HP Client Automation

Enterprise Manager

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誤り、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

機密性のあるコンピュータ ソフトウェアです。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

Adobe® は Adobe Systems Incorporated の登録商標です。

Java™ は Sun Microsystems, Inc. の米国における商標です。

Linux は、Linus Torvalds の登録商標です。

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

OpenLDAP は、OpenLDAP Foundation の登録商標です。

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、次のサイトにアクセスしてください。

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

または、HP 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。詳細は、HP 営業担当者までご連絡ください。

次の表には、前回のリリース以降に変更された箇所が示されています。

ドキュメントの変更点

章	バージョン	変更点
すべて	7.20	HP Configuration Management (CM) は、新しく HP Client Automation (HPCA) へとブランド変更されました。
第 3 章	7.20	新しいダッシュボードと HP Live Network 設定の設定方法に関する情報が追加されました。 通知ジョブ テンプレートに関する情報が追加されました。
第 4 章	7.20	通知デバイス プロセスが更新され、新しい通知ジョブ テンプレートが含まれました。
第 5 章	7.20	脆弱性管理に関する新しい章が追加されました。
第 6 章	7.20	新しい HPCA オペレーション、パッチ管理、および脆弱性管理の各ダッシュボードに関する情報が追加されました。

ドキュメントの変更点

章	バージョン	変更点
第 7 章	7.20	新しい脆弱性管理レポートおよび管理レポートが追加されました。
第 8 章	7.20	Internet Explorer 6 で SSL を使用する際のヒント、および ESX バージョン 3.5 Update 2 で仮想マシンの起動が妨げられる問題に関するトラブルシューティングのヒントが追加されました。
第 2 章	7.20	Adobe Flash Player が、9.0.124 以上のバージョンをサポートするようになりました。
第 4 章	7.50	Distributed Task Management (DTM) ジョブ、OS 管理、Satellite の同期化、アウトバンド (OOB) 管理のサポートが追加されました。 通知ジョブ テンプレートの名前がジョブ アクション テンプレートに変更されました。DTM または通知ジョブのいずれかで使用できます。
第 5 章	7.50	既存の脆弱性管理製品に、コンプライアンス (SCAP) およびセキュリティ ツール管理機能が追加されました。
第 6 章	7.50	適用状況管理ダッシュボードおよびセキュリティ ツール管理ダッシュボードが追加され、基準 (グローバル、モバイルおよび仮想) およびカスタム フィルタのサポートも追加されました。
第 7 章	7.50	適用状況管理レポートおよびセキュリティ ツール レポートが追加されました。
第 9 章	7.50	カスタムのデバイスとフィルタの有効化に関する情報が追加されました。

サポート

HP Software のサポート Web サイトは次のとおりです。

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の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 サイトを使って以下のことができます。

- 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 サポートの問い合わせ先の検索
- 利用可能なサービスに関する情報の確認
- 他のソフトウェア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

サポート エリアのほとんどでは、HP Passport ユーザーとして登録し、サインインすることが必要です。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 Enterprise Manager (Enterprise Manager) は、Web ベースのエージェント管理ツールで、お使いの環境のソフトウェア、パッチ、およびインベントリを素早く簡単に管理できます。

このガイドでは Enterprise Manager を紹介し、コンポーネントのインストールと設定方法、および Enterprise Manager の使用における詳細情報や指示について説明します。次のトピックが含まれます。

Enterprise Manager は、従来のコンポーネント ベースの Client Automation Enterprise (CAE) インストールでのみご利用いただけます。Core または Satellite のインストールではご利用いただけません。Core および Satellite のインストールでは、Enterprise Manager と共通する機能を多く搭載している HPCA Enterprise Console が使用されます。

Core および Satellite Server をお使いの場合は、『HP Client Automation Core および Satellites 入門およびコンセプト ガイド』を参照してください。

対象者

このガイドは、従来のコンポーネント ベースの CAE インストールに Enterprise Manager をインストールして設定し、使用する管理者を対象にしています。

各章の概要

このガイドには、本章以外に次の章が含まれています。

- 第 2 章、Enterprise Manager のインストールには、システム要件やインストールの指示についての情報が含まれています。
- 第 3 章、Enterprise Manager へのアクセスと設定では、貴社での使用に合わせて Enterprise Manager を設定する方法を説明します。
- 第 4 章、Enterprise の管理では、Enterprise Manager を使用してデバイスにポリシーを適用し、オペレーション、脆弱性管理、およびパッチ管理の各ダッシュボードを監視する方法を説明します。
- 第 5 章、セキュリティと適用状況の管理では HPCA 脆弱性管理ソリューションの概要と、関連タスクに関する指示を示します。
- 第 6 章、ダッシュボードの使用では、Enterprise Manager で利用可能なさまざまなダッシュボードについて説明します。
- 第 7 章、レポートの使用では、HPCA オペレーション、脆弱性および適用状況管理、パッチ管理、監査に関するレポートの表示とフィルタ方法について説明します。
- 第 8 章、トラブルシューティングでは、一般的な問題を解決するためのヒントを説明します。
- 第 9 章、カスタム ダッシュボード フィルタとデバイスの追加では、ダッシュボードに独自のフィルタとデバイスを追加する方法を説明します。

変数と略語

表 1　このガイドで使われている略語

略語	定義
HPCA	HP Client Automation
CAE	個別のサーバー コンポーネント (Core や Satellite 以外) からインストールされた従来の HPCA Enterprise 環境
CSDB	Configuration Server Database
Portal	HPCA Portal (以前の Management Portal)

表 2　このガイドで使われている変数

変数	説明	デフォルト値
<InstallDir>	Enterprise Manager がインストールされる場所	従来の HPCA Enterprise インストールの場合 : C:\Program Files\HP\HP BTO Software Core および Satellites インストールの場合 : C:\Program Files\Hewlett-Packard
<DataDir>	Enterprise Manager のデータ ファイルが保存される場所	従来の HPCA Enterprise インストールの場合 : C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software Core および Satellites インストールの場合 : C:\Documents and Settings\All Users\Application Data\Hewlett-Packard\HPCA

関連ドキュメント

次のガイドは、Enterprise Manager に関連する製品を説明するものです。

HP Client Automation Configuration Server ユーザー ガイド

HP Client Automation Portal インストールおよび設定ガイド

HP Client Automation Reporting Server インストールおよび設定ガイド

次の手順

第 2 章、Enterprise Manager のインストールに進みます。

2 Enterprise Manager のインストール

この章は、次の各トピックで構成されています。

この章の内容は、従来の CAE のインストールにのみ当てはまります。

Core および Satellite サーバー環境では、Enterprise Manager ではなく、Enterprise Console を使用してください。詳細については、『HP Client Automation Core および Satellites 入門およびコンセプト ガイド』を参照してください。

システム要件

従来の HP Client Automation (HPCA) インストール プロセスを使用している場合、Enterprise Manager に加えて次のコンポーネントもインストールする必要があります。また、Enterprise Manager がどのコンポーネントを使用するのかも確認する必要があります。

- HP Client Automation Configuration Server (Configuration Server)
- HP Client Automation Configuration Server Administrator (Administrator)
- HP Client Automation Reporting Server (Reporting Server)
- HP Client Automation Portal (Portal)
- HP Client Automation Messaging Server (Messaging Server)

Reporting Server 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や、レポートを提供します。企業内で、Reporting Server がインストールされていない、または確認されない場合は、これらの機能を Enterprise Manager で使用できません。

Reporting Server のインストールおよび設定の詳細については、『HP Client Automation Reporting Server ガイド (Reporting Server ガイド)』を参照してください。

Core および Satellite のインストールを使用している場合、Enterprise Manager とこれが使用するコンポーネントは Core サーバーのインストールの一部として自動的にインストールされます。

Enterprise Manager のインストール先デバイスには、次のいずれかのブラウザが必要です。

- Microsoft Internet Explorer 6.x または 7.x、パッチ適用済み Internet Explorer 8.x は現在サポートされていません。
- Mozilla Firefox 2 (以降)

ブラウザには、Adobe Flash Player のバージョン 9.0.124 (以降) をインストールしておく必要があります。次を参照してください。

www.adobe.com/go/getflashplayer

Enterprise Manager でデータを正しく表示するためには、次のデスクトップ表示設定が最低要件となります。

- 画面解像度 : 1024x768

- 色品質 : 中 (16 ビット)

Enterprise Manager のインストールと実行は、Windows Terminal Server として機能するように設定されているサーバー上ではサポートされません。

プラットフォーム サポート

本リリースでサポートされているプラットフォームの詳細については、添付のリリース ノートを参照してください。

インストール タスク

Core および Satellite サーバー環境の場合、まず『Core および Satellite Server 入門ガイド』を参照してください。そのガイドにあるインストール、設定、トラブルシューティングに関する情報は、このガイドの情報より優先である場合があります。

Enterprise Manager の全機能を使用するためには、次のタスクを完了する必要があります。Configuration Server、Portal、および Reporting Server の IP アドレス、ホスト名、ポートを確認しておいてください。

Enterprise Manager は Tomcat アプリケーション サーバーのインスタンスで実行されます。Tomcat で使用されるデフォルトは、HTTP 通信ではポート 8080、HTTPS 通信ではポート 8443 です。

ファイアウォールの内側に Enterprise Manager をインストールしており、ファイアウォールの外側から Enterprise Manager にアクセスする場合、Tomcat へのネットワーク接続の受信を許可していることを確認してください。

これが正しく設定されていない場合、ファイアウォールの外側から Enterprise Manager へアクセスできません。SSL (セキュア) アクセスが必要である場合、セキュア Tomcat アクセス ポートでもネットワーク接続を受信できるようにファイアウォールを設定しておく必要があります。

前述の 8080 および 8443 以外のポートで Tomcat インストールを設定する場合は、それに応じて Enterprise Manager の設定を修正する必要があります。詳細な手順については、26 ページの「Enterprise Manager ポートが競合する」を参照してください。

Enterprise Manger をインストールし、Portal 設定を行うには :

1 インストール メディアで、次のディレクトリに進みます。

```
Enterprise Manager\win32
```

2 インストール実行ファイルをダブルクリックします。

3 言語を選択して **[OK]** をクリックします。

4 ウィザードの手順に従って、先に進みます。

5 インストールが完了すると、Portal の設定を行うための画面が表示されます。

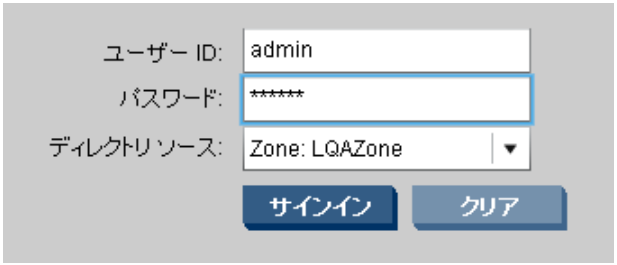
Web ブラウザでこの設定ウィンドウが表示されない場合、手動でアクセスする必要があります。Enterprise Manager が現在インストールされているシステムで Web ブラウザを開き、次の URL へ移動します。

CAE: **http://localhost:8080/em**

6 適切な設定を入力または選択し、**[保存]** をクリックします。設定が検証されます。検証が失敗すると、エラーが表示されます。

合格であった場合、**[閉じる]** をクリックして続行します。Enterprise Manager 開始ページに自動的にリダイレクトされます。

7 **ユーザー ID** admin と**パスワード** secret でサインインします。これらはデフォルトです。現時点で、ディレクトリ ソースは Portal をインストールしたときに作成したゾーンになっています。



プロダクション環境で Enterprise Manager を使用する前に、admin ユーザーのパスワードを変更する必要があります。詳細については、44 ページの「Enterprise Manager ユーザーの作成」を参照してください。

8 **[サインイン]** をクリックします。

Enterprise Manager のメイン画面が表示されます。これで正常にサインインしました。

Enterprise Manager を削除するには :

- コントロール パネルの **[プログラムの追加と削除]** アプレットで、HPCA Enterprise Manager を選択します。使用しているオペレーティング システムの通常の削除手順を使用します。

インストール後の手順

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 agent 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、90 ページの「ジョブを管理する」を参照してください。

Enterprise Manager を設定し、すべてのジョブ タイプを正しく一覧するには :

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 または 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。

インストールのトラブルシューティング

このセクションでは、Enterprise Manager のインストールに関するトラブルシューティング情報について説明します。

MySQL ポートが競合する

ポート アドレスが競合する問題が発生した場合、MySQL で使用するデフォルト ポートを変更する必要があります。Enterprise Manager のインストールでは、MySQL はデフォルトでポート 3479 を使用するようになっています。他のアプリケーションがすでにこのポートを使用している場合は、このポート番号を変更できます。

MySQL のポート番号を変更するには :

1. CAE インストールでは、次のサービスを停止します。

   HP Client Automation Enterprise Manager

   このサービスの停止により、データベース サービスも停止して再開されます。これにより、ポートの変更が反映されます。Core および Satellite のインストールでは、この手順は必要ありません。
2. 次のファイルを編集します。

   CAE: `<InstallDir>\CM-EC\database\bin\opedb.ini`

   Core および Satellite: `<InstallDir>\HPCA\database\bin\my.ini`
3. `port=3479` 行を検索します。

   ここを変更し、使用するポート番号と一致させます。インスタンスは 2 つあり、クライアント セクションとサーバー セクションのそれぞれにインスタンスがあります。両方のポート宣言のインスタンスを同じ値に変更します。
4. ファイルを保存します。
5. `hibernate.cfg.xml` ファイルを編集します。このファイルを編集するには、`ope-core-<version>.jar` ファイルを開く必要があります。WinZip などのアーカイブ展開ツールでこのファイルを開きます。このファイルは次のディレクトリに格納されています。

   CAE: `<InstallDir>\CM-EC\tomcat\webapps\ope\WEB-INF\lib`

   Core および Satellite: `<InstallDir>\HPCA\tomcat\webapps\ope\WEB-INF\lib`
6. `hibernate.cfg.xml` ファイルを検索し、編集するためにそのファイルを開きます。
7. `hibernate.connection.url` 値を検索し、ポート番号 3479 を前述の `opedb.ini` ファイル (または `my.ini` ファイル) で設定したポート番号と同じものに変更します。
8. `hibernate.cfg.xml` ファイルを保存し、`ope-core-<version>.jar` ファイルをまとめて直します。

9 手順 1 で停止したサービスを開始します。

新しいポート設定でデータベースへアクセスできるか検証するには :

1 MySQL コマンドラインツールを確認します。このツールは次のディレクトリに格納されています。

CAE: <*InstallDir*>\CM-EC\database\bin

Core および Satellite: <*InstallDir*>\HPCA\database\bin

2 次のコマンドを実行します。

mysql.exe -uope -pope ope -P<*portNumber*>**>**

この場合、<portNumber> は、前述の手順 port=3479 行を検索します。で指定したポート番号です。例 :

mysql.exe -uope -pope ope -P3479

このコマンドはツールに、ログイン ID は **ope**、パスワードは **ope**、データベースは **ope**、ポートは **3479** であると伝えます。新しく更新したポート番号は必ず指定してください。

3 ログインしたあと、**status** コマンドを実行し、現在のデータベース情報を表示します。

4 **[閉じる]** をクリックして、ツールを閉じます。

Enterprise Manager ポートが競合する

次の情報は、従来の HPCA Enterprise (CAE) のインストールにのみ当てはまります。Core および Satellite のインストールについては、『HPCA Core および Satellites 入門ガイド』を参照してください。

Enterprise Manager で使用されるデフォルトは、HTTP 通信では Tomcat ポート 8080、HTTPS 通信ではポート 8443 です。Tomcat インストールを変更して他のポートを使用する場合、Enterprise Manager のポートも変更する必要があります。

Enterprise のポート番号を変更するには :

1 次のサービスを停止します。

CAE: HP Client Automation Enterprise Manager

Core および Satellite: HPCA Tomcat Server

2 次のファイルを編集します。

<*InstallDir*>\CM-EC\tomcat\conf\server.xml

3 次のテキストを検索します。

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->
<Connector port="8080"
```

このポートを変更し、使用するポート番号と一致させます。

4 また次のテキストも検索します。

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<Connector port="8443"
```

ここを変更し、使用するポート番号と一致させます。

5 server.xml ファイルを保存します。

6 次のファイルを編集します。

<*InstallDir*>\CM-EC\ tomcat\webapps\em\WEB-INF\ Console.properties

7 次の文字列を検索します。

```
opeurl=http\://localhost\:8080/ope/resources
```

```
dtmurl=http\://localhost\:8080/ope/resources
```

SSL を使用している場合、プロトコルは https で、ポートは 8443 です。

ここを変更し、使用するポート番号と一致させます。

8 次の文字列を検索します。

```
vulnerability_management_server_url=http\://localhost\:8080/
vms/livecontent
```

SSL を使用している場合、プロトコルは https で、ポートは 8443 です。

ここを変更し、使用するポート番号と一致させます。

9 Console.properties ファイルを保存します。

10 手順 1 で停止したサービスを開始します。

RMP または OS の配布ジョブが表示されない

[現在のジョブ] および [過去のジョブ] ページで RMP および OS 配布ジョブを正しく表示するには、インストール後に手動で Enterprise Manager を設定する必要があります。23 ページの「インストール後の手順」を参照してください。

3 Enterprise Manager へのアクセスと設定

この章のでは、Enterprise Manager へのアクセス、ナビゲーション、設定に使用できる情報を説明します。サインイン、ユーザーアクセスの設定、ディレクトリ サービスの設定、プロキシ設定の確立、セキュリティおよび適用状況設定の指定、ジョブ管理のためのテンプレート作成が含まれます。次のトピックが含まれます。

Enterprise Manager のナビゲーション

Enterprise Manager を使用すると、企業ディレクトリ サービスに設定ポリシーを設定することで、企業の要求ステートを定義できます。ここでは、Enterprise Manager にサインインする方法と、各タブの目的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取り扱います。

Enterprise Manager へのサインイン

Enterprise Manager を設定する前に、サインインする必要があります。

Enterprise Manager にサインインするには

1 デスクトップの [Enterprise Manager] アイコンをダブルクリックするか、Windows プログラム グループを使用します。

従来の CAE インストールでは、Web ブラウザを開き、次の URL からでも可能です。

`http://<EM_hostname>:8080/em`

<EM_hostname> は、Enterprise Manager がインストールされているデバイス名です。

セキュア (SSL) 通信を利用して Enterprise Manager にサインインするには、ブラウザを開き、次の URL にアクセスします。

`https://<EM_hostname>:8443/em`

Enterprise Manager には、一時証明書を含むデフォルトのトラストストアが内蔵されています。Enterprise Manager へのアクセスに SSL を使用したい場合、このデフォルト証明書を受け入れるか却下するかを質問されます。この証明書を受け入れると Enterprise Manager を使用できるようになりますが、ご使用のサーバーに対して有効な証明書を含むトラストストアにこの一時トラストストアを置き換える必要があります。永続的なトラストストアの作成についての詳細は、『HP Client Automation SSL 実装 ガイド (SSL ガイド)』を参照してください。

Enterprise Manager のポートを変更した場合は、8080 ではなく、Enterprise Manager のポートと同じポート番号をこの URL で使用してください。

Enterprise Manager のユーザー名とパスワード (デフォルトではそれぞれ「admin」と「secret」) でサインインします。まだサインインしていない場合は、デフォルトのユーザー パスワードを必ず変更してください。詳細については、44 ページの「Enterprise Manager ユーザーの作成」を参照してください。

パスワードの入力時は、非 ASCII 文字を使用しないでください。

2 ディレクトリ ソースを選択します。他の設定を完了するまで、ディレクトリ ソースは Portal をインストールしたときに作成したゾーンになっています。

3 **[サインイン]** をクリックします。

ファイアウォールの内側に Enterprise Manager をインストールしており、ファイアウォールの外側から Enterprise Manager にアクセスする場合、Tomcat へのネットワーク接続の受信を許可していることを確認してください (デフォルトのポートは 8080)。これが正しく設定されていない場合、ファイアウォールの外側から Enterprise Manager へアクセスできません。また、SSL (セキュア) アクセスが必要である場合には、ポート 8443 でのネットワーク接続の受信も許可するようにファイアウォールを設定する必要があります。

現在のセッション クレデンシャルが Enterprise Manager の右上隅に表示されます。

Enterprise Manager からサインアウトするには

Enterprise Manager ページの右上隅で、**[サインアウト]** をクリックします。

Enterprise Manager のタブ

次のタブは、完全に構成された Enterprise Manager インストールで利用可能です。

- **ホーム** : このタブでは、次のダッシュボードを表示できます。
  - HPCA 操作
  - 脆弱性管理
  - 適用状況管理

— セキュリティ ツール管理

— パッチ管理

詳細については、173 ページの「ダッシュボードの使用」を参照してください。Reporting Server が Enterprise Manager に統合されるまで、ダッシュボードは機能しません。

- **管理**：このタブでは、環境内のデバイスの表示や管理ができます。詳細については、75 ページの「Enterprise の管理」を参照してください。
- **レポート**：このタブでは、お使いの環境のレポートを確認できます。これらのレポートは Reporting Server が提供するものです。このタブを使用するには、Enterprise Manager で [レポート] を有効にする必要があります (51 ページの「Reporting Server の統合」を参照)。詳細については、『HHP Client Automation Reporting Server インストールおよび設定ガイド (Reporting Server ガイド)』を参照してください。
- **設定**：このタブでは、ディレクトリ サービス、ユーザー アカウント、HP Live Network 設定、ダッシュボードなど、Enterprise Manager の設定が可能です。内部ゾーンのあらゆるアカウントが (非 LDAP アカウント) [設定] タブにアクセスできます。詳細については、44 ページの「Enterprise Manager ユーザーの作成」を参照してください。

オンライン ヘルプ

Enterprise Manager 全体にわたって、状況に応じたオンライン ヘルプが使用できます。

ヘルプ ウィンドウを開くには、ページの右上隅にある  (オンライン ヘルプ) ボタンをクリックします。

ダッシュボード ペインでは、まずペインの右下隅にある  (クイック ヘルプ) ボタンをクリックし、クイック ヘルプ パネルが見えるようにする必要があります。その後、オンライン ヘルプ ボタンをクリックし、ヘルプ ウィンドウを開きます。

