HP Client Automation Enterprise

パッチ管理

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: 8.10

リファレンス ガイド

ドキュメントのリリース日: 2012 年 2 月
ソフトウェアのリリース日: 2012 年 2 月

ご注意

保証

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

本書に記載した内容は、予告なしに変更されることがあります。

権利の制限

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

著作権について

商標

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。

Oracle および Java は Oracle Corporation またはその関連会社、あるいはその両方の登録商標です。

UNIX® は、The Open Group の登録商標です。

謝辞

この製品は、Apache Software Foundation (http://www.apache.org/)（英語サイト）で開発されたソフトウェアを含みます。

この製品は、Eric Young (eay@cryptsoft.com) が開発した暗号化ソフトウェアを含みます。

この製品は、OpenSSLツールキットでの使用のために OpenSSL プロジェクト (http://www.openssl.org/)（英語サイト）が開発したソフトウェアを含みます。

この製品は、Tim Hudson (tjh@cryptsoft.com) が開発したソフトウェアを含みます。

ドキュメントの更新

本書のタイトル ページには、次の識別情報が含まれています。

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

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

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

このサイトを使用するには HP Passport に登録してサインインする必要があります。HP Passport ID を登録するには，次の URL を参照してください。

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

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

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

サポート

HP Software のサポート Web サイトは次のとおりです。

http://support.openview.hp.com/

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の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サブミットと追跡
- ソフトウェア パッチのダウンロード
- サポート契約の管理
- HP サポート連絡先の確認
- 利用可能なサービスに関する情報の確認
- 他のソフトウェア顧客とのディスカッションへの参加
- ソフトウェア トレーニングの検索と登録

サポート領域のほとんどでは HP Passport ユーザーとして登録しサインインする必要があります。また多くの場合サポート契約も必要です。HP Passport ID に登録するには、次のサイトにアクセスしてください。

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

アクセス レベルに関する詳細については、次を参照してください。

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

目次

1 はじめに 9
パッチ管理の概要 10
略語と変数. 11
用語 12

2 パッチ取得. 15
パッチ取得プロセス 16
取得の概要. 16
パッチ説明ファイル (XML) について 17
Microsoft パッチの取得と管理について 19
新しい Microsoft Update Catalog (wsusscn2.cab) の組み込みサポート. 19
Microsoft Update Catalog の要件 : 最低限必要な OS とサービス パックのレベル . . .19
Microsoft データ フィードに対する Patch Management のベンダー設定 19
Microsoft Office と Microsoft Update Catalog 20
Windows インストーラ 3.1 の要件. 20
Microsoft 自動更新について 20
Red Hat パッチの取得について. 22
カスタム パッチ説明ファイルの作成 25
mib (Manage Installed Bulletins) オプションの設定 27
パッチ取得レポート 28
取得の概要 28
取得 (ブリテン別). 28
取得 (パッチ別). 29

3 パッチの評価、分析、レポート 31
製品探索と分析 32
Microsoft Office セキュリティ ブリテンの検出と管理. 33
Microsoft Office セキュリティ ブリテン管理の最善実践 34

Windows インストーラ 3.1 の要件 34
Microsoft Office 製品の更新オプション 35
Patch Management を使用して Microsoft Office の更新を配布する場合 36
Patch Management の使用時に無効にされる Client Automation 管理機能 37
Microsoft Update Catalog による Office XP、Office 2003、および Office 2007 のサポート 37
Microsoft Office のサービス パック 38
Microsoft Update Catalog を有効にした最善実践 38
Patch Management および Microsoft Update Catalog について 38
Patch Management (バージョン 3.0.2 以上) での Microsoft Office 更新の有効化 . . . 40
デバイス適合性レポートで使用するパッチ オブジェクトについて 41
パッチの分析とレポート 42
Reporting Server によるパッチ レポートのフィルタリング 43
詳細な情報への掘り下げ 43
利用可能なレポートのアクションに追加されたデータ エクスポート オプション 44
概要 45
デバイス全体のステータス 46
デバイスのステータス 47
ブリテンのステータス 47
ベンダーのステータス 48
パッチ適合性レポート 48
デバイスのステータス 49
フル パッチが適用されていないデバイス 50
再起動を保留中のデバイス 51
ブリテンのインストール エラーがあるデバイス 51
ブリテンのステータス 51
製品ステータス 53
リリースのステータス 53
パッチのステータス 54
重大なエラーが発生したデバイス 54
取得レポート 55
リサーチ レポート 55
リサーチ (ブリテン別) 55
リサーチ (デバイス別) 56
リサーチ (パッチ別) 56
リサーチ (製品別) 57

リサーチ (リリース別). 57
適合性とリサーチ例外レポート 57
脆弱性の管理 58
SuSE 10 および 11 ブリテンのインスタンス名の命名規則 59
SuSE 10 の場合 59
SuSE 11 の場合 60
FINALIZE_PATCH サービスの使用許可 61
自動および対話型パッチの配布 61
レポーティング オプションのカスタマイズ 62
脆弱性の検出と配布の無効化 65
パッチの配布の制御 (PATCHARG) 65
パッチの削除 66
要約 68

A パッチで使用できる XML タグ 69
説明ファイル 69
Bulletin ノード 69
Products ノード 72
Products ノード 72
Releases ノード 72
Release ノード 73
Patch ノード 73
Patch Signature ノード 77
FileChg ノード 77
RegChg ノード 78
HPFileset ノード 80

B 管理対象デバイスの再起動 81
アプリケーション イベント 81
リブート タイプ 82
リブート修飾子 : 警告メッセージのタイプ 83
リブート修飾子 : マシン オプションとユーザー オプション 84
リブート修飾子 : 即時の再起動 85
複数の再起動イベントの指定 85

C Patch.cfg のパラメータ 87
Patch Management Server の設定パラメータ 87
パッチ取得パラメータ 93
データベース同期パラメータ 97
Patch Agent の更新パラメータ 99
索引 101

1 はじめに

このは、HP Client Automation Patch Management の概要を理解することを目的としています。トピックには次の内容が含まれます。

— 10 ページの「パッチ管理の概要」

— 12 ページの「用語」

パッチ管理の概要

HP Client Automation Patch Management は、ビジネスを継続し、セキュリティのイニシアチブを取ることによる価値を提供します。

パッチ管理アクティビティの主な機能は、以下のとおりです。

- **取得**
  サポートされるベンダーが提供する Web ベースのリポジトリの内容に基づいて、Microsoft のセキュリティ更新 (パッチ)、更新のロールアップ、およびサービス パックだけでなく、Red Hat および SuSE のセキュリティ ブリテン (アドバイザリ) の自動収集を可能にする設定可能なツールです。

  > HP-UX および Sun Solaris (Sparc) に関するセキュリティ ブリテン (アドバイザリ) の取得に対するサポートは含まれていません。HP-UX または Sun Solaris エージェント デバイスの管理はサポートされません。

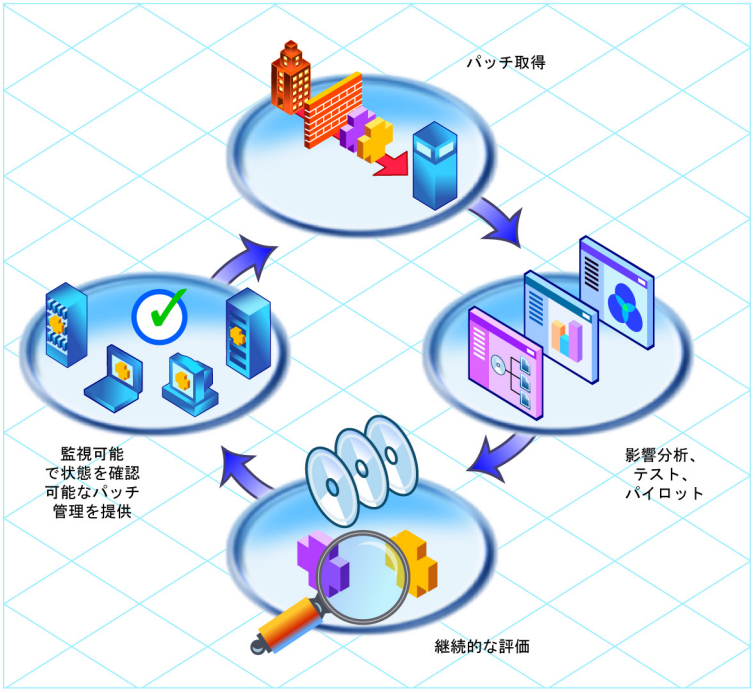
- **パイロット テスト**
  使用状況や重要度に応じて、対象とするパイロット グループを IT 管理者が選択できます。HP Client Automation は、このような固有のパイロット テストの機能を備えた唯一のソリューションで、業務上重要なシステムの安定性を確保するために有用です。

- **適用状況と脆弱性の評価**
  ネットワーク上のデバイス、各デバイスにインストールされているソフトウェア製品、および各ソフトウェア製品に適用済みのセキュリティ パッチの自動的かつ継続的な探索と、適用可能ソフトウェア製品の識別を行います。このように完全な探索および評価を行うプロセスにより、IT 管理者は全体的なセキュリティの脆弱性とシステムの適用状況を常に把握できます。

- **配布**
  さまざまな既存のポリシーの送信元 (Active Directory、LDAP、SQL のデータベースなど) と直接連結するポリシー ベースの配布機能を使用して、サーバー、デスクトップ、およびラップトップに配布するパッチを自動的に迅速かつ正確に特定できます。HP Client Automation は、差分計算、バンド幅の最適化、マルチキャスト、およびチェックポイントの再開機能で特許を取得しており、複数層インフラストラクチャにより、ネットワーク リソースに与える影響を最小限にした状態でセキュリティ パッチを配布し、あらゆる規模の企業でパッチを管理することが可能になります。

- **適用状況と保証**
  自動的かつ継続的に、セキュリティ パッチがポリシーで指定されているとおりの状態で適用されるようにする独自の要求ステート管理を行います。デバイスおよびユーザーをモニタし、ポリシーと比較して確認します。適合しない場合は、それらを適切なパッチ レベルに自動的に調整します。

図 1　パッチ管理のライフ サイクル



略語と変数

本ガイドでは、次の表に定義する略語と変数を使用します。

表 1　このガイドで使われている略語

略語	定義
HPCA	HP Client Automation
Core と 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

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	32 ビット OS の場合：`C:¥Program Files¥Hewlett-Packard¥HPCA` 64 ビット OS の場合：`C:¥Program Files(x86)¥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:`

用語

以下の用語は、このマニュアルで頻繁に使用されます。これらの用語を十分に理解してから、このマニュアルを読むことをお勧めします。

ブリテンまたはセキュリティ アドバイザリ

ブリテンは、あるベンダーの製品について、そのベンダーによって報告されるセキュリティの脆弱性です。この用語は、Red Hat および SuSE のセキュリティ アドバイザリとほぼ同じ意味で使用されます。

パッチ

パッチとは、ベンダーによって提供されるバイナリ ファイルあり、本来、脆弱性を修正するために配布され、適用される必要があるものです。影響を受ける製品、プラットフォーム、アーキテクチャ、および言語に応じて、ブリテンには複数のパッチが含まれる場合があります。

2 パッチ取得

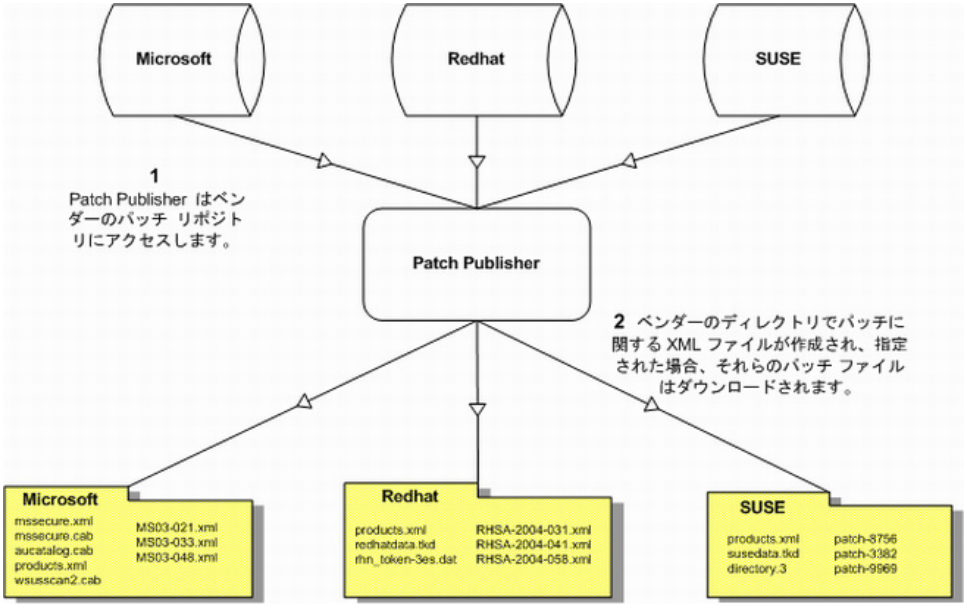
この章は以下を目的としています。

- パッチを取得できるようになる。
- パッチの取得とデータベースの同期で使用できるパラメータと、Patch Management の HPCA Console を使った操作を理解する。
- パッチ取得レポートへのアクセス方法と使用方法を習得する。
  - 取得の概要
  - 取得 (ブリテン別)
  - 取得 (パッチ別)

パッチ取得プロセス

Patch Management には、選択したベンダーの Web サイトに接続して、セキュリティ パッチに関する情報 (ファイルを含む) をダウンロードし、この情報を Configuration Server DB にパブリッシュするツールが用意されています。取得プロセスでは、ベンダーからのセキュリティ パッチをフェッチし、この情報を Configuration Server DB にパブリッシュします。

図 2　ベンダーのパッチ リポジトリとの接続



取得の概要

Patch Management は、セキュリティ パッチの取得と、Configuration Server の CSDB にあるパッチ情報と SQL または Oracle サーバーのパッチ データベースとの同期を行うために使用されます。既に取得を実行したことがある場合は、差分のあるインスタンスのみが更新されます。

取得時には、以下の処理が行われます。

- 取得の準備のためにベンダーの Web サイトに接続します。

- ブリテン、セキュリティ アドバイザリ、およびサービス パックと実際のパッチ ファイルに関する情報、またはパッチに関する情報のみのどちらかがダウンロードされます。ダウンロードされた情報には、影響を受けるファイル、リブート要件、プローブ情報など、各セキュリティ パッチに関する詳細データが含まれますが、それ以外の情報も含まれます。
- 取得される各ブリテン用の XML ファイルが作成され、Patch Management のディレクトリ内のベンダーのフォルダに配置されます。これらのファイルはパッチ説明ファイルと呼ばれます。
- Configuration Server Database の PATCHMGR ドメインは、この情報と一緒に取得されます。
- 取得した各ブリテンに対するサービスが PATCHMGR ドメインに作成されます。
- PATCHMGR ドメインは、作成済みの ODBC データベースと同期されます。

パッチ説明ファイル (XML) について

セキュリティ パッチが取得されると、パッチの情報を含む XML ファイル、つまりパッチ説明ファイルが作成され、ベンダーのディレクトリに配置されます。ベンダーのディレクトリは、デフォルトでは次の場所にあります。

<*InstallDir*>¥data¥PatchManager¥patch

たとえば、Microsoft ブリテンのパッチ説明ファイルは次の場所にあります。

<*InstallDir*>¥data¥PatchManager¥patch¥Microsoft

一方、Red Hat のパッチ説明ファイルは次のロケーションにあります。
<*InstallDir*>¥data¥PatchManager¥patch¥Redhat.

ブリテン番号は、.xml 拡張子を付けるとファイル名になります。ブリテンの番号が MS03-051 の場合、パッチ説明ファイルの名前は、MS03-051.xml となります。ブリテンに関連付けられた実際のファイルも取得する場合、ブリテンの名前でフォルダが作成され、そこにパッチ ファイルが格納されます。

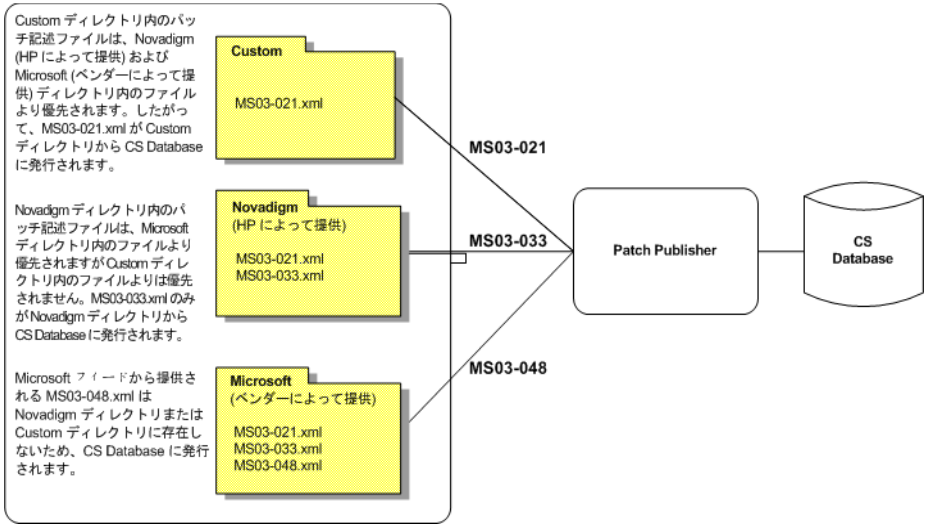
ベンダーから取得した情報の一部は、パッチの管理を開始する前に変更する必要があります。このため、¥data¥PatchManager¥patch サブフォルダには、他に novadigm および custom の 2 つのサブディレクトリがあります。HP では追加のパッチ説明ファイルを用意しており、それらは novadigm サブディレクトリにあります。novadigm サブディレクトリにあるパッチ説明ファイルは、

対応するベンダーのディレクトリにあるパッチ説明ファイルを上書きします。また、独自のパッチ説明ファイルを作成または変更して、それを custom サブディレクトリに配置することもできます。これらのカスタム ファイルは、novadigm、microsoft、redhat および suse ディレクトリにあるファイルを上書きします。これらの XML ファイルをテキスト エディタを使用して変更し、そのファイルにベンダーのディレクトリにあるものと*完全に*同じ名前を付けて、Custom サブディレクトリに配置します。次の図は、Microsoft ブリテンを使用して、この階層の例を説明したものです。

Windows オペレーティング システムのサービス パック、MSSP-WIN2k_4.xml および MSSP-WINXP_1.xml の 2 つの*サンプル*説明ファイルが用意されています。他の Microsoft オペレーティング システム サービス パックを配布する場合は、独自のパッチ説明ファイルを作成して、Custom サブディレクトリに保存する必要があります。配布を自動化する前に、テスト環境でサービス パックの配布を行ってください。

次の図は、パッチ説明ファイルが Microsoft セキュリティ ブリテンを上書きすることを説明しています。Microsoft、SuSE および RedHat など、すべてのベンダーに同じ階層があります。

