HP Client Automation

Core および Satellite

Enterprise Edition

Windows® および Linux オペレーティング システム用

ソフトウェア バージョン : 7.90

ユーザー ガイド

製造部品番号 : なし
ドキュメントのリリース日 : 2010 年 5 月
ソフトウェアのリリース日 : 2010 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

© Copyright 2009-2010 Hewlett-Packard Development Company, L.P.

商標

Apache Software License、Version 1.1
この製品には Apache Software Foundation (http://www.apache.org//) が開発したソフトウェアが含まれています。
Copyright © 1999-2001 The Apache Software Foundation. All rights reserved.

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。

PREBOOT EXECUTION ENVIRONMENT (PXE) SERVER
Copyright © 1996-1999 Intel Corporation.

TFTP サーバー
Copyright © 1983, 1993
The Regents of the University of California.

OpenLDAP
Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA.
Portions Copyright © 1992-1996 Regents of the University of Michigan.

OpenSSL License
Copyright © 1998-2001 The OpenSSLProject.

Original SSLeay License
Copyright © 1995-1998 Eric Young (eay@cryptsoft.com)

DHTML Calendar
Copyright Mihai Bazon, 2002, 2003

Lab PullParser
Copyright © 2002 The Trustees of Indiana University. All rights reserved
この製品には、Indiana University Extreme! Lab が開発したソフトウェアが含まれています。詳細については、http://www.extreme.indiana.edu/ を参照してください。

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、次を参照してください。

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

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

適切な製品サポート サービスを購読している場合にも、更新版や新版を受け取ることができます。詳細は、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。

表 1　　ドキュメントの変更点

章	バージョン	変更点
第 6 章、「Enterprise の管理」	7.80	アプリケーション利用状況データ収集フィルタの作成と管理、および利用状況収集エージェントの配布に関する手順が追加されました。215 ページの「利用状況収集フィルタ作成ウィザード」および 216 ページの「利用状況収集エージェントの配布」を参照してください。
第 6 章、「Enterprise の管理」	7.80	新しい詳細ポリシー管理機能が 157 ページの「ディレクトリ ポリシーの管理」に追加されました。
第 8 章、「オペレーション」	7.80	新しいエクスポート / インポート データ コンテンツ オプションが 264 ページの「ゲートウェイ設定」に追加されました。
第 8 章、「オペレーション」	7.80	手動での Live Network コンテンツのダウンロードの手順で、HPCA SCAP スキャナの名前が更新されました。527 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。

表 1　　ドキュメントの変更点

章	バージョン	変更点
第 9 章、「設定」	7.80	利用状況接続に新しいジョブ テンプレートが追加されました。310 ページの「サンプル テンプレート」を参照してください。
第 9 章、「設定」	7.80	アプリケーション利用状況データ収集が HPCA Enterprise で使用できるようになりました。372 ページの「利用状況管理」を参照してください。
第 9 章、「設定」	7.80	Suse 9、10、11 のベンダー フィードのイメージとテキストが変更されました。351 ページの「SuSE のフィード設定」を参照してください。
第 9 章、「設定」	7.80	Suse 11 が Novell に登録するための既存の要件に追加されました。360 ページの「SuSE 10 および SuSE 11 の登録要件」を参照してください。
第 9 章、「設定」	7.80	Suse 11 の取得名の形式の説明が追加されました。361 ページの「コンソールを使用して取得プロファイルを作成または編集するには」を参照してください。
第 9 章、「設定」	7.80	338 ページの「Download Manager オプション」は、分単位ではなく秒単位で遅延時間を指定するように修正されました。
第 9 章、「設定」	7.80	mib オプションとデフォルト値の変更についての説明がわかりやすく変更されました。340 ページの「Patch Manager のエージェント オプション」を参照してください。
第 9 章、「設定」	7.80	[設定] 領域に [インターネット アクセスの許可] が追加されました。342 ページの「設定」を参照してください。
第 9 章、「設定」	7.80	[エージェント オプション] 領域に [インストール済みのブリティンを管理する] が追加されました。340 ページの「Patch Manager のエージェント オプション」を参照してください。

表 1　　ドキュメントの変更点

章	バージョン	変更点
第 9 章、「設定」	7.80	[保存] ボタンでベンダー設定の保存と適用が両方とも行われるようになりました。345 ページの「ベンダーの設定」を参照してください。
第 9 章、「設定」	7.80	新しいブリティンの影響を受けるファイルのオプションについての説明が追加されました。364 ページの「Microsoft の設定」を参照してください。
第 8 章、「オペレーション」	7.90	設定可能なプロファイルがあるつソフトウェアの設定管理。276 ページの「設定管理」を参照してください。
第 9 章、「設定」	7.90	SuSE 10 SP 3 のサポート。
第 9 章、「設定」	7.90	パッチ ゲートウェイが Satellite Server でサポートされるようになりました。366 ページの「Satellite コンソールのパッチ管理」を参照してください。
第 9 章、「設定」	7.90	スマート カード認証。293 ページの「スマート カード認証」を参照してください。
第 4 章、「ダッシュボードの使用」 第 9 章、「設定」	7.90	137 ページの「HP Live Network Patch Manager アナウンスメント」のサポート。
第 6 章、「Enterprise の管理」	7.90	VDI でパッチ管理を効率的に行う方法に関する情報が追加されました。166 ページの「Virtual Desktop Infrastructure のポリシーの管理方法」を参照してください。

表 1　　ドキュメントの変更点

章	バージョン	変更点
第 7 章、「レポートの使用」	7.90	カテゴリ別の Application Management Profiles の新しいレポートが追加されました。225 ページの「設定管理レポート」を参照してください。
第 11 章、「メタデータを使用したパッチ管理」	7.90	パッチ メタデータの配布モデルは、デフォルトの配布モデルに変更されています。メタデータを使用したパッチ管理を参照してください。
第 12 章、「OS イメージの準備とキャプチャ」 第 13 章、「パブリッシュ」 第 10 章、「ウィザード」 付録 G、「Windows XP および Windows Server 2003 の OS イメージのキャプチャ」	7.9	実装された操作性の向上を反映して、OS イメージ キャプチャ、パブリッシュ、および配布プロセスに関する情報を再編成し、更新しました。

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

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

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

アクセス レベルに関する詳細については、次を参照してください。

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

目次

1 紹介

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

このマニュアルについて

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

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

HPCA のドキュメント

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

略語と変数

表 1　　このガイドで使われている略語

略語	定義
HPCA	HP Client Automation
Classic	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
Core および Satellite	1 つの Core Server と 0 以上の Satellite Server で構成される HPCA Enterprise 環境。すべての機能が Core Server または Satellite Server の一部としてインストールされます。
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	HPCA Server 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\Hewlett-Packard\CM`
		Core および Satellite インストールの場合 :
		`C:\Program Files\Hewlett-Packard\HPCA`

SystemDrive	HPCA Server のインストール先のドライブのドライブラベル	`C:`

このマニュアルは、ユーザーが HPCA Core インストールと Satellite インストールを使用していることを前提としています。
HPCA Classic インストールがある場合は、HPCA コンポーネントが使用するさまざまなファイルおよびフォルダへのパスが異なります。正しいパスについては、次のフォルダにある各コンポーネント ガイドを参照してください。
InstallDir`\Docs\Enterprise\Reference Library`

2 はじめに

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

この章のセクションでは、次の内容について説明します。

- さまざまな管理タスクや設定タスクを実行するために使用する HPCA Console。30 ページの「Web ベースの HPCA Console へのアクセス」を参照してください。
- HPCA 環境の管理を開始するために完了する必要のあるタスク。これには、設定手順や詳細情報の入手方法が含まれます。31 ページの「HPCA の実装」を参照してください。

Web ベースの HPCA Console へのアクセス

HPCA Server では、さまざまな管理タスクや設定タスクを実行できるコンソールを使用します。これらのタスクの詳細については、237 ページの「オペレーション」および 281 ページの「設定」を参照してください。

HPCA Console を起動するために使用できる方法には、次の 4 つがあります。以下が可能です。

- **[HP Client Automation Console]** デスクトップ アイコンをダブルクリックします。
- HPCA Server がインストールされたマシンで、Windows の **[スタート]** メニュー パスに移動します。
- 環境内の任意のデバイスで Microsoft® Internet Explorer® (バージョン 7.0 以上) または Mozilla Firefox (バージョン 2.0 以上) の Web ブラウザを開き、次の URL に移動します。

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

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

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

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

デフォルトのユーザー名とパスワードを変更する方法、およびコンソールへのアクセス権限リストにユーザーを追加する方法については、281 ページの「設定」を参照してください。

- スマート カードを挿入します。

  スマート カード認証は、Enterprise Core Server でのみ使用できます。

  使用環境内の任意のデバイスで Microsoft® Internet Explorer® (バージョン 7.0 以上) または Mozilla Firefox (バージョン 2.0 以上) の Web ブラウザを開き、次の URL に移動します。

  https://*HPCA_host***/**

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

[**スマート カードを使用したサインオン**] をクリックします。

[**スマート カードを使用したサインオン**] を表示するには、SSL を有効にしてから SSL を使用してログイン ページにアクセスする必要があります。正常にログインするには、293 ページの「スマート カード認証」を参照してください。

入力を求めるメッセージが表示されたら、Core Server トラストストアの信頼できる証明書に一致する証明書を選択します。これは、HPCA Console の SSL セクションを使用して設定できます。

入力を求めるメッセージが表示されたら、スマート カードの暗証番号を指定します。

重要

- ウィザードを実行したり警告を表示したりするときに、HPCA Console が追加のブラウザ インスタンスを開く場合があります。これらのウィザードや警告にアクセスするには、ブラウザのポップアップ ブロック設定で [許可されたサイト] に HPCA を指定します。
- セキュリティのため、HPCA では、20 分間操作を行わないと、自動的に現在のユーザーをログアウトさせます。コンソールの使用を続けるには、再度ログインする必要があります。
- コンソールの **[レポート]** セクションでグラフィカル レポートを表示するには、Java Runtime または Java Virtual Machine が必要です。Java は、**http://java.com/en/index.jsp** からインストールできます。
- **Windows 2003 Server**: Windows 2003 Server オペレーティング システムがインストールされたデバイスで HPCA にローカル アクセスできるようにするには、**ローカル エリア ネットワーク (LAN)** の設定で **[ローカル アドレスにはプロキシ サーバーを使用しない]** を有効にする必要があります。

HPCA の実装

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

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

- ダッシュボード
- 管理
- レポート
- オペレーション
- 設定

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

必須のタスク

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

1 **デバイスのインポート**：クライアント デバイスを HPCA 環境にインポートして、デバイスが HPCA Server に認識されるようにします。33 ページの「デバイスのインポート」を参照してください。

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

HPCA Agent の配布方法にはいくつかあります。これらの方法は、33 ページの「HPCA Agent の配布」で説明します。

3 **ポリシーの設定**：HPCA を使用して、クライアント デバイス上の HPCA Agent の「状態」を確立します。33 ページの「ポリシーの設定」を参照してください。

オプションのタスク

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

- 36 ページの「脆弱性の管理」
- 37 ページの「クライアント操作プロファイルの設定」
- 42 ページの「パッチ管理の設定」
- 44 ページの「オペレーティング システム イメージの配布」
- 46 ページの「アウトバンド管理の有効化」

デバイスのインポート

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

- [デバイス管理] の [一般] タブで、**[インポート]** をクリックしてデバイス インポート ウィザードを起動します (170 ページの「デバイスのインポート」を参照)。
- ウィザードの手順に従って、デバイスをインポートします。

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

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

HPCA Agent の配布

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

HPCA Agent は、エージェント配布ウィザードを使用してデバイスに配布されます (172 ページの「HPCA Agent の配布」を参照)。ウィザードが完了すると、エージェント配布ジョブが作成されます。

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

ポリシーの設定

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

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

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

内部ポリシーの設定

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

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

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

外部ポリシーの設定

ポリシー設定を既存の LDAP (または、その他の外部) ディレクトリに適用した後、HPCA 環境で使用できるようにすることができます。このサポートを有効にするための手順は、35 ページの「外部ポリシー ストアの実装」に記載されています。

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

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

外部ポリシー ストアの実装

外部ポリシー ストアのためのポリシーの設定は、デフォルトで LDAP ディレクトリに接続するように設定され、HPCA Agent で管理されたマシンの完全なドメイン名を使用してポリシーを管理します。別のパラメータを使用してポリシーを管理するには、LDAP_RESOLVE メソッドの ZMTHPRMS 属性を調整します。これについては、35 ページの「外部の LDAP ポリシー ストアを実装するには」で説明します。

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

外部の LDAP ポリシー ストアを実装するには

1 ポリシー サービスが、ポリシーに使用される外部のディレクトリ サービスに接続できるように Core を設定します。この方法については、288 ページの「ディレクトリ サービス アカウントを使用するには」を参照してください。

2 外部のディレクトリ サービスに接続するフルサービス Satellite を有効化および設定します。

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

   既存の LDAP をバックアップするためのコマンドは次のとおりです。

   LDIFDE -f *OutputFileName*

   外部のディレクトリ サービスを更新するためのコマンドは次のとおりです。

   LDIFDE -i -f HPCAExtensions.ldif -v

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

   詳細については、*Policy Server Guide* を参照してください。

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

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

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

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

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

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

Policy Server の設定に従い、[管理] タブを使用して、LDAP ポリシー ストア内のポリシー資格の追加、管理、およびクエリを実行します。

ポリシー解決の確認

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

1 [管理] タブを使用してポリシー ディレクトリを参照し、そのディレクトリ サービス オブジェクトを介してサービスに HPCA Agent を付与します。150 ページの「ディレクトリ オブジェクト」を参照してください。

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

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

脆弱性の管理

HPCA 脆弱性管理をサポートするには、次の操作を実行する必要があります。

- 通知の設定を作成する
- コンソール設定を確認する

- コンソールの [設定] タブで、**HP Live Network** の設定を行う

詳細については、「*セキュリティと適合性の管理*」の章を参照してください。

クライアント操作プロファイルの設定

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

COP の詳細とサーバー アクセス プロファイルの詳細オプションについては、『HPCA Application Manager および Application Self-Service Manager の Windows 用インストールおよび設定ガイド』の「クライアント オペレーション プロファイルを設定する」の章を参照してください。

サーバー アクセス プロファイル インスタンスの作成

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

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

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

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

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

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

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

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

OS Manager に固有の SAP 情報については、『HPCA OS Manager システム管理者ガイド』を参照してください。

例

2 つの Satellite (PARISSAT3 と EUROSAT1) が含まれており、38 ページの表 3 にある 3 つの SAP インスタンスが必要な環境があるとします。

表 3　　2 つの Satellite のための SAP インスタンスの例

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

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

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

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

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

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

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

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

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

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

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

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

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

8 変更を保存します。

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

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

- パッチ メタデータのみのダウンロードを有効化
- ゲートウェイの有効化

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

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

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

SAP インスタンスの作成または編集に関する基本的な情報については、37 ページの「サーバー アクセス プロファイル インスタンスの作成」を参照してください。

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

   a **P** という ROLE 値を追加します。

   これらの値には、次の太字の部分を追加する必要があります。

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

2 変更を CORE_RPS インスタンスに保存します。

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

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

SAP インスタンスの LOCATION クラス インスタンスへの接続

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

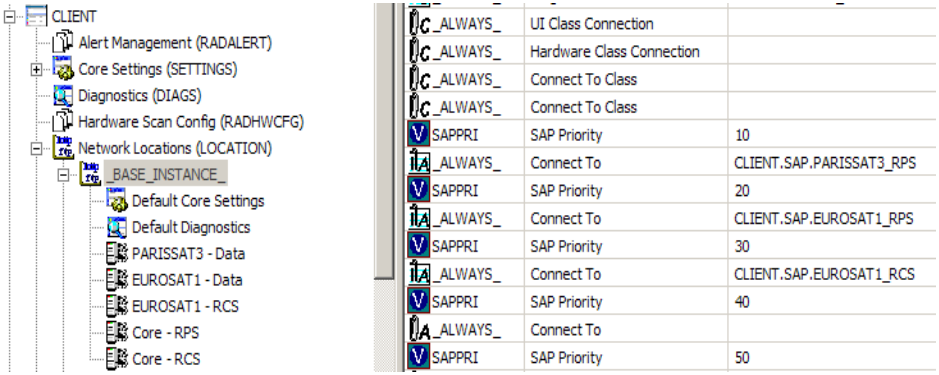
デフォルトでは、CORE_RPS インスタンスと Core_RCS インスタンスは、それぞれ 60 と 70 の優先度を持つ CLIENT.LOCATION._BASE_INSTANCE_ に接続されます。

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

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

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

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



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

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

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

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

HPCA Agent でのクライアント操作プロファイルの有効化

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

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

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

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

Satellite の同期

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

パッチ管理の設定

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

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

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

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

— ポリシー (外部ポリシー ディレクトリを使用している場合)

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

- Satellite Server をインストールします (推奨)。

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

パッチ管理の管理タスク

1. Core のインストール中にパッチを有効にします。
2. コンソールの [設定] タブから、すべてのパッチ管理の設定を完了します。
   - — 必要に応じて、Microsoft、RedHat、および SuSE のパッチを取得するための取得ジョブを作成します。

     メタデータを使用したパッチ管理は、デフォルトで Microsoft パッチで有効になっています。この機能によって、パッチを取得するためにかかる時間や Core Configuration Server に対する全体的な負荷が削減されます。詳細については、391 ページの「メタデータを使用したパッチ管理」を参照してください。

   - — HP Softpaq は、事前設定された 1 つの取得ジョブを使用します。このジョブを利用するには、各デバイスの HP Softpaq SysID を HP Softpaq のための取得設定に自動的に追加できるように、HP の管理対象デバイスに対してインベントリを実行します。
3. Core コンソールの **[操作]** タブから、パッチ取得を実行します。
4. パッチを取得して Core CSDB にパブリッシュした後、スケジュールされたジョブまたは Satellite コンソールの操作タスクのいずれかを使用して、Core Server と Satellite Server のコンテンツを同期します。
   - — Core コンソールの [管理] タブを使用して、Core Server と Satellite Server のコンテンツを同期するためのジョブを作成して実行します。
   - — Satellite コンソールの **[操作]** タブを使用して、Core Server と Satellite Server を同期します。Satellite コンソールは、**http://***satellite_hostname***:3466** でアクセスできます。

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

6 管理対象デバイスにブリティンを付与するためのポリシーを適用します。適用可能なパッチは、ユーザーの介入なしに配布されます。管理対象デバイスのパッチ適用状況ステータスを表示するには、[ダッシュボード] タブおよび [レポート] タブを使用します。

設定ファイルの変更に関する制限

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

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

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

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

オペレーティング システム イメージの配布

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

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

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

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

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

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

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

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

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

Core Server と Satellite Server の機能

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

- Core Server は、次の目的に使用されるツールとサービスをホストします。
  - 権限を持つ CSDB にオペレーティング システム イメージをパブリッシュする。
  - コンソールで OS Manager 管理タスクを実行する。
  - ポリシー資格を作成する。
- Satellite Server に OS Manager Server と Proxy Server のロールが設定されていることが前提になります。Satellite Server は、Configuration Server からのオペレーティング システム イメージに対するリクエストを処理し、これらのイメージのリソースを管理対象デバイスに提供します。

  オペレーティング システム イメージを Core CSDB にパブリッシュしたら、Satellite コンソールの **[操作]** タブを使用してオペレーティング システム イメージのリソースを*同期*し、Satellite Server に*事前読み込み*します。

HPCA OS Manager に関する注意事項

- デフォルトでは、OS Manager が Core Server または Satellite Server にインストールされると、OS Manager は Linux サービス OS を使用するように設定されます。サービス OS として WinPE を実行するようには設定されません。

  デフォルトのサービス OS として WinPE を使用するように環境を変換するには、『OS Manager ガイド Windows 用』の第 3 章を参照してください。
- HPCA Thin Client サーバーは、HPCA Console を介してインストールできます。また、そこで有効にしたり、無効にしたりすることもできます。
- OS Manager に固有の SAP 情報については、『HPCA OS Manager システム管理者ガイド』を参照してください。

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

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

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

アウトバンド管理の有効化

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

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

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

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

機能

HPCA Console の OOBM 機能を次に示します。

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

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

設定タスク

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

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

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

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

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

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

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

  システム防御設定は、DASH デバイスには適用されません。

操作タスク

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

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

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

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

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

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

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

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

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

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

3 セキュリティと適合性の管理

HPCA のセキュリティと適合性機能により、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。

紹介

HPCA のセキュリティと適合性の管理ソリューションには、次の領域があります。

- 50 ページの「脆弱性管理」
- 53 ページの「適用状況管理」
- 57 ページの「セキュリティ ツール管理」

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 4　　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 4　　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** を参照してください。
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 4　　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 5　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。

表 5　適用状況管理用語

用語	定義
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 5　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 (50 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 (50 ページの「脆弱性管理」を参照) • CVSS (50 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。
CIS	Center for Internet Security CIS は、NIST が SCAP を作成するよりも前に、一連の順守基準を開発しました。このドキュメントの出版時点で、CIS は新しい操作システムに関して追加のベンチマークをリリースしていません。 HP Live Network チームは、SCAP 形式で CIS ベンチマークを Live Network コンテンツの登録契約者に提供しています。 詳細については、**http://cisecurity.org** を参照してください。

関連する適用要件のグループは、**ベンチマーク** (FDCC-Windows-Vista など) として知られています。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、新しい名前が付けられます (FDCC-Windows-Vista v1.1.0.0 など)。

ベンチマークには**規則**が含まれます。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。

ベンチマークは 1 つ以上の**プロファイル**で構成され、プロファイルはベンチマーク内でさまざまなレベルの適用状況を定義するために使用されます。プロファイルでは、次の各項目を指定します。

- ベンチマーク内の一連の規則 (そのすべての場合もあり)
- 各規則で、その規則に対する適用状況を決定する値

規則への適用状況は、プロファイルによって決定します。HPCA が管理対象クライアント デバイスで適用状況スキャンを実行すると、適用可能なベンチマーク プロファイルの要件が評価されます。

それぞれの FDCC ベンチマークには単一のプロファイルが含まれます。CIS ベンチマークには、異なるタイプのシステム用の個別のプロファイルが含まれます。たとえば Windows XP (v2.01) CIS ベンチマークには、レガシー システム、エンタープライズ スタンドアロン システム、エンタープライズ モバイル システム、セキュリティ特化システム用のプロファイルが含まれます。

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、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。管理対象クライアント デバイス上で適用状況スキャンを実行すると、合格および失敗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。

ある適用状況レポートおよびダッシュボードで、特定のベンチマークの適用状況結果は各管理対象クライアント デバイスに関連するすべてのプロファイルで集約されます。詳細については、228 ページの「適用状況管理レポート」および 110 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。

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 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。

HP Live Network

HPCA は HP Live Network と統合され、セキュリティと適用状況管理のコンテンツ (データ) および実行可能なスキャナを提供します。HPCA インストールには、デモ用に機能が限定されたの一部の HP Live Network コンテンツが付属しています。更新された定義およびスキャナを取得し、HPCA Console でセキュリティと適用状況管理の機能を使用するには、第 5 章、「HPCA および HP Live Network」を参照してください。

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、および分析を行う登録契約サービスです。60 ページの図 1 を参照してください。

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

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

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

HPCA Console では、企業のセキュリティおよび適応状況のステータスが一目でわかるダッシュボードが表示されます。また、パッチ管理ダッシュボードも表示され、企業全体にわたるパッチ ポリシーの適用状況をすばやく評価できます。詳細については、77 ページの「ダッシュボードの使用」を参照してください。

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 6　　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合性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

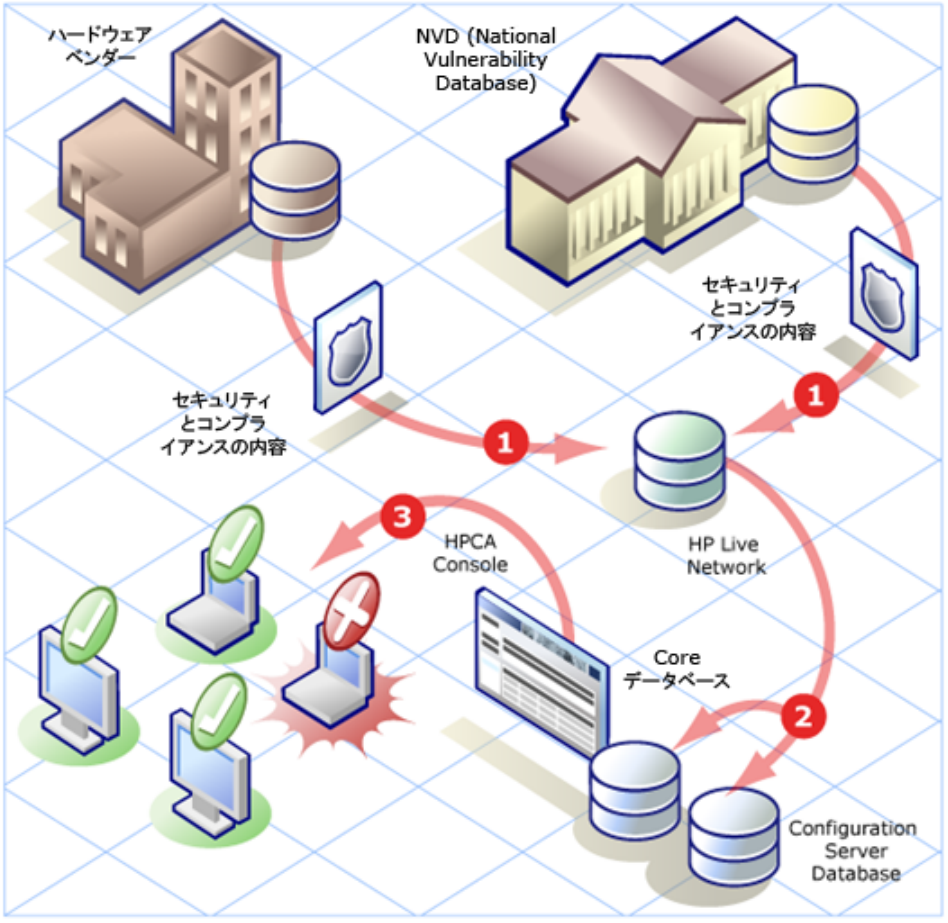
HP Live Network コンテンツにアクセスするには、第 5 章、「HPCA および HP Live Network」を参照してください。

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 Core データベースに追加されます。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 に読み込まれます。

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

図 1　　HPCA でのセキュリティと適合性の管理



1　更新されたセキュリティと適合性のコンテンツが 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 Core データベースにパブリッシュされます。

3　クライアント デバイスは、セキュリティと適合性の問題がないかどうか HPCA によってスキャンされます。

CSDB に読み込まれたセキュリティと適合性のコンテンツには、「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 (529 ページの「テスト環境からプロダクション環境への HP Live Network コンテンツの移動」を参照)。

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

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

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

スキャン サービスの詳細

Configuration Server Database (CSDB) には、セキュリティと適合性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合性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。このバージョンは 32 ビットプラットフォームでのみ使用できます。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、確立されている付与資格は変更されません。

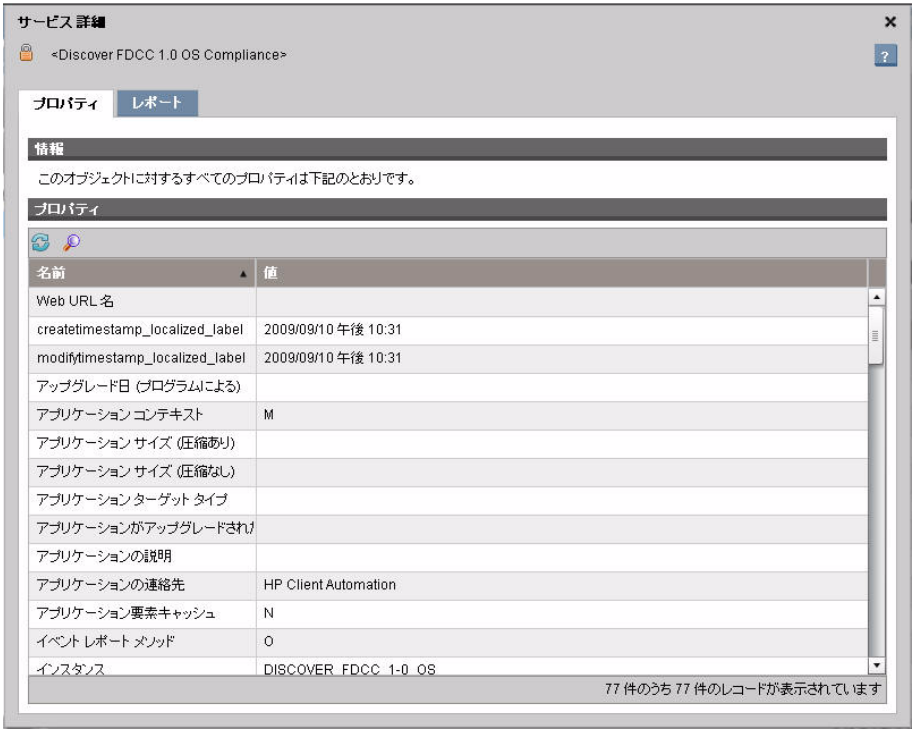
スキャン サービスを表示するには

1. HPCA Console にサインインします。
2. **[管理]** タブをクリックします。
3. 左側のペインで、**[サービス]** をクリックします。使用可能な CSDB ドメインの一覧が表示されます。
4. 左側のペインで、**[セキュリティ]** をクリックします。
5. [カタログ] ペインで、セキュリティ サービスのいずれかをクリックします。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、169 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。67 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 のいずれかの方法が実行されます。これらのいずれかの方法が実行されると、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 デバイスを明示的に付与する必要があります。詳細については、65 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。

セキュリティと適合性の管理の設定

312 ページの「Live Network」を参照してください。

一般的なセキュリティと適合性管理のタスク

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 のコンテンツを更新するには、第 5 章、「HPCA および HP Live Network」を参照してください。

スキャンのスケジュール設定または起動

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

1 1 つ以上のセキュリティ サービスにデバイス (またはデバイスのグループ) を付与します。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。

66 ページの「スキャンのためのデバイスの付与」を参照してください。

2 [セキュリティ接続] ジョブ アクション テンプレートを使用してジョブを作成することによって、HPCA Console からスキャンをスケジュール設定または起動します。67 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。正しく付与ターゲット 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。68 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、62 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付与

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を正しく付与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) を付与するには

1 [管理] タブで、付与デバイスが含まれているゾーンを展開します。

2 1 つのデバイスを付与する場合は、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付与する場合は、**[グループ]** をクリックします。

3 付与するデバイスまたはグループのショートカット メニューから、**[プロパティの表示 / 編集]** を選択します。新しいウィンドウである [ディレクトリ オブジェクト] ウィンドウが表示されます。

4 左のナビゲーション ツリーで、**[ポリシー]** をクリックします。

5 [ポリシー管理の起動] () ボタンをクリックして、ポリシー管理ウィザードを開きます。

6 [サービス ドメイン] の一覧から、**[セキュリティ]** を選択します。

7 1 つ以上のセキュリティ サービスの左にあるボックスを選択します。HPCA をインストールすると、次のサービスがすぐに使用可能になります。

- SECURITY.ZSERVICE.DISCOVER_VULNERABILITY
- SECURITY.ZSERVICE.DISCOVER_FDCC_1-0_OS
- HP Live Network の更新を実行した後、追加のセキュリティ サービスが使用可能になります。

  たとえば、最初の更新の後、SECURITY.ZSERVICE.DISCOVER_SECTOOLS_AV_AS_FW サービスが使用可能になります。

8 **[追加]** をクリックします。

9 **[次へ]** をクリックします。

10 [ポリシー設定] の下の **[許可]** を選択します。

11 [優先度] の下で、管理対象クライアント デバイス (1 つまたは複数) に対するスキャンが実行されるときに、そのスキャンに割り当てる優先度を選択します。

12 **[次へ]** をクリックします。

13 サービス (1 つまたは複数) の設定を確認します。設定を変更する場合は、**[前へ]** をクリックします。続行する準備ができたら、**[適用]** をクリックします。

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

スキャンをスケジュール設定または起動する HPCA ジョブの作成

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

スキャンをスケジュール設定または起動するジョブを作成するには

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

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

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

ウィザードでは、必要なフィールドにアスタリスク (*) が付いています。

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

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

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

5 ジョブの **[名前]** を指定します。

6 **[ジョブの説明]** を指定します。

7 **[ジョブ アクション テンプレート]** の一覧から、**[Security Connect]** 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、177 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、174 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合性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　デバイスが付与されている、SECURITY ドメインのすべてのサービス (セキュリティと適合性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

HPCA Console で使用可能なレポートを使用すると、脆弱性、適用状況、またはセキュリティ ツールのスキャンの結果を表示できます。また、HP Live Network コンテンツの更新のステータスを表示することもできます。レポートをフィルタして、興味のある情報のみを表示することができます。詳細については、217 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、77 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ィ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ィンを見つけるには、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、**[ブリティン]** 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、231 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、**[ブリティン]** 列のリンクをクリックします。

ブリティンにパッチが含まれている場合は、HPCA Console のパッチ管理機能を使用して、そのパッチに関連デバイスを付与できます。

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

適用状況の失敗に関する情報の検索

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

上位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 [概要] の下の **[上位の SCAP 非コンプライアント 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、バージョン、プロファイルの最新のスキャン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、バージョン、プロファイル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、バージョン、プロファイルの最新のスキャン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。関係するデバイスの次のレポートが開きます。

— デバイスの詳細 – 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

— デバイスごとのベンチマーク – このデバイスでテストされた各ベンチマーク、バージョン、プロファイルの最新スキャン結果

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、バージョン、プロファイル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、バージョン、プロファイル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 7

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
ファイアウォール	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 (Windows XP SP2 以降および Windows Vista のファイアウォールのみに適用)

詳細については、次のトピックを参照してください。

- 124 ページの「セキュリティ ツール管理ダッシュボード」
- 229 ページの「セキュリティ ツール管理レポート」

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。

セキュリティと適合性の管理に関する詳細情報

次のセクションには、HPCA Console でのセキュリティと適合性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。

- 77 ページの「ダッシュボードの使用」
- 217 ページの「レポートの使用」
- 312 ページの「Live Network」

セキュリティと適合性の管理の詳細については、次の Web サイトを参照してください。

http://cve.mitre.org

http://nvd.nist.gov

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

http://oval.mitre.org

http://www.us-cert.gov

4　ダッシュボードの使用

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

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

- 83 ページの「HPCA 操作ダッシュボード」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。
- 90 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。
- 110 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。
- 124 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。
- 133 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 8　　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。
操作ビュー	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、373 ページの「ダッシュボード」を参照してください。

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

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

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

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

図 2　　タイム スタンプ

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

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

ダッシュボード ペインでは、次のアクションを実行できます。

表 9　　ダッシュボード ペインのアクション

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

表 9　　ダッシュボード ペインのアクション

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

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

図 3　　ダッシュボード ペインを復元するボタン

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

ダッシュボード内の各ペインのサイズや配置を変更して外観をカスタマイズした場合、または 1 つ以上のペインのグラフとグリッドのビューを切り替えた場合、このカスタマイズは次回 HPCA Console に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、504 ページの「ダッシュボード レイアウト設定の削除」を参照してください。

いずれかのダッシュボードの表示中に **F5** ファンクション キーを押すと、ブラウザが HPCA Console を再度読み込んだ後にそのダッシュボードのページに戻ります。

一部のグリッド表示では、特定のパラメータ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 10　　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、91 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。

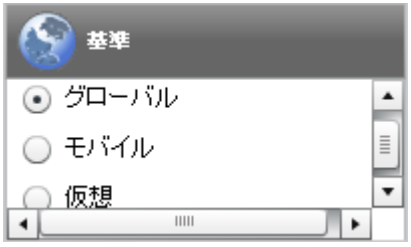
ダッシュボード デバイス

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 または Xen (Citrix を含む) であるすべてのデバイスが含まれます。

追加のデバイスを最大 2 つ定義することもできます。詳細については、『Enterprise Manager ガイド』の*「カスタム ダッシュボード デバイスとフィルタの追加」*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 [基準] ボックスでデバイスを選択します。



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

フィルタまたはデバイスが適用できません

また、デバイスの設定が適用されないペインは外枠がオレンジ色になります。

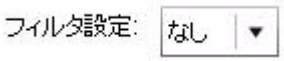
デバイスの設定が適用されないダッシュボード ペインは次のとおりです。

- 93 ページの「脆弱性履歴の評価」
- 116 ページの「適用状況評価履歴」
- 139 ページの「Microsoft セキュリティ ブリティン」
- 100 ページの「HP Live Network アナウンスメント」
- 137 ページの「HP Live Network Patch Manager アナウンスメント」

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

ダッシュボード フィルタ

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



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

HPCA 操作ダッシュボード

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

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

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

84 ページの「クライアント接続」

86 ページの「サービス イベント」

エグゼクティブ ビューには、次のペインも含まれます。

88 ページの「ドメイン別 12 か月サービス イベント」

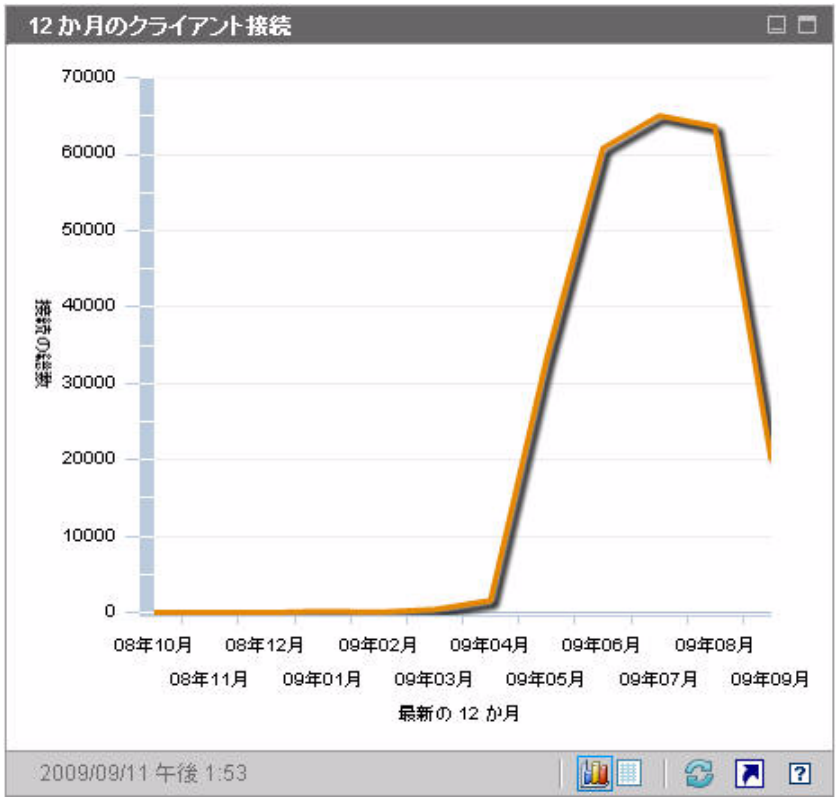
デフォルトではこれらのペインがすべて表示されます。ダッシュボードでは、これらの任意のペインの表示 / 非表示を切り替えることができます。373 ページの「ダッシュボード」を参照してください。

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

クライアント接続

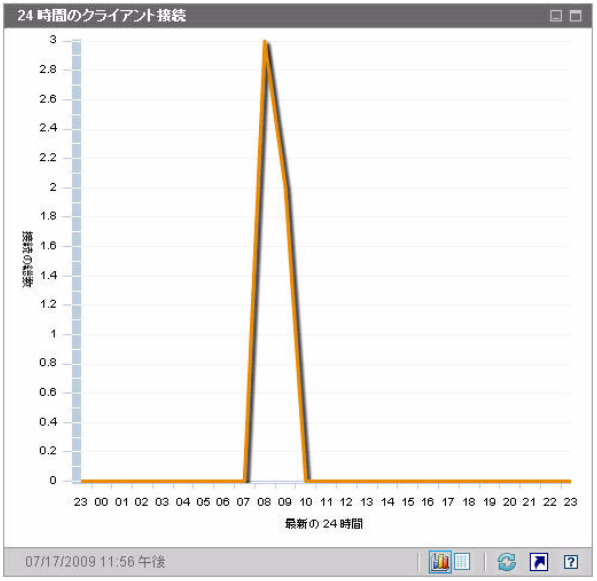
このペインのグラフ表示には、過去 12 か月 (エグゼクティブ ビュー) または 24 時間 (操作ビュー) に発生した HPCA Agent クライアント接続の数が表示されます。データ ポイントの上にカーソルを置くと、その月または時間の合計接続数が表示されます。

図 4　　12 か月のクライアント接続



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

図 5　　24 時間のクライアント接続



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

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

サービス イベント

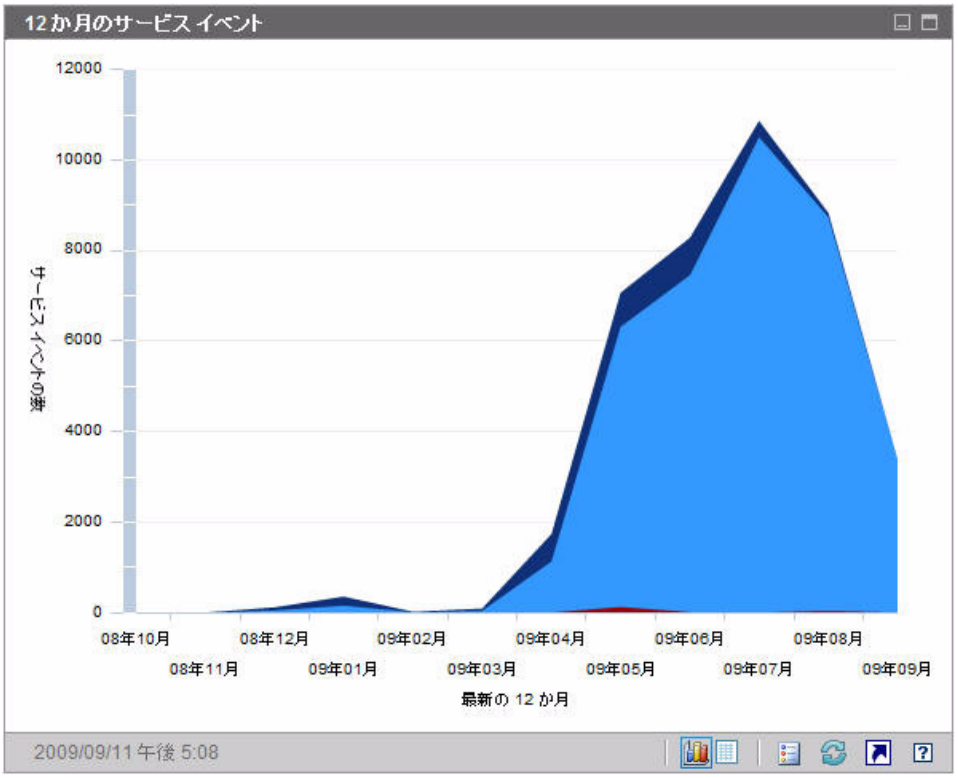
このペインのグラフ表示では、過去 12 か月 (エグゼクティブ ビュー) または 24 時間 (操作ビュー) に企業のクライアント デバイスにおいて HPCA で完了したサービス イベントの数が表示されます。これらのサービス イベントには、HPCA により次の作業が行われたアプリケーションの数が含まれます。

- インストール済み
- アンインストール済み

- 更新済み
- 修復済み
- 検証済み

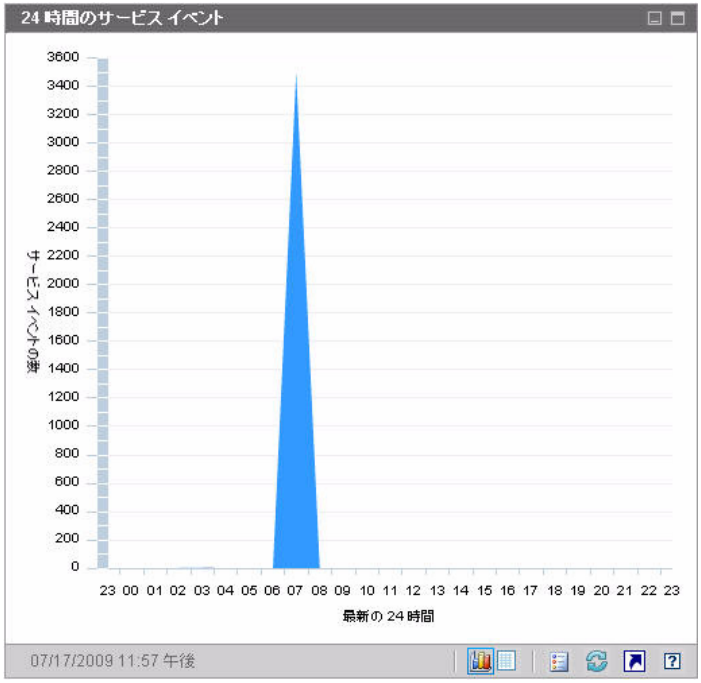
データ ポイントの上にカーソルを置くと、特定の月または時間に完了したサービス イベント数が表示されます。

図 6　　12 か月のサービス イベント



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

図 7　　24 時間のサービス イベント



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

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

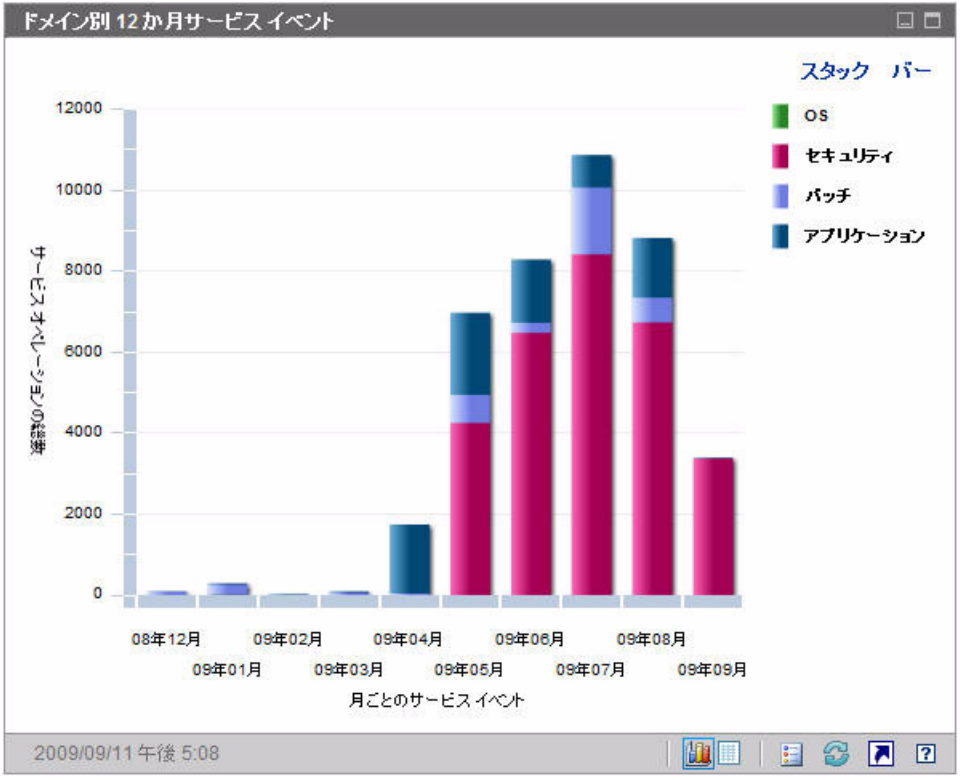
ドメイン別 12 か月サービス イベント

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

- オペレーティング システム (OS) の操作
- セキュリティ操作
- パッチ操作
- アプリケーション操作

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

図 8　　ドメイン別 12 か月サービス イベント



このグラフには、2 とおりのデータ表示方法があります。

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

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

脆弱性管理ダッシュボード

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

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

脆弱性管理ダッシュボードおよび各種レポートで使用される共通の脆弱性管理用語の詳細は、49 ページの「セキュリティと適合性の管理」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 11　　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。

- 91 ページの「脆弱性の重大度別影響 (円グラフ)」
- 102 ページの「重大度別にした脆弱性の影響 (棒グラフ)」
- 95 ページの「脆弱性の影響」
- 93 ページの「脆弱性履歴の評価」

[操作] ビューには、次の 4 つの情報ペインが含まれます。

- 100 ページの「HP Live Network アナウンスメント」
- 103 ページの「最も脆弱性の高いデバイス」
- 105 ページの「最も脆弱性の高いサブネット」
- 107 ページの「脆弱性のトップ」

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。373 ページの「ダッシュボード」を参照してください。

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

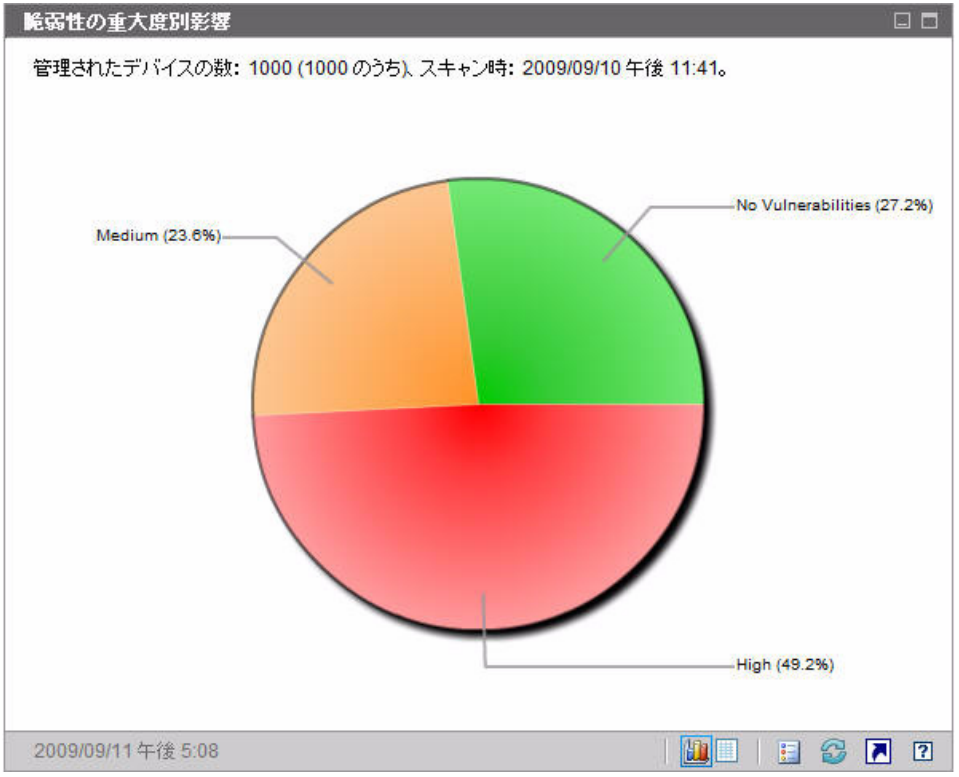
脆弱性の重大度別影響 (円グラフ)

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)

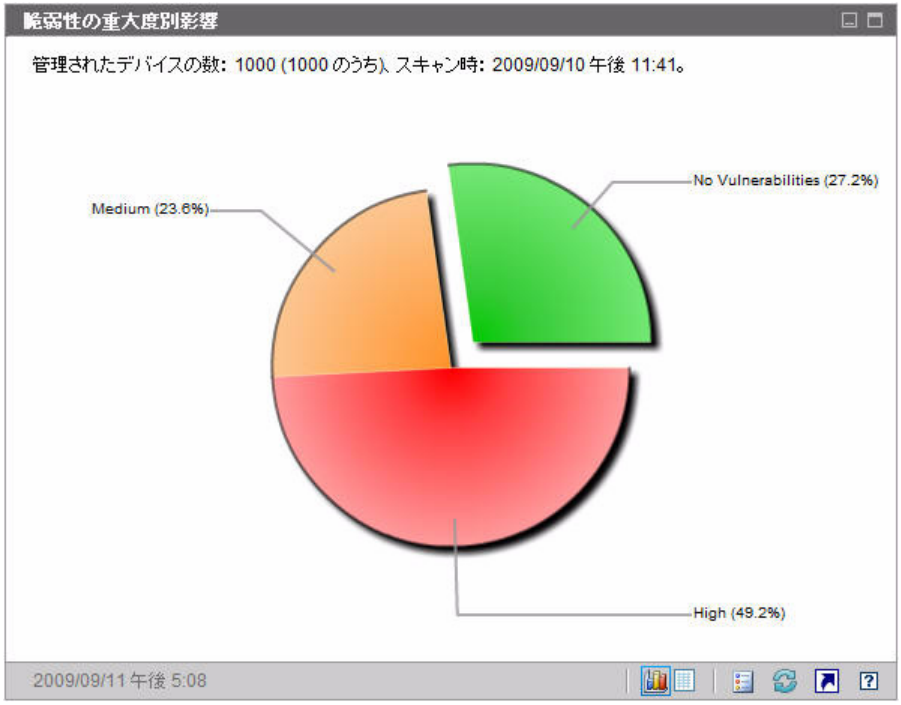
各重大度カテゴリのデバイス数を表示するには、円グラフの対応するセクタの上にカーソルを置きます。

図 9　　脆弱性の重大度別影響



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

図 10　　脆弱性の重大度別影響



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

関連トピック：

77 ページの「ダッシュボードの使用」

90 ページの「脆弱性管理ダッシュボード」

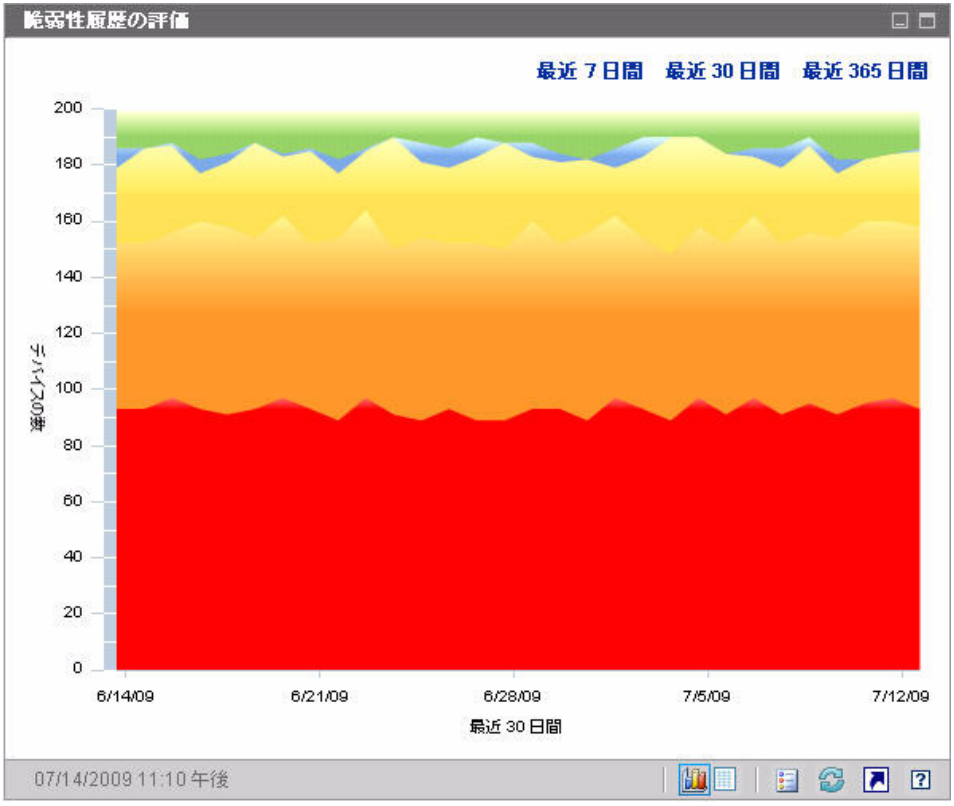
49 ページの「セキュリティと適合性の管理」

脆弱性履歴の評価

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

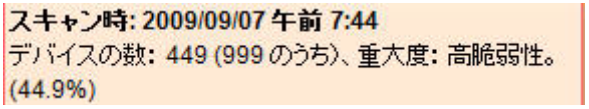
このペインのグラフ表示では、一定の期間における企業のリスク集計の平均が表示されます。垂直軸はデバイス数を表します。水平軸は時間を表します。過去 7 日、30 日、または 365 日のデータを表示できます。色分けされたそれぞれの領域は、各重大度カテゴリのデバイス数を表します。カテゴリは、高 (赤)、中 (オレンジ)、低 (黄)、脆弱性なし (緑)、および不明 (青) に分類されています。

図 11　　脆弱性履歴の評価



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

図 12　　ツール チップ



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

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

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

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

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

関連トピック：

77 ページの「ダッシュボードの使用」

90 ページの「脆弱性管理ダッシュボード」

49 ページの「セキュリティと適合性の管理」

脆弱性の影響

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

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

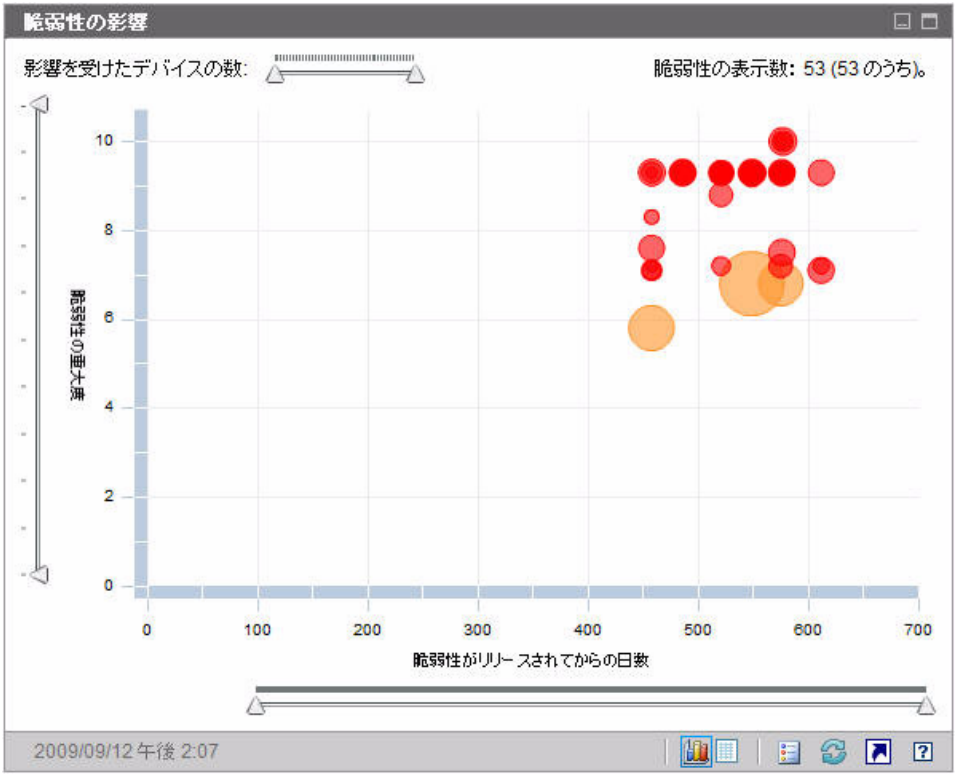
- グラフの左下部分に小さな黄色の円がある場合、少数のデバイスに影響を与え、NVD でパブリッシュされたのが比較的最近である重大度が低い問題の存在を表しています。
- 右上隅に赤い円がないグラフが理想的と言えます。これは、重大な脆弱性が迅速に処置されたことを示しています。

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

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

図 13　　脆弱性の影響



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

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

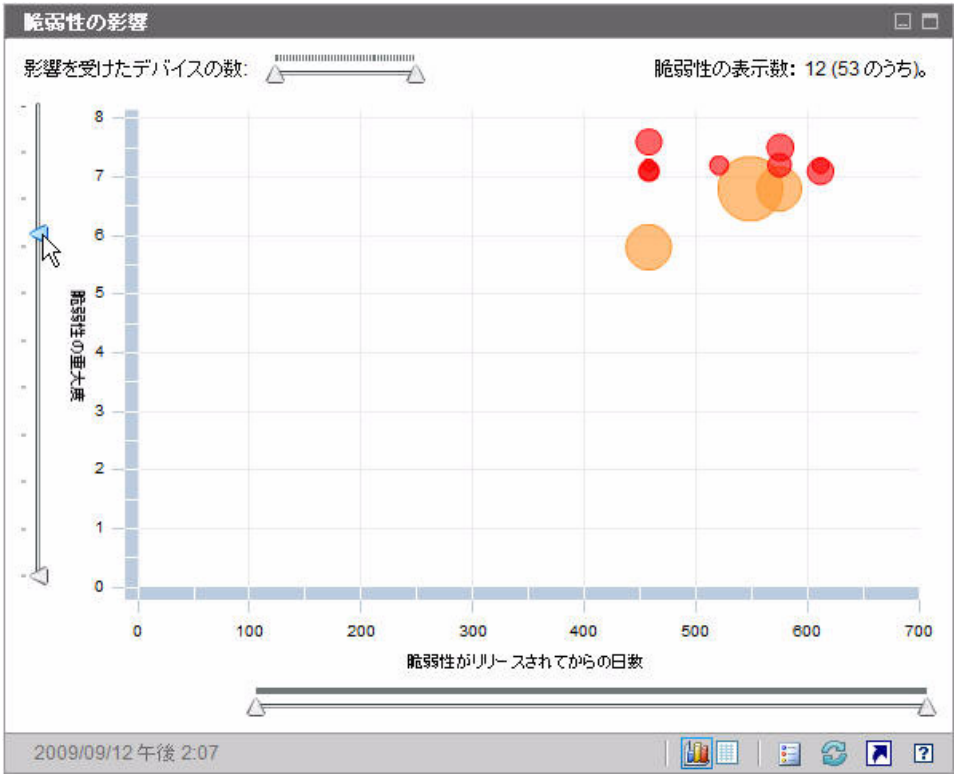
  デフォルトでは、表示される有効期間は 45 日間です。脆弱性管理ダッシュボードの設定時に、このデフォルト値を指定できます。373 ページの「ダッシュボード」を参照してください。

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

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

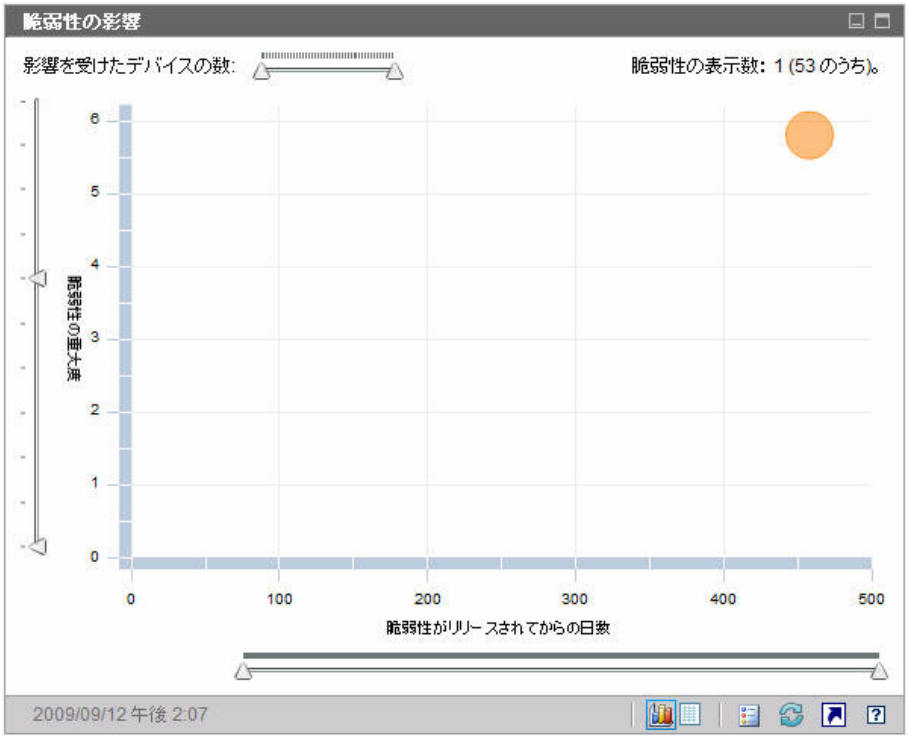
次の例では、CVSS ベースのスコアが 6 以上の脆弱性が表示されています。

図 14　　CVSS が 6 以上



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

図 15　　過去 500 日以内



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

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

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

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

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

関連トピック：

77 ページの「ダッシュボードの使用」

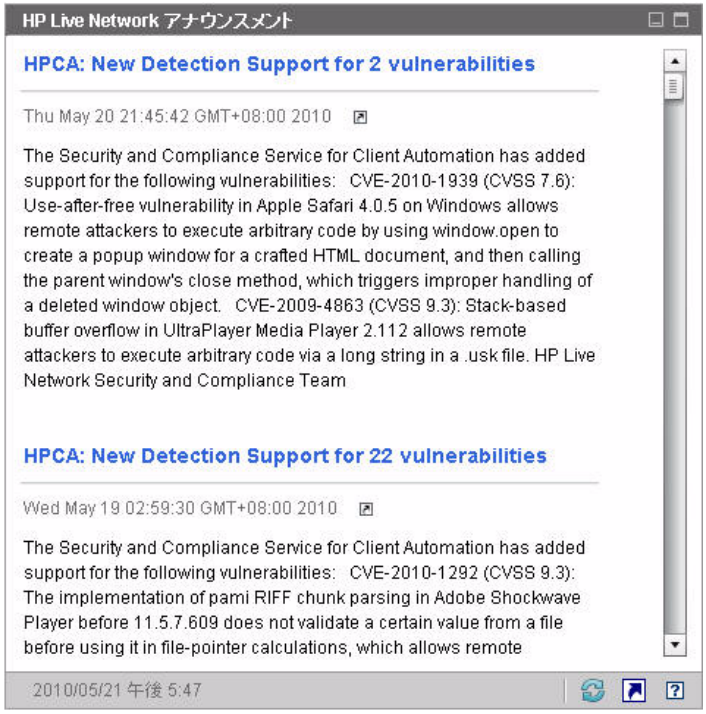
90 ページの「脆弱性管理ダッシュボード」

49 ページの「セキュリティと適合性の管理」

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、373 ページの「ダッシュボード」を参照してください。また、「HPCA および HP Live Network」の章も参照してください。

図 16　　HP Live Network アナウンスメント



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

このペインにはグラフ表示はありません。

[設定] タブでこのペインを有効にするとき、RSS フィードの URL および HP Live Network 認証サーバーの場所を変更できます (373 ページの「ダッシュボード」を参照)。また、プロキシ サーバーを有効にする必要が生じる場合もあります (312 ページの「HP Live Network サーバーへの接続の設定」および 291 ページの「プロキシ設定」を参照)。

関連トピック：

77 ページの「ダッシュボードの使用」

90 ページの「脆弱性管理ダッシュボード」

49 ページの「セキュリティと適合性の管理」

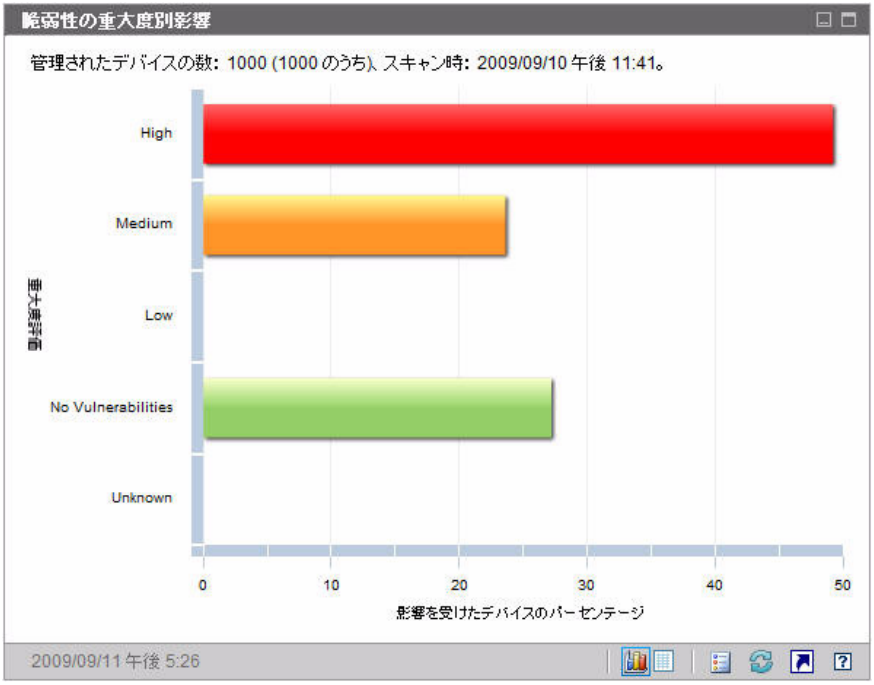
重大度別にした脆弱性の影響 (棒グラフ)

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

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

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

図 17　　脆弱性の重大度別影響



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

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

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

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

関連トピック：

77 ページの「ダッシュボードの使用」

90 ページの「脆弱性管理ダッシュボード」

49 ページの「セキュリティと適合性の管理」

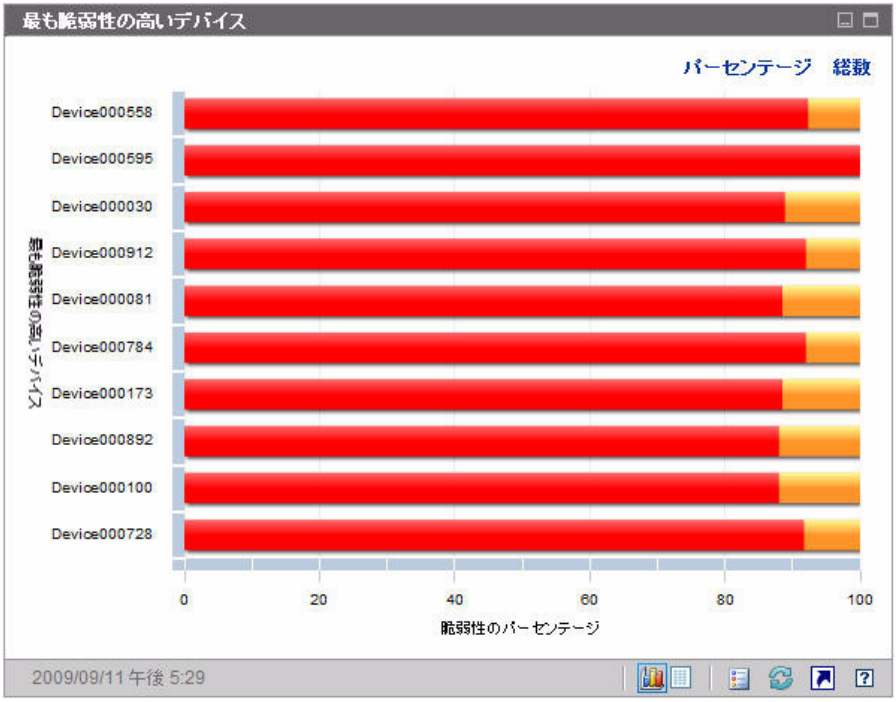
最も脆弱性の高いデバイス

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

- 高 (赤)
- 中 (オレンジ)
- 低 (黄)
- 不明 (青)

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

図 18　　最も脆弱性の高いデバイス



リストにある各デバイスの脆弱性の総数を表示するには、**[総数]** をクリックします。この場合、水平軸は、対数目盛りになります。

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

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

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

グリッド表示では、各デバイスについて次の情報が提供されます。

- 最大重大度 – 該当デバイスで検出された最も重大度が高い脆弱性の CVSS ベースのスコア

- デバイス – デバイス ID
- 失敗したテスト – 検出された脆弱性の数
- 前回のスキャン日 – 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：

77 ページの「ダッシュボードの使用」

90 ページの「脆弱性管理ダッシュボード」

49 ページの「セキュリティと適合性の管理」

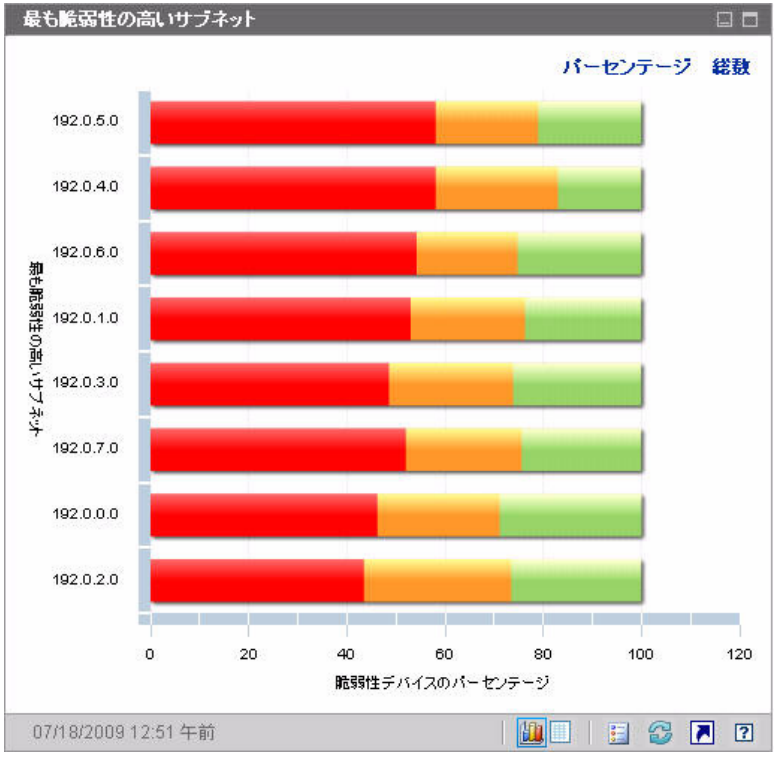
最も脆弱性の高いサブネット

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

デフォルトではこのペインは無効です。有効化するには、373 ページの「ダッシュボード」を参照してください。

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

図 19　　最も脆弱性の高いサブネット



パーセンテージではなく、脆弱性のある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：

77 ページの「ダッシュボードの使用」

90 ページの「脆弱性管理ダッシュボード」

49 ページの「セキュリティと適合性の管理」

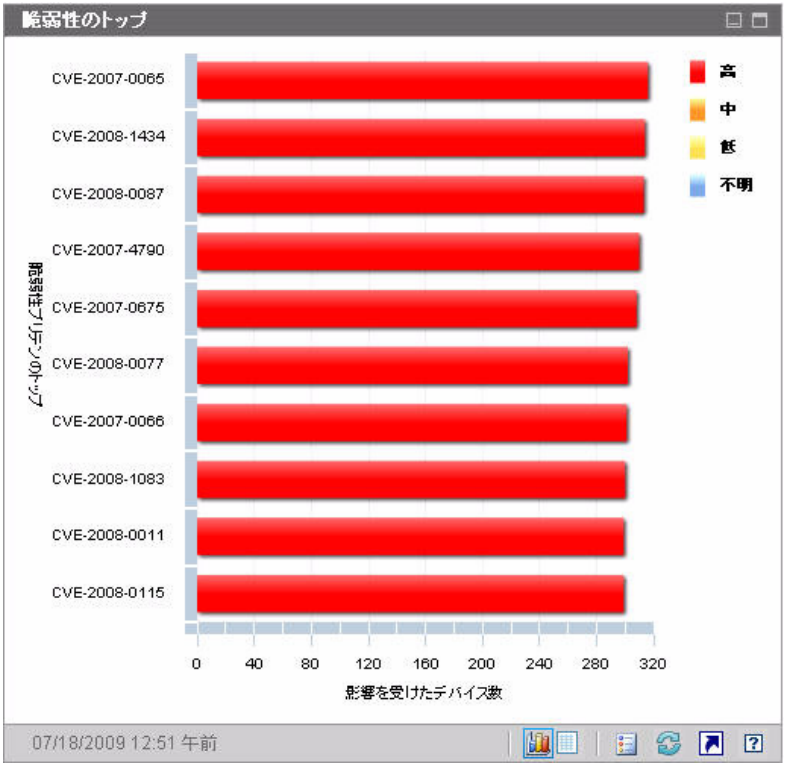
脆弱性のトップ

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

- 高 (赤)
- 中 (オレンジ)
- 低 (黄)
- 不明 (青)

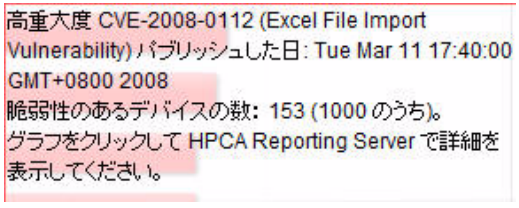
このグラフでは対数尺度を使用するため、特定の脆弱性が 1 つのデバイスのみに影響する場合、グラフ表示にはその脆弱性に関するデータが表示されません。これは、対数目盛りの既知の制限です。ただし、グリッド表示ではデータが表示されます。

図 20　　脆弱性のトップ



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

図 21　　ツール チップ



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

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

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

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

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

関連トピック :

77 ページの「ダッシュボードの使用」

90 ページの「脆弱性管理ダッシュボード」

49 ページの「セキュリティと適合性の管理」

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 デバイス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) や Center for Internet Security (CIS) 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、CIS および SCAP の詳細は、49 ページの「セキュリティと適合性の管理」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。

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

操作ビューには、次の情報ペインがあります。

- 120 ページの「失敗した SCAP ルールのトップ」
- 121 ページの「失敗回数の多いデバイス (SCAP ルール別)」

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、373 ページの「ダッシュボード」を参照してください。

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

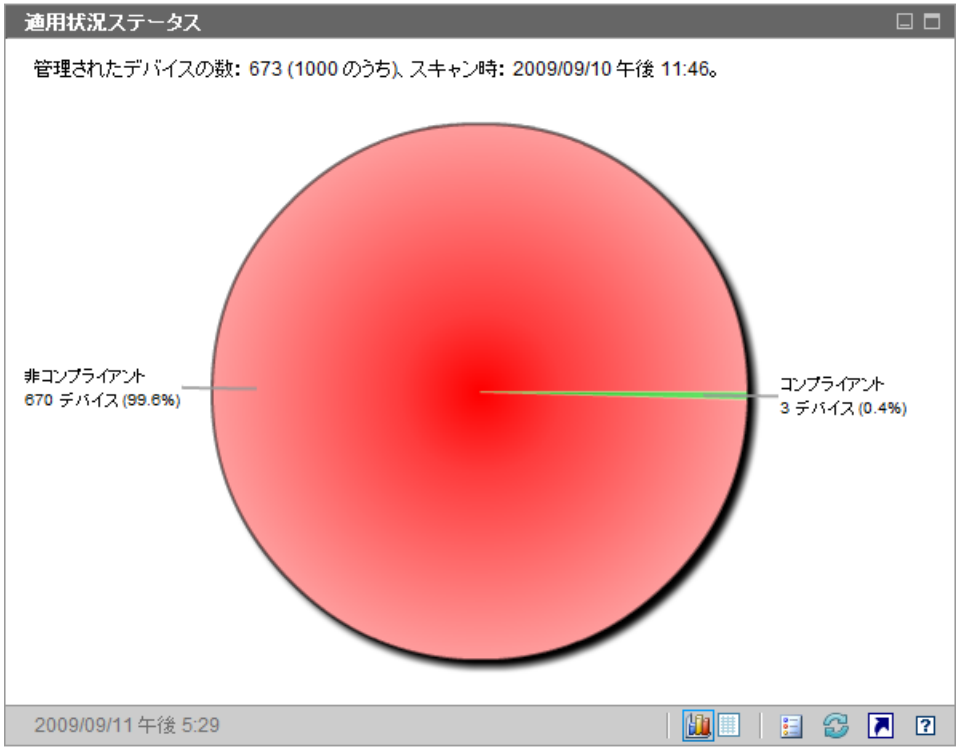
適用状況ステータス

このペインには、各管理対象クライアント デバイスで完了した最新の適用状況スキャンの結果に基づき、企業全体の法規制適用状況の状態が表示されます。このペインのグラフ表示は、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。

- 準拠デバイス (緑)
- 非準拠デバイス (赤)

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

図 22　　適用状況ステータス



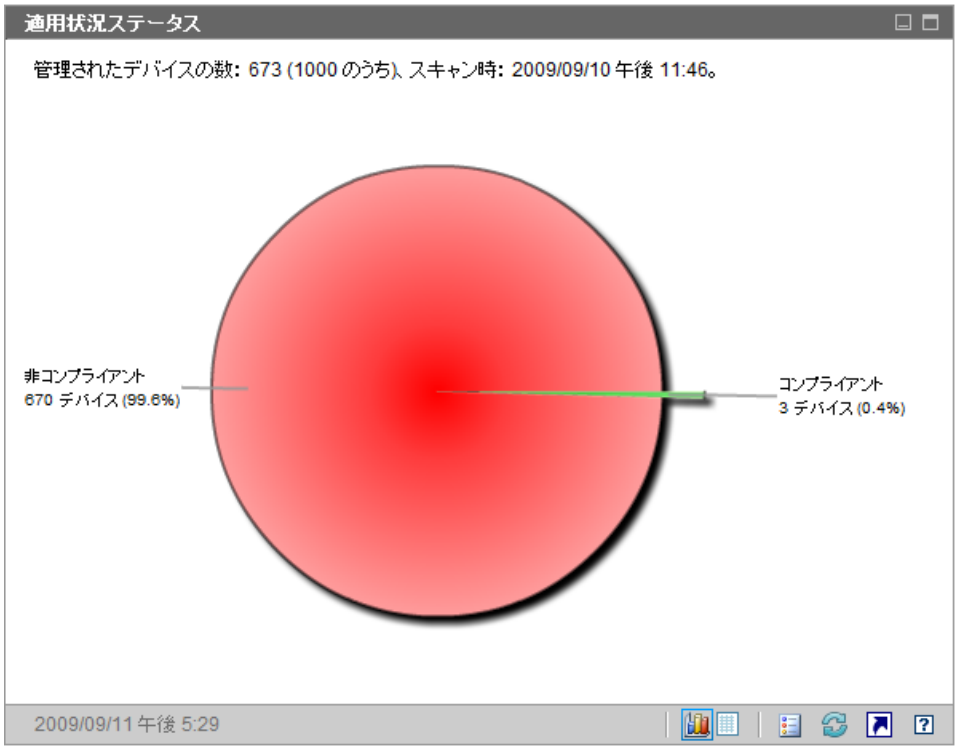
ペインの左上隅の数は、スキャンされた管理対象デバイスの総数です。特定のデバイスに適用されないベンチマークもあるため、この数は準拠しているデバイスと準拠していないデバイスの総数と同じにはならない可能性があります。たとえば、fdcc-ie-7 ベンチマークは、Internet Explorer 7 がインストールされていないデバイスには適用されません。適用できるベンチマークがないデバイスは、準拠しているデバイスでも準拠していないデバイスでもないと判断されます。

各デバイスのデータは、ベンチマークのすべてのプロファイルを対象として集計されます。デバイスがベンチマークの該当するすべてのプロファイルに準拠している場合、デバイスはそのベンチマークに準拠していると判断されます。デバイスがベンチマークのプロファイルに 1 つでも準拠していない場合、デバイスは準拠していないと判断されます。

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

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

図 23　　レポートを開いた後の適用状況ステータス



グリッド表示には、準拠デバイスと非準拠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。

このペインの**レポートの起動** ボタンをクリックすると、[ベンチマーク要約] レポートが表示されます。このレポートには、スキャン結果があるすべてのプロファイルがフィルタされていない状態で表示されます。

関連トピック：

77 ページの「ダッシュボードの使用」

110 ページの「適用状況管理ダッシュボード」

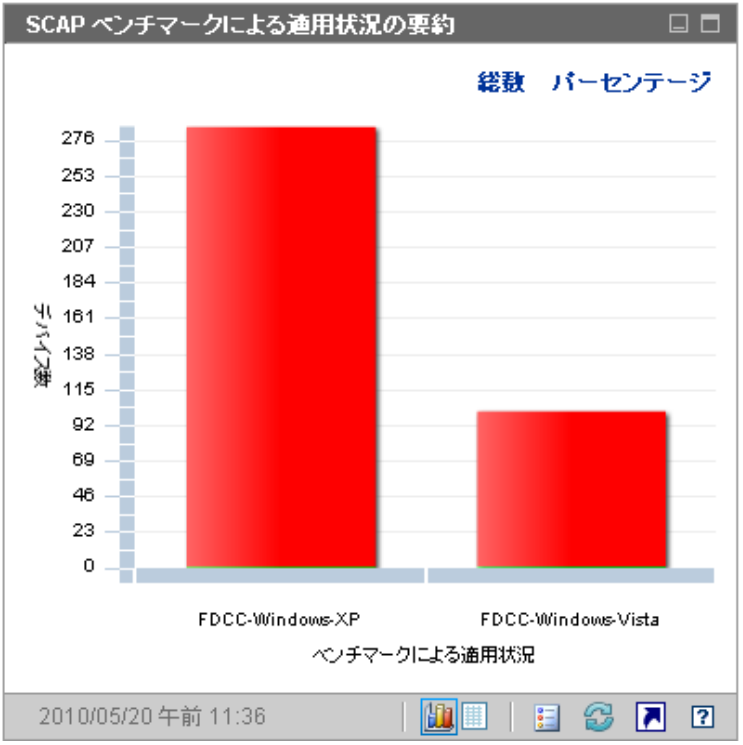
49 ページの「セキュリティと適合性の管理」

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。

- 準拠デバイス (緑)
- 非準拠デバイス (赤)

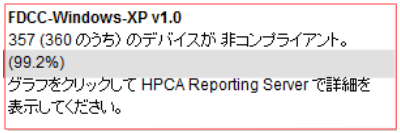
図 24　　SCAP ベンチマークによる適用状況の要約



スキャン結果があるベンチマークのみが表示されます。各デバイスのデータは、ベンチマークのすべてのプロファイルを対象として集計されます。デバイスがベンチマークの該当するすべてのプロファイルに準拠している場合、デバイスはそのベンチマークに準拠していると判断されます。デバイスがベンチマークのプロファイルに 1 つでも準拠していない場合、デバイスは準拠していないと判断されます。

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

図 25　　ツールチップ



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

棒グラフの色分けされたセグメントの 1 つをクリックすると、新しいブラウザ ウィンドウが開き、[SCAP スキャン済みデバイス] レポートが表示されます。レポートは、クリックしたセグメントに対応するベンチマーク、バージョン、および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 バージョンに準拠している、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。

このペインの**レポートの起動** ボタンをクリックすると、[ベンチマーク要約] レポートが表示されます。このレポートには、スキャン結果があるすべてのプロファイルがフィルタされていない状態で表示されます。

異なるバージョンのベンチマークがテストされた場合は、このペインのグラフ表示に同じベンチマーク ID が複数回表示されます。ベンチマーク バージョンは、グラフ表示のツールチップまたはグリッド表示に表示されます。スキャン結果があるすべてのバージョンのベンチマークが、グラフ表示およびグリッド表示に表示されます。

関連トピック：

77 ページの「ダッシュボードの使用」

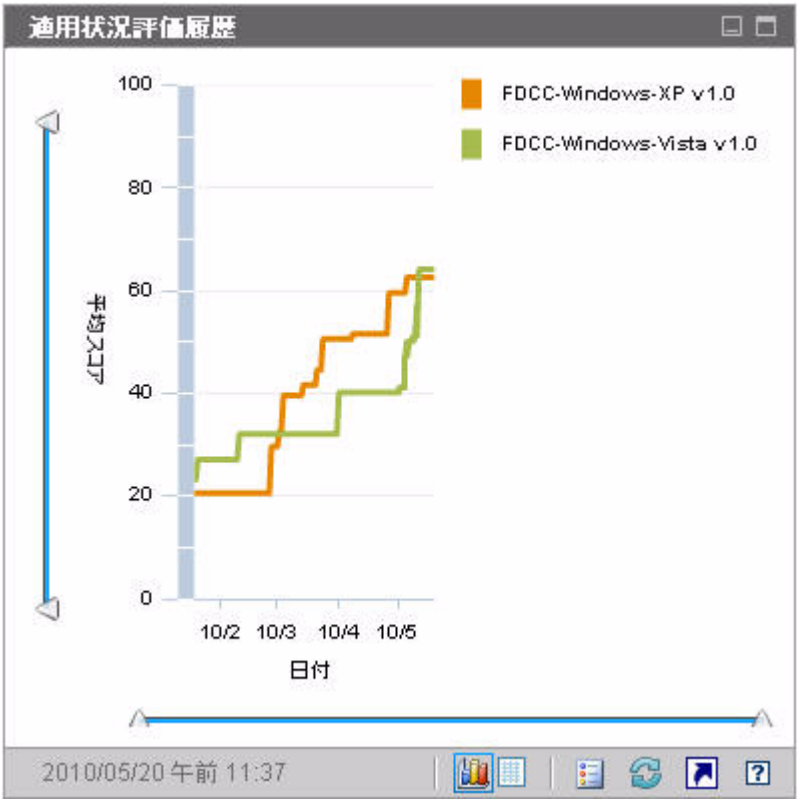
110 ページの「適用状況管理ダッシュボード」

49 ページの「セキュリティと適合性の管理」

適用状況評価履歴

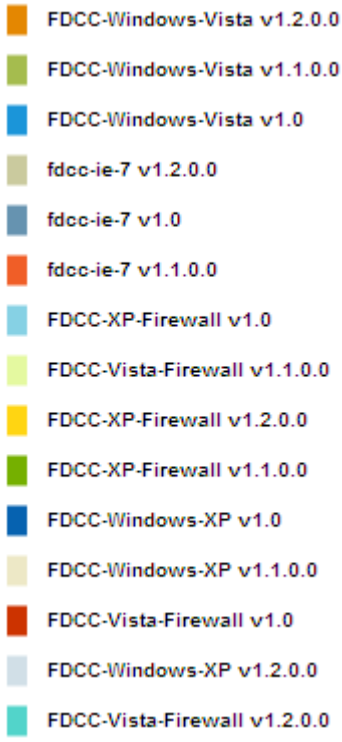
毎日 1 回、企業全体の適用状況スキャン結果のスナップショットが作成されます。このスナップショットに基づいて、プロファイルが適用されるデバイスに対して各ベンチマーク、バージョン、およびプロファイルの平均デフォルト スコアが計算されます。この情報ペインには、長期にわたる各ベンチマーク バージョンの平均デフォルト スコアが表示されます。

図 26　　適用状況評価履歴



特定のベンチマーク バージョンに複数のプロファイルが含まれている場合、「平均の平均」が計算されます。該当するベンチマーク バージョンのすべてのプロファイルの平均スコアが計算されます。

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およびバージョンを表します。このグラフには、次のベンチマーク バージョンが表示されます。



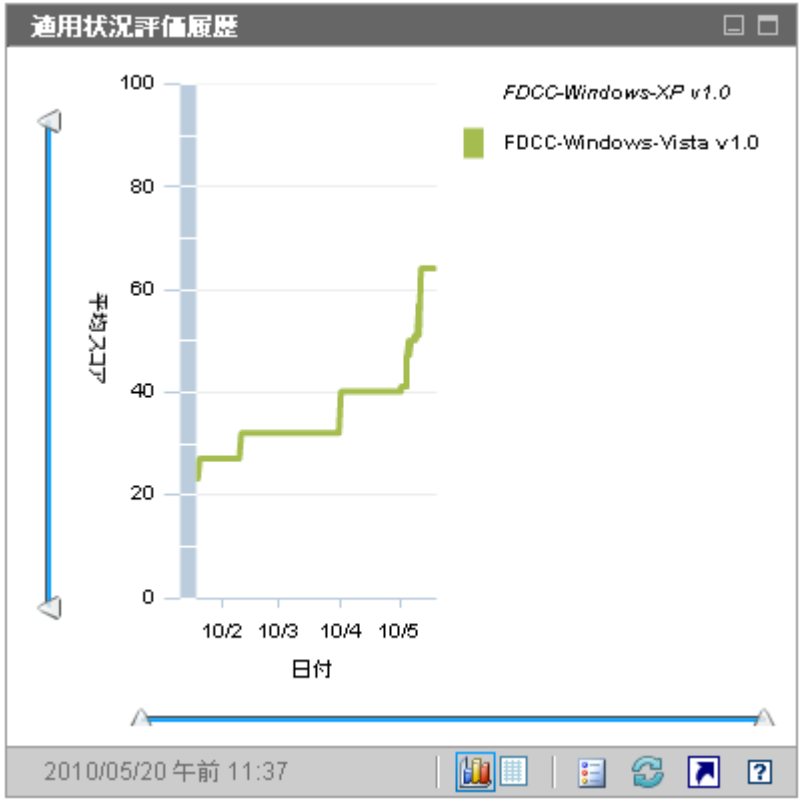
これらの色は動的に割り当てられ、特定のベンチマークおよびバージョンに常に同じ色が使用されるわけではありません。現在の色の割り当てについては、凡例を参照してください。

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

- ベンチマークの名前とバージョン
- スナップショットの日付
- このベンチマーク　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。ベンチマークに複数のプロファイルがある場合、このスコアはすべてのプロファイルの平均を表します。

グラフ表示の特定のラインを非表示にするには、凡例の対応するアイテムをクリックします。非表示のアイテムは、太字ではないイタリックのテキストで凡例に表示されます。このラインをグラフに再度表示するには、凡例のアイテムをもう一度クリックします。

次の図では、Internet Explorer 7 に関連するベンチマークのみがグラフに表示されています。



スライダを使用して、特定のデータ領域を拡大できます。スライダによってグラフに表示されるデータ量が決まります。スライダで選択した範囲のみが表示されるように、軸の範囲 (スケール) が変わります。いずれかのスライダを動かすかクリックすると、ツールチップに日付やスコアが表示されます。

- ペインの下部の水平スライダにより、日付範囲を指定できます。
- 左側の垂直スライダにより、平均デフォルト スコアの範囲を指定できます。

デフォルトで表示される日付範囲は、最も早い適用状況スキャンのスナップショットの日付から、最新のスナップショットの日付までです。デフォルトでは、平均スコアの範囲は 0 ～ 100 です。次の図では、日付とスコアの両方の範囲がスライダによって制約されています。

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。

実行された日次の適用状況スキャンのスナップショットが 3 回よりも少ない場合や、デバイスがまだスキャンされていない場合、このペインにデータは表示されません。

履歴データの収集を開始した直後でも、グリッド表示に切り替えてそのデータを表示できます。このペインのグリッド表示は、各ベンチマーク バージョンの日次平均デフォルト スコアを示します。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。

