタスク]ページに各タスクの詳細を表示します。</li> <li>[子タスクを表示]：オンにすると、子タスクが表示されます。</li> <li>タスクのステータス：表示するタスクのステータスを1つ以上オンにします。</li> </ul> <p>ステータスを変更したら、必ず[リフレッシュ]をクリックしてください。</p>
チェックボックス	左側のチェックボックスを使用してタスクを削除できます。タスクを選択したら、[アクション]ドロップダウンメニューをクリックし、[削除]をクリックします。横の[選択]ドロップダウンメニューにより、すべてのタスクを選択または削除できます。
完了日	NAがタスクの実行を開始した日付と時刻を表示します。
タスク名	タスクタイプを表示します。
ホスト/グループ	タスクに関連するネットワークデバイスのホスト名またはグループ名を表示します。リンクをクリックすると、[デバイス情報]ページが開きます。このページで、グループ内のデバイスの詳細情報を表示できます。

フィールド	説明/アクション
タスクのステータス	<p>次のようにタスクのステータスを表示します。</p> <ul style="list-style-type: none"> <li>• 成功：タスクは成功しました。</li> <li>• 失敗：タスクは失敗しました。</li> <li>• 重複：タスクが別のタスクと重複しました。</li> <li>• スキップ：タスクを実行する時間に同一のタスクが既に実行されていたため、タスクをスキップしました。</li> </ul> <p>タスクのステータスの全リストについては、「<a href="#">[タスク情報] ページのフィールド</a>」(406 ページ) を参照してください。</p>
優先度	<p>タスクの優先度を表示します。タスクの優先度レベルは1～5であり、1が最も高いタスク優先度レベルです。詳細については、「<a href="#">タスクの予定</a>」(278 ページ) を参照してください。</p>
スケジュール作成者	<p>タスクをスケジュールリングしたユーザ（またはタスクを最後に変更したユーザ）のログイン名を表示します。</p>
コメント	<p>タスクについてのコメントを表示します。</p>
アクション	<p>[最近のタスク] テーブルの各タスクに対して、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>• 詳細：[タスク情報] ページが開きます。このページでタスクの詳細を表示できます。</li> <li>• 再実行：[タスクを再実行] ページが開きます。このページでタスクの編集や再実行ができます。（<b>注意</b>：このオプションは、タスクを再実行できる場合のみ表示されます。）</li> <li>• テンプレートの作成：[タスクテンプレート] ページが開きます。このページでは、タスク定義を保存できるようになり、いちから作業を始めなくても、新しいタスクまたは既存のタスクを容易に構成および実行できます。詳細については、「<a href="#">タスクテンプレート</a>」(280 ページ) を参照してください。</li> </ul>
1 ページに表示する結果の数	<p>ドロップダウンメニューから、ページあたりの表示項目数を設定できます。デフォルトでは 25 です。</p>

## [タスク情報]ページのフィールド

[タスク情報]ページには、タスクについて次の詳細な情報が表示されます。

- タスクのステータス
- タスク優先度
- 作成者
- 影響を受けるデバイス
- 継続時間
- 承認情報
- 結果の詳細
- タスク履歴

[タスク情報]ページには、警告または失敗のイベントのより詳細な情報へのリンクも表示されます。タスクは、正常に完了することができても、エラーが含まれている場合があります。たとえば、実行構成を正常に配布することができても、その構成に無効なコマンドが含まれている場合があります。

[タスク情報]ページを開くには：

1. [インベントリ]ページからデバイスを選択します。[デバイス詳細]ページが開きます。
2. [表示]ドロップダウンメニューで、[デバイスタスク]をクリックします。[デバイスタスク]ページが開きます。
3. 詳細な情報を表示させるタスクの[アクション]列にある[詳細]オプションをクリックします。[タスク情報]ページが開きます。

フィールド	説明/アクション
タスクを編集	タスクを編集するためのタスクページが開きます。このリンクは、保留タスクの場合にのみ表示されます。 「 <a href="#">タスクとは</a> 」(277 ページ) を参照してください。
再実行	タスクを再実行するためのタスクページが開きます。このリンクは、完了タスクの場合にのみ表示されます。 「 <a href="#">タスクとは</a> 」(277 ページ) を参照してください。
リストに戻る	[自分のタスク]ページが開きます。「 <a href="#">[自分のタスク]の表示</a> 」(397 ページ) を参照してください。
<b>一般情報</b>	
タスク名	タスク名を表示します。

フィールド	説明/アクション
タスクのステータス	<p>次に示すタスクのステータスを表示します。</p> <ul style="list-style-type: none"> <li>• ドラフト</li> <li>• 重複</li> <li>• 失敗</li> <li>• 一時停止</li> <li>• 保留</li> <li>• 要求（<b>注意</b>：要求とは、タスクが承認を待っていることを示します。「<b>タスクの承認</b>」（672 ページ）を参照してください。）</li> <li>• 実行中</li> <li>• スキップ</li> <li>• 成功</li> <li>• 同期（<b>注意</b>：NAは通常、スレッドを作成し、バックグラウンドで非同期に実行させることによりタスクを実行します。CLIおよびAPIによって同期タスクが可能になり、この場合タスクは、コマンドが完了するまで現在のスレッドとコマンドブロックで実行されます）。</li> <li>• 待機中</li> <li>• 警告</li> </ul> <p><b>注意</b>：警告があった場合でも、マルチタスクプロジェクトでは処理を続行します。警告ステータスは親タスクで示されます。</p>
コメント	タスクについてのコメントを表示します。
作成者	タスクをスケジュールしたユーザ名またはプロセスを表示します。
優先度	タスクの優先度を表示します。タスクの優先度レベルは1～5であり、1が最も高いタスク優先度レベルです。詳細については、「 <b>タスクの予定</b> 」（278 ページ）を参照してください。
作成日	タスクが作成された日時を表示します。
影響を受けるデバイス	影響を受けるデバイスのホスト名またはIPアドレスを表示します。
スケジュール日	タスクの実行予定日時を表示します。
開始日	タスクの開始日を表示します。
完了日	タスクの完了日を表示します。
継続時間	タスクの継続時間を表示します。
反復タイプ	たとえば、非反復などの反復タイプを表示します。
親タスク	親タスクを表示します。
<b>承認情報</b>	
承認者	タスクの承認者リストを表示します。
承認のステータス	タスクの承認ステータスを表示します。
優先度	タスクの優先度を表示します。

フィールド	説明/アクション
承認者	タスクの承認期限となる日時を表示します。
新規コメント	タスクについての追加コメントを入力します。
承認ボタン	[承認]ボタンをクリックしてタスクを承認します。
タスクの詳細を表示	[タスクの表示]へのリンクをクリックすると、[診断履歴]ページが開きます。
<b>追加情報</b>	
結果の詳細	<p>(デバイスタイプに応じて) 自動的に実行された診断を表示します。たとえば、次のような診断があります。</p> <ul style="list-style-type: none"><li>• Diagnostic NA Module Status completed (診断 'NA モジュールのステータス' が完了しました)</li><li>• Diagnostic NA Routing Table completed (診断 'NA ルーティングテーブル' が完了しました)</li><li>• 診断 'NA インターフェイス' が完了しました。</li><li>• 診断 'NA OSPF ネイバー' が完了しました。</li></ul>
<b>タスク履歴</b>	
タスク履歴情報	タスクの実行日時、反復タイプ、およびステータスなどのタスク履歴情報を表示します。



## タスク負荷の表示

[タスク負荷]ページでは、システム内の現在のタスク数を表示します。タスクは3つのカテゴリに分類されます。

- 15分以内に開始予定のタスク
- 実行待機中のタスク
- 現在実行中のタスク

[タスク負荷]ページには、現在のユーザに表示権限がないタスクを含む、システム内のタスクがすべて含まれています。そのため、タスク数が[タスクの検索]ページのタスク数と必ずしも一致しません。

[タスク負荷]ページを表示するには、[タスク]メニューバーから[タスク負荷]をクリックします。[タスク負荷]ページが開きます。([管理]からこのページにアクセスすることもできます。)

## [タスク負荷]ページ

フィールド	説明
タスク開始（15分後）	15分以内に開始する予定のタスク数を表示します。
タスク待機中	待機中のタスク数を表示します。同時タスクの最大数に達している場合は、タスクは別のタスクが終了するまで待機します。
タスク実行中	実行中のタスク数を表示します。



## 第8章：ポリシー保証の管理

### トピックの参照先リスト

トピック	参照先：
はじめに	<a href="#">「はじめに」</a> （412ページ）
ポリシーの作成	<a href="#">「ポリシーの作成」</a> （414ページ）
ポリシーールールの作成	<a href="#">「[ルールの新規作成]ページのフィールド」</a> （420ページ）
ポリシーのインポート/エクスポート	<a href="#">「ポリシーのインポート/エクスポート」</a> （424ページ）
ポリシーの編集	<a href="#">「ポリシーを編集」</a> （425ページ）
適用されるポリシーの表示	<a href="#">「適用されるポリシーの表示」</a> （429ページ）
ポリシーアクティビティの表示	<a href="#">「ポリシーアクティビティの表示」</a> （430ページ）
ポリシー準拠の表示	<a href="#">「ポリシー準拠の表示」</a> （431ページ）
新規準拠の追加	<a href="#">「新規ソフトウェアレベルの追加」</a> （433ページ）
ポリシー準拠のテスト	<a href="#">「ポリシー準拠のテスト」</a> （439ページ）

## はじめに

HP Network Automation (NA) Policy Manager では、標準、またはベストプラクティスを確立し、ネットワークがセキュリティ、信頼性、および品質の目標を満たすことを保証します。ポリシー施行能力と統合された修正機能を提供することで、NAは、デバイスと構成が定義されたベストプラクティスに一致することを検証する困難なタスク、およびデバイスをベストプラクティスに準拠する状態に戻すのに必要となる修正手順を自動化します。

NA Policy Managerは、費用効果が高い、効率的な方法で、PCIやSarbanes-Oxley (SOX)などの法令遵守要件を満たすための重要な役割を果たします。

このセクションでは、次の用語を使用します。

- **ポリシー**：ポリシーとはデバイスの構成と実行時ステータスをテストする、ルールの集合です。
- **ルール**：ルールとは、以下の1項目以上を検証する自動テストのことです。
  - － 特定の構成設定
  - － 特定のデータモデル要素
  - － デバイスの実行時ステータス（診断）
  - － デバイスで動作しているソフトウェアのバージョン
- **診断**：診断とは、デバイスの構成ファイルではキャプチャされないデバイスに関する情報を収集するための、デバイス上で実行するコマンドです。Cisco ルータ上での診断の一例として、Show NTP Status コマンドの出力が挙げられます。診断リストについては、「[表示メニューオプション](#)」(201 ページ) セクションの[診断]フィールドを参照してください。
- **ルール例外**：ルール例外とはルールの一部です。ただし、その目的は元のルールに一致するデバイス構成内のテキストから、ルール例外に一致するテキストを除外することにあります。
- **自動修正**：デバイスがポリシールールに非準拠である場合に自動的に実行される、事前定義されたスクリプトです。

## NA Policy Managerの動作方法

NA Policy Managerの使用を開始するには、先にNA内で、デバイスが準拠する必要があるベストプラクティス標準を定義するためのポリシーを作成します。次に、ポリシーをテストしてポリシーが違反を正しく捕らえることを検証します。最後に、特定デバイスグループ（またはデバイスグループのセット）に、各ポリシーを割り当てます。これにより、NAはデバイスが定義されたポリシーに一致することを自動的に検証します。

デバイスが変更されるたび、つまり、デバイスがリロードされたり構成変更が発生した場合、NAはデバイスとそのデバイスグループに割り当てられたポリシーとを検証します。デバイスがポリシー確認に失格すると、デバイスは非準拠としてマークされます。デバイス（またはデバイスグループ）への変更が非準拠である場合、NA Policy Managerはイベントを生成し、通知ルールを実行します。これにより、準拠とネットワーク可用性の両方を維持しながら、非準拠の変更を修正できます。

管理している全デバイスのポリシー準拠ステータスをまとめることができます。これによって、ポリシー準拠ステータスについてリスク評価しているスナップショットを提供でき、ただちにハイリスクな構成とソフトウェアレベル違反を特定して解決できます。

NAがデバイスに対してポリシー確認を実行するとき、NAは各ルールを処理し、ルールがデバイスに適用されるかどうかを確認します。ルールが適用される場合、デバイスはルールと照らし合わせてテストされます。ルールが適用されない場合、そのルールはそのデバイスをスキップします。

ルールは以下の2通りの方法で適用できます。

- ルールがデバイスファミリに固有の場合。デバイスがCisco IOSやJuniper JunOSなどの特定のドライバを使用している場合、ルールはそのデバイスに対してのみ確認されます。たとえば、Cisco IOSドライバを使用するデバイスに適用するルールを作成する場合、ルールはExtremeスイッチに対して検証されることはありません。
- ルールはデバイスファミリに対して中立です。ルールは正規化されたデータモデル内の検証基準であるため、デバイスファミリに固有ではありません。デフォルトでは、NAは構成とデバイス情報を、そのデータモデルの正規化された要素へと解析します。これには、モデル番号やホスト名、場所などのデバイス属性が含まれます。このデータはすべてのデバイスファミリで正規化されるため、このデータはデバイスファミリに固有ではありません。このため、ルールをすべてのデバイスファミリに適用でき、結果としてネットワーク内の各デバイスファミリに固有のルールを作成する必要がなくなります。

**注意：**すべてのデバイスファミリにルールを設定する場合、そのルール内の構成、または構成ブロック基準は使用できません。構成および構成ブロックフォーマットは、デバイスファミリ固有のもので、構成、または構成ブロック基準を使用し、すべてのデバイスファミリをサポートするルールを設定すると、NAは各デバイス構成内で構成テキストの検索を試行するため、数多くの失敗が発生します。

構成テキストを確認するポリシーを実行すると、デフォルトでNAは先行するすべての空白を削除します。したがって、先行する空白が存在する可能性がある構成テキストを定義する場合は、必ず空白文字を検出する正規表現を作成するようにしてください。

たとえば、検索対象となる構成テキストが以下の場合（行の先頭に2つの空白があるのに注意してください）：

```
description this yields unexpected results
```

通常、ポリシーが検索する構成テキストブロックを定義するために以下の正規表現を使用します。

```
\s+description.*
```

**注意：**\sは、任意の空白文字に一致する正規表現です。ただし、構成に対してポリシーを実行すると、構成はポリシーに失敗します。ポリシールール内の構成テキスト定義から\sを削除すると、デフォルトでNAによって構成テキストから先行する空白が削除されるため、構成はポリシーをパスします。

## ポリシーの作成

ポリシールールを作成するには、先にポリシーを作成する必要があります。ポリシーを作成するには、[ポリシー]のメニューバーで[ポリシーリスト]をクリックします。[ポリシー]ページが開きます。

NAには、[NSAルータセキュリティベストプラクティス]ポリシーなど、複数のデフォルトポリシーが備わっています。構成できるポリシーの例を次に示します。

- デバイスグループ内の全構成は、定義されたアクセスリスト110が必要です。
- すべての高速イーサネットインターフェイスは、自動ネゴシエートが設定されている通信モードが必要です。
- すべてのボーダルータには、特定のDNSサーバが必要です。

**注意：**[ポリシーの新規作成]オプションをクリックして、[ポリシーの新規作成]ページへ直接ナビゲートできます。また、[ポリシー]ページに既存のポリシーを表示して、このページの最上部にある[ポリシーの新規作成]リンクをクリックすることもできます。

## [ポリシー]ページのフィールド

フィールド	説明
ポリシーの新規作成	[ポリシーの新規作成]ページが開きます。そのページで、新しい構成のポリシーを作成できます。詳細については、「 <a href="#">[ポリシーの新規作成]ページのフィールド</a> 」(417ページ)を参照してください。
ポリシー準拠の確認	[ポリシー準拠の確認]タスクページが開きます。そのページで、ポリシー準拠を確認できます。詳細については、「 <a href="#">[ポリシー準拠の確認]タスクページのフィールド</a> 」(372ページ)を参照してください。(注意: メニューバーの[ポリシー - ポリシータスク]の下にある[ポリシー準拠の確認]をクリックして、[ポリシー準拠の確認]ページへのナビゲートもできます。)
インポートとエクスポート	[ポリシーのインポート/エクスポート]ページが開きます。そのページで、構成前の構成ポリシーをインポートしたり、構成ポリシーをファイルへエクスポートできます。詳細については、「 <a href="#">ポリシーのインポート/エクスポート</a> 」(424ページ)を参照してください。(注意: [ポリシーのインポート/エクスポート]オプションをクリックして、[ポリシーのインポート/エクスポート]ページへのナビゲートもできます。)
[ポリシータグ]ドロップダウンメニュー	ポリシータグを選択できます。これにより、ポリシーを簡単にグループ化できます。
チェックボックス	<p>左側のチェックボックスを使用して、構成ポリシーを管理できます。ポリシーを選択して、[アクション]のドロップダウンメニューをクリックし、次のいずれかをクリックします。</p> <ul style="list-style-type: none"> <li>• アクティブ化: 選択したポリシーに対して、準拠構成を確認するようにNAに指示します。</li> <li>• 非アクティブ化: 選択したポリシーに対して、準拠構成を確認しないようにNAに指示します。</li> <li>• 一括編集: ポリシーを一括編集できます。これにより、ポリシーステータス（アクティブ、または非アクティブ）、およびポリシーの適用先となるデバイスグループ（適用範囲）を容易に変更できます。</li> <li>• 削除: 選択したデバイスが削除されます。</li> </ul> <p>隣接する[選択]ドロップダウンメニューで、全ポリシーを選択（または選択解除）できます。</p>
ポリシー名	ポリシー名を表示します。
ステータス	アクティブ、または非アクティブの値をとるポリシーのステータスを表示します。
パーティション	セキュリティや業務上の理由でパーティションを作成した場合、特定パーティションのポリシーをパーティションできます。ポリシーを特定のパーティション内の特定ユーザに加え、すべてのパーティション内のすべてのユーザで共有するように構成できます。ポリシーがすべてのパーティションで利用できる場合、[共有]と表示されます。パーティションの作成の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」(148ページ)を参照してください。
CVE	CVE（Common Vulnerabilities and Exposures）名を表示します。CVE とは、セキュリティ問題に関する脆弱性やその他の情報に付けられた標準名のリストです。
作成日	ポリシーが作成された日付が表示されます。

フィールド	説明
アクション	<p>次のアクションを選択できます。</p> <ul style="list-style-type: none"><li>• 表示と編集 : [ポリシーを編集] ページが開きます。そのページで、構成ポリシーを編集できます。詳細については、「<a href="#">ポリシーを編集</a>」(425 ページ) を参照してください。</li><li>• テスト : [ポリシーをテスト] ページが開きます。そのページで、デバイスやデバイスグループに対して、ポリシーのテストができます。(注意 : ポリシーにパフォーマンス上の問題となるルールが含まれる場合、テストが可能かどうかを問わず、各ポリシーの隣に[テスト] オプションが表示されます詳細については、「<a href="#">[ポリシーをテスト] ページのフィールド</a>」(439 ページ) を参照してください。)</li></ul>



## [ポリシーの新規作成]ページのフィールド

[ポリシーの新規作成]ページを開くには、[ポリシー]メニューバーの[ポリシーの新規作成]をクリックします。  
[ポリシーの新規作成]ページが開きます。

フィールド	説明/アクション
<b>ポリシーの新規作成</b>	
ポリシー名	ポリシー名を入力します。ポリシーとは、デバイスまたはデバイスグループに適用するルールのセットのことです。
ポリシーの説明	ポリシーの説明を入力します。
パーティション	ドロップダウンメニューからパーティションを選択します。(注意：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。) 一般的に、パーティションとは一意のIPアドレスを持つデバイスのグループです。単一のNAコアで複数のパーティションを管理できます。NA コアはNA サーバのインスツールコンポーネントの1つで、単一の管理エンジン、関連サービス、および単一のデータベースからなります。パーティションの作成の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」(148 ページ)を参照してください。
ポリシータグ	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• 汎用：ポリシーにタグ付けしない場合、このタグを汎用ポリシーとして使用します。</li> <li>• 既存：ドロップダウンメニューからタグを選択します。</li> <li>• 新規作成：タグ名を入力して新規ポリシータグを作成します。</li> </ul>
範囲	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• デバイスグループポリシーの適用先を選択：デバイスセクタを使用してグループを選択します。デバイスセクタの使用の詳細については、「<a href="#">デバイスセクタ</a>」(142 ページ)を参照してください。</li> <li>• フィルタを使用して、動的ポリシー範囲を定義：ポリシー範囲には、ポリシーが影響を及ぼす可能性があるデバイスが含まれます。ポリシーに指定したデバイスを含むデバイスファミリに影響するポリシールールがある場合、ポリシー範囲はそのデバイスにのみ影響します。ポリシーを定義する場合、動的グループを定義する方法で歩シリー範囲を定義できます。そのため、ポリシーとともにプライベートな動的グループを作成できます。(動的グループの作成の詳細については、「<a href="#">動的デバイスグループ</a>」(140 ページ)を参照してください)。</li> </ul>
<b>検索条件</b> (動的ポリシー範囲を定義するためにフィルタを使用する場合)	
検索条件は[条件を追加]ドロップダウンメニューから選択するたびに、[検索条件]セクションに表示されます。このセクションでは、「含む」、「一致する」、または「等しい」といった演算子を選択したり、検索する情報を入力したりできます。定義済みの条件を削除する場合は、検索条件インデックス文字の横に表示されている「X」をクリックします。	
条件を追加	ドロップダウンメニューから検索条件を1つ以上選択します。選択可能な条件は次のとおりです。 <ul style="list-style-type: none"> <li>• 構成テキスト</li> <li>• デバイスIP</li> <li>• デバイスステータス</li> <li>• ホスト名</li> <li>• パスワードルール</li> </ul>

フィールド	説明/アクション
<b>ブール式</b>	
式	デフォルトでは、定義済みの条件インデックス文字がブール式「and」で結合されて表示されます。たとえば、3つの検索条件が定義されている場合、式は <i>A and B and C</i> のようになります。ブール式は、必要に応じて編集できます。[式をリセット] ボタンをクリックすると、式がデフォルト値にリセットされます（ <b>注意</b> ：ブール演算子は小文字で入力する必要があります。また、条件の最大数は10です）。
<b>デバイスグループで検索を絞り込み</b>	
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• 選択グループ内のいずれか（デフォルト）</li> <li>• 選択グループのすべて</li> <li>• 選択グループになし</li> </ul> <p><b>注意</b>：[Shift] キーとクリックを使用すると、複数のデバイスグループを選択または選択解除できます。デバイスグループを選択しない場合、検索時にデバイスグループフィルタが失われます。</p>
<b>ビューとパーティションで検索を絞り込み</b> （この情報は、ビューとパーティションを構成した場合のみ表示されます。詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」（148ページ）を参照してください）。	
例外とするデバイス	右側のボックスにデバイスのIPアドレスまたはホスト名を入力して、[例外を追加 <<] をクリックします。デバイスを削除するには、左側のボックスにあるデバイスのIPアドレスまたはホスト名を選択して、[例外を削除] をクリックします。
ポリシールール	ポリシールールテーブルでは、ポリシーが適用されるすべてのルールを表示します。ポリシーは、このポリシー用に選択した保存されたデバイスそれぞれに対し、すべての構成ルールを適用します。ルールは順不同で適用されます。
ルールの新規作成ボタン	このポリシーの新規ルールを作成するには、[ルールの新規作成] ボタンをクリックします。[ルールの新規作成] ページが開きます。詳細については、「 <a href="#">[ルールの新規作成] ページのフィールド</a> 」（420ページ）を参照してください。
詳細な説明	ポリシーの詳細な説明を入力します。ポリシーが表示されるリストには、ポリシーについての簡単な説明が表示されます。このフィールドでは、ポリシーの詳細な説明を追加できます。
ポリシーのステータス	<p>次のオプションから1つをクリックします。</p> <ul style="list-style-type: none"> <li>• アクティブ：ポリシーをアクティブにします（デフォルト）。</li> <li>• 非アクティブ：ポリシーを非アクティブにします。</li> </ul>
<b>追加ポリシーフィールド</b> （これらのフィールドは、ポリシーがHP Security and Compliance Serviceに基づく場合に自動的に入力されます。）	
CVE	CVE（Common Vulnerabilities and Exposures）名を入力します。CVE とは、セキュリティ問題に関する脆弱性やその他の情報に付けられた標準名のリストです。（詳細については、 <a href="http://www.cve.mitre.org">www.cve.mitre.org</a> を参照してください）。
ベンダー諮問URL	脆弱性に関する諮問情報の外部参照のURLを入力します。ベンダー諮問URLやベンダーソリューションURLを含めてポリシーを作成する場合、URLの先頭には「http://」を付ける必要があります。そうしないと、リンクがブラウザによって正しく解釈されないことがあります。[URL] フィールドを空白にすると、リンクを選択したときに、NAホームページが開くことがあります。

フィールド	説明/アクション
ベンダーソリューション URL	脆弱性への実行可能なソリューションの詳細に関する、外部参照の URL を入力します。
開示日	ソフトウェアの脆弱性が警告された日付を <i>yyyy-MM-dd</i> フォーマットで入力します。
解決策	解決策の詳細な情報を入力します。

終了時に、必ず[保存]をクリックしてください。

## [ルールの新規作成]ページのフィールド

[ポリシーの新規作成]ページの[ルールの新規作成]ボタンをクリックすると、[ルールの新規作成]ページが開きます。ルールは以下の2通りの方法で適用できます。

- ルールがデバイスファミリに固有の場合。デバイスがCisco IOSやJuniper JunOSなどの特定のドライバを使用している場合、ルールはそのデバイスに対してのみ確認されます。たとえば、Cisco IOSドライバを使用するデバイスに適用するルールを作成する場合、ルールはExtremeスイッチに対して検証されることはありません。
- ルールはデバイスファミリに対して中立です。ルールは正規化されたデータモデル内の検証基準であるため、デバイスファミリに固有ではありません。デフォルトでは、NAは構成とデバイス情報を、そのデータモデルの正規化された要素へと解析します。これには、モデル番号やホスト名、場所などのデバイス属性が含まれます。このデータはすべてのデバイスファミリで正規化されるため、このデータはデバイスファミリに固有ではありません。このため、ルールをすべてのデバイスファミリに適用でき、結果としてネットワーク内の各デバイスファミリに固有のルールを作成する必要がなくなります。

フィールド	説明/アクション
<b>ルールの新規作成</b>	
ルール名	ルール名を入力します。
ルールタイプ	<p>ルールタイプを選択します。たとえば、構成テキスト、または選択したデバイスの構成テキストからブルされたデータモデル要素を基に、ルールを定義できます。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• 構成：選択すると、構成ルールは、選択したデバイスの構成テキストが現在の構成ルールに準拠しているかどうかを確認します。</li> <li>• 診断：選択すると、ルールは、選択したデバイスの診断テキストが現在の診断ルールに準拠しているかどうかを確認します。診断テキストは診断を実行することで生成されます。詳細については、「<a href="#">[診断の実行] タスクページのフィールド</a>」(310 ページ)を参照してください。(注意：ポリシールールの基になる診断の名前を変更するときには注意してください。ポリシールールの基になる診断の名前を変更する場合、ポリシールールの条件が失われます。)</li> <li>• ソフトウェア：選択すると、ルールは、選択したデバイスが現在のソフトウェアルールに準拠しているかどうかを確認します。詳細については、「<a href="#">ソフトウェアレベルレポートのフィールド</a>」(614 ページ)を参照してください。</li> </ul>
ルールの説明	ルールの説明を入力します。
<b>以下のドライバを持つデバイスに適用されます</b>	
全デバイスファミリ	<p>すべてのデバイスファミリにルールを適用する場合、このラジオボタンをクリックします。デフォルトでは、NAは構成とデバイス情報を、そのデータモデルの正規化された要素へと解析します。これには、モデル番号やホスト名、場所などのデバイス属性が含まれます。このデータはすべてのデバイスファミリで正規化されるため、このデータはデバイスファミリに固有ではありません。</p> <p><b>注意：</b>すべてのデバイスファミリにルールを設定する場合、そのルール内の構成、または構成ブロック基準は使用できません。構成および構成ブロックフォーマットは、デバイスファミリ固有のものです。構成、または構成ブロック基準を使用し、すべてのデバイスファミリをサポートするルールを設定すると、NAは各デバイス構成内で構成テキストの検索を試行するため、数多くの失敗が発生します。</p>

フィールド	説明/アクション
デバイスファミリ	<p>ルールを適用するデバイスファミリを、ドロップダウンメニューから選択します。たとえば、BayStack、Cisco IOS、Nortel ASF などです。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 適用できる全ドライバ：オンの場合（デフォルト）、NAは適用できる全ドライバを選択します。ルールが適用されるのは、特定のドライバに割り当てられたデバイスの構成のみです。</li> <li>• 特定のドライバの選択：オンの場合は、リストから1つまたは複数のドライバを選択します。構成ルールが適用されるのは、特定のドライバに割り当てられたデバイスの構成のみです。</li> </ul>
テキストブロックを定義	<p>構成ブロック条件が使用するようにテキストブロックを設定できます。[テキストブロックを定義]オプションを選択すると、[ブロック開始パターン]、と[ブロック終了パターン]フィールドが表示されます。これらは、タイプの条件「構成ブロック」が追加されている場合のみ使用されます。条件は構成ファイルにある特定のテキストのブロックに適用されます。たとえば、Cisco IOS デバイス内のシングルインターフェイスなどです。構成ファイルにある特定のブロックの各インスタンスに、ルールを適用する場合は、ブロック開始パターン（たとえば、「interface.*」）とブロック終了パターン（たとえば、「!」）を入力します。</p>
テキストブロックを定義 (続き)	<p>ブロックの開始パターンと終了パターンによって抽出される構成テキストには、開始パターンと終了パターンに一致する行が含まれます。したがって、開始パターンと終了パターンの間にある行ばかりでなく開始パターンと終了パターンに一致する行も構成ブロック条件と一致します。たとえば、次のブロック開始パターンと終了パターンがあるとします。</p> <pre> ブロック開始：interface .* ブロック終了：!</pre> <p>構成テキストには以下の行が含まれます。</p> <pre> ... no service pad service timestamps log uptime service timestamps log uptime interface FastEthernet0/7 description testfor bug 145762 speed 100 duplex full ! ip default-gateway 10.255.1.1 ip http server ...</pre> <p>構成ブロック条件の一致で使用される構成の抽出部分は以下のとおりです。</p> <pre> interface FastEthernet0/7 description testfor bug 145762 speed 100 duplex full !</pre> <p>開始パターンと終了パターンに一致する行、interface FastEthernet0/7 と ! も抽出されるので注意してください。</p>

フィールド	説明/アクション
ルール条件	<p>ドロップダウンメニューから1つまたは複数の条件（「構成ブロック」、「フラッシュメモリ」、「ホスト名」など）を選択します。</p> <ul style="list-style-type: none"> <li>• 正規表現：オンにするとパターンは正規表現になります。オンにしないと、パターンは構成（診断）テキスト、またはデータモデル要素値に一致する文字列になります。</li> <li>• 次を含む必要がある：構成（診断）テキスト、またはデータモデル要素の値がパターンを含む必要があります。</li> <li>• 次を含まない：構成（診断）テキスト、またはデータモデル要素の値がパターンを含まない必要があります。</li> <li>• 次のみを含む必要がある：構成（診断テキスト）、またはデータモデル要素の値がパターンを含む必要がある一方、[ただし次の項目を含む追加行は含めない：] フィールドに指定されているパターンのその他の一致を含まない必要があります。</li> <li>• 行（正しい順序）：オンにすると、パターン行は指定された順番に一致する必要があります。条件パターンの各行は、独立パターンとして判断され、別個に確認されます。このオプションをオンにすると、これらの独立した一致は空白以外の不一致文字を含むことなく、指定された順番に並ぶ必要があります。</li> </ul> <p>「and」と「or」を使用してブール式を作成できるほか、「if-then-else」論理を使用して条件ルールを構成できます。この場合の「else」はオプションです。たとえば、「A」～「E」までの5つの条件を定義する場合、次のようなブール式が作成できます。“<i>if (A and B) then (C or D) else E</i>”。（<b>注意</b>：ブール演算子は小文字で入力する必要があります。また、条件の最大数は10です。）</p> <p>[<a href="#">ヘルプの取得</a>] リンクで、正規表現に関する情報が得られます。[<a href="#">デバイス変数</a>] リンクで、[デバイス変数] ページが開きます。このページには、ポリシールールの定義で利用できるビルトイン変数のリストが記載されています。ポリシールールが確認される際、これらの値が置換されます。</p> <p>[<a href="#">式のリセット</a>] ボタンをクリックすると、式がデフォルト値にリセットされます。</p>
重要度	<p>重要度レベルを選択します。これは、ポリシールールの非準拠リスクレーティングを示します。NAでは、この重要度に基づいて違反をソートできます。たとえば、重要な違反では、[変更管理] システム内のトラブルチケットを自動的に開くことができます。また、情報違反については、デイリーレポート内で特定することができます。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• 情報：一般的に対応を必要としないイベント。</li> <li>• 低：時間的な余裕がある場合に対応を必要とするイベント。</li> <li>• 中：適時に対応が必要なイベント。通常は72時間以内（デフォルト）。</li> <li>• 高：緊急の対応を必要とするイベント（通常は24時間以内）。</li> <li>• 重要：即時の対応を必要とするイベント。</li> </ul>
詳細な説明	<p>ルールの説明を入力します。</p>
ルール例外	<p>該当する場合は、ルール例外のリストを表示します。ルール例外は、ルールの一部です。たとえば、ルール例外は、元のルールに一致するデバイス構成内のテキストから、ルール例外に一致するテキストを除外できます。</p> <p>[ルール例外] を追加するには、[例外の新規作成] リンクをクリックします。[ルール例外の新規作成] ページが開きます。（詳細については、「<a href="#">ルール例外の追加</a>」（428ページ）を参照してください。）</p>

フィールド	説明/アクション
自動修正スクリプト	<p data-bbox="444 241 1463 296">自動修正ポップアップウィンドウは、[ポリシールール]ページのデータにアクセスして、変数マッピングを表示し、サンプルコードを生成し、保存前にスクリプトを検証します。</p> <p data-bbox="444 329 1463 411">自動修正スクリプトを使用することで、違反されたポリシールール内の正規表現パターングループからのデータを参照する、スクリプト内の変数を定義します。(詳細については、「<a href="#">自動修正スクリプトの作成</a>」(581ページ)を参照してください)。</p> <p data-bbox="444 445 1463 527">新規修正スクリプトを作成を追加するには、[自動修正スクリプトの新規作成]リンクをクリックします。自動修正スクリプトポップアップウィンドウには、[コマンドスクリプト]ページが含まれます。自動修正スクリプトを容易に入力するため、次のリンクを選択できます。</p> <ul data-bbox="444 548 1463 793" style="list-style-type: none"> <li>• 変数を表示：正規表現パターンでの変数マッピングが表示されます。これにより、パターンのどの部分が、どの正規表現グループに適用されるかを確認できます。正規表現パターンの強調表示された部分は、左側の変数で参照されます。変数の(.*)の手前のセクションは、@foreachループ変数によって置き換えられます。変数名は正規表現グループを示します。さらに、正規表現グループ0（ゼロ）はパターン全体を表します。</li> <li>• サンプルコードの生成：使用できる変数付きのサンプルテンプレートコードが生成されます。デバイスコマンドを@foreachループに追加する必要があります。デバイスコマンドは、上記の生成された各ループにリストされる変数を参照できます。</li> </ul>

終了時には、[保存]ボタンをクリックしてルールを保存するか、[保存してさらに追加]ボタンをクリックして現在のルールを保存して新規ルールを追加、または[例外の新規作成]リンクをクリックして新規ルール例外を追加できます。

## ポリシーのインポート/エクスポート

定義前のポリシーのインポートや、ポリシーのファイルへのエクスポートが可能です。これにより、簡単にポリシーを共有できます。

**注意：**別の NA アプリケーションサーバからエクスポートしたポリシーをインポートする場合、インポートしたポリシーから参照されるすべての診断の名前を特定します。ターゲットシステムに同じ名前と機能システムの診断が存在する必要があります。

ポリシーのインポートまたはエクスポートをするには、[ポリシー]メニューバーの[ポリシーのインポート/エクスポート]をクリックします。[ポリシーのインポート/エクスポート]ページが開きます。

**注意：**NAは、NA 6.2以降の旧バージョンのポリシーをインポートできます。

## [ポリシーのインポート/エクスポート]ページのフィールド

フィールド	説明/アクション
ポリシーをインポート	インポートするポリシーファイルを入力するか、[参照]ボタンをクリックしてポリシーファイルを検索します。ポリシーファイルが表示されたら、[インポート]ボタンをクリックします。ポリシーが既に存在する場合は、名前を変更するように要求されます。
ポリシーをエクスポート	現在の構成ポリシーのリストを表示します。エクスポートする構成ポリシーをクリックして、次に[エクスポート]ボタンをクリックします。構成ポリシーに関連するデバイスグループはエクスポートされません。また、構成ポリシー例外ルールは、いずれもエクスポートされません。



## ポリシーを編集

ポリシーを編集するには：

1. [ポリシー]メニューバーの[ポリシーリスト]をクリックします。[ポリシー]ページが開きます。
2. 編集するポリシーの[表示と編集]アクションをクリックします。[ポリシーを編集]ページが開きます。終了時に、必ず[保存]をクリックしてください。

## [ポリシーを編集]ページのフィールド

フィールド	説明/アクション
ポリシー名	ポリシー名を表示します。
ポリシーの説明	ポリシーの説明を表示します。
パーティション	ドロップダウンメニューからパーティションを選択します。(注意：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます)。一般的に、パーティションとは一意のIPアドレスを持つデバイスのグループです。単一のNAコアで複数のパーティションを管理できます。NA コアはNA サーバのインストールコンポーネントの一つで、単一の管理エンジン、関連サービス、および単一のデータベースからなります。パーティションの作成の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」(148 ページ)を参照してください。
ポリシータグ	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• 汎用：ポリシーにタグ付けしない場合、このタグを汎用ポリシーとして使用します。</li> <li>• 既存：ドロップダウンメニューから新規ポリシーを選択します。</li> <li>• 新規作成：ポリシーの場所を入力します。</li> </ul>
範囲	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• デバイスグループポリシーの適用先を選択：リストから1つまたは複数のデバイスグループを選択します。[Shift]+クリックまたは[Ctrl]+クリックを使用して、複数のデバイスグループを選択できます。</li> <li>• フィルタを使用して、動的ポリシー範囲を定義：ポリシー範囲には、ポリシーが影響を及ぼす可能性があるデバイスが含まれます。ポリシーに指定したデバイスを含むデバイスファミリに影響するポリシールールがある場合、ポリシー範囲はそのデバイスにのみ影響します。ポリシーを定義する場合、動的グループを定義する方法で歩シリー範囲を定義できます。そのため、ポリシーとともにプライベートな動的グループを作成できます。(動的グループの作成の詳細については、「<a href="#">動的デバイスグループ</a>」(140 ページ)を参照してください)。</li> </ul>

フィールド	説明/アクション
<p><b>検索条件</b>（動的ポリシー範囲を定義するためにフィルタを使用する場合）</p> <p>検索条件は[条件を追加]ドロップダウンメニューから選択するたびに、[検索条件]セクションに表示されます。このセクションでは、「含む」、「一致する」、または「等しい」といった演算子を選択したり、検索する情報を入力したりできます。定義済みの条件を削除する場合は、検索条件インデックス文字の横に表示されている「X」をクリックします。</p>	
条件を追加	<p>ドロップダウンメニューから検索条件を1つ以上選択します。選択可能な条件は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 構成テキスト</li> <li>• デバイスIP</li> <li>• デバイスステータス</li> <li>• パスワードルール</li> <li>• ホスト名</li> </ul>
<b>ブール式</b>	
式	<p>デフォルトでは、定義済みの条件インデックス文字がブール式「and」で結合されて表示されます。たとえば、3つの検索条件が定義されている場合、式は <i>A and B and C</i> のようになります。ブール式は、必要に応じて編集できます。[式をリセット]ボタンをクリックすると、式がデフォルト値にリセットされます（<b>注意</b>：ブール演算子は小文字で入力する必要があります。また、条件の最大数は10です）。</p>
<b>デバイスグループで検索を絞り込み</b>	
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• 選択グループ内のいずれか（デフォルト）</li> <li>• 選択グループのすべて</li> <li>• 選択グループになし</li> </ul> <p><b>注意</b>：[Shift]キーとクリックを使用すると、複数のデバイスグループを選択または選択解除できます。デバイスグループを選択しない場合、検索時にデバイスグループフィルタが失われます。</p>
<b>ビューとパーティションで検索を絞り込み</b> （この情報は、ビューとパーティションを構成した場合のみ表示されます。詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」（148ページ）を参照してください）。	
例外とするデバイス	<p>デバイスのIPアドレスまたはホスト名を追加するには、右側のボックスにホスト名またはIPアドレスを入力して、[例外を追加 &lt;&lt;]をクリックします。デバイスを削除するには、左側のボックスにあるデバイスのIPアドレスまたはホスト名を選択して、[例外を削除]をクリックします。</p>
ポリシールール	<p>ポリシーが適用されるすべてのルールを表示します。ポリシーは、このポリシー用に選択した保存されたデバイスそれぞれに対し、すべての構成ルールを適用します。ルールは順不同で適用されます。[重要度]列では、情報、低、中、高、最重要のいずれかを表示します。これは、ポリシールールの非準拠リスクレーティングを示します。[アクション]列にある[表示と編集]リンクをクリックして、ルールを編集します。</p>
ルールの新規作成ボタン	<p>このポリシーの新規ルールを作成するには、[ルールの新規作成]ボタンをクリックします。[ルールの新規作成]ページが開きます。詳細については、「<a href="#">[ルールの新規作成]ページのフィールド</a>」（420ページ）を参照してください。</p>
詳細な説明	<p>ポリシーの詳細な説明を表示します。</p>

フィールド	説明/アクション
ポリシーのステータス	次のオプションから1つをクリックします。 <ul style="list-style-type: none"> <li>• アクティブ：ポリシーをアクティブにします（デフォルト）。</li> <li>• 非アクティブ：ポリシーを非アクティブにします。</li> </ul>
<b>追加ポリシーフィールド</b> （これらのフィールドは、ポリシーがHP Security and Compliance Serviceに基づく場合に自動的に入力されます。）	
CVE	CVE（Common Vulnerabilities and Exposures）名を表示します。CVE とは、セキュリティ問題に関する脆弱性やその他の情報に付けられた標準名のリストです。（詳細については、 <a href="http://www.cve.mitre.org">www.cve.mitre.org</a> を参照してください。）
ベンダー諮問URL	脆弱性に関する助言情報の外部参照のURLを表示します。
ベンダーソリューションURL	脆弱性への実行可能なソリューションの詳細に関する、外部参照のURLを表示します。
開示日	ソフトウェアの脆弱性が警告された日付を yyyy-MM-dd フォーマットで表示します。
解決策	詳細な解決策情報を表示します。

## ルール例外の追加

ルール例外は、ルールの一部です。ルールと同様に、正規表現で記述します。ただし、その構成ルールによって、デバイス構成内で一致するテキストを除外することが、構成ルール例外の目的です。

例外ルールでは、通常、テキストパターンまたは特定のデバイス構成を、構成ルールから除外します。1つ以上のデバイス構成がルールに準拠しない場合に、例外は作成されますが、類似の全構成に適合させるためにルールを変更することはできません。

ルール例外を既存の構成ルールに追加するには：

1. [ポリシー]メニューバーの[ポリシーリスト]をクリックします。[ポリシー]ページが開きます。
2. 例外を追加するポリシーを選択して、[表示と編集]をクリックします。[ポリシーを編集]ページが開きます。
3. 例外を必要とするポリシー内のルールを探し、[表示と編集]をクリックします。[ルールの新規作成]ページが開きます。
4. ページの最下部にある[例外の新規作成]リンクをクリックします。[ルール例外の新規作成]ページが開きます。

## [ルール例外の新規作成]ページのフィールド

フィールド	説明/アクション
デバイス	この例外ルールを適用するデバイスのIPアドレスまたはホスト名を入力します。
失効日	オンの場合は、年、月、日、時、分を選択します。これ以降は、ルールによって例外が無視されます。例外ルールの有効期限とは、属すルールに対して例外が影響を与えなくなる日付のことです。有効期限後も例外ルールは存在しつづけますが、構成ポリシーは例外ルールが存在しないかのようにルールを適用します。
構成ルールを確認するとき にこのパターンに一致する テキストを無視	オンにした場合、テキストを入力します。入力したテキストに一致するデバイスの構成の全テキストは、この構成ルールには従いません（ <b>注意：</b> <a href="#">ヘルプの取得</a> オプションに例があります。）
構成ルールを確認するとき にこのデバイスを完全に 無視	オンの場合は、構成ルールの確認時に、NAはこのデバイスをスキップします。

終了時に、必ず[保存]をクリックしてください。

## 適用されるポリシーの表示

デバイスに適用するポリシーを表示できます。これにより、次のことを実行できます。

- デバイスに適切なポリシーが適用されたことの確認
- ポリシーが成功したか失敗したかの表示
- NAにデバイスを追加した際にデバイスに適用されるポリシーの表示
- デバイスに適用されたポリシーに対して適切に指定されている例外の表示

適用されるポリシーを表示するには：

1. デバイスの新しいポリシーを作成します。詳細については、「[ポリシーの作成](#)」(414ページ)を参照してください。
2. デバイスに対してポリシーを実行します。詳細については、「[\[ポリシー準拠\] ページのフィールド](#)」(431ページ)を参照してください。
3. そのデバイスの[デバイス詳細]ページを開きます。
4. [表示]メニューをクリックします。
5. [デバイス詳細]を選択し、[ポリシー]をクリックします。[デバイスポリシー]ページが開きます。詳細については、「[\[デバイスポリシー\] ページのフィールド](#)」(221ページ)を参照してください。

## ポリシーアクティビティの表示

デバイス構成が、1つまたは複数のポリシーに含まれるルールに非準拠であることを示すイベントを表示できます。デバイスが非準拠であることをNAが検出して記録した日時を、このイベントが表示します。

[ポリシーアクティビティ]ページを表示するには、[ポリシー]メニューバーの[ポリシーアクティビティ]をクリックします。[ポリシーアクティビティ]ページが開きます。

## [ポリシーアクティビティ]ページのフィールド

フィールド	説明/アクション
対象（期間）	非準拠イベントを表示する期間を選択します。デフォルトでは過去1時間です。
現在の作業グループ	非準拠イベントを表示するグループを選択します。デフォルトではインベントリです。インベントリには、その他すべてのグループが含まれています。
イベント日時	ポリシーが非準拠であることが検出された日時を表示します。
ポリシー名	ポリシーの名前が表示されます。このリンクをクリックすると、[ポリシーを編集]ページが開きます。ポリシーおよび含まれているルールを編集できます。詳細については、「 <a href="#">ポリシーを編集</a> 」(425 ページ)を参照してください。
ホスト名	デバイスのホスト名が表示されます。このリンクをクリックすると、デバイスの基本情報を表示します。
デバイスIP	デバイスのIPアドレスを表示します。このリンクをクリックすると、デバイスの基本情報と構成履歴を表示します。
サマリ	イベントタイプを表示します（構成ポリシーに非準拠）。このリンクをクリックすると、[システムイベントの詳細]ページが開きます。そのページで、非準拠イベントの詳細を表示できます。
重要度	違反をしていた準拠ルールの重要度を次のように表示します。 <ul style="list-style-type: none"> <li>・情報：一般的に対応を必要としないイベント。</li> <li>・低：時間的な余裕がある場合に対応を必要とするイベント。</li> <li>・中：適時に対応を必要とするイベント（通常は72時間以内）。</li> <li>・高：緊急の対応を必要とするイベント（通常は24時間以内）。</li> <li>・重要：即時の対応を必要とするイベント。</li> </ul>

## ポリシー準拠の表示

[ポリシー準拠]ページでは、デバイスの構成が構成ポリシーに準拠しているかどうかを表示できます。

[ポリシー準拠]ページを表示するには、[ポリシー]メニューバーの[ポリシー準拠]をクリックします。[ポリシー準拠]ページが開きます。

## [ポリシー準拠]ページのフィールド

フィールド	説明/アクション
ポリシー準拠の確認	[ポリシー準拠の確認]ページが開きます。そのページで、構成の準拠性をチェックできます。詳細については、 <a href="#">「[ポリシー準拠の確認]タスクページのフィールド」(372ページ)</a> を参照してください。
現在の作業グループ	デバイスの準拠ステータスを表示するグループを選択します。
準拠しないデバイスのみを表示	オンの場合は、準拠しているデバイスは表示しません。
ホスト名	デバイスのホスト名が表示されます。このリンクをクリックすると、デバイスの基本情報を表示します。
デバイスIP	デバイスのIPアドレスを表示します。このリンクをクリックすると、デバイスの基本情報と構成履歴を表示します。
ポリシー準拠	<ul style="list-style-type: none"> <li>• はい：デバイス構成がすべてのポリシーに準拠していることを示します。</li> <li>• いいえ：デバイス構成がすべての構成ポリシーには準拠していないことを示します。[いいえ]を選択すると、[ポリシーアクティビティ]ページが開きます。詳細については、<a href="#">「[ポリシーアクティビティ]ページのフィールド」(430ページ)</a>を参照してください。</li> <li>• 不明：ポリシー準拠が確認されていないデバイスを示します。</li> </ul>
パーティション	該当する場合、デバイスが属すパーティションを表示します。
最終変更時間	デバイスの構成を最後に変更した日付と時刻が表示されます。
アクション	<p>次のオプションを選択できます。</p> <ul style="list-style-type: none"> <li>• ポリシーイベント：[ポリシーアクティビティ]ページが開きます。そのページで、非準拠イベントの詳細を表示できます。詳細については、<a href="#">「[ポリシーアクティビティ]ページのフィールド」(430ページ)</a>を参照してください。</li> <li>• ポリシーの適用：[デバイスに適用されるポリシー]ページが開きます。そのページで、構成ポリシーとルールを表示できます。詳細については、<a href="#">「[デバイスに適用される構成ポリシー]ページのフィールド」(432ページ)</a>を参照してください。</li> </ul>

## [デバイスに適用される構成ポリシー]ページのフィールド

[デバイスに適用されるポリシー]ページを表示するには：

1. [ポリシー]メニューバーの[ポリシー準拠]をクリックします。
2. 情報が必要なデバイスの[アクション]列にある[ポリシーの適用]リンクをクリックします。[デバイスに適用されるポリシー]ページが開きます。

フィールド	説明/アクション
ポリシー名	デバイスに適用される構成ポリシー名を表示します。
ルール名	デバイスに適用される構成ルール名を表示します。
非準拠キー	現時点でのデバイスの非準拠ステータスを次のように表示します。 <ul style="list-style-type: none"><li>• 高重要度（赤）</li><li>• 中重要度（アンバー）</li><li>• 低重要度（緑）</li></ul>
アクション	次のオプションを選択できます。 <ul style="list-style-type: none"><li>• ホスト名またはIPアドレス：[デバイス情報]ページが開きます。そのページでは、デバイスの基本情報や構成履歴を表示できます。</li><li>• ポリシー名：[ポリシーを編集]ページが開きます。そのページで、ポリシーの編集や構成ルールの追加と編集ができます。「<a href="#">ポリシーを編集</a>」（425 ページ）を参照してください。</li><li>• ルール名：[ポリシールールを編集]ページが開きます。そのページで構成ルールを編集できます。「<a href="#">ルール例外の追加</a>」（428 ページ）を参照してください。</li></ul>



## 新規ソフトウェアレベルの追加

セキュリティ脆弱性に関して、ネットワークデバイスセキュリティからの警告や通知が増え続けており、各デバイスに搭載されているOSバージョンや、そのOSバージョンにセキュリティ脆弱性があるかどうかの追跡作業に、多くの組織が直面しています。NAでは、セキュリティの問題を受けやすいOSのバージョンを指定して、そのバージョンを検出したときに警告や自動応答を生成することができます。イメージを「実稼働前」や「廃止」などのカテゴリに分類できます。また、最近検出した脆弱性に基づいて、イメージを「セキュリティリスク」などと分類することもできます。

新規ソフトウェアレベルを追加する、または既存の準拠定義を確認するには：

1. [ポリシー]メニューバーの[ソフトウェアレベル]をクリックします[ソフトウェアレベル]ページが開きます。([ソフトウェアレベル]ページの詳細については、[「\[ソフトウェアレベル\]ページのフィールド」\(435ページ\)](#)を参照してください)。
2. [レベルを追加]リンクをクリックします。[ソフトウェアレベルを追加]ページが開きます。終了時に、必ず[保存]をクリックしてください。

## [ソフトウェアレベルを追加]ページのフィールド

フィールド	説明/アクション
<b>ソフトウェアレベルを追加</b>	
レベル名	レベル名を入力します。
ステータス	次のオプションから1つを表示します。 <ul style="list-style-type: none"> <li>• アクティブ：構成ポリシーをアクティブにします（デフォルト）。</li> <li>• 非アクティブ：構成ポリシーを非アクティブにします。非アクティブポリシーでは、非準拠イベントを生成しません。</li> </ul>
レベル	準拠の評価名を選択します。ユーザの要件と検証手順によって与えられる、準拠定義を使用できます。次のオプションが用意されています。 <ul style="list-style-type: none"> <li>• セキュリティリスク</li> <li>• 実稼働前</li> <li>• 廃止</li> <li>• ブロンズ</li> <li>• シルバー</li> <li>• ゴールド</li> <li>• プラチナ</li> </ul>
説明	準拠の説明を入力します。セキュリティ問題の意識を向上させるには、脆弱性についての短いタイトル、適用できるCVE/CANまたはCERTの表示、可能であればベンダの通知へのリンクなどを、セキュリティリスクの説明に入れてください。

フィールド	説明/アクション
パーティション	ドロップダウンメニューからパーティションを選択します。セキュリティや業務上の理由でパーティションを作成した場合、特定パーティションのソフトウェアレベルをパーティションできます。ポリシーを特定のパーティション内の特定ユーザに加え、すべてのパーティション内のすべてのユーザで共有するように構成できます。ソフトウェアレベルがすべてのパーティションで利用できる場合、[共有]と表示されます。
<b>一致基準</b> （一致条件にワイルドカード演算子（*および?）を使用することができます。）	
ソフトウェアバージョン	この準拠ポリシーが適用されるソフトウェアバージョンを入力します。
デバイスドライバ	デバイスへのアクセスに使用するデバイスドライバを、ドロップダウンメニューから選択します。（デフォルトでは[任意のドライバ]です。）
デバイスモデル	デバイスモデルを入力します。
ファイル名	該当する場合、ファイル名を入力します。
構成に含まれる項目	指定したデバイスに準拠が適用されているかどうかを判別するために、現在のデバイス構成に一致するパターンを入力します。
<b>ソフトウェアの脆弱性情報（セキュリティリスクレベル）</b>	
開示日	ソフトウェアの脆弱性が警告された日付を yyyy-MM-dd フォーマットで入力します。
重要度	セキュリティ脆弱性の重要度を、ドロップダウンメニューの次の項目から選択します。 <ul style="list-style-type: none"> <li>• 情報</li> <li>• 低</li> <li>• 中</li> <li>• 高</li> <li>• 重要</li> </ul>
CVE 名	CVE（Common Vulnerabilities and Exposures）名を入力します。CVE とは、セキュリティ問題に関する脆弱性やその他の情報に付けられた標準名のリストです。（詳細については、 <a href="http://www.cve.mitre.org">www.cve.mitre.org</a> を参照してください。）
解決策	解決策情報を入力します。
諮問リンク	脆弱性に関する諮問情報の外部参照の URL を入力します。
ソリューション URL	脆弱性への実行可能なソリューションの詳細に関する、外部参照の URL を入力します。

## [ソフトウェアレベル]ページのフィールド

NAは、ソフトウェアレベル、本質的にはソフトウェアバージョンに一致する正規表現を定義できます。その正規表現にソフトウェアレベルを割り当てられます。正規表現に一致するソフトウェアバージョンのあらゆるデバイスは、そのレベルであると見なされます。

**注意：** ソフトウェアレベルをパーティション化することで、適切な権限のあるソフトウェアレベルのみを表示して、編集できます。詳細については、「[パーティション](#)」(156ページ)を参照してください。

[ソフトウェアレベル]ページでは、既存のソフトウェアレベル定義を確認できます。

フィールド	説明/アクション
レベルを追加	[ソフトウェアレベルを追加]ページが開きます。そのページでソフトウェアレベルを追加できます。「 <a href="#">[ソフトウェアレベルを追加]ページのフィールド</a> 」(433ページ)を参照してください。
デバイスソフトウェアレポート	デバイスソフトウェアレポートが開きます。このレポートでは、各デバイスのソフトウェアバージョンと割り当てられている現在の準拠レベルを表示できます。「 <a href="#">デバイスソフトウェアレポートのフィールド</a> 」(612ページ)を参照してください。
ソフトウェアレベルレポート	ソフトウェアレベルレポートが開きます。このレポートでは、各デバイスに割り当てられているソフトウェアレベルを表示できます。「 <a href="#">ソフトウェアレベルレポートのフィールド</a> 」(614ページ)を参照してください。
表示	[ユーザ定義のレベル]または[セキュリティアラートサービスアラート]をドロップダウンメニューから選択します。[セキュリティアラートサービスアラート]は、セキュリティアラートサービスで発生したイベントです。(注意：セキュリティアラートサービスは、登録によるサービスです。)
チェックボックス	<p>左側のチェックボックスを使用して、ソフトウェアレベル定義を管理できます。準拠定義を選択して、[アクション]のドロップダウンメニューをクリックし、次のいずれかをクリックします。</p> <ul style="list-style-type: none"> <li>• アクティブ化：ソフトウェアレベル定義をアクティブ化するようにNAに指示します。</li> <li>• 非アクティブ化：ソフトウェアレベル定義を非アクティブ化するようにNAに指示します。</li> <li>• 削除：ソフトウェアレベル定義を削除します。</li> </ul> <p>隣接する[選択]ドロップダウンメニューで、全ポリシーを選択（または選択解除）できます。</p>
名前	準拠名を表示します。
バージョン	ソフトウェアのバージョンを表示します。
ドライバ	ドライバ名を表示します。
モデル	デバイスのモデル名が表示されます。
ファイル名	ファイル名を入力できます(ワイルドカードが使用可能)。これで準拠を特定します。たとえば、「router5*.bin」で始まるすべてのイメージを「廃止」としてタグ付けできます。

フィールド	説明/アクション
ソフトウェアレベル	<p>準拠評価名を表示します。評価には次の項目があります。</p> <ul style="list-style-type: none"> <li>• セキュリティリスク</li> <li>• 実稼動前</li> <li>• 廃止</li> <li>• ブロンズ</li> <li>• シルバー</li> <li>• ゴールド</li> <li>• プラチナ</li> </ul>
重要度	<p>情報、低、中、高、最重要のいずれかを表示します。これは違反のあった準拠ルール的重要度を示します。</p> <ul style="list-style-type: none"> <li>• 情報：一般的に対応を必要としないイベント。</li> <li>• 低：時間的な余裕がある場合に対応を必要とするイベント。</li> <li>• 中：適時に対応を必要とするイベント（通常は72時間以内）。</li> <li>• 高：緊急の対応を必要とするイベント（通常は24時間以内）。</li> <li>• 重要：即時の対応を必要とするイベント。</li> </ul>
最終変更	ソフトウェアレベルが最後に変更された日時を表示します。
パーティション	<p>セキュリティや業務上の理由でパーティションを作成した場合、特定パーティションのソフトウェアレベルをパーティションできます。ソフトウェアレベルを、特定のパーティション内の特定ユーザに加え、すべてのパーティション内のすべてのユーザで共有するように構成できます。パーティションの作成の詳細については、「<a href="#">デバイスとユーザのセグメント化</a>」(148ページ)を参照してください。</p>
CVE	<p>CVE（Common Vulnerabilities and Exposures）名を表示します。CVE とは、セキュリティ問題に関する脆弱性やその他の情報に付けられた標準名のリストです。</p>
コメント	準拠の説明を表示します。
アクション	<p>次のオプションを選択できます。</p> <ul style="list-style-type: none"> <li>• 編集：[準拠を編集]ページが開き、そのページで準拠を編集できます。</li> <li>• 削除：準拠を削除できます。</li> </ul>

## ソフトウェアレベルの編集

ソフトウェアレベルを編集するには：

1. [ポリシー]メニューバーの[ソフトウェアレベル]をクリックします。[ソフトウェアレベル]ページが開きます。
2. 編集するソフトウェアレベルの[編集]アクションをクリックします。[Edit Software Level]ページが開きます。終了時に、必ず[保存]をクリックしてください。

### [ソフトウェアレベルの編集]ページのフィールド

フィールド	説明/アクション
<b>準拠の編集</b>	
レベル名	ポリシー名を表示します。
ステータス	次のオプションから1つを表示します。 <ul style="list-style-type: none"> <li>• アクティブ：構成ポリシーをアクティブにします（デフォルト）。</li> <li>• 非アクティブ：構成ポリシーを非アクティブにします。非アクティブポリシーでは、非準拠イベントを生成しません。</li> </ul>
レベル	ソフトウェアレベル評価名を表示します。ユーザの要件と検証手順により決定する定義を使用できます。次のオプションが用意されています。 <ul style="list-style-type: none"> <li>• セキュリティリスク</li> <li>• 実稼動前</li> <li>• 廃止</li> <li>• ブロンズ</li> <li>• シルバー</li> <li>• ゴールド</li> <li>• プラチナ</li> </ul>
説明	準拠の説明を表示します。
<b>一致基準</b>	
ソフトウェアバージョン	この準拠ポリシーが適用されるソフトウェアバージョンが表示されます。
デバイスドライバ	デバイスへのアクセスに使用するデバイスドライバを表示します。
デバイスモデル	デバイスモデルを表示します。
構成に含まれる項目	指定したデバイスに準拠ポリシーが適用されているかどうかを判別するために、現在のデバイス構成に一致するパターンを入力します。
<b>ソフトウェアの脆弱性情報（セキュリティリスクレベル）</b>	
開示日	ソフトウェアの脆弱性が警告された日付を表示します。

フィールド	説明/アクション
重要度	セキュリティの脆弱性を次の重要度で表示します。 <ul style="list-style-type: none"><li>• 情報</li><li>• 低</li><li>• 中</li><li>• 高</li><li>• 重要</li></ul>
CVE 名	CVE（Common Vulnerabilities and Exposures）名を表示します。CVE とは、セキュリティ問題に関する脆弱性やその他の情報に付けられた標準名のリストです。（詳細については、 <a href="http://www.cve.mitre.org">www.cve.mitre.org</a> を参照してください。）
解決策	解決策情報を表示します。
諮問リンク	脆弱性に関する助言情報の外部参照の URL を表示します。
ソリューションリンク	脆弱性への実行可能なソリューションの詳細に関する、外部参照の URL を表示します。

## ポリシー準拠のテスト

1つ以上の構成ポリシーに対するデバイスの構成準拠をテストすることができます。または、1つ以上の構成に対する構成ポリシーをテストできます。デバイスの構成準拠のテスト、または配布前の構成ポリシーのテストができます。

[ポリシー]メニューバーの[ポリシー準拠のテスト]をクリックします。[ポリシー準拠のテスト]ページが開きます。

### [ポリシー準拠のテスト]ページのフィールド

フィールド	説明/アクション
ポリシーリスト	[ポリシー]ページが開きます。そのページで、ポリシーのリストを表示できます。詳細については、「 <a href="#">[ポリシー]ページのフィールド</a> 」(415ページ)を参照してください。
テストするポリシーを選択	次のオプションからいずれか1つを選択できます。 <ul style="list-style-type: none"> <li>• 全ポリシー：オンの場合（デフォルト）は、構成ポリシーをすべてテストします。</li> <li>• 選択デバイスグループに適用できるポリシー：テストを実行するデバイスグループを選択します。複数のデバイスグループを選択するには、[Shift]キーを押しながらデバイスグループを選択します。</li> <li>• 選択したポリシー：特定のポリシーを選択します。複数のポリシーを選択するには、[Shift]キーを押しながらポリシーを選択します。</li> </ul>
既存のデバイスに対してポリシーをテスト	ポリシーのテスト対象とするデバイスを選択します。デバイスセレクトタの使用法の詳細については、「 <a href="#">デバイスセレクトタ</a> 」(142ページ)を参照してください。
構成に対してポリシーをテスト	このオプションを選択する場合は、構成テキストをボックスに入力またはペーストして、ドロップダウンメニューから入力した構成テキストのデバイスファミリを選択します。

終了時に、[テストの実行]をクリックします。構成ポリシーのテストを通過した場合は、新しいウィンドウに「デバイス[デバイス名]は選択された適用可能なポリシーに準拠しています」メッセージが表示されます。構成ポリシーのテストを通過しなかった場合は、新しいウィンドウに、詳細情報へのリンクと併せて各違反のリストが表示されます。

### [ポリシーをテスト]ページのフィールド

初めてポリシーを作成するとき、ポリシーをテストし、そのポリシーがデバイスの問題を正しく捉えることを確認できます。ただし、NAが非準拠イベントを作成すると、生涯管理システムでアラートが発生したり、ネットワーク準拠測定を混乱させてしまう可能性があります。この場合、「ポリシーをテスト」機能を使用することが最善です。「ポリシーをテスト」条件を使用すれば、イベントは生成されません。このため、非準拠イベントを発生させることなく、ポリシーをテストできます。

デバイスを選択して、[テストの実行]ボタンをクリックします。

フィールド	説明/アクション
テストするポリシーを選択	ドロップダウンメニューからポリシーを選択します。
テスト対象のデバイスを 選択	ポリシーのテスト対象とするデバイスを選択します。デバイスセレクトタの使用方法の詳細については、「 <a href="#">デバイスセレクトタ</a> 」(142 ページ) を参照してください。



## 第9章：ソフトウェアの配布

### トピックの参照先リスト

トピック	参照先：
はじめに	<a href="#">「はじめに」</a> （442ページ）
ソフトウェアイメージ	<a href="#">「ソフトウェアイメージ」</a> （444ページ）
イメージセットの追加	<a href="#">「イメージセットの追加」</a> （445ページ）
ソフトウェアの配布	<a href="#">「ソフトウェアの配布」</a> （448ページ）
新規準拠の追加	<a href="#">「新規ソフトウェアレベルの追加」</a> （449ページ）
デバイスソフトウェアのバージョンの表示	<a href="#">「デバイスソフトウェアのバージョンの表示」</a> （451ページ）

## はじめに

HP Network Automation (NA) では、オペレーティングシステム (OS) イメージを含む、デバイスソフトウェアの中央リポジトリを提供しており、同一のソフトウェアを共有する1つ以上のデバイスに配布できます。中央の保存場所を持つことで、正常であると認識された最新のソフトウェアを、組織内で使用できることを保証します。

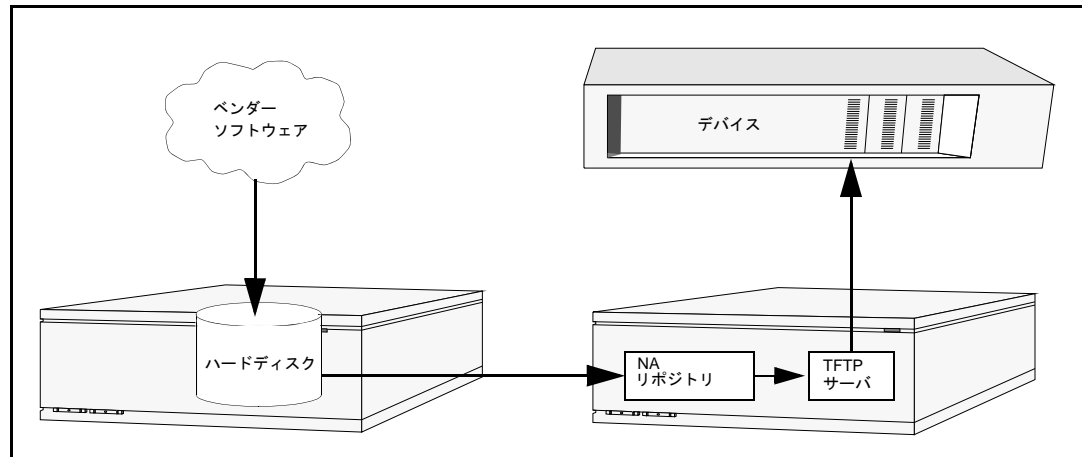
次のことが可能です。

- ソフトウェアイメージセットをシステムにアップロードします。イメージセットとは、デバイスに同時に配布できるイメージのグループのことです。イメージセットは1つ以上のイメージを含むことができます。ソフトウェアのアップロードを開始するときに、アップロードするイメージセットを選択します。イメージセット内の各イメージは、順々にアップロードされます。デバイスに問題があると（たとえば、メモリ不足）、残りのアップロードは中止されます。
- デバイスにファイルを追加、またはアップロードします。
- イメージの実行を成功させるために必要なイメージセットの最小要件を定義。たとえば、デバイスファミリ、デバイスモデル、最小のRAM、プロセッサ、ブートROMバージョンなどです。
- イメージを配布する前に、フラッシュメモリ空間を確保するためのファイル削除や、フラッシュメモリの圧縮などをしてデバイスの準備をします。
- イメージの配布後にデバイスをリブートします。
- NA を通じて更新をスケジュールリング。たとえば、日中の作業中に新規イメージを1つのデバイスに配布してから、オフピーク時にさらに多くのデバイスの更新をスケジュールリングする場合があります。
- ソフトウェアのバージョンを特定し、リソースの許可どおりにデバイスをアップグレードするために、複数の準拠評価を定義します。
- どのイメージを、複数のブートイメージがあるデバイスのブートイメージとするかを指定します。現在のデバイス上のブートイメージと、必要であればOSイメージを選択でき、新規ブート、OSのいずれかまたは両方のイメージをダウンロードできます。単一のブート、OSのいずれかまたは両方のイメージを選択すると、デバイス上でコマンドが発行され、これらのイメージがブート、OSのいずれかまたは両方に使用するイメージとして設定されます。デバイスによっては、デバイスが再ブートするまで効果が現れない場合があります。再ブートはデバイスソフトウェアの更新タスクとして選択できます。詳細については、[「\[デバイスソフトウェアの更新\]タスクページのフィールド」\(323ページ\)](#) を参照してください。

他の機能にはイメージ同期レポートがあります。この機能では、デバイスやデバイスのグループ上にあってNAソフトウェアイメージリポジトリにはない、現在実行中のソフトウェアイメージ、またはバックアップソフトウェアイメージを表示できます。詳細については、[「イメージ同期レポートのフィールド」\(618ページ\)](#) を参照してください。

**注意：** ブートイメージには、システムストレージメディアの完全なコンテンツと構造が含まれます。ブートイメージは、関連するハードウェアをブートできるようにします。OSイメージには、デバイスの電源を投入し、デバイスがそれ自体のインターフェイスに関する情報を収集した後にデバイスを動作させる命令が含まれます。OSイメージには、ルーティングプロトコルなどの項目が含まれます。

次の図は、ダウンロードのプロセスを示します。



ソフトウェア更新機能の使用時に従うべきベストプラクティスがいくつかあります。ソフトウェアイメージの配布時に、HPは次のプラクティスを推奨します。

- 標準の変更制御と承認プロセスに従います。デバイスのステータスを変更するときは、常にリスクがあります。ネットワークに与える影響を最小にするには、組織内で定義された変更プロセスにすべて従います。たとえば、承認、通知、ウィンドウの変更などです。
- 特定のデバイスとOSバージョンの更新のために、適切な方法を調査して理解します。デバイスによっては、複数のイメージをアップグレードする必要があります。また、ファームウェアやハードウェアに依存することもあります。
- 運用ネットワーク上に配布する前に、特定のOSバージョンの機能をテストします。OSバージョンのアップグレード（または特にダウングレード）をするときには、デバイス構成が警告を受けたり、変更前後にデバイス構成の更新が必要な場合があります。特定のバージョンを運用環境に配布する前に、実験環境で詳細にテストを行い、構成のアップグレードが成功して、デバイス機能が予想どおりに動作することを確認します。
- 現在のデバイスイメージをバックアップします。NAリポジトリを使用して、アップグレード前に既存のイメージをデバイスに保存します。新規イメージが予想外の結果を示した場合でも、この方法によりただちに回復できます。イメージ同期レポートでは、デバイスやデバイスのグループ上においてNAソフトウェアイメージリポジトリにはない、現在実行中のソフトウェアイメージ、またはバックアップソフトウェアイメージを表示できます。詳細については、「[イメージ同期レポートのフィールド](#)」(618 ページ) を参照してください。
- デバイスをアップグレードする際、デバイスへのアクセスをコンソールサーバ経由で帯域外管理をするのは良い考えです。
- イメージ要件を提供し、慎重にその要件を検証します。NAでは、ソフトウェアイメージごとに要件を指定できます。
- 業務上で重要なデバイスにイメージを配布する場合は、自動リブート機能は使用しないでください。それよりも、ソフトウェア更新機能を使用して、デバイスの準備とイメージのロードを行います。次に、各デバイスがクリーンなステータスにあるかどうかをリブート前に手動で検査します。
- デバイスグループを更新する前に、まず1つのデバイスを更新します。

## ソフトウェアイメージ

デバイスのソフトウェアをアップグレードする前に、各デバイスに現在インストールされているソフトウェアについて注意する必要があります。注意点を以下に挙げます。

- イメージセット
- ファイル名
- 必要なドライバ

[デバイス]メニューで[デバイスツール]を選択して、[ソフトウェアイメージ]をクリックします。[ソフトウェアイメージ]ページが開きます。

## [ソフトウェアイメージ]ページのフィールド

フィールド	説明/アクション
Cisco.comからイメージセットを追加	[Cisco.com からイメージをダウンロード]タスクページが開きます。詳細については、「 <a href="#">[Cisco.com からイメージをダウンロード]タスクページ</a> 」(367 ページ) を参照してください。
イメージセットを追加	[ソフトウェアイメージセットを追加]ページが開きます。そのページで、イメージセットを追加できます。詳細については、「 <a href="#">イメージセットの追加</a> 」(445 ページ) を参照してください。
ソフトウェアレベル	[ソフトウェアレベル]ページが開きます。そのページで、新規ソフトウェアレベルを追加したり、デバイスソフトウェアレポートを表示できます。新しいレベルを追加する方法の詳細については、「 <a href="#">新規ソフトウェアレベルの追加</a> 」(433 ページ) を参照してください。デバイスソフトウェアレポートの詳細については、「 <a href="#">デバイスソフトウェアレポート</a> 」(612 ページ) を参照してください。
イメージセット	イメージセット名を表示します。
必要なドライバ	このプラットフォームに必要なNAドライバの名前を表示します。
必要なモデル	必要なモデルの名前を表示します。このフィールドは、すべての可能なモデルを格納するように255文字から4,000文字に拡張されています。
必要なハードウェア	該当する場合は、ハードウェア要件を表示します。
パーティション	セキュリティや業務上の理由でパーティションを作成した場合、パーティションに沿ってソフトウェアイメージをパーティションできます。ソフトウェアイメージがすべてのパーティションで利用できる場合、構成に応じてソフトウェアイメージは[共有] (または[グローバル]) と表示されます。適切な権限がない場合、ソフトウェアイメージの編集や削除を実行できません。パーティションの作成の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」(148 ページ) を参照してください。
アクション	次のオプションを選択できます。 <ul style="list-style-type: none"> <li>• 編集 : [ソフトウェアイメージの編集]ページが開きます。そのページで、既存のソフトウェアの情報を編集できます。詳細については、「<a href="#">[ソフトウェアイメージの編集]ページのフィールド</a>」(447 ページ) を参照してください。</li> <li>• ソフトウェアイメージ : [セット内のイメージを管理]ページが開きます。そのページで、イメージセットの編集、イメージの追加、ソフトウェアの配布ができます。「<a href="#">[ソフトウェアイメージセットを追加]ページのフィールド</a>」(445 ページ)、「<a href="#">[ソフトウェアイメージの編集]ページのフィールド</a>」(447 ページ)、または「<a href="#">ソフトウェアの配布</a>」(448 ページ) を参照してください。</li> <li>• 削除 : イメージを削除できます。</li> <li>• デバイスの更新 : [デバイスソフトウェアの更新]タスクページが開きます。詳細については、「<a href="#">ソフトウェアの配布</a>」(448 ページ) を参照してください。</li> </ul>