図 3　パッチ説明ファイル



Microsoft パッチの取得と管理について

新しい Microsoft Update Catalog (wsusscn2.cab) の組み込みサポート

最近、Microsoft は、新しい Microsoft Update Catalog (`wsusscn2.cab`) を、現在サポートされているすべてのパッチの集中管理リポジトリとして発表しました。このマニュアルを作成している時点で、次の見解を示しています。Microsoft は、新しい Microsoft 製品のパッチが新しい Microsoft Update リポジトリ以外では入手できなくなることを言明しています。

現在、Patch Management は既存のレガシー カタログ以外に新しい Microsoft Update Catalog もサポートしています。

Microsoft Update Catalog テクノロジを使用して取得および配布されるパッチは、HP メタデータの修正が不要です。管理できる製品については、製品に関連付けられたパッチはテストされ、Configuration Server にパブリッシュされると、すぐに配布できます。Microsoft が Microsoft Update Catalog でサポートする製品を拡大するのに対応して、Patch Management は、これらの製品に対するパッチ管理サポートを有効にしていきます。

Microsoft Update Catalog の要件: 最低限必要な OS とサービス パックのレベル

Patch Management で使用する Microsoft Update Catalog および Windows Update テクノロジで必要なオペレーティング システムとサービス パックの最低要件については、Microsoft 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、サポートされる OS のバージョンおよび言語は、次の Microsoft Update ホームページのリンクで確認できます:
http://update.microsoft.com/microsoftupdate/v6/default.aspx

[ヘルプとサポートを参照する] をクリックしてよくある質問にアクセスします。

顧客は、Microsoft Update Catalog で必要な最低のサービス パック レベルになっていなくても、古いオペレーティング システムにパッチを適用することができますが、

Microsoft データ フィードに対する Patch Management のベンダー設定

現在使用できる Microsoft の更新リポジトリおよびメソッドをサポートするために、Patch Management にはベンダー設定のページに以下の [Microsoft データ フィード優先化] オプションがあります。

- **Microsoft Update Catalog のみ**

- **Microsoft Update Catalog、レガシー カタログ。**

Microsoft Office と Microsoft Update Catalog

Microsoft Update Catalog で配布される Office パッチは、Office アプリケーションが現在 HP Client Automation 管理アプリケーション (Application Manager や Application Self-service Manager など)、または管理制御ポイントで管理される場合は検出されません。いずれの場合も、Office アプリケーションに影響を与えるブリテンがデバイスに指定された場合は、Patch Management 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 Office を使用するデバイスにパッチを適用する詳細については、33 ページの「Microsoft Office セキュリティ ブリテンの検出と管理」を参照してください。

Windows インストーラ 3.1 の要件

Patch Management を実行する場合、ターゲット デバイスに Windows インストーラ バージョン 3.1 *以上*が必要です。この MSI 3.1 の要件を満たすには、次のいずれかを実行することをお勧めします。

- 最新の MSI 3.1 パッケージを Microsoft Web サイトからダウンロードして手動で配布する。このブリテンは、複数の言語で定義されています。このマニュアルを作成している時点で、米国英語バージョンは **http://support.microsoft.com/kb/893803/ja-jp** にあります。

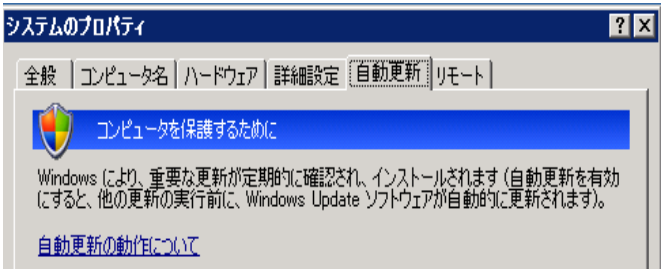
  または

- Patch Management を使用して、ブリテン MS-KB893803 を取得、配布、および管理する。取得リストの一部としてこのブリテンを指定し、Windows Agent マシンにブリテンのエンタイトルメントを設定します。

Microsoft 自動更新について

自動更新は Microsoft Windows の機能で、ユーザーは必要なパッチについて自分のシステムのスキャンを開始できます。Microsoft 自動更新では、パッチのダウンロードおよびインストールもできます。この Microsoft の機能は、次の図で示すように [**マイ コンピュータ**] > [**プロパティ**] > [**システムのプロパティ]** ダイアログ ボックスの **[自動更新]** タブからアクセスできます。

図 6　[システムのプロパティ] -- [自動更新] タブ



自動更新では、現在、[自動] 以外に次の設定オプションを使用できます。

1　更新を自動的にダウンロードするが、インストールは手動で実行する

2　更新を通知するのみで、自動的なダウンロードまたはインストールを実行しない

3　自動更新を無効にする

Microsoft 自動更新と Patch Management は、両方ともベースとなる Windows コンポーネント、Windows Update Agent (WUA) を使用してデバイスをスキャンし、更新をインストールします。

WUA が別のパッチ管理製品で使用中にならないように、**[自動更新を無効にする]** を選択することを強くお勧めします。この推奨事項は、Microsoft が Windows Update Agent にソフトウェアの更新を提供するときまでに、パッチ管理製品で不一致が発生しないようにするためのものです。

Patch Management で自動更新オプションを使用することの潜在的重要性については、以下で説明します。

- HP がお勧めするように **[自動更新を無効にする]** をオンにすると、自動更新はその製品をサポートするものの、Patch Management はそれをサポートしないため、使用可能なすべての更新が通知されない可能性があります。
- 自動更新を　**[更新を通知するのみで、自動的なダウンロードまたはインストールを実行しない]** に設定すると、Patch Management Agent で更新をスキャンおよびインストールしている間、ユーザーは自動更新のダウンロードプロセスを開始しません。自動更新プロセスが手動で開始されると、管理対象デバイスの*いずれか*のプロセスが更新のダウンロードおよびインストールに失敗します。この動作は Patch Management 特有のものではありません。他のパッチ管理製品が WUA を使用しようとしたときに WUA がすでに使用中の場合も、同じことが起こります。

詳細については、以下の Microsoft KB の記事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、Microsoft KB 記事 910748 の URL は次のとおりです: **http://support.microsoft.com/kb/910748**
- このマニュアルを作成している時点で、Microsoft KB 記事 931127 の URL は次のとおりです: **http://support.microsoft.com/kb/931127**

自社でウィルス スキャナをインストールし、それを有効にしている場合は、Microsoft KB の記事 922358 を参照してください。この文書には、ウィルス スキャンではフォルダ `%Windir%¥SoftwareDistribution` を除外する必要があると記載されています。この Microsoft 文書は、Microsoft パッチ管理テクノロジに特定して言及していますが、Patch Management も Windows Update Agent テクノロジを利用しているため、同じ制約が Patch Management を使用している企業でも関係する可能性があります。次の Microsoft KB 記事を確認してください。

- このマニュアルを作成している時点で、Microsoft KB 記事 922358 の URL は次のとおりです: **http://support.microsoft.com/kb/922358**

WUA は、**自動更新サービス**と呼ばれる Microsoft Windows のサービスを使用しています。この Windows のサービスは、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。

自動更新の設定に関する詳細については、以下の Microsoft の記事を参照してください。

- 「*Windows XP での自動更新の構成方法および使用方法*」このマニュアルを作成している時点で、URL は **http://support.microsoft.com/kb/306525** です。
- 「*Windows 2000 で自動更新を設定する方法と使用する方法*」このマニュアルを作成している時点で、URL は **http://support.microsoft.com/kb/327850/** です。

Red Hat パッチの取得について

Red Hat のセキュリティ パッチを取得するには

- Red Hat Web サイトで Red Hat Network アカウントを作成します。このマニュアルを作成している時点で、ロケーションは **http://www.jp.redhat.com/** です。

- パッチを取得および管理する各 Red Hat サーバーの OS フィルタ オプション (バージョン + リリース + ハードウェア アーキテクチャの組み合わせ) に対して 1 つのシステム エンタイトルメントを持つ Red Hat Network アカウントが必要です。これらは、Patch Management の設定で選択した [OS フィルタ] オプションに対応します。

  たとえば、x86 システムの Red Hat Enterprise Server (ES) バージョン 4 のみでパッチを取得するには、Red Hat Network システム エンタイトルメントを持った Red Hat Network アカウントが必要です。x86-64 システムの Red Hat ES バージョン 4 でパッチを取得するには、追加の Red Hat Network システム エンタイトルメントが必要です。

  x86 および x86-64 の両方のシステムの Red Hat バージョン 5 のサーバーで取得を実行する場合、追加で 2 つの Red Hat Network システム エンタイトルメントが必要です。

  x86 および x86-64 の両方のシステムの Red Hat バージョン 6 のサーバーで取得を実行する場合、追加で 2 つの Red Hat Network システム エンタイトルメントが必要です。

  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 Network からダウンロードするか、Red Hat Linux インストール メディアをコピーした場合はローカルに見つけることができます。Patch Management は、取得時にまず適切なディレクトリで `.rpm` パッケージを検索します。次に例を示します。

  — x86 の Red Hat Enterprise Linux 4ES では、Red Hat インストール メディアで提供されたベースライン オペレーティング システムの rpm ファイルを `data/patch/redhat/packages/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/patch/redhat/packages/4es-x86_64` に配置します。

  — `data/patch/redhat/packages/` サブディレクトリに名前を付ける場合は、『HP Client Automation Core and Satellite Enterprise Edition ユーザー ガイド』(「*設定*」の章の「Red Hat のフィード設定」の項) に掲載されている**OS フィルタのアーキテクチャ**の値の一覧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、インストール メディアの RedHat/RPMS ディレクトリの下にあります。

- Red Hat Network (RHN) systemid ファイルを作成するには rhn_register ツール を使用します。このファイルは、取得中に RHN 認証情報を渡すために使用されます。詳細については、以下の手順を参照してください。

Red Hat systemid ファイルを作成するには

1. セキュリティ パッチを自動取得する Red Hat OS を実行している Linux サーバーに対してルート ログインを実行します。
2. システムにルートとしてログインしたら、コマンド ラインでコマンド rhn_register を実行します。
3. rhn_register ツールによって既存または新規アカウントの使用を選択する画面が表示されたら、既存を選択し、Red Hat Web サイトで作成した Red Hat Network ユーザー名とパスワードを入力します。
4. IP アドレスまたはホスト名など、このコンピュータに固有のプロファイル名を入力し、rhn_register を実行したシステムにはパッチを適用しないで rhn_register ツールを終了します。systemid という名前のファイルが作成されます。
5. rhn_register ツールで作成されたファイル /etc/sysconfig/rhn/systemid をお使いの Patch Management Server の ¥PatchManager¥etc ディレクトリにコピーします。
6. ファイル名 systemid を、次の redhat-*.sid ファイル名の命名規則のいずれかに従って変更します。名前はハードウェア アーキテクチャによって異なります。
   - x86 システムでは、systemid を redhat-*version+release*.sid に変更します。ここで、*version+release* は、Red Hat のバージョン 4 の直後にリリース (as、es、または ws) 、または Red Hat バージョン 5 の場合、*version+release* は 5server または 5client のいずれかになる、3 つの組み合わせのうちの 1 つを表します。Red Hat バージョン 6 の場合は、*version+release* は 6server または 6client のいずれかです。

     たとえば、コンピュータが Red Hat Enterprise Server V 4 を実行している場合、systemid ファイルの名前は redhat-4es.sid に変更されます。

— x86_64 システムでは、systemid を redhat-*version+release*-x86_64.sid に変更します。これは、ファイル名の .sid 拡張子の前にアーキテクチャ タイプ **–x86_64** を追加する点以外は、上記と同じ命名規則です。

たとえば、x86_64 コンピュータが Red Hat Enterprise Server V 4 を実行している場合、systemid ファイルの名前は redhat-4es-x86_64.sid に変更されます。

ネットワークによりパッチの取得頻度が非常に高いと判断された場合、Red Hat Network へのアクセスが無効になる場合があります。エラーは、テキスト「Abuse of Service detected for server linux」とともに patch-acquire.log に表示されます。この問題を解決するには、登録されているシステムを Red Hat Network Web インターフェイス (**https://rhn.redhat.com**) から削除します。上の手順を使用して、Red Hat 認証情報ファイル (systemid) を再作成します。

これで、Red Hat Enterprise Server パッチの取得を実行できます。必ず、正しい Configuration Server および ODBC パラメータを設定してください。

カスタム パッチ説明ファイルの作成

acquire コマンドを使用して作成されるパッチ説明ファイルは、ベンダーのデータフィードの情報を使用します。これらのファイルには、パッチに関して情報が不足している場合や、誤った情報が含まれている場合があります。**プローブ**は、パッチが修正するセキュリティの問題に応じて、必要なものを定義します。サポートされる XML タグを使用して、カスタム パッチ説明ファイルを作成できます。カスタム説明ファイルは、custom ディレクトリに配置し、microsoft、redhat、suse、または novadigm ディレクトリで上書きするファイルと同じ名前にする必要があります。以下は、Microsoft ブリテン用のカスタム説明ファイルを作成する例です。

カスタム説明ファイルを作成するには

1 取得中に生成された *<InstallDir>*¥data¥PatchManager¥patch¥microsoft ディレクトリにある Microsoft バージョンの XML ファイルを、*<InstallDir>*¥data¥PatchManager¥patch¥custom ディレクトリにコピーします。

2 テキスト エディタまたは XML エディタを使用して、パッチ説明ファイルを表示します。XML の一番上にある URL で、項目別に分類されたリリースに関するデータを検証します。Source を Custom に変更します。

```
<Bulletin PopularitySeverityID="0" URL="http://www.microsoft
.com/technet/security/bulletin" FAQURL="http://www
.microsoft.com/technet/security/bulletin"
MitigationSeverityID
="0" Supported="Yes" ImpactSeverityID="0" SchemaVersion="1.0"
PreReqSeverityID="0" DateRevised="20021119"
Source="NOVADIGM" Name="MS02-065" Title="Buffer Overrun in
Microsoft Data Access Components Could Lead to Code Execution
(Q329414)" DatePosted="20021119" >
```

カスタム XML を作成する場合は、すべての製品リリースを含めることをお勧めします。これにより、製品の使用可能なすべてのリリースを実行する管理対象デバイスを探索できます。

3 データを調整するために必要な変更をすべて行い、カスタム パッチ説明ファイルを保存します。Source タグを Custom に変更します。この値は、BULLETIN インスタンスの SOURCE 属性に反映されます。

HPCA Console で Patch Management を使用してカスタム パッチ説明ファイルをパブリッシュします。Configuration Server にパブリッシュする前にブリテンをすべて置換する場合は、[置換] オプションを「はい」に設定してください。

4 次のように、patch-acquire.log を表示して、パブリッシュ プロセスで取得される XML の場所を確認できます。

```
20100722 10:13:09 Info:Syncing bulletin <InstallDir>/Data/
PatchManager/patch/custom/MS10-001.xml

20100722 10:13:09 Info:Publishing bulletin MS10-001, 1 of 1

20100722 10:13:09 Info:Loading XML file <InstallDir>/Data/
PatchManager/patch/custom/MS10-001.xml

20100722 10:13:10 Info:Loading BULLETIN.MS10-001 from RCS
```

mib (Manage Installed Bulletins) オプションの設定

Patch Management は、-mib (インストール済みのブリテンを管理する) オプションをサポートします。デフォルトでは、Patch Management がターゲット デバイスで探索を実行すると、ターゲット デバイスにインストールされているすべての適用可能なブリテンの管理を開始します。これは、接続の継続性を意味しており、Patch Management は以前にインストール済みのブリテンがまだインストールされていることを確認します。

–mib オプションは、Patch Management が、すでにターゲット マシンにインストール済みの適用可能なブリテンの処理をスキップし、マシンにまだインストールされていないブリテンのみを処理する場合に使用できます。指定した–mib オプションには、次の値を指定できます。

-mib none
Patch Management によってインストールされたブリテンのみを管理し、別の方法でインストールされたブリテンのサービス 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。

-mib hppm (または n)
HP Patch Management によってインストールされたブリテ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ンは管理しません。

-mib all (または y)
Patch Management 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。

Patch Management を、**-mib** オプションに **hppm** または **none** を指定して設定すると、処理の負荷は、Configuration Server および Patch Management Agent の両方で大幅に削減されます。

mib (Manage Installed Bulletins) オプションを設定するには

HPCA Consoleの [エージェント オプション] ページを使用し、-mib (インストール済みのブリテンを管理する) オプションを設定します。[エージェント オプション] ページには、[設定] タブの [パッチ管理] グループからアクセスできます。

パッチ取得レポート

取得ベースのレポートは、ベンダーの Web サイトからのパッチの取得が成功したか失敗したかを示します。

レポートを表示するには、**[レポート ビュー]** の下で **[パッチ管理レポート]** をクリックし、レポートの一覧を展開します。使用可能なレポートの一覧を展開するには、**[取得レポート]** をクリックします。、レポートの使用およびフィルタリングの詳細については、『HP Client Automation Reporting Server リファレンス ガイド』を参照してください。

取得の概要

取得の概要レポートは、各取得セッションのブリテン、パッチ、およびエラーの数を示します。また、レポートには、すべてのブリテンおよびパッチの取得レポートに対するリンクがあります。パブリッシュ セッションの日時も一覧表示されます。

- **[追加されたブリテン数]** または **[更新されたブリテン数]** をクリックして、ブリテン別にソートされた取得の概要を参照します。
- **[追加されたパッチ数]** または **[更新されたパッチ数]** をクリックして、パッチ ファイル別にソートされた取得の概要を参照します。
- **[ブリティンの依存関係数]** をクリックして、「ブリティンの依存関係」レポートの下に表示される依存ブリテンによってソートされた取得の概要を参照します。ブリティンの依存関係は Redhat ベンダーのみに取得されてパブリッシュされるため、ブリティンの依存関係数はこのベンダーにのみ表示されます。その他のベンダーのブリティンの依存関係数はゼロになります。
- **[エラー数]** をクリックして、取得が失敗した理由の詳しい説明を参照します。エラー レポートに表示される数字のエラー コードは、標準の HTTP ステータス コードです。これらのコードの詳細については、インターネットで「HTTP ステータス コード」を検索してください。

このレポートはベンダー名でフィルタ *できません*。

取得 (ブリテン別)

取得 (ブリテン別) レポートを使用して、ブリテンの取得の概要を参照します。

このレポートの適用可能なパッチの番号をクリックして、ブリテンに関連付けられたファイルを参照します。1 つのブリテンには、プラットフォームに応じて複数のパッチが関連付けられている場合があります。

- ブリテンに Patch Management がサポートしない製品に適用されるパッチがある場合、ブリテン名の前にアスタリスク (*) が表示されます。
- [重大度] 列のアイコンは、Windows ブリテンの重大度を示します。重要度の範囲は、[最重要] から、[重要]、[中]、[低] までです。ブリテンが Windows プラットフォーム用でない場合、[不明] アイコンが表示されます。重大度が同じブリテンをすべて表示するには、[重大度] 列のアイコンをクリックします。既存ブリテンに重大度評価はありません。既存のブリテンおよびパッチの重大度評価を表示するには、[強制] および [置換] オプションを使用して再取得する必要があります。