スライダを使用したり、一部のベンチマーク バージョンを非表示にしたりしてグラフに表示されるデータ範囲を限定すると、グリッド表示には、そのカスタマイズに応じて制限されたデータ セットのみが表示されるようになります。

環状矢印アイコンをクリックしてグラフをリフレッシュすると、グラフは初期状態に戻ります。スライダは全範囲の位置に戻り、すべての使用可能なデータとすべてのベンチマーク バージョンが表示されます。

このペインの**レポートの起動** ボタンをクリックすると、[適用状況評価履歴] レポートが表示されます。このレポートには、スキャン結果があるすべてのプロファイルが表示されます。各プロファイルの平均スコアが表示されます。

関連トピック：

77 ページの「ダッシュボードの使用」

110 ページの「適用状況管理ダッシュボード」

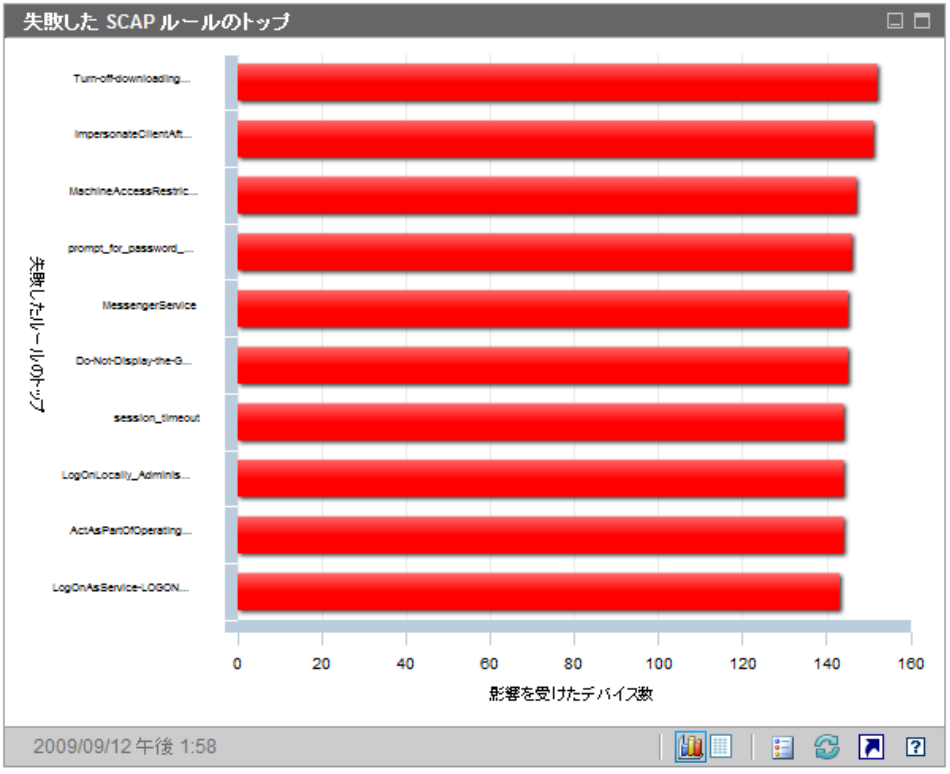
49 ページの「セキュリティと適合性の管理」

失敗した SCAP ルールのトップ

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 27　　失敗した SCAP ルールのトップ



グラフの色付き棒の 1 つをクリックすると、新しいブラウザ ウィンドウが開き、[SCAP 適用状況規則 (CCE 別)] レポートが表示されます。レポートは、クリックした棒に対応するベンチマーク、バージョン、プロファイル、および規則 ID によっ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、規則に関連付けられているベンチマーク、バージョン、およびプロファイルを示します。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。また、レポートは、クリックしたグリッド表示の行に対応するベンチマーク、バージョン、プロファイル、および規則 ID によってフィルタされます。

このペインの**レポートの起動**  ボタンをクリックすると、[失敗した SCAP ルールのトップ] レポートが表示されます。このレポートには、失敗したデバイス数が最も多い上位 10 件の規則が表示されます。これはフィルタされません。

関連トピック：

77 ページの「ダッシュボードの使用」

110 ページの「適用状況管理ダッシュボード」

49 ページの「セキュリティと適合性の管理」

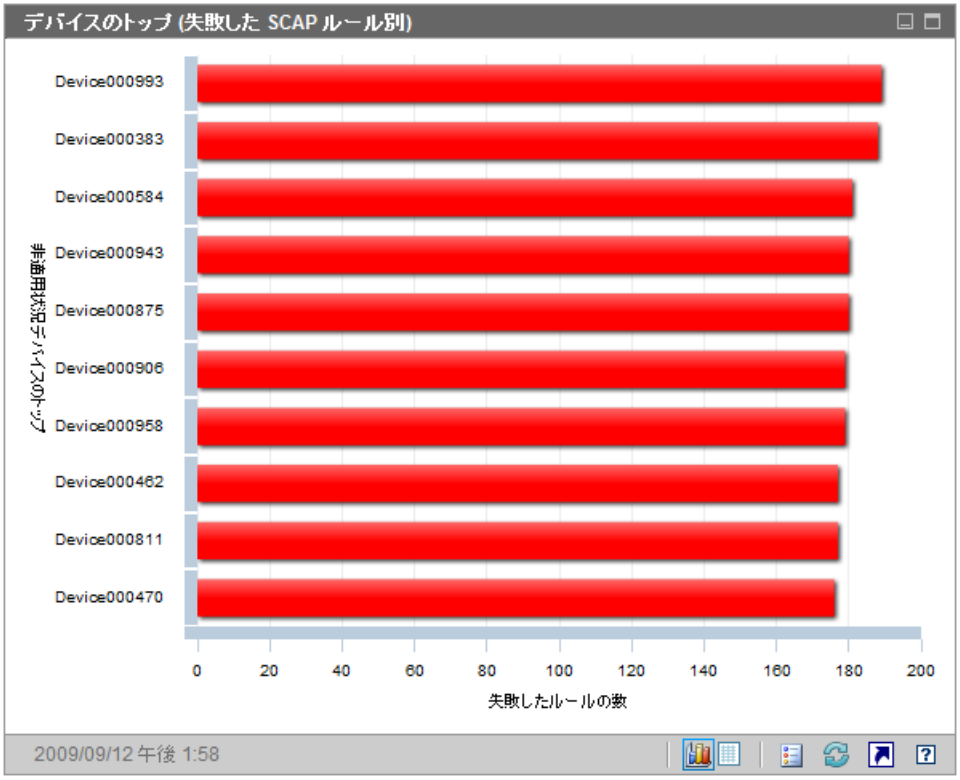
失敗回数の多いデバイス (SCAP ルール別)

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) の失敗回数が最も多い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。

各棒は、特定のデバイスの特定のベンチマーク、バージョン、およびプロファイルのスキャン結果を表しています。詳細を表示するには、グラフの色付き棒の 1 つにカーソルを置きます。

各棒は各ベンチマーク、バージョン、およびプロファイルに対応しているため、このペインに同じデバイスが複数回表示される場合があります。

図 28　　失敗回数の多いデバイス (SCAP ルール別)



グラフ内の色付き棒のいずれかをクリックすると、新しいブラウザ ウィンドウが開き、詳細なレポートが表示されます。レポートは、クリックした棒に対応するデバイス、ベンチマーク、バージョン、およびプロファイル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 [適用状況スキャン済みデバイス] 部分には、このデバイスのベンチマーク、バージョン、およびプロファイル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、このベンチマーク、バージョン、およびプロファイルに関連付けられているすべての規則が表示されます。

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 [適用状況スキャン済みデバイス] レポートが表示されます。レポートは、このベンチマーク、バージョン、およびプロファイルの最新スキャン結果を示すためにフィルタされます。

このペインの**レポートの起動**  ボタンをクリックすると、[上位の SCAP 非コンプライアント デバイス] 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。

関連トピック：

77 ページの「ダッシュボードの使用」

110 ページの「適用状況管理ダッシュボード」

49 ページの「セキュリティと適合性の管理」

セキュリティ ツール管理ダッシュボード

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

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

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

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

セキュリティ ツール管理ダッシュボードには、エグゼクティブ ビューと操作ビューの 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。

- 125 ページの「セキュリティ製品のステータス」
- 127 ページの「セキュリティ製品の概要」

操作ビューには、次の情報ペインがあります。

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

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、373 ページの「ダッシュボード」を参照してください。

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

管理対象デバイス – 各種セキュリティ製品の情報を収集する HPCA セキュリティ ツールのサービスに付与されたデバイスの数

スキャン済みデバイス – 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、65 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 12　　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 12　　セキュリティ ツールの検出状態

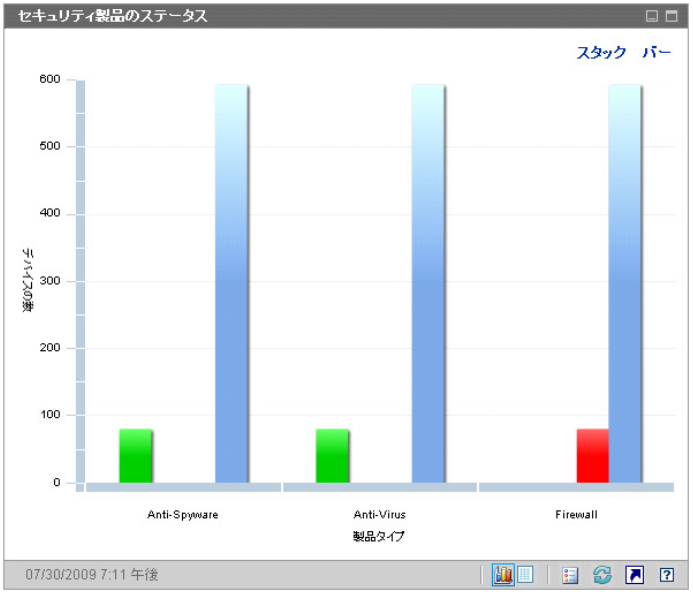
色		間隔
	赤	製品が検出されなかった。
	青	不明

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

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

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

図 29　　セキュリティ製品ステータス ペイン



マウス カーソルを色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。

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

このペインのグリッド表示には、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：

77 ページの「ダッシュボードの使用」

124 ページの「セキュリティ ツール管理ダッシュボード」

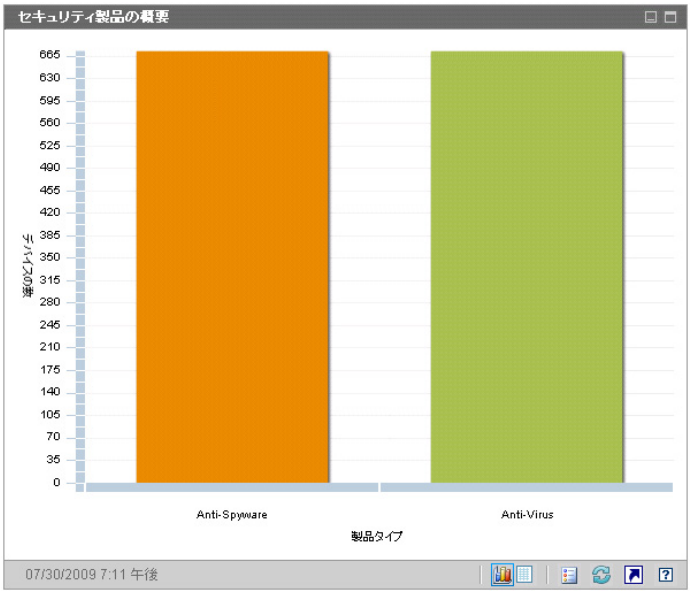
49 ページの「セキュリティと適合性の管理」

セキュリティ製品の概要

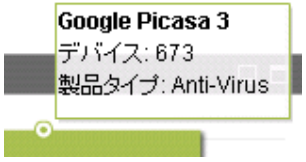
このペインのグラフ表示には、管理対象クライアント デバイスで検出された特定のセキュリティ製品が表示されます。垂直軸はそれぞれの製品が検出されたデバイスの数を示し、水平軸は検出されたセキュリティ ツールのタイプを示します。

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 30　　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。



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

このペインのグリッド表示には、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：

77 ページの「ダッシュボードの使用」

124 ページの「セキュリティ ツール管理ダッシュボード」

49 ページの「セキュリティと適合性の管理」

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 (計数) 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。

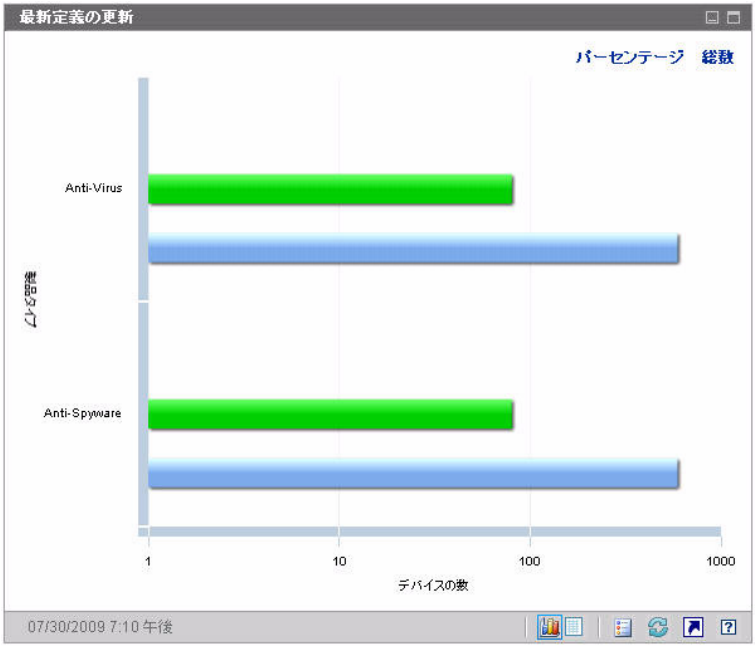
表 13　　更新間隔

色		間隔
	赤	4 週間を超える
	黄色	2 ～ 4 週間
	緑	2 週間未満
	グレー	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 31　　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。注：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。

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

関連トピック：

77 ページの「ダッシュボードの使用」

124 ページの「セキュリティ ツール管理ダッシュボード」

49 ページの「セキュリティと適合性の管理」

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 (計数) またはパーセンテージの形式で表示できます。棒の色は、次の更新間隔を表します。

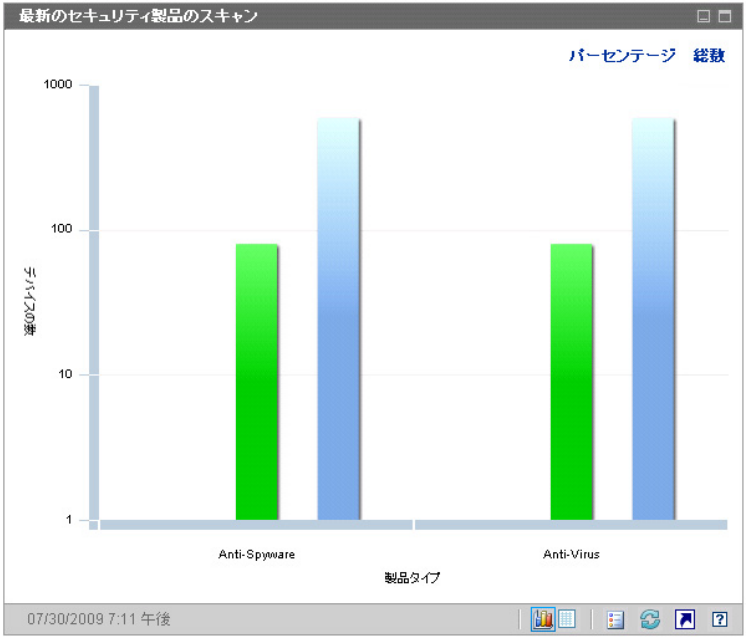
表 14　　スキャン間隔

色		間隔
	赤	4 週間を超える
	黄色	2 ～ 4 週間
	緑	2 週間未満
	グレー	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 32　　最新のセキュリティ製品のスキャン



このペインのグリッド表示には、同じ情報がテーブル形式で表示されます。注：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。

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

関連トピック：

77 ページの「ダッシュボードの使用」

124 ページの「セキュリティ ツール管理ダッシュボード」

49 ページの「セキュリティと適合性の管理」

パッチ管理ダッシュボード

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

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

- 133 ページの「ステータス別デバイス適用状況」
- 135 ページの「ブリティン別デバイス適用状況」

操作ビューには、次の情報ペインがあります。

- 137 ページの「HP Live Network Patch Manager アナウンスメント」
- 138 ページの「ステータス別デバイス適用状況」
- 139 ページの「Microsoft セキュリティ ブリティン」
- 140 ページの「最も脆弱性の高い製品」

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。373 ページの「ダッシュボード」を参照してください。

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

ステータス別デバイス適用状況

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。

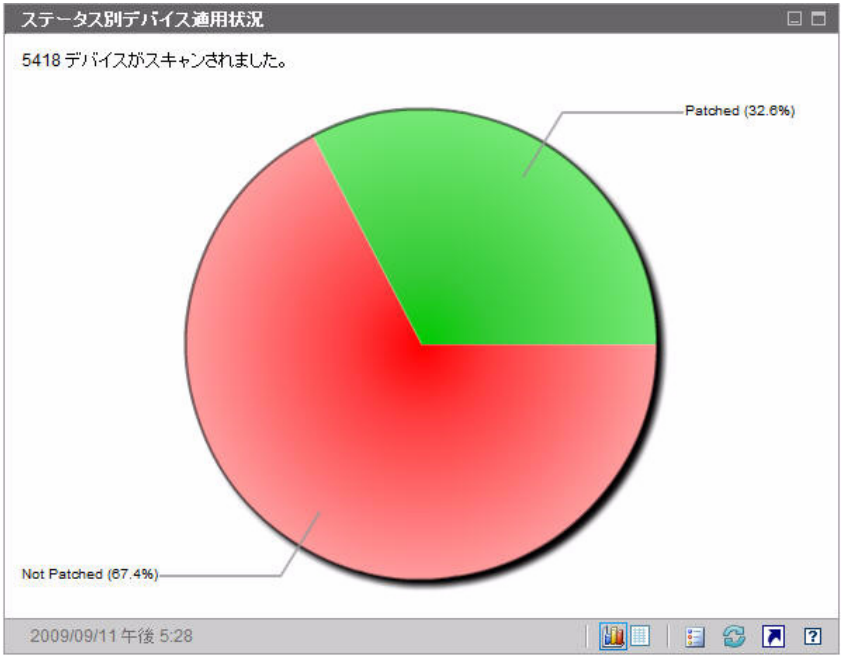
- パッチ適用済み (緑)
- パッチ未適用 (赤)

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

表 15　　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	操作ビュー
パッチ適用済み	パッチ適用済み 警告
パッチ未適用	パッチ未適用 再起動の保留 その他

図 33　　ステータス別デバイス適用状況



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

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

このペインのグリッド表示には、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。

ブリティ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 ブリティ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。

特定のブリティンが 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ィ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。

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

図 34　　ブリティン別デバイス適用状況

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

グリッド表示には、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。

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

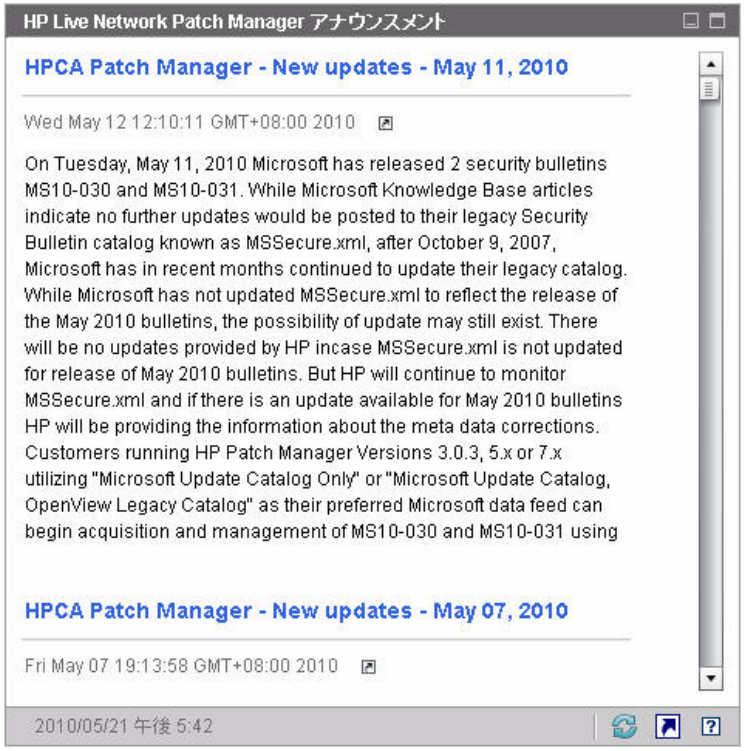
初期状態のテーブルは、[パッチ未適用] を基準にソートされています。ソートパラメータを変更するには、対応するカラム見出しをクリックします。

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

HP Live Network Patch Manager 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 Patch Manager アナウンスメントが表示されます。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。第 5 章、「HPCA および HP Live Network」を参照してください。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、373 ページの「ダッシュボード」を参照してください。

図 35　　HP Live Network Patch Manager 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 認証サーバーの場所を変更できます (373 ページの「ダッシュボード」を参照)。また、プロキシ サーバーを有効にする必要が生じる場合もあります (312 ページの「HP Live Network サーバーへの接続の設定」および 291 ページの「プロキシ設定」を参照)。

関連トピック :

77 ページの「ダッシュボードの使用」

133 ページの「パッチ管理ダッシュボード」

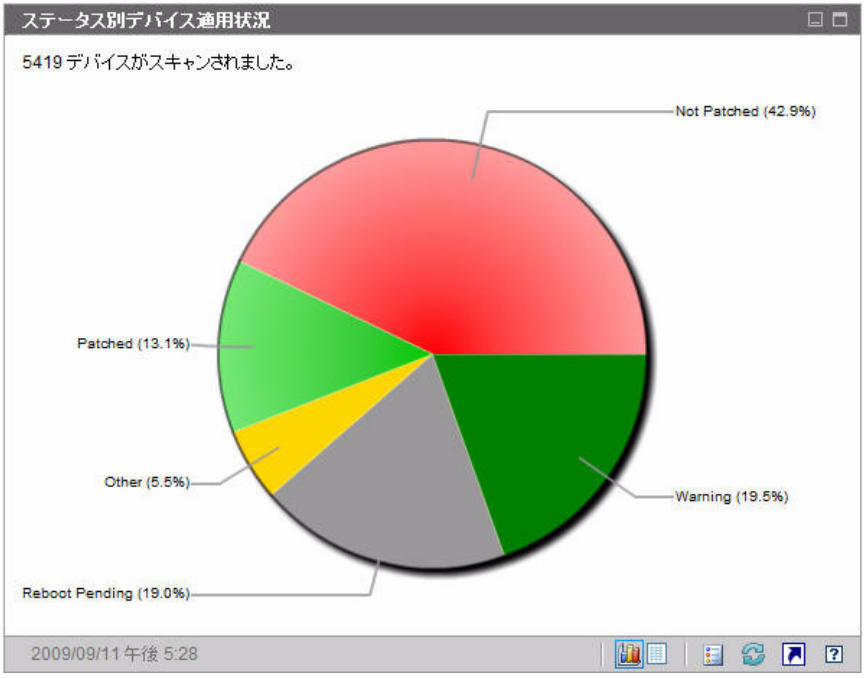
ステータス別デバイス適用状況

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 (薄いグレー)
- 警告 (深緑)
- その他 (黄)
- 適用できません (濃いグレー)

図 36　　ステータス別デバイス適用状況 (操作ビュー)



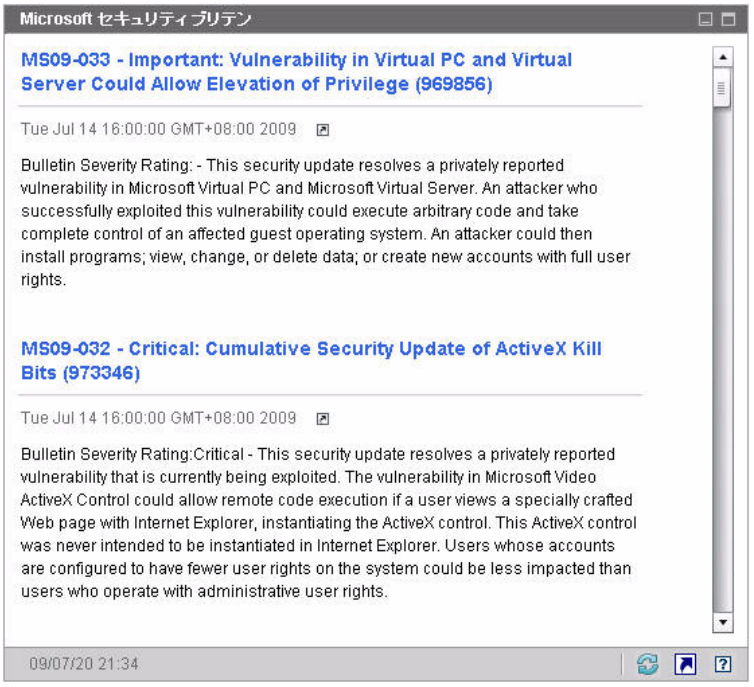
円グラフ内の色付きの扇形をクリックすると、新しいブラウザ ウィンドウが開き、フィルタされたレポートが表示されます。レポートには、クリックした扇形に対応するパッチ適用状況ステータスのすべてのデバイスが表示されます。

グリッド表示には、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 ブリティン

このペインには、最新の Microsoft セキュリティ ブリティンが表示されます。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 (373 ページの「ダッシュボード」を参照してくだい)。

図 37　　Microsoft セキュリティ ブリティン



特定のブリティンの詳細を表示するには、ブリティ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。有効化するには、373 ページの「ダッシュボード」を参照してください。

このペインのグラフ表示には、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ィンが 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

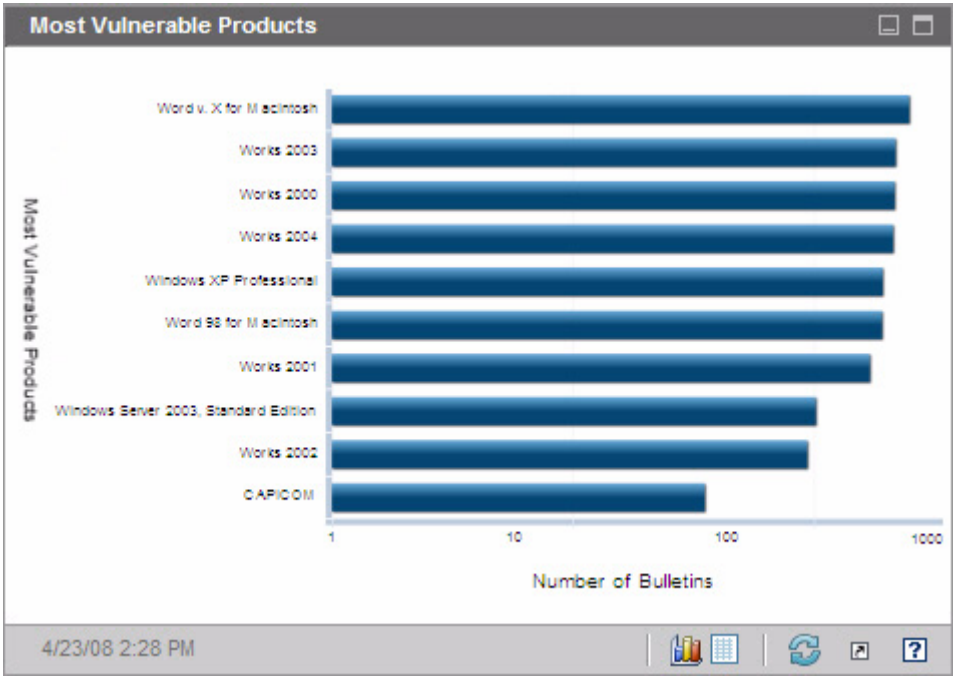
— 50 個の管理対象デバイスでそれらのパッチのうち 1 件のみを必要としている

ABC のブリティンの数 = (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ィンの数が 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 38　　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 – 特定の製品の適用可能なすべてのデバイスでパッチが適用されていないブリティンの数
- 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

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

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

5 HPCA および HP Live Network

概要

HP Live Network は、HPCA の最新のコンテンツを取得できる登録契約サービスです。HPCA ライセンスに応じて、HP Live Network から使用できるコンテンツのタイプが異なります。

HPCA Enterprise では、設定プロファイルの最新のコンテンツ、セキュリティおよび適合性管理の最新の定義およびスキャナを提供します。Live Network を介してレポートの強化機能も配布できます。入手できる場合、HP Live Network 更新を実行して、これらの強化機能を取得できます。Live Network サイトから最新のレポートをダウンロードしても、レポートに実行したカスタマイズは上書きされません。

更新されたコンテンツを取得するには、該当するコンテンツの有効な Live Network の登録認証情報を含むアクティブな HP Software サポートの連絡先が必要です。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 を設定できます。

登録契約に付随する HP Live Network コンテンツ サーバーの URL は、HPCA Console の [設定] タブの Live Network 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。登録契約に付随する URL を使用してください。詳細については、312 ページの「Live Network」を参照してください。

HP Live Network 登録契約の購入についての詳細は、次の Web サイトにある HP BSA Essentials Network Security & Compliance Service for Client Automation にアクセスしてください。

https://h20109.www2.hp.com/

このサイトを表示するには、HP パスポート認証情報を入力する必要があります。

ライセンスの要件

HP Live Network から最新のコンテンツを取得するには、次のアイテムが必要です。

- HPCA Enterprise Edition のライセンス
- HPCA Security Manager および HPCA Compliance Manager のライセンス
- Live Network 登録の認証情報を持つアクティブな HP Software サポートの連絡先
- 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。適用可能なコンテンツはダウンロードおよび使用には使用できません。

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。

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 登録が必要です。

HP Live Network コンテンツの更新

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。

Live Network のコンテンツを取得するには、HP Live Network コネクタ を使用して、HP Live Network コンテンツの更新方法を理解している必要があります。

HP Live Network コネクタ

HP Live Network のコンテンツにアクセスするには、HP Live Network 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 登録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。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。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。145 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、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 コンテンツの読み込みを管理します。

HPCA 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)、通常、次のアクションが実行されます。

1 コンテンツが一時ディレクトリにコピーされます。

2 コンテンツは HPCA データベースに読み込まれます。これらのアクションにより収集されたデータがデータベースによって処理され、HPCA が関連サービスを配布し、詳細レポートを作成できます。

3 HPCA Console は関連する UI コンテンツを使用して更新されます。

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

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、[インフラストラクチャ管理] 領域を展開し、**[Live Network]** をクリックします。

2 [HP Live Network コネクタ] ボックスの右側にある **[ダウンロード]** リンクをクリックします。新しいブラウザ ウィンドウが開き、HP Live Network サイトが表示されます。そこから LNC の実行可能ファイルをダウンロードできます。ログインするには、HP Live Network 登録契約のユーザー名とパスワードが必要です。

3 LNC をダウンロードしてインストールするには、HP Live Network サイトの指示に従ってください。

LNC を元のインストール場所以外の場所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場所は次のとおりです。

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 Server:

`<InstallDir>\HPCA\LiveNetwork\lnc\bin\live-network-connector.bat`

HP Live Network コンテンツの更新方法

HP Live Network 登録 Web サイトから HP Live Network コンテンツを更新するには、次の手順を実行します。

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

  詳細な手順については、240 ページの「Live Network」を参照してください。

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

  手順については、521 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。

最新のコンテンツ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を明示的に付与してください。

HP Live Network からダウンロードしたサービスの表示名は山かっこ (< >) で囲まれており、Live Network サイトの HP がサポートするサービスとして一意に特定できます。使用環境でサービスを変更する場合は、HP Live Network コンテンツを次回更新するときに変更が失われる可能性があることに注意してください。

6 Enterprise の管理

[管理] 領域には、使用環境のクライアント デバイスの管理に使用するツールが配置されています。この章のは、次の各トピックで構成されています。

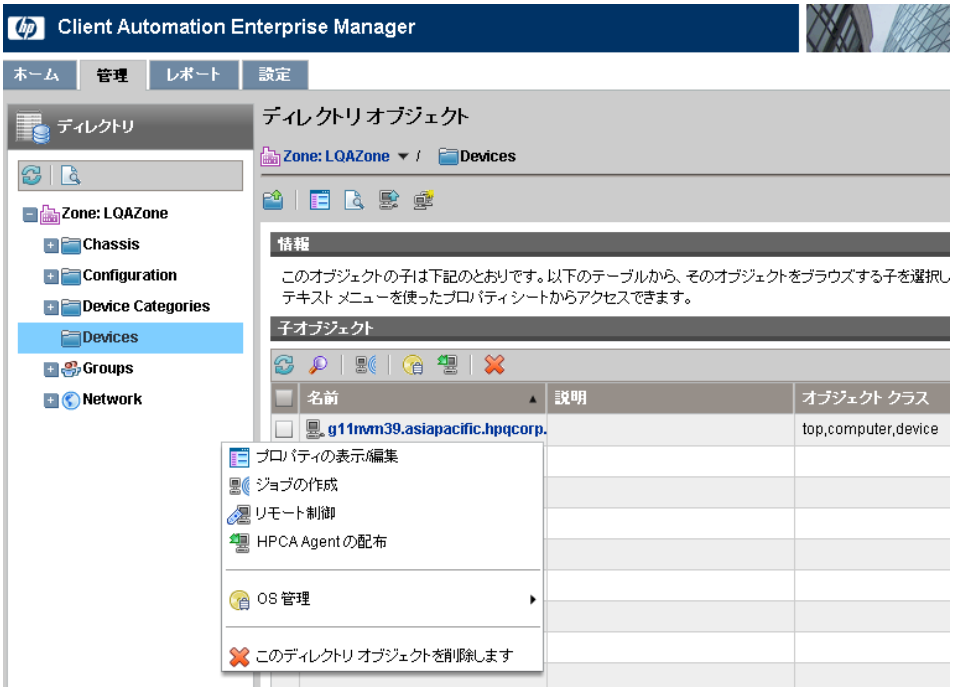
ディレクトリ オブジェクト

[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 サービスのオブジェクトを確認できます。297 ページの「ディレクトリ サービス」を参照してください。たとえば、オブジェクトのプロパティを表示して編集したり、ディレクトリを検索したり、デバイスをインポートしたり、新しいグループを作成したりできます。

左のナビゲーション ツリーにあるディレクトリ オブジェクトをクリックすると、内容ペインにそのディレクトリ オブジェクトの子またはメンバーのリストが表示されます。内容ペインには、選択したディレクトリ オブジェクトのタイプに応じて、子またはメンバーのいずれかが表示されます。ディレクトリ オブジェクトがコンテナ タイプである場合は、ディレクトリ オブジェクトの子が表示されます。ディレクトリ オブジェクトがグループ タイプである場合は、ディレクトリ オブジェクトのメンバーが表示されます。

リストにある子オブジェクトまたはメンバー オブジェクトの名前の上にカーソルを置くと、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 39　　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 16　　ドロップダウン メニューに表示されるアクション

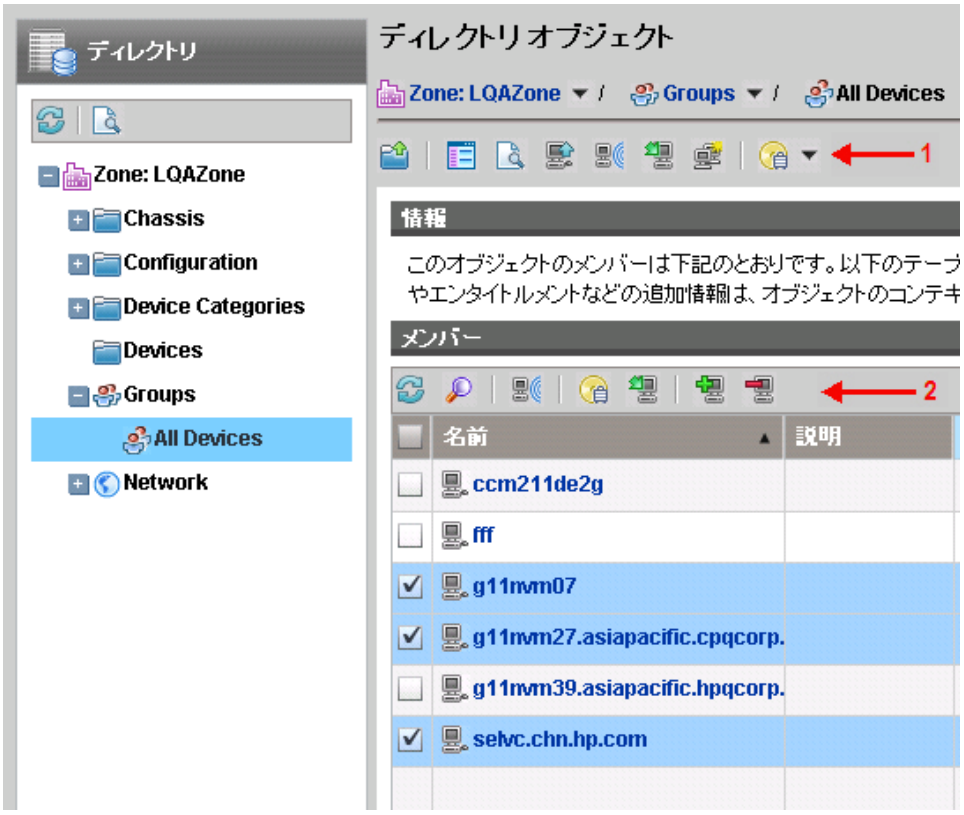
アイコン	アクション	説明
	プロパティの表示 / 編集	新しいブラウザ ウィンドウで、この子オブジェクトのプロパティを表示または編集する。151 ページの「ディレクトリ オブジェクト ビュー」を参照してください。
	ジョブの作成	このオブジェクトの通知ジョブまたは DTM ジョブを作成する。174 ページの「ジョブを管理する」を参照してください。
	リモート制御	管理対象デバイスにリモート アクセスする。196 ページの「デバイスのリモート制御」を参照してください。
	HPCA Agent の配布	このデバイスに HPCA Agent を配布し、HPCA によって管理できるようにする。172 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。203 ページの「オペレーティング システムの管理」を参照してください。
	アウトバンドの詳細を表示	Intel vPro を搭載するデバイスまたは DASH が有効なデバイスのアウトバンドの詳細を表示する。214 ページの「アウトバンドの詳細の表示」を参照してください。
	このディレクトリ オブジェクトを削除	HPCA データベースからこのオブジェクトを削除する。170 ページの「デバイスのインポート」を参照してください。

ディレクトリ オブジェクト ビューには、2 種類のツールバーがあります。

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

153 ページの図 40 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 40　　ディレクトリ オブジェクト ビューのツールバー

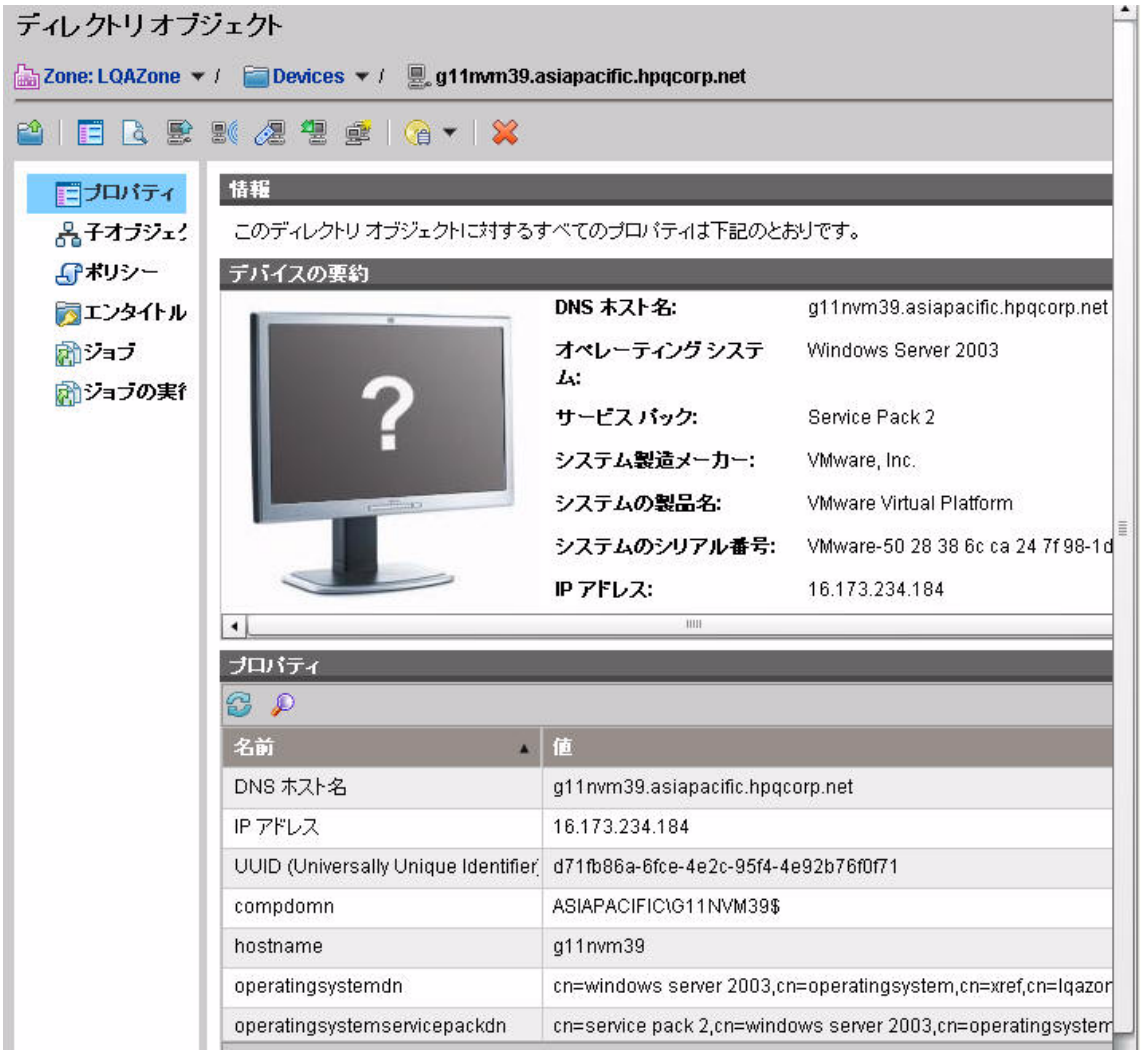


この例では、上側のツールバー (1) が全デバイス グループに関連し、下側のツールバー (2) がグリッドで選択した子 (またはメンバー) に関連しています (この場合は、g11nvm07、g11nvm27.asiapacific.cpqcorp.net と selvc.chn.hp.com)。

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 (154 ページの図 41 を参照)。

図 41　　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。内容ペインで子オブジェクトを参照するには、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。
- **[資格]** 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、176 ページの「ジョブおよびジョブの実行」を参照してください。
- **[仮想マシン]** をクリックすると、サーバー上に存在するすべての仮想マシンのリストを表示できます。このリンクが表示されるのは、選択したオブジェクトが VMware ESX Server である場合のみです。詳細については、189 ページの「仮想マシンの管理」を参照してください。

オブジェクトの検索

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

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

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

ディレクトリ オブジェクトを検索するには

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

2 [ディレクトリ検索] ボックスで、次のパラメータを定義できます。

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

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

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

4 [**リセット**] をクリックして、新しい検索を開始します。

ディレクトリ ポリシーの管理

これまで説明したように、HPCA Console の [管理] タブではディレクトリ オブジェクトのポリシーを作成したり、付与資格を表示したりできます。

ポリシーとは

ポリシーは、ユーザーと管理対象デバイスが使用できるサービスを定義します。アプリケーション サービスの付与資格の指定を表します。ポリシーは、どのパッケージにどの管理対象デバイスを割り当てるかを示します。パッケージは、配布可能なソフトウェアやデータの単位です。通常、サービスをユーザーにマッピングするには、複数のユーザーを作成してグループに割り当て、それらのグループにサービスを割り当てます。これらのサービスに関連付けられているポリシー情報は、ユーザー、グループ、またはコンピュータで管理するデータを決定します。また、Agent 用に配布および管理するサービスを決定します。ポリシー ベース管理の HPCA モデルでは、外部の Active Directory に接続してポリシー資格を定義できます。

ポリシーのタイプとしくみ

ディレクトリ オブジェクトのポリシーの管理を開始する前に、ポリシーのタイプ、複数のポリシー タイプを併用してディレクトリ オブジェクトで実際に解決されるポリシーの値を決定する方法について理解しておく必要があります。

ポリシーには 3 つのタイプがあります。

ポリシー タイプは、サービスに対するオブジェクトの付与資格を定義する、実際にアクセス権を付与するポリシーです。

デフォルト ポリシー タイプは、アクセス権の付与も拒否も行なわないポリシーです。ただし、ディレクトリ オブジェクトにアクセス権が付与されている場合は、デフォルト ポリシーの値がオブジェクトに割り当てられているポリシーのデフォルト テンプレートとして使用されます。

上書きポリシー タイプは、アクセス権の付与も拒否も行なわないポリシーです。ただし、ディレクトリ オブジェクトにアクセス権が付与されている場合は、上書きポリシーの値が実際にアクセス権を付与するポリシーの対応する属性をすべて上書きします。

特定のアプリケーションでは、ポリシーの解決に 2 つ以上のデフォルト ポリシーが設定されている場合があります。この場合、デフォルトは pri 属性に基づいて最下位から最上位までランク付けされます。この属性の数値が低いほど優先度は高くなります。同様に、上書きポリシーにも適用されます。

Configuration Server に戻される実際の結果として得られるポリシーは、順序付けた上書きが実行される論理セットの集合です。つまり、同じ名前の属性は置き換えられます。これは、次のように実行されます。

1 優先度の最も低いデフォルトから最も高いデフォルト (0...n のオカレンス)

2 実際にアクセス権を付与するポリシー (常に 1 つ)

3 優先度の最も低い上書きから最も高い上書き (0...n のオカレンス)

ポリシー解決の例

このセクションでは、サービスの付与資格をポリシーに設定しているディレクトリ オブジェクトにデフォルト ポリシーおよび上書きポリシーが割り当てられている場合に、Configuration Server に実際に戻されるポリシーを示します。

例 1: 単純な上書き

- policy: Firefly <version=7 mode=typical>
- override: Firefly <version=8>
- OUTCOME: Firefly <version=8 mode=typical>

例 2: 単純なデフォルト

- policy: Firefly <mode=typical>
- default: Firefly <version=7>
- OUTCOME: Firefly <version=7 mode=typical>

例 3: デフォルトおよび上書き

- default: Firefly <mode=typical>
- policy: Firefly <version=7 issue=4>
- override: Firefly <version=8 mode=complete>
- OUTCOME: Firefly <version=8 issue=4 mode=complete>

例 4: 複数のデフォルトと複数の上書き

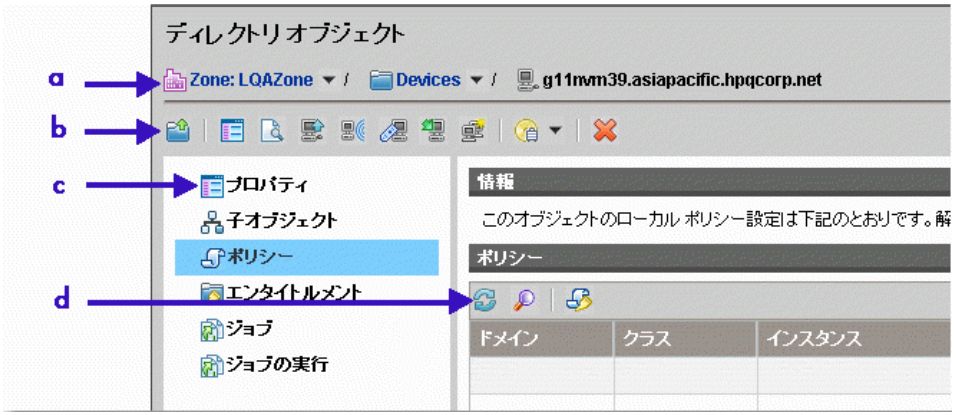
- default: Firefly <version=7> - Note: pri defaults to 10
- default Firefly <version=6 pri=5>
- policy: Firefly <mode=typical>
- override: Firefly <mode=complete> - Note: pri defaults to 10
- override: Firefly <mode=typical pri=5>
- OUTCOME: Firefly <version=6 mode=typical>

デフォルトも上書きも、対象にアクセス権を付与しないポリシー解決には影響を及ぼしません (前例の Firefly)。デフォルトおよび上書きは、アプリケーションへのアクセス権が付与されているポリシー オブジェクトにのみ影響します。また、これらのポリシーが与える唯一の影響は、Configuration Server で対象オブジェクトを解決するときに提示される POLICY オブジェクトに関連する一連の属性を変更できることでそのアクセスの定義を詳細に設定することです。

ディレクトリ オブジェクトのポリシーの管理方法

[ディレクトリ オブジェクトのプロパティ] ウィンドウでは、左側のナビゲーション ツリーの **[ポリシー]** リンクを選択して、ディレクトリ 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 42　　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：

- 親オブジェクトの参照
- 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

ポリシー管理ウィザードの起動 (ドロップダウン メニューでポリシー タイプを選択できる)

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

c オブジェクト リンク (153 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

左側のナビゲーション ツリーにある [**ポリシー**] リンクを選択すると、[ディレクトリ オブジェクト プロパティ] ウィンドウに 3 つのタブが表示されます。これらのタブでは、ポリシーの表示および割り当て、ポリシーへのデフォルトおよび上書きの設定、ポリシーの継承に影響を与えるのその他のオブジェクトとの関係の作成、ポリシー解決時の Policy Server の動作を決定する解決オプションの設定を実行できます。

[ポリシー] リンクをクリックすると、HPCA Console によってパーミッションが確認されます。書き込みパーミッションがない場合は、ツールバーに**ポリシー管理ウィザードの起動**アイコンが表示されません。

これらのタブで実行できるアクションは、次のセクションで説明します。この例では、1 つのデバイスに 1 つのポリシーを作成します。160 ページの図 42 では、[ディレクトリ オブジェクトのプロパティ] ウィンドウのさまざまなセクションを示します。この図では、タスクを実行するときに管理コンソールのどの場所にいるかがわかります。

ポリシーの表示および作成の手順を確認するため、[ディレクトリ オブジェクトのプロパティ] ウィンドウに進み、次の手順を実行します。

1 **[管理]** タブで、[ディレクトリ] の下にあるディレクトリ構造を展開します。使用可能なディレクトリ サービスのリストが表示されます。

2 展開するディレクトリ サービスをクリックします。この例では、**[デバイス]** をクリックしています。子のリストが内容ペインに表示されます。

3 デバイスを操作するには、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。

4 新しいブラウザ ウィンドウの左側のナビゲーション ツリーで、**[ポリシー]** リンクをクリックします。

例のように、選択しているディレクトリ オブジェクトは単一のデバイスです。この単一デバイスのためのポリシーを作成します。

割り当て

[ディレクトリ オブジェクト ポリシー] ウィンドウの **[割り当て]** タブで、ディレクトリ オブジェクトに割り当てられているポリシーのタイプを確認できます。

157 ページの「ポリシーのタイプとしくみ」で説明したように、オブジェクトに割り当てられるポリシーには、ポリシー、デフォルト ポリシー、上書きポリシーの 3 つのタイプがあります。次のポリシー タイプの割り当て手順を実行すると、追加サービスの付与資格をディレクトリ オブジェクトに設定できます。

ディレクトリ オブジェクトにポリシーを割り当てるには

1 [ディレクトリ オブジェクト] ツールバーにある**ポリシー管理ウィザード**  アイコンのドロップダウン メニューから **[ポリシー管理ウィザードの起動 (ポリシー)]** を選択します。画面の右側には、特定のサービス ドメインで使用可能なディレクトリ サービスのリストが表示されます。

このウィザードでは、HPCA Configuration Server が提供するサービスの付与資格をグループ、ユーザーなどとしてディレクトリ オブジェクトに設定できます。右側にあるツリーには、このディレクトリ オブジェクトに現在割り当てられているサービスのリストが表示されます。このテーブルから新しいサービスを選択したり、ツリーから既存のサービスを削除したりして、ポリシー設定を変更できます。

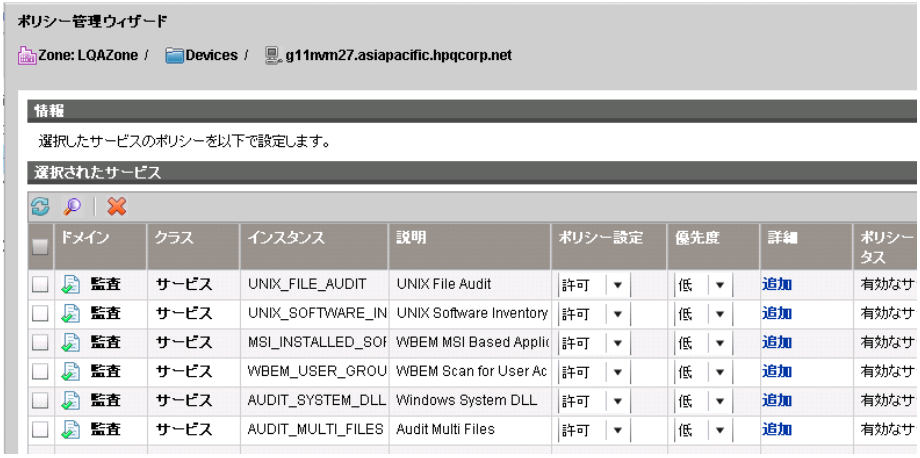
2 [サービス ドメイン] フィールドのドロップダウン メニューから、サービスを選択するサービス ドメインを選択します。

3 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。

4 **[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。

5 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。ウィンドウが開き、選択したサービスが表示されます。

6 このウィンドウでは、選択したサービスのポリシー設定、優先度、属性を設定します。次のスクリーン ショットには、Audit ドメインの 2 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。

— **[属性と式]** 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 Guide を参照してください。

> **[属性と式]** 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。

7 ポリシーを設定したら、**[次へ]** をクリックします。ウィンドウが開き、選択したサービスの要約情報が表示されます。

8 設定の要約情報を確認します。**[適用]** をクリックして、変更を保存します。

[閉じる] をクリックして、ウィザードを終了します。新しく作成されたポリシーが **[割り当て]** タブのポリシーの表に表示されます。また、**[エンタイトルメント]** タブをクリックすると、付与資格テーブルにもポリシーが表示されます。

ディレクトリ オブジェクトにポリシーのデフォルトを割り当てるには

ディレクトリ オブジェクトにポリシーのデフォルトを割り当てるには、162 ページの「ディレクトリ オブジェクトにポリシーを割り当てるには」と同じ手順を実行します。ただし、[ディレクトリ オブジェクト] ツールバーにある**ポリシー管理ウィザード**  アイコンのドロップダウン メニューから **[ポリシー管理ウィザードの起動 (PolicyDefault)]**  を選択した場合は除きます。

ディレクトリ オブジェクトにポリシーの上書きを割り当てるには

ディレクトリ オブジェクトにポリシーの上書きを割り当てるには、162 ページの「ディレクトリ オブジェクトにポリシーを割り当てるには」と同じ手順を実行します。ただし、[ディレクトリ オブジェクト] ツールバーにある**ポリシー管理ウィザード**  アイコンのドロップダウン メニューから **[ポリシー管理ウィザードの起動 (PolicyOverride)]**  を選択した場合は除きます。

関係

[関係] タブでは、オブジェクト間にリンクを設定し、リンク先のオブジェクトからポリシーを継承できます。たとえば、登録契約者が組織単位 (OU) の子ではないが、Active Directory の OU に割り当てられているポリシーを継承する必要があるとします。このためには、その OU にリンクしているデバイスにポリシー関係を追加して、OU に付与されているポリシーを継承します。デバイスがポリシー関係を使用してグループにリンクしている場合、そのグループのメンバーでない場合でも、デバイスはそのグループに付与されているポリシーを継承します。ポリシー関係の通常の使用方法の 1 つに、ポリシーが割り当てられている 1 つ以上のグループに OU 全体をリンクするという方法があります。OU は LDAP のグループのメンバーになることはできないため、このタイプのリンクがポリシー関係を使用できる唯一の方法です。

この機能は、ディレクトリ モデルでは慎重に使用してください。この機能の主要な目的は、親—子関係または「memberOf」関係の形式で存在するのではない限り、また、そのような関係が複数の動的な条件に基づいて制約される関係でない場合は、2 つのオブジェクト間のポリシー関係を表すことです。

次の例では、別のディレクトリ オブジェクトに単一のデバイスを追加して、単一のデバイスにポリシー関係を追加します。

オブジェクト間の関係を作成するには

1 **[関係]** タブを選択します。選択したデバイスのポリシーの関係がテーブルに表示されます。最初は、ポリシーの関係を追加するまでこの表は空白です。

2 ポリシーの関係を追加するには、[ポリシー管理] ツールバーにある **[ポリシー関係の追加]**  アイコンをクリックします。[ポリシー関係の追加] ウィンドウが表示されます。

3 検索パラメータを使用するか、または現在選択されているデバイスにリンクするディレクトリ オブジェクトを選択します。

4 単一デバイスのリンク先である各リンク可能なオブジェクトの横にあるボックスをオンにします。

5 **[追加]** または **[追加して閉じる]** をクリックして、ディレクトリ オブジェクトの関係を現在選択されているデバイスに追加します。**[追加して閉じる]** をクリックすると、関係が追加され、ウィザードが終了します。

6 [実行ステータス] ポップアップ ウィンドウの **[閉じる]** をクリックして、ウィンドウを閉じます。関連するオブジェクトのポリシー付与資格がすべて、元々選択されていたデバイスに継承されます。

新しく選択されたディレクトリ オブジェクトが、元々選択されていたデバイスのポリシー関係テーブルに表示されます。また、選択されているデバイスの [エンタイトルメント] ページにリンク先のディレクトリ オブジェクトのポリシーが表示されるようになります。

解決

[解決] タブでは、ポリシーの解決方法を調整できます。たとえば、特定のオブジェクトのポリシー解決の範囲を限定する必要があるとします。これを実行するには、このタブに表示されているポリシー解決オプションを使用します。これらのオプションは、単一の値の整数として実装されています。Policy Server がポリシーを解決するときにこれらの整数の論理 OR 演算を行い、必要な動作を生成できます。

このようなフラグは慎重に使用してください。ポリシー モデルの明確さや機能に重大な影響を与える可能性があります。

解決オプションを設定するには

1 **[解決]** タブで、ポリシー解決の決定に使用する解決オプションを選択します。次のオプションから選択できます。

— **分離**：結果に親オブジェクトを含めないよう Policy Manager に指示します。これは、組織内の半自律型単位をサポートする場合に主に使用します。

— **続行**：Policy Server に該当オブジェクトの属性以外はすべて無視するように指示します。**[分離]** オプションが設定されていない限り、親オブジェクトは引き続き処理されます。

— **中断**： ポリシー解決を中断させて、クライアントにその条件を戻すよう Policy Server に指示します。この状況では、クライアント デバイスはポリシーを適用しません。このオプションを使用すると、「変更管理の禁止」を実装して、組織の特定の部分に適用されているポリシーが変更されないようにできます。

— **厳密**:「memberOf」属性を無視し、Policy Flags および Policy Connections のみを処理するよう Policy Server に指示します。

2 **[保存]** をクリックして、ポリシーを更新します。

3 **[閉じる]** をクリックして、ウィザードを終了します。

選択されているデバイスのポリシー モデルでの解決オプションの影響は、選択されているデバイスの付与資格ページには反映されません。

Virtual Desktop Infrastructure のポリシーの管理方法

Virtual Desktop Infrastructure (VDI) の仮想マシン (VM) を管理する場合は、一部のタイプの VM のポリシー管理で特別な注意が必要です。一部のケースでは VM でのサービスが不要であるため、不要なネットワーク トラフィックを生じさせないようにポリシーに VM 上のサービスを拒否させる必要があります。

Patch Service Domain は特殊なケースです。特定のタイプの VM では、これらの仮想デスクトップへのパッチの配布を回避するために拒否するサービスのポリシー設定を設定します。これは、パッチの配布が不要でコストがかかるためです。

次のセクションでは、VDI の背景と、仮想環境の該当タイプでのポリシー付与資格を効率的に設定する方法について説明します。各セクションでは、次の内容について説明します。

- 167 ページの「VDI の概要」
- 167 ページの「Active Directory グループへのクローン デスクトップの追加」
- 168 ページの「クローン デスクトップに対するパッチ サービスを拒否」

VDI の概要

VDI は物理ホスト マシンで Windows XP Professional、Windows Vista、または Linux などの個別のクライアント オペレーティング システムをホストし、仮想化するテクノロジです。VDI の目的は、データ センターでのエンタープライズ デスクトップの配布、セキュリティ保護、および管理を可能にすることです。

VMware View の正式名は Virtual Desktop Infrastructure (VDI) です。このビューは、単一のベース イメージから複数のデスクトップを配布できるリンクされたクローン テクノロジを使用しています。自動化デスクトップ プールでは、リンクされたクローン機能を使用して、単一の親 VM から複数のデスクトップを迅速に配布できます。View Manager は VMware View Composer を使用して、VMware vCenter Server からリンクされたクローン デスクトップを作成し、配布します。

XenDesktop は Citrix の VDI ソリューションです。XenDesktop は、仮想デスクトップ接続の管理および専用またはプールされた仮想デスクトップへのユーザーの割り当てに使用されます。プロビジョニング サービスでは、要求に応じて、単一のデスクトップ イメージから仮想デスクトップを作成してプロビジョニングします。これにより、ストレージの使用率を最適化し、ユーザーがログオンするたびに各ユーザーに元の状態の仮想デスクトップを提供します。Provisioning Services VM テンプレートは、XenDesktop セットアップ ウィザードで VM ベースのプール デスクトップ グループを作成するために使用します。

VMware View を使用して作成したクローン デスクトップ、または XenDesktop を使用して作成した仮想デスクトップは、HPCA Enterprise Console で管理できます。複数のクローン デスクトップを単一の組織単位 (OU) にグループ化して、ポリシーをこの OU に適用し、サービスを拒否できます。この拒否ポリシーは、親 VM には使用できません。親 VM にインストールされているすべてのサービスに、この拒否ポリシーが付与されてしまうためです。VMware View を使用して親 VM からクローン デスクトップを自動的に更新し、親のベース イメージにインストールされたサービスを反映させることができます。

Active Directory グループへのクローン デスクトップの追加

付与資格から除外する必要のある、クローン デスクトップをすべて含む AD のグループを作成する必要があります。そのグループは OU です。この OU は HPCA Enterprise のディレクトリ オブジェクトです。このオブジェクトは、この OU へのパッチ サービスを拒否するポリシーに関連付けることができます。168 ページの「クローン デスクトップに対するパッチ サービスを拒否」を参照してください。

Active Directory でクローン デスクトップの新しいグループを作成するには

1 AD で新しいグループを作成します。

2 クローン　デスクトップをグループに追加します。このグループに追加するクローン デスクトップを検索するときは、デバイスの指定に使用するパターンを使用します。このパターン検索文字列では、グループにクローン デスクトップを追加する作業を簡略化するクローン デスクトップのみを表示します。

3 **[OK]** をクリックします。

ネットワークにさらにクローン デスクトップを追加する場合、必ずこのグループに追加されることを確認します。この確認は自動的には行なわれません。

クローン デスクトップに対するパッチ サービスを拒否

AD に OU を作成したため、この OU に含まれているデバイスへのパッチの取得を効果的に拒否するポリシーを関連付けることができます。

クローン デスクトップに対するパッチ サービスを拒否するには

基本的に、162 ページの「ディレクトリ オブジェクトにポリシーを割り当てるには」で説明している一般的な手順に従います。ただし、この手順、つまり、サービスを*拒否*するデバイスへのポリシーの付与に関する手順では、サービス拒否のために入力する実際の値に注意する必要があります。

1 クローン デスクトップを含む OU ディレクトリ オブジェクトの **[プロパティの表示 / 編集]** を選択します。

2 **ポリシー管理ウィザード** アイコンのドロップダウン メニューから通常のポリシーを追加する **[ポリシー管理ウィザードの起動 (ポリシー)]** を選択します。

3 ポリシー管理ウィザードで、サービス ドメインとして **[パッチ]** を選択します。

4 リストで **DISCOVER_PATCH** サービスおよび **FINALIZE_PATCH** サービスを選択し、**[追加]** をクリックします。

5 **[次へ]** をクリックします。

6 選択されたサービスのリストですべてのサービスを選択し、表示されているすべてのサービスに次の変更を指定します。

— [ポリシー設定] を **[拒否]** に設定

— [優先度] を **[高]** に設定

7 **[次へ]**、**[適用]** の順にクリックして、変更を保存します。

この手順では、クローン デスクトップを含む OU へのパッチ サービスを拒否するポリシーを割り当てました。このポリシーの優先度は高に指定されているため、解決時には、階層内のその他すべてのポリシーに優先してこのポリシーが適用されます。リストの任意のデバイスのポリシー資格リストを確認することで、これを確認できます。

これで、指定の OU に含まれるクローン デスクトップのいずれかでパッチ接続が実行されても、パッチ サービス付与資格が解決されず、パッチはインストールされません。このポリシーは、クローン デスクトップに対して付与されている他のサービスには影響しないため、その他のサービスは解決されます。

OU にクローン デスクトップのみが含まれていることを確認する必要があります。この OU にその他のデバイスが含まれている場合、そのデバイスのパッチ サービスも拒否されます。

どのレベルでもポリシー付与資格を使用してパッチ サービスを拒否できます。つまり、コンテナ、OU またはデバイスのレベルでパッチ サービスを拒否できます。

重要なのは、すべてのデバイスではなく、必要なデバイスのみにポリシーが適用されるように、階層の正しいレベルでポリシーを適用することです。

サービス情報

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

使用可能なサービスを表示するには

1. **[管理]** タブで、**[サービス]** をクリックします。使用可能な Configuration Server Database ドメインの一覧が表示されます。
2. 表示するサービスを含むドメインをクリックします。
3. 表示される使用可能なサービスの一覧を絞り込むには、**[フィルタ入力の表示 / 非表示]** ボタンをクリックしてフィルタ オプションを表示します。
4. 詳細を表示するサービスをクリックします。
   - **[カタログ]** タブには、Configuration Server Database (CSDB) のサービスの属性が表示されます。
   - [**レポート**] タブに、サービスについての要約レポートが表示されます。

デバイスのインポート

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

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

デバイスをインポートするには

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

2  (デバイス インポート ウィザード) ボタンをクリックします。

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

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

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

   — **VMware ESX Server** ñ 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。189 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) ボタンをクリックします。

グループの管理

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

外部ディレクトリ グループを作成するには

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

内部ディレクトリ グループを作成するには

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

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

HPCA グループ作成ウィザードが開きます。

2 グループの名前と説明を入力します。

3 **[デバイスの追加]**  をクリックします。

[デバイスの追加] ウィンドウが開きます。

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

5 追加するデバイスを選択し、**[追加]** をクリックします。

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

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

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

グループの説明またはデバイスを修正するには

1 ナビゲーション ツリーを使用し、修正するグループを選択します。

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

グループの [ディレクトリ オブジェクト] ウィンドウが開きます。

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

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

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

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

グループを削除するには

1 ナビゲーション ツリーを使用し、削除するグループを選択します。

2 **[このディレクトリ オブジェクトを削除]** 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。エージェント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、エージェント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 エージェント配布ウィザードの起動**  をクリックします。エージェント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 (174 ページの「ジョブを管理する」を参照) を使用します。

ジョブを管理する

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

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

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

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

表 17　　ジョブ タイプ

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

現在と過去のジョブ

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

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

タイプ – [通知]、[DTM]、または [RMP]。

表示名 – ジョブの作成時に指定した名前。

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

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

説明 – ジョブの作成時に指定したテキスト説明。

スケジュール – ジョブに関連付けられたスケジュール。

ターゲット – ジョブを実行するターゲット デバイスまたはグループ。

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

作成時刻 – このジョブが作成された日時。

作成者 – ジョブを作成した HPCA Console ユーザー。

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

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

表 18　　ジョブ テーブルのコントロール

アイコン	説明
	データのリフレッシュ
	フィルタ入力の表示 / 非表示

表 18　ジョブ テーブルのコントロール

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

ジョブおよびジョブの実行

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

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

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

ターゲット

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

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

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

[ターゲットの詳細] ウィンドウにアクセスするには

1 [現在のジョブ] または [過去のジョブ] テーブルで、**[ジョブ ID]** をクリックします。

2 [ジョブの詳細] ウィンドウで、**[プロパティ]** タブをクリックします。

3 [ターゲット] セクションで、ターゲット グループまたはデバイスの名前をクリックします。

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

スケジュール

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

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

[スケジュールの詳細] ウィンドウにアクセスするには

1 [現在のジョブ] または [過去のジョブ] テーブルで、DTM ジョブの **[ジョブ ID]** をクリックします。

2 [ジョブの詳細] ウィンドウで、**[プロパティ]** タブをクリックします。

3 [スケジュール] セクションで、**[修正]** をクリックします。

DTM ジョブのスケジュールを指定するには

1 **[タスクの開始]** リストで、**[スケジュール]** または **[起動]** を選択します。

[起動] を選択する場合は、以降の手順をスキップできます。

2 このジョブを実行する頻度を [一度]、[時間単位]、[日単位]、[週単位]、[月単位] の中から選択します。

3 [一度] 以外の頻度を選択した場合は、**[間隔]** 情報を指定して、このジョブの再実行間隔を定義してください。

4 ジョブの **[開始日]** を指定します。

5 このジョブの新しいジョブの実行を開始することを一定の日付で中止する場合は、**[終了日]** フィールドの左にあるチェックボックスをオンにし、終了日を指定します。

6 ジョブの **[開始時刻]** を指定します。

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

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

詳細については、182 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。176 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。177 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。180 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。179 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 19　　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。176 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。180 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。178 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 (179 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。注 : 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)。181 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 20　　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

注：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、179 ページの「通知ジョブのジョブの詳細」または 178 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、181 ページの「ジョブの実行状態」を参照してください。

ジョブの実行状態

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

表 21　　ジョブの実行状態の説明

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

新しい DTM または通知ジョブの作成

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、172 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、203 ページの「オペレーティング システムの管理」を参照してください。

新しい DTM ジョブまたは通知ジョブを作成するには

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

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

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

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

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

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

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

5 ジョブの **[名前]** と **[説明]** を指定します。

6 **[ジョブ アクション テンプレート]** リストで、ここで使用するジョブ アクション テンプレートを選択します。詳細については、307 ページの「ジョブ アクション テンプレート」を参照してください。

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

8 **[次へ]** をクリックします。

9 このジョブのスケジュールを指定します。詳細については、177 ページの「スケジュール」を参照してください。

10 **[次へ]** をクリックします。

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

ジョブを表示するには、[管理] タブの [ジョブ] 領域をクリックします。

DTM ジョブのスケジュールを修正する場合は、ターゲット デバイスのそれぞれでスケジュールをリフレッシュする必要があります。186 ページの「古いジョブの実行レコードの削除」を参照してください。

ジョブの削除

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

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

  DTM ジョブを削除すると、それ以降に HPCA Core Server との間で行われる Agent の同期で、そのジョブをターゲット デバイスにダウンロードすることができなくなります。削除されたジョブがすでに存在するターゲット デバイスの場合、HPCA Core Server との同期を行うまでは、そのジョブを実行できます。

ターゲットの DTM スケジュールのリフレッシュ

HPCA Core Server で DTM ジョブのスケジュールを修正する場合は、各ターゲット デバイスでもスケジュールをリフレッシュする必要があります。これには、「DTM ジョブ スケジュールのリフレッシュ」サンプル ジョブ アクション テンプレートを使用してジョブを作成します。

デフォルトでは、Configuration Server Database (CSDB) に DTM_DAILY_TIMER があり、管理対象デバイスに対して付与を行って、Core Server と 1 日に 1 回の頻度でジョブ情報の同期を実行するようにその Agent に指示することができます。

DTM スケジュールのリフレッシュ ジョブでは、別の方法を使用して Core Server との同期をスケジュールできます。たとえば、DTM スケジュールのリフレッシュ ジョブを作成して、Core Server と 12 時間ごとにジョブ情報の同期を

実行するように Agent に依頼することができます。ターゲット デバイスの Agent に対しては、この DTM スケジュールのリフレッシュ ジョブは、ジョブ タイマーが期限切れになると、ソフトウェア接続などの他の Agent ジョブとまったく同じように実行されます。

クライアント デバイスで DTM スケジュールのリフレッシュ ジョブを正常に実行できるようにするには、そのクライアントの HPCA Agent で HPCA Core Server への事前接続操作を実行しておく必要があります。

DTM スケジュールのリフレッシュ ジョブを作成するには

1 [管理] タブの **[ディレクトリ]** 領域で、関係する DTM ジョブのターゲット デバイスを含むオブジェクトに移動します。

2 リフレッシュするターゲット デバイスを選択します。

3  ツールバー アイコンをクリックして **HPCA ジョブ作成ウィザード**を起動します。

4 直ちにリフレッシュするには、**[ジョブ タイプ]** ドロップダウン ボックスで **[通知]** を選択します。スケジュールに従ってリフレッシュするには、**[DTM]** を選択します。

[DTM] を選択すると、ターゲット デバイスでは、Core Server と同期するときにこのジョブが必要になります。このジョブでは、指定するスケジュール設定に従って Core Server に再接続し、ジョブ情報を取得するようにデバイスに指示します。

Agent で新しい同期スケジュールをできるだけ早く使用するには、DTM スケジュールのリフレッシュ ジョブの **[通知]** もスケジュールして、指定した時刻に Core Server との同期を実行するようにターゲット デバイスの Agent に指示し、*次に* DTM スケジュールのリフレッシュ ジョブの **[DTM]** をダウンロードすることをお勧めします。

5 リフレッシュ ジョブの名前および説明を入力します。

6 **[ジョブ アクション テンプレート]** リストで、**[DTM ジョブ スケジュールのリフレッシュ]** を選択します。

7 **[次へ]** をクリックします。

8 スケジュール設定 (177 ページの「スケジュール」を参照) を入力し、**[サブミット]** をクリックします。

ジョブが追加され、定義した設定に基づいてターゲット デバイスが設定されている DTM ジョブ スケジュールをリフレッシュします。

ジョブのステータスを表示するには、[管理] タブの **[ジョブ]** 領域をクリックします。

通知ジョブのデバイス解決

通知ジョブに含まれるデバイスは、次のファイルで定義されている順序に従って解決されます。

<*tomcatDir*>\webapps\em\web-inf\console.properties

<*tomcatDir*> のデフォルト値は次のとおりです。

C:\Program Files\Hewlett-Packard\HPCA\tomcat

デフォルトの順序 :

group.target.host.attributes=ipaddress,dnshostname,displayname,cn

必要に応じて、このリストを変更できます。このファイルに変更を加える場合は、HPCA Tomcat サービスを再起動する必要があります。

解決できなかったデバイスについては、[ジョブの詳細] ウィンドウの [詳細] タブにメッセージが表示されます。[ジョブの詳細] ウィンドウを開くには、ジョブ ID をクリックします。

DTM ジョブのデバイス解決

DTM ジョブに含まれるデバイスは、次の順序で解決されます。

1. ipaddress
2. dnshostname
3. displayname
4. cn

DTM ジョブのターゲット デバイスを解決するため、サービスが定期的に実行されます。このサービスは、次のファイルで設定可能です。

<*tomcatDir*>/webapps/ope/config/dtm.properties

表 22　　DTM ジョブのデバイス解決サービスのパラメータ

パラメータ	デフォルト値	コメント
enableTargetRefresh	true	このサービスを有効または無効にする
rmpProtocol	http\:\\	SSL の場合は https\:\\
rmpServer	localhost	HPCA Portal Server

表 22　　DTM ジョブのデバイス解決サービスのパラメータ

パラメータ	デフォルト値	コメント
rmpPort	3466	接続先の Portal Server ポート
rmpUser	SYSTEM	
rmpPassword		セキュリティ上の理由により非表示
userDS	“”	接続先のユーザー ディレクトリ
targetRefreshInterval	360	デフォルトは 6 分 (360 秒)
targetRefreshInitDelay	60	起動してから DTM がターゲット解決サービスを開始するまでの待機時間 (秒)

古いジョブの実行レコードの削除

過去の DTM および通知のジョブの実行を HPCA データベースに保存する期間を指定できます。また、保存するレコードの最大数を指定することもできます。この設定は、次のファイルで行います。

<*tomcatDir*>\webapps\ope\config\dtm.properties

<*tomcatDir*> のデフォルト値は次のとおりです。

C:\Program Files\Hewlett-Packard\HPCA\tomcat

次のパラメータを使用してこれらの設定値を指定します。

```
dtmJobRunKeepDays=30
opeJobRunKeepDays=30
dtmJobRunKeepRecords=-1
opeJobRunKeepRecords=-1
```

これらのパラメータによって指定される期間のデフォルト設定は、ここに示すとおりです。値 -1 は、保存可能なレコード数に制限がないことを示します。

Satellite 同期ジョブの作成

管理対象デバイスへのデータ キャッシュと設定値の配布を行うには、Satellite Server を使用します。Satellite は、それらのデバイスに最新のデータを配布するために、Core Server と同期を取る必要があります。Satellite Console から同期を実行するか、HPCA Console でジョブを作成してこの同期タスクをスケジュールすることができます。

- Satellite Server のデータを同期できるようにするには、最初に Satellite を設定しておく必要があります。詳細については『HPCA Core および Satellite 入門およびコンセプト ガイド』を参照してください。
- クライアント デバイスで Satellite 同期ジョブを正常に実行できるようにするには、そのクライアントの HPCA Agent で HPCA Core Server への事前接続操作を実行しておく必要があります。

Satellite 同期ジョブを作成するには

1. [管理] タブの **[ディレクトリ]** 領域で、Satellite デバイスを含むオブジェクトに移動します。
2. Satellite デバイスを選択し、  ツールバー アイコンをクリックして **HPCA ジョブ作成ウィザード**を起動します。

   - Satellite Server ではないデバイスを選択すると、そのジョブは失敗します。

3. Satellite を即時に同期するには、**[ジョブ タイプ]** ドロップダウン ボックスから **[通知]** を選択します。スケジュールに従って同期するには、**[DTM]** を選択します。

   [DTM] を選択すると、Satellite デバイス上のエージェントが DTM スケジュールのリフレッシュを実行した*後*のみ、この Satellite 同期ジョブが Satellite にダウンロードされます。
4. 同期ジョブの名前および説明を入力します。
5. スケジュールする同期タイプの **[ジョブ アクション テンプレート]** を選択します。

   — **Satellite の同期 (すべて)**

   設定の設定とデータの両方を同期するには、このテンプレートを選択します。

— **Satellite の同期 (設定)**

設定の設定のみを同期するには、このテンプレートを選択します。

— **Satellite の同期 (データ)**

このテンプレートでは、データのみが同期されます。

6 **[次へ]** をクリックします。

7 スケジュール設定 (177 ページの「スケジュール」を参照) を入力し、**[サブミット]** をクリックします。

ジョブが追加され、Satellite Server では定義した設定に基づいてデータまたは設定の設定が同期されます。

ジョブのステータスを表示するには、[管理] タブの **[ジョブ]** 領域をクリックします。

仮想マシンの管理

HPCA Console を使用すると、仮想ホスト 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。154 ページの図 41 に示すように、別のブラウザ ウィンドウが開きます。

5 使用している ESX Server の [ディレクトリ オブジェクト] ウィンドウで、左ナビゲーション メニューの **[仮想マシン]** リンクをクリックします。

> [仮想マシン] リンクは、このデバイスが **[VMware ESX Server]** デバイスの分類を使用してインポートされた場合のみ表示されます。詳細については、設定に関する章の「デバイスのインポート」を参照してください。

この HPCA Console セッション中に初めて ESX Server のリンクをクリックした場合、ログイン認証情報を入力する必要があります。

ESX Server の **[ユーザー ID]** と **[パスワード]** を入力して、**[サインイン]** をクリックします。

192 ページの図 44 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 43　　VMware ESX Server のデバイス プロパティ

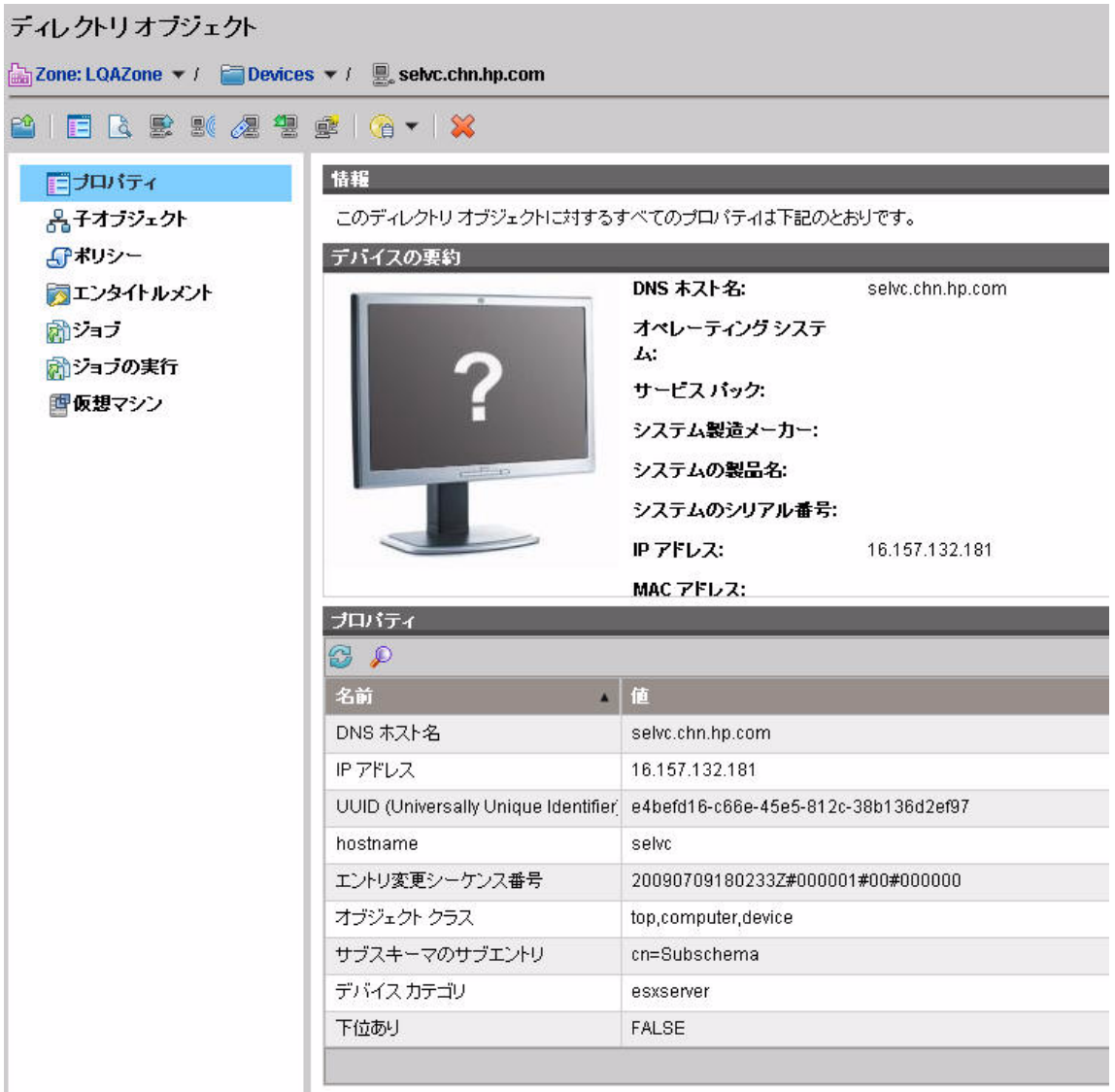


図 44　　ESX Server でホストされる仮想マシン一覧

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 23　　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 24　　[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 :

1 189 ページの「仮想マシンの管理」の手順 1 ～ 5 に従って、使用している ESX Server 上の仮想マシンの一覧を開きます。

2 **[新しい仮想マシンの作成]**  をクリックします。仮想マシン作成ウィザードが表示されます。

3 作成したい仮想マシンについての情報を入力します。

- **データ センター** : ドロップダウン リストを使用して、新しい仮想マシンを作成するデータ センターを選択します。
- **ホスト システム** : ドロップダウン リストを使用して、仮想マシンのホスト システムを選択します。
- **名前** : 仮想マシンの名前を入力します。仮想マシンの名前は 80 文字以内とし、英数字、スペース、ハイフン、アンダースコアを使用できます。仮想マシンの名前は、各データ センター内および各フォルダ内で一意である必要があります。
- **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。注 : 仮想マシンに割り当てることができるプロセッサの数は、ホスト デバイス上の論理プロセッサの実際の数までです。

11 仮想マシンの **[メモリ サイズ]** を入力します。メモリ サイズをメガバイト単位で入力するには、数字を入力するか、上向き矢印または下向き矢印を使用します。サイズをギガバイト単位で入力するには、スライダ ツールを使用します。メモリ サイズの下限は 4MB です。

12 **[次へ]** をクリックします。

13 ドロップダウン リストを使用して、この仮想マシンに対して設定する **[NIC の数]** (ネットワーク インターフェイス カードの数) と **[NIC 番号 1 仮想ネットワーク]** を選択します。

14 仮想マシンの起動時に各 NIC をネットワークに接続する場合は、**[電源オン時に接続]** をオンにします。

15 **[次へ]** をクリックします。

16 要約情報を確認し、**[適用]** をクリックします。

17 これで、仮想マシンが作成されました。仮想マシンのリストで、新しい仮想マシンを確認します。仮想マシンの名前をクリックすると、プロパティ ウィンドウが開きます。

デバイスのリモート制御

HPCA Console では、次の 3 種類の方法のいずれかを使用して、内部および外部リポジトリのデバイスへリモート アクセスできます。

- Windows リモート デスクトップ接続
- Virtual Network Computing (VNC)
- Windows リモート アシスタンス

HPCA Console では、各ターゲット デバイスのリモート制御機能を判別して、最適な通信方法が決定されます。特定のターゲット デバイスへのリモート制御接続を開始すると、そのデバイス上で使用可能な接続のタイプを選択できます。

VNC および Windows リモート デスクトップ接続については、リモート デバイスがリモート接続をリスンするポートを指定する必要があります。Windows リモート アシスタンスは常にポート 135 の Distributed Component Object Model (DCOM) インターフェイスを使用するため、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。

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、331 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、197 ページの「リモート接続の要件」を参照してください。

デバイスにリモート アクセスするには :

1 **[管理]** タブをクリックします。

2 リモート アクセスするデバイスが含まれているゾーンを展開します。

3 左ナビゲーション ペインで、**[デバイス]** をクリックします。

4 アクセスするデバイスの右クリック ショートカット メニューで、**[リモート制御]** をクリックします。

[プロパティの表示 / 編集] を選択して、[ディレクトリ オブジェクト] ウィンドウの  (リモート制御) アイコンをクリックすることもできます。

HPCA Console で Windows リモート デスクトップ接続、VNC、または Windows リモート アシスタンスを使用して接続できない場合、[リモート制御] をクリックするとエラー メッセージが表示されます。

5 Windows リモート デスクトップ接続では、次の項目を指定します。

— **メソッド** : [Windows リモート デスクトップ] を選択します。

— **解像度** : 画面上の Windows リモート デスクトップ接続ウィンドウのサイズを選択します。

VNC 接続では、次の項目を指定します。

— **メソッド** : [VNC (Virtual Network Computing)] を選択します。

Windows リモート アシスタンス接続では、次の項目を指定します。

— **メソッド** : [Windows リモート アシスタンス] を選択します。

6 **[接続]** をクリックします。新しいブラウザ ウィンドウが開いて、リモート接続が確立されます。

VNC 接続では、最初に VNC パスワードの入力が必要な場合があります。

Windows リモート アシスタンス接続では、現在ターゲット デバイスにログオンしているユーザーは接続を許可する必要があります。

関連トピック :

331 ページの「リモート制御の設定」

202 ページの「リモート制御の監査」

リモート接続の要件

HPCA Console を使用してリモート接続するターゲット デバイスでは、次の要件が満たされている必要があります。

- リモート デバイスの電源がオンになっている。
- ファイアウォールが有効な場合は、リモート デバイス上のリモート アクセス ポートが開いている。

- リモート デバイスは、HPCA Console サーバーとリクエストを開始するクライアント システムの両方に接続できる。

また、各タイプのリモート アクセスには、特定の要件があります。

Windows リモート デスクトップの要件

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 デバイスで、Windows リモート デスクトップ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 デスクトップを使用するには、Internet Explorer (バージョン 7.0 以降) を使用して HPCA Console にアクセスする必要があります。これは、このタイプの接続がリクエストされたときに ActiveX コンポーネントを使用するラッパーをコンソールが起動するためです。

Windows リモート デスクトップを使用すると、ActiveX コントロールをインストールするように要求される場合があります。これは、Windows リモート デスクトップが適切に機能するのに必要です。また、ローカル デバイスに接続するようにも要求されます。これは必須ではありません。

Windows リモート デスクトップの詳細については、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

関連トピック：

198 ページの「VNC の要件」

199 ページの「Windows リモート アシスタンスの要件」

VNC の要件

VNC 接続では、ターゲット デバイスで VNC サーバー プロセスを実行する必要があります。このプロセスでは、特定のポートをリスンする必要があります。また、URL (HTTP) ベースのリモート制御セッションのサポートが有効である必要があります。

VNC 接続を確立するには、HPCA Console でリモート URL をブラウザ内の Java アプレットとして起動します。このため、HPCA Console にアクセスしているシステム (ブラウザを実行しているシステム) に Java Runtime Environment (JRE) バージョン 1.5 (またはそれ以降) がインストールされている必要があります。JRE は、**www.java.com** からダウンロードできます。

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、HPCA Console では、Web ベースの統合機能を持つすべての VNC サーバーがサポートされます。この機能は、UltraVNC、RealVNC、および TightVNC で利用できます。通常、VNC サーバーはポート 5800 上で実行され、すべての Web ブラウザからアクセスできます。

Application Management Profile (AMP) を使用して、UltraVNC、RealVNC、および TightVNC サーバー ソフトウェアをクライアント システムに配布できます。上記アプリケーション用の AMP は、HP Live Network の Web サイトの AMP Community から入手できます。AMP の詳細については、『Application Management Profiles ユーザー ガイド』を参照してください。

関連トピック：

198 ページの「Windows リモート デスクトップの要件」

199 ページの「Windows リモート アシスタンスの要件」

Windows リモート アシスタンスの要件

Windows Vista、Windows Server 2008、Windows 7 システムから HPCA Console にアクセスしている場合、作成できる接続は Windows リモート アシスタンスのみです。次のオペレーティング システムを実行しているターゲット デバイスに接続できます。

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 Release 2 (R2) x64

ターゲット デバイスへの Windows リモート アシスタンス接続が開始したら、ターゲット デバイスにログオンしているユーザーは接続を許可する必要があります。自動実行のデバイスへの Windows リモート アシスタンス接続は作成できません。

この接続タイプを使用してリモート アクセスするすべてのターゲット デバイス上で、Windows リモート アシスタンスを有効にする必要があります。詳細については、ネットワーク管理者に問い合わせるか、次の Microsoft サポート ドキュメントを参照してください。

http://support.microsoft.com/kb/305608/en-us

Windows リモート アシスタンス接続を有効にするには、さらに次の 3 つの要件を満たす必要があります。

- HPCA Console にアクセスしているシステムとターゲット デバイスは同じドメインに参加している必要があります。
- HPCA Console にアクセスしているシステム (Windows リモート アシスタンス操作の上級者側) には、次のソフトウェアがインストールされている必要があります。
  - Java Runtime Environment (JRE) バージョン 5 (またはそれ以降)
  - オペレーティング システムが Windows 2008 Server の場合は、リモート インスタンス機能がインストールされている必要があります。詳細については、次の記事を参照してください。

    http://technet.microsoft.com/en-us/library/cc753881.aspx
- すべてのターゲット デバイス上で、[リモート アシスタンスを提供する] グループ ポリシーが有効である必要があります。ターゲット デバイスへのアクセスが許可される「支援者」も指定する必要があります。ユーザーまたはグループのどちらかを支援者として設定できます。支援者は次のように指定します。

  `domain_name\user_name`

  `domain_name\groupname`

  ターゲット デバイスへの Windows リモート アシスタンス接続を作成するには、接続するユーザー (またはユーザーが所属するグループ) がこの支援者のリストに含まれている必要があります。
- すべてのターゲット デバイスで、リモート アシスタンスを Windows ファイアウォールの例外として有効にする必要があります。

Windows リモート アシスタンスの詳細については、次の Microsoft のサポート ドキュメントを参照してください。

http://technet.microsoft.com/en-us/library/cc753881.aspx

関連トピック：

198 ページの「Windows リモート デスクトップの要件」

198 ページの「VNC の要件」

ファイアウォールの考慮事項

HPCA Console をホストするサーバーとリモート デバイスの間にファイアウォールが存在する場合、適切なポートを開く必要があります。

Windows リモート デスクトップ接続では、TCP ポート 3389 を使用します。

デフォルトでは、Windows リモート アシスタンスには、Windows XP または Windows Server 2003 のターゲット デバイスへの接続時に TCP ポート 3389 が必要です。Windows Vista、Windows Server 2008、または Windows 7 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

関連トピック：

198 ページの「Windows リモート デスクトップの要件」

198 ページの「VNC の要件」

199 ページの「Windows リモート アシスタンスの要件」

リモート制御の監査

HPCA 管理対象環境内のいずれかのユーザーが、HPCA Console を使用して管理対象デバイスへリモート接続を試行するたびに、リモート制御監査イベントとしてログに記録されます。次の情報が記録されます。

