HP Network Automation

ソフトウェアバージョン : 9.0

ユーザガイド

ドキュメント発行日 :2010 年 8 月
ソフトウェアリリース日 :2010 年 8 月

invent

法的制限事項

保証

HP 製品およびサービスに対する保証は、当該製品またはサービスに付帯する明示的保証条項でのみ規定されます。本規定のいかなる部分も、他の保証を構成すると解釈されるものではありません。HP は本書の技術上または編集上の誤謬、欠落についての責任は負わないものとします。

本書に含まれる内容は、予告なく変更される場合があります。071410

限定保証条項

機密コンピュータソフトウェア。所有、使用、コピーには、HP による有効なライセンスが必要です。FAR 12.211 および 12.212 準拠。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マニュアル、技術データは、ベンダの標準商用ライセンスに基づき、米国政府にライセンス供与されています。

著作権

商標情報

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

Java™ は，米国 SunMicrosystems,Inc. の商標です。

謝辞

ANTLR、Apache, Bouncy Castle、GNU、Jaxen、Jython、Netaphor、MetaStuff、Radius, Sleepcat、TanukiSoftware

ドキュメントの更新

本ガイドのタイトルページには、次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を示すソフトウェアバージョン番号
- ドキュメント更新の際に更新されるドキュメントリリース日
- ソフトウェアの本バージョンのリリース日を示すソフトウェアリリース日

最新の更新を確認する場合、または最新版のドキュメントを使用しているかを判断するには、次の Web サイトにアクセスしてください。

http://h20230.www2.hp.com/selfsolve/manuals

このサイトでは、HP パスポートへの登録とサインインが必要です。HP パスポートのユーザー ID を登録するには、次の Web サイトにアクセスしてください。

http://h20229.www2.hp.com/passport-registration.html

または、[HP パスポート サインイン] ページにて **[新規ユーザ - ご登録ください]** リンクをクリックしてください。

該当する製品サポートサービスに加入すると、更新版や新版を入手できます。詳細については、HP の営業担当にまで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 サイトにアクセスしてください。

http://www.hp.com/go/hpsoftwaresupport

この Web サイトでは、連絡先、製品、サービス、および HP Software が提供するサポートに関する詳細情報を提供します。

HP Software Support Online は、お客様によるセルフソルブ機能を提供します。お客様のビジネスの管理に必要となる、対話型の技術サポートツールに迅速かつ効率的にアクセスする手段を提供します。HP ソフトウェアサポート Web サイトでは、大切なサポートカスタマとして、次の操作が実行できます。

- 興味のあるナレッジドキュメントの検索
- サポートケースと拡張リクエストの送信と追跡
- 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 サポート連絡先の検索
- 利用可能なサービスに関する情報の確認
- 他のソフトウェアカスタマとのディスカッションへの参加
- ソフトウェアトレーニングの調査と登録

サポート領域の多くは、HP パスポートのユーザとして登録し、サインインする必要があります。また、サポート連絡先も必要となります。

アクセスレベルに関する情報の詳細については、次の Web サイトを参照してください。

http://h20230.www2.hp.com/new_access_levels.jsp

HP パスポートのユーザー ID を登録するには、次の Web サイトにアクセスしてください。

http://h20229.www2.hp.com/passport-registration.html

目次

第 1 章：はじめに

トピックの参照先リスト

トピック	参照先：
製品の概要	「製品の概要」（20 ページ）
NA 7.50 の機能	「NA 7.50 の機能」（21 ページ）
NA 7.60 の機能	「NA 7.60 の機能」（22 ページ）
NA 9.0 の機能	「NA 9.0 の機能」（24 ページ）
メインのメニューバー	「メインのメニューバー」（27 ページ）
メニューバーのオプション	「ヘルプメニューオプション」（28 ページ）
NA ホームページ	「NA ホームページ」（29 ページ）
コマンドウィンドウを開く	「コマンドウィンドウを開く」（30 ページ）
ドキュメントへのアクセス	「ドキュメントへのアクセス」（30 ページ）
顧客サポートへのお問い合わせ	「顧客サポートへのお問い合わせ」（33 ページ）
最新ソフトウェアバージョンの表示	「最新ソフトウェアバージョンの表示」（35 ページ）
ライセンス情報の表示	「ライセンス情報を表示」（35 ページ）
[システム構成を表示] ページ	「[システム構成を表示] ページ」（36 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、Cisco、Nortel、F5 Networks、および 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 9.0 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 9.0 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て使用できます。
- 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。自動修正スクリプトポップアップウィンドウは、[ポリシールール] ページ上のデータにアクセスし、変数マッピングの表示、サンプルコードの生成、保存前のスクリプトの検証を実行します。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。例えば、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イ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共に管理し、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 9.0 の機能

NA 9.0 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。例えば、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 経由で実行するようになります。
- 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の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
- NA 9.0 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、「customname」と「customvalue」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。
- NA9.0 には次のプラットフォームサポートが含まれています。
  - 64 ビット版 Windows 2008
  - Oracle 11g
  - 64 ビット版 Linux
  - MS SQL 2008

メインのメニューバー


HP Network Automation
ログアウト
デバイス
タスク
ポリシー
レポート
管理
ヘルプ
インベントリ
グループ
新規作成
デバイス
デバイステンプレート
デバイスグループ
親グループ
デバイスの新規作成ウィザード
構成変更
デバイスツール
コマンドスクリプト
構成 / テンプレート
デバイスパスワード / ルール
デバイステンプレート
診断
ポリシー
ソフトウェアイメージ
VTP ドメイン
デバイスタスク
ポリシーとタスクの準拠
Syslog の構成
パスワードの配布
ドライバの検出
デバイスのリブート
ICMP テストの実行
コマンドスクリプトの実行
診断の実行
スナップショットの取得
スタートアップとランニングの同期
デバイスの更新 / ソフトウェアインポート
ネットワークの検出 / デバイス
重複の削除
OS 分析
テンプレートからデバイスをプロビジョニング
ACL の削除
一括挿入 / ACL 行
一括削除 / ACL 行
自分のタスク
承認の要求
マルチタスクプロジェクトの新規作成
タスク負荷
アクティビティカレンダー
タスクテンプレート
予定タスク
実行中のタスク
最近のタスク
タスクの新規作成
Syslog の構成
パスワードの配布
ドライバの検出
デバイスのリブート
ICMP テストの実行
コマンドスクリプトの実行
診断の実行
スナップショットの取得
スタートアップとランニングの同期
デバイスの更新 / ソフトウェアインポート
ネットワークデバイスの検出
重複の削除
OS 分析
ポートスキャン
テンプレートからデバイスをプロビジョニング
ポリシーとタスクの準拠
サマリレポートのレポート
電子メールレポート
リモートエージェントの配布
FQDN の解決
データの整理
外部アプリケーションの実行
ポリシーリスト
ポリシーの新規作成
ポリシーのインポート / エクスポート
ポリシーアクティビティ
ポリシー準拠
ポリシーをテスト / 準拠
ソフトウェアレベル
ポリシータスク
ポリシーとタスクの準拠
シングルビュー
シングルサーチ
ユーザとシステム / レポート
検索
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
Telnet/SSH セッション
イベント
ユーザ
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
コンプライアンスセンター
ネットワークステータス
ベストプラクティス
デバイスステータス
統計ダッシュボード
ダイアグラム
デバイスソフトウェア
ソフトウェア / 脆弱性
イメージ同期 / レポート
システムとネットワーク / イベント
サマリレポート
レポート作成タスク
サマリレポートのレポート
電子メールレポート
ユーザ
ユーザグループ
ユーザの新規作成
ユーザグループの新規作成
ログオンしているユーザ
ユーザロールと権限
セキュリティパーティション
ゲートウェイ
デバイスパスワード / ルール
イベント通知とレスポンスルール
カスタムデータの設定
LDAP 設定
ワークフロー設定
管理 / 設定
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
タスク負荷
システムステータス
サービスの開始 / 停止
トラブルシューティング
ドライバ
システムタスク
インポート
ネットワークの検出 / デバイス
重複の削除
OS 分析
リモート配布 / エージェント
FQDN の解決
データの整理
外部アプリケーションの実行
ドキュメント
サポート
HP Live Network
HP ネットワークについて / Automation について

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」（768 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、『*HP Network Automation 9.0 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」（35 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」(349 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」(333 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」(344 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、画面の左側の [検索] タブで、デバイスの IP アドレスまたはホスト名を入力し、[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でコピーするテキストを選択して 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。

- 『*HP Network Automation 9.0 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 9.0 ユーザガイド*] を選択します。
- オンライン HTML ヘルプファイル : オンライン HTML 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。
- 『*HP Network Automation 9.0 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 9.0* 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。
- 『*HP Network Automation 9.0* リリースガイド』: 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 9.0* リリースノート] 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 9.0 Multimaster Distributed System on Oracle Users Guide*
- *NA 9.0 Multimaster Distributed System on SQL Server Users Guide*
- *NA 9.0 Horizontal Scalability Users Guide*
- *NA 9.0 Satellite Users Guide*

HP Network Automation 9.0 ユーザガイド

『*HP Network Automation 9.0 ユーザガイド*』では、以下の内容について説明しています。

- 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： 『*HP Network Automation 9.0 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。

次の表は、『*HP Network Automation 9.0 ユーザガイド*』で使用する表記規則の一覧です。

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。例えば、*C:\hp\sdk\docs.*
リンク	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。このユーザガイドでは、相互参照先とページ数をそれぞれ鍵かっこと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、角かっこを含めないように注意してください。

顧客サポートへのお問い合わせ

HP ソフトウェアサポートオンライン Web サイトにアクセスしてください。

http://www.hp.com/go/hpsoftwaresupport

この Web サイトでは、連絡先、製品、サービス、および HP Software が提供するサポートに関する詳細情報を提供します。

問題を報告する場合は、状況をできるだけ詳しく説明してください。

HP と別添に有効なサポート契約がある場合を除き、HP ソフトウェアのバージョンサポートポリシーに基づき、HP は現在のメジャーリリースの現行バージョンとそれより前のマイナーバージョン、および以前のメジャーリリースの最新マイナーバージョンのサポートを提供します。

製品の新しいメジャーバージョンが公開された場合のサポート状況は、以下のようになります。

- サポートに新規、および現在のメジャーバージョンが提供されます。
- 現在のメジャーバージョンより、メジャーバージョンで2バージョン前の最新マイナーバージョンは、サポート終了（EOS）となります。

例えば、NA 9.0 がリリースされると、NA 7.50 と NA 7.60 は引き続きサポートされますが、NA 7.00 はサポートされなくなります。

[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係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	次のオプションから、1 つ以上選択します。 • [過去 < > 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。 • [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。 • [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。 • [ラッパーログ]：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。 • 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です。

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 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、以下へ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、「ライセンス情報を表示」（35 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」（36 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、Device Driver Reference（DRS）ドキュメントを参照してください。DRS は、新しく自動化されたドライバリリースおよびデリバリシステムです。

ライセンス情報を表示

[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 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と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」（188 ページ）を参照してください。マルチマスタ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、『*HP Network Automation 9.0 Multimaster Distributed System on Oracle User's Guide*』、または『*HP Network Automation 9.0 Multimaster Distributed System on SQL Server User's Guide*』を参照してください。

第 2 章：システム管理設定の構成

トピックの参照先リスト

トピック	参照先：
はじめに	「はじめに」（39 ページ）
構成管理	「構成管理」（40 ページ）
デバイスアクセス	「[デバイスアクセス] ページのフィールド」（54 ページ）
サーバ	「サーバ」（65 ページ）
ワークフロー	「ワークフロー」（75 ページ）
ユーザインターフェイス	「ユーザインターフェイス」（78 ページ）
Telnet/SSH	「Telnet/SSH」（83 ページ）
レポート作成	「レポート作成」（88 ページ）
ユーザ認証	「ユーザ認証」（95 ページ）
LDAP 認証の設定	「LDAP 外部認証の設定」（103 ページ）
サーバ監視	「サーバ監視」（107 ページ）
サードパーティ統合	「サードパーティ統合」（112 ページ）
監視結果の表示	「監視結果の表示」（114 ページ）
サービスの開始および停止	「サービスの開始および停止」（120 ページ）
ログ記録	「ログ記録」（122 ページ）
デバイスドライバのレビュー	「デバイスドライバのレビュー」（128 ページ）

システム管理設定へのナビゲート

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。例えば、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
- Telent/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	次のオプションのいずれかを選択します。 • 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）。 • 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。 • 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。 変更の検出の詳細については、「変更の検出」（49 ページ）を参照してください。
変更検出間隔	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。
Syslog の検出パターン	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 <<] 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、一致が見つかると、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。（**注意**：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。） Syslog メッセージパターンの詳細については、「Syslog メッセージ」（50 ページ）を参照してください。
無視する Syslog パターン	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 <<] 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。

フィールド	説明 / アクション
セカンダリ IP タイプ	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。 • プライマリ • 代替 • コンソール • ホップボックス • NAT • 接続スルー • 内部スルー • 内部ダイレクト IP アドレス管理の詳細については、「[デバイス管理対象 IP アドレス] ページのフィールド」（303 ページ）を参照してください。
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。
ユーザ ID の変更	
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。

フィールド	説明 / アクション
syslog ユーザパターン	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： • 認証されたユーザ (\S+) • ユーザ (\S+) の開いたセッション • ユーザ (\S+) の成功したログイン 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。一致が見つかると、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。例えば、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。
スタートアップとランニング構成	

フィールド	説明 / アクション
スタートアップ構成をキャプチャ	次のオプションのいずれかを選択します。 • オフ：スタートアップ構成をキャプチャしません。 • 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。 • 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。
ACL 解析	
各スナップショットで ACL データを解析	次のオプションのいずれかを選択します。 • 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。 • 無効：各スナップショットで ACL データを解析しません。 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。バッチ編集を使用して、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。（**注意**：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。）
ACL 編集	
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。
構成ポリシーの検証	

フィールド	説明 / アクション
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。自動修正スクリプの詳細については、「自動修正スクリプトの作成」（720 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。
タスク前とタスク後のスナップショット	
ユーザによるタスク前 / 後のスナップショットの無効化	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、「タスク前とタスク後のスナップショットの構成」（52 ページ）を参照してください）。
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	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。 **注意**：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。 詳細については、「タスク前とタスク後のスナップショットの構成」（52 ページ）を参照してください。
コマンドスクリプト実行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。 • なし（デフォルト） • タスクの一部として

フィールド	説明 / アクション
コマンドスクリプト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。 • 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
構成配布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。 • なし • タスクの一部として（デフォルト）
構成配布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。 • 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
デバイスのプロビジョニング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。 • 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
診断実行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。 • なし（デフォルト） • タスクの一部として
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。 • なし（デフォルト） • タスクの一部として • 個別のタスクとしてスケジュール
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。 • なし • タスクの一部として（デフォルト）

フィールド	説明 / アクション
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。 • 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
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。 • なし（デフォルト） • タスクの一部として • 個別のタスクとしてスケジュール
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。
診断	
トポロジーデータの収集頻度	トポロジーデータは、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。トポロジーデータは、ネットワーク図のレンダリングに使用します。トポロジーデータの収集は、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。トポロジー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。デフォルトは 168 時間です。
格納されたトポロジーデータ	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。デフォルトは 168 時間です。

フィールド	説明 / アクション
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。デフォルトは 72 時間です。
フラッシュ記憶域容量	
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。
ブートの検出	
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。
カスタムサービスタイプ	
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、「デバイス詳細の表示」（245 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。例えば、あるユーザがパスワード変更をスケジューリングし、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] メニューバーで、[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. [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」に割り当てることはできず、「N/A」とすることができます。

フィールド	説明 / アクション
イベントの詳細を変更	
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」（230 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」（393 ページ）を参照）
- ACL の削除（「ACL の削除タスクページ」（882 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」（404 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」（385 ページ）を参照）
- ACL 行の一括挿入（「ACL 行の一括挿入」（875 ページ）を参照）
- ACL 行の一括削除（「ACL 行の一括削除」（876 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。例えば、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、『*HP Network Automation 9.0 Satellite Users 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	次のオプションのいずれかを選択します。 • 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。 • 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、「デバイスパスワードルールの作成」（167 ページ）を参照してください。

フィールド	説明 / アクション
デフォルトの接続方法	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。 • Telnet • SSH • RLogin • SNMP • SCP • FTP • TFTP **注意**：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。
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
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	
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。（**注意**：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、稼動中のポートと提供されているサービスを把握できます。namp の詳細については、www.Insecure.Org 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 9.0 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 の使用方法の詳細については、「[ポストスキャン] ページのフィールド」（436 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 の使用方法の詳細については、「[ポストスキャン] ページのフィールド」（436 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。（**注意**：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、「[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」（422 ページ）を参照してください。）

フィールド	説明 / アクション
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。
要塞ホストの設定	
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。（**注意**：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。
SecurID のデバイスアクセス	
SecurID のライセンス使用	次のオプションのいずれかを選択します。 • 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。 • 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。 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。

フィールド	説明 / アクション
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。デフォルト値は 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。
FTP と SSH デバイスアクセス	
FTP/SSH ユーザ	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。 **注意**：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。
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。
タスク単位のパスワード	

フィールド	説明 / アクション
標準デバイスの資格情報を許可	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。 • Syslog の構成 • ACL の削除 • 構成ファイルを配布 • パスワードの配布 • ドライバの検出 • デバイスのリロード • コマンドスクリプトの実行 • 診断の実行 • ICMP テストの実行 • スタートアップとランニングの同期 • スナップショットの取得 • デバイスソフトウェアの更新 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、「タスク単位の資格情報」（63 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、「[デバイスパスワードルール] ページのフィールド」（169 ページ）を参照してください。

フィールド	説明 / アクション
タスクごとのデバイスの資格情報を許可	次のいずれかのタスク（複数の場合あり）を選択します。 • Syslog の構成 • ACL の削除 • 構成ファイルを配布 • ドライバの検出 • パスワードの配布 • デバイスのリロード • コマンドスクリプトの実行 • 診断の実行 • ICMP テストの実行 • スタートアップとランニングの同期 • スナップショットの取得 • デバイスソフトウェアの更新 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、「タスク単位の資格情報」（63 ページ）を参照してください。

フィールド	説明 / アクション
ユーザの AAA 資格情報を許可	次のいずれかのタスク（複数の場合あり）を選択します。 • Syslog の構成 • ACL の削除 • 構成ファイルを配布 • ドライバの検出 • パスワードの配布 • デバイスのリロード • コマンドスクリプトの実行 • 診断の実行 • ICMP テストの実行 • スタートアップとランニングの同期 • スナップショットの取得 • デバイスソフトウェアの更新 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。（**注意**：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、「タスク単位の資格情報」（63 ページ）を参照してください。
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。
nortel の検出	
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 >、バ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/）。
ゲートウェイのメッシュ	
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、「重複 IP ネットワーク」（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
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。デフォルトは 3002 です。ゲートウェイメッシュの詳細については、「重複 IP ネットワーク」（191 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。
ゲートウェイ管理の秘密鍵ファイル名	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の場合があります。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:\NA* 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。 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 `opswgw-mngt-server.pkcs8` 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 *saOPSWgw*/certificates* 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 *C:\Rendition*）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、`spog.pkcs` 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 *C:\Rendition*）へコピーします。[システム管理設定] でファイル名を `spog.pkcs8` に変更してください。 **注意**：`.pcks8` ファイルは PKCK#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。 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。
ゲートウェイのメッシュ接続の待ち時間	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。

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の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。資格情報を指定して、以下ができます。

- 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。

例えば、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。例えば、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 を設定する
- 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
サーバ	
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 サポートについての詳細は、『*NA 9.0 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名 \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（**注意**：指定しないと、NA サーバの最初の非ループバック IPv4 アドレスが使用されます）。
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（**注意**：指定しないと、NA サーバの最初の非ループバック 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。
タスク	
最大同時タスク	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。 **注意**：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。

フィールド	説明 / アクション
最大同時グループタスク	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。デバイススインベ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）。 **注意**：[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。例えば、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。
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。
Syslog の設定	
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。
デバイスのインポート	
既存デバイスを上書き	次のオプションのいずれかを選択します。 • 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。 • 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。
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。
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。

フィールド	説明 / アクション
不明またはアクセス不能なデバイスアクション	次のオプションのいずれかを選択します。 • 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。 • 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。 • 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。
プライマリ IP の再割り当てと重複の削除の設定	
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	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。 • 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） • 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

フィールド	説明 / アクション
重複の検出	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。 **注意**：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。 • 重複を無視 • 重複を非アクティブ化（デフォルト） • 重複を削除
ドメイン名の解決	
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。
監査ログ	
監査ログ	次のオプションのいずれかを選択します。 • 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。 • 無効：ユーザ操作の監査ログを保存しません（デフォルト）。
データベースの整理	
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があるため、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。

フィールド	説明 / アクション
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。
高度なスクリプティング	
スクリプト言語 1	[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。 [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。 [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）。 **注意**：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。
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。

フィールド	説明 / アクション
スクリプト言語 [2-5]	[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。 **注意**：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。
インタープリタのパス [2-5]	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。 **注意**：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。
動的グループ	
動的グループの自動再計算	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。（**注意**：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）。
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。
デバイス変更イベント	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。 • デバイスが追加されました • デバイス構成の変更 • デバイスが削除されました • デバイスが編集されました • デバイスソフトウェアの変更 • デバイスが管理解除されました
ソフトウェアイメージ管理	

フィールド	説明 / アクション
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ンするポートです。通常 6099 です。
ドライバ	
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。
パフォーマンスの調整	
イベントのリストについては、「はじめに」（559 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。
特殊なパフォーマンス設定	
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。

フィールド	説明 / アクション
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。
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 9.0 Multimaster Distributed System on Oracle User's 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 9.0 Multimaster Distributed System on Oracle User's Guide*』を参照してください。

フィールド	説明 / アクション
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 9.0 Multimaster Distributed System on Oracle User's 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
ワークフロー	
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	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。 • 低 • 中 • 高 [緊急] や [通常] などの異なる値を入力し、[値を追加 <<] 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。 **注意**：NA Scheduler では、値は考慮されません。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。
イベント通知とレスポンスルール	

フィールド	説明 / アクション
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。例えば、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。
デバイス予約システム	
デバイス予約システム	次のオプションのいずれかを選択します。 • 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、「デバイスの予約」（242 ページ）を参照してください。 • 無効 : [デバイス予約システム] が無効になります。
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。デフォルトは 1024 です。アクティビティカレンダーの詳細については、「アクティビティカレンダー」（243 ページ）を参照してください。
30 分間の延長を決定する時間（分）	予約を延長する最短時間 (分)。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。
Telnet/SSH プロキシの予約	

フィールド	説明 / アクション
Telnet/SSH プロキシのデバイス予約	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。 • 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、「デバイスの予約」（242 ページ）を参照してください。 • 警告：Telnet/SHH 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 • 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。 「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。
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。*警告：現在、このデバイスの承認された予約がありません。*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
- デバイスセレクタ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
セキュリティ	
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、次回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。

フィールド	説明 / アクション
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 コードが見つかると、エラーが返されます。
日付 / 時刻の表示	
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。例えば、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。
メニューのカスタマイズ	
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。
構成の比較	
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。
ソフトウェアセンター	
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。

フィールド	説明 / アクション
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。
テンプレート	
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。
スクリプト	
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。
拡張カスタムフィールド	
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、「[カスタムデータの設定] ページのフィールド」（688 ページ）を参照してください。
その他	
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。

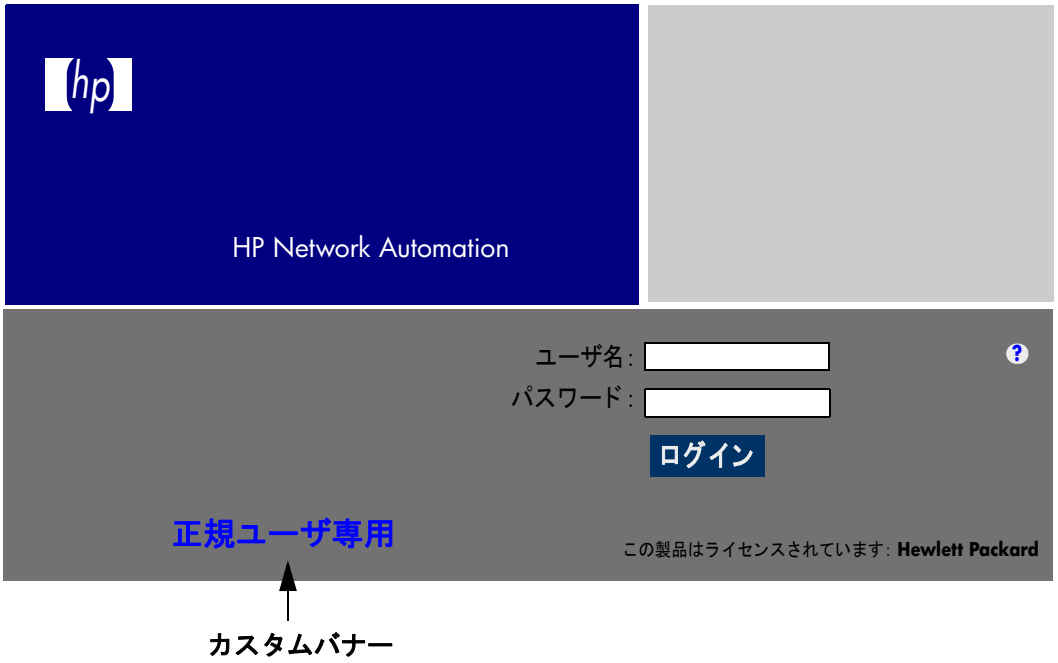
フィールド	説明 / アクション
プレーンテキストとして表示する場合のサイズのしきい値を設定	プレーンテキストとして表示する場合のサイズのしきい値を入力します。デフォルトでは 200,000 バイトです。容量の大きな一部の設定では、サーバやブラウザのリソースを大量に消費する行番号指定などの特別な処理ができない場合もあります。設定値がデフォルト値を超えると、その値は <per>/</pre> タグで囲まれた状態でプレーンテキストとして表示されます。
コミュニティ文字列を隠す	オンにすると、コミュニティ文字列が Web UI に平文で表示されなくなります。このオプションは、NA が表示するコミュニ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判断した場合は、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。

HP 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_install_dir/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. テキストエディタ (HTML 可) でファイルを開き、[HP ログイン] ページで表示するテキストを入力します。
3. ファイルを保存して NA にログインします。[ログイン] ボックス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
Telnet/SSH セッションのログ記録	
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、「コマンドスクリプトの追加」（714 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、「コマンドスクリプトの追加」（714 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。
Telnet/SSH プロキシ	
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ーク、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	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（Telent または SSH）を選択します。ここで選択する接続方法は、*-method* 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。 **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。
非アクティブなデバイスのタイムアウト	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。
SSH ログインのタイムアウト	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。
同時セッション時にアラート	次のオプションのいずれかを選択します。 • 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。 • 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。 • 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。
分散システムの同時セッション処理	次のオプションのいずれかを選択します。 • 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）。 • 非ローカルデバイスのセッションを拒否 分散システムの詳細については、『*NA 9.0 Multimaster Distributed System on Oracle User's Guide*』を参照してください。
不明デバイスに接続	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。

フィールド	説明 / アクション
最大デバイス接続リスト	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。
デバイスのシングルサインオン	
シングルサインオンを使用	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。 **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。
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。 • ログインのプロンプトを表示 • 制限付きアクセスモードでサインオン • ログインを拒否
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	オンにしていて（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。
Telnet クライアント	

フィールド	説明 / アクション
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。 • NA の統合 Telnet クライアントを使用（デフォルト）（**注意**：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）。 • 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 • 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
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）	
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。
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）	
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 20 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て、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。例えば、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、ダイアグラムパラメータも設定できます。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」（758 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。例えば、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
ポリシールール違反	
デバイスステータスの色	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。 • 赤色（デフォルト） • 黄色 • 緑色
カテゴリステータスの色	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。 • 黄色：デフォルト値は 1% です。 • 赤色：デフォルト値は 2% です。
ソフトウェア準拠違反	
デバイスステータスの色	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。 • 赤色（デフォルト） • 黄色 • 緑色 次の準拠レベルは違反と見なされます。 • セキュリティリスク • 実稼動前 • 廃止 • ブロンズ • シルバー • ゴールド • プラチナ
カテゴリステータスの色	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。 • 黄色：デフォルト値は 1% です。 • 赤色：デフォルト値は 2% です。

フィールド	説明 / アクション
スタートアップとランニング構成の不一致	
デバイスステータスの色	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。 • 赤色 • 黄色（デフォルト） • 緑色
カテゴリステータスの色	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。 • 黄色：デフォルト値は 1% です。 • 赤色：デフォルト値は 2% です。
デバイスアクセスエラー	
デバイスステータスの色	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。 • 赤色 • 黄色（デフォルト） • 緑色
カテゴリステータスの色	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。 • 黄色：デフォルト値は 1% です。 • 赤色：デフォルト値は 2% です。
構成の変更	
デバイスステータスの色	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。 • 赤色 • 黄色（デフォルト） • 緑色

フィールド	説明 / アクション
カテゴリステータスの色	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。 • 黄色：デフォルト値は 1% です。 • 赤色：デフォルト値は 2% です。
電子メールレポート	
電子メールレポート形式	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。次のオプションがあります。 • HTML メール（デフォルト） • CSV ファイルの添付 • プレーンテキスト • HTML メール（リンクなし）
テキストの詳細を電子メールに含める	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。
電子メールリンク	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。次のオプションがあります。 • ホスト名（解決できる場合） • IP アドレス • 標準名（解決できる場合は FQDN）（デフォルト） • 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。
シングルビュー	

フィールド	説明 / アクション
追跡するデバイス変更イベント	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。「[シングルビュー] ページのフィールド」（675 ページ）を参照してください。イベントは次のとおりです。 • デバイス構成の変更 • デバイスがブートしました • デバイス診断の変更 • デバイスパスワードの変更 • モジュールの追加 • モジュールの変更 • モジュールの削除 • ソフトウェアの変更 • ユーザメッセージ
追跡する診断	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。「[シングルビュー] ページのフィールド」（675 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。 • ハードウェア情報 • メモリトラブルシューティング • NA デバイスのブート検出 • NA デバイスファイルシステム • NA フラッシュ記憶域容量 • NA インターフェイス • NA 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 **注意**：診断の詳細については、「表示メニューオプション」（257 ページ）を参照してください。

ダイアグラム

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を制御します。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。

イメージ同期レポート

フィールド	説明 / アクション
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。イメージ同期レポートの詳細については、「イメージ同期レポートのフィールド」（770 ページ）を参照してください。
その他	
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 >\addins* 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しません。詳細については、「[ユーザの新規作成] ページのフィールド」（318 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」（99 ページ）を参照してください。

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」（334 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については、「LDAP 外部認証の設定」（103 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」（787 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」（250 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」（707 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」（707 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」（300 ページ）を参照してください。

HP OO の詳細については、『*HP Operation Orchestration ユーザーガイド*』と『*HP Operation Orchestration Software Development Kit Guide（HP Operation 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
ユーザパスワードのセキュリティ	
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。 • その他の制限なし（デフォルト） • 英字以外に 1 文字以上の数字と特殊文字を含める • 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

フィールド	説明 / アクション
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。（**注意**：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。）
外部認証の種類	
外部認証の種類	使用する外部認証の種類を選択します。次のオプションがあります。 • なし（ローカル認証） • HP Server Automation Software • HP Server Automation Software & TACACS+ • TACACS+ • RADIUS • SecurID • LDAP [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、「LDAP 外部認証の設定」（103 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。
TACACS+ 認証 /RADIUS 認証	
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	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。 • PAP（パスワード認証プロトコル） • CHAP（チャレンジハンドシェイク認証プロトコル） • MCHAP（Microsoft チャレンジハンドシェイク認証プロトコル） • ARAP（TACACS+ のみ） • ASCII（TACACS+ のみ）
デフォルト NA-ID の代わりに RADIUS NA-IP を使用	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。（**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。）
固定 RADIUS NA-IP 文字列	[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。（**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。）
HP Server Automation Software の認証	
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 User's 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 *wsapiReadUser*）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。

フィールド	説明 / アクション
OCC サーバ	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、「[サーバ] ページのフィールド」（288 ページ）を参照してください。
デフォルトのユーザグループ	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、「NA/SA 統合」（250 ページ）を参照してください。
HP Operations Orchestration の認証	
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	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。 • https:// • http:// 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。
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	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 <<] 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。 フローの構成については、『*HP Operations Orchestration User's Guide*』を参照してください。HP OO へのログインについては、「編集メニューオプション」（300 ページ）を参照してください。

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。例えば、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	[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。 • 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。 • 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。 • ポート：LDAP 要求ポート番号を入力します。Windows 2000 AD のドメインコントローラはすべて、ポート番号 389 で LDAP 要求をリスンします。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。ただし、複数ドメインの AD 環境の場合、ポート 3268 または 3269（SSL を使用している場合）を使用する必要があります。 • 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。（**注意**：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、「LDAP SSL 構成」（105 ページ）を参照してください。 • 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。
2	次の情報を入力して [次へ] をクリックします。 • 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。*jsmith@hp.com* は、Windows 2000 UPN の DN の例です。 • 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。 • 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。

手順	アクション
3	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。
4	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。 これで外部認証の設定は更新されます。

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」（108 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
サーバ監視	
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。
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。例えば、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。

フィールド	説明 / アクション
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 サテライト構成の詳細については、『*NA 9.0 Satellite User's 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。
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、SoftwareImanageManagement 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。

フィールド	説明 / アクション
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。
監視の構成	
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。デフォルト値は 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。

フィールド	説明 / アクション
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 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
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（NNM）統合により、HP NNM および NA ソフトウェアの両方を実行するシステムに対し、以下に挙げる機能と利点がもたらされます。

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

[サードパーティ統合] ページでは、HP NNM 資格情報を更新できます。[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。

注意： NNM サーバに NNM コネクタをインストールするとき、[サードパーティ統合] ページ上の情報は、NNMコネクタをインストールするときに指定した値で更新されます。NNMコネクタのインストールの詳細については、『*HP NA 7.60.01 NNM Integration Users Guide*』を参照してください。

[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
サードパーティ統合	
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。 • 有効 • 無効（デフォルト）
NNM 統合	
NNM ホスト	NNM サーバのホスト名または IP アドレスを入力します。
NNM HTTP ポート	NNM HTTP ポート番号を入力します。デフォルトはポート 80 です。
NNM ユーザ名	NNM ログインユーザ名を入力します。
NNM パスワード	NNM ログインパスワードを入力します。

フィールド	説明 / アクション
非稼動イベント	オプションリストからデバイスタスクを選択します。デフォルトのタスクを以下に挙げます。 • デバイスソフトウェアの更新 • パスワードの配布 • デバイスのリブート タスク開始時には、NA は NNM Web サービスを呼び出し、デバイスを「非稼動中」に指定します。これにより、NNM 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 NNM 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。
デバイスタスクが失敗する場合	次のオプションのいずれかを選択します。 • デバイスをサービス中に設定する（デフォルト）。 • デバイスを稼働状態に設定しない。
タスク完了後にデバイス準拠の確認に失敗する場合	次のオプションのいずれかを選択します。 • デバイスを稼働状態に設定する。（デフォルト）。 • デバイスを稼働状態に設定しない。
SNMP コミュニティ文字列の送信	次のオプションのいずれかを選択します。 • 有効 • 無効（デフォルト）

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、「[サーバ監視] ページのフィールド」（108 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。「監視のメッセージ」（115 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。 • OK • 警告 • エラー • 無効
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。 • 直ちに実行：監視が直ちに実行されます。 • 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。 • 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、「サービスの開始および停止」（120 ページ）を参照してください。

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	< スレッド名 > 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。
ConfigMonitor	• < ファイル名 >.rcx が見つかりません。：NA に必要な構成ファイルの 1 つが見つかりません。サポートに問い合わせてください。 • < ファイル名 >.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 1 つが破損しています。サポートに問い合わせてください。 • 次の .rcx ファイルの解析で例外が発生しました：< ファイル名 >：NA 構成ファイルの 1 つが破損しています。サポートに問い合わせてください。
MySQL の DatabaseMonitor	• < サーバ名 >: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。 • 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。 • 次のユーザのアクセスが拒否されました：< データベース名 > への < ユーザ名 > の接続：NA が無効なデータベースへの接続を試みているか、または既存データベースに対する権限に問題があります。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。 • 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：< ユーザ名 >（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。 • 一般エラー：NA.RN_CRYPTO_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_CRYPTO_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。

監視	説明 / 対応策
Oracle の DatabaseMonitor	• 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。 • 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。 • ORA-12505 接続が拒否されました。指定した SID（< データベース名 >）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。 • 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。 • 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_CRYPTO_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。
SQLServer の DatabaseMonitor	• 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。 • 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。 • 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：< データベース名 >。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。 • < ユーザ名 > 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。 • RN_CRYPTO_KEY 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_CRYPTO_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。

