HP Server Automation

Ultimate Edition

ソフトウェアバージョン: 10.10

ユーザーガイド: サーバーのパッチ適用

ドキュメントリリース日: 2014年6月30日 (英語版)
ソフトウェアリリース日: 2014年6月30日 (英語版)

ご注意

保証

HP製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載は、追加保証を提供するものではありません。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。

ここに記載する情報は、予告なしに変更されることがあります。

権利の制限

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、HPからの有効な使用許諾が必要です。商用コンピューターソフトウェア、コンピューターソフトウェアに関する文書類、および商用アイテムの技術データは、FAR12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

商標について

Adobe®は、Adobe Systems Incorporated (アドビシステムズ社)の登録商標です。

Intel®およびItanium®は、Intel Coporationの米国およびその他の国における登録商標です。

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

OracleとJavaは、Oracle Corporationおよびその関連会社の登録商標です。

UNIX®は、The Open Groupの登録商標です。

サポート

次のHPソフトウェアサポートオンラインのWebサイトを参照してください。

http://support.openview.hp.com

このサイトでは、HPのお客様窓口のほか、HPソフトウェアが提供する製品、サービス、およびサポートに関する詳細情報をご覧いただけます。

HPソフトウェアオンラインではセルフソルブ機能を提供しています。お客様のビジネスを管理するのに必要な対話型の技術サポートツールに、素早く効率的にアクセスできます。HPソフトウェアサポートのWebサイトでは、次のようなことができます。

- 関心のあるナレッジドキュメントの検索
- サポートケースの登録とエンハンスメント要求のトラッキング
- 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サポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部のサポートを除き、サポートのご利用には、HP Passportユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HP Passport IDを登録するには、次のWebサイトにアクセスしてください。

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

アクセスレベルの詳細については、次のWebサイトをご覧ください。

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

サポートマトリクス

サポートおよび互換性情報については、関連する製品リリースのサポートマトリクスを参照してください。サポートマトリクスと製品マニュアルは、次のHPソフトウェアサポートオンラインのWebサイトで参照できます。

http://h20230.www2.hp.com/sc/support_matrices.jsp

また、本リリースの『HP Server Automation Support and Compatibility Matrix』は、次の HP ソフトウェアサポートオンラインの製品マニュアルWebサイトからダウンロードできます。

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

ドキュメントの更新情報

このリリースのServer Automation製品の最新のドキュメントは、すべて次のSA Documentation Libraryから入手できます。

http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html

SA Documentation Library では、このリリースに関連するガイドライン、リリースノード、サポートマトリクス、およびホワイトペーパーにアクセスできます。また、フルドキュメントセットを一括してダウンロードすることもできます。SA Documentation Library は、リリースごとに更新されます。また、リリースノートが更新されたときや、新しいホワイトペーパーが発行されたときにも更新されます。

情報リソースを見つける方法

Server Automationの情報リソースは、次のいずれの方法でもアクセスできます。

方法1: 新しいSA Documentation Libraryから、最新のドキュメントにタイトルとバージョンを指定してアクセスします。

方法2: [All Manuals Download] からローカルディレクトリにフルドキュメントメントセットを保存します。

方法 3: サポートされるリリースの HP 製品ドキュメントを HP ソフトウェアドキュメントポータルで検索します。

各ドキュメントにアクセスするには、次の手順を実行します。

1. SA 10.x Documentation Libraryにアクセスします。

   http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html

2. HP Passportの資格情報を使ってログインします。
3. ドキュメントのタイトルとバージョンを指定して、[**go**] をクリックします。

ローカルディレクトリ内の完全なドキュメントセットを使用するには、次の手順を実行します。

1. フルドキュメントセットをローカルディレクトリにダウンロードするには、次の手順を実行します。
   a. SA Documentation Libraryにアクセスします。

      http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html

   b. HP Passportの資格情報を使ってログインします。
   c. SA 10.1バージョンの [All Manuals Download] タイトルを探します。
   d. [**go**] リンクをクリックして、ローカルディレクトリにZIPファイルをダウンロードします。
   e. ファイルを解凍します。
2. ローカルディレクトリ内のドキュメントを探すには、ドキュメントカタログ (docCatalog.html) を使用します。ローカルディレクトリにダウンロードしたドキュメントの索引ポータルが表示されます。
3. ドキュメントセット内のすべてのドキュメントを対象としてキーワードを検索するには、次の手順を実行します。
   a. ローカルディレクトリ内の任意のPDFドキュメントを開きます。
   b. [**編集**] > [**高度な検索**] を選択します (またはShift＋Ctrl＋Fキー)。
   c. [以下の場所にあるすべてのPDF文書] オプションを選択し、ローカルディレクトリを指定します。
   d. キーワードを入力し、[検索] をクリックします。

HPソフトウェアドキュメントポータルで追加ドキュメントを探すには、次の手順を実行します。

HPソフトウェアドキュメントポータルにアクセスします。

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

このサイトを利用するには、HP Passport への登録とサインインが必要です。HP Passport ID の登録は、HP Passportのサインインページの [**New users - please register**] 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お申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、HP の営業担当にお問い合わせください。改訂状況については、「ドキュメントの更新情報」を参照してください。

製品エディション

Server Automationには、次の2つの製品エディションがあります。

- Server Automation (SA) は、Server AutomationのUltimate Editionです。Server Automationについては、『SAリリースノート』および『SAユーザーガイド: Server Automation』を参照してください。
- Server Automation Virtual Appliance (SAVA) は、Server AutomationのPremium Editionです。SAVAの機能については、『SAVA Release Notes』および『SAVAクイックガイド』を参照してください。

ドキュメントの更新情報

次の表は、前回リリースされたエディション以降の本ドキュメントに対する変更を示します。

日付	変更内容
2014年7月9日 (英語版)	SA 10.1に伴う本ドキュメントのオリジナルリリース。

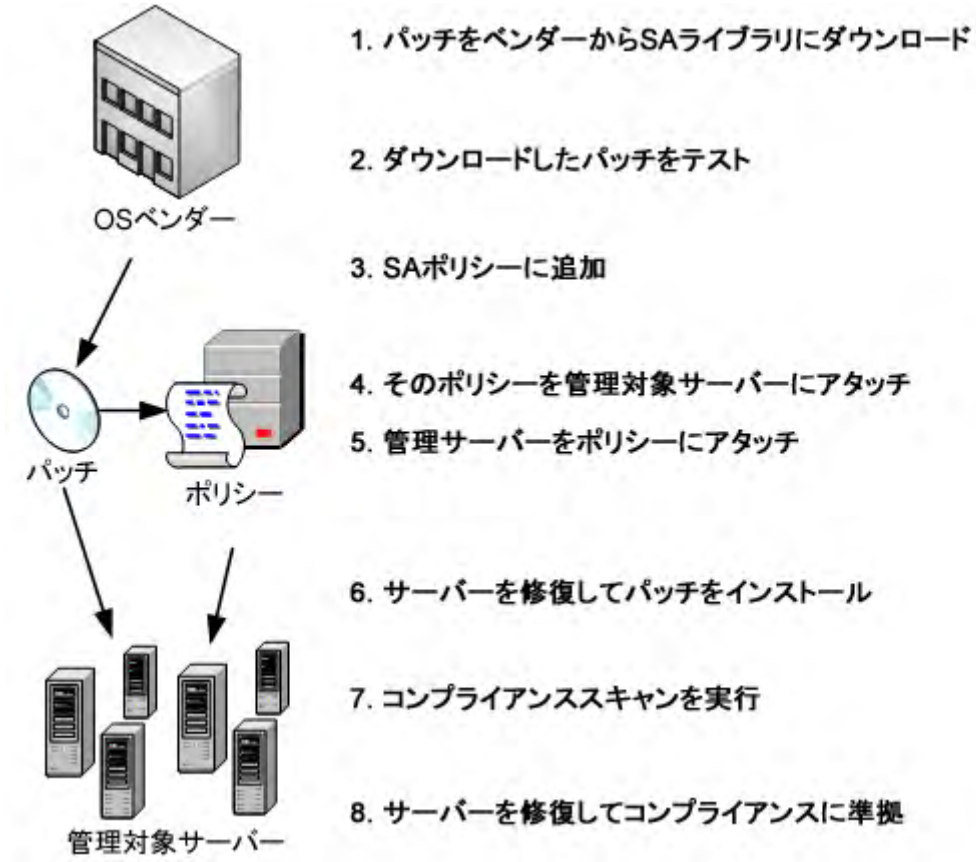
目次

第1章 パッチ管理のクイックスタート

このクイックスタートでは、IT環境内のSA管理対象サーバーでパッチのダウンロード、インストール、メンテナンスを行う手順の概要について説明します。ここでは、サポート対象のすべてのオペレーティングシステムで、パッチの設定と管理に必要な手順を示します。

図1は、パッチのダウンロード、パッチのテスト、SAポリシーへのパッチの追加、サーバーに対するポリシーのアタッチ、ポリシーに対するサーバーのアタッチ、サーバーの修復によるパッチのインストール、コンプライアンススキャンの実行によるコンプライアンス違反状態のサーバーの特定、およびサーバーをコンプライアンス状態に戻すためのサーバーの修復を行う一般的なワークフローです。SAポリシーはパッチポリシーまたはソフトウェアポリシーのいずれかで、パッチを適用するオペレーティングシステムに応じて使用します。

図1　　パッチ管理のワークフロー



特定のオペレーティングシステムでのSAパッチ管理の詳細については、次の各項を参照してください。

- Windowsパッチ管理 (17ページ)
- HP-UXパッチ管理 (93ページ)
- Solarisパッチ管理 (113ページ)

- Solaris 11パッチ管理 (157ページ)
- Ubuntuパッチ管理 (169ページ)
- Unixパッチ管理 (211ページ)
- Oracle Enterprise Linuxパッチ管理 (239ページ)

第2章 Windowsパッチ管理

概要

HP Server Automation (SA) では、Windowsパッチ管理により、Microsoft® Windowsパッチの確認、インストール、削除を行い、組織内の管理対象サーバーのセキュリティを確保することができます。SAでサポートされる管理対象サーバープラットフォームのセキュリティ脆弱性に対して、対応するパッチを確認してインストールすることができます。

お使いのバージョンのSAでサポートされる管理対象サーバープラットフォームについては、『SA Support and Compatibility Matrix』を参照してください。

SA ではパッチ管理の主要な機能が自動化されていますが、パッチのインストール方法やインストール条件は、細かく制御することができます。パッチ適用プロセスを自動化することで、パッチ適用に伴うダウンタイムを短縮できます。また、SAでは、パッチアクティビティのスケジュールを設定することで、ピーク以外の時間帯にパッチを適用することができます。

Windows ではセキュリティ上の脅威に対処するパッチが頻繁にリリースされます。システムのセキュリティ被害を未然に防ぐには、迅速にパッチを適用する必要があります。ただし、パッチを誤って適用すると、パフォーマンスの低下や重大なエラーなど深刻な問題が発生する原因になるので注意が必要です。

パッチ管理では、新しく検出された脅威に迅速対応できるだけでなく、パッチインストールの厳格なテストと標準化をサポートします。さらに、パッチが原因で問題が発生する場合には、テストと承認の後であっても、Windowsパッチ適用では安全かつ標準化された方法でパッチをアンインストールできます。

本書では、パッチポリシーを使用して Windows パッチをインストールする方法、および一連のタスクを使用してパッチをアンインストールする方法について説明します。また、パッチコンプライアンススキャンの実行とパッチポリシーのコンプライアンスレポートの作成についても説明します。

機能

SAでは、次のような機能や特徴を利用して、Windowsパッチ適用を自動化しています。

- **セントラルリポジトリ**: パッチがそれぞれの標準形式で保存され、整理されます
- **データベース**: これまでに適用したすべてのパッチの情報を保存します
- **カスタマイズスクリプト**: パッチのインストールの前後に実行できます
- **高度な検索機能**: パッチの適用が必要なサーバーを識別できます
- **監査機能**: 重要なパッチのデプロイメントをトラッキングします
- **マルチバイナリパッチサポート**: Windowsマルチバイナリパッチのインストールが可能です
- **すべてのWindows製品サポート**: 任意のWindows製品またはオペレーティングシステムのパッチ適用に対応します

これらの機能や特徴を利用することで、特定のオペレーティングシステムのパッチの参照、パッチのダウンロードとインストールのスケジュール設定、電子メール通知の設定、パッチインストールのプレビュー、ポリシーと修復によるパッチのインストール、再利用可能なファイル形式へのパッチ情報のエクスポートなどを実行できます。パッチの参照のタイプ

SAクライアントのインタフェースでは、Windowsパッチがオペレーティングシステム別に構成され、Microsoftセキュリティ情報などの各パッチに関する詳細なベンダーセキュリティ情報が表示されます。Microsoftがパッチをリリースした日付、セキュリティレベル、セキュリティ情報番号、QNumberなどを使用して、パッチを参照することができます。また、サーバーにインストールされているすべてのパッチを参照し、パッチメタデータを表示して編集することもできます。

スケジュール設定と通知

SAクライアントでは、MicrosoftからServer Automationにパッチを(スケジュールまたはオンデマンドで)インポートするタイミング、およびこれらのパッチを管理対象サーバーにダウンロードするタイミングを個別にスケジュール設定できます。

ベストプラクティス: パッチのインストールは業務への影響の最も少ない日時にスケジュール設定します。

Windowsパッチ適用では、ダウンロードやインストール操作の完了や成否に関する通知を受け取るように、電子メール通知を設定することもできます。パッチのインストールをスケジュール設定する際には、再起動設定を指定して、ベンダーの再起動オプションの使用、無効化、延期、または抑制を設定することもできます。

パッチポリシーと例外

管理対象サーバーまたはサーバーグループでパッチの確認と配布を柔軟に行えるように、Windowsパッチ適用では、インストールが必要なパッチのグループを定義したパッチポリシーを作成することができます。

パッチポリシーを作成してサーバーまたはサーバーグループにアタッチすることにより、組織内でインストールするパッチとそのインストール先を効果的に管理することができます。特定のパッチをパッチのインストールに追加または除外する必要がある場合は、特定のパッチをパッチポリシー例外に指定して、パッチポリシーと異なる処理を行うことができます。

追加するパッチとは、パッチポリシーで未指定のパッチで、パッチのインストールに含める必要のあるパッチです。パッチのインストールから除外するパッチとは、パッチポリシーで指定済みのパッチで、パッチポリシー例外でインストール対象から外す必要のあるパッチです。

ベストプラクティス: 特定のWindowsパッチが原因でサーバーやアプリケーションが正常に機能しなくなる可能性があることがわかっている場合は、パッチポリシー例外を作成して、該当するサーバーまたは該当するアプリケーションを含むすべてのサーバーで、そのパッチをインストール対象から除外する必要があります。

パッチインストールのプレビュー

パッチ管理では、新しく見つかったセキュリティ脆弱性に迅速に対応できるだけでなく、パッチインストールの厳格なテストと標準化もサポートされます。

インストールするパッチの確認後、実際にパッチをインストールする前に、パッチ管理でパッチインストールをシミュレート(プレビュー)することができます。パッチのプレビューを使用して、パッチのインストール対象として選択したサーバーに該当するパッチがすでにインストールされているかどうかを確認します。システム管理者がパッチを手動でインストールしている場合、サーバーにパッチがすでにインストールされている可能性があります。

プレビューでは、サーバーのパッチの状態に関する最新のレポートが作成されます。プレビューでは、特定のWindows製品を必要とするパッチ、および他のパッチよりも優先されるパッチや他のパッチの方が優先されるパッチなどの、依存関係情報や優先情報に関するレポートが作成されます。

パッチアンインストールのプレビュー

パッチ管理には、パッチのインストールが原因で正しく動作していないサーバーを修復するためのソリューションも用意されています。パッチのインストールが原因で問題が発生した場合には、テストと承認の後であっても、Windowsパッチ適用で安全かつ標準化された方法でパッチをアンインストールできます。アンインストールオプションを指定して、サーバーの再起動とアンインストールコマンド、アンインストール前スクリプト、アンインストール後スクリプトの実行を制御することができます。パッチインストールのプレビューと同様に、パッチアンインストールのプレビューを行うこともできます。

パッチデータのエクスポート

サーバーまたはサーバーグループのパッチ状態のトラッキングに役立つように、パッチ管理では、パッチデータをエクスポートできます。パッチデータはカンマ区切り(.csv)ファイルにエクスポートできます。このデータには、パッチがインストール済みとして最後に検出された日時、Server Automationでパッチがインストールされた日時、パッチのコンプライアンスレベル、パッチポリシー例外などに関する詳細情報が含まれます。エクスポートしたデータはスプレッドシートやデータベースにインポートして、さまざまなパッチ分析タスクを実行できます。

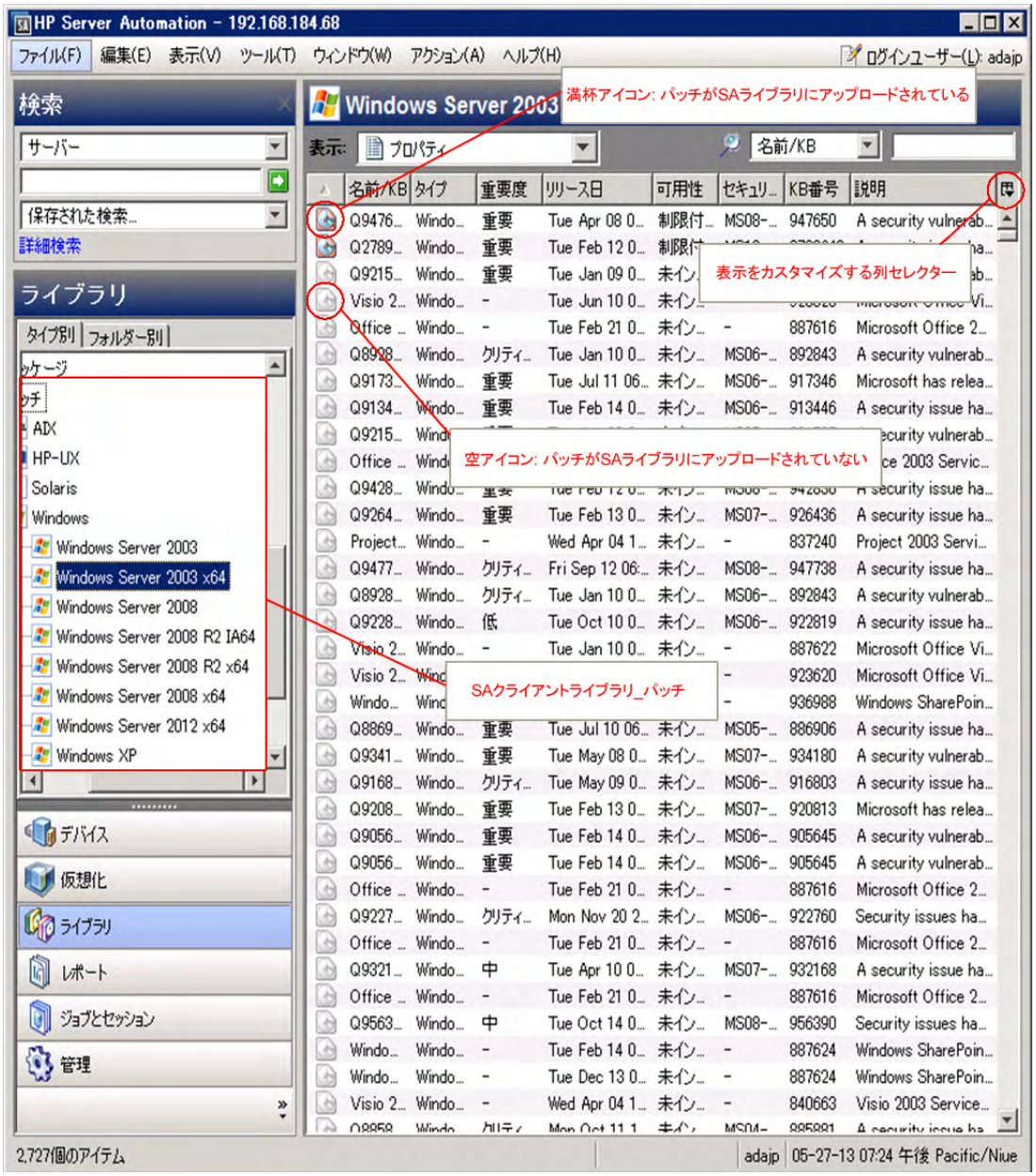
SAクライアントライブラリ

SAクライアントライブラリでは、セキュリティ情報番号、リリース日、重要度レベル、オペレーティングシステムなどを使用して、Microsoftパッチを柔軟に検索または表示することができます。図2を参照してください。

内容ペインの薄く表示されたパッチアイコンは、パッチがライブラリにアップロードされていないことを示します。表示するパッチメタデータ情報の列を制御するには、列セレクターを使用します。

SA クライアントライブラリの Windows フォルダーには、Microsoft からダウンロードされた Microsoft Offline Catalogからプルされたパッチ情報が表示されます。このビューでは、最新の更新時点での、Microsoftからの解析済みパッチデータが表示されます。

図2　　SAクライアントライブラリのWindowsパッチ



前提条件

パッチを適用する管理対象サーバーの要件は、次のとおりです。

- Microsoft Core XML Services (MSXML) または Internet Explorer (IE) が管理対象サーバーにインストールされている必要があります。インストール済みの MSXML と IE のバージョンは、Microsoft XML パーサーと関連する DLL ファイルをサポートしている必要があります。
- Windowsサーバーを実行している管理対象サーバーに、Windowsインストーラーがインストールされている必要があります。このインストーラーは、次のようなMicrosoftのサポートサイトから入手できます。

http://support.microsoft.com/kb/893803/

このURLは一例です。MS製品の情報については、Microsoft のサポートを参照してください。

- 管理対象サーバーで、Windows Updateサービスを自動または手動のいずれかに設定する必要があります。Windowsサービスを設定するには、Windowsのコントロールパネルで [**管理ツール**] > [**サービス**] を選択します。
- Windowsサーバーの場合は、Windowsパッチ管理タスクを実行する際に [プログラムの追加と削除] ダイアログを閉じる必要があります。
- パッチのインストール/アンインストールと、修復を実行するには、サポート対象バージョンの SA エージェントがインストールされている必要があります。
- 管理対象サーバーは、サーバーにインストールされているSAエージェントのサポート対象の言語に設定されている必要があります。
  - 管理対象サーバーで言語を設定するには、コントロールパネルを開き、[地域と言語のオプション] を開いて、[地域オプション] タブを選択し、[標準と形式] セクションのドロップダウンリストから言語を選択します。[**OK**] をクリックして変更内容を保存します。

➤ プラットフォームバージョンのサポートと互換性の詳細については、『SA Support and Compatibility Matrix』を参照してください。

パッチおよびパッチポリシーの検索

SAクライアントでは、SAクライアントの検索機能を使用して、運用環境に関する情報を検索できます。検索機能を使用すると、パッチ、パッチポリシー、サーバーなどを検索できます。『SA ユーザーガイド : Server Automation』の「SAクライアントの検索に関する項」を参照してください。

Windowsサーバーパッチ管理サポート

SAのWindowsパッチ管理を使用して、Microsoft® Windowsパッチの確認、インストール、削除を行い、組織内の管理対象サーバーのセキュリティを確保することができます。

SAのWindowsサーバーパッチ管理サポートは、バージョンが混在するマルチマスターメッシュ (パッチ適用済みのコアとパッチ未適用のコアが混在する環境) に対応しています。Windowsプラットフォームパッチ管理では、次の機能がサポートされています。

:

- パッチデータベースのインポート後に、Windowsサーバーのパッチがライブラリの下に表示されます。
- [**管理**] > [**パッチ設定**] > [**Windowsパッチダウンロード**] > [**パッチ製品**] で特定のバージョンのWindowsサーバーを選択して、Windowsサーバーのパッチメタデータをインポートするかどうかを指定できます。
- Windowsサーバーのパッチ管理では、次の操作を実行できます。
  - パッチブラウザーを起動して、パッチのプロパティ、説明、再起動/インストール/アンインストールフラグを編集できます。
  - Windowsサーバーを選択した場合に、次のパッチビューを参照できます。
    - 必要とされるパッチ
    - ベンダーが推奨するパッチ
    - ポリシーまたは例外のあるパッチ
    - インストール済みのパッチ
    - 例外のあるパッチ
    - すべてのパッチ
- パッチバイナリはSAクライアントを使用してベンダーからインポートするか、またはファイルからインポートできます。

- Windowsサーバーのパッチポリシーをサーバーおよびサーバーグループにアタッチできます。
- サーバーおよびサーバーグループでWindowsサーバーのパッチのパッチポリシー例外を定義できます。

populate-opsware-update-libraryスクリプト

`populate-opsware-update-library` スクリプトには、パッチのバイナリのアップロードで省略するWindowsサーバーのバージョンを指定するためのコマンドライン引数があります。例:

- `no_w2k8`は、Windows Server 2008 x86のパッチバイナリをアップロードしないように指定します。
- `no_w2k8x64`は、Windows Server 2008 x64のパッチバイナリをアップロードしないように指定します。

この例は、サポートされているWindows製品のバージョンによって変更される場合があります。プラットフォームバージョンのサポートと互換性の詳細については、『SA Support and Compatibility Matrix』を参照してください。スクリプトのオプションについては、次を参照してください。表2: populate-opsware-update-libraryのオプション (35ページ)

Windowsサーバーのパッチのポリシーと例外

SA では、Windows サーバーの推奨されるパッチポリシーが用意されています。また、『SA User Guide: Application Automation』に記載された手順でカスタムパッチポリシーを追加で定義することもできます。

修復およびアドホックインストール/アンインストール

Window サーバーのパッチポリシーの修復および Windows サーバーのパッチのアドホックインストール/アンインストールを行うことができます。Windowsサーバーのパッチは、ソフトウェアポリシーおよびソフトウェアのインストール/アンインストールを使用したアドホックインストールで修復できます。ただし、ソフトウェアコンプライアンスでは適用可能性は考慮されません。

パッチコンプライアンス

Windows サーバーでパッチコンプライアンススキャンを実行すると、アタッチされたポリシーおよび例外に関連するコンプライアンスを確認できます。パッチコンプライアンスは、選択したサーバーのパッチ適用可能性に基づいています。

SAクライアントの[コンプライアンス]ビューに、Windowsサーバーのコンプライアンスの詳細が表示されます。

既知の制限事項

- パッチがインストール/アンインストール対象として選択されている場合、[パッチのインストール/アンインストール]ウィンドウでは、通常、インストール/アンインストールフラグを指定できます。パッチのファイル形式は.EXEでなければなりません。Microsoftは、Windowsサーバーのパッチを.EXEと.CABの両方の形式で提供します。SAで、パッチのファイル形式が.CABである場合、[パッチ]、[パッチのインストール]、[パッチのアンインストール]ウィンドウでインストール/アンインストールフラグを指定することはできません。これは、.CAB形式のパッチでは、コマンドライン引数がサポートされないためです。
- Windows パッチブラウザーを使用してインストールフラグまたはアンインストールフラグを追加すると、SAで別の方法ですでに使用されているフラグがあっても、そのフラグは上書きされます。

  そのため、Windowsパッチブラウザーで追加フラグを使用する必要がある場合は、追加フラグで`-q`フラグを指定する必要があります。たとえば、インストール/アンインストールプロセスをログ記録し、デフォルトフラグをオーバーライドしない場合は、次のように指定する必要があります。

  ```
  /log:c:\mylog.txt /q /z
  ```

  注: `-q`フラグをオーバーライドすると(パッチで`-q`がサポートされている場合)、パッチのインストールが失敗します。このタイプのインストールは、タイムアウトするのに1時間かかる可能性があります。

WindowsパッチによるMicrosoftパッチカタログのすべての製品のサポート

SA Windowsパッチでは、オペレーティングシステム (OS) やOS以外の製品を含む、すべてのMicrosoft製品をサポートしています。

旧バージョンのSAのWindowsパッチではOSパッチのみがサポート対象で、MS Office 2010やMS Wordなどの製品固有のパッチはサポートされていませんでした。そのため、Windows 製品のパッチは、Microsoft Offline Catalogファイル (`wsusscn2.cab`) 内にあっても、cabファイルのインポート時にSAデータベースにはアップロードされませんでした。

現バージョンでは、Microsoft Offline Catalogファイル (`wsusscn2.cab`) をインポートする際に、パッチ製品の設定で選択された製品に応じて、製品固有のすべてのパッチがインポートされるようになりました。

➤ 製品を選択する手順については、パッチ管理のWindows製品のパッチサポートの設定 (58ページ) を参照してください。

要件

製品固有のパッチは、その製品がインストールされているサーバーにのみインストールできます。

製品のインストールとスクリプトのアップグレードにより、必要に応じて設定が調整されます。コアでその他の設定を行う必要はありません。

デフォルトの選択済み製品

デフォルトの製品リストは、当バージョンのSAのリリース時点でのMicrosoft製品のリストに基づいています。

使用環境の製品に応じて、製品のリストを変更できます。デフォルトの選択リストに不要な製品が含まれている場合、パッチのインポートを実行する前に削除する必要があります。これにより、SAコアおよびソフトウェアリポジトリでのデータストレージに関する問題を最小限に抑えられます。製品の選択と、この機能の使用の手順については、パッチ管理のWindows製品のパッチサポートの設定 (58ページ) を参照してください。

•

非サポート製品について

Windowsパッチのインポートでは、SAでサポートされているオペレーティングシステム (OS) のパッチのみがインポートされます。非サポートのOSのパッチは、インポート時に除外されます。非サポートのWindows OSと、非サポートのWindows OSに固有の製品はすべて除外対象になります。SAでサポートされているオペレーティングシステムの詳細については、お使いのバージョンのSAの『SA Support and Compatibility Matrix』を参照してください。

➤ Microsoft Offline Catalog (`wsusscn2.cab`) には、SAでサポートされていないWindows OSまたはOS固有の製品のパッチが含まれている可能性があります。これらの非サポートのパッチが、SAの [パッチ設定] の [パッチ設定] 選択リストに表示される場合があります。ただし、非サポートのWindowsパッチは、製品の選択リストで選択されていても、パッチのインポートからは除外されます。

推奨パッチが見つからない製品名の識別

ベンダー推奨パッチポリシー(VRPP)により、インポート済みのパッチに含まれていないパッチがサーバーに対して推奨された場合、コンプライアンススキャンは、見つからないパッチを薄いグレーのフォントで表示します。見つからないパッチをインポートする必要があるMS製品を特定するには、KB番号と製品のマッピングスクリプトを使用できます。詳細については、HPSAのカスタマーサポートにお問い合わせください。

すべてのWindows製品のサポートの概要

製品の選択手順の詳細については、パッチ管理のWindows製品のパッチサポートの設定(58ページ)を参照してください。

Microsoftパッチデータベース

Microsoftパッチデータベースには、リリース済みのパッチとそれらの適用方法に関する情報が含まれています。パッチ管理では、すべてのWindowsサーバーをMicrosoftパッチデータベースと比較して、適用する必要のあるパッチを確認します。

Microsoftでは、緊急リリースが必要な場合を除き、毎月第2火曜日に自社のWebサイトでパッチを公開します。毎月のパッチ公開日にリリースされたWindowsパッチは、Server Automationにすぐにインポートできます。パッチ管理でパッチを管理対象サーバーにインストールするには、事前にMicrosoftのWebサイトからパッチをダウンロードして、ソフトウェアリポジトリにインポートしておく必要があります。パッチをダウンロードしてインポートするには、SAクライアントを使用するか、スクリプトを実行します。

Windowsサーバー上のSAエージェントは、パッチ管理者によってSAにインポートされたMicrosoftパッチデータベースとサーバーの現在の状態とを(`wsusscn2.cab`の最新バージョンに基づいて)24時間ごとに比較します。エージェントは比較の結果をレポートし、そのデータをモデルリポジトリに保存します。コンプライアンススキャンを要求した場合、スキャンに数分かかることがあります。サーバーのコンプライアンスを確認する場合、ステータス情報はモデルリポジトリからも取得されます。

UbuntuおよびWindowsデータベースのビューでは、ベンダーパッチキーが現在利用可能です。ベンダーパッチキーはベンダー固有の値で、ユーザーはこれを使用して、SAのユニット(パッチ)をベンダーが提供する特定のパッチに関連付けることができます。

SAとの統合

サーバーがHP Server Automationで管理されている場合、サーバーにインストールされたSAエージェントは、インストール済みのパッチなどのサーバーの構成をSAに登録します。SAエージェントは、この登録を24時間ごとに繰り返します。この情報はモデルリポジトリ内に直ちに記録されます。この情報には、オペレーティングシステムバージョン、ハードウェアタイプ、インストール済みソフトウェアとパッチなどあります。SAでサーバーを初めてプロビジョニングする際には、同じデータがすぐに記録されます。

新規のパッチが発行されると、SAクライアントを使用して、パッチを適用する必要のあるサーバーをすぐに確認できます。SAでは、パッチやその他のソフトウェアをアップロードするソフトウェアリポジトリが利用できます。SAクライアントを使用して、このソフトウェアにアクセスし、関連するサーバーにパッチをインストールします。

ベストプラクティス: サーバーがSAの管理下に移されたら、SAのWindowsパッチ管理を使用してすべてのWindowsパッチをインストールすることをお勧めします。パッチを手動でインストールした場合、次にソフトウェア登録を行うまでSAにはそのパッチに関するデータがありません。パッチを手動でインストールした

場合、モデルリポジトリ内の該当するサーバーに関するデータが更新されるまでに最大24時間かかります。ただし、SAのWindowsパッチ管理を使用してパッチをインストールすると、エージェントによってモデルリポジトリ内の該当するサーバーに関する情報がすぐに更新されます。

HP Server Automationを使用して、SAのWindowsパッチ管理を使用してインストールしたものではないパッチをアンインストールすることはできません。

Windowsパッチのテストおよびインストール標準化のサポート

HP Server Automationでは、パッチ適用のリスクを最小限に抑えることができます。パッチがSAに最初にインポートされると、パッチのステータスは**制限付き**となります。このときは、必要なアクセス権を持つ管理者のみがパッチをインストールできます。

その後パッチ管理者は、パッチインストールオプションとアンインストールオプションを定義して、パッチをテストします。パッチのテストが完了し、パッチ管理者がパッチを**利用可能**にマークすると、その他の管理者もパッチをインストールできるようになります。

HP Server Automationでは、Windowsパッチ管理を使用して、パッチをインストール/アンインストールする方法を標準化し、アドホックなインストールが行われないようにすることができます。パッチ管理者は、インストール前スクリプトとインストール後スクリプト、インストールフラグとアンインストールフラグ、再起動指示、エラー処理オプションを指定して、パッチのインストールを標準化します。

Windowsパッチデータベース競合レポートの[最終インポートのサマリー]フィールド

パッチデータベースに、[最終インポートのサマリー]フィールドが新しく追加されました。このフィールドは、データベースに重複が検出された場合にレポートします。SAクライアントで、**[管理]>[パッチ設定]>[パッチデータベース]**に移動し、このフィールドを表示します。

フィールドには、最初は空白が表示されます。パッチのインポートを実行するとフィールドが更新され、インポートされたデータベースの状態が反映されます。

表1

フィールド値	説明
完了しました。	インポート処理が完了しました。
警告：<数値> 重複が見つかりました。『SAリリースノート』を参照してください。	重複したパッチがあるため、パッチデータベースで競合が検出されました。 警告が表示された場合、重複を削除してから、コンプライアンススキャンまたは修復処理を実行します。

インポートの実行後も[**最終インポートのサマリー**]フィールドが空白の場合は、インポートに長時間かかり、パッチライブラリのアップデートが完了していないか、レンダリング遅延のためにSAクライアントのキャッシュを再ロードする必要がある(SAクライアントのメニューで、**[ツール]>[オプション]**に移動し、[キャッシュの再ロード]をクリック)などの、既知の問題が原因である可能性があります。

パッチ管理でサポートされるテクノロジー

HP Server AutomationのWindowsパッチ管理にはさまざまなツールが統合されているため、1つのインタフェースを使用してサーバーのパッチ適用を行うことができます。

次のパッチ管理およびインストール用ツールは、サポート対象のWindowsオペレーティングシステムで使用します。

- **msiexec.exe**: MSIパッケージのインストールとアンインストールを行います。
- **pkgmgr.exe**: CABパッチのインストールとアンインストールを行います。
- **unzip.exe**: Info-ZIP互換ZIPアーカイブを解凍します。
- **Windows Update エージェント (WUA)**: パッチのインストールおよび更新用の Microsoft フレームワークにアクセスできます。

これらのユーティリティをHP Server Automationにインポートする手順については、Windowsパッチユーティリティのインポート (68ページ) を参照してください。

Windowsパッチ管理で使用する役割

Server Automation では、パッチ管理の役割を組織内の複数のタイプのユーザーに割り当てることで、厳密な変更管理を行うことができます。パッチ管理には、ポリシー設定担当者、パッチ管理者、システム管理者などの役割を持つユーザーが関与します。

これらの役割は、SAでパッチを管理するためのアクセス権を割り当てることで制御します。必要なアクセス権の取得については、SAの管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

- **ポリシー設定担当者**: ポリシー設定担当者は、パッチリリースを確認し、組織のパッチポリシーに含まれるベンダーパッチを識別するセキュリティ標準グループのメンバーです。ポリシー設定担当者は、最新のセキュリティ上の脅威を確認し、これらの問題に対処するためにベンダーがリリースしたパッチを確認する必要があります。一般にポリシー設定担当者は、管理対象のオペレーティングシステムとアプリケーションに精通しており、ベンダーが発行したパッチを適用する必要があるかどうかを評価することができます。また、ポリシー設定担当者は、パッチ適用プロセスの詳細なテストを考慮に入れて、パッチのインストール後に発生する一般的な問題を診断することもできます。
- **パッチ管理者**: パッチ管理者には、パッチオプションのインポート、テスト、編集を行う権限があります。パッチ管理者は、多くの場合、組織内でセキュリティ管理者と呼ばれます。パッチ管理者には、パッチをHP Server Automationにインポートしてパッチをテストし、利用可能とマークするのに必要なアクセス権が割り当てられます。基本ユーザーはパッチをインポートすることはできますが、パッチをインストールしたり、利用可能とマークしたりすることはできません。パッチ管理者は、パッチ管理を使用してパッチオプション (インストールスクリプトなど) を編集することもできます。その他のタイプのユーザーは、パッチのインポートや編集を行うことはできません。通常、パッチ管理者はMicrosoftパッチデータベースをインポートして、非運用環境の基準ハードウェア上でパッチをテストします。パッチをテストして、運用システムに適用しても問題がないことが確認できたら、パッチ管理者はライブラリでパッチに利用可能のマークを付けて、そのパッチを適用する必要のあるシステム管理者に通知します。
- **システム管理者**: システム管理者は、パッチ管理者が指定したオプションに従って、(使用承認済みの) パッチを均等かつ機械的にインストールします。システム管理者は、デプロイメント中のサーバーの日常的なメンテナンスを担当するSAユーザーです。これらのユーザーには、低レベルシステムの詳細について、ポリシー設定担当者やパッチ管理者と同じ水準の技術力は必要ありません。パッチ管理者がパッチのインストールをすでにセットアップしているため、システム管理者はポリシーをサーバーへアタッチし、パッチの例外を設定して、多数の管理対象サーバーにパッチをインストールすることができます。システム管理者は、承認済みパッチが必要なサーバーを検索し、パッチをインストールして、パッチが正常にインストールされたことを確認する必要があります。システム管理者はパッチをインポートできますが、パッチ管理者が利用可能とマークしない限り、パッチをインストールすることはできません。システム管理者はパッチをアンインストールすることもできます。

HP Server Automationでは、Patch DeployersやPatch Policy Settersの事前定義のパッチユーザーグループを利用することもできます。詳細については、事前定義のパッチユーザーグループ (27ページ) を参照してください。

事前定義のパッチユーザーグループ

SAのインストールまたはアップグレード時には、Patch DeployersやPatch Policy Settersなどの事前定義のパッチユーザーグループが作成されます。

- **Patch Deployers**—パッチのインストールへのアクセス。
- **Patch Policy Setters**—パッチポリシーの設定へのアクセス。

事前定義のアクションのアクセス権の次に、必要なリソースのアクセス権をこれらのユーザーグループに割り当てる必要があります。これらの事前定義のユーザーグループの使用はオプションです。事前定義のユーザーグループのアクセス権は変更可能で、これらのグループを削除したり、コピーして新規グループを作成したりすることもできます。これらの事前定義のユーザーグループの変更や削除が、SAのアップグレードによる影響を受けることはありません。詳細については、『SAユーザーガイド: Server Automation』を参照してください。

パッチ管理のプロセス

Windowsパッチ適用プロセスは、次のフェーズで構成されます。

- **セットアップ**: このフェーズでは、Microsoftデータベース (パッチおよびメタデータ) をServer Automationに取り込み、パッチをトラッキングする製品を識別し、パッチコンプライアンスを構成します。
- **ポリシー管理**: このフェーズでは、リリースされたパッチを調べ、パッチポリシーまたは例外の作成と更新を行い、パッチに利用可能のマークを付け、ポリシーまたは例外をサーバーまたはサーバーグループにアタッチします。
- **パッチコンプライアンス**: このフェーズでは、コンプライアンススキャンを実行してサーバーがコンプライアンス違反状態かどうかを確認し、ポリシーの修復、インストールオプションの設定、適用可能なパッチのインストールを行います。

- **デプロイメント**: パッチをオンデマンドでデプロイするには、必要なパッチをインポートし、パッチをテストし、新しいポリシーの作成して、パッチを利用可能とマークし、インストールオプションを指定して、必要なパッチをインストールします。図3および図4は、これらのフェーズと必要な手順について説明したものです。

図3　Windowsパッチ適用プロセス: パートAおよびパートB

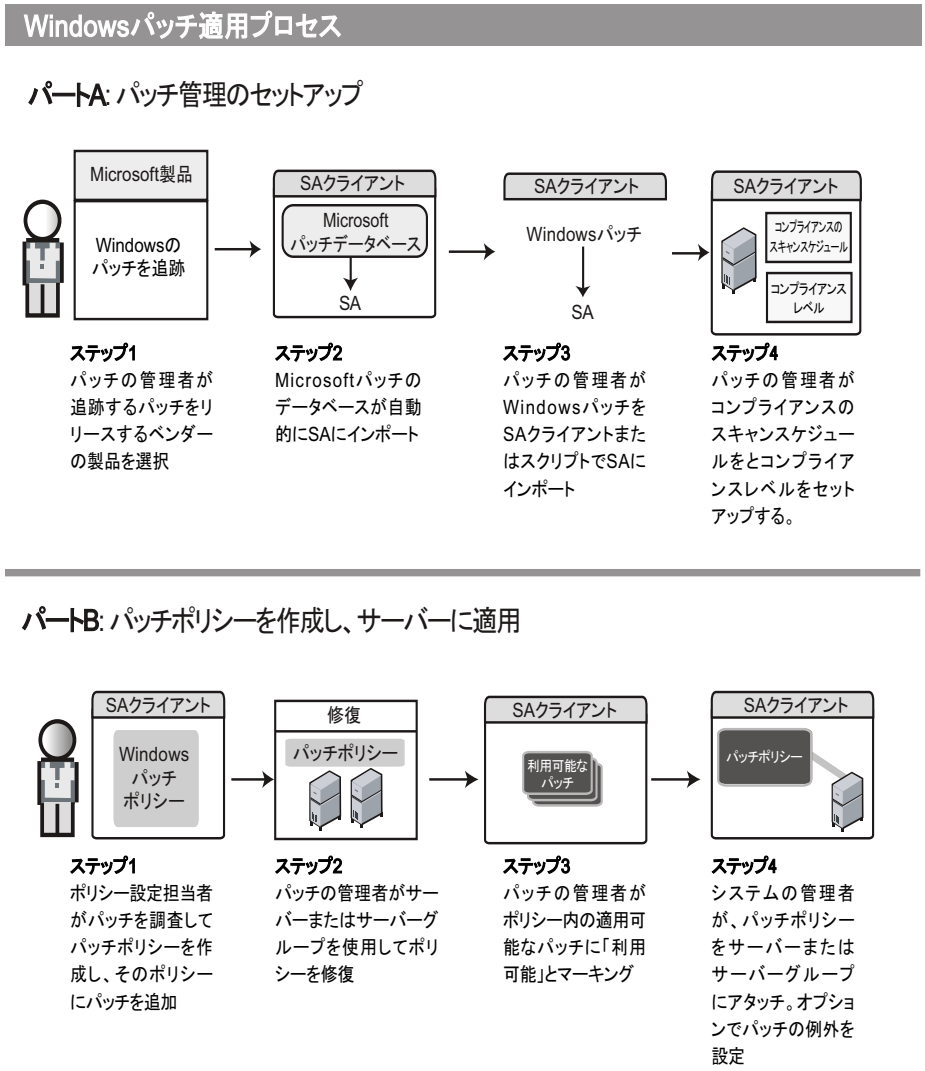
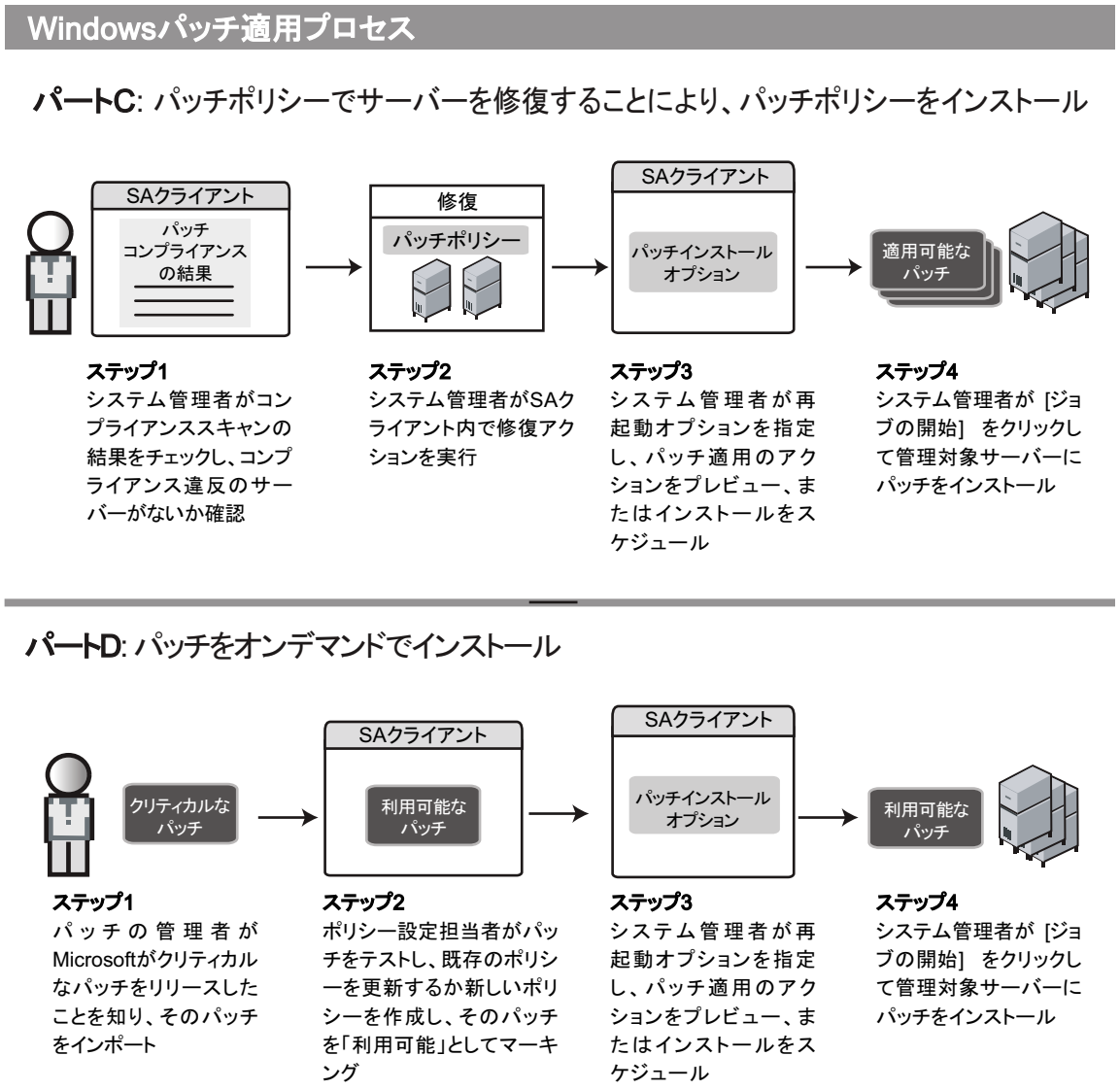


図4　Windowsパッチ適用プロセス: パートCおよびパートD



パッチ管理のタスク

この項では、Windowsパッチに関する情報の検索と管理の方法について説明します。

- パッチ情報の表示
- パッチの依存関係と優先度
- Windowsパッチの表示
- Windowsパッチのプロパティの編集
- パッチのカスタムドキュメントのインポート
- パッチのカスタムドキュメントの削除

- ベンダー推奨Windowsパッチの確認
- Windowsパッチがインストールされたサーバーの確認
- Windowsパッチがインストールされていないサーバーの確認
- SAクライアントライブラリからのWindowsパッチのインポート
- コマンドラインからのMicrosoftパッチデータベースのダウンロード
- Windowsパッチのエクスポート
- Windowsパッチ情報のエクスポート

パッチ情報の表示

パッチに関する詳細 (プロパティ) を表示するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。

2 [パッチ] を展開して、特定のオペレーティングシステムを選択します。

内容ペインに、選択したオペレーティングシステムに関連するすべてのパッチが表示されます。

3 内容ペインで、パッチを開いて [パッチ] ウィンドウにプロパティを表示します。

[**F1**] キーを押すと、[パッチのプロパティ] ウィンドウに表示されるフィールドの説明が表示されます。

パッチの依存関係と優先度

パッチメタデータでは、パッチと Windows 製品間やパッチ間の既知の依存関係と優先度がすべて識別されます。

HP Server Automationでは、次の依存関係と優先度が識別されます。

- **依存関係**の関係では、特定のパッチをインストールする際にサーバー上にすでに存在している必要のあるWindows製品が識別されます。
- **優先度**の関係では、他のパッチを置き換えるパッチや他のパッチで置き換えられるパッチが識別されます。Windowsのパッチ管理では、「これが優先するもの」はパッチが別のパッチを置き換えることを意味し、「これよりも優先するもの」はインストールするパッチが別のパッチで置き換えられることを意味します。

HP Server AutomationのWindowsパッチ管理では、2つのパッチが相互に排他的 (インストールできるのはいずれか一方で、両方をインストールすることはできない) かどうかは検出されません。そのため、パッチ管理で 1 つのサーバーに両方のパッチがインストールされるのを防ぐことはできません。これは、他のパッチで置き換えられるパッチと他のパッチを置き換えるパッチの両方を 1 つのサーバーにインストールできることを意味します。

Windowsパッチの表示

SA クライアントには、Server Automation にインポート済みの Microsoft Windows パッチに関する情報が表示されます。

パッチに関する情報を表示するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。

2 [パッチ] を展開して、特定のWindowsオペレーティングシステムを選択します。

内容ペインに、選択したWindowsオペレーティングシステムのMicrosoftパッチデータベース内に存在するすべてのパッチが表示されます。

3 (オプション) 列セレクターを使用して、名前、タイプ、重要度、可用性、リリース日、セキュリティ情報番号に基づいてパッチをソートします。

4 内容ペインで、パッチを開いて [パッチ] ウィンドウにプロパティを表示します。

Windowsパッチのプロパティの編集

パッチの説明、可用性、インストールパラメーター、アンインストールパラメーターを編集できます。

可用性プロパティは、HP Server Automationでのパッチのステータスを示します。可用性が未インポートである場合、このプロパティを変更することはできません。

インストールパラメーターやアンインストールパラメーターは、パッチを1つずつインストールまたはアンインストールする場合にのみ、パッチのプロパティページまたはパッチのアクションで設定できます。プロパティページのパラメーターはモデルリポジトリに保存されますが、パッチのアクションのパラメーターはそのアクションで使用されるだけです。パッチのアクションのパラメーターは、パッチのプロパティページのパラメーターよりも優先されます。

パッチのプロパティを編集するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。

2 [パッチ] を展開して、特定のWindowsオペレーティングシステムを選択します。

内容ペインに、選択したオペレーティングシステムに関連するすべてのパッチが表示されます。

3 内容ペインで、パッチを開いて [パッチ] ウィンドウにプロパティを表示します。

4 次のフィールドを必要に応じて編集します: 説明、可用性、インストールパラメーター、アンインストールパラメーター

5 [**ファイル**] メニューの [**保存**] を選択して、変更内容を保存します。

パッチのカスタムドキュメントのインポート

パッチの [カスタムドキュメント] ビューには、ローカルファイルシステムからインポートしたテキストファイルが表示されます。プレーンテキスト以外のテキストファイルタイプ (.htmlや.docなど) はサポートされていません。

パッチのカスタムドキュメントをインポートするには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。

2 [パッチ] を展開して、特定のWindowsオペレーティングシステムを選択します。

内容ペインに、選択したオペレーティングシステムに関連するすべてのパッチが表示されます。

3 内容ペインで、パッチを開いて [パッチ] ウィンドウにプロパティを表示します。

4 [ビュー] ペインで [**カスタムドキュメント**] を選択します。

5 [**アクション**] メニューから [**インポート**] を選択します。

6 [カスタムドキュメントのインポート] ウィンドウで、テキストファイルを確認してエンコードを指定します。

7 [**インポート**] をクリックします。

パッチのカスタムドキュメントの削除

パッチの [カスタムドキュメント] ビューには、ローカルファイルシステムからインポートしたテキストファイルが表示されます。プレーンテキスト以外のテキストファイルタイプ (.htmlや.docなど) はサポートされていません。

パッチのカスタムドキュメントを削除するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。
2. [パッチ] を展開して、特定のWindowsオペレーティングシステムを選択します。

   内容ペインに、選択したオペレーティングシステムに関連するすべてのパッチが表示されます。
3. 内容ペインで、パッチを開いて [パッチ] ウィンドウにプロパティを表示します。
4. [ビュー] ペインで [**カスタムドキュメント**] を選択します。
5. [**アクション**] メニューから [**削除**] を選択します。
6. [カスタムドキュメントの削除] ウィンドウで、[**削除**] をクリックします。

ベンダー推奨Windowsパッチの確認

Windows Updateエージェント (WUA) に基づいて特定サーバー向けにMicrosoftが推奨するパッチを確認するには、次の手順を実行します。

1. ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択します。
2. 内容ペインで、[**表示**] ドロップダウンリストから [**パッチ**] を選択します。
3. サポート対象のWindowsサーバーを実行しているサーバーを選択します。
4. 詳細ペインで、ドロップダウンリストから [**ベンダーが推奨するパッチ**] を選択して、選択したサーバーのパッチのタイプを表示します。

Windowsパッチがインストールされたサーバーの確認

特定のパッチがインストールされたサーバーを確認するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。
2. [パッチ] を展開して、特定のWindowsオペレーティングシステムを選択します。

   内容ペインに、選択したオペレーティングシステムに関連するすべてのパッチが表示されます。
3. 内容ペインで、パッチを選択します。
4. 内容ペインの [表示] ドロップダウンリストから、[**サーバー**] を選択します。
5. 選択したパッチの [表示] ドロップダウンリストから、[**パッチがインストールされたサーバー**] を選択します。

   このリストのサーバーを参照して、すべてのインストール済みのパッチのリストを表示することができます。このリストには、Windowsの [プログラムの追加と削除] で表示するリストよりも詳細なインストール済みのパッチのリストが表示される場合があります。

Windowsパッチがインストールされていないサーバーの確認

特定のパッチがインストールされていないサーバーを確認するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**パッチ**] を選択します。
2. [パッチ] を展開して、特定のWindowsオペレーティングシステムを選択します。

   内容ペインに、選択したオペレーティングシステムに関連するすべてのパッチが表示されます。
3. 内容ペインで、パッチを選択します。
4. [表示] ドロップダウンリストから、[**サーバー**] を選択します。
5. [表示] ドロップダウンリストで、[**パッチがインストールされていないサーバー**] を選択します。

SAクライアントライブラリからのWindowsパッチのインポート

WindowsパッチはMicrosoftのWebサイトからダウンロードされて、Server Automationにインポート (アップロード) されます。パッチがインポートされたかどうかを確認するには、パッチの可用性プロパティを表示します。インポート済みパッチの可用性は、制限付き、利用可能、または非推奨のいずれかになります。

ベストプラクティス: パッチのインポートは、SAクライアントまたは`populate-opsware-update-library`を使用して実行できます。選択したパッチをダウンロードする場合は、SAクライアントの使用を推奨します。スクリプトの使用の詳細については、コマンドラインからのMicrosoftパッチデータベースのダウンロード (34ページ) を参照してください。

SAクライアントでパッチをインポートするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。
2. パッケージリポジトリを展開して、特定のWindowsオペレーティングシステムを選択します。

   内容ペインに、選択したオペレーティングシステムに関連するすべてのパッチが表示されます。
3. 内容ペインで、パッチを選択します。
4. MicrosoftのWebサイトからパッチを直接インポートするには、[**アクション**] メニューから、[**内容のインポート(I)**] > [**ベンダーからインポート**] を選択します。

   [ベンダーからインポート] ウィンドウに、Microsoftの Webサイト上のパッチの場所の URLが表示されます。(オプション) このURLはオーバーライドできます。

   または

   ローカルファイルシステムにダウンロード済みのパッチをインポートするには、[**アクション**] メニューから、[**インポート**] > [**ファイルからインポート**] を選択します。

   ファイルブラウザーウィンドウで、パッチを確認します。
5. [**インポート**] をクリックします。

[管理対象サーバー] ビューからのWindowsパッチの内容のインポート

SA 10.0より、[内容のインポート(I)] メニューオプションが [管理対象サーバー] ビューで利用可能になりました。これを使用して、ファイルからパッチの内容をインポートできます。Windows パッチの内容 (バイナリ) は、ベンダーから直接インポートすることもできます。

[管理対象サーバー] ビューからWindowsパッチの内容をインポートするには、次の手順を実行します。

1. パッチの管理 (読み取り/書き込み) 権限でSAクライアントにログインします。
2. **[デバイス] > [すべての管理対象サーバー]** に移動します。
3. ビューで、[**パッチ**] を選択します。
4. [パッチ] の内容ペインで、1つまたは複数のパッチを選択します。
5. 右クリックして、[**内容のインポート(I)**] を選択し、[**ベンダーから(V)...**] または [**ファイルから(F)...**] を選択します。

   1 つのパッチの内容は、ローカルファイルまたは直接ベンダーからダウンロードできます。ただし、複数のパッチを選択した場合は、[**ベンダーから(V)...**] オプションのみを使用できます。
6. **ベンダーから(V)...**: このオプションを使用して、パッチの内容をベンダーから直接インポートできます。(**注**: このオプションは、Windowsパッチにのみ使用できます。)
7. **ファイルから(F)...**: " このオプションを使用して、SAクライアントを実行しているシステムからアクセス可能なローカルファイルから、パッチの内容をインポートできます。

コマンドラインからのMicrosoftパッチデータベースのダウンロード

`populate-opsware-update-library`シェルスクリプトでは、Microsoft サイトから Microsoft パッチデータベースとパッチがダウンロードされます。また、Microsoft パッチデータベースとパッチの Server Automation へのインポートも実行されます。

関連トピック:

- SAクライアントを使用したインポートについては、SAクライアントライブラリからのWindowsパッチのインポート (33ページ) を参照してください。
- パッチメタデータの構成とインポートの手順については、Microsoftパッチデータベースメタデータの構成とインポート (65ページ) を参照してください (注: メタデータのインポート方法の機能は上記のシェルスクリプトと同じです)。

ベストプラクティス: パッチのインポートは、このスクリプトまたはSAクライアントを使用して実行できます。利用可能なすべてのパッチをシステムにダウンロードする場合は、コマンドラインスクリプトの方が便利です。パッチを毎月更新するような場合は、コマンドラインツールを使用して、引数を保存しておくのが一般的です。

スクリプトのオプション:

- このシェルスクリプトでは、新しくインポートしたパッチの初期ステータスが利用可能または制限付きに設定されます。
- また、スクリプトでは、オペレーティングシステム (特定のバージョンのWindowsサーバーなど) に従って、インポートされるパッチをフィルター処理することもできます。このスクリプトを実行すると、いずれかのコマンドラインオプションで明確に除外されない限り、パッチ設定の製品リストで選択されたすべての製品のパッチがインポートされます (表 2: populate-opsware-update-library のオプション (35ページ)を参照してください)。

このスクリプトには、特定の Windows オペレーティングシステムのパッチを除外するオプションが用意されています。ただし、Microsoft OfficeやExchangeなど、OS以外の製品を除外するオプションはありません。

コマンドラインスクリプトを実行するには、SAコアからインターネットまたはWebプロキシへのアクセスが必要です。

パッチバイナリをSAにインポートするには、パッチメタデータがソフトウェアリポジトリ内の現在ロードされているMicrosoftパッチデータベースに存在している必要があります。

スクリプトの実行:

populate-opsware-update-libraryスクリプトを実行するには、ソフトウェアリポジトリサーバーにrootとしてログオンする必要があります。

このスクリプトは次のディレクトリにあります。

/opt/opsware/mm_wordbot/util/

通常は、このスクリプトは、ソフトウェアリポジトリサーバー上でcronジョブとして定期的に実行するようにスケジュール設定します。SAクライアントからは、このスクリプトでインポートされたパッチが自動的にインポートされたように見えます。

このスクリプトは同時に複数実行しないでください。

表2に、このスクリプトで使用できるオプションを示します。

表2　　populate-opsware-update-libraryのオプション

オプション	説明
--spin ホスト名またはIP	データアクセスエンジン (spin) ホストのホスト名またはIPアドレス。 デフォルト: spin
--theword ホスト名またはIP	ソフトウェアリポジトリ (theword) ホストのホスト名またはIPアドレス。 デフォルト: theword
--cert_path ファイルパス	spinの接続に使用する証明書ファイルの指定。 デフォルト: /var/opt/opsware/crypto/wordbot/wordbot.srv
--ca_path ファイルパス	spinの接続に使用するCAファイルの指定。 デフォルト値: /var/opt/opsware/crypto/wordbot/opsware-ca.crt
--verbose	アップロード時にスキップされたパッチを含む詳細な出力を表示します。
--set_available	パッチのアップロード時に可用性ステータスを利用可能に設定します。--set_availableオプションと--set_limitedオプションを同時に指定することはできません。
--set_limited	アップロード時にパッチの可用性ステータスを制限付きに設定します。
--no_w2k	Windows 2000のパッチを処理しません。
--no_w2k3	Windows 2003のパッチを処理しません。
--no_w2k3x64	Windows 2003 (64ビット) のパッチを処理しません。
--no_w2k8	Windows 2008のパッチを処理しません。
--no_w2k8x64	Windows 2008 (64ビット) のパッチを処理しません。
--no_xp	Windows XP (32ビット) のパッチを処理しません。
--use_proxy_url url	バイナリをダウンロードする際にこのプロキシURL経由で接続します。
--proxy_userid ユーザー ID	プロキシサーバーに提供する基本認証のユーザー ID。
--proxy_passwd パスワード	プロキシサーバーに提供する基本認証のパスワード。

表2 populate-opsware-update-libraryのオプション（続き）

オプション	説明
--no_hotfixes	ホットフィックスをアップロードしません。
--no_servicepacks	サービスパックをアップロードしません。
--no_updaterollups	更新プログラムのロールアップをアップロードしません。
--no_wsusscan_upload	Microsoftパッチデータベースをアップロードしません。
--wsusscan_url_override url	このURLからMicrosoftパッチデータベースをダウンロードします。
--update_all	SAにアップロード済みのパッチを更新します。
--download_only パス	ベンダーのWebサイトから指定のパス(ディレクトリ)にファイルをダウンロードします。ただし、SAにファイルをアップロードしません。ファイルは指定したパスの下の<プラットフォームのバージョン>/<ロケール>サブディレクトリにダウンロードされます。
--upload_from_update_root パス	ベンダーのWebサイトではなく、指定したパス(ディレクトリ)からファイルをアップロードします。スクリプトは指定したパスの下の<プラットフォームのバージョン>/<ロケール>サブディレクトリ内のパッチを検索します。このサブディレクトリ内にパッチが見つからない場合、スクリプトは指定したパス内でパッチを検索します。パッチが見つからない場合、パッチはスキップされ、アップロードされません。--download_onlyを併せて指定した場合、このオプションは無視されます。
--wget_path	--wget_path <ファイルパス> ビルトインプロキシサポートではなくプロキシダウンロードを使用する場合は、wgetを使用します。wgetユーティリティのファイル指定では、次を併せて指定する必要があります。 --proxy_userid --proxy_passwd --wget_http_proxy --wget_ftp_proxy --wget_http_proxy <サーバー:ポート> wgetのHTTPプロキシサーバーは次の形式で指定します。 proxyserver:httpport --wget_ftp_proxy <サーバー:ポート> wgetのFTPプロキシサーバーは次の形式で指定します。 proxyserver:ftpport --use_temp_download_path <パス> ヒント:ファイルをサブディレクトリではなく、一時ダウンロードディレクトリ(/var/tmp)にダウンロードします。
--help	このスクリプトの構文を表示します。

Windowsパッチのエクスポート

HP Server Automationからローカルファイルシステムにパッチをエクスポートするには、次の手順を実行します。

1 ナビゲーションペインで、[ライブラリ] > [タイプ別] > [パッチ] を選択します。

2 [パッチ] を展開して、特定のWindowsオペレーティングシステムを選択します。

内容ペインに、選択したオペレーティングシステムに関連するすべてのパッチが表示されます。

3 内容ペインで、パッチを選択します。

4 [**アクション**] メニューで、[**エクスポート**] を選択します。

5 [パッチのエクスポート] ウィンドウで、パッチファイルを含むフォルダー名を [ファイル名] フィールドに入力します。

6 [**エクスポート**] をクリックします。

Windowsパッチ情報のエクスポート

SA の管理対象サーバー上のインストール済みパッチおよびベンダーが推奨するパッチに関する情報をエクスポートできます。また、パッチポリシーやパッチポリシー例外など、選択したサーバーに関するモデル情報とともにベンダーが推奨するパッチの情報をエクスポートすることもできます。次の情報が .csv ファイルにエクスポートされます。

- **サーバー名**: 管理対象サーバーの名前。
- **OS**: サーバーのオペレーティングシステム。
- **サービスパック**: レポートされているサーバーのサービスパックレベル (サービスパック3、サービスパック4など)。
- **KB番号**: Microsoftサポート技術情報でのこのパッチの記事番号。
- **セキュリティ情報**: ホットフィックスに関連付けられている MSYY-XXX ID (MS05-012、MS06-012 など)。MSYY-XXX IDが不明の場合、この列は空白になります。
- **説明**: パッチの目的の簡単な説明。
- **クエリ時刻**: エージェントによる最終ソフトウェア登録。
- **インストール時刻**: パッチがインストールされた時刻。
- **タイプ**: パッチのタイプ。
- **コンプライアンスレベル**: コンプライアンスレベルを表す整数。
- **コンプライアンス**: [パッチのプレビュー] ペインの [コンプライアンス] 列にカーソルを置いたときに表示されるテキスト。
- **例外タイプ**: 常にインストール/常にインストールしないなどの例外のタイプ。
- **例外の理由**: 例外の目的を説明する記述。

Windows パッチ管理では、[パッチのプロパティ] ウィンドウに表示される [説明] フィールドのテキストは、カンマを含めてすべて.csvファイルの [説明] 列に表示されます。パッチに関するすべてのテキストが.csvファイルの [説明] フィールドに表示されるようにするには、パッチ管理で ([パッチのプロパティ] ウィンドウに表示される) 説明全体を二重引用符で囲みます。

パッチ情報を.csvファイルにエクスポートするには、次の手順を実行します。

1 ナビゲーションペインで、[**デバイス**] > [**すべての管理対象サーバー**] を選択します。

2 内容ペインで、1つまたは複数の管理対象サーバーを選択します。

3 [表示] ドロップダウンリストから、いずれかのオプションを選択します。

4 [**アクション**] メニューで [**パッチ情報をCSVにエクスポート**] を選択します。

5 [CSVにエクスポート]ウィンドウで、フォルダーを選択して、ファイル名を入力します。

6 ファイルタイプがカンマ区切り値ファイル(*.csv)になっていることを確認します。

.csvファイルタイプを選択した場合にかぎり、[ファイル名]フィールドで.csv拡張子を追加しなくても、SAによって拡張子が追加されます。

7 [**エクスポート**]をクリックしてパッチ情報を.csvファイルに保存します。パッチ情報をエクスポートしない場合は、[**キャンセル**]をクリックします。

ポリシー管理

Windowsパッチ管理で、パッチポリシーおよびパッチポリシー例外を使用すると、環境内でのパッチ配布をカスタマイズすることができます。ポリシーおよび例外では、管理対象サーバーにインストールするWindowsパッチまたはインストールしないWindowsパッチを定義します。

これらのポリシーや例外で規定するモデルに従ってサーバー環境でパッチを適用することも、モデルとは異なる形でパッチを適用することもできます。パッチポリシーや例外に従わず、アドホックなパッチインストールを行う場合は、修復を行う必要があります。修復を行うことで、適用可能なパッチをサーバー上にインストールすることが可能になります。

パッチポリシー

パッチポリシーは、SAの管理対象サーバー上にインストールするパッチのグループです。1つのパッチポリシーのパッチはすべて、同じWindowsオペレーティングシステムに適用する必要があります。

パッチポリシーを使用することで、柔軟なパッチの配布が可能になります。たとえば、営業部門で使用するサーバーのみに配布するセキュリティパッチを含むパッチポリシーを作成することができます。また、サーバー上にすでにインストールされている特定のソフトウェア(Exchange Server、Internet Information Services(IIS)、SQL Serverなど)に適用可能なセキュリティパッチを含むパッチポリシーを作成することもできます。または、Microsoftが重要なパッチに指定したすべてのパッチを含むパッチポリシーを作成し、組織内のすべてのユーザーが使用するすべてのサーバーにインストールすることができます。

➤ パッチポリシーを作成したくない場合は、(オペレーティングシステム別の)ベンダー推奨のパッチセットをデフォルトのパッチポリシーとして使用できます(wsusscn2.cabで提供されるパッチなど)。

パッチポリシーはサーバーまたはサーバーグループに必要なだけアタッチできます。1つのサーバーに複数のポリシーをアタッチした場合、インストールは累積的に実行され、アタッチされたすべてのポリシーのすべてのパッチがサーバー上にインストールされます。[修復]ウィンドウでは、修復する個別のパッチポリシーを選択できます。サーバーにアタッチされているすべてのポリシーを修復する必要はありません。パッチポリシーをネストすることはできません。

パッチポリシーの説明が定義されている場合は、モデルリポジトリのサーバーのパッチ状態にその説明が記録されます。パッチ管理ではこの情報を使用して、パッチコンプライアンス用にパッチポリシーに関するレポートを作成できます。パッチコンプライアンスでは、パッチポリシーと対応するパッチポリシー例外とを比較します。

Windowsのパッチ管理は、次のタイプのパッチポリシーをサポートしています。

- **ユーザー定義のパッチポリシー**: このタイプのパッチポリシーでは、ポリシー内に必要なパッチを指定できます。ユーザー定義のパッチポリシーは、必要なアクセス権を持つユーザーが編集または削除できます。

  このタイプのパッチポリシーを使用すると、ポリシー設定担当者はパッチを選択することができます。ポリシー設定担当者は、ベンダー推奨のパッチポリシーで利用可能なすべてのパッチのサブセットから成るユーザー定義のパッチポリシーを作成できます。これにより、ポリシー設定担当者は、それぞれの環境に必要なパッチのみを適用することができます。

- **ベンダー推奨のパッチポリシー**：パッチの構成は`wsusscn2.cab`の推奨項目によってサーバー単位で定義されます。ベンダー推奨のパッチポリシーはシステムで定義されるため、ユーザーが編集または削除することはできません。

エクスポートできるのはユーザー定義のパッチポリシーだけです。ベンダー推奨のパッチポリシーをエクスポートすることはできません。

パッチポリシーには、次の特性があります。

- 1つのパッチポリシーのパッチはすべて、同じオペレーティングシステムに適用する必要があります。
- パッチポリシーは、オペレーティングシステムバージョンに関連付けられています。
- パッチポリシーにはそれぞれ名前があり、(必要に応じて) パッチの目的を示す説明を追加することができます。
- パッチポリシーはユーザー定義またはベンダー定義のいずれかです。
- パッチポリシーにサブポリシーはありません。継承は存在しません。
- パッチポリシーはカスタマー独立です。つまり、パッチポリシー内のパッチは、関連するカスタマーに関係なく、任意の管理対象サーバーにインストールできます。詳細については、『SA ユーザーガイド : Server Automation』を参照してください。
- パッチポリシーは常にパブリックです。
- パッチポリシーは、任意の数のサーバーまたはパブリックデバイスグループにアタッチできます。
- 複数のパッチポリシーを1つのサーバーまたはパブリックデバイスグループにアタッチできます。
- ユーザー定義のパッチポリシーは、アクセス権を持つユーザーが作成、編集、削除できます。

パッチポリシー例外

パッチポリシー例外では、特定の管理対象サーバーに明示的に追加するパッチまたは除外するパッチを 1 つ指定します。必要に応じて、例外を使用する理由を追加することもできます。1 つのパッチポリシー例外のパッチは、既存のパッチポリシーがアタッチされている同じ Windows オペレーティングシステムに適用する必要があります。

パッチポリシー例外を使用すると、既存のパッチポリシー (サーバーまたはサーバーグループにすでにアタッチされているポリシー) から逸脱したパッチ適用を行うことができます。これを行うには、サーバーに対して個別のパッチを選択解除または追加します。パッチポリシー例外はサーバーにアタッチされているすべてのパッチポリシーをオーバーライドします。そのため、パッチポリシー例外を使用して、サーバー単位でパッチポリシーから意図的に逸脱したパッチ適用を行うことができます。

パッチポリシー例外の理由が定義されている場合、モデルリポジトリのサーバーのパッチ状態にその説明が記録されます。SA ではこの情報を使用して、パッチコンプライアンス用にパッチポリシー例外に関するレポートを作成できます。パッチコンプライアンスの結果には、パッチポリシー例外と対応する既存のパッチポリシーとの比較に関する説明が示されます。管理対象サーバーにアクセスできるすべてのユーザーが、該当するサーバーにアタッチされたパッチポリシー例外を表示できます。

Windowsパッチ管理は、次のタイプのパッチポリシー例外をサポートしています。

- **常にインストール**: パッチがポリシー内に存在しない場合でも、パッチはサーバーにインストールされます。
- **常にインストールしない**: パッチがポリシーに存在する場合でも、パッチをサーバーにインストールしません。

パッチポリシー例外をオーバーライドする必要がある場合は、パッチを手動でインストールします。

パッチポリシー例外には、次の特性があります。

- パッチポリシー例外には、(必要に応じて) 例外の目的を示す説明を追加することができます。
- パッチポリシー例外では、常にインストールしない/常にインストールのルールを指定できます。

- パッチポリシー例外は、同じオペレーティングシステムバージョンの1つのパッチおよび1つのサーバーに対して設定できます。パッチポリシー例外がパブリックデバイスグループに対して設定され、そのグループ内のサーバーがパッチポリシー例外で指定されたオペレーティングシステムバージョンと一致しない場合、そのパッチポリシー例外は適用されません。
- パッチポリシー例外は、アクセス権を持つユーザーが設定、コピー、削除できます。

ポリシー適用の優先ルール

複数のパッチポリシーおよびパッチポリシー例外を作成して、サーバーに直接アタッチするか、サーバーグループにアタッチすることで、サーバーにインストールするパッチやインストールしないパッチを制御できます。パッチ管理での優先順位の階層によって、パッチのインストールに対するパッチポリシーまたはパッチポリシー例外の適用方法が決まります。この階層は、パッチポリシーまたはパッチポリシー例外がサーバーまたはデバイスグループのどちらのレベルでアタッチされているかに基づいています。

ポリシーおよび例外には、次の優先ルールが適用されます。

- サーバーに直接アタッチされたパッチポリシー例外は、サーバーに直接アタッチされたパッチポリシーよりも常に優先されます。
- サーバーに直接アタッチされたパッチポリシーは、パブリックデバイスグループにアタッチされたパッチポリシーやパッチポリシー例外よりも優先されます。
- パブリックデバイスグループにアタッチされたパッチポリシー例外は、パブリックデバイスグループにアタッチされたパッチポリシーよりも優先されます。
- サーバーが複数のパブリックデバイスグループに含まれる場合、[常にインストールしない] のパッチポリシー例外の方が [常にインストール] のパッチポリシー例外よりも常に優先されます。

修復プロセス

SAの修復の基本事項については、『SA ユーザーガイド : ソフトウェア管理』の「ソフトウェアの修復とインストール」を参照してください。

パッチコンプライアンスを確保するため、Windowsパッチ管理は脆弱性のある管理対象サーバーを識別し、修復プロセスを実行したときに複数のサーバーに同時にパッチをデプロイします。修復プロセスでは、パッチポリシーがアタッチされている管理対象サーバーを調べて、ポリシー全体 (複数のポリシーを含む) を適用します。サーバーまたはサーバーグループでポリシーを修復するには、前もってサーバーまたはサーバーグループにポリシーがアタッチされている必要があります。

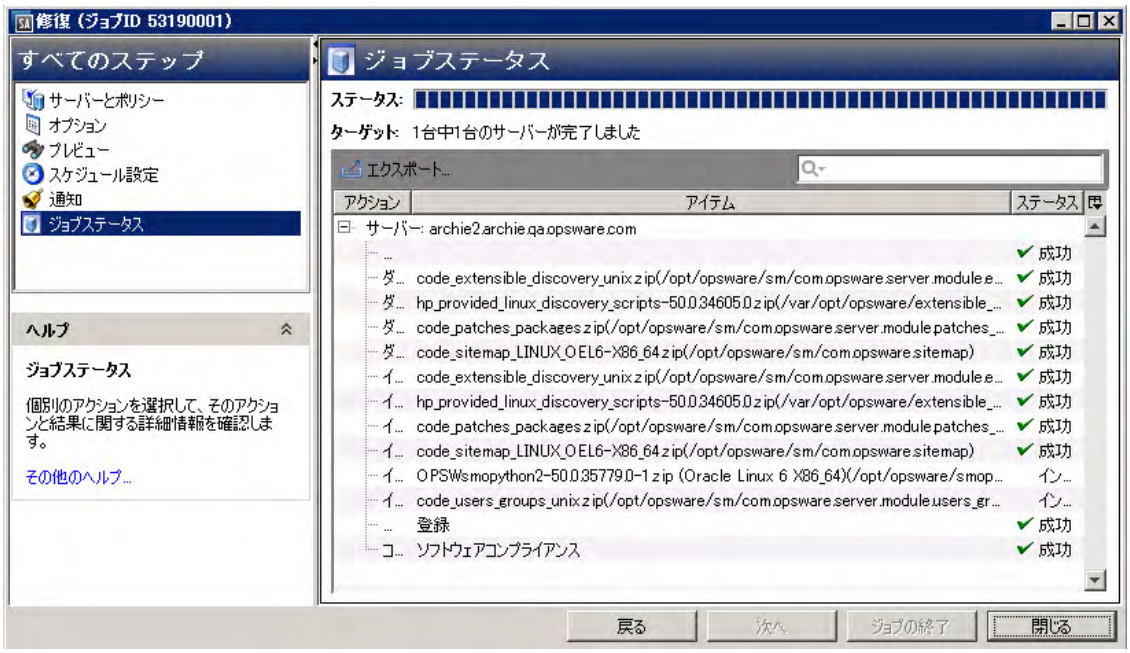
ベストプラクティス: 最新のMicrosoftパッチリリースを確認した後に、新しいパッチをパッチポリシーに追加してポリシーを更新した場合は、修復を実行することをお勧めします。このような場合は、修復プロセスで需要予測情報が提供されます。これにより、このポリシーがアタッチされているサーバーがパッチポリシーの変更でどのように影響を受けるかを確認することができます。

修復プロセスで適用可能なパッチの欠落が見つかった場合、これらのパッチがサーバー上にインストールされます。

SA で修復プロセスを完了するのにインストールが必要なパッチが特定されたら、一連の標準システムユーティリティを使用して処理が実行されます。詳細については、パッチ管理でサポートされるテクノロジー (25 ページ) を参照してください。

修復の条件を適切に管理できるように、SAでは、修復オプションの指定、前と後のアクションの指定、修復プロセスのステータスを知らせるためのチケット ID と電子メール通知の設定を行うことができます。これらの条件は、[修復] ウィザードを使用して設定することができます。

図5 [修復] ウィザード



パッチポリシーの修復

このアクションを実行すると、管理対象サーバーにアタッチされているポリシー内のパッチがインストールされます。このアクションでは、パッチのアンインストールは行われません。パッチポリシーは、特定のサーバーでパッチを常にインストールまたは常にインストールしないことを指定する例外でオーバーライドできます。

パッチポリシーを修復するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] を選択します。
2. [パッチポリシー] を展開して、特定のWindowsオペレーティングシステムを選択します。

   内容ペインに、選択したオペレーティングシステムに関連するすべてのパッチポリシーが表示されます。
3. 内容ペインで、パッチポリシーを開きます。
4. [表示] ドロップダウンリストから、[**サーバー**] を選択します。
5. 内容ペインの [表示] ドロップダウンリストから、[**ポリシーがアタッチされたサーバー**] を選択します。
6. プレビューペインで、1つまたは複数のサーバーを選択します。

7 [**アクション**] メニューから [**修復**] を選択します。

[修復] ウィンドウの最初のステップ: [サーバーおよびデバイスグループ] が表示されます。
各ステップの手順については、次の項を参照してください。

- 修復オプションの設定
- 修復の再起動オプションの設定
- 修復でのインストール前スクリプト/インストール後スクリプトの指定
- 修復でのパッチインストールのスケジュール設定
- 修復での電子メール通知の設定
- 修復のプレビューと開始

1つのステップが完了したら、[**次へ**] をクリックして次のステップへ進みます。[**ジョブの開始**] をクリックする前に、ステップリストに表示される完了したステップをクリックすることで、そのステップに戻って変更を行うことができます。