- リモート制御セッションを開始したユーザーと開始日時
- ターゲット デバイス
- 使用された接続のタイプ

リモート制御監査ログを表示するには、管理レポート ビューでリモート制御レポートを開きます。

リモート制御レポートには、次の情報が含まれています。

時刻 – リモート制御イベントが発生した日時

接続ステータス – リモート制御イベントの説明

ユーザー – リモート制御イベントを開始した HPCA Console ユーザーの ID

接続タイプ – VNC、リモート デスクトップ、またはリモート アシスタンス

ターゲット ホスト – リモート制御を通してアクセスされたデバイスのホスト名または IP アドレス

HPCA ホスト – HPCA Console をホストしているシステムのホスト名または IP アドレス

レポートは、カラム見出しをクリックして、任意のアイテムでソートできます。グレーの矢印は、ソート順を示しています。

関連トピック：

196 ページの「デバイスのリモート制御」

217 ページの「レポートの使用」

オペレーティング システムの管理

HPCA Console のオペレーティング システム (OS) 管理機能を使用して、クライアント デバイス上のオペレーティング システムのインストール、置換、更新、または修復ができます。また、HPCA を使用して、OS の配布前に完了する必要がある各種の低レベル タスク (BIOS ファームウェアの更新、設定、およびドライブ設定など) を実行できます。

ここでは、次のトピックを取り扱います。

- 203 ページの「OS 管理の前提条件」
- 205 ページの「配布シナリオ」
- 204 ページの「OS 配布の動作」
- 207 ページの「OS イメージの配布」
- 213 ページの「OS 管理アクティビティのステータスの表示」

HPCA における OS 管理の総合的な説明については、『HPCA OS Manager システム管理者ガイド』を参照してください。

OS 管理の前提条件

HPCA Console を使用してオペレーティング システム (OS) を配布する前に、次の前提条件が満たされている必要があります。

- 適切な OS イメージが利用可能である。

  詳細については、『HPCA OS Manager システム管理者ガイド』の「OS イメージの準備とキャプチャ」を参照してください。

- OS イメージは、HPCA Configuration Server Database (CSDB) にパブリッシュされる必要があります。

  詳細については、『HPCA OS Manager システム管理者ガイド』の「パブリッシュ」を参照してください。

ターゲット デバイス (複数可) 用に適切なハードウェア設定オブジェクトの作成が必要になる場合もあります。詳細については、『HPCA OS Manager ハードウェア設定管理ガイド』を参照してください。

これらの前提条件が満たされると、HPCA Console の OS 管理ウィザードを使用したオペレーティング システムの配布および管理ができるようになります。

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 配布の対象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 (175 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。

配布シナリオ

お使いの環境のデバイスにオペレーティング システムを配布する方法は、いくつかの変数によって異なります。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。詳細については、『HP Client Automation System Administrator ユーザー ガイド』を参照してください。

表 25　　配布シナリオ

デバイスの状態	配布の手順
管理対象 (Agent をインストール済み)	デバイスがすでに管理されている場合 • デバイスをグループに追加 • オペレーティング　システムの付与資格をグループに設定する (付与がまだの場合) • OS 配布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 やサービス CD を準備する必要はありません。

表 25　　配布シナリオ

デバイスの状態	配布の手順
非管理対象 (Agent が未インストール)	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 • ベアメタル デバイスへの OS の配布については、下記の手順を参照してください。
ベアメタル (OS が未インストール)	(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 の付与資格がまだ有効です。PXE またはサービス 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 またはサービス CD でデバイスを起動 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て HPCA にデバイスを追加 • 新しいデバイスを OS 付与資格を持つグループに追加 デバイスが再起動され、サービス CD または PXE が OS の配布を続けます。 注意 : OS は、全デバイス グループに接続されている場合、自動的にインストールされます。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。 注意 : ベアメタル デバイスへの OS の配布には、LSB は使用できません。

OS イメージの配布

HPCA Console から OS を配布するには、5 つの手順が必要です。

手順 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。

手順 2 配布する OS イメージを選択します。

手順 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。

手順 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。172 ページの「HPCA Agent の配布」を参照してください。

手順 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。203 ページの「OS 管理の前提条件」および 205 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 配布方法を選択します。

- **ローカル サービスの起動 (LSB)**: OS を配布するために LSB をインストールする場合、このオプションを選択します。ローカル サービスの起動には、既存のマシンは PXE 対応である必要がなく、各ターゲット デバイスについて、起動の順序を BIOS でローカルに設定する必要がないという利点があります。210 ページの「LSB の使用」を参照してください。
- **ネットワークの起動 (PXE)**: デバイスにオペレーティング システムをインストールするために PXE サーバーを使用する場合は、このオプションを選択します。210 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。211 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、既存のデータのキャプチャおよび保存を試行せずに OS をインストールまたは再インストールする場合は、**[緊急モード]** を選択します。

このオプションにより、クライアント デバイスで管理アクティビティの必要性を判別できるようになります。このオプションが無効の場合、管理アクティビティの必要性を判別するには、クライアント デバイスに対して、既存の起動可能なオペレーティング システム、稼働中の HPCA Agent、および良好な一般整合性 (ウイルスが存在しないなど) が必要になります。

緊急モードを使用しない場合のデータの取得および保存に関する詳細については、『HPCA OS Manager System Administrator ガイド』の「ドライブ レイアウトの定義」を参照してください。

c 現在電源がオフになっているマシンでの管理操作を 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。(174 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、205 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、205 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付与されている場合、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ある必要があります。

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、205 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次の形式で入力します。

`xxx.xxx.xxx.xxx:port`

例 :

`HPCA.acmecorp.us.com:3466` または `192.168.1.100:3466`

注 : 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。HPCA Classic インストールでは、ポート 3469 がこの目的のために予約されています。

e **Enter** キーを押して続行します。

デバイスは、HPCA Server に接続され、MAC アドレスのバリエーションをデバイス名として使用して、デバイス リストに追加されます。ImageDeploy CD によって HPCA Server に接続すると、次のメッセージが表示されます。

このマシンにローカル `OS` がないか、`OS` が無効です。

マシンは使用できず、管理者がポリシーを指定して Wake On LAN を実行するまでシャットダウンされます。

2 HPCA Console で次の手順を実行します。

a [管理] タブで、207 ページの「OS イメージの配布」の手順に従います。

b 配布方法として **[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付与されている場合、インストールする OS の選択画面が表示されます。

イメージの配布が終了したら、ターゲット デバイスを再起動し、Windows を起動します。Sysprep プロセスが、新しいイメージを起動し、初期化します。

1 回限りのハードウェア メンテナンス操作の実行

HPCA Console を使用して、ハードウェア設定要素を使用するジョブを作成し、特別なハードウェア メンテナンス操作をクライアント デバイス上で実行できます。特定のデバイスに対して OS のインストール、更新、および修復を行う前に、このジョブが必要となる場合があります。たとえば、アクティブ ホット スペア (AHS) が変更された場合の RAID (独立ディスクの冗長アレイ) の検証または再同期を起動する必要がある場合、このジョブを使用します。

BIOS ファームウェアの更新またはディスク アレイ コントローラ (DAC) の設定など、日常的な低レベルの操作については、通常の LDS/LME 管理プロセスを使用してください。

詳細については、『HPCA OS Manager ハードウェア設定管理ガイド』を参照してください。

1 回限りのハードウェア メンテナンス操作を実行するには :

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

— 1 つ以上のターゲット デバイスを個別に指定するには、**[デバイス]** をクリックします。

— グループを指定するには、**[グループ]** をクリックします。

2 ディレクトリ オブジェクトの表で、作業対象のデバイスまたはグループを選択します。

3 選択したいずれかのデバイスまたはグループのドロップダウン メニューで、[OS 管理] サブメニューの **[1 回限りのハードウェア メンテナンスの実行]** を選択します。

ハードウェア メンテナンス ウィザードが起動します。

4 災害復旧シナリオなど、既存のデータのキャプチャ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での管理操作を 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。(174 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 (175 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)。205 ページの「OS 配布状態の表示」を参照してください。

アウトバンドの詳細の表示

HPCA Console で使用可能なアウトバンド管理 (OOBM) 機能により、システムの電源状態やオペレーティング システムの状態とは無関係に、アウトバンド管理操作を実行できるようになります。

インバンド管理は、コンピュータの電源がオンでオペレーティング システムが稼働しているときに実行される操作を指します。

アウトバンド管理は、コンピュータが次のいずれかの状態のときに実行される操作を指します。

- コンピュータは電源に接続されているが稼働していない (オフ、スタンバイ、休止)
- オペレーティング システムに読み込まれていない (ソフトウェア障害またはブートの失敗)
- ソフトウェア ベースの管理エージェントが使用できない

HPCA Console では、Intel の vPro デバイスおよび DASH 対応デバイスのアウトバンド管理がサポートされます。

このオプションは、アウトバンド管理が有効な場合のみ使用できます。詳細については、367 ページの「アウトバンド管理」を参照してください。詳細については、『HP Client Automation アウトバンド管理ガイド』を参照してください。

デバイスのアウトバンドの詳細を表示するには :

1 [管理] タブで [ディレクトリ] 領域に移動して、使用するゾーンを展開します。次に、**[デバイス]** (または **[グループ]**) をクリックします。

2 対象デバイスのショートカット メニューから **[アウトバンド デバイスの詳細]** を選択します。

デバイスに DASH または vPro が実装され、OOBM が有効で適切に設定されている場合、選択したデバイスの [アウトバンド デバイスの詳細] ウィンドウが表示されます。

アウトバンド デバイスの詳細  アイコンをクリックしても、特定のデバイスの OOB の詳細を表示できます。

アウトバンド管理が有効な場合、このアイコンが対象デバイスのディレクトリ オブジェクト ビューのツールバーに表示されます。

利用状況収集フィルタ作成ウィザード

利用状況収集フィルタ作成ウィザードを使用して、新しい利用状況収集フィルタを作成します。

新しい収集フィルタを作成するには

1. [利用状況] タブで **[新しいフィルタの作成]**  ツールバー ボタンをクリックします。ウィザードが開きます。
2. フィルタ パラメータを設定するには、各テキスト ボックスにフィルタ条件を入力します。

   利用状況データのフィルタを適用するフィールドにのみ値を入力します。空のテキスト ボックスは無視され、フィルタ条件として使用されません。

   入力した値が、ソフトウェアの実行可能ファイルのファイル ヘッダーと比較され、収集された利用状況データがフィルタ条件に合致するか判断されます。

   特定のソフトウェアにフィルタを適用する方法を決めるには、373 ページの「ダッシュボード」を参照してください。

   50 を超えるアプリケーションについてデータを収集し、報告するようにフィルタを設定すると、大量のデータが収集され、結果的にレポートのパフォーマンスに重大な問題が生じる可能性があります。
3. **[作成]** をクリックします。
4. **[閉じる]** をクリックします。

   新しいフィルタが、収集フィルタ リストに追加されます。

利用状況収集エージェントの配布

利用状況収集エージェントを配布するには、利用状況接続ジョブ テンプレートを使用してターゲット デバイスまたはグループのジョブを作成します。

利用状況収集エージェントを配布するには、次の手順を実行します。

1 [管理] タブで **[デバイス]** または **[グループ]** をクリックします。

2 160 ページの「ディレクトリ オブジェクトのポリシーの管理方法」の指示に従って、次のサービスの付与資格を関連デバイスまたはグループに設定します。

USAGE.ZSERVICE.CCM_USAGE_AGENT

3 182 ページの「新しい DTM または通知ジョブの作成」の指示に従い、利用状況接続ジョブ テンプレートを指定します。

このジョブに指定するスケジュールは、利用状況データの収集に使用するスケジュールです。

これにより、ターゲット デバイスに利用状況収集エージェントをインストールし、その後、ターゲット デバイスの利用状況情報を収集するジョブが作成されます。保留中のジョブをすべて表示するには、[ジョブ] 領域で [現在のジョブ] 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

HPCA Console の [レポート] タブには、222 ページの「レポートのタイプ」に説明されているとおり、レポートの複数の収集に対するリンクが表示されます。

それぞれの収集には、特定のタイプのデータまたは特定の視聴者に焦点を当てたレポートのグループが含まれています。これらのレポートには、ダッシュボードに値を設定するために使用されるデータも表示されます。

次のレポートは、すべてのエディションの HPCA で使用可能です。

レポート パック	レポート タイプ	説明
rpm.kit	パッチ管理	パッチ ポリシーへの準拠デバイスと非準拠デバイス
rim.kit	インベントリ	現在 HPCA で管理されているデバイス

次のレポートは、HPCA Enterprise でのみ使用できます。

レポート パック	レポート タイプ	説明
vm.kit	脆弱性管理	脆弱性定義とクライアント デバイスのスキャン結果などのセキュリティ脆弱性情報
compliance.kit	適用状況管理	Secure Content Automation Protocol (SCAP) 適用状況規則と管理対象クライアント デバイスでの適用状況スキャン結果などの適用状況管理情報
stm.kit	セキュリティ ツール管理	ウイルス対策、スパイウェア対策、およびソフトウェア ファイアウォールのインストールと設定などのセキュリティ ツール管理情報
hpca.kit	HPCA 管理	監査レポート

[レポート] セクションのグラフィカル レポートを表示するには、Java Runtime Environment (JRE) または Java Virtual Machine (JVM) が必要です。詳細については、次のサイトを参照してください。

http://java.com/en/index.jsp

レポート間の移動

[レポート] タブをクリックすると、[レポートのホーム ページ] が表示されます。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)、および利用状況管理 (有効な場合) に関して、企業のスナップショットが表示されます。

[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 26　　レポートのアクション

アイコン	説明
	レポート ビュー内を 1 ページ戻る。
	レポートのホーム ページに戻る。
	データをリフレッシュする。リフレッシュは、フィルタを適用または削除するときにも実行されます。

表 26　　レポートのアクション

アイコン	説明
	このレポートをお気に入りのリストに追加する。
	このレポートへのリンクを電子メールで送る。
	「クイック ヘルプ」ボックスまたはツール チップが開きます。これは、フィルタにのみ適用されます。
	このレポートを印刷する。
	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。
	レポートの内容をカンマ区切り値 (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。
	レポートの内容を 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 – このブリティンをポストしたベンダーの Web サイトに移動する

マウス カーソルを青色テキストのアイテム上に置くと、そのアイテムをクリックするとどのようなアクションが行われるかがツール チップに表示されます。

デフォルトでは、レポートでグリニッジ標準時 (GMT) が使用されます。個々のレポート パックは、GMT またはローカル時刻のいずれかを使用するように設定できます。

レポートのタイプ

HPCA Console では、次のタイプのレポートを使用できます。

- 222 ページの「インベントリ管理レポート」
- 224 ページの「Application Management Profiles レポート」
- 225 ページの「設定管理レポート」
- 226 ページの「HPCA 管理レポート」
- 226 ページの「パッチ管理レポート」
- 227 ページの「利用状況管理レポート」
- 227 ページの「脆弱性管理レポート」
- 228 ページの「適用状況管理レポート」
- 229 ページの「セキュリティ ツール管理レポート」

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。

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、S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) 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。これらのレポートに含めるには、デバイスは AUDIT.ZSERVICE.DISCOVER.INVENTORY に付与されている必要があります。特定のデータを使用するには、HPCA を完全に設定する必要があります。設定の詳細については、330 ページの「デバイス管理」を参照してください。

一般的な管理対象デバイス レポートには、次のテーブル見出しがあります。

- **詳細** – このデバイスの [デバイスの要約] ページを開く。
- **前回の接続** – デバイスが最後に接続された日時。
- **HPCA Agent ID** – デバイス名。
- **HPCA Agent のバージョン** – 現在インストールされている Management Agent のバージョン。
- **デバイス** – デバイス名。
- **前回ログオン ユーザー** – デバイスへのログオンで使用された最後のユーザー アカウント。複数のユーザーがログオンしている場合は、最後にログオンしたユーザーのみが記録されます。現在ログオンしているユーザーを切り替えても、これには影響しません。
- **IP アドレス** – デバイスの IP アドレス。
- **MAC アドレス** – デバイスの MAC アドレス。
- **オペレーティング システム** – デバイスにインストールされているオペレーティング システム。
- **OS レベル** – 現在のオペレーティング システム レベル (サービス パック 2 など)。

HP ハードウェア レポート

HP ハードウェア レポートは、インベントリ レポートのサブセットで、互換性のある HP デバイスの HP Client Management Interface (CMI) でキャプチャ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。

Windows レポート

Windows Vista および Windows Experience Index レポートは、インベントリ レポートのサブセットです。これらのレポートには、システム ステータスの情報が含まれています。

Windows Vista および Windows Experience Index レポートは、[即時レポート] の下の [インベントリ レポート] にあります。

Windows Experience Index レポート

Windows Experience Index には、Agent の Windows System Assessment Tool (WinSAT) の結果が表示されます。このツールでは、さまざまなカテゴリのスコア (1.0 ～ 7.9) と複合スコアが提供されます。複合スコアは、レポートされるコンポーネントで最も低いスコアになります。

レポートされるコンポーネントの評価状態は、次のようになります。

0 = 不明

1 = 有効

2 = 前回の評価が実行されてからハードウェアが変更されている

3 = 評価が実行されたことがない

4 = 無効

結果が有効でない場合、レポートを再生成する必要があります。レポートを再生成する前に、Agent の WinSAT に戻って Agent にインベントリ スキャンを実行します。

Application Management Profiles レポート

Application Management Profiles レポートには、Application Management Profiles (AMPs) の詳細情報が表示されます。AMPs には、Client Automation 環境の管理対象クライアントおよびサーバーで通常必要とされる複雑なソフトウェア製品の配布と管理ができるツール セットがあります。

Application Management レポートでは、デバイスおよびサービスごとに AMP 情報を掘り下げて詳細を表示できます。

レポート オプションを表示するには、[Application Management] レポート ビューを展開します。[Application Management] の下には、次のレポートがあります。

- **デバイス別ジョブ ステータス** – AMP の詳細情報がデバイス順に表示されます。このレポートには、各デバイスのプロファイルの配布ステータスとスケジュールされた配布ジョブの情報が表示されます。
- **サービス別ジョブ ステータス** – AMP の詳細情報が AMP のサービス ID 順に表示されます。このレポートには、サービスの説明、サービスが配布されているデバイスの数、および AMP の配布ステータスとスケジュールされている配布ジョブの情報が表示されます。

設定管理レポート

設定管理レポートには、設定プロファイルが配布されているデバイスの設定プロファイル情報が表示されます。設定プロファイルは、使用環境の管理対象デバイスにインストールされている特定のソフトウェアの設定で構成されています。設定プロファイルを作成して配布すると、ソフトウェアの概要レポートを表示できるようになるため、管理者はこのソフトウェアのランタイム データを視覚的に確認できます。

この設定管理レポートでは、提供されるレポートの個々のカラムをクリックして、デバイス、プロファイル サービス ID、およびカテゴリごとに設定プロファイル情報を掘り下げて詳細を表示できます。

レポート オプションを表示するには、[設定管理] レポート ビューを展開します。[設定管理] には、次のレポートがあります。

- **デバイス別プロファイル ステータス** – ソフトウェアがインストールされている各デバイスのプロファイルの詳細情報がデバイス順に表示されます。このレポートには、各デバイスのプロファイルの配布ステータスとスケジュールされた配布ジョブの情報が表示されます。
- **サービス別プロファイル ステータス** – プロファイルの詳細情報が設定プロファイルのプロファイル サービス ID 順に表示されます。このレポートには、サービスの説明、サービスが配布されているデバイスの数、プロファイルの配布ステータス、スケジュールされた配布ジョブの情報が表示されます。
- **カテゴリ別プロファイル ステータス** – プロファイルの詳細情報がソフトウェアのタイプ順に表示されます。このレポートでは、カテゴリのリスト、およびプロファイルの配布ステータスとカテゴリごとのスケジュールされているジョブ配布情報を表示できます。カテゴリとは、ソフトウェア機能の概要です。

  たとえば、[HP 電源管理]、[ワイヤレス設定]、および [セキュリティ設定] などがこれに該当します。各カテゴリには、カテゴリの設定の特定の設定であるプロファイルが含まれている場合があります。たとえば、[HP 電源管理] カテゴリには、[低]、[中]、または [高] の電源プロファイル設定があります。
- **取得の詳細** – HP Live Network からのコンテンツの更新のステータスが表示されます。

HPCA 管理レポート

HPCA 管理レポートには、さまざまな HPCA 機能の管理情報が表示されます。次のレポート オプションを表示するには、そのビューを展開します。

- **Live Network** – このオプションの下には、取得履歴レポートを表示できます。ここには、取得イベントのリスト、各取得の日付、取得の詳細 (別のレポートに表示可能)、取得ソース、および取得ステータスが表示されます。
- **監査** – このオプションの下には、リモート制御レポートを表示できます。ここには、HPCA Console から管理対象クライアント デバイスに対して試みられたリモート制御セッションごとのエントリが含まれています。

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ィ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、ブリティン、およびベンダー別のブリティ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。

利用状況管理レポート

利用状況管理レポートには、利用状況収集エージェントがインストールされているデバイスの利用状況の情報が表示されます。利用状況収集エージェントの配布を使用して、収集エージェントをインストールし、利用状況データの収集を開始します。

- **概要** – 収集されたデバイスと利用状況がベンダーおよび製品ごとに視覚的に表示されます。
- **デバイス レポートの概要** – アプリケーションを使用しているデバイスおよびユーザーの詳細などの利用状況固有の情報が表示されます。
- **月次利用状況レポート** – ベンダー、製品、製品バージョン、およびアプリケーション別に、月単位の利用状況の情報が表示されます。
- **インベントリ レポート** – ベンダー、製品、製品バージョン、およびアプリケーション別に、インベントリ情報が表示されます。
- **操作レポート** – データが収集されたデバイスの数または過去 30 日間に収集されていないデバイスの数が表示されます。

利用状況管理レポートの使用方法の詳細については、『HPCA Application Usage Manager ユーザー ガイド』を参照してください。

➤ 収集エージェントが配布された後、利用時間の収集がただちに開始されます。集中時の収集は、ユーザーが次回ログインしてから開始されます。

➤ ほとんどの論理フォルダ (Program Files など) は、マシンに関連付けられており、個々のユーザーとは関連付けられていません。このため、利用状況管理レポート、デバイス レポート、ユーザー別利用状況レポートでは、[ユーザー名] カラムに [未定義] と表示される場合があります。

[設定] タブの [レポート] セクションで指定した [利用状況の設定] によっては、利用状況データの一部または全部が難読化される場合があります。

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 ブリティン (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ィンには、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、231 ページの「レポートのフィルタ」を参照してください。

これらのレポートは、[レポート] タブに表示されます。一部のレポートは、脆弱性管理ダッシュボードからも使用できます。

適用状況管理レポート

適用状況管理レポートは、次の 3 つのグループに整理できます。

- **概要** – これらのレポートには、適用状況管理の観点から見たお使いの環境のスナップショットが示されます。概要レポートを使用して、次の項目について容易に評価できます。
  - 準拠している、または準拠していないクライアント デバイスの数
  - 違反される頻度が最も多い適用状況規則
  - 非適用状況の程度が最も高いクライアント デバイス
- **SCAP レポート** – これらのレポートには、スキャンに含まれる各 Secure Content Automation Protocol (SCAP) ベンチマークに現在準拠している、または準拠していないクライアント デバイスの数が示されます。
- **デバイス レポート** – これらのレポートには、スキャンされたクライアント デバイスごとに、最後に実行された適用状況スキャンの結果が示されます。また、スキャンされなかったクライアント デバイスも示されます。

これらのレポートの多くをフィルタしたり、掘り下げて詳細を調べたりできます。詳細については、72 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、231 ページの「レポートのフィルタ」を参照してください。

これらのレポートは、[レポート] タブに表示されます。一部のレポートは、適用状況管理ダッシュボード からも使用できます。

セキュリティ ツール管理レポート

セキュリティ ツール管理レポートは、次の 3 つのグループに整理できます。

- **概要** – これらのレポートには、管理対象デバイスでウイルス対策定義とスパイウェア対策定義が最後に更新された日時と、これらのデバイスでウイルスとスパイウェアの存在について最後にスキャンされた日時が示されます。
- **製品レポート** – これらのレポートには、クライアント デバイスで検出されたウイルス対策製品、スパイウェア対策製品、およびファイアウォール製品についての情報が含まれます。
  - 製品のタイプごとに、検出された全製品のリストと、これらの製品が検出されたデバイスのリストを表示できます。
  - ウイルス対策ツールとスパイウェア対策ツールについては、最後の定義更新日付を表示し、関係する各デバイスをスキャンできます。
  - ファイアウォール製品については、ファイアウォール規則のリストを表示できます。
- **デバイス レポート** – これらのレポートには、各タイプのセキュリティ ツールが各クライアント デバイスにインストールされているかどうか、有効になっているかどうか、またはインストールされ有効になっているかどうかが示されます。

セキュリティ ツール管理レポートは、[レポート] タブに表示されます。一部のレポートは、セキュリティ ツール管理ダッシュボードからも使用できます。

これらのレポートの多くをフィルタしたり、掘り下げて詳細を調べたりできます。詳細については、74 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、231 ページの「レポートのフィルタ」を参照してください。

これらのレポートは、[レポート] タブに表示されます。一部のレポートは、セキュリティ ツール管理ダッシュボードからも使用できます。

次の各レポートには、管理対象クライアント デバイスにインストールされているセキュリティ ツールの状態に関する要約の統計値が含まれています。

- 製品の要約 ([概要] の下)
- 検出された製品 ([製品レポート] > [全製品] の下)
- スキャン済みデバイス ([デバイス レポート] > [スキャン済みデバイス] の下)

これらの統計情報は、特定のスキャン済みデバイスの [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。

- 69 ページの「脆弱性改善情報の検索」
- 72 ページの「適用状況の失敗に関する情報の検索」
- 74 ページの「セキュリティ ツールに関する情報の検索」

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 操作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、パッチ管理フィルタはパッチ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 *オプション*: 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。

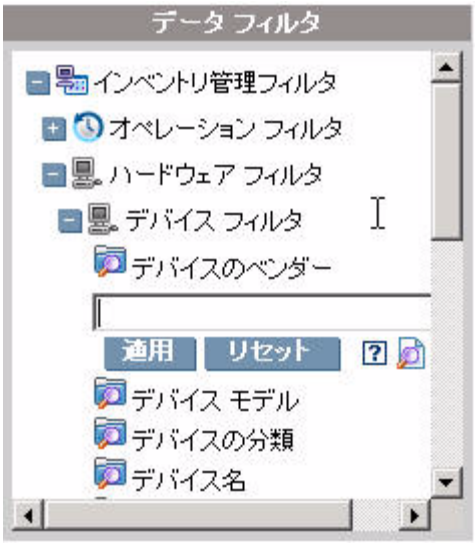
3 テキスト ボックスでフィルタ条件を指定するか、  (条件) ボタンをクリックしてリストから条件を選択します (表示された場合。すべてのフィルタでリストが表示されるとは限りません)。

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 27　　特殊文字とワイルドカード

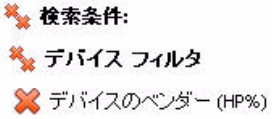
文字	機能	デバイスのベンダーフィルタの例	一致するレコード
* または %	特定のテキスト文字列を含むすべてのレコードに一致する	HP*	「HP」で始まるすべてのレコード
		%HP%	「HP」を含むすべてのレコード
? または _	任意の 1 文字に一致にする	Not?book	「Not」で始まり「book」で終わるすべてのレコード
		Note_ook	「Note」で始まり「ook」で終わるすべてのレコード
!	フィルタを否定する	!HP*	「HP」で始まらないすべてのレコード

たとえば、フィルタに関連付けるデバイスのテキスト ボックスに「HP%」と指定すると、フィルタはベンダー名に HP を含むすべてのデバイスに一致します。



4 **[適用]** ボタンをクリックします。レポートがリフレッシュされます。フィルタを削除するには、**[リセット]** ボタンをクリックします。

フィルタをレポートに適用すると、レポート ヘッダーに次のようにフィルタが表示されます。



一度適用されたフィルタは、明示的に削除されるまで有効な状態が維持されます。フィルタ名の左側にある ([削除] ボタン) をクリックして、現在のレポートからフィルタを削除できます。

また、現在表示されているレポートのデータ フィールドをクリックすることにより、「インライン」フィルタを作成することもできます。たとえば、脆弱性定義レポートを表示しているときに、[高] 重大度の脆弱性のみを表示するには、[重大度] カラムの (高重大度) アイコンをクリックします。

データ ロールアップ用のデバイス グループの作成

HPCA Console には、データの「ロールアップ」操作を実行するための特定のデバイス グループを定義するメカニズムがあります。これらのデバイスの情報は HPCA データベースから取得され、指定の期間で集計 (ロールアップ) されます。

これは、HPCA と通信する別の HP Software 製品を使用して、HPCA レポートの形式で配布されるデータ (レポートに値を設定するために使用されるデータベース テーブル) を取得する場合などに便利です。

実際にデータのロールアップを実行するには、HPCA 要約 (夜間) テンプレートなどの適切なジョブ アクション テンプレートを使用して DTM ジョブを作成します。24 時間以上の間隔を空けてデータのロールアップが実行されるようにジョブ スケジュールを指定してください。詳細については、182 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。

この機能では、今後の HP Software 製品の統合がサポートされます。現在、他の製品では HPCA ロールアップ データは取得されません。

データ ロールアップ用のデバイス グループを作成するには

1 [レポート] タブで、デバイスを表示するレポートを開きます。例 :

[インベントリ管理レポート] > [ハードウェア レポート] > [詳細レポート] > [管理対象デバイス]

2 使用するフィルタ条件を適用します。表示するデバイスがレポートに含まれていることを確認します。詳細については、231 ページの「レポートのフィルタ」を参照してください。

3 左上隅の **[検索条件]** 見出しのすぐ右側にある **[保存]** リンクをクリックします。

レポート フィルタ保存ウィザードが表示されます。

4 デバイス グループの **[表示名]** を入力します。この名前は、ロールアップ データを取得する他の HP Software 製品によって使用されます。最大 32 文字を入力できます。

5 デバイス グループの **[説明]** を入力します。これは、ロールアップ データを表示するユーザーにとって有益な情報になります。最大 255 文字を入力できます。

6 データのロールアップ操作にこのデバイス グループを使用する場合、**[レポートのロールアップに使用する]** を選択します。

7 保存したデバイス　グループの前のバージョンをこのバージョンで置換する場合、**[既存のバージョンを上書き]** を選択します。

8 **[作成]** をクリックします。これで、デバイス グループが保存され、使用できます。

8 オペレーション

[操作] タブでは、インフラストラクチ。ャ タスクを管理したり、コンポーネント サービスのステータスを表示したり、一部のパッチ管理タスクを実行したりすることができます。詳細については、次のセクションで説明します。

Satellite コンソールの [操作] タブには、次のセクションで説明する [サーバーのステータス] と [サポート] 情報が表示されます。

インフラストラクチャ管理

[インフラストラクチャ管理] 操作は、次のセクションで説明します。

サーバーのステータス

[サーバーのステータス] には、現在インストールされているライセンス情報のほか、HPCA Server によって制御されるコンポーネント サービスの一覧が表示されます。これらのコンポーネント サービスは、HPCA 処理の異なる側面を処理します。[サーバーのステータス] の **[要約]** テーブルでは、これらのどのサービスが有効になっているかを確認できます。

コンポーネント サービスのステータスを確認するには

1. HPCA Console で、[操作] タブに移動し、**[サービスのステータス]** をクリックします。
2. コンポーネント サービスの一覧と各サービスが有効になっているかどうかを示す [要約] テーブルが表示されます。

Satellite コンソールの [サーバーのステータス] ページには、その他のプロパティが表示されます。

- 上位サーバー
- データ キャッシュの利用状況
- データ キャッシュの容量
- 同期ステータス

Satellite コンソールの [サーバーのステータス] ページには、データ キャッシュを更新できる **[タスク]** 領域が表示されます。

Satellite を今すぐ同期

Satellite Server のコンテンツ (オペレーティング システム、パッチ、およびオペレーティング システム イメージ) を上位ホストと同期する必要があります。

Satellite Server のデータをキャッシュおよび同期するには、まず Satellite を設定する必要があります。詳細については『HPCA Core および Satellite 入門およびコンセプト ガイド』を参照してください。

同期を実行すると、Satellite 上で有効になっている、各サービスで使用されるコンテンツが同期されます。たとえば、Satellite が完全に有効になっている場合は、次の内容が同期されます。

- HPCA Agent のメンテナンス
- 設定のメタデータ
- ソフトウェアとパッチのためのデータ キャッシュ リソース (データ キャッシュが有効になっている必要があります)
- オペレーティング システム イメージ (オペレーティング システム サービスが有効になっている必要があります)

Satellite Server の同期は、Core Server でジョブを作成することによってスケジュールできます。詳細については、187 ページの「Satellite 同期ジョブの作成」を参照してください。

データ キャッシュをフラッシュ

上位サーバーから重要な新しいリソースをダウンロードする必要があるが、現在のデータ キャッシュの利用状況が容量の限界に近づいているか、またはデータ キャッシュに古いファイルや破損したファイルが含まれている場合は、リソース キャッシュをフラッシュして新しいリソースをすばやく読み込むための空き容量を確保できます。

このオプションによってキャッシュ全体 (ダイナミックおよび事前読み込み) がフラッシュされるため、使用する場合は注意してください。

このアクションで重要なファイルが誤って削除される可能性があります。

サポート

[サポート] 領域には、現在インストールされているライセンス情報が表示されます。また、設定ファイル、ログ ファイル、およびオペレーティング システム情報を含む圧縮ファイル (zip) を生成したりダウンロードしたりすることもできます。

詳細については、240 ページの「ログ ファイルのダウンロード」を参照してください。

これらのファイルは、HP サポートでトラブルシューティングに必要になった場合に使用可能になります。

ログ ファイルのダウンロード

弊社サポート センターに連絡すると、ログ ファイルの提供を求められる場合があります。用意されているリンクを使用して、現在のサーバー ログ ファイルの圧縮ファイルをダウンロードし保存します。

ログ ファイルをダウンロードするには

1 [トラブルシューティング] 領域で、**[現在のサーバー ログ ファイルをダウンロード]** リンクをクリックします。新しいウィンドウが開きます。

2 ログ ファイルが準備できたら、**[logfiles.zip をダウンロードします]** をクリックします。

3 表示メッセージに応じて **[保存]** をクリックし、圧縮ファイルをコンピュータに保存します。

4 ファイルを保存する場所を指定して、**[OK]** をクリックします。

5 ログ ファイルがコンピュータにダウンロードされ、1 つの ZIP 形式ファイルで保存されます。

> Internet Explorer のセキュリティ設定により、これらのファイルをダウンロードできない場合があります。信頼できるサイトに HPCA Console の URL を追加するか、またはファイルのダウンロード時にダイアログを表示しないように Internet Explorer の設定を変更することをお勧めします。

Live Network

Live Network の設定を使用して、HP Live Network のコンテンツを更新する方法と時期を指定します。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。最新のコンテンツ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。

第 5 章、「HPCA および HP Live Network」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。次の中から選択できます。

- **HP Live Network から**

  Live Network のコンテンツ ソースは HP Live Network のコンテンツ 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、別の場所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 登録契約が必要です。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。

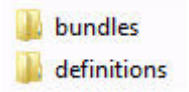
  アクセス権に応じて、コンテンツのタイプ (プレミアムまたは基本) を選択できます。

  取得権利のないコンテンツのタイプを選択した場合 (たとえばプレミアム コンテンツ)、取得は完全に失敗します。つまり、基本的なサポート契約でカバーされているコンテンツ (基本コンテンツ) も含めて、どのコンテンツのタイプも更新されません。取得の失敗を避けるために、取得権利のあるコンテンツのタイプのみを選択してください。

- **ファイル システムから**

  Live Network コンテンツのコピーは、HPCA Core がインストールされているシステムのファイル システム内の場所からパブリッシュされます。コンテンツが格納されているフォルダのパス名を指定し、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 システム内の場所のフォルダ構造が、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、527 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コンテンツがレポート データベースに読み込まれます。

  529 ページの「テスト環境からプロダクション環境への HP Live Network コンテンツの移動」を参照してください。

Live Network の自動更新のスケジュール

選択したコンテンツの送信元からの HP Live Network の自動更新のスケジュールを確立するには、次の手順を使用します。

HP Live Network のコンテンツの自動更新をスケジュールするには

1 [操作] タブで、[インフラストラクチャ管理] 領域を展開し、**[Live Network]** をクリックします。

2 **[スケジュールの更新]** タブをクリックします。

3 [更新] セクションで、コンテンツの送信元を選択します。

4 自動更新のスケジュールを指定します。

   a **スケジュール** - [一度]、[時間単位]、[日単位]、[週単位]、または [なし] を選択します。

   [なし] は、たとえば以前にスケジュールされた [一度] のタスクが既に完了している場合など、現在実行対象のスケジュールがないときに HPCA Console に表示されます。新しい更新スケジュールがない場合や既存のスケジュールを停止する場合に、[なし] を指定できます。反復スケジュールがある場合は、最後に保存されたスケジュールが表示されます (たとえば、[時間単位]、[日単位]、[週単位] など)。

   b **開始時刻** - 更新を開始する時刻。

   c **開始日** - 自動更新を開始する日付  。(カレンダー) ボタンをクリックし、日付を選択します。

[スケジュールの更新] タブが表示されたとき、時刻と日付のフィールドには、最後に保存されたスケジュールの時刻と日付が表示されます。たとえば、以前にスケジュールされた [一度] の更新が既に完了している場合、スケジュールは [なし] に設定され、[開始時刻] と [開始日] のフィールドには最後の更新の時刻と日付が表示されます。

d **[スケジュール]** として [時間単位]、[日単位] または [週単位] を選択した場合は、**[間隔]** ボックスに更新の間隔を指定します。

たとえば、[日単位] を選択し、**[間隔]** に 2 を指定すると、2 日ごとに更新が実行されます。

5 **[保存]** をクリックして、変更内容を実装します。

このタブから離れると、**[保存]** をクリックする前に入力した情報はすべて失われます。情報を保存する場合は、必ず **[保存]** をクリックしてください。

[リセット] ボタンを使用して、最後に保存された設定を復元できます。

HP Live Network コンテンツを今すぐ更新する

HP Live Network のコンテンツを今すぐ更新するには、次の手順を使用します。これは、自動更新用に設定したスケジュールには影響しません。

HP Live Network のコンテンツを直ちに更新するには

1 [操作] タブで、[インフラストラクチャ管理] 領域を展開し、**[Live Network]** をクリックします。

2 **[すぐに更新]** タブをクリックします。

3 この更新のためのコンテンツの送信元を選択します。これは、現在スケジュールされている自動更新には影響しません。

4 **[すぐに更新]** ボタンをクリックします。指定したコンテンツの送信元からコンテンツを更新するためのリクエストが発行されます。

更新は、完了するまでにある程度の時間が必要な非同期のプロセスです。取得レポートを使用すると、更新の結果を表示したり、そのステータスをチェックしたりできます。

更新の結果またはステータスの表示

HPCA レポートを使用すると、HP Live Network コンテンツの更新ステータスをチェックできます。この情報を表示するレポートには、次のいずれかの方法でアクセスできます。

- **[操作] > [インフラストラクチャ管理] > [Live Network]** から [レポート] タブをクリックします。これは、この場所からコンテンツ更新のステータスを確認する最も便利な方法です。
- HPCA Console の [レポート] タブをクリックします。**[HPCA 管理] > [Live Network] > [取得履歴]** へ進みます。
- HPCA Console の [レポート] タブをクリックします。脆弱性、適用状況、またはセキュリティ ツールのコンテンツ更新ステータスについては、次のそれぞれに進んでください。
  - **[脆弱性管理] > [脆弱性レポート] > [取得の詳細]**
  - **[適用状況管理] > [SCAP レポート] > [取得の詳細]**
  - **[セキュリティ ツール管理] > [製品レポート] > [全製品] > [取得の詳細]**

HP Live Network に関連した設定情報が不完全か正しくない場合は、更新が失敗します。これはレポートと次のログ ファイルの両方に反映されます。

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

ただし、この他に更新が失敗したことを示すものは HPCA Console にはありません。

データベース メンテナンス

[データベース メンテナンス] 領域には、HPCA にレポート データが格納されているすべてのデバイスが表示されます。[メンテナンス] ツールバーを使用して、データベースに既に存在しない可能性のあるデバイスのレポート データをクリーンアップします。

デバイスのレポート データを削除するには

1 [メンテナンス] 領域で、レポート データを削除するデバイスを選択します。

2 [レポート データの削除]  ボタンをクリックします。

3 レポート データがデータベースから削除されます。

デバイスのレポート データが削除されると、そのデータはレポートの生成に利用できなくなります。

アクティブに管理されているデバイスのレポート データを削除する場合、レポート データの矛盾を避けるため、削除してから、そのデバイスに Management Agent を再配布します。

ソフトウェア管理

[操作] タブのソフトウェア管理ツールを使用して、管理対象クライアント デバイスに配布できるソフトウェア サービス (アプリケーション) のカタログを管理します。ソフトウェア サービスが HPCA ソフトウェア ライブラリに追加されると、クライアント デバイスのエンドユーザーは Application Self-Service Manager の使用によって付与されているソフトウェアのインストール、更新、または削除を実行できます。

[ソフトウェア ライブラリ] ページには、HPCA にパブリッシュされたソフトウェア サービスがリストされます。このページのツールを使用して、ソフトウェア サービスをインポートまたはエクスポートできます。このインポートおよびエクスポートのツールは、たとえばサービスをテスト環境からプロダクション環境に移動するなど、ソフトウェア サービスを 1 つの HPCA サーバーから別の HPCA サーバーに移動する場合に便利です。

特定のソフトウェア サービスの設定を表示または変更するには、248 ページの「[ソフトウェアの詳細] ウィンドウ ([操作] タブ)」を参照してください。

表 28　ソフトウェア ライブラリ ツール

ボタン	説明
	**データのリフレッシュ** - [ソフトウェア ライブラリ] テーブルのデータをリフレッシュします。
	**CSV にエクスポート** - 開いたり、表示したり、保存したりできる、カンマ区切りのソフトウェア サービスのリストを作成します。
	**サービスのインポート** - ソフトウェア サービスを HPCA にインポートします。246 ページの「ソフトウェア サービスのインポート」を参照してください。 ソフトウェア サービスをインポートしたら、グループまたは特定の管理対象クライアント デバイスをそのサービスに付与できます。次にサービスをこうしたデバイスに配布できます。
	**サービスのエクスポート** - パブリッシュされたソフトウェア サービスを**サービス デッキ**と呼ばれるバイナリ ファイル形式でエクスポートします。247 ページの「ソフトウェア サービスのエクスポート」を参照してください。 ソフトウェア サービスをエクスポートしたら、そのサービス デッキを別の HPCA サーバーにコピーしてから、そのサービスをインポートできます。

ソフトウェア サービスのインポート

HPCA ではソフトウェア サービスをソフトウェア ライブラリにインポートできます。サービスをインポートするには、サービス インポート デッキが HPCA Server の `ServiceDecks` ディレクトリに格納されている必要があります。デフォルトでは、このディレクトリは次の場所にあります。

`InstallDir``\Data\ServiceDecks`

これは、テスト環境を構築してある場合に便利です。テスト環境で特定のサービスを承認したら、プロダクション環境の HPCA Server の `ServiceDecks` ディレクトリにそのサービスをエクスポートします (「ソフトウェア サービスのエクス

ポート」を参照してください)。次に、サービス インポート ウィザードを使用して、そのサービスをプロダクション環境のソフトウェア ライブラリにインポートして、管理対象デバイスに配布します。

サービスをインポートするには

1 **[サービスのインポート]**  をクリックしてサービス インポート ウィザードを起動します。

2 ウィザードの手順に従って、サービスをソフトウェア ライブラリにインポートします。

ServiceDecks フォルダにある、名前に SOFTWARE という単語が含まれるサービスのみをインポートできます。例:

PRIMARY.SOFTWARE.ZSERVICE.ORCA

ソフトウェア サービスのエクスポート

パブリッシュされたソフトウェア サービスは、HPCA Server の ServiceDecks ディレクトリにエクスポートできます。デフォルトでは、このディレクトリは次の場所にあります。

InstallDir\Data\ServiceDecks

エクスポートされたサービスは、別の HPCA Server にコピーして、そのサーバーのソフトウェア ライブラリにインポートできます(「ソフトウェア サービスのインポート」を参照してください)。

サービスをエクスポートするには

1 最初のカラムのチェック ボックスをオンにして、サービスとしてエクスポートするソフトウェアを選択します。

2 **[サービスのエクスポート]**  をクリックして、サービス エクスポート ウィザードを起動します。

3 ウィザードの手順に従って、そのサービスを HPCA Server マシンの ServiceDecks ディレクトリにエクスポートします。

[ソフトウェアの詳細] ウィンドウ ([操作] タブ)

ソフトウェア ライブラリで任意のソフトウェア サービスのサービス ID をクリックして、[ソフトウェアの詳細] ウィンドウを開きます。[ソフトウェアの詳細] ウィンドウを使用して、特定のソフトウェア サービスの設定を表示または変更します。

[ソフトウェアの詳細] ウィンドウでは、次の設定を使用できます。

- **表示名**
  ソフトウェア サービスの名前です。これは HPCA Console で使用される「簡略」名です。これは必須のフィールドです。
- **ソフトウェア カテゴリ**
  ソフトウェアのタイプを定義するためのカテゴリを指定します。ソフトウェア カテゴリは、ソフトウェア ライブラリに表示され、ソート オプションとして利用できます。
- **カタログの表示**
  管理対象クライアント デバイスのカタログにこのソフトウェアを表示するかどうかを指定します。カタログにソフトウェアを表示すると、エンドユーザーは、そのソフトウェアをインストール、更新、または削除できます。
- **再起動の設定**
  ソフトウェアがインストールされた後、管理対象クライアント デバイスの再起動が必要かどうか、およびエンドユーザーに再起動を要求するかどうかを指定します。
- **作成者**
  ソフトウェアの作成者 (たとえば、Hewlett- Packard など)。
- **ベンダー**
  ソフトウェアのベンダー (たとえば、Hewlett- Packard など)。
- **Web サイト**
  ソフトウェアについての情報を参照できる URL。
- **事前アンインストール コマンド ライン**
  ソフトウェアがデバイスから削除される前に実行するコマンド。たとえば、ソフトウェア削除のコマンドを実行する前に、いくつかのレジストリ キーを削除する必要がある場合があります。

- **インストール コマンド ライン**
  ソフトウェアをインストールするために実行するコマンド。
- **アンインストール コマンド ライン**
  ソフトウェアがデバイスから削除された後に実行するコマンド。

ソフトウェアの設定に変更を加えた後は、必ず **[保存]** をクリックしてください。

[管理] タブから [ソフトウェアの詳細] ウィンドウを開く場合、これらの設定は読み取り専用の形式で表示されます。サービスの設定を変更する場合は、必ず [操作] タブから [ソフトウェアの詳細] ウィンドウを開いてください。

ただし、[管理] タブから [ソフトウェアの詳細] ウィンドウを開いた場合、その他の機能は使用可能です。157 ページの「[ソフトウェアの詳細] ウィンドウ ([管理] タブ)」を参照してください。

アウトバンド管理

アウトバンド (OOB) 管理は、[設定] タブを使用して有効にします。OOB 管理の設定については、281 ページの「設定」を参照してください。

OOB 管理の使用方法の詳細については、『HPCA アウトバンド管理ユーザー ガイド』を参照してください。

次のセクションでは、コンソールで実行できる OOB 管理タスクについて説明します。

プロビジョニングと設定情報

vPro デバイスや DASH デバイスを検出したり管理したりできるようにするには、事前にそれらのデバイスをプロビジョニングする必要があります。vPro デバイスが、最初にネットワークに接続されたときに自動的にプロビジョニングされなかった場合は、HPCA Console からこれらのデバイスをプロビジョニングできます。

HPCA Console からの vPro デバイスのプロビジョニングは、『HPCA アウトバンド管理ユーザー ガイド』の「vPro デバイスのプロビジョニング」の章で説明されています。DASH デバイスのみを管理することを選択した場合、このオプションはこのタイプのデバイスに関連しないため、[アウトバンド管理] の下にある [操作] タブには表示されません。

詳細については、『HPCA アウトバンド管理ユーザー ガイド』の「vPro デバイスのプロビジョニング」の章を参照してください。

DASH 設定関連ドキュメント

ここでは、DASH 対応デバイスがこれらのデバイスに付随するドキュメントに従って既にプロビジョニングされていることを前提にしています。DASH 設定の情報は、「Broadcom NetXtreme Gigabit Ethernet Plus NIC」のホワイト ペーパーに記載されています。このホワイト ペーパーは、この NIC をサポートする各製品の [マニュアル] のセクションにあります。

この情報は、当社の DASH 対応デバイスにのみ関連しています。

このドキュメントにアクセスするには

1 http://www8.hp.com/jp/ja/home.html に移動します。

2 [サポート & ドライバ] > [製品マニュアル、トラブルシューティング、修理など] を選択します。

3 この NIC をサポートする製品 (たとえば、dc5850) を入力します。

4 dc5850 モデルの 1 つを選択します。

5 [マニュアル] を選択します。

6 「Broadcom NetXtreme Gigabit Ethernet Plus NIC」のホワイト ペーパーを選択します。

DASH 設定ユーティリティ

DASH 設定ユーティリティ (BMCC アプリケーション) は、この NIC をサポートする各製品のドライバ セクションにある Broadcom NetXtreme Gigabit Ethernet Plus NIC ドライバ Softpaq の一部です。

このユーティリティにアクセスするには

1 http://www8.hp.com/jp/ja/home.html に移動します。

2 [サポート & ドライバ] > [ドライバ & ソフトウェア ダウンロード] を選択します。

3 この NIC をサポートする製品 (たとえば、dc7900) を入力します。

4 dc7900 モデルの 1 つを選択します。

5 オペレーティング システムを選択します。

6 [ドライバ - ネットワーク] セクションまでスクロールし、NetXtreme Gigabit Ethernet Plus NIC ドライバを選択してダウンロードします。

デバイス管理

[デバイス管理] 領域では、複数の OOB デバイスおよび個々の OOB デバイスを管理できます。

[操作] タブの [アウトバンド管理] の下で、[デバイス管理] をクリックします。[デバイス管理] ウィンドウが表示されます。デバイス テーブルのツールバーにあるアイコンから、複数のデバイスに次のタスクを実行できます。

- データのリフレッシュ
- デバイス情報のリロード
- デバイスの探索
- デバイスの電源オン / オフおよび再起動
- vPro 警告のサブスクライブ
- vPro デバイスに関する共通ユーティリティの管理
- 選択された vPro デバイスへのシステム防御ポリシーの配布
- 選択された vPro デバイスへのヒューリスティック ワーム封じ込め情報の配布
- 選択された vPro デバイスへのエージェント ウォッチドッグの配布
- 選択された vPro デバイスへのエージェント ソフトウェア リストとシステム メッセージの配布

個々の OOB デバイスを管理するには、デバイス テーブル内のホスト名のリンクをクリックします。管理ウィンドウが開き、左側のナビゲーション ペインにいくつかのオプションが表示されます。使用可能なオプションは、選択した管理対象デバイスのタイプによって異なります。

詳細については、『HPCA アウトバンド管理ユーザー ガイド』の「グループ管理」の章を参照してください。

グループ管理

[グループ管理] オプションでは、Client Automation ソフトウェアで定義された vPro デバイスのグループを管理できます。vPro デバイスを含む Client Automation グループに対して OOB 操作を実行できます。vPro デバイスのグループを管理することにより、さまざまな検出、自己回復、および保護タスクを実行できます。これには、電源管理、警告の登録契約のほか、システム防御ポリシー、エージェント ウォッチドッグ、ローカルのエージェント ソフトウェア リスト、およびヒューリスティックの配布が含まれます。

[操作] タブの [アウトバンド管理] の下で、[グループ管理] をクリックします。[グループ管理] ウィンドウが表示されます。グループ テーブルのツールバーにあるアイコンから、複数のグループに対して次のタスクを実行できます。

- データのリフレッシュ
- グループ情報のリロード
- グループの電源オン / オフおよび再起動
- vPro 警告のサブスクライブ
- 選択された vPro グループへのエージェント ソフトウェア リストとシステム メッセージの配布
- vPro デバイス グループのプロビジョニング
- 選択された vPro デバイスへのシステム防御ポリシーの配布および回収
- 選択された vPro グループへのエージェント ウォッチドッグの配布および回収
- 選択された vPro グループへのヒューリスティック ワーム封じ込め情報の配布および回収

掘り下げてグループ内の個々のデバイスを管理するには、テーブルの [説明] 列の下にあるグループ名のリンクをクリックします。[デバイス管理] ウィンドウが開き、選択されたグループに属するデバイスの一覧が表示されます。グループ内の複数のデバイスまたは個々のデバイスを管理できます。「デバイスの管理」を参照してください。

詳細については、『HPCA アウトバンド管理ユーザー ガイド』の「グループ管理」の章を参照してください。

警告の通知

vPro デバイスの場合、デバイスに警告のサブスクリプションを割り当てていれば、プロビジョニング済みの vPro デバイスによって生成された警告を表示できます。警告の通知を監視すると、ネットワーク上のデバイスの状態についての適切な情報が得られます。

詳細については、『HPCA アウトバンド管理ユーザー ガイド』の「警告の通知」の章を参照してください。

パッチ管理

[操作] タブのパッチ管理ツールを使用して、管理対象デバイスに配布できるパッチ ブリティンのカタログを管理します。

パッチ ライブラリの操作

[パッチ ライブラリ] ページには、HPCA にパブリッシュされたブリティンがリストされます。このページのツールを使用して、ブリティンをインポートまたはエクスポートできます。このインポートおよびエクスポートのツールは、たとえばパッチをテスト環境からプロダクション環境に移動するなど、パッチを 1 つの HPCA サーバーから別の HPCA サーバーに移動する場合に便利です。

特定のパッチの設定を表示または変更するには、257 ページの「[パッチの詳細] ウィンドウ ([操作] タブ)」を参照してください。

表 29　　パッチ ライブラリのツール

ボタン	説明
	**データのリフレッシュ** - [パッチ ライブラリ] テーブルのデータをリフレッシュします。
	**CSV にエクスポート** - 開いたり、表示したり、保存したりできる、カンマ区切りのパッチのリストを作成します。
	**サービスのインポート** - パッチを HPCA にインポートします。254 ページの「パッチ サービスのインポート」を参照してください。 パッチをインポートしたら、グループまたは特定の管理対象クライアント デバイスをそのサービスに付与できます。次に、パッチをこうしたデバイスに配布できます。
	**サービスのエクスポート** - パブリッシュされたパッチを**サービス デッキ**と呼ばれるバイナリ ファイル形式でエクスポートします。255 ページの「パッチ サービスのエクスポート」を参照してください。 パッチをエクスポートしたら、そのサービス デッキを別の HPCA サーバーにコピーしてから、そのパッチをインポートできます。

パッチ サービスのインポート

HPCA では、パッチをパッチ ライブラリにインポートできます。パッチをインポートするには、デッキ (つまり `xpi` ファイルと `xpc` ファイルと `xpr` ファイル) および `zip` ファイルを HPCA Server の `ServiceDecks` ディレクトリに配置する必要があります。また、`PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.*` ファイルもコピーします。これらには、カタログと Agent 情報が格納されています。これらのファイルがコピーされないか、古いファイルがあると、「インポート

が失敗しました - ブリティンが最近エクスポートされ、最新の PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.* ファイルがコピーされていることを確認してください。」というメッセージが表示されてブリティンのインポートは失敗します。

デフォルトでは、このディレクトリは次の場所にあります。

InstallDir\Data\ServiceDecks

これは、テスト環境を構築してある場合に便利です。テスト環境で特定のパッチを承認したら、プロダクション環境の HPCA Server の ServiceDecks ディレクトリにそのブリティンをエクスポートします (「パッチ サービスのエクスポート」を参照してください)。次に、サービス インポート ウィザードを使用して、そのパッチをプロダクション環境のパッチ ライブラリにインポートして、管理対象デバイスに配布します。

パッチをインポートするには

1 **[サービスのインポート]** をクリックしてサービス インポート ウィザードを起動します。これで、ServiceDecks ディレクトリにある xpi ファイルのリストが表示されます。

2 ウィザードの手順に従って、サービスをパッチ ライブラリにインポートします。

PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpi を明示的に選択する必要はありません。インポートするブリティンを選択すると、黙示的に選択されます。Agent ファイルまたはカタログ ファイルのみをインポート先サーバーに移動する必要がある場合、PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpi を選択できます。

パッチ サービスのエクスポート

パブリッシュされたブリティンは、HPCA Server の ServiceDecks ディレクトリにエクスポートできます。デフォルトでは、このディレクトリは次の場所にあります。

InstallDir\Data\ServiceDecks

パッチをエクスポートするには

1 最初のカラムのチェック ボックスをオンにして、サービスとしてエクスポートするブリティンを選択します。グリッド オプションを使用して、タイプ、名前などに基づいてブリティンを検索します。

2 **[サービスのエクスポート]**  をクリックして、サービス エクスポート ウィザードを起動します。

3 ウィザードの手順に従って、そのブリティンを HPCA Server マシンの ServiceDecks ディレクトリにエクスポートします。

これで、エクスポートされた各ブリティンについて、サーバーの ServiceDecks ディレクトリに次のファイルが作成されます。

- PRIMARY.PATCHMGR.ZSERVICE.*[BULLETIN NAME]*.xpi
- PRIMARY.PATCHMGR.ZSERVICE.*[BULLETIN NAME]*.xpr
- PRIMARY.PATCHMGR.ZSERVICE.*[BULLETIN NAME]*.xpc
- PRIMARY.PATCHMGR.ZSERVICE.*[BULLETIN NAME]*.zip
- PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpi
- PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpr
- PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpc
- PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.zip

メタデータ ベースのパッチ配布モデルでは、この zip ファイルにはゲートウェイ キャッシュにあるバイナリと一部のメタデータ情報が格納されます。これらのバイナリは、エクスポートやインポートの操作中にインポート先サーバーに移動することもできます。Agent とカタログの情報は PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.* ファイルにあります。これらのファイルも明示的にインポート先マシンに移動する必要があります。Redhat ブリティンの場合、依存ブリティンのデータは zip ファイルにあります。

サービスをエクスポートすると、最新の Agent、カタログなど、探索プロセスに必要な関連ファイルが自動的にエクスポートされます。

インポートの場合、PRIMARY.PATCHMGR.ZSERVICE.*[BULLETIN NAME]* という語幹を持つすべてのファイルを PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.* とともに別の

HPCA Server にコピーして、そのサーバーのパッチ ライブラリにインポートする必要があります。254 ページの「パッチ サービスのインポート」を参照してください。

[パッチの詳細] ウィンドウ ([操作] タブ)

パッチ ライブラリで任意のパッチのブリティン名をクリックして [パッチの詳細] ウィンドウを開きます。[パッチの詳細] ウィンドウを使用して、特定のパッチの次のプロパティを表示します。

- **ブリティン タイプ**
  パッチのタイプ (セキュリティ更新など)。
- **ベンダー**
  ソフトウェア ベンダー (Microsoft など)。
- **ブリティン**
  ベンダーによって割り当てられたブリティン名。一般的にはシーケンスコードです。
- **説明**
  ベンダーがそのブリティンに含めた説明テキスト。
- **ベンダーの公開日**
  このブリティンがベンダーによって最初に公開された日付。
- **ベンダーの改訂日**
  このブリティンがベンダーによって改訂された最新の日付。
- **ブリティン情報**
  ベンダーの Web サイトにあるこのブリティンに関する情報の URL。
- **その他の情報**
  ベンダーの Web サイトにある関連情報の URL。

このウィンドウに表示される情報は読み取り専用であり、変更できません。

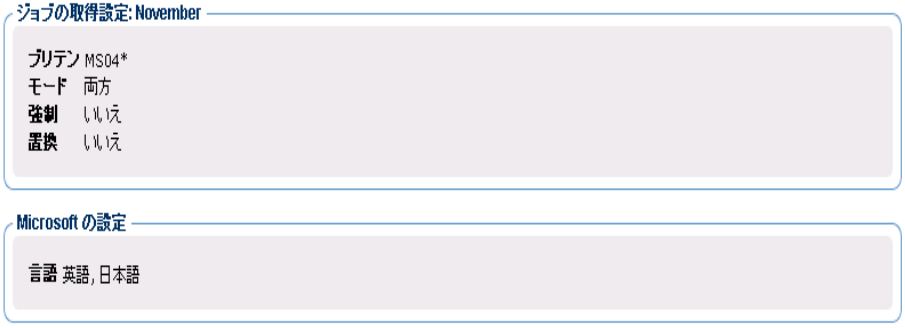
[管理] タブから [パッチの詳細] ウィンドウを開いた場合、その他の機能は使用可能です。172 ページの「[パッチの詳細] ウィンドウ ([管理] タブ)」を参照してください。

取得を開始

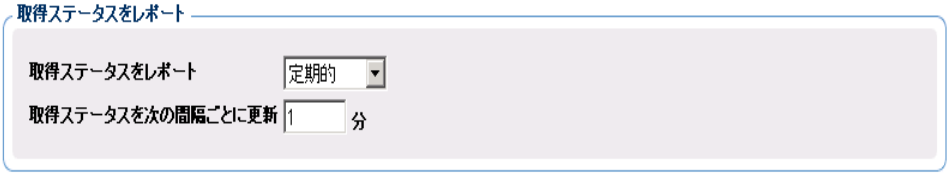
1 [操作] で **[パッチ管理]** を展開し、**[取得を開始]** をクリックします。

2 名前をクリックして、ファイルを選択します。

3 この取得の設定を確認します。



取得ステータスをレポート



- **取得ステータスをレポート** : 取得ログ以外に、取得ジョブを表示したときに表示される現在の取得ステータスを更新する頻度を指定できます。
- **取得ステータスを次の間隔ごとに更新** : [取得ステータスをレポート] フィールドで **[定期的]** を指定した場合は、ステータス ファイルを更新する頻度を選択します。

4 エージェント アップデート設定の注意を読み、**[サブミット]** をクリックして取得を開始します。

取得のステータスをチェックするには

- [レポート] タブを使用して、パッチ取得レポートを表示します。

- [操作] タブの [パッチ管理] 領域を使用して、**取得ジョブを表示**します。

同期を実行

HPCA Configuration Server DB に送信されたパッチ情報は、評価と分析のために Patch SQL データベースと同期する必要があります。HPCA Configuration Server DB と Patch SQL データベースには、同期されるクラスとインスタンスのセットの同じ情報が格納されます。

- PATCHMGR ドメイン内の各クラスは、Patch SQL データベース内のテーブルになります。対応するテーブルは、nvd_classname という名前です。
- 各クラスの各属性は、そのテーブルの列になります。対応する列名は nvd_attributename です。式と接続変数は複製されません。
- クラスの各インスタンスは、対応するテーブルのレコードになります。

この同期は、パッチ取得後、および通常の HPCA 操作で自動的に実行されます。

ただし、手動で同期を実行する必要がある場合があります。たとえば、別の HPCA Server からパッチ情報をインポートした後は、手動でデータベースを同期します。また、ある程度取得を実行した後でパッチ管理用に設定された SQL データベースを切り替える場合も、手動でデータベースを同期します。

HPCA Core Console を使用して、手動でデータベースを同期できます。

データベースを同期するには

1 [操作] タブから、**[パッチ管理]** タスクを展開し、**[同期を実行]** をクリックします。

2 **[サブミット]** をクリックします。

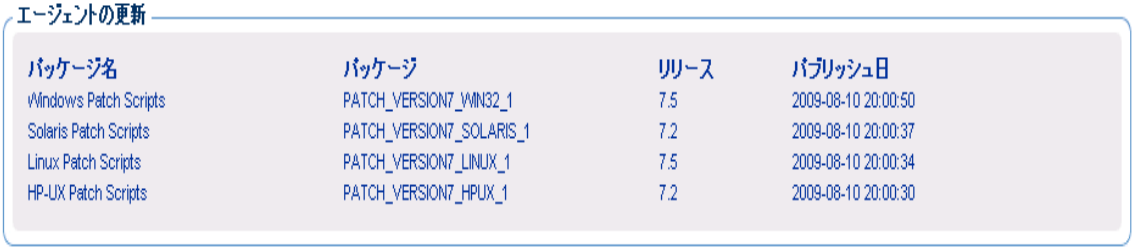
エージェントの更新を表示

パッチの取得を実行するときに、最新バージョンと Patch Agent ファイルの更新情報もダウンロードできます。Patch Agent ファイルには、製品の検出と管理を実行するためのスクリプトが含まれています。これらのファイルは、

HP が提供するパッチ更新の Web サイトから取得されます。ダウンロードした後、ファイルは PATCHMGR ドメインにパブリッシュされ、DISCOVER_PATCH サービス インスタンスに接続されます。

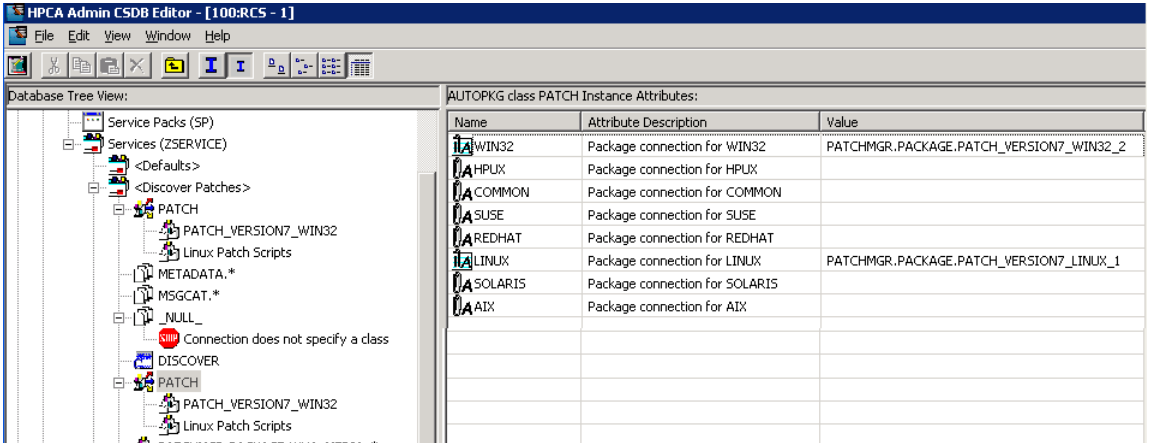
更新のステータスを確認するには、[エージェントの更新を表示] タスクを使用します。[エージェントの更新を表示] は、HPCA Core Console で [操作] タブの [パッチ管理] 領域からアクセスします。これを実行するには、**[エージェントの更新を表示]** をクリックします。

図 45　　エージェントの更新を表示



エージェント ファイルは、DISCOVER_PATCH サービスが Patch Manager ターゲット デバイスで処理されるときに配布されます。これは、DISCOVER_PATCH サービスで、AUTOPKG クラスの PATCH インスタンスに接続することによって実現します。同様に、AUTOPKG.PATCH インスタンスは、**[パブリッシュ]** または **[パブリッシュと配布]** を選択したときに作成されたエージェントのメンテナンス パッケージに接続します。パブリッシュのみを選択した (配布を選択しなかった) 場合は、PACKAGE クラスの適切なインスタンスから AUTOPKG.PATCH インスタンスへの接続を作成する必要があります。これには Admin CSDB Editor を使用します。例は次のとおりです。

図 46　　パブリッシュされたパッケージへの接続の作成



AIX、HP-UX、および Solaris は現在サポートされていません。

[エージェントの更新] には以下の値があります。

- **なし**：エージェントの更新は PATCHMGR ドメインにパブリッシュされません。
- **パブリッシュと配布**：これはデフォルトの値です。更新を PATCHMGR ドメインにパブリッシュし、それらを DISCOVER_PATCH インスタンスに接続して、更新を Patch Manager の管理対象デバイスに配布します。
- **パブリッシュ**：更新は PATCHMGR ドメインにパブリッシュされますが、Patch Manager の管理対象デバイスへの配布のために接続されることはありません。これらの接続は作成する必要があります。

ダウンロードを更新するエージェントの制御のために次の 2 つのパラメータがあります。

- **OS**: エージェントの更新を取得する対象となるオペレーティング システムを指定します。デフォルトは、すべてのオペレーティング システムをダウンロードするものです。有効な値は **Windows** と **Linux** です。

- **バージョン**: エージェントの更新を取得する Patch Manager のバージョンを選択します。Configuration Server には 1 つのバージョンのみをパブリッシュできます。1 つの Configuration Server が複数のバージョンのエージェントをホストすることはできません。その場合は、もう 1 つのバージョン用に別の Configuration Server を作成してください。

最初にインストールした Patch Manager、または現在実装されている Patch Manager より低いバージョンのエージェントは絶対に選択しないでください。

現在のバージョンに更新するには、**バージョン 7** を指定します。新しい Patch Manager 7.50 インストールでは、これがデフォルトです。

移行するお客様は、**[パブリッシュと配布]** オプションを設定し、[エージェントの更新] の [バージョン] を **[バージョン 7]** に設定することをお勧めします。これにより、Windows と Linux の Patch Agent をバージョン 7.50 に正常に移行できます。これは、Microsoft が新しい Microsoft Update Catalog フィードを優先して、`MSSecure.xml` への更新を打ち切った場合に、Microsoft セキュリティ パッチの管理を継続するために必要です。

Microsoft Update からパッチを取得する場合、レポートの [ソース] 列には「Microsoft」ではなく「Microsoft Update」と表示されるため注意してください。

Microsoft Update テクノロジを利用するには、ターゲット デバイスに Windows Update Agent をインストールする必要があります。Patch Manager の取得プロセスでは、Microsoft Update Catalog テクノロジを利用する際、脆弱性のスキャンとパッチの適用に必要な最新の Windows Update Agent を自動的に取得します。DISCOVER_PATCH サービスは、次のエージェント接続で最新の Windows Update Agent を自動的に管理対象デバイスに適用します。

Windows Update Agent (**WUA**) は Windows の自動更新サービスを使用します。これは、ターゲット デバイスで **[自動]** または **[手動]** のいずれかに設定する必要があります。自動更新サービスは、WUA が必要に応じて起動するため、停止状態の場合があります。

取得履歴

以前の取得の詳細を表示するには、パッチ取得ステータス ページを選択します。

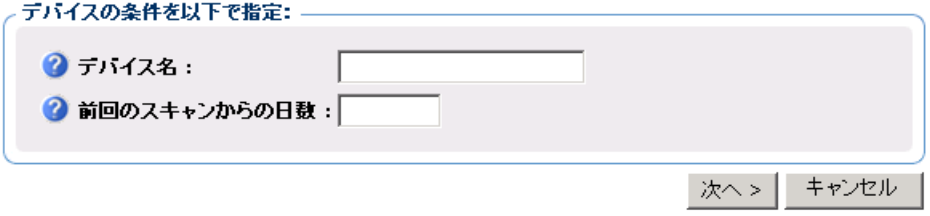
デバイスを削除

コンソールの [操作] タブを使用して、特定のデバイスの Patch Manager 適用状況データを削除できます。

Patch Manager ODBC データベースから適用状況データを削除するには

1 **[操作]** タブをクリックし、**[パッチ管理]** タスクを展開します。

2 **[デバイスを削除]** をクリックします。



3 削除するデバイスのデバイス選択条件を指定します。以下のように行います。

- カンマ区切りのリストで、1 つまたは複数のデバイスを指定します。
- ワイルドカードを使用します。
- そのデバイスで前回の脆弱性スキャンが実行された後の経過日数を指定します。これは、Patch Manager Infrastructure コンポーネントに適合性データをレポートしなくなったデバイスの適合性情報を削除するために使用されます。

4 **[次へ]** をクリックします。コンソールでは、データベースからデバイスを削除する前に、選択フィルタに一致するデバイスをプレビューできます。

5 Patch Manager ODBC データベースからデバイスを削除するには、**[削除]** をクリックします。

このデータベースからデバイスを削除する場合は注意してください。この操作は元に戻せません。

ゲートウェイ設定

Patch Manager ゲートウェイは、**[パッチ管理] > [配布設定]** ページで **[パッチ メタデータのダウンロード]** オプションが有効になっているときに、パッチ バイナリ ファイルを取得してキャッシュするために使用されます。[パッチ メタデータのダウンロード] オプションは、Microsoft Update Catalog データ フィードを使用して Microsoft デバイスにパッチを適用する場合にのみ使用できます。

[操作] タブの [パッチ管理] > [ゲートウェイ設定] 領域では、ゲートウェイに保存されているパッチ ファイルのキャッシュを確認したり管理したりすることができます。

次の各セクションで説明しているパッチ ゲートウェイの操作は Core Server のみに適用され、Satellite Server には適用されません。

事前読み込みゲートウェイ オプション

- 事前読み込みゲートウェイ オプションが無効になっている場合、ゲートウェイは、エージェントからリクエストされた時点でパッチ ファイルをキャッシュします。これがデフォルトであり、この設定をお勧めします。
- 事前読み込みゲートウェイ オプションが有効になっている場合、ゲートウェイは、パッチが取得された時点でパッチ ファイルをキャッシュします。

次のゲートウェイ 操作は、コンソールの領域から使用できます。

- 265 ページの「キャッシュの統計値の表示」
- 266 ページの「キャッシュ コンテンツの詳細」
- 266 ページの「URL リクエストのエクスポート」
- 267 ページの「URL リクエストのインポート」

キャッシュの統計値の表示

現在ゲートウェイにキャッシュされているパッチ ファイルに関する統計、およびゲートウェイがエージェントのパッチ リクエストをどれだけ満たしているかを測定できるヒット、不足、エラー情報を表示するには、[キャッシュの統計値の表示] ページを使用します。ヒット、不足、およびエラー情報のカウンタはリセットできます。

[キャッシュの統計値の表示] ページにアクセスするには

- コンソールの **[操作]** タブから、**[パッチ管理] > [ゲートウェイ設定] > [キャッシュの統計値の表示]** を選択します。

ゲートウェイ キャッシュの統計値

- **合計キャッシュ サイズ** : ゲートウェイ キャッシュ内のすべてのパッチの合計サイズ (MB)。

  キャッシュ サイズが、[パッチ配布設定] ページの [パッチ ゲートウェイ オペレーション] で設定されている [最大キャッシュ サイズ] を超えた場合は、最も使用頻度の低い、古いパッチが削除されます。
- **ファイル数** : パッチ ゲートウェイ キャッシュのダウンロードできるアクティブなファイルの数。
- **ヒットしたキャッシュ** : 前回のカウンタ リセット以降に対応したリクエストの数。
- **不明キャッシュ** : 前回のカウンタ リセット以降にベンダーからのダウンロードを必要としたリクエストの数。
- **キャッシュ ダウンロード エラー** : 前回のカウンタリセット以降にゲートウェイで検出されたダウンロード エラーの数。このエラーは、HPCA-PATCH-3467.log ファイルに含まれています。
- **ヒット率** : 全リクエスト数のうち、キャッシュで対応したリクエストの割合。
- **キャッシュ カウンタ リセット日時** : キャッシュ カウンタの統計値がリセットされた日付と時刻。
- **リセットされたキャッシュ カウンタの統計値** : このエントリをクリックすると、ヒットしたキャッシュ、不明キャッシュ、およびキャッシュダウンロード エラーのカウンタがリセットされます。

キャッシュ コンテンツの詳細

ゲートウェイにキャッシュされているパッチ バイナリ ファイルの現在のセット (ブリティン番号単位) を表示するには、[キャッシュ コンテンツの詳細] ページを使用します。

[キャッシュの統計値の表示] ページにアクセスするには

- コンソールの **[操作]** タブから、**[パッチ管理] > [ゲートウェイ設定] > [キャッシュ ファイルの統計値]** を選択します。

キャッシュ コンテンツの詳細の表示

[キャッシュ コンテンツの詳細] ページには、キャッシュされたブリティンが番号単位で表示されます。特定のブリティンでキャッシュされたバイナリのリストを表示するには、そのブリティン番号をクリックします。さらに詳細な情報を表示するには、バイナリ ファイルをダブルクリックします。

URL リクエストのエクスポート

ゲートウェイ サーバーがベンダーのダウンロード サイトに接続できない場合は、これらの未対応の Agent リクエスト ファイルをエクスポートし、インターネットに接続された別のゲートウェイ サーバーにインポートできます。

[URL リクエストのエクスポート] 操作を使用すると、未対応の URL リクエストのリストを表示およびフィルタし、そのリストを別のパッチ ゲートウェイ サーバーにインポートできます。

URL をエクスポートすると、任意の名前を付けた XML ファイルとして、それらのコンテンツを保存するよう求められます。この XML ファイルには、エクスポート中に選択されたパッチ URL が含まれます。

[URL リクエストのエクスポート] ページにアクセスするには

- コンソールの **[操作]** タブから、**[パッチ管理] > [ゲートウェイ設定] > [URL リクエストのエクスポート]** を選択します。

未対応の URL リクエストのリストをエクスポートするには

1 [表示設定のリスト] 領域を使用して、未対応のリストにフィルタを適用し、エクスポートするリストを絞り込みます。

表示設定のリスト

すべての未対応パッチ リクエストのリストを URL 名でフィルタするには、**[URL フィルタの式]** を入力します。ワイルドカードを指定できます。**[適用]** をクリックして、フィルタを適用します。

1 ページに含める URL リストの数を設定するには、**[ページ数]** ドロップダウンを使用します。

URL の完全なリストに戻すには、エントリを * にリセットし、**[適用]** をクリックします。

このページに未対応の URL リクエストが表示されている場合は、[サブミット] をクリックして、現在未対応のリクエストのエクスポート ファイルをダウンロードします。

URL リクエストのインポート

[URL リクエストのエクスポート] 操作からエクスポートされた URL は、[URL リクエストのインポート] ページを使用して、別のパッチ ゲートウェイ サーバーにインポートできます。インポートされたファイルはパッチ ゲートウェイ サーバーに格納され、そのサーバーでのみ使用できます。

[URL リクエストのエクスポート] ページにアクセスするには

- コンソールの **[操作]** タブから、**[パッチ管理] > [ゲートウェイ設定] > [URL リクエストのインポート]** を選択します。

URL リクエストをインポートするには

1. URL リクエストをインポートするゲートウェイのローカル ドライブに [URL リクエストのエクスポート] タスクの使用後に保存されたファイルをコピーします。
2. **[インポートするリクエスト ファイル]** 領域で、**[ブラウズ]** をクリックして、[URL リクエストのエクスポート] タスクで保存された XML ファイルを見つけます。
3. 指定したファイルへの未対応リクエストのインポートを開始するには、**[サブミット]** をクリックします。

   [ゲートウェイ URL リクエストのインポート] ページには、インポートされる URL、完了ステータス、および完了のパーセンテージが表示されます。

OS 管理

[操作] タブの OS 管理ツールを使用して、管理対象デバイスに配布できるオペレーティング システムのカタログを管理します。

[OS ライブラリ] ページには、HPCA にパブリッシュされたオペレーティング システムがリストされます。このページのツールを使用して、オペレーティング システムをインポートまたはエクスポートできます。ライブラリでは、任意のオペレーティング システムについて配布可能な CD (または DVD) を作成することもできます。

このインポートおよびエクスポートのツールは、たとえば OS をテスト環境からプロダクション環境に移動するなど、オペレーティング システムを 1 つの HPCA サーバーから別の HPCA サーバーに移動する場合に便利です。

特定のオペレーティング システムの設定を表示または変更するには、271 ページの「[OS の詳細] ウィンドウ ([操作] タブ)」を参照してください。

表 30　　OS ライブラリのツール

ボタン	説明
	**データのリフレッシュ** - [OS ライブラリ] テーブルのデータをリフレッシュします。
	**CSV にエクスポート** - 開いたり、表示したり、保存したりできる、カンマ区切りのオペレーティング システムのリストを作成します。
	**サービスのインポート** - オペレーティング システムを HPCA にインポートします。269 ページの「OS サービスのインポート」を参照してください。 オペレーティング システムをインポートしたら、グループまたは特定の管理対象クライアント デバイスをその OS に付与できます。次に、OS をこうしたデバイスに配布できます。

表 30　OS ライブラリのツール

ボタン	説明
	**サービスのエクスポート** - パブリッシュされたオペレーティング システムを**サービス デッキ**と呼ばれるバイナリ ファイル形式でエクスポートします。270 ページの「OS サービスのエクスポート」を参照してください。 オペレーティング システムをエクスポートしたら、そのサービス デッキを別の HPCA サーバーにコピーしてから、その OS をインポートできます。
	**CD 配布メディアの作成** - OS イメージをダウンロードして、オペレーティング システム配布用の DVD に保存できます。270 ページの「配布メディアの作成」を参照してください。

OS サービスのインポート

HPCA では、オペレーティング システムを OS ライブラリにインポートできます。サービスをインポートするには、サービス インポート デッキが HPCA Server の `ServiceDecks` ディレクトリに格納されている必要があります。デフォルトでは、このディレクトリは次の場所にあります。

`InstallDir``\Data\ServiceDecks`

これは、テスト環境を構築してある場合に便利です。テスト環境で特定のサービスを承認したら、プロダクション環境の HPCA Server の `ServiceDecks` ディレクトリにそのサービスをエクスポートします (「OS サービスのエクスポート」を参照してください)。次に、サービス インポート ウィザードを使用して、そのサービスをプロダクション環境の OS ライブラリにインポートして、管理対象デバイスに配布します。

サービスをインポートするには

1　**[サービスのインポート]**  をクリックしてサービス インポート ウィザードを起動します。

2 ウィザードの手順に従って、サービスを OS ライブラリにインポートします。

ServiceDecks フォルダにある、名前に OS という単語が含まれるサービスのみをインポートできます。例 :

PRIMARY.OS.ZSERVICE.WIN732

OS サービスのエクスポート

パブリッシュされたオペレーティング システムは、HPCA Server の ServiceDecks ディレクトリにエクスポートできます。デフォルトでは、このディレクトリは次の場所にあります。

InstallDir\Data\ServiceDecks

エクスポートされたサービスは、別の HPCA Server にコピーして、そのサーバーの OS ライブラリにインポートできます (「OS サービスのエクスポート」を参照してください)。

サービスをエクスポートするには

1 最初のカラムのチェック ボックスをオンにして、サービスとしてエクスポートする OS を選択します。

2 **[サービスのエクスポート]** をクリックして、サービス エクスポート ウィザードを起動します。

3 ウィザードの手順に従って、そのサービスを HPCA Server マシンの ServiceDecks ディレクトリにエクスポートします。

配布メディアの作成

CD 配布メディアの作成ツールを使用すると、イメージをダウンロードしてオペレーティング システムの配布用の DVD に保存できます。

OS ライブラリには、HPCA にパブリッシュされたすべてのオペレーティング システムがリストされます。

DVD 配布のためにオペレーティング システム イメージをダウンロードするには

1 [操作] タブで、**[OS 管理] > [CD ライブラリ]** に移動します。

2 OS ライブラリからオペレーティング システムを選択します。

3 **[CD 配布メディアの作成]** ボタンをクリックして CD 配布ウィザードを起動します。

4 要約情報を確認し、**[ダウンロード]** をクリックします。OS イメージのダウンロードがバックグラウンドで開始されます。

5 **[閉じる]** をクリックします。

ダウンロードの進行状況が [OS ライブラリ] に表示されます。現在のステータスを [CD 作成ステータス] カラムに表示するには、**[リフレッシュ]** ボタンをクリックします。

ダウンロードが完了すると、OS イメージはデフォルトで次のディレクトリに格納されます。

InstallDir\Data\ServiceDecks\CDDeployment

このディレクトリが空の場合は、リストにあるオペレーティング システムの [CD 作成ステータス] カラムが空白です。

この機能は、通常は複数のイメージを格納するために、DVD で使用するためのものです。複数の CD-ROM または DVD-ROM を同時に使用して、リソースをスパンしないでください。

DVD-ROM は Joliet 形式である必要があります。

[OS の詳細] ウィンドウ ([操作] タブ)

OS ライブラリで任意のオペレーティング システムのサービス ID をクリックして、[OS の詳細] ウィンドウを開きます。[OS の詳細] ウィンドウを使用して、特定のオペレーティング システムの設定を表示または変更します。

[OS の詳細] ウィンドウでは、次の設定を使用できます。

- **表示名**
  [OS ライブラリ] ページに表示される OS の名前。これは必須のフィールドです。
- **作成者**
  OS の作成者。

- **ベンダー**
  OS のベンダー。
- **Web サイト**
  OS についての情報を参照できる URL。

OS の設定に変更を加えた後は、必ず **[保存]** をクリックしてください。

[管理] タブから [OS の詳細] ウィンドウを開く場合、これらの設定は読み取り専用の形式で表示されます。サービスの設定を変更する場合は、必ず [操作] タブから [OS の詳細] ウィンドウを開いてください。

ただし、[管理] タブから [OS の詳細] ウィンドウを開いた場合、その他の機能は使用可能です。157 ページの「[ソフトウェアの詳細] ウィンドウ ([管理] タブ)」を参照してください。

利用状況管理

[利用状況管理] セクションを使用して、利用状況収集フィルタを設定します。

HPCA を使用した利用状況データの収集および分析および名前を変更したデバイスの処理の詳細については、『Application Usage Manager ユーザー ガイド』を参照してください。

収集フィルタ

[利用状況の収集] ページを使用して、利用状況収集フィルタの作成および管理を行います。

アプリケーション利用状況データを収集するには、HP Client Automation Standard または HP Client Automation Enterprise が必要です。

利用状況収集フィルタは、利用状況収集エージェントがどの利用状況データをレポートに利用できるようにするかを決定します。利用状況収集エージェントがデバイスに配布されると、全アプリケーションの全利用状況データが収集されローカルに保存されます。作成して有効にした利用状況フィルタによって、HPCA に送信するローカルの利用状況データが決定します。

利用状況収集エージェントがすでに配布された後にフィルタを有効にすると、フィルタで指定され、収集されてローカルに保存されていた利用状況データがすべて HPCA にレポート用に送信されます。

たとえば、利用状況収集エージェントが 5 月に配布され、フィルタが Microsoft Word に対して有効になると、Microsoft Word の利用状況データのすべてが、指定したスケジュールに基づいて HPCA に送信されます。さらに 6 月に、Microsoft Excel に対して新しいフィルタを作成し、有効にすると決めました。次回利用状況データが HPCA に送信されるとき、5 月に初めて利用状況収集エージェントがインストールされた日から 6 月の現在の日付までの、収集されローカルに保存されていた Excel 利用状況データもすべて送信されます。その後、両方のアプリケーションについて、利用状況の送信が続きます。

利用状況データは、12 か月の間、管理対象デバイスでローカルに保存されます。

利用状況収集フィルタの設定手順は、次を参照してください。

- 273 ページの「利用状況収集フィルタの設定」
- 274 ページの「利用状況条件の定義」

利用状況収集エージェントを配布し、収集スケジュールを指定する方法については、利用状況収集エージェントの配布を参照してください。

利用状況収集フィルタの設定

HPCA にはデフォルトで、あらかじめ設定された収集フィルタが備えられています。これらの収集フィルタは、新しいフィルタを作成する場合にモデルとして使用したり、ニーズに合うように変更したりできます。

利用状況収集フィルタ作成ウィザードを使用して、新しい利用状況収集フィルタを作成します。既存のフィルタを変更するには、[フィルタの詳細] ウィンドウを使用してください。

ワイルドカード文字を使用して利用状況データを収集するフィルタを設定すると、大量のデータが収集されることになる場合があります。この場合、データベースのサイズが大きくなるにつれて、レポートのパフォーマンスに重大な問題が生じる可能性があります。HP では、利用状況情報が必要なアプリケーションについてのみ、データを収集するフィルタを作成することを強くお勧めします。すべてのアプリケーションの利用状況データを収集するのは避けてください。

収集フィルタを作成するには

1 [収集フィルタ] ページで **[新しいフィルタの作成]**  ツールバー ボタンをクリックします。利用状況収集フィルタ作成ウィザードが起動します。

2 ウィザードの手順に従って、新しい収集フィルタを作成し有効にします。

収集フィルタを有効にするには

1 フィルタ リストで、フィルタの説明の左にあるボックスをクリックし、有効にするフィルタを選択します。

2 **[選択したアイテムの有効化]**  ツールバー ボタンをクリックします。

3 **[OK]** をクリックして、選択したフィルタを有効にします。ステータス ダイアログに結果が表示されます。

4 **[閉じる]** をクリックして、ステータス ダイアログを閉じます。

既存のフィルタを変更するには

1 フィルタ リストで、フィルタの説明リンクをクリックして、[フィルタの詳細] ウィンドウを開きます。

2 [フィルタ条件] 領域に、利用状況データを収集するときに使用する具体的なフィルタ条件を入力します。選択する条件を決定するには、274 ページの「利用状況条件の定義」を参照してください。

3 **[保存]** をクリックします。

利用状況条件の定義

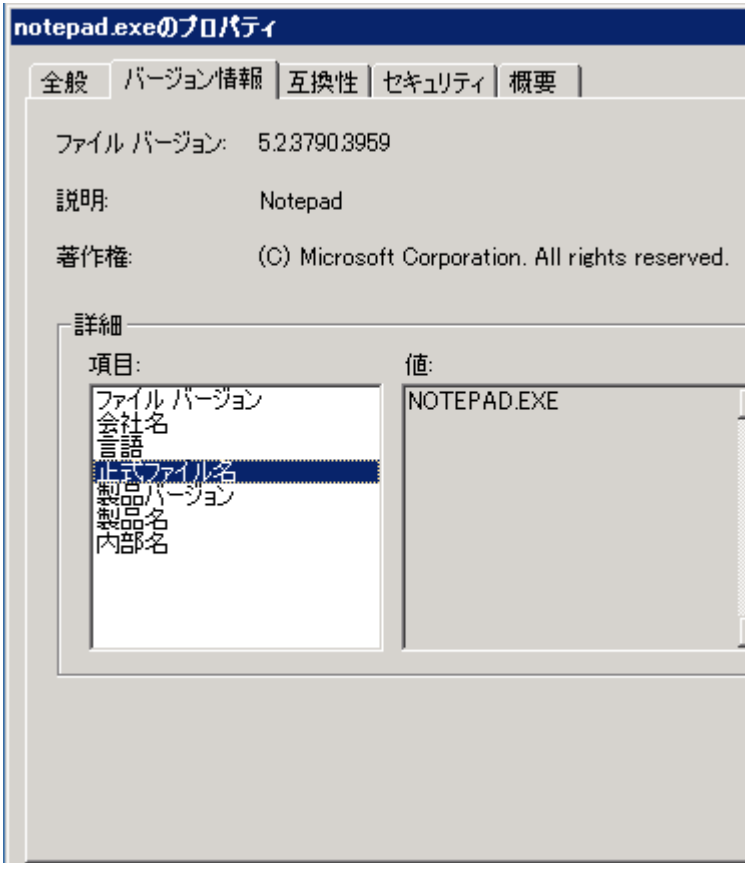
利用状況収集エージェントは、ローカルの各実行可能ファイルのファイル ヘッダー情報を使用して、そのアプリケーションが定義されたフィルタ条件に適合するか判断します。フィルタを定義するときに、ファイル ヘッダー情報を使用して、どの条件を使用するか決定できます。

ファイル ヘッダー情報を決定するには

1 システムの実行可能ファイルを右クリックします。

2 ショートカット メニューから **[プロパティ]** を選択します。

3 [プロパティ] ウィンドウで **[バージョン]** タブをクリックします。



[項目] および **[値]** ボックスに含まれる情報は、利用状況収集エージェントが、利用可能な利用状況データをフィルタするために使用します ([言語] および [内部名] の各項目は、現在サポートされていないため除外されます)。

すべての実行可能ファイルで、ファイル ヘッダーに格納された値のサポートや、正しい取得が行われるわけではありません。

次の例は、特定のアプリケーションについて検索するフィルタの作成方法を説明しています。

notepad.exe の利用状況データにフィルタを設定するには

1 利用状況収集フィルタ作成ウィザードを起動して、新しい利用状況フィルタを作成します。

2 [プロパティ] の手順で、次のフィルタ条件を定義します。

— **説明** : Notepad

— **有効** : Yes

— **ファイル / アプリケーション名** : notepad.exe

3 利用状況収集エージェントを 1 つ以上の管理対象デバイスに配布します。詳細については、216 ページの「利用状況収集エージェントの配布」を参照してください。

利用状況データが毎週 HPCA に送信されます。これには利用状況収集エージェントがインストールされている全デバイスに対するメモ帳の利用状況データのすべてが含まれます。

設定管理

[設定管理] セクションを使用して、設定プロファイルを作成、変更、削除します。設定プロファイルを使用して、使用環境で管理対象デバイスにインストールされているソフトウェアの設定のグループを作成できます。設定プロファイルは、デバイスのカスタマイズした設定で構成されています。これには、アプリケーション、オペレーティング システム、およびハードウェアに関連する設定が含まれています。設定プロファイルを作成または変更することで、目的の製品の設定の制御データを分析およびパラメータ化できます。

設定プロファイルを作成または変更すると、関連するソフトウェアがインストールされている管理対象システムに配布できます。HPCA Enterprise では、設定プロファイルはサービスとしてリストされ、他のサービスの配布と同じように、ポリシー付与資格を通じて管理対象マシンに配布できます。

設定プロファイルを作成して配布すると、ソフトウェアの概要レポートを表示できるようになるため、管理者はこのソフトウェアのランタイム データを視覚的に確認できます。

このセクションは、次のトピックで構成されています。

設定テンプレート

設定テンプレートを使用して、設定プロファイルのインスタンスを作成します。設定テンプレートの最新コンテンツは、HP Live Network サイトからダウンロードできます。HPCA および HP Live Network を参照してください。

提供されている任意の設定テンプレートを選択して、追加のプロファイルを作成したり、既存のプロファイルを変更したりできます。HPCA Console の [操作] タブには [設定管理] の下に **[設定テンプレート]** 領域があり、システムで設定可能なプロファイルを持つソフトウェアを確認できます。

新規プロファイルの作成

システムには、設定可能なプロファイルが含まれるソフトウェアの追加プロファイルを作成できます。設定テンプレートは、この目的で提供されています。テンプレートを使用して、関連するソフトウェアの設定プロファイルのインスタンスを作成できます。空白のプロファイルで開始することも、作成するプロファイルと似ているものがあれば既存のプロファイルを複製することもできるため、実行手順は簡単です。

新しい設定プロファイルを作成するには

1. [操作] タブで左側のナビゲーション ペインの [設定管理] を展開し、**[設定テンプレート]** リンクをクリックします。プロファイル設定が可能なソフトウェアは、右側のコンテンツ エリアに表示されます。
2. **[表示名]** カラムで、新しいプロファイルを作成するソフトウェアの名前をクリックします。ウィンドウが開き、次のタブが表示されます。
   - プロファイル : 選択したソフトウェアの既存のプロファイルを表示します。このタブで、設定プロファイルを作成、表示、変更、および削除できます。山かっこ (< >) で囲まれて表示されるプロファイル名は、HP が提供するプロファイルです。

     これらのプロファイルを変更した場合、次回 HP Live Network サイトから設定コンテンツを更新すると、変更内容が失われることにご注意ください。
   - 詳細 : テンプレートの目的と使用方法に関する情報が表示されます。

