HP Client Automation

Core および Satellites

Enterprise Edition

Windows® オペレーティング システム用

ソフトウェア バージョン : 7.50

ユーザー ガイド

製造パート番号 : なし
ドキュメントのリリース日 : 2009 年 5 月
ソフトウェアのリリース日 : 2009 年 5 月

ご注意

保証

HP の製品およびサービスで保証されるのは、製品およびサービスに添付される明確な保証文で説明されているものだけですここでの記載で追加保証を意図するものは一切ありませんここに含まれる技術的、編集上の誤り、または欠如について、HP はいかなる責任も負いません。

本書に記載した内容は、予告なしに変更することがあります。

権利の制限

コンピュータ ソフトウェアの機密保持所有、使用、または複製を行う場合には、HP からの正規のライセンスが必要です FAR 12.211 および 12.212 に従い、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 ドキュメンテーション、および市販品の技術データは、各販売業者の標準営業許可のもとに米国政府にライセンスされています。

著作権

商標

Apache Software License、Version 1.1
この製品には Apache Software Foundation (http://www.apache.org//) が開発したソフトウェアが含まれています。

Linux は、Linus Torvalds の登録商標です。

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

PREBOOT EXECUTION ENVIRONMENT (PXE) SERVER

TFTP SERVER

OpenLDAP

ドキュメントの更新

本書のタイトル ページには、次の識別情報が含まれています。

- ソフトウェア バージョン番号。ソフトウェアのバージョンを示します。
- ドキュメントのリリース日。ドキュメントが更新されるごとに変わります。
- ソフトウェアのリリース日。ソフトウェアのこのバージョンのリリース日を示します。

最近の更新がないか確認したり、最新版のドキュメントを使用していることを確認したりするには、次の URL に移動してください。

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

このサイトでは、HP Passport に登録し、サインインする必要があります。HP Passport ID に登録するには、次を参照してください。

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

または、HP Passport サインインのページの **[New users - please register]** のリンクをクリックしてください。

適切な製品サポート サービスを購読している場合にも、更新版や新版を受け取ることができます詳細については、HP 営業担当者までご連絡ください。

サポート

次の HP Software のサポート Web サイトを参照してください。

www.hp.com/go/hpsoftwaresupport

この Web サイトには、HP Software の製品、サービス、サポートに関するお問い合わせ先情報が掲載されています。

HP Software オンライン サポートでは、お客様自身が問題を解決するために有益な情報を提供しますビジネスを管理するために必要な対話型技術サポート ツールに素早く効率的にアクセスする方法を提供していますサポートを受けるお客様は、サポート Web サイトを使用して次のことができます。

- 関心がある知識ドキュメントの検索
- サポート事例および機能強化リクエストの提出とサポート状況の追跡
- 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 サポート連絡先の確認
- 利用可能なサービスに関する情報の確認
- 他のソフトウェア顧客とのディスカッションへの参加
- ソフトウェア トレーニングの検索と登録

多くのサポート エリアは、HP Passport のユーザー登録とサインインを必要とします。サポート契約が必要なエリアもあります HP Passport ID に登録するには、次を参照してください。

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

アクセス レベルに関する詳細については、次を参照してください。

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

目次

1 はじめに

HP Client Automation < ライセンス タイプ。は、PC ソフトウェア設定管理ソリューションです。OS イメージの配布、パッチの管理、リモート コントロール、HP ハードウェアのドライバや BIOS の更新、およびソフトウェアの配布と利用状況の測定などのソフトウェアおよび HP ハードウェア管理機能すべてを、Web ベースの統合コンソールから提供します。

このマニュアルについて

このガイドでは、HP Client Automation console、Publisher、Application Self-Service Manager、および Image Preparation Wizard を使用するための詳細な情報を提供し、手順について説明します。

HPCA Core および Satellites サーバーのインストールと初期設定の要件および方法については、『HP Client Automation Core および Satellite 入門およびコンセプト ガイド』を参照してください。

HPCA のドキュメント

メディアに収録されている HP Client Automation のドキュメントは、Core インストール時にもインストールされます。これらは PDF 形式のドキュメントで、Windows の [スタート] メニューやデスクトップのショートカット リンクからアクセスするか、Core サーバーにアクセスできる任意のデバイスからブラウザからアクセスできます (URL:`http://HPCA_Host:3466/docs` (`HPCA_Host` は HPCA がインストールされているサーバー名))。

2 はじめに

HPCA をインストールし、Web ベースの HPCA Console (コンソール) を使用して環境の管理を始める準備ができました。

この章のセクションでは、次の内容について説明します。

- さまざまな管理タスクや設定タスクを実行するために使用する HPCA Console。24 ページの「Web ベースの HPCA Console へのアクセス」を参照してください。
- HPCA 環境の管理を開始するために完了する必要のあるタスク。これには、設定手順や詳細情報の入手方法が含まれます。25 ページの「HPCA の実装」を参照してください。

Web ベースの HPCA Console へのアクセス

HPCA Server では、さまざまな管理タスクや設定タスクを実行できるコンソールを使用します。これらのタスクの詳細については、229 ページの「オペレーション」および 253 ページの「設定」を参照してください。

HPCA Console を起動するために使用できる方法には、次の 3 つがあります。以下が可能です。

- **[Client Automation Console]** デスクトップ アイコンをダブルクリックします。
- HPCA Server がインストールされたマシンで、Windows の **[スタート]** メニュー パスに移動します。
- 環境内の任意のデバイスで Microsoft® Internet Explorer® (バージョン 6.0 以上) または Mozilla Firefox (バージョン 2.0 以上) の Web ブラウザを開き、次の URL に移動します。

  http://*HPCA_host***:3466/**

  ここで、*HPCA_host* は、HPCA がインストールされているサーバーの名前です。

どの方法でも HPCA Console が起動され、ログイン認証情報の入力を求めるプロンプトが表示されます。プロンプトが表示されたら、ユーザー名とパスワードを指定し、**[サインイン]** をクリックします。

デフォルトのユーザー名は **admin**、デフォルトのパスワードは **secret** です。

デフォルトのユーザー名とパスワードを変更する方法、およびコンソールへのアクセス権限リストにユーザーを追加する方法については、253 ページの「設定」を参照してください。

重要

- ウィザードを実行したり警告を表示したりするときに、HPCA Console が追加のブラウザ インスタンスを開く場合があります。これらのウィザードや警告にアクセスするには、ブラウザのポップアップ ブロック設定で [許可されたサイト] に HPCA を指定します。
- セキュリティのため、HPCA では、20 分間操作を行わないと、自動的に現在のユーザーをログアウトさせます。コンソールの使用を続けるには、再度ログインする必要があります。
- コンソールの **[レポート]** セクションでグラフィカル レポートを表示するには、Java Runtime または Java Virtual Machine が必要です。Java は、**http://java.com/en/index.jsp** からインストールできます。

- **Windows 2003 Server**: Windows 2003 Server オペレーティング システムがインストールされたデバイスで HPCA にローカル アクセスできるようにするには、**ローカル エリア ネットワーク (LAN)** の設定で **[ローカル アドレスにはプロキシ サーバーを使用しない]** を有効にする必要があります。

HPCA の実装

次のセクションでは、HPCA を使用して環境の管理を開始するために完了する必要のある初期タスクについて説明します。これらのタスクは、すべて HPCA Core Console を使用して実行されます。一部のタスクは、実行可能な HPCA 環境を確立するために必要 (*必須*) です。その他のタスクは *オプション* ですが、追加で基本的な管理機能を有効にするためのものとして含まれています。

HPCA Core Console の各タブ (下記参照) を使用すると、さまざまな管理タスクにアクセスできます。

- ダッシュボード
- 管理
- レポート
- オペレーション
- Configuration

設定タスクを完了するために、これらのすべてのタブにアクセスする必要はありません。

必須のタスク

HPCA 管理環境を確立して実行可能にし、さらに機能するようにするには、このセクションに記載されているタスクを必ず実行する必要があります。

1 **デバイスのインポート** : クライアント デバイスを HPCA 環境にインポートして、デバイスが HPCA Server に認識されるようにします。26 ページの「デバイスのインポート」を参照してください。

2 **HPCA Agent の配布** : インポートしたクライアント デバイスに HPCA Agent を配布します。これにより、これらのデバイスが HPCA の管理対象になります。

HPCA Agent の配布方法にはいくつかあります。これらの方法は、26 ページの「HPCA Agent の配布」で説明します。

3 **ポリシーの設定**：HPCA を使用して、クライアント デバイス上の HPCA Agent の「状態」を確立します。27 ページの「ポリシーの設定」を参照してください。

オプションのタスク

このセクションに記載しているタスクは、HPCA 環境でのその他の管理制御や機能を確立する必要がある場合に実行します。それぞれのタスクの詳細は、次の各セクションで説明します。

- 脆弱性の管理 30 ページ
- クライアント オペレーション プロファイルの設定 30 ページ
- パッチ管理の設定 36 ページ
- オペレーティング システム イメージの配布 38 ページ
- アウトバンド管理の有効化 40 ページ

デバイスのインポート

使用環境にある HPCA の管理対象デバイスを (HPCA に) インポートする必要があります。これにより、それらのデバイスが HPCA によって認識されるため、インベントリ情報を収集したり、ソフトウェアやパッチを配布したりできるようになります。

- [デバイス管理] の [一般] タブで、**[インポート]** をクリックしてデバイス インポート ウィザードを起動します (153 ページの「デバイスのインポート」を参照)。
- ウィザードの手順に従って、デバイスをインポートします。

  ほとんどのタスクは、[現在のジョブ] タブおよび [過去のジョブ] タブまたは [ジョブ管理] セクションで監視できるジョブを生成します。

デバイスがインポートされたら、ソフトウェア、パッチ、およびインベントリを管理するために HPCA Agent の配布を開始できます。

HPCA Agent の配布

HPCA 管理者によるデバイスの管理を容易にするために、HPCA Agent がデバイスに配布され、インストールされます。このエージェントは、デバイスに個別に配布するか、またはグループに属する複数のデバイスに配布することができます。

HPCA Agent は、エージェント配布ウィザードを使用してデバイスに配布されます (156 ページの「HPCA Agent の配布」 を参照)。ウィザードが完了すると、エージェント配布ジョブが作成されます。

HPCA Agent の詳細については、『HP Client Automation Application Manager および Application Self-Service Manager ガイド』を参照してください。

ポリシーの設定

HPCA は、HPCA 管理者がマシンまたはユーザーに定義したポリシー エンタイトルメントに従って管理対象エージェントの要求ステートを解決します。このポリシー エンタイトルメントは、次のように定義できます。

- **内部** : Configuration Server Database (CSDB) の PRIMARY.POLICY ドメイン内。
- **外部** : Active Directory などの LDAP ディレクトリ内。

  Core CSDB には、既存の外部ポリシーの実装を容易にするデフォルト インスタンスが事前設定されています。また、Core および Satellite Server には、外部ポリシーの接続を有効および設定するための設定内容が含まれています。

内部ポリシーの設定

HPCA Agent のポリシーは、Core CSDB の PRIMARY.POLICY.USER クラスで設定できます。HPCA Agent が CSDB に接続したときに、そのユーザー ID が USER クラスのインスタンスとして定義されている場合は、そのインスタンスで定義されているポリシーに従って解決が実行されます。ポリシー ストアにこの方法を使用する場合は、次の操作を実行する必要があります。

- Core サーバーと Satellite Server のポリシー サービスを無効にします。
- USER クラスに USER インスタンスを追加し、それらのインスタンスをユーザーが使用できるサービスに接続します。

内部ポリシーのこの方法の確立の詳細については、『HPCA Application Manager および Application Self-service Manager インストールおよび設定ガイド』のポリシーに関する章を参照してください。

外部ポリシーの設定

ポリシー設定を既存の LDAP (または、その他の外部) ディレクトリに適用した後、HPCA 環境で使用できるようにすることができます。このサポートを有効にするための手順は、28 ページの「外部ポリシー ストアの実装」に記載されています。

外部ポリシー ストアを使用する場合、Core CSDB のデフォルトの動作は次のとおりです。

- ユーザーが USER インスタンスで定義されていない HPCA Agent 接続の場合、解決にはマシンのドメイン名がデフォルトで使用され、コア コンソールと Satellite コンソールのポリシー設定を使用してアクセスするように設定された、外部の LDAP ディレクトリで定義されたポリシーが検索されます。
- 外部のディレクトリからのマシン名による解決は、PRIMARY.POLICY.USER の _NULL_INSTANCE_ で定義されています。このインスタンスには、属性が SYSTEM.ZMETHOD.LDAP_RESOLVE に設定された _ALWAYS_ (ユーティリティ メソッド) 接続が含まれています。

外部ポリシー ストアの実装

外部ポリシー ストアのためのポリシーの設定は、デフォルトで LDAP ディレクトリに接続するように設定され、HPCA Agent で管理されたマシンの完全なドメイン名を使用してポリシーを管理します。別のパラメータを使用してポリシーを管理するには、LDAP_RESOLVE メソッドの ZMTHPRMS 属性を調整します。これについては、28 ページの「外部の LDAP ポリシー ストアを実装するには」で説明します。

デフォルトでは、外部のディレクトリ サービスの Core を設定すると、ポータルも (ポリシーに) 同じ外部のディレクトリ サービスを使用するように設定されます。外部のディレクトリ サービスの接続は、ベース DN から派生します。

外部の LDAP ポリシー ストアを実装するには

1. ポリシー サービスが、ポリシーに使用される外部のディレクトリ サービスに接続できるように Core を設定します。この方法については、260 ページの「ディレクトリ サービス アカウントを使用するには」を参照してください。
2. 外部のディレクトリ サービスに接続するフルサービス Satellite を有効化および設定します。

3 Core コンソールの [ポリシー] ページで生成された (スキーマの変更を含む) LDIF ファイルを使用して、HPCA ポリシー設定が使用されるようにディレクトリ スキーマを変更します。

既存の LDAP をバックアップするためのコマンドは次のとおりです。

LDIFDE -f *OutputFileName*

外部のディレクトリ サービスを更新するためのコマンドは次のとおりです。

LDIFDE -i -f HPCAExtensions.ldif 没

LDIFDE コマンドは、Windows サーバー プラットフォームにのみ適用されます。詳細については、Microsoft サポート技術情報の記事「LDIFDE を使用したディレクトリ オブジェクトの Active Directory へのインポート / エクスポート」を参照してください。

詳細については、『Policy Server ガイド』を参照してください。

4 必要に応じて、Core Configuration Server Database の PRIMARY.SYSTEM.ZMETHOD クラスの LDAP_RESOLVE メソッドを変更します。

デフォルトでは、CSDB は LDAP_RESOLVE メソッドを使用し、マシンの完全なドメイン名でポリシーを管理するように事前設定されています。これは、ZMTHPRMS 属性によって次のように定義されています。

```
ZMTHPRMS = ldap:\\\<ADINFO.COMPDN>>
```

これには、このマシンがポリシーの定義されているディレクトリに対応するドメインのメンバーである必要があります。マシンがそのドメインのメンバーでない場合、ADINFO.COMPDN は空白になります。

a 別の値を使用してポリシーを管理するには、ZMTHPRMS 値を調整します。それには、『Policy Server ガイド』の「Configuring the LDAP_RESOLVE Method」を参照してください。

b 重要 : Core CSDB の ZMTHPRMS 値を調整した場合は、新しい値を設定とポリシーが有効になっている各 Satellite に転送するために、必ず Satellite との同期を実行してください。

Policy Server の設定に従い、[管理] タブを使用して、LDAP ポリシー ストア内のポリシー エンタイトルメントの追加、管理、およびクエリを実行します。

ポリシー解決の確認

ポリシーが Satellite を介して解決されていることを確認するには、次の手順を実行します。

1 [管理] タブを使用してポリシー ディレクトリをブラウズし、そのディレクトリ サービス オブジェクトを介してサービスに HPCA Agent のエンタイトルメントを設定します。144 ページの「ディレクトリ ポリシーの管理」を参照してください。

2 デバイスに HPCA Agent をインストールし、SAP エントリが、Satellite には **PRI 10** として、Core には **PRI 20** として、その HPCA Agent を送信するようにします。

3 HPCA Agent 接続を実行し、エンタイトルメント サービスが (Application Self-Service Manager を使用して) インストールできるか、または (Application Manager の場合は) インストールされていることを確認します。

脆弱性の管理

HPCA 脆弱性管理をサポートするには、次の操作を実行する必要があります。

- 通知の設定を作成する
- コンソール設定を確認する
- コンソールの [設定] タブで、**HP Live Network** の設定を行う

詳細については、「セキュリティとコンプライアンスの管理」の章を参照してください。

クライアント オペレーション プロファイルの設定

HPCA Server 環境では、**クライアント オペレーション プロファイル** (**COP**) を使用して、HPCA Agent をその設定やデータ リソースのために企業内の Satellite アクセス ポイントに送信します。

COP の詳細とサーバー アクセス プロファイルの詳細オプションについては、『HPCA Application Manager および Application Self-Service Manager の Windows 用インストールおよび設定ガイド』の「Configuring Client Operations Profiles」の章を参照してください。

サーバー アクセス プロファイル インスタンスの作成

Core Configuration Server Database の SAP クラスには、各タイプの**サーバー アクセス プロファイル (SAP)** のサンプルが含まれています。

環境内の各 Satellite の新しいインスタンスを作成する必要があります。このセクションで説明しているように、通常フルサービス Satellite ごとに 2 つのインスタンスがあり、ストリームライン Satellite には 1 つのインスタンスがあります。

ここで詳述する Configuration Server Database の変更は、Core CSDB で実行する必要があります。

Satellite Server CSDB は、そのアップストリーム サーバー CSDB (Core または別の Satellite のいずれか) の複製であるため、決して変更しないでください。

- **hostname_RCS** インスタンス : フルサービス Satellite の `hostname_RCS` インスタンスを作成するには、CORE_RCS インスタンスを使用します。

  `hostname_RCS` インスタンスの `URI` 値を、Satellite をホストしているマシンのホスト名を指すように変更する必要があります。

- **hostname_RPS** インスタンス : 各フルサービス Satellite および各ストリームライン Satellite の **`SAT_RPS`** インスタンスを作成するには、CORE_RPS インスタンスを使用します。簡略名の場合は、`hostname - Data` を使用して、HPCA Agent にデータ リソースを提供するロールを表すことができます。

  `hostname_RPS` インスタンスの `URI` 値を、Satellite をホストしているマシンのホスト名を指すように変更する必要があります。

  OS Manager に固有の SAP 情報については、『HPCA OS Manager System Administrator ユーザー ガイド』を参照してください。

例

2 つの Satellite (PARISSAT3 と EUROSAT1) が含まれており、32 ページの表 1 にある 3 つの SAP インスタンスが必要な環境があるとします。

表 1　2 つの Satellite のための SAP インスタンスの例

ホスト名	**Satellite** のモード	**SAP** インスタンス名 **(** 簡略名 **)**	**SAP** のタイプ	**SAP** 優先度
PARISSAT3	ストリームライン	PARISSAT3_RPS (PARISSAT3 - DATA)	データ	10
EUROSAT1	フルサービス	EUROSAT1_RPS (EUROSAT1 - DATA)	データ	20
EUROSAT1	フルサービス	EUROSAT1_RCS (EUROSAT1 - RCS)	RCS	30

Satellite のサーバー アクセス プロファイル インスタンスを作成するには

1 Core Server で、HPCA Admin CSDB Editor を使用して、CSDB の**プライマリ** ファイル、**クライアント** ドメイン、**サービス アクセス プロファイル (SAP)** クラスに移動します。

HPCA Administrator にアクセスする方法については、『HPCA Administrator ユーザー ガイド』を参照してください。

2 PRIMARY.CLIENT.SAP クラスから、CORE_RCS インスタンス (簡略名 : Core - RCS) を、hostname - RCS の簡略名を持つ hostname_RCS という名前のインスタンスにコピーします (この例では、EUROSAT1_RCS インスタンスの簡略名は EUROSAT1 - RCS の簡略名です)。

3 hostname_RCS インスタンスを選択して変更します。次のように、URI 属性を、Satellite をホストしているマシンのホスト名を指すように変更します。

```
URI = tcp://satellite_hostname:3464
TYPE = RCS
ROLE = OSMR
```

4 CORE_RPS インスタンス (簡略名 : Core - RPS) を、hostname - Data の簡略名を持つ CLIENT.SAP.hostname_RPS インスタンスにコピーします。

Data は、この SAP エントリが、HPCA Agent にデータ リソースを提供するサーバーのロールに対応していることを示しています (この例では、EUROSAT1_RPS インスタンスの簡略名は EUROSAT1 - Data です)。

5 新しい hostname_RPS インスタンスを選択して変更します。次のように、URI 属性をフルサービス Satellite のホスト名を指すように変更します。

URI = **http://***satellite_hostname***:3466**
http://EUROSAT1:3466
TYPE = **DATA**
ROLE = **DZ** になります

6 ストリームライン Satellite のもう一つのインスタンスを作成するために、新しく作成した hostname_RPS インスタンスをコピーします (この例では、PARISSAT3_RPS インスタンスの簡略名は PARISSAT3 - Data です)。

7 新しく作成した SAP インスタンスを変更して、URI 属性をストリームライン Satellite のホスト名を指すように設定します。

8 変更を保存します。

ゲートウェイを使用したパッチ配布のためのサービス アクセス プロファイルの変更

Microsoft デバイスにパッチを適用する場合は、次のパッチ配布設定を行うことによって軽量のパッチ適用モデルを使用できます。

- パッチ メタデータのみのダウンロードを有効化
- ゲートウェイの有効化

これらのパッチ配布設定を使用している場合は、**DATA** の TYPE で定義されたコアおよび Satellite の SAP インスタンスにも **P** という ROLE が含まれていることを確認してください。これらのインスタンスには、通常 Core_RPS および satellite_hostname_RPS という名前が付けられます。

これらの SAP エントリに **P** という ROLE が含まれていない場合は、次の手順を使用してこれらのエントリを変更します。

ゲートウェイからパッチ バイナリを配布するように SAP インスタンスを変更するには

SAP インスタンスの作成または編集に関する基本的な情報については、31 ページの「サーバー アクセス プロファイル インスタンスの作成」を参照してください。

1 Core Server から、CSDB Editor を使用して CORE_RPS の SAP インスタンス (TYPE = DATA のインスタンス) を開き、次のように変更します。

a **P** という ROLE 値を追加します。

これらの値には、次の太字の部分を追加する必要があります。

```
TYPE = DATA
URI = http://hostname:3466
ROLE = DZP
```

2 変更を CORE_RPS インスタンスに保存します。

3 TYPE = DATA で定義された Satellite の SAP インスタンスにも、ROLE の変更を手順 1 から同様に適用します。これらのインスタンスには、通常 satellite_hostname_RCS という名前が付けられます。

4 すべての変更を Satellite の * _RPS インスタンスに保存します。

SAP インスタンスの LOCATION クラス インスタンスへの接続

Core Server で、PRIMARY.CLIENT.LOCATION クラス インスタンスを使用して、ロケーション基準に基づいて SAP 優先度を定義します。SAP の優先度は、接続先を示す SAP インスタンスのすぐ上にある SAPPRI 属性で定義します。

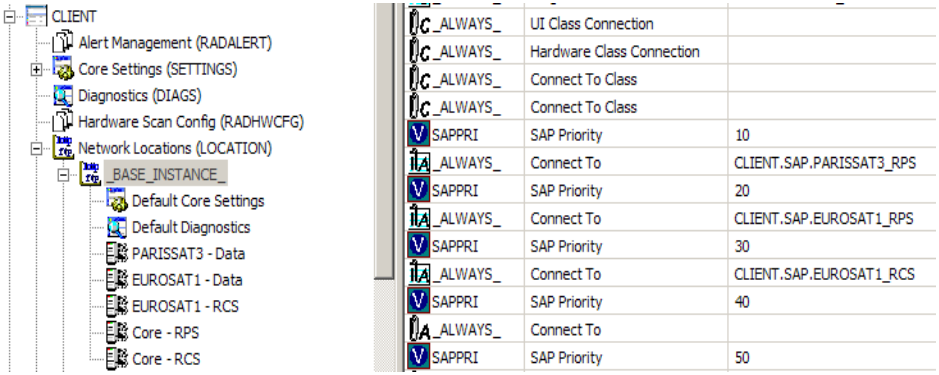
デフォルトでは、CORE_RPS インスタンスと Core_RCS インスタンスは、それぞれ 60 と 70 の優先度を持つ CLIENT.LOCATION._BASE_INSTANCE_ に接続されます。

優先度の値は小さい方から並べられます。つまり数値が小さいほど、優先度は高くなります。そのため、Satellite により小さい数値の優先度を割り当てることによって、HPCA Agent は優先されるアクセス ポイントとしてそれらの Satellite に接続しようとします。Core (優先度の数値が大きい) は、フェールオーバー アクセス ポイントとして使用されます。

Core および Satellite の SAP インスタンスを LOCATION クラス インスタンスに接続するには

1 Core Server で、HPCA Admin CSDB Editor を使用して、各 LOCATION クラス インスタンスに対する各 SAP インスタンスの優先度を設定します。

たとえば、次の図は、すべての HPCA Agent が Satellite を優先されるアクセス ポイントとして使用するように、CLIENT.LOCATION._BASE_INSTANCE_ に接続された SAP インスタンスを示しています。



2 CLIENT.SAP.PARISSAT3_RPS インスタンスを CLIENT.LOCATION._BASE_INSTANCE_ 内の最初の使用可能な接続先に接続し、そのインスタンスに 10 の優先度を割り当てます。

3 CLIENT.SAP.EUROSAT1_RPS インスタンスを 2 番目の使用可能な [接続先] に接続し、そのインスタンスに 20 の優先度を割り当てます。

4 CLIENT.SAP.EUROSAT1_RCS インスタンスを 3 番目の使用可能な [接続先] に接続し、そのインスタンスに 30 の優先度を割り当てます。

Satellite の SAP インスタンスに Core の SAP インスタンスより高い優先度を割り当てることによって、HPCA Agent はまず、これらの Satellite に接続しようとします。これらの Satellite が使用できない場合は、Core に接続しようとします。

HPCA Agent でのクライアント オペレーション プロファイルの有効化

HPCA Agent で COP を有効にする方法は複数あり、それらの HPCA Agent が既にインストールされているかどうかによって異なります。すべてのオプションについては、『HPCA Application Manager および Application Self-Service Manager の Windows 用インストールおよび設定ガイド』の「クライアント オペレーション プロファイルを設定する」の章を参照してください。

HPCA Agent が既にデバイスにインストールされている場合は、args.xml ファイルを変更して **<COP>Y</COP>** エントリを追加できます。このエントリを </ARGUMENTS> エントリの上に配置し、変更を保存します。

args.xml ファイルは、HPCA Agent がインストールされたディレクトリの \lib にあります。デフォルトは C:\Program Files\Hewlett-Packard\HPCA\Agent です。

または、コマンド ラインから radskman (あるいは、HPCA Agent 接続を実行する任意のコマンド) を実行しているときに、アクションで **COP=Y** を使用します。詳細については、『Application Manager ガイド』を参照してください。

Satellite の同期

Core CSDB へのこれらの変更が Satellite で確実に有効になるようにするために、各 Satellite コンソールから同期を実行します。

パッチ管理の設定

パッチ管理が含まれるように HPCA 環境を設定する前に、HPCA データベースが適切に設定されていることを確認してください。詳細については、『HP Client Automation Core および Satellite 入門およびコンセプト ガイド』を参照してください。

パッチ管理を実装するには、Core Server と Satellite Server を設定した後に Core コンソールを使用してベンダーや取得に関連した設定を行い、パッチ取得を開始する必要があります。

HPCA を使用して、Microsoft、RedHat、SuSE のパッチや HP Softpaq を配布および管理します。次の手順を使用して、サーバー アーキテクチャを設定します。

- パッチおよびインベントリ レポート データのための SQL データベースを作成します。
- ODBC DSN を定義します。
- Core Server をインストールし、次の設定を行います。
  - インフラストラクチャ管理
  - パッチ管理

— ポリシー (外部ポリシー ディレクトリを使用している場合)

コア コンソールで Patch ODBC 設定が保存されると、Core Server でパッチ管理データベースと Core Configuration Server Database 間の最初の同期が自動的に実行されます。

- Satellite Server をインストールします (推奨)。

上のタスクを完了すると、パッチ管理のための HPCA Server 環境が作成されます。

パッチ管理の管理タスク

1 Core のインストール中にパッチを有効にします。

2 コンソールの [設定] タブから、すべてのパッチ管理の設定を完了します。

— 必要に応じて、Microsoft、RedHat、および SuSE のパッチを取得するための取得ジョブを作成します。

Microsoft のパッチには、メタデータを使用したパッチ管理を有効にすることをお勧めします。この機能によって、パッチを取得するためにかかる時間や Core Configuration Server に対する全体的な負荷が削減されます。詳細については、325 ページの「メタデータを使用したパッチ管理」を参照してください。

— HP Softpaq は、事前設定された 1 つの取得ジョブを使用します。このジョブを利用するには、各デバイスの HP Softpaq SysID を HP Softpaq のための取得設定に自動的に追加できるように、HP の管理対象デバイスに対してインベントリを実行します。

3 Core コンソールの **[オペレーション]** タブから、パッチ取得を実行します。

4 パッチを取得して Core CSDB にパブリッシュした後、スケジュールされたジョブまたは Satellite コンソールのオペレーション タスクのいずれかを使用して、Core Server と Satellite Server のコンテンツを同期します。

— Core コンソールの [管理] タブを使用して、Core Server と Satellite Server のコンテンツを同期するためのジョブを作成して実行します。

— Satellite コンソールの **[オペレーション]** タブを使用して、Core Server と Satellite Server を同期します。Satellite コンソールは、**http://***satellite_hostname***:3466** でアクセスできます。

5 次回のエージェント接続時に、どのデバイスにどのブリテンを適用できるかを検出するためのパッチ スキャンが実行されます。パッチ スキャンの結果を表示するには、[ダッシュボード] タブおよび [レポート] タブを使用します。

6 管理対象デバイスにブリテンのエンタイトルメントを設定するためのポリシーを適用します。適用可能なパッチは、ユーザーの介入なしに配布されます。管理対象デバイスのパッチ適用状況ステータスを表示するには、[ダッシュボード] タブおよび [レポート] タブを使用します。

設定ファイルの変更に関する制限

Core Server と Satellite Server にインストールされているコンポーネントの設定ファイルは、いずれもカスタマイズすることはお勧めしません。

HPCA の Core Server と Satellite Server の機能の環境は、従来の HPCA インフラストラクチャ サーバー環境とは若干異なります。

Patch Manager の設定ファイルを変更するように指示している『Patch Manager インストールおよび設定ガイド』の手順には従わないでください。

さらにサポートが必要な場合は、HP カスタマー サポートにお問い合わせください。

オペレーティング システム イメージの配布

HPCA を使用して、オペレーティング システム イメージを配布および管理できます。これを行うには、次の手順を実行することをお勧めします。

1 Core Server で OS Manager サービスを有効にします。

— コア コンソールの [設定] タブ、[OS 管理] オプション、[設定] 領域で、**[有効]** を選択します。

このガイドの「オペレーション」、「設定」、および「エンタープライズの管理」の章では、コア コンソールでの OS Manager の設定についてさらに詳細に説明しています。

2 デフォルトの Core Server 名 (ゾーン) の **HP** をそのままにします。

3 少なくとも 1 つの Satellite Server で OS Manager サービスを有効にします。

— Satellite コンソールの [設定] タブ、[オペレーティング システム] 領域で、**[有効]** を選択します。

このガイドの「設定」の章では、Satellite コンソールでの OS Manager の設定についてさらに詳細に説明しています。

これで、HPCA Server 環境が、デフォルトの設定で OS Manager を使用するようにセットアップされました。

Core サーバーと Satellite Server の機能

HPCA Server は、次の OS Manager 関連の機能を実行します。

- Core Server は、次の目的に使用されるツールとサービスをホストします。
  - 権限を持つ CSDB にオペレーティング システム イメージをパブリッシュする。
  - コンソールで OS Manager 管理タスクを実行する。
  - ポリシー エンタイトルメントを作成する。
- Satellite Server に OS Manager Server と Proxy Server のロールが設定されていることが前提になります。Satellite Server は、Configuration Server からのオペレーティング システム イメージに対するリクエストを処理し、これらのイメージのリソースを管理対象デバイスに提供します。
  オペレーティング システム イメージを Core CSDB にパブリッシュしたら、Satellite コンソールの **[オペレーション]** タブを使用してオペレーティング システム イメージのリソースを同期 し、Satellite Server にプレロードします。

HPCA OS Manager に関する注意事項

- デフォルトでは、OS Manager が Core Server または Satellite Server にインストールされると、OS Manager は Linux サービス OS を使用するように設定されます。サービス OS として WinPE を実行するようには設定されません。
  デフォルトのサービス OS として WinPE を使用するように環境を変換するには、『OS Manager ガイド Windows 用』の第 3 章を参照してください。
- HPCA Thin Client サーバーは、HPCA Console を介してインストールできます。また、そこで有効にしたり、無効にしたりすることもできます。
- OS Manager に固有の SAP 情報については、『HPCA OS Manager System Administrator ユーザー ガイド』を参照してください。

『HPCA OS Manager System Administrator ガイド』に関する注意事項

『OS Manager ガイド』には、Core Satellite 環境での OS Manager の設定に必要な追加情報が含まれています。このガイドは、HPCA Core および Satellite のドキュメントとともに使用してください。ガイドに記載されている一部の情報に関連した重要な注意事項を次に示します。

- 「サーバー アーキテクチャのインストールと設定」の章は、コア Satellite 環境での OS Manager には関連がありません。
- Core Server と Satellite Server に自動的にインストールされるコンポーネントの設定ファイルのカスタマイズや変更について説明しているすべてのセクションの情報を無視してください。
- Core Server および Satellite Server にインストールされる**シン クライアント サーバー**は、『OS Manager ガイド』では **Mini Management Server** と呼ばれています。

アウトバンド管理の有効化

アウトバンド管理 (OOBM) とは、次のいずれかの状態にあるコンピュータ上で実行される操作のことを指します。

- 接続されているが、アクティブに実行されていない (オフ、スタンバイ、休止)
- オペレーティング システムがロードされていない (ソフトウェアまたはブートの失敗)
- ソフトウェア ベースの管理エージェントが使用できない

HPCA Console は、**Intel vPro** および **DASH** 対応デバイスの OOBM をサポートしています。

このセクションでは、HPCA OOBM の概要について説明します。HPCA OOBM の特徴および機能の詳細については、『HPCA Out of Band Management ユーザー ガイド』を参照してください。

機能

HPCA Console の OOBM 機能を次に示します。

- vPro テクノロジを使用した PC や DASH 標準の実装を含む PC のハードウェア ベースの管理機能を利用します。
- ハードウェアおよびソフトウェアのインベントリの機能を強化して、デスクサイドに向かう必要性を減らします。
- 選択的なネットワーク分離を可能にする、vPro デバイスのためのシステム防御機能を提供します。
- vPro システム上で実行されているローカル エージェントの監視を可能にする、エージェント存在機能を提供します。

- vPro デバイスのための、オペレーティング システムに依存しない、改ざん防止対策機能のあるワーム封じ込めシステムを提供します。
- **HTTP** (**Hypertext Transfer Protocol**) 認証と **TLS** (**Transport Layer Security**) を介したセキュアな通信チャネルを提供します。

設定タスク

このセクションでは、HPCA Console の **[設定]** タブで実行される、管理者ベースのいくつかのタスクについて簡単に説明します。HPCA 管理者は、これらの設定タスクを OOB デバイスを管理するための準備として実行する必要があります。これらのタスクの詳細については、『HPCA Out of Band Management ユーザー ガイド』を参照してください。

- **アウトバンド管理の有効化** : OOBM タスクを実行するために HPCA 管理者が実行する必要のある最初のタスクです。

  [アウトバンド管理] の下で、**[使用可能性]** をクリックします。

- **デバイス タイプの選択** : HPCA Console では、[DASH デバイス]、[vPro デバイス]、[両方] という 3 つのデバイス タイプの選択肢が提供されます。

  [アウトバンド管理] の下で、**[デバイス タイプの選択]** をクリックします。

- **vPro システム防御の管理** : このオプションは、管理対象のデバイス タイプとして [vPro デバイス] が選択された場合にのみ表示されます。

  [アウトバンド管理] の下で、**[vPro システム保護の設定]** をクリックします。

  システム防御設定は、DASH デバイスには適用されません。

オペレーション タスク

このセクションでは、HPCA の管理者およびオペレータ ロールで実行できるいくつかのタスクについて簡単に説明します。これらの OOB デバイス管理タスクは、HPCA Console の **[オペレーション]** タブで、HPCA 管理者または*オペレータ*によって実行されます。これらのタスクの詳細については、『HPCA Out of Band Management ユーザー ガイド』を参照してください。

- **デバイスのプロビジョニング** : HPCA が vPro デバイスを検出および管理できるようにするには、事前にそれらのデバイスをプロビジョニングしておく必要があります。

[アウトバンド管理] の下で、**[vPro プロビジョニング]** をクリックします。

DASH デバイスのみを管理することを選択した場合、このオプションはこれらのデバイスに関連しないため、**[オペレーション]** タブには表示されません。

- **デバイスの管理** : HPCA 管理者およびオペレータは、複数の OOB デバイスおよび個々の OOB デバイスを管理できます。

  [アウトバンド管理] の下で、**[デバイス管理]** をクリックします。

- **グループの管理** : HPCA 管理者およびオペレータは、vPro デバイスのグループを管理できます。

  [アウトバンド管理] の下で、**[グループ管理]** をクリックします。

- **警告の表示** : HPCA 管理者およびオペレータは、プロビジョニング済みの vPro デバイスに警告の予約を割り当てていれば、それらのデバイスによって生成された警告を表示できます。

  [アウトバンド管理] の下で、**[警告の通知]** をクリックします。

3 セキュリティとコンプライアンスの管理

HPCA のセキュリティとコンプライアンス機能により、お使いの環境全体のセキュリティの脆弱性、設定の適用状況、およびセキュリティ ツールのパフォーマンスを監視および管理できます。この章は、次の各トピックで構成されています。

はじめに

HPCA のセキュリティとコンプライアンスの管理ソリューションには次の領域があります。

- 脆弱性管理 44 ページ
- 適用状況管理 46 ページ
- セキュリティ ツール管理 49 ページ

この章では、それぞれの領域の概要について説明します。

脆弱性管理

脆弱性管理は、企業内のソフトウェアのセキュリティと脆弱性の問題を識別、特定、および修正するプロセスです。このプロセスには、次の 3 つの主な手順があります。

1 最新の脆弱性定義およびスキャナを入手する。

2 企業内の管理対象デバイスをスキャンして脆弱性の有無を確認する。

3 スキャン済みのデバイスの脆弱性評価レポートを作成する。このレポートには、企業全体の要約情報が含まれます。

次の用語は、HPCA の脆弱性管理ソリューション全体を通して使用されます。

表 2　脆弱性管理用語

期限	定義
脆弱性	システム、システムの設定、またはシステム ソフトウェアの弱点です。この弱点によりシステムの整合性が危険にさらされ、リソースへの不正アクセスを可能にします。
発覚	発覚は、環境内のさまざまな脆弱性の危険度を意味します。また、システムの攻撃または不正利用に使用される恐れがある情報または機能をハッカーに渡すソフトウェアの一部という意味としても使用されます。

表 2　脆弱性管理用語

期限	定義
CVE	Common Vulnerabilities and Exposures の略称です。 CVE は、セキュリティの脆弱性および発覚に関する公開情報の共通名 (CVE 識別子) の辞書です。 CVE は 1999 年に開始されました。現在、米国国土安全保障省が出資し、MITRE Corporation が管理しています。 詳細については、**http://cve.mitre.org**
NVD	National Vulnerability Database の略称です。 NVD は、米国政府が運用する標準ベースの脆弱性管理データのリポジトリです。このデータにより、脆弱性管理、セキュリティ管理、および適用状況管理の自動化が可能になります。 詳細については、**http://nvd.nist.gov** を参照してください。
CVSS	Common Vulnerability Scoring System の略称です。 CVSS は、標準の重大度スコア付与システムで、セキュリティ脆弱性に関する情報を提供します。CVSS には、Base (基本)、Temporal (現状)、および Environmental (環境) の 3 種類の評価基準があります。 詳細については、次の Web サイトを参照してください。 **http://www.first.org/cvss/index.html**

表 2　脆弱性管理用語

期限	定義
OVAL	Open Vulnerability and Assessment Language の略称です。 OVAL は、セキュリティ情報とシステムの詳細をエンコードして転送するために使用する標準です。 CVE は、すべての既知の脆弱性のカタログ化を目的としています。一方、OVAL は特定の脆弱性の識別方法を記述することを目的としています。 詳細については、次の Web サイトを参照してください。 **http://oval.mitre.org/oval/about**

適用状況管理

適用状況管理は、企業内の管理対象クライアント デバイス上のソフトウェア設定に関する問題を識別、特定、および修正するプロセスです。このプロセスには、次の 3 つの主な手順があります。

1　最新の適用状況ベンチマークおよびスキャナを入手する。

2　企業内の管理対象クライアント デバイスをスキャンして、関連ポリシーまたは適用状況ベンチマークで定義された規制基準が設定に適用されているかどうかを判別する。

3　適用状況スキャンの結果レポートを作成する。このレポートには、企業全体の要約情報が含まれます。

この時点で、管理者は識別されたすべての設定問題の解決に取り組むことができます。

次の用語は、HPCA の適用状況管理ソリューション全体を通して使用されます。

表 3　適用状況管理用語

期限	定義
CCE	Common Configuration Enumeration の略称です。 CCE は、ソフトウェア セキュリティの設定に関する問題 (アクセス制御設定、パスワード ポリシー設定など) の名前の辞書です。システム設定に関する問題に一意の識別子を付与することにより、CCE は複数の情報ソースおよびツールに存在する設定データの迅速で正確な関連付けを可能にします。 CCE は現在 MITRE Corporation が管理しています。 詳細については、**http://cce.mitre.org** を参照してください。
FDCC	Federal Desktop Core Configuration の略称です。 FDCC は、米国行政管理予算局 (Office of Management and Budget、OMB) によってすべての米国政府機関に義務付けられたセキュリティ設定です。現在、Microsoft Windows Vista および XP オペレーティング システムに対する FDCC が存在します。 Windows Vista の FDCC は、Microsoft Vista セキュリティ ガイドに基づいています。このガイドは、米国国防情報システム局 (Defense Information Security Agency、DISA)、米国国家安全保障局 (National Security Agency、NSA)、および米国標準技術局 (NIST) により共同開発されました。このガイドには、DISA、NSA、および NIST で合意された Windows Vista プラットフォームの推奨設定が反映されています。 Windows XP の FDCC は、NIST SP 800-68 内のセキュリティ特化 - 機能制限 (Specialized Security-Limited Functionality、SSLF) 勧告の米国空軍カスタマイズ版および Microsoft の Internet Explorer 7.0 セキュリティ ガイドにおける推奨事項の米国国防総省 (Department of Defense、DoD) カスタマイズ版に基づいています。 また、Windows XP ファイアウォール、Windows Vista ファイアウォール、および Internet Explorer 7 の FDCC ベンチマークも存在します。 詳細については、**http://nvd.nist.gov/fdcc** を参照してください。

表 3　適用状況管理用語

期限	定義
SCAP	Security Content Automation Protocol の略称 (読み : エスカップ) です。 SCAP は、相互運用および自動化が可能なセキュリティ標準のフレームワークです。米国標準技術局 (National Institute of Standards and Technology、NIST) により確立されています。SCAP により、組織はセキュリティの監視、脆弱性管理、およびセキュリティ ポリシー適用状況の評価を自動化できます。 SCAP には次の仕様が採用されています。 • CVE (44 ページの「脆弱性管理」を参照) • CCE (上述) • Common Platform Enumeration (CPE)。ハードウェア、オペレーティング システム (OS)、およびアプリケーション製品の名称基準です。 • Extensible Configuration Checklist Description Format (XCCDF)。OS およびアプリケーション プラットフォームで使用される、構造化された一連のセキュリティ設定ルールの XML 仕様です。 • OVAL (44 ページの「脆弱性管理」を参照) • CVSS (44 ページの「脆弱性管理」を参照) SCAP では XML ベースの標準が使用されているため、人間と機械の両方で SCAP のコンテンツを判読できます。 NIST により、National Vulnerability Database (NVD) が供給するリポジトリを介して、脆弱性や製品の列挙識別子などの SCAP のコンテンツが提供されます。 詳細については **http://nvd.nist.gov/scap.cfm** を参照してください。

SCAP では、一連の適用要件を、**ベンチマーク** (例 : FDCC-Windows-Vista) と呼ばれるものにグループ化できます。ベンチマークは改訂が可能です。ベンチマークが改訂されると、新しいバージョンが与えられます。

SCAP 要件の各セットは、さらに特定の**プロファイル**に細分化されます。プロファイルは、ベンチマーク内の異なる適用レベルの定義に使用されることがあります。クライアント デバイス上で適用状況スキャンを実行すると、ベンチマークの特定のプロファイルの要件が評価されます。

プロファイルの要件は、SCAP **規則**として定義されます。各規則には、1 つ以上の自動化されたテストが含まれます。このテストは、クライアント デバイスがプロファイルの規則で指定された要件を満たしているかどうかを判定します。各規則には、クライアント デバイスがその規則に適合していない場合に企業が受ける影響と発覚の度合いに基づいて重みが割り当てられます。クライアント デバイス上で適用状況スキャンを実行すると、合格および不合格の適用状況規則の数が反映されたスコアが確定されます。このスコアは、特定のベンチマーク プロファイル (SCAP チェックリスト) に対するデバイスの適用状況を表します。

ベンチマーク、プロファイル、および規則は、すべて SCAP **データストリーム**と呼ばれるファイルの集合として提供されます。これらのファイルは、HPCA の適用状況スキャナなどの SCAP 対応ツールで読み取られます。

セキュリティ ツール管理

HPCA では、存在するセキュリティ ツールのタイプを確認し、検出された製品に関する関連情報を収集するために、企業内の管理対象クライアント デバイスをスキャンできます。次のタイプのセキュリティ製品がサポートされます。

- スパイウェア対策ツール
- ウイルス対策ツール
- ソフトウェア ファイアウォール

HPCA では、各クライアント デバイスについてインストールされている特定のセキュリティ製品、有効なセキュリティ製品、およびウイルス対策とスパイウェア対策のスキャンの最新の実行日時が判別されます。また、クライアント デバイス上のウイルスおよびスパイウェア定義の最新の更新日時が判別されます。

収集された情報は集計されて、セキュリティ ツール管理ダッシュボードおよび関連レポートに表示されます。

HPCA は、実行可能なセキュリティ ツール スキャナを提供する HP Live Network と統合されます。このスキャナは、新しいセキュリティ製品のサポートが追加されるたびに HP Live Network 経由で更新されます。

セキュリティ ツール管理スキャナには、さまざまなセキュリティ製品に関する情報が組み込まれています。この情報は、新しい製品が検出可能製品リストに追加されるたびに更新されます。

HPCA と HP Live Network

HPCA インストールには、デモ用に機能が限定された HP Live Network の一部のセキュリティおよび適用状況管理コンテンツが付属しています。最新の定義とスキャナを入手して HPCA Console でセキュリティおよび適用状況管理機能を使用するには、HP Live Network サブスクリプションを購入してアクティブ化する必要があります。アクティブ化すると、ユーザー ID、パスワード、およびコンテンツ サーバーの URL が通知されます。これらを使用して、[設定] タブで Live Network 設定を行います。

サブスクリプションに付随する HP Live Network コンテンツ サーバーの URL は、Live Network 設定の設定ページに表示されるデフォルトの URL と異なる場合があります。サブスクリプションに付随する URL を使用してください。

HP Live Network 認証情報を入手したら、Live Network 設定を設定できます。詳細については、281 ページの「Live Network」を参照してください。

HP Live Network サブスクリプションについての詳細は、当社の営業担当者にお問い合わせください。

ライセンスの要件

HPCA で脆弱性管理、適用状況管理、およびセキュリティ ツール管理の各機能を使用するには、次のものが必要です。

- HPCA Security Manager および HPCA Compliance Manager のライセンス
- HP Live Network のサブスクリプションと有効なログイン認証情報
- HPCA Patch Manager のライセンス

これらのアイテムがない場合、関連するダッシュボードには何も表示されません。最初の 2 つのアイテムは脆弱性管理、適用状況管理、およびセキュリティ ツール管理の各ダッシュボードに必要です。Patch Manager のライセンスは、パッチ管理ダッシュボードに必要です。

各ダッシュボードには、さらに ソフトウェアの前提条件 が必要です。

HPCA ソフトウェアに含まれているスキャン サービスのデモ版には、HP Live Network の認証情報は必要ありません。ただし、このデモ版には、セキュリティ ツール管理用のスキャナは含まれていません。HPCA でセキュリティ ツール管理を実行するには、アクティブな HP Live Network サブスクリプションが必要です。

ソフトウェアの前提条件

HPCA のセキュリティおよび適用状況管理ソリューションには、少なくとも次の前提条件が必要です。

- Configuration Server および Configuration Server Database (CSDB) がインストールされ、適切に設定されている。
- Messaging Server で、`core.dda` モジュールが有効化されている。収集されたスキャン データは、インベントリ データとともに `core.dda` で処理されます。詳細については、『Messaging Server ガイド』を参照してください。
- 次のレポート パックが有効になっている。これらは、ダッシュボードの機能をすべて利用するために必要です。
  - インベントリ管理レポート パック。インベントリ管理レポートおよび HPCA 操作ダッシュボードを駆動します。
  - 脆弱性管理レポート パック。脆弱性管理レポートおよびダッシュボードを駆動します。
  - 適用状況管理レポート パック。適用状況管理レポートおよびダッシュボードを駆動します。
  - セキュリティ ツール管理レポート パック。セキュリティ ツール管理レポートおよびダッシュボードを駆動します。
  - パッチ管理レポート パック。パッチ管理レポートおよびダッシュボードを駆動します。

  これらのレポート パックの有効化についての詳細は、『Reporting Server ガイド』を参照してください。

Core および Satellite のインストールでは、ここに挙げられている前提条件は自動的に対応されています。

従来の CAE インストールでは、これらのすべての前提条件が明示的に満たされていることを確認する必要があります。

HPCA のセキュリティ管理および適用状況管理の動作

HP Client Automation によって、セキュリティおよび適用状況管理ソリューションが提供され、企業内の管理対象デバイス上のセキュリティ脆弱性および設定ポリシー適用に関する問題を検出できます。このソリューションにより、関連リスクの重大度および範囲を迅速に評価できるようになります。その後、検出された問題の修正に取り組むことができます。

HPCA は、HP Live Network と統合されています。HP Live Network は、入手可能な最新のセキュリティ脆弱性および規制適応情報の追跡、優先順位付け、および分析を行うサブスクリプション サービスです。55 ページの図 1 を参照してください。

HPCA Console を使用して、定期的に新しいセキュリティおよび適用状況に関するコンテンツを HP Live Network から自動的にダウンロードするように HPCA を設定できます。これにより、手動によるプロセスは不要になります。このコンテンツには、次が含まれます。

- クライアント デバイス用のセキュリティおよび適用状況スキャナ
- 個々の脆弱性に関する詳細情報 (説明、開示日、重大度レベル、使用可能なベンダー製パッチまたはブリテンなど)
- NIST から入手可能な最新の FDCC SCAP データ ストリーム

次に、HP Live Network のコンテンツは、配布可能なサービスとして Configuration Server Database (CSDB) に強制配布されます。続いて、指定したスケジュールおよびポリシーに従って管理対象デバイスでスキャンが実行され、セキュリティおよび適用状況の問題が検出されます。このコンテンツは、レポート データベースにも強制配布されます。

HPCA Console では、企業のセキュリティおよび適応状況のステータスが一目でわかるダッシュボードが表示されます。また、パッチ管理ダッシュボードも表示され、企業全体にわたるパッチ ポリシーの適用状況をすばやく評価できます。詳細については、83 ページの「ダッシュボードの使用」を参照してください。

HPCA 7.50 では、次のオペレーティング システムを実行している管理対象クライアントに対するセキュリティおよび適用状況のスキャンがサポートされています。

表 4　サポートされているプラットフォーム

スキャン タイプ	サポートされているオペレーティング システム
脆弱性	Windows 2000、Windows 2003、Windows 2008、Windows XP、および Windows Vista
適用状況	Windows XP および Windows Vista (FDCC 標準はデスクトップ デバイスにのみ適用されるため)
セキュリティ ツール	Windows XP、Windows Vista、WIndows 2003、および Windows 2008

HP Live Network コンテンツが更新されるしくみ

HP Live Network では、次の 2 種類のセキュリティとコンプライアンスの管理コンテンツを提供します。

- データ – 脆弱性定義と SCAP データ
- スキャナ – 脆弱性スキャナ、適用状況スキャナ、およびセキュリティ ツール管理スキャナ

HP Live Network コンテンツにアクセスするために、HPCA は HP Live Network コネクタを使用します。このコネクタは、最初にどのコンテンツが使用可能かを判断し、次に HP Live Network サブスクリプション サイトから適切なコンテンツをダウンロードします。

デフォルト バージョンの HP Live Network コネクタは、HPCA のインストール時にインストールおよび設定されます。このコネクタは自己更新されます。すべてのコネクタへの変更は、HP Live Network コンテンツを更新したときに自動的にダウンロードされます。

何らかの理由で HP Live Network コネクタを再インストールする場合は、いつでも新しいコピーをダウンロードできます。236 ページの「HP Live Network コネクタのダウンロード」を参照してください。

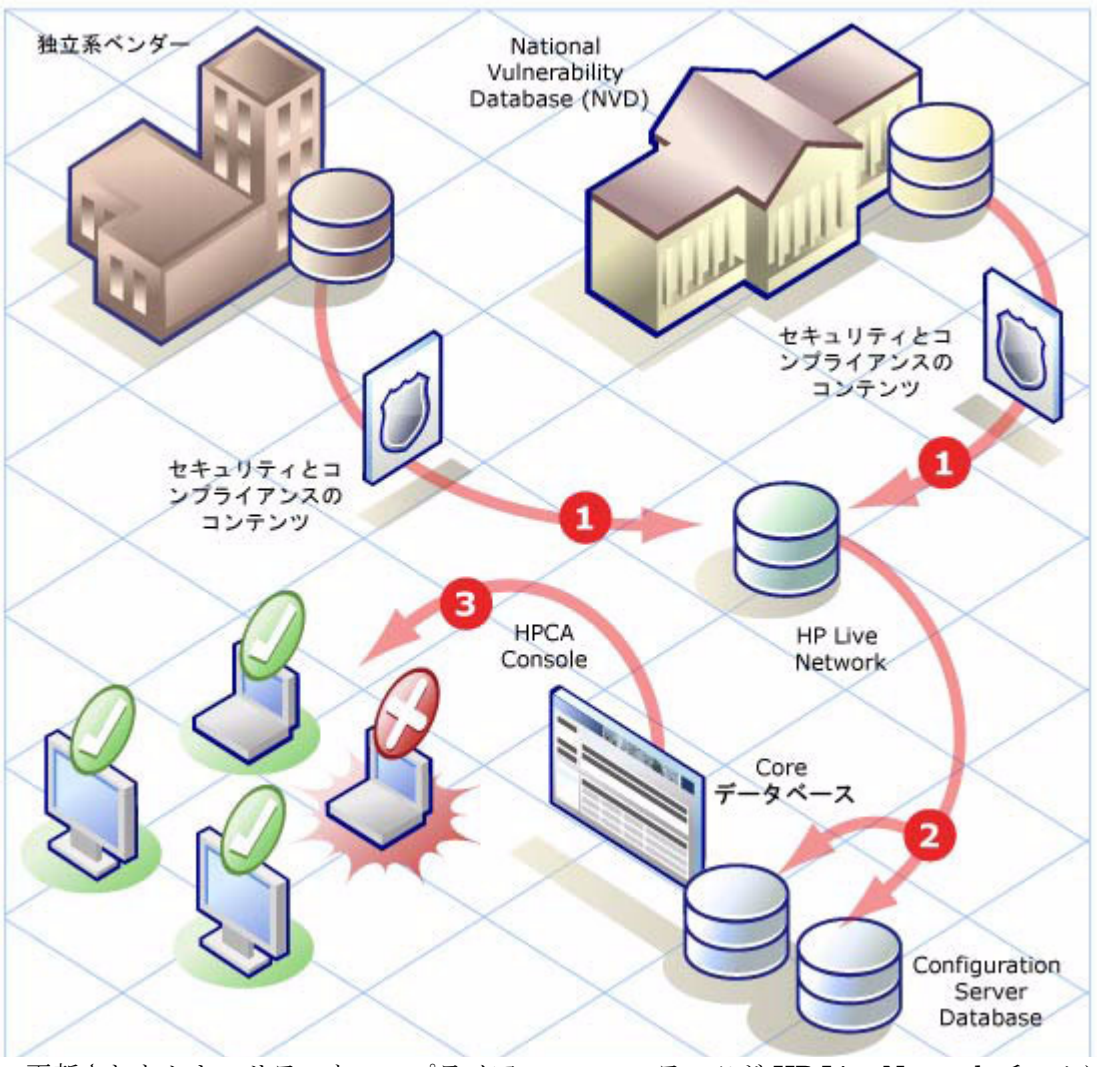
HP Live Network コネクタは HP Live Network への認証を実行し、セキュリティとコンプライアンスの管理コンテンツをダウンロードします。このコネクタ自体は、HPCA インフラストラクチャに何もインストールしません。HPCA は、更新された HP Live Network コンテンツのロードを管理します。

HPCA セキュリティとコンプライアンスの管理コンテンツを更新すると (HP Live Network からまたはファイル システムからのいずれの場合も)、次の 3 つの処理が実行されます。

1. 更新されたスキャナとデータの両方が一時ディレクトリにコピーされます。
2. データが一時ディレクトリから Core データベースにプッシュされます。これにより、詳細な定義レポートが作成され、収集されたスキャン結果がデータベースによって処理されます。
3. データとスキャナの両方が CSDB にロードされます。

その後、セキュリティ ポリシーが設定されたクライアント デバイスが CSDB の SECURITY ドメインへの接続を確立すると、このデータとスキャナがそのクライアント デバイスに配布されます。この時点で、そのクライアント デバイスがスキャンされます。次に、スキャンの結果が Core データベースに送信されます。

図 1　HPCA でのセキュリティとコンプライアンスの管理



1　更新されたセキュリティとコンプライアンスのコンテンツが HP Live Network チームによってダウンロードされ、分析されます。必要に応じて、HP Live Network スキャナが更新されます (このようなケースはまれです)。

2　更新されたセキュリティとコンプライアンスのコンテンツ (HP Live Network スキャナなど) が、HPCA によって HP Live Network からダウンロードされ、CSDB と Core データベースにパブリッシュされます。

3　クライアント デバイスは、セキュリティとコンプライアンスの問題がないかどうか HPCA によってスキャンされます。

CSDB にロードされたセキュリティとコンプライアンスのコンテンツには、「サービス」定義と「マスター」定義の両方が含まれています。サービス定義はスキャン サービスに関連しており、スキャンを実行するためにプラットフォーム固有の Agent に配布されます。マスター定義は、コンテンツをテスト環境からプロダクション環境に移動するときに使用されます (78 ページの「テスト環境からプロダクション環境への HP Live Network コンテンツの移動」を参照)。

脆弱性スキャンの場合、マスター定義には、National Vulnerability Database (NVD) CVE 定義と HPCA に必要なプラットフォーム固有の Open Vulnerability Assessment Language (OVAL) 定義が含まれます。HPCA による脆弱性管理レポートの作成を可能にするのは、各プラットフォームのこれらの 2 つの定義セットの組み合わせです。

適用状況スキャンの場合、マスター定義に SCAP 形式の適用状況ベンチマークが含まれます。

セキュリティ ツール管理スキャンの場合、定義はありません。スキャナは、単にサポートされているすべてのセキュリティ ツールの存在を検索し、各ツールが有効になっているかどうかを判断します。ウイルス対策およびスパイウェア対策ツールの場合、スキャナは、各ツールで最後に定義が更新された時間や最後に完全なシステム スキャンが実行された時間も判断します。

スキャン サービスの詳細

Configuration Server Database (CSDB) には、セキュリティとコンプライアンスのスキャンを行うサービスを含む SECURITY ドメインが含まれています。HPCA をインストールすると、SECURITY ドメインで次のサービスが使用可能になります。

< 脆弱性の検出 (限定版)>

<FDCC 1.0 OS 適用状況の検出 >

HP Live Network コンテンツの更新を実行すると、その他のサービスが使用可能になります。これらのサービスを使用して、Agent システム上でセキュリティとコンプライアンスのスキャンを実行し、結果をレポート データベースに送り返すことができます。

セキュリティ ツール管理スキャン サービスは、最初の HP Live Network コンテンツの更新を実行するまで使用可能になりません。

< セキュリティ ツールの検出 >

最初の HP Live Network コンテンツの更新を実行すると、脆弱性スキャナ サービスの名前が次のように変更されます。

< 脆弱性の検出 >

HPCA に同梱されるスキャナのバージョンには、脆弱性定義のサブセットのみが含まれているため、「限定版」というラベルが付いています。最初の更新を実行すると、HPCA に認識される完全な定義のセットをスキャンに使用できるようになります。

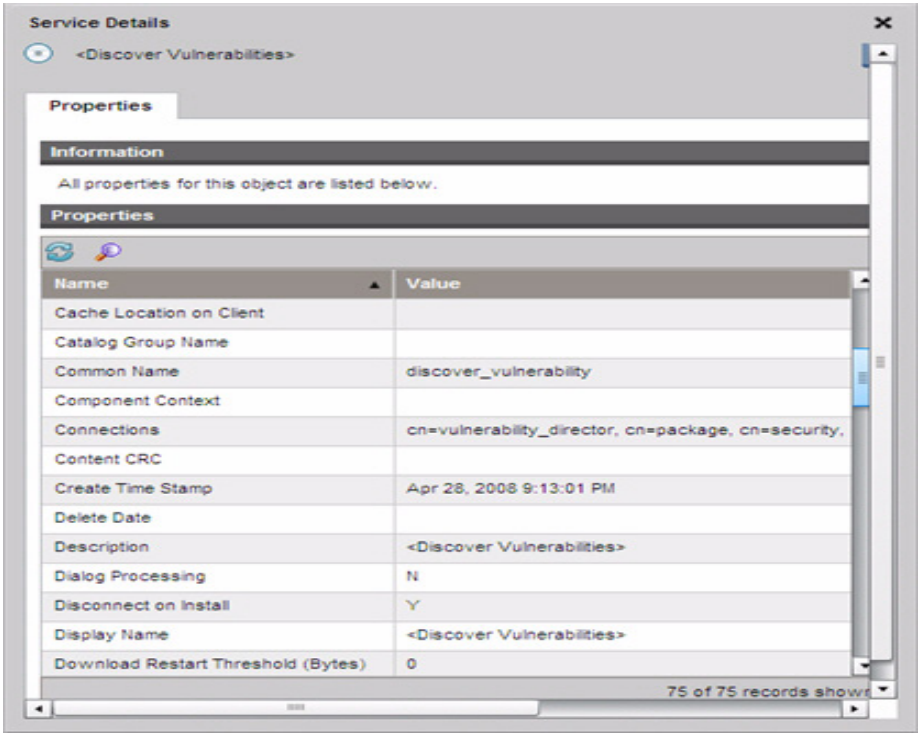
サービスの名前は変更されますが、確立されているエンタイトルメントは変更されません。

スキャン サービスを表示するには

1. HPCA Console にサインインします。
2. **[管理]** タブをクリックします。
3. 左側のペインで、**[サービス]** をクリックします。使用可能な CSDB ドメインの一覧が表示されます。
4. 左側のペインで、**[セキュリティ]** をクリックします。
5. [カタログ] ペインで、セキュリティ サービスのいずれかをクリックします。次に例を示します。
   - SECURITY.ZSERVICE.DISCOVER_VULNERABILITY
   - SECURITY.ZSERVICE.DISCOVER_FDCC_1-0_OS

— SECURITY.ZSERVICE.DISCOVER_SECTOOLS_AV_AS_FW

[サービス詳細] ウィンドウが表示されます。サービスの詳細については、153 ページの「サービス情報」を参照してください。



この図は、DISCOVER_VULNERABILITY サービスを示します。セキュリティ ツール管理の DISCOVER_SECTOOLS_AV_AS_FW サービスと、DISCOVER_FDCC_1-0_OS などの適用状況管理サービスはよく似ています。

CSDB には最初、脆弱性スキャンの < 脆弱性の検出 (限定版)> と呼ばれる PRIMARY.SECURITY.ZSERVICE のインスタンスと、適用状況スキャンの <FDCC 1.0 適用状況の検出 > と呼ばれる別のインスタンスが含まれています。HP Live Network コンテンツに他のベンチマークが追加されると、新しいインスタンスが使用可能になります。最初の HP Live Network の更新を実行した後、< セキュリティ ツールの検出 > サービスが追加されます。

CSDB には、ターゲット システムに対して脆弱性スキャナを実行する時期を決定する、日単位の脆弱性スキャンと呼ばれる PRIMARY.SECURITY.TIMER のインスタンスも含まれています。別のインスタンスであるにもかかわらず、< 脆弱性の検出 > サービスは日単位の脆弱性スキャン タイマーに接続されています。

適用状況またはセキュリティ ツールのスキャンのための組み込みのタイマーはありません。ターゲット デバイスに対する定期的な適用状況とセキュリティ ツールのスキャンのスケジュールを設定する DTM ジョブをセットアップする必要があります。63 ページの「スキャンをスケジュール設定または起動する HPCA ジョブの作成」を参照してください。または、CSDB に独自の適用状況スキャン タイマーをセットアップできます。

次の例は、日単位の脆弱性スキャン サービスのパラメータのサブセットを示す Admin CSDB Editor のスナップショットです。

ZSCHDEF	Timer Parameter	DAILY(&ZSYSDATE,08:30:00,16:30:00)
ZSCHTYPE	Type [IMMEDIATE/DEFERRED]	DEFERRED
ZSCHFREQ	Frequency [PERIODIC/ONCE/RANDOM]	RANDOM

このタイマーがスキャナを直接呼び出すことはありません。タイマーが期限に達すると、radskman が SECURITY ドメインへの接続操作を実行します。これにより、ZCREATE、ZVERIFY、ZUPDATE、ZREPAIR のいずれかのメソッドが実行されます。これらのいずれかのメソッドが実行されると、ターゲット システムでスキャナが起動されます。

デフォルトでは、毎日ローカル (システム) 時間の 08:30 ～ 16:30 の間のランダムに選択された時間に実行されるようにタイマーが設定されます。

スキャン サービスを使用する前に、それらのスキャン サービスにターゲット デバイスのエンタイトルメントを明示的に設定する必要があります。詳細については、61 ページの「スキャンのスケジュール設定または起動」を参照してください。

セキュリティとコンプライアンスの管理の設定

281 ページの「Live Network」を参照してください。

一般的なセキュリティとコンプライアンス管理のタスク

このセクションには、次のタスクに関する情報が含まれています。

HP Live Network コンテンツの更新

HP Live Network サブスクリプション Web サイトから HP Live Network コンテンツ (スキャナおよびデータ) を更新するには、次の 2 つの方法があります。

- HP Live Network の [操作] ページにある [スケジュールの更新] タブを使用して、更新されたコンテンツを定期的にダウンロードするように HPCA Console を設定するか、または [すぐに更新] タブを使用して HP Live Network サブスクリプション サイトから即時に更新を開始します。

  手順の詳細については、232 ページの「Live Network」を参照してください。

- `content-update.bat` コマンド ライン ユーティリティを使用して、更新を手動で起動します。

  手順については、70 ページの「コマンド ライン ユーティリティの使用」を参照してください。

最新のスキャナとデータが確実に使用されるようにするために、HPCA ソフトウェアをインストールまたはアップグレードした後は、HP Live Network コンテンツを必ず更新してください。

新しい HP Live Network コンテンツをダウンロードするときに、単に既存サービスの更新情報を入手する場合もあれば、新しいサービスにアクセスできる場合もあります。新しいサービスを使用するには、これらのサービスにクライアントデバイスのエンタイトルメントを明示的に設定してください。

スキャンのスケジュール設定または起動

HPCA Console を使用すると、ターゲット デバイス (またはデバイスのグループ) に対して、定期的な脆弱性スキャン、適用状況スキャン、またはセキュリティ ツール スキャン (あるいは、これらの 3 つのスキャンの任意の組み合わせ) のスケジュールを設定できます。また、即時スキャンを起動することもできます。次の 2 つの手順を実行する必要があります。

1 1 つ以上のセキュリティ サービスにデバイス (またはデバイスのグループ) のエンタイトルメントを設定します。HPCA をインストールすると、SECURITY ドメインで次の 2 つのサービスが使用可能になります。

< 脆弱性の検出 (限定版)>

<FDCC 1.0 OS 適用状況の検出 >

HP Live Network コンテンツの更新を実行すると、新しいベンチマークが追加されるため、追加のサービスが使用可能になります。最初の更新を実行した後、脆弱性サービスの名前が変更され、(限定版) の修飾子が削除されます。また、最初のコンテンツを更新した後、< セキュリティ ツールの検出 > サービスも使用可能になります。

62 ページの「スキャンのためのデバイスのエンタイトルメントの設定」を参照してください。

2 [セキュリティ接続] ジョブ アクション テンプレートを使用してジョブを作成することによって、HPCA Console からスキャンをスケジュール設定または起動します。63 ページの「スキャンをスケジュール設定または起動する HPCA ジョブの作成」を参照してください。

また、1 つのターゲット デバイスから CSDB 内の SECURITY ドメインへの Agent の接続操作を実行することによって、そのデバイスに対して即時スキャンを起動することもできます。エンタイトルメントが正しく設定されたターゲット デバイスから CSDB 内の SECURITY ドメインへの Agent の接続操作が実行されると常に、スキャンが起動されます。64 ページの「ターゲット デバイスからのスキャンの開始」。

HPCA でのスキャンの実行方法については、57 ページの「スキャン サービスの詳細」を参照してください。

スキャンのためのデバイスのエンタイトルメントの設定

管理対象クライアント デバイス (またはデバイスのグループ) に対して脆弱性、適用状況、またはセキュリティ ツールのスキャンを開始するには、事前に目的のスキャン サービスに対象デバイスのエンタイトルメントを正しく設定しておく必要があります。

スキャンのためのデバイス (またはデバイスのグループ) のエンタイトルメントを設定するには

1 [管理] タブで、エンタイトルメントを設定するデバイスが含まれているゾーンを展開します。
2 1 つのデバイスのエンタイトルメントを設定する場合は、左のナビゲーション ツリーで **[デバイス]** をクリックします。デバイスのグループのエンタイトルメントを設定する場合は、**[グループ]** をクリックします。
3 エンタイトルメントを設定するデバイスまたはグループのショートカット メニューから、**[プロパティの表示 / 編集]** を選択します。新しいウィンドウである [ディレクトリ オブジェクト] ウィンドウが表示されます。
4 左のナビゲーション ツリーで、**[ポリシー]** をクリックします。
5 [ポリシー管理の起動] () ボタンをクリックして、ポリシー管理ウィザードを開きます。
6 [サービス ドメイン] の一覧から、**[セキュリティ]** を選択します。
7 1 つ以上のセキュリティ サービスの左にあるボックスを選択します。HPCA をインストールすると、次のサービスがすぐに使用可能になります。
   — SECURITY.ZSERVICE.DISCOVER_VULNERABILITY
   — SECURITY.ZSERVICE.DISCOVER_FDCC_1-0_OS
   — HP Live Network の更新を実行した後、追加のセキュリティ サービスが使用可能になります。
   たとえば、最初の更新の後、SECURITY.ZSERVICE.DISCOVER_SECTOOLS_AV_AS_FW サービスが使用可能になります。
8 **[追加]** をクリックします。
9 **[次へ]** をクリックします。
10 [ポリシー設定] の下の **[許可]** を選択します。
11 [優先度] の下で、管理対象クライアント デバイス (1 つまたは複数) に対するスキャンが実行されるときに、そのスキャンに割り当てる優先度を選択します。
12 **[次へ]** をクリックします。
13 サービス (1 つまたは複数) の設定を確認します。設定を変更する場合は、**[前へ]** をクリックします。続行する準備ができたら、**[適用]** をクリックします。

14 **[閉じる]** をクリックして、[実行ステータス] ダイアログ ボックスを閉じます。

スキャンをスケジュール設定または起動する HPCA ジョブの作成

HPCA Console から 1 つ以上のターゲット デバイスに対するセキュリティまたは適用状況スキャンをスケジュール設定または起動するには、これらのデバイスのためのジョブを作成する必要があります。[セキュリティ接続] ジョブ アクション テンプレートで作成されたジョブが実行されると、これらのデバイスのエンタイトルメントが設定された、SECURITY ドメイン内のすべてのサービスが実行されます。

スキャンをスケジュール設定または起動するジョブを作成するには

1 [管理] タブで、スキャンするデバイスが含まれているゾーンを展開します。

2 1 つのデバイスをスキャンする場合は、左のナビゲーション ツリーで **[デバイス]** をクリックします。デバイスのグループをスキャンする場合は、**[グループ]** をクリックします。

3 スキャンするデバイスまたはグループのドロップダウン メニューから **[ジョブの作成]** を選択して、ジョブ作成ウィザードを開きます。

ウィザードでは、必要なフィールドにアスタリスク (*) が付いています。

4 **[ジョブ タイプ]** の一覧から、**[DTM]** または **[通知]** のいずれかを選択します。

DTM ジョブでは、ターゲット デバイスの Agent が HPCA Core Server に接続してジョブの一覧を取得し、その後ジョブ タイマーが期限切れになったときにそれらのジョブを実行します。これらのデバイスに対して定期的なスキャン スケジュールをセットアップする場合は、DTM ジョブが最適です。

通知ジョブでは、HPCA Core Server が Agent にスキャンを実行するよう依頼します。特定のターゲット デバイスが 1 つのスキャンを特定の時刻または直ちに実行するようにする場合は、通知ジョブが最適です。

5 ジョブの **[名前]** を指定します。

6 **[ジョブの説明]** を指定します。

7 **[ジョブ アクション テンプレート]** の一覧から、**[セキュリティ接続]** を選択します。

8 **[次へ]** をクリックします。

9 ジョブのスケジュールを指定します。詳細については、161 ページの「スケジュール」を参照してください。

DTM ジョブは、1 回のみ、または定期的なスケジュールで実行できます。通知ジョブは 1 回のみ実行できるため、ウィザードのこのページではスケジュール設定の多くが無効になっています。

10 ジョブの設定を確認します。スキャンされるデバイスを表示するには、**[ターゲットの表示]** をクリックします。設定を変更する場合は、**[前へ]** をクリックします。続行する準備ができたら、**[サブミット]** をクリックします。

11 **[閉じる]** をクリックして、[実行ステータス] ダイアログ ボックスを閉じます。

HPCA ジョブの詳細については、158 ページの「ジョブを管理する」を参照してください。

ターゲット デバイスからのスキャンの開始

クライアント デバイスに最新のセキュリティとコンプライアンスの管理コンテンツをインストールし、即時スキャンを起動するには、単にそのデバイスから CSDB 内の SECURITY ドメインへのクライアント接続を実行するだけで済みます。

SECURITY ドメインへの Agent 接続を実行するには

管理対象クライアント デバイスでコマンド ライン ウィンドウを開き、次のコマンドを実行します。

```
radskman dname=security,context=m,uid=$machine,cop=y
```

このコマンドによって、そのクライアント デバイスのエンタイトルメントが設定されている、SECURITY ドメインのすべてのサービス (セキュリティとコンプライアンスの管理サービスを含む) への更新が起動されます。

脆弱性スキャンのみを起動するには、radskman コマンドに次のパラメータを追加します。

```
sname=DISCOVER_VULNERABILITY
```

適用状況スキャンのみを起動するには、radskman コマンドに、起動する適用状況サービスのための sname パラメータを追加します。次に例を示します。

```
sname=DISCOVER_FDCC_1-0_OS
```

セキュリティ ツールのスキャンのみを起動するには、radskman コマンドに次のパラメータを追加します。

```
sname=DISCOVER_SECTOOLS_AV_AS_FW
```

radskman オプションは、スペースではなく、必ずカンマで区切ってください。

クライアント デバイスで Management Agent をアンインストールしても、スキャナは削除されません。セキュリティ サービスを削除するには、まずポリシーを削除し、次にクライアント接続を実行してサービスを削除します。これを、Agent をアンインストールする前に実行します。

スキャンまたは更新の結果の表示

HPCA Console で使用可能なレポートを使用すると、脆弱性、適用状況、またはセキュリティ ツールのスキャンの結果を表示できます。また、HP Live Network コンテンツの更新のステータスを表示することもできます。レポートをフィルタして、興味のある情報のみを表示することができます。詳細については、203 ページの「レポートの使用」を参照してください。

また、ダッシュボードを使用して、グラフまたはグリッドのいずれかの形式の要約情報を検索することもできます。詳細については、83 ページの「ダッシュボードの使用」を参照してください。

脆弱性改善情報の検索

多くの場合は、脆弱性管理レポートまたはダッシュボードを使用して、特定の脆弱性の改善情報を含むベンダーのブリテンへのリンクを見つけることができます。この情報は非常に役立つ場合があり、また影響を受けるアプリケーションやオペレーティング システムのソフトウェア パッチが含まれていることもあります。

特定の脆弱性のためのベンダーのブリテンを見つけるには、多くの方法があります。次の手順は、そのための 2 つの簡単な方法を説明しています。

特定の脆弱性に対処する手順を示した改善情報を見つけるには

1 [レポート] タブで、脆弱性管理レポートの一覧を展開します。

2 [脆弱性のトップ] レポートや [アプリケーションの脆弱性] レポートなどの、脆弱性が一覧表示されたレポートを開きます。

3 特定の脆弱性の **[CVE ID]** または **[OVAL 定義]** をクリックします。この脆弱性のパッチや勧告情報を含む新しいレポートが開きます。

> ⚠ 特定の脆弱性のステータスが [不明] で、CVSS スコアが null の場合は、NVD、CVE リポジトリ、その他の任意のリソースを使用して、この脆弱性を徹底的に調査してください。この場合、HPCA はこの問題に関して確証を持てる判断を行うために必要な情報を提供できない場合があります。

4 ベンダーのサイトに移動する場合は、**[ブリテン]** 列のリンクをクリックします。

特定のデバイスの手順を示した改善情報を見つけるには

1 [レポート] タブで、脆弱性管理レポートの一覧を展開します。

2 [デバイス レポート] の下の **[スキャン実施済みデバイス]** をクリックします。

3 特定のデバイスの [詳細] ( ) アイコンをクリックします。このデバイスの次のレポートが開きます。

   — デバイスの詳細

   — デバイス脆弱性の詳細

   [デバイス脆弱性の詳細] レポートは、[重大度] または [OVAL 定義 ID] でフィルタを実行できます。詳細については、219 ページの「レポートのフィルタ」を参照してください。

4 特定の脆弱性の [詳細] ( ) アイコンをクリックします。次のレポートが開きます。

   — 脆弱性の詳細

   — 脆弱性改善の詳細

   [脆弱性改善の詳細] レポートは、[重大度]、[ベンダー]、または [CVE ID] でフィルタを実行できます。

5 ベンダーのサイトに移動する場合は、**[ブリテン]** 列のリンクをクリックします。

ブリテンにパッチが含まれている場合は、HPCA Console のパッチ管理機能を使用して、そのパッチに関連デバイスのエンタイトルメントを設定できます。

ここで説明した方法に加えて、特定の脆弱性管理ダッシュボードペインを使用して特定の脆弱性レポートに掘り下げることもできます。

適用状況の失敗に関する情報の検索

適用状況管理レポートを使用すると、最新の適用状況スキャン中に特定のデバイスで失敗した特定の規則に関する詳細情報に掘り下げられます。

上位 10 個の非適用状況デバイスのいずれかの詳細を表示するには

1 [レポート] タブで、適用状況管理レポートの一覧を展開します。

2 [エグゼクティブ レポート] の下の **[上位の SCAP 非適用状況デバイス]** をクリックします。

3 [詳細ビューに切り替え] ( ) アイコンをクリックして、データをテーブル形式で表示します。このテーブル内の各行が、特定のデバイスに対する特定の適用状況ベンチマークのテスト結果に対応しています。

4 **[失敗した規則]** 列の値をクリックします。このデバイスで失敗した、このベンチマークに関連付けられた任意の適用状況規則の一覧が表示されます。

任意のデバイスの適用状況テスト結果に関する詳細を表示するには

1 [レポート] タブで、適用状況管理レポートの一覧を展開します。

2 [デバイス レポート] の下の **[スキャン実施済みデバイス]** をクリックします。

このテーブル内の各行が、特定のデバイスに対する特定の適用状況ベンチマークのテスト結果に対応しています。

3 任意の行の [詳細] ( ) アイコンをクリックします。次のレポートが開き、関連するベンチマークとデバイスが表示されます。

- デバイス – ハードウェア、IP アドレス、オペレーティング システムなどのデバイス自体に関する情報。
- ベンチマーク (デバイス別) – 各行が、このデバイスに対してテストされたベンチマークを表します。

4 [ベンチマーク (デバイス別)] レポートで、次の 3 つの列のいずれかにある値をクリックします。

- **合格した規則**

  このデバイスで合格した、このベンチマークに関連付けられた任意の適用状況規則の一覧が表示されます。

- **失敗した規則**

このデバイスで失敗した、このベンチマークに関連付けられた任意の適用状況規則の一覧が表示されます。

— **その他のすべての規則の状態**

このデバイスで失敗も合格もしなかった適用状況規則の一覧。このカウンタは、テストから次のいずれかのコードが返されると増分されます。

- エラー
- 不明
- NOT_APPLICABLE
- NOT_CHECKED
- NOT_SELECTED
- INFORMATIONAL
- FIXED

ここで説明した方法に加えて、特定の適用情報管理ダッシュボードペインを使用して詳細情報に掘り下げることもできます。

セキュリティ ツールに関する情報の検索

HPCA では、デバイス上で実行されているウイルス対策、スパイウェア対策、およびファイアウォール ツールを検出できます。セキュリティ ツール管理ダッシュボードおよびレポートには、次の情報が表示されます。

表 5

セキュリティ ツール	入手可能な情報
ウイルス対策	インストールされている製品の名前とバージョン ツールが現在有効になっているかどうか ツールが最後に完全なシステム スキャンを実行した時間 最後にウイルス定義が更新された時間 現在の定義の特定のバージョン
スパイウェア対策	インストールされている製品の名前とバージョン ツールが現在有効になっているかどうか ツールが最後に完全なシステム スキャンを実行した時間 最後にスパイウェア定義が更新された時間 現在の定義の特定のバージョン
Firewall	インストールされているソフトウェア ファイアウォールの名前とバージョン ファイアウォールが有効になっているかどうか そのファイアウォールで使用されている規則 (HPCA 7.50 のリリース日の時点で、これは Windows XP SP2 以降および Windows Vista ファイアウォールにのみ適用されます)

詳細については、次のトピックを参照してください。

- セキュリティ ツール管理ダッシュボード 125 ページ
- セキュリティ ツール管理レポート 215 ページ

適用状況または脆弱性管理とは異なり、セキュリティ ツール管理では、追加の「定義」ファイルをダウンロードする必要はありません。デバイスにインストールされているセキュリティ ツールに関連した情報の収集に関するすべての知識がスキャナに組み込まれています。HP Live Network は必要に応じて、新しくリリースされたセキュリティ ツール (ウイルス対策、スパイウェア対策、およびファイアウォール) をサポートするようにスキャナを更新します。

高度なトピック

このセクションでは、完全にサポートされているが、毎日のセキュリティとコンプライアンスの管理アクティビティの標準的な範囲には含まれないトピックについて説明します。次のトピックが含まれます。

コマンド ライン ユーティリティの使用

HP Live Network コンテンツの更新をスケジュール設定または起動するために、[操作] タブの下の [HP Live Network] ページを使用する代わりに、次のディレクトリにある content-update.bat コマンド ライン ユーティリティを使用できます。

<*InstallDir*>\HPCA\VulnerabilityServer\bin

このディレクトリは、HPCA のインストール時には自動的に PATH に配置されません。

このユーティリティの構文は次のとおりです。

content-update.bat [-settingName <*settingValue*>]...