監視	説明 / 対応策
DatabaseDataMonitor	• 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • プルーナ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。
DiskMonitor	< ファイルシステム名 > ディスク / ファイルシステムの空き容量が < 数値 > バイトしかありません。エラーのしきい値は < 制限値 > 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。
HTTPMonitor	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。
LDAPMonitor	• 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。 • LDAPMonitor の例外：javax.naming。通信の例外：< ホスト名 >：389：< ホスト名 > 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。 • LDAPMonitor の例外：javax.naming。通信の例外：< ホスト名 >：389：< ホスト名 > 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。 • 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。

監視	説明 / 対応策
LicenseMonitor	「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。）
MemoryMonitor	空き容量が < バイト数 > 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。
RMIMonitor	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。
RunExternalTask Monitor	• CreateProcess：< パス名 >\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。 • CreateProcess：< パス名 >\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。 • < パス名 > ディレクトリから < パス名 >\tc_test.bat を実行しています。結果コード：0 Got output< テキスト > 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。
SMTPMonitor	• 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。 • < ホスト名 >25 への Telnet 接続を開けません。：NA から < ホスト名 > 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。 • 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。

監視	説明 / 対応策
SSHMonitor	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 ポートをリスン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。
SyslogMonitor	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。
TelnetMonitor	• < ホスト名 > 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。 • 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。
FTPMonitor	• 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。 • 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。 • 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。
TFTPMonitor	• 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。 • 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。 • 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。

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	次のオプションのいずれかを選択します。 • 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。 • 再開：管理エンジンを再起動します。
HP Live Network	次のオプションのいずれかを選択します。 • 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。 • 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。例えば 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、「[ソフトウェアレベル] ページのフィールド」（536 ページ）を参照してください。

フィールド	説明 / アクション
TFTP サーバ	次のオプションのいずれかを選択します。 • 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。（**注意**：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。） • 停止：TFTP サーバを停止します。 • 再開：TFTP サーバを再起動します。
FTP サーバ	次のオプションのいずれかを選択します。 • 開始：Starts the FTP server.NA では、主に設定の取得と配布に使用します。（**注意**：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。） • 停止：FTP サーバを停止します。 • 再開：FTP サーバを再起動します。
Syslog サーバ	次のオプションのいずれかを選択します。 • 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。 • 停止：Syslog サーバを停止します。 • 再開：Syslog サーバを再起動します。
ソフトウェアイメージ管理サーバ	次のオプションのいずれかを選択します。 • 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、「[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」（289 ページ）を参照してください。 • 停止：ソフトウェアイメージ管理サーバを停止します。 • 再開：ソフトウェアイメージ管理サーバを再起動します。

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。例えば、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。

- Device
- 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すが、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」（351 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、特定の結果が予期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 は可能なかぎ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。例えば、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。例えば、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て、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。詳細については、「第 7 章： タスクの予定」（351 ページ）を参照してください。

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」（127 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」（66 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、ユーザが設定をその変更するための性能管理技術については、「サーバ監視」（107 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、「[トラブルシューティングの送信] ページのフィールド」（34 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、「[トラブルシューティングの送信] ページのフィールド」（34 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、「ログ記録」（122 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	ログ記録のレベルを選択します。次のオプションがあります。 • 致命的（メッセージ数が最少） • エラー（デフォルト） • デバッグ • トレース（メッセージ数が最多） 詳細については、「ログのレベル」（122 ページ）を参照してください。
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。（**注意**：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。

デバイス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	「はじめに」（131 ページ）
デバイスの追加	「デバイスの追加」（133 ページ）
デバイスの編集	「[デバイスの編集] ページのフィールド」（142 ページ）
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」（149 ページ）
新規デバイステンプレートの追加	「新しいデバイステンプレートの追加」（157 ページ）
デバイスの追加ウィザードの使用	「デバイスの新規作成ウィザードの使用」（161 ページ）
デバイスのインポート	「デバイスのインポート」（163 ページ）
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の作成」（167 ページ）
デバイスグループの追加	「デバイスグループの追加」（172 ページ）
動的グループ	「動的デバイスグループ」（177 ページ）
デバイスセレクタ	「デバイスセレクタ」（180 ページ）
デバイスグループの表示	「デバイスグループの表示」（183 ページ）
デバイスとユーザのセグメント化	「デバイスとユーザのセグメント化」（188 ページ）
HP Gateway の設定	「HP Gateway の設定」（192 ページ）
デバイスグループの編集	「デバイスグループの編集」（204 ページ）
デバイスの一括編集	「デバイスの一括編集」（206 ページ）
デバイスドライバの検出	「デバイスドライバの検出」（209 ページ）
Telnet/SSH セッションのリスト表示	「Telnet/SSH セッションのリスト表示」（212 ページ）
要塞ホストの使用	「要塞ホストの使用」（215 ページ）

デバイスの追加へのナビゲート

はじめに

デバイスを追加すると、HP Network Automaton（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」（257 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] 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」(422 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方法の詳細については、「デバイスの新規作成ウィザードの使用」（161 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 >	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。（詳細は、「[パーティション] ページのフィールド」（199 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。 **注意**：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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。）
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。デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。
変更の検出とポーリング	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）、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。 • 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。 • 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。

フィールド	説明 / アクション
管理ステータス	次のオプションのいずれかを選択します。 • 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。 • 実稼動前：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。（**注意**：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）。 • 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。
デバイスドライバ	次のオプションのいずれかを選択します。 • 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。（**注意**：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。） • 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。
コメント	デバイスに関するコメントを入力します。
パスワード情報	
ネットワーク全体のパスワードルールの使用	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。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。 **注意**：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、「デバイスパスワードルールの作成」（167 ページ）を参照してください。
このパスワードルールを最初に使用	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。

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	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。 • 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よう構成されている場合、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。 • 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。 • パスワードの確認：パスワードを再度入力します。 • 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。（**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。） • 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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 暗号化パスワードの確認：SNMPv3 暗号化パスワードを再度入力します。
デバイスアクセス設定	

フィールド	説明 / アクション
デバイスアクセス設定	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、「TACACS+ 認証」（96 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、「SecurID を使用したログイン」（788 ページ）を参照してください。 **注意**：デバイスアクセス設定の使用方法の詳細については、[デバイスアクセス設定の使用方法] 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。
NAT 情報	
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 アドレスを入力します。（**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。
接続情報	

フィールド	説明 / アクション
接続方法	NA では、次のプロトコルを組み合わ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。 • SNMP • SNMPv1 または SNMPv2c（コミュニティ文字列認証） • 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。 • RLogin • Telnet • 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。） • [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。 • [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。
転送プロトコル	次のいずれかの転送プロトコルを選択します（複数可）。 • SCP • SFTP • FTP • TFTP

フィールド	説明 / アクション
要塞ホスト	[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。 • 要塞ホストの IP アドレスまたはホスト名 • 要塞ホストへのアクセスに使用するユーザ名（通常は root） • 要塞ホストへのアクセスに使用するパスワード • パスワード確認のための再入力 （**注意**：要塞ホスト情報を変更するには、「[デバイス管理対象 IP アドレス] ページのフィールド」（303 ページ）を参照してください）。
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：リレーホストのホスト名または IP アドレスを入力します。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。

フィールド	説明 / アクション
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。
階層レイヤ	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。例えば、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、「ダイアグラム」（752 ページ）を参照してください。 **注意**：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、「appserver.rcx ファイルの編集」（762 ページ）を参照してください）。 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。 • 未設定レイヤ • コア • 分散 • アクセス • エッジ

フィールド	説明 / アクション
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）。

[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）	デバイスの IP アドレスまたは DNS ホスト名を表示します。
ホスト名	該当する場合、デバイスのホスト名を表示します。
サイト < 名 >	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。（詳細は、「[パーティション] ページのフィールド」（199 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。 **注意**：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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。）
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。デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。
変更の検出とポーリング	次のオプションが用意されています。 • 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。 • 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。 • 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。

フィールド	説明 / アクション
管理ステータス	次のオプションが用意されています。 • 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。 • 実稼動前：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。（**注意**：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）。 • 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。
デバイスドライバ	次のオプションが用意されています。 • 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。 • 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。
コメント	デバイスについてのコメントを表示します。
パスワード情報	
ネットワーク全体のパスワードルールの使用	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。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。 **注意**：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、「デバイスパスワードルールの作成」（167 ページ）を参照してください。
このパスワードルールを最初に使用	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。

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	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。 • 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よう構成されている場合、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。 • 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。 • パスワードの確認：パスワードを再度入力します。 • 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。（**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。） • 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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 暗号化パスワードの確認：SNMPv3 暗号化パスワードを再度入力します。
最後に使用したパスワードルールのリセット	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。
デバイスアクセス設定	

フィールド	説明 / アクション
デバイスアクセス設定	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、「TACACS+ 認証」（96 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、「SecurID を使用したログイン」（788 ページ）を参照してください。 **注意**：デバイスアクセス設定の使用方法の詳細については、[デバイスアクセス設定の使用方法] 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。
NAT 情報	
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。
接続情報	

フィールド	説明 / アクション
接続方法	NA では、次のプロトコルを組み合わ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。 • SNMP • SNMPv1 または SNMPv2c（コミュニティ文字列認証） • 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。 • RLogin • Telnet • 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。） • [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、「[デバイス管理対象 IP アドレス] ページのフィールド」（303 ページ）を参照してください）。 **注意**：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。
転送プロトコル	転送プロトコルには、以下があります。 • SCP • SFTP • FTP • TFTP

フィールド	説明 / アクション
要塞ホスト	要塞ホスト情報を変更するには、「[デバイス管理対象 IP アドレス] ページのフィールド」（303 ページ）を参照してください）。

ACL 解析

次のオプションが用意されています。

- 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。

フィールド	説明 / アクション
階層レイヤ	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。例えば、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、「ダイアグラム」（752 ページ）を参照してください。 **注意**：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、「appserver.rcx ファイルの編集」（762 ページ）を参照してください）。 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。 • 未設定レイヤ • コア • 分散 • アクセス • エッジ
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。例えば、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」（157 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、実稼働前デバイス）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」（133 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。Refer to 「新しいデバイステンプレートの追加」（157 ページ）。
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」（708 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」（440 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」（663 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、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。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」（149 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。「新しいデバイステンプレートの追加」（157 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、「[デバイステンプレートの詳細] ページのフィールド」（153 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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。

フィールド	説明 / アクション
アクション	次のアクションを選択できます。 • 編集 : [デバイステンプレートの編集] 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」（151 ページ）を参照してください。 • 構成を表示 : [構成を表示] ページが開きます。「[デバイス構成の詳細] ページのフィールド」（223 ページ）を参照してください。 • 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、「[ポリシー準拠のテスト] ページのフィールド」（541 ページ）を参照してください。

[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	次のオプションを選択できます。 • 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。「[デバイステンプレート] ページのフィールド」（151 ページ）を参照してください。 • 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。 • 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。 • 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。「[デバイス構成] ページのフィールド」（220 ページ）を参照してください。 • 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、「ACL の表示」（868 ページ）を参照してください。 • 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、「[デバイスインターフェイス] ページのフィールド」（263 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
編集メニュー	次のオプションを選択できます。 • 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えます。詳細については、「[テンプレート構成を編集] ページ」（155 ページ）を参照してください。 • 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。「[デバイステンプレートの新規作成] ページのフィールド」（157 ページ）を参照してください。 • 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。 • 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。「[デバイステンプレート] ページのフィールド」（151 ページ）を参照してください。 • 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。
プロビジョニングメニュー	次のオプションを選択できます。 • 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。「デバイス固有のテンプレート」（160 ページ）を参照してください。
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。
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。

メニューオプション	説明 / アクション
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」（300 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] 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	デバイステンプレート名を入力します。
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）。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、「デバイスとユーザのセグメント化」（188 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。

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、「デバイステンプレート」（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
接続方法	NA では、次のプロトコルを組み合わ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。 • SNMP • SNMPv1 または SNMPv2c（コミュニティ文字列認証） • 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。 • RLogin • Telnet • 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。）
転送プロトコル	次のいずれかの転送プロトコルを選択します（複数可）。 • SCP • FTP • TFTP

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。

フィールド	説明 / アクション
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。
階層レベル	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。例えば、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、「ダイアグラム」（752 ページ）を参照してください。 **注意**：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、「appserver.rcx ファイルの編集」（762 ページ）を参照してください）。 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。 • 未設定レイヤ • コア • 分散 • アクセス • エッジ
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	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。 • すべて • アクティブ • 実稼動前
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。
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、「デバイスとユーザのセグメント化」（188 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。 • 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。「[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」（440 ページ）を参照してください。 • 構成の比較：[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」（227 ページ）を参照してください。

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サード] 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	次の情報を入力します。 • 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。 • コメント：デバイスに関するコメントを入力します。 • 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（**注意**：実稼働前デバイスは、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）。 終了したら、次のいずれかをクリックします。 • 次へ：[認証] ページが開きます （以下参照）。 • 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。

手順	説明 / アクション
手順 2：デバイスを認証	次のオプションのいずれかを選択します。 • 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。「デバイスパスワードルールの作成」（167 ページ）を参照してください。 • 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。 終了したら、次のいずれかをクリックします。 • 戻る：[デバイスを作成] 手順に戻ります。 • 次へ：[構成] ページが開きます（以下参照）。 • 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。
手順 3：デバイスを構成	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。 • 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。 • 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。（**注意**：変更検出の正しいログレベルが設定されます。） [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。

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。「[インポート] ページのフィールド」（417 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」（167 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」（54 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。「デバイスとパスワードのデータを含む CSV ファイルの作成」（164 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」（422 ページ）を参照してください。

デバイスとパスワードのデータを含む CSV ファイルの作成

CSV デバイスデータファイル（device.csv）では、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入力されています。最も一般的に使用される列名を次に示します。列名は大文字と小文字を区別します。

列名	説明 / アクション
primaryIPAddress	デバイスのプライマリ IP アドレスです。この列が唯一の必須フィールドです。
deviceDriver	デバイスドライバの名前です。
deviceGroupName	デバイスが属するグループの名前です。
hostName	デバイスのホスト名です。
consoleIPAddress	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。
consolePort	コンソールのポート番号です。デバイスアクセスにコンソールサーバを使用するかどうかを指定します。（**注意**：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。）
accessMethods	デバイスのアクセス方法です。accessMethods の構成と例を以下に挙げます。 access_methods[+connect_methods[+console]] • CLI:TFTP+ssh+console • CLI:FTP+ssh:telnet • SNMP:TFTP 「access method」の箇所に使用できるのは、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。（**注意**：「connect_methods」は CLI がサポートされている場合に限り適用できます。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。）
managementStatus	デバイスがアクティブ（管理対象）、非アクティブ（管理対象ではない）、または実稼働前（構成が未完了）、またはデバイステンプレートのいずれであるかを示します。数値を以下に挙げます。 • 0：アクティブ（デフォルト） • 1：非アクティブ • 2：デバイステンプレート • 3：実稼働前
assetTag	デバイスの資産タグ文字列です。

列名	説明 / アクション
siteName	デバイスが属するサイトの名前です。
comments	デバイスの説明文です。
deviceCustom1	[カスタムデータ] ページの [デバイス] セクションでは、最大 6 つのカスタムフィールドを作成できます。データをインポートする前に、これらのフィールドを作成します。

NA では、デバイス構成から次のフィールドが自動的に入力されます。[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、デバイスデータのインポート時に手動でこれらのフィールドを入力すると、データが上書きされます。詳細については、「サーバ」（65 ページ）を参照してください。

- ホスト名
- シリアル番号
- 場所
- ベンダー
- モデル
- オペレーティングシステム

注意： 空白の列には列名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。

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詳細情報を表示するには、次の手順に従います。」（185 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」（167 ページ）を参照してください。
3. デバイスが属するグループを含むインポート済みデバイス。「デバイスのインポート」（163 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」（209　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、Device Driver Reference（DRS）ドキュメントを参照してください。DRS は、新しく自動化されたドライバリリースおよびデリバリシステムです。

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と、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」（54 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」（54 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、「[デバイスパスワードルール] ページのフィールド」（169 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。

フィールド	説明 / アクション
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。 • IP 範囲 • ホスト名 • デバイスグループ
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。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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。 **注意**：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」（169 ページ）を参照してください。
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	各ルールで次のアクションを選択できます。 • 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、「[デバイスパスワードルール] ページのフィールド」（169 ページ）を参照してください。（**注意**：[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。）

[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、AES 256 ビット鍵で暗号化され、NA データベースに格納されます。各 NA インストールで一意の鍵が作成されます。

フィールド	説明 / アクション
ルール定義	
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、「デバイスとユーザのセグメント化」（188 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レ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。
パスワード情報	

フィールド	説明 / アクション
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。 （**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。）
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。
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。

フィールド	説明 / アクション
デバイスアクセス設定の表示	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。 • 実行モードプロンプト • 構成モードプロンプト • システム管理プロンプト **注意**：デバイスパスワード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方法の詳細については、[デバイスアクセス設定の使用方法] リンクをクリックしてください。

終了時に、必ず [保存] をクリックしてください。[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）

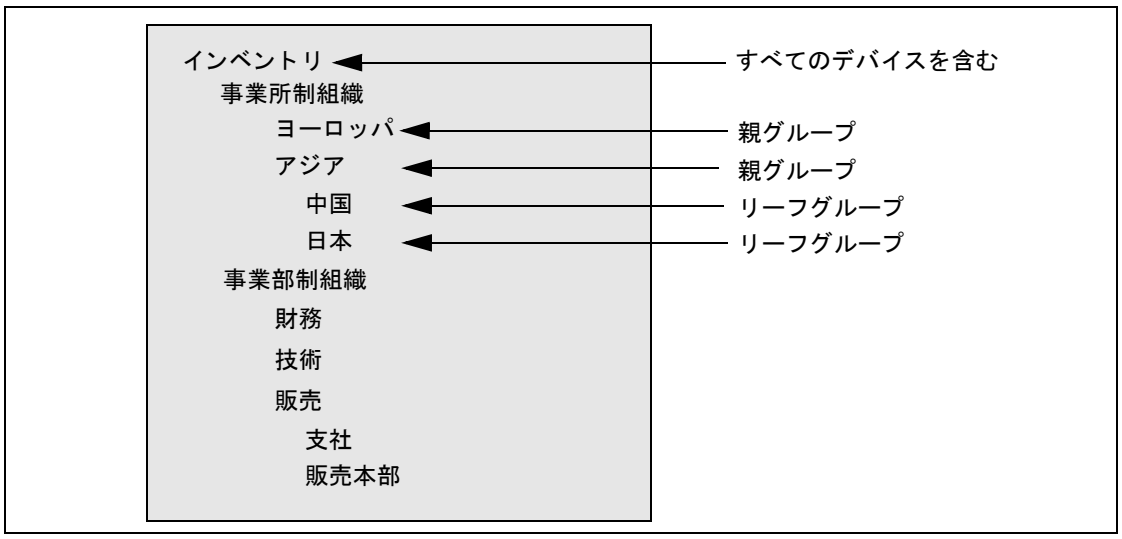
[デバイスグループ] ページには、初期設定でインベントリグループというシステムグループが含まれています。インベントリグループには、NA に追加されるすべてのデバイスが含まれます。ただし、ユーザ定義のグループを作成すると、そのグループもこのページに表示されます。

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すが、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。



例えば、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。（詳細は、「[パーティション] ページのフィールド」（199 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。

フィールド	説明 / アクション
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。 **注意**：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。 • 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：デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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、「動的デバイスグループ」（177 ページ）を参照してください。

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。「[デバイスグループ] ページのフィールド」（183 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。（詳細は、「[パーティション] ページのフィールド」（199 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	• 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 >>] 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。 • 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 [<< 削除] をクリックします。

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、「デバイスグループの追加」（172 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、「[親グループの新規作成] ページのフィールド」（175 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、「[デバイスグループの詳細] ページのフィールド」（185 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	次のオプションを選択できます。 • 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、「[グループを編集] ページのフィールド」（204 ページ）を参照してください。 • 削除：グループを完全に削除します。 • ダイアグラム：[ダイアグラム] ページが開きます。「ダイアグラム」（752 ページ）を参照してください。 • 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。

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
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」（173 ページ）を参照してください。	検索基準のセット、ルールのセットのいずれか、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。
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。	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。
グループからデバイスを手動で削除できます。	グループからデバイスを手動で削除できません。

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。例えば、[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」（173 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。
   - 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。）
   - 必要に応じて、ブール演算子（AND/OR）を使用して検索をフィルタする。
   - 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」（65 ページ）を参照してください。

デバイスセレクタ

デバイスセレクタには次の 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、例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、例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 つのセレクタによって、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、デバイスセレクタは閉じています。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。

例えば「`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。例えば「`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レクタ] 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、「パーティション」（198 ページ）を参照してください。

デバイスセレクタボタン

次のデバイスセレ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。[デバイスセレクタ] ウィンドウまたは [デバイスグループセレクタ] 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、[デバイスセレクタ] ウィンドウまたは [デバイスグループセレクタ] 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、[デバイスセレクタ] ウィンドウまたは [デバイスグループセレクタ] ウィンドウを閉じます。

注意： [デバイスセレクタ] ウィンドウまたは [デバイスグループセレクタ] 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。

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、「デバイスグループの追加」（172 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、「[親グループの新規作成] ページのフィールド」（175 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、「[デバイスグループの詳細] ページのフィールド」（185 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。

フィールド	説明 / アクション
アクション	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。 • 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、「[グループを編集] ページのフィールド」（204 ページ）を参照してください。 • 削除：グループを完全に削除します。 • ダイアグラム：[ダイアグラム] ページが開きます。「ダイアグラム」（752 ページ）を参照してください。 • 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。

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] メニューバーで [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、「[デバイスグループ] ページのフィールド」（183 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、「デバイスの追加」（133 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、「デバイスグループの追加」（172 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、「親グループの追加」（175 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、「[グループを編集] ページのフィールド」（204 ページ）を参照してください。
Update Device List link (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、「タスクとは」（354 ページ）を参照してください。

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。 • 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。 • 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。 • 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、「[デバイスを一括編集] ページのフィールド」（206 ページ）を参照してください。 • ダイアグラム：[ダイアグラム] ページが開きます。「ダイアグラム」（752 ページ）を参照してください。 • 削除：選択したデバイスが削除されます。 • 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。 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。
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。
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。）
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。

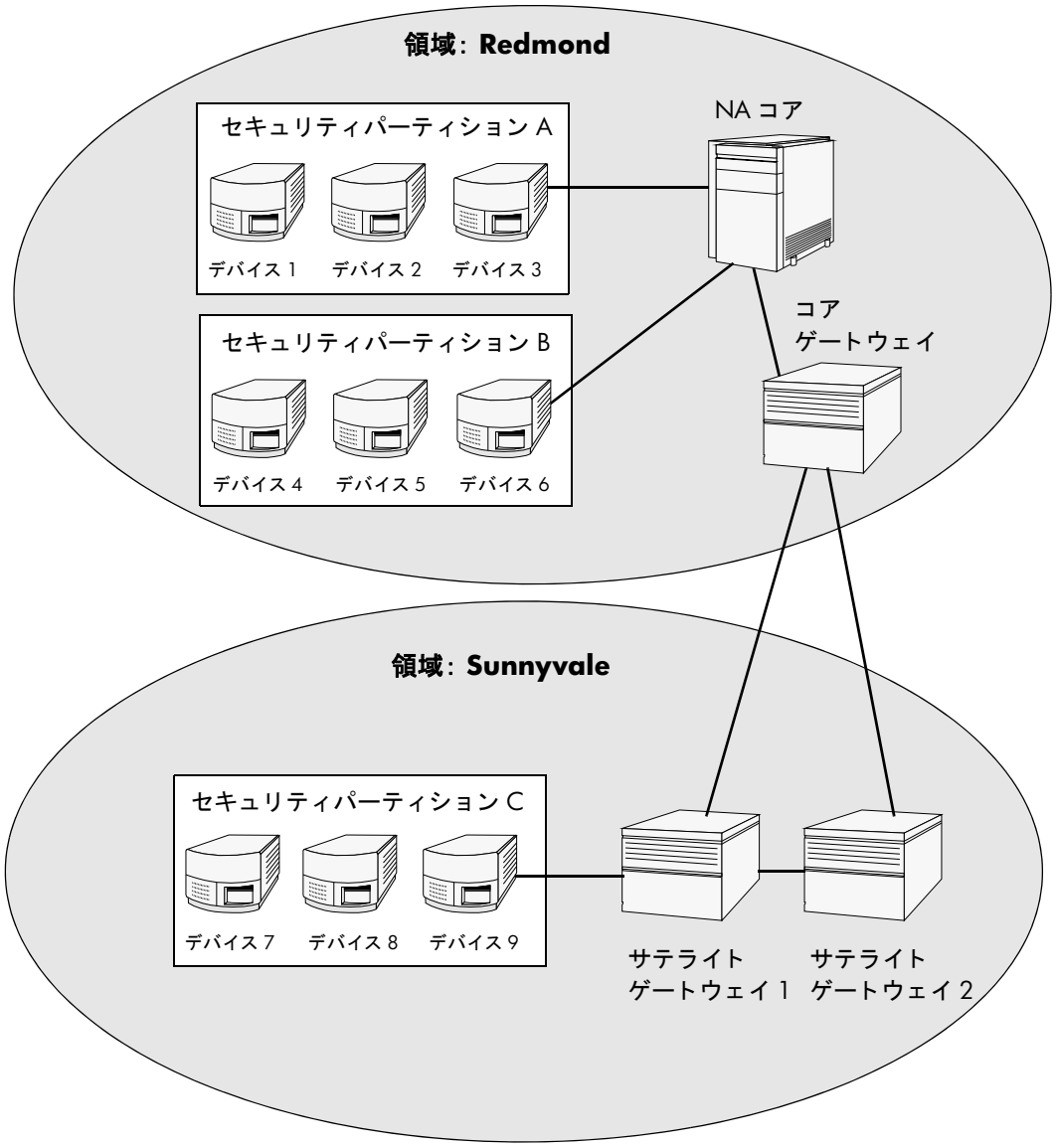
フィールド	説明 / アクション
アクション	次のアクションを選択できます。 • 編集：[デバイスを編集] ページが開きます。そのページでデバイスの情報を編集できます。詳細については、「[デバイスの編集] ページのフィールド」（142 ページ）を参照してください。 • Telnet：[Telnet] ウィンドウが開きます。 • SSH：[SSH] ウィンドウを開きます。 • 構成を表示：[現在の構成] ページが開きます。このページでは、最新の構成を表示してコメントを追加できます。

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、『*HP Network Automation 9.0 Multimaster Distributed System on Oracle User's Guide*』、または『*HP Network Automation 9.0 Distributed System on SQL Server User's 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。例えば、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」（54 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 9.0 Distributed System on Oracle User's 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。

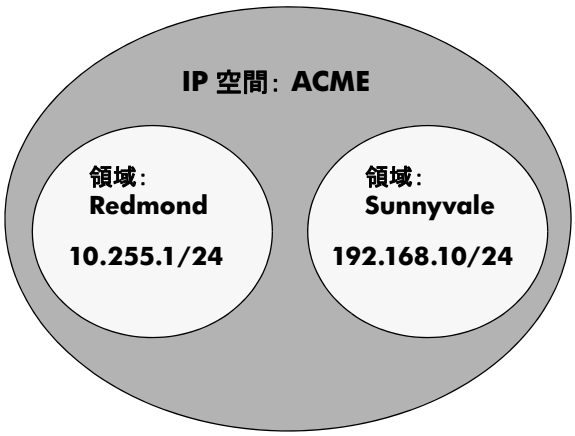
HP Gateway を NA と併用することで、重複 IP アドレス（同一 IP アドレスを持つ複数のデバイス）のサポートが得られます。さらに、管理対象とするデバイスと同一の LAN 上に NA リモートエージェントをインストールすることで、Syslog および TFTP をローカルで使用してデバイスを管理できます。詳細については、「[リモートエージェントの配布] タスクページのフィールド」（468 ページ）を参照してください。

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 9.0 Multimaster Distributed System on Oracle User's 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： サテライト構成のインストール方法の詳細については、『*HP Network Automation 9.0 Satellite User's 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用します。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用します。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ー的に近くなければ、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ー的に近い位置に 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 は、次のプラットフォーム上でサポートされます。

- RedHat-Linux-3AS、および 4AS
- SuSE-Linux-9ES
- SunOS-5.9、および 5.10

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はあります。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、『*HP Network Automation 9.0 Satellite User's 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」（54 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」（197 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の配布] 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、「[リモートエージェントの配布] タスクページのフィールド」（468 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。

フィールド	説明 / アクション
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 9.0 Satellite User's 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 9.0 Satellite User's 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。**注意**：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、「パーティション」（198 ページ）を参照してください。
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 9.0 Multimaster Distributed System on Oracle User's 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、「[リモートエージェントの配布] タスクページのフィールド」（468 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。 • 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、「[ゲートウェイの編集] ページのフィールド」（197 ページ）を参照してください。

[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」（188 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。例えば、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、「[デバイスの新規作成] ページのフィールド」（134 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、「[パーティションの新規作成] ページ」（200 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。**注意**：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。（『*NA 9.0 Multimaster Distributed System on Oracle User's Guide*』、または『*NA 9.0 Distributed System on SQL Server User's 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。**注意**：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。
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。 • 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、「[パーティションの編集] ページのフィールド」（201 ページ）を参照してください。 • 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。

[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、デバイスセレクタを使用して、パーティションに含めるデバイスを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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、「重複 IP ネットワーク」（191 ページ）を参照してください。）
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	デバイスセレクタの [デバイス] ボックスにデバイスのリストが表示されます。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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。（詳細は、「[インベントリ] ページのフィールド」（237 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」（188 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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」（237 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] メニューバーで [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。 • デバイスセレ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：デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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、ブール式（and/or）を使っ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。

フィールド	説明 / アクション
子デバイスグループ	• 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 >>] をクリックします。 • 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 [<< 削除] をクリックします。

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。

フィールド	説明 / アクション
接続方法を設定	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。 接続方法： • SNMP • 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。 • SNMPv1 または SNMPv2c（デフォルト） • Telnet • 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。 転送プロトコル（デフォルト） • SCP • SFTP • FTP • TFTP
要塞ホスト情報を設定	オンにして、次の情報を入力します。 • 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。 • IP アドレスまたはホスト名 • ユーザ名 • パスワード • パスワードの確認
最後に使用されたパスワードのリセット	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。

フィールド	説明 / アクション
ACL 解析を設定	オンにして、次のオプションのいずれかを選択します。 • 有効（各スナップショットで ACL を解析して格納） • 無効（各スナップショットで ACL を解析しない）
階層レイヤを設定	ドロップダウンメニューから階層レイヤを選択します。
カスタムサービスタイプの設定	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）。
カスタムデータフィールドを設定	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、「拡張カスタムフィールド設定」（693 ページ）を参照してください。

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、Device Driver Reference（DRS）ドキュメントを参照してください。DRS は、新しく自動化されたドライバリリースおよびデリバリシステムです。

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」（371 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。例えば、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」（83 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： お使いのコンピュータに 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。 • 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。 • 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。

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. 例えば、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」（134 ページ）を参照してください。

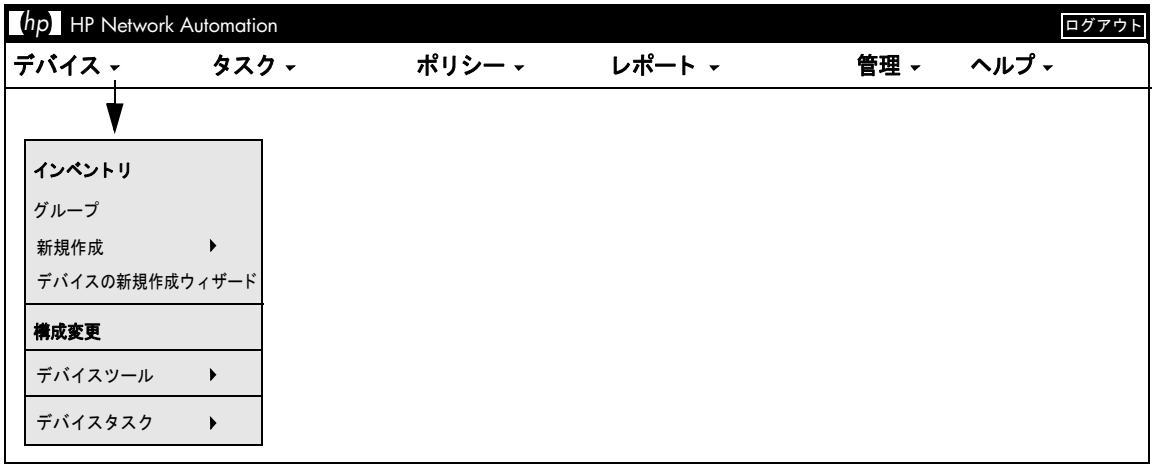
新規デバイスのデフォルトで Telnet および SSH アクセスに要塞ホストを使用するよう指定するには、[管理] メニューバーから [システム管理設定] を選択して、[デバイスアクセス] をクリックします。詳細については、「[デバイスアクセス] ページのフィールド」（54 ページ）を参照してください。

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	「はじめに」（218 ページ）
デバイス構成変更の表示	「デバイス構成変更の表示」（219 ページ）
デバイス構成の比較	「デバイス構成の比較」（227 ページ）
デバイス構成の配布	「デバイス構成の展開」（229 ページ）

デバイス構成の変更へのナビゲート



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 アカウンティングログ、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」（873 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」（223 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	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。
最終のスナップショットの結果	前回のスナップショットの結果を表示します。例えば、「構成が変更されませんでした」と表示されます。
表示メニュー	詳細については、「表示メニューオプション」（257 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、「編集メニューオプション」（300 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、「プロビジョニングメニューオプション」（310 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、「接続メニューオプション」（312 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、「[構成の検索結果] ページのフィールド」（609 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、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。 • 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 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ハイライト表示されます。 • 削除：オンにしたデバイス構成を削除します。 横の [選択] ドロップダウンメニューにより、すべてのデバイス構成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
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。
アクション	次のアクションを選択できます。 • 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ハイライト表示されます。 • 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、「[デバイス構成の詳細] ページのフィールド」（223 ページ）を参照してください。 • 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 インターフェース、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、「表示メニューオプション」（257 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」（223 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」（227 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 」(404 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。例えば、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。例えば、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	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	前回のスナップショットの結果を表示します。例えば、「構成が変更されませんでした」と表示されます。

フィールド	説明 / アクション
デバイスを監視	[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。 • デバイスアクセスエラー • デバイスがブートしました • デバイス構成の変更 • デバイスが削除されました • デバイス診断の変更 • デバイスが編集されました • デバイスソフトウェアの変更 • ソフトウェアの脆弱性が検出されました **注意**：[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。「[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」（567 ページ）を参照してください。 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。
表示メニュー	詳細については、「表示メニューオプション」（257 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、「編集メニューオプション」（300 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、「プロビジョニングメニューオプション」（310 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、「接続メニューオプション」（312 ページ）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。（**注意**：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）。詳細については、「[構成を配布] タスクページのフィールド」（230 ページ）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）。（**注意**：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）。詳細については、「[構成を配布] タスクページのフィールド」（230 ページ）を参照してください。

フィールド	説明 / アクション
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。
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ハイライト表示されます。**注意**：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、「デバイス構成データの編集」（226 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」（688 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、例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す。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] のメニューバーから、[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。（**注意**：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）。（**注意**：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）。

フィールド	説明 / アクション
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、「[デバイス構成の詳細] ページのフィールド」（223 ページ）を参照してください。**注意**：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] のメニューバーから、[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）。
   - 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。
   - 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。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
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、「ログ記録」（122 ページ）を参照してください。）
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拠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」（66 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] の下の [サーバ] ページで有効にす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。 • 標準の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を使用（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 （詳細は、「[構成管理] ページのフィールド」（41 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。

フィールド	説明 / アクション
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、値は考慮されません。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	
再試行カウント	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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、次の条件に従って繰り返します。次のオプションのいずれかを選択します。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。

フィールド	説明 / アクション
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：繰り返しの回数を入力します。 • 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。
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、「ログ記録」（122 ページ）を参照してください。