3 [プロファイル] タブで、[設定プロファイル] テーブルにあるツールバーの **[プロファイルの新規作成]**  をクリックします。設定プロファイル作成ウィザードが開きます。

別の方法として、コピーする既存のプロファイルの隣にあるチェック ボックスをオンにして **[選択したプロファイルをコピー]**  をクリックします。この場合、設定プロファイルのコピーおよび変更ウィザードが開きます。このウィザードでは、選択した既存のプロファイルを複製できます。既存のプロファイルをコピーするように選択すると、プロファイルの [表示名] を除き、すべてのフィールドには選択した既存のプロファイルの値が入力されます。

4 どちらのウィザードでも、次の情報を指定します。

— **表示名** : プロファイルの名前を入力します

— **説明** : プロファイルの説明を入力します

5 **[次へ]** をクリックします。ウィザードの次のページが開くと、特定のソフトウェアに固有のプロパティを入力できます。コピーの場合、これらのフィールドは最初から入力されています。必要に応じて、これらのフィールドを変更します。

ソフトウェアのマニュアルを参照して、関連するプロパティ設定の詳細を確認してください。

6 ウィザードに従って、**[作成]** または **[コピー]** をクリックします。新規作成されたプロファイルは、[プロファイル] タブの [設定プロファイル] テーブルにリストされます。[操作] 領域のプロファイルの数も、最新の追加を反映して更新されます。

既存のプロファイルの変更

設定可能なプロファイルがあるソフトウェアのプロパティ設定は、表示して変更できます。

設定プロファイルを変更するには

1 [操作] タブで左側のナビゲーション ペインの [設定管理] を展開し、**[設定テンプレート]** リンクをクリックします。プロファイル設定が可能なソフトウェアは、右側のコンテンツ エリアに表示されます。

2 **[表示名]** カラムで、プロファイルを変更するソフトウェアの名前をクリックします。ウィンドウが開き、[プロファイル] タブで選択したソフトウェアの既存のプロファイルが表示されます。

3 **[表示名]** カラムの [プロファイル] タブで、変更するプロファイルの名前をクリックします。[要約] タブと [プロパティ] タブがあるウィンドウが開き、選択したプロファイルのすべてのプロパティが表示されます。

4 必要に応じて、両方のタブでプロパティの値を変更します。

5 **[保存]** をクリックして、変更を保存します。

プロファイルの削除

必要なくなったソフトウェアの設定プロファイルは削除できます。

設定プロファイルを削除するには

1 [操作] タブで左側のナビゲーション ペインの [設定管理] を展開し、**[設定テンプレート]** リンクをクリックします。プロファイル設定が可能なソフトウェアは、右側のコンテンツ エリアに表示されます。

2 **[表示名]** カラムで、プロファイルを削除するソフトウェアの名前をクリックします。ウィンドウが開き、[プロファイル] タブで選択したソフトウェアの既存のプロファイルが表示されます。

3 [プロファイル] タブで、削除するプロファイル名の隣にあるチェック ボックスをオンにします。

4 ツールバーで **[設定プロファイルの削除]**  をクリックします。ポップアップの確認ウィンドウが開きます。

選択したプロファイルが外部のポリシー ディレクトリに付与されている場合、続行する前にこれらの付与資格を手動で削除する必要があります。削除しないと、Agent 接続障害 (エラー コード 650 としてレポートされます) が起こる場合があります。

5 続行する場合は **[はい]** をクリックします。ウィンドウが開き、操作のステータスが表示されます。

6 **[閉じる]** をクリックして、ステータス ウィンドウを閉じます。削除されたプロファイルは、そのアプリケーションの [設定プロファイル] テーブルにリストされません。[操作] 領域のプロファイルの数は、最新の削除を反映して更新されます。

9 設定

[設定] 領域では、コンソールへのユーザー アクセスの管理、インフラストラクチャ サーバーの定義と設定、パッチ取得のスケジュールと設定の管理、ハードウェアの管理、および ODBC の設定を行うことができます。

[設定] タブは、管理者ロール グループに属しているゾーン アカウントを持つ Enterprise ライセンス ユーザーのみ使用できます。

[設定] タブの左側にあるナビゲーション領域のリンクを使用して、さまざまな設定オプションにアクセスします。これらのオプションについては、次のセクションで説明します。

Core の設定オプション

- 282 ページの「ライセンス」
- 283 ページの「Core コンソールのアクセス制御」
- 291 ページの「インフラストラクチャ管理」
- 330 ページの「デバイス管理」
- 333 ページの「パッチ管理」
- 367 ページの「アウトバンド管理」
- 371 ページの「OS 管理」
- 373 ページの「ダッシュボード」
- 372 ページの「利用状況管理」

Satellite の設定オプション

- 282 ページの「ライセンス」
- 282 ページの「アップストリーム ホスト」
- 292 ページの「SSL」
- 287 ページの「Satellite コンソールのアクセス制御」

- 289 ページの「設定」
- 290 ページの「データ キャッシュ」
- 366 ページの「Satellite コンソールのパッチ管理」
- 295 ページの「ポリシー」
- 371 ページの「OS 管理」
- 331 ページの「シン クライアント」
- 312 ページの「マルチキャスト」

ライセンス

機能的な HPCA 環境を実現するには、HP によって発行された有効なライセンスが必要です。コンソールのこの領域でライセンス ファイルが保存され、インストールされているライセンスのエディション (Starter、Standard、または Enterprise) が表示されます。このセクションを使用して HPCA ライセンスを確認および更新することもできます。

新しいライセンスを適用するには

1 新しい `license.nvd` ファイルからライセンス情報をコピーして、**[ライセンス データ]** テキスト ボックスに貼り付けます。

ライセンス ファイルからライセンス情報をコピーする場合、`[MGR_LICENSE]` という行より前のテキストは含めないでください。含めた場合、ライセンス情報がコンソールから読み取れなくなります。

2 **[保存]** をクリックします。更新されたライセンス情報が、**[現在のライセンス]** の後に表示されます。

アップストリーム ホスト

アップストリーム ホスト サーバーの情報を編集するには、Satellite コンソールの [設定] タブにある **[アップストリーム ホスト]** 領域を使用します。アップストリーム サーバーは、この Satellite が同期を取り、サービスが無効またはリソー

スが使用不可の場合にリクエストの情報をフェッチするサーバーです。このサーバー間通信には SSL を使用できますが、使用するには、アップストリーム サーバーが SSL リクエストを受信できる必要があります。

アクセス制御

このパネルの管理制御は、Core コンソールと Satellite コンソールで異なります。

- HPCA 管理者は、Core コンソールのアクセス制御を使用してコンソールへのユーザー アクセスを設定および管理できます。283 ページの「Core コンソールのアクセス制御」を参照してください。
- HPCA 管理者は、Satellite コンソールのアクセス制御を使用して認証メソッドを選択および設定できます。287 ページの「Satellite コンソールのアクセス制御」を参照してください。

Core コンソールのアクセス制御

[アクセス制御] セクションを使用して、一意のカスタム ID とパスワードを持つコンソール **ユーザー** (283 ページの「[ユーザー] パネル」を参照) のインスタンスを作成します。次に、**ロール** (286 ページの「[ロール] パネル」を参照) をユーザーに割り当てて、ユーザーがアクセスできるコンソールの領域と許可されている管理タスクを管理します。

[ユーザー] パネル

[ユーザー] パネルで、ユーザー インスタンスを作成してロールを各インスタンスに割り当てます。ロールによって、各ユーザーがアクセスできるコンソールの領域が決まります。ユーザーを削除したり、そのロールを変更したりできます。

管理ジョブには、ジョブを作成するため使用されたユーザー ID を表示する、[作成者] フィールドがあります。表示されるユーザー ID は、この領域で作成されたユーザー ID です。

- デフォルトでは、インストール後のデフォルトのコンソール ユーザーは **admin** の 1 人だけで、デフォルトのパスワードは **secret** です。この「フェイルセーフ」ユーザー アカウントにはコンソールへの完全なアクセス権があり、削除できません。

- HPCA Console ユーザーは、次で説明するように**内部**または**外部**のいずれかになります。
  - **内部ユーザー**
    [ユーザー] パネルで作成するユーザーは、すべて「内部」ユーザーとして作成されます。これらのユーザーは、Core コンソールを使用して削除および更新できます。
  - **外部ユーザー**
    Enterprise Edition の場合、HPCA 管理者は外部ディレクトリ (LDAP や Active Directory など) を使用してユーザーを追加したり、アクセス許可や認証情報を設定したりできます。これらの「外部」ユーザーは、Core コンソールでは作成、削除、または更新できません。これを行うには、管理者は LDAP/AD ツールを使用する必要があります。ただし、HPCA 管理者は認証用のディレクトリ ソースを設定できます。このソースは [ユーザー] パネルに表示されます。[ソース] カラムでは、ユーザーの取得元のディレクトリが参照されます。
- 現在アクティブなユーザーも削除できません。現在アクティブなユーザーを削除するには、ログアウトして、別のユーザーとしてログインしなおす必要があります。これで、以前にアクティブだったユーザーを削除できます。

次のセクションでは、[ユーザー] パネルで実行できる管理タスクの詳細について説明します。

コンソール ユーザーを作成するには

1 **[新しいユーザーの作成]** ボタン  をクリックして、ユーザー作成ウィザードを起動します。

2 ウィザードの手順に従って、コンソール ユーザーを追加します。

ユーザー ID の考慮事項

ユーザー ID には、スペース、スラッシュ (/)、またはバックスラッシュ (\) を含めることはできません。

- スペースまたはバックスラッシュが含まれている場合、「作成できません」というエラー メッセージが表示されます。
- スラッシュが含まれている場合、ユーザー ID が生成されるときに自動的に削除されます。たとえば、ユーザー ID が **`jdoe/1`** の場合、`jdoe1` になります。

パスワードの考慮事項

- パスワードの作成時は、ASCII 文字のみを使用してください。
- *現在のユーザー*のパスワードを変更する場合、自動的にログアウトされます。そのユーザーとして新しいパスワードでログインします。

3 ユーザーを作成すると、次のことが可能になります。

— 別のユーザーを作成する (このセクションの手順 1 を参照)。

— ユーザー ID をクリックしてユーザーのプロパティを表示および変更する (次のセクションを参照)。

— ユーザーにロールを割り当てる (このセクションの 286 ページの「[ロール] パネル」を参照)。

ユーザーのプロパティを表示および変更するには

このセクションの手順は「内部」ユーザーにのみ該当します。「外部」ユーザーのプロパティは Core コンソールでは変更できません。

1 内部ユーザーのユーザー ID をクリックして、そのプロパティを表示します。

2 [ユーザー プロパティ] ウィンドウで表示名や説明などのユーザーのプロパティを変更して、[パスワードの変更] ウィンドウにアクセスします。

3 **[保存]** をクリックし、変更を確定して保存します。

4 これにより、次のことが可能になります。

— 別のユーザーを作成する (前のセクションの手順 1 を参照)

— 別のユーザー ID をクリックしてそのプロパティを表示および変更する (このセクションの手順 1 を参照)

— ユーザーにロールを割り当てる (このセクションの 286 ページの「[ロール] パネル」を参照)。

コンソール ユーザーを削除するには

このセクションの手順は「内部」ユーザーにのみ該当します。「外部」ユーザーのプロパティは Core コンソールでは変更できません。

- リストからユーザー ID を選択して、**[ユーザーの削除]**  をクリックします。

  *現在のユーザー*は削除できません。
  このユーザー ID を削除するには、ログアウトして、別の管理者としてログインしなおしてから削除を実行する必要があります。

[ロール] パネル

さまざまなレベルの管理者権限 (**ロール**) をユーザーに割り当てることができます。ユーザーに付与するアクセスおよび管理のアクセス許可に基づいて、ロールをユーザーに割り当てます。コンソール ユーザーのロールは次のとおりです。

- **管理者** : このユーザーには Core コンソールへの無制限のアクセス権限があり、すべての管理機能を実行できます。これは、「スーパーセット」ロールで、オペレータ ロールとレポータ ロールのすべての機能と権限が含まれています。
- **オペレータ** : このユーザーは、Core コンソールで管理タスク、操作タスク、およびレポート関連タスクを実行できます。このユーザーは [設定] タブにはアクセスできません。このロールには、レポータ ロールの機能と権限が含まれています。
- **レポータ** : このユーザーのアクセス許可では、Core コンソールでレポートデータの表示、コンパイル、および印刷のみを行うことができます。このユーザーは、[レポート] タブと [ダッシュボード] タブにのみアクセスできます。

  ユーザーには複数のロールを割り当てることができます。

ユーザーへのロールの割り当て

コンソールでは、次の 2 つのいずれかの方法で、ユーザーにロールを割り当てることができます。

- [ロール] パネルで、次の手順を実行します。
  a. テーブルのロールをクリックして [ロール プロパティ] ウィンドウを呼び出します。このウィンドウには、該当のロールに割り当てられているユーザーのリストが表示されます。
  b. ツールバーのボタンを使用して、ユーザーをロールに追加したり、ユーザーをロールから削除したりします。

- [ユーザー] パネルで、次の手順を実行します。
  a テーブルのユーザー ID をクリックして [ユーザー プロパティ] ウィンドウを呼び出します。
  b [ロール] タブをクリックします。
  c ツールバーのボタンを使用して、ユーザーをロールに追加したり、ユーザーをロールから削除したりします。

Satellite コンソールのアクセス制御

HPCA 管理者は、Satellite コンソールの [アクセス制御] セクションで、コンソールのアクセス認証メソッド (**ローカル アカウント**または**ディレクトリ サービス アカウント**) を選択してその設定を行うことができます。

[アクセス制御] セクションの [要約] 領域には、現在有効になっている認証メソッドが表示されます。デフォルト (ローカル アカウント) が表示されます。

認証メソッドを選択および設定するには

1 **[認証の設定]** をクリックします。認証ウィザードが開きます。

2 [サーバー認証タイプの設定] 領域で、[認証メソッド] ドロップダウンを使用して次のいずれかを選択します。

— **ローカル アカウント** - このメソッドでは、管理者は Satellite コンソールの *管理者*および*オペレータ* ログオン認証情報を設定できます。これらの認証情報によって、コンソールのさまざまな部分へのアクセスが制限されます。これがデフォルトとなります。設定情報については、288 ページの「ローカル アカウントを使用するには」セクションを参照してください。

— **ディレクトリ サービス アカウント** - このメソッドでは、環境内のディレクトリ サービス アカウント (Active Directory など) を使用して管理者認証ができます。設定情報については、288 ページの「ディレクトリ サービス アカウントを使用するには」を参照してください。

3 **[次へ]** をクリックして [設定] 領域に進み、選択したアクセス メソッドの設定を指定します。

ローカル アカウントを使用するには

ローカル アカウントを使用して Satellite コンソールへのアクセスの安全性を確保する場合、Satellite Server をインストールしたらすぐにパスワードを変更します。

パスワードの考慮事項

- パスワードの作成時は、ASCII 文字のみを使用してください。
- *現在*のユーザーのパスワードを変更する場合、自動的にログアウトされます。そのユーザーとして新しいパスワードでログインします。

a 適切な領域で管理者またはオペレータのコンソールへのアクセスを設定します。

- **管理者**のアクセス許可では、ユーザーはコンソールのすべての領域にアクセスできます。
- **オペレータ**のアクセス許可では、ユーザーのアクセスはコンソールの [操作] 領域に制限されます。

b **[次へ]** をクリックします。

c 設定が完了したら、**[閉じる]** をクリックします。

次にローカル アカウントを使用して Satellite コンソールにログインするときには、新しいパスワードを使用します。

ディレクトリ サービス アカウントを使用するには

外部ディレクトリ サービス アカウントを使用して、Satellite コンソールへのユーザー アクセスを認証できます。

a [ディレクトリ サービスの設定] 領域で、次の設定パラメータを指定します。

- **ディレクトリ ホスト**：認証に使用する外部ディレクトリ サーバーのホスト名または IP アドレスです。
- **ディレクトリ ポート**：外部ディレクトリ サーバーにアクセスするために使用するポートです。デフォルトは 389 です。
- **ベース DN**: ユーザーのクエリ時に検索を開始するディレクトリのベース オブジェクトです。

  たとえば、**`dc=europe,dc=acme,dc=com`** のようになります。

- **アクセス グループ DN**: 管理者権限で Core コンソールにアクセスできるすべてのメンバーを含むグループ DN です。
- **ディレクトリ ユーザー ID**: ディレクトリ サーバーにアクセスできる有効なユーザー ID です。Core にログオンするユーザーが上記のグループ DN のメンバーであることを検証するために使用されます。デフォルトは administrator です。
- **ディレクトリ パスワード**: 上記のユーザー ID に関連付けられているパスワードです。

b [LDAP グループ ユーザーのテスト] 領域で、テスト ユーザーの認証情報を入力します。

テスト ユーザーは、上記で指定されているアクセス グループ DN のメンバーである必要があります。

このテストで、ディレクトリ サービス アカウントの設定後にこのサーバーにアクセスできることを確認できます。

- **ユーザー名** : 既存のアクセス グループ DN ユーザーのユーザー名です。
- **パスワード** : 上記のユーザー名に関連付けられているパスワードです。

c **[次へ]** をクリックします。

d 設定が完了したら、**[閉じる]** をクリックします。

これで管理者は、ディレクトリ サービス アカウントの認証情報を使用して Satellite コンソールにサインインできます。

設定

[設定] 領域は Satellite コンソールでのみ使用できます。

設定サービスは、それぞれの付与資格に基づいて HPCA Agent に「モデル」とサービス情報を提供します。エージェントはサーバーに接続して、この情報を取得し、変更内容を反映させます。このサービスが Satellite Server で無効になっている場合、HPCA Agent は別のサーバーを使用して、リクエストした情報を取得する必要があります。この「フォールバック サーバー」の指定は、Configuration Server Database の CLIENT.SAP インスタンスに設定されているユーザーのインフラストラクチャ モデルに組み込む必要があります。

- 設定サービスを有効にするには、**[有効]** チェック ボックスをオンにして **[保存]** をクリックします。

データ キャッシュ

[データ キャッシュ] 領域は Satellite コンソールでのみ使用できます。

データ キャッシュ サービスは、基本となる HPCA キャッシュ管理サービスを制御します。HPCA キャッシュ管理サービスは、Satellite が同期されているアップストリーム ホストからデータ (ソフトウェア、パッチ、セキュリティ、および監査など) を取得するために使用されます。このページでは、次のことができます。

- この Satellite のデータ キャッシュ サービスを有効または無効にする。
- リソース データ キャッシュの制限をメガバイト単位で設定する。

Satellite Server のデータをキャッシュおよび同期するには、まず Satellite を設定する必要があります。詳細については、『HPCA Core および Satellite 入門およびコンセプト ガイド』を参照してください。

データ キャッシュを設定するには

1 [設定] タブで、**[データ キャッシュ]** をクリックします。

2 次のオプションを設定します。

— **[有効]** (チェック ボックスがオン) は、データ サービスがこの Satellite で有効になっていることを示します。これはデフォルトで、これによって、この Satellite に接続されている HPCA Agent が Satellite からソフトウェアやパッチを受信できるようになります。

— **[有効]** (チェック ボックスがオフ、つまり**無効**) は、データ サービスがこの Satellite で無効になっていることを示します。

– アップストリーム　ホストと同期しても、ソフトウェアやパッチのデータ キャッシュはこの Satellite に送信されません。

– この Satellite に接続されている HPCA Agent によって、データのリクエストがアップストリーム ホストに渡されます。

— **[データ キャッシュの制限 (MB)]** をリソース キャッシュの最大サイズ (メガバイト) に設定します。デフォルトは 40000 MB です。

3 **[保存]** をクリックして、変更内容を実装します。

[操作] タブがリフレッシュされると、このサービスのステータスが [要約] の下に表示されます。

インフラストラクチャ管理

[インフラストラクチャ管理] セクションでは、HPCA インフラストラクチャのさまざまな設定を行うことができます。詳細については、次のセクションを参照してください。

- 291 ページの「プロキシ設定」
- 292 ページの「SSL」
- 295 ページの「ポリシー」
- 296 ページの「データベース設定」
- 297 ページの「ディレクトリ サービス」
- 307 ページの「ジョブ アクション テンプレート」
- 312 ページの「マルチキャスト」
- 312 ページの「Live Network」
- 316 ページの「Satellite 管理」

プロキシ設定

HPCA Core Server と外部のデータ ソースまたは受信者間の、インターネットベースの通信に使用するプロキシ サーバーの設定を指定するには、[プロキシ設定] 設定ページを使用します。

HTTP 通信と FTP 通信で別々のプロキシ設定を確立できます。HTTP プロキシサーバーは、Patch Manager の取得、HP Live Network のコンテンツの更新、および特定のダッシュボード ペインで使用される Real Simple Syndication (RSS) フィードに使用されます。これらの HTTP プロキシ設定がないと、たとえば Patch Manager の取得が失敗した場合に、ブリティン、パッチ、および Windows Update Agent (WUA) ファイルなどの関連項目をダウンロードできなくなります。

FTP プロキシ サーバーは、HP Softpaq 取得を実行するために Patch Manager によって使用されます。

プロキシを設定するには

1 [設定] タブで、[インフラストラクチャ管理] 領域を展開し、**[プロキシ設定]** をクリックします。

2 設定するプロキシ サーバーのタブ (**[HTTP]** または **[FTP]**) を選択します。

3 **[有効]** ボックスをオンにします。

4 プロキシ サーバーに関する次の情報を入力します。

- **ホスト** : プロキシ サーバーのネットワーク アドレスの名前
- **ポート** : プロキシ サーバーがリスンするポート
- **ユーザー ID**: プロキシ サーバーで認証が必要な場合のユーザー ID
- **パスワード** : プロキシ サーバーで認証が必要な場合のプロキシ ユーザーのパスワード

5 **[保存]** をクリックして、変更内容を実装します。

6 **[閉じる]** をクリックして、ダイアログを確認します。

SSL

SSL を有効にすると、Core コンソールへのアクセスが保護されます。SSL を有効にすると、コンソールに接続している間に作成されるトランザクションが暗号化されます。

SSL を有効にしてサーバーとクライアントの証明書を定義するには、[SSL] セクションを使用します。

- 293 ページの「SSL サーバー」
- 293 ページの「SSL クライアント」

SSL サーバー

SSL サーバーの証明書は、HPCA Server のホスト名に基づいています。これにより、サーバーで SSL 接続が許可されます。これは、Verisign など既知の認証局によって署名される必要があります。

HPCA Server の SSL の有効化および設定を行うには

1 **[SSL を有効化]** の後にあるチェック ボックスをオンにします。

2 **[既存の証明書を使用]** または **[新しい証明書のアップロード]** のいずれかを選択します。

3 **[保存]** をクリックします。

SSL クライアント

認証局のファイルには、信頼された認証局の署名入り証明書が含まれています。これにより、HPCA Server は他の SSL 対応サーバーに接続するときに SSL クライアントとして機能できます。サーバーのインストールには、信頼された認証機関のデフォルトのセットが含まれています。これはほとんどの組織において十分な権限を持ちます。

CA 証明書ファイルを定義するには

1 **[ブラウズ]** をクリックして移動し、CA 証明書ファイルを選択します。

2 この証明書ファイルを既存の証明書に追加するのか、または既存の証明書をこの新しいファイルで置き換えるのかを選択します。

3 **[保存]** をクリックします。

スマート カード認証

Client Automation の Enterprise Edition では、スマート カードを使用した双方向認証がサポートされています。スマート カード認証では、SSL を有効にする必要があります。

スマート カード ログイン プロセス時に、ユーザーは Core Server のトラストストアにある信頼できる証明書に一致する証明書を選択する必要があります。ディレクトリのユーザーに対してこの証明書を検証するプロセスでは、次のチェックが行われます。

- **subjectdn**

  証明書のドメイン名 (subjectdn) の値が取得されます。認証が有効になっているマウント済みディレクトリのいずれかで subjectdn と対応する userdn が一致しているかどうかを判断するためのチェックが実行されます。一致している場合、ユーザーはログインできます。一致していない場合、altsubjectname チェックが実行されます。

- **altsubjectname**

  証明書の代替サブジェクト名 (altsubjectname) の値が取得されます。認証が有効になっているマウント済みのディレクトリのいずれかで altsubjectname と AD userprincipal 名が一致しているかどうかを判断するためのチェックが実行されます。一致している場合、ユーザーはログインできます。一致していない場合、電子メール アドレス チェックが実行されます。

- **電子メール アドレス**

  証明書の subjectdn に電子メール アドレス値があるかどうかが確認されます。電子メール アドレスがある場合、認証が有効になっているマウント済みのディレクトリのいずれかのメール属性と一致しているかどうかを判断するためのチェックが実行されます。一致している場合、ユーザーはログインできます。電子メール アドレスがない場合、usercertificate の照合が実行されます。

- **usercertificate の照合**

  認証が有効になっているマウント済みのディレクトリのいずれかで usercertificate と usercertificate 属性が一致しているかどうかを判断するためのチェックが実行されます。一致している場合、ユーザーはログインできます。一致していない場合、ログインは失敗します。

SSL、ポリシー、ディレクトリ サービスの詳細については、HP セルフ ソルブ サイト **http://h20230.www2.hp.com/selfsolve/manuals** の『SSL 実装ガイド』を参照してください。

スマート カードのアクセスに関するトラブルシューティングの詳細については、519 ページの「スマート カードのアクセスに関する問題のトラブルシューティング」を参照してください。

ポリシー

付与資格情報を含むディレクトリ サービスに HPCA Server から接続するには、ポリシーを有効にする必要があります。無効にすると、リクエストした情報がアップストリーム サーバーから取得されます。

このパネルでポリシーを設定すると、(設定を含む) ディレクトリ サービス インスタンス がディレクトリ サービスの HPCA リストに自動的に作成されます。これは、コンソールの [ディレクトリ サービス] パネルからアクセスできます。

認証などの追加機能のためにディレクトリ サービスのこのインスタンスを変更できますが、ポリシーのためにディレクトリ サービスを作成する必要はありません。

ポリシーの有効化および設定を行うには

1 [ポリシー設定] 領域で、**[有効]** を選択します (これにより、Policy Server サービスが開始します)。

2 次の設定パラメータを指定します。

ディレクトリ ホスト : 認証に使用する外部ディレクトリ サーバーの完全なマシンのホスト名または IP アドレスを指定します。

SSL を使用している場合は、このフィールドに IP アドレスを指定しないでください。SSL では、IP アドレスは検証されません。

ベース DN: 管理者権限で Core コンソールにアクセスできるすべてのメンバーを含むグループ DN を指定します。

ディレクトリ ポート : 外部ディレクトリ サーバーにアクセスするために使用するポートを指定します。デフォルトは 389 です。

ディレクトリ ユーザー名 : ディレクトリ サーバーにアクセスできる有効なユーザー名を指定します。これは、Core にログオンするユーザーが上記のグループ DN のメンバーであることを検証するために使用されます。デフォルトは Administrator です。

ディレクトリ パスワード : 上記のユーザー名に関連付けられているパスワードを指定します。

3 **[保存]** をクリックします。

Core Server によって、外部ディレクトリ サービスへの接続が自動的にテストされます。

LDAP 接続のテストが成功すると、Core Server によってこのディレクトリ サービスに接続するための Portal のマウント ポイントが作成され、ポリシーに使用できるようになります。

4 外部ディレクトリへの接続が成功したら、[ポリシー] ページの下部で **[LDIF の生成]** をクリックします。

LDIF の生成

この領域では、HPCA ポリシー設定を使用したディレクトリ スキーマの更新に使用できる LDIF (LDAP Data Interchange Format) ファイルを生成できます。

このオプションをクリックすると、[ポリシー] ページで指定したポリシー設定を使用してカスタマイズした LDIF ファイルを保存できます。

上記のポリシー設定を保存してから LDIF ファイルを生成してください。

1 **[LDIF の生成]** をクリックします。

これにより、HPCA が外部 LDAP ディレクトリを使用するために必要な、カスタマイズしたスキーマの変更を含むファイルが作成されます。

2 表示メッセージに応じて、生成された LDIF ファイルを、選択した場所に保存します。

3 35 ページの「外部ポリシー ストアの実装」セクションの手順に従い、LDIF ファイルを使用してスキーマの変更を外部 LDAP ディレクトリに適用します。

データベース設定

Core Server オブジェクトの SQL および Oracle データベースへの ODBC 接続を設定するには、[データベース設定] を使用します。

前提条件

Core データベースを作成し、そのデータベースの ODBC 接続を定義する必要があります。詳細については、製品マニュアルのインストール手順を参照してください。

メッセージングを設定するには

1 [設定] タブで、**[インフラストラクチャ管理]**、**[データベース設定]** の順にクリックします。

2 次のオプションを設定します。

- **ODBC DSN**: Core データベースの DSN を選択します。
- **ODBC のユーザー ID**: DSN のユーザー ID を指定します。
- **ODBC のパスワード**: ODBC ユーザー ID に関連付けられているパスワードを指定します。
- **サーバーのホスト**: データベースをホストするサーバーの名前を指定します。
- **サーバーのポート**: サーバーのポート (デフォルトは 1433) を指定します。

3 **[保存]** をクリックします。

ディレクトリ サービス

ディレクトリ サービスは、次のように多くの操作に使用されます。

- Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) のコンテナおよびグループに基づくレポートの実行
- HPCA Console の認証を可能にする外部 AD/LDAP ソースの有効化
- ポリシーの割り当て (ポリシーは、ユーザー、エージェント コンピュータ、または管理対象デバイスがアクセスできるサービスの指定です)
- OS 管理作業
- AD/LDAP ソースに基づくエージェントの通知

HP Client Automation では、次の 2 つの基本的なポリシーの使用パターンがサポートされています。

- **通常**のパターンでは、提供される外部 LDAP ディレクトリ (Active Directory など) に保存される (ソフトウェアやパッチなどの) ポリシーを管理できます。このポリシー ソースは、Configuration Server の解決を支援するために Policy Server によって使用されます。ディレクトリのポリシーは HPCA Console 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 Guide)』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 Installation and Configuration Guide (Portal Guide)』を参照してください。

- サポートされている他のポリシーの使用パターンは、**オペレーティング システム (OS) 管理**に関連しています。OS 管理のポリシーは、HPCA Management Portal (Portal) に内部的に保存されます。このケースでは、OS の解決をサポートするために、Configuration Server への操作インターフェイスが Portal によって提供されます。ポリシーの管理は、HPCA Console の OS 管理機能を使用して行われます。詳細については、『HP Client Automation OS Manager System Administrator ガイド (OS Manager ガイド)』を参照してください。

  外部 LDAP ディレクトリでは、現在 OS 管理ポリシーがサポートされています。

関連トピック：

298 ページの「[ディレクトリ サービス] ページへの移動」

301 ページの「Configuration Server ディレクトリ サービスへの接続の設定」

303 ページの「外部ディレクトリ サービスへの接続の設定」

[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 31　　[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。

   — 301 ページの「Configuration Server ディレクトリ サービスへの接続の設定」

   — 303 ページの「外部ディレクトリ サービスへの接続の設定」

6 **[保存]** をクリックします。

7 **[閉じる]** をクリックして、[実行ステータス] ダイアログを確認します。右上隅にある **X** をクリックして [プロパティ設定] ウィンドウを閉じます。

ディレクトリ サービスのオプションが変更されました。変更した設定によっては、HPCA Console をログアウトしてからログインしなおす必要がある場合もあります。

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

外部ディレクトリ サービスへの接続を設定するには、まず内部の Configuration Server ディレクトリ サービスへの接続を作成する必要があります。これは、HPCA-CS 接続と呼ばれます。

HPCA-CS 接続はポリシーの解決に使用できません。

Configuration Server ディレクトリ サービス接続 (HPCA-CS) は、HPCA Console を使用してポリシーを管理するための前提条件です。LDAP または LDAPS (セキュア) 接続を設定する前に、まずこの接続の設定を行ってください。

Configuration Server ディレクトリ サービスを設定するには :

1 [設定] タブで、左側のペインにある **[ディレクトリ サービス]** をクリックします。

2 ディレクトリ サービスの詳細セクションで、[新しいディレクトリ サービスを作成します] ボタン をクリックします。ディレクトリ サービスの作成ウィザードが開始します。

3 [表示名] と [説明] を指定します。**[タイプ]** 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、HPCA Console が Configuration Server への接続を何回試行すると接続失敗となるかを指定します。

   — **[接続遅延]** を使用して、接続試行と接続試行の間の遅延時間を秒単位で指定します。

6 **[次へ]** をクリックします。

7 [要約] 画面を確認します。すべてのプロパティが正しければ、**[適用]** をクリックします。

8 **[閉じる]** をクリックして、ダイアログを確認します。

ディレクトリ ソースが [ディレクトリ サービス] リストに追加されます。

外部ディレクトリ サービスへの接続の設定

外部ディレクトリ サービスへの接続を設定する前に、301 ページの「Configuration Server ディレクトリ サービスへの接続の設定」の手順に従ってください。

HPCA Console では、サービスをディレクトリ サービス オブジェクトに割り当てて LDAP ポリシーを管理できます。

ただし、これを行うには、まず外部ディレクトリ サービスへの接続を設定する必要があります。次のタイプの外部ディレクトリ サービスがサポートされています。

- Lightweight Directory Authentication Protocol(LDAP)
- SSL (Secure Sockets Layer) をサポートする LDAP (LDAPS (セキュア))

LDAP サーバーで SSL を使用している場合、LDAPS (セキュア) タイプの接続を使用する必要があります。

各外部 LDAP ディレクトリ サービスは、次の任意の組み合わせに対して使用できます。

- 認証
- レポート
- ポリシー資格

たとえば、2 つのディレクトリがあるとします。一方のディレクトリにはすべてのユーザー アカウントが含まれており、もう一方のディレクトリはポリシー専用です。ユーザー アカウント ディレクトリに対して認証を行います。このケースでは、2 つのディレクトリ サービスを、接続を別々に定義して次のように作成する必要があります。

- 接続を次のように設定した認証用のディレクトリ サービスを 1 つ作成します。
  - **[認証で使用]** がオン

— **[ポリシーに使用]** がオフ

— **[サービス アカウントの使用]** がオフ

[認証で使用] をオンにすると、ユーザーはこのディレクトリ サービスの外部 LDAP ディレクトリ アカウントを使用して HPCA Console にログインできるようになります。

- ポリシー用のもう 1 つのディレクトリ サービスを次のように作成します。

  — **[認証で使用]** がオフ

  — **[ポリシーに使用]** がオン

  — **[サービス アカウントの使用]** がオン

このように設定することにより、1 つ目のディレクトリ サービスを使用してサインインして、2 つ目のディレクトリ サービスでポリシーを設定できます。

注 : 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 HPCA Console ユーザー名とパスワードを使用してサインインできます。

LDAP または LDAPS (セキュア) ディレクトリ サービスを設定するには

1 [設定] タブで、**[ディレクトリ サービス]** をクリックします。

2 ディレクトリ サービスの詳細セクションで、  ([新しいディレクトリ サービス]) ボタンをクリックします。ディレクトリ サービス作成ウィザードが開始します。

3 **[表示名]** と **[説明]** を指定します。

4 **[タイプ]** 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。LDAP (セキュア) の場合、デフォルト値は 636 です。

— ディレクトリ サービス サーバーにサインインするために HPCA Console によって使用されるアカウントを設定するには、**[サービス アカウント ID]** を使用します。このサービス アカウントは、読み取り処理と書き込み処理の両方で使用されます。このディレクトリ ソースへの完全な読み取り / 書き込みアクセス権が必要です。

— **[パスワード]** を使用して、サービス アカウント ID のパスワードを指定します。[パスワードの確認] にパスワードを再入力します。

— **[ベース DN]** は、HPCA Console からディレクトリを参照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 HPCA Console の [レポート] タブでフィルタ ソースとして有効になります。この機能を有効にするには、Portal をディレクトリ ソースとして使用するように Reporting Server を設定する必要があります。

— **ポリシーに使用**：このオプションを有効にすると、このディレクトリ サービスは HPCA Console でポリシーの管理に使用できます。

— **認証で使用**：このオプションを有効にすると、このディレクトリ サービスは HPCA Console のログイン画面でサインイン オプションとして有効になり、既存のディレクトリ ユーザーに基づいたユーザー認証が可能になります。次の 2 つのパラメータを使用できます。

– **認証グループ DN**: これは、HPCA Console に対して認証されるユーザーのソースとして使用されます。このグループのメンバーであるすべてのユーザーは、HPCA Console へのサインインが可能になります。

– **サービス アカウントの使用**：このオプションを有効にすると、このディレクトリ サービスへのすべての読み取り要求および書き込み要求に対して、**[接続設定]** で指定した **[サービス アカウント ID]** が使用されるようになります。無効にすると、このディレクトリ サービスへのすべての読み取り要求および書き込み要求では、サインオンしているユーザーの認証情報が使用されます。

— **リーフ ノード フィルタ**：LDAP 形式のフィルタ値を入力して、多数のデータ タイプを持つノードをフィルタリングして、それらがツリー ナビゲーション ビューに表示されないようにします。使いやすさを向上させるために、コンピュータやユーザーなどのオブジェクトにフィルタを実行する必要があります。各ノードをフィルタリングする最適な方法を決定するには、ディレクトリ固有のスキーマを参考にしてください。次の例では、コンピュータとユーザーをフィルタリングしています。

```
(!(|(objectclass=user)(objectclass=computer)))
```

9 **[次へ]** をクリックします。

10 要約情報を確認します。すべてのプロパティが正しければ、**[適用]** をクリックします。

11 **[閉じる]** をクリックして、ダイアログを確認します。

ジョブ アクション テンプレート

ジョブ アクション テンプレートを使用して、新しいジョブの作成時に使用するパラメータを事前に定義できます。

ジョブ アクション テンプレートは、[設定] タブの [インフラストラクチャ管理] 領域で管理します。使用可能なジョブ アクション テンプレートの一覧を表示するには、左側のナビゲーション メニューにある **[ジョブ アクション テンプレート]** リンクをクリックします。

[ジョブ アクション テンプレート] ウィンドウの [有効] カラムでは、HPCA ジョブ作成ウィザードを使用して新しいジョブを作成するときにテンプレートが使用可能かどうかが示されます。パラメータを編集するテンプレートの名前をクリックするか、**[新しいジョブ アクション テンプレート]** ボタンをクリックして新しいテンプレートを作成します。詳細な手順については、308 ページの「新しいテンプレートの作成」を参照してください。

HPCA Core のインストール時に、次のジョブ アクション テンプレートが提供されます。

- 監査接続
- HPCA 要約 (夜間)
- パッチ接続
- DTM スケジュールのリフレッシュ
- Satellite の同期 (すべて)
- Satellite の同期 (設定)
- Satellite の同期 (データ)
- セキュリティ接続
- ソフトウェア接続
- 利用状況接続
- VMware ThinApp Sync

これらの各テンプレートを使用して、CSDB の関連するドメインに接続するようにターゲット デバイスのエージェントに指示を与えます。たとえば、セキュリティ接続テンプレートの場合、エージェントは SECURITY ドメインに接続します。これにより、デバイスがアクセスできる SECURITY ドメインのすべてのサービスが強制的に実行されます。

Satellite の同期または DTM スケジュールのリフレッシュのジョブをクライアント デバイスで正常に実行するには、そのクライアントの HPCA Agent によって HPCA Core への接続操作が事前に実行されている必要があります。

新しいテンプレートの作成

新しいジョブ アクション テンプレートを作成するには、次の手順を使用します。既存のテンプレートを変更するには、[ジョブ アクション テンプレート] リストでその名前をクリックします。

新しいジョブ アクション テンプレートを作成するには

1 **[設定]** タブから、**[インフラストラクチャ管理]** をクリックして展開します。

2 **[ジョブ アクション テンプレート] をクリックします。**

3 **[新しいジョブ アクション テンプレート]** ボタン をクリックします。ジョブ アクション テンプレート作成ウィザードが開きます。

4 新しいテンプレートの作成を開始します。次のテンプレートから選択できます。

   — 空白テンプレート - 使用可能なすべてのパラメータを定義できます。

   — サンプル テンプレート - 事前に定義されたパラメータが含まれています。これは、テンプレートを作成したときに選択した接続タイプやオプションによって異なります。310 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。このリストには付与された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。この実行可能ジョブは、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。注 : **[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 つの対象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、174 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。

監査接続

このテンプレートは、HPCA Server に接続し、HPCA 管理レポートの作成に使用するデータを収集するように管理対象クライアントに指示を与えます。

HPCA 要約 (夜間)

このテンプレートは、指定のデバイス グループのデータを定期的に「ロールアップ」するために使用します。234 ページの「データ ロールアップ用のデバイス グループの作成」を参照してください。

パッチ接続

パッチ接続は、デバイスに付与されたパッチを更新するために使用します。

DTM スケジュールのリフレッシュ

DTM ジョブのスケジュールは、通知ジョブまたは DTM ジョブを作成したり、DTM スケジュールのリフレッシュ ジョブ アクションのテンプレートを使用してリフレッシュできます。183 ページの「ターゲットの DTM スケジュールのリフレッシュ」を参照してください。

Satellite の同期 (すべて、設定、およびデータ)

Satellite の同期テンプレートは、Satellite で最新のデータを使用できるように Satellite Server と Core Server を同期させるために使用します。187 ページの「Satellite 同期ジョブの作成」を参照してください。

セキュリティ接続

セキュリティ接続によって、SECURITY ドメインのすべてのセキュリティ関連の付与資格が解決されます。

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に付与されたソフトウェアのリストを更新するために使用します。

利用状況接続

利用状況接続は、利用状況 Agent をデバイスにインストールして、利用状況データの収集を開始するために使用します。

VMware ThinApp Sync

このテンプレートは、Core Server または Satellite Server が付与された ThinApp サービスの更新があるかどうかをチェックするように管理対象デバイスに指示を与えます。

マルチキャスト

マルチキャストは、最も効率的な方法を使用して配信先グループに情報を同時に配信し、オペレーティング システム イメージおよびアプリケーションの配信に使用されます。

- マルチキャストを有効にするには、このチェック ボックスをオンにして **[保存]** をクリックします。

Live Network

HP Live Network コンテンツ サーバーとの通信に必要な Live Network 設定は、[設定] タブの [インフラストラクチャ管理] 領域で設定します。312 ページの「HP Live Network サーバーへの接続の設定」を参照してください。

Live Network の更新は、[操作] タブの [インフラストラクチャ管理] 領域で設定します。240 ページの「Live Network」を参照してください。

HP Live Network サーバーへの接続の設定

HP Live Network から最新のコンテンツを自動的にダウンロードし、HP Live Network アナウンスメントおよび HP Live Network Patch Manager アナウンスメントのダッシュボード ペインの RSS フィードを確立するために使用する接続を設定するには、Live Network 設定を使用します。これには、次の項目が含まれています。

- 最新のスキャナおよびデータをダウンロードするために使用する HP Live Network コンテンツ サーバーの URL

- HP Passport ログイン認証情報です。

HP Live Network コンテンツ サ。ーバーでは、HP Passport 認証を使用してセキュリティと利便性が確保されます。HP Passport は、1 つのユーザー ID とパスワードを使用して HP Passport に対応するすべての Web サイトに登録できるシングル サインイン サービスです。HP Passport プロファイルをセットアップするには、次のサイトに移動します。

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

HP Passport プロファイルに、HPCA サポート契約に関連付けられている 12 桁の Service Agreement Identifier (SAID) が含まれていることを確認してください。HP Live Network コンテンツ サーバーにアクセスできるように、この SAID には HP BSA Essentials に対する付与資格が含まれている必要があります。サポートについては、HP Software の営業担当者にお問い合わせください。

このページで入力したパスワードは暗号化されます。

保存する前に設定情報をテストできます。テストをリクエストすると、HPCA Console は HP Live Network コンテンツ サーバーへの接続を試行します。接続に成功すれば、設定情報は有効です。詳細については、25 ページの「Live Network の設定のテスト」を参照してください。

HP Live Network の接続設定を指定するには

1 [設定] タブで、[インフラストラクチャ管理] 領域を展開し、**[Live Network]** をクリックします。

2 次の情報を指定します。アスタリスク (*) の付いているパラメータはすべて必須です。

- **HP Live Network ユーザー ID** - HP Passport のユーザー ID です。
- **HP Live Network パスワード** - HP Passport 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 サーバーの場所です (URL はデフォルトで設定されています)。
- **HP Live Network コネクタ** - HPCA Core をホストするシステムの Live Network コネクタ実行可能ファイルへのパスです (パスはデフォルトで設定されています)。

詳細については、527 ページの「HP Live Network コネクタの手動での実行」および 145 ページの「HP Live Network コネクタのダウンロード」を参照してください。

3 指定した設定をテストするには、**[テスト]** をクリックします。詳細については、25 ページの「Live Network の設定のテスト」を参照してください。

4 **[保存]** をクリックして、変更内容を実装します。

- テストが成功しても、その設定は HPCA Console では自動的に保存されません。設定を保存するには、**[保存]** ボタンをクリックする必要があります。
- このページから離れると、**[保存]** をクリックする前にテキスト ボックスに入力した情報はすべて失われます。情報を保存する場合は、必ず **[保存]** をクリックしてください。
- **[リセット]** ボタンを使用して、最後に保存した設定に戻すことができます。

Live Network の設定のテスト

Live Network を設定する場合、保存する前に、設定が機能するかどうかをテストできます。

テストを実行するには、ページの右下隅にある **[テスト]** ボタンをクリックします。HPCA Console では、まず必要なすべての設定が指定されていることと、すべての設定の形式が正しいことが確認されます。その後で、次のアクションを実行します。

HPCA Console から HP Live Network コンテンツ サーバーへの接続を試行して、指定されているユーザー名とパスワードを使用してログインします。[インフラストラクチャ管理] 設定領域の [プロキシ設定] ページに表示されるプロキシ情報が使用されます。

ネットワーク トラフィックやその他のパラメータによって異なりますが、このテストは最大で 3 分かかります。テストを続行するかどうかを確認するダイアログ ボックスが表示されます。続行する場合、**[はい]** をクリックします。

テストが完了すると、[テスト結果] ダイアログ ボックスにテストの結果が表示されます。次の表に、表示される結果と各結果の意味を示します。

表 32　　Live Network の設定のテスト結果

アイコン	結果	説明と推奨アクション
	テストは成功しました。	すべての設定が有効です。設定を保存してください。
	テストに失敗しました。	テストが失敗する一般的な理由を次にいくつか挙げます。 • 必要な設定が見つからない。 • 無効な形式で設定が指定されている (無効な URL またはパス名など)。 • 設定のスペルに誤りがある。 • HP Live Network コンテンツ サーバーのログイン認証情報が無効 (登録の期限切れなど)。
	不明	この結果は、必ずしも設定情報が無効であることを意味しているわけではありません。これは、テストを完了できなかったということだけを表しています。 たとえば、HPCA Console が HP Live Network コンテンツ サーバーに 3 分以内に接続できず、テストがタイムアウトした場合などが該当します。これは、次のような理由で発生します。 • サーバーが使用できない。 • ネットワーク トラフィックによって接続が妨げられる。 • ファイアウォールによって接続がブロックされる。 また、接続がプロキシ サーバー経由の場合に指定したプロキシ情報が正しくなかったり、プロキシ サーバーによって接続がブロックされていたりすると、この結果となることがあります。

失敗または不明瞭なテスト結果のトラブルシューティングを行うには、タブですべての設定のスペルおよび形式を確認します。エラーがないかどうか `vms-server.log` ファイルも確認します。

テストが成功していても、設定を保存するには **[保存]** ボタンをクリックする必要があります。設定は HPCA Console によって自動的に保存されません。

Satellite 管理

[設定] タブにある [インフラストラクチャ管理] の [Satellite 管理] 領域では、HPCA Console から Satellite Server を配布および管理できます。Satellite Server を使用すると、管理対象デバイスにデータ キャッシングなどのリモート サービスを提供することにより、バンド幅を最適化し、ネットワーク パフォーマンスを向上させることができます。

HPCA Enterprise Edition の場合、次の 3 つの配布モードから選択できます。

- **簡素** (標準) モード。Satellite からデータ キャッシング サービスのみが Client Automation Agent に提供されます。
- **フル** サービス モード。Satellite から設定サービス、データ キャッシング サービスおよび OS 設定サービスが Client Automation Agent に提供されます。
- **カスタム** モード。Satellite で有効にする特定のサービスを選択できます。

配布モードの詳細については、『HPCA Core および Satellite 入門およびコンセプト ガイド』の「Satellite 配布モデル」を参照してください。

Satellite Server を定義および設定するために必要な手順は次の 3 つです。

1 デバイスを HPCA Satellite Server グループに追加します。

319 ページの「Satellite Server の追加」を参照してください。

デバイスを HPCA Satellite Server グループに追加するには、まずそのデバイスを HPCA デバイス リポジトリにインポートする必要があります。詳細については、170 ページの「デバイスのインポート」を参照してください。

2 Satellite Server コンポーネントをこれらのデバイスに配布します。これにより、データ キャッシングなどのリモート サービスがこれらのデバイスで有効になります。

320 ページの「Satellite Server コンポーネントの配布」を参照してください。

3 サブネット ロケーションを作成し、Satellite Server に割り当てます。

326 ページの「サブネット ロケーション」を参照してください。

管理対象デバイスは、サブネットの割り当てに基づいて Satellite Server に接続されます。たとえば、デバイスがサブネット 208.77.1.0 にあり、そのサブネットが Satellite Server A に割り当てられている場合、このデバイスは HPCA Core Server に接続する前に Server A からリソースを取得します。

[Satellite 管理] 領域には、次の 2 つのタブがあります。

- 317 ページの「Satellite Server」
- 326 ページの「サブネット ロケーション」

Satellite Server は、オペレーティング システム イメージを除く、リクエストされたデータをすべて自動的にキャッシュします。同期機能を使用して、HPCA Core Server のすべてのデータを事前に入力することもできます。詳細については、324 ページの「Satellite Server の同期」を参照してください。

Satellite Server は、HPCA Core Server からのみ定義および設定できます。別の Satellite Server から行うことはできません。

ポリシー解決は、HPCA Core Server でのみサポートされています。Satellite Server ではサポートされていません。Satellite Server でポリシー解決を有効にしないでください。

Satellite Server

HPCA Satellite Server グループにデバイスを追加してから、それらのデバイスに Satellite Server コンポーネントを配布して、Satellite Server を定義できます。サーバーの追加が終了したら、各サーバーにサブネット ロケーションを割り当てる必要があります。詳細については、326 ページの「サブネット ロケーション」を参照してください。

[Satellite Server] ツールバーには、使用環境の Satellite Server の定義および設定に使用できるボタンがあります。

表 33　[Satellite Server] ツールバー ボタン

ボタン	説明
	**データのリフレッシュ** - サーバーのリストをリフレッシュします。
	**CSV にエクスポート** - 開いたり保存したりできる、カンマ区切りのサーバーのリストを作成します。
	**Satellite Server の追加** - HPCA Satellite Server グループにデバイスを追加します。
	**Satellite Server の削除** - HPCA Satellite Server グループからデバイスを削除します。
	**Satellite Server の配布** - Satellite 配布ウィザードを起動し、選択したデバイスに Satellite Server をインストールします。
	**Satellite Server の削除** - Satellite 削除ウィザードを起動し、選択したデバイスから Satellite Server をアンインストールします。
	**選択された Satellite Server のサービス キャッシュの同期 -** 選択した Satellite Server のサービス キャッシュを HPCA Core Server と同期させます。
	**デバイスの削除** - HPCA データベースからデバイスを削除します。

Satellite Server は、HPCA Satellite Server デバイス グループに追加されたデバイスで、Satellite Server コンポーネントがインストールされています。

次のセクションでは、Satellite Server の定義と設定の方法を説明しています。

Satellite Server の考慮事項

Satellite Server として追加するデバイスを選択する場合、次の事項を考慮してください。

- デバイスには、パブリッシュされたサービスを保管するのに十分な領域が必要です。

- デバイスには、高性能の高速ネットワーク カード (データ転送速度 100 MB または 1 GB) が必要です。
- デバイスは、そのネットワークへのダウンロード トラフィックをローカライズするサブネット上に存在する必要があります。

ツールバーを使用して、Satellite Server グループでのデバイスの追加および削除を行います。

使用する Satellite Server のいずれかでファイアウォールが有効になっている場合は、次のポートを除外する必要があります。

- TCP 139、445、3463、3464、3465、および 3466

注 : デフォルトの HPCA ポートは 3466 です。HPCA のインストール時にこのポートをカスタマイズしている場合、使用しているポートが開いていることも確認します。

- UDP 137 および 138

Windows ファイアウォールのユーザーは、ファイルとプリンタの共有を選択し、TCP ポート 139 と 445、および UDP ポート 137 と 138 を除外できます。

Satellite Server の追加

Satellite Server コンポーネントを配布するには、まずデバイスを HPCA Satellite Server デバイス グループに追加する必要があります。

Satellite Server を追加するには

1 [Satellite Server] ツールバーで、**[デバイスの追加]** ツールバー ボタンをクリックします。

[HPCA Satellite Server グループ メンバーシップ] ウィンドウが開き、HPCA にインポートされた全デバイスのリストが表示されます。

2 リストから 1 つ以上のデバイスを選択して、**[デバイスの追加]** をクリックします。

3 **[閉じる]** をクリックして、ダイアログ ボックスを閉じます。

4 **[閉じる]** をクリックして、[グループ メンバーシップ] ウィンドウを閉じます。

追加したデバイスが Satellite Server リストに表示されます。

Satellite Server の削除

デバイスを Satellite Server として管理しない場合、そのサーバーを HPCA Satellite Server デバイス グループから削除できます。

Satellite Server コンポーネントがインストールされているデバイスを HPCA Satellite Server デバイス グループから削除する場合、Satellite Server コンポーネントを明示的に削除するまで、このデバイスは Satellite Server として機能し続けます。また、このデバイスは HPCA Satellite Server デバイス グループのメンバーのままです。デバイスから Satellite Server コンポーネントを削除するまで、デバイス グループからデバイスを削除できません。322 ページの「Satellite Server コンポーネントの削除」を参照してください。

HPCA Satellite Server デバイス グループからサーバーを削除するには

1 [Satellite Server] ツールバーで、HPCA Satellite Server デバイス グループから削除するデバイスを選択します。

2 **[デバイスの削除]** ツールバー ボタンをクリックします。

3 **[閉じる]** をクリックして、ダイアログ ボックスを閉じます。

選択したデバイスがグループから削除されます。

Satellite Server コンポーネントの配布

HPCA Satellite Server グループにデバイスを追加したら、そのデバイスに Satellite Server コンポーネントを配布できます。これを行うには、データ キャッシングなどのリモート サービスをそのサーバーで有効にする必要があります。

HPCA Console から Satellite Server コンポーネントをデバイスに配布する場合、次の処理が実行されます。

- HPCA Core Server によって、入力した認証情報を使用してデバイスへの接続が確立されます。

  これらの認証情報で、リモート システムの IPC$ 共有への管理者アクセスを提供する必要があります。このアクセス レベルが使用環境で使用できない場合、HPCA Console で配布する代わりに、Satellite Server コンポーネントを手動でインストールします。

- HPCA Management Agent がデバイスにまだインストールされていない場合はインストールされます。
- Management Agent によって Satellite Server コンポーネントが Core Server からダウンロードされ、デバイスにインストールされます。
- Management Agent によって、初回セットアップ ウィザードがデバイスで自動的に実行され、[ホスト デバイス] フィールドに Core Server の名前が設定されます。
- Satellite Server が Core Server に登録されます。

また、HPCA インストール メディアを使用して Satellite Server コンポーネントを手動でインストールすることもできます。手動でインストールした Satellite Server と HPCA Console から配布した Satellite Server の両方を HPCA Core Server に登録します。

関連する CLIENT.SAP と POLICY.USER インスタンスは、この Satellite 登録プロセスで自動的に管理されます。SAP/USER の変更が必要なときなどに Satellite データを変更する場合、この変更は HPCA によって自動的に行われます。

HPCA 管理者は、`rmp.cfg` のオプション ENABLE_SAP_MANAGEMENT を 0 に設定して、この自動管理プロセスを無効にできます。デフォルトでは、このオプションはオンになっていて、`rmp.cfg` にはありません。注意 : このオプションを無効にすると、Satellite 管理の UI を操作できない状態になり、使用できなくなります。

これは、高度な配布のみが対象になります。経験豊富な HPCA 管理者でない限り、`rmp.cfg` の設定は変更しないでください。

Satellite Server コンポーネントを配布するには

1. 左のカラムのチェック ボックスを使用して、Satellite Server リストから 1 つ以上のデバイスを選択します。
2. **[Satellite Server の配布]**  ツールバー ボタンをクリックして、Satellite Server 配布ウィザードを起動します。
3. ウィザードの手順に従って、選択したデバイスに Satellite Server コンポーネントを配布します。Satellite Server が次の場所にインストールされます。

システム ドライブ:\Program Files\Hewlett-Packard\HPCA

Satellite Server を各デバイスに手動でインストールできます。ネットワーク トラフィックを削減する場合などにこの方法を選択します。

インストール手順については、『HPCA Core および Satellite 入門およびコンセプト ガイド』を参照してください。

Satellite Server を手動でインストールすると、その Satellite Server が Satellite Server リストに表示されます。ただし、サブネット ロケーションを割り当てるまで Satellite Server はクライアント デバイスとして機能しません。

サービスは、同期機能を使用して Satellite Server に事前に読み込めます。いずれかの Satellite Server ジョブ アクション テンプレートを使用して、DTM ジョブをスケジュールすることもできます。詳細については、324 ページの「Satellite Server の同期」を参照してください。

Satellite Server の作成が終了したら、サブネット ロケーションを定義し、その後、Satellite Server をこれらのロケーションに割り当てる必要があります。詳細については、326 ページの「サブネット ロケーション」を参照してください。

Satellite Server コンポーネントの削除

デバイスを HPCA Satellite Server として機能させない場合、Satellite Server コンポーネントをそのデバイスから削除する必要があります。

Satellite Server コンポーネントを削除するには

1 左のカラムのチェック ボックスを使用して、Satellite Server リストからデバイスを選択します。

2 **[Satellite Server の削除]**  ツールバー ボタンをクリックして、Satellite Server 削除ウィザードを起動します。

3 ウィザードの手順に従って、選択したデバイスから Satellite Server コンポーネントを削除します。

[管理] タブの [ジョブ] 領域で、Satellite Server の削除ジョブの進捗状況を確認できます。このジョブが完了したら、このデバイスに Satellite Server コンポーネントがインストールされていないことが Satellite Server リストに示されます。

[サーバーの詳細] ウィンドウ

[サーバーの詳細] ウィンドウにアクセスするには、Satellite Server リストから任意のサーバー名のリンクをクリックします。

[サーバーの詳細] ウィンドウからは、Satellite Server の詳細情報を表示したり、さまざまなサーバー管理タスクを実行したりできます。

全般
[全般] タブでは、サーバーに関する情報を表示したり、Satellite Server の配布や設定、またはサービス キャッシュの同期化などのタスクを実行したりできます。

[要約] 領域には、サーバーに割り当てられているサブネット ロケーションの数、および更新のためにそのサーバーに接続しているデバイスの数が表示されます。ステータスには、Satellite Server コンポーネントのインストールの有無、およびサーバーのサービス キャッシュと HPCA Server とが前回いつ同期されたかが表示されます。

プロパティ
[プロパティ] タブを使用して、デバイスの使用可能なすべての情報を表示します。その他の詳細情報を表示するには、[詳細プロパティ] セクションを展開します。

キャッシュ
[キャッシュ] タブでは、Satellite Server のサービス キャッシュに格納されるサービスの種類を選択できます。詳細については、324 ページの「Satellite Server の同期」を参照してください。

サブネット ロケーション
[サブネット ロケーション] タブでは、サーバーに割り当てるサブネットを定義します。サブネットの追加および割り当ての詳細については、326 ページの「サブネット ロケーション」を参照してください。

デバイス
[デバイス] タブには、サーバーに現在割り当てられているすべてのデバイスが表示されます。このリストは、各デバイスの前回接続に基づいており、デバイスのサブネットが変更されたら、変化する場合があります。

レポート
[レポート] タブを使用して、サービスの事前読み込み要約を表示します。事前に読み込まれたサービスのみが表示されます。(デバイスの要求後に) 自動的にキャッシュされたサービスは表示されません。各事前読み込みステータスの詳細については、324 ページの「Satellite Server の同期」を参照してください。

オペレーション
このタブでは、該当の Satellite Server の HPCA Satellite コンソールの [操作] タブが開きます。このタブには、設定可能な Satellite サービスのステータスと状態が表示されます (281 ページの「Satellite の設定オプション」を参照)。また、アップストリーム ホストなど、サーバーの基本プロパティも表示されます。このタブから、Satellite を同期したり、そのキャッシュをフラッシュしたりできます。このタブにアクセスするには、該当の Satellite Server の有効な HPCA Console ログイン認証情報を入力する必要があります。

設定
このタブでは、281 ページの Satellite の設定オプションを設定できます。このタブにアクセスするには、該当の Satellite Server の有効な HPCA Console ログイン認証情報を入力する必要があります。

Satellite Server の同期

Satellite Server のローカル キャッシュで使用できないリソースをデバイスがリクエストするたびに、データが HPCA Core Server から取得され、Satellite Server の動的キャッシュに格納されて、クライアント デバイスに提供されます。

Satellite Server のサービス キャッシュには、管理対象デバイスによって要求されるデータを事前に入力できます。通常、Satellite Server は、クライアント デバイスから要求されると、オペレーティング システム イメージを除くデータを自動的にキャッシュします。同期機能を使用することで、HPCA Core Server 上の使用可能なすべてのデータを Satellite Server のキャッシュに事前に読み込めます。

(Satellite Server が配布された後に) [サーバーの詳細] ウィンドウの [キャッシュ] タブを使用して、どのデータを事前に読み込むかを選択できます。

事前読み込みには、大規模なバイナリ ファイルのダウンロードが含まれるため、ネットワークの全体的なパフォーマンスに影響を及ぼす可能性があります。可能な限り、最適なネットワーク パフォーマンスが優先事項とならない空き時間に同期を実行するようにしてください。

各サーバーの現在の同期ステータスを表示するには、Satellite Server のリストにある **[前回の同期]** カラムを確認するか、[サーバーの詳細] ウィンドウの [一般] タブの [要約] セクションを参照してください。**[前回の同期]** では、同期機能がサーバー上で最後にいつ*開始*されたかが記録されます。

Satellite Server の最初の同期が行われると、HPCA Agent ID である RPS_<DEVICENAME> を使用して、管理対象デバイス レポートに新しいエントリが追加されます。このエントリは、特に Satellite Server のサービスの事前読み込みのステータスを表示するために存在し、関連デバイスの詳細なハードウェア情報は含まれていません。

Satellite Server から事前読み込みまたは削除されたサービスに関する情報は、その Satellite Server の [サーバーの詳細] ウィンドウにある [レポート] タブの [事前に読み込まれたサービス] にあります。

どのデータを事前に読み込むかを選択するには

1. Satellite Server の配布後に、Satellite Server のリストの中からサーバーのリンクをクリックし、**[サーバーの詳細]** ウィンドウを開きます。
2. **[キャッシュ]** タブをクリックします。
3. ドロップダウン リストを使用して、HPCA Core Server から事前に読み込めるようにするサービスの有効 / 無効を切り替えます。デフォルトでは、事前読み込みはすべてのサービスに対して無効になっています。
4. **[保存]** をクリックして、変更を適用します。
5. **[同期]** をクリックし、使用可能なデータを使用して Satellite Server を即時に事前読み込みします。

Satellite Server を同期するには

1. [設定] タブで、[インフラストラクチャ管理] の [Satellite 管理] 領域に移動します。
2. [サーバー] タブで、同期するサーバーを選択します。

3 **[選択された Satellite Server のサービス キャッシュの同期]**  ツールバー ボタンをクリックし、HPCA Server の最新データを使用して、選択したすべてのサーバーを更新します。各サーバーに事前に読み込まれている特定のサービスは、各サーバーの [サーバーの詳細] ウィンドウの **[キャッシュ]** タブの設定内容に依存します。

[サーバーの詳細] ウィンドウから Satellite Server を同期することもできます。または、いずれかの Satellite 同期ジョブ アクション テンプレートを使用して、DTM ジョブをスケジュールすることもできます。詳細については、182 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。

Satellite Server のキャッシュ内の事前に読み込まれたサービスの要約を表示するには

[サーバーの詳細] ウィンドウを開き、**[レポート]** タブをクリックします。

[レポート] タブにキャッシュ内で利用できる事前に読み込まれたサービスおよびそれぞれのステータスが表示されます。

[イベント] カラムでは、次のような現在のステータスが説明されます。

- **更新 (事前読み込み)** - サービスは、前回のキャッシュ同期で更新されました。
- **インストール (事前読み込み)** - サービスが正常に事前読み込みされました (初期事前読み込み)。
- **アンインストール (事前読み込み)** - サービスが事前読み込みキャッシュから削除されました。
- **修復 (事前読み込み)** - サービス用のキャッシュは、ファイルが不明であるか無効なファイルを含んでおり、前回の同期で修復されました。

レポートには、事前に読み込まれたサービスのみが表示されます。デフォルトのメソッド (管理対象デバイスによって要求された際に自動的にキャッシュされる) によって Satellite Server に格納されているサービスは、表示されません。

サブネット ロケーション

[サブネット ロケーション] タブを使用して、既存のサブネット ロケーションを表示したり、新しいロケーションを追加したりします (このロケーションには、Satellite Server を後から割り当てることができます)。管理対象デバイスは、サブネットの割り当てに基づいて Satellite Server に接続されます。

[サブネット ロケーション] ツールバーには、使用環境のサブネット ロケーションの定義および設定に使用できるボタンがあります。

表 34　[サブネット ロケーション] ツールバー ボタン

ボタン	説明
	**データのリフレッシュ** - ロケーション (サブネット) のリストをリフレッシュします。
	**CSV にエクスポート** - 開いたり保存したりできる、カンマ区切りの場所のリストを作成します。
	**新しいサブネット ロケーションの作成** - インフラストラクチャ ロケーションの作成ウィザードを起動します。
	**インベントリ データに基づくサブネット ロケーションの自動作成** - 管理対象デバイスからのインベントリ データに基づいて、ロケーションのリストを作成します。
	**ロケーションの削除** - 選択したロケーションを削除します。

サブネット ロケーションのリストには、追加された各サブネット ロケーションの情報が含まれています。たとえば、割り当てられているサーバーやサブネット内に存在するデバイスの数などの情報です。任意の **[サブネット アドレス]** をクリックして、[[サブネット ロケーションの詳細] ウィンドウ] ウィンドウを開きます。

HPCA に格納されているインベントリ データに基づいて、新しいサブネット ロケーションを手動で作成するか、自動的に作成することができます。必要なインベントリ データを取得するには、HPCA Agent が配布されている必要があります。

新しいサブネット ロケーションの作成

サブネット ロケーションを作成する方法は 2 つあります。サブネット アドレスを明示的に指定するか、既存の HPCA インベントリ データに基づいてロケーションを生成できます。

新しいサブネット ロケーションを手動で作成するには

1　**[新しいサブネット ロケーションの作成]**  ツールバー ボタンをクリックして、サブネット ロケーション作成ウィザードを起動します。

2　ウィザードの手順に従って、新しいサブネット ロケーションを作成します。

インベントリ データに基づいて新しいロケーションを作成するには

1 **[インベントリ データに基づくサブネット ロケーションの自動作成]**  をクリックします。

2 **[OK]** をクリックします。

3 **[閉じる]** をクリックします。

サブネット ロケーションのリストが更新されます。このメソッドでは、見つかった新しいサブネットごとに 1 つのロケーションが作成されます。

サブネット ロケーションを追加したら、Satellite Server をそのロケーションに割り当てることができます。

Satellite Server へのサブネット ロケーションの割り当て

サブネット ロケーションを Satellite Server に割り当てると、そのサブネットのすべての管理対象クライアント デバイスが該当の Satellite Server を介して HPCA と通信するようになります。

サブネット ロケーションを Satellite Server に割り当てるまで、そのサブネットのすべての管理対象クライアントは HPCA Core Server と直接通信します。

サブネット ロケーションを Satellite Server に割り当てるには

1 **[サーバー]** タブをクリックします。

2 サブネット ロケーションを割り当てるサーバーをクリックします。[サーバーの詳細] ウィンドウが開きます。

3 **[サブネット ロケーション]** タブをクリックします。

4 **[Add Subnet Locations]**  ツールバー ボタンをクリックします。[サブネット ロケーション] ウィンドウが開きます。

5 Satellite Server に割り当てるサブネット ロケーションを選択し、**[ロケーションの追加]** をクリックします。

6 **[閉じる]** をクリックします。

7 サブネット ロケーションの追加が完了したら、**[閉じる]** を再度クリックし、[サーバーの詳細] ウィンドウを閉じます。

以上の手順が完了すると、サブネット ロケーションが Satellite Server に割り当てられ、定義されたサブネット内で接続を行うデバイスは、リソースのニーズに応じてそのサーバーに振り分けられます。

Satellite Server に割り当てられているサブネット ロケーションを削除するには

1 **[サーバー]** タブをクリックします。

2 サブネット ロケーションを削除するサーバーをクリックします。[サーバーの詳細] ウィンドウが開きます。

3 **[サブネット ロケーション]** タブをクリックします。

4 削除するサブネット ロケーションをリストから選択して、**[サブネット ロケーションの削除]**  ツールバー ボタンをクリックします。

5 **[閉じる]** をクリックします。

6 サブネットロケーションの削除が完了したら、**[閉じる]** を再度クリックし、[サーバーの詳細] ウィンドウを閉じます。

[サブネット ロケーションの詳細] ウィンドウ

[サブネット ロケーション] テーブルで、サブネット アドレスをクリックして [サブネット ロケーションの詳細] ウィンドウを開きます。

- **[プロパティ]** タブを使用して、このサブネット ロケーションの説明を変更します。

  変更後、**[保存]** をクリックします。

- **[デバイス]** タブを使用して、このサブネット内に存在するすべてのデバイスをリストします。

デバイス管理

[デバイス管理] セクションを使用して、警告オプション、シン クライアント、およびリモート制御を設定します。

次のセクションでは、利用可能なデバイス管理オプションについて説明します。

- 330 ページの「警告中」
- 331 ページの「シン クライアント」
- 331 ページの「リモート制御の設定」

警告中

[警告中] セクションを使用して、CMI の警告およびレポート オプションを設定します。

- 330 ページの「CMI」

CMI

CMI Softpaq は、HPCA Agent 配布の一部として、各 HP ターゲット デバイスにインストールされます。HP Client Management Interface(CMI) は、企業管理者や IT プロフェッショナルに、HP ビジネスクラス デスクトップ、ノートブックおよびワークステーションに対する高レベルの管理システムを提供します。

CMI のハードウェア固有の情報がキャプチャされ、レポートに利用できます。[レポート] タブの [表示オプション] セクションで **[HP 固有のレポート]** レポート ビューを使用して、CMI ハードウェア関連レポートを作成します。(CMI 関連のレポート オプションを表示するには、**[インベントリ管理レポート]**、**[ハードウェア レポート]**、**[HP 固有のレポート]** の順で選択します)。

CMI に関する詳細は、次を参照してください。

http://h20331.www2.hp.com/Hpsub/cache/284014-0-0-225-121.html

[CMI] タブを使用して、HP CMI 設定を変更します。変更した設定は、管理対象のクライアントが次に HPCA インフラストラクチャに接続したときに、有効になります。

CMI は、特定の HP デバイス モデルでしか互換性がありません。互換性に関する情報は、デバイスの説明を参照してください。

CMI を設定するには

1 HPCA Console で、**[設定]** タブをクリックし、**[デバイス管理]** を選択します。

2 管理対象 HP デバイスからキャプチャしたクライアント警告についてレポートするには、**[クライアント警告のレポート]** ドロップダウン リストから **[有効]** を選択します。警告レポートはデフォルトでは無効になっています。[有効] を選択すると、[レポートする最低の重大度] ドロップダウン リストが使用できるようになります。

3 レポートする最低の警告重大度を選択します。

4 管理対象 HP デバイスのクライアント警告を有効にするには、**[クライアント警告の表示]** ドロップダウン リストから **[有効]** を選択します。警告はデフォルトでは無効です。[有効] を選択すると、[表示する最低の重大度] ダイアログと [警告ウィンドウのタイムアウト] ダイアログが使用できるようになります。

5 クライアント デバイスに表示する最低の警告重大度を選択します。

6 警告をクライアント デバイスに表示する秒数を入力します。デフォルトでは、警告は 5 秒間表示されます。

7 **[保存]** をクリックします。

シン クライアント

シン クライアント管理サービスによって Windows CE デバイスに設定データが提供されます。Core でこのサービスが無効になっている場合、この情報をリクエストする Satellite またはエージェントはこの情報を使用できません。

- シン クライアント管理を有効にするには、このチェック ボックスをオンにして **[保存]** をクリックします。

リモート制御の設定

HPCA Console では、Windows リモート デスクトップ接続、Virtual Network Computing (VNC)、または Windows リモート アシスタンスを使用して内部リポジトリまたは外部リポジトリのデバイスにリモート アクセスできます。

HPCA 管理者は、HPCA Console を設定して任意またはすべての接続タイプを有効にできます。リモート制御をすべて無効にすることもできます。

接続タイプごとに、リモート ターゲット デバイスがリモート接続をリスンするポートを指定する必要があります。各接続タイプに関連する追加要件については、197 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、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。

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、196 ページの「デバイスのリモート制御」を参照してください。

パッチ管理

パッチ管理を有効にして、パッチ データベースの ODBC パラメータを定義するには、[パッチ管理] リンクを使用します。

このリンクの管理オプションは、Core コンソールと Satellite コンソールで異なります。

このセクションでは、Core コンソールの [パッチ管理] リンクから実行できるパッチ管理オプションについて説明します。Satellite コンソールで使用できるオプションの詳細については、366 ページの「Satellite コンソールのパッチ管理」を参照してください。

パッチ管理のオプションについては、次のセクションで説明します。

- 333 ページの「データベース設定」
- 342 ページの「設定」
- 337 ページの「エージェント オプション」
- 345 ページの「ベンダーの設定」
- 334 ページの「パッチ配布設定」
- 361 ページの「取得ジョブ」

[パッチ配布設定] では、Microsoft パッチを適用するための新しい軽量なモデルを選択できます。詳細については、次の章を参照してください。

- 391 ページの「メタデータを使用したパッチ管理」。

データベース設定

コンソールの [パッチ管理] 領域とパッチ取得機能を使用するには、パッチを有効にする必要があります。

パッチ管理サービス (`HPCA Patch Manager`) を開始して、パッチ データベースと Core 権限のある CSDB パッチ ライブラリに保存された情報と SQL データベースの情報を同期する機能を有効にするには、[データベース設定] 領域を使用します。

前提条件

- パッチ データベースを作成し、そのデータベースの ODBC 接続を定義する必要があります。詳細については、『HPCA Core および Satellite Servers 入門およびコンセプト ガイド』を参照してください。

パッチの有効化および設定を行うには

1 **[有効]** を選択します (これにより、`HPCA Patch Manager` サービスが開始します)。

2 パッチの [ODBC 設定] 領域で、次のオプションを設定します。

   — **ODBC DSN**: Patch SQL データベースの DSN を選択します。

   — **ODBC のユーザー ID**: DSN のユーザー ID を指定します。

   — **ODBC のパスワード**: ODBC ユーザー ID に関連付けられているパスワードを指定します。

3 **[保存]** をクリックします。

4 パッチの ODBC 設定を変更した場合、確認メッセージに従って Patch Manager サービスを再開します。

パッチ配布設定

[パッチ配布設定] 領域を使用して、次のオプションの有効化および設定を行います。

- [パッチ メタデータのダウンロード] オプション

このオプションが有効になっている場合、次の設定に関連するオプションもページに表示されます。

- [パッチ ゲートウェイ オペレーション] 設定

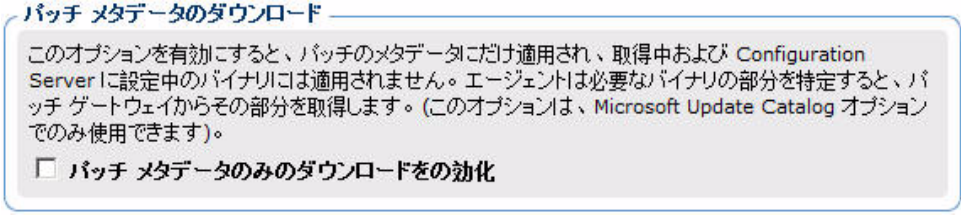
これらのオプションにより、軽量な取得および配布モデルで Microsoft Update Catalog を使用して Microsoft デバイスにパッチを適用できます。

メタデータによるパッチ管理を使用する場合も、**[Download Manager を有効化]** をオンにする *必要* があります。これを行うには、**[設定] > [パッチ管理] > [エージェント オプション]** ページに移動します。

Microsoft デバイスにパッチを適用する場合、可能な限り [パッチ メタデータのダウンロード] と [パッチ ゲートウェイ オペレーション] を使用することをお勧めします。これには、391 ページの「メタデータを使用したパッチ管理」の章で説明されているようにいくつかの利点があります。

- 軽量なメタデータ メカニズムを使用して Microsoft パッチを管理するには、**[パッチ メタデータのみのダウンロードを有効化]** チェック ボックスをオンにします。Microsoft Update Catalog データ フィードを使用する必要があります。

  このオプションをオンにすると、メタデータのみが Configuration Server Database にダウンロードおよびパブリッシュされます。エージェントのリクエスト時またはゲートウェイの事前読み込み時に、パッチ バイナリ ファイルが Patch Manager ゲートウェイにダウンロードおよびキャッシュされます。



パッチ メタデータのダウンロードを有効にする場合、取得を実行する前に次のオプションの有効化および設定も行う必要があります。

- Core または Satellite の [パッチ ゲートウェイ オペレーション] (必須)

- エージェント オプション : Download Manager を有効化 (必須)

[パッチ メタデータのダウンロードの有効化] がオンの場合、パッチを取得するためのベンダー値が MICROSOFT から MSFT に切り替わります。

メタデータのダウンロードおよびゲートウェイ操作を使用した環境の設定とパッチの取得の詳細については、391 ページの「メタデータを使用したパッチ管理」を参照してください。必ずオフライン スキャンを設定して Download Manager の事前読み込みオプションを設定してください。

パッチ ゲートウェイ オペレーション

[パッチ配布設定] ページの [パッチ メタデータのダウンロード] オプションが有効になっている場合、パッチ ゲートウェイ オペレーションの設定を使用できます。

このセクションで説明しているパッチ ゲートウェイ オペレーションは、Core Server のパッチ ゲートウェイにのみ適用されます。Satellite Server で使用できるパッチ ゲートウェイ オペレーションについては、366 ページの「Satellite コンソールのパッチ管理」を参照してください。

これらの設定を使用して、ゲートウェイを有効にします。

有効にすると、追加のエントリを使用してパッチ バイナリのキャッシングおよび管理を行うように設定できます。

Microsoft Update Catalog データ フィードのいずれかを使用して Microsoft Agent に軽量なパッチ適用を実現する [パッチ メタデータのダウンロード] オプションを使用するには、パッチ ゲートウェイが必要です。

パッチ ゲートウェイの役割は、[パッチ メタデータのダウンロードの有効化] がオンの場合にのみ、実際のパッチ バイナリ データをダウンロードしてキャッシュし、エージェントに配信することです。任意指定の [ゲートウェイ事前読み込み] オプションを使用すると、エージェントからのリクエスト時ではなく取得時にパッチ バイナリをゲートウェイにキャッシュできます。

- **[ゲートウェイの有効化]** チェック ボックスをオンにすると、Microsoft パッチ バイナリ データのオンデマンド ダウンロードおよびキャッシングがゲートウェイで可能になります。これを行うには、**Microsoft Update Catalog** データ フィードのいずれかを使用する軽量な [パッチ メタデータのダウンロード] オプションを使用する必要があります。

[ゲートウェイの有効化] がオンになっていると、次のフィールドを使用できます。

- **[最大キャッシュ サイズ]** では、ゲートウェイ キャッシュの最大サイズ (MB) を指定します。空白または 0 の場合は「キャッシュの上限がない」ことを意味します。

  デフォルト : 1000 MB

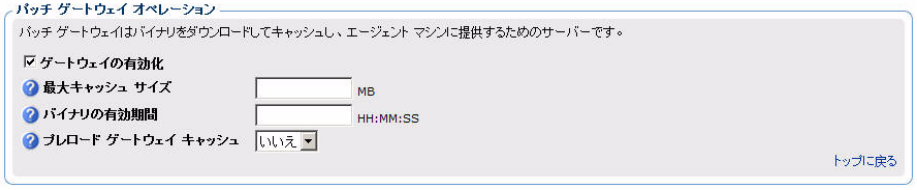
- **[バイナリの有効期間]** では、キャッシュされたバイナリ ファイルをアップストリーム サーバーから再検証せずにゲートウェイに保持する最大期間 (時間 : 分 : 秒の形式) を指定します。値が -1 または空白の場合は、バイナリを

リフレッシュしないことを意味します。値が 10:00:00 の場合は、バイナリがキャッシュに 10 時間保持された後に再度ダウンロードされることを意味します。

デフォルト : 空白 (リフレッシュなし)

- **[事前読み込みゲートウェイ キャッシュ]** (オプション) で **[はい]** を指定すると、取得の実行時にパッチ バイナリがゲートウェイにキャッシュされます。事前読み込みオプションを設定する前に次の点に注意してください。事前読み込みのメリットの 1 つは、パッチ バイナリを最初にリクエストするエージェントが、ゲートウェイによるパッチ バイナリのダウンロードを待たずにパッチ バイナリを取得できるという点です。ただし、事前読み込みのデメリットとして、エージェントで必要とされているかどうかに関係なく、取得時にすべてのパッチ バイナリがダウンロードされます。

  エージェントからパッチのリクエストを受信したときにのみゲートウェイからパッチ バイナリ データをダウンロードおよびキャッシュするようにする場合、**[いいえ]** (デフォルト) を指定します。



エージェント オプション

これらのエージェント オプションは、Microsoft デバイスのパッチにのみ適用されます。

Microsoft デバイスにパッチを適用するための Patch Manager Agent のオプションを有効化および設定するには、[設定] タブ > [パッチ管理] 領域からアクセスできる [エージェント オプション] を使用します。

Patch Agent が次に HPCA Server に接続するときに、これらのパネルで指定した設定の変更が受信されます。

- 338 ページの「Download Manager オプション」
- 340 ページの「Patch Manager のエージェント オプション」

Download Manager オプション

- **Download Manager を有効化**: このチェック ボックスをオンにすると、Agent マシンに必要なパッチ ファイルのダウンロードが、Download Manager によってバックグラウンドの非同期プロセスで制御されます。Download Manager は、通常の HPCA Agent Connect プロセスの外部で動作します。

  メタデータによるパッチ配布を使用するには、Download Manager を有効にする必要があります。

  オンにすると、Download Manager のオプションがいくつか表示されます。

  次の表を参考にして、Download Manager オプションを設定します。

  ネットワーク利用、スクリーン セーバー モードでのネットワーク利用、初期化後の遅延、およびダウンロード完了後のパッチ適用の有無を指定するオプションを設定します。

表 35　Patch Agent の Download Manager オプション

オプションと有効な値	説明
ネットワーク利用 値 = 0 ～ 100 % デフォルトは 0	デバイスがアクティブな場合にパッチ ファイルのダウンロードに使用できるネットワークの最大バンド幅の割合を指定します。 値が 0 の場合、使用可能なネットワークのバンド幅でダウンロードが行われます。 例 : 25 を指定すると、使用可能なバンド幅の 25% 以下でパッチのダウンロード プロセスが行われます。
スクリーンセーバー モードでのネットワーク利用 値 = 0 ～ 100 % デフォルトは 0	スクリーン セーバーのネットワーク利用のオプションです。スクリーン セーバーがオンの場合にパッチ ファイルのダウンロードに使用できるネットワークの最大バンド幅の割合を指定します。通常、このオプションの値はスクリーン セーバーがオフの場合よりも大きな割合になります。 値が 0 の場合、スクリーン セーバーがオンのときに使用可能なネットワークのバンド幅でダウンロードが行われます。 例 : 80 を指定すると、スクリーン セーバーがオンのときにパッチ ファイルをダウンロードするために使用するバンド幅が 80% に増加します。
遅延初期化 値 = 0 ～ 999 秒 デフォルトは 0	初期化してからパッチのダウンロードを開始または再開するまでの遅延時間 (秒) を指定します。これにより、他のプロセスを起動してからパッチのダウンロードを再開できます。 例 : 15 に設定すると初期化が 15 秒遅延します。 値が 0 の場合は遅延はありません。
ダウンロード完了後にパッチを適用 値 = [はい] または [いいえ] (デフォルト)	[はい] に設定すると、ダウンロードの完了後に Patch Agent 接続を起動してパッチを適用します。[はい] に設定することをお勧めします。 デフォルトの [いいえ] のままにしておくと、Patch Agent 接続が次に実行されたときにパッチが適用されます。

[保存] をクリックして、これらの設定オプションを設定します。Patch Agent が次に HPCA Server に接続するときに、新しい設定が受信されます。

Patch Manager のエージェント オプション

次のエージェント オプションを使用して Microsoft デバイスにパッチを適用できます。

- **自動更新を無効化**：ドロップダウン ボックスから [はい] または [いいえ] を選択します。自動更新が有効になっていることが原因で Patch Agent のスキャンまたは配布が中断される問題に対応するには、このオプションを使用します。
  - **はい**：Patch Agent によって各スキャンまたは配布の前に Microsoft 自動更新が無効化されます。パッチのスキャンと配布が実行されたら、自動更新は元の状態に戻ります。
  - **いいえ**：(デフォルト) Patch Agent によって各スキャンまたは配布の前に自動更新が無効化されません。
- **ソフトウェア配布フォルダの削除**：ドロップダウン ボックスから [はい]、[バックアップ]、または [いいえ] を選択します。このオプションは、次の問題の対応に使用できます。
  - ソフトウェア配布フォルダのサイズの大幅な増加
  - ソフトウェア配布フォルダの破損
  - パッチ接続時に Configuration Server にかかる負荷の増加

  [ソフトウェア配布フォルダの削除] を [はい] または [バックアップ] に設定すると、Microsoft 自動更新とバックグラウンド インテリジェント転送サービス (BITS) のサービスが自動的に再起動されます。サービスの再起動によって環境に問題が発生する場合、特に共存するパッチ ソリューションとして HPCA パッチ管理と自動更新の両方を使用しているとき、このオプションの設定には注意が必要です。

  このオプションを [はい] または [バックアップ] に設定すると、フォルダ サイズ、破損、またはインフラストラクチャの負荷に問題がある場合に Patch Manager のパフォーマンスが向上します。
  - **はい**：Patch Agent によって、各パッチのスキャンの前にソフトウェア配布フォルダの内容が削除されます。サービスの再起動に関する警告 (上記) を参照してください。

— **バックアップ** : Patch Agent によって、各パッチのスキャンの前にソフトウェア配布フォルダの内容がバックアップされてから削除されます。サービスの再起動に関する警告 (上記) を参照してください。

— **いいえ : (デフォルト)** ソフトウェア配布フォルダに対して何も行われません。

- **-mib (インストール済みのブリティンを管理する):** ドロップダウン ボックスから [なし]、[いいえ]、または [はい] を選択します。このオプションは、ターゲット デバイスにインストール済みのブリティンの処理方法を制御します。

  — **なし : (デフォルト)** Patch Manager によってインストールされたブリティンのみを管理します。別の方法でインストールされたブリティンのサービス ライブラリまたはバイナリ リソースは確認しません。これはデフォルトの動作です。脆弱性または再パッチに関してクライアント エージェントは何も影響を受けず、高いパフォーマンスを得られるためです。

  — **いいえ :** Patch Manager によってインストールされたブリティンのみを管理します。外部ソースによってインストールされたブリティンは管理しません。

  — **はい** : Patch Manager または外部ソースのどちらでインストールされたかに関係なく、すべてのインストール済みブリティンを管理します。このオプションはリソースを大きく消費します。

[保存] をクリックして、設定オプションを設定します。Patch Agent が次に HPCA Server に接続するときに、新しい設定が受信されます。

エージェントの更新

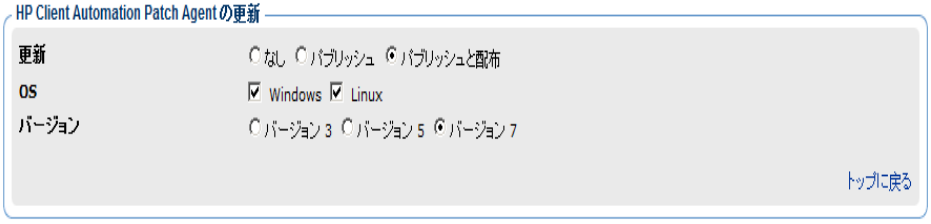
[エージェントの更新] を使用して、パッチ管理のエージェントの更新を設定します。

HP Patch Agent の更新設定

これらの設定を使用して、HP Client Automation (HPCA) Patch Manager Agent ファイルに対するメンテナンスを取得および適用します。詳細については、259 ページの「エージェントの更新を表示」を参照してください。[HP Patch Agent の更新] セクションで、次の設定を行います。

- **更新**: [パブリッシュ] を選択すると更新は PATCHMGR ドメインにパブリッシュされますが、配布するために Patch Manager ターゲット デバイスに接続されることはありません。これらの接続は作成する必要があります。[パブリッシュと配布] を選択すると、更新が PATCHMGR ドメインにパブリッシュされ、DISCOVER_PATCH インスタンスに接続されます。このオプションでは、更新が Patch Manager ターゲット デバイスに配布されます。
- **OS**: Patch Manager Agent の更新を取得および管理するベンダーのオペレーティング システムのタイプを指定します。
- **バージョン**: エージェントの更新を取得する Patch Manager のバージョンを選択します。1 つの Configuration Server には 1 つのバージョンのみをパブリッシュできます。デフォルトは、使用可能な最新のバージョンです。

  Patch Manager を最初にインストールする場合は、[バージョン] パラメータをインストール時のデフォルトから変更しないでください。



設定

ここでは、ベンダーと取得の設定を行います。これらの設定は、[ベンダーの設定] と [取得ジョブ] に反映されます。

- **次のものについてパッチ管理を有効にする**: パッチを取得する OS のベンダーを指定します。これらのベンダーは、[ベンダーの設定] と [取得の設定] に表示されます。後日、その他のベンダーのパッチを取得することにした場合、最初にここで指定する必要があります。

- **取得の概要を保存** : PASTORE (Patch Auth Store) インスタンスを維持する日数を指定します。このクラスには、各パッチ取得セッションにつき 1 つのインスタンスが含まれます。この値が [履歴の詳細を保存] の値より小さい場合、[履歴の詳細を保存] は [取得サマリを保存] の値に設定されます。値 0 は、パッチ取得の履歴を削除しないことを意味します。
- **履歴の詳細を保存** : PUBERROR (Publisher Error) インスタンスを維持する日数を指定します。このクラスには、各パッチ取得エラーにつき 1 つのインスタンスが含まれます。
- **パッチ データのリポジトリ パス** : Configuration Server にパブリッシュされる前に、パッチがダウンロードされるディレクトリ。前回の取得のデータを事前に設定したディレクトリを使用して取得を実行する場合は、このパラメータに事前に設定するディレクトリを指定します。
- **過去のブリティン** : 過去のブリティンをカンマで区切って表示します。このパラメータは、製品またはリリース レベルではなく、ブリティン レベルで作用します。

  過去の機能で、以下を実行します。

  — 指定したブリティンが Configuration Server DB に存在する場合は、現在のパブリッシュ セッション中に削除します。

  — 過去のパラメータで指定したブリティンは、現在のパブリッシュ セッション中に Configuration Server DB にパブリッシュしないでください。過去オプションはブリティン オプションより優先されます。
- **除外された製品** : カンマで区切った *vendor*::*product* の形式で、除外する製品の先頭に感嘆符 (!) を付けます。包括フィルタが設定されていない場合はすべての製品が対象となります。包括フィルタを指定する場合は、除外フィルタは包括される製品のサブセットになります。これはベンダーの命名基準に従って指定してください。たとえば、Microsoft は、Internet Explorer を IE のような一般的な省略名でなく、完全名で使用します。また、Windows 95 以外のすべての Windows 製品を含める場合は、`{Microsoft::Windows*,Microsoft::!Windows 95}` と入力します。

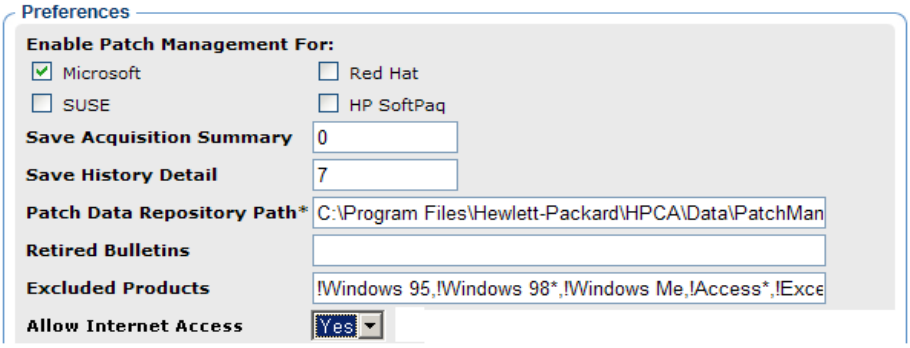
新しい Patch Manager インストールの場合、セキュリティ パッチの取得と管理では、Microsoft Office、Windows 95、Windows 98、Window Me、Microsoft Office 製品および SuSE 特有の製品 *-yast2、*-yast2-*、および *-liby2 は、デ

*フォルトで除外*されています。SuSE OS yast 特有製品の自動管理は、Patch Manager ではサポートされません。

以前のバージョンの Patch Manager からの移行で、移行前に `patch.cfg` を削除しなかった場合、すべての Microsoft Office 製品またはそのスタンドアロン バージョンを Patch Manager の取得と管理から除外するには、製品除外リストに次のテキストを追加します。

",!Access*,!Excel*,!FrontPage 200[023],!FrontPage 9[78],!InfoPath*,!Office*,!OneNote*,!Outlook*,!PowerPoint*,!Project 200[023],!Project 98,!Publisher*,!Visio*,!Word*,!Works*"

上のテキストはすべて 1 行で表示され、ユーザー インターフェイスの [除外された製品] テキスト ボックスには上で表示されている引用符が含まれないため注意してください。