このコマンドには、必須設定と省略可能な設定の両方があります。content_source 設定の値を常に指定する必要があります。

コマンド ラインで指定するすべての値が、別の場所で指定された保存済み設定より優先されます (75 ページの「保存済み設定」を参照)。特定の設定の値を指定しない場合は、保存済み設定が使用されます。

content-update コマンドでは、ステータスとエラー メッセージが vms-commandline.log ファイルに書き込まれます。

content-update.bat コマンドの一般的な使用については、75 ページの「例」を参照してください。

必須設定

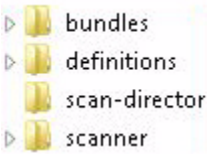
次の表は、content-update.bat コマンドの必須設定を示します。

コマンド ラインで指定するすべての値が、別の場所で指定された保存済み設定より優先されます (75 ページの「保存済み設定」を参照)。特定の設定の値を指定しない場合は、保存済み設定が使用されます。

表 6　content-update.bat の必須設定

設定	説明
content_source	この設定は必須です。更新されたコンテンツの送信元を指定します。次のいずれかの値である必要があります。 LIVENETWORK – HP Live Network コネクタを使用して HP Live Network サブスクリプション サイトからコンテンツを取得します。このオプションが機能するには、HP Live Network の設定とダウンロードされるコネクタへのパスを正しく設定する必要があります。281 ページの「Live Network」を参照してください。 FILESYSTEM – ファイル システム内のロケーションからコンテンツを取得します。その前に、HP Live Network からこのファイル システム ロケーションにそのコンテンツをダウンロードしておく必要があります。さらに、コマンド ラインまたは [操作] タブの [インフラストラクチャ管理] の下の [HP Live Network] ページのいずれかで、content_path 設定を指定する必要があります。281 ページの「Live Network」を参照してください。 CSDB_MASTER – 以前に Configuration Server Database (CSDB) にパブリッシュされたマスター コンテンツからコンテンツを取得します。このデータは、レポート データベースをロードするために使用されます。サービス配布コンテンツは再パブリッシュされません。これは、Configuration Server セキュリティ デッキのテスト版が Configuration Server の製品版にインポートされた場合の使用を対象にしています。70 ページの「高度なトピック」を参照してください。

表 6　content-update.bat の必須設定

設定	説明
content_path	HP Live Network から手動で取得したコンテンツを含むファイル システム ロケーションへの完全なパス。この設定は、content_source として FILESYSTEM を指定した場合にのみ必要です。 このパスは、ディレクトリまたは ZIP アーカイブ ファイルのいずれかを指定できます。このディレクトリ構造 (または ZIP ファイル構造) は、HP Live Network の自動更新が実行されたときに作成されたディレクトリやファイルの構造に正確に一致している必要があります。  また、これらのフォルダの下にあるサブディレクトリを自動更新の構造に一致するように複製することも必要です。 場合によっては、HP Live Network によってコンテンツのサブセットのみが更新されることがあります。この場合は、HP Live Network の更新中に、これらのディレクトリの一部が提供されない可能性があります。いずれの場合も、ファイル システムから更新する場合は、ディレクトリ構造が HP Live Network で提供される構造に一致している必要があります。

省略可能な設定

content-update.bat コマンドの次の設定は省略可能です。

コマンド ラインで指定するすべての値が、別の場所で指定された保存済み設定より優先されます (75 ページの「保存済み設定」を参照)。特定の設定の値を指定しない場合は、保存済み設定が使用されます。

表 7　content-update.bat の省略可能な設定

設定	説明
csdb_host	Configuration Server ネットワークのアドレス指定可能なシステム名。完全なホスト名、「localhost」、または IP アドレスを指定できます。
livenetwork_connector_executable	ローカル ファイル システムの HP Live Network コネクタへの完全なパス。デフォルトでは、次のようになります。 C:\Program Files\Hewlett-Packard\HPCA\LiveNetwork HP Live Network コネクタは、HP Live Network コンテンツ配布サーバーへのセキュアな接続を作成したり、更新された脆弱性管理コンテンツをダウンロードしたりするために、HPCA によって使用されるツールです。
livenetwork_connector_maxruntimeminutes	HP Live Network コネクタが、失敗したとされるまでに実行を許可される時間 (分単位)。最小値は 60 です。
livenetwork_contenturl	HP Live Network コンテンツ配布サイトの URL。HP Live Network コネクタが新しいコンテンツをダウンロードするために使用するロケーションです。
livenetwork_username	HP Live Network サブスクリプションのユーザー名。
livenetwork_password	HP Live Network サブスクリプションのパスワード。
livenetwork_proxy_http_server	HP Live Network ダウンロード サイトへの接続に使用される HTTP プロキシ サーバー。このオプションは、次の形成である必要があります。 <http|https>://<*host*>:<*port*>

表 7　content-update.bat の省略可能な設定

設定	説明
livenetwork_proxy_http_username	HP Live Network ダウンロード サイトへの接続に使用される HTTP プロキシ サーバー (存在する場合) のユーザー名。
livenetwork_proxy_http_password	HP Live Network ダウンロード サイトへの接続に使用される HTTP プロキシ サーバー (存在する場合) のパスワード。
reporting_db_databasename	レポート データベースのデータベース インスタンス名 (例 : inventory)。
reporting_db_drivername	使用するデータベース ドライバの名前 (oracle または sqlserver のいずれか)。サポートされているドライバに対応している必要があります。
reporting_db_server	レポート データベースがある、ネットワーク アドレス指定可能なサーバーの名前。
reporting_db_port	レポート データベースのポート番号。ダイナミック ポートの場合は空白にする必要があります。スタティック ポートの場合は 1 ～ 65536 の範囲の値を指定する必要があります。
reporting_db_username	レポート データベースのユーザー名。
reporting_db_password	レポート データベースのパスワード。

保存済み設定

content-update 設定いずれかの値を指定しない場合は、次の Live Network 設定ページで指定されている値がデフォルトで使用されます。

表 8　content-update.bat の保存済み設定

オプション	指定の場所
csdb_host csdb_port csdb_username csdb_password	HPCA 初回セットアップ ウィザード
livenetwork_connector_executable livenetwork_contenturl livenetwork_username livenetwork_password livenetwork_proxy_http_server livenetwork_proxy_http_username livenetwork_proxy_http_password	Live Network ページおよび [プロキシ設定] ページ
reporting_db_databasename reporting_db_drivername reporting_db_server reporting_db_port reporting_db_username reporting_db_password	HPCA のインストール時に自動的に設定される

例

例 1 – 以前に設定された HP Live Network の設定を使用してコンテンツの更新を実行する

```
content-update.bat -content_source LIVENETWORK
```

例 2 – ローカル ディレクトリからコンテンツの更新を実行する

```
content-update.bat -content_source FILESYSTEM -content_path
c:\mycontent
```

例 3 – ローカルの ZIP ファイルからコンテンツの更新を実行する

```
content-update.bat -content_source FILESYSTEM -content_path
c:\mycontent\content.zip
```

content-update.bat の利用状況の情報をすべて表示するには、<installDir>\bin ディレクトリから次のコマンドを入力します。

```
content-update.bat -?
```

HP Live Network コネクタの手動での実行

状況によっては、HPCA Core Server がインターネットにアクセスできない場合があります。この場合でも引き続き、インターネットにアクセスできるシステムを使用して HP Live Network コンテンツを更新した後、そのコンテンツを HPCA Core Server に手動で転送できます。このプロセスには、次の 4 つの手順が含まれます。

1. インターネットにアクセスできるシステムで、HP Live Network サブスクリプション Web サイトから HP Live Network コネクタを手動でダウンロードします。手順については、HP Software の営業担当者にお問い合わせください。
2. インターネットにアクセスできるシステムで、HP Live Network コネクタを実行します。
3. コンテンツを HPCA Core Server に転送します。
4. HPCA Core Server で、ファイル システムから HP Live Network コンテンツを更新します。60 ページの「HP Live Network コンテンツの更新」を参照してください。

HP Live Network コネクタを実行すると、71 ページの表 6 の content_path の説明にあるフォルダ構造が作成され、この構造内に出力ファイルが保存されます。

重要な警告

コマンド ラインから HP Live Network コネクタを実行する前に、HP Live Network コンテンツの「インポート」先のディレクトリが、コネクタの実行前に空であることを確認してください。

このディレクトリは、次のパラメータで指定されます。

```
--setting=hpca.import_directory=<LNC-output-dir>
```

この場合、<LNC-output-dir> は HP Live Network コンテンツが保存されるロケーションです。

「インポート」ディレクトリが空でない場合は、その後 FILESYSTEM オプションを使用して HP Live Network コンテンツを更新したときに、古いコンテンツが HPCA に移動される可能性があります。これにより、新しい名前を持つ新しいスキャナがリリースされた場合に古いスキャナが誤って配布されるなどの悪影響が発生することがあります。

この警告は、コマンド ラインから HP Live Network コネクタを実行する場合にのみ適用されます。HPCA Console を使用して実行する HP Live Network の更新には影響を与えません。

HP Live Network コンテンツをダウンロードするには

インターネットにアクセスできるシステムで、次のコマンドを実行します。

```
<LNC-install-dir>\bin\live-network-connector.bat
--url=https://dist.opsware.com
--http-proxy=<http|https://server:port>
--username=<user> --password=<pass> --product=hpca
--setting=hpca.import_directory=<LNC-output-dir>
--stream=security.hpca_scanner
--stream=security.hpca_oval
--stream=security.hpca_nvd
--stream=security.hpca_scap_fdcc
--stream=security.hpca_sectools_scanner
--stream=security.hpca_sectools_services
```

ここで、< かっこ > 内のすべてのアイテムは、指定する必要のある値のプレースホルダです。

この場合、<LNC-install-dir> は HP Live Network コネクタをインストールしたファイル システム ロケーションであり、<LNC-output-dir> は出力ファイルを含むフォルダ構造がコネクタによって作成されるロケーションです。たとえば、<LNC-output-dir> が c:\temp の場合、フォルダ階層は c:\temp の下に作成されます。

プロキシ サーバーの設定は、HPCA Console をホストしているシステムと HP Live Network サブスクリプション サイトの間にプロキシ サーバーが存在する場合にのみ必要です。

次の手順

インターネットにアクセスできるシステムで HP Live Network コネクタを実行した後、そのフォルダ構造を、HPCA Console をホストしている HPCA Core Server に手動でコピーする必要があります。このフォルダ構造は、ファイル システム内に直接配置することも、ZIP アーカイブ内に配置することもできます。

この時点で、このコンテンツが存在する場所を HPCA に通知する必要があります。これには、次の 2 つの方法があります。

- [操作] タブの [インフラストラクチャ管理] の下の [Live Network] ページで、**[ファイル システムから]** を選択し、フォルダ構造 (または ZIP ファイル) のロケーションを指定します。
- コマンド ラインから、`content-update` コマンドを実行し、コンテンツの送信元として `FILESYSTEM` を指定します。`content_path` 設定を使用して、フォルダ構造 (または ZIP ファイル) のロケーションを指定します。

テスト環境からプロダクション環境への HP Live Network コンテンツの移動

大規模な導入を実行する前に、小規模の管理された環境で HP Live Network コンテンツをテストすると有用な場合があります。そのためには、まず独自の「テスト」Configuration Server Database (CSDB) を含む HPCA のテスト環境を作成して、レポート データベースを「テスト」します。テストを完了した後、「テスト」SECURITY ドメインをエクスポートしてから、その CSDB コンテンツを HPCA のプロダクション環境にインポートします。

CSDB コンテンツのエクスポートやインポートに使用されるファイルは、「デッキ」と呼ばれます。

次の手順に従う前に、53 ページの「HP Live Network コンテンツが更新されるしくみ」を確認してください。

管理されたテスト環境で HP Live Network コンテンツをテストするには

1. テスト環境で、HP Live Network サブスクリプション サイトから自動的に、またはファイル システムから手動で HP Live Network コンテンツの更新を実行します。
2. スキャンを実行し、関連するレポートおよびダッシュボード ペインを確認することによって、その更新をテストします。

HP Live Network コンテンツを管理されたテスト環境からプロダクション環境に移動するには

ここに示す **raddbutil** コマンドには、カンマの後にスペースがありません。これらのコマンドをこのガイドやオンライン ヘルプから切り取って貼り付ける場合は、貼り付け操作によって付いたスペースをすべて必ず削除してください。

1 テスト CSDB に接続し、**raddbutil** ツールを使用してセキュリティ デッキをエクスポートします。

   a データをエクスポートするシステム (テスト環境) 上の Configuration Server の bin ディレクトリに移動します。

   b **RAD_MAST** ユーザーにパスワードが設定されている場合は、次のコマンドを使用します。

   raddbutil EXPORT DATA=TRUE,WALK=TRUE,
   OUTPUT=<*tempDir*>,USERID=RAD_MAST,PASSWORD=<*password*>
   PRIMARY.SECURITY

   RAD_MAST ユーザーにパスワードが設定されていない場合は、次のコマンドを使用します。

   raddbutil EXPORT DATA=TRUE,WALK=TRUE,
   OUTPUT=<*tempDir*>,USERID=RAD_MAST PRIMARY.SECURITY

   どちらの場合も、<tempDir> は、エクスポートされるファイルが保存されるテスト CSDB システム上のディレクトリです。

   詳細については、『Configuration Server ユーザー ガイド』の「Configuration Server Database Utility (RadDBUtil)」を参照してください。

2 選択したファイル転送メカニズムを使用して、セキュリティ デッキ ファイルをプロダクション CSDB システムに転送します。

3 プロダクション CSDB システム上で、raddbutil ツールを使用してセキュリティ デッキをインポートします。

   a データをインポートするシステム (プロダクション環境) 上の Configuration Server ディレクトリに移動します。

   b **RAD_MAST** ユーザーにパスワードが設定されている場合は、次のコマンドを使用します。

   raddbutil IMPORT INPUT=<*tempDir*>,COMMIT=TRUE,
   ACCEPT=A+D+U,USERID=RAD_MAST,PASSWORD=<*password*>

   RAD_MAST ユーザーにパスワードが設定されていない場合は、次のコマンドを使用します。

raddbutil IMPORT INPUT=<*tempDir*>,COMMIT=TRUE, ACCEPT=A+D+U,USERID=RAD_MAST

この場合、<tempDir> は、手順 3 でファイルが保存されたプロダクション CSDB システム上のディレクトリです。

4 プロダクション環境で、先ほどインポートしたセキュリティ デッキ内の「マスター」コンテンツを使用して、プロダクション レポート データベースをロードします。

これには、次の 2 つの方法があります。

— **タスク 1:** HPCA Console を使用する

a **[操作]** タブをクリックします。

b 左のナビゲーション メニューで、**[Live Network]** を選択します。

c **[すぐに更新]** タブをクリックします。

d **[Configuration Server から]** 更新オプションを選択します。

e **[すぐに更新]** ボタンをクリックします。

[すぐに更新] タブの詳細については、281 ページの「Live Network」を参照してください。

— **タスク 2:** content-update コマンド ライン ユーティリティを使用する

content-update.bat -content_source CSDB_MASTER

content-update コマンドの詳細については、70 ページの「コマンド ライン ユーティリティの使用」を参照してください。

いずれの場合も、コンテンツの送信元として CSDB_MASTER を使用することにより、更新ツールがレポート データベースのコンテンツのみを更新し、脆弱性、適用状況、またはセキュリティ ツール管理スキャン サービスにリンクされたパッケージへの更新の実行を迂回するように強制します。これにより、テスト環境で配布したサービス コンテンツがプロダクション環境で配布されるコンテンツに正確に一致するようになります。

セキュリティとコンプライアンスの管理に関する詳細情報

次のセクションには、HPCA Console でのセキュリティとコンプライアンスの管理情報の設定や表示に関する情報が含まれています。

- ダッシュボードの使用 83 ページ
- レポートの使用 203 ページ
- Live Network 281 ページ

セキュリティとコンプライアンスの管理の詳細については、次の Web サイトを参照してください。

http://cve.mitre.org

http://nvd.nist.gov

http://nvd.nist.gov/scap.cfm

http://oval.mitre.org

http://www.us-cert.gov

4　ダッシュボードの使用

ダッシュボードを使用すると、お使いの環境のステータスをさまざまな方法で迅速に評価できます。ダッシュボードでは、[レポート] 領域における特定のタイプの情報が視覚的に表現されます。保有している HPCA ライセンスのタイプによって、特定のダッシュボードが使用できます。この章は、次の各トピックで構成されています。

ダッシュボードの概要

HPCA Console には、企業内のステータスの概要を簡単に表示および評価できるダッシュボードが含まれます。

- 89 ページの「HPCA オペレーション ダッシュボード」には、HPCA インフラストラクチャで行われた作業の量が表示されます。
- 96 ページの「脆弱性管理ダッシュボード」には、企業内のスキャン済みデバイスから検出された既知のセキュリティ脆弱性に関する情報が表示されます。
- 115 ページの「適用情報管理ダッシュボード」には、環境内の管理対象クライアント デバイスの、Federal Desktop Core Configuration (FDCC) などの確立された規制および標準に基づいた事前定義ポリシーへの順守状況が表示されます。
- 125 ページの「セキュリティ ツール管理ダッシュボード」には、企業内の管理対象クライアント デバイスにインストールされているスパイウェア対策、ウイルス対策、およびソフトウェア ファイアウォール製品に関する情報が表示されます。
- 134 ページの「パッチ管理ダッシュボード」には、ネットワーク内のデバイスで検出されたパッチ脆弱性に関する情報が表示されます。

各ダッシュボードにはそれぞれ 2 つのビューがあります。

表 9　ダッシュボードのビューのタイプ

タイプ	説明
エグゼクティブ ビュー	マネージャを対象とした高レベルの要約情報です。企業の履歴情報などが含まれます。
オペレーション ビュー	日常業務に HPCA を使用する一般ユーザーを対象とした詳細情報です。特定デバイス、サブネット、脆弱性、および特定の適応状況またはセキュリティ ツールの問題に関する情報が含まれます。

各ビューには数多くの情報ペインがあります。HPCA を設定して、これらのペインをすべて表示したり一部を表示したりできます。詳細については、318 ページの「ダッシュボード」を参照してください。

各ダッシュボードには、統計の要約と関連レポートへのリンクが掲載されたホーム ページが含まれます。これらのリンクのいずれかをクリックすると、別のブラウザ ウィンドウが開き、HPCA によりレポートが表示されます。

大部分のダッシュボード ペインでは、情報をグラフまたはグリッド形式で表示できます。グリッド表示では、現在のソート パラメータがカラム見出し内で ▼ アイコンで表示されます。ソート パラメータを変更するには、別のカラム見出しをクリックします。ソート順を逆にするには、カラム見出しを再度クリックします。カラムを移動するには、カラム見出しセルの背景部分をクリックして、カラムを移動先までドラッグします。

大部分のダッシュボード ペインでは、棒グラフまたは円グラフの色分けされた領域や線グラフのデータ ポイントにカーソルを置くと、詳細情報が表示されます。また、大部分のペインでは、レポートをドリル ダウンしてより詳細な情報を得ることができます。

各ペインの左下隅のタイム スタンプは、その情報の取得元からの最新のリフレッシュ日時を示しています。

図 2　タイム スタンプ

ダッシュボード ペインでは、現地のタイム ゾーンを使用して日時が表示されます。[レポート] タブで利用可能なレポートでは、デフォルトでグリニッジ標準時 (GMT) が使用されます。ただし、個々のレポート パックでは、GMT または現地時間のどちらを使用するかを設定できます。

セキュリティおよび適用情報管理データがレポート データベース内に存在しない場合 (最初のスキャンが実行される前など)、ダッシュボード ペインにはデータは何も表示されません。

ダッシュボード ペインでは、次のアクションを実行できます。

表 10　ダッシュボード ペインのアクション

アイコン	説明
	情報をグラフ形式で表示します。
	情報をグリッド形式で表示します。
	該当グラフの凡例を表示します。

表 10　ダッシュボード ペインのアクション

アイコン	説明
	データの取得元からデータをリフレッシュします。個々のペインのデータをリフレッシュするには、それぞれのペインのリフレッシュ アイコンをクリックします。すべてのペインをリフレッシュするには、ダッシュボードの右上隅のリフレッシュ アイコンをクリックします。 HPCA Console セッションがタイムアウトした場合、ダッシュボードのペインは自動的にリフレッシュされません。データベースから最新の情報を取得するには、再度サインインしてから手動で各ペインをリフレッシュする必要があります。
	ダッシュボード内のすべてのペインの表示を出荷時の設定にリセットします。
	HPCA データが含まれているペインについて、対応するレポートを表示します。外部 Web サイトまたは RSS フィードからの情報が含まれているペインの場合は、情報元の Web サイトに移動します。
	「クイック ヘルプ」ボックスまたはツール チップが開きます。このボタンを 1 回クリックすると、該当ダッシュボード ペインの簡単な説明が表示されます。再度クリックすると、クイック ヘルプ テキストが非表示になります。
	該当ペインに関する状況に応じたオンライン ヘルプ トピックが開きます。このコントロールは、クイック ヘルプ テキストが表示されている場合にのみ使用できます。
	ダッシュボード ペインを最小化します。
	ダッシュボード ペインを最大化します。
	最大化されたペインを元のサイズに戻します。

あるダッシュボード ペインを最小化すると、その他のペインはダッシュボードのウィンドウに合うようにサイズが拡大します。同様に、あるダッシュボード ペインを最大化すると、その他のペインは下に隠れます。最小化されたペインを元に戻すには、ダッシュボードの下部にあるペインの名前が表示されたグレーのボタンをクリックします。この例では、24 時間のサービス イベント ペインが最小化されています。

図 3　　ダッシュボード ペインを復元するボタン

ペインをドラッグ アンド ドロップして、ダッシュボード ウィンドウ内でペインの配置を変更できます。ただし、ダッシュボードの外にはドラッグできません。

ダッシュボード内の各ペインのサイズや配置を変更して外観をカスタマイズした場合、または 1 つ以上のペインのグラフとグリッドのビューを切り替えた場合、このカスタマイズは次回の HPCA Console へのサインイン後にも適用されます。ダッシュボードのレイアウト設定は、お使いのコンピュータのローカル フラッシュ共有オブジェクト (ブラウザ cookie など) として格納されます。この設定は、明示的に削除する場合を除き保存されます。詳細については、430 ページの「ダッシュボード レイアウト設定の削除」を参照してください。

いずれかのダッシュボードの表示中に **F5** ファンクション キーを押すと、ブラウザが HPCA Console をリロードした後にそのダッシュボードのページに戻ります。

一部のグリッド表示では、特定のパラメータついての以前のスキャンからの傾向が、次に示すようなトレンド インジケータにより表示されます。

表 11　トレンド インジケータ

アイコン	色	方向	説明
	赤	上へ	パラメータが増加しています。傾向は望ましくありません。
	緑	上へ	パラメータが増加しています。傾向は良好です。
	赤	下へ	パラメータが減少しています。傾向は望ましくありません。
	緑	下へ	パラメータが減少しています。傾向は良好です。

たとえば、97 ページの「重大度別にした脆弱性の影響 (円グラフ)」では、高重大度の脆弱性が増加した場合、上向きの赤色矢印が表示されます。高重大度の脆弱性の数が減少した場合、緑色の下向き矢印が表示されます。

傾向を評価するために、HPCA では、現地時間の毎深夜に 1 日分のデータが要約されます。そのため、現在の日付のデータは不完全です。トレンド インジケータは過去 2 日間のデータを基にしています。

ダッシュボード デバイス

デバイスにより、特定のタイプのデバイスに対してダッシュボードの各ペインに表示される情報を制限できます。デフォルトでは次の 3 種類のデバイスが使用可能です。

- グローバル – すべてのデバイス (フィルタは適用されません)。
- モバイル – ラップトップやその他のモバイル コンピューティング デバイスです。これには、次のシャーシ タイプのすべてのデバイスが含まれます。
  - ポータブル
  - ラップトップ
  - ノートブック
  - ハンドヘルド
  - サブ ノートブック
- 仮想 – 仮想デバイスです。これには、ベンダーおよびモデルのプロパティが VMware であるすべてのデバイスが含まれます。

追加のデバイスを最大 2 つ定義することもできます。詳細については、『Enterprise Manager ガイド』の「カスタム ダッシュボード基準とフィルタの追加」を参照してください。

基準を適用するには、コンソールの左上隅の [基準] ボックスでデバイスを選択します。

表示されるデータの特性により、一部のダッシュボード ペインでは、デバイスの設定が適用されません。[モバイル] または [仮想] デバイスを選択した場合、これらが適用されないペインの上部に、次の強調表示のメッセージが表示されます。

フィルタまたはデバイスが適用できません

また、デバイスの設定が適用されないペインは外枠がオレンジ色になります。

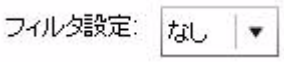
デバイスの設定が適用されないダッシュボード ペインは次のとおりです。

- 脆弱性履歴の評価 99 ページ
- 適用状況評価履歴 119 ページ
- Microsoft セキュリティ ブリテン 139 ページ
- HP Live Network アナウンスメント 106 ページ

デバイスを選択すると、HPCA Console 内のすべてのダッシュボード パネルに設定が適用されますが、例外として上記の「フィルタまたはデバイスが適用できません」が表示されたペインには適用されません。デバイスは個別のダッシュボード ペインには適用できません。

ダッシュボード フィルタ

ダッシュボードに表示されるデータの量を制限するには、カスタマイズしたレポート フィルタを作成してそれを使用する方法もあります。フィルタは、次に示すように、ダッシュボードの右上隅のドロップダウン メニューから選択できます。



ドロップダウン メニューには、Console.properties ファイルで現在定義されているすべてのフィルタが含まれています。このメニューにカスタム フィルタを追加する方法については、『Enterprise Manager ガイド』の「カスタム ダッシュボード基準とフィルタの追加」を参照してください。

HPCA オペレーション ダッシュボード

このダッシュボードには、企業内の HPCA インフラストラクチャで行われる作業が表示されます。表示されるのは次の 3 点です。

- HPCA クライアント接続の数

- 発生したサービス イベント (インストール、アンインストール、更新、修復および検証) の数
- HPCA で実行された操作のタイプ (OS、セキュリティ、パッチまたはアプリケーション)

また、2 つの期間のクライアント接続およびサービス イベントの指標が表示されます。エグゼクティブ ビューには、最新の 12 か月が表示されます。操作ビューには、最新の 24 時間が表示されます。どちらのビューにも、次の情報ペインが含まれます。

クライアント接続 90 ページ

サービス イベント 92 ページ

エグゼクティブ ビューには、次のペインも含まれます。

ドメイン別 12 か月サービス イベント 94 ページ

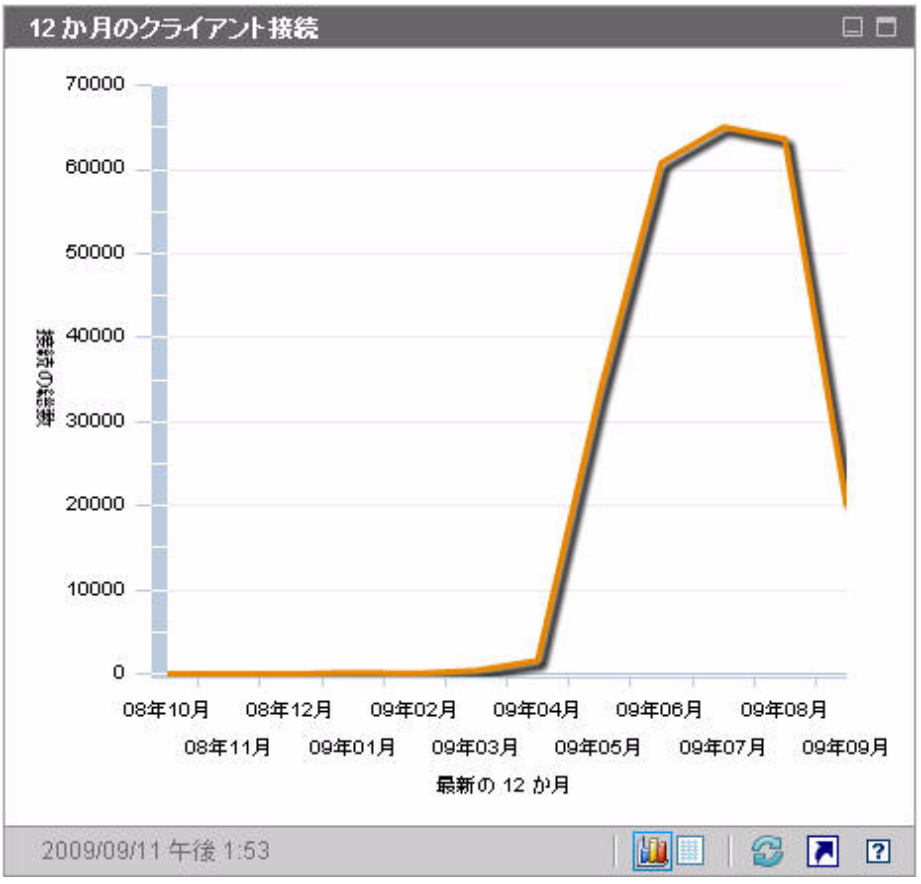
デフォルトではこれらのペインがすべて表示されます。ダッシュボードでは、これらの任意のペインの表示 / 非表示を切り替えることができます。318 ページの「ダッシュボード」を参照してください。

左側のナビゲーション ペインの [HPCA 操作] をクリックすると、[HPCA 操作] ホームページが表示されます。このページには統計と関連レポートへのリンクが掲載されています。

クライアント接続

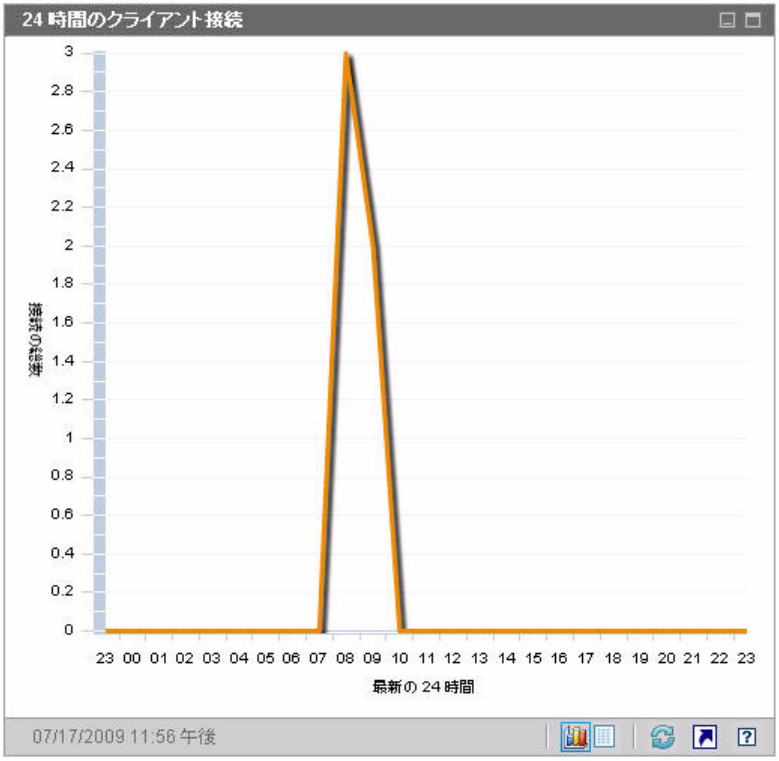
このペインのグラフ表示には、過去 12 か月 (エグゼクティブ ビュー) または 24 時間 (オペレーション ビュー) に発生した HPCA Agent クライアント接続の数が表示されます。データ ポイントの上にカーソルを置くと、その月または時間の合計接続数が表示されます。

図 4　12 か月のクライアント接続



このペインのグリッド表示では、過去 12 か月の各月に完了したクライアント接続の合計数がリストされます。

図 5　24 時間のクライアント接続



ダッシュボード ペインでは、現地のタイム ゾーンを使用して日時が表示されます。[レポート] タブで利用可能なレポートでは、デフォルトでグリニッジ標準時 (GMT) が使用されます。ただし、個々のレポート パックでは、GMT または現地時間のどちらを使用するかを設定できます。

このペインのグリッド表示では、過去 24 時間の各時間帯に完了したクライアント接続の数がリストされます。

サービス イベント

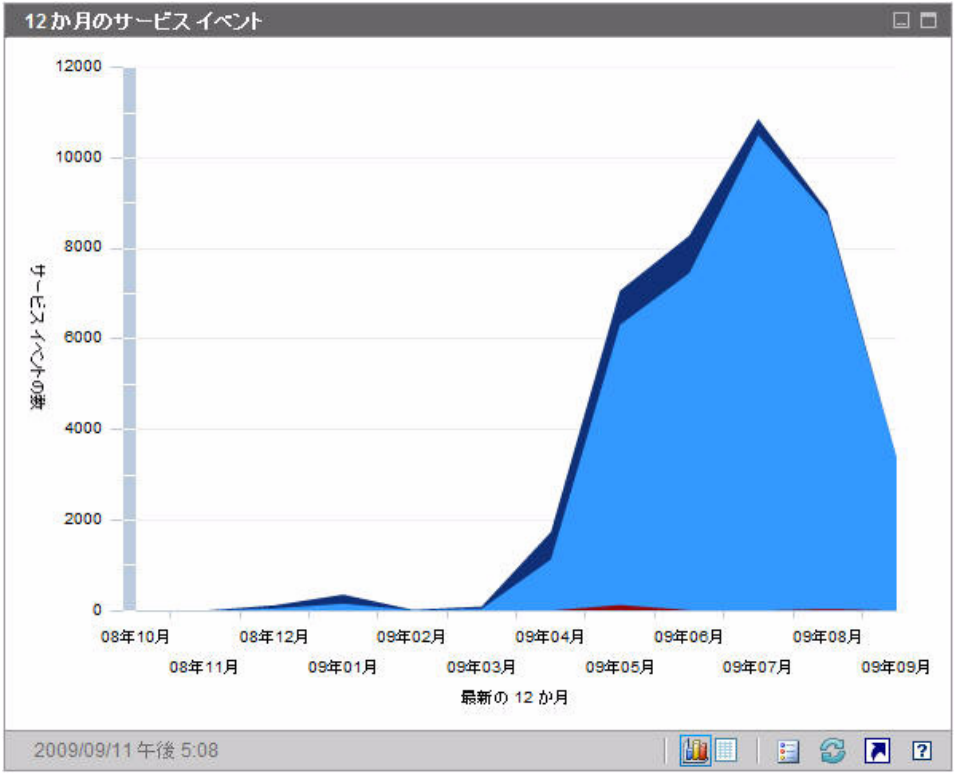
このペインのグラフ表示では、過去 12 か月 (エグゼクティブ ビュー) または 24 時間 (オペレーション ビュー) に企業のクライアント デバイスにおいて HPCA で完了したサービス イベントの数が表示されます。これらのサービス イベントには、HPCA により次の作業が行われたアプリケーションの数が含まれます。

- インストール済み
- アンインストール済み

- 更新済み
- 修復済み
- 検証済み

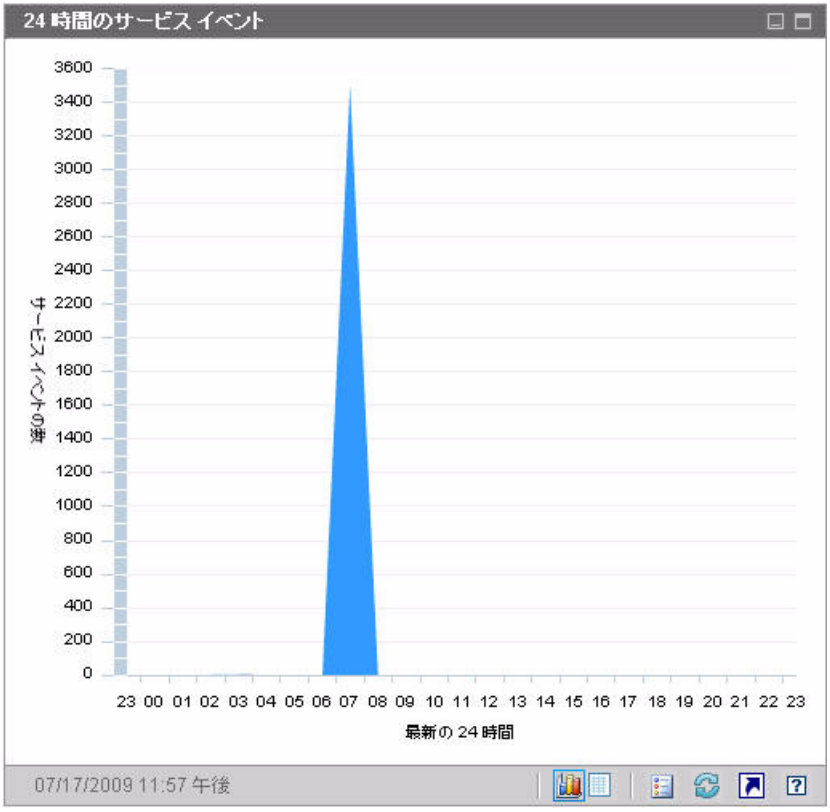
データ ポイントの上にカーソルを置くと、特定の月または時間に完了したサービス イベント数が表示されます。

図 6　12 か月のサービス イベント



このペインのグリッド表示では、過去 12 か月の各月に HPCA で完了した各種サービス イベントの数がリストされます。

図 7　24 時間のサービス イベント



ダッシュボード ペインでは、現地のタイム ゾーンを使用して日時が表示されます。[レポート] タブで利用可能なレポートでは、デフォルトでグリニッジ標準時 (GMT) が使用されます。ただし、個々のレポート パックでは、GMT または現地時間のどちらを使用するかを設定できます。

このペインのグリッド表示では、過去 24 時間の各時間帯に HPCA により開始された各種サービス イベントの数がリストされます。

ドメイン別 12 か月サービス イベント

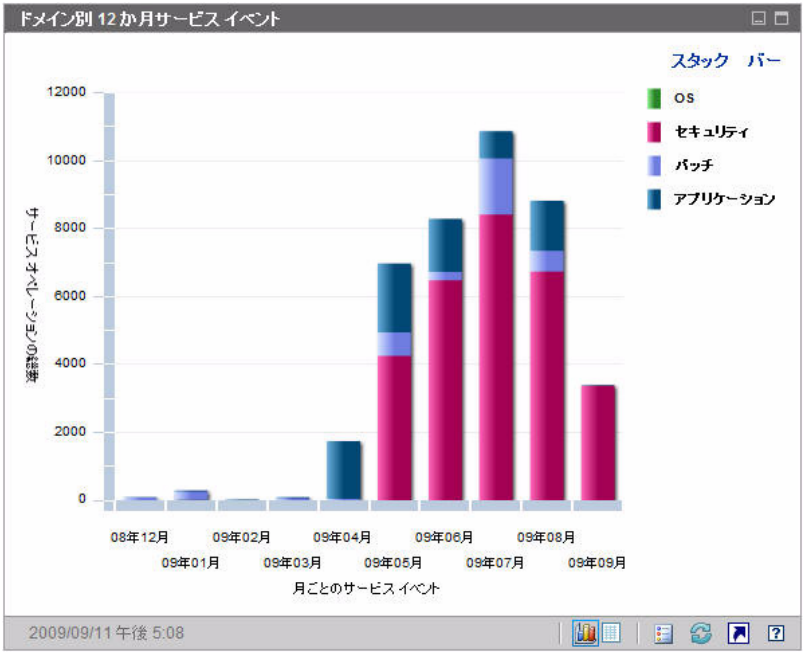
このペインのグラフ表示では、過去 12 か月の各月に HPCA により実行された次のサービスの数が表示されます。

- オペレーティング システム (OS) の操作
- セキュリティ オペレーション
- パッチ オペレーション

- アプリケーション オペレーション

取得可能なデータが 12 か月以下の場合、このグラフに表示されるバーの数は少なくなります。

図 8　ドメイン別 12 か月サービス イベント



このグラフには、2 とおりのデータ表示方法があります。

- スタック – 異なるタイプのサービス イベントが、各月に対応した単一のバー内に垂直にスタックされます (図示)。
- バー – 月ごとに各タイプのサービス イベントが個別のバーで表示されます。

グリッド表示では、過去 12 か月の各月に HPCA により実行された各種サービスの数がリストされます。

脆弱性管理ダッシュボード

HPCA には、企業内の各管理対象クライアント システムのセキュリティ脆弱性情報を収集する機能があります。この情報が集計されて、脆弱性管理ダッシュボードに表示されます。

HPCA は、更新された脆弱性定義と実行可能なクライアント スキャナを提供する HP Live Network と統合されています。

脆弱性管理ダッシュボードおよび各種レポートで使用される共通の脆弱性管理用語の詳細は、43 ページの「セキュリティとコンプライアンスの管理」を参照してください。

HPCA では、Common Vulnerability Scoring System (CVSS、共通脆弱性評価システム) ベースのスコアにより、企業内の各クライアント デバイスが次の重大度カテゴリのいずれかに分類されます。

表 12　重大度カテゴリ

アイコン	カテゴリ	該当デバイスの CVSS ベース スコアの最高値
	高	7.0 ～ 10
	中	4.0 ～ 6.9
	低	3.9 以下
	脆弱性なし	脆弱性が検出されない
	不明	該当デバイスに利用可能なデータが存在しない

カテゴリは、デバイス上に存在する最も高い重大度の脆弱性で決定されます。デバイスに 1 つでも高重大度の脆弱性が存在すれば、カテゴリは高になります。デバイスに、高重大度の脆弱性が存在しないが、中重大度の脆弱性が 1 つでも存在すれば、カテゴリは中になります。以下、同様に続きます。

特定の脆弱性の重大度が不明であり、CVSS スコアが null である場合、NVD、CVE リポジトリ、またはその他の利用可能なリソースを駆使して、この脆弱性を十分に調査してください。この場合、HPCA はこの問題に関して確証を持てる判断を行うために必要な情報を提供できない場合があります。

脆弱性管理ダッシュボードのエグゼクティブ ビューには、次の 4 つの情報ペインが含まれます。

- 重大度別にした脆弱性の影響 (円グラフ) 97 ページ
- 重大度別にした脆弱性の影響 (棒グラフ) 107 ページ
- 脆弱性の影響 101 ページ
- 脆弱性履歴の評価 99 ページ

操作ビューには、次の 4 つの情報ペインが含まれます。

- HP Live Network アナウンスメント 106 ページ
- 最も脆弱性の高いデバイス 109 ページ
- 最も脆弱性の高いサブネット 110 ページ
- 脆弱性のトップ 112 ページ

ダッシュボードでは、これらの任意のペインの表示 / 非表示を切り替えることができます。318 ページの「ダッシュボード」を参照してください。

[ホーム] タブの左側のナビゲーション ペインで [脆弱性管理] をクリックすると、[脆弱性管理] ホーム ページが表示されます。このページには統計と関連レポートへのリンクが掲載されています。

重大度別にした脆弱性の影響 (円グラフ)

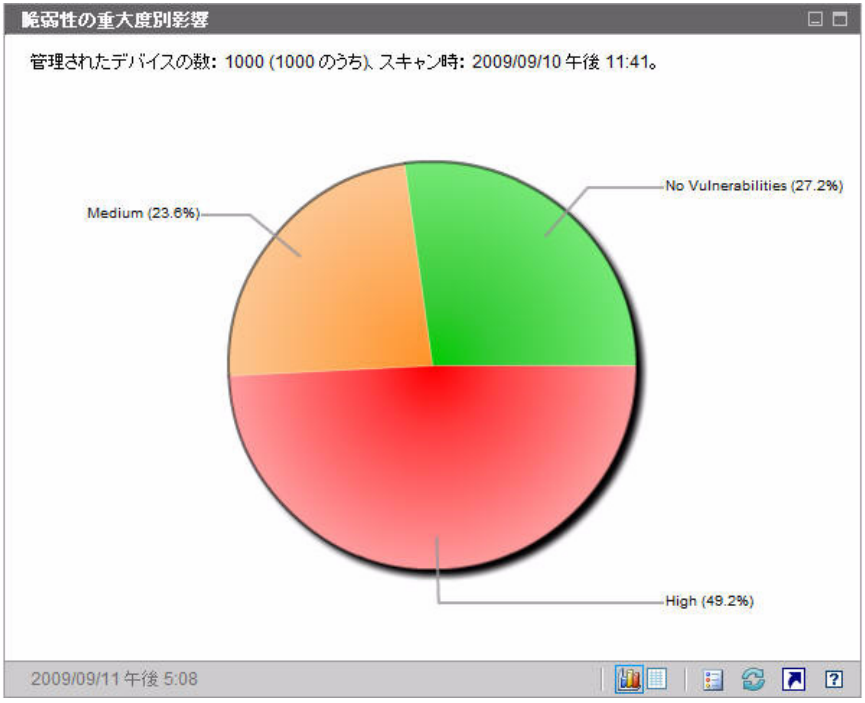
このペインのグラフ表示では、企業内のスキャン済みデバイスの次の 5 種類のカテゴリ別のパーセンテージが表示されます。分類は、各デバイスで検出された最も高い重大度の脆弱性に基づいて行われます。

- 高 (赤)

- 中 (オレンジ)
- 低 (黄)
- 脆弱性なし (緑)
- 不明 (青)

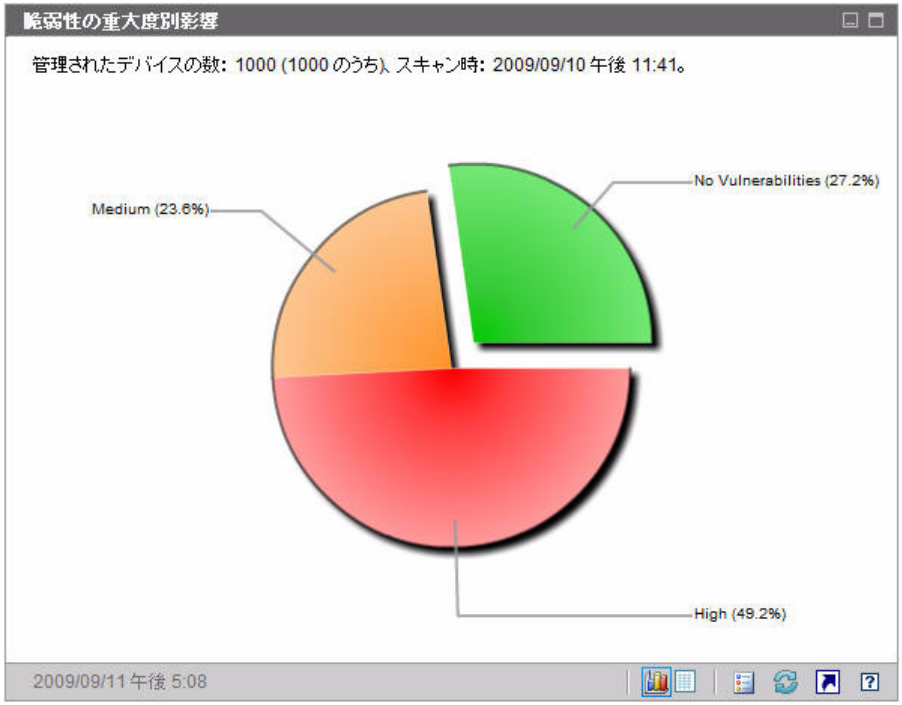
各重大度カテゴリのデバイス数を表示するには、円グラフの対応するセクタの上にカーソルを置きます。

図 9　脆弱性の重大度別影響



円グラフのいずれかの分割部分をクリックすると、新しいブラウザ ウィンドウが開いて詳細なレポートが表示されます。レポートには、クリックした分割部分に対応する重大度カテゴリに基づいたフィルタが適用されます。分割部分をクリックしてレポートを表示すると、次に示すようにその分割部分が円グラフから分離します。

図 10　脆弱性の重大度別影響



グリッド表示では、重大度カテゴリごとのデバイス数が表示されます。また、そのデバイス数が以前の脆弱性スキャンと比較して増加したか、減少したか、または同じであるかが表示されます。

関連トピック：

ダッシュボードの使用 83 ページ

脆弱性管理ダッシュボード 96 ページ

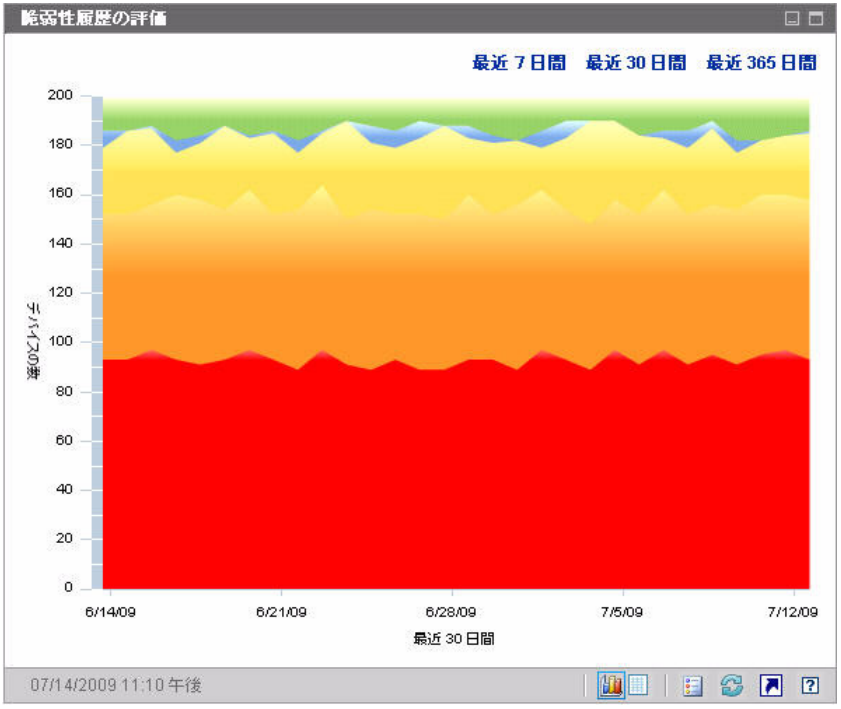
セキュリティとコンプライアンスの管理 43 ページ

脆弱性履歴の評価

このペインには、[脆弱性の重大度別影響] ペインに表示される情報が時間とともにどのような変化をたどるかが示されます。

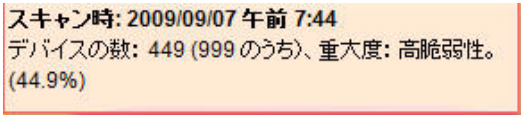
このペインのグラフ表示では、一定の期間における企業のリスク集計の平均が表示されます。垂直軸はデバイス数を表します。水平軸は時間を表します。過去 7 日、30 日、または 365 日のデータを表示できます。色分けされたそれぞれの領域は、各重大度カテゴリのデバイス数を表します。カテゴリは、高 (赤)、中 (オレンジ)、低 (黄)、脆弱性なし (緑)、および不明 (青) に分類されています。

図 11　脆弱性履歴の評価



色分けされた領域の間の線上にあるデータ ポイントにカーソルを置くと、そのデータ ポイントを強調する円が表示され、ツール チップに該当日における該当脆弱性カテゴリのデバイスの数とパーセンテージが表示されます。

図 12　ツール チップ



この例では、スキャンされた 490 個のデバイスの 46.9% に、少なくとも 1 つの高重大度脆弱性が存在することを示しています。ツール チップには、常に前回実行された脆弱性スキャンの情報が表示されます。通常、スキャンは毎日実行されます。数日間スキャンが実行されなかった場合、その期間はグラフが平坦になり、ツール チップの情報は変わりません。

ツール チップには、常に脆弱性スキャンの最新の実行日時が表示されます。脆弱性のデータを分析する場合、最新のスキャンの実行日時を必ず確認してください。

ツール チップの表示時にデータ ポイントに表示される円の外観は、円の下の領域の色により異なる点に注意してください。

このペインのグリッド表示では、指定された期間の各日について各リスク カテゴリのデバイス数がリストされます。また、グリッドには前回行われた環境のスキャン日時が表示されます。

グラフには不明重大度カテゴリのデバイスが表示されませんが、グリッド表示にはこれらのデバイスに関するカラムが含まれます。

関連トピック：

ダッシュボードの使用 83 ページ

脆弱性管理ダッシュボード 96 ページ

セキュリティとコンプライアンスの管理 43 ページ

脆弱性の影響

このペインのグラフ表示では、特定の脆弱性に影響されたデバイスの相対数が表示されます。1 つの脆弱性が 1 つの円に対応しています。円のサイズは、影響を受けたデバイスの数を示しています。それぞれの円の色は、脆弱性の重大度を表します。重大度は、高 (赤)、中 (オレンジ)、低 (黄)、および不明 (青) に分類されています。

垂直軸は、CVSS ベースのスコアで計測された重大度を、水平軸は脆弱性が National Vulnerability Database (NVD) で最初にパブリッシュされてからの経過時間を表します。次に例を示します。

- グラフの右上部分に大きな赤色の円がある場合、多数のデバイスに影響を与え、パブリッシュされてから比較的長期間が経過している重大な脆弱性の存在を表します。

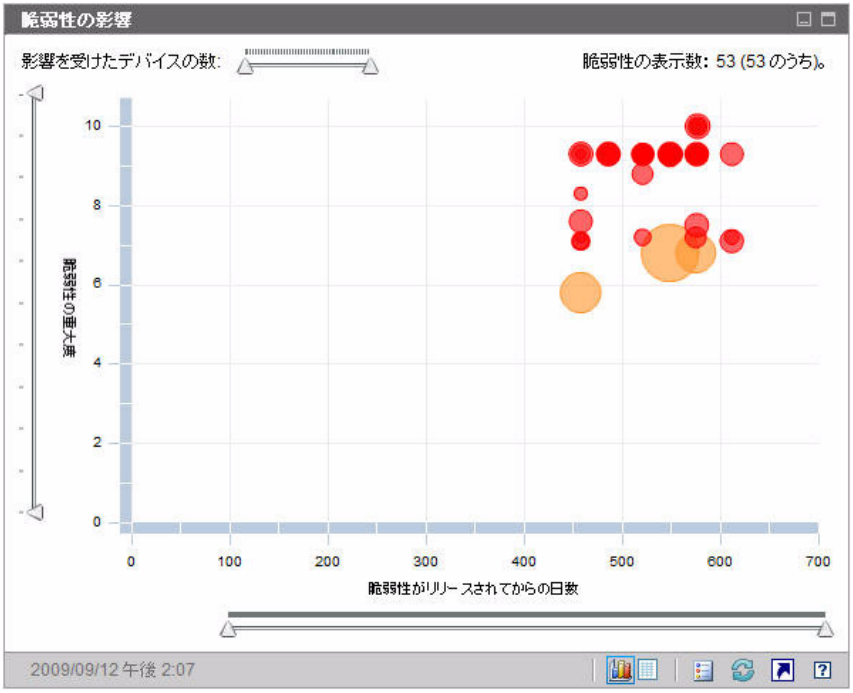
- グラフの左下部分に小さな黄色の円がある場合、少数のデバイスに影響を与え、NVD でパブリッシュされたのが比較的最近である重大度が低い問題の存在を表しています。
- 右上隅に赤い円がないグラフが理想的と言えます。これは、重大な脆弱性が迅速に処置されたことを示しています。

特定の円にカーソルを置くと、円が表している脆弱性に関する次の情報がツールチップに表示されます。

- 重大度のカテゴリ (高、中、または低)
- CVE ID およびタイトル
- パブリッシュの日付
- 影響を受けたデバイス数
- スキャン済みデバイスの合計数

グラフ内のいずれかの円をクリックすると、新しいブラウザ ウィンドウが開いて詳細なレポートが表示されます。レポートには、この脆弱性の影響を受けたデバイス数および脆弱性自身の情報が表示されます。影響を受けたデバイスの一覧を入手するには、レポートの [影響を受けたデバイス] の数字をクリックします。

図 13　脆弱性の影響



3 つのスライダを使用して、特定のデータ領域を拡大できます。スライダにより、グラフ内に表示される円の数と各軸の目盛りが決定されます。

- ペイン上部の水平スライダにより、特定の脆弱性の影響を受けた管理対象デバイス数で表される影響の範囲を指定できます。
- 左側の垂直スライダにより、CVSS ベースのスコアで表される任意の重大度の範囲を拡大できます。
- ペインの下部の水平スライダにより、表示される脆弱性の有効期間を指定できます。有効期間は、脆弱性が最初にパブリッシュされた日に基づきます。脆弱性定義に後で加えられた変更は反映されません。

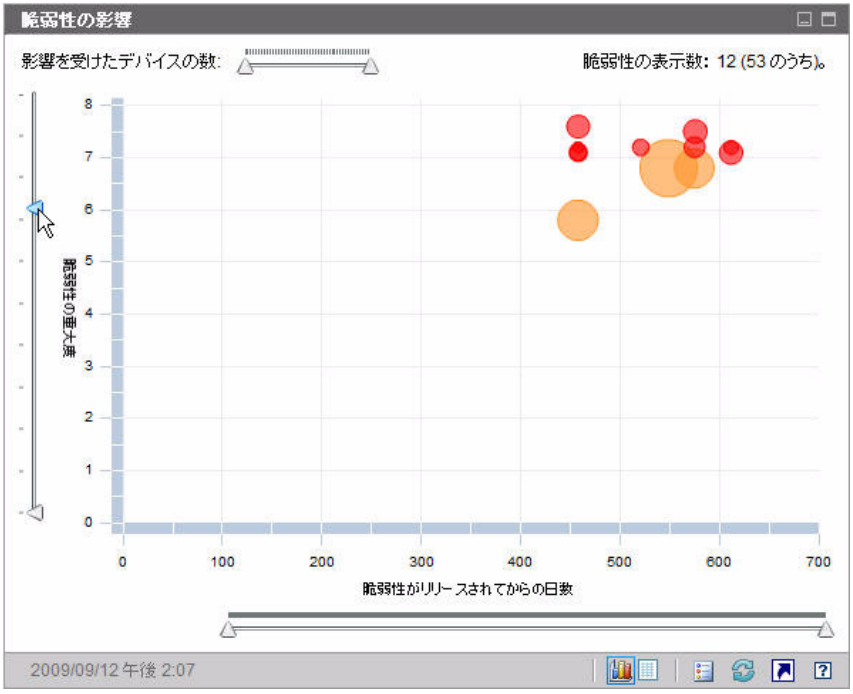
  デフォルトでは、表示される有効期間は 45 日間です。脆弱性管理ダッシュボードの設定時に、このデフォルト値を指定できます。318 ページの「ダッシュボード」を参照してください。

三角形 (△) がスライダの両端にある場合、データ範囲全体が表示されています。三角形の間隔が狭い場合、データ範囲の一部のみが表示されています。各スライダで、両方の三角形を調節できます。

グラフに何もデータが表示されていない場合、3 つのすべてのスライダの三角形を両端に移動して、データ範囲全体を表示します。

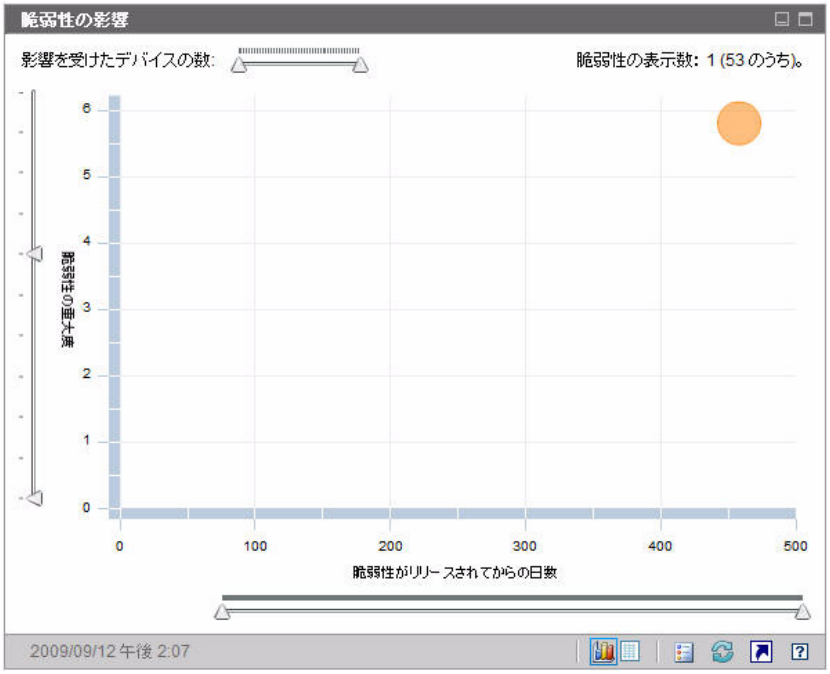
次の例では、CVSS ベースのスコアが 6 以上の脆弱性が表示されています。

図 14　CVSS が 6 以上



次の例では、過去 500 日以内にリリースされた CVSS ベースのスコアが 6 以上の脆弱性のみが表示されています。

図 15　過去 500 日以内



このペインのグリッド表示では、検出された各脆弱性について次の情報が提供されます。

- OVAL ID – この脆弱性の OVAL ID
- CVE ID – この脆弱性の CVE ID
- 説明 – OVAL 定義からの説明
- 重大度 – この脆弱性の高、中、または低重大度アイコンおよび CVSS ベースのスコア
- 有効期間 – 脆弱性が NVD でパブリッシュされてからの経過日数
- デバイス数 – 影響を受けたクライアント デバイスの数

グリッド表示では、グリッド表示を選択した時点でグラフに表示されているデータに対応するデータが表示されます。グラフ上のスライダを調節してデータの一部のみを表示している場合、グリッド表示にはグラフの表示部分のみが表示されます。

グリッドは、最初に [デバイス数] でソートされます。ソート パラメータを変更するには、対応するカラム見出しをクリックします。

特定の脆弱性の詳細な情報を得るには、OVAL または CVE の ID をクリックします。

関連トピック：

ダッシュボードの使用 83 ページ

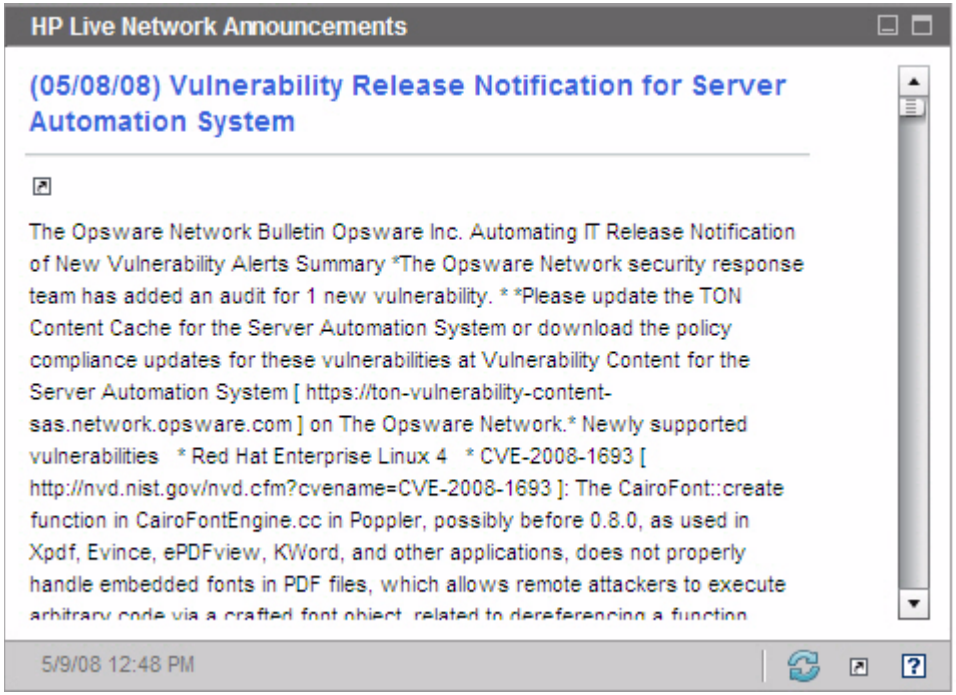
脆弱性管理ダッシュボード 96 ページ

セキュリティとコンプライアンスの管理 43 ページ

HP Live Network アナウンスメント

このペインには、最も新しくパブリッシュされた HP Live Network 脆弱性のリリース アナウンスメントが含まれています。この情報は、HP Live Network 登録サイトからの RSS フィードにより提供されたものです。このペインは、情報を表示するために HP Live Network の認証情報を指定する必要があるため、デフォルトでは有効ではありません。HP Live Network 認証情報の設定についての詳細は、318 ページの「ダッシュボード」を参照してください。

図 16　HP Live Network アナウンスメント



特定のアナウンスメントの詳細な情報を入手するには、そのタイトルのすぐ下にある アイコンをクリックします。新しいブラウザ ウィンドウが開き、HP Live Network 登録サポート サイトが表示されます。このサイトにアクセスするには、アクティブな HP Live Network 登録が必要です。

このペインにはグラフ表示はありません。

[設定] タブでこのペインを有効にするとき、RSS フィードの URL および HP Live Network 認証サーバーのロケーションを変更できます (318 ページの「ダッシュボード」を参照)。また、プロキシ サーバーを有効にする必要が生じる場合もあります (281 ページの「HP Live Network サーバーへの接続の設定」および 263 ページの「プロキシ設定」を参照)。

関連トピック :

ダッシュボードの使用 83 ページ

脆弱性管理ダッシュボード 96 ページ

セキュリティとコンプライアンスの管理 43 ページ

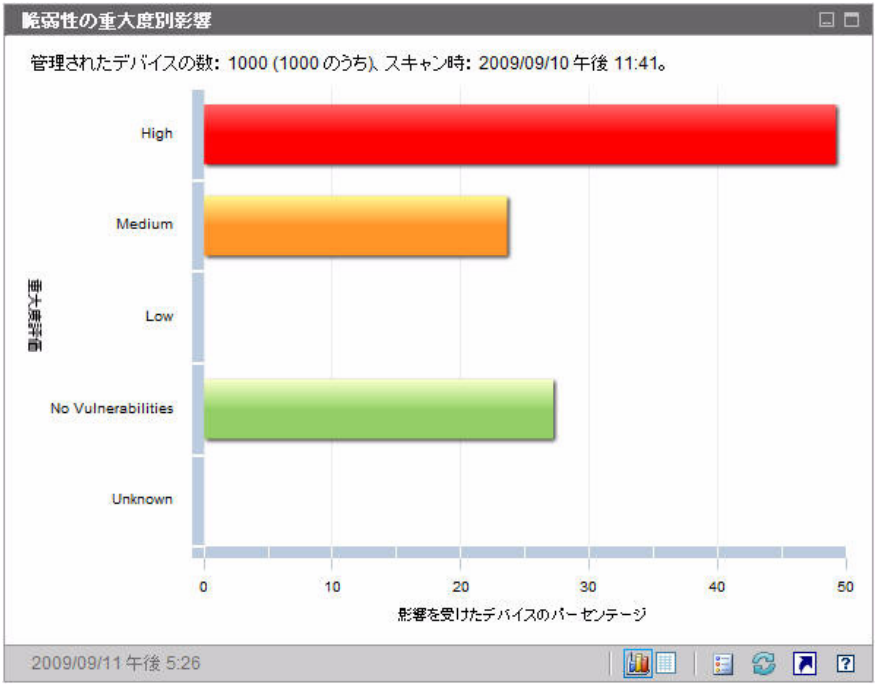
重大度別にした脆弱性の影響 (棒グラフ)

このペインのグラフ表示では、企業内のスキャン済みデバイスの次の 5 種類のカテゴリ別のパーセンテージが表示されます。分類は、各デバイスで検出された最も高い重大度の脆弱性に基づいて行われます。

- 高 (赤)
- 中 (オレンジ)
- 低 (黄)
- 脆弱性なし (緑)
- 不明 (青)

水平軸は、環境内で影響を受けたデバイスのパーセンテージを表します。垂直軸は、4 つの重大度カテゴリを表します。

図 17　脆弱性の重大度別影響



グラフ内の色付き棒のいずれかをクリックすると、新しいブラウザ ウィンドウが開き、詳細なレポートが表示されます。レポートには、クリックした棒に対応した重大度カテゴリに基づいたフィルタが適用されています。

このペインのグリッド表示では、同じ情報がテキスト形式で表示されます。グリッド表示には 2 つのカラムがあります。

- ステータス – 重大度カテゴリ
- 影響を受けたデバイスのパーセンテージ – グラフ表示と同じ

グリッドには、各カテゴリのデバイスのパーセンテージが以前のスキャンと比較して増加したか、減少したか、変わらないかどうかも表示されます。

関連トピック：

ダッシュボードの使用 83 ページ

脆弱性管理ダッシュボード 96 ページ

セキュリティとコンプライアンスの管理 43 ページ

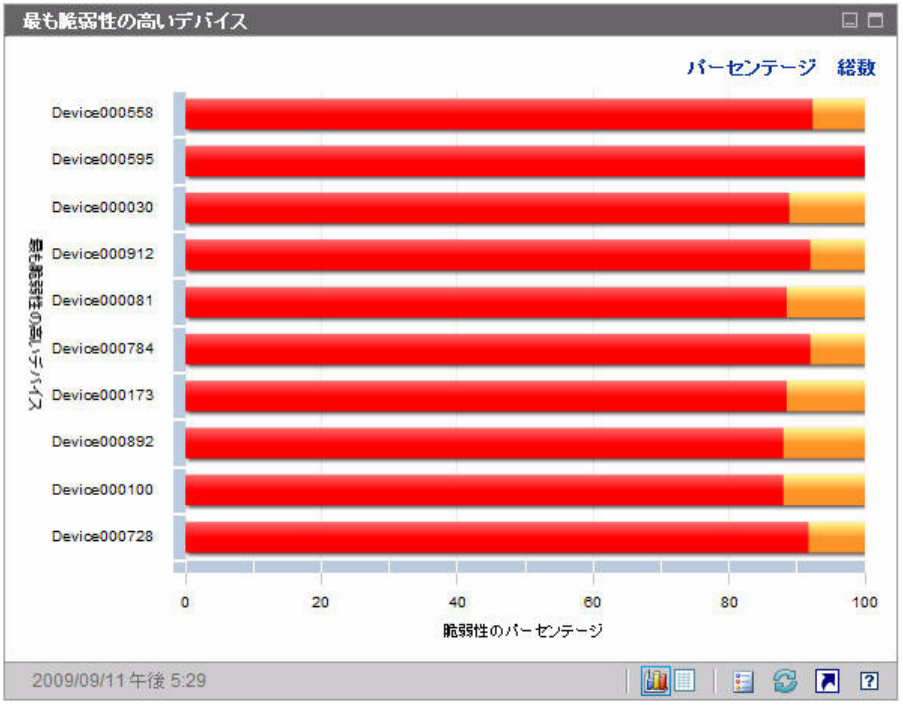
最も脆弱性の高いデバイス

このペインのグラフ表示では、ネットワーク内で最も多く脆弱性が存在するデバイスの上位 10 個が表示されます。グラフで色分けされた各部分は、該当デバイスに存在する脆弱性のパーセンテージ (または数) を表しています。脆弱性は次の 4 つのカテゴリに分類されています。

- 高 (赤)
- 中 (オレンジ)
- 低 (黄)
- 不明 (青)

垂直軸にはデバイス ID でデバイスが表示され、水平軸には、該当デバイスの失敗したテスト (脆弱性) のパーセンテージまたは数がリスク カテゴリに分類されて表示されます。

図 18　最も脆弱性の高いデバイス



パーセンテージではなく、スキャン済みデバイスの数を表示するには **[総数]** をクリックします。この場合、水平軸は、対数目盛りになります。

特定のデバイスで脆弱性が 1 つしかない場合、総数ビューではそのデバイスのデータは表示されません。これは、対数目盛りの既知の制限です。ただし、グリッド表示ではデータが表示されます。

グラフ内の色付き棒のいずれかをクリックすると、新しいブラウザ ウィンドウが開き、該当デバイスに関する詳細なレポートが表示されます。このレポートは重大度でフィルタリングされていません。どの色の部分をクリックしても該当デバイスのすべての脆弱性がリストされます。

グラフ内の、色付き棒のいずれかの上にカーソルを置くと、特定デバイスについて各重大度カテゴリの脆弱性の数 (およびパーセンテージ) が表示されます。

グリッド表示では、各デバイスについて次の情報が提供されます。

- 最大重大度 – 該当デバイスで検出された最も重大度が高い脆弱性の CVSS ベースのスコア
- デバイス – デバイス ID
- 失敗したテスト – 検出された脆弱性の数
- スキャン日付 – 最新の HP Live Network スキャン実施日時

テーブルは最初に [失敗したテスト] でソートされます。ソート パラメータを変更するには、対応するカラム見出しをクリックします。

関連トピック :

ダッシュボードの使用 83 ページ

脆弱性管理ダッシュボード 96 ページ

セキュリティとコンプライアンスの管理 43 ページ

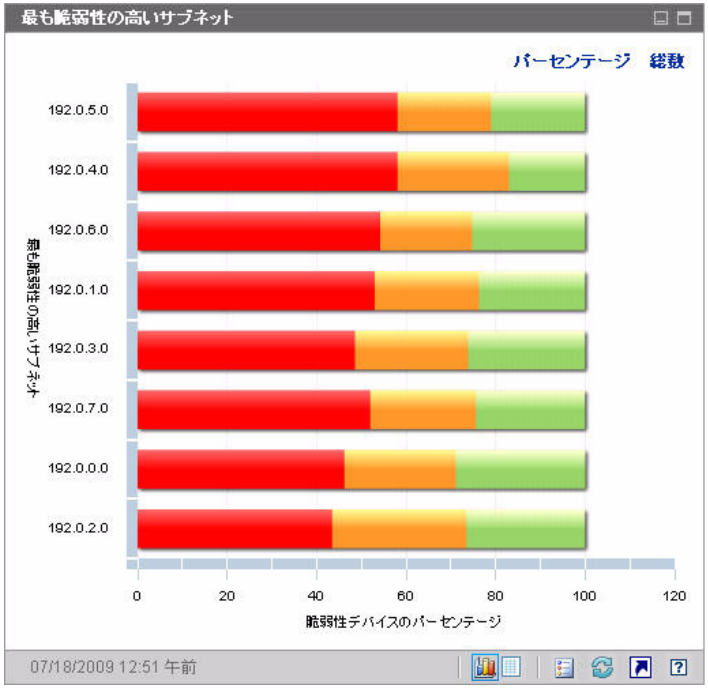
最も脆弱性の高いサブネット

このペインのグラフ表示では、企業内の最も脆弱性の高いサブネットの上位 10 個が表示されます。このグラフでは、重大度カテゴリごとに分類されたデバイス数のパーセンテージを表します。カテゴリは、高 (赤)、中 (オレンジ)、低 (黄)、不明 (青) および脆弱性なし (緑) で表示されます。

デフォルトではこのペインは無効です。有効化するには、318 ページの「ダッシュボード」を参照してください。

各サブネットのデバイスに関する情報を表示するには、該当サブネットの水平バーの上にカーソルを置きます。ポップアップ ボックスが表示され、特定のサブネットにおける各重大度カテゴリのデバイス数およびパーセンテージを確認できます。

図 19　最も脆弱性の高いサブネット



パーセンテージではなく、スキャン済みデバイスの数を表示するには **[総数]** をクリックします。この場合、水平軸は、対数目盛りになります。

特定のサブネットで脆弱性が 1 つしかない場合、総数ビューではそのデバイスのデータは表示されません。これは、対数目盛りの既知の制限です。ただし、グリッド表示ではデータが表示されます。

グリッド表示には、各サブネットについて次の情報が表示されます。

- サブネット アドレス
- サブネット内のデバイスの総数
- 各重大度カテゴリのデバイスの数

テーブルは最初に高リスク デバイスでソートされます。ソート パラメータを変更するには、対応するカラム見出しをクリックします。

関連トピック：

ダッシュボードの使用 83 ページ

脆弱性管理ダッシュボード 96 ページ

セキュリティとコンプライアンスの管理 43 ページ

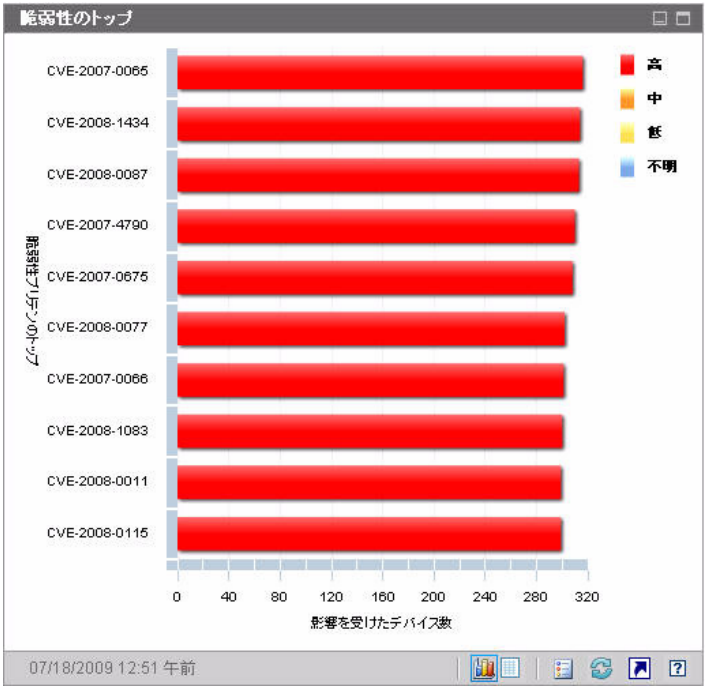
脆弱性のトップ

このペインのグラフ表示は、ネットワーク上の大多数のデバイスに影響する上位 10 件のセキュリティ脆弱性を示します。垂直軸には、これら 10 件の脆弱性の CVE ID が表示されます。水平軸は影響を受けたデバイスの数を表し、対数尺度を使用します。棒の色は各脆弱性の重大度を示します。

- 高 (赤)
- 中 (オレンジ)
- 低 (黄)
- 不明 (青)

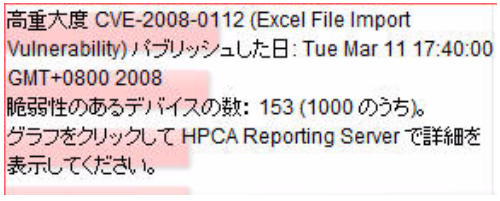
このグラフでは対数尺度を使用するため、特定の脆弱性が 1 つのデバイスのみに影響する場合、グラフ表示にはその脆弱性に関するデータが表示されません。これは、対数目盛りの既知の制限です。ただし、グリッド表示ではデータが表示されます。

図 20　脆弱性のトップ



特定の脆弱性を示す色付き棒にカーソルを置くと、CVE ID と説明、重大度、および影響を受けたデバイスの数が次のように表示されます。

図 21　ツール チップ



グラフの色付き棒の 1 つをクリックすると、新しいブラウザ ウィンドウが開き、フィルタされたレポートが表示されます。レポートには、この脆弱性があるすべてのデバイスが表示されます。

グリッド表示には、検出された上位 10 件の脆弱性について次の情報が表示されます。

- OVAL ID – この脆弱性の OVAL ID

- CVE ID – この脆弱性の CVE ID
- 説明 – CVE の説明
- 重大度 – この脆弱性の CVSS ベース スコア
- プラットフォーム ファミリ – オペレーティング システムのタイプ (たとえば Windows など)
- デバイス数 – この脆弱性によって影響を受けたデバイスの数

テーブルは最初にデバイス数でソートされます。ソート パラメータを変更するには、対応するカラム見出しをクリックします。

特定の脆弱性の詳細を表示するには、その脆弱性の CVE ID または OVAL ID をクリックします。

関連トピック :

ダッシュボードの使用 83 ページ

脆弱性管理ダッシュボード 96 ページ

セキュリティとコンプライアンスの管理 43 ページ

適用情報管理ダッシュボード

HPCA では、企業内の各管理対象クライアント システムに関する法規制の適用状況情報を収集できます。この情報は集計後、適用情報管理ダッシュボードに表示されます。

HPCA は、更新された適用状況の定義と実行可能なクライアント スキャナを提供する HP Live Network と統合されます。

クライアント デバイスは、Federal Desktop Core Configuration (FDCC) 基準 (米国連邦政府のデスクトップ基準) など、確立された法規制の順守基準に基づく適用状況規則を使用してスキャンされます。適用状況規則は、Security Content Automation Protocol (SCAP) を使用して指定されます。

適用情報管理ダッシュボードおよび適用状況管理レポートで使用される一般的な適用状況管理用語のリストを含め、FDCC および SCAP の詳細については 43 ページの「セキュリティとコンプライアンスの管理」を参照してください。

適用情報管理ダッシュボードには、要約ページと 2 つのビューがあります。

エグゼクティブ ビューには、次の情報ペインがあります。

- SCAP ベンチマークによる適用状況の要約 118 ページ
- 適用状況ステータス 116 ページ
- 適用状況評価履歴 119 ページ

オペレーション ビューには、次の情報ペインがあります。

- 上位の失敗した SCAP 規則 121 ページ
- 失敗した SCAP ルール別のデバイスのトップ 123 ページ

ダッシュボードでは、これらの任意のペインの表示 / 非表示を切り替えることができます。詳細については、318 ページの「ダッシュボード」を参照してください。

[ホーム] タブの左側のナビゲーション ペインで [適用状況管理] をクリックすると、[適用状況管理] ホーム ページが表示されます。このページには、スキャンされた管理対象クライアント デバイスの数と関連レポートへのリンクが表示されます。

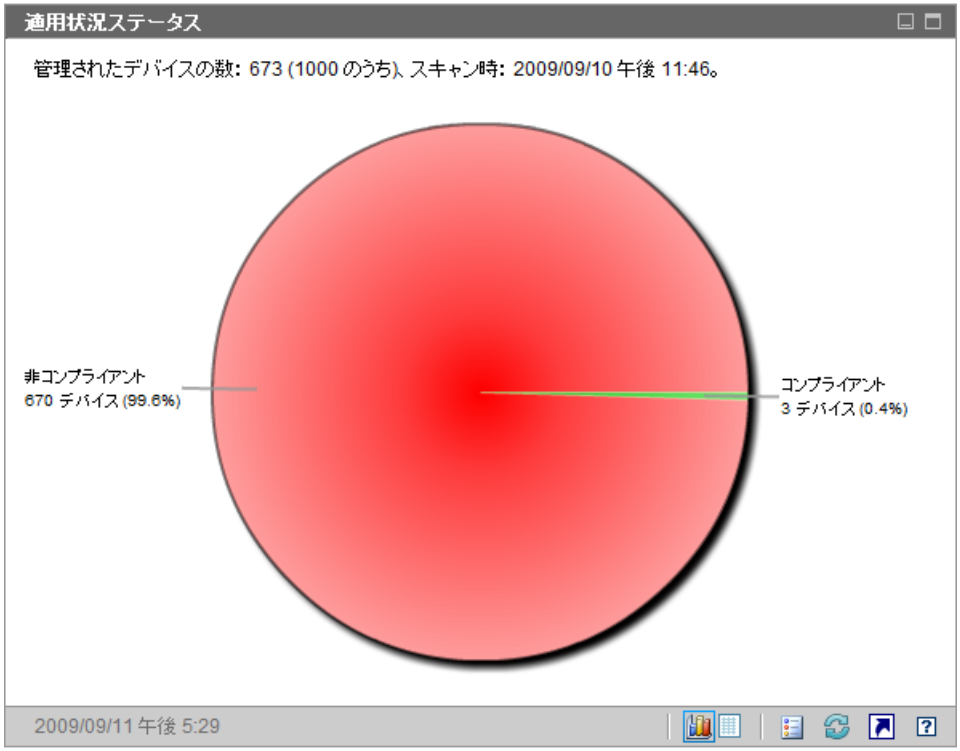
適用状況ステータス

このペインには、各管理対象クライアント デバイスで完了した最新の適用状況スキャンの結果に基づき、企業全体の法規制適用状況の状態が表示されます。このペインのグラフ表示は、適用状況に従っている、または従っていないスキャン済みデバイスのパーセンテージを示します。

- コンプライアント デバイス (緑)
- 非コンプライアント デバイス (赤)

適用状況の各状態にあるデバイスの数 (またはパーセンテージ) を確認するには、円グラフの該当する扇形の上にカーソルを置きます。

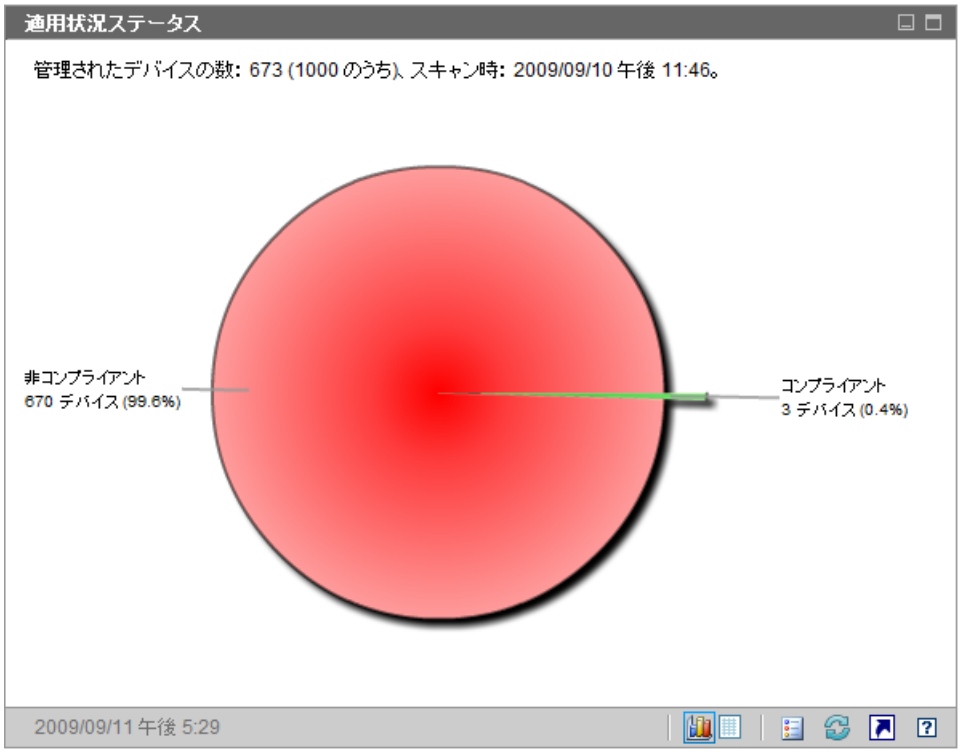
図 22　適用状況ステータス



円グラフの扇形の 1 つをクリックすると、新しいブラウザ ウィンドウが開き、[SCAP ベンチマークによる適用状況の要約] レポートが表示されます。このレポートはフィルタされません。

分割部分をクリックしてレポートを表示すると、次に示すようにその分割部分が円グラフから分離します。

図 23　レポートを開いた後の適用状況ステータス



グリッド表示には、コンプライアント デバイスと非コンプライアント デバイスの数が表示されます。グリッド表示で **[コンプライアント]** または **[非コンプライアント]** のいずれかをクリックすると、新しいブラウザ ウィンドウが開き、[SCAP ベンチマークによる適用状況の要約] レポートが表示されます。レポートはフィルタされません。

関連トピック：

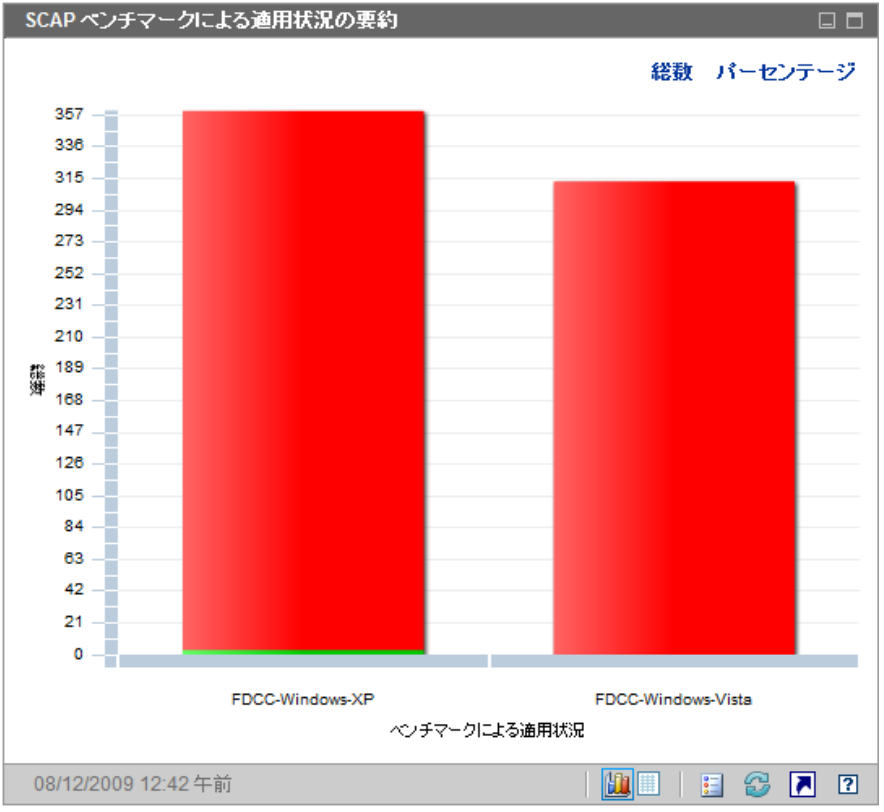
ダッシュボードの使用 83 ページ
適用情報管理ダッシュボード 115 ページ

SCAP ベンチマークによる適用状況の要約

このペインのグラフ表示は、関連する SCAP ベンチマークの適用状況に従っている、または従っていない、企業内のスキャン済みデバイスの数 (またはパーセンテージ) を示します。

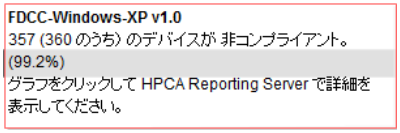
- コンプライアント デバイス (緑)
- 非コンプライアント デバイス (赤)

図 24　SCAP ベンチマークによる適用状況の要約



グラフの色付き棒の 1 つにカーソルを置くと、該当する適応状況状態にあるデバイスの数 (またはパーセンテージ) など、ベンチマークに関する情報がツール チップに表示されます。

図 25　ツールチップ



ツールチップには、常に最後に実行した適用状況スキャンの情報が表示されます。通常、スキャンは毎日実行されます。

棒グラフの色分けされたセグメントの 1 つをクリックすると、新しいブラウザウィンドウが開き、[SCAP スキャン済みデバイス] レポートが表示されます。レポートは、クリックしたセグメントに対応するベンチマークと適用状況ステータスに基づいてフィルタされます。

このペインのグリッド表示は、各ベンチマークの適用状況に従っている、または従っていないデバイスの数 (およびパーセンテージ) を示します。グリッド表示でベンチマーク ID をクリックすると、[SCAP 適用状況規則 (CCE 別)] レポートが表示されます。レポートは、クリックしたベンチマーク ID に基づいてフィルタされます。

関連トピック：

ダッシュボードの使用 83 ページ

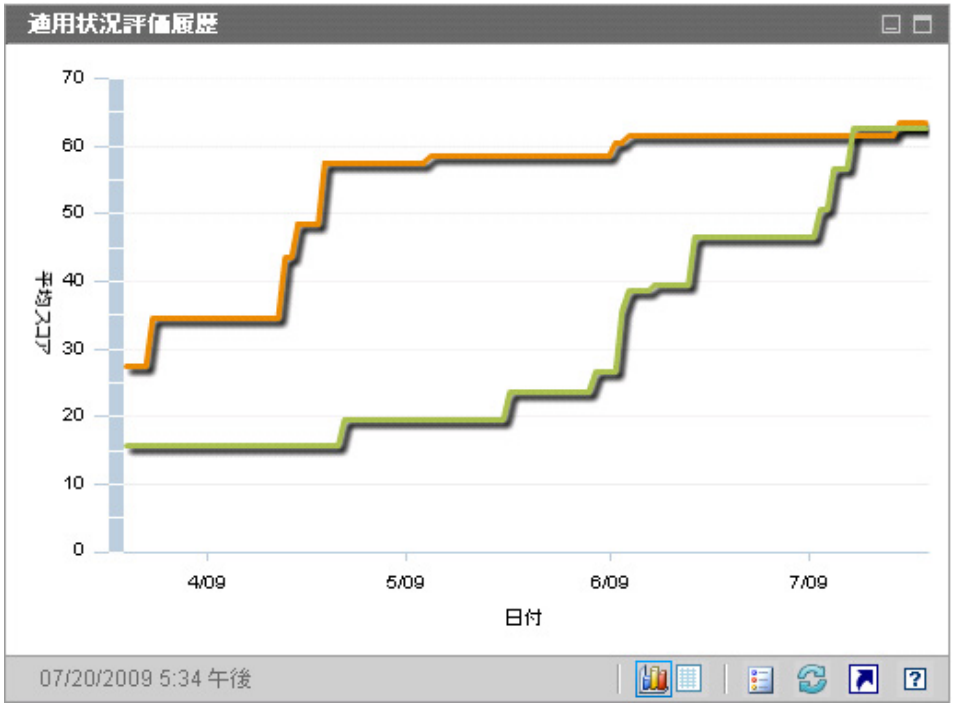
適用情報管理ダッシュボード 115 ページ

セキュリティとコンプライアンスの管理 43 ページ

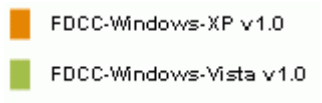
適用状況評価履歴

毎日 1 回、企業全体の適用状況スキャン結果のスナップショットが作成されます。このスナップショットに基づき、ベンチマークが適用されるデバイスに対して各ベンチマークの平均デフォルト スコアが計算されます。この情報ペインには、長期にわたる各ベンチマークの平均デフォルト スコアが表示されます。

図 26　適用状況評価履歴



垂直軸は平均デフォルト スコアを表します。水平軸は時間を表します。色分けされたラインは、それぞれ異なるベンチマーク (またはバージョン) を表します。



これらの色は動的に割り当てられ、特定のベンチマークおよびバージョンに常に同じ色が使用されるわけではありません。現在の色の割り当てについては、凡例を参照してください。

色分けされたラインのいずれかにカーソルを置くと、ツールチップに次の情報が表示されます。

- ベンチマークの名前とバージョン
- スナップショットの日付
- このベンチマークまたはバージョンに対してスキャンされたすべてのデバイスの平均デフォルト スコア

このペインのグリッド表示は、各ベンチマークの日次平均デフォルト スコアを示します。また、適用可能なデバイスのうち、その日のそのベンチマークの適用状況に従っているデバイスの数も示します。テーブルは最初に日付でソートされ、最新のスナップショットの日付が先頭に表示されます。

関連トピック：

ダッシュボードの使用 83 ページ

適用情報管理ダッシュボード 115 ページ

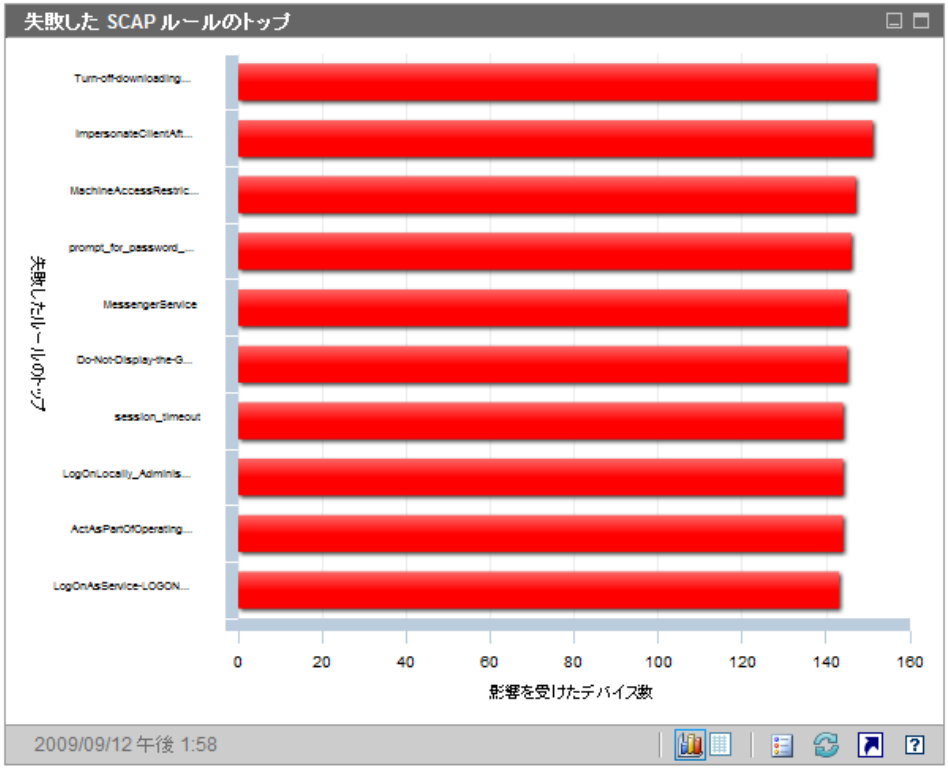
セキュリティとコンプライアンスの管理 43 ページ

上位の失敗した SCAP 規則

このペインのグラフ表示は、企業内で失敗頻度の高い上位 10 件の法規制適用状況チェック (SCAP 規則) を示します。垂直軸には、該当する適用状況規則の名前が表示されます。水平軸は、各規則の適用状況に従っていない管理対象クライアント デバイスの数を表します。