8 [**ジョブの開始**] をクリックして、修復ジョブを開始します。

ジョブを後で実行するようにスケジュール設定している場合でも、ジョブの開始後にパラメーターを変更することはできません。

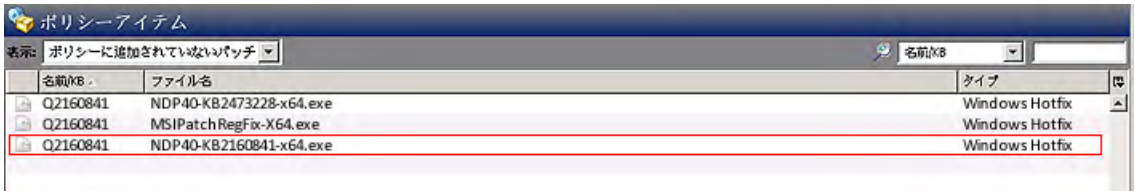
オブジェクトIDによるWindowsパッチポリシーへのアイテムの追加

KB重複エラーを防止するため、Windowsパッチポリシーへのアイテムの追加方法が変更されました。SAでは、KB番号ではなくオブジェクトIDを使用してWindowsホットフィックスを識別するようになりました。これにより、ポリシーに追加するパッチをより詳細に選択できます。ただし、特定のKB番号のパッチを選択しても、SAで同じKB番号のパッチが自動的に選択されるわけではありません。個別に選択するか、[Shift] キーを押しながらクリックして複数のアイテムを選択します。

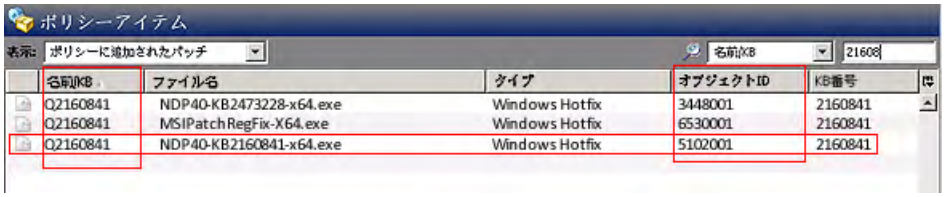
以前の動作 (SA 9.14より前):

9.14より前のバージョンのSAでは、同じKB番号を持つ複数のWindowsホットフィックスパッチをパッチポリシーに追加、またはパッチポリシーから削除する場合、[ポリシーアイテム] 画面でアイテムの1つを右クリックして、[**アイテムをパッチポリシーに追加**] を選択する必要がありました。ウィンドウ内の同じKB番号のアイテムは、すべて追加されました。これは、設定、コピー、パッチの例外の削除についても同様でした。このように複数のアイテムを追加する方法は、重複の発生や、複数のエントリが不要に追加される原因となっていました。

たとえば、同じKB番号 (Q2160841) を持つバイナリ (ファイル名) が3つあるとします。



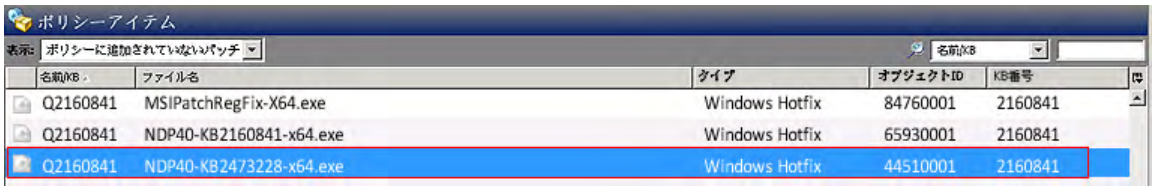
3つのバイナリのいずれかを右クリックし、[**アイテムをパッチポリシーに追加**] をクリックすると、Q2160841という名前のパッチがすべてパッチポリシーに追加されます。実際には、これらのパッチは、異なるオブジェクトIDを持つ別々のアイテムです。追加されたアイテムは、[ポリシーに追加されたパッチ] ビューに表示されます。



最新の動作 (9.14以降):

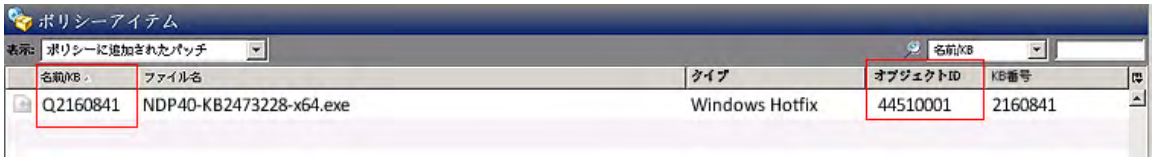
SA 9.14以降のSAでは、Windowsホットフィックスパッチまたはパッチ例外の識別にKB番号が使用されなくなりました。代わりに、オブジェクトIDが使用されます。そのため、1つのアイテムを選択して右クリックを1回するだけで、同じKB番号のアイテムをすべてハイライト表示することはできなくなりました。今後は、各アイテムを個別に右クリックするか、複数のアイテムを選択して、ポリシーに追加/削除/設定/コピーする必要があります。

たとえば、前述のように、同じKB番号 (Q2160841) を持つ3つのバイナリのデータセットを使用するとします。



ここで、いずれかのアイテムを右クリックして [**アイテムをパッチポリシーに追加**] をクリックすると、選択したアイテムのみが追加されます。ほかの2つのアイテムは追加されません。

[ポリシーに追加されたパッチ] ビューでは、Q2160841のアイテムが1つだけポリシーに追加されています。



[ポリシーに追加されていないパッチ] ビューには、追加されなかったQ2160841のアイテム2つが表示されます。

➤ オブジェクトIDは、SAコアサーバーごとに生成されます。つまり、バイナリのKB番号が同じ場合でも、コアが異なると、オブジェクトIDが異なります。新しい動作の例では、前の例とは異なるSAコアが使用されているため、KB番号が同じでもオブジェクトIDが異なっています。

修復オプションの設定

次の修復ポリシーオプションを指定できます。

いずれかのポリシーでエラーが発生した場合でも修復プロセスを中断しない。

このオプションを設定するには、次の手順を実行します。

1 [修復] ウィンドウで、[**次へ**] をクリックして [オプション] ステップに進みます。

2 再起動オプションを選択します。詳細については、修復の再起動オプションの設定 (45ページ) を参照してください。

3 パッチやスクリプトでエラーが発生した場合でも修復プロセスを続行する場合は、[エラー処理] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

4 [**次へ**] をクリックして次のステップに進むか、[**閉じる**] をクリックして [修復] ウィンドウを閉じます。

Windowsパッチポリシーの修復ジョブのオプション - Windowsパッチのインストール順序

修復ジョブウィンドウの [**Windows パッチのインストール順序**] の設定を使用すると、Windows パッチポリシーの修復ジョブでパッチのインストール順序を制御できます。このオプションを選択すると、異なるソースから取得したWindowsパッチデータの競合を防ぐことができます。

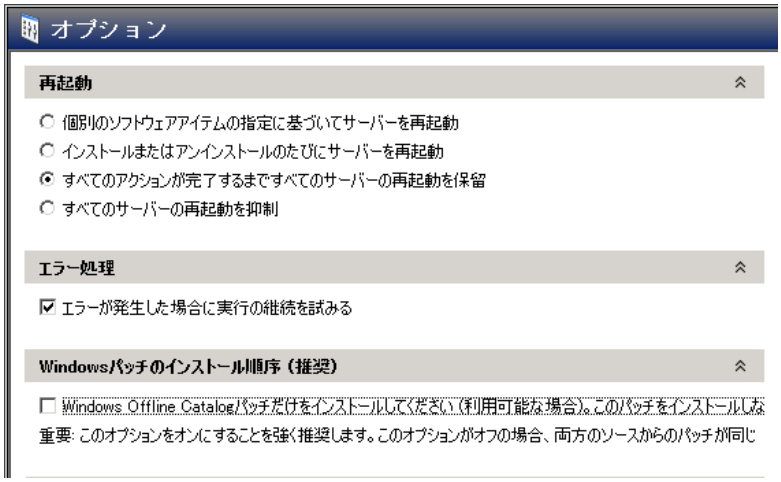
ベストプラクティス: Windowsパッチポリシーの修復ジョブの場合は、この設定の使用を強く推奨します。

SAのWindowsパッチ適用では、Microsoft Offline Catalog (wsusscn2.cab) とHPLN Microsoft Patch Supplementの2種類のソースのパッチをインストールします。Microsoft Patch Supplement で定義されたホットフィックスは、Microsoft Offline Catalogの最新のパッチに取り込まれたり、改良が加えられたりすることがあります。この場合、Microsoft Patch Supplementのパッチは廃止になります。そのため、wsusscn2.cabのパッチの前にMicrosoft Patch Supplementのパッチをインストールすると、パッチデータが損なわれる可能性があります。

動作の仕組み

1 Windowsパッチポリシーの修復ジョブの実行中に、[オプション] ビューで [Windowsパッチのインストール順序] の設定を選択します。

図6 [修復] ウィンドウでのWindowsパッチのインストール順序の設定



2 修復ジョブを実行すると、Microsoft Offline Catalogのすべてのパッチ (wsusscn2.cab) が最初にデプロイされ、HPLN Patch Supplementのパッチはジョブに Microsoft Offline Catalogのパッチが含まれなくなった時点で実行されます。

⚠ 警告: このオプションを選択しない場合、デフォルトの順序はKB番号順になります。この場合、Windows Offline Catalog (wsusscn2.cab) とHPLN Microsoft Patch Supplementの両方からパッチをインストールすると、問題が発生する可能性があります。

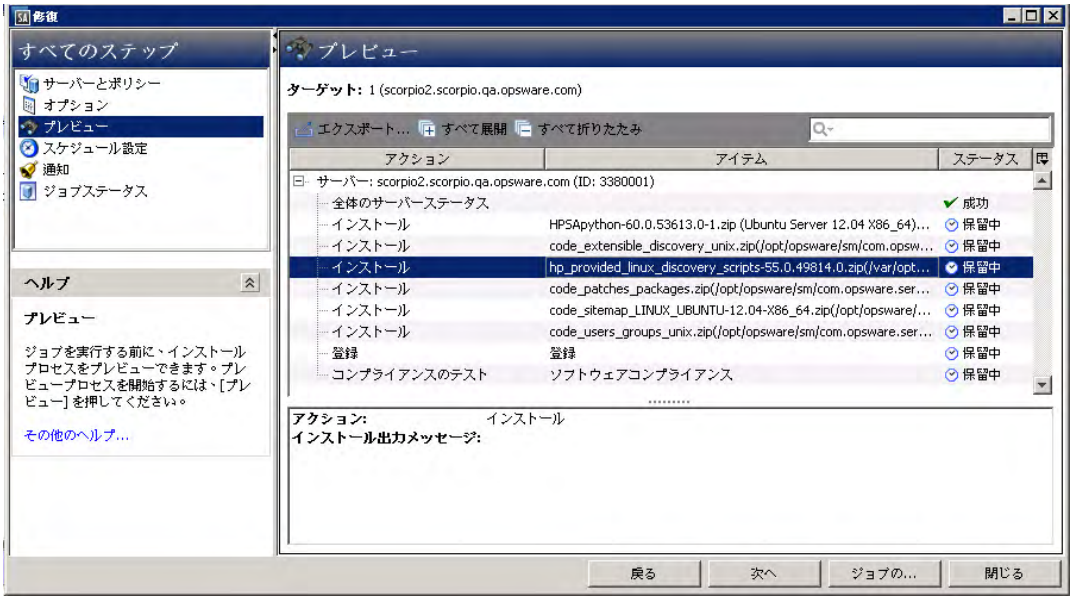
3 すべてのパッチをデプロイして、完全なコンプライアンスを実現するには、修復ジョブを複数回実行する必要があります。

➤ 重要: このオプションを使用する場合、サーバーを完全なコンプライアンス状態にするには、修復ジョブを複数回実行する必要があります。

4 各パッチのインストールのステータスは、[修復] ウィンドウの [プレビュー] または [ジョブステータス] ビューに表示されます。

特定のアイテムに関する詳細を追加表示するには、テーブルの行を選択して、下部のペインに詳細を表示します (図7を参照)。

図7 パッチのインストールステータスのプレビュー



注: ポリシーにwsusscn2.cabとHPLN Supplementの両方のパッチが含まれる場合、HPLNのパッチはインストールされません。次のメッセージが表示されます。

This patch is not a Windows Offline Catalog patch.The Windows Patch Ordering option was enabled for this job, so only Windows Offline Catalog patches will be considered. (このパッチはWindows Offline Catalogのパッチではありません。このジョブではWindowsパッチの順序オプションが有効になっているため、Windows Offline Catalog以外のパッチは考慮されません。)

修復の再起動オプションの設定

サーバーの再起動によるダウンタイムを最小限に抑えるため、パッチのインストール時にサーバーを再起動するタイミングを制御できます。

再起動オプションは、SAクライアントの次のウィンドウで指定できます。

- [パッチのプロパティ] ウィンドウ—[インストールパラメーター] タブ
- [修復] ウィンドウ—[インストール前後のアクション] ステップ

ベストプラクティス: [修復] ウィンドウで再起動オプションを選択する場合、Hewlett PackardではMicrosoftの再起動推奨設定 ([**個別のソフトウェアアイテムの指定に基づいてサーバーを再起動**] オプション) を使用することを推奨しています。Microsoftの再起動設定を使用できない場合は、単一再起動オプション ([**すべてのパッケージがインストールまたはアンインストールされるまですべてのサーバーの再起動を保留します。**] オプション) を選択します。このようにしないと、次の再起動が (SAの制御対象外)実行されるまで、Windows Update エージェント (WUA) でサーバーにインストールされているパッチが正しく通知されない可能性があります。

[修復] ウィンドウの次のオプションでは、パッチのインストール後にサーバーを再起動するかどうかを指定します。これらのオプションは、[修復] ウィンドウで起動されるジョブのみに適用されます。これらのオプションによって、[パッチのプロパティ] ウィンドウの [インストールパラメーター] タブにある [再起動が必要] オプションが変更されることはありません。次に示すオプションの設定は、最初のオプションを除いて、[再起動が必要] オプションの設定よりも優先します。

- **個別のソフトウェアアイテムの指定に基づいてサーバーを再起動** (デフォルト): デフォルトでは、パッチプロパティまたはパッケージプロパティの [再起動が必要] オプションの設定に従って再起動が行われます。
- **インストールまたはアンインストールのたびにサーバーを再起動:** ベストプラクティスとして、個別のパッチまたはパッケージのベンダーの再起動設定に関係なく、パッチまたはパッケージをインストール/アンインストールするたびにサーバーを再起動します。
- **すべてのパッケージがインストールまたはアンインストールされるまですべてのサーバーの再起動を保留する**: 選択したパッチの中に [再起動が必要] オプションが設定されているものが含まれていても、他のパッチにそのオプションが設定されていない場合、すべてのパッチのインストール後にサーバーが1回再起動されます。選択したパッチの中に [再起動が必要] オプションが設定されているものがない場合、サーバーは再起動されません。
- **すべてのサーバーの再起動を抑制**: パッチプロパティの [再起動が必要] オプションが設定されている場合でも、サーバーを再起動しません (ベンダー設定によっては、抑制オプションを無視して強制的に再起動を行う場合があります)。

再起動オプションを設定するには、次の手順を実行します。

1. [修復] ウィンドウで、[**次へ**] をクリックして [オプション] ステップに進みます。
2. いずれかの再起動オプションを選択します。
3. [**次へ**] をクリックして次のステップに進むか、[**閉じる**] をクリックして [修復] ウィンドウを閉じます。

修復でのインストール前スクリプト/インストール後スクリプトの指定

パッチの修復では、修復の前または後に実行するコマンドまたはスクリプトを指定できます。インストール前スクリプトでは、たとえば、管理対象サーバー上で特定の条件をチェックすることができます。条件が満たされない場合やインストール前スクリプトが失敗した場合、パッチはインストールされません。インストール前スクリプトを使用すると、パッチを適用する前にサービスやアプリケーションをシャットダウンすることもできます。インストール後スクリプトを使用すると、管理対象サーバー上でクリーンアッププロセスを実行することができます。

修復の前または後に管理対象サーバー上で次のタイプのスクリプトを実行するように指定することができます。

- **ダウンロード前**: SAから管理対象サーバーにパッチをダウンロードする前に実行するスクリプト。[修復オプション] ステップで [ステージ] を選択した場合にのみ利用できます。
- **ダウンロード後**: SAから管理対象サーバーにパッチをダウンロードした後で、パッチをインストールする前に実行するスクリプト。[修復オプション] ステップで [ステージ] を選択した場合にのみ利用できます。
- **インストール前**: 管理対象サーバーにパッチをインストールする前に実行するスクリプト。
- **インストール後**: 管理対象サーバーにパッチをインストールした後に実行するスクリプト。

インストール前スクリプトを指定するには、次の手順を実行します。

1. [修復] ウィンドウで、[**次へ**] をクリックして [インストール前後のアクション] ステップに進みます。
2. [インストール前] タブを選択します。

   各タブでさまざまなスクリプトとオプションを指定できます。
3. [スクリプトの有効化] チェックボックスをオンにします。このオプションを選択すると、タブのフィールドの残りの部分が有効になります。[スクリプトの有効化] を選択しない場合、スクリプトは実行されません。

4 ドロップダウンリストから、[保存されたスクリプト]または[アドホックスクリプト]を選択します。

保存されたスクリプトは、前にSA Webクライアントを使用してHP Server Automationに保存されたものです。スクリプトを指定するには、[**選択**] をクリックします。

アドホックスクリプトはこの操作に対してのみ実行され、SAに保存されません。タイプ (.batなど) を選択します。[スクリプト] ボックスに、スクリプトが存在する場所のドライブ文字を含むスクリプトの内容を入力します (`echo dir>> C:\temp\preinstall1.log`など)。ドライブ文字を入力しない場合、デフォルトは%SYSTEMDRIVE%になります。これは、Windowsのシステムフォルダーがインストールされている場所です。

5 スクリプトでコマンドラインフラグが必要である場合、[コマンド] テキストボックスにフラグを入力します。

6 [ユーザー] セクションで、システムがローカルシステムでない場合、名前を選択します。

7 システム名、パスワード、ドメイン名を入力します。

8 スクリプトがエラーを返した場合にインストールを停止するには、[エラー] チェックボックスを選択します。

9 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [修復] ウィンドウを閉じます。

修復でのパッチインストールのスケジュール設定

パッチをインストールする日時やパッチをダウンロードする日時をスケジュール設定できます。

パッチのインストールをスケジュール設定するには、次の手順を実行します。

1 [修復] ウィンドウで [スケジュール設定] ステップを選択します。

デフォルトでは、[スケジュール設定] ステップにはインストールフェーズ用のスケジュール設定オプションのみが表示されます。[修復オプション] ステップで [ステージ] を選択した場合、ダウンロードフェーズ用のスケジュール設定オプションも表示されます。

2 次のいずれかのスケジュール設定オプションを選択します。

- **分析のスケジュール**: 分析を実行する日付と時刻を指定できます。
- **ダウンロードのスケジュール**: ダウンロードとインストールを実行する日付と時刻を指定できます。
- **修復のスケジュール**: 修復プロセスを実行する日付と時刻を指定できます。

3 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [修復] ウィンドウを閉じます。

修復での電子メール通知の設定

ダウンロード操作やインストール操作が正常に終了した、あるいはエラーで終了したときに、ユーザーに知らせるために電子メール通知を設定できます。

電子メール通知を設定するには、次の手順を実行します。

1 [修復] ウィンドウで、[**次へ**] をクリックして [通知] ステップに進みます。

2 電子メールアドレスを追加するには、[**通知の追加**] をクリックして [通知電子メールアドレス] フィールドに電子メールアドレスを入力します。

3 ジョブが成功したときの通知ステータスを設定するには、  アイコンを選択します。ジョブが失敗したときの通知ステータスを設定するには、  アイコンを選択します。デフォルトでは、[通知] ステップにはインストールフェーズ用の通知ステータスのみが表示されます。[修復オプション] ステップで [ステージ] を選択した場合、ダウンロードフェーズ用の通知ステータスも表示されます。

4 [チケットID] フィールドに、このジョブに割り当てるチケットIDを入力します。

5 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [修復] ウィンドウを閉じます。

[修復オプション] ステップで [ステージ] を選択した場合、[通知] ペインにダウンロードとインストールの両方のフェーズに対する通知オプションが表示されます。

修復のプレビューと開始

修復のプレビューでは、サーバーのパッチの状態に関する最新のレポートが表示されます。プレビューは、管理対象サーバーにインストールされるパッチを確認するためのオプションステップです。プレビュープロセスでは、(`wsusscn2.cab` に基づいて) パッチのインストール対象として選択したサーバーに該当するパッチがすでにインストールされているかどうかを確認します。システム管理者がパッチを手動でインストールしている場合、サーバーにパッチがすでにインストールされている可能性があります。このような場合、パッチ管理ではパッチの存在を把握できません。

プレビューで、サマリーステップウィンドウに表示されるサーバー、デバイスグループ、およびパッチは、[**ジョブの開始**] をクリックすると、修復に送信されます。ベンダーで推奨されていないパッチは、このリストから除外されます。ポリシー内にQNumberが同じ他のパッチが存在する場合は、ベンダー推奨のパッチのみが表示されます。

このリストには、パッチポリシーやサーバーグループのメンバーシップの変更の有無に関係なく、パッチとそれに関係するサーバーが表示されます。修復をプレビューする場合、パッチポリシーやサーバーグループのメンバーシップが変更されている場合でも、これと同じサーバー、デバイスグループ、およびパッチのリストが使用されます。

[**プレビュー**] をクリックした後に [修復] ウィンドウでパラメーターを変更すると、プレビューで生成されるパッチ適用操作のシミュレートのサマリーが無効な内容になります。たとえば、[**プレビュー**] をクリックした後で、パッチ、パッチポリシー、サーバー、またはデバイスグループを追加した場合は、[**プレビュー**] を再度クリックして変更内容を結果に反映する必要があります。

修復のプレビューでは、パッチが適用済みの状態をシミュレートするためサーバーの動作に関するレポートは行われません。

修復をプレビューするには、次の手順を実行します。

1 [修復] ウィンドウの、[サーバーとポリシー] ステップで、サーバーまたはポリシーを選択します。

2 [**次へ**] をクリックするか、[オプション] ステップを選択して、再起動、エラー処理、およびスクリプトの設定を指定します。

3 [**次へ**] をクリックするか、[プレビュー] ステップを選択して、パッチのインストール時に実行される個々のアクションを表示します。

4 [プレビュー] ステップで、[**プレビュー**] をクリックしてプレビューしているアクションの詳細を表示します。

5 インストールジョブを起動するには、[**ジョブの開始**] をクリックします。

[スケジュール設定] ステップで [**分析後ただちに実行**] を選択した場合、ジョブはすぐに実行されます。特定の時刻を選択した場合、ジョブはその時刻に実行されます。

6 ジョブステータスが [修復] ウィンドウに表示されます。

ステータスバーとテキストで、テーブル内のアクションがどの程度完了したかを確認できます。次のアクションをサーバーごとに実行できます。

- **全体のサーバーステータス**: この修復ジョブに含まれるすべてのサーバーの全体ステータス。
- **分析**: SAは、インストールに必要なパッチの確認、管理対象サーバーにインストールされた最新パッチのチェック、他に実行が必要なアクション (ダウンロード、インストール、または再起動など) の確認を行います。
- **ダウンロード**: Server Automationから管理対象サーバーにパッチをダウンロードします。
- **インストール**: ダウンロードの完了後、パッチをインストールします。
- **再起動**: [オプション] ステップでこのアクションを指定すると、サーバーが再起動します。
- **登録**: ソフトウェアの登録を実行し、管理対象サーバーに現在インストールされているパッケージとパッチを取得します。
- **コンプライアンスのテスト**: コンプライアンススキャンを実行して、管理対象サーバーの現在のコンプライアンスステータスをレポートします。
- **スクリプトの実行**: [オプション] ステップでスクリプトを指定した場合、ダウンロードやインストールの前後にスクリプトが実行されます。
- **インストールと再起動**: ［オプション］ ステップで個々のパッチまたはパッケージの設定に従ってサーバーを再起動するように指定した場合、個別のパッチやパッケージがインストールされるとすぐにサーバーが再起動されます。

7 特定のアクションに関する詳細を追加表示するには、テーブルの行を選択して、下部のペインに内容を表示します。

または

8 ナビゲーションペインで、[ジョブとセッション] を選択してジョブに関する詳細を確認します。詳細については、ジョブログの表示 (44ページ) を参照してください。

9 [**ジョブの終了**] をクリックしてジョブを実行しないようにするか、[**閉じる**] をクリックして [修復] ウィンドウを閉じます。ジョブを終了できるのは、ジョブがスケジュール設定されている場合のみです。

(オプション) インストール、アンインストール、修復のキャンセルまたは終了 (86ページ) を参照してください。

パッチポリシーコンプライアンスの確認

管理対象サーバーがパッチポリシーや例外に適合しているかどうかを確認するには、次の手順を実行します。

1 ナビゲーションペインで、[**デバイス**] > [**すべての管理対象サーバー**] を選択します。

2 [表示] ドロップダウンリストから [コンプライアンス] を選択して、パッチコンプライアンスステータスを表示します。

3 特定のサーバーを選択するか、[**すべての行のチェックをオンにする**] をチェックして、詳細ペインにパッチコンプライアンスの詳細を表示します。いつでも [**すべての行のチェックをオフにする**] を選択して、サーバーの選択内容を変更することができます。

4 詳細ペインで、パッチの行を展開して、ステータスとコンプライアンスのサマリーの詳細を参照します。ステータスフィルターを使用して、コンプライアンスの表示設定を絞り込みます。デフォルトで、これは [**ステータスフィルターがありません**] に設定されています。

パッチポリシーの作成

パッチポリシーは、管理対象サーバー上にインストールする一連のパッチです。作成したばかりのパッチポリシーにパッチは含まれていません。また、サーバーにもアタッチされていません。

パッチポリシーを作成するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] を選択します。

2 特定のWindowsオペレーティングシステムを選択します。

3 [**アクション**] メニューで [**パッチポリシーの作成**] を選択します。

作成したポリシーには、「新規パッチポリシー n」という名前が付きます。ここで、nは、すでに存在する新規パッチポリシーの数に応じて割り当てられる番号です。

4 内容ペインで、新規パッチポリシーを開きます。

5 (オプション) [プロパティ] の [名前] フィールドに、ポリシーの目的または内容を表す名前を入力します。

パッチポリシーの削除

このアクションでは、SAからパッチポリシーが削除されます。ただし、管理対象サーバーからパッチが削除またはアンインストールされることはありません。サーバーまたはサーバーグループにアタッチされているパッチポリシーを削除することはできません。ポリシーをSAから削除するには、事前にサーバーまたはサーバーグループからポリシーをデタッチする必要があります。

パッチポリシーをSAから削除するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] を選択します。

2 特定のWindowsオペレーティングシステムを選択します。

3 メインウィンドウの内容ペインで、ポリシーを選択します。

4 [**アクション**] メニューで [**パッチポリシーの削除**] を選択します。

パッチポリシーへのパッチの追加

このアクションでは、パッチポリシーにパッチが追加されます。ただし、管理対象サーバー上にパッチをインストールするものではありません。パッチはポリシーを修復する際にインストールされます。

SAに対するパッチポリシーにパッチを追加するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] を選択します。

2 特定のWindowsオペレーティングシステムを選択して、Windowsパッチのリストを表示します。

3 内容ペインで、パッチを選択します。

4 [表示] ドロップダウンリストから、[パッチポリシー] を選択します。

5 [表示] ドロップダウンリストで、[**パッチが追加されていないポリシー**] を選択します。

6 ポリシーを選択します。

7 [**アクション**] メニューで [**パッチポリシーに追加**] を選択します。

8 [パッチポリシーに追加] ウィンドウで、[**追加**] をクリックします。

パッチポリシーからのパッチの削除

このアクションでは、パッチポリシーからパッチが削除されます。このアクションによって、管理対象サーバーからパッチがアンインストールされ、SAからパッチが削除されることはありません。

パッチポリシーからパッチを削除するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。
2. 特定のWindowsオペレーティングシステムを選択して、Windowsパッチのリストを表示します。
3. 内容ペインで、パッチを選択します。
4. [表示] ドロップダウンリストから、[**パッチポリシー**] を選択します。
5. [表示] ドロップダウンリストで、[**パッチが追加されたポリシー**] を選択します。
6. パッチを選択します。[**アクション**] メニューで [**パッチポリシーから削除**] を選択します。
7. [パッチをポリシーから削除] ウィンドウで、ポリシーを選択して [**削除**] をクリックします。

パッチポリシーのサーバーへのアタッチ

このアクションでは、パッチポリシーをサーバーまたはサーバーグループと関連付けます。このアクションは、サーバーまたはサーバーグループでポリシーを修復する前に行う必要があります。

ポリシーをアタッチするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] を選択します。
2. 特定のWindowsオペレーティングシステムを選択して、Windowsパッチポリシーのリストを表示します。
3. 内容ペインで、パッチポリシーを選択します。
4. [表示] ドロップダウンリストから、[**サーバーの使用**] または [**デバイスグループの使用**] を選択します。
5. [表示] ドロップダウンリストから、[**ポリシーがアタッチされていないサーバー**] または [**ポリシーがアタッチされていないサーバーグループ**] を選択します。
6. プレビューペインで、1つまたは複数のサーバーを選択します。
7. [**アクション**] メニューで、[**サーバーのアタッチ**] を選択します。
8. [**アタッチ**] をクリックします。

パッチポリシーのサーバーからのデタッチ

このアクションでは、パッチポリシーは削除されません。また、管理対象サーバーからパッチがアンインストールされることもありません。

ポリシーをデタッチするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] を選択します。
2. 特定のWindowsオペレーティングシステムを選択して、Windowsパッチポリシーのリストを表示します。
3. 内容ペインで、パッチポリシーを選択します。
4. [表示] ドロップダウンリストから、[サーバーの使用] (または [デバイスグループの使用]) を選択します。

5 [表示] ドロップダウンリストから、[**ポリシーがアタッチされたサーバー**] または [**ポリシーがアタッチされたサーバーグループ**] を選択します。

6 プレビューペインで、1つまたは複数のサーバーを選択します。

7 [**アクション**] メニューで、[**サーバーのデタッチ**] を選択します。

8 [**デタッチ**] を選択します。

パッチポリシー例外の設定

パッチポリシー例外では、修復プロセスでパッチをインストールするかどうかを指定します。パッチのインストールおよびパッチのアンインストールのアクションでは、パッチポリシー例外は無視されます。パッチポリシー例外は、ポリシーよりも優先されます。例外は特定のパッチおよびサーバーまたはサーバーグループに対して指定できます。特定のパッチポリシーに対して例外を指定することはできません。

パッチポリシー例外を設定するには、次の手順を実行します。

1 ナビゲーションペインで、[**デバイス**] > [**すべての管理対象サーバー**] を選択します。

2 サーバーを選択します。

3 内容ペインで、サーバーを選択します。

4 [表示] ドロップダウンリストから、[**パッチ**] を選択します。

5 プレビューペインで、パッチを選択します。

6 [**アクション**] メニューで [**例外の設定**] を選択します。

7 [ポリシー例外の設定] ウィンドウで、次の例外タイプを選択します。

- **常にインストールしない**: パッチがポリシーに存在する場合でも、パッチをサーバーにインストールしません。
- **常にインストール**: パッチがポリシーに存在しない場合でも、パッチがサーバーにインストールされます。

8 (オプション) [理由] フィールドに、説明を入力します。この説明は、プレビューペインの [例外] 列の上にマウスカーソルを置いたときに表示されます。[例外のあるパッチ] オプションは必ず選択する必要があります。終わったら、[**OK**] をクリックします。

既存のパッチポリシー例外の検索

パッチポリシー例外がすでにアタッチされている管理対象サーバーを検索し、例外のあるパッチを検索することができます。

既存のパッチポリシー例外を検索するには、次の手順を実行します。

1 ナビゲーションペインで、[**デバイス**] > [**すべての管理対象サーバー**] を選択します。

2 [表示] ドロップダウンリストから、[**パッチ**] を選択します。

3 内容ペインで、サーバーを選択します。

4 [表示] ドロップダウンリストから、[**ポリシーまたは例外のあるパッチ**] または [**例外のあるパッチ**] を選択します。

5 [例外] 列で、アイコンの上にマウスカーソルを置くと、その例外の理由が表示されます。パッチポリシー例外のタイプは、次のアイコンで示されます。

 パッチとサーバーの関連付けに対する例外 (常にインストール)。

 サーバーグループとパッチの関連付けからサーバーに継承された例外 (常にインストール)。

 パッチとサーバーの関連付けに対する例外 (常にインストールしない)。

 サーバーグループとパッチの関連付けからサーバーに継承された例外 (常にインストールしない)。

パッチポリシー例外のコピー

サーバーまたはサーバーグループ間で例外をコピーするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。
2. [パッチ] を展開して、特定のWindowsオペレーティングシステムを選択します。
3. 内容ペインで、パッチを選択します。
4. [表示] ドロップダウンリストから、[**サーバーの使用**] または [**デバイスグループの使用**] を選択します。
5. [表示] ドロップダウンリストから、[**例外のあるサーバー**] または [**例外のあるサーバーグループ**] を選択します。
6. プレビューペインで、サーバーを選択します。このサーバーは、例外のコピー元になります。
7. [**アクション**] メニューで [**例外のコピー**] を選択します。
8. [ポリシー例外のコピー] ウィンドウで、ターゲットのサーバーまたはデバイスグループを選択します。

   このサーバーは、例外のコピー先になります。この操作によって既存の例外が置き換えられる場合は、操作の続行を確認するメッセージが表示されます。
9. [**コピー**] をクリックします。

パッチポリシー例外の削除

パッチポリシー例外を削除するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。
2. [パッチ] を展開して、特定のWindowsオペレーティングシステムを選択します。
3. 内容ペインで、パッチを選択します。
4. [表示] ドロップダウンリストから、[**サーバー**] を選択します。
5. [表示] ドロップダウンリストから、[**例外のあるサーバー**] を選択します。
6. プレビューペインで、サーバーを選択します。
7. [**アクション**] メニューで [**例外の削除**] を選択します。

パッチコンプライアンス

HP Server Automation では、管理対象サーバーとパブリックデバイスグループに対する適合テスト (コンプライアンスチェック) を実行して、ポリシーおよびポリシー例外のパッチがすべて正常にインストールされているかどうかを判断します。組織に合わせてパッチコンプライアンス情報を最適化するため、パッチコンプライアンスレベルを設定し、カスタマイズしたパッチコンプライアンスレベルのルールを編集することができます。

パッチコンプライアンススキャン

パッチコンプライアンススキャンでは、サーバーにインストールされているパッチを、サーバーにアタッチされているパッチポリシーやパッチポリシー例外と比較します。このスキャンの結果には、コンプライアンス状態 (必須のパッチがすべてインストールされている) のサーバーとコンプライアンス違反状態 (必須のパッチが一部インストールされていない) のサーバーが示されます。

パッチコンプライアンススキャンは、パッチ適用環境に応じて実行またはスケジュール設定する必要があります。たとえば、パッチポリシーを更新したり、Server Automation 以外で (使用せずに) パッチをインストールした場合は、SAのモデルが変更されていて、コンプライアンス情報の再計算が必要であるため、コンプライアンススキャンを実行する必要があります。SAでは、スキャンが必要の表示を用いて、このような状況を示します。この場合は、定期的なスキャンのスケジュールを待たずに、1 つまたは複数のサーバーでコンプライアンススキャンを開始することができます。

パッチコンプライアンススキャンを開始する方法

パッチコンプライアンススキャンは、次の方法で開始できます。

- **すぐに実行**: サーバーまたはグループを選択してから、メニュー項目を選択します。

  詳細については、パッチコンプライアンススキャンの即時開始 (54ページ) を参照してください。

- **定期的に実行**: スケジュールを設定します。

  詳細については、パッチコンプライアンススキャンのスケジュール設定 (67 ページ) を参照してください。デフォルトでは、スキャンはスケジュール設定されていません。

- **別のタスクの結果として実行**

  SA は、タスクの終了時に管理対象サーバー上でパッチコンプライアンススキャンを実行します (次の各項を参照)。

  — Windowsパッチのインストール (78ページ)

  — Windowsパッチのアンインストール (87ページ)

  — パッチポリシーの修復 (41ページ)

パッチコンプライアンススキャンの即時開始

選択したサーバーでスキャンを開始するには、次の手順を実行します。

1 ナビゲーションペインで [**デバイス**] を選択します。

2 サーバーまたはデバイスグループのリストからエントリを選択します。

3 右クリックで [**スキャン**] > [**パッチコンプライアンス**] を選択して [パッチコンプライアンススキャンステータス] ウィンドウを表示します。

選択したサーバーのコンプライアンスステータスの更新

Windowsサーバーのコンプライアンスステータスを更新すると、SAクライアントはWebサービスデータアクセスエンジンから最新のデータを取得します。更新では、Windowsサーバーのコンプライアンス情報の再スキャンは行われません。

1つまたは複数のサーバーのコンプライアンスステータスを更新するには、次の手順を実行します。

1 ナビゲーションペインで[**デバイス**]を選択します。
2 [表示]ドロップダウンリストから、[コンプライアンス]を選択します。
3 内容ペインで、1つまたは複数のサーバーを選択します。
4 右クリックで、[**サーバーの更新**]を選択します。
5 [ステータス]列で変更されたコンプライアンス情報を確認します。

スキャンエラーの詳細の表示

スキャン操作に失敗した場合、サーバーがコンプライアンス状態かどうかを判断することができません。スキャン失敗はスキャン失敗アイコン で示されます。パッチコンプライアンススキャンが失敗した理由を確認するには、次の手順を実行します。

ナビゲーションペインで[**デバイス**]を選択します。

1 チェック対象のサーバーにドリルダウンします。
2 内容ペインで、サーバーを選択します。
3 右クリックで、[**スキャン**]>[**パッチコンプライアンススキャンエラーの詳細**]を選択します。
4 [パッチコンプライアンススキャンエラーの詳細]ウィンドウでサーバーを選択し、ウィンドウの下部に表示される詳細なエラーメッセージの内容を確認します。

パッチコンプライアンスのアイコン

HP Server Automationでは、表3に示すアイコンが表示されます。

表3 パッチコンプライアンスステータスのアイコン

ステータス/アイコン	説明
コンプライアンス	サーバーはすべてのパッチでコンプライアンス状態です。サーバーにアタッチされているポリシーのパッチはすべて、ターゲットサーバー上にインストール済みです。
部分コンプライアンス	サーバーは一部のパッチで部分コンプライアンス状態です。これらのパッチには例外が設定されています。
非コンプライアンス	サーバー上にインストールされたパッチが、パッチポリシーで定義された条件と一致していません。
スキャン失敗	スキャン操作に失敗しました。パッチ管理でサーバーのコンプライアンスをチェックできません。

パッチの非コンプライアンスについて

サーバーまたはサーバーグループのパッチの非コンプライアンスステータスは、さまざまな要因で発生します。たとえば、サーバーにアタッチされたパッチポリシーの定義に基づいてインストールする必要のある適用可能なパッチが存在する場合などです。また、サーバーのパッチコンプライアンスレベルに影響する例外が存在する可能性もあります。

たとえば、パッチポリシーに「常にインストールしない」という例外に指定されたパッチがあるにも関わらず、ターゲットサーバーにそのパッチがインストールされている場合、サーバーは非コンプライアンスとみなされます。

また、他のパッチで置き換えられるパッチが推奨されるパッチで、ポリシーや例外に含まれている場合、これらのパッチはコンプライアンスの計算にカウントされ、ターゲットサーバーにこれらのパッチが存在しない場合、サーバーのパッチコンプライアンスステータスは非コンプライアンスになります。

パッチコンプライアンスレベル

パッチコンプライアンスレベルでは、それぞれのパッチコンプライアンスルールを定義します。パッチコンプライアンススキャンの結果には、ポリシーのみ、ポリシーと例外の両方、または独自にカスタマイズしたレベルを含めることができます。

Windowsパッチ管理では、次のコンプライアンスレベルがサポートされます。

- **ポリシーのみ**: サーバーにインストールされているパッチがパッチポリシーに準拠しているかどうかを確認します。
- **ポリシーと例外**: サーバーにインストールされているパッチがパッチポリシーや例外に準拠しているかどうかを確認します。ポリシーと例外が一致せず、例外の [理由] フィールドにデータがない場合、部分的アイコンが表示されます。
- **カスタマイズ済み**: このコンプライアンスレベル用に編集したルールを確認します。

パッチコンプライアンスルール

パッチコンプライアンスルールは、[管理対象サーバー] ウィンドウに表示されるコンプライアンスアイコンを決める条件です。

Windowsパッチ管理では、次のコンプライアンスルールがサポートされます。

- **ポリシーに追加されたパッチ**: パッチポリシーに追加されているパッチ。
- **サーバーにインストールされたパッチ**: 管理対象サーバーにインストールされているパッチ。
- **例外タイプ**: [例外タイプ] の値は次のとおりです。
  - **常にインストール**: パッチがポリシー内に存在しない場合でも、パッチはサーバーにインストールされます。
  - **常にインストールしない**: パッチがポリシーに存在する場合でも、パッチをサーバーにインストールしません。
  - **なし**: このパッチとサーバーに指定されている例外はありません。
- **例外の理由**: [ポリシー例外の設定] ウィンドウの [例外の理由] に入力した説明。[パッチコンプライアンスルール] ウィンドウの [例外の理由] の値は次のとおりです。
  - **はい**: [例外の理由] にデータがあります。
  - **いいえ**: [例外の理由] は空です。
  - **該当しない**: このパッチとサーバーに指定されている例外はありません。
- **コンプライアンス結果**: パッチコンプライアンスのスキャン結果を示すアイコン。これらのアイコンは [管理対象サーバー] ウィンドウに表示されます。

パッチ管理

データセンター環境では、ベストプラクティスとしてWindowsパッチ管理をカスタマイズして、次の操作を実行できるようにしておくことをお勧めします。

- コマンドラインスクリプトまたはSAクライアントを使用して、パッチをすぐにインストールできるようにするかどうかを指定する。
- コマンドラインスクリプトまたはSAクライアントを使用して、Microsoftパッチデータベースをオンデマンドでインポートする。
- ポリシーのコンプライアンススキャン結果のアイコン表示をカスタマイズする。
- 再起動が必要なサーバーの検索を容易にする。
- 特定のMicrosoft製品または特定のロケールに適用するパッチのみをトラッキングしてインポートする。
- Windowsパッチユーティリティをインポートおよびエクスポートする。
- ポリシーコンプライアンススキャンをオンデマンドで手動で起動するか、定期的なスキャンをスケジュール設定して、管理対象サーバーのパッチの状態を確認する。

パッチデータベースおよびユーティリティのインポートに必要な前提条件

MicrosoftパッチデータベースまたはWindowsパッチユーティリティをインポートする前に、SAコアとの通信時にWebプロキシを使用しないようにブラウザーを設定する必要があります。

ブラウザーを設定するには、次の手順を実行します。

1. [Log in to HP Server Automation Client] ウィンドウで、[**More**] をクリックしてウィンドウを展開します。
2. [**Advanced Settings**] をクリックして、[Advanced Settings] ウィンドウを開きます。
3. [Proxies] セクションで、[Use Browser] が選択されている場合は、SAコアとの通信時にWebプロキシを使用しないようにブラウザーを設定します。

   または

4. [Proxies] セクションで [Manual] が選択されている場合 (つまり、プロキシを手動で設定) は、コアのIPまたはホスト名を [No Proxy Hosts] テキストボックスに入力します。これにより、SAクライアントがSAコアと直接通信できるようになります。

パッチの可用性の設定

デフォルトのパッチの可用性を設定するには、SAクライアントまたはコマンドラインスクリプトを使用します。SA クライアントで設定したデフォルト値よりも、スクリプトで使用するデフォルト値が優先されます。スクリプトについては、コマンドラインからのMicrosoftパッチデータベースのダウンロード (34ページ) を参照してください。

SAクライアントを使用して新規にインポートされるパッチの可用性のデフォルト値を設定するには、次の手順を実行します。

1. ナビゲーションペインで、[**管理**] > [**パッチ設定**] を選択します。
2. [**インポート済みパッチのデフォルトの可用性**] ドロップダウンリストから、[**制限付き可用性**] または [**利用可能**] を選択します。

   制限付き可用性 (デフォルト)— 制限付き可用性のマークの付いたパッチはHP Server Automationにインポート済みで、必要なアクセス権を持つパッチ管理者のみがインストールできます。必要なアクセス権の取得については、システム管理者にお問い合わせください。これらのアクセス権については、『SA 管理ガイド』を参照してください。

利用可能—利用可能のマークの付いたパッチは、管理対象サーバー上にインストールできます。

-

Windows製品のパッチサポートの設定

この機能の利点と要件の概要については、WindowsパッチによるMicrosoftパッチカタログのすべての製品のサポート (23ページ) を参照してください。

新機能である、すべてのWindows製品のサポートの開始手順を次に示します。

手順1 - SAクライアントからのMicrosoft製品の選択

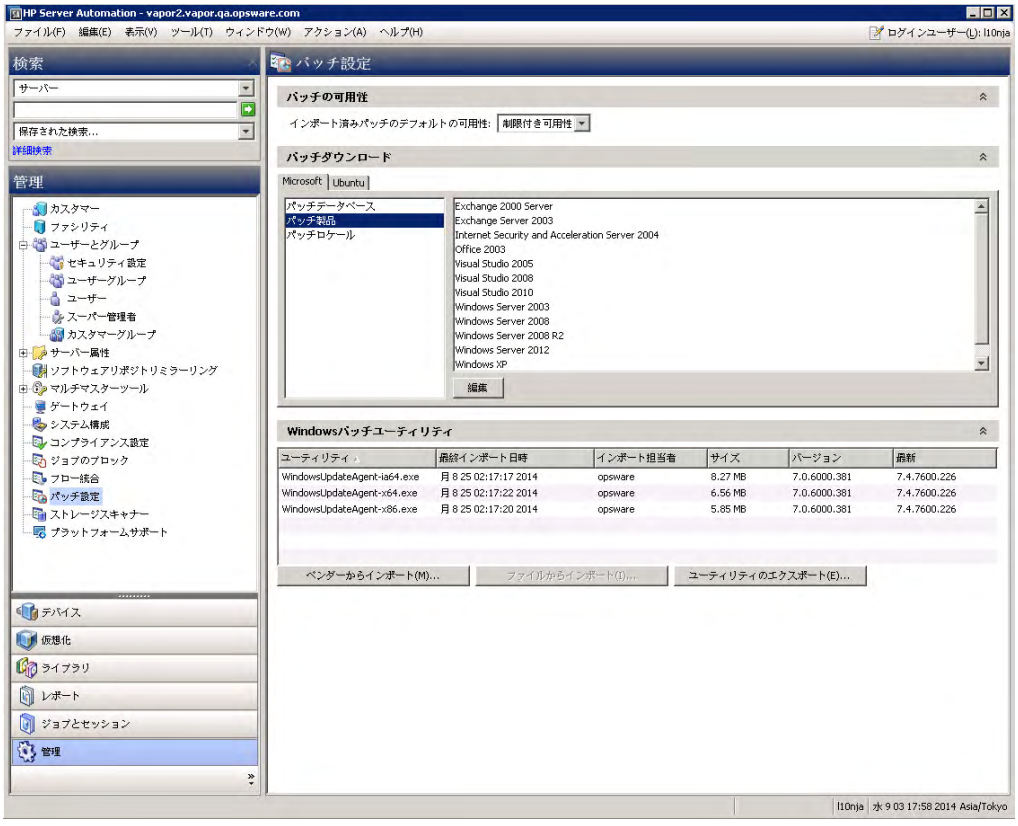
手順2 - 追加の製品のWindowsパッチのインポート

手順3 - サーバーのスキャンと修復

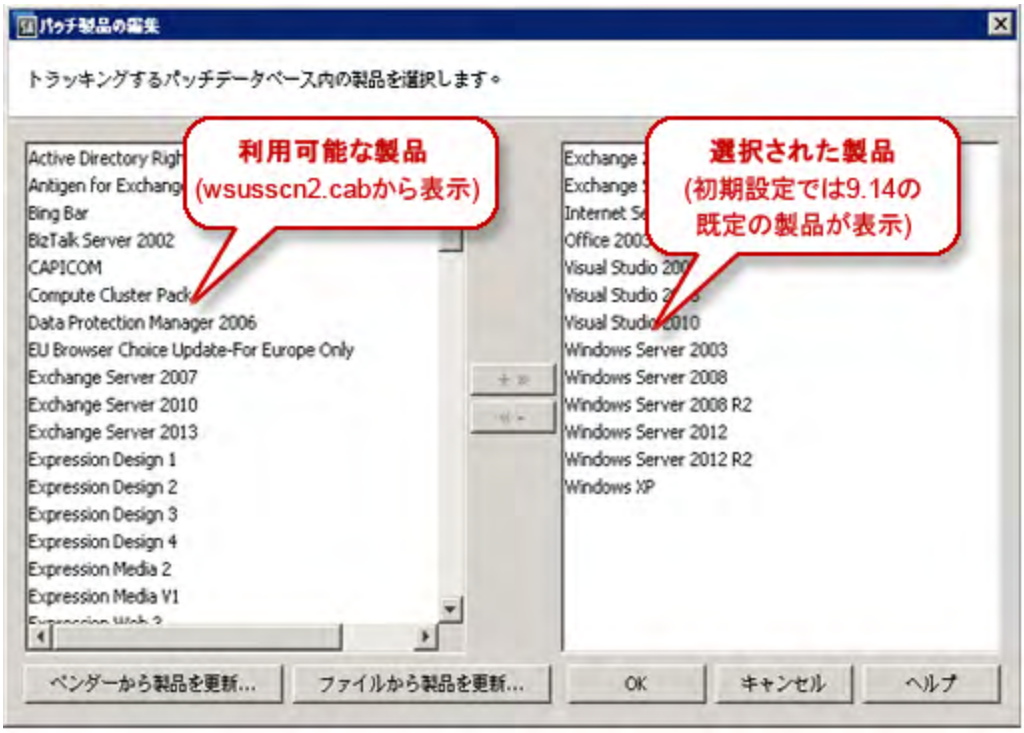
手順1 - SAクライアントからのMicrosoft製品の選択

製品固有のパッチをインポートするには、関連するMS製品を選択します。

1. **[管理] > [パッチ設定]** に移動します。
2. Windowsパッチダウンロード設定のリストから **[パッチ製品]** を選択します。



3 [**編集**] をクリックして [パッチ製品の編集] ウィンドウを開きます。



左に利用可能な製品、右に選択した製品が表示されます。

初回使用時に表示される選択した製品のセットは、システムの Microsoft Product Catalog (`wsusscn2.cab`) のバージョンによって異なります。`wsusscn2.cab`がシステムにインポートされていない場合、左のパネルには何も表示されません。

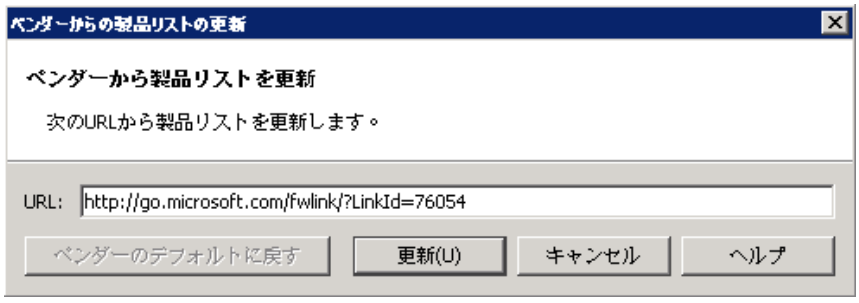
4 利用可能な製品のリストを作成するには、**更新**のアクションボタンのいずれかをクリックします。

ベンダーから製品を更新...: このオプションを使用して、製品リストをベンダーのサイトから直接更新します。ベンダーのサイトのURLは、MicrosoftのWebサイト上のデータベースのデフォルトURLです。

ファイルから製品を更新...: このオプションを使用して、製品リストをローカルマシン上の`wsusscn2.cab`ファイルから更新します。

e **ベンダーからの製品リストの更新**

新しい [ベンダーからの製品リストの更新] ウィンドウを使用して、利用可能な製品のリストをベンダーのWebサイトから直接更新できます。



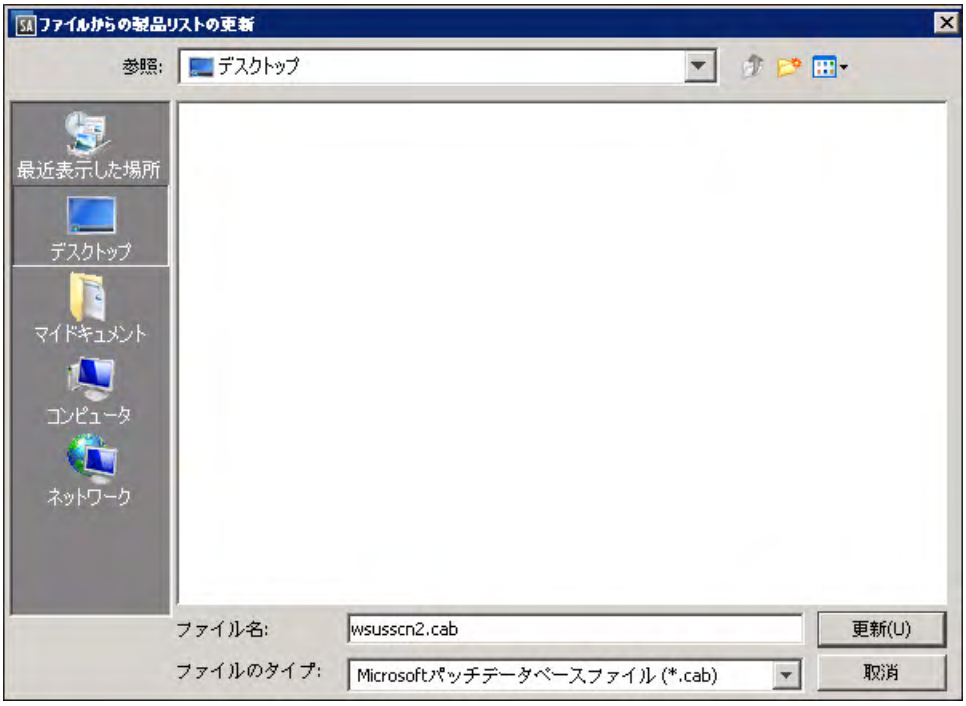
— **URL**: ベンダーのWebサイト上で、製品リストを含むパッチデータベースがある場所。この値は、システムの実装設定に基づいて自動的に入力されますが、変更可能です。

— **ベンダーのデフォルトに戻す**: URLを変更した場合、このボタンを選択すると、システムの実装設定で定義されたベンダーのパッチデータベースのデフォルトURLに戻すことができます。

— **更新**: 指定したURLのベンダーのパッチデータベースに基づいて、SAのMicrosoft製品リストを更新します。

f ファイルからの製品リストの更新

新しい[ファイルからの製品リストの更新]ウィンドウを使用して、利用可能な製品のリストをローカルマシン上のファイルから更新できます。この方法は、管理対象サーバーがインターネットに接続されていないエアギャップ環境で便利です。

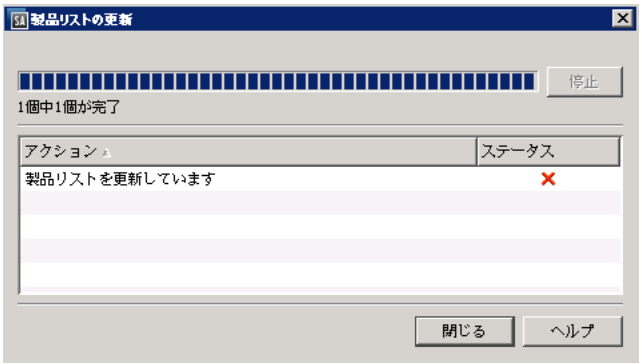


— **ファイル名**: ローカルマシンのMicrosoft Offline Catalog (`wsusscn2.cab`) ファイルの場所に移動します。

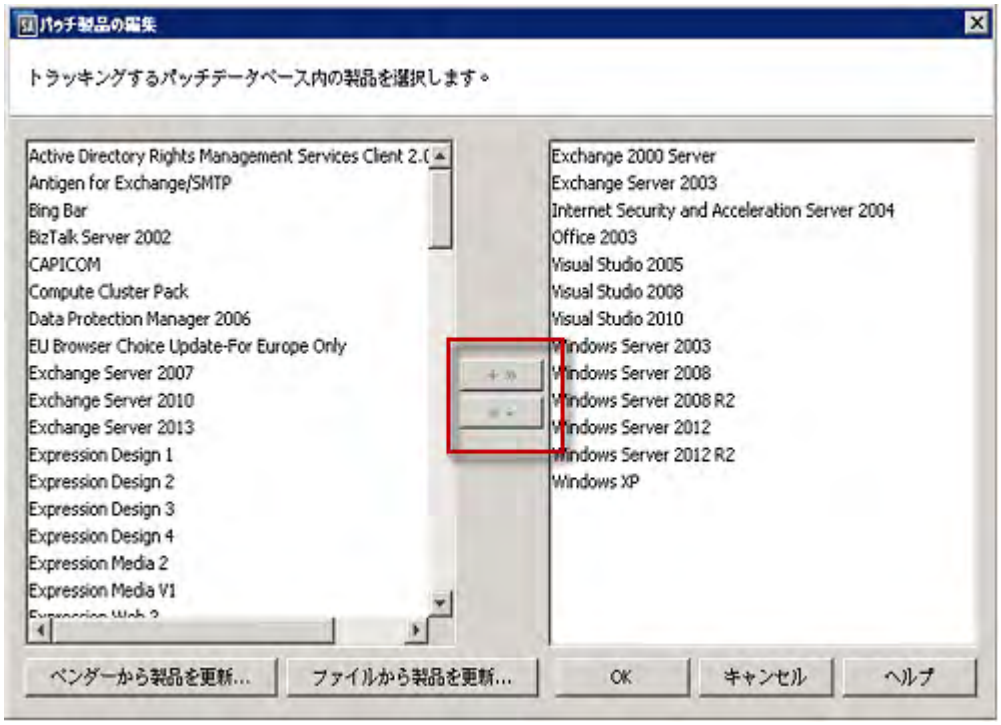
— **ファイルのタイプ**: デフォルトのMicrosoft Patch Databaseファイル (`*.cab`) を受け入れます。

— **更新**: 選択したファイルに基づいて、SAのMicrosoft製品リストを更新します。

更新の実行中に[**バックグラウンドで実行**]をクリックして、[更新]ウィンドウを最小化できます。



5 リストの更新後、選択した製品のリストを使用環境での必要に応じて変更します。



- **製品の追加**: 左側のペインで、利用可能な製品のリストから製品を選択し、[**+ >>**] をクリックして、選択した製品を右のリストに移動します。
- **製品の削除**: 右側のペインで、選択した製品のリストから製品を選択し、[**<<-**] をクリックして、左側の利用可能な製品のリストに移動します。

6 [**OK**] をクリックして選択内容を保存します。

Windowsパッチのインポートを次回に実行した際に、選択した製品のパッチがダウンロードに含まれます。

手順2 - 追加の製品のWindowsパッチのインポート

対象に含めるWindows製品を指定したら、パッチのインポートを実行できます。

Windowsパッチをインポートするには、次の手順を実行します。

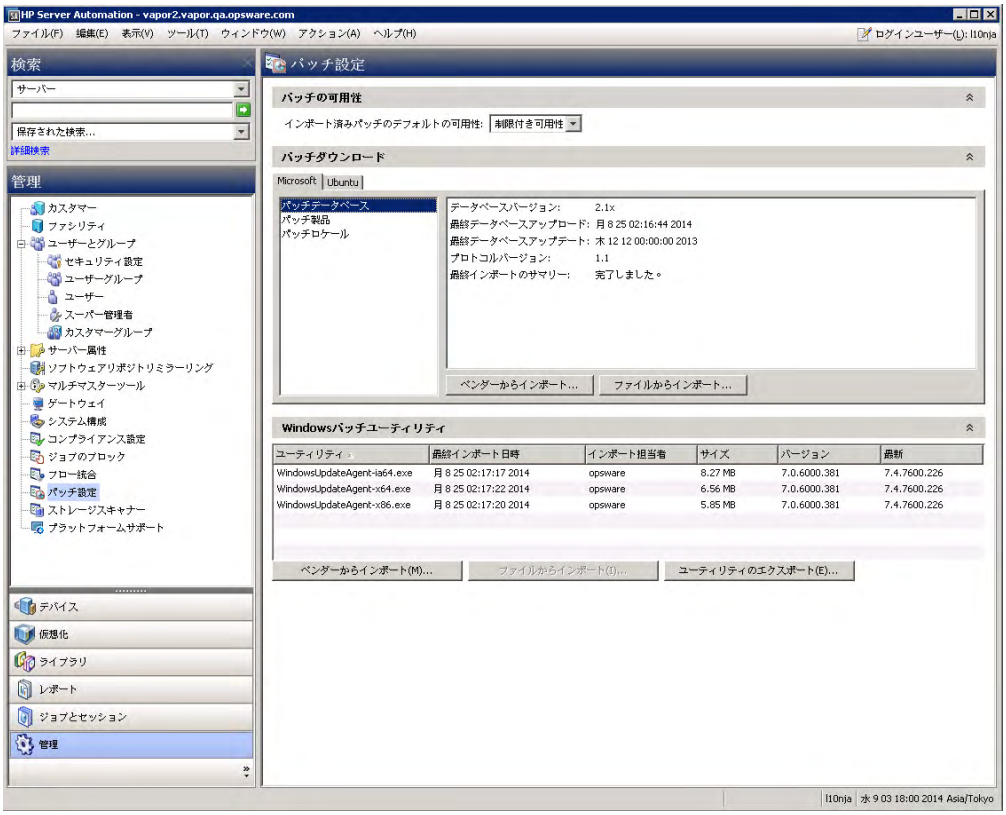
1 [管理] > [パッチ設定] に移動します。

2 Windowsパッチダウンロード設定のリストから [**パッチデータベース**] を選択します。

3 次のアクションボタンのいずれかをクリックして、パッチデータベースをインポートします。

- **ファイルからインポート...**: このオプションを使用して、選択した製品のWindowsパッチメタデータをローカルマシン上の`wsusscn2.cab`ファイルからインポートします。

- **ベンダーからインポート...**: このオプションを使用して、選択した製品のWindowsパッチメタデータをベンダーのサイトから直接インポートします。ベンダーのサイトのURLは、MicrosoftのWebサイト上のデータベースのデフォルトURLです。

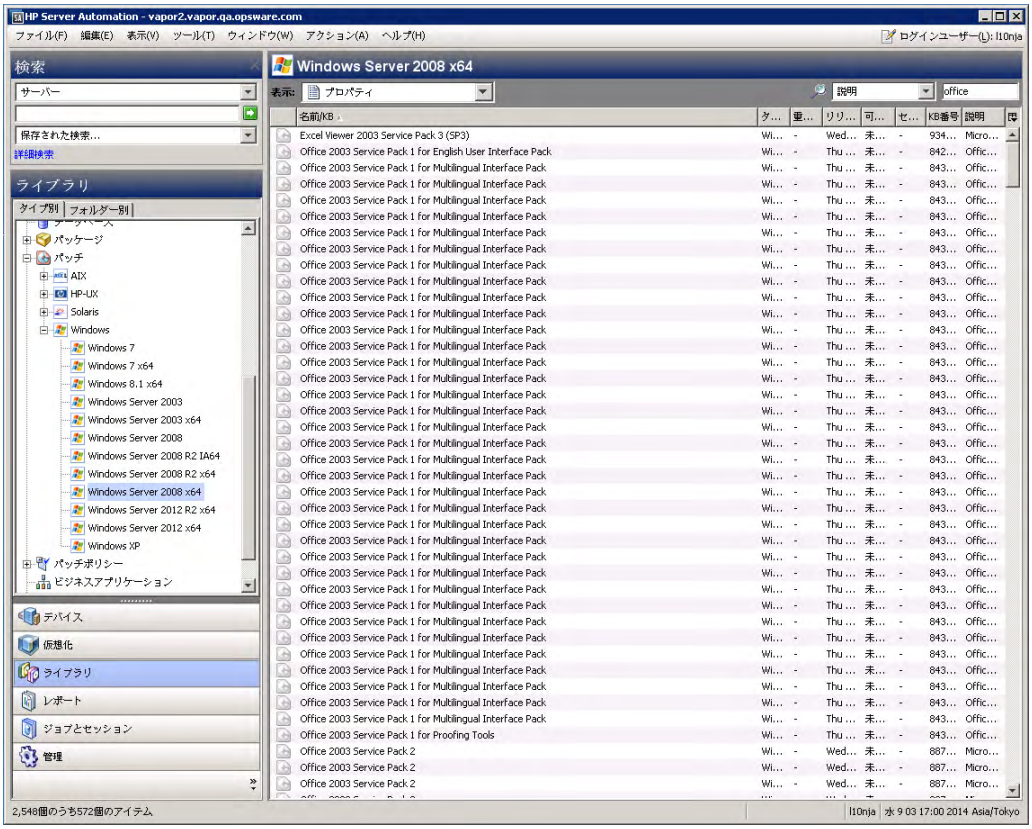


ヒント: 現在の状態を保持するには、毎月、Microsoft のパッチ火曜日の後に、パッチデータベースを再インポートします。

警告: 選択した製品の数が多くなるほど、パッチデータベースのインポート処理にかかる時間が長くなります。すべての製品を選択した場合、Windows パッチデータベースのインポートと、その後に続く対応するバイナリのインポートは、時間が長くかかり、大きなディスク容量を必要とします。

4 インポートが完了したら、SAのWindowsパッチライブラリに移動して、選択した製品のパッチがアップロードされていることを確認します。

5 **[ライブラリ] > [タイプ別] > [パッチ] > [Windows]** に移動します。



6 Windowsオペレーティングシステムを1つ選択し、そのOSの製品のパッチを確認します。

製品のパッチを検索するには、検索する値に **[説明]** を選択して、テキストボックスにOffice 2003などの製品名を入力します。

パッチのリストがフィルター処理され、検索条件に一致するものだけが表示されます。

手順3 - サーバーのスキャンと修復

対象の Windows 製品のパッチをすべてインポートしたら、コンプライアンススキャンを実行し、その結果に基づいて、必要に応じてサーバーを修復します。

残りの手順は、ベンダー推奨パッチポリシー (VRPP) がWindowsサーバーにアタッチ済みであるという想定のもとに実行されます。VRPPがサーバーにアタッチされていない場合は、通常の手順でアタッチしてから、コンプライアンススキャンを実行します。パッチポリシーをサーバーへアタッチする手順については、『SA 9.10 ユーザーガイド: Server Patching』を参照してください。

1 パッチコンプライアンス用にVPRRがアタッチされたWindowsサーバーをスキャンします。

2 **[デバイス]** で、スキャン対象のWindowsサーバーを選択します。

3 **[アクション] > [スキャン] > [パッチコンプライアンス]** を選択します。

スキャン結果により、サーバーを修復して製品固有のパッチを適用する必要があることが示されます。

4 通常の手順で、推奨パッチを修復します （パッチポリシーごとにサーバーを修復する手順については、『SA 9.10 ユーザーガイド: Server Patching』を参照してください)。

このスクリプトを実行すると、パッチ設定の製品リストで選択されたすべての製品のパッチがインポートされます。このスクリプトには、オペレーティングシステム以外の特定の製品について、パッチのインポートを省略するオプションはありません。このスクリプトには、特定のWindowsオペレーティングシステムのパッチを除外するオプションが用意されています。ただし、Microsoft OfficeやExchangeなど、OS以外の製品を除外するオプションはありません。

Windows Server 2008 Itanium (IA64) パッチの有効化/無効化

9.14以降のSAでは、Windowsパッチ適用で、Itanium (IA64) パッチはデフォルトでインポートされません。ただし、WindowsサーバーのIA64パッチをインポートするためのスクリプトが利用可能です。

旧バージョンでは、Windows Server 2008 R2のパッチ製品を選択すると、Itaniumのパッチがデフォルトでインポートされました。SA 9.14以降では、Itaniumのパッチはデフォルトでインポートされません。デフォルト設定の変更により、パッチインポートのフットプリントが削減され、Itaniumのパッチが不要なお客様がストレージ容量とダウンロード時間を節減できるようになりました。

enable-itanium-patchesスクリプトについて

- 場所: `/opt/opsware/mm_wordbot/util/enable-itanium-patches`
- 使用法: `enable-itanium-patches enable|disable`

WindowsサーバーのIA64パッチのインポートを有効にするには、次の手順を実行します。

1. rootとしてSAコアにログインします。
2. enable-itanium-patchesスクリプトを実行します。

   ```
   /opt/opsware/mm_wordbot/util/enable_itanium_patches enable
   ```

WindowsサーバーのIA64パッチのインポートを無効にするには、次の手順を実行します。

1. rootとしてSAコアにログインします。
2. enable-itanium-patchesスクリプトを実行します。

   ```
   /opt/opsware/mm_wordbot/util/enable_itanium_patches disable
   ```

現在の設定を表示するには、次の手順を実行します。

1. Opsware System Administratorsの権限を持つ管理者としてSA Webクライアントにログインします。

SA設定パラメーターには、SA Webクライアントからのみアクセスできます。Opsware System Administratorsユーザーグループの権限を持つシステム管理者だけが設定を変更できます。

2. SAソフトウェアリポジトリのシステム設定に移動します。[**管理**] > [**システム構成**] > [**ソフトウェアリポジトリ**] を選択します。
3. **patchman.ms_mbsa20_import_architectures**の設定で、有効/無効が示されます。
   - デフォルトは、`['x86', 'x64']` です。
   - `['x86', 'x64', 'ia64']` の場合、Itaniumパッチが有効であることを示します。

警告: この設定を変更するには、このビューを使用せずに、スクリプトを使用してください。このビューは、現在の設定を確認する目的のみに使用します。本ドキュメントに記載された、特定のSAコアの設定パラメーター値への変更は、HPで検証済みであるため、指示に従って安全に適用できます。ただし、SAコア構成パラメーターのデフォルト値を変更する場合には、コアの機能とパフォーマンスに悪影響を与える可能性があるので、十分注意してください。

Microsoftパッチデータベースメタデータの構成とインポート

Microsoftパッチデータベースを最初にインポートする際に、インポートのデフォルト設定を構成します。ここでは、初期のデータベースメタデータをインポートする際にSAクライアントを使用してどのパッチをいつインポートするかを構成する手順について説明します。

ここでは、実際のMicrosoftのパッチバイナリのインポート手順については説明しません。メタデータの構成とインポートが済んだら、SAクライアントまたはコマンドラインスクリプトを使用して、Microsoftパッチバイナリをインポートすることができます。これらのアクティビティについては、SAクライアントライブラリからのWindowsパッチのインポート (33ページ) およびコマンドラインからのMicrosoftパッチデータベースのダウンロード (34ページ) を参照してください。

Microsoftパッチデータベースをインポートする前に、SAコアとの通信時にWebプロキシを使用しないようにブラウザーを設定する必要があります。手順については、パッチデータベースおよびユーティリティのインポートに必要な前提条件 (57ページ) を参照してください。

SAクライアントを使用してデータベースをインポートするには、次の手順を実行します。

1. ナビゲーションペインで、[**管理**] > [**パッチ設定**] を選択します。
2. [Microsoft] タブで、[**パッチデータベース**] を選択します。
3. Microsoft Webサイトからデータベースをインポートするには、[**ベンダーからインポート**] をクリックします。

   [ベンダーからインポート] ウィンドウに、MicrosoftのWebサイト上のデータベースの場所のデフォルトURLが表示されます。[**インポート**] をクリックします。毎月リリースされるMicrosoftデータベースの最新バージョンを再度インポートする場合は、デフォルトURLを使用する必要があります。
4. データベースをローカルファイルシステムからインポートするには、[**ファイルからインポート**] をクリックします。

   [Microsoftパッチデータベースのインポート] ウィンドウで、ファイル名が`wsusscn2.cab`であることを確認して、[**インポート**] をクリックします。このファイルは、以前にMicrosoft Webサイトからダウンロードしてローカルファイルシステムにコピーしたものである必要があります。

インポートするには、SAソフトウェアリポジトリにインポート済みのMicrosoftパッチデータベースにパッチが存在する必要があります。詳細については、Windowsパッチデータベース競合レポートの [最終インポートのサマリー] フィールド (25ページ) も参照してください。

Microsoftパッチの補足データファイルの取得

SAでは、Microsoftから (wsusscn2.cabファイルから) Microsoftのパッチに関する情報を取得します。ただし、SAでは、Microsoftのパッチに関する有用な補足データが利用できます。これは、HP Live Networkから自動的に取得できます。この補足データが更新されたときに、SAのMicrosoftパッチデータベースに自動的にアップロードされるように、HP Live Networkを構成することができます。

データが更新されたときに補足データファイルを取得してSAライブラリにアップロードするには、次の手順を実行します。

1. 次のURLでHP Passport IDを取得します。

   http://h20229.www2.hp.com/passport-registration.html (英語サイト)
2. HP Passportの資格情報を使用して、HP Live Networkポータルにログインします。

   https://hpln.hp.com/group/hp-live-network-connector
3. HP Live Networkコネクター (LNc) は、SAのソフトウェアリポジトリコンポーネントがインストールされたコアサーバーにインストールされます。

   『HP Live Network Connector User Guide』は、次のURLにあるHP Live NetworkのLive Networkコネクターコミュニティからダウンロードできます。

https://hpln.hp.com/group/hp-live-network-connector

[**Resources**] タブをクリックして、[**Documentation**] フォルダーを開きます。

4 LNcがインストールされたシステムで、次のコマンドを実行して、Microsoftパッチ適用サービスを有効にします。

```
live-network-connector write-config --add --setting=content.ms_patch_supp=1
```

および

```
live-network-connector write-config --setting=sas.force_win_patch_import=1 --add
```

5 (オプション) Microsoftパッチ適用サービスを無効にするには、次のように値を0にして、同じコマンドを実行します。

```
live-network-connector write-config --setting=content.ms_patch_supp=0
```

および

```
live-network-connector write-config --setting=sas.force_win_patch_import=0
```

または、パッチの補足データファイルをHP Live Networkから手動でダウンロードして、SAデータベースにアップロードすることもできます。詳細については、Microsoftパッチの補足データファイルの手動ダウンロード (66ページ) を参照してください。

Microsoftパッチの補足データファイルの手動ダウンロード

ここでは、Microsoftパッチの補足データファイルをHP Live Networkから手動でダウンロードして、SAのパッチデータベースにアップロードする手順について説明します。Microsoftパッチの補足データファイルの取得 (65ページ) の手順に従って、このファイルが変更されたときに自動的にアップロードされるようにLNcをセットアップすることをお勧めします。ただし、ファイルを手動でダウンロードする場合は、定期的に更新を確認し、ここに記載した手順に従って、SAパッチデータベースにインストールするようにしてください。

補足データファイルを取得するには、次の手順を実行します。

1 次のURLでHP Passport IDを取得します。

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

2 HP Passportの資格情報を使用して、HP Live Networkポータルにログインします。

https://hpln.hp.com/group/hp-live-network-connector

3 HP Live Networkコネクター (LNc) は、SAのソフトウェアリポジトリコンポーネントがインストールされたコアサーバーにインストールされます。

『HP Live Network Connector User Guide』は、次のURLにあるHP Live NetworkのLive Networkコネクターコミュニティからダウンロードできます。

https://hpln.hp.com/group/hp-live-network-connector

[**Resources**] タブをクリックして、[**Documentation**] フォルダーを開きます。

4 HP Live Networkメニューで [Content Catalog] をクリックし、Server Automation製品の「MS Patch Supplement for Server Automation」を検索します。

5 最新の Microsoft Patch Supplement (`latest_OPSWWinPatchDB.zip`) をダウンロードして、次に示すコアのスライスサーバーディレクトリに配置します。

```
/opt/opsware/mm_wordbot/util
```

6 次のコマンドを使用して、Microsoft Patch Supplementメタデータをインポートします。

```
./import_win_patch_bundle --bundle latest_OPSWWinPatchDB.zip
```

7 HPではMicrosoftパッチの補足データファイルを更新します。そのため、このファイルの更新状況を定期的にチェックして、ファイルが更新されている場合は、これらの手順を再度実行して最新の補足パッチデータをSAのパッチデータベースにダウンロードすることをお勧めします。

パッチをトラッキングするWindows製品の選択

HP Server Automationでトラッキングするパッチを特定のWindows製品に制限することができます。Microsoftパッチデータベースをインポートする際にSAで表示される新規パッチは、選択した製品に限定されます。SAで以前に表示されていたパッチは引き続きトラッキングされます。Windows Update エージェント (WUA) のパッチをトラッキングすることもできます。

トラッキングするパッチを特定のWindowsオペレーティングシステムに制限するには、パッチを自動的にインポートするコマンドラインスクリプトを実行します。スクリプトの詳細については、コマンドラインからのMicrosoftパッチデータベースのダウンロード (34ページ) を参照してください。

SAクライアントを使用してパッチをトラッキングするWindows製品を選択するには、次の手順を実行します。

1 ナビゲーションペインで、[**管理**] > [**パッチ設定**] を選択します。

2 [Microsoft] タブで [パッチ製品] を選択して、[**編集**] をクリックします。

3 [パッチ製品の編集] ウィンドウで、追加 (+) および除外 (-) 矢印を使用して、パッチをインポートする製品を選択します。

4 [**OK**] をクリックして設定を保存します。

パッチコンプライアンススキャンのスケジュール設定

すべてのWindows管理対象サーバーでのパッチコンプライアンススキャンをスケジュール設定するには、次の手順を実行します。

1 ナビゲーションペインで、[**管理**] > [**コンプライアンス設定**] を選択します。

2 [コンプライアンス設定] の内容ペインの [パッチコンプライアンススケジュール] セクションで、[**設定の編集**] をクリックします。

3 [コンプライアンススキャンのスケジュール] ウィンドウで、[**コンプライアンススキャンの有効化**] を選択します。

4 [スケジュール] ドロップダウンリストから、スキャンの頻度を選択します。

[カスタム] を選択した場合は、次の値を使用して`crontab`文字列を指定します。

- 分 (0～59)
- 時間 (0～23)
- 日 (1～31)
- 月 (1～12)
- 曜日 (0～6、0=日曜)
- これらのフィールドにアスタリスク*を指定すると、可能なすべての値を表します。次の`crontab`文字列を指定すると、平日の深夜0時にジョブが実行されます。

```
0 0 * * 1-5
```

`crontab`文字列は、シリアル値 (1,2,3,4) と範囲 (1-5) でも指定できます。詳細については、Unixコンピューター上の`crontab`のmanページを参照してください。

5 [開始時刻] フィールドで、ジョブを開始する時刻を指定します。

6 [タイムゾーン] ドロップダウンリストから、ジョブ実行時刻のデフォルトタイムゾーンを選択するか、デフォルトのタイムゾーンを受け入れます。表示されたデフォルト時刻により、スケジュールされた時刻が [ユーザー設定] で設定したタイムゾーンに変換されます。希望のタイムゾーンを設定しなかった場合、タイムゾーンはHP Server Automationコアサーバーから導出されます (通常、UTC)。

7 [**OK**] をクリックして設定を保存します。

パッチコンプライアンスレベルの設定

パッチポリシーのコンプライアンスレベルでは、それぞれのパッチコンプライアンスレベルを定義します。

パッチコンプライアンスレベルを設定するには、次の手順を実行します。

1 ナビゲーションペインで、[**管理**] > [**コンプライアンス設定**] を選択します。

2 [コンプライアンスルール] ドロップダウンリストから、[ポリシーのみ]、[ポリシーと例外]、[カスタマイズ済み] のいずれかのコンプライアンスレベルを選択します。

[カスタマイズ済み] を選択する場合は、[**カスタムの編集**] をクリックして、[カスタマイズされたポリシーコンプライアンスレベルの編集] ウィンドウを開きます。コンプライアンスレベルを編集するには、[コンプライアンス結果] 列のアイコンをクリックします。[**適用**] をクリックして変更内容を保存します。

Windowsパッチユーティリティのインポート

Windowsサーバーでパッチ管理を行えるようにするには、Windowsパッチユーティリティをインポートする必要があります。

SAを使用したWindowsサーバーの管理を行わない場合は、必要に応じてこれらのファイルをインストールしないことを選択できます。この場合でも、インストールは正常に完了します。ただしこれらのファイルをインストールしないと、Windowsサーバーに対する操作を実行できません。ファイルは、Windowsパッチの適用以外にも、多数のWindowsベースの操作で必要となります。

SAコアのインストール時に、`windows_util_loc`パラメーターを`none`に設定した場合、コアのインストール時にWindowsユーティリティはインポートされないため、Windowsサーバーでの操作はサポートされません。詳細については、『SA Installation Guide』を参照してください。

Windowsユーティリティをインポートする前に、SAコアとの通信時にWebプロキシを使用しないようにブラウザーを設定する必要があります。手順については、パッチデータベースおよびユーティリティのインポートに必要な前提条件 (57ページ) を参照してください。

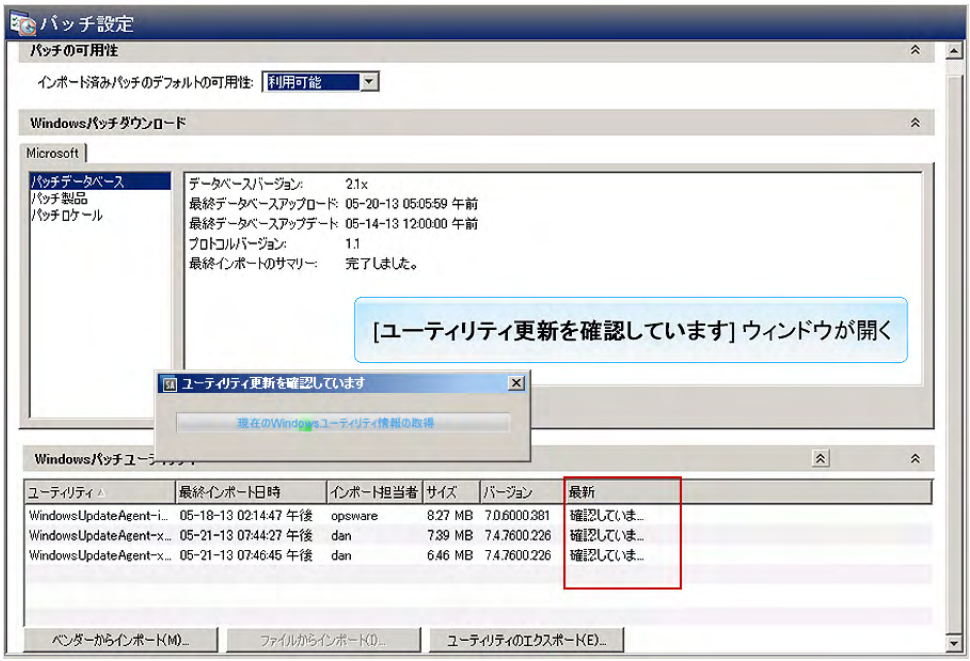
SAコアのインストール後に、ベンダーから次のWindowsユーティリティをインポート (ダウンロード) することができます。