オンライン ヘルプ ウィンドウでは、必要な情報を検索するために次のボタンを使用します。

表 3　オンライン ヘルプ ナビゲーション ツール

ボタン	説明
	目次パネルを表示し、目次内の現在のトピックの場所を強調表示します。
	目次内のひとつ「上」のトピックに移動します。
	目次内のひとつ「下」のトピックに移動します。
	現在表示されているヘルプ トピックを印刷します。
	目次を表示します。
	ヘルプ トピックのアルファベット順の索引を表示します。
	すべてのオンライン ヘルプのトピック内を、キーワードやフレーズで検索します。

基本設定

Enterprise Manager の設定を終了するには、次のタスクを最低限完了する必要があります:

- どのディレクトリ サービスを使用するかを選択する。
- コンソールへの管理者認証にどのディレクトリ サービスを使用するかを選択する。
- ポリシーの割り当てにどのディレクトリ サービスを使用するかを決定する。

これらのタスクについては、34 ページの「ディレクトリ サービスの設定」と 43 ページの「コンソール設定の指定」で説明します。

使用する Enterprise Manager の追加機能にあわせて、次のことも実行します。

- Enterprise Manager ユーザーの作成 44 ページ
- ジョブ アクション テンプレートの作成 47 ページ
- Reporting Server の統合 51 ページ
- セキュリティと適用状況の管理の設定 52 ページ
- ダッシュボードの設定 64 ページ
- リモート制御の設定 71 ページ
- イベント監査の設定 72 ページ

ディレクトリ サービスの設定

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
- Enterprise Manager 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 Enterprise Manager で管理されます。

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、Enterprise Manager 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 システム管理者ガイド (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 35 ページ

Configuration Server ディレクトリ サービスへの接続の設定 38 ページ

外部ディレクトリ サービスへの接続の設定 40 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 4　[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 38 ページ

— 外部ディレクトリ サービスへの接続の設定 40 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、Enterprise Manager 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、Enterprise Manager 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]** リストから、**[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、Enterprise Manager 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、38 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。

Enterprise Manager 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 Enterprise Manager 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 ディレクトリ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 Enterprise Manager 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]** リストから、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。

— 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 Enterprise Manager 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、Enterprise Manager 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。例 :

```
<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。例 :

```
<InstallDir>\HPCA\ManagementPortal\etc\CACertificates\
<LDAP Certificate File Name>
```

7 **[次へ]** をクリックします。

8 必要なユーザー インターフェイス パラメータを入力します。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 Enterprise Manager 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 Enterprise Manager 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 Enterprise Manager 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**: このパラメータは、Enterprise Manager 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、Enterprise Manager 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** : このパラメータを有効にすると、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。

コンソール設定の指定

Enterprise Manager ユーザー インターフェイスの詳細オプションを設定するには、[コンソール設定] を使用します。

Enterprise Manager コンソールを設定するには、次の手順を実行します。

1 [設定] タブで、**[コンソール設定]** をクリックします。

2 次のオプションを設定します。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。

— 指定されたデータ セットのキャッシュを期限切れにするときのしきい値を設定するには、**[最大キャッシュ期間 (分)]** を使用します。この値は分単位です。

— [ディレクトリ検索] ダイアログのドロップダウン フィルタのデフォルト属性セットを指定するには、**[ディレクトリ検索属性]** を使用します。

Portal データベースからクエリで取得したデータ (たとえば、テーブルに表示される子やサービスなど) は、Enterprise Manager がキャッシュします。最大キャッシュ期間は、指定されたデータ セットが期限切れになる期間を示します。

有効な値について詳しくは、ご使用のディレクトリ サービスのドキュメントを参照してください。

— リスンするときのポートを含め、オペレーション プロセス エンジン (OPE) の場所を指定するには、**[オペレーション プロセス エンジンの URL]** を指定します。OPE は、通知コマンドを実行する責任を持つ内部の HPCA コンポーネントです。デフォルト HTTP ポートは、8080 です。

— ダッシュボードでの Real Simple Syndication (RSS) フィードなど、Enterprise Manager からのアウトバウンド通信機能で使用するプロキシ サーバーがある場合は、**[HTTP プロキシ サーバー サポートを有効にする]** を選択します。このオプションを選択する場合は、次の設定値も指定する必要があります。

– **Proxy Server のホスト** : プロキシ サーバーのネットワーク アドレス指定可能な名前

– **ポート** : プロキシ サーバーがリスンするポート

3 **[保存]** をクリックして、変更内容を実装します。

4 **[閉じる]** をクリックして、ダイアログを確認します。

Enterprise Manager ユーザーの作成

[設定] タブを使用して、この Enterprise Manager にアクセスできる内部ユーザーを設定します。

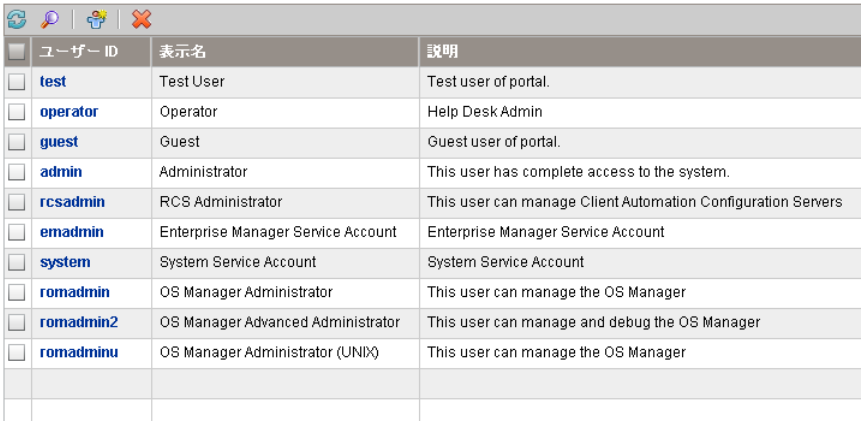
Enterprise Manager からユーザーを作成する場合、内部データ ストアへの管理アクセス権がある Portal ユーザーを作成することになります。ただし、ディレクトリ ソースの設定によっては、このユーザーはディレクトリ ソースにアクセスできない場合があります。LDAP サーバーを使用したくない場合や、認証に使用する LDAP サーバーがない場合には、Enterprise Manager ユーザーを作成する必要があります。

従来の CAE インストールでは、デフォルトで、次のユーザー ID が含まれています。

- test
- operator
- guest
- admin
- rcsadmin
- emadmin
- system

Core および Satellite のインストールでは、前述とは少し異なります。

図 1　ユーザー一覧



ユーザー ID	表示名	説明
test	Test User	Test user of portal.
operator	Operator	Help Desk Admin
guest	Guest	Guest user of portal.
admin	Administrator	This user has complete access to the system.
rcsadmin	RCS Administrator	This user can manage Client Automation Configuration Servers
emadmin	Enterprise Manager Service Account	Enterprise Manager Service Account
system	System Service Account	System Service Account
romadmin	OS Manager Administrator	This user can manage the OS Manager
romadmin2	OS Manager Advanced Administrator	This user can manage and debug the OS Manager
romadminu	OS Manager Administrator (UNIX)	This user can manage the OS Manager

凡例

a　フィルタ ツールバー。フィルタ ボタンをクリックすると表示されます。

b　すべてのユーザーを選択します。

c　ユーザー一覧をリフレッシュします。

d　フィルタ ツールバーを表示したり、非表示にしたりします。

e　ユーザーの作成ウィザードを表示します。

f　ユーザーを削除します。

Enterprise Manager ユーザーを作成するには :

1　[設定] タブで、左側のペインにある **[ユーザー]** ボタンをクリックします。

2　[ユーザー] セクションで、**[新規ユーザー]** ボタンをクリックします。指定した**ユーザー作成ウィザード**が開始されます。

3　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。

- **[ユーザー ID]** を作成します。
- **[表示名]** を作成します。

— そのユーザーに関する分かりやすい **[説明]** を入力します。

— **[パスワード]** を使用して、ユーザー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。

4 **[次へ]** をクリックします。

5 [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。

6 **[閉じる]** をクリックして、ダイアログを確認します。

ユーザーがすでに作成されている場合、そのプロパティを参照したり、パスワードを変更したりできます。

ユーザー詳細を表示するには :

1 [設定] タブで、左側のペインにある **[ユーザー]** をクリックします。

2 ユーザー名をクリックします。以下の画面キャプチャは、[ユーザー プロパティ] ウィンドウのサンプルです。

3 **[要約]** タブをクリックすると、ユーザー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、ユーザーの表示名と説明を参照できます。これらのプロパティは変更できます。

5 変更してから **[保存]** をクリックします。

6 **[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。

7 右上隅にある **X** をクリックして [ユーザー プロパティ] ウィンドウを閉じます。

パスワードを変更するには :

1 [設定] タブで、左側のペインにある **[ユーザー]** ボタンをクリックします。

2 パスワードを変更したいユーザーの名前をクリックします。

3 **[プロパティ]** タブをクリックすると、ユーザーの表示名と説明を参照できます。

4 **[パスワードの変更]** をクリックします。

5 新しいパスワードを入力します。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。

現在サインインしているユーザーのパスワードを変更すると、このセッションは無効になり、再度サインインする必要があります。

6 **[コミット]** 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] ダイアログを閉じます。

8 右上隅にある **X** をクリックして [ユーザー プロパティ] ウィンドウを閉じます。

パスワードが変更されました。

ジョブ アクション テンプレートの作成

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 ジョブ] 領域で管理されます。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、48 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。

次のジョブ アクション テンプレートは、Enterprise Manager をインストールするときに提供されます。

- パッチ接続
- セキュリティ接続
- ソフトウェア接続

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。

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]** タブで、**[ジョブ]** 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。50 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、90 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。

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。

Reporting Server の統合

Reporting Server を使用すると、企業内のデバイスについての情報を表示したり、フィルタリングしたりすることができます。Reporting Server を Enterprise Manager に統合すると、[レポート] タブをクリックすることで Reporting Server にアクセスができます。

この機能を使用するには、企業に合わせて Reporting Server を設定しておく必要があります。Reporting Server のインストールおよび設定については、『Reporting Server ガイド』を参照してください。

Reporting Server を統合するには

1 [設定] タブで、**[レポート]** をクリックします。

2 **[インテグレーションの有効化]** をクリックします。

3 **[HPCA Reporting の URL]** ボックスに、Reporting Server の URL を入力します。[設定] ボックスに完全なホスト名を入力します。

Reporting Server が Enterprise Manager と同じコンピュータ上にある場合でも、`localhost` は使用しないでください。

Core および Satellite のインストールでは、これは自動的に行われます。値は `http://<HPCACoreServer>:3466/rrs`

4 **[保存]** をクリックします。

5 **[閉じる]** をクリックします。統合を完了するには、ここで Enterprise Manager をログアウトする必要があります。

[OK] をクリックして、Enterprise Manager からログアウトします。再度ログインすると、[レポート] タブが表示されます。

セキュリティと適用状況の管理の設定

Enterprise Manager の Live Network の [設定] ページで、HPCA のセキュリティと適用状況の管理ソリューションを設定できます。

- **[設定]** タブでは、HP Live Network コンテンツ サーバーの URL、HP Live Network のログイン認証情報、プロキシ サーバー情報を入力できます。

  HPCA のセキュリティと適用状況の管理ソリューションをホストするシステムとインターネットとの間にプロキシ サーバーがある場合にのみ、プロキシ サーバーの情報を入力します。

  [設定] タブでは、HP Live Network コネクタをダウンロードすることも可能です。ただし、コネクタは HPCA によってインストール、自己更新されるため、ダウンロードが必要となることはほとんどありません。
- **[データベース]** タブでは、Configuration Server およびレポート データベースに関する情報を指定できます。
- **[スケジュールの更新]** タブでは、セキュリティと適用状況の管理コンテンツの更新を設定できます。
- **[すぐに更新]** タブでは、このタブで指定したソースから、セキュリティと適用状況の管理コンテンツをただちに更新できます。

セキュリティと適用状況の管理レポートを有効にするには、HPCA のレポート機能を正しく設定する必要があります。`vm.kit`、`compliance.kit`、`stm.kit` レポート パックは必須です。レポートの生成スピードを最適化するには、レポートのキャッシングも有効にする必要があります。

ここでは、手順を簡単に説明します。レポートおよびレポート パックの詳細については、『Reporting Server インストールおよび設定ガイド』を参照してください。

セキュリティと適用状況の管理レポートを設定するには :

1 Web ブラウザを開いて、次の URL を入力します。

CAE インストール : `http://<ReportingHost>/reportingserver/setup.tcl`

Core インストール : `http://<ReportingHost:3466>/reportingserver/setup.tcl`

ここでの `<ReportingHost>` は、Reporting Server 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 **[VM レポートの有効化]** 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。

4 オプション : 脆弱性管理レポートの生成スピードや表示スピードを最適化するには、次の手順に従います。

   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、20 分は 1200 秒とします。

5 **[適用]** をクリックします。

6 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。

7 適用状況管理の 手順 3 ～ 手順 5 を繰り返します。

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 セキュリティ ツール管理の 手順 3 ～ 手順 5 を繰り返します。

HP Live Network の設定

Enterprise Manager セキュリティと適用状況の管理機能の設定には、次の 3 つのステップがあります。

- HP Live Network サーバーへの接続の設定 54 ページ
- データベースの設定 55 ページ
- Live Network 更新の設定 58 ページ

Live Network の [設定] ページのタブには、これらのステップを実行するのに必要な設定が含まれています。[設定] および [データベース] タブでは、設定を保存前にテストできます。

Live Network の [設定] タブで入力したパスワードは暗号化されます。

Core および Satellite のインストールでは、このセクションで説明した設定手順の一部は必要ありません。ただし、従来の CAE のインストールではすべての手順を実行する必要があります。

HP Live Network サーバーへの接続の設定

HP Live Network から最新のセキュリティと適用状況のコンテンツを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、[設定] タブのを使用します。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
- Enterprise Manager と HP Live Network コンテンツ サーバーの間にインターネット プロキシ サーバーが存在する場合は、そのプロキシ サーバーの名前、ポート、および認証の認証情報。

このタブ 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、Enterprise Manager 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、62 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、**[Live Network]** をクリックします。
2. **[設定]** タブをクリックします。
3. 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** — Enterprise Manager をホストするシステムで実行可能な Live Network コネクタへのパスです (パスはデフォルトで設定されています)。

詳細については、166 ページの「HP Live Network コネクタの手動での実行」および 61 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。

— **HTTP プロキシ サーバー** — プロキシ サーバーが使用されている場合は、その URL とポート。これにより、Enterprise Manager と HP Live Network コンテンツ サーバーの間のインターネット通信を容易にします。

この URL は次の形式で指定してください。

[http|https]://*server*:*port*

例 : **https://webproxy.mycompany.com:8088**

プロキシ サーバーの URL に、正しいプロトコル、名前、およびポートを指定してください。Enterprise Manager は、この URL を検証しません。値が正しくないと、HP Live Network のコンテンツを更新できなくなります。

— **プロキシ ユーザー名** — プロキシ サーバーへのアクセスに使用するユーザー名。この設定は、プロキシ サーバーでの認証が必要な場合にのみ必須です。

— **プロキシのパスワード** — プロキシ サーバーへのアクセスに使用するパスワード。この設定は、プロキシ サーバーでの認証が必要な場合にのみ必須です。

4 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、62 ページの「Live Network の設定のテスト」を参照してください。

5 **[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 Enterprise Manager 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、最後に保存した設定に戻すことができます。

データベースの設定

HP Live Network からダウンロードしたセキュリティと適用状況の管理情報をパブリッシュする場所を指定するには、[データベース] タブを使用します。

- レポート データベース

最新の HP Live Network 脆弱性定義は、レポート データベースにパブリッシュされます。これらの定義はその後、さまざまなレポート (233 ページの「レポートの使用」を参照) とダッシュボード ペイン (173 ページの「ダッシュボードの使用」 を参照) に取り込むために使用されます。

これは、インベントリ データベースと同じデータベースです。したがって、レポート データベースへの接続で使用されるデータベース情報は、インベントリ データベースに ODBC DSN を設定するときに必要だった情報と同じです。この手順は、Core および Satellite インストールのインストールと設定作業の一部として実行しました。

従来の HPCA Enterprise インストールについては、『Configuration Server ガイド』および『Messaging Server ガイド』を参照してください。Core および Satellite のインストールについては、『HPCA Core および Satellites 入門ガイド』を参照してください。

- Configuration Server Database

  最新の HP Live Network スキャナとデータは、Configuration Server にパブリッシュされます。その後 Configuration Server は、Configuration Server Database (CSDB) の SECURITY ドメインにあるスキャナ サービスにこのコンテンツを強制配布します。最新のスキャナとデータは、脆弱性または適用状況のスキャンが実行されるたびに管理対象クライアント デバイスに配布されます。

このタブ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、Enterprise Manager は、脆弱性と適用状況管理のコンテンツを格納するデータベース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。

データベース設定を指定するには

1 [設定] タブで、**[Live Network]** をクリックします。

2 **[データベース]** タブをクリックします。

3 レポート データベースの [設定] で、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。

   — **データベースのタイプ** — リストから、[oracle] または [sqlserver] を選択します。

   — **データベース サーバー** — レポート データベースが存在するシステムの完全なホスト名と IP アドレスを指定します。

   SQL Server を使用していて、その SQL Server がデフォルトのデータベース インスタンス以外のデータベース インスタンスを使用するように設定されている場合は、そのインスタンスをサーバー名に付加する必要があります。例 :