## イメージセットの追加

イメージセットを追加するには：

1. [デバイス]メニューで[デバイスツール]を選択して、[ソフトウェアイメージ]をクリックします。[ソフトウェアイメージ]ページが開きます。
2. [イメージセットを追加]リンクをクリックします。[ソフトウェアイメージセットを追加]ページが開きます。終了時に、必ず[ソフトウェアを保存]ボタンをしてください。

**注意：** ファイルサイズは256MBより大きくはできません。

### [ソフトウェアイメージセットを追加]ページのフィールド

フィールド	説明/アクション
イメージセット名	イメージセット名を入力します。デバイス上の同一のファイルシステム位置へ、特定のイメージセット内の全イメージを適用します。
パーティション	ドロップダウンメニューからパーティションを選択します。（ <b>注意：</b> このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。）一般的に、パーティションとは一意のIPアドレスを持つデバイスのグループです。単一のNAコアで複数のパーティションを管理できます。NAコアはNAサーバのインストールコンポーネントの1つで、単一の管理エンジン、関連サービス、および単一のデータベースからなります。
イメージ1...5	最大5つの新規イメージまたは構成ファイルを、イメージセットに入力できます。
ベンダーのMD5 チェックサム	ベンダーのMD5チェックサムを入力します。チェックサムとは、MD5アルゴリズムを使用して計算された128ビットのチェックサムのことです。MD5とは、暗号的に安全なアルゴリズムです。チェックサムを同一に保ったままファイルを意図的に変更することは、非常に困難です。多くの場合、ベンダーはデバイスのソフトウェアイメージとともにチェックサムを提供します。イメージを基にしてチェックサムを計算する（またはNAが計算する）場合は、ベンダーが提供したものと一致しなければなりません。一致しない場合は、配布してはならない壊れたイメージファイルを使用したか、ベンダーが別のアルゴリズムを使用してチェックサムを計算した可能性があります。
複数のイメージを含むZIP	圧縮解凍するZIP圧縮ファイルを指定します。ZIPに含まれるすべてのファイルを、イメージセットに追加します。

フィールド	説明/アクション
イメージセットの要件	<p data-bbox="444 241 964 264">イメージセット要件には、次のようなものがあります。</p> <ul data-bbox="444 285 1464 751" style="list-style-type: none"><li data-bbox="444 285 1464 369">• ドライバ：ソフトウェアとともに保存するドライバ情報です。リストには認識されている全ドライバが含まれています。たとえば、Cisco Aironet 1100 Access Point 上のソフトウェアを更新する場合は、[Cisco Aironet access points, 350, 1100, and 1200 series, IOS version 12.2] ドライバを選択します。</li><li data-bbox="444 390 1464 474">• モデル：ソフトウェアとともに保存するモデル情報です。リストには認識されている全ドライバが含まれています。たとえば、Cisco Aironet 1200 series Access Point の場合は、[AIR-AP1220-IOS-UPGRD (C1200 Series)] を選択します。</li><li data-bbox="444 495 1464 632">• システムメモリ (バイト単位) <math>\geq</math>：処理が成功するためにイメージセットに必要な最小の RAM です。大半のデバイスでは、イメージは、システムメモリまたは DRAM として知られているプロセッサメモリ内に常駐しています。物理的に存在しているプロセッサメモリの容量は、ファイルシステム診断を使用してデバイスごとに計算します。たとえば、16384 バイトは 16k と同等です。ただし、すべてのデバイスがファイルシステム診断をサポートしているわけではありません。そのようなデバイスでは、RAM 要件は無視されます。</li><li data-bbox="444 653 1464 705">• プロセッサ：デバイスの CPU のことです。たとえば、Cisco Aironet 1200 series Access Point の場合は、[AIR-AP1220-IOS-UPGRD (PowerPC405GP)] を選択します。</li><li data-bbox="444 726 878 751">• ブート ROM：デバイスの ROM のことです。</li></ul>
説明	ダウンロードしたソフトウェアを他のソフトウェアと区別するために、簡単な説明を入力します。

## [ソフトウェアイメージの編集]ページのフィールド

ソフトウェアイメージを編集するには：

1. [デバイス]メニューで[デバイスツール]を選択して、[ソフトウェアイメージ]をクリックします。[ソフトウェアイメージ]ページが開きます。
2. 編集するイメージセットで、[アクション]列の[編集]オプションをクリックします。[ソフトウェアイメージセットを編集]ページが開きます。

フィールド	説明/アクション
イメージセット名	このイメージセットの名前を表示します。既存のイメージセットを指定することもできます。その場合は、NAが既存のイメージセットに新規イメージを追加します。デバイス上の同一のファイルシステム位置へ、特定のイメージセットにある全イメージを適用します。
パーティション	ドロップダウンメニューからパーティションを選択します。(注意：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。)
イメージセットの要件	<ul style="list-style-type: none"> <li>• ドライバ：ソフトウェアとともに保存するドライバ情報です。リストには認識されている全ドライバが含まれています。たとえば、Cisco Aironet 1100 Access Point上のソフトウェアを更新する場合は、[Cisco Aironet access points, 350, 1100, and 1200 series, IOS version 12.2]ドライバを選択します。</li> <li>• モデル：ソフトウェアとともに保存するモデル情報です。リストには認識されている全ドライバが含まれています。たとえば、Cisco Aironet 1200 series Access Pointの場合は、[AIR-AP1220-IOS-UPGRD (C1200 Series)]を選択します。</li> <li>• デバイスに必要なRAM &gt;=：デバイスの最小RAM。</li> <li>• プロセッサ：デバイスのCPUのことです。たとえば、Cisco Aironet 1200 series Access Pointの場合は、[AIR-AP1220-IOS-UPGRD (PowerPC405GP)]を選択します。</li> <li>• ブートROM：デバイスのROMのことです。</li> <li>• 説明：ダウンロードしたソフトウェアと別のソフトウェアとを区別するための簡単な説明。</li> </ul>

終了時に、必ず[ソフトウェアを保存]をクリックしてください。

## ソフトウェアの配布

[ソフトウェア更新]オプションでは、デバイスにインストールした現在のソフトウェアイメージを自動アップグレードできます。これにより、ネットワーク全体のソフトウェアアップグレードについて、手動でロールアウトする時間を大きく短縮します。また、ソフトウェア更新で監査証跡を実行して、すべてのポリシーとプロシージャを追跡します。

デバイス上の現在のソフトウェアイメージを自動アップグレードするには：

1. [デバイス]メニューで[デバイスツール]を選択して、[ソフトウェアイメージ]をクリックします。[ソフトウェアイメージ]ページが開きます。
2. 配布するイメージセットで、[アクション]列の[デバイスを更新]オプションをクリックします。[タスクの新規作成 - デバイスソフトウェアの更新]タスクが開きます。詳細については、「[\[デバイスソフトウェアの更新\]タスクページのフィールド](#)」(323ページ)を参照してください。

次のことに注意が必要です。

- 合計メモリとは、デバイスの物理メモリの合計です。
- 空きメモリとは、最後のメモリ診断の時点で、アップロードに使用できる空きメモリのことです。
- ネットメモリとは、デバイスソフトウェアの更新タスク実行後の空きメモリの推定値です。デバイスに追加または削除されるようにマークされたファイルも考慮されています（ただし、タスク処理前後の圧縮は考慮されていません）。



## 新規ソフトウェアレベルの追加

最後に承認されたソフトウェアをデバイスが実行することは非常に重要です。ネットワーク管理者は、イメージを[実稼働前]や[廃止]などのカテゴリに分類できます。また、最近検出した脆弱性に基づいて、イメージを「セキュリティリスク」などと分類することもできます。

新規ソフトウェアレベルを追加する、または既存の定義を確認するには：

1. [デバイス]メニューで[デバイスツール]を選択して、[ソフトウェアイメージ]をクリックします。[ソフトウェアイメージ]ページが開きます。
2. ページ最上部の[ソフトウェアレベル]オプションをクリックします。[ソフトウェアレベル]ページが開きます。
3. [レベルを追加]オプションをクリックします。[ソフトウェアレベルを追加]ページが開きます。終了時に、必ず[保存]をクリックしてください。

## [ソフトウェアレベルを追加]ページのフィールド

フィールド	説明/アクション
<b>ソフトウェアレベルを追加</b>	
レベル名	レベル名を入力します。
ステータス	次のオプションから1つを表示します。 <ul style="list-style-type: none"> <li>• アクティブ：構成ポリシーをアクティブにします（デフォルト）。</li> <li>• 非アクティブ：構成ポリシーを非アクティブにします。非アクティブポリシーでは、非準拠イベントを生成しません。</li> </ul>
レベル	準拠の評価名を選択します。ユーザの要件と検証手順によって与えられる、準拠定義を使用できます。次のオプションが用意されています。 <ul style="list-style-type: none"> <li>• セキュリティリスク</li> <li>• 実稼働前</li> <li>• 廃止</li> <li>• ブロンズ</li> <li>• シルバー</li> <li>• ゴールド</li> <li>• プラチナ</li> </ul>
説明	準拠の説明を入力します。
パーティション	ドロップダウンメニューからパーティションを選択します。（ <b>注意</b> ：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。）
<b>一致基準</b> （一致条件にワイルドカード演算子（*および?）を使用することができます。）	
ソフトウェアバージョン	デバイス上で現在実行しているソフトウェアのバージョンを入力します。
デバイスドライバ	デバイスへのアクセスに使用するデバイスドライバを、ドロップダウンメニューから選択します。（デフォルトでは[任意のドライバ]です。）

フィールド	説明/アクション
デバイスモデル	デバイスモデルを入力します。
ファイル名	OS ファイル名に一致する文字列を入力します。
構成に含まれる項目	指定したデバイスに準拠が適用されているかどうかを判別するために、現在のデバイス構成に一致するパターンを入力します。
<b>ソフトウェアの脆弱性情報（セキュリティリスクレベル）</b>	
開示日	ソフトウェアの脆弱性が警告された日付を yyyy-MM-dd フォーマットで入力します。
重要度	セキュリティ脆弱性の重要度を、ドロップダウンメニューの次の項目から選択します。 <ul style="list-style-type: none"> <li>• 重要</li> <li>• 高</li> <li>• 中</li> <li>• 低</li> <li>• 情報</li> </ul>
CVE 名	CVE（Common Vulnerabilities and Exposures）名を入力します。CVE とは、セキュリティ問題に関する脆弱性やその他の情報に付けられた標準名のリストです。（詳細については、 <a href="http://www.cve.mitre.org">www.cve.mitre.org</a> を参照してください。）
解決策	解決策の詳細な情報を入力します。
諮問リンク	脆弱性に関する諮問情報の外部参照の URL を入力します。
解決策リンク	脆弱性への実行可能なソリューションの詳細に関する、外部参照の URL を入力します。

## デバイスソフトウェアのバージョンの表示

デバイスソフトウェアレポートにより、各デバイスのソフトウェアバージョンと割り当てられている現在の準拠レベルを表示できます。

1. [デバイス]メニューで[デバイスツール]を選択して、[ソフトウェアイメージ]をクリックします。[ソフトウェアイメージ]ページが開きます。
2. ページ最上部の[ソフトウェアレベル]オプションをクリックします。[ソフトウェアレベル]ページが開きます。
3. ページ最上部の[デバイスソフトウェアレポート]オプションをクリックします。[デバイスソフトウェアレポート]が開きます。詳細については、「[デバイスソフトウェアレポートのフィールド](#)」(612 ページ) を参照してください。

**注意：** [レポート] ドロップダウンメニューから[デバイスソフトウェアレポート]へナビゲートもできます。



## 第10章：イベント通知ルール

### トピックの参照先リスト

トピック	参照先：
はじめに	<a href="#">「はじめに」</a> （454 ページ）
イベントルールの追加	<a href="#">「イベントルールの追加」</a> （459 ページ）
イベントルール検索結果	<a href="#">「[イベント通知とレスポンスルール] ページのフィールド」</a> （459 ページ）
イベント通知ルールの新規作成	<a href="#">「[イベント通知とレスポンスルールの新規作成] ページのフィールド」</a> （460 ページ）
イベントルールの変数	<a href="#">「イベントルール変数」</a> （464 ページ）

## はじめに

HP Network Automation (NA) を使用すると、システム内で次のようなイベントが発生したときに、各種アクションを実行できます。

- 実行されているタスク（スナップショット、診断など）
- 電子メール通知の送信
- 電子メール要約の送信
- SNMP トラップの送信
- syslog メッセージの送信

イベントルールは、特定のデバイスグループおよび時刻のすべてまたはいずれかに制限できます。次の表は、用意されている選択可能なイベントを示します。

イベント	説明
承認が拒否されました	ユーザが承認の要求を拒否しました。
承認が付与されました	ユーザがタスクを承認しました。
承認が必要なくなりました	タスクの承認は不要です。
承認が無効化されました	ユーザがタスクの承認を無効化しました。これにより、承認なしでタスクを実行できます。
承認の要求	ユーザが実行前に承認を必要とするタスクを作成しました。
承認タスクが変更されました	ユーザが実行前に承認を必要とするタスクを変更しました。
承認タスクが削除されました	ユーザが承認対象として割り当てたタスクを削除しました。
承認タスクがタイムアウトしました	タスクが割り当てられた時間内で承認されませんでした。
コマンド認可エラー	ユーザが使用権限を持たないコマンドを実行しようとした。
Telnet/SSH同時セッションが無効化されました	ユーザが同時ログインに対する制約を無視しました。別のユーザがすでにログインしているにもかかわらず、ユーザがプロキシ経由でデバイスにログインしました。
ポリシーが追加されました	ユーザが新規構成ポリシーを追加しました。
ポリシーが変更されました	ユーザが構成ポリシーを変更しました。
構成ポリシーに非準拠です	構成変更がポリシールールに違反しました。
ポリシーパターンのタイムアウト	ポリシーパターンが一致するまでの時間が30秒を超過しました。
ポリシールールが追加されました	ユーザが新規構成ルールを追加しました。
ポリシールールが変更されました	ユーザが構成ルールを変更しました。
デバイスアクセスエラー	NAがデバイスにアクセスできません。このエラーは、パスワードが間違っているか、ホストへのルートが存在しなかったことが原因の可能性があります。
デバイスが追加されました	ユーザがデバイスを追加しました。
デバイスがブートしました	デバイスがリブートされました。

イベント	説明
デバイスコマンドスクリプトが正常に終了しました	デバイスコマンドスクリプトが正常に終了しました。
デバイスコマンドスクリプトでエラーが発生しました	デバイスコマンドスクリプトでエラーが発生しました。
デバイス構成の変更	NAがスナップショットタスクの実行中に構成変更を検出しました。
デバイス構成の変更-ユーザなし	NAが不明ユーザによる構成変更を検出しました。
デバイス構成の配布	NAがデバイスに構成を正常に配布しました。
デバイス構成の配布エラー	NAがデバイスへの構成の配布に失敗しました。
デバイスデータエラー	NAがデータベースへの構成または診断出力の保存に失敗しました。
デバイスが削除されました	ユーザがデバイスを永久に削除しました。
デバイス診断が変化しました	診断の結果が前回の結果と異なっています。
デバイス診断が正常に終了しました	デバイス診断が正常に終了しました。
デバイス診断でエラーが発生しました	デバイス診断に失敗しました。
デバイスが編集されました	ユーザがデバイス情報を変更しました。
デバイスのフラッシュ記憶域が十分ではありません	デバイスのフラッシュ記憶域が少なくなっています。
デバイスグループが追加されました	ユーザがデバイスグループを追加しました。
デバイスグループが削除されました	ユーザがデバイスグループを削除しました。
デバイスグループが変更されました	ユーザがデバイスグループを変更しました。
デバイスにアクセスできません	デバイスがアクセス不能です。
デバイスが管理対象になりました	ユーザがデバイスをアクティブとしてマークしました。
インポートにデバイスがありません	定期的なインポートタスクの実行時にインポート対象のデバイスのファイルを指定した際、前回のインポートでファイルに含まれていたデバイスが今回のインポートではファイルに含まれていないと、このイベントが発生します。
デバイスパスワードの変更	ユーザがパスワード変更を配布しました。
デバイスパスワードの変更エラー	NAがデバイスパスワード変更の配布に失敗しました。
デバイス権限-変更	デバイスがグループに追加されたか、グループから削除されました。これにより、ユーザがデバイスを変更できる権限が変更されました。
デバイス権限-デバイスの新規作成	誰かがデバイスグループに新規デバイスを追加しました。これにより、そのデバイスグループに関連するユーザの権限が変更されました。
デバイスのリロードに失敗しました	デバイスのリロードに失敗しました。
デバイス予約の競合	デバイス予約の競合が発生しました。

イベント	説明
デバイスのスナップショット	NAが構成変更対象のデバイスを確認しました。
デバイスソフトウェアの変更	NAがデバイス上に新しいOSバージョンを検出しました（例：IOS 11からIOS 12）。
デバイスのスタートアップとランニング構成の差異	NAがスタートアップ構成と実行構成の間に差異を検出しました。
デバイスが管理解除されました	ユーザがデバイスを非アクティブとしてマークしました。特定の期間に到達できない場合は、インポートされたデバイスを非アクティブにすることもできます。
分散システム-破損したレプリケーションジョブ	NAは、破損したレプリケーションジョブを検出しました。
分散システム-データ同期遅延の警告	NAは、データ同期の遅延の警告を検出しました。
分散システム-遅延LOBがしきい値を超過	NAは、遅延LOBが超過したことを検出しました。
分散システム-デバイスソフトウェアの転送エラー	NAは、デバイスソフトウェア転送エラーを検出しました。
分散システム-修復したレプリケーションジョブ	NAは、修復したレプリケーションジョブを検出しました。
分散システム-RMIエラー	NAは、RMIエラーを検出しました。
分散システム-レプリケーションエラー	NAはレプリケーションエラーを検出しました。
分散システム-停止したマージエージェントジョブ	NAは、停止したマージエージェントジョブを検出しました。
分散システム-時刻同期の警告	NAは、時刻同期の警告を検出しました。
分散システム-削除不可能な異常の生成	NAは、削除不可能な異常の生成を検出しました。
分散システム-一意性の競合	NAは、一意性の競合を検出しました。
電子メールレポートの保存	ユーザが電子メールレポートを保存しました。
外部ディレクトリサーバの認証エラー	NAが外部のLDAP認証サーバに接続できませんでした。
最後に使用したデバイスパスワードが変更されました	デバイスへのアクセスで最後に使用されたパスワードが変更されました。
ライセンス数がほぼ上限です	デバイスにおけるライセンスノードの合計数が90%を超過しています。
ライセンスの期限切れが近づいています	NAライセンスの期限切れが間近になっています（日付ベースのライセンスのみ）。
ライセンス数が超過しました	デバイスにおけるライセンスノードの合計数が上限を超過しています。NAでは20%まで超過が許容されています。
ライセンスの期限が切れました	ライセンスの期限が切れました。これ以降NAにログインできなくなります。ただし、スケジュールされたスナップショットの取得および変更の記録は続行されます。



イベント	説明
モジュールが追加されました	誰かがデバイスにモジュール/ブレード/カードを追加しました。
モジュールが変更されました	誰かがデバイスに設置されているモジュール/ブレード/カードの属性を変更しました。
モジュールが削除されました	誰かがデバイスからモジュール/ブレード/カードを削除しました。
監視エラー	サーバ監視の実行に失敗しました。
監視の正常動作	サーバ監視が正常に実行されました。
保留タスクが削除されました	ユーザがスケジュールされたタスクを実行前に削除しました。
予約デバイス設定が変更されました	ユーザが予約デバイスのデバイス構成を変更しました。
配布予定構成が編集されました	ユーザが配布を予定していた構成を変更しました。
配布予定パスワードが変更されました	新規パスワードが配布されました。ただし、他にもスケジュールされたパスワードの配布タスクが存在します。このイベントは、配布された新規パスワードが、保留中のパスワードの配布タスクが実行されたときに再度変更されることを示します。
セキュリティアラート	NAは、セキュリティアラートを検出しました。
サーバスタートアップ	NA管理エンジンが起動しました。
セッションデータがキャプチャされました	プロキシが接続セッションをデータベースに保存しました。
ソフトウェア更新に失敗しました	NAがデバイス上のOSソフトウェアの更新に失敗しました。
ソフトウェア更新が正常に終了しました	NAがデバイス上のOSソフトウェアの更新を正常に終了しました。
ソフトウェアの脆弱性が検出されました	ソフトウェアレベルを「セキュリティリスク」に設定すると、NAがデバイスのスナップショットを取得し、かつ「セキュリティリスク」として見なされるOSバージョンを検出したときに、このイベントが生成されます。
サマリレポートが生成されました	ユーザがサマリレポートを生成しました。
タスクが完了しました	タスクが完了しました。
タスクが開始しました	タスクが開始されました。
チケットが作成されました	HP Remedy AR System Connector（またはサードパーティのチケットシステムと接続するHP Connector）を使用している場合、このイベントは、NAが対象サードパーティのチケットシステムにチケットを作成したことを示します。
ユーザが追加されました	ユーザが追加されました。
ユーザ認証エラー	ユーザがNAへのログイン時に間違ったパスワードを入力しました。
ユーザ認証エラーによるロックアウト	連続して何回もログインに失敗したため、ユーザがロックされています。
ユーザが削除されました	ユーザが削除されました。

イベント	説明
ユーザが無効になりました	ユーザレコードが編集されました。そのため、ユーザのステータスが有効から無効に変更されています。
ユーザが有効になりました	ユーザレコードが編集されました。そのため、ユーザのステータスが無効から有効に変更されています。
ユーザログイン	ユーザがNAにログインしました。
ユーザログアウト	ユーザがNAからログアウトしました。
ユーザメッセージ	ユーザが[メッセージの新規作成]リンクをクリックしてメッセージを作成しました。
ユーザ権限が変更されました	ユーザの権限が変更されました。

## イベントルールの追加

イベント通知ルールを追加するには、[管理]のメニューバーにある[イベント通知とレスポンスルール]をクリックします。[イベント通知とレスポンスルール]ページが開きます。このページには、現在定義されているルールが表示されます。これらのルールは、NA イベントによって実行されます。ポンド符号（#）の付いたイベントルールは非アクティブです。

**注意：** 管理ユーザはすべてのイベントルールを参照することができますが、それ以外のユーザは各自のイベントルールしか参照することができません。

## [イベント通知とレスポンスルール]ページのフィールド

フィールド	説明/アクション
[イベント通知とレスポンスルールの新規作成]リンク	[イベント通知とレスポンスルールの新規作成]ページが開きます。詳細については、「 <a href="#">[イベント通知とレスポンスルールの新規作成]ページのフィールド</a> 」（460ページ）を参照してください。
ルール名	イベントルール名が表示されます。
パーティション	セキュリティや業務上の理由でパーティションを作成した場合、パーティションに従ってイベントルールを分割できます。イベントルールがすべてのパーティションで利用できる場合、構成に応じてイベントルールは[共有]（または[グローバル]）と表示されます。適切な権限がない場合、イベントルールの編集や削除を実行できません。パーティションの作成の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」（148ページ）を参照してください。
アクション	イベントルールによって実行されるアクションが表示されます。次のアクションがあります。 <ul style="list-style-type: none"> <li>• タスクを実行</li> <li>• 電子メールを送信</li> <li>• SNMPトラップを送信</li> <li>• 電子メールの要約に追加</li> <li>• syslogメッセージを送信</li> </ul>
作成者	イベントルールの所有者が表示されます。
アクション	次のオプションから選択できます。 <ul style="list-style-type: none"> <li>• 編集：[イベント通知とレスポンスルールを編集]ページが開きます。このページでは、イベントルールを編集できます。詳細については、「<a href="#">[イベント通知とレスポンスルールの新規作成]ページのフィールド</a>」（460ページ）を参照してください。</li> <li>• 削除：削除してよいかを確認する確認ウィンドウが開きます。このオプションは、ユーザがイベントルールの削除権限を持っている場合にのみ表示されます。</li> </ul>

## [イベント通知とレスポンスルールの新規作成]ページのフィールド

[イベント通知とレスポンスルールの新規作成]ページでは、新しいイベント通知とレスポンスルールを追加および編集できます。

1. [管理]のメニューバーにある[イベント通知とレスポンスルール]をクリックします。[イベント通知とレスポンスルール]ページが開きます。
2. ページ上部の[イベント通知とレスポンスルールの新規作成]リンクをクリックします。[イベント通知とレスポンスルールの新規作成]ページが開きます。

フィールド	説明/アクション
電子メールとイベントのルールを次の名前を追加	イベントルール名を入力します。
このアクションを実行	<p>次のオプションのいずれかを選択します。(注意: 選択するオプションに応じてページが更新され、アクションに合った特定のフィールドが表示されます)。</p> <ul style="list-style-type: none"> <li>• タスクを実行: 「[タスクの実行]アクション」(461 ページ) を参照してください。</li> <li>• 電子メールの要約を送信: 「[電子メールの要約を送信]アクション」(461 ページ) を参照してください。</li> <li>• 電子メールメッセージを送信: 「[電子メールメッセージを送信]アクション」(462 ページ) を参照してください。</li> <li>• SNMP トラップを送信: 「[SNMP トラップを送信]アクション」(462 ページ) を参照してください。</li> <li>• syslog メッセージを送信: 「[syslog メッセージを送信]アクション」(463 ページ) を参照してください。</li> <li>• 作成/チケットへの追加: 「作成/チケットへの追加」(463 ページ) を参照してください。</li> </ul>
以下のイベントが発生するとき	<p>イベントリストから1つまたは複数のイベントを選択します。[Ctrl]キーとクリックまたは[Shift]キーとクリックを使用すると、複数のイベントを選択できます。イベントルールの説明については、「はじめに」(454 ページ) を参照してください。[ポリシーに非準拠です]イベントを選択した場合は、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 任意の重要度: このオプションを選択すると (デフォルト)、違反構成ポリシールールの重要度に関係なく、イベントルールが実行されます。構成ポリシールールの重要度の設定方法については、「[ルールの新規作成]ページのフィールド」(420 ページ) を参照してください。</li> <li>• 少なくとも&lt;重要度: 重要、高、中 (デフォルト)、低、または情報の中から選択できます。イベントルールは、重要度が選択した重要度以上になっている構成ポリシールールのエラーが原因でイベントが生成された場合にのみ実行されます。構成ルールの重要度の設定方法については、「[ルールの新規作成]ページのフィールド」(420 ページ) を参照してください。</li> <li>• 全ポリシー用: このオプションを選択すると (デフォルト)、すべての構成ポリシーが確認されます。</li> <li>• 選択したポリシー用: リストから1つまたは複数の構成ポリシーを選択します。[Shift]キーとクリックまたは[Ctrl]キーとクリックを使用すると、複数の構成ポリシーを選択できます。</li> </ul> <p>[デバイスコマンドスクリプトが正常に終了しました]イベントまたは[デバイスコマンドスクリプトでエラーが発生しました]イベントを選択した場合は、ドロップダウンメニューからコマンドスクリプトを選択できます。[デバイス診断が変化しました]イベントまたは[デバイス診断が正常に終了しました]イベントを選択した場合は、ドロップダウンメニューから診断を選択できます。</p>
ルールのステータス	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• アクティブ: オンにすると (デフォルト)、イベントが発生したときにイベントルールが実行されます。</li> <li>• 非アクティブ: オンにすると、イベントルールが実行されません。このオプションを使用すると、イベントルールを一時的にオフにできます。</li> </ul>

フィールド	説明/アクション
～から～の間	オンにした場合は、時間範囲を指定し、イベントルールの開始時間と終了時間を選択します。
このサイトのデバイス上	パーティションが有効である場合、ドロップダウンメニューからパーティションを選択します。パーティションの作成の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」(148ページ)を参照してください。
これらのグループ内のデバイス上	オンにした場合は、リストから1つまたは複数のグループを選択します。

[イベント通知とレスポンスルールの新規作成]ページの下部は、選択したアクションに応じて異なります。

#### [タスクの実行]アクション

イベントが発生したときに、何らかのNAタスクを実行できます。たとえば、スナップショットの取得、診断の保存、コマンドスクリプトの実行、外部アプリケーションの起動などを実行できます。さらに、イベント変数を外部アプリケーションのコマンドラインに転送することもできます。これにより、NAをカスタマイズし、ニーズに合った独自の操作を設定できます。

待機                      タスクが実行されるまでの待機時間（秒数、分数、時間数、または日数）を入力します。

タスク                      ドロップダウンメニューから実行するタスクを選択します。

#### [電子メールの要約を送信]アクション

電子メールの要約によって、複数のNAイベントが定期的に送信される単一の電子メールレポートにまとめられます。電子メールの要約を使用すると、ユーザに共通のシステムイベント（構成変更や、デバイスの追加、削除、および変更のアクティビティなど）を通知できます。

電子メールボリュームの最小化時に、興味のあるイベントの要約を迅速にスキャンできます。各ユーザが所有できる電子メールの要約は1つのみです。ユーザは複数のイベントルールを設定できます。各ルールによって、さまざまなイベントのセットが要約に送られます。

**注意:** 複数の電子メール要約を異なるスケジュールまたは受信者リストで使用する場合は、適切な要約ルールの定義のみを目的とするユーザを作成します。

すべての要約の送信を開始する時間                      NAが電子メールの要約を送信する時刻を入力します。

反復の間隔（時間）                      NAが電子メールの要約を送信する間隔を入力します。たとえば、「6」を入力すると、6時間ごとに要約が送信されます。

差出人                      送信者の電子メールアドレスを入力します。デフォルト値はNAです。

宛先                      受信者の電子メールアドレスを入力します。アドレスが複数の場合は、必ずカンマで区切ってください。注意：変数が\$EventUserEmail\$に設定されている場合、電子メールアドレスは電子メールの要約を作成したユーザに基づきます。そのため、ユーザの電子メールアドレスが変更されると、変更後の新しい電子メールアドレスが使用されます。

件名                      メッセージの件名を入力します。

メッセージヘッダー                      メッセージヘッダーを入力します。これは、メッセージのヘッダーセクションまたはサマリセクションを開始するテキストです。HTMLメッセージの場合、そのほとんどが番号付きリストタグ<ol>です。

サマリの終了                      メッセージのヘッダーセクションまたはサマリセクションを終了するテキストを入力します。HTMLメッセージの場合、そのほとんどが番号付きリスト終了タグ</ol>です。

フィールド	説明/アクション
メッセージフッター	メッセージフッターを入力します。メッセージフッターは必要に応じて独自に設定できます。たとえば、連絡先情報を入力したり、このメッセージがNAサーバによって送信されされたことを示したりすることができます。
[テキストメッセージ] または[HTMLメッセージ]	[テキストメッセージ]または[HTMLメッセージ]（デフォルト）のいずれかを選択します。[HTMLメッセージ]を選択すると、メールリーダーがメッセージ内のHTMLを解釈できるように、適切なメッセージヘッダーが送信されます。[テキストメッセージ]を選択すると、プレーンテキストメッセージが送信され、HTMLタグはそのまま表示されます。
イベントサマリ	このフィールドには、イベントを簡単に説明したサマリテキストが表示されます。特定のメッセージコンテンツはルールに対して一意です。HTMLメッセージの場合、この行は、通常、リスト項目タグ<li>で始まります。また、追加のHTMLタグおよびNA変数が含まれることがあります。[変数名を表示]リンクをクリックすると、[イベントルールの変数]ウィンドウが開きます。このウィンドウには、使用可能な変数がすべて表示されています。
イベントの詳細	このフィールドには、イベントを詳細に説明するテキスト、変数、およびオプションのHTMLタグが含まれます。

#### [電子メールメッセージを送信]アクション

NAイベントが発生したときに、電子メールメッセージをユーザまたは配信リストに送信できます。各イベントにつき1通の電子メールメッセージが送信されます。このアクションを使用すると、たとえば、コアデバイスの構成を変更したときにすべてのユーザにアラートを発行したり、デバイスがアクセス不能なときにシステム管理者に通知したり、システムイベントのアーカイブをパブリックフォルダに維持したりできます。また、簡単なメッセージを使用してテキストのみのイベントルールを定義し、ポケットベルに電子メールを送信することもできます。

差出人	電子メールメッセージ送信元のユーザやプロセス、および電子メールアドレスを入力します。[変数名を表示]リンクをクリックすると、[イベントルールの変数]ウィンドウが開きます。このウィンドウには、使用可能な変数がすべて表示されています。詳細については、「 <a href="#">イベントルール変数</a> 」（464 ページ）を参照してください。
宛先	メッセージを受信する電子メールアドレスのカンマ区切りリストを入力します。イベントに関連するユーザに電子メールを送信するには、変数\$EventUserEmail\$を使用します。
件名	電子メールメッセージの件名を入力します。変数を使用すると、システム情報を件名に追加できます。
テキストメッセージ	オンにすると、プレーンテキストメッセージが送信されます。HTMLタグはそのまま表示されます。
HTMLメッセージ	オンにすると、メールリーダーがメッセージ内のHTMLを解釈できるように、適切なメッセージヘッダーが送信されます。
テキストとHTMLの両方	オンにすると（デフォルト）、テキストメッセージとHTMLメッセージの両方が送信されます。NAではマルチパート電子メールメッセージが送信されます。電子メールクライアントには、いずれか適切な方の形式が表示されます。たとえば、Outlookの場合は、デフォルトでHTMLが表示されます。メッセージをポケットベル、PDA、または同様のデバイスで受信する場合は、ショートテキストのみのメッセージを使用することをお勧めします。

#### [SNMPトラップを送信]アクション

SNMPトラップは、RFC 1155および1215によって定義されたネットワークステータスメッセージです。このアクションは、NAイベントが発生したときにSNMPトラップを送信するために使用します。たとえば、スナップショットを取得するたびにSNMPトラップをネットワーク管理システム（NMS）に送信できます。トラップを正しく表示するには、まず、NA Management Information Base（MIB）をロードする必要があります。このMIBによってメッセージ形式を定義します。（**注意**：SNMPトラフィックがルータ、ファイアウォール、および他のネットワークデバイスを通じてできるようにネットワークを構成する必要があります）。

SNMPトラップレシーバの ホスト名	DNS名またはホストのIPアドレスを入力します。
-----------------------	--------------------------

フィールド	説明/アクション
SNMPトラップレシーバのポート	SNMPトラップを受信するホストポートを入力します。[デフォルトのポートを使用]リンクをクリックした場合は、デフォルトのポート番号が入力されます。標準のSNMPポートは162です。
SNMPコミュニティ文字列	SNMPトラップを送信するときに使用するコミュニティ文字列を入力します。受信者がこの文字列を受け入れるように構成する必要があります。[デフォルトのコミュニティ文字列の使用]リンクをクリックした場合は、デフォルトのコミュニティ文字列である[public]が入力されます。
SNMPのバージョン	使用するSNMPのバージョンv1（デフォルト）またはv2を選択します。
イベントの説明	イベントの説明を入力します。NA変数を組み込むことができます。[変数名を表示]リンクをクリックすると、[イベントルールの変数]ウィンドウが開きます。このウィンドウには、使用可能な変数がすべて表示されています。詳細については、「 <a href="#">イベントルール変数</a> 」(464ページ)を参照してください。
重要度	次のオプションのいずれかを選択して、イベントの重要度を指定します。各イベントに関連する固有の重要度レベルはないため、理にかなった任意の値を割り当てることができます。 <ul style="list-style-type: none"> <li>• アラート</li> <li>• 重要</li> <li>• デバッグ</li> <li>• 緊急</li> <li>• エラー</li> <li>• 情報</li> <li>• 通知</li> <li>• 警告</li> </ul>
<b>[syslogメッセージを送信]アクション</b>	
syslogメッセージを使用すると、任意のNAイベントを外部管理システムに転送できます。たとえば、NAがデバイス構成変更を検出したときにCA UniCenterシステムに通知して、運用コンソールのアラートを表示することができます。	
Syslogホスト名	syslogサーバのホスト名を入力します。
Syslogポート	syslogが使用するポートを入力します。[デフォルトのポートを使用]リンクをクリックした場合は、デフォルトのsyslogポートである514が入力されます。
Syslogメッセージ	変数などを含むsyslogメッセージを入力します。[変数名を表示]リンクをクリックすると、[イベントルールの変数]ウィンドウが開きます。このウィンドウには、使用可能な変数がすべて表示されています。詳細については、「 <a href="#">イベントルール変数</a> 」(464ページ)を参照してください。
<b>作成/チケットへの追加</b>	
チケットシステムのホスト名	チケットシステムのホスト名を入力します。
イベントの説明	イベントの説明を入力します。

終了したら、必ず[ルールを保存]をクリックしてください。

## イベントルール変数

次に示すイベントでは、複数のイベントルール変数を使用できます。

- デバイスイベント
- デバイス構成イベント
- デバイス診断イベント
- タスクイベント
- すべてのイベント

### デバイスイベントの変数

**注意：** 変数では大文字と小文字が区別されます。正しく入力する必要があります。

これらの変数は、デバイスイベントのルールに対してのみ使用できます。

変数	説明
\$DeviceID\$	デバイスに対するNAのID番号。
\$HostName\$	デバイスのホスト名。
\$IPAddress\$	デバイスのプライマリIPアドレス。
\$FQDN\$	デバイスの完全修飾ドメイン名。
\$Vendor\$	デバイスのメーカー。
\$Model\$	デバイスのモデル番号。



## デバイス構成イベントの変数

**注意：** 変数では大文字と小文字が区別されます。正しく入力する必要があります。

これらの変数は、デバイス構成イベントのルールに対してのみ使用できます。

変数	説明
\$DataID\$	最新の構成に対するNAのID番号。
\$Comments\$	構成コメント。
\$Diff\$	構成変更に関するテキストの差異。

## デバイス診断イベントの変数

**注意：** 変数では大文字と小文字が区別されます。正しく入力する必要があります。

これらの変数は、デバイス診断イベントのルールに対してのみ使用できます。

変数	説明
\$CurrentDiag\$	現在の診断のテキスト。
\$PreviousDiag\$	以前の診断のテキスト。
\$Diff\$	現在の診断と以前の診断との間の変更に関するテキストの差異。
\$DataID\$	診断イベントにも使用可能。

## タスクイベントの変数

**注意：** 変数では大文字と小文字が区別されます。正しく入力する必要があります。

これらの変数は、デバイス診断イベントのルールに対してのみ使用できます。

変数	説明
\$ApprovalDate\$	タスク承認日。
\$ApproverEmails\$	タスク承認者の電子メールアドレスのカンマ区切りリスト。
\$ApprovalPriority\$	タスク承認優先度。
\$OriginatorFirstName\$	タスク作成者の名。
\$OriginatorLastName\$	タスク作成者の姓。
\$OriginatorName\$	タスク作成者の名前。
\$TaskName\$	タスク名。
\$TaskComments\$	タスクコメント。
\$TaskDevices\$	タスクにより影響を受けるデバイスのリスト。
\$TaskFrequency\$	タスクの頻度。
\$TaskID\$	タスク識別子。

## すべてのイベントの変数

次の変数は、すべてのイベントのルールで使用できます。変数では、大文字と小文字が区別されます。正しく入力する必要があります。(注意: すべての変数が示されたリストを参照するには、[イベント通知とレスポンスルールの新規作成]ページの[変数名を表示]リンクをクリックします)。

変数	説明
\$AppURL\$	NA へのリンクを電子メールメッセージに直接挿入するために使用する NA のアプリケーション URL ( <i>https://host/</i> など)。
\$EventID\$	このイベントに対する NA の ID 番号。
\$EventType\$	イベントのタイプ。
\$EventDate\$	イベント発生日。
\$EventText\$	イベントの詳細。
\$EventUserFirstName\$	このイベントに関連する NA ユーザの名。(注意: このイベントに関連するユーザがない場合、またはユーザの名が設定されていない場合は、空白にします)。
\$EventUserLastName\$	このイベントに関連する NA ユーザの姓。(注意: このイベントに関連するユーザがない場合、またはユーザの姓が設定されていない場合は、空白にします)。
\$EventUserName\$	このイベントに関連する NA ユーザ名 (場合によっては「ユーザなし」)。
\$EventUserEmail\$	このイベントに関連するユーザの電子メールアドレス。
\$FyiEmails\$	タスク FYI 受信者の電子メールアドレスのカンマ区切りリスト。
\$LocalHostName\$	NA サーバのホスト名。
\$LocalHostAddress\$	NA サーバの IP アドレス。



# 第11章：検索の実行

## トピックの参照先リスト

検索	参照先：
構成テキストの検索	<a href="#">「全文検索機能の使用」</a> （470 ページ）
デバイスの検索	<a href="#">「デバイスの検索」</a> （472 ページ）
インターフェイスの検索	<a href="#">「インターフェイスの検索」</a> （480 ページ）
モジュールの検索	<a href="#">「モジュールの検索」</a> （483 ページ）
ポリシーの検索	<a href="#">「ポリシーの検索」</a> （486 ページ）
準拠の検索	<a href="#">「ポリシー、ルール、および準拠の検索」</a> （489 ページ）
構成の検索	<a href="#">「[構成を検索]ページのフィールド」</a> （494 ページ）
診断の検索	<a href="#">「診断の検索」</a> （498 ページ）
タスクの検索	<a href="#">「タスクの検索」</a> （502 ページ）
セッションの検索	<a href="#">「セッションの検索」</a> （508 ページ）
イベントの検索	<a href="#">「イベントの検索」</a> （512 ページ）
イベントの説明	<a href="#">「イベントの説明」</a> （515 ページ）
ユーザの検索	<a href="#">「ユーザの検索」</a> （520 ページ）
ACLの検索	<a href="#">「ACLの検索」</a> （522 ページ）
MACアドレスの検索	<a href="#">「MACアドレスの検索」</a> （526 ページ）
IPアドレスの検索	<a href="#">「IPアドレスの検索」</a> （530 ページ）
VLANの検索	<a href="#">「VLANの検索」</a> （533 ページ）
デバイステンプレートの検索	<a href="#">「デバイステンプレートの検索」</a> （536 ページ）
シングルサーチ	<a href="#">「シングルサーチ」</a> （539 ページ）
詳細検索	<a href="#">「詳細検索」</a> （542 ページ）

## 全文検索機能の使用

全文検索を有効にした後、次のレポートオプションで構成テキストの検索を高速化できます。

- [レポート]>[検索]>[デバイス]>[構成テキスト]>[含む（全文）]
- [レポート]>[検索]>[構成]>[構成テキスト]>[含む（全文）]
- [レポート]>[検索]>[デバイステンプレート]>[構成テキスト]>[含む（全文）]
- [レポート]>[詳細検索]>[検索条件]>[構成テキスト]>[含む（全文）]

また、[検索条件]>[構成テキスト]>[含む（全文）]の検索結果に基づき、動的グループを作成できます。

同様に、これらの検索では、[含まない（全文）]構成テキストの検索もできます。[含む（全文）]および[含まない（全文）]演算子による検索では、大文字小文字が常に区別されません。これらの演算子でサポートされる検索タイプの詳細については、表「[含む（全文）]と[含まない（全文）]の使用」を参照してください。

[含む（全文）]と[含まない（全文）]の使用

検索タイプ	注意	例
1つの単語を検索	単語はスペースを含まない一連の文字	<ul style="list-style-type: none"> <li>• interface</li> <li>• telnet</li> <li>• snmp</li> </ul>
ワイルドカードを使用して1つの単語を検索	使用できるワイルドカードはアスタリスク文字（*）のみ。ワイルドカードは検索フレーズの最後に置く必要があります。	<ul style="list-style-type: none"> <li>• interf*</li> <li>• tel*</li> </ul>
IPアドレスを検索	IPアドレス検索は、1つの単語の検索と同じように扱われます。使用できるワイルドカードはアスタリスク文字（*）のみ。ワイルドカードは検索フレーズの最後に置く必要があります。	<ul style="list-style-type: none"> <li>• 10.11.12.13とすると、完全に一致するアドレス</li> <li>• 10.11.12.*とすると、10.11.12で始まるすべてのアドレス</li> <li>• 10.11.*とすると、10.11で始まるすべてのアドレス</li> <li>• fe80:0000:0000:0000:0202:b3ff:fe1e:8329とすると、完全に一致するアドレス</li> <li>• fe80:0000:0000:0000:0202:b3ff:fe1e:*とすると、fe80:0000:0000:0000:0202:b3ff:fe1eで始まるすべてのアドレス</li> <li>• fe80:0000:0000:0000:0202:b3ff:*とすると、fe80:0000:0000:0000:0202:b3ffで始まるすべてのアドレス</li> </ul>
1つのフレーズを検索	フレーズは1つ以上のスペースを含む一連の文字	<ul style="list-style-type: none"> <li>• set vlan</li> <li>• set vpn name</li> </ul>

## [含む（全文）]と[含まない（全文）]の使用（続き）

検索タイプ	注意	例
ワイルドカードを使用して1つのフレーズを検索	<ul style="list-style-type: none"> <li>• 使用できるワイルドカードはアスタリスク文字（*）のみ。ワイルドカードは検索フレーズ内の1つ以上の完全な単語を表す必要があります。</li> <li>• *は検索フレーズの最後に置いてはなりません。</li> <li>• *の前後にスペースを使用します。スペースがない場合、NAは検索をワイルドカードを使用した単語として扱います。</li> </ul>	<ul style="list-style-type: none"> <li>• set * name</li> <li>• telnet * table * settings</li> </ul> <p><b>注意：</b>論理演算子（AND、OR、NOT、ACCUM、EQUIV）はサポートされておらず、検索文字列の一部とは見なされません。</p>

## デバイスの検索

デバイス検索では、条件と演算子の組み合わせを使用することで、デバイスを検索できます。指定したポリシーまたはルールに準拠していないデバイスも検索できます。（ポリシーの詳細については、「[ポリシーの作成](#)」（414ページ）を参照してください）。

デバイスを検索するには、[レポート]のメニューバーにある[検索]を選択し、[デバイス]をクリックします。[デバイスを検索]ページが開きます。検索基準を入力し終わったら、[検索]ボタンをクリックします。[デバイスの検索結果]ページに、指定した検索条件のすべてを含むデバイスのリストが表示されます。詳細については、「[\[デバイスの検索結果\]ページのフィールド](#)」（478ページ）を参照してください。

**注意：** 検索条件の入力後、検索を実行する前に別のページに移動すると、条件の設定が失われます。



## [デバイスを検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、[デバイス検索結果]ページに表示する情報を選択できます。
ホスト名	<p>演算子を選択し、ホスト名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul> <p>ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。 *は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。（注 意：ワイルドカードは「等しい」および「等しくない」演算子と併用できません。）</p>
デバイスIP	演算子を選択し、デバイスのIPアドレスを入力します。
セカンダリIPアドレス	演算子を選択し、デバイスのセカンダリIPアドレスを入力します。
デバイスのベンダー	演算子を選択し、デバイスを製造したベンダー名を入力します。
デバイスモデル	演算子を選択し、デバイスのモデル名を入力します。
デバイスタイプ	スクロールダウンメニューから、ネットワークデバイスのタイプ（ルータ、スイッチ、ファイアウォール、VPN、仮想スイッチ、ダイヤルアップ、DSL_ISDN、WAN、ワイヤレスAP、ロードバランサなど）を選択します。
デバイスステータス	<p>デバイスについて、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• アクティブ</li> <li>• 非アクティブ</li> <li>• 実稼働前（実稼働前デバイスとは、運用ネットワーク内でまだ動作していないデバイスのことです。詳細については、「<a href="#">ベアメタルプロビジョニング</a>」（116ページ）を参照してください。）</li> </ul>
ドライバ名	スクロールダウンメニューから、デバイスに関連するドライバを1つ以上選択します。複数のドライバを選択するには、1つめのドライバを選択し、Ctrlキーとクリックを使用して追加のドライバを選択します。
FQDN	演算子を選択し、完全修飾ドメイン名（FQDN）を入力します。

フィールド	説明/アクション
ポリシー準拠	<p>デバイスについて、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 任意（デフォルト）</li> <li>• 準拠したデバイス</li> <li>• 準拠しないデバイス</li> <li>• 適用できるポリシーがデバイスにない</li> <li>• ルール優先度で非準拠：ドロップダウンメニューからルール優先度を選択します。重要、高、中、低、情報を選択できます。これにより、指定の重要度を越えた、構成ルールの違反状態にあるデバイスのみが含まれるように検索をフィルタリングできます。（構成ポリシールールの重要度の詳細については、「<a href="#">[ルールの新規作成] ページのフィールド</a>」（420 ページ）を参照してください）。</li> <li>• 選択されたポリシーに非準拠：リストから1つまたは複数のポリシーを選択します。</li> <li>• 選択されたルールに非準拠：リストから1つまたは複数のルールを選択します。（ポリシールールの詳細については、「<a href="#">[ルールの新規作成] ページのフィールド</a>」（420 ページ）を参照してください）。</li> </ul>
アクセス方法	<p>スクロールダウンメニューからアクセス方法を選択します。選択可能なオプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• FTP</li> <li>• RLogin</li> <li>• SCP</li> <li>• SNMP</li> <li>• SSH</li> <li>• TFTP</li> <li>• Telnet</li> </ul>
デバイスの場所	演算子を選択し、デバイスの場所を入力します。
シリアル番号	演算子を選択し、デバイスのシリアル番号を入力します。
資産タグ	演算子を選択し、デバイス資産タグからの情報を入力します。
デバイスソフトウェアのバージョン	演算子を選択し、デバイス上で実行されているオペレーティングシステムのバージョン番号を入力します。
デバイスのファームウェアバージョン	演算子を選択し、デバイス上で実行されているファームウェアのバージョン番号を入力します。
デバイスの説明	演算子を選択し、説明を入力します。
コメント	<p>演算子を選択し、デバイスに関するコメントの一部（一意的な内容）を入力します。</p> <p>ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p>
空きポート	演算子（「等しい」、「未満」、または「超過」）を選択し、空きポート数を入力します。
空きポートの割合	演算子（「等しい」、「未満」、または「超過」）を選択し、空きポートの割合を入力します。

フィールド	説明/アクション
合計ポート数	演算子（「等しい」、「未満」、または「超過」）を選択し、デバイス上の合計ポート数を入力します。
使用中のポート	演算子（「等しい」、「未満」、または「超過」）を選択し、使用中のポート数を入力します。
使用中のポートの割合	演算子（「等しい」、「未満」、または「超過」）を選択し、使用中のポートの割合を入力します。
システムメモリ	演算子（「等しい」、「未満」、または「超過」）を選択し、デバイス上の合計RAM容量（MB）を入力します。
アップタイム	演算子（「未満」、または「超過」）を選択し、合計日数を入力します。デバイスが最後にリブートされてからの日数、時間、分数、秒数の合計数が、[デバイスの検索結果]ページに表示されます。  <b>注意:</b> アップタイムデータは、NAデバイスのブート検出診断中に収集されます。アップタイムデータの信頼性を高めるには、反復診断タスクを適切に実行して、定期的にこのデータを収集する必要があります。デバイスによっては、NAデバイスのブート検出診断をサポートしていないものもあります。診断をサポートしていないデバイスや、診断を実行できないデバイスでは、[アップタイム]および[アップタイムの保存日]のフィールドは空欄になります。診断の実行タスクの詳細については、「 <a href="#">[診断の実行]タスクページのフィールド</a> 」（310 ページ）を参照してください。
アップタイムの保存日	演算子（「次の日時以降」または「次の日時以前」）を選択し、プルダウンメニューから時間枠を選択します。「時間指定なし」がデフォルトです。カレンダーオプションを使用すると、特定の日を選択できます。NAデバイスのブート検出診断を最後に実行した時刻が、[デバイスの検索結果]ページに表示されます。NAデバイスのブート検出診断の詳細については、「 <a href="#">表示メニューオプション</a> 」（201 ページ）を参照してください。  <b>注意:</b> アップタイムデータは、NAデバイスのブート検出診断中に収集されます。アップタイムデータの信頼性を高めるには、反復診断タスクを適切に実行して、定期的にこのデータを収集する必要があります。デバイスによっては、NAデバイスのブート検出診断をサポートしていないものもあります。診断をサポートしていないデバイスや、診断を実行できないデバイスでは、[アップタイム]および[アップタイムの保存日]のフィールドは空欄になります。

フィールド	説明/アクション
構成テキスト	<p>演算子を選択し、検索するデバイス構成ファイルの一部（一意的な内容）を入力します。</p> <ul style="list-style-type: none"> <li>• 「含む」、「含まない」演算子では、ワイルドカードとして?および*を含む正規表現を使用できます。ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、これらの検索では大文字小文字が区別されます。</li> <li>• 「含む（全文）」および「含まない（全文）」演算子では、ワイルドカードとして*のみ使用できます。詳細については、「<a href="#">全文検索機能の使用</a>」（470ページ）を参照してください。これらの検索では、大文字小文字が常に区別されません。 （<b>注意</b>：これらの演算子を使用するには、データベースで全文検索が有効になっている必要があります）。</li> <li>• IPv6 アドレスの簡略表記（二重コロン）とワイルドカードを組み合わせて使用することはできません。</li> </ul> <p>検索演算子を「含む」または「含む（全文）」にする場合は、ページの最下部にある[一致した行の前後&lt;#&gt;コンテキスト行を表示]テキストボックスに値を入力します。結果ページに表示される検索テキストの前後に最大5行まで行を追加できます。デフォルト値は3です。（<b>注意</b>：ロード対象の結果が大量にある場合、コンテキスト行を表示するとパフォーマンスが大幅に低下することがあります。）</p>
異なるスタートアップとランニング構成	<p>オンにすると、スタートアップとランニング構成が異なるデバイスが検索されます。</p>
最終変更時間	<p>次の演算子を選択します。</p> <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」（これを選択するとカレンダーが開きます）、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意</b>：カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>
作成日	<p>次の演算子を選択します。</p> <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」（これを選択するとカレンダーが開きます）、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意</b>：カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>
パスワードルール	<p>演算子を選択し、パスワードルーン名を入力します。</p>
ACL ID	<p>演算子を選択し、ACLのIDを入力します。</p>
ACLハンドル	<p>演算子を選択し、ACLハンドルを入力します。</p>
ACLタイプ	<p>演算子を選択し、ACLタイプを入力します。</p>
ACL構成	<p>演算子を選択し、ACLタイプを入力します。</p> <p>ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p>
ACLアプリケーション	<p>演算子を選択し、ACLアプリケーションを入力します。</p> <p>ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p>

フィールド	説明/アクション
モジュールスロット	演算子を選択し、モジュールのスロットを入力します。
モジュールの説明	演算子を選択し、モジュールの説明を入力します。
モジュールモデル	演算子を選択し、モジュールモデルを入力します。
モジュールシリアル	演算子を選択し、モジュールシリアルを入力します。
モジュールメモリ	演算子を選択し、モジュールメモリを入力します。
モジュールのファームウェアバージョン	演算子を選択し、モジュールのファームウェアバージョンを入力します。
モジュールハードウェアの更新バージョン	演算子を選択し、モジュールハードウェアの説明を入力します。
ROMバージョン	演算子を選択し、モジュールのROMバージョンを入力します。ROMバージョンとは、デバイスにオペレーティングシステムのブートおよびロード方法を指示するために、ROMで使用されるブートストラップコードのバージョンです。
サービスタイプ	演算子を選択し、サービスタイプを入力します。
カスタムサービスタイプ	演算子を選択し、カスタムサービスタイプを入力します。
VTP ドメイン名	演算子を選択し、VLAN トランッキングプロトコル (VTP) ドメイン名を入力します。
VTP 動作モード	演算子を選択し、VLAN トランッキングプロトコル (VTP) 動作モードを入力します。
デバイスのカスタムデータ	演算子を選択し、表示されるカスタムフィールドのいずれかに示される一意のテキストを入力します。 <b>(注意: このセクションは、カスタムフィールドがない場合は表示されません。)</b>
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• 選択グループ内のいずれか (デフォルト)</li> <li>• 選択グループのすべて</li> <li>• 選択グループになし</li> </ul> <p><b>注意:</b> デバイスセクタを使用してグループを選択します。デバイスセクタの使用方法の詳細については、「<a href="#">デバイスセクタ</a>」(142 ページ) を参照してください。</p>
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション (名前はデフォルトサイト) には、当初、すべてのインベントリが含まれます。<b>(注意: このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」(156 ページ) を参照してください。)</b></p>

[検索] ボタンをクリックすると、[デバイスの検索結果] ページに、指定した検索条件のすべてを含むデバイスのリストが表示されます。詳細については、「[\[デバイスの検索結果\] ページのフィールド](#)」(478 ページ) を参照してください。

## [デバイスの検索結果]ページのフィールド

[デバイスの検索結果]ページの表示は、[デバイスを検索]ページで選択した検索条件によって異なります。検索条件の詳細については、[「\[デバイスを検索\]ページのフィールド」\(473ページ\)](#)を参照してください。次の表は、[デバイスの検索結果]ページに用意されているオプションを示します。

オプション	説明/アクション
この検索を変更	[デバイスの検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
チェックボックス	<p>左側のチェックボックスをオンにすると、デバイスを管理できます。デバイスを選択したら、[アクション]ドロップダウンメニューをクリックし、次のいずれかをクリックします。</p> <ul style="list-style-type: none"> <li>• アクティブ化：選択したデバイスを管理するようにNAに指示します。</li> <li>• 非アクティブ化：選択したデバイスを管理しないようにNAに指示します。</li> <li>• 一括編集：[一括編集]ページが開きます。<a href="#">「[デバイスを一括編集]ページのフィールド」(161ページ)</a>を参照してください。</li> <li>• ダイアグラム：<a href="#">「ダイアグラム」(603ページ)</a>を参照してください。</li> <li>• 削除：選択したデバイスが削除されます。</li> <li>• ポリシー準拠の確認：<a href="#">「[ポリシー準拠の確認]タスクページのフィールド」(372ページ)</a>を参照してください。</li> <li>• Syslogの構成：<a href="#">「[Syslogの構成]タスクページのフィールド」(284ページ)</a>を参照してください。</li> <li>• パスワードの配布：<a href="#">「[パスワードの配布]タスクページのフィールド」(288ページ)</a>を参照してください。</li> <li>• ドライバの検出：<a href="#">「[ドライバの検出]タスクページのフィールド」(293ページ)</a>を参照してください。</li> <li>• デバイスのリポート：<a href="#">「[デバイスのリポート]タスクページのフィールド」(296ページ)</a>を参照してください。</li> <li>• コマンドスクリプトの実行：<a href="#">「[コマンドスクリプトの実行]タスクページのフィールド」(304ページ)</a>を参照してください。</li> <li>• 診断の実行：<a href="#">「[診断の実行]タスクページのフィールド」(310ページ)</a>を参照してください。</li> <li>• ICMPテストの実行：<a href="#">「[ICMPテストの実行]タスクページのフィールド」(299ページ)</a>を参照してください。</li> <li>• スナップショットの取得：<a href="#">「[スナップショットの取得]タスクページのフィールド」(315ページ)</a>を参照してください。</li> <li>• スタートアップとランニングの同期：<a href="#">「[スタートアップとランニングの同期]タスクページのフィールド」(319ページ)</a>を参照してください。</li> <li>• デバイスソフトウェアの更新：<a href="#">「[デバイスソフトウェアの更新]タスクページのフィールド」(323ページ)</a>を参照してください。</li> <li>• ACLの削除：<a href="#">「ACLの削除タスクページ」(708ページ)</a>を参照してください。</li> <li>• OS分析：<a href="#">「[OS分析]タスクページのフィールド」(350ページ)</a>を参照してください。</li> <li>• デバイスのプロビジョニング：<a href="#">「[デバイスの編集]ページのフィールド」(111ページ)</a>を参照してください。</li> </ul> <p>左側にある[選択]ドロップダウンメニューを使用すると、デバイスを全選択または全選択解除できます。</p>

オプション	説明/アクション
アクション	<p>[デバイス検索結果]テーブルのエントリごとに、次のアクションを選択できます。</p> <ul style="list-style-type: none"><li>• <b>編集</b> : [デバイスを編集]ページが開きます。そのページでデバイスの情報を編集できます。</li><li>• <b>Telnet</b> : NA CLIに対する[Telnet]ウィンドウが開きます。NAによってデバイスへのログインが求められます。</li><li>• <b>SSH</b> : NA CLIに対する[SSH]ウィンドウが開きます。NAによってデバイスへのログインが求められます。</li><li>• <b>構成を表示</b> : [現在の構成]ページが開きます。このページでは、構成を編集したり、選択した構成にコメントを追加したりできます。</li></ul>
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"><li>• <b>新規デバイスグループとして指定した名前で保存</b> : [全結果デバイス]または[選択デバイスのみ]を選択し、新規グループ名を入力して、[グループを作成]をクリックします。</li><li>• <b>既存の静的デバイスグループに追加</b> : [全結果デバイス]または[選択デバイスのみ]を選択し、ドロップダウンメニューからデバイスグループを選択して、[追加]をクリックします。</li><li>• <b>検索を指定した名前でユーザレポートとして保存</b> : ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、「<a href="#">ユーザレポートとシステムレポート</a>」(593ページ)を参照してください。</li><li>• <b>検索結果を電子メール送信</b> : 検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li><li>• <b>検索結果をCSVファイルとして表示</b> : 検索結果をCSV形式でダウンロードします。</li></ul>

## インターフェイスの検索

インターフェイス検索を使用すると、デバイスにインストールされているインターフェイスに関する情報について、NAデータベースが検索されます。ポートがレイヤ2で、インターフェイスがレイヤ3であっても、NAはその区別をしません。

デバイスを検索するには、[レポート]のメニューバーにある[検索]を選択し、[インターフェイス]をクリックします。[インターフェイスを検索]ページが開きます。検索基準を入力し終えたら、[検索]ボタンをクリックします。[インターフェイスの検索結果]ページに、指定した検索条件のすべてを含むインターフェイスのリストが表示されます。詳細については、「[\[インターフェイスの検索結果\]ページのフィールド](#)」(482ページ)を参照してください。

**注意：** 検索条件の入力後、検索を実行する前に別のページに移動すると、条件の設定が失われます。

### [インターフェイスを検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、[インターフェイスの検索結果]ページに表示する情報を選択できます。
ポート名	<p>演算子を選択し、「Ethernet0」や「Serial1」などのポート名を入力します。ポートは、バインドとネットワークアドレスの組み合わせとして定義された、単一エンドポイントとして定義します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul>
ポートIP	演算子を選択し、ポートIPを入力します。
CIDR 範囲	演算子を入力し、192.168.1.0-192.168.2.0 や 192.168.31.0/24 のように、Classless Inter-Domain Routing (CIDR) 範囲を入力します。CIDR 範囲は両端の値を含みます。
ポートタイプ	演算子を選択し、「Ethernet」、「FastEthernet」、「PortChannel」などのポートタイプを入力します。
ポートのステータス	演算子を選択し、「Configured Up」や「Administratively Down」などのポートのステータスを入力します。
実行ポートステータス	ポートが、"Configured Up"または"Administratively Down"のどちらであるかを表示します。(注意：これはポートのプロトコルステータスには反映されず、構成ステータスのみに反映されます。)
説明	演算子を選択し、プライベートVLANの説明を入力します。
構成された通信モード	演算子を選択し、ポートの構成された通信モード設定を入力します。
構成された速度	演算子を選択し、ポートの構成された速度設定を入力します。
ネゴシエートされた通信モード	演算子を選択し、ポートの検出された通信モード設定を入力します。



フィールド	説明/アクション
ネゴシエートされた速度	演算子を選択し、ポートの検出された速度設定を入力します。
VLAN名	演算子を選択し、ポートのVLAN名を入力します。VLAN名は、VLAN2やVLAN3などのVLANの名前で、検索の絞り込みに使用します。
ホスト名	演算子を選択し、デバイスのホスト名を入力します。ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。*は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。（ <b>注意</b> ：ワイルドカードは「等しい」および「等しくない」演算子と併用できません。）
デバイスIP	演算子を選択し、デバイスのIPアドレスを入力します。
モジュールスロット	演算子を選択し、モジュールのスロット番号を入力します。
モジュールの説明	演算子を選択し、モジュールの説明を入力します。
モジュールモデル	演算子を選択し、モジュールのモデル番号を入力します。
モジュールシリアル	演算子を選択し、モジュールのシリアル番号を入力します。
モジュールのファームウェアバージョン	演算子を選択し、モジュールのファームウェアバージョンを入力します。
インターフェイスのカスタムデータ	演算子を選択し、表示されるカスタムフィールドのいずれかに示される一意のテキストを入力します。（ <b>注意</b> ：このセクションは、カスタムフィールドがない場合は表示されません。）
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• 選択グループ内のいずれか（デフォルト）</li> <li>• 選択グループのすべて</li> <li>• 選択グループになし</li> </ul> <p><b>注意</b>：デバイスセレクトを使用してグループを選択します。デバイスセレクトの使用方法の詳細については、「<a href="#">デバイスセクタ</a>」（142ページ）を参照してください。</p>
パーティション	パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（ <b>注意</b> ：このフィールドは複数パーティションを構成した場合にのみ表示されます。パーティションの詳細については、「 <a href="#">パーティション</a> 」（156ページ）を参照してください。）

## [インターフェイスの検索結果]ページのフィールド

[インターフェイスの検索結果]ページの表示は、[インターフェイスを検索]ページで選択した検索条件によって異なります。検索条件の詳細については、「[\[インターフェイスを検索\]ページのフィールド](#)」(480ページ)を参照してください。次の表は、[インターフェイスの検索結果]ページに用意されているオプションを示します。

オプション	説明/アクション
この検索を変更	[インターフェイスを検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
チェックボックス	<p>左側のチェックボックスをオンにすると、インターフェイスを選択できます。インターフェイスを選択したら、[アクション]ドロップダウンメニューをクリックし、[インターフェイススクリプトを実行]をクリックします。[タスクの新規作成]-[コマンドスクリプトの実行]ページが開きます。詳細については、「<a href="#">コマンドスクリプトの実行</a>」(590ページ)を参照してください。</p> <p>隣接の[選択]ドロップダウンメニューを使用すると、インターフェイスを全選択または全選択解除できます。</p>
アクション	<p>[インターフェイスの検索結果]テーブルのエントリごとに、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>• インターフェイスを編集 : [インターフェイスの詳細を編集]ページが開きます。そのページでインターフェイスの情報を編集できます。詳細については、「<a href="#">[インターフェイスの詳細を編集]ページのフィールド</a>」(208ページ)を参照してください。</li> <li>• インターフェイスを表示 : [インターフェイスの詳細]ページが開きます。そのページでインターフェイスの詳細を表示できます。詳細については、「<a href="#">[インターフェイスの詳細]ページのフィールド</a>」(206ページ)を参照してください。</li> </ul>
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"> <li>• 検索を指定した名前でユーザレポートとして保存 : ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、「<a href="#">ユーザレポートとシステムレポート</a>」(593ページ)を参照してください。</li> <li>• 検索結果を電子メール送信 : 検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li> <li>• 検索結果をCSVファイルとして表示 : 検索結果をCSV形式でダウンロードします。</li> </ul>

## モジュールの検索

モジュール検索を使用すると、デバイスに設置されているカード、ブレード、またはモジュールに関する情報について、NAデータベースが検索されます。

モジュールを検索するには、[レポート]のメニューバーにある[検索]を選択し、[モジュール]をクリックします。[モジュールを検索]ページが開きます。検索条件を入力して、[検索]ボタンをクリックすると、[モジュールの検索結果]ページに、指定した検索条件のすべてを含むモジュールのリストが表示されます。詳細については、「[ポリシーの検索](#)」(486ページ)を参照してください。

**注意：** 検索条件の入力後、検索を実行する前に別のページに移動すると、条件の設定が失われます。

### [モジュールを検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように[モジュールの検索結果]ページをカスタマイズできます。
ホスト名	<p>演算子を選択し、ホスト名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul> <p>ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。 *は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。（<b>注意：</b>ワイルドカードは「等しい」および「等しくない」演算子と併用できません。）</p>
デバイスIP	演算子を選択し、デバイスのIPアドレスを入力します。
モジュールスロット	演算子を選択し、モジュールが設置されているデバイス上のスロットを入力します。
モジュールの説明	演算子を選択し、モジュールの説明の一部（一意的な内容）を入力します。

フィールド	説明/アクション
モジュールモデル	<p>演算子を選択し、モジュールのモデルを入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul> <p>ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。 *は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。（<b>注意</b>：ワイルドカードは「等しい」および「等しくない」演算子と併用できません。）</p>
モジュールシリアル	演算子を選択し、モジュールのシリアル番号を入力します。
モジュールメモリ	演算子を選択し、モジュールの合計RAM容量（MB）を入力します。
モジュールのファームウェアバージョン	演算子を選択し、モジュールにロードされているファームウェアのバージョン番号を入力します。
モジュールハードウェアの更新バージョン	演算子を選択し、モジュールのハードウェアの更新バージョンの一部を入力します。
コメント	<p>演算子を選択し、モジュールのコメントの一部を入力します。</p> <p>ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p>
モジュールのカスタムデータ	演算子を選択し、表示されるカスタムフィールドのいずれかに示される一意のテキストを入力します。（ <b>注意</b> ：このセクションは、カスタムフィールドがない場合は表示されません。）
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• 選択グループ内のいずれか（デフォルト）</li> <li>• 選択グループのすべて</li> <li>• 選択グループになし</li> </ul> <p><b>注意</b>：デバイスセレクトアを使用してグループを選択します。デバイスセレクトアの使用方法的詳細については、「<a href="#">デバイスセレクトア</a>」（142ページ）を参照してください。</p>
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（<b>注意</b>：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」（156ページ）を参照してください。）</p>

## [モジュールの検索結果]ページのフィールド

[モジュールの検索結果]ページの表示は、[モジュールを検索]ページで選択した検索条件によって異なります。詳細については、「[\[モジュールを検索\]ページのフィールド](#)」(483 ページ)を参照してください。次の表は、[モジュールの検索結果]ページに用意されているオプションを示します。

オプション	説明/アクション
この検索を変更	[モジュールを検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
アクション	<p>[モジュールの検索結果]テーブルのエントリごとに、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>モジュールを編集:[ブレード/モジュール詳細を編集]ページが開きます。このページでは、当該モジュールに関する情報を編集できます。</li> <li>モジュールを表示:[ブレード/モジュール詳細]ページが開きます。このページには、モジュール詳細が表示されます。</li> </ul>
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"> <li>新規デバイスグループとして指定した名前で作成:[全結果デバイス]または[選択デバイスのみ]を選択し、新規グループ名を入力して、[グループを作成]をクリックします。</li> <li>既存の静的デバイスグループに追加:[全結果デバイス]または[選択デバイスのみ]を選択し、ドロップダウンメニューからデバイスグループを選択して、[追加]をクリックします。</li> <li>検索を指定した名前でユーザレポートとして保存:ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、「<a href="#">ユーザレポートとシステムレポート</a>」(593 ページ)を参照してください。</li> <li>検索結果を電子メール送信:検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li> <li>検索結果をCSVファイルとして表示:検索結果をCSV形式でダウンロードします。</li> </ul>

## ポリシーの検索

NA Policy Managerは、NAが検出したデバイス構成変更のそれぞれに対して、ルールやフィルタを適用します。デバイス（またはデバイスグループ）への変更が非準拠である場合は、NA Policy Managerで通知ルールを実行できるイベントを生成します。これにより、準拠とネットワーク可用性の両方を維持しながら、非準拠の変更を修正できます。ポリシー管理の詳細については、「[ポリシーの作成](#)」（414 ページ）を参照してください。自動修正機能の詳細については、「[NA Policy Managerの動作方法](#)」（413 ページ）を参照してください。

[ポリシーを検索]ページでは、表示するポリシーのリストを絞り込めます。これにより、次のことが可能になります。

- ポリシー属性を検索基準として使用することで、NA内のポリシーのリストを容易に生成できます。
- NA内のポリシーを容易に管理できます。

現在のポリシーのすべてを表示するには、メインメニューバーの[ポリシー]下で[ポリシーリスト]をクリックします。詳細については、「[\[ポリシー\]ページのフィールド](#)」（415 ページ）を参照してください。

ポリシーを検索するには、[レポート]のメニューバーにある[検索]を選択し、[ポリシー]をクリックします。[ポリシーの検索]ページが開きます。検索基準を入力し終わったら、[検索]ボタンをクリックします。[ポリシーの検索結果]ページに、指定した検索条件のすべてを含むポリシーのリストが表示されます。

**注意：** 検索条件の入力後、検索を実行する前に別のページに移動すると、条件の設定が失われます。

## [ポリシーの検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように[ポリシーの検索結果]ページをカスタマイズできます。
ポリシー名	<p>演算子を選択し、ポリシー名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul>
デバイスグループ	検索対象のポリシー範囲と一致するデバイスグループを選択します。グループを選択するには、デバイスセクタを使用します。デバイスセクタの使用方法的詳細については、「 <a href="#">デバイスセクタ</a> 」（142 ページ）を参照してください。
作成日	<p>次の演算子を選択します。</p> <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」（これを選択するとカレンダーが開きます）、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意：</b> カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>

フィールド	説明/アクション
ステータス	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• 任意（デフォルト）</li> <li>• アクティブ</li> <li>• 非アクティブ</li> </ul>
CVE	演算子と一緒にCVE（Common Vulnerabilities and Exposures）名を入力します。CVE とは、セキュリティ問題に関する脆弱性やその他の情報に付けられた標準名のリストです。
開示日	次の演算子を選択します。 <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」（これを選択するとカレンダーが開きます）、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意：</b> カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>
解決策	演算子と一緒にソリューション名を入力します。 ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。
ベンダー URL	脆弱性に対するソリューションの詳細に関する、外部参照のURLを演算子とともに入力します。
ソリューションURL	脆弱性に対する見込まれるソリューションの詳細に関する、外部参照のURLを演算子とともに入力します。
ポリシータグ	検索対象のポリシータグを選択します。ポリシータグにより、選択したタグのポリシーに関連する準拠エントリを検索できます。
パーティション	パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（ <b>注意：</b> このフィールドは 1 つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「 <a href="#">パーティション</a> 」（156 ページ）を参照してください。）

## [ポリシーの検索結果]ページのフィールド

[ポリシーの検索結果]ページは、[ポリシーを検索]ページで選択した検索条件を表示します。詳細については、[「\[ポリシーの検索\]ページのフィールド」\(486ページ\)](#)を参照してください。

オプション	説明/アクション
チェックボックス/ドロップダウンメニュー	<p>左側のチェックボックスをオンにすると、デバイスを管理できます。デバイスを選択したら、[アクション]ドロップダウンメニューをクリックし、次のいずれかをクリックします。</p> <ul style="list-style-type: none"> <li>• アクティブ化：選択したデバイスを管理するようにNAに指示します。</li> <li>• 非アクティブ化：選択したデバイスを管理しないようにNAに指示します。</li> <li>• 一括編集：[ポリシーの一括編集]ページが開きます。そのページでは、選択したポリシーの範囲の変更、デバイス例外の追加、およびポリシーステータスの変更を実行できます。</li> <li>• 削除：選択したデバイスが削除されます。</li> </ul>
この検索を変更	[ポリシーを検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
アクション	<p>各ルールで次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>• 表示と編集：[ポリシーを編集]ページが開きます。そのページで、ポリシーを編集できます。</li> <li>• テスト：[ポリシーをテスト]ページが開きます。詳細については、<a href="#">「[ポリシー準拠のテスト]ページのフィールド」(439ページ)</a>を参照してください。</li> </ul>
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"> <li>• 検索を指定した名前でユーザレポートとして保存：ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、<a href="#">「ユーザレポートとシステムレポート」(593ページ)</a>を参照してください。</li> <li>• 検索結果を電子メール送信：検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li> <li>• 検索結果をCSVファイルとして表示：検索結果をCSV形式でダウンロードします。</li> </ul>



## ポリシー、ルール、および準拠の検索

[ポリシー、ルール、および準拠を検索]ページでは、指定したデバイスやデバイスグループに対して、デバイスと関連する準拠、および適用可能なポリシーとルールを検索できます。これにより、次のことが可能になります。