- **インターネット アクセスの許可 :** ドロップダウン ボックスから [はい] または [いいえ] を選択します。このオプションを使用して、Patch Manager Server がインターネットにアクセスできるかどうかを指定します。
  - **はい :** (デフォルト) Patch Manager は、取得中にインターネットにアクセスします。
  - **いいえ :** Patch Manager は、取得中にインターネットにアクセスしません。この場合、データ フォルダに既に存在するブリティン (メタデータとバイナリ) のみがパブリッシュされます。

- **デフォルトのパッチ取得ダウンロードの言語**: セキュリティ パッチを取得および管理する言語を指定します。デフォルトは en(英語) です。

ベンダーの設定

ベンダーの設定には、自社のエージェントに関するベンダー特有の URL や、パッチの取得および管理アクティビティに必要なその他のオプションが表示されます。

ベンダーの設定を入力する前に、まず [設定] ページを使用して適切なベンダーと OS の選択を有効にしてください。

ある取得セッションから次のセッションの間にベンダーの設定を変更して、以前は選択されていた 1 つ以上の製品またはオペレーティング システムを除外した場合、除外した製品またはオペレーティング システムに特有のすべてのパッチが Configuration Server Database から削除されます。これは、除外された製品またはオペレーティング システムが、脆弱性の評価および管理の観点で今後は適格でなくなることを意味します。これは、すべてのベンダーに適用されます。

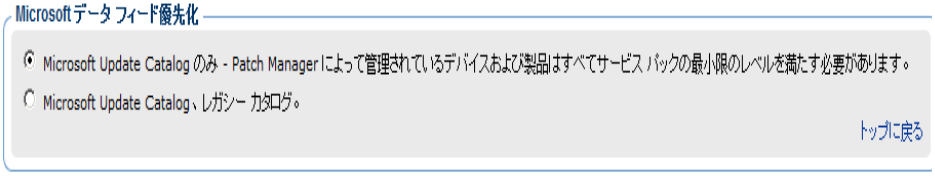
ベンダーの設定 :

- 345 ページの「Microsoft データ フィード優先化」
- 349 ページの「Red Hat のフィード設定」
- 351 ページの「SuSE のフィード設定」
- 356 ページの「HP SoftPaq のフィード設定」

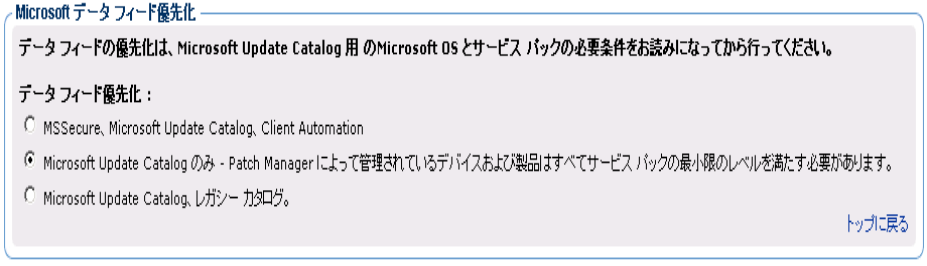
Microsoft データ フィード優先化

次の Microsoft データ フィード優先化設定は、使用可能な Microsoft の更新リポジトリとメソッドをサポートおよび優先化するために、[ベンダーの設定] セクションで設定します。

[パッチ配布設定] の **[パッチ メタデータのみのダウンロードを有効化]** オプションがオンになっている場合、Microsoft Update Catalog データ フィードのいずれかを選択できます。



[パッチ配布設定] の **[パッチ メタデータのみのダウンロードを有効化]** オプションがオフになっている場合、[Microsoft データ フィード優先化] パネルには次の 3 つのオプションが表示されます。



Microsoft パッチ管理アクティビティの詳細は、『HPCA Patch Manager インストールおよび設定ガイド』の「パッチ取得」の章を参照してください。

- **MSSecure、Microsoft Update Catalog、Client Automation**: このオプションは、[パッチ メタデータのダウンロード] オプションがオンの場合に表示されます。パッチは、MSSecure と Microsoft Update Catalog の両

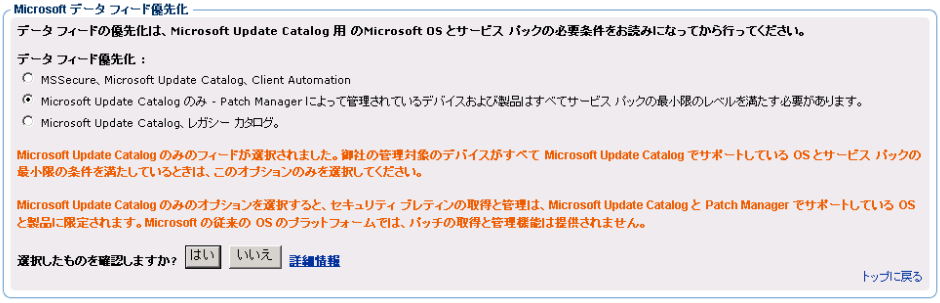
方から取得します。パッチが MSSecure と Microsoft Update Catalog の両方に存在する場合、MSSecure をサポートしているテクノロジが使用されます。

MSSecure テクノロジのために、このオプションでは Windows Vista(32 ビットまたは 64 ビット) または 64 ビット アーキテクチャの Windows を実行するデバイスにはパッチを適用できません。これらのデバイスにパッチを適用するには、Microsoft Update Catalog を含む [データ フィード優先化] を選択します。

このマニュアルを作成している時点で、Microsoft の Web サイトでは、レガシー カタログは 2008 年まで継続して更新されるが、MSSecure.xml は 2007 年 10 月 9 日以降は更新されないことを示唆しています。

- **Microsoft Update Catalog のみ** : (デフォルト オプション) すべてのパッチは Microsoft Update Catalog から取得されます。このオプションを使用するには、企業内のすべてのデバイスが Microsoft によって設定された最低レベルのオペレーティング システムおよび製品である必要があります。これらの最低要件に適合していないデバイスにはパッチは適用されません。

  このオプションを変更すると、次の警告メッセージが表示され、続行するにはこれに同意する必要があります。



[はい] をクリックすると、このオプションの選択を確認する画面がもう一度表示されます。**[保存]** をクリックして確定します。

- **Microsoft Update Catalog、レガシー カタログ**：パッチは、Microsoft Update Catalog と、現在の MSSECURE と HP が修正したメタデータを含む、レガシー カタログと呼ばれる HP リポジトリから取得されます。パッチが、Microsoft Update Catalog とレガシー リポジトリの両方に存在する場合は次のとおりです。
  - ターゲット デバイスが Microsoft Update Catalog でサポートされる最低要件に一致している場合、そのデバイスには Microsoft Update Catalog と Windows Update Agent テクノロジを利用してパッチが適用されます。
  - ターゲット デバイスが Microsoft Update Catalog でサポートされる OS の最低要件に適合していない場合、デバイスにはレガシー カタログでホストされるメタ データを使用する MSSecure テクノロジを使用してパッチが適用されます。

  HP レガシー カタログは、新しいパッチが MSSecure に追加されると、HP によって継続的に更新されます。HP レガシー カタログでホストされるパッチには、HP メタデータの修正が必要です。**[Microsoft Update Catalog、レガシー カタログ]** オプションをオンにすると、Microsoft セキュリティ ブリティンは古い Microsoft オペレーティング システム (各種のサービス パックも含めて) に適用可能とみなされます。また、Microsoft 製品には、Configuration Server の PATCHMGR ドメインと Reporting Server で表示される Patch Manager レポートで識別するために、Microsoft ブリティン名に「_L」が追加されます。

  Office アプリケーションが HP Client Automation Application Self-Service Manager または管理制御ポイントで管理されている場合、Microsoft Update Catalog テクノロジを使用して取得および管理される Office のパッチは検出されません。どちらの場合も、Office アプリケーションに影響を与えるブリティンがデバイスに指定された場合は、Patch Manager が Office のパッチを管理し、それを脆弱なデバイスにローカルにインストールします。

Microsoft のフィード設定

以下の設定はベンダー フィードのセクションで行います。

[詳細] だけで表示されるフィールド

- **MSSecure***: Microsoft が提供する MSSECURE.XML ファイルを含む、Microsoft の MSSecure キャビネット ファイルの URL を指定します。

  デフォルト : **http://download.microsoft.com/download/0/d/b/0db2e5d7-0ba9-4856-b51f-db7c0b838c68/MSSecure_1033.CAB**

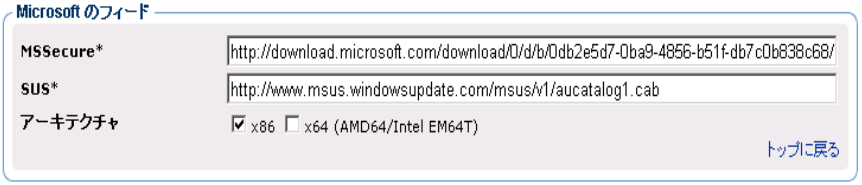
  このマニュアルを作成している時点で、Microsoft Knowledge の記事では、Microsoft は 2008 年までこのカタログの更新は継続するが、2007 年 10 月 9 日以降、MSSecure.xml のサポートおよび更新を継続しない計画であることを示唆しています。

- **SUS***: Microsoft SUS データ フィードを含む Microsoft キャビネット ファイルの URL を指定します。

  デフォルト : **http://www.msus.windowsupdate.com/msus/v1/aucatalog1.cab**

[基本] と [詳細] のフィールド

- **アーキテクチャ** : Microsoft のパッチを取得するアーキテクチャを選択します。サポートされるアーキテクチャは次のとおりです。
  - **x86**:32 ビット Intel アーキテクチャ用。
  - **x64**:AMD64 または Intel EM64T 用。この対象アーキテクチャを選択する場合は、[Microsoft データ フィード優先化] を「**Microsoft Update Catalog のみ**」または「**Microsoft Update Catalog、レガシー カタログ**」に設定する必要があります。



Red Hat のフィード設定

[Red Hat のフィード] セクションでは、以下の設定を行います。

[詳細] だけで表示されるフィールド

- **Red Hat**: Red Hat Network のデータ フィードの URL を指定します。デフォルトは **http://xmlrpc.rhn.redhat.com/XMLRPC** です。

[基本] と [詳細] のフィールド

- **パッケージ依存関係をパブリッシュ** : ダウンロードしたセキュリティ アドバイザリが依存する追加の Red Hat パッケージをパブリッシュする場合は、**yes** を指定します。デフォルトは「いいえ」です。

  Red Hat セキュリティ アドバイザリをインストールするための前提となる、または依存する Red Hat パッケージは、2 か所から取得できます。それらは、取得中に Red Hat ネットワークからダウンロードするか、以前に Red Hat Linux インストール メディアをコピーしたことがある場合はローカルに見つけることができます。Patch Manager は、取得時にまず適切なディレクトリで .rpm パッケージを検索します。例 :

  — x86 の Red Hat Enterprise Linux 4ES では、Red Hat インストール メディアで提供されたベースライン オペレーティング システムの rpm ファイルを `Data\PatchManager\Patch\redhat\4es` に配置します。

  — x86-64 の Red Hat Enterprise Linux 4ES では、Red Hat インストール メディアで提供されたベースライン オペレーティング システムの rpm ファイルを `Data\PatchManager\Patch\redhat\4es-x86_64` に配置します。

  — `Data\PatchManager\Patch\redhat\packages` サブディレクトリに名前を付けるときは、次の **OS フィルタのアーキテクチャ**の値のリストを参照してください。サブディレクトリ名には、`REDHAT:` に続く値に基づいて適切なフォルダ名を使用します。

  パッチの前提ソフトウェアがローカルに見つからない場合、パッケージを Red Hat Network からダウンロードします。取得に必要な時間を短縮するために、依存パッケージを Linux インストール メディアから適切なパッケージ ディレクトリにコピーすることをお勧めします。Red Hat RPM パッケージは、Linux インストール メディアの `RedHat/RPMS` ディレクトリにあります。

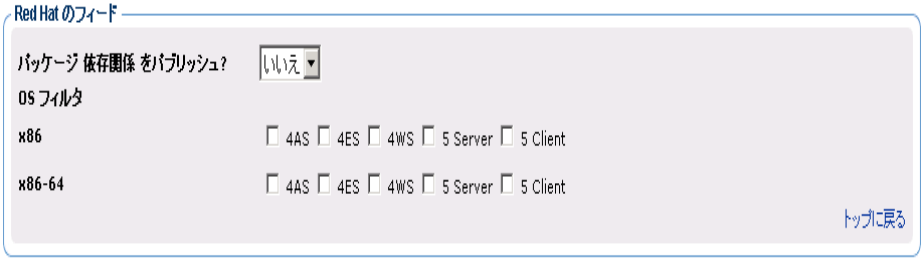
- **OS フィルタ** : x86 (32 ビット Intel) および x86-64 (Opteron/EMT64) アーキテクチャに対して、Red Hat バージョン 4 とリリース AS、ES および WS のすべての組み合わせ、および Red Hat バージョン 5 のサーバーおよびデスクトップ クライアント用リリースのすべての組み合わせがサポートされます。指定されたアーキテクチャの Red Hat パッチの取得については、オペレーティング システムとリリースの組み合わせを選択します。

— **x86** アーキテクチャ : Red Hat x86 アーキテクチャで patch.cfg ファイルに指定できる値は次のとおりです。

```
REDHAT::4as,      REDHAT::4es,      REDHAT::4ws,
REDHAT::5server,   REDHAT::5client
```

— **x86-64** アーキテクチャ: Red Hat x86-64 アーキテクチャで patch.cfg ファイルに指定できる値は次のとおりです。

```
REDHAT::4as-x86_64,      REDHAT::5server-x86_64,
REDHAT::4es-x86_64,      REDHAT::5client-x86_64,
REDHAT::4ws-x86_64
```



SuSE のフィード設定

SuSE Linux のパッチ適用を設定するには、お使いの環境のバージョン レベルと OS プラットフォームの [SuSE のフィード設定] を選択します。SuSE 9 のフィード設定は、SuSE 10 および 11 のフィード設定とは別に入力されます。SuSE 10 および 11 のフィード設定では、[製品タイプ] を [Enterprise Desktop] と [Enterprise Server] から選択します。

関連トピック :

- 359 ページの「SuSE のパッチ管理要件」

SuSE メタ データ フィードの URL を設定または修正する必要もある場合は、[基本] から [詳細] 設定に切り替えます。

SuSE 9 のフィード設定

次に挙げる SuSE 9 のフィード設定のデフォルト URL を表示または変更するには、**[詳細]** をクリックします。

[詳細] だけで表示されるフィールド

- **SuSE 9**: SuSE 9 のセキュリティ アドバイザリのメタ データを取得するためのセキュアな URL を指定します。デフォルトは以下のとおりです。

  https://you.novell.com/update/i386/update/SUSE-CORE/9/
  https://you.novell.com/update/i386/update/SUSE-SLES/9/

- **SuSE 9-x86_64**: AMD64 または Intel EM64T アーキテクチャの SuSE 9 の更新を取得するためのセキュアな URL を指定します。デフォルトは以下のとおりです。

  https://you.novell.com/update/x86_64/update/SUSE-CORE/9/
  https://you.novell.com/update/x86_64/update/SUSE-SLES/9/

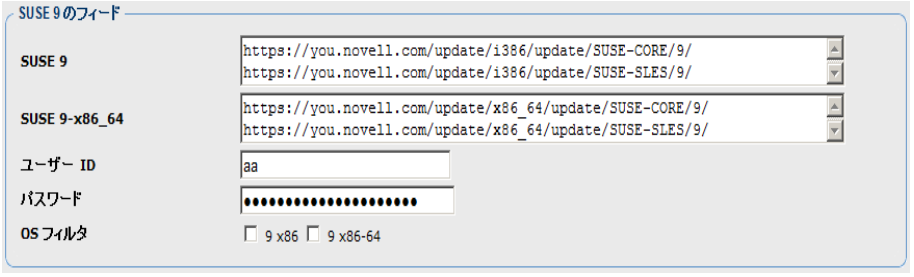
[基本] と [詳細] のフィールド

[基本] または [詳細] ページを使用して、SuSE 9 のデータフィードを取得するために必要な設定を入力します。

- **ユーザー ID**: お使いの SuSE ユーザー ID を指定します。ユーザー ID はベンダーから入手します。
- **パスワード**: SuSE ユーザー ID のパスワードを指定します。
- **OS フィルタ**: SuSE Linux Enterprise Server パッチを取得するオペレーティング システムのバージョンとアーキテクチャの組み合わせを選択します。x86 (32 ビット) アーキテクチャと x86-64 (AMD64 および Intel EM64T) アーキテクチャの SuSE バージョン 9 がサポートされています。

  patch.cfg で有効な x86 アーキテクチャの OS フィルタの値は `suse::9` です。

  patch.cfg で有効な x86-64 アーキテクチャの OS フィルタの値は `suse::9-x86_64` です。



SuSE 10 および 11 のフィード設定

[基本] ビューのフィールドを使用して、SuSE 10 および 11 デバイスのセキュリティ アドバイザリ パッチを取得するために必要なフィード設定を入力します。

次に挙げる SuSE 10 および 11 のフィード設定のデフォルト URL を表示または変更するには、**[詳細]** をクリックします。

[詳細] だけで表示されるフィールド

- **SUSE 10**: x86 アーキテクチャの SUSE 10 (SLES10 と SLED10) についてセキュリティ アドバイザリのメタ データを取得するためのセキュアな URL を指定します。

  デフォルト :
  https://nu.novell.com/repo/\$RCE/SLES10-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-Updates/sled-10-i586/

- **SUSE 10SP1:** x86 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 1 について更新を取得するためのセキュアな URL を指定します。

  デフォルト :
  https://nu.novell.com/repo/\$RCE/SLES10-SP1-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-SP1-Updates/sled-10-i586/

- **SUSE 10SP2:** x86 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 2 について更新を取得するためのセキュアな URL を指定します。

  デフォルト :
  https://nu.novell.com/repo/\$RCE/SLES10-SP2-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-SP2-Updates/sled-10-i586/

- **SUSE 10-x86_64**: x86-64 アーキテクチャの SUSE 10 (SLES10 と SLED10) についてセキュリティ アドバイザリのメタ データを取得するためのセキュアな URL を指定します。

  デフォルト :
  https://nu.novell.com/repo/\$RCE/SLES10-Updates/sles-10-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED10-Updates/sled-10-x86_64/

- **SUSE 10SP1-x86_64:** x86-64 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 1 について更新を取得するためのセキュアな URL を指定します。

デフォルト：
https://nu.novell.com/repo/\$RCE/SLES10-SP1-Updates/sles-10-x86_64
https://nu.novell.com/repo/\$RCE/SLED10-SP1-Updates/sled-10-x86_64/

- **SUSE 10SP2-x86_64:** x86-64 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 2 について更新を取得するためのセキュアな URL を指定します。

  デフォルト：
  https://nu.novell.com/repo/\$RCE/SLES10-SP2-Updates/sles-10-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED10-SP2-Updates/sled-10-x86_64/

- **SUSE 10SP3: x86 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 3 について更新を取得するためのセキュアな URL を指定します。**

  デフォルト：
  https://nu.novell.com/repo/\$RCE/SLES10-SP3-Updates/sles-10-i586/ https://nu.novell.com/repo/\$RCE/SLED10-SP3-Updates/ sled-10-i586/

- **SUSE 10SP3-x86_64: x86-64 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 3 について更新を取得するためのセキュアな URL を指定します。**

  デフォルト：
  https://nu.novell.com/repo/\$RCE/SLES10-SP3-Updates/sles-10-x86_64/ https://nu.novell.com/repo/\$RCE/SLED10-SP3-Updates/ sled-10-x86_64/

- **SUSE 11**: x86 アーキテクチャの SUSE 11 (SLES11 と SLED11) についてセキュリティ アドバイザリのメタ データを取得するためのセキュアな URL を指定します。

  デフォルト：
  https://nu.novell.com/repo/\$RCE/SLES11-Updates/sle-11-i586/
  https://nu.novell.com/repo/\$RCE/SLED11-Updates/sle-11-i586/

- **SUSE 11-x86_64**: x86-64 アーキテクチャの SUSE 11 (SLES11 と SLED11) についてセキュリティ アドバイザリのメタ データを取得するためのセキュアな URL を指定します。

デフォルト：
https://nu.novell.com/repo/\$RCE/SLES11-Updates/sle-11-x86_64/
https://nu.novell.com/repo/\$RCE/SLED11-Updates/sle-11-x86_64/

[基本] と [詳細] のフィールド

[基本] または [詳細] ページを使用して、SuSE 10 および 11 のデータフィードを取得するために必要な次の設定を入力します。SuSE バージョン 10 および 11 は、Enterprise Server と Enterprise Desktop の 2 つの製品タイプをサポートしています。

このページで選択された [製品タイプ] と [OS フィルタ] のすべての組み合わせが、SuSE の取得で使用可能です。取得を実行する前に、[除外] オプションを使用して取得しないすべての組み合わせを除外できます。

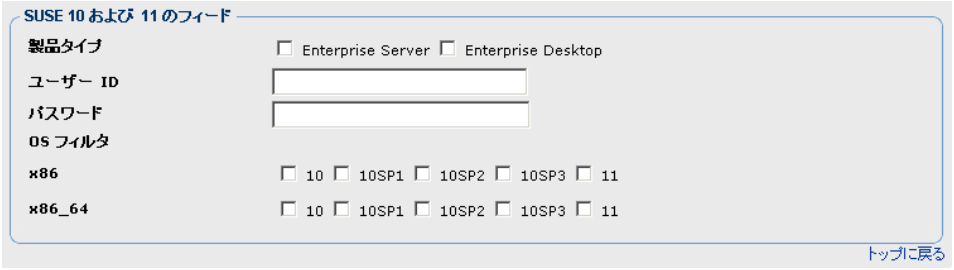
- **製品タイプ**：SUSE 10 または 11 について、お使いの環境のデバイスにインストールされている SUSE Linux 製品タイプを選択します。
  - **Enterprise Server:** SUSE Linux Enterprise Server (SLES) 製品タイプを指定します。SLES 10 または SLES 11 のセキュリティ アドバイザリを取得するには、[製品タイプ] の [Enterprise Server] をオンにします。
  - **Enterprise Desktop:** SUSE Linux Enterprise Desktop (SLED) 製品タイプを指定します。SLED 10 または SLED 11 のセキュリティ アドバイザリを取得するには、[製品タイプ] の [Enterprise Desktop] をオンにします。
- **ユーザー ID**: お使いの SUSE 10 または SUSE 11 のユーザー ID を指定します。ユーザー ID はベンダーから入手します。詳細については、359 ページの「SuSE のパッチ管理要件」を参照してください。
- **パスワード**：SUSE ユーザー ID のパスワードを指定します。
- **OS フィルタ**：SUSE バージョン 10 および 11 パッチを取得するオペレーティング システムのバージョン、*サービス パック*、およびアーキテクチャの組み合わせを選択します。次の OS がサポートされます。
  - x86 (32 ビット) アーキテクチャの SUSE バージョン 10 base、Service Pack 1、2、および 3 と、x86-64 (AMD64 および Intel EM64T) アーキテクチャの SUSE バージョン 10 base、Service Pack 1、2、および 3。
  - x86 (32 ビット) および x86-64 (AMD64 および Intel EM64T) アーキテクチャの SUSE バージョン 11 base。

patch.cfg で有効な x86 アーキテクチャの SUSE 10 OS フィルタの値は `suse::10`、`suse::10SP1`、`suse::10SP2`、および `suse::10SP3` です。

patch.cfg で有効な x86-64 アーキテクチャの SUSE 10 OS フィルタの値は `suse::10-x86_64`、`suse::10SP1-x86_64`、`suse::10SP2-x86_64`、および `suse::10SP3-x86_64` です。

patch.cfg で有効な x86 アーキテクチャの SUSE 11 OS フィルタの値は `suse::11` です。

patch.cfg で有効な x86-64 アーキテクチャの SUSE 11 OS フィルタの値は `suse::11-x86_64.` です。



HP SoftPaq のフィード設定

[HP SoftPaq フィード] セクションでは、次の設定を行います。[HP SoftPaq URL] フィールドを含むすべてのフィールドを表示するには、**[詳細]** をクリックします。[基本] ページに戻るには、**[基本]** をクリックします。

ここで指定した SysID とブリティンの HP SoftPaq を取得するには、`hpsoftpaq` という名前の事前定義されたジョブを使用します。`hpsoftpaq` ジョブと使用可能なジョブのリストは、**[取得を開始]** 操作に表示されます。

[詳細] フィールド

- **HP SoftPaq URL**: HP SoftPaq のデータフィードの URL を指定します。デフォルトは **http://h50203.www2.hp.com/hpapps/onlineDiag/ActiveCheck** です。
- **HP SoftPaq ActiveCheck URL**: HP SoftPaq ActiveCheck のデータフィードの URL を指定します。デフォルトは **http://h50203.www2.hp.com/hpapps/onlineDiag** です。

[基本] と [詳細] のフィールド

- **HP SoftPaq タイプ**: 取得および管理対象とする HP SoftPaq のタイプをオンにします。
  - アプリケーション
  - BIOS
  - ドライバ
  - ファームウェア
- **SysID:** HP SoftPaq に対して取得する SysID を指定します。

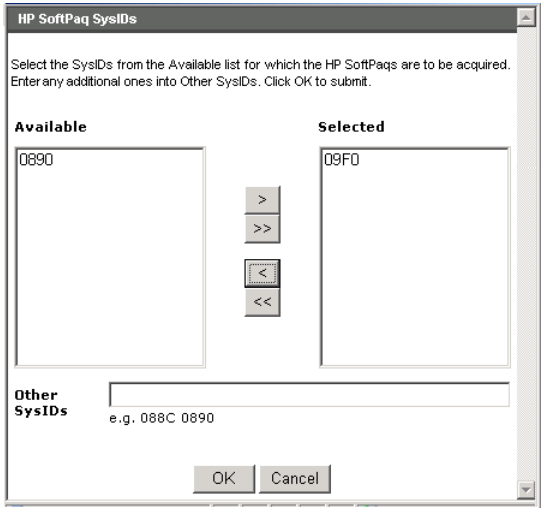
  お使いの HP デバイスで既に HPCA データベースにインベントリ情報がレポーティングされている場合は、[SysID の取得] ボタンを使用してリストからの SysID を選択できます。

  a **[SysID の取得]** ボタンをクリックします。これにより、[HP SoftPaq SysID] ダイアログ ボックスが開きます。[使用可能] カラムに、HPCA にインベントリが登録されている HP デバイスからレポーティングされた HP SoftPaq SysID のリストが表示されます。

  b 個々の SysID を **[使用可能]** カラムから **[選択済み]** カラムに移動するには、矢印ボタンを使用します。[選択済み] カラムの SysID が取得されます。

  c 必要に応じて、**[その他の SysID]** テキスト領域を使用して、[選択済み] カラムにまだリストされていない SysID をスペースで区切って入力できます。たとえば、次のように入力します。
  0890 8844 30A4 300F

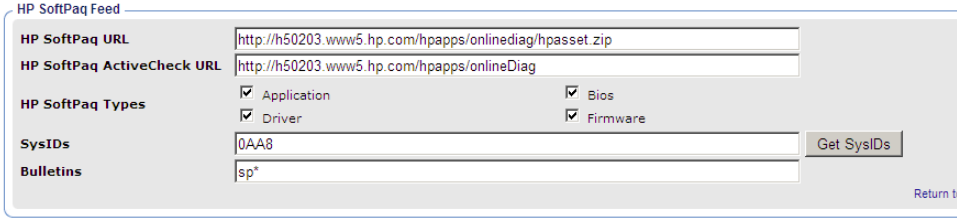
d **[OK]** をクリックすると、HP SoftPaq の [ベンダー] ページに戻ります。



[SysID] リストに、[HP SoftPaq SysID] ダイアログ ボックスで [選択済み] と [その他の SysID] に指定したエントリが表示されます。

- **ブリティン :** HP SoftPaq は、hpsoftpaq という名前の事前定義された取得ジョブを使用して取得されます。hpsoftpaq ジョブの実行時に取得するブリティンを入力するには、[ブリティン] 領域を使用します。SysID のすべてのブリティンを取得するには、次のように入力します。

  SP*



[保存] をクリックして、ベンダーの設定を保存します。

HP SoftPaq を取得するジョブは事前に定義されています。実行するには、**[取得を開始]** 操作内のリストから hpsoftpaq を選択します。

SuSE のパッチ管理要件

このトピックで説明したように、SuSE のフィード設定には、セキュアな (SSL) 接続と、ベンダーから入手したユーザー ID とパスワードが必要です。

SuSE 10 デバイスおよび SuSE 11 デバイスには要件が追加されました。360 ページの「SuSE 10 および SuSE 11 の登録要件」を参照してください。

SSL: Novell Web サイトでは、パッチの取得にセキュアな (SSL) 接続が必要です。Patch Manager 内でセキュアな接続を必要とするのは、Novell Web サイトからセキュアなパッチのダウンロードを実行するために使用するサーバーのみです。このマニュアルを作成している時点で、Novell Web サイトは証明書の検証を要求または実行していません。

SuSE Linux ベンダーのユーザー ID とパスワード : ベンダーのユーザー ID とパスワードを取得するための要件は、SuSE のバージョン番号に応じて異なります。

- **SuSE 9:** SuSE 9 のセキュリティ パッチを取得する場合、SuSE のインターネット リソースにアクセスするために、SuSE Linux ベンダーを介してユーザー ID とパスワードを設定する必要があります。これらの認証情報は、パッチ管理用に SuSE デバイスを設定するときに、コンソールの **[設定] タブ > [パッチ管理] > [ベンダーの設定]** ページで指定します。
- **SuSE 10 および SuSE 11:** SLES10、SLED10、SLES11、SLED11 の SuSE 10 および SuSE 11 セキュリティ パッチを取得する場合、SuSE 10 チャネルまたは SuSE 11 チャネルにアクセスするためには SuSE 10 または SuSE 11 の Linux ベンダーを介してミラー認証情報を設定する必要があります。これらの認証情報は、パッチ管理用に SuSE デバイスを設定するときに、コンソールの **[設定] タブ > [パッチ管理] > [ベンダーの設定]** ページで指定します。

SuSE 10 または SuSE 11 のミラー認証情報を取得するには

1. SuSE 10 製品または SuSE 11 製品の購入時に、SuSE Linux ベンダーを介して Novell Customer Center (NCC) にログインするためのユーザー名とパスワードを設定します。
2. SuSE 10 製品または SuSE 11 製品の購入時にベンダーから指定されたログイン アカウント情報を使用して NCC にログインします。
3. 左側のパネルにある、**[Myproduct]** リンクの下にある **[Mirror Credentials]** をクリックします。

[ミラー認証情報] ページの [認証情報] 領域に、ユーザー名とパスワードが表示されます。[チャネル] 領域に、SuSE 10 チャネルまたは SuSE 11 チャネルの詳細が表示されます。

4 SuSE 10 または SuSE 11 のパッチ取得用のユーザー ID とパスワード認証情報を入力するときは、上の手順で入手したユーザー名とパスワードを使用します。353 ページの「SuSE 10 および 11 のフィード設定」の設定については、「ベンダーの設定」のトピックを参照してください。

SuSE 10 および SuSE 11 の登録要件

SuSE 10 以降、Novell のポリシーとして、セキュリティ パッチと更新を受信するには、各 SuSE Agent オペレーティング システムを Novell に登録し、そのライセンスを Novell Customer Center (NCC) または登録管理ツールで直接管理および検証する必要があることが明示的に表明されています。

HPCA パッチ管理では、Novell のライセンスまたは登録に関するポリシーが、SuSE 10 以上のシステムで満たされているかどうかは検証されません。Novell のポリシーへの準拠と、有効なライセンスによる SuSE 10 および SuSE11 マシンの登録は、お客様の責任において実施してください。

SuSE 10 システムまたは SuSE 11 システムを Novell Customer Center に登録するには

SuSE 10 システムおよび SuSE 11 システムを Novell Customer Center に登録するための詳細については、Novell の Web サイトを参照してください。

このマニュアルを作成している時点で、「Registering and Updating SUSE Linux Enterprise 10」というトピックを以下のサイトで参照できます。

http://www.novell.com/support/dynamickc.do?cmd=show&forward=nonthreadedKC&docType=kc&externalId=3410833&sliceId=1

Linux パッチの再起動要件について

アプリケーション パッチを Linux マシンに適用する場合、再起動は不要です。ただし、カーネル関連の Linux パッチを適用するときは再起動が必要です。現在、HP PatchManager では、カーネルのパッチをインストールした場合の Linux マシンの自動再起動はサポートされていません。カーネルのパッチをインストールしたときは、必ず手動で再起動してください。

取得ジョブ

パッチ取得のスケジュールおよび設定を行うには、[取得ジョブ] セクションを使用します。

[パッチ管理] 取得ジョブを作成して実行するには、コンソールの次の領域を使用します。

- 必要な HTTP および FTP プロキシ設定を入力するには、[設定] タブの [インフラストラクチャ管理] 領域を使用します。
- 取得ジョブを定義するには、[設定] タブの [パッチ管理] 領域にある [取得ジョブ] タスクを使用します。
- ジョブを実行するには、[操作] タブの [パッチ管理] 領域にある [取得を開始] タスクを使用します。

パッチは、1 度に 1 つのベンダーから取得することをお勧めします。また、一部の SuSE セキュリティ アドバイザリおよび Microsoft Office セキュリティ ブリティンは、ダウンロードするために長時間かかる場合があります。

必要な取得ジョブの設定は、お使いの環境に依存します。

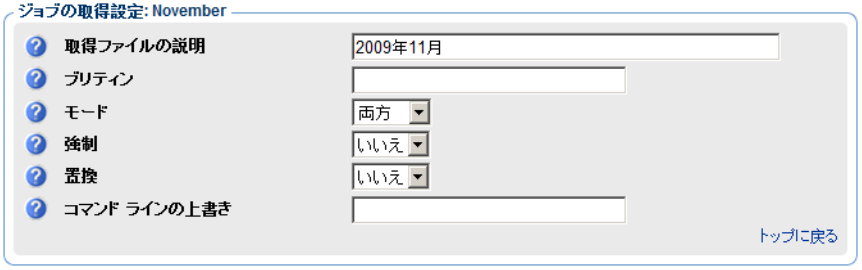
コンソールを使用して取得プロファイルを作成または編集するには

1 [設定] で、**[パッチ管理]**、**[取得ジョブ]** の順にクリックします。

2 編集する既存のファイルを選択するか、**[新規作成]** をクリックして新しいファイルを作成します。ごみ箱アイコンをクリックして取得ファイルを削除します。この例では、**[新規作成]** をクリックします。

3 新しいファイルを作成する場合、[ファイル名] と [説明] に入力して、**[次へ]** をクリックします。

4 手順 2 に進みます。ここで、新しいジョブの [取得の設定] を設定できます。



- **取得ファイルの説明** : 取得ファイルの説明を作成します。
- **ブリティン** : 取得するブリティンをカンマで区切って指定します。アスタリスク (*) のワイルドカード文字は認識されます。Red Hat セキュリティ アドバイザリでは、Red Hat によって発行されたときに Red Hat セキュリティ アドバイザリ番号に含まれるコロン (:) の代わりにハイフン (-) を使用します。

  ブリティンをダウンロードしない場合は、[ブリティン] フィールドに **NONE** と入力してください。

  — Microsoft セキュリティ ブリティンは、命名規則として `MSYY-###` を使用します。ここで、`YY` はブリティンが発行された年の下 2 桁で、`###` は指定した年にリリースされたブリティンのシーケンス番号です。HP によって提供される Microsoft サービス パックのパッチ説明ファイルの命名規則は、`MSSP_operatingsystem_spnumber` です。*サンプル*の Microsoft オペレーティング システムのサービス パックを取得する場合は、MSSP* を指定します。これにより、サンプルのサービス パックが `novadigm` または `custom` フォルダから取得されます。Microsoft アド

バイザリを取得するには、命名規則として MS-KB* を使用して KB の記事を指定します。ここで、* はサポート情報の記事に割り当てられている番号を表します。

— Red Hat セキュリティ アドバイザリは命名規則として RHSA-*CCYY:###* を使用して発行されます。ここで、CC は世紀を示し、YY はアドバイザリが発行された年の下 2 桁、### は Red Hat パッチ番号です。ただし、コロンは製品の予約文字であるため、Red Hat によって発行されたセキュリティ アドバイザリ番号に含まれるコロン (:) の代わりにハイフン (-) を使用する必要があります。変更された命名規則 RHSA-*CCYY-###* を使用して、Patch Manager には、Red Hat セキュリティ アドバイザリを個別に指定してください。

— SuSE セキュリティ パッチ では、次に示すようにバージョン固有の命名規則が使用されています。

カンマを使用して、複数の SuSE パッチ エントリを区切ります (各バージョン共通)。スペースを使用して複数のエントリを区切らないでください。この方法は受け付けられません。

– SuSE 9 では、SUSE-PATCH-#### を使用します。プレフィックス SUSE- の次に SuSE 9 パッチ メタデータ ファイル名が続きます。例 : SUSE-PATCH-1234

– SuSE 10 では、SUSE-PATCH-platformrel-package-#### を使用します。プレフィックス SUSE- の次に SuSE 10 パッチ メタデータ ファイル名が続きます。例 : SUSE-PATCH-SLESP1-MOZILLAFIREFOX-1234

– SuSE 11 では、UPDATEINFO-platformrel-package-#### を使用します。エントリは SuSE 11 パッチ ファイル名 UPDATEINFO*.xml の .xml 拡張子を除いた全体が使用されます。例 : UPDATEINFO-SLESSP0-MOZILLAFIREFOX-1234..

SuSE 11 のファイル名にカンマが含まれている場合、取得するブリティン名を入力するときにカンマをダッシュ (-) に置き換える必要があります。カンマは、複数のブリティンを区切るための予約済み文字です。

すべての SuSE 11 パッチ名は、CSDB の PRIMARY.PATCHMGR ドメインにパブリッシュされるときに自動的に短い一意の名前に再フォーマットされます。詳細については、『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。

- **モード**: パッチとパッチに関する情報をダウンロードする場合は [両方] を指定します。パッチのメタデータのみを取得する場合は、[モデル] を指定します。パッチのブリティンと番号だけがダウンロードされ、実際のパッチファイルはダウンロードされません。このモードを使用すると、管理対象デバイスの脆弱性を公開するレポートを使用できます。
- **強制**: 次の場合に [強制] を使用します。
  - 前回 [モデル] を使用して取得を実行し、今回は [両方] を使用する場合。
  - 前回はある言語をフィルタして取得を実行し、今回は別の言語のブリティンを取得する必要がある場合。
  - 以前に 1 つの製品を指定して取得を実行しており、今回は別の製品に関して取得する必要がある場合。

    たとえば、次のような場合があります。最初は企業内に Windows 2000 コンピュータしか所有していなかったため **`-product {Windows 2000*}`** を使用していました。1 か月後、Windows XP を展開しました。同じブリティンを取得する場合、**`-product {Windows XP*,Windows 2000*}`** と **`-force y`** を使用して取得を実行する必要があります。

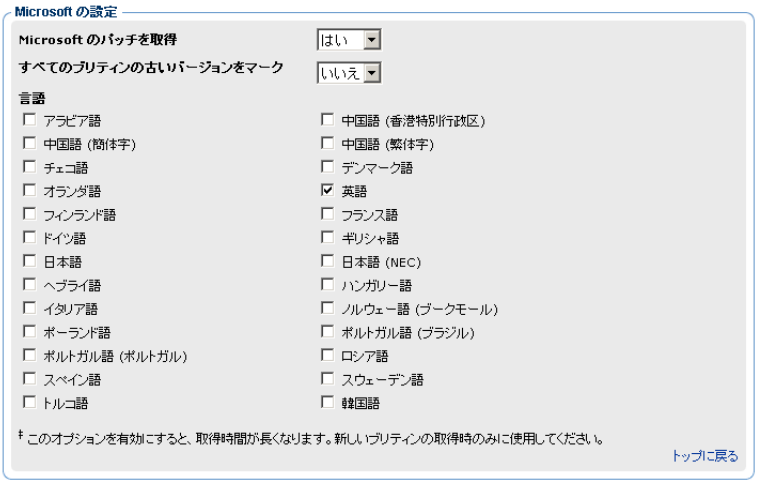
    replace が **`y`** に設定されると、ブリティンは force の値に関係なく削除されてから再取得されます。

- **置換**: **`y`** に設定すると、bulletins パラメータで指定した古いブリティンを削除してから、それらを再度取得します。これは、force の値より優先されます。つまり、[置換] を **`y`** に設定すると、[強制] を [N] と [Y] のどちらに設定しても、取得するように指定されたすべてのブリティンは削除され、再取得されます。
- **コマンド ラインの上書き**: 通常の取得パラメータを上書きする必要がある場合のみ、このパラメータを使用します。正しく使用しないと、取得は失敗します。*`-parameter value`* の形式を使用してください。

Microsoft の設定

- **Microsoft のパッチを取得しますか?**: Microsoft のパッチを取得する場合は **[はい]** を選択します。その他の設定を行う場合は、[ベンダーの設定] ページに移動してください。

  [はい] を選択すると、**[すべてのブリティンに置換をマーク]** オプションと **[言語]** オプションが表示されます。



特定のブリティンを取得して、同時に Configuration Server Database に存在するすべての既存のブリティンを更新する場合、**[すべてのブリティンに置換をマーク]** オプションに対して **[はい]** を選択します。Configuration Server Database 内のブリティンを更新しない場合は **[いいえ]** を選択します。このオプションで **[はい]** を選択すると、毎回すべてのブリティンの取得を実行することなく Configuration Server Database 内のブリティンを更新できます。

置換オプションに対して **[はい]** を選択して、Microsoft Update Catalog (MUC) または Optimized Patch Utility Service (OPUS) データ フィードを使用してすべての新しいブリティンの取得を実行すると、Configuration Server Database と `bulletins.xml` ファイル内のすべての既存の MUC ブリティンが更新されます。同時に、`patch_data` ファイル内のすべての既存の OPUS ブリティンが更新されます。その結果、Configuration Server Database、`bulletins.xml` ファイル、および `patch_data` ファイルは、新しいブリティンに対して選択されたデータ フィードに関係なくすべて変更されます。

ブリティンでは、MUC および OPUS データ フィードに対して置換をマークできます。MSSECURE データ フィードに対しては置換をマークできません。

Satellite コンソールのパッチ管理

メタデータ ベースの配布モデルを使用するように Core Server を設定する場合、脆弱性のパッチを適用するために、管理対象デバイスの Agent によって Satellite Server のバイナリがリクエストされます。

Satellite コンソールの [パッチ管理] リンクを使用して、リクエストされたバイナリをパッチ ゲートウェイを介してインターネットから取得するか、設定済みのアップストリーム サーバーにリクエストを転送するように Satellite Server を設定できます。

パッチ ゲートウェイを無効にすると、Satellite Server によってパッチ バイナリのリクエストがアップストリーム サーバーに転送されます。これは、このオプションのデフォルトの設定です。パッチ ゲートウェイを有効にすると、Satellite Server によってパッチ バイナリがインターネットから直接取得されます。バイナリをより効率的かつ直接的に取得でき、企業のニーズに基づいてバイナリのキャッシュ期間を微調整できるため、ゲートウェイを有効にすることをお勧めします。

インターネットへのアクセスに Proxy Server が必要な場合、Satellite コンソールの [設定] タブにある **[プロキシ設定]** リンクに移動します。Satellite コンソールの [インフラストラクチャ管理] に [プロキシ設定] リンクがないことを除き、Core コンソールの 291 ページの「プロキシ設定」と手順は同じです。このリンクは最上位になります。

Satellite Server でパッチ ゲートウェイを設定するには

1. [設定] タブで、**[パッチ管理]** をクリックします。[パッチ管理] ウィンドウが表示されます。
2. パッチ リクエストをアップストリーム サーバーに転送する場合、**[ゲートウェイの無効化]** を選択します。Satellite Server でインターネットからパッチ バイナリを取得する場合、**[ゲートウェイの有効化]** を選択します。
3. **[ゲートウェイの有効化]** オプションを選択した場合、次のオプションを設定する必要があります。
   - **キャッシュの存続期間 (日)**: 使用されたかどうかに関係なく、パッチ バイナリをキャッシュから削除できるようになるまでの日数を指定します。日数として 0 を指定しないでください。パッチを適用する日数を指定することをお勧めします。
   - **アップストリーム サーバーにフェイルオーバー** : ゲートウェイで Agent リクエスト ファイルをインターネットから取得できない場合にアップストリーム サーバーにフェイルオーバーする場合は、このオプションを有効にします。

4 **[保存]** をクリックして、設定を保存します。

アウトバンド管理

[設定] タブの [アウトバンド (OOB) 管理] 領域を使用して、OOB 管理を設定します。アウトバンド管理の使用方法の詳細については、『HP Client Automation アウトバンド管理ユーザー ガイド』を参照してください。次に示す各セクションで利用可能な設定オプションを説明します。

- 367 ページの「使用可能性」
- 367 ページの「デバイス タイプの選択」
- 369 ページの「vPro システム保護の設定」

使用可能性

vPro または DASH デバイスでサポートされるアウトバンド管理機能を有効または無効にするには、[アウトバンド管理の有効化] 領域を使用します。

- アウトバンド管理機能を有効にするには、**[有効化]** チェックボックスをオンにします。

OOB 管理オプションを表示するには、[操作] タブの「アウトバンド管理」セクションを参照してください。

アウトバンド管理の使用方法の詳細については、『HP Client Automation アウトバンド管理ユーザー ガイド』を参照してください。

デバイス タイプの選択

アウトバンド管理を有効にしたら、[デバイス タイプの選択] 領域を使用して、管理する OOB デバイスのタイプを選択します。

デバイス タイプごとに 3 つの選択肢からいずれかを選択できます。これらの選択肢について、次に示す各セクションで説明します。

- 368 ページの「DASH デバイス」
- 368 ページの「vPro デバイス」
- 368 ページの「両方」

選択したデバイス タイプに応じて、HPCA Console には、選択内容に関連するインターフェイスが表示されます (369 ページの「デバイス タイプの選択によって決まる設定および操作オプション」を参照)。

アウトバンド管理の使用方法の詳細については、『HP Client Automation アウトバンド管理ユーザー ガイド』を参照してください。

DASH デバイス

DASH を選択した場合、DASH 管理者がすべてのデバイスに同じユーザー名とパスワードを設定していれば、DASH デバイスに共通の認証情報を入力することができます。

認証情報の入力を間違えたり、内容に変更があったりした場合は、次回このウィンドウにアクセスしたときに認証情報を変更できます。

vPro デバイス

vPro デバイスを選択した場合、vPro デバイスにアクセスするための SCS ログイン認証情報、および SCS サービスとリモート設定の URL を入力する必要があります。

認証情報の入力を間違えたり、内容に変更があったりした場合は、次回このウィンドウにアクセスしたときに認証情報を変更できます。

両方

両方のタイプのデバイスを選択した場合、DASH デバイスの共通認証情報を入力できます。また、vPro デバイスにアクセスするために必要な SCS ログイン認証情報、および SCS サービスとリモート設定の URL を入力する必要があります。

詳細については、『HPCA アウトバンド管理ユーザー ガイド』の管理タスクでのデバイス タイプの選択に関する章を参照してください。

デバイス タイプの選択によって決まる設定および操作オプション

デバイス タイプを選択したら、[設定] タブと [操作] タブに選択内容を反映したオプションが表示されます。次の表に、オプションの要約を示します。

表 36　　設定と操作のオプション

	DASH	vPro
設定	追加オプションなし	vPro システム保護の設定
オペレーション	デバイス管理	vPro デバイスのプロビジョニング グループ管理 警告の通知

デバイス タイプを選択したり、選択内容を変更したりしたときに、[設定] タブと [操作] タブのナビゲーション パネルにデバイス タイプ関連のオプションを表示するには、HPCA Console からログアウトし、再度ログインする必要があります。

vPro システム保護の設定

vPro デバイスおよびデバイス グループのシステム防御機能を管理するには、[vPro システム保護の設定] を定義する必要があります。

この設定オプションは、vPro デバイス タイプを選択した場合にのみ表示されます。システム防御設定は、DASH デバイスには適用されません。

- **システム防御フィルタの管理**
  vPro デバイスでは、システム防御フィルタを作成、変更、および削除できます。システム防御フィルタにより、ネットワーク上のパケットの流れが監視され、フィルタ条件が一致するとパケットのドロップやパケット レートの制限が可能になります。フィルタは、システム防御ポリシーに割り当てられ、ポリシーを有効化してネットワークを保護することができます。

- **システム防御ポリシーの管理**
  vPro デバイスでは、システム防御ポリシーを作成、変更、および削除し、そのポリシーをネットワーク上の複数の vPro デバイスに配布できます。システム防御ポリシーによって、ネットワークを選択的に分離し、vPro デバイスを悪意のあるソフトウェアの攻撃から保護することができます。
- **システム防御ヒューリスティック情報の管理**
  vPro デバイスでは、ヒューリスティック仕様を作成、変更、および削除して、そのヒューリスティックをネットワーク上の複数の vPro デバイスに配布できます。これらのヒューリスティックにより、ワームの侵入を示す状況が検出され、他のデバイスが感染しないようにそのデバイスが制御されることで、ネットワーク上のデバイスが保護されます。
- **システム防御ウォッチドッグの管理**
  vPro デバイスでは、エージェント ウォッチドッグを作成、変更、および削除して、そのウォッチドッグをネットワーク上の複数の vPro デバイスに配布できます。エージェント ウォッチドッグは、vPro デバイス上のローカル エージェントが存在しているかどうかを監視します。ローカル エージェントの状態に変更があった場合にエージェント ウォッチドッグが取るアクションを指定できます。

  詳細については、『HPCA アウトバンド管理ユーザー ガイド』の管理タスクでの vPro システム防御の設定に関する章を参照してください。

HPCA Console で vPro デバイスのシステム防御機能を管理できるようにするために [設定] タブで実行する管理タスクはこれで終わりです。オペレータまたは管理者ロールのユーザーは、[操作] タブに移動して、ネットワークの OOB デバイスの管理を始めることができます (「オペレーション」の章を参照)。

OS 管理

オペレーティング システムの配布に関連するオプションを設定するには、[オペレーティング システム] 領域を使用します。

- 371 ページの「設定」

OS 管理の詳細については、HPCA リファレンス ライブラリの『OS Manager ガイド』を参照してください。

設定

オペレーティング システム サービスを使用すると、エージェントが HPCA Server に接続し、OS の付与資格およびプロビジョニング情報を取得できます。Core でこのサービスが無効になっている場合、この情報をリクエストする Satellite またはエージェントはこの情報を使用できません。

- オペレーティング システム サービスを有効にするには、**[有効]** ボックスをオンにして **[保存]** をクリックします。

OS 配布中、ネットワーク内のデバイスのブートを計画している場合は、最初に Core と一緒にインストールされた Boot Server (PXE/TFTP) を有効にする必要があります。これにより、Core Server で、Boot Server (PXE) と Boot Server (TFTP) という 2 つの Windows サービスが開始されます。

- Boot Server (PXE/TFTP) を有効にするには、**[Boot Server の有効化]** ボックスをオンにして **[保存]** をクリックします。

HPCA バージョン 7.9 から、HPCA Boot Server (PXE) と DHCP サーバーの両方を同じマシン上でホストできます。

OS 管理の詳細については、HPCA リファレンス ライブラリの『OS Manager ガイド』を参照してください。

利用状況管理

利用状況データベース接続設定と利用状況データ収集設定を設定するには、[利用状況管理] セクションを使用します。

- 372 ページの「データベース設定」
- 373 ページの「設定」

HPCA を使用した利用状況データの収集および分析の詳細については、『Application Usage Manager ユーザー ガイド』を参照してください。

データベース設定

利用状況データベース接続設定は、[データベース設定] ページを使用して設定できます。

利用状況データベース接続設定を設定するには

1 [設定] タブで、**[利用状況管理]**、**[データベース設定]** の順にクリックします。

2 利用状況データの収集を有効にするには、**[有効]** ボックスをオンにして、次の Open Database Connection (ODBC) の情報を指定します。

- **DSN** (データ ソース名)
- **ユーザー ID**
- **パスワード**

これらの設定は Client Automation サーバーのシステム ODBC DSN の設定と一致する必要があります。指定したデータベースがまだ初期化されていない場合、これらの設定を保存するときに初期化されます。

3 **[保存]** をクリックします。

利用状況データの収集を無効にするには、**[有効]** ボックスをオフにします。

設定

利用状況データは、利用状況収集エージェントが配布されたときに収集されます。利用状況の設定は、収集スケジュールの間に既存のクライアント デバイスに適用されます。必要な場合には、プライバシーを確保するため、利用状況データを難読化できます。

難読化は、利用状況収集エージェントを配布する前に有効にしておく必要があります。このエージェントを配布してから有効にすると、レポート データの一部が、難読化された形式や難読化されていない形式で表示されます。

利用状況データを難読化するには

1 ドロップダウン リストを使用して、次のどの利用状況データ情報を非表示にするかを選択します。

- **コンピュータ** - コンピュータ関連の情報を非表示にします。コンピュータ名はランダムな英数字列としてレポートされます。
- **ユーザー** - ユーザー固有の情報を非表示にします。ユーザー名は [AnyUser] としてレポートされます。
- **ドメイン** - ドメイン情報を非表示にします。ドメイン名はランダムな英数字列としてレポートされます。
- **利用状況** - 利用回数および利用時間を非表示にします。実行ファイルの利用時間および起動回数はすべてゼロ値とレポートされます。

利用状況レポート内で難読化する利用状況情報の隣にある **[有効]** を選択します。

2 **[保存]** をクリックして、変更を適用します。

利用状況収集エージェントを配布し、収集スケジュールを指定する方法については、利用状況収集エージェントの配布を参照してください。

ダッシュボード

ダッシュボードを設定するには、次に示す [設定] タブの [ダッシュボード] 領域を使用します。

HPCA 操作ダッシュボードでは、一定期間に発生したクライアント接続数とサービス イベント数に関する情報が提供されます。

脆弱性管理ダッシュボードでは、企業内のクライアント デバイスのセキュリティ脆弱性に関するデータが提供されます。

適用状況管理ダッシュボードでは、企業内の管理対象クライアント デバイスが FDCC などの規制標準にどの程度準拠しているかについての情報が提供されます。

セキュリティ ツール管理ダッシュボードには、企業内の管理対象クライアント デバイスにインストールされているスパイウェア対策、ウイルス対策、およびソフトウェア ファイアウォール製品に関する情報が表示されます。

パッチ管理ダッシュボードでは、企業内のクライアント デバイスのパッチ ポリシー適用状況に関するデータが提供されます。

デフォルトでは、有効になるのはダッシュボード ペインの一部です。管理者権限のあるユーザーは、すべてのペインを有効または無効にできます。

HPCA 操作

HPCA 操作ダッシュボードには、企業内で HPCA が実行中の作業が表示されます。また、2 つの期間のクライアント接続およびサービス イベントの指標が表示されます。エグゼクティブ ビューには、最新の 12 か月が表示されます。[操作] ビューには、最新の 24 時間が表示されます。どちらのビューにも、次の情報ペインが含まれます。

84 ページの「クライアント接続」

86 ページの「サービス イベント」

エグゼクティブ ビューには、次のペインも含まれます。

88 ページの「ドメイン別 12 か月サービス イベント」

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、83 ページの「HPCA 操作ダッシュボード」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 操作ダッシュボードの有効化]** ボックスをオフにし、**[保存]** をクリックします。

3 [HPCA 操作] の下で、**[エグゼクティブ ビュー]** または **[操作ビュー]** をクリックします。

4 ダッシュボードに表示するペイン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。

- 91 ページの「脆弱性の重大度別影響 (円グラフ)」
- 93 ページの「脆弱性履歴の評価」
- 102 ページの「重大度別にした脆弱性の影響 (棒グラフ)」
- 95 ページの「脆弱性の影響」

[操作] ビューには、次の 4 つの情報ペインが含まれます。

- 100 ページの「HP Live Network アナウンスメント」
- 103 ページの「最も脆弱性の高いデバイス」
- 105 ページの「最も脆弱性の高いサブネット」
- 107 ページの「脆弱性のトップ」

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、90 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 **[操作ビュー]** のいずれかをクリックします。

4 ダッシュボードに表示するペイン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 (操作ビュー)**
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。

適用情報管理ダッシュボードには、エグゼクティブ ビューと操作ビューの 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。

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

操作ビューには、次の情報ペインがあります。

- 120 ページの「失敗した SCAP ルールのトップ」
- 121 ページの「失敗回数の多いデバイス (SCAP ルール別)」

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、110 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 **[操作ビュー]** のいずれかをクリックします。

4 ダッシュボードに表示するペイン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 ビューと操作ビューの 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。

- 125 ページの「セキュリティ製品のステータス」
- 127 ページの「セキュリティ製品の概要」

操作ビューには、次の情報ペインがあります。

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

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、124 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 **[操作ビュー]** をクリックします。

4 ダッシュボードに表示するペイン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。

- 133 ページの「ステータス別デバイス適用状況」
- 135 ページの「ブリティン別デバイス適用状況」

操作ビューには、次の情報ペインがあります。

- 137 ページの「HP Live Network Patch Manager アナウンスメント」
- 138 ページの「ステータス別デバイス適用状況」
- 139 ページの「Microsoft セキュリティ ブリティン」
- 140 ページの「最も脆弱性の高い製品」

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、133 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 **[操作ビュー]** のいずれかをクリックします。

4 ダッシュボードに表示するペイン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。

— **[Microsoft セキュリティ ブリティン] (操作ビュー)**

a Microsoft セキュリティ ブリティン RSS フィードの URL を指定します。

通常、有効なデフォルト URL が指定されています。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。

— **HP Live Network Patch Manager アナウンスメント (操作ビュー)**
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。

10 ウィザード

HPCA Console の使用中は、多くのウィザードを使用してさまざまな管理機能を実行します。このセクションでは、各ウィザードの個別の手順について説明します。

ウィザードには、コントロール パネルの複数の領域から起動できるものがあります。

- 381 ページの「グループ作成ウィザード」
- 386 ページの「利用状況収集フィルタ作成ウィザード」
- 387 ページの「Satellite Server 配布ウィザード」
- 388 ページの「Satellite Server 削除ウィザード」
- 389 ページの「サブネット ロケーション作成ウィザード」

ウィザードを実行したり警告を表示したりするときに、HPCA Console が別のブラウザ インスタンスを開くことがあります。これらのウィザードや警告にアクセスするには、ブラウザのポップアップ ブロック設定で [許可されたサイト] にこのコンソールを含める必要があります。

グループ作成ウィザード

データベースにある管理対象デバイスのグループに、ソフトウェアまたはパッチを配布する必要があります。グループ作成ウィザードを使用して、指定したデバイス、探索したデバイス、またはレポート クエリの一部として返されたデバイスに基づき、デバイス グループを定義します。

グループ作成ウィザードの手順は、作成するグループのタイプにより異なります。

スタティック グループを作成するには

1 ウィザードを起動するには、次のいずれかを実行します。

— [グループ管理] の [全般] タブから、**[新しいスタティック グループの作成]** をクリックします。

— [グループ] タブから、**[新しいスタティック グループの作成]** ツールバー ボタン  をクリックします。

2 **[次へ]** をクリックして、グループの作成を開始します。

3 グループの名前および説明を入力します。

4 **[次へ]** をクリックします。

5 グループに含めたいデバイスを選択するには、該当する各デバイスの最初のカラムのボックスをチェックします。必要な場合、デバイスのリストの範囲を絞り込むには、[検索] 機能を使用できます。

6 **[次へ]** をクリックします。

7 要約情報を確認します。選択したデバイスの数が、**[デバイス数]** 要約と一致することを確認します。グループを変更する必要がある場合、**[前へ]** をクリックします。

8 **[作成]** をクリックします。グループが正常に作成されました。

9 **[閉じる]** をクリックして、ウィザードを終了します。

ダイナミック ディスカバリ グループを作成するには

探索グループ メンバーシップは、LDAP クエリまたはドメイン スキャンの間に発見されたデバイスをベースにしています。

1 ウィザードを起動するには

— [グループ管理] の [全般] タブから、**[新しいディスカバリ グループの作成]** をクリックします。

— [グループ] タブから、**新しいグループの作成**  ツールバー ボタンをクリックし、**[新しいダイナミック ディスカバリ グループの作成]** を選択します。

2 **[次へ]** をクリックして、グループの作成を開始します。

3 グループの名前および説明を入力します。

4 **[次へ]** をクリックします。

5 探索ソースを選択します。

— **LDAP/Active Directory** — LDAP ホストおよびポート番号、ユーザー ID、パスワード (必要な場合)、およびクエリする DN を入力します。

また、クエリに適用する、範囲、詳細フィルタ、またはデバイスの制限を選択します。

— **ドメイン** — インポートするデバイスのネットワーク ドメインをスキャンするには、ドメイン名 (たとえば、ABC ドメインの完全ドメイン スキャンには ABC と入力) またはドメイン名の一部とワイルドカード文字 (ABC* とすると、ABC で始まるドメインから全デバイスが返されます) を入力します。ドメインの特定のデバイスを含めるには、「ドメイン \ デバイス」という構文を使用します。たとえば、`Sales\WS*` は、`Sales` ドメインの `WS` で始まるデバイスのみを返します。
ドメインの特定のデバイスを除外するには、感嘆符 (!) を使用します。たとえば、`Sales,!Sales\WS*` は、`WS` で始まるデバイスを除く、Sales ドメインの全デバイスを返します。

6 **[次へ]** をクリックします。

7 ダイナミック グループのリフレッシュ スケジュールを設定します。

— **実行 :** 時間、日、週など、一定の間隔でダイナミック グループ メンバーシップを更新するかどうかを選択します。

— **間隔 :** 具体的な間隔 (時間、日、または週) を選択します。

— **開始日 :** ドロップダウン リストを使用して、グループがリフレッシュするデータを選択します。

— **[現在のサーバー時刻]** は、HPCAS Server の現在の時刻を表示します。

8 **[次へ]** をクリックします。

9 要約情報を確認し、**[作成]** をクリックします。

10 **[閉じる]** をクリックして、ウィザードを終了します。

探索グループは、LDAP クエリまたはドメイン スキャンの間に発見されたデバイスを含むように作成されます。発見されたデバイスがすでに HPCAS の一部でなかった場合、自動的にデバイス リストに追加されます。このグループのデバイス メンバーシップは、設定したリフレッシュ スケジュールに基づいて更新されます。

ダイナミック レポート グループを作成するには

レポート グループは、レポート クエリで返されたデバイスを使用して、作成されます。

1 [レポート] 領域のアクション バーからウィザードを起動するには、**[新しいダイナミック レポート グループの作成]**  をクリックします。

2 **[次へ]** をクリックして、ウィザードを開始します。

3 グループの名前および説明を入力します。

4 **[次へ]** をクリックします。

5 ダイナミック グループのリフレッシュ スケジュールを設定します。

- **実行 :** 時間、日、週など、一定の間隔でダイナミック グループ メンバーシップを更新するかどうかを選択します。
- **間隔 :** 具体的な間隔 (時間、日、または週) を選択します。
- **開始日 :** ドロップダウン リストを使用して、グループがリフレッシュするデータを選択します。
- **[現在のサーバー時刻]** は、HPCAS Server の現在の時刻を表示します。

6 **[次へ]** をクリックします。

7 要約情報を確認し、**[作成]** をクリックします。

8 レポート クエリの現在のデバイスを含む、レポート グループが作成されます。このグループのデバイス メンバーシップは、設定したリフレッシュ スケジュールに基づいて更新されます。

9 **[閉じる]** をクリックして、ウィザードを終了します。

サービス インポート ウィザード

サービス インポート ウィザードを使用して、HPCA Server の ServiceDecks ディレクトリからソフトウェア、パッチ、OS ライブラリにサービスをインポートします。デフォルトでは、このディレクトリは次の場所にあります。

InstallDir\Data\ServiceDecks

サービス インポート ウィザードを使用してサービスをインポートするには

1 [操作] タブで、次のいずれかのページから **[サービスのインポート]**  ツールバー ボタンをクリックします。

- [ソフトウェア管理] > [ソフトウェア ライブラリ]
- パッチ管理 > [パッチ] タブ
- OS 管理 > [オペレーティング システム] タブ

これにより、ウィザードが起動します。

2 インポートするサービスを選択します。HPCA Server の ServiceDecks ディレクトリにあり、次の単語が含まれるすべてのサービス デッキが、使用可能なサービスのリストに表示されます。

ライブラリ	サービス デッキ名に含まれる単語	HPCA ドメイン
ソフトウェア	SOFTWARE	SOFTWARE
パッチ	PATCH	PATCHMGR
OS	OS	OS

デフォルトでは、ServiceDecks ディレクトリは次の場所にあります。

InstallDir\Data\ServiceDecks

各サービスのファイル名の 4 番目の部分に、そのソフトウェア サービス、パッチ、または OS のわかりやすい名前が含まれています。たとえば、Orca ソフトウェア アプリケーション用のサービス デッキは次のような名前になります。

PRIMARY.SOFTWARE.ZSERVICE.ORCA

3 要約情報を確認し、**[インポート]** をクリックします。サービスがインポートされ、該当する (ソフトウェア、パッチ、OS) HPCA ライブラリで使用可能になります。

4 **[閉じる]** をクリックして、ウィザードを終了します。

サービス エクスポート ウィザード

サービス エクスポート ウィザードを使用して、HPCA ソフトウェア、パッチ、または OS ライブラリから、HPCA Server マシンの ServiceDecks ディレクトリにサービスをエクスポートします。

サービス エクスポート ウィザードを使用してサービスをエクスポートするには

1 [操作] タブで、次のいずれかのページから **[サービスのエクスポート]**  ツールバー ボタンをクリックします。

— [ソフトウェア管理] > [ソフトウェア ライブラリ]

— パッチ管理 > [パッチ] タブ

— OS 管理 > [オペレーティング システム] タブ

これにより、ウィザードが起動します。

2 エクスポートするサービスを選択します。

3 要約情報を確認し、**[エクスポート]** をクリックします。サービスが HPCA Server の ServiceDecks ディレクトリにエクスポートされます。デフォルトでは、このディレクトリは次の場所にあります。

InstallDir\Data\ServiceDecks

サービス デッキには複数のファイルが含まれていて、そのすべてに同じファイル名のプレフィックスが付いています。たとえば、Orca ソフトウェア アプリケーション用のサービス デッキ名は次のようになります。

PRIMARY.SOFTWARE.ZSERVICE.ORCA

サービス デッキの各ファイル名の 4 番目の部分に、エクスポートされたソフトウェア、パッチ、または OS のわかりやすい名前が含まれています。

4 **[閉じる]** をクリックして、ウィザードを終了します。

利用状況収集フィルタ作成ウィザード

利用状況収集フィルタ作成ウィザードを使用して、新しい利用状況収集フィルタを作成します。

新しい収集フィルタを作成するには

1 [利用状況] タブで **[新しいフィルタの作成]**  ツールバー ボタンをクリックします。ウィザードが開きます。

2 フィルタ パラメータを設定するには、各テキスト ボックスにフィルタ条件を入力します。

利用状況データのフィルタを適用するフィールドにのみ値を入力します。空のテキスト ボックスは無視され、フィルタ条件として使用されません。

入力した値が、ソフトウェアの実行可能ファイルのファイル ヘッダーと比較され、収集された利用状況データがフィルタ条件に合致するか判断されます。

特定のソフトウェアにフィルタを適用する方法を決めるには、373 ページの「ダッシュボード」を参照してください。

> 50 を超えるアプリケーションについてデータを収集し、報告するようにフィルタを設定すると、大量のデータが収集され、結果的にレポートのパフォーマンスに重大な問題が生じる可能性があります。

3 **[作成]** をクリックします。

4 **[閉じる]** をクリックします。

新しいフィルタが、収集フィルタ リストに追加されます。

Satellite Server 配布ウィザード

Satellite Server 配布ウィザードを使用して Satellite Server をインストールし、データ キャッシングなどのリモート サービスを有効にできます。

Satellite Server を配布するには

1 [設定] タブで [Satellite 管理] 領域の [インフラストラクチャ管理] に進みます。

2 **[サーバー]** タブをクリックします。

3 Satellite Server のリストでデバイスを 1 つ以上選択します。

4 **[Satellite Server の配布]**  ツールバー ボタンをクリックして、ウィザードを起動します。

5 配布に使用する **[ユーザー ID]** と **[パスワード]** を入力して **[次へ]** をクリックします。

6 **インストール ドライブデータ ドライブ**と**配布モード**を選択します。

HPCA Enterprise Edition の場合、次の 3 つのモードのいずれかを選択できます。

— **簡素** (標準) モード。Satellite からデータ キャッシング サービスのみが Client Automation Agent に提供されます。

— **フル** サービス モード。Satellite から設定サービス、データ キャッシング サービスおよび OS 設定サービスが Client Automation Agent に提供されます。

— **カスタム** モード。Satellite で有効にする特定のサービスを選択できます。

配布モードの詳細については、『HPCA Core および Satellite 入門およびコンセプト ガイド』の「Satellite 配布モデル」を参照してください。

7 **[次へ]** をクリックします。

8 配布ジョブの実行スケジュールを指定します。**[実行 : 今すぐ]** を選択して Satellite Server をすぐに配布するか、**[実行 : 後で]** を選択して配布の日付と時刻をスケジュール設定します。

9 **[次へ]** をクリックします。

10 要約情報を確認し、**[サブミット]** をクリックします。

Satellite Server 配布ジョブが作成されます。

Satellite Server ダウンロード ファイルは、サイズが大きいファイルです。ネットワーク トラフィック量が多い場合、配布に時間がかかる場合があります。ジョブのステータスは [管理] タブ の [ジョブ 領域で確認できます。

11 **[閉じる]** をクリックして、ウィザードを終了します。

Satellite Server 削除ウィザード

Satellite Server 削除ウィザードを使用して、HPCA Satellite Server グループから 1 つ以上の Satellite Server をアンインストールします。

Satellite Server をアンインストールするには

1 [設定] タブで [Satellite 管理] 領域の [インフラストラクチャ管理] に進みます。

2 **[サーバー]** タブをクリックします。

3 Satellite Server のリストでデバイスを 1 つ以上選択します。

4 **[インフラストラクチャ サービスの削除]** ツールバー ボタンをクリックします。

5 **[実行 : 今すぐ]** を選択してウィザードが完了した直後に Satellite Server をアンインストールするか、**[実行 : 後で]** を選択してアンインストールする日付と時刻を入力します。

6 **[次へ]** をクリックします。

7 要約情報を確認し、**[サブミット]** をクリックします。

Satellite Server 削除ジョブが作成されます。ジョブのステータスは [管理] タブ の [ジョブ 領域で確認できます。

8 **[閉じる]** をクリックして、ウィザードを終了します。

サブネット ロケーション作成ウィザード

サブネット ロケーション作成ウィザードを使用して、Satellite Server を割り当てることができる新しいサブネット ロケーションを追加します。

新しいサブネット ロケーションを追加するには

1 [設定] タブで [Satellite 管理] 領域の [インフラストラクチャ管理] に進みます。

2 **[サブネット ロケーション]** タブをクリックします。

3 明示的にサブネット アドレス (複数も可) を指定して新しいサブネット ロケーションを作成するには、次の手順に従います。

a **[新しいサブネット ロケーションの作成]** ツールバー ボタンをクリックします。

サブネット ロケーション作成ウィザードが開きます。

b サブネット ロケーションの説明を入力します。

c このサブネット ロケーションの一部として含めるサブネット アドレスを指定します。複数のサブネット アドレスはカンマで区切ります。

どのサブネット アドレスを使用すればよいかわからない場合、サブネット アドレス計算機を使用してください。

d **[作成]** をクリックします。

既存のインベントリ データに基づいてサブネット ロケーションを自動的に作成するには、次の手順に従います。

a **[サブネットのロケーションの自動作成 (インベントリ データに基づき)]**  ツールバー ボタンをクリックします。

b **[OK]** をクリックします。

c **[閉じる]** をクリックして結果ダイアログ ボックスを閉じます。

4 **[閉じる]** をクリックして、サブネット ロケーション作成ウィザードを終了します。

この時点でサブネット ロケーションは作成されますが、検証はされておらず、Satellite Server にマップされてはいません。詳細については、328 ページの「Satellite Server へのサブネット ロケーションの割り当て」を参照してください。

11 メタデータを使用したパッチ管理

HPCA では、パッチの更新を取得して Agent デバイスに配信するための軽量モデルが採用されています。このモデルではメタデータのみを使用してエージェントのパッチ スキャンを行うため、メタデータを使用したパッチ管理と呼ばれています。

この章では、メタデータを使用したパッチ管理を活用するために必要な概念、設定、および実装の詳細について説明します。

メタデータを使用したパッチ管理は、次の環境でのみ実行できます。

- Microsoft Update Catalog データ フィードを使用する Microsoft オペレーティング システム
- HPCA Core および Satellite の Enterprise レベルと Standard レベルの環境

トピックには次の内容が含まれます。

- 391 ページの「概要」
- 395 ページの「パッチ管理のメタデータ配布設定 (Miscrosoft のみ)」
- 398 ページの「Core での Patch Agent の設定」

注意 : メタデータ配布を使用するには、Download Manager を有効にする必要があります。

- 402 ページの「パッチに対するエージェントの付与」
- 403 ページの「パッチ取得および Core パッチ ゲートウェイ オペレーション」

概要

現在、メタデータを使用したパッチ管理の軽量モデルは、Microsoft デバイスのパッチ適用に使用でき、それには Microsoft Update Catalog フィードを使用する必要があります。

このモデルには、393 ページの図 47 で示すように次のような利点があります。

メタデータ パッチ管理モデルは、次の点で従来の HPCA パッチ適用モデルと異なります。

1 Core Server の Configuration Server Database (CSDB) には、実際のパッチ バイナリではなく、ブリティンのメタデータ情報のみが格納されます。

このモデルではパッチ取得の実行速度が向上し、またエージェントのパッチ探索および HPCA Server の同期では、インフラストラクチャ トラフィックの負荷も軽減されます。

2 実際のパッチ バイナリは、Core Server と Satellite Server の両方のコンポーネントであるパッチ ゲートウェイにダウンロードおよびキャッシュされます。ゲートウェイでは、エージェント マシンから最初のリクエストを受信するとパッチ バイナリがダウンロードされ、他のエージェント マシンが使用できるようにキャッシュされます。また、必要に応じて、パッチ ゲートウェイでは、ユーザーが取得を実行するときにパッチ バイナリを事前に読み込めます。

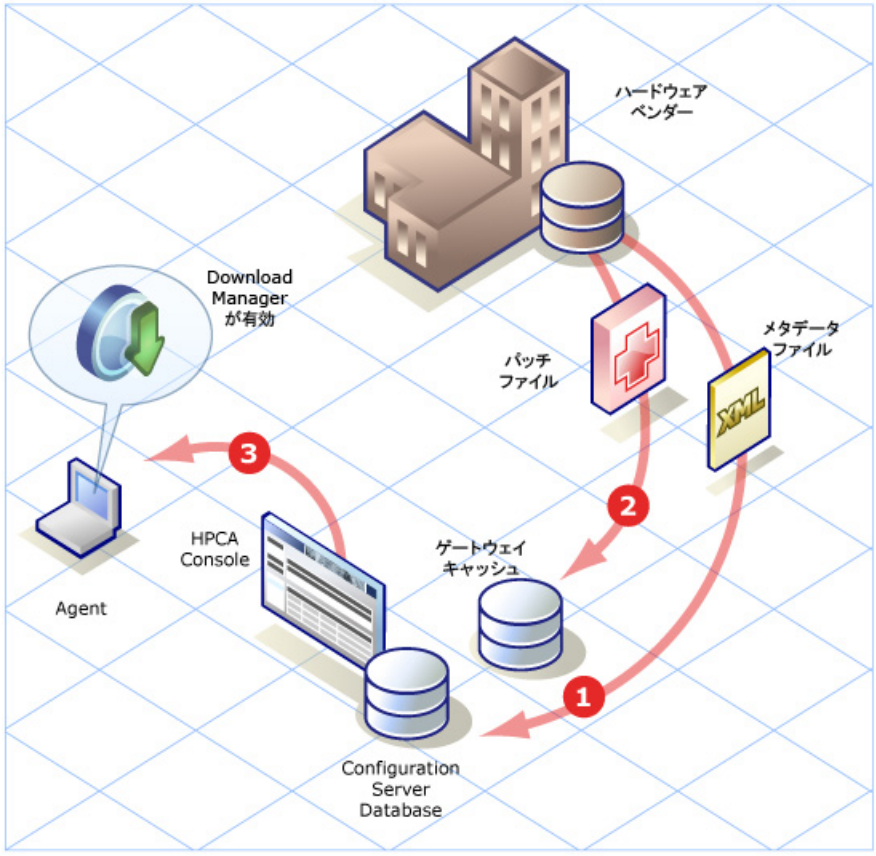
3 メタデータ モデルを使用する場合、スキャン フェーズの最後に、適用可能なパッチ バイナリのリクエストによってパッチ ゲートウェイに接続できるようにするためには、エージェントの Download Manager が有効になっている必要があります。

Download Manager では、エージェントへのパッチ ファイルの受動転送が処理されます。ファイルの転送が完了すると、パッチをインストールするためにエージェント接続が起動されます。

393 ページの図 47 に、メタデータを使用したパッチ管理モデルを示します。

比較のために、394 ページの図 48 には従来のパッチ管理モデルを示します。

図 47　　メタデータを使用したパッチ管理モデル



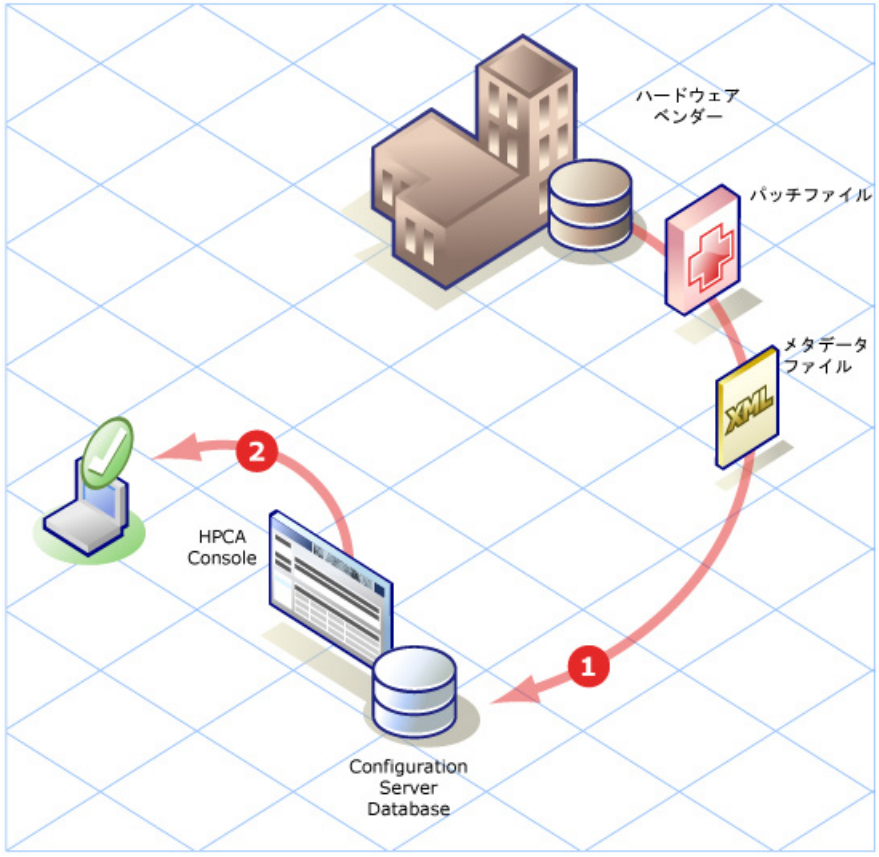
凡例 :

1　パッチ取得により、パッチのメタデータ ファイルのみがベンダーからダウンロードされます。パッチ メタデータは Core CSDB にパブリッシュされ、管理対象エージェントからリクエストされるパッチ ファイルの正確なリストを検出するために使用されます。

2　エージェントからの (または任意で選択できる事前読み込みでの) リクエスト、パッチ ゲートウェイがベンダーからパッチ ファイルをダウンロードし、他のエージェントが使用できるようにキャッシュします。パッチ ファイルを CSDB にパブリッシュする必要はありません。

3　Patch Agent では Download Manager を有効にする必要があります。Download Manager では、エージェントへの必要なパッチ ファイルの受動ダウンロードがバックグラウンド プロセスで処理されます。

図 48　　パッチ管理モデル - 従来



凡例 :

1　従来のパッチ取得では、ブリティンのメタデータとすべての関連パッチ ファイルがベンダーからダウンロードされます。これらのファイルは、企業内のエージェントに必要かどうかは関係なく、すべて Core CSDB にパブリッシュされます。

2　Patch Agent では、Download Manager オプションを使用しても使用しなくてもパッチを適用できます。使用しない場合は、エージェント接続によって、必要なパッチ ファイルのダウンロードがフォアグラウンド プロセスで処理されます。一方、Download Manager では、エージェントへの必要なパッチ ファイルの受動ダウンロードがバックグラウンド プロセスで処理されます。

関連トピック：

次のトピックでは、企業内でメタデータ配布およびパッチ管理用パッチ ゲートウェイを活用する方法について説明します。

- 395 ページの「パッチ管理のメタデータ配布設定 (Miscrosoft のみ)」
- 396 ページの「パッチ ゲートウェイの設定」
- 398 ページの「Core での Patch Agent の設定」
  - 398 ページの「エージェントのゲートウェイ アクセス設定」
  - 399 ページの「オフライン スキャンのエージェント設定」
  - 400 ページの「エージェントの Download Manager の設定」
- 402 ページの「パッチに対するエージェントの付与」
- 403 ページの「パッチ取得および Core パッチ ゲートウェイ オペレーション」

パッチ管理のメタデータ配布設定 (Miscrosoft のみ)

メタデータ配布はデフォルトで有効になっています。次の手順で説明されているように、Core コンソールの [設定] タブで有効にすることもできます。このリリースでは、メタデータ配布は Microsoft デバイスのみで使用でき、Microsoft Update Catalog (MUC) フィードが必要です。

1 Core コンソールで **[設定]** タブをクリックし、**[パッチ管理]** グループを開いて **[配布設定]** をクリックします。

[パッチ配布設定] ページが開き、[パッチ メタデータのダウンロード] 領域と [パッチ ゲートウェイ オペレーション] 領域が表示されます。

2 **[パッチ メタデータのダウンロード]** 領域で次のオプションを選択します。

パッチ メタデータのみのダウンロードを有効化

注意 : メタデータ配布 Microsoft を有効にすると、Patch Manager は MICROSOFT ではなく MSFT というベンダー フィードの使用に切り替わります。

パッチ ゲートウェイの設定

ゲートウェイは Patch Manager Server のコンポーネントで、エージェントにリクエストされるパッチ バイナリ データをダウンロードし、キャッシュします。これは、Core Server または Satellite Server のいずれか、または両方 (Core が Satellite のフェイルオーバー サーバーとして機能する場合) で有効にできます。Core Server のパッチ ゲートウェイには、Satellite Server にはないオプションがあります。詳細については、237 ページの「オペレーション」を参照してください。

Core での有効化

Core Server でパッチ ゲートウェイを有効にするには

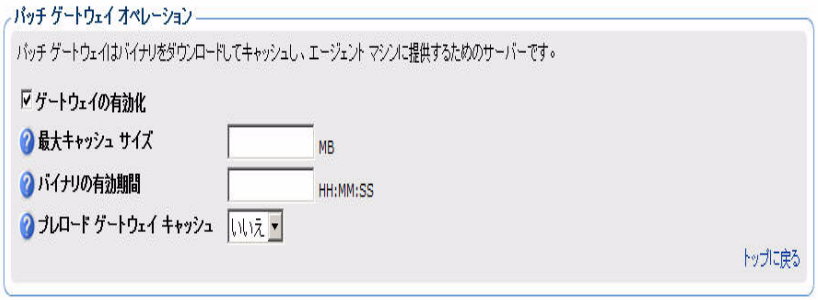
[パッチ ゲートウェイ オペレーション] 領域を使用して、Patch Manager ゲートウェイの有効化と設定を行います。次を指定します。

1 **[ゲートウェイの有効化]** チェック ボックスをオンにします。メタデータ配布の場合は必ずこれをオンにします。

ゲートウェイを有効にすると、設定する追加フィールドが表示されます。

2 **[最大キャッシュ サイズ]** をメガバイト単位で指定します。キャッシュ サイズを制限しない場合は空白のままにします。

3 **[バイナリの有効期間]** の最大値を「時 : 分 : 秒」(HH:MM:SS) の形式で指定します。エージェントからリクエストされたバイナリがこれより古い場合、ゲートウェイは、そのバイナリを提供する前に新しいバージョンがないか確認します。



4 必要に応じて、取得の実行時にパッチ バイナリをゲートウェイにキャッシュするには、**[事前読み込みゲートウェイ キャッシュ]** オプションを **[はい]** に設定します。ただし、このオプションを使用する際には注意してください。

事前読み込みのメリットは、エージェントが特定のパッチ バイナリを初めてリクエストするとき、ゲートウェイによるダウンロードを待つ必要がない点です。

事前読み込みのデメリットは、*エージェントで必要とされているかどうかに関係なく*、収集に関連するすべてのパッチ バイナリがゲートウェイによってダウンロードされる点です。

5 Agent から最初のリクエストを受信するとゲートウェイでパッチ バイナリのダウンロードとキャッシュが行われるようにするには (オンデマンド ダウンロード)、**[事前読み込みゲートウェイ]** オプションを **[いいえ]** のままにします。

[保存] をクリックして、設定を保存します。

Satellite での有効化

Satellite Server でパッチ ゲートウェイを有効にするには

1 Satellite コンソールで、[設定] タブを選択して **[パッチ管理]** をクリックします。このオプションにより、パッチ ゲートウェイを有効または無効にできます。

パッチ ゲートウェイを無効にすると、Satellite Server によってパッチ バイナリのリクエストがアップストリーム サーバーに転送されます。これは、このオプションのデフォルトの設定です。

パッチ ゲートウェイを有効にすると、Satellite Server によってパッチ バイナリがインターネットから直接取得されます。バイナリを取得する場合、この方法をお勧めします。366 ページの「Satellite コンソールのパッチ管理」を参照してください。

2 パッチ ゲートウェイを有効にする場合、追加オプションを設定する必要があります。366 ページの「Satellite コンソールのパッチ管理」を参照してください。

3 [保存] をクリックして、設定を保存します。

取得ジョブの有効化

[設定] タブの [パッチ管理] 領域の **[取得ジョブ]** パネルで、ブリティンを取得するためのジョブを定義します。このタスクは、メタデータ配布を使用してもしなくても同じです。

サービス アクセス プロファイル

Core Server および Satellite Server がサービス アクセス プロファイル (SAP) で定義されていることを確認します。詳細については、37 ページの「クライアント操作プロファイルの設定」を参照してください。

メタデータを使用したパッチ管理およびゲートウェイの場合、P のロールを含む Core および Satellite サーバーに対して SAP エントリを検証するには、HPCA Administrator CSDB Editor を使用します。これらの SAP エントリは通常、あるタイプの DATA によって作成されます。

P ロールは、パッチ バイナリのエージェント リクエストを Patch Manager ゲートウェイに渡します。

これで、サーバー側のメタデータ配布のパッチ ゲートウェイ設定が完了します。

Core での Patch Agent の設定

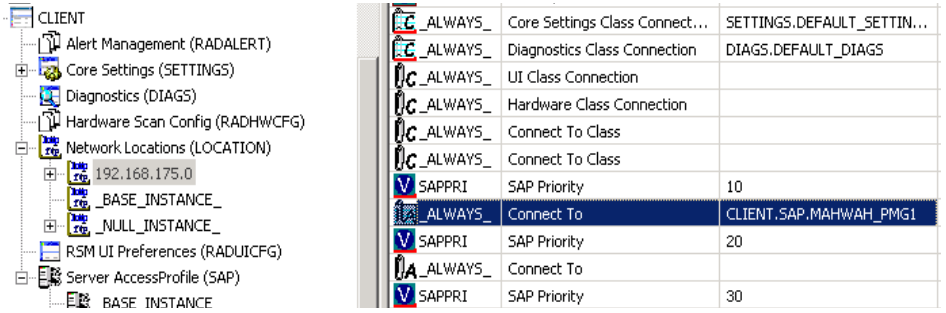
次の手順で、クライアント操作プロファイル (COP) を使用して Patch Manager ゲートウェイにアクセスできるように Patch Agent を設定し、パッチ バイナリのサイレント 事前読み込みを有効にします。これらの手順については次に説明します。

エージェントのゲートウェイ アクセス設定

Patch Manager ゲートウェイ サーバーにアクセスするために、クライアント操作プロファイル (COP) および適切な Patch Manager ゲートウェイ対応サーバーを使用するように Patch Manager Agent を設定します。

1. 最初に、COP を使用するようにエージェントを設定します。COP は、コンピュータ単位またはサブネット単位など、さまざまな形式に設定できます。COP の使用方法の詳細については、『HPCA Application Manager および Self-Service Manager ユーザー ガイド』、または『HPCA Configuration Server Database リファレンス ガイド』の「Client Domain」の章を参照してください。
2. エージェント マシンの COP を設定したら、データ配信の SAP エントリ (TYPE が DATA) に P のロールが含まれており、適切な PRIMARY.CLIENT.LOCATION インスタンスに関連付けられていることを確認します。

次の設定例では、データ配信の SAP インスタンスに PRIMARY.CLIENT.SAP.MAHWAH_PMG1 という名前が付けられ、ネットワーク サブネットの PRIMARY.CLIENT.LOCATION に関連付けられています。お使いの環境では、設定が異なる可能性があります。



3 COP=Y を含むようにエージェント接続パラメータを変更します。詳細については、『HPCA Application Manager および Application Self-Service Manager ユーザー ガイド』を参照してください。

これで、MSFT フィードを使用したメタデータ配布と COP を使用した Patch Manager ゲートウェイのセットアップが完了します。

オフライン スキャンのエージェント設定

メタデータ取得モデルでパッチを管理する場合、MSFT ベンダーの取得ファイルがエージェントにダウンロードされると、ネットワーク、あるいは HPCA Core Server または Satellite Server への接続に依存せずに、スキャン フェーズが開始されます。

スキャン フェーズが終了すると、適用状況に従うために各エージェントに必要なパッチ バイナリのリストが利用可能になります。

エージェントによって Download Manager が起動され、ネットワーク接続が確立されるとバイナリ ファイルの事前読み込みが開始します。

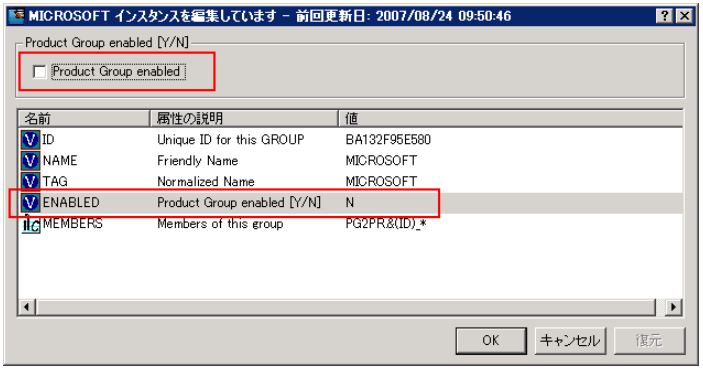
オフライン スキャン要件

バージョン 7.50 のエージェントには、パッチのオフライン スキャン機能が組み込まれており、次の条件下で自動的に有効になります。メタデータを使用したパッチ管理を使用する場合は、これらのオフライン スキャン条件を満たしていることを確認してください。

- [パッチ管理] > [配布設定] で **[パッチ メタデータのダウンロード]** を有効にします。
- [パッチ管理] > [エージェント オプション] で **[Download Manager]** を有効にします。詳細については、400 ページの「エージェントの Download Manager の設定」を参照してください。
- Core の Configuration Server Database で次のエントリが無効になっている必要があります。
  - PRIMARY.PATCHMGR.PROGROUP クラスの MICROSOFT インスタンスが無効になっている必要があります。この設定については、次で説明します。

PATCHMGR.PROGROUP クラスの MICROSOFT インスタンスを無効にするには

1. Core Server で、HPCA Administrator CSDB Editor にログインします。
2. PRIMARY.PATCHMGR.PROGROUP クラスの MICROSOFT インスタンスに移動します。
3. 次の図に示すように、チェック マークを編集および削除して Product Group Enabled 属性を N に設定します。



エージェントでオフライン スキャンを実行できるようにするためには、必ずこの Enabled 属性を N に設定してください。

エージェントの Download Manager の設定

メタデータ配布では、エージェントは、スキャン フェーズの最後にパッチ ゲートウェイからダウンロードするバイナリ ファイル セットをリクエストします。

Download Manager を使用できるように Patch Agent を設定する必要があります。Download Manager はバックグラウンドでサイレントに動作し、非同期プロセスとしてエージェントにパッチ ファイルをダウンロードします。Download Manager ではこの受動ファイル転送を必要に応じて停止および開始でき、停止した時点からダウンロードを続行します。

Patch Agent で Download Manager を有効にすると、エージェントへのバイナリのダウンロード方法を制御する複数のオプションを設定できます。Download Manager のオプションには、通常モードおよびスクリーン セーバー モードでのネットワーク利用、初期化後の遅延、およびダウンロード完了後のパッチ更新の適用があります。

Download Manager オプションはデフォルトで無効になっています。オプションを有効にするには、コンソールの **[設定]** タブ > **[パッチ管理]** 領域 > **[エージェント オプション]** ページを使用します。詳細については次に説明します。

コンソールで Download Manager を有効にし、オプションを保存すると、CSDB Database の Patch Manager の DISCOVER インスタンスが変更され、選択内容が反映されます。

Download Manager を使用できるように Patch Agent を設定するには

Download Manager を有効にし、関連オプションを設定するには、コンソールの [設定] タブ > [パッチ管理] 領域 > [エージェント オプション] ページを使用します。

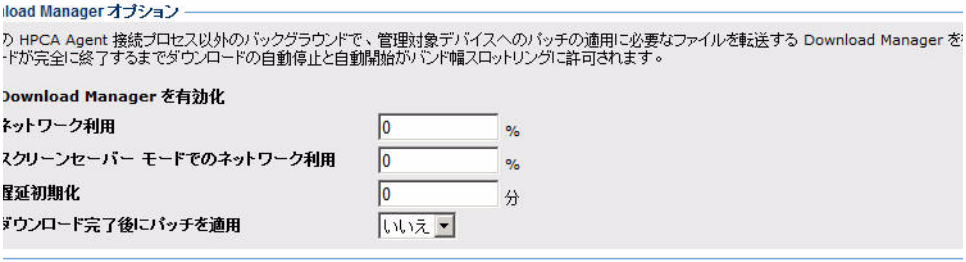
パッチのメタデータ配布を使用して Microsoft デバイスにパッチを適用するには、Download Manager を有効にする必要があります。

