HP Client Automation Enterprise

Patch Manager

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

インストールおよび設定ガイド

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、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

商標

Adobe® は、Adobe Systems Incorporated の商標です。

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

Linux は、Linus Torvalds の登録商標です。

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

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

ドキュメントの更新

本書のタイトル ページには、次の識別情報が含まれています。

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

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

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

このサイトでは、HP Passport に登録し、サインインする必要があります。HP Passport ID に登録するには、次のサイトにアクセスしてください。

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

または、HP Passport サインインのページの **[New 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。

次の表には、前回のリリース以降に変更された箇所が示されています。

ドキュメントの変更点

章	バージョン	変更点
すべて	7.50	「HPCA Portal の使用」への参照は、Patch Agent を配布するための「HPCA Enterprise Manager の使用」への参照に置き換わりました。 AIX、HP-UX または Solaris デバイスに対するパッチの適用は現在サポートされていません。これらのオペレーティング システムに対するパッチの適用のこれまでのサポートは、このマニュアルから削除されました。
すべて	7.20 2008 年 8 月	このマニュアルの無効なクロスリファレンスが修正されました。
すべて	7.20	大部分の HP Configuration Management バージョン 5.1x 製品の名前が HP Client Automation バージョン 7.20 の名前にブランド変更されました。詳細については、最新のリリース ノートを参照してください。

ドキュメントの変更点

章	バージョン	変更点
1	7.20	22 ページの「このマニュアルの Core Server および Satellite Server での使用」には、新しいトピックが追加されました。
1	7.50	22 ページの「用語」には、Patch Manager ゲートウェイが追加されました。 22 ページの「Patch Manager のコンポーネント」には、HPCA Enterprise Manager のエントリが追加されました。バージョン 7.50 では、Enterprise Manager コンソールを使用して HPCA Agent の一部として Patch Agent を配布したり、パッチ管理ダッシュボードやパッチ レポートを表示したりします。
2	7.50	26 ページの「Microsoft SQL Server または Oracle に対するデータベースの前提条件」では、トピックが変更されました。サポートされる Microsoft SQL Server または Oracle のバージョンについては、付属のリリース ノートのドキュメントにあるデータベース サポート表を参照してください。
2	7.20	26 ページの「Microsoft SQL Server または Oracle に対するデータベースの前提条件」では、Patch Manager データベースのホストとして使用できる Microsoft SQL Server または Oracle のサポートされるバージョンが変更されました。新しくサポートされるデータベースは次のとおりです。 • "SQL Server 2008 • " 最新の Oracle パッチ セットを適用した Oracle 11g リリース 1
2	7.20 2008 年 8 月	28 ページの「Patch Manager 用のデータベースの作成」では、トピックのタイトルが変更されました。また、Oracle を使用してデータベースを作成するときに定義するユーザー プロファイルにロールとシステム権限が追加されました。
2	7.50	27 ページの「実装タスク リスト」では、「HPCA Portal のインストール (オプション)」が「HPCA Enterprise Manager のインストール (オプション)」に置き換わりました。

ドキュメントの変更点

章	バージョン	変更点
2	7.20	「HPCA Patch Manager Server」はブランド変更された Windows サービス名です。
2	7.50	36 ページの「Patch Manager Administrator を使用して、Patch Manager を設定する」には、新しい設定タスク グループ ([環境の設定]、[取得の設定]、および [取得ジョブ]) について説明する新しいトピックが追加されました。
2	7.80	37 ページの「Patch Manager Administrator にアクセスして使用するには」は、**[保存]** ボタンによって変更の保存と適用が両方とも行われることを示すように修正されました。
2	7.50	42 ページの「エージェント オプション」には、Microsoft デバイスにパッチを適用するエージェント オプションを設定するために使用する新しい設定のトピックとパネルが追加されました。オプションには、[Download Manager を有効化]、[自動更新を無効化]、[ソフトウェア配布フォルダの削除] などがあります。
2	7.80	42 ページの「エージェント オプション」には、このページから -mib (インストール済みのブリテンを管理する) オプションを設定するフィールドが追加されました。
2	7.80	43 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。
2	7.80	45 ページの「Patch Agent のエージェント オプション」では mib オプションの説明が明確になり、デフォルトが none に変更されました。
2	7.50	47 ページの「設定」では、[基本] と [詳細] にのみ表示されるフィールドを定義するように変更されました。
2	7.80	47 ページの「設定」では、[インターネット アクセスの許可] フィールドが追加されました。

ドキュメントの変更点

章	バージョン	変更点
2	7.50	49 ページの「ベンダーの設定」では、サポートされなくなった HP-UX および Solaris に関する設定が削除されました。 すべての [ベンダーの設定] ページでは、デフォルトで [基本] フィールドが表示されます。また、[詳細] タブには、ほとんど変更されない設定が表示されます。ベンダーのトピックでは、[基本] と [詳細] のフィールドを区別しません。
2	7.20	50 ページの「Microsoft データ フィード優先化」では、デフォルトの [データ フィード優先化] が [MSSecure、Microsoft Update Catalog、Client Automation] から [Microsoft Update Catalog のみ] に変更されました。このデフォルト 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小限の要件を満たすオペレーティング システムおよび製品である必要があります。
2	7.50	56 ページの「SuSE のフィード設定」には、SuSE バージョン 10 のセキュリティ パッチを取得するために必要なフィード設定が追加されました。SuSE バージョン 10 のサポートでは、SuSE Linux Enterprise Server 10 (SLES10) と SuSE Linux Enterprise Desktop 10 (SLED10) の両方が対象となります。
2	7.50	61 ページの「ログを表示」には、新しいトピックが追加されました。
3	7.50 7.20	「HP-UX パッチの取得について」では、トピックが削除されました。 「HP-UX パッチの取得について」には、次の注意が追加されました。 新しい HP Patch Manager のバージョン 7.20 では HP-UX パッチ取得は使用できません。以前のバージョンの Patch Manager からアップグレードしたユーザーは引き続き以前のバージョンの HP Patch Manager Agent を使用することで HP-UX パッチを取得して管理対象デバイスに配布できます。

ドキュメントの変更点

章	バージョン	変更点
3	7.50	75 ページの「SuSE パッチの取得要件」では、トピックが変更されました。SuSE 10 のパッチおよびアップデートにアクセスするには、Novell からミラー認証情報 (ユーザー名とパスワード) を取得する必要があります。
3	7.80	75 ページの「SuSE パッチの取得要件」では、トピックが変更されました。SuSE 10 以上のパッチおよびアップデートにアクセスするには、Novell からミラー認証情報 (ユーザー名とパスワード) を取得する必要があります。 77 ページの「SuSE 10 および SuSE 11 の登録要件」には、SuSE 10 および SuSE 11 のオペレーティング システムを実行しているデバイスの Novell のライセンスおよび登録に関するポリシーをユーザーにアドバイスするための新しいトピックが追加されました。
3	7.80	78 ページの「取得ジョブの設定」では、[ブリテン] フィールドの説明が修正され、SuSE 9、10、11 のブリテンに必要となる形式について説明されています。SuSE ブリテンのファイル名のカンマをハイフンで入力する必要があることに注意してください。
3	7.80	81 ページの「Microsoft の設定」は修正され、新しい置き換えオプションが追加されました。
3	7.80	87 ページの「mib (Manage Installed Bulletins) オプションの設定」では mib オプションの説明が明確になり、デフォルトが none に変更されました。
3	7.50	88 ページの「パッチ取得レポート」では、レポートのイメージが更新されました。
4	7.50	以前のトピック「Patch Manager Agent を Portal からインストールするには」は 94 ページの「Patch Manager Agent を HPCA Enterprise Manager からインストールするには」に置き換わりました。

ドキュメントの変更点

章	バージョン	変更点
4	7.50	95 ページの「Patch Manager Agent を Linux オペレーティング システムにインストールするには」には、x86 (32 ビット) アーキテクチャおよび x86-64 (AMD64 と Intel EM64T) アーキテクチャの SuSE Linux Enterprise Server (SLES)、SuSE Linux Desktop Server (SLED) バージョン 10、10 SP1、10 SP2 上で使用する Linux Agent のサポートが追加されました。
4	7.50	111 ページの「パッチの分析とレポート」では、新しいトピックや新しいレポートが追加され、レポート コンテンツとイメージが変更されました。 • 114 ページの「詳細な情報への掘り下げ」には、新しいトピックが追加されました。 • 116 ページの「概要」は、このリリースで新たに追加されました。4 つのレポート (円グラフまたは棒グラフ) には、使用環境のパッチ適用状況ステータスの概要が表示されます。また、適用状況レポートのテーブルを掘り下げて詳細を表示できます。 • 120 ページの「パッチ適合性レポート」では、レポート、イメージ、およびコンテンツが変更されました。 • 130 ページの「リサーチ レポート」では、一部のレポートのイメージが更新されました。
4	7.80	118 ページの「デバイスのステータス」には、デバイスごとにパッチ適用状況のパーセンテージを示す適用状況ステータスのグラフィカル レポートが追加されました。
4	7.80	132 ページの「リサーチ (デバイス別)」には、MSI インストーラ バージョン、WUA バージョン、WUA ステータスの列が追加されました。
4	7.80	137 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」は、HP が SuSE ブリテン名を変更し、短い固有のインスタンス名を CSDB 用に作成する方法について説明する新しいトピックです。
付録 D	7.50	173 ページの「Patch.cfg のパラメータ」には、SuSE Linux Enterprise Server バージョン 10 および SuSE Linux Desktop Server バージョン 10 のパラメータが追加されました。

ドキュメントの変更点

章	バージョン	変更点
付録 D	7.80	173 ページの「Patch.cfg のパラメータ」では SuSE パラメータが修正され、SUSE Linux Enterprise Server および SUSE Linux Enterprise Desktop バージョン 11 のサポートが組み込まれました。
第 2 章および付録 D	7.90	SuSE 10 SP 3 のサポート
3	7.90	Redhat の取得が、取得の概要レポートで個別に表示されるようになりました。

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

ほとんどのサポート エリアでは、HP Passport ユーザーとして登録してサインインする必要があります。多くの場合は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

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

この章は以下を目的としています。

- HP Client Automation Enterprise Patch Manager (Patch Manager) の機能を理解する。トピックには次の内容が含まれます。
  - 20 ページの「HP Client Automation Patch Manager」
  - 22 ページの「このマニュアルの Core Server および Satellite Server での使用」
  - 22 ページの「用語」
  - 22 ページの「Patch Manager のコンポーネント」

HP Client Automation Patch Manager

HP Client Automation Patch Manager (Patch Manager) 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。Patch Manager は、完全なスタンドアロン ソリューションとして提供され、HP Client Automation Enterprise Suite (HPCAE Suite) に完全に統合されたコンポーネントとして使用できます。HPCAE Suite は、企業全体のすべてのソフトウェアに対して、自動化され、継続的な設定管理を提供し、ソフトウェア インフラストラクチャ全体が常に要求ステート、つまり、最新で、信頼性があり、セキュアな状態であるようにします。

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。

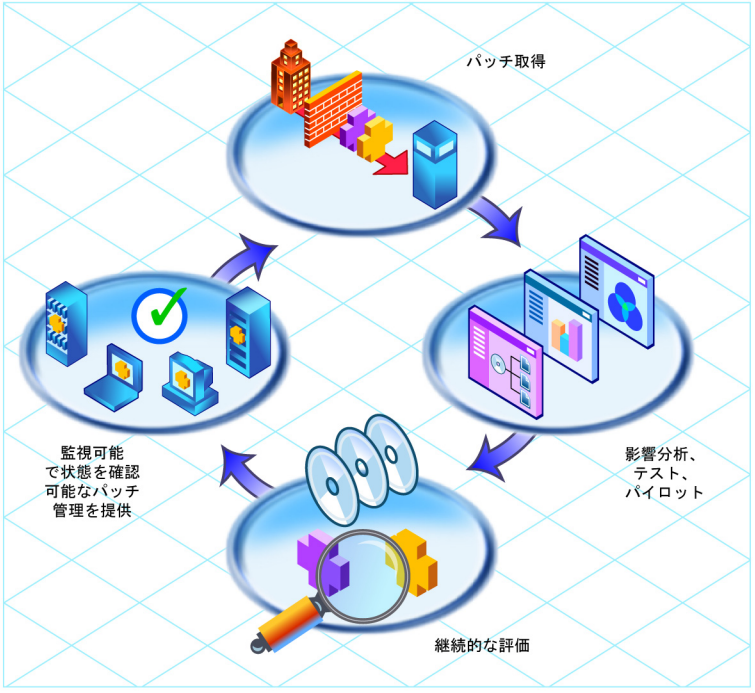
  > このリリースには、HP-UX および Sun Solaris (Sparc) に関するセキュリティ ブリテン (アドバイザリ) の取得に対するサポートは含まれていません。HP-UX または Sun Solaris エージェント デバイスの管理は、今後サポートされません。

- **パイロット テスト :**
  また、Patch Manager では、使用状況や重要度に応じて、IT 管理者が対象のパイロット グループを選択できます。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一意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



このマニュアルの Core Server および Satellite Server での使用

お使いの環境で、Core Server と Satellite Server を使用している場合、まず『HPCA Core および Satellite 入門およびコンセプト ガイド』をお読みください。このガイドのインストール、設定、およびトラブルシューティングに関する情報は、本ガイドの情報より優先されます。

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。

Patch Manager のコンポーネント

Patch Manager は、Patch Manager Server だけでなく、HP Client Automation (HPCA) インフラストラクチャの既存のコンポーネントも使用します。次の HPCA コンポーネントが必要です。

- **Configuration Server**
  アプリケーションおよびサブスクライバやデバイスに関する情報は、HP Client Automation Configuration Server (Configuration Server) の Configuration Server Database (CSDB) に格納されます。CSDB の PATCHMGR ドメインに

は、パッチ管理用のインスタンスが含まれます。Configuration Server は、Patch Manager Agent から受信した情報を処理します。Configuration Server は、管理者によって作成されたポリシーに基づいて脆弱性を管理します。詳細については、『HPCA Configuration Server ガイド』を参照してください。

- **Enterprise Manager**
  Patch Manager Agent を HPCA Agent の一部として配布し、Patch Manager ダッシュボードまたはレポートを表示するには、HP Client Automation Enterprise Manager (Enterprise Manager) を使用します。詳細については『HPCA Enterprise Manager ユーザー ガイド (Enterprise Manager ガイド)』を参照してください。

- **パッチ ゲートウェイ**
  パッチ ゲートウェイは Patch Manager Server のコンポーネントで、HPCA Core Server 上のメタデータを使用して、軽量のパッチ配布をサポートします。ゲートウェイでは、エージェントからのリクエストでパッチ バイナリ データがダウンロードされ、他のエージェントが使用できるようにキャッシュされます。詳細については『HPCA Core および Satellite Enterprise ユーザー ガイド』を参照してください。

- Patch Manager Server
  Patch Manager Server は、インターネットでセキュリティ パッチを取得し、それらを CSDB にロードしてから、Patch Manager 用 SQL または Oracle データベースと同期させます。パッチおよびお使いの環境の脆弱性に関する情報は、Patch Manager レポートを使用して分析できます。Patch Manager は、HPCA Patch Manager Server という独自のサービス名で実行されます。

- **Patch Manager Agent**
  脆弱性を管理するデバイスに Patch Manager Agent をインストールします。エージェントは、デバイス上で管理対象の製品とパッチを検出します。

- **Reporting Server**
  Client Automation 拡張インフラストラクチャの一部として、Web ベースの HP Client Automation Reporting Server (Reporting Server) を使用すると、組み合わされたデータのクエリを既存の HP Client Automation SQL データベースで行ったり、詳細なレポートを作成したりできます。また、既存の LDAP ディレクトリをマウントすることもできます。LDAP ディレクトリをマウントすることによって、LDAP ディレクトリ レベルを使用してデータにフィルタを適用できます。Reporting Server のインターフェイスでは、レポートの作成や全体的な環境の評価を行うために SQL データをダイナミックかつ直感的に使用できるようになっています。詳細については、『*HP Client Automation Reporting Server Installation and Configuration Guide (HPCA Reporting Server Guide)*』を参照してください。

- **Administrator CSDB Editor**
  HP Client Automation Administrator CSDB Editor (CSDB Editor) は、経験豊富な管理者に、Configuration Server Database に格納されるサービス エンタイトルメント ポリシーを表示または編集するユーザー インターフェイスを提供します。詳細については、『HP Client Automation 管理者ユーザー ガイド』を参照してください。

2 Patch Manager 環境の作成

この章は以下を目的としています。

- HP Client Automation Enterprise Patch Manager (Patch Manager) 環境を設定するために必要なタスクを理解する。
- Configuration Server および Configuration Server Database を変更する方法を理解する。
- Patch Manager をインストールできるようになる。
- Patch Manager Administrator コンソールにアクセスして使用し、次の作業を行えるようになる。
  - 設定タスク
  - 取得および操作
  - ステータスとログの表示
  - オンライン ヘルプ

お使いの環境で、Core Server および Satellite Server を使用している場合、まず『Core および Satellite Server 入門およびコンセプト ガイド』を読んでください。このガイドのインストール、設定、およびトラブルシューティングに関する情報は、本ガイドの情報より優先されます。

Patch Manager の実装タスク

Patch Manager の環境を設定する前に、最新バージョンの Configuration Server と、Microsoft SQL Server または Oracle をインストールしておく必要があります。

Microsoft SQL Server または Oracle に対するデータベースの前提条件

Patch Manager データベースには Microsoft SQL Server または Oracle が必要です。

- 付属の *リリース ノート*のデータベース サーバーに関するトピックに一覧表示されている Microsoft SQL Server または Oracle のサポートされるバージョンのいずれかをインストールして使用します。
- Oracle を使用している場合、Microsoft が提供する Oracle ODBC ドライバではなく、お使いの環境の Oracle バージョンに正しく対応した Oracle 社の ODBC ドライバを使用する必要があります。
- Oracle を使用している場合、HP は、データベース サーバー、Oracle クライアント、および Oracle ODBC ドライバが、すべて最新のパッチ セット レベルであることを確認することもお勧めします。次の手順を使用して、お使いの環境の Oracle バージョンを確認します。

Oracle データベースのバージョンを確認するには

- Web ベースの Oracle Enterprise Manager の場合 : **[ホーム]** タブにアクセスし、**[バージョン]** の横の **[全般]** セクションを探します。
- Oracle Enterprise Manager コンソールの場合 : ツリーでデータベース サーバーを選択し、**[インスタンス] → [設定] → [全般]** タブを選択します。バージョンは、**[DB のバージョン]** の横に表示されます。
- SQL*Plus の場合 : データベース サーバーにログインします。ログイン時のバナーにバージョンが表示されない場合は **`SELECT * FROM V$VERSION`** コマンドを発行します。

Oracle クライアントのバージョンを確認するには

- SQL*Plus の場合 : データベース サーバーにログインすると、ウィンドウの上部にバージョンが表示されます。次に例を示します。

```
SQL*Plus: Release 9.2.0.8.0 - Production on Tue Jan 8
12:10:232008
```

- Windows エクスプローラの場合：ORACLE_HOME\bin（例：C:\Oracle\Ora92\bin）に移動して、oci.dll を右クリックします。**[プロパティ] → [バージョン]** タブをクリックし、**[項目名]** リスト ボックスを使用して、**[ファイルのバージョン]** を選択します。