特定の規則に対して失敗したデバイスの正確な数とその規則の重大度を確認するには、グラフの色付き棒の 1 つにカーソルを置きます。

図 27　失敗した SCAP ルールのトップ



グラフの色付き棒の 1 つをクリックすると、新しいブラウザ ウィンドウが開き、[SCAP 適用状況規則 (CCE 別)] レポートが表示されます。レポートは、クリックした棒に対応する規則に基づいてフィルタされます。

このペインのグリッド表示は、各規則に対して失敗したデバイスの数とその規則自体に関する詳細情報を示します。グリッド表示で規則 ID またはデバイスの数をクリックすると、[SCAP 適用状況規則 (CCE 別)] レポートが表示されます。

関連トピック：

ダッシュボードの使用 83 ページ

適用情報管理ダッシュボード 115 ページ

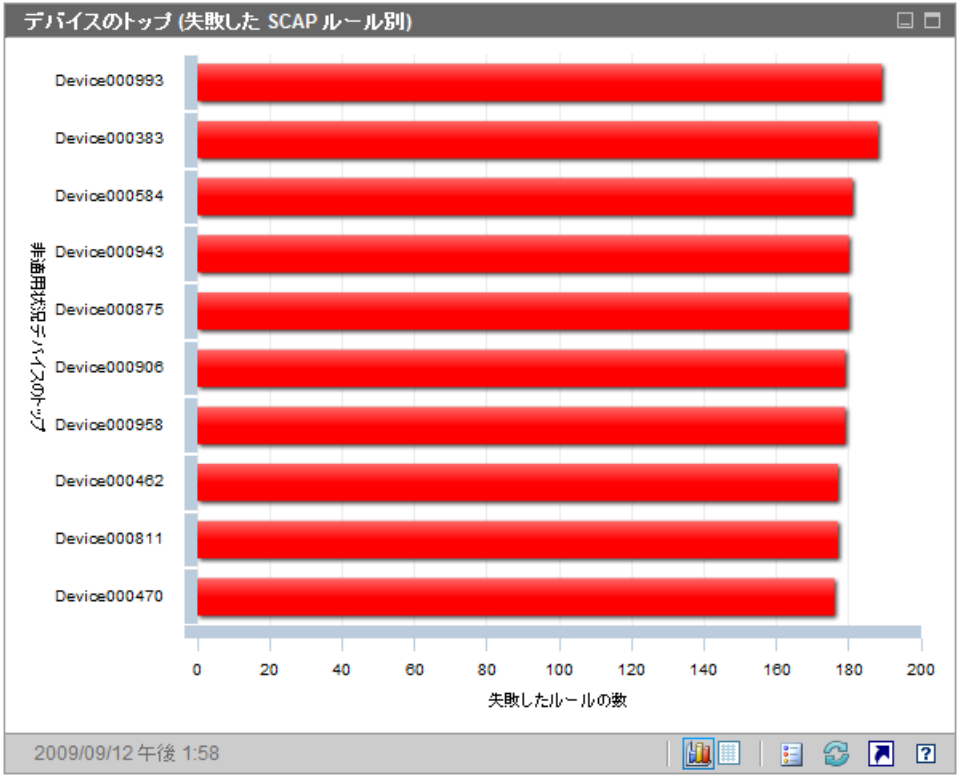
セキュリティとコンプライアンスの管理 43 ページ

失敗した SCAP ルール別のデバイスのトップ

このペインのグラフ表示は、企業内で法規制適用状況チェック (SCAP 規則) の失敗回数が多い上位 10 件の管理対象クライアント デバイスを示します。垂直軸には、該当するデバイスの名前が表示されます。水平軸は、各デバイスの最新の適用状況スキャンで失敗した適用状況規則の数を表します。

特定のデバイスの失敗した規則の正確な数を確認するには、グラフの色付き棒の 1 つにカーソルを置きます。

図 28　失敗した SCAP ルール別のデバイスのトップ



グラフ内の色付き棒のいずれかをクリックすると、新しいブラウザ ウィンドウが開き、詳細なレポートが表示されます。レポートは、クリックした棒に対応するデバイスに基づいてフィルタされます。レポートには次の 2 つの部分があります。

- レポートの [SCAP スキャン済みデバイス] 部分には、デバイスでテストされた各ベンチマークの最新のスキャン結果に関する要約情報が表示されます。
- レポートの [SCAP 適用状況規則 (CCE 別)] 部分には、最新のスキャン中にテストされた各規則の詳細結果が表示されます。

このペインのグリッド表示は、失敗した規則の数、デフォルト スコア、およびグラフ表示の各デバイスの最新スキャンの日付を示します。グリッド表示でデバイスをクリックすると、そのデバイスの [SCAP スキャン済みデバイス] レポートが表示されます。レポートは、このデバイスでテストされた各ベンチマークの最新スキャン結果を示すためにフィルタされます。

関連トピック：

ダッシュボードの使用 83 ページ

適用情報管理ダッシュボード 115 ページ

セキュリティとコンプライアンスの管理 43 ページ

セキュリティ ツール管理ダッシュボード

HPCA では、存在するセキュリティ ツールのタイプを確認し、検出された製品に関する関連情報を収集するために、企業内の管理対象クライアント デバイスをスキャンできます。次のタイプのセキュリティ製品がサポートされます。

- スパイウェア対策ツール
- ウイルス対策ツール
- ソフトウェア ファイアウォール

収集した情報は集計後、セキュリティ ツール管理ダッシュボードに表示されます。

HPCA は、実行可能なセキュリティ ツール スキャナを提供する HP Live Network と統合されます。

セキュリティ ツール管理ダッシュボードには、エグゼクティブ ビューとオペレーション ビューの 2 つのビューがあります。

エグゼクティブ ビューには、次の情報ペインがあります。

- セキュリティ製品のステータス 126 ページ
- セキュリティ製品の概要 128 ページ

オペレーション ビューには、次の情報ペインがあります。

- 最新定義の更新 130 ページ
- 最新のセキュリティ製品のスキャン 131 ページ

ダッシュボードでは、これらの任意のペインの表示 / 非表示を切り替えることができます。詳細については、318 ページの「ダッシュボード」を参照してください。

[ホーム] タブの左側のナビゲーション ペインで [セキュリティ ツール管理] をクリックすると、[セキュリティ ツール管理] ホーム ページが表示されます。このページには、関連レポートへのリンク、および環境内のセキュリティ ツール管理に関する次のようなさまざまな統計値が表示されます。

管理対象デバイス – 各種セキュリティ製品の情報を収集する HPCA セキュリティ ツール のサービスに対するエンタイトルメントを持っているデバイスの数

スキャン実施済みデバイス – HPCA セキュリティ ツール のサービスによってスキャンされたデバイスの数

前回のスキャン日 – 環境内のデバイスが HPCA セキュリティ ツール のサービスによって最後にスキャンされた日

前回ダウンロードしたスキャナ – HP Live Network サイトから HPCA へセキュリティ ツール スキャナが最後にダウンロードされた時刻 詳細については、60 ページの「HP Live Network コンテンツの更新」を参照してください。

セキュリティ製品のステータス

このペインのグラフ表示は、スパイウェア対策、ウイルス対策、ファイアウォール ソフトウェア製品などのセキュリティ ツールがインストールされ有効になっている管理対象クライアント デバイスの数を示します。この情報は、棒グラフまたは積み重ね棒グラフ形式で表示できます。どちらの場合でも、垂直軸はデバイスの数を示し、水平軸は検出されたセキュリティ ツールのタイプを示します。

グラフの色は、次の 4 つの状態を表します。

表 13　セキュリティ ツールの検出状態

色		間隔
	緑	製品が検出され有効になっている。
	黄色	製品が検出されたが有効になっていない。

表 13　セキュリティ ツールの検出状態

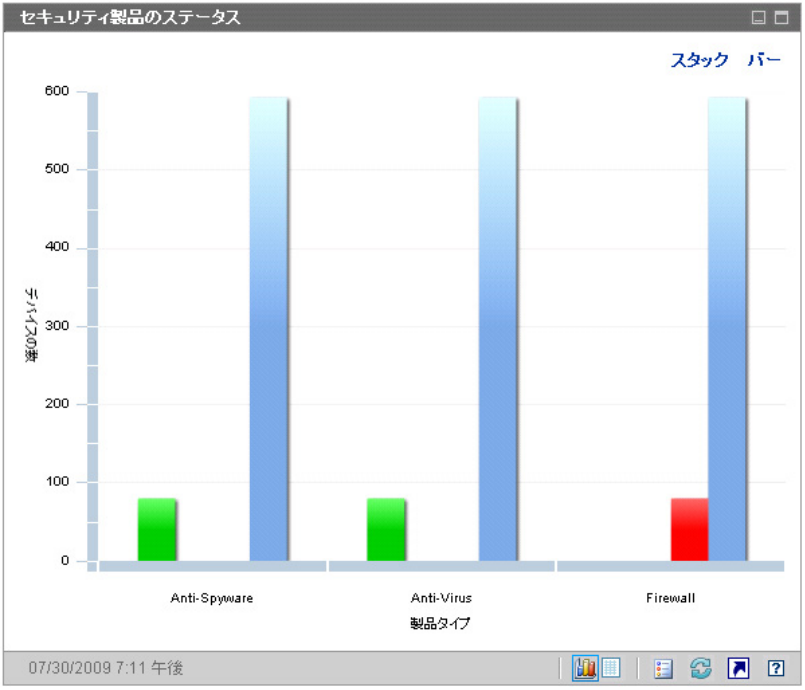
色		間隔
	赤	製品が検出されなかった。
	青	不明

次のいずれかの条件に適合する場合、スキャン済みデバイスの状態は不明とみなされます。

- HP Live Network セキュリティ ツール スキャナがこのツールを探したが、状態を判断できなかった。
- スキャナがこのツールを探したが、スキャン レコードが見つからなかった。
- スキャナがこのツールを探さなかった。

このグラフは、通常の棒グラフ形式 (次の図を参照) または積み重ね棒グラフ形式のいずれかで表示できます。

図 29　セキュリティ製品ステータス ペイン



マウス カーソルを色付きの棒上に移動すると、対応する状態のデバイスの数を示すツール チップが表示されます。

グラフの色付き棒の 1 つをクリックすると、新しいブラウザ ウィンドウが開き、フィルタされたレポートが表示されます。レポートには、そのタイプのセキュリティ製品 (ウイルス対策、スパイウェア対策、またはファイアウォール) が「検出と有効化」、「検出と無効化」、「検出されない」、または「不明」の状態になっている管理対象クライアント デバイスの数が、それぞれの状態ごとに表示されます。

このペインのグリッド ビューには、セキュリティ ツールがそれぞれの状態になっている管理対象クライアント デバイスの合計数が表示されます。

関連トピック：

ダッシュボードの使用 83 ページ

セキュリティ ツール管理ダッシュボード 125 ページ

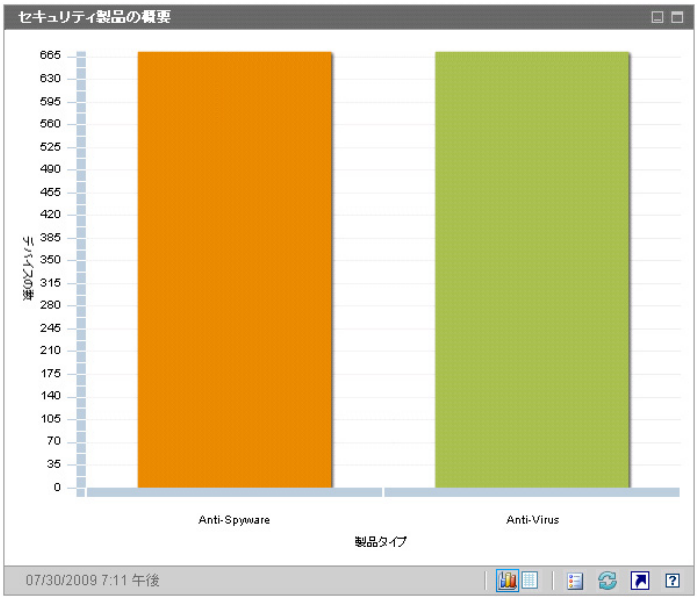
セキュリティとコンプライアンスの管理 43 ページ

セキュリティ製品の概要

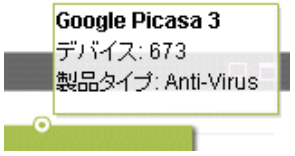
このペインのグラフ ビューには、管理対象クライアント デバイスで検出された特定のセキュリティ製品が表示されます。垂直軸はそれぞれの製品が検出されたデバイスの数を示し、水平軸は検出されたセキュリティ ツールのタイプを示します。

グラフの各色は製品の違いを表します。特定の製品の各バージョンは、異なる色で表現されます。

図 30　セキュリティ製品の概要ペイン



マウス カーソルを色付きの棒上に移動すると、特定のセキュリティ製品が検出されたデバイスの数を示すツール チップが表示されます。



グラフ内の色付きのセグメントをクリックすると、新しいブラウザ ウィンドウが開き、フィルタされたレポートが表示されます。レポートには、このタイプ (ウイルス対策、スパイウェア対策、またはファイアウォール) の特定のセキュリティ製品それぞれがインストールされている管理対象クライアント デバイスの数が表示されます。

このペインのグリッド ビューには、特定のセキュリティ製品それぞれがインストールされている管理対象クライアント デバイスの数が表示されます。

関連トピック：

ダッシュボードの使用 83 ページ

セキュリティ ツール管理ダッシュボード 125 ページ

最新定義の更新

このペインのグラフ ビューには、管理対象クライアント デバイスでウイルス定義とスパイウェア定義が最近いつ更新されたかが表示されます。この情報は、管理するクライアント デバイスで検出されたすべてのウイルス対策製品とスパイウェア対策製品に関するものです。

この情報は、デバイスの数 (カウント) またはパーセンテージの形式で表示できます。棒の色は、次の更新間隔を表します。

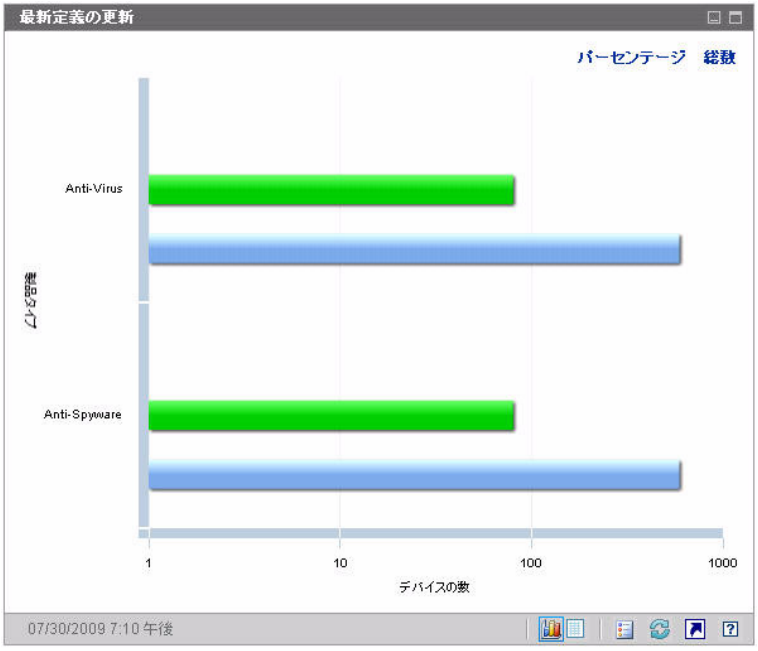
表 14　更新間隔

色		間隔
	赤	4 週間を超える
	黄色	2 ～ 4 週間
	緑	2 週間未満
	グレイ	なし
	青	不明な更新

マウス カーソルを色付きの棒上に移動すると、対応する時間間隔内に更新されたデバイスの数とパーセンテージを示すツール チップが表示されます。

このグラフの総数ビューでは対数スケールを使用するため、特定の時間間隔に含まれるデバイスが 1 つだけの場合、その時間間隔のデータはこのビューに表示されません。これは、対数目盛りの既知の制限です。データはパーセンテージ ビューで表示できますが、グリッド ビューでも表示可能です。

図 31　最新定義の更新



このペインのグリッド ビューには、同じ情報がテーブル形式で表示されます。グリッド ビューでは、パーセンテージではなく常にデバイス数が使用されます。

グラフ ビューの色付きの棒をクリックすると、新しいブラウザ ウィンドウが開き、フィルタされたレポートが表示されます。レポートには、それぞれの時間間隔内にウイルス対策定義またはスパイウェア対策定義が更新された管理対象クライアント デバイスの数が表示されます。

関連トピック：

ダッシュボードの使用 83 ページ

セキュリティ ツール管理ダッシュボード 125 ページ

セキュリティとコンプライアンスの管理 43 ページ

最新のセキュリティ製品のスキャン

このペインのグラフ ビューには、管理対象クライアント デバイスでウイルス対策製品とスパイウェア対策製品が最近いつスキャンされたかが表示されます。この情報は、管理するクライアント デバイスで検出されたすべてのウイルス対策製品とスパイウェア対策製品に関するものです。

この情報は、デバイスの数 (カウント) またはパーセンテージの形式で表示できます。棒の色は、次の更新間隔を表します。

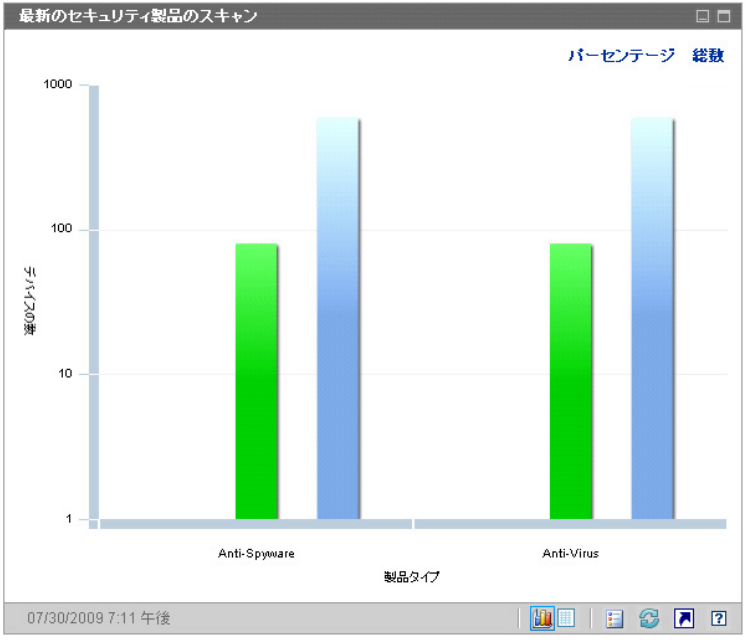
表 15　スキャン間隔

色		間隔
	赤	4 週間を超える
	黄色	2 ～ 4 週間
	緑	2 週間未満
	グレイ	なし
	青	不明なスキャン

マウス カーソルを色付きの棒上に移動すると、対応する時間間隔内にスキャンされたデバイスの数とパーセンテージを示すツール チップが表示されます。

このグラフの総数ビューでは対数スケールを使用するため、特定の時間間隔に含まれるデバイスが 1 つだけの場合、その時間間隔のデータはこのビューに表示されません。これは、対数目盛りの既知の制限です。データはパーセンテージ ビューで表示できますが、グリッド ビューでも表示可能です。

図 32　最新のセキュリティ製品のスキャン



このペインのグリッド ビューには、同じ情報がテーブル形式で表示されます。グリッド ビューでは、パーセンテージではなく常にデバイス数が使用されます。

グラフビューの色付きの棒をクリックすると、新しいブラウザウィンドウが開き、フィルタされたレポートが表示されます。レポートには、それぞれの時間間隔内に関係するセキュリティ ツール (ウイルス対策またはスパイウェア対策) によって最後にスキャンされた管理対象クライアントデバイスの数が表示されます。

関連トピック：

ダッシュボードの使用 83 ページ

セキュリティ ツール管理ダッシュボード 125 ページ

セキュリティとコンプライアンスの管理 43 ページ

パッチ管理ダッシュボード

パッチ管理ダッシュボードには、ネットワーク内の管理対象デバイスで検出された任意のパッチ脆弱性に関する情報が表示されます。

パッチ管理ダッシュボードのエグゼクティブ ビューには、次の 2 つの情報ペインがあります。

- ステータス別デバイス適用状況 (エグゼクティブ ビュー) 134 ページ
- ブリテン別デバイス適用状況 136 ページ

オペレーションビューには、次の 3 つの情報ペインがあります。

- ステータス別デバイス適用状況 (オペレーション ビュー) 138 ページ
- Microsoft セキュリティ ブリテン 139 ページ
- 最も脆弱性の高い製品 140 ページ

ダッシュボードでは、これらの任意のペインの表示 / 非表示を切り替えることができます。318 ページの「ダッシュボード」を参照してください。

[ホーム] タブの左側のナビゲーション ペインで [パッチ管理] をクリックすると、パッチ管理のホーム ページが表示されます。このページには統計と関連レポートへのリンクが掲載されています。

ステータス別デバイス適用状況 (エグゼクティブ ビュー)

このペインのグラフ ビューには、パッチ ポリシーに現在適合しているネットワーク内のデバイスのパーセンテージが表示されます。円グラフ内の色付きの扇形は、次の状態を表します。

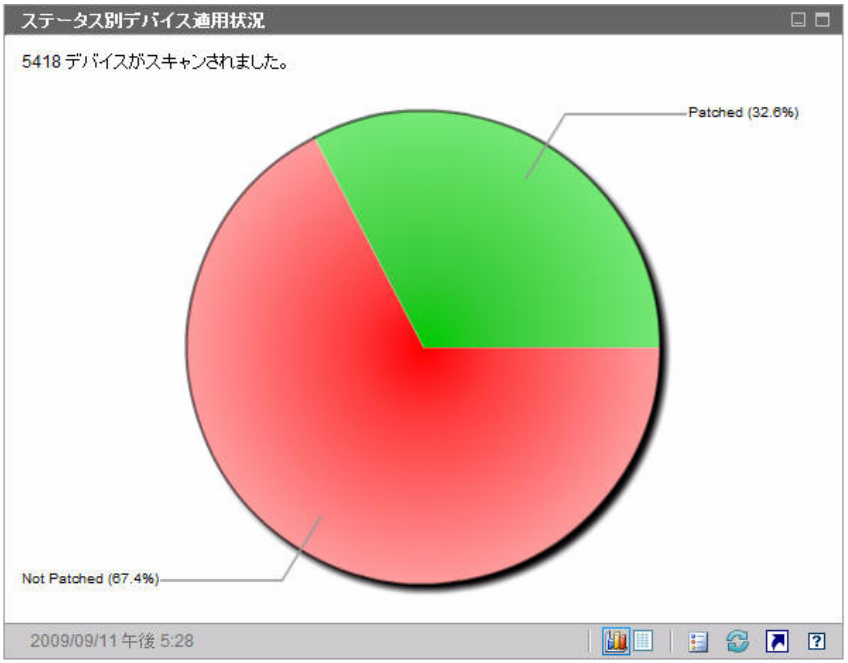
- パッチ適用済み (緑)
- パッチ未適用 (赤)

138 ページの「ステータス別デバイス適用状況 (オペレーション ビュー)」に似ていますが、オペレーション ビューにはさらに詳しい情報が表示されます。

表 16　ステータス別デバイス適用状況ビュー

エグゼクティブ ビュー	オペレーション ビュー
パッチ適用済み	パッチ適用済み 警告
パッチ未適用	パッチ未適用 再起動の保留 その他

図 33　ステータス別デバイス適用状況



特定のカテゴリのデバイス数を表示するには、カーソルを円グラフの色付き部に移動します。

円グラフ内の色付きの扇形をクリックすると、新しいブラウザ ウィンドウが開き、フィルタされたレポートが表示されます。レポートには、クリックした扇形に対応するパッチ適用状況ステータスのすべてのデバイスが表示されます。

このペインのグリッド ビューには、円グラフに表示されているそれぞれの適用状況にあるネットワーク デバイスの数が表示されます。

ブリテン別デバイス適用状況

このペインのグラフ ビューには、ネットワーク内で最大数のデバイスに影響するパッチ脆弱性が 10 種類表示されます。垂直軸には、これらの脆弱性についてのパッチ ブリテン番号の一覧が表示されます。水平軸は影響を受けたデバイスの数を表し、対数尺度を使用します。

特定のブリテンが 1 つのデバイスにのみ影響する場合、グラフ ビューにそのブリテンのデータは表示されません。これは、対数目盛りの既知の制限です。ただし、グリッド表示ではデータが表示されます。

ブリテンの名前と影響を受けるデバイスの数を表示するには、カーソルを色付きのいずれかの棒上に合わせます。

図 34　ブリテン別デバイス適用状況

グラフの色付き棒の 1 つをクリックすると、新しいブラウザ ウィンドウが開き、フィルタされたレポートが表示されます。このレポートには、このパッチ脆弱性を持つ管理対象デバイスが表示されます。

グリッド ビューには、検出された上位 10 件のパッチ脆弱性に関する次の情報が表示されます。

- ブリテン – この脆弱性の Microsoft セキュリティブリテン
- 説明 – ブリテンのタイトル
- パッチ未適用 – このパッチ脆弱性を持つデバイスの数

初期状態のテーブルは、[パッチ未適用] を基準にソートされています。ソート パラメータを変更するには、対応するカラム見出しをクリックします。

特定のブリテンについての詳細を表示するには、ブリテン番号をクリックしてください。

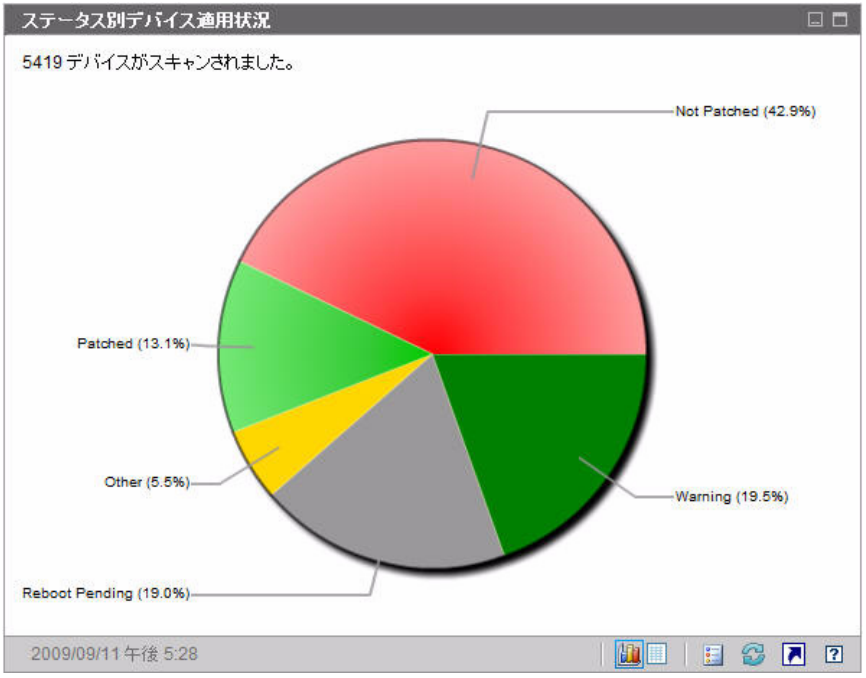
ステータス別デバイス適用状況 (オペレーション ビュー)

このペインのグラフ ビューには、パッチ ポリシーに現在適合しているネットワーク内のデバイスのパーセンテージが表示されます。特定のカテゴリのデバイス数を表示するには、カーソルを円グラフの色付き部に移動します。

このペインは、「ステータス別デバイス適用状況 (エグゼクティブ ビュー)」ペインに似ています。このペインにはより詳細な情報が表示され、使用される色は Patch Manager の場合と同じです。

- パッチ適用済み (薄緑)
- パッチ未適用 (赤)
- 再起動の保留 (薄いグレイ)
- 警告 (深緑)
- その他 (黄)
- 適用できません (濃いグレイ)

図 35　ステータス別デバイス適用状況 (オペレーション ビュー)



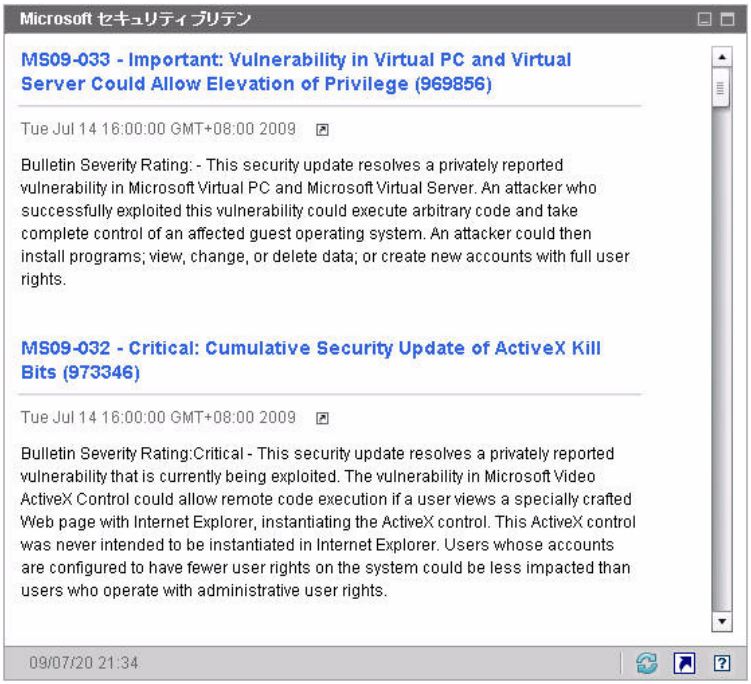
円グラフ内の色付きの扇形をクリックすると、新しいブラウザ ウィンドウが開き、フィルタされたレポートが表示されます。レポートには、クリックした扇形に対応するパッチ適用状況ステータスのすべてのデバイスが表示されます。

グリッド ビューには、円グラフに表示されているそれぞれの適用状況にあるネットワーク デバイスの数が表示されます。

Microsoft セキュリティ ブリテン

このペインには、最新の Microsoft セキュリティブリテンが表示されます。デフォルトでは、この情報は Microsoft Corporation から RSS フィードによって提供されます。フィードの URL は、[設定] タブを使用して変更できます (318 ページの「ダッシュボード」を参照してください)。

図 36　Microsoft セキュリティ ブリテン



特定のブリテンの詳細を表示するには、ブリテン名のすぐ下にある アイコンをクリックします。

このペインにはグラフ表示はありません。

最も脆弱性の高い製品

このペインはデフォルトで無効になっています。有効にする方法については、318 ページの「ダッシュボード」を参照してください。

このペインのグラフ ビューには、ネットワーク内で最多のパッチ脆弱性が存在するソフトウェア製品が表示されます。垂直軸には、ソフトウェア製品の一覧が表示されます。水平軸は、企業内の適用可能な管理対象デバイス全体でまだ適用されていない、特定の製品に関係するパッチの合計数が反映されます。次に例を示します。

ABC という製品にパッチを含むブリテンが 6 件あるとします。

— 10 個の管理対象デバイスで 6 件のパッチすべてを必要としている

— 20 個の管理対象デバイスでそれらのパッチのうちの 3 件を必要としている

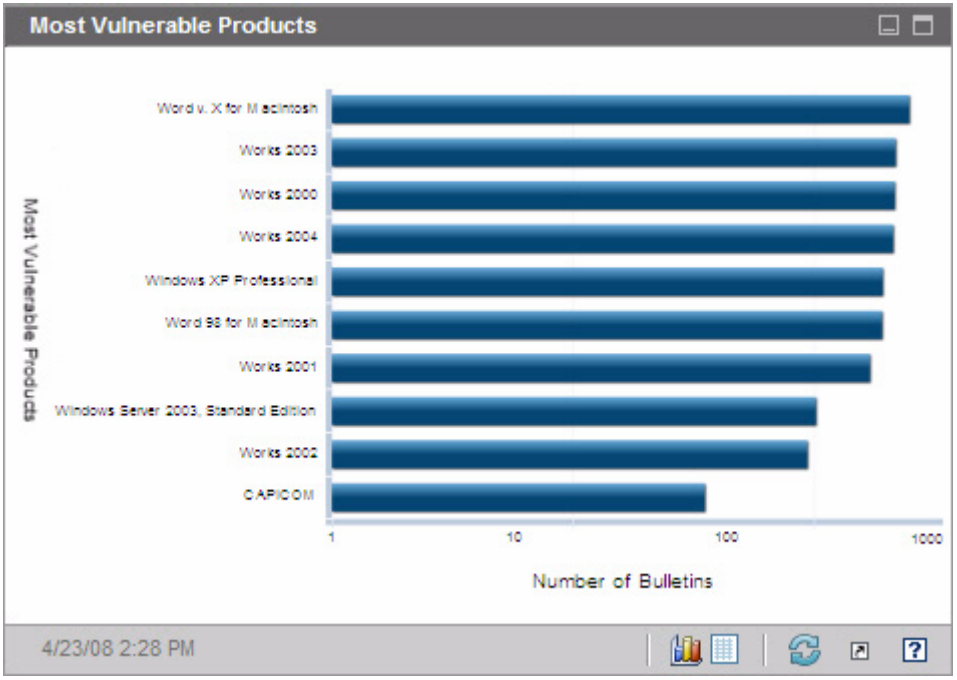
— 50 個の管理対象デバイスでそれらのパッチのうち 1 件のみを必要としている

ABC のブリテンの数 = (10 x 6) + (20 x 3) + (50 x 1) = 170

このグラフでは対数スケールを使用するため、特定の製品のブリテンの数が 1 の場合、その製品のデータはグラフ ビューに何も表示されません。これは、対数目盛りの既知の制限です。ただし、グリッド表示ではデータが表示されます。

特定のソフトウェア製品にパッチが適用されていないデバイスの数を表示するには、カーソルを色付きのいずれかの棒上に合わせます。

図 37　最も脆弱性の高い製品



グリッド ビューには、製品ごとに次の情報が表示されます。

- 製品 – ソフトウェア製品の名前
- パッチ未適用 – 特定の製品の適用可能なすべてのデバイスでパッチが適用されていないブリテンの数
- 適用可能なデバイス – この製品がインストールされているデバイスの数

- 適用可能なブリテン – この製品に関連する Microsoft セキュリティ ブリテンの数

初期状態のテーブルは、[パッチ未適用] を基準にソートされています。ソート パラメータを変更するには、対応するカラム見出しをクリックします。

5 Enterprise の管理

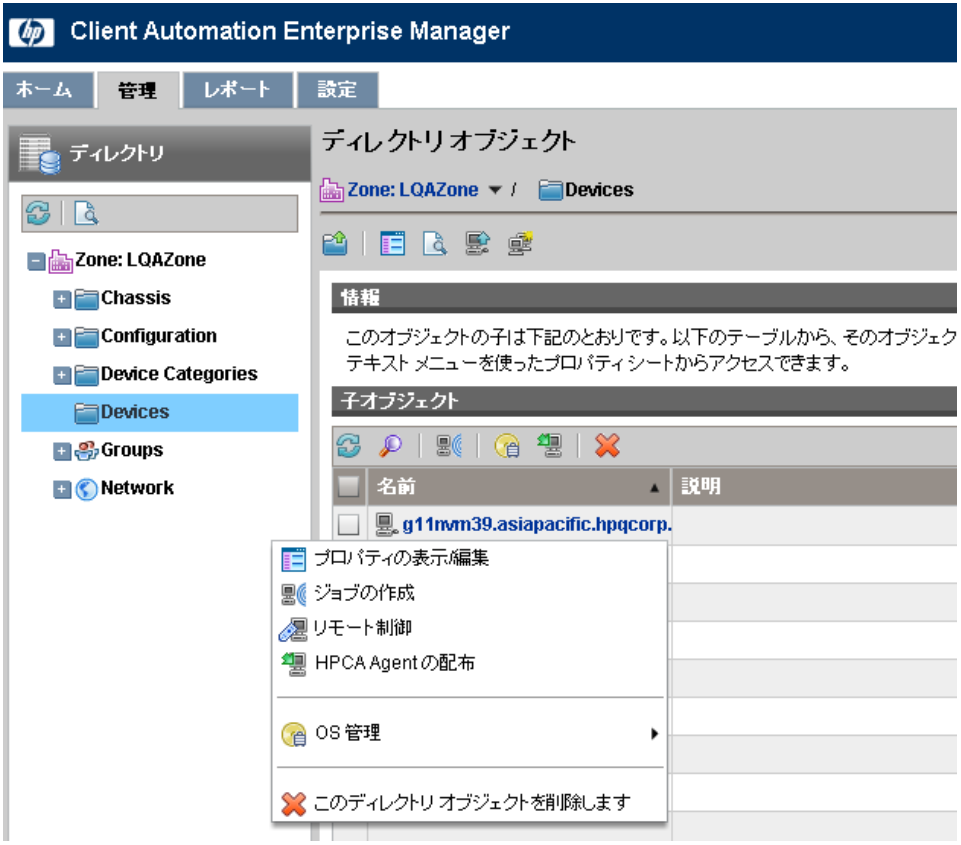
[管理] 領域には、使用環境のクライアント デバイスを管理するために使用するツールが配置されています。この章には、次のトピックがあります。

ディレクトリ ポリシーの管理

[管理] タブの [ディレクトリ] ツリーから、設定したディレクトリ サービス内のオブジェクトを確認できます。267 ページの「ディレクトリ サービス」を参照してください。たとえば、オブジェクトのプロパティを表示したり、そのポリシーを作成したり、そのエンタイトルメントを表示したりすることができます。

左のナビゲーション ツリーでディレクトリ オブジェクトをクリックすると、コンテンツ ペインにその子の一覧が表示されます。カーソルを一覧にある子オブジェクトの名前の上に合わせると、ドロップダウン メニューが表示されます。メニューを表示するには下矢印をクリックします。メニューに表示されるオプションは、オブジェクトが存在する階層コンテキストと現在有効になっている HPCA の機能によって異なります。

図 38　ディレクトリ オブジェクト ビュー



次の表に、子オブジェクトのドロップダウン メニューから実行可能なアクションをまとめます。

表 17　ドロップダウン メニューに表示されるアクション

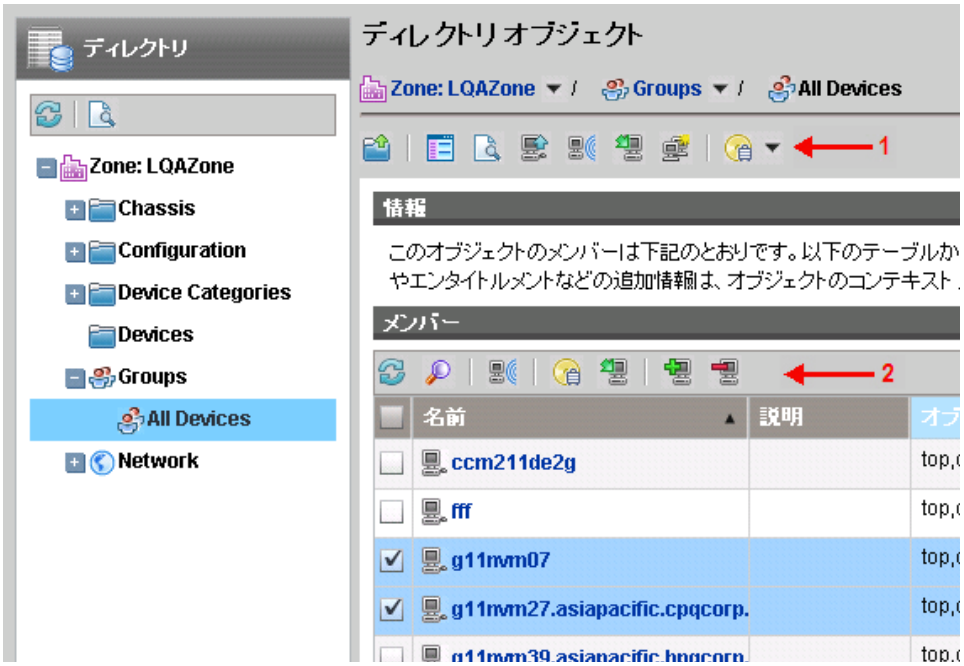
アイコン	アクション	説明
	プロパティの表示 / 編集	新しいブラウザ ウィンドウで、この子オブジェクトのプロパティを表示または編集する。144 ページの「ディレクトリ オブジェクト ビュー」を参照してください。
	ジョブの作成	このオブジェクトの通知ジョブまたは DTM ジョブを作成する。158 ページの「ジョブを管理する」を参照してください。
	リモート制御	管理対象デバイスにリモート アクセスする。180 ページの「デバイスのリモート制御」を参照してください。
	HPCA Agent の配布	このデバイスに HPCA Agent を配布し、HPCA によって管理できるようにする。156 ページの「HPCA Agent の配布」を参照してください。
	OS 管理	オペレーティング システムを配布するか、1 回限りのハードウェア メンテナンス操作を実行する。186 ページの「オペレーティング システムの管理」を参照してください。
	アウトバンドの詳細を表示	Intel vPro を搭載するデバイスまたは DASH が有効なデバイスのアウトバンドの詳細を表示する。200 ページの「アウトバンドの詳細の表示」を参照してください。
	このディレクトリ オブジェクトを削除します	HPCA データベースからこのオブジェクトを削除する。153 ページの「デバイスのインポート」を参照してください。

ディレクトリ オブジェクト ビューには、2 種類のツールバーがあります。

- 上側のツールバーは、[ディレクトリ] ツリーで選択されたオブジェクトに関連しています。
- 下側のツールバーは、グリッド内の選択された子オブジェクトに関連しています。

146 ページの図 39 に示す例では、全デバイス グループが選択されています。

図 39　ディレクトリ オブジェクト ビューのツールバー

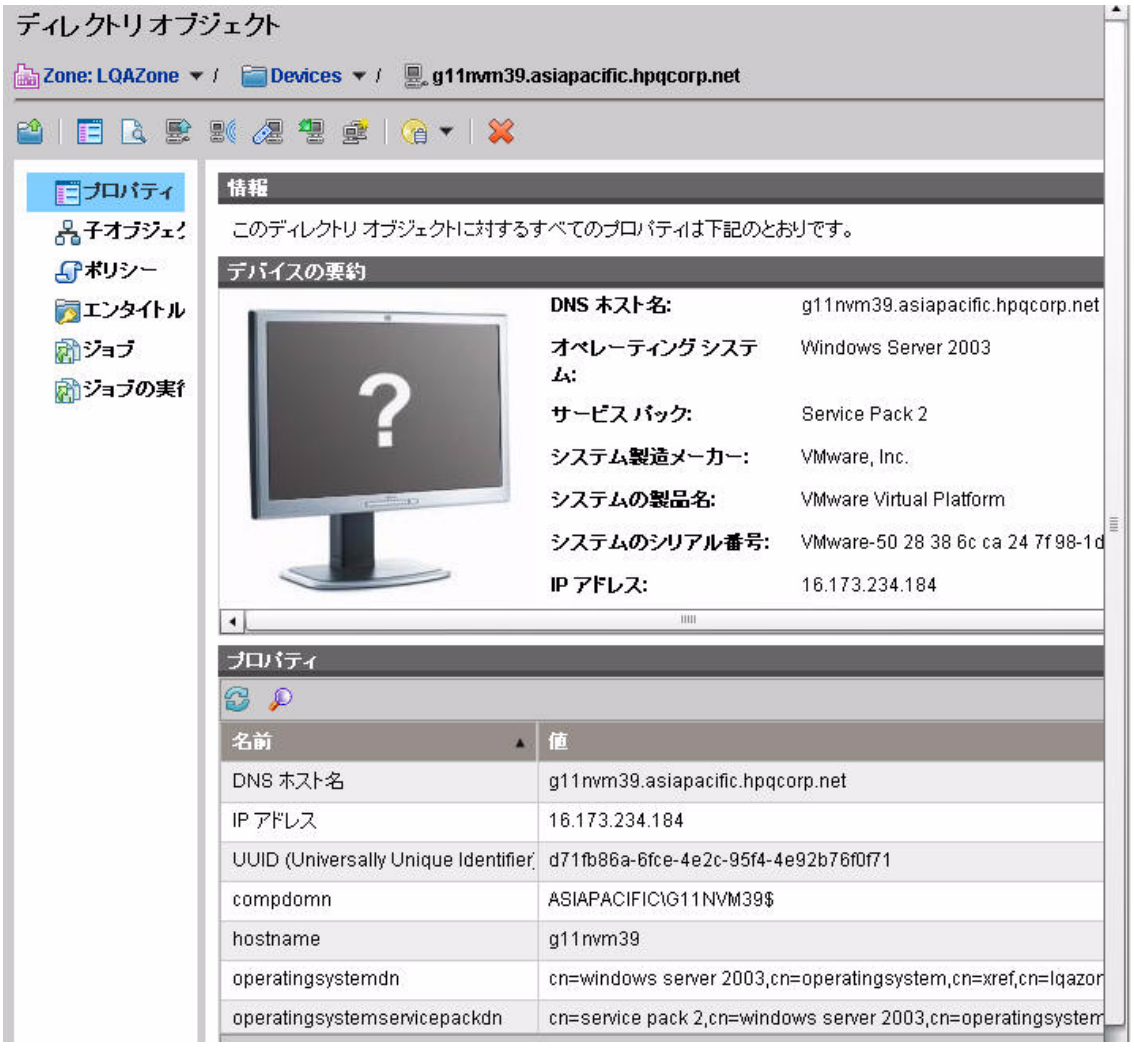


この例では、上側のツールバー (1) が全デバイス グループに関連し、下側のツールバー (2) がグリッドで選択した子 (またはメンバー) に関連しています (この場合は、Device110 と Device113)。

オブジェクトのプロパティの表示

ディレクトリ オブジェクトの **[プロパティの表示 / 編集]** を選択すると、このオブジェクトのプロパティが新しいブラウザ ウィンドウに表示されます (147 ページの図 40 を参照)。

図 40　ディレクトリ オブジェクトのプロパティ ウィンドウ



ここでは、次のアクションを実行できます。

- **[子オブジェクト]** をクリックすると、オブジェクトの子を表示できます。コンテンツ ペインで子オブジェクトをブラウズするには、そのオブジェクトをクリックします。
- **[メンバー]** をクリックすると、オブジェクトのメンバーを表示できます。オブジェクトにメンバーが含まれていない場合、このリンクは表示されません。
- **[ポリシー]** をクリックすると、オブジェクトのローカル ポリシーの設定を表示したり、このオブジェクトにポリシーを作成したりできます。
- **[エンタイトルメント]** をクリックすると、このオブジェクトの解決されたポリシーをすべて表示できます。
- **[ジョブ]** をクリックすると、このオブジェクトの現在と過去のジョブを一覧表示できます。このオブジェクトにジョブがない場合、このリンクは表示されません。
- **[ジョブの実行]** をクリックすると、このオブジェクトの DTM ジョブの実行を一覧表示できます。詳細については、160 ページの「ジョブおよびジョブの実行」を参照してください。
- **[仮想マシン]** をクリックすると、サーバー上に存在するすべての仮想マシンのリストを表示できます。このリンクが表示されるのは、選択したオブジェクトが VMware ESX Server である場合のみです。詳細については、173 ページの「仮想マシンの管理」を参照してください。

オブジェクトの検索

HPCA Console には、ディレクトリ オブジェクトを検索する機能が用意されています。この検索はコンテキストに基づきます。つまり、検索を開始するとき、その検索のルートは現在のディレクトリ オブジェクトになります。検索は、メイン ウィンドウと [ディレクトリ オブジェクト] ウィンドウのどちらからでも開始できます。両方のウィンドウに検索ボタンがあります。

子オブジェクトを大量に含むディレクトリ オブジェクトは、大量のレコードを取得しようとしてタイムアウトする場合があります。コンソールがタイムアウトしても、バックグラウンド プロセスはデータが 10,000 レコードに到達するまでデータの取得を続けます。この状態になったら、**[リフレッシュ]** ボタンをクリックしてリクエストをやり直してください。

子ノードが 5000 件を超えるディレクトリ オブジェクトでは、検索インターフェイスを使用してリスト内のノードに移動してください。この方法により、大量の子が含まれるノードをブラウズすることによるタイムアウトの可能性を回避できます。

ディレクトリ オブジェクトを検索するには

1 [管理] タブの **[ディレクトリ]** 領域で、[ディレクトリの検索]  ボタンをクリックします。

2 [ディレクトリ検索] ボックスで、次のパラメータを定義できます。

- 左のナビゲーション メニューで項目を選択することにより、検索の識別名 (DN) を指定します。
- 検索の **[範囲]** で、現在のレベルを選択するか、または現在のレベルとディレクトリ階層のそれ以下のすべてのレベルを選択します。
- 属性および演算子を選択し、条件を入力して、**[フィルタ]** を作成します。

> OBJECTCLASS フィルタを使用する場合の有効な条件は、「等しい」または「等しくない」のいずれかに限られます。また、Active Directory など特定のディレクトリは、一部の属性の検索文字列に含まれるワイルドカード文字をサポートしません。

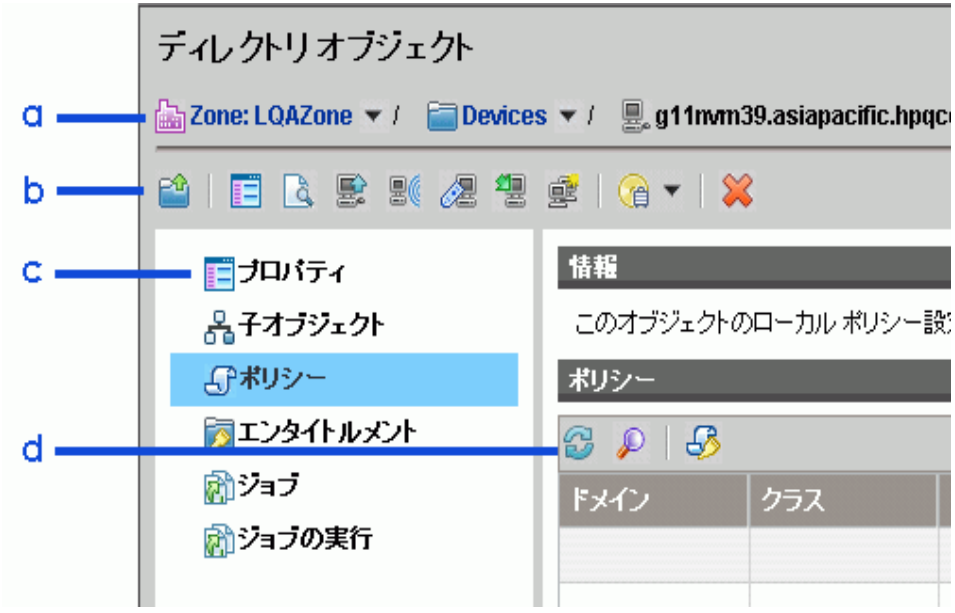
3 **[検索]** をクリックします。指定した条件と一致するオブジェクトは、[検索結果] テーブルに一覧表示されます。

4 **[リセット]** をクリックして、新しい検索を開始します。

ディレクトリ オブジェクトのポリシーの管理

[ディレクトリ オブジェクト] の [プロパティ] ウィンドウ (147 ページの図 40 を参照) では、オブジェクトのローカル ポリシー設定を管理できます。

図 41　ディレクトリ オブジェクト ポリシーの詳細



凡例

a　選択したディレクトリ オブジェクトへのパス

b　ディレクトリ オブジェクト ツールバー :

- 親オブジェクトのブラウズ
- このオブジェクトのプロパティを表示 / 編集
- ディレクトリの検索
- HPCA デバイス リポジトリにデバイスをインポート
- HPCA ジョブの作成

新しいリモート制御セッションの開始

HPCA Agent の配布

新しいグループの作成

OS 管理タスクの実行

このディレクトリ オブジェクトを削除します

c オブジェクト リンク (146 ページの「オブジェクトのプロパティの表示」を参照)

d ポリシー管理ツールバー :

リフレッシュ

フィルタの表示 / 非表示

ポリシー管理ウィザードの起動

ディレクトリ オブジェクトのポリシーを管理するには

1 **[管理]** タブで、**[ディレクトリ]** をクリックします。使用可能なディレクトリ サービスのリストが展開されます。

2 展開するディレクトリ サービスをクリックします。

3 そのディレクトリ サービスのコンテナまたは子をクリックします。

特定のディレクトリ オブジェクトを操作するには、そのオブジェクトに移動し、ドロップダウン メニューから **[プロパティの表示 / 編集]** を選択します。新しいブラウザ ウィンドウが開き、そのディレクトリ オブジェクトが表示されます。

ここでは例として、1 つのデバイスにポリシーを作成します。

150 ページの図 41 では、[ディレクトリ オブジェクト] ウィンドウのさまざまなセクションを説明しています。

4 左のナビゲーション メニューで、**[ポリシー]** リンクをクリックします。

[ポリシー] リンクをクリックすると、HPCA Console によってパーミッションが確認されます。書き込みパーミッションがない場合は、[ポリシー管理ウィザード] ボタンが無効 (グレー表示) になります。

5 **[ポリシー管理ウィザード]** ボタンをクリックします。

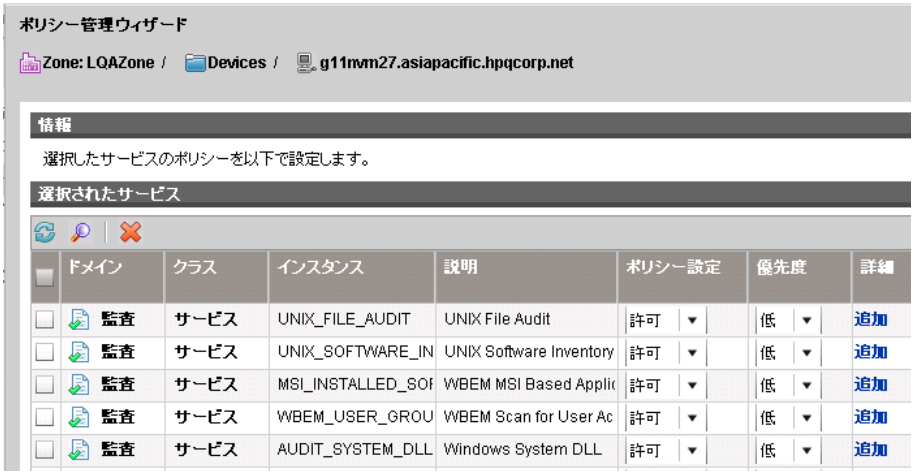
6 [手順 1/3 : サービスの選択] では、オブジェクトのポリシーに追加するサービスを選択します。サービスの選択元の Configuration Server Database ドメインを選択します。

7 追加する各サービスの左側にあるボックスをオンにします。

8 **[追加]** をクリックして、ウィザード画面の右側にあるツリー ビューにサービスを移動します。

9 必要なサービスをすべて追加したら、**[次へ]** をクリックします。

10 [手順 2/3 : ポリシーの設定] で、それぞれのサービスにポリシーのタイプと優先度を設定します。以下のサンプル画像には、Audit ドメインからの 1 つのサービスが表示されています。



— **[ポリシー設定]** を [許可] または [拒否] に設定します。

— **[優先度]** を [低]、[中]、または [高] に設定します。

— **[詳細]** カラムで **[追加]** をクリックして、オブジェクトの条件に Client Automation の属性と式を追加します。『Policy Server ガイド』を参照してください。

[詳細] 機能は、Configuration Server Database と HPCA インフラストラクチャに十分に精通している経験を積んだ HPCA 管理者のみが使用してください。

11 ポリシーを設定したら、**[次へ]** をクリックします。

12 [手順 3/3 : 設定の要約] で、設定を確認します。**[適用]** をクリックして、ポリシー管理ウィザードを完了します。

13 **[閉じる]** をクリックして、ダイアログを確認します。

サービス情報

HPCA Console にサインインした後は、Configuration Server から使用できるサービスを表示できます。サービスとは、たとえばアプリケーションのように 1 つのユニットとして管理されるデータのセットです。サービスは、CSDB Editor を使用して作成します。サービスの詳細については、『管理者ガイド』を参照してください。

使用可能なサービスを表示するには

1 **[管理]** タブで、**[サービス]** をクリックします。使用可能な Configuration Server Database ドメインの一覧が表示されます。

2 表示するサービスを含むドメインをクリックします。

3 表示される使用可能なサービスの一覧を絞り込むには、**[フィルタ入力の表示 / 非表示]** ボタンをクリックしてフィルタ オプションを表示します。

4 詳細を表示するサービスをクリックします。

- **[カタログ]** タブには、Configuration Server Database (CSDB) のサービスの属性が表示されます。
- **[レポート]** タブに、サービスについての要約レポートが表示されます。

デバイスのインポート

HPCA Agent をデバイスに配布するには、まずそのデバイスを HPCA にインポートする必要があります。また、HPCA を使用して管理するすべての VMware ESX Server もインポートする必要があります。

デバイスをインポートすると、そのデバイスのディレクトリ オブジェクトが作成されます。ただし、有効なデバイスを指定したかどうかの検証は行われません。

デバイスをインポートするには

1 **[管理]** タブで、[ディレクトリ] 領域に移動し、**[デバイス]** をクリックします。

2  (デバイス インポート ウィザード) ボタンをクリックします。

3 **[デバイスの IP/ ホスト名]** テキスト ボックスに、デバイスのホスト名または IP アドレスのカンマ区切りリストを入力するか、貼り付けます。

4 [デバイスの分類] ドロップダウンで、デバイスのグループに適切な分類を選択します。

   — **事前に設定された分類はありません** – デバイスは分類なしでインポートされます。

   — **VMware ESX Server** – この分類でインポートされるデバイスごとに、[デバイス オブジェクト] ウィンドウの [仮想マシン] リンクを有効にします。173 ページの「仮想マシンの管理」を参照してください。

5 **[追加]** をクリックします。[デバイスのインポート] リストにデバイスが追加されます。

   リストからデバイスを削除するには、デバイスの左にあるチェックボックスをオンにして、  (削除) ボタンをクリックします。

6 リストの内容を確認し、**[適用]** をクリックします。デバイスが [デバイス] コンテナにインポートされます。また、全デバイス グループにも追加されます。

7 **[閉じる]** をクリックして、ダイアログを確認します。

デバイスを削除するには

以前にインポートしたデバイスを削除するには、そのデバイス オブジェクトのページに移動し、  (このディレクトリ オブジェクトを削除します) ボタンをクリックします。

グループの管理

グループは、HPCA Agent を配布したり、更新されたソフトウェアが入手可能なことをデバイスに通知するジョブを作成したりなど、多くのデバイスで一度にタスクを実行するために使用します。デバイスは、グループ作成時に定義する検索条件に基づいてグループに追加されます。以降のセクションでは、実行可能なグループ管理タスクについて説明します。

外部ディレクトリ グループを作成するには

マウントされた外部ディレクトリ ソース (LDAP や Active Directory など) のグループは、ディレクトリ サービスで用意されているツールを使用して作成する必要があります。詳細については、システム管理者にお問い合わせください。

内部ディレクトリ グループを作成するには

次の手順に従って内部ディレクトリのグループを作成します。HPCA Console で作成するグループは、[グループ] コンテナの下の内部ゾーンに作成されます。

1 [管理] タブのツールバーで、**[新しいグループの作成]**  をクリックします。

HPCA グループ作成ウィザードが開きます。

2 グループの名前と説明を入力します。

3 **[デバイスの追加]**  をクリックします。

[デバイスの追加] ウィンドウが開きます。

4 [検索パラメータ] を定義し、**[検索]** をクリックしてデバイスの一覧を表示します (パラメータを定義せずに **[検索]** をクリックすると、使用可能なデバイスすべての一覧が返されます)。

5 追加するデバイスを選択し、**[追加]** をクリックします。

デバイスを追加し終えたら、[デバイスを新しいグループに追加] ウィンドウを閉じます。

6 デバイスを削除するには、メンバー グリッドでデバイスを選択し、**[デバイスを削除]**  をクリックします。

7 **[サブミット]** をクリックします。内部ゾーン内の [グループ] コンテナに新しいグループが追加されます。

グループの説明またはデバイスを修正するには

1 ナビゲーション ツリーを使用し、修正するグループを選択します。

2 ツールバーまたはグループのコンテキスト ドロップダウン メニューを使用して、**[プロパティの表示 / 編集]** を選択します。

グループの [ディレクトリ オブジェクト] ウィンドウが開きます。

3 **[プロパティ]** リンクをクリックしてプロパティ ページを表示し、グループの名前または説明を修正します。**[保存]** をクリックして、変更を適用します。

4 **[メンバー]** リンクをクリックして、そのグループに属するデバイスの一覧を表示します。

5 **[デバイスの追加]** または **[デバイスの削除]** ツールバー ボタンを使用して、グループ メンバーシップを更新します。

6 更新を完了したら、[ディレクトリ オブジェクト] ウィンドウを閉じます。

グループを削除するには

1 ナビゲーション ツリーを使用し、削除するグループを選択します。

2 **[このディレクトリ オブジェクトを削除します]** をクリックします。

これにより、そのグループ オブジェクトだけが削除されます。グループ内のサービスは削除されません。

HPCA Agent の配布

HPCA Agent は、使用環境のデバイスを管理するために使用します。Agent 配布ウィザードを使用して HPCA Agent を配布してください。HPCA Agent の詳細については、『HP Client Automation Application Manager および Application Self-Service Manager ガイド』を参照してください。

HPCA Agent は、単一デバイスやグループに属する複数のデバイスに配布できます。ディレクトリ オブジェクト ツリーを使用してデバイスを指定し、Agent 配布ウィザードを使用して配布ジョブを作成します。

HPCA Agent を正常に配布するには、クライアント デバイス側で次の要件を満たしている必要があります。

- Windows Firewall が無効になっている。

- ネットワーク経由でサーバーから HPCA Agent にアクセスできる。
- Windows XP に配布する場合は、簡易ファイルの共有が無効になっている。
- Windows Vista に配布する場合、ローカルに定義された管理者に対して Windows Vista デバイスの管理共有 (C$) へのアクセスが無効になっている。このため、Windows Vista デバイスがドメインの一部になっており、そのドメインの管理者の認証情報は、HPCA Agent の配布時に指定する必要があります。デバイスがドメインの一部でない場合、その他の手順ではローカルの管理者にアクセスを許可する必要があります。詳細な手順については、Microsoft のサポート Web サイトで次のリンクを参照してください。

  http://support.microsoft.com/kb/947232/en-us

  これらの変更が終了したら、デバイスを再起動します。

HPCA Agent を配布するには

1 ディレクトリ オブジェクト ツリーで、HPCA Agent の配布先デバイスを含むディレクトリ オブジェクトを選択します。

2 リストからデバイスを選択し、**[HPCA Agent 配布ウィザードの起動]**  をクリックします。Agent 配布ウィザードが開きます。

3 **手順 1**:

   a HPCA Agent の配布時に使用する認証情報を指定します。インストールを実行するには、これらの認証情報に適切な管理者パーミッションが含まれている必要があります。

   b HPCA Agent をサイレント モードでインストールするには、**[サイレント インストール]** チェックボックスをオンにします。これにより、インストール ユーザー インターフェイスによってターゲット デバイスが開かないようにします。

4 **[次へ]** をクリックします。

5 **手順 2** で、Agent 配布ジョブの実行時刻に関するスケジュール情報を入力します。

6 **[次へ]** をクリックします。

7 **手順 3** で、ジョブの要約情報の内容を確認します。

8 **[サブミット]** をクリックします。

ウィザードでの手順が完了すると、Agent 配布ジョブが作成されます。配布ジョブは、ジョブに含まれるすべてのデバイスに HPCA Agent が配布されると完了します。すべてのジョブのステータスを確認するには、**[ジョブ]** 領域 (158 ページの「ジョブを管理する」を参照) を使用します。

ジョブを管理する

[管理] タブの [ジョブ] 領域を使用して、現在および過去のジョブを表示および管理します。[ジョブ] 領域には、次の 2 つのカテゴリがあります。

- **[すべてのジョブ]** カテゴリには、すべての HPCA Console ユーザーがサブミットしたジョブの一覧が表示されます。
- **[マイ ジョブ]** カテゴリには、現在サインオンしている HPCA Console ユーザーがサブミットしたジョブの一覧が表示されます。

それぞれのカテゴリには、実行中か実行を待機中の **[現在のジョブ]** と、実行が完了している **[過去のジョブ]** の一覧が含まれています。

HPCA Console では、3 つの異なるタイプのジョブを管理できます。

表 18　ジョブ タイプ

ジョブ タイプ	説明
通知	特定のアクションを実行するため、HPCA Console がターゲット デバイスに Configuration Server への接続を指示します。これは、一元管理 (サーバープッシュ) 方式のジョブ管理です。 HPCA Console では、内部プロセス エンジンを使用してこれらのタイプのジョブを管理します。
分散タスク (DTM)	各ターゲット デバイスは、HPCA Core との間で定期的に同期を行い、指示を受信して指定されたスケジュールに従って特定のアクションを実行します。このスケジュールは、HPCA Console で設定および管理できます。 これは、HPCA Core から独立してジョブを実行できるため、分散 (クライアントプル) 方式のジョブ管理と言えます。
配布 (RMP)	これらのジョブには、Agent または OS の配布が関係しています。HPCA Console では RMP ジョブに関する情報を表示できますが、情報を修正することはできません。通知ジョブのような配布ジョブは、一元管理 (サーバープッシュ) されます。

現在と過去のジョブ

[現在のジョブ] ページには、実行中か実行待機中のジョブの一覧が表示されます。[過去のジョブ] ページには、実行が完了したジョブの一覧が表示されます。ジョブごとに、次の情報が表示されます。

ジョブ ID – このジョブの一意の ID。この ID は、ジョブの作成時に HPCA によって割り当てられます。特定のジョブのジョブ詳細を表示するには、そのジョブ ID をクリックします。

タイプ – [通知]、[DTM]、または [RMP]。

表示名 – ジョブの作成時に指定した名前。

状態 – [有効]、[無効]、[実行中]、[完了]、または [スケジュールされている]。有効なジョブは、ターゲット デバイスで実行するようにスケジュールできます。

ステータス – ジョブの現行ステータス。[成功]、[失敗]、[不明] (ジョブが [実行中] か [スケジュールされている] のいずれかの状態になっている間)。

説明 – ジョブの作成時に指定したテキスト説明。

スケジュール – ジョブに関連付けられたスケジュール。

ターゲット – ジョブを実行するターゲット デバイスまたはグループ。

アクション – ターゲット デバイスでジョブが実行されるときに実施されるアクション。

作成時刻 – このジョブが作成された日時。

作成者 – ジョブを作成した HPCA Console ユーザー。

前回実行時 – ジョブが最後に実行された日時。ジョブが一度も実行されたことがない場合は、日付として 12/31/1969 と表示されます。

ジョブ テーブルの一番上にあるボタンを使用して、次のアクションを実行します。

表 19　ジョブ テーブルのコントロール

アイコン	説明
	データのリフレッシュ
	フィルタ入力の表示 / 非表示

表 19　ジョブ テーブルのコントロール

アイコン	説明
	選択したジョブの削除
	選択したジョブの有効化 – 現在の DTM ジョブにのみ適用
	選択したジョブの削除 – 現在の DTM ジョブにのみ適用

ジョブおよびジョブの実行

ジョブは、特定のアクションとターゲット デバイスまたはグループのパラメータを定義するフレームワークです。ジョブは、次の 3 つの主要コンポーネントで構成されています。

- ターゲット – ジョブを実行するデバイスまたはデバイスのグループ
- アクション – 実行されるコマンド
- スケジュール – ターゲットでアクションを実行する日時

ジョブが実行されている、実行を待機中、実行を完了している場合、**ジョブの実行**は、特定のデバイスでのそのジョブのインスタンスを表します。

ターゲット

ターゲットは、ジョブを実行する単一のデバイスまたはデバイスのグループです。これは、通常、時間の経過に伴ってメンバーが変化する Active Directory グループです。ターゲットは、ジョブの作成時に指定します。

[ターゲットの詳細] ウィンドウには、1 つ以上のジョブに関連付けられているターゲット デバイスに関する情報が表示されます。このウィンドウには、次の 3 つのタブがあります。

- **[ターゲット デバイス]** タブには、このジョブに関連付けられているすべてのデバイスの一覧が表示されます。特定のデバイスに関する情報を表示するには、そのデバイスのショートカット メニューで **[プロパティの表示/編集]** を選択します。
- **[ターゲットのジョブの実行]** タブには、このターゲット (またはターゲット グループ) のこのジョブに対して実行するようにスケジュールされているジョブの実行、実行中のジョブの実行、または実行済みのジョブの実行が表示されます。
- **[選択されたターゲットのすべてのジョブ]** タブには、このターゲット (またはターゲット グループ) を使用するすべてのジョブが表示されます。

[ターゲットの詳細] ウィンドウにアクセスするには

1 [現在のジョブ] または [過去のジョブ] テーブルで、**[ジョブ ID]** をクリックします。
2 [ジョブの詳細] ウィンドウで、**[プロパティ]** タブをクリックします。
3 [ターゲット] セクションで、ターゲット グループまたはデバイスの名前をクリックします。

[ターゲットの詳細] ウィンドウには、[現在のジョブ] または [過去のジョブ] テーブルのいずれかで **[ターゲット]** カラムの値を選択することによってもアクセスできます。

スケジュール

DTM タスクは、特定の時刻に一度実行されるように、または指定するパラメータに従って定期的に実行されるようにスケジュールできます。

[スケジュールの詳細] ウィンドウでは、既存の DTM ジョブに関連付けられているスケジュールに関する情報を表示できます。このジョブが現在のジョブの場合は、スケジュールを修正することも可能です。

[スケジュールの詳細] ウィンドウにアクセスするには

1 [現在のジョブ] または [過去のジョブ] テーブルで、DTM ジョブの **[ジョブ ID]** をクリックします。
2 [ジョブの詳細] ウィンドウで、**[プロパティ]** タブをクリックします。
3 [スケジュール] セクションで、**[修正]** をクリックします。

DTM ジョブのスケジュールを指定するには

1 **[タスクの開始]** リストで、**[スケジュール]** または **[起動]** を選択します。
[起動] を選択する場合は、以降の手順をスキップできます。
2 このジョブを実行する頻度を [一度]、[時間単位]、[日単位]、[週単位]、[月単位] の中から選択します。
3 [一度] 以外の頻度を選択した場合は、**[間隔]** 情報を指定して、このジョブの再実行間隔を定義してください。
4 ジョブの **[開始日]** を指定します。
5 このジョブの新しいジョブの実行を開始することを一定の日付で中止する場合は、**[終了日]** フィールドの左にあるチェックボックスをオンにし、終了日を指定します。
6 ジョブの **[開始時刻]** を指定します。

7 このジョブの新しいジョブの実行の開始を特定の時刻で中止する場合は、**[終了時刻]** フィールドの左にあるチェックボックスをオンにし、終了時刻を指定します。

8 [開始時刻] と [終了時刻] の間のランダム化された時刻にジョブを開始する場合は、**[ランダム化された開始時刻]** ボックスをオンにします。

詳細については、166 ページの「新しい DTM または通知ジョブを作成する」を参照してください。

DTM ジョブのジョブの詳細

[現在のジョブ] または [過去のジョブ] のいずれかのテーブルで DTM ジョブのジョブ ID をクリックすると、[ジョブの詳細] ウィンドウが開き、次の情報が表示されます。

- **[要約]** タブには、ジョブの ID、名前、説明、および作成時刻とともに、ジョブの現在の状態 ([有効]、[無効]、または [完了]) が表示されます。このタブには、ターゲット デバイスのジョブのステータス ([成功]、[失敗]、[警告]、または [不明]) を示す円グラフも表示されます。

  このジョブの「ジョブの実行」が実行されると、ステータスは [不明] になります。

  DTM ジョブは、そのスケジュールで [終了日] が使用されており、この [終了日] が経過すると、[完了] 状態に移行します。

- **[プロパティ]** タブには、ジョブを作成するために使用された説明、アクション、ターゲット、およびスケジュールなど、ジョブに関する情報が表示されます。

  このジョブに関連付けられているターゲット デバイスに関する情報を表示するには、ターゲット名をクリックします。160 ページの「ターゲット」を参照してください。

  このジョブのスケジュールを表示または変更するには、**[スケジュールの変更]** リンクをクリックします。変更できるのは、現在のジョブのスケジュールのみです。161 ページの「スケジュール」を参照してください。

- **[ジョブの実行]** タブには、このジョブにスケジュールされているジョブの実行が表示されます。これには、すでに完了しているジョブの実行が含まれます。

  特定のジョブの実行についての詳細を表示するには、テーブルでそのジョブの実行の **ID** をクリックします。[ジョブの実行の詳細] ウィンドウが開きます。164 ページの「ジョブの実行の詳細」を参照してください。

[ジョブの詳細] ウィンドウには、通知ジョブについて若干異なる情報が表示されます。163 ページの「通知ジョブのジョブの詳細」を参照してください。

通知ジョブのジョブの詳細

[現在のジョブ] または [過去のジョブ] のいずれかのテーブルで通知ジョブのジョブ ID をクリックすると、[ジョブの詳細] ウィンドウが開き、次の情報が表示されます。

- **[要約]** タブには、ジョブの ID、名前、説明、および作成時刻とともに、ジョブの現在の状態が表示されます。

  表 20　通知ジョブの状態の説明

状態	説明	例
スケジュールされている	ジョブはまだ開始されていません。	通知ジョブは将来のある時点に実行するようスケジュールされていますが、まだ開始されていません。
実行中	ジョブはまだ完了状態に到達していません。実行中のジョブは、[現在のジョブ] リストに表示されます。	実行中の通知ジョブは、各デバイスへの通知を処理中です。
完了	ジョブは完了状態に到達しており、すべての手順が処理されました。完了したジョブは、[過去のジョブ] リストに表示されます。	通知ジョブは、ジョブに含まれるすべてのデバイスが通知されると完了します。

  このタブには、ターゲット デバイスのジョブのステータス ([実行中]、[成功]、[失敗]、[警告]、または [不明]) を示す円グラフも表示されます。

- **[プロパティ]** タブには、ジョブを作成するために使用されたアクション、ターゲット、およびスケジュールなど、ジョブに関する情報が表示されます。

  このジョブに関連付けられているターゲット デバイスに関する情報を表示するには、ターゲット名をクリックします。160 ページの「ターゲット」を参照してください。

- **[ジョブの実行]** タブには、各ターゲットでの*最後*のジョブの実行のステータスが表示されます。これには、すでに完了しているジョブの実行が含まれます。

  特定のジョブの実行についての詳細を表示するには、テーブルでそのジョブの実行の **ID** をクリックします。[ジョブの実行の詳細] ウィンドウが開きます。164 ページの「ジョブの実行の詳細」を参照してください。

[ジョブの詳細] ウィンドウには、DTM ジョブについて若干異なる情報が表示されます。162 ページの「DTM ジョブのジョブの詳細」を参照してください。

RMP ジョブに関するジョブの詳細

[現在のジョブ] または [過去のジョブ] のいずれかのテーブルで RMP ジョブのジョブ ID をクリックすると、[ジョブの詳細] ウィンドウが開きます。表示される情報は、通知ジョブの場合に表示される情報と同じです (163 ページの「通知ジョブのジョブの詳細」を参照)。

ジョブの実行の詳細

DTM ジョブの場合、[ジョブの実行の詳細] タブには、現在実行中か、またはすべてのターゲット デバイスでの実行が完了したジョブごとに、最後のジョブの実行の一覧が表示されます。通知ジョブと RMP ジョブの場合、このタブには、現在実行中か、実行を待機中か、またはすべてのターゲット デバイスでの実行が完了したジョブごとに、最後のジョブの実行についての一覧が表示されます。

次の情報が表示されます。

ID – このジョブの実行の一意の ID。この ID は、この実行 (インスタンス) にのみ関連し、ジョブ テーブルで指定されているジョブ ID と同じではありません。特定のジョブの実行の [ジョブの詳細] を表示するには、その ID をクリックします。

タイプ – [通知]、[RMP]、または [DTM] (分散タスク)

状態 – [実行中]、[完了]、または [開始を待機中] (通知ジョブと RMP ジョブの場合)。165 ページの「ジョブの実行状態」を参照してください。

説明 – ジョブの実行の作成時に指定したテキスト説明。

要約 – ジョブの実行に関連したステータス メッセージ。

開始時刻 – 現在のジョブの場合は、ターゲット デバイスでこのジョブの実行を開始するようにスケジュールされた時刻。過去のジョブの場合は、ジョブの実行が開始された時刻です。

終了時刻 – 現在のジョブの場合は空白。過去のジョブの場合は、このジョブの実行が中止された時刻です。

ジョブ – この実行の基となったジョブのジョブ ID。

テーブルの一番上にあるボタンを使用して、既存のジョブの実行を管理できます。

表 21　ジョブの実行アクション

アイコン	説明
	データのリフレッシュ
	フィルタ入力の表示 / 非表示

一部のボタンは、特定のジョブ状態の間にのみ表示されます。たとえば、完了したジョブの実行の場合には、[再開]、[一時停止]、または [キャンセル] ボタンがありません。

[ジョブの詳細] ウィンドウを開くには、任意のジョブのジョブ ID をクリックします。詳細については、163 ページの「通知ジョブのジョブの詳細」または 162 ページの「DTM ジョブのジョブの詳細」を参照してください。各ジョブのステータスの詳細については、165 ページの「ジョブの実行状態」を参照してください。

ジョブの実行状態

HPCA Console ジョブの実行には、ジョブのタイプに応じて任意の数の手順を含めることができます。たとえば、通知ジョブには、通知対象のデバイスごとに手順が 1 つあります。これらの手順の実行ステータスにより、現在のジョブの実行状態が決まります。

表 22　ジョブの実行状態の説明

状態	説明
実行中	ジョブの実行は、まだ完了状態に到達していません。実行中のジョブの実行は、[現在のジョブの実行] リストに含まれています。
完了	ジョブの実行は完了状態に到達しており、すべての手順が処理されました。完了したジョブの実行は、[過去のジョブの実行] リストに含まれています。
開始を待機中	このジョブの実行は、[スケジュールされている] の状態のジョブに基づいています。

新しい DTM または通知ジョブを作成する

HPCA ジョブ作成ウィザードを使用して、新しい DTM ジョブまたは通知ジョブを作成できます。新しい Agent 配布ジョブを作成する方法については、156 ページの「HPCA Agent の配布」を参照してください。新しい OS 配布ジョブを作成する方法については、186 ページの「オペレーティング システムの管理」を参照してください。

新しい DTM ジョブまたは通知ジョブを作成するには

1 [管理] タブで、[ディレクトリ] 領域に移動し、使用するゾーンを展開します。

2 作業する **[グループ]** または **[デバイス]** の一覧を表示します。

3 グループまたはデバイスのドロップダウン メニューから、**[ジョブの作成]** を選択します。HPCA ジョブ作成ウィザードが開きます。

または、グリッドからグループまたはデバイスを 1 つ以上選択し、ツールバーで **[HPCA ジョブ作成ウィザードを起動]**  アイコンをクリックして、そのウィザードを開くこともできます。

4 **[ジョブ タイプ]** リストで、**[DTM]** または **[通知]** を選択します。

DTM ジョブでは、ターゲット デバイスの Agent が HPCA Core Server に接続してジョブの一覧を取得し、その後ジョブ タイマーが期限切れになったときにそれらのジョブを実行します。DTM ジョブは、これらのデバイスで通常のスケジュールに従ってこのジョブを実行する場合に最適です。

通知ジョブでは、HPCA Core Server が HPCA Agent にスキャンの実行を依頼します。通知ジョブは、特定のターゲット デバイスで特定の時刻に (または直ちに) ジョブを実行する場合に最適です。

5 ジョブの **[名前]** と **[説明]** を指定します。

6 **[ジョブ アクション テンプレート]** リストで、ここで使用するジョブ アクション テンプレートを選択します。詳細については、276 ページの「ジョブ アクション テンプレート」を参照してください。

7 ジョブ アクション テンプレートで指定されていないジョブ アクションのパラメータを指定する場合は、**[その他のパラメータ]** ボックスにそれらのパラメータを入力します。

8 **[次へ]** をクリックします。

9 このジョブのスケジュールを指定します。詳細については、161 ページの「スケジュール」を参照してください。

10 **[次へ]** をクリックします。

11 指定した設定を確認し、準備ができたら **[サブミット]** をクリックします。

ジョブを表示するには、[管理] タブの [ジョブ] 領域をクリックします。

DTM ジョブのスケジュールを修正する場合は、ターゲット デバイスのそれぞれでスケジュールをリフレッシュする必要があります。170 ページの「古いジョブの実行レコードの削除」を参照してください。

ジョブの削除

現在または過去のジョブを削除するには、[現在のジョブ] または [過去のジョブ] テーブルを選択し、**[選択したジョブの削除]**  アイコンをクリックします。次の点に注意してください。

- 現在実行中の通知ジョブは削除できません。
- DTM ジョブの場合は、アイコンをクリックすると [現在のジョブ] リストにそのジョブが表示されなくなりますが、そのジョブからのジョブの実行は各ターゲット デバイスのディレクトリ オブジェクト ビュー (**[プロパティの表示 / 編集]** を選択して表示) に表示され続けます。

  DTM ジョブを削除すると、それ以降に HPCA Core Server との間で行われる Agent の同期で、そのジョブをターゲット デバイスにダウンロードすることができなくなります。削除されたジョブがすでに存在するターゲット デバイスの場合、HPCA Core Server との同期を行うまでは、そのジョブを実行できます。

ターゲットの DTM スケジュールのリフレッシュ

HPCA Core Server で DTM ジョブのスケジュールを修正する場合は、各ターゲット デバイスでもスケジュールをリフレッシュする必要があります。これには、「DTM ジョブ スケジュールのリフレッシュ」サンプル ジョブ アクション テンプレートを使用してジョブを作成します。

デフォルトでは、Configuration Server Database (CSDB) に DTM_DAILY_TIMER があり、管理対象デバイスに対してエンタイトルメントの設定を行って、Core Server と 1 日に 1 回の頻度でジョブ情報の同期を実行するようにその Agent に指示することができます。

DTM スケジュールのリフレッシュ ジョブでは、別の方法を使用して Core Server との同期をスケジュールできます。たとえば、DTM スケジュールのリフレッシュ ジョブを作成して、Core Server と 12 時間ごとにジョブ情報の同期を実行するように Agent に依頼することができます。ターゲット デバイスの Agent に対して

は、この DTM スケジュールのリフレッシュ ジョブは、ジョブ タイマーが期限切れになると、ソフトウェア接続などの他の Agent ジョブとまったく同じように実行されます。

クライアント デバイスで DTM スケジュールのリフレッシュ ジョブを正常に実行できるようにするには、そのクライアントの HPCA Agent で HPCA Core Server への事前接続操作を実行しておく必要があります。

DTM スケジュールのリフレッシュ ジョブを作成するには

1. [管理] タブの **[ディレクトリ]** 領域で、関係する DTM ジョブのターゲット デバイスを含むオブジェクトに移動します。
2. リフレッシュするターゲット デバイスを選択します。
3.  ツールバー アイコンをクリックして **HPCA ジョブ作成ウィザード**を起動します。
4. 直ちにリフレッシュするには、**[ジョブ タイプ]** ドロップダウン ボックスで **[通知]** を選択します。スケジュールに従ってリフレッシュするには、**[DTM]** を選択します。

   [DTM] を選択すると、ターゲット デバイスでは、Core Server と同期するときにこのジョブが必要になります。このジョブでは、指定するスケジュール設定に従って Core Server に再接続し、ジョブ情報を取得するようにデバイスに指示します。

   Agent で新しい同期スケジュールをできるだけ早く使用するには、DTM スケジュールのリフレッシュ ジョブの **[通知]** もスケジュールして、指定した時刻に Core Server との同期を実行するようにターゲット デバイスの Agent に指示し、*次に* DTM スケジュールのリフレッシュ ジョブの **[DTM]** をダウンロードすることをお勧めします。
5. リフレッシュ ジョブの名前および説明を入力します。
6. **[ジョブ アクション テンプレート]** リストで、**[DTM ジョブ スケジュールのリフレッシュ]** を選択します。
7. **[次へ]** をクリックします。
8. スケジュール設定 (161 ページの「スケジュール」を参照) を入力し、**[サブミット]** をクリックします。

   ジョブが追加され、定義した設定に基づいてターゲット デバイスが設定されている DTM ジョブ スケジュールをリフレッシュします。

ジョブのステータスを表示するには、[管理] タブの **[ジョブ]** 領域をクリックします。

通知ジョブのデバイス解決

通知ジョブに含まれるデバイスは、次のファイルで定義されている順序に従って解決されます。

<*tomcatDir*>\webapps\em\web-inf\console.properties

<*tomcatDir*> のデフォルト値は次のとおりです。

C:\Program Files\Hewlett-Packard\HPCA\tomcat

デフォルトの順序：

group.target.host.attributes=ipaddress,dnshostname,displayname,cn

必要に応じて、このリストを変更できます。このファイルに変更を加える場合は、HPCA Tomcat サービスを再起動する必要があります。

解決できなかったデバイスについては、[ジョブの詳細] ウィンドウの [詳細] タブにメッセージが表示されます。[ジョブの詳細] ウィンドウを開くには、ジョブ ID をクリックします。

DTM ジョブのデバイス解決

DTM ジョブに含まれるデバイスは、次の順序で解決されます。

1. ipaddress
2. dnshostname
3. displayname
4. cn

DTM ジョブのターゲット デバイスを解決するため、サービスが定期的に実行されます。このサービスは、次のファイルで設定可能です。

<*tomcatDir*>/webapps/ope/config/dtm.properties

表 23　DTM ジョブのデバイス解決サービスのパラメータ

パラメータ	デフォルト値	コメント
enableTargetRefresh	true	このサービスを有効または無効にする
rmpProtocol	http\:\\	SSL の場合は https\:\\
rmpServer	localhost	HPCA Portal Server

表 23　DTM ジョブのデバイス解決サービスのパラメータ

パラメータ	デフォルト値	コメント
rmpPort	3466	接続先の Portal Server ポート
rmpUser	SYSTEM	
rmpPassword		セキュリティ上の理由により非表示
userDS	“”	接続先のユーザー ディレクトリ
targetRefreshInterval	360	デフォルトは 6 分 (360 秒)
targetRefreshInitDelay	60	起動してから DTM がターゲット解決サービスを開始するまでの待機時間 (秒)

古いジョブの実行レコードの削除

過去の DTM および通知のジョブの実行を HPCA データベースに保存する期間を指定できます。また、保存するレコードの最大数を指定することもできます。この設定は、次のファイルで行います。

<*tomcatDir*>\webapps\ope\config\dtm.properties

<*tomcatDir*> のデフォルト値は次のとおりです。

C:\Program Files\Hewlett-Packard\HPCA\tomcat

次のパラメータを使用してこれらの設定値を指定します。

```
dtmJobRunKeepDays=30
opeJobRunKeepDays=30
dtmJobRunKeepRecords=-1
opeJobRunKeepRecords=-1
```

これらのパラメータによって指定される期間のデフォルト設定は、ここに示すとおりです。値 -1 は、保存可能なレコード数に制限がないことを示します。

Satellite 同期ジョブの作成

管理対象デバイスへのデータ キャッシュと設定値の配布を行うには、Satellite Server を使用します。Satellite は、それらのデバイスに最新のデータを配布するために、Core Server と同期を取る必要があります。Satellite Console から同期を実行するか、HPCA Console でジョブを作成してこの同期タスクをスケジュールすることができます。

Satellite Server のデータを同期できるようにするには、最初に Satellite を設定しておく必要があります。詳細については、『HPCA Core および Satellite 入門およびコンセプト ガイド』を参照してください。

クライアント デバイスで Satellite 同期ジョブを正常に実行できるようにするには、そのクライアントの HPCA Agent で HPCA Core Server への事前接続操作を実行しておく必要があります。

Satellite 同期ジョブを作成するには

1 [管理] タブの **[ディレクトリ]** 領域で、Satellite デバイスを含むオブジェクトに移動します。

2 Satellite デバイスを選択し、  ツールバー アイコンをクリックして **HPCA ジョブ作成ウィザード**を起動します。

Satellite Server ではないデバイスを選択すると、そのジョブは失敗します。

3 Satellite を即時に同期するには、**[ジョブ タイプ]** ドロップダウン ボックスから **[通知]** を選択します。スケジュールに従って同期するには、**[DTM]** を選択します。

[DTM] を選択すると、Satellite デバイス上のエージェントが DTM スケジュールのリフレッシュを実行した*後*のみ、この Satellite 同期ジョブが Satellite にダウンロードされます。

4 同期ジョブの名前および説明を入力します。

5 スケジュールする同期タイプの **[ジョブ アクション テンプレート]** を選択します。

— **Satellite の同期 (すべて)**

設定の設定とデータの両方を同期するには、このテンプレートを選択します。

— **Satellite の同期 (設定)**

設定の設定のみを同期するには、このテンプレートを選択します。

— **Satellite の同期 (データ)**

このテンプレートでは、データのみが同期されます。

6 **[次へ]** をクリックします。

7 スケジュール設定 (161 ページの「スケジュール」を参照) を入力し、**[サブミット]** をクリックします。

ジョブが追加され、Satellite サーバーでは定義した設定に基づいてデータまたは設定の設定が同期されます。

ジョブのステータスを表示するには、[管理] タブの **[ジョブ]** 領域をクリックします。

仮想マシンの管理

HPCA Console を使用すると、仮想ホスティング サーバー上で機能している仮想マシンを管理できます。たとえば、企業環境内の既存の VMware ESX Server 上に仮想マシンを作成し、管理できます。

仮想マシンを管理するには

1. **[管理]** タブで、管理するデバイスが含まれるゾーンを展開します。
2. 左ナビゲーション ツリーで、**[デバイス]** をクリックします。
3. デバイスのリストで、使用している ESX Server を探します。
4. このデバイスのドロップダウン メニューで、**[プロパティの表示 / 編集]** をクリックします。147 ページの図 40 に示すように、別のブラウザ ウィンドウが開きます。
5. 使用している ESX Server の [ディレクトリ オブジェクト] ウィンドウで、左ナビゲーション メニューの **[仮想マシン]** リンクをクリックします。