- 準拠、または非準拠のデバイスのリストを容易に生成できます。
- 特定ポリシールールによって確認されたデバイスのリストを容易に生成できます。
- ポリシールールの適用先であるデバイスを特定できます。
- 特定デバイスに適用されているポリシールールを特定できます。
- 適用可能なポリシーが存在しないデバイスを特定できます。

**注意：** デバイスと無関係にポリシーやルールを検索することはできません。

ポリシー、ポリシールール、および準拠違反を検索するには、[レポート]のメニューバーにある[検索]を選択し、[準拠]をクリックします。[ポリシー、ルール、および準拠を検索]ページが開きます。検索基準を入力し終わったら、[検索]ボタンをクリックします。[ポリシー、ルール、および準拠を検索]ページに、指定した検索条件のすべてを含むポリシーのリストが表示されます。

**注意：** 検索条件の入力後、検索を実行する前に別のページに移動すると、条件の設定が失われます。

## [ポリシー、ルール、および準拠を検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように[ポリシーの検索結果]ページをカスタマイズできます。
ホスト名	<p>演算子を選択し、ホスト名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul> <p>ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。 *は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。（注 意：ワイルドカードは「等しい」および「等しくない」演算子と併用できません。）</p>
デバイスIP	演算子を選択し、デバイスのIPアドレスを入力します。
デバイスグループ	デバイスセクタを使用してグループを選択します。デバイスセクタの使用方法的詳細については、「 <a href="#">デバイスセクタ</a> 」(142ページ)を参照してください。
準拠	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• すべての準拠状態</li> <li>• 準拠したデバイス</li> <li>• 準拠しないデバイス</li> <li>• デバイスは未確認です</li> <li>• 適用できるポリシーがデバイスにない</li> </ul>
ポリシー	ポリシーの名前を入力するか、リストからポリシーを選択します。
ルール	ポリシー構成ルールの名前を入力するか、リストから選択します。
ルールタイプ	<p>次の中からオプションを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• 構成</li> <li>• 診断</li> <li>• ソフトウェア</li> </ul>
ルール重要度	<p>重要度レベルを1つ以上選択します。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• 情報：一般的に対処を必要としないイベント。</li> <li>• 低：時間的な余裕がある場合に対処を必要とするイベント。</li> <li>• 中：適時に対処を必要とするイベント（通常は72時間以内）。</li> <li>• 高：緊急の対応を必要とするイベント（通常は24時間以内）。</li> <li>• 重要：即時の対応を必要とするイベント。</li> </ul>
ルールの説明	検索結果にルールの説明を含めます。

フィールド	説明/アクション
CVE	演算子と一緒に CVE（Common Vulnerabilities and Exposures）名を入力します。CVE とは、セキュリティ問題に関する脆弱性やその他の情報に付けられた標準名のリストです。
最終確認日	<p>次の演算子を選択します。</p> <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」（これを選択するとカレンダーが開きます）、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意：</b> カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>
ポリシータグ	ポリシータグを選択します。ポリシータグにより、選択したタグのポリシーに関連する準拠エントリを検索できます。
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（<b>注意：</b> このフィールドは 1 つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」（156 ページ）を参照してください）。</p>

## [ポリシー、ルール、および準拠の検索結果]ページのフィールド

[ポリシー、ルール、および準拠の検索結果]ページのフィールドページは、[ポリシー、ルール、および準拠を検索]ページで選択した検索条件を表示します。詳細については、「[\[ポリシー、ルール、および準拠を検索\]ページのフィールド](#)」(490 ページ) を参照してください。

オプション	説明/アクション
チェックボックス/ドロップダウンメニュー	<p>左側のチェックボックスをオンにすると、デバイスを管理できます。デバイスを選択したら、[アクション]ドロップダウンメニューをクリックし、アクションを選択します。例：</p> <ul style="list-style-type: none"> <li>• アクティブ化：選択したデバイスを管理するようにNAに指示します。</li> <li>• 非アクティブ化：選択したデバイスを管理しないようにNAに指示します。</li> <li>• 一括編集：[デバイスを一括編集]ページが開きます。このページでは、ドライバを割り当てたり、選択したすべてのデバイスについて接続方法を設定できます。</li> <li>• ダイアグラム：<a href="#">「ダイアグラム」</a> (603 ページ) を参照してください。</li> <li>• 削除：選択したデバイスが削除されます。</li> <li>• ポリシー準拠の確認：<a href="#">「[ポリシー準拠の確認]タスクページのフィールド」</a> (372 ページ) を参照してください。</li> <li>• Syslogの構成：<a href="#">「[Syslogの構成]タスクページのフィールド」</a> (284 ページ) を参照してください。</li> <li>• パスワードの配布：<a href="#">「[パスワードの配布]タスクページのフィールド」</a> (288 ページ) を参照してください。</li> <li>• ドライバの検出：<a href="#">「[ドライバの検出]タスクページのフィールド」</a> (293 ページ) を参照してください。</li> <li>• デバイスのリポート：<a href="#">「[デバイスのリポート]タスクページのフィールド」</a> (296 ページ) を参照してください。</li> <li>• コマンドスクリプトの実行：<a href="#">「[コマンドスクリプトの実行]タスクページのフィールド」</a> (304 ページ) を参照してください。</li> <li>• 診断の実行：<a href="#">「[診断の実行]タスクページのフィールド」</a> (310 ページ) を参照してください。</li> <li>• ICMPテストの実行：<a href="#">「[ICMPテストの実行]タスクページのフィールド」</a> (299 ページ) を参照してください。</li> <li>• スナップショットの取得：<a href="#">「[スナップショットの取得]タスクページのフィールド」</a> (315 ページ) を参照してください。</li> </ul>
チェックボックス/ドロップダウンメニュー (続き)	<ul style="list-style-type: none"> <li>• スタートアップとランニングの同期：<a href="#">「[ スタートアップとランニングの同期 ] タスクページのフィールド」</a> (319 ページ) を参照してください。</li> <li>• デバイスソフトウェアの更新：<a href="#">「[デバイスソフトウェアの更新]タスクページのフィールド」</a> (323 ページ) を参照してください。</li> <li>• ACLの削除：<a href="#">「ACLの削除タスクページ」</a> (708 ページ) を参照してください。</li> <li>• OS分析：<a href="#">「[OS分析]タスクページのフィールド」</a> (350 ページ) を参照してください。</li> <li>• デバイスのプロビジョニング：<a href="#">「[デバイスの編集]ページのフィールド」</a> (111 ページ) を参照してください。</li> </ul>
詳細CSVレポートを表示	非準拠となった理由を説明するイベントの詳細を含む、すべてのレコードが記載されたCSVファイルを作成できます。
この検索を変更	[ポリシー、ルール、および準拠を検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。

オプション	説明/アクション
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"><li>• 新規デバイスグループとして指定した名前で保存 : [全結果デバイス]または[選択デバイスのみ]を選択し、新規グループ名を入力して、[グループを作成]をクリックします。</li><li>• 既存の静的デバイスグループに追加 : [全結果デバイス]または[選択デバイスのみ]を選択し、ドロップダウンメニューからデバイスグループを選択して、[追加]をクリックします。</li><li>• 検索を指定した名前でユーザレポートとして保存: ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、「<a href="#">ユーザレポートとシステムレポート</a>」(593ページ)を参照してください。</li><li>• 検索結果を電子メール送信: 検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li><li>• 検索結果をCSVファイルとして表示 : 検索結果をCSV形式でダウンロードします。</li></ul>

## 構成の検索

構成検索では、条件と演算子の組み合わせを使用することにより、構成ファイルを検索できます。検索条件はすべて、ブール演算子ANDおよびORによって結合され、検索結果はすべての条件に一致します。

構成ファイルを検索するには、[レポート]のメニューバーにある[検索]を選択し、[構成]をクリックします。検索条件の入力後、検索を実行する前に別のページに移動すると、条件の設定が失われます。

**注意：** 検索に構成を含む条件を使用する場合、保存済みの構成が多いと、クエリに時間がかかることがあります。構成を検索するときには、[対象]オプションを選択することをお勧めします。こうすることで、OracleまたはSQL Serverデータベースのフルテキスト検索機能が使用されます。

検索条件を入力して、[検索]ボタンをクリックすると、[構成の検索結果]ページに、指定した検索条件のすべてを含む設定のリストが表示されます。詳細については、「[\[構成の検索結果\]ページのフィールド](#)」(497 ページ)を参照してください。

## [構成を検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように[構成の検索結果]ページをカスタマイズできます。
ホスト名	<p>演算子を選択し、デバイスのホスト名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul> <p>ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。 *は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。（<b>注意：</b>ワイルドカードは「等しい」および「等しくない」演算子と併用できません。）</p>
デバイスIP	演算子を選択し、デバイスのIPアドレスを入力します。
日付	<p>次の演算子を選択します。</p> <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」（これを選択するとカレンダーが開きます）、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意：</b> カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>
変更者	演算子を選択し、デバイスの構成を変更したと思われるユーザのログイン名を入力します。

フィールド	説明/アクション
デバイスステータス	<p>デバイスについて、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• アクティブ</li> <li>• 非アクティブ</li> <li>• 実稼働前（実稼働前デバイスとは、運用ネットワーク内でまだ動作していないデバイスのことです。詳細については、「<a href="#">ベアメタルプロビジョニング</a>」（116ページ）を参照してください。）</li> </ul>
デバイスタイプ	<p>スクロールダウンメニューから、ネットワークデバイスのタイプ（ルータ、スイッチ、ファイアウォール、VPN、ダイヤルアップ、DSL_ISDN、ロードバランサなど）を選択します。</p>
コメント	<p>演算子（「含む」または「含まない」）を選択し、検索対象のコメントテキストを入力します。これにより、[デバイス構成の詳細]ページの[構成コメント]ボックスに表示されるテキストだけが検索されます。</p> <p>ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p>
構成テキスト	<p>演算子を選択し、検索するデバイス構成ファイルの一部（一意的な内容）を入力します。</p> <ul style="list-style-type: none"> <li>• 「含む」、「含まない」演算子では、ワイルドカードとして?および*を含む正規表現を使用できます。ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、これらの検索では大文字小文字が区別されます。</li> <li>• 「含む（全文）」および「含まない（全文）」演算子では、ワイルドカードとして*のみ使用できます。詳細については、「<a href="#">全文検索機能の使用</a>」（470ページ）を参照してください。</li> </ul> <p>これらの検索では、大文字小文字が常に区別されません。</p> <p>（注意：これらの演算子を使用するには、データベースで全文検索が有効になっている必要があります。）</p> <ul style="list-style-type: none"> <li>• IPv6アドレスの簡略表記（二重コロン）とワイルドカードを組み合わせて使用することはできません。</li> </ul> <p>検索演算子を「含む」または「含む（全文）」にする場合は、ページの最下部にある[一致した行の前後&lt;#&gt;コンテキスト行を表示]テキストボックスに値を入力します。結果ページに表示される検索テキストの前後に最大5行まで行を追加できます。デフォルト値は3です。（注意：ロード対象の結果が大量にある場合、コンテキスト行を表示するとパフォーマンスが大幅に低下することがあります。）</p>
検索範囲	<p>次のオプションの1つをオンにします。</p> <ul style="list-style-type: none"> <li>• 現在の構成のみを検索：オンにすると、現在の構成のみが検索されます。</li> <li>• 全構成を検索：オンにすると、現在の構成と履歴の構成すべてが検索されます。</li> </ul>
異なるスタートアップとランニング構成	<p>オンにすると、スタートアップとランニング構成が異なるデバイスが検索されます。</p>
構成のカスタムデータ	<p>演算子を選択し、表示されるカスタムフィールドのいずれかに示される一意のテキストを入力します。（注意：このセクションは、カスタムフィールドがない場合は表示されません。）</p>

フィールド	説明/アクション
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"><li>• 選択グループ内のいずれか（デフォルト）</li><li>• 選択グループのすべて</li><li>• 選択グループになし</li></ul> <p><b>注意：</b> デバイスセレクトアを使用してグループを選択します。デバイスセレクトアの使用方法的詳細については、「<a href="#">デバイスセレクトア</a>」（142ページ）を参照してください。</p>
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（<b>注意：</b> このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」（156ページ）を参照してください）。</p>



## [構成の検索結果]ページのフィールド

[構成の検索結果]ページの表示は、[構成を検索]ページで選択した検索条件によって異なります。詳細については、[「\[構成を検索\]ページのフィールド」\(494ページ\)](#)を参照してください。次の表は、[構成の検索結果]ページに用意されているオプションを示します。

フィールド	説明/アクション
この検索を変更	[構成を検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
チェックボックス	<p>左側のチェックボックスをオンにすると、構成を比較したり、NAデータベースから構成を削除したりできます。構成を選択したら、[アクション]ドロップダウンメニューをクリックし、次のいずれかをクリックします。</p> <ul style="list-style-type: none"> <li>比較: [デバイス構成の比較]ページが開きます。このページでは、2つの構成を比較できます。わかりやすいように、差異が強調表示されています。このページから、構成を配布することもできます。</li> <li>削除: 選択した構成がNAデータベースから削除されます。</li> </ul> <p>左側にある[選択]ドロップダウンメニューを使用すると、デバイスを全選択または全選択解除できます。</p>
アクション	<p>[構成の検索結果]テーブルのエントリごとに、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>前と比較: [デバイス構成の比較]ページが開きます。このページには、現在の構成と以前の構成が並列表示されます。わかりやすいように、差異が異なる色で強調表示されています。</li> <li>構成を表示: [デバイス構成の詳細]ページが開きます。このページでは、構成を編集したり、選択した構成にコメントを追加したりできます。このページから、選択した構成を配布することもできます。</li> <li>診断: [診断]ページが開きます。このページには、当該構成の診断情報が表示されます。</li> </ul>
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"> <li>結果デバイスを新規デバイスグループとして指定した名前で保存: 新規グループ名を入力して、[グループを作成]をクリックします。</li> <li>既存のデバイスグループに結果デバイスを追加: ドロップダウンメニューからグループを選択して、[追加]をクリックします（<b>注意</b>: 動的グループの作成の詳細については、<a href="#">「動的デバイスグループ」(140ページ)</a>を参照してください）。</li> <li>検索を指定した名前でユーザーレポートとして保存: ユーザーレポート名を入力して、[保存]をクリックします。ユーザーレポートは、[ユーザーレポートとシステムレポート]ページから確認できます。</li> <li>検索結果を電子メール送信: 検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li> <li>検索結果をCSVファイルとして表示: 検索結果をCSV形式でダウンロードします。（<b>注意</b>: [構成の検索] ページで検索基準を定義するときに、[構成テキスト] オプションをオンにして、検索対象として構成テキストを入力した場合、[結果の詳細を含む] オプションをオンにしてください。[結果の詳細を含む]オプションをオンにしないと、構成テキストがCSV ファイルに含まれません。）</li> </ul>

## 診断の検索

診断の検索では、定義した検索条件に基づいて、デバイス診断情報にアクセスできます。結果はすべての検索条件に一致します。診断別に提供される情報のタイプはデバイス固有です。

診断を検索するには、[レポート]のメニューバーにある[検索]を選択し、[診断]をクリックします。[診断を検索]ページが開きます。

**注意：** 検索条件の入力後、検索を実行する前に別のページに移動すると、条件の設定が失われます。

検索条件を入力して、[検索]ボタンをクリックすると、[診断の検索結果]ページに、指定した検索条件のすべてを含む診断のリストが表示されます。詳細については、「[\[診断の検索結果\]ページのフィールド](#)」(501 ページ)を参照してください。

**注意：** NA VLAN データ収集と NA トポロジ収集の診断は検索できません。詳細については、「[表示メニューオプション](#)」(201 ページ)を参照してください。

## [診断を検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように[診断の検索結果]ページをカスタマイズできます。
ホスト名	<p>演算子を選択し、デバイスのホスト名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul> <p>ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。 *は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。（<b>注意</b>：ワイルドカードは「等しい」および「等しくない」演算子と併用できません。）</p>
デバイスIP	演算子を選択し、デバイスのIPアドレスを入力します。
日付	<p>次の演算子を選択します。</p> <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」（これを選択するとカレンダーが開きます）、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意</b>：カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>
診断タイプ	<p>スクロールダウンメニューから、検索対象の診断データタイプを選択します。複数のタイプを選択または選択解除するには、[Ctrl]+クリックを使用します。選択可能な診断タイプは次のとおりです。</p> <ul style="list-style-type: none"> <li>• NA デバイスファイルシステム</li> <li>• ハードウェア情報</li> <li>• ICMPテスト</li> <li>• メモリトラブルシューティング</li> <li>• NAがデバイスのブートを検出</li> <li>• NAフラッシュ記憶域容量</li> <li>• NAインターフェイス</li> <li>• NAモジュールのステータス</li> <li>• NA OSPF ネイバー</li> <li>• NAポートスキャン</li> <li>• NAルーティングテーブル</li> <li>• NA トポロジーデータ収集</li> </ul> <p><b>注意</b>：診断の詳細については、「<a href="#">表示メニューオプション</a>」（201ページ）の[診断]フィールドを参照してください。</p>

フィールド	説明/アクション
デバイスステータス	<p>デバイスについて、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• アクティブ</li> <li>• 非アクティブ</li> <li>• 実稼働前（実稼働前デバイスとは、運用ネットワーク内でまだ動作していないデバイスのことです。詳細については、「<a href="#">ベアメタルプロビジョニング</a>」（116ページ）を参照してください。）</li> </ul>
診断テキスト	<p>演算子（「含む」または「含まない」）を選択し、検索対象の診断または検索結果から除外する診断の一部（一意的な内容）を入力します。</p> <p>ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p>
診断のカスタムデータ	<p>演算子を選択し、表示されるカスタムフィールドのいずれかに示される一意のテキストを入力します。（<b>注意</b>：このセクションは、カスタムフィールドがない場合は表示されません。）</p>
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• 選択グループ内のいずれか（デフォルト）</li> <li>• 選択グループのすべて</li> <li>• 選択グループになし</li> </ul> <p><b>注意</b>：デバイスセクタを使用してグループを選択します。デバイスセクタの使用方法的詳細については、「<a href="#">デバイスセクタ</a>」（142ページ）を参照してください。</p>
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（<b>注意</b>：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」（156ページ）を参照してください。）</p>

## [診断の検索結果]ページのフィールド

[診断の検索結果]ページの表示は、[診断を検索]ページで選択した検索条件によって異なります。詳細については、「[\[診断を検索\]ページのフィールド](#)」(499ページ)を参照してください。次の表は、[診断の検索結果]ページに用意されているオプションを示します。

オプション	説明/アクション
この検索を変更	[診断を検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
チェックボックス	<p>左側のチェックボックスをオンにすると、NAデータベースの診断を選択できます。診断を選択したら、[アクション]ドロップダウンメニューをクリックし、次のいずれかをクリックします。</p> <ul style="list-style-type: none"> <li>• 比較：[診断タイプを比較]ページが開きます。このページでは、同じタイプの2つの診断を比較できます。</li> <li>• 削除：選択した構成がNAデータベースから削除されます。</li> </ul> <p>隣接の[選択]ドロップダウンメニューを使用すると、デバイスを全選択または全選択解除できます。</p>
アクション	<p>[診断の検索結果]テーブルのエントリごとに、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>• 詳細を表示：診断の詳細を表示できます。</li> <li>• 前と比較：この診断を前回の診断と比較します。</li> </ul>
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"> <li>• 新規デバイスグループとして指定した名前で保存：[全結果デバイス]または[選択デバイスのみ]を選択し、新規グループ名を入力して、[グループを作成]をクリックします。</li> <li>• 既存の静的デバイスグループに追加：[全結果デバイス]または[選択デバイスのみ]を選択し、ドロップダウンメニューからデバイスグループを選択して、[追加]をクリックします。</li> <li>• 検索を指定した名前でユーザレポートとして保存：ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、「<a href="#">ユーザレポートとシステムレポート</a>」(593ページ)を参照してください。</li> <li>• 検索結果を電子メール送信：検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li> <li>• 検索結果をCSVファイルとして表示：検索結果をCSV形式でダウンロードします。</li> </ul>

## タスクの検索

タスク検索では、ネットワークに対してスケジュールされたタスクについて、NAデータベースを検索できます。

タスクを検索するには、[レポート]のメニューバーにある[検索]を選択し、[タスク]をクリックします。[タスクを検索]ページが開きます。[検索]ボタンをクリックすると、[タスクの検索結果]ページに、指定した検索条件のすべてを含むタスクのリストが表示されます。詳細については、「[\[タスクの検索結果\]ページのフィールド](#)」(506 ページ)を参照してください。

**注意：** 検索条件の入力後、検索を実行する前に別のページに移動すると、条件の設定が失われます。

### [タスクを検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように[タスクの検索結果]ページをカスタマイズできます。
タスク名	<p>演算子を選択し、タスク名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul>
ホスト名	<p>演算子を選択し、デバイスのホスト名を入力します。ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。*は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。(注意：ワイルドカードは「等しい」および「等しくない」演算子と併用できません。)</p>
デバイスIP	演算子を選択し、タスクに関連するデバイスのIPアドレスを入力します。
スケジュール作成者	演算子を選択し、タスクをスケジュールしたユーザ名を入力します。
スケジュール日	<p>次の演算子を選択します。</p> <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」(これを選択するとカレンダーが開きます)、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意：</b> カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>

フィールド	説明/アクション
タスクのステータス	<p>スクロールダウンリストから、ステータスを1つ以上選択します。複数の項目を選択するには、[Ctrl]キーとクリックを使用します。選択可能なステータスは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 保留</li> <li>• 成功</li> <li>• 失敗</li> <li>• 実行中</li> <li>• 一時停止</li> <li>• ドラフト</li> <li>• 待機中</li> <li>• 重複</li> <li>• スキップ</li> <li>• 警告</li> <li>• 要求</li> <li>• テンプレート</li> </ul>
タスク優先度	<p>タスクの優先度を入力します。タスクのスケジューリングの詳細については、「<a href="#">タスクの予定</a>」(278 ページ) を参照してください。</p>
タスクタイプ	<p>検索対象のタスクタイプを選択します。複数のタスクタイプを選択または選択解除するには、[Ctrl]キーとクリックを使用します。選択可能なタスクタイプは次のとおりです。</p> <ul style="list-style-type: none"> <li>• デバイスソフトウェアのバックアップ</li> <li>• ポリシー準拠の確認</li> <li>• Syslogの構成</li> <li>• データの整理</li> <li>• 重複の削除</li> <li>• ACLの削除</li> <li>• 構成を配布</li> <li>• パスワードの配布</li> <li>• リモートエージェントの配布</li> <li>• デバイスコンテキスト</li> <li>• デバイスコンテキストの削除</li> <li>• ネットワークデバイスの検出</li> <li>• ドライバの検出</li> <li>• Cisco.comからイメージをダウンロード</li> <li>• 電子メールレポート</li> <li>• サマリレポートの生成</li> <li>• インポート</li> <li>• IOS XR ソフトウェア</li> <li>• マルチタスクプロジェクト</li> <li>• OS分析</li> </ul>

フィールド	説明/アクション
タスクタイプ（続き）	<ul style="list-style-type: none"> <li>• デバイスのプロビジョニング</li> <li>• デバイスのリブート</li> <li>• FQDNの解決</li> <li>• コマンドスクリプトの実行</li> <li>• 診断の実行</li> <li>• 外部アプリケーションの実行</li> <li>• ICMPテストの実行</li> <li>• スタートアップとランニングの同期</li> <li>• スナップショットの取得</li> <li>• デバイスソフトウェアの更新</li> <li>• VLANタスク</li> </ul>
エラータイプ	<p>スクロールダウンリストから、エラータイプを1つ以上選択します。複数の項目を選択するには、[Ctrl]キーとクリックを使用します。選択可能なエラータイプは次のとおりです。</p> <ul style="list-style-type: none"> <li>• デバイスに到達できません</li> <li>• パスワードが誤っています</li> <li>• 権限が不十分です</li> <li>• パスワードが見つかりません</li> <li>• デバイスが認識されません</li> <li>• デバイスがサポートされていません</li> </ul>
コメント	<p>演算子（「含む」または「含まない」）を選択し、タスクに関するコメントの一部（一意的な内容）を入力します。</p> <p>ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p>
結果	<p>演算子（「含む」または「含まない」）を選択し、検索対象のタスク結果から一意のテキストを入力します。</p> <p>ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p> <p>[タスクの検索結果]ページにタスク情報を表示するには、[この列を検索結果に含める]ボックスをオンにします。検索演算子が「含む」の場合は、ページの最下部にある[“#” コンテキスト行]ボックスに値を入力します。検索テキストの前後に最大5行まで行を追加できます。（<b>注意</b>：ロード対象の結果が大量にある場合、コンテキスト行を表示するとパフォーマンスが大幅に低下することがあります）。</p>
承認期限	<p>次の演算子を選択します。</p> <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」（これを選択するとカレンダーが開きます）、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意</b>：カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>



フィールド	説明/アクション
承認のステータス	<p>スクロールダウンリストから、承認のステータスを1つ以上選択します。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• 承認済み</li> <li>• ドラフト</li> <li>• 対応していません</li> <li>• 未承認</li> <li>• 無効化</li> <li>• 承認を待機中</li> </ul>
デバイスタイプ	<p>スクロールダウンメニューから、ネットワークデバイスのタイプ（ルータ、スイッチ、ファイアウォール、VPN、ダイヤルアップ、DSL、ISDN、ロードバランサなど）を選択します。</p>
子タスクを除く	<p>オンにすると、子タスクが検索から除外されます。</p>
カスタムデータ	<p>演算子を選択し、表示されるカスタムフィールドのいずれかに示される一意のテキストを入力します。（<b>注意</b>：このセクションは、カスタムフィールドがない場合は表示されません。）</p>
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• 選択グループ内のいずれか（デフォルト）</li> <li>• 選択グループのすべて</li> <li>• 選択グループになし</li> </ul> <p><b>注意</b>：デバイスセレクトアを使用してグループを選択します。デバイスセレクトアの使用方法的詳細については、「<a href="#">デバイスセレクトア</a>」（142ページ）を参照してください。</p>
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（<b>注意</b>：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」（156ページ）を参照してください。）</p>

## [タスクの検索結果]ページのフィールド

[タスクの検索結果]ページの表示は、[タスクを検索]ページで選択した検索条件によって異なります。詳細については、「[\[タスクを検索\]ページのフィールド](#)」(502ページ)を参照してください。次の表は、[タスクの検索結果]ページに用意されているオプションを示します。

オプション	説明/アクション
この検索を変更	[タスクを検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
チェックボックス	<p>左側のチェックボックスをオンにすると、[タスクの検索結果]テーブルからタスクを削除できます。タスクを選択したら、[アクション]ドロップダウンメニューをクリックし、次のオプションをクリックします。</p> <ul style="list-style-type: none"> <li>削除：選択したタスクが削除されます。</li> </ul> <p>隣接の[選択]ドロップダウンメニューを使用すると、タスクを全選択または全選択解除できます。</p>
アクション	<p>[タスクの検索結果]テーブルのエントリごとに、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>編集：[タスクを編集]ページが開きます。このページでは、繰り返し実行されているタスクまたはまだ実行されていないタスクを編集および再実行できます。このリンクは、タスクの編集が可能な場合にのみ表示されます。</li> <li>削除：タスクが削除されます。このリンクは、タスクがまだ実行されていない場合にのみ表示されます。</li> <li>一時停止：タスクが一時停止します。このリンクは、タスクがまだ実行されていない場合にのみ表示されます。</li> <li>直ちに実行：タスクが実行されます。このリンクは、タスクがまだ実行されていない場合にのみ表示されます。</li> <li>再実行：[タスクを再実行]ページが開き、タスクを再実行できます。</li> <li>詳細：[タスク情報]ページが開きます。そのページでタスクの詳細を表示できます。</li> <li>キャンセル：タスクをキャンセルします。</li> </ul>

オプション	説明/アクション
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"><li>• 新規デバイスグループとして指定した名前で保存 : [全結果デバイス]または[選択デバイスのみ]を選択し、新規グループ名を入力して、[グループを作成]をクリックします。</li><li>• 既存の静的デバイスグループに追加 : [全結果デバイス]または[選択デバイスのみ]を選択し、ドロップダウンメニューからデバイスグループを選択して、[追加]をクリックします。</li><li>• 検索を指定した名前でユーザレポートとして保存: ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、「<a href="#">ユーザレポートとシステムレポート</a>」(593ページ)を参照してください。</li><li>• 検索結果を電子メール送信: 検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li><li>• 検索結果をCSVファイルとして表示: 検索結果をCSV形式でダウンロードします。(注意: [結果]オプションをオンにして、[タスクの検索]ページで検索条件を定義する際に検索したいタスク結果を入力した場合、[結果の詳細を含む]オプションをオンにしてください。[結果の詳細を含む]オプションをオンにしないと、タスク結果がCSVファイルに含まれません)。</li></ul>

## セッションの検索

NAが提供するスクリプトの実行と管理の機能は、複数のデバイスに対し同時に変更を行う場合、多大なメリットをもたらします。ただし、スクリプト記述の経験が浅い方の場合、コマンドスクリプトを作成するのに困難を伴うことがあります。そのため、NAにはScriptMasterが用意されており、これを使用すると、Telnet/SSHプロキシによって記録されたTelnetセッションまたはSSHセッションに基づいて、スクリプトが自動的に生成されます。

セッション検索を使用すると、Telnet/SSH プロキシセッションを検出できます。さらに、一致するセッションデータの前後に表示されるセッションデータを含めるように[セッションの検索結果]ページを構成することにより、結果を読み取るためのコンテキストを提供できます。

NAにコマンドだけを保存するのか、Telnet/SSHコマンドセッション全体を保存するのかを決定するシステム管理設定があります。「[Telnet/SSH]ページのフィールド」(65 ページ) を参照してください。

セッションを検索するには、[レポート]のメニューバーにある[検索]を選択し、[Telnet/SSHセッション]をクリックします。[セッションを検索]ページが開きます。検索条件を入力して、[検索]ボタンをクリックすると、[セッションの検索結果]ページに、指定した検索条件のすべてを含むTelnet/SSHセッションのリストが表示されます。詳細については、「[セッションの検索結果]ページのフィールド」(511 ページ) を参照してください。

**注意：** 検索条件の入力後、検索を実行する前に別のページに移動すると、条件の設定が失われます。

## [セッションを検索]ページのフィールド

フィールド	説明/アクション
ホスト名	<p>演算子を選択し、セッションに関連するデバイスのホスト名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul> <p>ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。*は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。(注：ワイルドカードは「等しい」および「等しくない」演算子と併用できません。)</p>
デバイスIP	<p>演算子を選択し、セッションに関連するデバイスのIPアドレスを入力します。</p>
デバイスステータス	<p>デバイスについて、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• アクティブ</li> <li>• 非アクティブ</li> <li>• 実稼働前 (実稼働前デバイスとは、運用ネットワーク内でまだ動作していないデバイスのことです。詳細については、「ベアメタルプロビジョニング」(116 ページ) を参照してください。)</li> </ul>

フィールド	説明/アクション
作成者	演算子を選択し、セッションを作成したと思われるユーザのログイン名を入力します。
開始日	<p>次の演算子を選択します。</p> <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」（これを選択するとカレンダーが開きます）、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意：</b> カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>
終了日	<p>次の演算子を選択します。</p> <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」（これを選択するとカレンダーが開きます）、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意：</b> カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>
ステータス	<p>次のステータスオプションの中からオプションを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• 失敗</li> <li>• 開く</li> <li>• 終了</li> </ul>
セッションタイプ	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 任意</li> <li>• Telnet</li> <li>• SSH</li> </ul>
セッションデータ	<p>演算子（「含む」または「含まない」）を選択し、検索対象のセッションの一部（一意的な内容）を入力します。</p> <p>ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p> <p>検索演算子が「含む」の場合は、ページの最下部にある[&lt;#&gt; コンテキスト行]ボックスに値を入力します。結果に表示される検索テキストの前後に最大5行まで行を追加できます。（<b>注意：</b> ロード対象の結果が大量にある場合、コンテキスト行を表示するとパフォーマンスが大幅に低下することがあります）。</p>
セッションのカスタムデータ	<p>演算子を選択し、表示されるカスタムフィールドのいずれかに示される一意のテキストを入力します。（<b>注意：</b> このセクションは、カスタムフィールドがない場合は表示されません。）</p>
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• 選択グループ内のいずれか（デフォルト）</li> <li>• 選択グループのすべて</li> <li>• 選択グループになし</li> </ul> <p><b>注意：</b> デバイスセレクトアを使用してグループを選択します。デバイスセレクトアの使用方法的詳細については、「<a href="#">デバイスセレクトア</a>」（142ページ）を参照してください。</p>

フィールド	説明/アクション
パーティション	パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（ <b>注意</b> ：このフィールドは 1 つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「 <a href="#">パーティション</a> 」（156 ページ）を参照してください）。

## [セッションの検索結果]ページのフィールド

[セッションの検索結果]ページの表示は、[セッションを検索]ページで選択した検索条件によって異なります。詳細については、「[\[セッションを検索\]ページのフィールド](#)」(508 ページ)を参照してください。次の表は、[セッションの検索結果]ページに用意されているオプションを示します。

オプション	説明/アクション
この検索を変更	[セッションを検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
アクション	<p>[セッションの検索結果]テーブルのエントリごとに、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>• ホスト名 : [デバイス情報]ページが開きます。このページには、デバイスおよびその構成履歴に関する基本情報が表示されます。</li> <li>• デバイスIP : [デバイス情報]ページが開きます。このページには、デバイスおよびその構成履歴に関する基本情報が表示されます。</li> <li>• 全Telnet/SSHセッションを表示 : [Telnet/SSHセッション]ページが開きます。このページには、当該セッションのコマンドおよびシステム応答が表示されます。このページには、現在のセッション中に実行されるコマンドからのスクリプト作成を簡略化する[スクリプトに変換]へのリンクが含まれます。詳細については、「<a href="#">コマンドスクリプトの追加</a>」(576 ページ)を参照してください。また、当該セッションによって作成された構成がある場合は、その構成へのリンクも含まれます。</li> <li>• コマンドのみ表示 : [Telnet/SSHセッション]ページが開きます。このページには、当該セッションのコマンドのみが表示されます。このページには、現在のセッション中に実行されるコマンドからのスクリプト作成を簡略化する[スクリプトに変換]へのリンクが含まれます。また、当該セッションによって作成された構成がある場合は、その構成へのリンクも含まれます。</li> </ul>
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"> <li>• 新規デバイスグループとして指定した名前で保存 : [全結果デバイス]または[選択デバイスのみ]を選択し、新規グループ名を入力して、[グループを作成]をクリックします。</li> <li>• 既存の静的デバイスグループに追加 : [全結果デバイス]または[選択デバイスのみ]を選択し、ドロップダウンメニューからデバイスグループを選択して、[追加]をクリックします。</li> <li>• 検索を指定した名前でユーザレポートとして保存 : ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、「<a href="#">ユーザレポートとシステムレポート</a>」(593 ページ)を参照してください。</li> <li>• 検索結果を電子メール送信 : 検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li> <li>• 検索結果をCSVファイルとして表示 : 検索結果をCSV形式でダウンロードします。(注意 : [セッションデータ]オプションをオンにして、[セッションを検索]ページで検索条件を定義する際に検索したいセッションデータを入力した場合、[結果の詳細を含む]オプションをオンにしてください。[結果の詳細を含む]オプションをオンにしないと、セッションデータがCSVファイルに含まれません。)</li> </ul>

## イベントの検索

デバイスアクセスエラーなどのシステムイベントおよびユーザイベントを検索できます。NAイベントの説明については、「[イベントの説明](#)」(515ページ)を参照してください。

イベントを検索するには、[レポート]のメニューバーにある[検索]を選択し、[イベント]をクリックします。[イベントを検索]ページが開きます。検索条件を入力して、[検索]ボタンをクリックすると、[イベントの検索結果]ページに、指定した検索条件のすべてを含むイベントのリストが表示されます。詳細については、「[\[イベントの検索結果\]ページのフィールド](#)」(514ページ)を参照してください。

**注意：** 検索条件の入力後、検索を実行する前に別のページに移動すると、条件の設定が失われます。

### [イベントを検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように[イベントの検索結果]ページをカスタマイズできます。
日付	次の演算子を選択します。 <ul style="list-style-type: none"><li>• 「次の日時以降」または「次の日時以前」</li><li>• 「時間指定なし」、「カスタマイズ」(これを選択するとカレンダーが開きます)、「今」、または「1時間前」から「1年前」まで</li></ul> <b>注意：</b> カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。
サマリ	イベント名を1つ以上選択します。複数のイベントを選択/選択解除するには、[Ctrl]+クリックを使用します。各イベントの詳細については、「 <a href="#">イベントの説明</a> 」(515ページ)を参照してください。
追加ユーザ名	演算子を選択し、イベントを作成したユーザのログイン名を入力します。
重要度	次の中からオプションを1つ以上選択します。 <ul style="list-style-type: none"><li>• 情報：一般的に対応を必要としないイベント。</li><li>• 低：時間的な余裕がある場合に対応を必要とするイベント。</li><li>• 中：適時に対応を必要とするイベント (通常は72時間以内)。</li><li>• 高：緊急の対応を必要とするイベント (通常は24時間以内)。</li><li>• 重要：即時の対応を必要とするイベント。</li></ul>



フィールド	説明/アクション
ホスト名	<p>演算子を選択し、当該イベントに関連するデバイスのホスト名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul> <p>ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。*は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。（<b>注意</b>：ワイルドカードは「等しい」および「等しくない」演算子と併用できません。）</p>
デバイス IP	<p>演算子を選択し、当該イベントに関連するデバイスのIPアドレスを入力します。</p>
説明	<p>演算子（「含む」または「含まない」）を選択し、検索対象のイベントから一意のテキストを入力します。</p> <p>ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p> <p>結果ページにテキストを表示する場合、結果に表示される検索テキストの前後に最大5行まで行を追加できます。（<b>注意</b>：ロード対象の結果が大量にある場合、コンテキスト行を表示するとパフォーマンスが大幅に低下することがあります）。</p>
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• 選択グループ内のいずれか（デフォルト）</li> <li>• 選択グループのすべて</li> <li>• 選択グループになし</li> </ul> <p><b>注意</b>：デバイスセレクトを使用してグループを選択します。デバイスセレクトの使用方法の詳細については、「<a href="#">デバイスセレクト</a>」（142 ページ）を参照してください。</p>
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（<b>注意</b>：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」（156 ページ）を参照してください）。</p>

## [イベントの検索結果]ページのフィールド

[イベントの検索結果]ページの表示は、[イベントを検索]ページで選択した検索条件によって異なります。詳細については、「[\[イベントを検索\]ページのフィールド](#)」(512 ページ) を参照してください。次の表は、[イベントの検索結果]ページに用意されているオプションを示します。

フィールド	説明/アクション
この検索を変更	[イベントを検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
チェックボックス	<p>各イベントのチェックボックスをオンにすると、イベントを削除できます。イベントを選択したら、[アクション]ドロップダウンメニューをクリックし、次のオプションをクリックします。</p> <ul style="list-style-type: none"> <li>削除：選択したイベントが削除されます。</li> </ul> <p>隣接の[選択]ドロップダウンメニューを使用すると、タスクを全選択または全選択解除できます。</p>
アクション	<p>[イベントの検索結果]テーブルのエントリごとに、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>サマリ：[イベントの詳細]ページが開きます。このページには、当該イベントの詳細な結果が表示されます。</li> <li>ホスト名：[デバイス詳細]ページが開きます。このページには、デバイスおよびその構成履歴に関する基本情報が表示されます。</li> </ul>
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"> <li>新規デバイスグループとして指定した名前で保存：[全結果デバイス]または[選択デバイスのみ]を選択し、新規グループ名を入力して、[グループを作成]をクリックします。</li> <li>既存の静的デバイスグループに追加：[全結果デバイス]または[選択デバイスのみ]を選択し、ドロップダウンメニューからデバイスグループを選択して、[追加]をクリックします。</li> <li>検索を指定した名前でユーザーレポートとして保存：ユーザーレポート名を入力して、[保存]をクリックします。ユーザーレポートは、[ユーザーレポートとシステムレポート]ページから確認できます。詳細については、「<a href="#">ユーザーレポートとシステムレポート</a>」(593 ページ) を参照してください。</li> <li>検索結果を電子メール送信：検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li> <li>検索結果をCSVファイルとして表示：検索結果をCSV形式でダウンロードします。(注意：[説明]オプションをオンにして、[イベントを検索]ページで検索条件を定義する際に検索したいイベント説明テキストを入力した場合、[結果の詳細を含む]オプションをオンにしてください。[結果の詳細を含む]オプションをオンにしないと、イベント説明テキストがCSVファイルに含まれません。)</li> </ul>

## イベントの説明

次の表は、NAイベントを示します。イベントはアルファベット順で表示されています。

イベント	説明
承認が拒否されました	ユーザが承認の要求を拒否しました。
承認が付与されました	ユーザがタスクを承認しました。
承認が必要なくなりました	タスクの承認は不要です。
承認が無効化されました	ユーザがタスクの承認を無効化しました。これにより、承認なしでタスクを実行できます。
承認の要求	ユーザが実行前に承認を必要とするタスクを作成しました。
承認タスクが変更されました	ユーザが実行前に承認を必要とするタスクを変更しました。
承認タスクが削除されました	ユーザが承認対象として割り当てたタスクを削除しました。
承認タスクがタイムアウトしました	タスクが割り当てられた時間内で承認されませんでした。
コマンド認可エラー	ユーザが使用権限を持たないコマンドを実行しようとした。
コマンドスクリプトが変更されました	コマンドスクリプトが変更されました。
Telnet/SSH同時セッションが無効化されました	ユーザが同時ログインに対する制約を無視しました。別のユーザがすでにログインしているにもかかわらず、ユーザがプロキシ経由でデバイスにログインしました。
デバイスアクセスエラー	NAがデバイスにアクセスできません。このエラーは、パスワードが間違っているか、ホストへのルートが存在しなかったことが原因の可能性があります。
デバイスが追加されました	ユーザがデバイスを追加しました。
デバイスがブートしました	デバイスがリブートされました。
デバイスコマンドスクリプトが正常に終了しました	デバイスコマンドスクリプトが正常に終了しました。
デバイスコマンドスクリプトでエラーが発生しました	デバイスコマンドスクリプトでエラーが発生しました。
デバイスコンテキストの追加	デバイスコンテキストが正常に追加されました。
デバイスコンテキストの追加に失敗しました	デバイスコンテキストの追加に失敗しました。
デバイスコンテキストが削除されました	デバイスコンテキストが正常に削除されました。
デバイスコンテキストの削除に失敗しました	デバイスコンテキストの削除に失敗しました。
デバイス構成の変更	NAがスナップショットタスクの実行中に構成変更を検出しました。
デバイス構成の変更-ユーザなし	NAが不明ユーザによる構成変更を検出しました。
デバイス構成の配布	NAがデバイスに構成を正常に配布しました。
デバイス構成の配布エラー	NAがデバイスへの構成の配布に失敗しました。

イベント	説明
デバイスデータエラー	NAがデータベースへの構成または診断出力の保存に失敗しました。
デバイスが削除されました	ユーザがデバイスを永久に削除しました。
デバイス診断が変化しました	診断の結果が前回の結果と異なっています。
デバイス診断が正常に終了しました	デバイス診断が正常に終了しました。
デバイス診断でエラーが発生しました	デバイス診断に失敗しました。
デバイスが編集されました	ユーザがデバイス情報を変更しました。
デバイスのフラッシュ記憶域が十分ではありません	デバイスのフラッシュ記憶域が少なくなっています。
デバイスグループが追加されました	ユーザがデバイスグループを追加しました。
デバイスグループが削除されました	ユーザがデバイスグループを削除しました。
デバイスグループが変更されました	ユーザがデバイスグループを変更しました。
デバイスにアクセスできません	デバイスがアクセス不能です。
デバイスが管理対象になりました	ユーザがデバイスをアクティブとしてマークしました。
インポートにデバイスがありません	定期的なインポートタスクの実行時にインポート対象のデバイスのファイルを指定した際、前回のインポートでファイルに含まれていたデバイスが今回のインポートではファイルに含まれていないと、このイベントが発生します。
デバイスパスワードの変更	ユーザがパスワード変更を配布しました。
デバイスパスワードの変更エラー	NAがデバイスパスワード変更の配布に失敗しました。
デバイス権限-変更	デバイスがグループに追加されたか、グループから削除されました。これにより、ユーザがデバイスを変更できる権限が変更されました。
デバイス権限-デバイスの新規作成	誰かがデバイスグループに新規デバイスを追加しました。これにより、そのデバイスグループに関連するユーザの権限が変更されました。
デバイスポートの通信モードの不一致が検出されました	デバイスポートの通信モードの不一致が検出されました。
デバイスのプロビジョニングに失敗しました	デバイスを正常にプロビジョニングできませんでした。
デバイスのプロビジョニングに成功しました	デバイスが正常にプロビジョニングされました。
デバイス関係が追加されました	デバイス関係が正常に追加されました。
デバイス関係が削除されました	デバイス関係が正常に削除されました。
デバイス関係が変更されました	デバイス関係が正常に変更されました。
デバイスのリロード	デバイスが正常にリロードされました。
デバイスのリロードに失敗しました	デバイスのリロードに失敗しました。
デバイス予約の競合	デバイス予約の競合が発生しました。

イベント	説明
デバイスのスナップショット	NAが構成変更対象のデバイスを確認しました。
デバイスソフトウェアの変更	NAがデバイス上に新しいOSバージョンを検出しました（例：IOS 11からIOS 12）。
デバイスのスタートアップとランニング構成の差異	NAがスタートアップ構成と実行構成の間に差異を検出しました。
デバイステンプレートが追加されました	デバイステンプレートが正常に追加されました。
デバイステンプレートが削除されました	デバイステンプレートが正常に削除されました。
デバイステンプレートが編集されました	デバイステンプレートが正常に編集されました。
デバイスが管理解除されました	ユーザがデバイスを非アクティブとしてマークしました。特定の期間に到達できない場合は、インポートされたデバイスを非アクティブにすることもできます。
診断が変更されました	ユーザが診断を変更しました。
分散システム-破損したレプリケーションジョブ	NAは、破損したレプリケーションジョブを検出しました。
分散システム-データ同期遅延の警告	NAは、データ同期の遅延の警告を検出しました。
分散システム-遅延LOBがしきい値を超過	NAがしきい値を超過した遅延LOBを検出しました。
分散システム-遅延トランザクションがしきい値を超過	NAがしきい値を超過した遅延トランザクションを検出しました。
分散システム-デバイスソフトウェアの転送エラー	NAは、デバイスソフトウェア転送エラーを検出しました。
分散システム-修復したレプリケーションジョブ	NAは、修復したレプリケーションジョブを検出しました。
分散システム-レプリケーションエラー	NAはレプリケーションエラーを検出しました。
分散システム-RMIエラー	NAは、RMIエラーを検出しました。
分散システム-停止したマージエージェントジョブ	NAは、停止したマージエージェントジョブを検出しました。
分散システム-時刻同期の警告	NAは、時刻同期の警告を検出しました。
分散システム-削除不可能な異常の生成	NAは、削除不可能な異常の生成を検出しました。
分散システム-一意性の競合	NAは、一意性の競合を検出しました。
ドライバ検出エラー	NAは、失敗したドライバ検出を検出しました。
ドライバ検出成功	NAは、成功したドライバ検出を検出しました。
ドライバのロードエラー	NAは、ドライバロードエラーを検出しました。

イベント	説明
デバイスの重複が検出されました	NAは重複するデバイスを検出しました。
動的グループの更新エラー	NAは、デバイスグループ更新エラーを検出しました。
電子メールレポートの保存	ユーザが電子メールレポートを保存しました。
外部ディレクトリサーバの認証エラー	NAが外部のLDAP 認証サーバに接続できませんでした。
最後に使用したデバイスパスワードが変更されました	デバイスへのアクセスで最後に使用されたパスワードが変更されました。
ライセンス数がほぼ上限です	デバイスにおけるライセンスノードの合計数が90%を超過しています。
ライセンスの期限切れが近づいています	NAライセンスの期限切れが間近になっています（日付ベースのライセンスのみ）。
ライセンス数が超過しました	デバイスにおけるライセンスノードの合計数が上限を超過しています。NA では20% まで超過が許容されています。
ライセンスの期限が切れました	ライセンスの期限が切れました。これ以降NAにログインできなくなります。ただし、スケジュールされたスナップショットの取得および変更の記録は続行されます。
モジュールが追加されました	誰かがデバイスにモジュール/ブレード/カードを追加しました。
モジュールが変更されました	誰かがデバイスに設置されているモジュール/ブレード/カードの属性を変更しました。
モジュールが削除されました	誰かがデバイスからモジュール/ブレード/カードを削除しました。
監視エラー	サーバ監視の実行に失敗しました。
監視の正常動作	サーバ監視が正常に実行されました。
保留タスクが削除されました	ユーザがスケジュールされたタスクを実行前に削除しました。
ポリシーが追加されました	ユーザが新規構成ポリシーを追加しました。
ポリシーが変更されました	ユーザが構成ポリシーを変更しました。
構成ポリシーに非準拠です	構成変更がポリシールールに違反しました。
ポリシーパターンのタイムアウト	ポリシーパターンが一致するまでの時間が30秒を超過しました。
ポリシールールが追加されました	ユーザが新規構成ルールを追加しました。
ポリシールールが変更されました	ユーザが構成ルールを変更しました。
予約デバイス設定が変更されました	ユーザが予約デバイスのデバイス構成を変更しました。
配布予定構成が編集されました	ユーザが配布を予定していた構成を変更しました。
配布予定パスワードが変更されました	新規パスワードが配布されました。ただし、他にもスケジュールされたパスワードの配布タスクが存在します。このイベントは、配布された新規パスワードが、保留中のパスワードの配布タスクが実行されたときに再度変更されることを示します。
セキュリティアラート	NAは、セキュリティアラートを検出しました。

イベント	説明
サーバスタートアップ	NA管理エンジンが起動しました。
セッションデータがキャプチャされました	プロキシが接続セッションをデータベースに保存しました。
ソフトウェア更新に失敗しました	NAがデバイス上のOSソフトウェアの更新に失敗しました。
ソフトウェア更新が正常に終了しました	NAがデバイス上のOSソフトウェアの更新を正常に終了しました。
ソフトウェアの脆弱性が検出されました	ソフトウェアレベルを「セキュリティリスク」に設定すると、NAがデバイスのスナップショットを取得し、かつ「セキュリティリスク」として見なされるOSバージョンを検出したときに、このイベントが生成されます。
サマリレポートが生成されました	ユーザがサマリレポートを生成しました。
タスクが完了しました	タスクが完了しました。
タスクが開始しました	タスクが開始されました。
チケットが作成されました	HP Remedy AR System Connector（またはサードパーティのチケットシステムと接続するHP Connector）を使用している場合、このイベントは、NAが対象サードパーティのチケットシステムにチケットを作成したことを示します。
ユーザが追加されました	ユーザが追加されました。
ユーザ認証エラー	ユーザがNAへのログイン時に間違ったパスワードを入力しました。
ユーザ認証エラーによるロックアウト	連続して何回もログインに失敗したため、ユーザがロックされています。
ユーザが削除されました	ユーザが削除されました。
ユーザが無効になりました	ユーザレコードが編集されました。そのため、ユーザのステータスが有効から無効に変更されています。
ユーザが有効になりました	ユーザレコードが編集されました。そのため、ユーザのステータスが無効から有効に変更されています。
ユーザログイン	ユーザがNAにログインしました。
ユーザログアウト	ユーザがNAからログアウトしました。
ユーザメッセージ	ユーザが[メッセージの新規作成]リンクをクリックしてメッセージを作成しました。
ユーザ権限が変更されました	ユーザの権限が変更されました。

## ユーザの検索

[ユーザを検索]ページを使用すると、名/姓別、電子メールアドレス別、AAAユーザ名別のすべてまたはいずれかでユーザを検索できます。ユーザを検索するには、[レポート]のメニューバーにある[検索]を選択し、[ユーザ]をクリックします。[ユーザを検索]ページが開きます。

[検索]ボタンをクリックすると、[ユーザの検索結果]ページに、指定した検索条件のすべてを含むユーザのリストが表示されます。詳細については、「[\[ユーザの検索結果\]ページ](#)」(521 ページ)を参照してください。

## [ユーザを検索]ページ

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように[ユーザ検索結果]ページをカスタマイズできます。
名	<p>演算子を選択し、ユーザの名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul>
姓	演算子を選択し、ユーザの姓を入力します。
ユーザ名	<p>演算子を選択し、ユーザのユーザ名を入力します。ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。*は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。(注意：ワイルドカードは「等しい」および「等しくない」演算子と併用できません。)</p>
電子メールアドレス	演算子を選択し、ユーザの電子メールアドレスを入力します。
AAAユーザ名	演算子を選択し、ユーザのAAAユーザ名を入力します。
コメント	演算子(「含む」または「含まない」)を選択し、検索対象のコメントテキストを入力します。
ユーザグループのメンバー	ユーザがメンバーとなっているユーザグループを選択します。
ユーザのカスタムデータ	演算子を選択し、ユーザのカスタムサービスデータを入力します。
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション(名前はデフォルトサイト)には、当初、すべてのインベントリが含まれます。(注意：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」(156 ページ)を参照してください)。</p>



## [ユーザの検索結果]ページ

[ユーザの検索結果]ページの表示は、[ユーザを検索]ページで選択した検索条件によって異なります。詳細については、「[\[ユーザを検索\]ページ](#)」(520ページ)を参照してください。

フィールド	説明/アクション
この検索を変更	[イベントの検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
アクション	<p>[タスクの検索結果]テーブルのエントリごとに、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>編集: [自分のプロフィール]ページが開きます。このページでは、ユーザのプロファイルを編集できます。詳細については、「<a href="#">[自分のプロフィール]ページのフィールド</a>」(260ページ)を参照してください。</li> <li>削除: 適切な権限を持っている場合、ユーザを削除できます。適切な権限がない場合、このオプションは灰色で表示されます。</li> <li>権限: [自分の権限]ページが開きます。このページでは、ユーザの権限を編集できます。詳細については、「<a href="#">[自分の権限]ページのフィールド</a>」(264ページ)を参照してください。</li> <li>構成変更: [構成の検索結果]ページが開きます。このページには、ユーザが行った構成変更が表示されます。</li> </ul>
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"> <li>検索を指定した名前でユーザレポートとして保存: ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、「<a href="#">ユーザレポートとシステムレポート</a>」(593ページ)を参照してください。</li> <li>検索結果を電子メール送信: 検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li> <li>検索結果をCSVファイルとして表示: 検索結果をCSV形式でダウンロードします。</li> </ul>

## ACLの検索

アクセス制御リスト（ACL）は、ほとんどのデバイスで構成に含まれています。ACLにより、ルータのインターフェイスでルーティングされたパケットを受け入れるのか、ブロックするのかを制御して、ネットワークトラフィックをフィルタリングします。一般に、ACLはステートメントの集合です。各ステートメントによって、IPパケット内で検出されるパターンを定義します。ACLは、ルーティングアップデートの内容を制限したり、ネットワークセキュリティを提供したりするために使用します。

NAは、デバイスから構成情報を取得し、構成からACLステートメントを抽出します。さらに、NAは、構成に依存しないACLを保存します。これにより、次のことを実行できます。

- デバイスに対する現在のACLの確認、および現在のACLと以前のACLの比較。
- ACLへのコメントの追加。
- ACLの変更/作成、およびACLのデバイスへの配布。

ACLの変更および作成の詳細については、「[ACLの作成](#)」（700ページ）を参照してください。

ACLを検索するには、[レポート]のメニューバーにある[検索]を選択し、[ACL]をクリックします。[ACLを検索]ページが開きます。

## [ACLを検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように[ACLの検索結果]ページをカスタマイズできます。
ホスト名	<p>演算子を選択し、セッションに関連するデバイスのホスト名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul> <p>ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。*は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。（<b>注意</b>：ワイルドカードは「等しい」および「等しくない」演算子と併用できません。）</p>
デバイスIP	演算子を選択し、デバイスのIPアドレスを入力します。
ACL ID	演算子を選択し、ACLのIDを入力します。ACLのIDはデバイスACLリストに基づく番号または名前です。一方、ACLハンドルは、ユーザによって割り当てられる説明的な名前または値です。デフォルトでは、ユーザがACLハンドルを定義するまで、ACL IDとACLハンドルは同一となっています。
ACLハンドル	演算子を選択し、ACLのハンドルを入力します。ACLハンドルは、ユーザによって割り当てられる説明的な名前または値です。デフォルトでは、ユーザがACLハンドルを定義するまで、ACL IDとACLハンドルは同一となっています。
ACLタイプ	演算子を選択し、ACLのタイプ（例：「拡張」）を入力します。ACLタイプはドライバに依存します。
ACL構成	<p>演算子（「含む」または「含まない」）を選択し、ACLを定義する構成コマンドを入力します。ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p> <p>検索演算子が「含む」の場合は、ページの最下部にある[&lt;#&gt; コンテキスト行]ボックスに値を入力します。結果に表示される検索テキストの前後に最大5行まで行を追加できます。（<b>注意</b>：ロード対象の結果が大量にある場合、コンテキスト行を表示するとパフォーマンスが大幅に低下することがあります）。</p>
ACLアプリケーション	<p>演算子（「含む」または「含まない」）を選択し、ACLを使用しているエンティティを入力します。たとえば、ACLがインターフェイスに適用されている場合は、インターフェイスがACLのアプリケーションになります。</p> <p>ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p>
検索範囲	オンにすると、検索結果が、現在すべてのドライバに対して構成されているACLに絞り込まれます。オンにしない場合は、検索結果に現在のACLと以前のACLの両方が含まれます。

フィールド	説明/アクション
コメント	<p>演算子（「含む」または「含まない」）を選択し、ACLコメントを入力します。</p> <p>ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p>
変更者	<p>演算子を選択し、最後にACLを変更したユーザ名を入力します。</p>
最終変更	<p>次の演算子を選択します。</p> <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」（これを選択するとカレンダーが開きます）、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意：</b> カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• 選択グループ内のいずれか（デフォルト）</li> <li>• 選択グループのすべて</li> <li>• 選択グループになし</li> </ul> <p><b>注意：</b> デバイスセレクトアを使用してグループを選択します。デバイスセレクトアの使用方法的詳細については、「<a href="#">デバイスセレクトア</a>」（142ページ）を参照してください。</p>
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（<b>注意：</b> このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」（156ページ）を参照してください）。</p>

[検索]ボタンをクリックすると、[ACLの検索結果]ページに、指定した検索条件のすべてを含むACLのリストが表示されます。詳細については、「[\[ACLの検索結果\]ページのフィールド](#)」（525ページ）を参照してください。

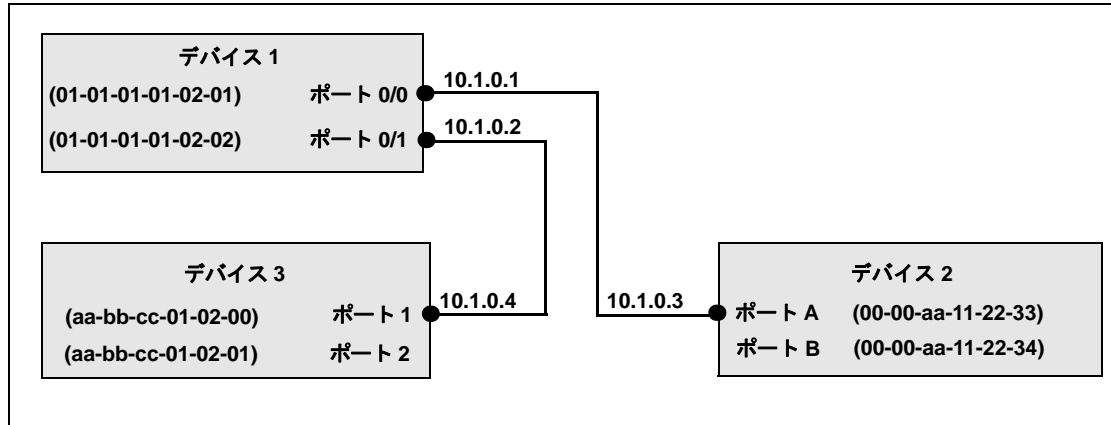
## [ACLの検索結果]ページのフィールド

[ACLの検索結果]ページの表示は、[ACLを検索]ページで選択した検索条件によって異なります。詳細については、[「\[ACLを検索\]ページのフィールド」\(523ページ\)](#)を参照してください。次の表は、[ACLの検索結果]ページに用意されているオプションを示します。

オプション	説明/アクション
この検索を変更	[ACLを検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
チェックボックス	<p>各ACLのチェックボックスをオンにすると、2つのACLを比較できます。ACLを選択したら、[アクション]ドロップダウンメニューをクリックし、次のオプションをクリックします。</p> <ul style="list-style-type: none"> <li>比較: [ACLを比較]ページが開きます。このページでは、2つのACLを比較できます。わかりやすいように、差異が強調表示されています。コンテキストとの差異の表示、全文の表示、またはUNIX形式での差異の表示といったオプションがあります。</li> </ul> <p>隣接の[選択]ドロップダウンメニューを使用すると、ACLを全選択または全選択解除できます。</p>
アクション	<p>[ACL検索結果]テーブルのエントリごとに、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>ACLを編集: [ACLを編集]ページが開きます。このページでは、ACLを編集できます。詳細については、<a href="#">「ACLの削除」(707ページ)</a>を参照してください。</li> <li>ACLを表示: [ACLを表示]ページが開きます。このページには、ACLが表示されます。詳細については、<a href="#">「ACLの表示」(695ページ)</a>を参照してください。</li> <li>ACL履歴: [ACL履歴]ページが開きます。このページでは、ACLを編集して表示できます。</li> </ul>
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"> <li>選択されたACLのハンドルを設定: ACLハンドルを入力します。ACLハンドルは、ユーザによって割り当てられる説明的な名前または値です。</li> <li>検索を指定した名前でユーザレポートとして保存: ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、<a href="#">「ユーザレポートとシステムレポート」(593ページ)</a>を参照してください。</li> <li>検索結果を電子メール送信: 検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li> <li>検索結果をCSVファイルとして表示: 検索結果をCSV形式でダウンロードします。</li> </ul>

## MACアドレスの検索

MACアドレスは、デバイス上のポートを識別する一意のアドレスです。MACアドレスは、Burned-in Addresses (BLA)、ハードウェアアドレス、物理アドレスといった別名でも知られています。NAは、デバイス上のポートに割り当てられているMACアドレスおよびこれらのポートから認識可能なMACアドレスに関する情報を収集します。次の図は、MACアドレス、IPアドレス、およびポートの関係を示します。



MACアドレスを検索するには、[レポート]のメニューバーにある[検索]を選択し、[MACアドレス]をクリックします。[MACアドレスを検索]ページが開きます。検索条件を入力して、[検索]ボタンをクリックすると、[MACアドレスの検索結果]ページに、指定した検索条件のすべてを含むMACアドレスのリストが表示されます。詳細については、「[\[MACアドレスの検索結果\]ページのフィールド](#)」(529ページ)を参照してください。

## [MACアドレスを検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように[MACアドレス検索結果]ページをカスタマイズできます。
ホスト名	<p>演算子を選択し、デバイスのホスト名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul> <p>ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。 *は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。（<b>注意</b>：ワイルドカードは「等しい」および「等しくない」演算子と併用できません。）</p>
デバイスIP	演算子を選択し、デバイスのIPアドレスを入力します。
ポート名	演算子を選択し、デバイスのポート名を入力します。ポート名は、デバイス上に実際に存在するポートの名前です。例：イーサネット0/1
Port Description	演算子を選択し、ポートの説明を入力します。
アドレス	演算子を選択し、検索対象のMACアドレスパターンを入力します。
アドレスタイプ	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 全アドレス（デフォルト）</li> <li>• ポートから認識：デバイス/ポートに接続されているMACアドレスのみ（つまり、デバイス/ポートの外側にあるが、デバイス/ポートから認識可能なMACアドレスタイプ）が表示されます。</li> <li>• ポートのアドレス：デバイスの内側にあるMACアドレスのみ（つまり、デバイス上のポートに割り当てられているMACアドレス）が表示されます。</li> </ul> <p><b>注意</b>：[認識されなくなったアドレスのみを検索]チェックボックスをオンにすると、最新のデータキャプチャで認識されなくなったMACアドレスのみに検索結果を絞り込むことができます。</p>
検索範囲	オンにすると、検索が認識されなくなったMACアドレスに絞り込まれます。
VLAN	演算子を選択し、ポートのVLAN名を入力します。VLAN名は、検索を絞り込むときに使用するVLANの名前（VLAN2やVLAN3など）です。
関連IP	演算子を選択し、検索しているMACに関連するIPアドレスを入力します。

フィールド	説明/アクション
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"><li>• 選択グループ内のいずれか（デフォルト）</li><li>• 選択グループのすべて</li><li>• 選択グループになし</li></ul> <p><b>注意：</b> デバイスセレクトアを使用してグループを選択します。デバイスセレクトアの使用方法的詳細については、「<a href="#">デバイスセレクトア</a>」（142ページ）を参照してください。</p>
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（<b>注意：</b> このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」（156ページ）を参照してください。）</p>



## [MACアドレスの検索結果]ページのフィールド

[MACアドレスの検索結果]ページは、[MACアドレスを検索]ページで選択した検索条件を表示します。詳細については、「[\[MACアドレスを検索\]ページのフィールド](#)」(527ページ)を参照してください。

オプション	説明/アクション
この検索を変更	[MACアドレスを検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
アクション	MACアドレスごとに、次のアクションを選択できます。 <ul style="list-style-type: none"><li>• 詳細 : [MACアドレスの詳細]ページが開きます。そのページで次の詳細を表示できます。デバイス、デバイスポート、MACアドレス、タイプ、最初の認識日時、および最終更新です。</li><li>• IPの表示 : 当該MACアドレスと相互参照される[IPアドレスの詳細]ページが開きます。これは、[ポートから認識]レコードでのみ使用できます。相互参照とは、NAがデータを収集したときに、IPアドレスとMACアドレスのソースが同一だったことを意味します。</li></ul>
検索条件	検索に使用した検索条件が表示されます。以下のことが可能です。 <ul style="list-style-type: none"><li>• 新規デバイスグループとして指定した名前で保存 : [全結果デバイス]または[選択デバイスのみ]を選択し、新規グループ名を入力して、[グループを作成]をクリックします。</li><li>• 既存の静的デバイスグループに追加 : [全結果デバイス]または[選択デバイスのみ]を選択し、ドロップダウンメニューからデバイスグループを選択して、[追加]をクリックします。</li><li>• 検索を指定した名前でユーザレポートとして保存 : ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、「<a href="#">ユーザレポートとシステムレポート</a>」(593ページ)を参照してください。</li><li>• 検索結果を電子メール送信 : 検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li><li>• 検索結果をCSVファイルとして表示 : 検索結果をCSV形式でダウンロードします。</li></ul>

## IP アドレスの検索

IP アドレス（インターネットプロトコルアドレス）は、ネットワークデバイスの一意の数値アドレスです。ルータ、スイッチ、ファイアウォールなどのあらゆる参加ネットワークデバイスが、独自の IP アドレスを持ちます。現在、NA がサポートする項目を以下に挙げます。

- IPv4 : IPv4 はオクテット表記の 32 ビットおよび 64 ビットアドレスをサポートします
- IPv6 : IPv6 はオクテット表記の 128 ビットアドレスをサポートします（IPv6 サポートの詳細については、『NA インストールおよびアップグレードガイド』を参照してください）。

IP アドレスを検索するには、[レポート] のメニューバーにある [検索] を選択し、[IP アドレス] をクリックします。[IP アドレスを検索] ページが開きます。検索基準を入力し終えたら、[検索] ボタンをクリックします。[IP アドレス検索結果] ページに、指定した検索条件のすべてを含むポリシーのリストが表示されます。

**注意：** 検索条件の入力後、検索を実行する前に別のページに移動すると、条件の設定が失われます。

## [IP アドレスの検索] ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように [IP アドレス検索結果] ページをカスタマイズできます。
ホスト名	<p>演算子を選択し、セッションに関連するデバイスのホスト名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul> <p>ワイルドカード文字を使用できます。? は、該当箇所に 1 文字の任意文字が入ることを表します。* は、該当箇所に任意個数の文字が入ることを表します。例 : usa-ny-ny-*, 10.0.*.2, ?jones。 (<b>注意：</b> ワイルドカードは「等しい」および「等しくない」演算子と併用できません。)</p>
デバイス IP	<p>演算子を選択し、デバイスの IP アドレスを入力します。例 : IPv4 : 10.255.?.255、192.*、172.16.30.1 IPv6 : aff:38:?:10、fc00:c0a8:*, ::1</p>
ポート名	<p>演算子を選択し、デバイスのポート名を入力します。ポート名は、デバイス上に実際に存在するポートの名前です。例 : イーサネット 0/1</p>
Port Description	<p>演算子を選択し、ポートの説明を入力します。</p>
アドレス	<p>演算子を選択し、検索対象の IP アドレスパターンを入力します。例 : IPv4 : 10.255.?.255、192.*、172.16.30.1 IPv6 : aff:38:?:10、fc00:c0a8:*, ::1</p>

フィールド	説明/アクション
アドレスタイプ	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 全アドレス（デフォルト）</li> <li>• ポートから認識：デバイス/ポートに接続されているIPアドレスのみ（つまり、デバイス/ポートの外側にあるが、デバイス/ポートから認識可能なIPアドレスタイプ）が表示されます。</li> <li>• ポートのアドレス：デバイスの内側にあるIPアドレスのみ（つまり、デバイス上のポートに割り当てられているIPアドレス）が表示されます。</li> </ul> <p><b>注意：</b> [認識されなくなったアドレスのみを検索] チェックボックスをオンにすると、最新のデータキャプチャで認識されなくなったIPアドレスのみに検索結果を絞り込むことができます。</p>
検索範囲	<p>オンにすると、検索が認識されなくなったIPアドレスに絞り込まれます。</p>
VLAN	<p>演算子を選択し、ポートのVLAN名を入力します。VLAN名は、検索を絞り込むときに使用するVLANの名前（VLAN2やVLAN3など）です。</p>
関連MAC	<p>演算子を選択し、関連MACアドレスを入力します。</p>
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• 選択グループ内のいずれか（デフォルト）</li> <li>• 選択グループのすべて</li> <li>• 選択グループになし</li> </ul> <p><b>注意：</b> デバイスセレクトアを使用してグループを選択します。デバイスセレクトアの使用の詳細については、「<a href="#">デバイスセレクトア</a>」(142ページ)を参照してください。</p>
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はパーティション）には、当初、すべてのインベントリが含まれます。（<b>注意：</b> このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」(156ページ)を参照してください）。</p>

## [IPアドレスの検索結果]ページのフィールド

[IPアドレスの検索結果]ページは、[IPアドレスを検索]ページで選択した検索条件を表示します。詳細については、[「\[IPアドレスの検索\]ページのフィールド」](#)（530 ページ）を参照してください。

オプション	説明/アクション
この検索を変更	[IPアドレスを検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
アクション	<p>MAC アドレスごとに、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>詳細: [IPアドレスの詳細]ページが開きます。そのページで次の詳細を表示できます。デバイス、デバイスポート、MAC アドレス、タイプ、最初の認識日時、および最終更新です。</li> <li>IP の表示: 当該IPアドレスと相互参照される[IPアドレスの詳細]ページが開きます。これは、[ポートから認識]レコードでのみ使用できます。相互参照とは、NAがデータを収集したときに、IPアドレスとMACアドレスのソースが同一だったことを意味します。</li> </ul>
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"> <li>新規デバイスグループとして指定した名前で保存: [全結果デバイス]または[選択デバイスのみ]を選択し、新規グループ名を入力して、[グループを作成]をクリックします。</li> <li>既存の静的デバイスグループに追加: [全結果デバイス]または[選択デバイスのみ]を選択し、ドロップダウンメニューからデバイスグループを選択して、[追加]をクリックします。</li> <li>検索を指定した名前でユーザレポートとして保存: ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、<a href="#">「ユーザレポートとシステムレポート」</a>（593 ページ）を参照してください。</li> <li>検索結果を電子メール送信: 検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li> <li>検索結果をCSVファイルとして表示: 検索結果をCSV形式でダウンロードします。</li> </ul>

## VLANの検索

VLAN（仮想ローカルエリアネットワーク）は、単一のブロードキャストドメインとして機能するポートの集合です。VLANは、レイヤ2（データリンクレイヤ）で動作します。NAは、デバイスに対して定義されているVLANおよび各ポートが割り当てられているVLANに関する情報を収集します。VLANの詳細については、「[仮想ローカルエリアネットワーク（VLAN）](#)」（213ページ）を参照してください。

VLANを検索するには、[レポート]のメニューバーにある[検索]を選択し、[VLAN]をクリックします。[VLANを検索]ページが開きます。検索基準を入力し終えたら、[検索]ボタンをクリックします。[VLANの検索結果]ページに、指定した検索条件のすべてを含むポリシーのリストが表示されます。

**注意：** 検索条件の入力後、検索を実行する前に別のページに移動すると、条件の設定が失われます。

### [VLANを検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように[VLANの検索結果]ページをカスタマイズできます。
ホスト名	<p>演算子を選択し、セッションに関連するデバイスのホスト名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul> <p>ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。*は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。（<b>注意：</b>ワイルドカードは「等しい」および「等しくない」演算子と併用できません。）</p>
デバイスIP	演算子を選択し、デバイスのIPアドレスを入力します。
VLAN ID	演算子を選択し、VLANのIDを入力します。VLAN IDは、VLANのタグ内の12ビットフィールドを使用してVLANを特定します。VLANの詳細については、「 <a href="#">仮想ローカルエリアネットワーク（VLAN）</a> 」（213ページ）を参照してください。
VLAN名	演算子を選択し、VLAN名を入力します。
VLANタイプ	演算子を選択し、VLANタイプを入力します。
VLANの説明	演算子を選択し、VLANの説明を入力します。
プライベートVLAN	演算子を選択し、プライベートVLANの説明を入力します。

フィールド	説明/アクション
デバイスが所属するグループ	<p>ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。</p> <ul style="list-style-type: none"><li>• 選択グループ内のいずれか（デフォルト）</li><li>• 選択グループのすべて</li><li>• 選択グループになし</li></ul> <p><b>注意：</b> デバイスセレクトアを使用してグループを選択します。デバイスセレクトアの使用方法的詳細については、「<a href="#">デバイスセレクトア</a>」（142ページ）を参照してください。</p>
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（<b>注意：</b> このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」（156ページ）を参照してください）。</p>

## [VLANの検索結果]ページのフィールド

[VLANの検索結果]ページは、[VLANを検索]ページで選択した検索条件を表示します。詳細については、「[\[VLANを検索\]ページのフィールド](#)」(533ページ)を参照してください。

オプション	説明/アクション
この検索を変更	[VLANを検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
アクション	<p>VLANごとに、次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>• 詳細を表示 : [VLANの詳細]ページが開きます。このページには、[デバイス]ページおよび[インターフェイスの詳細]ページへのリンクを使用する検索についての詳細が表示されます。詳細については、「<a href="#">[VLAN詳細]ページのフィールド</a>」(217ページ)を参照してください。</li> <li>• 編集 : [VLAN詳細を編集]ページが開きます。詳細については、「<a href="#">VLANの作成と編集</a>」(216ページ)を参照してください。</li> <li>• 削除 : VLANの削除を確認するダイアログボックスが開きます。</li> </ul>
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"> <li>• 新規デバイスグループとして指定した名前で保存 : [全結果デバイス]または[選択デバイスのみ]を選択し、新規グループ名を入力して、[グループを作成]をクリックします。</li> <li>• 既存の静的デバイスグループに追加 : [全結果デバイス]または[選択デバイスのみ]を選択し、ドロップダウンメニューからデバイスグループを選択して、[追加]をクリックします。</li> <li>• 検索を指定した名前でユーザレポートとして保存 : ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、「<a href="#">ユーザレポートとシステムレポート</a>」(593ページ)を参照してください。</li> <li>• 検索結果を電子メール送信 : 検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li> <li>• 検索結果をCSVファイルとして表示 : 検索結果をCSV形式でダウンロードします。</li> </ul>