- WindowsUpdateAgent-ia64.exe
- WindowsUpdateAgent-x64.exe
- WindowsUpdateAgent-x86.exe

Windowsパッチユーティリティの更新およびインポートを行うには、次の手順を実行します。

1 ナビゲーションペインで、[**管理**] > [**パッチ設定**] を選択します。

2 [パッチ設定] ウィンドウに、Windowsパッチユーティリティの更新状況が表示されます。



[Windowsパッチユーティリティ] セクションの [**最新**] 列に、更新の確認中であることが表示されます。

- [**最新**] 列には、ベンダーから提供されている最新バージョンが表示されます。
- [**バージョン**] 列には、SAデータベース内にすでに存在しているユーティリティのバージョンが表示されます。

3 インターネットに接続している場合、[**最新**] 列はベンダーから提供されている最新バージョンに更新されます。

a [**最新**] 列の値と [**バージョン**] 列の値を比較します。

b SA データベースの [**バージョン**] がベンダーから提供されている [**最新**] バージョンよりも低い場合は、ユーティリティを更新する必要があります。

c [**ベンダーからインポート**] をクリックして、最新のユーティリティを取得します。

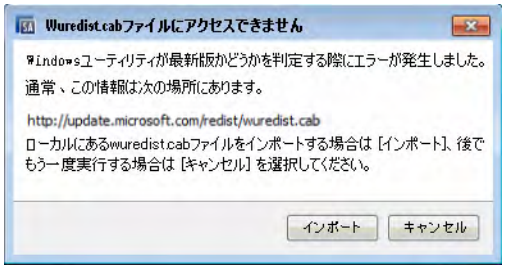
d [ベンダーからインポート] ウィンドウで、1つまたは複数のユーティリティを選択して、[**インポート**] をクリックします。

[ユーティリティアップデートをインポートしています] ウィンドウに、インポートプロセスのステータスが表示されます。

- ジョブが完了すると、[ステータス] 列に成功アイコン ✔ が表示されます。
- ジョブが失敗すると、[ステータス] 列にエラーアイコン ✘ が表示されます。エラーアイコンをクリックすると、エラーメッセージが表示されます。

e インポートプロセスが完了したら、[**閉じる**] をクリックします。

4 インターネットに接続されていない場合は、[Unable to Access wuredist.cab] ウィンドウが表示されます。このウィンドウでは、ローカルファイルからWindows Updateエージェント (wuredist.cab) をインポートすることができます。



a [**インポート**] をクリックします。

b [パッチユーティリティのインポート] ダイアログで、ローカルにあるwuredist.cabファイルを選択します。

c [**インポート**] をクリックして、ユーティリティアップデートをインポートします。

d インポートが完了したら、[最新] 列で更新されたユーティリティを確認できます。

Windowsパッチ管理ファイルのダウンロードとインストール (オプション)

SA Windowsパッチ管理機能を使用するには、Microsoftソフトウェアダウンロードリポジトリからのファイルが必要です。これらのファイルは、コアインストール中にインストールされます。

➤ SAを使用してWindowsサーバーを管理しない場合、ファイルをインストールしないことを選択しても、インストールは正常に完了します。ただしこれらのファイルをインストールしないと、Windowsサーバーに対する操作を実行できません。ファイルは、Windowsパッチの適用以外にも、多数のWindowsベースの操作で必要となります。

必要なWindowsパッチ管理ファイルの既存コアへのインストール

Windowsパッチを後から適用する場合、SAクライアントのインポート機能、または『SAユーザーガイド: サーバーのパッチ適用』で説明する `populate-opsware-update-library` コマンドラインスクリプトを使用して、必要なWindowsパッチ管理ファイルをインストールする必要があります。

Windowsパッチユーティリティの手動ダウンロードの詳細については、Windowsパッチユーティリティの手動での取得 (71ページ) を参照してください。

サポート対象のWindowsバージョン

お使いのバージョンのSAでサポートされる管理対象サーバープラットフォームについては、『SA Support and Compatibility Matrix』を参照してください。

➤ Windows Server 2003 RTMが実行されている管理対象サーバーにパッチを適用するには、これらのサーバーにMicrosoft 更新プログラム MS04-011 (またはそれ以降の更新プログラム) が適用されていることを確認する必要があります。

要件

管理対象サーバーは、次のWindowsパッチ適用要件を満たしている必要があります。

- Windowsインストーラー 3.1がインストールされている
- MSXML 3+がインストールされている (MSXMLはすべてのWindows管理対象サーバーの一般的な要件です。管理対象サーバーがWindowsパッチ適用機能を使用するかどうかは関係ありません)
- Windows Updateエージェントがインストールされている
- Windows Updateサービスが無効になっておらず、アップデートをチェックしないように設定されている

Windowsパッチユーティリティの手動での取得

コアのインストール時にWindowsパッチ管理ファイルをインストールしておらず、SAコアおよびSAクライアントにインターネットアクセスがない場合は、インターネットにアクセスできるマシンから次のタスクを実行して、ファイルの取得とコアへの転送を行うことができます。

Microsoftから次のパッチ管理ファイルを取得します。

ここでは、読者の便宜のためにファイルへのリンクを記載していますが、これらのリンクはドキュメントのリリース後にMicrosoft Corporationによって変更される可能性があります。そのため、これらのリンクを使用する際にリンクが無効になっている可能性があります。その場合は、Microsoftのサポート Webサイトで正しいファイルを検索してください。

1. wsusscn2.cab

   `wsusscn2.cab`ファイルにMicrosoftパッチデータベースが保存されています。

   `wsusscn2.cab`を次のサイトからダウンロードします。

   http://go.microsoft.com/fwlink/?LinkId=76054

2. `WindowsUpdateAgent30-x86.exe`

   `WindowsUpdateAgent30-x86.exe`ファイルは、SAがx86ベースの管理対象サーバーをスキャンして、どのWindowsパッチ/ホットフィックスがインストールされているかを判断する際に必要です。

   a. `WindowsUpdateAgent30-x86.exe`を含むパッケージを次のサイトからダウンロードします。

      http://go.microsoft.com/fwlink/?LinkID=100334

   b. ダウンロード後、ファイルの名前を"`WindowsUpdateAgent-x86.exe`"に変更します。

3. `WindowsUpdateAgent30-x64.exe`

   `WindowsUpdateAgent30-x64.exe`ファイルは、SAがx64ベースの管理対象サーバーをスキャンして、どのWindowsパッチ/ホットフィックスがインストールされているかを判断する際に必要です。

   a. `WindowsUpdateAgent30-x64.exe`を含むパッケージを次のサイトからダウンロードします。

      http://go.microsoft.com/fwlink/?LinkID=100335

   b. ダウンロード後、ファイルの名前を"`WindowsUpdateAgent-x64.exe`"に変更します。

4. **WindowsUpdateAgent30-ia64.exe**

   `WindowsUpdateAgent30-ia64.exe`ファイルは、SAがItanium x64ベースの管理対象サーバーをスキャンして、どのWindowsパッチ/ホットフィックスがインストールされているかを判断する際に必要です。

   a. `WindowsUpdateAgent30-ia64.exe`を含むパッケージを次のサイトからダウンロードします。

      http://go.microsoft.com/fwlink/?LinkID=100336

   b. ダウンロード後、ファイルの名前を"`WindowsUpdateAgent-ia64.exe`"に変更します。

Windowsパッチユーティリティのエクスポート

次のWindowsユーティリティをServer Automationからローカルファイルシステムにエクスポートすることができます。

- WindowsUpdateAgent-ia64.exe
- WindowsUpdateAgent-x64.exe
- WindowsUpdateAgent-x86.exe

Windowsパッチユーティリティをエクスポートするには、次の手順を実行します。

1. ナビゲーションペインで、[**管理**] > [**パッチ設定**] を選択します。
2. [Windowsパッチユーティリティ] セクションで、1つまたは複数のユーティリティを選択します。
3. [**ユーティリティのエクスポート**] をクリックします。
4. [パッチユーティリティのエクスポート] ウィンドウで、ファイルシステム内の場所を指定します。
5. [**エクスポート**] をクリックします。

再起動が必要なサーバーの検索

再起動保留中の状態が発生する代表的なケースは、次のとおりです。

- Windows パッチまたはパッケージをインストールまたはアンインストールして、再起動を実行していない場合、サーバーには再起動が必要のマークが付きます。
- Windowsパッケージをインストールまたはアンインストールして、パッケージのSAメタデータで再起動を要求する指示があるにも関わらず、再起動を実行していない場合、サーバーには再起動が必要のマークが付きます。

サーバーの状態が再起動保留中である場合、その後のパッチのインストールやアンインストールは失敗する可能性があります。サーバーまたはサーバーグループ (デバイスグループ) でパッチのインストールやアンインストールを行う前に、サーバーを再起動する必要があります。

SAでは、管理対象サーバーのプロパティを確認したり、管理対象サーバーのリストをフィルター処理したりして、個別の管理対象サーバーで再起動が必要かどうかを簡単に確認することができます。また、SAクライアントの検索機能を使用して、データセンター内の再起動が必要なすべての管理対象サーバーとデバイスグループを検索することもできます。

単一の管理対象サーバーでの再起動

管理対象サーバーのプロパティを確認して、サーバーの再起動が必要かどうかを判断します。

この情報を確認するには、次の手順を実行します。

1. [すべての管理対象サーバー] ペインでサーバーを選択し、[表示] ドロップダウンリストで [プロパティ] を選択します。
2. 下部の [プロパティ] ペインで、[再起動が必要] フィールドを確認します。値が「はい」の場合は、このサーバーの再起動が必要です。
3. 選択したサーバーで、右クリックして [サーバーの再起動] を選択し、サーバーの再起動ウィザードを使用して、サーバーを手動で再起動するか、サーバーを再起動するスケジュールを設定します。詳細については、サーバーの再起動 (92ページ) を参照してください。

すべての管理対象サーバーでの再起動

[すべての管理対象サーバー] ペインをフィルター処理すると、再起動が必要なサーバーを簡単に特定することができます。

この情報を確認するには、次の手順を実行します。

1 [すべての管理対象サーバー] ペインで、検索ツール  を使用して [再起動が必要] を選択します。

2 [再起動が必要] 列の値が「はい」の場合、このサーバーの再起動が必要です。

この列の表示設定を確認するには、列セレクター  を使用します。

3 1つまたは複数の選択したサーバーで、右クリックして [サーバーの再起動] を選択し、サーバーの再起動ウィザードを使用して、サーバーを手動で再起動するか、サーバーを再起動するスケジュールを設定します。詳細については、サーバーの再起動 (92ページ) を参照してください。

複数のサーバーとデバイスグループでの再起動

SAクライアントの検索機能を使用して、パッチまたはパッケージがインストールされたサーバーで、再起動が必要なすべてのサーバーを検索します。この情報を使用すると、これらのサーバーおよびデバイスグループの再起動をスケジュール設定することができます。

再起動が必要なサーバーおよびデバイスグループを検索するには、次の手順を実行します。

1 [詳細検索] ウィンドウの [場所] フィールドで、[再起動が必要] を選択します。

2 デフォルト演算子として [次の値に等しい] をそのまま使用します。

3 [値の選択] ダイアログの [利用可能] で「はい」を選択し、プラス (+) 矢印をクリックしてこの設定を [選択済み] に移動します。

4 [**OK**] をクリックして [値の選択] の設定を保存します。

5 [詳細検索] ウィンドウで、[**検索**] をクリックして、再起動が必要なサーバーのリストを表示します。このリストのサーバーは、[再起動が必要] 列に「はい」と表示されます。

6 このリストのサーバーを1つまたは複数選択します。

7 右クリックして [サーバーの再起動] を選択し、サーバーの再起動ウィザードを使用して、1つまたは複数のサーバーまたはデバイスグループを手動で再起動するか、再起動のスケジュールを設定します。詳細については、サーバーの再起動 (92ページ) を参照してください。

パッチのロケール

パッチのロケールでは、パッチを受け取るWindowsサーバーの言語を識別します。同じ名前の1つのパッチを異なる複数のロケールで利用できる場合があります。たとえば、Q123456 という名前のパッチは、英語版と日本語版の Windows が稼働するサーバーで利用できます。パッチの名前は同じでも、英語版のサーバーと日本語版のサーバーにインストールされるパッチのバイナリは異なります。

Windowsパッチ管理では、同じSAマルチマスターメッシュ内で複数のロケールをサポートしています。異なるロケールを持つWindowsサーバーにパッチをインストールする場合は、パッチを名前で指定します。SAでは、インストール (またはポリシー修復) 時に、パッチのロケールと各管理対象サーバーのロケールを照合します。ロケールごとにインストールを行う必要はありません。

サポートされるロケール

Windowsパッチ管理では、次のロケールに対するMicrosoftパッチをサポートしています。

- 英語 (en)

- フランス語 (fr)
- ドイツ語 (de)
- イタリア語 (it)
- 日本語 (ja)
- 韓国語 (ko)

ロケールの構成タスク

デフォルトでは、Windowsパッチ管理は、英語のロケールのみをサポートしています。英語以外のロケールでのWindowsパッチ適用をセットアップするには、次の各項の手順を実行します。

- 英語以外のロケールでのSAコアの構成 (74ページ)
- インポートするパッチのロケールの選択 (75ページ)
- 英語以外のロケールを使用する場合のエンドユーザー要件 (75ページ)

英語以外のロケールでのSAコアの構成

このタスクでは、コアサーバー対するrootアクセスとSA Webクライアントの再起動が必要です。

コアを英語以外のロケール用に構成するには、SA Webクライアントを実行している各コアサーバーで次の手順を実行します。

1. rootとしてサーバーにログオンします。
2. /etc/opt/opsware/occ/psrvr.properties内の次の行を

   pref.user.locales

   次のように変更します

   pref.user.localesAllowed=en;ja;ko
3. 次のコマンドでコア上のSA Webクライアントを再起動します。

   /etc/init.d/opsware-sas restart occ.server
4. テキストエディターで、次のファイルを開きます。

   /opt/opsware/occclient/jnlp.tmpl
5. 日本語の場合は、jnlp.tmplファイルの<resources>セクションに、次のXML要素を追加します。

```
<property name="com.opsware.ngui.font.japanese" value="Arial Unicode MS"/>
```

6. 韓国語の場合は、jnlp.tmplファイルの<resources>セクションに、次のXML要素を追加します。

```
<property name="com.opsware.ngui.font.korean" value="Arial Unicode MS"/>
```

7. /opt/opsware/occclientディレクトリで、次のファイルが存在する場合は、これらのファイルを削除します。

   $HOST_ja.jnlp
   $IP_ja.jnlp
   $HOST_ko.jnlp
   $IP_ko.jnlp
8. インポートするパッチのロケールの選択 (75ページ) の手順を実行します。

インポートするパッチのロケールの選択

この項の手順を実行する前に、英語以外のロケールでのSAコアの構成 (74ページ) の手順を実行します。

この操作では、HP Server Automationにインポートするwindowsパッチのロケールを選択します。ここで選択した内容は、次回パッチをSAにインポートする際に反映されます。パッチのインポートが済んだら、管理対象サーバーにインストールできます。この操作でリストからロケールを削除しても、すでにインポート済みの削除したロケールのパッチはSAから削除されません。

SAにインポートするWindowsパッチのロケールを選択するには、次の手順を実行します。

1. ナビゲーションペインで、[**管理**] を選択します。
2. [**パッチ設定**] を選択します。
3. [Microsoft] タブで、[パッチロケール] を選択します。
4. [**Edit**] をクリックします。
5. [パッチロケールの編集] ウィンドウで、追加 (+) および除外 (-) 矢印を使用して、パッチをインポートするロケールを選択します。

   サポートされるロケール (73ページ) に表示されていないロケールを選択したい場合には、サポートに連絡してください。
6. [**OK**] をクリックして設定を保存します。
7. 英語以外のロケールを使用する場合のエンドユーザー要件 (75ページ) の手順を実行します。

英語以外のロケールを使用する場合のエンドユーザー要件

SAクライアントで英語以外のフォントを表示するには、次の手順を実行します。

1. SAクライアントを実行しているWindowsデスクトップで、Arial Unicode MSフォントが使用されていることを確認します。
2. システム管理者が英語以外のロケールでのSAコアの構成 (74ページ) の手順を実行した後に、エンドユーザーはSAクライアントにログオンして、SAクライアントウィンドウの右上にある [ログインユーザー] リンクを選択します。これにより、[ユーザー] ウィンドウが表示されます。[プロパティ] ビューを選択します。
3. [ユーザーのプロパティ] ビューで、エンドユーザーは [ユーザー設定] セクションの [ロケール] フィールドを更新します。たとえば、システム管理者がコアを日本語用に構成した場合、エンドユーザーは [ロケール] フィールドを日本語に設定します。

パッチのインストール

パッチ管理では、次の2つのフェーズでパッチをインストールします。

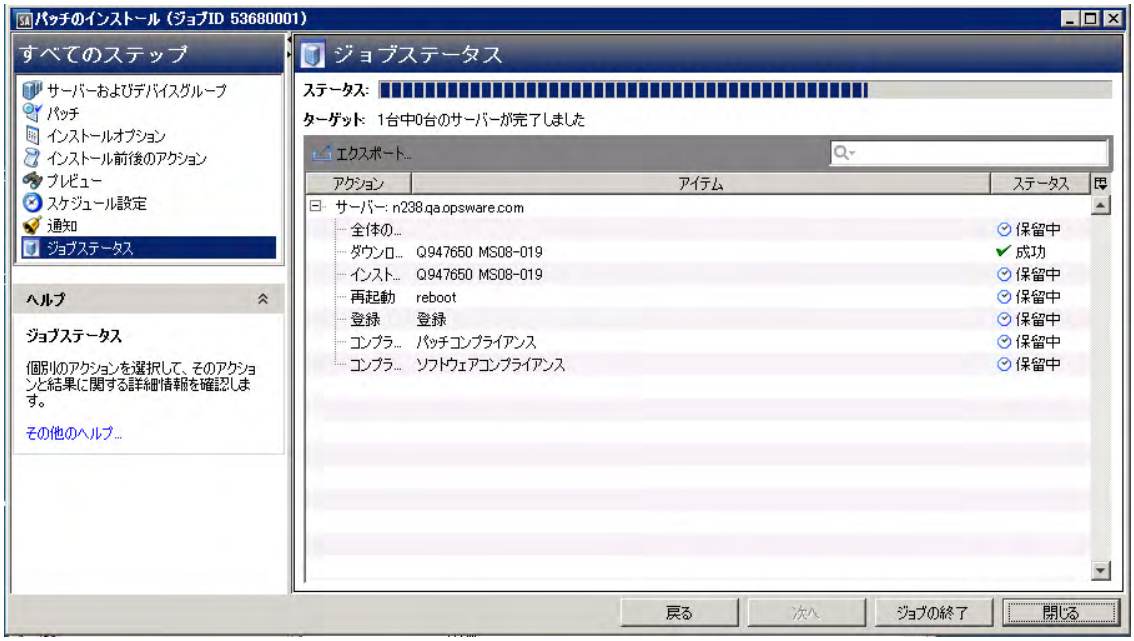
- **フェーズ1—ダウンロード/ステージング**: このフェーズでは、HP Server Automationから管理対象サーバーへパッチをダウンロードします。このフェーズは、一般的にステージングと呼ばれます。
- **フェーズ2—インストール/デプロイメント**: このフェーズでは、管理対象サーバーにパッチをインストールします。このフェーズは、一般的にデプロイメントと呼ばれます。

パッチがダウンロード (ステージング) されたらすぐにインストールを行うかどうかを指定できます。また、日時をスケジュール設定して後でインストールを行うこともできます。また、Windows パッチ管理では、複数のパッチのベストエフォート型インストールのニーズにも対応しており、いずれかのパッチでエラーが発生した場合でも、パッチのインストールを続行するように指定することが可能です。

Windowsパッチ管理では、パッチをインストールするためにSAエージェントが管理対象サーバー上で実行するコマンドの名前 (.exe ファイルや定義済みのコマンドライン引数など) が表示されます。これらのデフォルトのコマンドライン引数はオーバーライドできます。

パッチ管理では、Windows パッチのインストールを適切に管理できるように、サーバーの再起動オプションの管理、インストール前 / インストール後スクリプトの指定、パッチのインストールのシミュレート (プレビュー)、インストールプロセスのステータスを通知する電子メール通知の設定などを行うことができます。これらの条件は、[パッチのインストール] ウィザードを使用して設定することができます。詳細については、図8を参照してください。

図8　　[パッチのインストール] ウィザード



インストールフラグ

Windows パッチをインストールする際には、インストールフラグを指定できます。ただし、HP Server Automation では、デフォルトのインストールフラグが使用され、これらのフラグを使用してパッチをインストールする必要があります。そのため、HP Server Automationから渡されるデフォルトのインストールフラグを無効にするフラグや矛盾するフラグを指定しないようにする必要があります。コマンドおよびフラグの指定方法については、Windowsインストールオプションの設定 (79ページ) を参照してください。

Windowsホットフィックスの中には、-zフラグをサポートしないもの、-qフラグをサポートしないもの、いずれか一方をサポートしないものがあります。このような場合はそれぞれ、/-z 、/-q 、/-z -qという特殊な表記を使用する必要があります。これにより、Windowsパッチ管理で、-z、-q、または-z -qフラグでの受け渡しを防ぐことができます。SAでは、デフォルトで、パッチのインストール時に/z /qがコマンドライン引数に追加されます。これを無効にするには、/-z /-qを指定します。たとえば、再起動を抑制しない場合は、/-zを指定します。

次の表に、HP Server Automationで使用されるデフォルトのインストールフラグを示します。

表4　　デフォルトのインストールフラグ

Windowsパッチタイプ	フラグ
Windowsホットフィックス	-q -z
Windowsセキュリティロールアップパッケージ (Windowsパッチ管理でホットフィックスと同様に扱われる)	-q -z
Windows OSサービスパック	-u -n -o -q -z

アプリケーションのパッチ

Windowsパッチ管理では、パッチの対象ではないオペレーティングシステムにパッチを適用することはできません。アプリケーションのパッチをインストールする場合、アドホックインストールでは対応するアプリケーションがインストールされていないサーバーが自動的に除外されることはありません。Windowsパッチ管理では必要なアプリケーションがインストールされていないサーバーの除外は行われませんが、このようなサーバーにアプリケーションのパッチを適用しないように注意する必要があります。パッチがサーバーにインストールされていないアプリケーション用である場合、そのパッチは適用されず、「パッケージ<パッケージ名>でエラーが発生しました」といったエラーメッセージが表示されます。

アプリケーションのパッチが同じオペレーティングシステムの複数のバージョンで実行されているアプリケーション用である場合、このパッチをすべてのサーバーに同時に適用することはできません。アプリケーションのパッチは、1つのオペレーティングシステムバージョンのみに関連付けられます。最初に特定のオペレーティングシステム用のパッチを選択してから、アプリケーションがインストールされているサーバーを選択し、パッチを適用します。アプリケーションがインストールされているオペレーティングシステムのバージョンごとに、このプロセスを繰り返す必要があります。

同様に、同一のオペレーティングシステムの複数のバージョンにインストールされているアプリケーションのパッチをアンインストールする際に、すべてのパッチを同時にアンインストールすることはできません。パッチがインストールされているオペレーティングシステムのバージョンごとに、このアンインストールプロセスを繰り返す必要があります。

サービスパック、更新プログラムのロールアップ、ホットフィックス

サービスパック、更新プログラムのロールアップ、またはホットフィックスをインストールする場合、確認ダイアログが表示されたときに遅延が生じることが知られています。SAエージェントはパッチのインストールまたはアンインストールを実行しているため、確認ダイアログに応答することができません。ユーザーが確認ダイアログで **[OK]** をクリックしないと、エージェントはインストールまたはアンインストールをタイムアウトします。

- ホットフィックスの場合、5分間経過して確認ダイアログの [OK] がクリックされていない場合にタイムアウトします。
- サービスパックおよび更新プログラムのロールアップの場合は、60分間経過して確認ダイアログの **[OK]** がクリックされていない場合にタイムアウトします。

これを防ぐには、パッチのインストールコマンドやアンインストールコマンドで、サイレントモードのインストールやアンインストールを実行する引数を指定します。デフォルトでは、-qフラグが設定されます。

Windowsオペレーティングシステムのサービスパックの要件

Windowsオペレーティングシステム (OS) サービスパックは、単独でインストールする必要があります。

ホットフィックス、更新プログラム、サービスパックなどのWindows更新アイテムを組み合わせてインストールする場合には、他の更新アイテムをインストールする前に、各Windows OSサービスパックをそれぞれ単独でインストールする (それぞれのインストールの完了後にシステムを再起動する) ことが重要です。これにより、後続のサービスパックにロールアップされる不要なホットフィックスをインストールすることによって生じるエラーを防ぐことができます。

通常、ホットフィックスにはすぐに改良版がリリースされます。これらは、その後のサービスパックにロールアップされます。そのため、サービスパックの前にホットフィックスをインストールしたり、ホットフィックスとサービスパックを同時にインストールすると、ホットフィックスが重複してインストールされて、インストールエラーが発生する可能性があります。

要件: Windows OSサービスパックはそれぞれ専用のポリシーに分離し、それぞれを単独で (各サービスパックを個別の修復またはアドホックインストールジョブで) インストールします。システムを再起動してから、残りのベンダー推奨ポリシーの更新をインストールします。

他の更新アイテムと同じ修復ジョブでWindows OSサービスパックをインストールしないでください。インストールエラーが発生する可能性があります。

Windowsパッチのインストール

パッチを管理対象サーバーにインストールするには、事前にパッチを HP Server Automation にインポートして、ステータスを利用可能にしておく必要があります。制限付きのマークの付いたパッチは、必要なアクセス権を持つ管理者がインストールできます。

パッチを管理するにはアクセス権が必要です。必要なアクセス権の取得については、システム管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

パッチとサーバーを明示的に選択してインストールを実行できます。また、パッチポリシー例外が [常にインストールしない] の場合でも、パッチをインストールすることができます。

Windows OSサービスパックをインストールする必要がある場合は、OSサービスパックを個別の専用ポリシーに分離し、それぞれを単独で (個別の修復またはアドホックインストールジョブで) インストールした後に、残りのベンダー推奨のポリシーの更新をインストールすることが重要です。詳細については、Windowsオペレーティングシステムのサービスパックの要件 (77ページ) を参照してください。

管理対象サーバーにパッチをインストールするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。
2. [パッチ] を展開して、特定のWindowsオペレーティングシステムを選択します。
3. 内容ペインで、パッチを選択します。
4. [表示] ドロップダウンリストから、[サーバー] (または [デバイスグループ]) を選択します。
5. [表示] ドロップダウンリストから、[**パッチがインストールされていないサーバー**] または [**パッチがインストールされていないデバイスグループ**] を選択します。
6. プレビューペインで、1つまたは複数のサーバーを選択します。
7. [**アクション**] メニューで [**パッチのインストール**] を選択します。

   [パッチのインストール] ウィンドウの最初のステップ : 1. [サーバーおよびデバイスグループ] が表示されます。
   各ステップの手順については、次の項を参照してください。
   - Windowsインストールオプションの設定
   - Windowsパッチのインストールでの再起動オプションの設定
   - Windowsパッチのインストールでのインストールスクリプトの指定

- Windowsパッチのインストールのスケジュール設定
- Windowsパッチのインストールでの電子メール通知の設定
- Windowsパッチのインストールのプレビュー
- Windowsパッチのインストールジョブの進行状況の表示

1つのステップが完了したら、[**次へ**] をクリックして次のステップへ進みます。[**ジョブの開始**] をクリックする前に、ステップリストに表示される完了したステップをクリックすることで、そのステップに戻って変更を行うことができます。

8 インストールジョブを起動する準備ができたら、[**ジョブの開始**] をクリックします。

ジョブを後で実行するようにスケジュール設定している場合でも、ジョブの開始後にパラメーターを変更することはできません。

ジョブが完了するまで [パッチのインストール] ウィンドウが開いている場合、Windowsパッチ管理により [すべての管理対象サーバー] ウィンドウの [パッチコンプライアンス] 列の関連するサーバーのコンプライアンスカウント (括弧内) が更新されます。[**F5**] キーを押すか、[表示] メニューの [**更新**] を選択して、[パッチのプレビュー] ペインの情報を更新します。

パッチをインストールする別の方法については、パッチポリシーの修復 (41ページ) を参照してください。

Windowsインストールオプションの設定

次のタイプのパッチのインストールオプションを指定することができます。

- パッチがダウンロードされたらすぐにパッチのインストールを行うか、日時を指定して後でインストールを行う。
- いずれか1つのパッチでエラーが発生した場合でも、パッチのインストールプロセスを中断しない。
- さまざまなコマンドラインオプションを使用してインストールを行う。

これらのオプションを設定するには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [インストールオプション] ステップに進みます。

2 次のいずれかのステージインストールオプションを選択します。

- **継続**: すべてのフェーズを連続する1つの操作として実行できます。
- **ステージ**: ダウンロードとインストールをスケジュール設定して別々に実行することができます。

3 いずれかのパッチでエラーが発生した場合でもパッチのインストールプロセスを続行する場合は、[**エラーオプション**] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

4 [**インストールコマンド**] テキストボックスに、表示されるコマンド (.exeファイル) のコマンドライン引数を入力します。デフォルトで、HP Server Automationでは`/z /q`が追加されます。これらのインストールフラグを無効にする場合は、テキストボックスに`/-z /-q`と入力します。

5 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

Windowsパッチのインストールでの再起動オプションの設定

サーバーの再起動によるダウンタイムを最小限に抑えるため、サーバーを再起動するタイミングを制御できます。ベンダーの再起動割り当てを調整、パッチをインストールするたびにサーバーを再起動、すべてのサーバーの再起動を完全に抑制、またはすべてのパッチがインストールされるまで再起動を延期することができます。

[パッチのインストール] ウィンドウで再起動オプションを選択する場合、HPではMicrosoftの再起動推奨設定 ([**個別のソフトウェアアイテムの指定に基づいてサーバーを再起動**] オプション) を使用することを推奨しています。Microsoft の再起動設定を使用できない場合は、単一再起動オプション ([**すべてのパッケージがインストールまたはアンインストールされるまですべてのサーバーの再起動を保留する**] オプション) を選択します。このようにしないと、次の再起動が (SAの制御対象外)実行されるまで、WUAでサーバーにインストールされているパッチが正しく通知されない可能性があります。

パッチのインストールの完了後にサーバーを再起動するかどうかを指定するオプションです。これらのオプションは、[パッチのインストール] ウィンドウから起動したジョブのみに適用されます。これらのオプションを設定しても、[パッチのプロパティ] ウィンドウの [インストールパラメーター] タブにある [再起動が必要] オプションが変更されることはありません。

サーバーの状態が再起動保留中である場合、その後のパッチのインストールは失敗する可能性があります。サーバーでパッチのインストールを行う前に、サーバーを再起動する必要があります。詳細については、再起動が必要なサーバーの検索 (72ページ) を参照してください。

次に示すオプションの設定は、最初のオプションを除いて、[再起動が必要] オプションの設定よりも優先します。

- **個別のソフトウェアアイテムの指定に基づいてサーバーを再起動** (デフォルト): デフォルトでは、パッチプロパティの [再起動が必要] オプションの設定に従って再起動が行われます。
- **各パッチのインストール後にサーバーを再起動**: パッチプロパティの [再起動が必要] オプションが設定されていない場合でも、サーバーを再起動します。複数のパッチをインストールする場合、サーバーの再起動も複数回行われます。
- **すべてのサーバーの再起動を抑制**: パッチプロパティの [再起動が必要] オプションが設定されている場合でも、サーバーを再起動しません。ベンダー設定によっては、抑制オプションを無視して強制的に再起動を行う場合があります。サービスパックの場合、再起動を抑制すると、アクションが未完了になります (再起動するまでサービスパックは未インストールになります)。パッチやサービスパックはインストール済みの状態になりません。ステータスは「未インストール/アンインストール」になります。システムを手動でチェック (レジストリまたはサーバーのプロパティを確認) する場合、SAクライアントに表示される内容と同じにはなりません。再起動後、次にソフトウェア登録を行うまで、SAクライアントに正しいソフトウェアやパッチのインストール情報は反映されません。

  注: Windowsパッチのインストール時に再起動を抑制すると (サービスパックの場合など)、システムのソフトウェア状態が正しく表示されない可能性があります。正確な状態は、管理対象サーバーが再起動され、ソフトウェア登録が完了した後に表示されます。
- **すべてのパッケージがインストールまたはアンインストールされるまですべてのサーバーの再起動を保留する**: 選択したパッチの中に [再起動が必要] オプションが設定されているものが含まれていても、他のパッチにそのオプションが設定されていない場合、すべてのパッチのインストール後にサーバーが1回再起動されます。一般的に、このオプションは単一再起動オプションと呼ばれます。選択したパッチの中に [再起動が必要] オプションが設定されているものがない場合、サーバーは再起動されません。

再起動オプションを設定するには、次の手順を実行します。

1. [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [インストール前後のアクション] ステップに進みます。
2. いずれかの再起動オプションを選択します。
3. [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

Windowsパッチのインストールでのインストールスクリプトの指定

パッチごとにインストールの前または後に実行するコマンドまたはスクリプトを指定できます。インストール前スクリプトでは、たとえば、管理対象サーバー上で特定の条件をチェックすることができます。条件が満たされない場合やインストール前スクリプトが失敗した場合、パッチはインストールされません。インストール前スクリプトを使用すると、パッチを適用する前にサービスやアプリケーションをシャットダウンすることもできます。インストール後スクリプトを使用すると、管理対象サーバー上でクリーンアッププロセスを実行することができます。

また、インストールフェーズまたはダウンロードフェーズの前または後に、管理対象サーバー上で次のタイプのスクリプトを実行するように指定することもできます。

- **ダウンロード前**: SAから管理対象サーバーにパッチをダウンロードする前に実行するスクリプト。[インストールオプション] ステップで [ステージ] を選択した場合にのみ利用できます。
- **ダウンロード後**: SAから管理対象サーバーにパッチをダウンロードした後で、パッチをインストールする前に実行するスクリプト。[インストールオプション] ステップで [ステージ] を選択した場合にのみ利用できます。
- **インストール前**: 管理対象サーバーにパッチをインストールする前に実行するスクリプト。
- **インストール後**: 管理対象サーバーにパッチをインストールした後に実行するスクリプト。

インストール前スクリプトを指定するには、次の手順を実行します。

1. [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [インストール前後のアクション] ステップに進みます。
2. [インストール前] タブを選択します。各タブでさまざまなスクリプトとオプションを指定できます。
3. [スクリプトの有効化] を選択します。このオプションを選択すると、タブのフィールドの残りの部分が有効になります。[スクリプトの有効化] を選択しない場合、スクリプトは実行されません。
4. [保存されたスクリプト] または [アドホックスクリプト] を選択します。

   保存されたスクリプトは、前にSA Webクライアントを使用してServer Automationに保存されたものです。スクリプトを指定するには、[**選択**] をクリックします。

   アドホックスクリプトはこの操作に対してのみ実行され、Server Automation に保存されません。タイプ (.batなど) を選択します。[スクリプト] ボックスに、スクリプトが存在する場所のドライブ文字を含むスクリプトの内容を入力します (echo dir>> C:\temp\preinstall1.log など)。ドライブ文字を入力しない場合、デフォルトは%SYSTEMDRIVE%になります。これは、Windowsのシステムフォルダーがインストールされている場所です。
5. スクリプトでコマンドラインフラグが必要である場合、[コマンド] テキストボックスにフラグを入力します。
6. [ユーザー] セクションで情報を選択します。ローカルシステム以外のシステムを選択する場合は、ユーザー名、パスワード、ドメインを入力します。このユーザーによってスクリプトが管理対象サーバー上で実行されます。
7. スクリプトがエラーを返した場合にインストールを停止するには、[エラー] チェックボックスを選択します。
8. [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

Windowsパッチのインストールのスケジュール設定

Windowsのパッチ適用の2つのフェーズは切り離すことができます。そのため、パッチをインストールするタイミングをパッチをダウンロードするタイミングとは独立してスケジュール設定することができます。

パッチのインストールをスケジュール設定するには、次の手順を実行します。

1. [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [スケジュール設定] ステップに進みます。

   デフォルトでは、[スケジュール設定] ステップにはインストールフェーズ用のスケジュール設定オプションのみが表示されます。[インストールオプション] ステップで [ステージ] を選択した場合、ダウンロードフェーズ用のスケジュール設定オプションも表示されます。
2. 次のいずれかのインストールフェーズオプションを選択します。
   - **ただちにタスクを実行**: [サマリープレビュー] ステップでプレビュー分析を行うことができます。ダウンロードフェーズ用のスケジュール設定オプションは、[**ダウンロード後ただちに実行**] です。
   - **次の時刻にタスクを実行**: 日付と時刻を指定して、後でダウンロードまたはインストールを実行することができます。

3 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

スケジュール設定したパッチのインストールは、パッチのダウンロードが完了している場合でも、実行前にキャンセルできます。

Windowsパッチのインストールでの電子メール通知の設定

ダウンロード操作やインストール操作が正常に終了した、あるいはエラーで終了したときに、ユーザーに知らせるために電子メール通知を設定できます。

電子メール通知を設定するには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [通知] ステップに進みます。

2 電子メールアドレスを追加するには、[**通知の追加**] をクリックして [通知電子メールアドレス] フィールドに電子メールアドレスを入力します。

3 ジョブが成功したときの通知ステータスを設定するには、  アイコンを選択します。ジョブが失敗したときの通知ステータスを設定するには、  アイコンを選択します。デフォルトでは、[通知] ステップにはインストールフェーズ用の通知ステータスのみが表示されます。

4 [チケットID] フィールドに、このジョブに割り当てるチケットIDを入力します。

5 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

[インストールオプション] ステップで [ステージ] を選択した場合、[通知] ペインにダウンロードとインストールの両方のフェーズに対する通知オプションが表示されます。

Windowsパッチのインストールのプレビュー

インストールのプレビューでは、サーバーのパッチの状態に関する最新のレポートが表示されます。インストールのプレビューは、管理対象サーバーにインストールされるパッチと必要なサーバー再起動のタイプを確認するためのオプションステップです。プレビュープロセスでは、WUAに基づいて、パッチのインストール対象として選択したサーバーに該当するパッチがすでにインストールされているかどうかを確認します。システム管理者がパッチを手動でインストールしている場合、サーバーにパッチがすでにインストールされている可能性があります。このような場合、Windowsパッチ管理ではパッチの存在を把握できません。

プレビューでは、特定のWindows製品を必要とするパッチ、および他のパッチよりも優先されるパッチや他のパッチの方が優先されるパッチなど、依存関係情報や優先情報に関するレポートも作成されます。依存関係が満たされていない場合は、パッチ管理にその状態を示すエラーメッセージが表示されます。

次のリストは、パッチがインストールされないケースについて説明したものです。これらは、[パッチのインストール] または [修復] ウィンドウの [プレビュー] ステップに表示されます。

- このパッチには「常にインストールしない」パッチポリシー例外があるため、インストールされません。
- このパッチは同じジョブ内の別のパッチより優先順位が低いため、インストールされません。これは、現在のジョブの中にマークされたパッチよりも最新のパッチが存在することを意味します。
- このパッチは別のパッチより優先順位が低いため、インストールされません。これは、サーバーにインストールされたパッチがポリシー内のパッチよりも新しいため、インストールされないことを意味します。
- このパッチは、WUAで推奨されていないため適用できず、インストールされません。

- このパッチは別のロケール用のため、インストールされません。

この情報はジョブの結果ウィンドウにも表示されます。また、パッチインストールジョブで電子メール通知が構成されている場合は、電子メール内にも表示されます。

インストールのプレビューでは、パッチが適用済みの状態をシミュレートするため、サーバーの動作に関するレポートは行われません。

パッチのインストールをプレビューするには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [サマリーレビュー] ステップに進みます。

2 (オプション) [**プレビュー**] をクリックし、パッチのインストール時に実行される個々のアクションを表示します。テーブルの行を選択すると、プレビューしているアクションの詳細が表示されます。

3 [**ジョブの開始**] をクリックしてインストールジョブを起動するか、[**キャンセル**] をクリックしてインストールを起動せずに [パッチのインストール] ウィンドウを閉じます。

[スケジュール設定] ステップで [**ただちにタスクを実行**] を選択すると、ジョブがすぐに開始します。[**次の時刻にタスクを実行**] を選択すると、指定した日時にジョブが開始します。

Windowsパッチのインストールジョブの進行状況の表示

アクションが完了したか失敗したかなど、パッチのインストールジョブの進行状況を確認することができます。

ジョブの進行状況を表示するには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [ジョブの進行状況] ステップに進みます。これにより、インストールジョブが開始されます。

進行状況バーとテキストで、テーブル内のアクションがどの程度完了したかを確認できます。次のアクションをサーバーごとに実行できます。

- **分析**: HP Server Automationは、インストールに必要なパッチの確認、管理対象サーバーにインストールされた最新パッチのチェック、他に実行が必要なアクションの確認を行います。
- **ダウンロード**: HP Server Automationから管理対象サーバーにパッチをダウンロードします。
- **インストール**: ダウンロードの完了後、パッチをインストールします。
- **最後に再起動**: [インストール前後のアクション] ステップでこのアクションを指定すると、サーバーが再起動します。
- **インストール前スクリプト / インストール後スクリプト / ダウンロード前スクリプト / ダウンロード後スクリプト**: [インストール前後のアクション] ステップでこのアクションを指定した場合、インストール前または後にスクリプトが実行されます。
- **インストールと再起動**: パッチをインストールしたときに、サーバーが再起動します。
- **確認**: インストールしたパッチは、ソフトウェア登録に追加されます。

2 特定のアクションに関する詳細を追加表示するには、テーブルの行を選択して、ジョブの開始時刻と完了時刻を表示します。ナビゲーションペインで、[ジョブとセッション] を選択してジョブに関する詳細を確認します。ジョブログの参照については、『SAユーザーガイド: Server Automation』を参照してください。

Windows管理対象サーバー上でベンダー推奨パッチポリシーを修復すると、適用するパッチによっては、サーバーで追加の修復が必要な場合があります。修復によって、ベンダーアップデートが必要なパッチがインストールされた場合に、この状況が発生します。

3 [パッチのインストール] ウィンドウを閉じる場合は [**閉じる**] をクリックし、ジョブを実行しないようにする場合は [**ジョブの終了**] をクリックします。

(オプション) インストール、アンインストール、修復のキャンセルまたは終了 (86ページ) を参照してください。

-

Windowsパッチのインストール順序の設定

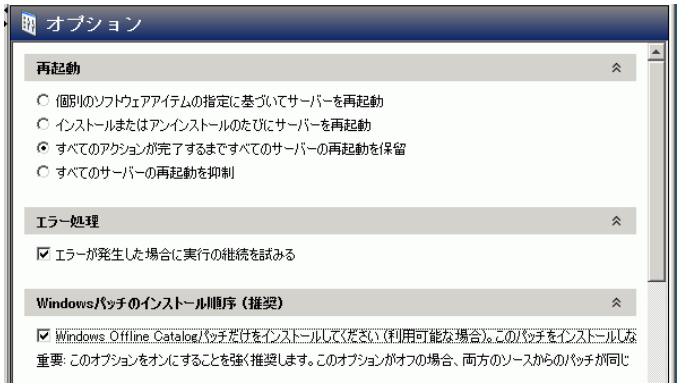
修復ジョブウィンドウの [**Windows パッチのインストール順序**] の設定を使用すると、Windows パッチポリシーの修復ジョブでパッチのインストール順序を制御できます。このオプションを選択すると、異なるソースから取得したWindowsパッチデータの競合を防ぐことができます。

ベストプラクティスのヒント: Windowsパッチポリシーの修復ジョブの場合は、この設定の使用を強く推奨します。

SAのWindowsパッチ適用では、Microsoft Offline Catalog (`wsusscn2.cab`) とHPLN Microsoft Patch Supplementの2種類のソースのパッチをインストールします。Microsoft Patch Supplementで定義されたホットフィックスは、Microsoft Offline Catalogの最新のパッチに取り込まれたり、改良が加えられたりすることがあります。この場合、Microsoft Patch Supplementのパッチは廃止になります。そのため、`wsusscn2.cab`のパッチの前にMicrosoft Patch Supplementのパッチをインストールすると、パッチデータが損なわれる可能性があります。

Windowsパッチのインストール順序を設定するには、次の手順を実行します。

1 Windowsパッチポリシーの修復ジョブの実行中に、[オプション] ビューで [**Windowsパッチのインストール順序**] の設定を選択します。



2 修復ジョブを実行すると、Microsoft Offline Catalogのすべてのパッチ (`wsusscn2.cab`) が最初にデプロイされ、HPLN Patch Supplementのパッチはジョブに Microsoft Offline Catalogのパッチが含まれなくなった時点で実行されます。

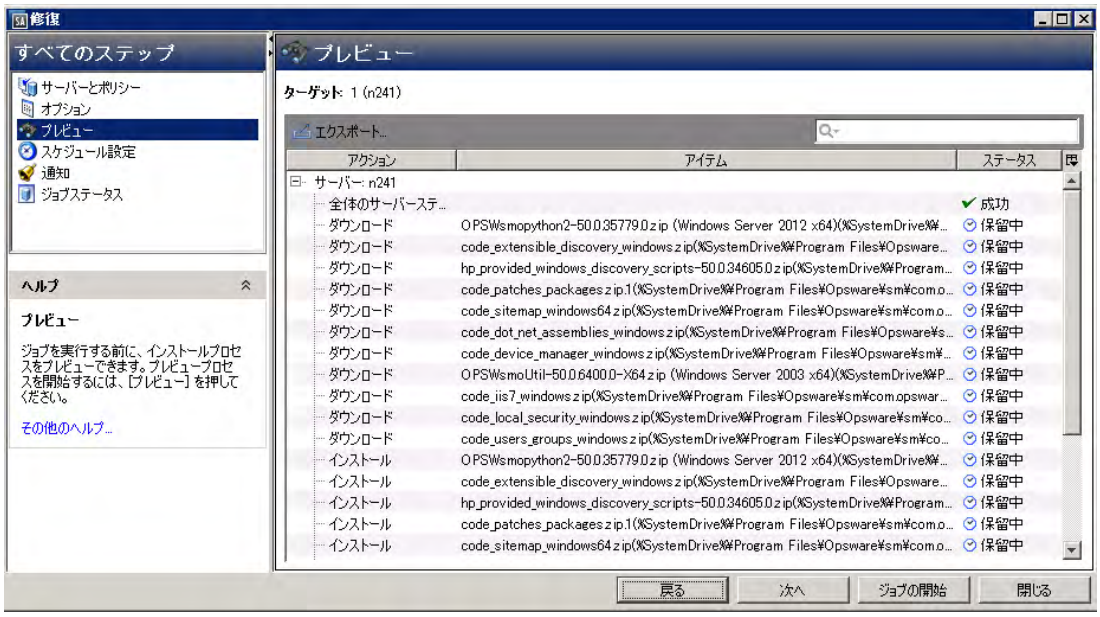
警告: このオプションを選択しない場合、デフォルトの順序はKB番号順になります。この場合、Windows Offline Catalog (`wsusscn2.cab`) とHPLN Microsoft Patch Supplementの両方からパッチをインストールすると、問題が発生する可能性があります。

3 すべてのパッチをデプロイして、完全なコンプライアンスを実現するには、修復ジョブを複数回実行する必要があります。

重要: このオプションを使用する場合、サーバーを完全なコンプライアンス状態にするには、修復ジョブを複数回実行する必要があります。

4 各パッチのインストールのステータスは、[修復] ウィンドウの [プレビュー] または [ジョブステータス] ビューに表示されます。

特定のアイテムに関する詳細を追加表示するには、テーブルの行を選択して、下部のペインに詳細を表示します。



ポリシーにwsusscn2.cabとHPLN Supplementの両方のパッチが含まれる場合、HPLNのパッチはインストールされません。次のメッセージが表示されます。

`This patch is not a Windows Offline Catalog patch.The Windows Patch Ordering option was enabled for this job, so only Windows Offline Catalog patches will be considered.`（このパッチは`Windows Offline Catalog`のパッチではありません。このジョブでは`Windows`パッチの順序オプションが有効になっているため、`Windows Offline Catalog`以外のパッチは考慮されません。）

-

パッチのアンインストール

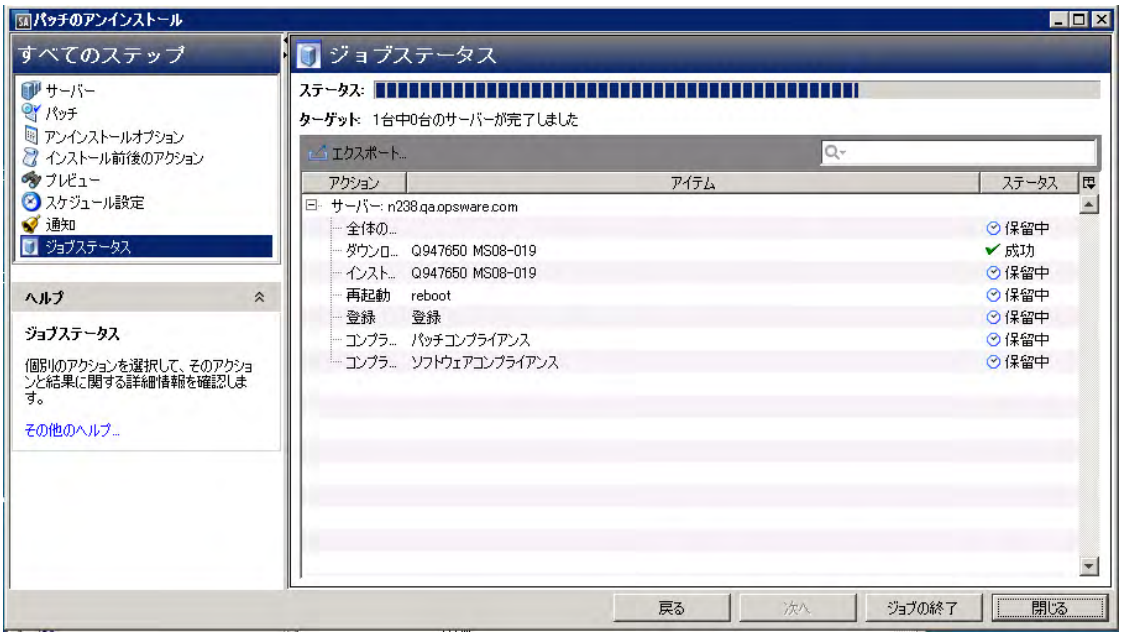
Windowsパッチ管理では、Microsoftパッチの管理対象サーバーからのアンインストール（削除）方法やアンインストール条件を細かく制御することができます。問題を最小限に抑えるため、パッチのアンインストールは1つずつ行う必要があります。最初にHP Server Automationを使ってインストールしたものではないパッチをHP Server Automationを使用してアンインストールすることはできません。

これらの条件を適切に管理できるように、パッチ管理では、次のことを行うことができます。

- サーバーの再起動オプション、およびインストール前スクリプト/インストール後スクリプトの管理。
- パッチのアンインストールのシミュレート（プレビュー）。
- アンインストールプロセスのステータスを把握するための電子メール通知の設定。

これらの条件は、[パッチのアンインストール] ウィザードを使用して設定することができます。詳細については、図9を参照してください。

図9　　[パッチのアンインストール] ウィザード



アンインストールフラグ

Windowsパッチをアンインストールする際には、アンインストールフラグを指定できます。ただし、SAでは、デフォルトのアンインストールフラグが使用され、これらのフラグを使用してパッチをアンインストールする必要があります。そのため、HP Server Automationから渡されるデフォルトのアンインストールフラグを無効にするフラグや矛盾するフラグを指定しないようにする必要があります。

Windowsホットフィックスの中には、`-z`フラグをサポートしないもの、`-q`フラグをサポートしないもの、いずれか一方をサポートしないものがあります。このような場合はそれぞれ、`/-z`、`/-q`、`/-z -q`という特殊な表記を使用して、HP Server Automation で `-z`、`-q`、`-z -q`フラグでの受け渡しを防ぐ必要があります。HP Server Automation では、デフォルトで、パッチのアンインストール時に`/z /q`がコマンドライン引数に追加されます。これを無効にするには、`/-z /-q`を指定します。たとえば、再起動を抑制しない場合は、`/-z`を指定します。

表5に、SAで使用されるデフォルトのアンインストールフラグを示します。

表5　　デフォルトのアンインストールフラグ

Windowsパッチタイプ	フラグ
Windowsホットフィックス	`-q -z`
セキュリティロールアップパッケージ	`-q -z`
Windows OSサービスパック	アンインストール不可

Windowsパッチのアンインストール

サービスパックをアンインストールできるのは、サービスパックが最初にSAによってインストールされ、サービスパックをコントロールパネルでサーバーから直接アンインストールできる場合です。コントロールパネルでサービスパックをアンインストールできない場合は、SAでサービスパックをアンインストールすることもできません。

管理対象サーバーからパッチを削除するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。
2. [パッチ] を展開して、特定のWindowsオペレーティングシステムを選択します。
3. 内容ペインで、パッチを選択します。
4. [表示] ドロップダウンリストから、[サーバー] を選択します。
5. [表示] ドロップダウンリストで、[パッチがインストールされたサーバー] を選択します。
6. プレビューペインで、1つまたは複数のサーバーを選択します。
7. [**アクション**] メニューで [**パッチのアンインストール**] を選択します。[パッチのアンインストール] ウィンドウの最初のステップ (サーバー) が表示されます。
   各ステップの手順については、次の項を参照してください。
   - アンインストールオプションの設定
   - Windowsパッチのアンインストールでの再起動オプションの設定
   - Windowsパッチのアンインストールでのインストールスクリプトの指定
   - Windowsパッチのアンインストールのスケジュール設定
   - Windowsパッチのアンインストールでの電子メール通知の設定
   - パッチのアンインストールジョブの進行状況の表示

   1つのステップが完了したら、[**次へ**] をクリックして次のステップへ進みます。[**ジョブの開始**] をクリックする前に、ステップリストに表示される完了したステップをクリックすることで、そのステップに戻って変更を行うことができます。
8. アンインストールジョブを起動する準備ができたら、[**ジョブの開始**] をクリックします。

   ジョブを後で実行するようにスケジュール設定している場合でも、ジョブの開始後にパラメーターを変更することはできません。

   ジョブが完了するまで [パッチのアンインストール] ウィンドウが開いている場合、パッチ管理により [すべての管理対象サーバー] ウィンドウの [パッチコンプライアンス] 列の関連するサーバーのコンプライアンスカウント (括弧内) が更新されます。[**F5**] キーを押すか、[表示] メニューの [更新] を選択して、[パッチのプレビュー] ペインの情報を更新します。

アンインストールオプションの設定

次のタイプのパッチのアンインストールオプションを指定することができます。

- いずれか1つのパッチでエラーが発生した場合でも、パッチのアンインストールプロセスを中断しない。
- さまざまなコマンドラインオプションを使用してアンインストールを行う。

これらのオプションを設定するには、次の手順を実行します。

1. [パッチのアンインストール] ウィンドウで、[**次へ**] をクリックして [アンインストールオプション] ステップに進みます。

2 いずれかのパッチでエラーが発生した場合でもパッチのインストールプロセスを続行する場合は、[エラーオプション] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

3 [アンインストールコマンド] テキストボックスに、表示されるコマンド (.exeファイル) のコマンドライン引数を入力します。デフォルトでは、HP Server Automationでは/z /qが追加されます。これらのアンインストールフラグを無効にする場合は、テキストボックスに/-z /-qと入力します。

4 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのアンインストール] ウィンドウを閉じます。

Windowsパッチのアンインストールでの再起動オプションの設定

サーバーの再起動によるダウンタイムを最小限に抑えるため、サーバーを再起動するタイミングを制御できます。ベンダーの再起動割り当てを調整、パッチを削除するたびにサーバーを再起動、すべてのサーバーの再起動を完全に抑制、またはすべてのパッチがアンインストールされるまで再起動を延期することができます。

[パッチのアンインストール] ウィンドウで再起動オプションを選択する場合、HPではMicrosoftの再起動推奨設定を使用することを推奨しています。これに該当するのは、[**個別のソフトウェアアイテムの指定に基づいてサーバーを再起動**] オプションです。Microsoftの再起動設定を使用できない場合は、単一再起動オプション ([**すべてのパッケージがインストールまたはアンインストールされるまですべてのサーバーの再起動を保留する**] オプション) を選択します。このようにしないと、次の再起動が (SAの制御対象外)実行されるまで、WUAでサーバーにインストールされているパッチが正しく通知されない可能性があります。

パッチのインストールの完了後にサーバーを再起動するかどうかを指定するオプションです。このオプションは、[パッチのアンインストール] ウィンドウから起動したジョブのみに適用されます。このオプションを設定しても、パッチのプロパティウィンドウの [アンインストールパラメーター] タブにある [再起動が必要] オプションが変更されることはありません。

サーバーの状態が再起動保留中である場合、その後のパッチのアンインストールは失敗する可能性があります。サーバーでパッチのアンインストールを行う前に、サーバーを再起動する必要があります。詳細については、再起動が必要なサーバーの検索 (72ページ) を参照してください。

次に示すオプションの設定は、最初のオプションを除いて、[再起動が必要] オプションの設定よりも優先します。

- **個別のソフトウェアアイテムの指定に基づいてサーバーを再起動** (デフォルト): デフォルトでは、パッチプロパティの [再起動が必要] オプションの設定に従って再起動が行われます。
- **各パッチのインストール後にサーバーを再起動**: パッチプロパティの [再起動が必要] オプションが設定されていない場合でも、サーバーを再起動します。複数のパッチをインストールする場合、サーバーの再起動も複数回行われます。
- **すべてのサーバーの再起動を抑制**: パッチプロパティの [再起動が必要] オプションが設定されている場合でも、サーバーを再起動しません。ベンダー設定によっては、抑制オプションを無視して強制的に再起動を行う場合があります。サービスパックの場合、再起動を抑制すると、アクションが未完了になります (再起動するまでサービスパックは未アンインストールになります)。ソフトウェアはシステムからアンインストール済みの状態になりません。ステータスは「未インストール/アンインストール」になります。システムを手動でチェック (レジストリまたはサーバーのプロパティを確認) する場合、SAクライアントに表示される内容と同じにはなりません。再起動後、次にソフトウェア登録を行うまで、SAクライアントに正しいソフトウェアやパッチの削除情報は反映されません。

  注: Windowsパッチのアンインストール時に再起動を抑制すると (サービスパックの場合など)、システムのソフトウェア状態が正しく表示されない可能性があります。正確な状態は、管理対象サーバーが再起動され、ソフトウェア登録が完了した後に表示されます。
- **すべてのパッケージがインストールまたはアンインストールされるまですべてのサーバーの再起動を保留する**: 選択したパッチの中に [再起動が必要] オプションが設定されているものが含まれていても、他のパッチにそのオプションが設定されていない場合、すべてのパッチのインストール後にサーバーが1回再起動されます。一般的に、これは単一再起動オプションと呼ばれます。選択したパッチの中に [再起動が必要] オプションが設定されているものがない場合、サーバーは再起動されません。

再起動オプションを設定するには、次の手順を実行します。

1. [パッチのアンインストール] ウィンドウで、[**次へ**] をクリックして [インストール前後のアクション] ステップに進みます。
2. いずれかの再起動オプションを選択します。
3. [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのアンインストール] ウィンドウを閉じます。

Windowsパッチのアンインストールでのインストールスクリプトの指定

パッチごとにアンインストールの前または後に実行するコマンドまたはスクリプトを指定できます。アンインストール前スクリプトでは、たとえば、管理対象サーバー上で特定の条件をチェックすることができます。条件が満たされない場合やアンインストール前スクリプトが失敗した場合、パッチはサーバーから削除されません。アンインストール前スクリプトを使用すると、サーバーからパッチを削除する前にサービスやアプリケーションをシャットダウンすることもできます。アンインストール後スクリプトを使用すると、管理対象サーバー上でクリーンアッププロセスを実行することができます。

パッチのアンインストールの前または後に、管理対象サーバー上で次のタイプのスクリプトを実行するように指定することもできます。

- **アンインストール前**: 管理対象サーバーからパッチを削除する前に実行するスクリプト。
- **アンインストール後**: 管理対象サーバーからパッチを削除した後で実行するスクリプト。

スクリプトを指定するには、次の手順を実行します。

1. [パッチのアンインストール] ウィンドウで、[**次へ**] をクリックして [インストール前後のアクション] ステップに進みます。
2. [アンインストール前] または [アンインストール後] タブを選択します。

   各タブでさまざまなスクリプトとオプションを指定できます。
3. [スクリプトの有効化] を選択します。

   このオプションを選択すると、タブのフィールドの残りの部分が有効になります。[スクリプトの有効化] を選択しない場合、スクリプトは実行されません。
4. [保存されたスクリプト] または [アドホックスクリプト] を選択します。

   保存されたスクリプトは、前にSA Webクライアントを使用してServer Automationに保存されたものです。スクリプトを指定するには、[**選択**] をクリックします。

   アドホックスクリプトはこの操作に対してのみ実行され、Server Automation に保存されません。タイプ (.batなど) を選択します。[スクリプト] ボックスに、スクリプトが存在する場所のドライブ文字を含むスクリプトの内容を入力します (`echo dir>> C:\temp\preinstall1.log`など)。ドライブ文字を入力しない場合、デフォルトは%SYSTEMDRIVE%になります。これは、Windowsのシステムフォルダーがインストールされている場所です。
5. スクリプトでコマンドラインフラグが必要である場合、[コマンド] にフラグを入力します。
6. [ユーザー] セクションで情報を選択します。このユーザーによってスクリプトが管理対象サーバー上で実行されます。
7. スクリプトがエラーを返した場合にアンインストールを停止するには、[エラー] を選択します。

Windowsパッチのアンインストールのスケジュール設定

パッチはサーバーからただちに削除するか、日時を指定して後で削除することができます。

パッチのアンインストールをスケジュール設定するには、次の手順を実行します。

1. [パッチのアンインストール] ウィンドウで、[**次へ**] をクリックして [スケジュール設定] ステップに進みます。

2 次のいずれかのインストールフェーズオプションを選択します。

- **ただちにタスクを実行**: [サマリープレビュー] ステップでアンインストールを行うことができます。
- **次の時刻にタスクを実行**: アンインストールを行う日付と時刻を指定することができます。

3 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのアンインストール] ウィンドウを閉じます。

Windowsパッチのアンインストールでの電子メール通知の設定

パッチのアンインストール操作が正常に終了した、あるいはエラーで終了したときに、ユーザーに知らせるために電子メール通知を設定できます。

電子メール通知を設定するには、次の手順を実行します。

1 [パッチのアンインストール] ウィンドウで、[**次へ**] をクリックして [通知] ステップに進みます。

2 電子メールアドレスを追加するには、[**通知の追加**] をクリックして [通知電子メールアドレス] フィールドに電子メールアドレスを入力します。

3 ジョブが成功したときの通知ステータスを設定するには、  アイコンを選択します。ジョブが失敗したときの通知ステータスを設定するには、  アイコンを選択します。デフォルトでは、[通知] ステップにはアンインストールフェーズ用の通知ステータスのみが表示されます。

4 [チケットID] フィールドに、このジョブに割り当てるチケットIDを入力します。

5 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのアンインストール] ウィンドウを閉じます。

Windowsパッチのアンインストールのプレビューおよび開始

アンインストールのプレビューでは、サーバーのパッチの状態に関する最新のレポートが表示されます。アンインストールのプレビューは、管理対象サーバーから削除されるパッチを確認するためのオプションステップです。プレビュープロセスでは、(`wsusscn2.cab`に基づいて) パッチのアンインストール対象として選択したサーバーに該当するパッチがすでにインストールされているかどうかを確認します。

アンインストールのプレビューでは、サーバーからパッチを削除した場合のシステムの動作に関するレポートやシミュレートは行われません。

パッチのアンインストールをプレビューするには、次の手順を実行します。

1 [パッチのアンインストール] ウィンドウで、[**次へ**] をクリックして [サマリーレビュー] ステップに進みます。

2 サーバー、デバイスグループ、およびパッチについてウィンドウの上部に表示されている情報を確認します。

3 (オプション) [**プレビュー**] をクリックし、パッチのアンインストール時に実行される個々のアクションを表示します。テーブルの行を選択すると、プレビューしているアクションの詳細が表示されます。

4 [**ジョブの開始**] をクリックしてジョブを起動するか、[**キャンセル**] をクリックしてアンインストールを起動せずに [パッチのアンインストール] ウィンドウを閉じます。

[スケジュール設定] ステップで [**ただちにタスクを実行**] を選択すると、ジョブがすぐに開始します。[**次の時刻にタスクを実行**] を選択すると、指定した日時にジョブが開始します。

パッチのアンインストールジョブの進行状況の表示

アクションが完了したか失敗したかなど、パッチのアンインストールジョブの進行状況を確認することができます。

ジョブの進行状況を表示するには、次の手順を実行します。

1 [パッチのアンインストール] ウィンドウで、[**次へ**] をクリックして [ジョブの進行状況] ステップに進みます。進行状況バーとテキストで、テーブル内のアクションがどの程度完了したかを確認できます。次のアクションをサーバーごとに実行できます。

- **分析**: HP Server Automation は、アンインストールに必要なパッチの確認、管理対象サーバーにインストールされた最新パッチのチェック、他に実行が必要なアクションの確認を行います。
- **アンインストール**: パッチをアンインストールします。
- **最後に再起動**: [インストール前後のアクション] ステップでこのアクションを指定すると、サーバーが再起動します。
- **アンインストール前スクリプト/アンインストール後スクリプト**: [インストール前後のアクション] ステップでこのアクションを指定した場合、アンインストール前または後にスクリプトが実行されます。
- **アンインストールと再起動**: パッチをインストールしたときに、サーバーが再起動します。
- **確認**: インストールしたパッチは、ソフトウェア登録に追加されます。

2 特定のアクションに関する詳細を追加表示するには、テーブルの行を選択して、ジョブの開始時刻と完了時刻を表示します。ナビゲーションペインで、[ジョブとセッション] を選択してジョブに関する詳細を確認します。ジョブログの参照については、『SAユーザーガイド: Server Automation』を参照してください。

3 [**ジョブの終了**] をクリックしてジョブを実行しないようにするか、[**閉じる**] をクリックして [パッチのアンインストール] ウィンドウを閉じます。

(オプション) インストール、アンインストール、修復のキャンセルまたは終了 (86ページ) を参照してください。

上位のバイナリで同じコンポーネントがすでにアンインストールされているため下位のバイナリをアンインストールできない場合があります。また、レジストリを編集するスクリプトのように、元々インストール用のコンポーネントでないためにアンインストールできない場合もあります。このような場合には、「ファイルが見つかりません」というエラーが表示される可能性があります。アンインストールを確認するには、コンプライアンススキャンを実行します。

第3章 HP-UXパッチ管理

概要

Server Automation (SA) で、HP-UXオペレーティングシステム用のパッチはデポとしてHPから独占的に提供されます。デポには複数のパッチプロダクトが含まれ、各パッチプロダクトには複数のパッチファイルセットが含まれます。これらのデポはServer Automationにアップロードできます。

HP-UXパッチ管理では、次の操作を実行できます。

- HP-UXパッチまたはパッチバンドルからのHP-UXソフトウェアポリシーの作成。
- サーバーに対するHP-UXパッチの確認、インストール、削除。
- ソフトウェアポリシーの修復によるソフトウェアおよびパッチのインストール。
- 各パッチに関連付けられたメタデータ情報のダウンロード。
- 複数プラットフォームのパッチ、パッチの依存関係、自動再起動のサポート。
- パッチコンプライアンススキャンの実行。

機能

SAでは、次の機能によってHP-UXパッチ管理を自動化します。

- モデルベースのアプローチで HP-UX サーバーを管理する HP-UX ソフトウェアポリシーを定義します。Server Automationでは、HP-UXソフトウェアポリシーを使用して、IT環境のモデルを作成できます。これらのソフトウェアポリシーでは、管理対象サーバーにインストール可能なパッチとスクリプトを指定します。
- HP-UXパッチを管理対象サーバーにインストールします。
- パッチインストールプロセスを確立します。
- パッチ管理の各ステージ (分析、ダウロード、インストール) のスケジュールを設定します。また、各ステージごとに電子メール通知を設定し、ジョブにチケットIDを関連付けることもできます。
- ソフトウェアポリシーに基づいて、サーバーのコンプライアンスステータスを検証します。
- コンプライアンスビューで、サーバーがソフトウェアポリシーに基づいて構成されているかを確認し、非コンプライアンスサーバーがあれば修復します。
- ソフトウェアリソースとサーバーを検索します。
- ライブラリでは、強力かつ柔軟な検索条件 (可用性、アーキテクチャー、オペレーティングシステム、再起動オプション、バージョンなど) を使用して、HP-UXパッケージ、パッチ、ソフトウェアポリシーを検索します。HP-UX ソフトウェアポリシーは、名前、フォルダー名、可用性、オペレーティングシステムで検索することも可能です。
- パッチインストールのプレビューでは、パッチの依存関係とパッチの適用性分析が表示されます。

前提条件

HP-UXのパッチ管理を使用するには、次のタスクを実行しておく必要があります。

- HP-UX Software Catalogファイルをダウンロードします。

  HP-UX Software Catalogファイルをダウンロードするには、サービスレベル契約が必要です。このファイルのダウンロードには、import_hpux_metadataスクリプトを使用します。詳細については、このスクリプトの -h オプションを確認してください。詳細については、/opt/opsware/mm_wordbot/util/import_hpux_depots (94ページ) を参照してください。
- SAに対して新規パッチをアップロードし、既存のHP-UXパッチ、デポ、バンドルを再アップロードします。
- 既存のすべての管理対象サーバーで　HP-UX　エージェントを更新します。エージェントバージョンはopsware-agent-37.0.0.2.130以上である必要があります。

サポート対象オペレーティングシステム

パッチ管理でサポートされているHP-UXオペレーティングシステムの詳細については、『SA Support and Compatibility Matrix』を参照してください。

HP-UXデポ

import_hpux_depotスクリプトは、HP-UXパッチ、バンドル、デポをSAライブラリにインポートします。ソースデポごとに、デポのプロダクトを含む<depot name>デポポリシーがSAライブラリに作成されます。

import_hpux_depotスクリプトでは、スクリプトの入力に拡張子.depotが必要です。

- デフォルトで、http://itrc.hp.com からダウンロードした標準HP-UXバンドルには、すでに.depotの拡張子が付いています。
- デフォルトで、http://itrc.hp.com からダウンロードしたHP-UXパッチには、.depotの拡張子は含まれていません。これらのパッチはHP-UXサーバーに手動でダウンロードして、個別の.depotファイルを作成し、import_hpux_depotスクリプトを使用してSAライブラリにアップロードする必要があります。

import_hpux_depotスクリプトは次のディレクトリにあります。

/opt/opsware/mm_wordbot/util/import_hpux_depots

スクリプトの代わりにSA クライアントを使用してパッチやデポをインポートした場合、ソフトウェアポリシーが作成されず、パッチの依存関係は機能しません。

SAライブラリにアップロードした後で、HP-UXパッチを削除することはできません。「HP-UXパッチプロダクト」や「HP-UXパッチファイルセット」を選択したときに、削除オプションが無効になります。

表6に、このスクリプトで使用できるオプションを示します。

表6　　import_hpux_depotのオプション

オプション	説明
import_hpux_depots [options]	現在の作業ディレクトリ内のすべての*.depotファイルをライブラリにインポートします。
import_hpux_depots [options] <source-directory>	指定したディレクトリ内のすべての*.depotファイルをライブラリにインポートします。
import_hpux_depots [options] <*.depot	指定したデポをライブラリにインポートします。
import_hpux_depots -h	追加オプションを表示します。
-b, --bundle-policies create a policy for each depot bundle	ソースデポ内のバンドルごとに、--bundle-policiesオプションを使用して、バンドルのプロダクトを含む<bundle name>バンドルポリシーがSAライブラリ内に作成されます。
-f、--force	すでにSAライブラリ内に存在する場合でも、デポのプロダクトを強制的にインポートします。
-h、--help	ヘルプメッセージを表示します。
-n、--silent	エラーのみを表示します。
-o OS、--os=OS	デポのプロダクトのHP-UXリリース10.20、11.00、11.11、11.23、11.31。 一部のパッチは11.23および11.31のオペレーティングシステムバージョンで共通です。これらのパッチをSAライブラリにアップロードする場合は、-o=11.23または-o=11.31を使用します。
-p POLICY_FOLDER、--policy_folder=POLICY_FOLDER	ポリシーを作成するライブラリフォルダーへのパス。
-s SPLIT, --split=SPLIT 各デポの分割方法 (デフォルト: product): 'product'、'instance'、'none'	--forceを指定しない限り、SAライブラリ内にすでに存在するプロダクトは再インポートされません。 デフォルトで、複数のプロダクトを含むデポはプロダクトごとに分割されるため、各プロダクトは自己完結型のデポとしてSAライブラリ内に保管されます。分割動作は、次のように--splitオプションで制御します。 • none— ソースデポは分割されずに、そのままの状態でインポートされます。 • product— ソースデポはプロダクト別に分割されます。デポに同じプロダクト(プロダクト名)の複数のインスタンスが含まれる場合、インスタンスはまとめて保持されます。これはデフォルト設定です。 • instance— ソースデポはプロダクトのインスタンス別に分割されます。デポに同じプロダクト(プロダクト名)の複数のインスタンスが含まれる場合、各インスタンスは個別のデポに分割されます。
--timeout=USER_TIMEOUT	デフォルトのタイムアウト値をオーバーライドします(--splitがnoneの場合は2時間、それ以外の場合は5分)。

表6　　import_hpux_depotのオプション（続き）

オプション	説明
-u USERNAME、 --username=USERNAME	指定されたユーザーとしてパッケージをアップロードします (デフォルト: opsware)。
-v、--verbose	詳細な出力を表示します。
--manual	マニュアルページを表示して終了します。
--version	バージョンを表示して終了します。

HP-UX Software Catalogファイル

HP-UX Software Catalog ファイルは、XML 形式の HP-UX パッチデータベースです。このカタログファイルは swa_catalog.xmlで、ftp://ftp.itrc.hp.com/export/patches からダウンロードできます。

HP-UX メタデータスクリプトは、HP-UX Software Catalog ファイルを SA ライブラリにインポートするのに使用します。このスクリプトは、Software Catalogファイル内に存在する任意のパッチが依存するパッチを列挙し、パッケージリポジトリ内の欠落している依存パッチを示します。

HP-UXメタデータスクリプトは次のディレクトリにあります。

/opt/opsware/mm_wordbot/util/import_hpux_metadata

表7に、このスクリプトで使用できるオプションを示します。

表7　　HP-UXメタデータスクリプトのオプション

オプション	説明
-a HPUX_ANALYZE_PATCHES、 --analyze_patches=HPUX_ANALYZE_ PATCHES	パッケージリポジトリで欠落している依存パッチの分析対象となるHP-UXパッチを指定します。カンマ (,) で区切って複数のHP-UXパッチを指定できます。パッケージリポジトリのすべてのHP-UXパッチを分析する場合は、キーワードallを追加します。
-c HPUX_SW_CATALOG_FILE、 --catalog_file=HPUX_SW_CATALOG_ FILE	HP-UX Software Catalog ファイルのソースの場所を指定します。このカタログファイルswa_catalog.xmlは、ftp://ftp.itrc.hp.com/export/patches からダウンロードできます。ユーザー ID とパスワードを指定した場合、このオプションは適用されません。
-d DISPLAY_DEPENDENCIES、 --display_dependencies=DISPLAY_ DEPENDENCIES	依存関係を表示する HP-UX パッチを指定します。ソフトウェアカタログのすべてのパッチの依存関係を表示する場合は、キーワードallを追加します。
-f、--force	カタログのアップロードを強制的に実行します。-uオプションと-pオプションまたは-cオプションを使用してカタログのアップロードを指定する場合に、このオプションを使用すると、チェックサムが現在のカタログと一致する場合でも新規カタログをアップロードできます。
-h、--help	ヘルプメッセージを表示します。

表7　HP-UXメタデータスクリプトのオプション（続き）

オプション	説明
-n、--no_supersedence	フラグは、存在しないパッチの通知に優先依存関係ツリーまたは基本依存関係ツリーのどちらを使用するかを示す-aオプションとともに使用します。優先依存関係ツリーは、HP-UXのパッチ適用のデフォルト設定です。優先依存関係ツリーでは、最新の依存関係のチェックが行われます。基本依存関係ツリーでは、最も古い依存関係のチェックが行われます。
-p PASSWORD、--password=PASSWORD	itrc.hp.comのWebサイトにアクセスしてswa_catalog.xmlファイルを自動的にダウンロードするのに必要なパスワード。ユーザーIDとパスワードの両方を指定する必要があります。
-t TEST_OPTION、 --test=TEST_OPTION	テストモードのオプション。指定できるのは、'bundle'、'product'、'all'です。
-u USERID、--user=USERID	itrc.hp.comのWebサイトにアクセスしてswa_catalog.xmlファイルを自動的にダウンロードするのに必要なユーザーID。ユーザーIDとパスワードの両方を指定する必要があります。
-w UPLOAD_WAIT、 --wait=UPLOAD_WAIT	カタログのアップロードを指定する際の、ファイルのアップロードとその後の更新との間の待機時間（秒数）を指定します。「オプティミスティック同時実行制御」が失敗する場合は、この値を大きくすることができます。

ソフトウェアポリシー管理

Server Automationでは、ソフトウェアポリシーを使用してHP-UXソフトウェアやパッチをサーバーやサーバーグループにインストールすることができます。ソフトウェアポリシーを作成して、サーバーまたはサーバーグループへアタッチします。サーバーまたはサーバーグループの修復を行うと、アタッチされたソフトウェアポリシーで指定されたパッチが自動的にインストールされます。修復プロセスでは、サーバー上に実際にインストールされている内容をサーバー上にインストールする必要のあるパッチを指定したソフトウェアポリシーと比較します。その後、SAで、ソフトウェアポリシーに準拠するようにサーバーを変更するのに必要な操作が特定されます。次の各項では、HP-UXソフトウェアポリシーを管理する方法について説明します。

HP-UXソフトウェアポリシーの作成

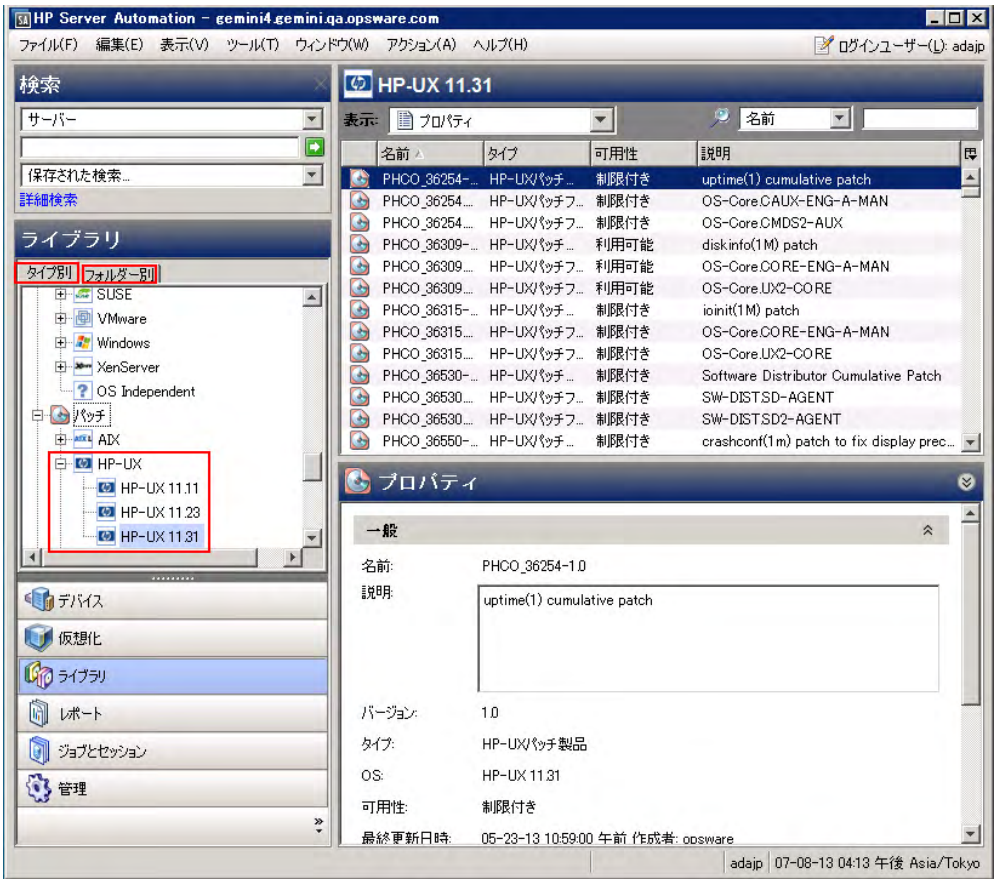
SAクライアントでは、次のいずれかのライブラリ機能を使用してソフトウェアポリシーを作成します。

- ライブラリ—タイプ別
- ライブラリ—フォルダー別

HP-UXソフトウェアポリシーの作成と管理を行うためのアクセス権が必要です。必要なアクセス権の取得については、システム管理者にお問い合わせください。ソフトウェア管理のアクセス権の詳細については、『SA管理ガイド』を参照してください。

内容ペインの薄く表示されたパッチアイコンは、パッチがライブラリにアップロードされていないことを示します。表示するパッチメタデータ情報の列を制御するには、列セレクターを使用します。詳細については、図10を参照してください。

図10　SAクライアントライブラリのHP-UXパッチ



ライブラリータイプ別

タイプ別機能を使用してソフトウェアポリシーを作成するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**ソフトウェアポリシー**] > [**HP-UX**] を選択します。内容ペインにソフトウェアポリシーのリストが表示されます。デフォルトで、ソフトウェアポリシーはオペレーティングシステムファミリ別に構成されます。
2. ダブルクリックしてオペレーティングシステムを選択します。
3. [アクション] メニューで、[**新規**] を選択して [新規ソフトウェアポリシー] ウィンドウを開きます。
4. [名前] フィールドに、HP-UXソフトウェアポリシーの名前を入力します。
5. (オプション) [説明] フィールドに、ポリシーの用途や内容の説明を入力します。
6. [場所] フィールドの横の [**選択**] をクリックして、フォルダー階層内でのソフトウェアポリシーの場所を指定します。
7. [フォルダーの選択] ウィンドウで、ライブラリ内のフォルダーを選択してソフトウェアポリシーの場所を指定した後に、[**選択**] をクリックして設定内容を保存します。
8. [可用性] ドロップダウンリストから、ソフトウェアポリシーに対するSAサーバーのライフサイクルの値 (利用可能または非推奨) を選択します。