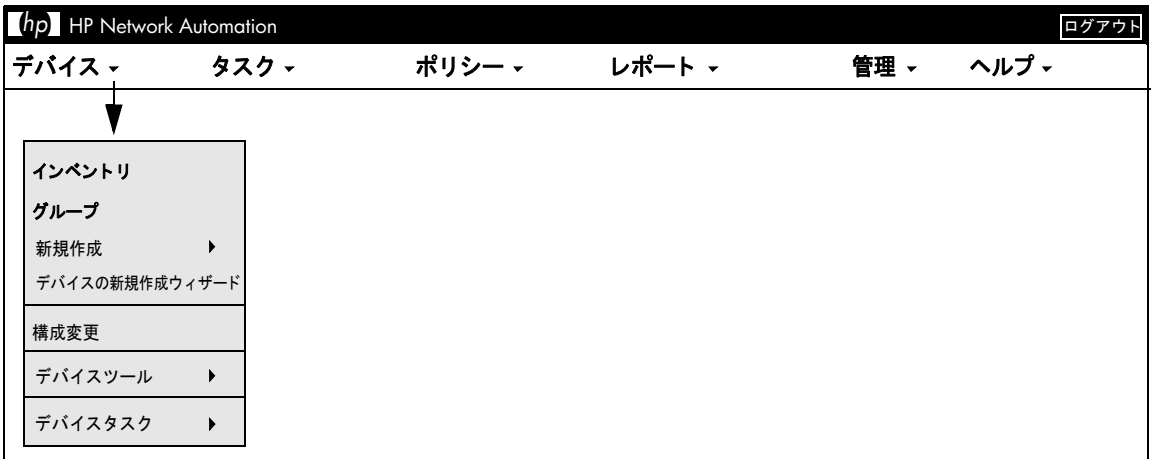
終了時に、必ず [タスクを保存] をクリックしてください。

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	「デバイスの表示」（237 ページ）
デバイスグループの表示	「デバイスグループの表示」（240 ページ）
デバイスの予約	「デバイスの予約」（242 ページ）
デバイス詳細の表示	「デバイス詳細の表示」（245 ページ）
NA/SA 統合	「NA/SA 統合」（250 ページ）
表示メニューオプション	「表示メニューオプション」（257 ページ）
仮想ローカルエリアネットワーク（VLAN）	「仮想ローカルエリアネットワーク（VLAN）」（274 ページ）
編集メニューオプション	「編集メニューオプション」（300 ページ）
プロビジョニングメニューオプション	「プロビジョニングメニューオプション」（310 ページ）
接続メニューオプション	「接続メニューオプション」（312 ページ）

デバイス情報へのナビゲート



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」（133 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、「デバイスグループの表示」（240 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、「デバイスの追加」（133 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、「デバイスグループの追加」（172 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、「親グループの追加」（175 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、「タスクとは」（354 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。

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。 • 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。 • 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。 • 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、「[デバイスを一括編集] ページのフィールド」（206 ページ）を参照してください。 • ダイアグラム：[ダイアグラム] ページが開きます。「ダイアグラム」（752 ページ）を参照してください。 • 削除：選択したデバイスが削除されます。 • 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、「アドホックデバイスグループへのタスクの実行」（354 ページ）を参照してください。 隣の [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。
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、「表示メニューオプション」（257 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。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、「表示メニューオプション」（257 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。）

フィールド	説明 / アクション
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。 • 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。「[デバイスの編集] ページのフィールド」（142 ページ）を参照してください。 • Telnet：[Telnet] ウィンドウが開きます。 • SSH：[SSH] ウィンドウを開きます。 • 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。
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] 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	[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。新規デバイスグループの作成の詳細については、「デバイスグループの追加」（172 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、「親グループの追加」（175 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。親グループが別の親グループの子でなければインデントはされません。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、「[デバイスグループ] ページのフィールド」（240 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は、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。）

フィールド	説明 / アクション
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。
アクション	[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。 • 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。 • 削除：デバイスグループを削除できます。 • 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、「ダイアグラム」（752 ページ）を参照してください。 • 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。

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」（75 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」（481 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。

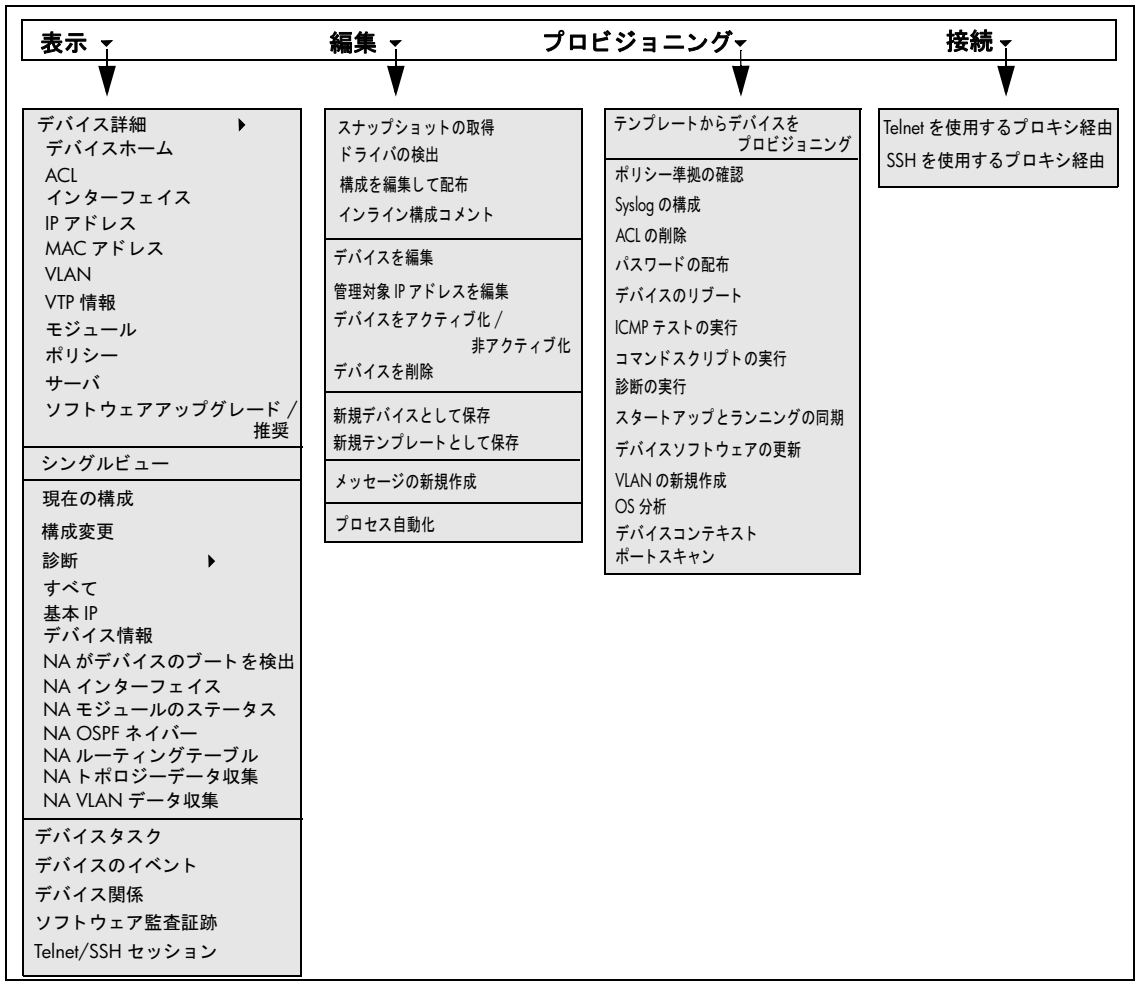
セルに表示されているリンクをクリックすると、[タスク] パネルの情報が更新されます。マルチタスクプロジェクトに解除されていないデバイス予約の競合がある場合は、セルは黄色で強調表示されます。マルチタスクプロジェクトの構成の詳細については、「マルチタスクプロジェクトの予定」（481 ページ）を参照してください。

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）。

次の図は、[デバイス詳細] ページで実行できるタスクの概要を示します。メニューのオプションは、表示しているデバイスによって変わります。



[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	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	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。例えば、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。 • スタートアップを表示 : [デバイス構成] ページが開きます。 • 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。 • 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。

フィールド	説明 / アクション
デバイスを監視	[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。 • デバイスアクセスエラー • デバイスがブートしました • デバイス構成の変更 • デバイスが削除されました • デバイス診断が変化しました • デバイスが編集されました • デバイスソフトウェアの変更 • ソフトウェアの脆弱性が検出されました **注意**：[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。「[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」（567 ページ）を参照してください。 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。
表示メニュー	[表示] メニューが開きます。詳細については、「表示メニューオプション」（257 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、「編集メニューオプション」（300 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、「プロビジョニングメニューオプション」（310 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、「接続メニューオプション」（312 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。

フィールド	説明 / アクション
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）。**注意**：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。「[構成管理] ページのフィールド」（41 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。
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。

フィールド	説明 / アクション
変更の検出とポーリング	次のいずれかを表示します。 • 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。 • 無効：NA がデバイスに対して定期的なポーリングやそのほかの管理をしません。
管理ステータス	次のいずれかを表示します。 • アクティブ：NA はデバイスの構成変更を記録します。 • 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。
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もあります。例えば、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」（752 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」（95 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」（752 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」（265 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」（288 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」（99 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：

- サーバー 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 のネットワード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」（263 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 Remote Method Protocol（JRMP）での Java RMI のみ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 JRMP は次のポートを使用します。

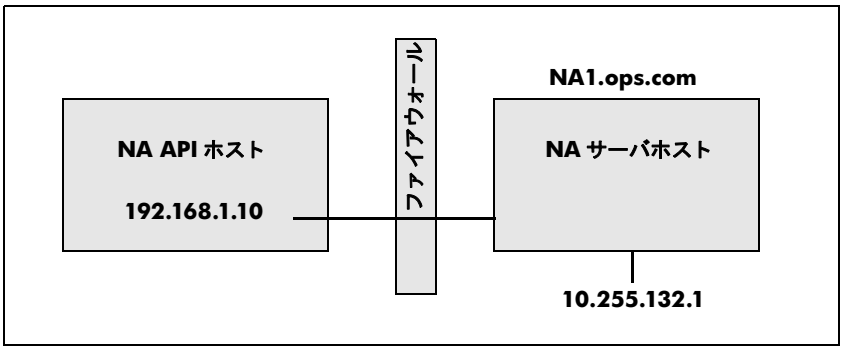
- Java Naming and Directory Interface（JNDI）（通常はポート 1099）
- RMI（通常はダイナミック 1098）
- RMI オブジェクト（通常はポート 4444）

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

1. ファイアウォールがポート 1098、1099、4444 を許可する構成にします。NA サーバホストがファイアウォールの両側で同一の IP アドレスを持てば、構成は完了です。NA 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つ場合は、手順 2 に進んでください。
2. 「`$NA/server/ext/jboss/server/default/conf/jnp.properties`」ファイルを作成して、`java.rmi.server.useLocalHostname=true` を含むことで、NA が（IP アドレスの代わりに）RMI サーバのホスト名を使用するように構成します。

3. ファイルを保存して NA サーバを再起動します。
4. 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 が稼働しています。ファイアウォールの外側で NA1.ops.com にアクセスするには、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 192.168.1.10 に適切に解決する必要があります。



高レベルでは、Java RMI/JRMP プロトコルは次のように機能します。

1. クライアントは、ホスト 192.168.1.10 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 192.168.1.10 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 192.168.1.10 のポート 4444 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. 「`$NA/server/ext/jboss/server/default/conf/jboss-service.xml`」ファイルを編集して、例えば、「1099」を「1199」に変更します。
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。例えば、「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. 「`$NA/server/ext/jboss/server/default/conf/jboss-service.xml`」ファイルを編集して、例えば、「1098」を「1198」に変更します。
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. 「*$NA/server/ext/jboss/server/default/conf/jboss-service.xml*」ファイルを編集して、例えば、「4444」を「4445」に変更します。
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> タグの間のどこか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： 注意：スナップショットタスクの実行後に、*「$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	次のオプションを選択できます。 • 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。 • 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、「ACL の表示」（868 ページ）を参照してください。 • 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 トポロジー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、「[デバイスインターフェイス] ページのフィールド」（263 ページ）を参照してください。 • 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、「[デバイス IP アドレス] ページのフィールド」（270 ページ）を参照してください。 • 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、「[デバイス MAC アドレス] ページのフィールド」（272 ページ）を参照してください。 • 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、「[デバイス VLAN] ページのフィールド」（276 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
デバイス詳細（*続き*）	• 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、「[VTP 詳細] ページのフィールド」（281 ページ）を参照してください。 • 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、「[デバイスブレード / モジュール] ページのフィールド」（285 ページ）を参照してください。 • 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、「[デバイスポリシー] ページのフィールド」（286 ページ）を参照してください。 • 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、「[サーバ] ページのフィールド」（288 ページ）を参照してください。 • 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、「[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」（289 ページ）を参照してください。
シングルビュー	[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、「イベントの連結ビュー（シングルビュー）」（674 ページ）を参照してください。
現在の構成	[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、「[デバイス構成] ページのフィールド」（220 ページ）を参照してください。
構成変更	[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、「デバイス構成の比較」（227 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
診断	[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。 • すべて：1 つのページにすべての診断を表示します。 • 基本 IP：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。 • メモリトラブルシューティング：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。 • デバイス情報：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。 • NA がデバイスのブートを検出：デバイスを最後にブートしたときの情報を表示します。 • NA デバイスファイルシステム：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。

メニューオプション	説明 / アクション
診断（*続き*）	• NA 通信モードデータ収集：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。 • NA フラッシュ記憶域容量：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。 • NA インターフェイス：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。 • NA モジュールのステータス：このデバイスのモジュール診断を表示します。 • NA OSPF ネイバー：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。 • NA ルーティングテーブル：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。 • HPNA トポロジーデータ収集：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。 • NA VLAN データの収集：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。（**注意**：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）。 • NA ポートスキャン：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。
デバイスタスク	[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、「[デバイスタスク] ページのフィールド」（293 ページ）を参照してください。

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、「[デバイスイベント] ページのフィールド」（262 ページ）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、「[デバイス関係] ページのフィールド」（295 ページ）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、「[デバイスソフトウェア履歴] ページのフィールド」（297 ページ）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。[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、「[デバイスセッション] ページのフィールド」（299 ページ）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、「[診断の実行] タスクページのフィールド」（393 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、「[デバイス構成] ページのフィールド」（220 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、「[診断の実行] タスクページのフィールド」（393 ページ）を参照してください。

フィールド	説明 / アクション
アクション	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。 • 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。「[インターフェイスの詳細を編集] ページのフィールド」（267 ページ）を参照してください。 • 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。「[インターフェイスの詳細] ページのフィールド」（265 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。 • 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。「[サブネット内のインターフェイス] ページのフィールド」（269 ページ）を参照してください。

[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トラバースできます。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」（263 ページ）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、「[VLAN 詳細] ページのフィールド」（279 ページ）を参照してください。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）」（274 ページ）を参照してください。 **注意**：トランクポートにネガティブ 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「ネガティブ 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 のネットワード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。

フィールド	説明 / アクション
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 のネットワード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。
VRF	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。 **注意**：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。
QoS	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。
ACL	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。
最終変更	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。
コメント	インターフェイスについてのコメントを表示します。
詳細を編集	[インターフェイスの詳細を編集] ページが開きます。「[インターフェイスの詳細を編集] ページのフィールド」（267 ページ）

[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、「仮想ローカルエリアネットワーク（VLAN）」（274 ページ）を参照してください。

フィールド	説明 / アクション
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 のネットワード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 のネットワード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。
VLAN トランク	特定のポートをトランクポート、物理ポート、ポートチャンネル（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、「[VLAN タスク] ページのフィールド」（448 ページ）を参照してください。 **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、[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。
ネイティブ VLAN ID	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。例えば、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。
メンバー VLAN	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。
VLAN ID を指定	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）。
コメント	インターフェイスについてのコメントを表示します。

[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。例えば、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	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。 • 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。 • 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。「[インターフェイスの詳細] ページのフィールド」（265 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。

[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	例えば、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。例えば、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。

フィールド	説明 / アクション
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。 • 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。 • 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。

[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	例えば、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、「NA/SA 統合」（250 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。例えば、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。

フィールド	説明 / アクション
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。 • 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。 • 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。 • 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。

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。

例えば企業環境では、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）」（274 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、「VLAN の作成と編集」（278 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。このフィールドはベンダー固有のフィールドです。
VLAN ID	VLAN ID 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デバイスの 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。

フィールド	説明 / アクション
アクション	VLAN ごとに、次のアクションを選択できます。 • 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、「[VLAN 詳細] ページのフィールド」（279 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。 • 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、「VLAN の作成と編集」（278 ページ）を参照してください。 • 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。

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ー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）」（274 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」（393 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。「デバイス詳細の表示」（245 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 の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。

フィールド	説明 / アクション
VLAN ポート	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、「[インターフェイスの詳細] ページのフィールド」（265 ページ）を参照してください。 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。 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。
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」（448 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、「デバイス詳細の表示」（245 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 ID 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。

フィールド	説明 / アクション
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。「[インターフェイスの詳細] ページのフィールド」（265 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、「[デバイスインターフェイス] ページのフィールド」（263 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、「VLAN の作成と編集」（278 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）」（274 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、「デバイス詳細の表示」（245 ページ）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。

フィールド	説明 / アクション
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、「[VTP ドメイン] ページ」（284 ページ）を参照してください。（**注意**：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。
VTP 動作モード	サーバ、クライアント、トランスペアレント、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、「[デバイス詳細] ページのフィールド」（246 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）」（274 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、「[VTP ドメイン] ページ」（284 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）」（274 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、「デバイス詳細の表示」（245 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、「デバイス詳細の表示」（245 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、トランスペアレント、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。 • VTP を表示：[VTP 詳細] ページが開きます。詳細については、「[VTP 詳細] ページのフィールド」（281 ページ）を参照してください。 • VLAN を表示：[デバイス VLAN] ページが開きます。詳細については、「[デバイス VLAN] ページのフィールド」（276 ページ）を参照してください。

[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。 • 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。 • 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。

[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」（506 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」（527 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、「[ルールの新規作成] ページのフィールド」（514 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、「[ルール例外の新規作成] ページのフィールド」（526 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。 • アクティブ • 非アクティブ • 合格 • 失敗

フィールド	説明 / アクション
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。 • 情報：一般的に対応を必要としないイベント。 • 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。 • 中：適時に対応を必要とするイベント（通常は 72 時間以内）。 • 高：緊急の対応を必要とするイベント（通常は 24 時間以内）。 • 重要：即時の対応を必要とするイベント。
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。 • 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、「[ポリシーを編集] ページのフィールド」（521 ページ）を参照してください。 • 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、「[ルールの新規作成] ページのフィールド」（514 ページ）を参照してください。

[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。例えば、FastEtherner1/0 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 User's 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」（336 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

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(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。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、デバイスの情報を表示できます。
デバイス IP	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、デバイスの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、「表示メニューオプション」（257 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、「編集メニューオプション」（300 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、「プロビジョニングメニューオプション」（310 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、「接続メニューオプション」（312 ページ）を参照してください。

フィールド	説明 / アクション
ソフトウェアイメージのダウンロード	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。 • 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。 • 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。 • 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、「[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」（409 ページ）を参照してください。
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、「[ユーザインターフェイス] ページのフィールド」（78 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。 • 成功：タスクは成功しました。 • 失敗：タスクは失敗しました。 • 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。 • 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。 • 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。
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、「タスクの予定」（355 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。

フィールド	説明 / アクション
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。 • 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。 • 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なときのみ表示されます。

[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、デバイス関係 API によって定義されます。例えば、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」（444 ページ）を参照してください。Device Relationship API の詳細については、*『NA 9.0 API Reference Guide(NA 7.60 API リファレンスガイド)』* 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。例えば、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」（246 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」（133 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」（444 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。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、デバイスの情報を表示できます。
デバイス IP	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、デバイスの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、「表示メニューオプション」（257 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、「編集メニューオプション」（300 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、「プロビジョニングメニューオプション」（310 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、「接続メニューオプション」（312 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。

フィールド	説明 / アクション
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、「新規ソフトウェアレベルの追加」（533 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	各セッションに対して次のアクションを選択できます。 • 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。 • 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。

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、「[スナップショットの取得] タスクページのフィールド」（399 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、「[ドライバの検出] タスクページのフィールド」（371 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、「[構成を配布] タスクページのフィールド」（230 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、「[デバイスの編集] ページのフィールド」（142 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
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、「[デバイス管理対象 IP アドレス] ページのフィールド」(303 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。
新規デバイスとして保存	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。 • グループ • ドライバ • パスワード情報 • 接続情報 • モデル • ベンダー 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」(134 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
新規テンプレートとして保存	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。 • 構成ファイル • ドライバ • 接続情報 • モデル • ベンダー • 階層レイヤ 詳細については、「[デバイステンプレート] ページのフィールド」（151 ページ）を参照してください。
メッセージの新規作成	[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、「イベントの連結ビュー（シングルビュー）」（674 ページ）を参照してください。
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できます。HP Operations Orchestration ユーザ認証の詳細については、「ユーザ認証」（95 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。

[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	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、「[IP アドレスの新規作成] ページ（要塞ホスト）」（305 ページ）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。 • 要塞ホストの編集 • 要塞ホストの削除
IP アドレスの新規作成	[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、「[IP アドレスの新規作成] ページ（カスタム IP アドレス）」（306 ページ）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。
コンソールサーバの新規作成	[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、「[IP アドレスの新規作成] ページ（コンソールサーバ）」（307 ページ）を参照してください。
ホップボックスの新規作成	[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、「[IP アドレスの新規作成] ページ（ホップボックス）」（308 ページ）を参照してください。
新規接続スルー	[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、「[IP アドレスの新規作成] ページ（新規接続スルー）」（309 ページ）を参照してください。

フィールド	説明 / アクション
最後に使用した IP のリセット	最後に使用した IP アドレスをリセットできます。
ポート IP	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。）
デバイスへのアクセスに使用	[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]）。
タイプ	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。
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	各デバイスに対して次のアクションを選択できます。 • 編集：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、変更に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、「[デバイスの編集] ページのフィールド」（142 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。「[IP アドレスの新規作成] ページ（カスタム IP アドレス）」（306 ページ）を参照してください。 • 上へ移動：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。） • 下へ移動：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。）

[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、`(\x23|\x24|%)` です。これは、'#'、'$'、または '%' に変換されます。 （**注意**：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。 • [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。 • [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。 • [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。
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。 • [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。 • [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。 • [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。
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、`(\x23|\x24|%)` です。これは、'#'、'$'、または '%' に変換されます。 （**注意**：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」（444 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	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。 • [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。 • [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。 • [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。
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、「[デバイステンプレート] ページのフィールド」（151 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。「[ポリシー準拠の確認] タスクページのフィールド」（458 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。「[Syslog の構成] タスクページのフィールド」（362 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。「ACL の削除」（881 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。「[パスワードの配布] タスクページのフィールド」（366 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。「[デバイスのリブート] タスクページのフィールド」（375 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 台または複数のデイバスに対する ping、または traceroute テストをスケジューリングできます。「[ICMP テストの実行] タスクページのフィールド」（379 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。「[コマンドスクリプトの実行] 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。
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。「[診断の実行] タスクページのフィールド」（393 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。「[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」（404 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
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。「[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」（409 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、「[VLAN タスク] ページのフィールド」（448 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、「[OS 分析] タスクページのフィールド」（432 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、「[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」（444 ページ）を参照してください。
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、「[ポストスキャン] ページのフィールド」（436 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。

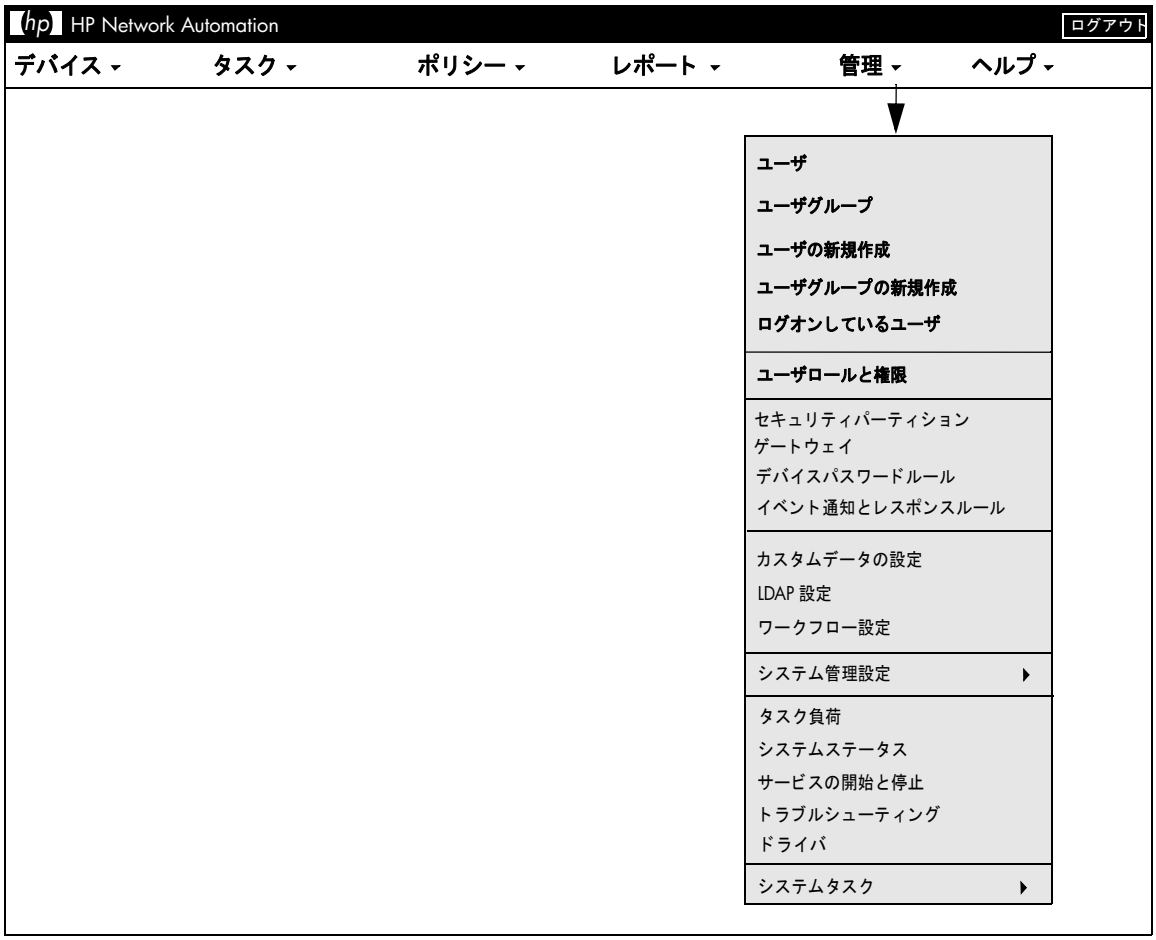
メニューオプション	説明 / アクション
Telnet を使用するプロキシ経由	[Telnet] ウィンドウが開きます。そのウィンドウで、デバイスに対して Telnet コマンドを入力できます。
SSH を使用するプロキシ経由	[SSH] ウィンドウが開きます。そのウィンドウで、デバイスに対して SSH コマンドを入力できます。

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	「ユーザの追加」（315 ページ）
ユーザパスワードの構成	「ユーザパスワードの構成」（321 ページ）
ユーザグループの追加	「ユーザグループの追加」（325 ページ）
新規ユーザロールの追加	「ユーザロールの追加」（330 ページ）
ユーザ設定の編集	「ユーザ設定の編集」（333 ページ）
クイック起動	「クイック起動とは」（340 ページ）
NA ホームページのカスタマイズ	「NA ホームページのカスタマイズ」（344 ページ）
検索 / 接続機能	「検索 / 接続機能」（349 ページ）

ユーザ管理へのナビゲート



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。

- ロール：同一のセキュリティ権限を共有するグループに、ユーザを分類することです。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。例えば、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。ページの上部にある [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」（318 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。

[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、「[ユーザの新規作成] ページのフィールド」（318 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、「ユーザの検索」（643 ページ）を参照してください。
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）。
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、「[ユーザグループ] ページのフィールド」（325 ページ）を参照してください。
[ユーザロールと権限] リンク	[ユーザロールと権限] 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、「[ユーザロールと権限] ページのフィールド」（330 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。 •  通常のユーザアカウント •  無効のユーザアカウント
ユーザ名	NA ユーザ名を表示します。
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。

フィールド	説明
アクション	次のオプションを選択できます。 • 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、[自分のプロファイル] ページが開きます。[自分のプロファイル] 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、「[自分のプロファイル] ページのフィールド」（334 ページ）を参照してください。[ユーザリスト] ページには、自分のプロファイルへの変更内容が表示されます。 • 削除：ユーザを削除できます（システム管理権限を使用）。 • 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 [ユーザプロファイルの編集] をクリックすると、[ユーザの編集] ページが開きます。ユーザプロファイルに変更を加え、[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、「[ユーザの新規作成] ページのフィールド」（318 ページ）を参照してください。 • 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、「デバイス構成変更の表示」（219 ページ）を参照してください。

[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
ユーザ情報	
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。（**注意**：ユーザ名にはスペースを入れないでください。変数名には、英字、数字、アンダースコア、ハイフン、およびバックスラッシュのみを使用できます。）
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、「ユーザパスワードの構成」（321 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	次のオプションから、1 つ以上選択します。 • 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 パスワードオプションの設定の詳細については、「ユーザパスワードの構成」（321 ページ）を参照してください。
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	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）。 • 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。 • 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。 • 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。 • 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。 • 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は、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。
デフォルト	次のオプションのいずれかを選択します。 • 有効：アカウントは有効です（デフォルト）。 • 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。

フィールド	説明 / アクション
外部認証フェイルオーバー	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。
コメント	アカウントについてのコメントを入力します。
パーティション	このユーザが属するパーティションを選択します。このユーザは、当該パーティションへの表示権限を持つ他のユーザからのみ見えます。（**注意**：ユーザが 1 つのパーティションにのみアクセスできる場合、[パーティション] ドロップダウンメニューは表示されません。）
AAA	
AAA ユーザ名	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しません。
AAA パスワード	ユーザの 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 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、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」（787 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」（334 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 ユーザがいない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。「アカウントはロックアウトされています。」

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」(339 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」（326 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。

[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、「[ユーザグループの新規作成] ページのフィールド」（326 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、「[全ユーザ] ページのフィールド」（316 ページ）を参照してください。
[ユーザロールと権限] リンク	[ユーザロールと権限] 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、「[ユーザロールと権限] ページのフィールド」（330 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ァイルの編集についての詳細については、「[全ユーザ] ページのフィールド」（316 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、「ユーザロールの追加」（330 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。 • 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、「[ユーザグループ] ページのフィールド」（325 ページ）を参照してください。 • 削除：グループを削除できます（管理（Admin）権限を使用）。 • 権限：[表示権限] 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」（326 ページ）を参照してください。

[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
一般情報	
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。
パーティション	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。パーティションの詳細は、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。（**注意**：ユーザが 1 つのパーティションにのみアクセスできる場合、[パーティション] ドロップダウンメニューは表示されません。）
コマンド権限	

フィールド	説明 / アクション
既存のコマンド権限ロール	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）、次のオプションを 1 つ以上選択します。 • 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。 • パワー：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。 • フルアクセス：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。 • 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。 **注意**：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。

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	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、「付録 B：コマンド権限」（911 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。 • 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。 • 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。 **注意**：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。
デバイスの修正権限	
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。 **注意**：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。
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。

フィールド	説明 / アクション
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。
スクリプト権限	
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。
パーティションの表示権限	
全オブジェクト	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。（詳細は、「デバイスとユーザのセグメント化」（188 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。
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められます。
ユーザ	
グループのユーザ / 全ユーザ	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、[<< 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。

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。例えば、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リプ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] の下のメニューバーで、[ユーザロールと権限] 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」（332 ページ）を参照してください。

[ユーザロールと権限] 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、「[ユーザロールの新規作成] ページのフィールド」（332 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、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、「[全ユーザ] ページのフィールド」（316 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、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、「[ユーザグループ] ページのフィールド」（325 ページ）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。

フィールド	説明 / アクション
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。 • 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、「ユーザロールの追加」（330 ページ）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。 • 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」（332 ページ）を参照してください。 • 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。
ユーザ定義ロール	
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	例えば、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。 • 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」（332 ページ）を参照してください。 • 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」（332 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。 • 削除：ロールを削除できます（システム管理権限のみ）。

[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	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。 • コマンド権限：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、「付録 B：コマンド権限」（911 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。 • デバイスの修正権限：ユーザロールの名前と説明を入力します。デバイスセレクタを使用してデバイスグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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。 • スクリプト権限：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。 • パーティションの表示権限：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、「デバイスとユーザのセグメント化」（188 ページ）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。

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」（326 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」（340 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」（333 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。

- 自分のプロファイル：「[自分のプロファイル] 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」（336 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」（336 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」（338 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」（339 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」（340 ページ）を参照してください。

[自分のプロファイル] ページのフィールド

[自分のプロファイル] 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」（321 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 [自分のプロファイル] をクリックします。[自分のプロファイル] 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。
パスワードオプション	次のオプションから、1 つ以上選択します。 • 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 パスワードオプションの設定の詳細については、「ユーザパスワードの構成」（321 ページ）を参照してください。
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。「[パスワードの変更] ページのフィールド」（339 ページ）を参照してください。
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。

フィールド	説明 / アクション
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。
AAA	
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。
SecurID	
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、「SecurID ソフトウェアトークンの追加」（787 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」(289 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。

フィールド	説明 / アクション
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。
ソフトウェアイメージ推奨設定	
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」（332 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、「ユーザロールの追加」（330 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、「コマンド権限の付与」（911 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、「デバイスとユーザのセグメント化」（188 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
ローカル認証パスワード	
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。
外部リソース認証 / 新規外部リソース資格情報の追加	
資格情報タイプ	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。 • 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、「[Cisco.com からイメージをダウンロード] タスクページ」（452 ページ）を参照してください。 • 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。
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、「[サーバ] ページのフィールド」（66 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。

NA9.0 では、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。例えば、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。

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」（617 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に注意してください。

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」（357 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」（342 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。例えば、[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] の下の [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。`successfully saved task`（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。

例えば、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」（340 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、「タスクテンプレート」（357 ページ）を参照してください。
クイック起動のアクション：デバイス	
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。
クイック起動のアクション：ポリシー	
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。

フィールド	説明 / アクション
	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。
クイック起動のアクション：レポート	
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。
クイック起動設定	
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、「ユーザ設定の編集」（333 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、それらを 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」（349 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」（333 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」（345 ページ）および 「[統計ダッシュボード] タブのフィールド」（348 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
ワークフロー承認（該当する場合）	
自分の承認を待機しているタスク	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。 • タスク名：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、「[タスク情報] ページのフィールド」（860 ページ）を参照してください。 • 承認期限：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、「承認の要求」（857 ページ）を参照してください。 • 承認：承認のステータスを表示します。 • スケジュール日時：タスクが予定された日付を表示します。 • ステータス：現在のステータスを表示します。 [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、「承認の要求」（857 ページ）を参照してください。
自分のタスク	
タスク名	タスクのリストを表示します。詳細については、「タスクとは」（354 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、「[タスク情報] ページのフィールド」（499 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、「タスクとは」（354 ページ）を参照してください。
最近の変更	

フィールド	説明 / アクション
期間	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。 • 過去 1、2、4、8、12、24、および 48 時間 • 過去 1 および 2 週間 • 過去 1ヶ月 • 全構成
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。
アクション	次のアクションを選択できます。 • 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ハイライト表示されます。 • 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。
すべて表示	[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、「デバイス構成変更の表示」（219 ページ）を参照してください。

最近のイベント

フィールド	説明 / アクション
期間	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。 • 過去 1、2、4、8、12、24、および 48 時間 • 過去 1 および 2 週間 • 過去 1ヶ月 • 全構成
イベントサマリ	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、「イベントの連結ビュー（シングルビュー）」（674 ページ）を参照してください。
カウント	このタイプのイベント数を表示します。
イベントリストページ	[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、「イベントの連結ビュー（シングルビュー）」（674 ページ）を参照してください。
自分のデバイスグループ（該当する場合）	
デバイスグループ	[デバイスグループ] ページが開きます。このページで、現在のデバイスグループを表示できます。
お気に入りレポート（該当する場合）	
全お気に入りレポート	[ユーザ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。