## デバイステンプレートの検索

デバイステンプレートにより、構成、OS/ファイルの仕様、および既存のデバイスに適用可能なその他デバイス固有情報を定義できます。デバイステンプレートには、実際にテストするデバイスを必要としないで、ポリシー確認などのある種のデバイス操作をサポートする機能も備わっています。詳細については、「[デバイステンプレート](#)」(118 ページ) を参照してください。

デバイステンプレートを検索するには、[レポート]のメニューバーにある[検索]を選択し、[デバイステンプレート]をクリックします。[DeviceTemplateを検索]ページが開きます。検索基準を入力し終えたら、[検索]ボタンをクリックします。[DeviceTemplateの検索結果]ページに、指定した検索条件のすべてを含むデバイステンプレートのリストが表示されます。

**注意：** 検索条件の入力後、検索を実行する前に別のページに移動すると、条件の設定が失われます。

### [DeviceTemplateを検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように[DeviceTemplateの検索結果]ページをカスタマイズできます。
テンプレート名	<p>演算子を選択し、デバイステンプレートの名前を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul> <p>ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。 *は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。(注 意：ワイルドカードは「等しい」および「等しくない」演算子と併用できません。)</p>
デバイスのベンダー	演算子を選択し、デバイスのベンダーを入力します。
デバイスモデル	演算子を選択し、デバイスモデルを入力します。
ドライバ名	リストからドライバを選択します。
デバイスの説明	演算子を選択し、説明を入力します。
コメント	<p>演算子を選択し、コメントを入力します。</p> <p>ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、このフィールドでは大文字小文字が区別されます。</p>



フィールド	説明/アクション
構成テキスト	<p>演算子を選択し、検索するデバイス構成ファイルの一部（一意的な内容）を入力します。</p> <ul style="list-style-type: none"> <li>• 「含む」、「含まない」演算子では、ワイルドカードとして?および*を含む正規表現を使用できます。ページ上部のヒントにすべてのテキストフィールド検索で大文字小文字が区別されないという記載がないかぎり、これらの検索では大文字小文字が区別されます。</li> <li>• 「含む（全文）」および「含まない（全文）」演算子では、ワイルドカードとして*のみ使用できます。詳細については、「<a href="#">全文検索機能の使用</a>」（470ページ）を参照してください。これらの検索では、大文字小文字が常に区別されません。 （<b>注意</b>：これらの演算子を使用するには、データベースで全文検索が有効になっている必要があります）。</li> <li>• IPv6 アドレスの簡略表記（二重コロン）とワイルドカードを組み合わせることはできません。</li> </ul> <p>検索演算子を「含む」または「含む（全文）」にする場合は、ページの最下部にある[一致した行の前後&lt;#&gt;コンテキスト行を表示]テキストボックスに値を入力します。結果ページに表示される検索テキストの前後に最大5行まで行を追加できます。デフォルト値は3です。（<b>注意</b>：ロード対象の結果が大量にある場合、コンテキスト行を表示するとパフォーマンスが大幅に低下することがあります）。</p>
作成日	<p>次の演算子を選択します。</p> <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」（これを選択するとカレンダーが開きます）、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意</b>：カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>
デバイスのカスタムデータ	<p>演算子を選択し、デバイスのカスタムデータを入力します。</p>
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（<b>注意</b>：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」（156ページ）を参照してください）。</p>

## [DeviceTemplateの検索結果]ページのフィールド

[DeviceTemplateの検索結果]ページは、[DeviceTemplateを検索]ページで選択した検索条件を表示します。詳細については、「[デバイステンプレートの検索](#)」(536ページ)を参照してください。

オプション	説明/アクション
この検索を変更	[DeviceTemplateを検索]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
アクション	各デバイステンプレートに対して次のアクションを選択できます。 <ul style="list-style-type: none"><li>編集 : [デバイステンプレートの編集]ページが開きます。そのページでデバイステンプレートの情報を編集できます。「<a href="#">[デバイステンプレート]ページのフィールド</a>」(118ページ)を参照してください。</li><li>構成を表示 : [現在の構成]ページが開きます。このページでは、構成を編集したり、選択した構成にコメントを追加したりできます。</li></ul>
検索条件	検索に使用した検索条件が表示されます。以下のことが可能です。 <ul style="list-style-type: none"><li>新規デバイスグループとして指定した名前で保存 : [全結果デバイス]または[選択デバイスのみ]を選択し、新規グループ名を入力して、[グループを作成]をクリックします。</li><li>既存の静的デバイスグループに追加 : [全結果デバイス]または[選択デバイスのみ]を選択し、ドロップダウンメニューからデバイスグループを選択して、[追加]をクリックします。</li><li>検索を指定した名前でユーザレポートとして保存 : ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、「<a href="#">ユーザレポートとシステムレポート</a>」(593ページ)を参照してください。</li><li>検索結果を電子メール送信 : 検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li><li>検索結果をCSVファイルとして表示 : 検索結果をCSV形式でダウンロードします。</li></ul>

## シングルサーチ

デバイス変更イベントを検索するには、[レポート]のメニューバーにある[シングルサーチ]をクリックします。[シングルサーチを検索]ページが開きます。[検索]ボタンをクリックすると、[シングルサーチの検索結果]ページに、指定した検索条件のすべてを含むイベントのリストが表示されます。「[\[シングルサーチの検索結果\]ページのフィールド](#)」(541 ページ) を参照してください。

## [シングルサーチを検索]ページのフィールド

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、選択した情報だけが表示されるように[シングルサーチの検索結果]ページをカスタマイズできます。
日付	<p>次の演算子を選択します。</p> <ul style="list-style-type: none"> <li>• 「次の日時以降」または「次の日時以前」</li> <li>• 「時間指定なし」、「カスタマイズ」（これを選択するとカレンダーが開きます）、「今」、または「1時間前」から「1年前」まで</li> </ul> <p><b>注意：</b> カレンダーアイコンをクリックするとカレンダーが開き、日付および時刻を選択できます。</p>
サマリ	イベント名を1つ以上選択します。複数のイベントを選択/選択解除するには、[Ctrl]+クリックを使用します。各イベントの詳細については、「 <a href="#">イベントの説明</a> 」(515 ページ) を参照してください。
追加ユーザ名	<p>演算子を選択し、イベントを作成したユーザのログイン名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul>
重要度	<p>重要度レベルを1つ以上選択します。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• 情報：一般的に対応を必要としないイベント。</li> <li>• 低：時間的な余裕がある場合に対応を必要とするイベント。</li> <li>• 中：適時に対応を必要とするイベント（通常は72時間以内）。</li> <li>• 高：緊急の対応を必要とするイベント（通常は24時間以内）。</li> <li>• 重要：即時の対応を必要とするイベント。</li> </ul>

フィールド	説明/アクション
ホスト名	<p>演算子を選択し、当該イベントに関連するデバイスのホスト名を入力します。選択可能な演算子は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 含む</li> <li>• 含まない</li> <li>• 一致する</li> <li>• 等しい</li> <li>• 等しくない</li> </ul>
デバイス IP	<p>ワイルドカード文字を使用できます。?は、該当箇所に1文字の任意文字が入ることを表します。*は、該当箇所に任意個数の文字が入ることを表します。例：usa-ny-ny-*、10.0.*.2、?jones。（<b>注意</b>：ワイルドカードは「等しい」および「等しくない」演算子と併用できません。）</p>
説明	<p>演算子（「含む」または「含まない」）を選択し、検索対象のイベントから一意のテキストを入力します。イベントの説明を表示する際、一致した行の周囲にコンテキスト行を表示するには、表示をオンにし、行数を入力します。デフォルト値は3です。</p>
デバイスが所属するグループ	<p>演算子（「選択グループ内のいずれか」、「選択グループすべて」、または「選択グループになし」）を選択し、スクロールダウンリストからグループを1つ以上選択します。</p>
パーティション	<p>パーティションを選択すると、検索結果が当該パーティション内のデバイスに絞り込まれます。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。（<b>注意</b>：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「<a href="#">パーティション</a>」（156ページ）を参照してください。）</p>

## [シングルサーチの検索結果]ページのフィールド

[シングルサーチの検索結果]ページの表示は、[シングルサーチを検索]で選択した検索条件によって異なります。詳細については、「[\[シングルサーチを検索\]ページのフィールド](#)」(539 ページ)を参照してください。次の表は、[シングルサーチの検索結果]ページに用意されているオプションを示します。

フィールド	説明/アクション
この検索を変更	[シングルサーチ]ページに戻ります。このページでは、検索条件を編集したり、検索を再実行したりできます。
検索条件を表示	検索条件情報までスクロールダウンします。
チェックボックス	<p>各イベントのチェックボックスをオンにすると、イベントを削除できます。イベントを選択したら、[アクション]ドロップダウンメニューをクリックし、次のオプションをクリックします。</p> <ul style="list-style-type: none"> <li>• 削除：選択したイベントが削除されます。</li> </ul> <p>隣接の[選択]ドロップダウンメニューを使用すると、タスクを全選択または全選択解除できます。</p>
検索条件	<p>検索に使用した検索条件が表示されます。以下のことが可能です。</p> <ul style="list-style-type: none"> <li>• 新規デバイスグループとして指定した名前で保存：[全結果デバイス]または[選択デバイスのみ]を選択し、新規グループ名を入力して、[グループを作成]をクリックします。</li> <li>• 既存の静的デバイスグループに追加：[全結果デバイス]または[選択デバイスのみ]を選択し、ドロップダウンメニューからデバイスグループを選択して、[追加]をクリックします。</li> <li>• 検索を指定した名前でユーザレポートとして保存：ユーザレポート名を入力して、[保存]をクリックします。ユーザレポートは、[ユーザレポートとシステムレポート]ページから確認できます。詳細については、「<a href="#">ユーザレポートとシステムレポート</a>」(593 ページ)を参照してください。</li> <li>• 検索結果を電子メール送信：検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。アドレスが複数の場合は、必ずカンマで区切ってください。</li> <li>• 検索結果をCSVファイルとして表示：検索結果をCSV形式でダウンロードします。</li> </ul>

## 詳細検索

[詳細検索]ページを使用すると、次のことを実行できます。

- ANDおよびOR演算子を使用したブール式を作成して検索をフィルタする。ブール式で括弧を使用して、検索を絞り込むことができます。

**注意：** このツールでは、正規表現は使用できません。

- 1つまたは複数の検索条件（IPアドレス、ドメイン名、およびポリシー準拠など）を使用した検索の構成。
- デバイスグループ別での検索の制限。
- 詳細検索の検索結果ページの出力のカスタマイズ。

[詳細検索]ページを表示するには、[レポート]のメニューバーにある[詳細検索]をクリックします。[検索]ボタンをクリックすると、指定した検索条件が表示されます。

## [詳細検索]ページのフィールド

フィールド	説明/アクション
検索	<p>ドロップダウンメニューから、次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• ACL</li> <li>• 準拠</li> <li>• 構成</li> <li>• デバイス</li> <li>• 診断</li> <li>• イベント</li> <li>• インターフェイス</li> <li>• モジュール</li> <li>• セッション</li> <li>• タスク</li> </ul>
検索条件	<p>検索条件は、条件を選択するたびに、[検索条件]セクションに表示されます。このセクションでは、「含む」、「一致する」、または「等しい」といった演算子を選択したり、検索する情報を入力したりできます。定義済みの条件を削除する場合は、検索条件インデックス文字の横に表示されている「X」をクリックします。</p>
条件を追加	<p>ドロップダウンメニューから検索条件を1つ以上選択します。選択可能な条件は次のとおりです。</p> <ul style="list-style-type: none"> <li>• ホスト名</li> <li>• デバイスIP</li> <li>• ドメイン名</li> <li>• デバイスステータス</li> <li>• ポリシー準拠</li> </ul>

フィールド	説明/アクション
<b>ブール式</b>	
式	デフォルトでは、定義済みの条件インデックス文字がブール式「and」で結合されて表示されます。たとえば、3つの検索条件が定義されている場合、式は <i>A and B and C</i> のようになります。ブール式は、必要に応じて編集できます。[式をリセット] ボタンをクリックすると、式がデフォルト値にリセットされます。 <b>(注意：条件の最大数は10です。)</b>
<b>デバイスグループで検索を絞り込み</b>	
デバイスが所属するグループ	ドロップダウンメニューから次の演算子のいずれかを選択し、さらにデバイスグループを1つ以上選択します。 <ul style="list-style-type: none"> <li>• 選択グループ内のいずれか（デフォルト）</li> <li>• 選択グループのすべて</li> <li>• 選択グループになし</li> </ul> <b>注意：</b> デバイスセレクトアを使用してグループを選択します。デバイスセレクトアの使用方法的詳細については、「 <a href="#">デバイスセレクトア</a> 」(142ページ) を参照してください。
パーティション	パーティションを選択します。デフォルトパーティション（名前はデフォルトサイト）には、当初、すべてのインベントリが含まれます。 <b>(注意：</b> このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。パーティションの詳細については、「 <a href="#">パーティション</a> 」(156ページ) を参照してください。 <b>)</b>
<b>出力のカスタマイズ</b>	
検索結果に含めるフィールドを選択	詳細検索の検索結果ページに表示するフィールドを選択します。複数のフィールドを選択するには、1つめのフィールドをクリックし、Ctrlキーとクリックを使用して、後続のフィールドを選択/選択解除します。
結果のソート基準	ドロップダウンメニューから、検索結果をソートする検索条件を選択します。昇順（デフォルト）または降順を指定できます。
1ページに表示する結果の数	詳細検索の検索結果ページに表示する項目の数を入力します。デフォルト値は25です。
テキストフィールドを表示するときに一致した行の前後<#>コンテキスト行を表示	詳細検索の検索結果ページにテキストフィールドを表示するときに、一致する行の周囲に表示される行数を入力します。デフォルト値は3です。

## 詳細検索の例

次の詳細検索は、2つのデータセンターが管理下にあることを前提としています。一方のデータセンターはニューヨークに、もう一方はカリフォルニアにあるとします。検索により、いずれかのデータセンターに適切なタイムゾーンが設定されていないすべてのCiscoデバイスが通知されます。

1. NAにログインします。
2. [レポート]のメインメニューバーから、[詳細検索]をクリックします。[詳細検索]ページが開きます。
3. [検索]フィールドで、ドロップダウンメニューから[デバイス]を選択します。
4. [検索条件]フィールドで、ドロップダウンメニューから[ドライバ名]を選択します。
5. NAで使用するCiscoドライバをすべて選択します。
6. [条件を追加]ドロップダウンメニューから、[ホスト名]を選択します。
7. ドロップダウンメニューから[含まない]を選択し、次のように入力します。redmond
8. [条件を追加]ドロップダウンメニューから、[構成テキスト]を選択します。
9. ドロップダウンメニューから[含まない]を選択し、次のように入力します。set timezone PST
10. [ブール式]フィールドで、デフォルトの文字列をA or (B and C)に変更します。
11. [検索]ボタンをクリックします。



## 第12章：イベントおよび診断の管理

### トピックの参照先リスト

トピック	参照先：
イベントの連結ビュー（シングルビュー）	<a href="#">「イベントの連結ビュー（シングルビュー）」（546ページ）</a>
診断	<a href="#">「診断」（549ページ）</a>
診断の追加およびカスタマイジング	<a href="#">「カスタム診断の追加および編集」（552ページ）</a>

## イベントの連結ビュー（シングルビュー）

シングルビューを使用すると、単一デバイスまたは全デバイスへの変更を示すイベントを1ページ上で追跡できます。イベントタイプのリストからイベントを選択します。選択可能なイベントは次のとおりです。

- デバイスがブートしました
- デバイス構成の変更
- デバイス診断の変更
- デバイスパスワードの変更
- 再ロードされたデバイス
- デバイスソフトウェアの変更
- モジュールが追加されました
- モジュールが変更されました
- モジュールが削除されました
- 予約デバイス設定が変更されました
- ユーザメッセージ

NA イベントの全リストについては、「[イベントの説明](#)」（515 ページ）を参照してください。

[シングルビュー] ページを表示するには、[レポート] のメニューバーにある [シングルビュー] をクリックします。  
[シングルビュー] ページが開きます。

## [シングルビュー]ページのフィールド

フィールド	説明/アクション
検索結果を CSV ファイルとして表示	CSV ファイルとして表示された結果を保存する場所の入力が要求されます。
表示される変更イベントのタイプ	[表示される変更イベントのタイプ]メニューを下にスクロールして、表示するイベントを選択します。
対象：	<p>イベントを表示するための時間枠が表示されます。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• 過去 1、2、4、8、12、24、および 48 時間</li> <li>• 過去 1 および 2 週間</li> <li>• 過去 1 ヶ月</li> <li>• 全イベント</li> </ul>
現在の作業グループ	ドロップダウンメニューからデバイスグループを選択します。
チェックボックス	左側のチェックボックスをオンにすると、NA データベースからイベントを削除できます。イベントを選択したら、[アクション] ドロップダウンメニューをクリックし、[削除] をクリックします。これにより、選択したイベントが NA データベースから削除されます。隣接の [選択] ドロップダウンメニューを使用すると、イベントを全選択または全選択解除できます。
イベント日付	イベントの日付/時刻が MMM-dd-yy HH:mm:ss 形式で表示されます。(フォーマットはシステム管理者が自由に設定できます。)
ホスト名	デバイスのホスト名または IP アドレスが表示されます。ホスト名または IP アドレスをクリックすると、[デバイス詳細] ページが開きます。このページには、デバイスおよびデバイス構成履歴に関する情報が表示されます。
サマリ	<p>イベントのタイプが表示されます。NA イベントのリストについては、「<a href="#">イベントの説明</a>」(515 ページ) を参照してください。イベントタイプのリンクをクリックすると、[イベントの詳細] ページが開きます。このページの内容は次のとおりです。</p> <ul style="list-style-type: none"> <li>• イベントが発生した日付および時刻。</li> <li>• イベントを追加したユーザのログイン名またはプロセス。</li> <li>• イベントタイプ。</li> <li>• イベントの簡単な説明。</li> <li>• デバイスに関する詳細情報へのリンク。</li> </ul>
追加ユーザ名	イベントが作成される原因となったアクションを起こしたユーザのログイン名が表示されます。
アクション	<p>次のイベントについて、[前と比較] リンクが表示されます。</p> <ul style="list-style-type: none"> <li>• デバイス構成の変更：[デバイス構成の比較] ページが開きます。詳細については、「<a href="#">デバイス構成の比較</a>」(179 ページ) を参照してください。</li> <li>• デバイス診断が変化しました：変更した診断のタイプに応じて、対応する比較ページが開きます。[NA デバイスファイルシステムを比較] ページや [NA モジュールステータスを比較] ページなどです。</li> <li>• デバイスパスワードの変更：[デバイス構成の比較] ページが開きます。詳細については、「<a href="#">デバイス構成の比較</a>」(179 ページ) を参照してください。</li> </ul>

フィールド	説明/アクション
表示される変更イベントのタイプ	<p data-bbox="446 239 1219 264">イベントタイプのリストが表示されます。選択可能なイベントは次のとおりです。</p> <ul data-bbox="446 283 803 758" style="list-style-type: none"><li data-bbox="446 283 716 308">• デバイスがブートしました</li><li data-bbox="446 327 654 352">• デバイス構成の変更</li><li data-bbox="446 371 740 396">• デバイス診断が変化しました</li><li data-bbox="446 415 719 441">• デバイスパスワードの変更</li><li data-bbox="446 459 696 485">• 再ロードされたデバイス</li><li data-bbox="446 504 740 529">• デバイスソフトウェアの変更</li><li data-bbox="446 548 740 573">• モジュールが追加されました</li><li data-bbox="446 592 740 617">• モジュールが変更されました</li><li data-bbox="446 636 740 661">• モジュールが削除されました</li><li data-bbox="446 680 803 705">• 予約デバイス設定が変更されました</li><li data-bbox="446 724 634 749">• ユーザメッセージ</li></ul>

## 診断

NAでは、構成ファイルだけでなく、ルーティングテーブル、ポート統計、IP設定といった他のデバイス情報も収集されます。これらをまとめて診断といいます。診断を使用すると、構成変更による影響を判断したり、ルーティングエラーやパフォーマンス低下といった複雑な問題を解決したりできます。

デフォルトでは、NAが対象デバイスで構成変更を検出するたびに、デバイスから診断の基本セットがキャプチャされます。追加の診断タスクまたはイベントルールを定義して、そのときどきの診断をキャプチャしたり、追加のカスタム診断を定義して、使用環境に有用な特定のデバイス情報をキャプチャしたりできます。

NAを使用すると、特定のイベントの結果として発生する診断を自動的に起動できます。さらに、CPU使用率などの環境診断を作成および監視することにより、特定のしきい値に到達したときに自動化された反応および応答を実行できます。構成変更またはその他のイベントによる診断の自動実行の詳細については、「[イベントルールの追加](#)」(459ページ)を参照してください。

[デバイス]のメニューバーにある[デバイスツール]を選択し、[診断]をクリックします。[診断]ページが開きます。このページには、使用可能な診断のリストが表示されます。

## [診断]ページのフィールド

フィールド	説明/アクション
診断の新規作成	[診断の新規作成]ページが開きます。このページでは、新規診断を作成できます。詳細については、「 <a href="#">診断の新規作成</a> 」ページのフィールド」(551ページ)を参照してください。
診断の実行	[タスクの新規作成 - 診断の実行]ページが開きます。このページでは、あらゆる診断を実行できます。詳細については、「 <a href="#">診断の実行</a> 」タスクページのフィールド」(310ページ)を参照してください。
診断のインポート/エクスポート	[スクリプト/診断のインポート/エクスポート]ページが開きます。そのページで、構成前のコマンドスクリプトや診断スクリプトをインポートしたり、コマンドスクリプトや診断スクリプトをファイルへエクスポートできます。詳細については、「 <a href="#">スクリプト/診断のインポート/エクスポート</a> 」(575ページ)を参照してください。
チェックボックス	左側のチェックボックスをオンにすると、診断を削除できます。診断を選択したら、[アクション]ドロップダウンメニューをクリックし、[削除]をクリックします。これにより、選択した診断が削除されます。隣接の[選択]ドロップダウンメニューを使用すると、デバイスを全選択または全選択解除できます。
スクリプト名	診断名が表示されます。
モード/デバイスファミリー	診断を実行する際のデバイスアクセスモード（Cisco IOS enable モードなど）が表示されます。
最終変更	診断を最後に変更した日付および時刻が表示されます。
パーティション	診断を特定パーティションに適用できます。「[共有]」とラベル付けされた診断はすべてのパーティションに適用可能であることから、すべてのユーザが表示できます。  <b>注意：</b> NA管理者がデバイスをパーティション化した場合、ユーザは自分が表示権限を持つ特定パーティションに属す診断（とそのパーティションに属すデバイス）を表示、編集、実行できます。デバイスおよびユーザのセグメント化の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」(148ページ)を参照してください。

フィールド	説明/アクション
最終変更者	診断を最後に変更したユーザ名が表示されます（該当する場合）。
アクション	<p>次のオプションから選択できます。</p> <ul style="list-style-type: none"><li>• 編集 : [診断を編集] ページが開きます。このページでは、診断を編集できます。詳細については、「<a href="#">[診断の新規作成] ページのフィールド</a>」（551 ページ）を参照してください。</li><li>• 実行 : [タスクの新規作成 - 診断の実行] タスクページが開きます。このページでは、診断を実行できます。詳細については、「<a href="#">[診断の実行] タスクページのフィールド</a>」（310 ページ）を参照してください。</li></ul>

## [診断の新規作成]ページのフィールド

新規診断を作成するには、次の手順に従います。

1. [デバイス]のメニューバーにある[デバイスツール]を選択し、[診断]をクリックします。[診断]ページが開きます。
2. ページ上部の[診断の新規作成]リンクをクリックします。[診断の新規作成]ページが開きます。終了したら、必ず[スクリプトを保存]ボタンをクリックしてください。

フィールド	説明/アクション
診断	[診断]ページが開きます。このページでは、事前に定義された診断を作成または実行できます。詳細については、「 <a href="#">[診断]ページのフィールド</a> 」(549ページ)を参照してください。
名前	診断名を入力します。
説明	診断を説明するコメントを入力します。
パーティション	<p>診断を特定パーティションに適用できます。「[共有]」とラベル付けされた診断はすべてのパーティションに適用可能であることから、すべてのユーザが表示できます。</p> <p><b>注意:</b> NA管理者がデバイスをパーティション化した場合、ユーザは自分が表示権限を持つ特定パーティションに属す診断（とそのパーティションに属すデバイス）を表示、編集、実行できます。デバイスおよびユーザのセグメント化の詳細については、「<a href="#">デバイスとユーザのセグメント化</a>」(148ページ)を参照してください。</p>
高度なスクリプティング	<p>オンにすると、診断をユーザ定義変数のない高度なスクリプトとして定義できます。[モード]フィールドと[ドライバ]フィールドが以下のフィールドに置き換わります。</p> <ul style="list-style-type: none"> <li>• デバイスファミリ: このスクリプトの実行対象であるデバイスファミリの名前を選択します。デバイスファミリとは、類似する構成CLIコマンドシンタックスを共有する、デバイスの集合のことです。</li> <li>• 言語: スクリプトの記述に使用した言語を表示します。</li> <li>• パラメータ: スクリプトのパラメータを入力します。</li> </ul> <p>高度なスクリプトの作成の詳細については、「<a href="#">コマンドスクリプトの追加</a>」(576ページ)を参照してください。</p>
モード	デバイスアクセスモード（Cisco Exec、Nortel Managerなど）を選択します。
ドライバ	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 適用できる全ドライバ（デフォルト）</li> <li>• 特定のドライバを選択</li> </ul> <p>リストからドライバを1つ以上選択する場合は、ドライバを1つ選択するか、[Shift]+クリックまたは[Ctrl]+クリックを使用して複数のドライバを選択します。</p> <p>(<b>注意:</b> カスタム診断では、Baystack 470などのメニュー主導型デバイスにアクセスできません。)</p>

フィールド	説明/アクション
スクリプト	<p>実行するデバイス固有のコマンドを入力します。[スクリプト]ボックスの高さと幅は、[システム管理設定]オプションの設定によって制御されます。スクリプティング機能を広範囲にわたって使用する場合、スクロールしなくてもスクリプトを確認できるように、これらの設定の調整が必要となることがあります。</p> <p><b>注意：</b> スクリプトに同じ名前を付けることはできませんが、モードは別にしてください。この方法によって、NAはマルチベンダースクリプトを管理します。スクリプトを実行するには、単にスクリプト名を選択するだけです。各バージョンのスクリプトによってロードが行われます。デバイスグループに対してスクリプトを実行すると、NAはデバイスタイプを識別し、適切なスクリプトを適用します。</p>

特定のデバイスに対する診断を表示するには、次の手順に従います。

1. [デバイス]のメニューバーにある[インベントリ]をクリックします。
2. 診断情報を必要とするデバイスのホスト名またはIPアドレスをクリックします。
3. [表示]ドロップダウンメニューから、[診断]を選択し、表示する診断をクリックします。各オプションにより、デバイス固有の診断の履歴リストが示されます。

## カスタム診断の追加および編集

NAを使用すると、カスタム診断を定義し、使用環境に有用な特定の情報をキャプチャできます。各ユーザがカスタム診断を実行できるため、どのユーザもネットワーク問題を解析できます。これは、デバイス構成の変更権限を持たないユーザであっても同じです。

カスタム診断を定義するには、デバイスで実行するコマンドを1つ以上入力します。診断の結果として、これらのコマンドの結果がNAに保存されます。診断を実行する権限はすべてのユーザが持っています。そのため、これらのコマンドでデバイス構成を変更しないようにしてください。カスタム診断では、読み取り専用タスクを実行する必要があります。

イベントルールを使用することにより、診断を実行できます。たとえば、構成の配布に失敗するたびに診断を実行するようにルールを設定できます。

マルチベンダーネットワークの場合は、同じ名前で複数の診断を作成できますが、実行はそれぞれ別のデバイスで行います。同じ名前が付けられた診断は、互いにリンクします。グループタスクを実行すると、デバイスごとに適切なバージョンの診断が自動的に実行されます。たとえば、サンフランシスコにあるすべてのルータに関するデータを収集するようにグループ診断を実行できます。これは、ルータのベンダーが複数に及ぶ場合であっても同じです。

**注意：** NA データベースから定期的に古くなったデータを消去する必要があります。古くなったデータをすべて定期的に消去して、パフォーマンスを維持し、ディスク空き容量を回復することも重要ですが、特に重要なのは、診断とスクリプトデータを消去することです。以前のインスタンスと異なる場合にのみ保存される構成とは異なり、診断およびスクリプトデータはすべて保存されます。デフォルトでは、45日を経過した診断データが消去の対象となります。詳細については、[「\[データの整理\]タスクページのフィールド」\(385 ページ\)](#) を参照してください。



## 第13章：カスタムデータの設定

### トピックの参照先リスト

トピック	参照先：
はじめに	<a href="#">「はじめに」</a> （554ページ）
[カスタムデータの設定]ページのフィールド	<a href="#">「[カスタムデータの設定]ページのフィールド」</a> （554ページ）
拡張カスタムフィールド設定	<a href="#">「拡張カスタムフィールド設定」</a> （558ページ）

## はじめに

カスタムデータフィールドの目的は、有用なデータを特定のデバイス、構成、ユーザなどに割り当てることです。これにより、柔軟性が向上し、NAと他のアプリケーションの統合が実現します。

デフォルトで、HP Network Automation (NA) は最大で6個のカスタムデータフィールドをサポートします。拡張カスタムデータフィールドにより、[デバイス詳細] ページおよび [デバイスのインターフェイス] ページで最大25の追加カスタムデータフィールドを使用できます。拡張カスタムフィールドの有効化の詳細については、「[拡張カスタムフィールド](#)」(62 ページ) を参照してください。拡張カスタムフィールドの構成の詳細については、「[拡張カスタムフィールド設定](#)」(558 ページ) を参照してください。25を超える拡張カスタムフィールドの有効化の詳細については、『NA Administration Guide』を参照してください。

これまでは、いくつかのCLIコマンドに、コマンドの `customname` と `customvalue` オプションを使用してカスタムフィールドを変更する機能がありました。一度に1つのフィールドしか処理できませんでした。これは、複数のフィールドを変更する必要がある場合面倒な作業でした。今回のバージョンでは、「`customnames`」と「`customvalues`」の新しい値を使用して、複数のフィールドを指定して同時に変更できるようになりました。

ただし、名前と値はカンマ区切りリストで表示されます。カンマを含む値がある場合は、一重引用符で囲むようにしてください。例：

```
mod device -customnames "Location, Floor, Rack" -customvalues "'Seattle, WA', 3rd, '126-18, 10'"
```

**注意：** 既存のスクリプトとの後方互換性を維持するために、古いオプションも使用できます。

カスタムデータを追加するには、[管理]のメニューバーにある[カスタムデータの設定]をクリックします。[カスタムデータの設定]ページが開きます。

## [カスタムデータの設定]ページのフィールド

フィールド	説明/アクション
カスタムデータの設定	<p>ドロップダウンメニューから[カスタムデータの設定]を選択します。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>• デバイス構成と診断</li> <li>• デバイス</li> <li>• デバイスのブレード/モジュール</li> <li>• デバイスのインターフェイス</li> <li>• デバイスグループ</li> <li>• ユーザ</li> <li>• タスク</li> <li>• Telnet/SSH セッション</li> </ul>
チェックボックス	<p>左側のチェックボックスをオンにすると、フィールドを有効にできます。これにより、ユーザインターフェイスにフィールドが表示され、統合APIで使用できるようになります。</p>

フィールド	説明/アクション
-------	----------

### デバイス構成と診断

ここで設定するフィールドは、[デバイス構成の詳細]ページに表示されます。値を入力または変更するには、[コメントを編集]リンクをクリックします。これにより、[デバイス構成の詳細を編集]ページが開きます。

API名	統合APIおよび通知ルールに対するフィールドです。API名には、A～Z、a～z、0～9、_、-、&を使用できます（カンマは含まれません）。
表示名	ユーザインターフェイスに表示される名前が表示されます。
値	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>HTMLを含めることができる：オンにした場合（デフォルト）、ユーザ（または統合API）は、このフィールドにHTMLコードを入力する必要があります。NAのユーザインターフェイスのフィールドが、テキストではなく、HTMLで表示されます。これにより、外部トラブルチケットアプリケーションへのリンクを追加できます。</li> <li>絞り込み：オンにした場合、値をカンマで区切って入力します。これらの値は、ドロップダウンリストボックスに表示されます。</li> </ul>

### デバイス

ここで設定するフィールドは、[デバイス情報]ページに表示されます。値を入力または変更するには、[編集]リンクまたは[デバイス]ドロップダウンメニューの[追加]をクリックします。[編集]リンクをクリックすると、[デバイスの編集]ページが開き、[追加]をクリックすると、[デバイスの新規作成]ページが開きます。

API名	統合APIおよび通知ルールに対するフィールドです。API名には、A～Z、a～z、0～9、_、-、&を使用できます（カンマは含まれません）。
表示名	ユーザインターフェイスに表示される名前が表示されます。
値	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>HTMLを含めることができる：オンにした場合（デフォルト）、ユーザ（または統合API）は、このフィールドにHTMLコードを入力する必要があります。NAのユーザインターフェイスのフィールドが、テキストではなく、HTMLで表示されます。これにより、外部トラブルチケットアプリケーションへのリンクを追加できます。</li> <li>絞り込み：オンにした場合、値をカンマで区切って入力します。これらの値は、ドロップダウンリストボックスに表示されます。</li> </ul>

### デバイスのブレード/モジュール

ここで設定するフィールドは、[モジュールを表示]ページおよび[モジュールを編集]ページに表示されます。

API名	統合APIおよび通知ルールに対するフィールドです。API名には、A～Z、a～z、0～9、_、-、&を使用できます（カンマは含まれません）。
表示名	ユーザインターフェイスに表示される名前が表示されます。
値	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>HTMLを含めることができる：オンにした場合（デフォルト）、ユーザ（または統合API）は、このフィールドにHTMLコードを入力する必要があります。NAのユーザインターフェイスのフィールドが、テキストではなく、HTMLで表示されます。これにより、外部トラブルチケットアプリケーションへのリンクを追加できます。</li> <li>絞り込み：オンにした場合、値をカンマで区切って入力します。これらの値は、ドロップダウンリストボックスに表示されます。</li> </ul>

フィールド	説明/アクション
-------	----------

### デバイスのインターフェイス

ここで設定するフィールドは、[モジュールを表示]ページおよび[モジュールを編集]ページに表示されます。

API名	統合APIおよび通知ルールに対するフィールドです。API名には、A～Z、a～z、0～9、_、-、&を使用できます（カンマは含まれません）。
表示名	ユーザインターフェイスに表示される名前が表示されます。
値	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>HTMLを含めることができる：オンにした場合（デフォルト）、ユーザ（または統合API）は、このフィールドにHTMLコードを入力する必要があります。NAのユーザインターフェイスのフィールドが、テキストではなく、HTMLで表示されます。これにより、外部トラブルチケットアプリケーションへのリンクを追加できます。</li> <li>絞り込み：オンにした場合、値をカンマで区切って入力します。これらの値は、ドロップダウンリストボックスに表示されます。</li> </ul>

### デバイスグループ

ここで設定するフィールドは、対象グループの[デバイスリスト]ページに表示されます。値を入力または変更するには、[グループを編集]リンクまたは[デバイス]ドロップダウンメニューの[グループ]をクリックします。[グループを編集]リンクをクリックすると、[グループを編集]ページが開き、[グループ]をクリックすると、[グループの新規作成]ページが開きます。

API名	統合APIおよび通知ルールに対するフィールドです。API名には、A～Z、a～z、0～9、_、-、&を使用できます（カンマは含まれません）。
表示名	ユーザインターフェイスに表示される名前が表示されます。
値	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>HTMLを含めることができる：オンにした場合（デフォルト）、ユーザ（または統合API）は、このフィールドにHTMLコードを入力する必要があります。NAのユーザインターフェイスのフィールドが、テキストではなく、HTMLで表示されます。これにより、外部トラブルチケットアプリケーションへのリンクを追加できます。</li> <li>絞り込み：オンにした場合、値をカンマで区切って入力します。これらの値は、ドロップダウンリストボックスに表示されます。</li> </ul>

### ユーザ

次に示すフィールドは、[自分のプロフィール]ページに表示されます。値を入力または編集するには、[ユーザリスト]ページの[編集]リンクまたは[ユーザリスト]ページの[ユーザの新規作成]をクリックします。[編集]リンクをクリックすると、[ユーザを編集]ページが開き、[ユーザの新規作成]をクリックすると、[ユーザの新規作成]ページが開きます。

API名	統合APIおよび通知ルールに対するフィールドです。API名には、A～Z、a～z、0～9、_、-、&を使用できます（カンマは含まれません）。
表示名	ユーザインターフェイスに表示される名前が表示されます。
値	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>HTMLを含めることができる：オンにした場合（デフォルト）、ユーザ（または統合API）は、このフィールドにHTMLコードを入力する必要があります。NAのユーザインターフェイスのフィールドが、テキストではなく、HTMLで表示されます。これにより、外部トラブルチケットアプリケーションへのリンクを追加できます。</li> <li>絞り込み：オンにした場合、値をカンマで区切って入力します。これらの値は、ドロップダウンリストボックスに表示されます。</li> </ul>

フィールド	説明/アクション
<b>タスク</b>	
ここで設定するフィールドは、[タスク]ページに表示されます。ユーザインターフェイスから値を入力または編集することはできません。値の入力または編集は、統合APIを介してのみ可能です。	
API名	統合APIおよび通知ルールに対するフィールドです。API名には、A～Z、a～z、0～9、_、-、&を使用できます（カンマは含まれません）。
表示名	ユーザインターフェイスに表示される名前が表示されます。
値	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• HTMLを含めることができる：オンにした場合（デフォルト）、ユーザ（または統合API）は、このフィールドにHTMLコードを入力する必要があります。NAのユーザインターフェイスのフィールドが、テキストではなく、HTMLで表示されます。これにより、外部トラブルチケットアプリケーションへのリンクを追加できます。</li> <li>• 絞り込み：オンにした場合、値をカンマで区切って入力します。これらの値は、ドロップダウンリストボックスに表示されます。</li> </ul>
<b>Telnet/SSHセッション</b>	
ここで設定するフィールドは、[Telnet/SSHセッションリスト]ページに表示されます。ユーザインターフェイスから値を入力または編集することはできません。値の入力または編集は、統合APIを介してのみ可能です。	
API名	統合APIおよび通知ルールに対するフィールドです。API名には、A～Z、a～z、0～9、_、-、&を使用できます（カンマは含まれません）。
表示名	ユーザインターフェイスに表示される名前が表示されます。
値	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• HTMLを含めることができる：オンにした場合（デフォルト）、ユーザ（または統合API）は、このフィールドにHTMLコードを入力する必要があります。NAのユーザインターフェイスのフィールドが、テキストではなく、HTMLで表示されます。これにより、外部トラブルチケットアプリケーションへのリンクを追加できます。</li> <li>• 絞り込み：オンにした場合、値をカンマで区切って入力します。これらの値は、ドロップダウンリストボックスに表示されます。</li> </ul>

## 拡張カスタムフィールド設定

カスタムフィールドを使用すると、有用なデータを特定のデバイスに割り当てることができます。これにより、柔軟性が向上し、NAと他のアプリケーションの統合が実現します。

**注意：** 拡張カスタムフィールドを追加する前に、[拡張カスタムフィールド]アプリケーションを有効化する必要があります。詳細については、「[\[ユーザインターフェイス\]ページのフィールド](#)」(61 ページ) を参照してください。

現在のカスタムフィールドを表示したり、データを[デバイス詳細]ページおよび[デバイスのインターフェイス]ページに追加したりするには、[管理]のメニューバーにある[拡張カスタムフィールド設定]をクリックします。[拡張カスタムフィールド設定]ページが開きます。

フィールド	説明/アクション
ドロップダウンメニュー	ドロップダウンメニューから、次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• Devices (デフォルト)</li> <li>• Device Interfaces</li> </ul>
[カスタムデバイスフィールドの新規作成]へのリンク	[カスタムデバイスフィールドの新規作成]リンクをクリックすると、[カスタムデータフィールドの新規作成]ページが開きます。このページでは、カスタムデータフィールドを追加できます。これらのデータフィールドは、[デバイス詳細]ページおよび[デバイスのインターフェイス]ページに表示されます。詳細については、「 <a href="#">[カスタムデータフィールドの新規作成]ページ</a> 」(559 ページ) を参照してください。[デバイス詳細]ページおよび[デバイスのインターフェイス]ページの詳細については、「 <a href="#">表示メニューオプション</a> 」(201 ページ) および「 <a href="#">[デバイスインターフェイス]ページのフィールド</a> 」(205 ページ) を参照してください。
<b>Devices / Device Interfaces</b>	
有効	カスタムデータフィールドが有効かどうかを示します。
フィールド名	カスタムデータフィールド名が表示されます。
値	カンマで区切られた値のリストが表示されます。このリストは、実際のデータを編集する際、ドロップダウンメニューとして表示されます。
HTMLを含めることができる	ユーザがこのデータフィールドにHTMLコードを入力できるかどうかを示します。データフィールドがテキストではなく、HTMLとして表示されます。
アクション	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• 編集：[カスタムデータフィールドの編集]ページが開きます。このページでは、現在の情報を編集できます。「<a href="#">[カスタムデータフィールドの新規作成]ページ</a>」(559 ページ) を参照してください。</li> <li>• 削除：カスタムデータフィールドを削除できます。データフィールドを削除すると、削除したフィールドに関連するあらゆるデータが同様に削除されます。</li> </ul>

## [カスタムデータフィールドの新規作成]ページ

[デバイス詳細]ページおよび[デバイスのインターフェイス]ページにカスタムデータフィールドを追加するには、[管理]のメニューバーにある[拡張カスタムフィールド設定]をクリックします。[拡張カスタムフィールド設定]ページが開きます。ページ上部の[カスタムデバイスフィールドの新規作成]リンクをクリックします。

フィールド	説明/アクション
有効	オンにすると、カスタムデータフィールドが有効になります。
フィールド名	データフィールド名を入力します。
値を制限	カンマで区切られた値のリストを入力します。このリストは、実際のデータを編集する際、ドロップダウンメニューとして表示されます。
HTMLを許可	オンにすると、このフィールドにHTMLコードを入力できます。フィールドがテキストではなく、HTMLとして表示されます。

終了したら、[保存]ボタンをクリックします。[拡張カスタムフィールド設定]ページに新規フィールドが表示されます。





## 第14章：構成テンプレートの作成

### トピックの参照先リスト

トピック	参照先：
はじめに	<a href="#">「はじめに」</a> （562ページ）
構成テンプレートの表示	<a href="#">「構成テンプレートの表示」</a> （563ページ）
新規構成テンプレートの作成	<a href="#">「新規構成テンプレートの作成」</a> （565ページ）

## はじめに

構成テンプレートを使用すると、新規デバイス構成を迅速かつ簡単に配布できます。構成テンプレートを使用することにより、次のことを実行できます。

- エンジニアは、部門別の構成標準に準拠しつつ、デバイスまたはサービスを迅速に提供できます。
- ネットワーク設計者は、検証パラメータを使用することにより、使い勝手のよいGUIプロンプトを作成できます。これにより、テンプレートユーザは、空欄を埋めるだけで、速やかに新規構成を実装および配布できます。

一般的に構成テンプレートは、スクリプトを構成するためにさまざまな方法で組み合わせることが可能である、構成データの断片です。さらに、このスクリプトをデバイス上のデータに追加したり、構成の一部と置き換えられます。

デバイステンプレートの作成の詳細については、「[デバイステンプレート](#)」(118ページ)を参照してください。

構成テンプレートを作成し、コマンドを使用してそれを実装すると、そのテンプレートからスクリプトを作成できます。スクリプトを実行すると、構成コマンドが断片または構成全体として、1つまたは複数のデバイスに配布されます。

## 構成テンプレートの表示

現在の構成テンプレートを表示するには、[デバイス]のメニューバーにある[デバイスツール]を選択し、[構成テンプレート]をクリックします。[構成テンプレート]ページが開きます。このページを使用すると、ベンダー別にソートされた構成テンプレートのリストを表示できます。

## [構成テンプレート]ページのフィールド

フィールド	説明/アクション
テンプレートの新規作成	[テンプレートの新規作成]ページが開きます。このページでは、新規構成テンプレートを作成できます。詳細については、「 <a href="#">新規構成テンプレートの作成</a> 」(565ページ)を参照してください。
ベンダー	<p>この構成テンプレートが適用されるデバイスのベンダーが表示されます。ベンダーのリンクをクリックすると、[構成テンプレート]ページが開きます。このページには、このベンダーのテンプレートが表示されます。このページでできることは次のとおりです。</p> <ul style="list-style-type: none"> <li>• スクリプトへの構成テンプレートの追加およびテンプレートからのフルスクリプトの構築</li> <li>• 新規構成テンプレートの作成</li> </ul>
チェックボックス	左側のチェックボックスをオンにすると、構成テンプレートを削除できます。テンプレートを選択したら、[アクション]ドロップダウンメニューをクリックし、[削除]をクリックします。これにより、選択した構成テンプレートが削除されます。隣接の[選択]ドロップダウンメニューを使用すると、構成テンプレートを全選択または全選択解除できます。
名前	構成テンプレート名が表示されます。
パーティション	<p>セキュリティや業務上の理由でパーティションを作成した場合、特定パーティションの各デバイスについて構成テンプレートをパーティションできます。構成テンプレートを、特定のパーティション内の特定デバイスに加え、すべてのパーティション内のすべてのデバイスで共有するように構成できます。パーティションの作成の詳細については、「<a href="#">デバイスとユーザのセグメント化</a>」(148ページ)を参照してください。</p> <p><b>注意:</b> このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。一般的に、パーティションとは一意のIPアドレスを持つデバイスのグループです。単一のNAコアで複数のパーティションを管理できます。NAコアはNAサーバのインストールコンポーネントの1つで、単一の管理エンジン、関連サービス、および単一のデータベースからなります。</p>
ロール	<p>構成テンプレートのロールが表示されます。デフォルトのロールは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 任意</li> <li>• コア</li> <li>• 境界</li> <li>• テスト</li> </ul>
モデル	この構成テンプレートが適用されるデバイスのモデルが表示されます。
プロセッサ/ コンポーネント	この構成テンプレートが適用されるデバイスのプロセッサが表示されます。
ドライバ	この構成テンプレートが適用されるデバイスに割り当てられたドライバが表示されます。

フィールド	説明/アクション
アクション	<p>次のオプションからいずれか1つを選択できます。</p> <ul style="list-style-type: none"><li>• <b>詳細を表示</b>:[テンプレートを表示]ページが開きます。このページでは、構成テンプレートがHTMLとして個別ブラウザウィンドウに表示されます。詳細については、「<b>[テンプレートを表示]ページのフィールド</b>」(567 ページ)を参照してください。</li><li>• <b>テキストを表示</b>:テキストウィンドウが開きます。このページでは、構成テンプレートがテキストとして個別ブラウザウィンドウに表示されます。詳細については、「<b>[テンプレートを表示]ページのフィールド</b>」(567 ページ)を参照してください。</li><li>• <b>編集</b>:[テンプレートを編集]ページが開きます。このページでは、構成テンプレートを追加または編集できます。詳細については、「<b>[テンプレートの新規作成]ページのフィールド</b>」(565 ページ)を参照してください。</li></ul>

## 新規構成テンプレートの作成

新規構成テンプレートを作成するには：

1. [デバイス]のメニューバーにある[デバイスツール]を選択し、[構成テンプレート]をクリックします。[構成テンプレート]ページが開きます。
2. ページ上部の[テンプレートの新規作成]リンクをクリックします。[テンプレートの新規作成]ページが開きます。終了時に、必ず[テンプレートを保存]ボタンをしてください。

## [テンプレートの新規作成]ページのフィールド

フィールド	説明/アクション
テンプレート	[構成テンプレート]ページが開きます。このページでは、現在のすべての構成テンプレートを表示できます。詳細については、「 <a href="#">構成テンプレートの表示</a> 」(563ページ)を参照してください。
名前	構成テンプレートの名前を入力します。
パーティション	ドロップダウンメニューからパーティションを選択します。(注意：このフィールドは1つ以上のパーティションを構成した場合にのみ表示されます。) <p>セキュリティや業務上の理由でパーティションを作成した場合、特定パーティションの各デバイスについて構成テンプレートをパーティションできます。構成テンプレートを、特定のパーティション内の特定デバイスに加え、すべてのパーティション内のすべてのデバイスで共有するように構成できます。パーティションの作成の詳細については、「<a href="#">デバイスとユーザのセグメント化</a>」(148ページ)を参照してください。</p>
コメント	構成テンプレートの説明を入力します。コメントはすべてのテーブルに追加されるため、重要情報のみを入力してください。
ロール	構成テンプレートのロールを選択します。デフォルトのロールは次のとおりです。 <ul style="list-style-type: none"> <li>• 任意</li> <li>• コア</li> <li>• 境界</li> <li>• テスト</li> </ul>
モデル	この構成テンプレートが適用されるデバイスのモデルを入力します。
プロセッサ/ コンポーネント	この構成テンプレートが適用されるデバイスのプロセッサを入力します。
モード	構成テンプレートを実行する際のデバイスコマンドラインインターフェイス (CLI) モードを選択します。(注意：コマンドではCLIのプロンプトまたはモードを変更しないでください。変更すると、そのコマンドでのスクリプトの実行が停止され、エラーが返されます。)
ドライバ	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• 適用できる全ドライバ (デフォルト)</li> <li>• 特定のドライバを選択：この構成テンプレートを適用するデバイスに割り当てられたドライバを選択します。リストには、選択したモードと互換性があるドライバのみが表示されます。</li> </ul>

フィールド	説明/アクション
テンプレート	<p>構成テンプレートを実装する構成コマンドおよびコメントを入力します。入力する各行は、デバイスに対する1つの完全なコマンドを表す必要があります。コマンドの後に、デバイスのプロンプトが再度表示されます。構成テンプレートをデバイスに適用すると、この構成が配布されます。</p> <p>変数名の先頭に「tc_」を付けることはできません。ただし、変数には、大文字のアルファベット、小文字のアルファベット、0～9、およびアンダースコア文字のあらゆる組み合わせを使用できます。</p>

## [テンプレートを表示]ページのフィールド

特定の構成テンプレートを表示するには：

1. [デバイス]のメニューバーにある[デバイスツール]を選択し、[構成テンプレート]をクリックします。[構成テンプレート]ページが開きます。
2. 表示対象の構成テンプレートの[アクション]列にある[詳細を表示]オプションをクリックします。[テンプレートを表示]ページが開きます。

フィールド	説明/アクション
テンプレートを編集	[テンプレートを編集]ページが開きます。このページでは、新規構成テンプレートを作成できます。詳細については、「 <a href="#">[テンプレートの新規作成]ページのフィールド</a> 」(565 ページ) を参照してください。
テキストバージョン	テキストウィンドウが開きます。このページでは、構成テンプレートがテキストとして個別ブラウザウィンドウに表示されます。テキストは次のように表示されています。 <pre>sflow destination \$dest_ip_1\$ \$dest_udp_port1\$ sflow destination \$dest_ip_2\$ \$dest_udp_port2\$</pre>
テンプレート	[構成テンプレート]ページが開きます。このページには、ベンダー別にソートされたテンプレートのリストが表示されます。詳細については、「 <a href="#">[構成テンプレート]ページのフィールド</a> 」(563 ページ) を参照してください。
コメント	構成テンプレート作成者によって入力されたコメント、または後から編集されたコメントが表示されます(注意：コメントが入力されていない場合、[コメント]ボックスは表示されません)。
行	構成テンプレート内での各行の番号が表示されます。
テンプレートテキスト	構成テンプレートを実装する構成コマンドおよびコメントが表示されます。
名前	構成テンプレート名が表示されます。
パーティション	セキュリティや業務上の理由でパーティションを作成した場合、特定パーティションの各デバイスについて構成テンプレートをパーティションできます。構成テンプレートを、特定のパーティション内の特定デバイスに加え、すべてのパーティション内のすべてのデバイスで共有するように構成できます。パーティションの作成の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」(148 ページ) を参照してください。
モデル	この構成テンプレートが適用されるデバイスのモデルが表示されます。
最終変更者	構成テンプレートを最後に変更したユーザ、またはプロセスが表示されます。
ロール	構成テンプレートのロールが表示されます。デフォルトのロールは次のとおりです。 <ul style="list-style-type: none"> <li>• 任意</li> <li>• コア</li> <li>• 境界</li> <li>• テスト</li> </ul>
最終変更日	構成テンプレートを最後に変更した日付が表示されます。
プロセッサ/ コンポーネント	この構成テンプレートが適用されるデバイスのプロセッサが表示されます。

フィールド	説明/アクション
モード	構成テンプレートを実行する際のデバイスコマンドラインインターフェイス（CLI）モードが表示されます。
ドライバ	この構成テンプレートが適用されるデバイスに割り当てられたドライバが表示されます。



## 第15章：コマンドスクリプトの管理

### トピックの参照先リスト

トピック	参照先：
はじめに	<a href="#">「はじめに」</a> (570 ページ)
コマンドスクリプトの追加および編集	<a href="#">「コマンドスクリプトの追加」</a> (576 ページ)
コマンドスクリプトの実行	<a href="#">「コマンドスクリプトの実行」</a> (590 ページ)
自動修正スクリプトの作成	<a href="#">「自動修正スクリプトの作成」</a> (581 ページ)
コマンドスクリプトと診断のインポートとエクスポート	<a href="#">「スクリプト/診断のインポート/エクスポート」</a> (575 ページ)

## はじめに

コマンドスクリプトを定義することにより、1つまたは複数のアクティブデバイス上で一連のコマンドを実行できます。コマンドスクリプトは、デバイスのグループに対するバッチ処理に特に便利です。たとえば、インベントリグループに対してスクリプトを実行すると、SNMPトラップロギングホスト、NTPサーバ、または企業ログインバナーの設定など、標準ポリシーに一致するすべてのデバイスを更新できます。

高度なスクリプティング機能を使用すると、ExpectやPERLなど、さまざまなコマンドライン言語で記述されたカスタムスクリプトを実行できます。高度なスクリプティングでは、条件付きロジックの拡張機能を使用できます。高度なスクリプトは、フル機能搭載のExpectエンジンをサポートしているため、外部のTelnet/SSHクライアントが個別のプロセスで呼び出され、実行されます。高度なスクリプティング機能の詳細については、[「\[コマンドスクリプトの新規作成\]ページのフィールド」\(578ページ\)](#)を参照してください。

**注意：** 高度なスクリプティング機能を使用するには、言語サポートをインストールする必要があります。さらに、システム管理設定を構成して、有効化する必要があります。Expect言語のサポートは、NAと一緒にインストールされます。Windows環境でPERLスクリプティング機能を使用する場合は、PERL（CPAN）をインストールする必要があります。

## HP Operations Orchestration（HP OO）のフロー

高度なコマンドスクリプト経由でHP Operations Orchestration（HP OO）のフローを実行するには：

1. HP Operations Orchestrationの認証設定が正しく構成されていることを確認します。詳細については、[「ユーザ認証」\(73ページ\)](#)を参照してください。
2. [高度なスクリプティング]ボックスをオンにし、言語として「Flow」を選択します。高度なスクリプティングによって、NAは「Flow」言語タイプを使用するようになります。それ以外の場合、NAでは、シンタックスをIOSなどのデバイスシンタックスとして解釈しようとします。
3. スクリプトフィールドに次のように入力します。`/PAS/services/http/execute/Library/<path to flow>?flowvariable=value,flowvariable2=value2`

**注意：** 必要に応じてコマンドスクリプト変数、および任意の数のHP OOフロー入力変数を使用することもできます。HP OOの使用の詳細については、『HP Operations Orchestration Software Development Kit Guide（HP Operations Orchestrationソフトウェア開発キットガイド）』を参照してください。

## ベアメタルプロビジョニングスクリプト

ベアメタルプロビジョニングスクリプトにより、ベアメタルデバイスをNAデバイスドライバがアクセス可能なステータスにまで移行できます。ベアメタルスクリプトの作成は、標準コマンドスクリプトの作成と同じです。ベアメタルスクリプト内ではすべてのカスタムスクリプト変数が使用できます。ただし、ベアメタルスクリプト作成時に必須である作業がいくつかあります。

- スクリプトタイプとして「ベアメタルスクリプト」を選択する
- ベアメタルモードの1つを選択する
- コマンドスクリプトに適切な名前を付ける。名前にはスクリプトの実行対象であるデバイスファミリを含める

**注意：**ベアメタルスクリプトタイプを選択すると、高度なスクリプティングを使用できますが、[高度なスクリプト]チェックボックスを選択しないことを推奨します。

ベアメタルプロビジョニングの詳細については、「[\[デバイスの編集\]ページのフィールド](#)」(111ページ)を参照してください。

通常のベアメタルスクリプトシナリオを以下に挙げます。

1. デバイスをラックマウントします。
2. デバイスへのコンソールアクセス（または管理IPアドレス）をセットアップします。
3. NAにログインします。
4. [デバイス]の下メニューバーで、[新規作成]を選択し[デバイス]をクリックします。[デバイスの新規作成]ページが開きます。NAへのデバイスの追加の詳細については、「[デバイスの追加](#)」(106ページ)を参照してください。
5. 以下の情報によりNAにデバイスを追加します。
  - IPアドレス
  - ホスト名
  - パスワード
  - コンソールアドレス/ポート（デバイスにアクセス可能な管理IPアドレスが構成されていない場合）
  - その他の適切なデバイスフィールド
6. 「実稼動前」管理ステータスを選択します。
7. このデバイスのベアメタルドライバを指定します。
8. デバイスを保存します。[デバイス詳細]ページが開きます。
9. [プロビジョニング]メニューから、[コマンドスクリプトの実行]をクリックします。[タスクの新規作成 - コマンドスクリプトの実行]ページが開きます。ページには、ベアメタルスクリプトのリストが自動的に表示されます。「[コマンドスクリプトの実行](#)」(590ページ)を参照してください。
10. デバイスに合ったベアメタルスクリプトを選択し、必要に応じてスクリプト変数の値を入力します。
11. スクリプトを実行します。[タスクの新規作成 - コマンドスクリプトの実行]ページで[ドライバ検出]をオンにした場合、スクリプトが正常に動作すれば、検出タスクが自動的にスケジュールされます。必要に応じてこのオプションを無効にできます。

## 12. 検出タスクが正常に動作すれば、デバイスはベアメタル段階から実稼働前デバイスへと移行します

Cisco 2800 デバイスのベアメタルスクリプトの一例を以下に挙げます。

```
#scriptvar.carriage_return="\r"
#scriptvar.command_delay="3"
#scriptvar.baremetal_timeout="5"
#scriptvar.success_pattern=/Building configuration/
yes
yes
$tc_device_hostname$
$tc_device_password$
$legacy_enable_password$
$tc_device_enable_password$
no
FastEthernet0/0
yes
no
yes
$tc_device_ip$
$network_mask$
2
```

ベアメタルスクリプト作成時には、以下の点に注意してください。

- ベアメタルスクリプトの先頭で、いくつかのスクリプト設定を定義できます（すべてオプション）。これらの行は#scriptvarで始まります。
- Carriage\_returns は、各コマンドでデバイスに送信される改行のフォーマットを定義します。これは、\r、\n、\r\n、またはnone（各コマンド後に改行が送信されない）のいずれかにできます。
- Command\_delaysは、NAがスクリプトの次のコマンドをデバイスに送信するまでの待機時間（秒）を定義します。
- Baremetal\_timeoutは、コマンドの予測されるタイムアウトを定義します。
- Success\_patterns は、正規表現パターンです。有効な正規表現パターンが定義されている場合、このようなパターンがデバイス出力と一致する場合のみ、タスクが成功したと考えられます。

## コマンドスクリプトの表示

事前に定義されたコマンドスクリプトおよびカスタムコマンドスクリプトのリストを表示する場合は、[デバイス]のメニューバーにある[デバイスツール]を選択して、[コマンドスクリプト]をクリックします。[コマンドスクリプト]ページが開きます。このページには、権限を持っているコマンドスクリプトのリストが表示されます。コマンドスクリプトに対するフルアクセスを有するユーザは、NAに用意されている事前定義済みスクリプトを選択できます。

## [コマンドスクリプト]ページのフィールド

フィールド	説明/アクション
コマンドスクリプトの新規作成	[コマンドスクリプトの新規作成]ページが開きます。このページでは、新規スクリプトを記述したり、スクリプトから変数を取り出したりすることにより、プロンプトを定義できます。詳細については、「 <a href="#">[コマンドスクリプトの新規作成]ページのフィールド</a> 」(578ページ)を参照してください。
コマンドスクリプトの実行	[タスクの新規作成 - コマンドスクリプトの実行]ページが開きます。このページでは、コマンドスクリプトを実行するタスクを設定できます。スクリプト内の変数を編集し、スクリプトの一意のインスタンスを作成してからタスクを保存してください。詳細については、「 <a href="#">[コマンドスクリプトの実行]タスクページのフィールド</a> 」(304ページ)を参照してください。
コマンドスクリプトのインポート/エクスポート	[スクリプト/診断のインポート/エクスポート]ページが開きます。そのページで、構成前のコマンドスクリプトをインポートしたり、コマンドスクリプトをファイルへエクスポートできます。詳細については、「 <a href="#">スクリプト/診断のインポート/エクスポート</a> 」(575ページ)を参照してください。
スクリプトタイプ	[スクリプトタイプ]ドロップダウンメニューを使用すると、特定のタイプのスクリプトだけが表示されるようにスクリプトのリストをフィルタリングできます。
チェックボックス	左側のチェックボックスをオンにすると、スクリプトを削除できます。スクリプトを選択したら、[アクション]ドロップダウンメニューをクリックし、[削除]をクリックします。これにより、選択したスクリプトが削除されます。隣接の[選択]ドロップダウンメニューを使用すると、スクリプトを全選択または全選択解除できます。
スクリプト名	スクリプト名が表示されます。
モード/デバイスファミリ	スクリプトを実行するときのデバイスアクセスモード（Cisco Exec、Nortel Managerなど）が表示されます。高度なスクリプティングで使用する[デバイスファミリ]には、類似する構成のCLIコマンド構文を共有するデバイスの集合が表示されます。
最終変更	スクリプトを最後に変更した日付および時刻が表示されます。
パーティション	コマンドスクリプト、診断結果のいずれかまたは両方を、特定パーティションに適用できます。「グローバル」とラベル付けされたコマンドスクリプト、診断結果のいずれかまたは両方は、すべてのパーティションに適用可能であることから、すべてのユーザが表示できます。  <b>注意：</b> NA管理者がデバイスをパーティション化した場合、ユーザが表示権限を持つ特定パーティションに属すコマンドスクリプト、診断結果のいずれかまたは両方のみ、ユーザは表示、編集、実行できます。デバイスおよびユーザのセグメント化の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」(148ページ)を参照してください。
最終変更者	スクリプトを最後に変更したユーザ名が表示されます。たとえば、スクリプトがスクリプトテンプレートである場合、このフィールドには、特定のインスタンスに対するスクリプトを変更したユーザが表示されます。

フィールド	説明/アクション
アクション	<p>次のオプションからいずれか1つを選択できます。</p> <ul style="list-style-type: none"><li>• <b>編集</b> : [コマンドスクリプトを編集] ページが開きます。このページでは、既存のスクリプトを変更できます。詳細については、「<a href="#">[コマンドスクリプトの新規作成] ページのフィールド</a>」(578 ページ) を参照してください。</li><li>• <b>実行</b> : [タスクの新規作成 - コマンドスクリプトの実行] ページが開きます。このページでは、コマンドスクリプトを実行できます。詳細については、「<a href="#">[コマンドスクリプトの実行] タスクページのフィールド</a>」(304 ページ) を参照してください。</li></ul>

## スクリプト/診断のインポート/エクスポート

[コマンドスクリプト]ページにある[コマンドスクリプトのインポート/エクスポート]リンクをクリックすると、[スクリプト/診断のインポート/エクスポート]ページが開きます。

フィールド	説明/アクション
インポート	<p>インポートする内容を選択します。</p> <ul style="list-style-type: none"><li>• ドライバ以外のソースからコマンドスクリプトまたは診断をインポートするには、[ファイルからインポート]を選択し、ファイル名を入力して[参照]をクリックします。</li><li>• NA で提供されるデバイスドライバからコマンドスクリプトまたは診断をインポートするには、[ドライバからインポート]を選択し、カスタムコンテンツを含むドライバのリストから選択します。</li></ul> <p>[インポート]をクリックしてインポートするスクリプトを選択し、[続行]をクリックします。コマンドスクリプトや診断スクリプトが既に存在する場合、名前を変更するように求められます。</p>
スクリプトのエクスポート	<p>現在のコマンドスクリプト、および診断スクリプトのリストが表示されます。エクスポートするスクリプトをクリックしてから、[エクスポート]ボタンをクリックします。</p>

## コマンドスクリプトの追加

コマンドスクリプトを実行すると、次のことが可能になります。

- 1つまたは複数のデバイス上で一連のカスタムコマンドを実行できます。
- スクリプトをスケジュールされたタスクとして実行したり、イベントルールを使用してスクリプトを実行できます。たとえば、特定のデバイスタイプのデバイスが追加されるたびに、そのデバイスタイプに対して標準設定が構成されるようにルールを設定できます。

NAには、スクリプトを追加するためのオプションが複数用意されています。以下のことが可能です。

- [コマンドスクリプトの新規作成] ページにスクリプトを記述したり、スクリプトをコピーしたりできます（必要に応じて、変数の追加やプロンプトの定義も可能です）。
- スクリプトを実行する前にユーザが変数値を変更できるテンプレートスクリプトを作成します。詳細については、「[構成テンプレートからのスクリプトの作成](#)」（590ページ）を参照してください。
- セッションログを Expect または Perl スクリプトに変換します。NA は Expect をインストールするため、[Expectスクリプトに変換]リンクはなにもしなくても利用できます。[Convert to Perl(Perlに変換)]リンクが表示されるのは、[システム管理設定]でPerlをスクリプト用言語として構成した場合のみです。詳細については、「[\[サーバ\]ページのフィールド](#)」（52ページ）を参照してください。Perlスクリプトに変換リンクは、NAのインストール時に `Opware::NA::Connect Perl` モジュールを必要とします。

NAでは、単純なスクリプティングと高度なスクリプティングの両方をサポートしています。

単純なスクリプティングはモードベース（CLI コマンド言語）です。単純なコマンドスクリプトは、デバイス CLI エラーを認識しません。そのため、NAでは、実行されたデバイス CLI コマンドが正常に終了していることが前提となります。単純なコマンドスクリプトは、デバイスに到達できない場合、またはスクリプトの実行中にデバイスへの接続が失われた場合にのみエラーとなります。

高度なスクリプティングは、ExpectやPERLなどの任意のコマンドラインスクリプト言語を基にします。これらの言語には、条件付きロジック（*if*、*while*、および *for* などの条件）を含むスクリプトが含まれます。変数を組み合わせることにより、スクリプトのインスタンスをカスタマイズできます。スクリプトを実行すると、各変数について値の入力が要求されます。詳細は、次の表を参照してください。

**注意：**文字「\$」は、変数名用に予約されています。スクリプト中にリテラルの「\$」を入力する必要がある場合、エスケープシーケンス `\x24` を使用してください。

単純なスクリプト	高度なスクリプト
<ul style="list-style-type: none"> <li>• ifまたはループは使用不可</li> <li>• デバイスコマンド（<i>show conf</i>のようなCiscoのコマンド）を使用</li> <li>• エラー処理なし</li> <li>• ログイン不要</li> <li>• NAデバイス変数なし</li> </ul>	<ul style="list-style-type: none"> <li>• ifまたはループ使用可能</li> <li>• 言語コマンドを使用（<i>send "show conf\n"</i>や<i>print SOCKET "show conf\n"</i>などのPERLまたはExpectのコマンド）</li> <li>• エラー処理可能</li> <li>• ログインコード必須</li> <li>• NAデバイス変数へのアクセス可能</li> </ul>

スクリプトを使用する場合、同じ名前のスクリプトを複数作成することにより、さまざまなタイプのデバイス上で同じタスクを実行できるため、すべてのスクリプトを1つの名前で、単一タスクとして実行できます。（デバイスはデバイスグループとして構成する必要があります。）スクリプトを実行すると、グループ内のデバイスに適用



されるスクリプトのインスタンスがすべて表示されます。たとえば、すべてのルータに対してNTPサーバを変更するスクリプトを実行できます。これは、ルータのベンダーが異なる場合も同じです。同じ名前のスクリプトを複数実行する場合、スクリプトの各インスタンスを編集できます。

新規コマンドスクリプトを追加するには：

1. [デバイス]のメニューバーにある[デバイスツール]を選択し、[コマンドスクリプト]をクリックします。[コマンドスクリプト]ページが開きます。
2. ページ上部の[コマンドスクリプトの新規作成]リンクをクリックします。[コマンドスクリプトの新規作成]ページが開きます。終了したら、必ず[スクリプトの保存]をクリックしてください。スクリプトが正常に保存されると、[コマンドスクリプト]ページが開きます。追加したスクリプトが強調表示された状態でリストに表示されます。スクリプトは、タスクとしてスケジュールされるまで実行されません。

**注意：**「tc\_」で始まる変数は、特別な用途のために予約されています。この文字の並びで始まる変数をカスタムスクリプトまたは高度なスクリプトで定義することはできません。

## [コマンドスクリプトの新規作成]ページのフィールド

コマンドスクリプトを実行すると、次のことが可能になります。

- 1つまたは複数のデバイス上で一連のカスタムコマンドを実行できます。
- スクリプトをスケジュールされたタスクとして実行したり、イベントルールを使用してスクリプトを実行したりできます。たとえば、特定のデバイスタイプのデバイスが追加されるたびに、そのデバイスタイプに対して標準設定が構成されるようにルールを設定できます。

コマンドスクリプトを作成する場合、\$MyVar\$などの独自のカスタム変数を定義できます。[コマンドスクリプトの実行]タスクページで、カスタム変数はユーザ入力変数として表示されます。

CSV ファイルにカスタム変数を入力するのであれば、既存の scriptField1、scriptField2 などのヘッダーを、スクリプトによるカスタム変数で置換できます。これにより、コマンドスクリプトを実行すると、そのスクリプトのあらゆるカスタム変数（CSV ファイルでも参照される）が、CSV データファイルに入力された[コマンドスクリプトの実行]-[タスクオプション/変数]フィールドに入力されます。

スクリプトで定義され、CSV ファイルで参照されないカスタム変数は、ユーザが入力できるように表示されます。詳細については、「[\[コマンドスクリプトの実行\]タスクページのフィールド](#)」(304 ページ) を参照してください。

フィールド	説明/アクション
コマンドスクリプト	[コマンドスクリプト]ページが開きます。このページには、コマンドスクリプトのリストが表示されます。詳細については、「 <a href="#">[コマンドスクリプト]ページのフィールド</a> 」(573 ページ) を参照してください。
名前	新規スクリプト名を入力します。
説明	スクリプトの説明（テンプレートから作成されたのか、作成者は誰かなど）を入力します。
パーティション	スクリプト、診断のいずれかまたは両方を、特定パーティションに、またはグローバルに適用できます。「[共有]」とラベル付けされたスクリプト、診断のいずれかまたは両方は、すべてのパーティションに適用可能であることから、すべてのユーザが表示できます。ドロップダウンメニューから特定のパーティションを選択できます。  <b>注意：</b> NA 管理者がデバイスをパーティション化した場合、ユーザが表示権限を持つ特定パーティションに属すスクリプト、診断のいずれかまたは両方のみ、ユーザは表示、編集、実行できます。デバイスおよびユーザのセグメント化の詳細については、「 <a href="#">デバイスとユーザのセグメント化</a> 」(148 ページ) を参照してください。
スクリプトタイプ	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• 汎用（デフォルト）</li> <li>• 既存：ドロップダウンメニューからスクリプトを選択します。</li> <li>• 新規作成：新規スクリプトタイプを入力します。</li> </ul>

フィールド	説明/アクション
高度なスクリプティング	<p>オンにすると、ページが更新され、ExpertやPERLなどのコマンドライン言語で記述されたカスタムスクリプトに固有の設定が入力できるようにページが書き換えられます。高度なスクリプティングに固有のフィールドは次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>デバイスファミリ</b>：デバイスファミリとは、似たような構成CLIコマンド構文を共有するデバイスの集合です。デバイスファミリを選択します。これにより、スクリプトの実行対象が、選択したデバイスファミリにドライバが含まれているデバイスに制限されます。この機能を使用すると、さまざまなデバイスに対して作成されたスクリプトの複数の実装に同じ名前を割り当てることができるため、それらのスクリプトを単一タスクとして実行できます。</li> <li>• <b>言語</b>：追加するスクリプトの記述に使用したスクリプト言語を選択します。この機能を使用するには、言語サポートをインストールし、[システム管理設定/サーバ/高度なスクリプティング]で言語を構成する必要があります。オプションには、[Expect]、[Perl]、および[Flow]があります。（<b>注意</b>：ExpectサポートはNAと一緒にインストールされますが、パスを構成する必要があります。）フローの詳細については、「<b>HP Operations Orchestration (HP OO)</b>」(76ページ)を参照してください。</li> <li>• <b>パラメータ</b>：スクリプトの認証パラメータを入力します。NAの変数または独自のカスタム変数を組み込むことができます。（<b>注意</b>：この方針を使用すると、ファイルにパスワードが書き込まれるというセキュリティリスクが減少するため、認証にはパラメータを使用することをお勧めします）。</li> <li>• <b>スクリプト</b>：高度なスクリプティングには、条件付きロジックおよび事前に定義された変数を組み込むことができます。変数名には、アルファベット、数字、アンダースコア（_）のみを使用することができます。書式は、\$report\$や\$my_address\$、\$port_3_ip\$などのように、2つのドル記号（\$）の間に変数名を入れてください。高度なスクリプトには、デバイスへの接続およびログインに必要なコードが含まれている必要があります。たとえば、\$tc_device_ip\$に接続し、\$tc_device_password\$を使用してログインします。</li> <li>• <b>変数</b>：高度なカスタムスクリプトで使用可能なデバイス変数のリストが表示されます。これらの変数は、通常、\$tc_で始まり、名前は大文字と小文字が区別されます。（独自の変数を作成することもできます。）</li> <li>• <b>変数をプル</b>：ページを更新します。これにより、ページ下部にスクリプトで使用される各変数の入力フィールドが追加されます。これらのフィールドを使用して、変数のカスタムプロンプトを定義したり、各プロンプトの許容値を制限したりします。変数ごとに、次のオプションを選択できます。 <ul style="list-style-type: none"> <li>-値に複数行を許可</li> <li>-値を限定：（先頭、最後、最後の1つ前）</li> <li>-パスワード（オンにすると、NAは[コマンドスクリプトを実行]タスクページで値の入力を求める際、パスワードをエコーしません）</li> </ul> </li> </ul>
モード	デバイスアクセスモード（Cisco Exec、Nortel Managerなど）を選択します。
ドライバ	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 適用できる全ドライバ（デフォルト）</li> </ul>
スクリプト	<p>特定のドライバを選択：リストからドライバを1つ以上選択する場合は、ドライバを1つ選択するか、[Shift]+クリックまたは[Ctrl]+クリックを使用して複数のドライバを選択します。（<b>注意</b>：カスタムスクリプトでは、Baystack 470などのメニュー主導型デバイスにアクセスできません）。</p> <p>デバイスに送信するデバイス固有のコマンドを入力するか、既存のスクリプトにデバイス固有のコマンドを貼り付けて編集します。コマンドの入力方法については、[コマンドスクリプト]ページに関するヘルプ情報を参照してください。</p> <p><b>注意</b>：変数名の先頭をtc_にすることはできません（tc_はNA用に予約されています）。ただし、変数には、大文字のアルファベット、小文字のアルファベット、0～9、およびアンダースコア文字のあらゆる組み合わせを使用できます。</p>

フィールド	説明/アクション
[変数をプル]ボタン	<p data-bbox="444 243 1463 325">ページが更新されます。これにより、ページ下部にスクリプトで使用される各変数の入力フィールドが追加されます。これらのフィールドを使用して、変数のカスタムプロンプトを定義したり、各プロンプトの許容値を制限したりします。フィールド例は次のとおりです。</p> <ul data-bbox="444 344 583 411" style="list-style-type: none"><li>• HOSTNAME</li><li>• ETH_SLOT1</li></ul> <p data-bbox="444 451 1463 558">このスクリプトを実行したときにユーザが対応するカスタムプロンプト、およびこのプロンプトが受け入れる対応値を入力します。値はカンマで区切る必要があります。このため、カンマが含まれる値は使用できません。複数の値を指定すると、ユーザにプロンプトが表示されたときに、許容値のリストがプロンプトダイアログに提供されます。</p>

## 自動修正スクリプトの作成

自動修正スクリプトを使用することで、違反されたポリシールール内の正規表現パターングループからのデータを参照する、スクリプト内の変数を定義します。自動修正変数は、非正規表現パターンにも使用できます。

自動修正スクリプトは、標準コマンドスクリプトとは異なります。複雑なポリシー定義の可能性がある場合、自動修正スクリプトはデバイス上で実行する実際のコマンドスクリプトを生成するためのプリプロセスステップが必要となり、for ループおよび if-文などの基本的な言語構造を持つ必要があります。

自動修正スクリプトは、一致した行に対する繰り返し処理を可能にするシンタックスを含みます。自動修正スクリプトは、正規表現変数の代入によりコマンドスクリプトに変換されます。テンプレートプロセッサ（コマンドスクリプトジェネレータ）は、実行可能コマンドスクリプトを分析して生成します。これを自動修正タスクが実行します。

新しい自動修正スクリプトの追加方法については、「[\[ルールの新規作成\] ページのフィールド](#)」（420 ページ）を参照してください。

## 自動修正スクリプトのシンタックス

NAには、違反データにアクセスできる新しい自動修正スクリプトのシンタックスが含まれます。以下の表で自動修正スクリプトで使用されるスクリプト言語要素を説明します。

言語要素	説明
@foreach	一致した行に対する繰り返し処理を行うためのループ構文です。
@ifexists	変数に一致があるかどうかをテストするための制御構文です。
@end	@foreach、または@ifexistsの終了を示します。
\$loop_variable\$	条件の正規表現パターン行に一致した行に対する繰り返し処理をするのに使用する任意の変数名です。
\$line_match_variable\$	条件の正規表現パターン行に一致する、構成行の配列を表します。たとえば、\$condition_A_line_1\$は条件Aの最初の行に一致する構成行を指します。
\$regex_group_match_variable\$	正規表現グループに一致するテキストを表します。
@	デバイスコマンドと区別するための自動修正言語要素の接頭辞です。
//	自動修正スクリプトの行をコメントアウトするための接頭辞です。

## 自動修正スクリプト変数の命名規則

次の表で、自動修正スクリプトの命名規則を説明します。

変数	命名規則	例
ループ	<code>\$any_string\$</code>	<code>\$interface\$</code> : 正規表現パターンに一致する各構成行です。
パターン行一致 (正規表現パターンの 行の一致を表す)	<code>\$condition_&lt;label&gt;_line_&lt;number&gt;\$</code>	<code>\$condition_A_line_2</code> : 条件Aの2行目に一致する構成行です。
正規表現グループ一致	<code>\$&lt;loop_variable&gt;.regex_group_&lt;number&gt;\$</code>	<code>\$interface.regex_group_1\$</code> : 正規表現パターンに一致した構成行に存在する、最初の正規表現グループの一致です。  • <code>number = 0</code> : 全体一致  • <code>number &gt; 0</code> : 正規表現キャプチャグループ
ブロック開始パターン	<code>\$block_start\$</code>	ブロック開始パターン用ビルトイン変数の名前です。
ブロック終了パターン	<code>\$block_end\$</code>	ブロック終了パターン用ビルトイン変数の名前です。

注意 :

- `$line_match_variable$` の `@foreach $loop_variable$`。ここで `$loop_variable$` は、条件の正規表現パターンの1行に対する一致の配列である `$line_match_variable$` の各一致行を表すのに使用されます。たとえば、`$condition_A_line_1$` は、条件Aの最初の行に一致するすべての構成行を表わす一致変数です。
- `@ifexists $regex_group_match_variable$`。ここで、`$regex_group_match_variable$` は、正規表現グループの一致を表すのに使用されます。
- 入れ子の `@foreach` ループが使用できます。
- ブロック開始パターン、およびブロック終了パターンは、`$block_start$`、および `$block_end$` 配列変数でアクセスします。(586ページの例3を参照してください。)
- 正規表現グループは、括弧で囲まれた正規表現パターンの一部です。たとえば、パターン「`interface (.*)`」、「`(.*)`」は正規表現グループ（キャプチャグループとも呼びます）です。
- 違反データは「含まない」、および「次のみを含む必要がある」演算子で利用できます。「含む」演算子に対する違反データは存在しません。「含む」演算子を使用して一致が存在しない場合に違反が発生するためです。変数の参照なしに自動修正スクリプトを作成できます。この場合、自動修正スクリプトのシンタックス要素は使用されません。
- 自動修正変数は、非正規表現パターンに使用できます。この場合、正規表現グループ変数は存在しません。全体一致には、グループ0変数を使用してアクセスできます（たとえば、`$matching_line.regex_group_0$` などです。ここで、`$matching_line$` は `@foreach` ループ変数です）。

- 自動修正タスクはコマンドスクリプトの実行タスクとして実行されます。ただし、デバイス上で実際に実行されるのは、コマンドスクリプトの実行タスクがスケジュールされる前に自動修正スクリプトのプリプロセッシングにより生成されたコマンドスクリプトです。コマンドスクリプトの実行の詳細については、「[\[コマンドスクリプトの実行\]タスクページのフィールド](#)」(304 ページ) を参照してください。
- 自動修正スクリプトは、[\[構成管理\]](#)ページの[\[構成ポリシーの検証\]](#)セクションで有効にする必要があります。詳細については、「[構成管理](#)」(35 ページ) を参照してください。

## 自動修正スクリプトの例

### 例1：違反データなし（最も簡単な場合）

最も簡単な自動修正スクリプトは、結果により違反データが生成されない、「含む」演算子と一緒に使用されます。このため、スクリプトは自動修正スクリプトのシンタックスを必要としません。

以下の条件を仮定します（パターンが正規表現ではない点に注意してください）。

条件 A：構成テキスト

含む

```
ntp server 169.243.103.34
ntp server 170.242.62.16
ntp server 170.242.62.17
ntp server 169.243.226.94
```

構成テキストにパターンの行が含まれない場合、条件Aに違反します。違反を修正するため、以下の自動修正スクリプトが構成に行を挿入します。

スクリプト：

```
ntp server 169.243.103.34
ntp server 170.242.62.16
ntp server 170.242.62.17
ntp server 169.243.226.94
```

上述の但し書きのとおり、スクリプトに自動修正スクリプトのシンタックスを使用する必要はありません。

### 例2：違反データ

次の例では、違反データ参照がある場合の自動修正の使用方法を説明します。これは例であり、実際の場合で使用することを目的としていません。

以下に与えられた条件（2つの正規表現パターン行を含む）に対し、構成の次の行を確認する場合があります。

## 構成テキスト :

```
...
access-list 139 deny    ip host 192.168.139.1 any
access-list 139 deny    ip host 192.168.139.2 any
access-list 139 permit ip any any
...
```

条件 A : 構成テキスト  
含まない

```
access-list (.* ) deny    ip host (.* ) any
access-list (.* ) permit (192\.0\.0\..*)
```

上記構成テキストの次の行が条件を違反します。

```
access-list 139 deny ip host 192.168.139.1 any
access-list 139 deny ip host 192.168.139.2 any
```

2つの行は、条件Aの最初のパターン行に一致するため、`$condition_A_line_1$` 配列変数内に格納されます。一致した行の太字テキスト部分は正規表現グループに一致し、正規表現グループ一致変数で参照できます。

自動修正変数には、`@foreach`ループからのみアクセスできます。各パターン行が複数の構成行と一致する可能性があることから、一致行はループ内で繰り返されます。条件Aの最初のパターン行に一致する上記の2行にアクセスするには、`@foreach`ループシンタックスを使用します。

```
@foreach $matching_line$ in $condition_A_line_1$
...
@end
```

上記行の意味 : `$matching_line$` ループ変数を使用して、`$condition_A_line_1$` の配列変数 (パターン行一致変数) に格納される、各一致構成行にアクセスします。

`$matching_line$` ループ変数を使用することで、自動修正スクリプトはループの各繰り返しで1つの一致行にアクセスできます。一致した行と正規表現グループに対応する部分には、下記の要領でループ変数を經由してアクセスします (上記`@foreach`ループ内)。

```
$matching_line.regex_group_0$
$matching_line.regex_group_1$
$matching_line.regex_group_2$
```



グループ0の変数（`$matching_line.regex_group_0$`）は、一致構成行全体を保持します。他のグループ1およびグループ2は、括弧内で定義された正規表現グループを保持します。このため、ループの最初の繰り返しにある変数の値は以下のようになります。

```
$matching_line.regex_group_0$: access-list 139 deny ip host 192.168.139.1 any
$matching_line.regex_group_1$: 139
$matching_line.regex_group_2$: 192.168.139.1
```

例として、次の自動修正スクリプトが違反を修正する場合を考えます。

```
@foreach $matching_line$ in $condition_A_line_1$
  no $matching_line.regex_group_0$
  access-list 100 permit $matching_line.regex_group_2$ any
@end
```

@foreachループ内の各行は、デバイス上で実行されるコマンドです。この例では、最初の行（`no <line>`）はデバイスの構成テキストから行を削除し、2番目の行はデバイスの構成テキストに行を挿入します。

サンプルの自動修正スクリプトでは、2つの変数参照`$matching_line.regex_group_0$`と`$matching_line.regex_group_2$`が使用されています。この自動修正スクリプトが、準拠確認後にポリシーマネージャによって実行されると、次のコマンドスクリプトが生成され、デバイス上で実行されるようにスケジュールされます。

```
no access-list 139 deny ip host 192.168.139.1 any
access-list 100 permit 192.168.139.1
no access-list 139 deny ip host 192.168.139.2 any
access-list 100 permit 192.168.139.2
```

**例3：ブロック**

ブロックベースの条件には、条件パターンのブロックと一致を繰り返す入れ子のループが必要です。次のポリシールール定義に、ブロック開始/終了パターンと1つのブロックテキスト条件が含まれている場合を考えます。

構成テキスト：

```
...
interface Ethernet0/0
  description New York LAN Back Bone
  ip address 10.16.241.1 255.255.255.224
  no ip mroute-cache
  half-duplex
!
interface Ethernet0/1
  description Chicago LAN Back Bone
  ip address 10.1.1.1 255.255.255.252
  half-duplex
!
...
```

Block Start: interface (.\*)

Block End: !