9 [OS] ドロップダウンリストから、オペレーティングシステムファミリまたはファミリ内の特定のオペレーティングシステムを選択します。

10 [テンプレート] の値をデフォルトの「いいえ」のままにします。

11 [ファイル] メニューから [保存] を選択します。

ライブラリーフォルダー別

フォルダー別機能を使用してソフトウェアポリシーを作成するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**フォルダー別**] を選択します。内容ペインにライブラリ内のフォルダー階層が表示されます。

2 内容ペインで、ソフトウェアポリシーを格納するフォルダーを選択します。

3 [アクション] メニューで、[**新規**] > [**ソフトウェアポリシー**] を選択して [新規ソフトウェアポリシー] ウィンドウを開きます。

4 [名前] フィールドに、HP-UXソフトウェアポリシーの名前を入力します。

5 (オプション) [説明] フィールドに、ポリシーの用途や内容の説明を入力します。

6 [場所] フィールドの横の [**選択**] をクリックして、フォルダー階層内でのソフトウェアポリシーの場所を変更します。

7 [フォルダーの選択] ウィンドウで、ライブラリ内のフォルダーを選択してソフトウェアポリシーの場所を指定した後に、[**選択**] をクリックして設定内容を保存します。

8 [可用性] ドロップダウンリストで、ソフトウェアポリシーに対するSAサーバーのライフサイクルの値 (利用可能または非推奨) を選択します。

9 [OS] ドロップダウンリストで、オペレーティングシステムファミリまたはファミリ内の特定のオペレーティングシステムを選択します。

10 [テンプレート] の値をデフォルトの「いいえ」のままにします。

11 [ファイル] メニューから [保存] を選択します。

HP-UXソフトウェアポリシーの表示

SAクライアントでは、次のナビゲーション機能を使用してソフトウェアポリシーを表示します。

- 検索
- デバイス
- ライブラリ—タイプ別
- ライブラリ—フォルダー別

検索

検索機能を使用してソフトウェアポリシーを表示するには、次の手順を実行します。

1 ナビゲーションペインで [検索] を選択します。

2 ドロップダウンリストで [ソフトウェアポリシー] を選択し、テキストフィールドにポリシー名を入力します。

3  をクリックして、内容ペインに検索結果を表示します。

検索機能の詳細については、SAクライアントでのオブジェクトの検索 (33ページ) を参照してください。

4 内容ペインでソフトウェアポリシーを選択し、右クリックで[ソフトウェアポリシー]ウィンドウを開きます。

デバイス

デバイス機能を使用してソフトウェアポリシーを表示するには、次の手順を実行します。

1 ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択して、内容ペインにサーバーのリストを表示します。

または

ナビゲーションペインで、[**デバイス**] > [**デバイスグループ**] を選択して、内容ペインにサーバーのリストを表示します。

2 内容ペインで、サーバーを選択します。

3 選択したサーバーを右クリックして、[サーバー]ウィンドウを開きます。

4 [情報]ペインで[**管理ポリシー**]を選択します。

5 [管理ポリシー]ペインで、ソフトウェアポリシーを選択して、内容ペインにサーバーにアタッチされているソフトウェアポリシーを表示します。

6 内容ペインでソフトウェアポリシーを選択し、右クリックで[ソフトウェアポリシー]ウィンドウを開きます。

ライブラリータイプ別

タイプ別機能を使用してソフトウェアポリシーを作成するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**ソフトウェアポリシー**] > [**HP-UX**] とオペレーティングシステムバージョンを選択します。内容ペインにソフトウェアポリシーのリストが表示されます。デフォルトで、ソフトウェアポリシーはオペレーティングシステムファミリ別に構成されます。

2 内容ペインでソフトウェアポリシーを選択し、右クリックで[ソフトウェアポリシー]ウィンドウを開きます。

ライブラリーフォルダー別

フォルダー別機能を使用してソフトウェアポリシーを表示するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**フォルダー別**] を選択します。内容ペインにライブラリ内のフォルダー階層が表示されます。

2 内容ペインで、ソフトウェアポリシーを格納するフォルダーを選択します。

3 右クリックしてそのフォルダーを開きます。

4 ソフトウェアポリシーを選択し、右クリックで[ソフトウェアポリシー]ウィンドウを開きます。

HP-UXソフトウェアポリシーの編集

HP-UXソフトウェアポリシーの作成後に、HP-UXソフトウェアポリシーのプロパティを表示して変更することができます。表示可能なプロパティには、ソフトウェアポリシーを作成したSAユーザー、作成日、ソフトウェアポリシーのSA IDなどがあります。ソフトウェアポリシーの名前、説明、可用性、ライブラリ内の格納場所、ソフトウェアポリシーのオペレーティングシステムは変更(編集)することもできます。

HP-UXソフトウェアポリシーを管理するためのアクセス権が必要です。必要なアクセス権の取得については、システム管理者にお問い合わせください。ソフトウェア管理のアクセス権の詳細については、『SA 管理ガイド』を参照してください。

ソフトウェアポリシーのプロパティを編集するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**ソフトウェアポリシー**] > [**HP-UX**] とオペレーティングシステムバージョンを選択します。
2. 内容ペインでソフトウェアポリシーを選択し、右クリックで [ソフトウェアポリシー] ウィンドウを開きます。
3. [ソフトウェアポリシー] ウィンドウの [ビュー] ペインで、[プロパティ] を選択します。
4. [プロパティ] の内容ペインで、ソフトウェアポリシーの名前、説明、場所、可用性、OSを編集することができます。これらのフィールドの内容に関するガイドラインについては、HP-UXソフトウェアポリシーの作成 (97ページ) を参照してください。
5. 変更が完了したら、[ファイル] メニューから [保存] を選択します。

パッチポリシーへのHP-UXパッチの追加

作成したHP-UXソフトウェアポリシーには、HP-UXパッチ、HP-UXソフトウェア、サーバースクリプトを追加できます。これらを追加しても、管理対象サーバー上にインストールされるわけではありません。ソフトウェアポリシーを管理対象サーバーにアタッチして、サーバーを修復する必要があります。

HP-UXパッチ、HP-UXソフトウェア、サーバースクリプトをHP-UXソフトウェアポリシーに追加するためのアクセス権が必要です。必要なアクセス権の取得については、システム管理者にお問い合わせください。ソフトウェア管理のアクセス権の詳細については、『SA 管理ガイド』を参照してください。

ソフトウェアリソースをソフトウェアポリシーに追加するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**ソフトウェアポリシー**] > [**HP-UX**] とオペレーティングシステムバージョンを選択します。
2. 内容ペインで、ソフトウェアポリシーを選択します。
3. 選択したソフトウェアポリシーを右クリックして、[ソフトウェアポリシー] ウィンドウを開きます。
4. [ビュー] ペインで [ポリシーアイテム] を選択します。
5.  をクリックするか、[アクション] メニューから [追加] を選択して、[ライブラリアイテムの選択] ウィンドウを表示します。
6. [タイプの参照] タブを選択して、ソフトウェアポリシーに追加できるアイテムを表示します。
7. ポリシーに追加するアイテムを1つまたは複数選択して、[**選択**] を押します。アイテムがポリシーに追加されます。

   または

   [フォルダーの参照] タブを選択して、ライブラリ内のフォルダー階層とフォルダーに含まれるアイテムのリストを表示します。ポリシーに追加するアイテムを1つまたは複数選択して、[**選択**] を押します。アイテムがポリシーに追加されます。
8. ソフトウェアのインストール順序を変更する場合は、  の矢印を使用します。
9. ポリシーからアイテムを除外する場合は、そのアイテムを選択して  をクリックします。この操作の詳細については、ソフトウェアのソフトウェアポリシーからの削除 (102ページ) を参照してください。
10. [ファイル] メニューから [保存] を選択して、変更内容をポリシーに保存します。

ソフトウェアのソフトウェアポリシーからの削除

HP-UX ソフトウェアポリシーからソフトウェアを削除しても、ソフトウェアは管理対象サーバーからアンインストールされません。このアクションでは、ポリシーからソフトウェアが削除されるだけです。管理対象サーバーから HP-UX ソフトウェアをアンインストールするには、管理対象サーバーからソフトウェアを直接アンインストールする必要があります。

HP-UXソフトウェアポリシーからHP-UXソフトウェアを削除するためのアクセス権が必要です。必要なアクセス権の取得については、システム管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

ソフトウェアポリシーからHP-UXソフトウェアを削除するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**ソフトウェアポリシー**] > [**HP-UX**] とオペレーティングシステムバージョンを選択します。
2. 内容ペインでソフトウェアポリシーを選択し、右クリックで [ソフトウェアポリシー] ウィンドウを開きます。
3. [ビュー] ペインで [ポリシーアイテム] を選択します。
4. 内容ペインに表示されるポリシーアイテムのリストから削除するアイテムを選択します。
5.  をクリックするか、[アクション] メニューから [削除] を選択します。
6. [ファイル] メニューから [保存] を選択して、変更内容をポリシーに保存します。

ソフトウェアポリシーの履歴の表示

HP-UXソフトウェアポリシーに関連付けられたイベントを表示するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**ソフトウェアポリシー**] > [**HP-UX**] とオペレーティングシステムバージョンを選択します。
2. 内容ペインでソフトウェアポリシーを選択し、右クリックで [ソフトウェアポリシー] ウィンドウを開きます。
3. [ビュー] ペインで [履歴] を選択します。ソフトウェアポリシーに関連付けられているイベントが内容ペインに表示されます。ポリシーで実行されたアクション、アクションを実行したユーザー、アクションを実行した時刻を表示できます。
4. [表示] ドロップダウンリストから、適切な期間を選択して表示するイベントの量を調整します。

ソフトウェアポリシーにアタッチされているサーバーの表示

SA クライアントでは、選択した HP-UX ソフトウェアポリシーがアタッチされているすべてのサーバーおよびデバイスグループのリストを表示できます。

選択したHP-UXソフトウェアポリシーがアタッチされているすべてのサーバーのリストを表示するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**ソフトウェアポリシー**] > [**HP-UX**] とオペレーティングシステムバージョンを選択します。
2. 内容ペインでソフトウェアポリシーを選択し、右クリックで [ソフトウェアポリシー] ウィンドウを開きます。
3. ビューペインで [サーバーの使用状況] を選択します。内容ペインに、選択したソフトウェアポリシーがアタッチされているサーバーのリストが表示されます。

フォルダー内のソフトウェアポリシーの検索

フォルダー階層内のHP-UXソフトウェアポリシーを検索するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**ソフトウェアポリシー**] > [**HP-UX**] とオペレーティングシステムバージョンを選択します。
2. 内容ペインで、ソフトウェアポリシーを選択します。
3. 右クリックで [**フォルダー内で検索**] を選択して、内容ペインにソフトウェアポリシーのフォルダー階層を表示します。

カスタム属性

HP-UXパッチ管理では、任意の管理対象サーバーに対して`hpuxpatch_dont_supersede`カスタム属性を設定できます (図11を参照)。

図11　　カスタム属性: hpuxpatch_dont_supersede

Server Automationでは、ソフトウェアポリシーに最新のパッチが含まれている必要があります (カスタム属性を設定しない場合)。このデフォルトの動作は、ソフトウェアポリシー内の最新のパッチを検索して依存関係を解決するように設計されています。最新のパッチが利用できない場合は、HP から最新のパッチをダウンロードする必要があることを通知するエラーメッセージがSAに表示されます。

パッチコンプライアンス

HP-UX パッチコンプライアンススキャンでは、管理対象サーバーにインストール済みのパッチをサーバーにアタッチされているパッチポリシーと比較します。実際のサーバー構成がサーバーにアタッチされているパッチポリシーと一致しない場合、サーバーはパッチポリシーに対するコンプライアンス違反となります。また、パッチポリシーのパッチがすでに新しいパッチで置き換えられていて、新しいパッチがサーバーにインストール済みである場合、サーバーはコンプライアンス状態とみなされます。

SAクライアントでは、パッチコンプライアンススキャンを実行したときに、サーバーにアタッチされているすべての HP-UX パッチポリシーに関するサーバーの全体的なコンプライアンスが示されます。サーバーにアタッチされているHP-UXパッチポリシーのうちの1つだけが非コンプライアンスであったとしても、そのサーバーは非コンプライアンスとみなされます。その場合は、非コンプライアンスのサーバーを表示して、適用可能なパッチポリシーに基づいてサーバーを修復できます。

SAクライアントでは、パッチポリシーに関する次のコンプライアンス情報が表示されます。

表8　管理対象サーバーのコンプライアンスステータス

アイコン	ステータス	説明
	**コンプライアンス**	サーバーにアタッチされているすべてのパッチポリシーがコンプライアンス状態です。つまり、すべてのパッチポリシーで指定されたすべてのパッチがサーバーにインストールされています。
	**非コンプライアンス**	サーバーにアタッチされているパッチポリシーの少なくとも1つが非コンプライアンス状態です。つまり、ポリシー内の少なくとも1つのパッチがサーバーにインストールされていません。
	**スキャン開始済み**	パッチコンプライアンス情報は現在収集中です。
	**スキャン失敗**	パッチコンプライアンススキャンを実行できませんでした。
	**スキャンが必要**	パッチコンプライアンス情報の収集が必要か、またはコンプライアンス情報が正しくありません。
—	**該当しない**	パッチコンプライアンス情報は適用されません。

標準的なHP-UXバンドルのパッチコンプライアンスステータスの例については、図12を参照してください。

図12　パッチコンプライアンスステータス

この例で、Server Automationは標準HP-UX QPKバンドルのコンプライアンスステータスが「258中2つのルールがコンプライアンス違反」であるとレポートします。QPKバンドル内のパッチの総数は259です。SAはこのバンドル内の1つのパッチがこの管理対象サーバーに該当しないと判断しました。そのため、259個のパッチではなく258個のパッチに対するコンプライアンスステータスをレポートしています。

また、SAは2つのパッチに優先されるパッチが存在することと、これらの優先されるパッチはサーバー上にインストール済みであるが、リポジトリにアップロードされていないことを特定しました。そのため、これらのパッチはコンプライアンス違反としてレポートされています。

パッチのインストール

パッチのインストールプロセスは、次の2つのフェーズで構成されます。

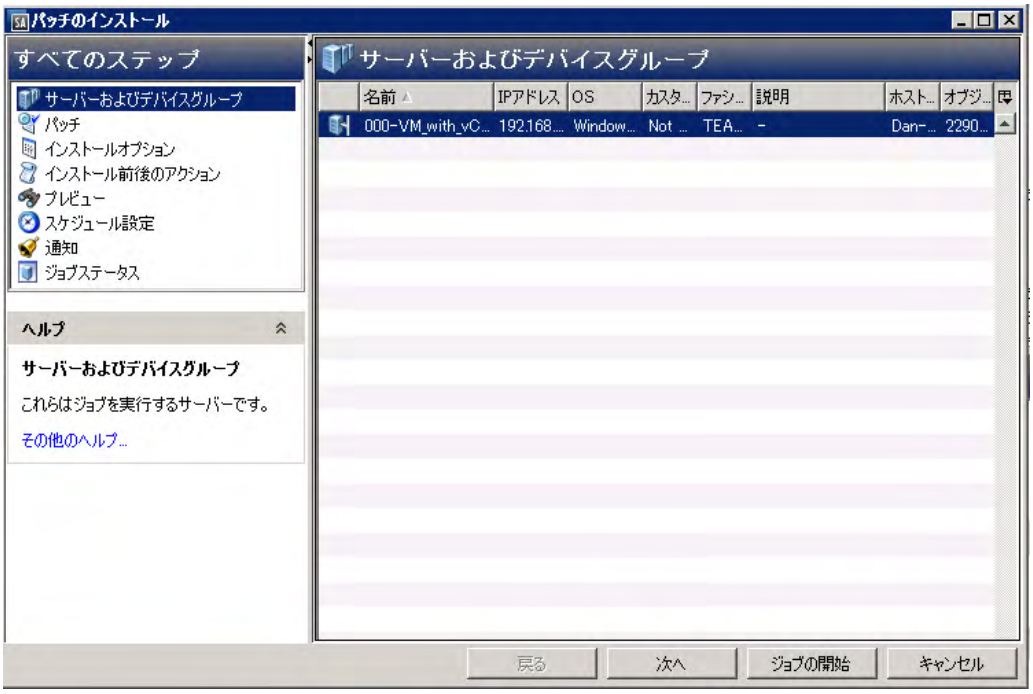
- **ダウンロードフェーズ**: このフェーズでは、Server Automationから管理対象サーバーへパッチをダウンロードします。このフェーズは、一般的にステージングと呼ばれます。
- **インストールフェーズ**:このフェーズでは、管理対象サーバーにパッチをインストールします。このフェーズは、一般的にデプロイメントと呼ばれます。

パッチがダウンロード(ステージング)されたらすぐにインストールを行うかどうかを指定できます。また、日時をスケジュール設定して後でインストールを行うこともできます。また、パッチ管理では、複数のパッチのベストエフォート型インストールのニーズにも対応しており、いずれかのパッチでエラーが発生した場合でも、パッチのインストールを続行するように指定することが可能です。

SAでは、パッチをインストールするコマンドの名前が表示されます。SAエージェントは、管理対象サーバー上でこのコマンドを実行します。デフォルトのコマンドライン引数はオーバーライドできます。

パッチ管理では、HP-UXパッチのインストールを適切に管理できるように、サーバーの再起動オプションやインストール前/インストール後スクリプトの管理、パッチのインストールのシミュレート(プレビュー)、インストールプロセスのステータスを通知する電子メール通知の設定などを行うことができます。セットアップは、[パッチのインストール]ウィザードの手順に沿って実行します。詳細については、図13を参照してください。

図13　[パッチのインストール]ウィザード



インストールフラグ

HP-UXパッチをインストールする際には、インストールフラグを指定できます。ただし、Server Automationでは、デフォルトのインストールフラグが使用され、これらのフラグを使用してパッチをインストールする必要があります。SAから渡されるデフォルトのインストールフラグを無効にするフラグや矛盾するフラグを指定しないようにする必要があります。

HP-UXパッチのインストール

パッチを管理対象サーバーにインストールするには、事前にパッチをSAにインポートして、ステータスを利用可能にしておく必要があります。制限付きのマークの付いたパッチは、必要なアクセス権を持つシステム管理者のみがインストールできます。

パッチを管理するにはアクセス権が必要です。必要なアクセス権の取得については、システム管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

パッチとサーバーを明示的に選択してインストールを実行できます。

管理対象サーバーにパッチをインストールするには、次の手順を実行します。

1. ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択します。
2. 内容ペインで、HP-UXサーバーを選択します。
3. [アクション] メニューで、[**パッチのインストール**] を選択します。[パッチのインストール] ウィンドウの最初のステップ (サーバーとサーバーグループ) が表示されます。
4. [**次へ**] をクリックして、[パッチのインストール] ウィンドウの次のステップへ進みます。
5. パッチのリストから、インストールするパッチを選択します。
6. 1つのステップが完了したら、[**次へ**] をクリックして次のステップへ進みます。[ジョブの開始] をクリックする前に、ステップリストに表示される完了したステップに戻って変更を行うことができます。
7. インストールジョブを起動する準備ができたら、[**ジョブの開始**] をクリックします。

   ジョブを後で実行するようにスケジュール設定している場合でも、ジョブの開始後にパラメーターを変更することはできません。

HP-UXインストールオプションの設定

次のタイプのパッチのインストールオプションを指定することができます。

- パッチがダウンロードされたらすぐにパッチのインストールを行うか、日時を指定して後でインストールを行う。
- いずれか1つのパッチでエラーが発生した場合でも、パッチのインストールプロセスを中断しない。
- さまざまなコマンドラインオプションを使用してインストールを行う。

これらのインストールオプションを設定するには、次の手順を実行します。

1. [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [オプション] ステップに進みます。
2. 次のいずれかのステージインストールオプションを選択します。
   - **継続**: すべてのフェーズを連続する1つの操作として実行できます。
   - **ステージ**: ダウンロードとインストールをスケジュールして別々に実行することができます。
3. いずれかのパッチでエラーが発生した場合でもパッチのインストールプロセスを続行する場合は、[エラーオプション] チェックボックスをオンにします。デフォルトで、このチェックボックスはオフになっています。

4 [インストールコマンド]テキストボックスに、表示されるコマンドのコマンドライン引数を入力します。

5 [**次へ**] をクリックして次のステップを進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

再起動オプションの設定

サーバーの再起動によるダウンタイムを最小限に抑えるため、サーバーを再起動するタイミングを制御できます。ベンダーの再起動割り当てを調整、パッチをインストールするたびにサーバーを再起動、すべてのサーバーの再起動を完全に抑制、またはすべてのパッチがインストールされるまで再起動を延期することができます。

[パッチのインストール]ウィンドウで再起動オプションを選択する場合、HPではHP-UXの再起動推奨設定(「パッチのプロパティの指定に基づいてサーバーを再起動する」オプション)を使用することを推奨しています。HP-UXの再起動設定を使用できない場合は、単一再起動オプション(「すべてのパッチがインストールされるまでサーバーを再起動しない」オプション)を選択します。

パッチのインストールの完了後にサーバーを再起動するかどうかを指定するオプションです。これらのオプションは、[パッチのインストール]ウィンドウで起動されるジョブのみに適用されます。これらのオプションによって、[パッチのプロパティ]ウィンドウの[インストールパラメーター]タブにある[再起動が必要]オプションが変更されることはありません。次に示すオプションの設定は、最初のオプションを除いて、[再起動が必要]オプションの設定よりも優先します。

- パッチのプロパティの指定に基づいてサーバーを再起動する
- デフォルトでは、パッチプロパティの[再起動が必要]オプションの設定に従って再起動が行われます。サーバーは最後に一度だけ再起動されます。これはパッチの依存関係を満たすために実行されます。実質的に、このオプションは、すべてのパッチがインストールされるまでサーバーを再起動しない3番目のオプションとして機能します。
- 各パッチのインストール後にサーバーを再起動する
- パッチプロパティの[再起動が必要]オプションが設定されていない場合でも、サーバーを再起動します。複数のパッチをインストールする場合、サーバーはすべてのパッチがインストールされた後に一度だけ再起動されます。
- すべてのパッチがインストールされるまでサーバーを再起動しない
- 選択したパッチの中に[再起動が必要]オプションが設定されているものが含まれていても、他のパッチにそのオプションが設定されていない場合、すべてのパッチのインストール後にサーバーが1回再起動されます。選択したパッチの中に[再起動が必要]オプションが設定されているものがない場合、サーバーは再起動されません。
- すべてのサーバーの再起動を抑制
- パッチプロパティの[再起動が必要]オプションが設定されている場合でも、サーバーを再起動しません。(ベンダー設定によっては、抑制オプションを無視して強制的に再起動を行う場合があります)。

再起動オプションを設定するには、次の手順を実行します。

1 [パッチのインストール]ウィンドウで、[**次へ**]をクリックして[アクション前と後]ステップに進みます。

2 いずれかの再起動オプションを選択します。

3 [**次へ**] をクリックして次のステップを進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

インストールスクリプトの指定

パッチごとにインストールの前または後に実行するコマンドまたはスクリプトを指定できます。インストール前スクリプトでは、たとえば、管理対象サーバー上で特定の条件をチェックすることができます。条件が満たされない場合やインストール前スクリプトが失敗した場合、パッチはインストールされません。インストール前スクリプトを使用すると、パッチを適用する前にサービスやアプリケーションをシャットダウンすることもできます。インストール後スクリプトを使用すると、管理対象サーバー上でクリーンアッププロセスを実行することができます。また、インストールフェーズまたはダウンロードフェーズの前または後に、管理対象サーバー上で次のタイプのスクリプトを実行するように指定することもできます。

- **インストール前**: 管理対象サーバーにパッチをインストールする前に実行するスクリプト。

- **インストール後**: 管理対象サーバーにパッチをインストールした後に実行するスクリプト。

インストール前スクリプトを指定するには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [アクション前と後] ステップに進みます。

2 [インストール前] タブを選択します。各タブでさまざまなスクリプトとオプションを指定できます。

3 [**スクリプトの有効化**] を選択します。このオプションを選択すると、タブのフィールドの残りの部分が有効になります。[スクリプトの有効化] を選択しない場合、スクリプトは実行されません。

4 [**保存されたスクリプト**] または [**アドホックスクリプト**] を選択します。

5 保存されたスクリプトは、SA Webクライアントを使用して前にSAに保存されたものです。スクリプトを指定するには、[**選択**] をクリックします。

6 スクリプトでコマンドラインフラグが必要である場合、[コマンド] テキストボックスにフラグを入力します。

7 実行時オプションの情報を選択します。ユーザーアカウントに root 以外を選択した場合は、ユーザー名とパスワードを入力します。このユーザーによってスクリプトが管理対象サーバー上で実行されます。

8 スクリプトがエラーを返した場合にインストールを停止するには、[**エラー**] チェックボックスを選択します。

9 [**次へ**] をクリックして次のステップを進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

パッチのインストールのスケジュール設定

パッチ適用の2つのフェーズは切り離すことができます。そのため、パッチのインストール (デプロイ) とパッチのダウンロード (ステージング) を独立して実行するようにスケジュール設定することができます。

パッチのインストールをスケジュール設定するには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [スケジュール設定] ステップに進みます。

デフォルトで、[スケジュール設定] ステップにはインストールフェーズ用のスケジュール設定オプションのみが表示されます。[インストールオプション] ステップで [ステージ] を選択した場合、ダウンロードフェーズ用のスケジュール設定オプションも表示されます。

2 次のいずれかのインストールフェーズオプションを選択します。

— **ただちにタスクを実行**: [サマリープレビュー] ステップでプレビュー分析を行うことができます。ダウンロードフェーズ用のスケジュール設定オプションは、[ダウンロード後ただちに実行] です。

— **次の時刻にタスクを実行**: 日付と時刻を指定して、後でダウンロードまたはインストールを実行することができます。

3 [**次へ**] をクリックして次のステップを進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。スケジュール設定したパッチのインストールは、パッチのダウンロードが完了している場合でも、(実行前に) キャンセルできます。

電子メール通知の設定

ダウンロード操作やインストール操作が正常に終了した、あるいはエラーで終了したときに、ユーザーに知らせるために電子メール通知を設定できます。

電子メール通知を設定するには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [通知] ステップに進みます。

2 ジョブが成功したときの通知ステータスを設定するには、アイコンを選択します。ジョブが失敗したときの通知ステータスを設定するには、アイコンを選択します。デフォルトでは、[通知] ステップにはインストールフェーズ用の通知ステータスのみが表示されます。

3 [チケットID] フィールドに、このジョブに割り当てるチケットIDを入力します。

4 [**次へ**] をクリックして次のステップを進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

[インストールオプション] ステップで [ステージ] を選択した場合、[通知] ペインにダウンロードとインストールの両方のフェーズに適用される通知オプションが表示されます。

パッチのインストールのプレビュー

インストールのプレビューでは、サーバーのパッチの状態に関する最新のレポートが表示されます。インストールのプレビューは、管理対象サーバーにインストールされるパッチ (標準HP-UXバンドルの1つまたは複数のパッチ) と必要なサーバーの再起動のタイプを確認するためのオプションステップです。プレビュープロセスでは、パッチのインストール対象として選択したサーバーに該当するパッチがすでにインストールされているかどうかを確認します。システム管理者がパッチを手動でインストールしている場合、サーバーにパッチがすでにインストールされている可能性があります。このような場合、SAではパッチの存在を把握できません。

プレビューでは、特定のHP-UXプロダクトを必要とするパッチ、および他のパッチを置き換えるパッチや他のパッチで置き換えられるパッチなどの、依存関係情報に関するレポートも作成されます。依存関係が満たされていない場合は、SAにその状態を示すエラーメッセージが表示されます。

パッチのインストールをプレビューするには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [サマリーレビュー] ステップに進みます。

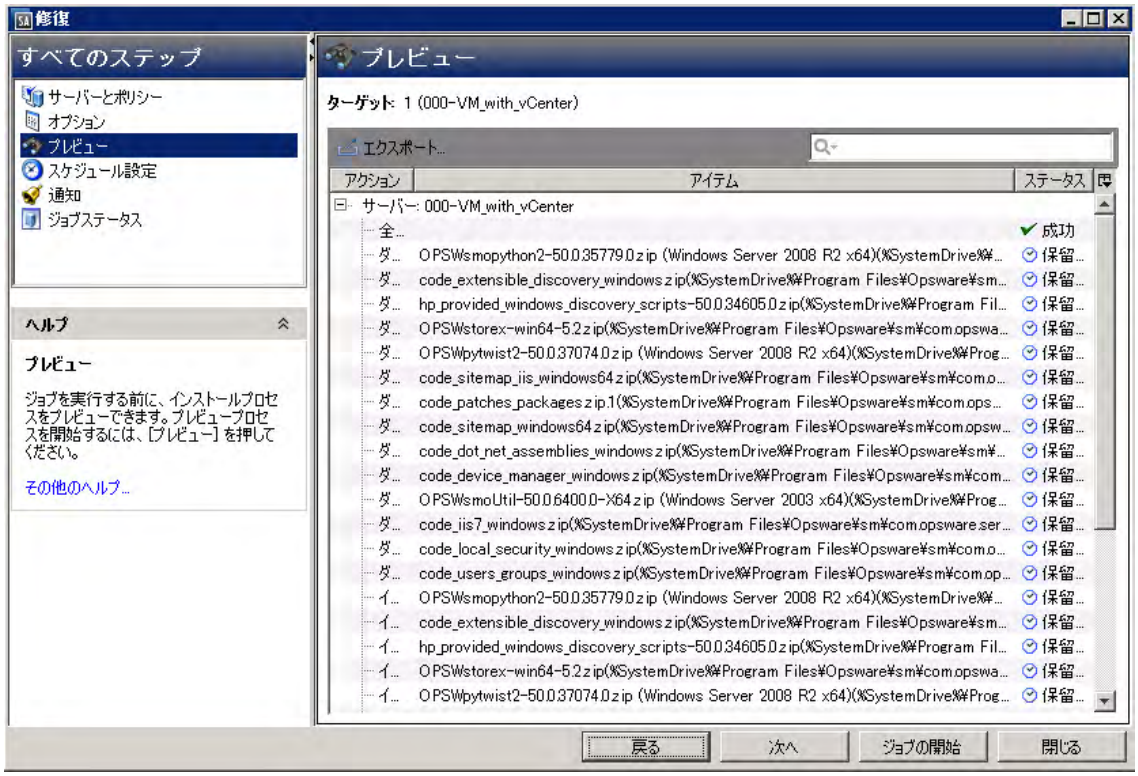
2 ウィンドウの上部にサーバー、サーバーグループ、およびパッチについて表示されている情報を確認します。

3 (オプション) [**プレビュー**] をクリックし、パッチのインストール時に実行される個々のアクションを表示します。テーブルの行を選択すると、プレビューしているアクションの詳細が表示されます。詳細については、図14を参照してください。

4 [**ジョブの開始**] をクリックしてインストールジョブを起動するか、[**キャンセル**] をクリックしてインストールを起動せずに [パッチのインストール] ウィンドウを閉じます。

[スケジュール設定] ステップで [ただちにタスクを実行] を選択すると、ジョブがすぐに開始します。[次の時刻にタスクを実行] を選択すると、指定した日時にジョブが開始します。

図14　　パッチインストールのプレビュー



ジョブの進行状況の表示

アクションが完了したか失敗したかなど、パッチのインストールジョブの進行状況を確認することができます。

ジョブの進行状況を表示するには、次の手順を実行します。

1　[パッチのインストール] ウィンドウで、[**次へ**] をクリックして [ジョブの進行状況] ステップに進みます。これにより、インストールジョブが開始されます。

進行状況バーとテキストで、テーブル内のアクションがどの程度完了したかを確認できます。次のアクションをサーバーごとに実行できます。

- **分析**: SAは、インストールに必要なパッチの確認、管理対象サーバーにインストールされた最新パッチのチェック、他に実行が必要なアクションの確認を行います。
- **ダウンロード**: SAから管理対象サーバーにパッチをダウンロードします。
- **インストール**: ダウンロードの完了後、パッチをインストールします。
- **最後に再起動**: [インストール前後のアクション] ステップでこのアクションを指定すると、サーバーが再起動します。
- **インストール前スクリプト / インストール後スクリプト / ダウンロード前スクリプト / ダウンロード後スクリプト**: [インストール前後のアクション] ステップでこのアクションを指定した場合、アンインストール前または後にスクリプトが実行されます。
- **インストールと再起動**: パッチをインストールすると、サーバーも再起動されます。
- **確認**: インストールしたパッチは、ソフトウェア登録に追加されます。

2 特定のアクションに関する詳細を追加表示するには、テーブルの行を選択して、ジョブの開始時刻と完了時刻を表示します。ナビゲーションペインで、[ジョブとセッション] を選択してジョブに関する詳細を確認します。

3 [**ジョブの終了**] をクリックしてジョブを実行しないようにするか、[**閉じる**] をクリックして [パッチのインストール] ウィンドウを閉じます。

パッチのアンインストール

HP-UX パッチおよびバンドルのアンインストールは、このリリースではサポートされていません。管理対象サーバーからHP-UXパッチおよびバンドルをアンインストールするには、管理対象サーバーからHP-UXパッチおよびバンドルを直接アンインストールする必要があります。

第4章 Solarisパッチ管理

概要

HP Server Automation (SA) では、Solarisパッチ管理により、SolarisパッチやIPSパッケージの確認、インストール、削除を行い、組織内にある管理対象サーバーのセキュリティを確保することができます。次のSolarisオペレーティングシステムについて、セキュリティの脆弱性に対するパッチを確認し、インストールできます。

表9 サポートされているオペレーティングシステムバージョン

OSバージョン	アーキテクチャー
Solaris 10 (アップデート1～9)	Sun SPARC、64ビットx86、32ビットx86、Niagara
Solaris 11	Sun SPARC、64ビットx86、32ビットx86、Niagara

Oracle Solaris 11では、パッチユニットはImage Packaging System (IPS) と呼ばれます。IPSは、ソフトウェアパッケージのインストール、アップグレード、削除などのソフトウェアライフサイクル管理のフレームワークを提供するネットワークベースのパッケージ管理システムです。Solaris 11の詳細と手順については、第5章「Solaris 11パッチ管理」(157ページ)を参照してください。

詳細な管理対象サーバープラットフォームのサポート情報については、『SA Support and Compatibility Matrix』を参照してください。

機能

SAでは、次の機能によってSolarisでのパッチ適用を自動化します。

- **管理対象サーバーで必要なパッチとIPSパッケージを特定します。**

  SAでは、OSバージョン、サーバー上にインストールされているアプリケーション、サーバー上にインストール済みのパッチを調べて、管理対象のSolarisサーバーに必要なパッチやIPSパッケージを特定できます。SAは、利用可能なすべてのSolarisパッチを調べた後に、それぞれのサーバーに必要なパッチ、インストール順序、再起動の要件を特定します。

- **Solarisパッチポリシーを作成します。**

  これは、モデルベースによるSolarisサーバーの管理です。SAでは、ポリシー設定担当者がSolarisパッチポリシーを作成して、IT環境のモデルを定義できます。Solarisパッチポリシーでは、管理対象サーバーにインストールする必要のあるパッチ、パッチクラスター、スクリプトを指定します。その後、システム管理者がIT環境内のSolarisサーバーにパッチポリシーを適用します。Solarisパッチポリシーは、ダウンロードしたSolarisパッチおよびパッチクラスターから作成します。

- **Solarisパッチ、パッチクラスター、パッチバンドルをダウンロードし、さらにそれらと関連ベンダー情報をSAライブラリに保存します。**

SAでは、My Oracle Webサイトから、Solarisパッチ、パッチクラスター、Fujitsuクラスター、IPSパッケージ、および関連するベンダー情報をインポートして、Solarisパッチポリシーに追加することができます。ベンダー情報には、再起動の指定、プラットフォームの設定(マルチプラットフォームパッチのサポートなど)、パッチの依存関係、リリースノートファイルなどが含まれます。パッチポリシーはSAライブラリに保存され、SAクライアントからアクセスできます。

- **Solarisパッチが依存するパッチをすべて解決します。**

  SAでは、Solarisパッチのメタデータをすべて調べて、現在不使用のパッチ、他のパッチが優先されるパッチ、互換性のないパッチ、必要な依存パッチ、取り消し済みのパッチを識別し、パッチポリシーを更新することができます。また、SAでは、パッチおよびIPSパッケージを正しいインストール順序に配置することもできます。

- **管理対象サーバーにSolarisパッチ、パッチクラスター、IPSパッケージをインストールします。**

  SAでは、管理対象サーバーにSolarisパッチ、パッチクラスター、IPSパッケージを直接インストールするか、Solarisパッチポリシーを使用してインストールすることができます。SAクライアントでは、パッチポリシー内のパッチおよびパッチクラスターのインストール順序を設定できます。ポリシーには、Solarisパッチの再起動設定も含まれます。

  SAでは、管理対象のSolarisサーバーでパッチポリシーを修復することにより、パッチ、パッチクラスター、Fujitsuクラスター、パッチバンドル、IPSパッケージをインストールします。修復プロセスでは、シングルユーザーモード、再構成の再起動、即時の再起動など、さまざまな再起動設定が利用できます。

  SAでは、個々のパッチが各サーバーに適用可能であることを確認します。たとえば、パッチを適用するパッケージやアプリケーションがサーバー上にインストールされていない場合や、さらに新しいパッチがすでにサーバー上にインストールされている場合、SAは該当するパッチをサーバー上にインストールしません。

- **Solarisパッチをシングルユーザーモードでインストールします。**

  Oracleが公開したパッチメタデータで指定されている場合、SAはシングルユーザーモードでSolarisパッチをインストールします。パッチのインストールが完了すると、SAはマルチユーザーモードに戻ります(インストールモードに関する関連情報については、パッチのインストールのトラブルシューティングを参照してください)。

- **Solarisゾーンごとにパッチをインストールします。**

  SAクライアントでは、Solarisパッチポリシーを使用して、Solarisグローバルゾーンや非グローバルゾーンにパッチをインストールできます。

- **パッチインストールプロセスを確立します。**

  SAでは、Solarisパッチ管理のステージ(分析、ダウロード、インストールなど)を分けて、個別にスケジュール設定することができます。各ステージ完了のジョブステータスに対応した電子メール通知を設定し、各ジョブにチケットIDを関連付けることができます。

- **パッチポリシーに基づいて、サーバーのコンプライアンスステータスを検証します。**

  コンプライアンスビューでは、サーバーがパッチポリシーに基づいて構成されているかを確認し、非コンプライアンスサーバーを修復することができます。サーバープラットフォーム、パッチの優先度、パッケージの適用可能性のチェックを含むコンプライアンススキャンを実行できます。

- **ソフトウェアリソースとサーバーを検索します。**

  SAクライアントのライブラリでは、強力かつ柔軟な検索条件(可用性、アーキテクチャー、オペレーティングシステム、再起動オプション、バージョン、その他のパラメーターなど)を使用して、Solarisパッチ、クラスター、パッチポリシーを検索できます。また、名前、フォルダー名、可用性、オペレーティングシステムなどでSolarisパッチポリシーを検索することもできます。検索機能については、SAクライアントでのオブジェクトの検索 (33ページ)を参照してください。

ポリシーベースのパッチ管理

Solaris パッチポリシーを使用すると、パッチポリシーを作成することにより、Solaris サーバーに適切なパッチを確実にインストールすることができます。パッチポリシーは望ましい IT 環境を表すモデルです。Solaris パッチポリシーでは、すべてのサーバーに標準的な内容をプロビジョニングするため、サーバーのベースラインを定義します。SAを使用すると、Solarisパッチの自動ダウンロード、ダウンロードしたパッチのポリシーへの追加、ポリシー内のパッチのインストール順序の定義、パッチのすべての依存関係の自動解決、ポリシー内のすべてのパッチの再起動設定の指定を行うことができます。

その後、システム管理者がSolarisパッチポリシーをサーバーに適用して、それぞれの環境内のサーバーを管理することができます。パッチポリシーに基づいて管理対象サーバーを修復する際に、SA は管理対象サーバーに変更を適用します。パッチポリシーに変更を加える必要がある場合、ポリシー設定担当者はポリシーで定義したベースラインを変更するだけで、追加の差分がターゲットサーバーに適用されます。

Solarisパッチバンドル

Solarisパッチバンドルをインポートしてインストールできます。

- Solarisパッチバンドルは、`solpatch_import`コマンドを使用してダウンロードして、SAライブラリにインポートできます。
- Solaris パッチバンドルは管理対象サーバーに直接インストールすることも、デバイスグループのすべてのサーバーにインストールすることもできます。また、SolarisパッチバンドルをSolarisパッチポリシー(またはソフトウェアポリシー)に追加し、そのポリシーを管理対象サーバーまたはデバイスグループにアタッチして、ポリシーに基づいてサーバーを修復することもできます。サーバーまたはデバイスグループを修復すると、アタッチされているポリシーで指定されたSolarisパッチが管理対象サーバーに自動的にインストールされます。
- `solpatch_import`のすべてのアクション(ポリシーに関するアクションを除く)をパッチバンドルで実行できます。
- バンドルをインポートすると、バンドルに含まれるすべてのパッチに基づいて、SAライブラリ内のメタデータが更新されます。SAライブラリ内のパッチの数によっては、バンドルのインポートに時間がかかる場合があります。
- SAライブラリからパッチバンドルを削除するか、`solpatch_import`コマンドを使用すると、バンドルのすべての内容が削除されます。
- パッチバンドルのデフォルトの再起動設定を次に示します。これらの設定を変更する場合は、SAクライアントでパッチバンドルを開き、プロパティビューを選択して、インストールパラメーターを編集します。
  - 再起動が必要: [はい] - パッチバンドルが正常にインストールされたときに管理対象サーバーを再起動します。
  - インストールモード: [シングルユーザーモード] - パッチバンドルをシングルユーザーモードでインストールします。ただし、Solaris システムは再起動してシングルユーザーモードになり、パッチバンドルのインストール後に再起動してマルチユーザーモードになります(インストールモードに関する関連情報については、パッチのインストールのトラブルシューティング (154 ページ)を参照してください)。
  - 再起動タイプ: [再構成] - パッチバンドルのインストール後に再構成の再起動を実行します。
  - 再起動時刻: [即時] - パッチバンドルのインストール後すぐにサーバーを再起動します。
- 前提となる必要なパッチがインストールされていないためにバンドル内の 1 つ以上のパッチがインストールされなかった場合、パッチバンドルが正常にインストールされた場合でも、Solaris パッチコンプライアンススキャンでサーバーはコンプライアンス違反状態と表示されます。インストールされなかったパッチバンドル内のパッチの詳細については、パッチバンドルのインストールジョブのログファイルを参照してください。

パッチバンドルがソフトウェアポリシーに含まれている場合に、同様の状態になった場合は、ソフトウェアコンプライアンススキャンでも同じようにサーバーがコンプライアンス違反状態と表示されます。

このサーバーをコンプライアンス状態にするには、関連するパッチをパッチポリシーに追加し、ポリシーの依存関係を解決して必要なすべてのパッチをポリシーに追加し、サーバー上でポリシーの修復を行います。

- `solpatch_import`コマンドを使用するには、「パッケージの管理」のアクセス権を読み取り/書き込みに設定する必要があります。アクセス権の詳細については、『SA 管理ガイド』を参照してください。
- Solaris パッチバンドルのインポート時にエラーが発生した場合は、次のトラブルシューティング手順を実行します。
  a. SAパッチがインストールされているSAコアにrootとしてログインします。
  b. パッチのインストールのログファイルを確認します。通常、ログファイルは次の場所にあります。

     `/var/log/opsware/install_opsware/patch_opsware.<タイムスタンプ>.log`

  c. このログファイルで「update_supplements」を含むメッセージを検索します。たとえば、次の grep コマンドを使用することができます。

     `grep update_supp patch_opsware*`

  d. 検索結果に、「update_supplements successfully completed」を含むログメッセージが表示されます。update_supplements が失敗したことを示すメッセージが検出された場合は、次のように Solaris パッチの補足ファイルを手動で更新します。
  e. `solpatch_import`コマンドがインストールされているSAコアシステムにrootとしてログインします。
  f. 次の`solpatch_import`コマンドが存在するディレクトリに変更します。

     `/opt/opsware/solpatch_import/bin`

  g. 次のコマンドを実行します。

     `./solpatch_import -a update_supplements`

  h. Solarisパッチバンドルのインポートを再度実行します。

Fujitsuクラスター

Fujitsuクラスターは、Fujitsu製ハードウェアで実行されるSolarisオペレーティングシステム用に作成されたクラスターです。SAはFujitsuクラスターをサポートしています。

SAコマンド

Fujitsuクラスターでは、標準のSolarisクラスターと同じクラスターコマンドを使用できます。

クラスターコマンドに関する関連情報を表示する場合は、次のコマンドを使用します。

`/opt/opsware/solpatch_import/bin/solpatch_import --manual`

Fujitsuクラスターをインポートするには、`solpatch_import`コマンドを使用する必要があります。

クラスターのダウンロード

1つの`solpatch_import`コマンドを使用してFujitsuクラスターとSolaris推奨クラスターファイルの両方をダウンロードする場合、両方のファイルが同じ場所にダウンロードされ、SAコアにはインポートされません。最初にダウンロードしたクラスターは、次のダウンロードするクラスターで上書きされます。これは、両方のクラスターの名前が同じであるためです(10_Recommended.zipなど)。ファイルが上書きされるのを避ける

ため、1つのsolpatch_importコマンドを使用して2つのクラスターをダウンロードしないようにしてください。最初にダウンロードしたクラスターを別の場所に移動してから、次のクラスターをダウンロードする必要があります。

1 つの solpatch_import コマンドを使用して、同じオペレーティングシステムの Fujitsu クラスターと標準の Solaris 推奨クラスターをダウンロードすることはできます。これは、SA でファイルをインポートする際に、ダウンロードしたファイルがすぐにコアにインポートされるためです。ファイルの上書きは発生しません。

パッチポリシー

コマンドラインまたはSAクライアントを使用して、任意のクラスターに関するパッチポリシーを作成できます。

コマンドラインから `-a policy` または `--action=policy` オプションを使用して Fujitsu クラスターに関するパッチポリシーを作成すると、クラスター内の適用可能なすべてのパッチが適用されます。これは、Fujitsu がクラスターのインストールを使用してクラスターに含まれている適用可能なすべてのパッチをお使いのハードウェアモデルにインストールすることを意図しているかどうかに関係なく実行されます。余分なパッチを適用しても悪影響はありません。

Fujitsuがお使いのハードウェアモデル向けに作成したパッチのみを適用する場合は、SA クライアントを使用して新規ポリシーを作成して、Fujitsu クラスターを追加します。ポリシーを修復する際に、SAによって関連するパッチのみが正しく適用されます。

クイックスタート

SAでSolarisパッチ適用のセットアップと初期化を行うには、次の手順を実行します。

1. 次のアクセス権を持つSAユーザーを作成します。
   - `/Opsware/Tools/Solaris Patching`フォルダーの読み取り/書き込みアクセス権
   - 「パッチの管理」機能のアクセス権の読み取り/書き込みアクセス権
   - 次の機能のアクセス権を「はい」に設定
     - 「パッチのインストールの許可」
     - 「パッチのアンインストールの許可」
     - 「パッチコンプライアンスルールの管理」

   ユーザーの作成とアクセス権の設定の詳細については、『SA 管理ガイド』を参照してください。
2. SAスライスコアサーバーまたはマスターコアサーバーに`root`としてログインします。
3. `/etc/opt/opsware/solpatch_import/solpatch_import.conf` にある構成ファイルを次のように更新します。

   `hpsa_user`および`hpsa_pass`で始まる行にSAのユーザー名とパスワードを追加します。

   例:

   ```
   hpsa_user=お使いのSAのユーザー名
   hpsa_pass=<パスワード>
   ```

   - `download_user`および`download_pass`で始まる行にMy Oracleアカウントのユーザー名とパスワードを追加します。

     例:

     ```
     download_user=My_Oracleユーザー名
     download_pass=<パスワード>
     ```

     この構成ファイルは、`solpatch_import`コマンドで使用します。

専用の構成ファイルを個別に作成して、solpatch_importで-cオプションまたは--confオプションを使用して構成ファイルを指定することができます。

4 (オプション) 次のコマンドを実行して、構成ファイル内のパスワードを暗号化します。

```
solpatch_import --hide_passwords
```

solpatch_importコマンドは/opt/opsware/solpatch_import/binにあります。

SAでSolarisパッチ管理を使用するのが初めての場合は、新規のSolarisパッチデータベースを作成する必要があります。solpatch_import -a create_dbコマンドを実行すると、Solarisパッチデータベースが作成されて、Oracleからパッチ情報が (patchdiag.xrefファイルに) ダウンロードされ、パッチ情報がデータベースにアップロードされます。

```
solpatch_import -a create_db
```

patchdiag.xrefファイルがすでに存在する場合は、次のコマンドを使用して、Solarisパッチデータベースを作成し、patchdiag.xrefファイルからパッチ情報をデータベースにアップロードします。

```
solpatch_import -a create_db -x <ローカルのpatchdiag.xrefファイル>
```

SAライブラリ内に存在するSolarisパッチの数によっては、このコマンドの処理に数時間かかることがあります。

これで、SAでSolarisパッチをダウンロードして、サーバーにインストールする準備ができました。次の各項の手順を参照してください。

5 Solaris パッチデータベースに最新のパッチが含まれていることを確認します。詳細については、Solarisパッチデータベースの管理 (135ページ) を参照してください。

パッチ管理のプロセス

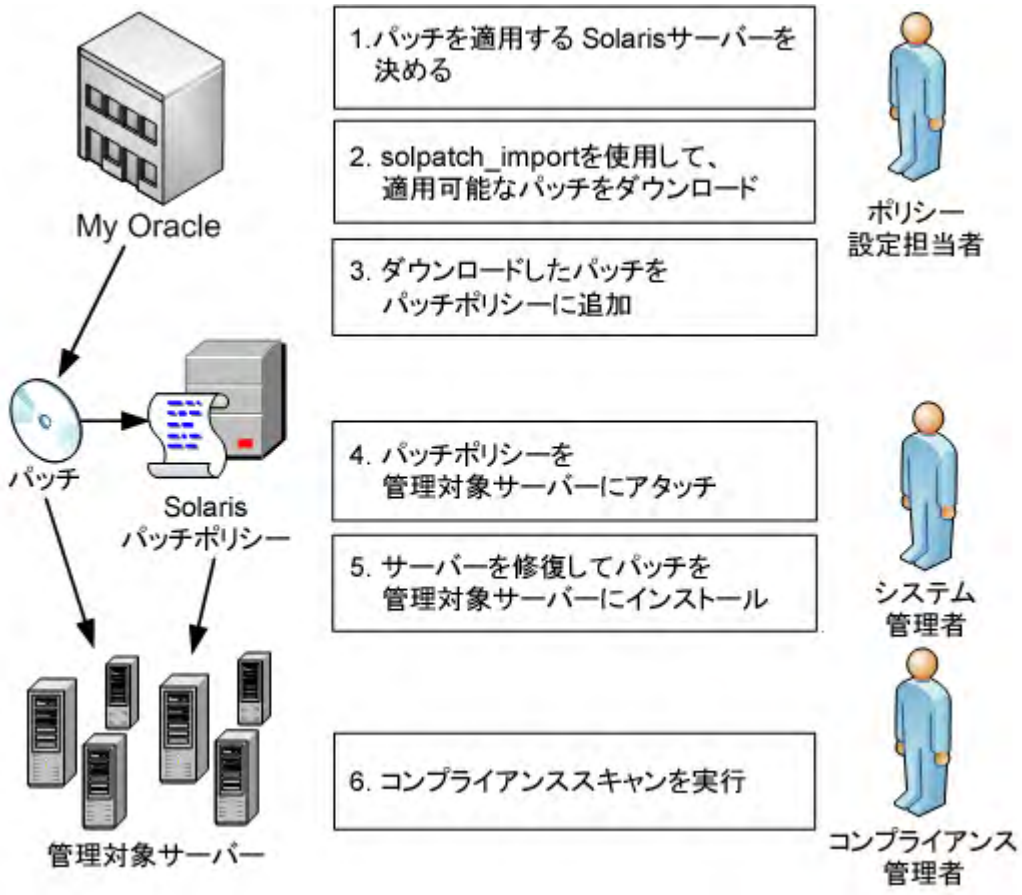
Solarisのパッチ適用プロセスは、次のフェーズで構成されます。

- サーバーへのパッチの適用 (119ページ)
- パッチのインストール (120ページ)

サーバーへのパッチの適用

図15は、パッチを適用するSolarisサーバーを特定し、それぞれのサーバーに必要なパッチを識別するための手順を示しています。これらの手順には、パッチのダウンロードと管理対象のSolarisサーバーへのパッチのインストールも含まれています。

図15　　選択したサーバーへのパッチの適用



1. ポリシー設定担当者が、パッチを適用する必要のあるSolarisサーバーを特定します。たとえば、ある特定のSolarisサーバー、Solaris 5.10を実行しているすべてのサーバー、特定の部門で使用しているすべてのサーバー、または使用しているSolarisサーバーの一部などにパッチを適用することができます。
2. ポリシー設定担当者が`solpatch_import`コマンドを使用して、選択したSolarisサーバーに必要なパッチをOracleからダウンロードします。`solpatch_import`コマンドは、選択したサーバーで必要なパッチを特定し、パッチのすべての依存関係を解決し、すべての適用可能なパッチを取り込みます。
3. ポリシー設定担当者が、これらのパッチをSolarisパッチポリシーに追加します。

   この手順は`solpatch_import`コマンドを**手順2**の一部として実行することにより、実行できます (パッチバンドルを除く)。または、SAクライアントを使用して、Solarisパッチをパッチポリシーに手動で追加することもできます。
4. システム管理者がパッチポリシーを管理対象サーバーにアタッチします。

   システム管理者はパッチをテストするために、パッチポリシーを1つまたは複数のテストサーバーにアタッチして、サーバーが期待どおりに動作することを確認できます。問題が発生した場合は、パッチポリシーへのパッチの追加または削除を行って、パッチを再度テストすることができます。テストが完了したら、システム管理者はパッチポリシーを他のすべてのSolarisサーバーにアタッチできます。

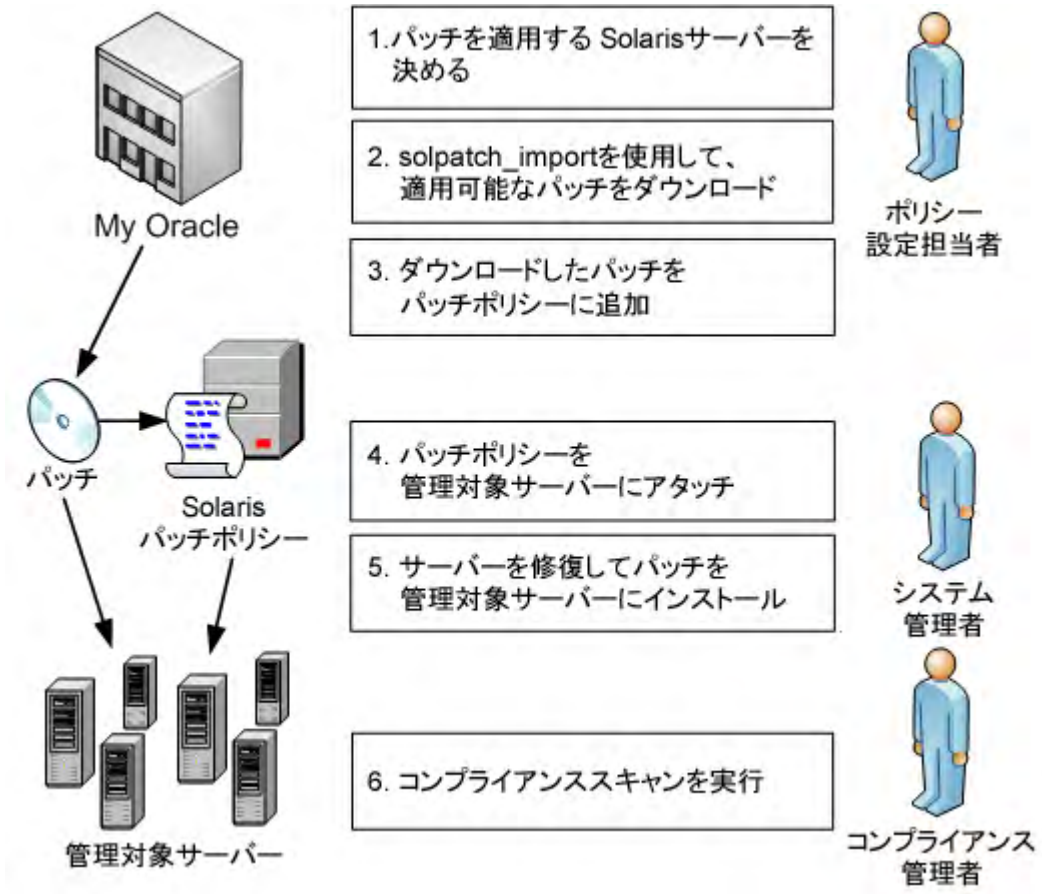
5 システム管理者がパッチポリシーを修復します。修復プロセスでは、管理対象サーバーにパッチがインストールされます。

6 コンプライアンス管理者がコンプライアンススキャンを実行して、必要なパッチがインストールされていないサーバーを特定します。

パッチのインストール

図16は、インストールが必要なSolarisパッチを特定し、依存するすべてのパッチを識別するための手順を示しています。これらの手順には、1つまたは複数のSolarisパッチのダウンロードとインストールも含まれています。

図16 選択したパッチのインストール



1 ポリシー設定担当者が、インストールする必要のあるSolarisパッチを特定します。管理対象サーバーに個別のSolarisセキュリティパッチや既知の問題を修正するパッチをインストールすることを要求される場合があります。

2 ポリシー設定担当者が`solpatch_import`コマンドを使用して、特定のパッチ、パッチクラスター、またはパッチバンドルをOracleからダウンロードします。

3 ポリシー設定担当者が、これらのパッチをSolarisパッチポリシーに追加します。

この手順は`solpatch_import`コマンドを**手順2**の一部として実行することにより、実行できます (パッチバンドルを除く)。または、SAクライアントを使用して、Solarisパッチをパッチポリシーに手動で追加することもできます。

4 ポリシー設定担当者がSAクライアントの 依存関係の解決(S) ボタンを使用して、パッチポリシー内のパッチのすべての依存関係を解決します。これには、依存するパッチ、優先パッチ、使用されなくなったパッチ、互換性のないパッチ、取り消し済みのパッチの特定などが含まれます。

5 システム管理者がパッチポリシーを管理対象サーバーにアタッチします。

システム管理者はパッチをテストするために、パッチポリシーを1つまたは複数のテストサーバーにアタッチして、サーバーが期待どおりに動作することを確認できます。問題が発生した場合は、パッチポリシーへのパッチの追加または削除を行って、パッチを再度テストすることができます。テストが完了したら、システム管理者はパッチポリシーを他のすべてのSolarisサーバーにアタッチできます。

6 システム管理者がパッチポリシーを修復します。修復プロセスでは、管理対象サーバーにパッチがインストールされます。

7 コンプライアンス管理者がコンプライアンススキャンを実行して、必要なパッチがインストールされていないサーバーを特定します。

パッチコンプライアンス

Solarisパッチコンプライアンススキャンでは、管理対象サーバーにインストール済みのSolarisパッチとサーバーにアタッチされているSolarisパッチポリシー内のパッチと比較して、結果をレポートします。実際のサーバー構成がサーバーにアタッチされているSolarisパッチポリシーと一致しない場合、サーバーはSolarisパッチポリシーに対するコンプライアンス違反となります。

特定のSolarisサーバーに適用不可能なパッチがサーバーのコンプライアンスステータスに影響することはありません。次に例を示します。

- ポリシーにパッケージSUNWpkga用のパッチが含まれているが、サーバー上にSUNWpkgaがインストールされていない場合、このパッチはサーバーに適用できません。そのため、このパッチがこのサーバーでのコンプライアンススキャンの結果に影響することはありません。コンプライアンスのサマリーには、適用不可能なパッチは含まれません。たとえば、ポリシーに5つのパッチが含まれているが、特定のサーバーに適用可能なパッチが3つだけで、これらの3つのパッチがサーバー上にインストールされている場合、コンプライアンスのサマリーには「3個中3個のルールがコンプライアンス準拠」と表示され、適用不可能な2つのパッチは無視されます。
- パッチポリシーの特定のパッチがすでに新しいパッチで置き換えられていて、新しいパッチがサーバーにインストール済みである場合、サーバーはコンプライアンス準拠と表示されます (このパッチポリシーは古くなっています。パッチポリシーはパッチの依存関係の解決 (128 ページ) の手順に従って更新できます)。
- 手動インストールパッチは常にコンプライアンス違反と表示されます。これは、SAで手動インストールパッチがSolarisサーバーにインストールされているかどうかを特定できないためです。詳細については、手動パッチのインストール—patchadd (149ページ) を参照してください。

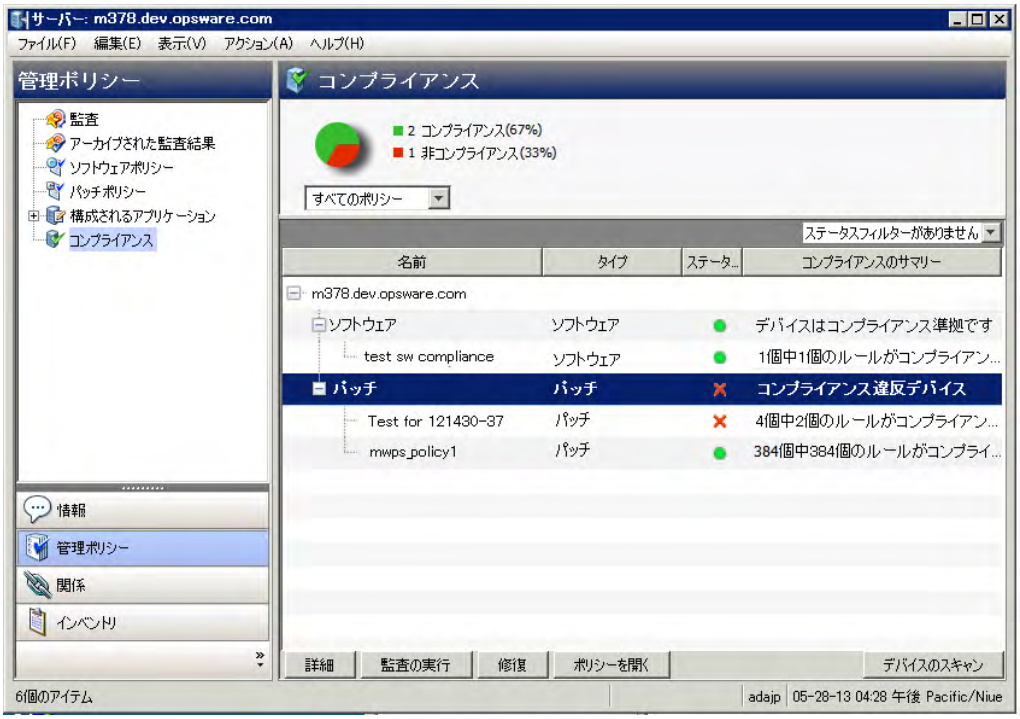
SAクライアントで、パッチコンプライアンススキャンを実行すると、スキャン結果にサーバーにアタッチされているすべてのSolarisパッチポリシーに関するサーバーの全体的なコンプライアンスが示されます。サーバーにアタッチされているSolarisパッチポリシーのうちの1つだけが非コンプライアンスであったとしても、そのサーバーは非コンプライアンスとみなされます。その場合は、非コンプライアンスのサーバーを表示して、適用可能なパッチポリシーに基づいてサーバーを修復できます。

図17は、Solarisサーバーのコンプライアンスビューです。いくつかのパッチがサーバー上にインストールされていないため、サーバーはコンプライアンス違反状態になっています。

- パッチポリシー「Test for 121430-37」には、適用可能なパッチが4つ含まれていますが、サーバーにインストールされているのは2つだけです。

- パッチポリシー「mwps_policy1」には、適用可能なパッチが 384 個含まれていて、そのすべてのがサーバーにインストールされています。

図17　　Solarisサーバーのコンプライアンス結果



次の表は、[ステータス]列の値について説明したものです。

表10　　管理対象サーバーのコンプライアンスステータス

コンプライアンスアイコン	コンプライアンスステータス	説明
	**コンプライアンス**	サーバーにアタッチされているすべてのパッチポリシーがコンプライアンス状態です。すなわち、すべてのパッチポリシーで指定されたすべてのパッチがサーバーにインストールされています。
	**非コンプライアンス**	サーバーにアタッチされているパッチポリシーの少なくとも1つが非コンプライアンス状態です。つまり、ポリシー内の少なくとも1つのパッチがサーバーにインストールされていません。
	**スキャン開始済み**	パッチコンプライアンス情報は現在収集中です。
	スキャン失敗	パッチコンプライアンススキャンを実行できませんでした。
	**スキャンが必要**	パッチコンプライアンス情報の収集が必要か、またはコンプライアンス情報が正しくありません。
—	**該当しない**	パッチコンプライアンス情報は適用されません。

SAクライアントでは、個別のサーバーのパッチコンプライアンスのチェックや、ファシリティ内のすべてのサーバーおよびサーバーグループの全体的なコンプライアンスレベルの確認を行うことができます。

データセンター内のすべてのサーバーのコンプライアンススキャンについては、『SA User Guide: Application Automation』を参照してください。

パッチコンプライアンススキャンの実行

パッチコンプライアンススキャンを実行するためのアクセス権が必要です。アクセス権の取得については、SAの管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

サーバーでSolarisパッチコンプライアンスのスキャンを行うには、次の手順を実行します。

1. ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択します。内容ペインにサーバーのリストが表示されます。
2. 内容ペインで、Solarisサーバーを選択します。
3. 右クリックまたは[**アクション**] メニューから、[**スキャン**] > [**パッチコンプライアンス**] を選択します。[パッチコンプライアンススキャンステータス] ウィンドウが表示され、パッチコンプライアンススキャンが開始されます。
4. [ステータス] 列のステータスアイコンをクリックすると、現在のステータスの詳細が表示されます。
5. スキャンが終了したら、[パッチコンプライアンススキャンステータス] ウィンドウの [ステータス] 列の結果を確認します。詳細については、図16も参照してください。
6. (オプション) 内容ペインで、[表示] ドロップダウンリストから [コンプライアンス] を選択して、非コンプライアンス状態のパッチポリシーを表示します。これには、サーバーにアタッチされているすべてのパッチポリシーと各ポリシーのコンプライアンスステータスが表示されます。

パッチポリシー管理

HP Server Automationでは、Solarisパッチポリシーを使用して、それぞれの環境内の管理対象サーバーや管理対象サーバーグループにパッチやパッチクラスターをインストールできます。パッチポリシーを作成して、サーバーやサーバーグループにアタッチすることができます。サーバーまたはサーバーグループの修復を行うと、アタッチされたポリシーで指定されたパッチがインストールされます。修復プロセスでは、ポリシーに基づいて、サーバー上に実際にインストールされている内容とサーバー上にインストールすべきパッチとの比較を行います。その後、SAで、ポリシーに準拠するようにサーバーを構成するのに必要な操作が特定されます。

Solaris パッチやパッチクラスターは、パッチポリシーに追加した後で、インストールする順序を指定することができます。パッチポリシーをサーバーにアタッチしてサーバーを修復すると、SAによりパッチポリシー内のパッチやパッチクラスターが指定された順序でインストールされます。

また、ソフトウェアポリシーを使用してパッチの管理やインストールを行うこともできます。Solarisパッチポリシーに他のパッチポリシーを含めることはできませんが、ソフトウェアポリシーにSolarisパッチポリシーを含めることは可能です。詳細については、『SAユーザーガイド: ソフトウェア管理』を参照してください。

SA クライアントを使用すると、Solaris パッチポリシーを OS シーケンスにアタッチすることもできます。OS シーケンスを実行したときに、([ポリシーの修復] ウィンドウで) 修復オプションが有効になっている場合、パッチポリシー内のすべてのパッチが OS シーケンスをインストール中のサーバーにインストールされます。修復オプションが無効になっている場合、どのパッチもサーバーにインストールされません。詳細については、『SA ユーザーガイド: プロビジョニング』を参照してください。

Solarisパッチポリシー管理に含まれるタスクは、次のとおりです。

- Solarisパッチポリシーの作成 (124ページ)
- Solarisパッチポリシーの表示 (125ページ)
- Solarisパッチポリシーの編集 (127ページ)

- パッチポリシーへのSolarisパッチの追加 (127ページ)
- Solarisパッチポリシーからのパッチの削除 (128ページ)
- パッチの依存関係の解決 (128ページ)
- カスタム属性のパッチポリシーへの追加 (131ページ)
- カスタム属性のパッチポリシーからの削除 (131ページ)
- パッチポリシーの履歴の表示 (132ページ)
- パッチポリシーに関連するソフトウェアポリシーの表示 (132ページ)
- パッチポリシーに関連するOSシーケンスの表示 (132ページ)
- パッチポリシーにアタッチされているサーバーの表示 (132ページ)
- フォルダー内のSolarisパッチポリシーの検索 (133ページ)
- パッチポリシーを使用したパッチのインストール (150ページ)

『SAユーザーガイド: プロビジョニング』も参照してください。

Solarisパッチポリシーの作成

SAクライアントでは、次のいずれかのライブラリ機能を使用してSolarisパッチポリシーを作成します。

- ライブラリ—タイプ別 (124ページ)
- ライブラリ—フォルダー別 (125ページ)
- solpatch_import (125ページ)

Solaris パッチポリシーの作成と管理を行うためのアクセス権が必要です。アクセス権の取得については、システム管理者にお問い合わせください。パッチ管理のアクセス権の詳細については、『SA 管理ガイド』を参照してください。

ライブラリータイプ別

タイプ別機能を使用してパッチポリシーを作成するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] > [**Solaris**] を選択します。内容ペインにパッチポリシーのリストが表示されます。デフォルトで、パッチポリシーはオペレーティングシステムファミリ別に構成されます。
2. ダブルクリックしてオペレーティングシステムを選択します。
3. [アクション] メニューで、[**新規**] を選択して [Solarisパッチポリシー] ウィンドウを開きます。
4. [名前] フィールドに、Solarisパッチポリシーの名前を入力します。
5. (オプション) [説明] フィールドに、ポリシーの用途や内容の説明を入力します。
6. [**参照**] をクリックし、フォルダー階層内のSolarisパッチポリシーの場所を指定します。[フォルダーの選択] ウィンドウが開きます。
7. [フォルダーの選択] ウィンドウで、ライブラリ内のフォルダーを選択してSolarisパッチポリシーの場所を指定した後に、[**選択**] をクリックして設定内容を保存します。
8. [可用性] ドロップダウンリストから、Solarisパッチポリシーに対するSAサーバーのライフサイクルの値を選択します。
9. [OS] ドロップダウンリストから、オペレーティングシステムファミリまたはファミリ内の特定のオペレーティングシステムを選択します。

10 変更内容を保存するには、[**ファイル**] メニューの [**保存**] を選択します。

ライブラリーフォルダー別

フォルダー別機能を使用してパッチポリシーを作成するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**フォルダー別**] を選択します。内容ペインにライブラリ内のフォルダー階層が表示されます。

2 Solarisパッチポリシーを保存するフォルダーを選択します。

3 [**アクション**] メニューで、[**新規**] > [**Solarisパッチポリシー**] を選択して、[Solarisパッチポリシー] ウィンドウを開きます。

4 [名前] フィールドに、Solarisパッチポリシーの名前を入力します。

5 (オプション) [説明] フィールドに、ポリシーの用途や内容の説明を入力します。

6 [**参照**] をクリックし、フォルダー階層内のSolarisパッチポリシーの場所を変更します。[フォルダーの選択] ウィンドウが開きます。

7 ライブラリ内のフォルダーを選択してSolarisパッチポリシーの場所を指定し、[**選択**] をクリックします。

8 [可用性] ドロップダウンリストから、Solarisパッチポリシーに対するSAサーバーのライフサイクルの値を選択します。

9 [OS] ドロップダウンリストから、オペレーティングシステムファミリまたはファミリ内の特定のオペレーティングシステムを選択します。

10 [ファイル] メニューから [**保存**] を選択します。

solpatch_import

`solpatch_import`コマンドを使用してSolarisパッチポリシーを作成し、作成したポリシーにパッチを追加することができます。

例A: ベンダー推奨パッチの表示

次のコマンドでは、Solaris 5.8を実行しているすべての管理対象サーバーのすべてのベンダー推奨Solarisパッチを表示します。

```
solpatch_import --action=show --filter=”rec,OS=5.8”
```

例B: ベンダー推奨パッチとセキュリティパッチをポリシーに追加

次のコマンドでは、Solaris 5.8を実行しているすべての管理対象サーバーのすべてのベンダー推奨パッチとセキュリティパッチをダウンロードし、ダウンロードしたパッチをSAライブラリにアップロードして、SAライブラリの`Sol/SolPatches`パッチポリシーに追加します。

```
solpatch_import --action=policy --policy_path=/Sol/Solpatches \
  --filter=”rec,sec,OS=5.8”
```

例C: パッチクラスターをポリシーに追加

次のコマンドでは、`Solaris 10 SPARC Sun Alert Patch Cluster`をダウンロードして、このクラスター内のすべてのパッチを`SolClusterPatches`ポリシーに追加します。クラスターがポリシーに追加されるわけではなく、クラスター内のすべてのパッチがポリシーに追加されます。

```
echo “Solaris 10 SPARC Sun Alert Patch Cluster” | solpatch_import\
  -a policy --policy_path=”/Sol/SolClusterPatches”
```

Solarisパッチポリシーの表示

SAクライアントでは、次のナビゲーション機能を使用してパッチポリシーを表示します。

検索

検索機能を使用してパッチポリシーを表示するには、次の手順を実行します。

1. ナビゲーションペインで [検索] を選択します。
2. ドロップダウンリストで [Solarisパッチポリシー] を選択し、テキストフィールドにポリシー名を入力します。
3.  をクリックして、内容ペインに結果を表示します。
4. 内容ペインでパッチポリシーを選択し、右クリックで [Solarisパッチポリシー] ウィンドウを開きます。

デバイス

デバイス機能を使用してパッチポリシーを表示するには、次の手順を実行します。

1. ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択して、内容ペインにサーバーのリストを表示します。

   または

   ナビゲーションペインで、[**デバイス**] > [**デバイスグループ**] を選択して、内容ペインにデバイスグループのリストを表示します。
2. 内容ペインでサーバーを選択し、右クリックでサーバーエクスプローラーウィンドウを開きます。
3. [ビュー] ペインで、[**管理ポリシー**] > [**パッチポリシー**] を選択して、内容ペインにサーバーにアタッチされているパッチポリシーを表示します。
4. 内容ペインでパッチポリシーを選択し、右クリックで [Solarisパッチポリシー] ウィンドウを開きます。

ライブラリータイプ別

タイプ別機能を使用してパッチポリシーを表示するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] > [**Solaris**] を選択して、内容ペインにSolarisパッチポリシーを表示します。
2. 内容ペインでSolarisパッチポリシーを選択し、右クリックで [Solarisパッチポリシー] ウィンドウを開きます。

ライブラリーフォルダー別

フォルダー別機能を使用してパッチポリシーを表示するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**フォルダー別**] を選択します。内容ペインにライブラリ内のフォルダー階層が表示されます。
2. 内容ペインで、パッチポリシーを含むフォルダーを選択します。
3. 右クリックしてそのフォルダーを開きます。

4 パッチポリシーを選択し、右クリックで [Solarisパッチポリシー] ウィンドウを開きます。

Solarisパッチポリシーの編集

Solarisパッチポリシーの作成後に、Solarisパッチポリシーのプロパティを表示して変更することができます。表示可能なプロパティには、Solarisパッチポリシーを作成したSAユーザー、作成日、SolarisパッチポリシーのSA IDなどがあります。Solarisパッチポリシーの名前、説明、可用性、ライブラリ内の格納場所、Solarisパッチポリシーのオペレーティングシステムは変更 (編集) することもできます。

Solarisパッチポリシーのプロパティを編集するためのアクセス権が必要です。アクセス権の取得については、システム管理者にお問い合わせください。アクセス権の詳細については、『SA 管理ガイド』を参照してください。

パッチポリシーのプロパティを編集するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] > [**Solaris**] を選択します。
2 内容ペインでSolarisパッチポリシーを選択し、右クリックで [Solarisパッチポリシー] ウィンドウを開きます。
3 [ビュー] ペインで、[プロパティ] を選択します。
4 [プロパティ] の内容ペインで、ソフトウェアポリシーの名前、説明、場所、可用性、OSを編集することができます。
5 内容ペインで、Solaris パッチポリシーの名前、説明、場所、ライフサイクル、オペレーティングシステムを編集できます。これらのフィールドの内容に関するガイドラインについては、Solarisパッチポリシーの作成 (124ページ) を参照してください。
6 変更が完了したら、[ファイル] メニューから [保存] を選択します。

パッチポリシーへのSolarisパッチの追加

作成したSolaris パッチポリシーには、Solaris パッチ、パッチクラスター、パッチバンドル、サーバースクリプトを追加できます。これらを追加しても、管理対象サーバー上にインストールされるわけではありません。Solaris パッチポリシーに追加した後に、パッチポリシーを管理対象サーバーにアタッチしてから、サーバーを修復する必要があります。

また、`solpatch_import`コマンドを使用して、パッチポリシー内にパッチを追加することもできます。

Solarisパッチ、Solarisパッチクラスター、サーバースクリプトをSolarisパッチポリシーに追加するためのアクセス権が必要です。アクセス権の取得については、システム管理者にお問い合わせください。アクセス権の詳細については、『SA 管理ガイド』を参照してください。

パッチリソースをパッチポリシーに追加するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] > [**Solaris**] を選択します。
2 内容ペインでSolarisパッチポリシーを選択し、右クリックで [Solarisパッチポリシー] ウィンドウを開きます。
3 [ビュー] ペインで [ポリシーアイテム] を選択します。
4 をクリックするか、[**アクション**] メニューから [**追加**] を選択して、[ライブラリアイテムの選択] ウィンドウを表示します。
5 [タイプの参照] タブを選択して、Solarisパッチポリシーに追加できるアイテムを表示します。
6 ポリシーに追加するアイテムを1つまたは複数選択して、[**選択**] を押します。アイテムがポリシーに追加されます。

または

[フォルダーの参照] タブを選択して、ライブラリ内のフォルダー階層とフォルダーに含まれるアイテムのリストを表示します。ポリシーに追加するアイテムを1つまたは複数選択して、[**選択**] を押します。アイテムがポリシーに追加されます。

7 パッチのインストール順序を変更する場合は、  の矢印を使用します。

8 ポリシーからパッチを除外する場合は、そのパッチを選択して  をクリックします。

9 依存するパッチ、現在不使用のパッチ、優先するパッチ、互換性のないパッチ、取り消し済みのパッチをすべて特定するには、[**アクション**] > [**依存関係の解決**] を選択するか、 

を選択します。

10 [ファイル] メニューから [保存] を選択して、変更内容をポリシーに保存します。

11 ポリシーに変更内容を保存するには、[**ファイル**] メニューの [**保存**] を選択します。

Solarisパッチポリシーからのパッチの削除

Solaris パッチポリシーからパッチやパッチクラスターを削除しても、パッチやパッチクラスターが管理対象サーバーからアンインストールされるわけではありません。このアクションでは、パッチポリシーからパッチまたはパッチクラスターが削除されるだけです。管理対象サーバーから Solaris パッチまたはパッチクラスターをアンインストールするには、管理対象サーバーから Solaris パッチまたはパッチクラスターを直接アンインストールする必要があります。

Solaris パッチまたは Solaris パッチクラスターを Solaris パッチポリシーから削除するためのアクセス権が必要です。アクセス権の取得については、システム管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

Solarisパッチポリシーから Solarisパッチまたはパッチクラスターを削除するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] > [**Solaris**] を選択して、Solaris のバージョンを選択します。

2 内容ペインでSolarisパッチポリシーを選択し、右クリックで [Solarisパッチポリシー] ウィンドウを開きます。

3 [ビュー] ペインで [ポリシーアイテム] を選択します。

4 内容ペインに表示されるポリシーアイテムのリストから削除するアイテムを選択します。

5  をクリックするか、[アクション] メニューから [削除] を選択します。

6 [ファイル] メニューから [保存] を選択して、変更内容をポリシーに保存します。

パッチの依存関係の解決

フィルターオプションを指定して`solpatch_import`コマンドを使用した場合、すべてのパッチの依存関係が解決され、インストール可能なすべてのパッチが特定されます。

パッチをパッチポリシーに手動で追加する場合は、SAでパッチポリシー内のすべてのパッチの依存関係を特定できます。

SAでは、Solarisパッチポリシー内のパッチごとに、次の状況を確認します。

- 特定のパッチよりも優先されるパッチや特定のパッチに代わるパッチで、そのパッチの代わりにインストールする必要のあるパッチ。
- 特定のパッチに先行して必要で前もってインストールしておく必要のあるパッチ。

- 互換性がないため同時にインストールすることができないパッチ。互換性のないパッチは、どちらのパッチをインストールするかを指定する必要があります。
- ベンダーによって取り消し済みのパッチ。
- すべてのパッチの有効なインストール順序 (変更が必要ない限り、ポリシー内の元のパッチのインストール順序が維持されます)。

パッチの依存関係を特定するには、Solarisパッチポリシーにパッチを追加する必要があります。

パッチポリシー内の依存関係のあるパッチを解決するには、次の手順を実行します。

1. [**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] > [**Solaris**] を選択します。
2. SunOSのバージョンを選択してから、パッチポリシーを選択します。
3. Solarisパッチをダブルクリックして、[パッチポリシー] ウィンドウを開きます。
4. [パッチポリシー] ウィンドウの [表示] ペインでポリシーアイテムを選択します。パッチポリシー内のSolarisパッチのリストが表示されます。
5. [パッチポリシー] ウィンドウで、[**アクション**] > [**依存関係の解決**] を選択するか、依存関係の解決(S) をクリックします。このアクションでは、SA内のSolarisパッチデータベースを調べ、すべての依存関係を識別して結果を表示します。これにより、インストールが必要なパッチのリストが表示されます。

例: Solarisパッチの依存関係の解決

図18は、2つのスクリプトと3つのパッチを含むSolarisパッチポリシーを示しています。表示されている順序は、スクリプトを実行する順序とパッチをインストールする順序です。

図18　　Solarisパッチポリシー : 依存関係の解決

図19は、このパッチポリシーで [**依存関係の解決**] を選択したときの結果を示しています。このパッチポリシーには、次の変更が加えられています。

- パッチ105181-25は新規バージョン (105181-39) に置き換えられています。
- パッチ117435-02はポリシー内に残っています。
- パッチ137124-01によってパッチ138170-01が置き換えられています。
- パッチ137124-01が必要とする23個のパッチが追加されています。
- 2つのスクリプトはポリシー内のそれぞれの場所に残っています。