Oracle ODBC ドライバのバージョンを確認するには

- ODBC Data Source Administrator の場合：ODBC Data Source Administrator（odbcad32.exe）を開き、**[ドライバ]** タブを選択して、「Oracle in OraHome92」などにスクロールします。バージョンは、[バージョン] カラムに表示されます。
- Windows エクスプローラの場合：ORACLE_HOME\bin（例：C:\Oracle\Ora92\bin）に移動して、SQORA32.DLL を右クリックします。**[プロパティ]** ①↗ **[バージョン]** タブをクリックし、**[項目名]** リスト ボックスで **[ファイルのバージョン]** を選択します。

実装タスク リスト

Patch Manager を使用するには、以下のタスクを完了する必要があります。

- SQL または Oracle パッチ データベースおよび ODBC DSN を作成します。
- 最新バージョンの Configuration Server をインストールします。『Client Automation Getting Started Guide』を参照してください。
- Configuration Server に Messaging Server をインストールします。『HPCA Messaging Server Installation and Configuration Guide』を参照してください。
- Administrator CSDB Editor をインストールします。『HP Client Automation 管理者ユーザー ガイド』を参照してください。
- Patch Manager のインストールを実行します。このインストールには、以下のタスクが含まれます。
  - Patch Manager Server のインストール
  - Patch Manager で必要な Configuration Server コンポーネントの更新のインストール
  - Patch Manager で必要な Configuration Server Database (CSDB) の更新のインストール
  - 自社で使用する Patch Manager のオプションの設定
  - CSDB の SQL または Oracle データベースとの同期
- CSDB へのメソッド接続の追加

- Enterprise Manager のインストール (オプション)。『HPCA Enterprise Manager ユーザー ガイド』を参照してください。
- Reporting Server のインストール。『*HPCA Reporting Server Installation and Configuration Guide*』を参照してください。

Patch Manager 用のデータベースの作成

Patch Manager をインストールする前に、Microsoft SQL Server または Oracle を使用してデータベースを作成します。データベースを作成するセキュリティ権限を持たない場合は、データベースの管理者に連絡してください。

必要なサイズは、お使いの環境でのパッチおよび管理対象デバイスの数に応じて変わります。以下の手順は、単に推奨事項を反映したものです。

Patch Manager 用 SQL Server データベースを作成するには

1 Microsoft SQL Server 上で、次の推奨設定のデータベースを作成します。

[全般] タブ	名前: 空白またはアンダースコアを含まない任意の名前 (**PATCH** など)
[データ ファイル] タブ	初期サイズ : 500 MB 20 % ずつの自動拡張を選択
[トランザクション ログ] タブ	初期サイズの変更 : 100 MB

2 SQL Server 認証を使用します。

3 デフォルトのデータベースを手順 1 で使用したデータベース名に変更します。

SQL Server 名、admin ユーザーの ID およびパスワードが、HPCA のインストール中に必要となります。

Windows 認証を使用している場合、データベースのオーナー名は **sa** にはできません。

4 Patch Manager Server をホストするコンピュータで、任意の名前 (**PATCHMGR** など) で ODBC DSN を作成し、SQL Server 上で新しい PATCH データベースに対して指定します。

ODBC DSN の作成方法が不明な場合は、SQL Server データベースの管理者に問い合わせてください。

Microsoft Data Access Components (MDAC) を、お使いの Patch Manager Server にインストールします。それを、Microsoft の Web サイトからダウンロードします。最低限必要なバージョンは MDAC 2.8 です。

Patch Manager 用 Oracle データベースを作成するには

お使いの Oracle サーバー ODBC ドライバと Core Server が完全に一致していることをご確認ください。ODBC ドライバ バージョンが一致していない場合、Oracle データベースへの接続に失敗することがあります。

詳細については、Oracle データベースの管理者にお問い合わせください。

1 Oracle サーバー上に、次の推奨設定の表領域を作成します。

表領域名	任意の名前 (**PATCHDATA** など)
ステータス	オンライン
タイプ	永続
データファイル	データファイルのフルパスと名前 (patchdata.dbf など)
ストレージ	最小サイズは 200 MB で、上限なし
エクステント管理	自動割り当てでローカルに管理
セグメント領域の管理	自動
ロギングを有効化	いいえ

2 次の推奨設定で一時的な表領域を作成します。

表領域名	任意の名前 (**PATCHTEMP** など)
ステータス	オンライン
タイプ	一時
データファイル	データファイルのフルパスと名前 (patchtemp.dbf など)
ストレージ	サイズ 1000 MB

表領域名	任意の名前 (**PATCHTEMP** など)
エクステント管理	自動割り当てでローカルに管理
セグメント領域の管理	自動
ロギングを有効化	いいえ

3 ユーザーを作成し、データと一時表領域をデフォルト プロファイルを持つユーザーに関連付けます。

ユーザー名	任意の名前 (**PATCH** など)
パスワード	自社のセキュリティに関する推奨事項に基づいて作成
デフォルト表領域	PATCHDATA
一時表領域	PATCHTEMP
プロファイル	このスキーマでは DEFAULT または PROFILE NAME を使用
ロール	CONNECT および RESOURCE
システム権限	CREATE ANY VIEW SELECT ANY TABLE UNLIMTED TABLESPACE UPDATE ANY TABLE

4 Configuration Server および Messaging Server をホストするコンピュータで、任意の名前 (**PATCHMGR** など) で ODBC DSN を作成し、Oracle サーバーで新しい PATCH データベースを参照するようにします。

ODBC DSN の作成方法が不明な場合は、Oracle データベースの管理者に問い合わせてください。

これでデータベースが接続されました。

Administrator のインストール

Configuration Server のメディアには、Administrator インストールが含まれます。Administrator コンポーネントのインストールおよび CSDB Editor の使用法については、『HP Client Automation 管理者ユーザー ガイド』を参照してください。

Patch Manager Server のインストール

システム要件

- Patch Manager Server として動作するコンピュータを特定します。このコンピュータは、Configuration Server、お使いの ODBC サーバー、およびインターネットと通信できる必要があります。Patch Manager Server は、付属の *HP Client Automation バージョン 7.50 リリース ノート*で特定されている Windows Server バージョンのいずれかを実行しているコンピュータにインストールできます。

  Configuration Server コンポーネントおよび Configuration Server DB の更新をインストールするには、Configuration Server コンピュータで Patch Manager インストール プログラムを実行する必要があります。これらは、ネットワーク接続ではインストールできません。

- Patch Manager Server で必要な Microsoft Data Access Components (MDAC) の最小バージョンは、2.8 です。
- パッチ データベースに Oracle を使用している場合、Microsoft が提供する Oracle ODBC ドライバではなく、お使いの環境の Oracle バージョンに正しく対応した Oracle 社の ODBC ドライバを使用する必要があります。

インストール

バージョン 5.10 では、Patch Manager は、別の HP Client Automation (HPCA) インフラストラクチャ コンポーネントやサービスをホストしていないパスにインストールする必要があります。たとえば、Patch Manager を別の HPCA コンポーネントをすでにホストしている共通の Integration Server フォルダにインストールすることはできません。

デフォルトの Patch Manager サービス名、およびデフォルトのポートおよびインストール ディレクトリは以下のとおりです。

- サービス名 : `httpd-patchmanager`
- サービスの簡略名 : `Patch Manager Server`
- デフォルト ポート : `3467`
- デフォルト インストール ディレクトリ : `C:\Program Files\Hewlett-Packard\CM\PatchManager`

ポートおよびインストール パスはインストール時に変更できます。

移行の詳細およびオプションについては、Patch Manager メディアの `\Migration` フォルダにある『HPCA Patch Manager 移行ガイド』を参照してください。

Patch Manager Server のコンポーネントをインストールするには

1. Client Automation バージョン 7.50 インストール メディアの Patch Manager フォルダにアクセスします。
2. `\extended_infrastructure\patch_manager_server\win32` ディレクトリに移動し、**setup.exe** をダブルクリックします。

   [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。[HP Software License Terms] 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。[新規インストール]/[移行] ウィンドウが表示されます。
5. これが Patch Manager の新規インストールの場合は、**[新規インストール]** を選択します。以前の Patch Manager バージョンから移行する場合は、**[移行]** を選択します。完全な移行方法については、Patch Manager メディアの `\Migration` ディレクトリを参照してください。

   移行の場合は、続ける前に必ず移行方法を参照してください。

   [インストールするコンポーネントを選択] ウィンドウが表示されます。

6 インストールするコンポーネントを選択します。初めて Patch Manager のインストールを実行する場合は、すべてのオプションを選択する必要があります。

— Patch Manager Server
HPCA Integration Server の実行可能ファイル `nvdkit` および `httpd.tkd` を含む Patch Manager Server をインストールします。

— **Configuration Server コンポーネントの更新**
Configuration Server Database の更新

Patch Manager 7.50 の機能を使用する場合は、**[Configuration Server Database の更新]** を選択する必要があります。PATCHMGR ドメインだけが置換され、そのドメインのすべてのデータが削除されます。

Patch Manager のインストールで、Configuration Server コンポーネントの更新と Configuration Server DB の更新は、Configuration Server コンピュータでのみ実行されます。これらは、ネットワーク接続ではインストールできません。

また、Configuration Server Database の更新を適用した後、お使いの Configuration Server Database 内の PATCHOBJ インスタンスに正しい接続が含まれることも確認します。78 ページの「Configuration Server Database の PATCHOBJ インスタンスの内容の検証」を参照してください。

選択を行ったら **[次へ]** をクリックします。[警告] ウィンドウが表示されます。

7 [警告] ウィンドウで **[次へ]** をクリックします。[インストール フォルダ] ウィンドウが表示されます。

8 Configuration Server がインストールされているロケーションを入力するか、**[ブラウズ]** をクリックしてそのロケーションに移動します。

Patch Manager Server をインストールするロケーションを入力するか、**[ブラウズ]** をクリックしてそのロケーションに移動します。

可能であれば、デフォルトの Patch Manager Server ディレクトリを使用します。

Patch Manager Server は、他の HPCA コンポーネントをホストするディレクトリにはインストールできません。Patch Manager Server は、独自のディレクトリにインストールする必要があります。

9 **[次へ]** をクリックします。

10 続行する場合は、**[OK]** をクリックしてディレクトリの内容を更新します。

ライセンス ファイルのロケーションを指定するウィンドウが表示されます。

11 ライセンス ファイルのロケーションを入力するか、**[ブラウズ]** をクリックしてそのライセンス ファイルに移動します。

12 **[次へ]** をクリックします。[HTTP サーバーの IP アドレス] ウィンドウが表示されます。

HTTP サーバーの IP アドレスは、インストールの直後に [Client Automation Patch Administrator] ページを表示するために使用されます。

13 Patch Manager Server の IP アドレスを入力し、**[次へ]** をクリックします。

[HTTP サーバーのポート] ウィンドウが表示されます。

14 HTTP サーバーのポートとして、デフォルトを使用するか、Patch Manager Server で使用できるポート番号を入力して、**[次へ]** をクリックします。

ポートが使用できるかどうかが確認されます。

選択したポートが使用できない場合は、[検証に失敗しました] ダイアログに警告が表示されます。**[OK]** をクリックして、別のポート番号を選択します。

FINALIZE_PATCH サービスのウィンドウが表示されます。

15 すべての Agent が PATCHMGR.ZSERVICE.FINALIZE_PATCH サービスを使用するための要件を確認し、**[次へ]** をクリックします。

Agent が FINALIZE_PATCH サービスを使用できるようにする方法の詳細については、78 ページの「FINALIZE_PATCH サービスの使用許可」を参照してください。

[要約] ウィンドウが表示されます。

16 要約の画面を確認して **[インストール]** をクリックします。

表示されるすべての警告ダイアログを読んで、応答します。表示されるダイアログ ボックスは設定によって異なります。

17 **[完了]** をクリックします。

これで、Configuration Server とそのデータベースが更新され、Patch Manager Server バージョン 7.50 がインストールされました。

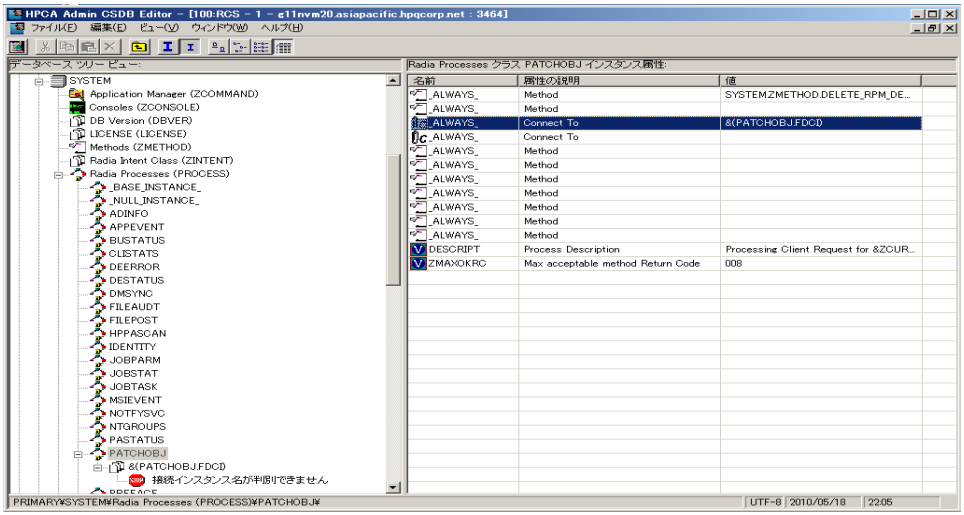
最終的な設定およびデータベースの同期を行う場合は、**[Client Automation Patch Administrator]** ページに移動します。移動しない場合は、Web ブラウザを開いて、**http://<*patchserveripaddress*>:<*port*>/patch/manage/admin.tsp** に移動して Patch Manager の設定を完了し、データベースの同期を実行します。

Configuration Server Database の PATCHOBJ インスタンスの内容の検証

Patch Manager の Configuration Server Database コンポーネントを更新した後、Administrator CSDB Editor を使用して Configuration Server Database の PRIMARY.SYSTEM.PROCESS.PATCHOBJ インスタンスの内容を検証します。

PRIMARY.SYSTEM.PROCESS.PATCHOBJ インスタンスを表示し、**&(PATCHOBJ).FDCI** の値を検索します。これは、_ALWAYS_ Connect To 属性として定義されており、次のように表示されます。

下の図は、&(PATCHOBJ).FDCI に必要な接続タイプを示しています。



&(PATCHOBJ).FDCI が _ALWAYS_ Method 属性の隣にある場合は、次のように表示されます。

&(PATCHOBJ).FDCI の値をコピーして _ALWAYS_ Connect To 属性に貼り付け、_ALWAYS_ Method 属性からその値を削除します。

属性値は大文字にする必要があります。

PRIMARY.SYSTEM.PROCESS のクラス定義の最初の 3 行を、HP が提供するデフォルトのものからカスタマイズすると、不正な接続タイプが発生する場合があります。

Patch Manager Administrator を使用して、Patch Manager を設定する

HP Client Automation Patch Manager Administrator (Patch Manager Administrator) には、**[設定]** 領域があり、Patch Manager Server 設定ファイル、`patch.cfg` のインターフェイスとなっています。

[設定] 領域は、次の 3 つの領域にグループ化されています。

- 次の情報を入力するには、**[環境の設定]** を展開します。
  - 78 ページの「インフラストラクチャの設定」
    Configuration Server と Patch ODBC DSN、Reporting Server と外部 HP Patch 更新サイトとの接続の定義およびテストに使用します。
  - 78 ページの「プロキシ設定」
    HTTP または FTP プロキシ サーバーの定義に使用します。
  - 78 ページの「エージェント オプション」
    Microsoft 管理対象デバイス用 Patch Agent のオプションの設定に使用します。[Download Manager を有効化]、[自動更新を無効化]、[ソフトウェア配布フォルダの削除]、および -mib (インストール済みのブリテンを管理する) オプションがあります。
- 次の事項を指定するには、**[取得の設定]** を展開します。
  - 78 ページの「設定」
  - 78 ページの「設定」
  - 78 ページの「ベンダーの設定」
- ベンダーのブリテンを取得するジョブを定義するには、**[取得ジョブ]** をクリックします。78 ページの「取得ジョブの設定」を参照してください。

これらの設定を入力または変更するには、Patch Manager Administrator を使用します。

Patch Manager Administrator にアクセスして使用するには

1 ご使用の Web ブラウザから、**http://***patchserver_ip_address***:***port***/patch/manage/admin.tsp** に移動します。

2 [設定] 領域の設定および入力または変更するパラメータの値を、入力または選択します。最後にアスタリスク (*) のある設定は必須です。使用できる設定の詳細については、以降の [設定の設定] の情報を参照してください。

3 **[保存]** をクリックして、Patch Manager Server の設定変更を保存して適用します。このアクションの実行時に、Patch Manager Server は新しい設定を使用して初期化されます。初期化時には、Patch Manager は ODBC DSN 設定で指定された DSN 名との接続を確立します。情報が最新であるためには、この接続が取得や同期を行う前に確立されている必要があります。

Patch Manager Administrator オンライン ヘルプを使用するには

Patch Manager Administrator 全体で、状況に応じたオンライン ヘルプを利用できます。

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

オンライン ヘルプ ウィンドウでは、次のボタンを使用して必要な情報を検索できます。

表 1　　オンライン ヘルプ ナビゲーション ツール

ボタン	説明
	目次パネルを表示し、目次内の現在のトピックの場所を強調表示します。
	目次のトピックを 1 つ「上に」移動します。
	目次のトピックを 1 つ「下に」移動します。
	現在表示されているヘルプ トピックを印刷します。

表 1　　オンライン ヘルプ ナビゲーション ツール

ボタン	説明
目次	目次を表示します。
索引	ヘルプ トピックのアルファベット順の索引を表示します。
検索	キーワードまたはフレーズに対応する、すべてのオンライン ヘルプ トピックを検索します。

インフラストラクチャの設定

[環境の設定] グループ > **[インフラストラクチャの設定]** ページを使用して、HP Client Automation コンポーネントのパラメータを設定します。設定では、HP Configuration Server、データソース名 (DSN)、HP Patch Manager 更新サイト、および HP Client Automation Reporting Server のエイリアスを指定する必要があります。可能な場合は、インストールのデフォルト値が表示されます。

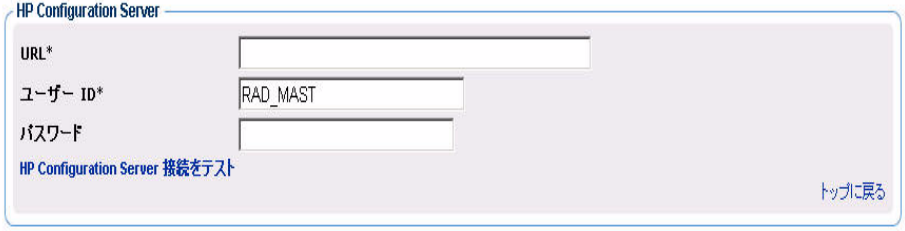
HP Configuration Server の設定

[HP Configuration Server] セクションでは、以下の設定を行います。**[詳細]** タブをクリックして、[詳細] にのみ表示されるフィールドを表示します。

[基本] と [詳細] のフィールド

- **URL**: `radia://ipaddress` または `hostname:port` の形式を使用して、Configuration Server の場所を指定します。
- **ユーザー ID**: Configuration Server にアクセスするための管理ユーザー ID を指定します。
- **パスワード**: お使いの Configuration Server でパスワード認証が有効にされている場合は、ユーザー ID に対してパスワードを指定します。
- **HP Configuration Server 接続をテスト**: Patch Manager Administrator から Configuration Server 接続をテストできます。接続をテストするには、**[HP Configuration Server 接続をテスト]** をクリックします。プロンプト画面が表示されたら、**[接続をテスト]** をクリックします。結果を待ちます。テスト ペー