条件 A：構成ブロック

含まない

```
ip address (10\..*)\s(.*)
```

上記条件の違反データにアクセスするのに使用される@foreachループは、次のようになります。

```
@foreach $matching_line$ in $condition_A_line_1$
  no $matching_line.regex_group_0$
@end
```

ただし、条件Aの一致はブロックにより整理されます。上記@foreachループは、\$condition\_A\_line\_1\$配列がどのブロックと一致したのかを把握していません。このため、以下の要領でブロック用に条件パターンを@foreachループで囲む必要があります。

```
@foreach $matching_block$ in $block_start$
  @foreach $matching_line$ in $condition_A_line_1$
    interface $matching_block.regex_group_1$
    no $matching_line.regex_group_0$
  @end
@end
```

生成されるコマンドスクリプトは以下のようになります。

```
interface Ethernet0/0
no ip address 10.16.241.1 255.255.255.224
interface Ethernet0/1
no ip address 10.1.1.1 255.255.255.252
```

#### 例4:「次のみを含む必要がある」演算子

「次のみを含む必要がある」演算子には2つのパターンがあります。

- 最初のパターンは、含まれる必要のある構成テキストを定義します。
- 2番目のパターンは、最初のパターンの一致以外に含まれてはいけな構成テキストを定義します。

違反データは2番目のパターンに対して生成されます。例：

```
条件 A : 構成テキスト
次のみを含む必要がある :
これらの行を必ず含む :
ntp server 169\.243\.103\.34
ntp server 170\.242\.62\.16
ntp server 170\.242\.62\.17
ntp server 169\.243\.226\.94
ただし次の項目を含む追加行は含めない :
ntp server(.*)
```

次の2つの違反が考えられます。

1. 「これらの行を必ず含む」パターンの任意の行が、構成テキストに一致しません。違反は目的の行が存在しないことによって生じることから、違反データは生成されません。
2. 「ntp server(.\*)」パターンに一致する任意の構成テキスト行は、「これらの行を必ず含む」パターンの任意の行に一致しません。この場合、違反データが存在します。この違反データには、`$condition_A_line_1$` array変数を経由してアクセスできます。

考えられる違反を修正する自動修正スクリプトは、次のようになります。

```
ntp server 169.243.103.34
ntp server 170.242.62.16
ntp server 170.242.62.17
ntp server 169.243.226.94

@foreach $matching_line$ in $condition_A_line_1$
no ntp server $matching_line.regex_group_1$
@end
```

最初の4行は、構成テキストに「これらの行を必ず含む」パターンで定義された行が存在することを保証します。`@foreach`ループは、違反の原因となる`ntp server(.*)`に一致する任意の行を削除します。

**例5 : @ifexists 文**

正規表現には、一致テキストが存在しない可能性があるグループを含められます。このため、このようなグループを参照する変数には格納された値が存在しない可能性があります。例：

```
logging ((10\.1\..*)|(172\.1\..*))
```

正規表現グループ：

グループ 0 : logging ((10\.1\..\*)|(172\.1\..\*))

グループ 1 : ((10\.1\..\*)|(172\.1\..\*))

グループ 2 : (10\.1\..\*)

グループ 3 : (172\.1\..\*)

グループ2や3のIPアドレスの正規表現キャプチャグループの1つは、値を持ちません。

上記正規表現パターンを持つ、次の条件がある場合を考えます。

条件 A : 構成テキスト

含まない

```
logging ((10\.1\..*)|(172\.1\..*))
```

上記の違反データにアクセスするための自動修正スクリプトは、@ifexistsステートメントを使用して、グループ2と3のキャプチャグループ変数に使用可能な違反データがあるかどうかをテストする必要があります。それ以外の場合、自動修正スクリプトが値を持たないキャプチャグループ変数にアクセスしても、コマンドスクリプトは生成されません。

自動修正スクリプトは次のような内容になります。

```
@foreach $matching_line$ in $condition_A_line_1$
  @ifexists $matching_line.regex_group_2$
    no logging $matching_line.regex_group_2$
  @end
  @ifexists $matching_line.regex_group_3$
    no logging $matching_line.regex_group_3$
  @end
@end
```

## 例6：複数条件

次の例では、複数条件を説明します。

```
Block Start: interface (.*)  
Block End:    !
```

条件 A：構成ブロック

含まない

```
ip address (10\..*)\s(.*)
```

条件 B：構成テキスト

次のみを含む必要がある：

これらの行を必ず含む：

```
ntp server 169\.243\.103\.34  
ntp server 170\.242\.62\.16  
ntp server 170\.242\.62\.17  
ntp server 169\.243\.226\.94
```

ただし次の項目を含む追加行は含めない：

```
ntp server(.*)
```

ブール式：A AND B

自動修正スクリプトは次のような内容になります。

```
@foreach $matching_block$ in $block_start$  
  @foreach $matching_line$ in $condition_A_line_1$  
    interface $matching_block.regex_group_1$  
    no $matching_line.regex_group_0$  
  @end  
@end  
  
ntp server 169.243.103.34  
ntp server 170.242.62.16  
ntp server 170.242.62.17  
ntp server 169.243.226.94  
  
@foreach $matching_line$ in $condition_B_line_1$  
  no ntp server $matching_line.regex_group_1$  
@end
```

## コマンドスクリプトの実行

コマンドスクリプトのインスタンスを実行および編集できるかどうかは、権限によって制限されています。制限付き権限が設定されたユーザ、およびデバイスの修正権限を持たないフルユーザまたはパワーユーザは、スクリプトを実行できません。

スクリプトを設定して、一度だけ実行したり、ユーザ定義の間隔で周期的に実行したり、反復タスクとして実行したりすることができます。さらに、タスクが特定の時間に、またはできるだけ早く開始されるようにスケジュールすることもできます。スクリプトは編集可能であり、実行する前に変数に値を指定する必要があります。

[コマンドスクリプト]ページからスクリプトを実行するには：

1. [デバイス]メニューで、[デバイスツール]を選択し、[コマンドスクリプト]をクリックします。[コマンドスクリプト]ページが開きます。
2. 実行するスクリプト名を選択します。
3. [アクション]列で、[実行]をクリックします。[コマンドスクリプトの実行タスク]ページが開きます。詳細については、「[\[コマンドスクリプトの実行\]タスクページのフィールド](#)」(304 ページ)を参照してください。

**注意：** [タスク]メニューからコマンドスクリプトを実行することもできます。

## 構成テンプレートからのスクリプトの作成

構成テンプレートからスクリプトを作成するには：

1. [デバイス]のメニューバーにある[デバイスツール]を選択し、[構成テンプレート]をクリックします。[構成テンプレート]ページが開きます。「[\[構成テンプレート\]ページのフィールド](#)」(563 ページ)を参照してください。
2. ベンダーのリンクをクリックします。対象ベンダーの[構成テンプレート]ページが開きます。
3. スクリプトに含める構成テンプレートを選択し、[スクリプトを更新]をクリックします。
4. 必要に応じてスクリプトを編集し、[スクリプトを作成]ボタンをクリックして、デバイスに配布可能なスクリプトを作成します。[Save Script from Template]ページが開きます。
5. [名前]フィールド、[説明]フィールド、および他のフィールドを編集します。変数名の先頭を「tc\_」にすることはできません。ただし、変数名には、大文字のアルファベット、小文字のアルファベット、0～9、およびアンダースコア文字のあらゆる組み合わせを使用できます。
6. [スクリプトを保存]をクリックします。[コマンドスクリプト]ページが開きます。新規スクリプトは強調表示されています。

# 第16章：レポート

## トピックの参照先リスト

レポート	参照先：
はじめに	<a href="#">「はじめに」</a> （592ページ）
ユーザレポートとシステムレポート	<a href="#">「ユーザレポートとシステムレポート」</a> （593ページ）
ネットワークステータスレポート	<a href="#">「ネットワークステータスレポート」</a> （596ページ）
ベストプラクティスレポート	<a href="#">「ベストプラクティスレポート」</a> （599ページ）
デバイスステータスレポート	<a href="#">「デバイスステータスレポート」</a> （601ページ）
統計ダッシュボード	<a href="#">「統計ダッシュボード」</a> （602ページ）
ダイアグラム	<a href="#">「ダイアグラム」</a> （603ページ）
デバイスソフトウェアレポート	<a href="#">「デバイスソフトウェアレポート」</a> （612ページ）
ソフトウェアレベルレポート	<a href="#">「ソフトウェアレベルレポートのフィールド」</a> （614ページ）
ソフトウェアの脆弱性レポート	<a href="#">「ソフトウェアの脆弱性レポート」</a> （616ページ）
イメージ同期レポート	<a href="#">「イメージ同期レポートのフィールド」</a> （618ページ）
システム/ネットワークイベントレポート	<a href="#">「システム/ネットワークイベントレポート」</a> （619ページ）
ソフトウェアの脆弱性イベントの詳細レポート	<a href="#">「ソフトウェアの脆弱性イベントの詳細レポート」</a> （620ページ）
サマリレポート	<a href="#">「サマリレポート」</a> （621ページ）
電子メールレポート	<a href="#">「電子メールレポート」</a> （624ページ）

## はじめに

HP Network Automation (NA) には、入力が必要なデフォルトのレポートと特別レポートがあります。デフォルトのレポートは次のとおりです。

- ユーザレポートとシステムレポート
- ダッシュボードレポート
- サマリレポート
- ベストプラクティスレポート
- ネットワークステータスレポート
- 構成レポート
- デバイスステータスレポート
- ソフトウェアの脆弱性レポート
- タスク/ジョブレポート
- Telnet/SSHユーザセッションログレポート
- コンプライアンスセンターレポート

特別レポートでは、NA 内のデータを調整して柔軟に報告できます。特別レポートは、1 つまたは複数のフィールドの正規表現基準に基づいて、手動または自動で生成できます。一般的な特別レポートには、次の項目が含まれます。

- 12.\*バージョンのIOSが実行されているすべてのCisco デバイス
- 構成管理で安全でないプロトコルを使用するすべてのデバイス
- 障害のあるモジュールが組み込まれているすべてのデバイス
- 一定期間に渡って一連のデバイスに対して行われたすべての構成変更
- 特定のユーザによって開始されたすべてのTelnet/SSHセッションログ
- 承認の無効化によるすべてのデバイスの変更
- 特定ポートのトラフィックを拒否するすべてのACL



## ユーザレポートとシステムレポート

ユーザレポートとシステムレポートは、検索機能を使用して定義および保存した検索結果です。ユーザが定義した検索のみがユーザレポートのリストに表示されます。次の項目を基準にして検索できます。

- デバイス
- インターフェイス
- モジュール
- 構成
- 診断
- ポリシー
- 準拠
- タスク
- セッション
- イベント
- ユーザ
- ACL
- IPアドレス
- MACアドレス
- VLAN

検索の実行方法の詳細については、「[デバイスの検索](#)」(472ページ)を参照してください。

各レポートには、検索で使った基準のサマリが表示されます。ユーザが保存した検索は、ユーザとNA管理者だけが使用できます。

**注意：** 検索を実行して保存しなかった場合には、ユーザレポートを生成できません。

システムは事前に定義されたクエリについて報告します。システムレポートは、そのレポートを選択したときに生成されます。各レポートには、検索で使った基準のサマリが表示されます。システムレポートには、次の項目が含まれます。

### 構成

- 過去12時間に行ったすべての変更
- 過去24時間に行ったすべての変更
- 過去48時間に行ったすべての変更
- 先週行ったすべての変更
- 先月行ったすべての変更
- 過去48時間に自分で行ったすべての変更

### ポリシーイベント

過去24時間のポリシールール違反

## デバイス

- 過去24時間に変更されたすべてのデバイス
- 先週変更されたすべてのデバイス
- アクセスに失敗したすべてのデバイス
- すべての非アクティブなデバイス（注意：非アクティブなデバイスを削除せずに、それらのデバイスを非アクティブに指定して構成履歴を保持できます）
- IPアドレスが重複しているすべてのアドレス
- ドライバが割り当てられていないすべてのデバイス
- ドライバは割り当てられているが構成が保存されていないすべてのデバイス
- スタートアップ構成とランニング構成が異なるすべてのデバイス

## 重複IP

IPアドレスが重複しているすべてのアドレス：このレポートは、同一IPアドレスで構成されているインターフェイスを持つデバイスを表示します。ただし、重複検出の原因となるIPアドレスは削除しません。

IPタイプは、IPアドレスの追加方法、または使用方法のいずれかです。この列の値が取り得る値を以下に挙げます。

- 1：手動（IPアドレスは手動で追加）
- 2：NAT（ネットワークアドレス変換。IPアドレスはユーザ定義のNATで変換）
- 3：ポートのプライマリ（ポートのプライマリIPアドレス）
- 4：ポートのセカンダリ（ポートのセカンダリIPアドレス）
- 5：デバイスへのTFTP用（TFTP経由でデバイスにアクセスするためのIPアドレス）
- 6：デバイスのプライマリ（デバイスにアクセスするのに使用するプライマリIPアドレス）
- 7：コンソール（デバイスへのコンソールアクセス用IPアドレス）

## セッション

- 過去24時間に作成したすべてのセッション
- 過去48時間に作成したすべてのセッション
- 先週作成されたすべてのセッション
- 過去48時間に自分で作成したすべてのセッション

## ソフトウェアレベル

- デバイスソフトウェア準拠

## タスク

- 過去24時間に失敗しスキップされたすべての重複タスク
- 先週失敗しスキップされたすべての重複タスク

## その他

- ベストプラクティスレポート
- ネットワークステータスレポート
- デバイスステータスレポート
- COBIT 準拠ステータス
- COBIT 準拠のステータス
- GLBA 準拠ステータス

ユーザレポートとシステムレポートを表示するには、[レポート]の下メニューバーで[ユーザレポートとシステムレポート]をクリックします。[ユーザレポートとシステムレポート]ページが開きます。

## ユーザレポートとシステムレポートのフィールド

フィールド	説明/アクション
タイプ	イベントまたはレポートのタイプを表示します。
レポート	たとえば、デバイスステータス、HIPAA 準拠ステータス、すべての非アクティブなデバイスなど、レポート名を表示します。レポート名をクリックするとレポートが開きます。
アクション	<p>次のアクションを選択できます。</p> <ul style="list-style-type: none"> <li>• 電子メールレポート：電子メールレポートを表示します。この画面では、レポートの出力を電子メール経由で送信するタスクを作成できます。受信者を指定することができ、ユーザのログインがデフォルトの設定です。電子メールメッセージを生成するには、タスクを保存する必要があります。</li> <li>• 変更：ユーザレポートの場合は、イベントの[変更]オプションをクリックできます。[イベントを検索]ページが開きます。</li> <li>• システムレポートとしてマーク：ユーザレポートで、[システムレポートとしてマーク]をクリックできます。そのレポートは、[システムレポート]セクションに移動します。</li> <li>• 削除（赤のXアイコン）：レポートを完全に削除します。</li> <li>• 上下矢印をクリックして、リスト内のレポートの位置を上下に動かします。</li> </ul>

## ネットワークステータスレポート

ネットワークステータスレポートには、ネットワーク構成、動作状態、およびコンプライアンスの概要とともに、独立した次の2つのネットワークのビューが表示されます。

- ベストプラクティス
- デバイスステータス

ネットワークステータスレポートでは、先行型のレポート機能を使用できます。ネットワーク管理者とエンジニアは、レポートを反復電子メールレポートタスクとして実行するようにスケジュールすることで最新情報を自動的に受信し、その情報に基づいてネットワークに影響が出る前に問題を解消できます。また、ネットワークステータスレポートにより管理担当者は、ポリシーとソフトウェア準拠問題を解決したり、構成変更を処理したりする場合のネットワーク操作の効果性について、概要を知ることができます。

**注意：** このレポートのデフォルトの構成は、インベントリデバイスグループに対して実行されます。

イベントは、ネットワークに存在するリスクに関して3段階の表示で報告されます。システム管理者は、カテゴリごとにしきい値を設定し、ネットワークへの影響度を反映するリスクレベルのインジケータ色を割り当てます。

- 赤：高リスク。黄レベルのイベントの他にポリシー違反、ソフトウェアレベル違反、およびデバイスアクセスエラーを含みます。
- 黄：中リスク。スタートアップとランニング構成の不一致、およびデバイスアクセスエラーを含みます。
- 緑：しきい値内であるか、低リスクです。これがベストプラクティスです。

デバイスグループのステータスは、そのグループの中でリスクレベルが最も高いデバイスに基づいて判断されます。ネットワークのステータスは、そのネットワークの中でリスクレベルが最も高いグループに基づいて判断されます。

ネットワークステータスレポートを表示するには、[レポート]の下メニューバーで[ネットワークステータス]をクリックします。必要が生じたときにレポートページの[再実行]ボタンを使用してこのレポートを実行するか、またはレポートをスケジュールしてタスクとして実行されるようにし、[電子メールレポート]オプションを使用して主要なネットワークおよび管理のスタッフにレポートを電子メールで送信することができます。電子メールレポートの詳細については、「[電子メールレポート](#)」(624ページ)を参照してください。

## ネットワークステータスレポートのフィールド

フィールド	説明/アクション
ベストプラクティスレポート	ベストプラクティスレポートを開きます。 <a href="#">「ベストプラクティスレポート」(599ページ)</a> を参照してください。
デバイスステータスレポート	デバイスステータスレポートを開きます。 <a href="#">「デバイスステータスレポート」(601ページ)</a> を参照してください。
レポート日	レポートを最後に実行した日付と時刻が表示されます。
デバイスグループのレポート	レポートされたデバイスグループの数が表示されます。

フィールド	説明/アクション
デバイスグループを変更	現在定義されているデバイスグループのリストを表示します。単独または複数のデバイスグループについてネットワークステータスレポートを実行できます。他のすべてのパラメータは事前定義されています。サマリと詳細な情報は、指定するデバイスグループそれぞれのカテゴリごとに表示されます。終了したら[再実行]ボタンをクリックします。
デバイスグループ	デバイスグループの名前とグループ内のデバイス数を表示します。
デバイスステータス	
デバイスステータス	<p>検出された問題の割合と一緒にステータスレベルインジケータを表示します。ステータスには次のレベルがあります。</p> <ul style="list-style-type: none"> <li>• 赤：高リスク</li> <li>• 黄：中リスク</li> <li>• 緑：低リスク</li> </ul> <p>[デバイスステータス]をクリックすると、デバイスステータスレポートが開きます。「<a href="#">デバイスステータスレポート</a>」(601ページ)を参照してください。</p>
ベストプラクティスのステータス	
問題	<p>NAが追跡する次の5つの主なネットワーク問題を表示します。</p> <ul style="list-style-type: none"> <li>• 24時間以内のポリシー違反：1つ以上の定義済み構成ポリシーに準拠しないデバイス。詳細を表示するには、情報アイコンの上にカーソルを移動します。</li> <li>• ソフトウェア準拠違反：未承認のソフトウェアバージョンを実行しているデバイス。詳細を表示するには、情報アイコンの上にカーソルを移動します。</li> <li>• スタートアップとランニング構成の不一致：スタートアップ構成とランニング構成が一致していないデバイス。詳細を表示するには、情報アイコンの上にカーソルを移動します。</li> <li>• デバイスアクセスエラー：NA がアクセスできないデバイス。詳細を表示するには、情報アイコンの上にカーソルを移動します。</li> <li>• 24時間以内の構成変更：過去24時間以内に検出されたデバイスの構成変更。詳細を表示するには、情報アイコンの上にカーソルを移動します。</li> </ul> <p>表示されるアクションリンクは、問題ごとに異なります。たとえば、報告されたすべてのデバイスアクセスエラーの場合には、リンクをクリックしてデバイス詳細の[タスクを表示]オプションを表示することにより、失敗したタスクを識別できます。スタートアップとランニング構成の不一致の場合には、リンクをクリックして[スタートアップと実行を比較]オプションを表示できます。このオプションには、差異が強調表示されて両方の設定が表示されます。</p> <p>[ベストプラクティスのステータス]をクリックすると、ベストプラクティスレポートが開きます。「<a href="#">ベストプラクティスレポート</a>」(599ページ)を参照してください。</p>

フィールド	説明/アクション
ネットワークステータスレポート 詳細	
高リスク（赤）の問題	<p>赤のステータスを返した5つの問題のいずれかのサマリを表示します。表示されるアクションリンクは、問題ごとに異なります。例：</p> <ul style="list-style-type: none"><li>• 報告されたすべてのデバイスアクセスエラー：リンクをクリックしてデバイス詳細の[タスクを表示]オプションを表示することにより、失敗したタスクを識別できます。</li><li>• ポリシールール違反：リンクをクリックして[ポリシーアクティビティ]ページを表示します。このページでは、デバイスの構成が1つ以上の構成ポリシーに含まれる構成ルールに準拠していなかったかどうかを示すイベントを表示できます。[ポリシー重要度]列に表示される値は、現行でデバイスが違反しているすべての構成ルールの中で最高の重要度を示します。</li><li>• スタートアップとランニング構成の不一致：リンクをクリックして、両方の設定を示す[スタートアップとランニング構成を比較]オプションを表示します。すべての差異が強調表示されます。</li></ul>

## ベストプラクティスレポート

ネットワーク管理のベストプラクティスでは、次の項目のいずれかに対する非準拠が慎重に監視されるよう徹底します。

- 24時間以内のポリシールール違反
- ソフトウェア準拠違反
- スタートアップとランニング構成の不一致
- デバイスアクセスエラー
- 24時間以内の構成変更

NAにより、これらの項目それぞれに対する非準拠の許容レベルを定義できます。しきい値を超えると、非準拠のレベルに応じて黄または赤の警告フラグが表示されます。NAは、準拠していないデバイスも表示するため、修正アクションを行うことができます。

5つのインジケータすべてが緑の場合は、NAがネットワークを評価し、ネットワークの稼動状態を良好と判断したことを示します。いくつかのインジケータが黄で表示された場合は、該当する領域を修正アクションの対象とします。いくつかのインジケータが赤で表示された場合は、フラグが表示された項目がネットワークの安定性を脅かす重大なリスクとなる可能性があるため、迅速に対処する必要があります。

ベストプラクティスレポートを表示するには、[レポート]の下メニューバーで[ベストプラクティス]をクリックします。ベストプラクティスレポートが開きます。

**注意：** ベストプラクティスレポートには、ネットワークステータスレポートから移動することもできます。

## ベストプラクティスレポートのフィールド

フィールド	説明/アクション
ネットワークステータスレポート	ネットワークステータスレポートを開きます。「 <a href="#">ネットワークステータスレポート</a> 」(596 ページ) を参照してください。
デバイスステータスレポート	デバイスステータスレポートを開きます。 <a href="#">「デバイスステータスレポート」</a> (601 ページ) を参照してください。
レポート日	レポートを最後に実行した日付と時刻が表示されます。
デバイスグループのレポート	レポートされたデバイスグループの数が表示されます。
デバイスグループを変更	現在定義されているグループのリストが表示されます。単一グループまたは複数のグループのベストプラクティスレポートを実行できます。他のすべてのパラメータは事前定義されています。指定した各グループについて、カテゴリ別にサマリおよび詳細情報が提供されます。終了したら、[再実行] ボタンをクリックします。
ステータス	<p>グループの名前とグループ内のデバイスの数が表示されます。ステータスには次のレベルがあります。</p> <ul style="list-style-type: none"> <li>• 赤：高リスク</li> <li>• 黄：中リスク</li> <li>• 緑：しきい値範囲内</li> </ul>
問題	<p>NA が追跡する次の 5 つの主なネットワーク問題を表示します。</p> <ul style="list-style-type: none"> <li>• 24 時間以内のポリシー違反：1 つ以上の定義済み構成ポリシーに準拠しないデバイス。詳細を表示するには、情報アイコンの上にカーソルを移動します。</li> <li>• ソフトウェア準拠違反：未承認のソフトウェアバージョンを実行しているデバイス。詳細を表示するには、情報アイコンの上にカーソルを移動します。</li> <li>• スタートアップとランニング構成の不一致：スタートアップ構成とランニング構成が一致していないデバイス。詳細を表示するには、情報アイコンの上にカーソルを移動します。</li> <li>• デバイスアクセスエラー：NA がアクセスできないデバイス。詳細を表示するには、情報アイコンの上にカーソルを移動します。</li> <li>• 24 時間以内の構成変更：過去 24 時間以内に検出されたデバイスの構成変更。詳細を表示するには、情報アイコンの上にカーソルを移動します。</li> </ul>
<b>ベストプラクティスレポート 詳細</b>	
高リスク（赤）の問題	<p>赤のステータスを返した 5 つの問題のいずれかのサマリを表示します。表示されるアクションリンクは、問題ごとに異なります。たとえば、報告されたすべてのデバイスアクセスエラーの場合には、リンクをクリックしてデバイス詳細の [タスクを表示] オプションを表示することにより、失敗したタスクを識別できます。スタートアップとランニング構成の不一致の場合は、リンクをクリックして両方の設定がしめされた [スタートアップとランニング構成を比較] オプションを表示できます。すべての差異が強調表示されます。</p>



## デバイスステータスレポート

デバイスステータスレポートでは、ネットワーク内のデバイスすべてがリスト表示され、ベストプラクティスの項目ごとにデバイスが個別に分析されます。ベストプラクティスの各問題の詳細については、「[ネットワークステータスレポートのフィールド](#)」(596ページ)を参照してください。

項目の1つ以上に準拠していない各デバイスには、黄または赤の警告フラグが表示されます。レポートにはネットワーク全体のサマリも表示され、黄または赤の警告フラグを生成したデバイスの数が示されます。

デバイスステータスレポートを表示するには、[レポート]の下メニューバーで[デバイスステータス]をクリックします。デバイスステータスレポートが開きます。

**注意：** デバイスステータスレポートには、ネットワークステータスレポートまたはベストプラクティスレポートからナビゲートすることもできます。

## デバイスステータスレポートのフィールド

フィールド	説明/アクション
ネットワークステータスレポート	ネットワークステータスレポートを開きます。「 <a href="#">ネットワークステータスレポート</a> 」(596ページ)を参照してください。
ベストプラクティスレポート	ベストプラクティスレポートを開きます。「 <a href="#">ベストプラクティスレポート</a> 」(599ページ)を参照してください。
レポート日	レポートを最後に実行した日付と時刻が表示されます。
デバイスグループのレポート	レポートされたデバイスグループの数が表示されます。
デバイスグループを変更	現在定義されているグループのリストが表示されます。単一グループまたは複数のグループのベストプラクティスレポートを実行できます。他のすべてのパラメータは事前定義されています。指定した各グループについて、カテゴリ別にサマリおよび詳細情報が提供されます。終了したら、[再実行]ボタンをクリックします。
ステータス	グループの名前とグループ内のデバイスの数が表示されます。ステータスには次のレベルがあります。 <ul style="list-style-type: none"> <li>赤：高リスク</li> <li>黄：中リスク</li> <li>緑：しきい値範囲内</li> </ul>
<b>デバイスステータスレポートの詳細</b>	
中リスク（黄）と高リスク（赤）の項目	黄または赤のステータスを返した5つの問題のいずれかのサマリを表示します。利用可能なアクションリンクは問題ごとに変わります。たとえば、報告されたすべての24時間以内の構成変更の場合は、[設定の表示]リンクをクリックしてそのデバイスの構成情報を表示できます。デバイスアクセスエラーの場合は、[デバイスタスクを表示]リンクをクリックし、リンク先で失敗したタスクを確認できます。

## 統計ダッシュボード

統計ダッシュボードを表示するには、[レポート]の下のメニューバーで[統計ダッシュボード]をクリックします。統計ダッシュボードが開きます。統計ダッシュボードには、次のレポートの情報が表示されます。

- ベンダーのトップ5：詳細については、「[サマリレポート](#)」（621 ページ）を参照してください。
- OSバージョンのトップ5：詳細については、「[サマリレポート](#)」（621 ページ）を参照してください。
- 構成変更回数（過去7日間）：詳細については、「[ユーザレポートとシステムレポート](#)」（593 ページ）を参照してください。
- 時間ごとの変更履歴：詳細については、「[サマリレポート](#)」（621 ページ）を参照してください。
- 最もアクセスされるデバイスのトップ10：詳細については、「[サマリレポート](#)」（621 ページ）を参照してください。
- システムステータス：詳細については、「[ネットワークステータスレポート](#)」（596 ページ）を参照してください。
- ソフトウェアレベル：詳細については、「[サマリレポート](#)」（621 ページ）を参照してください。
- 構成ポリシー準拠を確認：詳細については、「[サマリレポート](#)」（621 ページ）を参照してください。

## ダイアグラム

ダイアグラムにより、ネットワークデバイスからトポロジーデータを収集できます。ネットワークダイアグラムは、Visio、静的JPEG、または対話的JPEGの形式で表示し、印刷することができます。レイヤ3のIPアドレスとサブネット、およびMACアドレスとVLANを包含するレイヤ2の詳細を含むトポロジーデータにより、ネットワークの現在状態のスナップショットを提供します。

[管理]>[システム管理設定]>[レポート作成]ページでダイアグラムを有効にする必要があります。詳細については、「[ダイアグラム](#)」(71ページ)を参照してください。

VLANの観点からは、指定されたVLANに関連付けられているポートは、VLANボックスに描画されます。該当する場合、CiscoのVLANトランッキングプロトコル(VTP)ドメイン情報も表示されます。すべての集合ポートは非表示となり、関連するポートチャンネルに対する注釈に集合ポート名がリストされます。VLANの詳細については、「[仮想ローカルエリアネットワーク\(VLAN\)](#)」(213ページ)を参照してください。

レイヤ3のデータには、デバイスの構成ファイルから得られるIPアドレスが含まれます。レイヤ2のデータは、各デバイスのインターフェイスのMACアドレスと、デバイスが認識するMACアドレスを示すMACテーブルからのデータに結び付けられます。NAは、同じネットワークに配置されることによって相互に通信できるようになったデバイスをマッピングします。

レイヤ1(物理ケーブル)接続を検出できます。レイヤ1接続は、レイヤ2のデータ(スイッチから見えるMACアドレス)から推測され、キャプチャされてからNAデータベースに追加されます。NAのレイヤ1ダイアグラムのタイプには、HP SAの場合と同じ接続が表示されます。詳細については、『HP Server Automation User's Guide』を参照してください。

推測されるレイヤ1のデータは、経験則に基づいています。NAでは、デバイスとサーバのすべてまたはいずれかの間のデータリンク接続数を減らすことにより、ネットワークダイアグラムを見やすくしています。この場合は、推移する接続から推測可能な接続のみが除かれます。

OSIモデルでは、下位のレイヤを隠すために各レイヤが抽象化されています。したがって、デバイスから収集されたレイヤ2のデータによって100%正確なレイヤ1のデータを生成することはできません。特に、次のいずれかの条件が当てはまる場合は、レイヤ1のデータが不正確になる可能性があります。

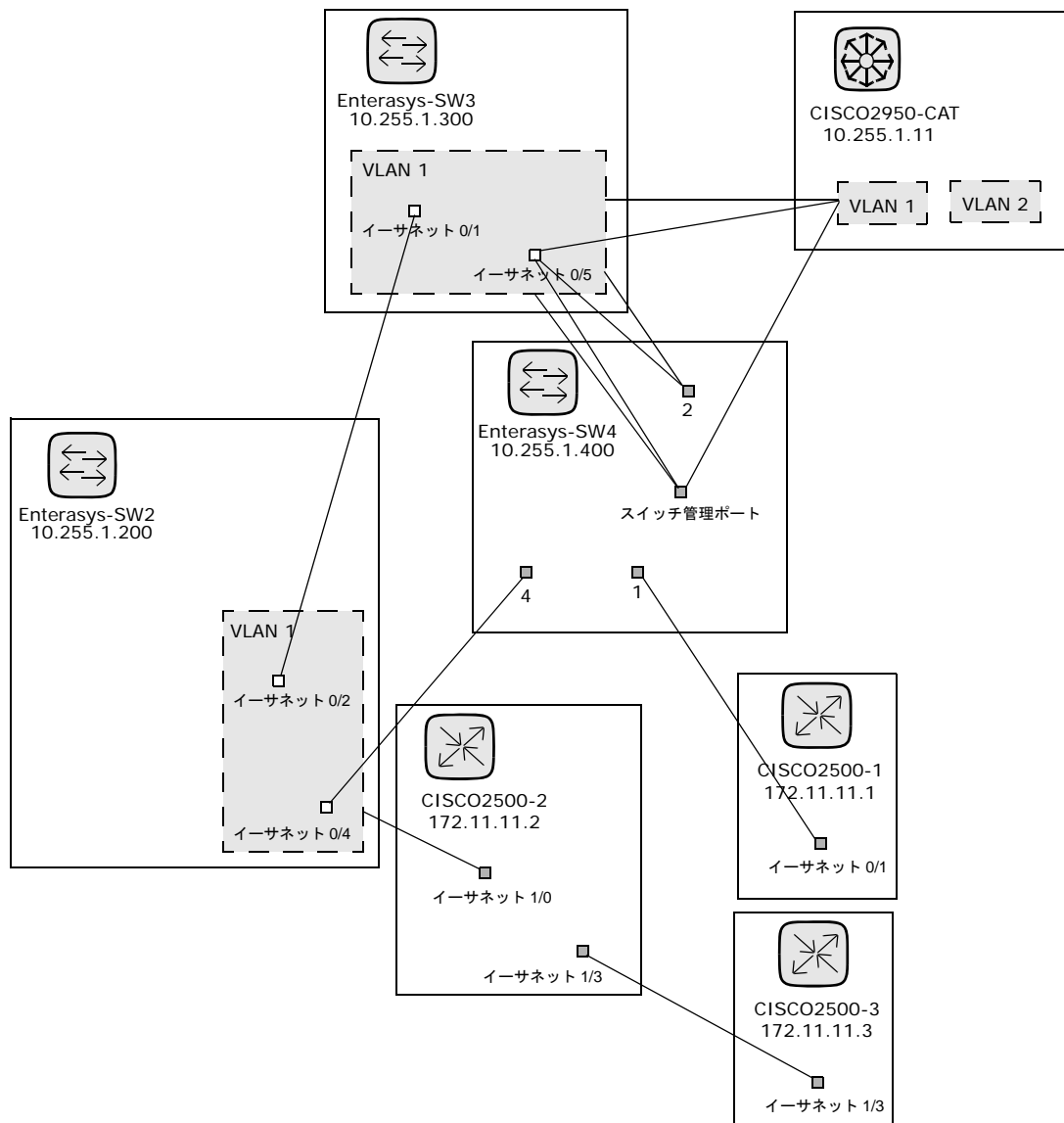
- デバイスが、MACアドレスが認識される場所のインターフェイス番号を返さない。
- NAが、(MACアドレスが認識される場所の)トポロジーデータを収集する数分の間に、デバイス間でトラフィックが発生しなかった。
- 2つの管理デバイスの間に、ハブなどのアドレス指定できないデバイスが存在する。

ダイアグラムでは、次の色、境界線、線、およびアイコンが使用されます。

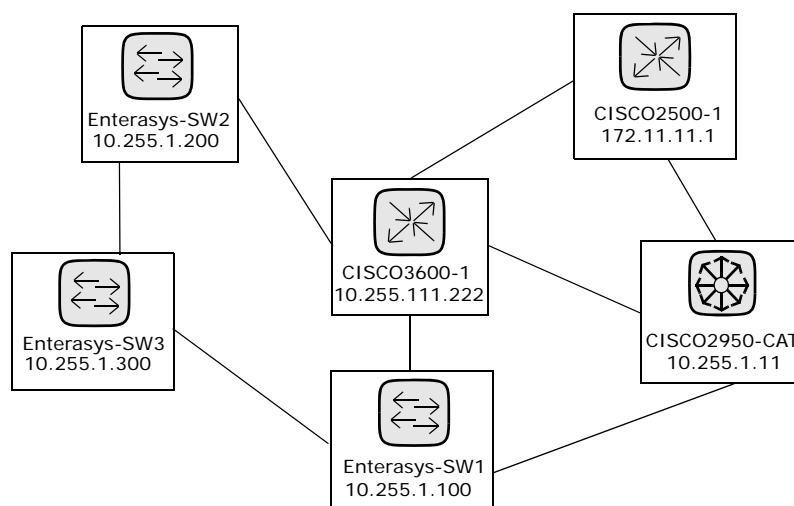
- 赤：デバイスは、スナップショットタスクまたは別のタスクのいずれかの結果として、最後のアクセスに失敗しました。（注意：VLANとポートの場合、赤はVLANが管理目的でダウンしていることを、グレーはVLANが実行されていることを示します）。
- グレー：デバイスにスナップショットデータは含まれていません。
- 白：デバイスは動作中です。
- デバイスの境界：実線の境界はデバイスを示します。点線の境界は仮想グループを示します。仮想グループでは、デバイス内の各VLANが、それ自体が所有するデバイスとして示されます。
- 点線：レイヤ3接続を表します。
- 実線：レイヤ2接続を表します。

	レイヤ3スイッチ		DSL モデム		ルータ
	レイヤ4～7スイッチ		ファイアウォール		サーバ
	ATM スイッチ		ISDN		スイッチ
	ネットワーククラウド		ロードバランサー		不明なデバイス
	デスクトップ		プロキシ		VPN
	非アクティブなデバイス		ポリシー準拠違反		スタートアップ / 実行不一致

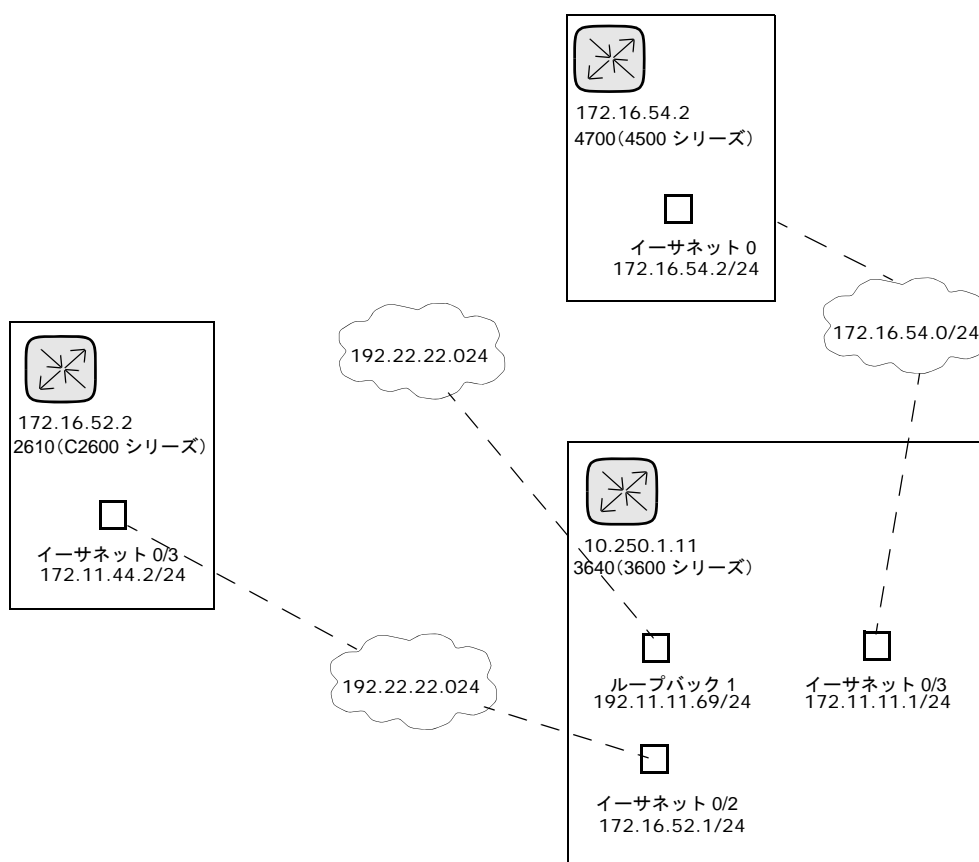
次の図に、VLANとポートの間の接続を含む単純なネットワークダイアグラムを示します。



次のサンプル図に、デバイスが縮小された状態の単純なネットワークダイアグラムを示します。



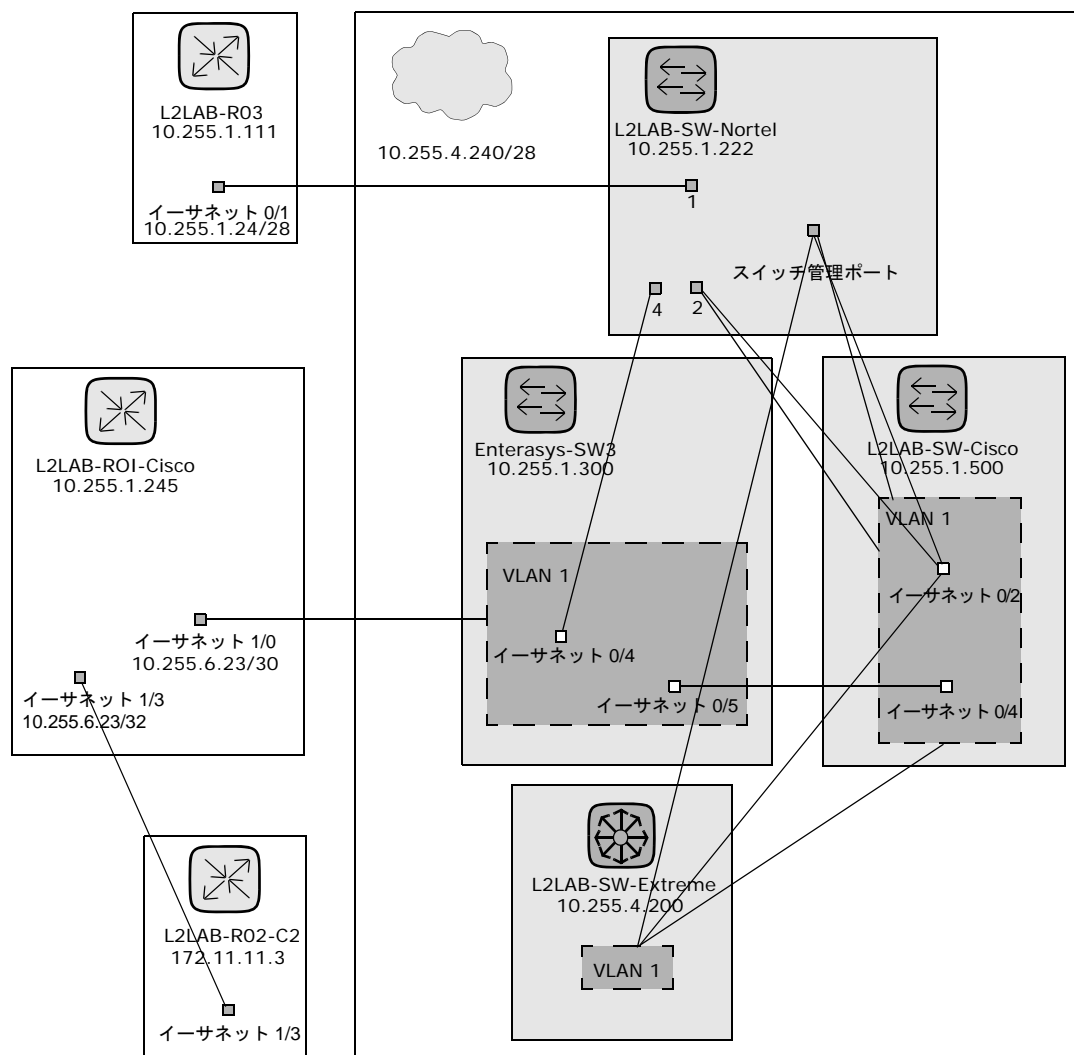
次のサンプル図に、同じサブネットを共有するデバイスを接続するための省略方法としてクラウド（雲形のイラスト）を使用した単純なネットワークダイアグラムを示します。クラウドは、ルータやスイッチなどのゲートウェイオブジェクトを論理的に表します。



レイヤ3のダイアグラムでは、選択されたすべてのデバイスを収集し、IPアドレスとサブネットマスクを使用して同じサブネットのデバイスを接続します。サブネット内の複数のデバイスがクラウドと接続されます。したがって、クラウドはサブネットを表します。

拡張レイヤ3ダイアグラムの開始点は、基本レイヤ3ダイアグラムです。複数のデバイスがサブネットに接続される場合は、サブネットが拡張され、サブネット内に存在するすべてのデバイスの場所が示されます。拡張レイヤ3ダイアグラムには、クラウドに接続され、既知のレイヤ2接続（トポロジー収集診断で検出）を介して他のデバイスにトラバースするすべてのインターフェイスが表示されます。これにより、拡張されたクラウドは、サブネット内に存在するすべてのデバイスのコンテナになります。レイヤ2接続をトラバースするときには、元々選択しなかったデバイスがダイアグラムに追加されます。

次のサンプル図に、拡張レイヤ3ネットワークダイアグラムを示します。基本レイヤ3ダイアグラムが生成された後、複数のデバイスが接続されているそれぞれのクラウドが拡張されます。NAはレイヤ2接続のすべてを調べます。そのため、クラウドの中のデバイスは1つのクラウドノード内でグループ化されます。



[ダイアグラム] ページを表示するには、[レポート] の下のメニューバーで [ダイアグラム] をクリックします。[ダイアグラム] ページが開きます。ダイアグラムの設定が完了したら、[生成] ボタンをクリックします。

## [ダイアグラム]ページのフィールド

フィールド	説明/アクション
ダイアグラムのタイプ	<p>ドロップダウンメニューから次のダイアグラムのタイプの1つを選択します。ダイアグラムのタイプを示すサンプルダイアグラムがドロップダウンメニューの右に表示されます。</p> <ul style="list-style-type: none"> <li>レイヤ1：ポート（推定）</li> <li>レイヤ2：ポート</li> <li>レイヤ3：ポート</li> <li>レイヤ3：ポート（拡張）</li> <li>レイヤ1：デバイス（推定）</li> <li>レイヤ2：デバイス</li> <li>レイヤ3：デバイス</li> <li>レイヤ3：デバイス（拡張）</li> </ul> <p><b>注意：</b>推測されるレイヤ1のデータは、経験則に基づいています。NAでは、デバイスとサーバのすべてまたはいずれかの間のデータリンク接続数を減らすことにより、ネットワークダイアグラムを見やすくしています。この場合は、推移する接続から推測可能な接続のみが除かれます。詳細については、「<a href="#">NA/SA統合</a>」(196ページ)を参照してください。</p>
出力書式	<p>ネットワークダイアグラムの書式を次の中から1つ選択します。</p> <ul style="list-style-type: none"> <li>JPEG（対話的）：ネットワークダイアグラムをJPEG（Joint Photographic Experts Group）出力で表示して、ネットワークダイアグラムのデバイスを選択できます。デバイスを選択すると、そのデバイスの[デバイス詳細]ページが開きます。（「<a href="#">表示メニューオプション</a>」(201ページ)を参照してください）。</li> <li>JPEG（静的）：JPEG（Joint Photographic Experts Group）形式でネットワークダイアグラムを表示します。</li> <li>Visio：Visioでネットワークダイアグラムを表示する場合は、Service Pack 2以上を含むVisio 2003以上、またはVisio Viewerがシステムにインストールされている必要があります。これらのファイルは.rdxファイルです。</li> </ul>
デバイス選択	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>デバイスとグループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセクタの使用方法的詳細については、「<a href="#">デバイスセクタ</a>」(142ページ)を参照してください。</li> <li>ルート：開始ルートデバイスと終了ルートデバイスを入力します。NAは2つのデバイス間でICMPテストタスクを実行します。（ICMPテストタスクの詳細については、「<a href="#">[ICMPテストの実行]タスクページのフィールド</a>」(299ページ)を参照してください）。テストはtracerouteとして実行され、送信元デバイスと宛先デバイス間で検出されたIPアドレスすべてが示されます。</li> <li>単独デバイス：デバイスのIPアドレスまたはホスト名を入力します。評価する接続数を3ホップまで指定できます。</li> </ul>



フィールド	説明/アクション
階層レイヤフィルタ	<p data-bbox="444 243 1466 384">階層レイヤはデバイス属性です。デバイスの階層レイヤは、デバイスを追加または編集するときに設定できます（詳細については、「<a href="#">デバイスの追加</a>」（106ページ）を参照してください）。そのため、ダイアグラムの設定を行うときに、フィルタ処理する階層レイヤを選択できます。たとえば、ネットワーク全体（インベントリ）をダイアグラムで表示し、「コア」でフィルタリングを行ってコアデバイス（階層レイヤが「コア」に設定されたデバイス）のみをダイアグラムで表示することもできます。</p> <p data-bbox="444 415 1466 499"><b>注意：</b>次に示すオプションはデフォルトのフィルタです。ここでフィルタを割り当てることができるようにするには、フィルタ値を割り当てる必要があります。カスタムフィルタの作成方法の詳細については、「<a href="#">appserver.rcx ファイルの編集</a>」（611ページ）を参照してください。</p> <p data-bbox="444 531 1086 558">ドロップダウンメニューから次のオプションを1つ以上選択します。</p> <ul data-bbox="444 579 548 737" style="list-style-type: none"> <li>• コア</li> <li>• 分散</li> <li>• アクセス</li> <li>• エッジ</li> </ul>
詳細オプション	
詳細フィルタ	<p data-bbox="444 821 873 842">次の中からオプションを1つ以上選択します。</p> <ul data-bbox="444 863 1466 1377" style="list-style-type: none"> <li>• 非アクティブのデバイスを非表示：非アクティブなデバイスすべてをネットワークダイアグラムから削除します。</li> <li>• 他の選択されたデバイスに接続されていないデバイスを非表示：他のデバイスへの接続がないデバイスすべてをネットワークダイアグラムから削除します。</li> <li>• 接続のないVLANを非表示：ポートまたは他のVLANへの接続のないVLANをネットワークダイアグラムから削除します。</li> <li>• 接続されていないインターフェイス/ポートを非表示：他のデバイスへの接続がないすべてのインターフェイスとポートをネットワークダイアグラムから削除します。</li> <li>• デバイスに関連付けられていないポートを非表示：ネットワークダイアグラムから、デバイスに関連付けられていないすべてのレイヤ2ポートを削除します。（<b>注意：</b>NAは、管理対象デバイスそれぞれからルーティング情報を収集します。）多くの場合、デバイスには非管理対象デバイスに接続されたデバイスおよびポートへのルートがあります。デバイスは、NAの管理対象デバイスにあるポートを認識できるとしても、HPNA トポロジーデータ収集診断機能をサポートしていない場合があります。この場合NAは、ポートとデバイスの間のグループ化接続を作成できません）。</li> <li>• サブネットクラウドを作成するための最小サブネット接続数を入力します。デフォルト値は2です。</li> </ul>
グループ化	<p data-bbox="444 1409 943 1430">次のオプションのいずれかまたは両方を選択します。</p> <ul data-bbox="444 1451 1466 1690" style="list-style-type: none"> <li>• 含まれるサブネットをそれらのスーパーネットに接続：複数のサブネットをグループ化できます。たとえば、IP アドレス範囲 10.255.0.0/23 と 10.255.1.0/24 があるとします。/24 ネットワークは、/23 ネットワーク内に含まれます。トラフィックは2つのネットワーク間を流れることが可能です。そのためダイアグラムでは、/23 ネットワークと /24 ネットワークが接続されたネットワークのように示されます。</li> <li>• VLAN を別のデバイスとして表示：1つのデバイスを同じデバイスの複数の表現に分割します（VLANあたり1つ）。VLAN デバイスは、他のグラフの種類のデバイス内の VLAN グループと同じ、点線のアウトラインで表示されます。（<b>注意：</b>このオプションは、拡張 L3 ダイアグラムの場合には自動的に選択され、無効にすることはできません。）</li> </ul>

フィールド	説明/アクション
<b>注釈</b>	
デバイスの注釈	<p>グラフ化された各デバイスに表示するフィールドを選択します。テキストでいっぱいになるほど多くのフィールドをグラフに表示することはできません。次に示すオプションを選択できます。</p> <ul style="list-style-type: none"> <li>• ホスト名</li> <li>• プライマリ IP</li> <li>• FQDN</li> <li>• デバイスの説明</li> <li>• パーティション</li> <li>• モデル</li> <li>• ベンダー</li> <li>• シリアル番号</li> <li>• 資産タグ</li> <li>• 最終変更日</li> <li>• カスタムフィールド</li> <li>• 最終アクセスのステータス</li> <li>• 非アクティブのデバイスを表示</li> <li>• ポリシー準拠のステータスを表示</li> <li>• スタートアップとランニング構成の不一致を表示</li> <li>• VTP 情報</li> </ul>
終点の注釈	<p>次の中からオプションを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• インターフェイスの説明</li> <li>• ポート名</li> <li>• IP アドレス</li> <li>• ポートタイプ</li> <li>• ポートのステータス</li> <li>• 実行ポートステータス</li> <li>• MAC アドレス</li> <li>• 領域</li> </ul>
相互接続の注釈	<p>次のオプションを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>• サブネット：サブネット情報を接続線にラベル付けします。</li> <li>• VLAN：VLAN情報を接続線にラベル付けします。</li> </ul>
クラウドの注釈	<p>次のオプションを選択します。</p> <ul style="list-style-type: none"> <li>• サブネット：レイヤ3クラウドにテキストが含まれます（同じサブネットを共有するデバイスを接続するための省略方法）。</li> <li>• 領域：レイヤ3クラウドにテキストが含まれます。（領域は、重複するIPアドレスが存在しないネットワークセグメントです。）</li> </ul>

フィールド	説明/アクション
グラフの注釈	次のオプションを選択します。 <ul style="list-style-type: none"> <li>注釈のタイトル：選択した各注釈にタイトルをつけます。例：ホスト名：L2LAB-SW01-C0000xl</li> </ul>
ダイアグラムを指定した名前 前でユーザレポートとして 保存：	ダイアグラムの名前として入力し、[保存]ボタンをクリックします。
ダイアグラムの電子メール 宛先：	電子メールアドレスを入力し、[電子メール]ボタンをクリックします。

[JPEG (対話的)] オプションを選択した場合は、図が生成された後、デバイスをクリックするとそのデバイスの[デバイス詳細]ページが開きます。詳細については、「[デバイス詳細の表示](#)」(193ページ)を参照してください。

## appserver.rcx ファイルの編集

階層フィルタレイヤには、登場する順序に値が指定されます。たとえば、コアは1、分散は2のようになります。この情報は、*Product/config*ディレクトリに格納されるappserver.rcxファイルに保存されます。ファイルには次のように情報が記述されます。

```
<array name="diagramming/hierarchy_layers">
  <value>core</value>
  <value>distribution</value>
  <value>access</value>
  <value>edge</value>
</array>
```

数値はデータベースに保存されます。appserver.rcx ファイルを編集する場合は、変更内容がデータベースに反映されません。したがって、デバイスに関連付けられているデータも変更する必要があります（詳細については、「[デバイスの新規作成](#)」ページのフィールド」(106ページ)を参照してください)。

## デバイスソフトウェアレポート

デバイスソフトウェアレポートにより、各デバイスのソフトウェアバージョンと割り当てられている現在の準拠レベルを表示できます。

デバイスソフトウェアレポートを表示するには、[レポート]の下メニューバーで[デバイスソフトウェア]をクリックします。[デバイスソフトウェアレポート]が開きます。

## デバイスソフトウェアレポートのフィールド

フィールド	説明
ソフトウェアレベルレポート	ソフトウェアレベルレポートが開きます。このレポートでは、各デバイスに現在割り当てられているソフトウェアのバージョンとレベルを表示できます。 <a href="#">「ソフトウェアレベルレポートのフィールド」(614 ページ)</a> を参照してください。
ソフトウェアレベル	[ソフトウェアレベル]ページが開きます。このページでは、ソフトウェアレベルを編集または削除できます。 <a href="#">「新規ソフトウェアレベルの追加」(449 ページ)</a> を参照してください。
現在の作業グループ	ドロップダウンメニューからデバイスグループを選択します。インベントリがデフォルトの設定です。
次のレベル以下	次の中からソフトウェアレベルを選択します。 <ul style="list-style-type: none"> <li>• 任意のレベル</li> <li>• セキュリティリスク</li> <li>• 実稼動前</li> <li>• ブロンズ</li> <li>• シルバー</li> </ul>
ホスト名	デバイスのホスト名を表示します。ホスト名をクリックすると[デバイス詳細]ページが開きます。このページでは、デバイスについての詳細な情報を表示できます。
デバイス IP	デバイスの IP アドレスを表示します。赤で表示されるデバイスは、最新のスナップショットの取得に失敗しています。非アクティブなデバイスは、IP アドレスの横のアイコンでマーキングされています。
変更日	ソフトウェアが最後にデバイスに配布された日時を表示します。
デバイスソフトウェアのバージョン	デバイスで実行されている検出されたソフトウェアのバージョンを表示します。
ソフトウェアレベル	該当する場合、ソフトウェアレベルを表示します。
重要度	セキュリティの脆弱性を次の重要度で表示します。 <ul style="list-style-type: none"> <li>• 情報：一般的に対応を必要としないイベント。</li> <li>• 低：時間的な余裕がある場合に対応を必要とするイベント。</li> <li>• 中：適時に対応を必要とするイベント（通常は72時間以内）。</li> <li>• 高：緊急の対応を必要とするイベント（通常は24時間以内）。</li> <li>• 重要：即時の対応を必要とするイベント。</li> </ul>
コメント	脆弱性の説明を入力します。

フィールド	説明
アクション	<p>次のアクションを選択できます。</p> <ul style="list-style-type: none"><li>ソフトウェア監査証跡を表示: デバイスの[ソフトウェア監査証跡]ページを開きます。このページでは、デバイスにロードされているソフトウェアを表示できます。詳細については、<a href="#">「[デバイスソフトウェア履歴] ページのフィールド」(228ページ)</a> を参照してください。</li></ul>

## ソフトウェアレベルレポート

ソフトウェアレベルレポートにより、各デバイスに現在割り当てられているソフトウェアバージョンとレベルを表示できます。

ソフトウェアレベルレポートを表示するには：

1. [ポリシー]の下にあるメニューバーの[ソフトウェアレベル]をクリックします。[ソフトウェアレベル]ページが開きます。詳細については、「[\[ソフトウェアレベル\]ページのフィールド](#)」(435ページ)を参照してください。
2. ページの最上部にある[ソフトウェアレベルレポート]リンクをクリックします。ソフトウェアレベルレポートが開きます。

## ソフトウェアレベルレポートのフィールド

フィールド	説明
デバイスソフトウェアレポート	デバイスソフトウェアレポートが開きます。このレポートでは、各デバイスのソフトウェアバージョンと割り当てられている現在の準拠レベルを表示できます。「 <a href="#">デバイスソフトウェアレポートのフィールド</a> 」(612ページ)を参照してください。
ソフトウェアレベル	[ソフトウェアレベル]ページが開きます。このページでは、ソフトウェアレベルを編集または削除できます。「 <a href="#">新規ソフトウェアレベルの追加</a> 」(449ページ)を参照してください。
現在の作業グループ	ドロップダウンメニューからデバイスグループを選択します。インベントリがデフォルトの設定です。
最低限の重要度	セキュリティの脆弱性の重要度について、次の重要度レベルを選択します。 <ul style="list-style-type: none"> <li>• 情報：一般的に対応を必要としないイベント。</li> <li>• 低：時間的な余裕がある場合に対応を必要とするイベント。</li> <li>• 中：適時に対応を必要とするイベント（通常は72時間以内）。</li> <li>• 高：緊急の対応を必要とするイベント（通常は24時間以内）。</li> <li>• 重要：即時の対応を必要とするイベント。</li> </ul>
ホスト名	デバイスのホスト名を表示します。ホスト名をクリックすると[デバイス詳細]ページが開きます。このページでは、デバイスについての詳細な情報を表示できます。
デバイスIP	デバイスのIPアドレスを表示します。IPアドレスをクリックすると[デバイス詳細]ページが開きます。このページでは、デバイスについての詳細な情報を表示できます。
変更日	ソフトウェアが最後にデバイスに配布された日時を表示します。
デバイスソフトウェアのバージョン	デバイスで実行されている検出されたソフトウェアのバージョンを表示します。
ソフトウェアレベル	ソフトウェアのソフトウェアレベル評価を表示します。

フィールド	説明
重要度	セキュリティの脆弱性を次の重要度で表示します。 <ul style="list-style-type: none"><li>• 情報：一般的に対応を必要としないイベント。</li><li>• 低：時間的な余裕がある場合に対応を必要とするイベント。</li><li>• 中：適時に対応を必要とするイベント（通常は72時間以内）。</li><li>• 高：緊急の対応を必要とするイベント（通常は24時間以内）。</li><li>• 重要：即時の対応を必要とするイベント。</li></ul>
コメント	脆弱性の詳細を示します。
アクション	次のアクションを選択できます。 <ul style="list-style-type: none"><li>• ソフトウェア監査証跡を表示：デバイスの[ソフトウェア監査証跡]ページを開きます。このページでは、デバイスにロードされているソフトウェアを表示できます。詳細については、<a href="#">「[デバイスソフトウェア履歴] ページのフィールド」</a>（228 ページ）を参照してください。</li></ul>

## ソフトウェアの脆弱性レポート

HP Live Network ポリシーをロードするまで、ソフトウェアの脆弱性レポートの検索結果ページにはなにも表示されません。

**注意：** HP Live Networkにより、セキュリティアラートサービスデータとその他のNAコンテンツサービスマテリアルをダウンロードできます。HP Live Networkの詳細については、「[ヘルプメニューオプション](#)」(24 ページ) を参照してください。

TON ポリシーをインストールして準拠の確認を実行すると、Common Vulnerabilities and Exposures (CVE) 値のあるポリシーに関する結果が表示されます。

ソフトウェアの脆弱性レポートは、準拠とポリシーの確認の結果を含むテーブルからデータを収集します。このため、特定のソフトウェアの脆弱性イベントは生成されません。生成されるイベントは、「構成ポリシーに非準拠です」イベントです。

ソフトウェアの脆弱性レポートを表示するには、[レポート] の下のメニューバーで [ソフトウェアの脆弱性] をクリックします。ソフトウェアの脆弱性レポートが開きます。

## ソフトウェアの脆弱性レポートのフィールド

フィールド	説明/アクション
チェックボックス/ドロップダウンメニュー	<p>左側のチェックボックスをオンにして、特定デバイスを選択できます。デバイスを選択したら、[アクション] ドロップダウンメニューをクリックし、次のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>一括編集</li> <li>ポリシー準拠の確認</li> <li>パスワードの配布</li> <li>デバイスのリブート</li> </ul>
ホスト名	デバイスのホスト名を表示します。
デバイス IP	デバイスの IP アドレスを表示します。
デバイス準拠ステータス	デバイスの準拠ステータスを表示します。
ポリシー	ポリシーの名前が表示されます。
ルール	ポリシー構成ルールが表示されます。
ルールの重要性	<p>重要度レベルを選択します。</p> <ul style="list-style-type: none"> <li>情報：一般的に対応を必要としないイベント。</li> <li>低：時間的な余裕がある場合に対応を必要とするイベント。</li> <li>中：適時に対応を必要とするイベント（通常は72時間以内）。</li> <li>高：緊急の対応を必要とするイベント（通常は24時間以内）。</li> <li>重要：即時の対応を必要とするイベント。</li> </ul>
ルールの説明	ルールの説明を表示します。



フィールド	説明/アクション
CVE	演算子と一緒に CVE（Common Vulnerabilities and Exposures）名を入力します。CVE とは、セキュリティ問題に関する脆弱性やその他の情報に付けられた標準名のリストです。
最終確認日	最終確認日を表示します。

## イメージ同期レポート

イメージ同期レポートでは、デバイスやデバイスのグループ上にあってNAソフトウェアイメージリポジトリにはない、現在実行中のソフトウェアイメージ、またはバックアップソフトウェアイメージを表示できます。デバイスからNAソフトウェアイメージリポジトリにソフトウェアイメージをコピーするタスクをスケジュールできます。これにより、緊急時にはすべてのソフトウェアイメージをNAソフトウェアリポジトリからダウンロードできます。

**注意：** この機能をサポートしていないドライバが存在します。サポートされるデバイスの詳細については、Driver Release Service（DRS）ドキュメントを参照してください。DRSは、自動化されたドライバのリリースと配信システムです。

イメージ同期レポートを表示するには、[レポート]の下メニューバーで[イメージ同期レポート]をクリックします。イメージ同期レポートが開きます。

## イメージ同期レポートのフィールド

フィールド	説明/アクション
現在の作業グループ	デフォルトグループを表示します。該当する場合は、ドロップダウンメニューから別のグループを選択できます。
チェックボックス/ ドロップダウンメニュー	左側のチェックボックスをオンにして、特定デバイスを選択できます。デバイスを選択すると、[選択]ドロップダウンメニューを選択して[すべて]や[なし]をクリックしたり、隣にある[アクション]ドロップダウンメニューを選択して[イメージを同期]、または[ファイル名を除く]オプションをクリックできます。[ファイル名を除く]オプションを使用することで、NAが無視するリストにファイル名を追加できます。こうすることで、イメージ同期レポートにファイル名が表示されなくなります。（ <b>注意：</b> [イメージを同期]オプションを使用するには、デバイスの修正権限が必要です）。
[イメージを同期] オプション	[デバイスソフトウェアのバックアップ]タスクのページを開きます。このページで、NAソフトウェアイメージリポジトリにソフトウェアイメージをコピーできます。（詳細については、「 <a href="#">[デバイスソフトウェアのバックアップ]タスクページのフィールド</a> 」（369ページ）を参照してください。）
ホスト名	デバイスのホスト名が表示されます。ホスト名をクリックすると、[デバイス詳細]ページが開きます。このページでは、デバイスとその構成履歴に関する情報を表示できます。
デバイスIP	デバイスのIPアドレスを表示します。IPアドレスをクリックすると、[デバイス詳細]ページが開きます。このページでは、デバイスとその構成履歴に関する情報を表示できます。
スロット	ソフトウェアイメージがインストールされているデバイスのスロットを表示します。
ファイル名	ソフトウェアイメージの名前を表示します。
ファイルサイズ	ソフトウェアイメージのサイズを表示します。
検索結果を電子メール送信	検索結果の送信先の電子メールアドレスを入力して、[送信]をクリックします。電子メールアドレスが複数の場合は、必ずカンマで区切ってください。
検索結果をCSVファイル として表示	Excel（Windows プラットフォーム）、Star Office、またはGnumeric（Unix プラットフォーム）を使用して、CSV形式で検索結果を開きます。