パッチの依存関係の解決は反復的に行われるため、パッチポリシーがどのように変更されたかが容易にわからない場合もあります。

図19　　パッチポリシー内のすべてのパッチの依存関係

[**差異の表示**] をクリックすると、元のパッチポリシーと提示された一連のパッチとの間の差異が詳細に表示されます。[差異の表示] ウィンドウで、[**エクスポート**] をクリックしてポリシー間の差異をファイルに保存します。`solpatch_import`コマンドでこの情報を使用すると、新規のパッチをSAにインポートできます。

カスタム属性

カスタム属性は、パッチポリシー用に作成して設定できる名前付きデータ値です。カスタム属性を使用すると、パッチポリシーに関する追加情報を保存することができます。カスタム属性は、スクリプト、ネットワークおよびサーバー構成、通知、CRONスクリプトの構成など、さまざまな用途で使用できます。パッチポリシーにカスタム属性を設定すると、そのポリシーにアタッチされたすべてのサーバーでカスタム属性が利用できます。カスタム属性の詳細については、『SAユーザーガイド: Server Automation』を参照してください。

カスタム属性のパッチポリシーへの追加

Solarisパッチポリシーに追加したカスタム属性の値は、そのパッチポリシーにアタッチされているサーバーに適用されます。カスタム属性をSolarisパッチポリシーに追加した後に、パッチポリシーを管理対象サーバーにアタッチしてから、サーバーを修復してパッチポリシーを適用する必要があります。

カスタム属性をSolarisパッチポリシーに追加するためのアクセス権が必要です。アクセス権の取得については、SAの管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

カスタム属性をパッチポリシーに追加するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] > [**Solaris**] を選択して、Solarisのバージョンを選択します。
2. 内容ペインで、Solarisパッチポリシーを選択して表示します。[Solarisパッチポリシー] ウィンドウが開きます。
3. [ビュー] ペインで [カスタム属性] を選択します。
4. をクリックするか、[**アクション**] メニューから [**追加...**] を選択します。カスタム属性が「新規属性」という名前で追加されます。
5. カスタム属性の名前を入力して、[Enter] キーを押します。
6. カスタム属性に値を追加するには、[値] 列の下の行をダブルクリックして値を入力するか、をクリックして入力ダイアログで値を入力します。
7. [**ファイル**] メニューから [**保存**] を選択します。

カスタム属性のパッチポリシーからの削除

カスタム属性をパッチポリシーから削除するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] > [**Solaris**] を選択して、Solarisのバージョンを選択します。
2. 内容ペインで、Solarisパッチポリシーを選択して表示します。[Solarisパッチポリシー] ウィンドウが開きます。
3. [ビュー] ペインで [カスタム属性] を選択します。ポリシーで定義されているカスタム属性が表示されます。
4. 内容ペインで、削除するカスタム属性を選択した後に、をクリックするか、[**アクション**] メニューの [**削除**] を選択します。
5. [**ファイル**] メニューから [**保存**] を選択します。

パッチポリシーの履歴の表示

Solarisパッチポリシーに関連付けられたイベントを表示するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] > [**Solaris**] を選択して、Solarisのバージョンを選択します。
2. 内容ペインで、Solarisパッチポリシーを選択します。
3. 右クリックして [Solarisパッチポリシー] ウィンドウを開きます。
4. [ビュー] ペインで [履歴] を選択します。内容ペインに、Solarisパッチポリシーに関連付けられたイベントが表示されます。ポリシーで実行されたアクション、アクションを実行したユーザー、アクションを実行した時刻を表示できます。
5. [表示] ドロップダウンリストから、イベントを表示する期間を選択します。

パッチポリシーに関連するソフトウェアポリシーの表示

ソフトウェアポリシーには、Solaris パッチポリシーを含めることができます。[Solaris パッチポリシー] ウィンドウでは、選択したSolarisパッチポリシーをインストール対象のアイテムの1つとして含むすべてのソフトウェアポリシーを表示できます。

選択したSolarisパッチポリシーを含むソフトウェアポリシーを表示するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] > [**Solaris**] を選択して、Solarisのバージョンを選択します。
2. 内容ペインで、Solarisパッチポリシーを選択します。
3. 右クリックして [Solarisパッチポリシー] ウィンドウを開きます。
4. [ビュー] ペインで [ソフトウェアポリシー] を選択します。内容ペインに、選択した Solaris パッチポリシーをインストール対象のアイテムの1つとして含むソフトウェアポリシーのリストが表示されます。

パッチポリシーに関連するOSシーケンスの表示

[Solarisパッチポリシー] ウィンドウでは、選択したパッチポリシーをインストール対象のアイテムの1つとして含むすべてのOSシーケンスを表示できます。

Solarisパッチポリシーに関連するOSシーケンスを表示するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] > [**Solaris**] を選択して、Solarisのバージョンを選択します。
2. 内容ペインで、Solarisパッチポリシーを選択します。
3. 右クリックして [Solarisパッチポリシー] ウィンドウを開きます。
4. [ビュー] ペインでOSシーケンスを選択します。内容ペインに、選択したパッチポリシーをインストール対象のアイテムの1つとして含むOSシーケンスのリストが表示されます。

パッチポリシーにアタッチされているサーバーの表示

SAクライアントでは、選択したSolarisパッチポリシーがアタッチされているすべてのサーバーおよびデバイスグループのリストを表示できます。

選択したSolarisパッチポリシーがアタッチされているすべてのサーバーのリストを表示するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**ソフトウェアポリシー**] > [**Solaris**] とオペレーティングシステムバージョンを選択します。

2 内容ペインでSolarisパッチポリシーを選択し、右クリックで [Solarisパッチポリシー] ウィンドウを開きます。

3 [ビュー] ペインで、[サーバー] を選択します。内容ペインに、選択したSolarisパッチポリシーがアタッチされているサーバーのリストが表示されます。

フォルダー内のSolarisパッチポリシーの検索

フォルダー階層内のSolarisパッチポリシーを検索するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] > [**Solaris**] を選択して、Solarisのバージョンを選択します。

2 内容ペインで、Solarisパッチポリシーを選択します。

3 右クリックで [**フォルダー内で検索**] を選択して、内容ペインにSolarisパッチポリシーのフォルダー階層を表示します。

パッチ管理のタスク

Solarisのパッチ管理は、次のタスクで構成されます。

- 良性エラーコードの検出 (150ページ)

solpatch_importの実行

マルチマスターメッシュの環境では、solpatch_importコマンドを複数のコアシステムで同時に実行しないでください。このような操作を行うと、データが失われる可能性があります。コアサーバーでsolpatch_importを実行する場合は、コマンドを1つずつ実行するようにしてください。

Solarisパッチ管理の一部のタスクでは、solpatch_importコマンドを使用します。solpatch_importコマンドを実行するには、次のアクセス権が必要です。

表11 solpatch_importの使用に必要なアクセス権

アクセス権のタイプ	アクセス権の設定
SAライブラリのフォルダー /Opsware, /Opsware/Toolsおよび/Opsware/Tools/Solaris Patchingに対するアクセス権	これらのフォルダーに対する完全なアクセス権が必要です。SAでSolarisパッチ情報が格納される場所です。
「パッチの管理」機能のアクセス権	「読み取り/書き込み」のアクセス権が必要です。
「パッチのインストールの許可」機能のアクセス権	「はい」に設定する必要があります。
「パッチのアンインストールの許可」機能のアクセス権	「はい」に設定する必要があります。
「パッチコンプライアンスルールの管理」機能のアクセス権	「はい」に設定する必要があります。

フォルダーのアクセス権とSolarisパッチのアクセス権の詳細については、『SA 管理ガイド』を参照してください。

solpatch_importコマンドを使用するには、SAコアサーバーにrootとしてログインする必要があります。

コマンドを実行するには、ソフトウェアリポジトリコンポーネント (スライスコンポーネントバンドルの一部) を実行しているコアサーバーにログインして、rootとして、次のディレクトリにあるsolpatch_importコマンドを実行します。

```
/opt/opsware/solpatch_import/bin/
```

次のオプションを指定してコマンドを実行すると、solpatch_importの詳細なドキュメントを参照できます。

```
solpatch_import --manual
```

Solarisパッチデータベースの初期化

Oracleからパッチおよびパッチデータをダウンロードするには、事前にSAでSolarisパッチデータベースのセットアップと初期化を行う必要があります。

Solarisパッチデータベースのセットアップと初期化を行うには、次の手順を実行します。

1 solpatch_importコマンドで使用する情報を指定する構成ファイルを作成します。

このファイルのデフォルトパスは/etc/opt/opsware/solpatch_import/solpatch_import.confです。

デフォルトパスを使用しない場合は、-cまたは--confオプションを使用する必要があります。デフォルトパスを使用する場合、-cまたは--confオプションを使用する必要はありません。

この構成ファイルの内容の詳細については、`solpatch_import --manual`を実行して`solpatch_import`のmanページを参照してください。次の例は、構成ファイルの内容の一部です。

```
[main]
hpsa_user=<SAユーザー名>
hpsa_pass=<SAユーザーパスワード>
download_user=<My Oracleアカウントのユーザー名>
download_pass=<My Oracleアカウントのパスワード>
```

2 次のコマンドを実行して、SAのSolarisパッチ情報を初期化します。

```
solpatch_import -a create_db
```

このコマンドは、patchdiag.xrefファイルをOracleからダウンロードし (すでにダウンロード済みの場合はこのファイルのローカルコピーを指定可)、パッチ情報を調べて、SA内にデータを格納します。

SAのSolarisパッチ情報を初期化するため、`-a create_db`オプションを1回だけ使用する必要があります。

3 Solaris パッチデータベースに最新のパッチが含まれていることを確認します。詳細については、Solaris パッチデータベースの管理 (135ページ) を参照してください。

Solarisパッチデータベースの管理

Solaris パッチデータベースに最新のパッチ情報が含まれていることを確認するには、次のタスクを実行します。

- Oracleからの最新のパッチデータの取得
- Solarisパッチの補足データファイルの取得
- Solarisパッチの補足データファイルの手動ダウンロード

ベストプラクティス: どの方法を使用する場合でも、定期的に更新を確認して、SAパッチデータベースにインストールすることをお勧めします。

Oracleからの最新のパッチデータの取得

通常、Oracle のパッチ情報は月曜から金曜までの毎日更新されます。Oracle から最新の Solaris パッチ情報 (`patchdiag.xref`ファイル) を入手して、SAパッチデータベースにアップロードするには、各社のポリシーに基づいて、次のコマンドを定期的に実行します。たとえば、cron ジョブで次のコマンドを指定することができます。

```
solpatch_import -a update_db
```

Solarisパッチの補足データファイルの取得

SAでは、Oracleから (patchdiag.xrefファイルから) Solarisパッチに関する情報を取得します。ただし、SAでは、Solaris パッチに関する有用な補足データが利用できます。これは、HP Live Network から自動的に取得できます。この補足データが更新されたときに、SAのSolarisパッチデータベースに自動的にアップロードされるように、HP Live Networkを構成することができます。

データが更新されたときに補足データファイルを取得してSAライブラリにアップロードするには、次の手順を実行します。

1 次のURLでHP Passport IDを取得します。

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

2 HP Passportの資格情報を使用して、HP Live Networkポータルにログインします。

https://hpln.hp.com/group/hp-live-network-connector

3 HP Live Networkコネクター(LNc)は、SAのソフトウェアリポジトリコンポーネントがインストールされたコアサーバーにインストールされます。

『HP Live Network Connector User Guide』は、次のURLにあるHP Live NetworkのLive Networkコネクターコミュニティからダウンロードできます。

https://hpln.hp.com/group/hp-live-network-connector

[**Resources**] タブをクリックして、[**Documentation**] フォルダーを開きます。

4 LNcがインストールされたシステムで、次のコマンドを実行して、Solarisパッチ適用サービスを有効にします。

```
live-network-connector write-config --setting=content.solaris_patching=1
```

5 (オプション) Solarisパッチ適用サービスを無効にするには、次のように値を0にして、同じコマンドを実行します。

```
live-network-connector write-config --setting=content.solaris_patching=0
```

または、Solarisパッチの補足データファイルをHP Live Networkから手動でダウンロードして、SAデータベースにアップロードすることもできます。詳細については、Solarisパッチの補足データファイルの手動ダウンロード (136ページ) を参照してください。

Solarisパッチの補足データファイルの手動ダウンロード

ここでは、Solarisパッチの補足データファイルをHP Live Networkから手動でダウンロードして、SAのパッチデータベースにアップロードする手順について説明します。Solarisパッチの補足データファイルの取得 (135ページ) の手順に従って、このファイルが変更されたときに自動的にアップロードされるようにLNcをセットアップすることをお勧めします。ただし、ファイルを手動でダウンロードする場合は、定期的に更新を確認し、ここに記載した手順に従って、SAパッチデータベースにインストールするようにしてください。

補足データファイルを取得するには、次の手順を実行します。

1 次のURLでHP Passport IDを取得します。

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

2 HP Passportの資格情報を使用して、HP Live Networkポータルにログインします。

https://hpln.hp.com/group/hp-live-network-connector

3 HP Live Networkコネクター(LNc)は、SAのソフトウェアリポジトリコンポーネントがインストールされたコアサーバーにインストールされます。

『HP Live Network Connector User Guide』は、次のURLにあるHP Live NetworkのLive Networkコネクターコミュニティからダウンロードできます。

https://hpln.hp.com/group/hp-live-network-connector

[**Resources**] タブをクリックして、[**Documentation**] フォルダーを開きます。

4 HP Live Networkメニューで [Content Catalog] をクリックし、Server Automation製品の「Solaris Patching for Server Automation」を検索します。

5 `solpatchdb_supplement.zip`という名前の最新のSolarisパッチパッケージをダウンロードして、コアスライスサーバーの一時ディレクトリ (/tmpなど) に保存します。

6 `solpatchdb_supplement.zip`ファイルを解凍します。

7 `solpatchdb_supplement.zip`ファイルから解凍したファイル`install.sh`を実行します。これにより、Solarisパッチの補足データがSAパッチデータベースにアップロードされます。

8 HPではSolarisパッチの補足データファイルを更新します。そのため、このファイルの更新状況を定期的にチェックして、ファイルが更新されている場合は、次の手順を再度実行して最新の補足パッチデータをSAのパッチデータベースにダウンロードすることをお勧めします。

Solarisパッチの検索

SAでは、Solarisサーバーに必要なパッチをすばやく簡単に特定することができます。

`solpatch_import`コマンドを使用すると、次の操作を実行できます。

- Solarisサーバーに必要なSolarisパッチを表示します。すべての依存パッチも表示され、正しいインストール順序でパッチが表示されます。
- これらのパッチをダウンロードして、SAライブラリにインポートできます。
- これらのパッチをSolarisパッチポリシーに追加できます。

次の表に、パッチ情報の表示、パッチのダウンロード、SAライブラリへのインポート、Solarisパッチポリシーへの追加を行うための、`solpatch_import`コマンドのオプションを示します。

表12 solpatch_importコマンドのアクションの指定

solpatch_importコマンドのオプション	説明

`-a show`
または
`--action show`
	指定したパッチに関する情報を表示します。

`-a import`
または
`--action import`
	指定したパッチをダウンロードして、SAライブラリにインポートします。

`-a policy`
または
`--action policy`
	指定したパッチをダウンロードし、SAライブラリにインポートして、指定したSolarisパッチポリシーに追加します。このアクションでは、`--policy_path`オプションを使用してSolarisパッチポリシーを指定する必要があります。

`solpatch_import`コマンドでは、管理対象サーバーに適用可能なすべてのパッチが検索されます。適用不可能なパッチは除外されます。たとえば、特定のソフトウェアアプリケーションや依存するパッチがインストールされていない場合、SAは特定のパッチを適用不可能とみなします。検索結果には適用可能なすべてのパッチが必要なインストール順序で表示されます。

表13に、必要なSolarisパッチを指定するsolpatch_importコマンドのフィルターを示します。

表13　　solpatch_importのフィルターオプションを使用した目的のパッチの指定

目的のパッチ	使用するフィルターオプション	フィルターオプションの例	フィルターオプションの例の説明
特定のサーバーに対してOracleが推奨するすべてのパッチ	rec server	-f “rec,server=sys01.hp.com”	管理対象サーバー sys01.hp.comに対してOracleが推奨するすべてのパッチを指定します。
一連のサーバーに対してOracleが推奨するすべてのパッチ	rec platform	-f “rec,OS=5.10”	Solaris 5.10 を実行しているすべての管理対象サーバーに対してOracle が推奨するすべてのパッチを指定します。
特定のサーバーに対するすべてのOracleセキュリティパッチ	sec server	-f “sec, server=sys01.hp.com”	管理対象サーバー sys01.hp.comに対するすべての Oracle セキュリティパッチを指定します。
一連のサーバーに対するすべてのOracleセキュリティパッチ	sec OS	-f “sec, OS=5.9”	Solaris 5.9 を実行しているすべての管理対象サーバーに対するすべてのOracle セキュリティパッチを指定します。
サーバーに対するすべてのOracleセキュリティパッチとすべてのOracle推奨パッチ	rec sec server	-f “rec, sec, OS=5.8”	Solaris 5.8 を実行しているすべての管理対象サーバーに対するすべてのOracle セキュリティパッチとOracle推奨パッチを指定します。

以下の例では、solpatch_importコマンドを使用してSolarisサーバーに必要なパッチを特定する方法について説明します。

- 選択したサーバーで必要なすべてのパッチの検索 (138ページ)
- サーバーに対するOracle推奨パッチの検索 (139ページ)
- サーバーに対するOracleセキュリティパッチの検索 (139ページ)
- 特定のパッチの検索 (139ページ)

詳細については、solpatch_importの実行 (134ページ) の手順でsolpatch_import --manualを実行してください。

選択したサーバーで必要なすべてのパッチの検索

次のサンプルコマンドでは、「sys01.hp.com」という名前のサーバーで必要なすべてのパッチを検索します。最初のコマンドでは、パッチのリストを表示します。2つ目のコマンドでは、パッチをダウンロードしてSAライブラリに格納します。3つ目のコマンドでは、これらのパッチを「SolPatches/MyPolicy」という名前のSolarisパッチポリシーに追加します。

```
solpatch_import --action=show --filter=”server=sys01.hp.com”
solpatch_import --action=import --filter=”server=sys01.hp.com”
solpatch_import --action=policy --policy_path=”SolPatches/MyPolicy”\
   --filter=”server=sys01.hp.com”
```

サーバーに対するOracle推奨パッチの検索

次のサンプルコマンドでは、Solaris 10を実行しているすべての管理対象サーバーのOracle推奨パッチを検索します。最初のコマンドでは、パッチのリストを表示します。2つ目のコマンドでは、パッチをダウンロードしてSAライブラリに格納します。3つ目のコマンドでは、これらのパッチを「MySolPolicy」という名前のSolarisパッチポリシーに追加します。

```
solpatch_import --action=show --filter="rec,OS=5.10"
solpatch_import --action=import --filter="rec,OS=5.10"
solpatch_import --action=policy --policy_path="MySolPolicy\"
   --filter="rec,OS=5.10"
```

サーバーに対するOracleセキュリティパッチの検索

次のサンプルコマンドでは、Solaris 9を実行しているすべての管理対象サーバーのOracleセキュリティパッチを表示します。

```
solpatch_import --action=show --filter="sec,OS=5.9"
```

特定のパッチの検索

テキストファイルでsolpatch_importコマンドに対してパッチ名を指定すると、1つまたは複数のパッチに関する情報を表示できます。この例では、ファイルmy_sol_patches.txtに次の行が記載されているものとします。

```
120900-04 121133-02 119254-67
119317-01 121296-01 127884-01
```

次のコマンドでは、ファイルmy_sol_patches.txtに記載された一連のパッチを表示します。

```
solpatch_import --action=show my_sol_patches.txt
```

次のコマンドでは、ファイルmy_sol_patches.txtに記載された一連のパッチをダウンロードして、SAライブラリに格納します。

```
solpatch_import --action=import my_sol_patches.txt
```

次のコマンドでは、ファイルmy_sol_patches.txtに記載された一連のパッチをダウンロードし、SAライブラリに格納して、「/SolPatches/SolPatchPolicy」という名前のSolarisパッチポリシーに追加します。

```
solpatch_import --action=policy --policy_path=/SolPatches/SolPatchPolicy \
  my_sol_patches.txt
```

solpatch_importの詳細については、solpatch_importの実行 (134ページ) を参照してください。

パッチまたはパッチクラスターのインポート

solpatch_importコマンドを使用するか、SAクライアントを使用して、パッチまたはパッチクラスターをインポートすることができます。

solpatch_import

ベストプラクティス:HPでは、solpatch_importコマンドを使用して、OracleからSolarisパッチまたはパッチクラスターをインポートすることを推奨しています。

solpatch_importコマンドを使用すると、Solarisパッチやパッチクラスターを Oracle から自動的にダウンロードして、SAにインポートし、Solarisパッチポリシーに追加して、パッチポリシーをSAライブラリ内のフォルダーに保存できます。solpatch_importコマンドでは、再起動設定やパッチの依存関係をダウンロードして、パッチとともに保存することもできます。

SAクライアントでのインポート

また、SAクライアントを使用してSolarisパッチをインポートすることもできます。

SolarisパッチはOracleからダウンロードされて、SAに保存されます。

パッチがインポートされたかどうかを確認するには、SAクライアントでパッチの可用性プロパティを表示します。インポートしたパッチの可用性プロパティは、表14のいずれかの値に設定できます。

表14　　パッチの可用性プロパティの設定

パッチの可用性の設定	説明
利用可能	パッチはSAにインポートおよびテスト済みであり、管理対象サーバーにインストール可能な状態です。
制限付き	パッチはSAにインポートされていますが、インストールにはアクセス権 (パッチの管理: 読み取り/書き込み) の追加が必要です。これは、パッチの可用性のデフォルト設定です。アクセス権の詳細については、『SA 管理ガイド』を参照してください。
非推奨	パッチをパッチポリシーに追加できませんが、インストールすることはできます。
未インポート	パッチはSAライブラリに格納されていません。

Solarisパッチまたはパッチクラスターをインポートするためのアクセス権が必要です。アクセス権の取得については、SAの管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

ファイルからSAにSolarisパッチまたはパッチクラスターをインポートするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。パッチはオペレーティングシステム別に構成されます。
2. [**アクション**] メニューで、[**ソフトウェアのインポート**] を選択して、[ソフトウェアのインポート] ウィンドウを開きます。
3. [**参照**] をクリックして、インポートするパッチまたはパッチクラスターを選択します。

   [開く] ウィンドウで [**開く**] をクリックする前に、[エンコード] ドロップダウンリストからパッチまたはパッチクラスターで使用する文字エンコードを選択します。

   SAでパッチまたはパッチクラスターに含まれるメタデータを抽出して、[パッチのプロパティ] ウィンドウなど、SAクライアントで非ASCII文字の情報を正しく表示できるように、文字エンコードを指定する必要があります。パッチのメタデータには、コメント、リリースノート、スクリプト、説明、内容リストが含まれます。
4. [**開く**] をクリックします。
5. [ソフトウェアのインポート] ウィンドウで、[タイプ] ドロップダウンリストから、Solarisパッチまたは Solarisパッチクラスターを選択します。

   このアクションでは、[フォルダー] 編集フィールドは薄いグレーで表示されます。これは、Solarisパッチおよびパッチクラスターがフォルダーに保存されていないためです。
6. [プラットフォーム] ドロップダウンリストから、適用可能なSolarisオペレーティングシステムを選択します。

7 [**インポート**] をクリックして、Solarisパッチまたはパッチクラスターを SAにインポートします。

8 次のコマンドを実行して、SAのSolarisパッチ情報を更新します。

```
solpatch_import -a update_db
```

パッチまたはパッチクラスターのエクスポート

Solaris パッチまたはパッチクラスターをローカルコンピューターにエクスポートして、テストまたはステージング用マシンでパッチまたはパッチクラスターのインストールをチェックすることができます。

パッチまたはパッチクラスターをローカルドライブにエクスポートするには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。内容ペインでは、パッチはオペレーティングシステム別に構成されます。目的のオペレーティングシステムバージョンに移動します。

2 内容ペインで、エクスポートするパッチまたはパッチクラスターを選択します。

3 右クリックまたは [**アクション**] メニューから、[**エクスポート**] を選択して、[パッチのエクスポート] ウィンドウを開きます。

4 パッケージのエクスポート先を指定します。

5 [**エクスポート**] をクリックします。

Solarisパッチを開く

SAクライアントでは、次のナビゲーション機能を使用してSolarisパッチを開きます。

- 検索 (141ページ)
- ライブラリ—タイプ別 (141ページ)

検索

1 ナビゲーションペインで [検索] を選択します。

2 ドロップダウンリストから [パッチ] を選択して、テキストフィールドにSolarisパッチまたはパッチクラスターの名前を入力します。

3  を選択します。検索結果が内容ペインに表示されます。

4 内容ペインで、パッチまたはパッチクラスターを選択します。

5 [**アクション**] メニューで、[**開く**] を選択して [パッチ] または [パッチクラスター] ウィンドウを開きます。

ライブラリータイプ別

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。内容ペインにパッチが表示されます。

2 内容ペインで、パッチまたはパッチクラスターを選択します。

3 [**アクション**] メニューで、[**開く**] を選択して [パッチ] または [パッチクラスター] ウィンドウを開きます。

プロパティの管理

Solarisパッチ、パッチクラスター、またはパッチバンドルのプロパティを表示するには、次の手順を実行します。

1 ナビゲーションペインで、**[ライブラリ]** > **[タイプ別]** > **[パッチ]** を選択します。内容ペインでは、パッチはオペレーティングシステム別に構成されます。目的のOSバージョンに移動します。

2 内容ペインで、表示するSolarisパッチ、パッチクラスター、またはパッチバンドルを選択します。

3 右クリックして **[開く]** を選択し、[パッチ] ウィンドウを表示します。

4 [ビュー] ペインで、図20に示すように、[プロパティ] を選択してパッチのプロパティを表示します。

図20 パッチのプロパティウィンドウ

一般プロパティ

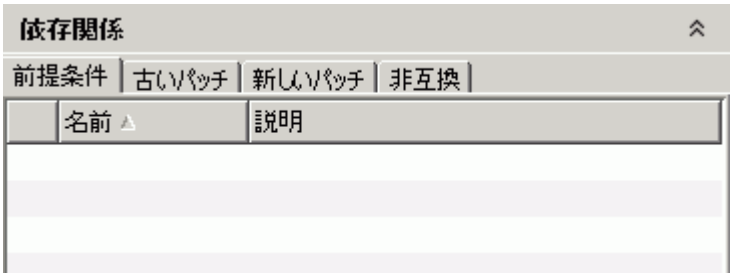
名前: Oracleで定義されたパッチ、パッチクラスター、またはパッチバンドルの名前。

- **説明**: パッチ、クラスター、またはバンドルの内容の説明。
- **バージョン**: Oracleで定義されたバージョン番号。
- **ステータス**: Oracleで定義されたステータス。
- **リリースノートのURL**: パッチに関するドキュメントへのリンク。この情報を表示するには、My Oracleの資格情報を提示する必要があります。
- **タイプ**: アイテムがパッチ、パッチクラスター、またはパッチバンドルのいずれであるかを指定します。
- **OS**: パッチ、クラスター、またはバンドルに関連するオペレーティングシステム。
- **可用性**: SAユーザーに対するパッチの可用性。制限付き、利用可能、または非推奨に設定できます。
- **最終更新日時**: パッチの最終更新日時とパッチを最後に更新したSAユーザー。
- **作成日時**: SAユーザーがパッチまたはパッチクラスターを作成した日時。
- **ファイル名**: パッケージのファイル名。
- **ファイルサイズ**: パッケージのファイルサイズ。
- **オブジェクトID**: パッケージを一意に識別するSA ID。

依存関係

図21は、パッチのプロパティウィンドウのパッチの依存関係を示しています。

図21　　パッチの依存関係



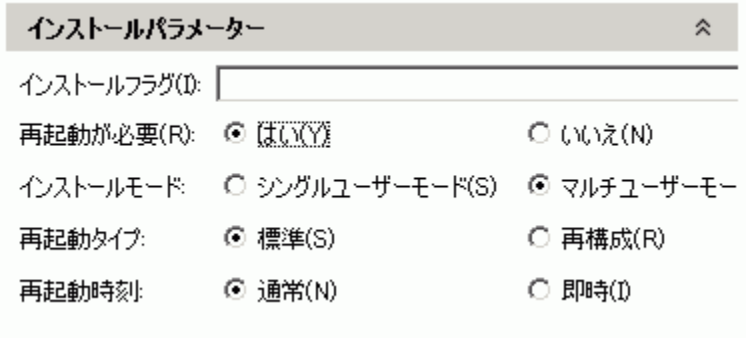
- **前提条件**: このパッチをインストールする前にインストールする必要があるパッチ。
- **古いパッチ**: このパッチよりも古いパッチ。
- **新しいパッチ**: このパッチよりも新しいパッチ。
- **非互換**: このパッチでインストールできないパッチ。

インストールパラメーター

図22は、パッチ用の実際の設定とパッチ用にOracleが指定している設定を表しています。ラジオボタンで選択された設定は、パッチのインストール時に実際に使用される設定です。Oracleが推奨する設定には、「Oracleデフォルト」と表示されます。Oracleデフォルト設定は、パッチとともにダウンロードされた値です。

ラジオボタンで選択された設定は、パッチのインストール時に使用されます。ただし、これらの設定は、パッチポリシーに基づいてサーバーを修復する際やパッチをインストールする際にオーバーライドできます。詳細については、再起動オプション (153ページ) を参照してください。

図22 パッチのプロパティウィンドウのインストールパラメーター



- **インストールフラグ**: (オプション) 管理対象サーバーでのパッチまたはパッチクラスターのインストール時に使用される引数。
- **再起動が必要**: パッチまたはパッチクラスターのインストール完了時に管理対象サーバーを再起動するかどうかを指定します。Oracleが推奨する設定には、「Oracleデフォルト」と表示されます。
- **インストールモード**: パッチまたはパッチクラスターをシングルユーザーモードまたはマルチユーザーモードのどちらでインストールするかを指定します。Oracleが推奨する設定には、「Oracleデフォルト」と表示されます。Solarisシステムは再起動してシングルユーザーモードになり、パッチをインストールした後に、システムが再起動してマルチユーザーモードになります。
- **再起動タイプ**: パッチまたはパッチクラスターのインストール後に再起動を標準または再構成のいずれで実行するかを指定します。Oracleが推奨する設定には、「Oracleデフォルト」と表示されます。
- **再起動時刻**: パッチまたはパッチクラスターのインストール後に、サーバーの再起動をすぐに実行するか、後で実行するかを指定します。Oracleが推奨する設定には、「Oracleデフォルト」と表示されます。

  再起動時刻: 通常の設定を使用してパッチをインストールする場合、ジョブ内の別のパッチでジョブ終了前の即時再起動が要求される場合を除き、ジョブの終了時に再起動が実行されます。ただし、ジョブのプレビューや[ジョブステータス]ウィンドウには、パッチに関する**インストールと再起動**のメッセージが表示されます。この場合、パッチのインストール後すぐではなく、パッチのインストール後のいずれかの時点で再起動が実行されます。

インストールスクリプト

- **インストール前スクリプト**: パッチまたはパッチクラスターのインストール前に管理対象サーバーで実行する必要のあるスクリプト。
- **インストール後スクリプト**: パッチまたはパッチクラスターのインストール後に管理対象サーバーで実行する必要のあるスクリプト。
- **スクリプトがエラーを返した場合**: スクリプトが失敗した場合にパッチまたはパッチクラスターのインストールを停止するかどうかを指定します。

アンインストールパラメーター

- **アンインストールフラグ**: (オプション) 管理対象サーバーでのパッチまたはパッチクラスターのアンインストール時に使用される引数。
- **再起動が必要**: パッチまたはパッチクラスターのアンインストール完了時に管理対象サーバーを再起動するかどうかを指定します。Oracleが推奨する設定には、「Oracleデフォルト」と表示されます。

- **アンインストールモード**: パッチまたはパッチクラスターをシングルユーザーモードまたはマルチユーザーモードのどちらでアンインストールするかを指定します。Oracleが推奨する設定には、「Oracleデフォルト」と表示されます。Solarisシステムは再起動してシングルユーザーモードになり、パッチのアンインストール後に再起動してマルチユーザーモードになります(インストールモードに関する関連情報については、パッチのインストールのトラブルシューティング (154ページ)を参照してください)。
- **再起動タイプ**: パッチまたはパッチクラスターのアンインストール後に再起動を標準または再構成のいずれで実行するかを指定します。Oracleが推奨する設定には、「Oracleデフォルト」と表示されます。
- **再起動時刻**: パッチまたはパッチクラスターのアンインストール後に、サーバーの再起動をすぐに実行するか、後で実行するかを指定します。Oracleが推奨する設定には、「Oracleデフォルト」と表示されます。

アンインストールスクリプト

- **アンインストール前スクリプト**: パッチまたはパッチクラスターのアンインストール前に管理対象サーバーで実行する必要のあるスクリプト。
- **アンインストール後スクリプト**: パッチまたはパッチクラスターのアンインストール後に管理対象サーバーで実行する必要のあるスクリプト。
- **スクリプトがエラーを返した場合**: スクリプトが失敗した場合にパッチまたはパッチクラスターのアンインストールを停止するかどうかを指定します。

プロパティの編集

新規のSolarisパッチ、パッチクラスター、またはパッチバンドルのアップロード後、または既存のパッチ、パッチクラスター、またはパッチバンドルの選択後に、SAクライアントで各種プロパティの追加や編集を行うことができます。

パッチまたはパッチクラスターのプロパティを編集するためのアクセス権が必要です。アクセス権の取得については、SAの管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

Solarisパッチ、パッチクラスター、またはパッチバンドルのプロパティを編集するには、次の手順を実行します。

1. [パッチ]ウィンドウで、パッチを選択します。
2. 右クリックしてパッチのプロパティを開きます。
3. SAクライアントで編集可能なプロパティを編集します。

ベンダーのリリースノートの表示

SAクライアントでは、ダウンロードしたパッチ、クラスター、またはバンドルで提供されるURLを使用して、Oracleから提供されるパッチ情報にアクセスできます。

リリースノートを表示するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**]を選択します。パッチはオペレーティングシステム別に構成されます。OSバージョンに移動します。
2. 内容ペインで、表示するSolarisパッチ、パッチクラスター、またはパッチバンドルを選択します。
3. [**アクション**]メニューから[**開く**]を選択します。パッチ情報ウィンドウが表示されます。
4. [ビュー]ペインで、[プロパティ]を選択します。パッチ情報へのURLリンクを含むパッチに関する情報が表示されます。
5. リリースノートのURLを選択し、My Oracleの資格情報を入力してベンダーの情報を表示します。

カスタムドキュメントのインポート

SAクライアントを使用して、Solarisパッチまたはパッチクラスターのカスタムドキュメントをインポートするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。パッチはオペレーティングシステム別に構成されます。目的のOSバージョンに移動します。
2. 内容ペインで、表示するSolarisパッチまたはパッチクラスターを選択します。
3. 右クリックして [**開く**] を選択します。[パッチ] または [パッチクラスター] ウィンドウが表示されます。
4. [ビュー] ペインで [カスタムドキュメント] を選択します。内容ペインに、パッチまたはパッチクラスターに関するカスタムドキュメントの内容が表示されます。
5. [**アクション**] メニューから [**インポート**] を選択します。[カスタムドキュメントのインポート] ウィンドウが開きます。
6. [カスタムドキュメントのインポート] ウィンドウで、テキストファイルを確認してエンコードを指定します。
7. [**インポート**] をクリックします。

パッチとパッチクラスター

SAクライアントでは、次の機能を利用して、Solarisパッチおよびパッチクラスターを管理できます。

- パッチクラスターの内容の表示 (146ページ)
- パッチに関連するパッチクラスターの表示 (146ページ)
- パッチまたはパッチクラスターに関連するソフトウェアポリシーの表示 (147ページ)
- パッチまたはパッチクラスターに関連するパッチポリシーの表示 (147ページ)
- パッチまたはパッチクラスターに関連するサーバーの表示 (147ページ)
- パッチまたはパッチクラスターの削除 (148ページ)

パッチクラスターの内容の表示

Solarisパッチクラスターの内容を表示するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。内容ペインでは、パッチはオペレーティングシステム別に構成されます。目的のOSバージョンに移動します。
2. 内容ペインで、Solarisパッチクラスターを選択します。
3. [**アクション**] メニューから [**開く**] を選択します。[パッチクラスター] ウィンドウが表示されます。
4. [ビュー] ペインで、[内容] を選択します。パッチクラスターに含まれるパッチのリストが内容ペインに表示されます。
5. 内容ペインでパッチを選択します。
6. [**アクション**] メニューで、[開く] を選択してパッチのプロパティを表示します。

パッチに関連するパッチクラスターの表示

Solarisパッチを含むパッチクラスターを表示するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。内容ペインでは、パッチはオペレーティングシステム別に構成されます。目的のOSバージョンに移動します。
2. 内容ペインで、Solarisパッチを選択します。

3 [**アクション**] メニューから [**開く**] を選択します。[パッチ] ウィンドウが表示されます。

4 [ビュー] ペインで [パッチクラスター] を選択します。パッチを含むパッチクラスターのリストが内容ペインに表示されます。

5 内容ペインでパッチクラスターを選択し、[アクション] メニューから [開く] を選択してパッチクラスターのプロパティを表示します。

パッチまたはパッチクラスターに関連するソフトウェアポリシーの表示

Solarisパッチまたはパッチクラスターを含むソフトウェアポリシーを表示するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。内容ペインでは、パッチはオペレーティングシステム別に構成されます。目的のOSバージョンに移動します。

2 内容ペインで、Solarisパッチまたはパッチクラスターを選択します。

3 [**アクション**] メニューから [**開く**] を選択します。[パッチ] または [パッチクラスター] ウィンドウが表示されます。

4 [ビュー] ペインで [ソフトウェアポリシー] を選択します。内容ペインに、ポリシーアイテムの1つとしてパッチまたはパッチクラスターを含むソフトウェアポリシーのリストが表示されます。

5 内容ペインでソフトウェアポリシーを選択し、[**アクション**] メニューから [開く] を選択してソフトウェアポリシーのプロパティを表示します。

パッチまたはパッチクラスターに関連するパッチポリシーの表示

Solarisパッチまたはパッチクラスターを含むパッチポリシーを表示するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。内容ペインでは、パッチはオペレーティングシステム別に構成されます。目的のOSバージョンに移動します。

2 内容ペインで、Solarisパッチを選択します。

3 [**アクション**] メニューから [**開く**] を選択します。[パッチ] または [パッチクラスター] ウィンドウが表示されます。

4 [ビュー] ペインで [パッチポリシー] を選択します。内容ペインに、ポリシーアイテムの1つとしてパッチまたはパッチクラスターを含むパッチポリシーのリストが表示されます。

5 内容ペインでソフトウェアポリシーを選択し、[**アクション**] メニューから [開く] を選択してパッチポリシーのプロパティを表示します。

パッチまたはパッチクラスターに関連するサーバーの表示

SAでSolarisパッチまたはパッチクラスターがインストールされたサーバーを表示するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。内容ペインでは、パッチはオペレーティングシステム別に構成されます。目的のOSバージョンに移動します。

2 内容ペインで、Solarisパッチを選択します。

3 [**アクション**] メニューから [**開く**] を選択します。[パッチ] または [パッチクラスター] ウィンドウが表示されます。

4 [ビュー] ペインで、[サーバー] を選択します。内容ペインに、パッチまたはパッチクラスターがインストールされたサーバーのリストが表示されます。

5 内容ペインでサーバーを選択し、[**アクション**] メニューから [開く] を選択してサーバーのプロパティを表示します。

パッチまたはパッチクラスターの削除

Solarisパッチまたはパッチクラスターを削除すると、SAからは削除されますが、管理対象サーバーからアンインストールされるわけではありません。パッチポリシーまたはソフトウェアポリシーにアタッチされている場合、パッチやパッチクラスターを削除することはできません。

パッチまたはパッチクラスターを削除するためのアクセス権が必要です。アクセス権の取得については、SAの管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

Solarisパッチまたはパッチクラスターを削除するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。内容ペインでは、パッチはオペレーティングシステム別に構成されます。目的のOSバージョンに移動します。
2. 内容ペインで、削除するパッチまたはパッチクラスターを選択します。
3. [**アクション**] メニューから [**削除**] を選択します。

Solarisゾーン

SAクライアントでは、次の機能を利用して、Solarisゾーンを管理できます。

- Solarisゾーンへのパッチの適用 (148ページ)
- Solarisゾーンの表示 (148ページ)

Solarisゾーンへのパッチの適用

SA の仮想サーバーの管理では、監査、修復、アプリケーション構成、ソフトウェア管理、パッチ管理など、物理サーバーと同様の操作を仮想サーバー上で行うことができます。

Solaris グローバルゾーンおよび非グローバルゾーンでパッチをインストールするには、Solaris パッチポリシーを使用するか、仮想サーバー上にパッチを直接インストールします。SA クライアントでは、管理対象サーバーのリストまたは仮想サーバーのリストからSolarisゾーンを表示できます。

Solarisゾーンの表示

Solarisゾーンを表示するには、次の手順を実行します。

1. ナビゲーションペインで [デバイス] を選択します。
2. [サーバー] を展開します。
3. [仮想サーバー] を選択して、内容ペインに仮想サーバーのリストを表示します。

   または

   [管理対象サーバー] を選択します。[すべての管理対象サーバー] でサーバーがハイパーバイザーか仮想サーバーかを識別するには、列セレクターで [仮想化] を選択します。
4. [表示] ドロップダウンリストで、[仮想化] を選択して仮想サーバーの構成プロパティを表示します。

パッチのインストール

Solarisパッチは管理対象サーバーに直接インストールすることも、デバイスグループのすべてのサーバーにインストールすることもできます。また、Solarisパッチを Solarisパッチポリシー(またはソフトウェアポリシー)に追加し、そのポリシーを管理対象サーバーまたはデバイスグループにアタッチして、ポリシーに基づいてサーバーを修復することもできます。サーバーまたはデバイスグループを修復すると、アタッチされているポリシーで指定されたSolarisパッチが管理対象サーバーにインストールされます。

SAでは、次の方法でSolarisパッチを管理対象サーバー上にインストールできます。

- [パッチのインストール]ウィザードを使用して、Solarisパッチを管理対象サーバーに直接インストールします。
- [ソフトウェアのインストール]ウィザードを使用して、Solarisパッチを管理対象サーバーに直接インストールします。
- Solarisパッチポリシーを使用して、Solarisパッチまたはパッチクラスターを管理対象サーバーにインストールします。
- ソフトウェアポリシーを使用して、Solarisパッチまたはパッチクラスターを管理対象サーバーにインストールします。

SAを使用してSolarisパッチをインストールまたは削除する場合は、ソフトウェア登録とコンプライアンススキャンを実行して、SAの管理対象サーバーに関する情報を最新の状態にする必要があります。詳細については、パッチコンプライアンス (121ページ) を参照してください。

パッチクラスターのインストール

Solarisパッチクラスターをインストールする際には、事前に各クラスターのリリースノートファイルを確認してください。SAでは、パスコードが必要なクラスターで、リリースノートファイルにあるパスコードの手動での入力を要求しません。

SAでは、パスコードが必要なクラスターを含む、すべてのSolarisパッチクラスターをインストールできます。一部のクラスターでは、インストール中にサーバーの再起動が複数回必要になる場合があります。クラスターのインストールパラメーターで[**再起動が必要**]が[**はい**]に設定され、修復ジョブの再起動オプションが[**個別のソフトウェアアイテムの指定に基づいてサーバーを再起動**](デフォルト)または[**インストールまたはアンインストールのたびにサーバーを再起動**]に設定されている場合、SAは自動的に再起動を実行します。

これらの再起動オプションのいずれかが設定されていない場合、クラスターは再起動が必要なポイントまでインストールを行います(再起動が必要な場合)。修復ジョブが完了した時点で、クラスターステータスは[**未インストール**]、ジョブステータスは[**失敗**]と表示されます。ジョブの出力には、パッチのインストールを続行する前にサーバーの再起動が必要であることを示すメッセージが表示されます。サーバーを再起動すると、ジョブが再度実行されてクラスターの残りの内容がインストールされます。クラスターで再起動が要求された場合、サーバーを再起動するまで他のパッチをインストールすることはできません。

手動パッチのインストール—patchadd

SAは`patchadd`ユーティリティを使用してSolarisパッチをインストールします。ただし、ファームウェアの更新などの一部のパッチは`patchadd`でインストールできません。これらのパッチは、リリースノートファイルに記載された特別なインストール手順に従って、Solarisサーバーに手動でインストールする必要があります。

これらのパッチはSAソフトウェアリポジトリにインポートし、サーバーに手動でインストールできますが、手動インストールパッチを修復しようとすると、修復ジョブのステータスが警告になります。パッチのステータスには[**インストールしない**]と表示され、出力には特別なインストール手順に従ってパッチを手動でインストールする必要があることが示されます。

SAでは、これらの手動インストールパッチがインストールされているかどうかを判断できません。手動インストールパッチを含むパッチポリシーに対してコンプライアンススキャンを実行すると、ポリシーが非コンプライアンスであるというレポートが作成されます。このような場合には、該当するパッチを手動でインストールし、ポリシーから削除してください。

良性エラーコードの検出

Solarisパッチをインストールすると、良性エラーコードが生成される場合があります。良性エラーコードは、実際のエラー状態を反映しないエラーコードです。たとえば、パッチがすでにインストールされていたり、優先パッチがすでにインストールされていたりすると、パッチのインストールが失敗して、良性エラーコードが生成される場合があります。実際にパッチが正当な理由でインストールされなかった場合、Solarisの`patchadd`コマンドの終了コードはエラーを示します。

サーバーのディスク容量不足などの実際のエラー状態によってパッチがインストールされない場合、SAはエラーと有効なエラーコードを通知します。

SAでは良性エラーコードを検出しても、ほとんどの場合は正常終了を通知します。ただし、次の場合、Solarisは良性エラーコードを検出できません。

- Solarisの遅延実行パッチ
- ローカルゾーンが定義されているSolarisグローバルゾーンにインストールされたパッチ

良性エラーコードを検出するようにSAを構成するには、次の手順を実行します。

1. Solaris 10を実行しているすべてのサーバーに、次のパッチをインストールします。
   - 119254-36 (sparc)
   - 119255-36 (i386)
2. SAクライアントで [**管理**] タブを選択します。
3. ナビゲーションペインで [**システム構成**] を選択します。これにより、システム構成パラメーターを含むSAコンポーネント、ファシリティ、およびレルムが表示されます。
4. SAコンポーネントのリストで、[**コマンドエンジン**] を選択します。これにより、そのコンポーネントのシステム構成パラメーターが表示されます。
5. パラメーター `way.remediate.sol_parse_patchadd_output`を**1**に設定します。
6. [**元に戻す**] を選択して変更を破棄するか、[**保存**] を選択して変更を保存します。

パッチポリシーを使用したパッチのインストール

パッチポリシーを使用したSolarisパッチのインストールは、次のフェーズで構成されます。

- パッチポリシーのサーバーへのアタッチ (150ページ)
- サーバーのパッチポリシーへのアタッチ (151ページ)

パッチポリシーのサーバーへのアタッチ

Solarisパッチポリシーをサーバーまたはサーバーグループにアタッチすると、そのSolarisパッチポリシーとサーバーまたはサーバーグループが関連付けられます。このアクションでは、Solarisパッチポリシーに含まれるパッチやパッチクラスターのインストールは行われません。パッチやパッチクラスターをインストールするには、Solarisパッチポリシーに基づいてサーバーを修復する必要があります。

Solarisパッチポリシーをサーバーにアタッチするためのアクセス権が必要です。アクセス権の取得については、SAの管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

Solarisパッチポリシーをサーバーにアタッチするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] > [**Solaris**] を選択します。
2. Solarisのバージョンを選択して、内容ペインにパッチポリシーを表示します。
3. (オプション) 内容ペインで、Solarisパッチポリシーを選択します。

a 右クリックして[Solarisパッチポリシー]ウィンドウでパッチポリシーを開きます。

b [表示]ドロップダウンリストから、[サーバー]を選択します。

c 内容ペインで、サーバーを選択します。

4 [**アクション**]メニューで、[**サーバーのアタッチ**]を選択します。

5 [サーバーのアタッチ]ウィンドウで、サーバーまたはデバイスグループを選択して、[**アタッチ**]をクリックします。

斜体表記ではないサーバーのみを選択できます。斜体表記のサーバーは、Solarisパッチポリシーをサーバーにアタッチするアクセス権がないことを表しています。

6 (オプション)[**サーバーをただちに修復**]を選択して、Solarisパッチポリシーに基づいてサーバーを修復します。このオプションを選択すると、[修復]ウィンドウが表示されます。このオプションを選択するには、[サーバーの修復]アクセス権が必要です。

サーバーのパッチポリシーへのアタッチ

サーバーまたはサーバーグループをSolarisパッチポリシーにアタッチすると、Solarisパッチポリシーとサーバーまたはサーバーグループが関連付けられます。このアクションでは、Solarisパッチポリシーに含まれるパッチやパッチクラスターのインストールは行われません。パッチやパッチクラスターをインストールするには、Solarisパッチポリシーに基づいてサーバーを修復する必要があります。

サーバーをSolarisパッチポリシーにアタッチするためのアクセス権が必要です。アクセス権の取得については、SAの管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

サーバーをSolarisパッチポリシーにアタッチするには、次の手順を実行します。

1 ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**]を選択して、内容ペインに管理対象サーバーのリストを表示します。

または

ナビゲーションペインで、[**デバイス**] > [**デバイスグループ**]を選択します。デバイスグループに移動して、内容ペインにデバイスグループのリストを表示します。

2 内容ペインで、サーバーまたはデバイスグループを選択します。

3 [**アクション**]メニューで、[**アタッチ**] > [**パッチポリシー**]を選択して、[Solarisパッチポリシーのアタッチ]ウィンドウを開きます。

4 [**Solarisパッチポリシーの参照**]をクリックして、リストに表示された1つまたは複数のポリシーを選択します。

または

[**フォルダーの参照**]をクリックして、フォルダー階層の1つまたは複数のポリシーを選択します。

5 [**アタッチ**]をクリックします。

6 (オプション)[**サーバーをただちに修復**]を選択して、Solarisパッチポリシーに基づいてサーバーを修復します。このオプションを選択すると、[修復]ウィンドウが表示されます。このオプションを選択するには、[サーバーの修復]アクセス権が必要です。

パッチポリシーに基づいたサーバーの修復

Solarisサーバーでパッチポリシーの Solarisパッチをインストールするには、パッチポリシーに基づいてサーバーを修復します。Solarisパッチポリシーに基づいてSolarisサーバーを修復するには、『SAユーザーガイド:ソフトウェア管理』に記載された手順を実行します。

パッチの適用可能性の分析

管理対象のSolarisサーバーにパッチをダウンロードしてインストールする前に、SAはサーバーでそのパッチが必要であることを確認します。この適用可能性の分析では、次の確認を行います。

1 サーバープラットフォームがパッチでサポートされるプラットフォームと一致すること。

2 パッチまたは優先するパッチがサーバー上にすでにインストールされていないこと。

3 パッチを適用するパッケージがサーバー上にすでにインストールされていること。

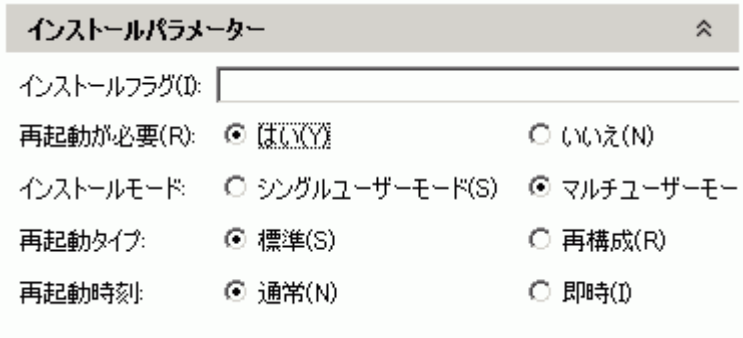
これらの条件のいずれかが満たされていない場合、パッチは適用不可能なパッチとなり、ダウンロードや管理対象サーバーへのインストールは行われません。適用不可能なパッチが全体のジョブステータスに影響することはなく、ジョブは正常に終了できます。

インストールパラメーター

個々のSolarisパッチには、Oracleが指定した再起動設定があります。これらの再起動設定は、SAクライアントの[インストールパラメーター]に表示されます。詳細については、図23を参照してください。Oracleの設定は「Oracleデフォルト」と表示されます。実際に使用される設定は、ラジオボタンで選択された設定です。

図23に示すパッチの場合、Oracleはインストール後に再起動することを指定していませんが、サーバーは再起動します。Oracleの推奨設定をオーバーライドして、このパッチのインストール後にシステムを再起動するように、ポリシー設定担当者が**[再起動が必要]**の設定を**[はい]**に変更しています。

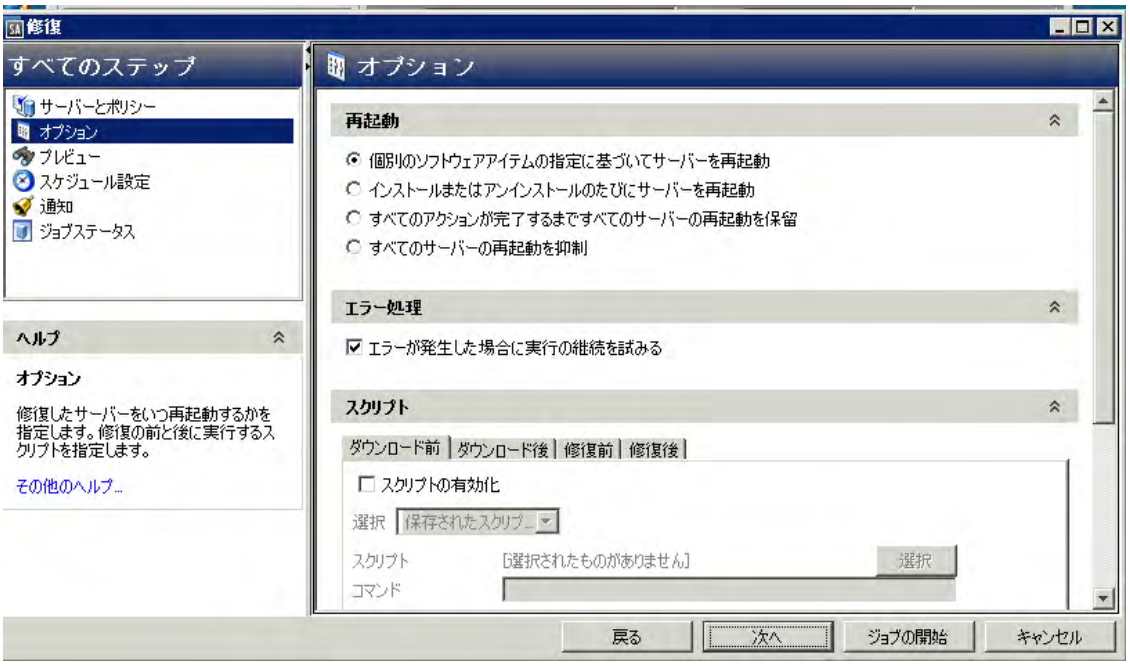
図23 インストールパラメーター



再起動オプション

Solaris パッチポリシーに基づいて Solaris サーバーを修復する場合、SA はパッチポリシーのパッチをインストールし、各パッチで指定された再起動設定を使用します。ただし、これらの設定は、修復ジョブを始める際にオーバーライドすることができます。図24は、パッチポリシーの修復ジョブに関するオプションの設定を示しています。

図24　　再起動オプション



[修復] ウィザードの次のオプションでは、パッチのインストール後にサーバーを再起動するかどうかを指定します。これらのオプションは、[修復] ウィンドウで起動されるジョブのみに適用されます。これらのオプションによって、[パッチのプロパティ] ウィンドウの [インストールパラメーター] タブにある [再起動が必要] オプションが変更されることはありません。次に示すオプションの設定は、最初のオプションを除いて、[再起動が必要] オプションの設定よりも優先します。

- **個別のソフトウェアアイテムの指定に基づいてサーバーを再起動** (デフォルト): デフォルトでは、パッチプロパティまたはパッケージプロパティの [再起動が必要] オプションの設定に従って再起動が行われます。
- **インストールまたはアンインストールのたびにサーバーを再起動:** ベストプラクティスとして、個別のパッチまたはパッケージのベンダーの再起動設定に関係なく、パッチまたはパッケージをインストール/アンインストールするたびにサーバーを再起動します。
- **すべてのパッケージがインストールまたはアンインストールされるまですべてのサーバーの再起動を保留する**: 選択したパッチの中に [再起動が必要] オプションが設定されているものが含まれていても、他のパッチにそのオプションが設定されていない場合、すべてのパッチのインストール後にサーバーが 1 回再起動されます。選択したパッチの中に [再起動が必要] オプションが設定されているものがない場合、サーバーは再起動されません。
- **すべてのサーバーの再起動を抑制**: パッチプロパティの [再起動が必要] オプションが設定されている場合でも、サーバーを再起動しません (ベンダー設定によっては、抑制オプションを無視して強制的に再起動を行う場合があります)。

パッチのインストールのトラブルシューティング

Solarisパッチのインストールモードの変更

(プロパティビューのインストールパラメーターで) インストールモードが**シングルユーザーモード**に設定されたSolarisパッチの修復を行うと、サーバーが再起動してシングルユーザーモードになった後にパッチがインストールされます。何らかの理由 (ネットワークの停止やハードウェア故障など) で修復が失敗した場合、システムはシングルユーザーモードのままになります。

システムをマルチユーザーモードに戻すには、次の手順を実行します。

1. Solarisサーバーコンソールにログインします。
2. Solarisのバージョンに応じて、次のいずれかのコマンドを入力してディレクトリを変更します。

```
cd /etc/rcS.d/    # On Solaris 5.10
cd /etc/rc1.d    # On Solaris 5.6 - 5.9
```

3. 次のコマンドを入力します。

```
./S99zOpswPatching exit_single_user_mode
```

4. 次のコマンドを入力するか、または別の方法でサーバーを再起動します。これにより、サーバーが再起動してマルチユーザーモードになります。

```
shutdown -y -g 0 -i 6
```

Solaris サーバーのサーバーコンソールにアクセスできない場合は、SA Global Shell (OGSH) の rosh ユーティリティを使用します。

1. OGFSアクセス権「サーバーへのログイン」を持つSAユーザーを使用して、OGSHセッションを開始します。たとえば、次のようなsshコマンドを入力できます。

```
ssh -p 2222 <ユーザー名>@<OGFSホスト>
```

2. 次のようなコマンドを使用して、それぞれのSolarisサーバーに移動します。

```
cd /opsw/Server/@/<サーバー名>/files/root
```

3. roshユーティリティを起動します。
4. Solarisのバージョンに応じて、次のいずれかのコマンドを入力してディレクトリを変更します。

```
cd /etc/rcS.d/    # On Solaris 5.10
cd /etc/rc1.d    # On Solaris 5.6 - 5.9
```

5. 次のコマンドを入力します。

```
./S99zOpswPatching exit_single_user_mode
```

6. 次のコマンドを入力するか、または別の方法でサーバーを再起動します。これにより、サーバーが再起動してマルチユーザーモードになります。

```
shutdown -y -g 0 -i 6
```

サーバーを再起動すると、roshのプロセスは終了します。サーバーが自動再起動に設定されていることを確認してください。

パッチでシングルユーザーモードが要求され、その他の理由 (依存するパッチがインストールされていないなど) でパッチのインストールに失敗した場合は、Solarisホストが再起動してシングルユーザーモードになり、パッチのインストール後にSolarisホストが再起動してマルチユーザーモードになります。この2回の再起動は、パッチのインストールに失敗した場合でも実行されます。

シングルユーザーモードでのステージングディレクトリのマウント

修復プロセスのあるアイテムでサーバーをシングルユーザーモードで再起動する必要があり、そのアイテムがシングルユーザーモードで利用できない特殊なディレクトリに格納されている場合に、残りのアイテムが処理されないようにすることができます。

シングルユーザーモードでは、開始時にステージングディレクトリをマウントする必要があります。デフォルトのステージングディレクトリは、/var/opt/opsware/agentです。次のアイテムがデフォルトディレクトリにない場合、修復プロセスでアイテムを見つけることができないため、ジョブは失敗します。

これを解決するには、管理対象サーバーでステージングディレクトリをマウントし、修復を行う前にこのステージングディレクトリにアイテムを格納します。これを行うには、マウント手順を含むサーバースクリプトを作成して、Solarisの既存の開始スクリプトに追加するのが最も簡単です。

次に例を示します。

```
echo "mount<stage_dir>">>/etc/rcS.d/S99mount_stage
```

<stage_dir>はアイテムを格納するディレクトリで、/etc/rcS.d/S99mount_stageはSolaris管理対象サーバー上の開始スクリプトです。

オフラインボリュームを使用したパッチのインストール

オフラインボリュームを使用してSolarisパッチをインストールすることができます。この項では、Solarisボリュームマネージャーに関する知識が必要です。

用意されているサンプルスクリプトを変更して、オフラインボリュームを使用したSolarisパッチのインストールに使用することができます。

オフラインボリュームを使用してSolarisパッチをインストールするには、次の手順を実行します。

1. サーバーにインストールするパッチを含むSolarisパッチポリシーを作成します。詳細については、Solarisパッチポリシーの作成 (124ページ) を参照してください。
2. パッチの適用対象のサーバーにディスクミラーを作成します。
3. ミラーを分離します。
4. オフラインディスクをマウントします。
5. サーバー上に/etc/opt/opsware/agent/offline_diskという名前のテキストファイルを作成します。
6. このファイルを編集して、オフラインディスクのマウントポイント (/altなど) を入力します。
7. パッチポリシーに基づいてサーバーを修正して、サーバー上にパッチをインストールします。

   SAは、オフラインディスクのマウントポイントでオフラインディスクにパッチをインストールします。オフラインディスクのマウントポイントは/etc/opt/opsware/agent/offline_diskに記載されています。
8. サーバーを再起動して、新しくパッチを適用したオフラインディスクに切り替えます。
9. パッチ適用済みディスクにパッチがインストールされていること、およびサーバーが正常に実行されていることを確認します。
10. パッチ適用済みディスクが期待どおりに動作している場合は、ミラーを同期します。

    パッチ適用済みディスクが期待どおりに動作していない場合、システムを再起動して元のディスクに戻して、ミラーを同期します。

パッチのアンインストール

Solarisパッチポリシーから Solarisパッチやパッチクラスターを削除しても、パッチやパッチクラスターが管理対象サーバーからアンインストールされるわけではありません。このアクションでは、Solarisパッチポリシーから Solarisパッチまたはパッチクラスターが削除されるだけです。管理対象サーバーから Solarisパッチをアンインストールするには、管理対象サーバーから Solarisパッチを直接アンインストールする必要があります。パッチクラスターを削除するには、管理対象サーバーからパッチクラスター内のそれぞれのパッチを削除する必要があります。

SAでは、次の方法を利用して管理対象のサーバーやデバイスグループからSolarisパッチをアンインストールできます。

- [パッチのアンインストール]ウィザードを使用して、Solarisパッチを管理対象サーバーから直接アンインストールします。
- [ソフトウェアのアンインストール]ウィザードを使用して、Solarisパッチを管理対象サーバーから直接アンインストールします。

SAクライアントでは、個別のサーバーのパッチコンプライアンスのチェックや、ファシリティ内のすべてのサーバーおよびサーバーグループの全体的なコンプライアンスレベルの確認を行うことができます。

第5章 Solaris 11パッチ管理

概要

Oracle Solaris 11では、IPSパッケージを使用してソフトウェアやソフトウェアの更新を提供します。IPS (Image Packaging System) は、ネットワークベースのパッケージ管理システムで、パッケージのインストール、アップグレード、削除を含むソフトウェアのライフサイクル全体で使用します。

Server Automation は Solaris 11 プラットフォームのサーバーパッチ適用をサポートしており、新規のソフトウェアをインストールすることなく、管理対象サーバーにインストールされたソフトウェアを最新バージョンに更新することができます。これは、明示的なパッチユニットがサポートされなくなった環境で、システムを最新の状態に維持するための優れた機能です。

Solaris 11パッチ適用のサポートでは、Solarisの既存のパッチ適用機能を利用します。ただし、Solarisの新しいIPSパッケージの配布体系に合わせるため、いくつか相違点があります。また、最初にIPSパッケージデータベースをセットアップするのに必要な条件も存在します。この章では、Solaris 11パッチ適用のセットアップ手順とSolaris 11でのパッチ適用の相違点について説明します。

Solaris 11パッチ適用の概要

IPSパッケージには、メタデータとバイナリを組み合わせて格納できるという構造上の利点があります。IPSパッケージは、ソフトウェアの初期インストールおよびソフトウェアの更新のすべてに使用します。IPSパッケージはすべてが揃った完全なもので、内部で完結しています。そのため、IPSパッケージには完全なパッケージが必要で、パッチユニットには分割されません。

このような構造上の違いにより、一般的なパッチ適用機能の中にはSolaris 11に当てはまらないものがあります。

ベンダー推奨のパッチポリシーを作成するプロセスには違いがあります。たとえば、Solaris 10 ではインストール済みのパッケージを確認して、既存のインストール内容に基づいて更新が必要なものを計算します。Solaris 11の場合、Server AutomationはIPSツールを使用して、推奨されるパッチとそれらの依存関係を検索します。

SA 9.13には、IPSパッケージデータベースの初期セットアップに使用できる定義済みのソフトウェアポリシー (Solaris 11 IPSパッケージ取得ツール) が付属しています。

手順のサマリー

次の手順を実行すると、IPSパッケージデータベースをセットアップして、SAでSolaris 11パッチ適用が利用できるようになります。最初のIPSパッケージの取得は、1つのSolaris 11管理対象サーバーを使用して実行します。その後は、コンプライアンスを維持するために、定期的に追加で更新を行う必要があります。ここで説明するのは、最初の取得の手順です。

推奨: IPSパッケージのリポジトリは全体で40 GBになる可能性があります。サーバーに十分な容量を確保するため、100GB以上の容量のあるSolaris 11サーバーを使用してください。

このサマリーは、次の2つのパートで構成されています。

- Solaris 11のIPSパッケージデータベースをセットアップする
- 推奨パッチポリシーを作成してSolaris 11管理対象サーバーを修復する

これらの手順の詳細な説明は、Solaris 11管理対象サーバーでのSAパッチ適用のセットアップ (158ページ) に記載しています。

Solaris 11のIPSパッケージデータベースをセットアップするには、次の手順を実行します。

1. SAに付属しているソフトウェアポリシー (**Solaris 11 IPSパッケージ取得ツール**) を使用して、選択したSolaris 11管理対象サーバーを修復します。

   これにより、ベンダーからIPSパッケージを取得するのに使用する、SA UAPIアクセスツールとIPSインポートツールがサーバーにインストールされます。
2. IPSパッケージをインポートする前に、インポートの前提条件となる次の手順を実行します。
   a. 管理対象サーバーのカスタマーをセットアップして、SA ライブラリ内の関連するすべての IPS パッケージに対する表示設定を割り当てます。
   b. それぞれの環境で目的のリポジトリにアクセスするのに HTTP プロキシが必要である場合は、IPS パッケージをインポートする前に、管理対象サーバー上でプロキシをセットアップします。
   c. `sol_ips_import.conf`を構成します。
3. 選択したSolaris 11管理対象サーバーからIPSインポートスクリプト (`sol_ips_import`) を実行して、すべてのIPSパッケージをコアにインポートします。
4. ソフトウェアの登録がまだ行われていない場合は、ソフトウェア登録スクリプト (`bs_software`) を実行します。

これで、IPSパッケージデータベースのセットアップは完了です。次に、パッチポリシーを作成してSolaris 11サーバーを修復します。

推奨パッチポリシーを作成してSolaris 11管理対象サーバーを修復するには、次の手順を実行します。

1. コアでパッチポリシースクリプト (`solpatch_import`) を実行して、管理対象サーバー用の推奨パッチポリシーを作成します。
2. SAクライアントから、作成した推奨パッチポリシーをサーバーにアタッチして修復を行います。

Solaris 11管理対象サーバーでのSAパッチ適用のセットアップ

手順1:「Solaris 11 IPSパッケージ取得」ソフトウェアポリシーに基づいて管理対象サーバーを修復する

1. SAクライアントで、[**SAライブラリ**] > [**タイプ別**] の順に移動して、[**Solaris 11 IPSパッケージ取得ツール**] を選択します。
2. [アクション] メニューで、[**サーバーのアタッチ...**] を選択します。
3. [**サーバーをただちに修復**] を選択します(このオプションを使用すると、サーバーのアタッチ後すぐに修復プロセスを実行できます)。
4. 修復するサーバーを選択して、[**アタッチ**] をクリックします。
5. [修復] ウィンドウで、他の設定にはすべてデフォルト値を適用し、[**ジョブの開始**] をクリックして選択したサーバーを修復します。

手順2: インポートの前提条件となる手順を実行する

管理対象サーバーのカスタマーにSAライブラリ内の関連するすべてのIPSパッケージに対する表示設定を割り当てる

sol_ips_importスクリプトを実行してIPSパッケージをインポートするには、事前にカスタマーに表示設定を割り当てる必要があります。

IPSパッケージはコア上のSAライブラリ内のディレクトリに配布されますが、インポートスクリプトは管理対象サーバーから実行されます。管理対象サーバーごとに1つのカスタマーが存在し、カスタマーによってSAライブラリに対する管理対象サーバーの表示設定が決まります。sol_ips_importスクリプトを実行すると、管理対象サーバーのカスタマーが参照できるIPSパッケージに基づいて、インポート内容の分析が行われます。このため、インポートが実行される管理対象サーバーに関連するカスタマーには、すべてのIPSパッケージに対する表示設定が必要です。

これを実現するには、IPSパッケージのターゲットディレクトリの親フォルダーに対するフォルダーのアクセス権をカスタマーに割り当てます。

1 次の手順で、管理対象サーバーのプロパティビューで管理対象サーバーのカスタマーを確認します。

a SAクライアントで、[**デバイス**]に移動して、更新する管理対象サーバーを選択します。

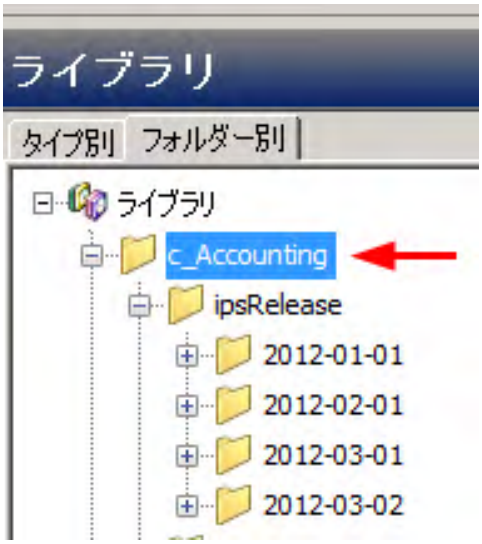
b [**表示**]>[**プロパティ**]を選択して、詳細ペインにサーバーのプロパティを表示します。

c カスタマーは[管理情報]セクションの下に表示されます。

2 次の手順で、IPSパッケージフォルダーのアクセス権をカスタマーに割り当てます。

a SAクライアントで、[**SAライブラリ**]>[**フォルダー別**]の順に移動して、カスタマーのSolaris 11 IPSパッケージの親フォルダーを選択します。

たとえば、次の例は「Accounting」カスタマーのファイル構造を表しています。



この例のライブラリは、AccountingとEngineeringのカスタマー別構成になっています。各カスタマーに関連するIPSパッケージはすべて、そのカスタマーのフォルダーに含まれています。この場合は、すべてのIPSパッケージに対する表示設定を確保するため、カスタマーに最上位のディレクトリに対するアクセス権を付与する必要があるため、親ディレクトリ「c_Accounting」を選択します。

b [**アクション**]>[**フォルダーのプロパティ**]>[**カスタマー**]タブの順に選択します。

c [**追加**]をクリックして、IPSインポートツールを持つ管理対象サーバーのカスタマーを選択します。

d [**追加**]をクリックして、[**OK**]をクリックします。

管理対象サーバーのカスタマーにこのフォルダーに対する表示設定を付与せずに、sol_ips_importスクリプトを実行すると、悪影響が生じる可能性があります。カスタマーのフォルダーのアクセス権は、サーバーに対して推奨されるパッチに影響を及ぼします。カスタマーのフォルダーのアクセス権が適切でないと、スクリプトで必要のない数多くのパッチがコアにアップロードされる可能性があります。

HTTPプロキシの設定

それぞれの環境で目的のリポジトリにアクセスするのにHTTPプロキシ (http_proxyやhttps_proxyなど) が必要な場合は、IPSパッケージをインポートする前に管理対象サーバーでHTTPプロキシが正しく設定されていることを確認します。

IPSパッケージのインポート構成ファイル (sol_ips_import.conf) の構成

1 時間の節約と信頼性の向上のため、sol_ips_importインポートスクリプトを実行する前に、sol_ips_import.conf構成ファイルをセットアップすることをお勧めします。

1 リモートサーバーのウィンドウから、管理対象のSolaris 11サーバーにログインします。

2 /opt/opsware/solimport#に移動します。

3 次の構成ファイルを開きます: sol_ips_import.conf

4 構成ファイルを編集して、IPSパッケージダウンロードプロセスの設定を定義します。

定義済みのIPS構成ファイルオプション

表15

構成ファイルオプション	説明および例
ユーザー名とパスワード	SAのログイン認証情報を指定します。
ローカルのダウンロードディレクトリ	パッケージをベンダーから最初にダウンロードする管理対象サーバー上のステージングディレクトリを指定します。 例: download_dir=/var/<UserFolderName>/IPSPkg_Stage **推奨**: IPSパッケージのリポジトリは全体で40 GBになる可能性があります。サーバーに十分な容量を確保するため、100GB以上の容量のあるSolaris 11サーバーを使用してください。
SAフォルダーアップロードディレクトリ	IPSパッケージを最終的に格納するSAコア上のディレクトリを指定します。 例: core_destination_folder=/Home/<AllSolaris11CustomersFolderName>/

表15

構成ファイルオプション	説明および例

IPSリポジトリのURL	パッケージを取得するベンダーのIPSリポジトリのURLを指定します。
	例:
	`repo_url=https://pkg.oracle.com/solaris/support`
	または
	`repo_url=https://pkg.oracle.com/solaris/release`
	注: これは説明用のOracleのリポジトリの例です。この例で、…/releaseのURLにはOracle Solarisの各リリースの更新が含まれ、…/supportのURLにはバグ修正と更新が含まれます。後者のURLは、サポート契約をしているユーザー専用です。数多くのベンダーがIPSパッケージを供給しており、さまざまな目的で異なるディレクトリにパッケージを提供できます。それぞれの目的に合わせて指定します。

最新パッケージのみの取得	すべてのパッケージを取得する場合は`True`に設定し、最新バージョンのみを取得する場合は`False`に設定します。 例: `all_versions=False`

証明書とキーファイル	ベンダーのリポジトリで証明書とキー認証が要求される場合は、このオプションを設定します。
	例:
	`cert=/var/pkg/ssl/Oracle_Solaris_11_Support.certificate.pen`
	`key=/var/pkg/ssl/Oracle_Solaris_11_Support.key.pen`
	注: 例はすべて説明用です。

手順3: IPSインポートスクリプト (sol_ips_import) を実行して、すべてのIPSパッケージをコアにインポートする

コマンドラインで異なる指定をした場合を除き、`sol_ips_import`コマンドは、前の手順の`sol_ips_import.conf`構成ファイルで指定した内容に基づいて実行されます。

1. IPS取得ツールをインストールしたSolaris 11サーバーにログインします。
2. インポートを実行する前にリモートリポジトリへの接続をテストし、最初に文字列フィルターを指定して`sol_ips_import`コマンドを実行します。たとえば、'telnet' を含むすべてのパッケージを表示するには、次のコマンドを実行します。

   ```
   ./sol_ips_import -f 'telnet' -n
   ```

   ここで、`-n`はダウンロードせずにプレビューすることを指定し、`-f`はフィルターを指定します。
3. IPSパッケージのインポートを実行します。次のコマンドを実行します。

   ```
   ./sol_ips_import
   ```

   `.conf`ファイルで指定したように、IPSパッケージがベンダーのリポジトリから管理対象サーバー上のローカルのステージングディレクトリにダウンロードされ、最終的にコア上のディレクトリにアップロードされます。

アップロードの失敗を処理するためのオプション:

IPSパッケージのインポート処理が完了すると、fmrifail_<DATE>ファイルで、コアへのアップロードに失敗したファイルがトラッキングされます。このファイルは、次のように--fmri_fileオプションを指定して手動で実行できます。

```
./sol_ips_import --fmri_file fmrifail_<DATE>
```

ここで、<DATE>はアップロードが開始された日時です(ファイル名に含まれます)。

アップロードに失敗したファイルがある場合、インポートスクリプトは自動的にそれらのファイルを再度ダウンロードしてアップロードします。自動アップロードが機能しない場合は、--force_processフラグを使用して手動で再ダウンロードとアップロードを強制的に実行することもできます。

```
./sol_ips_import -f '<パッケージ名>' --force_process
```

ダウンロードの再試行回数を設定するためのオプション:

失敗したパッケージのダウンロードはデフォルトで3回試行されます。再試行回数はコマンドラインで変更できます。また、構成ファイルsol_ips_import.confを変更して再試行回数を変更することもできます。

コマンドラインのオプション:

```
-a <MAX_RETRY_ATTEMPTS>
```

または

```
--max_download_attempts=<MAX_RETRY_ATTEMPTS>
```

ここで、<MAX_RETRY_ATTEMPTS>は、最大再試行回数を表す整数で置き換えます。

構成ファイルの設定:

```
max_retry_attempts=3
```

ここで、"3"はデフォルト値で、最大再試行回数を表す任意の整数を指定できます。

原則として、コマンドラインのオプションの方が構成ファイルの設定よりも優先されます。コマンドラインのオプションを使用せず、構成ファイルの設定も定義されていない場合、デフォルト設定の再試行回数は3回になります。

注: その他のコマンドオプションについては、./sol_ips_import -hを実行してください。

次のコマンドオプション一覧で、変数はすべて大文字で表記しています。

表16　　sol_ips_importのコマンドオプション

コマンドオプション	説明
-a MAX_RETRY_ATTEMPTS --max_download_attempts=MAX_RETRY_ATTEMPTS	失敗したパッケージダウンロードの最大再試行回数を指定します。値を指定しない場合、デフォルト値は3回です。
--all_versions	リモートリポジトリから利用可能なすべてのパッケージバージョンを取得します。デフォルトは最新です。パッケージ数が最大30%増加します。
-c REPO_CERT、または --cert=REPO_CERT	Oracle_Solaris_11_Support.certificate.pemなどのIPSリポジトリの証明書ファイル
--config=CONFIG_PATH	このファイルからコマンドラインオプションを読み取ります。デフォルトはsol_ips_import.confです。

表16 sol_ips_importのコマンドオプション

コマンドオプション	説明
-d DOWNLOAD_DIR、または --download_dir=DOWNLOAD_DIR	パッケージを格納するローカルシステム上のディレクトリ
--download_only	パッケージのダウンロードのみ
-f PKG_FILTER、または --filter=PKG_FILTER	Python 正規表現の文字列を使用して、利用可能なパッケージをフィルター処理します。アップロードのみのモードの場合は、ファイル名がフィルター処理されます
--fmri_file=FMRI_FILE	各行に1つのFMRIを含むファイル。リポジトリの利用可能なパッケージのフィルター処理に使用されます。アップロードのみのモードの場合は、ファイルに関連するFMRIに対してフィルター処理されます
--force_process	以前にコアにアップロードされたパッケージの取得とアップロードを強制的に実行します。
-h、または --help	このヘルプメッセージを表示して終了します
-k REPO_KEY、または --key=REPO_KEY	Oracle_Solaris_11_Support.key.pem などのIPSリポジトリのキーファイル
-m、または --manual	マニュアルページを表示して終了します
-n、または --preview	リモートリポジトリからダウンロードされる内容を表示します(ドライラン)
-p HPSA_PASS、または --hpsa_pass=HPSA_PASS	パッケージをアップロードするのに使用するSAパスワード
-s REPO_URL、または --sourcerepourl=REPO_URL	IPSリポジトリのURL
-u HPSA_USER、または --hpsa_user=HPSA_USER	パッケージをアップロードするのに使用するSAユーザー
--upload_only	次のオプションで指定したローカルディレクトリからパッケージをアップロード --download_dir
--version	プログラムのバージョン番号を表示して終了します。
-w OPSWARE_FOLDER、または --core_destination_folder=OPSWARE_FOLDER	SAフォルダーシステム内のターゲットフォルダー

手順4: ソフトウェアを登録する

ソフトウェアの登録は、デプロイメント時に設定されたオプションに応じて、SAエージェントデプロイメントの最中またはデプロイメントから24時間以内に自動的に実行されます。

ソフトウェアの登録がまだ行われていない場合は、次の手順でソフトウェア登録スクリプトを手動で実行できます。

1 管理対象サーバーにログインします。

2 次のソフトウェア登録スクリプトを実行します。

```
/opt/opsware/agent/pylibs/cog/bs_software -full
```

手順5: 推奨パッチポリシーの作成 (solpatch_importの実行)

1 rootとしてSAコアサーバーにログインします。

2 solpatch_importスクリプトを実行して、管理対象サーバー用の推奨パッチポリシーを作成します。

例:

```
/opt/opsware/solpatch_import/bin/solpatch_import -a policy
--policy_path='svrname-policy-all-new' --filter="rec,server=svrname"
```

ここで、path =ポリシー名、filter =サーバー名、rec =推奨パッチです。

特定のサーバー用の推奨パッチポリシーを作成するには、pathとfilterの両方のオプションが必要です。

ポリシーを作成する前にプレビューを行うには、-a showオプションを使用します。

たとえば、サーバー「kalai」用の推奨パッチを含むポリシーをプレビューする場合は、次のコマンドを実行します。

```
/opt/opsware/solpatch_import/bin/solpatch_import -a show
--filter="rec,server=kelai"
```

その後、サーバー「kalai」に「kalai-policy-all-new」という名前のパッチポリシーを作成するには、次のコマンドを実行します。

```
/opt/opsware/solpatch_import/bin/solpatch_import -a policy
--policy_path='kelai-policy-all-new' --filter="server=kelai"
```

その他のコマンドオプションを参照する場合は、/opt/opsware/solpatch_import/bin/solpatch_import -hを実行します。solpatch_importコマンドオプションの追加情報については、第4章「Solarisパッチ管理」(113ページ)を参照してください。