```
mydbserver.mycompany.com\myinstance
```

また、**[データベース名]** フィールドにデータベース名を指定する必要があります。

- **ポート** — Reporting Server へのアクセスに使用するポートを指定します。デフォルトでは、Oracle は 1521、SQL Server は 1433 です。

  SQL Server などの一部のデータベースでは、データベース管理ソフトウェアでスタティック ポートを使用するように特に設定されていない限り、ダイナミック ポートを使用できます。データベースがダイナミック ポートを使用するよう設定されている場合は、このフィールドは空白にします。

- **データベース名** — レポート データベースの名前を指定します。Oracle の場合、この名前はデータベースの SID と同じです。

- **データベース ユーザー** — レポート データベースへのアクセスに使用するユーザー名を指定します。

- **パスワード** — 上で指定したレポート データベース ユーザー用のパスワードを入力します。

4. Configuration Server の下で、一覧にある CSDB サービスのアカウント ID 用の **[パスワード]** を指定します。

   ここに示す Configuration Server の他のパラメータは、[設定] タブの [ディレクトリ サービス] ページで設定します。

5. 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。

6. **[保存]** をクリックして、変更内容を実装します。

Enterprise Manager は、テストに成功した後に設定を自動的に保存しません。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、最後に保存した設定に戻すことができます。

Live Network 更新の設定

HP Live Network のセキュリティと適用状況の管理コンテンツを更新する方法と時期を指定するには、[スケジュールの更新] タブと [すぐに更新] タブを使用します。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適用状況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、61 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**

  セキュリティと適用状況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`

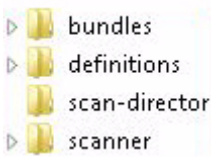
  このパスは、HPCA によって自動的に設定されます。HP Live Network コネクタの新しいコピーをダウンロードして、別のロケーションにインストールしていない限り、このパスを指定する必要はありません。

  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、セキュリティと適用状況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、166 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。

  168 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。

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 [設定] タブで、**[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 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 [設定] タブで、**[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。

CAE インストール :

`<InstallDir>\VulnerabilityServer\logs\vms-server.log`

Core および Satellite インストールでの Core Server:

`<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。

[データベース] タブでレポート データベースが正しく設定されていない場合、このレポートにレコードがない可能性があり、ログ ファイルを使用する必要が生じます。レポートの詳細については、233 ページの「レポートの使用」を参照してください。

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、だれかが誤ってアンインストールした場合) 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、**[Live Network]** をクリックします。

2 [設定] タブをクリックします。

3 [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。

4 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`

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。Enterprise Manager 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、次のアクションが実行されます。

- [設定] タブ

  Enterprise Manager 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。このタブ に表示されるすべての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。

- [データベース] タブ

  Enterprise Manager は、指定した設定を使用して、まずレポート データベースへの接続を試行し、それから Configuration Server への接続を試行します。

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。[データベース] タブでは、レポート データベースと Configuration Server のテスト結果が別々に表示されます。

表 5　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)。 • レポート データベースのデータベース情報が正しくない。 • Configuration Server のパスワードが正しくない。 レポート データベースまたは Configuration Server により、その他のエラーが報告されることもあります。

表 5　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
	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、Enterprise Manager 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。また、エラーがないかどうか `vms-server.log` ファイルも確認してください (73 ページの「ログ ファイル」参照)。

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。Enterprise Manager は自動的に設定を保存しません。

ダッシュボードの設定

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 オペレーション 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。オペレーション 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 181 ページ

サービス イベント 182 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 184 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、180 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 **[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したいペインの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。

- 脆弱性の重大度別影響 (円グラフ) 187 ページ
- 脆弱性履歴の評価 189 ページ
- 重大度別にした脆弱性の影響 (棒グラフ) 197 ページ
- 脆弱性の影響 191 ページ

オペレーション 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 196 ページ
- 最も脆弱性の高いデバイス 199 ページ
- 最も脆弱性の高いサブネット 200 ページ
- 脆弱性のトップ 202 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、186 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したいペインの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

適用状況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。

適用状況管理ダッシュボードには、エグゼクティブ ビューおよびオペレーション 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 208 ページ
- 適用状況ステータス 206 ページ
- 適用状況評価履歴 209 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。

- 失敗頻度の高い SCAP 規則 211 ページ
- 失敗回数の多いデバイス (SCAP ルール別) 213 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、205 ページの「適用状況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。

適用状況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、**[適用状況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したいペインの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 ビューおよびオペレーション 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 216 ページ
- セキュリティ製品の概要 218 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 220 ページ
- 最新のセキュリティ製品のスキャン 221 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、215 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したいペインの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) 225 ページ
- ブリテン別デバイス適用状況 227 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) 228 ページ
- Microsoft セキュリティ ブリテン 229 ページ
- 最も脆弱性の高い製品 230 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、224 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したいペインの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。

リモート制御の設定

Enterprise Manager 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、Enterprise Manager 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、110 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。

- **VNC (Virtual Network Computing) の有効化**
- **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、109 ページの「デバイスのリモート制御」を参照してください。

関連トピック：

イベント監査の設定 72 ページ

イベント監査の設定

セキュリティと適用状況のデータ取得やリモート制御の記録をするには、HPCA イベント監査サブシステムを正しく設定する必要があります。次の要件を満たす必要があります。

- HPCA Messaging Server の「Core」データ配信エージェント (core.dda) を有効にし、設定する必要があります。これにより監査テーブルが作成されます。
  - — Core および Satellite のインストールでは、このコンポーネントは自動的にインストールされるため、HPCA Core Console でメッセージ設定を指定して設定するだけです。
  - — 従来の CA Enterprise インストールでは、core.dda を選択し、Messaging Server のインストールの一部として設定します。

  詳細な手順については、『Core および Satellite 入門ガイド』または『Messaging Server インストールおよび設定ガイド』を参照してください。
- HPCA 管理レポートを有効にするには、HPCA Reporting Server を正しくインストールし設定する必要があります。HPCA 管理レポート パック (admin.kit) は必須です。レポートの生成スピードを最適化するには、HPCA 管理レポートのキャッシングも有効にする必要があります。

  以下にて手順を簡単に説明します。レポートおよびレポート パックの詳細については、『Reporting Server インストールおよび設定ガイド』を参照してください。
- 脆弱性管理サブシステムを設定する必要があります。監査サブシステムでは、脆弱性管理サブシステムで使用するデータベース接続設定と同じものを使用します。150 ページの「セキュリティと適用状況の管理の設定」を参照してください。

HPCA 管理レポートを設定するには次の手順を実行します。

1 Web ブラウザを開いて、次の URL を入力します。

CAE インストール : `http://<ReportingHost>/reportingserver/setup.tcl`

Core インストール : `http://<ReportingHost:3466>/reportingserver/setup.tcl`

ここでの <ReportingHost> は、Reporting Server 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、[HPCA 管理レポート設定] をクリックします。

3 **[HPCA 管理レポートの有効化]** 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。

4 オプション : 管理レポートの生成スピードや表示スピードを最適化するには、次の手順に従います。

   a **[HPCA 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 **[HPCA キャッシュの存続期間]** を秒単位で指定します。たとえば、20 分は 1200 秒とします。

5 **[適用]** をクリックします。

ログ ファイル

Enterprise Manager への接続や Enterprise Manager 機能の使用で問題が発生したときには、ログ ファイルの参照が必要な場合もあります。Enterprise Manager のログ ファイルは、デフォルトで次の場所に保存されています。

CAE: <*InstallDir*>\CM-EM\tomcat\logs

Core および Satellite: <*InstallDir*>\HPCA\tomcat\logs

Enterprise Manager は複数のログ ファイルに情報を保存します。

- catalina.<date>.log Enterprise Manager のサーバー ログ メッセージが含まれています。デフォルトのログ ディレクトリには、指定した <date> (たとえば、catalina.2007-10-22.log) のサーバー ログが複数見つかる場合があります。
- OvCMEmTomcat
  Tomcat サービスのインストール、停止、開始に関連するメッセージが含まれています。

- ope.log Enterprise Manager ジョブのプロセス エンジンのメッセージが含まれています。デフォルトのログ設定では、5 MB 未満のバックアップ ログ ファイルが最大 10 ファイルまで許可されています。1 つめのログ ファイルは ope.log となり、それ以降のファイルには番号が付加されます (たとえば、ope.log.1、ope.log.2)。バックアップ ファイルが 10 個生成されると、現在のログ ファイルのバック アップ時には最も古いファイルが置き換えられます。

セキュリティと適用状況の管理ログ ファイルは、次の場所に保存されています。

CAE: <*InstallDir*>\VulnerabilityServer\logs

Core および Satellite: <*InstallDir*>\HPCA\VulnerabilityServer\logs

- vms-server.log には、脆弱性管理サーバー メッセージが含まれています。デフォルトのログ設定では、5 MB 未満のバックアップ ログ ファイルが最大 5 ファイルまで許可されています。1 つめのログ ファイルは vms-server.log となり、それ以降のファイルには番号が付加されます (vms-server.log.1、vms-server.log.2 等)。
- vms-commandline.log には、content-update.bat コマンドで記録されるステータスおよびエラー メッセージが含まれています。詳細については、150 ページの「HP Live Network コンテンツの更新」を参照してください。デフォルトのログ設定では、5 MB 未満のバックアップ ログ ファイルが最大 5 ファイルまで許可されています。

  vms-commandline.log では、vms-server.log と同じファイル命名規則が使用されます。どちらの場合も、バックアップ ファイルが 5 個生成されると、現在のログ ファイルのバック アップ時には最も古いファイルが置き換えられます。

  サーバーを再起動せずに、脆弱性管理サーバーのログ レベルを変更できます (たとえば、INFO または DEBUG など)。ログ レベルは次のファイルで指定されています。

  log4j-server.properties

  log4j-commandline.properties

  どちらのファイルも次の場所に保存されています。
  <*InstallDir*>VulnerabilityServer\conf

  ログ レベルを変更すると、その変更は、該当ファイルの保存後約 60 秒でログ ファイルのメッセージに反映されます。

ログのすべての内容を理解する必要はありませんが、次の場合のためにログについて認識しておく必要があります。

- **SEVERE**、**FATAL**、**ERROR** とラベルされたエントリを探せるようになる。
- HP Support の指示に従って、このファイルにアクセスする。

4 Enterprise の管理

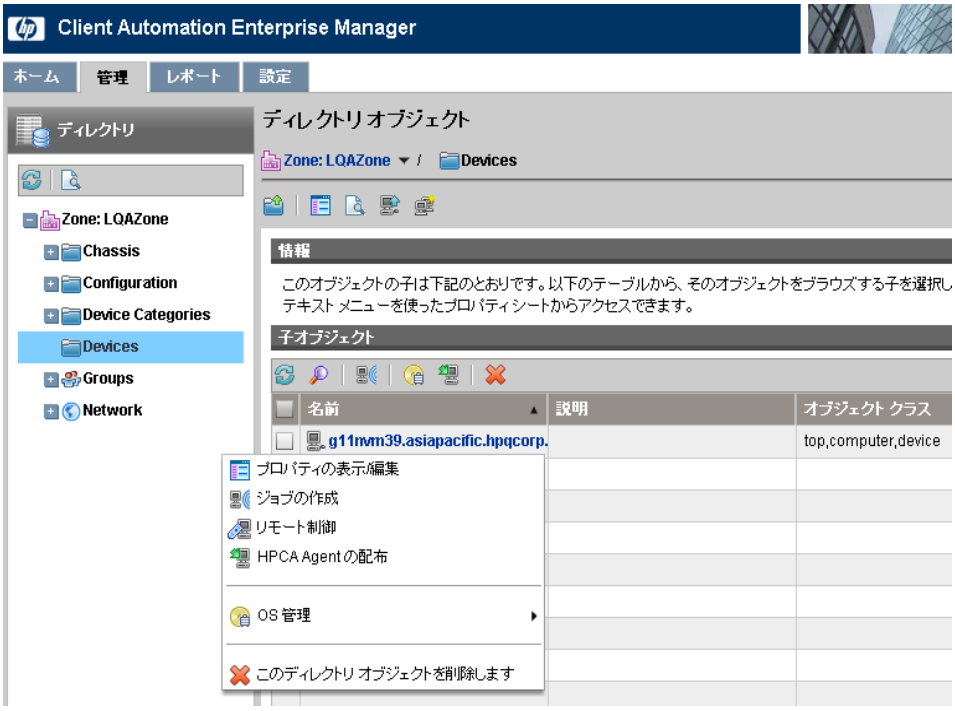
管理領域には、お使いの環境におけるクライアント デバイスの管理に使用するツールが含まれています。この章のは、次の各トピックで構成されています。

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。34 ページの「ディレクトリ サービスの設定」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 2　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 6　ドロップダウン メニューに表示されるアクション

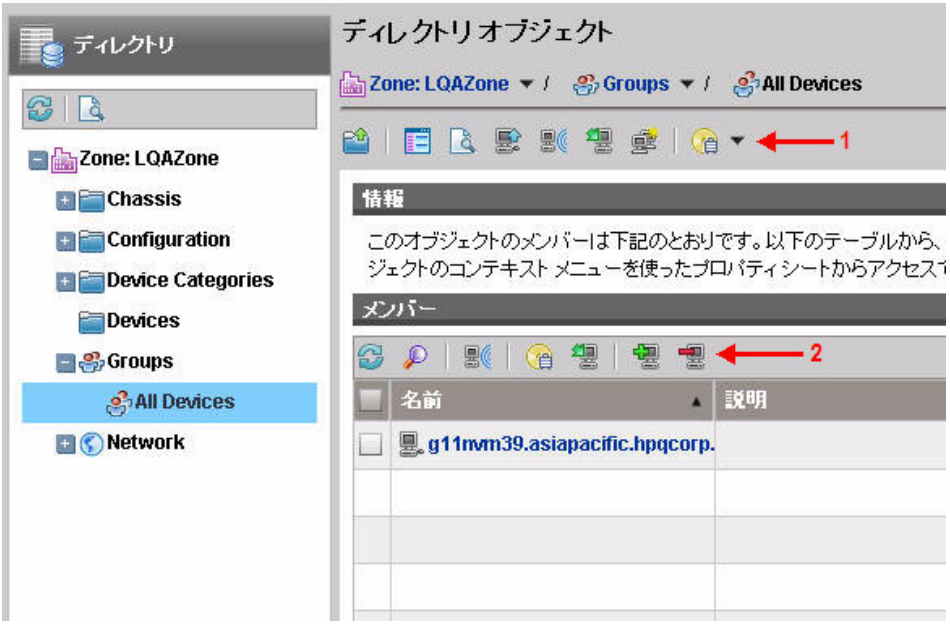
アイコン	アクション	説明
	プロパティの表示 / 編集	新しいブラウザ ウィンドウで、この子オブジェクトのプロパティを表示または編集する。76 ページの「ディレクトリ オブジェクト ビュー」を参照してください。
	ジョブの作成	このオブジェクトの通知ジョブまたは DTM ジョブを作成する。90 ページの「ジョブを管理する」を参照してください。
	リモート制御	管理対象デバイスにリモート アクセスする。109 ページの「デバイスのリモート制御」を参照してください。
	HPCA Agent の配布	このデバイスに HPCA Agent を配布し、HPCA によって管理できるようにする。88 ページの「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。115 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。
	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。86 ページの「デバイスをインポートする」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。

78 ページの図 3 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 3　ディレクトリ オブジェクト ビューのツールバー

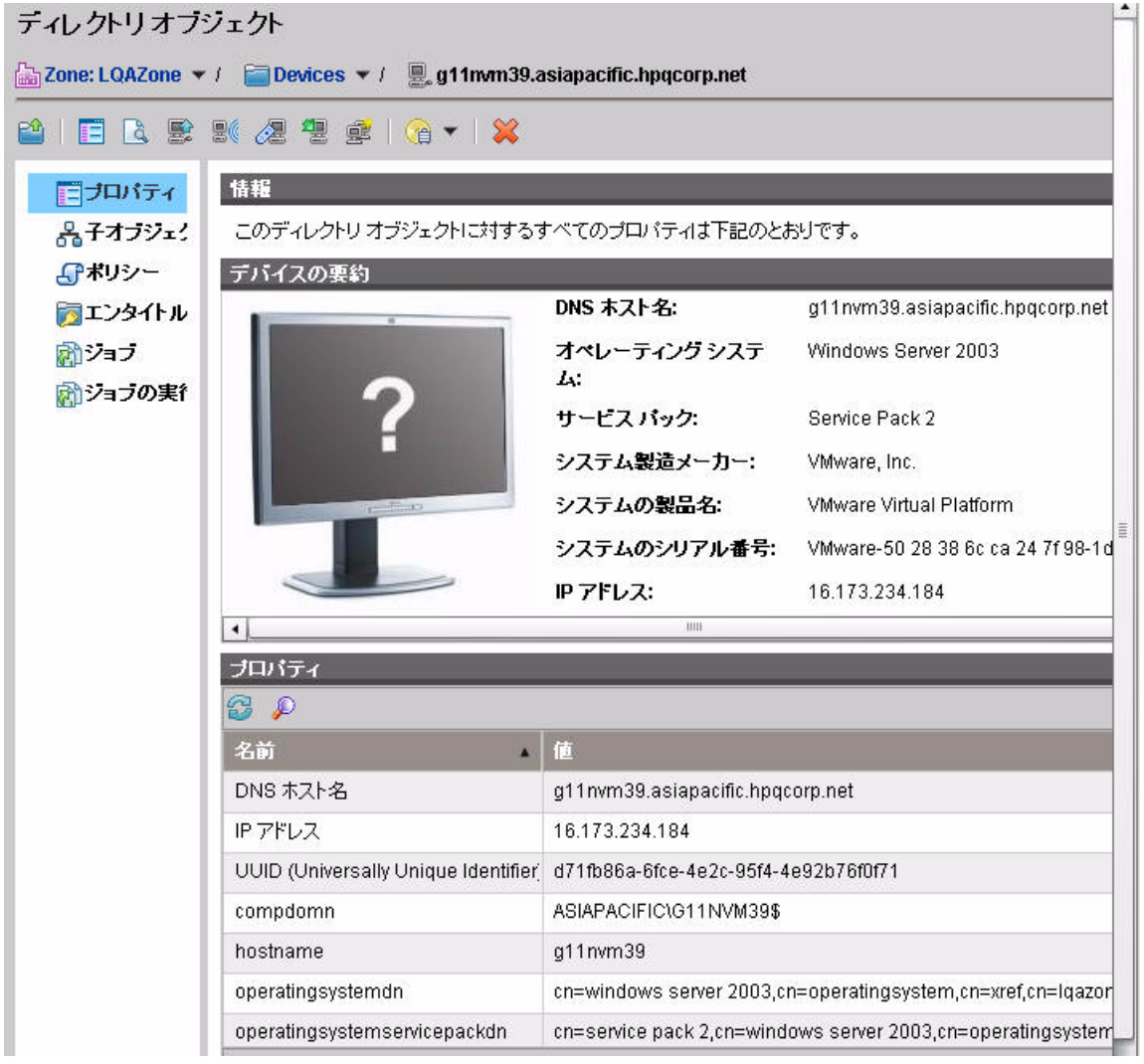


この例では、上側のツールバー (**1**) が全デバイス グループに関連し、下側のツールバー (**2**) がグリッドで選択した子 (またはメンバー) に関連しています (この場合は、Device110 と Device113)。

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 (79 ページの図 4 を参照)。

図 4　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、92 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。
- **[Virtual Machines (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、102 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

Enterprise Manager 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、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。使用可能な属性のリストを設定する方法は、43 ページの「コンソール設定の指定」を参照してください。

> 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。

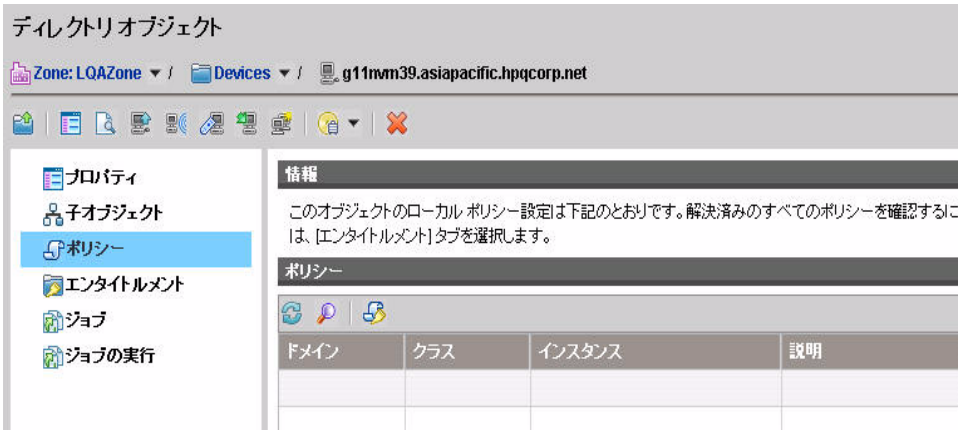
3 **[検索]** をクリックします。指定した条件と一致するオブジェクトは、[検索結果] テーブルに一覧表示されます。

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 (79 ページの図 4 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 5　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 (78 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。

   82 ページの図 5 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、Enterprise Manager 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。

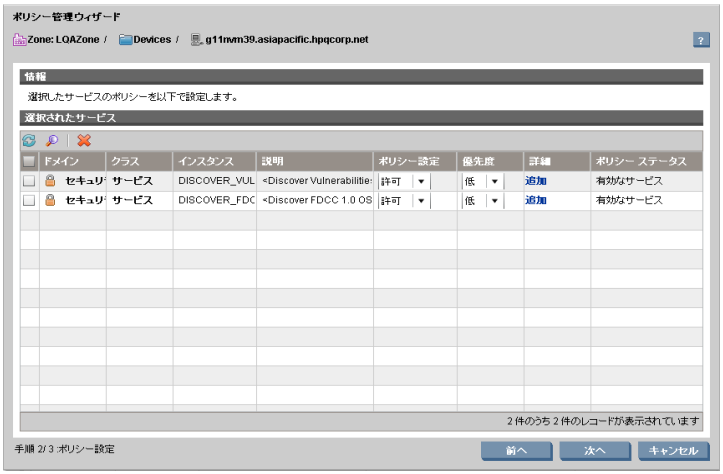
6 [手順 1/3 : サービスの選択] では、オブジェクトのポリシーに追加するサービスを選択します。サービスの選択元の Configuration Server Database ドメインを選択します。

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順位を設定します。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

Enterprise Manager 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。

  Reporting Server 統合を有効にしていなければ、ここに情報が表示されません。統合を有効にする方法は、51 ページの「Reporting Server の統合」を参照してください。レポートについての詳細は、「Reporting Server ガイド」を参照してください。

[レポート] タブで概要レポートを表示するには、Reporting Server で **Use Portal for Logon Authentication** を有効化する必要があります。このオプションはデフォルトでは無効になっています。

デバイスをインポートする

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。102 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。Enterprise Manager 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 (90 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 Enterprise Manager 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 Enterprise Manager 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。

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

表 7　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、Enterprise Manager 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。 Enterprise Manager 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 infrastructure 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、Enterprise Manager で設定および管理できます。 これは、HPCA infrastructure
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。Enterprise Manager 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。

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。詳細については、261 ページの「ジョブの問題」を参照してください。

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 Enterprise Manager 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 8　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
	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、98 ページの「新しい DTM または通知ジョブの作成」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。92 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。93 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。96 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。95 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 9　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。92 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。96 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。94 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 (95 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)。97 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 10　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、95 ページの「通知ジョブのジョブの詳細」または 94 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、97 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

Enterprise Manager 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 11　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。

表 11　ジョブの実行状態の説明

状態	説明
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 または通知ジョブの作成

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、88 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、115 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 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 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、47 ページの「ジョブ アクション テンプレートの作成」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、93 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。

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 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 Server との同期を行うまでは、そのジョブを実行できます。

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。

CAE インストール : `C:\Program Files\HP\HP BTO Software\CM-EC\tomcat`

Core および Satellite: `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、HPCAEnterprise Manager 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 12　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
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

表 12　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
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。

CAE インストール : C:\Program Files\HP\HP BTO Software\CM-EC\tomcat

Core および Satellite: 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。

仮想マシンの管理

Enterprise Manager 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。

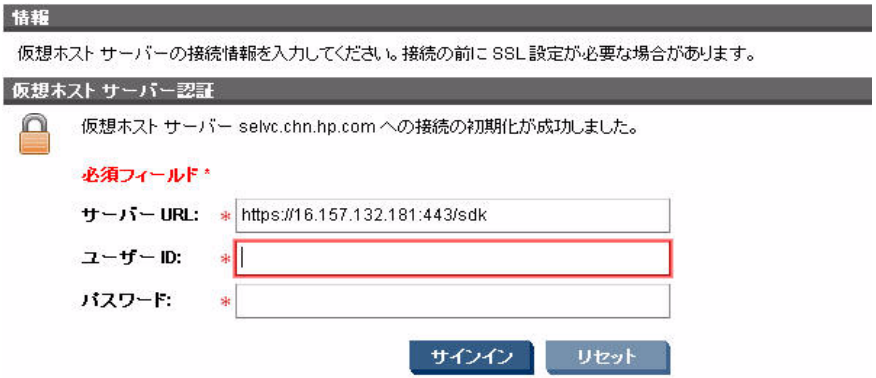
3 デバイスのリストで、使用している ESX Server を探します。

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。79 ページの図 4 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 Enterprise Manager 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。

105 ページの図 7 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 6　VMware ESX Server のデバイス プロパティ

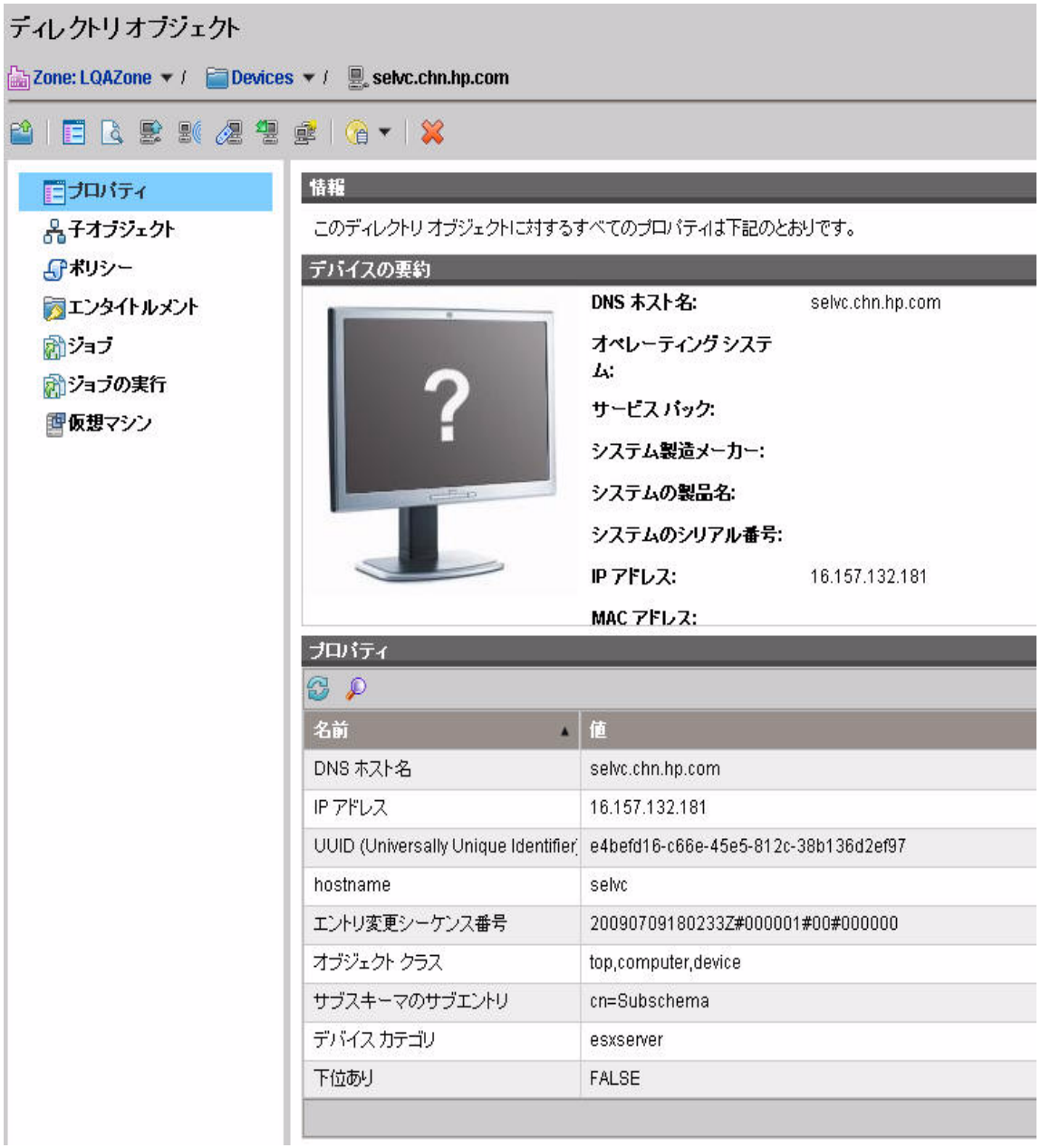
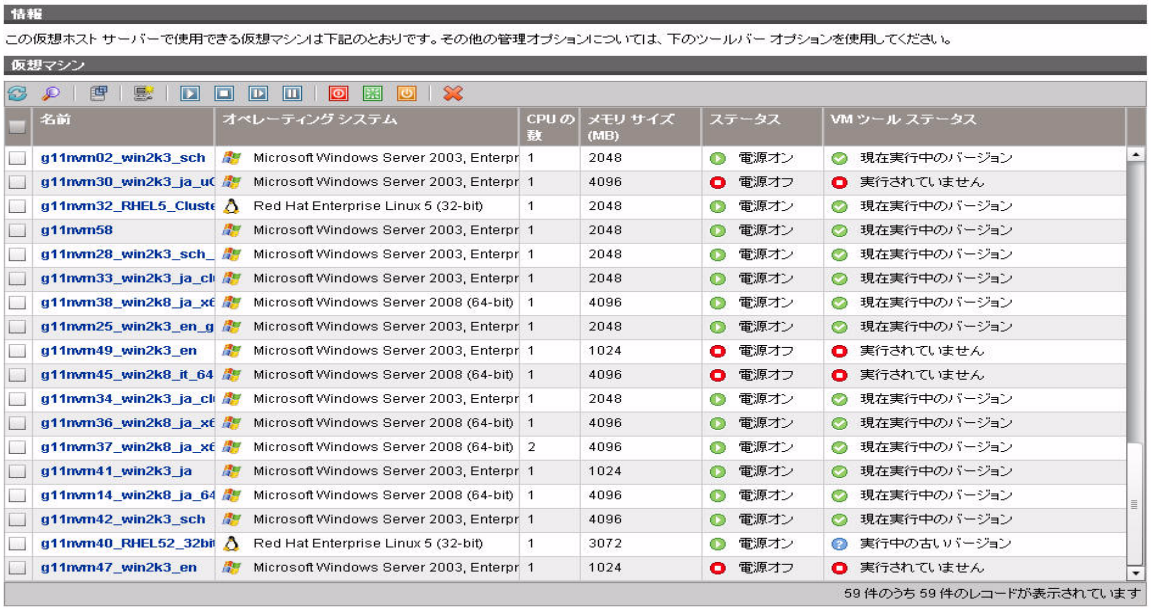


図 7　ESX Server でホストされる仮想マシン一覧



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 13　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 14　[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 :

1 102 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。

- **Data Center（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。
- **Host System（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

Enterprise Manager 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

Enterprise Manager 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、71 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、110 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。

Enterprise Manager 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 110 ページ
リモート制御の設定 71 ページ
リモート制御の監査 114 ページ

リモート接続の要件

Enterprise Manager 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、Enterprise Manager 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 Enterprise Manager 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、Enterprise Manager 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、Enterprise Manager 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。例 :

`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、Enterprise Manager 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 Enterprise Manager 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。

- Enterprise Manager 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。
- Enterprise Manager 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

Enterprise Manager 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。例:

- Windows システムでは、TCP ポート 5900 のみが必要です。

- Linux システムにおいて、VNC Sever がホスト 1 で実行しているとします。この場合、サーバーとリモート デバイスの間のファイアウォールは TCP ポート 5901 へのアクセス許可が必要となります。

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。

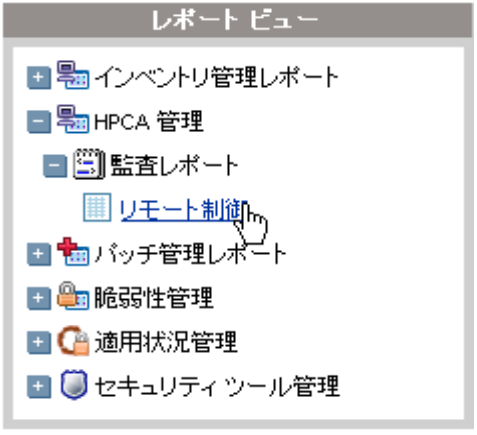
http://www.realvnc.com/support/faq.html#firewall

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、Enterprise Manager 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 Enterprise Manager 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 – Enterprise Manager 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 109 ページ

イベント監査の設定 72 ページ

レポートの使用 233 ページ

オペレーティング システムの管理

Enterprise Manager 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

Enterprise Manager 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、「Preparing and Capturing OS Images」(『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、「Using the Publisher」(『HPCA OS Manager System Administrator ユーザー ガイド』) を参照してください。

- OS イメージを含むサービスをターゲットのデバイスへ展開するのに使用したプロキシ サーバーがインストールされ、正常に設定されている必要があります。

詳細については、『HPCA Proxy Server インストールおよび設定ガイド』を参照してください。このサーバーのインストール、および Configuration Server との共存について説明しています。

- HPCA OS Manager をインストールし、正しく設定しておく必要があります。

  詳細については、『HPCA OS Manager システム管理者ユーザー ガイド』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、Enterprise Manager 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 15　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 • オプション : デバイスをグループに追加 • OS 管理ウィザードを使用して OS を配布 注意 : OS 配布プロセスの間に LSB を使用する場合、PXE やイメージ配布 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

表 15　配布シナリオ

デバイスの状態	配布の手順
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 : 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 Satellites 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。例 :