## システム/ネットワークイベントレポート

システム/ネットワークイベントレポートにより、1つのデバイスまたはすべてのデバイスのいずれかに対する変更を示すイベントを追跡できます。イベントの全リストは、「[イベントの説明](#)」(515 ページ) を参照してください。

システム/ネットワークイベントレポートを表示するには、[レポート]の下のメニューバーで[システム/ネットワークイベント]をクリックします。システム/ネットワークイベントレポートが開きます。

## システム/ネットワークイベントレポートのフィールド

フィールド	説明/アクション
メッセージの新規作成	[メッセージの新規作成] ページを開きます。このページでは、このデバイスを参照して、すべてのユーザに対するメッセージをポストできます。シングルビューでイベントを追跡するオプションも選択できます。
対象：	<p>イベントを表示するための時間枠が表示されます。次のオプションが用意されています。</p> <ul style="list-style-type: none"> <li>過去1、2、4、8、12、24、および48時間</li> <li>過去1および2週間</li> <li>過去1ヶ月</li> <li>全イベント</li> </ul>
現在の作業グループ	ドロップダウンメニューからデバイスグループを選択します。
チェックボックス	左側のチェックボックスをオンにすると、NA データベースからイベントを削除できます。イベントを選択して[アクション]ドロップダウンメニューをクリックし、[削除]をクリックしてください。これにより、選択したイベントがNA データベースから削除されます。隣接の[選択]ドロップダウンメニューを使用すると、イベントを全選択または全選択解除できます。
イベント日時	イベントの日付/時刻がMMM-dd-yy HH:mm:ss形式で表示されます。(フォーマットはシステム管理者が自由に設定できます。)
ホスト名	デバイスのホスト名またはIP アドレスが表示されます。ホスト名またはIP アドレスをクリックすると、[デバイス詳細]ページが開きます。このページには、デバイスおよびデバイス構成履歴に関する情報が表示されます。
サマリ	<p>イベントのタイプが表示されます。イベントのリストについては、「<a href="#">イベントの説明</a>」(515 ページ) を参照してください。イベントタイプのリンクをクリックすると、[イベントの詳細]ページが開きます。このページの内容は次のとおりです。</p> <ul style="list-style-type: none"> <li>イベントが発生した日付および時刻。</li> <li>イベントを追加したユーザのログイン名またはプロセス。診断変更の[詳細]リンクをクリックすると、[タスク結果]ページが開きます。このページには、タスク詳細が表示されます。「<a href="#">[タスク情報]ページのフィールド</a>」(406 ページ) を参照してください。</li> <li>イベントタイプ。</li> <li>イベントの簡単な説明。</li> <li>デバイスに関する詳細情報へのリンク。</li> </ul>
追加ユーザ名	イベントが作成される原因となったアクションを起こしたユーザのログイン名が表示されます。

## ソフトウェアの脆弱性イベントの詳細レポート

ソフトウェアの脆弱性イベントの詳細レポートにより、助言情報および解決策を含むソフトウェアの脆弱性の詳細を表示できます。

ソフトウェアの脆弱性イベントの詳細を表示するには：

1. メニューバーで[検索]を選択し、[イベント]をクリックします。[イベントを検索]ページが開きます。
2. [ソフトウェアの脆弱性が検出されました]イベントサマリを選択し、[検索]ボタンをクリックします。[イベントの検索結果]ページが開きます。

フィールド	説明/アクション
チェックボックス	左側のチェックボックスをオンにすると、NAデータベースからイベントを削除できます。イベントを選択して[アクション]ドロップダウンメニューをクリックし、[削除]をクリックしてください。これにより、選択したイベントがNAデータベースから削除されます。隣接の[選択]ドロップダウンメニューを使用すると、イベントを全選択または全選択解除できます。
日付	イベントの日付/時刻がMMM-dd-yy HH:mm:ss形式で表示されます。(フォーマットはシステム管理者が自由に設定できます。)
サマリ	<p>検出されたソフトウェアの脆弱性を表示します。リンクをクリックすると、[イベントの詳細]ページが開きます。このページでは、セキュリティの脆弱性について次の情報を表示できます。</p> <ul style="list-style-type: none"> <li>• 日付</li> <li>• 追加ユーザ名</li> <li>• サマリ</li> <li>• 記述。名前、重要度、およびCVE（共通の脆弱性と公開）を含みます</li> <li>• アクション：NAレポートへのリンクと、諮問およびソリューション情報への外部リンクを表示します。</li> <li>• デバイス</li> </ul>
ホスト名	デバイスのホスト名またはIPアドレスが表示されます。ホスト名またはIPアドレスをクリックすると、[デバイス詳細]ページが開きます。このページには、デバイスおよびデバイス構成履歴に関する情報が表示されます。
追加ユーザ名	イベントを追加したユーザ名を表示します。

## サマリレポート

サマリレポートには、ネットワークでの構成アクティビティの概要が示されます。このレポートは、傾向を分析し、特に注意を要する問題領域を識別するのに役立ちます。サマリレポートは上級管理者に容易に提出することができ、これにより、チームが行う作業の内容と組織への貢献度を示すことができます。データは標準のMicrosoft Excel形式のスプレッドシートで提供されるため、情報をソートおよびフィルタし、切り取って他のアプリケーションに貼り付ける操作も容易に行うことができます。

デフォルトでは、週次単位でサマリレポートを更新するようにNAが構成されます。更新時には、前のサマリレポートファイルが毎回バックアップされるため、それらのレポートのアーカイブを保持して、履歴分析で使用したり、監査証跡を提供したりできます。レポートは、デフォルトでは `.\<install directory>\addins` に保存されます。

サマリレポートを手動で更新するには：

1. [タスク]の下メニューバーで[タスクの新規作成]をクリックし、[サマリレポートの生成]を選択します。  
[タスクの新規作成 - サマリレポートの生成]ページが開きます。
2. [すぐに開始]が選択されていることを確認します。
3. [タスクを保存]をクリックします。

タスクによってサマリレポートが更新され、[タスク情報]ページにタスクのステータスが表示されます。ステータスが[成功]の場合は、最新のサマリレポートを開くことができます。

**注意：** サマリレポートはMicrosoft Excelで開くことができます。Excelのマクロを使用して、レポートデータが計算されます。ブラウザとExcelのセキュリティ設定によっては、サマリレポートを開くときにマクロを有効にするかどうかを尋ねるメッセージが表示されます。

サマリレポートを開くには、[レポート]の下メニューバーで[サマリレポート]をクリックします。ドロップダウンメニューに[サマリレポート]と表示されない場合、システム管理者は管理設定を確認してください。

特定のサマリレポートにナビゲートするには、最上位のサマリレポートでコンテンツリンクをクリックし、[ホーム]リンクを使用して最上位のサマリレポートに戻るか、または各レポートの下部にあるタブを使用します。下部に表示されないタブがある場合は、ウィンドウを最大化するか、または列のアジャスタをクリックして右方向にドラッグします。

## サマリレポートの説明

レポート	報告される情報
サマリ	<p>最近の変更アクティビティの割合、最もアクティブなユーザ、およびネットワークプロファイルの概要を表示します。レポートには次の情報が含まれています。</p> <ul style="list-style-type: none"> <li>• ベンダーのトップ5：ベンダーのトップ5あたりのデバイス数を表示します。</li> <li>• OSバージョンのトップ5：使用中のOSバージョンのトップ5を表示します。</li> <li>• 構成変更回数（過去7日間）：過去7日間における1日あたりの平均構成変更回数を表示します。</li> <li>• 時間ごとの変更履歴：構成変更が行われた時刻を表示します。</li> <li>• 最もアクセスされるデバイスのトップ1：報告期間中にアクセスが最も多いデバイスのトップ10を表示します。</li> </ul>
変更頻度	<p>ネットワークで行われた変更の概要を表示します。レポートには、過去30日間の週単位の平均変更数が、ユーザとデバイスグループに分けて示されます。これにより、最高のパフォーマンスとともに、変更の不均衡割合を示すネットワーク領域を識別できます。</p>
1日あたりの変更数	<p>過去2週間の1日あたりの構成変更回数を表示します。レポートには、同じデータが棒グラフと表形式で示されます。縦軸には変更回数が表示されます。横軸には、2週間分の日付が表示されます。</p>
統計グラフ	<p>先週中に行われた構成変更を表示します。[変更の検出方法]円グラフには、変更が検出された方法について次の情報が表示されます。</p> <ul style="list-style-type: none"> <li>• Syslog</li> <li>• Telnet/SSH</li> <li>• プロキシ</li> <li>• 通常または手動のポーリング</li> <li>• AAA</li> <li>• 構成またはスクリプトの配布</li> </ul> <p>[時間ごとの変更履歴]棒グラフには、NAが変更を検出した時刻が表示されます。これらのグラフを使用して、行った変更を監視できます。また、Telnet/SSHプロキシ、コマンドスクリプト、または構成の編集と配布を使用して、ネットワークエンジニアに変更を行わせるポリシーを設定することもできます。</p>
構成変更	<p>過去の週について次の情報を表示します。</p> <ul style="list-style-type: none"> <li>• 変更の原因と変更数を含む変更検出。</li> <li>• 時間ごとの変更履歴。</li> <li>• ホスト名、IPアドレス、最後の変更日時を含むデバイス構成変更、プロキシからのユーザ名、AAA、Syslogなど。</li> </ul>

レポート	報告される情報
デバイスステータス	<p>NAによって追跡された非アクティブなデバイスを表示します。</p> <ul style="list-style-type: none"> <li>• 最もアクセスされるデバイスのトップ10：過去の週において構成スナップショットを最も取得したデバイスを表示します。通常は、エンジニアが最も頻繁にログインまたは変更するデバイスです。</li> <li>• デバイスパスワードの変更：過去の週にパスワードが変更されたすべてのデバイスのレコードを表示します。</li> <li>• アクセス障害があったデバイス：デバイスが動作していなかったか、またはパスワード情報が誤っていたことにより、NAがアクセスできなかったデバイスを表示します。このリストをチェックリストとして使用し、NAによってデバイスが正常に管理されるようにすることができます。</li> </ul>
デバイスのインベントリ	<p>NAによって追跡されたすべてのデバイスについて、次の情報を表示します。</p> <ul style="list-style-type: none"> <li>• ホスト名（[デバイス情報]ページより）</li> <li>• IPアドレス（[デバイス情報]ページより）</li> <li>• 資産タグ（[デバイス情報]ページより）</li> <li>• 場所（構成ファイルより）</li> <li>• ベンダー（構成ファイルより）</li> <li>• モデル（構成ファイルより）</li> <li>• オペレーティングシステムのバージョン（構成ファイルより）</li> <li>• シリアル番号（構成ファイルより）</li> <li>• デバイスの説明（[デバイス情報]ページより）</li> <li>• 最後のスナップショットの結果（タスクより）</li> <li>• 最後に変更された構成（タスクより）</li> </ul>
オペレーティングシステム（OS）のインベントリ	<p>ネットワークで稼動するすべてのデバイスのOSバージョンを表示し、各バージョンを実行しているデバイスの数をリスト表示します。このレポートは次の場合に役立ちます。</p> <ul style="list-style-type: none"> <li>• 受け入れられているOSバージョンの企業標準に準拠します。</li> <li>• アーキテクチャまたはサービスに対して提案される変更をテストまたは評価します。</li> <li>• ベンダーのセキュリティアラートまたはパッチを特定のOSバージョンに適用する時間を節約します。</li> </ul>
システムステータス	<p>NAシステムの動作と動作状態を表示します。レポートには、デバイスドライバが割り当てられていないために管理できないデバイスがリスト表示されます。また、最近のシステム動作とNAデータベース内のレコード数についてのサマリも表示されます。</p> <ul style="list-style-type: none"> <li>• システムステータス：レポートには、デバイスおよびグループについて、構成、デバイス、デバイスグループ、非管理デバイス、および認証ルールの合計数が表示されます。ユーザの場合は、ユーザの合計数およびNAアカウントなしのAAAユーザがレポートに表示されます。レポートには、カスタムレポートの数も表示されます。</li> <li>• システムアクティビティ：レポートには、タスクおよびメッセージについて、成功したタスク、失敗したタスク、およびシステムイベントの合計数が表示されます。統合されたTelnet/SSHクライアントについては、記録されたTelnetセッションとSSHセッションの合計数がレポートに表示されます。</li> <li>• ドライバがないデバイス：ドライバがないデバイスのホスト名とIPアドレスを表示します。</li> </ul>

レポート	報告される情報
ポリシー準拠	<p>準拠しているポリシーと準拠していないポリシーの数を表示します。ホスト名、IPアドレス、および最後の構成変更情報が表示されます。レポートには、次の情報について数値合計を表した1つの簡単な円グラフと、詳細なデータを示した3つの表が表示されます。</p> <ul style="list-style-type: none"><li>• 準拠している構成ポリシー</li><li>• 準拠していない構成ポリシー</li><li>• 構成ポリシー（構成ポリシーの名前と関連付けられたルールを含む）</li></ul>

## 電子メールレポート

レポートを電子メールで送信できます。[レポート]の下メニューバーで[レポートタスクの新規作成]を選択し、[電子メールレポート]をクリックします。[タスクの新規作成 - 電子メールレポート]ページが開きます。詳細については、「[\[電子メールレポート\]タスクページのフィールド](#)」(377ページ)を参照してください。



## 第17章：SecurIDの使用

### トピックの参照先リスト

トピック	参照先：
はじめに	<a href="#">「はじめに」</a> （626 ページ）
インストールの前提条件	<a href="#">「インストールの前提条件」</a> （627 ページ）
RSA Server Authentication Manager	<a href="#">「RSA Server Authentication Manager」</a> （627 ページ）
ユーザ認証	<a href="#">「ユーザ認証」</a> （627 ページ）
ネットワークデバイスへのアクセス	<a href="#">「ネットワークデバイスへのアクセス」</a> （628 ページ）
SecurID トークンの追加	<a href="#">「SecurID ソフトウェアトークンの追加」</a> （630 ページ）
SecurID を使用したNAへのログイン	<a href="#">「SecurID を使用したログイン」</a> （631 ページ）
SecurID のトラブルシューティング	<a href="#">「SecurID のトラブルシューティング」</a> （633 ページ）

## はじめに

RSA SecurID ソリューションは、認証されたユーザにのみネットワーク構成されたリソースへのアクセス権を与えることで確実に組織を保護するように設計されています。一般にSecurIDは、2つの部分で構成される認証方式で、パスワード/PINとともに物理ハードウェアコンポーネントを必要とします。ハードウェアコンポーネントは、60 秒ごとにパスコードを変更します。一部のデバイス製造者は、この認証システムをネットワークデバイスに組み込んでいます。SecurIDの仕組みの詳細については、ご使用のSecurIDのマニュアルを参照してください。

**注意：** 外部認証としてSecurIDを使用するようにNAを構成している場合は、NAプロキシに接続するときのシングルサインオン機能が無効になります。SecurIDのパスコードは再利用できないため、お使いのSecurIDの資格情報を使用して再認証する必要があります。

HP Network Automation (NA) は次の場合に、安全性に優れた2要素認証機能で使用するSecurIDをサポートします。

- NAにログインするユーザを認証する
- NA経由でネットワークデバイスにアクセスする

次の表は、NAのSecureIDサポートを示します。

NAへのアクセス	接続方法	SecurIDのサポート
Webユーザインターフェイス	HTTP	はい
SSH/Telnet プロキシ	SSH	はい
	Telnet	はい
API	RMI	いいえ

**注意：** デバイスでSecurID認証と一緒にSSHを使用するには、デバイスがキーボード対話を使用するSecurID over SSH、特にNext-token-codeモードをサポートしていることを確認してください。

## インストールの前提条件

NA へのログインに SecurID を使用している場合、NA では次のトークンアルゴリズムとトークンバージョンがサポートされます。

- AES SDTID 3.0
- SID SDTID 2.0

**注意：** NA が Windows 2003 (64 ビット) プラットフォームにインストールされている場合、RSA SecurID 6.1 は機能しません。

## RSA Server Authentication Manager

NA インストーラは、インストール時に `NA_DIRECTORY/jre` ディレクトリの `rsa_api.properties` ファイルをインストールします。以下を含めるようにこのファイルを編集する必要があります。

- `RSA_AGENT_HOST` : NA が存在するサーバの IP アドレス。
- `SDCONF_LOC` : RSA Server Authentication Manager が生成する RSA 構成ファイルの格納場所。

下の例では、IP アドレスが 10.255.140.124 のサーバに NA がインストールされていることが示されています。RSA 構成ファイルは、`c:\NA\jre\sdconf.rec` に保存されています。

```
RSA_AGENT_HOST=10.255.140.124
```

```
SDCONF_LOC=C:/NA/jre/sdconf.rec (Unix プラットフォーム)
```

```
SDCONF_LOC=C:\\NA\\jre\\sdconf.rec (Windows プラットフォーム)
```

## ユーザ認証

NA へのユーザ認証の場合は、次の点を確認します。

- ハードウェアかソフトウェアのトークンを RSA から購入している。
- ACEServer が稼動しており、NA サーバからアクセスできる。
- NA が稼動しているホストが、ACEServer でエージェントホストとして追加されている。
- ホストエージェントの設定で、エージェントタイプが「UNIX Agent」になっている。
- ACEServer でユーザを作成した。
- ソフトウェアトークンを ACEServer のユーザに割り当てた。
- ユーザがエージェントホストから接続できるようにした。

NA からデバイスにアクセスする場合は、次の点を確認します。

- NA が実行中である。
- NA サーバに RSA ソフトウェアトークンソフトウェアがインストールされている。
- ACEServer が稼動しており、デバイスからアクセスできる。
- RSA からソフトウェアトークンを入手している。
- RSA ソフトウェアトークンアプリケーションを使用して、NA サーバに SecurID トークンをインポートした。
- ライセンスを ACEServer に追加した。

- ACEServerでユーザを1人作成している。
- ソフトウェアトークンをユーザに割り当てた。
- トークンのPINを設定した。
- ユーザがデバイスに接続できるようにした。
- NAにおいて、SecurIDユーザに対応するユーザを追加した。
- ユーザごとの固有のトークン、またはトークンのプールを使用するかどうかを選択した。
- トークンプールを使用する場合は、トークンプールのユーザ名を割り当てた。
- トークンをユーザに割り当てた。

## ネットワークデバイスへのアクセス

NAからデバイスにアクセスする場合は、ソフトウェアトークンソフトウェアとライセンスをRSAのサイトからダウンロードする必要があります。FOBSやピンパッドなどのハードウェアトークンライセンスは使用できません。

ソフトウェアトークンソフトウェアは、RSAのWebサイトからダウンロードできます。このソフトウェアは、必ずNAがインストールされているシステムにインストールしてください。また、通常のSecurIDメカニズムにより、ソフトウェアトークンライセンスをこのシステムにインポートする必要もあります。

**注意：** ACEServerおよびNAを実行しているサーバは、時刻を同期させる必要があります。ご存知のように、ソフトウェアトークンは時間差に対して敏感です。2つのサーバの同期差が1分より大きくなると、生成されるパスワードが無効になります。両方のサーバでNTPを使用して、クロック精度を維持できます。

NAは、SecurIDが使用されるときにデバイスへのアクセスを監視し、与えられたトークンコードが2度使用されることがないようにします。したがって、SecurIDによるデバイスアクセスを使用するときには、NA内での動作速度が遅くなります。この状態に対処するため、NAには複数のソフトウェアトークンシードをシステムにロードする機能が用意されています。次に示すトークン管理モードのいずれかを使用できます。

- ユーザ単位：各NAユーザは、1つ以上の対応するソフトウェアトークンシードを持ちます。このモードでは、各デバイスアクセスで、タスクまたはNAプロキシ接続を開始したユーザに対応するシードのみを使用します。システム内のすべてのユーザに有効なソフトウェアトークンを割り当てることをお勧めします。
  - － ホームページの[自分の設定]の下にある[自分のプロフィール]をクリックします。[自分のプロフィール]ページが開きます。[自分のプロフィール]ページのフィールドの詳細については、「[\[自分のプロフィール\]ページのフィールド](#)」(260ページ)を参照してください。

**注意：** SecurID トークンの追加または更新の詳細については、「[SecurID ソフトウェアトークンの追加](#)」(630ページ)を参照してください。

- プール：NAには、通常使用されるソフトウェアトークンシードのプールがあり、最大限のパフォーマンスを得るためにできるだけ効率良く使用されます。[管理]メニューバーから[システム管理設定]を選択し、[デバイスアクセス]をクリックします。[デバイスアクセス]ページが開きます。このページでは、SecurIDによるデバイスアクセスを構成できます。詳細については、「[\[デバイスアクセス\]ページのフィールド](#)」(45ページ)を参照してください。

ソフトウェアシードがNAにロードされた後は、特定のデバイスまたはデバイスセットをRSA SecurID 認証経由の管理対象に指定できます。特定のデバイスへのSecurIDアクセスを有効にするには：

1. [デバイス]メニューで、[インベントリ]をクリックします。すべての管理対象デバイスのリストが開きます。
2. SecurIDアクセスを有効にするデバイスをクリックします。[デバイス詳細]ページが開きます。
3. [アクション]列で、[編集]をクリックします。[デバイスを編集]ページが開きます。詳細については、**「[デバイスの新規作成]ページのフィールド」(106ページ)**を参照してください。
4. [パスワード情報]セクションまでスクロールし、[デバイス固有パスワード情報を使用]オプションを選択します。
5. 下にスクロールし、[デバイスアクセス設定を表示]（デバイス固有の設定）をクリックします。
6. [設定]ドロップダウンメニューから[SecurIDを使用]を選択し、値として「*exec*」または「*enable*」と入力します。SecurIDを実行モードで使用する場合は、「*exec*」と入力します。*exec*を使用すると実行モードが有効になります。通常このモードは、デバイスにログインするときの最初のモードです。SecurIDを実行モードと有効モードの両方で使用する場合は、「*enable*」と入力します。
7. このデバイスがSecurIDトークンの特定ユーザプールを使用するように設定するには、[カスタム設定]フィールドに「*securid\_pool\_override*」と入力します。[値]フィールドにユーザ名を入力します。
8. [保存]ボタンをクリックします。

デバイス（またはデバイスグループ）がSecurIDによってアクセスするように構成されており、ソフトウェアシードが入力されている場合、NAは、デバイスにアクセスする必要があるたびに正確な時間制限トークンコードを自動生成します。

RSA SecurID 認証による管理のために、デバイスでネットワークパスワードルールを設定することもできます。詳細については、**「[デバイスパスワードルール]ページのフィールド」(134ページ)**を参照してください。次に、上の4、5、および6の手順に従います。

## SecurID ソフトウェアトークンの追加

SecurID ソフトウェアトークンを追加するには：

1. RSA ソフトウェアトークンアプリケーションを使用して、NA が稼動しているサーバにトークンをインポートします。
2. ホームページの [自分の設定] の下にある [自分のプロフィール] をクリックします。[自分のプロフィール] ページが開きます。[自分のプロフィール] ページのフィールドの詳細については、「[\[自分のプロフィール\] ページのフィールド](#)」(260 ページ) を参照してください。
3. ページ下部の [SecurID] セクションの下で、[ソフトウェアトークンライセンスを管理] へのリンクをクリックします。[SecurID トークンの表示] ページが開きます。このページでは、ユーザのユーザログインに関連付けられたソフトウェアトークンライセンスを表示、追加、または更新できます。デバイスが SecurID 資格情報を要求するように構成されている場合には、それらのライセンスを使用してデバイスにログインします。
4. [トークンを追加] リンクをクリックします。[SecurID トークンの新規作成] ページが開きます。このページでは、ユーザあたり 1 つのソフトウェアトークンまたは一般使用ソフトウェアトークンのプールを追加できます。

**注意：** [管理] の下の [ユーザ] オプションをクリックして、そのユーザの [編集] オプションをクリックすることにより、[ソフトウェアトークンライセンスの管理] リンクにナビゲートすることもできます。

### [SecurID トークンの新規作成] ページ

フィールド	説明/アクション
SecurID ユーザ	ACE/Server のトークンに割り当てられているユーザ名を入力します。
ソフトウェアトークンのシリアル番号	トークンのシリアル番号を入力します（ゼロで埋める）。
PIN	ACE/Server でトークン発行時に PIN を構成する場合は、ここに入力します。（ <b>注意：</b> PIN が更新された場合、ここでも更新する必要があります。）
PIN を確認	確認のため PIN を再入力します。
パスワード	ACE/Server で発行されるときに、パスワードが構成される場合は、ここに入力します。

入力が完了したら、必ず [保存] をクリックします。

## SecurIDを使用したログイン

RSA SecurIDは、外部認証メカニズムとして指定できます。詳細については、「[\[ユーザ認証\]ページのフィールド](#)」(77ページ)を参照してください。

RSA SecurID ACE サーバからNAサーバに、`sdconf.rec` ファイルをインストールする必要があります(例: `C:\WINDOWS\SYSTEM32\sdconf.rec`)。このファイルには、NAがSecurIDにアクセスする場合に必要な接続情報が記述されています。

**注意：**Linux、またはSolarisプラットフォームの場合、NAはデフォルトで`/var/ace`ディレクトリ内の`sdconf.rec`ファイルを検索します。このファイルには、NAがSecurIDにアクセスする場合に必要な接続情報が記述されています。

インストールが完了したら、NA マネージメントエンジンを再起動する必要があります。NA 管理エンジンの再起動の詳細については、「[サービスの開始および停止](#)」(94ページ)を参照してください。

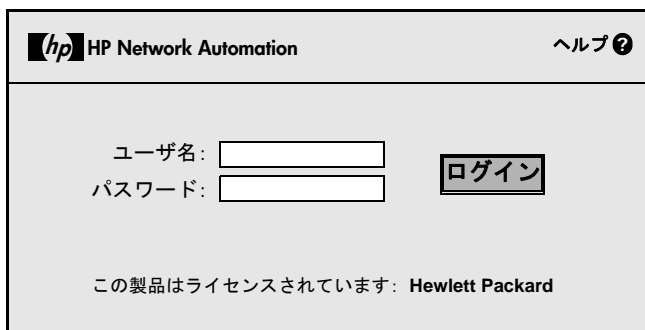
トークンが新規PINモードの場合は、SecurIDを介して次の2つの方法でNAにログインできます。

- SecurID システムPINを使用する
- 新規SecurID PINを使用する

RSAのログイン手順では、すべての場合に、ユーザが新規PINで再認証する必要があります。

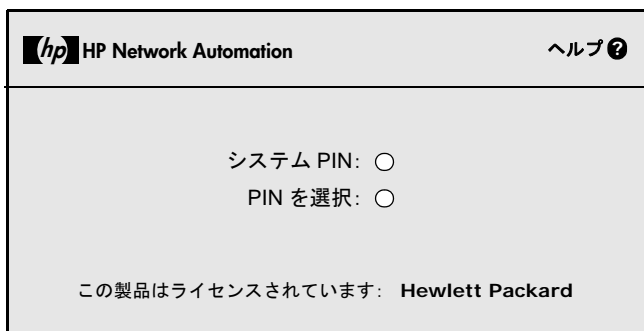
NA ログインプロンプト(下の図)で、次の手順に従います。

1. NAユーザ名を入力します。
2. [パスワード]フィールドにパスコードを入力します。
3. [ログイン]をクリックします。



The screenshot shows the HP Network Automation login interface. At the top, there is a header with the HP logo and 'HP Network Automation' on the left, and a 'ヘルプ ?' (Help ?) link on the right. The main area contains two input fields: 'ユーザ名:' (Username:) and 'パスワード:' (Password:). To the right of the password field is a button labeled 'ログイン' (Login). Below the input fields, there is a line of text: 'この製品はライセンスされています: Hewlett Packard'.

ご使用のSecurIDシステムが、システムPINまたは新規PINを使用するように構成されている場合は、次のページが開きます。



The screenshot shows the HP Network Automation system PIN selection interface. At the top, there is a header with the HP logo and 'HP Network Automation' on the left, and a 'ヘルプ ?' (Help ?) link on the right. The main area contains two radio buttons: 'システム PIN: ○' (System PIN: ○) and 'PIN を選択: ○' (Select PIN: ○). Below the radio buttons, there is a line of text: 'この製品はライセンスされています: Hewlett Packard'.

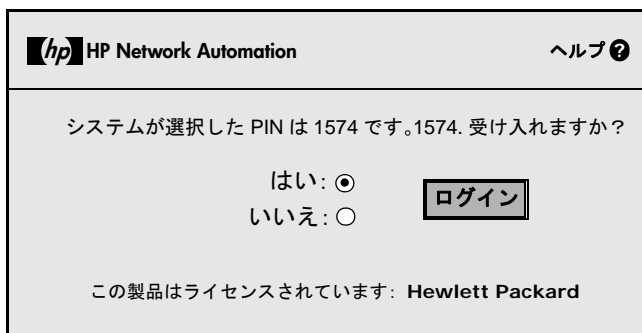
[システムPIN]をクリックする場合は、「**ログイン方法1：システムPINの使用**」(632 ページ)を参照してください。[PINを選択]をクリックする場合は、「**ログイン方法2：新しいPINの使用**」(632 ページ)を参照してください。

**注意：** ご使用の SecurID システムが、システムPINまたは新規PINを指定するように構成されていない場合は、SecurID システム設定に応じて、「ログイン方法1」または「ログイン方法2」を参照してください。

## ログイン方法1：システムPINの使用

ログインページで次の手順に従います。

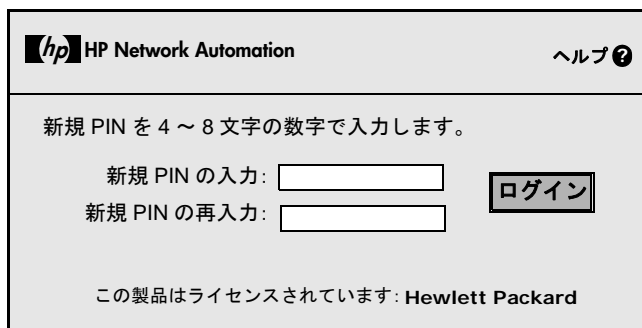
1. [システムPIN]をクリックします。SecurIDからシステムPINを獲得した後、次に示すように[はい]をクリックします。
2. [ログイン]をクリックします。
3. 待機して、次のトークンコードを使用してログインするよう指示するメッセージが表示されます。



## ログイン方法2：新しいPINの使用

ログインページで次の手順に従います。

1. [PINを選択]をクリックします。
2. 次の図に示すように、新規PINを2回入力します。
3. [ログイン]をクリックします。PINパラメータに適合するかどうかについて、PINの確認が行われます。





## SecurIDのトラブルシューティング

I. SecurIDを使用してNAにログインできない場合は、RSA管理者にお問い合わせください。

II. デバイスアクセスでSecurIDを使用する場合は、変更の検出で[syslogユーザの特定]オプションをオフにすることをお勧めします。このオプションをオフにしないと、[スナップショットタスクの失敗]メッセージが表示されることがあります。

1. [管理]の下メニューバーで[システム管理設定]を選択し、[構成管理]をクリックします。[構成管理]ページが開きます。
2. [ユーザIDの変更]セクションの[syslogユーザの特定]で、[可能な場合、syslogメッセージテキストから構成を変更したユーザを特定します。]チェックボックスをオフにします。
3. [ユーザIDの変更]セクションの[syslogからユーザを自動作成]で、[syslogから認証された変更の実行者が存在しない場合、HP Network Automationの新規ユーザを作成します（ユーザを自動作成を有効にする必要があります）。]チェックボックスをオフにします。
4. [保存]ボタンをクリックします。

III. 外部認証に失敗すると、NAは、次の場合にローカルユーザ資格情報へのフォールバックを試みます。

- 外部認証サービスが停止したりアクセス不能になったりした場合。
- 外部認証方法で一度も正常にログインしたことのない静的ユーザアカウントの場合。
- 組み込み管理ユーザアカウントの場合。

IV. RSA ACE/AgentクライアントとRSA ACE/Serverの間の通信では、ノードシークレットファイルを使用して認証を行います。ACE/Server ログファイルに次の種類のメッセージが記録されている場合は、NA サーバのノードシークレットファイルを更新する必要があります。

```
07/12/2006 22:00:19U -----/core15.hp.com ----->/
07/12/2006 18:00:19L Node verification failed      NArsa.rduNA.HP.com
```

ノードシークレットを作成するには：

1. [エージェントホスト] → [エージェントホストの追加（または編集）]をクリックします。
2. [ノードシークレットを作成]をクリックします。
3. [パスワード]ボックスにパスワードを入力し、[パスワードの確認]ボックスにパスワードをもう一度入力します。
4. デフォルトの名前とディレクトリでノードシークレットファイルを保存する場合は、[OK] をクリックします。デフォルトの名前 *nodesecret.rec* を使用して、デフォルトのディレクトリにノードシークレットファイルが作成されます。デフォルトのディレクトリは、別のディレクトリを指定するまで ACEPROG のままです。その場合、指定するディレクトリは、Database Administration アプリケーションが再起動されるまでデフォルトのディレクトリになります。別の名前とディレクトリでファイルを作成する場合は、[参照] をクリックします。[ノードシークレットファイル名の指定]ダイアログボックスで名前とディレクトリを変更して、[保存] をクリックします。

**注意：** 指定したディレクトリに同じ名前のノードシークレットファイルが存在する場合は、[はい] をクリックして上書きするか、[いいえ] をクリックして [ノードシークレットファイル名の指定] ダイアログボックス

に戻ります。[はい]をクリックすると、指定した名前とディレクトリを使用してノードシークレットファイルが作成されます。

[エージェントホストの追加（または編集）]ダイアログボックスの[ノードシークレットファイルの作成]ボタンが無効になります。作成したノードシークレットを選択します。

5. [OK]をクリックします。
6. 新しいノードシークレットファイルをエージェントホストにコピーします。
7. ロードノードシークレットユーティリティ (*agent\_nsload*) をRSA Authentication Managerメディアからエージェントホストにコピーします。エージェントホストのオペレーティングシステムに対して適切な *agent\_nsload* プロセスをコピーしてください。
8. エージェントホストでロードノードシークレットユーティリティを実行し、新しいノードシークレットファイルをロードします。コマンドラインプロンプトで、「*agent\_nsload -f path -p password*」と入力します（*path*はノードシークレットファイルのディレクトリと名前、*password*はノードシークレットファイルを保護するパスワードです）。

**注意：**ACE/ServerがNAサーバと異なるプラットフォームにある場合は、*agent\_nsload*実行可能ファイルに互換性がない可能性があります。この場合は、RSAに連絡して正しいバイナリを入手してください。また、NAサーバを再起動して、RSA dllが新しいノードシークレットファイルの場所を認識できるようにする必要もあります。

## 第18章：コンプライアンスセンター

### トピックの参照先リスト

トピック	参照先：
はじめに	<a href="#">「はじめに」</a> （636ページ）
COBIT 準拠のステータスレポート	<a href="#">「COBIT 準拠のステータスレポート」</a> （638ページ）
COSO 準拠のステータスレポート	<a href="#">「COSO 準拠のステータスレポート」</a> （646ページ）
ITIL 準拠のステータスレポート	<a href="#">「ITIL 準拠のステータスレポート」</a> （649ページ）
GLBA 準拠のステータスレポート	<a href="#">「GLBA 準拠のステータスレポート」</a> （652ページ）
HIPAA 準拠のステータスレポート	<a href="#">「HIPAA 準拠のステータスレポート」</a> （655ページ）
PCI データセキュリティ標準準拠のステータスレポート	<a href="#">「PCI データセキュリティ標準準拠のステータスレポート」</a> （662ページ）

**注意：** コンプライアンスセンターは、公表されているルールと標準に関するHPの認識に基づいています。HPは監査人でも監督当局でもありません。したがって、導入に際しては、自社の監査役または法務担当の指示を仰ぐことをお勧めします。

## はじめに

コンプライアンスセンターは、Sarbanes-Oxley 法（セクション404）および対応する内部統制フレームワークに対するネットワークインフラストラクチャの現在の準拠のステータスを判断するときに材料となるレポート、および情報にアクセスする際の入り口となるNAのポータルサイトです。

Public Company Accounting Reform and Investor Protection Act（2002年）は一般に Sarbanes-Oxley 法（サーベンスオクスリー法）と呼ばれ、会社が投資家に情報公開する際の精度と信頼性を高めることを目的として作成されています。一般的に Sarbanes-Oxley 法は、米国証券取引委員会（SEC）に上場しているか、SECに財務報告書の提出が必要な米国の全企業に適用されます。この法律では、財務報告書を提出する企業のCEOとCFOに対し、その報告書に偽りが無いことを保証するようデフォルトしています。

Sarbanes-Oxley 法の重要な条項はセクション404で、特に財務報告書に関する内部統制についてデフォルトしています。セクション404では、財務報告書を提出する企業に対し、その報告書の一部として、内部統制に関する報告と評価を含めることを義務付けています。Sarbanes-Oxley 法（セクション404）ではIT関連の準拠努力についての具体的な統制要件を定めていないため、組織は、COSO、COBIT、ITIL、またはPCI データセキュリティ標準などの内部統制フレームワークを選択するとともに、そのフレームワークを実施して報告する必要があります。NAを使用して Sarbanes-Oxley 法（セクション404）に準拠する方法の詳細については、コンプライアンスセンターのホームページにあるオンライン情報を参照してください。

コンプライアンスセンターのホームページにアクセスするには、[レポート]メニューバーで[コンプライアンスセンター]をクリックします。コンプライアンスセンターのホームページが開きます。

## コンプライアンスセンターのホームページ

オプション	説明/アクション
Sarbanes-Oxley（セクション404）	Sarbanes-Oxley法（セクション404）の準拠のステータスの概要を開きます。
COBIT 準拠のステータス	COBIT 準拠のステータスレポートを開きます。詳細については、「 <a href="#">COBIT 準拠のステータスレポート</a> 」（638 ページ）を参照してください。
COSO 準拠のステータス	COSO 準拠のステータスレポートを開きます。詳細については、「 <a href="#">COSO 準拠のステータスレポート</a> 」（646 ページ）を参照してください。
ITIL 準拠のステータス	ITIL 準拠のステータスレポートを開きます。詳細については、「 <a href="#">ITIL 準拠のステータスレポート</a> 」（649 ページ）を参照してください。
GLBA 準拠のステータス	GLBA 準拠のステータスレポートを開きます。詳細については、「 <a href="#">GLBA 準拠のステータスレポート</a> 」（652 ページ）を参照してください。
HIPAA 準拠のステータス	HIPAA 準拠のステータスレポートを開きます。詳細については、「 <a href="#">HIPAA 準拠のステータスレポート</a> 」（655 ページ）を参照してください。
[PCI データセキュリティ標準準拠のステータス]リンク	PCI データセキュリティ標準準拠のステータスレポートを開きます。詳細については、「 <a href="#">PCI データセキュリティ標準準拠のステータスレポート</a> 」（662 ページ）を参照してください。

## COBIT 準拠のステータスレポート

COBIT (Control Objectives for Information and related Technology) は、IT とそのプロセスにおけるリスクと収益のバランスを取りながら、事業のリスク、制御の必要性、および技術的な問題の間のギャップを埋めることにより、管理の必要を満たすことに貢献する内部統制フレームワークです。

NA は、COBIT で定義される次の 4 つの分野の働きを強化し、効果的な内部統制システムを実現します。

- **モニタリング** : NA は、プロセスの監視、内部制御の妥当性の評価、単独の保証の取得、および単独の監査の提供を行います。
- **サービス提供とサポート** : NA により、サービスレベル、サードパーティサービス、およびパフォーマンスとキャパシティの管理、継続的なサービスの確保とシステムセキュリティの確保、コストの特定と割り当て、ユーザの教育とトレーニング、ユーザへの支援とアドバイス、および構成、データ、設備、運用の管理を行うことができます。
- **計画と組織** : NA により、戦略的 IT 計画の定義付け、技術的な方針の決定、IT 投資と人的リソースの管理、管理目的および方針の伝達、および外部的な要件への確実な準拠を支援します。
- **調達と導入** : NA により、自動化ソリューションの特定、技術インフラストラクチャの調達と保守、手順の構築と保守、システムのインストールと認可、および変更の管理を支援します。

COBIT および NA による COBIT の実装の強化方法の詳細については、[COBIT 準拠のステータス] ページの [COBIT および HP Network Automation を使用した遵法実現に関する詳細情報] リンクをクリックしてください。

COBIT 準拠のステータスレポートを表示するには :

1. [レポート] のメニューバーで、[コンプライアンスセンター] をクリックします。コンプライアンスセンターのホームページが開きます。
2. [COBIT 準拠のステータス] リンクをクリックします。[COBIT 準拠のステータス] ページが開きます。

## [COBIT 準拠のステータス] ページのフィールド

フィールド	説明/アクション
<b>モニタリング</b>	
M1 プロセスのモニタリング	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• スタートアップとランニング構成が異なるデバイス。[デバイスリスト]リンクをクリックするとデバイス検索結果レポートが開きます。</li> <li>• 非アクティブなデバイス。[非アクティブのデバイス]リンクをクリックすると、デバイス検索結果ページが開きます。</li> <li>• ACL。[全ACL]リンクをクリックすると、ACL 検索結果ページが開きます。</li> <li>• 使用中のACL。[使用中のACL]リンクをクリックすると、ACL 検索結果ページが開きます。</li> <li>• 過去7日間のACLの変更。[ACL変更]リンクをクリックすると、ACL 検索結果ページが開きます。</li> <li>• 過去7日間に承認された変更。[承認された変更]リンクをクリックすると、承認された変更検索結果ページが開きます。</li> </ul>
M2 内部統制の妥当性を評価	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 適用されているワークフロールール。[ワークフロー設定]リンクをクリックすると、ワークフローウィザードが開きます。</li> <li>• 適用されている構成ポリシー。[ポリシー]リンクをクリックすると、[ポリシー]ページが開きます。</li> <li>• 過去7日間に承認されなかった変更。[未承認の変更]リンクをクリックすると、[未承認の変更検索結果]ページが開きます。</li> </ul>
M3 第三者保証を取得	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 「OK」ステータスを示す監視。[システムステータス]リンクをクリックすると、システムステータスレポートが開きます。</li> <li>• ソフトウェアレベルのデバイス。[ソフトウェアの脆弱性レポート]リンクをクリックすると、ソフトウェアの脆弱性レポートが開きます。</li> <li>• 過去24時間の構成ポリシーに非準拠のイベント。[ポリシーイベント (24時間)]リンクをクリックすると、[ポリシーアクティビティ]ページが開きます。</li> <li>• 過去7日間の構成ポリシーに非準拠のイベント。[ポリシーイベント (7日間)]リンクをクリックすると、[ポリシーアクティビティ]ページが開きます。</li> <li>• 緑のステータス（しきい値内）の構成管理「ベストプラクティス」。[ネットワークステータスレポート]リンクをクリックすると、ネットワークステータスレポートが開きます。</li> </ul>
M4 独立監査に提供	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• アクセス可能なユーザレポート。[ユーザレポートとシステムレポート]リンクをクリックすると、[ユーザレポートとシステムレポート]ページが開きます。</li> <li>• アクセス可能なシステムレポート。[ユーザレポートとシステムレポート]リンクをクリックすると、[ユーザレポートとシステムレポート]ページが開きます。</li> </ul>

フィールド	説明/アクション
<b>提供とサポート</b>	
DS1 サービスレベルの定義と管理	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 緑のステータス（しきい値内）の構成管理「ベストプラクティス」。<a href="#">[ネットワークステータスレポート]</a>リンクをクリックすると、ネットワークステータスレポートが開きます。</li> <li>• 1日あたりの平均変更（過去7日間）。<a href="#">[サマリレポート]</a>リンクをクリックすると、サマリレポートが開きます。</li> <li>• 1日あたりの平均変更（過去30日間）。<a href="#">[サマリレポート]</a>リンクをクリックすると、サマリレポートが開きます。</li> </ul>
DS2 サードパーティのサービスの管理	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• アクセスエラーがあるデバイス。<a href="#">[アクセス不能なデバイス]</a>リンクをクリックすると、デバイス検索結果ページが開きます。</li> <li>• スタートアップとランニング構成が異なるデバイス。<a href="#">[デバイスリスト]</a>リンクをクリックすると、デバイス検索結果ページが開きます。</li> <li>• 非アクティブなデバイス。<a href="#">[非アクティブのデバイス]</a>リンクをクリックすると、デバイス検索結果ページが開きます。</li> </ul>
DS3 性能とキャパシティの管理	<p>利用できるポート数が10%未満のデバイス数を表示します。<a href="#">[ポートの可用性]</a>リンクをクリックすると、デバイス検索結果ページが開きます。</p>
DS4 継続的なサービスの保証	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 最後の24時間の診断実行。<a href="#">[診断（24時間）]</a>リンクをクリックすると、診断検索結果ページが開きます。</li> <li>• 最後の7日間の診断実行。<a href="#">[診断（7日間）]</a>リンクをクリックすると、診断検索結果ページが開きます。</li> </ul>
DS5 システムセキュリティの保証	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 特定のデバイス群に制限されたユーザ。<a href="#">[ユーザリスト]</a>リンクをクリックすると、ユーザ検索結果ページが開きます。</li> <li>• 管理者アクセス権限が割り当てられたユーザ。<a href="#">[ユーザリスト]</a>リンクをクリックすると、<a href="#">[全ユーザ]</a>ページが開きます。</li> <li>• 適用されているデバイスパスワードルール。<a href="#">[デバイスパスワードルール]</a>リンクをクリックすると、<a href="#">[デバイスパスワードルール]</a>ページが開きます。</li> <li>• ACL。<a href="#">[全ACL]</a>リンクをクリックすると、ACL検索結果ページが開きます。</li> <li>• 使用中のACL。<a href="#">[使用中のACL]</a>リンクをクリックすると、ACL検索結果ページが開きます。</li> <li>• 過去7日間のACLの変更。<a href="#">[ACL変更]</a>リンクをクリックすると、ACL検索結果ページが開きます。</li> </ul>
DS6 費用の捕捉と配賦	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• インベントリ内のデバイス。<a href="#">[デバイスリスト]</a>リンクをクリックすると、<a href="#">[インベントリ]</a>ページが開きます。</li> <li>• インベントリ内のモジュール。<a href="#">[モジュール]</a>リンクをクリックすると、<a href="#">[モジュールの検索結果]</a>ページが開きます。</li> </ul>



フィールド	説明/アクション
DS7 利用者の教育と研修	<p>次の文書へのリンクがあります。</p> <ul style="list-style-type: none"> <li>• 『NA ユーザガイド』</li> <li>• 『NA Release Notes』</li> </ul>
DS8 顧客への支援と助言	<p>次の項目へのリンクがあります。</p> <ul style="list-style-type: none"> <li>• ドライバ更新パッケージのダウンロード</li> <li>• 最新のリリースノートを表示</li> <li>• ライセンス情報を表示</li> <li>• 技術サポートチケットを作成</li> <li>• 顧客サポートに連絡</li> </ul>
DS9 構成管理	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 過去7日間に検出された構成変更。[構成変更]リンクをクリックすると、構成検索結果ページが開きます。</li> <li>• 保存されたデバイスの構成。[アクティブな構成]リンクをクリックすると、構成検索結果ページが開きます。</li> <li>• 承認保留中の変更。[承認保留中の変更]リンクをクリックすると、保留中の変更検索結果ページが開きます。</li> <li>• 過去7日間に承認された変更。[承認された変更]リンクをクリックすると、承認された変更検索結果ページが開きます。</li> <li>• 過去7日間に承認されなかった変更。[未承認の変更]リンクをクリックすると、[未承認の変更検索結果]ページが開きます。</li> </ul>
DS10 問題管理とインシデント管理	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 過去24時間に検出された構成変更。[イベントリスト]リンクをクリックすると、[システム/ネットワークイベント]ページが開きます。</li> <li>• 過去24時間に発生したNAイベント。[イベントリスト]リンクをクリックすると、[システム/ネットワークイベント]ページが開きます。</li> </ul>
DS11 データ管理	<p>保存されたデバイスの構成の数を表示します。</p>
DS12 物理的環境の管理	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• インベントリ内のデバイス。[デバイスリスト]リンクをクリックすると、[インベントリ]ページが開きます。</li> <li>• インベントリ内のモジュール。[モジュール]リンクをクリックすると、モジュール検索結果ページが開きます。</li> </ul>

フィールド	説明/アクション
DS13 オペレーション管理	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 24時間以内に予定されているデバイスの変更タスク。[保留タスク（24時間）]リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>• 7日以内に予定されているデバイスの変更タスク。[保留タスク（7日間）]リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>• 24時間以内に予定されているソフトウェア配布。[保留中の配布（24時間）]リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>• 7日以内に予定されているソフトウェア配布。[保留中の配布（7日間）]リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>• 承認保留中の変更。[承認保留中の変更]リンクをクリックすると、保留中の変更検索結果ページが開きます。</li> </ul>
<b>計画と組織</b>	
PO1 IT戦略計画の策定	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• インベントリ内のデバイス。[デバイスリスト]リンクをクリックすると、[インベントリ]ページが開きます。</li> <li>• インベントリ内のモジュール。[モジュール]リンクをクリックすると、[モジュール検索結果]ページが開きます。</li> <li>• 利用できるポート数が10%未満のデバイス数を表示します。[ポートの可用性]リンクをクリックすると、デバイス検索結果ページが開きます。</li> </ul>
PO2 情報アーキテクチャの定義	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• インベントリ内のデバイス。[デバイスリスト]リンクをクリックすると、[インベントリ]ページが開きます。</li> <li>• インベントリ内のモジュール。[モジュール]リンクをクリックすると、[モジュール検索結果]ページが開きます。</li> <li>• 保存されたデバイスの構成。[アクティブな構成]リンクをクリックすると、構成検索結果ページが開きます。</li> </ul>
PO3 技術指針の決定	<p>ベンダーの合計数から、インベントリ内のデバイス数を表示します。[ベンダー別デバイスリスト]リンクをクリックすると、[インベントリ]ページが開きます。</p>
PO4 ITプロセスと組織およびそのかわりの定義	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 特定のデバイス群に制限されたユーザ。[ユーザリスト]リンクをクリックすると、[全ユーザ]ページが開きます。</li> <li>• 管理者アクセス権限を割り当てられたユーザ。[ユーザリスト]リンクをクリックすると、[全ユーザ]ページが開きます。</li> <li>• 適用されているデバイスパスワードルール。[デバイスパスワードルール]リンクをクリックすると、[デバイスパスワードルール]ページが開きます。</li> </ul>
PO5 IT投資の管理	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• インベントリ内のデバイス。[デバイスリスト]リンクをクリックすると、[インベントリ]ページが開きます。</li> <li>• インベントリ内のモジュール。[モジュール]リンクをクリックすると、[モジュール検索結果]ページが開きます。</li> <li>• デバイスがアクティブではありません。[デバイスリスト]リンクをクリックすると、[インベントリ]ページが開きます。</li> </ul>

フィールド	説明/アクション
PO6 マネジメントの意図と指針の周知	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>緑のステータス（しきい値内）の構成管理「ベストプラクティス」。<a href="#">[ネットワークステータスレポート]</a>リンクをクリックすると、ネットワークステータスレポートが開きます。</li> <li>アクティブな構成ポリシー。<a href="#">[ポリシー]</a>リンクをクリックすると、<a href="#">[ポリシー]</a>ページが開きます。</li> </ul>
PO7 人材の管理	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>特定のデバイス群に制限されたユーザ。<a href="#">[ユーザリスト]</a>リンクをクリックすると、ユーザ検索結果ページが開きます。</li> <li>管理者アクセス権限が割り当てられたユーザ。<a href="#">[ユーザリスト]</a>リンクをクリックすると、ユーザ検索結果ページが開きます。</li> <li>適用されているデバイスパスワードルール。<a href="#">[デバイスパスワードルール]</a>リンクをクリックすると、<a href="#">[デバイスパスワードルール]</a>ページが開きます。</li> </ul>
PO8 外部要件との準拠の管理	<p>アクティブな構成ポリシーの数を表示します。<a href="#">[ポリシー]</a>リンクをクリックすると、<a href="#">[ポリシー]</a>ページが開きます。<a href="#">[コンプライアンスセンター]</a>リンクをクリックすると、コンプライアンスセンターのホームページが開きます。</p>
PO9 リスクの評価	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>緑のステータス（しきい値内）の構成管理「ベストプラクティス」。<a href="#">[ネットワークステータスレポート]</a>リンクをクリックすると、ネットワークステータスレポートが開きます。</li> <li>アクセスエラーがあるデバイス。<a href="#">[アクセス不能なデバイス]</a>リンクをクリックすると、デバイス検索結果ページが開きます。</li> <li>利用できるポート数が10%未満のデバイス数を表示します。<a href="#">[ポートの可用性]</a>リンクをクリックすると、デバイス検索結果ページが開きます。</li> </ul>
PO10 プロジェクトの管理	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>24時間以内に予定されているデバイスの変更タスク。<a href="#">[保留タスク（24時間）]</a>リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>7日以内に予定されているデバイスの変更タスク。<a href="#">[保留タスク（7日間）]</a>リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>24時間以内に予定されているソフトウェア配布。<a href="#">[保留中の配布（24時間）]</a>リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>7日以内に予定されているソフトウェア配布。<a href="#">[保留中の配布（7日間）]</a>リンクをクリックすると、タスク検索結果ページが開きます。</li> </ul>
PO11 品質管理	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>「OK」ステータスを示す監視。<a href="#">[システムステータス]</a>リンクをクリックすると、システムステータスレポートが開きます。</li> <li>ソフトウェア準拠のデバイス。<a href="#">[デバイスソフトウェアレポート]</a>リンクをクリックすると、<a href="#">[ソフトウェア準拠検索結果]</a>ページが開きます。</li> <li>過去24時間の構成ポリシーに非準拠のイベント。<a href="#">[ポリシーイベント（24時間）]</a>リンクをクリックすると、<a href="#">[ポリシーアクティビティ]</a>ページが開きます。</li> <li>過去7日間の構成ポリシーに非準拠のイベント。<a href="#">[ポリシーイベント（7日間）]</a>リンクをクリックすると、<a href="#">[ポリシーアクティビティ]</a>ページが開きます。</li> <li>緑のステータス（しきい値内）の構成管理「ベストプラクティス」。<a href="#">[ネットワークステータスレポート]</a>リンクをクリックすると、ネットワークステータスレポートが開きます。</li> </ul>

## 調達と導入

フィールド	説明/アクション
AI1 自動ソリューションを特定	<p>次のデフォルトのリンクがあります。</p> <ul style="list-style-type: none"> <li>• 週次で実行されるデータベースを整理するシステムタスク。[保留タスク]リンクをクリックすると、[予定タスク]ページが開きます。</li> <li>• 週次で実行されるモジュールインベントリデータを収集するシステムタスク。[保留タスク]リンクをクリックすると、[予定タスク]ページが開きます。</li> <li>• 日次で実行されるサマリレポートを更新するシステムタスク。[保留タスク]リンクをクリックすると、[予定タスク]ページが開きます。</li> <li>• 日次で実行されるデバイスの構成の変更をポーリングするシステムタスク。[保留タスク]リンクをクリックすると、[予定タスク]ページが開きます。</li> </ul>
AI2 アプリケーションソフトウェアの調達と保守	このフィールドは該当しません。
AI3 技術インフラストラクチャの調達と保守	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• インベントリ内のデバイス。[デバイスリスト]リンクをクリックすると、[インベントリ]ページが開きます。</li> <li>• インベントリ内のモジュール。[モジュール]リンクをクリックすると、[モジュール検索結果]ページが開きます。</li> <li>• 保存されたデバイスの構成。[アクティブな構成]リンクをクリックすると、構成検索結果ページが開きます。</li> </ul>
AI4 手順を作成して保守	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 緑のステータス（しきい値内）の構成管理「ベストプラクティス」。[ネットワークステータスレポート]リンクをクリックすると、ネットワークステータスレポートが開きます。</li> <li>• アクティブな構成ポリシー。[ポリシー]リンクをクリックすると、[ポリシー]ページが開きます。</li> </ul>
AI5 システムのインストールと認可	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 「OK」ステータスを示す監視。[システムステータス]リンクをクリックすると、システムステータスレポートが開きます。</li> <li>• デバイスソフトウェア準拠。[ソフトウェアの脆弱性レポート]リンクをクリックすると、ソフトウェアの脆弱性レポートが開きます。</li> <li>• 緑のステータス（しきい値内）の構成管理「ベストプラクティス」。[ネットワークステータスレポート]リンクをクリックすると、ネットワークステータスレポートが開きます。</li> </ul>

フィールド	説明/アクション
AI6 変更管理	<p data-bbox="444 243 773 264">次の点についての数を表示します。</p> <ul data-bbox="444 285 1466 684" style="list-style-type: none"><li data-bbox="444 285 1466 338">• 過去7日間のTelnet/SSHプロキシセッション。[セッション]リンクをクリックすると、セッション検索結果ページが開きます。</li><li data-bbox="444 359 1466 411">• 過去7日間に予定されたデバイス変更タスク。[過去のタスク（7日間）]リンクをクリックすると、タスク検索結果ページが開きます。</li><li data-bbox="444 432 1466 485">• 7日以内に予定されているデバイスの変更タスク。[保留タスク（7日間）]リンクをクリックすると、タスク検索結果ページが開きます。</li><li data-bbox="444 506 1466 537">• 承認保留中の変更。[承認保留中の変更]リンクをクリックすると、保留中の変更検索結果ページが開きます。</li><li data-bbox="444 558 1466 611">• 過去7日間に承認された変更。[承認された変更]リンクをクリックすると、承認された変更検索結果ページが開きます。</li><li data-bbox="444 632 1466 684">• 過去7日間に承認されなかった変更。[未承認の変更]リンクをクリックすると、[未承認の変更検索結果]ページが開きます。</li></ul>

## COSO 準拠のステータスレポート

1992年、Committee of Sponsoring Organizations of the Treadway Commission (COSO) は内部統制に関して画期的なレポートを発表しました。*Internal Control-Integrated Framework*は、"COSO"と呼ばれることも多く、内部統制システムを確立してその効果性を判断する際の基準となっています。

NAでは、次の5つの基本要素によって効果的な内部統制システムを実現します。

- 統制環境：基本的な規律と構成を実現することで、内部統制システムの基礎を確立します。
- リスク評価：目的の達成に関連するリスクについての管理者による特定と解析が含まれます。
- 統制活動：確実に管理目的が達成され、リスク緩和戦略が実行されるようにします。
- 情報および伝達：統制の責務を従業員に伝え、その職責の遂行を可能にする方法と時間枠で情報を提供することにより、他のすべての統制要素をサポートします。
- モニタリング：管理者または処理の部外者による内部統制の外部からの監督を含みます。

COSOの詳細については、[COSOに関する詳細情報と HP Network Automation を使用した遵法実現に関する詳細情報]リンクをクリックして参照してください。

COSO準拠のステータスレポートを表示するには：

1. [レポート]のメニューバーで、[コンプライアンスセンター]をクリックします。コンプライアンスセンターのホームページが開きます。
2. [COSO準拠のステータス]リンクをクリックします。[COSO準拠のステータス]ページが開きます。

## COSO 準拠のステータスページのフィールド

フィールド	説明/アクション
統制環境	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 特定のデバイス群に制限されたユーザ。[ユーザリスト]リンクをクリックすると、ユーザ検索結果ページが開きます。</li> <li>• 管理者アクセス権限を割り当てられたユーザ。[ユーザリスト]リンクをクリックすると、ユーザ検索結果ページが開きます。</li> <li>• 適用されているデバイスパスワードルール。[デバイスパスワードルール]リンクをクリックすると、[デバイスパスワードルール]ページが開きます。</li> <li>• 適用されている構成ポリシー。[ポリシー]リンクをクリックすると、[ポリシー]ページが開きます。</li> <li>• 適用されているワークフロールール。[ワークフロー設定]リンクをクリックすると、ワークフローウィザードが開きます。</li> <li>• ACL。[全ACL]リンクをクリックすると、ACL検索結果ページが開きます。</li> <li>• 使用中のACL。[使用中のACL]リンクをクリックすると、ACL検索結果ページが開きます。</li> </ul>

フィールド	説明/アクション
リスク評価	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 緑のステータス（しきい値内）の構成管理「ベストプラクティス」。<a href="#">[ネットワークステータスレポート]</a>リンクをクリックすると、ネットワークステータスレポートが開きます。</li> <li>• アクセスエラーがあるデバイス。<a href="#">[アクセス不能なデバイス]</a>リンクをクリックすると、デバイス検索結果ページが開きます。</li> <li>• 利用できるポート数が10%未満のデバイス数を表示します。<a href="#">[ポートの可用性]</a>リンクをクリックすると、デバイス検索結果ページが開きます。</li> </ul>
統制活動	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 過去7日間のTelnet/SSHプロキシセッション。<a href="#">[セッション]</a>リンクをクリックすると、セッション検索結果ページが開きます。</li> <li>• 24時間以内に予定されているデバイスの変更タスク。<a href="#">[保留タスク（24時間）]</a>リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>• 7日以内に予定されているデバイスの変更タスク。<a href="#">[保留タスク（7日間）]</a>リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>• 24時間以内に予定されているソフトウェア配布。<a href="#">[保留中の配布（24時間）]</a>リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>• 7日以内に予定されているソフトウェア配布。<a href="#">[保留中の配布（7日間）]</a>リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>• 承認保留中の変更。<a href="#">[承認保留中の変更]</a>リンクをクリックすると、保留中の変更検索結果ページが開きます。</li> </ul>
情報と伝達	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 過去24時間に検出された構成変更。<a href="#">[ダッシュボード]</a>リンクをクリックすると、ホームページが開きます。</li> <li>• 過去24時間に発生したNAイベント。<a href="#">[ダッシュボード]</a>リンクをクリックすると、ホームページが開きます。</li> <li>• 1日あたりの平均変更数（過去7日間）。<a href="#">[サマリレポート]</a>リンクをクリックすると、サマリレポートが開きます。</li> <li>• 1日あたりの平均変更数（過去30日間）。<a href="#">[サマリレポート]</a>リンクをクリックすると、サマリレポートが開きます。</li> </ul>

フィールド	説明/アクション
モニタリング	<p data-bbox="444 239 773 264">次の点についての数を表示します。</p> <ul data-bbox="444 285 1463 905" style="list-style-type: none"><li data-bbox="444 285 1463 342">• 「OK」ステータスを示す監視。[システムステータス]リンクをクリックすると、システムステータスレポートが開きます。</li><li data-bbox="444 363 1463 420">• デバイスソフトウェア準拠。[デバイスソフトウェアレポート]リンクをクリックすると、[ソフトウェア準拠検索結果]ページが開きます。</li><li data-bbox="444 441 1463 497">• 過去24時間の構成ポリシーに非準拠のイベント。[ポリシーイベント (24時間)]リンクをクリックすると、[ポリシーアクティビティ]ページが開きます。</li><li data-bbox="444 518 1463 575">• 過去7日間の構成ポリシーに非準拠のイベント。[ポリシーイベント (7日間)]リンクをクリックすると、[ポリシーアクティビティ]ページが開きます。</li><li data-bbox="444 596 1463 653">• スタートアップとランニング構成が異なるデバイス。[デバイスリスト]リンクをクリックすると、デバイス検索結果ページが開きます。</li><li data-bbox="444 674 1463 730">• 非アクティブなデバイス。[非アクティブのデバイス]リンクをクリックすると、デバイス検索結果ページが開きます。</li><li data-bbox="444 751 1463 808">• 過去7日間に承認された変更。[承認された変更]リンクをクリックすると、承認された変更検索結果ページが開きます。</li><li data-bbox="444 829 1463 886">• 過去7日間に承認されなかった変更。[未承認の変更]リンクをクリックすると、[未承認の変更検索結果]ページが開きます。</li><li data-bbox="444 907 1463 905">• 過去7日間のACLの変更。[ACL変更]リンクをクリックすると、ACL検索結果ページが開きます。</li></ul>



## ITIL 準拠のステータスレポート

ITIL (IT Infrastructure Library) は、CCTA (現在のOGC : Office of Government Commerce) が英国政府のために開発したもので、IT サービスを提供するときのベストプラクティスの標準として、世界的に採用が急速に進んでいます。ITILには、次の主要な領域があります。

- サービスサポート : IT サービスを効果的に提供できるようにします。
- サービスデリバリー : IT サービスの管理を可能にします。
- セキュリティ管理 : データおよびインフラストラクチャを保護できるようにします。

ITILの詳細については、[ITILに関する詳細情報と HP Network Automation を使用した遵法実現に関する詳細情報] リンクをクリックして参照してください。

ITIL 準拠のステータスレポートを表示するには :

1. [レポート]のメニューバーで、[コンプライアンスセンター]をクリックします。コンプライアンスセンターのホームページが開きます。
2. [ITIL 準拠のステータス]リンクをクリックします。[ITIL 準拠のステータス]ページが開きます。

## ITIL 準拠のステータスページのフィールド

フィールド	説明/アクション
<b>構成管理</b>	
サービスサポートプロセス	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>• 過去7日間に検出された構成変更。[構成変更]リンクをクリックすると、構成検索結果ページが開きます。</li> <li>• 保存されたデバイスの構成。[アクティブな構成]リンクをクリックすると、構成検索結果ページが開きます。</li> </ul>
<b>インシデント管理</b>	
サービスサポートプロセス	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>• 過去24時間に検出された構成変更。[ダッシュボード]リンクをクリックすると、ホームページが開きます。</li> <li>• 過去24時間に発生したNAイベント。[ダッシュボード]リンクをクリックすると、ホームページが開きます。</li> </ul>
<b>問題管理</b>	
サービスサポートプロセス	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>• 緑のステータス (しきい値内) の構成管理「ベストプラクティス」。[ネットワークステータスレポート]リンクをクリックすると、ネットワークステータスレポートが開きます。</li> <li>• アクセスエラーがあるデバイス。[アクセス不能なデバイス]リンクをクリックすると、デバイス検索結果ページが開きます。</li> </ul>

フィールド	説明/アクション
<b>変更管理</b>	
サービスサポートプロセス	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 過去7日間のTelnet/SSHプロキシセッション。[セッション]リンクをクリックすると、セッション検索結果ページが開きます。</li> <li>• 24時間以内に予定されているデバイスの変更タスク。[保留タスク（24時間）]リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>• 7日以内に予定されているデバイスの変更タスク。[保留タスク（7日間）]リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>• 承認保留中の変更。[承認保留中の変更]リンクをクリックすると、保留中の変更検索結果ページが開きます。</li> <li>• 過去7日間に承認された変更。[承認された変更]リンクをクリックすると、承認された変更検索結果ページが開きます。</li> <li>• 過去7日間に承認されなかった変更。[未承認の変更]リンクをクリックすると、[未承認の変更検索結果]ページが開きます。</li> <li>• 適用されている構成ポリシー。[ポリシー]リンクをクリックすると、[ポリシー]ページが開きます。</li> <li>• 適用されているワークフロールール。[ワークフロー設定]ページをクリックすると、ワークフローウィザードが開きます。</li> </ul>
<b>サービスデスク</b>	
サービスサポート機能	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 24時間以内に予定されているデバイスの変更タスク。[保留タスク（24時間）]リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>• 7日以内に予定されているデバイスの変更タスク。[保留タスク（7日間）]リンクをクリックすると、タスク検索結果ページが開きます。</li> </ul>
<b>リリース管理</b>	
サービスサポートプロセス	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 24時間以内に予定されているソフトウェア配布。[保留中の配布（24時間）]リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>• 7日以内に予定されているソフトウェア配布。[保留中の配布（7日間）]リンクをクリックすると、タスク検索結果ページが開きます。</li> <li>• ソフトウェア準拠のデバイス。[デバイスソフトウェアレポート]リンクをクリックすると、[ソフトウェア準拠検索結果]ページが開きます。</li> </ul>
<b>サービスレベル管理</b>	
サービスデリバリプロセス	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 緑のステータス（しきい値内）の構成管理「ベストプラクティス」。[ネットワークステータスレポート]リンクをクリックすると、ネットワークステータスレポートが開きます。</li> <li>• 1日あたりの平均変更（過去7日間）。[サマリレポート]リンクをクリックすると、サマリレポートが開きます。</li> <li>• 1日あたりの平均変更（過去30日間）。[サマリレポート]リンクをクリックすると、サマリレポートが開きます。</li> </ul>

フィールド	説明/アクション
<b>キャパシティ管理</b>	
サービスデリバリプロセス	利用できるポート数が10%未満のデバイス数を表示します。[ポートの可用性]リンクをクリックすると、デバイス検索結果ページが開きます。
<b>ITサービス継続性管理</b>	
サービスデリバリプロセス	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>最後の24時間の診断実行。[診断（24時間）]リンクをクリックすると、診断検索結果ページが開きます。</li> <li>最後の7日間の診断実行。[診断（7日間）]リンクをクリックすると、診断検索結果ページが開きます。</li> </ul>
<b>可用性管理</b>	
サービスデリバリプロセス	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>過去24時間の構成ポリシーに非準拠のイベント。[ポリシーイベント（24時間）]リンクをクリックすると、[ポリシーアクティビティ]ページが開きます。</li> <li>過去7日間の構成ポリシーに非準拠のイベント。[ポリシーイベント（7日間）]リンクをクリックすると、[ポリシーアクティビティ]ページが開きます。</li> </ul>
<b>ITサービス財務管理</b>	
サービスデリバリプロセス	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>「OK」ステータスを示す監視。[システムステータス]リンクをクリックすると、システムステータスレポートが開きます。</li> <li>インベントリ内のデバイス。[デバイスリスト]リンクをクリックすると、[インベントリ]ページが開きます。</li> <li>インベントリ内のモジュール。[モジュール]リンクをクリックすると、[モジュールの検索結果]ページが開きます。</li> </ul>
<b>セキュリティ管理</b>	
サービスデリバリプロセス	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>特定のデバイス群に制限されたユーザ。[ユーザリスト]リンクをクリックすると、[全ユーザ]ページが開きます。</li> <li>管理者アクセス権限が割り当てられたユーザ。[ユーザリスト]リンクをクリックすると、ユーザ検索結果ページが開きます。</li> <li>適用されているデバイスパスワードルール。[デバイスパスワードルール]リンクをクリックすると、[デバイスパスワードルール]ページが開きます。</li> <li>ACL。[全ACL]リンクをクリックすると、ACL検索結果ページが開きます。</li> <li>使用中のACL。[使用中のACL]リンクをクリックすると、ACL検索結果ページが開きます。</li> <li>過去7日間のACLの変更。[ACL変更]リンクをクリックすると、ACL検索結果ページが開きます。</li> </ul>

## GLBA 準拠のステータスレポート

Financial Modernization Act of 1999（1999年金融サービス近代化法）はGramm-Leach-Bliley Act（GLBA）とも呼ばれますが、これには金融機関が管理している消費者の個人的な金融情報を保護するための条項が含まれています。この法律には、次の3つの主要なプライバシー要件があります。

- プリテキスティング条項
- 金融プライバシールール
- セーフガードルール

セーフガード（保護手段）ルールでは、すべての金融機関に対し保護手段の設計、実装、保守を実施し、顧客情報を保護することを要求しています。この保護手段のルールは、自社の顧客から情報を収集する金融機関に適用されるだけでなく、他の金融機関から顧客情報を受け取る信用調査機関などにも適用されます。

GLBAの詳細については、[GLBAに関する詳細情報と HP Network Automation を使用した遵法実現に関する詳細情報]リンクをクリックして参照してください。

GLBA 準拠のステータスレポートを表示するには：

1. [レポート]のメニューバーで、[コンプライアンスセンター]をクリックします。コンプライアンスセンターのホームページが開きます。
2. [GLBA 準拠のステータス]リンクをクリックします。[GLBA 準拠のステータス]ページが開きます。

## GLBA 準拠のステータスページのフィールド

フィールド	説明/アクション
<b>整合性ガイドラインセクション</b>	
II.A. 情報セキュリティ プログラム	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>• インベントリ内のデバイス。</li> <li>• インベントリ内のモジュール。</li> <li>• 保存されたデバイスの構成。</li> </ul>
II.B. 目的	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>• 特定のデバイスグループに制限されたユーザ。</li> <li>• 管理者権限が割り当てられたユーザ。</li> <li>• 過去7日間に失敗したユーザログイン試行。</li> <li>• 承認保留中の変更。</li> <li>• 過去7日間に承認された変更。</li> <li>• 過去7日間に承認されなかった変更。</li> <li>• 特定されたACL。</li> <li>• 使用中のACL。</li> <li>• 過去7日間のACLの変更。</li> </ul>
III.A. 役員会を含む	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>• 使用可能なユーザレポート。</li> <li>• 使用可能なシステムレポート。</li> </ul>
III.B. リスクを評価	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>• 緑のステータスの構成管理「ベストプラクティス」。</li> <li>• デバイスソフトウェアレベル。</li> <li>• 「OK」ステータスを示す監視。</li> <li>• アクセスエラーがあるデバイス。</li> <li>• 利用できるポートが10%未満のデバイス。</li> <li>• スタートアップとランニング構成が異なるデバイス。</li> </ul>
III.C.1. リスクを管理して 制御（ポリシーと手順）	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>• 適用されているワークフロールール。</li> <li>• 適用されている構成ポリシー。</li> <li>• 適用されているデバイスパスワードルール。</li> </ul>
III.C.2. リスクを管理して 制御（トレーニング）	次の文書にアクセスできます。 <ul style="list-style-type: none"> <li>• 『NA ユーザガイド』</li> <li>• 『NA Release Notes』</li> </ul>

フィールド	説明/アクション
III.C.3. リスクを管理して 制御（テスト中）	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>過去24時間の構成ポリシーに非準拠のイベント。</li> <li>過去7日間の構成ポリシーに非準拠のイベント。</li> <li>ソフトウェアレベルにないデバイス。</li> <li>過去の24時間の診断実行。</li> <li>過去の7日間の診断実行。</li> </ul>
III.D. サービスプロバイダ 協定を監視	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>格納された構成。</li> <li>スタートアップとランニング構成が異なるデバイス。</li> <li>アクティブでないデバイス。</li> <li>アクセスエラーがあるデバイス。</li> </ul>
III.E. プログラムを調整	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>先月に追加されたユーザ。</li> <li>先月に追加されたデバイス。</li> <li>先月に追加されたデバイスグループ。</li> <li>先月に格納された構成。</li> </ul>
III.F. 役員会にレポート	<p>次の要素を表示します。</p> <ul style="list-style-type: none"> <li>緑のステータスの構成管理「ベストプラクティス」の個数。</li> <li>システムステータスレポート。</li> <li>サマリレポート。</li> <li>HP Network Automation コンプライアンスセンター。</li> </ul>
III.G. 標準の実装	この要件はNAの対象範囲外です。

## HIPAA 準拠のステータスレポート

HIPAAとは、1996年に施行されたHealth Insurance Portability & Accountability Act（医療保険の携行と責任に関する法律）のことです。最終的なHIPAAセキュリティ規則が、2003年2月20日に公布されました。この最終規則に基づき、規制対象の団体には、米厚生省（HHS）のメディケアプログラム、医療保険の運営または医療サービスの提供に関わるその他の連邦機関、州のメディケイド機関、個人向け医療保険、ヘルスケアプロバイダ、および保護された医療情報（PHI）を電子形式で処理、転送、保存している医療情報センターがあります。

HIPAAの詳細については、[HIPAAOに関する詳細情報と HP Network Automation を使用した遵法実現に関する詳細情報]リンクをクリックして参照してください。