1. コンソールの **[設定]** タブで **[パッチ管理]** および **[エージェント オプション]** をクリックします。
2. [エージェント オプション] ページで、[Download Manager オプション] 領域に移動します。
3. **[Download Manager を有効化]** チェック ボックスをオンにします。

   オンにすると、Download Manager オプションが表示されます。
4. Download Manager オプションを設定します。ネットワーク利用、スクリーン セーバー モードでのネットワーク利用、初期化後の遅延、およびダウンロード完了後のパッチ適用の有無を指定するオプションを設定します。

   これらのオプションの設定の詳細については、337 ページの「エージェント オプション」を参照してください。

例 : 次のエントリは、デバイス動作中は最大 34% のネットワーク利用率、スクリーン セーバー モードでは最大 45% のネットワーク利用率、および初期化後遅延が 45 秒で、Patch Agent の Download Manager を有効にします。パッチ ファイルがダウンロードされると、次回の Patch Agent 接続時に適用が可能になります。



5 オプションとして、[エージェント オプション] 領域で次のエージェント オプションを設定できます。

— 自動更新を無効化

— ソフトウェア配布フォルダの削除

これらのオプションの設定の詳細については、337 ページの「エージェント オプション」を参照してください。

注意 : Patch Agent のオプションを保存すると、Configuration Server Database ですべての方法 (作成、削除、検証、更新、修復) の Patch Manager の DISCOVER インスタンスが変更されます。

6 **[保存]** をクリックして、変更を保存します。

パッチに対するエージェントの付与

標準のパッチ展開手順を使用して、適切なパッチに対する付与資格をエージェントに設定します。詳細については、管理に関する章のトピックを参照してください。

Patch Agent では、適用可能なパッチ ファイルの非同期転送を行う Download Manager のバックグラウンド プロセスを利用して、適用可能なバイナリがパッチ ゲートウェイを経由してダウンロードされます。

ゲートウェイは、リクエストされたパッチ ファイルを取得すると、他のエージェントが使用できるようにそれらをキャッシュします。

パッチ取得および Core パッチ ゲートウェイ オペレーション

メタデータを使用したパッチ取得は軽量であるため、つまり、CSDB にはパッチ情報のみダウンロードおよびパブリッシュされるため、平均すると数分で終了します。

1 収集を実行するには、[操作] タブの [パッチ管理] 領域を使用します。

コンソールの [操作] タブをクリックして、[パッチ管理] グループに移動します。**[取得を開始]** を選択します。

取得後、CSDB には実際のパッチ バイナリ データではなく、パッチのメタデータ情報のみが含まれます。

2 必要に応じて、取得のステータスを表示できます。

コンソールの [操作] タブをクリックします。[パッチ管理] グループを展開し、**[取得ステータスをレポート]** をクリックします。

3 標準のパッチ展開手順を使用して、適切なパッチに対する付与資格をエージェントに設定します。

Patch Agent はパッチ ゲートウェイを経由して適用可能なバイナリをダウンロードします。ゲートウェイは、他のクライアントが使用できるようにバイナリをキャッシュします。

4 ゲートウェイでファイルがダウンロードおよびキャッシュされると、使用可能なパッチ URL が [キャッシュ ファイルの統計値] ページに表示されます。

コンソールからこのページにアクセスするには、[操作] をクリックし、[Patch Manager]、[ゲートウェイ操作]、**[キャッシュ ファイルの統計値]** の順に選択します。

12 OS イメージの準備とキャプチャ

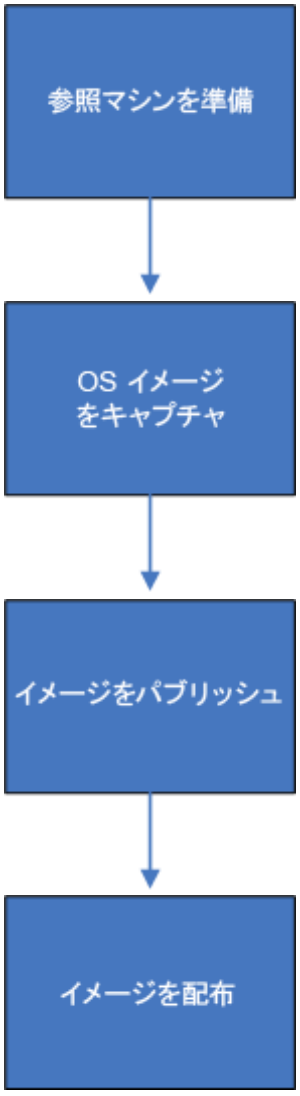
この章は、次のトピックで構成されています。

OS イメージのキャプチャを試みる*前*に Windows Automated Installation Kit (AIK) が HPCA Core Server にインストールされていることを確認します。

詳細については、『HPCA Core および Satellite 入門およびコンセプト ガイド』の「HPCA を使用して Windows オペレーティング システムを管理する」を参照してください。

プロセスの概要

HPCA では、オペレーティング システムの管理プロセスに次の 4 つの手順があります。



参照マシンは、使用環境の管理対象デバイスに配布できる「ゴールド」OS イメージの作成に使用するシステムです。

412 ページの「参照マシンの準備」を参照してください。

HPCA では、対話型の OS の Image Capture ツールを用意しています。このツールでは、参照マシン上の OS イメージを簡単にキャプチャできます。

415 ページの「OS イメージのキャプチャ」を参照してください。

OS イメージをキャプチャしたら、HPCA データベースにそのイメージをパブリッシュする必要があります。HPCA では、イメージのパブリッシュに役立つ対話型の Publisher ツールを用意しています。

439 ページの「オペレーティング システム イメージのパブリッシュ」を参照してください。

次に、HPCA Console を使用して、使用環境にある管理対象のクライアント デバイスのグループにオペレーティング システムのイメージを配布できます。

203 ページの「オペレーティング システムの管理」

この章では、OS イメージの準備およびキャプチャに焦点を当てています。パブリッシュおよび配布については、この概要で示した章で説明します。

紹介

この章では、使用環境で、次のオペレーティング システムのイメージを準備またはキャプチャし、管理対象の クライアント デバイスに配布する方法について説明します。

- Windows 7
- Windows Server 2008 R2 (x64)
- Windows Vista
- Windows Server 2008

古いオペレーティング システムのイメージをキャプチャするには、571 ページの「Windows XP および Windows Server 2003 の OS イメージのキャプチャ」を参照してください。

既存の OS WIM イメージ (これには、Microsoft Windows OS インストール メディアにある OS `.WIM` ファイルが含まれる) を使用しているか、または Microsoft Windows Automated Installation Kit (AIK) で OS WIM イメージを作成する場合は、イメージを準備またはキャプチャする必要はないため、次の章に進んでください。

デスクトップ OS イメージの準備とキャプチャ

このセクションの情報は、デスクトップ、ラップトップ、ノートブック、ネットブック、およびワークステーションのクライアント デバイスに関するものです。シン クライアント デバイスについては、418 ページの「シン クライアント OS イメージの準備とキャプチャ」を参照してください。

前提条件

HPCA OS Image Capture ツールで OS イメージのキャプチャを試行する前に、Microsoft Windows Automated Installation Kit (AIK) が HPCA Core Server にインストールされていることを確認します。

- HPCA Core Server のインストール*前*に Windows AIK をインストールした場合、必要な操作はありません。
- HPCA Core のインストール*後*に Windows AIK をインストールした場合、HPCA Core を再起動する必要があります。

Windows AIK は Microsoft ダウンロード センター (`http://www.microsoft.com/downloads`) からダウンロードして入手できます。通常の Windows インストールには含まれていません。

使用しているオペレーティング システムに適したバージョンが次のデフォルトの場所にインストールされていることを確認してください。

```
C:\Program Files\Windows AIK
```

詳細については、『HPCA Core および Satellite 入門およびコンセプト ガイド』を参照してください。

Microsoft .NET Framework バージョン 2.0 (またはそれ以降) が参照マシンにインストールされていることを確認します。.NET Framework は、次の Microsoft ダウンロード センターから入手できます。

http://www.microsoft.com/downloads

どのバージョンの .NET Framework が参照マシンに存在しているのかを確認するには、次のディレクトリのフォルダを表示します。

```
%SYSTEMROOT%/Microsoft.NET/Framework
```

配布方法

OS Manager を使用してイメージを配布する方法には、次の 2 つがあります。

- **ImageX** を使用して、Windows PE や ImageX ユーティリティで配布される `.WIM` フォーマットでイメージをキャプチャします。
- **Windows セットアップ** を使用して、Windows PE や Windows セットアップで配布される `.WIM` フォーマットでイメージをキャプチャします。

Windows セットアップでは、インストールをより適切に制御できます。ImageX では、単純なファイル抽出と同様の操作で実行できます。いずれかの方法でキャプチャしたイメージを使用して、無人インストールまたはアップグレードを実行できます。

Windows セットアップ配布メソッドを使用してイメージを正常にキャプチャするには、参照マシンの OS パーティションに十分な空きディスク領域がある必要があります。たとえば、7 GB のイメージをキャプチャするには、50 ～ 60 GB の空きディスク領域が必要です。

表 37 では、それぞれの配布方法の概要を説明します。実行する OS イメージを準備またはキャプチャする手順は、オペレーティング システムと選択する配布方法によって若干異なります。

表 37　　配布方法

メソッド	Service OS タイプ *	作成したファイル **	サポートされているプラットフォーム
Microsoft ImageX	WinPE	`ImageName.WIM` `ImageName.EDM`	Windows XP SP2 (またはそれ以降) Professional x86 または x64 Windows Vista Enterprise Edition、Business Edition および Ultimate Edition x86 または x64 Windows 7 Windows Server 2008 Standard Edition および Business Edition x86 または x64 Windows 2003 Server SP1 および Advanced Server x86 または x64 Windows Server 2008 Release 2 (R2) x64
Microsoft Windows セットアップ	WinPE	`ImageName.WIM` `ImageName.EDM`	Windows Vista Business Edition および Ultimate Edition x86 Windows 7 Windows Server 2008 Standard Edition および Business Edition x86 Windows Server 2008 Release 2 (R2) x64

*SOS 内のターゲット デバイスに対して互換性があるドライバを使用する必要があります。Windows PE を使用しており、ドライバが提供されていない場合、597 ページの「カスタム Windows PE Service OS のビルド」を参照してください。Linux SOS を使用している場合、HP から Linux SOS の更新プログラムが定期的に提供されます。

** 作成したファイルは、イメージがキャプチャされた後 HPCA server の次のディレクトリに格納されます。

InstallDir\Data\OSManagerServer\upload

ImageX 配布および Windows セットアップ配布の詳細については、Microsoft のドキュメントを参照してください。

OS Image Capture ツールについて

HPCA OS Image Capture ツールは、次のタスクを実行します。

1. 参照マシンに関する情報 (ハードウェア機能と OS 機能についての情報) を収集して格納します。
2. 必要に応じて、使用可能な終了ポイントを実行します。Image Preparation Wizard で、イメージを封印する SysPrep が起動される前に PRE.CMD が実行されます。Sysprep によってイメージが封印された後、POST.CMD が実行されます。詳細については、573 ページの「Image Preparation Wizard の終了ポイント」を参照してください。

   Image Capture の終了ポイントは、ImageX および Windows セットアップのキャプチャ タイプの場合にのみサポートされます。
3. Microsoft Sysprep を実行します。
4. 参照マシンを (適切なメディアから起動された) Service OS で再起動します。実行した Service OS でイメージと関連ファイルが収集されます。
5. ファイルを作成し、HPCA server の次のディレクトリにコピーします。

   InstallDir\Data\OSManagerServer\upload

   アップロードされるファイルは、次のとおりです。

   - ImageName.WIM
     このファイルには参照マシンの一連のファイルとファイル システムが含まれています。
   - ImageName.EDM
     このファイルにはインベントリ情報を含むオブジェクトが含まれています。

OS Image Capture ツールでは、Microsoft .NET Framework バージョン 2.0 (またはそれ以降) が必要になります。これは、次の Microsoft ダウンロード センターから入手できます。

http://www.microsoft.com/downloads

どのバージョンの .NET Framework が参照マシンに存在しているのかを確認するには、次のディレクトリのフォルダを表示します。

```
%SYSTEMROOT%/Microsoft.NET/Framework
```

参照マシンの準備

参照マシンの準備プロセスは、キャプチャするオペレーティング システムによって若干異なります。詳細な手順については、次のトピックを参照してください。

- 412 ページの「Windows 7 または Windows Server 2008 R2 x64」
- 414 ページの「Windows Vista または Windows Server 2008」

Windows 7 または Windows Server 2008 R2 x64

単一パーティションまたはデュアル パーティションいずれかの OS セットアップからキャプチャできます。デュアル パーティションの OS セットアップの場合、システム予約パーティションにはブート マネージャと HPCA Service OS (SOS) のファイルが格納されます。OS パーティションには Boot Loader および OS 自体が格納されます。

1. オリジナル製品メディアから、オペレーティング システムをインストールします。参照マシンは、インストール対象のオペレーティング システムを実行できる必要があります。参照マシンが DHCP を使用していることを確認します。
   - インストールの種類の指定を求められたら、**[カスタム (高度)]** オプションを選択します。
   - Windows 7 をインストールする場所の指定を求められたら、**[ドライブ オプション (高度)]** を選択します。
2. **[新規作成]** をクリックして、Windows 7 を格納する新しいパーティションを作成します。
3. **[サイズ]** ボックスで、最大値を選択します。
4. **[適用]** をクリックします。ダイアログ ボックスが開き、Windows が追加パーティションを作成する場合があることを警告します。**[OK]** をクリックして、ダイアログ ボックスを閉じ、操作を続行します。
5. **単一パーティション** インストールを作成するには、次の手順を実行します。
   a. 小さいシステム予約パーティションを選択し、**[削除]** をクリックします。ダイアログ ボックスが開き、このパーティションに格納されているすべてのデータが失われることを警告します。
   b. **[OK]** をクリックして、ダイアログ ボックスを閉じて、操作を続行します。
   c. 残りのパーティションを選択して、**[次へ]** をクリックします。その後、Windows 7 のインストールを続行します。

   デュアル パーティション インストールを作成するには、次の手順を実行します。

a 手順 4 で作成されたパーティションを選択し、**[削除]** をクリックします。ダイアログ ボックスが開き、このパーティションを削除すると、パーティションに格納されているすべてのデータが失われることを警告します。

b **[OK]** をクリックして、ダイアログ ボックスを閉じて、操作を続行します。

c システム予約パーティションを選択し、**[拡張]** をクリックします。

d **[サイズ]** ボックスで、1,024 MB を指定します。

e **[適用]** をクリックします。再度、ダイアログ ボックスが開き、パーティションの拡張は元に戻せない操作であることを警告します。

f **[OK]** をクリックして、ダイアログ ボックスを閉じ、操作を続行します。

g 手順 4 で作成されたパーティションを再度選択し、**[新規作成]** をクリックします。

h **[サイズ]** ボックスで、最大値を選択します。

i **[適用]** をクリックします。再度、ダイアログ ボックスが開き、Windows が追加パーティションを作成する場合があることを警告します。

j **[OK]** をクリックして、ダイアログ ボックスを閉じ、操作を続行します。

k **[次へ]** をクリックします。その後、Windows 7 のインストールを続行します。

6 コンピュータの場所の選択を求められた場合は、**[作業ネットワーク]** を選択します。

7 必要に応じて OS をカスタマイズします。これには、基本的なまたは必要な複数のアプリケーションのインストールが含まれる場合があります。OS とアプリケーションの最新のサービス パック、およびイメージの配布先となるデバイスに必要なドライバが含まれることを確認してください。

参照マシンへの HPCA Agent のインストールは推奨されません。HPCA Agent は、OS が配布されるときにインストール (インストール済みである場合はアップグレード) されます。

8 HPCA Server へのアップロード プロセスが終了するまで、キーボードやマウスによる操作が数分間行われなくても、デバイスの電源が切れないように、BIOS の電源管理を設定してください。

9 [コントロール パネル] で、ユーザー アクセス制御のレベルを **[通知しない]** に設定します。

10 .WIM ファイルのサイズを抑えるために、ファイル システムのサイズをできるだけ小さくします。

> Windows セットアップ配布メソッドを使用してイメージを正常にキャプチャするには、参照マシンの OS パーティションに十分な空きディスク領域がある必要があります。たとえば、7 GB のイメージをキャプチャするには、50 ～ 60 GB の空きディスク領域が必要です。

a ファイル システムから、必須ではないファイルとディレクトリを削除します。

b システムの復元を無効にします。

11 Windows 7 および Windows Server 2008 R2 x64 のキャプチャ プロセスの一部として、システムがローカル ディスクから再起動する場合、キャプチャ モードで起動するようにシステムが設定されます。CD またはネットワークに Image Capture メディアを保持する必要はありません。

Windows Vista または Windows Server 2008

1 オリジナル製品メディアから、オペレーティング システムをインストールします。参照マシンは、インストールするオペレーティング システムを実行できる必要があります。参照マシンが DHCP を使用していることを確認します。

> OS は C: ドライブに格納してください。C: ドライブ以外はキャプチャされません。

必要に応じて OS をカスタマイズします。これには、基本的なまたは必要な複数のアプリケーションのインストールが含まれる場合があります。OS とアプリケーションの最新のサービス パック、およびイメージの配布先となるデバイスに必要なドライバが含まれることを確認してください。

> 参照マシンへの HPCA Agent のインストールは推奨されません。HPCA Agent は、OS が配布されるときにインストール (インストール済みである場合はアップグレード) されます。

2 HPCA Server へのアップロード プロセスが終了するまで、キーボードやマウスによる操作が数分間行われなくても、デバイスの電源が切れないように、BIOS の電源管理を設定してください。

3 User Access Control を無効にします。

4 .WIM ファイルのサイズを抑えるために、ファイル システムのサイズをできるだけ小さくします。

Windows 7 より前の Windows オペレーティング システムの場合、プライマリ ブート ドライブのプライマリ ブート パーティションへのイメージの配布がサポートされます。

Windows セットアップ配布メソッドを使用してイメージを正常にキャプチャするには、参照マシンの OS パーティションに十分な空きディスク領域がある必要があります。たとえば、7 GB のイメージをキャプチャするには、50 ～ 60 GB の空きディスク領域が必要です。

a ファイル システムから、必須ではないファイルとディレクトリを削除します。

b システムの復元を無効にします。

5 Vista および Windows Server 2008 のキャプチャ プロセスの一部として、システムがローカル ディスクから再起動する場合、キャプチャ モードで起動するようにシステムが設定されます。CD/DVD またはネットワーク上に ImageCapture メディアを保持する必要はありません。

OS イメージのキャプチャ

OS Image Capture ツールで参照マシンのイメージをキャプチャし、HPCA Server にイメージをアップロードできます。その後、そのイメージをパブリッシュして、使用環境の管理対象デバイスに配布できます。

Image Capture ツールは、次のオペレーティング システムで使用できます。

- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2 (64 ビット)

OS Image Capture ツールでは、Windows Preinstallation Environment (Windows PE) ベースのキャプチャのみをサポートしています。シン クライアント キャプチャを実行するには、418 ページの「シン クライアント OS イメージの準備とキャプチャ」を参照してください。古い OS イメージをキャプチャするには、571 ページの「Windows XP および Windows Server 2003 の OS イメージのキャプチャ」を参照してください。

OS Image Capture ツールにアクセスするには

1 管理者権限のあるアカウントを使用して参照マシンにログオンします。

2 ImageCapture メディアの CD を参照マシンに挿入します。

このメディアを入手する場所についての詳細は、『HPCA OS Manager システム管理者ガイド』の「製品メディア」を参照してください。

3 ImageCapture CD で、次のフォルダを参照します。

```
image_preparation_wizard\win32
```

4 `oscapture.exe` を実行します。

OS Image Capture ツールが開きます。[ようこそ] ページに参照マシンのハードウェアおよびオペレーティング システムについての情報が表示されます。

> 参照マシンのオペレーティング システムが前述のオペレーティング システムより古い場合は、代わりに、HPCA Image Preparation Wizard が開きます。詳細については、571 ページの「Windows XP および Windows Server 2003 の OS イメージのキャプチャ」を参照してください。

5 **[次へ]** をクリックして続行します。[イメージ オプション] ページが開きます。

イメージ オプション

[イメージ オプション] ページでは、次の情報を指定します。

- **[イメージ メソッド]** - ImageX または Windows セットアップを選択します。
  - ImageX では Windows PE や ImageX ユーティリティで配布される `.WIM` フォーマットでイメージをキャプチャします。
  - Windows セットアップでは、Windows PE や Windows セットアップで配布される `.WIM` フォーマットでイメージをキャプチャします。

  Windows セットアップでは、インストールをより適切に制御できます。ImageX では、単純なファイル抽出と同様の操作で実行できます。いずれかの方法でキャプチャしたイメージを使用して、無人インストールまたはアップグレードを実行できます。

  ImageX および Windows セットアップについての詳細は、**http://technet.microsoft.com** で入手できる Windows ドキュメントを参照してください。
- **[イメージ名]** - このイメージ用に選択する名前。HPCA Server にアップロードされ、このイメージの配布に使用するファイルがこの名前を使用します。

イメージ名に入力できる文字数は、半角で 8 文字までです。大文字と小文字は区別されません。

- **[イメージの説明]** - ユーザーが提供する説明情報。イメージをパブリッシュするときに、HPCA Server で使用可能なオペレーティング システム イメージの一覧にこの情報が表示されます。

  イメージの説明に入力できる文字数は、半角で 80 文字までです。

- **[移行先サーバー]** - キャプチャ後のこのイメージのアップロード先の HPCA Server のホスト名または IP アドレス。

  Image Capture ツールでは、キャプチャ後イメージをアップロードできるようにするために、HPCA Server への接続を試行します。接続できない場合は、エラー メッセージが表示されます。参照マシンのシステム プロキシ設定およびファイアウォール設定でサーバーと通信できることを確認します。

- **[ポート]** - 前述の項目で指定した HPCA Server がリスンするポート番号。デフォルト ポートは 3466 です。

[次へ] をクリックして、[要約] ページに進みます。

要約

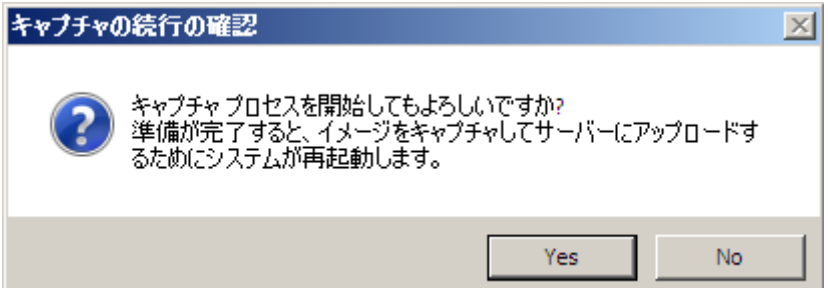
[要約] ページには、指定した名前、イメージの推定サイズなどキャプチャ対象のイメージに関する情報が表示されます。

このキャプチャで指定したパラメータのいずれかを変更するには、**[戻る]** ボタンをクリックして、[イメージ オプション] ページに戻ります。

イメージをキャプチャして指定の HPCA Server にアップロードするには、**[キャプチャ]** をクリックします。

次の処理が実行されます。

1 次のダイアログ ボックスが表示されます。



2 マシンの準備や再起動をしたり、イメージをキャプチャしたりするには、**[はい]** をクリックします。

このキャプチャには 15 ～ 20 分かかります。処理時間はイメージのサイズによって異なります。キャプチャ中は、Service OS の画面にステータス情報が表示されます。詳細については、430 ページの「Windows PE Service OS 画面について」を参照してください。

3 イメージのキャプチャ後、OS Image Capture ツールがネットワークに接続されて HPCA Server の次のディレクトリにそのイメージが格納されます。

```
InstallDir\Data\OSManagerServer\upload
```

4 アップロード プロセスが完了すると、マシンを再起動するかどうかを確認されます。

次に、イメージを HPCA データベースにパブリッシュします。HPCA Console のオンライン ヘルプの「パブリッシュ」を参照してください。

シン クライアント OS イメージの準備とキャプチャ

次の各セクションでは、サポートされているシン クライアント オペレーティング システムのイメージを準備しキャプチャする方法を説明します。

- 418 ページの「Windows XPe イメージおよび WES OS イメージ」
- 422 ページの「Windows CE OS イメージ」
- 425 ページの「Embedded Linux OS イメージ」

Windows XPe イメージおよび WES OS イメージ

次のセクションでは、Windows XPe および Windows Embedded Standard (WES) シン クライアント オペレーティング システムのイメージを準備してキャプチャする方法を説明します。

- 419 ページの「Windows XPe または WES 参照マシンの準備」

- 419 ページの「Image Preparation Wizard の実行」

XPe または WES シン クライアント デバイスのイメージをキャプチャし、その後、キャプチャしたイメージを容量の大きなフラッシュ ドライブを持つ XPe または WES シン クライアント デバイスに配布できます。これは、リリース ノートのドキュメントに記述されているような一定の制限に従う必要があります。

タスク 1: Windows XPe または WES 参照マシンの準備

イメージのキャプチャのため Windows XPe または WES シン クライアントを準備するには、次のものが必要です。

- HPCA メディア
- XP Embedded Feature Pack 2007 メディア
- イメージ準備 CD-ROM

Windows XPe または WES イメージをキャプチャする前に、次の操作を行う必要があります。

1. Windows XPe または WES に管理者としてログインします。
2. XP Embedded Feature Pack 2007 メディアから、`etprep.exe` を `C:\Windows` にコピーします。
3. XP Embedded Feature Pack 2007 メディアから、`fbreseal.exe` を `C:\Windows\fba` にコピーします。
4. イメージをキャプチャする前に、HPCA Agent を Windows XPe または WES デバイスにインストールする必要があります。詳細については、131 ページの「HP シン クライアントでの HPCA Agent のインストール」または、『HPCA Application Manager および Application Self-Service Manager ユーザー ガイド』を参照してください。

タスク 2: Image Preparation Wizard の実行

Image Preparation Wizard は以下のタスクを実行します。

1. マシンに十分な空きディスク領域があるかどうかをチェックし、HPCA agent がインストールされていることを確認します。十分な空きディスク領域がない場合、Image Preparation Wizard はメッセージを表示して終了します。
2. 参照マシンに関する情報 (ハードウェアおよび BIOS の機能など) を含むオブジェクトを作成します。

3 参照マシンを、作成した Image Preparation CD から起動したサービス オペレーティング システムから再起動します。Image Preparation Wizard の Linux ベースの部分が実行され、イメージとその関連ファイルが収集されます。

4 次のファイルを作成し、OS Manager Server の *InstallDir*\Data\OSManagerServer\upload にコピーします。

— ImageName.IBR
このファイルにイメージが含まれます。シン クライアント イメージ ファイルは、参照マシンのフラッシュ ドライブと同じサイズです。Windows XPe または WES のイメージは、同等以上のサイズのフラッシュ ドライブを備えたコピー先マシンに配布できます。このファイルには、イメージがインストールされるときにアクセス可能な組み込みファイル システムが含まれています。

— ImageName.EDM
このファイルにはインベントリ情報を含むオブジェクトが含まれています。

これらのファイルが転送される間は、ネットワーク速度は最大速度より遅くなります。

イメージが配布された後、包括的なログ (*machineID*.log) は *InstallDir*\Data\OSManagerServer\upload ディレクトリで利用できます。

Image Preparation Wizard を使用するには

1 作成した Image Preparation Wizard CD-ROM を参照マシンの CD-ROM ドライブに挿入します (シン クライアント デバイスには、USB CD-ROM ドライブが必要です)。この CD は、お使いの HPCA メディアの Media\iso\roms ディレクトリにある ImageCapture.iso を使用して作成されます。

2 自動実行が有効な場合、HPCA OS の準備とキャプチャ CD のウィンドウが開きます。

3 \image_preparation_wizard\win32 ディレクトリを参照します。

4 **prepwiz.exe** をダブルクリックします。

Image Preparation Wizard では、続行する前に、etprep.exe および fbreseal.exe が利用できるかどうかが確認されます。[ようこそ] ウィンドウが表示されます。

5 **[次へ]** をクリックします。

[エンド ユーザー ライセンス契約] ウィンドウが表示されます。

6 **[同意する]** をクリックします。

7 HPCA server の IP アドレスまたはホスト名およびポートを入力します。これは、次の形式で指定する必要があります。

xxx.xxx.xxx.xxx:port

HPCA Core および Satellite インストールで OS のイメージングと配布用に使用される HPCA server ポートは 3466 です。HPCA Classic 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。

Image Preparation Wizard が HPCA server サーバーに接続できない場合は、メッセージが表示され、次の手順を実行する必要が生じます。

— **[はい]** をクリックして続行します。

— **[いいえ]** をクリックして、ホスト名または IP アドレスを変更します。

— **[キャンセル]** をクリックして、Image Preparation Wizard を終了します。

8 **[次へ]** をクリックします。

[イメージ名] ウィンドウが開きます。

9 イメージ ファイルの名前を入力します。これは、HPCA server の `\upload` ディレクトリに格納されるイメージ名です。

10 **[次へ]** をクリックします。

イメージの説明を入力するウィンドウが開きます。

11 イメージ ファイルの説明を入力します。

12 **[次へ]** をクリックします。

[オプション] ウィンドウが表示されます。

13 適切なオプションを選択します。

OS のインストール後にクライアント接続を実行する

OS のインストール後に HPCA server に接続し、OS が正しくインストールされたことを確認するには、このチェック ボックスをオンにします。このチェック ボックスをオンにしない場合は、OS がインストールされた後、OS 接続は自動的に実行されません。

14 デフォルトを受け入れて、**[次へ]** をクリックします。

[要約] ウィンドウが表示されます。

15 **[開始]** をクリックします。

16 **[完了]** をクリックします。

ウィザードがイメージを準備します。

17 **[OK]** をクリックします。

デバイスは、CD-ROM ドライブの Image Preparation Wizard CD から起動されます。このような動作になるように必要な設定の調整します (たとえば、BIOS のバージョンによっては、再起動プロセスの間に F10 キーを押して、設定内の起動順序を変更できます)。

デバイスが CD を起動せずに Windows XPe を起動する場合は、419 ページの「Windows XPe または WES 参照マシンの準備」からプロセスをやり直す必要があります。

イメージのアップロードは、長時間かかるように感じられる場合があります。転送速度は、プロセッサの速度やネットワーク環境により異なる場合があります。

必要に応じて取得できるように、\upload ディレクトリに格納するファイルのコピーを作成できます。

キャプチャ中は、Service OS の画面にステータス情報が表示されます。詳細については、430 ページの「Windows PE Service OS 画面について」を参照してください。

18 OS Image Preparation Wizard でネットワークに接続し、OS Manager Server の \upload ディレクトリにイメージが格納されます。

アップロード プロセスが完了すると、次のメッセージが表示されます。

OS イメージが正常に OS Manager Server へ送信されました。

**** CD を挿入している場合、CD を取り出して再起動します。

19 参照マシンを再起動して、必要な場合は起動設定を再調整し、元のオペレーティング システムに戻ります。

次に、イメージを HPCA database にパブリッシュします。433 ページの「パブリッシュ」を参照してください。

Windows CE OS イメージ

次のセクションでは、Windows CE シン クライアント オペレーティング システムのイメージを準備し、キャプチャする方法を説明します。

- 423 ページの「CE 参照マシンの準備」
- 423 ページの「Image Preparation Wizard の実行」

タスク 1: CE 参照マシンの準備

- 製品メディア
- イメージ準備 CD-ROM

イメージをキャプチャする前に、HPCA Agent を Windows CE デバイスにインストールする必要があります。詳細については、131 ページの「HP シン クライアントでの HPCA Agent のインストール」または、『HPCA Application Manager および Application Self-Service Manager ユーザー ガイド』を参照してください。

Local Service Boot (LSB) を使用して OS を Windows CE デバイスに配布する場合は、LSB サービスをインストールおよび抽出するデバイスに十分なディスク容量が必要です。デバイスを再起動しても Linux Service OS (SOS) を起動できなかった場合は、デバイスに割り当てられている「ストレージ メモリ」の量が十分でない可能性があります。少なくとも 10 MB が必要です。

Windows CE デバイスで次の手順を実行します。

1 **[開始]** をクリックします。

2 **[設定]** > **[コントロール パネル]** を選択します。

3 **[システム]** アイコンをクリックします。

4 **[メモリ]** タブを選択します。

5 左にあるスライダを使用して、**[ストレージ メモリ]** を 10 MB 以上に増やします。

タスク 2: Image Preparation Wizard の実行

Image Preparation Wizard は以下のタスクを実行します。

1 参照マシンに関する情報 (ハードウェアおよび BIOS の機能など) を含むオブジェクトを作成します。

2 参照マシンを ImageCapture メディアから起動されたサービス オペレーティング システムで再起動します。Image Preparation Wizard の Linux ベースの部分が実行され、イメージとその関連ファイルが収集されます。

3 次のファイルを作成し、HPCA server の *InstallDir*\Data\OSManagerServer\upload にコピーします。

   ImageName.IBR
   このファイルにイメージが含まれます。シン クライアント イメージ ファイルは、参照マシンのフラッシュ ドライブと同じサイズです。

Windows CE のイメージは、同等のサイズのフラッシュ ドライブを備えたコピー先マシンに配布できます。このファイルには、イメージがインストールされるときにアクセス可能な組み込みファイル システムが含まれています。

`ImageName.EDM`
このファイルにはインベントリ情報を含むオブジェクトが含まれています。

これらのファイルが転送される間は、ネットワーク速度は最大速度より遅くなります。

イメージが配布された後、包括的なログ (`machineID.log`) は *`InstallDir`*`\Data\OSManagerServer\upload` ディレクトリで利用できます。

Image Preparation Wizard を使用するには

1. 作成した Image Preparation Wizard CD-ROM を参照マシンの CD-ROM ドライブに挿入します (シン クライアント デバイスには、USB CD-ROM ドライブが必要です)。この CD は、お使いの HPCA メディアの `Media\iso\roms` ディレクトリにある `ImageCapture.iso` を使用して作成されます。
2. 自動実行が有効な場合、HPCA OS の準備とキャプチャ CD のウィンドウが開きます。
3. CD で、`\image_preparation_wizard\WinCE` ディレクトリを参照します。
4. **prepwiz.exe** をダブルクリックします。Image Preparation Wizard が開始されます。
5. HPCA server の IP アドレスまたはホスト名およびポートを入力します。これは、次の形式で指定する必要があります。

   `xxx.xxx.xxx.xxx:port`

   HPCA Core および Satellite インストールで OS のイメージングと配布用に使用される HPCA server ポートは 3466 です。HPCA Classic 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。

   Image Preparation Wizard が HPCA server に接続できない場合は、メッセージが表示され、次の手順を実行する必要が生じます。

   — **[はい]** をクリックして続行します。

   — **[いいえ]** をクリックして、ホスト名または IP アドレスを変更します。

   — **[キャンセル]** をクリックして、Image Preparation Wizard を終了します。
6. **[OK]** をクリックします。

   ウィザードがイメージを準備します。

デバイスは、CD-ROM ドライブの Image Preparation Wizard CD から起動されます。このような動作になるように必要な設定の調整します (たとえば、BIOS のバージョンによっては、再起動プロセスの間に F10 キーを押して、設定内の起動順序を変更できます)。

デバイスが CD を起動せずに Windows CE を起動する場合は、423 ページの「CE 参照マシンの準備」からプロセスをやり直す必要があります。

イメージのアップロードは、長時間かかるように感じられる場合があります。転送速度は、プロセッサの速度やネットワーク環境により異なる場合があります。

必要に応じて取得できるように、\upload ディレクトリに格納するファイルのコピーを作成できます。

キャプチャ中は、Service OS の画面にステータス情報が表示されます。詳細については、430 ページの「Windows PE Service OS 画面について」を参照してください。

7 Image Preparation Wizard でネットワークに接続し、OS Manager Server の \upload ディレクトリにイメージが格納されます。

アップロード プロセスが完了すると、次のメッセージが表示されます。

OS イメージが正常に OS Manager Server へ送信されました。

**** CD を挿入している場合、CD を取り出して再起動します。

8 参照マシンを再起動して、必要な場合は起動設定を再調整し、元のオペレーティング システムに戻ります。

次に、イメージを Configuration Server DB にパブリッシュする場合、433 ページの「パブリッシュ」を参照してください。

Embedded Linux OS イメージ

次のセクションでは、Embedded Linux オペレーティング システムのイメージを準備しキャプチャする方法を説明します。

- 426 ページの「Embedded Linux 参照マシンの準備」
- 427 ページの「Image Preparation Wizard の実行」

タスク 1: Embedded Linux 参照マシンの準備

イメージ キャプチャのため Embedded Linux シン クライアントを準備するには、以下のものが必要です。

- HPCA メディア
- イメージ準備 CD-ROM

イメージをキャプチャする前に、HPCA Agent を Embedded Linux デバイスにインストールする必要があります。詳細は、131 ページの「HP シン クライアントでの HPCA Agent のインストール」 *または*、『HPCA Application Manager および Application Self-Service Manager ユーザー ガイド』を参照してください。

xterm 用のカスタム接続を作成するには

HPCA Registration and Loading Facility (RALF) が参照マシンに事前にインストールされていない場合は、HPCA Agent のインストール後にインストールする必要があります。

ThinPro オペレーティング システムを使用している場合は、xterm 接続を作成するために、カスタム接続の作成が必要になることがあります。

1 左下隅の HP メニューで **[シャットダウン]** を選択します。

2 [Thin Client Action] ドロップダウンで **[Switch to admin mode]** を選択し、管理者パスワード (デフォルトのパスワードは root) を指定します。

注 : Control Center の背景が青から赤に変化します。

3 [Control Center] で **[追加]** ドロップダウン リストをクリックし、**[カスタム]** オプションを選択します。

4 [名前] を **[xterm]** に設定します。

5 [コマンド] に次を入力して実行します。

sudo xterm -e bash &

6 **[完了]** をクリックします。

これで、xterm セッションを開くために使用できる接続ができました。

タスク 2: Image Preparation Wizard の実行

Image Preparation Wizard は以下のタスクを実行します。

1. マシンに十分な空きディスク領域があるかどうかをチェックし、HPCA agent がインストールされていることを確認します。十分な空きディスク領域がない場合、Image Preparation Wizard はメッセージを表示して終了します。
2. 参照マシンに関する情報 (ハードウェアおよび BIOS の機能など) を含むオブジェクトを作成します。
3. 参照マシンを、作成したイメージ準備 CD から起動したサービス オペレーティング システムから再起動します。OS Manager の Image Preparation Wizard の Linux ベースの部分が動作して、イメージおよび関連ファイルを収集します。
4. 次のファイルを作成し、HPCA server の *InstallDir*\Data\OSManagerServer\upload にコピーします。

   — ImageName.DD
   このファイルにイメージが含まれます。シン クライアント イメージ ファイルは、参照マシンのフラッシュ ドライブと同じサイズです。Linux ベースのイメージは、サイズが同じフラッシュ ドライブを備えたコピー先マシンにしか配布できません。このファイルには、イメージがインストールされるときにアクセス可能な組み込みファイル システムが含まれています。

   — ImageName.EDM
   このファイルにはインベントリ情報を含むオブジェクトが含まれています。

   これらのファイルが転送される間は、ネットワーク速度は最大速度より遅くなります。

   イメージが配布された後、包括的なログ (*machineID*.log) は *InstallDir*\Data\OSManagerServer\upload ディレクトリで利用できます。

Image Preparation Wizard を使用するには

1 作成した Image Preparation Wizard CD-ROM を参照マシンの CD-ROM ドライブに挿入します (シン クライアント デバイスには、USB CD-ROM ドライブが必要です)。この CD は、HPCA メディアの `Media\iso\roms` ディレクトリにある `ImageCapture.iso` を使用して作成されます。

> **!** Linux シン クライアント モデルでは、CD-ROM が実行されないように、マウント時にデフォルトで noexec オプションが設定される場合があります。これにより、Image Preparation Wizard を実行しようとすると、アクセス許可のエラーが起こったり、実行に失敗したりします。この問題を解決するには、noexec オプションを設定せずに CD-ROM を再マウントしてください。

2 Image Preparation CD で、`/image_preparation_wizard/linux` に移動し、`./prepwiz.` を実行します。

[ようこそ] ウィンドウが表示されます。

3 **[次へ]** をクリックします。

[エンド ユーザー ライセンス契約] ウィンドウが表示されます。

4 **[同意する]** をクリックします。

5 HPCA server の IP アドレスまたはホスト名およびポートを入力します。これは、次の形式で指定する必要があります。

`xxx.xxx.xxx.xxx:port`

HPCA Core および Satellite インストールで OS のイメージングと配布用に使用される HPCA server ポートは 3466 です。HPCA Classic 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。

Image Preparation Wizard が HPCA server に接続できない場合は、メッセージが表示され、次の手順を実行する必要が生じます。

— **[はい]** をクリックして続行します。

— **[いいえ]** をクリックして、ホスト名または IP アドレスを変更します。

— **[キャンセル]** をクリックして、Image Preparation Wizard を終了します。

6 **[次へ]** をクリックします。

[イメージ名] ウィンドウが開きます。

7 イメージ ファイルの名前を入力します。これは、HPCA server の `\upload` ディレクトリに格納されるイメージ名です。

8 **[次へ]** をクリックします。

イメージの説明を入力するウィンドウが開きます。

9 イメージ ファイルの説明を入力します。

10 **[次へ]** をクリックします。

[オプション] ウィンドウが表示されます。

11 適切なオプションを選択します。

OS のインストール後にクライアント接続を実行する

OS のインストール後に HPCA server に接続し、OS が正しくインストールされたことを確認するには、このチェック ボックスをオンにします。このチェック ボックスをオンにしない場合は、OS がインストールされた後、OS 接続は自動的に実行されません。

12 デフォルトを受け入れて、**[次へ]** をクリックします。

[要約] ウィンドウが表示されます。

13 **[開始]** をクリックします。

14 **[完了]** をクリックします。

ウィザードがイメージを準備します。

15 **[OK]** をクリックします。

デバイスは、CD-ROM ドライブの Image Preparation Wizard CD から起動されます。このような動作になるように必要な設定の調整します (たとえば、BIOS のバージョンによっては、再起動プロセスの間に F10 キーを押して、設定内の起動順序を変更できます)。

デバイスが CD を起動せずに Linux を起動する場合は、426 ページの「Embedded Linux 参照マシンの準備」からプロセスをやり直す必要があります。

イメージのアップロードは、長時間かかるように感じられる場合があります。転送速度は、プロセッサの速度やネットワーク環境により異なる場合があります。

必要に応じて取得できるように、`\upload` ディレクトリに格納するファイルのコピーを作成できます。

16 Image Preparation Wizard でネットワークに接続し、OS Manager Server の `\upload` ディレクトリにイメージが格納されます。

アップロード プロセスが完了すると、次のメッセージが表示されます。

`OS イメージが正常に OS Manager Server へ送信されました。`

**** CD を挿入している場合、CD を取り出して再起動します。

17 参照マシンを再起動して、必要な場合は起動設定を再調整し、元のオペレーティング システムに戻ります。

次に、管理対象デバイスに配布するため、イメージを HPCA database にパブリッシュします。433 ページの「パブリッシュ」を参照してください。

OS イメージのパブリッシュおよび配布

イメージをキャプチャしたら、Publisher を使用して HPCA データベースにそのイメージをパブリッシュします。手順については、433 ページの「パブリッシュ」を参照してください。

HPCA に OS イメージをパブリッシュしたら、[操作] タブの [OS ライブラリ] ページを更新して、新しいイメージを表示します。HPCA Console ツール バーを使用して、選択したデバイスにイメージを配布します。

Windows PE Service OS 画面について

Service OS は Linux や Windows PE のような軽量のオペレーティング システムに基づくインストール前環境です。Service OS が次のことを行います。

1 ターゲット ハードウェアの起動

2 ハードウェアを正しく機能させるために、必要なすべてのドライバを読み込みます。

3 HPCA プログラムをダウンロードして実行します。つまり、OS イメージをダウンロードしてインストールします。

Service OS を使用して次のタイプの操作を実行します。

- ターゲット デバイスのハードウェアに対する操作 (BIOS の更新またはハードウェアの設定など)
- ターゲット デバイスのプロビジョニング (OS の配布など)
- OS イメージのキャプチャ

Service OS を起動するたびに、関連デバイスで [Service OS] 画面が表示されます。OS イメージのキャプチャ中は、参照マシンで [Service OS] 画面が表示されます。OS の配布中は、ターゲット デバイスで [Service OS] 画面が表示されます。

Windows PE の [Service OS] 画面では操作の状況を示します。図 49 にイメージ キャプチャの操作中に表示される画面の例を示します。

図 49　Windows PE の [Service OS] 画面の例

Windows PE の [Service OS] 画面の右側には、実行手順のログがスクロール表示されます。

- 緑のチェックマーク アイコンは、特定の手順が進行中であるか、正常に完了したことを示します。
- 黄色の三角のアイコンは、問題が発生している可能性があることを示す警告です。

- 赤い X アイコンは、キャプチャまたは配布のこの手順が失敗したことを示します。
- 青い疑問符 (?) アイコンは、入力が必要であることを示します。

現在の手順に関する情報は、常にメッセージ一覧の下部に表示されます。メッセージをすべて表示する十分な領域がない場合は、右端にスクロール バーが表示されます。

操作が完了すると、詳細な手順がある場合は、[Service OS] 画面の左側に緑のチェック マークが表示されます。操作が正常でない場合は、この場所に赤い X が表示され、失敗の原因に関する情報を表示します。

操作が失敗した場合は、スクロール バーを使用して検出されたハードウェアに関する情報を表示し、プロセスで失敗が発生した場所を特定できます。

13 パブリッシュ

HPCA Publisher を使用して HP Client Automation (HPCA) に次の項目をパブリッシュします。

- ソフトウェア
- BIOS 設定
- HP Softpaq
- OS イメージ

パブリッシュされたソフトウェアは、メイン HPCA Console の [操作] タブにある [ソフトウェア ライブラリ] にあります。パブリッシュされたオペレーティング システムは、[オペレーティング システム] タブの [OS ライブラリ] にあります。

Publisher は HPCA Core のインストール時に自動的にインストールされます。マシンに HPCA Agent がすでにインストールされている場合、Publisher は Agent のフォルダにインストールされます。別の場所にインストールする場合は、製品メディアの HP Client Automation Administrator インストール ファイルを使用するか、ソフトウェア ライブラリの HPCA Administrator Publisher サービスを使用できます。詳細については、『HP Client Automation Core および Satellite 入門およびコンセプト ガイド』の「HPCA Administrator の手動インストール」を参照してください。

ソフトウェアはパブリッシュした後、使用環境の管理対象デバイスへ付与と配布を行う必要があります。

Publisher を起動するには

1. **[スタート] > [すべてのプログラム] > [HP Client Automation Administrator] > [HP Client Automation Administrator Publisher]** に移動します。
2. Publisher にログインするには、HPCA Administrator のユーザー名とパスワードを使用します。デフォルトでは、ユーザー名は **admin**、パスワードは **secret** です。

パブリッシュ オプションは、ターゲット デバイスおよびインストールしている HPCA ライセンスによって異なります。

434 ページの表 38 に、3 種類のライセンス レベルごとに選択可能なパブリッシュ オプションを示します。

表 38　　各 HPCA ライセンスで選択可能なパブリッシュ オプション

パブリッシュ オプション	Starter	Standard	Enterprise
コンポーネントの選択	いいえ	はい	はい
ハードウェア設定	いいえ	いいえ	はい
HP BIOS 設定	はい	はい	いいえ
HP Softpaq	はい	はい	いいえ
OS ADDON/ 追加 POS ドライバ	いいえ	はい	はい
OS イメージ	いいえ	はい	はい
Windows インストーラ	いいえ	はい	はい
シン クライアントのコンポーネントの選択	はい	はい	はい
シン クライアントの OS イメージ	はい	はい	はい

次の各セクションでは、ライセンスに応じたパブリッシュ オプションで Publisher を使用する方法を説明します。シン クライアント パブリッシュ オプションを選択する場合は、次の該当するセクションの手順に従ってください。

- 435 ページの「ソフトウェアのパブリッシュ」
- 439 ページの「オペレーティング システム イメージのパブリッシュ」
- 447 ページの「OS ADDON および追加 Production OS (POS) ドライバのパブリッシュ」
- 448 ページの「BIOS 設定のパブリッシュ」
- 452 ページの「VMware ThinApp のパブリッシュ」

ソフトウェアのパブリッシュ

パブリッシュするソフトウェアのタイプにより、2 つのパブリッシュ オプションの 1 つを使用します。ログイン画面で、[Windows インストーラ] を使用して Windows インストーラ ファイル (.msi) をパブリッシュするのか、[コンポーネントの選択] を使用して Windows 以外のインストーラ ファイルをパブリッシュするのかを選択します。次のセクションでは、各ファイル タイプをパブリッシュする手順を説明します。

- 435 ページの「Windows インストーラ ファイルのパブリッシュ」
- 437 ページの「[コンポーネントの選択] を使用したパブリッシュ」

Windows インストーラ ファイルのパブリッシュ

Windows インストーラは、MSI ファイルを使用して、オペレーティング システムにソフトウェア サービスを配布します。Publisher では、このファイルによりサービスが作成され、そのサービスが HPCA にパブリッシュされます。ソフトウェア サービスが HPCA に格納されると、お使いの環境の管理対象デバイスに配布する準備が整います。

Windows インストーラ ファイルをパブリッシュするには

1 Publisher を起動します (433 ページの「Publisher を起動するには」を参照)。

2 ログオン画面で、管理者ユーザー ID およびパスワードを入力して、**[OK]** をクリックします。

> HPCA のユーザー名とパスワードを使用して、Publisher にログインします。デフォルトでは、ユーザー名は **admin**、パスワードは **secret** です。

3 [パブリッシュ オプション] 領域で、**[Windows インストーラ]** を選択して、**[OK]** をクリックします。

4 左ペインの Windows インストーラ ファイルへ移動します。右ペインには、選択した MSI ファイルで利用可能な情報が表示されます。

5 **[次へ]** をクリックします。

6 使用できるパブリッシュ オプションを確認します。

— **管理オプション**
管理インストール ポイント (AIP) を作成するには、**[setup を使用]** または **[msiexec を使用]** を選択します。

> AIP のパスは、一時的な場所であり、パブリッシュ セッションが完了したら、削除されます。

— **変換**
Windows インストーラ ファイルに関連付けられた変換ファイルのアプリケーションを選択し、順序を変更します。

— **追加のファイル**
AIP の一部として追加のファイルを含めます。

– リストに表示された利用可能なファイルをすべて選択するには、**[すべて選択]** をクリックします。

– すべてのファイルの選択を解除するには、**[選択なし]** をクリックします。

— **プロパティ**
msi ファイルのプロパティを表示して変更します。Windows インストーラ ファイルには、正しく配布するために追加のコマンド ライン パラメータが必要な場合があります。たとえば、アプリケーションはインストール中にシリアル番号を渡すカスタム プロパティを必要とすることがあります。[プロパティ] ダイアログを使用して、パラメータを追加します。

– 新しいプロパティを追加するには **[追加]** をクリックします。

– 既存のプロパティを削除するには **[削除]** をクリックします。

– プロパティの **[名前]** または **[値]** を変更するには、変更するアイテムをクリックして新しい値を入力します。

パブリッシュ オプションの編集が終わったら、**[次へ]** をクリックします。

7 [アプリケーションの情報] セクションでソフトウェア サービスの情報を入力します。

8 **[パッケージを適用する対象システム]** セクションを使用して、特定のオペレーティング システムまたはハードウェアへのサービスを制限します。いずれかのリンクをクリックして、設定可能なオプションを表示します。

9 **[次へ]** をクリックします。

10 [要約] セクションで、前の手順で指定したサービス情報を確認します。情報を確認したら、**[パブリッシュ]** をクリックします。

11 パブリッシュ プロセスが完了したら、**[完了]** をクリックして Publisher を終了します。

これで、Windows インストーラ サービスを企業へ配布する準備が整いました。

変換ファイルを使用してその他のパラメータを適用するには

1 Orca や他の MSI エディタを使用して変換を作成します。変換は、必ず Windows インストーラ ファイルがパブリッシュされるディレクトリと同じディレクトリに保存します。

2 Windows インストーラのパブリッシュ セッションを開始します。詳細は、上記の指示に従います。

3 編集手順で **[変換]** をクリックします。

4 利用可能な変換ファイルを選択して、パブリッシュ セッションを続けます。

ソフトウェア サービスが配布されると、変換ファイルが適用され、追加のコマンド ライン パラメータが指定されます。

[コンポーネントの選択] を使用したパブリッシュ

Windows インストーラ ファイル以外のソフトウェアをパブリッシュするには、[コンポーネントの選択] オプションを使用して、パブリッシュするソフトウェアを選択します。

[コンポーネントの選択] を使用してパブリッシュするには

1 Publisher を起動します (433 ページの「Publisher を起動するには」を参照)。

2 ログオン画面で、管理者ユーザー ID およびパスワードを入力して、**[OK]** をクリックします。

> HPCA のユーザー名とパスワードを使用して、Publisher にログインします。デフォルトでは、ユーザー名は **admin**、パスワードは **secret** です。

3 [パブリッシュ オプション] 領域で以下の操作を実行します。

— シン クライアントへパブリッシュしている場合は、**[シン クライアントのパブリッシュ]** を選択します。

— ドロップダウン リストから **[コンポーネントの選択]** を選択します。

4 **[OK]** をクリックします。[パブリッシュするファイルを選択] ウィンドウが開きます。

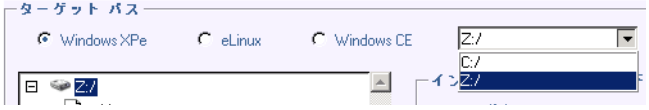
5 パブリッシュするファイルを選択して、**[次へ]** をクリックします。

ソフトウェアがある (パブリッシュ元の) ディレクトリ パスは、ソフトウェアが配布されるターゲット デバイスのディレクトリ パスになります。

ネットワーク共有が表示されますが、配布中に利用できなくなる場合があるためソフトウェアのパブリッシュには使用しません。

[ターゲット パス] ウィンドウが開きます。

6 シン クライアントへパブリッシュしている場合、インストール ポイントを選択します。次の図を参照してください。



7 コマンドを入力して、アプリケーションのインストールおよびアンインストールを実行します。たとえば、インストールを実行するコマンドは、`C:\temp\installs\install.exe /quietmode /automatic c:\mydestination` です。

アンインストールを実行するコマンドは、C:\temp\installs\uninstall.exe /quietmode /automatic です。

ファイルを右クリックして、インストールまたはアンインストールコマンドとして設定できます。

8 **[次へ]** をクリックします。[アプリケーションの情報] ウィンドウが表示されます。

9 [アプリケーションの情報] セクションでソフトウェア サービスの情報を入力します。

10 **[パッケージを適用する対象システム]** セクションを使用して、特定のオペレーティング システムまたはハードウェアへのサービスを制限します。いずれかのリンクをクリックして、設定可能なオプションを表示します。

11 **[次へ]** をクリックします。

12 [要約] セクションで、前の手順で指定したサービス情報を確認します。設定を終了したら、**[パブリッシュ]** をクリックします。

13 パブリッシュ プロセスが完了したら、**[完了]** をクリックして Publisher を終了します。

これで、ソフトウェア サービスを企業へ配布する準備が整いました。

オペレーティング システム イメージのパブリッシュ

Image Preparation Wizard を使用して作成されるオペレーティング システム イメージは、HPCA Server の次のディレクトリに格納されます。

InstallDir\Data\OSManagerServer\upload

Publisher を使用して、管理対象デバイスに配布するオペレーティング システム イメージ ファイルをパブリッシュできます。必要なファイルは、使用する配布方法によって異なります (440 ページの表 39 を参照)。

参照マシンから OS イメージをキャプチャする場合、キャプチャ プロセスで生成されるファイルが必要になります。詳細については、405 ページの「OS イメージの準備とキャプチャ」を参照してください。

.WIM イメージをパブリッシュする場合は、441 ページの「.WIM イメージのパブリッシュの前提条件」を参照してからパブリッシュ プロセスを開始してください。

表 39　　OS イメージのパブリッシュに必要なファイル

配布メソッド	必要なファイル	参照先
DVD から直接	DVD `WIM` ファイル HPCA `unattend-dvd.xml`	442 ページの「DVD から直接パブリッシュする場合の前提条件」

Microsoft ImageX	`ImageName.WIM`
	`ImageName.EDM`
	HPCA
	`unattend-capture.xml`
		441 ページの「.WIM イメージのパブリッシュの前提条件」

Windows セットアップ	`ImageName.WIM`
	`ImageName.EDM`
	HPCA
	`unattend-capture.xml`
		441 ページの「.WIM イメージのパブリッシュの前提条件」

レガシー	`ImageName.IMG`
	`ImageName.MBR`
	`ImageName.EDM`
	`ImageName.PAR`
	WinXPe または Windows CE の場合
	`ImageName.IBR`
	`ImageName.EDM`
	Linux の場合
	`ImageName.DD`
	`ImageName.EDM`
		444 ページの「OS イメージのパブリッシュ」

表 39 の `unattend` ファイルの名前は、Image Capture ISO によって提供されるファイルを表しています。このファイル名は適切な名前に変更できます。

`unattend` ファイルのカスタマイズの詳細については、557 ページの「Windows 応答ファイルのカスタマイズ」を参照してください。

.WIM イメージのパブリッシュの前提条件

このセクションの情報は、次の Windows オペレーティング システムに関連しています。

- Windows XP SP2/SP3
- Windows 2003 SP1/SP2
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 リリース 2 (R2)

これらのバージョンの Windows の .WIM イメージをパブリッシュする場合は、次の条件を満たしている必要があります。

- HPCA メディアの Media\client\default フォルダにアクセスできること。

  このフォルダは、.WIM ファイルを初めてパブリッシュするとき、または更新したエージェント パッケージをパブリッシュする場合にのみ必要になります。HPCA Agent は個別のパッケージとしてパブリッシュされます。これにより、それ以降のすべての .WIM ファイルの配布では、必ず使用可能な最新の Agent が自動的に受信されます。

- Windows Vista、Windows Server 2008、または Windows 7 の場合

  Windows セットアップを使用して配布する場合、.WIM ファイルの取得または作成に使用した Windows インストール メディアから、イメージのパブリッシュ先のデバイス上の \sources フォルダにアクセスできる必要があります。

  Windows XP または Windows 2003 の .WIM ファイルには適用されません。

- イメージのパブリッシュ先のデバイスに Windows Automated Installation Kit (AIK) for Windows 7 をインストールします。Windows AIK は、Microsoft Web サイトからダウンロードできます。

  Windows 7 バージョンの Windows AIK がインストールされていることを確認します。このバージョンは、前のリストのすべてのオペレーティング システムで機能します。

  次のデフォルトの場所に Windows AIK をインストールします。

  ```
  C:\Program Files\Windows AIK
  ```

- 既存の *filename*.wim を使用している場合、イメージのパブリッシュ先のデバイスにそのファイルをコピーします。

- Image Preparation Wizard を使用して .WIM ファイルを準備およびキャプチャした場合、*filename*.wim および *filename*.edm を HPCA server の \upload ディレクトリ (*InstallDir*\Data\OSManagerServer\upload) からイメージのパブリッシュ先デバイスにコピーします。

  ファイルがスパンされている場合、filename.swm や filename2.swm などを \upload ディレクトリからコピーします。ファイルは *filename*.wim、*filename*.002、*filename*.003 などのようにパブリッシュされます。

- HPCA には、無人インストールで使用できる Windows セットアップ応答ファイルが用意されています。Publisher を実行するときに、HPCA が提供する応答ファイルを使用する (推奨メソッド) のか、独自のファイルを作成するのかを選択できます。詳細については、443 ページの「Windows セットアップの応答ファイルの指定」を参照してください。

  HPCA が提供する応答ファイルは unattend.xml と呼ばれます。各オペレーティング システムおよびアーキテクチャ (32 ビットまたは 64 ビットなど) には、独自の unattend.xml ファイルがあります。これらのファイルは、次のサブディレクトリにあります。

  InstallDir\Data\OSManagerServer\capture-conf

  HP が提供する unattend.xml ファイルを使用する場合、使用環境に合わせて変更してから Publisher を実行する必要があります。最低でも、パブリッシュするイメージの ProductKey は指定する必要があります。TimeZone や RegisteredOrganization など、このファイルの他の設定も変更できます。詳細については、557 ページの「Windows 応答ファイルのカスタマイズ」を参照してください。

このディレクトリ内のファイルやフォルダが読み取り専用に設定されていないことを確認してください。読み取り専用に設定されていると、イメージは配布できません。

DVD から直接パブリッシュする場合の前提条件

DVD から直接 OS イメージをパブリッシュする方法が、最も簡単な使用方法です。これは、Windows セットアップを使用して配布が行われることを意味します。イメージを直接配布する場合、Image Preparation Wizard を使用して、配布方法として ImageX を選択する必要があります。

DVD から直接 OS イメージをパブリッシュする準備をするには

1 イメージをパブリッシュするデバイスのローカル フォルダに DVD の install.wim ファイルをコピーします。

2 Image Capture ISO をマウントします。

Windows セットアップの応答ファイルの指定

バージョン 7.90 より前の HPCA では、HPCA で使用するファイルとその名前を手動で変更して、特定の OS イメージの無人インストールをサポートする必要がありました。

このバージョンでは、Publisher の実行時にこの情報のソースを指定できます。この新しいメソッドは、手動の場合に比べてはるかに簡単でエラーが発生しにくくなります。これは、この情報を指定する場合に推奨されるメソッドです。

下位互換性のために、このガイドの付録で古いメソッドについて説明します。557 ページの「Windows 応答ファイルのカスタマイズ」を参照してください。

OS イメージのパブリッシュ

次のセクションでは、Publisher を使用してオペレーティング システム イメージをパブリッシュする方法を説明します。次の 4 つの基本手順があります。

- OS イメージの選択
- 無人インストールで使用する Windows 応答ファイルの選択 (必要な場合)
- パッケージ オプションの指定
- パブリッシュ

次の手順で詳しく説明します。注 : 手順は、選択するオプションによって変わります。

Publisher を起動する前に「.WIM イメージのパブリッシュの前提条件」または 442 ページの「DVD から直接パブリッシュする場合の前提条件」を満たしていることを確認します。

オペレーティング システム イメージをパブリッシュするには

1. Publisher を起動します。433 ページの「Publisher を起動するには」を参照してください。
2. [パブリッシュ オプション] 領域で以下の操作を実行します。
   - シン クライアントへパブリッシュしている場合は、**[シン クライアントのパブリッシュ]** を選択します。
   - ドロップダウン メニューから、**[OS イメージ]** を選択します。
3. **[OK]** をクリックします。[OS イメージ ファイルの選択] ページが開きます。
4. パブリッシュする OS イメージ ファイルを選択します。

   Image Preparation Wizard を使用して作成されるイメージは、HPCA server の次のフォルダに格納されます。

   InstallDir\Data\OSManagerServer\upload
5. 続行する前に、**[説明]** 領域を使用して、正しいファイルを選択していることを確認します。説明に情報を追加することもできます。
6. **[次へ]** をクリックします。
7. 手順 4 で .WIM ファイルを選択しなかった場合（たとえば、シン クライアント イメージをパブリッシュする場合など）は、手順 18 に進みます。

8 このイメージの *.subs および *.xml ファイルを手動で作成した場合、手順 10 に進んでください。この方法は推奨しません。詳細については、557 ページの「Windows 応答ファイルのカスタマイズ」を参照してください。

9 ディレクトリ ツリーで、無人インストールで使用する Windows 応答ファイル (unattend.xml) を選択します。

詳細については、441 ページの「.WIM イメージのパブリッシュの前提条件」を参照してください。

10 **[次へ]** をクリックします。

11 手順 4 で .WIM ファイルを選択した場合は、次の操作 1 または操作 2 のいずれかを実行します。

操作 1: ImageX を配布するために Image Preparation Wizard メソッドを使用して作成された .WIM ファイルを選択した場合

a **[配布方法]** ドロップダウン メニューで、**[Microsoft ImageX]** を選択します。

b **[送信元]** ボックスは無視します。

または

操作 2: Windows セットアップを配布するために Image Preparation Wizard を使用して作成された .WIM ファイルを手順 4 で選択した場合、または .WIM ファイルを DVD メディアからパブリッシュする場合

a **[配布方法]** ドロップダウン メニューで、**[Microsoft セットアップ]** を選択します。

b **[送信元]** ボックスで、**[ブラウズ]** ボタンを使用して Windows インストール メディア DVD の \sources ディレクトリを選択します。この DVD は、Image Preparation Wizard を使用してキャプチャした参照マシンをセットアップするために使用されたものです。

64 ビットのイメージ ファイルをパブリッシュする場合でも、必ず 32 ビットの Windows インストール メディア DVD の \sources ディレクトリを使用してください。

12 [クライアント メディアのロケーション] で、HPCA Agent メディアの正しいパスに沿って参照します (これは、HPCA メディアの Media\client\default フォルダにあります)。

通常のマシンまたはシン クライアントのいずれかでパブリッシュする対象プラットフォームに応じて、適切なサブディレクトリを選択します。

このファイルを既にパブリッシュしている場合は、**[以前にパブリッシュされた既存のパッケージを使用]** を選択し、適切なパッケージを選択できます。

13 **[次へ]** をクリックします。

14 **[パッケージ情報]** セクションで、このパッケージの詳細を入力します。OS イメージをパブリッシュしている間、**[パッケージを限定する対象システム]** セクションは使用できないため注意してください。

15 **[次へ]** をクリックします。

16 **[サービス情報]** セクションで、**[新規作成]** を選択します。

Agent をパブリッシュする場合、**[サービスなし]** を選択します。

17 表示されている残りの

[割り当てのタイプ] グループ ボックスで、**[必須]** を選択します。

18 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。

19 **[要約]** 情報を確認して、前の手順で指定したパッケージおよびサービスの情報を検証します。情報を確認したら、**[パブリッシュ]** をクリックします。

20 パブリッシュ プロセスが完了したら、**[完了]** をクリックして Publisher を終了します。

これで、企業内の管理対象デバイスへサービスを配布する準備が整いました。

パブリッシュされたオペレーティング システム イメージ サービスは、[オペレーション] タブの [OS ライブラリ] で確認できます。

OS ADDON および追加 Production OS (POS) ドライバのパブリッシュ

このプロセスについての詳細は、『HPCA OS Manager システム管理者ガイド』の「終了ポイントを使用しデバイス ドライバを追加しての OS 配布のカスタマイズ」を参照してください。

イメージが新しいローカル パーティションにインストールされた後に配布される**デルタ パッケージ**を作成することにより、以前に準備したイメージにドライバを追加できます。この操作は、Microsoft Windows セットアップおよび ImageX の配布方法に限定されます。

前提条件

- OS サービスをパブリッシュします。Publisher により、このサービスの下に OS.ADDON.ServiceName_* という接続が自動的に作成されます。
- OS ドライバをパブリッシュする場合
  - 次のディレクトリを作成します。

    `C:\MyDrivers\osmgr.hlp\drivers`
  - パブリッシュする各ドライバをこのディレクトリに格納します。

デルタ パッケージをパブリッシュするには

1. **[スタート] > [すべてのプログラム] > [HP Client Automation Administrator] > [HP Client Automation Administrator Publisher]** に移動します。ログオン画面が表示されます。
2. HPCA Administrator のユーザー ID とパスワード (デフォルトでは **admin** と **secret**) を入力します。
3. [パブリッシュ オプション] ウィンドウで、ドロップダウン リストから **[OS アドオン / 追加 POS ドライバ]** を選択します。
4. **[OK]** をクリックします。
5. [ドライバのディレクトリの選択] ウィンドウを使用して、次の各項目を指定します。
   a. ディレクトリ ツリーで、`C:\MyDrivers` ディレクトリを選択します。

      ディレクトリ以下のすべてが再帰的にスキャン、組み込み、パブリッシュされます。

b **[ADDON タイプ]** ドロップダウン リストから、**OS ドライバ** ファイルを選択します。

c **[ターゲット サービスの選択]** ドロップダウン リストから、これらのドライバまたは ADDON に追加する OS サービスを選択します。

d 任意指定の **[サフィックス]** テキスト ボックスには、パッケージの追跡に使用可能な番号を入力できます。たとえば、VISTA_PDD というインスタンスの場合にこのテキスト ボックスに「0」と入力すると、新しい ADDON インスタンス名は VISTA_PDD_0 となります。

[ADDON インスタンス名] テキスト ボックスには、選択した OS サービス名に基づいて、インスタンス名があらかじめ設定されます。この名前はそのままにすることをお勧めします。

この名前はそのままにすることをお勧めします。この名前を修正すると、自分で接続を作成しない限り、OS サービスと ADDON インスタンスの間の接続がなくなります。

6 **[次へ]** をクリックします。

7 要約画面の内容を確認し、**[パブリッシュ]** をクリックします。

CSDB Editor を使用して、PRIMARY.OS.ADDON の新しい ADDON インスタンスを確認できます。オペレーティング システム サービスを次回に配布するときには、そのサービスと一緒にデルタ パッケージが自動的に配布されます。

オペレーティング システム サービスがターゲット デバイスに配布されると、OS ドライバはターゲット デバイスの `C:\OSMGR.HLP\Drivers` ディレクトリに格納されます。

BIOS 設定のパブリッシュ

Publisher を使用して、クライアント デバイスへ配布するために、BIOS 設定ファイルをサービスとしてパブリッシュします。設定ファイルを使用して、BIOS 設定 (起動順序など) の更新や変更、またはクライアント デバイスの BIOS パスワードの変更ができます。

BIOS 設定ファイルのサンプル (`Common HP BIOS Settings.xml`) は、Publisher のインストールに組み込まれており、デフォルトでは `C:\Program Files\Hewlett-Packard\HPCA\Agent\BIOS` にあります。このファイルを使用して、ターゲット デバイスの BIOS 設定を変更します。

BIOS 設定ファイルのサンプルに必要なオプションが含まれていない、または特定のデバイス用の設定ファイルを作成する場合は、450 ページの「BIOS 設定ファイルの作成」を参照してください。

BIOS 設定をパブリッシュするには

1 Publisher を起動します (433 ページの「Publisher を起動するには」を参照)。

2 ログオン画面で、管理者ユーザー ID およびパスワードを入力して、**[OK]** をクリックします。

> HPCA のユーザー名とパスワードを使用して、Publisher にログインします。デフォルトでは、ユーザー名は **admin**、パスワードは **secret** です。

3 [パブリッシュ オプション] 領域で、**[HP BIOS 設定]** を選択して、**[OK]** をクリックします。[選択] ウィンドウが開きます。

4 パブリッシュする BIOS 設定ファイルを選択します。BIOS 設定ファイルのサンプル (`Common HP BIOS Settings.xml`) は、デフォルトでは `C:\Program Files\Hewlett-Packard\HPCA\Agent\BIOS` にあります。

5 必要な場合は、**[現在の BIOS 管理パスワード]** 領域に BIOS パスワードを入力して確認します。ターゲット デバイスに BIOS パスワードがある場合、設定を変更するにはこれが必要です。

6 現在の BIOS パスワードを変更する場合、**[BIOS パスワードの変更]** を選択し、新しいパスワードを入力して確認します。これが必要なのは、クライアント デバイスの BIOS パスワードを変更する場合だけです。

7 **[次へ]** をクリックします。[BIOS オプション] ウィンドウが表示されます。

8 パブリッシュする BIOS 設定を選択するには、BIOS 設定名の左にあるチェック ボックスをクリックします。

9 BIOS 設定の値を変更する必要がある場合、設定名をクリックして、必要に応じて使用可能なオプションを調整します。

10 **[次へ]** をクリックします。[アプリケーションの情報] ウィンドウが表示されます。

11 アプリケーション情報を表示し、必要な場合は変更します。アプリケーション情報は、設定ファイルから利用できる情報に基づいて、あらかじめ決まっています。

12 **[次へ]** をクリックします。[要約] ウィンドウが表示されます。

13 要約情報を確認し、それで良ければ、**[パブリッシュ]** をクリックします。

14 パブリッシュ プロセスが完了したら、**[完了]** をクリックして Publisher を終了します。

BIOS 設定サービスは、HPCA Console のソフトウェア ライブラリで利用できます。

BIOS 設定ファイルの作成

HPCA に付属のファイル以外の BIOS 設定ファイルを使用する場合は、HP System Software Manager(SSM) の BIOS 設定ユーティリティを使用して独自の設定ファイルを生成できます。

SSM は、HPCA Agent (`C:\Program Files\Hewlett-Packard\SSM`) と一緒にインストールされます。または、HP のサポート サイトからダウンロードできます。

BIOS 設定ファイルを作成するには

1 コマンド プロンプトを開き、SSM BIOS 設定ユーティリティがあるディレクトリ (デフォルトでは `C:\Program Files\Hewlett-Packard\SSM`) に移動します。

2 次のように入力します。

```
BiosConfigUtility.exe /
GetConfig:"C:\tmp\MyBIOSconfig.xml" /Format:XML
```

このコマンドにより、`MyBIOSconfig.xml` という名前の XML ファイルが生成され、`C:\tmp` に格納されます。

XML ではなくテキスト ファイルを作成する場合は、次のように入力します。

```
BiosConfigUtility.exe /
GetConfig:"C:\tmp\MyBIOSconfig.txt" /Format:REPSET
```

このコマンドにより、`MyBIOSconfig.txt` という名前のテキスト ファイルが生成され、`C:\tmp` に格納されます。

3 BIOS 設定をパブリッシュする準備ができたら、449 ページの「BIOS 設定をパブリッシュするには」の手順 6 でこのファイルを選択します。

ハードウェア設定要素のパブリッシュ

このセクションでは、Publisher を使用して、ハードウェア設定要素を HP Client Automation Configuration Server Database にパブリッシュします。

HWCE をパブリッシュする前に、リソース ファイルを 1 つのフォルダに集めてください。詳細については、『HP Client Automation OS Manager ハードウェア設定管理ガイド』を参照してください。

ハードウェア設定要素をパブリッシュするには

1 **[スタート] > [すべてのプログラム] > [HP Client Automation Administrator] > [HP Client Automation Administrator Publisher] に移動します。**Publisher の使用方法については、『HP Client Automation Administrator ユーザー ガイド』を参照してください。

2 ユーザー ID とパスワードを入力します。

3 [パブリッシュ オプション] ドロップダウン リストから、[ハードウェア構成] を選択します。

4 **[OK]** をクリックします。

5 HWCE の作成に必要なリソースを含むフォルダを選択します。この例では、[C:\HWCEs\BIOS] を選択しています。

6 [説明] フィールドに、パブリッシュする要素の説明を入力します。この例では、「**Pro32 WS Bios Rev 1.00 Resources**」と入力します。

7 [パッケージ インスタンス名] フィールドに、パッケージのインスタンス名を入力します。この例では、「**P32_BIOS_100**」と入力します。

8 **[次へ]** をクリックします。

9 情報を確認し、**[パブリッシュ]** をクリックします。パッケージのリソースは、圧縮されない形式でパブリッシュされます。

10 Publisher の処理が完了したら、**[完了]** をクリックします。

11 [**Yes**] をクリックして、Publisher の終了を確定します。

PRIMARY.OS.PACKAGE で作成されたパッケージを表示するには、CSDB Editor を使用します。

VMware ThinApp のパブリッシュ

HPCA Enterprise Edition リファレンス ライブラリの「HP Client Automation VMware Thin App Updater - VMware ThinApp のパブリッシュと更新」を参照してください。

パブリッシュされたサービスの表示

[管理] タブの [ソフトウェア管理] 領域で、パブリッシュされたソフトウェアを確認します。

パブリッシュされたオペレーティング システムは、[オペレーティング システム] 領域に保存されます。

HP Client Automation Administrator Agent Explorer

HP Client Automation Administrator の一部として、Publisher と一緒にインストールされる、Agent Explorer は、トラブルシューティングや問題解決に役立ちますが、HP サポートからの直接の指示がない場合は使用しないでください。

14 Application Self-Service Manager の使用

HP Client Automation Application Self-Service Manager (Self-Service Manager) は、クライアントに常駐し、ユーザーが追加で利用できるアプリケーションをインストール、削除、および更新できるようにする製品です。それらのアプリケーションは、HPCA 管理者がユーザーに付与する必要があります。Self-Service Manager では、ユーザーに付与されたアプリケーションのカタログが表示され、ユーザーは、それらのアプリケーションのインストール、削除、および更新を自分で管理できます。Self-Service Manager は、Management Agent がクライアント デバイスに配布されたときにそのデバイスにインストールされます。

次の各セクションで、Self-Service Manager ユーザー インターフェイスの使用方法を説明します。

Application Self-Service Manager へのアクセス

Self-Service Manager ユーザー インターフェイスには、次のいずれかの方法でアクセスできます。

ユーザー インターフェイスにアクセスするには

- **[スタート] > [プログラム] > [HP Client Automation Agent] > [Client Automation Application Self-Service Manager]** へと移動します。

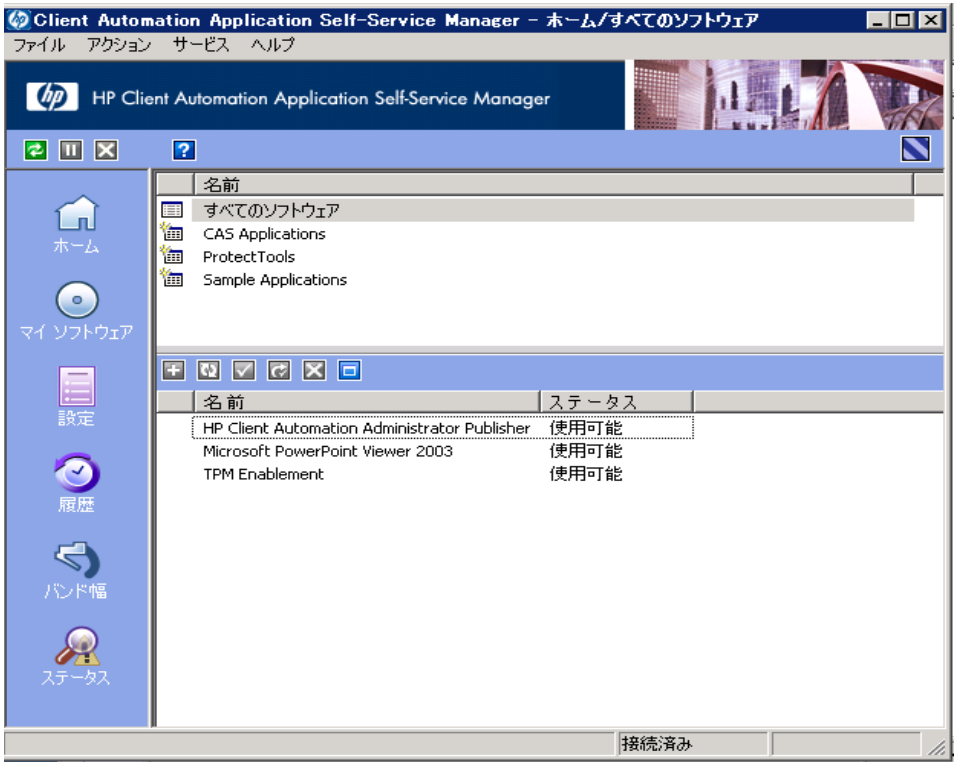
  または

- **[Client Automation Application Self-Service Manager]** デスクトップ ショートカットをダブルクリックします。

Application Self-Service Manager の概要

Self-Service Manager インターフェイス (455 ページの図 50 を参照) には、4 つの主要なセクションがあります。各セクションでは、利用可能なアプリケーションの管理、カタログにあるソフトウェアの情報やステータスの表示、ユーザー インターフェイス表示のカスタマイズができます。

図 50　Application Self-Service Manager ユーザー インターフェイス



凡例

a　**グローバル ツールバー —** カタログのリフレッシュや、現在のアクションの一時停止または取り消しができます。

b　**メニュー バー —** Application Self-Service Manager を使用するときに使用可能なメニューの選択肢が表示されます。

c　**カタログ リスト —** 使用できるさまざまなソフトウェア カタログの一覧が表示されます。

d　**サービス リスト —** 付与されているアプリケーションの一覧が表示されます。

次に示すセクションでは、ユーザー インターフェイスの各セクションを詳細に説明します。

- グローバル ツールバー (この後のセクション)
- 456 ページの「メニュー バー」
- 457 ページの「カタログ リスト」
- 457 ページの「サービス リスト」

グローバル ツールバー

グローバル ツールバーでは、カタログのリフレッシュ、現在のアクションの一時停止、または現在のアクションの取り消しができます。アクションを一時停止すると、**[一時停止]** ボタンを再度クリックしてアクションを再開するか、**[キャンセル]** ボタンをクリックして一時停止したアクションをキャンセルするまで、他のアクションを実行できません。

[グローバル ツールバー] のボタンのうち、現在のアクションで使用できないボタンは、グレー表示になります。

カタログをリフレッシュするには

- 選択したカタログをリフレッシュするには、グローバル ツールバーの **[リフレッシュ]** をクリックします。

現在のアクションを一時停止または再開するには

- 現在のアクションを停止するには、グローバル ツールバーの **[一時停止]** をクリックします。
- 停止したアクションを再開するには、**[再開]** をクリックします。(アクションを一時停止すると、**[一時停止]** ボタンがこのボタンに変わります)。

現在のアクションをキャンセルするには

- 現在のアクションをキャンセルするには、グローバル ツールバーの **[キャンセル]** をクリックします。

メニュー バー

メニュー バーを使用して、Application Self-Service Manager の設定およびカスタマイズを行います。次のセクションでは、メニュー バーの各アイコンについて説明します。

ホーム : このボタンをクリックすると、ホーム カタログにアクセスできます。

マイ ソフトウェア : このボタンをクリックすると、インストールしたアプリケーションだけが表示されます。

設定 : このボタンをクリックすると、Self-Service Manager のさまざまな表示オプション、アプリケーション リスト オプション、および接続オプションにアクセスできます。

このセクションの右上隅にある **[OK]**、**[適用]**、または **[キャンセル]** をクリックして、いつでも変更内容を保持または無視できます。

カタログ リスト

[カタログ リスト] セクションには、使用可能なソフトウェア カタログおよび仮想カタログの一覧が表示されます。

カタログを選択するには

- [カタログ リスト] で、[サービス リスト] セクションに表示するカタログをクリックします。カタログをリフレッシュするには、カタログの名前を右クリックして、ショートカット メニューから **[リフレッシュ]** を選択します。

仮想カタログ

仮想カタログは、HPCA の [ソフトウェアの詳細] で管理者が定義した、デフォルトのカタログのサブセットです。カタログ グループの値が同じサービスは、1 つの仮想カタログにグループ化されます。次のイメージは、いくつかのサンプルのカタログを表示しています。

サービス リスト

[サービス リスト] セクションには、利用可能なアプリケーションが一覧表示されます。インストール済みのアプリケーションの横には、チェック マークが表示されます。カラムの見出しは、必要に応じて変更できます。詳細については、

456 ページの「設定 : このボタンをクリックすると、Self-Service Manager のさまざまな表示オプション、アプリケーション リスト オプション、および接続オプションにアクセスできます。」を参照してください。

表 40　　[サービス リスト] セクションのボタン

ボタン	アクション	説明
	インストール	選択したサービスをマシンにインストールします。
	検証	選択したサービスのファイルを検証します。
	修復	選択したサービスを修復します。
	削除	選択したサービスをマシンから削除します。
	展開 / 折りたたむ	選択したサービスを展開したり、折りたたんだりします。

[サービス リスト] セクションのボタンは、選択したアプリケーションに対して使用できない場合、グレー表示になります。

Application Self-Service Manager ユーザー インターフェイスの使用

ユーザー インターフェイスを使用して、ソフトウェアのインストールと削除、利用可能なアプリケーションのカタログのリフレッシュ、およびアプリケーションに関する情報の表示を行います。メニュー バーには、セッション履歴の表示、バンド幅の調整、およびアプリケーションの現在のステータスの表示のためのボタンがあります。詳細については、次の各セクションを参照してください。

- 459 ページの「ソフトウェアのインストール」
- 460 ページの「カタログのリフレッシュ」
- 460 ページの「情報の表示」
- 461 ページの「ソフトウェアの削除」

- 462 ページの「ソフトウェアの検証」
- 462 ページの「ソフトウェアの修復」
- 462 ページの「履歴の表示」
- 463 ページの「バンド幅の調整」
- 463 ページの「ステータスの表示」

ソフトウェアのインストール

利用可能なアプリケーションは、サービス リストに一覧表示されます。これらのアプリケーションから 1 つ以上をいつでもインストールできます。

ソフトウェアをインストールするには

1 サービス リストで、インストールするアプリケーション名をクリックします。

2 **[インストール]** ボタン をクリックします。

インストールによっては、一連のダイアログ ボックスが表示される場合があります。その場合、表示される指示に従ってください。それ以外の場合は、インストールがすぐに始まります。

インストールするアプリケーションの名前を右クリックして、表示されるショートカット メニューの **[インストール]** をクリックしても同じ操作を実行することができます。

インストールの進行状況が、進行状況バーに表示されます。

— インストールをキャンセルするには、グローバル ツールバーの **[キャンセル]** をクリックします。

— インストールを一時停止するには、グローバル ツールバーの **[一時停止]** をクリックします。アクションを一時停止すると、一時停止しているアクションをキャンセルまたは再開するまで、他のアクションを実行できません。

カタログのリフレッシュ

カタログは、Self-Service Manager のユーザー インターフェイスにログインするたびにリフレッシュされます。ログインしている間に、使用が認可されているアプリケーションのリストが変わった、またはインストールしたアプリケーションの更新が使用可能になったと考えられる場合は、グローバル ツールバーの **[カタログのリフレッシュ]** をクリックして、アプリケーションのリストを更新します。

ソフトウェア リストの任意のアイテムを右クリックして、表示されるショートカット メニューの **[カタログをリフレッシュ]** をクリックしても同じ操作を実行することができます。

情報の表示

サービス リストには基本的な情報が表示されますが、アプリケーションに関する詳細な情報 (ベンダー、バージョン、サイズ、インストール日など) は、次の方法で取得できます。

- これらのカラムをサービス リストに追加する。
- 展開したサービス ボックスで、**[拡張情報を表示]** をクリックする。

メーカーからの詳細情報が必要な場合は、ベンダーのリンクをクリックします。

詳細情報を表示するには

1 サービス リストでアプリケーションを選択し、**[拡張情報を表示]** をクリックします。

アプリケーションを右クリックし、表示されるショートカット メニューの **[プロパティ]** をポイントし、**[情報]** をクリックしても同じ操作を実行することができます。

2 サービス リストに戻るには、対応する **[キャンセル]** ボタンをクリックします。

ソフトウェアの削除

コンピュータからアプリケーションを削除するには、**[削除]** ボタン を使用します。

ソフトウェアを削除するには

1 削除するアプリケーションを選択します。

2 **[削除]** をクリックします。

3 アプリケーションの削除を確認するメッセージが表示されたら、**[はい]** をクリックします。

削除するアプリケーションの名前を右クリックして、表示されるショートカット メニューの **[削除]** をクリックしても同じ操作を実行することができます。

ソフトウェアの検証

アプリケーションのインストールをチェックするには

1 インストールされている検証対象のサービスをサービス リストで選択します。

2 [**検証**] をクリックします。

> ソフトウェア名を右クリックし、表示されるショートカット メニューの [**検証**] をクリックしても同じ操作を実行することができます。

— 検証でアプリケーションに問題がない場合は、アプリケーションの [検証した日付] カラムに検証の日付と時刻が表示されます。

— 検証でアプリケーションに問題がある場合は、[ステータス] カラムに [破損] と表示されます。

3 ソフトウェアを修復するには、[**修復**] をクリックします。

ソフトウェアの修復

アプリケーションに何らかの問題がある場合、それを修復するには、[**修復**] をクリックします。

ソフトウェアを修復するには

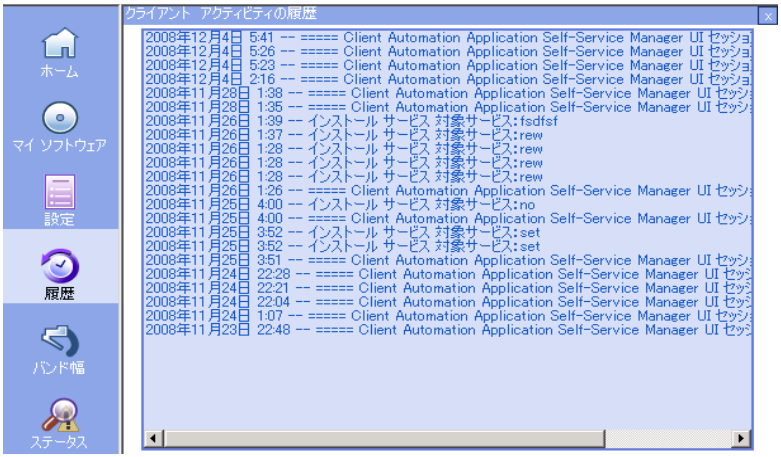
1 修復する必要があるアプリケーションを選択します。該当するアプリケーションには、最初のカラムに X、[ステータス] カラムに [破損] と表示されます。

2 [**修復**] をクリックします。HPCA によってアプリケーションの修復に必要なファイルが取得されます。

履歴の表示

1 メニュー バーの **[履歴]** をクリックして、現在のセッションの履歴を表示します。

図 51　　[履歴] ウィンドウ



2　[履歴] ウィンドウを閉じて、サービス リストに戻ります。

バンド幅の調整

メニュー バーの **[バンド幅]** をクリックして、バンド幅のスライダを表示します。この値を変更すると、スロットリングの値が動的に変化します。

バンド幅のスライダを使用してバンド幅の設定を調整するには

- スライダをドラッグして、目的のバンド幅スロットリングの量にまで値を増減して調整します。
- バンド幅スロットリングは、[設定] の [接続オプション] セクションでも調整できます。

ステータスの表示

メニュー バーの **[ステータス]** をクリックすると、サイズ、推定時間、進捗状況、使用可能なバンド幅など、現在のアクションのステータスが表示されます。

図 52　　選択したアプリケーションのステータス表示

[ステータス] ウィンドウは、Application Self-Service Manager からドッキングしたりドッキングを解除したりできます。これにより、画面上の任意の位置に [ステータス] ウィンドウを移動できます。デフォルトでは、[ステータス] ウィンドウはドッキングされています。

[ステータス] ウィンドウのドッキングを解除するには

1　メニュー バーの **[ステータス]** をクリックします。

2　表示された [ステータス] ウィンドウ上で右クリックします。

3　ショートカット メニューから **[ドッキング済み]** を選択します。[ステータス] ウィンドウがドッキングされている場合、ショートカット メニューの **[ドッキング済み]** の横にチェック マークが表示されます。

Application Self-Service Manager インターフェイスから [ステータス] ウィンドウが分離され、画面上の任意の場所に移動できるようになります。

[ステータス] ウィンドウをドッキングするには

1　メニュー バーの **[ステータス]** をクリックします。

2　表示された [ステータス] ウィンドウ上で右クリックします。

3 ショートカット メニューの **[ドッキング済み]** をクリックします (チェック マークが表示されていない場合のみ)。

[ステータス] ウィンドウが Application Self-Service Manager インターフェイスにドッキングされます。

ユーザー インターフェイスのカスタマイズ

メニュー バーの **[設定]** ボタンをクリックして、利用可能なカスタマイズ オプションを表示します。次のセクションで各カスタマイズ領域について説明します。

- 465 ページの「全般オプション」
- 467 ページの「サービス リスト オプション」
- 470 ページの「接続オプション」

全般オプション

Application Self-Service Manager インターフェイスの外観を変更するには、[全般オプション] ウィンドウを使用します。

図 53　　[全般オプション] ウィンドウ

表示を変更するには

- メニューを表示する場合は、**[メニューを表示]** を選択します。
- カタログ リストを表示する場合は、**[カタログ リストを表示]** を選択します。
- 各セッションの開始時にオフライン　モードで　Application　Self-Service Manager を使用するかどうかを確認するには、**[オフライン モードのプロンプトを表示]** チェック ボックスをオンにします。
- オプション バーを自動的に非表示にするには、**[自動非表示オプションバー]** をオンにします。

色を変更するには

- システムの色を使用する場合は、**[システムの色を使用]** をオンにします。
- カラー スキームをカスタマイズする場合は、**[色のカスタマイズ]** をオンにします。
  - [色のカスタマイズ] をクリックした場合、目的に応じて以下のラベルのボックスをクリックします。

- **[選択色を設定]**。選択した色を変更します。
- **[ボタンの色を設定]**。ボタンの色を変更します。
- **[背景色を設定]**。背景色を変更します。
- **[作業領域の色を設定]**。作業領域を変更します。

サービス リスト オプション

サービス リストの外観を変更するには、**[サービス リスト オプション]** を使用します。

図 54　　サービス リスト オプション

サービス リストのカラム名をカスタマイズするには

サービス リストに表示されるカラムをカスタマイズするには、[カラム] 領域を使用します。右のカラムには、現在サービス リストに表示されているカラムの名前が一覧表示されます。利用可能な各カラム見出しの説明については、468 ページの「表示のカスタマイズ」を参照してください。

サービス リストにカラムを追加するには

- [使用可能なカラム] リスト ボックスで、1 つ以上の名前を選択し、**[追加]** をクリックします。選択したカラムが [表示するカラム] リスト ボックスの一覧に表示されます。

サービス リストからカラムを削除するには

1. [表示するカラム] リスト ボックスで、1 つ以上の名前を選択します。連続した複数のカラム名を選択するには **Shift** キーを押しながらカラム名をクリックし、連続していない複数のカラム名を選択するには **Ctrl** キーを押しながらカラム名をクリックします。
2. **[削除]** をクリックします。選択したカラムが [表示するカラム] リスト ボックスから削除され、元の [使用可能なカラム] ボックスに表示されます。

表示のカスタマイズ

- サービス リストで、現在のサービス アイテムを展開するには、**[アクティブなサービス アイテムを展開]** チェック ボックスをオンにします。
- 各サービスを仕切るグリッド線付きでサービス リストを表示するには、**[グリッド線を表示]** を選択します。
- 現在選択しているカタログを展開するには、**[アクティブなカタログ アイテムを展開]** を選択します。
- **[詳細な操作を表示]** は現時点では利用できません。