ジで指定した値が元の値と異なり、テストが正常に終了した場合は、**[変更を適用]** をクリックして新しい値を [設定] ページにコピーします。新しい設定値が保存され、Patch Manager Server に適用されます。



ODBC DSN の設定

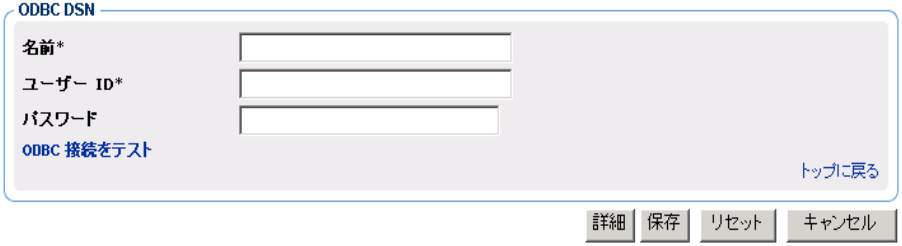
[ODBC DSN] セクションで、以下の設定を行います。

- **名前** *: Patch Manager SQL または Oracle データベースにデータ ソース名 (DSN) を指定します。
- **ユーザー ID***: Patch Manager ODBC データベースの DSN のユーザーを指定します。
- **パスワード** : Patch Manager ODBC データベースのユーザー ID にパスワードを指定します。
- **データベースのタイプ** : データベースのタイプを指定します。これは、`patch.cfg` の db_type パラメータと同じです。指定できる値は、Microsoft SQL Server の `mssql` と Oracle の `oracle` の 2 つです。mssql は、新規インストールの場合のデフォルト値です。

  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。

- **ODBC 接続をテスト** : Patch Administrator の ODBC 接続をテストできます。接続をテストするには、**[ODBC 接続をテスト]** をクリックします。プロンプト画面が表示されたら、**[接続をテスト]** をクリックします。結果を待ちま

す。テスト ページで指定した値が元の値と異なり、テストが正常に終了した場合は、**[変更を適用]** をクリックして新しい値を [設定] ページにコピーします。新しい設定値が保存され、Patch Manager Server に適用されます。



[詳細] にのみ表示されるフィールド

HP Patch Manager 更新サイト、および HP Client Automation Reporting Server 設定のエントリを表示するには、[詳細] タブをクリックします。

HP Patch Manager 更新サイト

[HP Patch Manager 更新サイト] セクションで、次の設定を行います。

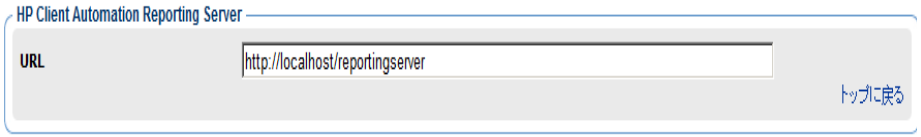
- URL*: HP が提供する HP Patch Manager 更新 Web サイトに接続するための URL を指定します。デフォルトは **http://managementsoftware.hp.com/Radia/patch_management/data** です。

  これについては、インストール時のデフォルト値を変更する必要はありません。

HP Client Automation Reporting Server 設定

この設定は、HP Client Automation (HPCA) Reporting Server の URL ロケーション (エイリアス) を指定します。[Patch Manager Administrator] ページのツールバー領域で [レポート] アイコンをクリックして、パッチ レポートの表示に使用される Reporting Server にアクセスします。

- URL: Patch Manager に使用する Reporting Server の場所を指定します。



プロキシ設定

企業の HTTP プロキシと FTP プロキシを設定するには、[プロキシ設定] ページを使用します。

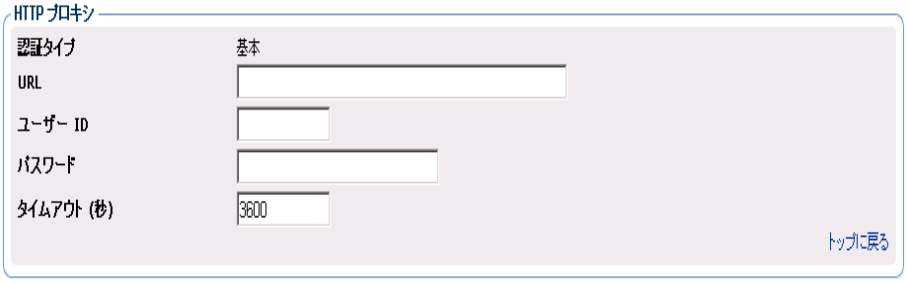
Patch Manager Administrator から [プロキシ設定] ページにアクセスするには、**[設定]** 領域で **[環境の設定]** を展開し、**[プロキシ設定]** をクリックします。

HTTP プロキシの設定

[HTTP プロキシ] 設定セクションで、以下の設定を行います。

- **認証タイプ** : 基本 このパラメータは設定できません。
- **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。
- **ユーザー ID**: http トラフィックにプロキシ サーバーを使用し、プロキシが認証の認証情報を必要とする場合は、ユーザー ID を指定します。
- **パスワード** : http トラフィックにプロキシ サーバーを使用し、プロキシが認証の認証情報を必要とする場合は、パスワードを指定します。
- **タイムアウト (秒)**: ファイルがすべてダウンロードされ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

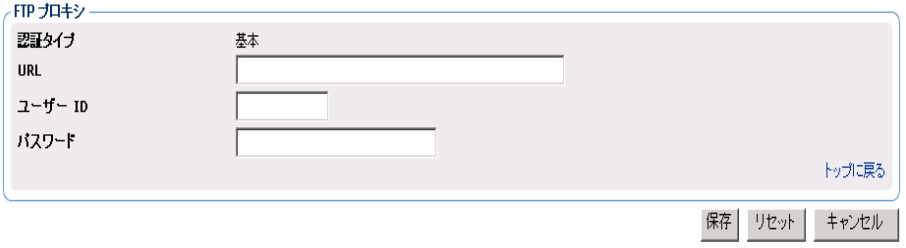
する必要がある場合は、http_timeout の値を増やしてください。http_timeout は、管理者インターフェイスには秒単位で表示されますが、patch.cfg にはミリ秒単位で格納されます。



FTP プロキシの設定

[FTP プロキシの設定] セクションで、次の設定を行います。

- **認証タイプ** : 基本 このパラメータは設定できません。
- **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。
- **ユーザー ID**: ftp トラフィックに ftp プロキシを使用し、プロキシが認証の認証情報を必要とする場合は、ユーザー ID を指定します。
- **パスワード** : ftp トラフィックに ftp プロキシを使用し、プロキシが認証の認証情報を必要とする場合は、パスワードを指定します。



エージェント オプション

これらのエージェント オプションは、Microsoft デバイスのパッチにのみ適用されます。

Microsoft デバイスにパッチを適用するときの Patch Manager Agent のオプションを有効化および設定するには、Patch Manager Administrator の [設定] > [インフラストラクチャの設定] グループにある [エージェント オプション] を使用します。

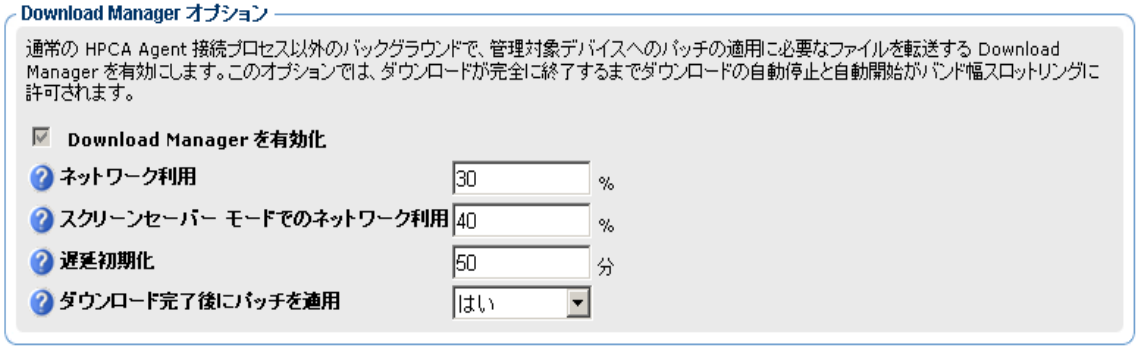
Patch Agent が次に HPCA Server に接続するときに、これらのパネルで指定した設定の変更が受信されます。

- 78 ページの「Download Manager オプション」
- 78 ページの「Patch Agent 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、エージェントのマシンに必要なパッチ　ファイルのダウンロードが、Download Manager によってバックグラウンドの非同期プロセスで制御されます。Download Manager は、通常の HPCA Agent Connect プロセスの外部で動作します。

  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 2　　Patch Agent の Download Manager オプション

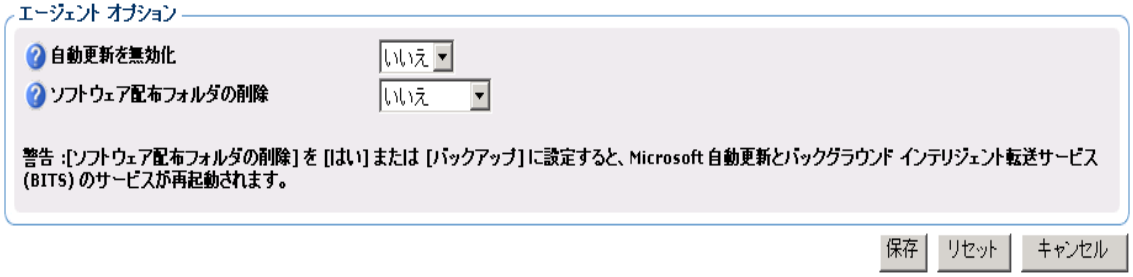
オプションと有効な値	説明
ネットワーク利用 値 = 0 ～ 100 % デフォルトは 0	デバイスがアクティブな場合にパッチ ファイルのダウンロードに使用できるネットワークの最大バンド幅の割合を指定します。 値が 0 の場合、使用可能なネットワークのバンド幅でダウンロードが行われます。 例 : 25 を指定すると、使用可能なバンド幅の 25% 以下でパッチのダウンロード プロセスが行われます。
スクリーンセーバー モードでのネットワーク利用 値 = 0 ～ 100 % デフォルトは 0	スクリーン セーバーのネットワーク利用のオプションです。スクリーン セーバーがオンの場合にパッチ ファイル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 Agent のエージェント オプション

次のエージェント オプションを使用して Microsoft デバイスにパッチを適用できます。

- **Microsoft 自動更新を無効化**：ドロップダウン ボックスから [はい] または [いいえ] を選択します。自動更新が有効になっていることが原因で Patch Agent のスキャンまたは配布が中断される問題に対応するには、このオプションを使用します。
  - **はい**：Patch Agent によって各スキャンまたは配布の前に Microsoft 自動更新が無効化されます。パッチのスキャンと配布が実行されたら、自動更新は元の状態に戻ります。
  - **いいえ**：(デフォルト) Patch Agent によって各スキャンまたは配布の前に自動更新が無効化されません。



- **ソフトウェア配布フォルダの削除**：ドロップダウン ボックスから [はい]、[バックアップ]、または [いいえ] を選択します。このオプションは、次の問題の対応に使用できます。
  - ソフトウェア配布フォルダのサイズの大幅な増加
  - ソフトウェア配布フォルダの破損
  - パッチ接続時に Configuration Server にかかる負荷の増加

  [ソフトウェア配布フォルダの削除] を [はい] または [バックアップ] に設定すると、Microsoft 自動更新とバックグラウンド インテリジェント転送サービス (BITS) のサービスが自動的に再起動されます。サービスの再起動によって環境に問題が発生する場合、特に共存するパッチ ソリューションとして HPCA 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コンテンツが削除されます。サービスの再起動に関する警告 (上記) を参照してください。

— **バックアップ** : Patch Agent によって、各パッチのスキャン前にソフトウェア配布フォルダのコンテンツがバックアップされてから削除されます。サービスの再起動に関する警告 (上記) を参照してください。

— **いいえ : (デフォルト)** ソフトウェア配布フォルダに対して何も行われません。

- **-mib (インストール済みのブリテンを管理する)**: 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。

  — **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

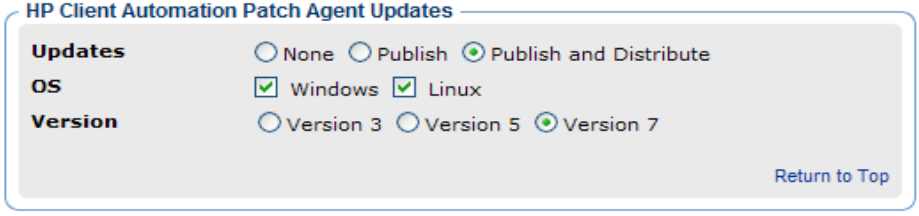
[エージェントの更新] を使用して、パッチ管理のエージェントの更新を設定します。

Patch Manager Administrator で、**[設定]** 領域の **[取得の設定]** グループにある [HP Patch Agent の更新] 設定にアクセスします。**[エージェントの更新]** をクリックします。

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、9 ページの「Updating the Patch Manager Agent」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 [取得の概要を保存] 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。

HP は、Patch Manager Administrator インターフェイスで **[取得の概要を保存]** と **[履歴の詳細を保存]** の値を指定することを推奨しています。また、コマンド ラインを使用した取得の場合は、これらのパラメータを指定しないことを推奨しています。

- **履歴の詳細を保存** : PUBERROR (Publisher Error) インスタンスを維持する日数を指定します。このクラスには、各パッチ取得エラーにつき 1 つのインスタンスが含まれます。
- **パッチ データのリポジトリ パス** : Configuration Server にパブリッシュされる前に、パッチがダウンロードされるディレクトリ。前回の取得のデータを事前に設定したディレクトリを使用して取得を実行する場合は、このパラメータに事前に設定するディレクトリを指定します。
- **過去のブリテン** : 過去のブリテンをカンマで区切って表示します。このパラメータは、製品またはリリース レベルではなく、ブリテン レベルで作用します。

  過去の機能で、以下を実行します。

  — 指定したブリテンが Configuration Server DB に存在する場合は、現在のパブリッシュ セッション中に削除します。

  — 過去のパラメータで指定したブリテンは、現在のパブリッシュ セッション中に Configuration Server DB にパブリッシュしないでください。過去オプションはブリテン オプションより優先されます。

- **除外された製品** : 除外する製品の先頭に感嘆符 (!) を付けます。 *vendor*::*product* の形式で、カンマで区切って指定します。包括フィルタが設定されていない場合はすべての製品が対象となります。包括フィルタを指定する場合は、除外フィルタは包括される製品のサブセットになります。これはベンダーの命名基準に従って指定してください。たとえば、Microsoft は、Internet Explorer を IE のような一般的な省略名でなく、完全名で使用します。また、Windows 95 以外のすべての Windows 製品を含める場合は、`{Microsoft::Windows*,Microsoft::!Windows 95}` と入力します。

新しい Patch Manager インストールの場合、Microsoft Office、Windows 95、Windows 98、Window Me、および Microsoft Office 製品、および SuSE 特有の *-yast2、*-yast2-*、および *-liby2 製品などのセキュリティ パッチの取得および