```
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 (91 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

Enterprise Manager 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 オプション: 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。88 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 システム管理者ユーザー 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。117 ページの「OS 管理の前提条件」および 118 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（オプション）

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は、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。126 ページの「LSB の使用」を参照してください。
- **ネットワーク ブート (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。126 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。126 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 システム管理者ガイド』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。(90 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、118 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、118 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、118 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。例 :

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 Enterprise Manager で次の手順を実行します。

a [管理] タブで、123 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

Enterprise Manager 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。(90 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 (91 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)。122 ページの「OS 配布状態の表示」を参照してください。

OS 配布用の CD/DVD の作成

このトピックは、従来の HPCA インストールにのみ関連しています。

次のスクリプトを使用して、Configuration Server データベースにアップロードされた OS イメージ サービスをダウンロードすることができます。

`<OSMInstallDir>\OSManagerServer\modules\osm-download.tcl`

この場合、<OSMInstallDir> は OS Manager 用のインストール ディレクトリです。デフォルトでは、次のようになります。

C:\Program Files\Hewlett-Packard\HPCA

次に、これらのサービスを使用して OS 配布用の CD または DVD を作成することができます。

スクリプト構文は以下のとおりです。

nvdkit.exe < スクリプトの場所 >\osm-download.tcl -host < ホスト名 > -csport <CS ポート > -port < プロキシ ポート > -user < ユーザー ID> -pass < パスワード > -logfile < ログファイル > -outdir <out-dir> -service < サービス >

- <script-location>: OS Manager Server インストール \modules ディレクトリ（上記参照）
- -host <ホスト名>: Configuration Server ホスト名（デフォルトは localhost）
- -csport <CS ポート >: Configuration Server ポート（デフォルトは 3464）
- -port <プロキシ サーバー>: CA Proxy サーバー ポート（デフォルトは 3466）。プロキシ サーバーからリソースをダウンロードするには時間がかかることがあります。
- -user < ユーザー ID>: Configuration Server のユーザー ID
- -pass < パスワード >: Configuration Server のパスワード
- -outdir <out-dir>: ダウンロードしたサービス用の出力フォルダ。
- -logfile < ログファイル >: このスクリプトのログ ファイル。デフォルトでは、次のようになります。

  .\osm-download.log
- -service < サービス >: スペースで区切られたサービスのリスト。少なくとも 1 つ以上のサービスが必要。サービス名の形式は次のようになります。

  PRIMARY.OS.ZSERVICE.SERVICENAME

  例：

  PRIMARY.OS.ZSERVICE.EMCPET5 PRIMARY.OS.ZSERVICE.MY_OS

実行ファイル nvdkit.exe はデフォルト OS Manager Server インストール ディレクトリ：

C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer に配置されます。

次の例では、デフォルトのインストール先とデフォルトの Configuration Server ユーザー名証明書を使用してスクリプトか実行され、c:/tmp/CDDeploy/out ディレクトリに EMCPET5 および MY_OS サービスがダウンロードされます。

```
nvdkit.exe "C:\Program
Files\Hewlett-Packard\HPCA\OSManagerServer\modules\osm-download.
tcl" -host localhost -port 3466 -user admin -pass secret -logfile
c:/tmp/CDDeploy/osm-download.log -outdir c:/tmp/CDDeploy/out
-service PRIMARY.OS.ZSERVICE.EMCPET5 PRIMARY.OS.ZSERVICE.MY_OS
```

実行ファイル nvdkit.exe およびスクリプト osm-download.tcl は、必要に応じて別のデバイスにコピーすることができます。スクリプトを実行して Configuration Server と CA Proxy Server を接続すると、Configuration Server データベースからリソースを直接ダウンロードする場合よりも時間がかかります。

5 セキュリティと適用状況の管理

HPCA のセキュリティと適用状況機能により、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。この章のは、次の各トピックで構成されています。

はじめに

HPCA のセキュリティと適用状況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 134 ページ
- 適用状況管理 136 ページ
- セキュリティ ツール管理 139 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 16　脆弱性管理用語

用語	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。
露出	露出は、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 16　脆弱性管理用語

用語	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露出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 16　脆弱性管理用語

用語	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。OVAL は 3 つの XML スキーマに基づいており、システム設定の表示、マシンの特定の状態の表現、および評価結果のレポート作成の 3 つの手順で構成されるセキュリティ脆弱性評価プロセスです。 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。OVAL 定義の大部分は CVE に基づいていますが、一部基づかないものもあります。HP Live Network では、OVAL および CVE 形式の情報が HPCA に転送されます。 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 17　適用状況管理用語

用語	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 17　適用状況管理用語

用語	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 (134 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 (134 ページの「脆弱性管理」を参照) • CVSS (134 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露出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 Enterprise Manager 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、53 ページの「HP Live Network の設定」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。
- ダッシュボードに値を設定するために使用されるレポートが表示されるよう Reporting Server を正常に設定する必要があります。
- Enterprise Manager でレポートを有効にする必要があります。51 ページの「Reporting Server の統合」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。

- パッチ管理ダッシュボードとパッチ管理レポートを使用するには、お使いの環境に HPCA Patch Manager をインストールする必要があります。詳細については、『HP Client Automation Patch Manager インストールおよび設定ガイド (Patch Manager 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。145 ページの図 8 を参照してください。

Enterprise Manager 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。

Enterprise Manager 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、173 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 18　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適用状況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。61 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、セキュリティと適用状況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 セキュリティと適用状況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。

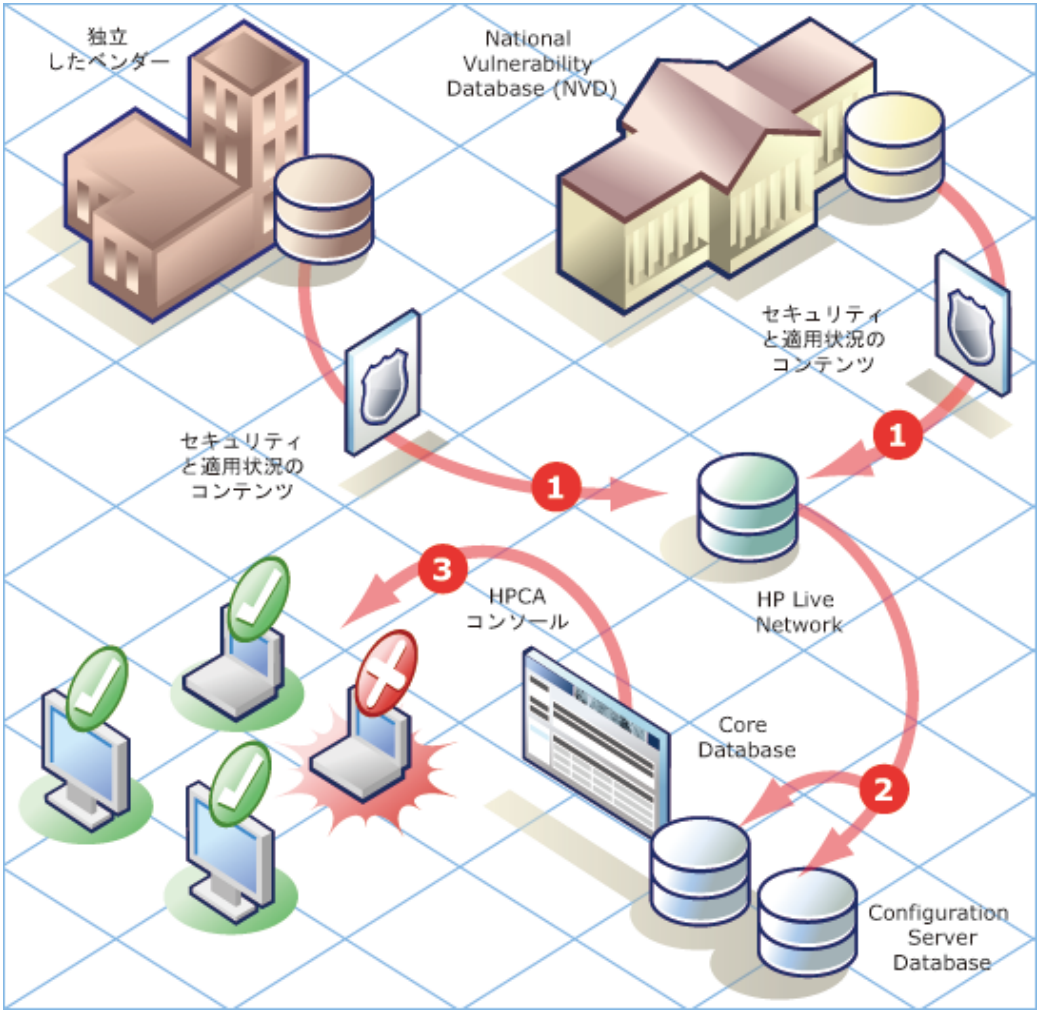
1 更新されたスキャナとデータの両方が一時ディレクトリにコピーされます。

2 データが一時ディレクトリから Reporting 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 Reporting データベースに送信されます。

図 8　HPCA でのセキュリティと適用状況の管理



1　更新されたセキュリティと適用状況のコンテンツが 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適用状況のコンテンツ (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 Reporting 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、セキュリティと適用状況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適用状況のコンテンツには、「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 (168 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。Reporting Server 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、セキュリティと適用状況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適用状況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. Enterprise Manager 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。例 :
   - SECURITY.ZSERVICE.DISCOVER_VULNERABILITY
   - SECURITY.ZSERVICE.DISCOVER_FDCC_1-0_OS

— SECURITY.ZSERVICE.DISCOVER_SECTOOLS_AV_AS_FW

[サービスの詳細] ウィンドウが表示されます。サービスの詳細については、85 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。153 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、151 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。

セキュリティと適用状況の管理の設定

52 ページの「セキュリティと適用状況の管理の設定」を参照してください。

一般的なセキュリティと適用状況管理のタスク

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 [設定] 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 Enterprise Manager 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、58 ページの「Live Network 更新の設定」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、160 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

Enterprise Manager 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。

152 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、Enterprise Manager からスキャンをスケジュール設定または起動します。153 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。154 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、147 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