  > WSUS でサポートされていないパッチがブリテンに含まれており、それらのパッチの重大度が同じブリテンに含まれている他のパッチよりも高い場合、このレポートに表示される重大度評価が [Microsoft セキュリティ ブリテン サマリー] ページと一致しない場合があります。この問題は、ブリテンに含まれているパッチの重大度によってブリテンの重大度評価が決定されるために発生します。WSUS でサポートされないレガシー パッチがブリテンに含まれている場合、それらのパッチを除外して重要度の評価が決定されます。

- このレポートの一番下には、Patch Management によってサポートされない製品に適用されるブリテンを含む第 2 セクションがあります。これらのブリテンは、リサーチ レポートには表示されません。

取得 (パッチ別)

取得 (パッチ別) レポートを使用して、各パッチの取得の概要を参照します。

- 特定のブリテンの [製品/リリース] 列の項目をクリックして、パッチの完全な詳細に掘り下げます。

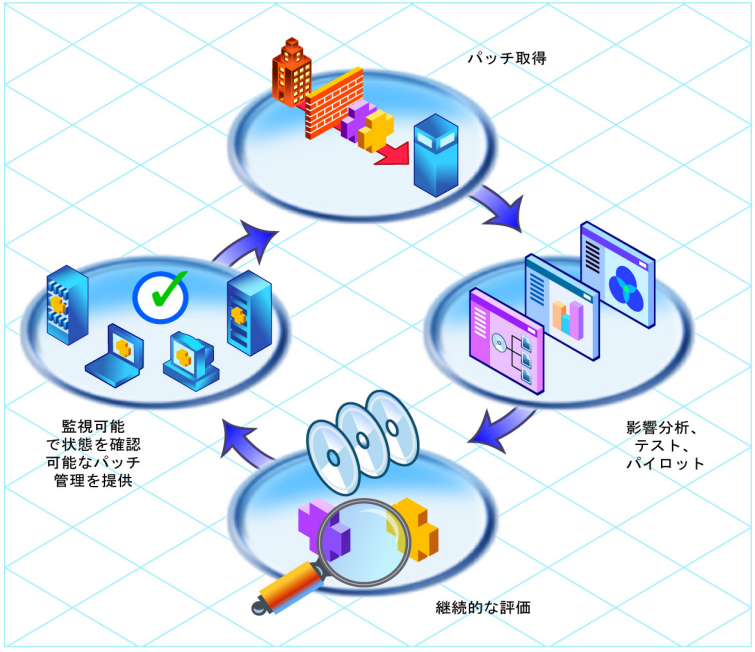
[重大度] 列のアイコンは、Windows パッチの重大度を示します。重要度の範囲は、[最重要] から、[重要]、[中]、[低] までです。パッチが Windows プラットフォーム用でない場合は、[不明] アイコンが表示されます。重大度が同じパッチをすべて表示するには、[重大度] 列のアイコンをクリックします。既存パッチに重大度評価はありません。既存のブリテンおよびパッチの重大度評価を表示するには、[強制] および [置換] オプションを使用して再取得する必要があります。

3　パッチの評価、分析、レポート

この章は以下を目的としています。

- ターゲット デバイスでのパッチの管理方法を理解する。
- パッチの分析とレポートについて理解する。Reporting Server で生成されるパッチ ファイルに関するレポートには、概要、適合性レポート、取得レポート、リサーチ レポートがあります。

図 4　製品探索と分析



製品探索と分析

脆弱性を管理する前に、Patch Management Agent がデバイス上の製品を探索する必要があります。Patch Management オブジェクトは、管理対象デバイスにローカルにキャッシュされ、バンド幅を最適化します。オブジェクトは、ローカルのものと異なる場合だけダウンロードされます。また、Patch Management Agent は、探索された各製品にインストールされているパッチを検出する必要があります。これを行うには、DISCOVER_PATCH および FINALIZE_PATCH の Patch Management サービスを、管理対象デバイスに割り当てます。

Patch Management Agent の接続を実行するには、**dname** パラメータを **PATCH** に設定する必要があります。これにより、Patch Management Agent 用のサービスの解決が、Application Manager Agent 用のサービスの解決と区別されます。

パッチ検索を実行するには

1 管理対象デバイス (例、POLICY.USER.&(ZUSERID)) を PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH サービスに直接接続します。

このサービスは、Patch Management Agent の最初のサービスとして優先的に実行されます。このサービスは、Patch Management Agent 接続の間に、Patch Management Agent にメソッドを配布し、製品探索と脆弱性の評価を実行します。

2 管理対象デバイス (例、POLICY.USER.&(ZUSERID)) を PRIMARY.PATCHMGR.ZSERVICE.FINALIZE_PATCH に直接接続します。

Patch Management Agent 接続の間に、適用可能なパッチがダウンロードされ、キューに追加されて、FINALIZE_PATCH と呼ばれる Patch Management サービスにより管理されます。このサービスは、Patch Management Agent の最後のサービスとして優先的に実行されます。このサービスでは、リアルタイムでパッチ適合情報のレポートを作成する必要があります。

パッチ以外に、すべての管理対象デバイスのポリシーに FINALIZE_PATCH サービスを追加します。

このサービスが使用できないと、拡張パッチ管理アクティビティになり、リアルタイムでパッチ適合性情報レポートが作成できません。

3 radskman コマンド ラインを作成して、通常のエージェント接続を行います。コマンド ラインは少なくとも次のようになります。

radskman ip=<*ConfigurationServerIPaddress*>,port=<*ConfigurationServerport*>,dname=patch,catexp=runmode:automatic

radskman コマンド ライン作成の詳細については、『HP Client Automation 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。

Microsoft Office セキュリティ ブリテンの検出と管理

Patch Management は、Microsoft Office の更新の取得と配布を管理できます。ただし、Microsoft Office アプリケーションは Windows インストーラ テクノロジを利用するため、基本的にパッチ適用機能と自己修復機能が提供されています。このため、Patch Management を有効にして Microsoft Office のパッチを配布する前に、お使いの環境で Microsoft Office のインストールや更新を現在どのように行っているかを検討することが重要です。

現在、外部の **ACP (管理インストール ポイント**または **AIP** とも呼ばれます) または Client Automation 管理アプリケーション (Application Manager または Application Self-service Manager) を使用して Microsoft Office を配布している場合、Microsoft Office アプリケーションの更新については、それらのソリューションを継続することをお勧めします。

Patch Management を使用した Microsoft Office アプリケーションの更新を開始する場合は、ACP または Client Automation 管理アプリケーションを使用した Microsoft Office アプリケーションへの更新の配布を中止する必要がありま

す。Microsoft Office アプリケーションを配布するために ACP または Client Automation 管理アプリケーションの使用を継続することもできますが、更新は Patch Management で単独に管理する必要があります。

Patch Management を使用して Microsoft Office アプリケーションの更新を配布すると、それ以降、ACP 管理および Client Automation 管理の Microsoft Office アプリケーションは、それらの各テクノロジを使用した更新の受信ができなくなります。すなわち、ACP で管理されたアプリケーションは、登録済みのクライアント側の同期メカニズムに依存しており、このメカニズムによって ACP からデバイスに更新を配布します。また、Client Automation で管理されたアプリケーションは、要求ステート テクノロジを使用して、更新を Microsoft Office アプリケーションに配布します。したがって、Microsoft Office アプリケーションを更新する目的で Patch Management を有効にする前に、今後は Microsoft Office の更新を配布するために ACP または Client Automation アプリケーションを使用しないことを確認してください。

このトピックでは、Patch Management を使用した Microsoft Office の更新管理に関する選択肢、最善実践、および実装の詳細を説明します。このトピックには以下の内容が含まれます。

- 34 ページの「Microsoft Office セキュリティ ブリテン管理の最善実践」
- 38 ページの「Microsoft Update Catalog を有効にした最善実践」
- 40 ページの「Patch Management (バージョン 3.0.2 以上) での Microsoft Office 更新の有効化」

Microsoft Office セキュリティ ブリテン管理の最善実践

以下の情報は、移行および新規インストールの両方に適用されます。これは、Microsoft Office にパッチを適用するソリューションとして、Patch Management をいつ、どのように有効にするかを明確にします。

Windows インストーラ 3.1 の要件

Patch Management を実行する場合、すべてのターゲット デバイスに Microsoft Windows インストーラ バージョン 3.1 以上が必要です。Microsoft Office アプリケーションの更新を検出するために、Windows インストーラ 3.1 が必要です。

Microsoft Office 製品の更新オプション

Microsoft Office 製品を配布するために最初に使用されるメソッドは、エージェント ソフトウェアにパッチを適用するために使用できるオプションを決定します。Microsoft Office 製品は、Windows インストーラ テクノロジを使用します。これは、一般に CD-ROM または AIP にある圧縮されたメディアからのインストールをサポートします。Microsoft の最善実践の詳細については、Microsoft の記事、「*Distributing Office 2003 Product Updates*」を参照してください。

Microsoft Office を HP Client Automation アプリケーションを使用しないで Agent に配布する場合、Microsoft による以下の推奨事項が適用されます。

- 最初に CD-ROM またはネットワーク ファイル サーバーの圧縮メディアを使用して Microsoft Office 製品をインストールした場合、Microsoft は、バイナリ パッチをエージェント デバイスに配布することで、これらのエージェントを更新し、Windows インストーラがアプリケーションにローカル パッチを適用できるようにすることを推奨しています。
- Microsoft Office 製品が AIP からインストールされた場合、Microsoft は、管理者が適切な管理更新を取得し、中央にある AIP の更新を継続することを推奨しています。これにより、エージェントが確実に同期されます。

Microsoft Office を HP Client Automation (HPCA) アプリケーションを使用して Agent に配布する場合、HP による以下の推奨事項が適用されます。

- Microsoft Office 製品が Application Manager または Application Self-service Manager を使用して配布された場合、アプリケーションが基本管理ガイドラインまたは詳細管理ガイドラインのどちらに準拠してパブリッシュされたかを確認します。基本アプローチが使用された場合、メディアは圧縮 (CD-ROM) 形式で、Patch Management ソリューションに移行するときに、潜在的なソフトウェア競合はありません。HP は、このモデルに Patch Management を導入することを推奨しています。
- Microsoft Office 製品が、詳細管理ガイドラインを使用する Application Manager または Application Self-service Manager によって配布された場合、メディアは AIP 形式です。HP は、このモデルに Patch Management

を導入することを推奨しません。管理者は、引き続き Admin Publisher を使用して AIP 更新プロセスを簡素化し、Application Self-service Manager を使用して更新を配布する必要があります。

この推奨事項を無視し、詳細管理ガイドライン (AIP 形式のメディア) を使用して配布した Office 製品で Patch Management を有効にする場合は、事前に、このトピックの ⚠ 注意や ■ 警告の項目をすべて読み、潜在的なソフトウェア競合について理解してください。

Patch Management を使用して Microsoft Office の更新を配布する場合

Application Manager、Application Self-service Manager、または外部 AIP など、Patch Management 以外のソリューションを使用しない場合に限り、Patch Management を使用して Microsoft Office アプリケーションのパッチのパブリッシュと配布を行います。パッチをパブリッシュおよび配布するソリューションは 1 つだけ選択する必要があります。

Microsoft Office 製品が以下のいずれかからインストールされたことが確認されている場合に限り、Patch Management を使用して Microsoft Office 製品の更新を配布します。

- 圧縮メディア (CD-ROM)。
- AIP。ただし、今後、Microsoft Office 製品の更新に AIP 同期プロセスを使用しない場合。
- Application Manager または Application Self-service Manager。ただし、今後、Application Manager または Application Self-service Manager を使用して、Microsoft Office パッチのパブリッシュや配布を行わない場合。

⚠ 現在 AIP 同期プロセスでパッチを適用している Microsoft Office 製品を実行しているエージェント デバイスを管理する管理者は、これらのパッチ適用方法 (AIP 同期プロセスと Patch Management) を交換しないように気をつける必要があります。交換すると、エージェント デバイスと AIP の間の同期を破壊する原因になります。

同期プロセスの詳細については、Microsoft の記事、「*Updating Office XP Clients from a Patched Administrative Image*」を参照してください。

Patch Management の使用時に無効にされる Client Automation 管理機能

メソッド フィールド ZCREATE、ZVERIFY および ZUPDATE から派生する Application Manager および Application Self-service Manager の管理機能は、Microsoft Office アプリケーションを 1 度 Patch Management で管理すると、それ以降、Microsoft Office アプリケーションでは使用できなくなります。この管理機能には、初回使用時のインストール機能、および MSI 機能やプロパティの管理機能が含まれます。

これらの機能を継続して使用する場合は、このモデルに Patch Management を導入しないでください。代わりに、Admin Publisher を使用して Microsoft Office パッチをパブリッシュし、Application Manager または Application Self-service Manager を使用して Microsoft Office パッチの配布と管理を行います。

Microsoft Office は、Patch Management によるパッチの適用を有効にした後でも、依然として Application Manager または Application Self-service Manager を使用してアンインストールできます。これは、ZDELETE メソッドが決して無効にされないためです。

Microsoft Update Catalog による Office XP、Office 2003、および Office 2007 のサポート

新しい Microsoft Update Catalog データ フィードを使用する場合、Patch Management は、スタンドアロン製品と同様に、Microsoft Office XP、Microsoft Office 2003、および Microsoft Office 2007 へのパッチ適用をサポートします。たとえば、Microsoft Update Catalog と一緒に Patch Management を使用してパッチを適用できる Microsoft Office 2007 のスタンドアロン製品は以下のとおりです。

- Access 2007
- Excel 2007
- Groove 2007
- InfoPath 2007
- OneNote 2007
- Outlook 2007
- PowerPoint 2007
- Project 2007
- Publisher 2007
- SharePoint Designer 2007
- Visio 2007
- Word 2007

新しい Microsoft Update Catalog データ フィードを使用する場合、Patch Management は Microsoft Office 2000 以前のアプリケーションに対するパッチ

適用をサポートしません。この制約は、Patch Management Agent が Microsoft の脆弱性を検出するのに Microsoft Update Catalog に依存している結果です。19 ページの「Microsoft パッチの取得と管理について」を参照してください。

Microsoft Office のサービス パック

HPCA Patch Management は、Microsoft Office サービス パックの配布と取得をサポートします。Microsoft では、特定の Microsoft Office パッチが特定のサービス パックを前提とする場合があります。この場合、そのパッチのインストールより先に、指定の Microsoft Office サービス パックを配布する必要があります。

Microsoft データ フィード優先化の選択により、Patch Management が前提のサービス パックをデバイスにレポートおよび適用できるかどうかが決まります。

- **Microsoft Update Catalog のみの場合**: このデータ フィードの変更のため、サービス パックの依存関係は Patch Management で取得およびレポートされません。管理者は、適用可能なブリテンの前提サービス パックをリサーチし、それらをデバイスがアクセスできるようにする必要があります。
- **Microsoft Update Catalog、Legacy の場合**: Windows 2000 のみを実行しているデバイスの場合、Patch Management はデフォルトのデータ フィードの動作に従い、ポリシーでアクセス権のあるデバイスに、依存サービス パックをレポートおよび配布します。Windows 2000 以外のプラットフォームで稼動しているデバイスの場合、Patch Management は Microsoft Update Catalog の動作に従います。したがって、管理者は前提サービス パックをリサーチして、デバイスにそれらへのアクセス権を与える必要があります。

Microsoft Update Catalog を有効にした最善実践

Patch Management および Microsoft Update Catalog について

Patch Management バージョン 3.0.2 で導入された拡張機能により、Microsoft Update Catalog データ フィードや Windows Update Agent などの新しいテクノロジを使用できます。Microsoft Update Catalog の詳細については、Microsoft FAQ 記事 (*http://update.microsoft.com/microsoftupdate/v6/about.aspx?ln=ja-jp*) を参照してください。

Patch Management は、脆弱性のスキャン、更新のインストール、および更新の検証に Windows Update Agent を使用することで、Microsoft Update Catalog を活用します。Windows Update Agent は、Windows オペレーティング システムだけでなく、Microsoft Office などのアプリケーションの更新もインストールします。したがって、Patch Management は、Microsoft Office アプリケーションが Application Manager、Application Self-service Manager、または管理制御ポイント (ACP) で管理されているかどうかを判断する必要がありません。

Microsoft Update Catalog を使用する Windows インストーラ対応アプリケーション (Microsoft Office など) のパッチを検出するには、Windows インストーラ バージョン 3.1 が必要です。

Patch Management バージョン 3.0.2 以上を使用する場合、Microsoft Office アプリケーションの更新が自動的に検出され、レポートされますが、更新はデバイスがパッチにアクセスできる場合のみインストールされます。

- Microsoft Office のパッチを、有効な Microsoft Update Catalog と Patch Management を使用して配布する場合、それ以降は、Application Manager や Application Self-service Manager、または外部 ACP を使用して、Microsoft Office のパッチのパブリッシュや配布を行わないでください。パッチ管理について、Patch Management によるソリューションと既存のソリューションのどちらかを選択する必要があります。
- ZCREATE、ZVERIFY、または ZUPDATE メソッドから派生した機能 (MSI 機能やプロパティが管理できることや、初回使用時にインストールできるなど) を利用するために Application Manager または Application Self-service Manager を選択する場合、Publisher を介して Microsoft Office パッチをパブリッシュし、Application Manager または Application Self-service Manager を使用してそれらを配布および管理することをお勧めします。このモデルには Patch Management を導入しないでください。
- 外部 ACP を継続して使用する場合は、このモデルに Patch Management を導入しないでください。CM Patch Management を導入すると、エージェントと ACP の間の同期を破壊することになります。
- Microsoft Update Catalog データ フィードを使用する Patch Management を有効にする場合、次のトピック「Patch Management (バージョン 3.0.2 以上) での Microsoft Office 更新の有効化」のタスクを実行します。

Patch Management (バージョン 3.0.2 以上) での Microsoft Office 更新の有効化

Patch Management は、インストール時のデフォルトでは Microsoft Office (`!Office*`) パッチが取得から除外される設定になっています。バージョン 5.0 では、Microsoft Office とその一連のスタンド アロン製品はデフォルトで取得から除外される設定です。

以下の手順で、Microsoft Office の取得と Microsoft Update Catalog フィードを使用する Patch Management 環境のエージェントへの配布を有効にします。

1 すべてのデバイスに Windows インストーラ 3.1 をインストールします。

2 Microsoft Update Catalog データ フィードと Patch Management を使用して Microsoft Office のパッチを配布する場合、Patch Management メソッドを変更する必要はありません (バージョン 3.0.2 以前では変更が必要でした)。Microsoft パッチのデータ フィードが変更され、–IR および –IACP パラメータを含むコードは実行されないためです。

以前に説明したとおり、Microsoft Office の更新を、Application Manager、Application Self-service Manager、または AIP のいずれかの既存のソリューションで管理しない場合は、Patch Management での Microsoft Update Catalog フィードの使用を有効にしないでください。Patch Management が Microsoft Update Catalog を使用してパッチを適用すると同時に、Client Automation で管理されているアプリケーションは検証を実行できなくなり、AIP 同期エージェントは AIP に接続できなくなります。