管理は*デフォルトで除外されています*。SuSE OS yast 特有製品の自動管理は Patch Manager ではサポートされていません。

以前のバージョンの Patch Manager からの移行で、移行前に `patch.cfg` を削除しなかった場合、すべての Microsoft Office 製品またはそのスタンドアロン バージョンを Patch Manager の取得と管理から除外するには、製品除外リストに次のテキストを追加します。

```
",!Access*,!Excel*,!FrontPage 200[023],!FrontPage
9[78],!InfoPath*,!Office*,!OneNote*,!Outlook*,!Powe
rPoint*,!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。

Patch Manager Administrator で、**[設定]** 領域の **[取得の設定]** グループにある [ベンダーの設定] にアクセスします。

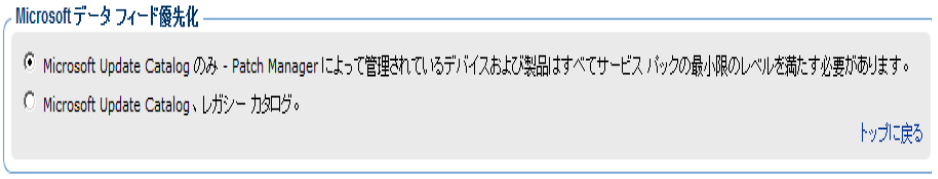
[ベンダーの設定] にアクセスする前に、まず [取得の設定]、[設定] ページで適切なベンダーと OS の選択を有効にしてください。

ある取得セッションから次のセッションの間にベンダーの設定を変更して、以前は選択されていた 1 つ以上の製品またはオペレーティング システムを除外した場合、除外した製品またはオペレーティング システムに特有のすべてのパッチが Configuration Server Database から削除されます。これは、除外された製品またはオペレーティング システムが、脆弱性の評価および管理の観点で今後は適格でなくなることを意味します。これは、すべてのベンダーに適用されます。

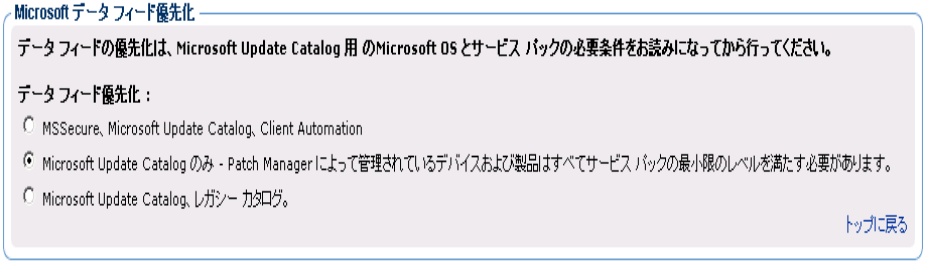
Microsoft データ フィード優先化

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に関する重要な情報については、78 ページの「Microsoft パッチの取得と管理について」および 78 ページの「Microsoft 自動更新について」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。78 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 Update Catalog のみ** : (デフォルト オプション) すべてのパッチは Microsoft Update Catalog から取得されます。このオプションを使用するには、企業内のすべてのデバイスが Microsoft によって設定された最低レベルのオペレーティング システムおよび製品である必要があります。これらの最低要件に適合していないデバイスにはパッチは適用されません。

このオプションを変更すると、次の警告メッセージが表示され、続行するにはこれに同意する必要があります。

[はい] をクリックすると、このオプションの選択を確認する画面がもう一度表示されます。**[保存]** をクリックして確定します。

- **Microsoft Update Catalog、レガシー カタログ** : パッチは、Microsoft Update Catalog と、現在の MSSECURE と HP が修正したメタデータを含む、レガシー カタログと呼ばれる HP リポジトリから取得されます。パッチが、Microsoft Update Catalog とレガシー リポジトリの両方に存在する場合は次のとおりです。
  - ターゲット デバイスが Microsoft Update Catalog でサポートされる最低要件に一致している場合、そのデバイスには Microsoft Update Catalog と Windows Update Agent テクノロジを利用してパッチが適用されます。

— ターゲット デバイスが Microsoft Update Catalog でサポートされる OS の最低要件に適合していない場合、デバイスにはレガシー カタログでホストされるメタ データを使用する MSSecure テクノロジを使用してパッチが適用されます。

HP レガシー カタログは、新しいパッチが MSSecure に追加されると、HP によって継続的に更新されます。HP レガシー カタログでホストされるパッチには、HP メタデータの修正が必要です。**[Microsoft Update Catalog、レガシー カタログ]** オプションをオンにすると、Microsoft セキュリティ ブリテンは古い Microsoft オペレーティング システム (各種のサービス パックも含めて) に適用可能とみなされます。また、Microsoft 製品には、Configuration Server の PATCHMGR ドメインと Reporting Server で表示される Patch Manager レポートで識別するために、Microsoft ブリテン名に「_L」が追加されます。

Office アプリケーションが HP Client Automation Application Self-Service Manager または管理制御ポイントで管理されている場合、Microsoft Update Catalog テクノロジを使用して取得および管理される Office のパッチは検出されません。どちらの場合も、Office アプリケーションに影響を与えるブリテンがデバイスに指定された場合は、Patch Manager が Office のパッチを管理し、それを脆弱なデバイスにローカルにインストールします。

Microsoft のフィード設定

以下の設定はベンダー フィードのセクションで行います。

[詳細] にのみ表示されるフィールド

- **MSSecure***: Microsoft が提供する `MSSECURE.XML` ファイルを含む、Microsoft の MSSecure キャビネット ファイルの URL を指定します。

  デフォルト : **http://download.microsoft.com/download/0/d/b/0db2e5d7-0ba9-4856-b51f-db7c0b838c68/MSSecure_1033.CAB**

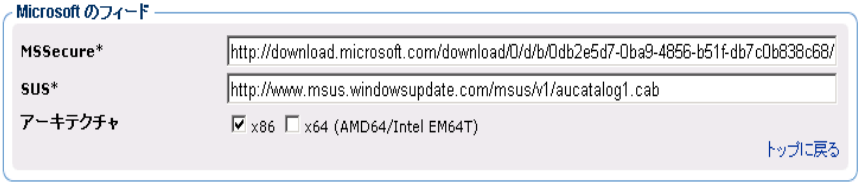
  このマニュアルを作成している時点で、Microsoft Knowledge の記事では、Microsoft は 2008 年までこのカタログの更新は継続するが、2007 年 10 月 9 日以降、`MSSecure.xml` のサポートおよび更新を継続しない計画であることを示唆しています。78 ページの「Microsoft パッチの取得と管理について」を参照してください。

- **SUS***: Microsoft SUS データ フィードを含む Microsoft キャビネット ファイルの URL を指定します。

デフォルト : **http://www.msus.windowsupdate.com/msus/v1/aucatalog1.cab**

[基本] と [詳細] のフィールド

- **アーキテクチャ**： Microsoft のパッチを取得するアーキテクチャを選択します。サポートされるアーキテクチャは次のとおりです。
  - **x86**:32 ビット Intel アーキテクチャ用。
  - **x64**:AMD64 または Intel EM64T 用。このターゲット アーキテクチャを選択する場合は、[Microsoft データ フィード優先化] を「**Microsoft Update Catalog のみ**」または「**Microsoft Update Catalog、レガシー カタログ**」に設定する必要があります。



Red Hat のフィード設定

[Red Hat のフィード] セクションでは、以下の設定を行います。

[詳細] にのみ表示されるフィールド

- **Red Hat**: Red Hat Network のデータ フィードの URL を指定します。デフォルトは **http://xmlrpc.rhn.redhat.com/XMLRPC** です。

[基本] と [詳細] のフィールド

- **パッケージ依存関係をパブリッシュ**： ダウンロードしたセキュリティ アドバイザリが依存する追加の Red Hat パッケージをパブリッシュする場合は、[はい] を指定します。デフォルトは [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。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ときは、次の **OS フィルタのアーキテクチャ**の値を参照してください。サブディレクトリ名には、REDHAT:: に続く値に基づいて適切なフォルダ名を使用します。

パッチの前提ソフトウェアがローカルに見つからない場合、パッケージを Red Hat Network からダウンロードします。取得に必要な時間を短縮するために、依存パッケージを Linux インストール メディアから適切なパッケージ ディレクトリにコピーすることをお勧めします。Red Hat RPM パッケージは、Linux インストール メディアの RedHat/RPMS ディレクトリにあります。

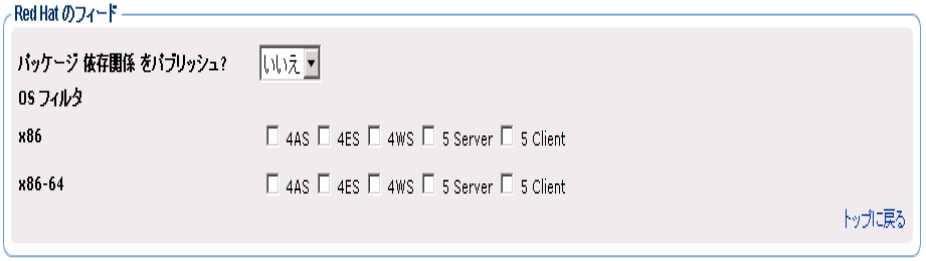
- **OS フィルタ** : x86 (32 ビット Intel) および x86-64 (Opteron/EMT64) アーキテクチャに対して、Red Hat バージョン 4 とリリース AS、ES および WS のすべての組み合わせ、および Red Hat バージョン 5 のサーバーおよびデスクトップ クライアント用リリースのすべての組み合わせがサポートされます。指定されたアーキテクチャの Red Hat パッチの取得については、オペレーティング システムとリリースの組み合わせを選択します。

  — **x86** アーキテクチャ : Red Hat x86 アーキテクチャで patch.cfg ファイルに指定できる値は次のとおりです。

  ```
  REDHAT::4as,       REDHAT::4es,      REDHAT::4ws,
  REDHAT::5server,    REDHAT::5client
  ```

  — **x86-64** アーキテクチャ : Red Hat x86-64 アーキテクチャで patch.cfg ファイルに指定できる値は次のとおりです。

  ```
  REDHAT::4as-x86_64,      REDHAT::5server-x86_64,
  REDHAT::4es-x86_64,      REDHAT::5client-x86_64,
  REDHAT::4ws-x86_64
  ```



SuSE のフィード設定

SuSE Linux のパッチ適用設定を設定するには、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：

- 78 ページの「SuSE パッチの取得要件」

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] にのみ表示されるフィールド

- **SuSE 9**: SuSE 9 のセキュリティ アドバイザリのメタ データを取得するためのセキュアな URL を指定します。デフォルトは以下のとおりです。

  https://you.novell.com/update/i386/update/SUSE-CORE/9/
  https://you.novell.com/update/i386/update/SUSE-SLES/9/

- **SuSE 9-x86_64**: AMD64 または Intel EM64T アーキテクチャの SuSE 9 の更新を取得するためのセキュアな URL を指定します。デフォルトは以下のとおりです。

  https://you.novell.com/update/x86_64/update/SUSE-CORE/9/
  https://you.novell.com/update/x86_64/update/SUSE-SLES/9/

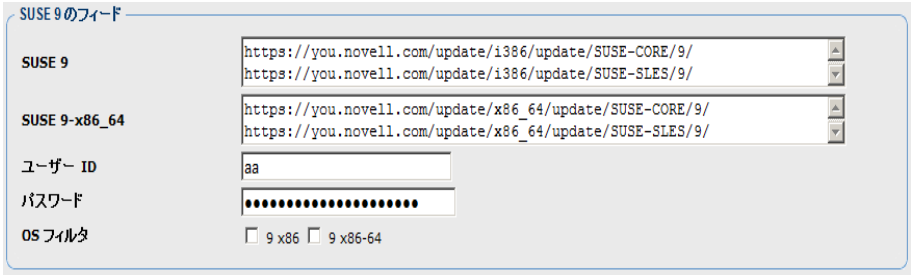
[基本] と [詳細] のフィールド

[基本] または [詳細] ページを使用して、SuSE 9 のデータフィードを取得するために必要な設定を入力します。

- **ユーザー ID**: お使いの SuSE ユーザー ID を指定します。ユーザー ID はベンダーから入手します。
- **パスワード**: SuSE ユーザー ID のパスワードを指定します。
- **OS フィルタ** : SuSE Linux Enterprise Server パッチを取得するオペレーティング システムのバージョンとアーキテクチャの組み合わせを選択します。x86 (32 ビット) アーキテクチャと x86-64 (AMD64 および Intel EM64T) アーキテクチャの SuSE バージョン 9 がサポートされています。

  patch.cfg で有効な x86 アーキテクチャの OS フィルタの値は `suse::9` です。

  patch.cfg で有効な x86-64 アーキテクチャの OS フィルタの値は `suse::9-x86_64` です。



SuSE 10 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] にのみ表示されるフィールド

- **SUSE 10**: x86 アーキテクチャの SUSE 10 (SLES10 と SLED10) についてセキュリティ アドバイザリのメタ データを取得するためのセキュアな URL を指定します。

  デフォルト :
  https://nu.novell.com/repo/\$RCE/SLES10-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-Updates/sled-10-i586/

- **SUSE 10SP1:** x86 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 1 について更新を取得するためのセキュアな URL を指定します。

  デフォルト：
  https://nu.novell.com/repo/\$RCE/SLES10-SP1-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-SP1-Updates/sled-10-i586/

- **SUSE 10SP2:** x86 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 2 について更新を取得するためのセキュアな URL を指定します。

  デフォルト：
  https://nu.novell.com/repo/\$RCE/SLES10-SP2-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-SP2-Updates/sled-10-i586/

- **SUSE 10-x86_64**: x86-64 アーキテクチャの SUSE 10 (SLES10 と SLED10) についてセキュリティ アドバイザリのメタ データを取得するためのセキュアな URL を指定します。

  デフォルト：
  https://nu.novell.com/repo/\$RCE/SLES10-Updates/sles-10-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED10-Updates/sled-10-x86_64/

- **SUSE 10SP1-x86_64:** x86-64 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 1 について更新を取得するためのセキュアな URL を指定します。

  デフォルト：
  https://nu.novell.com/repo/\$RCE/SLES10-SP1-Updates/sles-10-x86_64
  https://nu.novell.com/repo/\$RCE/SLED10-SP1-Updates/sled-10-x86_64/

- **SUSE 10SP2-x86_64:** x86-64 アーキテクチャの SUSE 10 (SLES10 と SLED10) Service Pack 2 について更新を取得するためのセキュアな URL を指定します。

  デフォルト：
  https://nu.novell.com/repo/\$RCE/SLES10-SP2-Updates/sles-10-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED10-SP2-Updates/sled-10-x86_64/

- **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、78 ページの「SuSE パッチの取得要件」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。

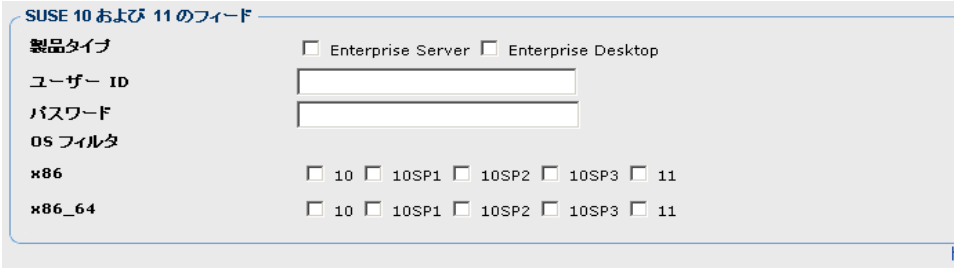
  — x86 (32 ビット) および x86-64 (AMD64 および Intel EM64T) アーキテクチャの SUSE バージョン 11 base。

  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。



Patch の設定ファイル

Patch Manager Administrator を使用できない場合、Patch Manager Server をインストールした場所の \etc フォルダにある patch.cfg ファイルを直接変更できます。

デフォルト ロケーションは、*System Drive*:\Program Files\Hewlett-Packard\CM\PatchManager\etc です。

詳細については、付録 D、「Patch.cfg のパラメータ」を参照してください。

ログを表示

Patch Manager Server ログを使用して、パッチ管理環境を確認したり、トラブルシューティングしたりすることができます。これらのログは、Patch Manager Administrator からオンラインで使用できます。

Patch Manager Administrator コンソールの **[ステータスとログ]** 領域に移動して、**[ログを表示]** をクリックします。

表示されているリストからログ ファイルを選択して開き、そのファイルをオンラインで確認するか、またはローカルに保存して後で HP サポートを利用して確認します。

- **HPCA-PATCH-3467.log** Patch Manager Server のログです。
- **httpd-3467.yy.mm.dd.log** Patch Manager Server の Web サーバー アクセス ログです。このログは、だれがサーバーにアクセスしているか、Web サービスまたはコンソール インターフェイスのどちらを経由しているか、および実行されたアクセスの回数を示します。

これらのログは、Patch Manager Server インストール ディレクトリの \logs フォルダにあります。

データベースの同期

HPCA Configuration Server DB に送信されたパッチ情報は、評価と分析のために Patch SQL データベースと同期する必要があります。HPCA Configuration Server DB と Patch SQL データベースには、同期されるクラスとインスタンスのセットの同じ情報が格納されます。

- PATCHMGR ドメイン内の各クラスは、Patch SQL データベース内のテーブルになります。対応するテーブルは、nvd_classname という名前です。

- 各クラスの各属性は、そのテーブルの列になります。対応する列名は nvd_attributename です。式と接続変数は複製されません。
- クラスの各インスタンスは、対応するテーブルのレコードになります。

この同期は、パッチ取得後、および通常の HPCA オペレーションで自動的に実行されます。

ただし、手動で同期を実行することが必要になる場合があります。たとえば、別の HPCA Server からパッチ情報をインポートした後は、手動でデータベースを同期します。また、ある程度取得を実行した後でパッチ管理用に設定された SQL データベースを切り替える場合も、手動でデータベースを同期します。

データベースは、Patch Manager Administrator またはコマンド ラインを使用して手動で同期できます。

Patch Manager Administrator を使用してデータベースを同期するには

1 Web ブラウザから、**http://<***patchserveripaddress***>:<***port***>/patch/manage/admin.tsp** に移動します。

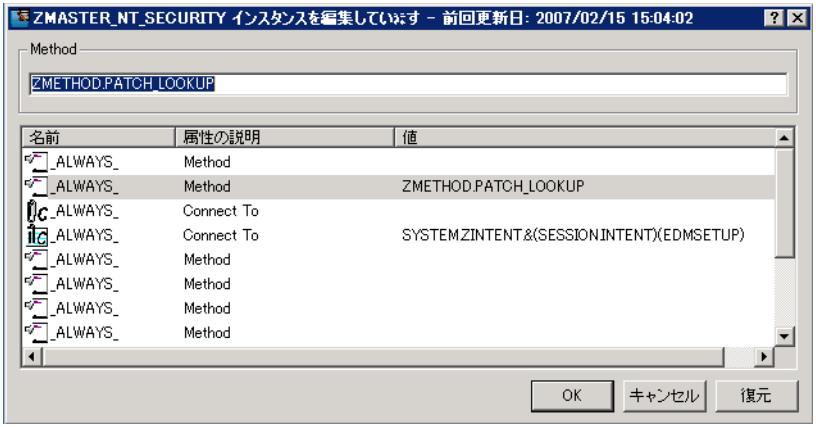
2 [オペレーション] の **[同期を実行]** をクリックします。

3 **[サブミット]** をクリックします。

メソッド接続の追加

Admin CSDB Editor を使用して、_ALWAYS_ Method 接続を次の図の PRIMARY.SYSTEM.PROCESS.ZMASTER インスタンスに追加します。

図 2　　ZMASTER インスタンスの編集



ZMETHOD.PATCH_LOOKUP へのメソッド エントリは、ユーザーに対するすべてのサービスの解決の前に配置する必要があります。

Messaging Server

Messaging Server の最新バージョンをインストールすることを推奨します。バージョン 5.10 以上をインストールする必要があります。Patch Manager レポートには、Patch Manager Data Delivery Agent で Messaging Server を有効にする必要があります。詳細については、『HPCA Messaging Server Installation and Configuration Guide』を確認してください。

Reporting Server

Reporting Server の最新バージョンを推奨します。バージョン 5.10 以上が必要です。インストール前に、付属の HP Client Automation リリース ノートの Reporting Server のセクションを確認してください。『*HPCA Reporting Server Guide*』には、Reporting Server の使用方法に関する指示も含まれています。

3　パッチ取得

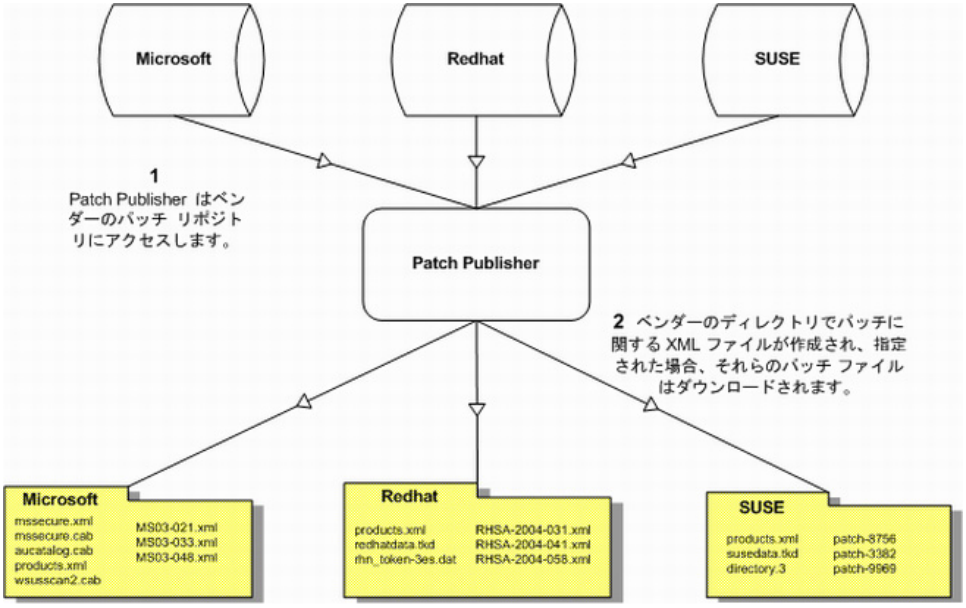
この章は以下を目的としています。

- 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 Manager Administrator の操作を理解する。
- 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

Patch Manager 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 3　　ベンダーのパッチ リポジトリとの接続



取得の概要

Patch Manager 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 Manager 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

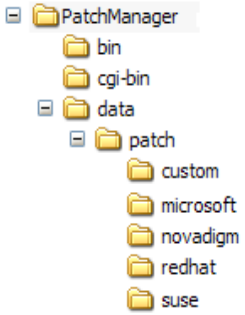
セキュリティ パッチが取得されると、パッチの情報を含む XML ファイル、つまりパッチ説明ファイルが作成され、ベンダーのディレクトリに配置されます。ベンダーのディレクトリは、デフォルトで次のロケーションにあります。*System Drive*:\Program Files\Hewlett-Packard\CM\PatchManager\Data\Patch

たとえば、Microsoft ブリテンのパッチ説明ファイルは次のロケーションにあります。*System Drive*:\Program Files\Hewlett-Packard\CM\PatchManager\Data\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。*System Drive*:\Program Files\Hewlett-Packard\CM\PatchManager\Data\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。

図 4　　取得されたパッチ説明ファイルのディレクトリ構造

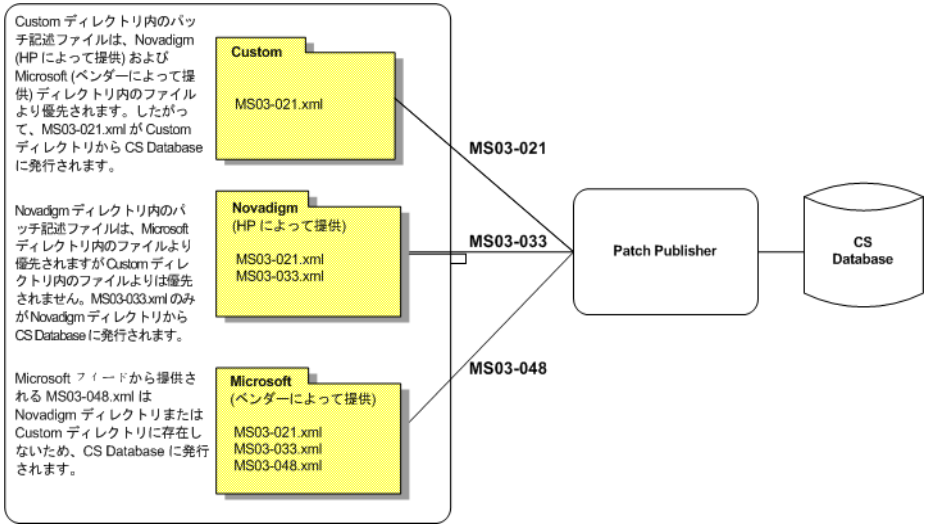


ベンダーから取得した情報の一部は、パッチの管理を開始する前に変更する必要があります。このため、\data\patch サブフォルダには、他に novadigm および custom の 2 つのサブディレクトリがあります。HP では追加のパッチ説明ファイルを用意しており、それらは novadigm サブディレクトリにあります。novadigm サブディレクトリにあるパッチ説明ファイルは、対応するベンダーのディレクトリにあるパッチ説明ファイルを上書きします。また、独自のパッチ説明ファイルを作成または変更して、それを custom サブディレクトリに配置することもできます。これらのカスタム ファイルは、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 5　　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) に組み込まれたサポート

Microsoft は、これまで、一般に MSSECURE と呼ばれるパッチ リポジトリにパッチをホストしてきました。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。
- Microsoft Web サイトの記事は、2007 年 10 月 9 日以降、MSSECURE の更新は行わない意向であることを示しています。

Microsoft が MSSECURE のサポートを終了する日付である 2007 年 10 月 9 日を過ぎても、Microsoft は MSSECURE のアップデートを継続してパブリッシュしていますが、Microsoft Update Catalog でホストされるパッチのみが更新および維持されます。

現在、Patch Manager は、既存のレガシー カタログ以外に MSSECURE および新しい Microsoft Update Catalog もパッチの送信元として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 Manager 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 Manager 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、この時点でデバイスを最低のサービス パック レベルにアップグレードした方が、Microsoft が MSSECURE テクノロジのサポートを終了したときの影響が少なくなります。

Microsoft データ フィードに対する Patch Manager 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 Manager Administrator 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。

- **MSSecure、Microsoft Update Catalog、Client Automation**
- **Microsoft Update Catalog のみ**
- **Microsoft Update Catalog、レガシー カタログ**

詳細については、50 ページの「Microsoft データ フィード優先化」を参照してください。

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 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 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、101 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 Manager 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/en-us** にあります。

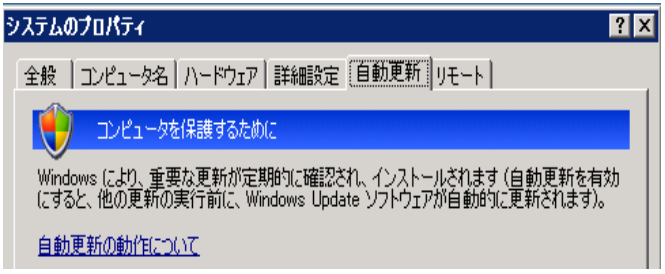
  または

- Patch Manager 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 Manager 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 Manager 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 Manager 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 Manager 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 Manager 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 Manager も Windows Update Agent テクノロジを利用しているため、同じ制約が Patch Manager 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://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 Manager 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。

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 Manager は、取得時にまず適切なディレクトリで .rpm パッケージを検索します。次に例を示します。

— x86 の Red Hat Enterprise Linux 4ES では、Red Hat インストール メディアで提供されたベースライン オペレーティング システムの rpm ファイルを data/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、54 ページの「Red Hat のフィード設定」の **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 Manager 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。

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。

SuSE パッチの取得要件

SuSE フィードの設定では、このトピックで説明するセキュア (SSL) 接続およびベンダーから提供されるユーザー ID と パスワードが必要になります。

➤ SuSE 10 デバイスおよび SuSE 11 デバイスには要件が追加されました。77 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、Patch Manager Administrator コンソールを使用して指定します。**[設定] > [取得の設定] > [ベンダーの設定]** ページに移動します。
- **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、Patch Manager Administrator コンソールを使用して指定します。**[設定] > [取得の設定] > [ベンダーの設定]** ページに移動します。

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。

   [Mirror Credentials ｜ミラー認証情報] ページの [Credentials ｜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。[Channels ｜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。57 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 マシンおよび SuSE 11 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。

パッチ取得の実行

Client Automation Patch Manager Administrator (Patch Manager Administrator) コンソールには、繰り返し保存して使用できる取得ジョブ プロファイルを作成するための使いやすいユーザー インターフェイスがあります。

- 取得ジョブを定義するには、[設定] 領域の [取得ジョブ] タスクを使用します。

- ジョブを実行するには、[オペレーション] 領域の [取得を開始] タスクを使用します。

取得ジョブまたは取得コマンド ラインで指定したパラメータは、Patch Manager の設定ファイル `patch.cfg` で設定されたパラメータより優先されます。スペースを含む値は必ず引用符で囲んでください。詳細については、36 ページの「Patch Manager Administrator を使用して、Patch Manager を設定する」を参照してください。

パッチは、1 度に 1 つのベンダーから取得することをお勧めします。また、一部の SuSE セキュリティ アドバイザリおよび Microsoft Office セキュリティ ブリテンは、ダウンロードするために長時間かかる場合があります。これを考慮して、HTTP タイムアウトのパラメータを調整することを検討してください。

必要な取得ジョブの設定は、お使いの環境に依存します。

取得ジョブの設定

Patch Manager Administrator 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

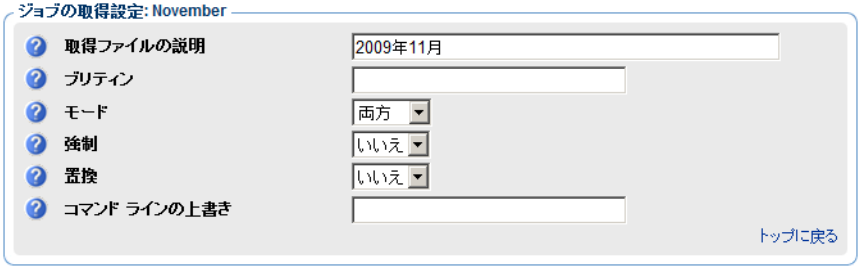
1 ご使用の Web ブラウザから、**http://***patchserveripaddress***:***port* **/patch/manage/admin.tsp.** に移動します。

2 [設定] 領域の **[取得ジョブ]** をクリックします。

3 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。

4 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。

5 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。

- **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。

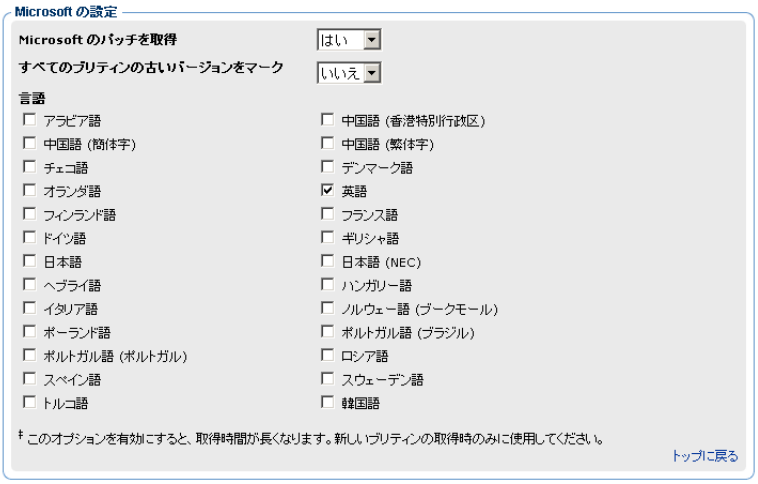
replace が **`Y`** に設定されると、ブリティンは force の値に関係なく削除されてから再取得されます。

- **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。パラメータの完全なリストについては、付録 D、「Patch.cfg のパラメータ」を参照してください。

Microsoft の設定

- **Microsoft のパッチを取得しますか ?**: Microsoft のパッチを取得する場合は **[はい]** を選択します。その他の設定については、Patch Manager Administrator の [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の古いバージョンをマーク]** 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ンを更新する場合、**[すべてのブリティンの古いバージョンをマーク]** 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ンの取得を実行することなく Configuration Server Database 内のブリテンを更新できます。

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。

Red Hat の設定

- **Red Hat のパッチを取得しますか?**: Red Hat のパッチを取得する場合は **[はい]** を選択します。その他の設定については、Patch Manager Administrator の [ベンダーの設定] ページに移動してください。

SuSE の設定

- **SUSE のパッチを取得しますか ?**: SuSE のパッチを取得する場合は [**はい**] を選択します。その他の設定については、Patch Manager Administrator の [ベンダーの設定] ページに移動してください。

6 **[次へ]** をクリックして手順 7 に進みます。ここで、取得セッションで除外する製品を選択します。

1 つ以上の製品またはオペレーティング システムを次々に取得から除外すると、取得から除外した製品またはオペレーティング システムに固有のすべてのパッチが Configuration Server Database から削除されます。その結果、削除された製品またはオペレーティング システムは、脆弱性の評価および管理の観点で今後は適格でなくなります。これは、すべてのベンダーに適用されます。

7 適切なベンダーの製品を展開し、取得対象から除外する製品にチェックを入れます。含める製品のチェックは外します。

8 **[完了]** をクリックして、作成した取得ファイルを保存します。

これで、保存した設定を使用して、Patch Manager Administrator で取得を実行できます。**[オペレーション]** 領域で、**[取得を開始]** をクリックし、このジョブを選択します。

取得を開始

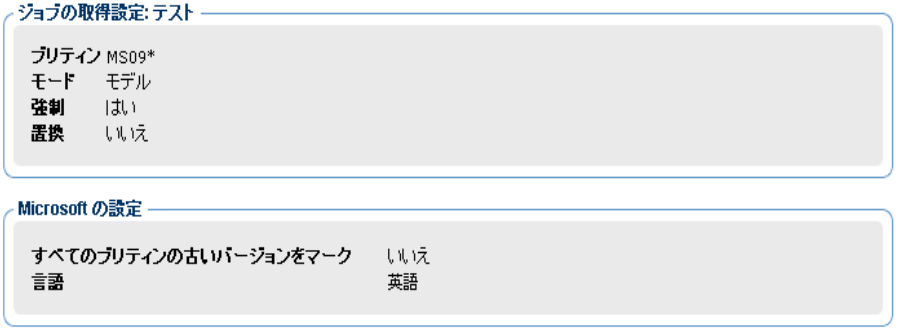
Patch Manager Administrator から取得ジョブを実行するには

1 Web ブラウザから、**http://***patchserveripaddress***:***port* **/patch/manage/admin.tsp** に移動します。

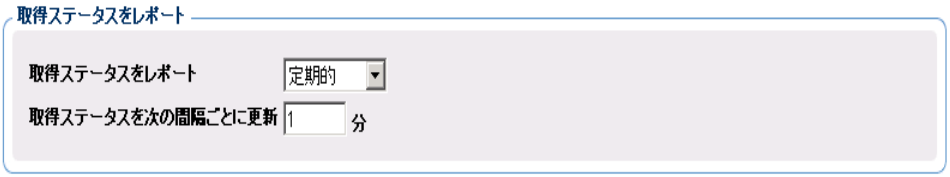
2 [オペレーション] で、**[取得を開始]** をクリックします。

3 名前をクリックして、ファイルを選択します。

4 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。

5 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

- HP Reporting Server を使用して、パッチ取得レポートを表示します。
- Patch Manager Administrator の **[ステータスとログ]** 領域に移動して、**取得ジョブを表示**します。

- また、**[ステータスとログ]** 領域を使用して **[ログを表示]** ページにアクセスし、patch-acquire.log を選択します。このパッチ取得ログ ファイルは、Patch Manager のログ ディレクトリに作成されます。また、このログ ファイルには、patch.tkd のバージョンとビルド番号が記述されます。

取得履歴を表示

Patch Manager Administrator の **[ステータスとログ]** 領域で、**[取得履歴を表示]** をクリックして以前の取得のステータスと詳細を表示します。

ステータスと詳細を表示するには、リストの取得ジョブを選択します。

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 C:\Program Files\Hewlett-Packard\CM\PatchManager\data\patch\microsoft ディレクトリにある Microsoft バージョンの XML ファイルを、C:\Program Files\Hewlett-Packard\CM\PatchManager\data\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。

Patch Manager Administrator 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。