> [仮想マシン] リンクは、このデバイスが **[VMware ESX Server]** デバイスの分類を使用してインポートされた場合のみ表示されます。詳細については、設定に関する章の「デバイスのインポート」を参照してください。

この HPCA Console セッション中に初めて ESX Server のリンクをクリックした場合、ログイン認証情報を入力する必要があります。

ESX Server の **[ユーザー ID]** と **[パスワード]** を入力して、**[サインイン]** をクリックします。

176 ページの図 43 に示すように、この ESX Server でホストされる仮想マシンの一覧が表示されます。

特定の仮想マシンのプロパティを表示するには、仮想マシン名をクリックします。

図 42　VMware ESX Server のデバイス プロパティ

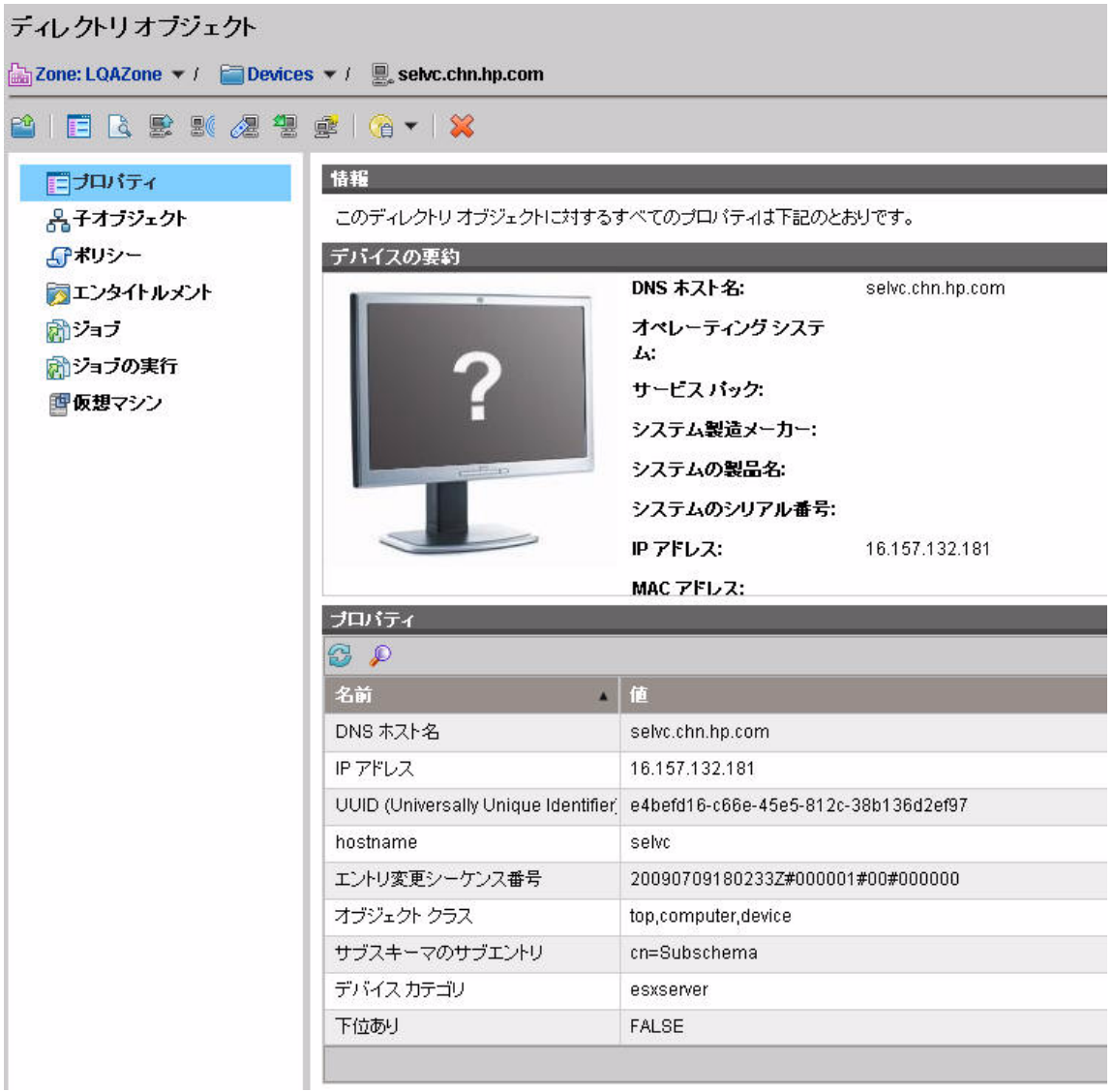
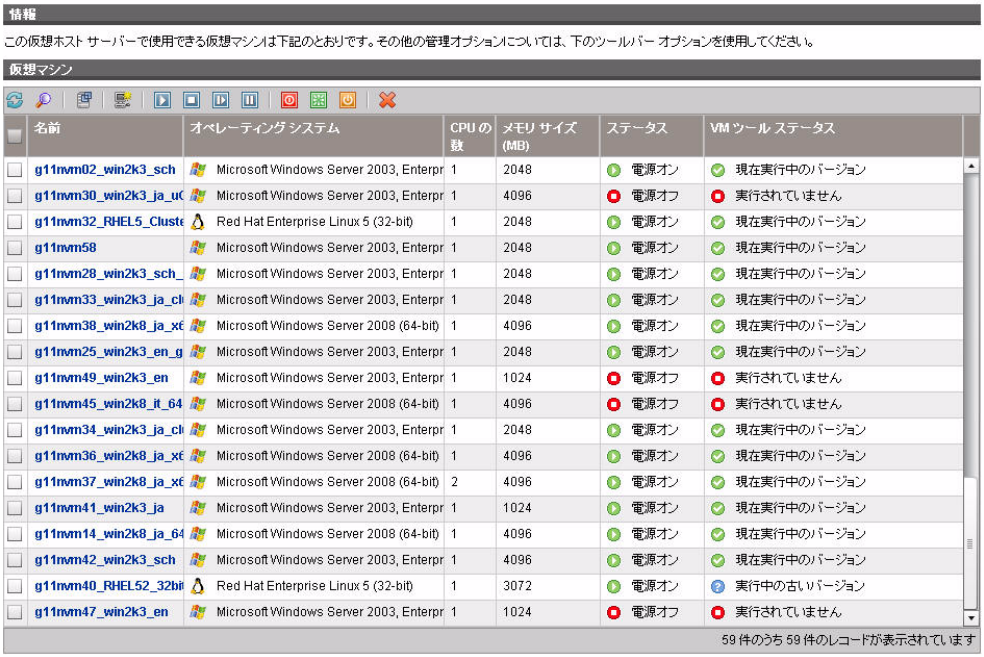


図 43　ESX Server でホストされる仮想マシン一覧



仮想マシン一覧の各カラムには、次の情報が含まれます。

表 24　仮想マシン一覧のカラム

カラム名	説明
名前	仮想マシンの名前
オペレーティング システム	仮想マシンのオペレーティング システム
CPU の数	仮想マシンに割り当てられた CPU の数
メモリ サイズ	仮想マシンに割り当てられたメモリ容量
ステータス	仮想マシンの現在のステータス
VM ツール ステータス	仮想マシン上の VM ツールの現在のステータス

仮想マシンの名前をクリックすると、そのマシンの [仮想マシンのプロパティ] ウィンドウが開きます。

次のコントロールを使用して、ESX Server 上に仮想マシンを作成し、管理できます。

表 25　[仮想マシン] ツールバー

アイコン	説明
	データのリフレッシュ
	フィルタ入力の表示 / 非表示
	VM ホスト システムのプロパティの表示
	新しい仮想マシンの作成
	選択した仮想マシンを中断します
	選択した仮想マシンをリセットします
	選択した仮想マシンを停止します
	選択した仮想マシンを起動します
	選択した仮想マシンの OS をスタンバイします [1]
	選択した仮想マシンの OS を再起動します [1]
	選択した仮想マシンの OS をシャットダウンします [1]
	選択した仮想マシンを削除します

[1] 仮想マシンで実行する VMWare ツールが必要です。

管理する仮想マシンごとにチェック ボックスをオンにしてから適切な仮想マシン コントロールをクリックし、必要なアクションを完了させます。

仮想マシンの新規作成

仮想マシン テーブルの **[新しい仮想マシンの作成]**  コントロールを使用すると、仮想マシン作成ウィザードを使用して ESX Server 上に新しい仮想マシンを作成できます。このウィザードは、VMware 仮想マシン作成ウィザードが要求する情報と類似した情報を要求します。このウィザードを使用する前に、VMware の用語について理解を深める必要があります。

新しい仮想マシンを作成するには :

1 173 ページの「仮想マシンの管理」の手順 1 ～ 5 に従って、使用している ESX Server 上の仮想マシンの一覧を開きます。

2 **[新しい仮想マシンの作成]**  をクリックします。仮想マシン作成ウィザードが表示されます。

3 作成したい仮想マシンについての情報を入力します。

- **データ センター** : ドロップダウン リストを使用して、新しい仮想マシンを作成するデータ センターを選択します。
- **ホスト システム** : ドロップダウン リストを使用して、仮想マシンのホスト システムを選択します。
- **名前** : 仮想マシンの名前を入力します。仮想マシンの名前は 80 文字以内とし、英数字、スペース、ハイフン、アンダースコアを使用できます。仮想マシンの名前は、各データ センター内および各フォルダ内で一意でなければなりません。
- **説明** : 仮想マシンの説明を入力します。

4 **[次へ]** をクリックします。

5 ドロップダウン リストを使用して、**[データ ストア]** を選択します。仮想マシンとその仮想ディスク ファイルを十分格納できる容量のあるデータ ストアを必ず選択してください。

6 **[ディスク サイズ]** を入力します。ディスク サイズをメガバイト単位で入力するには、数字を入力するか、上向き矢印または下向き矢印を使用します。サイズをギガバイト単位で入力するには、スライダ ツールを使用します。

7 **[次へ]** をクリックします。

8 **[ゲスト オペレーティング システム]** を選択してから、新しい仮想マシンに割り当てる **[バージョン]** および **[オペレーティング システムのポリシー]** を選択します。選択可能なポリシーは、HPCA OS Manager によって定義されます。

9 **[次へ]** をクリックします。

10 数字を入力するかドロップダウン リストを使用して、仮想マシンの **[仮想プロセッサの数]** を入力します。仮想マシンに割り当てることができるプロセッサの数は、ホスト デバイス上の論理プロセッサの実際の数までです。

11 仮想マシンの **[メモリ サイズ]** を入力します。メモリ サイズをメガバイト単位で入力するには、数字を入力するか、上向き矢印または下向き矢印を使用します。サイズをギガバイト単位で入力するには、スライダ ツールを使用します。メモリ サイズの下限は 4MB です。

12 **[次へ]** をクリックします。

13 ドロップダウン リストを使用して、この仮想マシンに対して設定する **[NIC の数]**（ネットワーク インターフェイス カードの数）と **[NIC 番号 1 仮想ネットワーク]** を選択します。

14 仮想マシンの起動時に各 NIC をネットワークに接続する場合は、**[電源オン時に接続]** をオンにします。

15 **[次へ]** をクリックします。

16 要約情報を確認し、**[適用]** をクリックします。

17 これで、仮想マシンが作成されました。仮想マシンのリストで、新しい仮想マシンを確認します。仮想マシンの名前をクリックすると、プロパティウィンドウが開きます。

デバイスのリモート制御

HPCA Console では、次の 3 種類の方法のいずれかを使用して、内部および外部リポジトリのデバイスへリモート アクセスできます。

- Windows リモート デスクトップ接続
- Virtual Network Computing (VNC)
- Windows リモート アシスタンス

HPCA Console では、各ターゲット デバイスのリモート制御機能を判別して、最適な通信方法が決定されます。特定のターゲット デバイスへのリモート制御接続を開始すると、そのデバイス上で使用可能な接続のタイプを選択できます。

VNC および Windows リモート デスクトップ接続については、リモート デバイスがリモート接続をリスンするポートを指定する必要があります。Windows リモート アシスタンスの場合はポートを指定する必要はありません。これは、Windows リモート アシスタンスは常にポート 135 の Distributed Component Object Model (DCOM) インターフェイスを使用するためです。

HPCA 管理者は、リモート制御機能をすべて同時に有効化または無効化できます。または、1 つ以上の特定のリモート制御ツールを有効化できます。詳細については、286 ページの「リモート制御の設定」を参照してください。

各タイプのサポート対象接続を確立するには、特定の条件を満たす必要があります。詳細については、181 ページの「リモート接続の要件」を参照してください。

デバイスにリモート アクセスするには :

1 **[管理]** タブをクリックします。

2 リモート アクセスするデバイスが含まれているゾーンを展開します。

3 左ナビゲーション ペインで、**[デバイス]** をクリックします。

4 アクセスするデバイスの右クリック ショートカット メニューで、**[リモート制御]** をクリックします。

[プロパティの表示 / 編集] を選択して、[ディレクトリ オブジェクト] ウィンドウの  (リモート制御) アイコンをクリックすることもできます。

HPCA Console で Windows リモート デスクトップ接続、VNC、または Windows リモート アシスタンスを使用して接続できない場合、[リモート制御] をクリックするとエラー メッセージが表示されます。

5 Windows リモート デスクトップ接続では、次の項目を指定します。

— **メソッド** : [Windows リモート デスクトップ] を選択します。

— **解像度** : 画面上の Windows リモート デスクトップ接続ウィンドウのサイズを選択します。

VNC 接続では、次の項目を指定します。

— **メソッド** : [VNC (Virtual Network Computing)] を選択します。

Windows リモート アシスタンス接続では、次の項目を指定します。

— **メソッド** : [Windows リモート アシスタンス] を選択します。

6 **[接続]** をクリックします。新しいブラウザ ウィンドウが開いて、リモート接続が確立されます。

VNC 接続では、最初に VNC パスワードの入力が必要な場合があります。

Windows リモート アシスタンス接続では、現在ターゲット デバイスにログオンしているユーザーは接続を許可する必要があります。

関連トピック :

リモート接続の要件 181 ページ

リモート制御の設定 286 ページ

リモート制御の監査 185 ページ

リモート接続の要件

HPCA Console を使用してリモート接続するターゲット デバイスでは、次の要件が満たされている必要があります。

- リモート デバイスの電源がオンになっている。
- ファイアウォールが有効な場合は、リモート デバイス上のリモート アクセス ポートが開いている。

- リモート デバイスは、HPCA Console サーバーとリクエストを開始するクライアント システムの両方に接続できる。

また、各タイプのリモート アクセスには、特定の要件があります。

Windows リモート デスクトップ接続の要件

この接続タイプを使用してリモート アクセスするすべてのターゲット デバイス上で、Windows リモート デスクトップ接続を有効にする必要があります。デフォルトでは、この機能は無効です。

Windows リモート デスクトップ接続を使用するには、Internet Explorer (バージョン 6.0 以降) を使用して HPCA Console にアクセスする必要があります。これは、このタイプの接続がリクエストされたときに ActiveX コンポーネントを使用するラッパーをコンソールが起動するためです。

Windows リモート デスクトップ接続の詳細については、次の Microsoft サポート ドキュメントを参照してください。

http://www.microsoft.com/windowsxp/using/mobility/getstarted/remoteintro.mspx

VNC の要件

VNC 接続では、ターゲット デバイスで VNC サーバー プロセスを実行する必要があります。このプロセスでは、特定のポートをリスンする必要があります。また、URL (HTTP) ベースのリモート制御セッションのサポートが有効である必要があります。

VNC 接続を確立するには、HPCA Console でリモート URL をブラウザ内の Java アプレットとして起動します。このため、HPCA Console にアクセスしているシステム (ブラウザを実行しているシステム) に Java Runtime Environment (JRE) バージョン 1.5 (またはそれ以降) がインストールされている必要があります。

リモート URL のポート番号は、リモート システム上の VNC サーバーがリスンしているポートと一致している必要があります。デフォルトでは、このポートは 5800 です。次に例を示します。

`http://<RemoteSystem>:5800`

この場合、<RemoteSystem> への接続にポート 5800 が使われ、VNC リモート制御アプレットがブラウザで開いて、<RemoteSystem> のリモート制御が可能になります。

HP では、VNC サーバー プログラムを提供していません。ただし、HPCA Console では、Web ベースの統合機能を持つすべての VNC サーバーがサポートされます。この機能は、UltraVNC、RealVNC、および TightVNC で利用できます。通常、VNC サーバーはポート 5800 上で実行され、すべての Web ブラウザからアクセスできます。

Application Management Profile (AMP) を使用して、UltraVNC、RealVNC、および TightVNC サーバー ソフトウェアをクライアント システムに配布できます。上記アプリケーション用の AMP は、HP Live Network の Web サイトの AMP Community から入手できます。AMP の詳細については、『Application Management Profiles ユーザー ガイド』を参照してください。

Windows リモート アシスタンスの要件

Windows Vista または Windows Server 2008 システムから HPCA Console にアクセスしている場合、作成できる接続は Windows リモート アシスタンスのみです。次のオペレーティング システムを実行しているターゲット デバイスに接続できます。

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

ターゲット デバイスへの Windows リモート アシスタンス接続が開始したら、ターゲット デバイスにログオンしているユーザーは接続を許可する必要があります。自動実行のデバイスへの Windows リモート アシスタンス接続は作成できません。

この接続タイプを使用してリモート アクセスするすべてのターゲット デバイス上で、Windows リモート アシスタンスを有効にする必要があります。詳細については、ネットワーク管理者に問い合わせるか、次の Microsoft サポート ドキュメントを参照してください。

http://support.microsoft.com/kb/305608/en-us

Windows リモート アシスタンス接続を有効にするには、さらに次の 3 つの要件を満たす必要があります。

- HPCA Console にアクセスしているシステムとターゲット デバイスは同じドメインに参加していなければなりません。
- HPCA Console にアクセスしているシステム (Windows リモート アシスタンス操作の上級者側) には、次のソフトウェアがインストールされている必要があります。
  - Java Runtime Environment (JRE) バージョン 5 (またはそれ以降)

— オペレーティング システムが Windows 2008 Server の場合は、リモート インスタンス機能がインストールされている必要があります。詳細については、次の記事を参照してください。

http://technet.microsoft.com/en-us/library/cc753881.aspx

- すべてのターゲット デバイス上で、[リモート アシスタンスを提供する] グループ ポリシーが有効である必要があります。ターゲット デバイスへのアクセスが許可される「支援者」も指定する必要があります。ユーザーまたはグループのどちらかを支援者として設定できます。支援者は次のように指定します。

  `domain_name\user_name`

  `domain_name\groupname`

  ターゲット デバイスへの Windows リモート アシスタンス接続を作成するには、接続するユーザー (またはユーザーが所属するグループ) がこの支援者のリストに含まれている必要があります。

- すべてのターゲット デバイスで、リモート アシスタンスを Windows ファイアウォールの例外として有効にする必要があります。

Windows リモート アシスタンスの詳細については、次の Microsoft のサポート ドキュメントを参照してください。

http://technet.microsoft.com/en-us/library/cc753881.aspx

ファイアウォールの考慮事項

HPCA Console をホストするサーバーとリモート デバイスの間にファイアウォールが存在する場合、適切なポートを開く必要があります。

Windows リモート デスクトップ接続では、TCP ポート 3389 を使用します。

デフォルトでは、Windows リモート アシスタンスには、Windows XP または Windows Server 2003 のターゲット デバイスへの接続時に TCP ポート 3389 が必要です。Windows Vista または Windows Server 2008 のデバイスへの接続時には、ポート 135 (DCOM ポート) が必要です。

VNC の初回接続には、TCP ポート 5800 が必要です。さらに、TCP ポート 5900 (関与するシステムのタイプに応じて必要なポートがさらに増加) が必要です。次に例を示します。

- Windows システムでは、TCP ポート 5900 のみが必要です。

- Linux システムでは、たとえば VNC サーバーは host:1 で実行されるとします。この場合、サーバーとリモート デバイス間のファイアウォールでは、TCP ポート 5901 へのアクセスが許可される必要があります。

同様に、Java VNC ビューアでは TCP ポート 5800 (関与するシステムのタイプに応じて必要なポートがさらに増加) が必要です。

ファイアウォールと共に VNC を使用する方法の詳細については、次を参照してください。

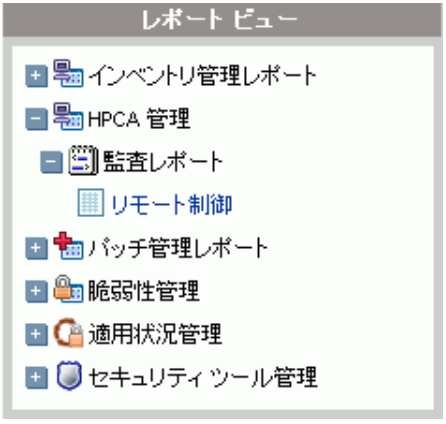
http://www.realvnc.com/support/faq.html#firewall

リモート制御の監査

HPCA 管理対象環境内のいずれかのユーザーが、HPCA Console を使用して管理対象デバイスへリモート接続を試行するたびに、リモート制御監査イベントとしてログに記録されます。次の情報が記録されます。

- リモート制御セッションを開始したユーザーと開始日時
- ターゲット デバイス
- 使用された接続のタイプ

リモート制御監査ログを表示するには、管理レポート ビューでリモート制御レポートを開きます。



リモート制御レポートには、次の情報が含まれています。

時刻 – リモート制御イベントが発生した日時

接続ステータス – リモート制御イベントの説明

ユーザー – リモート制御イベントを開始した HPCA Console ユーザーの ID

接続タイプ – VNC、リモート デスクトップ、またはリモート アシスタンス

ターゲット ホスト – リモート制御を通してアクセスされたデバイスのホスト名または IP アドレス

HPCA ホスト – HPCA Console をホストしているシステムのホスト名または IP アドレス

レポートは、カラム見出しをクリックして、任意のアイテムでソートできます。グレーの矢印は、ソート順を示しています。

関連トピック：

デバイスのリモート制御 180 ページ

レポートの使用 203 ページ

オペレーティング システムの管理

HPCA Console のオペレーティング システム (OS) 管理機能を使用して、クライアント デバイス上のオペレーティング システムのインストール、置換、更新、または修復ができます。また、HPCA を使用して、OS の配布前に完了する必要がある各種の低レベル タスク (BIOS ファームウェアの更新、設定、およびドライブ設定など) を実行できます。

ここでは、次のトピックを取り扱います。

HPCA における OS 管理の総合的な説明については、『HPCA OS Manager System Administrator ユーザー ガイド』を参照してください。

OS 管理の用語

次の用語は、HPCA の OS 管理の説明で全体を通して使用されます。

ベアメタル デバイス

ローカル OS がインストールされていないデバイスです。

HPCA Agent

ターゲット デバイスで稼動し、HPCA Configuration Server と通信するソフトウェア。

ハードウェア設定オブジェクト

HPCA データベースに保存されたオブジェクト。ターゲット デバイスにオペレーティング システムをインストールするためのターゲット デバイスのハードウェアの設定情報が含まれています。

ローカル サービスの起動 (LSB)

LSB は PXE の代替です。これにより、ネットワークから起動されていないデバイスの OS の管理を HPCA で行うことができます。

ベアメタルまたは障害復旧シナリオでは LSB は使用できません。LSB は、稼働中の OS から別の OS に移行する場合、またはドライブ管理に関連しない低レベルの管理タスクの実行にのみ使用できます。

管理対象デバイス

HPCA で認識され、管理されるデバイスです。

起動前実行環境 (PXE)

ネットワークを経由して HPCA Agent を開始するネットワーク ブート テクノロジ。

参照マシン

クローンする OS イメージを作成するためのワークステーションやサーバーです。

サービス オペレーティング システム (Service OS)

Service OS (SOS) は、Linux や WinPE のような軽量のオペレーティング システムを使用したプレインストール環境です。この環境はターゲット デバイスのハードウェアを実行する場合や、ターゲット デバイスをセットアップするときに使用します。

ターゲット デバイス

OS をインストール、置換、または更新するワークステーションまたはサーバーです。

管理対象外 OS

「管理対象外 OS」という用語は、次の両方の状態に当てはまります。

- ターゲット デバイスが探索されたが、そのデバイスにポリシーが割り当てられていない。
- ポリシーは割り当てられたが、既存の OS を上書きする準備ができていない。

OS 管理の前提条件

HPCA Console を使用してオペレーティング システム (OS) を配布する前に、次の前提条件が満たされている必要があります。

- 適切な OS イメージが利用可能である。

  詳細については、『HPCA OS Manager System Administrator ユーザー ガイド』の「OS イメージの準備と取得」を参照してください。

- OS イメージは、HPCA Configuration Server Database (CSDB) にパブリッシュされる必要があります。

  詳細については、『HPCA OS Manager System Administrator ユーザー ガイド』の「Publisher の使用」を参照してください。

ターゲット デバイス (複数可) 用に適切なハードウェア設定オブジェクトの作成が必要になる場合もあります。詳細については、『HPCA OS Manager ハードウェア設定管理ガイド』を参照してください。

これらの前提条件が満たされると、HPCA Console の OS 管理ウィザードを使用したオペレーティング システムの配布および管理ができるようになります。

配布シナリオ

お使いの環境のデバイスへの OS の配布は、いくつかの要因により異なります。次の表は、複数の OS イメージ配布シナリオおよびデバイスにオペレーティング システムを配布する手順を説明しています。

表 26　配布シナリオ

デバイスの状態	配布の手順
管理対象 (HPCA Agent インストール済み)	デバイスがすでに管理されている場合 • 省略可能 : グループにデバイスを追加 • OS 管理ウィザードを使用して OS を配布 注意 : OS 配布プロセスで LSB を使用する場合、PXE や ImageDeploy CD の準備は必要ありません。
非管理対象 (HPCA Agent 未インストール)	非管理対象デバイスに OS がインストールされている場合 • デバイスに HPCA Agent を配布 • 上の管理対象デバイスに関する手順を参照 非管理対象デバイスに OS がインストールされ*ていない*場合 • OS がインストールされていないデバイスへの OS の配布については、下の手順を参照
ベアメタル (OS 未インストール)	(ハード ディスクの復旧など) デバイスが以前管理されていた場合 • グループ メンバーシップおよび OS エンタイトルメントがまだ有効です。PXE または ImageDeploy CD を使用して OS を配布 デバイスが以前管理されたことがない場合 • PXE または ImageDeploy CD/DVD を使用してデバイスを起動 • MAC アドレスのバリエーションをデバイス名として使用し、デバイス オブジェクトが HPCA に追加される • OS 管理ウィザードを使用して OS を配布 • PXE または ImageDeploy CD/DVD を使用してデバイスを再起動 注意 : ベアメタル デバイスへの OS の配布には、LSB は使用できません。

OS を全デバイス グループに接続すると、その時点で存在しているデバイスには、自動的にその OS のエンタイトルメントが設定されます。複数の OS が全デバイスに接続されている場合、インストールする OS を選択します。OS がすべてのデバイスに接続された後に追加されたデバイスには、OS のエンタイトルメントは自動的に設定されません。

ターゲット デバイスの要件

ターゲット デバイスとは、OS をインストール、更新、または置換するワークステーションまたはサーバーです。ターゲット デバイスは次の要件を満たす必要があります。

- デバイスは、HPCA により配布される OS を実行するために、Microsoft (Windows オペレーティング システムの場合)、またはマシンのメーカーから公表されているハードウェアおよび BIOS の最低要件を満たす必要があります。
- デバイスは、DHCP サーバーに接続し、IP アドレスを取得する必要があります。
- ポリシー用に、マシンのモデル、メーカー、および一意の識別子のレポートを作成する場合、またはこれらを利用する場合、BIOS はシステム管理用の SMBIOS 仕様をサポートする必要があります。ターゲット デバイスが SMBIOS をサポートしていない場合、そのマシンでポリシーを指定するのに利用できる基準は MAC アドレスだけです。
- デバイスには、英語、フランス語、またはドイツ語のキーボードが必要です。
- デバイスには、128 MB 以上の RAM が必要です。
- ネットワーク (PXE) ブートを使用している場合、デバイスは次の条件を満たす必要があります。
  - Boot Server から起動できる。このためには、ハード ディスクの前にネットワークから起動するように BIOS を設定しておく必要があります。
  - PXE をサポートするネットワーク インターフェイス カード (NIC) がある。ネットワーク カードには PXE 対応のものがありますが、実際は、ネットワーク ブート ROM を追加しないと PXE はサポートされません。これらのカードに、ネットワーク ブート ROM が装備されている必要があります。以前の 3Com カードには、ファームウェアの MBA 4.3 へのアップグレードおよび PXE スタック バージョン 2.2 を必要とするものがあります。
  - Microsoft Sysprep を使用するには、ターゲット デバイスに、参照マシンと同じまたは互換性のある Hardware Abstraction Layer (HAL) を実装する。`HAL.DLL` のバージョンが同じマシンは、同じ Hardware Abstraction Layer を共有しています。マシンの HAL を判別する方法の詳細については、Microsoft サポート技術情報の記事、「Windows 2000 のハードウェア抽象層のトラブルシューティング」を参照してください。

HAL.DLL を確認できない場合、テスト環境でターゲット マシンにイメージを配布して、正しく配布されるかどうか確認することをお勧めします。

- デバイスには、IDE または SCSI (Adaptec のみ) ブート ドライブ インターフェイスが実装されている必要があります。
- デバイスでは、参照マシンの ACPI 特性 (HAL 内で示される ACPI と非 ASPI) およびブート ドライブ インターフェイスが一致している必要があります。
- デバイスには、参照マシンで取得された、HAL 内の Programmable Interrupt Controller の機能との互換性が必要です。Advanced Programmable Interrupt Controller (APIC) HAL は、APIC が実装されていないマシンでは実行できません。ただし、PIC (標準のオンボード Programmable Interrupt Controller) HAL は、APIC が実装されているマシン上で実行できます。比較的新しい HP/Compaq コンピュータでは、多くの場合、APIC が実装されています。
- デバイスは、NTFS および FAT32 ファイル システムをサポートしている必要があります。
- Windows XPe のイメージは、同等以上のサイズのフラッシュ ドライブを備えたターゲット マシンに配布できます。たとえば、256 MB のイメージは、256 MB または 512 MB のターゲット デバイスに配布できます。
- Embedded Linux または Windows CE のイメージは、サイズが同じフラッシュ ドライブを備えたターゲット マシンにしか配布できません。たとえば、256 MB のイメージは、256 MB のフラッシュ ドライブを装備したターゲット デバイスにしか配布できません。

OS イメージを配布すると、ターゲット デバイスのハード ドライブおよびパーティションの数によっては、既存のデータが上書きされる場合があります。次のシナリオは、イメージ配布プロセスで、影響を受けるパーティションと影響を受けないパーティションについて説明しています。

2 つのパーティションを持つ 1 台の HDD

ブート パーティションにイメージが配布され、もう 1 つのパーティションは影響を受けません。

1 つのパーティションを持つ 1 台の HDD

ハード ドライブにイメージが配布され、すべての既存のデータが上書きされます。

各 1 つのパーティションを持つ 2 台の HDD

1 台目のハード ドライブにイメージが配布され、このドライブ上のすべての既存のデータが上書きされます。2 台目のハード ディスクは影響を受けません。

各 2 つのパーティションを持つ 2 台の HDD

1 台目のハード ドライブのブート パーティションにイメージが配布され、もう 1 つのパーティションおよび 2 台目のハード ドライブは影響を受けません。

シン クライアントの出荷時イメージの配布

サポートされているシン クライアントのオペレーティング システム、Windows XP Embedded (XPe)、Windows CE、または Embedded Linux の出荷時イメージを配布する場合、次の点に注意します。

イメージがデバイスに配布された後、デバイスの管理を始めるために HPCA Agent をインストールする必要があります。詳細については、『HPCA Core および Satellite Enterprise Edition ユーザー ガイド』の「Installing the HPCA Agent on Thin Clients」を参照してください。

OS 配布の動作

OS 管理ウィザードを使用して、単一のデバイス、同時に選択した複数のデバイス、または Active Directory (AD) や Lightweight Directory Access Protocol (LDAP) グループなどの既存のデバイス グループにイメージを配布できます。

OS イメージを既存のグループ以外の複数のデバイスに配布する場合、[管理] タブの [ディレクトリ] 領域の [グループ] の下に新しいダイナミック グループが作成されます。このグループには、OS 配布のターゲットとなるすべてのデバイスが含まれます。グループの名前は「OS Deployment」で始まり、配布される OS の名前が含まれます。次に例を示します。

```
OS Deployment of WINXP Service to 2 devices (2009.Mar.11
06:08:046 PM)
```

OS を単一デバイスまたは複数デバイスのいずれに配布する場合でも、HPCA では、次の動作が実行されます。

- 選択されたイメージを OS ポリシーとして各デバイスに割り当てる。
- 各デバイスの ROM オブジェクトを、指定された OS 配布オプションに基づいて変更する。
- 通知を実行する RMP タイプのジョブを作成する。[現在のジョブ] ページで、このジョブのステータスを確認できます (159 ページの「現在と過去のジョブ」を参照)。

OS 配布状態の表示

デバイス用の OS を HPCA で管理している場合、OS 配布の状態がデバイスのディレクトリ オブジェクト ビューの [OS 管理] セクションに表示されます (このビューを表示するには **[プロパティの表示 / 編集]** を選択します)。

OS 配布待機中 – OS 配布ジョブは、スケジュールされ、実行を待機中です。

OS 配布進行中 – OS 配布ジョブが実行中です。

通常 – OS 配布ジョブは正常に完了し、OS が配布されました。

失敗 – OS の配布は失敗しました。

不明 – OS 配布ジョブの状態を判別できません。

OS イメージの配布

HPCA Console から OS を配布するには、5 つの手順が必要です。

1 ターゲット デバイス (複数可) またはデバイスを含む既存のグループを選択します。

2 配布する OS イメージを選択します。

3 省略可能: OS のインストール前に使用するハードウェア設定オブジェクトを選択します。

一部のターゲット デバイスでは、オペレーティング システムがインストール済みで特別な設定が不要な場合があります。ただし、オペレーティング システムのインストールを実施する前に、重要な操作を特定して適用する必要がある場合もあります。必要な操作の例として、BIOS ファームウェアの更新、ディスク アレイ コントローラ (DAC) の設定などがあります。

4 配布タイプを、LSB、PXE、または CD/DVD から選択します。

LSB 配布では、HPCA Agent が必要です。156 ページの「HPCA Agent の配布」を参照してください。

5 配布の開始日時を指定します。

ここでは、それぞれの手順について簡単に説明します。詳細については、『HPCA OS Manager System Administrator ユーザー ガイド』を参照してください。

OS イメージを配布する前に、次の前提条件が満たされていることを確認してください。188 ページの「OS 管理の前提条件」および 189 ページの「配布シナリオ」を参照してください。

OS イメージを配布するには :

1 **[管理]** タブで、[ディレクトリ] 領域に移動して、使用するゾーンを展開します。

- 1 つ以上のターゲット デバイスを個別に指定するには、**[デバイス]** をクリックします。
- グループを指定するには、**[グループ]** をクリックします。

> OS 配布に使用するグループは、同様の互換性のあるハードウェアで構成されている必要があります。

2 ディレクトリ オブジェクトの表で、使用するデバイスまたはグループを選択します。

3 **[オペレーティング システムの配布 / 管理]** ボタンをクリックします。「OS 管理ウィザード」が起動します。ウィザードの指示に従って、OS 配布ジョブを設定および開始します。

[管理] タブで、**[OS 管理]** の下のグループを監視すると、配布のステータスを確認できます。

OS 管理ウィザード

OS 配布の対象となるデバイスまたはグループを選択したら、次の手順に従って OS 管理ウィザードを完了します。

手順 1/5: オペレーティング システムの選択

a 次のいずれかのオプションを選択します。

- **新しいオペレーティング システムの設定** – 現在の OS を置き換えます
- **既存のオペレーティング システムを変更しない** – OS は変更されません

b 使用可能な OS イメージを 1 つ選択します。

c **[次へ]** をクリックします。

手順 2/5: ハードウェア設定オブジェクトの選択 (省略可能)

a ハードウェア設定オブジェクトを使用する場合、**[ハードウェア設定管理の使用]** を選択します。ハードウェア設定オブジェクトを使用しない場合は、手順 d に進みます。

詳細については、『HPCA OS Manager ハードウェア設定管理ガイド』を参照してください。

b 次のいずれかのオプションを選択します。

- **新しいハードウェア設定オプションの設定**
- **既存のハードウェア設定オプションの維持**

c 使用可能なハードウェア設定オプションを 1 つ選択します。

d **[次へ]** をクリックします。

手順 3/5: 追加オプション

a 使用する OS 配布メソッドを選択します。

- **ローカル サービスの起動 (LSB)**: OS を配布するために LSB をインストールする場合、このオプションを選択します。ローカル サービスの起動には、既存のマシンは PXE 対応である必要がなく、各ターゲット デバイスについて、起動の順序を BIOS でローカルに設定する必要がないという利点があります。196 ページの「LSB の使用」を参照してください。
- **ネットワークの起動 (PXE)**: デバイスにオペレーティング システムをインストールするために PXE サーバーを使用する場合は、このオプションを選択します。196 ページの「ネットワーク ブートの使用」を参照してください。
- **CD/DVD**: デバイスにオペレーティング システムをインストールするために ImageDeploy CD または DVD を使用する場合は、このオプションを選択します。197 ページの「ImageDeploy CD または DVD の使用」を参照してください。

b 災害復旧シナリオなど、既存のデータの取得および保存を試行せずに OS をインストールまたは再インストールする場合は、**[緊急モード]** を選択します。

このオプションにより、クライアント デバイスで管理アクティビティの必要性を判別できるようになります。このオプションが無効の場合、管理アクティビティの必要性を判別するには、クライアント デバイスに対して、既存の起動可能なオペレーティング システム、稼働中の HPCA Agent、および良好な一般整合性 (ウイルスが存在しないなど) が必要になります。

緊急モードを使用しない場合のデータの取得および保存に関する詳細については、『HPCA OS Manager System Administrator ガイド』の「ドライブ レイアウトの定義」を参照してください。

c 現在電源がオフになっているマシン上の管理操作を HPCA で起動するには、**[Wake on Lan]** を選択します。

d **[次へ]** をクリックします。

手順 4/5: スケジュール

a OS 配布ジョブを開始する **[開始日]** と **[開始時刻]** を指定します。

b **[次へ]** をクリックします。

手順 5/5: 要約

ウィザードの [要約] ページでは、OS 配布ジョブ用に指定したすべての設定を確認できます。ターゲット デバイスの一覧などが表示されます。**[サブミット]** をクリックしてジョブを作成します。RMP タイプの新しいジョブが、[管理] タブの **[現在のジョブ]** に表示されます。(158 ページの「ジョブを管理する」を参照)。

LSB の使用

ローカル サービスの起動 (LSB) オプションにより、ネットワークから起動されていないデバイスの OS の管理を HPCA で行うことができます。

LSB を使用するとき、既存のマシンは PXE 対応である必要はありません。また、各ターゲット デバイスについて、起動の順序を BIOS でローカルに設定する必要はありません。

OS 配布の前提要件については、189 ページの「配布シナリオ」を参照してください。

ネットワーク ブートの使用

PXE ベースの環境により、ネットワークから起動されるターゲット デバイスの OS の管理を HPCA で行うことができます。OS 配布の前提要件については、189 ページの「配布シナリオ」を参照してください。

PXE の使用は、ネットワークから起動しているクライアントにブート イメージを提供する DHCP サーバー、およびこれらのファイルを提供する TFTP サーバーの設定からなります。

DHCP サーバーおよび TFTP サーバーは、OS 配布に PXE を使用する前に、設定する必要があります。設定の指示は製品のドキュメントを参照してください。

PXE が設定されている場合、ターゲット デバイスがネットワークから起動すること、またはプライマリ ブート デバイスとして PXE が有効になっていることを確認してください。このような設定になるように、必要な設定の調節を行います (たとえば、BIOS の一部のバージョンでは、再起動プロセスの間に **ESC** キーを押して、起動順序設定を変更できます)。

ネットワーク ブートを使用して OS イメージを配布する場合、DHCP サーバーで指定した設定を使用して、ターゲット デバイスが再起動されます。次に、OS イメージが配布され、ターゲット デバイス上にインストールされます。複数の OS イメージがデバイスにエンタイトルメント設定されている場合、インストールする OS の選択画面が表示されます。

ImageDeploy CD または DVD の使用

ImageDeploy CD/DVD を使用して、オペレーティング システムがまだインストールされていないターゲット デバイス (ベアメタル マシン) をローカルに起動します。ImageDeploy CD/DVD は、ターゲット デバイスでローカルに利用可能でなければなりません。

CD または DVD を作成するには、HPCA に付属している `ImageDeploy.iso` ファイルを使用します。このファイルは、HPCA メディアの次の場所に格納されています。

`\Media\iso\roms\ImageDeploy.iso`

LSB は、まだ OS をインストールしていないデバイスには使用できないため、OS の配布前にベアメタル マシンを起動するには、ImageDeploy CD または PXE サーバーのいずれかを使用する必要があります。

OS 配布の前提要件については、189 ページの「配布シナリオ」を参照してください。

ImageDeploy CD を使用して OS イメージを配布するには :

1. ターゲット デバイス上で次の手順を実行します。
   a. ターゲット デバイスに ImageDeploy CD (または DVD) を挿入し、CD (または DVD) から起動します。
   b. 起動する SOS (**[Linux]** または **[WinPE]**) を指定します。

c 起動元メニューから、**[ネットワークからインストール]** を選択します。

d 入力を要求されたら、HPCA Server の IP アドレスまたはホスト名とポート番号を入力します。次に例を示します。

`HPCA.acmecorp.com:3466` または `192.168.1.100:3466`

ポート 3466 は、HPCA Core および Satellite のインストールでの OS のイメージングと配布用に予約されています。従来の CAE インストールでは、ポート 3469 がこの目的のために予約されています。

e **Enter** キーを押して続行します。

デバイスは、HPCA Server に接続され、MAC アドレスのバリエーションをデバイス名として使用して、デバイス リストに追加されます。ImageDeploy CD によって HPCA Server に接続すると、次のメッセージが表示されます。

`このマシンにローカル OS がないか、OS が無効です。`

`マシンは使用できず、管理者がポリシーを指定して Wake On LAN を実行するまでシャットダウンされます。`

2 HPCA Console で次の手順を実行します。

a [管理] タブで、193 ページの「OS イメージの配布」の手順に従います。

b 配布メソッドとして **[CD/DVD]** を選択します。

3 ウィザードが完了したら、ImageDeploy CD を使用して、ターゲット デバイスを再起動します。

この再起動の間に、OS イメージが検出され配布されます。この処理には 10 ～ 15 分かかります。処理時間はイメージのサイズおよびネットワークのバンド幅によって異なります。複数の OS イメージがデバイスにエンタイトルメント設定されている場合、インストールする OS の選択画面が表示されます。

イメージの配布が終了したら、ターゲット デバイスを再起動し、Windows を起動します。Sysprep プロセスが、新しいイメージを起動し、初期化します。

1 回限りのハードウェア メンテナンス操作の実行

HPCA Console を使用して、ハードウェア設定要素を使用するジョブを作成し、特別なハードウェア メンテナンス操作をクライアント デバイス上で実行できます。特定のデバイスに対して OS のインストール、更新、および修復を行う前に、

このジョブが必要となる場合があります。たとえば、アクティブ ホット スペア (AHS) が変更された場合の RAID (独立ディスクの冗長アレイ) の検証または再同期を起動する必要がある場合、このジョブを使用します。

BIOS ファームウェアの更新またはディスク アレイ コントローラ (DAC) の設定など、日常的な低レベルの操作については、通常の LDS/LME 管理プロセスを使用してください。

詳細については、『HPCA OS Manager ハードウェア設定管理ガイド』を参照してください。

1 回限りのハードウェア メンテナンス操作を実行するには :

1 **[管理]** タブで、[ディレクトリ] 領域に移動して、使用するゾーンを展開します。

   — 1 つ以上のターゲット デバイスを個別に指定するには、**[デバイス]** をクリックします。

   — グループを指定するには、**[グループ]** をクリックします。

2 ディレクトリ オブジェクトの表で、作業対象のデバイスまたはグループを選択します。

3 選択したいずれかのデバイスまたはグループのドロップダウン メニューで、[OS 管理] サブメニューの **[1 回限りのハードウェア メンテナンスの実行]** を選択します。

   ハードウェア メンテナンス ウィザードが起動します。

4 災害復旧シナリオなど、既存のデータの取得および保存を試行せずに OS をインストールまたは再インストールする場合は、**[緊急モード]** を選択します。

5 現在電源がオフになっているマシン上の管理操作を HPCA で起動するには、**[Wake on Lan]** を選択します。

6 [使用可能なメンテナンス オプション] リストから、使用するハードウェア設定要素を選択します。

7 OS 配布ジョブを開始する **[開始日]** と **[開始時刻]** を指定します。

8 **[次へ]** をクリックします。

   [要約] ページが表示されます。このページでは、このハードウェア メンテナンス ジョブ用に指定したすべての設定を確認できます。ターゲット デバイスの一覧などが表示されます。

9 **[サブミット]** をクリックしてジョブを作成します。

RMP タイプの新しいジョブが、[管理] タブの **[現在のジョブ]** に表示されます。(158 ページの「ジョブを管理する」を参照)。

OS 管理アクティビティのステータスの表示

OS 管理ウィザードで **[サブミット]** をクリックすると、RPM ジョブが作成されて **[現在のジョブ]** リストに表示されます (159 ページの「現在と過去のジョブ」を参照)。

OS 配布ジョブが終了すると、このジョブは **[過去のジョブ]** リストに移動します。

デバイス用の OS を HPCA で管理している場合、OS 配布の状態がデバイスのディレクトリ オブジェクト ビューの [OS 管理] セクションに表示されます (このビューを表示するには **[プロパティの表示 / 編集]** を選択します)。193 ページの「OS 配布状態の表示」を参照してください。

アウトバンドの詳細の表示

HPCA Console で使用可能なアウトバンド管理 (OOBM) 機能により、システムの電源状態やオペレーティング システムの状態とは無関係に、アウトバンド管理操作を実行できるようになります。

インバンド管理は、コンピュータの電源がオンでオペレーティング システムが稼働しているときに実行される操作を指します。

アウトバンド管理は、コンピュータが次のいずれかの状態のときに実行される操作を指します。

- コンピュータは電源に接続されているが稼働していない (オフ、スタンバイ、休止)
- オペレーティング システムがロードされていない (ソフトウェア障害またはブートの失敗)
- ソフトウェア ベースの管理エージェントが使用できない

HPCA Console では、Intel の vPro デバイスおよび DASH 対応デバイスのアウトバンド管理がサポートされます。

このオプションは、アウトバンド管理が有効な場合のみ使用できます。詳細については、314 ページの「アウトバンド管理」を参照してください。詳細については、『HP Client Automation Out of Band Management ガイド』を参照してください。

デバイスのアウトバンドの詳細を表示するには :

1 [管理] タブで [ディレクトリ] 領域に移動して、使用するゾーンを展開します。次に、**[デバイス]** (または **[グループ]**) をクリックします。

2 対象デバイスのショートカット メニューから **[アウトバンド デバイスの詳細]** を選択します。

デバイスに DASH または vPro が実装され、OOBM が有効で適切に設定されている場合、選択したデバイスの [アウトバンド デバイスの詳細] ウィンドウが表示されます。

アウトバンド デバイスの詳細  アイコンをクリックしても、特定のデバイスの OOB の詳細を表示できます。

アウトバンド管理が有効な場合、このアイコンが対象デバイスのディレクトリ オブジェクト ビューのツールバーに表示されます。

6　レポートの使用

[レポート] 領域には、多くの種類のレポートの要約と詳細が表示されます。保有している HPCA ライセンスのタイプによって、特定のレポートが使用できます。この章では、次のトピックについて説明します。

レポートの概要

HPCA Console の [レポート] タブには、次のレポートの収集に対するリンクが表示されます。

- HPCA 管理レポート
- 適用状況管理レポート
- インベントリ管理レポート
- パッチ管理レポート
- 脆弱性管理レポート
- セキュリティ ツール管理レポート

それぞれの収集には、特定のタイプのデータまたは特定の視聴者に焦点を当てたレポートのグループが含まれています。これらのレポートには、ダッシュボードに値を設定するために使用されるデータも表示されます。

次のレポートは、すべてのエディションの HPCA で使用可能です。

レポート パック	レポート タイプ	説明
rpm.kit	パッチ管理	パッチ ポリシーへの準拠デバイスと非準拠デバイス
rim.kit	インベントリ	現在 HPCA で管理されているデバイス

次のレポートは、HPCA Enterprise でのみ使用できます。

レポート パック	レポート タイプ	説明
vm.kit	脆弱性管理	脆弱性定義とクライアント デバイスのスキャン結果などのセキュリティ脆弱性情報
compliance.kit	適用状況管理	Secure Content Automation Protocol (SCAP) 適用状況規則と管理対象クライアント デバイスでの適用状況スキャン結果などの適用状況管理情報
stm.kit	セキュリティ ツール管理	ウイルス対策、スパイウェア対策、およびソフトウェア ファイアウォールのインストールと設定などのセキュリティ ツール管理情報
hpca.kit	HPCA 管理	監査レポート

[レポート] セクションのグラフィカル レポートを表示するには、Java Runtime Environment (JRE) または Java Virtual Machine (JVM) が必要です。詳細については、次のサイトを参照してください。

http://java.com/en/index.jsp

レポート間の移動

[レポート] タブをクリックすると、[レポートのホーム ページ] が表示されます。ここに示すように、ホーム ページには、適用状況管理、脆弱性管理、セキュリティ ツール管理、インベントリ管理、およびパッチ管理 (インストールされて有効になっている場合)

[レポートのホーム ページ] では、次の 3 種類の方法で詳細な情報を見つけることができます。

- クイックリンクを使用して頻繁に要求されるレポートを開く。
- クイック検索を使用して特定のデバイスまたはサービスについてのインベントリ情報を検索する。この機能は、インベントリ レポート (たとえば、管理対象デバイス) のみに適用されます。脆弱性管理レポートや適用状況管理レポートには適用されません。
- 左のナビゲーション ツリーの [レポート ビュー] セクションにあるリンクを使用して、特定のレポートを開きます。

  [レポート ビュー] では、現在のデータ セットで表示するレポート ウィンドウのセットと、各ウィンドウに関連した初期設定 (最小化や最大化、各ウィンドウのアイテム数など) が定義されます。初めてレポートにアクセスするときには、デフォルト ビューが適用されます。現在のビューは、グローバル ツールバーの右に表示されます。[レポート ビュー] は、変更やカスタマイズが可能です。

レポートが表示されているとき、[レポート] ページでは次のアクションを実行できます。

表 27　レポートのアクション

アイコン	説明
	レポート ビュー内を 1 ページ戻る。
	レポートのホーム ページに戻る。
	データをリフレッシュする。リフレッシュは、フィルタを適用または削除するときにも実行されます。
	このレポートをお気に入りのリストに追加する。
	このレポートへのリンクを電子メールで送る。
	「クイック ヘルプ」ボックスまたはツール チップが開きます。これは、フィルタにのみ適用されます。
	このレポートを印刷する。

表 27　レポートのアクション

アイコン	説明
	レポート ビューのデータ部分を折りたたむ。
	レポート ビューのデータ部分を展開する。
	このレポートのグラフィカル ビューを表示する。
	このレポートのグリッド (詳細) ビューを表示する。
	レポートのコンテンツをカンマ区切り値 (CSV) ファイルにエクスポートする。このファイルのデータは、実際にはカンマではなくタブで区切られます。ただし、ファイル拡張子は CSV です。
	レポートのコンテンツを Web クエリ (IQY) ファイルにエクスポートする。

レポートに青色テキストで表示されるアイテムには、さまざまな機能があります。

- 詳細を表示 – このアイテムに関してより詳細な情報まで掘り下げる
- このレポート ビューを起動 – このアイテムに基づいて新しいレポートを開く
- 検索条件に追加 – このアイテムに基づいて、現在のレポートに追加フィルタを適用する
- ベンダーのサイトに移動 – このブリテンの掲示板をポストしたベンダーの Web サイトに移動する

マウス カーソルを青色テキストのアイテム上に置くと、そのアイテムをクリックするとどのようなアクションが行われるかがツール チップに表示されます。

デフォルトでは、レポートでグリニッジ標準時 (GMT) が使用されます。個々のレポート パックは、GMT またはローカル時刻のいずれかを使用するように設定できます。

レポートのタイプ

HPCA Console では、次のタイプのレポートを使用できます。

- HPCA 管理レポート 209 ページ
- 適用状況管理レポート 213 ページ
- インベントリ管理レポート 209 ページ
- パッチ管理レポート 210 ページ
- 脆弱性管理レポート 211 ページ
- セキュリティ ツール管理レポート 215 ページ

ここでは、それぞれのレポートについて簡単に説明します。

HPCA 管理レポート

このビューには、さまざまな HPCA 機能に関する監査レポートが表示されます。たとえば、リモート制御監査レポートには、HPCA Console から管理対象クライアント デバイスに対して試みられたリモート制御セッションごとのエントリが含まれています。

インベントリ管理レポート

インベントリ管理レポートには、HPCA の全デバイスに関するハードウェアとソフトウェアの情報が表示されます。これには、HP 固有のハードウェア用レポート、詳細と要約のデバイス コンポーネント、ブレード サーバー、TPM チップセットと SMBIOS 情報、Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) 警告が含まれます。

レポート オプションを表示するには、インベントリ管理レポートのレポート ビューを展開します。たとえば、S.M.A.R.T 警告や HP 固有のレポートなどのいくつかの特定のデータは、HPCA コンポーネントを設定して初めて利用できることに注意してください。設定の詳細については、284 ページの「デバイス管理」を参照してください。

一般的な管理対象デバイス レポートには、次のテーブル見出しがあります。

- **詳細** – このデバイスの [デバイスの要約] ページを開く。
- **前回の接続** – デバイスが最後に接続された日時。
- **HPCA Agent ID** – デバイス名。
- **HPCA Agent のバージョン** – 現在インストールされている Management Agent のバージョン。
- **デバイス** – デバイス名。

- **前回ログオン ユーザー** – デバイスへのログオンで使用された最後のユーザー アカウント。複数のユーザーがログオンしている場合は、最後にログオンした ユーザーのみが記録されます。現在ログオンしているユーザーを切り替えても、これには影響しません。
- **IP アドレス** – デバイスの IP アドレス。
- **MAC アドレス** – デバイスの MAC アドレス。
- **オペレーティング システム** – デバイスにインストールされているオペレーティング システム。
- **OS レベル** – 現在のオペレーティング システム レベル (サービス パック 2 など)。

HP ハードウェア レポート

HP ハードウェア レポートは、インベントリ レポートのサブセットで、互換性のある HP デバイスの HP Client Management Interface (CMI) で取得された簡易警告情報が含まれます。

HP ハードウェア レポートは、インベントリ管理レポートの下のハードウェア レポート ビューに配置されます。

選択したレポート ビューに基づいて具体的な警告タイプまたは BIOS 設定を検索するには、[レポート] ウィンドウの一番上に表示される追加のデータ フィルタ検索ボックスを使用します。

パッチ管理レポート

パッチ管理レポートには、管理対象デバイスのパッチ適用状況情報や、パッチおよび Softpaq の取得情報が表示されます。

- **概要レポート** – 概要レポートには、お使いの環境で管理されているデバイスとブリテンのパッチ適用状況のスナップショットを視覚的に示す円グラフまたは棒グラフが表示されます。このレポートでは、すべてのデバイス、パッチ適用状態別のデバイス、ブリテン、およびベンダー別のブリテンの適用状況が要約されます。この要約レポートから、より詳細な適用状況レポートまで掘り下げ、フィルタを追加できます。
- **適用状況レポート** – HPCA Agent は、製品とパッチの情報を HPCA に送ります。この情報は利用可能なパッチと比較され、管理対象デバイスの脆弱性を削除するためパッチを必要とするかどうかが調査されます。適用状況レポートには、お使いの環境で検出されたデバイスに該当する情報しか表示されません。

- **パッチ取得レポート** – 取得ベースのレポートには、ベンダーの Web サイトからのパッチ取得プロセスの成功および失敗が表示されます。
- **リサーチ レポート** – リサーチ ベースのレポートには、ソフトウェア ベンダーの Web サイトから取得したパッチに関する情報が表示されます。リサーチ ベースのレポートでは、フィルタ バーが利用できます。

パッチ管理レポートの使用方法の詳細については、『HPCA Enterprise Patch Manager インストールおよび設定ガイド』を参照してください。

脆弱性管理レポート

脆弱性管理レポートは、次の 3 つのグループに整理できます。

- **概要** – これらのレポートには、お使いの環境での脆弱性管理アクティビティのスナップショットと傾向が示されます。
- **脆弱性レポート** – これらのレポートには、お使いの環境での脆弱性定義と、検出された脆弱性に関する詳細な情報が含まれています。
- **デバイス レポート** – これらのレポートには、お使いの環境の特定のデバイスで検出された脆弱性に関する情報が含まれています。

これらのレポートの多くをフィルタしたり、掘り下げて詳細を調べたりできます。たとえば脆弱性の一覧を表示するレポートの場合、特定の脆弱性の OVAL ID や CVE ID を使用して掘り下げ、関係するベンダー ブリテン (存在する場合) へのリンクにアクセスできます。一般にベンダーのブリテンには、脆弱性改善情報が含まれており、ソフトウェア パッチが含まれている場合もあります。

レポートを掘り下げてより詳細な情報を調べる場合は、要約レベル レポートに表示されるデータとは異なる方法でデータをフィルタできます。詳細については、219 ページの「レポートのフィルタ」を参照してください。

表 28　概要

レポート名	説明
脆弱性のトップ	企業において、最大数の管理対象クライアント デバイスで検出された脆弱性 10 件
脆弱性の高いサブネット	脆弱性を持つ管理対象クライアント デバイスの数および各デバイスの重大度カテゴリに基づいて判断された、最も脆弱なサブネットのリスト
脆弱性の高いデバイス	最大数の脆弱性が存在する、ネットワーク内のクライアントと デバイス 10 件のリスト
脆弱性の重大度別影響	昨年中に実行されたすべての脆弱性スキャンの結果。そのときの各重大度カテゴリにおける管理対象クライアント デバイスの数を含む
脆弱性履歴の評価	昨年中に実行されたすべての脆弱性スキャンの結果。そのときの各重大度カテゴリにおける管理対象クライアント デバイスの数を含む

表 29　脆弱性レポート

レポート名	説明
OVAL の定義	現在の脆弱性スキャンに含まれるすべての脆弱性の OVAL ID 別のリスト
アプリケーションの脆弱性	HPCA が現在スキャンしているすべてのソフトウェア アプリケーションの脆弱性のリスト
オペレーティング システムの脆弱性	HPCA が現在スキャンしているすべてのオペレーティング システム アプリケーションの脆弱性のリスト

表 29　脆弱性レポート

レポート名	説明
影響を受けたデバイス別の脆弱性	影響を受けるデバイスの数によってソートされた、管理対象クライアント デバイスで検出された脆弱性のリスト
取得履歴	実行された HP Live Network コンテンツ更新の履歴。各更新の高、中、および低脆弱性の数を含む

表 30　デバイス レポート

レポート名	説明
スキャン実施済みデバイス	スキャンされた管理対象クライアント デバイスと、各デバイスで検出された脆弱性の数のリスト
スキャン未実施のデバイス	スキャンされていない管理対象クライアント デバイスのリスト

これらのレポートは、[レポート] タブに表示されます。一部のレポートは、脆弱性管理ダッシュボードからも使用できます。

適用状況管理レポート

適用状況管理レポートは、次の 3 つのグループに整理できます。

- **概要** – これらのレポートには、適用状況管理の観点から見たお使いの環境のスナップショットが示されます。概要レポートを使用して、次の項目について容易に評価できます。
  - 準拠している、または準拠していないクライアント デバイスの数
  - 違反される頻度が最も多い適用状況規則
  - 非適用状況の程度が最も高いクライアント デバイス
- **SCAP レポート** – これらのレポートには、スキャンに含まれる各 Secure Content Automation Protocol (SCAP) ベンチマークに現在準拠している、または準拠していないクライアント デバイスの数が示されます。

- **デバイス レポート** – これらのレポートには、スキャンされたクライアント デバイスごとに、最後に実行された適用状況スキャンの結果が示されます。また、スキャンされなかったクライアント デバイスも示されます。

これらのレポートの多くをフィルタしたり、掘り下げて詳細を調べたりできます。詳細については、67 ページの「適用状況の失敗に関する情報の検索」を参照してください。

レポートを掘り下げてより詳細な情報を調べる場合は、要約レベル レポートに表示されるデータとは異なる方法でデータをフィルタできます。詳細については、219 ページの「レポートのフィルタ」を参照してください。

表 31　概要

レポート名	説明
適用状況ステータス	企業内の適用状況と非適用状況のスキャン実施済みクライアント デバイスの総数。
上位の SCAP 非適用状況デバイス	企業内で上位 10 件の非適用状況のスキャン実施済みクライアント デバイス。つまり、準拠している SCAP 規則の数が最も少ないデバイス。
上位の失敗した SCAP 規則	最大数のスキャン実施済みクライアント デバイスで適用されていなかった、上位 10 件の SCAP 規則。
適用状況評価履歴	1 年間で各ベンチマークに対してスキャンされた該当デバイスの平均デフォルト スコア (コンプライアント デバイスと非適用状況デバイスの数も示されます)。

表 32　SCAP レポート

レポート名	説明
適用状況の要約	現在の適用状況スキャンに含まれる全 SCAP ベンチマークのリストと、各ベンチマークに準拠している、または準拠していないスキャン実施済みクライアント デバイスの数。
適用状況規則	現在の適用状況スキャンに含まれる全 SCAP 規則のリストと、各規則に合格または失格したスキャン実施済みクライアント デバイスの数。
取得履歴	実行された HP Live Network 適用状況コンテンツ更新の履歴。更新のソース、スキャナがダウンロードされたかどうか、およびダウンロードされた各ベンチマークのベンチマーク ID とバージョンなど。

表 33　デバイス レポート

レポート名	説明
スキャン実施済みデバイス	スキャンされた管理対象クライアント デバイスの適用状況スキャン結果。これには、デバイスごとに、適用状況ステータス、デフォルト スコア、最後に実施された適用状況スキャンの日付、合格した規則の数、失格した規則の数が含まれます。
スキャン未実施のデバイス	SCAP ベンチマークへの適用状況がスキャンされなかった管理対象クライアント デバイスのリスト。

これらのレポートは、[レポート] タブに表示されます。一部のレポートは、適用情報管理ダッシュボードからも使用できます。

セキュリティ ツール管理レポート

セキュリティ ツール管理レポートは、次の 3 つのグループに整理できます。

- **概要** – これらのレポートには、管理対象デバイスでウイルス対策定義とスパイウェア対策定義が最後に更新された日時と、これらのデバイスでウイルスとスパイウェアの存在について最後にスキャンされた日時が示されます。
- **製品レポート** – これらのレポートには、クライアント デバイスで検出されたウイルス対策製品、スパイウェア対策製品、およびファイアウォール製品についての情報が含まれます。
  - 製品のタイプごとに、検出された全製品のリストと、これらの製品が検出されたデバイスのリストを表示できます。
  - ウイルス対策ツールとスパイウェア対策ツールについては、最後の定義更新日付を表示し、関係する各デバイスをスキャンできます。
  - ファイアウォール製品については、ファイアウォール規則のリストを表示できます。
- **デバイス レポート** – これらのレポートには、各タイプのセキュリティ ツールが各クライアント デバイスにインストールされているかどうか、有効になっているかどうか、またはインストールされ有効になっているかどうかが示されます。

セキュリティ ツール管理レポートは、[レポート] タブに表示されます。一部のレポートは、セキュリティ ツール管理ダッシュボードからも使用できます。

これらのレポートの多くをフィルタしたり、掘り下げて詳細を調べたりできます。詳細については、69 ページの「セキュリティ ツールに関する情報の検索」を参照してください。

レポートを掘り下げてより詳細な情報を調べる場合は、要約レベル レポートに表示されるデータとは異なる方法でデータをフィルタできます。詳細については、219 ページの「レポートのフィルタ」を参照してください。

表 34　概要

レポート名	説明
前回の定義更新の要約	管理対象クライアント デバイスで、スパイウェア対策定義とウイルス対策定義が最後に更新された日時
前回のスキャン日の要約	管理対象クライアント デバイスで、スパイウェアとウイルスの存在について最後にスキャンされた日時

表 34　概要

レポート名	説明
製品の要約	検出されたスパイウェア対策製品、ウイルス対策製品、ソフトウェア ファイアウォール製品のすべてのリストと、各製品がインストールされているクライアント デバイスの数
製品ステータスの要約	各タイプのセキュリティ ツールが検出され有効になっているデバイスの数、検出され無効になっているデバイスの数、検出されなかったデバイスの数、または不明なデバイスの数

表 35　製品レポート

レポート名	説明
Anti-Spyware	
検出されたスパイウェア対策製品	企業内の管理対象クライアント デバイスで検出されたスパイウェア対策ツールのリスト
スパイウェア対策製品がインストールされたデバイス	関係する各デバイスで実行された、スパイウェア定義の最後の更新とスパイウェア スキャンの日付
Anti-Virus	
検出されたウイルス対策製品	企業内の管理対象クライアント デバイスで検出されたウイルス対策ツールのリスト
ウイルス対策製品がインストールされたデバイス	関係する各デバイスで実行された、ウイルス定義の最後の更新とウイルス スキャンの日付
Firewall	
検出されたファイアウォール製品	企業内の管理対象クライアント デバイスで検出されたソフトウェア　ファイアウォール ツールのリスト

表 35　製品レポート

レポート名	説明
ファイアウォール製品がインストールされたデバイス	リアルタイム保護が有効になっており、バイナリが認証されているかどうかを含む、ソフトウェア ファイアウォール製品がインストールされている製品のリスト
ファイアウォール規則	検出された各ソフトウェア　ファイアウォール製品で現在適用されている規則のリスト
全製品	
検出された製品	企業内の管理対象クライアント デバイスで検出されたスパイウェア対策製品、ウイルス対策製品、およびソフトウェア ファイアウォール製品のすべてのリスト
取得履歴	HP Live Network からのセキュリティ ツール管理コンテンツの更新日付とステータス

表 36　デバイス レポート

レポート名	説明
スキャン実施済みデバイス	セキュリティ ツールの存在についてスキャンされた各管理対象クライアント デバイスで、インストールされている、有効になっている、またはインストールされて有効になっているセキュリティ ツールのリスト
スキャン未実施のデバイス	セキュリティ ツールの存在についてスキャンされていない管理対象クライアント デバイスのリスト

これらのレポートは、[レポート] タブに表示されます。一部のレポートは、セキュリティ ツール管理ダッシュボードからも使用できます。

次の各レポートには、管理対象クライアント デバイスにインストールされているセキュリティ ツールの状態に関する要約の統計値が含まれています。

- 製品の要約 ([概要] の下)

- 検出された製品 ([製品レポート] > [全製品] の下)
- スキャン実施済みデバイス ([デバイス レポート] > [スキャン実施済みデバイス] の下)

これらの統計情報は、特定のスキャン実施済みデバイスの [デバイスの詳細ビュー] にある **[検出されたセキュリティ製品の統計値]** の展開時にも表示されます。このビューを表示するには、次の手順に従います。

1 [デバイス レポート] > [スキャン実施済みデバイス] レポートを開きます。

2 特定のデバイスの **[詳細]** アイコンをクリックします。

3 [デバイスの詳細] セクションで、もう一度 **[詳細]** アイコンをクリックします。

詳細な情報への掘り下げ

多くのレポートでは、特定のデバイス、脆弱性、適用状況ベンチマーク、またはセキュリティ製品について、極めて詳細な情報まで掘り下げることができます。

データ グリッドに [詳細] ( ) アイコンが表示されている場合にはいつでも、クリックして詳細情報を表示できます。

また、一部のレポートでは、特定のカラムのデバイスの数をクリックすることにより、より詳細な情報まで掘り下げられます。

次のページも参照してください。

- 脆弱性改善情報の検索 65 ページ
- 適用状況の失敗に関する情報の検索 67 ページ
- セキュリティ ツールに関する情報の検索 69 ページ

レポートのフィルタ

レポートの多くでは、含まれるデータが膨大な量になります。レポートに 1 つ以上のフィルタを適用することにより、表示されるデータ量を減らすことができます。一度適用されたフィルタは、明示的に削除されるまで有効な状態が維持されます。

フィルタには、次の基本的な 3 つのタイプがあります。

- ディレクトリ / グループ フィルタを適用すると、特定のデバイスまたはデバイス グループのデータを表示できます。
- インベントリ管理フィルタを適用すると、ハードウェア、ソフトウェア、オペレーティング システム、または HPCA オペレーション ステータスなどの共通の特性とともに、デバイス グループのデータを表示できます。
- レポート固有のフィルタは、特定のレポート ビュー内で利用可能なデータにのみ適用されます。たとえば、適用状況管理フィルタは適用状況管理レポートに対してのみ適用されます。

フィルタは、フィルタ対象のデータ タイプがレポートに含まれる場合にのみ機能します。

現在のレポートのデータに関係しないフィルタの適用を試みても、そのフィルタによる影響は生じません。逆に、レポート内のデータが正しくないように見える場合は、誤ったフィルタが適用されていないことを確認してください。

概要レポートのほとんどは、元々含まれるデータ量が少ないため、フィルタを適用できません。

レポートにフィルタを適用するには

1 左のナビゲーション ツリーの [データ フィルタ] セクションで、使用するフィルタ グループを展開します。

2 省略可能 : 適用する特定のフィルタについて、  (表示 / 非表示) ボタンをクリックしてフィルタのコントロールを表示します。

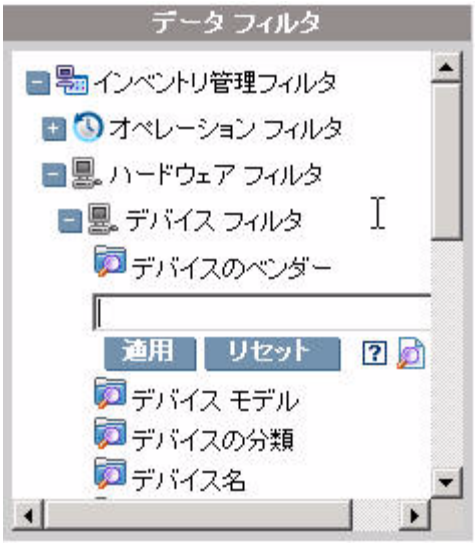
3 テキスト ボックスでフィルタ条件を指定するか、  (条件) ボタンをクリックしてリストから条件を選択します (表示された場合。すべてのフィルタでリストが表示されるとは限りません)。

フィルタの作成時には、ワイルドカード文字を使用できます。次の表に、検索文字列の入力時に使用可能な文字の説明を示します。

表 37　特殊文字とワイルドカード

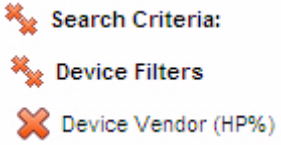
文字	機能	デバイスのベンダーフィルタの例	一致するレコード
* または %	特定のテキスト文字列を含むすべてのレコードに一致する	HP*	「HP」で始まるすべてのレコード
		%HP%	「HP」を含むすべてのレコード
? または _	任意の 1 文字に一致にする	Not?book	「Not」で始まり「book」で終わるすべてのレコード
		Note_ook	「Note」で始まり「ook」で終わるすべてのレコード
!	フィルタを否定する	!HP*	「HP」で始まらないすべてのレコード

たとえば、フィルタに関連付けるデバイスのテキスト ボックスに「HP%」と指定すると、フィルタはベンダー名に HP を含むすべてのデバイスに一致します。



4 **[適用]** ボタンをクリックします。レポートがリフレッシュされます。フィルタを削除するには、**[リセット]** ボタンをクリックします。

フィルタをレポートに適用すると、レポート ヘッダーに次のようにフィルタが表示されます。



一度適用されたフィルタは、明示的に削除されるまで有効な状態が維持されます。フィルタ名の左側にある ([削除] ボタン) をクリックして、現在のレポートからフィルタを削除できます。

また、現在表示されているレポートのデータ フィールドをクリックすることにより、「インライン」フィルタを作成することもできます。たとえば、脆弱性定義レポートを表示しているときに、[高] 重大度の脆弱性のみを表示するには、[重大度] カラムの (高重大度) アイコンをクリックします。

脆弱性管理フィルタ

次の表に、脆弱性管理フィルタとレポートの対応関係の概要を示します。

表 38　脆弱性管理フィルタ

レポート	適用可能なフィルタ
OVAL の定義 影響を受けたデバイス別の脆弱性	OVAL 定義 ID CVE ID 重大度
アプリケーションの脆弱性	OVAL 定義 ID CVE ID 重大度 アプリケーション ベンダー [a]
オペレーティング システムの脆弱性	OVAL 定義 ID CVE ID 重大度 オペレーティング システム [c] ベンダー [a]
脆弱性の高いデバイス	デバイス名 [b] 最大リスク
脆弱性の重大度別影響	デバイス名 [b] 最大リスク オペレーティング システム [c]
取得履歴	脆弱性取得ソース

表 38　脆弱性管理フィルタ

レポート	適用可能なフィルタ
スキャン実施済みデバイス	デバイス名 [b] 最大リスク ハードウェア ベンダー [b] ハードウェア モデル [b] ハードウェア クラス [b]
スキャン未実施のデバイス	デバイス名 [b] ハードウェア ベンダー [b] ハードウェア モデル [b] ハードウェア クラス [b]

a　ベンダー フィルタは、スキャン実施済みデバイス レポートを掘り下げるときに適用することも可能です。65 ページの「脆弱性改善情報の検索」を参照してください。

b　[インベントリ管理フィルタ] > [ハードウェア フィルタ] > [デバイス フィルタ] に配置されています。

c　[インベントリ管理フィルタ] > [OS フィルタ] に配置されています。

適用状況管理フィルタ

次の表に、適用状況管理フィルタとレポートの対応関係の概要を示します。

表 39　適用状況管理フィルタ

レポート	適用可能なフィルタ
上位の SCAP 非適用状況デバイス	ベンチマーク ベンチマーク バージョン ベンチマーク プロファイル
適用状況評価履歴	ベンチマーク ベンチマーク バージョン

表 39　適用状況管理フィルタ

レポート	適用可能なフィルタ
適用状況の要約	デバイス名 [a] デバイス適用状況ステータス ハードウェア ベンダー [a] ハードウェア モデル [a] ハードウェア クラス [a] ベンチマーク ベンチマーク バージョン ベンチマーク プロファイル
適用状況規則	ベンチマーク ベンチマーク バージョン ベンチマーク プロファイル 規則 CCE ID
取得履歴	取得ソース ベンチマーク ベンチマーク バージョン ベンチマーク プロファイル
スキャン実施済みデバイス	デバイス名 [a] デバイス適用状況ステータス ハードウェア ベンダー [a] ハードウェア モデル [a] ハードウェア クラス [a] ベンチマーク ベンチマーク バージョン ベンチマーク プロファイル

表 39　適用状況管理フィルタ

レポート	適用可能なフィルタ
スキャン未実施のデバイス	デバイス名 [a] ハードウェア ベンダー [a] ハードウェア モデル [a] ハードウェア クラス [a] オペレーティング システム [b] オペレーティング システムのレベル [b]

a　[インベントリ管理フィルタ] > [ハードウェア フィルタ] > [デバイス フィルタ] に配置されています。

b　[インベントリ管理フィルタ] > [OS フィルタ] に配置されています。

セキュリティ ツール管理フィルタ

次の表に、セキュリティ ツール管理フィルタとレポートの対応関係の概要を示します。

レポート	適用可能なフィルタ
検出された製品	製品タイプ
検出されたスパイウェア対策製品 検出されたウイルス対策製品 検出されたファイアウォール製品 検出された製品	製品名 製品のバージョン 製品ベンダー

レポート	適用可能なフィルタ
スパイウェア対策製品がインストールされたデバイス ウイルス対策製品がインストールされたデバイス ファイアウォール対策製品がインストールされたデバイス スキャン実施済みデバイス スキャン未実施のデバイス	デバイス名 [a] ハードウェア ベンダー [a] ハードウェア モデル [a] ハードウェア クラス [a] オペレーティング システム [b] オペレーティング システムのレベル [b]
ファイアウォール規則	ファイアウォール規則名 ファイアウォール規則タイプ ファイアウォール規則プロトコル

a [インベントリ管理フィルタ] > [ハードウェア フィルタ] > [デバイス フィルタ] に配置されています。

b [インベントリ管理フィルタ] > [OS フィルタ] に配置されています。

7 オペレーション

[オペレーション] タブでは、インフラストラクチャ タスクを管理したり、コンポーネント サービスのステータスを表示したり、一部のパッチ管理タスクを実行したりすることができます。詳細については、次のセクションで説明します。

Satellite コンソールの [オペレーション] タブには、次のセクションで説明する [サーバーのステータス] と [サポート] 情報が表示されます。

インフラストラクチャ管理

[インフラストラクチャ管理] オペレーションは、次のセクションで説明します。

サーバーのステータス

[サーバーのステータス] には、現在インストールされているライセンス情報のほか、HPCA Server によって制御されるコンポーネント サービスの一覧が表示されます。これらのコンポーネント サービスは、HPCA 処理の異なる側面を処理します。[サーバーのステータス] の **[要約]** テーブルでは、これらのどのサービスが有効になっているかを確認できます。

コンポーネント サービスのステータスを確認するには

1. HPCA Console で、[オペレーション] タブに移動し、**[サービスのステータス]** をクリックします。
2. コンポーネントサービスの一覧と各サービスが有効になっているかどうかを示す [要約] テーブルが表示されます。

Satellite コンソールの [サーバーのステータス] ページには、その他のプロパティが表示されます。

- アップストリーム サーバー
- データ キャッシュの利用状況
- データ キャッシュの容量
- 同期ステータス

Satellite コンソールの [サーバーのステータス] ページには、データ キャッシュを更新できる **[タスク]** 領域が表示されます。

Satellite を今すぐ同期

Satellite Server のコンテンツ (ソフトウェア サービス、パッチ、およびオペレーティング システム イメージ) をアップストリーム ホストと同期する必要があります。

Satellite Server のデータをキャッシュおよび同期するには、まず Satellite を設定する必要があります。詳細については、『HPCA Core および Satellite 入門およびコンセプト ガイド』を参照してください。

同期を実行すると、Satellite 上で有効になっている、各サービスで使用されるコンテンツが同期されます。たとえば、Satellite が完全に有効になっている場合は、次の内容が同期されます。

- HPCA Agent のメンテナンス
- 設定のメタデータ
- ソフトウェアとパッチのためのデータ キャッシュ リソース (データ キャッシュが有効になっている必要があります)
- オペレーティング システム イメージ (オペレーティング システム サービスが有効になっている必要があります)

Satellite Server の同期は、Core Server でジョブを作成することによってスケジュールできます。詳細については、171 ページの「Satellite 同期ジョブの作成」を参照してください。

データ キャッシュをフラッシュ

アップストリーム サーバーから重要な新しいリソースをダウンロードする必要があるが、現在のデータ キャッシュの利用状況が容量の限界に近づいているか、またはデータ キャッシュに古いファイルや破損したファイルが含まれている場合は、リソース キャッシュをフラッシュして新しいリソースをすばやくロードするための空き容量を確保できます。

このオプションによってキャッシュ全体 (ダイナミックおよびプレロード) がフラッシュされるため、使用する場合は注意してください。

このアクションで重要なファイルが誤って削除される可能性があります。

サポート

[サポート] 領域には、現在インストールされているライセンス情報が表示されます。また、設定ファイル、ログ ファイル、およびオペレーティング システム情報を含む圧縮ファイル (zip) を生成したりダウンロードしたりすることもできます。

詳細については、232 ページの「ログ ファイルのダウンロード」を参照してください。

これらのファイルは、HP サポートでトラブルシューティングに必要になった場合に使用可能になります。

ログ ファイルのダウンロード

弊社サポート センターに連絡すると、ログ ファイルの提供を求められる場合があります。用意されているリンクを使用して、現在のサーバー ログ ファイルの圧縮ファイルをダウンロードし保存します。

ログ ファイルをダウンロードするには

1. [トラブルシューティング] 領域で、**[現在のサーバー ログ ファイルをダウンロード]** リンクをクリックします。新しいウィンドウが開きます。
2. ログファイルが準備できたら、**[logfiles.zip をダウンロードします]** をクリックします。
3. 表示メッセージに応じて **[保存]** をクリックし、圧縮ファイルをコンピュータに保存します。
4. ファイルを保存する場所を指定して、**[OK]** をクリックします。
5. ログ ファイルがコンピュータにダウンロードされ、1 つの ZIP 形式ファイルで保存されます。

> Internet Explorer のセキュリティ設定により、これらのファイルをダウンロードできない場合があります。信頼できるサイトに HPCA Console の URL を追加するか、またはファイルのダウンロード時にダイアログを表示しないように Internet Explorer の設定を変更することをお勧めします。

Live Network

HP Live Network のセキュリティとコンプライアンス管理コンテンツを更新する方法と時期を指定するには、Live Network の設定を使用します。自動更新のスケジュールを設定するか、すぐに更新を開始できます。最新のセキュリティと

コンプライアンススキャナおよびデータが確実に使用されるようにするために、HPCA ソフトウェアをインストールまたはアップグレードした後は、必ず更新を実行してください。

HPCA で HP Live Network サイト (またはファイル システム) からコンテンツを更新する場合、HP Live Network コネクタ (LNC) と呼ばれるツールが使用されます。このツールは HPCA によってインストールされ、自己更新されます。特定の環境下では、LNC の新しいコピーをインストールすることもできます。詳細については、236 ページの「HP Live Network コネクタのダウンロード」を参照してください。

自動更新のスケジュールを選択するか、またはすぐに更新を開始するかどうかにかかわらず、更新のコンテンツの送信元を指定する必要があります。次の 3 つの選択肢があります。

- **HP Live Network から**

  セキュリティとコンプライアンススキャナおよびデータは HP Live Network コンテンツ サーバーから取得され、HPCA インフラストラクチャにパブリッシュされます。デフォルトでは、このパスは次のとおりです。

  `<InstallDir> \LiveNetwork\lnc\bin\live-network-connector.bat`

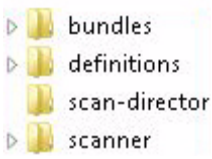
  このパスは、HPCA によって自動的に設定されます。HP Live Network コネクタの新しいコピーをダウンロードして、別のロケーションにインストールしていない限り、このパスを指定する必要はありません。

  このオプションを使用するには、アクティブな HP Live Network サブスクリプションが必要です。これは、HPCA ソフトウェアには含まれていません。詳細については、当社の担当にお問い合わせください。

- **ファイル システムから**

  Enterprise Manager がインストールされているシステムのファイル システム内のロケーションから、脆弱性と適用状況スキャナおよびデータのコピーがパブリッシュされます。スキャナおよびデータが含まれているフォルダのパス名を指定する必要があります。また、更新を開始する前に、HP Live Network コンテンツ サーバーからこれらのアイテムを手動でダウンロードする必要があります。

  指定されたファイル システム ロケーションのフォルダ構造が、次に示すように、HP Live Network コネクタがコンテンツをダウンロードするときに作成されたフォルダ構造に正確に一致している必要があります。



また、これらの各フォルダの下にあるサブディレクトリも正確に一致している必要があります。

場合によっては、HP Live Network によって、セキュリティとコンプライアンス管理コンテンツのサブセットのみが更新されることがあります。この場合は、Live Network の更新中に、これらのディレクトリの一部が提供されない可能性があります。

このオプションを使用する方法の詳細については、76 ページの「HP Live Network コネクタの手動での実行」を参照してください。

- **Configuration Server Database から**

  以前に CSDB にパブリッシュされた脆弱性の定義がレポート データベースにロードされます。

  78 ページの「テスト環境からプロダクション環境への HP Live Network コンテンツの移動」を参照してください。

Live Network の自動更新のスケジュール

選択したコンテンツの送信元からの HP Live Network の自動更新のスケジュールを確立するには、次の手順を使用します。

HP Live Network のコンテンツの自動更新をスケジュールするには

1. [オペレーション] タブで、[インフラストラクチャ管理] 領域を展開し、**[Live Network]** をクリックします。
2. **[スケジュールの更新]** タブをクリックします。
3. [更新] セクションで、コンテンツの送信元を選択します。
4. 自動更新のスケジュールを指定します。
   a. **スケジュール** — [一度] 、[時間単位] 、[日単位] 、[週単位] 、または [なし] を選択します。

      [なし] は、たとえば以前にスケジュールされた [一度] のタスクが既に完了している場合など、現在実行対象のスケジュールがないときに Enterprise Manager に表示されます。新しい更新スケジュールがない場

合や既存のスケジュールを停止する場合に、[なし] を指定できます。反復スケジュールがある場合は、最後に保存されたスケジュールが表示されます (たとえば、[時間単位] 、[日単位] 、[週単位] など)。

b **開始時刻** — 更新を開始する時刻。

c **開始日** — 自動更新を開始する日付。  (カレンダー) ボタンをクリックし、日付を選択します。

[スケジュールの更新] タブが表示されたとき、時刻と日付のフィールドには、最後に保存されたスケジュールの時刻と日付が表示されます。たとえば、以前にスケジュールされた [一度] の更新が既に完了している場合、スケジュールは [なし] に設定され、[開始時刻] と [開始日] のフィールドには最後の更新の時刻と日付が表示されます。

d **[スケジュール]** として [時間単位] 、[日単位] または [週単位] を選択した場合は、**[間隔]** ボックスに更新の間隔を指定します。

たとえば、[日単位] を選択し、**[間隔]** に 2 を指定すると、2 日ごとに更新が実行されます。

5 **[保存]** をクリックして、変更内容を実装します。

このタブから離れると、**[保存]** をクリックする前に入力した情報はすべて失われます。情報を保存する場合は、必ず **[保存]** をクリックしてください。

[リセット] ボタンを使用して、最後に保存された設定を復元できます。

HP Live Network コンテンツを今すぐ更新する

HP Live Network のコンテンツを今すぐ更新するには、次の手順を使用します。これは、自動更新用に設定したスケジュールには影響しません。

HP Live Network のコンテンツを直ちに更新するには

1 [オペレーション] タブで、[インフラストラクチャ管理] 領域を展開し、**[Live Network]** をクリックします。

2 **[すぐに更新]** タブをクリックします。

3 この更新のためのコンテンツの送信元を選択します。これは、現在スケジュールされている自動更新には影響しません。

4 **[すぐに更新]** ボタンをクリックします。指定したコンテンツの送信元からスキャナおよびデータを更新するためのリクエストが発行されます。

更新は、完了するまでにある程度の時間が必要な非同期のプロセスです。取得レポートを使用すると、更新の結果を表示したり、そのステータスをチェックしたりできます。

更新の結果またはステータスの表示

HPCA レポートを使用すると、HP Live Network コンテンツの更新ステータスをチェックできます。

更新の結果またはステータスを表示するには

1 **[レポート]** タブをクリックします。

2 コンテンツの更新ステータスを表示するには、次の各レポート ビューで **[取得履歴]** レポートを開きます。

[脆弱性管理] > [脆弱性レポート]

[適用状況管理] > [SCAP レポート]

[セキュリティ ツール管理] > [製品レポート] > [全製品]

HP Live Network に関連した設定情報が不完全か正しくない場合は、更新が失敗します。これはレポートと次のログ ファイルの両方に反映されます。

`<InstallDir > \HPCA\VulnerabilityServer\logs\vms-server.log`

ただし、この他に更新が失敗したことを示すものは Enterprise Manager にはありません。

HP Live Network コネクタのダウンロード

HP Live Network コネクタ (LNC) は HPCA に付属しており、Live Network の設定を初めて設定したときに自動的にインストールされます。LNC は自己更新されます。HP Live Network コンテンツを更新する場合は、必ず LNC によって使用可能な LNC 更新がすべてチェックされ、インストールされます。このようにして、Live Network の更新のたびに、最新バージョンの LNC がインストールされることが常に保証されます。

何らかの理由で LNC を再インストールする必要がある場合 (たとえば、だれかに誤ってアンインストールされた場合) は、次の手順を実行します。

HP Live Network コネクタの新しいコピーをダウンロードするには

1 [設定] タブで、[インフラストラクチャ管理] 領域を展開し、**[Live Network]** をクリックします。

2 [HP Live Network コネクタ] ボックスの右側にある **[ダウンロード]** リンクをクリックします。新しいブラウザ ウィンドウが開き、HP Live Network サイトが表示されます。そこから LNC の実行可能ファイルをダウンロードできます。ログインするには、HP Live Network サブスクリプションのユーザー名とパスワードが必要です。

3 LNC をダウンロードしてインストールするには、HP Live Network サイトの指示に従ってください。

LNC を元のインストール ロケーション以外のロケーションにインストールする場合は、それに応じて Live Network 設定ページの **[HP Live Network コネクタ]** のパスを必ず更新してください。デフォルトのインストール ロケーションは次のとおりです。

CAE インストール :

```
<InstallDir > \LiveNetwork\lnc\bin\live-network-connector.bat
```

Core および Satellite インストールの HPCA Core サーバー :

```
<InstallDir >\HPCA\LiveNetwork\lnc\bin\live-network-connector.bat
```

アウトバンド管理

アウトバンド (OOB) 管理は、[設定] タブを使用して有効にします。OOB 管理の設定については、253 ページの「設定」を参照してください。

OOB 管理の使用方法の詳細については、『HPCA Out of Band Management ユーザー ガイド』を参照してください。

次のセクションでは、コンソールで実行できる OOB 管理タスクについて説明します。

- グループ管理 240 ページ
- 警告の通知 241 ページ

プロビジョニングと設定情報

vPro デバイスや DASH デバイスを検出したり管理したりできるようにするには、事前にそれらのデバイスをプロビジョニングする必要があります。vPro デバイスが、最初にネットワークに接続されたときに自動的にプロビジョニングされなかった場合は、HPCA Console からこれらのデバイスをプロビジョニングできます。

HPCA Console からの vPro デバイスのプロビジョニングは、『HPCA Out of Band Management ユーザー ガイド』の「Provisioning vPro Devices」の章で説明されています。DASH デバイスのみを管理することを選択した場合、このオプションはこのタイプのデバイスに関連しないため、[アウトバンド管理] の下にある [オペレーション] タブには表示されません。