Enterprise Manager 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 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 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、93 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、90 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適用状況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 (セキュリティと適用状況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。例 :

```
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

Enterprise Manager 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、233 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、173 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、250 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、HP Client Automation Patch Manager 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。詳細については、『HP Client Automation Patch Manager インストールおよび設定ガイド (Patch Manager ガイド』を参照してください。

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や、特定のデバイスで失敗した特定の規則に関して、詳細情報まで掘り下げられます。

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、特定の適用状況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 19

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 215 ページ
- セキュリティ ツール管理レポート 246 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適用状況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 160 ページ
- HP Live Network コネクタの手動での実行 166 ページ
- 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 168 ページ

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、[設定] 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。

CAE: `<InstallDir>\VulnerabilityServer\bin`

Core および Satellite: `<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 (165 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。詳細については、73 ページの「ログ ファイル」を参照してください。

`content-update.bat` コマンドの一般的な使用については、165 ページの「例」を参照してください。

必須設定

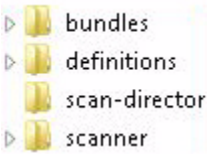
次の表は、content-update.bat コマンドの必須設定を示します。

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 (165 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 20　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。53 ページの「HP Live Network の設定」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 NetworkLive Network 設定ページのタブを更新します。53 ページの「HP Live Network の設定」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。160 ページの「高度なトピック」を参照してください。

表 20　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 (165 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 21　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。 CAE: C:\Program Files\HP\HP BTO Software\LiveNetwork Core および Satellite: 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。

表 21　content-update.bat の省略可能な設定

設定	説明
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*>
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] タブので指定されている値がデフォルトで使用されます。

表 22　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	[データベース] タブ
livenetwork_connector_executable livenetwork_contenturl livenetwork_username livenetwork_password livenetwork_proxy_http_server livenetwork_proxy_http_username livenetwork_proxy_http_password	[設定] タブ
reporting_db_databasename reporting_db_drivername reporting_db_server reporting_db_port reporting_db_username reporting_db_password	[データベース] タブ

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、Enterprise Manager をホストする 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 Enterprise Manager をホストする 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 Enterprise Manager をホストする Server に転送します。
4. Enterprise Manager をホストする 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。150 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、161 ページの 表 20 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。Enterprise Manager 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、Enterprise Manager 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、Enterprise Manager 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。

- [設定] タブの設定ページの下の [HP 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、143 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。

   a **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。

> Enterprise Manager 内の Live Network 設定ページの [データベース] タブ上にある [レポート データベース] の設定および [Configuration Server] の情報が正しくない場合、このプロセスは機能しません。

これには、次の 2 つの方法があります。

— **メソッド 1:** 製品名 Enterprise Manager

a **[設定]** 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、53 ページの「HP Live Network の設定」を参照してください。

— **メソッド 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、160 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。

セキュリティと適用状況の管理に関する詳細情報

次のセクションには、Enterprise Manager でのセキュリティと適用状況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 173 ページ
- レポートの使用 233 ページ
- HP Live Network の設定 53 ページ

セキュリティと適用状況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

6 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。この章のは、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

Enterprise Manager 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。

- 180 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。
- 186 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。
- 205 ページの「適用状況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。
- 215 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。
- 224 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 23　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ています。

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、64 ページの「ダッシュボードの設定」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、Reporting Server によりレポートが表示されます。

- HPCA レポートからの情報が、ダッシュボードに表示されます。これらのレポートを提供できるよう Reporting Server を正しく設定する必要があります。Core および Satellite のインストールでは、自動的に行われます。CAE インストールを使用している場合、Oracle または SQL Server 前提条件スクリプトを実行する必要があります (『Reporting Server ガイド』を参照)。

  またレポートについても、Enterprise Manager で有効にしておく必要があります。51 ページの「Reporting Server の統合」を参照してください。

- ダッシュボードでデータを表示するには、Reporting Server で次のレポート パックを有効にする必要があります。パッチ管理、インベントリ管理、脆弱性管理、適用状況管理、セキュリティ ツール管理。詳細については、『Reporting Server ガイド』を参照してください。

- Patch Manager からの情報が、パッチ管理ダッシュボードに表示されます。パッチ管理ダッシュボードでデータを表示するには、Patch Manager および Inventory Manager の両方が正しく設定され、機能している必要があります。詳細については、『Patch Manager ガイド』および『Inventory Manager ガイド』を参照してください。

- Patch Manager 機能は、Patch Manager のライセンスを購入されたお客様、Patch Manager を含むバンドルまたはスイートを購入されたお客様のみがご利用できます。

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 9　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。詳細については、『Reporting Server ガイド』を参照してください。

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 24　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。
	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。 Enterprise Manager 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、Reporting Server の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。

表 24　ダッシュボード ペインのアクション

アイコン	説明
	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 10　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に Enterprise Manager サインインした場合にも適用されます。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、明示的に削除しない限り保存されます。詳細については、263 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 Enterprise Manager 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。詳細については、260 ページの「F5 キーを使用してページをリフレッシュできない」を参照してください。

一部のグリッド表示では、特定のパラメータについての前回のスキャン以降の傾向が、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 25　トレンド インジケータ

アイコン	色	方向	説明
	赤	上向き	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	上向き	パラメータが増加しています。傾向は良好です。
	赤	下向き	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	下向き	パラメータが減少しています。傾向は良好です。

たとえば、187 ページの「脆弱性の重大度別影響 (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、273 ページの「カスタム ダッシュボード フィルタとデバイスの追加」を参照してください。

デバイスを適用するには、コンソールの左上隅の [デバイス] 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 189 ページ
- 適用状況評価履歴 209 ページ
- Microsoft セキュリティ ブリテン 229 ページ
- HP Live Network アナウンスメント 196 ページ

デバイスを選択すると、Enterprise Manager 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、273 ページの「カスタム ダッシュボード フィルタとデバイスの追加」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。オペレーション 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 181 ページ

サービス イベント 182 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 184 ページ

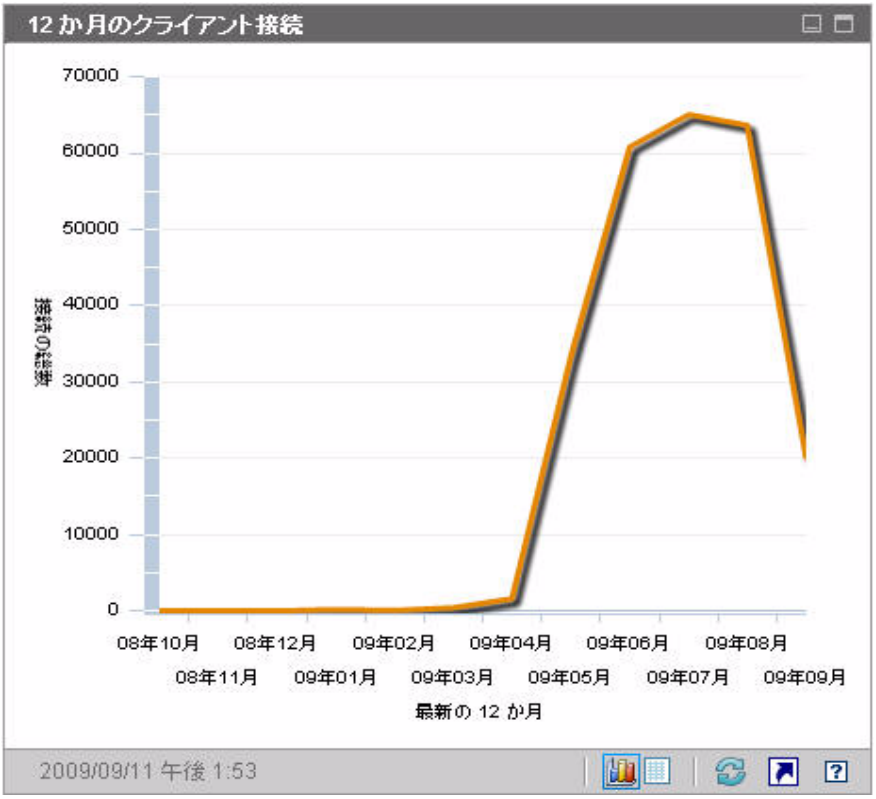
デフォルトではこれらのペインがすべて表示されます。ダッシュボードでは、これらの任意のペインの表示 / 非表示を切り替えることができます。64 ページの「ダッシュボードの設定」を参照してください。

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

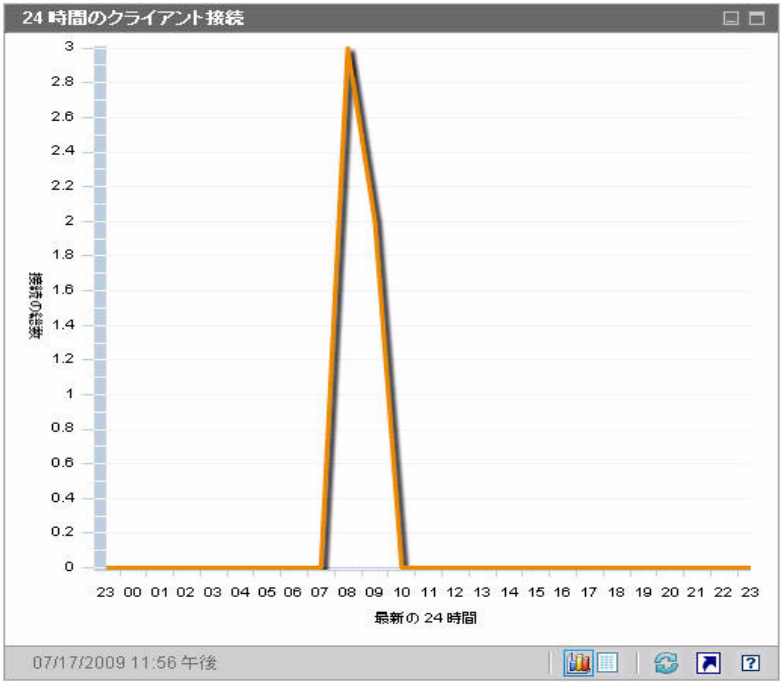
このペインのグラフ表示には、過去 12 か月 (エグゼクティブ ビュー) または 24 時間 (オペレーション ビュー) に発生した HPCA Agent クライアント接続の数が表示されます。データ ポイントの上にカーソルを置くと、その月または時間の合計接続数が表示されます。

図 11　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 12　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。詳細については、『Reporting Server ガイド』を参照してください。

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。

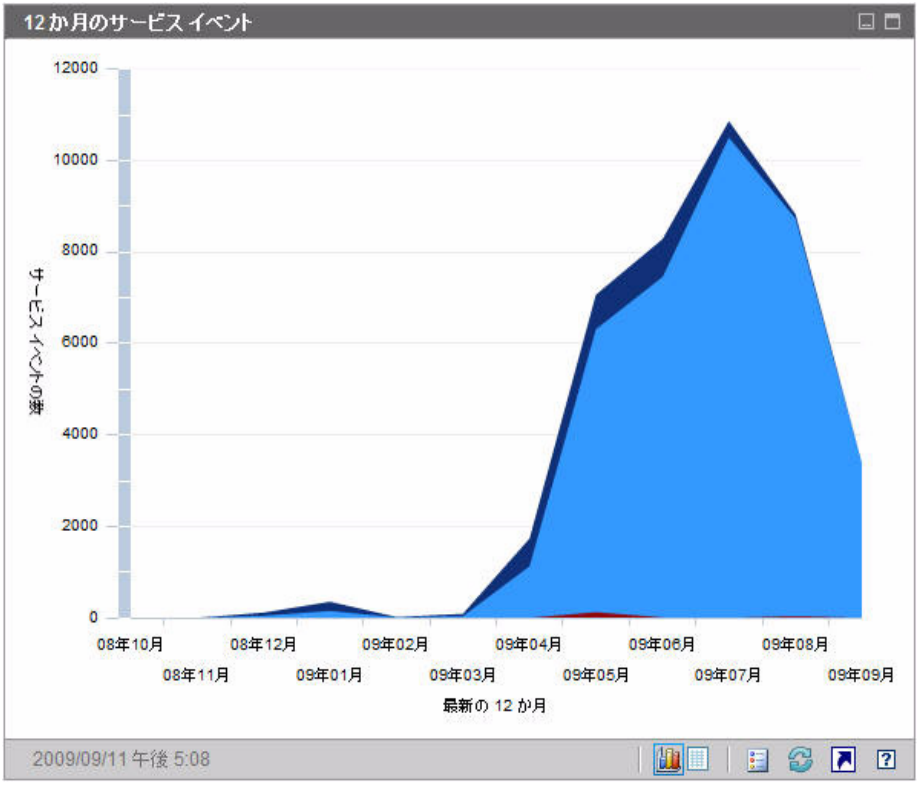
サービス イベント

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

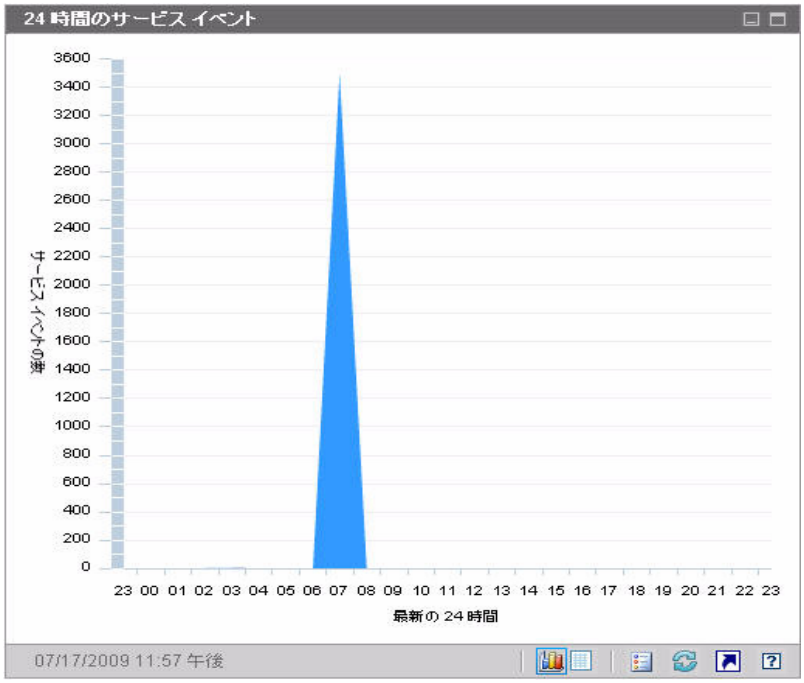
データ ポイントの上にカーソルを置くと、特定の月または時間に完了したサービス イベント数が表示されます。

図 13　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 14　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。詳細については、『Reporting Server ガイド』を参照してください。

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

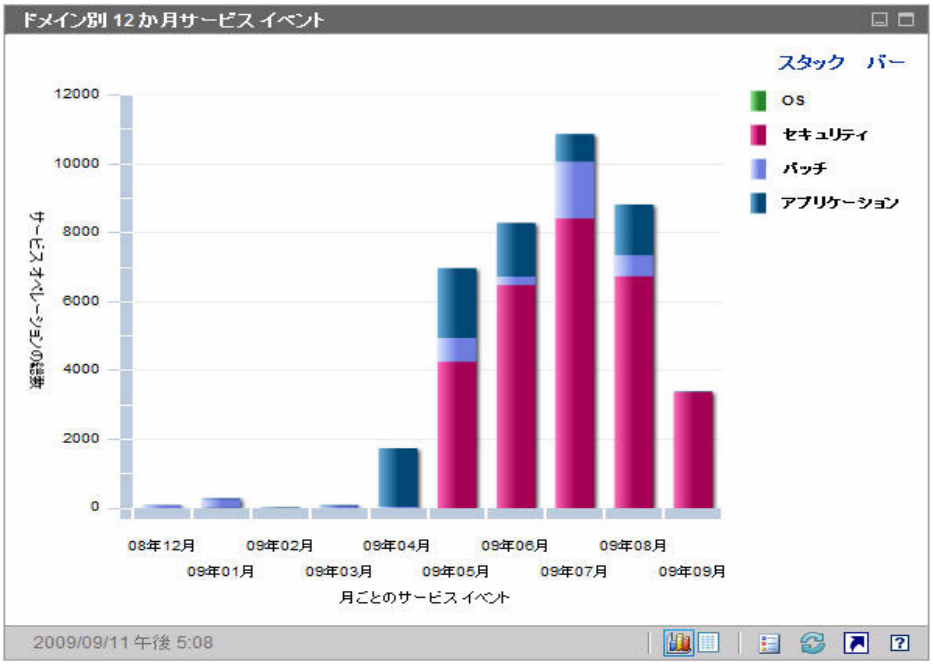
このペインのグラフ表示では、過去 12 か月の各月に HPCA により実行された次のサービスの数が表示されます。

- 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 15　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、133 ページの「セキュリティと適用状況の管理」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 26　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。

- 脆弱性の重大度別影響 (円グラフ) 187 ページ
- 重大度別にした脆弱性の影響 (棒グラフ) 197 ページ
- 脆弱性の影響 191 ページ
- 脆弱性履歴の評価 189 ページ

オペレーション 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 196 ページ
- 最も脆弱性の高いデバイス 199 ページ
- 最も脆弱性の高いサブネット 200 ページ
- 脆弱性のトップ 202 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。64 ページの「ダッシュボードの設定」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。

脆弱性の重大度別影響 (円グラフ)

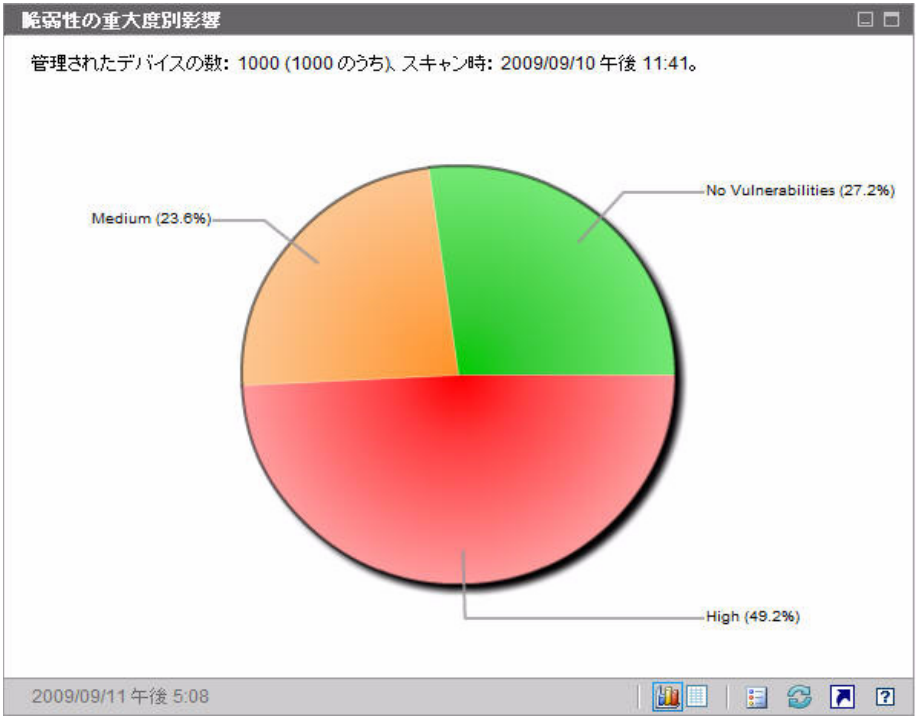
このペインのグラフ表示では、企業内のスキャン済みデバイスの次の 5 種類のカテゴリ別のパーセンテージが表示されます。分類は、各デバイスで検出された最も高い重大度の脆弱性に基づいて行われます。

- 高 (赤)

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

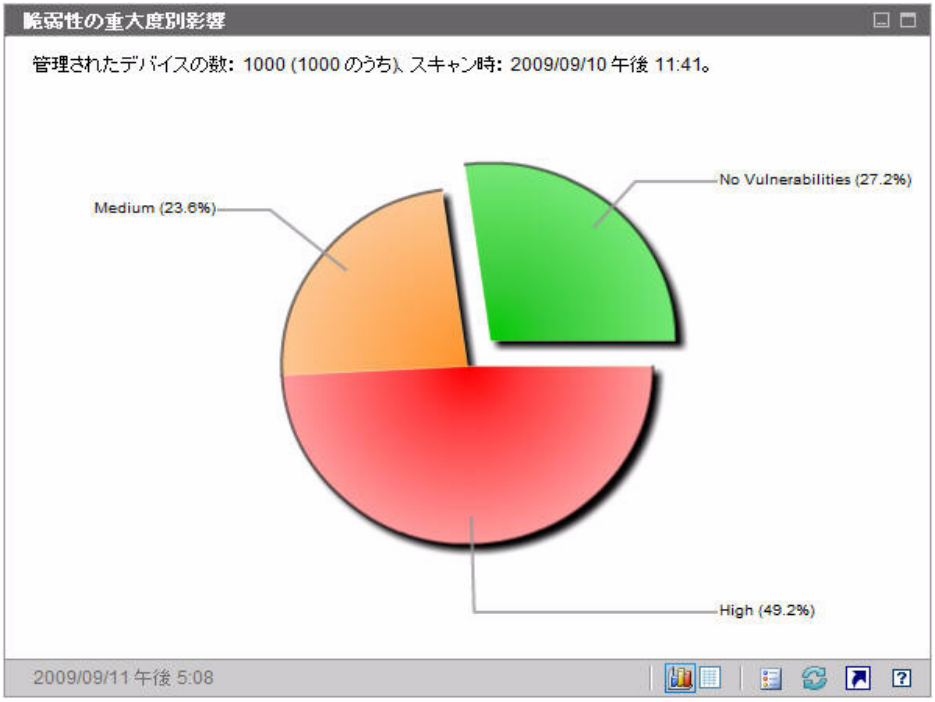
各重大度カテゴリのデバイス数を表示するには、円グラフの対応するセクタの上にカーソルを置きます。

図 16　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、Reporting Server により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 17　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 173 ページ

脆弱性管理ダッシュボード 186 ページ

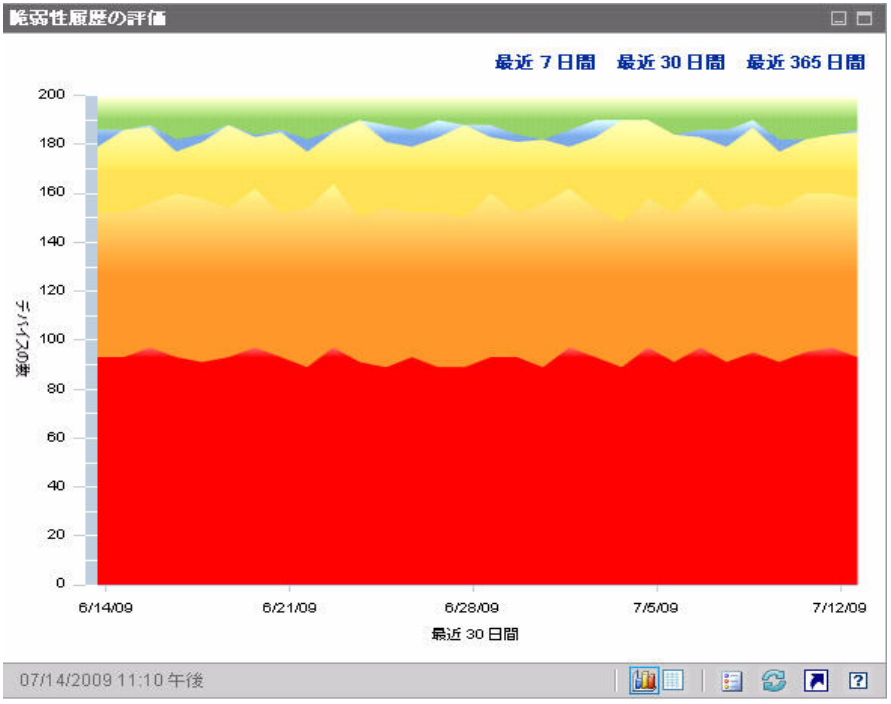
セキュリティと適用状況の管理 133 ページ

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。

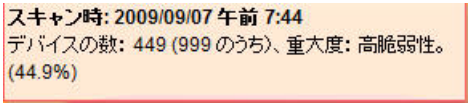