```
20040116 15:11:24 Info: Publishing MS02-065 1 of 1

20040116 15:11:24 Info: Using bulletin from custom C:/Program
Files/Hewlett-Packard/CM/PatchManager/data/patch/custom
/MS02-065.xml

20040116 15:11:24 Info: Loading XML file C:/Program Files/
Hewlett-Packard/CM/PatchManager/data/patch/custom
/MS02-065.xml

20040116 15:11:24 Info: Loading bulletin MS02-065 from RCS
```

RADDBUTIL を使用した変更管理

品質保証環境から実働環境にセキュリティ パッチを移動するには、RadDBUtil; と呼ばれる Configuration Server Database ユーティリティを使用する必要があります。

RadDBUtil の使用に関する全般的な情報については、以下を参照してください。

- 『HPCA Configuration Server User Guide』の HPCA Configuration Server Database Utility (RadDBUtil) に関する章。

RadDBUtil を Patch Manager で使用する場合の特定の情報については、HP Software のサポート サイトの次の技術的なドキュメントも参照してください。

- *Managing the Patch Bulletin Data Export and Import Process* (Document ID: KM112025)

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

Patch Manager 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 Manager 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 Manager 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 Manager 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。
–mib オプションには、次の値を指定できます。

-mib none
Patch Manager 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 Manager 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 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 Manager 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 Manager 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

Patch Manager Administrator コンソールの [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] 領域の [環境の設定] 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、Reporting Server にアクセスします。Patch Manager Administrator のツールバー領域にある [レポート] アイコンを使用できます。**[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。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、『*HPCA Reporting Server Guide*』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。

図 6　　取得の概要レポートの表示

開始時刻	終了時刻	ベンダー	ブリテン数	追加されたブリテン数	更新されたブリテン数	パッチ数	追加されたパッチ数	更新されたパッチ数	エラー数	パブリッシュするマシン
2009-07-28 13:31:44	2009-07-28 15:47:59	MICROSOFT	1	1	0	13	13	0	0	caem14
2009-07-28 11:06:29	2009-07-28 11:14:56		0	0	0	0	0	0	0	caem14

- **[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。

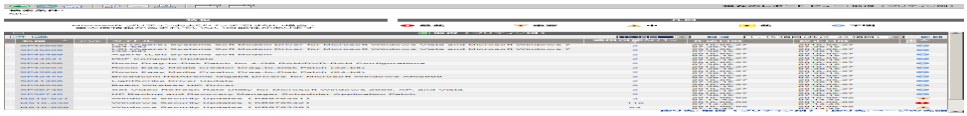
- **[エラー数]** をクリックして、取得が失敗した理由の詳しい説明を参照します。エラー レポートに表示される数字のエラー コードは、標準の HTTP ステータス コードです。これらのコードの詳細については、インターネットで「HTTP ステータス コード」を検索してください。

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。

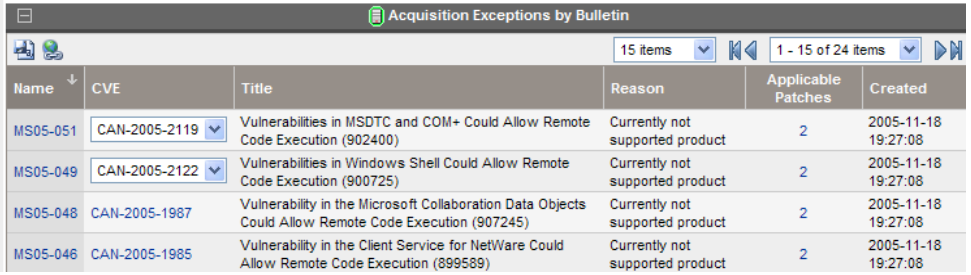
図 7　　ブリテン別取得の概要の表示



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 Manager 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。評価範囲は、[最重要] から、[重要] まで、[中] まで、[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。
- このレポートの一番下には、Patch Manager 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。

図 8　　取得例外 (ブリテン別) の表示



Acquisition Exceptions by Bulletin

15 items　1 - 15 of 24 items

Name	CVE	Title	Reason	Applicable Patches	Created
MS05-051	CAN-2005-2119	Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400)	Currently not supported product	2	2005-11-18 19:27:08
MS05-049	CAN-2005-2122	Vulnerabilities in Windows Shell Could Allow Remote Code Execution (900725)	Currently not supported product	2	2005-11-18 19:27:08
MS05-048	CAN-2005-1987	Vulnerability in the Microsoft Collaboration Data Objects Could Allow Remote Code Execution (907245)	Currently not supported product	2	2005-11-18 19:27:08
MS05-046	CAN-2005-1985	Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589)	Currently not supported product	2	2005-11-18 19:27:08

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。

図 9　　取得 (パッチ別) の表示

取得 (パッチ別)

15 項目　1 - 13 項目 (共に 13 項目)

ブリテン	製品/リリース	番号	パッチの言語	置換されるパッチ	ステータス	サイズ (バイト)	日付
MS09-013	Windows Server 2003 (MU)	960803	zh-cn	N	0	674,168	2009-07-28 23:44:54
MS09-013	Windows Server 2003 (MU)	960803	en	N	0	673,144	2009-07-28 23:45:18
MS09-013	Windows 2000 (MU)	960803	en	N	0	1,350,696	2009-07-28 23:47:00
MS09-013	Windows 2000 (MU)	960803	zh-cn	N	0	944,168	2009-07-28 23:46:25
MS09-013	Windows Server 2003, Datacenter Edition (MU)	960803	zh-cn	N	0	674,168	2009-07-28 23:44:54
MS09-013	Windows Server 2003, Datacenter Edition (MU)	960803	en	N	0	673,144	2009-07-28 23:45:18
MS09-013	Windows XP (MU)	960803	zh-cn	N	0	672,112	2009-07-28 23:47:45
MS09-013	Windows XP (MU)	960803	en	N	0	671,088	2009-07-28 23:45:56
MS09-013	Windows Vista (MU)	960803		N	0	276,307	2009-07-28 23:45:30
MS09-013	Windows Vista (MU)	960803		N	0	491,109	2009-07-28 23:47:26
MS09-013	Windows Server 2008 (MU)	960803		N	0	491,109	2009-07-28 23:47:26
MS09-013	Windows Server 2008 (MU)	960803		N	0	595,189	2009-07-28 23:45:43
MS09-013	Windows Server 2008 (MU)	960803		N	0	276,307	2009-07-28 23:45:30

- 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。

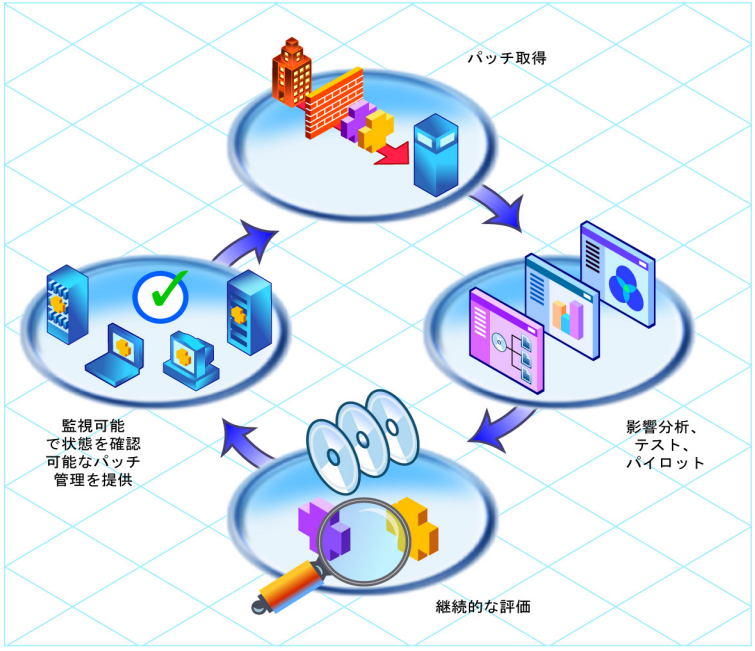
- [重大度] 列のアイコンは、Windows パッチの重大度を示します。評価範囲は、[最重要] から、[重要] まで、[中] まで、[低] までです。パッチが Windows プラットフォーム用でない場合は、[不明] アイコンが表示されます。重大度が同じパッチをすべて表示するには、[重大度] 列のアイコンをクリックします。既存パッチに重大度評価はありません。既存のブリテンおよびパッチの重大度評価を表示するには、[強制] および [置換] オプションを使用して再取得する必要があります。

4　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。

- Patch Manager Agent のインストールについて理解する。
- 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 10　　製品探索と分析



Patch Manager Agent のインストール

Patch Manager Agent は脆弱性を管理するターゲット デバイスにインストールする必要があります。インストールには、HPCA Enterprise Manager または提供された Patch Manager メディアを使用します。

Microsoft Update を使用するには、ターゲット デバイスに Windows Update Agent をインストールしておく必要があります。これは Patch Manager Agent 更新の一部で、HP Patch Manager 更新サイトからダウンロードできます。HP 取得プロセスは、Patch Manager Agent 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。

インストール手順の詳細については、『HPCA Enterprise Manager ユーザー ガイド』または『HPCA Application Manager および Application Self-service Manager ガイド』を参照してください。最低システム要件については、適切なオペレーティング システムに関して『HPCA Application Manager および Application Self-service Manager ガイド』も参照してください。

Patch Manager を使用して Microsoft Windows のデバイスを管理している場合、最低でも Windows インストーラ バージョン 3.1 を Patch Manager を実行するエージェント デバイスに事前にインストールしておく必要があります。

Patch Manager デバイスに対応する `nvdkit` の推奨バージョンは、HP Client Automation バージョン 7.50 のメディアで提供されているビルドです。Patch Agent で必要な `nvdkit` の絶対最小ビルドは、**427** です。お使いのターゲット デバイスがこの要件を満たさない場合は、HP サポート Web サイトを参照してください。

Patch Manager Agent を HPCA Enterprise Manager からインストールするには

Patch Manager Agent は、HPCA Agent を Enterprise Manager コンソールから企業のデバイスおよびデバイス グループに配布するときに自動的に含まれます。

エージェントの配布は、**エージェント配布ウィザード**を使用して、Enterprise Manager コンソールの **[管理]** タブから実行します。

Enterprise Manager とエージェント配布ウィザードの使用方法の詳細については、『HPCA Enterprise Manager ユーザー ガイド』を参照してください。

Windows Agent 用の HP Client Automation メディアからインストールするには

- HP Client Automation メディアの Agent フォルダにある、お使いのオペレーティング システムに適したサブディレクトリに移動します。**setup.exe** をダブルクリックします。プロンプト画面が表示されたら、**Patch Manager** 機能を選択します。

Windows Agent 用の install.ini ファイルを使用するには

- `install.ini` ファイルの [PROPERTIES] セクションに、行 **`ADDLOCAL=NVDINSTALLPATCH`** を追加します。

エージェントをインストールした後、適切なサービスをターゲット デバイスに割り当てる必要があります。

Patch Manager Agent を Linux オペレーティング システムにインストールするには

マニュアルに記載されいてる Patch Manager Agent バージョン 7.50 の機能をサポートする Client Automation Agent の最低バージョンは、Application Manager バージョン 5.0 ですが、Application Manager バージョン 7.50 を推奨します。Linux Agent 上の `nvdkit` の絶対最小ビルドは、ビルド 446 です。

Patch Manager' のメンテナンス ファイル `maint.tar` には、Patch Manager Agent を有効にするために必要な Agent ファイルが含まれています。このマニュアルを作成している時点で、Patch Manager Agent のバージョン 7.80 は、以下のオペレーティング システムでサポートされています。

- **Linux - RedHat**: x86 (32 ビット Intel) および x86-64 (Opteron/EMT64) アーキテクチャでは、リリース AS、ES、WS で Red Hat バージョン 4.x がサポートされ、サーバーおよびクライアント リリースでバージョン 5.x がサポートされます。
- **Linux - SuSE:** x86 (32 ビット) アーキテクチャと x86-64 (AMD64 および Intel EM64T) アーキテクチャでは、SuSE Linux Enterprise Server (SLES) バージョン 9、10、および 11 がサポートされます。x86 (32 ビット) アーキテクチャと x86_64 (AMD64 および Intel EM64T) アーキテクチャでは、SuSE Linux Enterprise Desktop (SLED) バージョン 10 および 11 がサポートされます。

HP-UX または Sun Solaris (SPARC) オペレーティング システムでは、Patch Manager Agent はサポートされません。

Patch Manager Agent のメンテナンス ファイル (maint.tar) は、Patch Manager メディアの以下のオペレーティング システム専用ディレクトリに配置されています。

— Patch Agent Maintenance\linux\ram

インストール メディアのオペレーティング システム専用フォルダに提供される maint.tar ファイルは、デバイス プラットフォーム間で交換できません。

RedHat および SuSE Linux 用の Patch Manager Agent を HPCA Enterprise Manager からインストールするには

再起動管理機能を有効にし、再起動後にパッチ管理処理を再開するには、最低でも HP Client Automation Application Manager 5.00 が必要です。この機能を使用するには、システム サービスとして HPCA スケジューラ デーモン (radsched) を有効にする必要があります。エージェント のシステム サービスとしてのインストールは、Application Manager Agent のインストール時にインストール後のタスクとして実行されます。UNIX Agent のインストール後タスクの詳細については、『HPCA Application Manager および Application Self-Service Manager インストールおよび設定ガイド』を参照してください。

HPCA Enterprise Manager から Client Automation Agent をインストールする手順については、『HPCA Enterprise Manager ユーザー ガイド』および『HPCA Application Manager および Application Self-service Manager ガイド』を参照してください。

RedHat および SuSE Linux 用の HP Client Automation メディアからインストールするには

インストール メディアで、お使いのオペレーティング システムに適したサブディレクトリに移動します。UNIX の **./install** コマンド ラインを使用してインストーラを開始し、Patch Manager Agent 機能を選択します。詳細については、『*HPCA Application Manager and Application Self-Service Manager Guide for UNIX*』を参照してください。

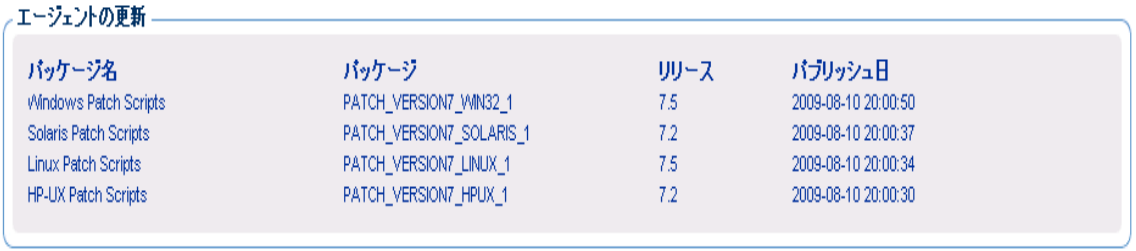
再起動管理機能を有効にし、再起動後にパッチ管理処理を再開するには、最低でも Application Manager 5.00 が必要です。この機能を使用するには、システム サービスとして HPCA スケジューラ デーモン (radsched) を有効にする必要があります。エージェント のシステム サービスとしてのインストールは、Application Manager Agent のインストール時にインストール後のタスクとして実行されます。Unix Agent のインストール後タスクについては、『*HPCA Application Manager and Application Self-Service Manager Guide for UNIX*』を参照してください。

Patch Manager Agent の更新

パッチの取得を実行するときに、最新バージョンと Patch Agent ファイルの更新情報もダウンロードできます。Patch Agent ファイルには、製品の検出と管理を実行するためのスクリプトが含まれています。これらのファイルは、HP が提供するパッチ更新の Web サイトで受信します。ダウンロードした後、ファイルは PATCHMGR ドメインにパブリッシュされ、DISCOVER_PATCH サービス インスタンスに接続されます。

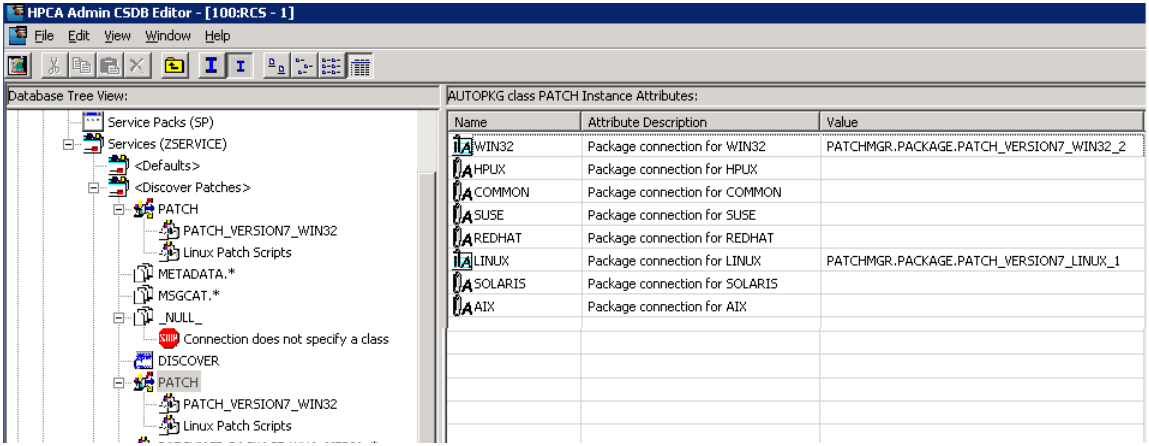
[パッチ アドミニストレータ] ページの [オペレーション] セクションで、[エージェントの更新を表示] タスクを使用して、更新のステータスを判断します。これを実行するには、**[エージェントの更新を表示]** をクリックします。

図 11　　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 Agent 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 12　　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。また、以前のリリースから移行し、移行の実行前に既存の `patch.cfg` を削除した場合でも、これがデフォルト値になります。

以前のバージョンから移行し、移行の実行前に既存の `patch.cfg` を削除しなかった場合、バージョン数はデフォルトで古い `patch.cfg` ファイルに含まれる値になります。移行するお客様は、Patch Manager Administrator を使用して **[パブリッシュと配布]** オプションを設定し、Agent の更新バージョンを **[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」と表示されます。

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 Agent 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。

製品探索と分析

脆弱性を管理する前に、Patch Manager Agent がデバイス上の製品を探索する必要があります。Patch Manager 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 Manager 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 Manager サービスを、管理対象デバイスに割り当てます。

Patch Manager 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 Manager 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。Policy Server を Patch Manager と一緒に使用している場合は、付録 C、「Policy Server の統合」を参照してください。