HIPAA 準拠のステータスレポートを表示するには：

1. [レポート]のメニューバーで、[コンプライアンスセンター]をクリックします。コンプライアンスセンターのホームページが開きます。
2. [HIPAA 準拠のステータス]リンクをクリックします。[HIPAA 準拠のステータス]ページが開きます。

## HIPAA 準拠のステータスページのフィールド

フィールド	説明/アクション
<b>セキュリティ標準：一般ルール</b>	
(1) 対象団体が作成、受信、維持、送信を行う電子保護医療情報すべての機密性、整合性、可用性を確保します。	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>• 保存されたデバイスの構成。</li> <li>• アクセスエラーがあるデバイス。</li> <li>• 利用できるポートが10%未満のデバイス。</li> </ul>
(2) このような情報のセキュリティや整合性に対して予想される脅威や危険性から保護します。	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>• 過去7日間に失敗したユーザログイン試行。</li> <li>• 特定されたACL。</li> <li>• 使用中のACL。</li> <li>• 過去7日間のACLの変更。</li> </ul>
(3) この項のEで許可または要求されていない場合、そうした情報の予想される利用または公開から保護します。	次の点についての数を表示します。 <ul style="list-style-type: none"> <li>• 特定のデバイス群に制限されたユーザ。</li> <li>• 管理者アクセス権限が割り当てられたユーザ。</li> </ul>
(4) 従業員がこの項に準拠するように徹底します。	HP Network Automation コンプライアンスセンターにHIPAA 準拠のステータスレポートを開くことができます。

フィールド	説明/アクション
<p><b>管理上の保護手段</b></p> <p>(A) リスク分析（必須）。対象団体が保持する電子保護医療情報の機密性、整合性、可用性に対して考えられるリスクおよび脆弱性を、正確かつ徹底的に評価します。</p> <p>(B) リスク管理（必須）。リスクや脆弱性を、§ 164.306 (a) に準拠する適切なレベルまで抑えることができるように、十分なセキュリティ対策を実施します。</p> <p>(C) 制裁ポリシー（必須）。対象団体のセキュリティポリシーや手順に準拠しない従業員に対して、適切な制裁を適用します。</p> <p>(D) 情報システムの動作確認（必須）。監査ログ、アクセスレポート、セキュリティインシデントの追跡レポートなど、情報システム動作の記録を定期的に確認するための手順を実施します。</p> <p>団体の所属部門が必要とするポリシーと手順を作成および実施する職務を持つセキュリティ担当者を特定します。</p>	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 緑のステータスの構成管理「ベストプラクティス」。</li> <li>• ソフトウェアレベルのデバイス。</li> <li>• 「OK」ステータスを示す監視。</li> <li>• アクセスエラーがあるデバイス。</li> <li>• 利用できるポートが10%未満のデバイス。</li> <li>• 検出されたソフトウェアの脆弱性。</li> <li>• スタートアップとランニング構成が異なるデバイス。</li> </ul> <p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 適用されているワークフロールール。</li> <li>• アクティブな構成ポリシー。</li> <li>• 適用されているデバイスパスワードルール。</li> </ul> <p>この要件はNAの対象範囲外です。</p> <p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 過去7日間のユーザログイン試行。</li> <li>• 過去7日間で追加されたユーザ。</li> <li>• 過去7日間に削除されたユーザ。</li> <li>• 過去7日間に変更されたユーザ権限。</li> <li>• 過去7日間に変更された構成ポリシー。</li> <li>• 過去7日間に追加された構成ポリシー。</li> </ul> <p>この要件はNAの対象範囲外です。</p>
<p><b>従業員のセキュリティ</b></p> <p>(A) 認可および監視（推奨）。電子保護医療情報を扱う従業員、またはそのような情報にアクセス可能な場所にいる従業員を許可または監視する手順を実施します。</p> <p>(B) 従業員離職時の手続き（推奨）。電子保護医療情報に対する従業員のアクセスが適切であるかどうかを判断する手順を実施します。</p>	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 特定のデバイス群に制限されたユーザ。</li> <li>• 過去7日間に承認された変更。</li> <li>• 過去7日間に承認されなかった変更。</li> </ul> <p>管理者アクセス権限が割り当てられたユーザ数を表示します。</p>



フィールド	説明/アクション
<p>(C) 終了手順（推奨）。従業員の離職時、またはこのセクションの段落 (a) (3) (ii) (b) のデフォルトに従って必要とされた場合、電子保護医療情報へのアクセスを停止する手順を実施します。</p>	<p>過去7日間に削除されたユーザ数を表示します。</p>
<p><b>情報アクセス管理</b></p>	
<p>(A) 医療情報センター機能を分離（必須）。医療情報センターが大規模な組織の一部である場合、情報センターは、電子保護医療情報を大規模な組織による不正アクセスから保護するポリシーと手順を実施する必要があります。</p>	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 特定のデバイスグループに制限されたユーザ。</li> <li>• 制限された（非管理者）アクセス権限を割り当てられたユーザ。</li> </ul>
<p>(B) アクセス認可（推奨）。電子保護医療情報に対するアクセス権を付与するポリシーと手順を実施します。たとえば、ワークステーション、トランザクション、プログラム、プロセス、または他のメカニズムへのアクセスを通じたアクセス権です。</p>	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 特定のデバイスグループに制限されたユーザ。</li> <li>• 制限された（非管理者）アクセス権限を割り当てられたユーザ。</li> </ul>
<p>(C) アクセスの確立と変更（推奨）。団体のアクセス認可ポリシーに基づいて、ワークステーション、トランザクション、プログラム、またはプロセスに対するユーザのアクセス権の確立、文書化、確認、および変更を行うポリシーと手順を実施します。</p>	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• HP Network Automation で有効にされたユーザアカウント。</li> <li>• HP Network Automation で無効にされたユーザアカウント。</li> </ul>
<p><b>セキュリティ意識とトレーニング</b></p>	
<p>(A) セキュリティ通知（推奨）。定期的なセキュリティ更新。</p>	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• HP Network Automation で有効にされたユーザアカウント</li> <li>• HP Network Automation で無効にされたユーザアカウント。</li> </ul>
<p>(B) 悪質なソフトウェアからの保護（推奨）。悪意のあるソフトウェアから保護し、検出とレポートを行う手順。</p>	<p>この要件はNAの対象範囲外です。</p>
<p>(C) ログイン監視（推奨）。ログイン試行を監視し、相違をレポートする手順。</p>	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 過去7日間のユーザログイン試行。</li> <li>• 過去7日間に失敗したユーザログイン試行。</li> </ul>
<p>(D) パスワード管理（推奨）。パスワードの作成、変更、保護を行う手順。</p>	<p>過去7日間に変更されたNAパスワードの数を表示します。</p>
<p><b>セキュリティインシデントの手順</b></p>	
<p>応答とレポート作成（必須）。疑わしいセキュリティインシデントまたは既知のセキュリティインシデントを特定して対処します。対象団体に知られているセキュリティインシデントの被害の影響を、業務の遂行が可能なレベルまで緩和します。また、セキュリティインシデントの内容および結果を文書化します。</p>	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 過去7日間のユーザログイン試行。</li> <li>• 過去7日間に失敗したユーザログイン試行。</li> <li>• 過去7日間に検出された構成変更。</li> </ul>

フィールド	説明/アクション
<p><b>緊急時対応計画</b></p> <p>(A) データバックアップ計画(必須)。取得可能な電子保護医療情報の複製を作成、維持するための手順を確立し、実施します。</p> <p>(B) 災害復旧計画(必須)。データ損失を回復する手順を確立します(また、必要に応じて実施します)。</p> <p>(C) 緊急モード運用計画(必須)。緊急モード時の運用でも、電子保護医療情報のセキュリティを保護するために、重要な業務プロセスを継続できる手順を確立します(また、必要に応じて実施します)。</p> <p>(D) テストと改版の手順(推奨)。緊急時対応計画を定期的にテストし、改版する手順を実施します。</p> <p>(E) アプリケーションとデータの重要度解析(推奨)。他の緊急時対応計画コンポーネントをサポートする特定のアプリケーションおよびデータについて、相対的な重要度を評価します。</p>	<p>NAは、電子保護医療情報の作成や維持は行いません。</p> <p>NAは、データを損失することなく、自動エラー検出と自動(または手動)フェイルオーバーをサポートする高可用性(HA)システムです。</p> <p>NAは、データを損失することなく、自動エラー検出と自動(または手動)フェイルオーバーをサポートする高可用性(HA)システムです。</p> <p>NAは、自動エラー検出と自動(または手動)フェイルオーバーの定期的なテストをサポートします。</p> <p>NAの強固なレポート機能をベースとして、他の緊急時対応計画コンポーネントに対するNAの相対的な重要度を評価することができます。</p>
<p><b>評価</b></p> <p>定期的な技術的評価と非技術的評価を実行します。</p> <p>書面契約などの協定(必須)。§ 164.314 (a) の該当要件に適合する業務提携先との書面の契約や他の協定を通じて、このセクションの段落 (b) (1) が必須とする十分な保証を文書化します。</p>	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 特定のデバイス群に制限されたユーザ。</li> <li>• 管理者アクセス権限を割り当てられたユーザ。</li> <li>• 適用されているワークフロールール。[ワークフロー設定]ページをクリックすると、ワークフローウィザードが開きます。</li> <li>• 適用されている構成ポリシー。</li> <li>• 適用されているデバイスパスワードルール。</li> </ul> <p>この要件はNAの対象範囲外です。</p>
<p><b>物理的な保護手段</b></p> <p>(i) 緊急時の運用(推奨)。緊急時に災害復旧計画や緊急モード運用計画の下で、損失データの回復をサポートする施設アクセスを可能にする手順を確立します(また、必要に応じて実施します)。</p>	<p>この要件はNAの対象範囲外です。</p>

フィールド	説明/アクション
<p>(ii) 施設のセキュリティ計画（推奨）。認可されていない物理アクセス、不正、盗用から施設と設備を保護するポリシーと手順を実施します。</p> <p>(iii) アクセス制御と検証手順（推奨）。個人のロールや職務に基づいて、施設への個人のアクセスを制御し検証する手順を実施します。たとえば、ビジターの制御、テストや改版を行うソフトウェアプログラムへのアクセス制御などです。</p> <p>(iv) 保守記録（推奨）。セキュリティに関連する施設の物理環境の修復と変更を文書化するポリシーと手順を実装します（たとえば、ハードウェア、壁、ドア、鍵などです）。</p>	<p>この要件はNAの対象範囲外です。</p> <p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• 過去7日間のユーザログイン試行。</li> <li>• 過去7日間に失敗したユーザログイン試行。</li> <li>• 特定のデバイスグループに制限されたユーザ。</li> <li>• 制限された（非管理者）アクセス権限を割り当てられたユーザ。</li> </ul> <p>この要件はNAの対象範囲外です。</p>
<p><b>ワークステーションの使用</b></p> <p>実行すべき適切な機能を指定するポリシーと手順を実施します。</p> <p>電子保護医療情報にアクセスするすべてのワークステーションについて、物理的な保護手段を実施します。これによって権限があるユーザにアクセスを制限します。</p>	<p>この要件はNAの対象範囲外です。</p> <p>この要件はNAの対象範囲外です。</p>
<p><b>デバイスとメディアの制御</b></p> <p>(i) 廃棄（必須）。電子保護医療情報および情報が格納されているハードウェアまたは電子メディアの最終的な処分に関するポリシーと手順を実施します。</p> <p>(ii) メディアの再利用（必須）。電子保護医療情報を格納した電子メディアが再利用される前に電子保護医療情報を削除する手順を実施します。</p> <p>(iii) 責任（推奨）。ハードウェアおよび電子メディアの移動記録を維持し、移動の責任者を設置します。</p> <p>(iv) データのバックアップと保管（推奨）。必要に応じて、設備を移動する前に、取得可能な電子保護医療情報の複製を作成します。</p>	<p>この要件はNAの対象範囲外です。</p> <p>この要件はNAの対象範囲外です。</p> <p>この要件はNAの対象範囲外です。</p> <p>この要件はNAの対象範囲外です。</p>
<p><b>技術的な保護手段</b></p> <p>(i) 固有のユーザID（必須）。ユーザIDを特定し追跡するために、固有の名前や識別番号を割り当てます。</p>	<p>次の点についての数を表示します。</p> <ul style="list-style-type: none"> <li>• HP Network Automationで有効にされたユーザアカウント。</li> <li>• HP Network Automationで無効にされたユーザアカウント。</li> </ul>

フィールド	説明/アクション
<p>(ii) 緊急時のアクセス手順（必須）。緊急時に必要な電子保護医療情報を取得する手順を確立します（また、必要に応じて実施します）。</p> <p>(iii) 自動ログオフ（推奨）。事前に指定した非アクティブな時間が経過した後電子セッションを終了する手順を実施します。</p> <p>(iv) 暗号化と復号化（推奨）。電子保護医療情報の暗号化と複合化を行うメカニズムを実施します。</p>	<p>HP Network Automationは、データを損失することなく、自動エラー検出と自動（または手動）フェイルオーバーをサポートする高可用性（HA）システムです。</p> <p>Webユーザセッションが1800秒の非アクティブな時間が経過した後を終了しました。デフォルト値は1800です。この値は設定できます。</p> <p>この要件はNAの対象範囲外です。</p>
<p><b>監査の制御</b></p> <p>電子保護医療情報を格納または使用する情報システムについて、その動作を記録し確認するためのハードウェア、ソフトウェア、手続きのメカニズムを実施します。</p>	<p>この要件はNAの対象範囲外です。</p>
<p><b>標準の整合性</b></p> <p>電子保護医療情報を認証するメカニズム（推奨）。電子保護医療情報が不正に変更または破棄されないようにする、確実な電子メカニズムを実施します。</p>	<p>この要件はNAの対象範囲外です。</p>
<p><b>個人または団体の認証</b></p> <p>電子保護医療情報に対するアクセスを要求する個人または団体について、アクセス権があるかどうかを検証する手順を実施します。</p>	<p>この要件はNAの対象範囲外です。</p>
<p><b>送信セキュリティ</b></p> <p>(i) 整合性の制御（推奨）。電子的に送信される電子保護医療情報が、破棄されるまでの間、不正に変更されて未検出のままにならないよう、セキュリティ対策を実施します。</p> <p>(ii) 暗号化（推奨）。適切な場合、電子保護医療情報を暗号化するメカニズムを実施します。</p>	<p>この要件はNAの対象範囲外です。</p> <p>この要件はNAの対象範囲外です。</p>
<p><b>ポリシーと手順</b></p> <p>標準、実装仕様、または他の要件に準拠する適切なポリシーおよび手順を実施します。</p>	<p>この要件はNAの対象範囲外です。</p>

フィールド	説明/アクション
<b>ドキュメント</b>  (i) 時間制限（必須）。このセクションの段落（b）（1）で必須とされている文書は、作成日または最後の実施日（最新の日付を適用します）から6年間保持します。  (ii) 可用性（必須）。文書に保存されている手順を実施する責任者が、その文書を使用できるようにします。  (iii) 更新（必須）。電子保護医療情報のセキュリティに影響を与える環境の変化や運用上の変化に応じて、文書を定期的に確認し、必要に応じて更新します。	

## PCI データセキュリティ標準準拠のステータスレポート

データ盗用に対処し、消費者の信頼を維持するために、主要なクレジットカード発行会社はいずれも、以下のよう  
に詳細なセキュリティプログラムを構築してきました。

- Visa USA Cardholder Information Security Program (CISP)
- MasterCard Site Data Protection (SDP) プログラム
- Discover Information Security and Compliance (DISC) プログラム
- American Express Data Security Operating Policy (DSOP)

2004 年後半、Visa と MasterCard は、1 つの標準の下に両社のプログラムを提携しました。それが Payment Card Industry (PCI) データセキュリティ規格です。カード所有者データを保護するために策定された基本セキュリティベストプラクティスは、12 の PCI 要件から構成されています。以上の要件に準拠できなかった場合、またはセキュリティ問題を修正できなかった場合の罰則は重大です。業者に対する制限の適用、または業者の Visa プログラムへの参加の永久的禁止、および 1 件の事故に付き最高 \$500,000 の罰金という罰則があります。

PCI データセキュリティ標準に関する NA の機能の詳細については、[PCI データセキュリティ標準と、HP Network Automation を使用した準拠実現に関する詳細な情報] リンクをクリックして参照してください。

PCI データセキュリティ標準準拠のステータスレポートを表示するには：

1. [レポート] のメニューバーで、[コンプライアンスセンター] をクリックします。  
コンプライアンスセンターのホームページが開きます。
2. [PCI データセキュリティ標準準拠のステータス] リンクをクリックします。  
[PCI データセキュリティ標準準拠のステータス] ページが開きます。

## [PCI データセキュリティ標準準拠のステータス] ページ

[PCI データセキュリティ標準準拠のステータス] ページには、PCI データセキュリティ標準の要件に基づき、NA の情報がまとめられています。標準の各要件について、次の各列を含む表がページに表示されます。

- **仕様**：表の各行に 1 つの要件が記述されています。
- **ステータス**：この要件が適用される管理ネットワークのサマリが表示されます。
- **詳細情報**：[サマリ] 列の情報に関連する NA console ページへのリンクです。

## 第19章：ワークフローの作成

### トピックの参照先リスト

トピック	参照先：
はじめに	<a href="#">「はじめに」</a> （664 ページ）
ワークフローウィザード	<a href="#">「ワークフローウィザード」</a> （665 ページ）
自分のタスク	<a href="#">「自分のタスク」</a> （667 ページ）
承認の要求	<a href="#">「承認の要求」</a> （670 ページ）
タスクの承認	<a href="#">「タスクの承認」</a> （672 ページ）
電子メール通知	<a href="#">「電子メール通知」</a> （675 ページ）

## はじめに

HP Network Automation (NA) Workflow Integration & Routing Engine (WIRE) は、ネットワーク構成のプロセスを管理し、あらかじめ定義されたポリシーに従ってネットワークの変更が行われ、正しい順序で完了し、適切な担当者によって承認されるようにします。

ネットワークに対する操作、操作を実行するユーザ、およびその理由を統制することにより、デバイスの構成を正確に、また組織の目的に調和した方法で行うことができます。ワークフローでは、タスクの順序付け、承認の取得、および結果の監査を管理するため、ポリシーを無視した変更や不注意による構成のエラーが発生する確率をほとんど無くすることができます。

この章では次の用語を使用します。

- **タスク**：タスクは、NAがネットワークと対話するときの手段となる主要なメカニズムです。タスクは特定のアクションであり、スケジュールすることも、すぐに実行することもできます。タスクが完了すると、NAアクティビティの結果が出力されます。ワークフロータスクには、次のタスクがあります。
  - パスワードの配布
  - デバイスのリブート
  - タスクスナップショット
  - コマンドスクリプトの実行
  - スタートアップとランニングの同期
  - デバイスソフトウェアの更新
  - 診断の実行

タスクの全リストについては、「**タスクとは**」(277ページ)を参照してください。

- **プロジェクト**：プロジェクトは、順序付けられた一連のタスクです。NA の観点から見たプロジェクトは、(並列ではなく) 順番に実行されるサブタスクを持つ別のタイプのタスクに過ぎません。
- **作成者**：承認を受けるためにタスクを送信する個人です。
- **承認者**：タスクを承認し、タスクがすべての内部ポリシーに準拠することを確認することができる個人または個人のグループです。
- **FYI受信者**：作成者または承認者によって実行されたアクションに基づく通知を受信する個人または個人のグループです。
- **承認済み**：実行する承認を受けたタスクの承認ステータスです。
- **未承認**：拒否されたタスクの承認ステータスです。拒否されたタスクには、十分なデータが存在しないか、またはネットワークにマイナスの影響を及ぼす可能性がある不正なデータが含まれています。拒否されたタスクは、再使用できません。
- **中断**：一時的に（または無期限に）保留されているタスクの承認ステータスです。



- 無効化：承認プロセスを無効化する必要がある場合に、タスクの作成者によって実行される緊急時のアクションです。この機能は、システム管理設定で有効に設定されている場合にのみ使用できます。

**注意：** パワーユーザに対しては、タスクを作成しても承認を受ける必要がないように設定することもできます。ルールの作成方法の詳細については、「[ワークフローウィザード](#)」(665ページ)を参照してください。たとえば、「全ユーザは管理者による承認が必要」というルールの前に「全パワーユーザは承認が不要」というルールを作成して、パワーユーザの場合は承認を無視可能にすることができます。

## ワークフローウィザード

ワークフローウィザードにより、タスクのワークフローを容易に設定できます。ワークフローウィザードを開くには、[管理]の下メニューバーで[ワークフロー設定]をクリックします。ワークフローウィザードが開きます。

手順	説明/アクション
ようこそページ	[ようこそ]ページには、ワークフローウィザードについての短い説明が表示されます。[次へ]をクリックして続行します。
手順1：ワークフローを有効にする	ワークフローを有効にするかどうかを尋ねるメッセージが表示されます。タスクの一部または全部を承認する必要があります。[はい]をクリックし、[次へ]をクリックして続行します。[いいえ]をクリックして[次へ]をクリックすると、[設定完了]ページが開きます。このページからワークフローウィザードのホームページに戻ることができます。
手順2：ワークフローを有効にする - 続き	[ワークフローを有効にする - 続き]ページには、ワークフローの作成時に入力する必要がある情報の概要が表示されます。[次へ]をクリックして続行します。
手順3：承認ルールを管理	<p>新しいワークフロー承認ルールの名前を入力し、[次へ]をクリックして続行します。既存のワークフロー承認ルールを変更または削除することもできます。既存のすべてのワークフロー承認ルールが、ページの最下部に表示されます。<b>(注意：</b>出荷時のNAには、[管理者によって承認された全ユーザ]という1つのデフォルトワークフロー承認ルールが存在します)。</p> <p><b>注意：</b>ワークフロー承認ルールは、パーティションに従いパーティション化できます。すべてのパーティションで利用できるワークフロー承認ルールがいくつか存在します。これらのワークフロー承認ルールは、構成により[共有]（または[グローバル]）とラベル付けされます。ただし、適切な権限がない場合には、これらのワークフロー承認ルールは編集したり削除できません。パーティションの作成の詳細については、「<a href="#">デバイスとユーザのセグメント化</a>」(148ページ)を参照してください。</p>
手順4：作成者の設定	[作成者の設定]ページでは、タスクを作成するときにこのルールを適用するユーザを割り当てることができます。ユーザの追加操作が完了したら、[次へ]をクリックして続行します。
手順5：タスク設定	[タスク設定]ページでは、承認を必要とするタスクを指定できます。タスクの追加操作が完了したら、[次へ]をクリックして続行します。承認を必要とするタスクを指定しないと、そのタスクの承認設定は「未対応」として表示されます。

手順	説明/アクション
手順6：デバイスグループの設定	<p>[デバイスグループの設定]ページでは、デバイスグループに基づいてワークフロー承認ルールを定義できます。これにより、デバイスの使用法やデバイスタイプなどについてのワークフロー承認ルールを構成できます。デバイスのパーティションが有効である場合、パーティション選択ドロップダウンメニューが表示されます。優先度レベルは、パーティション内部でのみ調整できます。グローバルルールは、常にパーティションルールよりも高い優先度を持ちます。デバイスグループの追加操作が完了したら、[次へ]をクリックします。タスクの作成時には、次の場合にのみワークフロー承認ルールが適用されます。</p> <ul style="list-style-type: none"> <li>• タスクが単独のデバイスに対するもので、ワークフロー承認ルールのデバイスグループにそのデバイスが含まれている。</li> <li>• タスクはデバイスグループに対するもので、ワークフロー承認ルールのデバイスグループにそのタスクのデバイスグループとのnon-emptyインターセクションがある。</li> </ul>
手順7：承認者の設定	<p>[承認者の設定]ページでは、タスクを承認し、タスクがすべての内部ポリシーに準拠していること、または承認が不要であることを確認するユーザを割り当てることができます。タスクの作成者は、自分で作成したタスクを確認することはできません。ユーザの追加操作が完了したら、[次へ]をクリックして続行します。</p>
手順8：FYI受信者の設定	<p>[FYI受信者の設定]ページでは、ワークフロー承認ルールの作成者または承認者によって実行されたタスクに基づく通知を受信するユーザを割り当てることができます。ユーザの追加操作が完了したら、[保存]をクリックします。作成者および承認者を受信者として追加する必要はありません。電子メール通知の詳細については、「<a href="#">電子メール通知</a>」(675ページ)を参照してください。</p>
設定完了	<p>ワークフロー承認ルールが正常に追加されると、ページの上部に「新規ルール“ルール名”が正常に作成されました」というメッセージが表示されます。これで、他のユーザ（作成者）の新規ワークフロー承認ルールを作成したり、[承認ルールを管理]へのリンクをクリックして既存の承認ルールを変更/削除したりできるようになります。また、[タスク]ドロップダウンメニューの[自分のタスク]オプションをクリックして、作成者と承認者のアクションの概要を表示できます。詳細については、「<a href="#">自分のタスク</a>」(667ページ)を参照してください。</p>

## 自分のタスク

[自分のタスク]ページでは、現在ログインしているユーザが作成したタスクを表示します。タスクが実行されていない場合、該当するものがあればタスクの承認ステータスも表示します。

[自分のタスク]ページを表示するには、[タスク]メニューで[自分のタスク]をクリックします。[自分のタスク]ページが開きます。

## [自分のタスク]ページのフィールド

フィールド	説明/アクション
自分のドラフト	該当する場合は、[自分のドラフト]ページが開きます。
承認の要求	<p>タスク承認を受ける必要がある場合は、[承認の要求]ページが開きます。このページでは、現在ログインしているユーザによる承認を必要とするタスクを確認できます。デフォルトでは、次のステータスのタスクを含む未完了のタスクがページに表示されます。</p> <ul style="list-style-type: none"> <li>• 未承認</li> <li>• 承認を待機中</li> <li>• 実行待ち</li> </ul> <p>詳細については、「<a href="#">承認の要求</a>」(670 ページ) を参照してください。</p>
予定タスク	[予定タスク]ページが開きます。このページでは、キュー内に存在していてまだ実行されていない予定されたタスクを確認できます。詳細については、「 <a href="#">[予定タスク]ページのフィールド</a> 」(400 ページ) を参照してください。
実行中のタスク	[実行中のタスク]ページが開きます。このページでは、実行中のすべてのタスクを確認できます。詳細については、「 <a href="#">[実行中のタスク]ページのフィールド</a> 」(402 ページ) を参照してください。
最近のタスク	[最近のタスク]ページが開きます。このページでは、最近のすべてのタスクを確認できます。詳細については、「 <a href="#">[最近のタスク]ページのフィールド</a> 」(404 ページ) を参照してください。
タスクの表示の チェックボックス	<p>タスクの承認を受ける必要がある場合は、次の表示オプションを選択できます。</p> <ul style="list-style-type: none"> <li>• 承認済み</li> <li>• 未承認</li> <li>• 承認を待機中</li> <li>• 無効化</li> <li>• ドラフト</li> <li>• 承認は不要</li> </ul>
チェックボックス	左側のチェックボックスを使用してタスクを削除できます。タスクを選択したら、[アクション]ドロップダウンメニューをクリックし、[削除]をクリックします。横の[選択]ドロップダウンメニューにより、すべてのタスクを選択または削除できます。
スケジュール日	タスクが作成された日時を表示します。
タスク名	タスク名を表示します。タスクをクリックすると、[タスク情報]ページが開きます。タスクの詳細については、「 <a href="#">タスクとは</a> 」(277 ページ) を参照してください。

フィールド	説明/アクション
承認期限	該当する場合は、タスクの承認期限となる日時を表示します。タスクが承認期限までに承認されない場合、ステータスが「未承認」に設定されます（ <b>注意</b> ：承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます）。
承認のステータス	<p>該当する場合は、タスクの承認ステータスを表示します。承認ステータスは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。次に示す承認のステータスがあります。</p> <ul style="list-style-type: none"> <li>承認を待機中</li> <li>承認済み</li> <li>未承認</li> <li>無効化</li> <li>承認は不要</li> </ul>
タスクのステータス	<p>タスクのステータスを表示します。次に示すステータスがあります。</p> <ul style="list-style-type: none"> <li>警告：すべてのタスクが失敗していなくても、グループタスクの一部のサブタスクが失敗しています。</li> <li>ドラフト：ドラフトステータスの場合、NAはタスクを実行せず、また承認を受けるためにタスクが送信されることもありません。</li> <li>重複：同一のタスクがすでに実行されているため、タスクは開始されませんでした。</li> <li>失敗：タスクは失敗しました。</li> <li>一時停止：他のユーザによりタスクが一時停止されました。タスクは、予定時刻になるまで実行されません。</li> <li>保留：タスクはキューに送られ、予定時刻になるまで待機します。</li> <li>実行中：タスクは開始しましたが、まだ終了していません。</li> <li>スキップ：タスクはエラー（たとえば、不正な権限や非管理デバイスなど）のためにスキップされました。</li> <li>成功：タスクは成功しました。</li> <li>待機中：予定時刻になりましたが、「最大同時タスク」制限に達したため、タスクは待機中です。</li> </ul>
優先度	タスクの優先度を表示します。タスクの優先度の詳細については、「 <b>タスクの予定</b> 」（278 ページ）を参照してください。
タスクタイプ	<p>次のようなタスクタイプを表示します。</p> <ul style="list-style-type: none"> <li>パスワードの配布</li> <li>構成を配布</li> <li>ドライバの検出</li> <li>デバイスのリポート</li> <li>スナップショットの取得</li> <li>スタートアップとランニングの同期</li> </ul> <p>タスクの全リストについては、「<b>タスクとは</b>」（277 ページ）を参照してください。（<b>注意</b>：マルチタスクプロジェクトタスクは、[自分のタスク]結果ページに表示される場合とされない場合があります。表示されるかどうかは、マルチタスクプロジェクトのタスクに上記のタスクタイプの1つがサブタスクとして含まれているかどうかによって決まります）。</p>

フィールド	説明/アクション
アクション	次のオプションからいずれか1つを選択できます。 <ul style="list-style-type: none"><li>• 削除：タスクを削除できます。</li><li>• 一時停止：タスクを一時停止し、その予定された時刻に実行されないようにします（<b>注意</b>：タスクを再開する場合は、[再開]を選択します）。</li><li>• 直ちに実行：できるだけすぐにタスクを実行します。同時タスクの最大数に到達していない場合は、タスクが直ちに実行されます。</li><li>• 編集：対象タスクの[タスクを編集]ページが開きます。</li></ul>
1ページに表示する結果の数	ドロップダウンメニューから、ページあたりの表示項目数を設定できます。デフォルト値は25です。

## 承認の要求

[承認の要求]ページでは、現在ログインしているユーザによる承認を必要とするタスクを確認できます。デフォルトでは、承認ステータスが「承認済み」、「承認待ち」、「未承認」になっている未完了のタスクがページに表示されます。

**注意：**完了したタスクを表示するには、[レポート]の下メニューバーで[検索]を選択し、[タスク]をクリックします。詳細については、「[\[タスクを検索\]ページのフィールド](#)」(502ページ)を参照してください。

[承認の要求]ページを表示するには、[タスク]の下メニューバーで[承認の要求]をクリックします。[承認の要求]ページが開きます。

## [承認の要求]ページのフィールド

フィールド	説明/アクション
自分のタスク	[自分のタスク]ページが開きます。このページでは、各タスクのステータスを確認できます。詳細については、「 <a href="#">[自分のタスク]ページのフィールド</a> 」(667ページ)を参照してください。
予定タスク	[予定タスク]ページが開きます。このページでは、キュー内に存在していてまだ実行されていない予定されたタスクを確認できます。詳細については、「 <a href="#">[予定タスク]ページのフィールド</a> 」(400ページ)を参照してください。
実行中のタスク	[実行中のタスク]ページが開きます。このページでは、実行中のすべてのタスクを確認できます。詳細については、「 <a href="#">[実行中のタスク]ページのフィールド</a> 」(402ページ)を参照してください。
最近のタスク	[最近のタスク]ページが開きます。このページでは、最近のすべてのタスクを確認できます。詳細については、「 <a href="#">[最近のタスク]ページのフィールド</a> 」(404ページ)を参照してください。
タスクの表示	オンにすると、次の承認ステータスのタスクが表示されます。 <ul style="list-style-type: none"> <li>承認済み</li> <li>未承認</li> <li>承認を待機中</li> </ul>
タスク名	タスク名を表示します。タスクを承認するには、タスク名をクリックします。[タスク情報]ページが開きます。詳細については、「 <a href="#">[タスク情報]ページのフィールド</a> 」(672ページ)を参照してください。
承認期限	タスクの承認期限となる日時を表示します。タスクが承認期限までに承認されない場合、ステータスが「未承認」に設定されます（ <b>注意：</b> 実行されたタスクは[承認の要求]ページから削除されます。承認期限を過ぎたタスクには「未承認」のマークが付けられ、データブルーナによって削除されるまで[承認の要求]ページに表示されます。データの整理の詳細については、「 <a href="#">[データの整理]タスクページのフィールド</a> 」(385ページ)を参照してください。）
承認のステータス	タスクの承認ステータスを表示します。次に示す承認のステータスがあります。 <ul style="list-style-type: none"> <li>承認を待機中</li> <li>未承認</li> </ul>
優先度	タスクの優先度を表示します。
日付	タスクが作成された日時を表示します。

フィールド	説明/アクション
ステータス	<p>タスクのステータスを表示します。次に示すステータスがあります。</p> <ul style="list-style-type: none"><li>• 警告：すべてのタスクが失敗していなくても、グループタスクの一部のタスクが失敗しています。</li><li>• ドラフト：ドラフトステータスの場合、NAはタスクを実行せず、また承認を受けるためにタスクが送信されることもありません。</li><li>• 重複：同一のタスクがすでに実行されているため、タスクは開始されませんでした。</li><li>• 失敗：タスクは失敗しました。</li><li>• 一時停止：他のユーザによりタスクが一時停止されました。タスクは、予定時刻になるまで実行されません。</li><li>• 保留：タスクはキューに送られ、予定時刻になるまで待機します。</li><li>• 実行中：タスクは開始しましたが、まだ終了していません。</li><li>• スキップ：タスクはエラー（たとえば、不正な権限や非管理デバイスなど）のためにスキップされました。</li><li>• 成功：タスクは成功しました。</li><li>• 待機中：予定時刻になりましたが、「最大同時タスク」制限に達したため、タスクは待機中です。</li></ul>
スケジュール作成者	タスクをスケジュールしたユーザの名前を表示します。

## タスクの承認

タスクを承認する権限が割り当てられている場合は、次の手順に従います。

1. [タスク]の下メニューバーで、[承認の要求]をクリックします。[承認の要求]ページが開きます。「[\[承認の要求\]ページのフィールド](#)」(670ページ)を参照してください。
2. タスク名をクリックして承認オプションを表示します。[タスク情報]ページが開きます。
3. [承認]ボタンをクリックします。

## [タスク情報]ページのフィールド

[タスク情報]ページには、タスクについて次の詳細な情報が表示されます。

- タスクのステータス
- 作成者
- 影響を受けるデバイス
- 継続時間
- 承認情報
- 結果の詳細

[タスク情報]ページには、警告または失敗のイベントのより詳細な情報へのリンクも表示されます。タスクは、正常に完了することができても、エラーが含まれている場合があります。たとえば、実行構成を正常に配布することができても、その構成に無効なコマンドが含まれている場合があります。

[タスク情報]ページを開くには：

1. [インベントリ]ページからデバイスを選択します。[デバイス詳細]ページが開きます。
2. [表示]ドロップダウンメニューで、[デバイスタスク]をクリックします。[デバイスタスク]ページが開きます。
3. 詳細な情報を表示させるタスクの[アクション]列にある[詳細]オプションをクリックします。[タスク情報]ページが開きます。

フィールド	説明/アクション
タスクを編集	タスクを編集するためのタスクページが開きます。このリンクは、保留タスクの場合にのみ表示されます。
再実行	タスクを再実行するためのタスクページが開きます。このリンクは、完了タスクの場合にのみ表示されます。
リストに戻る	[自分のタスク]ページが開きます。「 <a href="#">[自分のタスク]ページのフィールド</a> 」(397ページ)を参照してください。
一般情報	
タスク名	タスク名を表示します。



フィールド	説明/アクション
タスクのステータス	<p>次に示すタスクのステータスを表示します。</p> <ul style="list-style-type: none"> <li>• ドラフト</li> <li>• 重複</li> <li>• 失敗</li> <li>• 一時停止</li> <li>• 保留</li> <li>• 要求（<b>注意</b>：要求とは、タスクが承認を待っていることを示します。「<b>タスクの承認</b>」（672 ページ）を参照してください。）</li> <li>• 実行中</li> <li>• スキップ</li> <li>• 成功</li> <li>• 同期（<b>注意</b>：NAは通常、スレッドを作成し、バックグラウンドで非同期に実行させることによりタスクを実行します。CLIおよびAPIによって同期タスクが可能になり、この場合タスクは、コマンドが完了するまで現在のスレッドとコマンドブロックで実行されます）。</li> <li>• 待機中</li> <li>• 警告</li> </ul> <p><b>注意</b>：警告があった場合でも、マルチタスクプロジェクトでは処理を続行します。警告ステータスは親タスクで示されます。</p>
コメント	タスクについてのコメントを表示します。
作成者	タスクをスケジュールしたユーザ名またはプロセスを表示します。
作成日	タスクが作成された日時を表示します。
影響を受けるデバイス	影響を受けるデバイスのホスト名またはIPアドレスを表示します。
スケジュール日	タスクの実行予定日時を表示します。
開始日	タスクの開始日を表示します。
完了日	タスクの完了日を表示します。
継続時間	タスクの継続時間を表示します。
反復タイプ	たとえば、非反復などの反復タイプを表示します。
<b>承認情報</b>	
承認者	タスクの承認者リストを表示します。
承認のステータス	タスクの承認ステータスを表示します。
優先度	タスクの優先度を表示します。
承認者	タスクの承認期限となる日時を表示します。
新規コメント	タスクについての追加コメントを入力します。
承認ボタン	[承認]ボタンをクリックしてタスクを承認します。

フィールド	説明/アクション
タスクの詳細を表示	[タスクの表示]へのリンクをクリックすると、[診断履歴]ページが開きます。
<b>追加情報</b>	
結果の詳細	<p>(デバイスタイプに応じて) 自動的に実行された診断を表示します。たとえば、次のような診断があります。</p> <ul style="list-style-type: none"><li>• Diagnostic NA Module Status completed (診断 'NA モジュールのステータス' が完了しました)</li><li>• Diagnostic NA Routing Table completed (診断 'NA ルーティングテーブル' が完了しました)</li><li>• 診断 'NA OSPF ネイバー' が完了しました。</li></ul>
<b>タスク履歴</b>	
タスク履歴情報	タスクの実行日時、反復タイプ、およびステータスなどのタスク履歴情報を表示します。

## 電子メール通知

タスクの承認者は、ワークフローの作成者によって実行されたアクションに基づいた電子メール通知を受信します。ワークフローウィザードの[FYI受信者の設定]ページを使用して、タスクの承認者以外のユーザに通知できます。「[ワークフローウィザード](#)」(665 ページ) を参照してください。

電子メール通知のサンプルを次に示します。

差出人: HP on jbreannan1  
送信日: 2007 年 1 月 10 日木曜日 2:00PM  
宛先: Tad Martin  
件名: 承認の要求

---

Liza は、承認を得るためにタスク スナップショット を送信しました。  
承認の期日は 2004-11-06 00:00:00:0 です。

タスク名: スナップショット  
説明: Lab2 のスナップショット  
優先度: 高  
承認の期日: 2004-11-06 00:00:00:0  
作成者: Liza  
影響を受けるデバイス: 172.22.123.26  
タスクの頻度: 1 回  
タスクの開始日: 2004-11-06 15:00:00.0

<http://liza/task.view.htm/taskID=10023> で  
HP Network Automation にアクセスして、  
承認、否認、または分類の要求を行えます

電子メールの最後にあるリンクをクリックすると、[承認の要求]ページが開きます。このページでは、タスクを承認または拒否することができます。「[\[承認の要求\]ページのフィールド](#)」(670 ページ) を参照してください。



## 第21章：トラブルシューティング

### トピックの参照先リスト

トピック	参照先：
ドライバ検出の失敗	<a href="#">「ドライバ検出の失敗」</a> (678 ページ)
デバイスのスナップショット取得の失敗	<a href="#">「デバイスのスナップショット取得の失敗」</a> (679 ページ)
syslog によるリアルタイム変更検出機能なし	<a href="#">「syslog によるリアルタイム変更検出機能なし」</a> (680 ページ)
セッションログ	<a href="#">「セッションログ」</a> (681 ページ)
SWIM エラーメッセージ	<a href="#">「SWIM エラーメッセージ」</a> (682 ページ)

ログ記録の詳細については、[「ログ記録」](#) (96 ページ) を参照してください。トラブルシューティング情報をカスタマーサポートに送信する方法の詳細については、[「\[トラブルシューティングの送信\] ページのフィールド」](#) (29 ページ) を参照してください。

## ドライバ検出の失敗

デバイスのドライバを検出できない場合は：

1. 検出対象のデバイスのデバイスモデルとOSのバージョンがサポートされていることを確認します。サポートされるデバイスの詳細については、Driver Release Service (DRS) ドキュメントを参照してください。DRSは、自動化されたドライバのリリースと配信システムです。デバイスがサポートされていない場合、顧客サポートに問い合わせてください。デバイスがサポートされていれば、ステップ2に進みます。
2. NAサーバからデバイスに、Telnet、SSHのいずれかまたは両方でアクセスします。NAがデバイスにTelnetやSSHでアクセスできることを簡単に確認するには、[デバイスリスト]ページにあるデバイスの[Telnet]または[SSH]リンクをクリックしてください。詳細については、「[\[インベントリ\]ページのフィールド](#)」(186ページ)を参照してください。NAは自動的にデバイスへのログインを試みます。デバイスにログインできない場合、デバイス上のアクセスリストが正しくない、パスワード情報が正しくない、またはネットワークの接続に関する問題が原因である可能性があります。顧客サポートに問い合わせてください。デバイスにTelnetまたはSSH経由で接続できても、ドライバの検出が失敗する場合は、ステップ3に進みます。
3. デバイス上で読み取り専用SNMPが有効であることを確認してください。読み取り専用SNMPが有効になっている場合は、このOIDを使用し、読み取り専用SNMP経由でNAサーバからデバイスへの接続を試みます。NA内でデバイスに構成されているコミュニティ文字列を使用してください。読み取り専用SNMPを有効にしない場合、デバイスの追加や編集時に、ドライバのドロップダウンリストからドライバを手動で選択できます。詳細については、「[デバイス構成データの編集](#)」(178ページ)を参照してください。読み取り専用SNMPを有効にしたら、NAにログインし、追加するデバイスを選択して、[デバイスを編集]をクリックします。読み取り専用SNMPコミュニティ文字列が正しいデバイスを更新し、[ドライバの検出]をクリックします。それでもドライバの検出が失敗する場合は、ステップ4に進みます。
4. NAにログインします。メニューバーで[管理]を選択し、[トラブルシューティング]をクリックします。[トラブルシューティング]ページが開きます。リストボックスで、[device/session/log]と[device/driver/discovery]を選択します。レベルを[トレース（メッセージ数が最多）]に設定します。[送信]をクリックします。検出対象のデバイスをクリックしてから、[ドライバの検出]をクリックします。ドライバの検出に失敗したら、メニューバーで[管理]を選択し、[トラブルシューティング]をクリックします。[トラブルシューティング情報の送信]をクリックします。コメントセクションで、失敗の内容およびデバイスモデルとOSバージョンを指定します。ログ記録の詳細については、「[ログ記録](#)」(96ページ)を参照してください。

## デバイスのスナップショット取得の失敗

デバイスのスナップショットの取得に失敗した場合は：

1. スナップショットの取得対象であるデバイスのデバイスモデルと OS のバージョンが、NA でサポートされていることを確認します。サポートされるデバイスの詳細については、Driver Release Service (DRS) ドキュメントを参照してください。DRS は、自動化されたドライバのリリースと配信システムです。デバイスがサポートされていない場合、顧客サポートに問い合わせてください。デバイスがサポートされていれば、ステップ2に進みます。
2. デバイスに割り当てられているデバイスドライバが存在することを確認します。[ デバイスリスト ] ページで、問題のあるデバイスをクリックします。詳細については、「[表示メニューオプション](#)」(201 ページ) を参照してください。[ ドライバ名 ] フィールドまでスクロールし、値が表示されているかどうかを確認します。ドライバが表示されていない場合は、顧客サポートにお問い合わせください。ドライバが表示されている場合は、[ ドライバの検出 ] リンクをクリックします。それでもスナップショットタスクが失敗する場合は、ステップ3に進みます。
3. NA サーバからデバイスに、Telnet、SSH のいずれかまたは両方でアクセスします。NA がデバイスに Telnet や SSH でアクセスできることを簡単に確認するには、[ デバイスリスト ] ページにあるデバイスの [ Telnet ] または [ SSH ] リンクをクリックしてください。詳細については、「[\[インベントリ\] ページのフィールド](#)」(186 ページ) を参照してください。デバイスにログインできない場合、デバイス上のアクセスリストが正しくない、パスワード情報が正しくない、またはネットワークの接続に関する問題が原因である可能性があります。顧客サポートに問い合わせてください。デバイスに Telnet または SSH 接続できても、ドライバの検出タスクに失敗する場合は、ステップ4に進みます。
4. デバイス上で読み取り専用 SNMP が有効であることを確認してください。デバイスで読み取り専用 SNMP が有効になっている場合は、この OID を使用して、読み取り専用 SNMP 経由で NA サーバからデバイスへの接続を試みます。NA 内でデバイスに構成されているコミュニティ文字列を使用してください。読み取り専用 SNMP を有効にしない場合、デバイスの追加や編集時に、ドライバのドロップダウンリストからドライバを手動で選択できます。詳細については、「[デバイス構成データの編集](#)」(178 ページ) を参照してください。読み取り専用 SNMP を有効にしたら、NA にログインし、追加するデバイスを選択して、[ デバイスを編集 ] をクリックします。読み取り専用 SNMP コミュニティ文字列が正しいデバイスを更新し、[ スナップショット ] をクリックします。それでもスナップショットタスクが失敗する場合は、顧客サポートにお問い合わせください。

## syslogによるリアルタイム変更検出機能なし

syslogによるリアルタイム変更検出機能がない場合は：

1. スナップショットの取得対象であるデバイスのデバイスモデルとOSのバージョンが、NAでサポートされていることを確認します。サポートされるデバイスの詳細については、Driver Release Service（DRS）ドキュメントを参照してください。DRSは、自動化されたドライバのリリースと配信システムです。デバイスがサポートされていない場合、顧客サポートに問い合わせてください。デバイスがサポートされていれば、ステップ2に進みます。
2. syslogメッセージがNAサーバに届くようにsyslogが正しく設定されていることを確認します。NAへのsyslog変更メッセージの送信処理をトリガするイベントを開始します。
3. デバイス/OSの組み合わせが、syslogによるリアルタイム変更検出機能をサポートしていることを確認します。サポートされるデバイスの詳細については、Driver Release Service（DRS）ドキュメントを参照してください。DRSは、自動化されたドライバのリリースと配信システムです。可能であれば、ベンダーのWebサイトにアクセスし、このデバイスとOSの組み合わせで変更のsyslog通知が使用可能かどうかを検証します。デバイスがsyslogによるリアルタイム変更検出機能をサポートしていない場合は、ステップ4に進みます。
4. NAによるリアルタイム変更検出機能は、AAAログインという方法でも実行できます。AAA変更検出機能を有効にしているかどうかを確認します。詳細については、「[\[構成管理\]ページのフィールド](#)」（36ページ）を参照してください。AAAを使用している場合は、デバイスがAAAによるリアルタイム変更検出機能をサポートしているかどうかを確認してください。



## セッションログ

自動タスクで問題となるのは、自動化そのものではなく、自動タスクに失敗した場合に失敗の原因を突き止めることです。NAには、失敗の原因とその解決策を迅速に識別するのに役立つ、きめ細かなトラブルシューティング機能があります。

NAでは、すべてのデバイスタスクから詳細なデバイスセッションログを作成します。このログにより、NAがデバイスに送信する情報やデバイスの応答方法を調べることができます。

1. NAにログインします。
2. [デバイス]メニューで[デバイスタスク]を選択し、[コマンドスクリプトの実行]をクリックします。[タスクの新規作成 - コマンドスクリプトの実行]ページが開きます。
3. [適用先]フィールドで、設定の変更を許可されているデバイスのホスト名またはIPアドレスを入力します。
4. [タスクオプション]-[セッションログ]で、[完全なデバイスセッションログを格納]ボックスをオンにします。
5. [タスクオプション]-[実行するコマンドスクリプト]で、実行するコマンドスクリプトをドロップダウンメニューから選択します。
6. 実行モードを指定します。たとえばIOSデバイスの場合は、[Cisco IOS Configuration]を選択します。
7. デバイスに送信するコマンドを入力します。
8. [タスクの保存]ボタンをクリックします。

タスクを実行すると、NA<->デバイス間の対話が出力されます。これにより次の点を判断できます。

- NAからデバイスに送信された情報。
- NAがデバイスから受け取ることを予期していた情報。
- NAがデバイスから実際に受信した情報。

## SWIM エラーメッセージ

メッセージID	エラーメッセージ	推定原因	取り得るアクション
SWIM0019	Could not perform Image recommendation for the selected device(s) because of insufficient data. (データが十分ではないため、選択したデバイスのイメージ推奨を実行できませんでした。)	データベースからイメージ情報を取得できませんでした。	インベントリ収集が成功していることを確認してください。選択したデバイスについて、OS分析タスクを実行し、ソフトウェアアップグレード推奨を起動してください。
SWIM0089	Could not perform Image Import from Cisco.com on the selected device(s). (選択したデバイス上で、Cisco.comからのイメージインポートを実行できませんでした。)	デバイスに対応していない Cisco.comからのイメージを追加しようとしています。これは、Cisco.comがデバイスプラットフォームをサポートリストから検出できなかったためです。	なし
SWIM0092	Error while fetching inventory information for the device. (デバイスのインベントリ情報の取得中にエラーが発生しました。)	このデバイスを使用する権限があること、およびこのデバイスのインベントリが完了していることを確認してください。	選択したデバイスについて、OS分析タスクを実行してください。
SWIM0093	Could not get Image information from Cisco.com (Cisco.comからイメージ情報を取得できませんでした。)	CWNCM Serverから Cisco.com に接続できませんでした。これは、Cisco.com資格情報が正しくないか、プロキシ構成が存在しないことが原因です。	Cisco.com 資格情報が正しいことを確認してください。正しい場合、プロキシサーバが正しいプロキシ情報で構成されていることを確認してください。  プロキシを構成するには、CWNCM ホームページにアクセスし、[Change Password (パスワードの変更)] をクリック、>[Cisco.com Proxy for Credential Type (クレデンシャルタイプの Cisco.com プロキシ)] を選択して、ユーザー名とパスワードを入力します。
SWIM0125	An unexpected error has occurred. (予期しないエラーが発生しました。) Contact Cisco support and attach the SWIMNG_server.log file. (Cisco サポートに SWIMNG_server.log ファイルを添付して問い合わせてください。)	なし	以下のフォルダ配下にあるログを添付して、Cisco テクニカルアシスタンスセンター (TAC) に問い合わせてください。Windows : <CWNCMのインストールフォルダ> \server\ext\swim\log\SWIMNG_server.log Solaris & Linux : <CWNCMのインストールフォルダ>\server\ext\swim\log\SWIMNG_server.log
SWIM0126	予期しないエラーが発生しました。 Cisco サポートに SWIMNG_server.log ファイルを添付して問い合わせてください。	なし	以下のフォルダ配下にあるログを添付して、Cisco テクニカルアシスタンスセンター (TAC) に問い合わせてください。Windows : <CWNCMのインストールフォルダ> \server\ext\swim\log\SWIMNG_server.log Solaris & Linux : <CWNCMのインストールフォルダ>\server\ext\swim\log\SWIMNG_server.log
SWIM0155	User is not authorized to download crypto image from Cisco.com (ユーザには、Cisco.comから暗号イメージをダウンロードする権限がありません。)	ユーザには、Cisco.comから暗号イメージをダウンロードする権限がありません。	Cisco.com にアクセスし、暗号化に関する契約書に同意してください。

メッセージID	エラーメッセージ	推定原因	取り得るアクション
SWIM0156	No response stream was obtained for the download request. (ダウンロード要求に対する応答ストリームが得られません。)	ダウンロード要求に対する応答ストリームが得られません。	後で再度試みるか、Ciscocomからイメージを直接ダウンロードして、システムに追加してください。
SWIM1003	SNMP Agent does not support the required instrumentation to get information about the Flash File system. (SNMPエージェントは、Flash ファイルシステムに関する情報を得るのに必要なインスツルメンテーションをサポートしていません。)	デバイス上のSNMPエージェントはCISCO-FLASH-MIB/OLD-CISCO-FLASH-MIBをサポートしません。	デバイス上に動作しているイメージバージョンについては、これらのMIBに関連する既知のバグを確認してください。
SWIM1004	Cannot get details about the Flash File system on the device. (デバイス上のFlash ファイルシステムに関する詳細を取得できません。)	デバイス上に、問題のあるMIBの実装が存在する可能性があります。	実行中のイメージバージョンの既知の問題については、Cisco.comを確認してください。
SWIM1005	Flash Device or Partition does not exist on the device. (デバイス上にFlash デバイス、またはパーティションが存在しません。)	デバイス上のインベントリデータが最新ではないか、選択したFlash デバイスやパーティションが正しくありません。	選択したデバイスについて、OS 分析タスクを実行し、ソフトウェアアップグレード推奨を起動してください。
SWIM1006	Flash Partition does not exist on the device. (Flash パーティションが存在しません。)	デバイス上のインベントリデータが最新ではないか、選択したFlash パーティションが正しくありません。	選択したデバイスについて、OS 分析タスクを実行し、ソフトウェアアップグレード推奨を起動してください。
SWIM1027	Error while fetching inventory information. (インベントリ情報の取得中にエラーが発生しました。)	選択したタスクに必要なデータが不完全であるか、インベントリに存在しません。	選択したデバイスについて、OS 分析タスクを実行し、ソフトウェアアップグレード推奨を起動してください。
SWIM1029	Cannot get the required inventory information for the device. (デバイスの必須インベントリ情報を取得できません。)	デバイスのインベントリ収集がないか、デバイスが応答しません。	選択したデバイスについて、OS 分析タスクを実行し、ソフトウェアアップグレード推奨を起動してください。
SWIM1030	This is a Run From Flash (RFF) device, but the application cannot find the running image on the Flash. (これはRun From Flash (RFF) デバイスですが、アプリケーションはFlash上にランニングイメージを検出できません。)	インベントリが更新されていないか、Flash ファイルがFlashから削除されています。	選択したデバイスについて、OS 分析タスクを実行し、ソフトウェアアップグレード推奨を起動してください。
SWIM1031	実行中のソフトウェアのための候補イメージが見つかりません。	自分の環境設定にCisco.comが含まれていないか、ソフトウェアリポジトリやCisco.comに利用できるイメージが存在しません。	[管理]>[ユーザ]>をクリックし、自分のユーザ名を選択してその[権限]をクリックします。>[自分の環境設定]を確認するか、ソフトウェアリポジトリにイメージを追加します。ソフトウェアアップグレード推奨を再起動してください。
SWIM1032	Images obtained for Recommendation do not meet the hardware and software requirements of the selected device. (推奨用に得られたイメージが、選択したドライブのハードウェア、およびソフトウェアの要件を満たしません。)	選択した[自分の環境設定]を基準にして候補イメージがフィルタされたか、候補イメージが、デバイス上で実行するためのFlash/RAM/BootROMの要件を満たしません。	[管理]>[ユーザ]>をクリックし、自分のユーザ名を選択してその[権限]をクリックします。>[自分の環境設定]を確認するかソフトウェアリポジトリにイメージを追加します。ソフトウェアアップグレード推奨を再起動してください。

メッセージID	エラーメッセージ	推定原因	取り得るアクション
SWIM1033	Cannot find the Best-fit image for the device by applying compatibility checks. (互換性確認を適用して、デバイスの最適イメージを見つけられません。)	選択した[自分の環境設定]を基準にして候補イメージがフィルタされたか、候補イメージが、デバイス上で実行するためのFlash/RAM/BootROMの要件を満たしません。	[管理]>[ユーザ]をクリックし、自分のユーザー名を選択してその[権限]をクリックします。>[自分の環境設定]を確認するか、ソフトウェアリポジトリにイメージを追加します。ソフトウェアアップグレード推奨を再起動してください。
SWIM1034	No applicable images found for the device from the configured image sources. (構成イメージソースからデバイスに適用できるイメージが検出されませんでした。)	自分の環境設定にCisco.comが含まれていないか、ソフトウェアリポジトリやCisco.comに利用できるイメージが存在しません。	[管理]>[ユーザ]をクリックし、自分のユーザー名を選択してその[権限]をクリックします。>[自分の環境設定]を確認するか、ソフトウェアリポジトリにイメージを追加します。ソフトウェアアップグレード推奨を再起動してください。
SWIM1035	Error while performing Recommendation option. (推奨オプション実行中にエラーが発生しました。)	なし	Runtime error encountered while filtering images caused by a problem with a running image on the device. (イメージのフィルタ中に、デバイス上のランニングイメージによる問題が原因でランタイムエラーが発生しました。)
SWIM1036	Runtime error while performing Recommendation. (推奨オプション実行中にランタイムエラーが発生しました。)	なし	操作を再試行してください。問題が出続ける場合は、Ciscoテクニカルアシスタンスセンター (TAC) にデバッグログを送信してください。デバッグログの位置を以下に挙げます。Windows : <CWNCMのインストールフォルダ> \server\ext\swim\log\SWIMNG_server.log Solaris & Linux : <CWNCMのインストールフォルダ>/server/ext/swim/log/SWIMNG_server.log
SWIM1037	Error while fetching inventory information. (Flash パーティション情報の取得中にエラーが発生しました。)	Flash情報をインベントリから取得できないか、デバイス上のランニングイメージに問題があります。	操作を再試行してください。問題が出続ける場合は、Ciscoテクニカルアシスタンスセンター (TAC) にデバッグログを送信してください。デバッグログの位置を以下に挙げます。Windows : <CWNCMのインストールフォルダ> \server\ext\swim\log\SWIMNG_server.log Solaris & Linux : <CWNCMのインストールフォルダ>/server/ext/swim/log/SWIMNG_server.log
SWIM1038	No Read-Write Partition found on the device. (デバイス上に読み取り専用パーティションが存在しません。)	なし	読み取り専用パーティションのFlashデバイスをインストールして、インベントリを更新してください。
SWIM1039	No Storage Recommendation is made for the device. (デバイスの記憶域推奨がありません。)	選択したデバイスには、イメージをコピーするのに十分な空きサイズのパーティションが存在しない可能性があります。	選択したデバイスに、イメージをコピーするのに十分な空きサイズのパーティションが存在することを確認してください。

メッセージID	エラーメッセージ	推定原因	取り得るアクション
SWIM1040	Cannot get the Flash information for the device. (デバイスのFlash情報を取得できません。)	インベントリからFlash情報を取得できないか、デバイス上のランニングイメージに問題があります。	選択したデバイスについて、OS分析タスクを実行し、ソフトウェアアップグレード推奨を起動してください。問題が出続ける場合は、実行中のイメージバージョンの既知の問題については、Cisco.comを確認してください。
SWIM1041	This device upgrade requires opening an SSH/Telnet connection to the device. (このデバイスのアップグレードには、デバイスにSSH/Telnet接続を開く必要があります。)	デバイスの Enable password が正しく構成されていません。	デバイスに対して適切な SSH/Telnet パスワードが構成されていることを確認してください。
SWIM1042	The amount of Bootflash on the device may not be enough to run the selected image. (デバイスの Bootflash の合計が、選択したイメージを実行するのに十分ではない可能性があります。)	デバイスの Bootflash の合計が、選択したイメージを実行するのに十分ではない可能性があります。	なし
SWIM1043	Runtime error while performing Bootloader image verification. (Bootloader イメージ確認の実行中にランタイムエラーが発生しました。)	選択したイメージバージョンは、標準バージョンフォーマットではない可能性があります。	操作を再試行してください。問題が出続ける場合は、Cisco テクニカルアシスタンスセンター (TAC) にデバッグログを送信してください。デバッグログの位置を以下に挙げます。 Windows : <CWNCM のインストールフォルダ> \\server\ext\swim\log\SWIMNG_server.log Solaris & Linux : <CWNCM のインストールフォルダ>/server/ext/swim/log/SWIMNG_server.log
SWIM1044	Bootflash partition will be erased before copying new image. (新規イメージをコピーする前に Bootflash パーティションが削除されます。)	選択した Bootloader イメージは、Bootflash の空き領域に適合しません。	他にあれば、別の Bootloader を選択してください。
SWIM1046	Selected software does not fit in selected Flash partition. (選択したソフトウェアは、選択した Flash パーティションに適合しません。)	選択したソフトウェアイメージは、Bootflash の空き領域に適合しません。	アップグレードには別の Flash パーティションを選択してください。
SWIM1048	The system software that is active on the device, cannot run the selected image. (デバイス上でアクティブなシステムソフトウェアは、選択したイメージを実行できません。)	デバイス上でアクティブなシステムソフトウェアは、選択したイメージと互換性がありません。	現在のシステムソフトウェアでアップグレード可能である別のイメージを選択するか、システムソフトウェアをソフトウェアバージョンにアップグレードしてください。
SWIM1049	The selected image requires Flash to be erased during image upgrade. (選択したイメージは、イメージのアップグレード中に Flash を削除する必要があります。)	なし	必要なバックアップを行っていることを確認してください。
SWIM1050	Read-Write SNMP community string is not available for the device. (デバイスの読み取り専用 SNMP コミュニティ文字列が利用できません。)	デバイスの読み書き SNMP コミュニティ文字列が利用できません。	デバイスの読み書きコミュニティ文字列を追加してください。
SWIM1051	Credential information cannot be obtained for the device. (デバイスのクレデンシャル情報を取得できません。)	デバイスが CWNCM サーバで管理されていないか、デバイスクレデンシャルが正しくない、またはデバイスアクセス権限が不十分です。	なし

メッセージID	エラーメッセージ	推定原因	取り得るアクション
SWIM1052	Enable password is not configured for the device. (デバイスのEnable passwordが構成されていません。)	Run From Flash (RFF)パーティションソフトウェアのアップグレードの場合、Enable passwordを構成する必要があります。	デバイスのEnable passwordを構成してください。
SWIM1053	Selected MICA Image is the same as the running image on the device. (選択したMICAイメージが、デバイス上のランニングイメージと同一です。)	デバイスのイメージのソフトウェアバージョンは最新です。	なし
SWIM1054	Error while checking the Telnet credential of the device. (デバイスのTelnetクレデンシャルの確認中にエラーが発生しました。)	なし	デバイスのTelnetクレデンシャルが正しいことを確認してください。
SWIM1055	Selected Flash partition is Read-Only. (選択したFlashパーティションが読み取り専用です。)	Flashパーティションが書き込み可能ではないか、読み書きパーティションが存在しません。	読み書きパーティションが存在することを確認してください。Flashパーティションを書き込み可能に設定してください。
SWIM1056	The method to update the software on the selected storage device is unknown. (選択した記憶域デバイス上のソフトウェアをアップグレードする方法が不明です。)	なし	他にあれば、別のFlashパーティションを選択してください。
SWIM1057	The device will be put into Rxboot mode for the image upgrade. (イメージのアップグレードで、デバイスはRxbootモードになります。)	なし	他にあれば、システムソフトウェア用の別のFlashデバイスを選択してください。
SWIM1058	The selected software version has some known issues in the Flash MIB options that make this application unable to perform software upgrades on the device. (選択したソフトウェアバージョンには、Flash MIBオプションで、このアプリケーションがデバイス上でソフトウェアアップグレードを実行できなくなる、いくつかの既知の問題があります。)	なし	可能であれば、デバイスを手動でアップグレードするか、最新ソフトウェアバージョンを選択してください。
SWIM1059	Ensure Dial Shelf runs a compatible software image with the newly loaded Router Shelf software image. (Dial Shelfが、新しくロードされたRouter Shelfソフトウェアイメージで互換ソフトウェアイメージを実行していることを確認してください。)	Router shelf ソフトウェアイメージが、Dial Shelf ソフトウェアイメージと互換ではありません。	Router Shelf ソフトウェアイメージのリリースノートを参照して、現在のDial Shelfソフトウェアが互換であることを確認してください。互換ではない場合、Dial Shelfソフトウェアをアップグレードしてください。
SWIM1060	Cannot obtain the file size of the selected image. (選択したイメージのファイルサイズを取得できません。)	選択したイメージは、Cisco.comから削除されている可能性があります。	アップグレード用に他のイメージを選択してください。
SWIM1062	Selected image is already running on the device. (選択したイメージは、既にデバイス上で実行されています。)	なし	このイメージが、デバイスをアップグレードするためのイメージであることを確認してください。
SWIM1063	Minimum RAM requirement of the selected image cannot be determined. (選択したイメージの最小RAM要件を判断できません。)	デバイス上で利用できるRAMが、このイメージを有効にするのに十分ではない可能性があります。	なし
SWIM1064	RAM available on the device may not be large enough to activate the selected image. (デバイス上で利用できるRAMが、選択したイメージを有効にするのに十分ではない可能性があります。)	デバイス上で利用できるRAMが、選択したイメージを有効にするのに十分ではない可能性があります。	他のイメージを選択するか、デバイス上のRAMをアップグレードしてください。



メッセージID	エラーメッセージ	推定原因	取り得るアクション
SWIM1065	RAM available on the device may not be enough to activate the selected image. (デバイス上で利用できるRAMが、選択したイメージを有効にするのに十分ではない可能性があります。)	デバイス上で利用できるRAMが、選択したイメージを有効にするのに十分ではない可能性があります。	アップグレード用に他のイメージを選択してください。
SWIM1067	Runtime error while performing verification of the selected image. (選択したイメージの確認を実行中にランタイムエラーが発生しました。)	なし	アップグレード用に他のイメージを選択してください。問題が出続ける場合は、Cisco テクニカルアシスタンスセンター (TAC) にデバッグログを送信してください。デバッグログの位置を以下に挙げます。Windows : <CWNCMのインストールフォルダ> \server\ext\swim\log\SWIMNG_server.log Solaris & Linux : <CWNCMのインストールフォルダ>/server/ext/swim/log/SWIMNG_server.log
SWIM1068	Selected image does not have the minimum system software version required for the upgrade. (選択したイメージに、アップグレードに必要な最小システムソフトウェアバージョンがありません。)	選択したイメージに、アップグレードに必要な最小システムソフトウェアバージョンがありません。	バージョンが11.0より大きい他のイメージを選択してください。
SWIM1069	Feature subset of the selected image is a subset or equal to running software feature set. (選択したイメージの機能サブセットが、ランニングソフトウェアイメージセットのサブセット、またはそのものです。)	選択したイメージの機能サブセットが、ランニングソフトウェアイメージセットのサブセット、またはそのものです。	他のイメージを選択してください。
SWIM1070	Feature subset of the running image cannot be determined. (ランニングイメージの機能サブセットを判断できません。)	選択したイメージの機能サブセットが、ランニングソフトウェアイメージセットのサブセット、またはそのものです。	他のイメージを選択してください。
SWIM1075	Cannot find an image that is newer and can fit on the Bootflash. (より新しい、Bootflashに適合するイメージを見つけられません。)	なし	ランニングイメージバージョンよりも大きいバージョンを持ち、Bootflashに適合するBootloader イメージをソフトウェアリポジトリに追加してください。
SWIM1076	Cannot find a Read-Write Boot partition on the device. (デバイス上に読み書きパーティションが存在しません。)	デバイス上に読み書きブートパーティションがありません。	デバイスに読み書き Bootflash を挿入し、インベントリを更新してください。
SWIM1077	Cannot find a Bootflash partition for the Bootloader image. (Bootloader イメージ用の Bootflash パーティションがありません。)	Bootloader イメージ用の Bootflash パーティションがありません。	デバイスに読み書き Bootflash を挿入し、インベントリを更新してください。
SWIM1079	Image version cannot be compared. (イメージバージョンを比較できません。)	両イメージのイメージフォーマットに、比較するための互換性がない可能性があります。	バージョンのフォーマットを確認してください。アップグレード用に他のイメージを選択してください。

メッセージID	エラーメッセージ	推定原因	取り得るアクション
SWIM1082	Runtime error while comparing Modem Image. (モデムイメージを比較中にランタイムエラーが発生しました。)	誤ったモデムイメージを比較用 に選択したか、モデムイメージの フォーマットに互換性がありま せん。	アップグレード用に他のモデムイメージを 選択してください。 問題が出続ける場合は、Cisco テクニカルア シスタンスセンター (TAC) にデバッグログ を送信してください。デバッグログの位置を 以下に挙げます。Windows : <CWNCMのインストールフォルダ> \\server\ext\swim\log\SWIMNG_server.log Solaris & Linux : <CWNCMのインストールフォルダ>/server/ ext/swim/log/SWIMNG_server.log
SWIM1083	Cannot find an image that is newer and fits in the Flash. (より新しい、Flash に適合するイメージを見つけられませ ん。)	なし	ソフトウェアリポジトリに他のイメージを 追加して、操作を再試行してください。
SWIM1084	Cannot find a Minimum Flash Requirement for the device. (デバイ スの最小Flash要件を見つけられませ ん。)	デバイス上の空きFlash領域が、選 択したイメージには十分ではない 可能性があります。	イメージがデバイスに適合することを確認 してください。
SWIM1085	The MinFlash Attribute is unknown for the selected image. (選択したイメ ージのMinFlash属性が不明です。)	選択したイメージは、選択した パーティションに適合しません。	イメージが選択したパーティションに適合 することを確認するか、他のイメージを選択 してください。
SWIM1087	Cannot get the device representation. (デバイス表現を取得できません。)	インベントリからデバイス詳細を 取得できません。	ログを取得して、Cisco テクニカルアシスタ ンスセンター (TAC) に問い合わせください。 デバッグログの位置を以下に挙げます。 Windows : <CWNCMのインストールフォル ダ>\\server\ext\swim\log\SWIMNG_ server.log Solaris & Linux : <CWNCMのインストール フォルダ>/server/ext/swim/log/SWIMNG_ server.log
SWIM1092	Selected image does not have the minimum system software version required for system upgrade. (選択し たイメージに、システムアップグレー ドに必要な最小システムソフトウェア バージョンがありません。)	なし	サポートされる最低バージョン以降のバー ジョンであるイメージを選択してください。 Cisco IOS ソフトウェアの互換対応表につい ては、マニュアルを参照してください。
SWIM1093	Cannot get Chassis Information from the inventory. (インベントリから シャーシ情報を取得できません。)	なし	選択したデバイスについて、OS 分析タスク を実行し、ソフトウェアアップグレード推奨 を起動してください。
SWIM1094	SNMP-V3 parameters is incorrect or not available for the device. (SNMP- V3パラメータが正しくないか、この デバイスで利用できません。)	これは、以下の条件のいずれかに より発生した可能性があります。 <ul style="list-style-type: none"> <li>• SNMP-V3 パスワードが誤って 構成されている</li> <li>• SNMP-V3 アルゴリズムが誤っ て構成されている</li> <li>• デバイスの SNMP-V3 エンジン IDが構成されていない。</li> </ul>	デバイスのSNMP-V3パスワード、SNMP-V3 アルゴリズム、およびSNMP-V3エンジンID が構成されていることを確認してください。
SWIM1095	Error while checking the SNMP-V3 user name in the device context. (デバ イスコンテキストのSNMP-V3ユーザ 名を確認中にエラーが発生しました。)	なし	デバイスのSNMP-V3クレデンシャルを更新 してください。 選択したデバイスについて、OS 分析タスク を実行し、ソフトウェアアップグレード推奨 を起動してください。



メッセージID	エラーメッセージ	推定原因	取り得るアクション
SWIM1097	Selected Bootloader image is a lower version than the version of the Bootloader running on the device. (選択したBootloaderイメージが、デバイスで実行中のBootloaderのバージョン未満です。)	デバイス上で実行中のBootloaderイメージバージョンは最新です。	より高いバージョンがアップグレード用にあるかどうかを確認してください。
SWIM1098	The selected image is lower than the running image on the device. (選択したイメージが、デバイス上のランニングイメージ未満です。)	デバイス上で実行中のイメージバージョンは最新です。	デバイスソフトウェアアップグレード用により高いイメージを選択してください(変更は必要ありません)。
SWIM1099	Image Upgrade procedure may revert to the SSH/Telnet-based approach, based on the MIB instrumentation on the running image. (ランニングイメージのMIBインストールメンテションを基に、イメージアップグレード手順はSSH/Telnetベースのアプローチに戻る可能性があります。)	デバイスのSSH/Telnetパスワードが構成されていない可能性があります。	デバイスに対して適切なSSH/Telnetパスワードが構成されていることを確認してください。
SWIM1100	Cannot find SNMP-V2 Read-Write Community String for the device. (デバイスのSNMP-V2読み書きコミュニティ文字列を見つけられません。)	デバイスのSNMP-V2クレデンシャルが正しく構成されていない可能性があります。	デバイスのSNMP-V2クレデンシャルが正しく構成されていることを確認してください。
SWIM1101	This Device Upgrade requires opening an SSH/Telnet connection to the device. (このデバイスのアップグレードには、デバイスにSSH/Telnet接続を開く必要があります。)	デバイスのEnable passwordが構成されていません。	デバイスに対して適切なSSH/Telnetパスワードが構成されていることを確認してください。
SWIM1102	This Device Upgrade requires opening a SSH/Telnet connection to the device. (このデバイスのアップグレードには、デバイスにSSH/Telnet接続を開く必要があります。)	デバイスのクレデンシャルを確認中にエラーが発生しました。	デバイスに対して適切なSSH/Telnetパスワードが構成されていることを確認してください。
SWIM1103	Selected image may not be compatible to the device. (選択したイメージは、デバイスに互換ではない可能性があります。)	イメージは、デバイス上のランニングイメージと同じデバイスファミリに属します。ただし、イメージは非互換であると識別されます。	Cisco.com マニュアルを確認して、選択したイメージの注意事項が挙げられているかどうかを確認してください。
SWIM1105	Image status for the selected image cannot be determined. (選択したイメージのイメージステータスを判定できません。)	選択したイメージは、DEFERREDステータスにある可能性があります。	イメージがDEFERREDステータスにないことを確認してください。イメージをアップグレードする前に、Cisco.comで該当マニュアルを参照してください。
SWIM1106	Image selected for upgrade is compressed in .tar format. (アップグレード用に選択したイメージは、.tarフォーマットで圧縮されています。) Flash will be overwritten while upgrading the image. (イメージのアップグレード中にFlashは上書きされます。)	なし	アップグレード前に、必要なバックアップジョブを完了していることを確認してください。
SWIM1107	This option requires <i>devicename</i> data in the inventory. (このオプションでは、インベントリに <i>devicename</i> データが必要です。)	必要なデバイス情報がインベントリに存在しません。	選択したデバイスについて、OS分析タスクを実行し、ソフトウェアアップグレード推奨を起動してください。  次のページに続く
SWIM1109	Image status for the selected image is either Deferred or Not Supported. (選択したイメージのイメージステータスが、DEFERREDであるかNOT SUPPORTEDです。)	選択したイメージのイメージステータスが、DEFERREDであるかNOT SUPPORTEDです。	CWNCM アプリケーションがイメージをサポートしていることを確認してください。イメージをアップグレードする前に、Cisco.comでマニュアルを参照してください。

