CA SiteMinder®

アップグレード ガイド

r12.0 SP3

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA SiteMinder®
- CA SOA Security Manager
- CA Security Command Center
- eTrust® Audit iRecorder for SiteMinder

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

目次

第 1 章: アップグレードの計画

このセクションには、以下のトピックが含まれています。

SiteMinder のドキュメント

SiteMinder のドキュメントは、マニュアル選択メニューから参照可能です。SiteMinder マニュアル選択メニューを使用すると、以下のことを実行できます。

- 1 つのコンソールを使用して SiteMinder について公開されているすべてのドキュメントを表示する。
- アルファベット順の索引を使用して、すべてのドキュメントのトピックを検索する。
- すべてのドキュメントで 1 つ以上の単語を検索する。

SiteMinder 製品ドキュメントは引き続き別々にインストールされます。このガイドでは、他の SiteMinder ガイドを参照します。アップグレードを開始する前に、ドキュメントをインストールすることをお勧めします。

注: r6.0 SP6 および r12.0 SP2 のマニュアル選択メニューはテクニカル サポート サイトで提供されています。これらのバージョン用のインストール キットもありますが、ドキュメントのインストールは必須ではありません。マニュアル選択メニューはテクニカル サポート サイトから表示およびダウンロードできます。

Windows でのマニュアル選択メニューのインストール

テクニカル サポート サイトのインストール メディアを使用して、SiteMinder マニュアル選択メニューをインストールします。

注: r6.0 SP6 および r12.0 SP2 のマニュアル選択メニューはテクニカル サポート サイトで提供されています。これらのバージョン用のインストール キットもありますが、ドキュメントのインストールは必須ではありません。マニュアル選択メニューはテクニカル サポート サイトから表示およびダウンロードできます。

Windows にマニュアル選択メニューをインストールする方法

1. 実行中のすべてのアプリケーションを終了します。
2. インストール実行可能ファイルをダブルクリックします。

   インストール ウィザードが起動されます。
3. 必要な情報を入力し、インストール設定を確認します。
4. [インストール]をクリックします。

   インストーラによりインストールが開始されます。
5. [終了]をクリックします。

   マニュアル選択メニューがインストールされました。

詳細情報:

マニュアル選択メニューの使用 (P. 156)

UNIX でのマニュアル選択メニューのインストール

テクニカル サポート サイトのインストール メディアを使用して、SiteMinder マニュアル選択メニューをインストールします。

注: r6.0 SP6 および r12.0 SP2 のマニュアル選択メニューはテクニカル サポート サイトで提供されています。これらのバージョン用のインストール キットもありますが、ドキュメントのインストールは必須ではありません。マニュアル選択メニューはテクニカル サポート サイトから表示およびダウンロードできます。

ウィザードを使用してマニュアル選択メニューをインストールする方法

1. 実行中のすべてのアプリケーションを終了します。
2. シェルを開き、インストール実行可能ファイルに移動します。
3. 以下のコマンドを実行します。

   `./installation_media gui`

   installation_media

   SiteMinder マニュアル選択メニューのインストール実行可能ファイルの名前を指定します。

   インストーラが起動します。
4. 必要な情報を入力し、インストールの概要を確認します。
5. [インストール]をクリックします。

   インストーラによりインストールが開始されます。
6. [終了]をクリックします。

   マニュアル選択メニューがインストールされました。

UNIX コンソールを使用してマニュアル選択メニューをインストールする方法

1. 実行中のすべてのアプリケーションを終了します。
2. シェルを開き、インストール実行可能ファイルに移動します。
3. 以下のコマンドを実行します。

   `./installation_media -i console`

   installation_media

   SiteMinder マニュアル選択メニューのインストール実行可能ファイルの名前を指定します。

   インストーラが起動します。

4. 必要な情報を入力し、インストールの概要ダイアログを確認します。
5. Enter キーを押します。

   インストーラによりマニュアル選択メニューがインストールされます。

詳細情報:

マニュアル選択メニューの使用 (P. 156)

SiteMinder マニュアル選択メニューの使用

マニュアル選択メニューを使用する方法

1. *bookshelf_home*\CA\ca_documents に移動します。

   bookshelf home

   マニュアル選択メニューのインストール パスを指定します。

   注: このフォルダには、リリース ノート、ガイドの PDF バージョン、Javadoc (HTML) ファイル、および Perl POD ファイルの場所が記述された readme.txt があります。
2. ca-siteminder マニュアル選択メニュー フォルダを開きます。
3. CA-SiteMinder-*version*-BookShelf フォルダを開きます。

   バージョン

   最新の SiteMinder バージョンを指定します。
4. マニュアル選択メニューを開くには、以下のいずれかの方法を使用します。
   - マニュアル選択メニューがローカル システム上にあり、Internet Explorer を使用している場合
     - Bookshelf.hta をダブルクリックします。

       または
     - [スタート]-[プログラム]をクリックし、SiteMinder のマニュアルをクリックします。

- Mozilla Firefox を使用しており、Bookshelf.html をダブルクリックする場合
- マニュアル選択メニューがリモート システム上にある場合は、Bookshelf.html をダブルクリックします。