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 Manager 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 Manager Agent 接続の間に、Patch Manager 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 Manager 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 Manager サービスにより管理されます。このサービスは、Patch Manager 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、『HPCA Application Manager および Application Self-service Manager 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 Manager 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 Manager 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 Manager 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 Manager で単独に管理する必要があります。

Patch Manager 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 Manager 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 Manager 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。

- 102 ページの「Microsoft Office セキュリティ ブリテン管理の最善実践」
- 107 ページの「Microsoft Update Catalog を有効にした最善実践」
- 108 ページの「Patch Manager (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 Manager 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 Manager 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 Manager 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 Manager 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 Manager 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 Manager 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 Manager 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 Manager 以外のソリューションを使用しない場合に限り、Patch Manager 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 Manager 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 Manager) 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 Manager 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 Manager 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 Manager 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 Manager 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 Manager 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 Manager 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 Manager 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 Manager 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。Microsoft Office 2000 を使用しているお客様は、Microsoft が MSSECURE の更新を停止するまでは、MSSECURE データ フィードと Patch Manager を使用して更新の適用を継続できます。Microsoft は 2008 年以降も MSSECURE の更新を続けて

いますが、このマニュアルを作成している時点で、2007 年 10 月 9 日以降は MSSECURE の更新を行わないことを発表しています。69 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。

現在、Microsoft Office XP または Microsoft Office 2003 に Patch Manager と MSSECURE データ フィードを使用してパッチを適用しているお客様は、新しい Microsoft Update Catalog フィードに移行することをお勧めします。これにより、Microsoft が MSSECURE フィードを停止した後も、パッチ適用機能が継続されます。

Microsoft Office のサービス パック

HPCA Patch Manager 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 Manager 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。

- **MSSecure、Microsoft Update Catalog、Client Automation の場合**：依存サービス パックのあるブリテンの情報が製品探索時に収集されるため、Patch Manager レポートは、そのようなブリテンの判別に役立ちます。たとえば、Microsoft Project 2002 Gold をお使いのエージェント コンピュータにローカルにインストールしているとします。Patch Manager は、このコンピュータが MS05-005 に対して脆弱であると判断します。これは、Patch Manager 適合性 (デバイス別) レポートに掲載されます。Microsoft は、あるブリテンを適用する前に、指定のサービス パックのインストールを要求する場合があります。その場合、エージェント コンピュータに MS05-005 を配布する前に、Microsoft Project 2002 Service Pack 1 を配布する必要があります。そのサービス パックのアプリケーションが、そのブリテンで検出された脆弱性を排除する場合があります。たとえば、このサービス パックをインストールした後も、MS05-005 がインストールされていないため、エージェント コンピュータは依然として適合しません。すなわち、このエージェント コンピュータを適合させるには、Service Pack 1 を配布してから、MS05-005 を配布する必要があります。すべてのブリテンまたはサービス パックは、エージェント コンピュータがポリシーでそれらにアクセスする資格がない場合は配布されないため注意してください。
- **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 Manager 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 Manager 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 Manager 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 Manager および Microsoft Update Catalog について

Patch Manager 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=en-us*) を参照してください。

Patch Manager 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 Manager 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 Manager 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 Manager 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 Manager 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 Manager 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 Manager を導入しないでください。CM Patch Manager 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 Manager を有効にする場合、次のトピック「Patch Manager (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 Manager (バージョン 3.0.2 以上) での Microsoft Office 更新の有効化

Patch Manager 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 Manager 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 Manager を使用して Microsoft Office のパッチを配布する場合、Patch Manager 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、蜂 R および蜂 ACP 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 Manager 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 Manager 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 Manager 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 Manager 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。

- `Drive:\Program Files\Hewlett-Packard\CM\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 Manager ODBC データベースのテーブルに自動的にポストします。

Patch Manager Administrator のアイコン

Patch Manager Administrator を使用している場合、Reporting Server などの利用可能な機能にアクセスするためのアイコンが使用できます。

図 13　　クリックできるアイコン

-  アイコンをクリックすると、ページをリフレッシュできます。
-  アイコンをクリックすると、Patch Manager Administrator のホームページに戻ります。
-  アイコンをクリックすると、現在表示されているページを印刷します。
-  アイコンをクリックすると、Reporting Server を使用する Patch Manager Reporting に移動します。
-  アイコンをクリックすると、最新のブリテンの修正情報を参照できます。
-  アイコンをクリックすると、最新のエージェント更新情報を参照できます。

パッチの分析とレポート

HPCA Reporting Server では、Patch Manager の Web ベースのレポートが提供されます。Reporting Server のインストールおよび設定については、『*HPCA Reporting Server Guide*』を参照してください。Reporting Server のインストール メディアは、Client Automation Infrastructure メディアと一緒です。

レポートを表示するには、ツール　バー内にあるこのアイコンを使用して Reporting Server にアクセスします。 

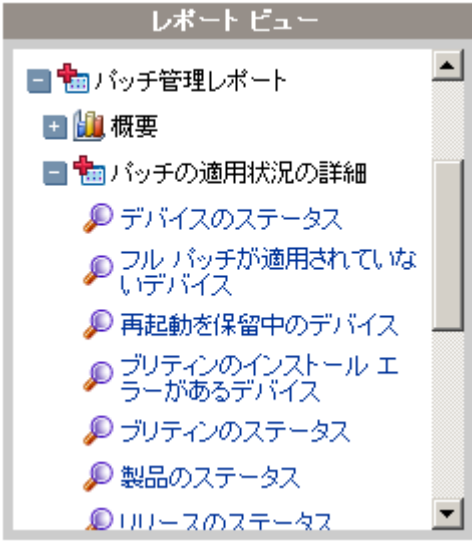
次に、[レポート ビュー] の下で、**[パッチ管理レポート]** をクリックし、レポートの一覧を展開します。

Patch Manager レポートには 4 つのタイプがあります。

- 116 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。
- 120 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。
- 130 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。
- 130 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。たとえば、112 ページの図 14 には、概要とパッチ適用状況の詳細を展開するパッチ管理レポートの一覧が示されています。

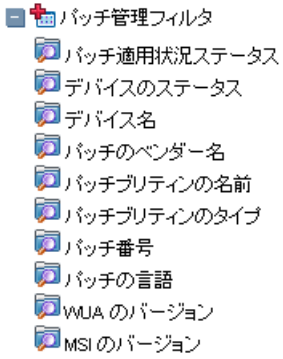
図 14　　パッチ管理レポートの一覧の表示



Reporting Server によるパッチ レポートのフィルタリング

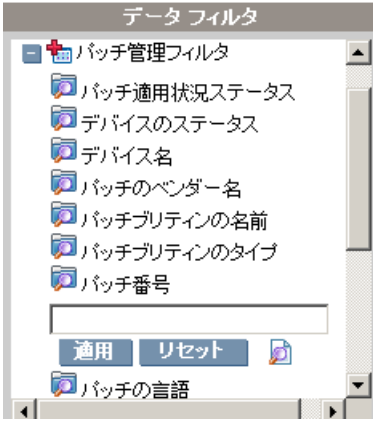
Reporting Server には、フィルタリング機能もあります。フィルタにアクセスするには、Reporting Server ページの検索制御セクションでパッチ管理の関連情報を展開します。

図 15　　パッチ管理の関連情報データ フィルタの表示



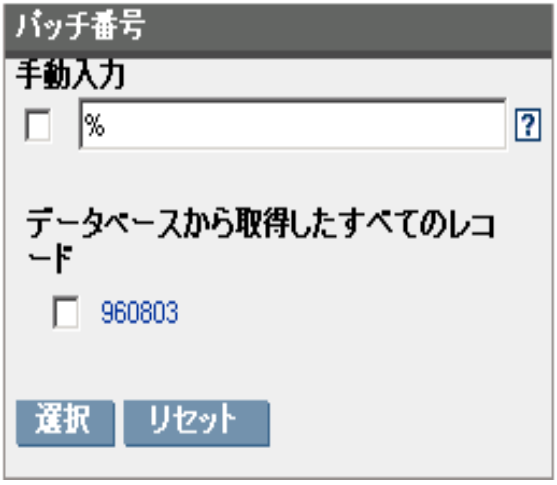
一部のフィルタではテキスト エントリしか使用できません。その他のフィルタには、使用できるオプションを表示するボタンやフィルタ検索ウィンドウを表示する虫眼鏡があります。

図 16　　フィルタの展開



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。

図 17　　フィルタの選択



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、『*Reporting Server Guide*』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 - このブリテンの掲示板をポストしたベンダーの Web サイトに移動する

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

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
グレイ	再起動の保留
濃いグレイ	適用できません

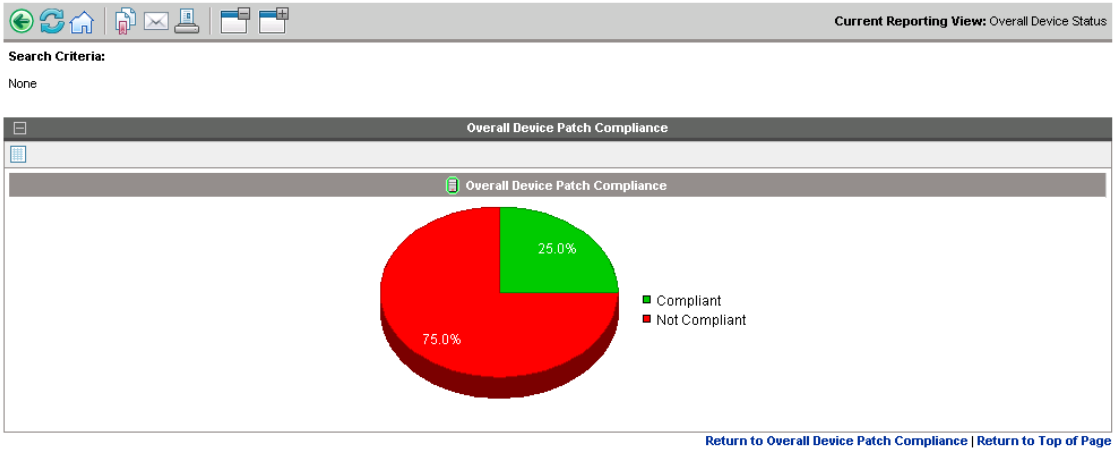
概要レポートのサンプルは次のとおりです。

- 117 ページの「デバイス全体のステータス」
- 118 ページの「デバイスのステータス」
- 119 ページの「ブリテンのステータス」
- 120 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

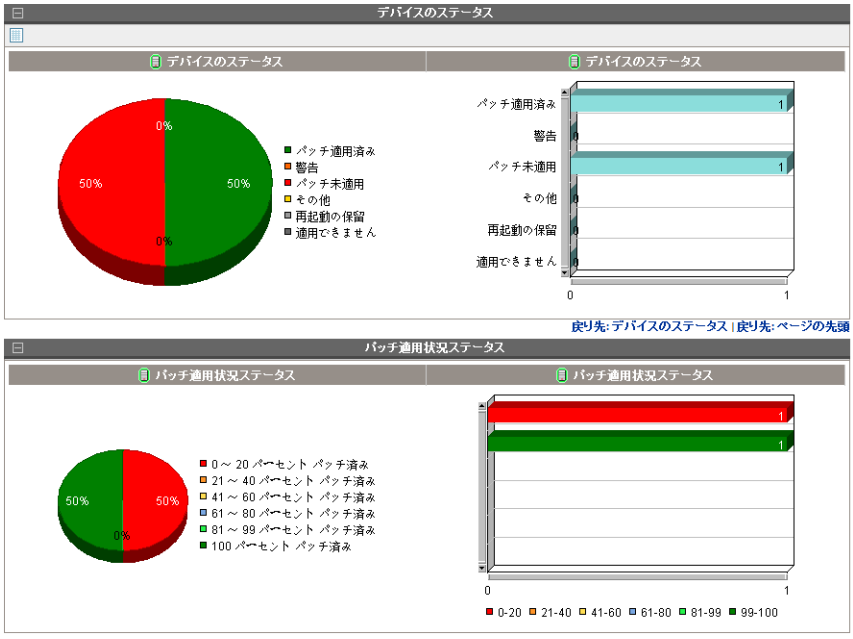
パッチ適用済みステータスに従って、デバイスの円グラフと棒グラフ詳細が示されます。使用できるグラフィカル レポートは以下の 2 つです。

- **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)。

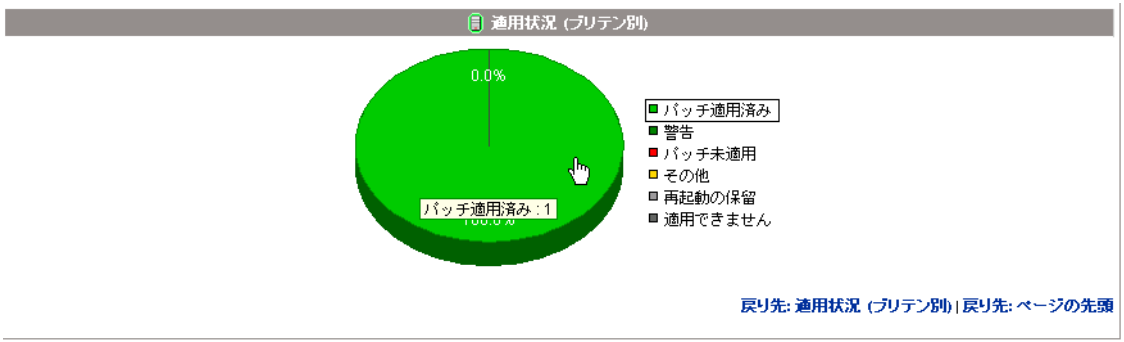


ブリテンのステータス

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 Manager Agent を実行している場合、製品およびパッチの情報は Patch Manager 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。

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 Manager 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 Manager 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 Manager 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 Manager 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。

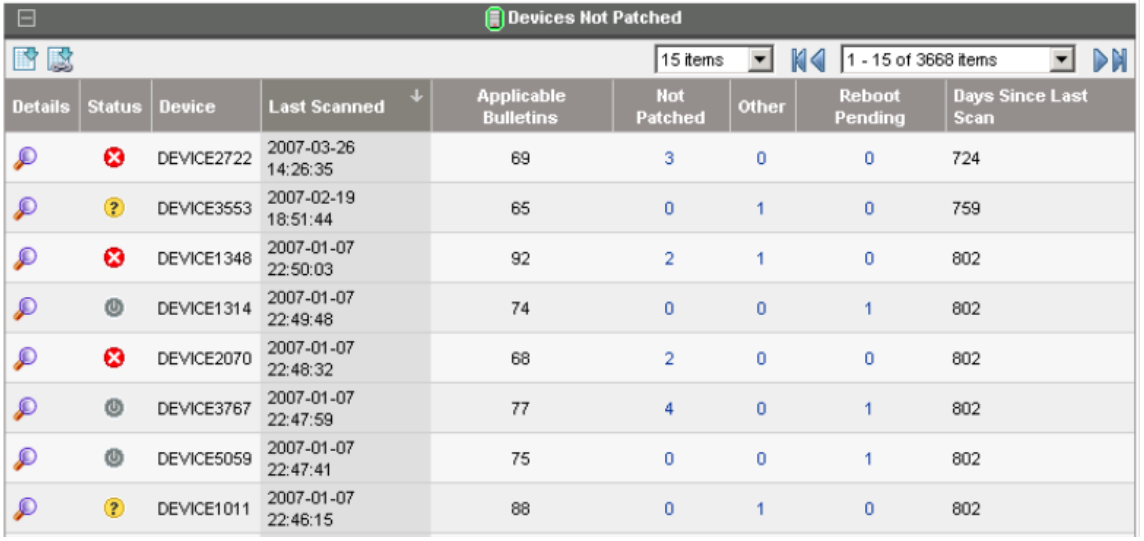
— [その他] 列の項目は、Patch Manager が検証できなかったパッチまたはデバイスのエラーにより適用できなかったパッチを示します。

— [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 121 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。



Devices Not Patched

15 items | 1 - 15 of 3668 items

Details	Status	Device	Last Scanned	Applicable Bulletins	Not Patched	Other	Reboot Pending	Days Since Last Scan
		DEVICE2722	2007-03-26 14:26:35	69	3	0	0	724
		DEVICE3553	2007-02-19 18:51:44	65	0	1	0	759
		DEVICE1348	2007-01-07 22:50:03	92	2	1	0	802
		DEVICE1314	2007-01-07 22:49:48	74	0	0	1	802
		DEVICE2070	2007-01-07 22:48:32	68	2	0	0	802
		DEVICE3767	2007-01-07 22:47:59	77	4	0	1	802
		DEVICE5059	2007-01-07 22:47:41	75	0	0	1	802
		DEVICE1011	2007-01-07 22:46:15	88	0	1	0	802

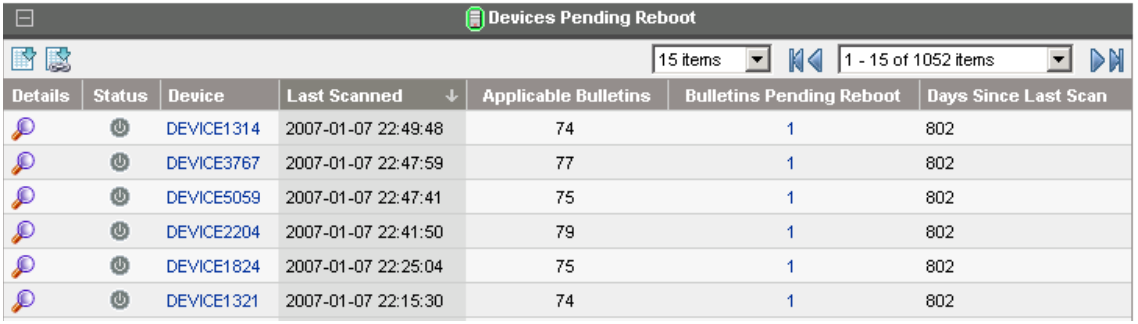
— 各デバイスに対して、121 ページの「デバイスのステータス」の適合性レポートで説明したものと同じ操作を実行できます。

— 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。



Devices Pending Reboot

15 items | 1 - 15 of 1052 items

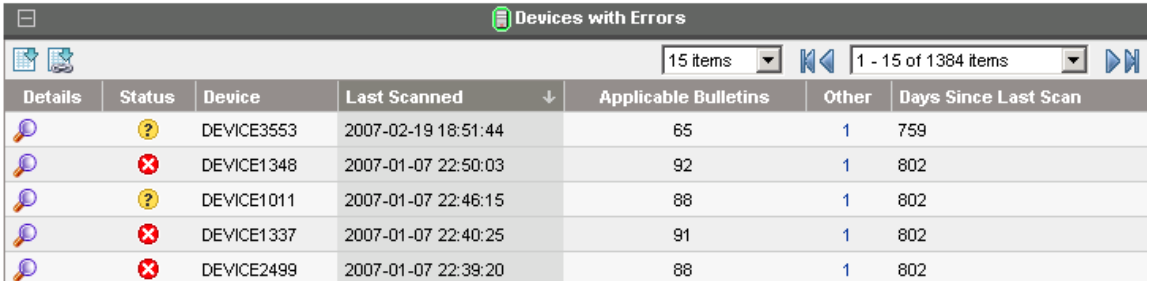
Details	Status	Device	Last Scanned	Applicable Bulletins	Bulletins Pending Reboot	Days Since Last Scan
		DEVICE1314	2007-01-07 22:49:48	74	1	802
		DEVICE3767	2007-01-07 22:47:59	77	1	802
		DEVICE5059	2007-01-07 22:47:41	75	1	802
		DEVICE2204	2007-01-07 22:41:50	79	1	802
		DEVICE1824	2007-01-07 22:25:04	75	1	802
		DEVICE1321	2007-01-07 22:15:30	74	1	802

— 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。



Devices with Errors

15 items | 1 - 15 of 1384 items

Details	Status	Device	Last Scanned	Applicable Bulletins	Other	Days Since Last Scan
		DEVICE3553	2007-02-19 18:51:44	65	1	759
		DEVICE1348	2007-01-07 22:50:03	92	1	802
		DEVICE1011	2007-01-07 22:46:15	88	1	802
		DEVICE1337	2007-01-07 22:40:25	91	1	802
		DEVICE2499	2007-01-07 22:39:20	88	1	802

— 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。例は次のとおりです。

適用状況 (デバイス別、ブリテン別)

15 項目 | 1 - 2 項目 (共に 2 項目)

ステータス	ブリテン	デバイス	タイトル	原因
	MS09-013	CAVMC10	Windows Security Updates (KB960803)	パッチ OK ブリテン MS09-013 - リスクは検出されませんでした
	MS09-013	CAVMC12	Windows Security Updates (KB960803)	パッチ OK ブリテン MS09-013 - リスクは検出されませんでした

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。

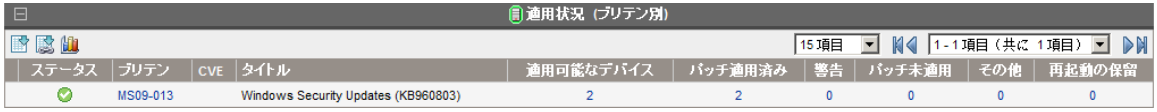
— 電源ボタンは、少なくとも 1 つのデバイスが適合するための再起動を保留していることを示します。

> 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 Manager 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 Manager 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 Manager 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 Manager 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。

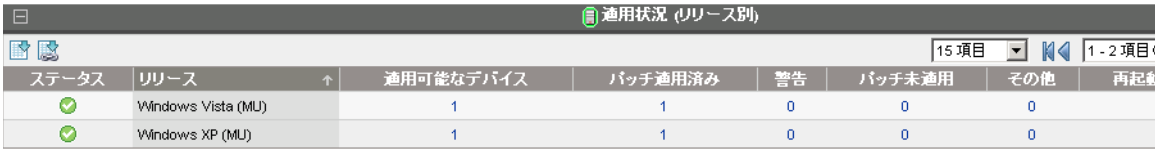
— (MSFT) の付いたリリース名では、「メタデータのダウンロードの有効化」がオンにされてブリテンが配布されています。

— 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、またはパッチ適用状況ステータス。