手順6: 推奨パッチポリシーをサーバーにアタッチして修復する

Solarisパッチポリシーをサーバーにアタッチするには、次の手順を実行します。

1 ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] または [**デバイス**] > [**デバイスグループ**] を選択します。

2 内容ペインで、目的のSolaris 11サーバーまたはデバイスグループを選択します。

3 [**アクション**] メニューで、[**アタッチ**] > [**パッチポリシー**] を選択して、[Solarisパッチポリシーのアタッチ] ウィンドウを開きます。

4 [**Solarisパッチポリシーの参照**] または [**フォルダーの参照**] タブで、作成した推奨パッチポリシーを選択します。

5 [**サーバーをただちに修復**] を選択します(このオプションを使用すると、サーバーのアタッチ後すぐに修復プロセスを実行できます)。

6 [**アタッチ**] をクリックします。

7 [修復] ウィンドウで、他の設定にはすべてデフォルト値を適用し、[**ジョブの開始**] をクリックして選択したサーバーを修復します。

ベストプラクティス: 複数のサーバーを一度に修復することは可能ですが、ポリシー内のIPSパッケージは特定のサーバーに基づいているため、ポリシーが完全に適合するには、修復するサーバーのメンテナンスレベルが同じである必要があります。ベストプラクティスでは、サーバーごとに1つのポリシーを使用するか、デバイスグループを介してサーバーを管理することで、メンテナンスレベルの同期を維持することを推奨しています。

SAでのSolaris 11のパッチ適用

Solaris 11パッチ適用のサポートでは、Solarisの既存のパッチ適用機能を利用します。ただし、SolarisのIPSパッケージの配布体系に合わせるため、いくつか相違点があります。

Solaris 11の推奨パッチポリシーでのIPSパッケージとサーバータイプ

`solpatch_import`コマンドで作成するSolaris 11の推奨パッチポリシーは、SunOS 5.11 (SPARC) またはSunOS 5.11 x86 (x86) の両方のタイプのSolaris 11サーバーに適用されます。個別のIPSパッケージは、SPARCアーキテクチャー、x86アーキテクチャー、またはその両方のSolaris 11サーバーに適用できます。SAの修復プロセスでは、無関係のパッケージや間違ったパッケージがインストールされることはありません。

Solaris 11パッチポリシーの相違点

- すべてのパッチユニットがIPSパッケージであるため、Solaris 11パッチポリシーにアイテムを追加する際には、IPSパッケージとスクリプトの2つのタイプのアイテムしか存在しません。
- Solaris 11の修復時に依存関係チェックが行われるため、[依存関係の解決] を実行する必要はありません。以前のバージョンのSolarisでは、[依存関係の解決] は独立した手順で、修復前にポリシー内で実行する必要がありました。
- Solaris 11パッチポリシーでは、管理対象サーバーにインストール済みのIPSパッケージに対して適用可能な更新のみを行います。

  例:

  管理対象サーバーに次のファイルが存在し、

  — Xバージョン1

  — Yバージョン2

  次のファイルをインストールしようとした場合:

  — Xバージョン2

  — Yバージョン2

  — Zバージョン2

  Xバージョン2のみがインストールされます。これは、Xバージョン2がXバージョン1に対する更新で、サーバー上にすでにインストールされているためです。

パッケージYはすでに最新であるためインストール対象になりません。Zはサーバーにすでに存在するパッケージの更新ではないため対象になりません。

Solaris 11の修復の相違点

- **適用可能性分析**: SAでは、前のバージョンのパッケージがサーバー上にすでにインストールされているかどうかを確認して、IPSパッケージがサーバーに関連するものであることを確認します。前のバージョンが存在しないか、優先パッケージが存在する場合、IPSパッケージは適用不可能とみなされます。
- **修復プロセス**: IPSパッケージの修復では、基本的に、前のバージョンのIPSパッケージの上に新規バージョンのIPSパッケージがインストールされます。

修復ジョブを実行すると、新しいブート環境 (BE) が作成される場合があります。この場合、サーバーが再起動して新規パッケージが利用できるようになるまで、サーバーはコンプライアンス状態になりません。新しいBEが必要な場合は、システムを再起動する必要があります。修復ジョブ用に定義した再起動オプションに従った処理が行われます。

Solaris 11パッチポリシーの再起動設定を変更しないことを強く推奨します。Solaris 11パッチポリシーを修復する場合、修復の再起動オプションは自動的に [すべてのアクションが完了するまですべてのサーバーの再起動を保留] に設定されます。このデフォルトの再起動設定を変更すると、パッチポリシーの修復時にパッチがインストールされない可能性があります。

Solaris 11のブート環境とゾーンについては、Solarisのドキュメントを参照してください。

Solaris 11パッチポリシーのルール

Solaris 11パッチポリシーの優先ルール

IPSパッケージZバージョン1とバージョン2がポリシーに含まれている場合､Zバージョン1よりもZバージョン2が優先されると判断され、Zバージョン1はインストールされません。

Solaris 11パッチポリシーの適用可能性ルール

1. IPSパッケージZバージョン2がポリシーに含まれていて、前のバージョンのZが管理対象サーバー上にインストールされていない場合、Zバージョン2はインストールされません。
2. IPSパッケージZバージョン1がポリシーに含まれていて、Zバージョン2が管理対象サーバー上にインストールされている場合、Zバージョン1よりもインストール済みのパッケージが優先されると判断され、Zバージョン1はインストールされません。
3. IPSパッケージZバージョン1がポリシーに含まれていて、Zバージョン1が管理対象サーバー上にインストールされている場合、Zバージョン1はインストール済みと判断され、インストールされません。

IPSパッケージをインストールできない理由

最初に次のパッチポリシーのルールが適用されます。

1. **ベースパッケージが存在しない**: 管理対象サーバーに前のバージョンのパッケージAがインストールされていないため、IPSパッケージAバージョン1をインストールできません。
2. **新しいバージョンがすでにインストール済み**:
   a. 新しいバージョン (パッケージAバージョン2) がポリシーに含まれていて、パッケージAバージョン1の代わりにバージョン2がインストールされるため、パッケージAバージョン1をインストールできません。
   b. 管理対象サーバーにパッケージAバージョン2 (新しいバージョン) がすでにインストールされているため、パッケージAバージョン1をインストールできません。

次にすべてのポリシー (ソフトウェアまたはパッチ) の一般ルールが適用されます。

1. **依存関係**: パッケージBバージョン1のインストールにSAのリポジトリ内に存在しないパッケージAバージョン3が必要であるため、パッケージBバージョン1をインストールできません。
2. **ブロック**: 管理対象サーバーにインストールされているパッケージXによってパッケージAバージョン1のインストールが阻止されるため、パッケージAバージョン1をインストールできません。
3. **重複**: パッケージAバージョン1がすでにインストールされているため、パッケージAバージョン1をインストールできません。
4. **その他**: Solaris IPSの分析に基づいてその他の理由が適用される場合があります。SAはSolarisのエラーメッセージをSAの修復ジョブに渡します。

その他の相違点

Solaris 11には`patchadd`ユーティリティを適用できません。これは、前のバージョンのSolarisに存在したようなパッチユニットの概念が存在しないためです。ユニットはすべてIPSパッケージです。IPSパッケージでは、代わりにpkgコマンドを使用します。

第6章 Ubuntuパッチ管理

概要

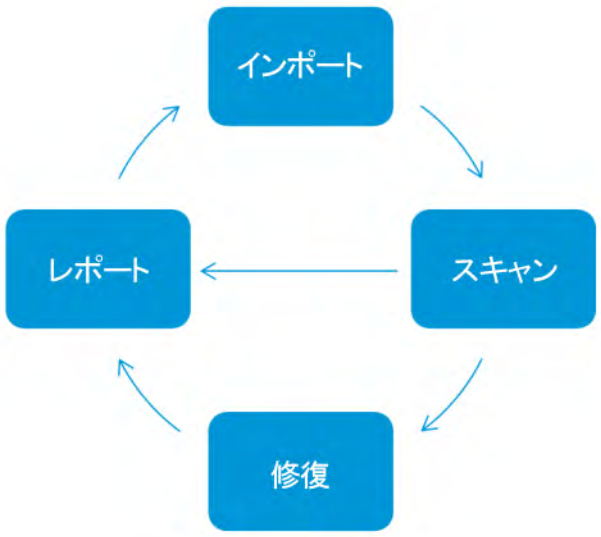
HP Server Automation (SA) のUbuntuパッチ管理では、Ubuntu Debianパッケージ更新の確認、インストール、削除によって、組織内にある管理対象サーバーのセキュリティを確保します。SA でサポートされる管理対象サーバープラットフォームのセキュリティ脆弱性に対して、対応する Ubuntu パッケージを確認してインストールすることができます。

注: Ubuntuでは、"パッチ"とはDebian"パッケージ"のことです。SAでは、Ubuntuパッチ管理を使用して、Ubuntuパッケージを適用します。

SA ではパッチ管理の主要な機能が自動化されていますが、Ubuntu パッケージのインストール方法やインストール条件は、細かく制御することができます。パッチ適用プロセスを自動化することで、パッチ適用に伴うダウンタイムを短縮できます。また、SA では、パッチアクティビティのスケジュールを設定することで、ピーク以外の時間帯にパッチを適用することができます。

Ubuntu ではセキュリティ上の脅威に対処するパッケージが頻繁にリリースされます。システムのセキュリティ被害を未然に防ぐには、迅速にパッケージを適用する必要があります。ただし、パッケージを誤って適用すると、パフォーマンスの低下や重大なエラーなど深刻な問題が発生する原因になるので注意が必要です パッチ管理では、新しく検出された脅威に迅速対応できるだけでなく、パッチインストールの厳格なテストと標準化をサポートします。

図25 SAとUbuntuの統合パッチ適用プロセス



ベストプラクティス: SA の Ubuntu パッチ適用を使用して、バイナリパッケージをインポートする前にメタデータをインポートできます。ダウンロードしたメタデータのみを使用して、Ubuntu スキャナーを実行し、サーバーの脆弱性を特定できます。その後、Ubuntuパッケージインポーターを実行して、管理対象サーバーに必要なパッケージのみをインポートできます。この方法により、ストレージ容量と、スキャンおよび修復プロセス時間を節約できます。

本書では、パッチポリシーを使用して、Ubuntu メタデータとパッケージのインポート、脆弱性のスキャン、Ubuntuパッケージ更新のインストールを実行する方法について説明します。

機能

SAでは、次のような機能や特徴を利用して、Ubuntuパッチ適用を自動化しています。

- **セントラルリポジトリ**: パッケージがそれぞれの標準形式で保存され、整理されます
- **データベース**: これまでに適用したすべてのパッケージの情報を保存します
- **動的パッチポリシー**: ベンダーの最新メタデータに基づいて、プラットフォーム脆弱性を分析します。
- **高度な検索機能**: パッケージ更新が必要なサーバーを識別できます
- **監査機能**: 重要なパッケージ更新のデプロイメントをトラッキングします

パッチの参照のタイプ

SAクライアントのインタフェースでは、Ubuntuパッケージおよびメタデータがオペレーティングシステム別に構成され、各パッケージに関する詳細な情報が表示されます。また、ソフトウェアポリシーの使用状況や、サーバーおよびデバイスグループの使用状況など、使用状況に関する情報を参照できます。パッケージは、作成日、更新日、オブジェクトIDなどで並べ替えられます。また、サーバーにインストールされているすべてのパッケージを参照し、パッケージメタデータを表示して編集することもできます。

スケジュール設定と通知

SAクライアントでは、Ubuntuからパッケージ更新をスケジュールまたはオンデマンドでServer Automationにインポートするかどうか、およびこれらのパッケージを管理対象サーバーにダウンロードするタイミングを設定できます。

ベストプラクティス: パッケージのインストールは業務への影響の最も少ない日時にスケジュール設定します。

Ubuntuパッチ適用では、ダウンロードやインストール操作の完了や成否に関する通知を受け取るように、電子メール通知を設定することもできます。パッチのインストールをスケジュール設定する際には、再起動設定を指定して、ベンダーの再起動オプションの使用、無効化、延期、または抑制を設定することもできます。

-

パッチポリシー

管理対象サーバーまたはサーバーグループでパッケージの確認と配布を柔軟に行えるように、Ubuntuパッチ適用では、インストールが必要なパッケージのグループを定義したパッチポリシーを作成することができます。パッチポリシーを作成してサーバーまたはサーバーグループにアタッチすることにより、組織内でインストールするパッケージとそのインストール先を管理することができます。

Ubuntuで使用するパッチポリシーのモデルは、パッチとしてインポートされたソフトウェアおよびパッケージに基づいています。

- 動的ポリシーにより、最新の Ubuntu パッケージがベンダーから自動的にインポートされます。新しいDebianバイナリパッケージがインポートされると、ポリシーに最新パッケージの内容が含まれ、ポリシーが有効であることがアイコンで表示されます。

  動的ポリシーは、サーバーを修復するように設計されています。
- 静的パッチポリシーには、Debianバイナリパッケージの更新を定義するメタデータが含まれます。

ベストプラクティス: 更新を自動化するには、動的ポリシーを使用します。

詳細については、パッチポリシーの作成を参照してください。

パッチインストールのプレビュー

パッチ管理では、新しく見つかったセキュリティ脆弱性に迅速に対応できるだけでなく、パッチインストールの厳格なテストと標準化もサポートされます。

サーバーをスキャンし、インストールするパッケージを確認した後、実際にパッケージをインストールする前に、パッチ管理でインストールをシミュレート (プレビュー) することができます。パッチのプレビューを使用して、パッチのインストール対象として選択したサーバーに該当するパッケージがすでにインストールされているかどうかを確認します。システム管理者がパッケージを手動でインストールしている場合、サーバーにパッケージがすでにインストールされている可能性があります。

このような形でパッケージがインストールされた場合、コンプライアンススキャンを実行するか、インストール済みパッケージを登録していない限り、SAではパッケージの存在を把握できません。プレビューでは、サーバーのパッケージの状態に関する最新のレポートが作成されます。

プレビューでは、特定のUbuntu製品を必要とするパッケージ、および他のパッケージよりも優先されるパッケージや他のパッケージの方が優先されるパッケージなどの、パッケージの依存関係情報や優先情報に関するレポートも作成されます。

パッチデータのエクスポート

サーバーまたはサーバーグループのパッチ状態のトラッキングに役立つように、パッチ管理では、パッチデータをエクスポートできます。パッチデータはカンマ区切り (.csv) ファイルにエクスポートできます。このデータには、パッチがインストール済みとして最後に検出された日時、Server Automation でパッチがインストールされた日時、コンプライアンスレベル、パッチポリシー例外などに関する詳細情報が含まれます。エクスポートしたデータはスプレッドシートやデータベースにインポートして、さまざまなパッチ分析タスクを実行できます。

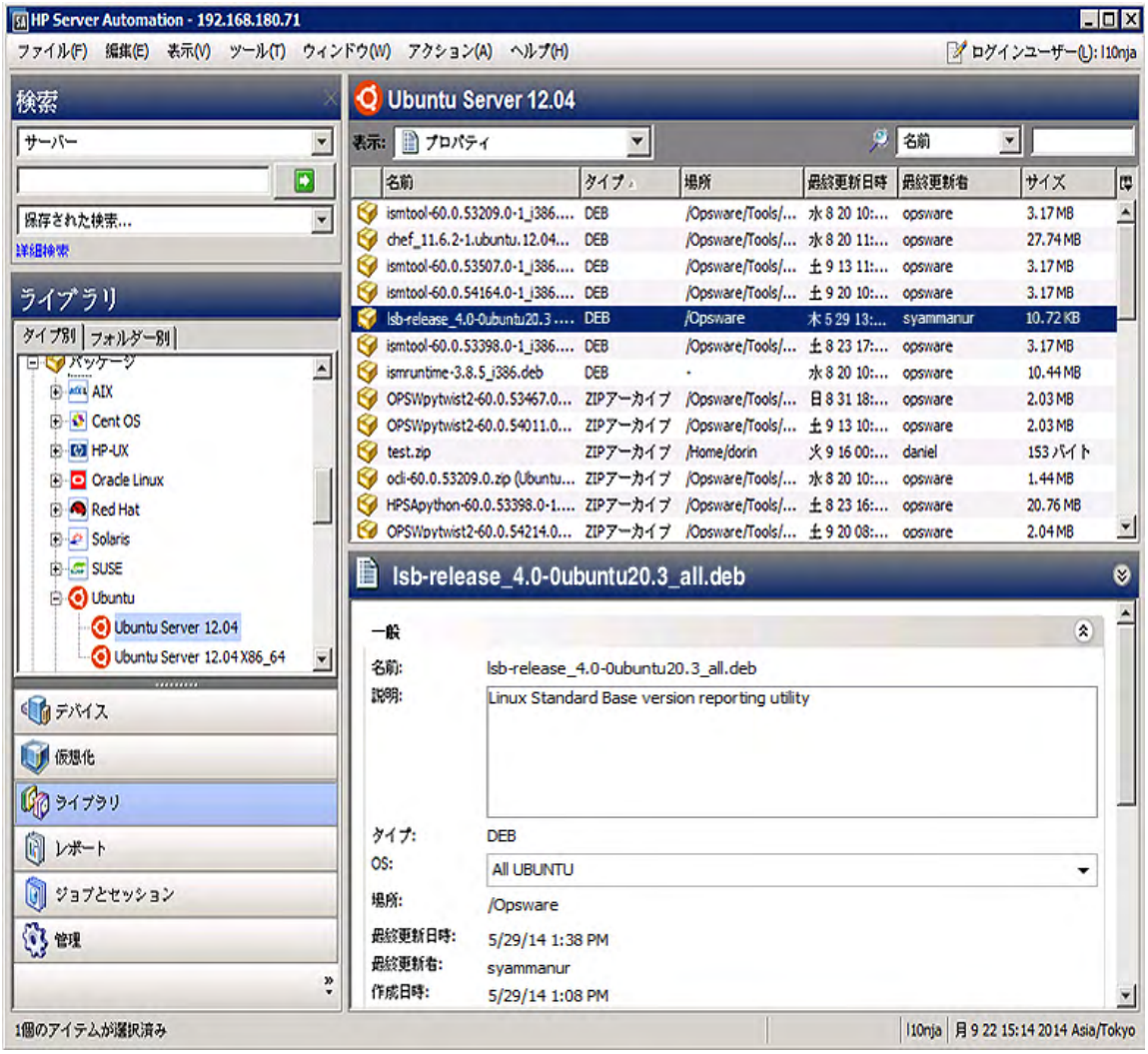
SAクライアントライブラリ

SAクライアントライブラリでは、オブジェクトID、作成日、更新日、オペレーティングシステムなどを使用して、Ubuntuパッケージを柔軟に検索または表示することができます。詳細については、図26を参照してください。

内容ペインの薄く表示されたパッケージアイコンは、パッケージのバイナリファイルがライブラリにアップロードされていないことを示します。バイナリをアップロードすると、アイコンがアクティブとして表示されます。表示するパッケージメタデータ情報の列を制御するには、列セレクターを使用します。

ライブラリはUbuntuパッケージメタデータと統合されているため、プレビューペインでリアルタイムにベンダー情報を確認することができます。

図26　SAクライアントライブラリのUbuntuパッケージおよびメタデータ



前提条件 - 管理対象サーバーのパッチ適用

管理対象サーバーにパッチを適用するには、次の前提条件が満たされている必要があります。

1　Ubuntuメタデータが SAにインポート されている

2　管理対象サーバーで、メタデータのインポート後にコンプライアンススキャンが実行済みである

プラットフォームバージョンのサポート情報については、『SA Support and Compatibility Matrix』を参照してください。

パッチおよびパッチポリシーの検索

SAクライアントでは、SAクライアントの検索機能を使用して、運用環境に関する情報を検索できます。検索機能を使用すると、パッケージ、パッチポリシー、サーバーなどを検索できます。『SAユーザーガイド: Server Automation』の「SAクライアントの検索に関する項」を参照してください。

SAでのDebianメタデータデータベースの管理

Debian メタデータデータベースには、リリース済みのパッケージとそれらの適用方法に関する情報が含まれています。パッチ管理では、すべてのUbuntuサーバーをDebianメタデータと比較して、適用する必要のあるパッケージを確認します。

サーバーがHP Server Automationで管理されている場合、サーバーにインストールされたSAエージェントは、インストール済みのパッケージなどのサーバーの構成をSAに登録します。SAエージェントは、この登録を24時間ごとに繰り返します。この情報はモデルリポジトリ内に直ちに記録されます。この情報には、オペレーティングシステムバージョン、ハードウェアタイプ、インストール済みソフトウェアとパッケージなどあります。SAでサーバーを初めてプロビジョニングする際には、同じデータがすぐに記録されます。

新規のパッケージが発行されると、SAクライアントを使用して、パッチを適用する必要のあるサーバーを確認できます。SAでは、パッケージやその他のソフトウェアをアップロードするソフトウェアリポジトリが利用できます。SAクライアントを使用して、このソフトウェアにアクセスし、関連するサーバーにパッケージをインストールします。

Ubuntuでは、Debianパッケージメタデータは自動的にインポートされますが、パッケージユニットはインポートされません。Ubuntu データベースで検出されたパッケージをすべてインポートするか、またはこれらのパッケージのうち、管理対象サーバーで必要なパッケージのみをインポートするかを選択できます。この機能を使用して、インポートするパッケージの数を制限し、ストレージ容量とユーザー時間を節約できます。

UbuntuおよびWindowsデータベースのビューでは、ベンダーパッチキーが現在利用可能です。ベンダーパッチキーはベンダー固有の値で、ユーザーはこれを使用して、SAのユニット (パッチ) をベンダーが提供する特定のパッチに関連付けることができます。

ベストプラクティス: UbuntuサーバーがSAの管理下に移されたら、SAのUbuntuパッチ管理を使用してすべてのUbuntu パッケージをインストールすることをお勧めします。パッケージを手動でインストールした場合、次にソフトウェア登録を行うまでSAにはそのパッケージに関するデータがありません。ただし、SAのUbuntuパッチ管理を使用してパッケージをインストールすると、エージェントによってモデルリポジトリ内の該当するサーバーに関する情報がすぐに更新されます。

Ubuntuパッチ管理で使用する役割

Server Automation では、パッチ管理の役割を組織内の複数のタイプのユーザーに割り当てることで、厳密な変更管理を行うことができます。パッチ管理には、ポリシー設定担当者、パッチ管理者、システム管理者などの役割を持つユーザーが関与します。

これらの役割は、SAでパッチを管理するためのアクセス権を割り当てることで制御します。必要なアクセス権の取得については、SAの管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

- **ポリシー設定担当者**: ポリシー設定担当者は、パッケージリリースを確認し、組織のパッチポリシーに含まれるベンダーパッケージを識別するセキュリティ標準グループのメンバーです。ポリシー設定担当者は、最新のセキュリティ上の脅威を確認し、これらの問題に対処するためにベンダーがリリースしたパッ

ケージを確認する必要があります。一般にポリシー設定担当者は、管理対象のオペレーティングシステムとアプリケーションに精通しており、ベンダーが発行したパッケージを適用する必要があるかどうかを評価することができます。また、ポリシー設定担当者は、パッチ適用プロセスの詳細なテストを考慮に入れて、パッケージのインストール後に発生する一般的な問題を診断することもできます。

ベストプラクティス: 更新を自動化するには、静的パッチポリシーではなく、動的パッチポリシーを使用します。

- **パッチ管理者**: パッチ管理者には、パッケージオプションのインポート、テスト、編集を行う権限があります。パッチ管理者は、多くの場合、組織内でセキュリティ管理者と呼ばれます。パッチ管理者には、パッケージをHP Server Automationにインポートしてパッケージをテストし、利用可能とマークするのに必要なアクセス権が割り当てられます。パッチ管理者は、パッチ管理を使用してパッケージオプション (インストールスクリプトなど) を編集することもできます。その他のタイプのユーザーは、パッケージのインポートや編集を行うことはできません。通常、パッチ管理者はUbuntu Debian メタデータデータベースをインポートして、非運用環境の基準ハードウェア上でパッケージをテストします。パッケージをテストして、運用システムに適用しても問題がないことが確認できたら、パッチ管理者はライブラリでパッケージに利用可能のマークを付けて、そのパッケージを適用する必要のあるシステム管理者に通知します。
- **システム管理者**: システム管理者は、パッチ管理者が指定したオプションに従って、(使用承認済みの) パッケージを均等かつ機械的にインストールします。システム管理者は、デプロイメント中のサーバーの日常的なメンテナンスを担当するSAユーザーです。これらのユーザーには、低レベルシステムの詳細について、ポリシー設定担当者やパッチ管理者と同じ水準の技術力は必要ありません。パッチ管理者がパッチのインストールをすでにセットアップしているため、システム管理者はポリシーをサーバーへアタッチし、パッケージの例外を設定して、多数の管理対象サーバーにパッケージをインストールすることができます。システム管理者は、承認済みパッケージが必要なサーバーを検索し、パッケージをインストールして、パッケージが正常にインストールされたことを確認する必要があります。システム管理者はパッケージをインポートできますが、パッチ管理者が利用可能とマークしない限り、パッケージをインストールすることはできません。システム管理者はパッケージをアンインストールすることもできます。

HP Server Automationでは、Patch DeployersやPatch Policy Settersの事前定義のパッチユーザーグループを利用することもできます。詳細については、事前定義のパッチユーザーグループ (174ページ) を参照してください。

事前定義のパッチユーザーグループ

SAのインストールまたはアップグレード時には、Patch DeployersやPatch Policy Settersなどの事前定義のパッチユーザーグループが作成されます。

- **Patch Deployers**—パッケージのインストールへのアクセス。(Ubuntuパッチポリシーをサーバーにアタッチするには、このグループが必要です。)
- **Patch Policy Setters**—パッチポリシーの設定へのアクセス。(Ubuntuパッチポリシーを管理するには、このグループが必要です。)
- **Software Policy Setters**—ソフトウェアポリシーの設定へのアクセス。(Ubuntuパッチポリシーを管理するには、Patch Policy SettersとSoftware Policy Settersの両方のグループが必要です。)

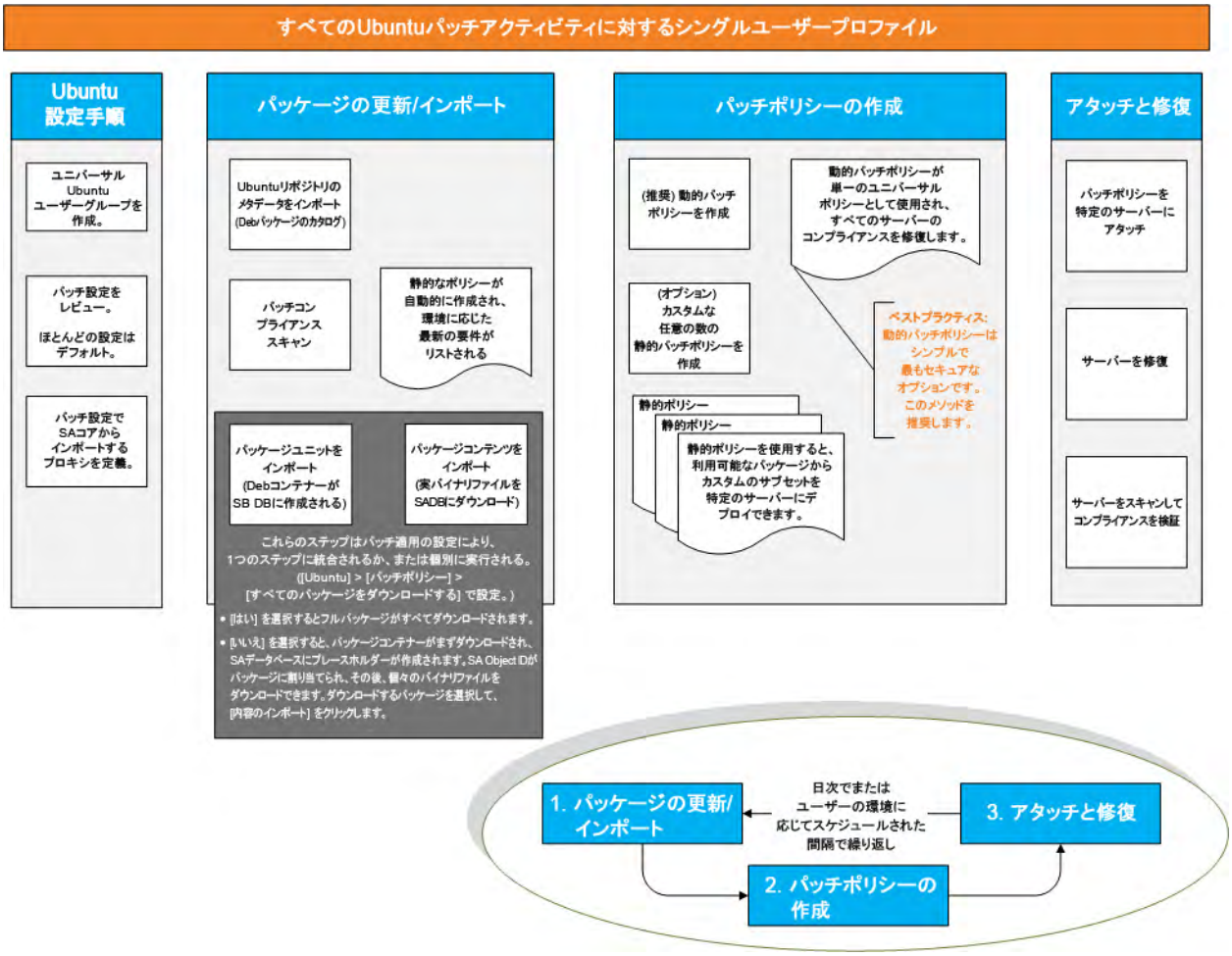
その際には、読み取りまたは読み取り / 書き込みのアクセス権を最初のファシリティに割り当て、これらのユーザーグループに適切なアクセス権を割り当てる必要があります。これらの事前定義のユーザーグループの使用はオプションです。事前定義のユーザーグループのアクセス権は変更可能で、これらのグループを削除したり、コピーして新規グループを作成したりすることもできます。これらの事前定義のユーザーグループの変更や削除が、SAのアップグレードによる影響を受けることはありません。詳細については、『SAユーザーガイド: Server Automation』を参照してください。

パッチ管理のプロセス

Ubuntuパッチ適用プロセスは、次のフェーズで構成されます。

1. **設定の定義**: このフェーズでは、Ubuntuプロキシ、リポジトリ、ポリシー設定、スキャナーの動作に関するUbuntuパッチ適用の設定を行います。
2. **メタデータのインポート**: このフェーズでは、Ubuntuの初期メタデータをServer Automationに取り込みます。
3. **パッチコンプライアンススキャンの実行**: このフェーズでは、コンプライアンススキャンを実行して、サーバーがコンプライアンス違反でないかどうかを確認します。通常、サーバーのSAエージェント設定に基づいて、24時間ごとに自動処理で実行されます。また、空のポリシーを使用して、パッチコンプライアンススキャンを手動で実行することもできます。パッチコンプライアンススキャンを開始する方法 (196ページ) およびパッチコンプライアンススキャンの即時開始 (197ページ) を参照してください。
4. **パッケージのバイナリのインポート**: パッケージのバイナリは、修復フェーズの前にインポートする必要があります。
5. **修復**: このフェーズでは、パッチポリシーを使用してパッケージをダウンロードし、推奨サーバーに更新をインストールします。

図27　Ubuntuパッチ適用プロセス



Ubuntuパッチ設定の指定

Ubuntuパッチ設定

Ubuntuパッチ設定では、使用環境に適したパッチ適用オプションや機能を設定するための幅広いオプションが用意されています。

表17 Ubuntuパッチ設定

設定	説明
Proxy	Ubuntuプロキシ構成を定義します。
リポジトリ	アクセスするUbuntuリポジトリを定義します。
ポリシー設定	Ubuntuパッチのポリシー設定を構成します。
スキャナーオプション	Ubuntuスキャナーの動作を指定します。
一般	Ubuntuのログ設定を指定します。

Ubuntuパッチ設定: プロキシの設定

使用環境のプロキシ情報を指定します。プロキシはネットワークセキュリティを提供し、多くの環境で使用されます。

表18 Ubuntuプロキシ設定

設定	説明
ユーザー ID	Webプロキシにアクセスするためのユーザー IDを入力します。
パスワード	Webプロキシにアクセスするためのパスワードを入力します。
プロキシURL	Webプロキシにアクセスするための完全なURLを入力します。 例: http://web-proxy.company.com:8080
ユーザーエージェント	必要な場合、プロキシサーバーに渡すユーザーエージェントを指定します。

Ubuntuパッチ設定: リポジトリの設定

使用環境のリポジトリの設定を定義します。リポジトリの設定には、対象のUbuntuリポジトリと、SAでのその保存方法が含まれます。

表19　Ubuntuリポジトリ設定

設定	説明
Ubuntu URL	Ubuntuリポジトリにアクセスするための完全なURLを入力します。 例e: http://archive.ubuntu.com/ubuntu/dists/
リポジトリ	使用する1つ以上のリポジトリを選択します。 **セキュリティ**: セキュリティパッケージをインポートします。 **更新**: 公式なパッケージに更新をインポートします。
スイートコード名	次のUbuntuスイートコード名を指定します。 Precise Pangolin
コンポーネント名	次のUbuntuコンポーネント名を指定します。 **Main**: 公式にサポートされるソフトウェア。配布の大部分を占め、Ubuntuでサポートされています。 **Restricted**: 無償ライセンスで利用できないサポート対象のソフトウェア。このソフトウェアはUbuntuでサポートされています。 **Universe**: コミュニティによって維持されるソフトウェア、すなわち公式にはサポートされないソフトウェア。(注: このリポジトリにあるソフトウェアはすべて、Ubuntuチームのサポート対象外です。Ubuntuセキュリティチームでは、Universeリポジトリのソフトウェアのレビューや更新は一切行いません。) **Multiverse**: 無償でないソフトウェア。(注: このリポジトリにあるソフトウェアはすべて、Ubuntuチームのサポート対象外です。Ubuntuセキュリティチームでは、Multiverseリポジトリのソフトウェアのレビューや更新は一切行いません。)
アーキテクチャー	環境内のSAでサポートされるUbuntuアーキテクチャーを選択します。 32ビットまたは64ビットを選択できます。
リポジトリポリシー名形式	リポジトリポリシーの作成時に、Ubuntuリポジトリパスに加えて日付と時刻を含めるかどうかを選択します。次の形式を使用できます。 **Ubuntuパスを使用**: リポジトリポリシーの作成時に、Ubuntuパスだけを使用します。 **Ubuntuパスに日付を追加**: リポジトリポリシーの作成時に、Ubuntuパスに年-月-日を追加します。 **Ubuntuパスに日付と時刻を追加**: リポジトリポリシー名の作成時に、Ubuntuパスに年-月-日-時:分を追加します。

Ubuntuパッチ設定: ポリシー設定の構成

[ポリシー設定] セクションを使用して、Ubuntuパッチポリシーを処理するデフォルト設定を指定します。

表20 Ubuntuポリシー設定

設定	説明
依存パッケージを自動的に含める	Ubuntuパッチ修復ジョブに依存パッケージを自動的に含めさせるかどうかを指定します。 **はい**: 依存パッケージはUbuntuパッチ修復ジョブにデフォルトで含められます。 **いいえ**: 依存パッケージはUbuntuパッチ修復ジョブに手動で追加する必要があります。
スキャン結果に基づくインポート	インポート内容をフィルターして、環境に必要なものだけをインポートするかどうかを指定します。注: ポリシーのベストプラクティスとして、デフォルト値を「はい」のままにしておくことを推奨します。 **はい**: (デフォルト) スキャンが実行され、結果に基づいてインポート内容がフィルターされます。 **いいえ**: 先にスキャンを実行せずに、すべてのコンテンツがインポートされます。
すべてのパッケージをダウンロードする	リポジトリからのすべてのUbuntuパッケージのインポートを制御します。 **はい**: ポリシー作成時にUbuntuパッケージをインポートします。 **いいえ**: 環境に必要なパッケージを決定するためのスキャンが実行されるまでUbuntuパッケージのダウンロードを遅らせます。
運用要件ファイル	運用環境で必要なパッケージを特定するSAスライスサーバーまたは1つのコアサーバー上のファイルへの完全パスを入力します。Ubuntuパッチまたはパッケージの更新を実行する前に、このサーバーにログインする必要があります。 パッケージインポーターが実行されると、Ubuntuメタデータカタログの情報と一致するパッケージがこのリストからインポートされます。
静的ポリシーの作成	リポジトリに定義されたDebianパッケージに基づいて静的ポリシーを作成できるかどうかを決定します。 **はい**: 静的ポリシーの作成を有効にします。 **いいえ**: 静的ポリシーの作成を無効にします。
パッケージポリシー名形式	パッケージポリシーの作成時に、Ubuntuリポジトリパスに加えて日付と時刻を含めるかどうかを選択します。 **Ubuntuパスを使用**: パッケージポリシー名の作成時に、Ubuntuパスだけを使用します。 **Ubuntuパスに日付を追加**: パッケージポリシー名の作成時に、Ubuntuパスに年-月-日を追加します。 **Ubuntuパスに日付と時刻を追加**: パッケージポリシー名の作成時に、Ubuntuパスに年-月-日-時:分を追加します。

Ubuntuパッチ設定: スキャナーの動作の指定

[スキャナーの設定] セクションを使用して、Ubuntuスキャナーの動作を設定します。

表21　　Ubuntuスキャナーの設定

設定	説明
Ubuntuスキャナーを有効にする	Ubuntuスキャナーを有効にするかどうかを決定します。 **はい**: Ubuntuスキャナーを有効にします。 **いいえ**: Ubuntuスキャナーを無効にします。 **注**: Ubuntuスキャナーは、Ubuntuパッチにおいて非常に重要な機能です。このオプションが無効の場合、Ubuntuパッチ機能は実質的に無効になります。
暗黙のスキャンポリシーを使用する	暗黙のスキャンポリシーを有効にすると、デフォルトで最新のUbuntuリポジトリポリシーがインポートされるため、変更されたポリシーをサーバーに手動でアタッチする必要がなくなります。 **はい**: 暗黙のスキャンポリシーを有効にします。 **いいえ**: 暗黙のスキャンポリシーを無効にします。Ubuntuリポジトリポリシーをサーバーに手動でアタッチする必要があります。
ロギングオプション	スキャンおよび修復時の管理対象サーバーのロギングオプションを定義します。 **エラーのみ**: エラーのみをログに記録します。 **エラーおよび警告メッセージ**: エラーおよび警告メッセージをログに記録します。 **エラーおよびデバッグメッセージ**: エラーおよびデバッグメッセージをログに記録します。 **エラーおよび情報のみ**: エラーおよび情報メッセージだけをログに記録します。
リポジトリスコープ	管理対象サーバー上のリポジトリスコープを定義します。 **パブリック**: 管理対象サーバー上でリポジトリをパブリックに維持します。 **プライベート**: 管理対象サーバー上でリポジトリをプライベートに維持します: repoコントロールファイルはSAが使用した後で削除され、次の機会に再作成されます。
リポジトリファイル名	管理対象サーバー上に作成するリポジトリファイルの名前を入力します。
リポジトリディレクトリ	管理対象サーバー上に作成するリポジトリディレクトリの名前を入力します。
スキャナーハンドラーディレクトリ	管理対象サーバー上に作成するハンドラーディレクトリの名前を入力します。
すべてのパッケージの情報をリスト表示する	現在のリポジトリに存在しないものも含めて、すべてのパッケージのインストール情報を取得できるかどうかを決定します。 **はい**: 管理対象サーバー上にインストールされているすべてのパッケージの情報を取得します。 **いいえ**: 現在のリポジトリにあるインストール済みパッケージの情報だけを収集します。
デバッグサーバー	デバッグサーバーのリスト

Ubuntuパッチ設定: 一般ロギングオプションの指定

[一般] セクションを使用して、エラーのロギング方法を指定できます。

表22　　Ubuntuの一般ロギング設定

設定	説明
ロギングオプション	Ubuntuインポーターのロギングオプションを選択します。 **エラーのみ**: エラーのみをログに記録します。 **エラーおよび警告メッセージ**: エラーおよび警告メッセージをログに記録します。 **エラーおよびデバッグメッセージ**: エラーおよびデバッグメッセージをログに記録します。 **エラーおよび情報のみ**: エラーおよび情報メッセージをログに記録します。

Ubuntuパッチ管理のタスク

この項では、Ubuntuパッケージに関する情報の検索と管理の方法について説明します。

- パッケージ情報の表示
- パッケージの依存関係と優先度
- Ubuntuパッケージの表示
- Ubuntuパッケージプロパティの編集
- Ubuntuパッケージがインストールされたサーバーの確認
- Ubuntuパッケージがインストールされていないサーバーの確認
- SAクライアントライブラリからのUbuntuパッチのインポート
- Ubuntuパッケージのエクスポート

パッケージ情報の表示

パッケージに関する詳細 (プロパティ) を表示するには、次の手順を実行します。

1. ナビゲーションペインで [**ライブラリ**] を選択します。**[タイプ別] タブで、[パッケージ] > [Ubuntu] を選択します。**
2. [**Ubuntu**] を展開して、特定のUbuntuオペレーティングシステムを選択します。

   内容ペインに、選択したオペレーティングシステムに関連するすべてのパッケージが表示されます。
3. 内容ペインで、パッケージを開いて [パッケージ: プロパティ] ウィンドウを表示します。

[**F1**] キーを押すと、[パッケージ: プロパティ] ウィンドウに表示されるフィールドの説明が表示されます。

パッケージの依存関係と優先度

パッケージメタデータでは、パッケージとUbuntu製品間やパッケージ間の既知の依存関係と優先度がすべて識別されます。

HP Server Automationでは、次の依存関係と優先度が識別されます。

- **依存関係**の関係では、特定のパッケージをインストールする際にサーバー上にすでに存在している必要のあるUbuntu製品が識別されます。
- **優先度**の関係では、他のパッケージを置き換えるパッケージや他のパッケージで置き換えられるパッケージが識別されます。Ubuntuのパッチ管理では、「これが優先するもの」はパッケージが別のパッケージを置き換えることを意味し、「これよりも優先するもの」はインストールするパッケージが別のパッケージで置き換えられることを意味します。

HP Server AutomationのUbuntuパッチ管理では、2つのパッケージが相互に排他的(インストールできるのはいずれか一方で、両方をインストールすることはできない)かどうかは検出されません。そのため、パッチ管理で1つのサーバーに両方のパッケージがインストールされるのを防ぐことはできません。つまり、優先順位が低いパッケージと優先順位が高いパッケージが両方ともUbuntuサーバーで推奨されている場合は、両方のパッケージをサーバーにインストールできます。

Ubuntuパッケージの表示

SAクライアントには、Server Automationにインポート済みのUbuntuパッケージに関する情報が表示されます。

パッケージに関する情報を表示するには、次の手順を実行します。

1. ナビゲーションペインで[**ライブラリ**]を選択します。**[タイプ別]タブで、[パッケージ]>[Ubuntu]を選択します。**
2. [**Ubuntu**]を展開して、特定のUbuntuオペレーティングシステムを選択します。

   内容ペインに、選択したUbuntuオペレーティングシステムのUbuntuパッケージデータベース内に存在するすべてのパッケージが表示されます。
3. (オプション)列セレクターを使用して、名前、タイプ、場所、最終更新日時、最終更新者、サイズに基づいてパッケージをソートします。
4. 内容ペインで、パッケージを開いて[パッケージ]ウィンドウにプロパティを表示します。

Ubuntuパッケージプロパティの編集

パッケージの名前と説明を編集できます。

パッケージのプロパティを編集するには、次の手順を実行します。

1. ナビゲーションペインで[**ライブラリ**]を選択します。**[タイプ別]タブで、[パッケージ]>[Ubuntu]を選択します。**
2. [**Ubuntu**]を展開して、特定のUbuntuオペレーティングシステムを選択します。

   内容ペインに、選択したUbuntuオペレーティングシステムのUbuntuパッケージデータベース内に存在するすべてのパッケージが表示されます。
3. 内容ペインで、パッケージを開いて[パッケージ]ウィンドウにプロパティを表示します。
4. 次のフィールドを編集します。名前と説明
5. [**ファイル**]メニューの[**保存**]を選択して、変更内容を保存します。

Ubuntuパッケージの検索

特定のUbuntuサーバーのパッケージを検索するには、次の手順を実行します。

1 ナビゲーションペインで、[**デバイス**] > [**サーバー**] > [**すべての管理対象サーバー**] を選択します。

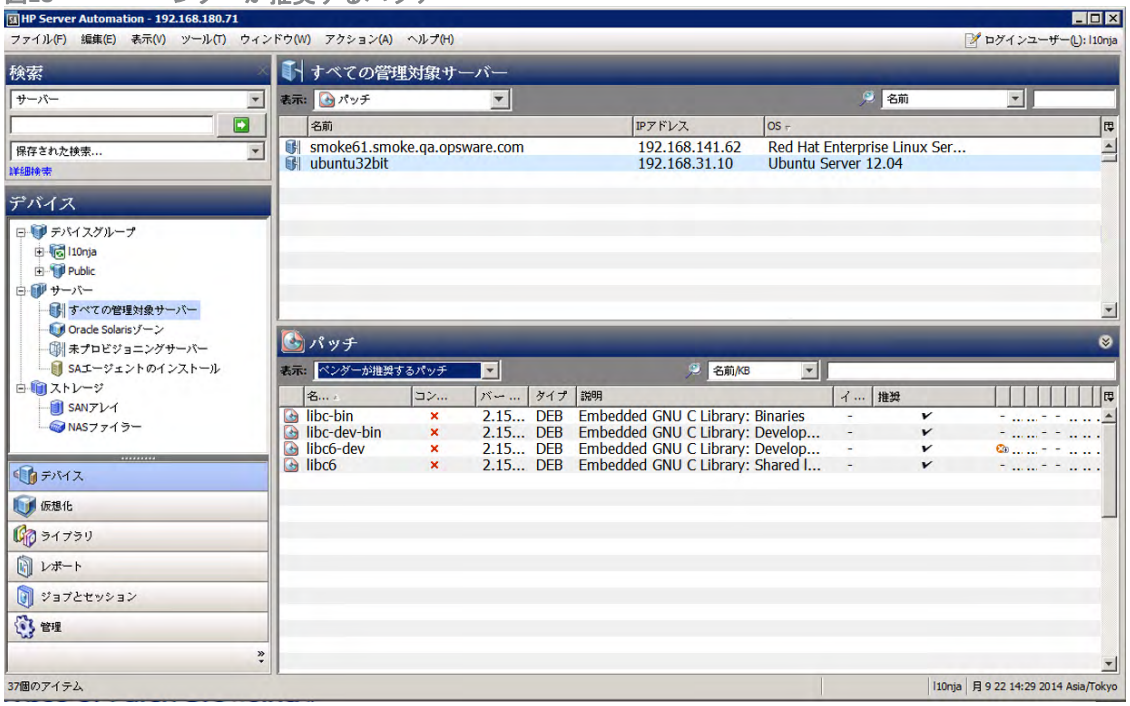
2 [表示] ドロップダウンリストから、[**パッチ**] を選択します。

3 内容ペインで、SAエージェント 5.5およびUbuntuを実行しているサーバーを選択します。

4 プレビューペインで、[表示] ドロップダウンリストを使用して、次のいずれかをパッチの詳細に選択します。

- 必要とされるパッチ
- ベンダーが推奨するパッチ (詳細は、図28を参照)
- ポリシーまたは例外のあるパッチ
- インストール済みのパッチ
- 例外のあるパッチ
- すべてのパッチ

図28 ベンダーが推奨するパッチ



[パッチ] ウィンドウに次の値が表示されます。

- 名前 - パッチの名前。
- コンプライアンス - パッチが使用しているUbuntuサーバーのバージョンに準拠しているかどうかを示します。
- バージョン - パッチのバージョン。
- パッチのタイプ - Debianパッケージ。
- 説明 - パッチの説明。

- インストール済み - パッチが特定のサーバーにインストール済みかどうかを示します。
- 推奨 - パッチがベンダー推奨かどうかを示します。
- 例外 - パッチに例外が含まれているかどうかを示します。
- セキュリティ情報 - Ubuntuセキュリティ勧告のセキュリティ情報番号。
- ベンダーパッチキー - ベンダーパッチキー。
- リリース日 - パッチが提供された日付。
- 公開時刻 - パッチのインストール時刻とパッチのリリース時刻との差により求められた期間
- アクション - スキャナーから取得した情報。
- カテゴリ - パッチカテゴリ。
- レーティング - パッチのインストールが必須かオプションかを示します。
- オブジェクトID - パッチのオブジェクトID。

—

Ubuntuパッケージがインストールされたサーバーの確認

特定のパッケージがインストールされたサーバーを確認するには、次の手順を実行します。

1. ナビゲーションペインで [**ライブラリ**] を選択します。**[タイプ別] タブで、[パッケージ] > [Ubuntu] を選択します。**
2. [**Ubuntu**] を展開して、特定のUbuntuオペレーティングシステムを選択します。

   内容ペインに、選択したオペレーティングシステムに関連するすべてのパッケージが表示されます。
3. 内容ペインで、パッケージを選択します。
4. 内容ペインの [検索] ドロップダウンリストから、[**サーバーの使用状況**] を選択します。

   このリストのサーバーを参照して、すべてのインストール済みのパッケージのリストを表示することができます。このリストには、Ubuntuの [プログラムの追加と削除] で表示するリストよりも詳細なインストール済みのパッチのリストが表示される場合があります。

ヒント:リストの各バイナリについて、[公開時刻] 列にリリース日とインストール日との差分が表示され、脆弱性の分析に役立ちます。

特定のパッケージがインストールされたサーバーを確認する別の方法として、次の手順を実行します。

1. ナビゲーションペインで、[**詳細検索**] リンクをクリックします。
2. [詳細検索] ペインで、[**検索対象**] フィールドで [**サーバー**] を選択します。
3. [場所:] を [インストール済みソフトウェア] に設定します。
   a. 適切な値 (次の値に等しい、次の値を含むなど) を設定します。
   b. パッチ名を指定します。
4. [**検索**] ボタンを押します。

Ubuntuパッケージがインストールされていないサーバーの確認

特定のパッケージがインストールされていないサーバーを確認するには、次の手順を実行します。

1. ナビゲーションペインで [**ライブラリ**] を選択します。**[タイプ別] タブで、[パッケージ] > [Ubuntu] を選択します。**
2. [**Ubuntu**] を展開して、特定のUbuntuオペレーティングシステムを選択します。

   内容ペインに、選択したオペレーティングシステムに関連するすべてのパッケージが表示されます。
3. 内容ペインで、パッケージを選択します。
4. [表示] ドロップダウンリストで [**サーバーの使用**] を選択します。

SAクライアントライブラリからのUbuntuパッチのインポート

UbuntuパッケージはUbuntuのWebサイトからダウンロードし、Server Automationにインポート (アップロード) します。パッケージがインポートされたかどうかを確認するには、パッケージの可用性プロパティを表示します。インポート済みパッケージの可用性は、制限付き、利用可能、または非推奨のいずれかになります。

SAクライアントでパッチをインポートするには、次の手順を実行します。

1. ナビゲーションペインで [**ライブラリ**] を選択します。**[タイプ別] タブで、[パッケージ] > [Ubuntu] を選択します。**
2. [**Ubuntu**] を展開して、特定のUbuntuオペレーティングシステムを選択します。

   内容ペインに、選択したオペレーティングシステムに関連するすべてのパッケージが表示されます。
3. 内容ペインで、パッケージを選択します。
4. UbuntuのWebサイトからパッケージを直接インポートするには、[**アクション**] メニューから、[**内容のインポート**] > [**ベンダーからインポート**] を選択します。

   [ベンダーからインポート] ウィンドウに、UbuntuのWebサイト上のパッケージの場所のURLが表示されます。(オプション) このURLはオーバーライドできます。

   または

   ローカルファイルシステムにダウンロード済みのパッケージをインポートするには、[**アクション**] メニューから、[**インポート**] > [**ファイルからインポート**] を選択します。

   ファイルブラウザーウィンドウで、パッケージを確認します。
5. [**インポート**] をクリックします。

[管理対象サーバー] ビューからのUbuntuパッチの内容のインポート

[管理対象サーバー] ビューの [内容のインポート(I)] メニューオプションを使用して、ファイルからパッケージの内容をインポートできます。Ubuntuパッケージの内容 (バイナリ) は、ベンダーから直接インポートすることもできます。

[管理対象サーバー] ビューからパッチの内容をインポートするには、次の手順を実行します。

1. パッチの管理 (読み取り/書き込み) 権限でSAクライアントにログインします。
2. [**デバイス**] > [**すべての管理対象サーバー**] に移動します。
3. ビューで、[**パッチ**] を選択します。
4. [パッチ] の内容ペインで、1つまたは複数のパッケージを選択します。

5 右クリックして、[**内容のインポート(I)**] を選択し、[**ベンダーから(V)...**] または [**ファイルから(F)...**] を選択します。

1つのパッケージの内容は、ローカルファイルまたは直接ベンダーからダウンロードできます。ただし、複数のパッケージを選択した場合は、[**ベンダーから(V)...**] オプションのみを使用できます。

6 **ベンダーから(V)...**: このオプションを使用して、パッケージの内容をベンダーから直接インポートできます。(**注**: このオプションは、Ubuntuパッケージにのみ使用できます。)

7 **ファイルから(F)...**: このオプションを使用して、SAクライアントを実行しているシステムからアクセス可能なローカルファイルから、パッケージの内容をインポートできます。

Ubuntuパッケージのエクスポート

HP Server Automationからローカルファイルシステムにパッケージをエクスポートするには、次の手順を実行します。

1 ナビゲーションペインで [**ライブラリ**] を選択します。**[タイプ別] タブで、[パッケージ] > [Ubuntu] を選択します。**

2 [**Ubuntu**] を展開して、特定のUbuntuオペレーティングシステムを選択します。

内容ペインに、選択したオペレーティングシステムに関連するすべてのパッケージが表示されます。

3 内容ペインで、パッケージを選択します。

4 [**アクション**] メニューで、[**エクスポート**] を選択します。

5 [パッチのエクスポート] ウィンドウで、パッケージファイルを含むフォルダー名を [ファイル名] フィールドに入力します。

6 [**エクスポート**] をクリックします。

ポリシー管理

Ubuntuパッチ管理で、パッチポリシーおよびパッチポリシー例外を使用すると、環境内でのパッチ配布をカスタマイズすることができます。ポリシーおよび例外では、管理対象サーバーにインストールするUbuntuパッケージまたはインストールしないUbuntuパッケージを定義します。

これらのポリシーや例外で規定するモデルに従ってサーバー環境でパッチを適用することも、モデルとは異なる形でパッチを適用することもできます。パッチポリシーや例外に従わず、アドホックなパッチインストールを行う場合は、修復を行う必要があります。修復を行うことで、適用可能なパッケージをサーバー上にインストールすることが可能になります。

パッチポリシー

パッチポリシーは、SAの管理対象サーバー上にインストールするパッケージのグループです。1つのパッチポリシーのパッケージはすべて、同じUbuntuオペレーティングシステムに適用する必要があります。

パッチポリシーを使用することで、柔軟なパッケージの配布が可能になります。たとえば、営業部門で使用するサーバーのみに配布するセキュリティパッケージを含むパッチポリシーを作成することができます。また、サーバー上にすでにインストールされている特定のソフトウェア (Exchange Server、Internet Information Services (IIS)、SQL Serverなど) に適用可能なセキュリティパッケージを含むパッチポリシーを作成することもできます。または、Ubuntuが重要なパッケージに指定したすべてのパッケージを含むパッチポリシーを作成し、組織内のすべてのユーザーが使用するすべてのサーバーにインストールすることができます。

➤ パッチポリシーを作成しない場合は、(オペレーティングシステム別の) ベンダー推奨のパッケージセットをデフォルトのパッチポリシーとして使用できます。

パッチポリシーはサーバーまたはサーバーグループに必要なだけアタッチできます。1つのサーバーに複数のポリシーをアタッチした場合、インストールは累積的に実行され、アタッチされたすべてのポリシーのすべてのパッケージがサーバー上にインストールされます。[修復]ウィンドウでは、修復する個別のパッチポリシーを選択できます。サーバーにアタッチされているすべてのポリシーを修復する必要はありません。パッチポリシーをネストすることはできません。

パッチポリシーの説明が定義されている場合は、モデルリポジトリのサーバーのパッチ状態にその説明が記録されます。パッチ管理ではこの情報を使用して、パッチコンプライアンス用にパッチポリシーに関するレポートを作成できます。パッチコンプライアンスでは、パッチポリシーと対応するパッチポリシー例外とを比較します。

Ubuntuのパッチ管理は、次のタイプのパッチポリシーをサポートしています。

- **ユーザー定義のパッチポリシー**: このタイプのパッチポリシーでは、ポリシー内に必要なパッケージを指定できます。ユーザー定義のパッチポリシーは、必要なアクセス権を持つユーザーが編集または削除できます。

  このタイプのパッチポリシーを使用すると、ポリシー設定担当者はパッケージを選択することができます。ポリシー設定担当者は、ベンダー推奨のパッチポリシーで利用可能なすべてのパッケージのサブセットから成るユーザー定義のパッチポリシーを作成できます。これにより、ポリシー設定担当者は、それぞれの環境に必要なパッチのみを適用することができます。
- **動的パッチポリシー**: パッケージのメンバーシップは、Ubuntuパッケージメタデータに基づいて、個別のUbuntu管理対象サーバースキャン結果によって定義されます。動的パッチポリシーはシステムで定義されるため、ユーザーが編集または削除することはできません。

エクスポートできるのはユーザー定義のパッチポリシーだけです。ベンダー推奨のパッチポリシーをエクスポートすることはできません。

パッチポリシーには、次の特性があります。

- パッチポリシーにはそれぞれ名前があり、(必要に応じて)パッチの目的を示す説明を追加することができます。
- パッチポリシーはユーザー定義またはベンダー定義のいずれかです。
- パッチポリシーにサブポリシーはありません。継承は存在しません。
- パッチポリシーはカスタマー独立です。つまり、パッチポリシー内のパッチは、関連するカスタマーに関係なく、任意の管理対象サーバーにインストールできます。詳細については、『SAユーザーガイド: Server Automation』を参照してください。
- パッチポリシーは常にパブリックです。
- パッチポリシーは、任意の数のサーバーまたはパブリックデバイスグループにアタッチできます。
- 複数のパッチポリシーを1つのサーバーまたはパブリックデバイスグループにアタッチできます。
- ユーザー定義のパッチポリシーは、アクセス権を持つユーザーが作成、編集、削除できます。

ポリシー適用の優先ルール

複数のパッチポリシーおよびパッチポリシー例外を作成して、サーバーに直接アタッチするか、サーバーグループにアタッチすることで、サーバーにインストールするパッケージやインストールしないパッケージを制御できます。パッチ管理での優先順位の階層によって、パッチのインストールに対するパッチポリシーまたはパッチポリシー例外の適用方法が決まります。この階層は、パッチポリシーまたはパッチポリシー例外がサーバーまたはデバイスグループのどちらのレベルでアタッチされているかに基づいています。

ポリシーおよび例外には、次の優先ルールが適用されます。

- サーバーに直接アタッチされたパッチポリシー例外は、サーバーに直接アタッチされたパッチポリシーよりも常に優先されます。

- サーバーに直接アタッチされたパッチポリシーは、パブリックデバイスグループにアタッチされたパッチポリシーやパッチポリシー例外よりも優先されます。
- パブリックデバイスグループにアタッチされたパッチポリシー例外は、パブリックデバイスグループにアタッチされたパッチポリシーよりも優先されます。
- サーバーが複数のパブリックデバイスグループに含まれる場合、同じパッケージ内では、[常にインストールしない] のパッチポリシー例外の方が [常にインストール] のパッチポリシー例外よりも常に優先されます。

修復プロセス

SAの修復の基本事項については、『SA ユーザーガイド : ソフトウェア管理』のソフトウェアの修復とインストールを参照してください。

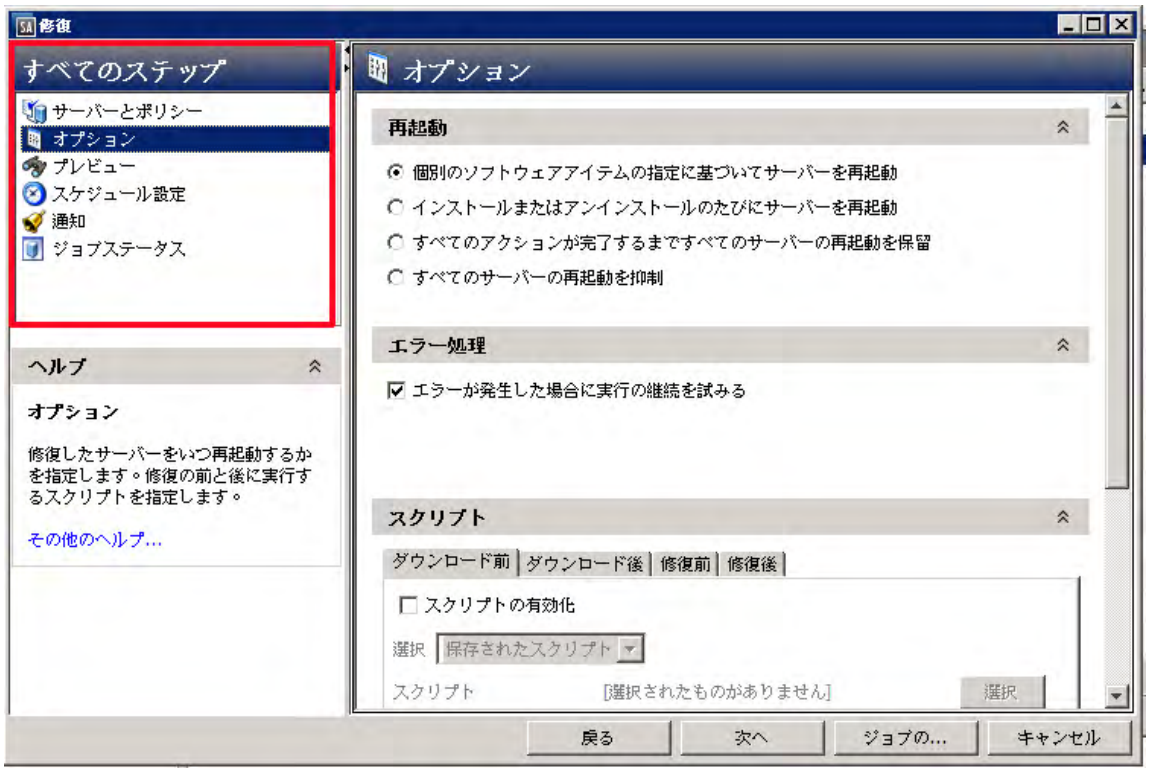
パッチコンプライアンスを確保するため、Ubuntuパッチ管理は脆弱性のある管理対象サーバーを識別し、修復プロセスを実行したときに複数のサーバーに同時にパッケージをデプロイします。修復プロセスでは、パッチポリシーがアタッチされている管理対象サーバーを調べて、パッチポリシー全体 (複数のポリシーを含む) を適用します。サーバーまたはサーバーグループでポリシーを修復するには、前もってサーバーまたはサーバーグループにポリシーがアタッチされている必要があります。

ベストプラクティス: 最新のUbuntuパッケージリリースを確認した後に、新しいパッケージをパッチポリシーに追加してポリシーを更新した場合は、修復を実行することをお勧めします。このような場合は、修復プロセスで需要予測情報が提供されます。これにより、このポリシーがアタッチされているサーバーがパッチポリシーの変更でどのように影響を受けるかを確認することができます。

修復プロセスで適用可能なパッケージの欠落が見つかった場合、これらのパッケージがサーバー上にインストールされます。

修復の条件を管理できるように、SAでは、修復オプションの指定、前と後のアクションの指定、修復プロセスのステータスを知らせるためのチケットIDと電子メール通知の設定を行うことができます。これらの条件は、[修復]ウィザードを使用して設定することができます。

図29 [修復]ウィザード



パッチポリシーの修復

このアクションを実行すると、管理対象サーバーにアタッチされているポリシー内のパッケージがインストールされます。このアクションでは、パッケージのアンインストールは行われません。パッチポリシーは、特定のサーバーでパッケージを常にインストールまたは常にインストールしないことを指定する例外でオーバーライドできます。

パッチポリシーを修復するには、次の手順を実行します。

1. ナビゲーションペインで[**ライブラリ**]を選択します。**[タイプ別]タブで、[パッケージ]>[Ubuntu]を選択します。**
2. [**Ubuntu**]を展開して、特定のUbuntuオペレーティングシステムを選択します。

   内容ペインに、選択したオペレーティングシステムに関連するすべてのパッチポリシーが表示されます。
3. 内容ペインで、パッチポリシーを開きます。
4. [表示]ドロップダウンリストから、[**サーバー**]を選択します。
5. 内容ペインの[表示]ドロップダウンリストから、[**ポリシーがアタッチされたサーバー**]を選択します。
6. プレビューペインで、1つまたは複数のサーバーを選択します。
7. [**アクション**]メニューから[**修復**]を選択します。

[修復] ウィンドウの最初のステップ: [サーバーおよびデバイスグループ] が表示されます。
各ステップの手順については、次の項を参照してください。

- 修復オプションの設定
- 修復の再起動オプションの設定
- 修復でのインストール前スクリプト/インストール後スクリプトの指定
- 修復でのパッチインストールのスケジュール設定
- 修復での電子メール通知の設定
- 修復のプレビューと開始

1つのステップが完了したら、[**次へ**] をクリックして次のステップへ進みます。[**ジョブの開始**] をクリックする前に、ステップリストに表示される完了したステップをクリックすることで、そのステップに戻って変更を行うことができます。

8 [**ジョブの開始**] をクリックして、修復ジョブを開始します。

ジョブを後で実行するようにスケジュール設定している場合でも、ジョブの開始後にパラメーターを変更することはできません。

修復オプションの設定

次の修復ポリシーオプションを指定できます。

いずれかのポリシーでエラーが発生した場合でも修復プロセスを中断しない。

このオプションを設定するには、次の手順を実行します。

1 [修復] ウィンドウで、[**次へ**] をクリックして [オプション] ステップに進みます。

2 再起動オプションを選択します。詳細については、修復の再起動オプションの設定 (189 ページ) を参照してください。

3 パッチやスクリプトでエラーが発生した場合でも修復プロセスを続行する場合は、[エラー処理] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

4 [**次へ**] をクリックして次のステップに進むか、[**閉じる**] をクリックして [修復] ウィンドウを閉じます。

修復の再起動オプションの設定

サーバーの再起動によるダウンタイムを最小限に抑えるため、パッチのインストール時にサーバーを再起動するタイミングを制御できます。

再起動オプションは、SAクライアントのUbuntuの次の場所で指定できます。

- [パッチのプロパティ] ウィンドウ—[インストールパラメーター] タブ
- [修復] ウィンドウ—[インストール前後のアクション] ステップ

ベストプラクティス: [修復] ウィンドウで再起動オプションを選択する場合、Hewlett PackardではUbuntuの再起動推奨設定 ([**個別のソフトウェアアイテムの指定に基づいてサーバーを再起動**] オプション) を使用することを推奨しています。Ubuntuの再起動設定を使用できない場合は、単一再起動オプション ([**すべてのパッケージがインストールまたはアンインストールされるまですべてのサーバーの再起動を保留します。**] オプション) を選択します。このようにしないと、次の再起動が (SAの制御対象外) 実行されるまで、サーバーにインストールされているパッチが正しく通知されない可能性があります。

[修復] ウィンドウの次のオプションでは、パッチのインストール後にサーバーを再起動するかどうかを指定します。これらのオプションは、[修復] ウィンドウで起動されるジョブのみに適用されます。これらのオプションによって、[パッチのプロパティ] ウィンドウの [インストールパラメーター] タブにある [再起動が必要] オプションが変更されることはありません。次に示すオプションの設定は、最初のオプションを除いて、[再起動が必要] オプションの設定よりも優先します。

- **個別のソフトウェアアイテムの指定に基づいてサーバーを再起動**(デフォルト): デフォルトでは、パッチプロパティまたはパッケージプロパティの[再起動が必要]オプションの設定に従って再起動が行われます。
- **インストールまたはアンインストールのたびにサーバーを再起動:** ベストプラクティスとして、個別のパッチまたはパッケージのベンダーの再起動設定に関係なく、パッチまたはパッケージをインストール/アンインストールするたびにサーバーを再起動します。
- **すべてのパッケージがインストールまたはアンインストールされるまですべてのサーバーの再起動を保留する**: 選択したパッチの中に[再起動が必要]オプションが設定されているものが含まれていても、他のパッチにそのオプションが設定されていない場合、すべてのパッチのインストール後にサーバーが1回再起動されます。選択したパッチの中に[再起動が必要]オプションが設定されているものがない場合、サーバーは再起動されません。
- **すべてのサーバーの再起動を抑制**: パッチプロパティの[再起動が必要]オプションが設定されている場合でも、サーバーを再起動しません(ベンダー設定によっては、抑制オプションを無視して強制的に再起動を行う場合があります)。

再起動オプションを設定するには、次の手順を実行します。

1. [修復]ウィンドウで、[**次へ**]をクリックして[オプション]ステップに進みます。
2. いずれかの再起動オプションを選択します。
3. [**次へ**]をクリックして次のステップに進むか、[**閉じる**]をクリックして[修復]ウィンドウを閉じます。

修復でのインストール前スクリプト/インストール後スクリプトの指定

パッチの修復では、修復の前または後に実行するコマンドまたはスクリプトを指定できます。インストール前スクリプトでは、たとえば、管理対象サーバー上で特定の条件をチェックすることができます。条件が満たされない場合やインストール前スクリプトが失敗した場合、パッチはインストールされません。インストール前スクリプトを使用すると、パッチを適用する前にサービスやアプリケーションをシャットダウンすることもできます。インストール後スクリプトを使用すると、管理対象サーバー上でクリーンアッププロセスを実行することができます。

修復の前または後に管理対象サーバー上で次のタイプのスクリプトを実行するように指定することができます。

- **ダウンロード前**: SAから管理対象サーバーにパッチをダウンロードする前に実行するスクリプト。[修復オプション]ステップで[ステージ]を選択した場合にのみ利用できます。
- **ダウンロード後**: SAから管理対象サーバーにパッチをダウンロードした後で、パッチをインストールする前に実行するスクリプト。[修復オプション]ステップで[ステージ]を選択した場合にのみ利用できます。
- **インストール前**: 管理対象サーバーにパッチをインストールする前に実行するスクリプト。
- **インストール後**: 管理対象サーバーにパッチをインストールした後に実行するスクリプト。

インストール前スクリプトを指定するには、次の手順を実行します。

1. [修復]ウィンドウで、[**次へ**]をクリックして[インストール前後のアクション]ステップに進みます。
2. [インストール前]タブを選択します。

   各タブでさまざまなスクリプトとオプションを指定できます。
3. [スクリプトの有効化]チェックボックスをオンにします。このオプションを選択すると、タブのフィールドの残りの部分が有効になります。[スクリプトの有効化]を選択しない場合、スクリプトは実行されません。
4. ドロップダウンリストから、[保存されたスクリプト]または[アドホックスクリプト]を選択します。

   保存されたスクリプトは、前にSA Webクライアントを使用してHP Server Automationに保存されたものです。スクリプトを指定するには、[**選択**]をクリックします。

アドホックスクリプトはこの操作に対してのみ実行され、SAに保存されません。タイプ (.batなど) を選択します。[スクリプト] ボックスに、スクリプトが存在する場所のドライブ文字を含むスクリプトの内容を入力します (`echo dir>> C:\temp\preinstall1.log`など)。ドライブ文字を入力しない場合、デフォルトは%SYSTEMDRIVE%になります。これは、Ubuntuのシステムフォルダーがインストールされている場所です。

5 スクリプトでコマンドラインフラグが必要である場合、[コマンド] テキストボックスにフラグを入力します。

6 [ユーザー] セクションで、システムがローカルシステムでない場合、名前を選択します。

7 システム名、パスワード、ドメイン名を入力します。

8 スクリプトがエラーを返した場合にインストールを停止するには、[エラー] チェックボックスを選択します。

9 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [修復] ウィンドウを閉じます。

修復でのパッチインストールのスケジュール設定

パッチをインストールする日時やパッチをダウンロードする日時をスケジュール設定できます。

パッチのインストールをスケジュール設定するには、次の手順を実行します。

1 [修復] ウィンドウで [スケジュール設定] ステップを選択します。

デフォルトでは、[スケジュール設定] ステップにはインストールフェーズ用のスケジュール設定オプションのみが表示されます。[修復オプション] ステップで [ステージ] を選択した場合、ダウンロードフェーズ用のスケジュール設定オプションも表示されます。

2 次のいずれかのスケジュール設定オプションを選択します。

- **分析のスケジュール**: 分析を実行する日付と時刻を指定できます。
- **ダウンロードのスケジュール**: ダウンロードとインストールを実行する日付と時刻を指定できます。
- **修復のスケジュール**: 修復プロセスを実行する日付と時刻を指定できます。

3 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [修復] ウィンドウを閉じます。

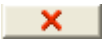
修復での電子メール通知の設定

ダウンロード操作やインストール操作が正常に終了した、あるいはエラーで終了したときに、ユーザーに知らせるために電子メール通知を設定できます。

電子メール通知を設定するには、次の手順を実行します。

1 [修復] ウィンドウで、[**次へ**] をクリックして [通知] ステップに進みます。

2 電子メールアドレスを追加するには、[**通知の追加**] をクリックして [通知電子メールアドレス] フィールドに電子メールアドレスを入力します。

3 ジョブが成功したときの通知ステータスを設定するには、  アイコンを選択します。ジョブが失敗したときの通知ステータスを設定するには、  アイコンを選択します。デフォルトでは、[通知] ステップにはインストールフェーズ用の通知ステータスのみが表示されます。[修復オプション] ステップで [ステージ] を選択した場合、ダウンロードフェーズ用の通知ステータスも表示されます。

4 [チケットID] フィールドに、このジョブに割り当てるチケットIDを入力します。

5 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [修復] ウィンドウを閉じます。

[修復オプション] ステップで [ステージ] を選択した場合、[通知] ペインにダウンロードとインストールの両方のフェーズに対する通知オプションが表示されます。

修復のプレビューと開始

修復のプレビューでは、サーバーのパッチの状態に関する最新のレポートが表示されます。プレビューは、管理対象サーバーにインストールされるパッチを確認するためのオプションステップです。プレビュープロセスでは、パッチのインストール対象として選択したサーバーに該当するパッチがすでにインストールされているかどうかを確認します。システム管理者がパッチを手動でインストールしている場合、サーバーにパッチがすでにインストールされている可能性があります。このような場合、パッチ管理ではパッチの存在を把握できません。

プレビューで、サマリーステップウィンドウに表示されるサーバー、デバイスグループ、およびパッチは、[**ジョブの開始**] をクリックすると、修復に送信されます。ベンダーで推奨されていないパッチは、このリストから除外されます。

このリストには、パッチポリシーやサーバーグループのメンバーシップの変更の有無に関係なく、パッチとそれに関係するサーバーが表示されます。修復をプレビューする場合、パッチポリシーやサーバーグループのメンバーシップが変更されている場合でも、これと同じサーバー、デバイスグループ、およびパッチのリストが使用されます。

[**プレビュー**] をクリックした後に [修復] ウィンドウでパラメーターを変更すると、プレビューで生成されるパッチ適用操作のシミュレートのサマリーが無効な内容になります。たとえば、[**プレビュー**] をクリックした後で、パッチ、パッチポリシー、サーバー、またはデバイスグループを追加した場合は、[**プレビュー**] を再度クリックして変更内容を結果に反映する必要があります。

修復のプレビューでは、パッチが適用済みの状態をシミュレートするためサーバーの動作に関するレポートは行われません。

修復をプレビューするには、次の手順を実行します。

1 [修復] ウィンドウの、[サーバーとポリシー] ステップで、サーバーまたはポリシーを選択します。

2 [**次へ**] をクリックするか、[オプション] ステップを選択して、再起動、エラー処理、およびスクリプトの設定を指定します。

3 [**次へ**] をクリックするか、[プレビュー] ステップを選択して、パッチのインストール時に実行される個々のアクションを表示します。

4 [プレビュー] ステップで、[**プレビュー**] をクリックしてプレビューしているアクションの詳細を表示します。

5 インストールジョブを起動するには、[**ジョブの開始**] をクリックします。

[スケジュール設定] ステップで [**分析後ただちに実行**] を選択した場合、ジョブはすぐに実行されます。特定の時刻を選択した場合、ジョブはその時刻に実行されます。

6 ジョブステータスが [修復] ウィンドウに表示されます。

ステータスバーとテキストで、テーブル内のアクションがどの程度完了したかを確認できます。次のアクションをサーバーごとに実行できます。

- **全体のサーバーステータス**: この修復ジョブに含まれるすべてのサーバーの全体ステータス。
- **分析**: SAは、インストールに必要なパッチの確認、管理対象サーバーにインストールされた最新パッチのチェック、他に実行が必要なアクション (ダウンロード、インストール、または再起動など) の確認を行います。
- **ダウンロード**: Server Automationから管理対象サーバーにパッチをダウンロードします。

- **インストール**: ダウンロードの完了後、パッチをインストールします。
- **再起動**: [オプション] ステップでこのアクションを指定すると、サーバーが再起動します。
- **登録**: ソフトウェアの登録を実行し、管理対象サーバーに現在インストールされているパッケージとパッチを取得します。
- **コンプライアンスのテスト**: コンプライアンススキャンを実行して、管理対象サーバーの現在のコンプライアンスステータスをレポートします。
- **スクリプトの実行**: [オプション] ステップでスクリプトを指定した場合、ダウンロードやインストールの前後にスクリプトが実行されます。
- **インストールと再起動**: ［オプション］ ステップで個々のパッチまたはパッケージの設定に従ってサーバーを再起動するように指定した場合、個別のパッチやパッケージがインストールされるとすぐにサーバーが再起動されます。

7 特定のアクションに関する詳細を追加表示するには、テーブルの行を選択して、下部のペインに内容を表示します。

または

8 ナビゲーションペインで、[ジョブとセッション] を選択してジョブに関する詳細を確認します。詳細については、ジョブログの表示 (44ページ) を参照してください。

9 [**ジョブの終了**] をクリックしてジョブを実行しないようにするか、[**閉じる**] をクリックして [修復] ウィンドウを閉じます。ジョブを終了できるのは、ジョブがスケジュール設定されている場合のみです。

(オプション) インストール、アンインストール、修復のキャンセルまたは終了 (86ページ) を参照してください。

パッチポリシーコンプライアンスの確認

管理対象サーバーがパッチポリシーや例外に適合しているかどうかを確認するには、次の手順を実行します。

1 ナビゲーションペインで、[**デバイス**] > [**すべての管理対象サーバー**] を選択します。

2 [表示] ドロップダウンリストから [コンプライアンス] を選択して、パッチコンプライアンスステータスを表示します。

3 特定のサーバーを選択するか、[**すべての行のチェックをオンにする**] をチェックして、詳細ペインにパッチコンプライアンスの詳細を表示します。いつでも [**すべての行のチェックをオフにする**] を選択して、サーバーの選択内容を変更することができます。

4 詳細ペインで、パッチの行を展開して、ステータスとコンプライアンスのサマリーの詳細を参照します。ステータスフィルターを使用して、コンプライアンスの表示設定を絞り込みます。デフォルトで、これは [**ステータスフィルターがありません**] に設定されています。

パッチポリシーの作成

パッチポリシーは、管理対象サーバー上にインストールする一連のパッチです。作成したばかりのパッチポリシーにパッチは含まれていません。また、サーバーにもアタッチされていません。

前述のとおり、Ubuntuパッチは単なる内部ソフトウェア/パッケージであるため、"パッチ設定"からインポートした際に、ライブラリ/パッケージ/Ubuntuに取り込まれます。ただし、タブのアイコンでは、パッチとパッケージが区別して表示されます。インポートされたパッチメタデータは、そのバイナリがまだインポートされていない場合は、薄いグレーのパッチアイコンで示されます。ユーザーは、[ライブラリ/パッケージ/Ubuntu] ビューのグレー表示のパッチを右クリックして、[ベンダーからインポート] または [ファイルからインポート] を選択して (Windows パッチの場合と同様)、バイナリをインポートできます。その後、アイコンは緑に変わります。

ユーザーは、[ライブラリ/パッチポリシー/Ubuntu] タブで右クリックし、[静的パッチポリシー] または [動的パッチポリシー] を選択して静的または動的パッチポリシーを作成することで、一般パッチポリシーを作成できます。ポリシー作成の新しい画面が表示されたら、ポリシーのオプションを選択します。ただし、[ポリシーアイテム] は、静的ポリシーにのみ使用できます。動的ポリシーにはアイテムがないため、動的ポリシーにはこのオプションは使用できません。

パッチポリシーを作成するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] を選択します。

2 特定のUbuntu オペレーティングシステムを選択します。

3 [**アクション**] メニューから、**[新規動的ポリシー (N)...] または [新規静的ポリシー (N)...]** を選択します。

4 [プロパティ] ウィンドウで、ポリシーに一意の名前を付けます。保存して閉じます。

5 内容ペインで、新規パッチポリシーを開きます。

6 (オプション) [プロパティ] の [名前] フィールドに、ポリシーの目的または内容を表す名前を入力します。

パッチポリシーの削除

このアクションでは、SAからパッチポリシーが削除されます。ただし、管理対象サーバーからパッチが削除またはアンインストールされることはありません。サーバーまたはサーバーグループにアタッチされているパッチポリシーを削除することはできません。ポリシーをSAから削除するには、事前にサーバーまたはサーバーグループからポリシーをデタッチする必要があります。

パッチポリシーをSAから削除するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] を選択します。

2 特定のUbuntu オペレーティングシステムを選択します。

3 メインウィンドウの内容ペインで、ポリシーを選択します。

[**アクション**] メニューで [**パッチポリシーの削除**] を選択します。

パッチポリシーへのパッチの追加

このアクションでは、パッチポリシーにパッチが追加されます。ただし、管理対象サーバー上にパッチをインストールするものではありません。パッチはポリシーを修復する際にインストールされます。

SAに対するパッチポリシーにパッチを追加するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] を選択します。

2 特定のUbuntuオペレーティングシステムを選択して、Ubuntuパッチのリストを表示します。

3 内容ペインで、パッチを選択します。

4 [表示] ドロップダウンリストから、[パッチポリシー] を選択します。

5 [表示] ドロップダウンリストで、[**パッチが追加されていないポリシー**] を選択します。

6 ポリシーを選択します。

7 [**アクション**] メニューで [**パッチポリシーに追加**] を選択します。

8 [パッチポリシーに追加] ウィンドウで、[**追加**] をクリックします。

パッチポリシーからのパッチの削除

このアクションでは、パッチポリシーからパッチが削除されます。このアクションによって、管理対象サーバーからパッチがアンインストールされ、SAからパッチが削除されることはありません。