詳細については、『HPCA Out of Band Management ユーザー ガイド』の「Provisioning vPro Devices」の章を参照してください。

DASH 設定関連ドキュメント

ここでは、DASH 対応デバイスがこれらのデバイスに付随するドキュメントに従って既にプロビジョニングされていることを前提にしています。DASH 設定の情報は、「Broadcom NetXtreme Gigabit Ethernet Plus NIC」のホワイト ペーパーに記載されています。このホワイト ペーパーは、この NIC をサポートする各製品の [Manuals (guides, supplements, addendums, etc)] のセクションにあります。

この情報は、当社の DASH 対応デバイスにのみ関連しています。

このドキュメントにアクセスするには

1. www.hp.com に移動します。
2. [サポート & ドライバ] > [製品マニュアル、トラブルシューティング、修理など] を選択します。
3. この NIC をサポートする製品 (たとえば、dc5850) を入力します。
4. dc5850 モデルの 1 つを選択します。
5. [Manuals (guides, supplements, addendums, etc)] を選択します。

6 「Broadcom NetXtreme Gigabit Ethernet Plus NIC」のホワイト ペーパーを選択します。

DASH 設定ユーティリティ

DASH 設定ユーティリティ (BMCC アプリケーション) は、この NIC をサポートする各製品のドライバ セクションにある Broadcom NetXtreme Gigabit Ethernet Plus NIC ドライバ Softpaq の一部です。

このユーティリティにアクセスするには

1 www.hp.com に移動します。

2 [サポート & ドライバ] > [ドライバ & ソフトウェア ダウンロード] を選択します。

3 この NIC をサポートする製品 (たとえば、dc7900) を入力します。

4 dc7900 モデルの 1 つを選択します。

5 オペレーティング システムを選択します。

6 [ドライバ - ネットワーク] セクションまでスクロールし、NetXtreme Gigabit Ethernet Plus NIC ドライバを選択してダウンロードします。

デバイス管理

[デバイス管理] 領域では、複数の OOB デバイスおよび個々の OOB デバイスを管理できます。

[オペレーション] タブの [アウトバンド管理] の下で、[デバイス管理] をクリックします。[デバイス管理] ウィンドウが表示されます。デバイス テーブルのツールバーにあるアイコンから、複数のデバイスに次のタスクを実行できます。

- データのリフレッシュ
- デバイス情報のリロード
- デバイスの探索
- デバイスの電源オン / オフおよび再起動
- vPro 警告のサブスクライブ
- vPro デバイスに関する共通ユーティリティの管理
- 選択された vPro デバイスへのシステム防御ポリシーの配布

- 選択された vPro デバイスへのヒューリスティック ワーム封じ込め情報の配布
- 選択された vPro デバイスへのエージェント ウォッチドッグの配布
- 選択された vPro デバイスへのエージェント ソフトウェア リストとシステム メッセージの配布

個々の OOB デバイスを管理するには、デバイス テーブル内のホスト名のリンクをクリックします。管理ウィンドウが開き、左側のナビゲーション ペインにいくつかのオプションが表示されます。使用可能なオプションは、選択した管理対象デバイスのタイプによって異なります。

詳細については、『HPCA Out of Band Management ユーザー ガイド』の「Device Management」の章を参照してください。

グループ管理

[グループ管理] オプションでは、Client Automation ソフトウェアで定義された vPro デバイスのグループを管理できます。vPro デバイスを含む Client Automation グループに対して OOB 操作を実行できます。vPro デバイスのグループを管理することにより、さまざまな検出、自己回復、および保護タスクを実行できます。これには、電源管理、警告のサブスクリプションのほか、システム防御ポリシー、エージェント ウォッチドッグ、ローカルのエージェント ソフトウェア リスト、およびヒューリスティックの配布が含まれます。

[オペレーション] タブの [アウトバンド管理] の下で、[グループ管理] をクリックします。[グループ管理] ウィンドウが表示されます。グループ テーブルのツールバーにあるアイコンから、複数のグループに対して次のタスクを実行できます。

- データのリフレッシュ
- グループ情報のリロード
- グループの電源オン / オフおよび再起動
- vPro 警告のサブスクライブ
- 選択された vPro グループへのエージェント ソフトウェア リストとシステム メッセージの配布
- vPro デバイス グループのプロビジョニング
- 選択された vPro デバイスへのシステム防御ポリシーの配布および回収
- 選択された vPro グループへのエージェント ウォッチドッグの配布および回収
- 選択された vPro グループへのヒューリスティック ワーム封じ込め情報の配布および回収

ドリル ダウンしてグループ内の個々のデバイスを管理するには、テーブルの [説明] 列の下にあるグループ名のリンクをクリックします。[デバイス管理] ウィンドウが開き、選択されたグループに属するデバイスの一覧が表示されます。グループ内の複数のデバイスまたは個々のデバイスを管理できます。「デバイスの管理」を参照してください。

詳細については、『HPCA Out of Band Management ユーザー ガイド』の「Group Management」の章を参照してください。

警告の通知

vPro デバイスの場合、デバイスに警告のサブスクリプションを割り当てていれば、プロビジョニング済みの vPro デバイスによって生成された警告を表示できます。警告の通知を監視すると、ネットワーク上のデバイスの状態についての適切な情報が得られます。

詳細については、『HPCA Out of Band Management ユーザー ガイド』の「Alert Notification」の章を参照してください。

パッチ管理

パッチ管理オペレーション タスクは、次のセクションで説明します。

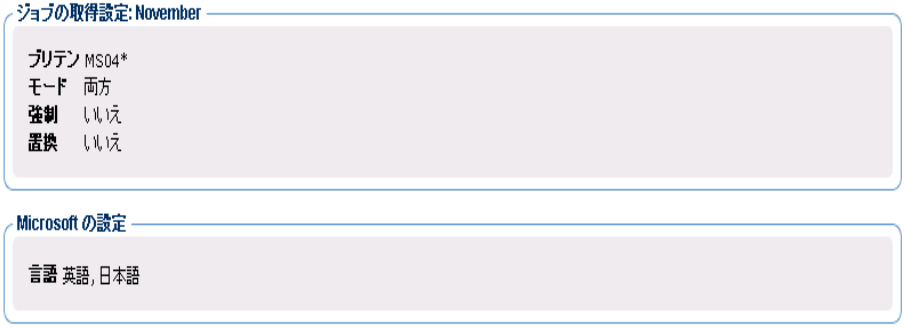
- 取得を開始 241 ページ
- 同期を実行 243 ページ
- エージェントの更新を表示 244 ページ
- 取得履歴を表示 247 ページ
- ログを表示 247 ページ
- デバイスを削除 247 ページ
- ゲートウェイ設定 248 ページ

取得を開始

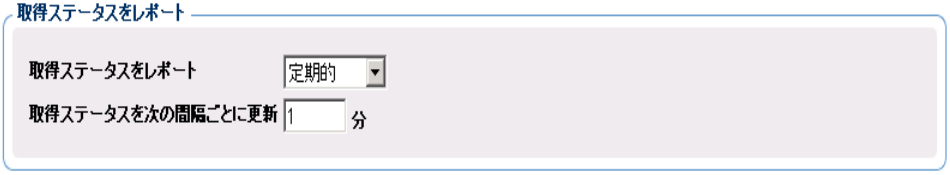
1 [オペレーション] で、**[パッチ管理]** を展開し、**[取得を開始]** をクリックします。

2 名前をクリックして、ファイルを選択します。

3 この取得の設定を確認します。



取得ステータスをレポート



- **取得ステータスをレポート**: 取得ログ以外に、取得ジョブを表示したときに表示される現在の取得ステータスを更新する頻度を指定できます。
- **取得ステータスを次の間隔ごとに更新**: [取得ステータスをレポート] フィールドで **[定期的]** を指定した場合は、ステータス ファイルを更新する頻度を選択します。

4 エージェント アップデート設定の注意を読み、**[サブミット]** をクリックして取得を開始します。

取得のステータスをチェックするには

- パッチ取得レポートを表示するには、[レポート] タブを使用します。
- [オペレーション] タブの [パッチ管理] 領域を使用して、**取得ジョブ**を表示します。

- また、[オペレーション] タブの [パッチ管理] 領域を使用して **[ログを表示]** ページにアクセスし、`patch-acquire.log` を選択します。

同期を実行

HPCA Configuration Server DB に送信されたパッチ情報は、評価と分析のために Patch SQL データベースと同期する必要があります。HPCA Configuration Server DB と Patch SQL データベースには、同期されるクラスとインスタンスのセットの同じ情報が格納されます。

- PATCHMGR ドメイン内の各クラスは、Patch SQL データベース内のテーブルになります。対応するテーブルは、nvd_classname という名前です。
- 各クラスの各属性は、そのテーブルの列になります。対応する列名は nvd_attributename です。式と接続変数は複製されません。
- クラスの各インスタンスは、対応するテーブルのレコードになります。

この同期は、パッチ取得後、および通常の HPCA オペレーションで自動的に実行されます。

ただし、手動で同期を実行するように指示される場合があります。たとえば、別の HPCA Server からパッチ情報をインポートした後は、手動でデータベースを同期します。また、ある程度取得を実行した後でパッチ管理用に設定された SQL データベースを切り替える場合も、手動でデータベースを同期します。

データベースは、HPCA Core Console を使用して手動で同期できます。

を使用してデータベースを同期するには

1 [オペレーション] タブから、**[パッチ管理]** タスクを展開し、**[同期を実行]** をクリックします。

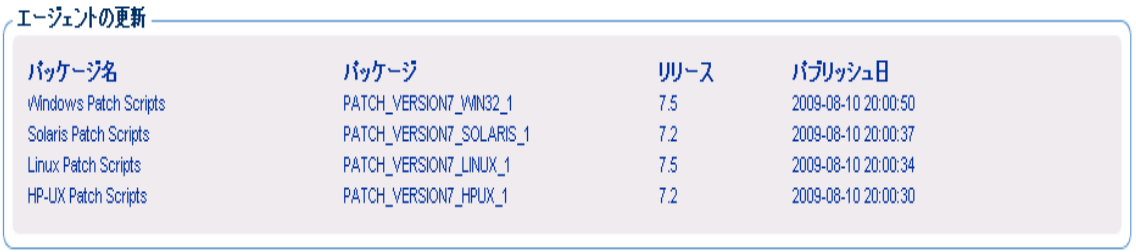
2 **[サブミット]** をクリックします。

エージェントの更新を表示

パッチの取得を実行するときに、最新バージョンと Patch Agent ファイルの更新情報もダウンロードできます。Patch Agent ファイルには、製品の検出と管理を実行するためのスクリプトが含まれています。これらのファイルは、HP が提供するパッチ更新の Web サイトで受信します。ダウンロードした後、ファイルは PATCHMGR ドメインにパブリッシュされ、DISCOVER_PATCH サービス インスタンスに接続されます。

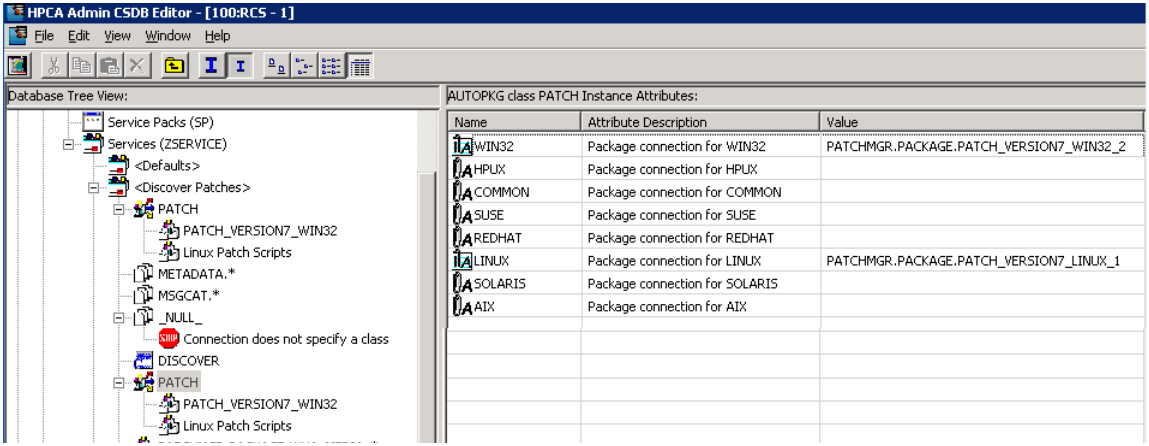
更新のステータスを確認するには、[エージェントの更新を表示] タスクを使用します。[エージェントの更新を表示] は、HPCA Core Console で [オペレーション] タブの [パッチ管理] 領域からアクセスします。これを実行するには、**[エージェントの更新を表示]** をクリックします。

図 44　エージェントの更新を表示



エージェント ファイルは、DISCOVER_PATCH サービスが Patch Manager ターゲットデバイスで処理されるときに配布されます。これは、DISCOVER_PATCH サービスで、AUTOPKG クラスの PATCH インスタンスに接続することによって実現します。同様に、AUTOPKG.PATCH インスタンスは、**[パブリッシュ]** または **[パブリッシュと配布]** を選択したときに作成されたエージェントのメンテナンス パッケージに接続します。パブリッシュのみを選択した (配布を選択しなかった) 場合は、PACKAGE クラスの適切なインスタンスから AUTOPKG.PATCH インスタンスへの接続を作成する必要があります。これには Admin CSDB Editor を使用します。例は次のとおりです。

図 45　パブリッシュされたパッケージへの接続の作成



AIX、HP-UX、および Solaris は現在サポートされていません。

[HP OVCM Patch Agent の更新] には以下の値があります。

- **なし**：エージェントの更新は PATCHMGR ドメインにパブリッシュされません。
- **パブリッシュと配布**：これはデフォルトの値です。更新を PATCHMGR ドメインにパブリッシュし、それらを DISCOVER_PATCH インスタンスに接続して、更新を Patch Manager の管理対象デバイスに配布します。
- **パブリッシュ**：更新は PATCHMGR ドメインにパブリッシュされますが、Patch Manager の管理対象デバイスへの配布のために接続されることはありません。これらの接続は作成する必要があります。

ダウンロードを更新するエージェントの制御のために次の 2 つのパラメータがあります。

- **オペレーティング システム**：エージェント更新を取得するオペレーティング システムを指定します。デフォルトは、すべてのオペレーティング システムをダウンロードするものです。有効な値は、**Windows** と **Linux** です。

- **バージョン**：エージェントの更新を取得する Patch Manager のバージョンを選択します。Configuration Server には 1 つのバージョンのみをパブリッシュできます。1 つの Configuration Server が複数のバージョンのエージェントをホストすることはできません。その場合は、もう 1 つのバージョン用に別の Configuration Server を作成してください。

最初にインストールした Patch Manager、または現在実装されている Patch Manager より低いバージョンのエージェントは絶対に選択しないでください。

現在のバージョンに更新するには、**[バージョン 7]** を指定します。新しい Patch Manager 7.50 インストールでは、これがデフォルトです。

を使用して **[パブリッシュと配布]** オプションを設定し、[エージェントの更新] を **[バージョン 7]** に設定することをお勧めします。これにより、Windows と Linux の Patch Agent をバージョン 7.50 に正常に移行できます。これは、Microsoft が新しい Microsoft Update Catalog フィードを優先して、`MSSecure.xml` への更新を打ち切った場合に、Microsoft セキュリティ パッチの管理を継続するために必要です。

Microsoft Update からパッチを取得する場合、レポートの [ソース] 列には「Microsoft」ではなく「Microsoft Update」と表示されるため注意してください。

Microsoft Update テクノロジを利用するには、ターゲット デバイスに Windows Update Agent をインストールする必要があります。Patch Manager の取得プロセスでは、Microsoft Update Catalog テクノロジを利用する際、脆弱性のスキャンとパッチの適用に必要な最新の Windows Update Agent を自動的に取得します。DISCOVER_PATCH サービスは、次のエージェント接続で最新の Windows Update Agent を自動的に管理対象デバイスに適用します。

Windows Update Agent (**WUA**) は Windows の自動更新サービスを使用します。これは、ターゲット デバイスで **[自動]** または **[手動]** のいずれかに設定する必要があります。自動更新サービスは、WUA が必要に応じて起動するため、停止状態の場合があります。

取得履歴を表示

以前の取得の詳細を表示するには、パッチ取得ステータス ページを選択します。

ログを表示

Patch Manager Server ログを使用して、パッチ管理環境を確認したり、トラブルシューティングしたりすることができます。これらのログは、[オペレーション] タブと [パッチ管理] 領域を使用して、コンソールからオンラインで使用できます。

コンソールから、**[オペレーション]** タブをクリックし、**[パッチ管理]** タスクを展開します。**[ログを表示]** をクリックします。

表示されているリストからログ ファイルを選択して開き、そのファイルをオンラインで確認するか、またはローカルに保存して後で HP サポートを利用して確認します。

- **`HPCA-PATCH-3467.log`** Patch Manager Server のログです。
- **`patch_acquire.log`** パッチ取得のログです。
- **`patch-sync.log`** Patch Manager Database と Configuration Server Database の間の同期のログです。
- **`httpd-3467.yy.mm.dd.log`** Patch Manager Server の Web サーバー アクセス ログです。このログは、だれがサーバーにアクセスしているか、Web サービスまたはコンソール インターフェイスのどちらを経由しているか、および実行されたアクセスの回数を示します。

これらのログは、Patch Manager Server インストール ディレクトリの `\logs` フォルダにあります。

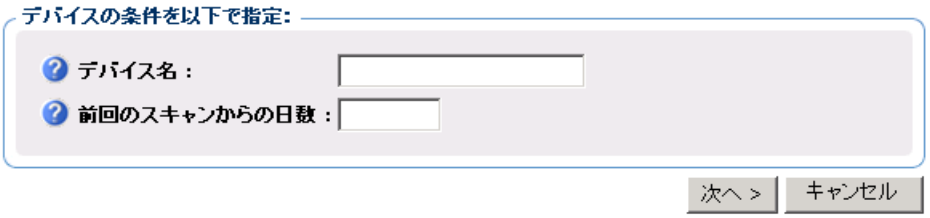
デバイスを削除

コンソールの [オペレーション] タブを使用して、特定のデバイスの Patch Manager 適用状況データを削除できます。

Patch Manager ODBC データベースから適用状況データを削除するには

1 **[オペレーション]** タブをクリックし、**[パッチ管理]** タスクを展開します。

2 **[デバイスを削除]** をクリックします。



3 削除するデバイスのデバイス選択条件を指定します。以下のように行います。

- カンマ区切りのリストで、1 つまたは複数のデバイスを指定します。
- ワイルドカードを使用します。
- そのデバイスで前回の脆弱性スキャンが実行された後の経過日数を指定します。これは、Patch Manager Infrastructure コンポーネントに適合性データをレポートしなくなったデバイスの適合性情報を削除するために使用されます。

4 **[次へ]** をクリックします。コンソールでは、データベースからデバイスを削除する前に、選択フィルタに一致するデバイスをプレビューできます。

5 Patch Manager ODBC データベースからデバイスを削除するには、**[削除]** をクリックします。

> このデータベースからデバイスを削除する場合は注意してください。この操作は元に戻せません。

ゲートウェイ設定

Patch Manager ゲートウェイは、**[パッチ管理] > [配布設定]** ページで **[パッチ メタデータのダウンロード]** オプションが有効になっているときに、パッチ バイナリ ファイルを取得してキャッシュするために使用されます。[パッチ メタデータのダウンロード] オプションは、Microsoft Update Catalog データ フィードを使用して Microsoft デバイスにパッチを適用する場合にのみ使用できます。

[オペレーション] タブの [パッチ管理] > [ゲートウェイ設定] 領域では、ゲートウェイに保存されているパッチ ファイルのキャッシュを確認したり管理したりすることができます。

プレロード ゲートウェイ オプション

- プレロード ゲートウェイ オプションが無効になっている場合、ゲートウェイは、エージェントからリクエストされた時点でパッチ ファイルをキャッシュします。これがデフォルトであり、この設定をお勧めします。
- プレロード ゲートウェイ オプションが有効になっている場合、ゲートウェイは、パッチが取得された時点でパッチ ファイルをキャッシュします。

コンソール の 領域では、次のゲートウェイ オペレーションを実行できます。

- キャッシュの統計値の表示 249 ページ
- キャッシュコンテンツの詳細 250 ページ
- URL リクエストのエクスポート 250 ページ
- URL リクエストのインポート 251 ページ

キャッシュの統計値の表示

現在ゲートウェイにキャッシュされているパッチ ファイルに関する統計、およびゲートウェイがエージェントのパッチ リクエストをどれだけ満たしているかを測定できるヒット、不足、エラー情報を表示するには、[キャッシュの統計値の表示] ページを使用します。ヒット、不足、およびエラー情報のカウンタはリセットできます。

[キャッシュの統計値の表示] ページにアクセスするには

- コンソールの **[オペレーション]** タブから、**[パッチ管理] > [ゲートウェイ設定] > [キャッシュの統計値の表示]** を選択します。

ゲートウェイ キャッシュの統計値

- **合計キャッシュ サイズ**: ゲートウェイ キャッシュ内のすべてのパッチの合計サイズ (MB)。

  キャッシュ サイズが、[パッチ配布設定] ページの [パッチ ゲートウェイ オペレーション] で設定されている [最大キャッシュ サイズ] を超えた場合は、最も使用頻度の低い、古いパッチが削除されます。
- **ファイル数**: パッチ ゲートウェイ キャッシュのダウンロードできるアクティブなファイルの数。
- **ヒットしたキャッシュ**: 前回のカウンタ リセット以降に対応したリクエストの数。
- **不明キャッシュ**: 前回のカウンタ リセット以降にベンダーからのダウンロードを必要としたリクエストの数。

- **キャッシュダウンロードエラー**: 前回のカウンタ リセット以降にゲートウェイで検出されたダウンロードエラーの数。エラー情報は、HPCA-PATCH-3467.log ファイルにあります。
- **ヒット率**: 全リクエスト数のうち、キャッシュで対応したリクエストの割合。
- **キャッシュ カウンタ リセット日時**: キャッシュ カウンタの統計値がリセットされた日付と時刻。
- **リセットされたキャッシュカウンタの統計値**: このエントリをクリックすると、ヒットしたキャッシュ、不明キャッシュ、およびキャッシュ ダウンロード エラーのカウンタがリセットされます。

キャッシュコンテンツの詳細

ゲートウェイにキャッシュされているパッチ バイナリ ファイルの現在のセット (ブリテン番号単位) を表示するには、[キャッシュ コンテンツの詳細] ページを使用します。

[キャッシュの統計値の表示] ページにアクセスするには

- コンソールの **[オペレーション]** タブから、**[パッチ管理] > [ゲートウェイ設定] > [キャッシュ ファイルの統計値]** を選択します。

キャッシュ コンテンツの詳細の表示

[キャッシュ コンテンツの詳細] ページには、キャッシュされたブリテンが番号単位で表示されます。特定のブリテンでキャッシュされたバイナリのリストを表示するには、そのブリテン番号をクリックします。さらに詳細な情報を表示するには、バイナリ ファイルをダブルクリックします。

URL リクエストのエクスポート

ゲートウェイ サーバーがベンダーのダウンロード サイトに接続できない場合は、これらの未対応のエージェント リクエスト ファイルをエクスポートし、インターネットに接続された別のゲートウェイ サーバーにインポートできます。

[URL リクエストのエクスポート] オペレーションを使用すると、未対応の URL リクエストのリストを表示およびフィルタし、そのリストを別のパッチ サーバーにインポートできます。

URL をエクスポートすると、任意の名前を付けた XML ファイルとして、それらのコンテンツを保存するよう求められます。この XML ファイルには、エクスポート中に選択されたパッチ URL が含まれます。

[URL リクエストのエクスポート] ページにアクセスするには

- コンソールの **[オペレーション]** タブから、**[パッチ管理] > [ゲートウェイ設定] > [URL リクエストのエクスポート]** を選択します。

未対応の URL リクエストのリストをエクスポートするには

1 [表示設定のリスト] 領域を使用して、未対応のリストにフィルタを適用し、エクスポートするリストを絞り込みます。

表示設定のリスト

すべての未対応パッチ リクエストのリストを URL 名でフィルタするには、**[URL フィルタの式]** を入力します。ワイルドカードを指定できます。**[適用]** をクリックして、フィルタを適用します。

1 ページに含める URL リストの数を設定するには、**[ページ数]** ドロップダウンを使用します。

URL の完全なリストに戻すには、エントリを * にリセットし、**[適用]** をクリックします。

このページに未対応の URL リクエストが表示されている場合は、[サブミット] をクリックして、現在未対応のリクエストのエクスポート ファイルをダウンロードします。

URL リクエストのインポート

[URL リクエストのエクスポート] オペレーションからエクスポートされた URL は、[URL リクエストのインポート] ページを使用して、別のパッチ ゲートウェイ サーバーにインポートできます。インポートされたファイルはパッチ ゲートウェイに格納され、そのゲートウェイ サーバーでのみ使用できます。

[URL リクエストのエクスポート] ページにアクセスするには

- コンソールの **[オペレーション]** タブから、**[パッチ管理] > [ゲートウェイ設定] > [URL リクエストのインポート]** を選択します。

URL リクエストをインポートするには

1 URL リクエストをインポートするゲートウェイのローカルドライブに [URL リクエストのエクスポート] タスクの使用後に保存されたファイルをコピーします。

2 **[インポートするリクエスト ファイル]** 領域で、**[ブラウズ]** をクリックして、[URL リクエストのエクスポート] タスクで保存された xml ファイルを見つけます。

3 指定したファイルへの未対応リクエストのインポートを開始するには、**[サブミット]** をクリックします。

[ゲートウェイ URL リクエストのインポート] ページには、インポートされる URL、完了ステータス、および完了のパーセンテージが表示されます。

OS 管理

オペレーティング システムの配布のために CD または DVD に保存できるイメージをダウンロードするには、[OS 管理] の [「CD 配布」] 領域を使用します。

CD 配布

CD 配布機能を使用すると、オペレーティング システムの配布のために CD または DVD に保存できるイメージをダウンロードできます。

[OS ライブラリ] リストには、CA サーバーにパブリッシュされたすべてのオペレーティング システム イメージが表示されます。

CD 配布用のサービスをダウンロードするには

1 [オペレーション] タブで、**[OS 管理] > [CD 配布]** に移動します。

2 [OS ライブラリ] リストから、ダウンロードするサービスを選択します。

3 CD 配布ウィザードを起動するには、**[CD 配布メディアの作成]** アイコンをクリックします。

4 要約情報を確認し、**[ダウンロード]** をクリックします。サービスのダウンロードがバックグラウンドで開始されます。

5 **[閉じる]** をクリックします。

6 ダウンロードの進行状況が [OS ライブラリ] リストに表示されます。各サービスの現在のステータスを [CD 作成ステータス] 列に表示するには、**[リフレッシュ]** アイコンをクリックします。

   完了すると、各サービスはデフォルトで次のディレクトリに格納されます。

   ```
   C:\Program Files\Hewlett-Packard\HPCA\Data\ServiceDecks\CDDeployment
   ```

   このディレクトリが空の場合は、リストにあるすべてのサービスの [CD 作成ステータス] が空白です。

この機能は、通常は複数のイメージを格納するために、DVD で使用するためのものです。複数の CD-ROM または DVD-ROM を同時に使用して、リソースをスパンしないでください。

CD-ROM または DVD-ROM は Joliet 形式である必要があります。

8 設定

[設定] 領域では、コンソールへのユーザー アクセスの管理、インフラストラクチャ サーバーの定義と設定、パッチ取得のスケジュールと設定の管理、ハードウェアの管理、および ODBC の設定を行うことができます。

[設定] タブは、管理者ロール グループに属しているゾーン アカウントを持つ Enterprise ライセンス ユーザーのみ使用できます。

[設定] タブの左側にあるナビゲーション領域のリンクを使用して、さまざまな設定オプションにアクセスします。これらのオプションについては、次のセクションで説明します。

Core の設定オプション

- ライセンス 254 ページ
- Core コンソールのアクセス制御 255 ページ
- インフラストラクチャ管理 263 ページ
- デバイス管理 284 ページ
- パッチ管理 287 ページ
- アウトバンド管理 314 ページ
- OS 管理 317 ページ
- ダッシュボード 318 ページ

Satellite の設定オプション

- ライセンス 254 ページ
- アップストリーム ホスト 254 ページ
- SSL 264 ページ
- Satellite コンソールのアクセス制御 259 ページ
- 設定 261 ページ

- データ キャッシュ 261 ページ
- ポリシー 265 ページ
- OS 管理 317 ページ
- シン クライアント 285 ページ
- マルチキャスト 280 ページ

ライセンス

機能的な HPCA 環境を実現するには、HP によって発行された有効なライセンスが必要です。コンソールのこの領域でライセンス ファイルが保存され、インストールされているライセンスのエディション (Starter、Standard、または Enterprise) が表示されます。このセクションを使用して HPCA ライセンスを確認および更新することもできます。

新しいライセンスを適用するには

1 新しい `license.nvd` ファイルからライセンス情報をコピーして、**[ライセンス データ]** テキスト ボックスに貼り付けます。

> ライセンス ファイルからライセンス情報をコピーする場合、`[MGR_LICENSE]` という行より前のテキストは含めないでください。含めた場合、ライセンス情報がコンソールから読み取れなくなります。

2 **[保存]** をクリックします。更新されたライセンス情報が、**[現在のライセンス]** の後に表示されます。

アップストリーム ホスト

アップストリーム ホスト サーバーの情報を編集するには、Satellite コンソールの [設定] タブにある **[アップストリーム ホスト]** 領域を使用します。アップストリーム サーバーは、この Satellite が同期を取り、サービスが無効またはリソースが使用不可の場合にリクエストの情報をフェッチするサーバーです。このサーバー間通信には SSL を使用できますが、使用するには、アップストリーム サーバーが SSL リクエストを受信できる必要があります。

アクセス制御

このパネルの管理制御は、Core コンソールと Satellite コンソールで異なります。

HPCA Starter および Standard ライセンス エディションでは、Satellite コンソールは提供されません。

- HPCA 管理者は、Core コンソールのアクセス制御を使用してコンソールへのユーザー アクセスを設定および管理できます。255 ページの「Core コンソールのアクセス制御」を参照してください。
- HPCA 管理者は、Satellite コンソールのアクセス制御を使用して認証メソッドを選択および設定できます。259 ページの「Satellite コンソールのアクセス制御」を参照してください。

Core コンソールのアクセス制御

[アクセス制御] セクションを使用して、一意のカスタム ID とパスワードを持つコンソール **ユーザー** (255 ページの「[ユーザー] パネル」を参照) のインスタンスを作成します。次に、**ロール** (258 ページの「[ロール] パネル」を参照) をユーザーに割り当てて、ユーザーがアクセスできるコンソールの領域と許可されている管理タスクを管理します。

[ユーザー] パネル

[ユーザー] パネルで、ユーザー インスタンスを作成してロールを各インスタンスに割り当てます。ロールによって、各ユーザーがアクセスできるコンソールの領域が決まります。ユーザーを削除したり、そのロールを変更したりできます。

管理ジョブには、ジョブを作成するため使用されたユーザー ID を表示する、[作成者] フィールドがあります。表示されるユーザー ID は、この領域で作成されたユーザー ID です。

- デフォルトでは、インストール後のデフォルトのコンソール ユーザーは **admin** の 1 人だけで、デフォルトのパスワードは **secret** です。この「フェイルセーフ」ユーザー アカウントにはコンソールへの完全なアクセス権があり、削除できません。
- HPCA Console ユーザーは、次で説明するように**内部**または**外部**のいずれかになります。

— **内部ユーザー**
[ユーザー] パネルで作成するユーザーは、すべて「内部」ユーザーとして作成されます。これらのユーザーは、Core コンソールを使用して削除および更新できます。

— **外部ユーザー**
Enterprise エディションの場合、HPCA 管理者は外部ディレクトリ (LDAP や Active Directory など) を使用してユーザーを追加したり、アクセスのパーミッションや認証情報を設定したりできます。これらの「外部」ユーザーは、Core コンソールでは作成、削除、または更新できません。これを行うには、管理者は LDAP/AD ツールを使用する必要があります。ただし、HPCA 管理者は認証用のディレクトリ ソースを設定できます。このソースは [ユーザー] パネルに表示されます。[ソース] カラムでは、ユーザーの取得元のディレクトリが参照されます。

- 現在アクティブなユーザーも削除できません。現在アクティブなユーザーを削除するには、ログアウトして、別のユーザーとしてログインしなおす必要があります。これで、以前にアクティブだったユーザーを削除できます。

次のセクションでは、[ユーザー] パネルで実行できる管理タスクの詳細について説明します。

コンソール ユーザーを作成するには

1 **[新しいユーザーの作成]** ボタン  をクリックして、ユーザー作成ウィザードを起動します。

2 ウィザードの手順に従って、コンソール ユーザーを追加します。

ユーザー ID の考慮事項

ユーザー ID には、スペース、スラッシュ (/)、またはバックスラッシュ (\) を含めることはできません。

- スペースまたはバックスラッシュが含まれている場合、「作成できません」というエラー メッセージが表示されます。
- スラッシュが含まれている場合、ユーザー ID が生成されるときに自動的に削除されます。たとえば、ユーザー ID が **`jdoe/1`** の場合、`jdoe1` になります。

パスワードの考慮事項

- パスワードの作成時は、ASCII 文字のみを使用してください。
- 現在のユーザーのパスワードを変更する場合、自動的にログアウトされます。そのユーザーとして新しいパスワードでログインします。

3 ユーザーを作成すると、次のことが可能になります。

— 別のユーザーを作成する (このセクションの手順 1 を参照)。

— ユーザー ID をクリックしてユーザーのプロパティを表示および変更する (次のセクションを参照)。

— ユーザーにロールを割り当てる (このセクションの 258 ページの「[ロール] パネル」を参照)。

ユーザーのプロパティを表示および変更するには

このセクションの手順は「内部」ユーザーにのみ該当します。「外部」ユーザーのプロパティは Core コンソールでは変更できません。

1 内部ユーザーのユーザー ID をクリックして、そのプロパティを表示します。

2 [ユーザー プロパティ] ウィンドウで表示名や説明などのユーザーのプロパティを変更して、[パスワードの変更] ウィンドウにアクセスします。

3 **[保存]** をクリックし、変更を確定して保存します。

4 これにより、次のことが可能になります。

— 別のユーザーを作成する (前のセクションの手順 1 を参照)

— 別のユーザー ID をクリックしてそのプロパティを表示および変更する (このセクションの手順 1 を参照)

— ユーザーにロールを割り当てる (このセクションの 258 ページの「[ロール] パネル」を参照)。

コンソール ユーザーを削除するには

このセクションの手順は「内部」ユーザーにのみ該当します。「外部」ユーザーのプロパティは Core コンソールでは変更できません。

- リストからユーザー ID を選択して、**[ユーザーの削除]**  をクリックします。

現在のユーザーは削除できません。
このユーザー ID を削除するには、ログアウトして、別の管理者としてログインしなおしてから削除を実行する必要があります。

[ロール] パネル

さまざまなレベルの管理者権限 (**ロール**) をユーザーに割り当てることができます。ユーザーに付与するアクセスおよび管理のパーミッションに基づいて、ロールをユーザーに割り当てます。コンソール ユーザーのロールは次のとおりです。

- **管理者**: このユーザーには Core コンソールへの無制限のアクセス権限があり、すべての管理機能を実行できます。これは、「スーパーセット」ロールで、オペレータ ロールとレポータ ロールのすべての機能と権限が含まれています。
- **オペレータ** : このユーザーは、Core コンソールで管理タスク、操作タスク、およびレポート関連タスクを実行できます。このユーザーは [設定] タブにはアクセスできません。このロールには、レポータ ロールの機能と権限が含まれています。
- **レポータ** : このユーザーのパーミッションでは、Core コンソールでレポートデータの表示、コンパイル、および印刷のみを行うことができます。このユーザーは、[レポート] タブと [ダッシュボード] タブにのみアクセスできます。

ユーザーには複数のロールを割り当てることができます。

ユーザーへのロールの割り当て

コンソールでは、次の 2 つのいずれかの方法で、ユーザーにロールを割り当てることができます。

- [ロール] パネルで、次の手順を実行します。
  a テーブルのロールをクリックして [ロール プロパティ] ウィンドウを呼び出します。このウィンドウには、該当のロールに割り当てられているユーザーのリストが表示されます。
  b ツールバーのボタンを使用して、ユーザーをロールに追加したり、ユーザーをロールから削除したりします。
- [ユーザー] パネルで、次の手順を実行します。
  a テーブルのユーザー ID をクリックして [ユーザー プロパティ] ウィンドウを呼び出します。
  b [ロール] タブをクリックします。
  c ツールバーのボタンを使用して、ユーザーをロールに追加したり、ユーザーをロールから削除したりします。

Satellite コンソールのアクセス制御

HPCA 管理者は、Satellite コンソールの [アクセス制御] セクションで、コンソールのアクセス認証メソッド (**ローカル アカウント**または**ディレクトリ サービス アカウント**) を選択してその設定を行うことができます。

[アクセス制御] セクションの [要約] 領域には、現在有効になっている認証メソッドが表示されます。デフォルト (ローカル アカウント) が表示されます。

認証メソッドを選択および設定するには

1 **[認証の設定]** をクリックします。認証ウィザードが開きます。

2 [サーバー認証タイプの設定] 領域で、[認証メソッド] ドロップダウンを使用して次のいずれかを選択します。

— **ローカル アカウント** – このメソッドでは、管理者は Satellite コンソールの管理者 および*オペレータ* ログオン認証情報を設定できます。これらの認証情報によって、コンソールのさまざまな部分へのアクセスが制限されます。これがデフォルトとなります。設定情報については、259 ページの「ローカル アカウントを使用するには」セクションを参照してください。

— **ディレクトリ サービス アカウント** – このメソッドでは、環境内のディレクトリ サービス アカウント (Active Directory など) を使用して管理者認証ができます。設定情報については、260 ページの「ディレクトリ サービス アカウントを使用するには」を参照してください。

3 **[次へ]** をクリックして [設定] 領域に進み、選択したアクセス メソッドの設定を指定します。

ローカル アカウントを使用するには

ローカル アカウントを使用して Satellite コンソールへのアクセスの安全性を確保する場合、Satellite サーバーをインストールしたらすぐにパスワードを変更します。

パスワードの考慮事項

- パスワードの作成時は、ASCII 文字のみを使用してください。
- 現在のユーザーのパスワードを変更する場合、自動的にログアウトされます。そのユーザーとして新しいパスワードでログインします。

a 適切な領域で管理者またはオペレータのコンソールへのアクセスを設定します。

- **管理者**のパーミッションでは、ユーザーはコンソールのすべての領域にアクセスできます。
- **オペレータ**のパーミッションでは、ユーザーのアクセスはコンソールの [操作] 領域に制限されます。

b **[次へ]** をクリックします。

c 設定が完了したら、**[閉じる]** をクリックします。

次にローカル アカウントを使用して Satellite コンソールにログインするときには、新しいパスワードを使用します。

ディレクトリ サービス アカウントを使用するには

外部ディレクトリ サービス アカウントを使用して、Satellite コンソールへのユーザー アクセスを認証できます。

a [ディレクトリ サービスの設定] 領域で、次の設定パラメータを指定します。

- **ディレクトリ ホスト**: 認証に使用する外部ディレクトリ サーバーのホスト名または IP アドレスです。
- **ディレクトリ ポート**: 外部ディレクトリ サーバーにアクセスするために使用するポートです。デフォルトは 389 です。
- **ベース DN**: ユーザーのクエリ時に検索を開始するディレクトリのベース オブジェクトです。

  たとえば、`dc=europe,dc=acme,dc=com` のようになります。
- **アクセス グループ DN**: 管理者権限で Core コンソールにアクセスできるすべてのメンバーを含むグループ DN です。
- **ディレクトリ ユーザー ID**:ディレクトリ サーバーにアクセスできる有効なユーザー ID です。Core にログオンするユーザーが上記のグループ DN のメンバーであることを検証するために使用されます。デフォルトは administrator です。
- **ディレクトリ パスワード**: 上記のユーザー ID に関連付けられているパスワードです。

b [LDAP グループ ユーザーのテスト] 領域で、テスト ユーザーの認証情報を入力します。

テスト ユーザーは、上記で指定されているアクセス グループ DN のメンバーである必要があります。

このテストで、ディレクトリ サービス アカウントの設定後にこのサーバーにアクセスできることを確認できます。

– **ユーザー名** : 既存のアクセス グループ DN ユーザーのユーザー名です。

– **パスワード**: 上記のユーザー名に関連付けられているパスワードです。

c **[次へ]** をクリックします。

d 設定が完了したら、**[閉じる]** をクリックします。

これで管理者は、ディレクトリ サービス アカウントの認証情報を使用して Satellite コンソールにサインインできます。

設定

[設定] 領域は Satellite コンソールでのみ使用できます。

設定サービスは、それぞれのエンタイトルメントに基づき、HPCA Agent に「モデル」とサービス情報を提供します。エージェントはサーバーに接続して、この情報を取得し、変更内容を反映させます。このサービスが Satellite サーバーで無効になっている場合、HPCA Agent は別のサーバーを使用して、リクエストした情報を取得する必要があります。この「フォールバック サーバー」の指定は、Configuration Server Database の CLIENT.SAP インスタンスに設定されているユーザーのインフラストラクチャ モデルに組み込む必要があります。

- 設定サービスを有効にするには、**[有効]** チェック ボックスをオンにして **[保存]** をクリックします。

データ キャッシュ

[データ キャッシュ] 領域は Satellite コンソールでのみ使用できます。

データ キャッシュ サービスは、基本となる HPCA キャッシュ管理サービスを制御します。HPCA キャッシュ管理サービスは、Satellite が同期されているアップストリーム ホストからデータ (ソフトウェア、パッチ、セキュリティ、および監査など) を取得するために使用されます。このページでは、次のことができます。

- この Satellite のデータ キャッシュ サービスを有効または無効にする。
- リソース データ キャッシュの制限をメガバイト単位で設定する。

Satellite Server のデータをキャッシュおよび同期するには、まず Satellite を設定する必要があります。詳細については、『HPCA Core および Satellite 入門およびコンセプト ガイド』を参照してください。

データ キャッシュを設定するには

1 [設定] タブで、**[データ キャッシュ]** をクリックします。

2 次のオプションを設定します。

— **[有効]** (チェック ボックスがオン) は、データ サービスがこの Satellite で有効になっていることを示します。これはデフォルトで、これによって、この Satellite に接続されている HPCA Agent が Satellite からソフトウェアやパッチを受信できるようになります。

— **[有効]** (チェック ボックスがオフ、つまり **無効**) は、データ サービスがこの Satellite で無効になっていることを示します。

– アップストリーム ホストと同期しても、ソフトウェアやパッチのデータ キャッシュはこの Satellite に送信されません。

– この Satellite に接続されている HPCA Agent によって、データのリクエストがアップストリーム ホストに渡されます。

— **[データ キャッシュの制限 (MB)]** をリソース キャッシュの最大サイズ (メガバイト) に設定します。デフォルトは 40000 MB です。

3 [**保存**] をクリックして、変更内容を実装します。

[操作] タブがリフレッシュされると、このサービスのステータスが [要約] の下に表示されます。

インフラストラクチャ管理

[インフラストラクチャ管理] セクションでは、HPCA インフラストラクチャのさまざまな設定を行うことができます。詳細については、次のセクションを参照してください。

プロキシ設定

HPCA Core Server と外部のデータ ソースまたは受信者間の、インターネットベースの通信に使用するプロキシ サーバーの設定を指定するには、[プロキシ設定] 設定ページを使用します。

HTTP 通信と FTP 通信で別々のプロキシ設定を確立できます。HTTP プロキシ サーバーは、Patch Manager の取得、HP Live Network のコンテンツの更新、および特定のダッシュボード ペインで使用される Real Simple Syndication (RSS) フィードに使用されます。これらの HTTP プロキシ設定がないと、たとえば Patch Manager の取得が失敗した場合に、ブリテン、パッチ、および Windows Update Agent (WUA) ファイルなどの関連項目をダウンロードできなくなります。

FTP プロキシ サーバーは、HP Softpaq 取得を実行するために Patch Manager によって使用されます。

プロキシを設定するには

1 [設定] タブで、[インフラストラクチャ管理] 領域を展開し、**[プロキシ設定]** をクリックします。

2 設定するプロキシ サーバーのタブ (**[HTTP]** または **[FTP]**) を選択します。

3 **[有効]** ボックスをオンにします。

4 プロキシ サーバーに関する次の情報を入力します。

- **ホスト**: プロキシ サーバーのネットワーク アドレスの名前
- **ポート**: プロキシ サーバーがリスンするポート
- **ユーザー ID**: プロキシ サーバーで認証が必要な場合のユーザー ID
- **パスワード**: プロキシ サーバーで認証が必要な場合のプロキシ ユーザーのパスワード

5 **[保存]** をクリックして、変更内容を実装します。

6 **[閉じる]** をクリックして、ダイアログを確認します。

SSL

SSL を有効にすると、Core コンソールへのアクセスが保護されます。SSL を有効にすると、コンソールに接続している間に作成されるトランザクションが暗号化されます。

SSL を有効にしてサーバーとクライアントの証明書を定義するには、[SSL] セクションを使用します。

- SSL サーバー 264 ページ
- SSL クライアント 265 ページ

SSL サーバー

SSL サーバーの証明書は、HPCA Server のホスト名に基づいています。これにより、サーバーで SSL 接続が許可されます。これは、Verisign など既知の認証局によって署名される必要があります。

HPCA Server の SSL の有効化および設定を行うには

1 **[SSL を有効化]** の後にあるチェック ボックスをオンにします。

2 **[既存の証明書を使用]** または **[新しい証明書のアップロード]** のいずれかを選択します。

3 **[保存]** をクリックします。

SSL クライアント

認証局のファイルには、信頼された認証局の署名入り証明書が含まれています。これにより、HPCA Server は他の SSL 対応サーバーに接続するときに SSL クライアントとして機能できます。サーバーのインストールには、信頼された認証機関のデフォルトのセットが含まれています。これはほとんどの組織において十分な権限を持ちます。

CA 証明書ファイルを定義するには

1 **[ブラウズ]** をクリックして移動し、CA 証明書ファイルを選択します。

2 この証明書ファイルを既存の証明書に追加するのか、または既存の証明書をこの新しいファイルで置き換えるのかを選択します。

3 **[保存]** をクリックします。

ポリシー

エンタイトルメント情報を含むディレクトリ サービスに HPCA Server から接続するには、ポリシーを有効にする必要があります。無効にすると、リクエストした情報がアップストリーム サーバーから取得されます。

このパネルでポリシーを設定すると、(設定を含む) ディレクトリ サービス インスタンス がディレクトリ サービスの HPCA リストに自動的に作成されます。これは、コンソールの [ディレクトリ サービス] パネルからアクセスできます。

認証などの追加機能のためにディレクトリ サービスのこのインスタンスを変更できますが、ポリシーのためにディレクトリ サービスを作成する必要はありません。

ポリシーの有効化および設定を行うには

1 [ポリシー設定] 領域で、**[有効]** を選択します (これにより、Policy Server サービスが開始します)。

2 次の設定パラメータを指定します。

ディレクトリ ホスト: 認証に使用する外部ディレクトリ サーバーの完全なマシンのホスト名または IP アドレスを指定します。

SSL を使用している場合は、このフィールドに IP アドレスを指定しないでください。SSL では、IP アドレスは検証されません。

ベース DN: 管理者権限で Core コンソールにアクセスできるすべてのメンバーを含むグループ DN を指定します。

ディレクトリ ポート: 外部ディレクトリ サーバーにアクセスするために使用するポートを指定します。デフォルトは 389 です。

ディレクトリ ユーザー名: ディレクトリ サーバーにアクセスできる有効なユーザー名を指定します。これは、Core にログオンするユーザーが上記のグループ DN のメンバーであることを検証するために使用されます。デフォルトは Administrator です。

ディレクトリ パスワード: 上記のユーザー名に関連付けられているパスワードを指定します。

3 **[保存]** をクリックします。

Core サーバーによって、外部ディレクトリ サービスへの接続が自動的にテストされます。

LDAP 接続のテストが成功すると、Core サーバーによってこのディレクトリ サービスに接続するための Portal のマウント ポイントが作成され、ポリシーに使用できるようになります。

4 外部ディレクトリへの接続が成功したら、[ポリシー] ページの下部で **[LDIF の生成]** をクリックします。

LDIF の生成

この領域では、HPCA ポリシー設定を使用したディレクトリ スキーマの更新に使用できる LDIF (LDAP Data Interchange Format) ファイルを生成できます。

このオプションをクリックすると、[ポリシー] ページで指定したポリシー設定を使用してカスタマイズした LDIF ファイルを保存できます。

上記のポリシー設定を保存してから LDIF ファイルを生成してください。

1 **[LDIF の生成]** をクリックします。
これにより、HPCA が外部 LDAP ディレクトリを使用するために必要な、カスタマイズしたスキーマの変更を含むファイルが作成されます。

2 表示メッセージに応じて、生成された LDIF ファイルを、選択したロケーションに保存します。

3 28 ページの「外部ポリシー ストアの実装」セクションの手順に従い、LDIF ファイルを使用してスキーマの変更を外部 LDAP ディレクトリに適用します。

データベース設定

Core サーバー オブジェクトの SQL および Oracle データベースへの ODBC 接続を設定するには、[データベース設定] を使用します。

前提条件

Core データベースを作成し、そのデータベースの ODBC 接続を定義する必要があります。詳細については、製品マニュアルのインストール手順を参照してください。

メッセージングを設定するには

1 [設定] タブで、**[インフラストラクチャ管理]**、**[データベース設定]** の順にクリックします。

2 次のオプションを設定します。

- **ODBC DSN**: Core データベースの DSN を選択します。
- **ODBC のユーザー ID**: DSN のユーザー ID を指定します。
- **ODBC のパスワード**: ODBC ユーザー ID に関連付けられているパスワードを指定します。
- サーバーのホスト: データベースをホストするサーバーの名前を指定します。
- **サーバーのポート**: サーバーのポート (デフォルトは 1433) を指定します。

3 **[保存]** をクリックします。

ディレクトリ サービス

ディレクトリ サービスは、次のように多くの操作に使用されます。

- Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) のコンテナおよびグループに基づくレポートの実行
- HPCA Enterprise Console の認証を可能にする外部 AD/LDAP ソースの有効化

- ポリシーの割り当て (ポリシーは、ユーザー、エージェント コンピュータ、または管理対象デバイスがアクセスできるサービスの指定です)
- OS 管理作業
- AD/LDAP ソースに基づくエージェントの通知

HP Client Automation では、次の 2 つの基本的なポリシーの使用パターンがサポートされています。

- **通常**のパターンでは、提供される外部 LDAP ディレクトリ (Active Directory など) に保存される (ソフトウェアやパッチなどの) ポリシーを管理できます。このポリシー ソースは、Configuration Server の解決を支援するために Policy Server によって使用されます。ディレクトリのポリシーは HPCA Enterprise Console によって管理されます。

  外部ディレクトリ サービスでポリシー管理を実行するには、まずスキーマを更新する必要があります。ポリシー用の外部ディレクトリを使用する環境の設定に関する詳細については、『HP Client Automation Policy Server インストールおよび設定ガイド (Policy Server ガイド)』を参照してください。

  このタイプのポリシーは、Portal の内部ディレクトリではサポートされていません。詳細については、『HP Client Automation Portal インストールおよび設定ガイド (Portal ガイド)』を参照してください。

- サポートされている他のポリシーの使用パターンは、**オペレーティング システム (OS) 管理**に関連しています。OS 管理のポリシーは、HPCA Management Portal (Portal) に内部的に保存されます。このケースでは、OS の解決をサポートするために、Configuration Server への操作インターフェイスが Portal によって提供されます。ポリシーの管理は、HPCA Enterprise Console の OS 管理機能を使用して行われます。詳細については、『HP Client Automation OS Manager System Administrator ガイド (OS Manager ガイド)』を参照してください。

  外部 LDAP ディレクトリでは、現在 OS 管理ポリシーがサポートされています。

関連トピック：

[ディレクトリ サービス] ページへの移動 269 ページ

Configuration Server ディレクトリ サービスへの接続の設定 272 ページ

外部ディレクトリ サービスへの接続の設定 273 ページ

[ディレクトリ サービス] ページへの移動

LDAP ポリシー管理を使用するには、まず接続先とする LDAP 環境を定義する必要があります。そのためには、ディレクトリ サービス オブジェクトを作成および設定する必要があります。

[ディレクトリ サービス] ページにアクセスするには、[設定] タブの左側にあるナビゲーション メニューの **[ディレクトリ サービス]** リンクをクリックします。

次の表は、[ディレクトリ サービス] ページで使用できるツールバーのボタンについて説明しています。これらのツールバー ボタンを使用すると、既存のディレクトリ サービスをすべて管理したり、新しいディレクトリ サービスを作成したりできます。

表 40　[ディレクトリ サービス] ツールバー ボタン

アイコン	ツールバー ボタンの名前	説明
	データのリフレッシュ	ディレクトリ サービスのリストをリフレッシュします。
	フィルタ入力の表示 / 非表示	フィルタ ツールバーを表示または非表示にするときに使用します。 テキスト文字列を使用してディレクトリ サービスのデータをフィルタすることも、検索に含める個別のディレクトリ サービスのカラムを選択して検索結果を絞り込むこともできます。
	新しいディレクトリ サービス	ディレクトリ サービスの作成ウィザードを起動します。
	選択したディレクトリ サービスを開始します	停止している既存のディレクトリ サービスを開始するために使用します。
	選択したディレクトリ サービスを停止します	すでに開始されている既存のディレクトリ サービスを停止するために使用します。
	選択したディレクトリ サービスを再開します	既存のディレクトリ サービスを再開するために使用します。
	選択したディレクトリ サービスを削除します	リストからディレクトリ サービスを削除します。

ディレクトリ サービスの詳細の表示

定義したディレクトリ サービス オブジェクトの情報を表示できます。

ディレクトリ サービスの詳細を表示するには

1 [設定] タブで、左側のペインにある [**ディレクトリ サービス**] をクリックします。

2 詳細を表示したいディレクトリ　サービス、またはオプションを変更したいディレクトリ サービスの名前をクリックします。次に、ディレクトリ サービスの要約ウィンドウのサンプルを示します。

3 **[要約]** タブをクリックすると、ディレクトリ サービスについての基本情報を参照できます。これらのプロパティを変更することはできません。

4 **[プロパティ]** タブをクリックすると、**[全般設定]** と **[接続設定]** を参照できます。これらの設定は変更できます。アスタリスク (*) の付いているパラメータはすべて必須です。変更してから **[保存]** をクリックします。

5 **[閉じる]** をクリックして、ダイアログを確認します。

ディレクトリ サービスのプロパティ設定の変更

定義したディレクトリ サービス オブジェクトのプロパティ設定を変更できます。

ディレクトリ サービスのオプションを変更するには :

1 [設定] タブで、左側のペインにある **[ディレクトリ サービス]** をクリックします。

2 変更したいディレクトリ サービスの名前をクリックします。

3 **[プロパティ]** タブをクリックして、ディレクトリ サービスのオプションを表示します。

4 **[全般設定]** または **[接続設定]** をクリックして、変更する設定を表示します。アスタリスク (*) の付いているパラメータはすべて必須です。

5 設定を変更します。これらの設定のリストを表示するには、次のトピックを参照してください。

— Configuration Server ディレクトリ サービスへの接続の設定 272 ページ

— 外部ディレクトリ サービスへの接続の設定 273 ページ

6 **[保存]** をクリックします。

7 **[閉じる]** をクリックして、[実行ステータス] ダイアログを確認します。右上隅にある **X** をクリックして [プロパティ設定] ウィンドウを閉じます。

ディレクトリ サービスのオプションが変更されました。変更した設定によっては、HPCA Enterprise Console をログアウトしてからログインしなおす必要がある場合もあります。

Configuration Server ディレクトリ サービスへの接続の設定

外部ディレクトリ サービスへの接続を設定するには、まず内部の Configuration Server ディレクトリ サービスへの接続を作成する必要があります。これは、HPCA-CS 接続と呼ばれます

HPCA-CS 接続はポリシーの解決に使用できません。

Configuration Server ディレクトリ サービス接続 (HPCA-CS) は、HPCA Enterprise Console を使用してポリシーを管理するための前提条件です。LDAP または LDAPS (セキュア) 接続を設定する前に、まずこの接続の設定を行ってください。

Configuration Server ディレクトリ サービスを設定するには :

1. [設定] タブで、左側のペインにある **[ディレクトリ サービス]** をクリックします。
2. ディレクトリ サービスの詳細セクションで、[新しいディレクトリ サービスを作成します] ボタン をクリックします。ディレクトリ サービスの作成ウィザードが開始します。
3. [表示名] と [説明] を指定します。**[タイプ]** 一覧から、**[HPCA-CS]** を選択します。作成できる HPCA-CS ディレクトリ サービスは 1 つだけです。
4. **[次へ]** をクリックします。
5. [接続設定] の下に、次のオプションがあります。アスタリスク (*) の付いているパラメータはすべて必須です。
   - **[起動]** で **[自動]** を選択すると、Portal の起動時にこのディレクトリ サービスが自動的に開始されるようになります。
   - **[ホスト]** には、Configuration Server のホスト名または IP アドレスを入力します。
   - **[ポート]** には、Configuration Server のポート番号を入力します。デフォルトは 3464 です。
   - Configuration Server にサインインするために使用するアカウントを設定するには、**[サービス アカウント ID]** を使用します。このサービス アカウントは、読み取り処理と書き込み処理の両方で使用されます。このディレクトリ ソースへの完全な読み取り / 書き込みアクセス権が必要です。
   - **[パスワード]** を使用して、サービス アカウント ID のパスワードを指定します。**[パスワードの確認]** テキスト ボックスにパスワードを再入力します。

— **[タイムアウト]** を使用して、Configuration Server への接続のタイムアウト時間を秒単位で指定します。HP Support が指示しない限り、デフォルトの 120 に設定したままにしてください。

— **[接続試行回数]** を使用して、HPCA Enterprise Console が Configuration Server への接続を何回試行すると接続失敗となるかを指定します。

— **[接続遅延]** を使用して、接続試行と接続試行の間の遅延時間を秒単位で指定します。

6 **[次へ]** をクリックします。

7 [要約] 画面を確認します。すべてのプロパティが正しければ、**[適用]** をクリックします。

8 **[閉じる]** をクリックして、ダイアログを確認します。

ディレクトリ ソースが [ディレクトリ サービス] リストに追加されます。

外部ディレクトリ サービスへの接続の設定

外部ディレクトリ サービスへの接続を設定する前に、272 ページの「Configuration Server ディレクトリ サービスへの接続の設定」の手順に従ってください。

HPCA Enterprise Console では、サービスをディレクトリ サービス オブジェクトに割り当てて LDAP ポリシーを管理できます。

ただし、これを行うには、まず外部ディレクトリ サービスへの接続を設定する必要があります。次のタイプの外部ディレクトリ サービスがサポートされています。

- Lightweight Directory Authentication Protocol(LDAP)
- SSL (Secure Sockets Layer) をサポートする LDAP (LDAPS (セキュア))

LDAP サーバーで SSL を使用している場合、LDAPS (セキュア) タイプの接続を使用する必要があります。

各外部 LDAP ディレクトリ サービスは、次の任意の組み合わせに対して使用できます。

- 認証
- レポート
- ポリシーのエンタイトルメント

たとえば、2 つのディレクトリがあるとします。一方のディレクトリにはすべてのユーザー アカウントが含まれており、もう一方のディレクトリはポリシー専用です。ユーザー アカウント ディレクトリに対して認証を行います。このケースでは、2 つのディレクトリ サービスを、接続を別々に定義して次のように作成する必要があります。

- 接続を次のように設定した認証用のディレクトリ サービスを 1 つ作成します。
  - **[認証で使用]** がオン
  - **[ポリシーに使用]** がオフ
  - **[サービス アカウントの使用]** がオフ

  [認証で使用] をオンにすると、ユーザーはこのディレクトリ サービスの外部 LDAP ディレクトリ アカウントを使用して HPCA Enterprise Console にログインできるようになります。
- ポリシー用のもう 1 つのディレクトリ サービスを次のように作成します。
  - **[認証で使用]** がオフ
  - **[ポリシーに使用]** がオン
  - **[サービス アカウントの使用]** がオン

このように設定することにより、1 つ目のディレクトリ サービスを使用してサインインして、2 つ目のディレクトリ サービスでポリシーを設定できます。

ディレクトリ ソースで **[認証で使用]** がオン、**[サービス アカウントの使用]** がオフに設定されている場合、ユーザーは外部 LDAP ディレクトの認証情報を使用してサインインする必要があります。**[サービス アカウントの使用]** がオンになっている場合、ユーザーはローカルの HPCA Enterprise Console ユーザー名とパスワードを使用してサインインできます。

LDAP または LDAPS (セキュア) ディレクトリ サービスを設定するには :

1. [設定] タブで、**[ディレクトリ サービス]** をクリックします。
2. ディレクトリ サービスの詳細セクションで、  ([新しいディレクトリ サービス]) ボタンをクリックします。ディレクトリ サービス作成ウィザードが開始します。
3. **[表示名]** と **[説明]** を指定します。
4. **[タイプ]** 一覧から、次のオプションの 1 つを選択します。
   - LDAP サーバーで SSL を使用しない場合、**[LDAP]** を選択します。
   - LDAP サーバーで SSL を使用する場合、**[LDAP (セキュア)]** を選択します。
5. **[次へ]** をクリックします。

6 必要な接続パラメータを入力します。次のオプションがあります。アスタリスク (*) の付いているパラメータはすべて必須です。

- **[起動]** で **[自動]** を選択すると、Portal の起動時にこのディレクトリ サービスが自動的に開始されるようになります。
- **[ホスト]** は、LDAP サーバーの完全なホスト名または IP アドレスです。
- **[ポート]** は、LDAP ポートです。SSL を使用しない LDAP の場合、デフォルト値は 389 です。LDAP (セキュア) の場合、デフォルト値は 636 です。
- ディレクトリ サービス サーバーにサインインするために HPCA Enterprise Console によって使用されるアカウントを設定するには、**[サービス アカウント ID]** を使用します。このサービス アカウントは、読み取り処理と書き込み処理の両方で使用されます。このディレクトリ ソースへの完全な読み取り / 書き込みアクセス権が必要です。
- **[パスワード]** を使用して、サービス アカウント ID のパスワードを指定します。[パスワードの確認] にパスワードを再入力します。
- **[ベース DN]** は、HPCA Enterprise Console からディレクトリをブラウズするときにルート識別名 (DN) として使用されます。
- LDAP (セキュア) の場合、次の情報も指定します。
  - **[CA 証明書ディレクトリ]** を使用して、SSL 証明書のディレクトリを指定します。これは、Portal が保存されているサーバーの相対パスです。次に例を示します。

    `<InstallDir>\HPCA\ManagementPortal\etc\CACertificates`
  - **[CA 証明書ファイル]** を使用して、SSL 証明書の場所を指定します。これも、Portal が保存されているサーバーの相対パスです。次に例を示します。

    `<InstallDir>\HPCA\ManagementPortal\etc\CACertificates\<LDAP Certificate File Name>`

7 **[次へ]** をクリックします。

8 必要なユーザ インターフェイスを入力します。次のオプションがあります。

- **レポートで使用** : このオプションを有効にすると、このディレクトリ サービスは HPCA Enterprise Console の [レポート] タブでフィルタ ソースとして有効になります。この機能を有効にするには、Portal をディレクトリ ソースとして使用するように Reporting Server を設定する必要があります。
- **ポリシーに使用** : このオプションを有効にすると、このディレクトリ サービスは HPCA Enterprise Console でポリシーの管理に使用できます。

— **認証で使用**：このオプションを有効にすると、このディレクトリ サービスは HPCA Enterprise Console のログイン画面でサインイン オプションとして有効になり、既存のディレクトリ ユーザーに基づいたユーザー認証が可能になります。次の 2 つのパラメータを使用できます。

– **認証グループ DN**：これは、HPCA Enterprise Console に対して認証されるユーザーのソースとして使用されます。このグループのメンバーであるすべてのユーザーは、HPCA Enterprise Console へのサインインが可能になります。

– **サービス アカウントの使用**：このオプションを有効にすると、このディレクトリ サービスへのすべての読み取り要求および書き込み要求に対して、**[接続設定]** で指定した **[サービス アカウント ID]** が使用されるようになります。無効にすると、このディレクトリ サービスへのすべての読み取り要求および書き込み要求では、サインオンしているユーザーの認証情報が使用されます。

— **リーフ ノード フィルタ**：LDAP 形式のフィルタ値を入力して、多数のデータ タイプを持つノードをフィルタリングして、それらがツリー ナビゲーション ビューに表示されないようにします。使いやすさを向上させるために、コンピュータやユーザーなどのオブジェクトにフィルタを実行する必要があります。各ノードをフィルタリングする最適な方法を決定するには、ディレクトリ固有のスキーマを参考にしてください。次の例では、コンピュータとユーザーをフィルタリングしています。

```
(!(|(objectclass=user)(objectclass=computer)))
```

9 **[次へ]** をクリックします。

10 要約情報を確認します。すべてのプロパティが正しければ、**[適用]** をクリックします。

11 **[閉じる]** をクリックして、ダイアログを確認します。

ジョブ アクション テンプレート

ジョブ アクション テンプレートを使用して、新しいジョブの作成時に使用するパラメータを事前に定義できます。

ジョブ アクション テンプレートは、[設定] タブの [インフラストラクチャ管理] 領域で管理します。使用可能なジョブ アクション テンプレートの一覧を表示するには、左側のナビゲーション メニューにある **[ジョブ アクション テンプレート]** リンクをクリックします。

[ジョブ アクション テンプレート] ウィンドウの [有効] カラムでは、HPCA ジョブ作成ウィザードを使用して新しいジョブを作成するときにテンプレートが使用可能かどうかが示されます。パラメータを編集するテンプレートの名前をクリックするか、**[新しいジョブ アクション テンプレート]** ボタンをクリックして新しいテンプレートを作成します。詳細な手順については、277 ページの「新しいテンプレートの作成」を参照してください。

HPCA Core のインストール時に、次のジョブ アクション テンプレートが提供されます。

- パッチ接続
- DTM スケジュールのリフレッシュ
- セキュリティ接続
- ソフトウェア接続
- Satellite の同期 (すべて)
- Satellite の同期 (設定)
- Satellite の同期 (データ)

これらの各テンプレートを使用して、CSDB の関連するドメインに接続するようにターゲット デバイスのエージェントに指示を与えます。たとえば、セキュリティ接続テンプレートの場合、エージェントは SECURITY ドメインに接続します。これにより、デバイスがアクセスできる SECURITY ドメインのすべてのサービスが強制的に実行されます。

Satellite の同期または DTM スケジュールのリフレッシュのジョブをクライアント デバイスで正常に実行するには、そのクライアントの HPCA Agent によって HPCA Core への接続操作が事前に実行されている必要があります。

新しいテンプレートの作成

新しいジョブ アクション テンプレートを作成するには、次の手順を使用します。既存のテンプレートを変更するには、[ジョブ アクション テンプレート] リストでその名前をクリックします。

新しいジョブ アクション テンプレートを作成するには

1 **[設定]** タブから、**[インフラストラクチャ管理]** をクリックして展開します。

2 **[ジョブ アクション テンプレート]** をクリックします。

3 **[新しいジョブ アクション テンプレート]** ボタン をクリックします。ジョブ アクション テンプレート作成ウィザードが開きます。

4 新しいテンプレートの作成を開始します。次のテンプレートから選択できます。

— 空白テンプレート – 使用可能なすべてのパラメータを定義できます。

— サンプル テンプレート – 事前に定義されたパラメータが含まれています。これは、テンプレートを作成したときに選択した接続タイプやオプションによって異なります。280 ページの「サンプル テンプレート」を参照してください。

— ユーザー定義されたテンプレート – 別のテンプレートで指定した設定が含まれています。

5 **[次へ]** をクリックします。

6 テンプレートのパラメータを定義します。アスタリスク (*) の付いているパラメータはすべて必須です。

一部のパラメータに関連付けられている **[UI 設定]** ドロップダウン ボックスによって、HPCA ジョブ作成ウィザードを使用してジョブを作成するときにそのパラメータが表示されるかどうかが決まります。

— **[非表示]** の場合、パラメータは表示されません。

— **[表示のみ]** の場合、ウィザードにパラメータが表示されます。

— **[表示と編集]** の場合、ジョブが表示されてパラメータを変更できます。

表示名 : テンプレートの名前を入力します。この名前は [ジョブ アクション テンプレート] ページに表示されます。

説明 : テンプレートの詳細な説明を入力します。この説明も [ジョブ アクション テンプレート] ページに表示されます。

テンプレートの有効化 : テンプレートを有効にする場合に選択します。有効化されたテンプレートは、ジョブの作成時に使用できます。

接続パラメータ

管理対象クライアント システムに関連している項目を次に示します。

通知ポート : 通知ポートを入力します。デフォルト ポートは 3465 です。

ジョブ ユーザー ID: ジョブ ユーザー ID を入力します。ジョブのセキュリティがクライアント デバイスで有効になっている場合、この入力は必須です。

パスワード : パスワードを入力します。ジョブのセキュリティがクライアント デバイスで有効になっている場合、この入力も必須です。パスワードの入力時にはアスタリスクのみが表示されます。

アクション パラメータ

通知ジョブと DTM ジョブの両方に関連している項目を次に示します。

サービスの選択 : HPCA ジョブ作成でサービスの選択リストを表示する場合に選択します。このリストにはエンタイトルメント サービスのみが含まれます。

コマンド: ジョブの実行時にリモート システムで実行するコマンドを入力します。この実行可能ファイルは、HPCA Agent のルートフォルダで使用できるものに限定されています。

パラメータ : コマンドのパラメータを入力します。

その他のパラメータ : コマンドのその他のパラメータを含めます。**[その他のパラメータ]** は、指定した **[パラメータ]** と結合します。

ジョブ パラメータ

同時プロセス制限 : ジョブに対して許可される最大プロセス数を入力します。これは、ジョブを処理するために使用する「スレッド」の数、つまり同時に実行する通知の数です。デフォルトは 25 です。

- 小規模なネットワークまたは危険を伴うジョブには小さい数を使用
- 大規模なネットワークには大きい数を使用

新規プロセス遅延: このジョブの新規プロセスをアクティブにしている間の待ち時間 (秒) を入力します。デフォルト値は、接続タイプに基づいています。この値は、1 つのターゲット システムでジョブが完了するまでの見積もり時間に応じて変わります。有効な範囲は、60 から 65,535 です。

このパラメータを使用して、ネットワーク トラフィックを管理したり、ネットワークの過剰使用 (氾濫) を回避できます。OS 接続の場合は最低でも 20 分、ソフトウェア接続の場合は最低でも 5 分にする必要があります。

7 **[サブミット]** をクリックします。

新しいテンプレートは、[ジョブ アクション テンプレート] ウィンドウに表示されます。**[テンプレートの有効化]** を選択した場合、HPCA ジョブ作成ウィザードを使用して新しいジョブを作成するときにテンプレートを使用できます。ウィザードを使用した通知ジョブの作成の詳細については、158 ページの「ジョブを管理する」を参照してください。

サンプル テンプレート

サンプル テンプレートを使用して、特定の接続タイプに通常使用される事前定義パラメータに基づいてジョブ アクション テンプレートを作成できます。次のサンプル テンプレートが定義されます。

パッチ接続

パッチ接続は、デバイスのエンタイトルメントを持っているパッチを更新するために使用します。

DTM スケジュールのリフレッシュ

DTM ジョブのスケジュールは、通知ジョブまたは DTM ジョブを作成したり、DTM スケジュールのリフレッシュのジョブ アクション テンプレートを使用してリフレッシュできます。167 ページの「ターゲットの DTM スケジュールのリフレッシュ」を参照してください。

Satellite の同期 (すべて、設定、およびデータ)

Satellite の同期テンプレートは、Satellite で最新のデータを使用できるように Satellite サーバーと Core サーバーを同期させるために使用します。171 ページの「Satellite 同期ジョブの作成」を参照してください。

セキュリティ接続

セキュリティ接続では、SECURITY ドメインのすべてのセキュリティ エンタイトルメントが解決します。

ソフトウェア接続

ソフトウェア接続は、グループまたはデバイスのエンタイトルメントを持っているソフトウェアのリストを更新するために使用します。

マルチキャスト

マルチキャストは、最も効率的な戦略を使用して配信先グループに情報を同時に配信し、オペレーティング システム イメージおよびアプリケーションの配信に使用されます。

- マルチキャストを有効にするには、このチェック ボックスをオンにして **[保存]** をクリックします。

Live Network

HP Live Network コンテンツ サーバーとの通信に必要な Live Network 設定は、[設定] タブの [インフラストラクチャ管理] 領域で設定します。281 ページの「HP Live Network サーバーへの接続の設定」を参照してください。

Live Network の更新は、[操作] タブの [インフラストラクチャ管理] 領域で設定します。232 ページの「Live Network」を参照してください。

HP Live Network サーバーへの接続の設定

最新のセキュリティとコンプライアンスのコンテンツを HP Live Network から自動的にダウンロードし、「HP Live Network アナウンスメント」のダッシュボード ペインの RSS フィードを確立するために使用する接続を設定するには、Live Network 設定を使用します。これには、次の項目が含まれています。

- 最新のスキャナおよびデータをダウンロードするために使用する HP Live Network コンテンツ サーバーの URL
- HP Live Network コンテンツ サーバーのログイン認証情報

このページで入力したパスワードは暗号化されます。

保存する前に設定情報をテストできます。テストをリクエストすると、HPCA Enterprise Console は HP Live Network コンテンツ サーバーへの接続を試行します。接続に成功すれば、設定情報は有効です。詳細については、282 ページの「Live Network の設定のテスト」を参照してください。

HP Live Network の接続設定を指定するには

1 [設定] タブで、[インフラストラクチャ管理] 領域を展開し、**[Live Network]** をクリックします。

2 次の情報を指定します。アスタリスク (*) の付いているパラメータはすべて必須です。

— **HP Live Network ユーザー ID** — HP Live Network 登録アカウントのユーザー ID です。

— **HP Live Network パスワード** — HP Live Network 登録アカウントのパスワードです。

— **HP Live Network コンテンツの URL** — 脆弱性定義とスキャナの HP Live Network コンテンツ サーバーのロケーションです (URL はデフォルトで設定されています)。

— **HP Live Network コネクタ** — HPCA Core をホストするシステムの Live Network コネクタ実行可能ファイルへのパスです (パスはデフォルトで設定されています)。

詳細については、76 ページの「HP Live Network コネクタの手動での実行」および 236 ページの「HP Live Network コネクタのダウンロード」を参照してください。

3 指定した設定をテストするには、**[テスト]** をクリックします。詳細については、282 ページの「Live Network の設定のテスト」を参照してください。

4 **[保存]** をクリックして、変更内容を実装します。

- テストが成功しても、その設定は HPCA Enterprise Console では自動的に保存されません。設定を保存するには、**[保存]** ボタンをクリックする必要があります。
- このページから離れると、**[保存]** をクリックする前にテキスト ボックスに入力した情報はすべて失われます。情報を保存する場合は、必ず **[保存]** をクリックしてください。
- **[リセット]** ボタンを使用して、最後に保存した設定に戻すことができます。

Live Network の設定のテスト

Live Network を設定する場合、保存する前に、設定が機能するかどうかをテストできます。

テストを実行するには、ページの右下隅にある **[テスト]** ボタンをクリックします。HPCA Enterprise Console では、まず必要なすべての設定が指定されていることと、すべての設定の形式が正しいことが確認されます。その後で、次のアクションを実行します。

HPCA Enterprise Console から HP Live Network コンテンツ サーバーへの接続を試行して、指定されているユーザー名とパスワードを使用してログインします。[インフラストラクチャ管理] 設定領域の [プロキシ設定] ページに表示されるプロキシ情報が使用されます。

ネットワーク トラフィックやその他のパラメータによって異なりますが、このテストは最大で 3 分かかります。テストを続行するかどうかを確認するダイアログ ボックスが表示されます。続行する場合、**[はい]** をクリックします。

テストが完了すると、[テスト結果] ダイアログ ボックスにテストの結果が表示されます。次の表に、表示される結果と各結果の意味を示します。

表 41　Live Network の設定のテスト結果

アイコン	結果	説明と推奨アクション
	テストは成功しました。	すべての設定が有効です。設定を保存してください。
	テストに失敗しました。	テストが失敗する一般的な理由を次にいくつか挙げます。 • 必要な設定が見つからない。 • 無効な形式で設定が指定されている (無効な URL またはパス名など)。 • 設定のスペルに誤りがある。 • HP Live Network コンテンツ サーバーのログイン認証情報が無効 (登録の期限切れなど)。
	不明	この結果は、必ずしも設定情報が無効であることを意味しているわけではありません。これは、テストを完了できなかったということだけを表しています。 たとえば、HPCA Enterprise Console が HP Live Network コンテンツ サーバーに 3 分以内に接続できず、テストがタイムアウトした場合などが該当します。これは、次のような理由で発生します。 • サーバーが使用できない。 • ネットワーク　トラフィックによって接続が妨げられる。 • ファイアウォールによって接続がブロックされる。 また、接続がプロキシ サーバー経由の場合に指定したプロキシ情報が正しくなかったり、プロキシ サーバーによって接続がブロックされていたりすると、この結果となることがあります。

失敗または不明瞭なテスト結果のトラブルシューティングを行うには、タブですべての設定のスペルおよび形式を確認します。エラーがないかどうか `vms-server.log` ファイルも確認します。

テストが成功していても、設定を保存するには **[保存]** ボタンをクリックする必要があります。設定は HPCA Enterprise Console によって自動的に保存されません。

デバイス管理

[デバイス管理] セクションを使用して、警告オプション、シン クライアント、およびリモート制御を設定します。

次のセクションでは、利用可能なデバイス管理オプションについて説明します。

- 警告中 284 ページ
- シン クライアント 285 ページ
- リモート制御の設定 286 ページ

警告中

[警告中] セクションを使用して、CMI の警告およびレポート オプションを設定します。

- CMI 284 ページ

CMI

CMI Softpaq は、HPCA Agent 配布の一部として、各 HP ターゲット デバイスにインストールされます。HP Client Management Interface(CMI) は、企業管理者や IT プロフェッショナルに、HP ビジネスクラス デスクトップ、ノートブックおよびワークステーションに対する高レベルの管理システムを提供します。

CMI のハードウェア固有の情報が取得され、レポートに利用できます。[レポート] タブの [表示オプション] セクションで **[HP 固有のレポート]** レポート ビューを使用して、CMI ハードウェア関連レポートを作成します。(CMI 関連のレポート オプションを表示するには、**[インベントリ管理レポート]**、**[ソフトウェア レポート]**、**[HP 固有のレポート]** の順で選択します)。

CMI に関する詳細は、次を参照してください。

http://h20331.www2.hp.com/Hpsub/cache/284014-0-0-225-121.html

[CMI] タブを使用して、HP CMI 設定を変更します。変更した設定は、管理対象のクライアントが次に HPCA インフラストラクチャに接続したときに、有効になります。

CMI は、特定の HP デバイス モデルでしか互換性がありません。互換性に関する情報は、デバイスの説明を参照してください。

CMI を設定するには

1. HPCA Console で、**[設定]** タブをクリックし、**[デバイス管理]** を選択します。
2. 管理対象 HP デバイスから取得したクライアント警告についてレポートするには、**[クライアント警告のレポート]** ドロップダウン リストから **[有効]** を選択します。警告レポートはデフォルトでは無効になっています。[有効] を選択すると、[レポートする最低の重大度] ドロップダウン リストが使用できるようになります。
3. レポートする最低の警告重大度を選択します。
4. 管理対象 HP デバイスのクライアント警告を有効にするには、**[クライアント警告の表示]** ドロップダウン リストから **[有効]** を選択します。警告はデフォルトでは無効です。[有効] を選択すると、[表示する最低の重大度] ダイアログと [警告ウィンドウのタイムアウト] ダイアログが使用できるようになります。
5. クライアント デバイスに表示する最低の警告重大度を選択します。
6. 警告をクライアント デバイスに表示する秒数を入力します。デフォルトでは、警告は 5 秒間表示されます。
7. **[保存]** をクリックします。

シン クライアント

シン クライアント管理サービスによって Windows CE デバイスに設定データが提供されます。Core でこのサービスが無効になっている場合、この情報をリクエストする Satellite またはエージェントはこの情報を使用できません。

- シン クライアント管理を有効にするには、このチェック ボックスをオンにして **[保存]** をクリックします。

リモート制御の設定

HPCA Enterprise Console では、Windows リモート デスクトップ接続、Virtual Network Computing (VNC)、または Windows リモート アシスタンスを使用して内部リポジトリまたは外部リポジトリのデバイスにリモート アクセスできます。

HPCA 管理者は、HPCA Enterprise Console を設定して任意またはすべての接続タイプを有効にできます。リモート制御をすべて無効にすることもできます。

接続タイプごとに、リモート ターゲット デバイスがリモート接続をリスンするポートを指定する必要があります。各接続タイプに関連する追加要件については、181 ページの「リモート接続の要件」を参照してください。

リモート制御を設定するには

1 [設定] タブで、左側のナビゲーション ツリーにある **[リモート制御]** をクリックします。

2 有効にする接続タイプを選択します。

- **有効 VNC (Virtual Network Computing)**
- **Windows リモート デスクトップ の有効化**
- **Windows リモート アシスタンス の有効化**

3 VNC および Windows リモート デスクトップの場合、リモート デバイスがリモート接続をリスンする **[ポート]** を指定します。

Windows リモート アシスタンスの場合はポートを指定する必要はありません。これは、Windows リモート アシスタンスは常にポート 135 の Distributed Component Object Model (DCOM) インターフェイスを使用するためです。

4 **[保存]** をクリックします。

5 **[閉じる]** をクリックして、[実行ステータス] ダイアログ ボックスを閉じます。

リモート制御機能の使用に関する情報については、180 ページの「デバイスのリモート制御」を参照してください。

パッチ管理

パッチ管理を有効にして、パッチ データベースの ODBC パラメータを定義するには、[パッチ管理] セクションを使用します。パッチ管理のオプションについては、次のセクションで説明します。

- データベース設定 287 ページ
- 設定 295 ページ
- エージェント オプション 291 ページ
- エージェントの更新 294 ページ
- ベンダーの設定 297 ページ
- パッチ配布設定 288 ページ
- 取得ジョブ 311 ページ

[パッチ配布設定] では、Microsoft パッチを適用するための新しい軽量なモデルを選択できます。詳細については、次の章を参照してください。

- メタデータを使用したパッチ管理 325 ページ

データベース設定

コンソールの [パッチ管理] 領域とパッチ取得機能を使用するには、パッチを有効にする必要があります。

パッチ管理サービス (`HPCA Patch Manager`) を開始して、パッチ データベースと Core 権限のある CSDB パッチ ライブラリに保存された情報と SQL データベースの情報を同期する機能を有効にするには、[データベース設定] 領域を使用します。

前提条件

- パッチ データベースを作成し、そのデータベースの ODBC 接続を定義する必要があります。詳細については、『HPCA Core および Satellite Servers 入門およびコンセプト ガイド』を参照してください。

パッチの有効化および設定を行うには

1. **[有効]** を選択します (これにより、`HPCA Patch Manager` サービスが開始します)。
2. パッチの [ODBC 設定] 領域で、次のオプションを設定します。

— **ODBC DSN**: Patch SQL データベースの DSN を選択します。

— **ODBC のユーザー ID**: DSN のユーザー ID を指定します。

— **ODBC のパスワード**: ODBC ユーザー ID に関連付けられているパスワードを指定します。

3 **[保存]** をクリックします。

4 パッチの ODBC 設定を変更した場合、プロンプトに従って Patch Manager サービスを再開します。

パッチ配布設定

[パッチ配布設定] 領域を使用して、次のオプションの有効化および設定を行います。

- [パッチ メタデータのダウンロード] オプション

このオプションが有効になっている場合、次の設定に関連するオプションもページに表示されます。

- [パッチ ゲートウェイ オペレーション] 設定

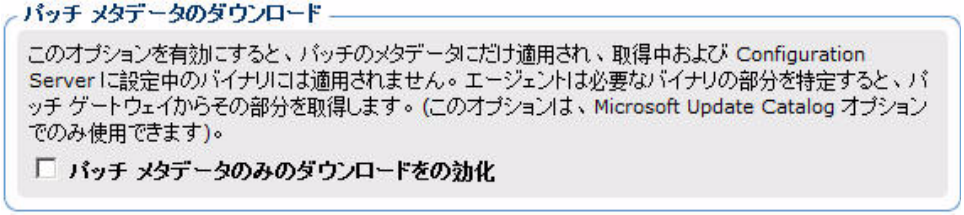
これらのオプションにより、軽量な取得および配布モデルで Microsoft Update Catalog を使用して Microsoft デバイスにパッチを適用できます。

メタデータによるパッチ管理を使用する場合も、**[Download Manager を有効化]** をオンにする必要があります。これを行うには、**[設定] > [パッチ管理] > [エージェント オプション]** ページに移動します。

Microsoft デバイスにパッチを適用する場合、可能な限り [パッチ メタデータのダウンロード] と [パッチ ゲートウェイ オペレーション] を使用することをお勧めします。これには、325 ページの「メタデータを使用したパッチ管理」の章で説明されているようにいくつかの利点があります。

- 軽量なメタデータ メカニズムを使用して Microsoft パッチを管理するには、**[パッチ メタデータのみのダウンロードを有効化]** チェック ボックスをオンにします。Microsoft Update Catalog データ フィードを使用する必要があります。

このオプションをオンにすると、メタデータのみが Configuration Server Database にダウンロードおよびパブリッシュされます。エージェントのリクエスト時またはゲートウェイのプレロード時に、パッチ バイナリ ファイルが Patch Manager ゲートウェイにダウンロードおよびキャッシュされます。



パッチ メタデータのダウンロードを有効にする場合、取得を実行する前に次のオプションの有効化および設定も行う必要があります。

- パッチ ゲートウェイ オペレーション (必須)

- エージェント オプション : Download Manager を有効化 (必須)

[パッチ メタデータのダウンロードの有効化] がオンの場合、パッチを取得するためのベンダー値が MICROSOFT から MSFT に切り替わります。

メタデータのダウンロードおよびゲートウェイ オペレーションを使用した環境の設定とパッチの取得の詳細については、325 ページの「メタデータを使用したパッチ管理」を参照してください。必ずオフライン スキャンを設定して Download Manager のプレロード オプションを設定してください。

パッチ ゲートウェイ オペレーション

[パッチ配布設定] ページの [パッチ メタデータのダウンロード] オプションが有効になっている場合、パッチ ゲートウェイ オペレーションの設定を使用できます。

これらの設定を使用して、ゲートウェイを有効にします。

有効にすると、追加のエントリを使用してパッチ バイナリのキャッシングおよび管理を行うように設定できます。

Microsoft Update Catalog データ フィードのいずれかを使用して Microsoft Agent に軽量なパッチ適用を実現する [パッチ メタデータのダウンロード] オプションを使用するには、パッチ ゲートウェイが必要です。

パッチ ゲートウェイの役割は、[パッチ メタデータのダウンロードの有効化] がオンの場合にのみ、実際のパッチ バイナリ データをダウンロードしてキャッシュし、エージェントに配信することです。オプションの [ゲートウェイ プレロード] オプションを使用すると、エージェントからのリクエスト時ではなく取得時にパッチ バイナリをゲートウェイにキャッシュできます。

- **[ゲートウェイの有効化]** チェック ボックスをオンにすると、Microsoft パッチ バイナリ データのオンデマンド ダウンロードおよびキャッシングがゲートウェイで可能になります。これを行うには、**Microsoft Update Catalog** データフィードのいずれかを使用する軽量な [パッチ メタデータのダウンロード] オプションを使用する必要があります。

[ゲートウェイの有効化] がオンになっていると、次のフィールドを使用できます。

- **[最大キャッシュ サイズ]** では、ゲートウェイ キャッシュの最大サイズ (MB) を指定します。空白または 0 の場合は「キャッシュの上限がない」ことを意味します。

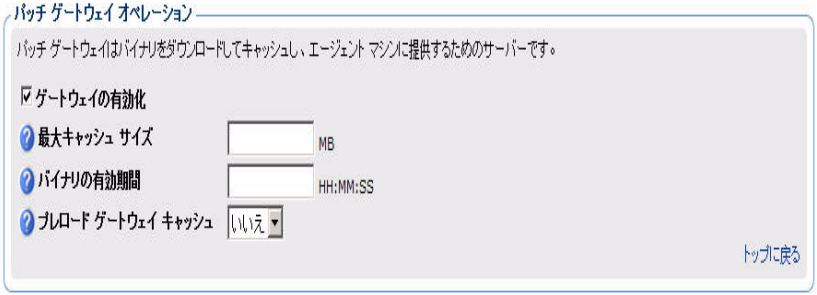
  デフォルト : 1000 MB

- **[バイナリの有効期間]** では、キャッシュされたバイナリ ファイルをアップストリーム サーバーから再検証せずにゲートウェイに保持する最大期間 (時間 : 分 : 秒の形式) を指定します。値が -1 または空白の場合は、バイナリをリフレッシュしないことを意味します。値が 10:00:00 の場合は、バイナリがキャッシュに 10 時間保持された後に再度ダウンロードされることを意味します。

  デフォルト : 空白 (リフレッシュなし)

- **[プレロード ゲートウェイ キャッシュ]** (オプション) で **[はい]** を指定すると、取得の実行時にパッチ バイナリがゲートウェイにキャッシュされます。プレロード オプションを設定する前に次の点に注意してください。プレロードのメリットの 1 つは、パッチ バイナリを最初にリクエストするエージェントが、ゲートウェイによるパッチ バイナリのダウンロードを待たずにパッチ バイナリを取得できるという点です。ただし、プレロードのデメリットとして、エージェントで必要とされているかどうかに関係なく、取得時にすべてのパッチ バイナリがダウンロードされます。

  エージェントからパッチのリクエストを受信したときにのみゲートウェイからパッチ バイナリ データをダウンロードおよびキャッシュするようにする場合、**[いいえ]** (デフォルト) を指定します。



エージェント オプション

これらのエージェント オプションは、Microsoft デバイスのパッチにのみ適用されます。

Microsoft デバイスにパッチを適用するときの Patch Manager Agent のオプションを有効化および設定するには、[設定] タブ > [パッチ管理] 領域にある [エージェント オプション] を使用します。