— 次の図のように、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。

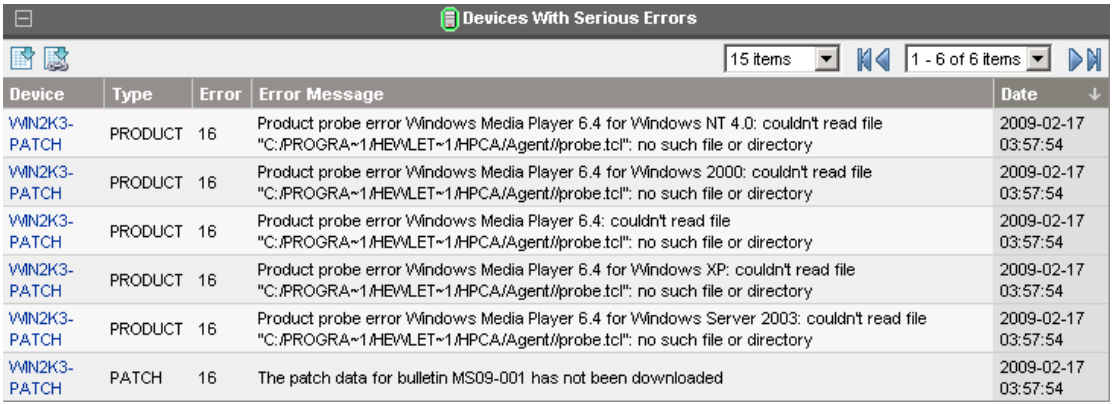
適用可能なフィルタ ：パッチの言語、パッチ番号、ブリテン名、およびパッチ適用状況ステータス。

— 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。

139 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。



Devices With Serious Errors

15 items | 1 - 6 of 6 items

Device	Type	Error	Error Message	Date
WIN2K3-PATCH	PRODUCT	16	Product probe error Windows Media Player 6.4 for Windows NT 4.0: couldn't read file "C:/PROGRA~1/HEWLET~1/HPCA/Agent//probe.tcl": no such file or directory	2009-02-17 03:57:54
WIN2K3-PATCH	PRODUCT	16	Product probe error Windows Media Player 6.4 for Windows 2000: couldn't read file "C:/PROGRA~1/HEWLET~1/HPCA/Agent//probe.tcl": no such file or directory	2009-02-17 03:57:54
WIN2K3-PATCH	PRODUCT	16	Product probe error Windows Media Player 6.4: couldn't read file "C:/PROGRA~1/HEWLET~1/HPCA/Agent//probe.tcl": no such file or directory	2009-02-17 03:57:54
WIN2K3-PATCH	PRODUCT	16	Product probe error Windows Media Player 6.4 for Windows XP: couldn't read file "C:/PROGRA~1/HEWLET~1/HPCA/Agent//probe.tcl": no such file or directory	2009-02-17 03:57:54
WIN2K3-PATCH	PRODUCT	16	Product probe error Windows Media Player 6.4 for Windows Server 2003: couldn't read file "C:/PROGRA~1/HEWLET~1/HPCA/Agent//probe.tcl": no such file or directory	2009-02-17 03:57:54
WIN2K3-PATCH	PATCH	16	The patch data for bulletin MS09-001 has not been downloaded	2009-02-17 03:57:54

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
- 取得 (パッチ別)

取得レポートの詳細については、88 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。

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] まで、[中] まで、[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。

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)

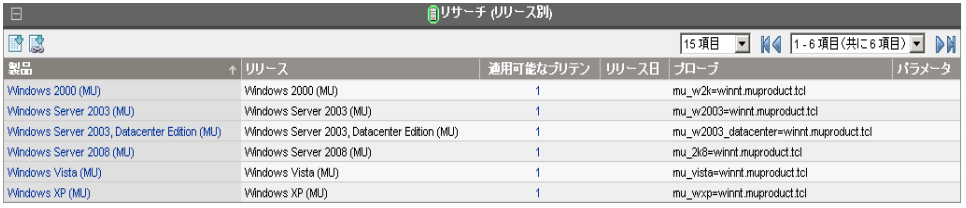
パッチ ファイルに関する情報を、取得ステータスを含めて表示するには、このレポートを使用します。Common Vulnerabilities Exposures の Web サイトに移動するには、[CVE] 列の数字をクリックします。[ダウンロード] 列のアイコンをクリックして、パッチ ファイルをダウンロードします。[重大度] 列のアイコンは、Windows パッチの重大度を示します。重大度の評価範囲は、[最重要] から、[重要] まで、[中] まで、[低] までです。パッチが Windows プラットフォーム用でない場合は、[不明] アイコンが表示されます。重大度が同じパッチをすべて表示するには、[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 Manager Agent。

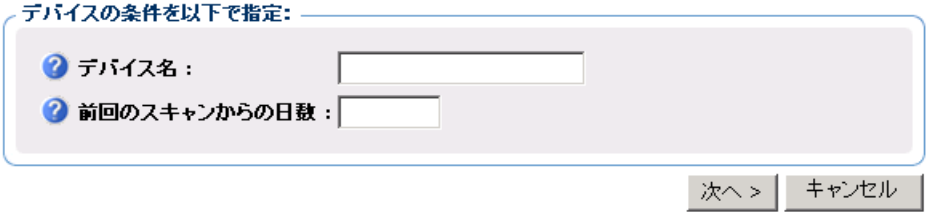
この例外を解決するには、デバイスで新しい探索を実行します。新しい探索で取得が切断される場合はエラーが解決されるか、接続性の問題が解決されます。また、操作できない Patch Manager Agent のトラブルシューティングで使用できるログが生成されます。リサーチ例外レポートは、リサーチ レポートの条件があまり厳しくないため、適合性例外レポートのデバイスの単なるサブセットとして表示されます。

デバイスの削除

Patch Administrator 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 Patch Manager Administrator の **[オペレーション]** 領域に移動して、**[デバイスを削除]** をクリックします。



2 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。

3 Patch Manager アドミニストレータを使用して、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。

4 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。

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 Manager 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、『HPCA Application Manager および Application Self-Service Manager 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、137 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 Manager 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 Manager 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 Manager 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 Manager サービスにより管理されます。このサービスは、Patch Manager 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 Manager 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 Manager 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 Manager 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 Manager 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、『Application Manager および Application Self-service Manager 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。

OPTIONS クラスに関する情報は、Microsoft Update ではなく、MSSECURE.XML を使用してダウンロードされたパッチに対してのみ適用されます。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 Manager 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 Manager に送信され、Patch Manager 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 Manager Server に過剰な負荷がかかる可能性があります。
- **使用**
  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。

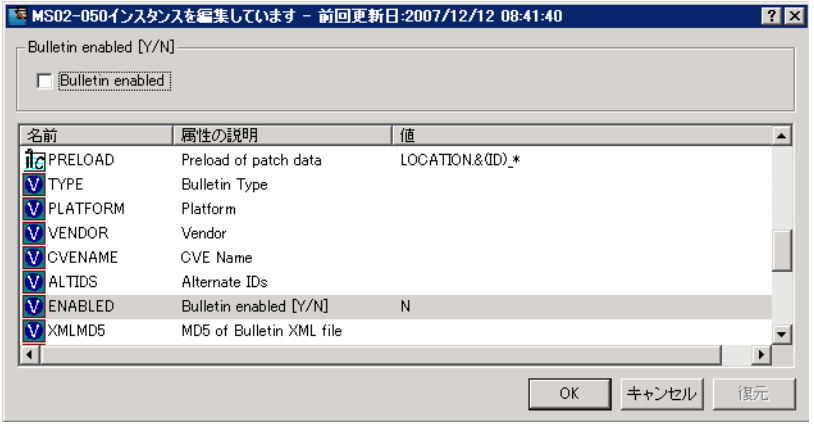
3 REPORT しきい値を設定します。ファイルまたはレジストリ キーのプロパティは、この値に基づいて Patch Manager に送信されます。リターン コードが REPORT 属性の値以上の場合、そのファイルとレジストリの情報は Patch Manager に送信され、Patch Manager レポートで使用できるようになります。たとえば、リターン コードが 4 (警告) または 8 (エラー) の場合、REPORT を 1 に設定してプロパティを送信します。

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。

図 18　　ブリテン MS00-001 の検出の無効化



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 Manager 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。

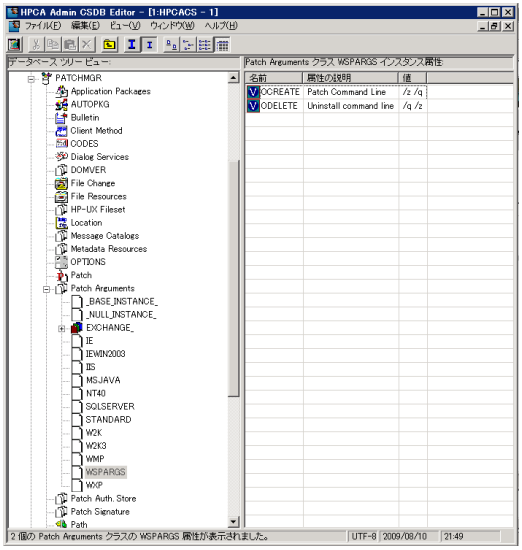
PATCHARG オプションは、Microsoft Update ではなく MSSECURE.XML を使用してダウンロードしたパッチにのみ適用されます。Microsoft Update からパッチを取得する場合、レポートの [ソース] 列には「Microsoft」ではなく「Microsoft Update」と表示されます。

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

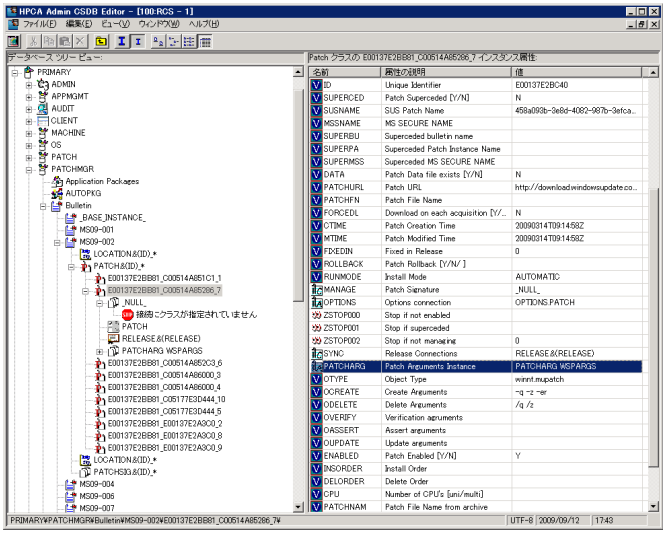
1 Admin CSDB Editor を使用して、PATCHMGR ドメインの PATCHARG クラスに移動します。

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。次の図のように、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。

Client Automation Proxy Server のプレロード

Client Automation Proxy Server を使用する場合、パッチ ファイルをプレロードすることがあります。プレロードするには、POLICY ドメインのプレロード ユーザー インスタンス (Proxy Server のデフォルトは **RPS**) に移動します。プレロード ユーザー インスタンスがまだない場合は作成します。DISCOVER_PATCH サービスと、ダウンロードするブリテンのサービスに接続を追加する必要があります。ダウンロードするブリテンの最後にサフィックスとして **(PRELOAD)** を付けます。たとえば、MS03-039 ブリテンだけをプレロードするには、**PATCHMGR.ZSERVICE.MS03-039(PRELOAD)** に接続を追加します。ブリテン名にはワイルドカードが使用できます。MS03 で始まるすべてのブリテンをプレロードする場合は、接続インスタンスに **PATCHMGR.ZSERVICE.MS03-*(PRELOAD)** と入力します。

次にプレロードを実行するときに、Proxy Server は圧縮されたデータ ファイルを PATCHMGR ドメインからロードします。プレロードの詳細については、『*HP Client Automation Proxy Server Installation and Configuration Guide* (*Proxy Server Guide*』を参照してください。

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 Manager 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。

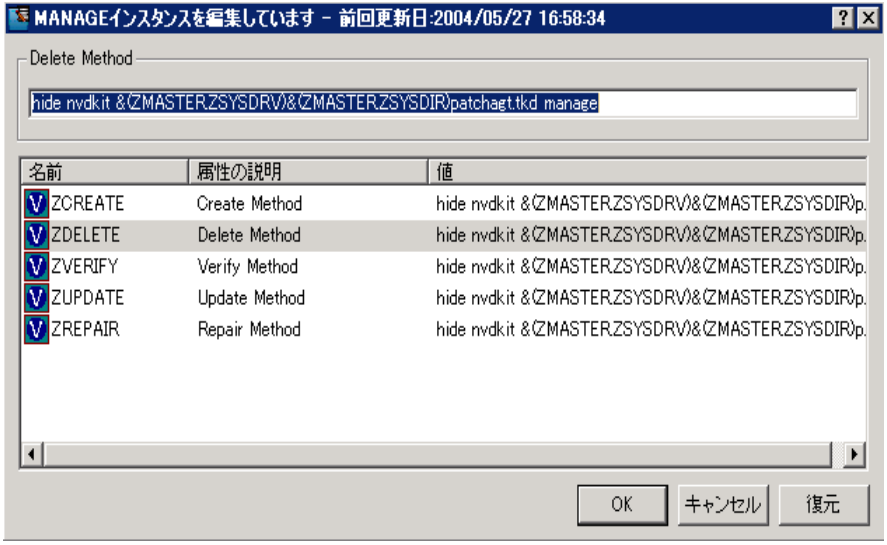
詳細については、147 ページの「パッチの削除」を参照してください。

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 Manager 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

- 管理するデバイスに Patch Manager Agent をインストールします。
- Patch Manager 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、151 ページの図 19 の後の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 19　　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 ソース：MSSECURE.XML
URL	URL	Bulletin URL ソース：MSSECURE.XML
FAQURL	FAQURL	FAQ URL ソース：MSSECURE.XML
Supported	SUPPORT	Supported [Y/N] ソース：MSSECURE.XML
ImpactSeverityID	IMPACT	ImpactID ソース：MSSECURE.XML、Red Hat Network、Novell (SuSE) のデータ フィード
MitigateSeverityID	MITIGATE	Mitigate ID ソース：MSSECURE.XML
PreReqSeverityID	PREREQ	Prereq ID ソース：MSSECURE.XML
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：MSSECURE.XML、Red Hat Network、Novell (SuSE) のデータ フィード

表 5　　BULLETIN クラスの XML タグ

XML タグ	HPCA 属性	説明
ソース	SOURCE	ソース [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。
ベンダー	VENDOR	MICROSOFT/REDHAT/SUSE
タイプ	TYPE	Type of Bulletin Security/ServicePack/Other
プラットフォーム	PLATFORM	winnt//redhat/suse
Name	NAME	External ID ソース：MSSECURE.XML、Red Hat Network、Novell (SuSE) のデータ フィード
タイトル	タイトル	タイトル ブリテンのタイトル。 ソース：MSSECURE.XML、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：MSSECURE.XML、Red Hat Network、Novell (SuSE) のデータ フィード
スキーマのバージョン		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。

表 5　　BULLETIN クラスの XML タグ

XML タグ	HPCA 属性	説明
	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。
配布	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

Product 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：MSSECURE.XML、Red Hat Network、Novell (SuSE) のデータフィード
Name	NAME	ソース：MSSECURE.XML、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：MSSECURE.XML、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：MSSECURE.XML/SUS、Red Hat Network、Novell (SuSE) のデータ フィード
再起動	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：MSSECURE.XML/SUS、Red Hat Network、Novell (SuSE) のデータ フィード
アーキテクチャ	ARCH	x86/i64 ソース：MSSECURE.XML/SUS、Red Hat Network、Novell (SuSE) のデータ フィード
言語	LANG	en、fr、de ソース：SUS
MSSUSName	SUSNAME	MSSECURE.XML からのパッチの SUS 名。 ソース：MSSECURE.XML

表 8　　PATCH クラスの XML タグ

XML タグ	HPCA 属性	説明
SupercededByBulletin	SUPERBU	このパッチより優先されるブリテン名。 ソース：MSSECURE.XML、 Red Hat Network、Novell (SuSE) のデータ フィード
SupercededByMSPatch	SUPERMSS	このパッチより優先される MSSECURE パッチ名。 ソース：MSSECURE.XML
置換されるパッチ	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：MSSECURE.XML、 Red Hat Network、Novell (SuSE) のデータ フィード
MSSecureName	MSSNAME	このパッチの MSSECURE 名。 ソース：MSSECURE.XML
OSVersion	OSVER	オペレーティング システムのバージョン
QNumber	QNUMBER	MSSECURE.XML からのパッチの QNUMBER。 ソース：MSSECURE.XML
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。
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。
プラットフォーム	PLATFORM	プラットフォーム タイプ： winnt、redhat、suse

表 8　　PATCH クラスの XML タグ

XML タグ	HPCA 属性	説明
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
	ID	このパッチに対して HPCA-CSDB で作成された一意の ID。

表 8　　PATCH クラスの XML タグ

XML タグ	HPCA 属性	説明
	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 : MSSECURE.XML、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
配布	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。 ソース : MSSECURE.XML
パス	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。 ソース : MSSECURE.XML
CRC32	CRC32	データの CRC。
Gmttime	GMTTIME	YYYYMMDD で示される GMTDATE 。 ソース : MSSECURE.XML
Gmtdate	GMTDATE	HH:MM:SS で示される GMTTIME。 ソース : MSSECURE.XML

表 9　　FILECHG クラスの XML タグ

XML タグ	HPCA 属性	説明
サイズ	SIZE	ファイルのサイズ。 ソース : MSSECURE.XML
Checksum	CHECKSUM	ファイルのチェックサム。 ソース : MSSECURE.XML
バージョン	バージョン	ファイルのバージョン。 ソース : MSSECURE.XML
	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。 ソース : MSSECURE.XML
パス	PATH	フルパスで指定するレジストリ キー名。 ソース : MSSECURE.XML
Value	VALUE	レジストリに格納されたデータ値。 ソース : MSSECURE.XML
タイプ	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 ソース : MSSECURE.XML
	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

表 10　　REGCHG クラスの XML タグ

XML タグ	HPCA 属性	説明
	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
タイプ	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 ソース : MSSECURE.XML
	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	バージョン	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 Manager 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 20　　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。

図 21　　再起動パネルを [OK] ボタンのみを表示するように変更

再起動修飾子 : 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 Manager 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。

再起動修飾子 : 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 Policy Server の統合

企業で、HP Client Automation Policy Server (Policy Server) を使用してエンタイトルメントを作成する場合、接続パラメータに基づいて Policy Server がサービスを割り当てるドメインをフィルタリングできます。

Policy Server を Patch Manager と一緒に使用する場合、通常のソフトウェア サービスと Patch Manager のソフトウェア サービスの解決を区別する必要があります。Policy Server は、radskman コマンド ラインで渡される dname に基づいてサービスをフィルタリングします。

Policy Server の設定ファイル `pm.cfg` には、次の形式のフィルタ設定が含まれます。