3 以前に Application Manager または Application Self-service Manager を使用して Microsoft Office 更新を管理していた場合、お使いのデータベース内にある Microsoft Office 用の既存の SOFTWARE.ZSERVICE クラス インスタンスの ZCREATE、ZVERIFY および ZUPDATE メソッドの既存の値をブランクにしてください。これにより、`radiamsi` 呼び出しは発生しなくなり、Application Manager または Application Self-service Manager による要求ステートの処理で、Patch Management が配布した更新は元に戻らなくなります。これらのメソッドの編集については、HP ソフトウェア サポート Web サイトでエンジニアリング ノート「*Radia Client Methods and Pre-method Variables*」(ドキュメント ID: KM99949) を参照してください。

ZDELETE メソッドは空白にしないでください。ZDELETE により Application Manager または Application Self-service Manager を使用して Office をアンインストールできます。

4 パッチを取得するマシンで、製品除外フィルタの **!Office*** を削除します。

5 Patch Management v 5.0 以上を新たにインストールして実行している場合、デフォルトのフィルタは Microsoft Office および個別の Office 製品のパッチの取得を除外します。パッチを取得するマシンで、以下の Microsoft Office スタンドアロン製品も必要に応じて製品除外フィルタから削除します。

```
,!Access*,!Excel*,!FrontPage 200[023],!FrontPage 9[78],
!InfoPath*,!Office*,!OneNote*,!Outlook*,!PowerPoint*,
!Project 200[023],!Project 98,!Publisher*,!Visio*,
!Word*,!Works*
```

必要なエントリを除外リストから削除した後、残りのエントリがカンマで区切られていることを確認します。

6 ポリシー内で、Microsoft Office ブリテンをデバイスで使用できるようにします。

デバイス適合性レポートで使用するパッチ オブジェクトについて

以下のエージェント オブジェクトは、管理対象デバイスにインストールされている製品およびパッチを識別するために作成されます。

- DESTATUS - デバイス ステータス オブジェクト: 各適合性ステータスのブリテンの数や最後のスキャン時刻などデバイス ステータス全般を確認する 1 つのヒープを含みます。適合性ステータスの値は、「OK」、「警告」、「再起動の保留」、「エラー」、および「適用できません」です。
- RESTATUS - リリース ステータス オブジェクト: 1 つのデバイスに存在するすべてのリリースに 1 つのヒープが含まれます。
- BUSTATUS - ブリテン ステータス オブジェクト: すべてのブリテンに 1 つのヒープが含まれ、ブリテン ステータスを指定します。
- PASTATUS - パッチ ステータス オブジェクト: すべてのパッチに 1 つのヒープが含まれ、パッチ ステータスを指定します。
- DEERROR - デバイス エラー オブジェクト: デバイスの探索または管理で発生するすべてのエラーが含まれます。

これらの 5 つのオブジェクトは、Patch ODBC データベースの NVD_DESTATUS、NVD_RESTATUS、NVD_BUSTATUS、NVD_PASTATUS および NVD_DEERROR の 5 つのテーブルに対応します。

Client Automation Agent 接続プロセスの間、これらのオブジェクトは Configuration Server に送信されます。その内容は Configuration Server Database に格納されませんが、Messaging Server でモニタされているディレクトリにコピーされます。このディレクトリのデフォルト ロケーションは、以下のようにプラットフォームよって異なります。

- `<InstallDir>¥ConfigurationServer¥data¥patch` (Windows).
- `/opt/HP/CM/ConfigurationServer/data/patch` (UNIX)。

Messaging Server の Patch Delivery Agent は、格納およびレポート作成のために、この情報を Patch ODBC データベースにポストします。各デバイスの最新のオブジェクトだけが維持されます。

バージョン 5.0 以前の Patch Agent では、これらの情報を ZOBJSTAT という 1 つのオブジェクトでレポートしていました。上で説明したように、Messaging Server バージョン 5.10 以上の Patch Data Delivery Agent は、着信 ZOBJSTAT オブジェクトを最新の Patch Management ODBC データベースのテーブルに自動的にポストします。

パッチの分析とレポート

HPCA Reporting Server では、Patch Management の Web ベースのレポートが提供されます。

HPCA Console の **[レポート]** タブをクリックします。[レポート ビュー] の下で、**[パッチ管理レポート]** をクリックし、レポートの一覧を展開します。

Patch Management レポートには 4 つのタイプがあります。

- 45 ページの「概要」：エグゼクティブ レポートには、パッチ適用状況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。この円グラフと棒グラフのレポートを使用して、準拠デバイスまたは非準拠デバイスに関する詳細レポート、またはデバイスが準拠しているまたは準拠していないブリテンに関する詳細レポートに掘り下げます。

- 48 ページの「パッチ適合性レポート」: 管理 Agent は、HPCA に製品およびパッチの情報を送信します。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。適合性レポートは、お使いの環境で検出されたデバイスに該当する情報だけを示します。
- 55 ページの「取得レポート」: 取得ベースのレポートは、ベンダーの Web サイトからのパッチの取得が成功したか失敗したかを示します。
- 55 ページの「リサーチ レポート」: リサーチ ベースのレポートは、ソフトウェア ベンダーの Web サイトで取得したパッチに関する情報を示します。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。

各レポート タイプを展開すると、利用可能なレポートの一覧が表示されます。パッチ管理レポートの一覧の表示

Reporting Server によるパッチ レポートのフィルタリング

Reporting Server には、フィルタリング機能もあります。フィルタにアクセスするには、Reporting Server ページの検索制御セクションでパッチ管理の関連情報を展開します。

一部のフィルタではテキスト エントリしか使用できません。その他のフィルタには、使用できるオプションを表示するボタンやフィルタ検索ウィンドウを表示する虫眼鏡があります。

虫眼鏡  をクリックして、フィルタ検索ウィンドウを表示します。

使用できる任意の条件チェック ボックスをクリックして、フィルタで使用する条件を選択します。

[選択] をクリックして、フィルタを適用し、フィルタ選択ウィンドウを閉じます。

フィルタの作成に関する詳細については、『HP Client Automation Reporting Server リファレンス ガイド』を参照してください。

詳細な情報への掘り下げ

多くのレポートでは、特定のデバイスまたはブリテンに関する情報を、極めて詳細なレベルまで掘り下げられます。

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。

利用可能なレポートのアクションに追加されたデータ エクスポート オプション

レポートが表示されているときに、[レポート] ページでは次のアクションを実行できます。また、レポート データをカンマ区切り値 (CSV) ファイルまたは Web クエリ (IQY) ファイルにエクスポートできます。

表 3　レポートのアクション

アイコン	説明
	レポート ビュー内を 1 ページ戻る。
	レポートのホーム ページに戻る。
	Reporting Server からデータをリフレッシュする。リフレッシュは、フィルタを適用または削除するときにも実行されます。
	このレポートをお気に入りのリストに追加する。
	このレポートへのリンクを電子メールで送る。
	「クイック ヘルプ」ボックスまたはツール チップが開きます。これは、フィルタにのみ適用されます。
	このレポートを印刷する。
	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。

表 3　レポートのアクション

アイコン	説明
	レポートのコンテンツをカンマ区切り値 (CSV) ファイルにエクスポートする。このファイルのデータは、実際にはカンマではなくタブで区切られます。ただし、ファイル拡張子は CSV です。
	レポートのコンテンツを Web クエリ (IQY) ファイルにエクスポートする。

レポートに青色テキストで表示されるアイテムには、さまざまな機能があります。

- 詳細を表示 – このアイテムに関してより詳細な情報まで掘り下げる
- このレポート ビューを起動 – このアイテムに基づいて新しいレポートを開く
- 検索条件に追加 – このアイテムに基づいて、現在のレポートに追加フィルタを適用する
- ベンダーのサイトに移動 – このブリテン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。

HPCA のレポートは、グリニッジ標準時 (GMT) タイムゾーンで表示されます。

概要

パッチ管理用の概要は 4 つあり、環境のパッチ適用状況ステータスに関する円グラフまたは棒グラフが示されます。

概要レポートはパッチ ステータス別に色分けされています。したがって、特定のパッチ ステータスに関する特定のレポートに概要レポートから簡単に掘り下げられます。

表 4　概要レポートのパッチ ステータス

色	パッチのステータス
緑	準拠 = パッチ適用済みまたは警告
赤	非準拠 = パッチ未適用、その他、または再起動の保留
緑	パッチ適用済み
深緑	警告
赤	パッチ未適用
黄色	その他
グレー	再起動の保留
濃いグレイ	適用できません

概要レポートのサンプルは次のとおりです。

- 46 ページの「デバイス全体のステータス」
- 47 ページの「デバイスのステータス」
- 47 ページの「ブリテンのステータス」
- 48 ページの「ベンダーのステータス」

デバイス全体のステータス

ネットワーク内のパッチ準拠の管理デバイスとパッチ非準拠の管理デバイスの全体パーセンテージを示す円グラフが表示されます。パッチ準拠のデバイスとは、適用可能なすべてのパッチが適用されているデバイスか、警告ステータスを返したデバイスです。

適用可能なフィルタ: なし。

デバイスのステータス

パッチ適用済みステータスに従って、デバイスの円グラフと棒グラフ詳細が示されます。使用できるグラフィカル レポートは以下の 2 つです。

- **デバイス ステータス**: このグラフィカル レポートは上部パネルに表示されます。グラフでは、デバイスのパーセンテージが、「パッチ適用済み」、返された「警告」、「再起動の保留」、「その他のエラー」、または「パッチ未適用」のステータスで示されます。
  - 個々のステータス ラベルまたはセクションをクリックすると、その状態のデバイス数が表示されます。
  - 個々のステータス ラベルまたはセクションをダブルクリックすると、その状態のデバイス一覧を示すレポートが表示されます。デバイス一覧のデバイス名をクリックすると、その特定のデバイスのパッチ ステータスが検索されます。
- **デバイス パッチ適用状況ステータス**: このグラフィカル レポートは下部パネルに表示されます。グラフでは、パッチ適用状況レベルを示すデバイスのパッチ パーセンテージが示されます。パッチ適用状況レベルは、ほぼ 20% のパーセンテージ バンドで表示されます。ただし、最終バンドは例外で、99 ～ 100% の適用状況レベルのパーセンテージ バンドで表示されます。たとえば、デバイスに 10 のブリテンが必要で、5 パッチのみが適用されている場合、デバイスは 50% パッチが適用済みとなるため、円グラフと棒グラフの 41 ～ 60% パッチ適用済みバンドに含まれます。
  - 円グラフのバンドをクリックすると、このバンドに含まれるデバイス一覧が表示されます。
  - デバイス一覧のデバイス名をクリックすると、その特定のデバイスのパッチ適用状況情報が表示されます。

適用可能なフィルタ: デバイス名 (特定のデバイスのパッチ ステータスと適用状況ステータスを検索する)。

ブリテンのステータス

パッチ ステータスに従って管理されるすべてのブリテンの円グラフ詳細が示されます。

- 個々のセクションまたはステータス ラベルをクリックすると、その状態のブリテン数が表示されます。
- 個々のセクションをダブルクリックすると、特定のステータスを持つブリテンの一覧が表示されます。

適用可能なフィルタ: デバイス名 (このデバイスの各種ブリテンのパッチ ステータスを検索する)。

ベンダーのステータス

ブリテン パッチ適用済みステータスに従って、各ベンダーのブリテンの棒グラフが示されます。異なるステータスのブリテンが異なる色の棒で表示されます。

適用可能なフィルタ: なし。

パッチ適合性レポート

企業のデバイスが Patch Management Agent を実行している場合、製品およびパッチの情報は Patch Management に送信されます。その後、この情報は使用可能なパッチと比較され、このデバイスに脆弱性を除去するパッチが必要かどうかが確認されます。パッチ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。

パッチ適合性レポートは次のとおりです。

- 49 ページの「デバイスのステータス」
- 50 ページの「フル パッチが適用されていないデバイス」
- 51 ページの「ブリテンのインストール エラーがあるデバイス」
- 51 ページの「ブリテンのステータス」
- 53 ページの「製品ステータス」
- 53 ページの「リリースのステータス」
- 54 ページの「パッチのステータス」
- 54 ページの「重大なエラーが発生したデバイス」

このガイドに記載されているパッチ適合性レポートを使用するには、Patch Management 環境のサーバーと Agent がバージョン 7.50 以上である必要があります。

バージョン 7.50 よりも前の Patch Agent では、特に、このガイドに記載されている製品ステータス レポート、リリース ステータス レポート、パッチ ステータス レポートを生成できません。

デバイスのステータス

Client Automation のパッチ管理下にあるすべてのデバイスのパッチ適用状況ステータスを表示するには、デバイス ステータス レポートを使用します。前回のスキャンの日付が [デバイス名] の横に表示されます。

注意: レポートのタイトルには [デバイスのステータス] と表示されます。

適用可能なフィルタ: デバイス名とパッチ適用状況ステータス (パッチ適用済み、パッチ未適用、再起動の保留など)。

各行には、特定のデバイスおよびアイコンに関連する情報が含まれます。

- チェック マークは、該当するすべての脆弱性にパッチが適用されていることを示します。このデバイスは、現在のパッチ ポリシーに準拠しています。
- 電源ボタンは、脆弱性は適合しており、デバイスの再起動を保留していることを示します。

  再起動の保留中ステータスは、通常、短期間のステータスのため、パッチ未適用ステータスよりも優先されます。再起動の後、デバイスは最悪のケースのステータスを再度表示します。たとえば、再起動後、デバイスにパッチが適用されていないという脆弱性が残っている場合、そのデバイスには脆弱性を示す赤い X が表示されます。

- 疑問符は、少なくとも 1 つの脆弱性が確定できなかったことを示します。
- 赤い X は、このデバイスの少なくとも 1 つの脆弱性にパッチが適用されていないことを示します。
- 感嘆符は警告を示します。
- 小文字の「i」は「*適用できません*」を示します。

各デバイスについて、以下のことが行えます。

- 詳細については虫眼鏡をクリックします。
- そのデバイスで探索される製品を表示するには、[適用可能な製品] 列の数字をクリックします。
- そのデバイスに適用可能なブリテンを表示するには、[適用可能なブリテン] 列の数字をクリックします。
- このデバイスにパッチとしてインストールされたブリテンの一覧を表示するには、[パッチ適用済み] 列の数字をクリックします。

— パッチ検証プロセスで何らかの不一致が発生した可能性があるため、Patch Management がパッチ適用済みと確定できない脆弱性を表示するには、[警告] 列の数字をクリックします。

たとえば、Microsoft SQL Server または Microsoft MSDE のパッチは、警告として表示される場合があります。MSDE は、SQL Server より少ないファイルをインストールします。MSDE があるデバイスは、SQL Server のあるデバイスと同じパッチを適用できますが、パッチの中のすべてのファイルが必要なわけではありません。Patch Management は、その脆弱性をパッチ適用済みとしてレポートできないため、これは警告としてレポートされます。

もう 1 つの例は、デバイス上のファイルのバージョンがパッチで配信されたものより新しい場合です。この場合も、Patch Management は、その脆弱性をパッチ適用済みとしてレポートできないため、警告としてレポートされます。

— このデバイスに適用可能であるが、まだ適用されていないパッチを表示するには、[パッチ未適用] 列の数字をクリックします。

— [その他] 列の項目は、Patch Management が検証できなかったパッチまたはデバイスのエラーにより適用できなかったパッチを示します。

— [再起動の保留] 列の項目は、デバイスの再起動後に適用が完了するパッチを示します。これらのデバイスには、デバイス名の横に電源ボタン アイコンもあります。

フル パッチが適用されていないデバイス

パッチ ポリシーに準拠していないデバイスに焦点を当てるには、この適合性レポートを使用します。このレポートに含まれるデバイスには、パッチ未適用、その他 (デバイス エラーを含む)、または再起動の保留のステータスを持つ 1 つ以上の適用可能なブリテンが表示されます。このレポートは49 ページの「デバイスのステータス」と似ています。ただし、すべての適用可能なブリテンがパッチ適用済みか警告を報告しているだけのために、準拠とみなされるデバイスはこのレポートでは対象外になります。

適用可能なフィルタ: デバイス名、およびパッチ未適用、その他、再起動の保留のパッチ適用状況ステータス。

— 各デバイスに対して、49 ページの「デバイスのステータス」の適合性レポートで説明したものと同じ操作を実行できます。

— 最後の列は、デバイスが前回スキャンされてからの日数を示します。

再起動を保留中のデバイス

少なくとも 1 つのブリテンが再起動の保留になっているデバイスに焦点を当てるには、この適合性レポートを使用します。

適用可能なフィルタ: デバイス名。

— デバイスの各列の詳細を表示するには、その列に含まれるリンクをクリックします。

ブリテンのインストール エラーがあるデバイス

ブリテンのインストール中にエラーが発生したデバイスの一覧を表示するには、この適合性レポートを使用します。

適用可能なフィルタ: デバイス名。

— エラーが発生したデバイスとエラーの説明に関するブリテン一覧にリンクするには、**[その他]** 列の番号をクリックします。

ブリテンのステータス

パッチの「適合性 (ブリテン別) レポートを表示するには、[ブリテンのステータス] を使用します。レポートには、指定されたブリテンに対して、そのブリテンを適用できるデバイスの数、およびそのブリテンの各パッチ ステータスを持つデバイスの数が表示されます。パッチ ステータスには、「パッチ適用済み」、「警告」、「パッチ未適用」、「その他」(発生したエラーが)、または「再起動の保留」が含まれます。各行には、特定のブリテンとアイコンに関する情報が含まれます。

適用可能なフィルタ: ブリテン名、ブリテン ベンダー、またはブリテン タイプ (セキュリティ更新やサービス パックなど)。

各行には、特定のブリテンおよびアイコンに関連する情報が含まれます。

— チェック マークは、このブリテンがすべての適用可能デバイスに適用されていることを示します。

— 電源ボタンは、少なくとも 1 つのデバイスが適合するための再起動を保留していることを示します。

再起動の保留中ステータスは、通常、短期間のステータスであるため、パッチ未適用ステータスより優位です。再起動の後、デバイスは最悪のケースのステータスを再度表示します。たとえば、再起動後、デバイスにパッチが適用されていないという脆弱性が残っている場合、そのブリテンには脆弱性を示す赤い X が表示されます。

— 疑問符は、少なくとも 1 つのデバイスでこの脆弱性が確定されていないことを示します。

— 赤い X は、少なくとも 1 つのデバイスで、このブリテンのパッチが適用されていないことを示します。

— 感嘆符は警告を示します。

各ブリテンについて、以下のことが行えます。

— ブリテンに関する詳細をベンダーの Web サイトで参照するには、[ブリテン] 列のブリテン番号をクリックします。

— Common Vulnerabilities and Exposures の Web サイトに移動するには、[CVE] 列の CVE 番号をクリックします。

— そのブリテンに適用可能なデバイスを表示するには、[適用可能なデバイス] 列の数字をクリックします。

— パッチ適用済みのデバイスを表示するには、[パッチ適用済み] 列の数字をクリックします。

— パッチ検証プロセスで何らかの不一致が発生した可能性があるため、Patch Management がパッチ適用済みと確定できない脆弱性を表示するには、[警告] 列の数字をクリックします。