Patch Agent が次に HPCA Server に接続するときに、これらのパネルで指定した設定の変更が受信されます。

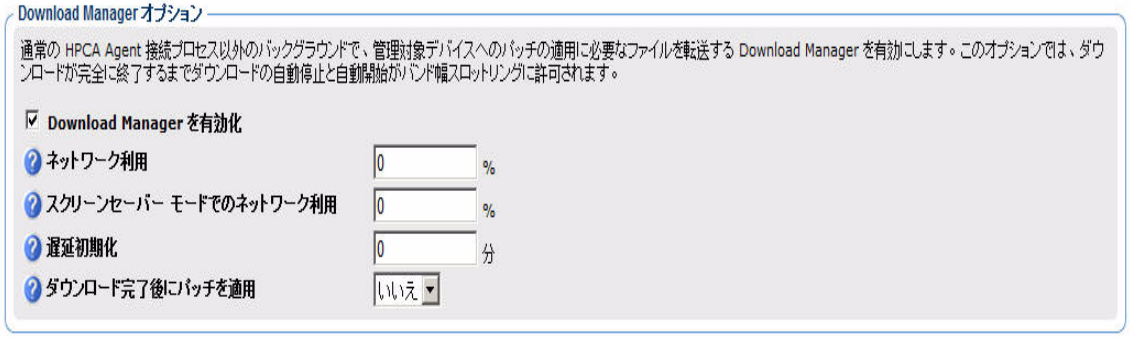
- Download Manager オプション 291 ページ
- Patch Agent のエージェント オプション 293 ページ

Download Manager オプション

- **Download Manager を有効化**: このチェック ボックスをオンにすると、エージェントのマシンに必要なパッチ ファイルのダウンロードが、Download Manager によってバックグラウンドの非同期プロセスで制御されます。Download Manager は、通常の HPCA Agent Connect プロセスの外部で動作します。

  メタデータによるパッチ配布を使用するには、Download Manager を有効にする必要があります。

  オンにすると、Download Manager のオプションがいくつか表示されます。



次の表を参考にして、Download Manager オプションを設定します。

ネットワーク利用、スクリーン セーバー モードでのネットワーク利用、初期化後の遅延、およびダウンロード完了後のパッチ適用の有無を指定するオプションを設定します。

表 42　Patch Agent の Download Manager オプション

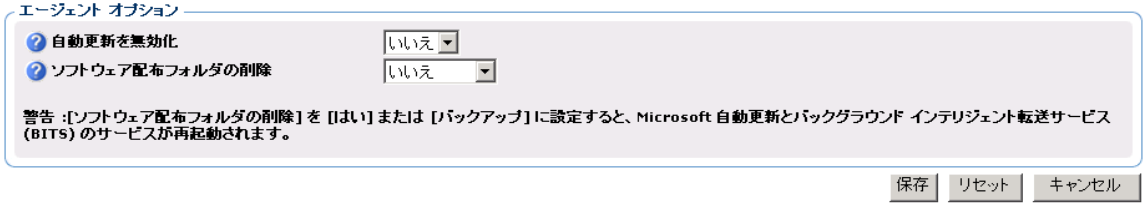
オプションと有効な値	説明
ネットワーク利用 値 = 0 ～ 100 % デフォルトは 0	デバイスがアクティブな場合にパッチ ファイルのダウンロードに使用できるネットワークの最大バンド幅の割合を指定します。 値が 0 の場合、使用可能なネットワークのバンド幅でダウンロードが行われます。 例: 25 を指定すると、使用可能なバンド幅の 25% 以下でパッチのダウンロード プロセスが行われます。
スクリーンセーバー モードでのネットワーク利用 値 = 0 ～ 100 % デフォルトは 0	スクリーン セーバーのネットワーク利用のオプションです。スクリーン セーバーがオンの場合にパッチ ファイルのダウンロードに使用できるネットワークの最大バンド幅の割合を指定します。通常、このオプションの値はスクリーン セーバーがオフの場合よりも大きな割合になります。 値が 0 の場合、スクリーン セーバーがオンのときに使用可能なネットワークのバンド幅でダウンロードが行われます。 例 : 80 を指定すると、スクリーン セーバーがオンのときにパッチ ファイルをダウンロードするために使用するバンド幅が 80% に増加します。
遅延初期化 値 = 0 ～ 999 分 デフォルトは 0	初期化してからパッチのダウンロードを開始または再開するまでの遅延時間 (分) を指定します これにより、他のプロセスを起動してからパッチのダウンロードを再開できます。 例 : 15 に設定すると初期化が 15 分遅延します。 値が 0 の場合は遅延はありません。
ダウンロード完了後にパッチを適用 値 = [はい] または [いいえ] (デフォルト)	[はい] に設定すると、ダウンロードの完了後に Patch Agent Connect を起動してパッチを適用します。[はい] に設定することをお勧めします。 デフォルトの [いいえ] のままにしておくと、Patch Agent Connect が次に実行されたときにパッチが適用されます。

[保存] をクリックして、これらの設定オプションを設定します。Patch Agent が次に HPCA Server に接続するときに、新しい設定が受信されます。

Patch Agent のエージェント オプション

次のエージェント オプションを使用して Microsoft デバイスにパッチを適用できます。

- **Microsoft 自動更新を無効化** : ドロップダウン ボックスから [はい] または [いいえ] を選択します。自動更新が有効になっていることが原因で Patch Agent のスキャンまたは配布が中断される問題に対応するには、このオプションを使用します。
  - **はい** : Patch Agent によって各スキャンまたは配布の前に Microsoft 自動更新が無効化されます。パッチのスキャンと配布が実行されたら、自動更新は元の状態に戻ります。
  - **いいえ** : (デフォルト) Patch Agent によって各スキャンまたは配布の前に自動更新が無効化されません。



- **ソフトウェア配布フォルダの削除** : ドロップダウン ボックスから [はい]、[バックアップ]、または [いいえ] を選択します。このオプションは、次の問題の対応に使用できます。
  - ソフトウェア配布フォルダのサイズの大幅な増加
  - ソフトウェア配布フォルダの破損
  - パッチ接続時に Configuration Server にかかる負荷の増加

  [ソフトウェア配布フォルダの削除] を [はい] または [バックアップ] に設定すると、Microsoft 自動更新とバックグラウンド インテリジェント転送サービス (BITS) のサービスが自動的に再起動されます。サービスの再起動によって環境に問題が発生する場合、特に共存するパッチ ソリューションとして HPCA Patch Management と自動更新の両方を使用しているとき、このオプションの設定には注意が必要です。

  このオプションを [はい] または [バックアップ] に設定すると、フォルダ サイズ、破損、またはインフラストラクチャの負荷に問題がある場合に Patch Manager のパフォーマンスが向上します。

— **はい** : Patch Agent によって、各パッチのスキャンの前にソフトウェア配布フォルダのコンテンツが削除されます。サービスの再起動に関する警告 (上記) を参照してください。

— **バックアップ** : Patch Agent によって、各パッチのスキャンの前にソフトウェア配布フォルダのコンテンツがバックアップされてから削除されます。サービスの再起動に関する警告 (上記) を参照してください。

— **いいえ: (デフォルト)** ソフトウェア配布フォルダに対して何も行われません。

[保存] をクリックして、設定オプションを設定します。Patch Agent が次に HPCA Server に接続するときに、新しい設定が受信されます。

エージェントの更新

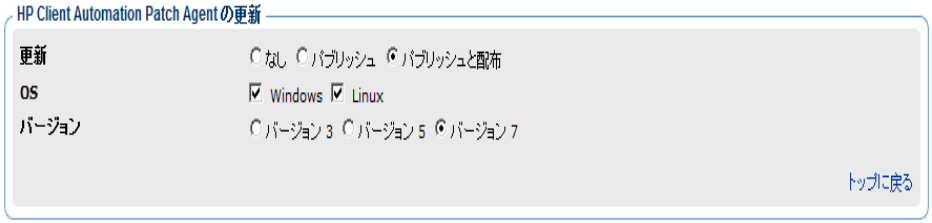
[エージェントの更新] を使用して、パッチ管理のエージェントの更新を設定します。

HP Patch Agent の更新設定

これらの設定を使用して、HP Client Automation (HPCA) Patch Manager Agent ファイルに対するメンテナンスを取得および適用します。詳細については、244 ページの「エージェントの更新を表示」を参照してください。[HP Patch Agent の更新] セクションで、次の設定を行います。

- **更新**: [パブリッシュ] を選択すると更新は PATCHMGR ドメインにパブリッシュされますが、配布するために Patch Manager ターゲット デバイスに接続されることはありません。これらの接続は作成する必要があります。[パブリッシュと配布] を選択すると、更新が PATCHMGR ドメインにパブリッシュされ、DISCOVER_PATCH インスタンスに接続されます。このオプションでは、更新が Patch Manager ターゲット デバイスに配布されます。
- **OS**: Patch Manager Agent の更新を取得および管理するベンダーのオペレーティング システムのタイプを指定します。
- **バージョン**: エージェントの更新を取得する Patch Manager のバージョンを選択します。1 つの Configuration Server には 1 つのバージョンのみをパブリッシュできます。デフォルトは、使用可能な最新のバージョンです。

  Patch Manager を最初にインストールする場合は、[バージョン] パラメータをインストール時のデフォルトから変更しないでください。



設定

ここでは、ベンダーと取得の設定を行います。これらの設定は、[ベンダーの設定] と [取得ジョブ] に反映されます。

- **次のものについてパッチ管理を有効にする**: パッチを取得する OS のベンダーを指定します。これらのベンダーは、[ベンダーの設定] と [取得の設定] に表示されます。後日、その他のベンダーのパッチを取得することにした場合、最初にここで指定する必要があります。
- **取得の概要を保存** : PASTORE (Patch Auth Store) インスタンスを維持する日数を指定します。このクラスには、各パッチ取得セッションにつき 1 つのインスタンスが含まれます。この値が [履歴の詳細を保存] の値より小さい場合、[履歴の詳細を保存] は [取得サマリを保存] の値に設定されます。値 0 は、パッチ取得の履歴を削除しないことを意味します。
- **履歴の詳細を保存** : PUBERROR (Publisher Error) インスタンスを維持する日数を指定します。このクラスには、各パッチ取得エラーにつき 1 つのインスタンスが含まれます。
- **パッチ データのリポジトリ パス** : Configuration Server にパブリッシュされる前に、パッチがダウンロードされるディレクトリ。前回の取得のデータを事前に設定したディレクトリを使用して取得を実行する場合は、このパラメータに事前に設定するディレクトリを指定します。
- **過去のブリテン** : 過去のブリテンをカンマで区切って表示します。このパラメータは、製品またはリリース レベルではなく、ブリテン レベルで作用します。

  過去の機能で、以下を実行します。

— 指定したブリテンが Configuration Server DB に存在する場合は、現在のパブリッシュ セッション中に削除します。

— 過去のパラメータで指定したブリテンは、現在のパブリッシュ セッション中に Configuration Server DB にパブリッシュしないでください。過去オプションはブリテン オプションより優先されます。

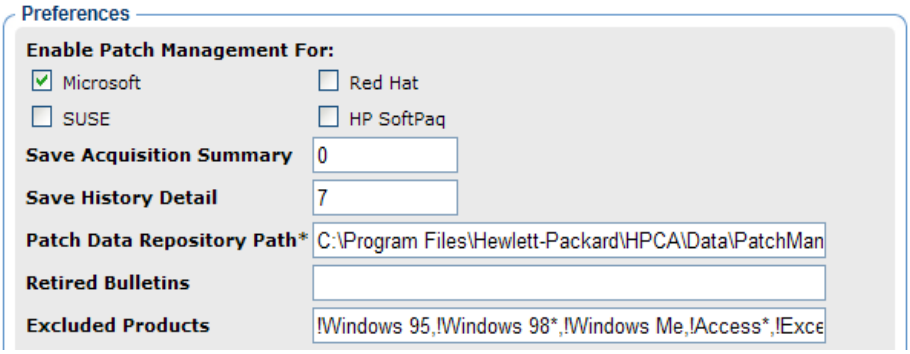
- **除外された製品**：カンマで区切った vendor::product の形式で、除外する製品の先頭に感嘆符 (!) を付けます。包括フィルタが設定されていない場合はすべての製品が対象となります。包括フィルタを指定する場合は、除外フィルタは包括される製品のサブセットになります。これはベンダーの命名基準に従って指定してください。たとえば、Microsoft は、Internet Explorer を IE のような一般的な省略名でなく、完全名で使用します。また、Windows 95 以外のすべての Windows 製品を含める場合は {Microsoft::Windows*,Microsoft::!Windows 95} と入力します。

新しい Patch Manager インストールの場合、Microsoft Office、Windows 95、Windows 98、Window Me、および Microsoft Office 製品および SuSE 特有の *-yast2、*-yast2-*、および *-liby2 製品などのセキュリティ パッチの取得および管理はデフォルトで除外されています。SuSE OS yast 特有製品の自動管理は Patch Manager ではサポートされていません。

以前のバージョンの Patch Manager からの移行で、移行前に patch.cfg を削除しなかった場合、すべての Microsoft Office 製品またはそのスタンドアロン バージョンを Patch Manager の取得と管理から除外するには、製品除外リストに次のテキストを追加します。

“,!Access*,!Excel*,!FrontPage 200[023],!FrontPage 9[78],!InfoPath*,!Office*,!OneNote*,!Outlook*,!Power Point*,!Project 200[023],!Project 98,!Publisher*,!Visio*,!Word*,!Works*”

上のテキストはすべて 1 行で表示され、ユーザー インターフェイスの [除外された製品] テキスト ボックスには上で表示されている引用符が含まれないので注意してください。



- **デフォルトのパッチ取得ダウンロードの言語**：セキュリティ パッチを取得および管理する言語を指定します。デフォルトは en(英語) です。

ベンダーの設定

ベンダーの設定には、自社のエージェントに関するベンダー特有の URL や、パッチの取得および管理アクティビティに必要なその他のオプションが表示されます。

[ベンダーの設定] にアクセスする前に、まず [設定] ページで適切なベンダーと OS の選択を有効にしてください。

ある取得セッションから次のセッションの間にベンダーの設定を変更して、以前は選択されていた 1 つ以上の製品またはオペレーティング システムを除外した場合、除外した製品またはオペレーティング システムに特有のすべてのパッチが Configuration Server Database から削除されます。これは、除外された製品またはオペレーティング システムが、脆弱性の評価および管理の観点で今後は適格でなくなることを意味します。これは、すべてのベンダーに適用されます。

ベンダーの設定：

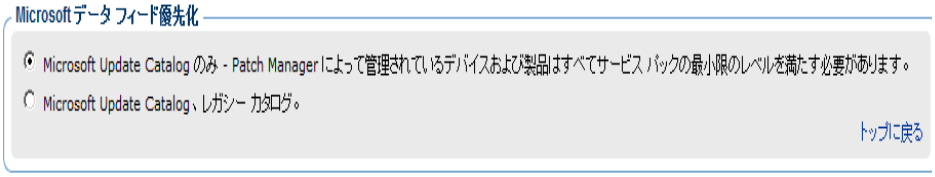
- Microsoft データ フィード優先化 298 ページ
- Red Hat のフィード設定 301 ページ
- SuSE のフィード設定 303 ページ

- HP SoftPaq のフィード設定 307 ページ

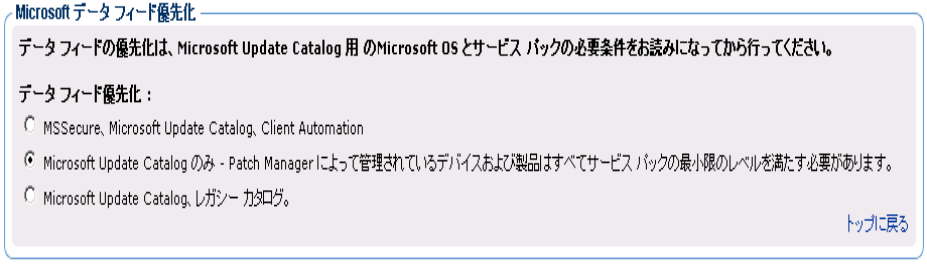
Microsoft データ フィード優先化

次の Microsoft データ フィード優先化設定は、使用可能な Microsoft の更新リポジトリとメソッドをサポートおよび優先化するために、[ベンダーの設定] セクションで設定します。

[パッチ配布設定] の **[パッチ メタデータのみのダウンロードを有効化]** オプションがオンになっている場合、Microsoft Update Catalog データ フィードのいずれかを選択できます。



[パッチ配布設定] の **[パッチ メタデータのみのダウンロードを有効化]** オプションがオフになっている場合、[Microsoft データ フィード優先化] パネルには次の 3 つのオプションが表示されます。



Microsoft パッチ管理アクティビティの詳細については、『HPCA Patch Manager インストールおよび設定ガイド』の「パッチ取得」の章を参照してください。

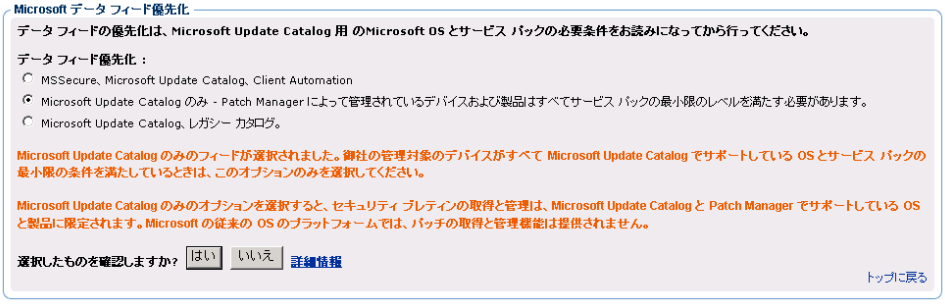
- **MSSecure、Microsoft Update Catalog、Client Automation**: このオプションは、[パッチ メタデータのダウンロード] オプションがオンの場合に表示されます。パッチは、MSSecure と Microsoft Update Catalog の両方から取得します。パッチが MSSecure と Microsoft Update Catalog の両方に存在する場合、MSSecure をサポートしているテクノロジが使用されます。

  MSSecure テクノロジのために、このオプションでは Windows Vista(32 ビットまたは 64 ビット) または 64 ビット アーキテクチャの Windows を実行するデバイスにはパッチを適用できません。これらのデバイスにパッチを適用するには、Microsoft Update Catalog を含む [データ フィード優先化] を選択します。

  このマニュアルを作成している時点で、Microsoft の Web サイトでは、レガシー カタログは 2008 年まで継続して更新されるが、MSSecure.xml は 2007 年 10 月 9 日以降は更新されないことを示唆しています。

- **Microsoft Update Catalog のみ**: (デフォルト オプション) すべてのパッチは Microsoft Update Catalog から取得されます。このオプションを使用するには、企業内のすべてのデバイスが Microsoft によって設定された最低レベルのオペレーティング システムおよび製品である必要があります。これらの最低要件に適合していないデバイスにはパッチは適用されません。

  このオプションを変更すると、次の警告メッセージが表示され、続行するにはこれに同意する必要があります。



[はい] をクリックすると、このオプションの選択を確認する画面がもう一度表示されます。**[保存]** をクリックして確定します。

- **Microsoft Update Catalog、レガシー カタログ :** パッチは、Microsoft Update Catalog と、現在の MSSECURE と HP が修正したメタデータを含む、レガシー カタログと呼ばれる HP リポジトリから取得されます。パッチが、Microsoft Update Catalog とレガシー リポジトリの両方に存在する場合は次のとおりです。
  - ターゲット デバイスが Microsoft Update Catalog でサポートされる最低要件に一致している場合、そのデバイスには Microsoft Update Catalog と Windows Update Agent テクノロジを利用してパッチが適用されます。
  - ターゲット デバイスが Microsoft Update Catalog でサポートされる OS の最低要件に適合していない場合、デバイスにはレガシー カタログでホストされるメタ データを使用する MSSecure テクノロジを使用してパッチが適用されます。

  HP レガシー カタログは、新しいパッチが MSSecure に追加されると、HP によって継続的に更新されます。HP レガシー カタログでホストされるパッチには、HP メタデータの修正が必要です。**[Microsoft Update Catalog、レガシー カタログ]** オプションをオンにすると、Microsoft セキュリティ ブリテンは古い Microsoft オペレーティング システム (各種のサービス パックも含めて) に適用可能とみなされます。また、Microsoft 製品には、Configuration Server の PATCHMGR ドメインと Reporting Server で表示される Patch Manager レポートで識別するために、Microsoft ブリテン名に「_L」が追加されます。

  Office アプリケーションが HP Client Automation Application Self-Service Manager または管理制御ポイントで管理されている場合、Microsoft Update Catalog テクノロジを使用して取得および管理される Office のパッチは検出されません。どちらの場合も、Office アプリケーションに影響を与えるブリテンがデバイスに指定された場合は、Patch Manager が Office のパッチを管理し、それを脆弱なデバイスにローカルにインストールします。

Microsoft のフィード設定

以下の設定はベンダー フィードのセクションで行います。

[詳細] にのみ表示されるフィールド

- **MSSecure***: Microsoft が提供する `MSSECURE.XML` ファイルを含む、Microsoft の MSSecure キャビネット ファイルの URL を指定します。

デフォルト :**http://download.microsoft.com/download/0/d/b/0db2e5d7-0ba9-4856-b51f-db7c0b838c68/MSSecure_1033.CAB**

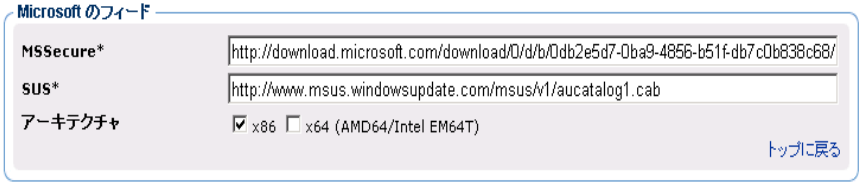
このマニュアルを作成している時点で、Microsoft Knowledge の記事では、Microsoft は 2008 年までこのカタログの更新は継続するが、2007 年 10 月 9 日以降、`MSSecure.xml` のサポートおよび更新を継続しない計画であることを示唆しています。

- **SUS***: Microsoft SUS データ フィードを含む Microsoft キャビネット ファイルの URL を指定します。

  デフォルト : **http://www.msus.windowsupdate.com/msus/v1/aucatalog1.cab**

[基本] と [詳細] のフィールド

- **アーキテクチャ**: Microsoft のパッチを取得するアーキテクチャを選択します。サポートされるアーキテクチャは次のとおりです。
  - **x86**: 32 ビット Intel アーキテクチャ用。
  - **x64**: AMD64 または Intel EM64T 用。このターゲット アーキテクチャを選択する場合は、[Microsoft データ フィード優先化] を「**Microsoft Update Catalog のみ**」または「**Microsoft Update Catalog、レガシー カタログ**」に設定する必要があります。



Red Hat のフィード設定

[Red Hat のフィード] セクションでは、以下の設定を行います。

[詳細] にのみ表示されるフィールド

- **Red Hat**: Red Hat Network のデータ フィードの URL を指定します。デフォルトは **http://xmlrpc.rhn.redhat.com/XMLRPC** です。

[基本] と [詳細] のフィールド

- **パッケージ依存関係をパブリッシュ**: ダウンロードしたセキュリティ アドバイザリが依存する追加の Red Hat パッケージをパブリッシュする場合は、[はい] を指定します。デフォルトは "No" です。

Red Hat セキュリティ アドバイザリをインストールするための前提となる、または依存する Red Hat パッケージは、2 か所から取得できます。それらは、取得中に Red Hat ネットワークからダウンロードするか、以前に Red Hat Linux インストール メディアをコピーしたことがある場合はローカルに見つけることができます。Patch Manager は、取得時にまず適切なディレクトリで .rpm パッケージを検索します。次に例を示します。

- x86 の Red Hat Enterprise Linux 4ES では、Red Hat インストール メディアで提供されたベースライン オペレーティング システムの rpm ファイルを `Data\PatchManager\Patch\redhat\4es` に配置します。
- x86-64 の Red Hat Enterprise Linux 4ES では、Red Hat インストール メディアで提供されたベースライン オペレーティング システムの rpm ファイルを `Data\PatchManager\Patch\redhat\4es-x86_64` に配置します。
- `Data\PatchManager\Patch\redhat\packages` サブディレクトリに名前を付けるときは、次の **OS フィルタのアーキテクチャ**の値を参照してください。サブディレクトリ名には、`REDHAT::` に続く値に基づいて適切なフォルダ名を使用します。

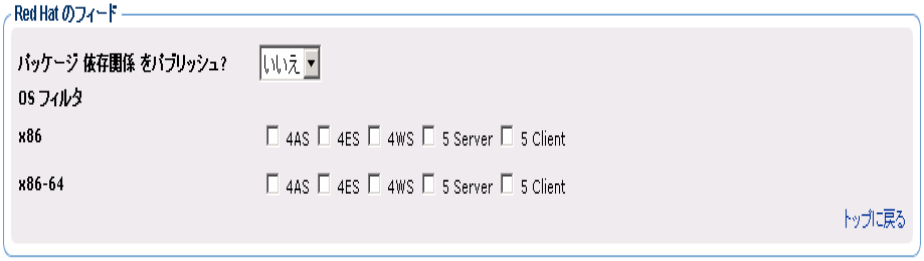
パッチの前提ソフトウェアがローカルに見つからない場合、パッケージを Red Hat Network からダウンロードします。取得に必要な時間を短縮するために、依存パッケージを Linux インストール メディアから適切なパッケージ ディレクトリにコピーすることをお勧めします。Red Hat RPM パッケージは、Linux インストール メディアの `RedHat/RPMS` ディレクトリにあります。

- **OS フィルタ** : x86 (32 ビット Intel) および x86-64 (Opteron/EMT64) アーキテクチャに対して、Red Hat バージョン 4 とリリース AS、ES および WS のすべての組み合わせ、および Red Hat バージョン 5 のサーバーおよびデスクトップ クライアント用リリースのすべての組み合わせがサポートされます。指定されたアーキテクチャの Red Hat パッチの取得については、オペレーティング システムとリリースの組み合わせを選択します。
  - **x86** アーキテクチャ: Red Hat x86 アーキテクチャで `patch.cfg` ファイルに指定できる値は次のとおりです。

    ```
    REDHAT::4as、      REDHAT::4es、     REDHAT::4ws、
    REDHAT::5server、   REDHAT::5client
    ```

  - **x86-64** アーキテクチャ : Red Hat x86-64 アーキテクチャで `patch.cfg` ファイルに指定できる値は次のとおりです。

    ```
    REDHAT::4as-x86_64、     REDHAT::5server-x86_64、
    REDHAT::4es-x86_64、     REDHAT::5client-x86_64、
    REDHAT::4ws-x86_64
    ```



SuSE のフィード設定

SuSE Linux のパッチ適用設定を設定するには、SuSE Linux 製品タイプのいずれか、または両方を選択してから、お使いの環境のバージョン レベルと OS プラットフォームの [SuSE のフィード設定] を選択します。SuSE 9 のフィード設定は、SuSE 10 のフィード設定とは別にグループ化されています。

関連トピック：

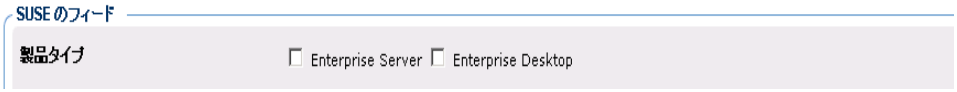
- SuSE のパッチ管理要件 309 ページ

SuSE メタ データ フィードの URL を設定または修正する必要もある場合は、[基本] から [詳細] 設定に切り替えます。

製品タイプ

お使いの環境にインストールされている SuSE Linux 製品タイプを選択します。

- **Enterprise Server:** SuSE バージョン 9 および 10 で使用可能な SuSE Linux Enterprise Server (SLES) 製品タイプを指定します。
- **Enterprise Desktop:** SuSE バージョン 10 で使用可能な SuSE Linux Enterprise Desktop (SLED) 製品タイプを指定します。



SuSE 9 のフィード設定

次に挙げる SuSE 9 のフィード設定のデフォルト URL を表示または変更するには、**[詳細]** をクリックします。

[詳細] にのみ表示されるフィールド

- **SuSE 9**: SuSE 9 のセキュリティ アドバイザリのメタ データを取得するためのセキュアな URL を指定します。デフォルトは以下のとおりです。

  https://you.novell.com/update/i386/update/SUSE-CORE/9/
  https://you.novell.com/update/i386/update/SUSE-SLES/9/

- **SuSE 9-x86_64**: AMD64 または Intel EM64T アーキテクチャの SuSE 9 の更新を取得するためのセキュアな URL を指定します。デフォルトは以下のとおりです。

  https://you.novell.com/update/x86_64/update/SUSE-CORE/9/
  https://you.novell.com/update/x86_64/update/SUSE-SLES/9/

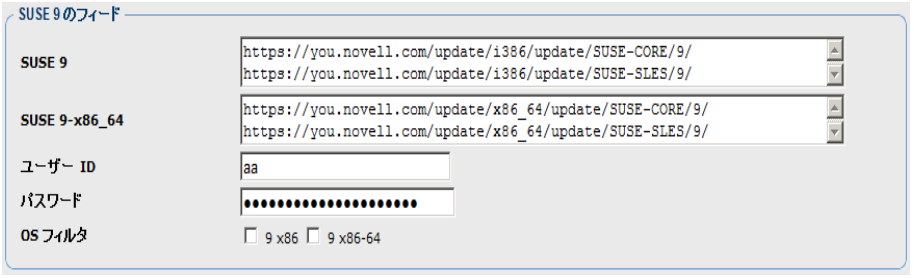
[基本] と [詳細] のフィールド

[基本] または [詳細] ページを使用して、SuSE 9 のデータフィードを取得するために必要な設定を入力します。

- **ユーザー ID**: お使いの SuSE ユーザー ID を指定します。ユーザー ID はベンダーから入手します。
- **パスワード**: SuSE ユーザー ID のパスワードを指定します。
- **OS フィルタ**: SuSE Linux Enterprise Server パッチを取得するオペレーティング システムのバージョンとアーキテクチャの組み合わせを選択します。x86 (32 ビット) アーキテクチャと x86-64 (AMD64 および Intel EM64T) アーキテクチャの SuSE バージョン 9 がサポートされています。

  patch.cfg で有効な x86 アーキテクチャの OS フィルタの値は `suse::9` です。

  patch.cfg で有効な x86-64 アーキテクチャの OS フィルタの値は `suse::9-x86_64` です。



SuSE 10 のフィード設定

SuSE バージョン 10 のサポートでは、SuSE Linux Enterprise Server 10 (SLES10) と SuSE Linux Enterprise Desktop 10 (SLED10) が対象となります。

- SLES 10 のセキュリティ アドバイザリを取得するには、[製品タイプ] の [Enterprise Server] をオンにします。
- SLED 10 のセキュリティ アドバイザリを取得するには、[製品タイプ] の [Enterprise Desktop] をオンにします。

次に挙げる SuSE 10 のフィード設定のデフォルト URL を表示または変更するには、**[詳細]** をクリックします。

[詳細] にのみ表示されるフィールド

- **SUSE 10**: x86 アーキテクチャの SUSE 10 (SLES10 と SLED10) についてセキュリティ アドバイザリのメタ データを取得するためのセキュアな URL を指定します。

  デフォルト :
  https://nu.novell.com/repo/\$RCE/SLES10-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-Updates/sled-10-i586/
- **SUSE 10SP1**: x86 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 1 について更新を取得するためのセキュアな URL を指定します。

  デフォルト :
  https://nu.novell.com/repo/\$RCE/SLES10-SP1-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-SP1-Updates/sled-10-i586/
- **SUSE 10SP2**: x86 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 2 について更新を取得するためのセキュアな URL を指定します。

  デフォルト :
  https://nu.novell.com/repo/\$RCE/SLES10-SP2-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-SP2-Updates/sled-10-i586/
- **SUSE 10-x86_64**: x86-64 アーキテクチャの SUSE 10 (SLES10 と SLED10) についてセキュリティ アドバイザリのメタ データを取得するためのセキュアな URL を指定します。

  デフォルト :
  https://nu.novell.com/repo/\$RCE/SLES10-Updates/sles-10-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED10-Updates/sled-10-x86_64/

- **SUSE 10SP1-x86_64**: x86-64 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 1 について更新を取得するためのセキュアな URL を指定します。

  デフォルト：
  https://nu.novell.com/repo/\$RCE/SLES10-SP1-Updates/sles-10-x86_64
  https://nu.novell.com/repo/\$RCE/SLED10-SP1-Updates/sled-10-x86_64/

- **SUSE 10SP2-x86_64**: x86-64 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 2 について更新を取得するためのセキュアな URL を指定します。

  デフォルト：
  https://nu.novell.com/repo/\$RCE/SLES10-SP2-Updates/sles-10-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED10-SP2-Updates/sled-10-x86_64/

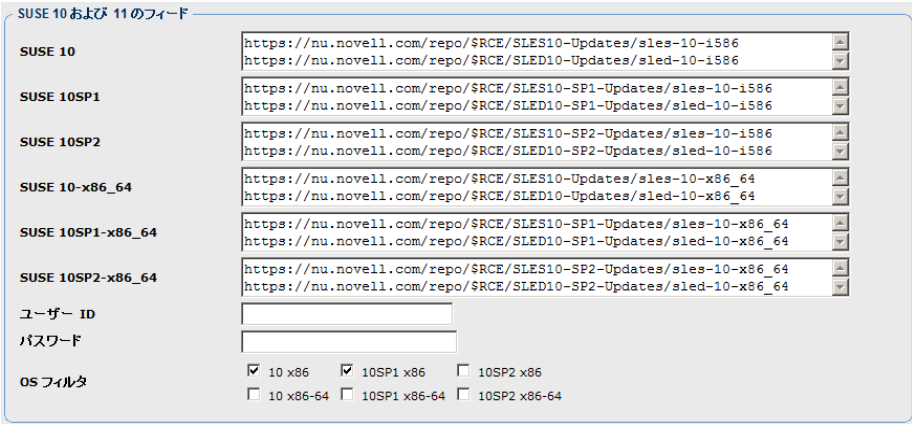
[基本] と [詳細] のフィールド

[基本] または [詳細] ページを使用して、SuSE 10 のデータフィードを取得するために必要な次の設定を入力します。

- **ユーザー ID**: お使いの SUSE 10 ユーザー ID を指定します。ユーザー ID はベンダーから入手します。詳細については、309 ページの「SuSE のパッチ管理要件」を参照してください。
- **パスワード**: SUSE ユーザー ID のパスワードを指定します。
- **OS フィルタ**: SUSE バージョン 10 パッチを取得するオペレーティング システムのバージョン、サービス パック、およびアーキテクチャの組み合わせを選択します。x86 (32 ビット) アーキテクチャの SUSE バージョン 10 base、Service Pack 1、Service Pack 2 と、x86-64 (AMD64 および Intel EM64T) アーキテクチャの SUSE バージョン 10 base、Service Pack 1、Service Pack 2 がサポートされています。

  patch.cfg で有効な x86 アーキテクチャの OS フィルタの値は `suse::10`、`suse::10SP1`、および `suse::10SP2` です。

  patch.cfg で有効な x86-64 アーキテクチャの OS フィルタの値は `suse::10-x86_64`、`suse::10SP1-x86_64`、および `suse::10SP2-x86_64` です。



HP SoftPaq のフィード設定

[HP SoftPaq フィード] セクションでは、次の設定を行います。[HP SoftPaq URL] フィールドを含むすべてのフィールドを表示するには、**[詳細]** をクリックします。[基本] ページに戻るには、**[基本]** をクリックします。

ここで指定した SysID とブリテンの HP SoftPaq を取得するには、`hpsoftpaq` という名前の事前定義されたジョブを使用します。`hpsoftpaq` ジョブと使用可能なジョブのリストは、**[取得を開始]** 操作に表示されます。

[詳細] フィールド

- **HP SoftPaq URL:** HP SoftPaq のデータフィードの URL を指定します。デフォルトは、**http://h20278.www2.hp.com/hpapps/onlineDiag/ActiveCheck** です。

[基本] と [詳細] のフィールド

- **HP SoftPaq タイプ :** 取得および管理対象とする HP SoftPaq のタイプをオンにします。
  - アプリケーション
  - BIOS
  - ドライバ
  - ファームウェア

- **SysID:** HP SoftPaq に対して取得する SysID を指定します。

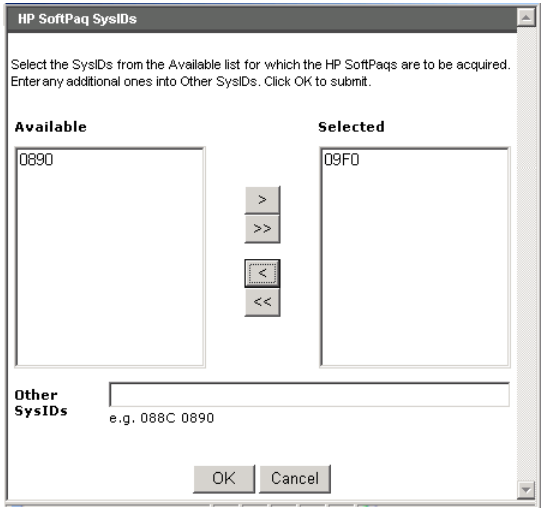
  お使いの HP デバイスで既に HPCA データベースにインベントリ情報がレポーティングされている場合は、[SysID の取得] ボタンを使用してリストからの SysID を選択できます。

  a **[SysID の取得]** ボタンをクリックします。これにより、[HP SoftPaq SysID] ダイアログ ボックスが開きます。[使用可能] カラムに、HPCA にインベントリが登録されている HP デバイスからレポーティングされた HP SoftPaq SysID のリストが表示されます。

  b 個々の SysID を **[使用可能]** カラムから **[選択済み]** カラムに移動するには、矢印ボタンを使用します。[選択済み] カラムの SysID が取得されます。

  c オプションとして、**[その他の SysID]** テキスト領域を使用して、[選択済み] カラムにまだリストされていない SysID をスペースで区切って入力できます。たとえば、次のように入力します。
  0890 8844 30A4 300F

  d **[OK]** をクリックすると、HP SoftPaq の [ベンダー] ページに戻ります。

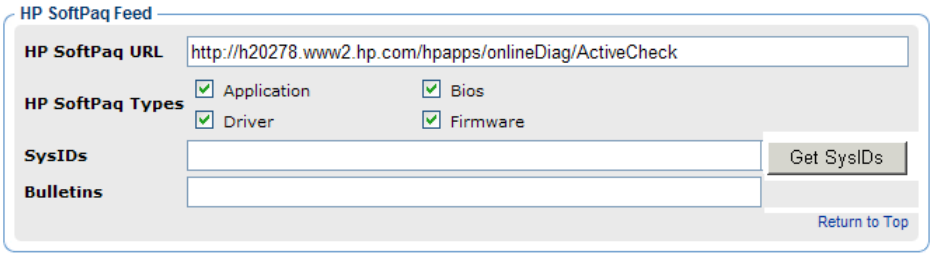


  [SysID] リストに、[HP SoftPaq SysID] ダイアログ ボックスで [選択済み] と [その他の SysID] に指定したエントリが表示されます。

- **ブリテン :** HP SoftPaq は、hpsoftpaq という名前の事前定義された取得ジョブを使用して取得されます。hpsoftpaq ジョブの実行時に取得するブリテンを入力するには、[ブリテン] 領域を使用します。SysID のすべてのブリテン

を取得するには、次のように入力します。

SP*



[保存] をクリックして、ベンダーの設定を保存します。[設定] タブの操作を終了する前に、設定変更をシステムに適用するには、**[設定の変更内容をいま適用する]** をクリックします。

HP SoftPaq を取得するジョブは事前に定義されています。実行するには、**[取得を開始]** 操作内のリストから hpsoftpaq を選択します。

SuSE のパッチ管理要件

SuSE フィードの設定では、このトピックで説明するセキュア (SSL) 接続およびベンダーから提供されるユーザー ID と パスワードが必要になります。

SUSE 10 デバイスの追加要件については、310 ページの「SuSE 10 登録要件」を参照してください。

SSL: Novell Web サイトでは、パッチの取得にセキュアな (SSL) 接続が必要です。Patch Manager 内でセキュアな接続を必要とするのは、Novell Web サイトからセキュアなパッチのダウンロードを実行するために使用するサーバーのみです。このマニュアルを作成している時点で、Novell Web サイトは証明書の検証を要求または実行していません。

SuSE Linux ベンダーのユーザー ID とパスワード : ベンダーのユーザー ID とパスワードを取得するための要件は、SuSE のバージョン番号に応じて異なります。

- **SuSE 9:** SuSE 9 のセキュリティ パッチを取得する場合、SuSE のインターネット リソースにアクセスするために、SuSE Linux ベンダーを介してユーザー ID とパスワードを設定する必要があります。コンソールの **[設定] タブ > [パッチ管理] > [ベンダーの設定]** ページを使用してパッチ管理用の SuSE デバイスを設定するときに、これらの認証情報を指定します。

- **SuSE 10:** SuSE 10 の SLES10 または SLED10 のセキュリティ パッチを取得する場合、SuSE 10 チャネルにアクセスするためには SuSE 10 Linux ベンダーを介してミラー認証情報を設定する必要があります。コンソールの **[設定] タブ > [パッチ管理] > [ベンダーの設定]** ページを使用してパッチ管理用の SuSE を設定するときに、これらの認証情報を指定します。

SuSE 10 のミラー認証情報を取得するには次の手順を実行します。

1. SuSE 10 製品の購入時に、SuSE Linux ベンダーを介して Novell Customer Center (NCC) にログインするためのユーザー名とパスワードを設定します。
2. SuSE 10 製品の購入時にベンダーから指定されたログイン アカウント情報を使用して NCC にログインします。
3. 左側のパネルにある、**[Myproduct]** リンクの下にある **[Mirror Credentials]** をクリックします。

   [Mirrors Credentials] ページの [Credentials] 領域に、ユーザー名とパスワードが表示されます。[Channels] 領域に、SuSE 10 チャネルの詳細が表示されます。
4. SuSE 10 パッチ取得用の SuSE 10 ユーザー ID とパスワード認証情報を入力するときは、上の手順で入手したユーザー名とパスワードを使用します。305 ページの「SuSE 10 のフィード設定」の設定については、「ベンダーの設定」のトピックを参照してください。

SuSE 10 登録要件

SuSE 10 以降、Novell のポリシーとして、セキュリティ パッチと更新を受信するには、各 SuSE 10 エージェント オペレーティング システムを Novell に登録し、そのライセンスを Novell Customer Center (NCC) または登録管理ツールで直接管理および検証する必要があることが明示的に表明されています。

HPCA Patch Management では、Novell の SuSE 10 ライセンスまたは登録に関するポリシーが満たされているかどうかは検証されません。Novell のポリシーへの準拠と、有効なライセンスによる SuSE 10 マシンの登録は、お客様の責任において実施してください。

SuSE 10 システムを Novell Customer Center に登録するには

SuSE 10 システムを Novell Customer Center に登録するための詳細については、Novell の Web サイトを参照してください。

本書の執筆時点では、「Registering and Updating SUSE Linux Enterprise 10」というトピックを以下のサイトで参照できます。

http://www.novell.com/support/dynamickc.do?cmd=show&forward=nonthreadedKC&docType=kc&externalId=3410833&sliceId=1

取得ジョブ

パッチ取得のスケジュールおよび設定を行うには、[取得ジョブ] セクションを使用します。

[パッチ管理] 取得ジョブを作成して実行するには、コンソールの次の領域を使用します。

- 必要な HTTP および FTP プロキシ設定を入力するには、[設定] タブの [インフラストラクチャ管理] 領域を使用します。
- 取得ジョブを定義するには、[設定] タブの [パッチ管理] 領域にある [取得ジョブ] タスクを使用します。
- ジョブを実行するには、[操作] タブの [パッチ管理] 領域にある [取得を開始] タスクを使用します。

パッチは、1 度に 1 つのベンダーから取得することをお勧めします。また、一部の SuSE セキュリティ アドバイザリおよび Microsoft Office セキュリティ ブリテンは、ダウンロードするために長時間かかる場合があります。

必要な取得ジョブの設定は、お使いの環境に依存します。

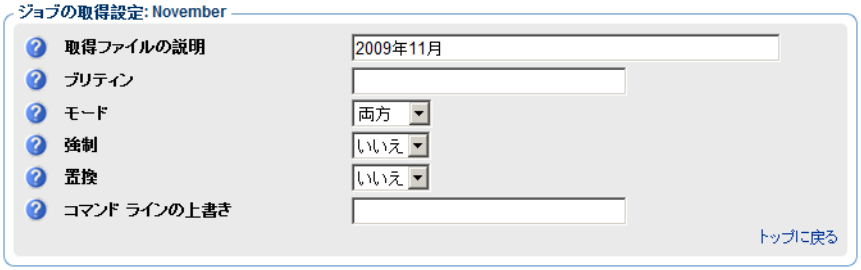
コンソールを使用して取得プロファイルを作成または編集するには

1 [設定] で、**[パッチ管理]**、**[取得ジョブ]** の順にクリックします。

2 編集する既存のファイルを選択するか、**[新規作成]** をクリックして新しいファイルを作成します。ごみ箱アイコンをクリックして取得ファイルを削除します。この例では、**[新規作成]** をクリックします。

3 新しいファイルを作成する場合、[ファイル名] と [説明] に入力して、**[次へ]** をクリックします。

4 手順 2 に進みます。ここで、新しいジョブの [取得の設定] を設定できます。



- **取得ファイルの説明** : 取得ファイルの説明を作成します。
- **ブリティン** : 取得するブリティンをカンマで区切って指定します。アスタリスク (*) のワイルドカード文字は認識されます。Red Hat セキュリティ アドバイザリでは、Red Hat によって発行されたときに Red Hat セキュリティ アドバイザリ番号に含まれるコロン (:) の代わりにハイフン (-) を使用します。
  - Microsoft セキュリティ ブリティンは、命名規則として `MSYY-###` を使用します。ここで、`YY` はブリティンが発行された年の下 2 桁で、`###` は指定した年にリリースされたブリティンのシーケンス番号です。HP によって提供される Microsoft サービス パックのパッチ説明ファイルの命名規則は、`MSSP_operatingsystem_spnumber` です。サンプルの Microsoft オペレーティング システムのサービス パックを取得する場合は、MSSP* を指定します。これにより、サンプルのサービス パックが `novadigm` または `custom` フォルダから取得されます。Microsoft アドバイザリを取得するには、命名規則として `MS-KB*` を使用して KB の記事を指定します。ここで、* はサポート情報の記事に割り当てられている番号を表します。
  - Red Hat セキュリティ アドバイザリは命名規則として `RHSA-CCYY:###` を使用して発行されます。ここで、`CC` は世紀を示し、`YY` はアドバイザリが発行された年の下 2 桁、`###` は Red Hat パッチ番号です。ただし、コロンは製品の予約文字なので、Red Hat によって発行されたセキュリティ アドバイザリ番号に含まれるコロン (:) の代わりにハイフン (-) を使用する必要があります。変更された命名規則 `RHSA-CCYY-###` を使用して、Patch Manager には、Red Hat セキュリティ アドバイザリを個別に指定してください。

— SuSE セキュリティ パッチは、命名規則として SUSE-PATCH-#### を使用します。ここで、### は SuSE によって指定されるナンバリング スキームです。

ブリテンをダウンロードしない場合は、[ブリテン] フィールドに **NONE** と入力してください。

- **モード**: パッチとパッチに関する情報をダウンロードする場合は [両方] を指定します。パッチのメタデータのみを取得する場合は、MODEL を指定します。パッチのブリティンブリティンと番号だけがダウンロードされ、実際のパッチ ファイルはダウンロードされません。このモードを使用すると、管理対象デバイスの脆弱性を公開するレポートを使用できます。
- **強制** : 次の場合に [強制] を使用します。
  - — 前回 [モデル] を使用して取得を実行し、今回は [両方] を使用する場合。
  - — 前回はある言語をフィルタして取得を実行し、今回は別の言語のブリティンを取得する必要がある場合。
  - — 以前に 1 つの製品を指定して取得を実行しており、今回は別の製品に関して取得する必要がある場合。

    たとえば、次のような場合があります。最初は企業内に Windows 2000 コンピュータしか所有していなかったので **-product {Windows 2000*}** を使用していました。1 か月後、Windows XP を展開しました。同じブリティンを取得する場合、**-product {Windows XP*,Windows 2000*}** と **-force y** を使用して取得を実行する必要があります。

    replace が **Y** に設定されると、ブリテンは force の値に関係なく削除されてから再取得されます。

- **置換** : **[Y]** に設定すると、bulletins パラメータで指定した古いブリティンを削除してから、それらを再度取得します。これは、force の値より優先されます。つまり、[置換] を **[Y]** に設定すると、[強制] を [N] と [Y] のどちらに設定しても、取得するように指定されたすべてのブリティンは削除され、再取得されます。
- コマンド ラインの上書き : 通常の取得パラメータを上書きする必要がある場合のみ、このパラメータを使用します。正しく使用しないと、取得は失敗します。-parameter value の形式を使用してください。

Microsoft の設定

- **Microsoft のパッチを取得しますか ?**: Microsoft のパッチを取得する場合は **[はい]** を選択します。その他の設定については、の [ベンダーの設定] ページに移動してください。

アウトバンド管理

[設定] タブの [アウトバンド (OOB) 管理] 領域を使用して、OOB 管理を設定します。アウトバンド管理の使用方法の詳細については、『HP Client Automation Out of Band Management ユーザー ガイド』を参照してください。次に示す各セクションで利用可能な設定オプションを説明します。

- 使用可能性 314 ページ
- デバイス タイプの選択 314 ページ
- vPro システム保護の設定 316 ページ

使用可能性

vPro または DASH デバイスでサポートされるアウトバンド管理機能を有効または無効にするには、[アウトバンド管理の有効化] 領域を使用します。

- アウトバンド管理機能を有効にするには、**[有効化]** チェックボックスをオンにします。

OOB 管理オプションを表示するには、[操作] タブの「アウトバンド管理」セクションを参照してください。

アウトバンド管理の使用方法の詳細については、『HP Client Automation Out of Band Management ユーザー ガイド』を参照してください。

デバイス タイプの選択

アウトバンド管理を有効にしたら、[デバイス タイプの選択] 領域を使用して、管理する OOB デバイスのタイプを選択します。

デバイス タイプごとに 3 つの選択肢からいずれかを選択できます。これらの選択肢について、次に示す各セクションで説明します。

- DASH デバイス 315 ページ

- vPro デバイス 315 ページ
- 両方 315 ページ

選択したデバイス タイプに応じて、HPCA Console には、選択内容に関連するインターフェイスが表示されます (316 ページの「デバイス タイプの選択によって決まる設定および操作オプション」 を参照)。

アウトバンド管理の使用方法の詳細については、『HP Client Automation Out of Band Management ユーザー ガイド』を参照してください。

DASH デバイス

DASH を選択した場合、DASH 管理者がすべてのデバイスに同じユーザー名とパスワードを設定していれば、DASH デバイスに共通の認証情報を入力することができます。

認証情報の入力を間違えたり、内容に変更があったりした場合は、次回このウィンドウにアクセスしたときに認証情報を変更できます。

vPro デバイス

vPro デバイスを選択した場合、vPro デバイスにアクセスするための SCS ログイン認証情報、および SCS サービスとリモート設定の URL を入力する必要があります。

認証情報の入力を間違えたり、内容に変更があったりした場合は、次回このウィンドウにアクセスしたときに認証情報を変更できます。

両方

両方のタイプのデバイスを選択した場合、DASH デバイスの共通認証情報を入力できます。また、vPro デバイスにアクセスするために必要な SCS ログイン認証情報、および SCS サービスとリモート設定の URL を入力する必要があります。

詳細については、『HPCA Out of Band Management ユーザー ガイド』の管理タスクでのデバイス タイプの選択に関する章を参照してください。

デバイス タイプの選択によって決まる設定および操作オプション

デバイス タイプを選択したら、[設定] タブと [操作] タブに選択内容を反映したオプションが表示されます。次の表に、オプションの要約を示します。

表 43　設定と操作のオプション

	DASH	vPro
Configuration	追加オプションなし	vPro システム保護の設定
オペレーション	デバイス管理	vPro デバイスのプロビジョニング グループ管理 警告の通知

デバイス タイプを選択したり、選択内容を変更したりしたときに、[設定] タブと [操作] タブのナビゲーション パネルにデバイス タイプ関連のオプションを表示するには、HPCA Console からログアウトし、再度ログインする必要があります。

vPro システム保護の設定

vPro デバイスおよびデバイス グループのシステム防御機能を管理するには、[vPro システム保護の設定] を定義する必要があります。

この設定オプションは、vPro デバイス タイプを選択した場合にのみ表示されます。システム防御設定は、DASH デバイスには適用されません。

- **システム防御フィルタの管理**
  vPro デバイスでは、システム防御フィルタを作成、変更、および削除できます。システム防御フィルタにより、ネットワーク上のパケットの流れが監視され、フィルタ条件が一致するとパケットのドロップやパケット レートの制限が可能になります。フィルタは、システム防御ポリシーに割り当てられ、ポリシーを有効化してネットワークを保護することができます。

- **システム防御ポリシーの管理**
  vPro デバイスでは、システム防御ポリシーを作成、変更、および削除し、そのポリシーをネットワーク上の複数の vPro デバイスに配布できます。システム防御ポリシーによって、ネットワークを選択的に分離し、vPro デバイスを悪意のあるソフトウェアの攻撃から保護することができます。
- **システム防御ヒューリスティック情報の管理**
  vPro デバイスでは、ヒューリスティック仕様を作成、変更、および削除して、そのヒューリスティックをネットワーク上の複数の vPro デバイスに配布できます。これらのヒューリスティックにより、ワームの侵入を示す状況が検出され、他のデバイスが感染しないようにそのデバイスが制御されることで、ネットワーク上のデバイスが保護されます。
- **システム防御ウォッチドッグの管理**
  vPro デバイスでは、エージェント ウォッチドッグを作成、変更、および削除して、そのウォッチドッグをネットワーク上の複数の vPro デバイスに配布できます。エージェント ウォッチドッグは、vPro デバイス上のローカル エージェントが存在しているかどうかを監視します。ローカル エージェントの状態に変更があった場合にエージェント ウォッチドッグが取るアクションを指定できます。

  詳細については、『HPCA Out of Band Management ユーザー ガイド』の管理タスクでの vPro システム防御の設定に関する章を参照してください。

HPCA Console で vPro デバイスのシステム防御機能を管理できるようにするために [設定] タブで実行する管理タスクはこれで終わりです。オペレータまたは管理者ロールのユーザーは、[操作] タブに移動して、ネットワークの OOB デバイスの管理を始めることができます (「オペレーション」の章を参照)。

OS 管理

オペレーティング システム サービス機能を設定するには、[オペレーティング システム] 領域を使用します。OS 管理の詳細については、『OS Manager ガイド』を参照してください。

- 設定 318 ページ

設定

オペレーティング システム サービスを使用すると、エージェントが HPCA Server に接続し、OS エンタイトルメントおよびプロビジョニング情報を取得できます。Core でこのサービスが無効になっている場合、この情報をリクエストする Satellite またはエージェントはこの情報を使用できません。OS 管理の詳細については、『OS Manager ガイド』を参照してください。

- オペレーティング システム サービスを有効にするには、チェック ボックスを選択してから **[保存]** をクリックします。

OS 配布中、ネットワーク内のデバイスのブートを計画している場合は、最初に Core と一緒にインストールされた Boot Server (PXE/TFTP) を有効にする必要があります。これにより、Core サーバーで、Boot Server (PXE) と Boot Server (TFTP) という 2 つの Windows サービスが開始されます。

- Boot Server (PXE/TFTP) を有効にするには、チェック ボックスを選択してから **[保存]** をクリックします。

ダッシュボード

ダッシュボードを設定するには、次に示す [設定] タブの [ダッシュボード] 領域を使用します。

「HPCA 操作」ダッシュボードでは、一定期間に発生したクライアント接続数とサービス イベント数に関する情報が提供されます。

「脆弱性管理」ダッシュボードでは、企業内のクライアント デバイスのセキュリティ脆弱性に関するデータが提供されます。

「適用状況管理」ダッシュボードでは、企業内の管理対象クライアント デバイスが FDCC などの規制標準にどの程度準拠しているかについての情報が提供されます。

「セキュリティ ツール管理」ダッシュボードには、企業内の管理対象クライアント デバイスにインストールされているスパイウェア対策、ウイルス対策、およびソフトウェア ファイアウォール製品に関する情報が表示されます。

「パッチ管理」ダッシュボードでは、企業内のクライアント デバイスのパッチ ポリシー適用状況に関するデータが提供されます。

デフォルトでは、有効になるのはダッシュボード ペインの一部です。管理者権限のあるユーザーは、すべてのペインを有効または無効にできます。

HPCA 操作

HPCA 操作ダッシュボードには、企業内で HPCA が実行中の作業が表示されます。また、2 つの期間のクライアント接続およびサービス イベントの指標が表示されます。エグゼクティブ ビューには、最新の 12 か月が表示されます。操作ビューには、最新の 24 時間が表示されます。どちらのビューにも、次の情報ペインが含まれます。

クライアント接続 90 ページ

サービス イベント 92 ページ

エグゼクティブ ビューには、次のペインも含まれます。

ドメイン別 12 か月サービス イベント 94 ページ

デフォルトではこれらのペインがすべて表示されます。設定を使用して、ダッシュボードに表示するペインを指定できます。これらのペインの詳細については、89 ページの「HPCA オペレーション ダッシュボード」を参照してください。

HPCA 操作ダッシュボードを設定するには次の手順を実行します。

1 [設定] タブで、**[ダッシュボード]** をクリックします。

2 [ダッシュボード] の下で、**[HPCA 操作]** をクリックします。

デフォルトではこのダッシュボードが有効になっています。無効にするには、**[HPCA オペレーション ダッシュボードの有効化]** ボックスをオフにし、**[保存]** をクリックします。

3 [HPCA 操作] の下で、**[エグゼクティブ ビュー]** または **[操作ビュー]** をクリックします。

4 ダッシュボードに表示するペインごとにボックスを選択します。ペインごとに必要な関連 HPCA 設定に関する情報を表示するには、? アイコンを使用します。

5 **[保存]** をクリックして、変更内容を実装します。

脆弱性管理

脆弱性管理ダッシュボードでは、ネットワーク内の管理対象クライアント デバイスで検出された、一般的に認知されているセキュリティ脆弱性に関する情報が提供されます。

脆弱性管理ダッシュボードのエグゼクティブ ビューには、次の 4 つの情報ペインが含まれます。

- 重大度別にした脆弱性の影響 (円グラフ) 97 ページ

- 脆弱性履歴の評価 99 ページ
- 重大度別にした脆弱性の影響 (棒グラフ) 107 ページ
- 脆弱性の影響 101 ページ

操作ビューには、次の 4 つの情報ペインが含まれます。

- HP Live Network アナウンスメント 106 ページ
- 最も脆弱性の高いデバイス 109 ページ
- 最も脆弱性の高いサブネット 110 ページ
- 脆弱性のトップ 112 ページ

設定を使用して、ダッシュボードに表示するペインを指定できます。これらのペインの詳細については、96 ページの「脆弱性管理ダッシュボード」を参照してください。

HP Live Network は、脆弱性スキャナと最新の脆弱性コンテンツを HPCA に提供します。HPCA の脆弱性管理機能を使用するには、Live Network を設定する必要があります。

脆弱性管理ダッシュボードを設定するには

1 [設定] タブで、**[ダッシュボード]** をクリックします。

2 [ダッシュボード] の下で、**[脆弱性管理]** をクリックします。

デフォルトでは、このダッシュボードは有効になっています。このダッシュボードを無効にするには、**[脆弱性管理ダッシュボードの有効化]** ボックスをオフにして、**[保存]** をクリックします。

3 [脆弱性管理] の下で、**[エグゼクティブ ビュー]** または **[オペレーション ビュー]** のいずれかをクリックします。

4 ダッシュボードに表示するペインごとにボックスを選択します。ペインごとに必要な関連 HPCA 設定に関する情報を表示するには、? アイコンを使用します。

次のペインには追加情報が必要です。

— **脆弱性の影響 (エグゼクティブ ビュー)**
グラフに表示する脆弱性のデフォルト有効期限を指定します。たとえば、90 日を入力すると、直近の 90 日間にパブリッシュされた脆弱性のみがグラフに表示されます。デフォルト値は 45 日です。

— **HP Live Network アナウンスメント (オペレーション ビュー)**
HP Live Network 登録に関連する次の情報を入力します。

a HP Live Network RSS 通知フィードの URL

b HP Live Network 認証サーバーの完全なホスト名

現在有効なデフォルト値が提供されます。また、**[コンソール設定]** ページを使用してプロキシ サーバーを有効にする必要がある場合もあります。

5 **[保存]** をクリックして、変更内容を実装します。

適用状況管理

適用情報管理ダッシュボードには、ネットワーク内の管理対象クライアント デバイスが、FDCC (Federal Desktop Core Configuration) 標準などのさまざまな規制標準にどれだけ準拠しているかについての情報が表示されます。

適用情報管理ダッシュボードには、エグゼクティブ ビューとオペレーション ビューの 2 つのビューがあります。

エグゼクティブ ビューには、次の情報ペインがあります。

- SCAP ベンチマークによる適用状況の要約 118 ページ
- 適用状況ステータス 116 ページ
- 適用状況評価履歴 119 ページ

オペレーション ビューには、次の情報ペインがあります。

- 上位の失敗した SCAP 規則 121 ページ
- 失敗した SCAP ルール別のデバイスのトップ 123 ページ

ダッシュボードでは、これらの任意のペインの表示 / 非表示を切り替えることができます。ペインの詳細については、115 ページの「適用情報管理ダッシュボード」を参照してください。

また、ダッシュボード全体を有効または無効にすることもできます。このダッシュボードを無効にすると、[ホーム] タブの左のナビゲーション メニューに [適用状況管理] リンクが表示されなくなります。

HP Live Network は、HPCA に適用状況スキャナと更新された適用状況のコンテンツを提供します。HPCA 適用状況管理機能を使用するには、Live Network を設定しておく必要があります。

適用情報管理ダッシュボードを設定するには

1 [設定] タブで、**[ダッシュボード]** をクリックします。

2 [ダッシュボード] の下で、**[適用状況管理]** をクリックします。

デフォルトでは、このダッシュボードは有効になっています。このダッシュボードを無効にするには、**[適用情報管理ダッシュボードの有効化]** ボックスをオフにして、**[保存]** をクリックします。

3 [適用状況管理] の下で、**[エグゼクティブ ビュー]** または **[オペレーション ビュー]** のいずれかをクリックします。

4 ダッシュボードに表示するペインごとにボックスを選択します。ペインごとに必要な関連 HPCA 設定に関する情報を表示するには、? アイコンを使用します。

5 **[保存]** をクリックして、変更内容を実装します。

セキュリティ ツール管理

「セキュリティ ツール管理ダッシュボード」には、企業内の管理対象クライアント デバイスにインストールされているスパイウェア対策、ウイルス対策、およびソフトウェア ファイアウォール製品に関する情報が表示されます。

セキュリティ ツール管理ダッシュボードには、エグゼクティブ ビューとオペレーション ビューの 2 つのビューがあります。

エグゼクティブ ビューには、次の情報ペインがあります。

- セキュリティ製品のステータス 126 ページ
- セキュリティ製品の概要 128 ページ

オペレーション ビューには、次の情報ペインがあります。

- 最新定義の更新 130 ページ
- 最新のセキュリティ製品のスキャン 131 ページ

ダッシュボードでは、これらの任意のペインの表示 / 非表示を切り替えることができます。ペインの詳細については、125 ページの「セキュリティ ツール管理ダッシュボード」を参照してください。

また、ダッシュボード全体を有効または無効にすることもできます。このダッシュボードを無効にすると、[ホーム] タブの左のナビゲーション メニューにセキュリティ ツール管理リンクが表示されなくなります。

HP Live Network は、HPCA にセキュリティ ツール スキャナと関連するコンテンツを提供します。HPCA セキュリティ管理機能を使用するには、Live Network を設定しておく必要があります。

セキュリティ ツール管理ダッシュボードを設定するには

1 [設定] タブで、**[ダッシュボード]** をクリックします。

2 [ダッシュボード] の下で、**[セキュリティ ツール管理]** をクリックします。

デフォルトでは、このダッシュボードは有効になっています。このダッシュボードを無効にするには、**[セキュリティ ツール管理ダッシュボードの有効化]** ボックスをオフにして、**[保存]** をクリックします。

3 [セキュリティ ツール管理] の下で、**[エグゼクティブ ビュー]** または **[オペレーション ビュー]** をクリックします。

4 ダッシュボードに表示するペインごとにボックスを選択します。ペインごとに必要な関連 HPCA 設定に関する情報を表示するには、? アイコンを使用します。

5 **[保存]** をクリックして、変更内容を実装します。

パッチ管理

パッチ管理ダッシュボードには、ネットワーク内の管理対象デバイスで検出された任意のパッチ脆弱性に関する情報が表示されます。デフォルトでは、パッチ管理ダッシュボードは無効になっています。

パッチ管理ダッシュボードのエグゼクティブ ビューには、次の 2 つの情報ペインがあります。

- ステータス別デバイス適用状況 (エグゼクティブ ビュー) 134 ページ
- ブリテン別デバイス適用状況 136 ページ

オペレーション ビューには、次の 3 つの情報ペインがあります。

- ステータス別デバイス適用状況 (オペレーション ビュー) 138 ページ
- Microsoft セキュリティ ブリテン 139 ページ
- 最も脆弱性の高い製品 140 ページ

設定を使用して、ダッシュボードに表示するペインを指定できます。これらのペインの詳細については、134 ページの「パッチ管理ダッシュボード」を参照してください。

パッチ管理ダッシュボードを設定するには

1 [設定] タブで、**[ダッシュボード]** をクリックします。

2 [ダッシュボード] の下で、**[パッチ管理]** をクリックします。

デフォルトでは、このダッシュボードは無効になっています。このダッシュボードを有効にするには、**[パッチ管理ダッシュボードの有効化]** ボックスをオンにして、**[保存]** をクリックします。

3 [パッチ管理] の下で、**[エグゼクティブ ビュー]** または **[オペレーション ビュー]** のいずれかをクリックします。

4 ダッシュボードに表示するペインごとにボックスを選択します。ペインごとに必要な関連 HPCA 設定に関する情報を表示するには、アイコンを使用します。

[Microsoft セキュリティ ブリテン] (オペレーション ビュー) ペインには追加情報が必要です。Microsoft セキュリティ ブリテン RSS フィードの URL を指定します (現在有効なデフォルトの URL が提供されます)。また、**[コンソール設定]** ページでプロキシ サーバーを有効にする必要がある場合もあります。

5 **[保存]** をクリックして、変更内容を実装します。

9 メタデータを使用したパッチ管理

このリリースでは、パッチの更新を取得してエージェント デバイスに配信するための軽量モデルが採用されています。このモデルではメタデータのみを使用してエージェントのパッチ スキャンを行うため、メタデータを使用したパッチ管理と呼ばれています。

この章では、メタデータを使用したパッチ管理を活用するために必要な概念、設定、および実装の詳細について説明します。

メタデータを使用したパッチ管理は、次の環境でのみ実行できます。

- Microsoft Update Catalog データ フィードを使用する Microsoft オペレーティング システム
- HPCA Core および Satellite エンタープライズ レベルの環境

トピックには次の内容が含まれます。

概要

現在、メタデータを使用したパッチ管理の軽量モデルは、Microsoft デバイスのパッチ適用に使用でき、それには Microsoft Update Catalog フィードを使用する必要があります。

このモデルには、327 ページの図 46 で示すように次のような利点があります。

メタデータ パッチ管理モデルは、次の点で従来の HPCA パッチ適用モデルと異なります。

1 Core サーバーの Configuration Server Database (CSDB) には、実際のパッチ バイナリではなく、ブリテンのメタデータ情報のみが格納されます。

このモデルではパッチ取得の実行速度が向上し、またエージェントのパッチ探索および HPCA Server の同期では、インフラストラクチャ トラフィックの負荷も軽減されます。

2 実際のパッチ バイナリは、Core サーバーのコンポーネントであるパッチ ゲートウェイにダウンロードおよびキャッシュされます。ゲートウェイでは、エージェント マシンから最初のリクエストを受信するとパッチ バイナリがダウンロードされ、他のエージェント マシンが使用できるようにキャッシュされます。また、パッチ ゲートウェイではオプションで、ユーザーが取得を実行するときにパッチ バイナリをプレロードできます。

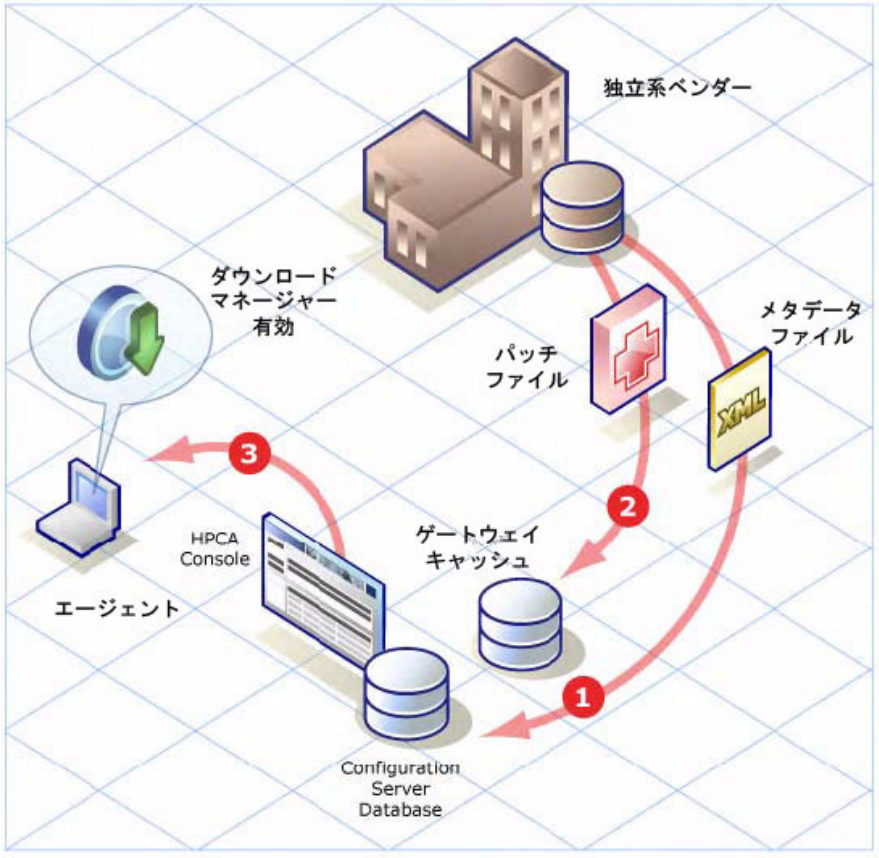
3 メタデータ モデルを使用する場合、スキャン フェーズの最後に、適用可能なパッチ バイナリのリクエストによってパッチ ゲートウェイに接続できるようにするためには、エージェントの Download Manager が有効になっている必要があります。

Download Manager では、エージェントへのパッチ ファイルの受動転送が処理されます。ファイルの転送が完了すると、パッチをインストールするためにエージェント接続が起動されます。

327 ページの図 46 に、メタデータを使用したパッチ管理モデルを示します。

比較のために、328 ページの図 47 には従来のパッチ管理モデルを示します。

図 46　メタデータを使用したパッチ管理モデル



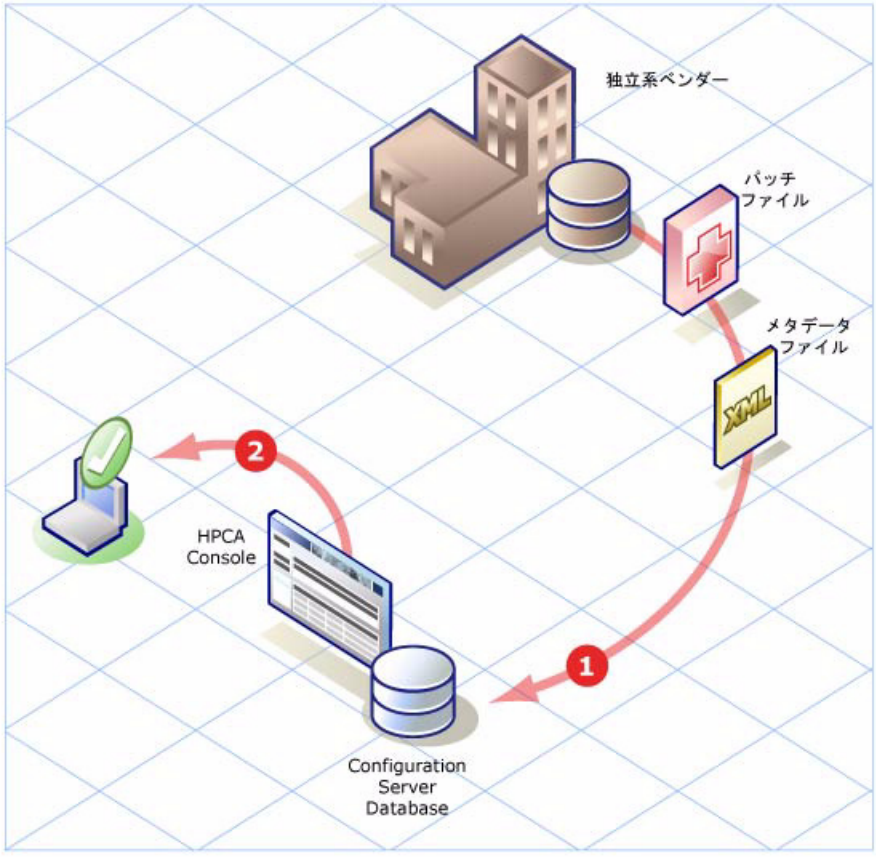
凡例 :

1　パッチ取得により、パッチのメタデータ ファイルのみがベンダーからダウンロードされます。パッチ メタデータは Core CSDB にパブリッシュされ、管理対象エージェントからリクエストされるパッチ ファイルの正確なリストを検出するために使用されます。

2　エージェント (またはオプションのプレロード) からリクエストを受信すると、パッチ ゲートウェイがベンダーからパッチ ファイルをダウンロードし、他のエージェントが使用できるようにキャッシュします。パッチ ファイルを CSDB にパブリッシュする必要はありません。

3　Patch Agent では Download Manager を有効にする必要があります。Download Manager では、エージェントへの必要なパッチ ファイルの受動ダウンロードがバックグラウンド プロセスで処理されます。

図 47　パッチ管理モデル - 従来



凡例 :

1　従来のパッチ取得では、ブリテンのメタデータとすべての関連パッチ ファイルがベンダーからダウンロードされます。これらのファイルは、企業内のエージェントに必要かどうかは関係なく、すべて Core CSDB にパブリッシュされます。

2　Patch Agent では、Download Manager オプションを使用しても使用しなくてもパッチを適用できます。使用しない場合は、エージェント接続によって、必要なパッチ ファイルのダウンロードがフォアグラウンド プロセスで処理されます。一方、Download Manager では、エージェントへの必要なパッチ ファイルの受動ダウンロードがバックグラウンド プロセスで処理されます。

関連トピック：

次のトピックでは、企業内でメタデータ配布およびパッチ管理用パッチ ゲートウェイを活用する方法について説明します。

- パッチ管理のメタデータ配布設定 (Miscrosoft のみ) 329 ページ
- エージェントのゲートウェイ アクセス設定 331 ページ
- エージェントのオフライン スキャン設定 332 ページ
- エージェントの Download Manager の設定 333 ページ
- パッチ取得およびゲートウェイ オペレーション 336 ページ

パッチ管理のメタデータ配布設定 (Miscrosoft のみ)

1 メタデータ配布はデフォルトで無効になっています。これは、Core コンソールの [設定] タブ > [パッチ管理] > [配布設定] ページで有効にします。このリリースでは、メタデータ配布は Microsoft デバイスのみで使用でき、Microsoft Update Catalog (MUC) フィードが必要です。

a Core コンソールで **[設定]** タブをクリックし、**[パッチ管理]** グループを開いて **[配布設定]** をクリックします。

[パッチ配布設定] ページが開き、[パッチ メタデータのダウンロード] 領域と [パッチ ゲートウェイ オペレーション] 領域が表示されます。

b **[パッチ メタデータのダウンロード]** 領域で次のオプションを選択します。

パッチ メタデータのみのダウンロードを有効化

注意：メタデータ配布 Microsoft を有効にすると、Patch Manager は MICROSOFT ではなく **MSFT** というベンダー フィードの使用に切り替わります。

c **[パッチ ゲートウェイ オペレーション]** 領域を使用して、Patch Manager ゲートウェイの有効化と設定を行います。ゲートウェイは Patch Manager Server のコンポーネントで、エージェントにリクエストされるパッチ バイナリ データをダウンロードし、キャッシュします。

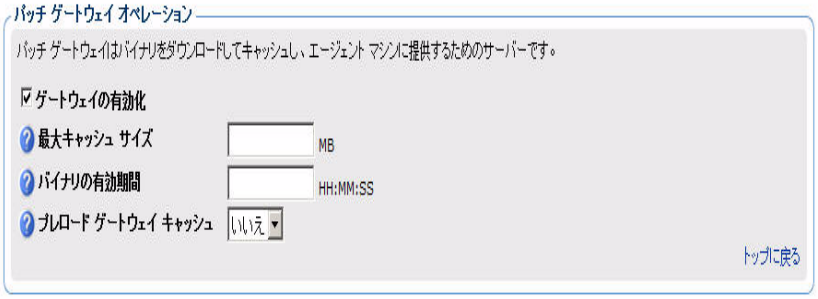
d 次を指定します。

[ゲートウェイの有効化] チェック ボックスをオンにします。メタデータ配布の場合は必ずこれをオンにします。

ゲートウェイを有効にすると、設定する追加フィールドが表示されます。

[最大キャッシュ サイズ] をメガバイト単位で指定します。キャッシュ サイズを制限しない場合は空白のままにします。

[バイナリの有効期間] の最大値を「時:分:秒」(HH:MM:SS) の形式で指定します。エージェントからリクエストされたバイナリがこれより古い場合、ゲートウェイは、そのバイナリを提供する前に新しいバージョンがないか確認します。



オプションとして、取得の実行時にパッチ バイナリをゲートウェイにキャッシュするには、**[プレロード ゲートウェイ キャッシュ]** オプションを **[はい]** に設定します。ただし、このオプションを使用する際には注意してください。

プレロードのメリットは、エージェントが特定のパッチ バイナリを初めてリクエストするとき、ゲートウェイによるダウンロードを待つ必要がない点です。

プレロードのデメリットは、エージェントで必要とされているかどうかに関係なく、収集に関連するすべてのパッチ バイナリがゲートウェイによってダウンロードされる点です。エージェントから最初のリクエストを受信するとゲートウェイでパッチ バイナリのダウンロードとキャッシュが行われるようにするには (オンデマンド ダウンロード)、[プレロード ゲートウェイ キャッシュ] オプションを **[いいえ]** のままにします。

e **[保存]** をクリックして、設定を保存します。

2 [設定] タブの [パッチ管理] 領域の **[取得ジョブ]** パネルで、ブリテンを取得するためのジョブを定義します。このタスクは、メタデータ配布を使用してもしなくても同じです。

3 次に、Core および Satellite サーバーがサービス アクセス プロファイル (SAP) で定義されていることを確認します。詳細については、30 ページの「クライアント オペレーション プロファイルの設定」を参照してください。

メタデータを使用したパッチ管理およびゲートウェイの場合、P のロールを含む Core および Satellite サーバーに対して通常タイプが DATA で作成される SAP エントリを検証するには、HPCA Administrator CSDB Editor を使用します。

P ロールは、パッチ バイナリのエージェント リクエストを Patch Manager ゲートウェイに渡します。

➤ タイプが DATA の SAP インスタンスに P のロールが含まれていない場合は、33 ページの「ゲートウェイを使用したパッチ配布のためのサービス アクセス プロファイルの変更」の説明に従って変更してください。

これで、サーバー側のパッチ管理のメタデータ配布設定が完了します。

Patch Agent の設定

次の手順で、クライアント オペレーション プロファイル (COP) を使用して Patch Manager ゲートウェイにアクセスできるように Patch Agent を設定し、パッチ バイナリのサイレント プレロードを有効にします。これらの手順については次に説明します。

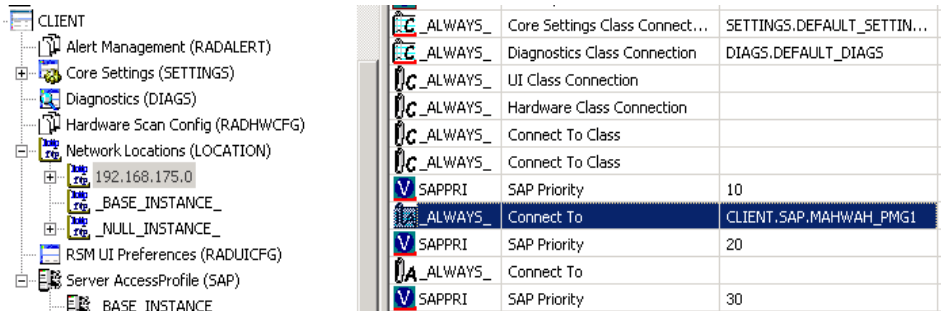
エージェントのゲートウェイ アクセス設定

Patch Manager ゲートウェイ サーバーにアクセスするために、クライアント オペレーション プロファイル (COP) および適切な Patch Manager ゲートウェイ対応サーバーを使用するように Patch Manager Agent を設定します。

1 最初に、COP を使用するようにエージェントを設定します。COP は、コンピュータ単位またはサブネット単位など、さまざまな形式に設定できます。COP の使用方法の詳細については、『HPCA Application Manager および Self-Service Manager ユーザー ガイド』、または『HPCA Application Manager および Self-Service Manager ユーザー ガイド』の「Client Domain」の章を参照してください。

2 エージェント マシンの COP を設定したら、データ配信の SAP エントリ (TYPE が DATA) に P のロールが含まれており、適切な PRIMARY.CLIENT.LOCATION インスタンスに関連付けられていることを確認します。

次の設定例では、データ配信の SAP インスタンスに PRIMARY.CLIENT.SAP.MAHWAH_PMG1 という名前が付けられ、ネットワーク サブネットの PRIMARY.CLIENT.LOCATION に関連付けられています。お使いの環境では、設定が異なる可能性があります。



3 COP=Y を含むようにエージェント接続パラメータを変更します。詳細については、『HPCA Application Manager および Application Self-Service Manager ユーザー ガイド』を参照してください。

これで、MSFT フィードを使用したメタデータ配布と COP を使用した Patch Manager ゲートウェイのセットアップが完了します。

エージェントのオフライン スキャン設定

メタデータ取得モデルでパッチを管理する場合、MSFT ベンダーの取得ファイルがエージェントにダウンロードされると、ネットワーク、あるいは HPCA Core または Satellite サーバーへの接続に依存せずに、スキャン フェーズが開始されます。

スキャン フェーズが終了すると、適用状況に従うために各エージェントに必要なパッチ バイナリのリストが利用可能になります。

エージェントによって Download Manager が起動され、ネットワーク接続が確立されるとバイナリ ファイルのプレロードが開始します。

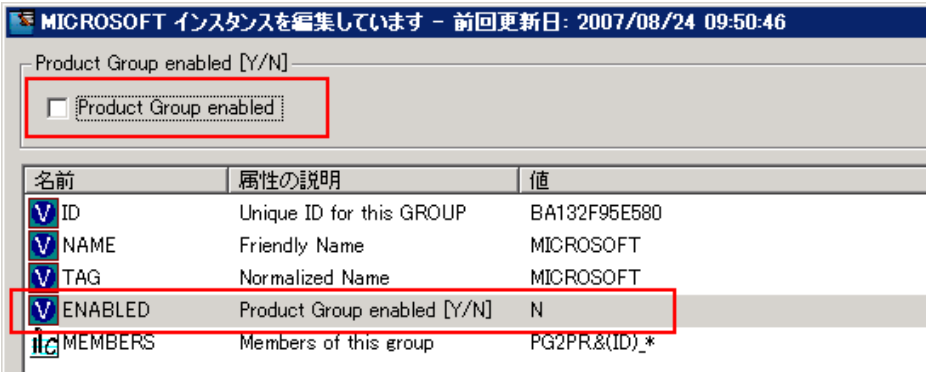
オフライン スキャン要件

バージョン 7.50 のエージェントには、パッチのオフライン スキャン機能が組み込まれており、次の条件下で自動的に有効になります。メタデータを使用したパッチ管理を使用する場合は、これらのオフライン スキャン条件を満たしていることを確認してください。

- [パッチ管理] > [配布設定] で **[パッチ メタデータのダウンロード]** を有効にします。
- [パッチ管理] > [エージェント オプション] で **[Download Manager]** を有効にします。詳細については、333 ページの「エージェントの Download Manager の設定」を参照してください。
- Core の Configuration Server Database で次のエントリが無効になっている必要があります。
  - PRIMARY.PATCHMGR.PROGROUP クラスの MICROSOFT インスタンスが無効になっている必要があります。この設定については、次で説明します。

PATCHMGR.PROGROUP クラスの MICROSOFT インスタンスを無効にするには

1. Core サーバーで、HPCA Administrator CSDB Editor にログインします。
2. PRIMARY.PATCHMGR.PROGROUP クラスの MICROSOFT インスタンスに移動します。
3. 次の図に示すように、チェック マークを編集および削除して Product Group Enabled 属性を N に設定します。



エージェントでオフライン スキャンを実行できるようにするためには、必ずこの Enabled 属性を N に設定してください。

エージェントの Download Manager の設定

メタデータ配布では、エージェントは、スキャン フェーズの最後にパッチ ゲートウェイからダウンロードするバイナリ ファイル セットをリクエストします。

Download Manager を使用できるように Patch Agent を設定する必要があります。Download Manager はバックグラウンドでサイレントに動作し、非同期プロセスとしてエージェントにパッチ ファイルをダウンロードします。Download Manager ではこの受動ファイル転送を必要に応じて停止および開始でき、停止した時点からダウンロードを続行します。

Patch Agent で Download Manager を有効にすると、エージェントへのバイナリのダウンロード方法を制御する複数のオプションを設定できます。Download Manager のオプションには、通常モードおよびスクリーン セーバー モードでのネットワーク利用、初期化後の遅延、およびダウンロード完了後のパッチ更新の適用があります。

Download Manager オプションはデフォルトで無効になっています。オプションを有効にするには、コンソールの **[設定]** タブ > **[パッチ管理]** 領域 > **[エージェント オプション]** ページを使用します。詳細については次に説明します。

コンソールで Download Manager を有効にし、オプションを保存すると、CSDB Database の Patch Manager の DISCOVER インスタンスが変更され、選択内容が反映されます。

Download Manager を使用できるように Patch Agent を設定するには

Download Manager を有効にし、関連オプションを設定するには、コンソールの [設定] タブ > [パッチ管理] 領域 > [エージェント オプション] ページを使用します。

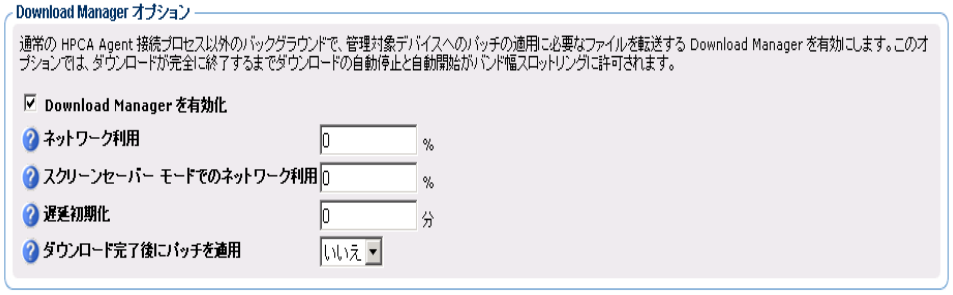
パッチのメタデータ配布を使用して Microsoft デバイスにパッチを適用するには、Download Manager を有効にする必要があります。

1. コンソールの **[設定]** タブで **[パッチ管理]** および **[エージェント オプション]** をクリックします。
2. [エージェント オプション] ページで、[Download Manager オプション] 領域に移動します。
3. **[Download Manager を有効化]** チェック ボックスをオンにします。

   オンにすると、Download Manager オプションが表示されます。
4. Download Manager オプションを設定します。ネットワーク利用、スクリーン セーバー モードでのネットワーク利用、初期化後の遅延、およびダウンロード完了後のパッチ適用の有無を指定するオプションを設定します。

   これらのオプションの設定の詳細については、291 ページの「エージェント オプション」を参照してください。

例 : 次のエントリは、デバイス動作中は最大 34% のネットワーク利用率、スクリーン セーバー モードでは最大 45% のネットワーク利用率、および初期化後遅延が 45 分で、Patch Agent の Download Manager を有効にします。パッチ ファイルがダウンロードされると、次回の Patch Agent 接続時に適用が可能になります。



5 オプションとして、[エージェント オプション] 領域で次のエージェント オプションを設定できます。

— 自動更新を無効化

— ソフトウェア配布フォルダの削除

これらのオプションの設定の詳細については、291 ページの「エージェント オプション」を参照してください。

注意: Patch Agent のオプションを保存すると、Configuration Server Database ですべてのメソッド (作成、削除、検証、更新、修復) の Patch Manager の DISCOVER インスタンスが変更されます。

6 **[保存]** をクリックして、変更を保存します。

パッチに対するエージェントのエンタイトルメント設定

標準のパッチ展開手順を使用して、適切なパッチに対するエンタイトルメントをエージェントに設定します。詳細については、管理に関する章のトピックを参照してください。

Patch Agent では、適用可能なパッチ ファイルの非同期転送を行う Download Manager のバックグラウンド プロセスを利用して、適用可能なバイナリがパッチ ゲートウェイを経由してダウンロードされます。