```
DNAME=<DOMAIN NAME>  { rule }
```

ここで、DOMAIN NAME は RADISH によって dname に渡される値です。この Patch Manager Agent の場合は、radskman の dname になります。dname は「patch」です。dname に渡されたフィルタ名が `pm.cfg` に見つからない場合、フィルタ `DNAME=*` が使用されます。Policy Server で最低限必要なバージョンは、バージョン 5.0 です。

これらのフィルタのデフォルトの設定は、以下のとおりです。

```
DNAME=*       { * !PATCHMGR !OS }

DNAME=PATCH   { PATCHMGR }

DNAME=OS      { OS }
```

この設定で、デフォルト ルール (*) は PATCHMGR および OS ドメインを無視し、それ以外はすべて許可します。「!」で示されるドメインは無視されます。PATCH および OS ルールは、それぞれ PATCH および OS ドメインのポリシーのみを許可します。インスタンスについて、OS Manager 解決のすべてのポリシーを許可する場合は、最後のフィルタを `DNAME=OS { * }` のように変更します。

D Patch.cfg のパラメータ

この付録では、Patch Manager 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 Patch Manager Administrator 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 Manager Server の設定パラメータ

HP は、Patch Manager Administrator に Patch Manager パラメータを設定することをお勧めしています。Patch Manager Administrator を使用できない場合は、patch.cfg ファイルの中で直接変更することができます。デフォルト ロケーションは、*Drive*:\Program Files\Hewlett-Packard\CM\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 Manager 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**: Patch Manager Administrator に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 Manager 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。デフォルトのロケーションは、*Drive*:\Program Files\Hewlett-Packard\CM\PatchManager\data\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**: Patch SQL データベースに**データ ソース名 (DSN)** を指定します。このパラメータは必須です。
- **dsn_user**: Patch SQL データベースの DSN に SQL ユーザー名を指定します。
- **dsn_pass**: Patch SQL データベースの DSN の SQL ユーザーに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 Manager 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 Manager 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**: ファイルがすべてダウンロードされ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 Manager 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。
- **microsoft_url**: Microsoft の MSSECURE.XML ファイルの URL を指定します。デフォルトは **http://download.microsoft.com/download/0/d/b/0db2e5d7-0ba9-4856-b51f-db7c0b838c68/MSSecure_1033.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 Manager 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 Manager は、取得時にまず適切なディレクトリで `.rpm` パッケージを検索します。次に例を示します。

— x86 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、54 ページの「Red Hat のフィード設定」の **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/

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/

- **suse10_user**: SuSE 10 および 11 のセキュリティ 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。
- **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 Manager Server のコマンド プロンプトから、Patch Manager 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。

System Drive:\Program Files\Hewlett-Packard\CM\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 肪ulletins 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、第 2 章、「Patch Manager 環境の作成」で、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 Manager には、Red Hat セキュリティ アドバイザリを個別に指定してください。
  - SuSE セキュリティ パッチは、命名規則として SUSE-PATCH-#### を使用します。ここで、### は SuSE によって指定されるナンバリング スキームです。

  ブリテンをダウンロードしない場合は、肪 ulletins 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 Manager 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。デフォルトのロケーションは、*Drive*:\Program Files\Hewlett-Packard\CM\PatchManager\data\patch です。
- **force**: 以下の場合に force 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、ブリテンは force の値に関係なく削除してから再取得されます。
- **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*
```

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

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。

- **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ンは削除され、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::2.1es、REDHAT::3ws、REDHAT::4as、
  REDHAT::2.1es-x86_64、REDHAT::3ws-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 Manager 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**: Patch ODBC データベースにデータ ソース名 (DSN) を指定します。このパラメータは必須です。
- **dsn_user**: Patch ODBC データベースの DSN にユーザーを指定します。
- **dsn_pass**: Patch ODBC データベースのユーザーに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 Manager Agent ファイルのメンテナンス用です。詳細については、97 ページの「Patch Manager Agent の更新」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 Manager 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 Manager 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 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。

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
BUILD 899
CFG_VER 7.5
DATA_DIR { C:/Program Files/Hewlett-Packard/CM/PatchManager/data}
DL_DATEFMT {%Y-%m-%d %T}
DSN PATCH
DSN_USER sa
ETC C:/Program Files/Hewlett-Packard/CM/PatchManager/etc/patch
FORCE no
FTP_PASS {{AES256}vQP8q3G7N5j4iMhgA2QUuw==}
HOME C:/Program Files/Hewlett-Packard/CM/PatchManager/modules/patch.tkd
HTTP_RETRIES 2
LABEL PATCH
LANGUAGE {}
LOG C:/Program Files/Hewlett-Packard/CM/PatchManager/logs
MODE both
MODULE patch
RCS_URL radia://localhost:3464
RCS_USER RAD_MAST
REPLACE no
RETIRE {}
ROOT C:/Program Files/Hewlett-Packard/CM/PatchManager/
SECTION all
TITLE {HPCA Patch Manager}
URL /patch
USING_DEFAULT_PATCH_CFG Y
VENDOR_OS_FILTER {}
VERSION {7.50.000}
}
```

索引

N

O

P

Q

R

S

T

U

V

W

X

Z

あ

い

え

か

き

け

さ

し

せ

そ

た

ち

て

は

ふ

む

も

り

れ

ろ