[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」（776 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」（579 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	「タスクとは」（354 ページ）
タスクの予定	「タスクの予定」（355 ページ）
タスクテンプレート	「タスクテンプレート」（357 ページ）
Syslog の構成タスク	「[Syslog の構成] タスクページのフィールド」（362 ページ）
パスワードの配布タスク	「[パスワードの配布] タスクページのフィールド」（366 ページ）
ドライバの検出タスク	「[ドライバの検出] タスクページのフィールド」（371 ページ）
デバイスのリブートタスク	「[デバイスのリブート] タスクページのフィールド」（375 ページ）
ICMP テストの実行タスク	「[ICMP テストの実行] タスクページのフィールド」（379 ページ）
コマンドスクリプトの実行タスク	「[コマンドスクリプトの実行] タスクページのフィールド」（385 ページ）
診断の実行タスク	「[診断の実行] タスクページのフィールド」（393 ページ）
スナップショットの取得タスク	「[スナップショットの取得] タスクページのフィールド」（399 ページ）
スタートアップとランニングの同期タスク	「[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」（404 ページ）
デバイスソフトウェアの更新タスク	「[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」（409 ページ）
インポートタスク	「[インポート] ページのフィールド」（417 ページ）
ネットワークデバイスの検出タスク	「[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」（422 ページ）
通信モードデータの削除タスク	「[重複の削除] タスクページのフィールド」（429 ページ）
OS 分析	「[OS 分析] タスクページのフィールド」（432 ページ）
ポートスキャン	「[ポストスキャン] ページのフィールド」（436 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」（440 ページ）
デバイスコンテキストを追加	「[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」（444 ページ）

トピック	参照先：
VLAN	「[VLAN タスク] ページのフィールド」（448 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」（452 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」（455 ページ）
ポリシー準拠の確認タスク	「[ポリシー準拠の確認] タスクページのフィールド」（458 ページ）
サマリレポートの生成タスク	「[サマリレポートの生成] タスクページのフィールド」（462 ページ）
電子メールレポートタスク	「[電子メールレポート] タスクページのフィールド」（465 ページ）
リモートエージェントを配布タスク	「[リモートエージェントの配布] タスクページのフィールド」（468 ページ）
FQDN の解決タスク	「[FQDN の解決] タスクページのフィールド」（471 ページ）
データの整理タスク	「[データの整理] タスクページのフィールド」（474 ページ）
外部アプリケーションの実行タスク	「[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」（477 ページ）
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の予定」（481 ページ）
[自分のタスク] の表示	「[自分のタスク] ページのフィールド」（487 ページ）
予定されたタスクの表示	「予定タスクの表示」（491 ページ）
実行中のタスクの表示	「実行中のタスクの表示」（494 ページ）
最近のタスクの表示	「最近のタスクの表示」（496 ページ）
タスク負荷の表示	「タスク負荷の表示」（502 ページ）

[タスク] ページへのナビゲート

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、スケジューリングしたりすぐに実行したりできます。[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」（237 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。例えば、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」（385 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」（483 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、管理者権限が持つか、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」（332 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、『*HP 9.0 Network Automation API Reference Guide(HP 7.60 Network Automation API リファレンスガイド)*』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、『*HP Network Automation 9.0 Multimaster Distributed System on Oracle User's Guide(Oracle 対応の HP Network Automation 7.60 マルチマスタ分散システムユーザガイド)*』、または『*HP Network Automation Multimaster Distributed System on SQL Server User's Guide(SQL Server 対応 HP Network Automation マルチマスタ分散システムユーザガイド)*』を参照してください。（マルチマスタ分散システムのドキュメントは、分散システム DVD および HP セルフソルブ manuals サイトで参照できます）。
- **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」（66 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。例えば、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」（360 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」（491 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」（496 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」（481 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」（617 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、「[自分のタスク] ページのフィールド」（487 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、「[自分のタスク] ページのフィールド」（487 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、「承認の要求」（857 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、「[予定タスク] ページのフィールド」（491 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、「[実行中のタスク] ページのフィールド」（494 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、「[最近のタスク] ページのフィールド」（496 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。
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、「タスクの予定」（355 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、「デバイスとユーザのセグメント化」（188 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。

フィールド	説明 / アクション
アクション	次のアクションを選択できます。 • 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。 • 編集：選択したタスクの [タスクを編集] ページが開きます。例えば、[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。（**注意**：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。） • 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。（**注意**：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。 • 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。 • 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、「クイック起動とは」（340 ページ）を参照してください。
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」（362 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」（366 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」（371 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」（375 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」（379 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」（385 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」（393 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」（399 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」（404 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」（409 ページ）
インポート	「[インポート] ページのフィールド」（417 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」（422 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」（429 ページ）
OS 分析	「[OS 分析] タスクページのフィールド」（432 ページ）
ポートスキャン	「[ポストスキャン] ページのフィールド」（436 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」（440 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」（444 ページ）
VLAN	「[VLAN タスク] ページのフィールド」（448 ページ）

タスク	参照先
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」（452 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」（440 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」（452 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」（455 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」（458 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」（462 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」（465 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の配布] タスクページのフィールド」（468 ページ）
FQDN の解決	「[FQDN の解決] タスクページのフィールド」（471 ページ）
データの整理	「[データの整理] タスクページのフィールド」（474 ページ）
外部アプリケーションの実行	「[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」（477 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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、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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：（[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。

フィールド	説明 / アクション
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
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。（**注意**：ログ記録の詳細については、「ログ記録」（122 ページ）を参照してください。）
Syslog の設定	次のオプションのいずれかを選択します。 • 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）。 • 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。
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」（54 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。 • 標準の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を使用（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。）
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、値は考慮されません。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	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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	タスクは、上で指定した日付 / 時刻に開始し、次の条件に従って繰り返します。次のオプションのいずれかを選択します。 • 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）。 • 定期的 : 繰り返し間隔を分単位で指定します。 • 日次 : タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了 : 繰り返しの回数を入力します。 • 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。
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、「ログ記録」（122 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」（499 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」（487 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： 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」（310 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、Device Release Service（DRS）ドキュメントを参照してください。DRS は、新しく自動化されたドライバのリリースと配信システムです。

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」（219 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 を再設定する必要もあります。

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」（167 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：([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。
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	

フィールド	説明 / アクション
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。(**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」(122 ページ) を参照してください。)
制限付きアクセスのユーザ名	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。)
制限付きアクセスパスワード	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。)
パスワードの確認	確認用にパスワードを再入力します。
フルアクセスのユーザ名	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。)
フルアクセスのパスワード	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。)
パスワードの確認	確認用にパスワードを再入力します。
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を追加するには、右側のボックスに文字列を入力して、<<[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。

フィールド	説明 / アクション
SNMP 書き込みコミュニティ文字列	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、<<[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。
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」（54 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。）

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。

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。
スケジューリングオプション	
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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
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、「ログ記録」（122 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」（499 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」（487 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：([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。
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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
タスクオプション	
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。(**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」(122 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。
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」(54 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。)
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。	

フィールド	説明 / アクション
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	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。

フィールド	説明 / アクション
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。
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、「ログ記録」（122 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」（499 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」（487 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：([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。
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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
タスクオプション	
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、「ログ記録」（122 ページ）を参照してください。
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」（54 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。）
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。	

フィールド	説明 / アクション
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	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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。
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、「ログ記録」（122 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」（499 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」（487 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。例えば 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：([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。
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	

フィールド	説明 / アクション
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。（**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」（122 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。

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」（54 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。）

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。

フィールド	説明 / アクション
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	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。

フィールド	説明 / アクション
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。
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、「ログ記録」（122 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」（487 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。スクリプトの書き込みの詳細については、「[コマンドスクリプトの新規作成] ページのフィールド」（716 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、「[コマンドスクリプト] ページのフィールド」（711 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：([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。
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。

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、「タスクの予定」（355 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。
タスクオプション	
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、「ログ記録」（122 ページ）を参照してください。

フィールド	説明 / アクション
実行するコマンドスクリプト	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。 • Cisco IOS Initial Setup • Cisco IOS による ACL ID に基づいた ACL への行の挿入 • Cisco IOS によるハンドルに基づいた ACL への行の挿入 • Cisco IOS による ACL ID に基づいた ACL からの行の削除 • Cisco IOS によるハンドルに基づいた ACL からの行の削除 • フラッシュの圧縮 • Contivity 1100 SNMP コミュニティ文字列の配布 • 拡張 Ping • 全二重通信 • ios_7k_reboot • ios_generic_reboot • ios_l3switch_reboot • Passport 8xxx - コミュニティ文字列の配布 • Passport 8xxx-SNMP-v3 コミュニティ文字列の配布 • Passport 8xxx - ユーザパスワードの配布 • Passport 8xxx-Radius の有効化 • Passport 8xxx-Web サーバの有効化 • サンプル - FastEther インターフェイスのプロビジョニング • バナー設定 • 必要なときのみバナー設定 • 場所設定 • NTP サーバ設定 • ディレクティッドブロードキャストを無効にする • インターフェイスの更新
プレビューオプション	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。

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。 • 高度な ACL スクリプト • ACL アプリケーションスクリプト • ACL 作成スクリプト • ACL 編集スクリプト
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。	
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、「[コマンドスクリプトの新規作成] ページのフィールド」（716 ページ）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。 **注意**：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。
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。

フィールド	説明 / アクション
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。

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」（54 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 （詳細は、「[構成管理] ページのフィールド」（41 ページ）を参照してください）。

タスク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。 • なし（デフォルト） • タスクの一部として

フィールド	説明 / アクション
タスク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。 • 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。
スケジューリングオプション	
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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	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。 • 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）。 • 定期的 : 繰り返し間隔を分単位で指定します。 • 日次 : タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了 : 反復回数を入力します。 • 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。
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、「ログ記録」（122 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」（499 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」（487 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] の下のメニューバーで[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、「[診断の新規作成] ページのフィールド」（680 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、「[診断] ページのフィールド」（678 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：（[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。

フィールド	説明 / アクション
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
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、「ログ記録」（122 ページ）を参照してください。

フィールド	説明 / アクション
実行する診断	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。 • ハードウェア情報 • メモリトラブルシューティング • NA がデバイスのブートを検出 • NA デバイスファイルシステム • NA 通信モードデータ収集 • NA フラッシュ記憶域容量 • 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 • NA トポロジーデータ収集 • NA VLAN データ収集 • NA ポートスキャン **注意**：診断の詳細については、「表示メニューオプション」（257 ページ）を参照してください。
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」（54 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 [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設定されている場合にのみ表示されます （詳細は、「[構成管理] ページのフィールド」（41 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。

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。
スケジューリングオプション	
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。
タスクログ	

フィールド	説明 / アクション
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、「ログ記録」（122 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」（499 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」（487 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：([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。

フィールド	説明 / アクション
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
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。（**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」（122 ページ）を参照してください。）
オプション	次のオプションのいずれかまたは両方を選択します。 • 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。 • 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。
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」（54 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。）

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

フィールド	説明 / アクション
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。
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、「ログ記録」（122 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」（499 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」（487 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：([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。
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。

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、「タスクの予定」（355 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。
タスクオプション	
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、「ログ記録」（122 ページ）を参照してください。
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」（54 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。）

フィールド	説明 / アクション

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 （詳細は、「[構成管理] ページのフィールド」（41 ページ）を参照してください）。

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。

スケジューリングオプション

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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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	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。 • 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）。 • 定期的 : 繰り返し間隔を分単位で指定します。 • 日次 : タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了 : 反復回数を入力します。 • 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。
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、「ログ記録」（122 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」（499 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」（487 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」（547 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。

フィールド	説明 / アクション
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 • 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。 **注意**：([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。
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
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、「ログ記録」（122 ページ）を参照してください。
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、「配布表」（414 ページ）を参照してください。

フィールド	説明 / アクション
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	次のオプションのいずれかを選択します。 • 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。 • 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。 • 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ブートすると、デバイスをブートできなくなる場合があります。）
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。
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] 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」（54 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。）
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	

フィールド	説明 / アクション
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。
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、「ログ記録」（122 ページ）を参照してください。

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。配布表には、ブートまたは OS イメージとして選択できる各ファイルシステム上のイメージが表示されます。複数のファイルシステムにイメージが存在する場合、最後にアップロードされたイメージがブート用イメージとなります。

デバイス上にない項目の [ブート] および [OS] ラジオボタンは、最初は無効です。デバイスにアップロードするイメージを選択すると、該当するイメージがブート、または OS イメージとして選択できるようになります。

ラジオボタンで、ブート、または OS イメージとして設定するイメージを選択できます。ただし、現在デバイス上にあるか、アップロード用に選択されているイメージのみを、ブート、または OS 用として選択できます。さらに、イメージはブート、または OS イメージのいずれかとしてのみ選択できますが、両方は選択できません。網掛け表示されている列のラジオボタンでは、ブート、および OS イメージすべてを選択、または選択解除できます。

注意： 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
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 （詳細は、「[診断の実行] タスク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。
名前	デバイスの名前が表示されます。
サイズ	ダウンロードするソフトウェアイメージのサイズを表示します。
ブート /OS	デバイス上にない項目の [ブート] および [OS] ラジオボタンは、最初は無効です。デバイスにアップロードするイメージを選択すると、該当するイメージがブートイメージ、または OS イメージとしてマークできるようになります。 **注意**：デバイスによっては OS イメージとは別にブートイメージを持っており、多くの場合、これを「キックスタート」イメージ（大規模なイメージと対照的なイメージ）として参照します。また、「Boot」コマンドを使用して、リブートで使用するイメージファイルを設定するデバイスもあります。イメージファイルのコピー後に実行する追加のコマンドが必要ない場合は、どちらのラジオボタンもオフにしてください。
準拠	「セキュリティリスク」、「実稼動前」、「廃止」などのソフトウェアイメージの準拠レベルを表示します。デフォルトではこのフィールドは表示されません。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」（78 ページ）を参照してください。
ファイルシステム名（Flash など）	ファイルシステムの合計未使用空き容量を表示します。
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。
チェックボックス	デバイス上に存在するファイルは強調表示されます。これらのファイルをデバイスに配布しない場合、このチェックボックスをオンにしてください。
追加	ファイル、イメージセット、およびソフトウェア配布の配布先を表示します。

フィールド	説明 / アクション
削除	ファイルが削除されることを表示します。
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。
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」（499 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」（487 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。

[インポート] ページのフィールド

インポートタスクでは、CSV（comma-separated value）フォーマットを使用して、デバイスやデバイスパスワードデータのインポートができます。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。1 つの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。

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	[インポート] 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。 • 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。 • 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、「タスクテンプレート」（357 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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。 **注意**：「Site」値は、コンマ区切り値（CSV）ファイルの「SiteName」値によって無効化されます。デバイスとパスワードを含む CSV ファイルの詳細については、「デバイスとパスワードのデータを含む CSV ファイルの作成」（164 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。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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
タスクオプション	
ファイルのインポート	インポートする CSV（Comma Separated Value）ファイルの名前を入力します。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。NA サーバのファイルへのフルパスを含めてください。テンプレートを使用して [データ型] フィールド（以下を参照）の新規 CSV ファイルを作成する場合、必ずローカルのハードドライブにファイルを保存してください。詳細については、「デバイスとパスワードのデータを含む CSV ファイルの作成」（164 ページ）を参照してください。
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。 • 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を登録するためのさまざまなフィールドがあります。例えば、IP アドレス、ホスト名、デバイスグループ名などです。 • 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、グループ名、パーティション名、親デバイスグループ名など、NA に入力されるデバイスグループに対応するさまざまなフィールドが含まれています。 • 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。 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、デバイス CSV テンプレートファイルまたはパスワード CSV テンプレートファイルへのリンクをクリックします。ファイルが開いたら、ローカルのハードドライブに別の名前で保存します。次に、デバイスデータやデバイスパスワードに適合するように保存したファイルを修正します。

フィールド	説明 / アクション
Syslog の設定	次のオプションのいずれかを選択します。 • NA syslog サーバでログを取得するようデバイスを設定する • 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 • syslog を構成しない 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。 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は、[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。
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。例えば、フィルタが Windows 用の PERL スクリプトの場合、「perl」を次のように指定する必要があります : `perl c:/filter.pl`
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。
デバイスのインポート元	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なときに役立ちます。
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。

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。

フィールド	説明 / アクション
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	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。

フィールド	説明 / アクション
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了 : 反復回数を入力します。 • 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。
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、「ログ記録」（122 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」（499 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」（487 ページ）を参照してください。

[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」(54 ページ)および「[サーバ] ページのフィールド」(66 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 デバイスドライバリファレンス*』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 スキャンに応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 スキャンに応答した 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。例えば、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。例えば、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。例えば、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。 • 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。 • 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、「タスクテンプレート」（357 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。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
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（例えば、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（例えば、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	次のスキャン方法から、1 つまたは両方を選択します。 • SNMP（デフォルト） • 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。ネットワークトポロジーによっては、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。） スキャン方法の詳細については、「スキャン方法」（423 ページ）を参照してください。
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は、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。
デバイスグループ名	次のオプションのいずれかを選択します。 • 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 <*nnn*>、*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。 • 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）。 **注意**：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。
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。

デバイス資格情報のオプション

フィールド	説明 / アクション
デバイス資格情報	次のオプションのいずれかを選択します。 • ネットワーク全体のパスワードルールの使用 • 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。
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	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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	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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。
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、「ログ記録」（122 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] ページでは、検出されたノードの詳細情報を表示します。詳細については、「[タスク情報] ページのフィールド」（499 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」（487 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。例えば、HP OpenView 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」（422 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：([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。

フィールド	説明 / アクション
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
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	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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	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。 • 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）。 • 定期的 : 繰り返し間隔を分単位で指定します。 • 日次 : タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了 : 反復回数を入力します。 • 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。
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、「ログ記録」（122 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」（499 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」（487 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」（289 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：([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。
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。

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、「タスクの予定」（355 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。
タスクオプション	
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。（**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」（122 ページ）を参照してください。）
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。
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	

フィールド	説明 / アクション
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。
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、「ログ記録」（122 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」（499 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」（487 ページ）を参照してください。

[ポストスキャン] 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」（246 ページ）を参照してください。

ポートスキャンタスク設定を行うには、「デバイスアクセス」（53 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」（54 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 9.0 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」（612 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。

フィールド	説明 / アクション
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：（[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。
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
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。（**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」（122 ページ）を参照してください。）
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
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	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。

フィールド	説明 / アクション
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了 : 反復回数を入力します。 • 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。
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、「ログ記録」（122 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」（499 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」（487 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」（151 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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、CVS 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、CVS 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、「[テンプレート構成を編集] ページ」（155 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。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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	
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。（**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」（122 ページ）を参照してください。）
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。
タスク前 / タスク後スナップショットオプション	
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 • 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 • 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。

フィールド	説明 / アクション
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	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。

フィールド	説明 / アクション
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了 : 反復回数を入力します。 • 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。
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、「ログ記録」（122 ページ）を参照してください。

[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 以前では、NA にはコンテキストを管理可能にするためにコンテキストに IP アドレスが必要でした。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）」（309 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」（295 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
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。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
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。（**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」（122 ページ）を参照してください。）

フィールド	説明 / アクション
変数	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。 • 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。 • 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。例えば、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。 • 構成ファイル名：例えば、「default.cfg」などの構成ファイル名を入力します。
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。

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

フィールド	説明 / アクション
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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	[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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。
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、「ログ記録」（122 ページ）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」（451 ページ）を参照してください。）

[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」（278 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
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、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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。

フィールド	説明 / アクション
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
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。（**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」（122 ページ）を参照してください。）
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。
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。

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。
スケジューリングオプション	
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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	[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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。
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、「ログ記録」（122 ページ）を参照してください。

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」（267 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」（448 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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。 • すぐに開始（デフォルト） • 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。
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	

フィールド	説明 / アクション
デバイス / グループリストを変更	[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、今後に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。 [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。以下のフィールドの詳細については、「[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」（289 ページ）を参照してください。 • 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。 • 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。 • 機能リスト：選択したデバイスの機能情報を表示します。
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、「[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」（549 ページ）を参照してください。
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。）セキュリティまたはビジネス上の理由からパーティションを作成した場合、パーティションに基づいてソフトウェアのイメージをパーティションできます。ソフトウェアのイメージがすべてのパーティションで利用可能な場合、そのソフトウェアのイメージには、構成に応じて「共有」（または「グローバル」）とラベルがつきます。
スケジューリングオプション	
再試行回数	使用不可
繰り返しオプション	使用不可
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、「ログ記録」（122 ページ）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」（770 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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。

フィールド	説明 / アクション
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
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。（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」（122 ページ）を参照してください。）
ベースイメージセット名	次のオプションから選択できます。 • ユーザ名：ベースイメージセット名を入力します。 • 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。
イメージストレージ	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。 • 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。 • イメージを一意の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。

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。
スケジューリングオプション	
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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	このタスクではこのオプションは利用できません。
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、「ログ記録」（122 ページ）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。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：([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。

フィールド	説明 / アクション
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
アクション	次のオプションの 1 つまたはすべてを選択します。 • 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。 • 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。 • 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。 • 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。
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。

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。
スケジューリングオプション	
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。
タスクログ	

フィールド	説明 / アクション
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、「ログ記録」（122 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」（499 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」（487 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。 • 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。 • 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、「タスクテンプレート」（357 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。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
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。

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。
スケジューリングオプション	
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。

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」（499 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」（487 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。 • 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。 • 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、「タスクテンプレート」（357 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。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
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。）レポートのリストについては、「各レポートへのナビゲート」（736 ページ）を参照してください。
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。

フィールド	説明 / アクション
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 • デフォルトの書式 • HTML メール • CSV ファイルの添付 • プレーンテキスト • HTML メール（リンクなし）
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。

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	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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	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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。
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、「ログ記録」（122 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」（499 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」（487 ページ）を参照してください。

[リモートエージェントの配布] 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の配布] 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」（195 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。 • 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。 • 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、「タスクテンプレート」（357 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。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
アクション	次のオプションのいずれかを選択します。 • 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。 • 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。

フィールド	説明 / アクション
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。 • 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。 • 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。
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。（**注意**：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。

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

フィールド	説明 / アクション
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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
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、「ログ記録」（122 ページ）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	次のオプションから、1 つ以上選択します。 • 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。
適用先	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。 **注意**：（[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。
開始日	次のオプションのいずれかを選択します。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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	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	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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	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。 • 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）。 • 定期的 : 繰り返し間隔を分単位で指定します。 • 日次 : タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了 : 反復回数を入力します。 • 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。
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、「ログ記録」（122 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」（499 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」（487 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。 • 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。 • 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、「タスクテンプレート」（357 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。 • すぐに開始（デフォルト） • 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。

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、「タスクの予定」（355 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。
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	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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	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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。
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、「ログ記録」（122 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」（499 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」（487 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。例えば、*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。例えば、*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。 • 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。 • 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、「タスクテンプレート」（357 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。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	

フィールド	説明 / アクション
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。例えば、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。
テキスト出力	次のオプションのいずれかを選択します。 • stdout の結果（デフォルト）：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。 • ファイル結果：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。

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

フィールド	説明 / アクション
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。
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、「ログ記録」（122 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」（499 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」（487 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。例えば、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、「[ユーザロールと権限] ページのフィールド」（330 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。例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 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。 • 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。 • 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、「タスクテンプレート」（357 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。 • すぐに開始（デフォルト） • 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。
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、「タスクの予定」（355 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。
タスクオプション	
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。例えば、[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。「[予定タスク] ページのフィールド」（491 ページ）を参照してください。
予約デバイス	デバイスセレクタを使用してデバイスを予約します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照するか、またはデバイスセレクタの右上にある疑問符（?）をクリックします。

フィールド	説明 / アクション
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。
承認オプション	
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	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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回
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

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、例えば「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」（172 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。例えば、[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」（366 ページ）を参照してください。
9. [タスクの保存] 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。[デバイスセレクタ] 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	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。 • 未承認 • 承認を待機中 • 実行待ち 詳細については、「承認の要求」（857 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、「[予定タスク] ページのフィールド」（491 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、「[実行中のタスク] ページのフィールド」（494 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、「[最近のタスク] ページのフィールド」（496 ページ）を参照してください。

フィールド	説明 / アクション
タスクの表示のチェックボックス	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。 • 承認済み • 未承認 • 承認を待機中 • 無効化 • ドラフト • 承認は不要
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。
スケジュール日時	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。タスクは、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。(**注意**：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。)
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、「タスクとは」(354 ページ) を参照してください。
承認のステータス	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。 • 承認を待機中 • 承認済み • 未承認 • 無効化 • 承認は不要

フィールド	説明 / アクション
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。 • 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。 • 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。 • 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。 • 失敗：タスクは失敗しました。 • 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。 • 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。 • 実行中：タスクは開始しましたが、まだ終了していません。 • スキップ：タスクはエラー（例えば、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。 • 成功：タスクは成功しました。 • 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。
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、「タスクの予定」（355 ページ）を参照してください。
タスクタイプ	次のようなタスクタイプを表示します。 • パスワードの配布 • 構成を配布 • ドライバの検出 • デバイスのリブート • スナップショットの取得 • スタートアップとランニングの同期 タスクの全リストは、「タスクとは」（354 ページ）を参照してください。（**注意**：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。）

フィールド	説明 / アクション
アクション	次のオプションのいずれかを選択します。 • 削除：タスクを削除できます。 • 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（**注意**：タスクを再開する場合は、[再開] を選択します）。 • 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。 • 編集：[タスクを編集] ページが開きます。
1 ページに表示する結果の件数	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。

予定タスクの表示

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、「[自分のタスク] ページのフィールド」（487 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、「タスクテンプレート」（357 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、「[自分のタスク] ページのフィールド」（487 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、「承認の要求」（857 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、「[実行中のタスク] ページのフィールド」（494 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、「[最近のタスク] ページのフィールド」（496 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。

フィールド	説明 / アクション
スケジュール日時	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。
タスクのステータス	次のようにタスクのステータスを表示します。 • 保留：タスクはキューにありますが、実行されていません。 • 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。 • 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。 タスクのステータスのリストについては、「[タスク情報] ページのフィールド」（499 ページ）を参照してください。
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、「タスクの予定」（355 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	[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。 • 削除：タスクが削除されます。 • 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（**注意**：タスクを再開する場合は、[再開] を選択します）。 • 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。 • 編集：[タスクを編集] 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。 • 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、「タスクテンプレート」（357 ページ）を参照してください。

フィールド	説明 / アクション
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。

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、「[自分のタスク] ページのフィールド」（487 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、「[自分のタスク] ページのフィールド」（487 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、「承認の要求」（857 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、「[予定タスク] ページのフィールド」（491 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、「[最近のタスク] ページのフィールド」（496 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、「[ユーザインターフェイス] ページのフィールド」（78 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。

フィールド	説明 / アクション
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（**注意**：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）。
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、「タスクの予定」（355 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	[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。 • 編集：[タスクを編集] ページが開き、タスクを編集できます。 • 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。 • キャンセル：タスクを削除できます。 • 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、「タスクの予定」（355 ページ）を参照してください。 • 優先度を下げる：タスク優先度レベルを下げることができます。

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、「[自分のタスク] ページのフィールド」（487 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、「タスクテンプレート」（357 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、「[自分のタスク] ページのフィールド」（487 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、「承認の要求」（857 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、「[予定タスク] ページのフィールド」（491 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、「[実行中のタスク] ページのフィールド」（494 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。

フィールド	説明 / アクション
フィルタの表示	[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。 • 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。 • 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。 • [子タスクを表示]：オンにすると、子タスクが表示されます。 • 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。 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。
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。
タスクのステータス	次のようにタスクのステータスを表示します。 • 成功：タスクは成功しました。 • 失敗：タスクは失敗しました。 • 重複：タスクが別のタスクと重複しました。 • 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。 タスクのステータスのリストについては、「[タスク情報] ページのフィールド」（499 ページ）を参照してください。
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、「タスクの予定」（355 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。

フィールド	説明 / アクション
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	[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。 • 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。 • 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。(**注意** : 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。) • 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、「タスクテンプレート」(357 ページ)を参照してください。
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。

[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。例えば、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。「タスクとは」（354 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。「タスクとは」（354 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。「[自分のタスク] の表示」（487 ページ）を参照してください。

フィールド	説明 / アクション
一般情報	
タスク名	タスク名を表示します。
タスクのステータス	次に示すタスクのステータスを表示します。 • ドラフト • 重複 • 失敗 • 休止 • 保留 • 要求（注意：要求とは、タスクが承認を待っていることを示します。「タスクの承認」（860 ページ）を参照してください）。 • 実行中 • スキップ • 成功 • 同期（**注意**：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。） • 待機中 • 警告 **注意**：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。
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、「タスクの予定」（355 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。

フィールド	説明 / アクション
スケジュール日時	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。
繰り返しタイプ	例えば、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。
承認情報	
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。
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。
追加情報	
結果の詳細	（デバイスタイプに応じて）自動的に実行された診断結果を表示します。例えば、次のような診断結果があります。 • 診断 'NA モジュールのステータス ' が完了しました • 診断 'NA ルーティングテーブル ' が完了しました • 診断 'NA インターフェイス ' が完了しました。 • 診断 'NA OSPF ネイバー ' が完了しました
タスク履歴	
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

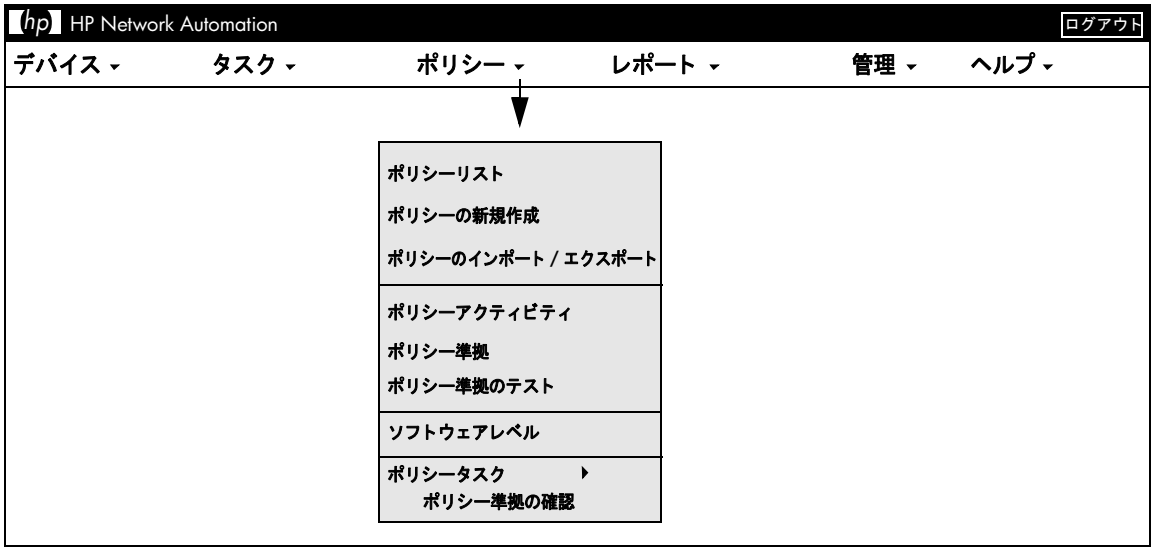
フィールド	説明
タスク開始（15 分後）	15 分以内に開始する予定のタスク数を表示します。
タスク待機中	待機中のタスク数を表示します。同時タスクの最大数に達している場合は、タスクは別のタスクが終了するまで待機します。
タスク実行中	実行中のタスク数を表示します。

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	「はじめに」（505 ページ）
ポリシーの作成	「ポリシーの作成」（507 ページ）
ポリシールールの作成	「[ルールの新規作成] ページのフィールド」（514 ページ）
ポリシーのインポート / エクスポート	「ポリシーのインポート / エクスポート」（520 ページ）
ポリシーの編集	「ポリシーを編集」（521 ページ）
適用されるポリシーの表示	「適用されるポリシーの表示」（527 ページ）
ポリシーアクティビティの表示	「ポリシーアクティビティの表示」（528 ページ）
ポリシー準拠の表示	「ポリシー準拠の表示」（530 ページ）
新規準拠の追加	「新規ソフトウェアレベルの追加」（533 ページ）
ポリシー準拠のテスト	「ポリシー準拠のテスト」（541 ページ）

ポリシー保証へのナビゲート



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」（257 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。例えば、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。

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。

例えば、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、「[ポリシーの新規作成] ページのフィールド」（510 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、「[ポリシー準拠の確認] タスクページのフィールド」（458 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、「ポリシーのインポート / エクスポート」（520 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	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。 • 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。 • 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。 • 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。 • 削除：選択したポリシーが削除されます。 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。
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。

フィールド	説明
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、「デバイスとユーザのセグメント化」（188 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。
アクション	次のアクションを選択できます。 • 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、「ポリシーを編集」（521 ページ）を参照してください。 • 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 詳細は、「[ポリシーをテスト] ページのフィールド」（542 ページ）を参照してください。）

[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
ポリシーの新規作成	
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。パーティションの作成の詳細については、「デバイスとユーザのセグメント化」(188 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。 • 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。 • 既存：ドロップダウンメニューからタグを選択します。 • 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。
範囲	次のオプションのいずれかを選択します。 • デバイスグループポリシーの適用先を選択：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」(180 ページ) を参照してください。 • 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、ポリシーと共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、「動的デバイスグループ」(177 ページ) を参照してください。)

フィールド	説明 / アクション

検索条件（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。

条件の追加	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。 • 構成テキスト • デバイス IP • デバイスステータス • ホスト名 • パスワードルール
ブール式	
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。例えば、3 つの検索条件が定義されている場合、式は *A and B and C* 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。（**注意**：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。）
デバイスグループで検索を絞り込み	
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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：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。

ビューとパーティションで検索を絞り込み（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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。）

フィールド	説明 / アクション
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、「[ルールの新規作成] ページのフィールド」（514 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	次のオプションから 1 つをクリックします。 • アクティブ：ポリシーをアクティブにします（デフォルト）。 • 非アクティブ：ポリシーを非アクティブにします。
追加ポリシーフィールド（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、www.cve.mitre.org. 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。
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次の形式で入力します。*yyyy-MM-dd*

フィールド	説明 / アクション
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。例えば、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
ルールの新規作成	
ルール名	ルール名を入力します。
ルールタイプ	ルールタイプを選択します。例えば、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プ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。 • 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。 • 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、「[診断の実行] タスクページのフィールド」（393 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。 • 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、「ソフトウェアレベルレポートのフィールド」（766 ページ）を参照してください。

フィールド	説明 / アクション
ルールの説明	ルールの説明を入力します。
以下のドライバを持つデバイスに適用されます	
全デバイスファミリ	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。 **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。
デバイスファミリ	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。例えば、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。 • 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。 • 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。
テキストブロックを定義	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。例えば、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（例えば、「*interface .**」）とブロック終了パターン（例えば、「*!*」）を入力します。

フィールド	説明 / アクション

テキストブロックを定義（*続き*）	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。例えば、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。
	
	ブロック開始： `interface .*`
	ブロック修了： `!`
	
	構成テキストには以下の行が含まれます。
	
	`...`
	`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`
	`...`
	
	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。
	
	`interface FastEthernet0/7`
	`description testfor bug 145762`
	`speed 100`
	`duplex full`
	`!`
	
	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。

フィールド	説明 / アクション
ルール条件	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。 • 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。 • 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。 • 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。 • 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。 • 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。 「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。例えば、「A」～「B」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。 *「if (A and B) then (C or D) else E」*。（**注意**：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。） [ヘルプの取得] リンクで、正規表現に関する情報が得られます。[デバイス変数] 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使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。 [式のリセット] 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。

フィールド	説明 / アクション
重要度	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。例えば、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。 • 情報：一般的に対応を必要としないイベント。 • 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。 • 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）。 • 高：緊急の対応を必要とするイベント（通常は 24 時間以内）。 • 重要：即時の対応を必要とするイベント。
詳細な説明	ルールの説明を入力します。
ルール例外	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。例えば、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。 [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。（詳細は、「ルール例外の追加」（525 ページ）を参照してください）。

フィールド	説明 / アクション
自動修正スクリプト	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。 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、「自動修正スクリプトの作成」（720 ページ）を参照してください）。 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。 • 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。 • 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。

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。

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 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、「デバイスとユーザのセグメント化」（188 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。 • 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。 • 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。 • 新規作成：ポリシーの場所を入力します。

フィールド	説明 / アクション
範囲	次のオプションのいずれかを選択します。 • 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。 • 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、ポリシーと共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、「動的デバイスグループ」（177 ページ）を参照してください。）

検索条件（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。

条件の追加	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。 • 構成テキスト • デバイス IP • デバイスステータス • パスワードルール • ホスト名
ブール式	
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。例えば、3 つの検索条件が定義されている場合、式は *A and B and C* 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。 （**注意**：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。）

デバイスグループで検索を絞り込み

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	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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：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。

ビューとパーティションで検索を絞り込み（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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。）

例外とするデバイス	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 <<] 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。
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、「[ルールの新規作成] ページのフィールド」（514 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表示します。
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。 • アクティブ：ポリシーをアクティブにします（デフォルト）。 • 非アクティブ：ポリシーを非アクティブにします。

追加ポリシーフィールド （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。）

フィールド	説明 / アクション
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、www.cve.mitre.org. 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次の形式で入力します。*yyyy-MM-dd*
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（**注意**：[ヘルプの取得] 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」（507 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」（530 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」（286 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、「ポリシーを編集」（521 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。