このペインのグラフ表示では、一定の期間における企業のリスク集計の平均が表示されます。垂直軸はデバイス数を表します。水平軸は時間を表します。過去 7 日、30 日、または 365 日のデータを表示できます。色分けされたそれぞれの領域は、各重大度カテゴリのデバイス数を表します。カテゴリは、高 (赤)、中 (オレンジ)、低 (黄)、脆弱性なし (緑) および不明 (青) で表示されます。

図 18　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 19　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 173 ページ

脆弱性管理ダッシュボード 186 ページ

セキュリティと適用状況の管理 133 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。円の色は脆弱性の重大度を示します。カテゴリは、高 (赤)、中 (オレンジ)、低 (黄)、不明 (青) で表示されます。

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。例：

- 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。

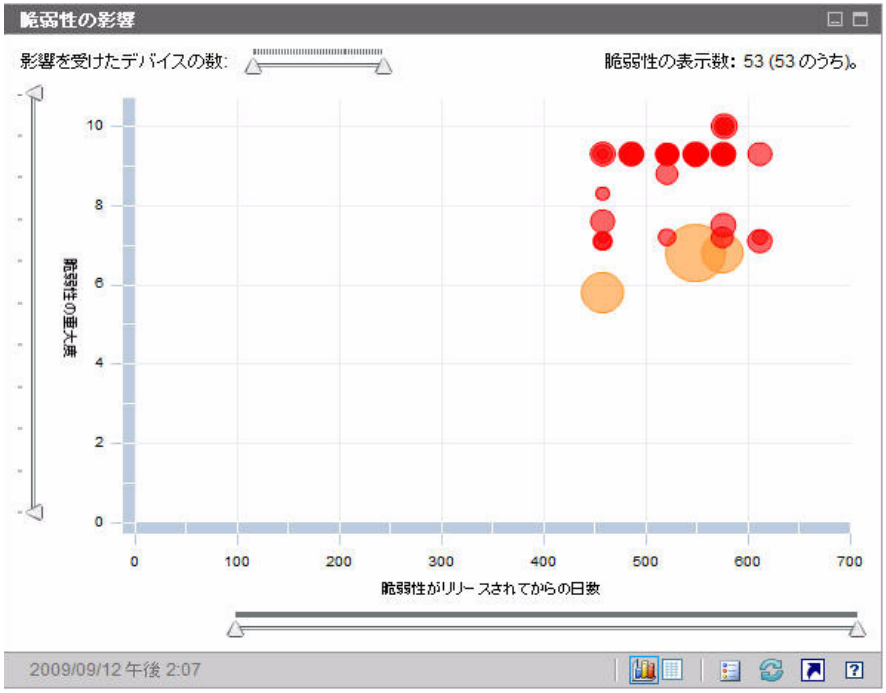
- グラフの左下部分に小さな黄色の円がある場合、少数のデバイスに影響を与え、NVD でパブリッシュされたのが比較的最近である重大度が低い問題の存在を表しています。
- 右上隅に赤い円がないグラフが理想的と言えます。これは、重大な脆弱性が迅速に処置されたことを示しています。

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

グラフ内の特定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、Reporting Server により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 20　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。

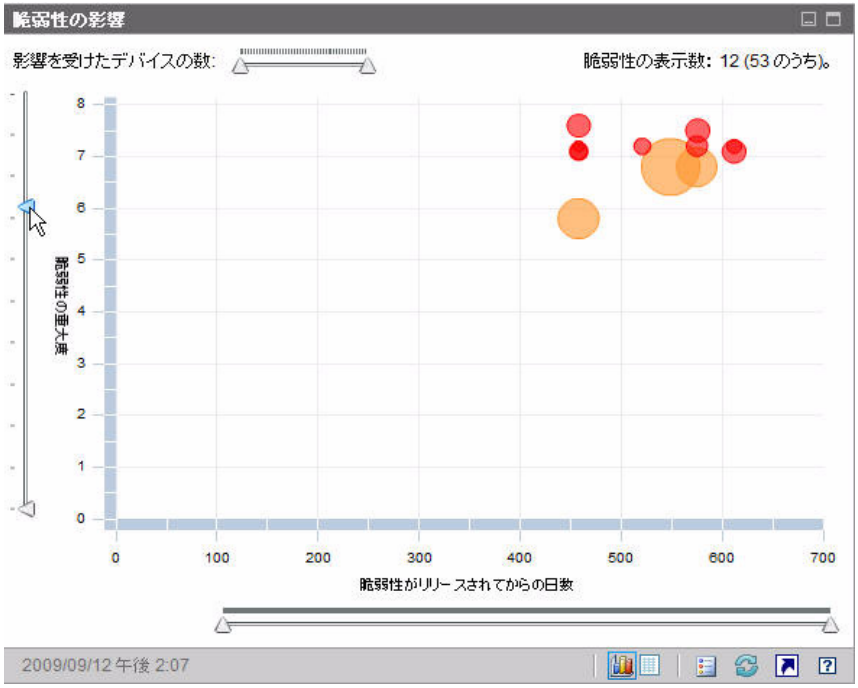
  デフォルトでは、表示される有効期間は 45 日間です。脆弱性管理ダッシュボードの設定時に、このデフォルト値を指定できます。64 ページの「ダッシュボードの設定」を参照してください。

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。

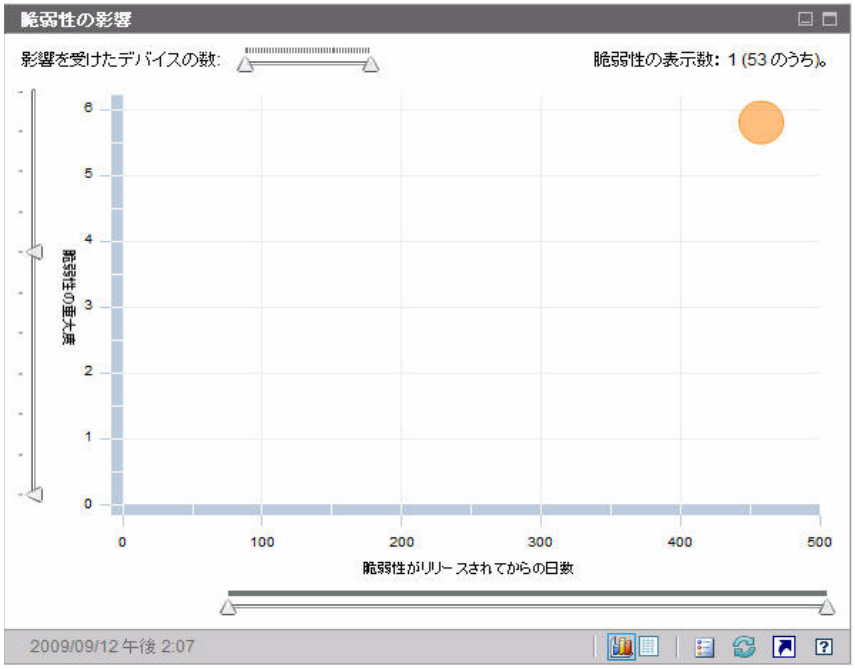
次の例では、CVSS ベースのスコアが 6 以上の脆弱性が表示されています。

図 21　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 22　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 173 ページ

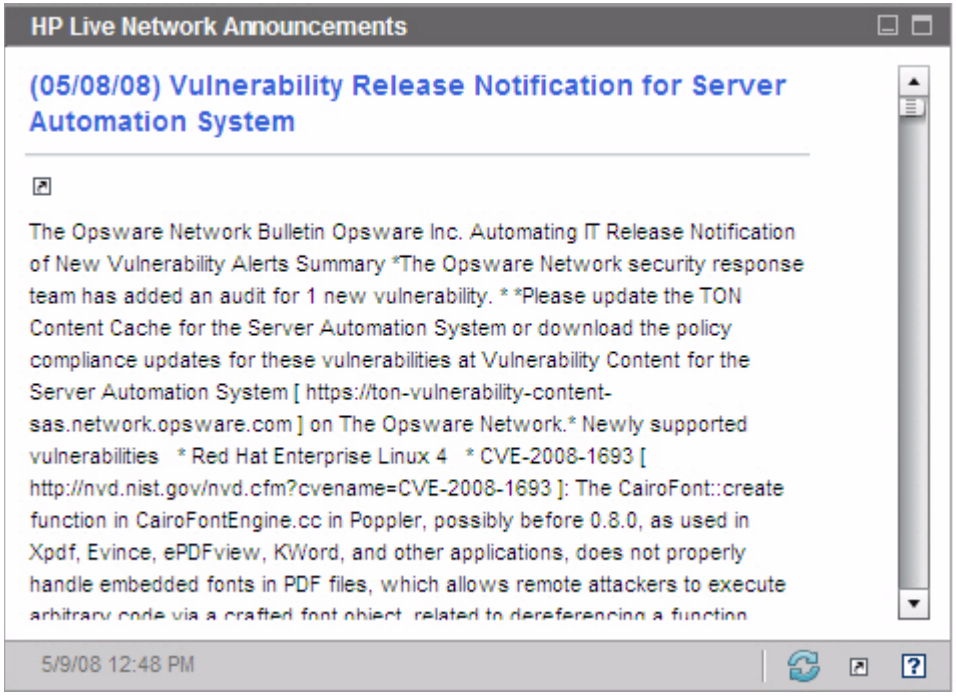
脆弱性管理ダッシュボード 186 ページ

セキュリティと適用状況の管理 133 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、64 ページの「ダッシュボードの設定」を参照してください。

図 23　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 (64 ページの「ダッシュボードの設定」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 (54 ページの「HP Live Network サーバーへの接続の設定」を参照)。

関連トピック：

ダッシュボードの使用 173 ページ

脆弱性管理ダッシュボード 186 ページ

セキュリティと適用状況の管理 133 ページ

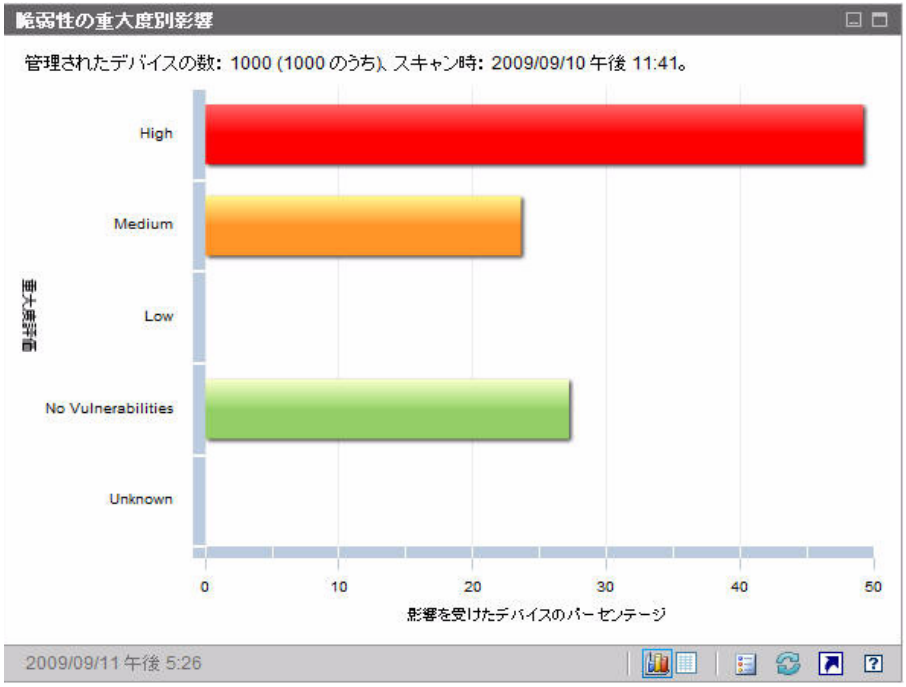
重大度別にした脆弱性の影響 (棒グラフ)

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 24　脆弱性の重大度別影響



グラフの色分けされた棒のいずれかをクリックすると、新しいブラウザ ウィンドウが開いて、Reporting Server により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 173 ページ

脆弱性管理ダッシュボード 186 ページ

セキュリティと適用状況の管理 133 ページ

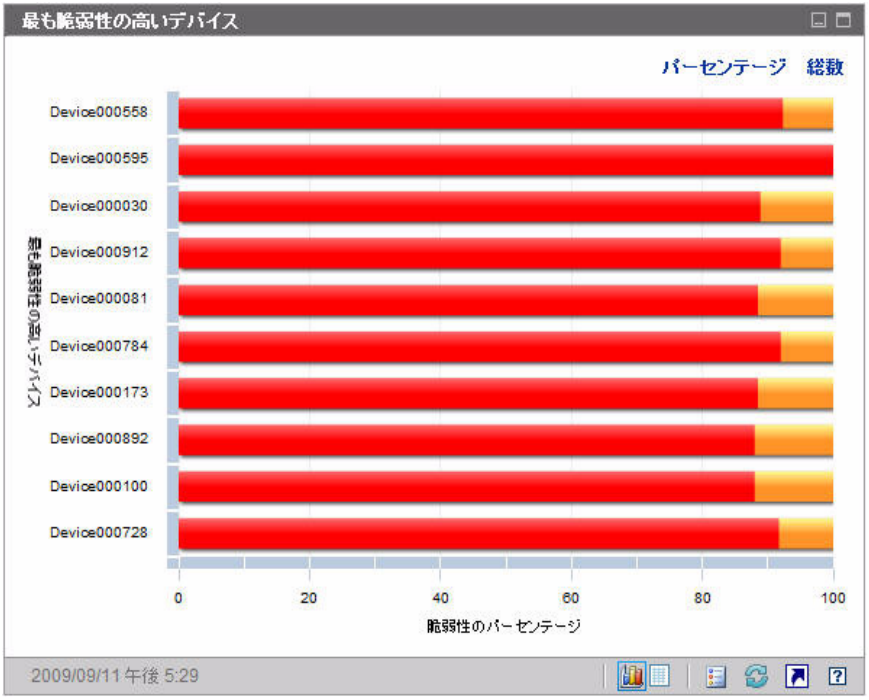
最も脆弱性の高いデバイス

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 25　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。

グラフの着色された棒のいずれかをクリックすると、新しいブラウザ ウィンドウが開いて、Reporting Server により該当デバイスの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 173 ページ

脆弱性管理ダッシュボード 186 ページ

セキュリティと適用状況の管理 133 ページ

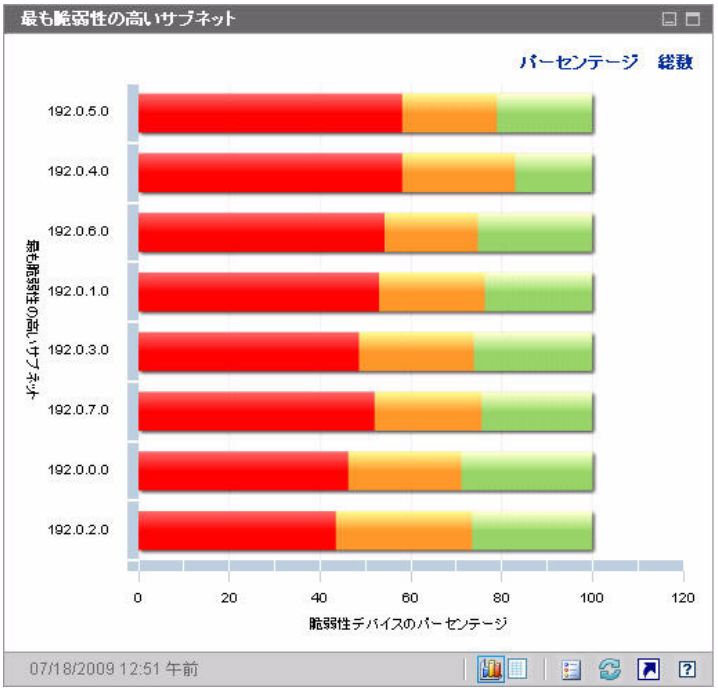
最も脆弱性の高いサブネット

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。各重大度カテゴリのデバイスのパーセンテージを示しています。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、64 ページの「ダッシュボードの設定」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 26　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サブネット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 173 ページ

脆弱性管理ダッシュボード 186 ページ

セキュリティと適用状況の管理 133 ページ

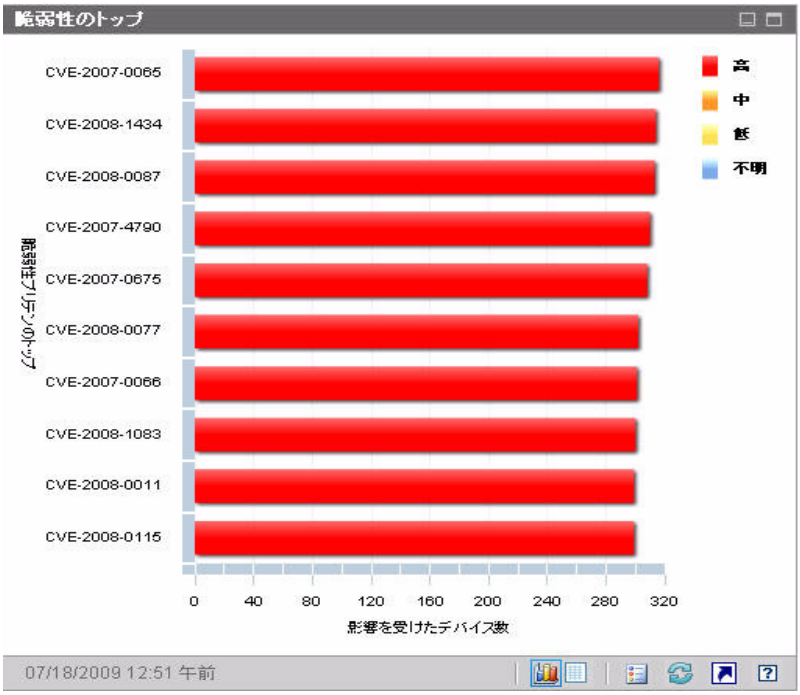
脆弱性のトップ

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)

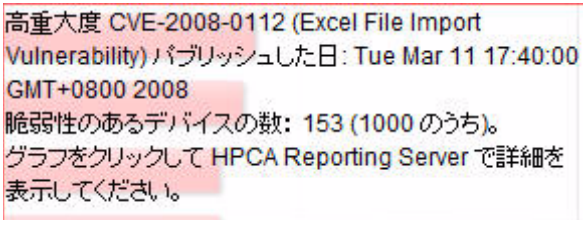
このグラフでは対数尺度を使用するため、特定の脆弱性が 1 つのデバイスのみに影響する場合、グラフ表示にはその脆弱性に関するデータが表示されません。これは、対数目盛りの既知の制限です。ただし、グリッド表示ではデータが表示されます。

図 27　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 28　ツール チップ



グラフの色分けされた棒のいずれかをクリックすると、新しいブラウザ ウィンドウが開いて、Reporting Server により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 173 ページ

脆弱性管理ダッシュボード 186 ページ

セキュリティと適用状況の管理 133 ページ

適用状況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、適用状況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。

適用状況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、133 ページの「セキュリティと適用状況の管理」を参照してください。

適用状況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 208 ページ
- 適用状況ステータス 206 ページ
- 適用状況評価履歴 209 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。

- 失敗頻度の高い SCAP 規則 211 ページ
- 失敗回数の多いデバイス (SCAP ルール別) 213 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、64 ページの「ダッシュボードの設定」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。

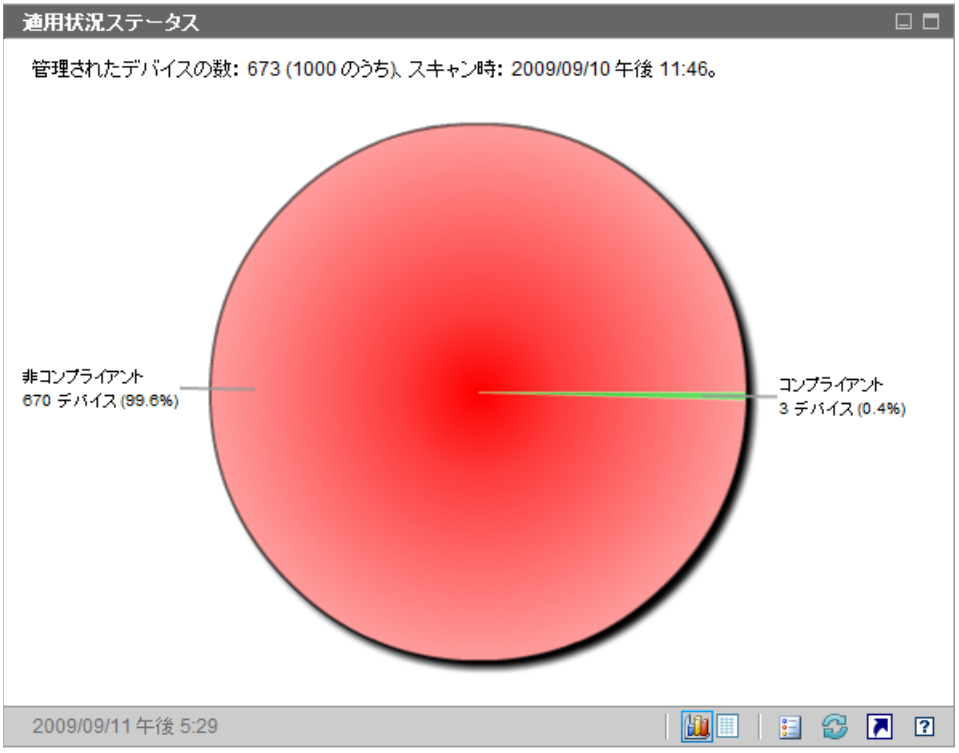
適用状況ステータス

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、準拠している、または準拠し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。

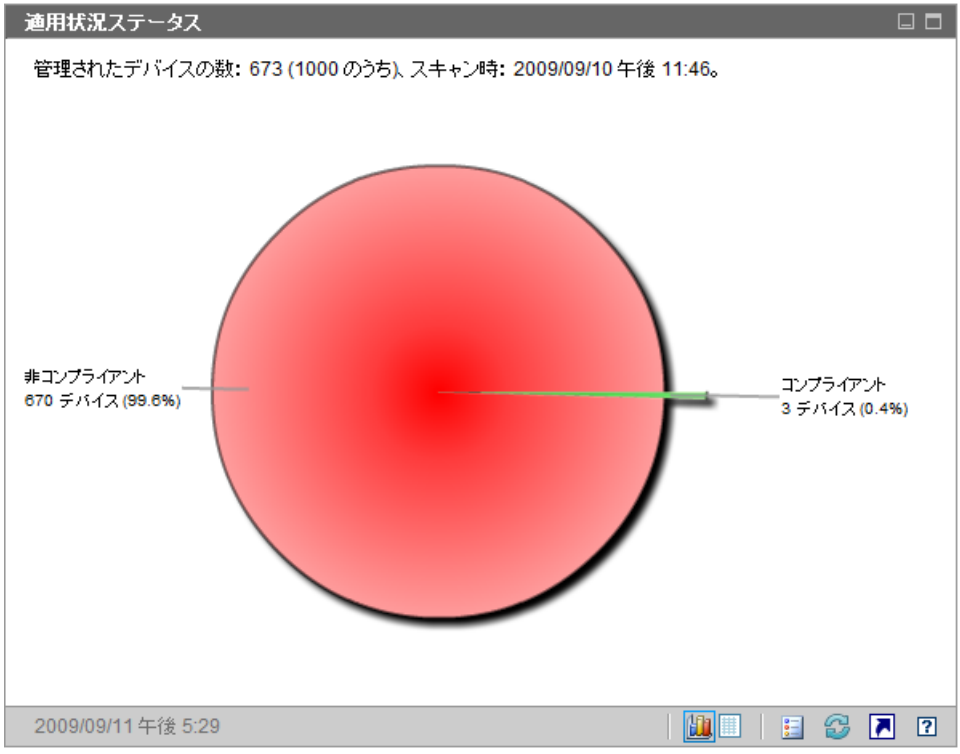
図 29　適用状況ステータス



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、Reporting Server により [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 30　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 173 ページ

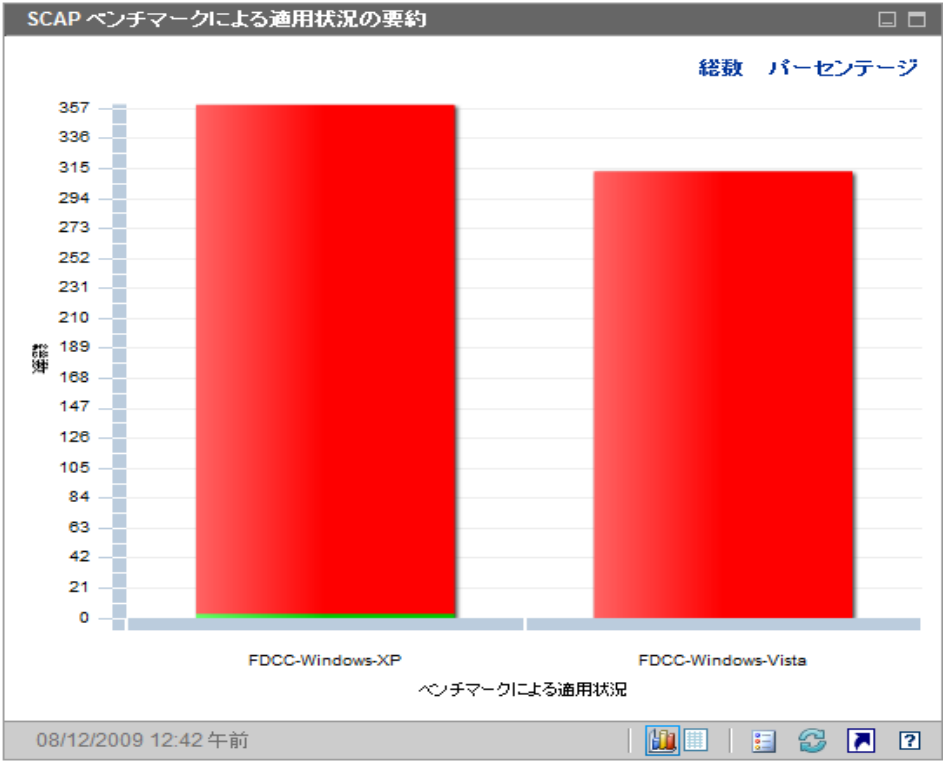
適用状況管理ダッシュボード 205 ページ

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 ベンチマークに準拠している、または準拠していない、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。

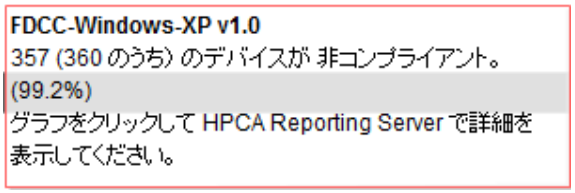
- コンプライアント デバイス (緑)
- 非コンプライアント デバイス (赤)

図 31　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 32　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、Reporting Server により [SCAP スキャン実施済みデバイス] 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、各ベンチマークに準拠している、または準拠し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 173 ページ

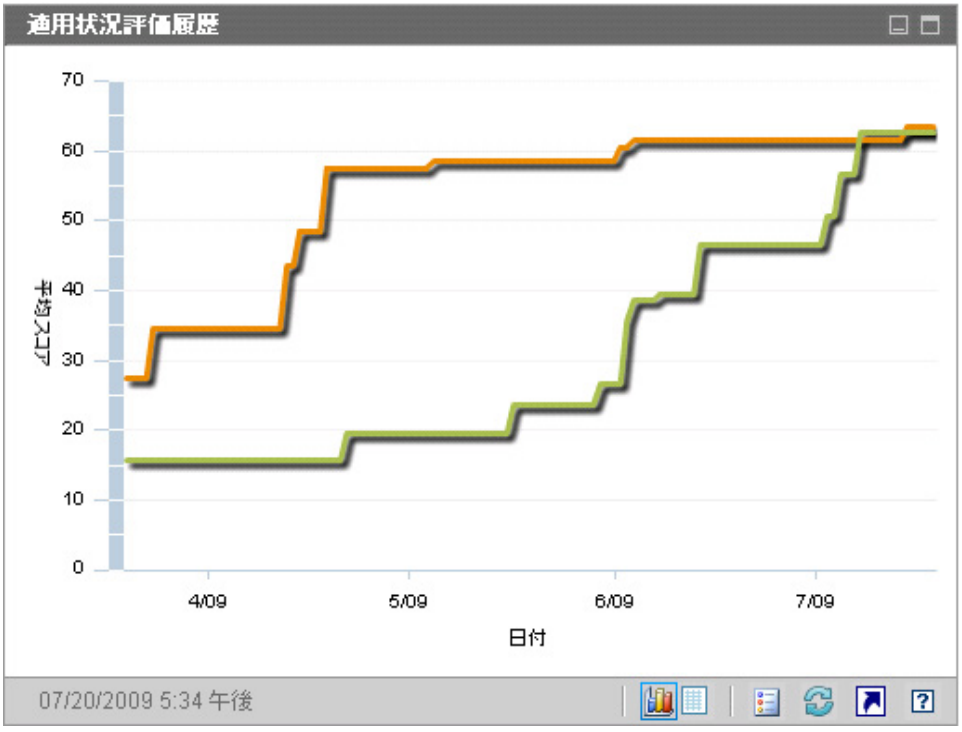
適用状況管理ダッシュボード 205 ページ

セキュリティと適用状況の管理 133 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 33　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。

- fdcc-ie-7 v1.1.0.0
- FDCC-Vista-Firewall v1.1.0.0
- FDCC-Windows-Vista v1.0
- FDCC-XP-Firewall v1.1.0.0
- FDCC-Windows-Vista v1.1.0.0
- fdcc-ie-7 v1.0
- FDCC-Windows-XP v1.1.0.0
- FDCC-Windows-XP v1.0

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、その日にそのベンチマークへ準拠し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 173 ページ

適用状況管理ダッシュボード 205 ページ

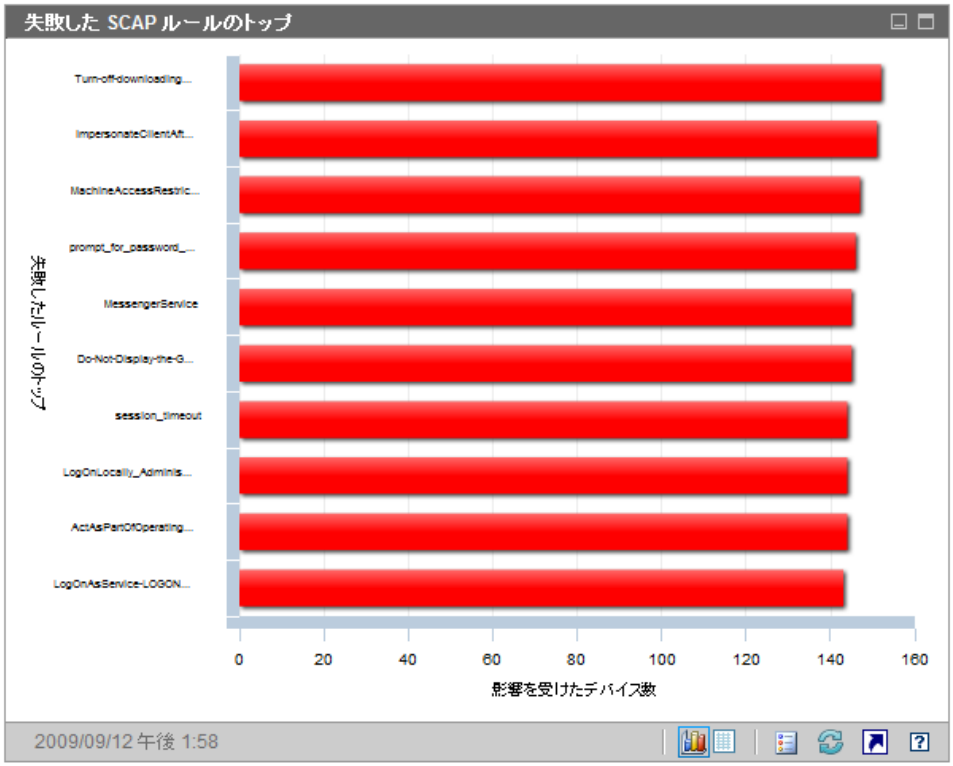
セキュリティと適用状況の管理 133 ページ

失敗頻度の高い 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 34　失敗頻度の高い SCAP 規則



グラフの色分けされた棒の 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、Reporting Server により [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 173 ページ

適用状況管理ダッシュボード 205 ページ

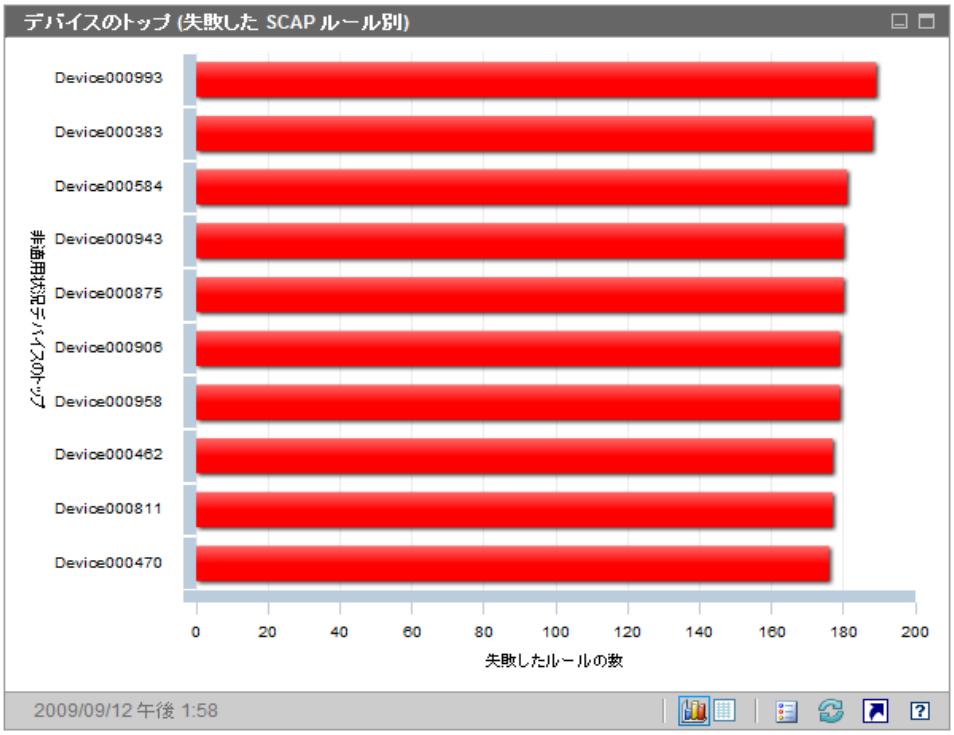
セキュリティと適用状況の管理 133 ページ

失敗回数の多いデバイス (SCAP ルール別)

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 35　失敗回数の多いデバイス (SCAP ルール別)



グラフの色分けされた棒のいずれかをクリックすると、新しいブラウザ ウィンドウが開いて、Reporting Server により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 スキャン実施済みデバイス] 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 スキャン実施済みデバイス] 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 173 ページ

適用状況管理ダッシュボード 205 ページ

セキュリティと適用状況の管理 133 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 ビューおよびオペレーション 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 216 ページ
- セキュリティ製品の概要 218 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 220 ページ
- 最新のセキュリティ製品のスキャン 221 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、64 ページの「ダッシュボードの設定」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 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、150 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 27　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 27　セキュリティ ツールの検出状態

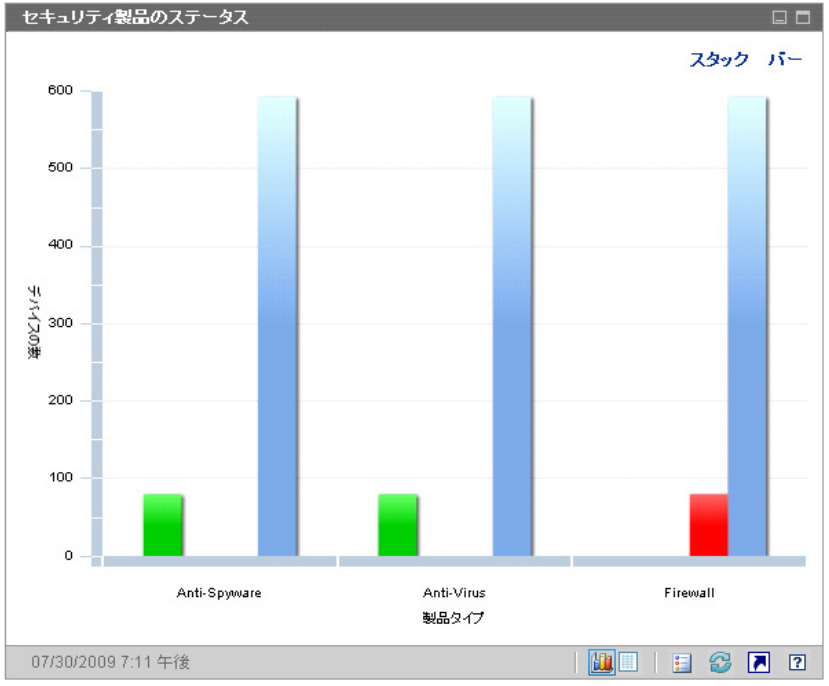
色		間隔
	赤	製品が検出されなかった。
	青	不明

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。

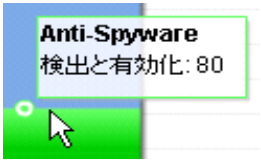
- HP Live Network セキュリティ ツール スキャナがこのツールを探したが、状態を判断できなかった。
- スキャナがこのツールを探したが、スキャン レコードが見つからなかった。
- スキャナがこのツールを探さなかった。

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 36　セキュリティ製品ステータス ペイン



マウス カーソルを色分けされた棒上に移動すると、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。



グラフの色分けされた棒のいずれかをクリックすると、新しいブラウザ ウィンドウが開いて、Reporting Server により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表示には、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 173 ページ

セキュリティ ツール管理ダッシュボード 215 ページ

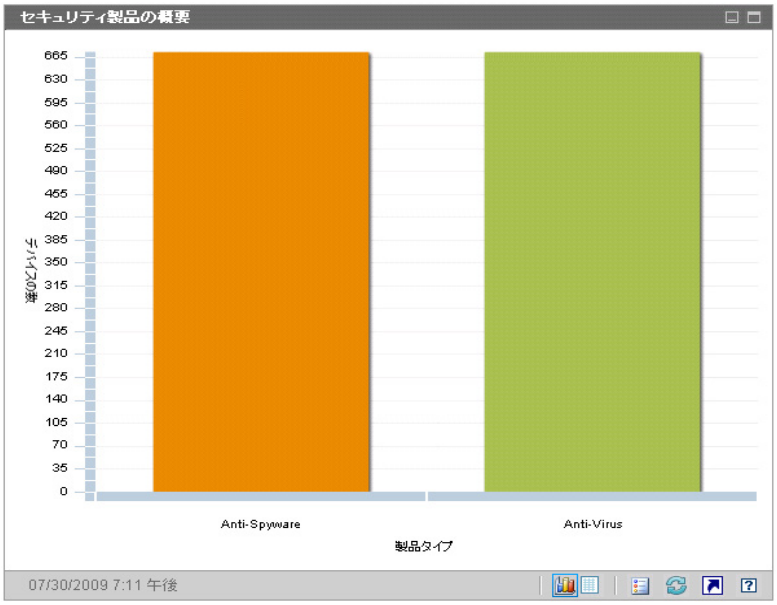
セキュリティと適用状況の管理 133 ページ

セキュリティ製品の概要

このペインのグラフ表示には、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 37　セキュリティ製品の要約ペイン



マウス カーソルを色分けされた棒上に移動すると、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。

グラフの色分けされたセグメントのいずれかをクリックすると、新しいブラウザ ウィンドウが開いて、Reporting Server により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表示には、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 173 ページ

セキュリティ ツール管理ダッシュボード 215 ページ

セキュリティと適用状況の管理 133 ページ

最新定義の更新

このペインのグラフ表示には、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。

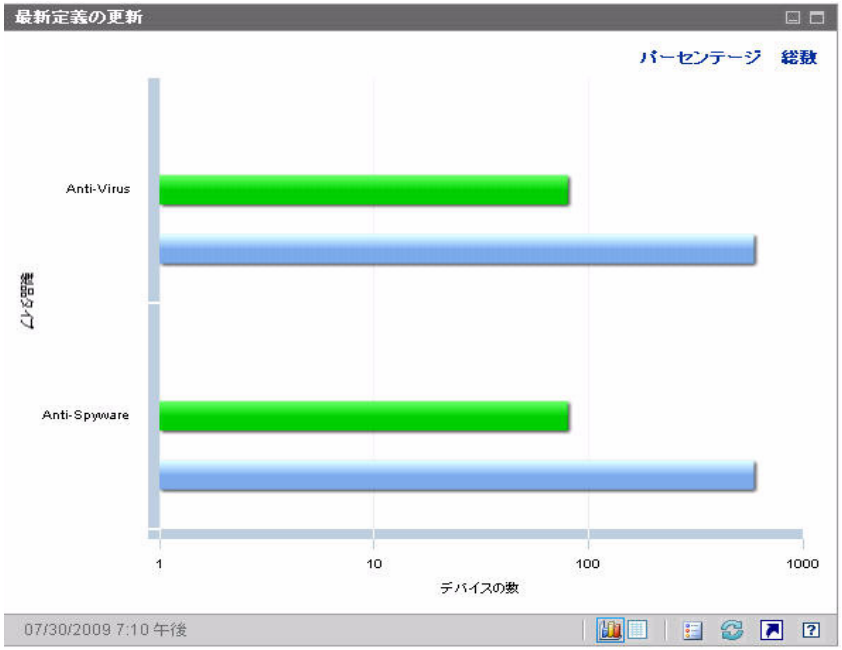
表 28　更新間隔

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。ただし、パーセンテージ表示およびグリッド表示ではデータが表示されます。

図 38　最新定義の更新



このペインのグリッド表示には、同じ情報がテーブル形式で表示されます。グリッド表示では、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。

グラフの色分けされた棒のいずれかをクリックすると、新しいブラウザ ウィンドウが開いて、Reporting Server により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 173 ページ

セキュリティ ツール管理ダッシュボード 215 ページ

セキュリティと適用状況の管理 133 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表示には、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。

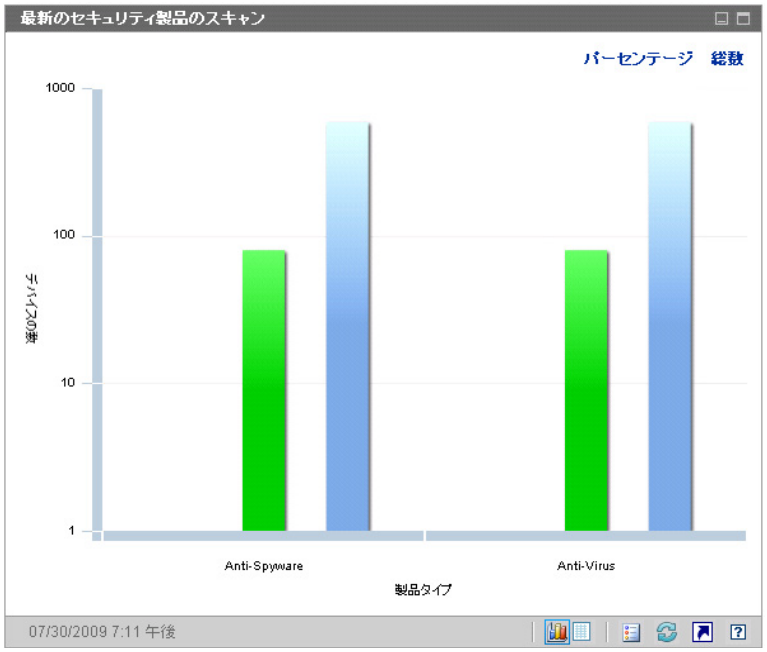
表 29　スキャン間隔

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。ただし、パーセンテージ表示およびグリッド表示ではデータが表示されます。

図 39　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表示には、同じ情報がテーブル形式で表示されます。グリッド表示では、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。

グラフの色分けされた棒のいずれかをクリックすると、新しいブラウザ ウィンドウが開いて、Reporting Server により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 173 ページ

セキュリティ ツール管理ダッシュボード 215 ページ

セキュリティと適用状況の管理 133 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。

デフォルトではこのダッシュボードが無効になっています。有効にする方法については、64 ページの「ダッシュボードの設定」を参照してください。

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) 225 ページ
- ブリテン別デバイス適用状況 227 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) 228 ページ
- Microsoft セキュリティ ブリテン 229 ページ
- 最も脆弱性の高い製品 230 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。64 ページの「ダッシュボードの設定」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。

Patch Manager から Reporting Server を通じて送られた情報が、パッチ脆弱性ダッシュボードに表示されます。詳細については、『Patch Manager ガイド』を参照してください。

このダッシュボードでデータを表示するには、次の項目を正しく設定する必要があります。

1. Reporting Server を設定する必要があります。詳細については、『Reporting Server ガイド』を参照してください。
2. Reporting Server でパッチ レポート パックを有効にする必要があります。詳細については、『Reporting Server ガイド』を参照してください。
3. レポート インテグレーションを有効にし、設定する必要があります。51 ページの「Reporting Server の統合」を参照してください。

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表示には、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。

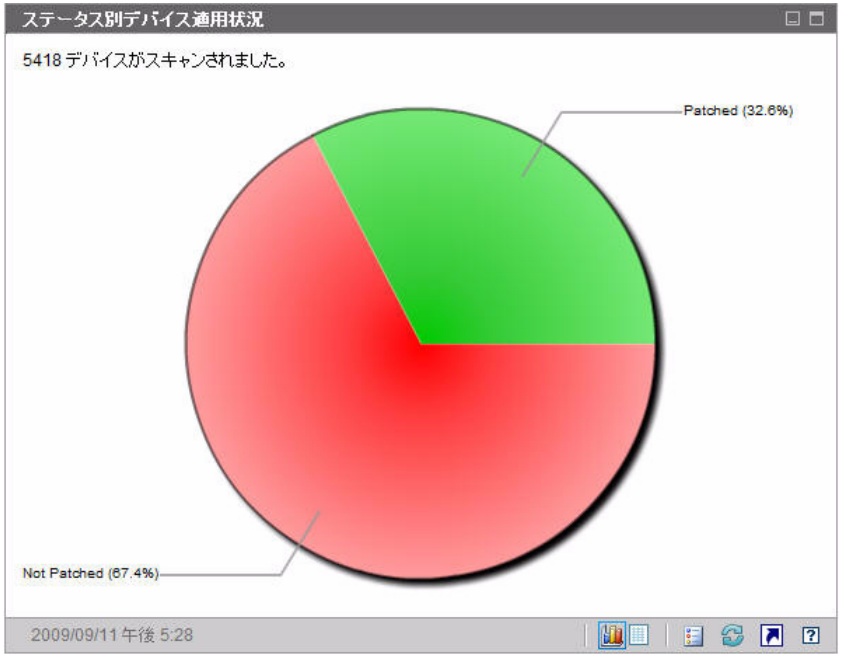
- パッチ適用済み (緑)
- パッチ未適用 (赤)

228 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、さらに詳しい情報が表示されます。

表 30　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 40　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。

円グラフ内の色分けされた扇形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いて、Reporting Server により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表示には、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。

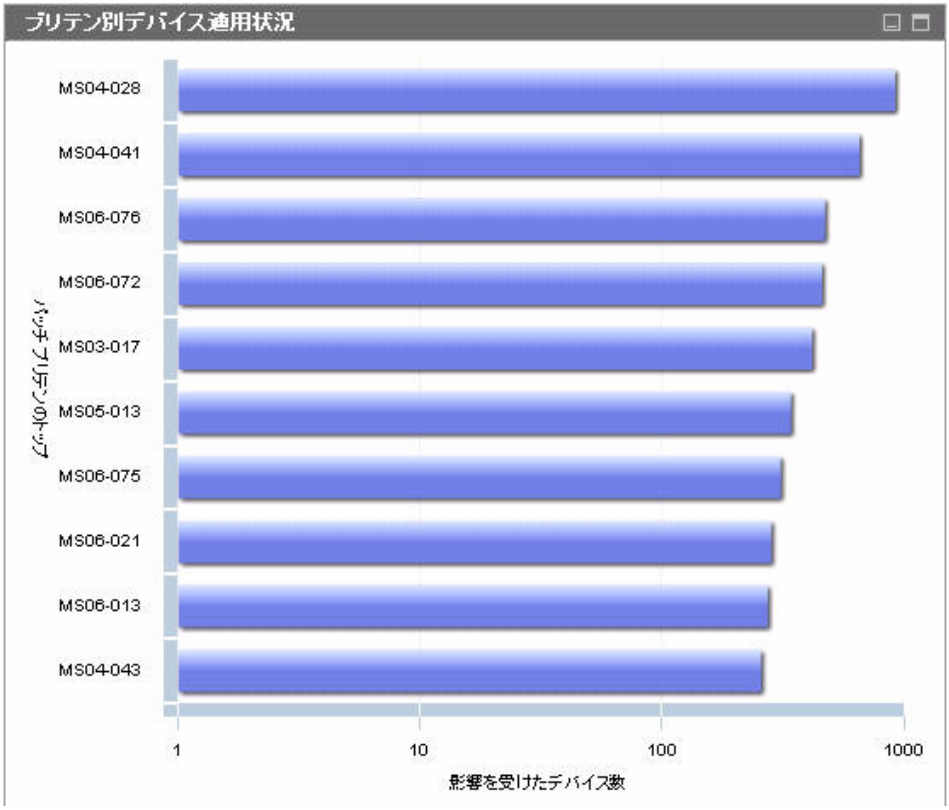