たとえば、Microsoft SQL Server または Microsoft MSDE のパッチは、警告として表示される場合があります。MSDE は、SQL Server より少ないファイルをインストールします。MSDE があるデバイスは、SQL Server のあるデバイスと同じパッチを適用できますが、パッチの中のすべてのファイルが必要なわけではありません。Patch Management は、その脆弱性をパッチ適用済みとしてレポートできないため、これは警告としてレポートされます。

もう 1 つの例は、デバイス上のファイルのバージョンがパッチで配信されたものより新しい場合です。この場合も、Patch Management は、その脆弱性をパッチ適用済みとしてレポートできないため、警告としてレポートされます。

— 適用可能であるが、まだ適用されていないパッチを表示するには、[パッチ未適用] 列の数字をクリックします。

— [その他] 列の項目は、Patch Management が検証できなかったパッチまたはエラーの発生したパッチを示しています。

— [再起動の保留] 列の項目は、デバイスの再起動後に適用が完了するパッチを示します。

製品ステータス

[製品のステータス] ビューには、適合性 (製品別) レポートが表示され、1 行に各製品とパッチ配布方法が表示されます。次に例を示します。

— (MSFT) の付いた製品名は、「メタデータのダウンロードの有効化」がオンにされて配布されています。

— 修飾子のない製品名は、「メータデータのダウンロードの有効化」がオフにされて配布されています。

このリストには、バージョン 7.50 以上の HPCA Agent が必要です。HPCA 7.50 サーバー環境で Version 7.50 よりも前の Patch Agent が動作している場合、レポートのデータは生成されず、表示されるレコードはありません。

適用可能なフィルタ: 製品名、デバイス名、パッチ適用状況ステータス。

各製品について、以下のことが行えます。

— 検出された脆弱性を表示します。

— その製品の適用可能なブリテン数とデバイスの詳細を表示するには、計数列のいずれかの数字をクリックします。

— 製品リリースに対して選択したデバイスに適用可能なブリテンの一覧を表示するには、結果のビューで [適用可能なブリテン] をクリックします。

リリースのステータス

[リリースのステータス] ビューには、リリース別に製品名を表示する「適合性 (リリース別)」レポートが表示されます。各製品の各リリースとパッチ配布方法につき 1 行で表示します。次に例を示します。

— (MSFT) の付いたリリース名では、「メタデータのダウンロードの有効化」がオンにされてブリテンが配布されています。

— 修飾子のないリリース名では、「メタデータのダウンロードの有効化」がオフにされてブリテンが配布されています。

適用可能なブリテンを表示するにはクリックします。

このリストには、バージョン 7.50 以上の HPCA Agent が必要です。HPCA 7.50 サーバー環境で Version 7.50 よりも前の Patch Agent が動作している場合、レポートのデータは生成されず、表示されるレコードはありません。

適用可能なフィルタ: リリース名、デバイス名、パッチ適用状況ステータス。

— デバイスの一覧と、この製品リリースの各デバイスの適用可能なブリテン数を表示するには、[適用可能なブリテン] の数字をクリックします。

— この製品リリースのこのデバイスに適用可能なブリテンの一覧を表示するには、[適用可能なブリテン] の数字をクリックします。

パッチのステータス

[パッチのステータス] ビューには、パッチ別に製品を表示する「適合性 (パッチ別)」レポートが表示されます。各パッチにつき 1 行で表示します。

このリストには、バージョン 7.50 以上の HPCA Agent が必要です。HPCA 7.50 サーバー環境で Version 7.50 よりも前の Patch Agent が動作している場合、レポートのデータは生成されず、表示されるレコードはありません。

適用可能なフィルタ: パッチの言語、パッチの Qnumber、パッチ番号、ブリテン名、およびパッチ適用状況ステータス。

— その特定の列のデバイスを表示するには、[適用可能なデバイス] 列または計数列の数字をクリックします。

重大なエラーが発生したデバイス

[重大なエラーが発生したデバイス] ビューには、エージェント デバイスで発生したエラーの一覧を示すレポートが表示されます。

61 ページの「FINALIZE_PATCH サービスの使用許可」セクションで説明したように、このレポートを使用するには、FINALIZE_PATCH サービスがお使いの環境の管理対象デバイスにアクセスできることを確認してください。

取得レポート

取得レポートは次の 3 つがあります。

- 取得の概要
- 取得 (ブリテン別)
- 取得 (パッチ別)

取得レポートの詳細については、28 ページの「パッチ取得レポート」を参照してください。

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 サイトで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。

リサーチ レポートは次のとおりです。

- 55 ページの「リサーチ (ブリテン別)」
- 56 ページの「リサーチ (デバイス別)」
- 56 ページの「リサーチ (パッチ別)」
- 57 ページの「リサーチ (製品別)」
- 57 ページの「リサーチ (リリース別)」
- 57 ページの「適合性とリサーチ例外レポート」

リサーチ (ブリテン別)

すべてのブリテンに掘り下げるには、このレポートを使用します。詳細を各ベンダーの Web サイトで参照するには、[名前] 列のブリテン番号をクリックします。Common Vulnerabilities Exposures の Web サイトに移動するには、[CVE] 列の数字をクリックします。このブリテンに必要なファイルを表示する、それらが配布できるかを確認する、およびそのパッチが別のパッチで置換されているかどうかを確認するには、[タイトル] または [適用可能なパッチ] 列の数字をクリックします。このブリテンによって影響を受ける製品を確認するには、[適用可能な製品] 列の数字をクリックします。[重大度] 列のアイコンは、Windows ブリテンの重大度を示します。重大度の評価範囲は、[最重要] から、[重要]、[中]、[低] までです。ブリテンが Windows プラットフォーム用でない場合、[不明] アイコンが表示され

ます。重大度が同じブリテンをすべて表示するには、[重大度] 列のアイコンをクリックします。既存ブリテンに重大度評価はありません。既存のブリテンおよびパッチの重大度評価を表示するには、[強制] および [置換] オプションを使用して再取得する必要があります。

このレポートは、ブリテン名フィルタを使用してフィルタリングすることはできません。

WSUS でサポートされていないパッチがブリテンに含まれており、それらのパッチの重大度が同じブリテンに含まれている他のパッチよりも高い場合、このレポートと取得 (ブリテン別) レポートに表示される重大度評価が [Microsoft セキュリティ ブリテン サマリー] ページと一致しない場合があります。この問題は、ブリテンに含まれているパッチの重大度によってブリテンの重大度評価が決定されるために発生します。WSUS でサポートされないレガシー パッチがブリテンに含まれている場合、それらのパッチを除外して重要度の評価が決定されます。

リサーチ (デバイス別)

特定のデバイスによってフィルタ設定されたすべてのブリテンに掘り下げるには、このレポートを使用します。そのデバイスで探索される製品を表示するには、[適用可能な製品] 列の数字をクリックします。Microsoft Windows インストーラのバージョンがあるデバイスをすべて表示するには、[MSI バージョン] 列のバージョン番号をクリックします。Windows Update Agent のバージョンがあるデバイスをすべて表示するには、[WUA バージョン] 列の数字をクリックします。デバイスの Windows Update Agent のバージョンがサーバーで使用可能な最新バージョンと比較して同じか、新しいか、または古いかに応じて、[ステータス] 列には [準拠] または [非準拠] を示すアイコンが表示されます。デバイスに使用できる Windows Update Agent バージョン情報がない場合は、[不明] アイコンが表示されます。Windows Update Agent のステータスがあるデバイスをすべて表示するには、[ステータス] 列のステータス アイコンをクリックします。このテーブルのフィルタは組み合わせて使用でき、情報は列見出しをクリックするとソートできます。

リサーチ (パッチ別)

パッチ ファイルに関する情報を、取得ステータスを含めて表示するには、このレポートを使用します。Common Vulnerabilities Exposures の Web サイトに移動するには、[CVE] 列の数字をクリックします。[ダウンロード] 列のアイコンをクリックして、パッチ ファイルをダウンロードします。[重大度] 列のアイコンは、

Windows パッチの重大度を示します。重大度の評価範囲は、[最重要] から、[重要]、[中]、[低] までです。パッチが Windows プラットフォーム用でない場合は、[不明] アイコンが表示されます。重大度が同じパッチをすべて表示するには、[重大度] 列のアイコンをクリックします。既存パッチに重大度評価はありません。既存のブリテンおよびパッチの重大度評価を表示するには、[強制] および [置換] オプションを使用して再取得する必要があります。

リサーチ (製品別)

製品によってフィルタ設定されたすべてのブリテンに掘り下げるには、このレポートを使用します。このレポートの「存在しない Redhat」製品の [適用可能ブリテン] 列の数字をクリックすると、「ブリティンの依存関係」レポートの下に Redhat 依存ブリテン一覧が表示されます。

リサーチ (リリース別)

製品リリースによってフィルタ設定するには、このレポートを使用します。そのリリースのすべてのブリテンを表示するには、[適用可能なブリテン] 列の数字をクリックします。このレポートの「存在しない Redhat」製品の [適用可能ブリテン] 列の数字をクリックすると、「ブリティンの依存関係」レポートの下に Redhat 依存ブリテン一覧が表示されます。

適合性とリサーチ例外レポート

適合性とリサーチ例外レポートは、標準のリサーチと適合性デバイス レポートの条件に一致しないデバイスの情報を提供するためのものです。これらの例外レポートのデバイスはすべて、ある種の例外状態にあります。この例外状態には、主に 3 つの理由があります。

- パッチ探索中の接続エラー。
- 取得が [強制] および [置換] オプションで実行されたことによる、デバイスのステータス情報からの切断。
- 操作できない Patch Management Agent。

この例外を解決するには、デバイスで新しい探索を実行します。新しい探索で取得が切断される場合はエラーが解決されるか、接続性の問題が解決されます。また、操作できない Patch Management Agent のトラブルシューティングで使用できるログが生成されます。リサーチ例外レポートは、リサーチ レポートの条件があまり厳しくないため、適合性例外レポートのデバイスの単なるサブセットとして表示されます。

脆弱性の管理

企業の中で脆弱性が存在する可能性がある場所を見つけたら、Patch Management を使用して、これらの脆弱性を管理対象デバイスで管理します。すべてのブリテンには、PATCHMGR ドメインに ZSERVICE (Services) インスタンスがあります。これは、SOFTWARE ドメインの ZSERVICE (Application) インスタンスに似ています。SOFTWARE ドメインの ZSERVICE インスタンスで使用できる属性の説明については、『HP Client Automation 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。また、PATCHMGR.ZSERVICE インスタンスは、バンド幅スロットリングをサポートします。詳細については、HP サポート Web サイトを参照してください。

ポリシー エンタイトルメントを ZSERVICE レベルで設定します。ブリテンと同じ名前を持つ ZSERVICE インスタンスを、POLICY ドメインのユーザー インスタンスか Null インスタンスに接続します。

SuSE 10 および 11 ブリテンには、元のブリテン名を基にしたインスタンス名が HP によって割り当てられます。詳細については、59 ページの「SuSE 10 および 11 ブリテンのインスタンス名の命名規則」を参照してください。

脆弱性を管理するには

1. Admin CSDB Editor を開始して PRIMARY.POLICY.USER クラスに移動します。
2. ユーザー インスタンスを右クリックして、**[接続を表示]** を選択します。
3. **[接続可能なクラスを表示するドメイン]** ドロップダウン ボックスで **[PATCHMGR ドメイン]** を選択します。
4. **[OK]** をクリックします。
5. 脆弱性を管理するブリテンをドラッグし、適切なユーザー インスタンスにドロップします。カーソルがペーパー クリップに変わったら、マウス ボタンを離します。
6. **[コピー]** をクリックします。
7. **[はい]** をクリックして接続を確認します。

パッチがユーザーのポリシーに追加されます。次回、ユーザーがログインするとき、必要であればインストールも含めて脆弱性が管理されます。

SuSE 10 および 11 ブリテンのインスタンス名の命名規則

CSDB のインスタンスのフィールド長は 32 文字に制限されているため、すべての SuSE 10 および 11 ブリテンは、実際の SuSE 10 および 11 ブリテン名より短く識別しやすいように、HP によって再フォーマットされたインスタント名を使用してパブリッシュされます。

SuSE 10 の場合

取得時に SuSE10 のブリテン名は新しい名前に変換され、PRIMARY.PATCHMNGR.BULLETIN および PRIMARY.PATCHMGR.ZSERVICE というインスタンス名が指定されます。

新しいインスタンス名は、次のように作成されます。

たとえば、HP Patch Management では取得用に入力された SuSE 10 ブリテン名は次のように変換されます。

SuSE Linux Enterprise Server 10 の場合:

```
SUSE-patch-MozillaFirefox-2683
```

は、次のように変換されます。

```
SLES10SP0-2683-MOZILLAFIREFOX
```

SuSE Linux Enterprise Desktop 10 の場合:

```
SUSE-patch-MozillaFirefox-2683
```

は、次のように変換されます。

```
SLED10SP0-2683-MOZILLAFIREFOX
```

SuSE Linux Enterprise Server 10SP3 の場合:

```
SUSE-patch-SLESP3-MozillaFirefox-2683
```

は、次のように変換されます。

```
SLES10SP3-2683-MOZILLAFIREFOX
```

SuSE Linux Enterprise Desktop 10SP3 の場合:

```
SUSE-patch-SLESP3-MozillaFirefox-2683
```

は、次のように変換されます。

```
SLED10SP3-2683-MOZILLAFIREFOX
```

再フォーマットにより、SUSE-PATCH プレフィックスが削除され、残りのコンテンツが並べ替えられ、固有のナンバリング スキームは形式の前方に移動されます。上の例の場合、PRIMARY.PATCHMGR.BULLETIN および PRIMARY.PATCHMGR.ZSERVICE にある CSDB インスタンスは名前 SLES10SP0-2683-MOZILLAFIREFOX を使用して作成されます。

注: 元の SuSE ブリテン名にあるカンマまたはドットは、CSDB で作成され再フォーマットされるインスタンス名では、常にハイフン (-) に置き換えられます。

SuSE 11 の場合

取得時に SuSE 11 ブリテン名は新しい名前に変換され、PRIMARY.PATCHMNGR.BULLETIN および PRIMARY.PATCHMGR.ZSERVICE にあるインスタンス名は新しい名前の形式で作成されます。

新しいインスタンス名は、次のように作成されます。

たとえば、HP Patch Management では取得用に入力された SuSE 11 ブリテン名は次のように変換されます。

UPDATEINFO-SLESSP0-MOZILLAFIREFOX**-1234**

は、次のように変換されます。

SLES**11**SP0**-1234**-MOZILLAFIREFOX

再フォーマットにより、UPDATEINFO- プレフィックスが削除され、残りのコンテンツが並べ替えられ、固有のナンバリング スキームは形式の前の方に移動されます。複数の SuSE バージョン間での一意性を維持するために、SLESSP0 は、製品名とサービス パック名の間に SLES**11**SP0 のようにバージョン (11) が含められるように拡張されます。

上の例の場合、PRIMARY.PATCHMGR.BULLETIN および PRIMARY.PATCHMGR.ZSERVICE にある CSDB インスタンスは名前 SLES11SP0-1234-MOZILLAFIREFOX を使用して作成されます。

元の SuSE ブリテン名にあるカンマ、ドット、または アンダースコアは、CSDB で作成され再フォーマットされるインスタンス名では常にハイフン (-) によって置き換えられます。

FINALIZE_PATCH サービスの使用許可

Patch Management Agent 接続の間に、適用可能なパッチがダウンロードされ、キューに追加されて、FINALIZE_PATCH と呼ばれる Patch Management サービスにより管理されます。このサービスは、Patch Management Agent の最後のサービスとして優先的に実行されます。このサービスでは、リアルタイムでパッチ適合情報のレポートを作成する必要があります。

パッチの他に、PRIMARY.PATCHMGR.ZSERVICE.FINALIZE_PATCH サービスをすべての管理対象デバイスのポリシーに追加します。

このサービスを使用しないと、拡張パッチ管理アクティビティとなり、リアルタイムのパッチ適合性情報レポートが作成できません。

自動および対話型パッチの配布

一部のパッチは、パッチのベンダーにより配布時にユーザーの介入が必要な設計になっています。配布にユーザーの介入が不要な場合、Patch Management はパッチを**自動**と定義します。配布にユーザーの介入が必要な場合、パッチを**対話型**と定義します。Patch Management は、自動パッチおよび対話型パッチの両方で脆弱性を検出できます。Patch Management は、対話型パッチおよび自動パッチの配布をどちらもサポートします。ただし、ベンダーが対話型として作成したものは、インストール時にユーザーの介入を求めるか、インストールに失敗します。

HP が XML ファイルの中でデータの修正を行ったものか、お客様がカスタマイズしたブリテンだけが対話型としてマークされます。この情報は、ブリテンの配布属性および HP が提供する XML ファイルの Patch ノードで参照できます。有効な値は、AUTOMATIC と INTERACTIVE です。デフォルトでは、ベンダーはこの情報を提供しません。このため、お客様は、お使いの環境でブリテンの使用許可を与える前に、パッチが対話型かどうかを検証するために配布のテストをする必要があります。

ブリテンが Configuration Server Database にパブリッシュされるときに、PATCHMGR ドメインにある ZSERVICE クラスの RUNMODE 属性でパッチのタイプが定義されます。radskman コマンド ラインの catexp パラメータを使用して、自動とマークされているブリテンのみにインストールを制限します。形式は catexp=runmode:automatic のようになります。catexp パラメータが存在しない場合は、すべてのブリテンが処理されます。一般的な Patch Management Agent 接続では、次のような radskman コマンド ラインを使用できます。

```
radskman ip=<RCSIP>,port=<RCSPORT>,dname=patch,catexp=
runmode:automatic
```

radskman の詳細については、『HP Client Automation 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。

レポーティング オプションのカスタマイズ

脆弱性をエラーとしてマーク (X で示される) したくない場合や、警告 (感嘆符で示される) を OK (チェック マーク) のステータスでマークしたくない場合があります。デフォルトは、OPTIONS クラスで指定されます。OPTIONS クラスのインスタンスを例として表示できます。

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」と表示されます。

この動作を変更する必要がある場合、次の 3 つの新しい説明属性を使用してカスタム .xml ファイルを作成します。

- **DesiredState**
  この属性は、OPTIONS、FILECHG、および REGCHG クラスの DSTATE 属性 にマップされます。この属性を使用して、USE 変数で示され、リターンコードがベースにする条件を設定します。
- **レポートのしきい値**
  この xml 属性は、OPTIONS、FILECHG、および REGCHG クラスの REPORT 属性にマップされます。ファイルまたはレジストリ キーのプロパティは、この値に基づいて Patch Management に送信されます。リターンコードが REPORT 属性の値以上の場合、そのファイルとレジストリの情報は Patch Management に送信され、Patch Management レポートで使用できるようになります。たとえば、リターン コードが 4 (警告) または 8 (エラー) の場合、REPORT を **1** に設定してプロパティを送信します。