フィールド	説明 / アクション
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。 • 情報：一般的に対応を必要としないイベント。 • 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。 • 中：適時に応答を必要とするイベント（通常は 72 時間以内）。 • 高：緊急の対応を必要とするイベント（通常は 24 時間以内）。 • 重要：即時の対応を必要とするイベント。

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、「[ポリシー準拠の確認] タスクページのフィールド」（458 ページ）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	• 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。 • 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、「[ポリシーアクティビティ] ページのフィールド」（528 ページ）を参照してください。 • 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。
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。

フィールド	説明 / アクション
アクション	次のオプションを選択できます。 • 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、「[ポリシーアクティビティ] ページのフィールド」（528 ページ）を参照してください。 • 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、「[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」（532 ページ）を参照してください。

[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。 • 高重要度（赤） • 中重要度（アンバー） • 低重要度（緑）
アクション	次のオプションを選択できます。 • 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。 • 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。「ポリシーを編集」（521 ページ）を参照してください。 • 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。「ルール例外の追加」（525 ページ）を参照してください。

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」、「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」（536 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
ソフトウェアレベルを追加	
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。 • 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）。 • 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。

フィールド	説明 / アクション
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。 • セキュリティリスク • 実稼動前 • 廃止 • ブロンズ • シルバー • ゴールド • プラチナ
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。
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。
一致基準（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。
ソフトウェアの脆弱性情報（セキュリティリスクレベル）	
開示日	ソフトウェアの脆弱性が警告された日付を次の形式で入力します。*yyyy-MM-dd*

フィールド	説明 / アクション
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。 • 情報 • 低 • 中 • 高 • 重要
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、www.cve.mitre.org. 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」（198 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。「[ソフトウェアレベルを追加] ページのフィールド」（533 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。「デバイスソフトウェアレポートのフィールド」（764 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。「ソフトウェアレベルレポートのフィールド」（766 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	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。 • 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。 • 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。 • 削除：ソフトウェアレベル定義を削除します。 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。
名前	準拠名を表示します。

フィールド	説明 / アクション
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。例えば、「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。
ソフトウェアレベル	準拠評価名を表示します。評価には次の項目があります。 • セキュリティリスク • 実稼動前 • 廃止 • ブロンズ • シルバー • ゴールド • プラチナ
重要度	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の重要度を示します。 • 情報：一般的に対応を必要としないイベント。 • 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。 • 中：適時に応答を必要とするイベント（通常は 72 時間以内）。 • 高：緊急の対応を必要とするイベント（通常は 24 時間以内）。 • 重要：即時の対応を必要とするイベント。
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	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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。

フィールド	説明 / アクション
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。
コメント	準拠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。 • 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。 • 削除：準拠を削除できます。

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
準拠の編集	
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。 • 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）。 • 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。
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。 • セキュリティリスク • 実稼動前 • 廃止 • ブロンズ • シルバー • ゴールド • プラチナ
説明	準拠の説明を表示します。
一致基準	
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。

フィールド	説明 / アクション
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。
ソフトウェアの脆弱性情報（セキュリティリスクレベル）	
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。
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。 • 情報 • 低 • 中 • 高 • 重要
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、www.cve.mitre.org. 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、「[ポリシー] ページのフィールド」（508 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。 • 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。 • 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。 • 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。
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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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。

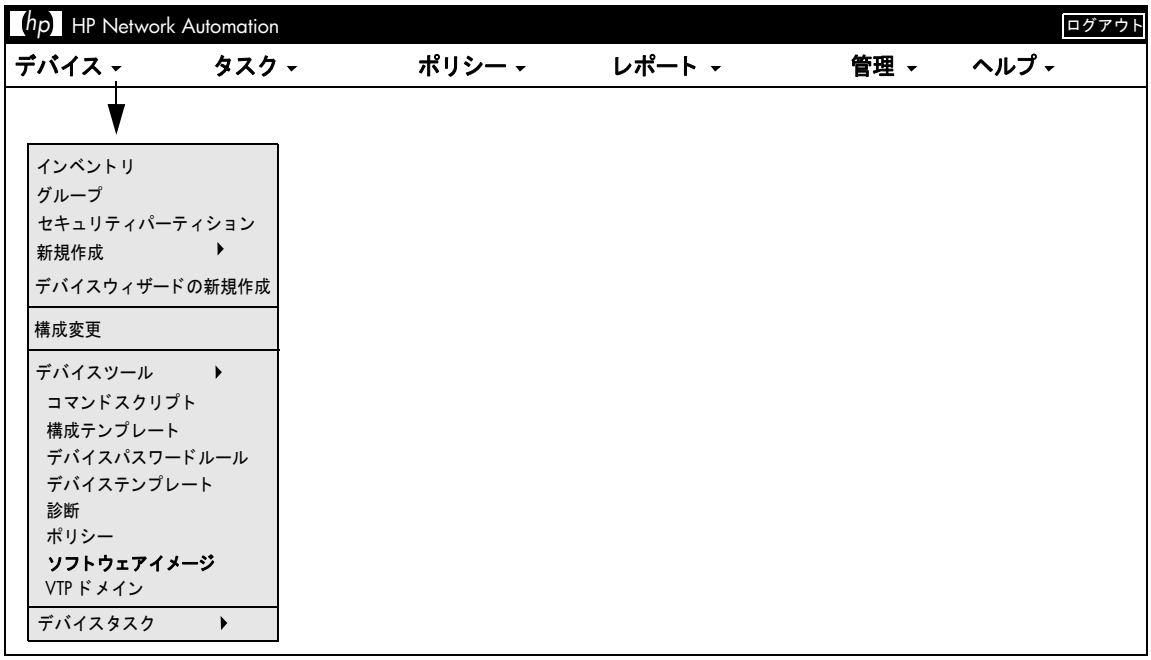
フィールド	説明 / アクション
テストするポリシーを選択	ドロップダウンメニューからポリシーを選択します。
テスト対象のデバイスを選択	ポリシーのテスト対象とするデバイスを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。

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	「はじめに」（544 ページ）
ソフトウェアイメージ	「ソフトウェアイメージ」（547 ページ）
イメージセットの追加	「イメージセットの追加」（549 ページ）
ソフトウェアの配布	「ソフトウェアの配布」（552 ページ）
新規準拠の追加	「新規ソフトウェアレベルの追加」（553 ページ）
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のバージョンの表示」（556 ページ）

ソフトウェアイメージへのナビゲート



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。

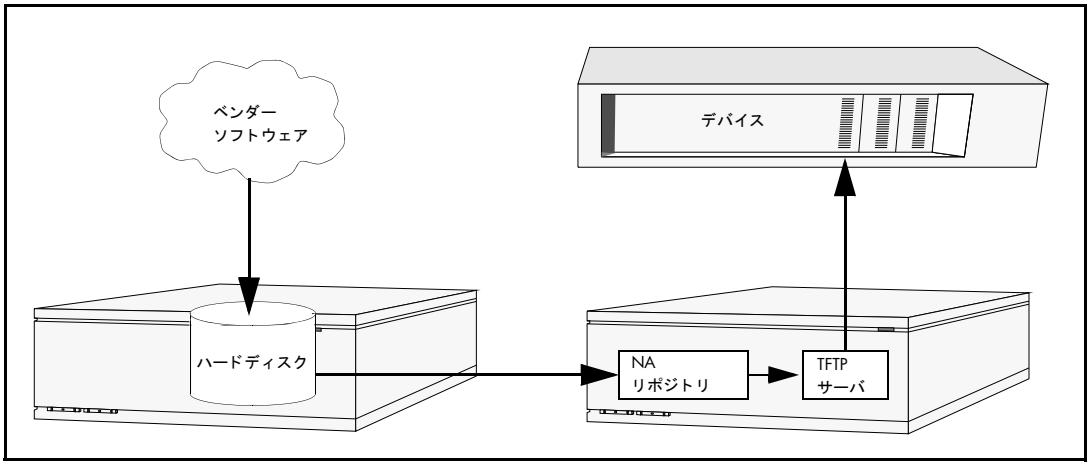
以下のことが可能です。

- 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（例えば、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。例えば、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リング。例えば、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リングする場合もあります。
- 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」（409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」（770 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。例えば、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」(770 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] メニューバーの [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	[タスクの新規作成]-[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、「[Cisco.com からイメージをダウンロード] タスクページ」（452 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、「イメージセットの追加」（549 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、「新規ソフトウェアレベルの追加」（533 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、「デバイスソフトウェアレポート」（764 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。

フィールド	説明 / アクション
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、「デバイスとユーザのセグメント化」（188 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。 • 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、「[ソフトウェアイメージの編集] ページのフィールド」（551 ページ）を参照してください。 • 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。「[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」（549 ページ）、「[ソフトウェアイメージの編集] ページのフィールド」（551 ページ）、または「ソフトウェアの配布」（552 ページ）を参照してください。 • 削除：イメージを削除できます。 • 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、「ソフトウェアの配布」（552 ページ）を参照してください。

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] メニューバーの [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。（**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。
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、暗号学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	イメージセット要件には、次のようなものがあります。 • 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。例えば、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。 • 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。例えば、Cisco Aironet 1200 series Access Point の場合は、[AIR-AP1220-IOS-UPGRD (C1200 Series)] を選択します。 • システムメモリ (バイト単位) >= ：処理が成功するためにイメージセットで必要な最小の 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。例えば、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。 • プロセッサ：デバイスの CPU のことです。例えば、Cisco Aironet 1200 series Access Point の場合は、[AIR-AP1220-IOS-UPGRD (PowerPC405GP)] を選択します。 • ブート ROM：デバイスの ROM のことです。
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] メニューの [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	• 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。例えば、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。 • 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。例えば、Cisco Aironet 1200 series Access Point の場合は、[AIR-AP1220-IOS-UPGRD (C1200 Series)] を選択します。 • デバイスに必要な RAM >= ：デバイスの最小 RAM。 • プロセッサ：デバイスの CPU のことです。例えば、Cisco Aironet 1200 series Access Point の場合は、[AIR-AP1220-IOS-UPGRD (PowerPC405GP)] を選択します。 • ブート ROM：デバイスの ROM のことです。 • 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。

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] メニューの [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」（409 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] メニューの [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
ソフトウェアレベルを追加	
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。 • 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）。 • 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。

フィールド	説明 / アクション
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。 • セキュリティリスク • 実稼動前 • 廃止 • ブロンズ • シルバー • ゴールド • プラチナ
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。（**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。）
一致基準（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。）
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。
ソフトウェアの脆弱性情報（セキュリティリスクレベル）	
開示日	ソフトウェアの脆弱性が警告された日付を次の形式で入力します。*yyyy-MM-dd*

フィールド	説明 / アクション
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。 • 重要 • 高 • 中 • 低 • 情報
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、www.cve.mitre.org. 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] メニューバーの [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」（764 ページ）を参照してください。

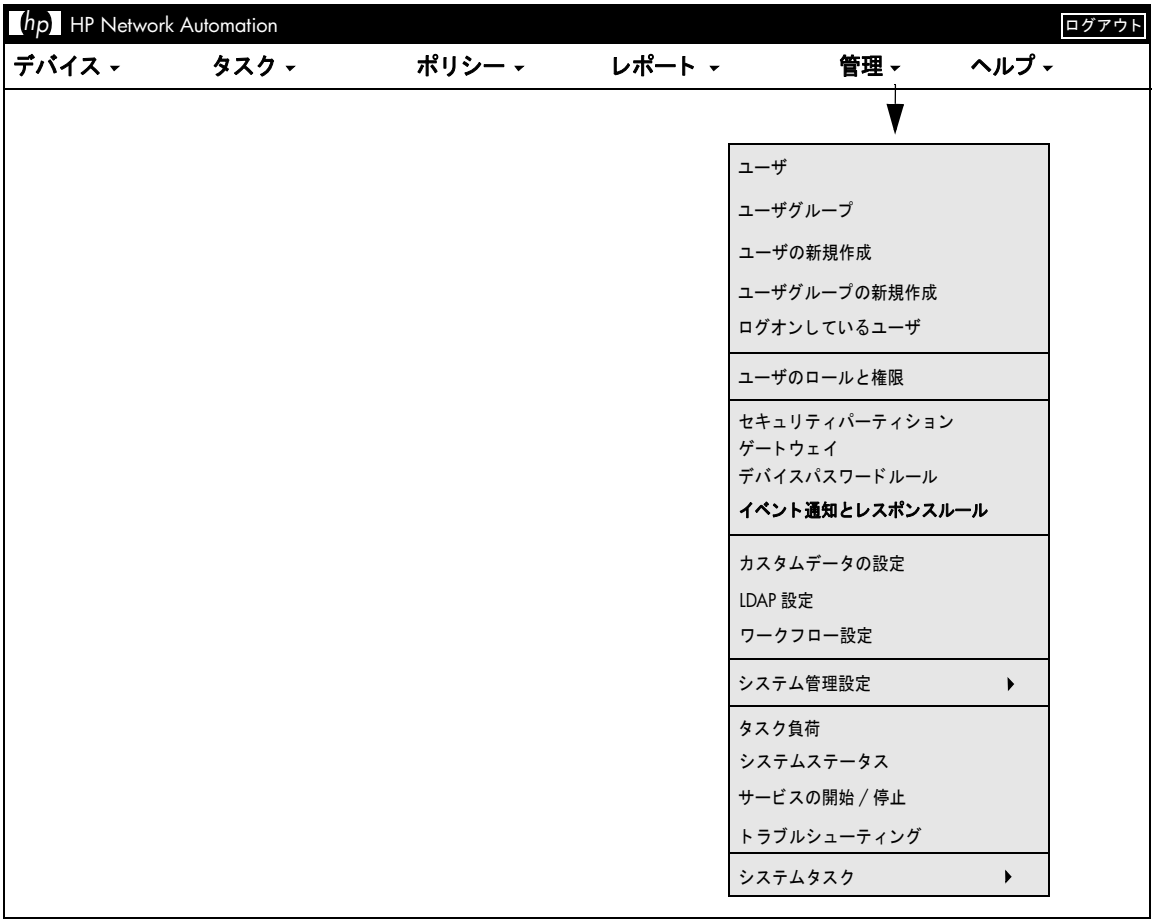
注意： [レポート] ドロップダウンメニューから [デバイスソフトウェアレポート] へナビゲートもできます。

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	「はじめに」（559 ページ）
イベントルールの追加	「イベントルールの追加」（565 ページ）
イベントルール検索結果	「[イベント通知とレスポンスルール] ページのフィールド」（566 ページ）
イベント通知ルールの新規作成	「[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」（567 ページ）
イベントルールの変数	「イベントルール変数」（573 ページ）

イベント通知ルールへのナビゲート



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。
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。

イベント	説明
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。
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。

イベント	説明
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。
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。
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。
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。

イベント	説明
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。
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。
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。
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）。

イベント	説明
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。
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。

イベント	説明
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。

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、「[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」（567 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、「デバイスとユーザのセグメント化」（188 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。 • タスクを実行 • 電子メールを送信 • SNMP トラップを送信 • 電子メールの要約に追加 • syslog メッセージを送信
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。 • 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、「[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」（567 ページ）を参照してください。 • 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。

[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で追加	イベントルール名を入力します。
このアクションを実行	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)。 • タスクを実行 :「[タスクの実行] アクション」(569 ページ) を参照してください。 • 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」(569 ページ) を参照してください。 • 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」(570 ページ) を参照してください。 • SNMP トラップを送信 :「[SNMP トラップを送信] アクション」(571 ページ) を参照してください。 • syslog メッセージを送信 :「[syslog メッセージを送信] アクション」(572 ページ) を参照してください。 • 作成 / チケットへの追加 :「作成 / チケットへの追加」(572 ページ) を参照してください。

フィールド	説明 / アクション
以下のイベントが発生するとき	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 Sfift 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」(559 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。 • 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」（514 ページ）を参照してください。 • 少なくとも < > 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」（514 ページ）を参照してください。 • 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。 • 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。 [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。
ルールのステータス	次のオプションのいずれかを選択します。 • 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。 • 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。
～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、「デバイスとユーザのセグメント化」（188 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。例えば、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、時間 (分)、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。

フィールド	説明 / アクション
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 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 です。
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。例えば、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 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。[変数名の表示] 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、「イベントルール変数」（573 ページ）を参照してください。
宛先	メッセージ送信先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。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。

フィールド	説明 / アクション
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過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。
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、「イベントルール変数」（573 ページ）を参照してください。

フィールド	説明 / アクション
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。 • アラート • 重要 • デバッグ • 緊急 • エラー • 情報 • 通知 • 警告
[syslog メッセージを送信] アクション	
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。例えば、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、「イベントルール変数」（573 ページ）を参照してください。
作成 / チケットへの追加	
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
- 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を表示します。
$IPAddress$	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。

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
$ApprovalPriority$	タスク承認優先度。
$ApprovalDate$	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。
$AppURL$	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（*https://host/* 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いない場合、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いない場合、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。
$OriginatorFirstName$	タスク作成者の名。

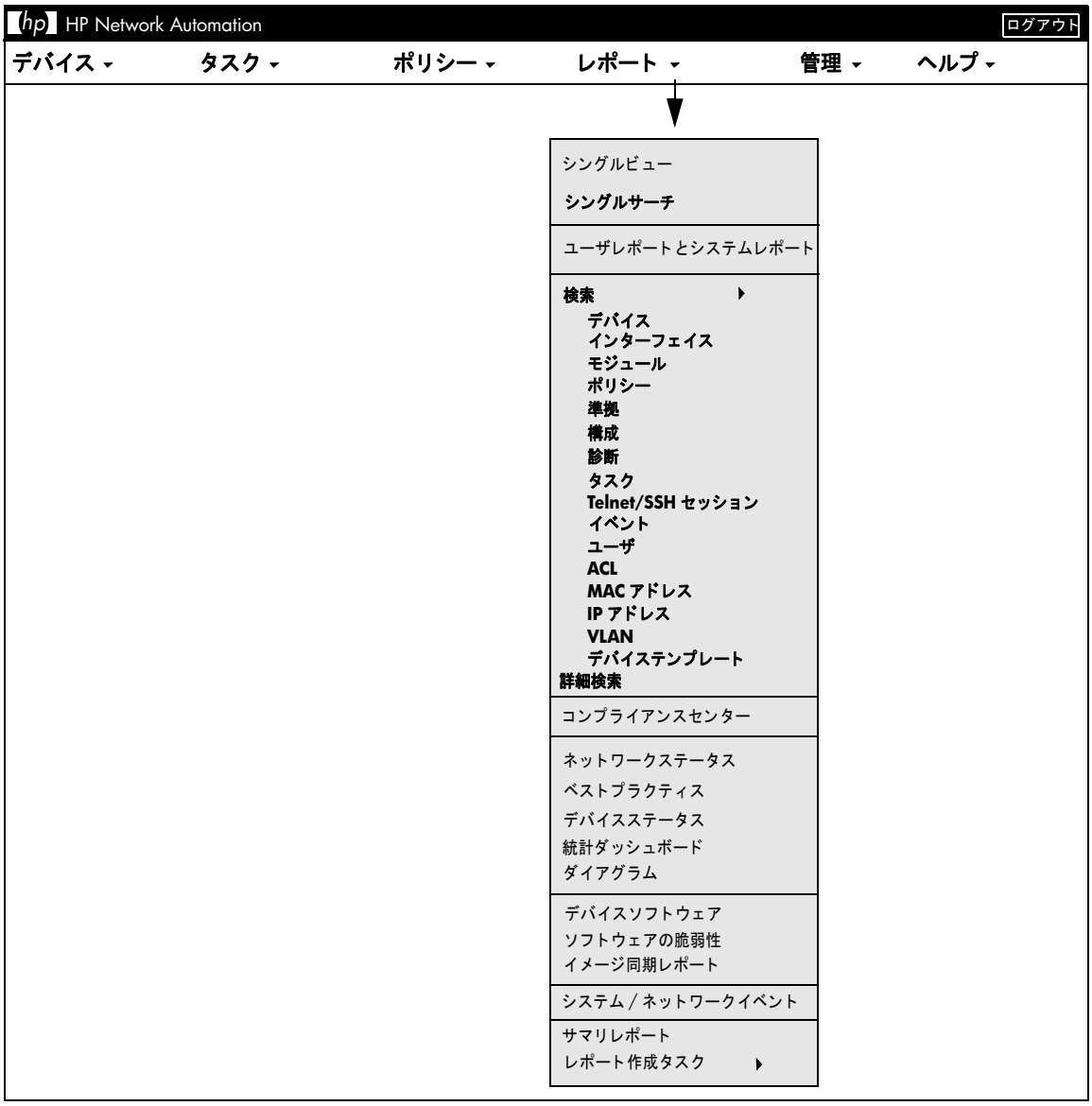
変数	説明
$OriginatorLastName$	タスク作成者の姓。
$OriginatorName$	タスク作成者の名前。
$TaskName$	タスク名。
$TaskComments$	タスクコメント。
$TaskDevices$	タスクにより影響を受けるデバイスのリスト。
$TaskFrequency$	タスクの頻度。
$TaskID$	イベントがタスクに関連しない場合は null 文字列。

第 11 章： 検索の実行

トピックの参照先リスト

検索	参照先：
デバイスの検索	「デバイスの検索」（579 ページ）
インターフェイスの検索	「インターフェイスの検索」（589 ページ）
モジュールの検索	「モジュールの検索」（593 ページ）
ポリシーの検索	「ポリシーの検索」（597 ページ）
準拠の検索	「ポリシー、ルール、および準拠の検索」（601 ページ）
構成の検索	「[構成を検索] ページのフィールド」（606 ページ）
診断の検索	「診断の検索」（611 ページ）
タスクの検索	「タスクの検索」（617 ページ）
セッションの検索	「セッションの検索」（625 ページ）
イベントの検索	「イベントの検索」（631 ページ）
イベントの説明	「イベントの説明」（635 ページ）
ユーザの検索	「ユーザの検索」（643 ページ）
ACL の検索	「ACL の検索」（646 ページ）
MAC アドレスの検索	「MAC アドレスの検索」（652 ページ）
IP アドレスの検索	「IP アドレスの検索」（656 ページ）
VLAN の検索	「VLAN の検索」（660 ページ）
デバイステンプレートの検索	「デバイステンプレートの検索」（663 ページ）
シングルサーチ	「シングルサーチ」（666 ページ）
詳細検索	「詳細検索」（669 ページ）

検索ページへのナビゲート



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」（507 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えたら、[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」（586 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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
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	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。 • アクティブ • 非アクティブ • 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。詳細は、「ベアメタルプロビジョニング」（149 ページ）を参照してください。）

フィールド	説明 / アクション
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。
ポリシー準拠	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。 • 任意（デフォルト） • 準拠したデバイス • 準拠しないデバイス • 適用できるポリシーがデバイスにない • ルール優先度に非準拠：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、指定の重要度を超えた、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、「[ルールの新規作成] ページのフィールド」（514 ページ）を参照してください。） • 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。 • 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、「[ルールの新規作成] ページのフィールド」（514 ページ）を参照してください。）
アクセス方法	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。 • FTP • RLogin • SCP • SNMP • SSH • TFTP • Telnet
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。

フィールド	説明 / アクション
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	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。
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。
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、時間 (分)、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。 **注意**：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、「[診断の実行] タスクページのフィールド」（393 ページ）を参照してください。

フィールド	説明 / アクション
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、「表示メニューオプション」（257 ページ）を参照してください。 **注意**：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。
構成テキスト	演算子（「含む」または「含まない」）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。検索演算子を「含む」にする場合は、ページの最下部にある [一致した行の前後 <#> 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、パフォーマンスが大幅に低下することがあります。）
異なるスタートアップとランニング構成	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。
最終変更時間	次の演算子を選択します。 • 「次の日時以降」または「次の日時以前」 • 「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 **注意**：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。
作成日	次の演算子を選択します。 • 「次の日時以降」または「次の日時以前」 • 「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 **注意**：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。

フィールド	説明 / アクション
パスワードルール	演算子を選択し、パスワードルー名を入力します。
ACL ID	演算子を選択し、ACL の ID を入力します。
ACL ハンドル	演算子を選択し、ACL ハンドルを入力します。
ACL タイプ	演算子を選択し、ACL タイプを入力します。
ACL 構成	演算子を選択し、ACL タイプを入力します。
ACL アプリケーション	演算子を選択し、ACL アプリケーションを入力します。
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。（**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。）

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	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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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、「パーティション」（198 ページ）を参照してください。）

[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」（586 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」(580 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。

オプション	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。 • 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。 • 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。 • 一括編集：[一括編集] ページが開きます。「[デバイスを一括編集] ページのフィールド」（206 ページ）を参照してください。 • ダイアグラム：「ダイアグラム」（752 ページ）を参照してください。 • 削除：選択したデバイスが削除されます。 • 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」（458 ページ）を参照してください。 • Syslog の構成：「[Syslog の構成] タスクページのフィールド」（362 ページ）を参照してください。 • 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」（366 ページ）を参照してください。 • 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」（371 ページ）を参照してください。 • 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」（375 ページ）を参照してください。 • 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」（385 ページ）を参照してください。 • 診断の実行：「[診断の実行] タスクページのフィールド」（393 ページ）を参照してください。 • 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」（379 ページ）を参照してください。 • 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」（399 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：「[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」（404 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：「[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」（409 ページ）を参照してください。 • ACL の削除：「ACL の削除タスクページ」（882 ページ）を参照してください。 • OS 分析：「[OS 分析] タスクページのフィールド」（432 ページ）を参照してください。 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。

オプション	説明 / アクション
アクション	[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。 • 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。 • Telnet：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。 • SSH：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。 • 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。
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。 • 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。 • 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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。

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」（592 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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない
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。

フィールド	説明 / アクション
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、ポート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。
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	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。(**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。)
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。

フィールド	説明 / アクション
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。（**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。）
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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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、「パーティション」（198 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」（589 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	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、「コマンドスクリプトの実行」（732 ページ）を参照してください。 隣接の [選択] ドロップダウンメニューを使用すると、インターフェイスを全選択または全選択解除できます。
アクション	[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。 • 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、「[インターフェイスの詳細を編集] ページのフィールド」（267 ページ）を参照してください。 • 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、「[インターフェイスの詳細] ページのフィールド」（265 ページ）を参照してください。
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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。

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」（597 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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
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。

フィールド	説明 / アクション
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。
モジュールモデル	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
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	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。
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。（**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。）

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	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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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、「パーティション」（198 ページ）を参照してください。）

[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」（593 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	[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。 • 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。 • 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。
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。 • 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。 • 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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。

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」（507 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」（506 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」（508 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えたら、[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。

フィールド	説明 / アクション
ポリシー名	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。 • 含む • 含まない • 一致する • 等しい • 等しくない
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、デバイスセレクタを使用します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。
作成日	次の演算子を選択します。 •「次の日時以降」または「次の日時以前」 •「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 **注意**：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。
ステータス	次のオプションのいずれかを選択します。 • 任意（デフォルト） • アクティブ • 非アクティブ
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。 •「次の日時以降」または「次の日時以前」 •「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 **注意**：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。
解決策	演算子と一緒にソリューション名を入力します。

フィールド	説明 / アクション
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 を演算子と共に入力します。
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 を演算子と共に入力します。
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。（**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、「パーティション」（198 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」（597 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	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。 • 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。 • 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。 • 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。 • 削除：選択したデバイスが削除されます。
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	各ルールで次のアクションを選択できます。 • 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。 • 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、「[ポリシー準拠のテスト] ページのフィールド」（541 ページ）を参照してください。
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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。

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えたら、[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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
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	デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。
準拠	次のオプションのいずれかを選択します。 • すべての準拠状態 • 準拠したデバイス • 準拠しないデバイス • デバイスは未確認です • 適用できるポリシーがデバイスにない
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。

フィールド	説明 / アクション
ルールタイプ	次のオプションを 1 つ以上選択します。 • 構成 • 診断 • ソフトウェア
ルール重要度	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。 • 情報：一般的に対応を必要としないイベント。 • 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。 • 中：適時に応答を必要とするイベント（通常は 72 時間以内）。 • 高：緊急の対応を必要とするイベント（通常は 24 時間以内）。 • 重要：即時の対応を必要とするイベント。
ルールの説明	検索結果にルールの説明を含めます。
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	次の演算子を選択します。 •「次の日時以降」または「次の日時以前」 •「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 **注意**：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。
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	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、「パーティション」（198 ページ）を参照してください。）

[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」（602 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	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： • 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。 • 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。 • 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。 • ダイアグラム：「ダイアグラム」（752 ページ）を参照してください。 • 削除：選択したデバイスが削除されます。 • 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」（458 ページ）を参照してください。 • Syslog の構成：「[Syslog の構成] タスクページのフィールド」（362 ページ）を参照してください。 • 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」（366 ページ）を参照してください。 • 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」（371 ページ）を参照してください。 • 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」（375 ページ）を参照してください。 • 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」（385 ページ）を参照してください。 • 診断の実行：「[診断の実行] タスクページのフィールド」（393 ページ）を参照してください。 • 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」（379 ページ）を参照してください。 • 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」（399 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（*続き*）	• 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」（404 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：「[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」（409 ページ）を参照してください。 • ACL の削除：「ACL の削除タスクページ」（882 ページ）を参照してください。 • OS 分析：「[OS 分析] タスクページのフィールド」（432 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：「[デバイスの編集] ページのフィールド」（142 ページ）を参照してください。
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。
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。 • 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。 • 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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。

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。

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、[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」（609 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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
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。

フィールド	説明 / アクション
日付	次の演算子を選択します。 • 「次の日時以降」または「次の日時以前」 • 「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 **注意**：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。
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。
デバイスステータス	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。 • アクティブ • 非アクティブ • 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。詳細は、「ベアメタルプロビジョニング」（149 ページ）を参照してください。）
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、ダイヤルアップ、DSL_ISDN、ロードバランサなど）を選択します。
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。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。
構成テキスト	演算子（「含む」または「含まない」）を選択し、現在の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。 検索演算子を「含む」にする場合は、ページの最下部にある [一致した行の前後 <#> 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、パフォーマンスが大幅に低下することがあります。）

フィールド	説明 / アクション
検索範囲	次のオプションの 1 つをオンにします。 • 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。 • 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。
異なるスタートアップとランニング構成	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。
構成のカスタムデータ	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。（**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。）
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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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、「パーティション」（198 ページ）を参照してください。）

[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」（606 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	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。 • 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。 • 削除：選択した構成が NA データベースから削除されます。 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。
アクション	[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。 • 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。 • 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。 • 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。

フィールド	説明 / アクション
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。 • 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。 • 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（**注意**：動的グループの作成の詳細については、「動的デバイスグループ」（177 ページ）を参照してください。） • 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。 • 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。 • 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**：［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。）

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」（615 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」（257 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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
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	次の演算子を選択します。 •「次の日時以降」または「次の日時以前」 •「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 **注意**：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。

フィールド	説明 / アクション
診断タイプ	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。 • NA デバイスファイルシステム • ハードウェア情報 • ICMP テスト • メモリトラブルシューティング • NA がデバイスのブートを検出 • NA フラッシュ記憶域容量 • 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 ポートスキャン • NA ルーティングテーブル • NA トポロジーデータ収集 • NA VLAN データ収集 **注意**：診断の詳細については、「表示メニューオプション」（257 ページ）の [診断] フィールドを参照してください。
デバイスステータス	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。 • アクティブ • 非アクティブ • 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。詳細は、「ベアメタルプロビジョニング」（149 ページ）を参照してください。）
診断テキスト	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。
診断のカスタムデータ	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。（**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。）

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	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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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、「パーティション」（198 ページ）を参照してください。）

[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」（612 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	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。 • 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。 • 削除：選択した構成が 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、デバイスを全選択または全選択解除できます。
アクション	[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。 • 詳細を表示：診断の詳細を表示できます。 • 前と比較：この診断を前回の診断と比較します。

オプション	説明 / アクション
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。 • 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。 • 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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。

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」（623 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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない
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。（**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。）
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。

フィールド	説明 / アクション
スケジュール日時	次の演算子を選択します。 • 「次の日時以降」または「次の日時以前」 • 「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 **注意**：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。
タスクのステータス	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。 • 保留 • 成功 • 失敗 • 実行中 • 一時停止 • ドラフト • 待機中 • 重複 • スキップ • 警告 • 要求 • テンプレート
タスク優先度	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、「タスクの予定」（355 ページ）を参照してください。

フィールド	説明 / アクション
タスクタイプ	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。 • デバイスソフトウェアのバックアップ • ポリシー準拠の確認 • Syslog の構成 • データの整理 • 重複の削除 • ACL の削除 • 構成を配布 • パスワードの配布 • リモートエージェントの配布 • デバイスコンテキスト • デバイスコンテキストの削除 • ネットワークデバイスの検出 • ドライバの検出 • Cisco.com からイメージをダウンロード • 電子メールレポート • サマリレポートの生成 • インポート • IOS XR ソフトウェア • マルチタスクプロジェクト • OS 分析 • デバイスのプロビジョニング • デバイスのリブート • FQDN の解決 • コマンドスクリプトの実行

フィールド	説明 / アクション
タスクタイプ（*続き*）	• 診断の実行 • 外部アプリケーションの実行 • ICMP テストの実行 • スタートアップとランニングの同期 • スナップショットの取得 • デバイスソフトウェアの更新 • VLAN タスク
エラータイプ	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。 • デバイスに到達できません • パスワードが誤っています • 権限が不十分です • パスワードが見つかりません • デバイスが認識されません • デバイスがサポートされていません
コメント	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。
結果	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。 [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。（**注意**：ロード対象の結果が大量にある場合、パフォーマンスが大幅に低下することがあります。）

フィールド	説明 / アクション
承認期限	次の演算子を選択します。 • 「次の日時以降」または「次の日時以前」 • 「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 **注意**：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。
承認のステータス	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。 • 承認済み • ドラフト • 対応していません • 未承認 • 無効化 • 承認を待機中
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、ダイヤルアップ、DSL_ISDN、ロードバランサなど）を選択します。
子タスクを除く	オンにすると、子タスクが検索から除外されます。
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。（**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。）
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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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	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、「パーティション」（198 ページ）を参照してください。）

[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」（617 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	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。 • 削除：選択したタスクが削除されます。 隣接の [選択] ドロップダウンメニューを使用すると、タスクを全選択または全選択解除できます。
アクション	[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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • キャンセル：タスクをキャンセルします。

オプション	説明 / アクション
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。 • 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。 • 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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。）

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」（84 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」（629 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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
デバイス IP	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。
デバイスステータス	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。 • アクティブ • 非アクティブ • 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。詳細は、「ベアメタルプロビジョニング」（149 ページ）を参照してください。）
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	次の演算子を選択します。 •「次の日時以降」または「次の日時以前」 •「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 **注意**：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。

フィールド	説明 / アクション
終了日	次の演算子を選択します。 •「次の日時以降」または「次の日時以前」 •「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 **注意**：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。
ステータス	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。 • 失敗 • 開く • 終了
セッションタイプ	次のオプションのいずれかを選択します。 • 任意 • Telnet • SSH
セッションデータ	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。 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。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。（**注意**：ロード対象の結果が大量にある場合、パフォーマンスが大幅に低下することがあります。）
セッションのカスタムデータ	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。（**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。）

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	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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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、「パーティション」（198 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」（626 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	[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。 • 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。 • 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。 • 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、「コマンドスクリプトの追加」（714 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。 • 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。

オプション	説明 / アクション
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。 • 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。 • 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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。）

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」（635 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」（634 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。 •「次の日時以降」または「次の日時以前」 •「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 **注意**：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、「イベントの説明」（635 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。

フィールド	説明 / アクション
重要度	次のオプションから、1 つ以上選択します。 • 情報：一般的に対応を必要としないイベント。 • 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。 • 中：適時に応答を必要とするイベント（通常は 72 時間以内）。 • 高：緊急の対応を必要とするイベント（通常は 24 時間以内）。 • 重要：即時の対応を必要とするイベント。
ホスト名	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
デバイス IP	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。
説明	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。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。（**注意**：ロード対象の結果が大量にある場合、パフォーマンスが大幅に低下することがあります。）

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	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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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、「パーティション」（198 ページ）を参照してください。）

[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」（631 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	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。 • 削除：選択したイベントが削除されます。 隣接の [選択] ドロップダウンメニューを使用すると、タスクを全選択または全選択解除できます。
アクション	[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。 • 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。 • 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。

フィールド	説明 / アクション
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。 • 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。 • 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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。）

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。

イベント	説明
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ました。
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。

イベント	説明
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。

イベント	説明
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。
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。

イベント	説明
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。
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。

イベント	説明
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。

イベント	説明
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。
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。

イベント	説明
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」（645 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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない
姓	演算子を選択し、ユーザの姓を入力します。
ユーザ名	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。）
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。

フィールド	説明 / アクション
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	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、「パーティション」（198 ページ）を参照してください。）