表 41　　サービス リストで利用可能なカラムの見出し

カラムの見出し	説明
適応バンド幅	バンド幅スロットリングを使用するときに使用されるバンド幅の適用最小割合。
警告メッセージ	エンド ユーザーに長いアプリケーション説明または指示のメッセージを表示 (警告 / 延期設定の一部として指定できる任意指定のサービス テキスト フィールド)。
作成者	サービスの作成者。
Avis	内部で使用するためだけのサービス ステータス フラグ。
圧縮後のサイズ	圧縮後のサービスのサイズ (バイト単位)。
説明	アプリケーションの簡単な説明。
エラーコード	現在のサービスのステータス。例 : 初期 = 999。メソッドの失敗 = 709。

表 41　　サービス リストで利用可能なカラムの見出し

カラムの見出し	説明
インストール日	アプリケーションがコンピュータにインストールされた日付。
ローカルの修復	ローカルでのデータ修復可能性 (データがローカル コンピュータにキャッシュされているかどうか)。
必須	アプリケーションで定義される必須またはオプションなファイル (内部使用)。
名前	アプリケーションの名前。
オーナー カタログ	アプリケーションの取得元のドメイン名。
価格	サービスの価格。
パブリッシュ日	アプリケーションがカタログにパブリッシュされた日付。
再起動	サービスの再起動設定 (内部使用)。
再パブリッシュ日	アプリケーションがカタログに再パブリッシュされた日付。
予約済みのバンド幅	バンド幅スロットリングを使用するときに使用されるバンド幅の予約済み最大割合。
スケジュールを許可	エンド ユーザーがローカルにアプリケーションの更新スケジュールを変更できるかどうかを指定。
サイズ	アプリケーションのサイズ (バイト単位)。 注意 ：アプリケーションを正常にインストールするには、このカラムで表示される空き容量がコンピュータに必要です。
ステータス	アプリケーションの現在のステータス • 使用可能 • インストール済み • 更新可能 • 破損
システムのインストール	システム アカウントを使用してアプリケーションがインストールされるかどうかを表示。
スロットリング タイプ	使用するバンド幅スロットリングのタイプ。可能な値は、ADAPTIVE、RESERVED、または NONE。
オプション	ステータス ウィンドウを表示するかどうかを決定。
アップグレード日	アプリケーションがアップグレードされた日付。

表 41　　サービス リストで利用可能なカラムの見出し

カラムの見出し	説明
URL	ソフトウェア ベンダーの Web アドレス。
ベンダー	アプリケーションを提供したソフトウェア ベンダー。
検証日	前回、アプリケーションが検証された日付。
バージョン	アプリケーションのバージョン。

接続オプション

使用するバンド幅スロットリングのタイプの選択や、プロキシ サーバー設定の指定には、**[接続オプション]**（470 ページの図 55 を参照 ）を使用します。

図 55　　接続オプション

- スロットリング
  - スロットリングを行わない場合、**[なし]** を選択します。

- 使用するネットワーク バンド幅の最大の割合をスケールに基づいてスライドするには、**[バンド幅を予約]** を選択します。ユーザーは、ダウンロード時に予約バンド幅をインターフェイスで変更できます。
- 使用するネットワーク バンド幅の最小の割合をスケールに基づいて指定するには、**[トラフィックに適応]** を選択します。適応バンド幅は、データ ダウンロード プロセスの間は変更できません。設定できるのは、ジョブがディスパッチされる前だけです。

- **プロキシ**
  - Application Self-Service Manager は、インターネット プロキシが使用されると、それを検出できます。検出されたインターネット プロキシのアドレスは、クライアント コンピュータの `IDMLIB` ディレクトリにある `PROXYINF.EDM` に格納されます。IDMLIB のデフォルトの場所は、*`SystemDrive`*`:\Program Files\Hewlett-Packard\HPCA\Agent\Lib` です。次回、HPCA Agent コンピュータが HPCA Server に接続するときには、指定したインターネット プロキシが使用されます。この機能を使用するには、HPCA Agent でインターネット プロキシを使用および検出できるようにする必要があります。

HPCA System Tray アイコン

HP Client Automation システム トレイ アイコンを使用すると、ユーザーは、ステータスや統計情報を確認したり、一時停止やキャンセルの操作を行ったりすることができます。

図 56　　HPCA System Tray アイコン

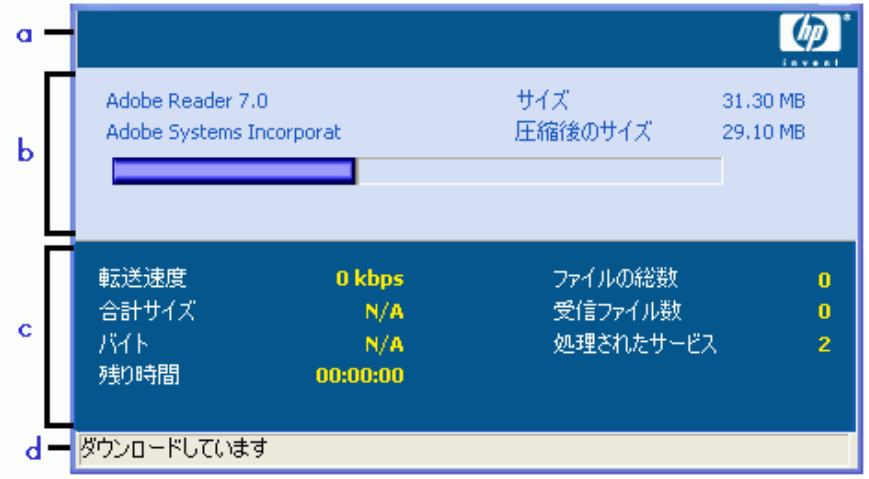
HPCA の状態を表示するには、カーソルをアイコンの上に移動します。

- **アイドル** : アクションが処理中でなく、ユーザーの介入を必要としないとき、アイコンは静的です。システム トレイ アイコンは、アイドル状態では非表示になる場合があります。
- **アクティブ** : Application Self-Service Manager が実行中のとき、またはユーザーの介入が必要なときに、アイコンはアクティブになります。アイコンの上にカーソルを合わせると、活動情報を示すポップアップが表示されます。重要な通知が発生した場合は、ポップアップが自動的に表示されます。

[HPCA ステータス] ウィンドウ

HPCA System Tray アイコンを左クリックして、[ステータス] ウィンドウを表示します。次の図で示すように [ステータス] ウィンドウが開きます。

図 57　　HPCA ステータス



凡例

a　ボタン バー

b　情報パネル

c　ステータス領域

d　ステータス メッセージ

[ステータス] ウィンドウには次の領域があります。

- **ボタン バー**: [一時停止] ボタン、[キャンセル] ボタン、および HPCA Agent が実行中にアニメーション表示になるロゴがあります。
- **情報パネル**：この領域には、アクティブなアプリケーションに関する情報が表示され、完了したタスクの割合を示す進行状況バーも表示されます。
- **ステータス領域**：転送速度、送信の合計サイズ、受信したバイト数、送信の推定残り時間、送信するファイルの総数、受信したファイルの数、処理されたサービスの数など、アクティブなプロセスに関する統計が表示されます。
- **ステータス メッセージ領域**：現在のプロセスに関するメッセージが表示されます。

— **バンド幅設定**: HPCA Server のアプリケーションにバンド幅スロットリングを設定している場合、システム トレイ コンソールのバンド幅トグル ボタン  をクリックすると、バンド幅設定用のスライダが表示されます。バンド幅スロットリングの値を変更するには、スライダを調整します。

15 Personality Backup and Restore

HPCA Personality Backup and Restore ソリューションでは、個々の管理対象デバイスにあるアプリケーションとオペレーティング システムのユーザー ファイルや設定をバックアップおよび復元できます。ファイルと設定は HPCA Core Server に格納され、元のデバイスや新しいデバイスへの復元に使用できます。また、管理対象デバイスのファイルおよび設定をローカルにバックアップしたり、復元したりすることもできます。

HPCA Personality Backup and Restore ソリューションは、オペレーティング システムの配布の一部としてファイルと設定を移行する場合にも使用できます。

HPCA Personality Backup and Restore ソリューションは、Microsoft ユーザー状態移行ツール (USMT) に基づいています。このソリューションでは、USMT で作成される移行ストアのリモートおよびローカル両方の管理を提供し USMT を強化します。また、必要な USMT の制御ファイルをダウンロードし、これらのファイルを個別に配布する必要性を解消します。HPCA では USMT バージョン 3.0.1 と 4.0 をサポートしています。

基づいているバックアップ テクノロジが異なるため、HPCA 7.5 より前のバージョンの HPCA で作成されたバックアップは復元できません。

次のセクションでは、使用環境で HPCA Personality Backup and Restore ソリューションを実装する方法について説明します。

要件

Personality Backup and Restore ソリューションを実装する前に、お使いの環境が次の要件を満たしていることを確認します。

オペレーティング システム

次のオペレーティング システムを使用する移行元コンピュータから、バックアップを作成できます。

- Windows 2000 Professional Service Pack 4 以降
- Windows XP
- Windows Vista
- Windows 7

次のオペレーティング システムを使用する移行先コンピュータに、ファイルおよび設定を復元できます。

- Windows XP
- Windows Vista
- Windows 7

ディスク容量

開始する前に、移行元コンピュータ、移行先コンピュータ、および HPCA Core Server にバックアップされるファイルおよび設定を格納できる十分なディスク容量があることを確認する必要があります。バックアップに必要なディスク容量を推定するには、次の URL にある Microsoft TechNet Web サイトの「データの保存場所の決定」を参照してください。

http://technet.microsoft.com/en-us/library/cc722431.aspx

注 : 格納場所は HPCA によって自動的に設定されます。移行元コンピュータ、移行先コンピュータ、HPCA Core Server にはそれぞれ、移行されるファイルおよび設定用に十分なディスク容量が必要です。

また、移行先コンピュータでは、移行されるファイルおよび設定が使用する 2 倍のディスク容量が必要です。

HPCA Personality Backup and Restore Utility を使用する場合、HPCA Core Server には、バックアップ時に作成された、アーカイブされたユーザー ファイルおよび設定が格納されます。復元時には、アーカイブされたファイルおよび設定が移行先コンピュータの一時的な場所にダウンロードされた後、元の場所に復元されます。復元が正常に行われたら、アーカイブされたファイルおよび設定は、移行先コンピュータから削除されます。

`/localstore` オプションを指定して `pbr.exe` コマンドを使用する場合、バックアップは `C:/OSMGR.PRESERVE/PBR.work` にあるディスクにローカルに格納されます。このバックアップは前述のファイルの唯一のコピーであるため、削除されません。

ソフトウェア

必要なアプリケーションは次のとおりです。

- **Microsoft USMT バージョン 3.0.1 または 4.0**
  このアプリケーションは、移行元および移行先のデバイスでデフォルトの場所にインストールする必要があります。USMT についてを参照してください。

  > ⚠ このソリューションでは、Microsoft USMT バージョン 3.0.1 またはバージョン 4.0 を使用する必要があります。これ以外のバージョンの USMT はサポートされていません。

- **HP Client Automation Personality Backup and Restore**
  このアプリケーションを、移行元と移行先両方のデバイスにインストールする必要があります。このアプリケーションは、HPCA Agent が管理対象デバイスにインストールされるときに自動的にインストールされます。

USMT について

HPCA Personality Backup and Restore ソリューションは Microsoft ユーザー状態移行ツール (USMT) に基づいているため、次の URL にある Microsoft Technet Web サイトのドキュメントを参照して、このツールとその機能について理解してください。

http://technet.microsoft.com/en-us/library/cc722032.aspx

このセクションでは、Microsoft USMT について、入手方法、インストール方法、および移行ファイルを使用する方法について説明します。Personality Backup and Restore ソリューションで提供される、バックアップおよび復元時に自動的に USMT を起動する Hewlett-Packard ユーザー インターフェイスの説明については、483 ページの「HPCA Personality Backup and Restore Utility の使用」を参照してください。

サポートされるファイル、アプリケーション、および設定

USMT では、ユーザー ファイルおよびフォルダ (XP の [マイ ドキュメント] フォルダまたは Vista の [ドキュメント] フォルダなど)、オペレーティング システム設定 (フォルダ オプションや壁紙設定など)、アプリケーション設定 (Microsoft Word の設定など) を含むさまざまなデータが移行されます。総合的な一覧については、次の URL にある Microsoft TechNet Web サイトの「USMT 3.0 によって移行されるもの」を参照してください。

http://technet.microsoft.com/en-us/library/cc722387.aspx

また、次の URL にある「USMT 4.0 の新機能」も参照してください。

http://technet.microsoft.com/en-us/library/dd560752(WS.10).aspx

- アプリケーションを正常に移行するためには、移行元コンピュータと移行先コンピュータのアプリケーションのバージョンが同一である必要があります。これには例外が 1 つあります。Microsoft Office の設定の場合は、移行元コンピュータの古いバージョンから移行先コンピュータの新しいバージョンに移行できます。
- USMT では、ユーザーがアクセスした、または変更したアプリケーション設定のみが移行されます。移行元コンピュータのユーザーがアクセスしたことがないアプリケーション設定は移行されません。
- フォント、壁紙、スクリーン セーバー設定などの一部のオペレーティング システム設定は、移行先コンピュータを再起動するまで適用されません。

Microsoft USMT 3.0.1 または 4.0 の入手とインストール

USMT をインストールする理由としては、次のいずれかまたは両方が考えられます。

- 管理者として、USMT の機能に慣れ、ソリューションを個人仕様にするために移行規則をカスタマイズする方法を学ぶ。
- + エンド ユーザーとして、管理対象デバイスのファイルおよび設定をバックアップしたり復元したりできるようになる。

Personality Backup and Restore を実装する場合は、バックアップする移行元コンピュータと復元する移行先コンピュータに Microsoft USMT 3.0.1 または 4.0 をインストールする必要があります。このセクションでは、このアプリケーションを入手できる場所、およびインストールする方法について説明します。

Microsoft ユーザー状態移行ツール バージョン 3.0.1 または 4.0 を使用する必要があります。これ以外のバージョンの USMT はサポートされていません。

Microsoft USMT 3.0.1 の入手

USMT 3.0.1 は次の URL にある Microsoft ダウンロード センターから入手できます。

http://www.microsoft.com/downloads

32 ビットと 64 ビットの 2 つのバージョンがあります。お使いの環境に適したバージョンを選択してください。

Microsoft USMT 4.0 の入手

USMT 4.0 は Windows Automated Installer Kit (AIK) for Windows 7 に含まれており、次の URL にある Microsoft ダウンロード センターから入手できます。

http://www.microsoft.com/downloads

32 ビットと 64 ビットの 2 つのバージョンがあります。お使いの環境に適したバージョンを選択してください。

管理対象デバイスでの Microsoft USMT のインストール

管理対象デバイスでは、2 つの方法で USMT をインストールできます。手動でインストールするか、HPCA Administrator Publisher を使用してサービスにパッケージ化してから (433 ページの「パブリッシュ」を参照)、管理対象デバイスに付与または配布します。USMT は移行元および移行先両方のクライアント デバイスで、デフォルトの場所にインストールする必要があります。

表 42　　USMT のデフォルトのインストール場所

USMT のバージョン	デフォルトの場所
3.0.1	`C:\Program Files\USMT301`
4.0	`C:\Program Files\Windows AIK\Tools\USMT`

管理対象デバイスのオペレーティング システムに応じて、必ず適切なバージョン (32 ビットまたは 64 ビット) をインストールしてください。

移行ファイル

Personality Backup and Restore ソリューションでは、次の 3 つの USMT 移行ファイルを使用して、移行に含めるコンポーネントを指定します。

- `MigSys.xml` – オペレーティング システム設定の移行
- `MigApp.xml` – アプリケーション設定の移行
- `MigUser.xml` – ユーザー フォルダおよびファイルの移行

お使いの環境でこのソリューションを実装する前に、これらのファイルを入手し、HPCA Core Server に保存する必要があります (480 ページの「Core Server への移行ルールの保存」を参照)。

これらのファイルを入手するには、サポートされているプラットフォームのいずれかに USMT をインストールする必要があります (478 ページの「Microsoft USMT 3.0.1 または 4.0 の入手とインストール」を参照)。インストール時にこれらのファイルは、479 ページの「管理対象デバイスでの Microsoft USMT のインストール」に示すディレクトリに配置されます。

配置されたファイルは、編集することも (480 ページの「ルールの編集」を参照)、そのまま使用することもできます。

ルールの編集

場合によっては、デフォルトの移行ルールの編集が必要になることがあります。たとえば、特定のアプリケーションの設定を移行しない場合や、特定のファイル タイプを除外する場合です。デフォルトの移行動作を変更するには、移行 XML ファイルを編集する必要があります。これらのファイルをカスタマイズする方法については、次のドキュメントを参照してください。

http://technet.microsoft.com/en-us/library/cc766203.aspx

Core Server への移行ルールの保存

移行ファイルの編集が完了したら、または移行ファイルを編集しない場合でも、HPCA Core Server の次のフォルダにファイルを保存します。

DataDir\PersonalityBackupAndRestore\conf

この場合の *DataDir* は、HPCA Core のインストール時に指定した、ユーザーが設定できるデータ ディレクトリです。

これらの移行ファイルは、同じファイル名であり、Microsoft USMT 3.0.1 または 4.0 インストールから入手した元のファイルと同じファイル名 (MigSys.xml、MigApp.xml、および MigUser.xml) を使用する必要があります。

ScanState コマンド ラインと LoadState コマンド ライン

移行ルールは、Personality Backup and Restore Utility によって Core Server からダウンロードされ、個人データの収集と復元を行う USMT 実行可能ファイル ScanState および LoadState によって使用されます。ScanState.exe は、移行元コンピュータの個人データを収集する実行可能ファイルです。Personality Backup and Restore Utility で使用される ScanState コマンド ラインは、次のとおりです。

```
ScanState.exe /i:MigApp.xml /i:MigUser.xml /i:MigSys.xml /o
/l:ScanState.log /localonly "Agent\Lib\PBR\work\store"
```

この場合の *Agent* は、Agent のインストール ディレクトリです。

LoadState は、移行先コンピュータに個人データを復元する実行可能ファイルです。Personality Backup and Restore Utility で使用される LoadState コマンド ラインは、次のとおりです。

```
LoadState.exe /i:MigApp.xml /i:MigUser.xml /i:MigSys.xml /
l:LoadState.log /lac:password /lae
"Agent\Lib\PBR\work\store"
```

この場合の *Agent* は、Agent のインストール ディレクトリです。

これらのコマンド ラインはカスタマイズできませんが、バックアップおよび復元される内容を理解していただくために記載しています。注：これらの ScanState および LoadState コマンド ライン引数によって、ローカル ユーザー アカウントも含め、システムのすべてのユーザー アカウントが移行されます。復元を実行するときに、移行先コンピュータにローカル ユーザー アカウントがない場合は、password というパスワードを使用して、LoadState によって作成されます (前述のコマンド ラインを参照)。そのため、復元後には、復元されたローカル ユーザー アカウントのパスワードを変更する必要があります。

Personality Backup and Restore の使用

HPCA Personality Backup and Restore 機能には、次の 3 つの方法でアクセスできます。

- 483 ページの「HPCA Personality Backup and Restore Utility の使用」
- 488 ページの「Personality Backup and Restore サービスの使用」
- 487 ページの「コマンド ライン インターフェイスの使用」

これらの 3 つの方法すべてで pbr.exe という名前の同一の HPCA アプリケーションを起動します。pbr.exe は、実行時に毎回、HPCA Core Server から管理対象デバイスに 3 つの移行 XML ファイル (480 ページの「移行ファイル」を参照) をダウンロードして、これらのファイルを使用してバックアップまたは復元を実行します。

デフォルトでは、pbr.exe がバックアップ ファイルを HPCA Core Server の次の場所に格納し、また、この場所からバックアップ ファイルを復元します。

DataDir\PersonalityBackupAndRestore\backups

この場合の *DataDir* は、HPCA Core のインストール時に指定したデータ ディレクトリです。サブディレクトリは、管理対象デバイスをバックアップするたびに backups フォルダに作成されます。このサブディレクトリには復元に必要なすべての情報が格納されています。

HPCA Core Server ではなく管理対象デバイスのローカル ハード ディスクにバックアップ ファイルを格納する場合は、pbr.exe コマンドに /localstore オプションを指定して使用します。この場合、ファイルは次の場所にあるローカル ディスクに格納されます。

C:/OSMGR.PRESERVE/PBR.work

復元に必要なすべての情報が、このサブディレクトリに格納されます。

詳細については、487 ページの「コマンド ライン インターフェイスの使用」を参照してください。

バックアップ ファイルの格納場所が HPCA Core Server であるか、管理対象デバイスのローカル ハード ディスクであるかに関わらず、バックアップ ファイルが自動的に削除されることはありません。特定のデバイスのバックアップ データが不要になった場合は、HPCA 管理者がそのバックアップ データを手動で削除できます。

HPCA Personality Backup and Restore Utility の使用

HPCA Personality Backup and Restore Utility は、USMT の使用法を簡略化するユーザー インターフェイスです。このユーティリティは、HPCA Agent のインストール時に、管理対象デバイスに配布されます。

開始する前に、HPCA Core Server、移行元および移行先の両方のコンピュータに、十分なディスク容量があることを確認してください (476 ページの「ディスク容量」を参照)。

Personality Backup and Restore Utility を起動するには :

管理対象デバイスで、[スタート] メニューから次のように選択します。

[すべてのプログラム] > [HP Client Automation Personality Backup and Restore] > [Client Automation Personality Backup and Restore Utility]

次のセクションでは、このユーティリティの使用方法について説明します。

- 483 ページの「パーソナリティのバックアップ」
- 485 ページの「パーソナリティの復元」

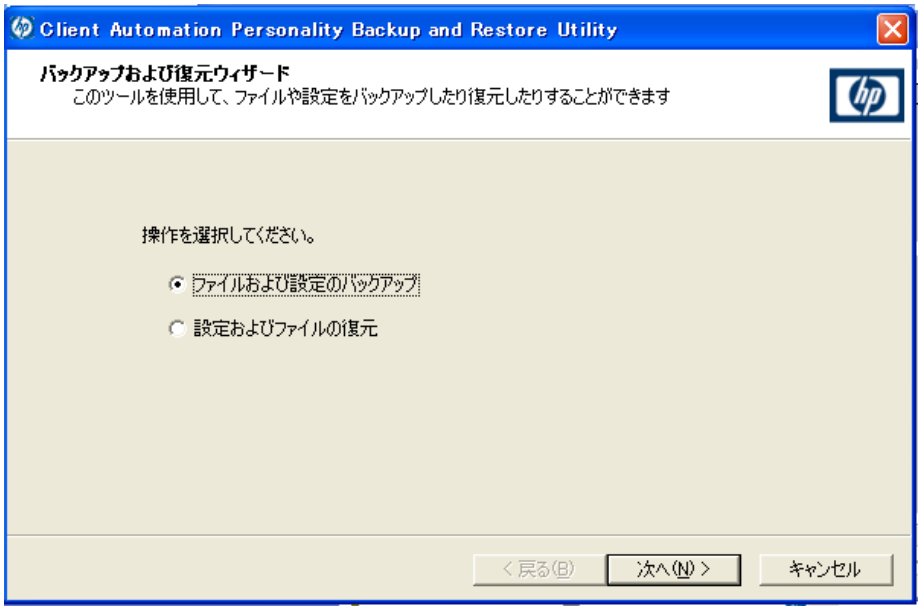
パーソナリティのバックアップ

管理者権限のあるユーザー アカウントから Personality Backup and Restore Utility を実行する必要があります。

バックアップが正常に行われるように、バックアップの実行前に、開いているファイルや実行中のアプリケーションはできる限り終了します。バックアップの実行中には、新しいアプリケーションを起動したり、ファイルを開いたりしないでください。バックアップが失敗する可能性があります。

ファイルと設定をバックアップするには :

1 管理対象デバイスで Personality Backup and Restore Utility を起動します (483 ページを参照)。



2 **[ファイルおよび設定のバックアップ]** を選択して、**[次へ]** をクリックします。[バックアップ] ダイアログ ボックスが表示されます。

3 バックアップするデバイスのコンピュータ名を入力します。

4 7 ～ 15 文字のパスワードを入力して、**[次へ]** をクリックします。[要約] ダイアログ ボックスが表示されます。

5 要約情報を確認します。ファイルと設定を復元するときに必要になるため、コンピュータ名と使用したパスワードを記録します。

6 **[完了]** をクリックしてバックアップ プロセスを開始します。バックアップされるデータの量によっては、このプロセスが完了するまでに数分から数時間かかることがあります。Personality Backup and Restore Utility からバックアップの完了が通知されるまで、アプリケーションは終了しないでください。

パーソナリティの復元

管理者権限のあるユーザー アカウントから Personality Backup and Restore Utility を実行する必要があります。

復元が正常に行われるように、復元の実行前に、開いているファイルや実行中のアプリケーションはできる限り終了します。復元の実行中には、新しいアプリケーションを起動したり、ファイルを開いたりしないでください。復元が失敗する可能性があります。

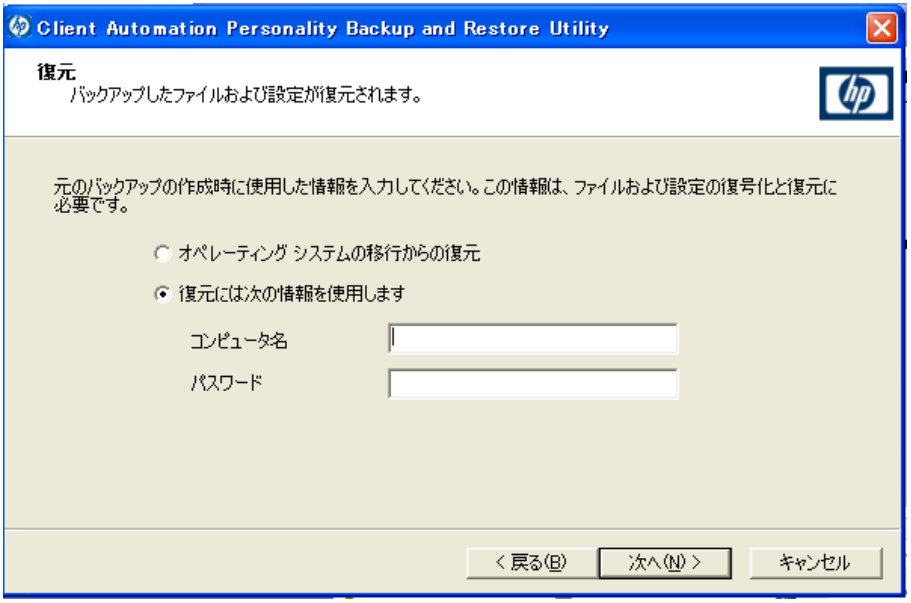
復元手順を開始する前に、設定を移行するすべてのアプリケーションを、移行先コンピュータにインストールする必要があります。注 : (新しいバージョンが使用できる) Microsoft Office 以外のすべてのアプリケーションについては、移行元コンピュータにインストールされているものと同じバージョンのアプリケーションを、移行先コンピュータにインストールする必要があります。

バックアップで使用されたドメインと同じ Windows ドメインにあるコンピュータに復元します。また、バックアップで使用されたロケールと同じロケール (例、米国英語) で復元します。

ファイルと設定を復元するには

1 移行先コンピュータで Personality Backup and Restore Utility を起動します (詳細については、483 ページを参照)。

2 **[設定およびファイルの復元]** を選択して、**[次へ]** をクリックします。[復元] ダイアログ ボックスが表示されます。



3 次のいずれかの操作を実行します。

— Personality Backup and Restore Utility でバックアップしたファイルおよび設定を復元するには、次の手順を実行します。

a **[復元には次の情報を使用します]** を選択します。

b バックアップ時に使用した **[コンピュータ名]** および **[パスワード]** を入力します。

— 移行を有効にした前回のオペレーティング システムの配布時に格納されたファイルと設定を復元するには、**[オペレーティング システムの移行からの復元]** を選択します。

4 **[次へ]** をクリックします。[要約] ダイアログ ボックスが表示されます。

5 **[完了]** をクリックして復元プロセスを開始します。復元されるデータの量によっては、このプロセスが完了するまでに数分から数時間かかることがあります。Personality Backup and Restore Utility から復元の完了が通知されるまで、アプリケーションを終了しないでください。

6 フォント、壁紙、スクリーン セーバー設定などの一部のオペレーティング システム設定は、移行先コンピュータを再起動するまで適用されません。これらの設定がすべて正常に適用されるように再起動を実行してください。

コマンド ライン インターフェイスの使用

HPCA Personality Backup and Restore コマンド ライン インターフェイスを使用して、管理対象デバイスのファイルと設定をバックアップしたり、復元したりできます。

構文は次のとおりです。

InstallDir\Agent\pbr.exe /B|/R [/localstore]

この場合の *InstallDir* は HPCA Agent のインストール先の場所です。デフォルトでは、これは C:\Program Files\Hewlett-Packard\HPCA です。

/B オプションを指定するとバックアップを実行し、/R オプションを指定すると復元を実行します。

例 1: HPCA Core Server のファイルおよび設定のバックアップ

InstallDir\Agent\pbr.exe /B

例 2: HPCA Core Server からの復元

InstallDir\Agent\pbr.exe /R

/localstore オプションを指定すると、ローカルのバックアップまたは復元操作を実行できます。この場合、ユーザー データは HPCA Core Server ではなく管理対象デバイスのローカル ハード ディスクに格納されます。または、ローカル ハード ディスクから復元されます。

例 3: ファイルおよび設定のローカルでのバックアップ

InstallDir\Agent\pbr.exe /B /localstore

例 4: ローカル バックアップ後の復元

InstallDir\Agent\pbr.exe /R /localstore

Personality Backup and Restore サービスの使用

HPCA が提供する次の 2 つの組み込みのサービスがあります。このサービスでは、ユーザー ファイルおよび設定のバックアップおよび復元のプロセスを自動化できます。

- HPCA Personality Backup (HPCA_PBR)
- HPCA Personality Restore (HPCA_RESTORE)

どちらのサービスも `pbr.exe` アプリケーションを起動します。これらのサービスは、オペレーティング システムの配布を行う状況で特に役立ちます。HPCA ライセンスのタイプに応じて、プロセスの動作が若干異なります。

HPCA Personality Backup サービス (`pbr.exe /B`) を使用してバックアップを実行した場合は、HPCA Personality Restore サービスを使用してのみユーザー データを復元できます。このユーティリティを使用してバックアップを実行した場合は、復元を実行する場合にもこのユーティリティを使用する必要があります。

HPCA Enterprise で OS 配布の一部としてユーザー データを移行するには

1 次の項目が、この OS 配布の一部であるすべての管理対象デバイスにインストールされていることを確認します。

   — HPCA Agent

   — USMT

2 配布する OS イメージに、デフォルトの場所にインストール済みで、使用環境に合わせて適切に設定してある USMT があることを確認します。

   または、OS 配布の直後に管理対象デバイスに USMT をインストールして設定します (477 ページの「USMT について」を参照)。

   HPCA がデフォルトの場所にインストールされている USMT を検出できなかった場合は、バックアップも復元も機能しません。

3 HPCA Policy Wizard を使用して、HPCA Personality Backup (HPCA_PBR) サービスに管理対象デバイスを付与します。

4 OS を配布します。HPCA Personality Backup サービスは、新しい OS をインストールする前に、各管理対象デバイス上で実行されます。バックアップ ファイルは HPCA Core Server に格納されます。

5 OS の配布が完了したら、HPCA Personality Restore (HPCA_Restore) サービスに各管理対象デバイスを付与します。

6 通知ジョブを作成して、HPCA Personality Restore サービスを各管理対象デバイスに配布します。

トラブルシューティング

このセクションでは、バックアップまたは復元が正常に完了しなかった場合に実行できるトラブルシューティング操作について説明します。

バックアップまたは復元が正常に完了しなかった

バックアップまたは復元が正常に完了しなかった場合は、Agent の Log ディレクトリにある pbr.log で、バックアップまたは復元時に発生したエラーを確認します。デフォルトの Log ディレクトリは、次のディレクトリです。

```
C:\Program Files\Hewlett-Packard\HPCA\Agent\Log
```

/localstore オプションを指定して pbr.exe を使用する場合、ログ ファイルは次のディレクトリに保存されます。

```
C:\OSMGR.PRESERVE\PBR.work\log
```

また、バックアップと復元時にそれぞれ作成された ScanState.log および LoadState.log ファイルを確認することもできます。これらのファイルは、Agent の Lib ディレクトリの下の PBR\work\log ディレクトリにあります。デフォルトの Lib ディレクトリは、次のディレクトリです。

```
C:\Program Files\Hewlett-Packard\HPCA\Agent\Lib
```

ユーザーがパスワードを忘れたためデータを復元できない

Personality Backup and Restore Utility を使用して復元を実行するには、バックアップでユーザーが入力したコンピュータ名とパスワードの両方が必要です。紛失したパスワードを回復する方法はありませんが、管理者はユーザーが復元を実行できるように新しいパスワードを作成できます。このプロセスは次のとおりです。

1. 管理者がユーザー ファイルと設定が格納されている HPCA Core Server のバックアップ ディレクトリを検索します。このディレクトリは、*DataDir*\PersonalityBackupAndRestore\backups にあります。この場合の *DataDir* は、HPCA Core のインストール時に指定した、ユーザーが設定できるデータ ディレクトリです。サブディレクトリの名前は次のとおりです。

   ComputerName_EncodedComputerNameAndPassword

2 管理者は Personality Backup and Restore Utility を使用してバックアップを実行します。このバックアップは、ユーザーがパスワードを忘れたコンピュータでは実行 *しない*でください。バックアップはそれ以外のマシン、できればバックアップの高速化を図るために、ユーザー データが少ないかまったくないマシンで実行します。

   このバックアップを実行するには、管理者は元のバックアップに使用したものと同じコンピュータ名 (前述のバックアップ フォルダ名の一部) を入力し、復元を実行するエンド ユーザーに支給するパスワードを作成する必要があります。

3 管理者は、*Data*\PersonalityBackupAndRestore\backups の下に作成された新しいディレクトリを見つけて、そのディレクトリの *内容*を削除し、手順 1 で説明した元のバックアップ ディレクトリの内容をコピーします。

4 エンド ユーザーは、Personality Backup and Restore Utility を実行し、元のコンピュータ名と管理者が作成したパスワードを入力して、自分のファイルと設定の復元を行います。

注 : エンド ユーザーが、パスワードを忘れたが過去のバックアップからデータを復元する必要がない場合は、次回バックアップを実行するときに新しいパスワードを入力すれば、そのパスワードを使用して復元を実行できます。

16 トラブルシューティング

次のセクションを使用して、HPCA の使用中に遭遇する一般的な問題のトラブルシューティングを行います。

ログ ファイル

HPCA の各種ログ ファイルは、サーバー上の `C:\Program Files\Hewlett-Packard\HPCA` 以下の次のディレクトリに格納されています。

- `\Agent\Log`
- `\ApacheServer\logs`
- `\ApacheServer\apps\cas\logs`
- `\ApacheServer\apps\console\logs`
- `\BootServer\logs`

- \ClientConfigurationManager\logs
- \ConfigurationServer\log
- \dcs\log
- \DistributedCS\logs
- \Knowledge Base Server\logs
- \ManagementPortal\logs
- \MessagingServer\logs
- \MiniManagementServer\logs
- \MulticastServer\logs
- \OOBM\logs
- \OSManagerServer\logs
- \PatchManager\logs
- \PolicyServer\logs
- \ProxyServer\logs
- \ReportingServer\log
- \tomcat\logs
- \VulnerabilityServer\logs

ログ ファイルのサイズは、時間が経過するにつれて大きくなります。ログには、HPCA サービスの動作中に使用されるものもあります。これらのアクティブなログ ファイルを削除しないでください。履歴ログ ファイルは必要に応じてアーカイブしたり削除したりできます。

ログファイルは、HPCA Core Console の [サポート] ページの [インフラストラクチャ管理] 領域にある [操作] タブを使用してダウンロードできます。

OS 配布の問題

この章では、オペレーティング システム イメージの配布中に遭遇する一般的な問題について説明します。

TFTP サーバーが起動後にシャットダウンする

- 同じコンピュータで他の TFTP サーバーが動作していないことを確認します。

PXE がサブネットを横断できない

- PXE がサブネットを自由に移動するには、DHCP ヘルパーが有効である必要があります。DHCP ヘルパーは、DHCP ポートでのブロードキャスト トラフィックの横断を許可します。通常、ブロードキャストはルータではオフになっています。

Application Self-Service Manager の問題

このセクションでは、HP Client Automation Application Self-service Manager (ASM) のよくある問題および問題を解決する手順を説明します。

アプリケーションのインストールが失敗し、カタログにはインストールされたと表示される

問題

インストール プログラムが失敗時にゼロを返すと、カタログには、アプリケーションがインストールされたと表示される場合があります。

対処法

ASD は、インストールが成功したかどうかを検出するのに、リターン コードを信頼しています。ASM が失敗を検出するには、インストールはゼロ以外のコードを返す必要があります。

このためには、インストールをコマンド ファイルにラッピングし、正しいコードを返すことでプロセスが成功したかどうかを確認するロジックを使用します。

電源管理の問題

このセクションでは、HPCA の電源管理機能に関連するタスクの問題と対処法を説明しています。

デバイスが HPCA Server からの電源コマンドに応答しない

管理対象デバイスが、HPCA Server からの電源オン コマンドに応答しない場合、ルータやスイッチなどのネットワーク デバイスの設定に問題があることがあります。

- Wake on LAN サポートについて、HPCA Server から管理対象デバイスへのネットワーク パスをテストします。ネットワーク デバイスにリモートの電源オン コマンドを送信するためのサード パーティ製ツールが、いくつかあります。インターネットで「Wake on Lan ツール」を検索すると、この機能をテストするための無料のツールが見つかります。

パッチ管理の問題

このセクションでは、パッチ管理に関連するタスクの問題と対処法を説明しています。

パッチ配布時のエラー

ターゲット デバイスへのパッチの配布時にエラーが発生する場合 (`WUA Install Result Code 3 HRESULT $hresult` などのエラー メッセージが表示されます)、パッチの更新を受け取るターゲット デバイスに適切なバージョンの Windows インストーラがインストールされているかを確認します。

HPCA Server のトラブルシューティング

次のセクションでは、HPCA Server に関する問題のトラブルシューティングについて説明します。

- 496 ページの「HPCA Core コンポーネントのトラブルシューティング」
- 500 ページの「HPCA Satellite コンポーネントのトラブルシューティング」

HPCA Core コンポーネントのトラブルシューティング

次のセクションでは、Core Server のコンポーネントに関連する問題のトラブルシューティングについて説明します。

HPCA Cpre の設定ファイル

Core Server のインストールでは、さまざまな Core Server コンポーネントのデフォルト値が設定されます。これらの値は変更する必要がありませんが、一部の値は Core Console で変更できます。次の表では、トラブルシューティングに必要な場合または HP テクニカル サポートからリクエストされた場合に備えて、設定ファイルの場所と名前を一覧表示します。

Core Server の製品設定ファイルへのデフォルトのパスは、`C:\Program Files\Hewlett-Packard\HPCA\xxxxxx` です。Core のインストール中に異なるパスを指定した場合、そのパスに従ってください。*xxxxxx* の値は、次の表の場所カラムの値で置き換えます。

表 43　　HPCA Cpre の設定ファイル

HPCA 製品	設定ファイルのタイプ	場所とファイル名 (C:\Program Files\Hewlett-Packard\HPCA\...)
HPCA Console	Apache Server	ApacheServer\apps\console\etc\service.cfg
	Apache Server	ApacheServer\apps\console\etc\proxy.cfg
	Sessionmanager	tomcat\webapps\sessionmanager\WEB-INF\sessionmanager.properties
	Sessionmanager	tomcat\webapps\sessionmanager\WEB-INF\classes\log4j.properties
Configuration Server		ConfigurationServer\bin\edmprof.dat
Distributed Configuration Server	Integration Server	DistributedCS\etc\HPCA-DCS.rc
	product	DistributedCS\etc\dcs.cfg
Messaging Server		MessagingServer\etc\core.dda.cfg

表 43　　HPCA Cpre の設定ファイル

HPCA 製品	設定ファイルのタイプ	場所とファイル名 (C:\Program Files\Hewlett-Packard\HPCA\...)
		MessagingServer\etc\patch.dda.cfg
		MessagingServer\etc\rms.cfg
		MessagingServer\etc\usage.dd.acfg
OS Manager Server		OSManagerServer\etc\HPCA-OSM.rc
		OSManagerServer\etc\roms.cfg
		OSManagerServer\etc\roms_upd.cfg
Patch Manager		PatchManager\etc\HPCA-PATCH.rc
		PatchManager\etc\patch.cfg
Policy Server		PolicyServer\etc\HPCA-PM.rc
		PolicyServer\etc\pm.cfg
Portal	Integration Server	ManagementPortal\etc\HPCA-RMP.rc
	product	ManagementPortal\etc\rmp.cfg
		ManagementPortal\etc\romad.cfg
	OpenLDAP	DirectoryService\openldap
Reporting Server		ReportingServer\etc\cba.cfg
		ReportingServer\etc\ccm.cfg
		ReportingServer \etc\ed.cfg
		ReportingServer\etc\rim.cfg
		ReportingServer\etc\rm.cfg

表 43　　HPCA Cpre の設定ファイル

HPCA 製品	設定ファイルのタイプ	場所とファイル名 (C:\Program Files\Hewlett-Packard\HPCA\...)
		ReportingServer\etc\rpm.cfg
		ReportingServer\etc\rrs.cfg
		ReportingServer\etc\rum.cfg
		ReportingServer\etc\scm.cfg
		ReportingServer\etc\vm.cfg
シン クライアント		TC\etc\HPCA-TC.rc TC\etc\rmms.cfg
Tomcat	Enterprise Manager	tomcat\webapps\em\WEB-INF\ Console.properties
	Enterprise Manager	tomcat\webapps\em\WEB-INF\classes\log4j.properties
	OPE	tomcat\webapps\ope\WEB-INF\classes\ log4j.properties（ログ レベル）
	VMS	tomcat\webapps\vms\WEB-INF\classes\ log4j.properties（ログ レベル）

HPCA Core のログ ファイル

Core Server に問題があり、トラブルシューティングのためにそのログ ファイルにアクセスする必要がある場合、Core Console ではすべてのログ ファイルに即座にアクセスできます。

Core Server のログ ファイルを生成するには

1　Core Console の [操作] タブで、**[サポート]** をクリックします。

2　[トラブルシューティング] 領域で、**[現在のサーバー ログ ファイルをダウンロード]** をクリックします。

3　WinZip ファイルを開くと、ファイルが展開され、保存されます。

ファイルのすべての内容を理解する必要はありませんが、次の場合のためにこれらのファイルのアクセス方法および表示方法は知っておく必要があります。

- HP サポートにログ ファイルを提出する。
- 「**severe**」ラベルが付与されたエントリを確認する。

HPCA Satellite コンポーネントのトラブルシューティング

次のセクションでは、Satellite コンポーネントのトラブルシューティング方法について説明しています。

- 500 ページの「HPCA Satellite のログ ファイル」

HPCA Satellite のログ ファイル

Satellite Server に問題があり、トラブルシューティングのためにそのログ ファイルにアクセスする必要がある場合、Satellite Console ではすべてのログ ファイルに即座にアクセスできます。

Satellite Server のログ ファイルにアクセスするには

1. Satellite Console の [操作] タブで、**[サポート]** をクリックします。
2. [トラブルシューティング] 領域で、**[現在のサーバー ログ ファイルをダウンロード]** をクリックします。
3. WinZip ファイルを開くと、ファイルが展開され、保存されます。

ログのすべての内容を理解する必要はありませんが、次の場合のためにこれらのログのアクセス方法および表示方法は知っておく必要があります。

- HP サポートにログ ファイルを提出する。
- 「**severe**」ラベルが付与されたエントリを確認する。

ブラウザの問題

次のトラブルシューティングのヒントは、ブラウザで発生する問題に関するものです。

- 501 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」
- 501 ページの「Internet Explorer 6 と SSL を使用して HTTP 1.1 を有効化できない」

F5 キーを使用してページをリフレッシュできない

HPCA Console の使用時に **F5** ファンクション キーを押すと、起動画面が短く表示され、最後に表示されていたダッシュボード ページに戻ります。現在表示されているページをリフレッシュできません。

解決策 :

現在表示されているページをリフレッシュするには、ページ内の  (リフレッシュ) ボタンを使用します。

Internet Explorer 6 と SSL を使用して HTTP 1.1 を有効化できない

HTTP 1.1 が有効な場合、SSL が有効である Internet Explorer 6 を使用して HPCA Console を実行できません。これは、Internet Explorer 6 の制限事項です。

解決策 :

Internet Explorer 6 のサポートは終了しました。Internet Explorer 7 以上にアップグレードする必要があります。

リモート制御を使用するとブラウザでエラーが発生する

HPCA Console から VNC またはリモート アシスタンスのリモート制御機能を開始すると、次のメッセージが表示される場合があります。

1 つのプロセスで複数の Java 仮想マシンが実行されることによってエラーが発生しました

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。

502 ページの「DTM ジョブが正しく動作しない / RMP ジョブが見つからない」

DTM ジョブが正しく動作しない / RMP ジョブが見つからない

従来の CAE インストールでは、ターゲットがグループである場合の DTM ジョブの実行時に、Enterprise Manager が正しくすべてのターゲット デバイスを解決するには、インストール後の手動作業が必要です。

この作業は、すべての RMP エージェント配布ジョブおよび OS 配布ジョブが **[現在のジョブ]** および **[過去のジョブ]** のリストに含まれるようにするためにも必要です。

このタイプのジョブの詳細については、174 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\:// *または* 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。373 ページの「ダッシュボード」を参照してください。

ダッシュボード ペイン読み込み状態が終了しない

次の両方の製品がインストールされているシステムで HPCA Console 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読み込み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、レポート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。

`アプリケーション ポップアップ : nvdkit.exe - アプリケーション エラー : ...`

解決策 :

これらの両方のプログラムを、HPCA Console をホストしているシステム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 {`*`RSS フィードの URL`*`} 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	Error processing refresh: connection timed out: connect
Live Network のパスワードが無効	Error processing refresh: Invalid Response: Login failed
フィードに登録していない	Error processing refresh: Error on line -1: premature end of file

解決策 :

次を確認してください。

1. RSS フィードの URL が正しいことを確認する
2. RSS フィード サイトにアクセスできる。RSS フィード サイトの URL をブラウザに張り付けて確認します。
3. HPCA Console のプロキシ設定が正しく指定されている。
4. HP Live Network 告示のフィードについて、次を確認してください。
   a. HP Live Network の登録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。

セキュリティと適合性の問題

次のトラブルシューティングのヒントは、セキュリティと適合性の設定、スキャン、およびレポートに関するものです。

- 507 ページの「HP Live Network コネクタが接続できない」

- 507 ページの「管理対象デバイスおよびスキャン済みデバイスの数がゼロである」
- 507 ページの「レポートの表示が遅い」

HP Live Network コネクタが接続できない

この問題で考えられる最も可能性が高い原因は、プロキシ サーバーの誤設定です。HPCA Console がインストールされているシステムで、インターネットに接続するためにプロキシが必要な場合、[プロキシ設定] 設定ページの [HTTP プロキシ] タブでプロキシ サーバーを指定する必要があります。

HPCA Console では、[HTTP プロキシ] 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済みデバイスの数がゼロの場合、レポート サブシステムに問題があることを示しています。

詳細については、HPCA 管理者にお問い合わせください。

レポートの表示が遅い

脆弱性、適用状況、またはセキュリティ ツールの管理レポートの HPCA Console 内での表示が遅い場合、レポートのキャッシングを有効にする必要があります。

解決策 :

1 Web ブラウザを開いて、次のように入力します。

`http://InstallHost:3466/reportingserver/setup.tcl`

ここで、*InstallHost* は HPCA がインストールされているシステムのホスト名または IP アドレスです。

設定ファイルのページが表示されます。

2 左ナビゲーション メニューで、**[脆弱性管理設定]** をクリックします。

3 次の 2 つのオプションを設定します。

a **[VM レポートのキャッシングを有効化]** オプションで、ドロップダウン リストから「1」を選択します。

b **[VM キャッシュの存続期間]** を秒単位で指定します。たとえば、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。

- 509 ページの「SQL Server データベースの設定の問題」
- 510 ページの「英語以外の環境でのレポート チャートの表示の問題」
- 510 ページの「レポートを開けない」

SQL Server データベースの設定の問題

初回セットアップ ウィザードまたは設定 UI から SQL Server データベースを設定すると、設定を正常に完了できないという問題が発生する場合があります。設定には、レポート データベース DSN、ユーザー ID、パスワード、サーバー、およびポートの指定が必要です。この設定を設定できない理由はさまざまです。

考えられる原因を以下にリストします。

- SQL Server のデフォルトのスタティック ポートは 1433 ですが、SQL Server のインストールが別のスタティック 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があります。HPCA では、スタティック ポートを使用する必要があります。SQL Server のポート設定を確認し、適切に更新してください。
- [サーバーのホスト] は、データベースが存在するホストの名前です。例 :

  ```
  mydbserver.mycompany.com
  ```

- SQL Server のセットアップでデフォルトのデータベース以外のインスタンスが使用されている場合、インスタンスをサーバー名に追加する必要があります。たとえば、指定されたインスタンスが HPCA である場合、次のように指定します。

  ```
  mydbserver.mycompany.com\HPCA
  ```

- SQL Server の認証設定を確認します。Windows 認証を使用している場合は、SQL Server の認証を使用してからレポート データベースの設定を適切に更新する必要があります。

英語以外の環境でのレポート チャートの表示の問題

英語以外の環境では、レポート チャートで特定の文字列に疑問符 (??) 文字が表示されます。このように誤って表示されるのは、クライアント デバイスにインストールされている JAVA JRE クライアントに英語以外のフォントのファイルがないことが原因です。

解決策 :

これは、`fonts.properties` ファイルに関する一般的な Java の問題です。この問題を解決するためには、JDK ホーム ディレクトリの `font.properties` ファイルを特定の英語以外の環境向けのものに置き換える必要があります。たとえば、日本語環境では、`font.properties.ja` ファイルを使用して、オリジナルのフォント ファイルに置き換える必要があります。

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 [レポート] ホーム ページが表示される。

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、レポート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。

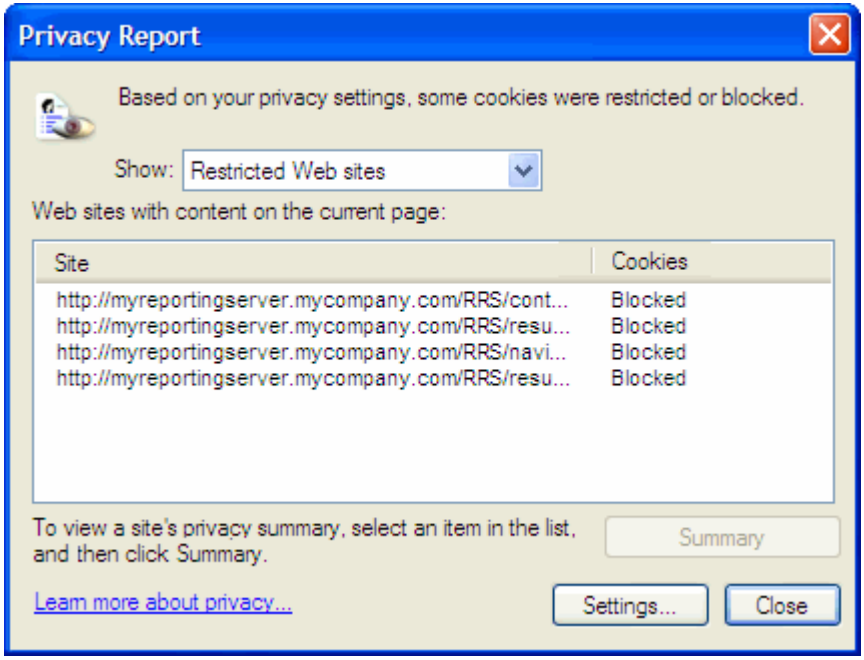
この動作は、Windows 2003 Server プラットフォーム上の Internet Explorer 7 で最も多く見られます。また、すべてのサポート対象プラットフォームでも発生する可能性があります。

解決策 :

1 ブロックされた URL のリストを開きます。

たとえば、Internet Explorer 7 では、ブラウザの下側のバーに表示された赤い丸印が付いた目の形のアイコンをクリックします。

次のようなダイアログが表示されます。



2 ブラウザのプライバシー設定を使用して、表示するレポートの URL を、cookie の使用が**許可される**サイトの一覧に追加します。

追加のパラメータが HPCA ジョブのウィザードで無視される

HPCA ジョブ作成ウィザードの使用時に「追加のパラメータ」を指定する場合、次の形式に従う必要があります。

```
option=value
```

この形式を使用しない場合は、追加のパラメータは無視されます。確認ページ (ウィザードの最後のページ) で、追加のパラメータがコマンド ラインに含まれていることを必ず確認してください。

仮想マシンが起動しない

ESX バージョン 3.5 Update 2 (ビルド番号 103908) のライセンスの欠陥により、特定の日付以降に仮想マシンが起動できなくなります。

このビルドの ESX を実行している場合に HPCA Console から仮想マシンを起動しようとすると、次のようなエラー メッセージがコンソールに表示されます。

結果： " マシン「< *マシン名* > 名の起動に失敗しました "

詳細： " タスク haTask-##-vim.VirtualMachine.powerOn-##### の実行中にメソッド障害を受け取りました : 一般システム エラーが発生しました : 内部エラー。 "

解決策 :

ESX バージョン 3.5 Update 2 build 110268 (またはそれ以降) をインストールしてください。

詳細については、この更新に関する VMware の次の *リリース ノート*を参照してください。

http://www.vmware.com/support/vi3//doc/vi3_esx35u2_vc25u2_rel_notes.html

クエリが限界に達しました

デフォルトでは、Active Directory オブジェクトの最初の 1000 件のメンバーのみが HPCA Console に表示されます。1000 件を超えるメンバーを持つ Active Directory オブジェクトを参照しようとすると、「クエリが限界に達しました」というエラー メッセージが表示されます。

推奨される解決策 :

検索機能を使用して、表示されるメンバーを微調整してください。

代替解決策 :

HPCA 管理者は、HPCA Console の Console.properties ファイルで directory_object_query_limit を指定できます。このファイルは次のディレクトリに格納されています。

<*tomcatDir*>\webapps\em\web-inf\Console.properties

<*tomcatDir*> のデフォルト値は次のとおりです。

C:\Program Files\Hewlett-Packard\HPCA\tomcat

Console.properties ファイルを変更した後は、必ず HPCA Tomcat サービスを再起動してください。

directory_object_query_limit プロパティを変更すると、HPCA Console のパフォーマンスに悪影響を与える場合があります。

スマート カードのアクセスに関する問題

スマート カードのアクセスに関する問題は、519 ページの「スマート カードのアクセスに関する問題のトラブルシューティング」の「付録 A、「HPCA Core Server と HPCA Satellite Server での SSL 設定」」で扱います。

A HPCA Core Server と HPCA Satellite Server での SSL 設定

HPCA Console で設定可能な SSL 設定値の使用方法を十分に理解するには、SSL のさまざまな「構成要素」およびその機能について理解することが重要です。この付録では、HPCA 環境との関連を含めた SSL の概要を示します。詳細は、次のセクションを参照してください。

- 515 ページの「SSL の構成要素」
- 516 ページの「HPCA 環境での SSL」
- 517 ページの「Console の SSL 証明書フィールド」
- 519 ページの「スマート カードのアクセスに関する問題のトラブルシューティング」

詳細については、『HP Client Automation SSL 実装ガイド』を参照してください。

SSL の構成要素

次の構成要素の概要については、『HP Client Automation SSL 実装ガイド』の第 1 章を参照してください。

- 証明書
- 認証局
- 証明書の生成
- プライベート キー ファイル
- パブリック キー ファイル

HPCA 環境での SSL

SSL では、ID を確証し、セキュアな通信を実現するための共有**暗号鍵**を確立するために、**デジタル証明書**を使用します。SSL の使用方法は、インフラストラクチャ コンポーネント間の通信方法に応じて異なります。このセクションでは、SSL を有効にすべき 2 つの主な例と、それぞれの例における SSL の役割について説明します。

SSL 認証局、SSL 証明書、および SSL 証明書の生成の詳細については、『HP Client Automation SSL 実装ガイド』の第 1 章を参照してください。

リモート サービスへの SSL 通信のサポート

Core Server と Satellite Server の間の通信をセキュリティ保護する必要がないと想定される場合、それらのサーバー間の SSL 接続は不要です。ただし、Core Server または Satellite Server が、外部サーバー (ベンダーの Web サイトをホストするサーバーなど)、他の HPCA Server、および Active Directory と通信する場合には、セキュアな通信 (LDAPS) が必要です。

これら他のサーバーが主張するとおりの「サーバー」であることを信頼できるようにするため、Core または Satellite は、各サーバーの**パブリックな証明書**または発行**認証局** (CA) の署名を取得する必要があります。Core または Satellite では、認証局から取得した **CA 証明書ファイル**も必要であり、他のサーバーでそれを入手できるようにして、Core または Satellite からのメッセージを復号化できるようにする必要があります。(Core および Satellite のインストールには、ほとんどの環境に適しているデフォルトの信頼された認証機関 `ca-bundle.crt` のセットが含まれています)。

コンシューマへのセキュアな通信サービスの提供

Core Server と Satellite Server の間の通信をセキュリティ保護する必要がある環境を想定します。この場合、Core はサーバーの役割を持ち、Satellite と共有可能なパブリック証明書が必要になります。Core Server のパブリック証明書には、そのパブリック キー、サーバー名、および (サーバーの ID を証明する) 認証局からの署名が含まれています。

- パブリック証明書 (**サーバー証明書**) は、自分を信頼してもらいたいユーザーすべてに与えることができます。

さらに、各 Satellite Server は「クライアント」の役割を持ち、Satellite と Core の間でメッセージの暗号化と復号化を実行できるように独自の証明書セットが必要になります。証明書は、その Satellite を証明するもので、Core がその Satellite を識別できるようにします。

個々の Core および Satellite は、メッセージを復号化するために独自のプライベート キーも必要になります。

- **プライベート証明書 (プライベート キー)** は、非公開の状態を維持し、一切共有しないでください。

Console の SSL 証明書フィールド

HPCA Console の [設定] タブの [インフラストラクチャ管理] 領域には、SSL サーバー および SSL クライアント があります。このセクションでは、2 つの領域の違いとそれぞれの領域の必要性について説明します。HPCA の SSL セットアップを完了するには、この付録の情報を確認してから、291 ページの「インフラストラクチャ管理」を参照してください。

SSL 証明書、SSL 認証局、および SSL 証明書の生成の詳細については、『HP Client Automation SSL 実装ガイド』の第 1 章を参照してください。

SSL サーバー

パネルのこの領域を使用して、SSL を有効にし、HPCA Server のプライベート キー ファイル (`server.key`) とサーバー証明書ファイル (`server.crt`) をアップロードして保存します。これらのファイルは、(組織内で) 自己生成されたか、認証局から取得されたものです。これらのファイルの入手方法については、システム管理者にお尋ねください。

- プライベート キー ファイルは、対応するパブリック キーによってセキュリティ保護されたメッセージを復号化するために必要です。
- サーバー証明書ファイルは、SSL が有効になっているサーバーがこのホストを識別できるようにするために必要です。

ファイルがアップロードされると (場所を指定して **[保存]** をクリックすると)、これらのファイルは次の場所に保存されます。

`C:\Program Files\Hewlett-Packard\HPCA\ApacheServer\conf\ssl`。

このパスは 32 ビット オペレーティング システムの保存場所を示しています。64 ビット オペレーティング システムの保存場所は次のとおりです。

C:\Program Files (X86)\Hewlett-Packard\HPCA\ApacheServer\conf\ssl。

デフォルトでは、これらのファイルは上記の名前で保存されますが、ファイル名はカスタマイズできます。

SSL クライアント

パネルのこの領域を使用して、HPCA Server の CA 証明書ファイル (ca-bundle.crt) をアップロードして保存します。このファイルには、ほとんどの環境で十分な権限を持つ信頼された認証機関のデフォルトのセットが含まれており、HPCA Server が LDAPS または HTTPS のいずれかを介して別のサーバーと通信する場合にのみ必要になります。

認証局から組織に取得された既存の CA 証明書ファイルを使用することが可能です。このファイルを入手する必要がある場合は、システム管理者にお尋ねください。

- CA 証明書ファイルには、信頼された認証局の署名入り証明書が含まれており、着信クライアントが「信頼できる」ものであることを確認するために必要です。

ファイルがアップロードされると (場所を指定して **[保存]** をクリックすると)、そのファイルは次の場所に保存されます。

C:\Program Files\Hewlett-Packard\HPCA\ApacheServer\conf\ssl.crt。

このパスは 32 ビット オペレーティング システムの保存場所を示しています。64 ビット オペレーティング システムの保存場所は次のとおりです。

C:\Program Files (X86)\Hewlett-Packard\HPCA\ApacheServer\conf\ssl.crt。

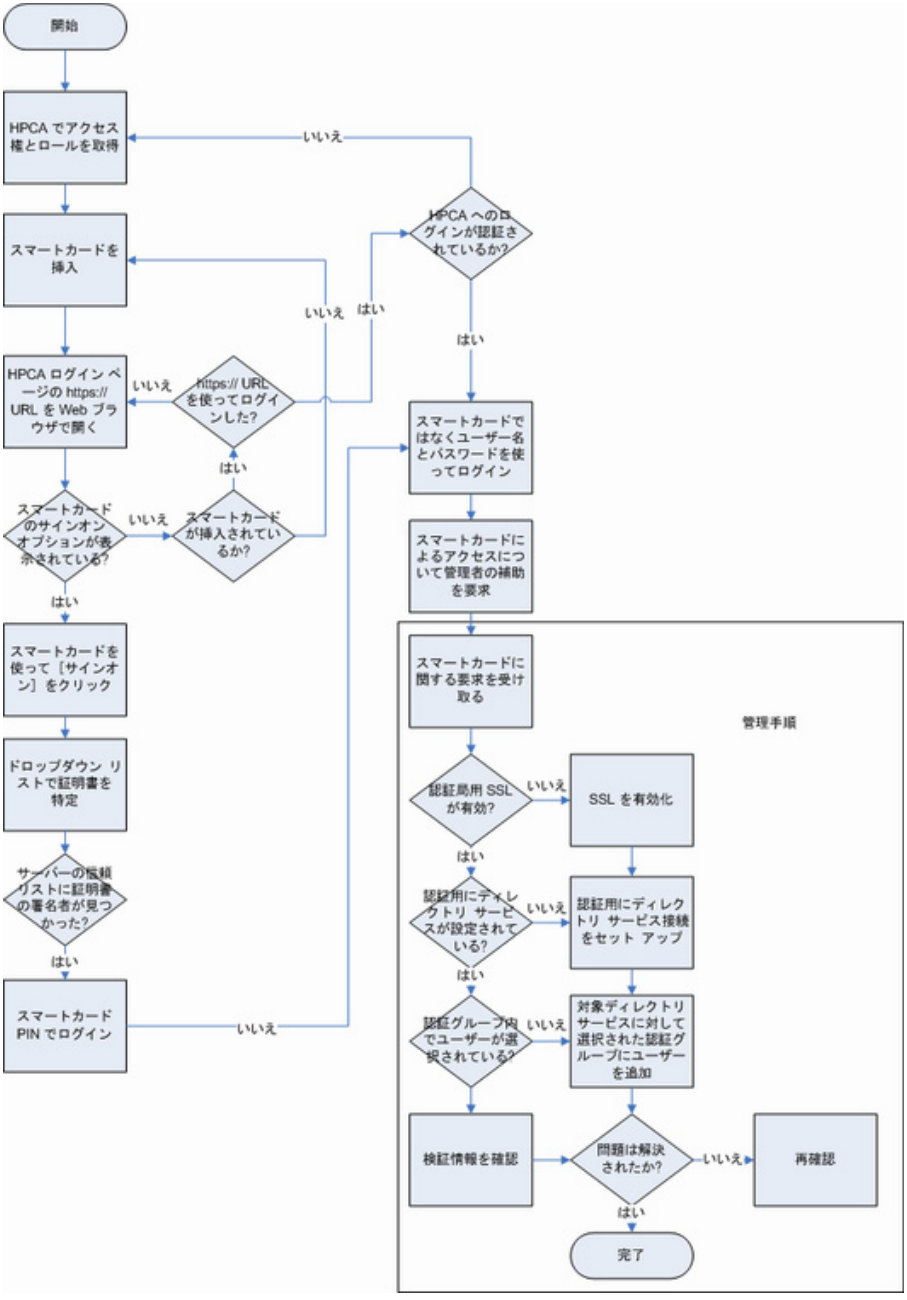
デフォルトでは、このファイルは上記の名前で保存されますが、ファイル名はカスタマイズできます。

スマート カードのアクセスに関する問題のトラブルシューティング

HPCA Console にログインしようとするときに発生する可能性がある、スマート カードへのアクセスに関する問題がいくつかあります。

次の図で、スマート カードのログイン プロセスに関連する手順を説明します。ここでは、通常プロセスの手順が失敗した場合の代替アクションと確認すべき質問事項を示しています。

図 58　　スマート カードのログイン プロセス



B Live Network の高度なトピック

このセクションでは、HP Live Network に関するより高度なトピックについて説明します。タスクには次が含まれます。

- 521 ページの「コマンド ライン ユーティリティの使用」
- 527 ページの「HP Live Network コネクタの手動での実行」
- 529 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」

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、[HP Live Network] ページ ([操作] タブの [インフラストラクチャ管理]) 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。

Core および Satellites: `<InstallDir>\HPCA\VulnerabilityServer\bin`

注 : 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、必須設定とオプションな設定の両方があります。注 : 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 (526 ページの「保存済み設定」を参照)。特定の設定の値を指定しない場合は、保存済み設定が使用されます。

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

content-update.bat コマンドの一般的な使用については、526 ページの「例」を参照してください。

必須設定

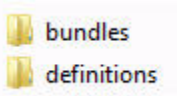
次の表は、content-update.bat コマンドの必須設定を示します。

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 (526 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 45　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 登録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。312 ページの「Live Network」を参照してください。 FILESYSTEM — ファイル システム内の場所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 システムの場所にそのコンテンツをダウンロードしておく必要があります。さらに、コマンド ラインまたは [操作] タブの [インフラストラクチャ管理] の下の [HP Live Network] ページのいずれかで、content_path 設定を指定する必要があります。312 ページの「Live Network」を参照してください。 CSDB_MASTER — 以前に Configuration Server Database (CSDB) にパブリッシュされたマスター コンテンツからコンテンツを取得します。このデータは、レポート データベースを読み込む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 コンテンツ 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。

表 45　　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 システムの場所への完全なパス。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。

オプションな設定

content-update.bat コマンドの次の設定はオプションです。

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 (526 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 46　content-update.bat のオプションな設定

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。 Core および Satellites: 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場所です。
livenetwork_username	HP Live Network 登録契約のユーザー名。
livenetwork_password	HP Live Network 登録契約のパスワード。
livenetwork_proxy_http_server	HP Live Network ダウンロード サイトへの接続に使用される HTTP プロキシ サーバー。このオプションは、次の形成である必要があります。 <http|https>://<*host*>:<*port*>

表 46　　content-update.bat のオプションな設定

設定	説明
livenetwork_proxy_http_username	HP Live Network ダウンロード サイトへの接続に使用される HTTP プロキシ サーバー (存在する場合) のユーザー名。
livenetwork_proxy_http_password	HP Live Network ダウンロード サイトへの接続に使用される HTTP プロキシ サーバー (存在する場合) のパスワード。
reporting_db_databasename	HPCA をインストールする前に作成したデータベース インスタンスの名前。『HPCA 入門ガイド』の「HPCA データベースの作成」のセクションを参照してください。
reporting_db_drivername	使用するデータベース ドライバの名前 (oracle または sqlserver のいずれか)。サポートされているドライバに対応している必要があります。
reporting_db_server	レポート データベースがある、ネットワーク アドレス指定可能なサーバーの名前。
reporting_db_port	レポート データベースのポート番号。ダイナミック ポートの場合は空白にする必要があります。スタティック ポートの場合は 1 ～ 65536 の範囲の値を指定する必要があります。
reporting_db_username	レポート データベースのユーザー名。
reporting_db_password	レポート データベースのパスワード。

保存済み設定

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

表 47　　content-update.bat の保存済み設定

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

例

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

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

例 2 — ローカル ディレクトリからコンテンツの更新を実行する

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

例 3 — ローカルの ZIP ファイルからコンテンツの更新を実行する

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

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

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

HP Live Network コネクタの手動での実行

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

1. インターネットにアクセスできるシステムで、HP Live Network 登録 Web サイトから HP Live Network コネクタを手動でダウンロードします。手順については、HP Software の営業担当者にお問い合わせください。
2. インターネットにアクセスできるシステムで、HP Live Network コネクタを実行します。
3. コンテンツを HPCA Core Server に転送します。
4. HPCA Core Server で、ファイル システムから HP Live Network コンテンツを更新します。65 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、522 ページの表 45 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。

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=<output-dir>
```

この場合、<output-dir> は HP Live Network コンテンツが保存される場所です。

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

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

HP Live Network コンテンツをダウンロードするには

インターネットにアクセスできるシステムで、次のコマンドを実行します。

```
<install-dir>\LiveNetwork\lnc\bin\live-network-connector.
bat
--url=https://bsaen-dist.hp.com
--username=<name>
--password=<password>
--product=hpca
--setting=hpca.installed_version=7.90.0
--setting=hpca.import_directory=<output-dir>
--stream=content.hpca_settings_mgmt
--stream=security.hpca_nvd
--stream=security.hpca_sectools_scanner
--stream=security.hpca_config --stream=security.hpca_oval
--stream=security.hpca_scap_scanner
--stream=content.hpca_config
--stream=security.hpca_sectools_services
--stream=security.hpca_scap_cis
--stream=security.hpca_scap_fdcc
```

ここで、*<brackets>* 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、*<install-dir>* は HP Live Network コネクタをインストールしたファイル システムの場所であり、*<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場所です。たとえば、*<output-dir>* が c:\temp の場合、フォルダ階層は c:\temp の下に作成されます。

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

次の手順

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

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

- [操作] タブの [インフラストラクチャ管理] の下の [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) の場所を指定します。
- 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) の場所を指定します。

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」関連の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、59 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 登録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** ツールを使用して関連する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.<*DOMAIN*>

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.<*DOMAIN*>

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、関連するデッキ 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 ツールを使用して関連するデッキをインポートします。

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

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

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

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

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

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

4 プロダクション環境で、先ほどインポートした関連するデッキ内の「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 データベースを読み込みます。

これには、次の 2 つの方法があります。

— **メソッド 1:** HPCA Console の使用

a [インフラストラクチャ管理] にある **[操作]** タブをクリックします。

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

c **[すぐに更新]** タブをクリックします。

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

e **[すぐに更新]** ボタンをクリックします。

[すぐに更新] タブの詳細については、312 ページの「Live Network」を参照してください。

— **メソッド 2:** content-update コマンドライン ユーティリティの使用

content-update.bat -content_source CSDB_MASTER

content-update コマンドの詳細については、521 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、関連するコンテンツ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。

C 2 バイト文字のサポートについて

このセクションでは、サービス オペレーティング システム (SOS) のロケールを設定する、設定の変更を説明します。詳細は、次のセクションを参照してください。

Image Preparation Wizard を使用してイメージを作成するときには、参照マシンとターゲット マシンの**ロケール**が一致する必要があります。たとえば、簡体中国語の OS イメージを作成する場合は、簡体中国語の参照マシンで Image Preparation Wizard を実行する必要があります。

- 533 ページの「サポートされる言語」
- 534 ページの「ロケールの変更」

2 バイト文字が必要でない場合は、以下の変更を行わないでください。

サポートされる言語

533 ページの表 48 に、サポートされる言語と有効な言語コードの一覧を示します。

表 48　　サポートされる言語とコード

言語	言語コード
韓国語	ko_KR
英語	ja
日本語	ja_JP
中国語 (簡体字)	zh_CN

ロケールの変更

PXE 環境でサポートされている言語にサポートを追加するには

1 テキスト エディタを使用して \X86PC\UNDI\linux-boot\linux.cfg \default を開きます。ファイルは次のように表示されます。

```
DEFAULT bzImage

APPEND initrd=rootfs.gz root=/dev/ram0 rw ISVR=10.10.10.1
ISVRPORT=3466
```

2 **LANG** パラメータを APPEND 行の最後に追加し、有効な言語コードを指定します (533 ページの表 48 を参照)。

結果として、言語が日本語に設定された、次の例のようなファイルが作成されます。

```
DEFAULT bzImage

APPEND initrd=rootfs.gz root=/dev/ram0 rw ISVR=10.10.10.1
ISVRPORT=3466 LANG=ja_JA
```

3 default ファイルを保存して閉じます。

サービス CD-ROM から復元するときにサポートされている言語にサポートを追加するには

- romsinfo.ini ファイルの ServiceCD セクションにある **LANG=*xx_XX*** を指定します。

  サポートされる言語と有効な言語コードの一覧については、533 ページの表 48 を参照してください。

- romsinfo.ini ファイルは、サービス CD iso の一部です。

Sysprep ファイルの 2 バイト文字サポート

Sysprep で 2 バイト文字サポートを使用する場合は、ファイルを UTF-8 でエンコードする必要があります。

D　レポートのパフォーマンスの強化

HPCA (Usage Manager) では、複数のスクリプトとマテリアライズド ビューを用意しています。このスクリプトとビューを Microsoft SQL Server データベースおよび Oracle データベースに適用すると、レポートのパフォーマンスを強化できます。

これらのスクリプトおよびビューは次の場所にあります。

- Microsoft SQL Server データベースの場合は `Media\Usage\Optional Features\SQL Server`
- Oracle データベースの場合は `Media\Usage\Optional Features\Oracle`

ビューの使用

ビューには、標準マテリアライズド ビューとフィルタ マテリアライズド ビューの 2 種類があります。どちらのビューもレポートのパフォーマンスを強化します。オプションで、いずれかのビューをデータベースに適用できます。各ビューの機能についての詳細は、スクリプトのコメントを参照してください。

スクリプト名では、`StepX_Define Filter Mat Tables` や `Indexes.sql` にあるように「Materialized」(マテリアライズド) を「Mat」と省略している場合があります。

[標準マテリアライズド ビュー (FMV)] - レポートがアクセスするすべてのビューをテーブルに変換します。このビューにはクエリの実行時間を改善するインデックスがあります。すべてのビュー (レポート アクセスの内容) をテーブルに変換する機能とインデックスが追加され、クエリの処理速度が高速化されます。

[フィルタ設定されたマテリアライズド ビュー (FMV)] - レポートがアクセスするすべてのビューをテーブルに変換します。ビューをテーブルに変換する前にフィルタを適用する必要があります。フィルタは個別のテーブルに格納されます。

たとえば、notepad.exe をフィルタとして選択すると、FMV テーブルにはすべてのデバイスの詳細がメモ帳を使用して入力されます。SMV と似ていますが、ビューをテーブルに変換するときにフィルタを適用する必要があるという点が異なります。フィルタは個別のテーブルに格納されます。例として、Notepad.exe のフィルタを選択する場合、FMV テーブルにはすべてのデバイスの詳細がメモ帳を使用して入力されます。

SMV または FMV のスクリプトを適用するには

1 **[HPCA Knowledge Base Server]** のサービスを停止します。このサービスは Windows の [コントロール パネル] の Administrative Tools\Services オプションを使用して停止および開始できます。

2 通常の手順で、所定の順序で次の場所にあるデータベース スクリプトを実行します。

— SQL Server の場合 :

```
\SQL Server\Optional Features\Filter Materialized Views
```

または、

```
\SQL Server\Optional Features\Standard Materialized Views
```

— Oracle の場合

```
\Oracle\Optional Features\Filtered Materialized Views
```

または、

```
\Oracle\Optional Features\Standard Materialized Views
```

上記の各場所には、データベースからビューを削除するのに使用するスクリプトも含まれています。たとえば、Microsoft SQL Server および Filtered Materialized Views のスクリプト名は次のとおりです。

```
SQLServer - Remove All Filter Mat Tables and Indexes.sql
```

ユーティリティ スクリプト

データベース管理者として、次のスクリプトを使用してレポート ビューのパフォーマンスを強化できます。

- Purge_Computer_Data.sql: コンピュータ名に関連付けられているすべてのデータを削除します。コンピュータ名が、スクリプト内の適切な場所に指定されている必要があります。デフォルト値は MYCOMPUTER です。

- Purge_User_Data.sql:　コンピュータ名とユーザー名に関連付けられているすべてのデータを削除します。コンピュータ名およびユーザー名が、スクリプト内の適切な場所に指定されている必要があります。デフォルト値は MYCOMPUTER および BOB です。
- Delete All Windows OS Files from Database.sql: Usage Manager データベースから Windows Operating System (OS) 関連のすべてのファイルを削除します。

Oracle 用のその他のスクリプト

その他のスクリプトは、ユーティリティ スクリプトとともに適用し、レポート ビューのパフォーマンスを強化できる追加のスクリプトです。

- Optional_Create_Public_Synonyms.sql: パブリック シノニムを作成します。スクリプトは Usage Manager のユーザー名向けに編集する必要がある場合があります。
- Optional_Drop_Public_Synonyms.sql: Optional_Create_Public_Synonyms スクリプトを使用して作成したパブリック シノニムを削除します。
- Step99a_DropAll.sql: Usage Manager データベースに存在するすべてのテーブルを削除します。

E IPv6 ネットワーキングのサポート

Client Automation Core Server および Satellite Server では、デュアル スタック (IPv4 と IPv6) 環境のネットワークでインターネット プロトコル バージョン 6 (IPv6) を使用するユーザーをサポートするための機能が追加されました。

この付録には次のトピックが含まれます。

IP ネットワーキングの用語と基本

このトピックでは、IP バージョン 4 と IP バージョン 6 に関連する用語と基本的な情報について説明します。

IP アドレスは、固有のデバイスまたはデバイスのポートを識別するための一意の数値です。IPv4 アドレスの 32 ビットのアドレス空間では、使用可能な固有アドレスの数の制限が厳しく、供給できるアドレスが残り少なくなっています。IPv6 の 128 ビットのアドレス空間は、この問題に対処するために作成されました。

用語

- **IPv4 アドレス :** IPv4 アドレスには、ピリオド (ドット) で区切られた 4 つのセクションが含まれます。オクテットと呼ばれる各セクションには、10 進数 (0 ～ 255) で表現された 8 ビットが含まれます。IPv4 アドレスを入力する場合、先行するゼロを省略できます。
- **IPv6 アドレス :** IPv6 アドレスには、コロンで区切られた 8 つのセクションが含まれます。各セクションには、大文字と小文字を区別しない 16 進数 (0000 ～ FFFF) で表現された 16 ビットが含まれます。

  例 : **`2001:0db8:0000:0001:f8f3:a7bb:2bcb:6037`**

  IPv6 アドレスを覚えやすく、入力しやすくするために、二重コロン (::) によって複数の連続したゼロからなるセクションを示すことができます。先行するゼロを省略することもできます。たとえば、アドレス **`2001:0db8:0000:0001:f8f3:a7bb:2bcb:6037`** を **`2001:db8:0:1:f8f3:a7bb:2bcb:6037`** または **`2001:db8::1:f8f3:a7bb:2bcb:6037`** に簡略化できます。
- **IPv6 アドレス タイプ**
  - **グローバル ユニキャスト アドレス** : これは、*外部通信*に使用できる IPv6 アドレスです。**`2001:db8:0:1:f8f3:a7bb:2bcb:6037`** はグローバル ユニキャスト アドレスの一例です。
  - **リンクローカル アドレス** : このアドレスは、*同じサブネット (リンク) 上の近隣ホストとの通信のみ*に使用できます。リンクローカル アドレスは、ルータによって転送されません。リンクローカル アドレスの構文では、最後に「%n」が追加されます。たとえば、**`fe80::20c:29ff:fed4:5ab%4`** のようになります。
  - **IPv4 マップ済みアドレス** : このアドレスは、IPv6 ネットワークで IPv4 アドレスをトンネリングするために使用できます。たとえば、**`fe80::5efe:192.168.6.154`** は、IPv4 アドレス **`192.168.6.154`** をトンネリングします。

IP アドレス ショートカット : IPv4 と IPv6

以下の表には、IPv4 と IPv6 の IP アドレス ショートカット規則がまとめられています。

表 49　　IPv4 と IPv6 の予約済み IP アドレス値

予約済みの意味	IPv4 値	IPv6 値
localhost	**127.0.0.1**	**::1**
任意のアドレス 任意のインターフェイス	**0.0.0.0**	**::**
IPv4/IPv6 のトンネリング	適用できません	**fe80::5efe:*<IPv4addr>*** この場合、***<IPv4addr>*** は、IPv4 アドレスです。例 : **fe80::5efe:192.168.1.2**

IPv6 アドレスへの角かっこの使用

URL、URI などの構文内の IPv6 のリテラル アドレスは、角かっこ ([と]) で囲み、その後に「:port」を続けられるようにする必要があります。例としては、HTTP、HTTPS、LDAP、および LDAPS エントリのスキームなどがあります。IPv6 アドレスを囲む角かっこは、IPv6 アドレス (コロンが含まれる) の開始と終了を、ポートの識別に使用するコロンと区別するために必要です。

例 :

http://[*literal_IPv6_address***]:port**

[Core コンソール] または [Satellite コンソール] ページ、またはフィールドでポート エントリを許可していない設定ファイルを使用して IPv6 アドレスを入力する場合は、角かっこを省略します。

例 :

- ユーザー インターフェイス : **上位ホスト : *literal_IPv6_address***
- 設定ファイル :　　**HOST=*literal_IPv6_address***

  -host *literal_IPv6_address*

HPCA の IPv6 サポートの概要

Client Automation では、Windows インフラストラクチャの Core Server および Satellite Server に IPv6 のサポートが追加されました。具体的には、次の点が変更されました。

- Core Server および Satellite Server は、IPv4 または IPv6 のいずれかを使用して HPCA *サーバー間*通信を実行できるようになりました。
- Core Server および Satellite Server と、HPCA Configuration Server サービスは、インストール中に検出された使用可能な IPv4 および IPv6 スタック上でリスンするように自動的に設定されます。IPv4 のみが検出された場合、IPv4 用に設定されます。IPv6 も検出された場合、両方のスタックでリスンするように設定されます。

IPv6 サポートの制限

次の Client Automation コンポーネントは、IPv4 のみをサポートし、IPv6 には対応していません。

- Client Automation エージェント。
- Client Automation 管理ツール。
- Core Server または Satellite Server とは別にインストールされた、従来の、コンポーネントベースの Client Automation インフラストラクチャ サーバー。
- アウトバンド管理 (OOBM) 面 : このリリースでは、IPv6 は次を含むすべての OOBM 面で意図的に除外されています。
  - Core エンジンから OOBM Web サービス
  - OOBM から SCS (SCS は Intel AMT のセットアップおよび設定サービス)
  - OOBM からエージェント

Core および Satellite 環境での IPv6 のサポート

現在のリリースでは、Client Automation の IPv6 サポートの重点は、Windows ベースの Core および Satellite インフラストラクチャ サーバー間でトラフィックの IPv6 による振り分けを可能にすることに置かれています。

このリリースの IP ネットワーキング機能では、Client Automation サーバーが必要に応じて IPv6 または IPv4 を使用し、次のトラフィックを振り分けられます。

- Configuration Server メタデータを同期するための Core および Satellite トラフィック
- キャッシュ データを同期するための Core および Satellite トラフィック
- Core または Satellite 認証およびポリシー トラフィック (HTTP と LDAP)
- Satellite および Core 間のメッセージング トラフィック
- Satellite および Core 間の HTTP トラフィック

IP 通信サポート テーブル

次の表は、Core、Satellite、エージェント、および外部ディレクトリ間の HPCA 通信経路を示しています。IPv4 のみをサポートする通信経路と、IPv4 または IPv6 (IPv4/IPv6) をサポートする通信経路が識別されています。IPv4/IPv6 サポートは、黄色で強調表示されています。

表 50　　IP 通信サポート テーブル

			通信先 (サーバー)		
		Agent	Satellite	Core	AD / LDAP
通信元:	Agent	なし	IPv4	IPv4	なし
(クライアント)	Satellite	IPv4	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6
	Core	IPv4	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6

Core Server および Satellite Server では、2 か所 (HTTP リスニング ポイントと Configuration Server リスニング ポイント) でリスンされます。これらの通信ポイントのどちらかは、必要に応じて IPv4 または混在にすることができます。

HPCA Agent では、IPv4 を使用した Core Server および Satellite Server との通信のみが行われます。

IPv6 サーバー通信を有効にするには

このリリースの Core Server および Satellite Server では、エージェント通信に引き続き IPv4 が必要です。そのため、サーバー間通信で IPv6 を利用するには、Core および Satellite Server をデュアル スタック (IPv4/IPv6) 環境にインストールする必要があります。

Core および Satellite のセットアップ プログラムが、ホスト サーバーで IPv6 スタックを検出すると、Core Server および Satellite Server は、IPv4 および IPv6 プロトコル上でリスンするように自動的に設定されます。

Core または Server インストールを実行する前に、544 ページの前提条件を確認してください。

IPv6 サポートの前提条件

- HPCA Core Server および Satellite Server は、IPv6 に対応し、IPv6 対応ネットワークで実行されている Windows XP、Windows 2003 Server、または Windows 2008 Server オペレーティング システムにインストールされている必要があります。サポート対象のプラットフォームの詳細については、付属の『HPCA 7.50 リリース ノート』のハードウェア サポート表を参照してください。
- このリリースでは、HPCA Agent に対する IPv6 サポートは提供されないため、HPCA Server は、デュアル スタックの IPv4/IPv6 環境で実行する必要があります。
- DNS と DHCP は、IPv6 をサポートするように設定する必要があります。
- HPCA Server と、ポリシーおよび認証通信に使用されているユーザー提供の外部 **Active Directory Service** (**ADS**) の間の IPv6 通信をサポートするには、次の条件を満たす必要があります。
  - ADS が Windows Server 2008 にインストールされている
  - ADS に IPv6 のサポートが設定されている
- Internet Explorer を Web ブラウザとして使用する場合、IPv6 をサポートするには、バージョン 7 以上が必要です。

HPCA Windows サーバーへの IPv6 サポートの設定

このセクションでは、HPCA Core および Satellite Windows Server コンポーネントが IPv6 対応環境にインストールされるときに、自動的に行われる IPv6 関連の設定変更について説明します。

このセクションでは、次のトピックを説明します。

- 545 ページの「コンポーネント : HPCA Apache ベースの Core Server および Satellite Server」
- 545 ページの「コンポーネント : HPCA Configuration Server」

コンポーネントごとに、次の詳細を説明します。

- IPv6 をコンポーネントに対して有効にする方法
- ログを使用して IPv6 が使用されているかどうかを識別する方法
- 制限事項と依存関係 (ある場合)

コンポーネント : HPCA Apache ベースの Core Server および Satellite Server

HPCA Core Server および Satellite Server は、Apache サービス (デフォルトで IPv6 対応) の下で実行されます。Apache サービスでは、IPv6 用の設定変更は要求されません。ただし、お使いの環境が前述の前提条件を満たすことを確認してください。

Apache が IPv6 アドレスをリスンしていることを確認するには

1. コマンド プロンプトを開きます。
2. 「**`netstat -an`**」と入力します。
3. 結果が表示されたら、[::]:3466 用のエントリが存在するかどうか確認します。存在する場合、これにより Apache が IPv6 アドレスをリスンしていることが確認されます。

コンポーネント : HPCA Configuration Server

Configuration Server では、IPv4 でエージェント通信がリスンされる必要があります。Core インストール プログラムで使用可能な IPv6 スタックが検出されると、Configuration Server は、IPv4 と IPv6 の両方のスタックでリスンできるように自動的に設定されます。

Configuration Server コンポーネントで IPv6 を有効にする方法

Core Server または Satellite Server のインストール時に Core または Satellite で IPv6 が有効になると、Configuration Server は自動的に IPv4 と IPv6 の両方のスタックでリスンできるように設定されます。これには、次の設定が含まれます。

- IPv4 に加えて IPv6 の接続も受け入れるためのセッション接続を有効にする。
- IPv6 に加えて IPv4 の **SSL** (**Secure Sockets Layer**) とのセッション接続を有効にする。

Configuration Server が SSL モード以外で IPv6 アドレスをリスンしていることを確認するには

これらの変更は、IPv6 がサーバー上で有効な場合に Core または Satellite セットアップ プログラムによって行われます。IPv6 を有効にするために使用された Configuration Server の設定変更を表示して確認するには、次の手順を実行します。

1 Microsoft のメモ帳を使用して、HPCA Server がインストールされた場所の \bin ディレクトリにある edmprof を開きます。メモ帳では edmprof ファイルの必須エンコーディングである UTF-8 がサポートされています。

2 MGR_ATTACH_LIST セクションに移動し、ATTACH_LIST_SLOTS 属性を見つけます。IPv6 が検出されると、Core セットアップ プログラムでは IPv6 を有効にするために、明示的に次の CMD_LINE エントリが追加されます (edmprof のデフォルトである、IPv4 でリスンするための ztcpmgr も有効になっています)。

```
CMD_LINE=(ztcpmgr, NAME=tcpmgr6,ADDR=::) RESTART=YES
```

> このコマンド ラインには、デフォルトのポート 3464 を使用する HPCA Configuration Server が反映されています。デフォルト以外のポートが使用されている場合、ADDR 属性の後に、547 ページの「Configuration Server が SSL モードで IPv6 アドレスをリスンしていることを確認するには」と同じ構文を使用して PORT も指定されます。

3 Core セットアップ プログラムはまた、新しい CMD_LINE エントリを追加するために ATTACH_LIST_SLOTS 値も 1 だけ増やします。

> edmprof ファイルが手動で変更された場合、必ず UTF-8 エンコーディングを使用して保存し、HPCA Configuration Server (ZTopTask.exe) のサービスを再起動してください。

4 これらの設定変更が、HPCA Configuration Server サービス (ZTopTask.exe) に反映されていることを確認するには、Configuration Server のログ ファイルを確認します。2 つの TCP マネージャが着信する要求の受け入れ待ちをしていることがわかります。例については、547 ページの「ログ メッセージ」を参照してください。

Configuration Server が SSL モードで IPv6 アドレスをリスンしていることを確認するには

これらの変更は、IPv6 がサーバー上で有効な場合に Core または Satellite セットアップ プログラムによって自動的に行われます。

1 Microsoft のメモ帳を使用して、HPCA Server がインストールされた場所の \bin フォルダにある edmprof を表示します。メモ帳では edmprof ファイルの必須エンコーディングである UTF-8 がサポートされています。

2 Core 設定プログラムでは、SSL Manager IPv4 および IPv6 を有効にするために、MGR_ATTACH_LIST セクションの下に次の行が追加されます。

```
[MGR_ATTACH_LIST]
CMD_LINE=(zsslmgr, NAME=sslmgr4,PORT=443) RESTART=YES
CMD_LINE=(zsslmgr, NAME=sslmgr6,ADDR=::,PORT=443) RESTART=YES
```

3 Core 設定プログラムはまた、新しい CMD_LINE エントリを追加するために ATTACH_LIST_SLOTS 値も 2 だけ増やします。

> edmprof ファイルが手動で変更された場合、必ず UTF-8 エンコーディングを使用して保存し、HPCA Configuration Server (ZTopTask.exe) のサービスを再起動してください。

4 SSL 設定変更が、HPCA Configuration Server サービス (ZTopTask.exe) に反映されていることを確認するには、ログ ファイルを確認します。2 つの SSL マネージャが着信する要求の受け入れ待ちをしていることがわかります。547 ページの「ログ メッセージ」の例を参照してください。

ログ メッセージ

SSL が無効な場合のセッション ログ メッセージ

```
02I 22:22:04 <ztcpmgr           /1DC>   System Task      --- TCP
Manager task has started

NVD0404I 22:22:04 <TCP/IP Manager   /1DC>   System Task      ---
TCP/IP Manager accepting requests at address <RPS> on port <3464>

NVD0402I 22:22:04 <ztcpmgr           /954>   System Task      ---
TCP Manager task has started

NVD0404I 22:22:04 <TCP/IP Manager   /954>   System Task      ---
TCP/IP Manager accepting requests at address <::> on port <3464>
```

SSL が有効な場合のセッション ログ メッセージ

```
NVD0414I 15:04:36 <zsslmgr          /7E8>   System Task     ---
SSL Manager Task has started

NVD0472I 15:04:36 <SSL Manager      /7E8>   System Task     ---
SSL Manager accepting requests at address <RPS> on port <0443>

NVD0414I 15:04:36 <zsslmgr          /188>   System Task     ---
SSL Manager Task has started