  REPORT を **0** に設定すると、OK ステータスで示されるすべてのファイルの情報が送信されます。これにより、Patch Management Server に過剰な負荷がかかる可能性があります。

- **用途**
  この xml 属性は、OPTIONS、FILECHG、および REGCHG クラスの USE 属性にマップされます。USE は判断基準になる条件を指定します。

ファイル (FILECHG) で考えられる条件は、GMTDATE、SIZE、VERSION、CHECKSUM、および CRC32 です。レジストリの場合、オプションは VALUE です。

ファイルまたはレジストリの変更のレポート方法をカスタマイズする場合、依然として脆弱性が存在してもレポートには反映されないことがあるため注意してください。検出された脆弱性のレポーティングステータスを変更する前に、お使いの環境に特有の露出や脆弱性を排除するための対策を取ってください。作成したカスタマイズについては、経過を追跡してください。

FILECHG および REGCHG インスタンスのこれらの属性の値は、接続される OPTIONS インスタンスの値を上書きします。FILECHG および REGCHG インスタンスでこれらの値を空白にすると、接続された OPTIONS クラスの値が使用されます。パッチ説明 XML ファイルにこれらの属性が含まれない場合、接続された OPTIONS インスタンスの値が使用されます。

レポーティング オプションをカスタマイズするには

ここでは、演習のために、すべての変更は OPTIONS クラスに対するものと仮定します。OPTIONS クラスのインスタンスを、レポーティングをカスタマイズするファイルまたはレジストリ コンポーネントに接続します。

1. 適切なクラス (またはパッチ説明ファイル) の USE 属性で、評価するファイルまたはレジストリ キーのプロパティを指定します。たとえば、ファイルの日付が必要な場合は GMTDATE に USE を設定します。
2. DSTATE (DesiredState) をリターン コードと同じステートに設定します。複数の条件は、カンマで区切ります。以下のリストから適切なステートを使用します。
   - ステータスの唯一の条件が、ファイルまたはレジストリ キーが存在するかどうかの場合、ステート E (存在する) を使用します。
   - ステータスの唯一の条件が、ファイルまたはレジストリ キーが存在しないかどうかの場合、ステート !E (存在しない) を使用します。
   - ファイルまたはレジストリ キーが条件と完全に一致する場合は、ステート EQ (等しい) を使用します。
   - ファイルまたはレジストリ キーが少なくとも条件の 1 つに一致しない場合は、ステート !EQ (等しくない) を使用します。
   - ファイルまたはレジストリ キーが少なくとも条件の 1 つより小さい場合は、ステート LT (より小さい) を使用します。

— ファイルまたはレジストリ キーが少なくとも条件の 1 つより大きい場合は、ステート GT (より大きい) を使用します。

以下のリストから適切なリターン コードを使用します。

— OK のステータスを示す場合は 0 を使用します。

— 警告ステータスを示す場合は 4 を使用します。

— エラー ステータスを示す場合は 8 を使用します。

有効な DSTATE 値のルール

— 少なくとも条件の 1 つはリターン コード 0 (OK) にする必要がありますが、複数の条件が 0 以外の値 (4、8) を返すようにすることができます。

— 同等 (EQ) のテストを行うことは、コンポーネントが存在し、DSTATE 変数で表現する必要がないことを意味します。

以下のサンプルは、ファイル オプションでカスタマイズされたオプションの例を示しています。Use タグで指定される条件は、VERSION、GMTDATE、および SIZE です。DesiredState タグは、以下を説明します。

— ファイルが存在しない (!E=0) 場合は、OK ステータスを返します。

— ファイルの VERSION、GMTDATE、または SIZE がパッチ適用済みファイルより大きい (GT=4) 場合は、警告ステータスを返します。

— ファイルの VERSION、GMTDATE、または SIZE がパッチ適用済みファイルより小さい (LT=8) 場合は、エラー ステータスを返します。

```
<FileChg Name="snmpsfx.dll" CRC32="" Gmttime=""
Path="%windir%¥system32" Size="" Checksum="14922"
Gmtdate="19990212" Version="4.0.1381.164"
DesiredState="!E=0,GT=4,LT=8" ReportThreshold="1"
Use="VERSION,GMTDATE,SIZE" />
```

XML ファイルの値は、すべてが引用符で囲まれています。

3 REPORT しきい値を設定します。ファイルまたはレジストリ キーのプロパティは、この値に基づいて Patch Management に送信されます。リターン コードが REPORT 属性の値以上の場合、そのファイルとレジストリの情報は Patch Management に送信され、Patch Management レポートで使用できるようになります。たとえば、リターン コードが 4 (警告) または 8 (エラー) の場合、REPORT を 1 に設定してプロパティを送信します。

変更は、次にパッチ説明ファイルを Configuration Server Database にパブリッシュしたときに有効になります。

脆弱性の検出と配布の無効化

ブリテンまたはパッチの検出や配布を無効にできます。このためには、Admin CSDB Editor を使用して、PATCHMGR ドメインの Bulletin または Patch インスタンスで ENABLED 属性を **N** に設定します。

特定のブリテンのすべてのパッチを無効にする場合、そのブリテンのインスタンスで ENABLED 属性を **N** に設定します。特定のパッチ ファイルの検出および配布のみを無効にする場合は、そのパッチ ファイルのインスタンスで ENABLED 属性を設定します。

パッチの配布の制御 (PATCHARG)

各パッチ ファイルで、Patch Management はパッチをインストールするためのパラメータ、および可能であればパッチを削除するためのパラメータも設定します。これらのパラメータは、PATCHMGR ドメインの PATCHARGS クラスの Patch Command Line (OCREATE) 属性および Uninstall Command Line (ODELETE) 属性にあります。

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」と表示されます。

パッチ ファイルのインストールとアンインストールで、コマンド ライン パラメータを変更できます。PATCHARG クラスを使用してインスタンスを作成し、それを適切なパッチ ファイルに接続します。

PATCHARG を使用して代替コマンド ライン パラメータを作成するには

1. Admin CSDB Editor を使用して、PATCHMGR ドメインの PATCHARG クラスに移動します。
2. **PATCHARG** を右クリックして新しいインスタンスを作成します。この例では、WSPARGS という新しいインスタンスが作成されます。
3. 使用する新しいパラメータを入力します。PATCHARG クラスには、パッチをインストールする OCREATE とパッチを削除する ODELETE の 2 つの属性があります。

4 BULLETIN クラスのパッチ ファイルの PATCHARG 属性の代わりに、PATCHARG インスタンスのパスを入力します。

作成したパラメータは、このパッチ ファイルで使用されます。

パッチの削除

デフォルトでは、ユーザーを ZSERVICE (Microsoft 脆弱性サービス) インスタンスから切断しても、インストール済みのパッチは削除されません。この動作は、CMETHOD (Client Method) クラスの MANAGE インスタンスの ZDELETE 属性で制御されており、デフォルトでは無効です。

Red Hat セキュリティ アドバイザリと SuSE セキュリティ アドバイザリの削除は、どちらも Patch Management では意図的に無効にされています。Linux ベンダーが提供するパッチがターゲット システムに適用されると、影響を受ける Linux ソフトウェアは、特定のセキュリティ脆弱性を解決する最新の rpm パッケージ バージョンとリリースに更新されます。アドバイザリ (パッチ) を提供した Linux ベンダーのアプリケーションは、元のパッケージのバックアップを維持しないため、以前のバージョンに自動的にロールバックすることはできません。Linux rpm パッケージをデバイスから削除しようとすると、パッチだけでなく、パッチが適用されている rpm ソフトウェア パッケージまで削除されます。新しい脆弱性が見つかると、Linux セキュリティ パッチのベンダーは新しいパッチをリリースします。これは、パッチのベンダーによって設定されている Red Hat および SuSE セキュリティ アドバイザリの性質です。

Microsoft パッチで、脆弱性管理からユーザーを削除するときにパッチ ファイルも削除する場合は、ZDELETE 属性を編集してください。

PATCHMGR.CMETHOD.MANAGE.ZDELETE メソッドを変更すると、ユーザーに脆弱性が割り当てられていない場合、*すべてのユーザーのすべてのパッチ*が削除されます。

詳細については、66 ページの「パッチの削除」を参照してください。

ユーザーがサービスに割り当てられていない場合にパッチを削除するには

1 Admin CSDB Editor を使用して、PATCHMGR ドメインの CMETHOD (Client Method) クラスの MANAGE インスタンスに移動します。

2 ツリー ビューで ZDELETE 属性をダブルクリックし、テキスト ボックスに次のように入力します。

```
hide nvdkit &(ZMASTER.ZSYSDRV)&(ZMASTER.ZSYSDIR)
patchagt.tkd manage
```

3 **[OK]** をクリックしてインスタンスを変更します。[インスタンスの編集の確認] 画面が表示されます。

4 **[はい]** をクリックして、変更を確定します。

Patch Management Agent は、管理対象デバイスが必要な設定変更を受信してパッチを削除できるようにするために、接続を行う必要があります。

次回ユーザーを PATCHMGR ドメインの ZSERVICE インスタンスから切断するときに、パッチ ファイルは削除されます。

要約

- Patch Management には、リサーチ、パッチの取得、および脆弱性のレポート機能があります。
- レポートを使用して、企業の脆弱性を確認します。
- パッチのサービスをお使いのデバイスに割り当てることで、脆弱性を管理します。

A パッチで使用できる XML タグ

説明ファイル

HP が提供するパッチ説明ファイルには、製品、リリース、パッチ、およびパッチ マニフェストに関する情報が含まれます。これらについては、次の図の下にある表を参照してください。

カスタム パッチ説明ファイルを作成する場合、サポートされているタグを使用してください。パッチ説明ファイルのノード階層は、次の図で示されているとおりです。

図 5　サンプルのパッチ説明ファイル

Bulletin ノード

ノード名: Bulletin

親ノード: なし

子: Products

表 5　BULLETIN クラスの XML タグ

XML タグ	HPCA 属性	説明
PopularitySeverityID	POPULAR	Popularity ID
URL	URL	Bulletin URL
FAQURL	FAQURL	FAQ URL
Supported	SUPPORT	Supported [Y/N]
ImpactSeverityID	IMPACT	ImpactID ソース : Red Hat Network、Novell (SuSE) のデータフィード
MitigateSeverityID	MITIGATE	Mitigate ID
PreReqSeverityID	PREREQ	Prereq ID
DateRevised	REVISED	Bulletin Revised On ブリテンが改訂された日付を YYYYMMDD 形式で示します。 ソース : Red Hat Network、Novell (SuSE) のデータフィード
Source	SOURCE	Source [MICROSOFT|NOVADIGM|CUSTOM|REDHAT|SUSE] パッチ説明ファイルのパブリッシュ元のディレクトリ。
Vendor	VENDOR	MICROSOFT/REDHAT/SUSE
Type	TYPE	Type of Bulletin Security/ServicePack/Other
Platform	PLATFORM	winnt//redhat/suse

表 5　BULLETIN クラスの XML タグ

XML タグ	HPCA 属性	説明
Name	NAME	External ID ソース： Red Hat Network、Novell (SuSE) のデータフィード
Title	TITLE	タイトル ブリテンのタイトル。 ソース： Red Hat Network、Novell (SuSE) のデータフィード
DatePosted	POSTED	Bulletin Posted On ブリテンがポストされた日付を YYYYMMDD 形式で示します。 ソース : Red Hat Network、Novell (SuSE) のデータフィード
Schema Version		パッチ スキーマ バージョンで、現在は 1.0 です。
	MTIME	インスタンスが CSDB で変更された時刻。
	CTIME	インスタンスが CSDB に作成された時刻。
	ID	内部インスタンス ID。
HPPosted	HPPOSTED	ブリテンが HP によって内部的にポストされた日付。
HPRevised	HPREVISD	ブリテンが HP によって改訂された日付。
Deployment	RUNMODE	パッチが自動的にインストールされる (AUTOMATIC) か、ユーザーの介入が必要 (INTERACTIVE) かを指定します。

Products ノード

ノード名: Products

親ノード: Bulletin

子: Product

属性: なし

Products ノード

ノード名: Product

親ノード: Products

子: Releases

表 6　PRODUCT クラスの XML タグ

XML タグ	HPCA 属性	説明
Name	NAME	ソース : Red Hat Network、Novell (SuSE) のデータ フィード
Name	NAME	ソース : Red Hat Network、Novell (SuSE) のデータ フィード

Releases ノード

ノード名: Releases

親ノード: Product

子: Release

属性: なし

Release ノード

ノード名: Release

親ノード: Releases

子: Patch

表 7　RELEASE クラスの XML タグ

XML タグ	HPCA 属性	説明
Name	NAME	ソース : Red Hat Network、Novell (SuSE) のデータ フィード

Patch ノード

ノード名: Patch

親ノード: Release

子: Package

表 8　PATCH クラスの XML タグ

XML タグ	HPCA 属性	説明
PatchURL	PATCHURL	.EXE または .MSI ファイルを参照する URL。 ソース : SUS、Red Hat Network、Novell (SuSE) のデータ フィード
再起動サイキドウ	REBOOT	パッチをインストールした後にデバイスを再起動する必要がある場合は指定します。 ソース : SUS、Red Hat Network、Novell (SuSE) のデータ フィード
Architecture	ARCH	x86/i64 ソース : SUS、Red Hat Network、Novell (SuSE) のデータ フィード
Language	LANG	en、fr、de ソース : SUS
MSSUSName	SUSNAME	このパッチの SUS 名。
SupercededByBulletin	SUPERBU	このパッチより優先されるブリテン名。 ソース : Red Hat Network、Novell (SuSE) のデータ フィード
Superceded	SUPERCED	パッチが置換された場合は指定します。有効な値は Y または N です。 ソース : Red Hat Network、Novell (SuSE) のデータ フィード
OSVersion	OSVER	オペレーティング システムのバージョン
OSType	OSTYPE	サーバーやワークステーションなど、オペレーティング システムのタイプ。

表 8　PATCH クラスの XML タグ

XML タグ	HPCA 属性	説明
OSSuite	OSSUITE	データセンターやブレードなど、オペレーティング システム スイート。
Platform	PLATFORM	プラットフォーム タイプ : winnt、redhat、suse
InstallCmdline	OCREATE	これは create プロシージャに渡される引数です。 ソース : SUS、Red Hat Network、Novell (SuSE) のデータ フィード
VerifyCmdline	OVERIFY	検証引数
UninstallCmdline	ODELETE	アンインストール引数
ObjectType	OTYPE	形式 : namespace=script filename デフォルト : winnt.patch これは、オブジェクトのタイプと以下のプロシージャを定義したスクリプト ファイルの名前を指定します。 検証 作成 削除 assert プロシージャは、名前の一部に winnt.patch::create のようにネームスペースが必要です。 スクリプト ファイル名が指定されていない場合、ファイル名は {namespace}.tcl です。 ソース : Novadigm
ProbeCmdline	OVERIFY	プローブ コマンド ライン。 ソース : Novadigm

表 8　PATCH クラスの XML タグ

XML タグ	HPCA 属性	説明
	ID	このパッチに対して HPCA-CSDB で作成された一意の ID。
	PATCHSIG	Patch Signature インスタンスの名前。 ソース : Novadigm
	LOCATION	パッチ データを含む LOCATION インスタンスの名前。
	BULLETIN	パブリッシュ時に設定されるブリテン名。 ソース : Red Hat Network、Novell (SuSE) のデータ フィード
	DATA	RCS にパッチ データがあるかどうかが [Y/N] でパブリッシュ時に指定されます。RCS にデータがある場合は Y、それ以外の場合は N です。
	DSTATE	パッチの要求ステート。これは通常、インスタンスから分類されます。 ソース : Novadigm
	REPORT	レポートしきい値。DSTATE と同様にインスタンスから分類されます。 ソース : Novadigm
	USE	要求ステートを確認するために使用される変数。 ソース : Novadigm
Deployment	RUNMODE	パッチが自動的にインストールされる (AUTOMATIC) か、ユーザーの介入が必要 (INTERACTIVE) かを指定します。

Patch Signature ノード

ノード名: PatchSignature

親ノード: Patch

子: FileChg、RegChg

属性: なし

FileChg ノード

ノード名: FileChg

親ノード: PatchSignature

子: なし

表 9　FILECHG クラスの XML タグ

XML タグ	HPCA 属性	説明
Name	NAME	ファイル名。
Path	PATH	ディレクトリ名。`%windir%` などの環境変数を含めることができ、Windows および Linux の適切なスクリプトで使用されます。
CRC32	CRC32	データの CRC。
Gmttime	GMTTIME	YYYYMMDD で示される GMTDATE 。
Gmtdate	GMTDATE	HH:MM:SS で示される GMTTIME。
Size	SIZE	ファイルのサイズ。
Checksum	CHECKSUM	ファイルのチェックサム。
Version	VERSION	ファイルのバージョン。

表 9　FILECHG クラスの XML タグ

XML タグ	HPCA 属性	説明
	DSTATE	FILECHG インスタンスの要求ステート。これは通常、CSDB の別のインスタンスから分類されます。 ソース : Novadigm
	REPORT	レポートのしきい値。このファイル変更インスタンスの評価時に RC がしきい値より大きい場合、そのインスタンスの ZOBJSTAT を作成します。 ソース : Novadigm
	USE	比較のときに使用する変数。Version、Checksum、Gmtdate など。 ソース : Novadigm

RegChg ノード

ノード名: RegChg

親ノード: PatchSignature

子: なし

表 10　REGCHG クラスの XML タグ

XML タグ	HPCA 属性	説明
Name	NAME	値の名前。
Path	PATH	フルパスで指定するレジストリ キー名。
Value	VALUE	レジストリに格納されたデータ値。

表 10　REGCHG クラスの XML タグ

XML タグ	HPCA 属性	説明
Type	TYPE	レジストリのデータ タイプは以下のいずれかです。 sz = Simple Registry String multi_sz = Registry Multi String expand_sz = Registry string with environment variables dword = Registry dword binary = Binary data
	DSTATE	FILECHG インスタンスの要求ステート。これは通常、RCS データベースの別のインスタンスから分類されます。 ソース : Novadigm
	REPORT	レポートのしきい値。このファイル変更インスタンスの評価時に RC がしきい値より大きい場合、そのインスタンスの ZOBJSTAT を作成します。 ソース : Novadigm
Type	TYPE	レジストリのデータ タイプは以下のいずれかです。 sz = Simple Registry String multi_sz = Registry Multi String expand_sz = Registry string with environment variables dword = Registry dword binary = Binary data
	DSTATE	FILECHG インスタンスの要求ステート。これは通常、RCS データベースの別のインスタンスから分類されます。 ソース : Novadigm

HPFileset ノード

ノード名: HPFileset

親ノード: PatchSignature

子: なし

表 11　HPFSET クラスの XML タグ

XML タグ	HPCA 属性	説明
Name	NAME	ファイルセット名
バージョン	VERSION	ファイルセット バージョン

B　管理対象デバイスの再起動

アプリケーション イベントに基づいて管理対象デバイスの再起動が必要な場合があります。再起動するには、ZSERVICE.REBOOT 属性で再起動の種類と再起動修飾子を指定します。修飾子を使用して以下のことが行えます。