メッセージID	エラーメッセージ	推定原因	取り得るアクション
SWIM1111	The available free space is not enough for upgrading this type of image. (このタイプのイメージをアップグレードするのに、十分な空き領域がありません。)	イメージのアップグレードに十分な空き領域がありません。	他のイメージを選択するか、領域を解放してください。インベントリを更新して、ジョブを再試行してください。
SWIM1112	This module can be upgraded if managed independently. (独立して管理している場合、このモジュールをアップグレードできます。)	このモジュールは、独立したデバイスとして管理している場合のみアップグレードできます。	このモジュールに独立したIPアドレスを割り当ててください。モジュールを独立デバイスとして管理し、そのデバイスを選択してこのモジュールをアップグレードしてください。
SWIM1116	Read-Write SNMP community string cannot be fetched from the Device Context. (読み書きSNMPコミュニティ文字列をデバイスコンテキストから取得できません。)	デバイスの読み書きコミュニティ文字列が利用できません。	デバイスの読み書きコミュニティ文字列を追加してください。
SWIM1118	Selected image has a lower version than the version of the running image. (選択したイメージのバージョンは、ランニングイメージのバージョンよりも低い。)	選択したイメージのバージョンは、ランニングイメージのバージョンよりも前のバージョンです。	なし
SWIM1119	Telnet credentials are not present for this device. (このデバイスのTelnetクレデンシャルが存在しません。) There was an error while checking the credentials for the device. (デバイスのクレデンシャルを確認中にエラーが発生しました。)	SSH/Telnet パスワードが正しく構成されていない可能性があります。	デバイスに対して適切なSSH/Telnet パスワードが構成されていることを確認してください。
SWIM1120	Cannot obtain the sysObjectID of the device. (デバイスのsysObjectIDを取得できません。)	なし	選択したデバイスについて、OS分析タスクを実行してください。問題が出続ける場合は、Cisco テクニカルアシスタンスセンター (TAC) にデバッグログを送信してください。デバッグログの位置を以下に挙げます。 Windows : <CWNCMのインストールフォルダ> \\server\ext\swim\log\SWIMNG_server.log Solaris & Linux : <CWNCMのインストールフォルダ>/server/ext/swim/log/SWIMNG_server.log
SWIM1122	Runtime error found during verification. (確認中にランタイムエラーが見つかりました。)	なし	操作を再試行してください。問題が出続ける場合は、Cisco テクニカルアシスタンスセンター (TAC) にデバッグログを送信してください。デバッグログの位置を以下に挙げます。 Windows : <CWNCMのインストールフォルダ> \\server\ext\swim\log\SWIMNG_server.log Solaris & Linux : <CWNCMのインストールフォルダ>/server/ext/swim/log/SWIMNG_server.log
SWIM1123	Telnet credentials are not present for this device. (このデバイスのTelnet ユーザ名が存在しません。)	なし	このデバイスのプライマリユーザ名が構成されているかどうかを確認してください。
SWIM1139	Select any available boot flash partition, for bootldr upgrade. (bootldr アップグレード用に任意のブートFlashパーティションを選択してください。) bootldrのアップグレードにブートflashを使用することを推奨します。	これは、ユーザが配布用にBootloader イメージを選択し、bootflash以外の記憶域の場所を選択した場合に発生します。	bootldr アップグレード用に任意のブートFlashパーティションを選択してください。

メッセージID	エラーメッセージ	推定原因	取り得るアクション
SWIM1162	Error when recommending image for the device. (デバイスのイメージを推奨中にエラーが発生しました。)	イメージソフトウェア推奨は、インベントリで収集したデバイスROM、RAM、およびFlashに基づきます。 デバイスにハードウェア故障（点滅）が発生すると、このデバイスはインベントリで利用できなくなります。	ハードウェア障害、またはデバイスソフトウェアのバグについて、デバイスを確認してください。 選択したデバイスについて、OS分析タスクを実行し、ソフトウェアアップグレード推奨を起動してください。問題が出続ける場合は、Cisco テクニカルアシスタンスセンター (TAC) にデバッグログを送信してください。デバッグログの位置を以下に挙げます。 Windows : <CWNCMのインストールフォルダ> \\server \ext\swim\log\SWIMNG_ server.log Solaris & Linux : <CWNCMのインストールフォルダ>/server/ext/swim/log/SWIMNG_ server.log
SWIM129	Selected image does not fit on the free Flash size on the device. (選択したイメージがデバイス上の空きFlashサイズに適合しません。)	次のいずれかが原因です。 アップグレード用にブートローダーイメージを選択した（それと一緒にシステムソフトウェアイメージを選択していない）か、ブートローダーイメージをコピーするために記憶域の位置を削除していないかです。	システムソフトウェアをアップグレード用に選択していないため、ランニングシステムソフトウェアは選択した記憶域パーティションに存在しません。ランニングシステムソフトウェアをバックアップし、ジョブが失敗したときにバックアップイメージからデバイスがブートするようにしてください。
SWIM1501	Supervisor cannot be downgraded to an image version less than 4.1(1). (Supervisorは4.1 (1) 未満のイメージバージョンにダウングレードできません。)	これは、4.1 (1) 未満のCATOSイメージを配布しようとすると発生します。	ダウングレードすると、デバイスが構成を失う場合があります。 より高いバージョンを使用してください。
SWIM1525	Unknown package type. (パッケージタイプが不明です。)	なし	選択したモジュールはサポートされていません。
SWIM1529	There is no module information available in the inventory for <i>devicename</i> . (インベントリに <i>devicename</i> のモジュール情報がありません。)	<i>devicename</i> のインベントリのモジュール情報はありません。	選択したデバイスについて、OS分析タスクを実行してください。
SWIM1530	Storage Recommendation is not supported for the Module <i>modulename</i> . (モジュール <i>modulename</i> では記憶域推奨はサポートされていません。)	なし	このモジュールでは記憶域推奨はサポートされていません。モジュールの販売が終了しているか、製品寿命である可能性があります。
SWIM1532	No read-write partition exists on the device to accommodate the selected image. (デバイス上に、選択したイメージを格納するための読み書きパーティションが存在しません。)	なし	十分な空き領域を作成してください。
SWIM1542	Minimum supported version for Supervisor is 3.8. (Supervisorの最小サポートバージョンは3.8です。)	なし	アップグレードするには、より高いバージョンのイメージを選択してください。
SWIM1543	Selected image has the same or a lower version than the version of the running image. (選択したイメージのバージョンは、ランニングイメージのバージョン以下です。)	選択したイメージのバージョンは、ランニングイメージのバージョン以下です。	なし
SWIM1546	The NVRAM size on the device may not be large enough to run the image. (デバイス上のNVRAMのサイズが、イメージを実行するのに十分な大きさではありません。)	デバイス上のNVRAMのサイズが、イメージを実行するのに十分な大きさではありません。	他のイメージを選択するか、デバイス上のNVRAMをアップグレードしてから、アップグレードオプションを再試行してください。

メッセージID	エラーメッセージ	推定原因	取り得るアクション
SWIM1547	Available NVRAM size on the selected image cannot be determined. (選択したイメージの利用可能なNVRAMを判断できません。)	モジュール上で利用できる RAM が、選択したイメージを格納するのに十分ではない可能性があります。	選択したイメージを実行するには、モジュールに十分なNVRAMがあることを確認してください。それ以外の場合は、他のイメージを選択するか、モジュール上のRAMをアップグレードしてください。
SWIM1548	There are no software requirements found for the selected image. (選択したイメージのソフトウェア要件が見つかりません。)	なし	他のイメージを選択してください。
SWIM1549	Verify that the new software selected is compatible. (選択した新しいソフトウェアが互換であることを確認してください。)	Software Managementは、ATMソフトウェアで機能を判断できません。	新しいソフトウェアのリリースノートを確認して、古いソフトウェアのすべての機能が新しいソフトウェアで利用できることを確認してください。
SWIM1554	The selected image cannot be used to upgrade the device. (選択したイメージを使用して、デバイスをアップグレードできません。)	デバイスには、選択したイメージを実行できるモジュールがありません。	他のイメージを選択してください。
SWIM1560	Slot number corresponding to the module cannot be got from inventory. (モジュールに対応するスロット番号をインベントリから取得できません。)	なし	選択したデバイスについて、OS分析タスクを実行し、ソフトウェアアップグレード推奨を起動してください。
SWIM2001	Telnet error while connecting to the device. (デバイスに接続中にTelnetエラーが発生しました。) デバイス Device に接続できません。	デバイスのアクセス情報が正しくありません。	デバイスのユーザ名とパスワードを確認してから、再試行してください。
SWIM2002	Cannot get details about Flash File system on the device. (デバイス上のFlashファイルシステムに関する詳細を取得できません。)	Flashデバイスが利用できないか、Flash情報フォーマットが変更されています。	Flashを確認して、OS分析タスクを実行してください。
SWIM3501	Cannot fetch device credentials for the selected device. (選択したデバイスのデバイスクレデンシャルを取得できません。)	デバイスのクレデンシャルが正しく構成されていない可能性があります。	このデバイスのクレデンシャルが構成されているかどうかを確認してください。
SWIM3703	Selected image does not have the minimum system software version required for system upgrade. (選択したイメージに、システムアップグレードに必要な最小システムソフトウェアバージョンがありません。)	なし	バージョンが11.3 (0) より大きい他のイメージを選択してください。
SWIM5001	Cannot connect to the device <i>devicename</i> using protocol. (プロトコルを使用してデバイス <i>devicename</i> に接続できません。)	デバイスは到達不可能であるか、デバイスのアクセス情報が正しくありません。	デバイスが到達可能であり、クレデンシャルが正しいことを確認してください。
SWIM4800	The version running on the device is less than the minimum supported version. (デバイスを実行するバージョンが、最低サポートバージョン未満です。)	なし	最低サポートバージョン以上にまで、デバイスを手動でアップグレードしてください。

## 第20章：ACLの扱い方

### トピックの参照先リスト

トピック	参照先：
はじめに	<a href="#">「はじめに」</a> （694 ページ）
ACL の表示	<a href="#">「ACL の表示」</a> （695 ページ）
コマンドスクリプトの実行	<a href="#">「コマンドスクリプトの実行」</a> （699 ページ）
ACL の作成	<a href="#">「ACL の作成」</a> （700 ページ）
ACL アプリケーションの変更	<a href="#">「ACL アプリケーションの変更」</a> （701 ページ）
ACL 行の一括挿入	<a href="#">「ACL 行の一括挿入」</a> （702 ページ）
ACL 行の一括削除	<a href="#">「ACL 行の一括削除」</a> （702 ページ）
ACL へのコメントの追加と ACL ハンドルの作成	<a href="#">「ACL へのコメント追加と ACL ハンドルの作成」</a> （704 ページ）
ACL テンプレートの作成	<a href="#">「ACL テンプレートの作成」</a> （705 ページ）
ACL の編集	<a href="#">「ACL の編集」</a> （706 ページ）
ACL の削除	<a href="#">「ACL の削除」</a> （707 ページ）

## はじめに

アクセス制御リスト（ACL）は、IP トラフィックフローを制御するために多くの組織で使用されています。主にセキュリティを強化するために使用されますが、公開されている Web サイトからのストリームオーディオやビデオなど、広帯域を使用するシステムの動作を防止することによってパフォーマンスを向上させる目的でも使用できます。

一般に ACL は、構成ステートメントの集合と定義されます。これらのステートメントにより、受け入れまたは拒否するアドレスまたはパターンを定義します。NA は、デバイスから構成情報を取得し、構成から ACL ステートメントを抽出します。さらに、NA は、構成に依存しない ACL を保存します。

NA の ACL Manager により、次の処理を簡単に行うことができます。

- デバイスの ACL を表示する
- ACL の履歴を維持する
- ACL についてコメントし、それらのコメントを構成に維持する

また、ACL Manager により、既存の ACL 構成を使用して ACL テンプレートを簡単に作成することもできます。

この章では、デバイスまたはデバイスのグループの ACL 解析を有効（および無効）にする方法についても説明します。

- 単独デバイスの ACL 解析を有効にする方法の詳細については、「[\[構成管理\] ページのフィールド](#)」(36 ページ) を参照してください。
- デバイスグループの ACL 解析を有効にする方法の詳細については、「[\[デバイスを一括編集\] ページのフィールド](#)」(161 ページ) を参照してください。
- ACL の検索方法の詳細については、「[\[ACL を検索\] ページのフィールド](#)」(523 ページ) を参照してください。

**注意：** ACL 情報は、ACL 解析が有効にされた後に、デバイスの最初に保存されたスナップショットまたはチェックポイントスナップショットが取得されるまでは表示できません。

## ACLの表示

デバイスのACLを表示するには：

1. [デバイス]メニューで、[インベントリ]をクリックします。
2. [インベントリ]ページで、ACL解析が有効になっているデバイスを選択します[デバイス詳細]ページが開きます。（注意：ACLをサポートするデバイスを追加する場合は、[有効]オプションがオンになっていることを確認します）。デバイスが検出され、チェックポイントスナップショットが取得されれば、デバイスのACLを表示できます（デバイスの追加方法の詳細については、「[デバイスの追加](#)」（106ページ）を参照してください）。
3. [表示]ドロップダウンメニューで[デバイス詳細]を選択し、[ACL]をクリックします。[デバイスACL]ページが開きます。「[\[デバイスACL\]ページのフィールド](#)」（695ページ）を参照してください。
4. [デバイスACL]ページで、リストにある任意のACLの[ACLの表示]オプションをクリックします。[ACLを表示]ページが開きます。「[\[ACLの表示\]ページのフィールド](#)」（697ページ）を参照してください。

## [デバイスACL]ページのフィールド

フィールド	説明/アクション
ホスト名	デバイスのホスト名を表示します。デバイスのホスト名をクリックすると、最後に表示した[デバイス詳細]ページが開きます。このページでは、このデバイスのACLに関する情報を確認できます。
デバイスIP	デバイスのIPアドレスを表示します。デバイスのIPアドレスをクリックすると、最後に表示した[デバイス詳細]ページが開きます。このページでは、このデバイスのACLに関する情報を確認できます。
最後のスナップショットの試行	最終のスナップショットを試行した日時を表示します。
最後のスナップショットの結果	たとえば「構成変更の検出」など、最後のスナップショットの結果を表示します。
チェックボックス	<p>左側のチェックボックスを使用して、2つのACLを比較できます。ACLを選択したら、[アクション]ドロップダウンメニューをクリックし、次のいずれかをクリックします。</p> <ul style="list-style-type: none"> <li>• 比較:[スクリプトを比較]ページが開きます。このページでは、選択した2つのACLを並べて比較できます。差異は、分かりやすいように異なる色で強調表示されます。</li> </ul> <p>横の[選択]ドロップダウンメニューにより、すべてのデバイス構成を選択または選択解除できます。</p>
ACL ID	ACL IDを表示します。ACL IDは、デバイスがその構成の中でACLを識別する場合の基準です。ACL IDとして整数インデックスを使用するデバイスは多く存在しますが、全部ではありません。そのため、ACL IDは文字列として保存されます。
ACLハンドル	ACLハンドルを表示します。ACLハンドルは、ユーザが定義するACL名です。デフォルトでは、ACLハンドルとACL IDは同じです。特定のACLハンドルが指定されない場合、ドライバはACL IDを使用します（注：デフォルトでは、ACLをソートするためにこのフィールドを使用します）。
ACLタイプ	デバイスによって定義されるACLタイプを表示します。
最終変更日	ACLを最後に変更した日付および時刻が表示されます。



フィールド	説明/アクション
アクション	<p data-bbox="448 239 753 264">次のアクションを選択できます。</p> <ul data-bbox="448 285 1463 516" style="list-style-type: none"><li data-bbox="448 285 1463 344">• ACLを編集 : [ACLを編集] ページが開きます。このページでは、ACLを編集できます。詳細については、「<a href="#">コマンドスクリプトの実行</a>」(699 ページ) を参照してください。</li><li data-bbox="448 359 1463 417">• ACL を表示 : [ACL を表示] ページが開きます。このページには、ACL が表示されます。詳細については、「<a href="#">[ACLの表示] ページのフィールド</a>」(697 ページ) を参照してください。</li><li data-bbox="448 432 1463 516">• ACL履歴 : [ACL履歴] ページが開きます。このページでは、すべての変更の総合的な監査証跡を表示できます。ACL履歴を活用することにより、ACLを以前の設定に復元することができます。復元するには、履歴ACLを確認してから、[ACLの編集] アクションへのリンクをクリックします。</li></ul>



## [ACLの表示]ページのフィールド

[ACLの表示]ページを開くには：

1. [デバイス]メニューで、[インベントリ]をクリックします。
2. [インベントリ]ページで、ACL解析が有効になっているデバイスを選択します[デバイス詳細]ページが開きます。（注意：ACLをサポートするデバイスを追加する場合は、[有効]オプションがオンになっていることを確認します）。デバイスが検出され、初期スナップショットが取得されれば、デバイスのACLを表示できます。
3. [表示]ドロップダウンメニューで[デバイス詳細]を選択し、[ACL]をクリックします。[デバイスACL]ページが開きます。
4. [デバイスACL]ページで、リストにある任意のACLの[ACLの表示]オプションをクリックします。[ACLを表示]ページが開きます。

フィールド	説明/アクション
デバイス	デバイスのホスト名またはIPアドレスを表示します。デバイスのIPアドレスをクリックすると、最後に表示した[デバイス詳細]ページが開きます。このページでは、このデバイスのACLに関する情報を確認できます。
ID	ACL IDを表示します。ACL IDは、デバイスがその構成の中でACLを識別する場合の基準です。
ACLハンドル	ACLハンドルを表示します。ACLハンドルは、ユーザが定義するACL名です。
ACLタイプ	ACLタイプを表示します。
最終変更日	ACLを最後に変更した日付および時刻が表示されます。
最終変更ユーザ	ACLを最後に変更したユーザを表示します。最後に変更したユーザが「N/A」と表示されることがあります。これは、この特定のACLバージョンに対して責任を持つユーザをNAが認識していないことを示します。ユーザが表示される場合は、[ユーザ属性の詳細]ページへのリンクが表示され、このバージョンのACLを取得する前に発生したすべてのアクティビティについてNAが認識している情報が示されます。ユーザはNAの推測に過ぎないため、他のアクティビティがACL変更の実際の原因になっている可能性があります。
ACLスクリプト	<p>ACLを定義する構成スクリプトを表示します。ACLスクリプトは、ACLを定義するために必要な構成行を表します。次のオプションを選択できます。</p> <ul style="list-style-type: none"> <li>• ACLの新規作成：[コマンドスクリプトの実行タスク]ページが開きます。このページでは、既存のACLをテンプレートとして使用できます（「<a href="#">ACLの作成</a>」（700ページ）を参照してください）。</li> <li>• ACLを編集：[コマンドスクリプトの実行タスク]ページが開きます。このページではACLを編集できます（「<a href="#">コマンドスクリプトの実行</a>」（699ページ）を参照してください）。</li> <li>• ACLテンプレートの新規作成：[コマンドスクリプトの新規作成]ページが開きます。このページでは、既存のACLをテンプレートとして保存できます（「<a href="#">ACLテンプレートの作成</a>」（705ページ）を参照してください）。</li> <li>• ACLテンプレートを編集：[コマンドスクリプトの新規作成]ページが開きます。このページでは、現在のACLを編集するテンプレートを作成できます（「<a href="#">ACLテンプレートの作成</a>」（705ページ）を参照してください）。</li> </ul>

フィールド	説明/アクション
ACL アプリケーション	<p>ACL を適用すると、ACL アプリケーションが表示されます。ACL アプリケーションには、ACL を使用する場所を定義する構成コマンドのリストが含まれています。ACL のタイプによっては、別々のアプリケーションスクリプティングがありません。これらの ACL には、アプリケーションスクリプトが何も表示されません。次のオプションを選択できます。</p> <ul style="list-style-type: none"><li>• ACL を適用 : [タスクの新規作成 - コマンドスクリプトの実行] ページが開きます。このページでは ACL を（再）適用できます（「<a href="#">ACL の作成</a>」（700 ページ）を参照してください）。</li><li>• ACL テンプレートを適用 : [コマンドスクリプトの新規作成] ページが開きます。このページでは、ACL アプリケーションテンプレートを作成します（「<a href="#">ACL テンプレートの作成</a>」（705 ページ）を参照してください）。</li></ul>
コメント	<p>ACL についてのコメントを表示します。次のオプションを選択できます。</p> <ul style="list-style-type: none"><li>• コメントを編集 : [ACL を編集] ページが開きます。</li><li>• 履歴 : [ACL 履歴] ページが開きます。</li><li>• 関連設定を表示 : [デバイス構成] ページが開きます（「<a href="#">[デバイス構成の詳細] ページのフィールド</a>」（175 ページ）を参照してください）。</li></ul>

## コマンドスクリプトの実行

コマンドスクリプトの実行タスクにより、コマンドスクリプトを実行できます。詳細については、「[\[コマンドスクリプトの実行\]タスクページのフィールド](#)」(304 ページ) を参照してください。[コマンドスクリプトの実行タスク]ページには、次のタスクオプションが表示されます。

- 実行するコマンドスクリプト: デバイスの特定のACLからACL編集スクリプトを実行することを示します。ACLは、IDとハンドル（カッコ内）の両方によって識別されます。
- スクリプトタイプを限定: スクリプトタイプは、自動的に「ACL編集スクリプト」に設定されます。
- モード: Cisco IOS構成などのデバイスアクセスモードを表示します。
- スクリプト: 実行するデバイス固有のコマンドを表示します。実行するスクリプトは自動的に入力され、既存のACL構成のコピーが提供されます。アプリケーションでACLを編集する場合は、ACL構成スクリプティングの前（必要に応じてアプリケーションを取り消す）およびACL構成スクリプティングの後（ACLを再適用）の両方で、ACLアプリケーションスクリプトのコピーが提供されます。多くの場合（IOSなど）、ACL構成とユーザがスクリプトで指定する内容を完全に一致させるには、そのACLをまず取り除いてから再び元に戻す必要があります。

## ACLの作成

ACLを新規作成するには、既存のACLをテンプレートとして使用します。

1. [デバイス]メニューで、[インベントリ]をクリックします。
2. ACL解析を有効にするデバイスを選択します。[デバイス詳細]ページが開きます。
3. [表示]ドロップダウンメニューで[デバイス詳細]を選択し、[ACL]をクリックします。[デバイスACL]ページが開きます。
4. [アクション]列の[ACLを編集]オプションをクリックします。[コマンドスクリプトの実行]ページが開きます。詳細については、「[\[コマンドスクリプトの実行\]タスクページのフィールド](#)」(304 ページ) を参照してください。

[コマンドスクリプトの実行タスク]ページの次のフィールドには、値が自動的に入力されます。

- 実行するコマンドスクリプト：スクリプトのタイプ（ACLの適用）とソースACLを表示します。
- スクリプトタイプを限定：スクリプトのタイプ（ACL編集スクリプト）を表示します。
- モード：デバイスにACLを適用する場合の正しいスクリプトモードを表示します。
- スクリプト：既存のACLアプリケーションスクリプトのコピーを表示します。これを必ず詳細に確認し、必要な変更を加えてください。

**注意：** ACLスクリプトは、1行ごとに実行しないでください。1行ごとに実行すると、ACLスクリプトの接続性が失われる可能性があります。

既存のACL IDと同じIDを使用してデバイスにACLを追加する場合、実際にはそのデバイスの既存ACLを編集することになります。

## ACLアプリケーションの変更

ACLアプリケーションを変更するには：

1. [デバイス]メニューで、[インベントリ]をクリックします。
2. ACL解析を有効にするデバイスを選択します。[デバイス詳細]ページが開きます。
3. [表示]ドロップダウンメニューで[デバイス詳細]を選択し、[ACL]をクリックします。[デバイスACL]ページが開きます。
4. [ACLを表示]オプションをクリックします。[ACLを表示]ページが開きます。(「[\[ACLの表示\]ページのフィールド](#)」(697ページ)を参照してください)。
5. [ACLの適用]オプションをクリックします。[コマンドスクリプトの実行]ページが開きます。(「[ACLの作成](#)」(700ページ)を参照してください)。

[コマンドスクリプトの実行タスク]ページの次のフィールドには、値が自動的に入力されます。

- 実行するコマンドスクリプト：スクリプトのタイプ（ACLの適用）とソースACLを表示します。
- スクリプトタイプを限定：スクリプトのタイプ（ACLアプリケーションスクリプト）を表示します。
- モード：デバイスにACLを適用する場合の正しいスクリプトモードを表示します。
- スクリプト：既存のACLアプリケーションスクリプトのコピーを表示します。

**注意：** ACLスクリプトは、1行ごとに実行しないでください。1行ごとに実行すると、ACLスクリプトの接続性が失われる可能性があります。

## ACL 行の一括挿入

ACL 行を一括配布できます。NA は、ACL ID または ACL ハンドルに基づいて、単独または複数のデバイスの適切な ACL に必要な行を自動的に追加します。次の手順は、Cisco IOS デバイスにのみ適用されます。

ACL に行を一括挿入するには：

1. [デバイス]メニューバーで[デバイスタスク]を選択し、[ACL 行の一括挿入]をクリックします。[タスクの新規作成] - [コマンドスクリプトの実行]ページが開きます。（「[ACL の作成](#)」（700 ページ）を参照してください）。
2. タスクを実行するデバイスまたはデバイスのグループを選択できます。デバイスまたはデバイスグループを選択すると、ページが更新されます。
3. 実行するコマンドスクリプト：次のいずれかを選択します。
  - a) Cisco IOS による ACL ID に基づいた ACL への行の挿入
    - 行を挿入するための ACL の ID：行の追加先 ACL の ID を入力します。これにより、デバイスのグループを選択した場合は、この ACL ID に一致する ACL を含むそれぞれのデバイスに行が追加されます。
    - 挿入する ACL 行：デバイスにあるとおりに、正確に ACL 行を入力します。
    - 行を追加する場所：行を追加する場所を選択します。オプションには、最初、最後、最後の 1 つ前などがあります。
    - スクリプトを更新：上記変数の入力完了したらクリックします。
    - パラメータ：オプションのパラメータです。
    - スクリプト：これは、ACL を更新する実際のスクリプトです。実行前にこのスクリプトを編集するオプションにより、この機能の柔軟性を高めることができます。
  - b) Cisco IOS によるハンドルに基づいた ACL への行の挿入
    - ACL ハンドル：行の追加先 ACL ハンドルを入力します。これにより、デバイスのグループを選択した場合は、この ACL ハンドルに一致する ACL を含むそれぞれのデバイスに行が追加されます。
    - 挿入する ACL 行（'access-list {id}' なし）："access-list ACLID" なしで挿入する ACL 行を入力します。スクリプトは、必要に応じてこのパラメータを配置します。
    - 行を追加する場所：この行を追加する場所を選択します。オプションには、最初、最後、最後の 1 つ前などがあります。
    - スクリプトを更新：上記変数の入力完了したらクリックします。
    - パラメータ：オプションのパラメータです。
    - スクリプト：これは、ACL を更新する実際のスクリプトです。実行前にこのスクリプトを編集するオプションにより、この機能の柔軟性を高めることができます。

## ACL 行の一括削除

ACL 行を一括削除できます。NA は、ACL ID または ACL ハンドルに基づいて、単独または複数のデバイスの適切な ACL から不要な行を自動的に削除します。次の手順は、Cisco IOS デバイスにのみ適用されます。

ACLの行を一括削除するには：

1. [デバイス]メニューバーで[デバイスタスク]を選択し、[ACL行の一括削除]をクリックします。[タスクの新規作成 - コマンドスクリプトの実行]ページが開きます。(「[ACLの作成](#)」(700ページ)を参照してください)。
2. タスクを実行するデバイスまたはデバイスのグループを選択できます。デバイスまたはデバイスグループを選択すると、ページが更新されます。
3. 実行するコマンドスクリプト：次のいずれかを選択します。
  - a) Cisco IOSによるACL IDに基づいたACLからの行の削除
    - 行を削除するためのACLのID：行の削除元となるACLのIDを入力します。これにより、デバイスのグループを選択した場合は、このACL IDに一致する各デバイスACLから行が削除されます。
    - 削除するACL行：デバイス上に表示されるとおりに正確にACL行を入力します。ACL行によっては、複数の空白文字が含まれるものがあります。たとえば、`access-list 139` と `deny ip host 192.168.139.2 any` では、「deny」と「ip」の間に3つの空白文字があります。
    - スクリプトを更新：上記変数の入力完了したらクリックします。
    - パラメータ：オプションのパラメータです。
    - スクリプト：これは、ACLを更新する実際のスクリプトです。実行前にこのスクリプトを編集するオプションにより、この機能の柔軟性を高めることができます。
  - b) Cisco IOSによるハンドルに基づいたACLからの行の削除
    - ACLハンドル：行の削除元となるACLハンドルを入力します。これにより、デバイスのグループを選択した場合は、このACLハンドルに一致するACLを含むそれぞれのデバイスから行が削除されます。
    - 削除するACL行（'access-list {id}' なし）："access-list ACLID" なしで削除するACL行を入力します。スクリプトは、必要に応じてこのパラメータを配置します。
    - スクリプトを更新：上記変数の入力完了したらクリックします。
    - パラメータ：オプションのパラメータです。
    - スクリプト：これは、ACLを更新する実際のスクリプトです。実行前にこのスクリプトを編集するオプションにより、この機能の柔軟性を高めることができます。

## ACLへのコメント追加とACLハンドルの作成

NAでは、インラインコメント機能とACLコメントが統合されています。これにより、ACLについてのコメントが構成に組み込まれ、構成コメント内の変更についてのコメントがACLに組み込まれて再適用されるようにすることができます。

インラインコメントをサポートしているデバイスでは、NAインラインコメントを識別する二重コメント文字シーケンスに続く ACLNAME : テキストは、ACLハンドルを示します。インラインコメントをサポートしないデバイスでは、構成との間でACLコメントを移動させる機能は使用できません。ただし、ACLコメントとハンドルはACL内に維持されます。

コメントを入力するには：

1. [デバイス]メニューで、[インベントリ]をクリックします。
2. [インベントリ]ページで、ACL解析が有効になっているデバイスを選択します[デバイス詳細]ページが開きます。
3. [表示]ドロップダウンメニューで[デバイス詳細]を選択し、[ACL]をクリックします。[デバイスACL]ページが開きます。
4. [ACLを表示]オプションをクリックします。[ACLを表示]ページが開きます。**「[ACLの表示]ページのフィールド」(697ページ)**を参照してください。
5. [コメントの編集]オプションをクリックします。[ACLの編集]ページが開きます。
6. [コメント]フィールドにコメントを入力します。
7. ACLハンドルを編集します。
8. [保存]をクリックします。

NAのインラインコメントをサポートするデバイスの場合は、構成内のコメントの変更がACLコメントに反映されます。



## ACLテンプレートの作成

既存のACLに基づいてスクリプトを直接に作成する以外に、ACLを使用してACLコマンドスクリプトテンプレートの原型を作成できます。ACLテンプレートを作成して、ACLを編集および適用することもできます。

1. [デバイス]メニューで、[インベントリ]をクリックします。
2. [インベントリ]ページで、ACL解析が有効になっているデバイスを選択します[デバイス詳細]ページが開きます。
3. [表示]ドロップダウンメニューで[デバイス詳細]を選択し、[ACL]をクリックします。[デバイスACL]ページが開きます。
4. [アクション]列で[ACLの表示]オプションをクリックします。[ACLを表示]ページが開きます。
5. [ACLスクリプト]の下で[ACLテンプレートの新規作成]へのリンクをクリックします。[コマンドスクリプトの新規作成]ページが開きます。**「[コマンドスクリプトの新規作成]ページのフィールド」(578ページ)**を参照してください。[コマンドスクリプトの新規作成]ページの次のフィールドには、値が自動的に入力されます。
  - － スクリプトタイプ：[ACL作成スクリプト]、[ACLのスクリプトを編集]、または[ACLスクリプトの適用]など、作成されるACLスクリプトのテンプレートタイプを表示します。
  - － モード：デバイスでACLスクリプトを実行する場合の正しいスクリプトモードを表示します。
  - － スクリプト：既存のACLアプリケーションスクリプトのコピーを表示します。

**注意：** ACL IDが必要な場合は、スクリプトで予約済み変数 "\$tc\_aclid\_for\_handle\$" を使用できます。スクリプトを実行する場合は、ACLハンドルの入力を求めるプロンプトが表示されます。スクリプトがデバイスで実際に実行されると、スクリプトで使用するこの変数の各インスタンスは、入力した値と一致するACLハンドルを持つデバイスのACL IDで置き換えられます。

6. ACLの新規スクリプトの名前を入力します。
7. スクリプトを編集します。詳細については、**「コマンドスクリプトの実行」(699ページ)**を参照してください。
8. 終了したら、必ず[スクリプトの保存]をクリックしてください。スクリプトが正常に保存されると、[スクリプト検索結果 (コマンドスクリプト)]ページが開きます。追加したスクリプトが強調表示された状態でリストに表示されます。スクリプトは、タスクとしてスケジュールされるまで実行されません。
9. 実行アクションを選択します。
10. スクリプトを実行することが可能な1つのデバイスのホスト名またはIPアドレスを指定します。
11. ACL IDを入力します。
12. タスクを保存します。タスクが完了すると、新規ACLが[ACLの表示]ページに表示されます。**「[デバイスACL]ページのフィールド」(695ページ)**を参照してください。

## ACLの編集

ACLを編集するには：

1. [デバイス]メニューで、[インベントリ]をクリックします。
2. [インベントリ]ページで、ACL解析が有効になっているデバイスを選択します[デバイス詳細]ページが開きます。
3. [表示]ドロップダウンメニューで[デバイス詳細]を選択し、[ACL]をクリックします。[デバイスACL]ページが開きます。
4. 編集するACLの[ACLの編集]オプションをクリックします。[コマンドスクリプトの実行]ページが開きます。詳細については、[「ACLの作成」\(700ページ\)](#)を参照してください。

[ACLの編集]へのリンクをクリックすると、[コマンドスクリプトの実行]タスク内の次のフィールドに値が自動的に入力されます。

- 実行するコマンドスクリプト：スクリプトのタイプ（ACLを編集）とソースACLを表示します。
- スクリプトタイプを限定：スクリプトのタイプ（ACL編集スクリプト）を表示します。
- モード：デバイスでACLを編集する場合の正しいスクリプトモードを表示します。
- スクリプト：実行するデバイス固有のコマンドを表示します。これを必ず詳細に確認し、必要な変更を加えてください。

編集されたACLを複数のデバイスに配布する場合は、ACLを配布するデバイスグループを選択します。詳細については、[「\[コマンドスクリプトの実行\]タスクページのフィールド」\(304ページ\)](#)を参照してください。

**注意：** ACLスクリプトは、1行ごとに実行しないでください。1行ごとに実行すると、ACLスクリプトの接続性が失われる可能性があります。

## ACLの削除

ACL 管理の中で多くの時間を要するタスクの1つは、古くなった未使用のACLをデバイスから削除して、より新しいアプリケーションやACLの動作を妨害しないようにすることです。単独デバイスのACLを削除する場合は、そのデバイスのACLがリスト表示されます。デバイスグループのACLを削除する場合は、グループ内のすべてのデバイスのACLハンドルがすべてリスト表示され、ACLの削除はACL IDではなくハンドルごとに実行されます。

ACLを削除するには、[デバイス]メニューから[デバイスタスク]を選択し、[ACLの削除]をクリックします。[タスクの新規作成 - ACLの削除]ページが開きます。**「ACLの削除タスクページ」(708ページ)**を参照してください。

デバイスの構成からACLを削除すると、そのACLは管理対象ACLのリストに表示されなくなります。ACLの履歴は、その後も[ACLを検索]オプションを使用して検索可能ですが、デバイス固有のACLを表示するときにACL履歴は表示されません。デバイス固有のインターフェイスからの、削除されたACLの追跡記録はありません。削除されたACLの構成をロールバックするには、そのACLを検索して再配布します。

アプリケーションを持たないACLは削除されます。ただし、アプリケーションを持つACLは削除されません。デフォルトにより、NAはアプリケーションスクリプトを持つACLを削除しません。オプションとして、アプリケーションを持つ場合でもACLを強制的に削除することができます。このオプションをオンにすると、選択したすべてのACLが削除されます。

**注意：** NAは、デバイスの構成内で1つのACLのすべてのアプリケーションを特定することを保証していません。ACLがアプリケーションスクリプトを持っていなくても、デバイスのどこかで実際に使用されている可能性があります。そのような場合は、（アプリケーションの存在を認識しないために）ACLの削除タスクによりACLの削除が試みられ、デバイスが予期しない動作をします。

## ACLの削除タスクページ

ACLの削除タスクにより、ACLを削除することができます。ACLを削除するには、[デバイス]メニューから[デバイスタスク]を選択し、[ACLの削除]をクリックします。[ACLの削除]ページが開きます。終了したら、[タスクを保存]ボタンをクリックします。

フィールド	説明/アクション
タスク名	[ACLの削除]を表示します。必要に応じて別のタスク名を入力できます。
適用先	次のオプションのいずれかを選択します。 <ul style="list-style-type: none"> <li>• デバイス/グループ：タスクを実行するIPアドレス、ホスト名、またはデバイスグループ名を入力するか、拡大鏡アイコンをクリックします。デバイスセレクトアの使用方法的詳細については、「<a href="#">デバイスセレクトア</a>」(142ページ)を参照してください。</li> <li>• CSVファイル：デバイスのリストを含むCSVファイルの名前を入力するか、または参照します。CSVファイルでは、CSVファイルの各行（IPアドレスとホスト名）に関連付けられたデバイスを識別する方法を提供する必要があります。[タスクのCSVテンプレート]へのリンクをクリックすると、サンプルのCSVファイルをダウンロードできます。</li> </ul>
開始日	次のオプションを選択できます。 <ul style="list-style-type: none"> <li>• すぐに開始：選択されている場合、デフォルトでは複数のタスクジョブがすぐに開始されます。</li> <li>• 開始時刻：選択されている場合は、カレンダーアイコンをクリックしてカレンダーを開き、複数のタスクジョブを開始する日時を選択できます。</li> </ul>
優先度	タスクの優先度を表示します。タスクの優先度レベルは1～5であり、1が最も高いタスク優先度レベルです。詳細については、「 <a href="#">タスクの予定</a> 」(278ページ)を参照してください。
コメント	複数のタスクジョブについてのコメントを追加します。
<b>タスクオプション</b>	
セッションログ	[完全なデバイスセッションログを格納]ボックスをオンにしてデバッグログを格納します。このオプションは失敗したスナップショットをデバッグする場合に役立ちますが、格納されるデータのサイズが大きくなる可能性があります。
強制的に保存	デバイス構成の更新設定です。この設定は、スタートアップ構成をサポートしているデバイスのみに適用されます。この設定のデフォルト値はタスクの種類ごとに構成されています。 <ul style="list-style-type: none"> <li>• このタスクの完了時に、NAで現在実行中の構成によってスタートアップ構成を上書きする場合、[強制的に保存]チェックボックスをオンにします。</li> <li>• NAでスタートアップ構成を変更しない場合、[強制的に保存]チェックボックスをオフにします。</li> </ul> <p>(注意：この設定はNA 9.20で新たに導入されました。デバイスのスタートアップ構成を更新するかどうかを決定するその他のすべての方法よりも優先されます)。</p>
削除するACL	次のオプションを選択できます。 <ul style="list-style-type: none"> <li>• アプリケーションがないACLを表示：既知のアプリケーションなしのACLのみを表示します(デフォルト)。</li> <li>• 全ACLを表示：選択されている場合は、ACL IDを含むすべてのACLがハンドルをかついで囲んで表示されます。リストから任意の数のACLを選択できます(注意：(デバイスグループに対してこのタスクを実行する場合は、そのグループ内のすべてのデバイスで検出されるすべてのACLハンドルがリストに表示されます。アプリケーションなしのACLごとにリストをフィルタするオプションはありません)。</li> </ul>

フィールド	説明/アクション
アプリケーションを 持つACLも 削除チェックボックス	オンにすると、既知のアプリケーションを持っている場合でも、選択したACLが削除されます。
推定継続時間	このタスクの実行対象となるデバイスまたはデバイスグループを予約するときの時間を入力します。デフォルト値は60分です。
<b>デバイス資格情報のオプション</b>	
デバイス資格情報のオプションは、[システム管理設定]の[サーバ]ページで設定する、[標準のデバイスの資格情報を許可]、[タスクごとのデバイスの資格情報を許可]、または[ユーザのAAA資格情報を許可]オプションに応じて表示されます。[タスクごとのデバイスの資格情報を許可]を有効にすると、適切なパスワード情報を入力するよう求めるプロンプトが表示されます。また、複数のデバイス資格情報オプションを有効にすると、タスクを実行するときにオプションを選択するよう求めるプロンプトが表示されます。デバイス資格情報オプションを1つだけ有効にした場合は自動的にオプションが使用され、プロンプトは表示されません（デバイス資格情報の有効化の詳細については、 <a href="#">「[デバイスアクセス]ページのフィールド」</a> （45 ページ）を参照してください）。	
デバイス資格情報	<p>[システム管理設定]の[デバイスアクセス]ページで有効にされるデバイス資格情報オプションに応じて、次の中からオプションを1つ以上選択します。</p> <ul style="list-style-type: none"> <li>標準デバイス固有の資格情報とネットワーク全体のパスワードルールの使用（デフォルト）。</li> <li>特定のタスク単位のパスワードを使用。[ユーザ名]、[パスワード]、[パスワードの確認]、[イネーブルパスワード]、[イネーブルパスワードの確認]、[SNMP読み取り専用コミュニティ文字列]、および[SNMP読み取り/書き込みコミュニティ文字列]への入力を求めるプロンプトが表示されます。</li> <li>タスク所有者のAAA資格情報の使用。タスク所有者には、定義された有効なAAA資格情報が必要です。（<b>注意</b>：標準パスワードルールとデバイス固有パスワードを使用します。ただし、タスク所有者のAAAユーザ名とパスワードが適用されます。）</li> </ul>
<b>タスク前/タスク後スナップショットオプション</b>	
スナップショットのオプションは、[システム管理設定]の下の[構成管理]ページでユーザによる無効化がシステムで有効に構成されている場合にのみ表示されます（詳細については、 <a href="#">「[構成管理]ページのフィールド」</a> （36 ページ）を参照してください）。	
タスク前スナップショット	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>なし</li> <li>タスクの一部として（デフォルト）</li> </ul>
タスク後スナップショット	<p>次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>なし</li> <li>タスクの一部として（デフォルト）</li> <li>個別のタスクとしてスケジュール</li> </ul>
<b>承認オプション</b>	
承認オプションは、タスクがワークフロー承認ルールの一部になっている場合にのみ表示されます。	
承認要求	タスクが実行前に承認を必要とする場合は、デフォルトでオンになっています。タスクの承認期限を変更するには、日付の横のカレンダーアイコンをクリックしてカレンダーを開き、日時を選択します。タスクの優先度を選択することもできます。ワークフローの設定時に、[緊急]や[通常]などの異なる優先度の値を追加することもできます。NA Schedulerでは、値が考慮されません。これは基本的に、ある時間内に承認が必要なタスクを判断するための視覚的なキューです。
承認の無効化	タスクで無効化が許可されている場合は、このオプションを選択して承認プロセスを無効化します。

フィールド	説明/アクション
ドラフトとして保存	オンになっている場合は、タスクをドラフトとして保存し、後でもう一度操作できます。タスクはドラフトモードでは実行されません。
<b>スケジューリングオプション</b>	
再試行回数	<p>タスクが失敗すると、NAはこの設定回数になるまで、再試行間隔ごとに再試行します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 再試行なし（デフォルト）</li> <li>• 1回</li> <li>• 2回</li> <li>• 3回</li> </ul>
再試行間隔	次の再試行までに待機する時間(分)を入力します。デフォルトでは5分です。
繰り返しオプション	<p>タスクは、上で指定した日付/時刻に開始し、次の条件に従って反復します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• 1回のみ：タスクは指定した日付/時刻に1回のみ発生します（デフォルト）。</li> <li>• 定期的：繰り返し間隔を分単位で指定します。</li> <li>• 日次：タスクは指定した時刻に毎日実行されます。</li> <li>• 週次：週の曜日を1つ以上選択します。タスクは選択した曜日の指定した時刻に実行されます。</li> <li>• 月次：毎月1度、指定した時刻にタスクを実行させる月の日付を1日選択します。</li> </ul>
繰り返しの範囲	<p>[1回のみ]を除く繰り返しオプションのいずれかを選択する場合は、次の中から繰り返しの範囲を指定できます。</p> <ul style="list-style-type: none"> <li>• 終了日なし（デフォルト）</li> <li>• &lt;&gt;オカレンス後に終了：繰り返しの回数を入力します。</li> <li>• 終了期限：カレンダーアイコンをクリックし、日時を選択します。</li> </ul>

## 付録A：コマンドラインリファレンス

コマンドウィンドウを開くには、ディスプレイの左側の[検索]タブでデバイスのIPアドレスかホスト名を入力し、[接続]ボタンをクリックします。

[接続]メニューの[デバイス詳細]ページからも開くことができます。コマンドウィンドウ内では、コピーするテキストを選択し、[Return]キーを押します。強調表示されたテキストはコピーバッファに保存されます。次にそのテキストを別のアプリケーションに貼り付けます。作業が終了したら、「exit」と入力してウィンドウを閉じます。

**注意：** Telnet/SSH プロキシを使用して直接デバイスに接続している場合は、デバイスを終了しても Telnet/SSH プロキシ内に留まったままになります。「exit」ともう一度入力するまでは、CLI コマンドを入力して他のデバイスに接続できます。

CLI コマンドのヘルプを参照するには、「help」と入力してすべてのコマンドリストを参照してください。特定のコマンドの詳細なヘルプを表示するには、「help <コマンド名>」と入力します。

**注意：** CLI では大文字と小文字が区別されません。すべてのコマンドとオプションを、大文字や小文字で入力できます。

次のコマンドを使用して、CLI ヘルプをオンラインで使用できます。

- CLI プロンプトで「help」と入力します。CLI コマンドのほとんどすべてをアルファベット順に並べたリストが表示されます。たとえば、Import コマンドのヘルプを表示するには、「import」と入力します。（**注意：** help コマンド、または exit および quit コマンドに関するヘルプテキストはありません）。
- Import コマンドのヘルプを参照するには、「help import」と入力します。「help <コマンド名>」というコマンドを入力すると、そのコマンドの名前、概要、説明、例などの詳細が返されます。
- コマンドラインを終了するには、「exit」と入力します。開始したセッションのタイプによっては、再度「exit」と入力して、手動でウィンドウを閉じることが必要な場合があります。

**注意：** help コマンドと任意のコマンドの最初のワードのみを入力して、そのワードで始まるすべてのコマンドのリストを返すこともできます。

CLIヘルプテキストで使用される入力規則には、特定の意味があります。次の表に、各種規則とそれぞれの意味を示します。

規則	意味
>	単一の右山かっこは、コマンドを入力するコマンドプロンプトを示します。
-	ダッシュは、続けてコマンドオプションを入力することを示します。
<>	左右両方の山かっこは、IPアドレスなどの必須の変数テキストを囲みます。これには、山かっこを含めないでください。
[]	角かっこは、1つ以上のオプション要素を区切ります。
	縦線は、かっこ内の引数を区切ります。1つの引数のみを含めるようにしてください。

CLIコマンドの全リスト、構文、および例については、『NA CLI/API Command Reference』を参照してください。



## 付録B：コマンド権限

ユーザがWeb ページの表示またはコマンドの実行などアクションを行うには、それぞれのアクションに対応するコマンド権限が明示的に付与されている必要があります。一連のコマンド権限によって、コマンド権限ロールを作成します。その後、作成したロールをユーザグループに適用して、そのユーザグループにコマンド権限を設定できます。詳細については、「[\[ユーザロールの新規作成\] ページのフィールド](#)」(259 ページ) を参照してください。

**注意：** NAには、コマンド権限、デバイス変更権限、スクリプト権限、およびデバイス表示権限を含む、4つのタイプの権限があります。一部のコマンド権限では、1つ以上の他の権限が必要な場合があります。詳細については、「[コマンド権限の定義](#)」(715 ページ) を参照してください。

### コマンド権限の付与

コマンド権限を付与するには：

1. [管理]メニューバーで、[ユーザのロールと権限]をクリックします。[ユーザのロールと権限]ページが開きます。
2. ページ上部の[ユーザロールの新規作成]へのリンクをクリックします。[ユーザロールの新規作成]ページが開きます。詳細については、「[ユーザロールの追加](#)」(257 ページ) を参照してください。

## コマンドのリスト

デバイスを追加	拡張カスタムデータの管理
デバイスグループの追加	分散システムの管理
イベントの追加	ゲートウェイの管理
SNMPトラップ構成の追加	IPアドレスの管理
システム管理設定	ライセンスの管理
デバイスグループの管理	パーティションの管理
ユーザの管理	ソフトウェア準拠の管理
ユーザグループの管理	ソフトウェアレベルの管理
デバイスの構成への注釈付け	ソフトウェアイメージの管理
TelnetとSSHの同時セッションを許可	システムレポートの管理
デバイスソフトウェアのバックアップ	テンプレートの管理
デバイスを一括編集	ユーザの管理
デバイスパスワードの変更	ユーザグループの管理
構成ポリシー準拠の確認	ユーザロールの管理
Syslogの構成	ビューの管理
コネクタのリダイレクト	デバイス構成の変更
データの整理	SecurIDの変更
重複の削除	マルチタスクプロジェクト
アクセスの削除	ワークフロー承認の無効化
デバイスを削除	デバイスのリポートタスク
デバイス構成の削除	FQDNの解決
診断の削除	コマンドスクリプトの実行
ドライバの削除	診断の実行
セッションの削除	外部アプリケーションの実行
ソフトウェア準拠の削除	ICMPテストの実行
ソフトウェアイメージの削除	タスクに最も高い優先度を設定
ソフトウェアレベルの削除	反復タスクの同期
システムイベントの削除	スナップショットの取得
タスクを削除	Telnet/SSHクライアント
リモートエージェントの配布	トラブルシューティング
ソフトウェアを配布	デバイスコメントの更新
ネットワークデバイスの検出	デバイスチケットの更新
デバイスドライバの検出	ワークフロー設定
ドライバ	ACLを表示
ACLを編集	コマンドスクリプトの表示
ACLコメントの編集	構成ポリシーイベントの表示
構成（変更）ユーザの編集	配布済みソフトウェアの表示
デバイスを編集	構成ポリシーの表示
非アクティブなデバイスの編集	デバイス構成の表示
タスクを編集	デバイス診断の表示
ユーザを編集	デバイス情報の表示
電子メールレポート	診断スクリプトの表示
外部認証の設定	ドライバの表示
サマリレポートの生成	イベントルールの表示
デバイスとパスワードのインポート	全デバイス構成の表示
SysOIDのリスト表示	スクリプトと診断の表示
リストの表示	SecurIDの表示
ACLの管理	セッションを表示
コマンドスクリプトの管理	ソフトウェアイメージアーカイブの表示
構成ポリシーの管理	タスクの表示
デバイスパスワードルールの管理	テンプレートの表示
診断スクリプトの管理	ユーザ情報の表示
イベントルールの管理	ワークフロー設定の表示

## コマンド権限の定義

コマンド権限	説明
デバイスをアクティブ化/非アクティブ化	デバイスをアクティブ化または非アクティブ化する権限です。
デバイスを追加	デバイスをNAシステムへ追加する権限です。この権限には、[デバイスの追加]ウィザードを使用したデバイスの追加も含まれます。
デバイスグループの追加	デバイスグループを作成する権限です。パブリック・デバイス・グループを作成するには、デバイスグループの管理権限も付与されている必要があります。
グループにデバイスを追加	デバイスをデバイスグループへ追加する権限です。デバイスは、既にNAデータベースに存在している必要があります。
イベントの追加	[編集]メニューの[メッセージの新規作成]オプションを使用する権限です。
SNMPトラップ構成の追加	SNMPトラップを設定し、"add SNMP trap config" CLI コマンド（このコマンドによって設定オプションに"snmp/traps/global"が追加されます）を実行する権限です。
システム管理設定	システム管理設定を変更する権限です。ワークフロー設定および外部認証の設定など、追加の権限を必要とするシステム管理設定もあることに注意してください。
デバイスグループの管理	親グループおよびパブリックグループの追加、変更および削除を含む、デバイスグループの管理操作を行う権限です。
デバイスの構成への注釈付け	デバイスの構成に注釈を付ける権限です。
TelnetとSSHの同時セッションを許可	デバイスへの複数プロキシ接続防止を無効にする権限です。
デバイスソフトウェアのバックアップ	デバイスソフトウェアのバックアップタスクを実行する権限です。
デバイスを一括編集	バッチ編集時に複数のデバイスを変更する権限です。
デバイスパスワードの変更	単一デバイスのパスワードを変更するタスクをスケジュールする権限です。このコマンドでは、コマンドを実行するデバイスに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要です。
デバイスパスワードの変更（グループ）	デバイスグループのパスワードを変更するタスクをスケジュールする権限です。このコマンドでは、コマンドを実行するデバイスグループに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要であることに注意してください。
構成ポリシー準拠の確認	[構成ポリシー準拠の確認]タスクを実行する権限です。[ポリシー準拠の確認]タスクにより、デバイスが、構成ポリシーまたはソフトウェアポリシーに準拠しているかどうかを判別できます。
デバイス予約のクリア	[アクティビティカレンダー]に表示されるデバイス予約競合をクリアする権限です。

コマンド権限	説明
Syslogの構成	デバイスのSyslog設定を構成するタスクをスケジュールする権限です。このコマンドでは、コマンドを実行するデバイスに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要です。
Syslogの構成（グループ）	デバイスのグループのSyslog設定を構成するタスクをスケジュールする権限です。このコマンドでは、コマンドを実行するデバイスグループに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要であることに注意してください。
コネクタのリダイレクト	NNM 7.xとNNM 8.xのURLアクションをリダイレクトします。コネクタのリダイレクトでは、NNMによるIPアドレスからデバイスIDを探します。さらに、コネクタのリダイレクトにより、構成履歴などのデバイス情報が転送されます。
データの整理タスク	単一デバイスに対して[データの整理]タスクをスケジュールする権限です。データの整理により、廃止されたファイル、診断、イベントおよびタスクが削除されます。
データの整理タスク（グループ）	デバイスのグループに対して[データの整理]タスクをスケジュールする権限です。データの整理により、廃止されたファイル、診断、イベントおよびタスクが削除されます。
重複の削除	単一デバイスを削除または非アクティブ化する権限です。これにより、NAデータベース内でそのデバイスのインターフェイスは1回のみ発生します。
重複の削除（グループ）	デバイスのグループを削除または非アクティブ化する権限です。これにより、NAデータベース内でそのデバイスグループのインターフェイスは1回のみ発生します。
アクセスの削除	デバイスのアクセスログを削除する権限です。
デバイスを削除	デバイスをNAデータベースから完全に削除する権限です。
デバイス構成の削除	デバイスの構成を削除する権限です。
デバイスグループの削除	デバイスグループを削除する権限です。
診断の削除	タスクがキャプチャした診断データを削除する権限です。ログには、診断データがどのようにキャプチャされたかが記録されます。
ドライバの削除	デバイスに割り当てられたドライバをクリアする権限です。
イベントルールの削除	イベント通知とレスポンスルールを削除する権限です。
セッションの削除	Telnet/SSHセッションレコードを削除する権限です。
ソフトウェア準拠の削除	ソフトウェア準拠レコードを削除する権限です。
ソフトウェアイメージの削除	NAソフトウェアリポジトリからソフトウェアイメージを削除する権限です。
ソフトウェアレベルの削除	構成されたソフトウェアレベルを削除する権限です。NAは、ソフトウェアレベル、本質的にはソフトウェアバージョンに一致する正規表現を定義できます。その正規表現にソフトウェアレベルを割り当てられます。正規表現に一致するソフトウェアバージョンのあらゆるデバイスは、そのレベルであると見なされます。
システムイベントの削除	システムイベントを削除する権限です。
タスクを削除	タスクを削除する権限です。

コマンド権限	説明
リモートエージェントの配布	NA リモートエージェントを配布する権限です。NA リモートエージェントは、SNMP を処理するプロセスを含み、NA コア上の NA 管理エンジン、ローカルデバイスからの syslog 通知を処理する syslog プロセス、およびローカルデバイスへの TFTP アクセスを可能にする TFTP プロセスと関係します。(詳細については、『NA Satellite Guide』を参照してください)。
ソフトウェアを配布	デバイスソフトウェアを単一デバイスに配布するタスクをスケジュールする権限です。このコマンドでは、コマンドを実行するデバイスに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要です。
ソフトウェアを配布 (グループ)	デバイスソフトウェアをデバイスグループに配布するタスクをスケジュールする権限です。このコマンドでは、コマンドを実行するデバイスグループに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要であることに注意してください。
ネットワークデバイスの検出	IP アドレスをスキャンして、不明なデバイスを自動的に NA データベースに追加する権限です。
ネットワークデバイスの検出 (グループ)	IP アドレスをスキャンして、不明なデバイスグループを自動的に NA データベースに追加する権限です。
デバイスのシングルサインオン	Telnet/SSH プロキシを経由して、デバイスに自動的に接続する権限です。
デバイスドライバの検出	デバイスのドライバを検出する権限です。このコマンドでは、コマンドを実行するデバイスに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要です。
デバイスドライバの検出 (グループ)	デバイスグループのドライバを検出する権限です。このコマンドでは、コマンドを実行するデバイスグループに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要であることに注意してください。
ドライバ	[ドライバ] ページを表示する権限です。[ドライバ] ページには、システムにインストールされているドライバのリストと、現在使用されているドライバの個数が表示されます。
ACL を編集	ACL スクリプトを編集する権限です。
ACL コメントの編集	ACL コメントを編集する権限です。
構成 (変更) ユーザの編集	デバイス構成の [変更者] をリセットする権限です。この権限は、管理ユーザにのみ設定することをお勧めします。
デバイスを編集	デバイスのグループメンバーシップ、デバイスアクセス設定、およびその他の属性を変更する権限です。このコマンドでは、コマンドを実行するデバイスに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要です。
デバイスグループの編集	デバイスグループを編集する権限です。これには、デバイスグループへのデバイスの追加およびデバイスグループからのデバイスの削除が含まれます。
非アクティブなデバイスの編集	非アクティブなデバイスの [コメント] フィールドを編集する権限です。
タスクを編集	スケジュールされたタスクを編集する権限です。

コマンド権限	説明
ユーザを編集	ユーザプロフィールを編集する権限です。デフォルトでは、ユーザは自分のユーザプロフィール以外は編集できません。
電子メールレポート	さまざまなレポートを実行し、指定の受信者に電子メールを送信するタスクをスケジュールする権限です。
外部認証の設定	LDAP、TACACS+、SecurID、および、RADIUSなどの外部認証を設定する権限です。
サマリレポートの生成	単一デバイスのサマリレポートを生成するタスクをスケジュールする権限です。
サマリレポートの生成（グループ）	デバイスのグループのサマリレポートを生成するタスクをスケジュールする権限です。
デバイスとパスワードのインポート	デバイスおよびデバイス認証情報をインポートする権限です。
SysOIDのリスト表示	サポートされるデバイスのsysOIDをリスト表示する権限です。
リストの表示	[リストの表示]ページを表示する権限です。1つまたは複数のパーティションのセットです。NAのデバイスは、すべてデバイスビュー内のパーティションに分割されています。
ACLの管理	ACLの削除を含む、デバイスACLの管理操作を行う権限です。
コマンドスクリプトの管理	コマンドスクリプトを作成、変更、および削除する権限です。
構成ポリシーの管理	構成ポリシーを作成、編集、および削除する権限です。
デバイスパスワードルールの管理	デバイスのパスワードルールを作成、編集、および削除する権限です。
診断スクリプトの管理	診断スクリプトを作成、編集、および削除する権限です。
分散システムの管理	[分散システム]ページを表示する権限です。これには、[分散監視結果]ページ、[分散エラーリスト]ページ、[分散競合リスト]ページ、[コアをリスト表示]ページなどが含まれます。分散システム環境の構成の詳細については、『NA Multimaster Distributed System on Oracle Guide』を参照してください。
イベントルールの管理	イベント通知とレスポンスルールを作成、編集、および削除する権限です。
ゲートウェイの管理	[ゲートウェイリスト]ページの表示、ゲートウェイの編集と削除、NAリモートエージェントの配布を行えます。NAリモートエージェントは、SNMPを処理するプロセスを含み、NAコア上のNA管理エンジン、ローカルデバイスからのsyslog通知を処理するsyslogプロセス、およびローカルデバイスへのTFTPアクセスを可能にするTFTPプロセスと関係します。
IPアドレスの管理	デバイスIPアドレスを追加、編集、および削除する権限です。
ライセンスの管理	NAライセンス情報を表示および更新する権限です。
パーティションの管理	パーティションを追加、編集、および削除する権限です。
ソフトウェア準拠の管理	ソフトウェア準拠情報を追加および編集する権限です。
ソフトウェアイメージの管理	ソフトウェアイメージを追加、編集、および削除する権限です。

コマンド権限	説明
ソフトウェアレベルの管理	ソフトウェア準拠を追加および編集する権限です。
システムレポートの管理	システムレポートおよびユーザレポートの順番を変更したり、システムレポートを削除したりする権限です。
テンプレートの管理	スクリプトテンプレートを作成、編集、および削除する権限です。
ユーザの管理	NAユーザを作成、編集、および削除する権限です。
ユーザグループの管理	ユーザグループを作成、編集、および削除する権限です。ユーザ権限は、このインターフェイスによって管理されるため、この権限の付与にあたっては注意が必要です。
ユーザロールの管理	ユーザロールを追加、編集、および削除する権限です。
デバイス構成の変更	編集済みの構成をデバイスに配布するタスクをスケジュールする権限です。このコマンドでは、コマンドを実行するデバイスに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要です。
SecurIDの変更	SecurID トークン情報を変更する権限です。
マルチタスクプロジェクト	マルチタスクプロジェクトを変更する権限です。
OS分析	OS分析タスクを実行する権限です。[OS分析]タスクページは、sysoid（デバイスモデルの一意の識別子）、OSバージョン、フラッシュストレージオプション、モジュール、その他のデバイスに関する情報を収集します。この情報を使用して、ソフトウェア推奨が作成されます。
ワークフロー承認の無効化	ワークフロー承認プロセスを通さずに、タスクを実行する権限です。
デバイスのリブートタスク	ドライバで提供されるリロードスクリプトを介して、デバイスをリロード（リブート）する権限です。このコマンドでは、コマンドを実行するデバイスに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要です。
FQDNの解決	デバイスの完全修飾ドメイン名を解決する、FQDNの解決タスクをスケジュールする権限です。
FQDNの解決（グループ）	デバイスグループの完全修飾ドメイン名を解決する、FQDNの解決タスクをスケジュールする権限です。
コマンドスクリプトの実行	指定のデバイス上でスクリプトを実行する、[コマンドスクリプトの実行]タスクをスケジュールする権限です。このコマンドでは、コマンドを実行するデバイスに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要です。また、選択したスクリプトに対するスクリプト権限も必要となります。
コマンドスクリプトの実行（グループ）	指定のデバイスグループ上でスクリプトを実行する、[コマンドスクリプトの実行]タスクをスケジュールする権限です。このコマンドでは、コマンドを実行するデバイスグループに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要であることに注意してください。また、選択したスクリプトに対するスクリプト権限も必要となります。
診断スクリプトの実行	指定のデバイス上で診断スクリプトを実行する、[診断の実行]タスクをスケジュールする権限です。このコマンドでは、コマンドを実行するデバイスに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要です。
診断スクリプトの実行（グループ）	指定のデバイスグループ上で診断スクリプトを実行する、[診断の実行]タスクをスケジュールする権限です。このコマンドでは、コマンドを実行するデバイスグループに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要であることに注意してください。

コマンド権限	説明
外部アプリケーションの実行	ユーザ定義の外部アプリケーションを実行する権限です。この権限の付与にあたっては注意が必要です。
ICMPテストの実行	デバイス上でICMPテストを実行する、[ICMPテストの実行]タスクをスケジュールする権限です。
ICMPテストの実行（グループ）	デバイスグループ上でICMPテストを実行する、[ICMPテストの実行]タスクをスケジュールする権限です。
タスクに最も高い優先度を設定	タスクの優先度を1に設定する権限です。
スタートアップとランニングの同期	ターゲットデバイスに対してスタートアップと実行時の構成を同期化する、[スタートアップとランニングの同期]タスクをスケジュールする権限です。このコマンドでは、コマンドを実行するデバイスに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要です。
スタートアップとランニングの同期（グループ）	ターゲットデバイスグループに対してスタートアップと実行時の構成を同期化する、[スタートアップとランニングの同期]タスクをスケジュールする権限です。このコマンドでは、コマンドを実行するデバイスグループに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要であることに注意してください。
スナップショットの取得	デバイスの構成のスナップショットを取得する、スナップショットの取得タスクをスケジュールする権限です。
スナップショットの取得（グループ）	デバイスグループの構成のスナップショットを取得する、スナップショットの取得タスクをスケジュールする権限です。
Telnet/SSHクライアント	NA プロキシサービスを介し、TelnetまたはSSH経由でデバイスにアクセスする権限です。
トラブルシューティング	[トラブルシューティング]ページへのアクセス、電子メールでのトラブルシューティング情報の送信、およびNAサーバのログingleベル変更を可能にする権限です。
デバイスコメントの更新	デバイスのコメントを変更する権限です。
デバイスチケットの更新	Remedyなどのサードパーティ製のチケットシステムと通信するように、NAを設定する権限です。
ACLを表示	ACLスクリプトを表示する権限です。
コマンドスクリプトの表示	コマンドスクリプトを表示する権限です。
構成ポリシーと準拠の表示	構成ポリシーおよび準拠についての情報を表示する権限です。



コマンド権限	説明
構成ポリシーイベントの表示	構成ポリシーのイベントの詳細を表示する権限です。このコマンドでは、コマンドを実行するデバイスに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要であることに注意してください。
配布済みソフトウェアの表示	ソフトウェアアーカイブではなく、配布されたソフトウェアを表示する権限です。
デバイス構成の表示	デバイスの構成を表示する権限です。パスワードやコミュニティ文字列といった機密情報はマスクされています。
デバイス診断の表示	デバイス診断を表示する権限です。
デバイス情報の表示	デバイスの構成を除く、デバイス関連のすべての情報を表示する権限です。
診断スクリプトの表示	診断スクリプトの詳細を表示する権限です。
ドライバの表示	ドライバの詳細を表示する権限です。
イベントルールの表示	イベントルールのリストを表示する権限です。
全デバイス構成の表示	マスクを解除された状態のデバイス構成を表示する権限です。このコマンドでは、コマンドを実行するデバイスに対するコマンド権限およびそれに対応するデバイス変更権限の両方が必要であることに注意してください。
スクリプトと診断の表示	コマンドスクリプトまたは診断タスクの結果の詳細を表示する権限です。
SecurIDの表示	SecurID トークン情報を表示する権限です。
セッションを表示	Telnet/SSHセッションコマンドおよび応答履歴を表示する権限です。
ソフトウェアイメージアーカイブの表示	NA アーカイブに格納されているソフトウェアイメージを表示する権限です。
タスクの表示	タスクの詳細を表示する権限です。
テンプレートの表示	スクリプトテンプレートの詳細を表示する権限です。
ユーザ情報の表示	ユーザ情報を表示する権限です。
ワークフロー設定	ワークフロー承認ルールを設定する権限です。



# 付録C：サンプルスクリプト

この付録はサンプルスクリプトです。

## PERLスクリプトのサンプル#1

このPERLスクリプトでは、Cisco 2600 シリーズおよびCisco 7200 シリーズで、すべてのファストイーサネットのインターフェイスを全二重に設定します。

```
#
# Cisco 2600 シリーズおよびCisco 7200 シリーズで、すべてのファストイーサネット
# のインターフェイスを全二重に設定するサンプルスクリプト。
#
use Socket;

$iaaddr = gethostbyname("$tc_device_ip$");
$telnet_port = 23;
$sin = sockaddr_in($telnet_port, $iaaddr);
socket(DEV, PF_INET, SOCK_STREAM, getprotobyname('tcp'));
connect(DEV, $sin) || die "Can't connect to $tc_device_hostname$: $!\n";

sendln("");
sendln("$tc_device_password$");
sendln("en");
sendln("$tc_device_enable_password$");
sendln("conf t");

for $name (split(" ", "$tc_device_port_name_list$")) {
    if ($name =~ /FastEthernet/)
        sendln("interface $name");
        sendln("duplex full");
        sendln("exit");
    }
}
sendln("exit");
sendln("exit");
sendln("");
close(DEV);
exit;
```

(次ページへ続く)

```
sub sendln {
    my ($line) = @_ ;
    $line .= "\n";
    syswrite(DEV,$line,length($line));
    while (<DEV>) {
        print;
```

```

die "Failed to execute command\n"
  if (/^% (Unknown|Unrecognized|Invalid|. *uthorization failed)/);
last if (/name:/ ||
        /word:/ ||
        />/ ||
        ^#/);
}
}

```

## PERL スクリプトのサンプル #2

この PERL スクリプトでは、すべてのインターフェイスを no ip directed-broadcast に設定にします。

---

```

#
# すべてのインターフェイスで IP 指定なしの
# ブロードキャストを設定するサンプルスクリプト。
#
use Socket;

$iaaddr = gethostbyname("$tc_device_ip$");
$telnet_port = 23;
$sin = sockaddr_in($telnet_port, $iaaddr);
socket(DEV, PF_INET, SOCK_STREAM, getprotobyname('tcp'));
connect(DEV, $sin) || die "Can't connect to $tc_device_hostname$: $!\n";

sendln("");
sendln("$tc_device_password$");
sendln("en");
sendln("$tc_device_enable_password$");
sendln("conf t");

for $name (split(" ", "$tc_device_port_name_list$")) {
    sendln("interface $name");
    sendln("no ip directed-broadcast");
    sendln("exit");
}
sendln("exit");
sendln("exit");
sendln("");
close(DEV);
exit;

sub sendln {
    my ($line) = @_;
    $line .= "\n";
    syswrite(DEV, $line, length($line));
    while (<DEV>) {
        print;
        die "Failed to execute command\n"
          if (/^% (Unknown|Unrecognized|Invalid|. *uthorization failed)/);
        last if (/name:/ ||
                /word:/ ||
                />/ ||
                ^#/);
    }
}

```

## Expect スクリプトのサンプル

この Expect スクリプトでは、バナーに所定の文字列が含まれていない場合にのみ、文字列を含むように変更します。

---

```
#
# バナーが正しく設定されていない場合にかぎり
# バナーを設定するサンプルスクリプト
#
spawn telnet $tc_device_ip$
set banner "****Unauthorized Access Prohibited****"
expect {
    $banner {
        puts "\nBanner is already set correctly\n"
        exit 0
    } "word:"
}
send "$tc_device_password$\r"
expect ">"
send "en\r"
expect "word:"
send "$tc_device_enable_password$\r"
expect "\#"
send "config t\r"
expect "\#"
send "banner motd /$banner/\r"
expect "\#"
send "exit"
```



# 用語集

この用語集には、Network Automation（NA）の用語の定義が収められています。

用語	定義
コア	単一のNA管理エンジン、関連サービス（SyslogおよびTFTP）、および単一のデータベースからなります。コアでは、複数のサイト（デバイスセット）を管理できます。
デバイス パスワードルール	同じユーザ名、パスワード、およびSNMPコミュニティ文字列を、デバイス、IPアドレスの範囲、またはホスト名のグループに適用できます。
デフォルトサイト パーティション	デフォルトパーティションは、「デフォルトサイト」という名前です。初めてNAを使用する場合、デフォルトパーティションのみが利用できる唯一のパーティションです。 NAが現在管理しているすべてのデバイスがリストされます。
デバイスビュー	デバイスとデバイスグループに適用されるビューです。
診断	デバイスの構成ファイルではキャプチャされないデバイスに関する情報を収集するための、デバイス上で実行するコマンドです。Ciscoルータ上での診断の一例として、Show NTP Statusコマンドの出力が挙げられます。
分散システム	別々のサーバで実行されているコアが複数存在するシステムです。
ゲートウェイ	他のゲートウェイへのIPトラフィックを振り分けるアプリケーションです。ゲートウェイソフトウェアにより、NATされたデバイスとファイアウォールの背後にあるサーバを管理できます。さらにゲートウェイは、領域間のトンネルで帯域幅の流量制御をサポートします。SSLプロキシ、またはTCPポートフォワーディングが使用されていればどこでも使用できます。トンネルは認証でき、オプションでSSLを使用して暗号化できます。
マルチマスタ	すべてのデータの完全なセットを含むデータベースが複数存在するシステムです。
マルチタスクプロジェクト	マルチタスクプロジェクトでは、単一プロジェクトの配下で結合された複数の異なるタスクを実行できます。マルチタスクプロジェクトに含まれる各タスクは指定された順に実行されます。
親グループ	NAにおけるデバイスグループの階層は、親グループとリーフグループからなります。親グループに指定できる親は1つのみです。親グループにデバイスグループを含めることはできますが、デバイスを含めることはできません。

用語	定義
パーティション	パーティションとは、NAオブジェクトのセットです。NAオブジェクトには、デバイス、ユーザ、コマンドスクリプト、デバイスパスワードルール、ポリシー、ソフトウェアイメージなどを含めることができます。パーティションは、権限モデル、グループ階層、NAコア間でのデバイスの分散、およびネットワークダイアグラムと併用できます。
ポリシー	ポリシーとはデバイスの構成と実行時ステータスをテストする、ルールの集合です。
領域	ネットワークセグメントの1つです。一般的に、領域は一意のIPアドレスの集合で識別されます。たとえば、1つの領域に10.255.111.128という番号の2つのデバイスを含めることはできません。その場合は、デバイスを個別の領域に分割する必要があります。サイトをNAコアの管理と同じ領域に含める必要はありません。
ロール	同一のセキュリティ権限を共有するグループに、ユーザ进行分类することです。ロールを割り当てられたユーザは、そのロールで定義している権限を付与されます。たとえば、デバイスの追加、構成ポリシーの管理、ソフトウェアの配布など、ある処理を実行する権限がユーザに与えられた場合、NAでは、リソースにアクセスするための固定ロールIDを使用します。
ルール	以下の項目の少なくとも1つを検証する、自動テストです。 <ul style="list-style-type: none"> <li>• 特定の構成設定</li> <li>• 特定のデータモデル要素</li> <li>• デバイスの実行時ステータス（診断）</li> <li>• デバイスで動作するソフトウェアバージョン</li> </ul>
ルール例外	ルール例外は、ルールの一部です。ただし、その目的は元のルールに一致するデバイス構成内のテキストから、ルール例外に一致するテキストを除外することにあります。
シングルサーチ	シングルサーチオプションで、[シングルサーチ結果]ページで指定した検索基準を含む、すべてのイベントを検索できます。
シングルビュー	シングルビューを使用すると、単一デバイスまたは全デバイスへの変更を示すイベントを1ページ上で追跡できます。
タスク	NAがユーザのネットワークとやりとりを行う手段として最も重要なメカニズムです。タスクは特定のアクションであり、スケジュールしたり、すぐに実行できます。たとえば、パスワードの展開、デバイスのリロード、およびタスクのスナップショットがあります。



用語	定義
タスクプールの初期化	NA 管理エンジンを起動すると、データベースにタスクプールの構築が指示されます。タスクの作成、更新、削除の際、NA ではローカルNA コアに接続されているデータベースのみ更新されます。リモートNA コアに接続されているデータベースで必要な変更の処理は、データベースレプリケーションメカニズムによって行われます。ただし、リモートNA コアを呼び出してメモリのタスクプールを更新する処理はアプリケーションで行います。
ユーザグループ	ユーザを管理するための論理的コンテナです。システム管理者はユーザにユーザグループを割り当てることができます。また、特定のロールもマッピングできます。
ユーザビュー	ユーザとユーザグループに適用されるビューです。
ワークフロー	NA Workflow Integration & Routing Engine (WIRE) は、ネットワーク構成のプロセスを管理し、あらかじめ定義されたポリシーに従ってネットワークの変更が行われ、正しい順序で完了し、適切な担当者によって承認されるようにします。



# ご意見、ご感想について

このシステムで電子メールクライアントが設定されている場合、デフォルトではここをクリックすると電子メールウィンドウが開きます。

使用できる電子メールクライアントがない場合は、Web メールクライアントの新規メッセージに次の情報をコピーし、**ovdoc-nsm@hp.com** までお送りください。

**製品名およびバージョン** : NA9.20

**ドキュメントタイトル** : 『NA ユーザガイド』、2012年5月

**ご意見、ご感想** :