ブリテン別デバイス適用状況

このペインのグラフ表示には、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、グラフ表示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 41　ブリテン別デバイス適用状況



グラフの色分けされた棒のいずれかをクリックすると、新しいブラウザ ウィンドウが開いて、Reporting Server により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。

グリッド表示には、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 ID
- 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。

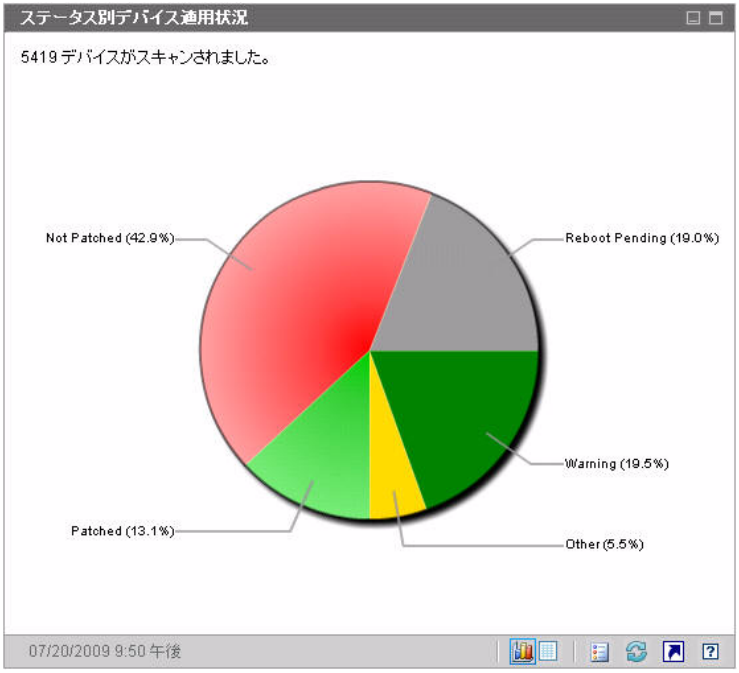
ステータス別デバイス適用状況 (オペレーション ビュー)

このペインのグラフ表示には、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 42　ステータス別デバイス適用状況 (オペレーション ビュー)



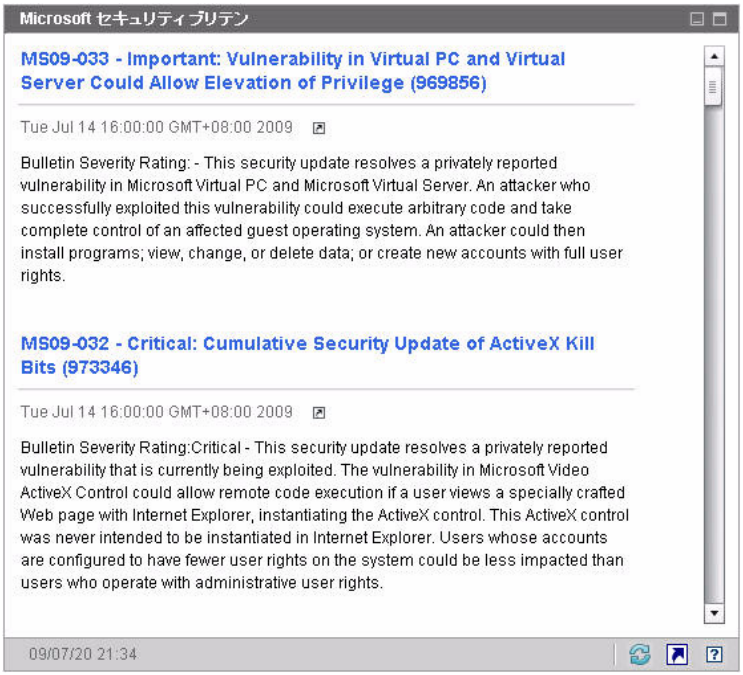
円グラフ内の色分けされた扇形のいずれかをクリックすると、新しいブラウザ ウィンドウが開いて、Reporting Server によりフィルタされたレポートが表示されます。レポートには、クリックした扇形に対応するパッチ適用状況ステータスのすべてのデバイスが表示されます。

グリッド表示には、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 (64 ページの「ダッシュボードの設定」を参照してください)。

図 43　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、64 ページの「ダッシュボードの設定」を参照してください。

このペインのグラフ表示には、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。例：

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

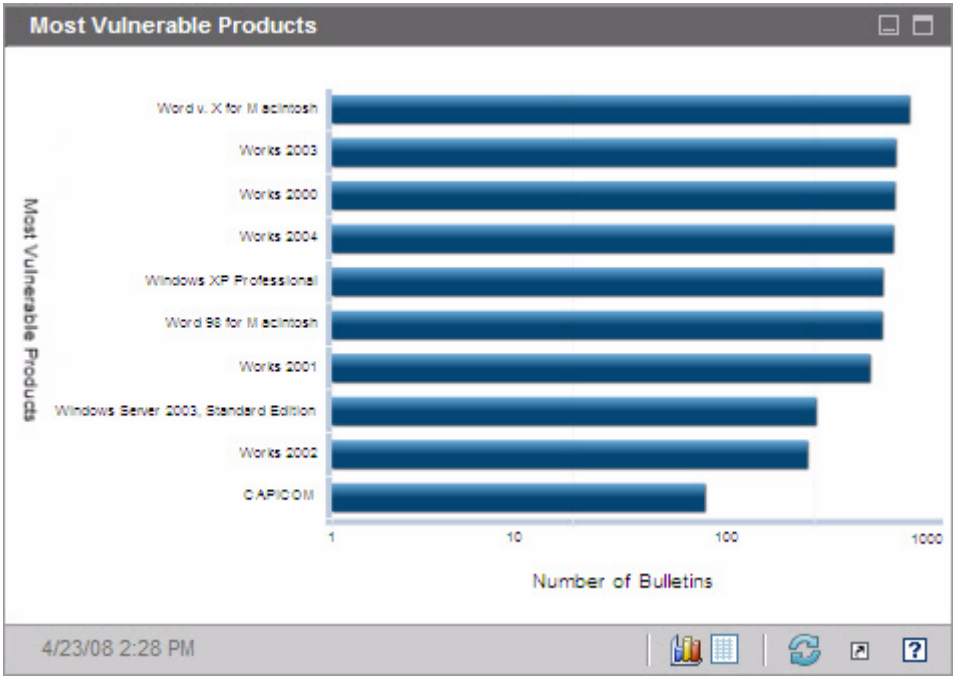
— 50 個の管理対象デバイスでそれらのパッチのうち 1 件のみを必要としている

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表示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 44　最も脆弱性の高い製品



グリッド表示には、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 – 特定製品のすべての適用可能なデバイスに対して、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。

7　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。この章のでは、次のトピックについて説明します。

レポートの概要

Enterprise Manager 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。

これらのレポートは Reporting Server が提供するもので、適切にインストールされ、設定する必要があります。またレポートインテグレーションは、Enterprise Manager で有効にする必要があります。51 ページの「Reporting Server の統合」を参照してください。

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 パックに関する詳細は、『Reporting Server ガイド』を参照してください。

[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)

従来の CAE インストールでは、[設定] タブでレポートを明示的に有効にする必要があります。[レポート] タブが表示されていない場合は、51 ページの「Reporting Server の統合」の手順に従います。

[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 31　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。
	Reporting Server からのデータをリフレッシュします。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。

表 31　レポートのアクション

アイコン	説明
	このレポートを印刷する。
	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。詳細については、『Reporting Server ガイド』を参照してください。

レポートのタイプ

Enterprise Manager 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 239 ページ
- 適用状況管理レポート 243 ページ
- インベントリ管理レポート 239 ページ
- パッチ管理レポート 240 ページ
- 脆弱性管理レポート 241 ページ
- セキュリティ ツール管理レポート 246 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、Enterprise Manager 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、Device Management on page 220 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、250 ページの「レポートのフィルタ」を参照してください。

表 32　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 33　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 33　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 34　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

Enterprise Manager で設定したように、これらのレポートは、Reporting Server により 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、157 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、250 ページの「レポートのフィルタ」を参照してください。

表 35　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 36　SCAP レポート

レポート名	説明
適合性の要約	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 37　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。

Enterprise Manager で設定したように、これらのレポートは、Reporting Server により 一部のレポートは、適用状況管理ダッシュボードからも使用できます。

詳細については、150 ページの「セキュリティと適用状況の管理の設定」を参照してください。

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。

Enterprise Manager で設定したように、セキュリティ ツール管理レポートは、Reporting Server により 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、159 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、250 ページの「レポートのフィルタ」を参照してください。

表 38　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 38　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 39　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 39　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 40　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

Enterprise Manager で設定したように、これらのレポートは、Reporting Server により 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。

詳細については、150 ページの「セキュリティと適用状況の管理の設定」を参照してください。

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 155 ページ
- 適用状況の失敗に関する情報の検索 157 ページ
- セキュリティ ツールに関する情報の検索 159 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。

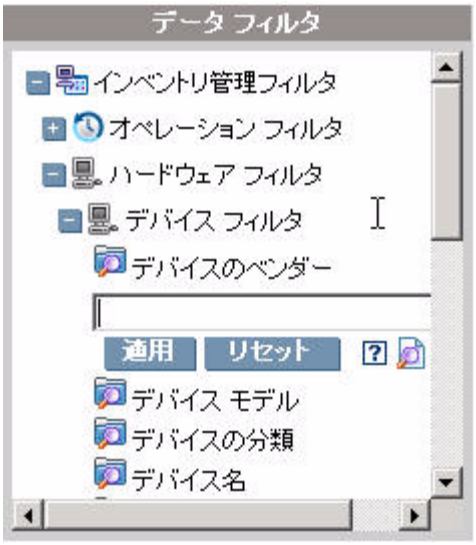
3 テキスト ボックスでフィルタ条件を指定するか、  (条件) ボタンをクリックしてリストから条件を選択します (表示された場合。すべてのフィルタでリストが表示されるとは限りません)。

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 41　特殊文字とワイルドカード

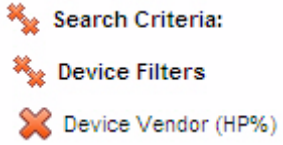
文字	機能	デバイスのベンダー フィルタの例	一致するレコード
* または %	特定のテキスト文字列を含むすべてのレコードに一致する	HP*	「HP」で始まるすべてのレコード
		%HP%	「HP」を含むすべてのレコード
? または or _	任意の 1 文字に一致にする	Not?book	「Not」で始まり「book」で終わるすべてのレコード
		Note_ook	「Note」で始まり「ook」で終わるすべてのレコード
!	フィルタを否定する	!HP*	「HP」で始まらないすべてのレコード

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で、「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 42　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 42　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。155 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 43　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 43　適用状況管理フィルタ

レポート	適用可能なフィルタ
適合性の要約	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 43　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。

8 トラブルシューティング

このセクションには、Enterprise Manager の使用中に遭遇する問題のトラブルシューティングに使用できる情報が含まれています。このセクションの各トピックでは、特定の問題について説明し、解決策または回避策を提示します。次の各領域について説明します。

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

Enterprise Manager 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 Enterprise Manager 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

Enterprise Manager 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 261 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 agent 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、90 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 または 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。64 ページの「ダッシュボードの設定」を参照してください。

ダッシュボード ペインはロードできません

このメッセージは、Reporting Server が統合されていない場合に表示されます。

解決策 :

51 ページの「Reporting Server の統合」を参照するか、HP のソフトウェア サポート担当者にお問い合わせください。

ダッシュボード ペインはロードできません – レポート クエリに失敗しました

このメッセージは、Reporting Server の URL が正しくない場合に表示されます。

解決策 :

51 ページの「Reporting Server の統合」を参照するか、HP のソフトウェア サポート担当者にお問い合わせください。

ダッシュボード ペインのロード状態が終了しない

Enterprise Manager が Reporting Server にアクセスしていて、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 Server 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、Reporting Server 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 44　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 Enterprise Manager 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。

セキュリティと適用状況の問題

次のトラブルシューティングのヒントは、セキュリティと適用状況の設定、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

HP Live Network 用にプロキシ サーバーが正しく設定されていないことが、この問題で最も可能性が高い原因と考えられます。Enterprise Manager 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] 設定ページの タブでプロキシ サーバーを指定する必要があります。プロキシ設定は、次の形式である必要があります。

`http|https://<servername>:<portNumber>`

ポート番号のほかに、`http` または `https` が必要です。例:

`http://web-proxy.mycompany.com:8088`

Enterprise Manager では、[設定] タブの **[Proxy Server]** 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、Reporting Server が統合されていないことを示しています。

解決策 :

詳細については、51 ページの「Reporting Server の統合」を参照するか、HPCA 管理者にお問い合わせください。

SQL サーバー接続エラー

`vms-server.log` または `vms-commandline.log` ファイルのいずれかに、文字列 `com.microsoft.sqlserver.jdbc.SQLServerException`、および SQL Server に接続できないことを示すテキストがメッセージに含まれている場合、Live Network 設定ページで指定された設定が間違っている可能性があります。

解決策 :

次の Live Network 設定の設定を確認してください。

- [データベース] タブの **[データベース サーバー]** は、レポート データベースが存在するシステムのホスト名である必要があります。例 :

  `mydbserver.mycompany.com`

  SQL Server のセットアップにデフォルトのデータベース インスタンス以外が使用されてる場合、そのインスタンスがサーバー名に追加されている必要があります。例 :

  `mydbserver.mycompany.com\HPCA`

  [データベース名] フィールドは、そのインスタンスの特定のデータベース名が反映されている必要があります。

- ただし、SQL Server インストールは、それ以外のスタティック ポート、またはダイナミック (特定されない) ポートを使用して設定されている可能性もあります。

SQL Server のポート設定を確認して、[データベース] タブの SQL Server ポートの情報を最新のものにしてください。SQL Server がダイナミック ポートを使用している場合、Live Network レポート データベースのポートを空白に設定します。

- SQL Server の認証設定を確認します。HPCA Core の Enterprise Manager から HPCA データベースに接続する場合、SQL Server 認証を使用する必要があります。このような場合、Windows 認証はサポートされません。SQL Server の認証設定を変更する場合、必ず Live Network データベース設定の設定を適切に更新してください。

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 Enterprise Manager 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://ReportingHost:/reportingserver/setup.tcl`

   ここで、`ReportingHost` は Reporting Server 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、20 分は 1200 秒とします。
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

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 Server] 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 Server 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。

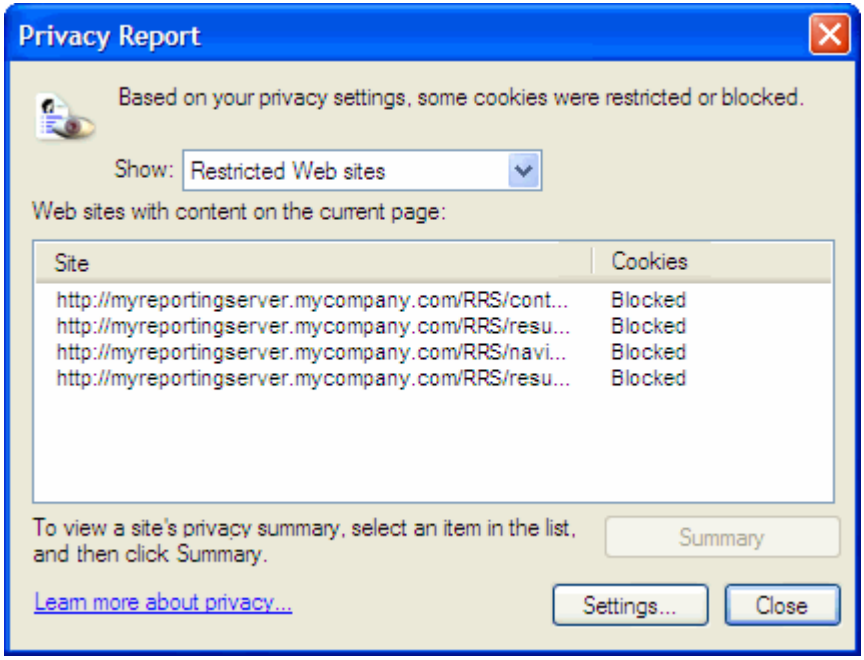
この動作は、Windows 2003 Server プラットフォーム上の Internet Explorer 6 および 7 で最も多く見られます。また、すべてのサポート対象プラットフォームでも発生する可能性があります。

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 Enterprise Manager 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 Enterprise Manager 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、Enterprise Manager 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。

CAE インストール：C:\Program Files\HP\HP BTO Software\CM-EC\tomcat

Core および Satellite: C:\Program Files\Hewlett-Packard\HPCA\tomcat

Console.properties ファイルを変更した後は、必ず HPCA Enterprise Manager 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、Enterprise Manager のパフォーマンスに悪影響を与える場合があります。

9 カスタム ダッシュボード フィルタとデバイスの追加

この付録では、Enterprise Manager でカスタム ダッシュボード フィルタとデバイスを使用できるようにする方法を説明します。

フィルタおよびデバイスは、Enterprise Manager で使用できるように、次のファイル内で設定されます。

`<InstallDir>\CM-EC\tomcat\webapps\em\WEB-INF\Console.properties`

HPCA Core のインストール当初は、このファイル内に設定がほとんど入っていません。しかし、コンソール設定を変更および保存した後、ファイルには非常に多くの情報が含まれます。

ダッシュボード フィルタとデバイスの使用についての詳細は、173 ページの「ダッシュボードの使用」を参照してください。

フィルタの追加

Enterprise Manager に任意の数のカスタム ダッシュボード フィルタを追加できます。

DEVICELIST フィルタから成るダッシュボードフィルタは `rim.kit` レポート パック内に実装されます。HPCA レポート パック内にフィルタを作成するのは高度なタスクです。この方法が分からない場合は、HP Software Support の営業担当にお問い合わせください。

カスタムのフィルタを追加するには

1 カスタマイズ可能な DEVICELIST フィルタを RIM レポート パック内に実装します。これに必要な手順は 2 つです。

   a フィルタを作成します。

b Oracle および SQL サーバーの両方にフィルタ SQL を作成します (DEVICELIST フィルタが利用可能であることを確認します)。

2 テキスト エディタで次のファイルを開きます。

<*InstallDir*>\CM-EC\tomcat\webapps\em\WEB-INF\Console.properties

3 次の形式で、新しいフィルタ名と必要な任意のパラメータ値を追加します。