[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」（643 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	[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。 • 編集：[自分のプロファイル] 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、「[自分のプロファイル] ページのフィールド」（334 ページ）を参照してください。 • 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。 • 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、「[自分の権限] ページのフィールド」（338 ページ）を参照してください。 • 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。
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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。

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」（873 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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
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。

フィールド	説明 / アクション
ACL 構成	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。 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。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。（**注意**：ロード対象の結果が大量にある場合、パフォーマンスが大幅に低下することがあります。）
ACL アプリケーション	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。例えば、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。
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。
コメント	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。
変更者	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。
最終変更	次の演算子を選択します。 • 「次の日時以降」または「次の日時以前」 • 「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 **注意**：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。
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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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	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、「パーティション」（198 ページ）を参照してください。）

[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」（650 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

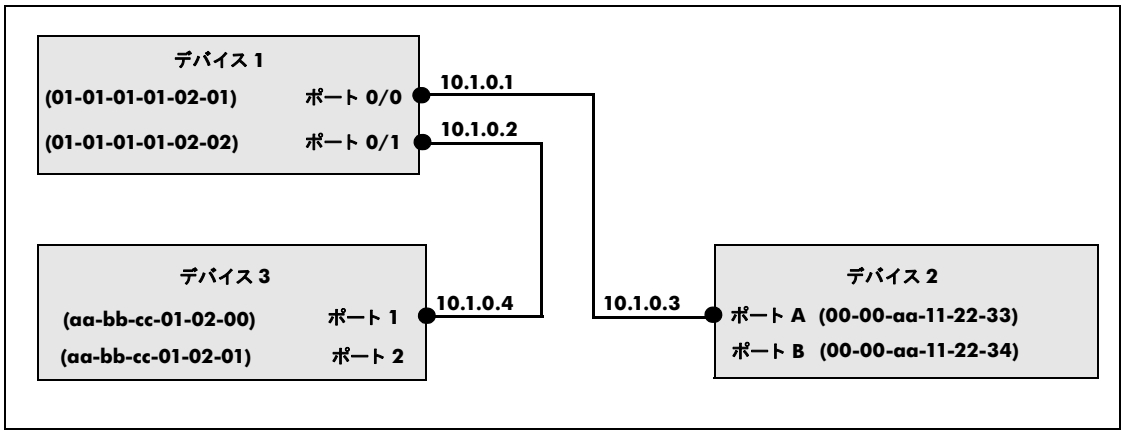
[ACL の検索結果] ページの表示は、[ACL を検索] ページで選択した検索条件によって異なります。詳細については、「[ACL を検索] ページのフィールド」（647 ページ）を参照してください。次の表は、[ACL の検索結果] ページに用意されているオプションを示します。

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	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。 • 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。 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。
アクション	[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。 • 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、「ACL の削除」（881 ページ）を参照してください。 • 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、「ACL の表示」（868 ページ）を参照してください。 • 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。

オプション	説明 / アクション
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。 • 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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。

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、およびポートの間の関係を示します。



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」（655 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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
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。
Port Name	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。

フィールド	説明 / アクション
アドレスタイプ	次のオプションのいずれかを選択します。 • 全アドレス（デフォルト） • 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。 • 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。 **注意**：[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。
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。
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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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、「パーティション」（198 ページ）を参照してください。）

[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」（653 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。 • 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。 • 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。
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。 • 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。 • 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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。

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 9.0 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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
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。例：IPv4：10.255.?.255、192.*、172.16.30.1 IPv6：aff:38:?:10、fc00:c0a8:*、::1

フィールド	説明 / アクション
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 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
アドレスタイプ	次のオプションのいずれかを選択します。 • 全アドレス（デフォルト） • 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。 • 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。 **注意**：[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。
検索範囲	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。
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 MAC	演算子を選択し、関連 MAC 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	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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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。（**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、「パーティション」（198 ページ）を参照してください。）

[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」（656 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	MAC アドレスごとに、次のアクションを選択できます。 • 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。 • 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。
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。 • 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。 • 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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。

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）」（274 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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
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。

フィールド	説明 / アクション
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、「仮想ローカルエリアネットワーク（VLAN）」（274 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。
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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 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、「パーティション」（198 ページ）を参照してください。）

[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」（660 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	VLAN ごとに、次のアクションを選択できます。 • 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、「[VLAN 詳細] ページのフィールド」（279 ページ）を参照してください。 • 編集：[VLAN 詳細を編集] ページが開きます。詳細については、「VLAN の作成と編集」（278 ページ）を参照してください。 • 削除：VLAN を削除することを確認できるダイアログボックスが開きます。
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。 • 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。 • 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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。

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」（151 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	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
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。

フィールド	説明 / アクション
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	演算子を選択し、コメントを入力します。
構成テキスト	演算子を選択し、構成テキストを入力します。 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。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。(**注意**：ロード対象の結果が大量にある場合、パフォーマンスが大幅に低下することがあります。)
作成日	次の演算子を選択します。 • 「次の日時以降」または「次の日時以前」 • 「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 **注意**：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。
デバイスのカスタムデータ	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。
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。(**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、「パーティション」(198 ページ）を参照してください。)

[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」（663 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。 • 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。「[デバイステンプレート] ページのフィールド」（151 ページ）を参照してください。 • 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。
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。 • 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。 • 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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。

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」（668 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	次の演算子を選択します。 •「次の日時以降」または「次の日時以前」 •「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 **注意**：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、「イベントの説明」（635 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。選択可能な演算子は次のとおりです。 • 含む • 含まない • 一致する • 等しい • 等しくない

フィールド	説明 / アクション
重要度	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。 • 情報：一般的に対応を必要としないイベント。 • 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。 • 中：適時に応答を必要とするイベント（通常は 72 時間以内）。 • 高：緊急の対応を必要とするイベント（通常は 24 時間以内）。 • 重要：即時の対応を必要とするイベント。
ホスト名	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。 • 含む • 含まない • 一致する • 等しい • 等しくない 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。）
デバイス IP	演算子（上記参照）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。
説明	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。
デバイスが所属するグループ	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。
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。（**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、「パーティション」（198 ページ）を参照してください。）

[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」（666 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	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。 • 削除：選択したイベントが削除されます。 隣接の [選択] ドロップダウンメニューを使用すると、タスクを全選択または全選択解除できます。
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。 • 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。 • 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。 • 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、「ユーザレポートとシステムレポート」（738 ページ）を参照してください。 • 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。 • 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。

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。

- ブール演算子（AND および OR）の使用による検索のフィルタリング。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。
- 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	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。 • ACL • 準拠 • 構成 • デバイス • 診断 • イベント • インターフェイス • モジュール • セッション • タスク

検索条件
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。

フィールド	説明 / アクション
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。 • ホスト名 • デバイス IP • ドメイン名 • デバイスステータス • ポリシー準拠
ブール式	
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。例えば、3 つの検索条件が定義されている場合、式は *A and B and C* 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。(**注意**：条件の最大数は 10 です。)
デバイスグループで検索を絞り込み	
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。 • 選択グループ内のいずれか（デフォルト） • 選択グループのすべて • 選択グループになし **注意**：デバイスセレクタを使用してグループを選択します。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」(180 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。(**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、「パーティション」(198 ページ）を参照してください。)
出力のカスタマイズ	
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。

フィールド	説明 / アクション
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。

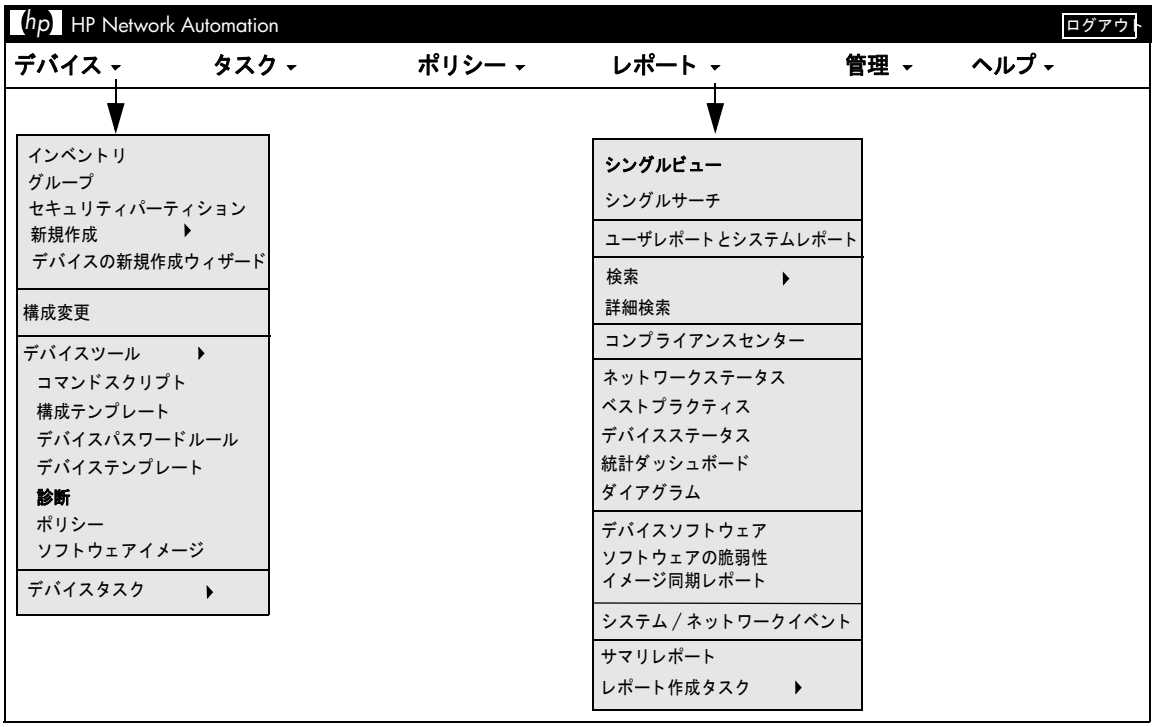
1. NA にログインします。
2. [レポート] のメインメニューバーから、[詳細検索] をクリックします。[詳細検索] ページが開きます。
3. [検索] フィールドで、ドロップダウンメニューから [デバイス] を選択します。
4. [検索条件] フィールドで、ドロップダウンメニューから [ドライバ名] を選択します。
5. NA で使用する Cisco ドライバをすべて選択します。
6. [条件を追加] ドロップダウンメニューから、[ホスト名] を選択します。
7. ドロップダウンメニューから [含まない] を選択し、次のように入力します。`redmond`
8. [条件を追加] ドロッ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）	「イベントの連結ビュー（シングルビュー）」（674 ページ）
診断	「診断」（678 ページ）
診断の追加およびカスタマイジング	「カスタム診断の追加および編集」（681 ページ）

シングルビューおよび診断へのナビゲート



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
- デバイス診断が変化しました
- 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は、「イベントの説明」（635 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 :	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。 • 過去 1、2、4、8、12、24、および 48 時間 • 過去 1 および 2 週間 • 過去 1ヶ月 • 全イベント
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。

フィールド	説明 / アクション
サマリ	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、「イベントの説明」（635 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。 • イベントが発生した日付および時刻。 • 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。 • イベントタイプ。 • イベントの簡単な説明。 • デバイスに関する詳細情報へのリンク。
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	次のイベントについて、[前と比較] リンクが表示されます。 • 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、「デバイス構成の比較」（227 ページ）を参照してください。 • 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。 • 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、「デバイス構成の比較」（227 ページ）を参照してください。

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	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。 • デバイスがブートしました • デバイス構成の変更 • デバイス診断が変化しました • 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

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」（565 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、「[診断の新規作成] ページのフィールド」（680 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、「[診断の実行] タスクページのフィールド」（393 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、「スクリプト / 診断のインポート / エクスポート」（713 ページ）を参照してください。

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、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	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。 **注意**：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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。
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	次のオプションから選択できます。 • 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、「[診断の新規作成] ページのフィールド」（680 ページ）を参照してください。 • 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、「[診断の実行] タスクページのフィールド」（393 ページ）を参照してください。

[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、「[診断] ページのフィールド」（678 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	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。 **注意**：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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。
高度なスクリプティング	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。 • 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。 • 言語：スクリプトの記述に使用した言語を表示します。 • パラメータ：スクリプトのパラメータを入力します。 高度なスクリプトの作成の詳細については、「コマンドスクリプトの追加」（714 ページ）を参照してください。

フィールド	説明 / アクション
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	次のオプションのいずれかを選択します。 • 適用できる全ドライバ（デフォルト） • 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。（**注意**：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）。
スクリプト	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。 **注意**：スクリプトに同じ名前を付けることはできますが、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。

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」（474 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	「はじめに」（687 ページ）
[カスタムデータの設定] ページのフィールド	「[カスタムデータの設定] ページのフィールド」（688 ページ）
拡張カスタムフィールド設定	「拡張カスタムフィールド設定」（693 ページ）

カスタムデータ設定へのナビゲート

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。この数量は拡張でき、無制限のカスタムデータフィールドを使用できます。拡張カスタムデータフィールドを有効にしている場合は、「拡張カスタムフィールド設定」（693 ページ）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	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。 • デバイス構成と診断 • デバイス • デバイスのブレード / モジュール • デバイスのインターフェイス • デバイスグループ • ユーザ • タスク • Telnet/SSH セッション
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、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。
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、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。 • 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。 • 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。
デバイス	

フィールド	説明 / アクション

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、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。 • 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。 • 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。

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、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。 • 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。 • 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。

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。

フィールド	説明 / アクション
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、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。 • 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。 • 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。

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、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。 • 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。 • 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。

ユーザ

次に示すフィールドは、[自分のプロファイル] 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。

フィールド	説明 / アクション
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、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。 • 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。 • 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。

タスク

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、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。 • 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。 • 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。

Telnet/SSH セッション

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、0 ～ 9、_、-、& を使用できます（カンマは含まれません）。

フィールド	説明 / アクション
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。 • 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。 • 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。

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」（78 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 • Devices（デフォルト） • Device Interfaces
[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、「[カスタムデータフィールドの新規作成] ページ」（694 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、「表示メニューオプション」（257 ページ）および「[デバイスインターフェイス] ページのフィールド」（263 ページ）を参照してください。
Devices / Device Interfaces	
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。

フィールド	説明 / アクション
アクション	次のオプションのいずれかを選択します。 • 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。「[カスタムデータフィールドの新規作成] ページ」（694 ページ）を参照してください。 • 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。

[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。

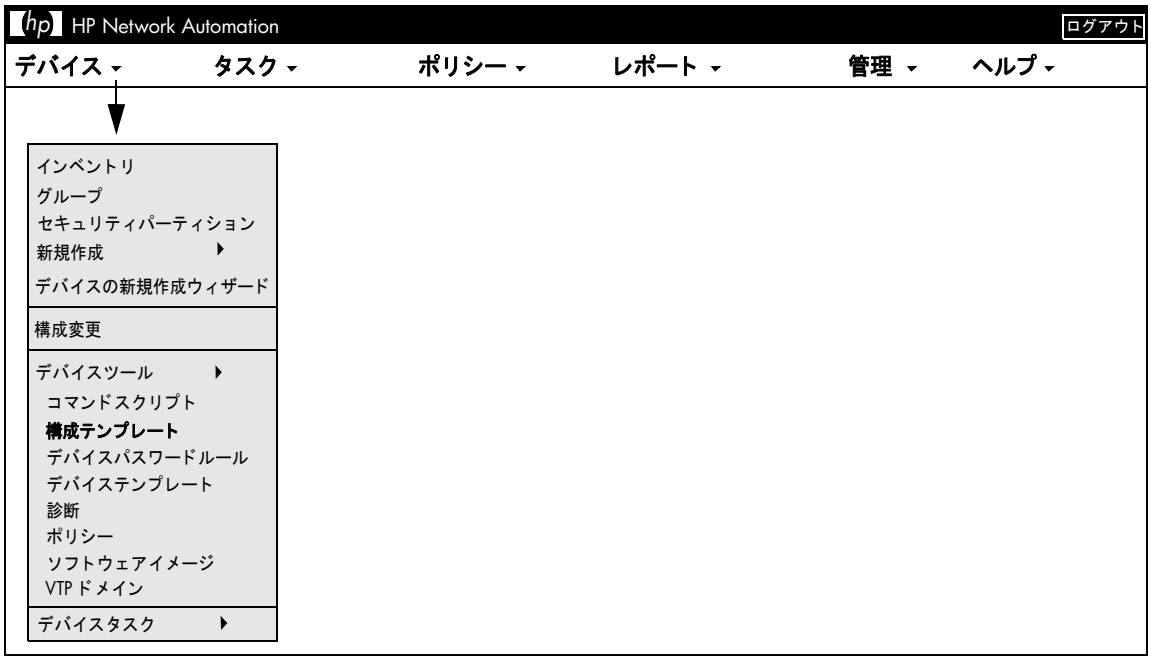
終了したら、[保存] ボタンをクリックします。[拡張カスタムフィールド設定] ページに新規フィールドが表示されます。

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	「はじめに」（696 ページ）
構成テンプレートの表示	「構成テンプレートの表示」（697 ページ）
新規構成テンプレートの作成	「新規構成テンプレートの作成」（700 ページ）

構成テンプレートへの移動



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」（151 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、「新規構成テンプレートの作成」（700 ページ）を参照してください。
ベンダー	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。 • 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 • 新規構成テンプレートの作成
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。

フィールド	説明 / アクション
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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。 **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。
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。 • 任意 • コア • 境界 • テスト
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	次のオプションからいずれか 1 つを選択できます。 • 詳細を表示 : [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、「[テンプレートを表示] ページのフィールド」（702 ページ）を参照してください。 • テキストを表示 : 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、「[テンプレートを表示] ページのフィールド」（702 ページ）を参照してください。 • 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、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、「[テンプレートの新規作成] ページのフィールド」（700 ページ）を参照してください。

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、「構成テンプレートの表示」（697 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。） 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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。
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。 • 任意 • コア • 境界 • テスト

フィールド	説明 / アクション
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。 • 適用できる全ドライバ（デフォルト） • 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。
テンプレート	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。 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。

[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、「[テンプレートの新規作成] ページのフィールド」（700 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。
	
	`sflow destination $dest_ip_1$ $dest_udp_port1$`
	`sflow destination $dest_ip_2$ $dest_udp_port2$`

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、「[構成テンプレート] ページのフィールド」（697 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。

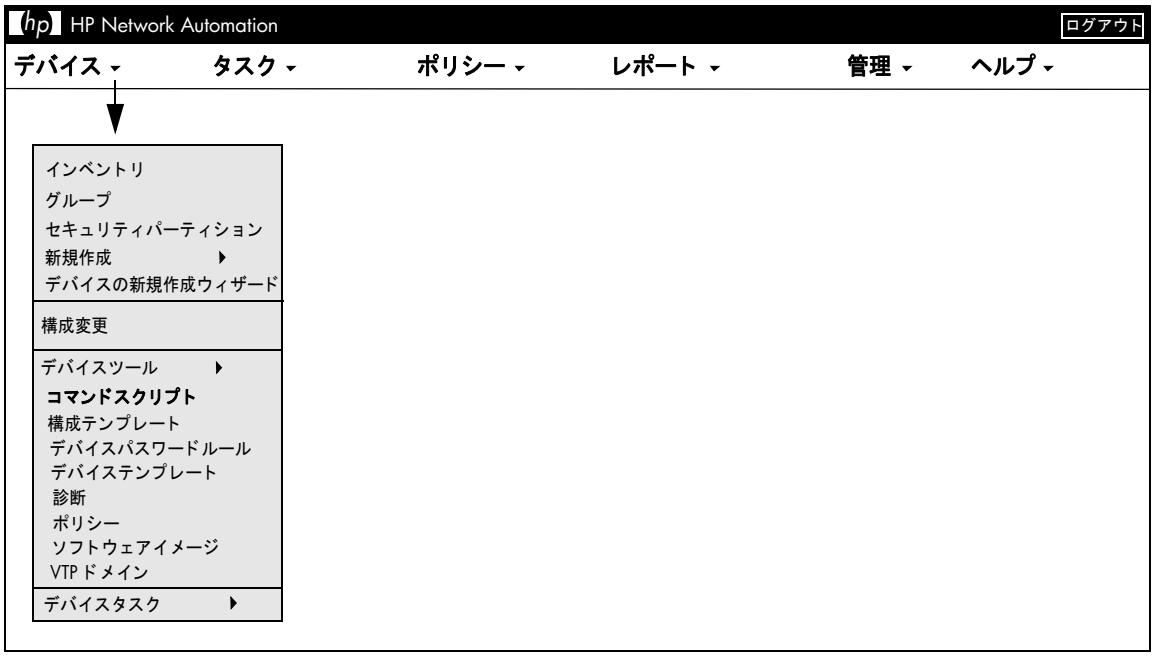
フィールド	説明 / アクション
パーティション	セキュリティや業務上の理由でパーティションを作成した場合、特定パーティションの各デバイスについて構成テンプレートをパーティションできます。構成テンプレートを、特定のパーティション内の特定デバイスに加え、すべてのパーティション内のすべてのデバイスで共有するように構成できます。パーティションの作成の詳細については、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。
モデル	この構成テンプレートが適用されるデバイスのモデルが表示されます。
最終変更者	構成テンプレートを最後に変更したユーザ、またはプロセスが表示されます。
ロール	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。 • 任意 • コア • 境界 • テスト
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。
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	「はじめに」（707 ページ）
コマンドスクリプトの追加および編集	「コマンドスクリプトの追加」（714 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」（732 ページ）
自動修正スクリプトの作成	「自動修正スクリプトの作成」（720 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	「スクリプト / 診断のインポート / エクスポート」（713 ページ）

コマンドスクリプトへのナビゲート



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」（716 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 Orchestrations 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」（95 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」（142 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] の下のメニューバーで、[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」（133 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. 「実稼働前」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」(732 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、「[コマンドスクリプトの新規作成] ページのフィールド」（716 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、「[コマンドスクリプトの実行] 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。
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、「スクリプト / 診断のインポート / エクスポート」（713 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。

フィールド	説明 / アクション
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。 **注意**：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、「デバイスとユーザのセグメント化」（188 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。
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。 • 編集：[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、「[コマンドスクリプトの新規作成] ページのフィールド」（716 ページ）を参照してください。 • 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」（385 ページ）を参照してください。

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	インポートするコマンドスクリプト、または診断スクリプトを選択するか、[参照] ボタンをクリックして、コマンドスクリプトや診断スクリプトを探します。コマンドスクリプトや診断スクリプトが表示されたら、[インポート] ボタンをクリックします。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。
スクリプトのエクスポート	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。

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。例えば、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）。
- ユーザがスクリプトを実行する前に変数値を変更可能な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」（733 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」（66 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 *Opsware::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。変数を組み込むことにより、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
• if またはループは使用不可 • デバイスコマンド（*show conf* のような Cisco のコマンド）を使用 • エラー処理なし • ログイン不要 • NA デバイス変数なし	• if またはループ使用可能 • 言語コマンドを使用（send "show conf\n" や print SOCKET "show conf\n" などの PERL または Expect のコマンド） • エラー処理可能 • ログインコード必須 • NA デバイス変数へのアクセス可能

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。例えば、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」（385 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、「[コマンドスクリプト] ページのフィールド」（711 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。 **注意**：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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。

フィールド	説明 / アクション
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。 • 汎用（デフォルト） • 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。 • 新規作成：新規スクリプトタイプを入力します。

フィールド	説明 / アクション
高度なスクリプティング	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。 • デバイスファミリ：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。 • 言語：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。（**注意**：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、「HP Operations Orchestration（HP OO）」（98 ページ）を参照してください。 • パラメータ：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。（**注意**：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）。 • スクリプト：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。 • 変数：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。） • 変数をプル：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。 - 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）

フィールド	説明 / アクション
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	次のオプションのいずれかを選択します。 • 適用できる全ドライバ（デフォルト） • 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。（**注意**：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）。
スクリプト	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。 **注意**：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。
[変数をプル] ボタン	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。 • HOSTNAME • ETH_SLOT1 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。

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」（514 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。例えば、`$condition_A_line_1$` は条件 A の最初の行に一致する構成行を指します。

言語要素	説明
`$regex_group_match_variable$`	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	`$any_string$`	`$interface$`：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）	`$condition_<label>_line_<number>$`	`$condition_A_line_2` ：条件 A の 2 行目に一致する構成行です。
正規表現グループ一致	`$<loop_variable>.regex_group_<number>$`	`$interface.regex_group_1$`：正規表現パターンに一致した構成行に存在する、最初の正規表現グループの一致です。 • number = 0：全体一致 • number > 0：正規表現キャプチャグループ
ブロック開始パターン	`$block_start$`	ブロック開始パターン用ビルトイン変数の名前です。