Patch Agent では、それらのサービスのエンタイトルメントが設定されていない限り、パッチ バイナリは受信されません。

ゲートウェイは、リクエストされたパッチ ファイルを取得すると、他のエージェントが使用できるようにそれらをキャッシュします。

パッチ取得およびゲートウェイ オペレーション

メタデータを使用したパッチ取得は軽量であるため、つまり、CSDB にはパッチ情報のみダウンロードおよびパブリッシュされるので、平均すると数分で終了します。

1 収集を実行するには、[操作] タブの [パッチ管理] 領域を使用します。

コンソールの [操作] タブをクリックして、[パッチ管理] グループに移動します。**[取得を開始]** を選択します。

取得後、CSDB には実際のパッチ バイナリ データではなく、パッチのメタデータ情報のみが含まれます。

2 オプションとして、取得のステータスを表示できます。

コンソールの [操作] タブをクリックします。[パッチ管理] グループを展開し、**[取得ステータスをレポート]** をクリックします。

3 標準のパッチ展開手順を使用して、適切なパッチに対するエンタイトルメントをエージェントに設定します。

Patch Agent はパッチ ゲートウェイを経由して適用可能なバイナリをダウンロードします。ゲートウェイは、他のクライアントが使用できるようにバイナリをキャッシュします。

4 ゲートウェイでファイルがダウンロードおよびキャッシュされると、使用可能なパッチ URL が [キャッシュ ファイルの統計値] ページに表示されます。

コンソールからこのページにアクセスするには、[操作] をクリックし、[Patch Manager]、[ゲートウェイ オペレーション]、**[キャッシュ ファイルの統計値]** の順に選択します。

10 OS イメージの準備と取得

この章では、ご使用の環境で、オペレーティング システム イメージを準備または取得し、デバイスに配布する方法について説明します。取得したイメージは、HPCA Server の \upload ディレクトリにアップロードされます。次に Publisher を使用して、イメージを HPCA DB に保存する必要があります。オペレーティング システムは、後で Console を使用して適切なターゲット デバイスに配布できます。

既存の .WIM イメージを使用しているか、または Microsoft WAIK で新規のイメージを作成する場合は、イメージを取得する必要はありませんから、次の章に進みます。

Windows オペレーティング システムのイメージについては、次のセクションを参照してください。

- イメージの準備と取得 338 ページ
- Microsoft Sysprep の使用 355 ページ
- Image Preparation Wizard について 358 ページ

シン クライアント オペレーティング システムについては、次を参照してください。

- シン クライアント イメージの準備と取得 367 ページ

イメージの準備と取得

OS イメージを準備または取得する手順は、オペレーティング システムと配布メソッドによって異なります。

シン クライアント イメージの準備と取得の手順については、367 ページの「シン クライアント イメージの準備と取得」を参照してください。

サポートされているディスク暗号化製品を使用する場合は、暗号化されていないパーティションからイメージを取得する必要があります。

レガシー配布用の Windows Vista 以前の取得

次の手順では、レガシー配布用に Windows Vista 以前のオペレーティング システムを準備して取得する方法を説明します。

タスク 1: 参照マシンの準備

1 オリジナル製品メディアから、オペレーティング システムをインストールします。参照マシンは、インストールするオペレーティング システムを実行できる必要があります。参照マシンが DHCP を使用していることを確認します。

OS は、C: ドライブに保存します (C: ドライブのみ取得されるため)。

2 必要に応じて OS をカスタマイズします。これには、基本的なまたは必要な複数のアプリケーションのインストールが含まれる場合があります。これには、OS とアプリケーションの最新のサービス パック、およびイメージの配布先となるデバイスに必要なドライバが含まれることを確認してください。次の Microsoft サポート技術情報の記事には、Windows OS のインストールに OEM ドライバを含めることに関する情報が記載されています。

http://support.microsoft.com/kb/314479/ja

3 HPCA メディアから HPCA Agent をインストールします。Agent は、OS イメージを配布するときにデバイスが HPCA Server に接続するために必要です。

4 HPCA Server へのアップロード プロセスが終了するまで、キーボードやマウスによる操作が数分間行われなくても、デバイスの電源が切れないように、BIOS の電源管理を設定してください。

5 イメージ ファイルのサイズはできるだけ小さくしておいてください。オペレーティング システムの収納に十分なパーティションの大きさに加えて、HPCA Agent 用の追加領域がある設定が理想的です。

プライマリ ブート ドライブのプライマリ ブート パーティションへのイメージの配布がサポートされます。

次の手順はイメージ ファイルのサイズを最小に抑えるのに役立ちます。

a 空き領域を作成します。

HP は、最小の空き容量で、最小のパーティションを作成した後、Sysprep.inf の [Unattended] のセクションに ExtendOemPartition = 1 を設定することを推奨します。これで、より大きなドライブを持つターゲット デバイスに小さなイメージをインストールできるようになります。ExtendOemPartition を true に設定すると、Microsoft ミニセットアップ ウィザードは、OS インストール パーティションをそのディスク上で、物理的に連続した、パーティションが設定されていない空き領域に拡張します。これで、HPCA Agent はボリューム上の空き領域をアプリケーションのインストールに使用できます。

b ラップトップを使用している場合は休止状態を無効にします。

c 必要があれば、復旧パーティションを削除します。

d ページング ファイルを無効にします。配布後、mini-setup が実行されると、ページング ファイルは、自動的に利用可能になります。

e システムの復元を無効にする。

f インデックス作成サービスとディスク圧縮を無効にします。

g On Resume Password Protect を無効にします。

タスク 2: 前提条件

1 クローン作成されたイメージを使用して Microsoft オペレーティング システムを配布するために、Microsoft Sysprep をダウンロードします。

Sysprep の使用方法、Sysprep.inf の作成方法、および利用可能なパラメータについては、Microsoft のドキュメントを確認してください。

2 Microsoft Sysprep をセットアップします。

3 Sysprep.inf を作成します。

詳細については、355 ページの「Microsoft Sysprep の使用」を参照してください。

タスク 3: Image Preparation Wizard の実行

358 ページの「Image Preparation Wizard について」を参照してください。

ImageX 配布用の Windows Vista 以前の取得

次の手順では、ImageX 配布用に Windows Vista 以前のオペレーティング システムを準備して取得するプロセスを説明します。

タスク 1: HPCA Server へのユーティリティのコピー

ImageX で配布するイメージを取得するには、HPCA Server に次のユーティリティをコピーします。

1. C:\Program Files\Windows AIK\Tools\PETools\x86 にある bootsect.exe を C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\OSM\SOS\winpe\utilities\Program Files にコピーします。
2. C:\Program Files\Windows AIK\Tools\x86 にある imagex.exe を C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\OSM\SOS\winpe\utilities\Program Files にコピーします。

Windows AIK は、Microsoft Web サイトから入手できます。通常の Vista インストールには含まれていません。

タスク 2: 参照マシンの準備

1. オリジナル製品メディアから、オペレーティング システムをインストールします。参照マシンは、インストールするオペレーティング システムを実行できる必要があります。参照マシンが DHCP を使用していることを確認します。

OS は、C: ドライブに保存します (C: ドライブのみ取得されるため)。

必要に応じて OS をカスタマイズします。これには、基本的なまたは必要な複数のアプリケーションのインストールが含まれる場合があります。これには、OS とアプリケーションの最新のサービス パック、およびイメージの配布先となるデバイスに必要なドライバが含まれることを確認してください。

2. HPCA Server へのアップロード プロセスが終了するまで、キーボードやマウスによる操作が数分間行われなくても、デバイスの電源が切れないように、BIOS の電源管理を設定してください。
3. WIM ファイルのサイズを抑えるために、ファイル システムのサイズをできるだけ小さくして下さい。

プライマリ ブート ドライブのプライマリ ブート パーティションへのイメージの配布がサポートされます。

a. ファイル システムから、必須ではないファイルとディレクトリを削除します。
b. システムの復元を無効にする。

タスク 3: 前提条件

1 クローン作成されたイメージを使用して Microsoft オペレーティング システムを配布するために、Microsoft Sysprep をダウンロードします。

Sysprep の使用方法、Sysprep.inf の作成方法、および利用可能なパラメータについては、Microsoft のドキュメントを確認してください。

2 Microsoft Sysprep をセットアップします。

3 Sysprep.inf を作成します。

詳細については、355 ページの「Microsoft Sysprep の使用」を参照してください。

タスク 4: Image Preparation Wizard の実行

358 ページの「Image Preparation Wizard について」を参照してください。

ImageX 配布用の Windows Vista の取得

次の手順では、ImageX 配布用に Windows Vista オペレーティング システムを準備して取得するプロセスを説明します。

タスク 1: HPCA Server へのユーティリティのコピー

ImageX で配布するイメージを取得するには、HPCA Server に次のユーティリティをコピーします。

1 C:\Program Files\Windows AIK\Tools\PETools\x86 にある bootsect.exe を C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\OSM\SOS\winpe\utilities\Program Files にコピーします。

2 C:\Program Files\Windows AIK\Tools\x86 にある imagex.exe を C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\OSM\SOS\winpe\utilities\Program Files にコピーします。

Windows AIK は、Microsoft Web サイトから入手できます。通常の Vista インストールには含まれていません。

タスク 2: 参照マシンの準備

1 オリジナル製品メディアから、オペレーティング システムをインストールします。参照マシンは、インストールするオペレーティング システムを実行できる必要があります。参照マシンが DHCP を使用していることを確認します。

OS は、C: ドライブに保存します (C: ドライブのみ取得されるため)。

必要に応じて OS をカスタマイズします。これには、基本的なまたは必要な複数のアプリケーションのインストールが含まれる場合があります。これには、OS とアプリケーションの最新のサービス パック、およびイメージの配布先となるデバイスに必要なドライバが含まれることを確認してください。

2 HPCA Server へのアップロード プロセスが終了するまで、キーボードやマウスによる操作が数分間行われなくても、デバイスの電源が切れないように、BIOS の電源管理を設定してください。

3 User Access Control を無効にします。

4 WIM ファイルのサイズを抑えるために、ファイル システムのサイズをできるだけ小さくして下さい。

プライマリ ブート ドライブのプライマリ ブート パーティションへのイメージの配布がサポートされます。

a ファイル システムから、必須ではないファイルとディレクトリを削除します。

b システムの復元を無効にする。

タスク 3: unattend.xml の作成

Image Capture メディアの samples\unattend\vista\x86 から、C:\windows\system32\sysprep に、サンプル unattend.xml をコピーします。このファイルは、お使いの環境に合わせて変更が必要な場合があります。

タスク 4: Image Preparation Wizard の実行

358 ページの「Image Preparation Wizard について」を参照してください。

ImageX 配布用の Windows Server 2008 の取得

次の手順では、ImageX 配布用に Windows Server 2008 オペレーティング システムを準備して取得するプロセスを説明します。

タスク 1: HPCA Server へのユーティリティのコピー

ImageX で配布するイメージを取得するには、HPCA Server に次のユーティリティをコピーします。

1. C:\Program Files\Windows AIK\Tools\PETools\x86 にある bootsect.exe を C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\OSM\SOS\winpe\utilities\Program Files にコピーします。
2. C:\Program Files\Windows AIK\Tools\x86 にある imagex.exe を C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\OSM\SOS\winpe\utilities\Program Files にコピーします。

Windows AIK は、Microsoft Web サイトから入手できます。通常の Vista インストールには含まれていません。

タスク 2: 参照マシンの準備

1. オリジナル製品メディアから、オペレーティング システムをインストールします。参照マシンは、インストールするオペレーティング システムを実行できる必要があります。参照マシンが DHCP を使用していることを確認します。

OS は、C: ドライブに保存します (C: ドライブのみ取得されるため)。

必要に応じて OS をカスタマイズします。これには、基本的なまたは必要な複数のアプリケーションのインストールが含まれる場合があります。これには、OS とアプリケーションの最新のサービス パック、およびイメージの配布先となるデバイスに必要なドライバが含まれることを確認してください。

2 HPCA Server へのアップロード プロセスが終了するまで、キーボードやマウスによる操作が数分間行われなくても、デバイスの電源が切れないように、BIOS の電源管理を設定してください。

3 WIM ファイルのサイズを抑えるために、ファイル システムのサイズをできるだけ小さくして下さい。

プライマリ ブート ドライブのプライマリ ブート パーティションへのイメージの配布がサポートされます。

a ファイル システムから、必須ではないファイルとディレクトリを削除します。

b システムの復元を無効にする。

タスク 3: unattend.xml の作成

Image Capture メディアの samples\unattend\vista\x86 から、C:\windows\system32\sysprep に、サンプル unattend.xml をコピーします。このファイルは、お使いの環境に合わせて変更が必要な場合があります。

タスク 4: Image Preparation Wizard の実行

358 ページの「Image Preparation Wizard について」を参照してください。

Windows セットアップ配布用の Windows Vista 以前の取得

Windows セットアップ配布用の Windows Vista 以前のイメージの取得および配布は、HPCA Starter および Standard ではサポートされていません。

この場合のみ、HPCA Windows Native Install Packager を使用してイメージを準備します。イメージは、参照マシンのハード ドライブ上の、Windows Vista 以前のオペレーティング システムのインストール メディアのイメージです。作成されるイメージは、Windows のインストールのファイル コピー フェーズを完了しており、HPCA Agent が含まれています。このイメージは HPCA Server の \upload ディレクトリに送信されます。次に、Admin Publisher を使用して、イメージを Configuration Server DB にパブリッシュします。

イメージがターゲット デバイスに配布されると、ターゲット デバイスは再起動します。Windows Native Install セットアップは引き続きテキスト モード セットアップ フェーズを実行し、その後 GUI フェーズを実行します。2 つのフェーズは Unattend.txt で制御され、完全自動セットアップが可能です。

タスク 1: 参照マシンの準備

参照マシン上で作成されたオリジナルのインストール メディアのイメージがターゲット デバイスに配布されます。HPCA Windows Native Install Packager を使用してイメージを作成する前に、HPCA メディアを持っていることと、参照マシンが次の条件を満たしていることを確認します。

1 HPCA Server に接続できる。

2 以下の条件を満たすターゲット ドライブ (拡張パーティションにあることを推奨)。

— ターゲット ドライブは現在フォーマットされており、空である (データがない) かのように扱われる。ターゲット ドライブがフォーマットされていない場合か、あるいはフォーマットされているが、データが含まれている場合に、ユーザーはドライブをフォーマットするよう要求されます。

— ユーザーがドライブにデータが確実に残らないようにドライブをフォーマットする場合は、あらかじめ FAT32 でフォーマットできる。

FAT32 では一度配布すると、拡張できないので注意してください。NTFS は拡張できるデフォルトのオプションです。

- 1.5 GB 以上。Image Preparation Wizard の [未使用のディスク スペースの圧縮を最適化する] チェック ボックスがどのように設定されているかによって、ターゲット ドライブが大きくなれば、ドライブのイメージ化の処理時間が長くなる、または、イメージが必要以上に大きくなる場合があります。

ターゲット ドライブに保存するすべてのデータが失われます。

3 HPCA Windows Native Install Packager ソフトウェアが既にインストールされている、C: ドライブなどの独立したドライブ (高速化のため)。348 ページの「タスク 3: HPCA Windows Native Install Packager のインストール」を参照してください。

4 また、次のアイテムにアクセスする権限が必要です。HPCA Windows Native Install Packager を使用する場合は、アイテムのロケーションを指定します。

— HPCA Agent のセットアップ ファイル。

— オペレーティング システム メディアの i386 ディレクトリ。

必要なサービス パックは、すべてこのディレクトリにスリップストリームできます。これを実行する方法の詳細については、各サービス パックに関連する readme.txt ファイルを参照してください。

Windows セットアップで、古いバージョンの Windows 用のセットアップを実行することはできません。次に例を示します。

- デバイスで Windows XP が稼働している場合は、Windows 2000 用の i386 ディレクトリを使用できません。
- デバイスで Windows 2003 が稼働している場合は、Windows 2000 用または Windows XP 用の i386 ディレクトリは使用できません。

— unattend.txt

ファイルは手動で作成するか、Windows メディアの Windows セットアップ マネージャを使用して作成できます。使用可能なサンプル ファイルは、Image Capture メディアの samples ディレクトリにあります。

タスク 2: Unattend.txt の作成

Unattend.txt では、ユーザー入力が必要ないように、OS のインストールが自動化されます。unattend.txt ファイルは i386 ディレクトリで指定されている Windows のリリースと一致している必要があります。これらのファイルはインストールされている Windows のバージョンによって、若干異なる場合があります。

Unattend.txt ファイルは、800 KB 以下にしてください。

以下は、イメージと共に保存する unattend.txt ファイルを作成するときのヒントです。

- ファイルの中の設定は、環境にあるどのデバイスでも使用できるように、できるだけ汎用的にする必要があります。
- このファイルの [GuiUnattended] セクションには、ステートメント [AutoLogon=YES] および [AutoLogonCount=1] を含めます。

HPCA Agent セットアップでは、Agent をターゲット デバイスにインストールするために Windows インストーラが使用されます。また OEM\cmdlines.txt では Windows インストーラを実行できないため、OEM\cmdlines.txt の代わりに [GuiUnattended] セクションを使用する必要があります。[AutoLogon] ステートメントと [AutoLogonCount] ステートメントを使用すると、オペレーティング システムのインストール後に初めてのユーザーがログオンするときに、Agent が確実にインストールされます。

- このファイルの [Unattended] セクションには、ステートメント [extendoempartition=1] を含めます。これにより、Windows はファイル システムとパーティションを拡張し、パーティションに続く未使用スペースを取り込むことができます。ターゲット パーティションが小さすぎる場合は、インストールのコピー フェーズを実行することはできますが (このフェーズは参照マシンで実行されます)、イメージが配布されると、テキスト モード フェーズは失敗します。あるいは、別のパーティションに OS をインストールする場合もあります。

  大きいターゲット パーティションを使用している場合は、ファイルの未使用スペースにゼロを埋めるプロセスに時間がかかります。

- 必要なカスタマイズをするには、別の unattend.txt ファイルを作成することもできます。Publisher を使用してこれらのファイルを HPCA DB の SYSPREP クラスにパブリッシュできます。次に、それらを適切な OS イメージに接続できます。イメージが配布されると、カスタマイズした unattend.txt ファイルはオリジナルのファイルに統合されます。

  ファイルをパブリッシュする方法の詳細については、パブリッシュについての章を参照してください。unattend.txt ファイルをパブリッシュするときは、Sysprep.inf ファイルをパブリッシュする場合と同じ手順に従います。

タスク 3: HPCA Windows Native Install Packager のインストール

1. Image Capture メディアで、\windows_native_install に移動して setup.exe をダブルクリックします。
2. **[次へ]** をクリックします。

   [エンド ユーザー ライセンス契約] ウィンドウが表示されます。
3. 条件を確認して、[同意する] をクリックします。
4. 製品のインストール先のディレクトリを選択して、[次へ] をクリックします。

   [要約] ウィンドウが表示されます。
5. [インストール] をクリックします。

   インストールが完了したら、**[完了]** をクリックします。

タスク 4: HPCA Windows Native Install Packager の実行

1 デスクトップにある HPCA Windows Native Install Packager アイコンをダブルクリックします。

[設定オプション] ウィンドウの [Client Automation]、[Windows セットアップ]、[パッケージ] という 3 つの領域で、情報を入力する必要があります。

a [Client Automation] 領域には、Client Automation 製品に関連する設定オプションが表示されます。

b [Windows セットアップ] 領域では、OS のインストールを実行するのに必要な情報を収集します。

c [パッケージ] 領域では、作成するパッケージに関して HPCA で必要な情報が収集されます。

これらの各ウィンドウで、入力必須フィールドに入力しないまま **[次へ]** をクリックした場合、そのフィールドに入力するように、メッセージが表示されます。

2 [Client Automation Client ソース ディレクトリ] フィールドに、HPCA Agent のパスを入力します。

3 インストールする Client Automation 製品のチェック ボックスをオンにします。

4 OS のインストール後、HPCA OS 接続を実行するには、[インストール後、最初の接続を実行] チェック ボックスをオンにします。このチェック ボックスがオンになっていないと、OS のインストール後に、HPCA OS 接続は自動的に実行されません。

5 [オプションの Packager コマンド ライン引数] ボックスに、WNI アプリケーションで使用されるパラメータを入力します。オプションは 1 行ですべてを入力することも、複数行にわたって入力することもできます。オプションは以下のような「キーワード 値」の形式で指定します。

-trace_level 9

キーワードの先頭には必ずダッシュ (-) を付けます。

テクニカル サポートの指示では、通常 [オプションの Packager コマンド ライン引数] テキスト ボックスのみを使用します。

ログを作成るためのパラメータが多数あります。以下の例は、C:\temp\nvdwni.log という名前のファイルを作成する方法を説明しています。

- "-trace_level 99
- "-trace_dir c:\temp

別の名前でログを作成する場合は、以下を使用します。

- "-trace_file filename.log

6 **[次へ]** をクリックします。

7 [unattend.txt ファイル] ボックスで、適切な unattend.txt ファイルを参照します。

イメージに保存する汎用 unattend.txt ファイルを選択します。このファイルは、イメージが適用するすべてのデバイスに適用可能なオプションを含んでいる必要があります。必要なカスタマイズをするには、イメージに個別の unattend.txt ファイルを添付することができます。

Unattend.txt ファイルは i386 ディレクトリで指定されている Windows のリリースに合致している必要があります。これらのファイルはインストールされている Windows のバージョンによって、若干異なる場合があります。

8 [i386 ディレクトリ] テキスト ボックスで、Microsoft の配布メディアで提供される Windows 配布元ディレクトリを選択します。Microsoft のスリップストリーム プロセスを使用して、サービス パックおよびその他の修正を統合できます。これを実行する方法の詳細については、各サービス パックに関連する readme.txt ファイルを参照してください。

必ず Windows CD-ROM から i386 を別のロケーションにコピーしてください。CD-ROM を使用する場合、Windows セットアップは、CD-ROM がターゲット デバイスにロードされたと想定して、必要なファイルをすべてコピーしない恐れがあります。

9 [ターゲット ドライブ] ドロップダウン リストで、ネイティブ インストール パッケージを作成するドライブを選択します。拡張パーティション上にあるドライブを選択することを推奨します。

このドライブに既存のすべてのデータが失われます。

10 [特別なコマンド ライン パラメータ] テキスト ボックスで、Windows セットアップ プログラムを実行する時に、プログラムに渡すパラメータをすべて入力します。パラメータの詳細については、Microsoft web サイトを参照してください。

11 **[次へ]** をクリックします。

12 [イメージ名] テキスト ボックスに、\upload ディレクトリに保存するパッケージの名前を入力します。この名前に入力する文字は、8 文字以内の英数字である必要があります。

13 [イメージの説明] テキスト ボックスにイメージの説明を入力します (半角 255 文字まで)。

14 [Client Automation OS Manager Server] テキスト ボックスに、イメージをアップロードする HPCA Server の IP アドレスまたはホスト名を指定します。

15 [Client Automation OS Manager ポート] テキスト ボックスに、HPCA Server のポートを指定します。

16 [未使用のディスク スペースの圧縮を最適化する] チェック ボックスをオンにし、ターゲット ドライブをイメージ化する前に、未使用ディスク スペースをすべて null にします。この設定によって、イメージのサイズを小さくすることができますが、Image Preparation Wizard の実行時間がより長くなります。

17 **[次へ]** をクリックします。

18 [要約] を確認し、**[作成]** をクリックします。

Windows 2000 デバイスで **[作成]** をクリックした後、Windows セットアップによってシステムの再起動が要求される場合があります。再起動をしない場合は、[キャンセル] をクリックします。再起動は必要ありませんが、再起動が起こっても、障害はありません。

Windows セットアップが実行され、HPCA Windows Native Install Packager に戻ります。

19 HPCA Windows Native Install Packager が完了すると、Linux CD-ROM でシステムの再起動を求めるメッセージが表示されます。これは、Image Capture メディアを指しています。

起動順は、まず CD-ROM から起動するように設定する必要があるため、注意してください。

20 イメージ キャプチャ メディアを挿入して、**[OK]** をクリックしてください。

21 **[完了]** をクリックします。

22 デバイスを再起動すると、イメージが \upload ディレクトリにアップロードされます。

23 OS イメージが正常に HPCA Server に送信されたことを示すメッセージが表示されたら、ドライブからメディアを取り出し、デバイスを再起動します。

Windows セットアップ配布用の Windows Vista の取得

次の各手順では、Winodws セットアップ配布用に Windows Vista オペレーティング システムを準備して取得するプロセスを説明します。

- タスク 1: HPCA Server へのユーティリティのコピー 352 ページ
- タスク 2: 参照マシンの準備 353 ページ
- タスク 3: Image Preparation Wizard の実行 353 ページ

タスク 1: HPCA Server へのユーティリティのコピー

Windows セットアップで配布するイメージを取得するには、HPCA Server に次のユーティリティをコピーします。

1 C:\Program Files\Windows AIK\Tools\PETools\x86 にある bootsect.exe を C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\OSM\SOS\winpe\utilities\Program Files にコピーします。

2 C:\Program Files\Windows AIK\Tools\x86 にある imagex.exe を C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\OSM\SOS\winpe\utilities\Program Files にコピーします。

Windows AIK は、Microsoft Web サイトから入手できます。通常の Vista インストールには含まれていません。

タスク 2: 参照マシンの準備

1 オリジナル製品メディアから、オペレーティング システムをインストールします。参照マシンは、インストールするオペレーティング システムを実行できる必要があります。参照マシンが DHCP を使用していることを確認します。

OS は、C: ドライブに保存します (C: ドライブのみ取得されるため)。

必要に応じて OS をカスタマイズします。これには、基本的なまたは必要な複数のアプリケーションのインストールが含まれる場合があります。これには、OS とアプリケーションの最新のサービス パック、およびイメージの配布先となるデバイスに必要なドライバが含まれることを確認してください。

2 HPCA Server へのアップロード プロセスが終了するまで、キーボードやマウスによる操作が数分間行われなくても、デバイスの電源が切れないように、BIOS の電源管理を設定してください。

3 User Access Control を無効にします。

4 WIM ファイルのサイズを抑えるために、ファイル システムのサイズをできるだけ小さくして下さい。

プライマリ ブート ドライブのプライマリ ブート パーティションへのイメージの配布がサポートされます。

a ファイル システムから、必須ではないファイルとディレクトリを削除します。

b システムの復元を無効にする。

タスク 3: Image Preparation Wizard の実行

358 ページの「Image Preparation Wizard について」を参照してください。

Windows セットアップ配布用の Windows Server 2008 の取得

次の各手順では、Winodws セットアップ配布用に Windows Server 2008 オペレーティング システムを準備して取得するプロセスを説明します。

タスク 1: HPCA Server へのユーティリティのコピー

Windows セットアップで配布するイメージを取得するには、HPCA Server に次のユーティリティをコピーします。

1. C:\Program Files\Windows AIK\Tools\PETools\x86 にある bootsect.exe を C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\OSM\SOS\winpe\utilities\Program Files にコピーします。
2. C:\Program Files\Windows AIK\Tools\x86 にある imagex.exe を C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\OSM\SOS\winpe\utilities\Program Files にコピーします。

Windows AIK は、Microsoft Web サイトから入手できます。通常の Vista インストールには含まれていません。

タスク 2: 参照マシンの準備

1. オリジナル製品メディアから、オペレーティング システムをインストールします。参照マシンは、インストールするオペレーティング システムを実行できる必要があります。参照マシンが DHCP を使用していることを確認します。

OS は、C: ドライブに保存します (C: ドライブのみ取得されるため)。

必要に応じて OS をカスタマイズします。これには、基本的なまたは必要な複数のアプリケーションのインストールが含まれる場合があります。これには、OS とアプリケーションの最新のサービス パック、およびイメージの配布先となるデバイスに必要なドライバが含まれることを確認してください。

2. HPCA Server へのアップロード プロセスが終了するまで、キーボードやマウスによる操作が数分間行われなくても、デバイスの電源が切れないように、BIOS の電源管理を設定してください。
3. WIM ファイルのサイズを抑えるために、ファイル システムのサイズをできるだけ小さくして下さい。

プライマリ ブート ドライブのプライマリ ブート パーティションへのイメージの配布がサポートされます。

a. ファイル システムから、必須ではないファイルとディレクトリを削除します。
b. システムの復元を無効にする。

4 Image Capture メディアから Image Preparation Wizard を実行する場合、起動順序を CD-ROM 優先に設定します。他のロケーションから Image Preparation Wizard を実行する場合、起動順序をネットワーク優先に設定します。

タスク 3: Image Preparation Wizard の実行

358 ページの「Image Preparation Wizard について」を参照してください。

Microsoft Sysprep の使用

ゴールド イメージ作成の最終手順で、Image Preparation Wizard によって Microsoft Sysprep が起動されます。これにより、ゴールド イメージのセキュリティ識別子がすべて取り除かれて、イメージがリセットされます。

オペレーティング システム イメージがターゲット デバイスに配布された後でターゲット デバイスが起動されると、Microsoft ミニウィザードが自動的に実行されます。Sysprep.inf からの応答を使用した後、Microsoft ミニウィザードは、ターゲット マシンの Sysprep ディレクトリを削除します。

Sysprep をセットアップするには

1 Microsoft オペレーティング システムのインストール メディアの SUPPORT\TOOLS フォルダにある DEPLOY.CAB に移動します。詳細については、Microsoft のドキュメントを参照してください。

2 適切な オペレーティング システム メディアを使用して、Deploy.cab ファイルから Microsoft Sysprep ファイルを展開します。これらのファイルを参照マシンの C:\SysPrep にコピーして、ディレクトリおよびファイルが読み取り専用に設定されていないことを確認します。

最新バージョンの Sysprep を使用していることを確認してください。古いバージョンを使用すると、エラーが発生する場合があります。

適切なバージョンの Sysprep がない場合は、Microsoft の Web サイトからダウンロードできます。

管理者権限を持っている場合でも、Sysprep を実行するための適切なユーザー権限を設定されていることを確認してください。Microsoft Web サイトの記事 #270032「Sysprep.exe プログラムの実行に必要なユーザー権利」を参照してください。適切なユーザー権限がない場合、Sysprep を実行すると、次のエラーが発生します。

「このアプリケーションを実行するには、管理者である必要があります。」

Image Preparation Wizard を終了し、適切なユーザー権限をセットアップしたら、再びウィザードを実行する必要があります。

3 Microsoft Sysprep を使用するために、参照マシンが、ドメインではなく WORKGROUP に所属していることを確認します。

4 Sysprep.inf を作成して、C:\Sysprep に保存します。

Sysprep.inf を作成するには

Sysprep.inf は手動で作成するか、Microsoft セットアップ マネージャ (Setupmgr.exe) を使用して作成できます。セットアップ マネージャは、Microsoft OS 配布メディアにある SUPPORT\TOOLS フォルダの Deploy.cab ファイルにあります。詳細については、Microsoft のドキュメントを参照してください。

Microsoft は、Windows 2000 用 Sysprep ユーティリティによる大容量ストレージ セクションの作成をサポートしていません。Windows 2000 でこのオプションを使用すると、イメージの取得または配布中に問題が発生する場合があります。

利用可能なサンプル Sysprep.inf ファイルはイメージ キャプチャ メディアの \samples\sysprep\ にあります。

Sysprep.inf ファイルのサイズは 800 KB を超えてはなりません。

以下は Sysprep.inf ファイルを作成するときのヒントです。

- TimeZone の値を環境に合わせて調整します。

- 管理者パスワードをセットアップします。
- ユーザーがターゲット デバイスに入力しなくて済むように、製品キーを作成します。
- 無人インストールを行うには、[Unattended] セクションに UnattendMode = FullUnattended を含める必要があります。
- ExtendOemPartition を 1 に設定します。これにより、Microsoft Sysprep は、OS のパーティションをそのディスク上で、物理的に連続した、パーティションが設定されていない利用可能な領域へ拡張します。
- Sysprep.inf に JoinDomain が存在する場合、Sysprep.inf はコンピュータをドメインに接続する権限があるアカウントの管理ユーザー ID とパスワードを持っている必要があります。JoinDomain は大文字と小文字を区別することに注意します。

Sysprep.inf ファイルの優先度の設定方法

Sysprep.inf ファイルはオペレーティング システム イメージと共に配布されるか、オペレーティング システム イメージに接続されたパッケージ (上書き Sysprep ファイル) として配布されます。sysprep.inf ファイルが個別にパブリッシュされた場合、イメージの NTFS にある sysprep.inf ファイルと統合され、1 つの sysprep.inf になります。

Sysprep.inf ファイルは次の順で低位から高位へ優先度が付けられます。

1. イメージに埋め込まれた Sysprep (優先度が最も低い)。個別にパブリッシュされる sysprep.inf (上書き sysprep) がない場合、イメージ内の sysprep.inf が使用されます。
2. 上書き Sysprep (ゴールド イメージと別の Sysprep ファイル)。

   上書き Sysprep.inf は 1 つだけ解決されます。

3. ポリシー条件に添付された Sysprep (優先度が最も高い)。

Image Preparation Wizard について

Image Preparation Wizard は以下のタスクを実行します。

1 参照マシンに関する情報 (ハードウェア機能と OS 機能についての情報) を含むオブジェクトを作成します。

2 (任意の終了ポイント。レガシー イメージでは使用不可) 必要に応じて使用可能な終了ポイントを実行します。Image Preparation Wizard で、イメージを封印する SysPrep が起動される前に PRE.CMD が実行されます。Sysprep によってイメージが封印された後、POST.CMD が実行されます。詳細については、359 ページの「Image Preparation Wizard の終了ポイントの使用」を参照してください。

3 サポートされているオペレーティング システム上で Microsoft Sysprep を実行します。

4 参照マシンを (適切なメディアから起動された) Service OS で再起動します。実行した Service OS でイメージと関連ファイルが収集されます。

5 ファイルを作成し、HPCA Server の SystemDrive:\Program Files\SystemDrive:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\upload にコピーします。

   レガシー イメージを作成する場合、以下のファイルがアップロードされます。

   — ImageName.IMG

     このファイルには、ゴールド イメージが含まれています。これは、非常に大きなハード ディスク ドライブ システムのブート パーティションをセクタごとにコピーして圧縮したファイルです。このファイルには、イメージがインストールされるときにアクセス可能な組み込みファイル システムが含まれています。

   — ImageName.MBR

     このファイルには、参照マシンのマスター ブート レコード ファイルが含まれています。

   — ImageName.PAR

     このファイルには、参照マシンのパーティション テーブル ファイルが含まれています。

   — ImageName.EDM

     このファイルにはインベントリ情報を含むオブジェクトが含まれています。

   ImageX または Windows セットアップを使用してイメージを作成する場合、次のファイルがアップロードされます。

— ImageName.WIM

このファイルには参照マシンの一連のファイルとファイル システムが含まれています。

— ImageName.EDM

このファイルにはインベントリ情報を含むオブジェクトが含まれています。

Image Preparation Wizard の終了ポイントの使用

必要に応じて、Image Preparation Wizard の終了ポイントを使用できます。たとえば、取得を実行する前にデバイスをクリーンアップするために使用できます。

これは、レガシー イメージではサポートされていません。

終了ポイントを使用するには

1 PRE.CMD ファイルと POST.CMD ファイルを作成します。

2 これらのファイルおよびサポート ファイルを、OSM\PREPWIZ\payload\default\pre と OSM\PREPWIZ\payload\default\post にそれぞれ保存します。

Image Preparation Wizard によって、これらのファイルは参照デバイスの %temp%\prepwiz\pre と %temp%\prepwiz\post にコピーされ、取得が始まる前に削除されます。Image Preparation Wizard で、イメージを封印する SysPrep が起動される前に PRE.CMD が実行されます。Sysprep によってイメージが封印された後、POST.CMD が実行されます。

リモート イメージ取得の準備

次のセクションでは、リモート マシン上のイメージを準備する方法を説明します。

現時点では、Microsoft ImageX のみがサポートされています。

リモート イメージを取得するには

1 取得するリモート マシンに接続します。

2 ImageCapture メディアから \image_preparation_wizard をネットワーク共有にコピーします。

3 イメージを取得するリモート マシンのドライブを、\image_preparation_wizard のあるネットワーク共有にマップします。

4 必要に応じてリモート マシンを準備します。マシンを準備する方法については、次を参照してください。

— ImageX 配布用の Windows Vista 以前の取得 340 ページ

— ImageX 配布用の Windows Vista の取得 342 ページ

— ImageX 配布用の Windows Server 2008 の取得 344 ページ

Image Preparation Wizard の使用

続行する前に、参照マシンを、CD-ROM ドライブから起動するように設定します。イメージ キャプチャ メディアが起動可能なため、この作業を実行する必要があります。イメージ キャプチャ メディアを実行すると、デバイスを再起動して、イメージを更新します。

Image Preparation Wizard を使用するには

1 イメージ キャプチャ メディアを参照マシンに挿入します。

2 image_preparation_wizard ディレクトリに移動し、prepwiz.exe をダブルクリックします。

レガシー オペレーティング システムを使用していて、Agent がインストールされていない場合、次のメッセージが表示されます。

「このコンピュータには HPCA Agent がインストールされていません。OS Manager 製品がインストールされているターゲット コンピュータは管理できない可能性があります。

デバイスを管理対象とするには、Image Preparation Wizard を実行する前に、必ず Agent をインストールしてください。」

— 配布するイメージをレガシー メソッドで取得する場合、Image Preparation Wizard では、続行する前に C:\Sysprep フォルダが存在するか、HPCA Agent がインストールされているかが確認されます。

— ImageX または Windows Setup で配布するイメージをキャプチャすると、Image Preparation Wizard は Sysprep を、Windows Vista の場合は C:\Windows\system32\sysprep に、それ以前のオペレーション システムでは C:\sysprep に置きます。

Publisher を使用する場合は、Agent のパブリッシュ元を選択するオプションが表示されます。これには、Agent を個別にパッケージ化し、新しいバージョンを必要に応じて HPCA DB にパブリッシュして Agent を更新できるという利点があります。これを実行すると、新たに配布する .WIM はすべて自動的に最新のエージェントを使用します。

3 **[次へ]** をクリックします。

[エンド ユーザー ライセンス契約] ウィンドウが表示されます。

4 **[同意する]** をクリックします。

配布方法は以下のようになります。

— **レガシー**はパーティションのディスク イメージをそのままキャプチャします (.IMG フォーマット)。

— **ImageX** では、WinPE や ImageX ユーティリティで配布される .WIM フォーマットでイメージが取得されます。

— **Windows セットアップ**では、WinPE や Windows セットアップ ユーティリティで配布される .WIM フォーマットでイメージが取得されます。

OS でサポートされていない配布メソッドは表示されません。

5 HPCA Server の IP アドレスまたはホスト名およびポートを入力します。これは、xxx.xxx.xxx.xxx:port という形式で指定する必要があります。OS のイメージ作成用に予約されている HPCA Server のポートは 3469 です。

6 **[次へ]** をクリックします。

7 イメージ ファイルの名前を入力します。これは、\upload ディレクトリに保存されるイメージ名です。

8 **[次へ]** をクリックします。

[ディスク イメージのスパン] ウィンドウが表示されます。

9 各イメージ ファイルに使用するディスク容量 (非圧縮) の合計を MB 単位で入力します。スパンしたイメージを作成しないときは、「0」(ゼロ) を入力します。

スパンしたイメージを使用して、イメージ ファイルを小さいセグメントに分割できます。スパンされたイメージの各セグメントのサイズは 4 GB に制限されます。イメージを Configuration Server に保存する場合、イメージ全体が 4 GB 以下である必要があるという条件を満たすことができるため、有用です。(0 を指定して) イメージをスパンするオプションを選択しない場合は、イメージを 4 GB 以下にしてください。

10 **[次へ]** をクリックします。

該当する場合は、[追加の Sysprep オプション] ウィンドウが表示されます。

このテキスト ボックスには、すべての SID をクリアし、キャプチャできるようにマシンを準備するコマンドが予め入力されています。

11 また、Sysprep に渡す追加オプションを、スペースで区切って入力することもできます。

これは高度なオプションです。入力するコマンドはチェックされないため、追加オプションを入力する時は注意してください。

12 追加の Sysprep オプションについては、Microsoft のドキュメントを参照してください。

13 **[次へ]** をクリックします。

配布方法で ImageX を選択すると、デフォルトのオプションが選択された [Image Preparation Wizard のペイロードの選択] ウィンドウが表示されます。

ペイロードには、ターゲット デバイスに配布されるローカル サービスの起動 (LSB) データが含まれます。

14 イメージ ファイルの説明を入力し、**[次へ]** をクリックします。

[Windows 版の選択] ウィンドウが表示される場合があります。

15 取得する Windows のエディションを選択し、**[次へ]** をクリックします。

[オプション] ウィンドウが表示されます。

HPCA Agent をインストールしていない場合は、[OS のインストール後にクライアント接続を実行する] チェック ボックスは表示されません。ただしレガシーでイメージをキャプチャする場合は、このエージェントをインストールすることが重要なため注意してください。

16 適切なオプションを選択します。

取得するオペレーティング システムによって異なるオプションが表示されます。

— **Sysprep.inf に大容量ストレージ セクションをビルドする**

Windows XP 以上の Sysprep.inf の [SysprepMassStorage] セクションで、大容量ストレージ ドライバのリストをビルドするには、このチェック ボックスをオンにします。

Microsoft は、Windows 2000 用 Sysprep ユーティリティによる大容量ストレージ セクションの作成をサポートしていません。Windows 2000 でこのオプションを使用すると、イメージの取得または配布中に問題が発生する場合があります。

— **未使用のディスク スペースの圧縮を最適化する**

未使用ディスク領域の圧縮を最適化するには、このチェック ボックスをオンにします。これは、システム ドライブ パーティションの最後までゼロを追加します。ハード ドライブの容量によっては、若干時間がかかる場合があります。

これにより、取得したイメージの圧縮率が大きくなり、サイズが小さくなります。イメージ ファイルのサイズが小さい方が、保存するディスク領域が少なく、ネットワーク上を転送するバンド幅が小さくて済みます。

— **OS のアップロードの前にパーティションのサイズを変更する**

パーティションのサイズをできるだけ小さくするには、このチェック ボックスをオンにします。このチェック ボックスをオンにしない場合は、パーティションのサイズが適切であるか確認してください。

— **OS のインストール後にクライアント接続を実行する**

OS をインストールした後に HPCA Server に接続するには、このチェック ボックスをオンにします。このチェック ボックスをオンにしない場合は、OS がインストールされた後、HPCA OS 接続は実行されません。

Agent をインストールしない方法を使用する (たとえば、レガシー メソッドを使用していて、HPCA Agent をインストールしなかった、あるいは配布時に Agent がインストールされデフォルトで接続が実行されるために Windows Vista イメージを取得する) 場合は、このオプションは表示されません。

17 **[次へ]** をクリックします。

[要約] ウィンドウが表示されます。

18 **[開始]** をクリックします。

19 **[完了]** をクリックします。

APIC デバイスで作業している場合は、[イメージを APIC 互換にする] ウィンドウが表示されます。Windows Vista オペレーティング システムは APIC 互換デバイスでなければキャプチャ / 配布できないため注意してください。

20 必要であれば、**[Make image compatible with machine with PIC(イメージを PIC を搭載したマシン互換にする)]** チェック ボックスを選択します。

Microsoft はこれを推奨していません。この選択を行う前に、Microsoft の Web サイトで詳細を確認してください。

21 **[次へ]** をクリックします。

上図のチェック ボックスを選択した場合は、[Select Windows CD(Windows CD の選択)] ウィンドウが表示されます。

22 [Windows CD-ROM] へ移動し、**[次へ]** をクリックします。

23 **[完了]** をクリックして、Sysprep を実行します。

Image Preparation Wizard により Sysprep が起動されます。これが完了するのに 15 ～ 20 分かかる場合があります。完了後に、sysprep はデバイスを再起動します。**[OK]** をクリックして、デバイスを再起動します。

- Windows 2000 を使用している場合、画面では活動していないように見えても、Sysprep の実行に時間がかかっている場合があります。
- 監視モード (以前の出荷時モード) を使用している場合、マシンはオペレーティング システムをネットワーキング有効状態で再起動します。カスタマイズが完了したら、Image Capture CD/DVD をマシンに挿入し、コマンド プロンプトから次を実行します。

  sysprep.exe -reseal -reboot

Sysprep が再起動すると、イメージがサーバーにアップロードされます。

- 起動順が最初に CD-ROM から起動する設定になっている場合は、Image Capture メディアがロードされ、デバイスは CD-ROM で起動されます。
- デバイスに CD-ROM が搭載されない場合は、PXE 環境が必要で、デバイスはネットワーク優先で起動されるように設定されている必要があります。これで、ネットワーク 起動中にキーボードの F8 を押して、PXE によりイメージを取得できます。メニューが表示された後、ぜひ [Remote Boot (Image Upload)(リモート ブート (イメージ アップロード))] を選択します。

デバイスで CD ではなくオペレーティング システムが起動される場合は、準備のプロセスをやり直す必要があります。

これで、デバイスがネットワークに接続され、HPCA Server にイメージが保存されます。

- イメージのアップロードは、長時間かかるように感じられる場合があります。それは、アップロードではなく、イメージの圧縮と圧縮のための未使用ディスク領域の最適化 (特に、空きディスク領域が多くある場合) によるものです。これは、イメージの転送中に行われるため、ネットワークのパイプはボトルネックになりません。転送速度は約 30 ～ 400 Kbps ですが、プロセッサの速度とネットワーク環境によって異なります。
- 必要なときに取得できるように、\upload ディレクトリに格納するファイルのコピーを作成します。

Image Preparation Wizard がネットワークに接続し、HPCA Server の upload ディレクトリにイメージが保存されます。

アップロード プロセスが完了すると、以下のメッセージが表示されます。

**** OS イメージは正常に HPCA OS Manager Server に送信されました。

24 参照マシンを再起動して、必要な場合は起動設定を再調整し、元のオペレーティング システムに戻ります。

次に、イメージを HPCA データベースにパブリッシュします。HPCA ドキュメントのパブリッシュについての情報を参照しくてください。

無人モードでの Image Preparation Wizard の使用

設定ファイルを使用して、無人モードで Image Preparation Wizard を実行できます。

無人モードで Image Preparation Wizard を使用するには

1 イメージ キャプチャ メディアを参照マシンに挿入します。

2 \samples\prepwiz_unattend に移動し、setup.cfg をローカル マシンまたはネットワーク ロケーションにコピーします。

3 必要な変更を行います。変更が必要な可能性がある値は、次のとおりです。

表 44　setup.cfg の変数

名前	説明	値の例
RISHOSTPORT	HPCA Server の IP アドレス。	xxx.xxx.x.x:port
IMAGENAME	アップロードされるファイルを作成するために使用するプレフィックス。これは、アップロードされるイメージの名前を作成するために、.WIM に追加されます。	Vista
IMAGEDESC	データベースにパブリッシュされるイメージの説明。	「Windows Vista 無人テスト イメージ」
PREPWIZPAYLOAD	管理者が使用するペイロード。ターゲット デバイスに配布される LSB データを含みます。	次のデフォルト値を使用します。“/OSM/PREPWIZ/payload/default/”
OSEDITION	使用する Vista のエディションを指定します。	“Enterprise”
設定 ::setup(DEPLOYOS,SELECTED)	1 または 0 に設定して、イメージ取得後に OS を再配布するかどうかを示します。	“0”
se ::setup(ClientConnect,SELECTED)	1 または 0 に設定して、イメージ配布後にターゲット デバイスで OS 接続を実行するかどうかを示します。	“1”

4　参照マシンで、コマンド ウィンドウを開き、ディレクトリを CD/DVD に変更します。Image_Preparation_Wizard\win32 に移動します。ここで、次のコマンドを実行します。

prepwiz -mode silent -cfg < フル パス >\setup.cfg

Image Preparation Wizard が Sysprep を起動します。これが完了するのに 15 ～ 20 分かかる場合があります。完了すると Sysprep によりデバイスが再起動され、ネットワークに接続されて HPCA Server の upload ディレクトリにそのイメージが保存されます。

シン クライアント イメージの準備と取得

次の各セクションでは、サポートされているシン クライアント オペレーティング システムのイメージを準備し取得する方法を説明します。

- Windows XPe OS イメージ 367 ページ
- Windows CE OS イメージ 371 ページ
- Embedded Linux OS イメージ 373 ページ

Windows XPe OS イメージ

次のセクションでは、Windows XPe シン クライアント オペレーティング システムのイメージを準備して取得する方法を説明します。

- タスク 1 – XPe 参照マシンの準備 367 ページ
- タスク 2 – Image Preparation Wizard の実行 368 ページ

シン クライアント デバイス上のイメージを取得し、その後、取得したイメージを容量の大きなフラッシュ ドライブを持つ XPe シン クライアント デバイスに配布できます。これは、リリース ノートのドキュメントに記述されているような一定の制限に従う必要があります。

タスク 1 – XPe 参照マシンの準備

イメージ取得のため XPe シン クライアントを準備するには、以下のものが必要です。

- HPCA メディア
- XPe Embedded Toolkit CD-ROM
- イメージ準備 CD-ROM

Windows XPe イメージを取得する前に、以下の操作を行う必要があります。

1 Windows XPe に管理者としてログインします。

2 XPe Embedded Toolkit から、etprep.exe を C:\Windows にコピーします。

3 XPe Embedded Toolkit から、fbreseal.exe を C:\Windows\fba にコピーします。

4 HPCA Agent をインストールします。エンタープライズ ライセンス ユーザーは、シン クライアント エージェントのインストールの詳細について、『HPCA Application および Application Self-service Manager ガイド』を参照してください。

タスク 2 – Image Preparation Wizard の実行

Image Preparation Wizard は以下のタスクを実行します。

1 マシンに十分な空きディスク領域があるかどうかをチェックし、HPCA Agent がインストールされていることを確認します。十分な空きディスク領域がない場合、Image Preparation Wizard はメッセージを表示して終了します。

2 参照マシンに関する情報 (ハードウェアおよび BIOS の機能など) を含むオブジェクトを作成します。

3 参照マシンを、作成したイメージ準備 CD から起動したサービス オペレーティング システムから再起動します。Image Preparation Wizard の Linux ベースの部分が実行され、イメージとその関連ファイルが収集されます。

4 次のファイルを作成し、HPCA Server の C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\upload にコピーします。

— ImageName.IBR
このファイルにイメージが含まれます。シン クライアント イメージ ファイルは、参照マシンのフラッシュ ドライブと同じサイズです。Windows XPe のイメージは、同等以上のサイズのフラッシュ ドライブを備えたターゲット マシンに配布できます。このファイルには、イメージがインストールされるときにアクセス可能な組み込みファイル システムが含まれています。

— ImageName.EDM

これらのファイルが転送される間は、オペレーティング システム イメージが転送の間に圧縮されるため、ネットワーク速度は最大速度より遅くなります。

イメージが配布された後、包括的なログ (machineID.log) も upload ディレクトリで利用できます。

Image Preparation Wizard を使用するには

1 作成した Image Preparation Wizard CD-ROM を参照マシンの CD-ROM ドライブに挿入します (シン クライアント デバイスには、USB CD-ROM ドライブが必要です)。この CD は、お使いの HPCA メディアの `Media\iso\roms` ディレクトリにある ImageCapture.iso を使用して作成されます。

2 自動実行が有効な場合、HPCA OS の準備と取得 CD のホームページが開きます。

3 **[ブラウズ]** をクリックして `\image_preparation_wizard\win32\` ディレクトリを開きます。

4 **prepwiz.exe** をダブルクリックします。Image Preparation Wizard では、続行する前に、`etprep.exe` および `fbreseal.exe` が利用できるかどうかが確認されます。[ようこそ] ウィンドウが表示されます。

5 **[次へ]** をクリックします。[エンド ユーザー ライセンス契約] ウィンドウが表示されます。

6 **[同意する]** をクリックします。

7 HPCA Server の IP アドレスまたはホスト名およびポートを入力します。これは、`xxx.xxx.xxx.xxx:port` という形式で指定する必要があります。OS のイメージ作成用に予約されている HPCA Server のポートは 3469 です。

   Image Preparation Wizard が HPCA Server に接続できない場合は、メッセージが表示され、以下の手順を実行する必要が生じます。

   — **[はい]** をクリックして続行します。

   — **[いいえ]** をクリックして、ホスト名または IP アドレスを変更します。

   — **[キャンセル]** をクリックして、Image Preparation Wizard を終了します。

8 **[次へ]** をクリックします。[イメージ名] ウィンドウが開きます。

9 イメージ ファイルの名前を入力します。これは、HPCA Server の `\upload` ディレクトリに保存されるイメージ名です。

10 **[次へ]** をクリックします。イメージの説明を入力するウィンドウが開きます。

11 イメージ ファイルの説明を入力します。

12 **[次へ]** をクリックします。[オプション] ウィンドウが開きます。

13 適切なオプションを選択します。

   OS のインストール後にクライアント接続を実行する
   OS のインストール後に HPCA Server に接続し、OS が正しくインストールされたことを確認するには、このチェック ボックスをオンにします。このチェック ボックスをオンにしない場合は、OS がインストールされた後、OS 接続は自動的に実行されません。

14 デフォルトを受け入れて、**[次へ]** をクリックします。[要約] ウィンドウが表示されます。

15 **[開始]** をクリックします。

16 **[完了]** をクリックします。ウィザードがイメージを準備します。

17 **[OK]** をクリックします。

デバイスは、CD-ROM ドライブの Image Preparation Wizard CD から起動されます。このような動作になるように必要な設定の調整を行います (たとえば、BIOS のバージョンによっては、再起動プロセスの間に F10 キーを押して、設定内の起動順序を変更できます)。

デバイスが CD を起動せずに Windows を起動する場合は、367 ページの「タスク 1 – XPe 参照マシンの準備」からプロセスを再開する必要があります。

イメージのアップロードは、長時間かかるように感じられる場合があります。それは、アップロードではなく、イメージの圧縮と圧縮のための未使用ディスク領域の最適化 (特に、空きディスク領域が多くある場合) によるものです。これは、イメージの転送中に行われるため、ネットワークのパイプはボトルネックになりません。転送速度は、約 30 ～ 400 Kbps ですが、プロセッサの速度やネットワーク環境により異なる場合があります。

必要に応じて取得できるように、`\upload` ディレクトリに格納するファイルのコピーを作成できます。

18 OS Image Preparation Wizard によってネットワークに接続し、HPCA Server の `\upload` ディレクトリにイメージが保存されます。

アップロード プロセスが完了すると、次のメッセージが表示されます。

「OS イメージが正常に OVCM OS Manager Server へ送信されました

**** CD を挿入している場合、CD を取り出して再起動します」

19 参照マシンを再起動して、必要な場合は起動設定を再調整し、元のオペレーティング システムに戻ります。

これで、Publisher を使用して、管理対象デバイスへの配布のためにイメージ ファイルを HPCA Server にパブリッシュできるようになりました。

Windows CE OS イメージ

次のセクションでは、Windows CE シン クライアント オペレーティング システムのイメージを準備し、取得する方法を説明します。

タスク 1 – CE 参照マシンの準備

イメージ取得のため CE シン クライアントを準備するには、以下のものが必要です。

- HPCA メディア
- イメージ準備 CD-ROM

イメージを取得する前に、HPCA Agent を Windows CE デバイスにインストールする必要があります。エンタープライズ ライセンス ユーザーは、シン クライアント エージェントのインストールの詳細について、『HPCA Application および Application Self-service Manager ガイド』を参照してください。

タスク 2 – Image Preparation Wizard の実行

Image Preparation Wizard は以下のタスクを実行します。

1. マシンに十分な空きディスク領域があるかどうかをチェックし、HPCA Agent がインストールされていることを確認します。十分な空きディスク領域がない場合、Image Preparation Wizard はメッセージを表示して終了します。
2. 参照マシンに関する情報 (ハードウェアおよび BIOS の機能など) を含むオブジェクトを作成します。
3. 参照マシンを、作成したイメージ準備 CD から起動したサービス オペレーティング システムから再起動します。Image Preparation Wizard の Linux ベースの部分が実行され、イメージとその関連ファイルが収集されます。
4. 次のファイルを作成し、HPCA Server の C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\upload にコピーします。

   — `ImageName.IBR`
   このファイルにイメージが含まれます。シン クライアント イメージ ファイルは、参照マシンのフラッシュ ドライブと同じサイズです。Windows

CE のイメージは、同等のサイズのフラッシュ ドライブを備えたターゲット マシンに配布できます。このファイルには、イメージがインストールされるときにアクセス可能な組み込みファイル システムが含まれています。

— `ImageName.EDM`

これらのファイルが転送される間は、オペレーティング システム イメージが転送の間に圧縮されるため、ネットワーク速度は最大速度より遅くなります。

イメージが配布された後、包括的なログ (`machineID.log`) も `upload` ディレクトリで利用できます。

Image Preparation Wizard を使用するには

1. 作成した Image Preparation Wizard CD-ROM を参照マシンの CD-ROM ドライブに挿入します (シン クライアント デバイスには、USB CD-ROM ドライブが必要です)。この CD は、お使いの HPCA メディアの `Media\iso\roms` ディレクトリにある `ImageCapture.iso` を使用して作成されます。
2. 自動実行が有効な場合、HPCA OS の準備と取得 CD のホームページが開きます。
3. **[ブラウズ]** をクリックして `\image_preparation_wizard\WinCE\` ディレクトリを開きます。
4. **prepwiz.exe** をダブルクリックします。Image Preparation Wizard が開始されます。
5. HPCA Server の IP アドレスまたはホスト名およびポートを入力します。これは、`xxx.xxx.xxx.xxx:port` という形式で指定する必要があります。OS のイメージ作成用に予約されている HPCA Server のポートは 3469 です。

   Image Preparation Wizard が HPCA Server に接続できない場合は、メッセージが表示され、以下の手順を実行する必要が生じます。

   — **[はい]** をクリックして続行します。

   — **[いいえ]** をクリックして、ホスト名または IP アドレスを変更します。

   — **[キャンセル]** をクリックして、Image Preparation Wizard を終了します。
6. **[OK]** をクリックします。ウィザードがイメージを準備します。

デバイスは、CD-ROM ドライブの Image Preparation Wizard CD から起動されます。このような動作になるように必要な設定の調整を行います (たとえば、BIOS のバージョンによっては、再起動プロセスの間に F10 キーを押して、設定内の起動順序を変更できます)。

デバイスが CD を起動せずに Windows を起動する場合は、371 ページの「タスク 1 – CE 参照マシンの準備」からプロセスを再開する必要があります。

イメージのアップロードは、長時間かかるように感じられる場合があります。それは、アップロードではなく、イメージの圧縮と圧縮のための未使用ディスク領域の最適化 (特に、空きディスク領域が多くある場合) によるものです。これは、イメージの転送中に行われるため、ネットワークのパイプはボトルネックになりません。転送速度は、約 30 ～ 400 Kbps ですが、プロセッサの速度やネットワーク環境により異なる場合があります。

必要に応じて取得できるように、\upload ディレクトリに格納するファイルのコピーを作成できます。

7 OS Image Preparation Wizard によってネットワークに接続し、HPCA Server の \upload ディレクトリにイメージが保存されます。

アップロード プロセスが完了すると、次のメッセージが表示されます。

「OS イメージが正常に OVCM OS Manager Server へ送信されました

**** CD を挿入している場合、CD を取り出して再起動します」

8 参照マシンを再起動して、必要な場合は起動設定を再調整し、元のオペレーティング システムに戻ります。

これで、Publisher を使用して、管理対象デバイスへの配布のためにイメージ ファイルを HPCA Server にパブリッシュできるようになりました。ページの「」を参照してください。

Embedded Linux OS イメージ

次のセクションでは、Embedded Linux オペレーティング システムのイメージを準備し取得する方法を説明します。

- タスク 1 – Embedded Linux 参照マシンの準備 374 ページ
- タスク 2 – Image Preparation Wizard の実行 374 ページ

タスク 1 – Embedded Linux 参照マシンの準備

イメージ取得のため Embedded Linux シン クライアントを準備するには、以下のものが必要です。

- HPCA メディア
- イメージ準備 CD-ROM

イメージを取得する前に、HPCA Agent を Embedded Linux デバイスにインストールする必要があります。エンタープライズ ライセンス ユーザーは、シン クライアント エージェントのインストールの詳細について、『HPCA Application および Application Self-service Manager ガイド』を参照してください。

シン クライアント デバイスの情報、および NFS を使用してインストールを実行する方法の詳細については、このガイドのインストールの章または `ThinClient.tar` の README ファイルを参照してください。

タスク 2 – Image Preparation Wizard の実行

Image Preparation Wizard は以下のタスクを実行します。

1. マシンに十分な空きディスク領域があるかどうかをチェックし、HPCA Agent がインストールされていることを確認します。十分な空きディスク領域がない場合、Image Preparation Wizard はメッセージを表示して終了します。
2. 参照マシンに関する情報 (ハードウェアおよび BIOS の機能など) を含むオブジェクトを作成します。
3. 参照マシンを、作成したイメージ準備 CD から起動したサービス オペレーティング システムから再起動します。Image Preparation Wizard の Linux ベースの部分が実行され、イメージとその関連ファイルが収集されます。
4. 次のファイルを作成し、HPCA Server の C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\upload にコピーします。

   — `ImageName.DD`
   このファイルにイメージが含まれます。シン クライアント イメージ ファイルは、参照マシンのフラッシュ ドライブと同じサイズです。Embedded Linux のイメージは、サイズが同じフラッシュ ドライブを備えたターゲット マシンにしか配布できません。このファイルには、イメージがインストールされるときにアクセス可能な組み込みファイル システムが含まれています。

— ImageName.EDM
このファイルにはインベントリ情報を含むオブジェクトが含まれています。

これらのファイルが転送される間は、オペレーティング システム イメージが転送の間に圧縮されるため、ネットワーク速度は最大速度より遅くなります。

イメージが配布された後、包括的なログ (machineID.log) も upload ディレクトリで利用できます。

Image Preparation Wizard を使用するには

1 作成した Image Preparation Wizard CD-ROM を参照マシンの CD-ROM ドライブに挿入します (シン クライアント デバイスには、USB CD-ROM ドライブが必要です)。この CD は、お使いの HPCA メディアの Media\iso\roms ディレクトリにある ImageCapture.iso を使用して作成されます。

Linux シン クライアント モデルでは、CD-ROM が実行されないように、マウント時にデフォルトで noexec オプションが設定される場合があります。これにより、Image Preparation Wizard を実行しようとすると、パーミッション エラーが起こったり、実行に失敗したりします。この問題を解決するには、noexec オプションを設定せずに CD-ROM を再マウントしてください。

2 Image Preparation CD で、/image_preparation_wizard/linux に移動し、./prepwiz を実行します。[ようこそ] ウィンドウが表示されます。

3 **[次へ]** をクリックします。[エンド ユーザー ライセンス契約] ウィンドウが表示されます。

4 **[同意する]** をクリックします。

5 HPCA Server の IP アドレスまたはホスト名およびポートを入力します。これは、xxx.xxx.xxx.xxx:port という形式で指定する必要があります。OS のイメージ作成用に予約されている HPCA Server のポートは 3469 です。

Image Preparation Wizard が HPCA Server に接続できない場合は、メッセージが表示され、以下の手順を実行する必要が生じます。

— **[はい]** をクリックして続行します。

— **[いいえ]** をクリックして、ホスト名または IP アドレスを変更します。

— **[キャンセル]** をクリックして、Image Preparation Wizard を終了します。

6 **[次へ]** をクリックします。[イメージ名] ウィンドウが開きます。

7 イメージ ファイルの名前を入力します。これは、HPCA Server の \upload ディレクトリに保存されるイメージ名です。

8 **[次へ]** をクリックします。イメージの説明を入力するウィンドウが開きます。

9 イメージ ファイルの説明を入力します。

10 **[次へ]** をクリックします。[オプション] ウィンドウが開きます。

11 適切なオプションを選択します。

OS のインストール後にクライアント接続を実行する
OS のインストール後に HPCA Server に接続し、OS が正しくインストールされたことを確認するには、このチェック ボックスをオンにします。このチェック ボックスをオンにしない場合は、OS がインストールされた後、OS 接続は自動的に実行されません。

12 デフォルトを受け入れて、**[次へ]** をクリックします。[要約] ウィンドウが表示されます。

13 **[開始]** をクリックします。

14 **[完了]** をクリックします。ウィザードがイメージを準備します。

15 **[OK]** をクリックします。

デバイスは、CD-ROM ドライブの Image Preparation Wizard CD から起動されます。このような動作になるように必要な設定の調整を行います (たとえば、BIOS のバージョンによっては、再起動プロセスの間に F10 キーを押して、設定内の起動順序を変更できます)。

デバイスが CD を起動せずに Windows を起動する場合は、374 ページの「タスク 1 – Embedded Linux 参照マシンの準備」からプロセスを再開する必要があります。

イメージのアップロードは、長時間かかるように感じられる場合があります。それは、アップロードではなく、イメージの圧縮と圧縮のための未使用ディスク領域の最適化 (特に、空きディスク領域が多くある場合) によるものです。これは、イメージの転送中に行われるため、ネットワークのパイプはボトルネックになりません。転送速度は、約 30 ～ 400 Kbps ですが、プロセッサの速度やネットワーク環境により異なる場合があります。

必要に応じて取得できるように、\upload ディレクトリに格納するファイルのコピーを作成できます。

16 OS Image Preparation Wizard によりネットワークに接続され、HPCA Server のイメージが /UPLOAD ディレクトリに保存されます。

アップロード プロセスが完了すると、次のメッセージが表示されます。

「OS イメージが正常に OVCM OS Manager Server へ送信されました

**** CD を挿入している場合、CD を取り出して再起動します」

17 参照マシンを再起動して、必要な場合は起動設定を再調整し、元のオペレーティング システムに戻ります。

これで、Publisher を使用して、管理対象デバイスへの配布のためにイメージ ファイルを HPCA Server にパブリッシュできるようになりました。

OS イメージのパブリッシュおよび配布

イメージを取得したら、Publisher を使用して HPCA データベースにそのイメージをパブリッシュします。方法については、HPCA ドキュメントのパブリッシュに関する情報を参照してください。

HPCA にパブリッシュするとき、OS ライブラリをリフレッシュして、新しいイメージを表示します。HPCA Console ツールバーを使用して、選択したデバイスにイメージを配布します。

11 Publisher の使用

Publisher を使用して、HP Client Automation (HPCA) に、ソフトウェア、BIOS 設定、HP SoftPaq、およびオペレーティング システム イメージをパブリッシュしますパブリッシュされたソフトウェアはすべて、メイン HPCA Console の [ソフトウェア管理] にある [ソフトウェア] タブで利用できますパブリッシュされたオペレーティング システムは、[OS 管理] の [オペレーティング システム] タブ内で利用できます。

ソフトウェアは、パブリッシュした後、環境の管理対象デバイスへエンタイトルメント設定と配布を行う必要があります。

Publisher は、HPCA Core のインストール中に HPCA Core に自動的にインストールされますマシンにエージェントがすでにインストールされている場合、Publisher はエージェントのフォルダにインストールされます別の場所にインストールする場合は、製品メディアの HP Client Automation Administrator インストール ファイルを使用するか、ソフトウェア ライブラリの HPCA Administrator Publisher サービスを使用できます詳細については、『HP Client Automation Core および Satellite 入門 およびコンセプト ガイド』の「Manually Installing the HPCA Administrator」を参照してください。

Publisher を起動するには

1. Publisher をインストールしたデバイスで、**[スタート]** メニューを使用して、以下のように移動します。

   [スタート] > [すべてのプログラム] > [HP Client Automation Administrator] > [HP Client Automation Administrator Publisher]

2. Publisher にログインするには、HPCA のユーザー名とパスワードを使用しますデフォルトでは、ユーザー名は **`admin`**、パスワードは **`secret`** です。

パブリッシュ オプションは、ターゲット デバイスおよびインストールしている HPCA ライセンスによって異なります。

380 ページの表 45 に、3 種類のライセンス レベルごとに選択可能なパブリッシュ オプションを示します。

表 45　各 HPCA ライセンスで選択可能なパブリッシュ オプション

パブリッシュ オプション	Starter	Standard	Enterprise
コンポーネントの選択	いいえ	はい	はい
ハードウェア設定	いいえ	いいえ	はい
HP BIOS 設定	はい	はい	いいえ
HP Softpaq	はい	はい	いいえ
OS ADDON/ 追加 POS ドライバ	いいえ	はい	はい
OS イメージ	いいえ	はい	はい
Windows インストーラ	いいえ	はい	はい
シン クライアントのコンポーネントの選択	はい	はい	はい
シン クライアントの OS ADDON/ 追加 POS ドライバ	いいえ	いいえ	いいえ
シン クライアントの OS イメージ	はい	はい	はい

次の各セクションでは、ライセンスに応じたパブリッシュ オプションで Publisher を使用する方法を説明しますシン クライアント パブリッシュ オプションを選択する場合は、次の該当するセクションの手順に従ってください。

- ソフトウェアのパブリッシュ 381 ページ
- オペレーティング システム イメージのパブリッシュ 385 ページ
- OS ADDON/ 追加 POS ドライバのパブリッシュ 390 ページ
- BIOS 設定のパブリッシュ 392 ページ

ソフトウェアのパブリッシュ

パブリッシュするソフトウェアのタイプにより、2 つのパブリッシュ オプションの 1 つを使用しますログイン画面で、[Windows インストーラ] を使用して Windows インストーラ ファイル (.msi) をパブリッシュするのか、[コンポーネントの選択] を使用して Windows 以外のインストーラ ファイルをパブリッシュするのかを選択します次のセクションでは、各ファイル タイプをパブリッシュする手順を説明します。

- Windows インストーラ ファイルのパブリッシュ 381 ページ
- [コンポーネントの選択] を使用したパブリッシュ 383 ページ

Windows インストーラ ファイルのパブリッシュ

Windows インストーラは、MSI ファイルを使用して、オペレーティング システムにソフトウェア サービスを配布します Publisher では、このファイルによりサービスが作成され、そのサービスが HPCA にパブリッシュされますソフトウェア サービスが HPCA に格納されると、お使いの環境の管理対象デバイスに配布する準備が整います。

Windows インストーラ ファイルをパブリッシュするには

1. Publisher を起動します (379 ページの「Publisher を起動するには」を参照)。
2. ログオン画面で、管理者ユーザー ID およびパスワードを入力して、**[OK]** をクリックします。

   HPCA のユーザー名とパスワードを使用して、Publisher にログインしますデフォルトでは、ユーザー名は **admin**、パスワードは **secret** です。
3. [パブリッシュ オプション] 領域で、**[Windows インストーラ]** を選択して、**[OK]** をクリックします。
4. 左ペインの Windows インストーラ ファイルへ移動します右ペインには、選択した MSI ファイルで利用可能な情報が表示されます。
5. **[次へ]** をクリックします。
6. 使用できるパブリッシュ オプションを確認します。

   — **管理オプション**
   管理インストール ポイント (AIP) を作成するには、**[setup を使用]** または **[msiexec を使用]** を選択します。

   AIP のパスは、一時的な場所であり、パブリッシュ セッションが完了したら、削除されます。

— **変換**
Windows インストーラ ファイルに関連付けられた変換ファイルのアプリケーションを選択し、順序を変更します。

— **追加のファイル**
AIP の一部として追加のファイルを含めます。

– リストに表示された利用可能なファイルをすべて選択するには、**[すべて選択]** をクリックします。

– すべてのファイルの選択を解除するには、**[選択なし]** をクリックします。

— **プロパティ**
msi ファイルのプロパティを表示して変更しますWindows インストーラ ファイルには、正しく配布するために追加のコマンド ライン パラメータが必要な場合がありますたとえば、アプリケーションはインストール中にシリアル番号を渡すカスタム プロパティを必要とすることがあります [プロパティ] ダイアログを使用して、パラメータを追加します。

– 新しいプロパティを追加するには **[追加]** をクリックします。

– 既存のプロパティを削除するには **[削除]** をクリックします。

– プロパティの **[名前]** または **[値]** を変更するには、変更するアイテムをクリックして新しい値を入力します。

パブリッシュ オプションの編集が終わったら、**[次へ]** をクリックします。

7 [アプリケーションの情報] セクションでソフトウェア サービスの情報を入力します。

8 **[パッケージを適用する対象システム]** セクションを使用して、特定のオペレーティング システムまたはハードウェアへのサービスを制限しますいずれかのリンクをクリックして、設定可能なオプションを表示します。

9 **[次へ]** をクリックします。

10 [要約] セクションで、前の手順で指定したサービス情報を確認します情報を確認したら、**[パブリッシュ]** をクリックします。

11 パブリッシュ プロセスが完了したら、**[完了]** をクリックして Publisher を終了します。

これで、Windows インストーラ サービスを企業へ配布する準備が整いました。

変換ファイルを使用してその他のパラメータを適用するには

1 Orca や他の MSI エディタを使用して変換を作成します変換は、Windows インストーラ ファイルがパブリッシュされるディレクトリと同じディレクトリに保存します。

2 Windows インストーラのパブリッシュ セッションを開始します詳細は、上記の指示に従います。

3 編集手順で **[変換]** をクリックします。

4 利用可能な変換ファイルを選択して、パブリッシュ セッションを続けます。

ソフトウェア サービスが配布されると、変換ファイルが適用され、追加のコマンド ライン パラメータが指定されます。

[コンポーネントの選択] を使用したパブリッシュ

Windows インストーラ ファイル以外のソフトウェアをパブリッシュするには、[コンポーネントの選択] オプションを使用して、パブリッシュするソフトウェアを選択します。

[コンポーネントの選択] を使用してパブリッシュするには

1 Publisher を起動します (379 ページの「Publisher を起動するには」を参照)。

2 ログオン画面で、管理者ユーザー ID およびパスワードを入力して、**[OK]** をクリックします。

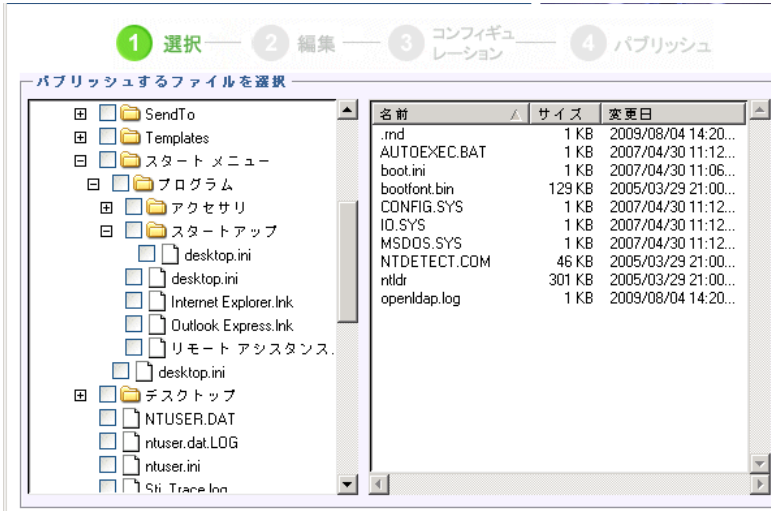
> HPCA のユーザー名とパスワードを使用して、Publisher にログインしますデフォルトでは、ユーザー名は **admin**、パスワードは **secret** です。

3 [パブリッシュ オプション] 領域で以下の操作を実行します。

— シン クライアントへパブリッシュしている場合は、**[シン クライアントのパブリッシュ]** を選択します。

— ドロップダウン リストから **[コンポーネントの選択]** を選択します。

4 **[OK]** をクリックします [パブリッシュするファイルを選択] ウィンドウが開きます。



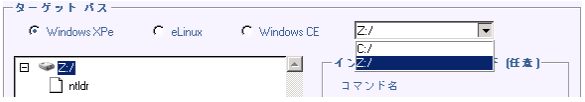
5 パブリッシュするファイルを選択して、**[次へ]** をクリックします。

ソフトウェアがある (パブリッシュ元の) ディレクトリ パスは、ソフトウェアが配布されるターゲット デバイスのディレクトリ パスになります。

ネットワーク共有が表示されますが、配布中に利用できなくなる場合があるためソフトウェアのパブリッシュには使用しません。

[ターゲット パス] ウィンドウが開きます。

6 シン クライアントへパブリッシュしている場合、インストール ポイントを選択します。次の図を参照してください。



7 コマンドを入力して、アプリケーションのインストールおよびアンインストールを実行しますたとえば、インストールを実行するコマンドは、`C:\temp\installs\install.exe /quietmode /automatic c:\mydestination` のようになります。

アンインストールを実行するコマンドは、C:\temp\installs\uninstall.exe /quietmode /automati のようになります。

ファイルを右クリックして、インストールまたはアンインストール コマンドとして設定できます。

8 **[次へ]** をクリックします [アプリケーションの情報] ウィンドウが表示されます。

9 [アプリケーションの情報] セクションでソフトウェア サービスの情報を入力します。

10 **[パッケージを適用する対象システム]** セクションを使用して、特定のオペレーティング システムまたはハードウェアへのサービスを制限しますいずれかのリンクをクリックして、設定可能なオプションを表示します。

11 **[次へ]** をクリックします。

12 [要約] セクションで、前の手順で指定したサービス情報を確認します設定を終了したら、**[パブリッシュ]** をクリックします。

13 パブリッシュ プロセスが完了したら、**[完了]** をクリックして Publisher を終了します。

これで、ソフトウェア サービスを企業へ配布する準備が整いました。

オペレーティング システム イメージのパブリッシュ

Image Preparation Wizard を使用して作成されるオペレーティング システム イメージは、HPCA Server の C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\upload に保存されます Publisher を使用して、管理対象デバイスへ配布するオペレーティング システム イメージ ファイル (.IMG) をパブリッシュします。

- .WIM イメージをパブリッシュする場合は、385 ページの「Vista OS の .WIM イメージをパブリッシュするための前提条件」を参照してください。
- Publisher を使用して OS イメージをパブリッシュするために必要な手順については、388 ページの「OS イメージのパブリッシュ」を参照してください。

Vista OS の .WIM イメージをパブリッシュするための前提条件

Vista オペレーティング システムの .WIM イメージをパブリッシュする場合は、以下の条件を満たしている必要があります。

- HPCA メディアの Media\client\default フォルダにアクセスできること このフォルダは、.WIM ファイルを初めてパブリッシュするとき、または更新したエージェント パッケージをパブリッシュする場合にのみ必要になります HPCA Agent は個別のパッケージとしてパブリッシュされます。これにより、それ以降のすべての .WIM ファイルの配布では、必ず利用可能な最新のエージェントが自動的に受信されます。
- WAIK がインストールされていること。(WAIK は、Microsoft の Web サイトから入手可能ですこれは、通常の Vista のインストールには含まれません。)
- filename.wim および filename.edm を、HPCA Server の \upload ディレクトリ (デフォルトでは C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\upload) から、イメージをパブリッシュするデバイスにコピーします。
- substitutes および unattend.xml を、filename.wim と同じディレクトリにコピーしますこれらのファイルのサンプルは、Image Capture メディアの \samples にありますサンプルを使用する場合は、タイム ゾーンの設定や製品キーの入力など、必要に応じて情報を変更してください詳細については、以下の説明を参照してくださいこれらのファイルはすべてプレフィックスが同じになっている必要がありますたとえば、install.wim、install.subs、install.xml のようになります。

このディレクトリ内のファイルやフォルダが読み取り専用に設定されていないことを確認してください読み取り専用に設定されていると、イメージは配布できません。

.subs および .xml ファイルについて

Filename.subs および filename.xml は、情報をカスタマイズするために使用しますオペレーティング システムの配布中、filename.subs と filename.xml が結合されて unattend.xml ファイルが作成されます。unattend.xml ファイルは、ターゲット デバイスでの Windows セットアップのすべてのフェーズにおいて、情報を提供するために使用されます。

Filename.xml は一般情報を含んだ応答ファイルであるとともに、filename.subs から取り込まれる情報のプレースホルダでもあります。提供されている filename.xml と、Microsoft の Windows System Image Manager (SIM) ツールを使用して、このファイルに情報を追加できます情報を追加する場合は、まず対応する wim ファイルを開いてから、filename.xml を開く必要があります。

Vista インストール用の製品キーをこのファイルに指定する必要があります。

このファイルの XML 値は、一切削除しないでくださいこの .xml ファイルを不正に変更すると、重大な問題が発生し、インストールに失敗する可能性があります。

SIM ツールの [Messages] セクションで「…値 $$SUBSTR$$ が無効です…」などのエラーが表示されても、無視して構いませんファイルを保存するときには、「応答ファイルには、検証エラーがあります続行してもよろしいですか ?」に類似したメッセージが表示される場合があります **[はい]** をクリックして続行してください。

filename.subs は、filename.xml で修正される各 XML アイテムと、推奨の修正値の一覧を示す置換ファイルです置換ファイル内の行は XPATH と呼ばれます。

filename.subs ファイルに入力した情報は、filename.xml の情報より優先されます。

置き換えの例

置き換えの仕組みについて理解するには、以下の例を検討してください。この例では、JoinDomain 属性を、filename.xml 内の anything から unattend.xml の VistaTeam に設定する方法を示しています。

< > で囲まれたコードは、xml ファイル内ではすべて 1 行で表示される必要があります。

1 sample.xml ファイルから抽出した JoinDomain の XML 要素を確認します。

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <settings pass="specialize">
```

```
<component name="Microsoft-Windows-UnattendedJoin"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS" xmlns:wcm="http://
schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http:/
/www.w3.org/2001/XMLSchema-instance">
            <Identification>
                <JoinDomain>anything</JoinDomain>
            </Identification>
        </component>
    </settings>
<cpi:offlineImage cpi:source="wim://hpfcovcm/c$/vista_inst/
vista.wim#Windows Vista ULTIMATE"
xmlns:cpi="urn:schemas-microsoft-com:cpi"/>
</unattend>
```

2 sample.subs. にある次の XPATH 要素を変更します。この XPATH 要素は、sample.subs ファイルでは 1 行で表示されていることに注意してください。

```
//un:settings[@pass='specialize']//
un:component[@name=Microsoft-Windows-UnattendedJoin'][@pr
ocessorArchitecture='x86']/un:Identification/
un:JoinDomain,VistaTeam
```

3 オペレーティング システムの配布中、filename.subs と filename.xml が結合されて unattend.xml ファイルが作成されます。unattend.xml ファイルは、ターゲット デバイスでの Windows セットアップのすべてのフェーズにおいて、情報を提供するために使用されますこの例では、JoinDomain 属性が VistaTeam に設定されます。

filename.xml の準備

SIM ツールを使用して、製品キーや、お使いの環境に合わせて変更する必要がある他の情報を変更します。

OS イメージのパブリッシュ

以下のセクションでは、Administrator Publisher を使用してオペレーティング システム イメージをパブリッシュする方法を説明します。

オペレーティング システム イメージをパブリッシュするには

1 Publisher を起動します (379 ページの「Publisher を起動するには」を参照)。

2 ログオン画面で、管理者ユーザー ID およびパスワードを入力して、**[OK]** をクリックします。

> HPCA のユーザー名とパスワードを使用して、Publisher にログインしますデフォルトでは、ユーザー名は **admin**、パスワードは **secret** です。

3 [パブリッシュ オプション] 領域で以下の操作を実行します。

— シン クライアントへパブリッシュしている場合は、**[シン クライアントのパブリッシュ]** を選択します。

— ドロップダウン リストから、**[OS イメージ]** を選択します。

4 **[OK]** をクリックします [OS イメージ ファイルの選択] ウィンドウが開きます。

5 [選択] ウィンドウを使用して、パブリッシュするファイルを探し、選択します (Image Preparation Wizard を使用して作成されるイメージは、HPCA Server の `C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\upload` に保存されます)。

6 続行する前に、**[説明]** 領域を使用して、ファイルを確認します説明に情報を追加することもできます。

7 **[次へ]** をクリックします。

`.WIM` ファイルをパブリッシュすることを選択した場合は、[WIM 配布設定] ウィンドウが開きます `.IMG` ファイルをパブリッシュする場合は、次の手順に進みます。

a **[配布方法]** ドロップダウン リスト ボックスで、[ImageX] を選択します。

b **[送信元]** ディレクトリは空白のままにしますこれは必須ではありません。

c **[クライアント メディアのロケーション]** で、HPCA Agent メディアの正しいパスに沿って参照します (これは、HPCA メディアの `Media\client\default` フォルダです)。

このファイルをすでにパブリッシュしている場合は、**[以前にパブリッシュされた既存のパッケージを使用]** を選択し、適切なパッケージを選択できます。

8 **[次へ]** をクリックします [アプリケーションの情報] ウィンドウが表示されます。

9 **[アプリケーションの情報]** セクションを使用して、サービスの情報を入力します。

10 **[次へ]** をクリックします [要約] ウィンドウが表示されます。

11 **[要約]** 情報を確認して、前の手順で指定したパッケージおよびサービスの情報を検証します情報を確認したら、**[パブリッシュ]** をクリックします。

12 パブリッシュ プロセスが完了したら、**[完了]** をクリックして Publisher を終了します。

これで、企業内の管理対象デバイスへサービスを配布する準備が整いました。

パブリッシュされたオペレーティング システム イメージ サービスは、[OS 管理] セクションのオペレーティング システム OS ライブラリのリストで確認できます。

OS ADDON/ 追加 POS ドライバのパブリッシュ

イメージが新しいローカル パーティションに置かれた後に配布されるデルタ パッケージを作成することにより、以前に準備したイメージにドライバを追加できますこの操作は、Microsoft のドキュメントに基づく Microsoft Windows セットアップの配布方式に限定されますそれ以外にもオプションがありますが、さらにスクリプトを作成する必要が生じます。

前提条件

- OS サービスをパブリッシュします Publisher により、このサービスの下に OS.ADDON.ServiceName_* という接続が自動的に作成されます。
- OS ドライバ ファイルを作成する場合は、次の操作を実行します。
  - C:\MyDrivers などのディレクトリを作成しますその下に、drivers というサブフォルダが存在する \osmgr.hlp という名前のフォルダを作成します。
  - 個々のドライバを …\drivers に保存するか、…\drivers の下に追加のサブディレクトリを作成します。
- Service OS ドライバ ファイルを作成する場合は、次の操作を実行します。
  - C:\MyServiceDrivers などのディレクトリを作成しますそのディレクトリの下に、\work という名前のディレクトリを作成します。
  - 個々のドライバを…\work に保存するか、…\work の下に追加のサブディレクトリを作成します。

デルタ パッケージをパブリッシュするには

1 **[スタート] > [すべてのプログラム] > [HP Client Automation Administrator Publisher] > [HP Client Automation Admin Publisher] に移動します**ログオン画面が表示されます。

2 [ユーザー ID] テキスト ボックスに、HPCA Administrator のユーザー ID とパスワード (**admin** と **secret**) を入力します。

3 [パブリッシュ オプション] ウィンドウで、ドロップダウン リストから [OS ADDON/ 追加 POS ドライバ] を選択します。

4 **[OK]** をクリックします。

5 [ドライバの選択] ウィンドウを使用して、適切なディレクトリからパブリッシュするファイルを選択します。

6 [ADDON タイプ] ドロップダウン リストから、OS ドライバ ファイルか Service OS ドライバを選択します。

7 [ターゲット サービスの選択] ドロップダウン リストから、これらのドライバに追加する OS サービスを選択します。

8 省略可能な [サフィックス] テキスト ボックスには、パッケージの追跡に使用可能な番号を入力できますたとえば、VISTA_PDD というインスタンスの場合にこのテキスト ボックスに「0」と入力すると、新しい ADDON インスタンス名は VISTA_PDD_0 となります。

9 [ADDON インスタンス名] テキスト ボックスには、選択した OS サービス名に基づいて、インスタンス名があらかじめ設定されますこの名前はそのままにすることをお勧めしますこの名前を修正すると、自分で接続を作成しない限り、OS サービスと ADDON インスタンスの間の接続がなくなります。

10 **[次へ]** をクリックします。

11 要約画面の内容を確認し、**[パブリッシュ]** をクリックします。

CSDB Editor を使用して、PRIMARY.OS.ADDON の新しい ADDON インスタンスを確認できます。オペレーティング システム サービスを次回に配布するときには、そのサービスと一緒にデルタ パッケージが自動的に配布されます。

BIOS 設定のパブリッシュ

Publisher を使用して、クライアント デバイスへ配布するために、BIOS 設定ファイルをサービスとしてパブリッシュします設定ファイルを使用して、BIOS 設定 (起動順序など) の更新や変更、またはクライアント デバイスの BIOS パスワードの変更ができます。

BIOS 設定ファイルのサンプル (`Common HP BIOS Settings.xml`) は、Publisher のインストールに組み込まれており、デフォルトでは `C:\Program Files\Hewlett-Packard\HPCA\Agent\BIOS` に配置されますこのファイルを使用して、ターゲット デバイスの BIOS 設定を変更します。

BIOS 設定ファイルのサンプルに必要なオプションが含まれていない、または特定のデバイス用の設定ファイルを作成する場合は、393 ページの「BIOS 設定ファイルの作成」を参照してください。

BIOS 設定をパブリッシュするには

1. Publisher を起動します (379 ページの「Publisher を起動するには」を参照)。
2. ログオン画面で、管理者ユーザー ID およびパスワードを入力して、**[OK]** をクリックします。

   HPCA のユーザー名とパスワードを使用して、Publisher にログインしますデフォルトでは、ユーザー名は **admin**、パスワードは **secret** です。

3. [パブリッシュ オプション] 領域で、**[HP BIOS 設定]** を選択して、**[OK]** をクリックします [選択] ウィンドウが開きます。
4. パブリッシュする BIOS 設定ファイルを選択します BIOS 設定ファイルのサンプル (`Common HP BIOS Settings.xml`) は、デフォルトでは `C:\Program Files\Hewlett-Packard\HPCA\Agent\BIOS` に配置されます。
5. 必要な場合は、**[現在の BIOS 管理パスワード]** 領域に BIOS パスワードを入力して確認しますターゲット デバイスに BIOS パスワードがある場合、設定を変更するにはこれが必要です。
6. 現在の BIOS パスワードを変更する場合、**[BIOS パスワードの変更]** を選択し、新しいパスワードを入力して確認しますこれが必要なのは、クライアント デバイスの BIOS パスワードを変更する場合だけです。
7. **[次へ]** をクリックします [BIOS オプション] ウィンドウが表示されます。
8. パブリッシュする BIOS 設定を選択するには、BIOS 設定名の左にあるチェック ボックスをクリックします。

9 BIOS 設定の値を変更する必要がある場合、設定名をクリックして、必要に応じて使用可能なオプションを調整します。

10 **[次へ]** をクリックします [アプリケーションの情報] ウィンドウが表示されます。

11 アプリケーション情報を表示し、必要な場合は変更しますアプリケーション情報は、設定ファイルから利用できる情報に基づいて、あらかじめ決まっています。

12 **[次へ]** をクリックします [要約] ウィンドウが表示されます。

13 要約情報を確認し、それで良ければ、**[パブリッシュ]** をクリックします。

14 パブリッシュ プロセスが完了したら、**[完了]** をクリックして Publisher を終了します。

BIOS 設定サービスは、HPCA Console のソフトウェア ライブラリで利用できます。

BIOS 設定ファイルの作成

HPCA に付属のファイル以外の BIOS 設定ファイルを使用する場合は、HP System Software Manager(SSM) の BIOS 設定ユーティリティを使用して独自の設定ファイルを生成できます。

SSM は、HPCA Agent (`C:\Program Files\Hewlett-Packard\SSM`) と一緒にインストールされます。または、HP のサポート サイトからダウンロードできます。

BIOS 設定ファイルを作成するには

1 コマンド プロンプトを開き、SSM BIOS 設定ユーティリティがあるディレクトリ (デフォルトでは `C:\Program Files\Hewlett-Packard\SSM`) に移動します。

2 次のように入力します。