パッチポリシーからパッチを削除するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。
2. 特定のUbuntuオペレーティングシステムを選択して、Ubuntuパッチのリストを表示します。
3. 内容ペインで、パッチを選択します。
4. [表示] ドロップダウンリストから、[**パッチポリシー**] を選択します。
5. [表示] ドロップダウンリストで、[**パッチが追加されたポリシー**] を選択します。
6. パッチを選択します。[**アクション**] メニューで [**パッチポリシーから削除**] を選択します。
7. [パッチをポリシーから削除] ウィンドウで、ポリシーを選択して [**削除**] をクリックします。

パッチポリシーのサーバーへのアタッチ

このアクションでは、パッチポリシーをサーバーまたはサーバーグループと関連付けます。このアクションは、サーバーまたはサーバーグループでポリシーを修復する前に行う必要があります。

ポリシーをアタッチするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] を選択します。
2. 特定のUbuntuオペレーティングシステムを選択して、Ubuntuパッチポリシーのリストを表示します。
3. 内容ペインで、パッチポリシーを選択します。
4. [表示] ドロップダウンリストから、[**サーバーの使用**] または [**デバイスグループの使用**] を選択します。
5. [表示] ドロップダウンリストから、[**ポリシーがアタッチされていないサーバー**] または [**ポリシーがアタッチされていないサーバーグループ**] を選択します。
6. プレビューペインで、1つまたは複数のサーバーを選択します。
7. [**アクション**] メニューで、[**サーバーのアタッチ**] を選択します。
8. [**アタッチ**] をクリックします。

パッチポリシーのサーバーからのデタッチ

このアクションでは、パッチポリシーは削除されません。また、管理対象サーバーからパッチがアンインストールされることもありません。

ポリシーをデタッチするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチポリシー**] を選択します。
2. 特定のUbuntuオペレーティングシステムを選択して、Ubuntuパッチポリシーのリストを表示します。
3. 内容ペインで、パッチポリシーを選択します。
4. [表示] ドロップダウンリストから、[サーバーの使用] (または [デバイスグループの使用]) を選択します。

5 [表示] ドロップダウンリストから、[**ポリシーがアタッチされたサーバー**] または [**ポリシーがアタッチされたサーバーグループ**] を選択します。

6 プレビューペインで、1つまたは複数のサーバーを選択します。

7 [**アクション**] メニューで、[**サーバーのデタッチ**] を選択します。

8 [**デタッチ**] を選択します。

パッチコンプライアンス

HP Server Automation では、管理対象サーバーとパブリックデバイスグループに対する適合テスト (コンプライアンスチェック) を実行して、ポリシーおよびポリシー例外のパッチがすべて正常にインストールされているかどうかを判断します。組織に合わせてパッチコンプライアンス情報を最適化するため、パッチコンプライアンスレベルを設定し、カスタマイズしたパッチコンプライアンスレベルのルールを編集することができます。

パッチコンプライアンススキャン

パッチコンプライアンススキャンでは、サーバーにインストールされているパッチを、サーバーにアタッチされているパッチポリシーやパッチポリシー例外と比較します。このスキャンの結果には、コンプライアンス状態 (必須のパッチがすべてインストールされている) のサーバーとコンプライアンス違反状態 (必須のパッチが一部インストールされていない) のサーバーが示されます。

パッチコンプライアンススキャンは、パッチ適用環境に応じて実行またはスケジュール設定する必要があります。たとえば、パッチポリシーを更新したり、Server Automation 以外で (使用せずに) パッチをインストールした場合は、SAのモデルが変更されていて、コンプライアンス情報の再計算が必要であるため、コンプライアンススキャンを実行する必要があります。SAでは、スキャンが必要の表示を用いて、このような状況を示します。この場合は、定期的なスキャンのスケジュールを待たずに、1 つまたは複数のサーバーでコンプライアンススキャンを開始することができます。

パッチコンプライアンススキャンを開始する方法

パッチコンプライアンススキャンは、次の方法で開始できます。

- **すぐに実行**: サーバーまたはグループを選択してから、メニュー項目を選択します。

  詳細については、パッチコンプライアンススキャンの即時開始 (197ページ) を参照してください。

- **定期的に実行**: スケジュールを設定します。

  詳細については、パッチコンプライアンススキャンのスケジュール設定 (202 ページ) を参照してください。デフォルトでは、スキャンはスケジュール設定されていません。

- **別のタスクの結果として実行**

  SA は、タスクの終了時に管理対象サーバー上でパッチコンプライアンススキャンを実行します (次の各項を参照)。

  — Ubuntuパッチのインストール (205ページ)

  — パッチポリシーの修復 (188ページ)

パッチコンプライアンススキャンの即時開始

パッチコンプライアンススキャンを手動で実行するには、空のポリシーを作成してサーバーまたはデバイスグループにアタッチします。

選択したサーバーでスキャンを開始するには、次の手順を実行します。

1. ナビゲーションペインで [**デバイス**] を選択します。
2. サーバーまたはデバイスグループのリストからエントリを選択します。
3. 右クリックで [**スキャン**] > [**パッチコンプライアンス**] を選択して [パッチコンプライアンススキャンステータス] ウィンドウを表示します。

選択したサーバーのコンプライアンスステータスの更新

Ubuntuサーバーのコンプライアンスステータスを更新すると、SAクライアントはWebサービスデータアクセスエンジンから最新のデータを取得します。更新では、Ubuntuサーバーのコンプライアンス情報の再スキャンは行われません。

1つまたは複数のサーバーのコンプライアンスステータスを更新するには、次の手順を実行します。

1. ナビゲーションペインで [**デバイス**] を選択します。
2. [表示] ドロップダウンリストから、[コンプライアンス] を選択します。
3. 内容ペインで、1つまたは複数のサーバーを選択します。
4. 右クリックで、[**サーバーの更新**] を選択します。
5. [ステータス] 列で変更されたコンプライアンス情報を確認します。

スキャンエラーの詳細の表示

スキャン操作に失敗した場合、サーバーがコンプライアンス状態かどうかを判断することができません。スキャン失敗はスキャン失敗アイコン で示されます。パッチコンプライアンススキャンが失敗した理由を確認するには、次の手順を実行します。

ナビゲーションペインで [**デバイス**] を選択します。

1. チェック対象のサーバーにドリルダウンします。
2. 内容ペインで、サーバーを選択します。
3. 右クリックで、[**スキャン**] > [**パッチコンプライアンススキャンエラーの詳細**] を選択します。
4. [パッチコンプライアンススキャンエラーの詳細] ウィンドウでサーバーを選択し、ウィンドウの下部に表示される詳細なエラーメッセージの内容を確認します。

パッチコンプライアンスのアイコン

HP Server Automationでは、表23に示すアイコンが表示されます。

表23　　パッチコンプライアンスステータスのアイコン

ステータス/アイコン	説明
コンプライアンス	サーバーはすべてのパッチでコンプライアンス状態です。サーバーにアタッチされているポリシーのパッチはすべて、ターゲットサーバー上にインストール済みです。
部分コンプライアンス	サーバーは一部のパッチで部分コンプライアンス状態です。これらのパッチには例外が設定されています。
非コンプライアンス	サーバー上にインストールされたパッチが、パッチポリシーで定義された条件と一致していません。
スキャン失敗	スキャン操作に失敗しました。パッチ管理でサーバーのコンプライアンスをチェックできません。

パッチの非コンプライアンスについて

サーバーまたはサーバーグループのパッチの非コンプライアンスステータスは、さまざまな要因で発生します。たとえば、サーバーにアタッチされたパッチポリシーの定義に基づいてインストールする必要のある適用可能なパッチが存在する場合などです。また、サーバーのパッチコンプライアンスレベルに影響する例外が存在する可能性もあります。

たとえば、パッチポリシーに「常にインストールしない」という例外に指定されたパッチがあるにも関わらず、ターゲットサーバーにそのパッチがインストールされている場合、サーバーは非コンプライアンスとみなされます。

また、他のパッチで置き換えられるパッチが推奨されるパッチで、ポリシーや例外に含まれている場合、これらのパッチはコンプライアンスの計算にカウントされ、ターゲットサーバーにこれらのパッチが存在しない場合、サーバーのパッチコンプライアンスステータスは非コンプライアンスになります。

パッチコンプライアンスレベル

パッチコンプライアンスレベルでは、それぞれのパッチコンプライアンスルールを定義します。パッチコンプライアンススキャンの結果には、ポリシーのみ、ポリシーと例外の両方、または独自にカスタマイズしたレベルを含めることができます。

Ubuntuパッチ管理では、次のコンプライアンスレベルがサポートされます。

- **ポリシーのみ**: サーバーにインストールされているパッチがパッチポリシーに準拠しているかどうかを確認します。
- **ポリシーと例外**: サーバーにインストールされているパッチがパッチポリシーや例外に準拠しているかどうかを確認します。ポリシーと例外が一致せず、例外の [理由] フィールドにデータがない場合、部分的アイコンが表示されます。
- **カスタマイズ済み**: このコンプライアンスレベル用に編集したルールを確認します。

パッチコンプライアンスルール

パッチコンプライアンスルールは、[管理対象サーバー] ウィンドウに表示されるコンプライアンスアイコンを決める条件です。

Ubuntuパッチ管理では、次のコンプライアンスルールがサポートされます。

- **ポリシーに追加されたパッチ**: パッチポリシーに追加されているパッチ。

- **サーバーにインストールされたパッチ**: 管理対象サーバーにインストールされているパッチ。
- **例外タイプ**: [例外タイプ] の値は次のとおりです。
  - **常にインストール**: パッチがポリシー内に存在しない場合でも、パッチはサーバーにインストールされます。
  - **常にインストールしない**: パッチがポリシーに存在する場合でも、パッチをサーバーにインストールしません。
  - **なし**: このパッチとサーバーに指定されている例外はありません。
- **例外の理由**: [ポリシー例外の設定] ウィンドウの [例外の理由] に入力した説明。[パッチコンプライアンスルール] ウィンドウの [例外の理由] の値は次のとおりです。
  - **はい**: [例外の理由] にデータがあります。
  - **いいえ**: [例外の理由] は空です。
  - **該当しない**: このパッチとサーバーに指定されている例外はありません。
- **コンプライアンス結果**: パッチコンプライアンスのスキャン結果を示すアイコン。これらのアイコンは [管理対象サーバー] ウィンドウに表示されます。

パッチ管理

パッチデータベース (メタデータ) のインポートに必要な前提条件

Ubuntuパッチデータベースをインポートする前に、SAコアとの通信時にWebプロキシを使用するようにSAクライアントを設定する必要があります。

SAクライアントを設定するには、次の手順を実行します。

1. [Log in to HP Server Automation Client] ウィンドウで、[**More**] をクリックしてウィンドウを展開します。
2. [**Advanced Settings**] をクリックして、[Advanced Settings] ウィンドウを開きます。
3. [Proxies] セクションで、次の手順を実行します。
   - ブラウザーと同じプロキシを使用する場合は、[Use Browser] を選択します。

   または
   - 異なるプロキシを設定する場合は、[Manual] を選択して SA コアの IP またはホスト名を [No Proxy Hosts] テキストボックスに入力します。これにより、SAクライアントがSAコアと直接通信できるようになります。

パッチの可用性の設定

デフォルトのパッチの可用性はSAクライアントを使用して設定できます。

SAクライアントを使用して新規にインポートされるパッチの可用性のデフォルト値を設定するには、次の手順を実行します。

1. ナビゲーションペインで、**[管理] > [パッチ設定]** を選択します。
2. [**インポート済みパッチのデフォルトの可用性**] ドロップダウンリストから、[**制限付き可用性**] または [**利用可能**] を選択します。

制限付き可用性(デフォルト)— 制限付き可用性のマークの付いたパッチはHP Server Automationにインポート済みで、必要なアクセス権を持つパッチ管理者のみがインストールできます。必要なアクセス権の取得については、システム管理者にお問い合わせください。これらのアクセス権については、『SA 管理ガイド』を参照してください。

利用可能—利用可能のマークの付いたパッチは、管理対象サーバー上にインストールできます。

•

Ubuntuパッチデータベースメタデータとパッケージのインポート

SAクライアントを使用してUbuntuメタデータをインポートするには、次の手順を実行します。

この手順を実行する前に、パッチデータベース (メタデータ) のインポートに必要な前提条件 (199ページ)を参照してください。

1 ナビゲーションペインで、[**管理**] > [**パッチ設定**] を選択します。

2 [**Ubuntu**] タブをクリックします。

3 プロキシが必要な場合は、[**プロキシ**] に値を設定します。プロキシにユーザー名、パスワード、またはユーザーエージェントが必要な場合は、必要に応じてこれらの値を設定します。

4 UbuntuリポジトリのメタデータをUbuntuのWebサイトからインポートするには、[**メタデータのインポート**] をクリックします。

[Ubuntu用リポジトリメタデータのインポート] ウィンドウにユニット全体の進行状況と、現在プロセス中のユニットが表示されます。

SAクライアントを使用してUbuntuパッケージをインポートするには、次の手順を実行します。

この手順を実行する前に、メタデータをインポートして、サーバーでパッチコンプライアンスのスキャンを実行します。サーバーのコンプライアンススキャンが完了したら、UbuntuパッチをSAクライアントを使用してインポートできます。

1 ナビゲーションペインで、[**管理**] > [**パッチ設定**] を選択します。

2 [**Ubuntu**] タブをクリックします。

3 UbuntuのWebサイトからデータベースをインポートするには、[**パッケージのインポート**] をクリックします。

[サーバースクリプトの実行] ウィンドウが表示され、実行するスクリプトが表示されます (デフォルトで、[Ubuntuパッケージのインポート] が選択されています)。パッケージのメタデータのみをインポートするには、[Ubuntuメタデータのインポート] に切り替えます。

スクリプトページには、バージョン、タイプ、場所 (インポート先)、説明などのスクリプトのメタデータも表示されます。

4 [**次へ**] をクリックするか、次の手順を選択して、サーバースクリプトの実行の手順を続行します。

a サーバーとグループ

b オプション

c スケジュール設定

d 通知

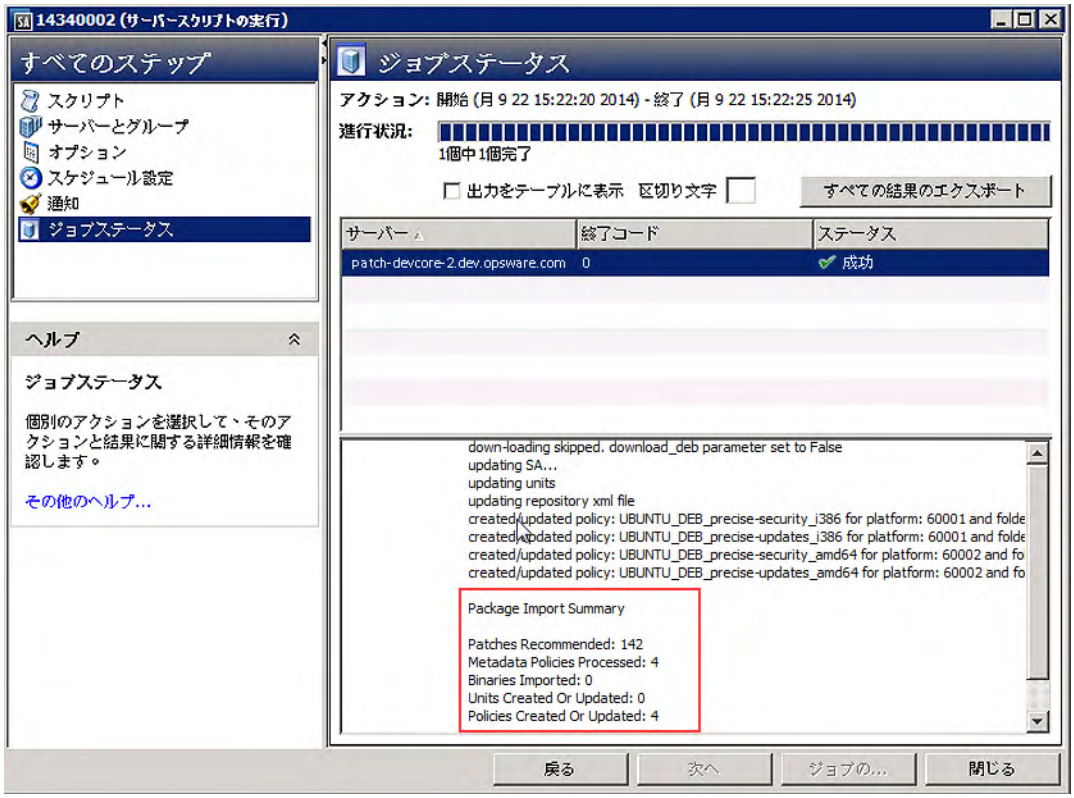
e ジョブステータス

➤ サーバースクリプトの実行の手順とオプションの詳細については、『SAユーザーガイド : Server Automation』のサーバースクリプトの実行の詳細を参照してください。

5 オプションの定義が完了したら、[**ジョブの開始**] をクリックします。

6 [ジョブステータス] にインポートのプロセス結果が表示されます。インポートのサイズによっては、インポートに時間が長くかかる場合があります。

インポートのジョブが完了したら、[ジョブステータス] にジョブのアクティビティの詳細が表示されます。任意のサーバーを選択して、そのサーバーのジョブの詳細情報のログを詳細ペインに表示できます。ジョブ結果のログの下部には、Ubuntuパッケージインポートの概要が含まれます。



パッチコンプライアンススキャンのスケジュール設定

すべてのUbuntu管理対象サーバーでのパッチコンプライアンススキャンをスケジュール設定するには、次の手順を実行します。

1 ナビゲーションペインで、**[管理]** > **[コンプライアンス設定]** を選択します (図30**を参照)。**

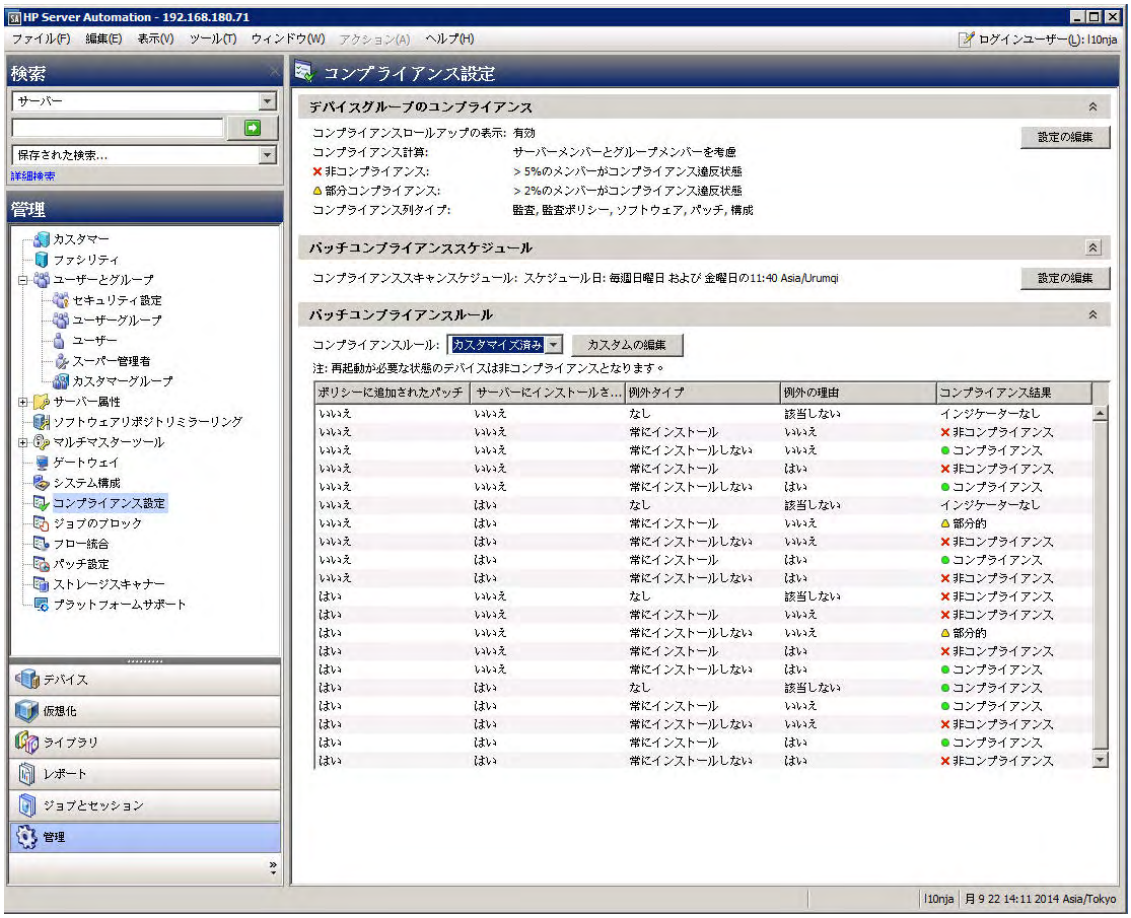


図30 コンプライアンススキャンのウィンドウ

2 [コンプライアンス設定] の内容ペインの [パッチコンプライアンススケジュール] セクションで、**[設定の編集]** をクリックします。

3 [コンプライアンススキャンのスケジュール] ウィンドウで、**[コンプライアンススキャンの有効化]** を選択します。

4 [スケジュール] ドロップダウンリストから、スキャンの頻度を選択します。

[カスタム] を選択した場合は、次の値を使用してcrontab文字列を指定します。

- 分 (0～59)
- 時間 (0～23)
- 日 (1～31)
- 月 (1～12)
- 曜日 (0～6、0=日曜)
- これらのフィールドにアスタリスク*を指定すると、可能なすべての値を表します。次のcrontab文字列を指定すると、平日の深夜0時にジョブが実行されます。

```
0 0 * * 1-5
```

crontab文字列は、シリアル値 (1,2,3,4) と範囲 (1-5) でも指定できます。詳細については、Unixコンピューター上のcrontabのmanページを参照してください。

5 [開始時刻] フィールドで、ジョブを開始する時刻を指定します。

6 [タイムゾーン] ドロップダウンリストから、ジョブ実行時刻のデフォルトタイムゾーンを選択するか、デフォルトのタイムゾーンを受け入れます。表示されたデフォルト時刻により、スケジュールされた時刻が [ユーザー設定] で設定したタイムゾーンに変換されます。希望のタイムゾーンを設定しなかった場合、タイムゾーンはHP Server Automationコアサーバーから導出されます (通常、UTC)。

7 [**OK**] をクリックして設定を保存します。

パッチコンプライアンスレベルの設定

パッチポリシーのコンプライアンスレベルでは、それぞれのパッチコンプライアンスレベルを定義します。

パッチコンプライアンスレベルを設定するには、次の手順を実行します。

1 ナビゲーションペインで、[**管理**] > [**コンプライアンス設定**] を選択します。

2 [コンプライアンスルール] ドロップダウンリストから、[ポリシーのみ]、[ポリシーと例外]、[カスタマイズ済み] のいずれかのコンプライアンスレベルを選択します。

[カスタマイズ済み] を選択する場合は、[**カスタムの編集**] をクリックして、[カスタマイズされたポリシーコンプライアンスレベルの編集] ウィンドウを開きます。コンプライアンスレベルを編集するには、[コンプライアンス結果] 列のアイコンをクリックします。[**適用**] をクリックして変更内容を保存します。

サポート対象のUbuntuバージョン

お使いのバージョンのSAでサポートされる管理対象サーバープラットフォームについては、『SA Support and Compatibility Matrix』を参照してください。

パッチロケールの構成タスク

デフォルトでは、Ubuntuパッチ管理は、英語のロケールのみをサポートしています。英語以外のロケールでのUbuntuパッチ適用をセットアップするには、次の各項の手順を実行します。

- 英語以外のロケールでのSAコアの構成 (203ページ)
- 英語以外のロケールを使用する場合のエンドユーザー要件 (204ページ)

英語以外のロケールでのSAコアの構成

このタスクでは、コアサーバー対するrootアクセスとSA Webクライアントの再起動が必要です。

コアを英語以外のロケール用に構成するには、SA Webクライアントを実行している各コアサーバーで次の手順を実行します。

1 rootとしてサーバーにログオンします。

2 /etc/opt/opsware/occ/psrvr.properties内の次の行を

pref.user.locales

次のように変更します

```
pref.user.localesAllowed=en;ja;ko
```

3 次のコマンドでコア上のSA Webクライアントを再起動します。

```
/etc/init.d/opsware-sas restart occ.server
```

4 テキストエディターで、次のファイルを開きます。

```
/opt/opsware/occclient/jnlp.tmpl
```

5 日本語の場合は、jnlp.tmplファイルの<resources>セクションに、次のXML要素を追加します。

```
<property name="com.opsware.ngui.font.japanese" value="Arial Unicode MS"/>
```

6 韓国語の場合は、jnlp.tmplファイルの<resources>セクションに、次のXML要素を追加します。

```
<property name="com.opsware.ngui.font.korean" value="Arial Unicode MS"/>
```

7 /opt/opsware/occclientディレクトリで、次のファイルが存在する場合は、これらのファイルを削除します。

```
$HOST_ja.jnlp
$IP_ja.jnlp
$HOST_ko.jnlp
$IP_ko.jnlp
```

英語以外のロケールを使用する場合のエンドユーザー要件

SAクライアントで英語以外のフォントを表示するには、次の手順を実行します。

1 SAクライアントを実行しているUbuntuデスクトップで、Arial Unicode MSフォントが使用されていることを確認します。

2 システム管理者が英語以外のロケールでのSAコアの構成（203ページ）の手順を実行した後に、エンドユーザーはSAクライアントにログオンして、SAクライアントウィンドウの右上にある[ログインユーザー]リンクを選択します。これにより、[ユーザー]ウィンドウが表示されます。[プロパティ]ビューを選択します。

3 [ユーザーのプロパティ]ビューで、エンドユーザーは[ユーザー設定]セクションの[ロケール]フィールドを更新します。たとえば、システム管理者がコアを日本語用に構成した場合、エンドユーザーは[ロケール]フィールドを日本語に設定します。

パッチのインストール

パッチ管理では、次の2つのフェーズでパッチをインストールします。

- **フェーズ1—ダウンロード/ステージング**: このフェーズでは、HP Server Automationから管理対象サーバーへパッチをダウンロードします。このフェーズは、一般的にステージングと呼ばれます。
- **フェーズ2—インストール/デプロイメント**: このフェーズでは、管理対象サーバーにパッチをインストールします。このフェーズは、一般的にデプロイメントと呼ばれます。

パッチがダウンロード（ステージング）されたらすぐにインストールを行うかどうかを指定できます。また、日時をスケジュール設定して後でインストールを行うこともできます。また、Ubuntuパッチ管理では、複数のパッチのベストエフォート型インストールのニーズにも対応しており、いずれかのパッチでエラーが発生した場合でも、パッチのインストールを続行するように指定することが可能です。

Ubuntuパッチ管理では、パッチをインストールするためにSAエージェントが管理対象サーバー上で実行するコマンドの名前（.debファイルや定義済みのコマンドライン引数など）が表示されます。これらのデフォルトのコマンドライン引数はオーバーライドできます。

パッチ管理では、Ubuntuパッチのインストールを適切に管理できるように、サーバーの再起動オプションの管理、インストール前 / インストール後スクリプトの指定、パッチのインストールのシミュレート (プレビュー)、インストールプロセスのステータスを通知する電子メール通知の設定などを行うことができます。これらの条件は、[パッチのインストール] ウィザードを使用して設定することができます。

Ubuntuパッチのインストール

パッチを管理対象サーバーにインストールするには、事前にパッチを HP Server Automation にインポートして、ステータスを利用可能にしておく必要があります。制限付きのマークの付いたパッチは、必要なアクセス権を持つ管理者がインストールできます。

パッチを管理するにはアクセス権が必要です。必要なアクセス権の取得については、システム管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

パッチとサーバーを明示的に選択してインストールを実行できます。また、パッチポリシー例外が [常にインストールしない] の場合でも、パッチをインストールすることができます。

管理対象サーバーまたはデバイスグループにパッチをインストールするには、次の手順を実行します。

1. ナビゲーションペインで [**デバイス**] > [**すべての管理対象サーバー**] または [**デバイスグループ**] を選択します。
2. 内容ペインで、サーバーまたはデバイスグループを選択します。
3. [表示] ドロップダウンリストで、[**ベンダーが推奨するパッチ**] を選択します。
4. 内容をインストール済みのパッチを右クリックし、[インストール] を選択します。

   [パッチのインストール] ウィンドウの最初のステップ : [サーバーおよびデバイスグループ] が表示されます。
   各ステップの手順については、次の項を参照してください。
   - Ubuntuインストールオプションの設定
   - Ubuntuパッチのインストールでの再起動オプションの設定
   - Ubuntuパッチのインストールでのインストールスクリプトの指定
   - Ubuntuパッチのインストールのスケジュール設定
   - Ubuntuパッチのインストールでの電子メール通知の設定
   - Ubuntuパッチのインストールのプレビュー
   - Ubuntuパッチのインストールジョブの進行状況の表示

   1つのステップが完了したら、[**次へ**] をクリックして次のステップへ進みます。[**ジョブの開始**] をクリックする前に、ステップリストに表示される完了したステップをクリックすることで、そのステップに戻って変更を行うことができます。
5. インストールジョブを起動する準備ができたら、[**ジョブの開始**] をクリックします。

   ジョブを後で実行するようにスケジュール設定している場合でも、ジョブの開始後にパラメーターを変更することはできません。

   ジョブが完了するまで [パッチのインストール] ウィンドウが開いている場合、Ubuntuパッチ管理により [すべての管理対象サーバー] ウィンドウの [パッチコンプライアンス] 列の関連するサーバーのコンプライアンスカウント (括弧内) が更新されます。[**F5**] キーを押すか、[表示] メニューの [**更新**] を選択して、[パッチのプレビュー] ペインの情報を更新します。

   パッチをインストールする別の方法については、パッチポリシーの修復 (188ページ) を参照してください。

Ubuntuインストールオプションの設定

次のタイプのパッチのインストールオプションを指定することができます。

- パッチがダウンロードされたらすぐにパッチのインストールを行うか、日時を指定して後でインストールを行う。
- いずれか1つのパッチでエラーが発生した場合でも、パッチのインストールプロセスを中断しない。
- さまざまなコマンドラインオプションを使用してインストールを行う。

これらのオプションを設定するには、次の手順を実行します。

1. [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [インストールオプション] ステップに進みます。
2. 次のいずれかのステージインストールオプションを選択します。
   - **継続**: すべてのフェーズを連続する1つの操作として実行できます。
   - **ステージ**: ダウンロードとインストールをスケジュール設定して別々に実行することができます。
3. いずれかのパッチでエラーが発生した場合でもパッチのインストールプロセスを続行する場合は、[**エラーオプション**] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。
4. [**インストールコマンド**] テキストボックスに、表示されるコマンド (.debファイル) のコマンドライン引数を入力します。
5. [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

Ubuntuパッチのインストールでの再起動オプションの設定

サーバーの再起動によるダウンタイムを最小限に抑えるため、サーバーを再起動するタイミングを制御できます。ベンダーの再起動割り当てを調整、パッチをインストールするたびにサーバーを再起動、すべてのサーバーの再起動を完全に抑制、またはすべてのパッチがインストールされるまで再起動を延期することができます。

[パッチのインストール] ウィンドウで再起動オプションを選択する場合、HPではUbuntuの再起動推奨設定 ([**個別のソフトウェアアイテムの指定に基づいてサーバーを再起動**] オプション) を使用することを推奨しています。Ubuntuの再起動設定を使用できない場合は、単一再起動オプション ([**すべてのパッケージがインストールまたはアンインストールされるまですべてのサーバーの再起動を保留する**] オプション) を選択します。このようにしないと、次の再起動が (SAの制御対象外) 実行されるまで、サーバーにインストールされているパッチが正しく通知されない可能性があります。

パッチのインストールの完了後にサーバーを再起動するかどうかを指定するオプションです。これらのオプションは、[パッチのインストール] ウィンドウから起動したジョブのみに適用されます。これらのオプションを設定しても、[パッチのプロパティ] ウィンドウの [インストールパラメーター] タブにある [再起動が必要] オプションが変更されることはありません。

サーバーの状態が再起動保留中である場合、その後のパッチのインストールは失敗する可能性があります。サーバーでパッチのインストールを行う前に、サーバーを再起動する必要があります。

次に示すオプションの設定は、最初のオプションを除いて、[再起動が必要] オプションの設定よりも優先します。

- **個別のソフトウェアアイテムの指定に基づいてサーバーを再起動** (デフォルト): デフォルトでは、パッチプロパティの [再起動が必要] オプションの設定に従って再起動が行われます。
- **各パッチのインストール後にサーバーを再起動**: パッチプロパティの [再起動が必要] オプションが設定されていない場合でも、サーバーを再起動します。複数のパッチをインストールする場合、サーバーの再起動も複数回行われます。

- **すべてのサーバーの再起動を抑制**: パッチプロパティの [再起動が必要] オプションが設定されている場合でも、サーバーを再起動しませんベンダー設定によっては、抑制オプションを無視して強制的に再起動を行う場合があります。サービスパックの場合、再起動を抑制すると、アクションが未完了になります (再起動するまでサービスパックは未インストールになります)。パッチやサービスパックはインストール済みの状態になりません。ステータスは「未インストール/アンインストール」になります。システムを手動でチェック (レジストリまたはサーバーのプロパティを確認) する場合、SAクライアントに表示される内容と同じにはなりません。再起動後、次にソフトウェア登録を行うまで、SAクライアントに正しいソフトウェアやパッチのインストール情報は反映されません。

  注: Ubuntuパッチのインストール時に再起動を抑制すると (サービスパックの場合など)、システムのソフトウェア状態が正しく表示されない可能性があります。正確な状態は、管理対象サーバーが再起動され、ソフトウェア登録が完了した後に表示されます。
- **すべてのパッケージがインストールまたはアンインストールされるまですべてのサーバーの再起動を保留する**: 選択したパッチの中に [再起動が必要] オプションが設定されているものが含まれていても、他のパッチにそのオプションが設定されていない場合、すべてのパッチのインストール後にサーバーが1回再起動されます。一般的に、このオプションは単一再起動オプションと呼ばれます。選択したパッチの中に [再起動が必要] オプションが設定されているものがない場合、サーバーは再起動されません。

再起動オプションを設定するには、次の手順を実行します。

1. [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [インストール前後のアクション] ステップに進みます。
2. いずれかの再起動オプションを選択します。
3. [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

Ubuntuパッチのインストールでのインストールスクリプトの指定

パッチごとにインストールの前または後に実行するコマンドまたはスクリプトを指定できます。インストール前スクリプトでは、たとえば、管理対象サーバー上で特定の条件をチェックすることができます。条件が満たされない場合やインストール前スクリプトが失敗した場合、パッチはインストールされません。インストール前スクリプトを使用すると、パッチを適用する前にサービスやアプリケーションをシャットダウンすることもできます。インストール後スクリプトを使用すると、管理対象サーバー上でクリーンアッププロセスを実行することができます。

また、インストールフェーズまたはダウンロードフェーズの前または後に、管理対象サーバー上で次のタイプのスクリプトを実行するように指定することもできます。

- **ダウンロード前**: SAから管理対象サーバーにパッチをダウンロードする前に実行するスクリプト。[インストールオプション] ステップで [ステージ] を選択した場合にのみ利用できます。
- **ダウンロード後**: SAから管理対象サーバーにパッチをダウンロードした後で、パッチをインストールする前に実行するスクリプト。[インストールオプション] ステップで [ステージ] を選択した場合にのみ利用できます。
- **インストール前**: 管理対象サーバーにパッチをインストールする前に実行するスクリプト。
- **インストール後**: 管理対象サーバーにパッチをインストールした後に実行するスクリプト。

インストール前スクリプトを指定するには、次の手順を実行します。

1. [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [インストール前後のアクション] ステップに進みます。
2. [インストール前] タブを選択します。各タブでさまざまなスクリプトとオプションを指定できます。
3. [スクリプトの有効化] を選択します。このオプションを選択すると、タブのフィールドの残りの部分が有効になります。[スクリプトの有効化] を選択しない場合、スクリプトは実行されません。
4. [保存されたスクリプト] または [アドホックスクリプト] を選択します。

   保存されたスクリプトは、前にSA Webクライアントを使用してServer Automationに保存されたものです。スクリプトを指定するには、[**選択**] をクリックします。

アドホックスクリプトはこの操作に対してのみ実行され、Server Automation に保存されません。タイプ (.batなど) を選択します。[スクリプト] ボックスに、スクリプトが存在する場所のドライブ文字を含むスクリプトの内容を入力します (echo dir>> C:\temp\preinstall1.log など)。ドライブ文字を入力しない場合、デフォルトは%SYSTEMDRIVE%になります。これは、Ubuntuのシステムフォルダーがインストールされている場所です。

5 スクリプトでコマンドラインフラグが必要である場合、[コマンド] テキストボックスにフラグを入力します。

6 [ユーザー] セクションで情報を選択します。ローカルシステム以外のシステムを選択する場合は、ユーザー名、パスワード、ドメインを入力します。このユーザーによってスクリプトが管理対象サーバー上で実行されます。

7 スクリプトがエラーを返した場合にインストールを停止するには、[エラー] チェックボックスを選択します。

8 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

Ubuntuパッチのインストールのスケジュール設定

Ubuntu のパッチ適用の 2 つのフェーズは切り離すことができます。そのため、パッチをインストールするタイミングをパッチをダウンロードするタイミングとは独立してスケジュール設定することができます。

パッチのインストールをスケジュール設定するには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [スケジュール設定] ステップに進みます。

デフォルトでは、[スケジュール設定] ステップにはインストールフェーズ用のスケジュール設定オプションのみが表示されます。[インストールオプション] ステップで [ステージ] を選択した場合、ダウンロードフェーズ用のスケジュール設定オプションも表示されます。

2 次のいずれかのインストールフェーズオプションを選択します。

- **ただちにタスクを実行**: [サマリープレビュー] ステップでプレビュー分析を行うことができます。ダウンロードフェーズ用のスケジュール設定オプションは、[**ダウンロード後ただちに実行**] です。
- **次の時刻にタスクを実行**: 日付と時刻を指定して、後でダウンロードまたはインストールを実行することができます。

3 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

➤ スケジュール設定したパッチのインストールは、パッチのダウンロードが完了している場合でも、実行前にキャンセルできます。

Ubuntuパッチのインストールでの電子メール通知の設定

ダウンロード操作やインストール操作が正常に終了した、あるいはエラーで終了したときに、ユーザーに知らせるために電子メール通知を設定できます。

電子メール通知を設定するには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [通知] ステップに進みます。

2 電子メールアドレスを追加するには、[**通知の追加**] をクリックして [通知電子メールアドレス] フィールドに電子メールアドレスを入力します。

3 ジョブが成功したときの通知ステータスを設定するには、  アイコンを選択します。ジョブが失敗したときの通知ステータスを設定するには、  アイコンを選択します。デフォルトでは、[通知] ステップにはインストールフェーズ用の通知ステータスのみが表示されます。

4 [チケットID] フィールドに、このジョブに割り当てるチケットIDを入力します。

5 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

[インストールオプション] ステップで [ステージ] を選択した場合、[通知] ペインにダウンロードとインストールの両方のフェーズに対する通知オプションが表示されます。

Ubuntuパッチのインストールのプレビュー

インストールのプレビューでは、サーバーのパッチの状態に関する最新のレポートが表示されます。インストールのプレビューは、管理対象サーバーにインストールされるパッチと必要なサーバー再起動のタイプを確認するためのオプションステップです。プレビュープロセスでは、パッチのインストール対象として選択したサーバーに該当するパッチがすでにインストールされているかどうかを確認します。システム管理者がパッチを手動でインストールしている場合、サーバーにパッチがすでにインストールされている可能性があります。このような場合、Ubuntuパッチ管理ではパッチの存在を把握できません。

プレビューでは、特定のUbuntu製品を必要とするパッチ、および他のパッチよりも優先されるパッチや他のパッチの方が優先されるパッチなど、依存関係情報や優先情報に関するレポートも作成されます。依存関係が満たされていない場合は、パッチ管理にその状態を示すエラーメッセージが表示されます。必要でないパッチは、「インストールしない」として表示されます。

次のリストは、パッチがインストールされないケースについて説明したものです。これらは、[パッチのインストール] または [修復] ウィンドウの [プレビュー] ステップに表示されます。

- このパッチには「常にインストールしない」パッチポリシー例外があるため、インストールされません。
- このパッチは同じジョブ内の別のパッチより優先順位が低いため、インストールされません。これは、現在のジョブの中にマークされたパッチよりも最新のパッチが存在することを意味します。
- このパッチは別のパッチより優先順位が低いため、インストールされません。これは、サーバーにインストールされたパッチがポリシー内のパッチよりも新しいため、インストールされないことを意味します。
- このパッチは推奨されていないため適用できず、インストールされません。

この情報はジョブの結果ウィンドウにも表示されます。また、パッチインストールジョブで電子メール通知が構成されている場合は、電子メール内にも表示されます。

インストールのプレビューでは、パッチが適用済みの状態をシミュレートするため、サーバーの動作に関するレポートは行われません。

パッチのインストールをプレビューするには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [サマリーレビュー] ステップに進みます。

2 (オプション) [**プレビュー**] をクリックし、パッチのインストール時に実行される個々のアクションを表示します。テーブルの行を選択すると、プレビューしているアクションの詳細が表示されます。

3 [**ジョブの開始**] をクリックしてインストールジョブを起動するか、[**キャンセル**] をクリックしてインストールを起動せずに [パッチのインストール] ウィンドウを閉じます。

[スケジュール設定] ステップで [**ただちにタスクを実行**] を選択すると、ジョブがすぐに開始します。[**次の時刻にタスクを実行**] を選択すると、指定した日時にジョブが開始します。

Ubuntuパッチのインストールジョブの進行状況の表示

アクションが完了したか失敗したかなど、パッチのインストールジョブの進行状況を確認することができます。

ジョブの進行状況を表示するには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [ジョブの進行状況] ステップに進みます。これにより、インストールジョブが開始されます。

進行状況バーとテキストで、テーブル内のアクションがどの程度完了したかを確認できます。次のアクションをサーバーごとに実行できます。

- **分析**: HP Server Automationは、インストールに必要なパッチの確認、管理対象サーバーにインストールされた最新パッチのチェック、他に実行が必要なアクションの確認を行います。
- **ダウンロード**: HP Server Automationから管理対象サーバーにパッチをダウンロードします。
- **インストール**: ダウンロードの完了後、パッチをインストールします。
- **最後に再起動**: [インストール前後のアクション] ステップでこのアクションを指定すると、サーバーが再起動します。
- **インストール前スクリプト / インストール後スクリプト / ダウンロード前スクリプト / ダウンロード後スクリプト**: [インストール前後のアクション] ステップでこのアクションを指定した場合、インストール前または後にスクリプトが実行されます。
- **インストールと再起動**: パッチをインストールしたときに、サーバーが再起動します。
- **確認**: インストールしたパッチは、ソフトウェア登録に追加されます。

2 特定のアクションに関する詳細を追加表示するには、テーブルの行を選択して、ジョブの開始時刻と完了時刻を表示します。ナビゲーションペインで、[ジョブとセッション] を選択してジョブに関する詳細を確認します。ジョブログの参照については、『SAユーザーガイド: Server Automation』を参照してください。

Ubuntu管理対象サーバー上でベンダー推奨パッチポリシーを修復すると、適用するパッチによっては、サーバーで追加の修復が必要な場合があります。修復によって、ベンダーアップデートが必要なパッチがインストールされた場合に、この状況が発生します。

3 [パッチのインストール] ウィンドウを閉じる場合は [**閉じる**] をクリックし、ジョブを実行しないようにする場合は [**ジョブの終了**] をクリックします。

(オプション) インストール、アンインストール、修復のキャンセルまたは終了 (86ページ) を参照してください。

-

第7章 Unixパッチ管理

概要

HP Server Automation (SA) では、Unixパッチ管理により、パッチの確認、インストール、削除を行い、組織内にある管理対象サーバーのセキュリティを確保することができます。SAクライアントは、AIXオペレーティングシステム環境に存在するセキュリティの脆弱性に対するパッチを特定して、インストールできます。

ここでは、ソフトウェアポリシーを使用したUnixパッチのインストールおよびアンインストール方法について説明します。

SA ではパッチ管理の主要な機能が自動化されていますが、パッチのインストール方法やインストール条件は、細かく制御することができます。

パッチは重大なセキュリティ上の脅威に対応するために頻繁にリリースされるため、迅速にパッチを適用してシステムのセキュリティ被害を未然に防ぐ必要があります。同時に、パッチはパフォーマンスの低下やサーバー障害などの重大な問題につながることもあります。

SAは、新しく検出された脅威に迅速対応できるだけでなく、パッチインストールの厳格なテストと標準化にも対応しています。さらに、パッチが原因で問題が発生した場合には、テストと承認の後であっても、安全かつ標準化された方法でパッチをアンインストールできます。

SAは、SAライブラリにパッチ情報を保存します。これには、管理対象サーバー、サーバー上にインストールされているパッチとソフトウェア、インストール可能なソフトウェアとパッチに関する詳細な情報が含まれます。このデータを元に新しく検出された脅威の重大度を判定し、パッチをインストールした場合のメリットとダウンタイムコストを比較して、テスト要件を特定します。

パッチの適用手順を自動化することで、パッチ適用に伴うダウンタイムを短縮できます。また、パッチアクティビティのスケジュールを設定することで、ピーク以外の時間帯にパッチを適用することができます。

HP Server Automationでは、次の機能によってパッチ管理が自動化されます。

- パッチの保存先であり、各形式で編成されているSAライブラリ
- これまでに適用したパッチの情報が格納されたデータベース
- パッチインストールの前後に実行できるカスタマイズスクリプト
- パッチの適用が必要なサーバーを特定できる高度な検索機能
- セキュリティ担当者が重要なパッチのデプロイメントを追跡できる監査機能

これらの機能を利用することで、特定のオペレーティングシステムのパッチの参照、パッチのダウンロードとインストールのスケジュール設定、電子メール通知の設定、パッチインストールのプレビュー、ソフトウェアポリシーと修復によるパッチのインストールとアンインストール、再利用可能なファイル形式へのパッチ情報のエクスポートなどを実行できます。

パッチの参照のタイプ

HP Server Automationクライアントのインタフェースには、Unixパッチがオペレーティングシステム別に構成され、各パッチに関する詳細なベンダーセキュリティ情報が表示されます。パッチタイプ、可用性、プラットフォームバージョンなどを使ってパッチを参照することができます。また、サーバーにインストールされているすべてのパッチを参照し、パッチメタデータを表示して編集することもできます。

スケジュール設定と通知

パッチをSAライブラリにアップロードする日時や管理対象サーバーにダウンロードする日時をスケジュール設定することができます。ベストプラクティスでは、組織の業務への影響の最も少ない時間にパッチのインストールをスケジュール設定するのが一般的です。1つのサーバーに1つのパッチをインストールする場合、インストール処理はダウンロード処理が完了してから開始されます。

ダウンロードやインストール操作の完了や成否に関する通知を受け取るように、電子メール通知を設定することができます。パッチのインストールをスケジュール設定する際には、再起動設定を指定して、ベンダーの再起動オプションの使用、無効化、延期、または抑制を設定することもできます。

ソフトウェアポリシーを使用したパッチの管理

ソフトウェアポリシーを使用すると、それぞれの環境内でのパッチ配布をカスタマイズできます。ソフトウェアポリシーでは、特定の管理対象サーバーにインストールするUnixパッチまたはインストールしないUnixパッチを定義します。ソフトウェアポリシーの作成によるUnixパッチのインストールの詳細については、『SAユーザーガイド: ソフトウェア管理』を参照してください。

パッチのインストールのプレビュー

SAでは、新しく見つかったセキュリティ脆弱性に迅速に対応できるだけでなく、パッチのインストールの厳格なテストと標準化もサポートされます。インストールするパッチの確認後、実際にパッチをインストールする前に、SAでパッチインストールをシミュレート (プレビュー) することができます。プレビュープロセスでは、パッチのインストール対象として選択したサーバーに該当するパッチがすでにインストールされているかどうかがわかります。システム管理者がパッチを手動でインストールしている場合、サーバーにパッチがすでにインストールされている可能性があります。プレビューでは、サーバーのパッチの状態に関する最新のレポートが作成されます。

ソフトウェアポリシーの修復

SAには、パッチのインストールが原因で正しく動作していないサーバーを修復するためのソリューションも用意されています。インストールしたパッチが原因で問題が発生した場合には、テストと承認の後であっても、安全かつ標準化された方法でパッチをアンインストールすることができます。SAでは、アンインストールオプションを指定して、サーバーの再起動とアンインストールコマンド、アンインストール前スクリプト、アンインストール後スクリプトの実行を制御することができます。パッチのインストールのプレビューと同様に、パッチのアンインストールのプレビューを行うこともできます。詳細については、『SAユーザーガイド: ソフトウェア管理』を参照してください。

パッチデータのエクスポート

サーバーまたはサーバーグループのパッチ状態のトラッキングに役立つように、SAでは、パッチデータをエクスポートすることができます。パッチデータはカンマ区切り (.csv) ファイルにエクスポートできます。このデータには、パッチがインストール済みとして最後に検出された日時、Server Automationでパッチがインストールされた日時、パッチのコンプライアンスレベル、パッチポリシー例外などに関する詳細情報が含まれます。エクスポートしたデータはスプレッドシートやデータベースにインポートして、さまざまなパッチ分析タスクを実行できます。詳細については、パッチのエクスポート (225ページ) を参照してください。

管理対象サーバーでのパッチのトラッキング

サーバーがSAによる管理下に移されたら、サーバーにインストールされたSAエージェントで、サーバーのハードウェアとソフトウェアの構成をSAに登録します。この情報にはインストール済みのソフトウェアとパッチが含まれています。この情報はSAライブラリ内に記録されます。SAエージェントは、この登録を24時間ごとに繰り返します。

新規のパッチが発行されると、Server Automationを使用して、パッチを適用する必要のあるサーバーをすぐに確認できます。SAライブラリには、パッチやその他のソフトウェアが格納されます。SAクライアントからSAライブラリにアクセスして、該当するサーバーにパッチをインストールすることができます。

サーバーが管理下に移されたら、必要なすべてのパッチをインストールします。パッチを手動でインストールした場合、次にSAエージェントの登録まで、そのパッチに関するデータはServer Automation内に存在しません。パッチを手動でインストールした場合、SAライブラリ内の該当するサーバーに関するデータが更新されるまでに最大24時間かかる可能性があります。

ただし、Server Automation でソフトウェアやパッチのインストールまたはアンインストールを行う場合、SA ライブラリのサーバーに関する情報はすぐに更新されます。

Unixパッチテストおよびインストールの標準化のサポート

SA では、パッチ適用のリスクを最小限に抑えることができます。最初に、パッチが SA ライブラリにアップロードされると、パッチのステータスは未テストとなります。このときは、特別な権限を持つ管理者のみがパッチをインストールすることができます。

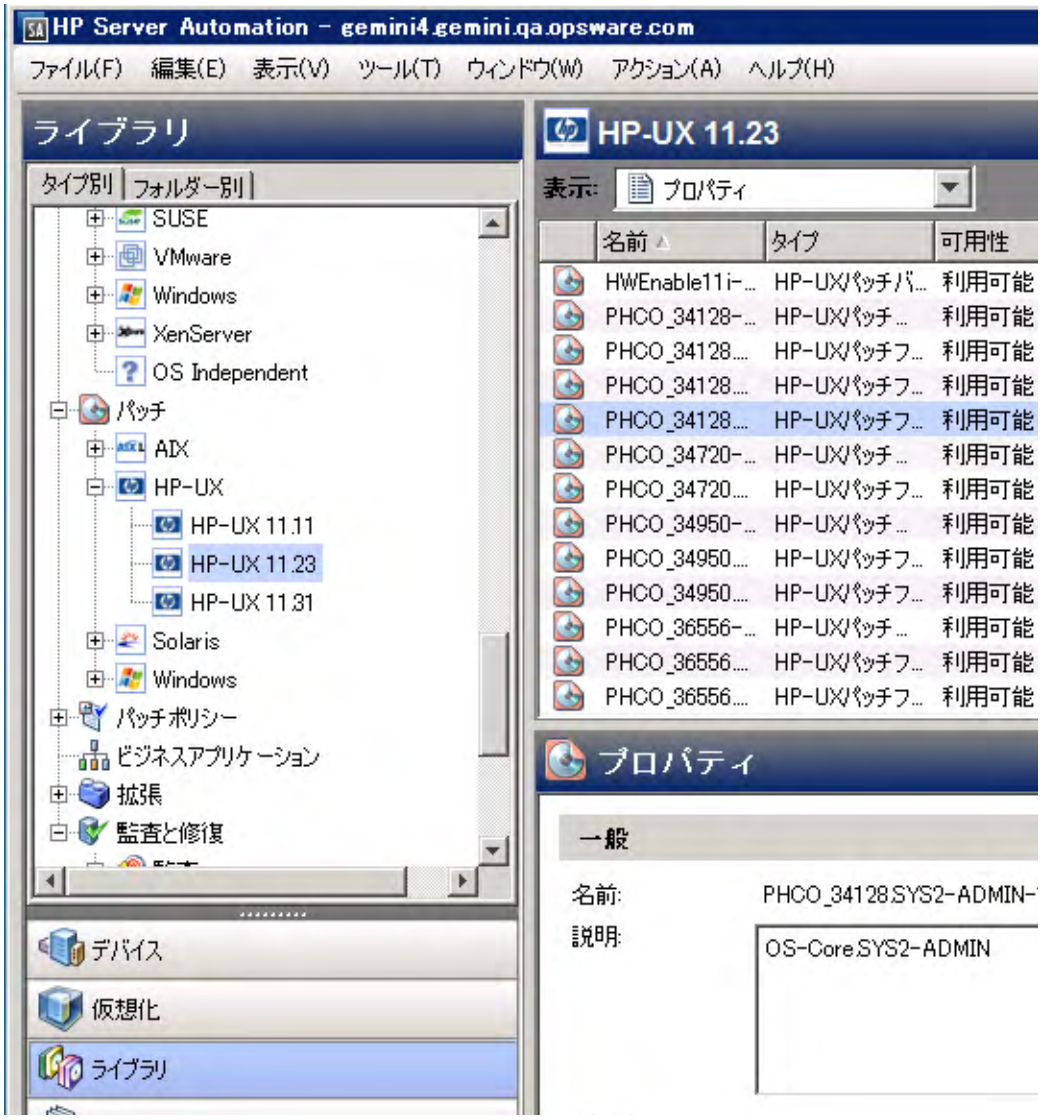
その後パッチ管理者は、パッチインストールオプションとアンインストールオプションを定義して、パッチをテストします。パッチのテストが完了し、パッチ管理者がパッチを利用可能にマークすると、その他の管理者もパッチをインストールできるようになります。

SAでは、パッチをインストール/アンインストールする方法を標準化し、アドホックなインストールが行われないようにすることができます。パッチ管理者は、インストール前スクリプトとインストール後スクリプト、インストールフラグとアンインストールフラグ、再起動指示、インストール前スクリプトとインストール後スクリプトのエラーコードの処理方法を指定して、パッチのインストールを標準化します。

SAクライアントでのパッチの表示

SAクライアントでは、名前、パッチのタイプ、オペレーティングシステム、他のパッケージとの関係などを使用して、Unixパッチを検索して表示できます。図31は、HP-UX 11.23用のパッチのリストを表しています。表示するパッチデータの列を制御するには、列ヘッダーの右側にある列セレクターを使用します。詳細については、Unixパッチ情報 (221ページ) およびUnixパッチのプロパティの表示と編集 (224ページ) を参照してください。

図31　　SAライブラリのHP-UXパッチ



パッチの検索

SAクライアントでは、SAクライアントを使用して、Server Automationで利用可能な運用環境に関する情報を検索できます。SAクライアントでは、パッチ、ソフトウェアポリシー、サーバーなどを検索できます。『SAユーザーガイド: Server Automation』の「SAクライアントの検索に関する項」を参照してください。

Unixパッチ管理の役割

Server Automationでは、次のようにパッチ管理の役割をパッチ管理者とシステム管理者に割り当てることで、厳密な変更管理を行うことができます。

- パッチ管理者(セキュリティ管理者と呼ばれることも多い)には、パッチオプションのアップロード、テスト、編集を行う権限があります。

- システム管理者は、パッチ管理者が指定したオプションに従って、(使用承認済みの)パッチを適用します。

高度な機能にアクセスできるパッチのアクセス権は、パッチ管理者のみに割り当てます。必要なアクセス権の取得については、SAの管理者にお問い合わせください。詳細については『SA 管理ガイド』の付録「アクセス権リファレンス」を参照してください。

パッチ管理者

多くの組織のパッチ管理者は、最新のセキュリティ上の脅威を確認し、これらの問題に対処するためにベンダーがリリースしたパッチを確認します。一般にパッチ管理者は、管理対象のオペレーティングシステムとアプリケーションに精通し、ベンダーが発行したパッチを適用する必要があるかどうかを評価することができます。また、パッチ管理者は、パッチ適用プロセスの詳細なテストを考慮して、パッチのインストール後に発生する一般的な問題を診断することもできます。

Server Automationでは、パッチをServer Automationにアップロードしてパッチをテストし、利用可能とマークするためのアクセス権がパッチ管理者に割り当てられます。基本ユーザーはパッチをアップロードすることはできますが、パッチをインストールしたり、利用可能とマークしたりすることはできません。パッチ管理者は、パッチ管理を使用してパッチオプション(インストールスクリプトなど)を編集することもできます。その他のタイプのユーザーは、パッチのアップロードや編集を行うことはできません。

通常、パッチ管理者はパッチをアップロードして、非運用環境の基準ハードウェア上でパッチをテストします。パッチをテストして、運用システムに適用しても問題がないことが確認できたら、パッチ管理者はHP Server Automation クライアントでパッチに利用可能のマークを付けて、そのパッチを適用する必要のあるシステム管理者に通知します。

システム管理者

システム管理者は、デプロイメント中のサーバーの日常的なメンテナンスを担当します。これらのユーザーには、低レベルシステムの詳細について、パッチ管理者と同じ水準の技術力は必要ありません。

パッチ管理者がパッチのインストールをすでにセットアップしているため、システム管理者はわずかな操作で多数のサーバーにパッチを適用することができます。システム管理者は、承認済みパッチが必要なサーバーを検索し、パッチをインストールして、パッチが正常にインストールされたことを確認する必要があります。

各Unixオペレーティングシステムでのパッチ管理

パッチのタイプやベースとなるテクノロジーは、オペレーティングシステムのベンダーによって異なる場合があります。ここでは、Server AutomationでのUnixパッチ管理のベンダーごとの詳細について説明します。

サポートされるUnixバージョンとパッチタイプ

SAはServer Automationでサポートされるすべてのオペレーティングシステムバージョン(Linuxを除く)をサポートしています。

Linuxは通常の意味でのパッチをサポートしていません。パッケージにはパッチを適用できません。代わりに、RPMの新規バージョンが配布されます。そのため、Server Automationで管理しているLinuxシステムは、パッチのインタフェースを通じて表示できません。新規のLinuxパッケージや更新は、ソフトウェアポリシーを介して管理または適用する必要があります。ソフトウェアポリシーを使用したRPMのインポートとインストールについては、『SAユーザーガイド: ソフトウェア管理』を参照してください。

SAでサポートされるUnixバージョンとパッチタイプを参照するには、次の手順を実行します。

1. SAクライアントで、[ライブラリ] タブを選択します。
2. [タイプ別] タブを選択します。
3. [パッチ] ノードを見つけて開きます。SAでパッチがサポートされるすべてのオペレーティングシステムが表示されます。
4. オペレーティングシステムを選択し、そのオペレーティングシステムのノードを開きます。SAでサポートされるオペレーティングシステムのすべてのバージョンが表示されます。例については、214ページの図31「SAライブラリのHP-UXパッチ」を参照してください。

Unixパッチ管理に使用されるテクノロジー

使用するユーティリティは異なりますが、Server Automationでは1つのインタフェースを使用してパッチタスクを実行することができます。Server Automationのパッチの処理方法は、使用するユーティリティでのパッチの処理方法に基づいています。たとえば、Solarisのpatchaddユーティリティでパッチクラスター内のあるパッチをインストールできない場合、このユーティリティはパッチクラスター内の残りのパッチのインストールを続行します。Server Automationでは、この動作を考慮して、このパッチインストール処理を続行させます。インストールされないパッチがある場合は、インストール処理が終了したときに通知されます。

次の表は、サポートされるUnixシステムで使用されるパッチ管理とインストールツールを示しています。

表24 Unixパッチ管理に使用されるテクノロジー

Solaris	AIX	HP-UX
Patchadd Solarisパッチのインストール	Installp ファイルセットのインストールとアンインストール	Swlist パッチプロダクト、ファイル、ファイルセットのリスト表示
Patchrm Solarisパッチのアンインストール	Lslpp インストール済みLPPのリスト表示	Swinstall デポのインストール
Showrev インストール済みSolarisパッチのリスト表示	Instfix インストール済みAPARのリスト表示	Swremove デポの削除
Pkgadd Solarisパッケージのインストール		
Pkginfo インストール済みSolarisパッケージのリスト表示		

AIXのパッチ

AIXでは、発見された問題の修正に必要な更新ファイルセット (LPPに含まれる) を指定したAPAR (Authorized Program Analysis Report) が定期的にリリースされます。APARでは、問題の修正に必要な更新ファイルセットの最小バージョンを指定しているため、同じファイルセットの後続バージョンを使用して問題を修正することもできます。ただし、互換性を維持するため、Server Automationでは、APARで指定された最小バージョンに適合するバージョン番号の最も低いファイルファイルを使用します。更新ファイルセットの後続バージョンがアップロードされた場合でも、Server Automationでは、以前のバージョンのファイルセットがAPARに関連付けられたままになります。

LPP をアップロードする際に、Server Automation は LPP に含まれるファイルセットが属する APAR を認識します。APARに関連付けられた最初のファイルセットがアップロードされると、SAライブラリ内にAPARのエントリが作成されます (1つのファイルセットが複数のAPARと関連付けられる場合もあります。エントリが存在しない場合、エントリはファイルセットが関連付けられたAPARごとに作成されます)。

APARで指定されたすべてのLPPをインストールする場合は、指定されたすべてのLPPをSAライブラリにアップロードする必要があります。

APARで指定されたすべてのLPPをアップロードしなくても、システム管理者はAPARを参照して、アップロードされた一部のLPPをインストールすることができます。この場合、管理者は、APARのファイルセットがすべてインストールされないことを示す警告を受け取ります。

- Server AutomationでLPPが一般に利用できるようになる前に、パッチ管理者はLPPをアップロードしてテストする必要があります。新しいファイルセットはLPPがテストされて承認された後にAPARに統合されます。APARが自動的に更新される場合でも、管理対象サーバーへのインストールを許可するファイルセットを厳密に制御することができます。

- サーバーに更新ファイルセットの対象となるベースファイルセットが存在しない場合、APAR 更新ファイルセットをサーバーにインストールすることはできません。

  ただし、サーバーにベースファイルセットの一部が存在する場合は、APAR を適用することができ、ベースファイルセットの該当するファイルセットのみがインストールされます。たとえば、APARで4つのベースファイルセットを更新する4つの更新ファイルセットが指定されている場合、その内の3つのベースファイルセットを含むサーバーにこのAPARを適用すると、APARの4つの更新ファイルセットのうちの3つがインストールされます。

  AIX更新ファイルセットをインストールする場合、通常、SAはファイルセットを適用します。この場合、ファイルセットを拒否 (アンインストール) することができます。(ファイルセットを削除できないように) ファイルセットをコミットする場合は、ここで-cオプションを使用します。

- パッチファイル (AIX 更新ファイルセットと APARS など) を特定のフォルダーに追加する操作は実行できません。また、特定のユーザーがパッチファイルを所有することはできません。フォルダーの使用方法については、『SAユーザーガイド: Server Automation』を参照してください。

AIXパッチのインポートと修復

SA では、AIX パッケージのセットをメンテナンスレベル (ML) またはテクノロジーレベル (TL) でインポートして修復し、AIXパッケージをインストールできます。

パッケージとパッチは、SAに個別にインポートされます。サーバーを特定のMLまたはTLに更新するには、そのMLまたはTLに属するすべてのパッケージとパッチを1回の操作でSAにインポートします。インポート時に、パッケージとパッチ用に作成する新規ポリシーを指定します。その結果、ML/TLを表すポリシーが作成され、これを管理対象サーバーにインストールできます。

AIXパッチをインポートするには、次の手順を実行します。

1. SAコアにrootとしてログインします。
2. IBMのWebサイトからAIX メンテナンスレベルまたはテクノロジーレベルのすべてのパッケージをダウンロードして、SAコアの一時ディレクトリに保存します。
3. `import_aix_packages` ツールを使用して、パッチをSAライブラリにインポートします。このツールを使用して、インポート済みのすべてのパッケージを含むソフトウェアポリシーを生成することもできます。

   ```
   /opt/opsware/mm_wordbot/util/import_aix_packages <AIXパッケージを含むディレクトリ>
   ```

   インポートコマンドは、必ずAIXパッケージを含むディレクトリのパスで終わります。AIXのインポートのオプションの詳細については、AIXのインポートオプション (219ページ) を参照してください。

AIXのインポートおよび修復処理の例

次の例は、SAコアの次の一時ディレクトリからのAIXパッケージのインポートを示します。
`/var/tmp/aix_package_files_directory`

1 次のAIXインポートツールを実行します。

a サンプルA: **AIXパッケージとパッチの簡易インポート**

```
/opt/opsware/mm_wordbot/util/import_aix_packages /var/tmp/
aix_package_files_directory
```

— デフォルトで、`import_aix_packages`ツールは、インポートするパッケージのOSバージョンを識別しようとします。また、'-o' または '--os' オプションを使用して、インポートされたパッケージのOSを明示的に定義できます。オプションの詳細については、AIXのインポートオプション (219ページ) を参照してください。

— インポート済みのAIXファイルは、SAクライアントで、**[ライブラリ] > [タイプ別] > [パッケージ] > [AIX]** または **[ライブラリ] > [タイプ別] > [パッチ] > [AIX]** を選択して表示できます。

b サンプルB: **AIXパッケージ/パッチのインポートとポリシーの作成**

'-p' オプションを使用してパッチをインポートし、ポリシーを指定します。

```
/opt/opsware/mm_wordbot/util/import_aix_packages -p /AIX/AIX6.1/
AIXPOLICY /var/tmp/aix_package_file_directory
```

— 新しく作成されたポリシーは、SAクライアントで、**[ライブラリ] > [タイプ別] > [ソフトウェアポリシー]** または **[ライブラリ] > [フォルダー別]** を選択すると、次のディレクトリの下に表示されます。

```
/AIX/AIX6.1/AIXPOLICY
```

2 新しく作成されたポリシー、`AIXPOLICY`をAIX管理対象サーバーにアタッチします。

3 AIXパッケージまたはパッチの通常のインストールと同様に、アタッチしたポリシーでサーバーを修復します。

AIXのインポートオプション

表25　import_aix_packagesのオプション

オプション	説明
-h、 --help	このヘルプメッセージを表示して終了します
-f、 --force	すでにライブラリ内に存在する場合でも、パッケージを強制的にインポートします。
-o OS、 --os=OS	パッケージのOSバージョン: '4.3'、'5.1'、'5.2'、'5.3'、'6.1'、'7.1' -oパラメーターは、引用符の有無にかかわらず機能しますが、一度に指定できる値は1つのみです。 たとえば、テクノロジーレベル6、サービスパック1を指定する場合、次のようになります。 /opt/opsware/mm_wordbot/util/ import_aix_packages –o '6.1' /var/tmp/ aix_package_file_directory または /opt/opsware/mm_wordbot/util/ import_aix_packages –o 6.1 /var/tmp/ aix_package_file_directory
-p POLICY_PATH、 --policy_path=POLICY_PATH	このオプションを使用すると、1回の操作でAIXパッチをインポートし、アップロードされたユニットを含む特定のソフトウェアポリシーを生成できます。 構文: /opt/opsware/mm_wordbot/util/ import_aix_packages –p <SAソフトウェアポリシーが作成される場所の完全な名前とパス> <AIXパッケージを含むディレクトリ> 例: /opt/opsware/mm_wordbot/util/ import_aix_packages –p /AIX/AIX6.1/ AIXPOLICY /var/tmp/ aix_package_file_directory
--policy_mode=POLICY_MODE	ポリシーインストールのセマンティクス: 'update_all'、'install_latest'
-s、 --silent	エラーのみを表示します。
-u USERNAME、 --username=USERNAME	指定されたユーザーとしてパッケージをアップロードします (デフォルト: opsware)。
-v、 --verbose	詳細な出力を表示します。
--manual	マニュアルページを表示して終了します

複数のオプションを使用する場合

複数のオプションを使用する場合、オプションの順序に関するルールはありませんが、コマンドが<AIXパッ

ケージを含むディレクトリ>パラメーターで終わっている必要があります。

たとえば、次のコマンドは、いずれも正常にAIX 6.1パッチをインストールし、アップロードされたファイルセットでポリシーを作成します。

```
/opt/opsware/mm_wordbot/util/import_aix_packages -p /AIX/AIX6.1/aix_policy
-o '6.1' /var/tmp/aix_package_file_directory
```

または

```
/opt/opsware/mm_wordbot/util/import_aix_packages -o '6.1' -p /AIX/AIX6.1/
aix_policy/var/ tmp/aix_package_file_directory
```

Solarisパッチ

Solarisパッチクラスターには、特定のSolarisリリースレベル用に選択されたパッチが含まれます。通常、パッチクラスターのインストール後に、特定のパッチクラスターを検索することはできません。パッチにはパッチとパッチがバンドルされていたパッチクラスターとを関連付けるメタデータが含まれていません。検索できるのは個別のパッチのみです。

Solarisパッチクラスターをインストールする場合、Server AutomationはSAライブラリのパッチクラスターをトラッキングします。そのため、パッチクラスターを検索して、パッチクラスター全体がインストールされているかどうかを特定することができます。パッチクラスターのインストール後には、クラスター内の個別のパッチをアンインストールすることができます。パッチクラスターをアンインストールすることはできません。

Solarisパッチの詳細については、第4章「Solarisパッチ管理」(113ページ)を参照してください。第5章「Solaris 11パッチ管理」(157ページ)も参照してください。

HP-UXパッチ

HP-UXパッチはデポとして独占的に配布されます。デポはパッチファイルセットを含むパッチプロダクトです。デポはServer Automationに直接アップロードされます。

デポがすでにアップロードされてノードにアタッチされている場合、SAでデポをアップロードすることはできません。SAでデポをアップロードする場合は、アタッチされているノードからデポをデタッチした後に、SAライブラリからデポを削除する必要があります。

詳細については、HP-UXパッチ管理 (93ページ) を参照してください。

UnixパッチのSAライブラリへのアップロード

Unixパッチを管理対象サーバーにインストールするには、事前にパッチをサーバーベンダーからダウンロードして、SAライブラリにアップロードする必要があります。詳細については、『SA 管理ガイド』を参照してください。

UnixパッチをSAライブラリへアップロードするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。パッチはオペレーティングシステム別に構成されます。
2. 目的のオペレーティングシステムバージョンに移動します。
3. [**アクション**] メニューで、[**ソフトウェアのインポート**] を選択して、[ソフトウェアのインポート] ウィンドウを開きます。
4. [ソフトウェアのインポート] ウィンドウで、[**参照**] をクリックしてインポートするパッチを選択します。

   [開く] ウィンドウで [**開く**] をクリックする前に、[エンコード] ドロップダウンリストからパッチで使用する文字エンコードを選択します。

SA でパッチに含まれるメタデータを抽出して、SA クライアント (パッチのプロパティページなど) で非ASCII文字の情報を正しく表示できるように、文字エンコードを指定する必要があります。パッチのメタデータには、コメント、リリースノート、スクリプト、説明、内容リストが含まれます。

5 [**開く**] をクリックします。

選択したアイテムが [ソフトウェアのインポート] ウィンドウの [**ファイル**] フィールドに表示されます。

6 [**タイプ**] ドロップダウンリストから該当するタイプを選択します。

通常、タイプは選択したファイルの拡張子に基づいて表示されます。表示されたタイプを確認して、最適なタイプがインポート用に選択されていることを確認します。

7 [**フォルダー**] フィールドで、SAライブラリの目的のディレクトリを選択します。

8 [**プラットフォーム**] ドロップダウンリストから、パッチを適用するすべてのオペレーティングシステムバージョンを選択します。選択したオペレーティングシステムを実行しているサーバーだけにパッチをインストールできます。

9 [**インポート**] をクリックして、パッチをSAライブラリにインポートします。

インポートが完了したら、[ステータス] 列に結果が表示されます。

— [ステータス] 列のチェックマークは成功を表します。

— [ステータス] 列のXマークはエラーを表します。Xをクリックしすると、エラーの詳細が表示されます。

10 インポートしたパッチを検索するには、SAライブラリの [**タイプ別**] タブの検索ツールを使用します。

Unixパッチ情報

SA クライアントでは、複数のビューでパッチに関する詳細情報を表示できます。たとえば、次の図 32 は、HP-UXパッチのプロパティビューを表しています。各パッチの詳細はパッチのタイプやOSによって異なることに注意してください。パッチのプロパティを表示または編集する場合は、Unixパッチのプロパティの表示と編集 (224ページ) を参照してください。

図32　　SAクライアントでのUnixパッチのプロパティ

パッチのプロパティビュー

パッチのプロパティには、次の情報が表示されます。ただし、一部の情報は特定のオペレーティングシステムのみで表示されます。

- **バージョン**: パッチのバージョン番号。
- **ステータス**: ベンダーのパッチのステータス。
- **タイプ**: Unixパッチのタイプ。HP-UXパッチプロダクト、HP-UXパッチファイルセット、Solarisパッチ、Solarisクラスター、AIX APAR、AIX更新ファイルセットなどがあります。
- **OS**: このパッチの影響を受けることがわかっているUnixオペレーティングシステム。

- **可用性**: Server Automationでのパッチのステータス。次のいずれかです。
  - **制限付き**: パッチはSAにインポートされていますが、インストールにはアクセス権 (パッチの管理: 読み取り/書き込み) の追加が必要です。これは、パッチの可用性のデフォルト設定です。アクセス権の詳細については、『SA 管理ガイド』を参照してください。
  - **利用可能**: パッチは、Server Automationへのインポートとテストが完了し、管理対象サーバーにインストール可能なパッチとしてマークされています。
  - **非推奨**: このパッチは、パッチポリシーに追加、またはパッチポリシー例外として設定することはできませんが、インストールは可能です。
- **オブジェクトID**: Server Automationでパッチに割り当てられる一意のID。
- **依存関係**: 存在する場合は、選択したパッチの依存関係を表示します。一部のタイプのパッチとプラットフォームのみで表示されます。詳細については、プロパティの管理 (142ページ) を参照してください。
- **インストールパラメーター**: 存在する場合、パッチのインストールで実際に使用される設定と、パッチ用にパッチベンダーが指定する設定です。一部のタイプのパッチとプラットフォームのみで表示されます。
- **インストールスクリプト**: 存在する場合、パッチインストールの前または後に、管理対象サーバー上で実行されるスクリプトです。一部のタイプのパッチとプラットフォームのみで表示されます。
- **アンインストールパラメーター**: 存在する場合、パッチのアンインストールで実際に使用される設定と、パッチ用にパッチベンダーが指定する設定です。一部のタイプのパッチとプラットフォームのみで表示されます。
- **アンインストールスクリプト**: 存在する場合、パッチアンインストールの前または後に、管理対象サーバー上で実行されるスクリプトです。一部のタイプのパッチとプラットフォームのみで表示されます。

内容ビュー

パッチの内容は、HP-UXパッチプロダクト、AIX APAR、Solarisクラスターなど、特定のタイプのパッチコンテナーでのみ表示されます。内容ビューには、選択したパッチコンテナーに含まれるすべてのパッチが表示されます。

デポビュー —HP-UXのみ

パッチデポは、HP-UX パッチプロダクトのみで表示されます。デポビューには、選択したパッチプロダクトを含むHP-UXデポが表示されます。SAでは、HP-UXデポをSAパッケージとして表示します。詳細については、HP-UXパッチ管理 (93ページ) を参照してください。

パッチプロダクトビュー —HP-UXのみ

パッチプロダクトは、HP-UX パッチファイルセットのみで表示されます。パッチプロダクトビューには、選択したHP-UXパッチファイルセットを含むHP-UXパッチプロダクトが表示されます。詳細については、HP-UXパッチ管理 (93ページ) を参照してください。

パッチクラスタービュー —Solarisのみ

パッチクラスターは、Solarisパッチのみで表示されます。パッチクラスタービューには、選択したSolarisパッチを含むSolarisパッチクラスターが表示されます。Solarisパッチの詳細については、Solarisパッチ管理 (113ページ) を参照してください。

LPP/APARビュー —AIXのみ

LPPS/APARビューは、AIXパッチのみで表示されます。このビューには、選択したパッチを含むLPPSとAPARが表示されます。

ソフトウェアポリシービュー

ソフトウェアポリシービューには、選択したパッチを含むすべてのソフトウェアポリシーが表示されます。

パッチポリシービュー

パッチポリシービューには、選択したパッチを含むすべてのパッチポリシーが表示されます。パッチポリシービューは、一部のプラットフォームでのみ表示されます。

サーバービュー

サーバービューには、選択したパッチがインストールされているすべてのサーバーが表示されます。

Unixパッチのプロパティの表示と編集

SA クライアントには、Server Automation にインポート済みの Unix パッチに関する情報が表示されます (Unix パッチ情報 (221ページ) を参照)。プロパティビューの一部のパッチのプロパティは編集できます。一部のプロパティは編集できません。

インストールパラメーターやアンインストールパラメーターは、パッチのプロパティページまたはパッチをインストール/アンインストールする際に設定できます。プロパティビューのパラメーターはSAライブラリに保存されますが、パッチのインストール/アンインストール時に指定したパラメーターはそのアクションで使用されるだけです。インストール / アンインストール時に指定するパラメーターは、パッチのプロパティビューの設定よりも優先されます。

パッチに関する情報を表示または編集するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。
2. [パッチ] を展開して、特定のUnixオペレーティングシステムを選択します。
3. (オプション) 列セレクターを使用して、名前、タイプ、可用性、説明に基づいてパッチをソートします。
4. 内容ペインで、パッチを選択します。
5. パッチを右クリックするか、[アクション] メニューで、[開く] メニューを選択します。別画面が開いてパッチが表示されます。
6. プロパティを変更した場合は、[**ファイル**] > [**保存**] を選択して、変更内容を保存します。
   -
   -
   -

Unixパッチがインストールされたサーバーの確認

特定のパッチがインストールされたサーバーを確認するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。
2. [パッチ] を展開して、特定のUnixオペレーティングシステムを選択します。内容ペインに、選択したオペレーティングシステムに関連するすべてのパッチが表示されます。
3. 内容ペインで、パッチを選択します。
4. 内容ペインの [表示] ドロップダウンリストから、[サーバー] を選択します。選択したパッチがインストールされているすべてのサーバーが表示されます。

パッチのエクスポート

パッチはローカルファイルシステムにエクスポートできます。ただし、すべてのパッチタイプをエクスポートできるわけではありません。パッチをエクスポートしようとして、[エクスポート] メニューが薄いグレーで表示されている場合、そのパッチをエクスポートすることはできません。

SAライブラリからローカルファイルシステムにパッチをエクスポートするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。
2. [パッチ] を展開して、特定のUnixオペレーティングシステムを選択します。内容ペインに、選択したオペレーティングシステムに関連するすべてのパッチが表示されます。
3. 内容ペインで、パッチを選択します。
4. [**アクション**] メニューで、[**エクスポート**] を選択します。[エクスポート] メニューが薄いグレーで表示される場合、そのパッチをエクスポートすることはできません。
5. [パッチのエクスポート] ウィンドウで、パッチファイルを含むフォルダー名を [ファイル名] フィールドに入力します。
6. [**エクスポート**] をクリックします。

パッチの削除

このアクションでは、SAライブラリからパッチが削除されますが、管理対象サーバーからパッチがアンインストールされるわけではありません。パッチがポリシーにアタッチされている場合、パッチを削除することはできません。

⚠ SA ライブラリからすべてのパッチを削除しないようにしてください。誤ってすべてのパッチを削除してしまった場合は、サポート担当者に連絡して、すべてのパッチをSAにアップロードし直してください。

パッチを削除するには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] > [**タイプ別**] > [**パッチ**] を選択します。
2. [パッチ] を展開します。
3. いずれかのUnixオペレーティングシステムを選択します。内容ペインに、選択したオペレーティングシステムに関連するすべてのパッチが表示されます。
4. 内容ペインで、パッチを選択します。
5. [**アクション**] メニューで、[**パッチの削除**] を選択します。
6. [パッチの削除] ウィンドウで、[**削除**] をクリックします。

ソフトウェアポリシーを使用したパッチの管理

WindowsおよびSolarisのパッチポリシーは、WindowsおよびSolarisプラットフォームでパッチを管理する最適な方法です。詳細については、Windowsパッチ管理 (17ページ) およびSolarisパッチ管理 (113ページ) を参照してください。

その他のプラットフォームでは、ソフトウェアポリシーを使用して、それぞれの環境内でのパッチ配布をカスタマイズできます。ソフトウェアポリシーでは、特定の管理対象サーバーにインストールするUnixパッチまたはインストールしないUnixパッチを定義します。

ソフトウェアポリシーを使用していて、アドホックなパッチインストールも行う場合は、修復プロセスを実行して適用可能なすべてのパッチをサーバーにインストールする必要があります。ソフトウェアポリシーの作成と修復によるUnixパッチのインストールの詳細については、『SAユーザーガイド: ソフトウェア管理』を参照してください。

パッチコンプライアンスレポート

パッチコンプライアンスの問題をトラブルシューティングして解決するには、SAクライアントでパッチコンプライアンスレポートを実行して調査します。次のパッチコンプライアンスレポートでは、ソフトウェアポリシーのすべてのパッチが環境内の管理対象サーバーに正常にインストールされているかどうかを特定できます。

パッチポリシーコンプライアンス (すべてのサーバー)

このレポートでは、すべての管理対象サーバーをパッチポリシーのコンプライアンスレベルごとにグループ化して、コンプライアンスサーバーと非コンプライアンスサーバーを表示します。