変数	命名規則	例
ブロック終了パターン	$block_end$	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。
  例えば、$condition_A_line_1$ 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。（639 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。
  例えば、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（例えば、$matching_line.regex_group_0$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スエンジン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」（385 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」（40 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
```

上述の但し書きの通り、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を考えます。

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経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いてはいけない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] 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. 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」（385 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」（697 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	「はじめに」（737 ページ）
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」（738 ページ）
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」（742 ページ）
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」（746 ページ）
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」（749 ページ）
統計ダッシュボード	「統計ダッシュボード」（751 ページ）
ダイアグラム	「ダイアグラム」（752 ページ）
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」（764 ページ）
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のフィールド」（766 ページ）
ソフトウェアの脆弱性レポート	「ソフトウェアの脆弱性レポート」（768 ページ）
イメージ同期レポート	「イメージ同期レポートのフィールド」（770 ページ）
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」（772 ページ）
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」（774 ページ）
サマリレポート	「サマリレポート」（776 ページ）
電子メールレポート	「電子メールレポート」（780 ページ）

各レポートへのナビゲート

はじめに

HP Network Automation（NA）には、入力が不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」（579 ページ）を参照してください。

各レポートには、検索で使用した基準のサマリが示されます。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、検索で使用した基準のサマリが示されます。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 • COSO 準拠ステータス • 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] の下のメニューバーで [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	次のアクションを選択できます。 • 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。 • 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。 • 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。 • 削除（赤の X アイコン）：レポートを完全に削除します。 • 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。

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] の下のメニューバーで [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」（780 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。「ベストプラクティスレポート」（746 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。「デバイスステータスレポート」（749 ページ）を参照してください。
レポート日	レポートが最後に実行された日時を表示します。
デバイスグループのレポート	報告されるデバイスグループの数を表示します。
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	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。 • 赤：高リスク • 黄：中リスク • 緑：低リスク [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。「デバイスステータスレポート」（749 ページ）を参照してください。
ベストプラクティスのステータス	

フィールド	説明 / アクション
問題	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。 • 24 時間以内のポリシールール違反：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。 • 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。 • 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。 • 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。 • 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。 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。 [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。「ベストプラクティスレポート」（746 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 詳細

フィールド	説明 / アクション
高リスク（赤）の問題	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： • 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。 • 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。 • 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。

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] の下のメニューバーで [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。「ネットワークステータスレポート」（742 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。「デバイスステータスレポート」（749 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。 • 赤：高リスク • 黄：中リスク • 緑：しきい値範囲内
問題	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。 • 24 時間以内のポリシールール違反：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。 • 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。 • 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。 • デバイスアクセスエラー：NA が到達できなかったデバイス。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。 • 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。

ベストプラクティスレポート 詳細

フィールド	説明 / アクション
高リスク（赤）の問題	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。

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」（743 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] の下のメニューバーで [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。「ネットワークステータスレポート」（742 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。「ベストプラクティスレポート」（746 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。 • 赤：高リスク • 黄：中リスク • 緑：しきい値範囲内

フィールド	説明 / アクション
デバイスステータスレポートの詳細	
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」(776 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」(776 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」(738 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」(776 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」(776 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」(742 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」(776 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」(776 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。

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）」（274 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 Users Guide（HP Server Automation ユーザガイド）』*を参照してください。

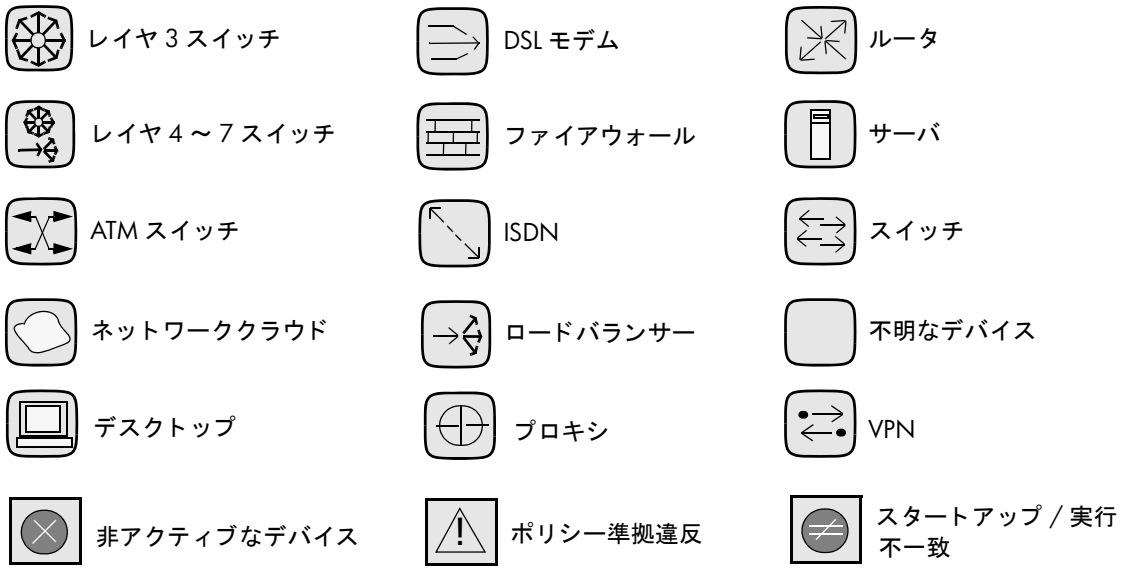
推測されるレイヤ 1 のデータは、経験則に基づいています。NA では、デバイスとサーバのすべてまたはいずれかの間のデータリンク接続数を減らすことにより、ネットワークダイアグラムを見やすくしています。この場合は、推移する接続から推測可能な接続のみが除かれます。

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。

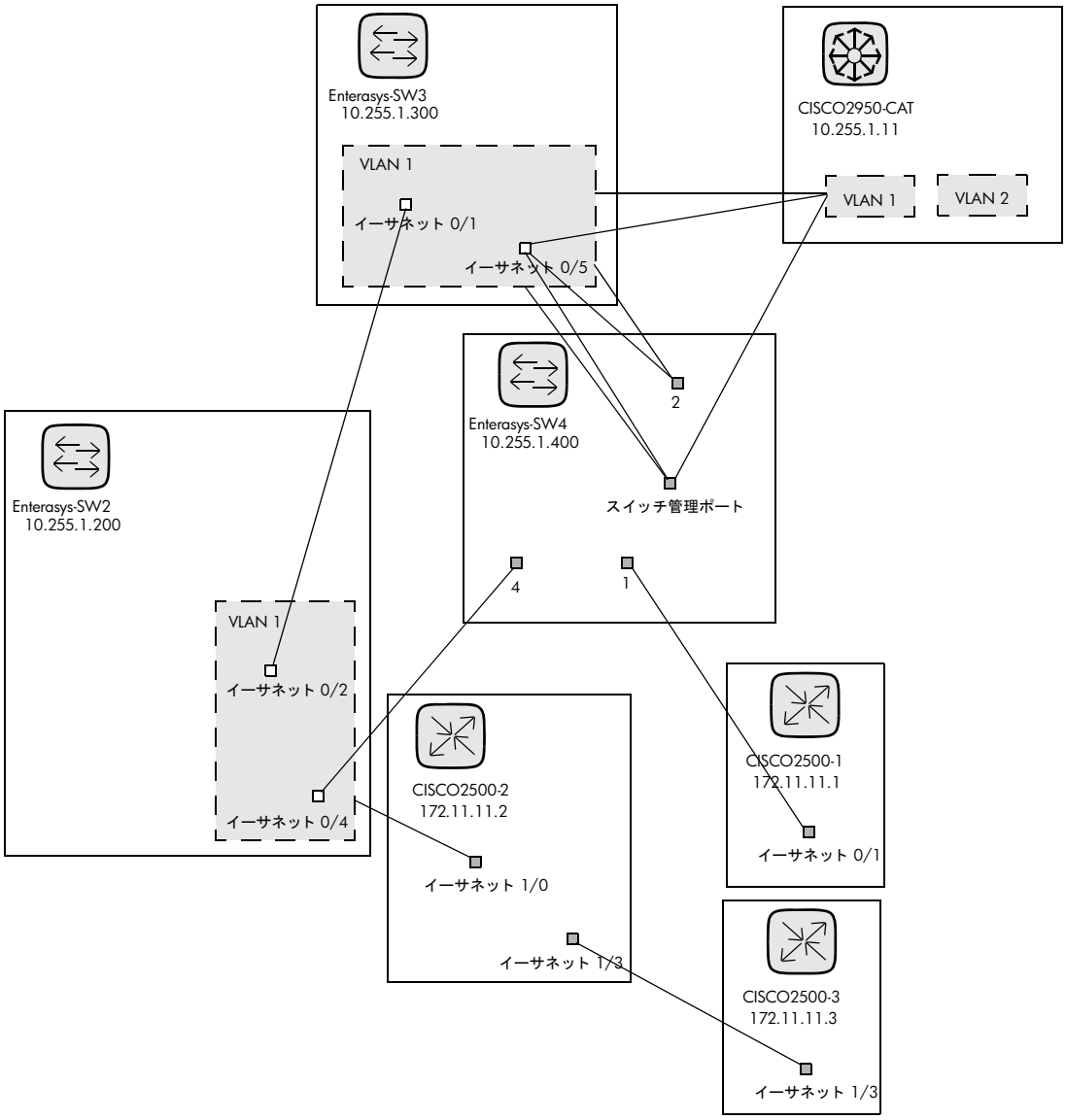
- デバイスが、MAC アドレスが認識される場所のインターフェイス番号を返さない。
- NA が、（MAC アドレスが認識される場所の）トポロジーデータを収集する数分の間に、デバイス間でトラフィックが発生しなかった。
- 2 つの管理デバイスの間に、ハブなどのアドレス指定できないデバイスが存在する。

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。

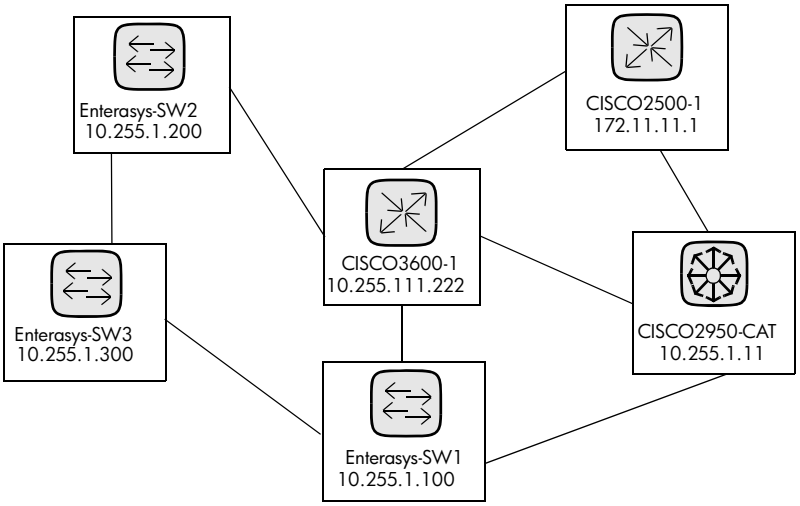
- 赤：デバイスは、スナップショットタスクまたは別のタスクのいずれかの結果として、最後のアクセスに失敗しました。(**注意**：VLAN とポートの場合、赤は VLAN が管理目的でダウンしていることを、グレーは VLAN が実行されていることを示します)。
- グレー：デバイスにスナップショットデータは含まれていません。
- 白：デバイスは動作中です。
- デバイスの境界：実線の境界はデバイスを示します。 点線の境界は仮想グループを示します。仮想グループでは、デバイス内の各 VLAN が、それ自体が所有するデバイスとして示されます。
- 点線：レイヤ 3 接続を表します。
- 実線：レイヤ 2 接続を表します。



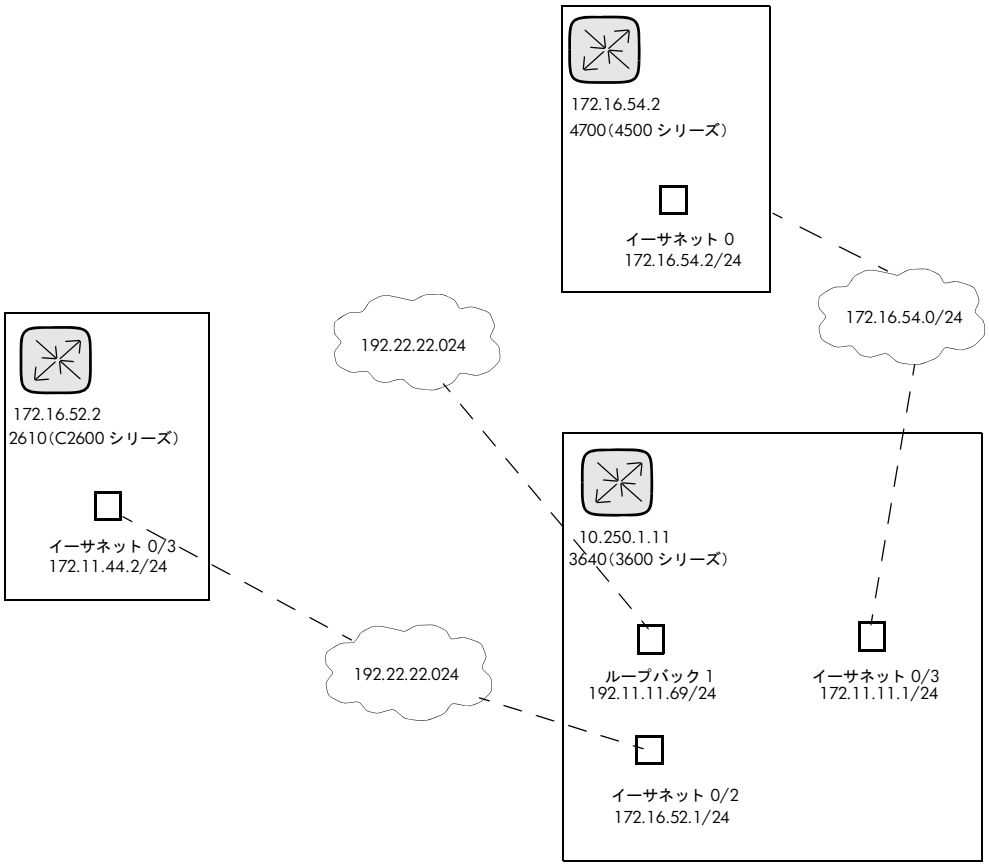
次の図に、VLAN とポートの間の接続を含む単純なネットワークダイアグラムを示します。



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。



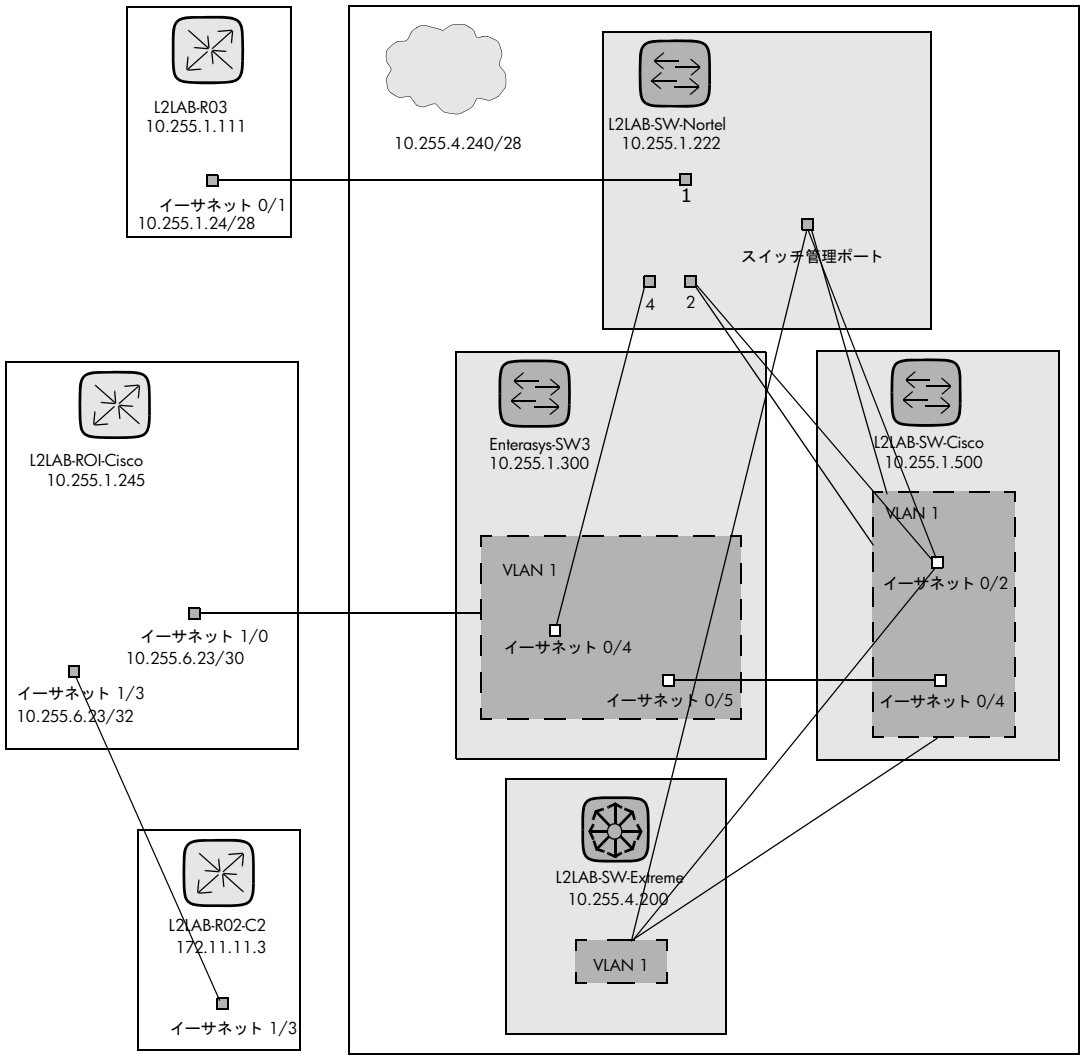
次のサンプル図に、同じサブネットを共有するデバイスを接続するための省略方法としてクラウド（雲形のイラスト）を使用した単純なネットワークダイアグラムを示します。クラウドは、ルータやスイッチなどのゲートウェイオブジェクトを論理的に表します。



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	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。 • レイヤ 1：ポート（推定） • レイヤ 2：ポート • レイヤ 3：ポート • レイヤ 3：ポート（拡張） • レイヤ 1：デバイス（推定） • レイヤ 2：デバイス • レイヤ 3：デバイス • レイヤ 3：デバイス（拡張） **注意**：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、「NA/SA 統合」（250 ページ）を参照してください。
出力書式	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。 • 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。（「表示メニューオプション」（257 ページ）を参照してください）。 • 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。 • 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。

フィールド	説明 / アクション
デバイス選択	次のオプションのいずれかを選択します。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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、「[ICMP テストの実行] タスクページのフィールド」（379 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の間で検出された IP アドレスすべてが示されます。 • 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。
階層レイヤフィルタ	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 （詳細は、「デバイスの追加」（133 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。例えば、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。 **注意**：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、「appserver.rcx ファイルの編集」（762 ページ）を参照してください。 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。 • コア • 分散 • アクセス • エッジ
詳細オプション	

フィールド	説明 / アクション
詳細フィルタ	次の中からオプションを 1 つ以上選択します。 • 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。 • 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。 • 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。 • 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。 • 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。（**注意**：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）。 • 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。
グループ化	次のオプションのいずれかまたは両方を選択します。 • 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。例えば、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。 • 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。（**注意**：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。）

注釈

フィールド	説明 / アクション
デバイスの注釈	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。 • ホスト名 • プライマリ IP • FQDN • デバイスの説明 • パーティション • モデル • ベンダー • シリアル番号 • 資産タグ • 最終変更日 • カスタムフィールド • 最終アクセスのステータス • 非アクティブのデバイスを表示 • ポリシー準拠のステータスを表示 • スタートアップとランニング構成の不一致を表示 • VTP 情報
終点の注釈	次の中からオプションを 1 つ以上選択します。 • インターフェイスの説明 • ポート名 • IP アドレス • ポートタイプ • ポートのステータス • 実行ポートステータス • MAC アドレス • 領域

フィールド	説明 / アクション
相互接続の注釈	次のオプションを 1 つ以上選択します。 • 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。 • VLAN：VLAN 情報を接続線にラベル付けします。
クラウドの注釈	次のオプションを選択します。 • 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）。 • 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。）
グラフの注釈	次のオプションを選択します。 • 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
ダイアグラムを指定した名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」（245 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 （詳細は、「[デバイスの新規作成] ページのフィールド」（134 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] の下のメニューバーで [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。「ソフトウェアレベルレポートのフィールド」（766 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。「新規ソフトウェアレベルの追加」（553 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。
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。 • 任意のレベル • セキュリティリスク • 実稼動前 • ブロンズ • シルバー
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。

フィールド	説明
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。 • 情報：一般的に対応を必要としないイベント。 • 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。 • 中：適時に応答を必要とするイベント（通常は 72 時間以内）。 • 高：緊急の対応を必要とするイベント（通常は 24 時間以内）。 • 重要：即時の対応を必要とするイベント。
コメント	脆弱性の説明を入力します。
アクション	次のアクションを選択できます。 • 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、「[デバイスソフトウェア履歴] ページのフィールド」（297 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」（536 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。「デバイスソフトウェアレポートのフィールド」（764 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。「新規ソフトウェアレベルの追加」（553 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。 • 情報：一般的に対応を必要としないイベント。 • 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。 • 中：適時に応答を必要とするイベント（通常は 72 時間以内）。 • 高：緊急の対応を必要とするイベント（通常は 24 時間以内）。 • 重要：即時の対応を必要とするイベント。

フィールド	説明
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。
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。 • 情報：一般的に対応を必要としないイベント。 • 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。 • 中：適時に応答を必要とするイベント（通常は 72 時間以内）。 • 高：緊急の対応を必要とするイベント（通常は 24 時間以内）。 • 重要：即時の対応を必要とするイベント。
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。 • 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、「[デバイスソフトウェア履歴] ページのフィールド」（297 ページ）を参照してください。

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」（28 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	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。 • 一括編集 • ポリシー準拠の確認 • パスワードの配布 • デバイスのリブート
ホスト名	デバイスのホスト名を表示します。
デバイス IP	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。

フィールド	説明 / アクション
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	重要度レベルを選択します。 • 情報：一般的に対応を必要としないイベント。 • 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。 • 中：適時に応答を必要とするイベント（通常は 72 時間以内）。 • 高：緊急の対応を必要とするイベント（通常は 24 時間以内）。 • 重要：即時の対応を必要とするイベント。
ルールの説明	ルールの説明を表示します。
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、Device Driver Reference（DRS）ドキュメントを参照してください。DRS は、新しく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] の下のメニューバーで [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。（**注意** : [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。（詳細は、「[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」（455 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。

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。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」（635 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：	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。 • 過去 1、2、4、8、12、24、および 48 時間 • 過去 1 および 2 週間 • 過去 1ヶ月 • 全イベント
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。

フィールド	説明 / アクション
サマリ	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、「イベントの説明」（635 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。 • イベントが発生した日付および時刻。 • 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。「[タスク情報] ページのフィールド」（499 ページ）を参照してください。 • イベントタイプ。 • イベントの簡単な説明。 • デバイスに関する詳細情報へのリンク。
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	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。 • 日付 • 追加ユーザ名 • サマリ • 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 • 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。 • デバイス
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。

フィールド	説明 / アクション
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] の下のメニューバーで [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] の下のメニューバーで [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	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。 • 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。 • 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。 • 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。 • 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。 • 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。
変更頻度	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。
1 日あたりの変更数	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。

レポート	報告される情報
統計グラフ	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。 • Syslog • Telnet/SSH • プロキシ • 通常または手動のポーリング • AAA • 構成またはスクリプトの配布 [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。
構成変更	過去の週について次の情報を表示します。 • 変更の原因と変更数を含む変更検出。 • 時間ごとの変更履歴。 • 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。
デバイスステータス	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。 • 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。 • 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。 • 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。

レポート	報告される情報
デバイスのインベントリ	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。 • ホスト名（[デバイス情報] ページより） • IP アドレス（[デバイス情報] ページより） • 資産タグ（[デバイス情報] ページより） • 場所（構成ファイルより） • ベンダー（構成ファイルより） • モデル（構成ファイルより） • 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） • シリアル番号（構成ファイルより） • デバイスの説明（[デバイス情報] ページより） • 最後のスナップショットの結果（タスクより） • 最後に変更された構成（タスクより）
オペレーティングシステム（OS）のインベントリ	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。 • 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。 • 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。 • 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。

レポート	報告される情報
システムステータス	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。 • 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。 • 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。 • 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。
ポリシー準拠	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。 • 準拠している構成ポリシー • 準拠していない構成ポリシー • 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の数を含む）

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] の下のメニューバーで [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」（465 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	「はじめに」（782 ページ）
インストールの前提条件	「インストールの前提条件」（783 ページ）
RSA Server Authentication Manager	「RSA Server Authentication Manager」（783 ページ）
ユーザ認証	「ユーザ認証」（783 ページ）
ネットワークデバイスへのアクセス	「ネットワークデバイスへのアクセス」（784 ページ）
SecurID トークンの追加	「SecurID ソフトウェアトークンの追加」（787 ページ）
SecurID を使用した NA へのログイン	「SecurID を使用したログイン」（788 ページ）
SecurID のトラブルシューティング	「SecurID のトラブルシューティング」（792 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 Telnet	はい 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、生成されるパスコ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 が使用されるときの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[自分のプロファイル]をクリックします。[自分のプロファイル] ページが開きます。[自分のプロファイル] ページのフィールドの詳細については、「[自分のプロファイル] ページのフィールド」（334 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」（787 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」（54 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] の下のメニューバーで、[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」（134 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生じ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」（169 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 [自分のプロファイル] をクリックします。[自分のプロファイル] ページが開きます。[自分のプロファイル] ページのフィールドの詳細については、「[自分のプロファイル] ページのフィールド」（334 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	ACEServer 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。（**注意**：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」（99 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 マネージメント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」（120 ページ）を参照してください。

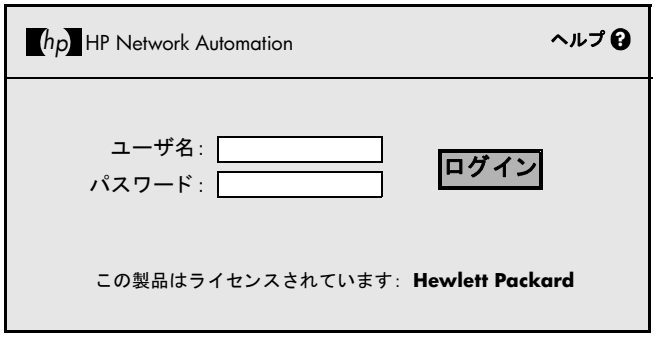
トークンが新規 PIN モードの場合は、SecurID を介して次の 2 つの方法で NA にログインできます。

- SecurID システム PIN を使用する
- 新規 SecurID PIN を使用する

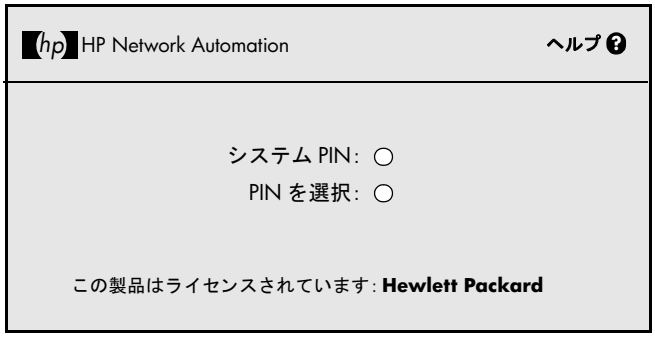
RSA のログイン手順では、すべての場合に、ユーザが新規 PIN で再認証する必要があります。

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。



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。



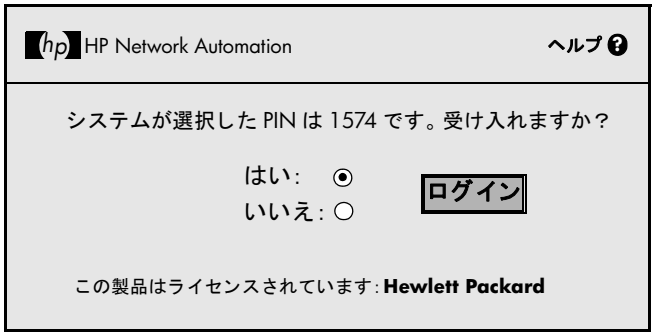
[システム PIN] をクリックする場合は、「ログイン方法 1 : システム PIN の使用」(790 ページ) を参照してください。[PIN を選択] をクリックする場合は、「ログイン方法 2 : 新しい PIN の使用」(791 ページ) を参照してください。

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。

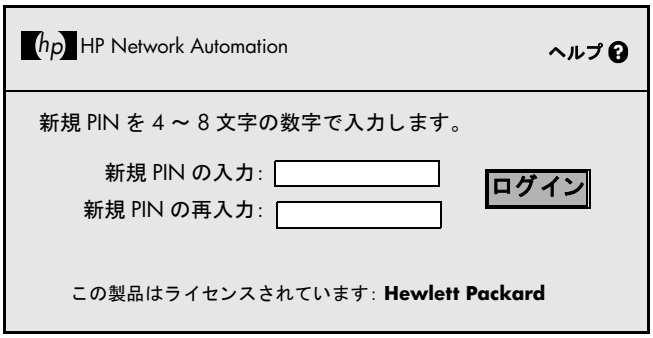
1. 460 ページに示される [システム PIN] をクリックします。SecurID からシステム PIN を獲得した後、次に示すように [はい] をクリックします。
2. [ログイン] をクリックします。
3. 待機して、次のトークンコードを使用してログインするよう指示するメッセージが表示されます。



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. 750 ページに示される [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] の下のメニューバーで [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。別の名前でファイルを保存する場合は、[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とロードノードシークレットユーティリティをエージェントホストにコピーします。ロードノードシークレットユーティリティは、新規ノードシークレットファイルをエージェントホストにロードします。RSA Security は、RSA Authentication Manager CD に、4 種類のプラットフォーム固有バージョン (Windows、Solaris、HP-UX、および IBM AIX）のユーティリティ（agent_nsload）を収録しています。
7. 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ます。コマンドラインプロンプトで、「`agent_nsload - path - 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	「はじめに」（797 ページ）
COBIT 準拠のステータスレポート	「COBIT 準拠のステータスレポート」（799 ページ）
COSO 準拠のステータスレポート	「COSO 準拠のステータスレポート」（810 ページ）
ITIL 準拠のステータスレポート	「ITIL 準拠のステータスレポート」（814 ページ）
GLBA 準拠のステータスレポート	「GLBA 準拠のステータスレポート」（819 ページ）
HIPAA 準拠のステータスレポート	「HIPAA 準拠のステータスレポート」（823 ページ）
Visa CISP 準拠のステータスレポート	「Visa CISP（PCI データセキュリティ標準）準拠の ステータスレポート」（832 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。

コンプライアンスセンターへのナビゲート

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な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 Visa CISP 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、「COBIT 準拠のステータスレポート」（799 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、「COSO 準拠のステータスレポート」（810 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、「ITIL 準拠のステータスレポート」（814 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、「GLBA 準拠のステータスレポート」（819 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、「HIPAA 準拠のステータスレポート」（823 ページ）を参照してください。
Visa CISP（PCI データセキュリティ標準）準拠のステータス	Visa CISP（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、「Visa CISP（PCI データセキュリティ標準）準拠の ステータスレポート」（832 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
モニタリング	
M1 プロセスのモニタリング	次の点についての数を表示します。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。
M2 内部統制の妥当性を評価	次の点についての数を表示します。 • 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。 • 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。 • 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。

フィールド	説明 / アクション
M3 第三者保証を取得	次の点についての数を表示します。 • 「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。 • 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。 • 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。 • 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。 • 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。
M4 独立監査に提供	次の点についての数を表示します。 • 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。 • 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。
提供とサポート	
DS1 サービスレベルの定義と管理	次の点についての数を表示します。 • 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。 • 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。 • 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。

フィールド	説明 / アクション
DS2 サードパーティのサービスの管理	次の点についての数を表示します。 • 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。 • 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。 • 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。
DS3 性能とキャパシティの管理	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。
DS4 継続的なサービスの保証	次の点についての数を表示します。 • 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。 • 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。
DS5 システムセキュリティの保証	次の点についての数を表示します。 • 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。 • 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、[全ユーザ] ページが開きます。 • 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リストページが開きます。 • 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。 • 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。 • 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。
DS6 費用の捕捉と配賦	次の点についての数を表示します。 • 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。 • 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。

フィールド	説明 / アクション
DS7 利用者の教育と研修	次の文書へのリンクがあります。 • *HP 7.60 Network Automation ユーザガイド* • *HP 7.60 Network Automation リリースノート*
DS8 顧客への支援と助言	次の項目へのリンクがあります。 • ドライバ更新パッケージのダウンロード • 最新のリリースノートを表示 • ライセンス情報を表示 • 技術サポートチケットを作成 • 顧客サポートに連絡
DS9 構成管理	次の点についての数を表示します。 • 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。 • 格納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。 • 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。 • 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。 • 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。
DS10 問題管理とインシデント管理	次の点についての数を表示します。 • 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。 • 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。
DS11 データ管理	保存されたデバイスの構成の数を表示します。

フィールド	説明 / アクション
DS12 物理的環境の管理	次の点についての数を表示します。 • 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。 • 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。
DS13 オペレーション管理	次の点についての数を表示します。 • 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。 • 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。 • 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。 • 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。 • 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。
計画と組織	
PO1 IT 戦略計画の策定	次の点についての数を表示します。 • 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。 • 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。 • 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。

フィールド	説明 / アクション
PO2 情報アーキテクチャの定義	次の点についての数を表示します。 • 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。 • 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。 • 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。
PO3 技術指針の決定	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。
PO4 IT プロセスと組織及びそのかかわりの定義	次の点についての数を表示します。 • 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。 • 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。 • 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リストページが開きます。
PO5 IT 投資の管理	次の点についての数を表示します。 • 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。 • 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。 • 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。
PO6 マネジメントの意図と指針の周知	次の点についての数を表示します。 • 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。 • 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。

フィールド	説明 / アクション
PO7 人材の管理	次の点についての数を表示します。 • 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。 • 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。 • 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。
PO8 外部要件との準拠の管理	アクティブな構成ポリシーの数を表示します。[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。[コンプライアンスセンター] 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。
PO9 リスクの評価	次の点についての数を表示します。 • 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。 • 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。 • 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。
PO10 プロジェクトの管理	次の点についての数を表示します。 • 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。 • 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。 • 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。 • 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。

フィールド	説明 / アクション
PO11 品質管理	次の点についての数を表示します。 • 「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。 • 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。 • 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。 • 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。 • 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。
調達と導入	
AI1 自動ソリューションを特定	次のデフォルトのリンクがあります。 • 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。 • 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。 • 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。 • 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。
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。

フィールド	説明 / アクション
AI3 技術インフラストラクチャの調達と保守	次の点についての数を表示します。 • 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。 • 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。 • 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。
AI4 手順を作成して保守	次の点についての数を表示します。 • 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。 • 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。
AI5 システムのインストールと認可	次の点についての数を表示します。 •「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。 • 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。 • 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。

フィールド	説明 / アクション
AI6 変更管理	次の点についての数を表示します。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。

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	次の点についての数を表示します。 • 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。 • 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。 • 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リストページが開きます。 • 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。 • 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。 • 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。 • 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。
リスク評価	次の点についての数を表示します。 • 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。 • 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。 • 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。

フィールド	説明 / アクション
統制活動	次の点についての数を表示します。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。
情報と伝達	次の点についての数を表示します。 • 過去 24 時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。 • 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。 • 1 日あたりの平均変更数（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。 • 1 日あたりの平均変更数（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。

フィールド	説明 / アクション
モニタリング	次の点についての数を表示します。 • 「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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。

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：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
構成管理	
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。 • 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。 • 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。
インシデント管理	

フィールド	説明 / アクション
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。 • 過去 24 時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。 • 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。
問題管理	
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。 • 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。 • 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。
変更管理	
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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。

フィールド	説明 / アクション
サービスデスク	
サービスサポート機能	次の点についての数を表示します。 • 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。 • 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。
リリース管理	
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。 • 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。 • 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。 • 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。
サービスレベル管理	
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。 • 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。 • 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。 • 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。
キャパシティ管理	
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。
IT サービス継続性管理	

フィールド	説明 / アクション
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。 • 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。 • 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。
可用性管理	
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。 • 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。 • 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。
IT サービス財務管理	
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。 •「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。 • 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。 • 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。
セキュリティ管理	

フィールド	説明 / アクション
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。 • 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。 • 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。 • 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リストページが開きます。 • 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。 • 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。 • 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。

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
整合性ガイドラインセクション	
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。 • インベントリ内のデバイス。 • インベントリ内のモジュール。 • 保存されたデバイスの構成。
II.B. 目的	次の点についての数を表示します。 • 特定のデバイスグループに制限されたユーザ。 • 管理者権限が割り当てられたユーザ。 • 過去 7 日間に失敗したユーザログイン試行。 • 承認保留中の変更。 • 過去 7 日間に承認された変更。 • 過去 7 日間に承認されなかった変更。 • 特定された ACL。 • 使用中の ACL。 • 過去 7 日間の ACL の変更。
III.A. 役員会を含む	次の点についての数を表示します。 • 使用可能なユーザレポート。 • 使用可能なシステムレポート。
III.B. リスクを評価	次の点についての数を表示します。 • 緑のステータスの構成管理「ベストプラクティス」。 • デバイスソフトウェアレベル。 •「OK」ステータスを示す監視。 • アクセスエラーがあるデバイス。 • 利用できるポートが 10% 未満のデバイス。 • スタートアップとランニング構成が異なるデバイス。

フィールド	説明 / アクション
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。 • 適用されているワークフロールール。 • 適用されている構成ポリシー。 • 適用されているデバイスパスワードルール。
III.C.2. リスクを管理して制御（トレーニング）	次の HP 文書にアクセスできます。 • *HP 7.60 Network Automation ユーザガイド* • *HP 7.60 Network Automation リリースノート*
III.C.3. リスクを管理して制御（テスト中）	次の点についての数を表示します。 • 過去 24 時間の構成ポリシーに非準拠のイベント。 • 過去 7 日間の構成ポリシーに非準拠のイベント。 • ソフトウェアレベルにないデバイス。 • 過去の 24 時間の診断実行。 • 過去の 7 日間の診断実行。
III.D. サービスプロバイダ協定を監視	次の点についての数を表示します。 • 格納された構成。 • スタートアップとランニング構成が異なるデバイス。 • アクティブでないデバイス。 • アクセスエラーがあるデバイス。
III.E. プログラムを調整	次の点についての数を表示します。 • 先月に追加されたユーザ。 • 先月に追加されたデバイス。 • 先月に追加されたデバイスグループ。 • 先月に格納された構成。

フィールド	説明 / アクション
III.F. 役員会にレポート	次の要素を表示します。 • 緑のステータスの構成管理「ベストプラクティス」の個数。 • システムステータスレポート。 • サマリレポート。 • HP Network Automation コンプライアンスセンター。
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
セキュリティ標準：一般ルール	
（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。 • 保存されたデバイスの構成。 • アクセスエラーがあるデバイス。 • 利用できるポートが 10% 未満のデバイス。
（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。 • 過去 7 日間に失敗したユーザログイン試行。 • 特定された ACL。 • 使用中の ACL。 • 過去 7 日間の ACL の変更。

フィールド	説明 / アクション
（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。 • 特定のデバイス群に制限されたユーザ。 • 管理者アクセス権限が割り当てられたユーザ。
（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。
管理上の保護手段	
（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。	次の点についての数を表示します。 • 緑のステータスの構成管理「ベストプラクティス」。 • ソフトウェアレベルのデバイス。 •「OK」ステータスを示す監視。 • アクセスエラーがあるデバイス。 • 利用できるポートが 10% 未満のデバイス。 • 検出されたソフトウェアの脆弱性。 • スタートアップとランニング構成が異なるデバイス。
（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。	次の点についての数を表示します。 • 適用されているワークフロールール。 • アクティブな構成ポリシー。 • 適用されているデバイスパスワードルール。
（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。	この要件は NA の対象範囲外です。

フィールド	説明 / アクション
(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。	次の点についての数を表示します。 • 過去 7 日間のユーザログイン試行。 • 過去 7 日間で追加されたユーザ。 • 過去 7 日間に削除されたユーザ。 • 過去 7 日間に変更されたユーザ権限。 • 過去 7 日間に変更された構成ポリシー。 • 過去 7 日間に追加された構成ポリシー。
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。	この要件は NA の対象範囲外です。
従業員のセキュリティ	
(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。	次の点についての数を表示します。 • 特定のデバイス群に制限されたユーザ。 • 過去 7 日間に承認された変更。 • 過去 7 日間に承認されなかった変更。
(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。	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。
(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。	過去 7 日間に削除されたユーザ数を表示します。
情報アクセス管理	

フィールド	説明 / アクション
(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。	次の点についての数を表示します。 • 特定のデバイスグループに制限されたユーザ。 • 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。
(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。例えば、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。	次の点についての数を表示します。 • 特定のデバイスグループに制限されたユーザ。 • 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。
(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。	次の点についての数を表示します。 • HP Network Automation で有効にされたユーザアカウント。 • HP Network Automation で無効にされたユーザアカウント。
セキュリティ意識とトレーニング	
(A) セキュリティ通知（推奨）。定期的なセキュリティ更新。	次の点についての数を表示します。 • HP Network Automation で有効にされたユーザアカウント • HP Network Automation で無効にされたユーザアカウント。
(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。	この要件は NA の対象範囲外です。
(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。	次の点についての数を表示します。 • 過去 7 日間のユーザログイン試行。 • 過去 7 日間に失敗したユーザログイン試行。

フィールド	説明 / アクション
(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。	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。
セキュリティインシデントの手順	
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。	次の点についての数を表示します。 • 過去 7 日間のユーザログイン試行。 • 過去 7 日間に失敗したユーザログイン試行。 • 過去 7 日間に検出された構成変更。
緊急時対応計画	
(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。	NA は、電子保護医療情報の作成や維持は行いません。
(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）。	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。
(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）。	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。
(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。	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。
(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。	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。

フィールド	説明 / アクション
評価	
定期的な技術的評価と非技術的評価を実行します。	次の点についての数を表示します。 • 特定のデバイス群に制限されたユーザ。 • 管理者アクセス権限を割り当てられたユーザ。 • 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。 • 適用されている構成ポリシー。 • 適用されているデバイスパスワードルール。
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。	この要件は NA の対象範囲外です。
物理的な保護手段	
(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）。	この要件は NA の対象範囲外です。
(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。	この要件は NA の対象範囲外です。