```
BiosConfigUtility.exe /
GetConfig:"C:\tmp\MyBIOSconfig.xml" /Format:XML
```

このコマンドにより、`MyBIOSconfig.xml` という名前の XML ファイルが生成され、`C:\tmp` に保存されます。

XML ではなくテキスト ファイルを作成する場合は、次のように入力します。

```
BiosConfigUtility.exe /
GetConfig:"C:\tmp\MyBIOSconfig.txt" /Format:REPSET
```

このコマンドにより、MyBIOSconfig.txt という名前のテキスト ファイルが生成され、C:\tmp に保存されます。

3 BIOS 設定をパブリッシュする準備ができたら、392 ページの「BIOS 設定をパブリッシュするには」の手順 6 でこのファイルを選択します。

ハードウェア設定要素のパブリッシュ

このセクションでは、Publisher を使用して、ハードウェア設定要素を HP Client Automation Configuration Server Database にパブリッシュします。

HWCE をパブリッシュする前に、リソース ファイルを 1 つのフォルダに集めてください詳細については、『HP Client Automation OS Manager ハードウェア設定管理ガイド』を参照してください。

ハードウェア設定要素をパブリッシュするには

1 **[スタート] > [すべてのプログラム] > [HP Client Automation Administrator] > [HP Client Automation Administrator Publisher] に移動します** Publisher の使用方法については、『HP Client Automation Administrator ユーザー ガイド』を参照してください。

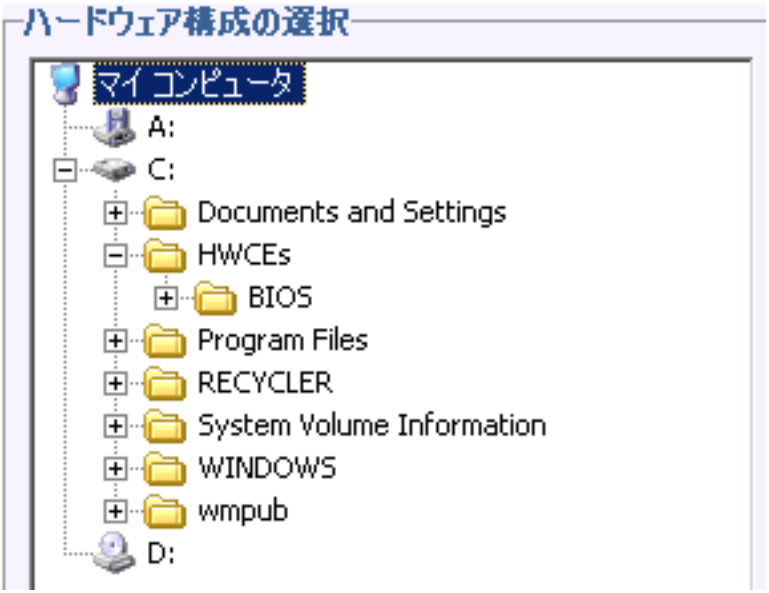
2 ユーザー ID とパスワードを入力します。

3 [パブリッシュ オプション] ドロップダウン リストから、[ハードウェア構成] を選択します。

4 **[OK]** をクリックします。

5 HWCE の作成に必要なリソースを含むフォルダを選択しますこの例では、[C:\HWCEs\BIOS] を選択しています。

このハードウェア構成の配布先システムに適合する正しいファイルを収集したことを確認してください誤ったファイルを選択すると、システムで障害が発生したままになる可能性があります。



6 [説明] フィールドに、パブリッシュする要素の説明を入力しますこの例では、「**Pro32 WS Bios Rev 1.00 Resources**」と入力します。

7 [パッケージ インスタンス名] フィールドに、パッケージのインスタンス名を入力しますこの例では、「**P32_BIOS_100**」と入力します。

8 **[次へ]** をクリックします。

9 情報を確認し、**[パブリッシュ]** をクリックしますパッケージのリソースは、圧縮されない形式でパブリッシュされます。

10 Publisher の処理が完了したら、**[完了]** をクリックします。

11 **[はい]** をクリックして Publisher の終了を確定します。

PRIMARY.OS.PACKAGE で作成されたパッケージを表示するには、CSDB Editor を使用します。

パブリッシュされたサービスの表示

[管理] タブの [ソフトウェア管理] 領域で、パブリッシュされたソフトウェアを確認します。

パブリッシュされたオペレーティング システムは、[オペレーティング システム] 領域に保存されます。

HP Client Automation Administrator Agent Explorer

HP Client Automation Administrator の一部として、Publisher と一緒にインストールされる、Agent Explorer は、トラブルシューティングや問題解決に役立ちますが、HP サポートからの直接の指示がない場合は使用しないでください。

12 Application Self-Service Manager の使用

HP Client Automation Application Self-Service Manager (Self-Service Manager) は、クライアントに常駐し、ユーザーが許可されたオプションのアプリケーションをインストール、削除、および更新できるようにする製品です。アプリケーションのエンタイトルメントは、HPCA 管理者がユーザーに設定する必要があります。Self-Service Manager では、ユーザーにエンタイトルメントのあるアプリケーションのカタログが表示され、ユーザーは、それらのアプリケーションのインストール、削除、および更新を自分で管理できます。Self-Service Manager は、管理エージェントがクライアント デバイスに配布されたときにそのデバイスにインストールされます。

次の各セクションで、Self-Service Manager ユーザー インターフェイスの使用方法を説明します。

Application Self-Service Manager へのアクセス

Self-Service Manager ユーザー インターフェイスには、次のいずれかの方法でアクセスできます。

ユーザー インターフェイスにアクセスするには

- **[スタート] > [プログラム] > [HP Client Automation Agent] > [Client Automation Application Self-Service Manager]** へと移動します。

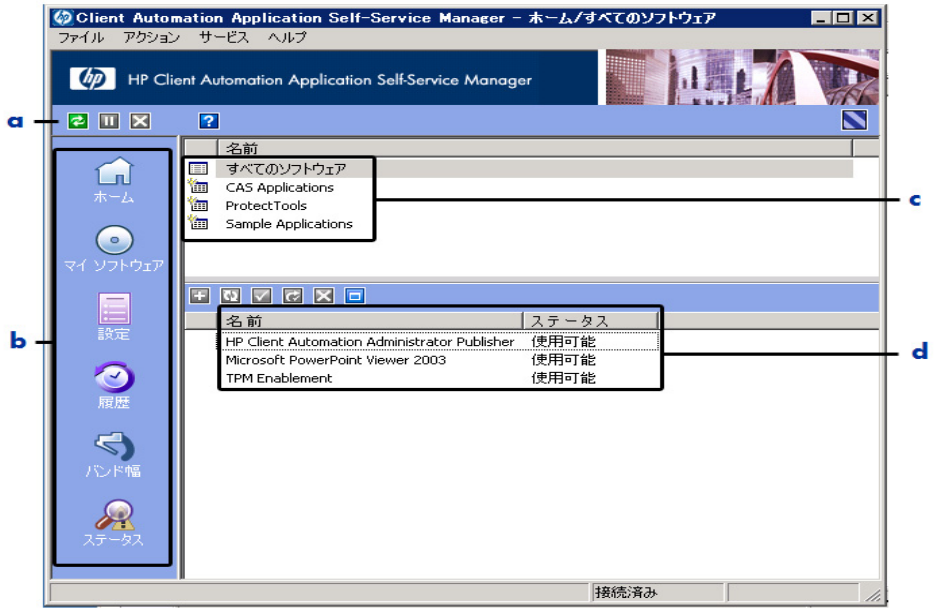
  または

- **[Client Automation Application Self-Service Manager]** デスクトップ ショートカットをダブルクリックします。

Application Self-Service Manager の概要

Self-Service Manager インターフェイス (399 ページの図 48 を参照) には、4 つの主要なセクションがあります。各セクションでは、利用可能なアプリケーションの管理、カタログにあるソフトウェアの情報やステータスの表示、ユーザー インターフェイス表示のカスタマイズができます。

図 48 Application Self-Service Manager ユーザー インターフェイス



凡例

a **グローバル ツールバー** — カタログのリフレッシュや、現在のアクションの一時停止または取り消しができます。

b **メニュー バー** — Application Self-Service Manager を使用するときに利用可能なメニューの選択肢を表示します。

c **カタログ リスト** — 使用できるさまざまなソフトウェア カタログの一覧が表示されます。

d **サービス リスト** — エンタイトルメントが設定されているアプリケーションの一覧が表示されます。

次に示すセクションでは、ユーザー インターフェイスの各セクションを詳細に説明します。

- 「グローバル ツールバー」(この後のセクション)
- メニュー バー 400 ページ
- カタログ リスト 401 ページ
- サービス リスト 401 ページ

グローバル ツールバー

グローバル ツールバーでは、カタログのリフレッシュ、現在のアクションの一時停止、または現在のアクションの取り消しができます。アクションを一時停止すると、**[一時停止]** ボタンを再度クリックしてアクションを再開するか、**[キャンセル]** ボタンをクリックして一時停止したアクションをキャンセルするまで、他のアクションを実行できません。

[グローバル ツールバー] のボタンのうち、現在のアクションで使用できないボタンは、グレー表示になります。

カタログをリフレッシュするには

- 選択したカタログをリフレッシュするには、グローバル ツールバーの **[リフレッシュ]** をクリックします。

現在のアクションを一時停止または再開するには

- 現在のアクションを停止するには、グローバル ツールバーの **[一時停止]** をクリックします。
- 停止したアクションを再開するには、**[リジューム]** をクリックします。(アクションを停止すると、**[停止]** ボタンがこのボタンに変わります)。

現在のアクションをキャンセルするには

- 現在のアクションをキャンセルするには、グローバル ツールバーの **[キャンセル]** をクリックします。

メニュー バー

メニュー バーを使用して、Application Self-Service Manager の設定およびカスタマイズを行います。次のセクションでは、メニュー バーの各アイコンについて説明します。

ホーム : このボタンをクリックすると、ホーム カタログにアクセスできます。

マイ ソフトウェア : このボタンをクリックすると、インストールしたアプリケーションだけが表示されます。

設定 : このボタンをクリックすると、Self-Service Manager のさまざまな表示オプション、アプリケーション リスト オプション、および接続オプションにアクセスできます。

このセクションの右上隅にある **[OK]**、**[適用]**、または **[キャンセル]** をクリックして、いつでも変更内容を保持または無視できます。

カタログ リスト

[カタログ リスト] セクションには、使用可能なソフトウェア カタログおよび仮想カタログの一覧が表示されます。

カタログを選択するには

- [カタログ リスト] で、[サービス リスト] セクションに表示するカタログをクリックします。カタログをリフレッシュするには、カタログの名前を右クリックして、ショートカット メニューから **[リフレッシュ]** を選択します。

仮想カタログ

仮想カタログは、HPCA の [ソフトウェアの詳細] で管理者が定義した、デフォルトのカタログのサブセットです。カタログ グループの値が同じサービスは、1 つの仮想カタログにグループ化されます。次のイメージは、いくつかのサンプルのカタログを表示しています。

サービス リスト

[サービス リスト] セクションには、利用可能なアプリケーションが一覧表示されます。インストール済みのアプリケーションの横には、チェック マークが表示されます。カラムの見出しは、必要に応じて変更できます。詳細については、

400 ページの「設定 : このボタンをクリックすると、Self-Service Manager のさまざまな表示オプション、アプリケーション リスト オプション、および接続オプションにアクセスできます。」を参照してください。

表 46　[サービス リスト] セクションのボタン

ボタン	アクション	説明
	インストール	選択したサービスをマシンにインストールします。
	検証	選択したサービスのファイルを検証します。
	修復	選択したサービスを修復します。
	削除	選択したサービスをマシンから削除します。
	展開 / 折りたたむ	選択したサービスを展開したり、折りたたんだりします。

[サービス リスト] セクションのボタンは、選択したアプリケーションに対して使用できない場合、グレー表示になります。

Application Self-Service Manager ユーザー インターフェイスの使用

ユーザー インターフェイスを使用して、ソフトウェアのインストールと削除、利用可能なアプリケーションのカタログのリフレッシュ、およびアプリケーションに関する情報の表示を行います。メニュー バーには、セッション履歴の表示、バンド幅の調整、およびアプリケーションの現在のステータスの表示のためのボタンがあります。詳細については、次の各セクションを参照してください。

- ソフトウェアのインストール 403 ページ
- カタログのリフレッシュ 404 ページ
- 情報の表示 404 ページ
- ソフトウェアの削除 405 ページ

ソフトウェアのインストール

利用可能なアプリケーションは、サービス リストに一覧表示されます。これらのアプリケーションから 1 つ以上をいつでもインストールできます。

ソフトウェアをインストールするには

1 サービス リストで、インストールするアプリケーション名をクリックします。

2 **[インストール]** ボタン をクリックします。

インストールによっては、一連のダイアログ ボックスが表示される場合があります。その場合、表示される指示に従ってください。それ以外の場合は、インストールがすぐに始まります。

インストールするアプリケーションの名前を右クリックして、表示されるショートカット メニューの **[インストール]** をクリックしても同じ操作を実行することができます。

インストールの進行状況が、進行状況バーに表示されます。

— インストールをキャンセルするには、グローバル ツールバーの **[キャンセル]** をクリックします。

— インストールを一時停止するには、グローバル ツールバーの **[一時停止]** をクリックします。アクションを一時停止すると、一時停止しているアクションをキャンセルまたは再開するまで、他のアクションを実行できません。

カタログのリフレッシュ

カタログは、Self-Service Manager のユーザー インターフェイスにログインするたびにリフレッシュされます。ログインしている間に、使用が認可されているアプリケーションのリストが変わった、またはインストールしたアプリケーションの更新が使用可能になったと考えられる場合は、グローバル ツールバーの **[カタログのリフレッシュ]** をクリックして、アプリケーションのリストを更新します。

ソフトウェア リストの任意のアイテムを右クリックして、表示されるショートカット メニューの **[カタログをリフレッシュ]** をクリックしても同じ操作を実行することができます。

情報の表示

サービス リストには基本的な情報が表示されますが、アプリケーションに関する詳細な情報 (ベンダー、バージョン、サイズ、インストール日など) は、次の方法で取得できます。

- これらのカラムをサービス リストに追加する。
- 展開したサービス ボックスで、**[拡張情報を表示]** をクリックする。

メーカーからの詳細情報が必要な場合は、ベンダーのリンクをクリックします。

詳細情報を表示するには

1 サービス リストでアプリケーションを選択し、**[拡張情報を表示]** をクリックします。

アプリケーションを右クリックし、表示されるショートカット メニューの **[プロパティ]** をポイントし、**[情報]** をクリックしても同じ操作を実行することができます。

2 サービス リストに戻るには、対応する **[キャンセル]** ボタンをクリックします。

ソフトウェアの削除

コンピュータからアプリケーションを削除するには、**[削除]** ボタン を使用します。

ソフトウェアを削除するには

1 削除するアプリケーションを選択します。

2 **[削除]** をクリックします。

3 アプリケーションの削除を確認するメッセージが表示されたら、**[はい]** をクリックします。

削除するアプリケーションの名前を右クリックして、表示されるショートカット メニューの **[削除]** をクリックしても同じ操作を実行することができます。

ソフトウェアの検証

アプリケーションのインストールをチェックするには

1 インストールされている検証対象のサービスをサービス リストで選択します。

2 [**検証**] をクリックします。

> ソフトウェア名を右クリックし、表示されるショートカット メニューの [**検証**] をクリックしても同じ操作を実行することができます。

— 検証でアプリケーションに問題がない場合は、アプリケーションの [検証した日付] カラムに検証の日付と時刻が表示されます。

— 検証でアプリケーションに問題がある場合は、[ステータス] カラムに [破損] と表示されます。

3 ソフトウェアを修復するには、[**修復**] をクリックします。

ソフトウェアの修復

アプリケーションに何らかの問題がある場合、それを修復するには、[**修復**] をクリックします。

ソフトウェアを修復するには

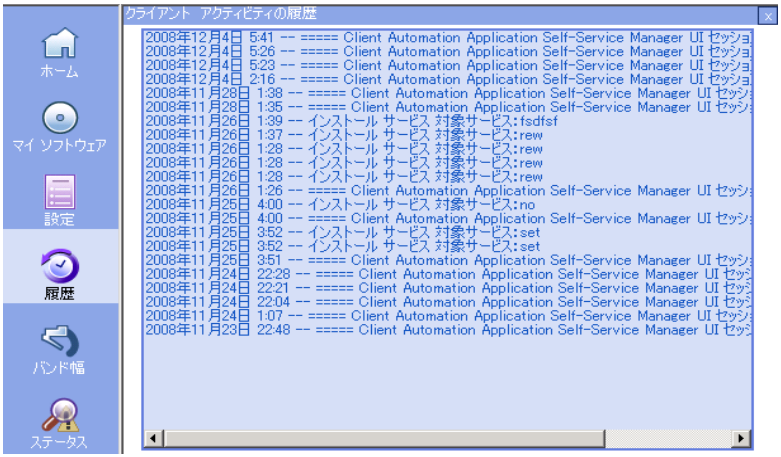
1 修復する必要があるアプリケーションを選択します （ 該当するアプリケーションには、最初のカラムに X、[ステータス] カラムに [破損] が表示されます)。

2 [**修復**] をクリックします。HPCA によってアプリケーションの修復に必要なファイルが取得されます。

履歴の表示

1 メニュー バーの **[履歴]** をクリックして、現在のセッションの履歴を表示します。

図 49　[履歴] ウィンドウ



2　[履歴] ウィンドウを閉じて、サービス リストに戻ります。

バンド幅の調整

メニュー バーの **[バンド幅]** をクリックして、バンド幅のスライダを表示します。この値を変更すると、スロットリングの値が動的に変化します。

バンド幅のスライダを使用してバンド幅の設定を調整するには

- スライダをドラッグして、目的のバンド幅スロットリングの量にまで値を増減して調整します。
- バンド幅スロットリングは、[設定] の [接続オプション] セクションでも調整できます。

ステータスの表示

メニュー バーの **[ステータス]** をクリックすると、サイズ、推定時間、進捗状況、使用可能なバンド幅など、現在のアクションのステータスが表示されます。

図 50　選択したアプリケーションのステータス表示

[ステータス] ウィンドウは、Application Self-Service Manager からドッキングしたりドッキングを解除したりできます。これにより、画面上の任意の位置に [ステータス] ウィンドウを移動できます。デフォルトでは、[ステータス] ウィンドウはドッキングされています。

[ステータス] ウィンドウのドッキングを解除するには

1　メニュー バーの **[ステータス]** をクリックします。

2　表示された [ステータス] ウィンドウ上で右クリックします。

3　ショートカット メニューから **[ドッキング済み]** を選択します。[ステータス] ウィンドウがドッキングされている場合、ショートカット メニューの **[ドッキング済み]** の横にチェック マークが表示されます。

Application Self-Service Manager インターフェイスから [ステータス] ウィンドウが分離され、画面上の任意の場所に移動できるようになります。

[ステータス] ウィンドウをドッキングするには

1　メニュー バーの **[ステータス]** をクリックします。

2　表示された [ステータス] ウィンドウ上で右クリックします。

3 ショートカット メニューの **[ドッキング済み]** をクリックします (チェック マークが表示されていない場合のみ)。

[ステータス] ウィンドウが Application Self-Service Manager インターフェイスにドッキングされます。

ユーザー インターフェイスのカスタマイズ

メニュー バーの **[設定]** ボタンをクリックして、利用可能なカスタマイズ オプションを表示します。次のセクションで各カスタマイズ領域について説明します。

- 全般オプション 409 ページ
- サービス リスト オプション 411 ページ
- 接続オプション 414 ページ

全般オプション

Application Self-Service Manager インターフェイスの外観を変更するには、[全般オプション] ウィンドウを使用します。

図 51　[全般オプション] ウィンドウ

表示を変更するには

- メニューを表示する場合は、**[メニューを表示]** を選択します。
- カタログ リストを表示する場合は、**[カタログ リストを表示]** を選択します。
- 各セッションの開始時にオフライン モードで Application Self-Service Manager を使用するかを確認するプロンプトを表示するには、**[オフライン モードのプロンプトを表示]** チェック ボックスをオンにします。
- オプション バーを自動的に非表示にするには、**[自動非表示オプションバー]** をオンにします。

色を変更するには

- システムの色を使用する場合は、**[システムの色を使用]** をオンにします。
- カラー スキームをカスタマイズする場合は、**[色のカスタマイズ]** をオンにします。
  - [色のカスタマイズ] をクリックした場合、目的に応じて以下のラベルのボックスをクリックします。

– **[選択色を設定]**。選択した色を変更します。
– **[ボタンの色を設定]**。ボタンの色を変更します。
– **[背景色を設定]**。背景色を変更します。
– **[作業領域の色を設定]**。作業領域を変更します。

サービス リスト オプション

サービス リストの外観を変更するには、**[サービス リスト オプション]** を使用します。

図 52　サービス リスト オプション

サービス リストのカラム名をカスタマイズするには

サービス リストに表示されるカラムをカスタマイズするには、[カラム] 領域を使用します。右のカラムには、現在サービス リストに表示されているカラムの名前が一覧表示されます。利用可能な各カラム見出しの説明については、412 ページの「表示のカスタマイズ」を参照してください。

サービス リストにカラムを追加するには

- [使用可能なカラム] リスト ボックスで、1 つ以上の名前を選択し、**[追加]** をクリックします。選択したカラムが [表示するカラム] リスト ボックスの一覧に表示されます。

サービス リストからカラムを削除するには

1. [表示するカラム] リスト ボックスで、1 つ以上の名前を選択します。連続した複数のカラム名を選択するには **Shift** キーを押しながらカラム名をクリックし、連続していない複数のカラム名を選択するには **Ctrl** キーを押しながらカラム名をクリックします。
2. **[削除]** をクリックします。選択したカラムが [表示するカラム] リスト ボックスから削除され、元の [使用可能なカラム] ボックスに表示されます。

表示のカスタマイズ

- サービス リストで、現在のサービス アイテムを展開するには、**[アクティブなサービス アイテムを展開]** チェック ボックスをオンにします。
- 各サービスを仕切るグリッド線付きでサービス リストを表示するには、**[グリッド線を表示]** を選択します。
- 現在選択しているカタログを展開するには、**[アクティブなカタログ アイテムを展開]** を選択します。
- **[詳細なオペレーションを表示]** は現時点では利用できません。

表 47　サービス リストで利用可能なカラムの見出し

カラムの見出し	説明
適応バンド幅	バンド幅スロットリングを使用するときに使用されるバンド幅の適用最小割合。
警告メッセージ	エンド ユーザーに長いアプリケーション説明または指示のメッセージを表示 (警告 / 延期設定の一部としてオプションのサービス テキスト フィールド)。
作成者	サービスの作成者。
Avis	内部で使用するためだけのサービス ステータス フラグ。
圧縮後のサイズ	圧縮後のサービスのサイズ (バイト単位)。
説明	アプリケーションの簡単な説明。
エラーコード	現在のサービスのステータス。例 : 初期 = 999。メソッドの失敗 = 709。

表 47　サービス リストで利用可能なカラムの見出し

カラムの見出し	説明
インストール日	アプリケーションがコンピュータにインストールされた日付。
ローカルの修復	ローカルでのデータ修復可能性 (データがローカル コンピュータにキャッシュされているかどうか)。
必須	アプリケーションで定義される必須 / オプション ファイル (内部使用)。
名前	アプリケーションの名前。
オーナー カタログ	アプリケーションの取得元のドメイン名。
価格	サービスの価格。
パブリッシュ日	アプリケーションがカタログにパブリッシュされた日付。
再起動	サービスの再起動設定 (内部使用)。
再パブリッシュ日	アプリケーションがカタログに再パブリッシュされた日付。
予約済みのバンド幅	バンド幅スロットリングを使用するときに使用されるバンド幅の予約済み最大割合。
スケジュールを許可	エンド ユーザーがローカルにアプリケーションの更新スケジュールを変更できるかどうかを指定。
サイズ	アプリケーションのサイズ (バイト単位)。 注意 ：アプリケーションを正常にインストールするには、このカラムで表示される空き容量がコンピュータに必要です。
ステータス	アプリケーションの現在のステータス • 使用可能 • インストール済み • 更新可能 • 破損
システムのインストール	システム アカウントを使用してアプリケーションがインストールされるかどうかを表示。
スロットリング タイプ	使用するバンド幅スロットリングのタイプ。可能な値は、ADAPTIVE、RESERVED、または NONE。
オプション	ステータス ウィンドウを表示するかどうかを決定。
アップグレード日	アプリケーションがアップグレードされた日付。

表 47　サービス リストで利用可能なカラムの見出し

カラムの見出し	説明
URL	ソフトウェア ベンダーの Web アドレス。
ベンダー	アプリケーションを提供したソフトウェア ベンダー。
検証日	前回、アプリケーションが検証された日付。
バージョン	アプリケーションのバージョン。

接続オプション

使用するバンド幅スロットリングのタイプの選択や、プロキシ サーバー設定の指定には、**[接続オプション]** (414 ページの図 53 を参照) を使用します。

図 53　接続オプション

- スロットリング
  - スロットリングを行わない場合、**[なし]** を選択します。

— 使用するネットワーク バンド幅の最大の割合をスケールに基づいてスライドするには、**[バンド幅を予約]** を選択します。ユーザーは、ダウンロード時に予約バンド幅をインターフェイスで変更できます。

— 使用するネットワーク バンド幅の最小の割合をスケールに基づいて指定するには、**[トラフィックに適応]** を選択します。適応バンド幅は、データ ダウンロード プロセスの間は変更できません。設定できるのは、ジョブがディスパッチされる前だけです。

- **プロキシ**

— Application Self-Service Manager は、インターネット プロキシが使用されると、それを検出できます。検出されたインターネット プロキシのアドレスは、クライアント コンピュータの `IDMLIB` ディレクトリにある `PROXYINF.EDM` に格納されます。IDMLIB のデフォルトのロケーションは、`SystemDrive:\Program Files\Hewlett-Packard\HPCA\Agent\Lib` です。次回、HPCA Agent コンピュータが HPCA Server に接続するときには、指定したインターネット プロキシが使用されます。この機能を使用するには、HPCA Agent でインターネット プロキシを使用および検出できるようにする必要があります。

HPCA System Tray アイコン

HP Client Automation システム トレイ アイコンを使用すると、ユーザーは、ステータスや統計情報を確認したり、一時停止やキャンセルの操作を行ったりすることができます。

図 54　HPCA System Tray アイコン

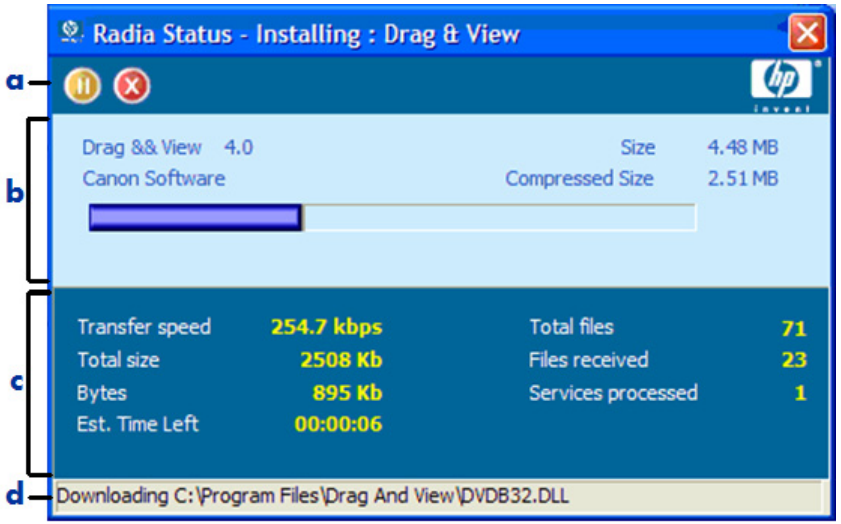
HPCA の状態を表示するには、カーソルをアイコンの上に移動します。

- **アイドル**: アクションが処理中でなく、ユーザーの介入を必要としないとき、アイコンはスタティックです。システム トレイ アイコンは、アイドル状態では非表示になる場合があります。
- **アクティブ**: Application Self-Service Manager が実行中のとき、またはユーザーの介入が必要なときに、アイコンはアクティブになります。アイコンの上にカーソルを合わせると、活動情報を示すポップアップが表示されます。重要な通知が発生した場合は、ポップアップが自動的に表示されます。

[HPCA ステータス] ウィンドウ

HPCA System Tray アイコンを左クリックして、[ステータス] ウィンドウを表示します。次の図で示すように [ステータス] ウィンドウが開きます。

図 55　HPCA ステータス



凡例

a　ボタン バー

b　情報パネル

c　ステータス領域

d　ステータス メッセージ

[ステータス] ウィンドウには次の領域があります。

- **ボタン バー**: [一時停止] ボタン、[キャンセル] ボタン、および HPCA Agent が実行中にアニメーション表示になるロゴがあります。
- **情報パネル**：この領域には、アクティブなアプリケーションに関する情報が表示され、完了したタスクの割合を示す進行状況バーも表示されます。
- **ステータス領域**：転送速度、送信の合計サイズ、受信したバイト数、送信の推定残り時間、送信するファイルの総数、受信したファイルの数、処理されたサービスの数など、アクティブなプロセスに関する統計が表示されます。

- **ステータス メッセージ領域**：現在のプロセスに関するメッセージが表示されます。
  - **バンド幅設定**：HPCA Server のアプリケーションにバンド幅スロットリングを設定している場合、システム トレイ コンソールのバンド幅トグルボタン  をクリックすると、バンド幅設定用のスライダが表示されます。バンド幅スロットリングの値を変更するには、スライダを調整します。

13 トラブルシューティング

次のセクションを使用して、HPCA の使用中に遭遇する一般的な問題のトラブルシューティングを行います。

ログ ファイル

HPCA の各種ログ ファイルは、サーバー上の `C:\Program Files\Hewlett-Packard\HPCA` 以下の次のディレクトリに格納されています。

- `\Agent\Log`
- `\ApacheServer\logs`
- `\ApacheServer\apps\cas\logs`
- `\ApacheServer\apps\console\logs`
- `\BootServer\logs`

- \ClientConfigurationManager\logs
- \ConfigurationServer\log
- \dcs\log
- \DistributedCS\logs
- \Knowledge Base Server\logs
- \ManagementPortal\logs
- \MessagingServer\logs
- \MiniManagementServer\logs
- \MulticastServer\logs
- \OOBM\logs
- \OSManagerServer\logs
- \PatchManager\logs
- \PolicyServer\logs
- \ProxyServer\logs
- \ReportingServer\log
- \tomcat\logs
- \VulnerabilityServer\logs

ログ ファイルのサイズは、時間が経過するにつれて大きくなります。ログには、HPCA サービスの動作中に使用されるものもあります。これらのアクティブなログ ファイルを削除しないでください。履歴ログ ファイルは必要に応じてアーカイブしたり削除したりできます。

ログファイルは、HPCA Core Console の [サポート] ページの [インフラストラクチャ管理] 領域にある [操作] タブを使用してダウンロードできます。

OS 配布の問題

この章では、オペレーティング システム イメージの配布中に遭遇する一般的な問題について説明します。

TFTP サーバーが起動後にシャットダウンする

- 同じコンピュータで他の TFTP サーバーが動作していないことを確認します。

PXE がサブネットを横断できない

- PXE がサブネットを自由に移動するには、DHCP ヘルパーが有効である必要があります。DHCP ヘルパーは、DHCP ポートでのブロードキャスト トラフィックの横断を許可します。通常、ブロードキャストはルーターではオフになっています。

Application Self-Service Manager の問題

このセクションでは、HP Client Automation Application Self-service Manager (ASM) のよくある問題および問題を解決する手順を説明します。

アプリケーションのインストールが失敗し、カタログにはインストールされたと表示される

問題

インストール プログラムが失敗時にゼロを返すと、カタログには、アプリケーションがインストールされたと表示される場合があります。

対処法

ASD は、インストールが成功したかどうかを検出するのに、リターン コードを信頼しています。ASM が失敗を検出するには、インストールはゼロ以外のコードを返す必要があります。

このためには、インストールをコマンド ファイルにラッピングし、正しいコードを返すことでプロセスが成功したかどうかを確認するロジックを使用します。

電源管理の問題

このセクションでは、HPCA の電源管理機能に関連するタスクの問題と対処法を説明しています。

デバイスが HPCA Server からの電源コマンドに応答しない

管理対象デバイスが、HPCA Server からの電源オン コマンドに応答しない場合、ルーターやスイッチなどのネットワーク デバイスの設定に問題があることがあります。

- Wake on LAN サポートについて、HPCA Server から管理対象デバイスへのネットワーク パスをテストします。ネットワーク デバイスにリモートの電源オン コマンドを送信するためのサード パーティ製ツールが、いくつかあります。インターネットで「Wake on Lan ツール」を検索すると、この機能をテストするための無料のツールが見つかります。

パッチ管理の問題

このセクションでは、パッチ管理に関連するタスクの問題と対処法を説明しています。

パッチ配布時のエラー

ターゲット デバイスへのパッチの配布時にエラーが発生する場合 (`WUA Install Result Code 3 HRESULT $hresult` などのエラー メッセージが表示されます)、パッチの更新を受け取るターゲット デバイスに適切なバージョンの Windows インストーラがインストールされているかを確認します。

HPCA Server のトラブルシューティング

次のセクションでは、HPCA Server に関する問題のトラブルシューティングについて説明します。

- HPCA Core コンポーネントのトラブルシューティング 422 ページ
- HPCA Satellite コンポーネントのトラブルシューティング 426 ページ

HPCA Core コンポーネントのトラブルシューティング

次のセクションでは、Core Server のコンポーネントに関連する問題のトラブルシューティングについて説明します。

- HPCA Cpre の設定ファイル 423 ページ

- HPCA Core のログ ファイル 425 ページ

HPCA Cpre の設定ファイル

Core Server のインストールでは、さまざまな Core Server コンポーネントのデフォルト値が設定されます。これらの値は変更する必要がありませんが、一部の値は Core Console で変更できます。次の表では、トラブルシューティングに必要な場合または HP テクニカル サポートからリクエストされた場合に備えて、設定ファイルの場所と名前を一覧表示します。

Core Server の製品設定ファイルへのデフォルトのパスは、`C:\Program Files\Hewlett-Packard\HPCA\`*`xxxxxx`* です。Core のインストール中に異なるパスを指定した場合、そのパスに従ってください。xxxxxx の値は、次の表の場所カラムの値で置き換えます。

表 48　HPCA Cpre の設定ファイル

HPCA 製品	設定ファイルのタイプ	場所とファイル名 (C:\Program Files\Hewlett-Packard\HPCA\...)
HPCA console	Apache Server	ApacheServer\apps\console\etc\service.cfg
	Apache Server	ApacheServer\apps\console\etc\proxy.cfg
	Sessionmanager	tomcat\webapps\sessionmanager\WEB-INF\sessionmanager.properties
	Sessionmanager	tomcat\webapps\sessionmanager\WEB-INF\classes\log4j.properties
Configuration Server		ConfigurationServer\bin\edmprof.dat
Distributed Configuration Server	Integration Server	DistributedCS\etc\HPCA-DCS.rc
	product	DistributedCS\etc\dcs.cfg
Messaging Server		MessagingServer\etc\core.dda.cfg

表 48　HPCA Cpre の設定ファイル

HPCA 製品	設定ファイルのタイプ	場所とファイル名 (C:\Program Files\Hewlett-Packard\HPCA\...)
		MessagingServer\etc\patch.dda.cfg
		MessagingServer\etc\rms.cfg
		MessagingServer\etc\usage.dd.acfg
OS Manager Server		OSManagerServer\etc\HPCA-OSM.rc
		OSManagerServer\etc\roms.cfg
		OSManagerServer\etc\roms_upd.cfg
Patch Manager		PatchManager\etc\HPCA-PATCH.rc
		PatchManager\etc\patch.cfg
Policy Server		PolicyServer\etc\HPCA-PM.rc
		PolicyServer\etc\pm.cfg
Portal	Integration Server	ManagementPortal\etc\HPCA-RMP.rc
	product	ManagementPortal\etc\rmp.cfg
		ManagementPortal\etc\romad.cfg
	OpenLDAP	DirectoryService\openldap
Reporting Server		ReportingServer\etc\cba.cfg
		ReportingServer\etc\ccm.cfg
		ReportingServer \etc\ed.cfg
		ReportingServer\etc\rim.cfg
		ReportingServer\etc\rm.cfg
		ReportingServer\etc\rpm.cfg

表 48　HPCA Cpre の設定ファイル

HPCA 製品	設定ファイルのタイプ	場所とファイル名 (C:\Program Files\Hewlett-Packard\HPCA\...)
		ReportingServer\etc\rrs.cfg
		ReportingServer\etc\rum.cfg
		ReportingServer\etc\scm.cfg
		ReportingServer\etc\vm.cfg
シン クライアント		TC\etc\HPCA-TC.rc TC\etc\rmms.cfg
Tomcat	Enterprise Manager	tomcat\webapps\em\WEB-INF\ Console.properties
	Enterprise Manager	tomcat\webapps\em\WEB-INF\classes\log4j.properties
	OPE	tomcat\webapps\ope\WEB-INF\classes\ log4j.properties（ログ レベル）
	VMS	tomcat\webapps\vms\WEB-INF\classes\ log4j.properties（ログ レベル）

HPCA Core のログ ファイル

Core Server に問題があり、トラブルシューティングのためにそのログ ファイルにアクセスする必要がある場合、Core Console ではすべてのログ ファイルに即座にアクセスできます。

Core Server のログ ファイルを生成するには

1　Core Console の [操作] タブで、**[サポート]** をクリックします。

2　[トラブルシューティング] 領域で、**[現在のサーバー ログ ファイルをダウンロード]** をクリックします。

3　WinZip ファイルを開くと、ファイルが展開され、保存されます。

ファイルのすべての内容を理解する必要はありませんが、次の場合のためにこれらのファイルのアクセス方法および表示方法は知っておく必要があります。

- HP サポートにログ ファイルを提出する。
- 「**severe**」ラベルが付与されたエントリを確認する。

HPCA Satellite コンポーネントのトラブルシューティング

次のセクションでは、Satellite コンポーネントのトラブルシューティング方法について説明しています。

- HPCA Satellite のログ ファイル 426 ページ

HPCA Satellite のログ ファイル

Satellite Server に問題があり、トラブルシューティングのためにそのログ ファイルにアクセスする必要がある場合、Satellite Console ではすべてのログ ファイルに即座にアクセスできます。

Satellite Server のログ ファイルにアクセスするには

1 Satellite Console の [操作] タブで、**[サポート]** をクリックします。

2 [トラブルシューティング] 領域で、**[現在のサーバー ログ ファイルをダウンロード]** をクリックします。

3 WinZip ファイルを開くと、ファイルが展開され、保存されます。

ログのすべての内容を理解する必要はありませんが、次の場合のためにこれらのログのアクセス方法および表示方法は知っておく必要があります。

- HP サポートにログ ファイルを提出する。
- 「**severe**」ラベルが付与されたエントリを確認する。

ブラウザの問題

次のトラブルシューティングのヒントは、ブラウザで発生する問題に関するものです。

F5 キーを使用してページをリフレッシュできない

HPCA Enterprise Console の使用時に **F5** ファンクション キーを押すと、起動画面が短く表示され、最後に表示されていたダッシュボード ページに戻ります。現在表示されているページをリフレッシュできません。

解決策 :

現在表示されているページをリフレッシュするには、ページ内の  (リフレッシュ) ボタンを使用します。

Internet Explorer 6 と SSL を使用して HTTP 1.1 を有効化できない

HTTP 1.1 が有効な場合、SSL が有効である Internet Explorer 6 を使用して HPCA Enterprise Console を実行できません。これは、Internet Explorer 6 の制限事項です。

解決策 :

Internet Explorer 6 で次の手順を実行します。

1. **[ツール]→[インターネット オプション]** の順にクリックします。
2. **[詳細設定]** タブをクリックします。
3. 画面を下にスクロールして [HTTP 1.1 設定] を表示します。
4. **[HTTP1.1 を使用する]** チェック ボックスをオフにします。

次に、Internet Explorer を閉じて、新しいブラウザ ウィンドウを開きます。現在の Internet Explorer のウィンドウをリフレッシュしただけでは問題は解決しません。

代替解決策 : Internet Explorer 7 にアップグレードします。

リモート制御を使用するとブラウザでエラーが発生する

HPCA Enterprise Console から VNC またはリモート アシスタンスのリモート制御機能を開始すると、次のメッセージが表示される場合があります。

```
Several Java Virtual Machines running in the same process caused an error
```

この問題は、Java ブラウザ プラグインの既知の欠陥が原因である可能性があります。詳細については、**http://bugs.sun.com/view_bug.do?bug_id=6516270** を参照してください。

解決策 :

このメッセージが表示された場合、ブラウザで使用している Java Runtime Environment (JRE) を、JRE version 6 update 10 (またはそれ以降) にアップグレードします。

ジョブの問題

次のトラブルシューティングのヒントは、ジョブ管理の問題に関するものです。

DTM ジョブが正しく動作しない / RMP ジョブが見つからない 428 ページ

DTM ジョブが正しく動作しない / RMP ジョブが見つからない

従来の CAE インストールでは、ターゲットがグループである場合の DTM ジョブの実行時に、Enterprise Manager が正しくすべてのターゲット デバイスを解決するには、インストール後の手動作業が必要です。

この作業は、すべての RMP エージェント配布ジョブおよび OS 配布ジョブが **[現在のジョブ]** および **[過去のジョブ]** のリストに含まれるようにするためにも必要です。

このタイプのジョブの詳細については、158 ページの ジョブを管理するを参照してください。

解決策 :

1 Enterprise Manager がインストールされているシステムで、次のファイルを開きます。

<*InstallDir*>\CM-EM\tomcat\webapps\ope\config\dtm.properties

2 次のパラメータを設定します。

rmpServer=<*rmpServerHostName or IPAddress*>

rmpPort=3471

rmpUser=admin

rmpPassword={AES256}3gMlspmbrGbqVXNPDx8tWg==

rmpProtocol=http\:// *or* https\://

ここで、<rmpServerHostName または IPAddress> は、HPCA Management Portal がインストールされているシステムの名前またはアドレスです。

Enterprise Manager のインストール後に admin アカウントのパスワードを変更している場合、必ず rmpPassword パラメータに新しいパスワードを反映させてください。

ダッシュボードの問題

次のトラブルシューティングのヒントは、HPCA ダッシュボードで発生する問題に関するものです。

ダッシュボード レイアウト設定の削除

ダッシュボードのレイアウト セッションは、使用しているコンピュータのローカル共有オブジェクト (ブラウザの cookie など) として格納されます。現在の設定を削除するには、Adobe Website Storage Settings Panel を使用して、Flash アプリケーションのローカル ストレージ設定を管理する必要があります。詳細については、次の Web サイトを参照してください。

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html

[最も危険性の高い製品] ダッシュボード ペインの読み込みに時間がかかる

このペインは、企業内に多数の管理対象デバイスがある場合に非常に長い時間を要することがあるデータベース クエリに依存しています。クエリがタイムアウトして、ペインでまったく読み込みができなくなる場合があります。このペインはデフォルトで無効になっています。

解決策 :

[最も危険性の高い製品] ダッシュボード ペインを無効にします。318 ページのダッシュボードを参照してください。

ダッシュボード ペインのロード状態が終了しない

HPCA Enterprise Console が 次の両方の製品がインストールされているシステムでその Reporting Server がホストされている場合、一部のダッシュボード ペインでは、結果が何も返されないままロード状態がずっと続く場合があります。

- Microsoft SQL Server (Service Pack 2 が適用済み)
- Oracle ODBC クライアント ソフトウェア

次のバージョンの Microsoft SQL Server と Oracle クライアントは、同一のシステムにインストールされた場合、Reporting と競合することが知られています。

Oracle ODBC Driver Version 10.2.0.1.0

Microsoft SQL Server 2005 Service Pack 2 (2005.90.3042)

原因がこの問題であることを検証するには

1 [コントロール パネル] の [管理ツール] で [イベント ビューア] を開きます。

2 左ナビゲーション ペインで **[システム]** を選択します。

3 [ソース] カラムが `Application Popup` になっているイベントを探します。

4 イベントに次の説明がある場合、次のエラーが発生していると考えられます。

```
Application popup: nvdkit.exe - Application Error: …
```

解決策 :

これらの両方のプログラムを、HPCA Enterprise Console をホストしているシステム上にインストールしないでください。

RSS クエリに失敗する

HPCA ダッシュボード ペインが、コンテンツを提供する RSS フィードに接続できない場合、ペインに次のエラー メッセージが表示されます。

`RSS フィード {URL for RSS feed} への接続に失敗しました。HPC Enterprise Manager のプロキシ サーバーが正しく設定され、RSS フィードの購読が正しく設定され、RSS フィードにアクセスが可能か確認してください。`

発生した接続の失敗のタイプを判別するには、ダッシュボード ペインの左下隅にある **RSS クエリに失敗しました**というメッセージの上にマウスを置きます。ツール チップに次のいずれかのメッセージが表示されます。

表 49　考えられる RSS フィードの失敗のタイプ

障害の原因	表示されるテキスト
プロキシが設定されていない	リフレッシュ処理中のエラー : 接続タイムアウト : 接続
Live Network のパスワードが無効	リフレッシュ処理中のエラー : 無効な応答 : ログイン失敗
フィードに登録していない	リフレッシュ処理中のエラー : ライン -1 のエラー : ファイルの終わりが早すぎます

解決策 :

次を確認してください。

1. RSS フィードの URL が正しいことを確認する
2. RSS フィード サイトにアクセスできる。RSS フィード サイトの URL をブラウザに張り付けて確認します。
3. HPCA Enterprise Console のプロキシ設定が正しく指定されている。
4. HP Live Network 告示のフィードについて、次を確認してください。
   a. HP Live Network のサブスクリプション契約は現行のものである。
   b. Live Network の認証情報は正しく指定されている。
5. 必要に応じて RSS フィードに登録している。フィードに登録するには、エラー メッセージに表示されている URL をクリックします。

セキュリティとコンプライアンスの問題

次のトラブルシューティングのヒントは、セキュリティとコンプライアンスの設定、スキャン、およびレポートに関するものです。

- HP Live Network コネクタが接続できない 433 ページ

HP Live Network コネクタが接続できない

HPCA Enterprise Console がインストールされているシステムで、インターネットに接続するためにプロキシが必要な場合、Live Network の [プロキシ設定] [HTTP プロキシの設定] タブでプロキシ サーバーを指定する必要があります。

HPCA Enterprise Console では、[**HTTP プロキシ**の設定] タブの フィールド上でいかなるタイプの検証も行われません。形式の検証は行われません。また、指定したプロキシ サーバーが有効なプロキシ ホストであるかどうかの判断は行われません。この変更を保存する前に、必ずこの設定を二重にチェックしてください。

管理対象デバイスおよびスキャン実施済みデバイスの数がゼロである

適用状況管理、脆弱性管理、またはセキュリティ ツール管理のダッシュボードのホーム ページで表示される管理対象デバイスおよびスキャン実施済みデバイスの数がゼロの場合、レポート サブシステムに問題があることを示しています。

詳細については、HPCA 管理者にお問い合わせください。

レポートの表示が遅い

脆弱性、適用状況、またはセキュリティ ツールの管理レポートの HPCA Enterprise Console 内での表示が遅い場合、レポートのキャッシングを有効にする必要があります。

解決策 :

1 Web ブラウザを開いて、次のように入力します。

`http://InstallHost:3466/reportingserver/setup.tcl`

ここで、InstallHost は HPCA がインストールされているシステムのホスト名または IP アドレスです。

設定ファイルのページが表示されます。

2 左ナビゲーション メニューで、**[脆弱性管理設定]** をクリックします。

3 次の 2 つのオプションを設定します。

a **[VM レポートのキャッシングを有効化]** オプションで、ドロップダウン リストから「1」を選択します。

b **[VM キャッシュの存続期間]** を秒単位で指定します。たとえば、1200 秒は 20 分です。

4 **[適用]** をクリックします。

5 左ナビゲーション メニューで、**[適用状況管理設定]** をクリックします。

6 次の 2 つのオプションを設定します。

a **[適用状況管理レポートのキャッシングを有効化]** オプションで、ドロップダウン リストから「1」を選択します。

b **[キャッシュの存続期間]** を秒単位で指定します。

7 **[適用]** をクリックします。

8 左ナビゲーション メニューで、**[セキュリティ ツール管理設定]** をクリックします。

9 次の 2 つのオプションを設定します。

a **[Security Tools Management レポートのキャッシングを有効化]** オプションで、ドロップダウン リストから「1」を選択します。

b **[キャッシュの存続期間]** を秒単位で指定します。

10 **[適用]** をクリックします。

その他の問題

次のトラブルシューティングのヒントは、前述の各トピックで解決できない問題に関するものです。

- レポートを開けない 435 ページ
- 追加のパラメータが HPCA ジョブのウィザードで無視される 436 ページ
- 仮想マシンが起動しない 436 ページ
- クエリが限界に達しました 437 ページ

レポートを開けない

このトピックでは、次の問題に対処します。

1 ダッシュボード ペインの アイコンをクリックして関連レポートを開く。

2 リクエストしたレポートが開かない。

3 代わりに [Reporting] ホーム ページが表示されます。

これは、特定の URL がブラウザでブロックされたために発生します。使用しているブラウザのセキュリティ レベルを高く設定している場合、レポートの URL がブロックされることがあります。特定のレポートの ULR がブロックされると、Reporting のデフォルトの動作として、ホーム ページが表示されます。

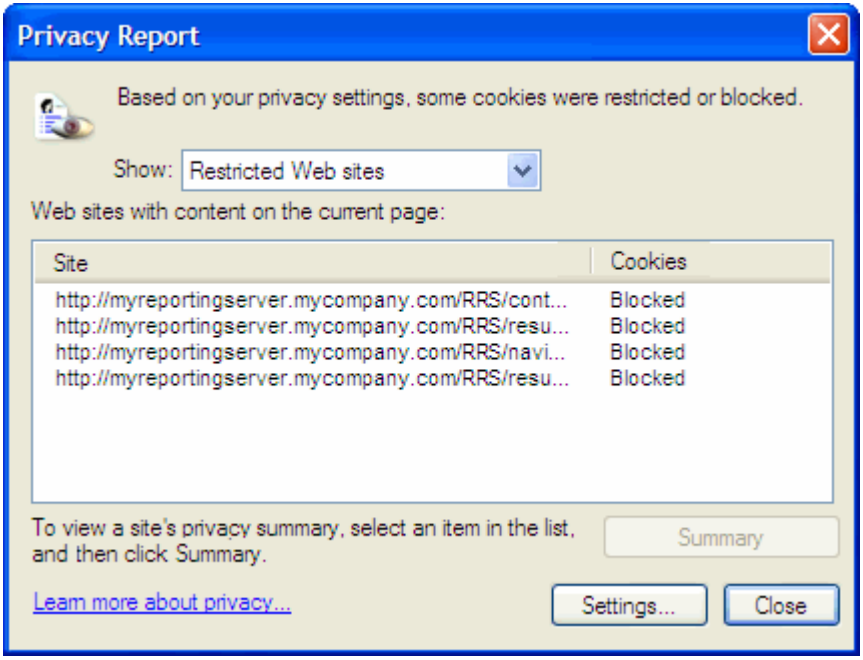
この動作は、Windows 2003 Server プラットフォーム上の Internet Explorer 6 および 7 で最も多く見られます。また、すべてのサポート対象プラットフォームでも発生する可能性があります。

解決策 :

1 ブロックされた URL のリストを開きます。

たとえば、Internet Explorer 7 では、ブラウザの下側のバーに表示された赤い丸印が付いた目の形のアイコンをクリックします。

次のようなダイアログが表示されます。



2 ブラウザのプライバシー設定を使用して、表示するレポートの URL を、cookie の使用が**許可される**サイトの一覧に追加します。

追加のパラメータが HPCA ジョブのウィザードで無視される

HPCA ジョブ作成ウィザードの使用時に「追加のパラメータ」を指定する場合、次の形式に従う必要があります。

```
option=value
```

この形式を使用しない場合は、追加のパラメータは無視されます。確認ページ (ウィザードの最後のページ) で、追加のパラメータがコマンド ラインに含まれていることを必ず確認してください。

仮想マシンが起動しない

ESX バージョン 3.5 Update 2 (ビルド番号 103908) のライセンスの欠陥により、特定の日付以降に仮想マシンが起動できなくなります。

このビルドの ESX を実行している場合に HPCA Enterprise Console から仮想マシンを起動しようとすると、次のようなエラー メッセージがコンソールに表示されます。

結果： 「マシン '< マシン名 >' の起動に失敗しました」

詳細： 「次のタスクの実行時にメソッドのエラーを受信しました haTask-##-vim.VirtualMachine.powerOn-#####: 一般的なシステム エラーが発生しました： 内部エラー。」

解決策 :

ESX バージョン 3.5 Update 2 build 110268 (またはそれ以降) をインストールしてください。

詳細については、この更新に関する VMware の次のリリース ノートを参照してください。

http://www.vmware.com/support/vi3//doc/vi3_esx35u2_vc25u2_rel_notes.html

クエリが限界に達しました

デフォルトでは、Active Directory オブジェクトの最初の 1000 件のメンバーのみが HPCA Enterprise Console に表示されます。1000 件を超えるメンバーを持つ Active Directory オブジェクトを参照しようとすると、「クエリが限界に達しました」というエラー メッセージが表示されます。

推奨される解決策 :

検索機能を使用して、表示されるメンバーを微調整してください。

代替解決策 :

HPCA 管理者は、HPCA Enterprise Console の `Console.properties` ファイルで `directory_object_query_limit` を指定できます。このファイルは次のディレクトリに格納されています。

`<tomcatDir>\webapps\em\web-inf\Console.properties`

`<tomcatDir>` のデフォルト値は次のとおりです。

`C:\Program Files\Hewlett-Packard\HPCA\tomcat`

Console.properties ファイルを変更した後は、必ず HPCATomcat サービスを再起動してください。

directory_object_query_limit プロパティを変更すると、HPCA Enterprise Console のパフォーマンスに悪影響を与える場合があります。

A HPCA Core Server と HPCA Satellite Server での SSL 設定

HPCA Console で設定可能な SSL 設定値の使用方法を十分に理解するには、SSL のさまざまな「構成要素」およびその機能について理解することが重要です。この付録では、HPCA 環境との関連を含めた SSL の概要を示します。詳細は、次のセクションを参照してください。

- SSL の構成要素 439 ページ
- HPCA 環境での SSL 440 ページ
- Console の SSL 証明書フィールド 441 ページ

詳細については、『HP Client Automation SSL 実装ガイド』を参照してください。

SSL の構成要素

次の構成要素の概要については、『HP Client Automation SSL 実装ガイド』の第 1 章を参照してください。

- 証明書
- 認証局
- 証明書の生成
- プライベート キー ファイル
- パブリック キー ファイル

HPCA 環境での SSL

SSL では、ID を確証し、セキュアな通信を実現するための共有**暗号鍵**を確立するために、**デジタル証明書**を使用します。SSL の使用方法は、インフラストラクチャ コンポーネント間の通信方法に応じて異なります。このセクションでは、SSL を有効にすべき 2 つの主な例と、それぞれの例における SSL の役割について説明します。

SSL 認証局、SSL 証明書、および SSL 証明書の生成の詳細については、『HP Client Automation SSL 実装ガイド』の第 1 章を参照してください。

リモート サービスへの SSL 通信のサポート

Core Server と Satellite Server の間の通信をセキュアにする必要がないと想定される場合、それらのサーバー間の SSL 接続は不要です。ただし、Core Server または Satellite Server が、外部サーバー (ベンダーの Web サイトをホストするサーバーなど)、他の HPCA Server、および Active Directory と通信する場合には、セキュアな通信 (LDAPS) が必要です。

これら他のサーバーが主張するとおりの「サーバー」であることを信頼できるようにするため、Core または Satellite は、各サーバーの**パブリックな証明書**または発行**認証局** (CA) の署名を取得する必要があります。Core または Satellite では、認証局から取得した **CA 証明書ファイル**`も必要であり、他のサーバーでそれを入手できるようにして、Core または Satellite からのメッセージを復号化できるようにする必要があります。(Core および Satellite のインストールには、ほとんどの環境に適しているデフォルトの信頼された認証機関 `ca-bundle.crt` のセットが含まれています)。

コンシューマへのセキュアな通信サービスの提供

Core Server と Satellite Server の間の通信をセキュアにする必要がある環境を想定します。この場合、Core はサーバーの役割を持ち、Satellite と共有可能なパブリック証明書が必要になります。Core Server のパブリック証明書には、そのパブリック キー、サーバー名、および (サーバーの ID を証明する) 認証局からの署名が含まれています。

- パブリック証明書 (**サーバー証明書**) は、自分を信頼してもらいたいユーザーすべてに与えることができます。

さらに、各 Satellite Server は「クライアント」の役割を持ち、Satellite と Core の間でメッセージの暗号化と復号化を実行できるように独自の証明書セットが必要になります。証明書は、その Satellite を証明するもので、Core がその Satellite を識別できるようにします。

個々の Core と Satellite は、メッセージを復号化するために独自のプライベートキーも必要になります。

- **プライベート証明書 (プライベート キー)** は、非公開の状態を維持し、一切共有しないでください。

Console の SSL 証明書フィールド

HPCA Console の [設定] タブの [インフラストラクチャ管理] 領域には、SSL サーバー および SSL クライアント という 2 つの SSL 証明書領域があります。このセクションでは、2 つの領域の違いとそれぞれの領域の必要性について説明します。HPCA の SSL セットアップを完了するには、この付録の情報を確認してから、263 ページの インフラストラクチャ管理を参照してください。

SSL 証明書、SSL 認証局、および SSL 証明書の生成の詳細については、『HP Client Automation SSL 実装ガイド』の第 1 章を参照してください。

SSL サーバー

パネルのこの領域を使用して、SSL を有効にし、HPCA Server のプライベートキー ファイル (`server.key`) とサーバー証明書ファイル (`server.crt`) をアップロードして保存します。これらのファイルは、(組織内で) 自己生成されたか、認証局から取得されたものです。これらのファイルの入手方法については、システム管理者にお尋ねください。

- プライベート キー ファイルは、対応するパブリック キーによってセキュアにされたメッセージを復号化するために必要です。
- サーバー証明書ファイルは、SSL が有効になっているサーバーがこのホストを識別できるようにするために必要です。

ファイルがアップロードされると (場所を指定して **[保存]** をクリックすると)、これらのファイルは次の場所に保存されます。

```
C:\Program Files\Hewlett-Packard\HPCA\ApacheServer\conf\ssl
```

デフォルトでは、これらのファイルは上記の名前で保存されますが、ファイル名はカスタマイズできます。

SSL クライアント

パネルのこの領域を使用して、HPCA Server の CA 証明書ファイル (ca-bundle.crt) をアップロードして保存します。このファイルには、ほとんどの環境で十分な権限を持つ信頼された認証機関のデフォルトのセットが含まれており、HPCA Server が LDAPS または HTTPS のいずれかを介して別のサーバーと通信する場合にのみ必要になります。

認証局から組織に取得された既存の CA 証明書ファイルを使用することが可能です。このファイルを入手する必要がある場合は、システム管理者にお尋ねください。

- CA 証明書ファイルには、信頼された認証局の署名入り証明書が含まれており、着信クライアントが「信頼できる」ものであることを確認するために必要です。

ファイルがアップロードされると (場所を指定して **[保存]** をクリックすると)、そのファイルは次の場所に保存されます。

`C:\Program Files\Hewlett-Packard\HPCA\ApacheServer\conf\ssl.crt` に配置されます。

デフォルトでは、このファイルは上記の名前で保存されますが、ファイル名はカスタマイズできます。

B　2 バイト文字のサポートについて

このセクションでは、サービス オペレーティング システム (SOS) のロケールを設定する、設定の変更を説明します。詳細は、次のセクションを参照してください。

Image Preparation Wizard を使用してイメージを作成するときには、参照マシンとターゲット マシンの**ロケール**が一致する必要があります。たとえば、簡体中国語の OS イメージを作成する場合は、簡体中国語の参照マシンで Image Preparation Wizard を実行する必要があります。

- サポートされる言語 443 ページ
- ロケールの変更 444 ページ

2 バイト文字が必要でない場合は、以下の変更を行わないでください。

サポートされる言語

443 ページの表 50 に、サポートされる言語と有効な言語コードの一覧を示します。

表 50　サポートされる言語とコード

言語	言語コード
韓国語	ko_KR
英語	ja
日本語	ja_JP
中国語 (簡体字)	zh_CN

ロケールの変更

PXE 環境でサポートされている言語にサポートを追加するには

1 テキスト エディタを使用して \X86PC\UNDI\linux-boot\linux.cfg\default を開きます。ファイルは次のように表示されます。

```
DEFAULT bzImage

APPEND initrd=rootfs.gz root=/dev/ram0 rw ISVR=10.10.10.1
ISVRPORT=3466
```

2 **LANG** パラメータを APPEND 行の最後に追加し、有効な言語コードを指定します (443 ページの表 50 を参照)。

結果として、言語が日本語に設定された、次の例のようなファイルが作成されます。

```
DEFAULT bzImage

APPEND initrd=rootfs.gz root=/dev/ram0 rw ISVR=10.10.10.1
ISVRPORT=3466 LANG=ja_JA
```

3 default ファイルを保存して閉じます。

サービス CD-ROM から復元するときにサポートされている言語にサポートを追加するには

- romsinfo.ini ファイルの ServiceCD セクションにある **LANG=xx_XX** を指定します。

  サポートされる言語と有効な言語コードの一覧については、443 ページの表 50 を参照してください。

- romsinfo.ini ファイルは、サービス CD iso の一部です。

Sysprep ファイルの 2 バイト文字サポート

Sysprep で 2 バイト文字サポートを使用する場合は、ファイルを UTF-8 でエンコードする必要があります。

C IPv6 ネットワーキングのサポート

Client Automation Core および Satellite サーバーでは、デュアル スタック (IPv4 と IPv6) 環境のネットワークでインターネット プロトコル バージョン 6 (IPv6) を使用するユーザーをサポートするための機能が追加されました。

この付録には次のトピックが含まれます。

IP ネットワーキングの用語と基本

このトピックでは、IP バージョン 4 と IP バージョン 6 に関連する用語と基本的な情報について説明します。

IP アドレスは、固有のデバイスまたはデバイスのポートを識別するための一意の数値です。IPv4 アドレスの 32 ビットのアドレス空間では、使用可能な固有アドレスの数の制限が厳しく、供給できるアドレスが残り少なくなっています。IPv6 の 128 ビットのアドレス空間は、この問題に対処するために作成されました。

用語

- **IPv4 アドレス :** IPv4 アドレスには、ピリオド (ドット) で区切られた 4 つのセクションが含まれます。オクテットと呼ばれる各セクションには、10 進数 (0-255) で表現された 8 ビットが含まれます。IPv4 アドレスを入力する場合、先行するゼロを省略できます。
- **IPv6 アドレス :** IPv6 アドレスには、コロンで区切られた 8 つのセクションが含まれます。各セクションには、大文字と小文字を区別しない 16 進数 (0000-FFFF) で表現された 16 ビットが含まれます。

  例 : **`2001:0db8:0000:0001:f8f3:a7bb:2bcb:6037`**

  IPv6 アドレスを覚えやすく、入力しやすくするために、二重コロン (::) によって複数の連続したゼロからなるセクションを示すことができます。先行するゼロを省略することもできます。たとえば、アドレス **`2001:0db8:0000:0001:f8f3:a7bb:2bcb:6037`** を **`2001:db8:0:1:f8f3:a7bb:2bcb:6037`** または **`2001:db8::1:f8f3:a7bb:2bcb:6037`** に簡略化できます。
- **IPv6 アドレス タイプ**
  - **グローバル ユニキャスト アドレス** : これは、外部通信に使用できる IPv6 アドレスです。次は、グローバル ユニキャスト アドレスの一例です。**`2001:db8:0:1:f8f3:a7bb:2bcb:6037`**
  - **リンクローカル アドレス** : このアドレスは、同じサブネット (リンク) 上の近隣ホストとの通信のみに使用できます。リンクローカル アドレスは、ルータによって転送されません。リンクローカル アドレスの構文では、最後に「%n」が追加されます。たとえば、**`fe80::20c:29ff:fed4:5ab%4`** のようになります。
  - **IPv4 マップ済みアドレス** : このアドレスは、IPv6 ネットワークで IPv4 アドレスをトンネリングするために使用できます。たとえば、**`fe80::5efe:192.168.6.154`** は、IPv4 アドレス **`192.168.6.154`** をトンネリングします。

IP アドレス ショートカット : IPv4 と IPv6

以下の表には、IPv4 と IPv6 の IP アドレス ショートカット規則がまとめられています。

表 51　IPv4 と IPv6 の予約済み IP アドレス値

予約済みの意味	IPv4 値	IPv6 値
localhost	`127.0.0.1`	`::1`
任意のアドレス 任意のインターフェイス	`0.0.0.0`	`::`

IPv4/IPv6 のトンネリング	適用できません	`fe80::5efe:<IPv4addr>`
		この場合、`<IPv4addr>` は、IPv4 アドレスです。例 :
		`fe80::5efe:192.168.1.2`

IPv6 アドレスへの角かっこの使用

URL、URI などの構文内の IPv6 のリテラル アドレスは、角かっこ ([と]) で囲み、その後に「:port」を続けられるようにする必要があります。例としては、HTTP、HTTPS、LDAP、および LDAPS エントリのスキームなどがあります。IPv6 アドレスを囲む角かっこは、IPv6 アドレス (コロンが含まれる) の開始と終了を、ポートの識別に使用するコロンと区別するために必要です。

例 :

`http://`[*literal_IPv6_address*]**`:port`**

[Core コンソール] または [Satellite コンソール] ページ、またはフィールドでポート エントリを許可していない設定ファイルを使用して IPv6 アドレスを入力する場合は、角かっこを省略します。

例 :

- ユーザーインターフェイス:**アップストリーム ホスト:*`literal_IPv6_address`***
- 設定ファイル :　　**`HOST=`*`literal_IPv6_address`***

  `-host` ***`literal_IPv6_address`***

HPCA の IPv6 サポートの概要

Client Automation では、Windows インフラストラクチャの Core および Satellite サーバーに IPv6 のサポートが追加されました。具体的には、次の点が変更されました。

- Core および Satellite サーバーは、IPv4 または IPv6 のいずれかを使用して HPCA サーバー間 通信を実行できるようになりました。
- Core および Satellite サーバーと、HPCA Configuration Server サービスは、インストール中に検出された使用可能な IPv4 および IPv6 スタック上でリスンするように自動的に設定されます。IPv4 のみが検出された場合、IPv4 用に設定されます。IPv6 も検出された場合、両方のスタックでリスンするように設定されます。

IPv6 サポートの制限

次の Client Automation コンポーネントは、IPv4 のみをサポートし、IPv6 には対応していません。

- Client Automation agent。
- Client Automation 管理ツール。
- Core または Satellite サーバーとは別にインストールされた、従来の、コンポーネントベースの Client Automation インフラストラクチャ サーバー。
- アウトバンド管理 (OOBM) 面 : このリリースでは、IPv6 は次を含むすべての OOBM 面で意図的に除外されています。
  - Core エンジンから OOBM Web サービス
  - OOBM から SCS (SCS は Intel AMT のセットアップおよび設定サービス)
  - OOBM からエージェント

Core および Satellite 環境での IPv6 のサポート

現在のリリースでは、Client Automation の IPv6 サポートの重点は、Windows ベースの Core および Satellite インフラストラクチャ サーバー間でトラフィックの IPv6 ルーティングを可能にすることに置かれています。

このリリースの IP ネットワーキング機能では、Client Automation サーバーが必要に応じて IPv6 または IPv4 を使用し、次のトラフィックをルーティングできます。

- Configuration Server メタデータを同期するための Core および Satellite トラフィック
- キャッシュ データを同期するための Core および Satellite トラフィック
- Core または Satellite 認証およびポリシー トラフィック (HTTP と LDAP)
- Satellite および Core 間のメッセージング トラフィック
- Satellite および Core 間の HTTP トラフィック

IP 通信サポート テーブル

次の表は、Core、Satellite、エージェント、および外部ディレクトリ間の HPCA 通信経路を示しています。IPv4 のみをサポートする通信経路と、IPv4 または IPv6 (IPv4/IPv6) をサポートする通信経路が識別されています。IPv4/IPv6 サポートは、黄色で強調表示されています。

表 52　IP 通信サポート テーブル

			ターゲット(サーバー)		
		Agent	Satellite	Core	AD / LDAP
ソース ：	Agent	N/A	IPv4	IPv4	N/A
(クライアント) ：	Satellite	IPv4	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6
	Core	IPv4	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6

Core および Satellite サーバーでは、2 か所 (HTTP リスニング ポイントと Configuration Server リスニング ポイント) でリスンされます。これらの通信ポイントのどちらかは、必要に応じて IPv4 または混在にすることができます。

HPCA Agent では、IPv4 を使用した Core および Satellite サーバーとの通信のみが行われます。

IPv6 サーバー通信を有効にするには

このリリースの Core および Satellite サーバーでは、エージェント通信に引き続き IPv4 が必要です。そのため、サーバー間通信で IPv6 を利用するには、Core および Satellite サーバーをデュアル スタック (IPv4/IPv6) 環境にインストールする必要があります。

Core および Satellite のセットアップ プログラムが、ホスト サーバーで IPv6 スタックを検出すると、Core および Satellite サーバーは、IPv4 および IPv6 プロトコル上でリスンするように自動的に設定されます。

Core または Server インストールを実行する前に、450 ページの前提条件を確認してください。

IPv6 サポートの前提条件

- HPCA Core および Satellite サーバーは、IPv6 に対応し、IPv6 対応ネットワークで実行されている Windows XP、Windows 2003 Server、または Windows 2008 Server オペレーティング システムにインストールされている必要があります。サポート対象のプラットフォームの詳細については、付属の『HPCA 7.50 リリース ノート』のハードウェア サポート表を参照してください。
- このリリースでは、HPCA Agent に対する IPv6 サポートは提供されないため、HPCA Server は、デュアル スタックの IPv4/IPv6 環境で実行する必要があります。
- DNS と DHCP は、IPv6 をサポートするように設定する必要があります。
- HPCA Server と、ポリシーおよび認証通信に使用されているユーザー提供の外部 **Active Directory Service** (**ADS**) の間の IPv6 通信をサポートするには、次の条件を満たす必要があります。
  - ADS が Windows Server 2008 にインストールされている
  - ADS に IPv6 のサポートが設定されている
- Internet Explorer を Web ブラウザとして使用する場合、IPv6 をサポートするには、バージョン 7 以上が必要です。

HPCA Windows サーバーへの IPv6 サポートの設定

このセクションでは、HPCA Core および Satellite Windows Server コンポーネントが IPv6 対応環境にインストールされるときに、自動的に行われる IPv6 関連の設定変更について説明します。

このセクションでは、次のトピックを説明します。

- コンポーネント : HPCA Apache ベースの Core および Satellite サーバー 451 ページ
- コンポーネント : HPCA Configuration Server 451 ページ

コンポーネントごとに、次の詳細を説明します。

- IPv6 をコンポーネントに対して有効にする方法
- ログを使用して IPv6 が使用されているかどうかを識別する方法
- 制限事項と依存関係 (ある場合)

コンポーネント : HPCA Apache ベースの Core および Satellite サーバー

HPCA Core および Satellite サーバーは、Apache サービス (デフォルトで IPv6 対応) の下で実行されます。Apache サービスでは、IPv6 用の設定変更は要求されません。ただし、お使いの環境が前述の前提条件を満たすことを確認してください。

Apache が IPv6 アドレスをリスンしていることを確認するには

1. コマンド プロンプトを開きます。
2. 「**netstat -an**」と入力します。
3. 結果が表示されたら、[::]:3466 用のエントリが存在するかどうか確認します。存在する場合、これにより Apache が IPv6 アドレスをリスンしていることが確認されます。

コンポーネント : HPCA Configuration Server

Configuration Server では、IPv4 でエージェント通信がリスンされる必要があります。Core インストール プログラムで使用可能な IPv6 スタックが検出されると、Configuration Server は、IPv4 と IPv6 の両方のスタックでリスンできるように自動的に設定されます。

Configuration Server コンポーネントで IPv6 を有効にする方法

Core または Satellite サーバーのインストール時に Core または Satellite で IPv6 が有効になると、Configuration Server は自動的に IPv4 と IPv6 の両方のスタックでリスンできるように設定されます。これには、次の設定が含まれます。

- IPv4 に加えて IPv6 の接続も受け入れるためのセッション接続を有効にする。
- IPv6 に加えて IPv4 の **SSL** (**Secure Sockets Layer**) とのセッション接続を有効にする。

Configuration Server が SSL モード以外で IPv6 アドレスをリスンしていることを確認するには

これらの変更は、IPv6 がサーバー上で有効な場合に Core または Satellite セットアップ プログラムによって行われます。IPv6 を有効にするために使用された Configuration Server の設定変更を表示して確認するには、次の手順を実行します。

1. Microsoft のメモ帳を使用して、HPCA Server がインストールされた場所の \bin ディレクトリにある edmprof を開きます。メモ帳では edmprof ファイルの必須エンコーディングである UTF-8 がサポートされています。
2. MGR_ATTACH_LIST セクションに移動し、ATTACH_LIST_SLOTS 属性を見つけます。IPv6 が検出されると、Core セットアップ プログラムでは IPv6 を有効にするために、明示的に次の CMD_LINE エントリが追加されます (edmprof のデフォルトである、IPv4 でリスンするための ztcpmgr も有効になっています)。

   ```
   CMD_LINE=(ztcpmgr, NAME=tcpmgr6,ADDR=::) RESTART=YES
   ```

   このコマンド ラインには、デフォルトのポート 3464 を使用する HPCA Configuration Server が反映されています。デフォルト以外のポートが使用されている場合、ADDR 属性の後に、453 ページの「Configuration Server が SSL モードで IPv6 アドレスをリスンしていることを確認するには」と同じ構文を使用して PORT も指定されます。
3. Core セットアップ プログラムはまた、新しい CMD_LINE エントリを追加するために ATTACH_LIST_SLOTS 値も 1 だけ増やします。

   edmprof ファイルが手動で変更された場合、必ず UTF-8 エンコーディングを使用して保存し、HPCA Configuration Server (ZTopTask.exe) のサービスを再起動してください。
4. これらの設定変更が、HPCA Configuration Server サービス (ZTopTask.exe) に反映されていることを確認するには、Configuration Server のログ ファイルを確認します。2 つの TCP マネージャが着信する要求の受け入れ待ちをしていることがわかります。例については、453 ページの「ログ メッセージ」を参照してください。

Configuration Server が SSL モードで IPv6 アドレスをリスンしていることを確認するには

これらの変更は、IPv6 がサーバー上で有効な場合に Core または Satellite セットアップ プログラムによって自動的に行われます。

1 Microsoft のメモ帳を使用して、HPCA Server がインストールされた場所の \bin フォルダにある edmprof を表示します。メモ帳では edmprof ファイルの必須エンコーディングである UTF-8 がサポートされています。

2 Core 設定プログラムでは、SSL Manager IPv4 および IPv6 を有効にするために、MGR_ATTACH_LIST セクションの下に次の行が追加されます。

```
[MGR_ATTACH_LIST]
CMD_LINE=(zsslmgr, NAME=sslmgr4,PORT=443) RESTART=YES
CMD_LINE=(zsslmgr, NAME=sslmgr6,ADDR=::,PORT=443) RESTART=YES
```

3 Core 設定プログラムはまた、新しい CMD_LINE エントリを追加するために ATTACH_LIST_SLOTS 値も 2 だけ増やします。

> edmprof ファイルが手動で変更された場合、必ず UTF-8 エンコーディングを使用して保存し、HPCA Configuration Server (ZTopTask.exe) のサービスを再起動してください。

4 SSL 設定変更が、HPCA Configuration Server サービス (ZTopTask.exe) に反映されていることを確認するには、ログ ファイルを確認します。2 つの SSL マネージャが着信する要求の受け入れ待ちをしていることがわかります。453 ページの「ログ メッセージ」の例を参照してください。

ログ メッセージ

SSL が無効な場合のセッション ログ メッセージ

```
02I 22:22:04 <ztcpmgr          /1DC>   System Task     --- TCP
Manager task has started

NVD0404I 22:22:04 <TCP/IP Manager   /1DC>   System Task     ---
TCP/IP Manager accepting requests at address <RPS> on port <3464>

NVD0402I 22:22:04 <ztcpmgr          /954>   System Task     ---
TCP Manager task has started

NVD0404I 22:22:04 <TCP/IP Manager   /954>   System Task     ---
TCP/IP Manager accepting requests at address <::> on port <3464>
```

SSL が有効な場合のセッション ログ メッセージ

```
NVD0414I 15:04:36 <zsslmgr          /7E8>   System Task     ---
SSL Manager Task has started

NVD0472I 15:04:36 <SSL Manager      /7E8>   System Task     ---
SSL Manager accepting requests at address <RPS> on port <0443>

NVD0414I 15:04:36 <zsslmgr          /188>   System Task     ---
SSL Manager Task has started

NVD0472I 15:04:36 <SSL Manager      /188>   System Task     ---
SSL Manager accepting requests at address <::> on port <0443>
```

Core および Satellite コンソールでの IPv6 リテラル アドレスの使用

IPv6 対応の環境では、以下に挙げる Core と Satellite に関連するフィールドに IPv6 アドレスまたは IPv4 アドレスを使用できます。つまり、これらのフィールドを使用して次の項目を指定できます。

- IPv6 アドレスまたは IPv4 アドレスに解決されるホスト名
- リテラルの IPv6 アドレスまたは IPv4 アドレス

  IPv6 アドレスの例 : `2001:db8:0:1:f8f3:a7bb:2bcb:6037`
  IPv4 アドレスの例 : `192.168.0.4`

サーバーの後にポートを指定可能な URL、URI などのフィールドに、リテラル IPv6 アドレスを入力する場合、IPv6 アドレスを必ず角かっこで囲んでください。例については、下記の「ブラウザ サポート」の項目を参照してください。

Core および Satellite の IPv6 アドレス サポート

ブラウザ サポート

- IPv6 サーバーにインストールされた Core または Satellite コンソールにアクセスする URL は次のようになります。
  例 : **`http://[`***`literal_IP_address`***`]:3466`**

Satellite サーバーのインストール

- **初回セットアップ ウィザードの手順 3: アップストリーム サーバー**

Satellite コンソール - [設定] タブ

- **[アップストリーム サーバー] ページ > [アップストリーム ホスト]**
- **[インフラストラクチャ管理] > [ポリシー] > [ディレクトリ ホスト]**

Core コンソール - [設定] タブ

- **[インフラストラクチャ管理] > [ディレクトリ サービス] > [Creation Wizard]**
- **[インフラストラクチャ管理] > [ポリシー] > [ディレクトリ ホスト]**
- **[パッチ管理] > [ベンダーの設定]**

Core コンソール - [操作] タブ

- **[操作] > [パッチ管理] > [同期を実行]**

IPv6 の使用方法とトラブルシューティング

次のセクションでは、IPv6 に関するよくある質問に対する回答を示し、HPCA で IPv6 を使用するときに発生する一般的な問題をトラブルシューティングできるようにします。

- 使用方法に関するよくある質問 456 ページ
- IPv6 環境のトラブルシューティング 458 ページ

使用方法に関するよくある質問

Q1. HPCA Server で IPv6 を有効にするにはどうすればよいですか？

A. この付録の前のトピックを参照してください。詳細については、451 ページの「HPCA Windows サーバーへの IPv6 サポートの設定」と、449 ページの「IPv6 サーバー通信を有効にするには」を参照してください。

Q2. IPv6 を有効にしましたが、Web ブラウザを使用して Core にアクセスすると、不正な要求や接続拒否に関するエラーが表示されます。どのように解決すればよいですか？

A. 次のどちらかの方法を使用して問題を切り分けてください。

- IPv4 のマシンと IPv6 のマシンに対して ping を実行します。
- telnet を使用して該当するアドレスとポート 3466 または 3464 に接続できるかどうか確認します。接続できた場合は、ローカルな問題 (IPv6 のリテラル サポートには IE7 が必要) か、またはサーバー側の何らかの問題です。サーバーが実行中で、リスンしていることをログで確認してください。

CA のログ ファイルは、サーバーの `C:\Program Files\Hewlett-Packard\HPCA` の下にある次のディレクトリにあります。

- `\ApacheServer\logs`
- `\ConfigurationServer\log`

Q3. Web ブラウザを使用して接続すると、速度が著しく遅くなります。特にこれといった理由もなく、数秒の待ちが発生します。一方、IPv4 を使用する隣席のユーザーでは、この問題は発生していません。解決方法はありますか？

A. ブラウザの接続速度が低下するのは、サーバーが呼び出し元のホスト名を判別しようとして一時的にハングするという、DNS の問題が原因である可能性があります。

Q4. IPv6 を有効にして、IPv6 対応の DNS を使用しています。「http://myCore:3466 」のようなホスト名を使用してコンソールに接続した場合、この接続が IPv4 と IPv6 のどちらを使用しているかをどのようにして確認できますか？

A. Apache と Configuration Server のログを確認してください。ログ エントリの例については、付録の「IPv6 ネットワーキングのサポート」のトピックを参照してください。

Q5. IPv6 を有効にして、IPv6 対応の DNS を使用しています。Satellite の同期を実行したとき、IPv4 と IPv6 のどちらを使用しているかをどのようにして確認できますか？

A. Apache と DCS のログを確認してください。

Q6. リテラル IPv6 アドレスを使用して HTTPS で Core/Satellite にアクセスすると、IE から証明書に関する警告が表示されます。何が起きているのでしょうか？

A. ホストの DNS でアドレスの逆検索ができない場合、中間者防御が行われているかどうかを検証できません。これは、証明書のキーが IP アドレスではなく FQDN に対して設定されているためです。同じことが、IPv6 アドレスだけでなく、どの IP アドレスにも当てはまります。

Q7. アップストリーム ホストにリンクローカル アドレスを指定したらエラーが表示されました。どのように解決すればよいですか？

A. HPCA Core Server は、Apache の下で実行されているため、リンクローカル アドレス エントリをサポートしていません。アップストリーム ホストには、グローバル ユニキャスト IPv6 アドレスを指定する必要があります。詳細については、このトラブルシューティングの項目である、460 ページの「使用している IP アドレスの問題でしょうか ？どうすれば IP アドレスを二重にチェックできますか ?」を参照してください。

IPv6 環境のトラブルシューティング

IPv6 環境で発生した単純な問題のトラブルシューティング時には、次に示す診断や検証に関するヒントを参考にしてください。ヒントの多くは、HPCA の IPv6 実装に関する作業に固有のものではなく、IPv6 全般に適用されます。

後述のトピックを参考にして、次のような診断上の問題を解決してください。

リモート ブラウザから Core または Satellite にアクセスできますが、ログインしようとすると「不明なログイン失敗です」というエラーで失敗するか、応答がありません。解決方法はありますか？

問題：リモート ブラウザから Core または Satellite にログインできない。「不明なログイン失敗です」というメッセージが表示されるか、応答がない。

解決方法：リモート ログインの失敗は、一般に次のいずれかの理由で発生します。

- ブラウザのセキュリティに原因がある場合。**解決方法：**信頼できるサイトのリストに「http://[<IPv6 address>]:3466/」を追加してください。
- IE7 ブラウザで Cookie が無効になっているか、リフレッシュされない場合。**解決方法：**IE7 ブラウザの Cookie を削除し、ページをリフレッシュしてから、再度ログインを試みてください。IE7 ブラウザの Cookie の削除機能へは、次のようにして移動します。

  [ツール] > [インターネット オプション] > [全般] タブ > [閲覧の履歴] >

[削除] > [Cookie の削除]

Cookie を削除したら、ページをリフレッシュしてから再度ログインしてください。

Web ブラウザの問題のような、ローカル ツールの問題が発生しているのでしょうか？

Core または Satellite コンソールへのアクセスを試みたときのブラウザの応答が「**`Internet Explorer`** はページを表示できません」である場合、使用している IE ブラウザのバージョンを確認してください。

IPv6 アドレスでページを開くには、IE7 以降を使用する必要があります。

ローカル OS の問題でしょうか? OS で IPv6 はサポートされているのでしょうか？

ローカル OS で IPv6 サポートが有効かどうかを確認するには、次の基本情報を参考にしてください。

- Windows 2000 の場合、IPv6 はサポートされていません。Windows 2003 以上が必要です。
- Windows 2003 の場合、IPv6 はサポートされていますが、デフォルトでは IPv6 スタックがロードされません。Windows 2003 で IPv6 スタックを (既存の IPv4 スタックと一緒に) 有効にするには、コマンド ライン ウィンドウ ボックスから **`netsh interface ipv6 install`** を実行します。このコマンドにより、IPv6 スタックがインストールされます。
- Windows 2008/Vista の場合、IPv6 はデフォルトでサポートされています。

ローカル OS の問題でしょうか？ホスト名の DNS 名前解決をテストするにはどうすればよいですか？

非常に長い IPv6 アドレスを使用する IPv6 環境では特に、ホスト名を使用して IPv6 アドレスに解決するのが最良の方法です。ホスト名が正しく解決されているかどうかは、次の方法で確認してください。

`ping` ツールか、**`Nslookup`** のどちらかを使用します。Nslookup を使用すると、IPv4 と IPv6 のどちらでも正しいホスト名と IP アドレスを解決できます。

ping ツールを使用する : DNS 名前解決をテストするには、ping ツールを使用し、ホスト名または完全修飾ドメイン名 (FQDN) で指定した送信先に対して ping を実行します。ping ツールが、FQDN および対応する IPv6 アドレスを表示します。

Nslookup を使用する : ping ツールが正しくない IPv6 アドレスを使用している場合、次の手順を実行します。

Nslookup ツールを使用すると、DNS Name Query Response メッセージで返された一連のアドレスを判別できます。

1 最初に、DNS リゾルバのキャッシュをフラッシュします。次のコマンドを使用してフラッシュできます。

ipconfig /flushdns

2 Nslookup > プロンプトで、**set d2** コマンドを使用して、DNS 応答メッセージに関する最大量の情報を表示します。

3 Nslookup を使用して目的の FQDN を検索します。次のいずれかを使用します。

— **nslookup <ip address>**

— **nslookup <hostname>**

DNS 応答メッセージの詳細表示で、AAAA レコードを探します。

使用している IP アドレスの問題でしょうか？どうすれば IP アドレスを二重にチェックできますか？

デバイスに対して正しい IPv6 アドレスを使用していることを確認するには、**ipconfig** コマンドを実行します。

Windows 2003 マシン (IPv6 が有効) の場合、**ipconfig** では、次の図のように IPv6 アドレスのセットが 3 つ返されます。

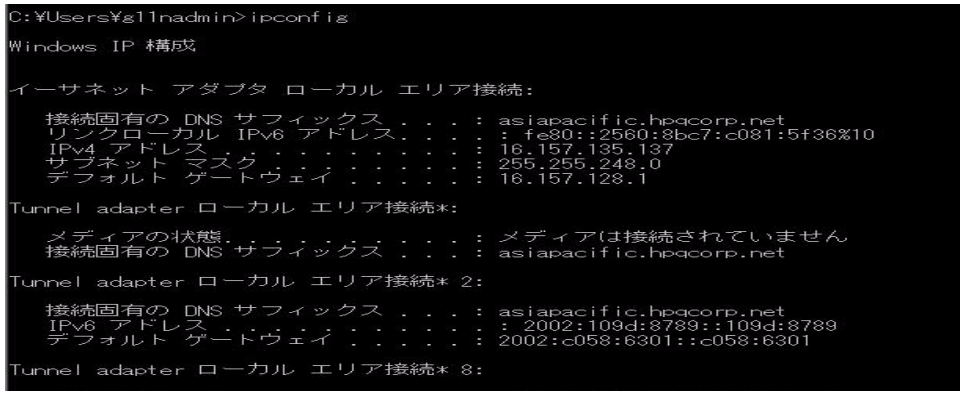
3 つの IP アドレスは、赤い丸で示すように (上から下) それぞれ異なります。

- アドレス「2001:db8:0:1:20c:29ff:fed4:5ab」はグローバル ユニキャスト IPv6 アドレスで、外部通信 に使用できます。
- アドレス「fe80::20c:29ff:fed4:5ab%4」は、リンクローカル アドレスです。このアドレスは、同じサブネット (リンク) 上の近隣ホストとの通信のみ に使用できます。リンクローカル アドレスは、ルータによって転送されません。
- アドレス「fe80::5efe:192.168.6.154%2」は、IPv4 マップ済み v6 アドレスで、トンネリング に使用できます。

デバイスは、複数のインターフェイスを持つことができます。コマンド「**`interface ipv6 show address`**」を実行すると、各インターフェイスに割り当てられた IPv6 アドレスを表示できます。

Windows 2008 マシンの場合、**`ipconfig`** コマンドでは、2 つの IPv6 アドレスのみが返されます。また、次の画像の「Ethernet adapter Local Area Connection 2:」の下に表示されているように、これらのアドレスは、明示的に **IPv6 Address** および **Link-local IPv6 Address** と表示されます。

このリストを参照して、外部接続には常に **IPv6 Address** を使用してください。



クライアントとサーバー間のネットワークに問題があるのでしょうか? どのようにして確認できますか ?

これには、多くの理由が考えられます。その一部を次に挙げます。

- ファイアウォールがクライアントまたはサーバー　マシンで有効になっている。この点を確認し、ファイアウォールを無効にしてください。

- デフォルトで HPCA Server が v4 と v6 の両方の接続をリスンしている。v4 にバインドしているクライアントは、サーバーが v4 接続をリスンしていないため失敗した可能性があります。サーバー側で、コマンド プロンプトを開き、「**netstat -an**」と入力します。これにより、サーバーがリスン中のアドレスとポートがすべて表示されます。
- サーバーがビジーで接続を受け入れられない。

索引

I

L

M

N

O

P

R

S

U

V

W

X

あ

い

え

お

し

す

せ

ひ

ふ

へ

ほ

ま

め

も

ゆ

よ

り

ろ