NVD0472I 15:04:36 <SSL Manager      /188>   System Task     ---
SSL Manager accepting requests at address <::> on port <0443>
```

Core および Satellite コンソールでの IPv6 リテラル アドレスの使用

IPv6 対応の環境では、以下に挙げる Core および Satellite に関連するフィールドに IPv6 アドレスまたは IPv4 アドレスを使用できます。つまり、これらのフィールドを使用して次の項目を指定できます。

- IPv6 アドレスまたは IPv4 アドレスに解決されるホスト名
- リテラルの IPv6 アドレスまたは IPv4 アドレス

  IPv6 アドレスの例 : `2001:db8:0:1:f8f3:a7bb:2bcb:6037`
  IPv4 アドレスの例 : `192.168.0.4`

サーバーの後にポートを指定可能な URL、URI などのフィールドに、リテラル IPv6 アドレスを入力する場合、IPv6 アドレスを必ず角かっこで囲んでください。例については、下記の「ブラウザ サポート」の項目を参照してください。

Core および Satellite の IPv6 アドレス サポート

ブラウザ サポート

- IPv6 サーバーにインストールされた Core または Satellite コンソールにアクセスする URL は次のようになります。
  例 : **`http://[`***`literal_IP_address`***`]:3466`**

Satellite Server のインストール

- **初回セットアップ ウィザードの手順 3: 上位サーバー**

Satellite コンソール - [設定] タブ

- **[アップストリーム サーバー] ページ > [上位ホスト]**
- **[インフラストラクチャ管理] > [ポリシー] > [ディレクトリ ホスト]**

Core コンソール - [設定] タブ

- **[インフラストラクチャ管理] > [ディレクトリ サービス] > [Creation Wizard]**
- **[インフラストラクチャ管理] > [ポリシー] > [ディレクトリ ホスト]**
- **[パッチ管理] > [ベンダーの設定]**

Core コンソール - [操作] タブ

- **[操作] > [パッチ管理] > [同期を実行]**

IPv6 の使用方法とトラブルシューティング

次のセクションでは、IPv6 に関するよくある質問に対する回答を示し、HPCA で IPv6 を使用するときに発生する一般的な問題をトラブルシューティングできるようにします。

- 550 ページの「使用方法に関するよくある質問」
- 552 ページの「IPv6 環境のトラブルシューティング」

使用方法に関するよくある質問

Q1. HPCA Server で IPv6 を有効にするにはどうすればよいですか ?

A. この付録の前のトピックを参照してください。詳細については、545 ページの「HPCA Windows サーバーへの IPv6 サポートの設定」と、543 ページの「IPv6 サーバー通信を有効にするには」を参照してください。

Q2. IPv6 を有効にしましたが、Web ブラウザを使用して Core にアクセスすると、不正な要求や接続拒否に関するエラーが表示されます。どのように解決すればよいですか ?

A. 次のどちらかの方法を使用して問題を切り分けてください。

- IPv4 のマシンと IPv6 のマシンに対して ping を実行します。
- telnet を使用して該当するアドレスとポート 3466 または 3464 に接続できるかどうか確認します。接続できた場合は、ローカルな問題 (IPv6 のリテラル サポートには IE7 が必要) か、またはサーバー側の何らかの問題です。サーバーが実行中で、リスンしていることをログで確認してください。

CA のログ ファイルは、サーバーの `C:\Program Files\Hewlett-Packard\HPCA` の下にある次のディレクトリにあります。

- `\ApacheServer\logs`
- `\ConfigurationServer\log`

Q3. Web ブラウザを使用して接続すると、速度が著しく遅くなります。特にこれといった理由もなく、数秒の待ちが発生します。一方、IPv4 を使用する隣席のユーザーでは、この問題は発生していません。解決方法はありますか？

A. ブラウザの接続速度が低下するのは、サーバーが呼び出し元のホスト名を判別しようとして一時的にハングするという、DNS の問題が原因である可能性があります。

Q4. IPv6 を有効にして、IPv6 対応の DNS を使用しています。「http://myCore:3466」のようなホスト名を使用してコンソールに接続した場合、この接続が IPv4 と IPv6 のどちらを使用しているかをどのようにして確認できますか？

A. Apache と Configuration Server のログを確認してください。ログ エントリの例については、付録の「IPv6 ネットワーキングのサポート」のトピックを参照してください。

Q5. IPv6 を有効にして、IPv6 対応の DNS を使用しています。Satellite の同期を実行したとき、IPv4 と IPv6 のどちらを使用しているかをどのようにして確認できますか？

A. Apache と DCS のログを確認してください。

Q6. リテラル IPv6 アドレスを使用して HTTPS で Core/Satellite にアクセスすると、IE から証明書に関する警告が表示されます。何が起きているのでしょうか？

A. ホストの DNS でアドレスの逆検索ができない場合、中間者防御が行われているかどうかを検証できません。これは、証明書のキーが IP アドレスではなく FQDN に対して設定されているためです。同じことが、IPv6 アドレスだけでなく、どの IP アドレスにも当てはまります。

Q7. 上位ホストにリンクローカル アドレスを指定したらエラーが表示されました。どのように解決すればよいですか？

A. HPCA Core Server は、Apache の下で実行されているため、リンクローカル アドレス エントリをサポートしていません。上位ホストには、グローバル ユニキャスト IPv6 アドレスを指定する必要があります。詳細については、このトラブルシューティングの項目である、554 ページの「使用している IP アドレスの問題でしょうか？どうすれば IP アドレスを二重にチェックできますか？」を参照してください。

IPv6 環境のトラブルシューティング

IPv6 環境で発生した単純な問題のトラブルシューティング時には、次に示す診断や検証に関するヒントを参考にしてください。ヒントの多くは、HPCA の IPv6 実装に関する作業に固有のものではなく、IPv6 全般に適用されます。

後述のトピックを参考にして、次のような診断上の問題を解決してください。

- 552 ページの「リモート ブラウザから Core または Satellite にアクセスできますが、ログインしようとすると「不明なログイン失敗です」というエラーで失敗するか、応答がありません。解決方法はありますか ?」
- 553 ページの「Web ブラウザの問題のような、ローカル ツールの問題が発生しているのでしょうか ?」
- 553 ページの「ローカル OS の問題でしょうか ? OS で IPv6 はサポートされているのでしょうか ?」
- 553 ページの「ローカル OS の問題でしょうか ? ホスト名の DNS 名前解決をテストするにはどうすればよいですか ?」
- 554 ページの「使用している IP アドレスの問題でしょうか ? どうすれば IP アドレスを二重にチェックできますか ?」
- 555 ページの「クライアントとサーバー間のネットワークに問題があるのでしょうか ? どのようにして確認できますか ?」

リモート ブラウザから Core または Satellite にアクセスできますが、ログインしようとすると「不明なログイン失敗です」というエラーで失敗するか、応答がありません。解決方法はありますか ?

問題 : リモート ブラウザから Core または Satellite にログインできない。「不明なログイン失敗です」というメッセージが表示されるか、応答がない。

解決方法 : リモート ログインの失敗は、一般に次のいずれかの理由で発生します。

- ブラウザのセキュリティに原因がある場合。**解決方法 :** 信頼できるサイトのリストに「http://[<IPv6 アドレス >]:3466/」を追加してください。
- IE7 ブラウザで Cookie が無効になっているか、リフレッシュされない場合。**解決方法 :** IE7 ブラウザの Cookie を削除し、ページをリフレッシュしてから、再度ログインを試みてください。IE7 ブラウザの Cookie の削除機能へは、次のようにして移動します。

  [ツール] > [インターネット オプション] > [全般] タブ > [閲覧の履歴] > [削除] > [Cookie の削除]

Cookie を削除したら、ページをリフレッシュしてから再度ログインしてください。

Web ブラウザの問題のような、ローカル ツールの問題が発生しているのでしょうか？

Core または Satellite コンソールへのアクセスを試みたときのブラウザの応答が「Internet Explorer はページを表示できません」である場合、使用している IE ブラウザのバージョンを確認してください。

IPv6 アドレスでページを開くには、IE7 以降を使用する必要があります。

ローカル OS の問題でしょうか？OS で IPv6 はサポートされているのでしょうか？

ローカル OS で IPv6 サポートが有効かどうかを確認するには、次の基本情報を参考にしてください。

- Windows 2000 の場合、IPv6 はサポートされていません。Windows 2003 以上が必要です。
- Windows 2003 の場合、IPv6 はサポートされていますが、デフォルトでは IPv6 スタックが読み込まれません。Windows 2003 で IPv6 スタックを (既存の IPv4 スタックと一緒に) 有効にするには、コマンド ライン ウィンドウ ボックスから **`netsh interface ipv6 install`** を実行します。このコマンドにより、IPv6 スタックがインストールされます。
- Windows 2008/Vista の場合、IPv6 はデフォルトでサポートされています。

ローカル OS の問題でしょうか？ホスト名の DNS 名前解決をテストするにはどうすればよいですか？

非常に長い IPv6 アドレスを使用する IPv6 環境では特に、ホスト名を使用して IPv6 アドレスに解決するのが最良の方法です。ホスト名が正しく解決されているかどうかは、次の方法で確認してください。

`Ping` ツールか、**`Nslookup`** のいずれかを使用して確認できます。注 : Nslookup を使用すると、IPv4 と IPv6 のどちらでも正しいホスト名と IP アドレスを解決できます。

ping ツールを使用する : DNS 名前解決をテストするには、ping ツールを使用し、ホスト名または完全修飾ドメイン名 (FQDN) で指定した送信先に対して ping を実行します。ping ツールが、FQDN および対応する IPv6 アドレスを表示します。

Nslookup を使用する : ping ツールが正しくない IPv6 アドレスを使用している場合、次の手順を実行します。

Nslookup ツールを使用すると、DNS Name Query Response メッセージで返された一連のアドレスを判別できます。

1. 最初に、DNS リゾルバのキャッシュをフラッシュします。次のコマンドを使用してフラッシュできます。

   ipconfig /flushdns

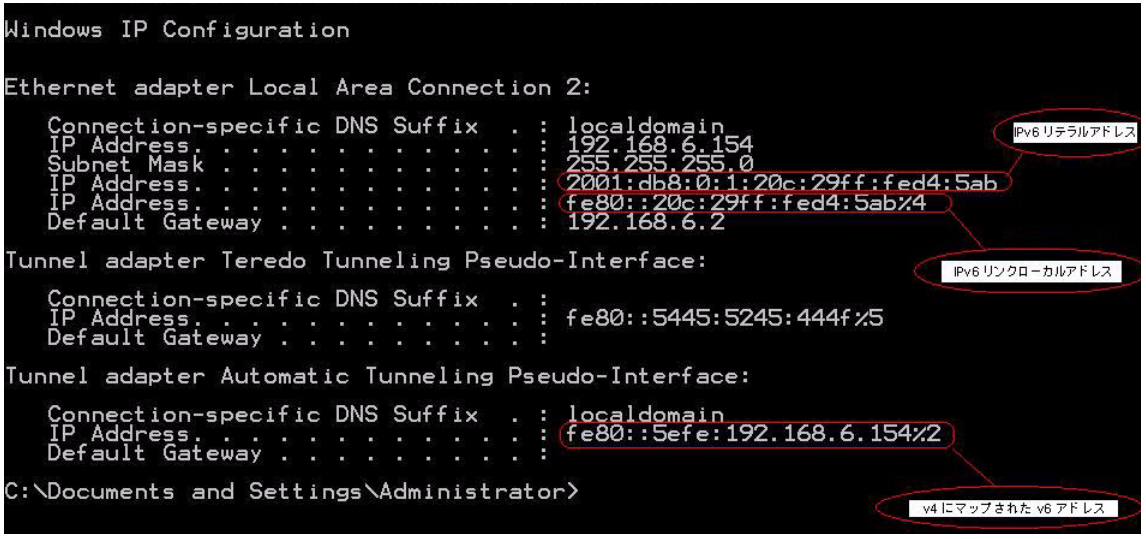
2. Nslookup > プロンプトで、**set d2** コマンドを使用して、DNS 応答メッセージに関する最大量の情報を表示します。
3. Nslookup を使用して目的の FQDN を検索します。次のいずれかを使用します。
   - **nslookup <ip address>**
   - **nslookup <hostname>**

   DNS 応答メッセージの詳細表示で、AAAA レコードを探します。

使用している IP アドレスの問題でしょうか？どうすれば IP アドレスを二重にチェックできますか？

デバイスに対して正しい IPv6 アドレスを使用していることを確認するには、**ipconfig** コマンドを実行します。

Windows 2003 マシン (IPv6 が有効) の場合、**ipconfig** では、次の図のように IPv6 アドレスのセットが 3 つ返されます。



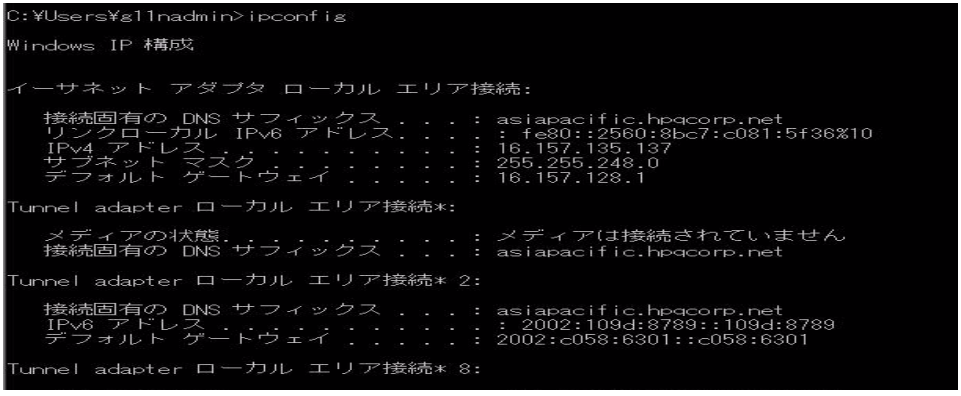
3 つの IP アドレスは、赤い丸で示すように (上から下) それぞれ異なります。

- アドレス「2001:db8:0:1:20c:29ff:fed4:5ab」は*グローバル ユニキャスト IPv6 アドレス*で、*外部通信*に使用できます。
- アドレス「fe80::20c:29ff:fed4:5ab%4」は、*リンクローカル　アドレス*です。このアドレスは、*同じサブネット (リンク) 上の近隣ホストとの通信のみ*に使用できます。リンクローカル アドレスは、ルータによって転送されません。
- アドレス「fe80::5efe:192.168.6.154%2」は、*IPv4　マップ済み v6　アドレス*で、*トンネリング*に使用できます。

注 : デバイスは、複数のインターフェイスを持つことができます。コマンド「**interface ipv6 show address**」を実行すると、各インターフェイスに割り当てられた IPv6 アドレスを表示できます。

Windows 2008 マシンの場合、**ipconfig** コマンドでは、2 つの IPv6 アドレスのみが返されます。また、次の画像の「Ethernet adapter Local Area Connection 2:」の下に表示されているように、これらのアドレスは、明示的に **IPv6 Address** および **Link-local IPv6 Address** と表示されます。

このリストを参照して、外部接続には常に **IPv6 Address** を使用してください。:



クライアントとサーバー間のネットワークに問題があるのでしょうか？どのようにして確認できますか？

これには、多くの理由が考えられます。その一部を次に挙げます。

- ファイアウォールがクライアントまたはサーバー　マシンで有効になっている。この点を確認し、ファイアウォールを無効にしてください。

- デフォルトで HPCA Server が v4 と v6 の両方の接続をリスンしている。v4 にバインドしているクライアントは、サーバーが v4 接続をリスンしていないため失敗した可能性があります。サーバー側で、コマンド プロンプトを開き、「**netstat -an**」と入力します。これにより、サーバーがリスン中のアドレスとポートがすべて表示されます。
- サーバーが混雑中で接続を受け入れられない。

F　Windows 応答ファイルのカスタマイズ

この付録は、次のトピックで構成されています。

これらは、無人モード (クライアント デバイスでユーザーの介入が不要) で管理対象デバイスにオペレーティング システムのイメージを配布できるようにするこのイメージのキャプチャおよびパブリッシュのプロセスに関するトピックです。

unattend.xml ファイルのカスタマイズ

HPCA では OS の無人インストールに使用できる応答ファイルを提供します。この応答ファイルは unattend.xml という名前です。

各オペレーティング システムおよびアーキテクチャ (32 ビットまたは 64 ビットなど) には、独自の unattend.xml ファイルがあります。これらのファイルは、次のサブディレクトリにあります。

InstallDir\Data\OSManagerServer\capture-conf

ファイルの先頭にあるヘッダーは、ファイルの適用先の OS、アーキテクチャ、および配布メソッドを示しています。

HP が提供する unattend.xml ファイルを使用する場合は、OS イメージをパブリッシュする前に環境に合わせてこのファイルを変更する必要があります。次に、カスタマイズの対象となる設定をいくつか挙げます。

- 559 ページの「ProductKey」
- 561 ページの「TimeZone」
- 562 ページの「RegisteredOwner および RegisteredOrganization」
- 562 ページの「JoinDomain」
- 564 ページの「MetaData」

少なくとも、有効な製品キーを指定する必要があります (559 ページの「ProductKey」を参照)。ここで説明するその他の設定の変更はオプションです。

テキスト エディタを使用して、該当する unattend.xml ファイルのコピーを変更します。このコピーのファイル名は任意に指定できますが、.xml ファイル拡張子は維持する必要があります。OS イメージをパブリッシュするときに、カスタマイズした応答ファイルがある場所を指定します。

Windows Automated Installation Kit (AIK) には Unattend.chm という名前のファイルが含まれています。これは、コンパイル済みのオンライン ヘルプのファイルであり、unattend.xml ファイルの内容に関する参照情報が記載されています。ここで説明する設定とカスタマイズできるその他の設定についての詳細は、このヘルプ ファイルを参照してください。Unattend.chm をダブルクリックするだけで、簡単にファイルを開けます。

ProductKey

<ProductKey> 要素は、使用している具体的な OS イメージ、アーキテクチャ、および配布メソッドによって、unattend.xml ファイルの異なる場所に表示されます。<ProductKey> は、次のように文字間が区切られている 29 個の文字で構成されている文字列です。

XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

すべての DVD インストールで、/IMAGE/INDEX が DVD の正しいイメージ (564 ページの「MetaData」を参照) を参照していることを確認してください。

リテール版

Windows のリテール版 (Windows 7 Ultimate など) では、次のように変更します。

- <ProductKey> 要素内の <Key> 要素に有効な製品キーを挿入します。例 :

```
<UserData>
    <AcceptEula>true</AcceptEula>
    <ProductKey>
        <Key>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</Key>
        <WillShowUI>OnError</WillShowUI>
    </ProductKey>
</UserData>
```

  この要素は、パスの "WindowsPE" の "Microsoft-Windows-Setup" コンポーネントにあります。

- "specialize" パスの "Microsoft-Windows-Shell-Setup" コンポーネントにある <ProductKey> 要素全体を削除します。

```
<ProductKey>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</ProductKey>
```

ビジネス版

Windows のビジネス版 (Business、Enterprise、Professional、Server 版を含む) では、次のように変更します。

- パスの "WindowsPE" の "Microsoft-Windows-Setup" コンポーネントにある <Key> 要素のすべての文字を削除します (上の例を参照)。

  ```
  <Key></Key>
  ```

- "specialize" パスの "Microsoft-Windows-Shell-Setup" コンポーネントにある <ProductKey> 要素に有効な製品キーを挿入します。

  ```
  <ProductKey>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</ProductKey>
  ```

  Volume License Multiple Activation Key (MAK) を使用する場合は、<ProductKey> 要素で使用してください。

Windows AIK では、<Key></Key> 要素は空の値をサポートしていますが、<ProductKey> 要素は空の値をサポートしていません。このため、<ProductKey> 要素を使用しない場合、この要素を削除する必要があります (559 ページの「リテール版」を参照)。

64 ビット プラットフォーム

一部の 64 ビット アーキテクチャで Windows セットアップ配布メソッドにより DVD を使用している場合は、次のように変更してください。

- パスの "WindowsPE" の "Microsoft-Windows-Setup" コンポーネントにある <Key> 要素のすべての文字を削除します (上の例を参照)。

  ```
  <Key></Key>
  ```

- "specialize" パスの "Microsoft-Windows-Shell-Setup" コンポーネントにある <ProductKey> 要素に有効な製品キーを挿入します。

  ```
  <ProductKey>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</ProductKey>
  ```

- /IMAGE/INDEX がメディアの正しいイメージを参照していることを確認してください (564 ページの「MetaData」を参照)。

- "WindowsPE" パスの次のコンポーネントの仕様で "amd64"; を "x86"; に変更します。

  ```
  <component name="Microsoft-Windows-International-Core-WinPE"
  processorArchitecture="amd64" ...
  ```

  ```
  <component name="Microsoft-Windows-Setup"
  processorArchitecture="amd64" ...
  ```

- パブリッシュ中、ソース ディレクトリの指定を求められたときは、同じオペレーティング システムの 32 ビット メディアのソース ディレクトリを指定します。

- Windows 2008 R2 x64 の場合、次の専用の手順を実行します。
  - Windows 7 Enterprise Edition 32 ビット インストール メディアを使用します。
  - OS イメージをパブリッシュする前に、次の手順を実行します。
    a. Windows 7 32 ビット インストール メディアから、*mediaDrive*:\sources フォルダを c:\temp にコピーします。
    b. Windows 7 メディアを取り出し、Windows 2008 R2 x64 メディアを読み込みます。
    c. Windows 2008 R2 x64 のインストール メディアから、*mediaDrive*:\sources\license フォルダを c:\temp\sources にコピーします。

    既存のファイルの上書きを確認するメッセージが表示されたら、上書きの実行を確認します。

    この操作により、Windows 2008 Server R2 EULA が Windows 7 インストーラのフォルダから使用できるようになります。

詳細については、Windows AIK に含まれているヘルプ ファイル Unattend.chm の「ProductKey」のトピックを参照してください。

HPCA は 64 ビット プラットフォームで Windows セットアップ配布のイメージ キャプチャを現在サポートしていません。

TimeZone

<TimeZone> 要素は、使用している具体的な OS イメージ、アーキテクチャ、および配布メソッドによって、unattend.xml ファイルの異なる場所に表示されます。

たとえば、キャプチャした Windows 7 (x86) イメージの unattend.xml ファイルでは、<TimeZone> 要素は次の 2 つの場所に表示されます。

- Microsoft-Windows-Shell-Setup コンポーネントでは、次の要素にあります。

  <settings pass="oobeSystem">
- Microsoft-Windows-Shell-Setup コンポーネントでは、次の要素にあります。

  <settings pass="specialize">

OS の配布先であるターゲット デバイスに合わせて <TimeZone> を変更します。例:

<TimeZone>Eastern Standard Time</TimeZone>

タイム ゾーンのスペルが Windows レジストリで使用しているスペルと厳密に一致していることが重要です。詳細については、Windows AIK に含まれているヘルプ ファイル Unattend.chm の「言語パックのデフォルト値」のトピックを参照してください。

- グリニッジ標準時は、現在、協定世界時として知られています。
- Windows 7 を実行しているコンピュータでは、tzutil コマンドを使用してコンピュータのタイム ゾーンを表示できます。

RegisteredOwner および RegisteredOrganization

これらの要素は、使用している具体的な OS イメージ、アーキテクチャ、および配布メソッドによって、unattend.xml ファイルの異なる場所に表示されます。

たとえば、キャプチャした Windows 7 (x86) イメージの unattend.xml ファイルでは、これら 2 つの要素は次の 2 つの場所にあります。

- Microsoft-Windows-Shell-Setup コンポーネントでは、次の要素にあります。

  ```
  <settings pass="oobeSystem">
  ```

- Microsoft-Windows-Shell-Setup コンポーネントでは、次の要素にあります。

  ```
  <settings pass="specialize">
  ```

これらの要素を会社 (オペレーティング システムを登録したエンティティ) の名前に変更します。例 :

```
<RegisteredOrganization>Hewlett-Packard</RegisteredOrganization>
<RegisteredOwner>Hewlett-Packard</RegisteredOwner>
```

これらの文字列に入力できる文字数は、半角で 256 文字までです。

詳細については、Windows AIK に含まれている Unattend.chm ヘルプ ファイルの「RegisteredOrganization」および「RegisteredOwner」のトピックを参照してください。

JoinDomain

OS のインストール後、ドメインまたはワークグループのいずれかに参加するようにターゲット デバイスに指示できます。デフォルトはワークグループ モードです。ターゲットにドメインに参加するよう指示するには、次の要素を変更します。

```
<component name="Microsoft-Windows-UnattendedJoin" ... >
   <Identification>
      <Credentials>
         <Domain></Domain>
         <Password></Password>
         <Username></Username>
      </Credentials>
      <JoinDomain></JoinDomain>
   </Identification>
</component>
```

例：

```
<component name="Microsoft-Windows-UnattendedJoin" ...>
   <Identification>
      <Credentials>
         <Domain>lan.mycompany.com.de</Domain>
         <Password>T3ch3d08</Password>
         <Username>administrator</Username>
      </Credentials>
      <JoinDomain>lan.mycompany.com.de</JoinDomain>
   </Identification>
</component>
```

- 指定されたユーザーには、ドメインに参加できる十分なアクセス レベルが必要です。
- この情報の一部が見つからないかまたは正しくない場合、デバイスはドメインではなくワークグループに参加します。
- ターゲット デバイスが以前 HPCA で管理されており、このデバイスが以前ドメインのメンバーであった場合、unattend.xml ファイルで <Domain> 要素および <JoinDomain> 要素の内容が格納されているドメイン情報で上書きされます。
- OS Manager Server のスクリプトを使用してドメインを設定するなど、一元的に設定されるすべての情報で unattend.xml の情報が上書きされます。

詳細については、Windows AIK に含まれている Unattend.chm ヘルプ ファイルの「JoinDomain」のトピックを参照してください。

MetaData

オペレーティング システムのイメージを DVD から直接配布する場合、DVD の WIM ファイルでそのイメージの場所を指定する必要があります。WIM ファイルでは、この情報は次のように構成されています。

```
<WIM>
    <IMAGE INDEX="2">
        <NAME>MyWIM</NAME>
        <DESCRIPTION>MyCustomWindowsImage</DESCRIPTION>
    </IMAGE>
</WIM>
```

unattend.xml ファイルでは、イメージの情報は、<settings pass="WindowsPE"> の下にある Microsoft-Windows-Setup コンポーネント階層の <MetaData> 要素で指定されています。例：

```
<MetaData>
    <Key>/IMAGE/INDEX</Key>
    <Value>2</Value>
</MetaData>
```

<Key> 要素は WIM ファイルのどのデータ項目に一致するかを指定します。次のいずれかを指定できます。

- IMAGE/INDEX
- IMAGE/NAME
- IMAGE/DESCRIPTION

<Value> 要素はこのデータ項目の推奨値を示します。この例では、配布するイメージの WIM ファイルの IMAGE/INDEX の値は 2 です。

WIM ファイルのイメージのリストを抽出するには、次のコマンドを使用します。

```
imagex /info WIMFileName > c:\info.txt
```

この例では、*WIMFileName* が WIM ファイル (install.wim など) の名前です。このコマンドの出力は、結果を簡単に検索できるよう、(この例に示すように) テキスト ファイルに必ずリダイレクトします。

詳細については、Windows AIK に含まれているヘルプ ファイル Unattend.chm の「MetaData」のトピックを参照してください。

HPCA OS Manager での XML ファイルの処理

パブリッシュする unattend.xml ファイルは、発行したイメージに存在するすべての unattend.xml ファイルの上に配置されます。

HPCA がイメージ インストールを開始する前に、パブリッシュした XML を substitutes ファイルと結合し、最終的な unattend.xml を生成します。

このファイルの結合は、HPCA が実際のイメージのインストールが開始する前に、HPCA によって実行されます。これまで前面に露出していた substitutes ファイルは、背後に隠れて使用されるようになります。各オペレーティング システムおよびアーキテクチャ (32 ビットまたは 64 ビットなど) には、独自のファイルがあります。これらのファイルは、次のサブディレクトリにあります。

InstallDir\Data\OSManagerServer\capture-conf

パブリッシュされるイメージのプロセッサのアーキテクチャに応じて、自動的に正しいファイルが選択されます。

表 51 では、substitutes ファイルをパブリッシュするときに更新される unattend.xml ファイルの設定がリストに表示されます。

青で示されている設定 (CommandLine、Path、および PartitionID の両方のインスタンス) は、HPCA が動作するために必要です。これらの設定を削除することはできません。

表 51　　substitutes ファイルに基づいて更新される設定

設定パス	コンポーネント	パス	設定	上書き値
windowsPE	Microsoft-Windows-Setup	DiskConfiguration/Disk/ModifyPartitions/ModifyPartition	PartitionID	HPCA が OS をインストールする先の DISKPART ボリュームの ID
windowsPE	Microsoft-Windows-Setup	ImageInstall/OSImage/InstallTo/	PartitionID	HPCA が OS をインストールする先の DISKPART ボリュームの ID
windowsPE	Microsoft-Windows-Setup	ImageInstall/OSImage/InstallFrom/	Path	インストールに使用する WIM ファイル

表 51　　substitutes ファイルに基づいて更新される設定

設定パス	コンポーネント	パス	設定	上書き値
oobeSystem	Microsoft-Windows-Shell-Setup	AutoLogon/	Domain	コンピュータ名 (自動ログオン用)
specialize	Microsoft-Windows-Shell-Setup	AutoLogon/	Domain	ローカル コンピュータ名 (自動ログオン用)
specialize	Microsoft-Windows-UnattendedJoin	Identification/Credentials/	Domain	HPCA Enterprise コンソールの getmachinename.tcl または既存のデバイス エントリを使用してドメインを一元的に設定する
specialize	Microsoft-Windows-UnattendedJoin	Identification/	JoinDomain	HPCA Enterprise コンソールの getmachinename.tcl または既存のデバイス エントリを使用してドメインを一元的に設定する
specialize	Microsoft-Windows-Shell-Setup		Computer Name	コンピュータ名
oobeSystem	Microsoft-Windows-Shell-Setup	FirstLogonCommands/SynchronousCommand	Command Line	Agent のインストール メディア インストーラへのパス

必要に応じて、substitutes ファイルをカスタマイズし、特定のカスタマイズを無効にしたり、新しいカスタマイズを追加したりできます。ただし、PartitionID 設定または CommandLine 設定を削除または変更できません。

.subs ファイルおよび .xml ファイルについて

HPCA では、Publisher の実行時にこの情報のソースを指定できるようになりました。詳細については、439 ページの「オペレーティング システム イメージのパブリッシュ」を参照してください。

このトピックは Windows XP または Windows 2003 には該当しません。

HPCA Publisher は下位互換性があります。.WIM ファイル、.EDM ファイル、.XML ファイル、および .SUBS ファイルで構成される、保存されている OS イメージのパブリッシュをサポートしています。

*.SUBS ファイルおよび *.XML ファイルを手動で事前に作成する場合は、これらのファイルに *.WIM ファイルと同じプレフィックスを指定する必要があります。たとえば、vista.WIM、vista.SUBS、および vista.XML と指定します。3 つのファイルすべてを同一のディレクトリに格納する必要があります。

HPCA Publisher を実行するときに、*.WIM ファイルと同じディレクトリに *.SUBS ファイルおよび *.XML ファイルがある場合は、unattend.xml ファイルは要求されません。

HPCA では、次のフォルダのサブディレクトリにある Image Capture メディアにこれらのファイルのサンプルを用意しています。

```
\samples\unattend
```

サンプル ファイルを使用する場合は、ファイル名を変更し、必要に応じて修正します (<TimeZone> および <ProductKey> の設定など)。

.XML ファイルは一般情報を格納している応答ファイルであるとともに、.SUBS から取り込まれる情報のプレースホルダでもあります。Microsoft の Windows System Image Manager (SIM) ツールを使用して、*.XML ファイルに情報を追加できます。情報を追加する場合は、まず対応する *.WIM ファイルを開いてから、*.XML を開く必要があります。

*.XML ファイルおよび *.SUBS ファイルを使用する場合は、Windows インストール用の製品キーを *.XML ファイルに指定する必要があります。

このファイルの XML 値は、一切削除しないでください。.XML ファイルの変更を間違えると、インストールが失敗する可能性があります。

SIM ツールの [メッセージ] セクションで「…値 $$SUBSTR$$ が無効です…」のようなエラーが表示されても無視して構いません。

このファイルを保存すると、「応答ファイルには、検証エラーがあります。続行してもよろしいですか ?」などのメッセージが表示される場合があります。[**はい**] をクリックして続行します。

.SUBS ファイルは、.XML で修正される各 XML 項目と推奨値の一覧を示す「置換」ファイルです。*.SUBS ファイルの行は XPATH と呼ばれます。

.SUBS ファイルに入力されている情報は、.XML ファイルの情報より優先されます。

置き換えの例

置き換えの仕組みについて理解するには、次の例を参照してください。この例では、JoinDomain 属性を、filename.xml ファイルの "anything" から unattend.xml ファイルの "VistaTeam" に設定する方法を示しています。

< > で囲まれたコードは、*.xml ファイル内ではすべて 1 行で表示される必要があります。

1. オペレーティング システム、ターゲット デバイス アーキテクチャ、配布メソッドのための適切な unattend*.xml ファイルおよび subsitutes ファイルを配置します。これらのレポートは、ImageCapture CD の samples\ にあります。
2. unattend*.xml ファイルのコピーを作成し、*filename*.xml という名前を付けます。ここで、*filename* は .WIM ファイルの名前に一致します。このコピーを .WIM ファイルと同じディレクトリに格納します。

3 substitutes ファイルのコピーを作成し、*filename*.subs という名前を付けます。このコピーを .WIM ファイルと同じディレクトリに格納します。

これで 1 つのディレクトリに次の 3 つのファイルが格納されます。

— *filename*.wim

— *filename*.xml

— *filename*.subs

4 *filename*.xml ファイルに JoinDomain の XML 要素を配置します。次の例のようになります。

```
<?xml version="1.0" encoding="utf-8"?>

<unattend xmlns="urn:schemas-microsoft-com:unattend">

    <settings pass="specialize">

<component name="Microsoft-Windows-UnattendedJoin"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <Identification>

                <JoinDomain>anything</JoinDomain>

            </Identification>

        </component>

    </settings>

    <cpi:offlineImage  cpi:source="wim://hpfcovcm/c$/
vista_inst/vista.wim#Windows Vista ULTIMATE"
xmlns:cpi="urn:schemas-microsoft-com:cpi"/>

</unattend>
```

5 次の *filename*.subs ファイルの XPATH 要素を変更します。注 : この XPATH 要素が、*filename*.subs ファイルでは 1 行で表示されています。

```
//un:settings[@pass='specialize']//
un:component[@name=Microsoft-Windows-UnattendedJoin'][@pr
ocessorArchitecture='x86']/un:Identification/
un:JoinDomain,VistaTeam
```

オペレーティング システムの配布中に *filename*.subs ファイルと *filename*.xml ファイルが結合され、unattend.xml ファイルが作成されます。このファイルは、Windows セットアップのすべてのフェーズで情報を提供するために使用されます。この例では、JoinDomain 属性が **VistaTeam** に設定されます。

G Windows XP および Windows Server 2003 の OS イメージのキャプチャ

この付録の情報は、Windows XP および Windows Server 2003 の OS イメージのキャプチャにのみ関連しています。

Windows Vista、Windows Server 2008、Windows 7、およびサポートされているすべてのシン クライアント オペレーティング システムのキャプチャと重要なイメージ キャプチャ プロセスの概要については、405 ページの「OS イメージの準備とキャプチャ」を参照してください。

HPCA は暗号化されていないパーティションのキャプチャのみをサポートしています。

この章は、次のトピックで構成されています。

HPCA Image Preparation Wizard について

HPCA Image Preparation Wizard では、ImageX、Windows セットアップ、レガシー配布で使用する Windows XP または Windows 2003 Server の OS イメージをキャプチャできます (詳細については、408 ページの「配布方法」を参照してください)。

Image Preparation Wizard は、次のタスクを実行します。

1 参照マシンに関する情報 (ハードウェア機能と OS 機能についての情報) を収集して格納します。

2 必要に応じて、使用可能な終了ポイントを実行します。Image Preparation Wizard で、イメージを封印する SysPrep が起動される前に PRE.CMD が実行されます。Sysprep によってイメージが封印された後、POST.CMD が実行されます。詳細については、573 ページの「Image Preparation Wizard の終了ポイント」を参照してください。

> Image Capture の終了ポイントは、ImageX および Windows セットアップのキャプチャ タイプの場合にのみサポートされます。

3 (サポートされているオペレーティング システムで) Microsoft Sysprep を実行します。

4 参照マシンを (適切なメディアから起動された) Service OS で再起動します。実行した Service OS でイメージと関連ファイルが収集されます。

キャプチャ中は、Service OS の画面にステータス情報が表示されます。詳細については、430 ページの「Windows PE Service OS 画面について」を参照してください。

5 ファイルを作成し、HPCA server の次のディレクトリにコピーします。

InstallDir\Data\OSManagerServer\upload

レガシー イメージを作成する場合、次のファイルがアップロードされます。

— ImageName.IMG
このファイルには、ゴールド イメージが含まれています。これは、非常に大きなハード ディスク ドライブ システムのブート パーティションをセクタごとにコピーして圧縮したファイルです。このファイルには、イメージがインストールされるときにアクセス可能な組み込みファイル システムが含まれています。

— ImageName.MBR
このファイルには、参照マシンのマスター ブート レコード ファイルが含まれています。

— ImageName.PAR
このファイルには、参照マシンのパーティション テーブル ファイルが含まれています。

— ImageName.EDM
このファイルにはインベントリ情報を含むオブジェクトが含まれています。

ImageX または Windows セットアップを使用してイメージを作成する場合、次のファイルがアップロードされます。

— ImageName.WIM
このファイルには参照マシンの一連のファイルとファイル システムが含まれています。

— ImageName.EDM
このファイルにはインベントリ情報を含むオブジェクトが含まれています。

Image Preparation Wizard の終了ポイント

必要に応じて、Image Preparation Wizard の終了ポイントを使用できます。たとえば、キャプチャを実行する前にデバイスをクリーンアップするために使用できます。

Image Capture の終了ポイントは、ImageX および Windows セットアップのキャプチャ タイプの場合にのみサポートされます。

終了ポイントを使用するには

1 PRE.CMD ファイルと POST.CMD ファイルを作成します。

2 これらのファイルおよびサポート ファイルを、OSM\PREPWIZ\payload\default\pre と OSM\PREPWIZ\payload\default\post にそれぞれ保存します。

Image Preparation Wizard によって、これらのファイルは参照デバイスの %temp%\prepwiz\pre と %temp%\prepwiz\post にコピーされ、キャプチャが始まる前に削除されます。Image Preparation Wizard で、イメージを封印する SysPrep が起動される前に PRE.CMD が実行されます。Sysprep によってイメージが封印された後、POST.CMD が実行されます。

PRE.CMD または POST.CMD のいずれかからゼロ以外のリターン値が返されると、Image Preparation Wizard が停止することがあります。対話モードでは、停止するか、エラーを無視して続行するかを選択できます。バッチ モードでは、Image Preparation Wizard は停止します。

イメージのキャプチャの前提条件

ImageX、Windows セットアップ、またはレガシー配布で使用する OS イメージをキャプチャする前に、次の手順を実行しておく必要があります。

- 574 ページの「参照マシンの準備」
- 576 ページの「Windows AIK のインストール」

- 576 ページの「Sysprep のインストールおよび設定」

参照マシンの準備

1 オリジナル製品メディアから、オペレーティング システムをインストールします。参照マシンは、インストールするオペレーティング システムを実行できる必要があります。参照マシンが DHCP を使用していることを確認します。

OS は C: ドライブに格納してください。C: ドライブ以外はキャプチャされません。

2 必要に応じて OS をカスタマイズします。これには、基本的なまたは必要な複数のアプリケーションのインストールが含まれる場合があります。OS とアプリケーションの最新のサービス パック、およびイメージの配布先となるデバイスに必要なドライバが含まれることを確認してください。次の Microsoft サポート技術情報の記事には、Windows OS のインストールに OEM ドライバを含めることに関する情報が記載されています。

記事 : 314479 - OEM プラグ アンド プレイ ドライバを Windows XP に追加する方法

http://support.microsoft.com/default.aspx?scid=kb;en-us;314479

3 Microsoft .NET Framework バージョン 2.0 (またはそれ以降) がインストールされていることを確認します。.NET Framework は、次の Microsoft ダウンロード センターから入手できます。

http://www.microsoft.com/downloads

どのバージョンの .NET Framework が参照マシンに存在しているのかを確認するには、次のディレクトリのフォルダを表示します。

```
%SYSTEMROOT%/Microsoft.NET/Framework
```

4 レガシー メソッドを使用してこのイメージを配布する場合は、HPCA Agent を参照マシンにインストールする必要があります。HPCA では Windows セットアップまたは ImageX の OS イメージとともに Agent をパブリッシュする必要があるため、Windows セットアップ配布または ImageX 配布では必要ありません。

レガシー配布の場合のみ、次の操作を実行する必要があります。

要件に応じて、HPCA インストール メディアから Agent をインストールします。少なくとも、Application Manager Agent および OS Manager Agent をインストールする必要があります。これらの操作は、OS イメージを配布するときに、デバイスを OS Manager Server に接続できるようにするために必要です。Agent を更新する必要がある場合は、Agent のセルフ メンテナンスを使用する必要があります。

5 HPCA Server へのアップロード プロセスが終了するまで、キーボードやマウスによる操作が数分間行われなくても、デバイスの電源が切れないように、BIOS の電源管理を設定してください。

6 イメージ ファイルのサイズはできるだけ小さくしておいてください。オペレーティング システムの収納に十分なパーティションの大きさに加えて、HPCA Agent 用の追加領域がある設定が理想的です。

Windows 7 より前の Windows オペレーティング システムの場合、プライマリ ブート ドライブのプライマリ ブート パーティションへのイメージの配布がサポートされます。

Windows セットアップ配布メソッドを使用してイメージを正常にキャプチャするには、参照マシンの OS パーティションに十分な空きディスク領域がある必要があります。たとえば、7 GB のイメージをキャプチャするには、50 ～ 60 GB の空きディスク領域が必要です。

次の手順は .WIM イメージ ファイルのサイズを最小に抑えるのに役立ちます。

a 空き領域を作成します。

HP は、最小の空き容量で最小のパーティションを作成した後、Sysprep.inf ファイルの [Unattended] のセクションに ExtendOemPartition = 1 を設定することを推奨します。これで、より大きなドライブを持つターゲット デバイスに小さなイメージをインストールできるようになります。

ExtendOemPartition = 1 の場合、Microsoft ミニセットアップ ウィザードは、OS インストール パーティションをそのディスクと物理的に連続した、パーティションが設定されていない使用可能な任意の空き領域に拡張します。これで、HPCA Agent はボリューム上の空き領域をアプリケーションのインストールに使用できます。

b ラップトップを使用している場合は休止状態を無効にします。

c 必要があれば、復旧パーティションを削除します。

d ページング ファイルを無効にします。配布後、mini-setup が実行されると、ページング ファイルは、自動的に利用可能になります。

e システムの復元を無効にします。

f インデックス作成サービスとディスク圧縮を無効にします。

g On Resume Password Protect を無効にします。

Windows AIK のインストール

ImageX または Windows セットアップを使用して配布を行う場合、Windows Automated Installation Kit (AIK) を HPCA Core (OS イメージを HPCA database にパブリッシュする場所) にインストールする必要があります。

Windows AIK がインストールされていない場合、Microsoft ダウンロード センター (www.microsoft.com/downloads) からダウンロードできます。通常の Windows インストールには含まれていません。使用しているオペレーティング システムに適したバージョンが次のデフォルトの場所にインストールされていることを確認してください。

```
C:\Program Files\Windows AIK
```

Windows AIK をインストールしたら、HPCA Core サービスを再起動します。

詳細については、『HPCA Core および Satellite 入門およびコンセプト ガイド』の「HPCA を使用して Windows オペレーティング システムを管理する」を参照してください。

Sysprep のインストールおよび設定

Microsoft Sysprep は、クローン作成されたイメージを使用して Microsoft オペレーティング システムを配布できるようにするプログラムです。HPCA OS Manager Image Preparation Wizard によって Microsoft Sysprep が実行されます。これにより、セキュリティ識別子がすべて取り除かれて、イメージがリセットされます。

オペレーティング システム イメージがターゲット デバイスに配布された後でターゲット デバイスが起動されると、Microsoft ミニウィザードが自動的に実行されます。Sysprep.inf からの応答を使用した後、Microsoft ミニウィザードは、ターゲット マシンの Sysprep ディレクトリを削除します。

Sysprep をインストールするには

1 クローン作成されたイメージを使用して Microsoft オペレーティング システムを配布するために、Microsoft Sysprep をダウンロードします。

> Sysprep の使用方法、Sysprep.inf ファイルの作成方法、および使用可能なパラメータの設定方法については、Microsoft のドキュメントを確認してください。

2 Microsoft オペレーティング システムのインストール メディアの SUPPORT\TOOLS フォルダにある DEPLOY.CAB ファイルを見つけます。詳細は、Microsoft のドキュメントを参照してください。

3 Deploy.cab ファイルから Microsoft Sysprep ファイルを抽出します。これらのファイルを参照マシンの C:\SysPrep にコピーして、ディレクトリおよびファイルが読み取り専用に設定されていないことを確認します。

最新バージョンの Sysprep を使用していることを確認してください。古いバージョンを使用すると、エラーが発生する場合があります。

適切なバージョンの Sysprep がない場合は、Microsoft の Web サイトからダウンロードできます。

管理者権限を持っている場合でも、Sysprep を実行するための適切なユーザー権限を設定されていることを確認してください。Microsoft Web サイトの記事 #270032「Sysprep.exe プログラムの実行に必要なユーザー権利」を参照してください。適切なユーザー権限がない場合、Sysprep を実行すると、次のエラーが発生します。

「このアプリケーションを実行するには、管理者である必要があります。」

Image Preparation Wizard を終了し、適切なユーザー権限をセットアップしたら、再びウィザードを実行する必要があります。

4 Microsoft Sysprep を使用するために、参照マシンが、ドメインではなく WORKGROUP に所属していることを確認します。

5 Sysprep.inf を作成して、C:\Sysprep に保存します。

Sysprep.inf を作成するには

Sysprep.inf は手動で作成するか、Microsoft セットアップ マネージャ (Setupmgr.exe) を使用して作成できます。セットアップ マネージャは、Microsoft OS 配布メディアにある SUPPORT\TOOLS フォルダの Deploy.cab ファイルにあります。詳細は、Microsoft のドキュメントを参照してください。

Microsoft は、Windows 2000 用 Sysprep ユーティリティによる大容量ストレージ セクションの作成をサポートしていません。Windows 2000 でこのオプションを使用すると、イメージのキャプチャまたは配布中に問題が発生する場合があります。

サンプル Sysprep.inf ファイルは、Image Capture メディアの \samples\sysprep\ ディレクトリでは使用可能です。

Sysprep.inf ファイルのサイズは 800 KB 以下にしてください。

Sysprep.inf ファイルを作成する場合、次の操作を行います。

- TimeZone の値を環境に合わせて調整します。
- AdminPassword をセットアップします。

- ユーザーがターゲット デバイスに入力しなくて済むように、製品キーを作成します。
- 無人インストールを行うには、[Unattended] セクションに UnattendMode = FullUnattended を含める必要があります。
- ExtendOemPartition を 1 に設定します。これにより、Microsoft Sysprep は、OS のパーティションをそのディスクと物理的に連続した、パーティションが設定されていない使用可能な任意の空き領域へ拡張します。
- Sysprep.inf に JoinDomain が存在する場合、Sysprep.inf はコンピュータをドメインに接続する権限があるアカウントの管理ユーザー ID とパスワードを持っている必要があります。JoinDomain は大文字と小文字を区別することに注意してください。

Sysprep.inf ファイルの優先度の設定方法

Sysprep.inf ファイルはオペレーティング システム イメージとともに配布されるか、オペレーティング システム イメージに接続されたパッケージ (上書き Sysprep ファイル) として配布されます。Sysprep.inf ファイルが個別にパブリッシュされた場合、イメージの NTFS にある Sysprep.inf ファイルと統合され、1 つの Sysprep.inf になります。

Sysprep.inf ファイルは、次の順で低位から高位へ優先度が付けられます。

1. イメージに埋め込まれた Sysprep (優先度が最も低い)。個別にパブリッシュされる Sysprep.inf (上書き Sysprep) がない場合、イメージ内の Sysprep.inf が使用されます。
2. 上書き Sysprep (ゴールド イメージと別の Sysprep ファイル)。詳細については、151 ページの「Using an Override Sysprep File」を参照してください。

   上書き Sysprep.inf は 1 つだけ解決されます。

3. ポリシー条件に添付された Sysprep (優先度が最も高い)。

   - ポリシーに Sysprep ファイルを添付するには、HPCA database に Sysprep ファイルをパブリッシュして、Administrator CSDB Editor を使用して手動で Sysprep インスタンスを適切な Policy インスタンスに接続します。
   - Sysprep.inf を上書きした場合でも、ComputerName (COMPNAME) と JoinDomain (COMPDOMN) は、Portal の ROM オブジェクトに格納された Computer Name と Domain に基づいて、OS Manager により更新されます。

OS イメージのキャプチャ

実行するキャプチャのタイプに対応する次の手順を参照してください。

配布メソッド	手順
ImageX、Windows セットアップ、レガシー	579 ページの「Image Capture Wizard を使用したイメージのキャプチャ」 または 587 ページの「無人モードでの Image Preparation Wizard を使用したイメージのキャプチャ」
Windows Native Install Packager	589 ページの「Windows Native Install Packager を使用した配布用のイメージのキャプチャ」

Image Capture Wizard を使用したイメージのキャプチャ

ImageX、Windows セットアップ、またはレガシー配布で使用する OS イメージのキャプチャに関する手順を次に示します。

HPCA OS Manager Image Preparation Wizard を使用するには

イメージをローカルでキャプチャする場合、続行する前に、参照マシンを CD-ROM/DVD ドライブから起動するように設定します。ImageCapture メディアが起動可能なため、この作業を実行する必要があります。ImageCapture メディアを実行すると、デバイスを再起動して、イメージをアップロードします。

1 ImageCapture メディアを参照マシンに挿入します。このメディアの入手先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「製品メディア」を参照してください。

2 ImageCapture メディアで、\image_preparation_wizard\win32 に移動し、oscapture.exe を実行します。

➤ HPCA Agent が参照マシンにインストールされていない場合、次のメッセージが表示されます。

このコンピュータには Application Manager がインストールされていません。OS Manager 製品がインストールされているターゲット コンピュータは管理できない可能性があります。

デバイスを管理対象とするには、Image Preparation Wizard を実行する前に、必ず HPCA Agent をインストールしてください。

➤ oscapture.exe プログラムでは、Microsoft .NET Framework バージョン 2.0 (またはそれ以降) が必要になります。これは、次の Microsoft ダウンロード センターから入手できます。

http://www.microsoft.com/downloads

どのバージョンの .NET Framework が参照マシンに存在しているのかを確認するには、次のディレクトリのフォルダを表示します。

%SYSTEMROOT%/Microsoft.NET/Framework

— レガシー メソッドで配布するイメージをキャプチャする場合、Image Preparation Wizard では、続行する前に C:\Sysprep フォルダが存在すること、および HPCA agent がインストールされていることが検証されます。

— ImageX または Windows セットアップで配布するイメージをキャプチャすると、Image Preparation Wizard は Sysprep を C:\sysprep に置きます。

Windows XP Service Pack 2 を使用して ImageX または Windows セットアップで配布する場合は、配布プロセス中に HPCA Agent がイメージに挿入されます。

Agent をターゲット デバイス上のデフォルト以外の場所にインストールする場合、install.ini の INSTALLDIR プロパティを編集する必要があります。install.ini の変更方法の詳細については、『HP Client Automation Enterprise Application Manager および Application Self-service Manager インストールおよび設定ガイド』を参照してください。

Agent が既にデフォルト以外の場所のイメージにインストールされている場合も、同様に install.ini の INSTALLDIR プロパティを更新する必要があることに注意してください。

Agent がデフォルトの場所にインストールされている場合、install.ini を変更しないでください。

Publisher を使用して HPCA データベースにイメージをパブリッシュする前に、install.ini を編集する必要があります。

Publisher を使用する場合は、Agent を取得する場所を選択するオプションが表示されます。これには、Agent を個別にパッケージ化し、新しいバージョンを必要に応じて HPCA database にパブリッシュして Agent を更新できるという利点があります。これを実行すると、新たに配布する .WIM はすべて自動的に最新の Agent を使用します。

HPCA Standard ライセンスを使用している場合は、キャプチャしたイメージに Agent が既に含まれている必要があります。ただしその場合でも、Publisher を実行するときにパブリッシュ元の Agent を選択する必要があります。

3 **[次へ]** をクリックします。

[エンド ユーザー ライセンス契約] ウィンドウが表示されます。

4 **[同意する]** をクリックします。

配布方法は以下のようになります。

— **レガシー**は、パーティションのディスク イメージをそのままキャプチャします (.IMG 形式)。

— **ImageX** では、Windows PE や ImageX ユーティリティで配布される .WIM 形式でイメージがキャプチャされます。

— **Windows セットアップ**では、Windows PE や Windows セットアップ ユーティリティで配布される .WIM 形式でイメージがキャプチャされます。

OS でサポートされていない配布メソッドは表示されません。

5 使用する配布メソッドを選択し、**[次へ]** をクリックします。

6 HPCA server の IP アドレスまたはホスト名およびポートを入力します。これは、次の形式で指定する必要があります。

xxx.xxx.xxx.xxx:*port*

HPCA Core および Satellite インストールで OS のイメージングと配布用に使用される HPCA server ポートは 3466 です。HPCA Classic 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。

7 **[次へ]** をクリックします。

8 イメージ ファイルの名前を入力します。これは、*InstallDir*\Data\OSManagerServer\upload ディレクトリに格納されるイメージ名です。

9 **[次へ]** をクリックします。

[ディスク イメージのスパン] ウィンドウが表示されます。

10 各イメージ ファイルに使用するディスク容量 (非圧縮) の合計を MB 単位で入力します。スパンしたイメージを作成しないときは、「**0**」(ゼロ) と入力します。

スパンしたイメージを使用して、イメージ ファイルを小さいセグメントに分割できます。スパンされたイメージの各セグメントのサイズは 4 GB に制限されます。イメージを HPCA database に格納する場合、イメージ全体が 4 GB 以下である必要があるという条件を満たすことができるため、有用です。

この値を 0 (ゼロ) に設定した場合、イメージ リソース ファイルのサイズが 4GB を超えると、自動的にイメージがスパンされます。

11 **[次へ]** をクリックします。

該当する場合は、[追加の Sysprep オプション] ウィンドウが表示されます。このテキスト ボックスには、すべての SID をクリアし、キャプチャできるようにマシンを準備するコマンドが予め入力されています。

また、Sysprep に渡す追加オプションを、スペースで区切って入力することもできます。

これは高度なオプションです。追加したオプションや行った変更は検証されないため、イメージのキャプチャまたは配布が失敗する可能性があります。HP Software サポート担当者からこのような指示があった場合は、注意して作業を行ってください。

追加の Sysprep オプションについては、Microsoft のドキュメントを参照してください。

12 **[次へ]** をクリックします。

13 配布メソッドで ImageX を選択すると、デフォルトのオプションが選択された [Image Preparation Wizard のペイロードの選択] ウィンドウが表示されます。

ペイロードには、ターゲット デバイスに配布されるローカル サービスの起動 (LSB) データが含まれます。

14 イメージ ファイルの説明を入力し、**[次へ]** をクリックします。

[Windows 版の選択] ウィンドウが表示される場合があります。

15 取得する Windows のエディションを選択し、**[次へ]** をクリックします。

[オプション] ウィンドウが表示されます。

HPCA agent をインストールしていない場合は、**[OS のインストール後にクライアント接続を実行する]** チェック ボックスは表示されません。レガシー メソッドでイメージをキャプチャする場合にのみ、この Agent をインストールすることが重要になります。

16 適切なオプションを選択します。

キャプチャするオペレーティング システムによってオプションが表示されます。

— **Sysprep.inf に大容量ストレージ セクションをビルドする**
Windows XP 以上の `Sysprep.inf` の `[SysprepMassStorage]` セクションで、大容量ストレージ ドライバのリストをビルドするには、このチェック ボックスをオンにします。

Microsoft は、Windows 2000 用 Sysprep ユーティリティによる大容量ストレージ セクションの作成をサポートしていません。Windows 2000 でこのオプションを使用すると、イメージのキャプチャまたは配布中に問題が発生する場合があります。

大容量ストレージ ドライバのリストは、レジストリにインストールされます。これには約 15 ～ 20 分かかりますが、マシンのモデルおよびメーカーを越えたイメージ配布を成功させるため、基本的な大容量ストレージ デバイスのドライバを提供します。

これらの入力内容にエラーがあると、この後の Sysprep の実行は失敗する場合があります。

— **未使用のディスク スペースの圧縮を最適化する**
未使用ディスク領域の圧縮を最適化するには、このチェック ボックスをオンにします。これは、システム ドライブ パーティションの最後までゼロを追加します。注 : ハード ドライブの容量によっては、若干時間がかかる場合があります。

これにより、キャプチャしたイメージの圧縮率が大きくなり、サイズが小さくなります。イメージ ファイルのサイズが小さい方が、保存するディスク領域が少なく、ネットワーク上を転送するバンド幅が小さくて済みます。

— **OS のアップロードの前にパーティションのサイズを変更する**
パーティションのサイズをできるだけ小さくするには、このチェック ボックスをオンにします。このチェック ボックスをオンにしない場合は、パーティションのサイズが適切であるか確認してください。

— **OS のインストール後にクライアント接続を実行する**
OS をインストールした後に HPCA server に接続するには、このチェック ボックスをオンにします。このチェック ボックスをオンにしない場合は、OS がインストールされた後、HPCA OS 接続は実行されません。

Agent をインストールしない方法を使用する (たとえば、レガシー メソッドを使用していて、HPCA agent をインストールしなかった、あるいは配布時に Agent がインストールされデフォルトで接続が実行されるために Windows Vista (またはそれ以降) イメージをキャプチャする) 場合は、このオプションは表示されません。

17 **[次へ]** をクリックします。

[要約] ウィンドウが表示されます。

18 **[開始]** をクリックします。

19 **[完了]** をクリックします。

APIC デバイスで作業している場合は、[イメージを APIC 互換にする] ウィンドウが表示されます。Windows Vista (およびそれ以降) オペレーティング システムは APIC 互換デバイスでなければキャプチャ / 配布できないため注意してください。

20 必要であれば、**[Make image compatible with machine with PIC(イメージを PIC を搭載したマシン互換にする)]** チェック ボックスを選択します。

Microsoft はこれを推奨していません。この選択を行う前に、Microsoft の Web サイトで詳細を確認してください。

21 **[次へ]** をクリックします。

上図のチェック ボックスを選択した場合は、[Select Windows CD (Windows CD の選択)] ウィンドウが表示されます。

22 [Windows CD-ROM] へ移動し、**[次へ]** をクリックします。

23 **[完了]** をクリックして、Sysprep を実行します。

Image Preparation Wizard により Sysprep が起動されます。イメージのサイズによって完了時間は異なります (15 ～ 20 分)。

システム予約パーティションに LSB の挿入ファイルを格納できるスペースがない場合、メッセージがポップアップされます。このメッセージを無視するか、Image Preparation Wizard を停止します。メッセージを無視すると、Image Preparation Wizard が続行されます (このパーティションに十分なスペースが作成されている場合)。十分なスペースが作成されていない場合、LSB ファイルが挿入できないことを示すメッセージが表示されて失敗します。

キャプチャ中は、Service OS の画面にステータス情報が表示されます。詳細については、430 ページの「Windows PE Service OS 画面について」を参照してください。

完了後に、Sysprep はデバイスを再起動します。[**OK**] をクリックして、デバイスを再起動します。

監視モード (以前の出荷時モード) を使用している場合、マシンはオペレーティング システムをネットワーク接続が有効な状態で再起動します。カスタマイズが完了したら、Image Capture CD/DVD をマシンに挿入し、コマンド プロンプトから次を実行します。

```
sysprep.exe -reseal -reboot
```

Sysprep が再起動すると、イメージがサーバーにアップロードされます。

— ブート順が最初に CD-ROM からブートする設定になっていて、Image Capture メディアが読み込まれた場合は、デバイスは CD-ROM で起動されます。

デバイスに CD-ROM が搭載されない場合は、PXE 環境が必要で、デバイスはネットワーク優先で起動されるように設定されている必要があります。これで、ネットワーク起動中にキーボードの **F8** を押して、PXE によりイメージをキャプチャできます。メニューが表示された後、ぜひ [Remote Boot (Image Upload) (リモート ブート (イメージ アップロード))] を選択します。

レガシー キャプチャ モードでは、デバイスで CD ではなくオペレーティング システムが起動される場合、準備のプロセスをやり直す必要があります。

これで、デバイスがネットワークに接続され、HPCA server にイメージが格納されます。

- イメージのアップロードは、長時間かかるように感じられる場合があります。それは、アップロードではなく、イメージの圧縮と圧縮のための未使用ディスク領域の最適化 (特に、空きディスク領域が多くある場合) によるものです。これは、イメージの転送中に行われるため、ネットワークのパイプはボトルネックになりません。転送速度は約 300 KB/ 秒 ～ 1 MB/ 秒ですが、プロセッサの速度とネットワーク環境によって異なります。
- 必要に応じて取得できるように、\upload ディレクトリに格納するファイルのコピーを作成できます。

Image Preparation Wizard がネットワークに接続し、HPCA Core の次のディレクトリにイメージが格納されます。

InstallDir\Data\OSManagerServer\upload

アップロード プロセスが完了すると、以下のメッセージが表示されます。

**** OS イメージは正常に HPCA OS Manager Server に送信されました。

次に、イメージを HPCA database にパブリッシュします。433 ページの「パブリッシュ」を参照してください。

無人モードでの Image Preparation Wizard を使用したイメージのキャプチャ

設定ファイルを使用して、無人モードで Image Preparation Wizard を実行できます。

無人モードで Image Preparation Wizard を使用するには

1. ImageCapture メディアを参照マシンに挿入します。このメディアの入手先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「製品メディア」を参照してください。
2. \samples\prepwiz_unattend に移動し、OS 固有の設定ファイル (vista.cfg または xp.cfg) をローカル マシンまたはネットワーク上の場所にコピーします。
3. 必要な変更を行います。表 52 に、変更が必要な可能性がある値を示します。

表 52　変更する設定ファイル内の変数

変数名	説明	値の例
RISHOSTPORT	OS Manager Server の IP アドレス。	*xxx.xxx.x.x:port*
IMAGENAME	アップロードされるファイルを作成するために使用するプレフィックス。これは、アップロードされるイメージの名前を作成するために、.WIM に追加されます。	Vista
IMAGEDESC	データベースにパブリッシュされるイメージの説明。	「Windows Vista 無人テスト イメージ」

表 52　　変更する設定ファイル内の変数

変数名	説明	値の例
PREPWIZPAYLOAD (今後のリリース用)	管理者が使用するペイロード。 ペイロードには、ターゲットデバイスに配布されるローカル サービスの起動 (LSB) データが含まれます。	デフォルト値「/OSM/PREPWIZ/payload/default/」を使用します。
OSEDITION (Vista 用)	使用する Vista のエディションを指定します。	“Enterprise”
set ::setup(DEPLOYOS,SELECTED)	イメージのキャプチャ後に OS を再配布するかどうかを示す 1 または 0 の値。	“0”
set ::setup(ClientConnect,SELECTED)	イメージ配布後にターゲットデバイスで OS 接続を実行するかどうかを示す 1 または 0 の値。	“1”

4　参照マシンで、コマンド ウィンドウを開き、ディレクトリを CD/DVD に変更します。Image_Preparation_Wizard\win32 に移動します。ここで、次のコマンドを実行します。

```
prepwiz -mode silent -cfg <fully qualified
path>\<config_file>
```

<*config_file*> には、オペレーティング システム固有の設定ファイル (setup.cfg など) を指定します。

Image Preparation Wizard が Sysprep を起動します。これが完了するのに 15 ～ 20 分かかる場合があります。完了すると Sysprep によりデバイスがリブートされ、ネットワークに接続されて HPCA server の /upload ディレクトリにそのイメージが格納されます。

Windows Native Install Packager を使用した配布用のイメージのキャプチャ

この配布モードの Windows XP および Windows 2003 イメージのキャプチャは、HPCA Enterprise Edition でのみサポートされています。

この場合のみ、HPCA Windows Native Install Packager を使用してイメージを準備します。イメージは、参照マシンのハード ドライブ上の、Windows Vista 以前のオペレーティング システムのインストール メディアのイメージです。作成されるイメージは、Windows のインストールのファイル コピー フェーズを完了しており、HPCA Agent が含まれています。イメージは HPCA server の *InstallDir*\Data\OSManagerServer\upload ディレクトリに送信されます。次に、Publisher を使用してイメージを HPCA database にパブリッシュします。

イメージがターゲット デバイスに配布されると、ターゲット デバイスはリブートします。Windows Native Install セットアップは引き続きテキスト モード セットアップ フェーズを実行し、その後 GUI フェーズを実行します。2 つのフェーズは unattend.txt で制御され、完全自動セットアップが可能です。

- 589 ページの「タスク 1: 参照マシンの準備」
- 591 ページの「タスク 2: unattend.txt の作成」
- 592 ページの「タスク 3: HPCA Windows Native Install Packager のインストール」
- 592 ページの「タスク 4: HPCA Windows Native Install Packager の実行」

タスク 1: 参照マシンの準備

参照マシン上で作成されたオリジナルのインストール メディアのイメージがターゲット デバイスに配布されます。HPCA Windows Native Install Packager を使用してイメージを作成する前に、HPCA メディアを持っていることと、参照マシンが次の条件を満たしていることを確認します。

1. HPCA server に接続できる。
2. 以下の条件を満たすターゲット ドライブ (拡張パーティションにあることを推奨)。
   - ターゲット ドライブは現在フォーマットされており、空である (データがない) かのように扱われる。ターゲット ドライブがフォーマットされていない場合か、あるいはフォーマットされているが、データが含まれている場合に、ユーザーはドライブをフォーマットするよう要求されます。

— ユーザーがドライブにデータが確実に残らないようにドライブをフォーマットする場合は、あらかじめ FAT32 でフォーマットできる。

FAT32 では一度配布すると、拡張できないため、注意してください。NTFS は拡張できるデフォルトのオプションです。

— 1.5 GB 以上。Image Preparation Wizard の [未使用のディスク スペースの圧縮を最適化する] チェック ボックスがどのように設定されているかによって、ターゲット ドライブが大きくなれば、ドライブのイメージ化の処理時間が長くなる、または、イメージが必要以上に大きくなる場合があります。

ターゲット ドライブに保存するすべてのデータが失われます。

3 HPCA Windows Native Install Packager ソフトウェアが既にインストールされている、C: ドライブなどの独立したドライブ (高速化のため)。592 ページの「タスク 3: HPCA Windows Native Install Packager のインストール」を参照してください。

4 また、次の項目にアクセスする権限が必要です。HPCA Windows Native Install Packager を使用する場合は、項目の場所を指定します。

— HPCA Agent のセットアップ ファイル。

— オペレーティング システム メディアの i386 ディレクトリ。

必要なサービス パックは、すべてこのディレクトリにスリップストリームできます。これを実行する方法の詳細については、各サービス パックに関連する readme.txt ファイルを参照してください。

Windows セットアップで、古いバージョンの Windows 用のセットアップを実行することはできません。例 :

- デバイスで Windows XP が実行されている場合は、Windows 2000 用の i386 ディレクトリを使用できません。
- デバイスで Windows 2003 Server が実行されている場合は、Windows 2000 用または Windows XP 用の i386 ディレクトリは使用できません。

— unattend.txt

ファイルは手動で作成するか、Windows メディアの Windows セットアップ マネージャを使用して作成できます。使用可能なサンプル ファイルは、Image Capture メディアの \samples ディレクトリにあります。

タスク 2: unattend.txt の作成

unattend.txt ファイルでは、ユーザー入力が必要ないように、OS のインストールが自動化されます。unattend.txt ファイルは i386 ディレクトリで指定されている Windows のリリースと一致している必要があります。これらのファイルはインストールされている Windows のバージョンによって、若干異なる場合があります。

Unattend.txt ファイルは、800 KB 以下にしてください。

イメージとともに格納する unattend.txt ファイルを作成するときのヒントを次に示します。

- ファイルの中の設定は、環境にあるどのデバイスでも使用できるように、できるだけ汎用的にする必要があります。
- このファイルの [GuiUnattended] セクションには、ステートメント AutoLogon=YES および AutoLogonCount=1 を含めます。

  HPCA Agent セットアップでは、Agent をターゲット デバイスにインストールするために Windows インストーラが使用されます。また OEM\cmdlines.txt では Windows インストーラを実行できないため、OEM\cmdlines.txt の代わりに [GuiUnattended] セクションを使用する必要があります。

  AutoLogon ステートメントと AutoLogonCount ステートメントを使用すると、オペレーティング システムのインストール後に初めてのユーザーがログオンするときに、Agent が確実にインストールされます。
- このファイルの [Unattended] セクションには、ステートメント extendoempartition=1 を含めます。これにより、Windows はファイル システムとパーティションを拡張し、パーティションに続く未使用スペースを取り込むことができます。ターゲット パーティションが小さすぎる場合は、インストールのコピー フェーズを実行することはできます (このフェーズは参照マシンで実行されます)。その後、イメージが配布されると、テキスト モード フェーズは失敗します。あるいは、別のパーティションに OS がインストールされることもあります。

  大きいターゲット パーティションを使用している場合は、ファイルの未使用スペースにゼロを埋めるプロセスに時間がかかります。

- 必要なカスタマイズをするには、別の unattend.txt ファイルを作成することもできます。Publisher を使用してこれらのファイルを HPCA DB の SYSPREP クラスにパブリッシュできます。次に、それらを適切な OS イメージに接続できます。イメージが配布されると、カスタマイズした unattend.txt ファイルはオリジナルのファイルに統合されます。

  ファイルをパブリッシュする方法の詳細については、433 ページの「パブリッシュ」を参照してください。unattend.txt ファイルをパブリッシュするときは、Sysprep.inf ファイルをパブリッシュする場合と同じ手順に従います。

タスク 3: HPCA Windows Native Install Packager のインストール

1. Image Capture メディアで、\windows_native_install に移動して setup.exe をダブルクリックします。
2. **[次へ]** をクリックします。

   [エンド ユーザー ライセンス契約] ウィンドウが表示されます。
3. 条件を確認して、**[同意する]** をクリックします。
4. 製品のインストール先のディレクトリを選択して、**[次へ]** をクリックします。

   [要約] ウィンドウが表示されます。
5. **[インストール]** をクリックします。

   インストールが完了したら、**[完了]** をクリックします。

タスク 4: HPCA Windows Native Install Packager の実行

1. デスクトップにある HPCA Windows Native Install Packager アイコンをダブルクリックします。

   [設定オプション] ウィンドウの [Client Automation]、[Windows セットアップ]、[パッケージ] という 3 つの領域で、情報を入力する必要があります。

   a. [Client Automation] 領域には、Client Automation 製品に関連する設定オプションが表示されます。

   b. [Windows セットアップ] 領域では、OS のインストールを実行するのに必要な情報を収集します。

c [パッケージ] 領域では、作成するパッケージに関して HPCA で必要な情報が収集されます。

これらの各ウィンドウで、入力必須フィールドに入力しないまま **[次へ]** をクリックした場合、そのフィールドに入力するように、メッセージが表示されます。

2 [Client Automation Client ソース ディレクトリ] フィールドに、HPCA Agent のパスを入力します。

3 インストールする Client Automation 製品のチェック ボックスをオンにします。

4 OS のインストール後、HPCA OS 接続を実行するには、**[インストール後、最初の接続を実行]** チェック ボックスをオンにします。このチェック ボックスがオンになっていないと、OS のインストール後に、HPCA OS 接続は自動的に実行されません。

5 **[任意指定の Packager コマンド ライン引数]** ボックスに、WNI アプリケーションで使用されるパラメータを入力します。オプションは 1 行ですべてを入力することも、複数行にわたって入力することもできます。オプションは次のような「キーワード値」の形式で指定します。

```
-trace_level 9
```

キーワードの先頭には必ずダッシュ (-) を付けます。

テクニカル サポートの指示では、通常 [任意指定の Packager コマンド ライン引数] テキスト ボックスのみを使用します。

ログを作成するためのパラメータが多数あります。次の例では、C:\temp\nvdwni.log という名前のファイルを作成する方法を説明します。

```
-trace_level    99
-trace_dir       c:\temp
```

別の名前でログを作成する場合は、以下を使用します。

```
-trace_file filename.log
```

6 **[次へ]** をクリックします。

7 **[unattend.txt ファイル]** ボックスで、適切な unattend.txt ファイルを参照します。

イメージに格納する汎用 unattend.txt ファイルを選択します。このファイルは、イメージが適用するすべてのデバイスに適用可能なオプションを含んでいる必要があります。必要なカスタマイズをするには、イメージに個別の unattend.txt ファイルを添付することができます。

unattend.txt ファイルは i386 ディレクトリで指定されている Windows のリリースと一致している必要があります。これらのファイルはインストールされている Windows のバージョンによって、若干異なる場合があります。

8 **[i386 ディレクトリ]** テキスト ボックスで、Microsoft の配布メディアで提供される Windows 配布元ディレクトリを選択します。Microsoft のスリップストリーム プロセスを使用して、サービス パックおよびその他の修正を統合できます。これを実行する方法の詳細については、各サービス パックに関連する readme.txt ファイルを参照してください。

必ず Windows CD-ROM から i386 ディレクトリを別の場所にコピーしてください。CD-ROM を使用する場合、Windows セットアップは、CD-ROM がターゲット デバイスに読み込まれたと想定して、必要なファイルをすべてコピーしない恐れがあります。

9 **[ターゲット ドライブ]** ドロップダウン リストで、ネイティブ インストール パッケージを作成するドライブを選択します。拡張パーティション上にあるドライブを選択することを推奨します。

このドライブに既存のすべてのデータが失われます。

10 **[特別なコマンド ライン パラメータ]** テキスト ボックスで、Windows セットアップ プログラムを実行するときに、プログラムに渡すパラメータをすべて入力します。パラメータの詳細については、Microsoft web サイトを参照してください。

11 **[次へ]** をクリックします。

12 **[イメージ名]** テキスト ボックスに、\upload ディレクトリに格納するパッケージの名前を入力します。この名前に入力する文字は、8 文字以内の英数字である必要があります。

13 **[イメージの説明]** テキスト ボックスにイメージの説明を入力します (半角 255 文字まで)。

14 **[Client Automation OS Manager Server]** テキスト ボックスに、イメージをアップロードする HPCA server の IP アドレスまたはホスト名を指定します。

15 **[Client Automation OS Manager ポート]** テキスト ボックスに、HPCA server のポートを指定します。

16 **[未使用のディスク スペースの圧縮を最適化する]** チェック ボックスをオンにし、ターゲット ドライブをイメージ化する前に、未使用ディスク スペースをすべて null にします。この設定によって、イメージのサイズを小さくすることができますが、Image Preparation Wizard の実行時間がより長くなります。

17 **[次へ]** をクリックします。

18 [要約] を確認し、**[作成]** をクリックします。

Windows 2000 デバイスで **[作成]** をクリックした後、Windows セットアップによってシステムのリブートが要求される場合があります。再起動をしない場合は、**[キャンセル]** をクリックします。再起動は必要ありませんが、再起動が起こっても、障害はありません。

Windows セットアップが実行され、HPCA Windows Native Install Packager に戻ります。

19 HPCA Windows Native Install Packager が完了すると、Linux CD-ROM/DVD でシステムのリブートを求めるメッセージが表示されます。これは、Image Capture メディアを指しています。

まず CD-ROM/DVD から起動するように起動順を設定する必要があるため、注意してください。

20 Image Capture メディアを挿入して、[**OK**] をクリックしてください。

21 **[完了]** をクリックします。

22 デバイスをリブートすると、イメージが *InstallDir*\Data\OSManagerServer\upload ディレクトリにアップロードされます。

23 OS イメージが正常に HPCA Server に送信されたことを示すメッセージが表示されたら、ドライブからメディアを取り出し、デバイスを再起動します。

OS イメージのパブリッシュおよび配布

イメージをキャプチャしたら、Publisher を使用して HPCA データベースにそのイメージをパブリッシュします。手順については、433 ページの「パブリッシュ」を参照してください。

イメージをパブリッシュしたら、OS ライブラリをリフレッシュして、使用可能な OS イメージのリストを表示します。HPCA Console ツール バーを使用して、選択したデバイスにイメージを配布します。

H カスタム Windows PE Service OS のビルド

この章は、次のトピックで構成されています。

カスタム ビルド スクリプトについて

HP が提供するスクリプトを利用して、次のことができます。

- 中国語または韓国語のフォントのサポートを追加する。
- 更新された Windows Automated Installation Kit (AIK) から新しい `winpe.wim` ファイルが使用可能になったときに、Windows Preinstallation Environment (PE) Service OS を更新する。
- 提供された Windows PE Service OS 内にはない、ドライバやパッケージを追加する。
- Microsoft Windows AIK に関する知識とともに、この章の情報を使用して、使用環境に必要なドライバやパッケージを含む Windows PE Service OS を再ビルドする。
- デフォルトの Service OS の変更やブート メニューの設定の変更など、適用する必要がある更新がある場合に新しい `ImageCapture.iso` を作成する。
- デフォルトの Service OS の変更やブート メニューの設定の変更など、適用する必要がある更新がある場合に新しい `ImageDeploy.iso` を作成する。

前提条件

HP が提供するスクリプトを使用してカスタム Windows PE Service OS をビルドするには、いくつかの前提条件を満たしている必要があります。詳細については、次のトピックを参照してください。

- 599 ページの「プロセスの知識」
- 599 ページの「Administrator マシン」
- 600 ページの「メディア」
- 600 ページの「ファイルとディレクトリ」
- 601 ページの「他の言語のサポート」
- 601 ページの「高度なオプション」

互換性のないソフトウェアがインストールされているマシンで、このスクリプトを実行しないでください。Administrator マシンの前提条件を参照してください。

プロセスの知識

Windows PE Service OS にドライバやその他の情報を追加するには、Microsoft のインストール前のカスタマイズ プロセスに関する基本的な理解が必要です。

Administrator マシン

スクリプトを実行するには、Windows Automated Installation Kit (AIK) の 32 ビットバージョンがインストールされている Administrator マシンが必要です。このマシンを使用して、カスタマイズされた Windows PE Service OS をビルドします。

次のソフトウェアがインストールされているマシンは使用しないでください。

- HPCA Boot Server
- HPCA Core Server または HPCA Satellite Server
- Cygwin

Windows AIK バージョン 1.1 および 2.0 がサポートされています。バージョン 1.1 は、Windows Vista および Windows Server 2008 に付属しています。バージョン 2.0 は、Windows 7 および Windows Server 2008 R2 に付属しており、下位互換性があります。どちらのバージョンも Microsoft Web サイトからダウンロードできます。

Windows AIK の 32 ビット バージョンがダウンロードされ、インストールされていることを確認します。

メディア

次のメディア (DVD または CD-ROM) が必要です。

- HPCA 製品メディア
- HPCA Image Capture メディア
- HPCA Image Deploy メディア

ファイルとディレクトリ

- HPCA 製品メディアの `build_scripts.zip` ファイルが必要です。
- 新しい `ImageCapture.iso` または `ImageDeploy.iso` を生成する場合、次の操作を行って必要な更新済みファイルを含めます。
  a. Administrator マシンに、`c:\build_items` のようなビルド アイテムのディレクトリを作成します。
  b. *オプション*: HP から受け取った更新されたファイルを、ビルド アイテムのディレクトリにコピーします。必要に応じて、Image Capture メディアまたは Image Deploy メディアの構造を基にサブディレクトリを作成します。

     このディレクトリに必要なファイルがすべて揃っていない場合は、ファイルをコピーするために、以前の Image Capture メディアまたは Image Deploy メディアの挿入が要求されます。
  c. *オプション*: ImageDeploy CD で使用するために、`romsinfo.ini` または `netinfo.ini` をビルド アイテムのディレクトリに含めることができます。
  d. *オプション:* 適切な ISO で使用するために、`rombl_capture.cfg` と `rombl_deploy.cfg` をビルド アイテムのディレクトリに含めます。このファイルには、メニューのタイムアウト設定やデフォルトの Service OS などの情報が含まれます。

これらのファイルを作成するために、必要に応じて以前の ImageCapture.iso または ImageDeploy.iso から rombl.cfg をコピーしてファイルを編集したり、名前を変更したりできます。

これらのファイルがビルド アイテムのディレクトリに含まれていない場合、以前の CD-ROM とそのメディアからのファイルの取得を促すメッセージがスクリプトによって表示されます。CD-ROM を挿入しないことを選択すると、標準の rombl.cfg ファイルが自動的に作成されます。

他の言語のサポート

ISO に変更を加えずに、中国語または日本語のサポートを追加する場合は、次のようにします。

- 既存の winpe.wim ファイルを build_items ディレクトリから削除します。
- 製品 CD-ROM の \custom_build\lang_support ディレクトリから、winpe_cjk.wim を build_items ディレクトリにコピーします。
- 名前を winpe_cjk.wim から winpe.wim に変更します。
- 603 ページの「カスタム Windows PE Service OS のビルド」を参照して、スクリプトを実行します。

  中国語または日本語が有効になった winpe.wim ファイルを、winpe.wim ファイルを再ビルドせずに使用するには、winpe.wim ファイルの再作成を求められたときに「**N**」と入力します。

- ImageDeploy CD を使用して、CD からインストールするかキャッシュからインストールしているときに、メッセージをローカル言語で表示する場合は、製品メディアにある \custom_build\lang_support\i18n ディレクトリをビルド アイテムのディレクトリにコピーします。ローカル言語で必要のない .msg ファイルは削除できます。

高度なオプション

次の情報は、経験を積んだ HPCA 管理者のみを対象としています。HPCA による OS 管理と Microsoft Windows AIK ツールの両方をよく理解している場合を除き、既存の winpe.wim ファイルをカスタマイズしないでください。

既存の winpe.wim ファイルを使用する場合

- 既存の winpe.wim は、ビルド スクリプトを実行しているマシンにインストールされている Windows AIK と同じバージョンの Windows AIK を使ってビルドすることを強く推奨します。
- winpe.wim ファイルには次のパッケージがインストールされている必要があります。
  - Windows AIK バージョン 1.1 の場合
    - WinPE-HTA-Package
    - WinPE-Scripting-Package
    - WinPE-XML-Package
    - WinPE-WMI Package
  - Windows AIK バージョン 2.0 の場合
    - WinPE-hta.cab
    - WinPE-scripting.cab
    - WinPE-wmi.cab
    - WinPE-setup.cab
    - WinPE-legacysetup.cab
    - WinPE-setup-client.cab
    - WinPE-setup-server.cab
- winpe.wim ファイルが peimg /prep コマンドを使用して作成されている場合は、Windows AIK、peimg、ImageX の Microsoft ドキュメントに記載されている制限 (Windows AIK 1.1 にのみ適用) を参照してください。

Windows PE Service OS へのドライバの追加

ビルド スクリプトを実行するときに Windows PE Service OS にドライバを追加できます。たとえば、リブートが必要なドライバがある場合、「オフライン」モードで実行する必要があります。つまり、ビルド スクリプトが一時停止し、そのときに必要な変更を実行できます。詳細については、次の手順で説明します。

また、Windows PE が実行されているときに (「オンライン」モード) ドライバを追加することもできます。すべてのドライバがリブートを必要とせずにすべて含まれていて、デバイスは HPCA server に接続されている必要があります。

Windows PE Service OS の起動中に、*InstallDir*\OSManagerServer\SOS\WinPE\drivers に存在するすべてのドライバがダウンロードされ、drvload.exe を使用してインストールされます。

カスタム Windows PE Service OS のビルド

次のトピックでは、HPCA によって提供されるスクリプトを取得および使用して、カスタム Windows PE Service OS をビルドする方法について説明します。

- スクリプトを取得して実行の準備をする方法については、603 ページの「スクリプトの取得」を参照してください。
- スクリプトを起動して必要な情報を指定する方法については、604 ページの「スクリプトの実行」を参照してください。
- スクリプトを実行したら、608 ページの「その他の情報」を参照してください。

スクリプトを起動する前に、599 ページの「前提条件」の内容を参照してその前提条件を満たしていることを確認してください。

スクリプトの取得

カスタム Windows PE Service OS のビルドに必要なスクリプトは、HPCA インストール メディアにあります。次の手順に従ってスクリプトを取得し、Administrator マシンで実行する準備をします。

スクリプトを取得し、Administrator マシンでスクリプトを使用できるようにするには

1 インストール メディアにある *InstallDir*\media\ISO\roms\build_scripts.zip を Administrator マシン (Windows AIK がインストールされている場所) にコピーします。

2 任意のディレクトリ (C:\Build_scripts など) に build_scripts.zip を展開します。

スクリプトの実行

この手順では、前提条件 (599 ページの「前提条件」を参照) を満たしていることと、スクリプトを取得 (603 ページの「スクリプトの取得」を参照) していることを前提としています。

カスタム Windows PE Service OS をビルドするには

1. Windows コマンド プロンプトで、作成したディレクトリ (`C:\Build_scripts` など) に移動します。
2. 「**run**」と入力します。
3. 使用する HPCA のバージョンに対応する番号を入力します。
4. 新しい WIM ファイルを作成するかどうか尋ねられたら、「**Y**」または「**N**」と入力します。

   `winpe_cjk.wim` を使用していて、`winpe.wim` ファイルを再ビルドしない場合、後で `winpe.wim` ファイルの再作成を求められたときに「**N**」と入力します。

   「**Y**」と入力すると、Windows AIK ツールのディレクトリへのパスの入力を求められます。たとえば、「`C:\Program Files\Windows AIK\Tools`」と入力します。
5. Microsoft Windows AIK の `winpe.wim` ファイルを使用するかどうか尋ねられたら、「**Y**」または「**N**」を入力します。

   Microsoft Windows AIK の `winpe.wim` ファイルを使用することを強く推奨します。

   「**N**」を入力した場合は、既存の `winpe.wim` ファイルが仕様通りにビルドされていることを確認するようにリマインダが表示されます。次に、既存の `winpe.wim` ファイルへのフル パスを指定するように促されます。
6. ローカル フォントのサポート パッケージを含めるかどうかを尋ねられたら、「**Y**」または「**N**」を入力します。
7. ドライバまたはパッケージを追加するために WIM 作成プロセスを一時停止するかどうかを尋ねられたら、「**Y**」または「**N**」を入力します。
8. WIM 作成プロセス中に追加するドライバのディレクトリのパスを指定するかどうかを尋ねられたら、「**Y**」または「**N**」を入力します。

「**Y**」と入力した場合は、ドライバを含むディレクトリへのフル パスを入力するように求められます。

9 次の一連の質問によって、Image Capture ISO と Image Deploy ISO のどちらを新規作成するのか、さらに、どの Service OS を含めるのかが決まります。

— 次の条件のいずれかに一致する場合、新しい Image Capture ISO を作成する必要があります (「**Y**」と入力)。

– HP Software サポートから更新済みファイルを受信している。

– winpe.wim を再ビルドしており、ISO を使用してキャプチャを実行する。

– 設定 (rombl.cfg、netinfo.ini、または rominfo.ini) を変更する必要がある。

— 次の条件のいずれかに一致する場合、新しい Image Deploy ISO を作成する必要があります (「**Y**」と入力)。

– HP Software サポートから更新済みファイルを受信している。

– winpe.wim を再ビルドしており、配布中に CD からブートする。

– 設定 (rombl.cfg、netinfo.ini、または rominfo.ini) を変更する必要がある。

ISO オプションを指定するには、次の手順に従います。

a 新しい Image Capture ISO を作成するかどうか尋ねられたら、「**Y**」または「**N**」を入力します。

b 新しい Image Deploy ISO を作成するかどうか尋ねられたら、「**Y**」または「**N**」を入力します。

c 質問 (a) または (b) に対して「**Y**」と入力すると、ISO に含める Service OS を尋ねられます。適切な Service OS を選択します。次に、**Enter** キーを押します。

d 新しい rombl.cfg ファイルを作成するか、既存の rombl.cfg ファイルを使用するかを尋ねられたら、次のいずれかの操作を行います。

– 新しい rombl.cfg ファイルを作成する場合は、「**1**」と入力し、**Enter** キーを押します。

– 既存の rombl.cfg ファイルを使用する場合は、「**2**」と入力し、**Enter** キーを押して手順 (h) に進みます。

e どの Service OS をデフォルトで起動するかを尋ねられたら、適切な選択を入力します。次に、**Enter** キーを押します。

f 作成する各 ISO のブート メニューの処理方法を指定します。次の 3 つの方法があります。

0 ブート メニューはターゲット デバイスのユーザーに表示されません。
手順 (d.e) で指定したデフォルトの Service OS が使用されます。

-1 ブート メニューが表示され、ユーザーからの応答を待機します。
この応答によってデフォルトの Service OS の設定が上書きされます。

1 以上の数値 ブート メニューが表示され、ユーザーからの応答をこの秒数の間待機します。この秒数を過ぎると、手順 (e) で指定したデフォルトの Service OS がブートされます。

g OS Manager インフラストラクチャに接続するために使用されるポートを変更するかどうかを尋ねられたら、「**Y**」または「**N**」を入力します。デフォルト ポートは 3466 です。

h ISO ブート セクタに含まれる ISO ブート ロード値を指定するかどうかを尋ねられたら、「**Y**」または「**N**」を入力します。

デフォルト値を使用していて問題が発生し、HP Software サポートにデフォルト値を変更するように指示された場合にのみこのオプションを使用します。

特定のハードウェア モデルでは、BIOS の問題が原因でブート ロード セグメントを 0x2000 にする必要があります。他のモデルの場合、ブート ロード セグメントが El Torito ISO 形式 (0x0000) のデフォルトのローダー セグメントでないと CD からブートできません。

ブート ロード セグメントの設定を指定するには、「**1**」、「**2**」または「**3**」を入力します。

1 HPCA のデフォルト (0x2000) ñ 大部分の BIOS で動作します。

2 ISO のデフォルト (0x0000) ñ 大部分の BIOS で 0x07c0 に変換されます。

3 手動で値を入力します。

次に、**Enter** キーを押します。「**3**」と入力した場合、0x で始まる 16 進数の文字列としてブート ロード セグメントの設定を指定します。

i ビルド アイテムのフル パスの入力を求められたら、ディレクトリ名 (`C:\build_items` など) を入力し、**Enter** キーを押します。

これで、Image Capture ISO および Image Deploy ISO に関連する質問は完了します。

10 一時作業ディレクトリのフル パスを求められたら、ディレクトリ名 (C:\build_work など) を入力します。このディレクトリは、以降の手順で *<work-dir>* と呼ばれます。

> そのディレクトリが既に存在しており、その中に情報がある場合、その情報を削除するかどうかを尋ねられます。削除しないことを選択すると、もう一度ディレクトリの入力を求められます。終了する場合は、**Ctrl + C** キーを押してプロセスを終了します。削除することを選択すると、情報は上書きされます。

11 出力ディレクトリのフル パスを求められたら、ディレクトリ名 (C:\build_output など) を入力します。

> CAS 用の ISO を作成するかどうか尋ねられたら、「**N**」と入力します。

画面に表示されるメッセージでわかるように、このビルド プロセスは時間がかかります。完了すると、Service OS 作成プロセスが正常に終了したことを示すメッセージが表示され、コマンド プロンプトに戻ります。

最後の手順

ビルドが完了したら、C:\WinPE_output など、Windows PE.wim が格納されたディレクトリに移動し、次の操作を実行します。

表 53

ターゲット デバイスのブート メソッド	必要な操作
PXE	出力ディレクトリから winpe.wim を *InstallDir*\BootServer\X86PC\UNDI\boot にコピーします。
LSB	CSDB Editor を使用して LSB パッケージの winpe.wim を置換します。
CD	Windows PE スクリプトを使用して、新しい ISO を作成します。

ImageCapture.iso または ImageDeploy.iso を作成することを選択した場合、同じ出力ディレクトリに格納されます。

その他の情報

Windows PE Service OS のカスタム ビルド スクリプトに必要なすべての情報を入力すると、次の処理が実行されます。

1. ISO のビルドに必要なファイルがビルド アイテムのディレクトリにない場合、CD/DVD を挿入し、ファイルをコピーする必要があります。CD/DVD の挿入を選択しない場合、ビルド プロセスは停止します。
2. 入力した情報が保存され、Windows PE ディレクトリの作成が始まります。
3. ドライバまたはパッケージを追加するために WIM 作成プロセスを一時停止することを指示した場合、Windows PE ディレクトリが作成された後にプロセスが一時停止され、`winpe.wim` の内容が WIM ディレクトリ (`C:\build_work\WIM` など) に抽出されます。これには、次の 2 つの方法があります。

   メソッド A: Windows AIK ツールを使用して変更を行います。

   Windows AIK バージョン 1.1 を使用している場合、`peimg.exe` コマンドを使用します。この実行ファイルのデフォルトの場所は、次のとおりです。

   ```
   C:\Program Files\Windows AIK\Tools\PETools\peimg.exe
   ```

   Windows AIK バージョン 2.0 を使用している場合、`dism.exe` コマンドを使用します。この実行ファイルのデフォルトの場所は、次のとおりです。

   ```
   C:\Program Files\Windows AIK\Tools\Servicing\dism.exe
   ```

   これらのコマンドの使用方法については、Windows AIK のドキュメントを参照してください (または **`/help`** コマンド ライン オプションを使用してください)。

   メソッド B: ドライバをドライバ リストに追加します。

   必要な情報がすべて収集されたことを示すメッセージが表示された後、`winpe.wim` および ISO をビルドするために必要な情報を格納する `C:\Build_scripts` ディレクトリに `build.config` ファイルが作成されます。テキスト エディタを使用してこのファイルを開き、空の `DRIVERS` リストの下に適切なドライバを追加できます。

   例 :

   ```
   declare DRIVERS = " cdrom.inf \
           e:\\tmp\\work\\WIM\\windows\\inf\\adp94xx.inf \
           e:\\tmp\\work\\WIM\\windows\\inf\\3com*.inf "
   ```

バック スラッシュ (\) は特殊文字であるため、この例のようにバック スラッシュを 2 つ使用して「エスケープ」する必要があります。

最後の行以外のすべての行がバック スラッシュで終わっていることに注意してください。この例では、バック スラッシュは宣言の継続を示しています。

ディレクトリを指定しない場合は、スクリプトが *<work-dir>*\WIM\Windows\inf ディレクトリの中のドライバを検索します。

指定する場合は、c:\\anydirectory\\mydrivers.inf のように場所とドライバをフル パスで指定できます。

また、c:\anydirectory にあるすべての md*.inf ファイルをインストールする、c:\\anydirectory\\md*.inf などのワイルド カードを含むファイル名を持つパスを指定することもできます。

完了後、「**run**」と入力して続行すると、ドライバが winpe.wim に追加されます。

今後再度スクリプトを実行すると、build.config ファイルを保持するか、新しいファイルと交換するか尋ねられます。また、スクリプトは自動的に一時停止されます。追加するパッケージまたはドライバが他にない場合は、「**run**」と入力して続行します。

カスタマイズした build.config ファイルの使用 (高度なオプション)

任意で、既存の build.config ファイルを別の名前で保存できます。多様な設定セットを維持する必要がある場合や、既存の設定を基にテストをしている場合、既存の build.config ファイルの別名保存が必要になる場合があります。ドライバは上で指定したようにファイルに追加できます。

ファイルは、C:\build_scripts など、build_scripts.zip ファイルを展開したディレクトリに配置します。

スクリプトを実行する場合は、「**run**」と入力する代わりに次のコマンドを使用します。

```
run.cmd -f mybuild.cfg
```

貿 パラメータを指定しない場合、デフォルトの build.config ファイルが作成され、使用されます。

索引

I

J

L

M

N

O

P

R

S

T

し

す

せ

そ

た

ち

つ

ろ

わ