```
global_filter_N_displayname=displayName
global_filter_N_filter=my_custom.filter
```

この場合、displayName はダッシュボードの右上の角のドロップ ダウン リスト内に表示されるフィルタ名、N は以下の利用可能な連続した整数です。

例 :

```
global_filter_2_displayname=Blades
global_filter_2_filter=blades_only.filter
```

4 Console.properties ファイルを保存します。

5 次のサービスを再起動します。

HP Client Automation Enterprise Manager

6 Enterprise Manager を再起動し、ドロップ ダウン メニューで新しいフィルタが利用可能になっていることを確認します。

デバイスの追加

Enterprise Manager には、デフォルトで 3 種類のダッシュボード デバイスがあります。

- グローバル
- モバイル
- 仮想

最大 2 つのカスタム ダッシュボード デバイスを追加することができます。また、お好みに応じて、デフォルトのデバイスを独自のカスタム デバイスと交換することができます。

カスタムのデバイスを追加するには

1 テキスト エディタで次のファイルを開きます。

`<InstallDir>\CM-EC\tomcat\webapps\em\WEB-INF\Console.properties`

2 次の形式で新しいデバイスに名前を追加します。

```
global_perspective_N_displayname=displayName
global_perspective_N_filter=filterName.filter
```

この場合、displayName は Enterprise Manager の左上の角に表示される [デバイス] ボックス内のフィルタ名、N は 4 または 5 のいずれかになります (デフォルトのデバイスと交換した場合の N は 1、2、3 のいずれかでも可能)。

例 :

```
global_perspective_4_displayname=MyCustom
global_perspective_4_filter=myfilter.filter
```

3 Console.properties ファイルを保存します。

4 次のサービスを再起動します。

HP Client Automation Enterprise Manager

5 Enterprise Manager を再起動し、[デバイス] ボックスで新しいデバイスが利用可能になっていることを確認します。

索引

て

は

ふ

へ

ほ

ゆ

り

れ

ろ