カスタマーごとのパッチポリシーコンプライアンス

このレポートでは、すべてのサーバーをサーバーが属するカスタマーごとに分けて、パッチポリシーのコンプライアンスレベルごとに表示します。

ファシリティごとのパッチポリシーコンプライアンス

このレポートでは、すべての管理対象サーバーをサーバーが属するファシリティごとに分けて、パッチのソフトウェアポリシーのコンプライアンスレベルごとに表示します。

➤ これらのレポートを実行、エクスポート、および印刷する方法については、『SA レポートガイド』を参照してください。

Unixパッチ管理

可用性フラグを設定すると、それぞれの環境に合うようにUnixパッチ管理をカスタマイズすることができます。

デフォルトのパッチの可用性の設定

デフォルトのパッチの可用性はSAクライアントで設定できます。SAクライアントで設定したデフォルト値よりも、スクリプトで使用するデフォルト値が優先されます。スクリプトについては、『SA 管理ガイド』を参照してください。

新規にインポートしたパッチの可用性のデフォルト値を設定するには、次の手順を実行します。

1 ナビゲーションペインで、**[管理]** を選択します。

2 [**パッチ構成**] を選択します。

3 インポート済みパッチの [**デフォルトの可用性**] で、[利用可能] または [制限付き] のいずれかを選択します。デフォルトは制限付きです。

パッチが利用可能の場合は、管理対象サーバー上にインストールできます。パッチが制限付きの場合は、パッチはServer Automationにインポート済みで、必要なアクセス権 (パッチの管理: 読み取り/書き込み) を持つパッチ管理者のみがインストールできます。必要なアクセス権の取得については、SAの管理者にお問い合わせください。『SA 管理ガイド』も参照してください。

パッチのインストール

パッチのインストールプロセスは、次の2つのフェーズで構成されます。

- **ダウンロードフェーズ**: このフェーズでは、Server Automation から管理対象サーバーへパッチをダウンロードします。このフェーズは、一般的にステージングフェーズと呼ばれます。
- **インストールフェーズ**: このフェーズでは、管理対象サーバーにパッチをインストールします。このフェーズは、一般的にデプロイメントフェーズと呼ばれます。

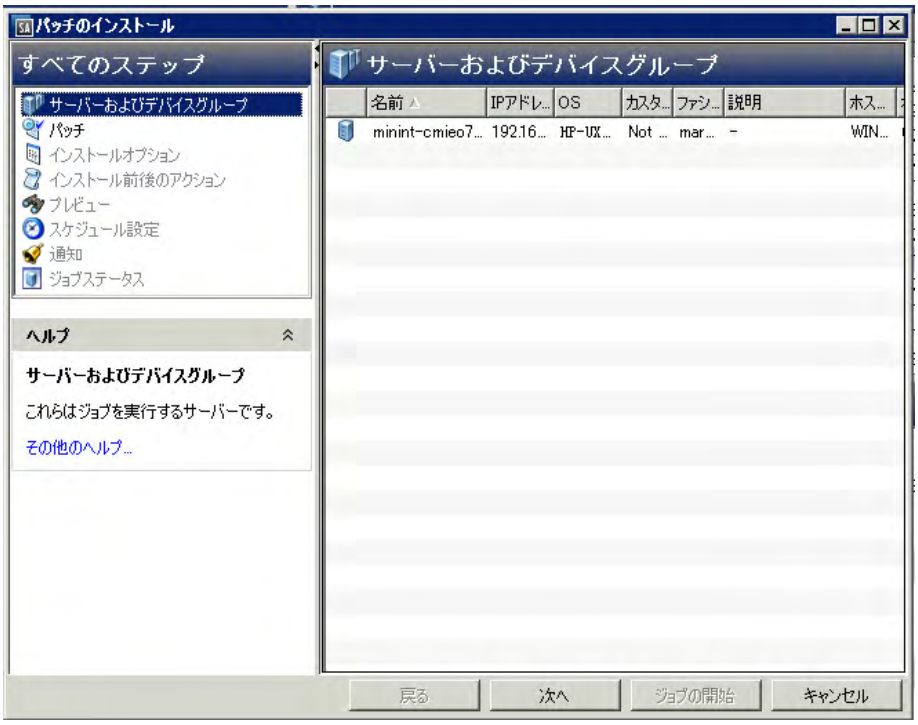
パッチがダウンロード (ステージング) されたらすぐにインストールを行うかどうかを指定できます。また、日時をスケジュール設定して後でインストールを行うこともできます。また、SAでは、複数のパッチのベストエフォート型インストールにも対応しており、いずれかのパッチでエラーが発生した場合でも、パッチのインストールを続行するように指定することが可能です。

SAでは、パッチをインストールするコマンドの名前が表示されます。SAエージェントは、管理対象サーバー上でこのコマンドを実行します。デフォルトのコマンドライン引数はオーバーライドできます。

SAでは、Unixパッチのインストールを適切に管理するため、サーバーの再起動オプションの管理、インストール前/インストール後スクリプトの指定、パッチのインストールのシミュレート (プレビュー)、インストールプロセスのステータスを通知する電子メール通知の設定を行うことができます。

これらの条件は、[パッチのインストール] ウィンドウを使用して設定することができます。

図33　[パッチのインストール] ウィンドウ



インストールフラグ

Unix パッチをインストールする際には、インストールフラグを指定できます。ただし、Server Automation では、デフォルトのインストールフラグが使用され、これらのフラグを使用してパッチをインストールする必要があります。そのため、Server Automation から渡されるデフォルトのインストールフラグを無効にするフラグや矛盾するフラグを指定しないようにする必要があります。コマンドの指定方法については、インストールオプションの設定 (230ページ) を参照してください。

次の表に、Server Automationで使用されるデフォルトのインストールフラグを示します。

表26　デフォルトのインストールフラグ

Unixパッチタイプ	フラグ
AIX	`-a -Q -g -X -w`
HP-UX	なし

アプリケーションのパッチ

SA では、パッチの対象ではないオペレーティングシステムにパッチを適用することはできません。アプリケーションのパッチをインストールする場合、SAで対応するアプリケーションがインストールされていないサーバーが自動的に除外されることはありません。SAでは、対応するアプリケーションがインストールされていないサーバーの除外は行われませんが、必要なアプリケーションがインストールされていないサーバーにアプリケーションのパッチを適用しないように注意する必要があります。パッチがサーバーにインストールされていないアプリケーション用である場合、そのパッチは適用されず、「パッケージ<パッケージ名>でエラーが発生しました」といったエラーメッセージが表示されます。

アプリケーションのパッチが同じオペレーティングシステムの複数のバージョンで実行されているアプリケーション用である場合、このパッチをすべてのサーバーに同時に適用することはできません。アプリケーションのパッチは、1つのオペレーティングシステムバージョンのみに関連付けられます。最初に特定のオペレーティングシステム用のパッチを選択してから、アプリケーションがインストールされているサーバーを選択し、パッチを適用します。アプリケーションがインストールされているオペレーティングシステムのバージョンごとに、このプロセスを繰り返す必要があります。

同様に、同一のオペレーティングシステムの複数のバージョンにインストールされているアプリケーションのパッチをアンインストールする際に、すべてのパッチを同時にアンインストールすることはできません。パッチがインストールされているオペレーティングシステムのバージョンごとに、このアンインストールプロセスを繰り返す必要があります。

パッチのインストール

パッチを管理対象サーバーにインストールするには、事前にパッチをServer Automationにインポートして、ステータスを利用可能にしておく必要があります。制限付きのマークの付いたパッチは、必要なアクセス権を持つ管理者がインストールできます。

パッチを管理するためのアクセス権が必要です。必要なアクセス権の取得については、SAの管理者にお問い合わせください。詳細については、『SA 管理ガイド』を参照してください。

パッチとサーバーを明示的に選択してインストールを実行できます。

管理対象サーバーにパッチをインストールするには、次の手順を実行します。

1. ナビゲーションペインで、[**ライブラリ**] を選択してから [**パッチ**] を選択します。
2. [パッチ] を展開して、特定のUnixオペレーティングシステムを選択します。
3. 内容ペインで、パッチを選択します。
4. [表示] ドロップダウンリストから、[サーバー] (または [サーバーグループ]) を選択します。
5. [表示] ドロップダウンリストから、[パッチがインストールされていないサーバー] (または [パッチがインストールされていないサーバーグループ]) を選択します。
6. プレビューペインで、1つまたは複数のサーバーを選択します。
7. [**アクション**] メニューで [**パッチのインストール**] を選択します。

   [パッチのインストール] ウィンドウの最初のステップ: サーバーとサーバーグループが表示されます。各ステップの手順については、次の項を参照してください。

   - インストールオプションの設定
   - 再起動オプションの設定
   - インストールスクリプトの指定
   - パッチのインストールのスケジュール設定
   - 電子メール通知の設定
   - パッチのインストールのプレビュー
   - パッチのインストールジョブの進行状況の表示

   1つのステップが完了したら、[**次へ**] をクリックして次のステップへ進みます。[**ジョブの開始**] をクリックする前に、ステップリストに表示される完了したステップをクリックすることで、そのステップに戻って変更を行うことができます。
8. インストールジョブを起動する準備ができたら、[**ジョブの開始**] をクリックします。

   ジョブを後で実行するようにスケジュール設定している場合でも、ジョブの開始後にパラメーターを変更することはできません。

ジョブが完了するまで [パッチのインストール] ウィンドウが開いたままの場合、[すべての管理対象サーバー] ウィンドウの [パッチコンプライアンス] 列が更新されて、関連するサーバーの修正済みのコンプライアンス数 (括弧内) が反映されます。[F5] キーを押すか、[**表示**] メニューの [**更新**] を選択して、[パッチのプレビュー] ペインの情報を更新します。

インストールオプションの設定

次のタイプのパッチのインストールオプションを指定することができます。

- パッチがダウンロードされたらすぐにパッチのインストールを行うか、日時を指定して後でインストールを行う。
- いずれか1つのパッチでエラーが発生した場合でも、パッチのインストールプロセスを中断しない。
- さまざまなコマンドラインオプションを使用してインストールを行う。

これらのオプションを設定するには、次の手順を実行します。

1. [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [インストールオプション] ステップに進みます。
2. 次のいずれかのステージインストールオプションを選択します。

   継続: すべてのフェーズを連続する1つの操作として実行できます。

   ステージ: ダウンロードとインストールをスケジュール設定して別々に実行することができます。
3. いずれかのパッチでエラーが発生した場合でもパッチのインストールプロセスを続行する場合は、[エラーオプション] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。
4. [インストールコマンド] テキストボックスに、表示されるコマンドのコマンドライン引数を入力します。
5. [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

再起動オプションの設定

サーバーの再起動によるダウンタイムを最小限に抑えるため、サーバーを再起動するタイミングを制御できます。ベンダーの再起動割り当てを調整、パッチをインストールするたびにサーバーを再起動、すべてのサーバーの再起動を完全に抑制、またはすべてのパッチがインストールされるまで再起動を延期することができます。

[パッチのインストール] ウィンドウで再起動オプションを選択する場合、Hewlett PackardではUnixの再起動推奨設定 (「パッチのプロパティの指定に基づいてサーバーを再起動する」オプション) を使用することを推奨しています。Unix の再起動設定を使用できない場合は、単一再起動オプション (「すべてのパッチがインストールされるまでサーバーを再起動しない」オプション) を選択します。

パッチのインストールの完了後にサーバーを再起動するかどうかを指定するオプションです。このオプションは、[パッチのインストール] ウィンドウから起動したジョブのみに適用されます。このオプションを設定しても、パッチのプロパティウィンドウの [インストールパラメーター] タブにある [再起動が必要] オプションが変更されることはありません。次に示すオプションの設定は、最初のオプションを除いて、[再起動が必要] オプションの設定よりも優先します。

- **パッチのプロパティの指定に基づいてサーバーを再起動する**: デフォルトでは、パッチプロパティの [再起動が必要] オプションの設定に従って再起動が行われます。
- **各パッチのインストール後にサーバーを再起動**: パッチプロパティの [再起動が必要] オプションが設定されていない場合でも、サーバーを再起動します。複数のパッチをインストールする場合、サーバーの再起動も複数回行われます。
- **すべてのサーバーの再起動を抑制**: パッチプロパティの [再起動が必要] オプションが設定されている場合でも、サーバーを再起動しません(ベンダー設定によっては、抑制オプションを無視して強制的に再起動を行う場合があります)。

- **すべてのパッチがインストールされるまでサーバーを再起動しない**: 選択したパッチの中に [再起動が必要] オプションが設定されているものが含まれていても、他のパッチにそのオプションが設定されていない場合、すべてのパッチのインストール後にサーバーが1回再起動されます。選択したパッチの中に [再起動が必要] オプションが設定されているものがない場合、サーバーは再起動されません。

再起動オプションを設定するには、次の手順を実行します。

1. [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [アクション前と後] ステップに進みます。
2. いずれかの再起動オプションを選択します。
3. [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

インストールスクリプトの指定

パッチごとにインストールの前または後に実行するコマンドまたはスクリプトを指定できます。インストール前スクリプトでは、たとえば、管理対象サーバー上で特定の条件をチェックすることができます。条件が満たされない場合やインストール前スクリプトが失敗した場合、パッチはインストールされません。インストール前スクリプトを使用すると、パッチを適用する前にサービスやアプリケーションをシャットダウンすることもできます。インストール後スクリプトを使用すると、管理対象サーバー上でクリーンアッププロセスを実行することができます。

また、インストールフェーズまたはダウンロードフェーズの前または後に、管理対象サーバー上で次のタイプのスクリプトを実行するように指定することもできます。

- **ダウンロード前**: SAから管理対象サーバーにパッチをダウンロードする前に実行するスクリプト。[インストールオプション] ステップで [ステージ] を選択した場合にのみ利用できます。
- **ダウンロード後**: SAから管理対象サーバーにパッチをダウンロードした後で、パッチをインストールする前に実行するスクリプト。[インストールオプション] ステップで [ステージ] を選択した場合にのみ利用できます。
- **インストール前**: 管理対象サーバーにパッチをインストールする前に実行するスクリプト。
- **インストール後**: 管理対象サーバーにパッチをインストールした後に実行するスクリプト。

インストール前スクリプトを指定するには、次の手順を実行します。

1. [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [アクション前と後] ステップに進みます。
2. [インストール前] タブを選択します。各タブでさまざまなスクリプトとオプションを指定できます。
3. [スクリプトの有効化] を選択します。このオプションを選択すると、タブのフィールドの残りの部分が有効になります。[スクリプトの有効化] を選択しない場合、スクリプトは実行されません。
4. [保存されたスクリプト] または [アドホックスクリプト] を選択します。

   保存されたスクリプトは、前にSA Webクライアントを使用してServer Automationに保存されたものです。スクリプトを指定するには、[**選択**] をクリックします。
5. スクリプトでコマンドラインフラグが必要である場合、[コマンド] テキストボックスにフラグを入力します。
6. 実行時オプションの情報を選択します。ユーザーアカウントにroot以外を選択した場合は、ユーザー名とパスワードを入力します。このユーザーによってスクリプトが管理対象サーバー上で実行されます。
7. スクリプトがエラーを返した場合にインストールを停止するには、[エラー] チェックボックスを選択します。
8. [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

パッチのインストールのスケジュール設定

パッチ適用の2つのフェーズは切り離すことができます。そのため、パッチのインストール (デプロイ) とパッチのダウンロード (ステージング) を独立して実行するようにスケジュール設定することができます。

パッチのインストールをスケジュール設定するには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [スケジュール設定] ステップに進みます。

デフォルトで、[スケジュール設定] ステップにはインストールフェーズ用のスケジュール設定オプションのみが表示されます。[インストールオプション] ステップで [ステージ] を選択した場合、ダウンロードフェーズ用のスケジュール設定オプションも表示されます。

2 次のいずれかのインストールフェーズオプションを選択します。

— **ただちにタスクを実行**: [サマリープレビュー] ステップでプレビュー分析を行うことができます。ダウンロードフェーズ用のスケジュール設定オプションは、[**ダウンロード後ただちに実行**] です。

— **次の時刻にタスクを実行**: 日付と時刻を指定して、後でダウンロードまたはインストールを実行することができます。

3 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

➤ スケジュール設定したパッチのインストールは、パッチのダウンロードが完了している場合でも、(実行前に) キャンセルできます。

電子メール通知の設定

ダウンロード操作やインストール操作が正常に終了した、あるいはエラーで終了したときに、ユーザーに知らせるために電子メール通知を設定できます。

電子メール通知を設定するには、次の手順を実行します。

1 [パッチのインストール] ウィンドウで、[**次へ**] をクリックして [通知] ステップに進みます。

2 ジョブが成功したときの通知ステータスを設定するには、  アイコンを選択します。ジョブが失敗したときの通知ステータスを設定するには、  アイコンを選択します。デフォルトでは、[通知] ステップにはインストールフェーズ用の通知ステータスのみが表示されます。

3 [チケットID] フィールドに、このジョブに割り当てるチケットIDを入力します。

4 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのインストール] ウィンドウを閉じます。

➤ [インストールオプション] ステップで [ステージ] を選択した場合、[通知] ペインにダウンロードとインストールの両方のフェーズに対する通知オプションが表示されます。

パッチのインストールのプレビュー

インストールのプレビューでは、サーバーのパッチの状態に関する最新のレポートが表示されます。インストールのプレビューは、管理対象サーバーにインストールされるパッチと必要なサーバーの再起動のタイプを確認するためのオプションステップです。プレビュープロセスでは、パッチのインストール対象として選択したサーバーに該当するパッチがすでにインストールされているかどうかを確認します。システム管理者がパッチを手動でインストールしている場合、サーバーにパッチがすでにインストールされている可能性があります。このような場合、SAではパッチの存在を把握できません。

プレビューでは、特定のUnix製品を必要とするパッチ、および他のパッチを置き換えるパッチや他のパッチで置き換えられるパッチなどの、依存関係情報に関するレポートも作成されます。依存関係が満たされていない場合は、SAにその状態を示すエラーメッセージが表示されます。

➤ インストールのプレビューでは、パッチが適用済みの状態をシミュレートするため、サーバーの動作に関するレポートは行われません。

パッチのインストールをプレビューするには、次の手順を実行します。

1 [パッチのインストール]ウィンドウで、[**次へ**]をクリックして[サマリーレビュー]ステップに進みます。

2 ウィンドウの上部にサーバー、サーバーグループ、およびパッチについて表示されている情報を確認します。

3 (オプション)[**プレビュー**]をクリックし、パッチのインストール時に実行される個々のアクションを表示します。テーブルの行を選択すると、プレビューしているアクションの詳細が表示されます。

4 [**ジョブの開始**]をクリックしてインストールジョブを起動するか、[**キャンセル**]をクリックしてインストールを起動せずに[パッチのインストール]ウィンドウを閉じます。

[スケジュール設定]ステップで[ただちにタスクを実行]を選択すると、ジョブがすぐに開始します。[次の時刻にタスクを実行]を選択すると、指定した日時にジョブが開始します。

パッチのインストールジョブの進行状況の表示

アクションが完了したか失敗したかなど、パッチのインストール(ジョブ)の進行状況を確認することができます。

ジョブの進行状況を表示するには、次の手順を実行します。

1 [パッチのインストール]ウィンドウで、[**次へ**]をクリックして[ジョブの進行状況]ステップに進みます。これにより、インストールジョブが開始されます。

進行状況バーとテキストで、テーブル内のアクションがどの程度完了したかを確認できます。次のアクションをサーバーごとに実行できます。

- **分析**: Server Automationは、インストールに必要なパッチの確認、管理対象サーバーにインストールされた最新パッチのチェック、他に実行が必要なアクションの確認を行います。
- **ダウンロード**: Server Automationから管理対象サーバーにパッチをダウンロードします。
- **インストール**: ダウンロードの完了後、パッチをインストールします。
- **最後に再起動**: [インストール前後のアクション]ステップでこのアクションを指定すると、サーバーが再起動します。
- **インストール前スクリプト / インストール後スクリプト / ダウンロード前スクリプト / ダウンロード後スクリプト**: [インストール前後のアクション]ステップでこのアクションを指定した場合、アンインストール前または後にスクリプトが実行されます。
- **インストールと再起動**: パッチをインストールすると、サーバーも再起動されます。
- **確認**: インストールしたパッチは、ソフトウェア登録に追加されます。

2 特定のアクションに関する詳細を追加表示するには、テーブルの行を選択して、ジョブの開始時刻と完了時刻を表示します。ナビゲーションペインで、[ジョブとセッション]を選択してジョブに関する詳細を確認します。ジョブログの参照については、『SAユーザーガイド: Server Automation』を参照してください。

3 [**ジョブの終了**]をクリックしてジョブを実行しないようにするか、[**閉じる**]をクリックして[パッチのインストール]ウィンドウを閉じます。

パッチのアンインストール

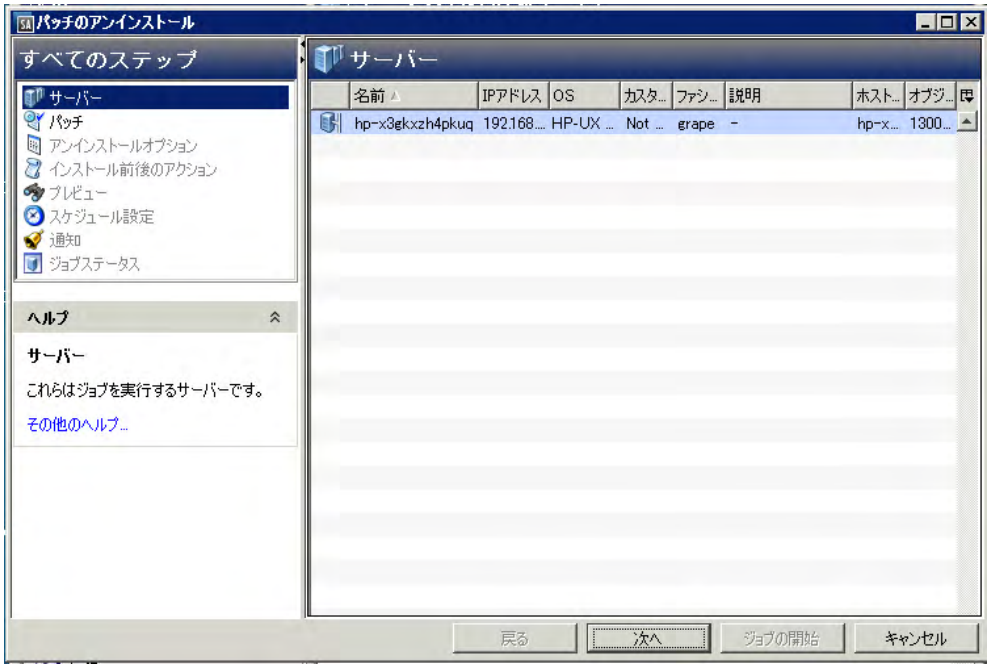
SAでは、Unixパッチの管理対象サーバーからのアンインストール(削除)方法やアンインストール条件を細かく制御することができます。問題を最小限に抑えるため、パッチのアンインストールは1つずつ行う必要があります。SAを使用して、SAでインストールしたものではないパッチをアンインストールすることはできません。

これらの条件を適切に管理できるように、SAでは、次のことを行うことができます。

- サーバーの再起動オプション、およびインストール前スクリプト/インストール後スクリプトの管理。
- パッチのアンインストールのシミュレート (プレビュー)。
- アンインストールプロセスのステータスを把握するための電子メール通知の設定。

これらの条件は、[パッチのアンインストール] ウィンドウを使用して設定することができます。

図34 [パッチのアンインストール] ウィンドウ



アンインストールフラグ

Unix パッチをアンインストールする際には、アンインストールフラグを指定できます。ただし、Server Automation では、デフォルトのアンインストールフラグが使用され、これらのフラグを使用してパッチをアンインストールする必要があります。そのため、Server Automationから渡されるデフォルトのアンインストールフラグを無効にするフラグや矛盾するフラグを指定しないようにする必要があります。

次の表に、Server Automationで使用されるデフォルトのアンインストールフラグを示します。

表27 デフォルトのアンインストールフラグ

オペレーティングシステム/パッチタイプ	フラグ
AIX	`-u -g -X`
AIXの拒否オプション	`-r -g -X`
HP-UX	なし

パッチのアンインストール

管理対象サーバーからパッチを削除するには、次の手順を実行します。

1 ナビゲーションペインで、[**ライブラリ**] を選択してから [**パッチ**] を選択します。

2 [パッチ] を展開して、特定のUnixオペレーティングシステムを選択します。

3 内容ペインで、パッチを選択します。

4 [表示] ドロップダウンリストから、[サーバー] を選択します。

5 [表示] ドロップダウンリストで、[パッチがインストールされたサーバー] を選択します。

6 プレビューペインで、1つまたは複数のサーバーを選択します。

7 [**アクション**] メニューで [**パッチのアンインストール**] を選択します。

[パッチのアンインストール] ウィンドウの最初のステップ (サーバー) が表示されます。
各ステップの手順については、次の項を参照してください。

- 再起動オプションの設定
- インストール前スクリプト/インストール後スクリプトの指定
- パッチのアンインストールのスケジュール設定
- 電子メール通知の設定
- パッチのアンインストールジョブの進行状況の表示

1つのステップが完了したら、[**次へ**] を選択して次のステップへ進みます。[**ジョブの開始**] をクリックする前に、ステップリストに表示される完了したステップをクリックすることで、そのステップに戻って変更を行うことができます。

8 アンインストールジョブを起動する準備ができたら、[**ジョブの開始**] を選択します。

ジョブを後で実行するようにスケジュール設定している場合でも、ジョブの開始後にパラメーターを変更することはできません。

ジョブが完了するまで [パッチのアンインストール] ウィンドウが開いたままの場合、[すべての管理対象サーバー] ウィンドウの [パッチコンプライアンス] 列が更新されて、関連するサーバーの修正済みのコンプライアンス数 (括弧内) が反映されます。[F5] キーを押すか、[表示] メニューの [更新] を選択して、[パッチのプレビュー] ペインの情報を更新します。

アンインストールオプションの設定

次のタイプのパッチのアンインストールオプションを指定することができます。

- いずれか1つのパッチでエラーが発生した場合でも、パッチのアンインストールプロセスを中断しない。
- さまざまなコマンドラインオプションを使用してアンインストールを行う。

これらのオプションを設定するには、次の手順を実行します。

1 [パッチのアンインストール] ウィンドウで、[**次へ**] をクリックして [アンインストールオプション] ステップに進みます。

2 いずれかのパッチでエラーが発生した場合でもパッチのインストールプロセスを続行する場合は、[エラーオプション] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

3 [アンインストールコマンド] テキストボックスに、表示されるコマンドのコマンドライン引数を入力します。

4 [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのアンインストール] ウィンドウを閉じます。

再起動オプションの設定

サーバーの再起動によるダウンタイムを最小限に抑えるため、サーバーを再起動するタイミングを制御できます。ベンダーの再起動割り当てを調整、パッチを削除するたびにサーバーを再起動、すべてのサーバーの再起動を完全に抑制、またはすべてのパッチがアンインストールされるまで再起動を延期することができます。

[パッチのアンインストール] ウィンドウで再起動オプションを選択する場合、Hewlett PackardではUnixの再起動推奨設定 (「パッチのプロパティの指定に基づいてサーバーを再起動する」オプション) を使用することを推奨しています。Unixの再起動設定を使用できない場合は、[パッチのアンインストール] ウィンドウで単一再起動オプション (「すべてのパッチがインストールされるまでサーバーを再起動しない」オプション) を選択します。

パッチのアンインストールの完了後にサーバーを再起動するかどうかを指定するオプションです。このオプションは、[パッチのアンインストール] ウィンドウから起動したジョブのみに適用されます。このオプションを設定しても、パッチのプロパティウィンドウの [アンインストールパラメーター] タブにある [再起動が必要] オプションが変更されることはありません。次に示すオプションの設定は、最初のオプションを除いて、[再起動が必要] オプションの設定よりも優先します。

- **パッチのプロパティの指定に基づいてサーバーを再起動する**: デフォルトでは、パッチプロパティの [再起動が必要] オプションの設定に従って再起動が行われます。
- **各パッチのインストール後にサーバーを再起動**: パッチプロパティの [再起動が必要] オプションが設定されていない場合でも、サーバーを再起動します。複数のパッチをインストールする場合、サーバーの再起動も複数回行われます。
- **すべてのサーバーの再起動を抑制**: パッチプロパティの [再起動が必要] オプションが設定されている場合でも、サーバーを再起動しません(ベンダー設定によっては、抑制オプションを無視して強制的に再起動を行う場合があります)。
- **すべてのパッチがインストールされるまでサーバーを再起動しない**: 選択したパッチの中に [再起動が必要] オプションが設定されているものが含まれていても、他のパッチにそのオプションが設定されていない場合、すべてのパッチのインストール後にサーバーが1回再起動されます。選択したパッチの中に [再起動が必要] オプションが設定されているものがない場合、サーバーは再起動されません。

再起動オプションを設定するには、次の手順を実行します。

1. [パッチのアンインストール] ウィンドウで、[**次へ**] をクリックして [アクション前と後] ステップに進みます。
2. いずれかの再起動オプションを選択します。
3. [**次へ**] をクリックして次のステップに進むか、[**キャンセル**] をクリックして [パッチのアンインストール] ウィンドウを閉じます。

インストール前スクリプト/インストール後スクリプトの指定

パッチごとにアンインストールの前または後に実行するコマンドまたはスクリプトを指定できます。アンインストール前スクリプトでは、たとえば、管理対象サーバー上で特定の条件をチェックすることができます。条件が満たされない場合やアンインストール前スクリプトが失敗した場合、パッチはサーバーから削除されません。アンインストール前スクリプトを使用すると、サーバーからパッチを削除する前にサービスやアプリケーションをシャットダウンすることもできます。アンインストール後スクリプトを使用すると、管理対象サーバー上でクリーンアッププロセスを実行することができます。

パッチのアンインストールの前または後に、管理対象サーバー上で次のタイプのスクリプトを実行するように指定することもできます。

- **アンインストール前**: 管理対象サーバーからパッチを削除する前に実行するスクリプト。
- **アンインストール後**: 管理対象サーバーからパッチを削除した後で実行するスクリプト。

スクリプトを指定するには、次の手順を実行します。

1. [パッチのアンインストール] ウィンドウで、[**次へ**] をクリックして [アクション前と後] ステップに進みます。

2 [アンインストール前] または [アンインストール後] タブを選択します。

各タブでさまざまなスクリプトとオプションを指定できます。

3 [スクリプトの有効化] を選択します。

このオプションを選択すると、タブのフィールドの残りの部分が有効になります。[スクリプトの有効化] を選択しない場合、スクリプトは実行されません。

4 [保存されたスクリプト] または [アドホックスクリプト] を選択します。

保存されたスクリプトは、前にSA Webクライアントを使用してServer Automationに保存されたものです。スクリプトを指定するには、**[選択]** をクリックします。

5 スクリプトでコマンドラインフラグが必要である場合、[コマンド] にフラグを入力します。

6 実行時オプションの情報を選択します。ユーザーアカウントに root 以外を選択した場合は、ユーザー名とパスワードを入力します。このユーザーによってスクリプトが管理対象サーバー上で実行されます。

7 スクリプトがエラーを返した場合にアンインストールを停止するには、[エラー] を選択します。

パッチのアンインストールのスケジュール設定

パッチをサーバーからただちに削除するか、日時を指定して後で削除するようにスケジュール設定することができます。

パッチのアンインストールをスケジュール設定するには、次の手順を実行します。

1 [パッチのアンインストール] ウィンドウで、**[次へ]** をクリックして [スケジュール設定] ステップに進みます。

2 次のいずれかのインストールフェーズオプションを選択します。

- **ただちにタスクを実行**: [サマリープレビュー] ステップでアンインストールを行うことができます。
- **次の時刻にタスクを実行**: アンインストールを行う日付と時刻を指定することができます。

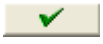
3 **[次へ]** をクリックして次のステップに進むか、**[キャンセル]** をクリックして [パッチのアンインストール] ウィンドウを閉じます。

電子メール通知の設定

パッチのアンインストール操作が正常に終了した、あるいはエラーで終了したときに、ユーザーに知らせるために電子メール通知を設定できます。

電子メール通知を設定するには、次の手順を実行します。

1 [パッチのアンインストール] ウィンドウで、**[次へ]** をクリックして [通知] ステップに進みます。

2 ジョブが成功したときの通知ステータスを設定するには、  アイコンを選択します。ジョブが失敗したときの通知ステータスを設定するには、  アイコンを選択します。デフォルトでは、[通知] ステップにはアンインストールフェーズ用の通知ステータスのみが表示されます。

3 [チケットID] フィールドに、このジョブに割り当てるチケットIDを入力します。

4 **[次へ]** をクリックして次のステップに進むか、**[キャンセル]** をクリックして [パッチのアンインストール] ウィンドウを閉じます。

パッチのアンインストールのプレビュー

アンインストールのプレビューでは、サーバーのパッチの状態に関する最新のレポートが表示されます。アンインストールのプレビューは、管理対象サーバーから削除されるパッチを確認するためのオプションステップです。プレビュープロセスでは、パッチのアンインストール対象として選択したサーバーに該当するパッチがインストールされているかどうかを確認します。

アンインストールのプレビューでは、サーバーからパッチを削除した場合のシステムの動作に関するレポートやシミュレートは行われません。

パッチのアンインストールをプレビューするには、次の手順を実行します。

1. [パッチのアンインストール] ウィンドウで、[**次へ**] をクリックして [サマリーレビュー] ステップに進みます。
2. ウィンドウの上部にサーバー、サーバーグループ、およびパッチについて表示されている情報を確認します。
3. (オプション) [**プレビュー**] をクリックし、パッチのアンインストール時に実行される個々のアクションを表示します。テーブルの行を選択すると、プレビューしているアクションの詳細が表示されます。
4. [**ジョブの開始**] をクリックしてジョブを起動するか、[**キャンセル**] をクリックしてアンインストールを起動せずに [パッチのアンインストール] ウィンドウを閉じます。

   [スケジュール設定] ステップで [ただちにタスクを実行] を選択すると、ジョブがすぐに開始します。[次の時刻にタスクを実行] を選択すると、指定した日時にジョブが開始します。

パッチのアンインストールジョブの進行状況の表示

アクションが完了したか失敗したかなど、パッチのアンインストール (ジョブ) の進行状況を確認することができます。

ジョブの進行状況を表示するには、次の手順を実行します。

1. [パッチのアンインストール] ウィンドウで、[**次へ**] をクリックして [ジョブの進行状況] ステップに進みます。進行状況バーとテキストで、テーブル内のアクションがどの程度完了したかを確認できます。次のアクションをサーバーごとに実行できます。
   - **分析**: Server Automation は、アンインストールに必要なパッチの確認、管理対象サーバーにインストールされた最新パッチのチェック、他に実行が必要なアクションの確認を行います。
   - **アンインストール**: パッチをアンインストールします。
   - **最後に再起動**: [インストール前後のアクション] ステップでこのアクションを指定すると、サーバーが再起動します。
   - **アンインストール前スクリプト/アンインストール後スクリプト**: [インストール前後のアクション] ステップでこのアクションを指定した場合、アンインストール前または後にスクリプトが実行されます。
   - **アンインストールと再起動**: パッチをインストールすると、サーバーも再起動されます。
   - **確認**: インストールしたパッチは、ソフトウェア登録に追加されます。
2. 特定のアクションに関する詳細を追加表示するには、テーブルの行を選択して、ジョブの開始時刻と完了時刻を表示します。ナビゲーションペインで、[ジョブとセッション] を選択してジョブに関する詳細を確認します。ジョブログの参照については、『SAユーザーガイド: Server Automation』を参照してください。
3. [**ジョブの終了**] をクリックしてジョブを実行しないようにするか、[**閉じる**] をクリックして [パッチのアンインストール] ウィンドウを閉じます。

第8章 Oracle Enterprise Linuxパッチ管理

HPSA Patch Importer for Oracle Enterprise Linux (OEL) では、Oracle Unbreakable Linux Network (ULN) からサブスクライブ済みチャネルのパッケージをインポートして、HPSAでインポートしたチャネルごとに対応するソフトウェアポリシーを自動的に作成できます。これはコマンドラインから手動で実行できます。また、定期的にインポートを実行するcronジョブの一部として実行することもできます。

始める前に

前提条件

HPSA Patch Importer for Oracle Enterprise Linuxを使用するには、次の前提条件を満たしている必要があります。

- Oracle Unbreakable Linuxストアからサポートライセンスを購入して、有効なCSI (カスタマーサポートID) を取得する必要があります。詳細については、**https://linux.oracle.com**を参照してください。
- Oracle Unbreakable Linux Network (ULN) に登録して、シングルサインオン用のユーザー名/パスワードを取得する必要があります。
- このツールを使用するシステムに100GB以上の空きディスク容量が必要です。

Oracleから購入するサポートライセンスのタイプに応じて、Oracleがサポートしている任意のチャネルをサブスクライブできます。ただし、HPSA Patch Importerは、HPSAでサポートしているプラットフォームのパッケージのみがインポートされます。

制限事項

HPSA Patch Importer for Oracle Enterprise Linuxは、HPSAコアプラットフォームのみで実行する必要があります。

Patch Importerのファイルの場所

表28 Patch Importerのファイルの場所

バイナリ	/opt/opsware/patch_importer/bin/
構成ファイル	/etc/opt/opsware/patch_importer/uln_import.conf
ログファイル	/var/log/opsware/patch_importer/patch_importer.log
パッケージダウンロードディレクトリ(ダウンロードしたパッケージを一時的に保管する場所)ファイルシステム上に100 GB以上の空きディスク容量を確保する必要があります。	/var/opt/opsware/patch_importer/
ライブラリ	/opt/opsware/patcher_importer/patch_importer/

作業の開始

HPSA Patch Importer for Oracle Enterprise Linuxは、次のタスクに使用できます。

1. 構成ファイル(/etc/opt/opsware/patch_importer/uln_import.conf)を編集して、必要な情報を指定する。
2. システムをULNに登録する。
3. ULNにログオンしてチャネルをサブスクライブする。
4. パッケージをインポートする。

最初の3つのタスクは1回(または限られた回数)だけ実行します。4番目のタスク(パッケージのインポート)はスケジュール設定して定期的に実行できます。

重要: このツールはコアホスト上でrootユーザーとして実行する必要があります。

構成ファイルの編集

HPSA Patch Importer for Oracle Enterprise Linuxの構成ファイルは、/etc/opt/opsware/patch_importer/uln_import.confにあります。構成ファイルは複数のセクションにわかれています。[main]と[system_id]の2つのセクションは必須で、その他のセクションはオプションで省略可能です。オプションのセクションは、チャネル固有の動作を制御するのに使用します。

次の表は、構成ファイルの各種セクションについて説明したものです。

[main] セクション

[main] セクションには、一般構成オプションがあります。

表29 [main] セクションのオプション

プロパティ名	予期される値	説明
username	文字列 (電子メールの形式)	ULNユーザー名
password	文字列	ULNパスワード
CSI	文字列 (連続する数字)	OracleカスタマーサポートID
hide_passwords	1、0 (デフォルト: 1)	パスワードを難読化するかどうかを指定します。 1 に設定すると、ツールを最初に使用したときに、このファイルのすべてのパスワードが難読化されます。難読化されたパスワードは難読化された状態のままになり、元に戻すことはできません。 パスワードが変更された場合は、クリアテキストのパスワードを再度入力すると、次回の実行時に入力したパスワードが難読化されます。ただし、hide_passwordsが1に設定されている必要があります。 また、--hide_passwords コマンドラインオプションを使用して、パスワードを難読化することもできます。コマンドラインで --hide_passwords オプションを指定した場合、構成ファイルの設定内容ではなく、指定したコマンドラインオプションが使用されます。
server_uri	有効なURI (デフォルト: https://linux-update.oracle.com/XMLRPC)	ULN RPCサーバーへのURI。デフォルトのULNインスタンスをポイントします。この時点でライブフェイルオーバー用のサーバーリストはサポートしていません。プライマリサーバーがダウンした場合、いずれかのミラーをポイントするように手動で変更する必要があります。
system_id	有効なファイルパス(デフォルト: /var/opt/opsware/oel_import/system_id)	system_idを保管する場所。ULNにシステムを登録している場合。 警告: このファイルの場所は削除または変更しないでください。削除または変更した場合、ULNに登録し直す必要があります。
proxy_host	<FQHN>:[<ポート>]	HTTPプロキシを使用する場合は、ここで指定します。
proxy_user	文字列	HTTPプロキシ認証が必要な場合は、プロキシのユーザー名を指定します。proxy_hostが指定されていない場合は無視されます。
proxy_pass	文字列	HTTPプロキシ認証が必要な場合は、プロキシのユーザーパスワードを指定します。proxy_hostが指定されていない場合は無視されます。
proxy_agent	文字列	HTTPプロキシ認証が必要な場合は、認証用にオプションでproxy_agent HTTP ヘッダーを指定できます。

表29 [main] セクションのオプション（続き）

プロパティ名	予期される値	説明
opsware_user	文字列	HPSAユーザーのコンテキストでパッケージをインポートすることができます。その場合は、ここでユーザー名を指定します。opsware_userを省略した場合、パッケージのインポートはシステム(内部)ユーザーのコンテキストで実行されます。
opsware_pass	文字列	HPSAユーザーのパスワード。opsware_userが指定されていない場合は無視されます。
continue_on_error	1、0(デフォルト:1)	このオプションはサポートされていません。
import_threads	数値(デフォルト:10)	インポートスレッドの最大数。これを非現実的な値に設定した場合、一部のソースネットワークが大きな負荷をサポートできずにサービスが停止する可能性があります。
limit_policy_description	1、0(デフォルト:1)	このオプションはサポートされていません。
channels	次のようにスペースや改行で区切ったチャネルの明示的なリストを指定できます。 channels: LABEL1 LABEL2 LABELn	channelsオプションを指定しない場合、HPSAでサポートされるすべての最上位(親)チャネルと、この構成ファイル内に専用の[channel]セクションを持つチャネルが有効になります。
package_path	有効なディレクトリパス。(デフォルト:/ULN/Packages/$channel_name)	特定のチャネルのパッケージのアップロード先のフォルダー。 $channel_nameは特殊なプレースホルダーです。このプレースホルダーは実行時にチャネルで置き換えられます。 パッケージが承認されるまで使用されないようにパッケージを隔離することができます。ただし、未承認フォルダーに対するアクセス権で、アクセスできるサーバーを確実に制限する必要があります。この目的で、特殊なフォルダーに対するpackage_pathを構成することができます。例:package_path=/ULN/Packages/Unapproved/$channel_name
channel_path	有効なディレクトリパス。(デフォルト:/ULN/Channels/$channel_name Policy)	特定のチャネルに対するチャネルソフトウェアポリシーを作成するフォルダー。 $channel_nameは特殊なプレースホルダーです。このプレースホルダーは実行時にチャネルで置き換えられます。

表29 [main] セクションのオプション（続き）

プロパティ名	予期される値	説明
erratum_path	有効なディレクトリパス。(デフォルト: /ULN/Errata/$erratum_type Policies/$erratum_name)	特定のチャネルに対するエラッタソフトウェアポリシーを作成するフォルダー。 $erratum_type と $erratum_name は特殊なプレースホルダーです。これらは、実行時にエラッタタイプとエラッタ名に置き換えられます。 チャネル別にロールアップポリシーを作成する代わりに、月別に作成することができます。以下に例を示します。 errata_path=/ULN/Errata/$Y-$m Advisory Roll-Up Policy $Y と $m は、それぞれ年と月に対応する特殊なプレースホルダーです。 この構成は現在使用されていません。
errata_path	有効なディレクトリパス。(デフォルト: /ULN/Errata/$channel_name Advisory Roll-Up Policy)	特定のチャネルに対するエラッタソフトウェアポリシーを作成するフォルダー。 $channel_name は特殊なプレースホルダーです。このプレースホルダーは実行時にチャネルで置き換えられます。 この構成は現在使用されていません。
package_search_path	次のようにスペースや改行で区切られたディレクトリパスの明示的なリストを指定できます。 channels: PATH1 PATH2 PATHn デフォルト: /Package Repository/OS Media/$opsware_platform /Package Repository/All Red Hat Linux/$opsware_platform /Migrated/Package Repository/Customer Independent/$opsware_platform	以前にアップロードしたパッケージを検索するパス。 $opsware_platform は特殊なプレースホルダーです。このプレースホルダーは実行時にプラットフォーム名で置き換えられます。

[system_profile] セクション

このセクションは、システムプロファイルのプロパティを指定するのに使用します。この情報は、ULN への登録に使用します。通常は、パッケージをダウンロードする前に、最初にシステムを ULN に登録する必要があります。登録すると、OSやハードウェアの情報を含むシステムプロファイルが作成されます。システムが登録されると、システムが実行されているプラットフォームに関連するデフォルトチャネルが ULN によって自動的に割り当てられます。ただし、HPSAはOEL以外のシステムで実行可能であるため、ここでは基本的に擬似システムプロファイルが生成されます。

システムプロファイルは、次の `[system_profile]` セクションの内容を使用して作成されます。

表30　　[system_profile] セクションのオプション

プロパティ名	予期される値	説明
profile_name	文字列 (デフォルト: ツールが実行されるシステムの FQDN)	プロファイルの名前。通常、これはツールが実行されるホストの完全修飾ドメイン名になります。
os_release	数値 (デフォルト: `5`)	Oracle Enterprise Linux OSのリリース番号。
release-name	文字列 (デフォルト: `enterprise-release`)	Oracle Enterprise Linux OSのリリース名。
architecture	X86またはx86_64 (デフォルト: `x86_64`)	OS アーキテクチャー。現在はx86 と x86_64 のみをサポートしています。
uuid	文字列	UUID。実行時に生成されます。 **警告**: システムへの影響が不明確な場合は、このプロパティを変更しないでください。このプロパティの使い方を誤ると、インポートツールが破損し、再登録が必要になる可能性があります。
rhnuuid	文字列	RHN UUID。実行時に生成されます。 **警告**: システムへの影響が不明確な場合は、このプロパティを変更しないでください。このプロパティの使い方を誤ると、インポートツールが破損し、再登録が必要になる可能性があります。

チャネル固有のセクション

ここでは、チャネル固有のセクションの例を示します。この例では、Oracle Enterprise Linux 5 Update 6パッチチャネルが有効化され、そのチャネルのすべてのパッケージで構成されるポリシーが作成されます。[main] セクションで`channels`オプションが指定されていない場合、このセクションはデフォルトで有効になることに注意してください。[main] セクションでchannelsオプションが指定されている場合は、enabledオプションを使用して明示的に有効化する必要があります。また、この例では、最上位チャネルに対してチャネルポリシーを作成したくないため、`channel_path`も定義しています。

```
[ol5_u6_x86_64_patch]
; enabled=1
# チャネルの各パッケージのすべてのバージョンをインポートできますが、デフォルトでは、
# 各パッケージの最新バージョンのみがインポートされます。ただし、
# すべてのバージョンをインポートする場合は、packages_only=1を併せて使用
# することをお勧めします。これは、各パッケージの複数のバージョンを含むポリシー
# を作成しても意味がないためです。
```

```
; which_packages=all
# このチャネルのパッケージをダウンロードした後に、
# ポリシーを手動で作成できます。また、which_packages=allと組み合わせて
# 次を使用すると便利です。
; packages_only=1
# ライブラリ内の対応するポリシーの横にある下位チャネルのパッケージを特定するには
# 次のようなパスを使用します。
; package_path=/ULN/Channels/$channel_name Packages
```

システムのULNへの登録

構成ファイルの編集が済んだら、システムをULNに登録することができます。

システムをULNに登録するには、次の手順を実行します。

1 –show_confオプションを指定して、/opt/opsware/patch_importer/bin/uln_importを実行します。

このオプションには、2つの主要な用途があります。このオプションは、現在の構成を表示するだけでなく、システムがULNに未登録の場合にシステムを登録します。

```
[root@vc002 patch_importer]# /opt/opsware/patch_importer/bin/uln_import
--show_conf
********** Configuration For ULN **********
Retrieving platform information from SA
Retrieving channel information from Oracle ULN
|
[system_profile]
rand_key_path        : /var/opt/opsware/crypto/wordbot/.randkey-rhn_import
package_path         : /var/opt/opsware/patch_importer/packages
which_packages       : latest
server_uri           : https://linux-update.oracle.com/XMLRPC
cache_path           : /var/opt/opsware/oel_import/cache
dbg_random_fail      : 0
erratum_path         : /$network_name/Errata/$erratum_type Policies/
$erratum_name
download_server_uri  : http://linux-update.oracle.com/XMLRPC
package_search_path  :
            /Package Repository/OS Media/$opsware_platform
            /Package Repository/All Red Hat Linux/$opsware_platform
            /Migrated/Package Repository/Customer Independent/
$opsware_platform

packages_only        : False
errata_path          : /$network_name/Errata/$parent_channel_name/$channel_name
Advisory Roll-Up Policy
hide_passwords       : 1
import_threads       : 5
show_config_only     : 0
tmp_path             : /var/opt/opsware/patch_importer
system_id            : /etc/opt/opsware/patch_importer/system_id
mode                 : all
continue_on_error    : 1
channel_path         : /$network_name/Channels/$parent_channel_name/
$channel_name Policy
```

```
[main]
rand_key_path        : /var/opt/opsware/crypto/wordbot/.randkey-rhn_import
erratum_path         : /ULN/Errata/$erratum_type Policies/$erratum_name
which_packages       : latest
package_path         : /ULN/Packages/$channel_name
download_server_uri  : http://linux-update.oracle.com/XMLRPC
package_search_path  :
/Package Repository/OS Media/$opsware_platform
/Package Repository/All Red Hat Linux/$opsware_platform
/Migrated/Package Repository/Customer Independent/$opsware_platform
packages_only        : False
csi                  : 1.234.567
proxy_host           : abc.acme.com:8080
errata_path          : /ULN/Errata/$channel_name Advisory Roll-Up Policy
import_threads       : 10
tmp_path             : /var/opt/opsware/patch_importer
system_id            : /etc/opt/opsware/patch_importer/system_id
channel_path         : /ULN/Channels/$channel_name Policy
continue_on_error    : 1
username             : test@hp.com
server_uri           : https://linux-update.oracle.com/XMLRPC
cache_path           : /var/opt/opsware/oel_import/cache
dbg_random_fail      : 0
password             : (Hidden)
hide_passwords       : 1
show_config_only     : 1
mode                 : all

<Configuration For Channel: ol5_x86_64_latest>

  Enabled         : True
  Packages Only   : False
  Which Packages  : latest
  Package Path    : /ULN/Packages/$channel_name
*****************************************
```

2 登録したシステムは、次のULNにある [**Systems**] タブに表示されます:**https://linux.oracle.com**デフォルトで、ULNでは最新のプラットフォームチャネルが新規に登録したシステムに自動的に割り当てられます。

`system_id`ファイルが`/etc/opt/opsware/patch_importer/uln/`に作成されます。ULNに登録できない場合は、`/var/log/opsware/patch_importer/patch_importer.log`にあるログファイルでエラーを確認することができます。また、必要な場合は、次のようにデバッグモードで`oel_import`を実行することもできます。

```
/opt/opsware/patch_importer/bin/uln_import --show_conf –v
```

ULNに登録する必用がある場合は、登録を行う前に古い`system_id`を削除し、ULNから登録済みのシステムを削除します。

```
rm –rf /etc/opt/opsware/patch_importer/uln/system_id
/opt/opsware/patch_importer/bin/uln_import –show_conf
```

ULNでのチャネルのサブスクライブとアンサブスクライブ

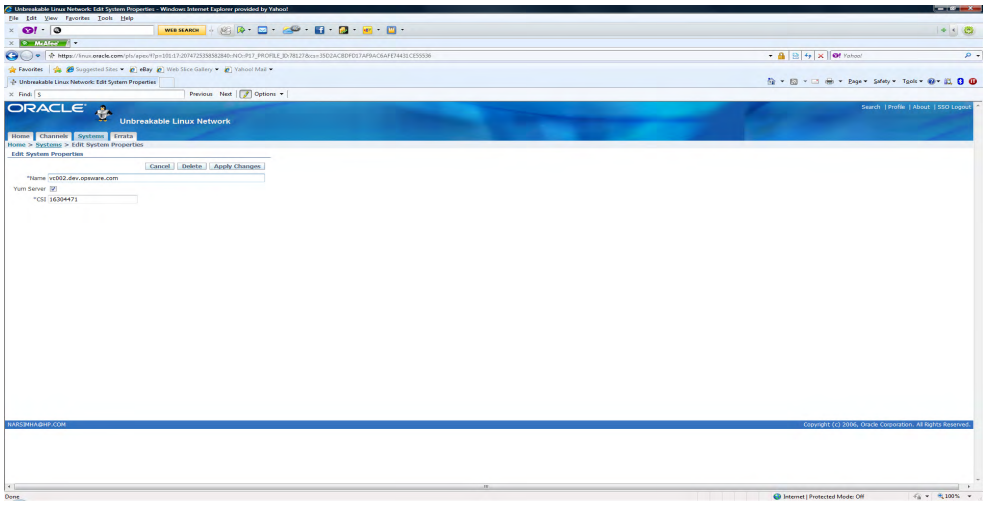
チャネルのサブスクライブとアンサブスクライブは、ULNで行う必要があります。サブスクライブ/アンサブスクライブを行うには、事前にシステムをYUMサーバーとして指定する必要があります。

登録済みシステムをYUMサーバーに指定するには、次の手順を実行します。

1 環境内にさまざまなEnterprise Linuxがデプロイされている場合は、利用可能なすべてのチャネルをサブスクライブするため、登録済みシステムの [**Edit System Properties**] タブにある [**Yum Server**] ボックスをオンにします。

重要: 必ず [**Yum Server**] ボックスをオンにしてください。このボックスをオンにしないと、ULNでチャネルが登録済みシステムのプラットフォームに関連するチャネルに制限されます。登録済みシステムを**Yum Server**として指定すると、現在利用可能な任意のチャネルをサブスクライブできるようになります。

2 [**Apply Changes**] をクリックして、変更内容を送信します。



登録済みシステムがYum Serverとして指定されたら、現在利用可能な任意のチャネルをサブスクライブできます。

チャネルをサブスクライブ/アンサブスクライブするには、次の手順を実行します。

1 登録済みシステムの [**Manage Subscriptions**] タブに移動します。

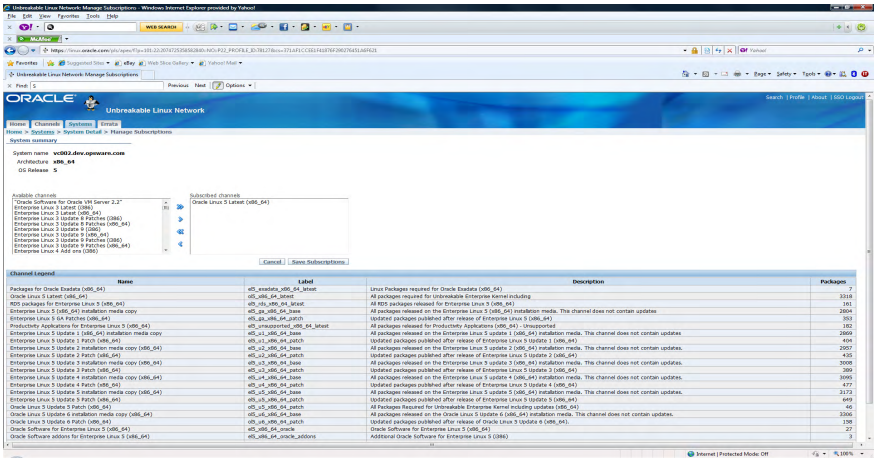
一部のチャネルには更新が含まれない場合があることに注意してください。これらはISOまたはリリースメディアのベースRPMです。一部のチャネルは他のチャネルのスーパーセットになっています。また、RedHatネットワークと異なり、ULNには「親チャネル」という概念はありません。

2 目的のチャネルを選択します。

3 チャネルをサブスクライブするには、[**Available channels**] 列から [**Subscribed channels**] 列にチャネルを移動します。

4 チャネルをアンサブスクライブするには、[**Subscribed channels**] 列から [**Available channels**] 列にチャネルを移動します。

5 [Save Subscriptions] をクリックします。



6 ULN からの目的のチャネルのサブスクライブが完了したら、-show_conf オプションを指定して /opt/opsware/patch_importer/bin/uln_import を実行し、チャネルが有効になっていることを確認することができます。

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import --show_conf
********** Configuration For ULN **********
Retrieving platform information from SA
Retrieving channel information from Oracle ULN
|
[system_profile]
rand_key_path         : /var/opt/opsware/crypto/wordbot/.randkey-rhn_import
package_path          : /var/opt/opsware/patch_importer/packages
which_packages        : latest
server_uri            : https://linux-update.oracle.com/XMLRPC
cache_path            : /var/opt/opsware/oel_import/cache
dbg_random_fail       : 0
erratum_path          : /$network_name/Errata/$erratum_type Policies/
$erratum_name
download_server_uri   : http://linux-update.oracle.com/XMLRPC
package_search_path   :
             /Package Repository/OS Media/$opsware_platform
             /Package Repository/All Red Hat Linux/$opsware_platform
             /Migrated/Package Repository/Customer Independent/
$opsware_platform

packages_only         : False
errata_path           : /$network_name/Errata/$parent_channel_name/
$channel_name Advisory Roll-Up Policy
hide_passwords        : 1
import_threads        : 5
show_config_only      : 0
tmp_path              : /var/opt/opsware/patch_importer
system_id             : /etc/opt/opsware/patch_importer/system_id
mode                  : all
continue_on_error     : 1
channel_path          : /$network_name/Channels/$parent_channel_name/
$channel_name Policy

[main]
rand_key_path         : /var/opt/opsware/crypto/wordbot/.randkey-rhn_import
```

```
erratum_path          : /ULN/Errata/$erratum_type Policies/$erratum_name
which_packages        : latest
package_path          : /ULN/Packages/$channel_name
download_server_uri   : http://linux-update.oracle.com/XMLRPC
package_search_path   :
/Package Repository/OS Media/$opsware_platform
/Package Repository/All Red Hat Linux/$opsware_platform
/Migrated/Package Repository/Customer Independent/$opsware_platform
packages_only         : False
csi                   : 12.345.678
proxy_host            : test.acme.com:8080
errata_path           : /ULN/Errata/$channel_name Advisory Roll-Up Policy
import_threads        : 10
tmp_path              : /var/opt/opsware/patch_importer
system_id             : /etc/opt/opsware/patch_importer/system_id
channel_path          : /ULN/Channels/$channel_name Policy
continue_on_error     : 1
username              : abc@hp.com
server_uri            : https://linux-update.oracle.com/XMLRPC
cache_path            : /var/opt/opsware/oel_import/cache
dbg_random_fail       : 0
password              : (Hidden)
hide_passwords        : 1
show_config_only      : 1
mode                  : all

<Configuration For Channel: el5_u5_i386_patch>

  Enabled         : True
  Packages Only   : False
  Which Packages  : latest
  Package Path    : /ULN/Packages/$channel_name


<Configuration For Channel: el5_u5_x86_64_patch>

  Enabled         : True
  Packages Only   : False
  Which Packages  : latest
  Package Path    : /ULN/Packages/$channel_name


****************************************
```

注: HPSA で現在サポートされていないプラットフォームのチャネルは除外されることに注意してください。たとえば、Enterprise Linux 3のチャネルをサブスクライブしても、HPSAでは無視されます。

パッケージのインポート

HPSA Patch Importerでは、ユーザーが`-package_only`オプションを指定してソフトウェアポリシーを作成しないようにした場合を除き、デフォルトでチャネルごとにソフトウェアポリシーが作成されます。

パッケージをインポートするには、次の手順を実行します。

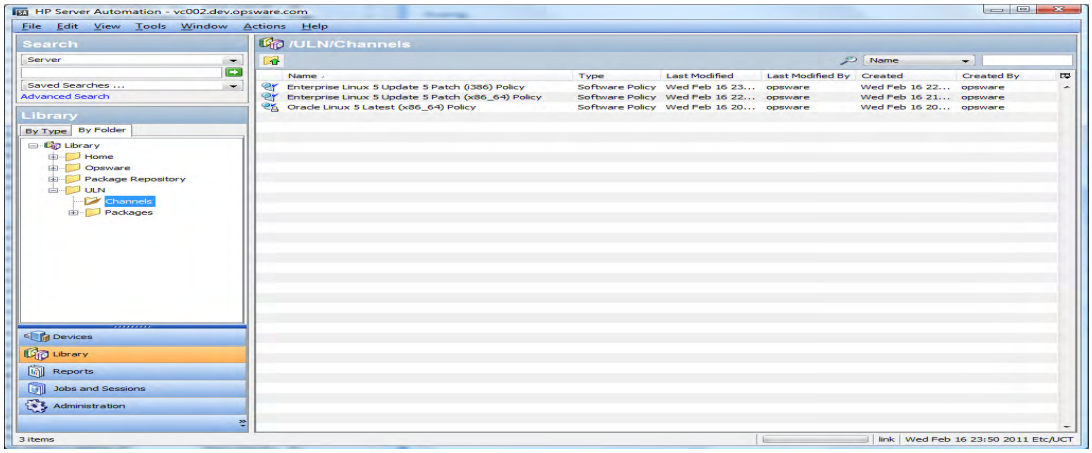
1 `/opt/opsware/patch_importer/bin/uln_import`を実行します。

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import
********** Importing Packages From ULN **********
Retrieving platform information from SA
Retrieving channel information from Oracle ULN
Processing package information
|

***** Import Phase *****

Importing 649 packages for channel Enterprise Linux 5 Update 5 Patch
(x86_64)
|============================================================| 100%
00:00:00
Elapsed Time: 912 seconds

Importing 530 packages for channel Enterprise Linux 5 Update 5 Patch (i386)
|============================================================| 100%
00:00:00
Elapsed Time: 978 seconds

ULN Import Completed

************************************************
```

2 インポートプロセスが完了したら、HPSA Javaクライアントにログオンして新規に作成されたポリシーを表示することができます。

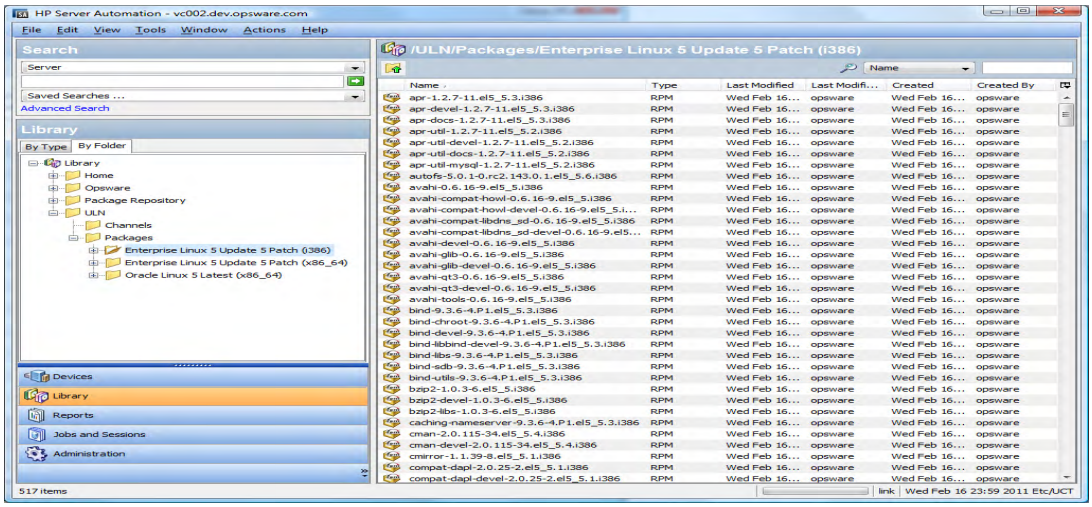
3 デフォルトで、ポリシーは/ULN/Channels/フォルダーに作成され、<Channel Name> Policyという名前が付きます(<Channel Name>はチャネルの名前)。例: /ULN/Channels/Enterprise Linux 5 Update 5 Patch (i386) Policy

注: 新規に作成されたポリシーを表示するには、/ULN/Channels/フォルダーに対する読み取り(またはそれ以上)のアクセス権が必要です。



4 デフォルトで、パッケージは/ULN/Packages/<Channel Name>/フォルダーにインポートされます(<Channel Name>はチャネルの名前)。例: /ULN/Packages/Enterprise Linux 5 Update 5 Patch (i386)/

注: 新規にインポートされたパッケージを表示するには、channelフォルダーに対する読み取り (またはそれ以上) のアクセス権が必要です。



5 新規に作成されたソフトウェアポリシーの確認が済んだら、OELサーバーの修復を開始できます。

修復タスクを実行するための適切なアクセス権が必要です。ソフトウェアの修復の詳細については、『SAユーザーガイド: ソフトウェア管理』を参照してください。

HPSA Patch Importer for Oracle Enterprise Linuxの使用

HPSA Patch Importer for Oracle Enterprise Linux はコマンドラインから実行できます。また、定期的にインポートを行うcronジョブの一部として実行することもできます。デフォルトで、このインポートツールは、サブスクライブされたチャネルのパッケージを ULN からインポートし、インポートしたチャネルごとに対応するソフトウェアポリシーを作成します。

一連のコマンドラインオプションを使用すると、インポートアクションを完全に制御することができます。たとえば、次の操作を行うことができます。

- 実行時に1つまたは複数のチャネルを選択的に有効化または無効化する
- 対応するソフトウェアポリシーを作成せずにパッケージをインポートするかどうかを指定する
- サポートされるプラットフォームに新しいチャネルを追加する
- サポートされるプラットフォームからチャネルを削除する
- サポートされるプラットフォームのサポート対象チャネルを表示する
- インポートのドライランを実行してアクションの実行結果を確認する

次の表は、uln_importのコマンドラインオプションについて説明したものです。

表31　　uln_importのコマンドラインオプション

オプション	説明
--version	このプログラムのバージョン番号を表示して終了します。
-h、--help	このヘルプメッセージを表示して終了します。
-E LABEL [LABEL...]、--enable=LABEL [LABEL...]	以前に無効化したチャンネルを有効化します。複数のラベルを指定できます。allを使用すると構成済みのすべてのチャネルが有効になります。 チャネルを無効化するには、構成ファイル/etc/opt/opsware/patch_importer/uln_import.conf の channel セクションで enabled=0を設定します。 このオプションは、実行時にチャネルを動的に有効化する場合に使用します。
-D LABEL [LABEL...]、--disable=LABEL [LABEL...]	以前に有効化したチャンネルを無効化します。複数のラベルを指定できます。allを使用すると構成済みのすべてのチャネルが無効になります。 all を使用するとすべてのチャネルが無効になります。この場合、チャネルは1つもインポートされません。これは、何も実行しないのと同じです。 このオプションはチャネルを恒久的に無効化するものではなく、このオプションを指定して実行した場合に限って、特定のチャネルを無効化するものです。
-m MODE、--mode=MODE	インポートモード: 'channel'、'erratum'、'errata'、'all' [デフォルト: all]
--source=SUPPORTED_SOURCES	ソース: 'uln'、'all'[デフォルト: all]
-c FILE、--conf=FILE	構成ファイル[デフォルト: none] このオプションは、代わりの構成ファイルを指定する場合に使用します。
--packages_only	ポリシーを作成せずに、パッケージのダウンロードのみを行います。
-n、--preview	実行される内容を表示します(ドライラン)。
-s、--silent	エラーのみを表示します。
-v、--verbose	デバッグモード。 デバッグメッセージはログファイルで参照できます。
--show_conf	構成設定を表示して終了します。
--show_labels	デフォルトRHNチャネルラベルを表示して終了します。
--hide_passwords	プレーンテキストのパスワードが表示されないように構成ファイルを編集して終了します。
--manual	マニュアルページを表示して終了します
--show_platform_labels	プラットフォームとサポートされるチャネルラベルを表示します。--platform_name オプションを使用すると、表示するプラットフォームをフィルター処理できます。

表31　uln_importのコマンドラインオプション（続き）

オプション	説明
--add_platform_label	特定のプラットフォームにチャネルラベルを追加します。追加するラベルと同時に、--platform_nameオプションを使用してプラットフォームを指定する必要があります。
--remove_platform_label	特定のプラットフォームからチャネルラベルを削除します。削除するラベルと同時に、--platform_nameオプションを使用してプラットフォームを指定する必要があります。
--platform_name=PLATFORM_NAME	プラットフォーム名を指定します。--show_platform_labelsオプションと組み合わせて使用する場合は、プラットフォーム名フィルターとして使用されます。--add_platform_labelオプションと組み合わせて使用する場合は、完全一致である必要があります。--remove_platform_labelオプションと組み合わせて使用する場合は、完全一致である必要があります。

実行時のチャネルの無効化

次の条件を満たす場合、デフォルトで、サブスクライブされたチャネルは有効になります。

1. チャネルがサポートされているHPSAエージェントプラットフォームのサポート対象チャネルである。
2. 構成ファイル/etc/opt/opsware/patch_importer/uln_import.confに [<Channel Label>] セクションが存在しない。
3. 構成ファイル/etc/opt/opsware/patch_importer/uln_import.confに [<Channel Label>] セクションが存在し、enabled=1が指定されている。

実行時に1つまたは複数のチャネルを無効にするには、-Dまたは-disableオプションを使用します。例:

```
/opt/opsware/patch_importer/bin/uln_import -D el5_u5_x86_64_patch
el5_u5_i386_patch
```

注: このオプションはチャネルを恒久的に無効化するものではありません。このオプションを指定して実行したときに、特定のチャネルを無効化するだけです。

実行時のチャネルの有効化

次の条件を満たす場合、デフォルトで、サブスクライブされたチャネルは無効になります。

構成ファイル /etc/opt/opsware/patch_importer/uln_import.conf に [<Channel Label>] セクションが存在し、enabled=0が指定されている。

実行時に1つまたは複数の無効化されたチャネルを有効にするには、-Eまたは-enableオプションを使用します。例:

```
/opt/opsware/patch_importer/bin/uln_import -E el5_u5_x86_64_patch
el5_u5_i386_patch
```

注: このオプションはチャネルを恒久的に有効化するものではありません。このオプションを指定して実行したときに、特定のチャネルを有効化するだけです。

制限事項:このオプションは、SAでサポートされるプラットフォームのチャネルを有効化する場合にのみ使用できます。このオプションを使用して、SAでサポートされないプラットフォームのチャネルを有効化することはできません。

対応するソフトウェアポリシーを作成せずにパッケージをインポートする

HPSAでは、次のいずれかの条件に当てはまる場合を除き、デフォルトで、チャネルに対応するソフトウェアポリシーが作成されます。

1. 構成ファイル/etc/opt/opsware/patch_importer/uln_import.confの [main] セクション内にpackages_only=1が存在する。
2. 構成ファイル/etc/opt/opsware/patch_importer/uln_import.confに [<Channel Label>] セクションが存在し、packages_only=1が指定されている。

ただし、実行時に-packages_onlyオプションを指定してデフォルトの動作をオーバーライドすることができます。例:

```
/opt/opsware/patch_importer/bin/uln_import -packages_only
```

他の実行時オプションと同様に、このオプションによって構成ファイルの内容が恒久的に変更されることはありません。

有効化されたチャネル情報の表示

有効化されたチャネルの情報を表示するには、-show_labelsオプションを指定します。例:

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import --show_labels
********** Supported Channels For ULN **********
Retrieving platform information from SA
Retrieving channel information from Oracle ULN
Processing package information

Supported Labels: ['el5_u5_x86_64_patch', 'el5_u5_i386_patch']

---------- Channels Details ----------

Channel Label       : el5_u5_x86_64_patch
Channel Name        : Enterprise Linux 5 Update 5 Patch (x86_64)
Channel Description : Updated packages published after release of
Enterprise Linux 5 Update 5 (x86_64)
Channel Version     : 20.110.111.133.047
Number of Packages  : 649

Channel Label       : el5_u5_i386_patch
Channel Name        : Enterprise Linux 5 Update 5 Patch (i386)
Channel Description : Updated packages published after release of
Enterprise Linux 5 Update 5 (i386)
Channel Version     : 20.110.111.125.211
Number of Packages  : 530

**********************************************
```

エージェントプラットフォームのサポート対象チャネルの表示

HPSAでサポートされているチャネルを、対応するプラットフォームとともに表示するには、-show_platform_labelsオプションを指定します。例:

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import
--show_platform_labels
Retrieving platform information from HPSA
|
---------- Channel Label ----------     ---------- Platform Name ----------
```

```
el5_exadata_i386_latest                Oracle Enterprise Linux 5
el5_exadata_x86_64_latest              Oracle Enterprise Linux 5 X86_64
el5_ga_i386_base                       Oracle Enterprise Linux 5
el5_ga_i386_patch                      Oracle Enterprise Linux 5
el5_ga_x86_64_base                     Oracle Enterprise Linux 5 X86_64
el5_ga_x86_64_patch                    Oracle Enterprise Linux 5 X86_64
el5_i386_addons                        Oracle Enterprise Linux 5
el5_i386_lsb4                          Oracle Enterprise Linux 5
el5_i386_ocfs2                         Oracle Enterprise Linux 5
el5_i386_oracle                        Oracle Enterprise Linux 5
el5_i386_oracle_addons                 Oracle Enterprise Linux 5
el5_rds_i386_latest                    Oracle Enterprise Linux 5
el5_rds_x86_64_latest                  Oracle Enterprise Linux 5 X86_64
el5_u1_i386_base                       Oracle Enterprise Linux 5
el5_u1_i386_patch                      Oracle Enterprise Linux 5
el5_u1_x86_64_base                     Oracle Enterprise Linux 5 X86_64
el5_u1_x86_64_patch                    Oracle Enterprise Linux 5 X86_64
el5_u2_i386_base                       Oracle Enterprise Linux 5
el5_u2_i386_patch                      Oracle Enterprise Linux 5
el5_u2_x86_64_base                     Oracle Enterprise Linux 5 X86_64
el5_u2_x86_64_patch                    Oracle Enterprise Linux 5 X86_64
el5_u3_i386_base                       Oracle Enterprise Linux 5
el5_u3_i386_patch                      Oracle Enterprise Linux 5
el5_u3_x86_64_base                     Oracle Enterprise Linux 5 X86_64
el5_u3_x86_64_patch                    Oracle Enterprise Linux 5 X86_64
el5_u4_i386_base                       Oracle Enterprise Linux 5
el5_u4_i386_patch                      Oracle Enterprise Linux 5
el5_u4_x86_64_base                     Oracle Enterprise Linux 5 X86_64
el5_u4_x86_64_patch                    Oracle Enterprise Linux 5 X86_64
el5_u5_i386_base                       Oracle Enterprise Linux 5
el5_u5_i386_patch                      Oracle Enterprise Linux 5
el5_u5_x86_64_base                     Oracle Enterprise Linux 5 X86_64
el5_u5_x86_64_patch                    Oracle Enterprise Linux 5 X86_64
el5_unsupported_i386_latest            Oracle Enterprise Linux 5
el5_unsupported_x86_64_latest          Oracle Enterprise Linux 5 X86_64
el5_x86_64_addons                      Oracle Enterprise Linux 5 X86_64
el5_x86_64_lsb4                        Oracle Enterprise Linux 5 X86_64
el5_x86_64_ocfs2                       Oracle Enterprise Linux 5 X86_64
el5_x86_64_oracle                      Oracle Enterprise Linux 5 X86_64
el5_x86_64_oracle_addons               Oracle Enterprise Linux 5 X86_64
ol5_i386_latest                        Oracle Enterprise Linux 5
ol5_u5_x86_64_patch                    Oracle Enterprise Linux 5 X86_64
ol5_u6_i386_base                       Oracle Enterprise Linux 5
ol5_u6_i386_patch                      Oracle Enterprise Linux 5
ol5_u6_x86_64_base                     Oracle Enterprise Linux 5 X86_64
ol5_u6_x86_64_patch                    Oracle Enterprise Linux 5 X86_64
ol5_x86_64_latest                      Oracle Enterprise Linux 5 X86_64
redhat-advanced-server-i386            Red Hat Enterprise Linux AS 2.1
redhat-ent-linux-i386-es-2.1           Red Hat Enterprise Linux ES 2.1
redhat-ent-linux-i386-ws-2.1           Red Hat Enterprise Linux WS 2.1
rhel-i386-as-3                         Red Hat Enterprise Linux AS 3
rhel-i386-as-4                         Red Hat Enterprise Linux AS 4
rhel-i386-client-5                     Red Hat Enterprise Linux Desktop 5
rhel-i386-es-3                         Red Hat Enterprise Linux ES 3
```

```
rhel-i386-es-4                          Red Hat Enterprise Linux ES 4
rhel-i386-server-5                      Red Hat Enterprise Linux Server 5
rhel-i386-ws-3                          Red Hat Enterprise Linux WS 3
rhel-i386-ws-4                          Red Hat Enterprise Linux WS 4
rhel-ia64-as-3                          Red Hat Enterprise Linux AS 3 IA64
rhel-ia64-as-4                          Red Hat Enterprise Linux AS 4 IA64
rhel-ia64-es-3                          Red Hat Enterprise Linux ES 3 IA64
rhel-ia64-es-4                          Red Hat Enterprise Linux ES 4 IA64
rhel-ia64-server-5                      Red Hat Enterprise Linux Server 5
IA64
rhel-ia64-ws-3                          Red Hat Enterprise Linux WS 3 IA64
rhel-ia64-ws-4                          Red Hat Enterprise Linux WS 4 IA64
rhel-x86_64-as-3                        Red Hat Enterprise Linux AS 3 X86_64
rhel-x86_64-as-4                        Red Hat Enterprise Linux AS 4 X86_64
rhel-x86_64-client-5                    Red Hat Enterprise Linux Desktop 5
X86_64
rhel-x86_64-es-3                        Red Hat Enterprise Linux ES 3 X86_64
rhel-x86_64-es-4                        Red Hat Enterprise Linux ES 4 X86_64
rhel-x86_64-server-5                    Red Hat Enterprise Linux Server 5
X86_64
rhel-x86_64-ws-3                        Red Hat Enterprise Linux WS 3 X86_64
rhel-x86_64-ws-4                        Red Hat Enterprise Linux WS 4 X86_64
```

また、-platform_nameオプションを使用して、プラットフォームをフィルター処理することもできます。これは大文字/小文字を区別した部分一致です。たとえば、プラットフォーム名に文字列Oracleを含むプラットフォームのみを表示する場合は、次のコマンドを実行します。

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import
--show_platform_labels --platform_name Oracle
Retrieving platform information from HPSA
|
---------- Channel Label ----------     ---------- Platform Name ----------
el5_exadata_i386_latest                 Oracle Enterprise Linux 5
el5_exadata_x86_64_latest               Oracle Enterprise Linux 5 X86_64
el5_ga_i386_base                        Oracle Enterprise Linux 5
el5_ga_i386_patch                       Oracle Enterprise Linux 5
el5_ga_x86_64_base                      Oracle Enterprise Linux 5 X86_64
el5_ga_x86_64_patch                     Oracle Enterprise Linux 5 X86_64
el5_i386_addons                         Oracle Enterprise Linux 5
el5_i386_lsb4                           Oracle Enterprise Linux 5
el5_i386_ocfs2                          Oracle Enterprise Linux 5
el5_i386_oracle                         Oracle Enterprise Linux 5
el5_i386_oracle_addons                  Oracle Enterprise Linux 5
el5_rds_i386_latest                     Oracle Enterprise Linux 5
el5_rds_x86_64_latest                   Oracle Enterprise Linux 5 X86_64
el5_u1_i386_base                        Oracle Enterprise Linux 5
el5_u1_i386_patch                       Oracle Enterprise Linux 5
el5_u1_x86_64_base                      Oracle Enterprise Linux 5 X86_64
el5_u1_x86_64_patch                     Oracle Enterprise Linux 5 X86_64
el5_u2_i386_base                        Oracle Enterprise Linux 5
el5_u2_i386_patch                       Oracle Enterprise Linux 5
el5_u2_x86_64_base                      Oracle Enterprise Linux 5 X86_64
el5_u2_x86_64_patch                     Oracle Enterprise Linux 5 X86_64
el5_u3_i386_base                        Oracle Enterprise Linux 5
el5_u3_i386_patch                       Oracle Enterprise Linux 5
el5_u3_x86_64_base                      Oracle Enterprise Linux 5 X86_64
el5_u3_x86_64_patch                     Oracle Enterprise Linux 5 X86_64
el5_u4_i386_base                        Oracle Enterprise Linux 5
el5_u4_i386_patch                       Oracle Enterprise Linux 5
```

```
el5_u4_x86_64_base                      Oracle Enterprise Linux 5 X86_64
el5_u4_x86_64_patch                     Oracle Enterprise Linux 5 X86_64
el5_u5_i386_base                        Oracle Enterprise Linux 5
el5_u5_i386_patch                       Oracle Enterprise Linux 5
el5_u5_x86_64_base                      Oracle Enterprise Linux 5 X86_64
el5_u5_x86_64_patch                     Oracle Enterprise Linux 5 X86_64
el5_unsupported_i386_latest             Oracle Enterprise Linux 5
el5_unsupported_x86_64_latest           Oracle Enterprise Linux 5 X86_64
el5_x86_64_addons                       Oracle Enterprise Linux 5 X86_64
el5_x86_64_lsb4                         Oracle Enterprise Linux 5 X86_64
el5_x86_64_ocfs2                        Oracle Enterprise Linux 5 X86_64
el5_x86_64_oracle                       Oracle Enterprise Linux 5 X86_64
el5_x86_64_oracle_addons                Oracle Enterprise Linux 5 X86_64
ol5_i386_latest                         Oracle Enterprise Linux 5
ol5_u5_x86_64_patch                     Oracle Enterprise Linux 5 X86_64
ol5_u6_i386_base                        Oracle Enterprise Linux 5
ol5_u6_i386_patch                       Oracle Enterprise Linux 5
ol5_u6_x86_64_base                      Oracle Enterprise Linux 5 X86_64
ol5_u6_x86_64_patch                     Oracle Enterprise Linux 5 X86_64
ol5_x86_64_latest                       Oracle Enterprise Linux 5 X86_64
```

チャネルラベルのプラットフォームへの追加

ベンダーによって特定のプラットフォームにチャネルラベルが追加される場合があります。HPSA で新しいチャネルをサポートするには、事前に新しいチャネルラベルを認識しておく必要があります。

HPSAのサポート対象リストに新しいラベルを追加するには、次のコマンドを実行します。

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import
--add_platform_label --platform_name "Oracle Enterprise Linux 5"
el5_new_label
Adding channel label el5_new_label for platform Oracle Enterprise Linux 5
Done
```

チャネルラベルのプラットフォームからの削除

チャネルが使用されなくなった場合には、HPSAのサポート対象リストからそのチャネルを削除することができます。

サポート対象リストから使用されなくなったチャネルを削除するには、次のコマンドを実行します。

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import
--remove_platform_label --platform_name "Oracle Enterprise Linux 5"
el5_new_label
Removing channel label el5_new_label for platform Oracle Enterprise Linux
5
Done
```

索引

U

W

あ

い

う

え

お

こ

さ

し

す

そ

て

と

は