(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。例えば、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。	次の点についての数を表示します。 • 過去 7 日間のユーザログイン試行。 • 過去 7 日間に失敗したユーザログイン試行。 • 特定のデバイスグループに制限されたユーザ。 • 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。

フィールド	説明 / アクション
（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（例えば、ハードウェア、壁、ドア、鍵などです）。	この要件は NA の対象範囲外です。
ワークステーションの使用	
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。	この要件は NA の対象範囲外です。
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。	この要件は NA の対象範囲外です。
デバイスとメディアの制御	
（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。	この要件は NA の対象範囲外です。
（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。	この要件は NA の対象範囲外です。
（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。	この要件は NA の対象範囲外です。
（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。	この要件は NA の対象範囲外です。
技術的な保護手段	

フィールド	説明 / アクション
(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。	次の点についての数を表示します。 • HP Network Automation で有効にされたユーザアカウント。 • HP Network Automation で無効にされたユーザアカウント。
(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）。	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。
(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に電子セッションを終了する手順を実施します。	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に終了しました。デフォルト値は 1800 です。この値は設定できます。
(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。	この要件は NA の対象範囲外です。
監査の制御	
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。	この要件は NA の対象範囲外です。
標準の整合性	
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。	この要件は NA の対象範囲外です。
個人または団体の認証	

フィールド	説明 / アクション
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。	この要件は NA の対象範囲外です。
送信セキュリティ	
(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。	この要件は NA の対象範囲外です。
(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。	この要件は NA の対象範囲外です。
ポリシーと手順	
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。	この要件は NA の対象範囲外です。
ドキュメント	
(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。	この要件は NA の対象範囲外です。
(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。	この要件は NA の対象範囲外です。
(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。	この要件は NA の対象範囲外です。

Visa CISP（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。

Visa CISP の詳細については、[Visa CISP（データセキュリティ標準）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参照してください。

Visa CISP 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. [Visa CISP 準拠のステータス] リンクをクリックします。[Visa CISP 準拠のステータス] ページが開きます。

Visa CISP（PCI データセキュリティ標準）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
安全なネットワークの構築と保守	
1.1: 以下のようなファイアウォール構成標準を確立します。 • すべての外部ネットワーク接続とファイアファイアウォール構成に対する変更を承認し、テストするための正式なプロセス。 • カード所有者データに対するすべての接続が記載された現在のネットワークダイアグラム。 • 各インターネット接続、および DMZ とイントラネット間にあるファイアウォールの要件。 • ネットワークコンポーネントを論理的に管理するためのグループ、ロール、職務の説明。 • 業務に必要なサービス / ポートの文書リスト。 • HTTP、SSL、SSH、VPN の他に使用できるプロトコルに関する理由付けと文書化。 • 危険性のあるプロトコルを許可する場合の理由付けと文書化。 • ファイアウォール / ルータのルール設定を定期的に確認。 • ルータの構成標準。	次の点についての数を表示します。 • 配布されたデバイス（ルータ / ファイアウォール）。 • 保存されたデバイスの構成。 • 過去 7 日間のファイアウォールの構成変更。 • 適用されている構成ポリシー。 • 過去 7 日間の NSA ルータセキュリティベストプラクティスポリシー違反。 • 過去 7 日間に承認されたファイアウォール変更。 • 過去 7 日間に承認されなかったファイアウォール変更。

フィールド	説明 / アクション
1.2: untrusted のネットワーク / ホストから送信されるすべてのトラフィックを拒否するようにファイアウォール構成を構築します : • Web プロトコル - HTTP（ポート 80）とセキュアソケットレイヤ（SSL）（通常はポート 443）。 • システム管理プロトコル。 • ビジネスで必要とされるその他のプロトコル。	次の点についての数を表示します。 • 構成ポリシーに非準拠のファイアウォール。 • 過去 7 日間のファイアウォールの構成に非準拠のイベント。

フィールド	説明 / アクション
1.3: パブリックアクセスが可能なサーバと、カード所有者データを格納している任意のシステムコンポーネントとの接続（ワイヤレスネットワークからの接続も含む）を制限するようファイアウォール構成を構築します。このファイアウォール構成には以下が含まれます： 次の制限があります。 • DMZ 内の IP アドレスへの受信インターネットトラフィックを制限（入り口フィルタ）。 • ポート 80 と 443 経由の送受信のインターネットトラフィックを制限。 • 内部アドレスによるインターネットから DMZ へのトラフィックを禁止（出口フィルタ）。 • 内部ネットワークゾーンにデータベースを配置。 • 決済カード環境からの送信トラフィックを業務上必要なレベルに制限。 • ルータの構成ファイルの保護と同期化。 • 具体的に許可されていないその他の送受信トラフィックを拒否。 • ワイヤレスネットワークと決済カード環境間に境界ファイアウォールをインストール。 • 組織のネットワークへのアクセスに使用されている、インターネットに直接接続可能なモバイル機器や従業員が所有するコンピュータ（従業員が使用しているノート PC など）に、個人のファイアウォールソフトウェアをインストール。	次の点についての数を表示します。 • 構成ポリシーに非準拠のファイアウォール。 • 過去 7 日間のファイアウォールの構成に非準拠のイベント。 • 配布されたファイアウォール。

フィールド	説明 / アクション
1.4: 外部ネットワークと、カード所有者情報を格納するシステムコンポーネントとの間の直接的なパブリックアクセスを次のように禁止します。 • DMZ を実装することで、すべてのトラフィックをフィルタ処理して選別し、送受信のインターネットトラフィックを直接ルーティングすることを禁止します。 • 決済カードアプリケーションからの DMZ 内の IP アドレスに対する送信トラフィックを制限します。	次の点についての数を表示します。 • 構成ポリシーに非準拠のファイアウォール。 • 過去 7 日間のファイアウォールの構成に非準拠のイベント。 • 配布されたファイアウォール。
1.5: インターネットプロトコル（IP）のマスカレード処理を実装して、内部アドレスが変換され、インターネット上に公開されることを防ぎます。	次の点についての数を表示します。 • 構成ポリシーに非準拠のファイアウォール。 • 過去 7 日間のファイアウォールの構成に非準拠のイベント。 • 配布されたファイアウォール。
2.1: 常にベンダー出荷時のデフォルト値を変更してから、ネットワークにシステムを組み込みます。ワイヤレス環境の場合、常にワイヤレスベンダーのデフォルト値を変更します。	次の点についての数を表示します。 • 適用されているデバイスパスワードルール。 • 過去 7 日間のパスワード変更。 • 過去 7 日間のデバイスパスワード変更エラー。
2.2: 次の点について、すべてのシステムコンポーネントの構成標準を作成します。 • 1 つのサーバにつき、1 つの主要機能のみを実装します。 • すべての不要で保護されていないサービスやプロトコルを無効にします。 • システムセキュリティパラメータを設定して、誤使用を防ぎます。 • スクリプト、ドライバ、機能、サブシステム、ファイルシステムなど、すべての不要な機能を削除します。	次の点についての数を表示します。 • 構成ポリシーに非準拠のデバイス。 • 過去 7 日間の構成ポリシーに非準拠のイベント。 • 適用されている構成ポリシー。 • 過去 7 日間に追加された構成ポリシーのルール。 • 過去 7 日間に変更された構成ポリシーのルール。
2.3: 非コンソール管理アクセスを暗号化します。	SSH または SCP を使用するように構成されたデバイスの数を表示します。

フィールド	説明 / アクション
カード所有者データの保護	
4.1: 強力な暗号法と暗号化技術を使用します。ワイヤレスネットワークでカード所有者データを送信する場合、Wi-Fi Protected Access（WPA）技術が使用できる場合は使用して送信を暗号化します。または VPN や 128 ビットの SSL を使用します。	次の点についての数を表示します。 • 構成ポリシーに非準拠のデバイス。 • 過去 7 日間の構成ポリシーに非準拠のイベント。 • 過去 7 日間の NSA ルータセキュリティベストプラクティスポリシー違反。 • 適用されている構成ポリシー。
4.2: 暗号化されていない電子メールではカード所有者情報を送信しないでください。	この要件は NA の対象範囲外です。
脆弱性管理プログラムの保守	
6.1: すべてのシステムコンポーネントとソフトウェアに、ベンダーから提供される最新のセキュリティパッチを適用し、関連するセキュリティパッチをリリース後の 1 ヶ月以内にインストールします。	次の点についての数を表示します。 • 過去 7 日間に成功したソフトウェア更新。 • 過去 7 日間に失敗したソフトウェア更新。
6.2: 新たに発見されたセキュリティ上の脆弱性を識別する処理を確立します。	次の点についての数を表示します。 • ソフトウェア準拠状態でないデバイスの数。 • 過去 7 日間に検出されたソフトウェアの脆弱性。

フィールド	説明 / アクション
6.3: 業界のベストプラクティスに基づいてソフトウェアアプリケーションを開発し、ソフトウェア開発のライフサイクル全体で情報セキュリティに取り組みます。以下の点が含まれます。 • 配布する前に、すべてのセキュリティパッチと、システムおよびソフトウェアの構成の変更をテスト • 開発 / テスト環境と運用環境を分離 • 運用データ（実際のクレジットカード番号）は、テストや開発時には使用しない • 運用システムをアクティブにする前に、テストデータおよびアカウントを削除 • カスタムコードを実運用またはユーザにリリースする前に確認し、コードに脆弱性があるかどうかを特定	NA には、システムに入力した構成データを配布する前にポリシーに照らしてテストし、ポリシーに非準拠のデータを特定する機能があります。
6.4: すべてのシステムとソフトウェアの構成の変更では、次の変更の制御手順に従います。 • 影響の文書化 • 適切な業務管理者による承認 • 運用機能を検証するテスト • 回復手順	次の点についての数を表示します。 • 特定のデバイス群に制限されたユーザ。管理者アクセス権限を割り当てられたユーザ。 • 適用されているワークフロールール。 • 過去 7 日間に承認された変更。 • 過去 7 日間に承認されなかった変更。 • 保存されたデバイスの構成。 • 過去 7 日間に格納されたデバイスの構成。

フィールド	説明 / アクション
6.5: 次に示す安全なコーディングガイドラインに基づいて、Web ソフトウェアとアプリケーションを開発します。 • 未検証の入力 • 破綻したアクセス制御 • 破綻した認証 / セッション管理 • クロスサイトスクリプティング（XSS）攻撃 • バッファオーバーフロー • インジェクションフロー • 不適切なエラー処理 • 保護されていないストレージ • サービス拒否攻撃 • 保護されていない構成管理	HP では、業界で認められているソフトウェア設計原則とコーディング方法を使用しています。また、内部のエンジニアリングポリシーでは、安全で高品質なコードを書くことに重点を置いています。 さらに、セキュリティに関するさまざまな掲示板やアラートを監視し、メーリングリストに参加し、定期的にコードの安全を確認しています。これによって、脆弱性が特定され、対処することができます。
強固なアクセス制御手法の導入	
7.1: コンピュータリソースやカード所有者情報に対するアクセスを、このようなアクセスを業務上必要とするユーザに限定します。	次の点についての数を表示します。 • 過去 7 日間のユーザログイン試行。 • 過去 7 日間で追加されたユーザ。 • 過去 7 日間に削除されたユーザ。 • 過去 7 日間に変更されたユーザ権限。
7.2: 複数のユーザーを持つシステムについては、ユーザーの業務要件に基づいてアクセスを制限し、個別に許可されないかぎり“すべて拒否”に設定されたメカニズムを確立します。	次の点についての数を表示します。 • 特定のデバイス群に制限されたユーザ。 • 管理者アクセス権限を割り当てられたユーザ。
8.1: システムコンポーネントまたはカード所有者データにアクセスを許可する前に、固有のユーザ名ですべてのユーザを識別します。	次の点についての数を表示します。 • NA で有効にされたユーザアカウント。 • NA で無効にされたユーザアカウント。

フィールド	説明 / アクション
8.2 固有の ID とは別に、少なくとも以下の方法のいずれか 1 つを使用して、すべてのユーザを認証します。 • パスワード • トークンデバイス • バイオメトリクス	次の点についての数を表示します。 • 過去 7 日間のパスワード変更。 • 外部認証は Active Directory によって有効化されます
8.3: 従業員、管理者、サードパーティがネットワークにリモートアクセスするために、2 要素認証を実装します。	Active Directory によって有効にされた外部認証の数を表示します。
8.4: すべてのシステムコンポーネントについて、送信と格納時にすべてのパスワードを暗号化します。	NA のパスワードは、ログイン時にキー入力するとき、ディスクに暗号化するとき、および送信中には非表示になります。

フィールド	説明 / アクション
8.5: すべてのシステムコンポーネントについて、非消費者ユーザと管理者の適切なユーザ認証とパスワード管理を徹底します。 • ユーザ ID、資格情報、その他の識別子オブジェクトの追加、削除、変更を制御します。 • パスワードのリセットを実行する前にユーザ ID を検証します。 • 初回のパスワードはユーザごとに固有な値を設定し、初回使用後は直ちに変更します。 • 少なくとも 90 日ごとに、非アクティブなユーザアカウントを削除します。 • リモート保守にベンダーが使用するアカウントは、必要な期間のみ有効にします。 • カード所有者データにアクセス権を持つすべてのユーザに対して、パスワードの手順とポリシーを配布します。 • グループ、共有、汎用のアカウント / パスワードを使用しないでください。 • ユーザパスワードは最低でも 90 日間ごとに変更してください。 • パスワードは 7 文字以上にする必要があります。 • 数字と英字の両方を含むパスワードを使用します。 • パスワードの入力を誤って 6 回繰り返しアクセスした場合、ユーザ ID はロックされます。 • ロックアウト継続時間は 30 分間に設定するか、または管理者がそのユーザ ID を有効にするまで継続します。 • カード所有者の情報が格納されているデータベースに対するすべてのアクセスを認証します。	次の点についての数を表示します。 • 過去 7 日間のユーザログイン試行。 • 過去 7 日間に失敗したユーザログイン試行。 • 過去 7 日間のパスワード変更。 • NA で有効にされたユーザアカウント。 • NA で無効にされたユーザアカウント。

フィールド	説明 / アクション
定期的なネットワークの監視とテスト	
10.1: システムコンポーネントに対するすべてのアクセスを関連付ける処理を確立します。	次の点についての数を表示します。 • NA で有効にされたユーザアカウント。 • NA で無効にされたユーザアカウント。
10.2: 以下のイベントを再構築するために自動監査証跡を実装します。 • カード所有者データに対する全個人ユーザアクセス。 • root 権限または管理者権限を持つ任意の個人の全操作。 • 全監査証跡に対するアクセス。 • 無効な論理アクセス試行。 • 識別メカニズムと認証メカニズムの使用。 • 監査ログの初期化。 • システムレベルオブジェクトの作成と削除。	次の点についての数を表示します。 • 無効にされたユーザ操作の監査ログ。 • 過去 7 日間に失敗したユーザログイン試行。 • 有効ではない外部認証。 • 過去 7 日間で追加されたユーザ。 • 過去 7 日間に削除されたユーザ。 • 過去 7 日間に追加されたデバイス。 • 過去 7 日間に削除されたデバイス。 • 過去 7 日間のデバイスの構成変更。
10.3: 各イベントについて、少なくとも以下の監査証跡エントリを記録します。 • ユーザ ID • イベントのタイプ • 日付と時刻 • 成功または失敗の表示 • イベントの起点 • 影響を受けるデータ、システムコンポーネント、またはリソースの ID または名前	次の点についての数を表示します。 • 過去 7 日間のユーザログイン試行。 • 過去 7 日間に失敗したユーザログイン試行。
10.4: すべての重要なシステムクロックと時間を同期します。	NTP で構成されたデバイスの数を表示します。

フィールド	説明 / アクション
10.5: 以下のように、監査証跡を変更できないように保護します。 • 監査証跡の表示を、ジョブ関連のニーズのあるユーザに制限します。 • 監査証跡ファイルが権限のないユーザによって変更されないように保護します。 • 変更作業が困難な中央管理のログサーバまたはメディアに監査証跡ファイルを直ちにバックアップします。 • ワイヤレスネットワークのログを内部 LAN のログサーバにコピーします。 • ファイルの整合性の監視 / 変更の検出ソフトウェアをログに使用して、既存のログデータを変更するときに必ず警告が生成されるようにします。	次の点についての数を表示します。 • セッションを削除できるユーザ。 • システムイベントを削除できるユーザ。
10.6: すべてのシステムコンポーネントのログを 1 日に 1 回以上確認します。	ログファイルが保存される日数を表示します。
10.7: 効率性と法的規制を考慮して、監査証跡の履歴を保持する期間を設定します。	保存された次の点についての数を表示します。 • 構成 • 診断： • イベント • タスク • セッション • ログファイル
11.1: セキュリティの制御、制限、ネットワーク接続、制約をテストします。	次の点についての数を表示します。 • 全 ACL。 • 使用中の ACL。 • 過去 7 日間の ACL の変更。
11.2: 内部ネットワークと外部ネットワークの脆弱性スキャンを実行します。頻度は四半期に 1 回以上、および重大なネットワークの変更があった後です。	この要件は NA の対象範囲外です。

フィールド	説明 / アクション
11.3: ネットワークのインフラストラクチャとアプリケーションに対する侵入テストを実行します。頻度は年に 1 回以上、およびインフラストラクチャやアプリケーションに重大なアップグレードまたは変更があった後です。	次の点についての数を表示します。 • 構成ポリシーに非準拠のデバイス。 • 過去 7 日間の構成ポリシーに非準拠のイベント。 • デバイスソフトウェアレベル。 • 過去 7 日間に検出されたソフトウェアの脆弱性。 • 適用されているイベント通知とレスポンスルール。
11.4: ネットワーク侵入検出システム、ホストベースの侵入検出システム、侵入防止システムのすべてまたはいずれかを使用して、すべてのネットワークトラフィックを監視し、侵入が疑われる場合はユーザに警告します。	NA は、IDS（侵入検出システム）と IPS（侵入防止システム）の各モジュールを使用してデバイスを安全に中央管理できます。
11.5: ファイルの整合性監視を配置して、1 日に 1 回以上（処理を自動化できる場合はより頻繁に）、重要なシステムやコンテンツファイルの不正な変更をユーザに通知し、重要ファイルの比較を実行します。	次の点についての数を表示します。 • 過去 7 日間のデバイスの構成変更。 • 過去 7 日間の構成ポリシーに非準拠のイベント。 • 構成ポリシーに非準拠のデバイス。 • 過去 7 日間に成功したソフトウェア更新。 • 過去 7 日間に失敗したソフトウェア更新。 • 過去 7 日間に検出されたソフトウェアの脆弱性。 • デバイスソフトウェアレベル。

情報セキュリティポリシーの保守

フィールド	説明 / アクション
12.2: 日常的な運用上のセキュリティ手順を開発します。	次の点についての数を表示します。 • 特定のデバイス群に制限されたユーザ。 • 管理者アクセス権限を割り当てられたユーザ。 • 過去 7 日間で追加されたユーザ。 • 過去 7 日間に削除されたユーザ。 • 過去 7 日間に変更されたユーザ権限。 • 保存された構成、保存された診断、保存されたイベント、保存されたタスク、保存されたセッション、および保存されたログファイル。
12.5: 個人やチームに以下の情報セキュリティ管理の職務を割り当てます。 • セキュリティポリシーとその手順を確立し、文書化し、配布します。 • セキュリティアラートとセキュリティ情報を監視して解析し、適切な担当者に配布します。 • 適時かつ効率的にあらゆる状況を処理できるように、セキュリティインシデントへの対応と上申の手順を確立し、文書化し、配布します。 • 追加、削除、変更など、ユーザアカウントを管理します。 • データに対するすべてのアクセスを監視し、制御します。	次の点についての数を表示します。 • 適用されている構成ポリシー。 • 適用されているイベント通知とレスポンスルール。 • 「OK」ステータスを示す監視。 • 緑のステータスの構成管理ベストプラクティス。 • NA で有効にされたユーザアカウント。 • NA で無効にされたユーザアカウント。 • 特定のデバイス群に制限されたユーザ。 • 管理者アクセス権限を割り当てられたユーザ。 • 過去 7 日間で追加されたユーザ。 • 過去 7 日間に削除されたユーザ。 • 過去 7 日間に変更されたユーザ権限。 • 過去 7 日間のユーザログイン試行。 • 過去 7 日間に失敗したユーザログイン試行。

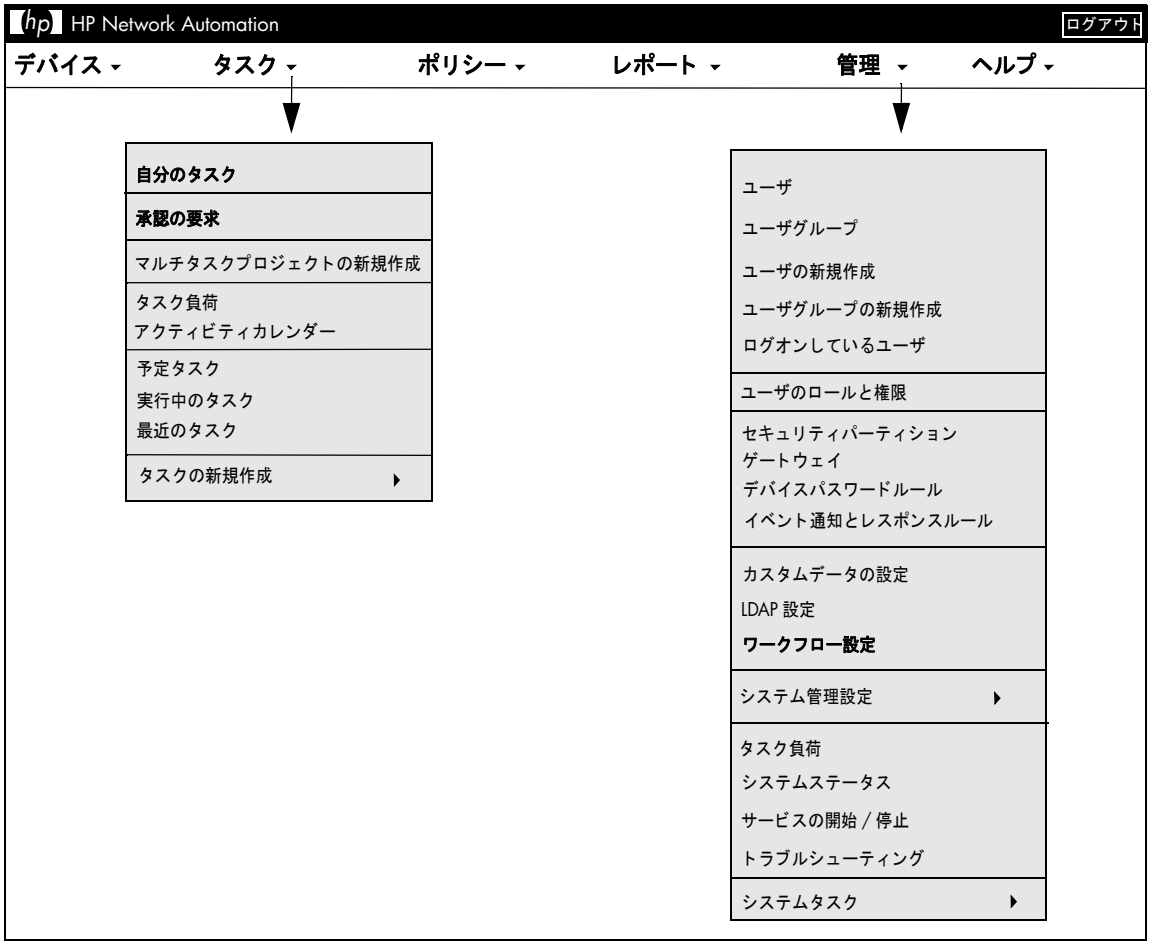
フィールド	説明 / アクション
12.9: 次のようにインシデント対応計画を実施します。 • インシデント対応計画を作成し、システム侵入が発生した場合に使用します。 • インシデント対応計画は 1 年に 1 回以上テストします。 • 警告に毎日 24 時間対応できるように、担当者を割り当てます。 • セキュリティ侵入に対応する職務を持つスタッフに、適切なトレーニングを提供します。 • 侵入検出システム、侵入防止システム、ファイルの整合性監視システムによる警告を含みます。 • インシデント対応計画を修正し発展させるプロセスを作成します。	次の点についての数を表示します。 • 過去 7 日間のデバイスの構成変更。 • 過去 7 日間の構成ポリシーに非準拠のイベント。 • 過去 7 日間に成功したソフトウェア更新。 • 過去 7 日間に失敗したソフトウェア更新。

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	「はじめに」（849 ページ）
ワークフローウィザード	「ワークフローウィザード」（850 ページ）
自分のタスク	「自分のタスク」（853 ページ）
承認の要求	「承認の要求」（857 ページ）
タスクの承認	「タスクの承認」（860 ページ）
電子メール通知	「電子メール通知」（863 ページ）

ワークフローへのナビゲート



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

  タスクの全リストは、「タスクとは」（354 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」（850 ページ）を参照してください。例えば、「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] の下のメニューバーで [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	説明 / アクション
手順 3：承認ルールを管理	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。（**注意**：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。） **注意**：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、「デバイスとユーザのセグメント化」（188 ページ）を参照してください。
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 6：デバイスグループの設定	[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。 • 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。 • 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。

手順	説明 / アクション
手順 7：承認者の設定	[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。
手順 8：FYI 受信者の設定	[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、「電子メール通知」（863 ページ）を参照してください。
設定完了	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、「自分のタスク」（853 ページ）を参照してください。

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	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。 • 未承認 • 承認を待機中 • 実行待ち 詳細については、「承認の要求」（857 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、「[予定タスク] ページのフィールド」（491 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、「[実行中のタスク] ページのフィールド」（494 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、「[最近のタスク] ページのフィールド」（496 ページ）を参照してください。

フィールド	説明 / アクション
タスクの表示のチェックボックス	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。 • 承認済み • 未承認 • 承認を待機中 • 無効化 • ドラフト • 承認は不要
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。
スケジュール日時	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、「タスクとは」（354 ページ）を参照してください。
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。タスクは、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。（**注意**：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	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。 • 承認を待機中 • 承認済み • 未承認 • 無効化 • 承認は不要

フィールド	説明 / アクション
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。 • 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。 • 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。 • 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。 • 失敗：タスクは失敗しました。 • 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。 • 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。 • 実行中：タスクは開始しましたが、まだ終了していません。 • スキップ：タスクはエラー（例えば、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。 • 成功：タスクは成功しました。 • 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。
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、「タスクの予定」（355 ページ）を参照してください。
タスクタイプ	次のようなタスクタイプを表示します。 • パスワードの配布 • 構成を配布 • ドライバの検出 • デバイスのリブート • スナップショットの取得 • スタートアップとランニングの同期 タスクの全リストは、「タスクとは」（354 ページ）を参照してください。 （**注意**：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）。

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。 • 削除：タスクを削除できます。 • 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（**注意**：タスクを再開する場合は、[再開] を選択します）。 • 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。 • 編集：対象タスクの [タスクを編集] ページが開きます。
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] の下のメニューバーで [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」（617 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] の下のメニューバーで [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、「[自分のタスク] ページのフィールド」（853 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、「[予定タスク] ページのフィールド」（491 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、「[実行中のタスク] ページのフィールド」（494 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、「[最近のタスク] ページのフィールド」（496 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。 • 承認済み • 未承認 • 承認を待機中

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、「[タスク情報] ページのフィールド」（860 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。タスクは、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。（**注意**：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、データプ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、「[データの整理] タスクページのフィールド」（474 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。 • 承認を待機中 • 未承認
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	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。 • 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。 • 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。 • 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。 • 失敗：タスクは失敗しました。 • 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。 • 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。 • 実行中：タスクは開始しましたが、まだ終了していません。 • スキップ：タスクはエラー（例えば、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。 • 成功：タスクは成功しました。 • 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。
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] の下のメニューバーで、[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」（857 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。例えば、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。「[自分のタスク] ページのフィールド」（487 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。
タスクのステータス	次に示すタスクのステータスを表示します。 • ドラフト • 重複 • 失敗 • 一時停止 • 保留 • 要求（注意：要求とは、タスクが承認を待っていることを示します。「タスクの承認」（860 ページ）を参照してください）。 • 実行中 • スキップ • 成功 • 同期（注意：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）。 • 待機中 • 警告 **注意**：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。
コメント	タスク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
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。
スケジュール日時	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	例えば、非反復などの反復タイプを表示します。
承認情報	
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。
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。
追加情報	
結果の詳細	（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。例えば、次のような診断があります。 • 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) • 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) • 診断 'NA OSPF ネイバー ' が完了しました。
タスク履歴	
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、ワークフロールール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」（850 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 jbrennan1
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

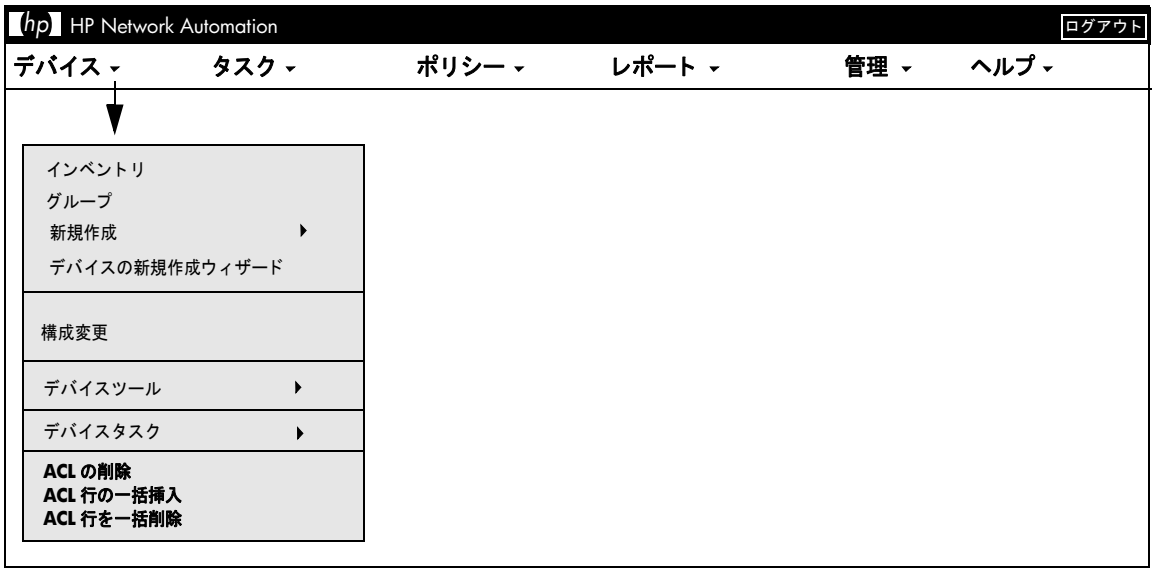
電子メールの最後にあるリンクをクリックすると、[承認の要求] ページが開きます。このページでは、タスクを承認または拒否することができます。「[承認の要求] ページのフィールド」（857 ページ）を参照してください。

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	「はじめに」（867 ページ）
ACL の表示	「ACL の表示」（868 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」（872 ページ）
ACL の作成	「ACL の作成」（873 ページ）
ACL アプリケーションの変更	「ACL アプリケーションの変更」（874 ページ）
ACL 行の一括挿入	「ACL 行の一括挿入」（875 ページ）
ACL 行の一括削除	「ACL 行の一括削除」（876 ページ）
ACL へのコメントの追加と ACL ハンドルの作成	「ACL へのコメント追加と ACL ハンドルの作成」（878 ページ）
ACL テンプレートの作成	「ACL テンプレートの作成」（879 ページ）
ACL の編集	「ACL の編集」（880 ページ）
ACL の削除	「ACL の削除」（881 ページ）

ACL へのナビゲート


HP Network Automation
ログアウト
デバイス
タスク
ポリシー
レポート
管理
ヘルプ
インベントリ
グループ
新規作成
デバイスの新規作成ウィザード
構成変更
デバイスツール
デバイスタスク
ACL の削除
ACL 行の一括挿入
ACL 行を一括削除

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」（41 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」（206 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」（647 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] の下のメニューバーで、[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」（133 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」（868 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 の表示] ページが開きます。「[ACL の表示] ページのフィールド」(870 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	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	例えば「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
チェックボックス	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。 • 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ハイライト表示されます。 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。
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。
アクション	次のアクションを選択できます。 • 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、「コマンドスクリプトの実行」（872 ページ）を参照してください。 • 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、「[ACL の表示] ページのフィールド」（870 ページ）を参照してください。 • 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。

[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] の下のメニューバーで、[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。

フィールド	説明 / アクション
ACL スクリプト	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。 • 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（「ACL の作成」（873 ページ）を参照してください）。 • 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（「コマンドスクリプトの実行」（872 ページ）を参照してください）。 • 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（「ACL テンプレートの作成」（879 ページ）を参照してください）。 • 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（「ACL テンプレートの作成」（879 ページ）を参照してください）。
ACL アプリケーション	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。 • 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（「ACL の作成」（873 ページ）を参照してください）。 • 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（「ACL テンプレートの作成」（879 ページ）を参照してください）。
コメント	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。 • コメントを編集：[ACL を編集] ページが開きます。 • 履歴：[ACL 履歴] ページが開きます。 • 関連設定を表示：[デバイス構成] ページが開きます（「[デバイス構成の詳細] ページのフィールド」（223 ページ）を参照してください）。

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」（385 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（かっこ内）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] の下のメニューバーで、[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」（385 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] の下のメニューバーで、[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 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」（870 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」（873 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」（873 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：上記変数の入力が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：上記変数の入力が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」（873 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。例えば、`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：上記変数の入力が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：上記変数の入力が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] の下のメニューバーで、[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」（870 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] の下のメニューバーで、[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 の表示] ページが開きます。
5. [ACL スクリプト] の下の [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」（716 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、スクリプトで使用され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」（872 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」（868 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] の下のメニューバーで、[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」（873 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」（385 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」（882 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。 • 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。デバイスセレクタの使用方法の詳細については、「デバイスセレクタ」（180 ページ）を参照してください。 • 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。
開始日	次のオプションを選択できます。 • 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。 • 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。
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、「タスクの予定」（355 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。
タスクオプション	
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。

フィールド	説明 / アクション
削除する ACL	次のオプションを選択できます。 • 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）。 • 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 がハンドルをかっこ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）。
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] の下の [サーバ] ページで構成する、[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]、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、「[デバイスアクセス] ページのフィールド」（54 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 [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]、[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。）

フィールド	説明 / アクション
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 （詳細は、「[構成管理] ページのフィールド」（41 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 • タスクの一部として（デフォルト）
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。
スケジューリングオプション	
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。 • 再試行なし（デフォルト） • 1 回 • 2 回 • 3 回

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	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。 • 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）。 • 定期的：繰り返し間隔を分単位で指定します。 • 日次：タスクは指定した時刻に毎日実行されます。 • 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。 • 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。
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。 • 終了日なし（デフォルト） • < > オカレンス後に終了：反復回数を入力します。 • 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。

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	「ドライバ検出の失敗」（888 ページ）
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取得の失敗」（889 ページ）
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なし」（890 ページ）
セッションログ	「セッションログ」（891 ページ）
SWIM エラーメッセージ	「SWIM エラーメッセージ」（892 ページ）

ログ記録の詳細については、「ログ記録」（122 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」（34 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、Device Driver Reference（DRS）ドキュメントを参照してください。DRS は、新しく自動化されたドライバリリースおよびデリバリシステムです。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」（237 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」（226 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」（122 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、Device Driver Reference（DRS）ドキュメントを参照してください。DRS は、新しく自動化されたドライバリリースおよびデリバリシステムです。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」（ 257 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」（237 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」（226 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、Device Driver Reference（DRS）ドキュメントを参照してください。DRS は、新しく自動化されたドライバリリースおよびデリバリシステムです。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、Device Driver Reference（DRS）ドキュメントを参照してください。DRS は、新しく自動化されたドライバリリースおよびデリバリシステムです。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 ロギング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」（41 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。例えば 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、ユーザ名とパスワードを入力します。

次のページに続く

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
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。
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。

次のページに続く

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
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。

次のページに続く

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
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。
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。）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。）	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

次のページに続く

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
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。	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。
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。
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。

次のページに続く

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
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。）	デバイスのイネーブルパスワード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。 *次のページに続く*

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
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
SWIM1052	Enable password is not configured for the device.（デバイスのイネーブルパスワード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、イネーブルパスワードを構成する必要があります。	デバイスのイネーブルパスワード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。

次のページに続く

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
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。
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

次のページに続く

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
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。）他のイメージを選択してください。	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。）Select a different image.（他のイメージを選択してください。）	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。

次のページに続く

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

次のページに続く

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
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。 • SNMP-V3 パスワードが誤って構成されている • SNMP-V3 アルゴリズムが誤って構成されている • デバイスの SNMP-V3 エンジン ID が構成されていない。	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。
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）。

次のページに続く

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
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 インストゥルメンテーションを基に、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。）	デバイスのイネーブルパスワード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 *devicename* data in the inventory.（このオプションでは、インベントリに *devicename* 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

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
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。
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。

次のページに続く

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
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。

次のページに続く

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。）Selected storage partition will be erased during the distribution.（選択した記憶域パーティションは、配布中に削除されます。）	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 *devicename*.（インベントリに *devicename* のモジュール情報がありません。）	*devicename* 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。

次のページに続く

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
SWIM1530	Storage Recommendation is not supported for the Module *modulename*.（モジュール *modulename* 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。
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。

次のページに続く

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
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。）	Either the Flash device is not available or the Flash information format has changed.（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 *devicename* using protocol.（プロトコルを使用してデバイス *devicename* 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。

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。ハイライトされたテキストはコピーバッファに保存されます。別のアプリケーションにペーストします。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表示するには、「`help`」と入力すると、すべてのコマンドのリストが表示されます。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。例えば、Import コマンドに関する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）。
- 例えば、Import コマンドに関するヘルプを表示するには、「`help import`」と入力します。help <command name> コマンドによって、名前、概要、説明、および例など、そのコマンドの詳細が戻されます。
- コマンドラインでの作業が終了したら、「`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。

シンタックスと例を含む CLI の完全なリストについては、『*HP Network Automation 7.60 API Reference Guide*』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」（332 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」（914 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」（330 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
デバイスグループの追加
イベントの追加
SNMP トラップ構成の追加
システム管理設定
デバイスグループの管理
ユーザの管理
ユーザグループの管理
デバイスの構成への注釈付け
Telnet と SSH の同時セッションを許可
デバイスソフトウェアのバックアップ
デバイスを一括編集
デバイスパスワードの変更
構成ポリシー準拠の確認
Syslog の構成
コネクタのリダイレクト
データの整理
重複の削除
アクセスの削除
デバイスを削除
デバイス構成の削除
診断の削除
ドライバの削除
セッションの削除
ソフトウェア準拠の削除
ソフトウェアイメージの削除
ソフトウェアレベルの削除
システムイベントの削除
タスクを削除
リモートエージェントの配布
ソフトウェアを配布
ネットワークデバイスの検出
デバイスドライバの検出
ドライバ
ACL を編集
ACL コメントの編集
構成（変更）ユーザの編集
デバイスを編集
非アクティブなデバイスの編集
タスクを編集
ユーザを編集
電子メールレポート
外部認証の設定
サマリレポートの生成
デバイスとパスワードのインポート
SysOID のリスト表示
リストの表示
ACL の管理
コマンドスクリプトの管理
構成ポリシーの管理
デバイスパスワードルールの管理
診断スクリプトの管理
イベントルールの管理
拡張カスタムデータの管理
分散システムの管理
ゲートウェイの管理
IP アドレスの管理
ライセンスの管理
パーティションの管理
ソフトウェア準拠の管理
ソフトウェアレベルの管理
ソフトウェアイメージの管理
システムレポートの管理
テンプレートの管理
ユーザの管理
ユーザグループの管理
ユーザロールの管理
ビューの管理
デバイス構成の変更
SecurID の変更
マルチタスクプロジェクト
ワークフロー承認の無効化
デバイスのリブートタスク
FQDN の解決
コマンドスクリプトの実行
診断の実行
外部アプリケーションの実行
ICMP テストの実行

(*次のページに続く*)

タスクに最も高い優先度を設定
反復タスクの同期
スナップショットの取得
Telnet/SSH クライアント
トラブルシューティング
デバイスコメントの更新
デバイスチケットの更新
ワークフロー設定
ACL を表示
コマンドスクリプトの表示
構成ポリシーイベントの表示
配布済みソフトウェアの表示
構成ポリシーの表示
デバイス構成の表示
デバイス診断の表示
デバイス情報の表示
診断スクリプトの表示
ドライバの表示
イベントルールの表示
全デバイス構成の表示
スクリプトと診断の表示
SecurID の表示
セッションを表示
ソフトウェアイメージアーカイブの表示
タスクの表示
テンプレートの表示
ユーザ情報の表示
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。

コマンド権限	説明
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。
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。

コマンド権限	説明
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 プロセスと連係します。（詳細については、『*NA 7.60 Satellite User's 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。

コマンド権限	説明
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。
ユーザを編集	ユーザプロファイ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ァイ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。

コマンド権限	説明
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 7.60 Multimaster Distributed System on Oracle User's 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 プロセスと連係します。
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。
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。

コマンド権限	説明
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。

コマンド権限	説明
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。
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	マルチタスクプロジェクトを変更する権限です。
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。

コマンド権限	説明
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 サーバのロギングレ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。
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。

コマンド権限	説明
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;

$iaddr = gethostbyname("$tc_device_ip$");
$telnet_port = 23;
$sin = sockaddr_in($telnet_port, $iaddr);
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;

$iaddr = gethostbyname("$tc_device_ip$");
$telnet_port = 23;
$sin = sockaddr_in($telnet_port, $iaddr);
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限り
# 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。用語はアルファベット順でリストされています。

用語	定義
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。
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。
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。
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。
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。
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。例えば、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 管理エンジンは起動時に、タスクプールの構成をデータベースに要求します。タスクが作成、更新、削除されると、NA はローカルの NA コアに付属するデータベー スの更新のみを行います。リモートの NA コアに付属するデータベース内で必要な 変更は、データベースのリプリケーション機能によって処理されます。しかし、メモリ内のタ スクプールの更新のために、リモートの NA コアを呼び出すのはアプリケーション の役割です
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。
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。
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。
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。
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。
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。
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。

用語	定義
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。例えば、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、ユーザを分類することです。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。例えば、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。 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） デバイスで動作するソフトウェアバージョン
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。
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。

索引

J

L

M

N

O

P

Q

R

S

T

V

あ

い

お

か

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

に

ね

の

は

ひ

ふ

へ

ほ

ま

め

も

ゆ

よ

ら

り

る

れ

ろ

わ