- 警告メッセージのタイプを設定する
- 再起動をマシン接続かユーザー接続のどちらかで実行する
- アプリケーション イベントの直後に再起動する

アプリケーション イベント

最初に、再起動を必要とするアプリケーション イベントを指定します。使用する必要があるリブート タイプおよびすべてのリブート修飾子に、アプリケーション イベント コードを設定します。以下のセクションでは、リブートの各タイプおよびすべてのリブート修飾子を説明します。

radskman コマンド ラインで hreboot パラメータが指定されていない場合、このパラメータはデフォルトでサービスの再起動のリクエストを処理する Y に設定されます。hreboot を p に設定すると、再起動を必要とするサービスの有無に関わらず、管理対象デバイスの*電源が切断されます*。

アプリケーションのインストールおよび修復に関する警告メッセージなしでアプリケーションのハード リブートを直ちに実行する必要がある場合は、ZSERVICE.REBOOT 変数を AI=HQI、AR=HQI に設定します。

パッチの要件だけに基づいて、ベンダーによって提供される再起動パネルの動作を変更する場合、AL イベントを使用してロック ファイルの再起動イベントをトリガします。バージョニング イベント (VA) は Patch Management では適用できません。

- AI を使用してアプリケーション インストール時の再起動動作を指定します。デフォルトは、再起動なしです。

- AD を使用してアプリケーション削除時の再起動動作を指定します。デフォルトは、再起動なしです。
- AL を使用して、ロック ファイルが検出されたときの再起動動作を指定します。ロック ファイルが検出された場合のデフォルトの動作は、[OK] ボタンだけでハード リブートを実行するものです (HY)。
- AU を使用してアプリケーション更新時の再起動動作を指定します。デフォルトは、再起動なしです。
- AR を使用してアプリケーション修復時の再起動動作を指定します。デフォルトは、再起動なしです。
- AV を使用してアプリケーション バージョンのアクティブ化時の再起動動作を指定します。デフォルトは、再起動なしです。

リブート タイプ

コンピュータの再起動が必要なアプリケーションを決定した後、再起動のタイプを選択する必要があります。Client Automation は、コンピュータの再起動が必要であることを伝えるメッセージをオペレーティング システムに送信します。リブートには 3 つのタイプがあります。

- **ハード リブート (H)**

  開いている未保存ファイルの有無に関係なく、すべてのアプリケーションがシャット ダウンされます。サブスクライバには、開いている変更済みファイルの保存を要求する画面が表示されません。

- **ソフト リブート (S)**

  アプリケーションで開いた未保存のファイルがある場合、ユーザーに保存を要求する画面が表示されます。アプリケーションに未保存のデータがある場合、データの保存を求めるアプリケーションのリクエストにユーザーが応答するまで再起動せずに待機します。

- **再起動なし (N) (デフォルトの再起動の種類)**

  指定されたアプリケーション イベントが完了した後にコンピュータは再起動しません。これは、ロック ファイル イベント (AL) を除くすべてのアプリケーション イベントでのデフォルトのリブート タイプです。AL=N を指定すると、ロック ファイルが検出されたとき、管理対象デバイスは [OK] ボタンと [キャンセル] ボタンが表示されるハード リブートを実行しません。アプリケーション イベントに再起動のタイプが指定されない場合、再起動は起こりません。

リブート修飾子: 警告メッセージのタイプ

再起動が起こる前にサブスクライバに送信する警告メッセージのタイプを指定できます。リブート タイプを指定しても警告メッセージのタイプを指定しない場合、そのリブート タイプのデフォルトの警告メッセージが表示されます。警告メッセージには 3 つのタイプがあります。Application Self-Service Manager および Application Manager の警告メッセージは、Client Automation システム トレイに自動的に表示されます。警告メッセージを表示しない場合は、radskman コマンド ラインで ask=N を指定します。

Linux 用の Application Manager には再起動パネルが表示されません。

- **Quiet (Q)**

  再起動パネルは表示されません。

- **OK Button (A)**

  警告メッセージは [OK] ボタンのみで表示されます。[OK] をクリックして、再起動を開始します。ユーザーは再起動をキャンセルできません。

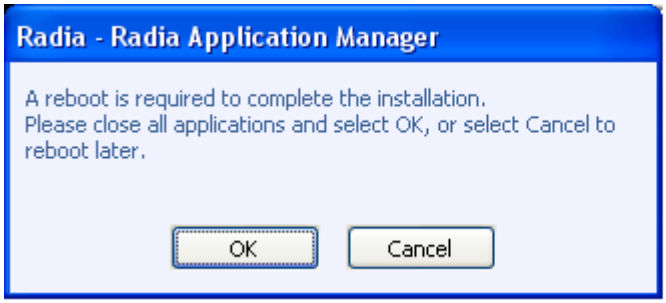
- **OK and Cancel Button (Y)**

  再起動を開始するには、[OK] をクリックします。サブスクライバが [キャンセル] をクリックすると、再起動が中止されます。

  radskman コマンド ラインに RTIMEOUT 値を追加することで、[警告メッセージ] ボックスにタイムアウト値を指定できます。管理対象デバイスが再起動プロセスを継続する前に待機する時間 (秒数) を RTIMEOUT で設定します。

たとえば、デフォルトの再起動パネルには、下の図のように **[OK]** と **[キャンセル]** が両方とも表示されます。

図 6　デフォルトの再起動の表示



エージェントの再起動パネルに [キャンセル] ボタンを表示しない場合、ZSERVICE.REBOOT 属性を AL=SA に指定します。これにより、次の図のようなダイアログ ボックスが表示されます。ベンダーから供給されたパッチのインストールを完了するために再起動が必須の場合は、これを使用します。

リブート修飾子: マシン オプションとユーザー オプション

管理対象デバイスは、radskman コマンド ラインのコンテキスト パラメータを指定することで、マシンまたはユーザーとして接続できます。マシンとユーザーの再起動修飾子を使用して、接続のタイプを基に再起動を完了する必要があるかどうかを指定します。

Patch Management Agent 接続はマシン コンテキストで発生します。

- **マシン接続での再起動 (空白)**
  マシンおよびユーザーの再起動修飾子が指定されていない場合は、デフォルトで、radskman に context=m が指定されているマシン接続で、またはコンテキスト パラメータが指定されていない場合にのみ、再起動が行われます。このデフォルトの動作は、大多数のリブート要件を満たします。
- **ユーザー接続のみでの再起動 (U)**
  radskman で context=u が指定されているユーザー接続、またはコンテキスト パラメータが指定されていない場合のみ再起動が行われます。radskman で context=m が指定されている場合は、再起動は行われません。
- **マシン接続とユーザー接続の両方での再起動 (MU)**
  アプリケーションのマシン コンポーネントとユーザー コンポーネントの両方がインストールされている場合にのみ再起動が行われます。

リブート修飾子: 即時の再起動

I を追加することで、再起動の各タイプを即時に実行するように変更できます。現在のサービスを解決した後、コンピュータを直ちに再起動する場合は、即時 (I) を使用します。Client Automation は、コンピュータが再起動した後でサブスクライバの残りのサービスを解決します。I を指定し、再起動のタイプに H または S を指定しない場合、ハード リブートが実行されます。

複数の再起動イベントの指定

同じエージェント接続で再起動イベントが必要なサービスが 2 つある場合、最も厳しい再起動の種類と再起動パネルが使用されます。最も制約が少ないリブートタイプはリブートなし (N) で、次がソフト リブート (S)、最も制約が厳しいのがハード リブート (H) です。最も制約の少ない再起動警告メッセージには、[OK] および [キャンセル] ボタン (Y) があり、次が [OK] ボタンのみ (A)、最も厳しい場合は完全に非表示 (Q) です。

サブスクライバは、インストール時に [OK] ボタンだけでソフト リブートすることが必要なアプリケーション AI=SA を割り当てられているとします。サブスクライバは、[OK] ボタンと [キャンセル] ボタンを両方表示して、ハード リブートが必要な (AI=HY) 2 番目のアプリケーションも割り当てられています。サブスクライバのすべてのアプリケーション イベントが完了すると、[OK] ボタンが表示され (A)、[OK] ボタンのみでハード リブート (H) が実行されます。

C Patch.cfg のパラメータ

この付録では、Patch Management Server 設定ファイル patch.cfg で使用できるすべてのパラメータについて説明します。可能な限り、これらのパラメータは HPCA Console を使用して編集してください。この一覧はサポート情報として提供されています。

Patch Management Server の設定パラメータ

HP は、HPCA Console で Patch Management パラメータを設定することをお勧めしています。HPCA Console を使用できない場合は、patch.cfg ファイルの中で直接変更できます。デフォルト ロケーションは、*<InstallDir>*¥PatchManager¥etc です。パラメータについては、この付録で説明します。

> 以前のバージョンの Patch Management から移行した場合、patch.cfg に古い値が維持されています。お使いの古い patch.cfg には新たに使用可能になったパラメータが取得されません。また、古いパラメータは新しいデフォルト値を取得しません。

- **admin_date_fmt**: HPCA Console の日付と時間の形式を指定します。デフォルトは {%Y-%m-%d %H:%M:%S} です。ここで、%Y は年号、%m は月、%d は日、%H は 24 時間形式の時間、%M は分、%S は秒です。
- **data_dir**: ローカル コンピュータ (Patch Management Server) のディレクトリを指定します。ここは、Configuration Server にパッチを送信する前にダウンロードしておく場所です。このパラメータを使用して、パッチ説明ファイルおよびパッチ データ ファイルを格納する代替ディレクトリを設定します。前回の取得時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、このパラメータに別のディレクトリを指定します。デフォルト ロケーションは、*<InstallDir>*¥data¥PatchManager¥patch です。

- **db_type**: データベースのタイプを指定します。指定できる値は、Microsoft SQL Server の **`mssql`** (デフォルト) と Oracle の **`oracle`** の 2 つです。Oracle を使用している場合は、パッチの取得やデータベースの同期を行う前に、この値を **`oracle`** に変更します。このパラメータは Oracle データベースと同期を行うために必須です。
- **dsn**: **データ ソース名 (DSN)** に Patch SQL データベースを指定します。このパラメータは必須です。
- **dsn_user**: DSN で Patch SQL データベースを使用するための SQL ユーザー名を指定します。
- **dsn_pass**: DSN で Patch SQL データベースを使用するための SQL ユーザーのパスワードを指定します。
- **ftp_proxy_pass**: FTP トラフィックにプロキシ サーバーを使用する場合は、パスワードを指定します。
- **ftp_proxy_url**: FTP トラフィックにプロキシ サーバーを使用する場合は、その URL を **ftp://ip:port** の形式で指定します。このマニュアルを作成している時点で、Patch Management は基本認証のみをサポートしています。
- **ftp_proxy_user**: FTP トラフィックにプロキシ サーバーを使用する場合は、ユーザー ID を指定します。
- **history**: 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。HP は、これをコマンド ラインではなく `patch.cfg` ファイルに指定することをお勧めします。history の値が purge_errors より小さい場合、purge_errors は history の値に設定されます。デフォルト値 0 は、パッチ取得の履歴を削除しないことを意味します。
- **http_proxy_pass**: HTTP トラフィックにプロキシ サーバーを使用する場合は、パスワードを指定します。
- **http_proxy_url**: HTTP トラフィックにプロキシ サーバーを使用する場合は、その URL を **http://ip:port** の形式で指定します。このマニュアルを作成している時点で、Patch Management は基本認証のみをサポートしています。
- **http_proxy_user**: HTTP トラフィックにプロキシ サーバーを使用する場合は、ユーザー ID を指定します。
- **http_timeout**: ファイルのダウンロードが完了するまで待機する合計時間を設定します。ある取得セッションが、この時間でファイルをダウンロードできない場合は、現在の HTTP ロケーションを中断し、次の HTTP ロケーションで取得を続行します。ブリテンをダウンロードするために、時間を追加する必要がある場合は、http_timeout を増加します。

このパラメータは、setup.tsp ページに秒単位で表示されます。
http_timeout は、patch.cfg ファイルまたはコマンド ラインでミリ秒単位で指定します。これは、patch.cfg では 3600000 となります。
http_timeout をコマンド ラインで指定する場合は、今回の取得セッションでのみ有効です。

- **lang**: Patch Management は非ダブル バイト言語をサポートします。パッチを取得する言語の省略名を指定します。除外する製品の先頭に感嘆符 (**!**) を付けます。デフォルトは en(英語) です。フランス語と英語を含める場合は、**-lang fr, en** のように指定します。
- **microsoft_sus_url**: Microsoft SUS フィードの URL を指定します。デフォルトは **http://www.msus.windowsupdate.com/msus/v1/aucatalog1.cab** です。
- **nvdm_url**: HP が提供する Patch Update Web サイトに接続するための URL を指定します。これは、patch.cfg の nvdm_url パラメータと同じです。デフォルトは **http://managementsoftware.hp.com/Radia/patch_management/data** です。
- **purge_errors**: 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。HP は、これをコマンド ラインではなく patch.cfg ファイルに指定することをお勧めします。history の値が purge_errors より小さい場合、purge_errors は history の値に設定されます。デフォルトは 7 です。
- **rcs_pass**: お使いの Configuration Server で認証が有効にされている場合、rcs_user のパスワードを指定します。
- **rcs_url**: お使いの Configuration Server のロケーションを URL 形式で指定します。このパラメータは必須です。**radia://***ipaddress***:***port* の形式を使用します。各要素の説明は以下のとおりです。
  - **radia** は Configuration Server で開始されるセッション タイプです。
  - *ipaddress* は Configuration Server をホストするコンピュータのホスト名または IP アドレスです。
  - *port* は Configuration Server のポート番号です。
- **rcs_user**: お使いの Configuration Server で認証が有効にされている場合、rcs_user を指定します。

- **reporting_url**: お使いの Reporting Server の URL を指定します。デフォルトは **http://localhost/reportingserver** です。
- **retire**: 過去化するブリテンをカンマで区切って指定します。以下の場合は -retire パラメータを使用します。
  - 指定したブリテンが Configuration Server Database 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する。
  - retire パラメータで指定したブリテンを、現在のパブリッシュ セッション中に Configuration Server Database にパブリッシュしない。過去オプションはブリテン オプションより優先されます。

  このパラメータは、製品またはリリース レベルではなく、ブリテン レベルで作用します。

  特定のブリテンのみを過去化し、新しいブリテンを取得しない場合は、retire パラメータに次のパラメータを追加します。**-bulletin NONE**

  以下の点に注意してください。
  - コマンド ラインで **retire** オプションを使用するのは、特定のブリテンを Configuration Server Database から削除する場合だけです。ただし、オプションをコマンド ラインで指定すると、過去化されたブリテンの累積リストは保持されません。
  - 過去化したブリテンのリストを `patch.cfg` に設定して、累積リストを維持することをお勧めします。必要に応じて、新しいブリテンを過去化するたびにコマンド ラインに過去化したブリテンのリストを再作成するのではなく、`patch.cfg` にそのリストを追加します。
  - パッチ削除機能が有効で、現在企業で管理されているブリテンを過去化すると、過去化されたセキュリティ パッチは Patch Management エージェント デバイスから削除される場合があります。

  例:**-retire MS00-001,MS00-029**
- **rh_depends**: 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。この設定は、取得設定により、特定の取得に対して上書きできます。

  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 Network からダウンロードするか、Red Hat Linux インストール メディアをコピーした場合はローカルに見つけることができます。Patch Management は、取得時にまず適切なディレクトリで `.rpm` パッケージを検索します。次に例を示します。

— x86 デバイスの 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/patch/redhat/packages/4es` に配置します。

— x86-64 デバイスの 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/patch/redhat/packages/4es-x86_64` に配置します。

— `data/patch/redhat/packages/` サブディレクトリに名前を付ける場合は、『HP Client Automation Core and Satellite Enterprise Edition ユーザー ガイド』(「*設定*」の章の「Red Hat のフィード設定」の項) に掲載されている**OS フィルタのアーキテクチャ**の値の一覧を参照してください。`REDHAT:` の後には、サブディレクトリ名として適切な値を使用してください。

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、インストール メディアの `RedHat/RPMS` ディレクトリの下にあります。

デフォルトは [いいえ] です。

- **rhn_url**: Red Hat Security Network の URL を指定します。デフォルトは **http://xmlrpc.rhn.redhat.com/XMLRPC** です。
- **suse_pass**: :SuSE 9 パッチをホストする Novell Web サイトのパスワードを指定します。
- **suse_urls**: :SuSE パッチをホストする Novell Web サイトの URL を指定します。デフォルトは以下のとおりです。

  9:

  {**https://you.novell.com/update/i386/update/SUSE-CORE/9/**}

  {**https://you.novell.com/update/i386/update/SUSE-SLES/9/**}

  9-x86_64:

  {**https://you.novell.com/update/x86_64/update/SUSE-CORE/9/**}

  {**https://you.novell.com/update/x86_64/update/SUSE-SLES/9/**}
- **suse_user**: SuSE 9 セキュリティ パッチをホストする Novell Web サイトのユーザーを指定します。
- **suse10_pass**: SuSE 10 および SuSE 11 のパッチをホストする Novell Web サイトのパスワードを指定します。

- **suse10_urls**: SuSE 10 および SuSE 11 のパッチをホストする Novell Web サイトの URL を指定します。デフォルトは以下のとおりです。

  10:

  {https://nu.novell.com/repo/$RCE/SLES10-Updates/sles-10-i586}

  {https://nu.novell.com/repo/$RCE/SLED10-Updates/sled-10-i586}

  10SP1:

  {**https://nu.novell.com/repo/$RCE/SLES10-Updates/sles-10-i586**}

  {**https://nu.novell.com/repo/$RCE/SLED10-Updates/sled-10-i586**}

  10SP2:

  {https://nu.novell.com/repo/$RCE/SLES10-SP2-Updates/sles-10-i586}

  {https://nu.novell.com/repo/$RCE/SLED10-SP2-Updates/sled-10-i586}

  10-x86_64:

  {https://nu.novell.com/repo/$RCE/SLES10-Updates/sles-10-x86_64}

  {https://nu.novell.com/repo/$RCE/SLED10-Updates/sled-10-x86_64}

  10SP1-x86_64:

  {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}

  10SP2-x86_64:

  {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}

  10SP3:

  {https://nu.novell.com/repo/$RCE/SLES10-SP3-Updates/sles-10-i586}

  {https://nu.novell.com/repo/$RCE/SLED10-SP3-Updates/sled-10-i586}

10SP3-x86_64:

{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}

11:

{https://nu.novell.com/repo/$RCE/SLES11-Updates/sle-11-i586/}

{https://nu.novell.com/repo/$RCE/SLED11-Updates/sle-11-i586/}

11SP1:

{https://nu.novell.com/repo/$RCE/SLES11-SP1-Updates/sles-11-i586}

{https://nu.novell.com/repo/$RCE/SLED11-SP1-Updates/sled-11-i586}

11-x86_64:

{https://nu.novell.com/repo/$RCE/SLES11-Updates/sle-11-x86_64/}

{https://nu.novell.com/repo/$RCE/SLED11-Updates/sle-11-x86_64/}

11SP1-x86_64:

{https://nu.novell.com/repo/$RCE/SLES11-SP1-Updates/sles-11-x86_64}

{https://nu.novell.com/repo/$RCE/SLED11-SP1-Updates/sled-11-x86_64}

suse10_user: SuSE 10 および SuSE 11 のパッチをホストする Novell Web サイトのユーザーを指定します。

- **sync**: 同期が必要なターゲットを指定します。デフォルトは rcs です。

パッチ取得パラメータ

コマンド ラインからパッチを取得するには

1 Patch Management Server のコマンド プロンプトから、Patch Management のディレクトリに移動します。デフォルトのロケーションは次のとおりです。

<*InstallDir*>¥data¥PatchManager¥

コマンド ラインから作成した取得ファイルを使用することもできます。その場合は、config パラメータを使用します。

2 以下で箇条書きしたパラメータを使用して、次のようなコマンド ラインを作成します。

nvdkit ./modules/patch.tkd acquire -bulletins MS04-*

ここでは、Microsoft Web サイトで MS04-* のフィルタに一致したブリテンのパッチ ファイルのみが取得されます。

コマンド ラインで指定したパラメータは、patch.cfg で指定したパラメータを上書きします。デフォルト パラメータの場合は patch.cfg を使用してください。

- **arch**: パッチを取得するコンピュータ アーキテクチャをカンマで区切って指定します。arch パラメータで有効な値については、『HP Client Automation Core and Satellite Enterprise Edition ユーザー ガイド』の「*設定*」の章に記載されているベンダーのフィード設定を参照してください。
- **bulletins**: 取得するブリテ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。これは、patch.cfg の bulletins パラメータと同じです。Red Hat セキュリティ アドバイザリでは、Red Hat によって発行されたときに Red Hat セキュリティ アドバイザリ番号に含まれるコロン (:) の代わりにハイフン (-) を使用します。
  - Microsoft セキュリティ ブリテンは、命名規則として MS*YY*-### を使用します。ここで、*YY* はブリテ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ンのシーケンス番号です。Microsoft サービス パックは MSSP_*operatingsystem_spnumber* の形式で一覧表示されます。*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 フォルダの情報を使用してダウンロードされます。たとえば、-bulletins MS00-001,MS00-029 と指定します。
  - 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 Client Automation 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 Management には、Red Hat セキュリティ アドバイザリを個別に指定してください。

— SuSE セキュリティ パッチは、命名規則として SUSE-PATCH-#### を使用します。ここで、### は SuSE によって指定されるナンバリング スキームです。

ブリテンをダウンロードしない場合は、–bulletins NONE を使用してください。エージェント更新のみを取得する場合は、この方法で行います。

- **config**: このパラメータは、取得に代替設定ファイルを追加して patch.cfg の設定を上書きする場合に使用します。デフォルトは patch.cfg です。
- **data_dir**: ローカル コンピュータ (Patch Management Server) のディレクトリを指定します。ここは、Configuration Server にパッチを送信する前にダウンロードしておく場所です。このパラメータを使用して、パッチ説明ファイルおよびパッチ データ ファイルを格納する代替ディレクトリを設定します。デフォルトは次のとおりです:
  <*InstallDir*>¥Data¥PatchManager¥data¥patch
- **force**: 次の場合に force (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。

  デフォルトは N です。replace が Y に設定されると、force の値に関係なくブリテンを削除してから再取得します。
- **mode**: 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 BOTH 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、エージェント デバイスの脆弱性を公開するレポートを使用できます。デフォルトは BOTH です。
- **product**: 取得に含める製品を、*vendor*::*product* の形式でカンマで区切って指定します。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。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。

デフォルトでは、次の Microsoft 製品がパッチの取得と管理から除外されます。

```
!Windows 95,!Windows 98*,!Windows
Me,!Access*,!Excel*,!FrontPage 200[023],!FrontPage
9[78],!InfoPath*,!Office*,!OneNote*,!Outlook*,!PowerPoint*,!P
roject 200[023],!Project
98,!Publisher*,!Visio*,!Word*,!Works*
```

次の製品は Patch Management でサポートされないため、除外リストに含まれています: Microsoft Windows 95、Windows 98、Windows Me および SuSE 特有の *-yast2、*-yast2-*、および *-liby2 製品。

除外する製品をコマンド ラインで指定する場合は、製品文字列フィルタ全体を引用符で囲んでください。

- **Replace**: Y に設定すると、bulletins パラメータで指定した古いブリテンを削除してから、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、replace を Y に設定すると、force 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ンは削除されてから再取得されます。デフォルトは N です。
- **superseded_patches**: パッチが置換済みとされている場合でもデータをパブリッシュする場合は、superseded_patches を Y に設定します。デフォルトは N です。
- **vendors**: パッチを取得するベンダーを指定します。例: -vendors Microsoft, RedHat, SuSE, HPUX, SOLARIS。デフォルトは Microsoft です。
- **vendor_os_filter**: ベンダーのオペレーティング システムに *vendor*::*operatingsystem* の形式でフィルタを指定します。x86_64 アーキテクチャの Red Hat および SUSE フィルタは、次の形式を使用します。*vendor*::*operatingsystem*-x86-64

  SUSE 10 フィルタでは、*vendor*::*operatingsystem*SP1-x86-64 のように、オペレーティング システム直後に関連するサービス パック (SP1 または SP2) を指定します。

  — RedHat の例:
  REDHAT::4es,REDHAT::4ws,REDHAT::4as;

  REDHAT::4es-x86_64,REDHAT::4ws-x86_64,

REDHAT::5Server,
REDHAT::5Client,REDHAT::6Server,REDHAT::6Client

REDHAT::5Server-x86_64,
REDHAT::5Client-x86_64,REDHAT::6Server-x86_64,REDHAT::6Client-x86_64

— SuSE の例: SUSE::8, SUSE::9, SUSE::10SP1-x86-64; SUSE::11; SUSE::11-x86_64

— Microsoft のオペレーティング システムは製品として扱われるため、vendor_os_filter の形式を使用しないでください。Microsoft のオペレーティング システムには、代わりに製品フィルタを使用します。

データベース同期パラメータ

データベースをコマンド ラインから同期するには

- Patch Management ディレクトリから以下のコマンド ラインを実行します。

```
nvdkit ./modules/patch.tkd sync -db_type mssql
-dsn patch -dsn_user rpmadmin -dsn_pass rpmdb
-host localhost:3464 -class "*"
```

dsn は必須パラメータです。db_type は、データベース タイプが Oracle の場合は必須パラメータです。

たとえば、SQL Server データベースの PRODUCT クラスだけを更新する場合は、次のように入力します。

```
nvdkit ./modules/patch.tkd sync -dsn PATCH ø
-host localhost:3464 -class "PRODUCT"
```

Oracle データベースの PRODUCT クラスを更新する場合は、次のように入力します。

```
nvdkit ./modules/patch.tkd sync -db_type oracle ø
-dsn PATCH -host localhost:3464   -class "PRODUCT"
```

dsn は PATCH と呼ばれ、Configuration Server はローカル マシンです。

パラメータについては、以下で説明します。

- **db_type**: データベースのタイプを指定します。有効な値は、Microsoft SQL Server の `mssql` と Oracle の `oracle` です。デフォルトは mssql です。Oracle データベースと同期するには、このパラメータ (`-db_type oracle` を指定します。
- **dsn**: データ ソース名 (DSN) に Patch ODBC データベースを指定します。このパラメータは必須です。
- **dsn_user**: DSN で Patch ODBC データベースを使用するためのユーザー名を指定します。
- **dsn_pass**: DSN で Patch ODBC データベースを使用するためのユーザーのパスワードを指定します。
- **host**: お使いの Configuration Server のロケーションを URL 形式で指定します。このパラメータは必須です。`radia://`*`ipaddress`*`:`*`port` の形式を使用します。
  - `radia` は Configuration Server で開始されるセッション タイプです。
  - *`ipaddress`* は Configuration Server をホストするコンピュータのホスト名または IP アドレスです。
  - *`port`* は Configuration Server のポート番号です。
- **class**: Configuration Server と Patch SQL データベースの間で同期するクラスを指定します。たとえば、DEVICE クラスだけを同期する場合は class="DEVICE" を指定します。このパラメータはワイルドカードも使用できます。デフォルトは "*" (すべてのクラスを同期する) です。
- **commit**: Configuration Server Database で検出された変更を SQL データベースに確定する場合は 1 を指定します。変更を自動的に確定しない場合は、0 を指定します。変更内容を表示することができます。デフォルトでは、すべての変更は確定されます。
- **rcs_pass**: お使いの Configuration Server で認証が有効にされている場合、rcs_user のパスワードを指定します。
- **rcs_user**: お使いの Configuration Server で認証が有効にされている場合、rcs_user を指定します。

Patch Agent の更新パラメータ

これらの設定は、Patch Management Agent ファイルのメンテナンス用です。詳細については、『HP Client Automation Core and Satellite Enterprise Edition ユーザー ガイド』(「*操作*」の章の「エージェントの更新を表示」の項) を参照してください。Patch Agent セクションで、以下の設定を行います。

- **agent_updates**: [パブリッシュと配布] を使用して、更新を PATCHMGR ドメインにパブリッシュし、それを DISCOVER_PATCH インスタンスに接続します。このオプションでは、更新が Patch Management 管理対象デバイスに配布されます。更新をパブリッシュするが、配布のために Patch Management 管理対象デバイスに接続しない場合は、Publish だけを使用します。
- **agent_os**: エージェントの更新を取得するオペレーティング システムを指定します。有効な値は、win32、linux および suse です。
- **agent_version**: エージェントの更新を取得する Patch Management 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。

以下のサンプル patch.cfg ファイルを参照してください。パラメータでかっこ (¥{¥}) を使用していることと、ディレクトリ パスをスラッシュ (/) で区切っている点に注意してください。取得で、これらをコマンド ラインから指定する場合は、スペースを含めて値を引用符で囲んでください。

```
patch::init {
AGENT_UPDATES PUBLISH,DISTRIBUTE
ARCH REDHAT::*,SUSE::*,HPUX::*,SOLARIS::*,MICROSOFT::x86
CFG_VER 7.5
DATA_DIR { C:/Program Files/Hewlett-Packard/HPCA/Data/PatchManager/data}
DSN PATCH
DSN_USER sa
FORCE no
FTP_PASS {{AES256}vQP8q3G7N5j4iMhgA2QUuw==}
HTTP_RETRIES 2
LANGUAGE {}
MODE both
MODULE patch
RCS_URL radia://localhost:3464
RCS_USER RAD_MAST
REPLACE no
RETIRE {}
SECTION all
USING_DEFAULT_PATCH_CFG Y
```

```
VENDOR_OS_FILTER {}
}
```

索引

A

acquire コマンド, 25
Architecture タグ, 74
ARCH 属性, 74
arch パラメータ, 94

B

bulletins パラメータ, 94
BULLETIN 属性, 76
Bulletin ノード, 69

C

catexp パラメータ, 61
CHECKSUM 属性, 77
Checksum タグ, 77
config パラメータ, 95
CRC32 属性, 77
CRC32 タグ, 77
CTIME 属性, 71
CVE 列, 52

D

data_dir パラメータ, 87, 95
DATA 属性, 76
DatePosted タグ, 71
DateRevised タグ, 70
db_type パラメータ, 88
Deployment タグ, 71, 76
DesiredState 属性, 62
DISCOVER_PATCH インスタンス, 99
dsn_pass パラメータ, 88
dsn_user パラメータ, 88
dsn パラメータ, 88
DSTATE
    有効な値, 64
DSTATE 属性, 62, 76, 78, 79

F

FAQURL 属性, 70
FAQURL タグ, 70
FILECHG インスタンス, 63
FILECHG クラス, 62
FileChg ノード, 77
FINALIZE_PATCH, 61
force パラメータ, 95
ftp_proxy_pass パラメータ, 88
ftp_proxy_url パラメータ, 88
ftp_proxy_user パラメータ, 88

G

GMTDATE 属性, 77
Gmtdate タグ, 77
GMTTIME 属性, 77
Gmttime タグ, 77

H

hard reboot, 82
history パラメータ, 88
HPFileset ノード, 80
HPPOSTED 属性, 71
HPPosted タグ, 71
HPREVISD 属性, 71
HPRevised タグ, 71
http_proxy_pass パラメータ, 88
http_proxy_url パラメータ, 88
http_proxy_user パラメータ, 88
http_timeout パラメータ, 88

I

ID 属性, 71, 76
ImpactSeverityID タグ, 70
IMPACT 属性, 70
InstallCmdline タグ, 75

L

Language タグ, 74
LANG 属性, 74
lang パラメータ, 89
LOCATION 属性, 76

M

microsoft_sus_url パラメータ, 89
Microsoft MSDE, 50, 52
Microsoft Office ブリテン
  Microsoft Update Catalog の最善実践, 38
  Patch Management での有効化, 40
  検出と管理, 33
  最善実践, 34
Microsoft SQL Server, 50, 52
Microsoft 自動更新, 20
MitigateSeverityID タグ, 70
MITIGATE 属性, 70
mode パラメータ, 95
MSSUSName タグ, 74
MTIME 属性, 71

N

NAME 属性, 71, 72, 73, 77, 78, 80
Name タグ, 71, 72, 73, 77, 78, 80
no reboot, 82
nvdm_url パラメータ, 89

O

ObjectType タグ, 75
OCREATE 属性, 65, 75
ODELETE 属性, 65, 75
OPTIONS インスタンス, 63
OPTIONS クラス, 62
OSSUITE 属性, 75
OSSuite タグ, 75

OSTYPE 属性, 74
OSType タグ, 74
OSVersion タグ, 74
OSVER 属性, 74
OTYPE 属性, 75
OVERIFY 属性, 75

P

PATCHARGS クラス, 65
Patch Manager
  機能
    影響分析, 10
    脆弱性の評価, 10
    適用状況の評価, 10
    配布, 10
    パイロット テスト, 10
  レポート
    パッチ取得
      要約, 28
    簡素化された適用状況
      デバイス別, 50
    脆弱性の評価
      製品別, 53
      適用状況
        パッチ別, 54
        リリース別, 53
    適合性, 48, 58
    適用状況デバイス エラー , 54
    リサーチ, 55
PATCHMGR ドメイン, 17
Patch signature ノード, 77
PATCHSIG 属性, 76
PATCHURL 属性, 74
PatchURL タグ, 74
Patch ノード, 73
PATH 属性, 77, 78
Path タグ, 77, 78
PLATFORM 属性, 70, 75
Platform タグ, 70, 75
PopularitySeverityID タグ, 70
POPULAR 属性, 70
POSTED 属性, 71
PreReqSeverityID タグ, 70
PREREQ 属性, 70
ProbeCmdline タグ, 75
Products ノード, 72
Product ノード, 72
product パラメータ, 95
purge_errors パラメータ, 89

R

radskman, 32
radskman コマンド ライン, 61
rcs_pass パラメータ, 89
rcs_url パラメータ, 89
rcs_user パラメータ, 89
REBOOT 属性, 74
Reboot タグ, 74
Red Hat systemid ファイル、作成する, 24
REGCHG インスタンス, 63
REGCHG クラス, 62
RegChg ノード, 78
Releases ノード, 72

Release ノード, 73
replace パラメータ, 96
reporting_url パラメータ, 90
Reporting Server
パッチ レポートのフィルタリング, 43
REPORT しきい値, 64
REPORT 属性, 76, 78, 79
retire パラメータ, 90
REVISED 属性, 70
rh_depends パラメータ, 90
rhn_register ツール, 24
rhn_url パラメータ, 91
RUNMODE 属性, 71, 76

S

Schema Version タグ, 71
SIZE 属性, 77
Size タグ, 77
soft reboot, 82
SOURCE 属性, 70
Source タグ, 70
SUPERBU 属性, 74
superceded_patches パラメータ, 96
SupercededByBulletin タグ, 74
Superceded タグ, 74
SUPERCED 属性, 74
Supported, 70
Supported タグ, 70
SUPPORT 属性, 70
suse_pass パラメータ, 91
suse_urls パラメータ, 91
suse_user パラメータ, 91
suse10_pass パラメータ, 91
suse10_urls パラメータ, 92
suse10_user パラメータ, 93
SUSNAME 属性, 74
sync パラメータ, 93
systemid ファイル, 24

T

TITLE 属性, 71
Title タグ, 71
TYPE 属性, 70, 79
Type タグ, 70, 79

U

UninstallCmdline タグ, 75
URL 属性, 70
URL タグ, 70
USE 属性, 62, 76, 78, 80

V

VALUE 属性, 78
Value タグ, 78
vendor_os_filter パラメータ, 96
vendors パラメータ, 96
VENDOR 属性, 70
Vendor タグ, 70
VerifyCmdline タグ, 75
VERSION 属性, 77

Version タグ, 77

W

Windows Update Agent, 21

X

XML タグ
    BULLETIN クラス, 70
    FILECHG クラス, 77
    PATCH クラス, 74
    PRODUCT クラス, 72
    REGCHG クラス, 78, 80
    RELEASE クラス, 73

Z

ZSERVICE.REBOOT 属性, 81

あ

赤い X, 49

い

複数の再起動, 85

え

影響分析, 10

か

カスタム XML ファイル、作成する, 62
感嘆符, 49

き

疑問符, 49

け

[警告] 列, 50, 52

さ

再起動
    修飾子, 81, 83
    タイプ, 81, 82
    複数のイベント, 85
再起動の保留中, 49
[再起動の保留] 列, 50, 53
再起動を保留中のデバイスのレポート, 51
サポート, 26

し

自動パッチ、定義, 61
重大なエラーが発生したデバイスのレポート, 54

せ

脆弱性
    管理, 58
    評価, 10
セキュリティ アドバイザリ、定義, 13
説明ファイル、作成する, 25

そ

[その他] 列, 50, 53

た

対話型パッチ、定義, 61

て

データベース
Oracle データベースと同期する, 98
手動で同期する, 97
適合性 (製品別), 53
適合性とリサーチ例外レポート, 57
適合性 (パッチ別), 54
適合性 (ブリテン別) レポート, 51
適合性 (リリース別), 53
適合性レポート, 48
[適用可能な製品] 列, 49
[適用可能なデバイス] 列, 52
[適用可能なブリテン] 列, 49, 53
適用状況の評価, 10

は

配布, 10
パイロット テスト, 10
パッチ
削除, 66
定義, 13
パッチ取得レポート
エラーの要約, 28
セッション別の要約, 28
ブリテン別の要約, 29
パッチ説明ファイル, 17
パッチ探索、実行する, 32
[パッチ適用済み] 列, 49, 52
パッチの分析, 42
パッチのレポート, 42
パッチ未適用ステータス, 49
[パッチ未適用] 列, 50, 52
パッチ レポートのフィルタリング, 43
バンド幅の最適化, 32

ふ

フィルタ バー , 55
ブリテン エラーがあるデバイスのレポート, 51
ブリテン、定義, 13
[ブリテン] 列, 52
フル パッチが適用されていないデバイスのレポート, 50
プローブ、定義, 25

む

虫眼鏡, 49

り

リサーチ レポート, 55
リリースのステータス, 53

れ

レポーティング オプション、カスタマイズする, 63