マニュアル選択メニューが開きます。

5. マニュアル選択メニューを Internet Explorer のお気に入りに追加するか、Mozilla Firefox のブックマークを作成してマニュアル選択メニューに戻ります。

このガイド内のコンポーネント バージョン

このガイドでは、SiteMinder 環境を r12.0 SP3 にアップグレードするためのパスについて詳述します。r12.0 SP3 へのアップグレードは、以下のバージョンからのアップグレードがサポートされています。

- r6.0 (ベース) 以上
- r12.0 (ベース) 以上

このガイド内のコンポーネント バージョンには、以下が含まれます。

- r12.x からの CA SiteMinder 管理 UI のアップグレード このガイドでは、以下のようになっています。
  - r12.x は r12.0 SP1 および r12.0 SP2 を指します。
- r6.x および r12.x からのポリシー サーバとポリシー ストアのアップグレード このガイドでは、以下のようになっています。
  - r6.x は、r6.0、r6.0 SP1、r6.0 SP2、r6.0 SP3、r6.0 SP4、r6.0 SP5、r6.0 SP6 を指します。
  - r12.x は r12.0、r12.0 SP1、r12.0 SP2 を指します。
- CA Business Intelligence Common Reporting コンポーネント (レポート サーバ) は、r12.x からアップグレードされます。このガイドでは、以下のようになっています。
  - r12.x は r12.0、r12.0 SP1、r12.0 SP2 を指します。

- r6.x および r12.x からの Web エージェントのアップグレード このガイドでは、以下のようになっています。
  - r6.x は、r6.0、r6.x QMR 1、r6.x QMR 2、r6.x QMR 3、r6.x QMR 4、r6.x QMR 5、6.x QMR 6 を指します。
  - r12.x は r12.0、r12.0 SP1、r12.0 SP2 を指します。

アップグレード パス

アップグレードは、既存の SiteMinder 環境への r12.0 SP3 コンポーネントの展開で構成されます。r12.0 SP3 へのアップグレードすは、以下の 2 つの方法で実行できます。

- 移行を完了する。
- 既存の環境と並行する r12.0 SP3 環境を設定する。どちらの環境でも、1 つ以上のキー ストアを使用してシングル サインオンが維持されます。

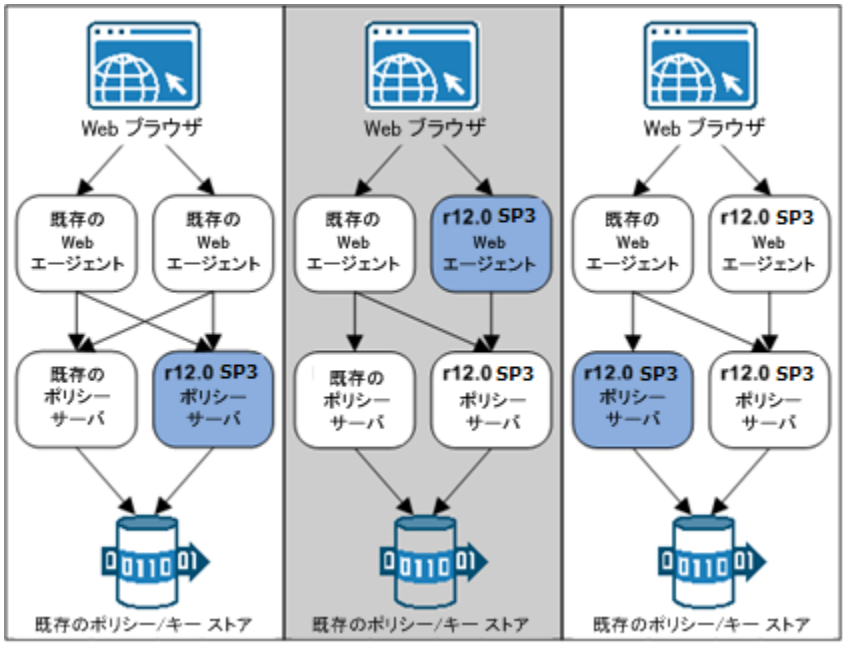
移行

移行は、環境が r12.0 SP3 で動作するまで個々の SiteMinder コンポーネントをアップグレードする処理です。個々のコンポーネントのアップグレードは、以下の作業中に行う 1 つ以上の手順で構成されます。

- コンポーネントをオフラインにします。
- コンポーネントをアップグレードします。
- コンポーネントをオンラインにします。

個々のコンポーネントを長期間にわたってアップグレードすることで、システム可用性を維持します。システム可用性を維持する鍵は、コンポーネントをアップグレードする順序です。移行中、アップグレードされた特定のコンポーネントは、以前のバージョンと通信し続けることができます。この種類の通信は、混在モード サポートと呼ばれます。

以下の図は、移行の概念を示しています。r6.x または r12.0 SP1 からの移行の詳細については、対応する章を参照してください。

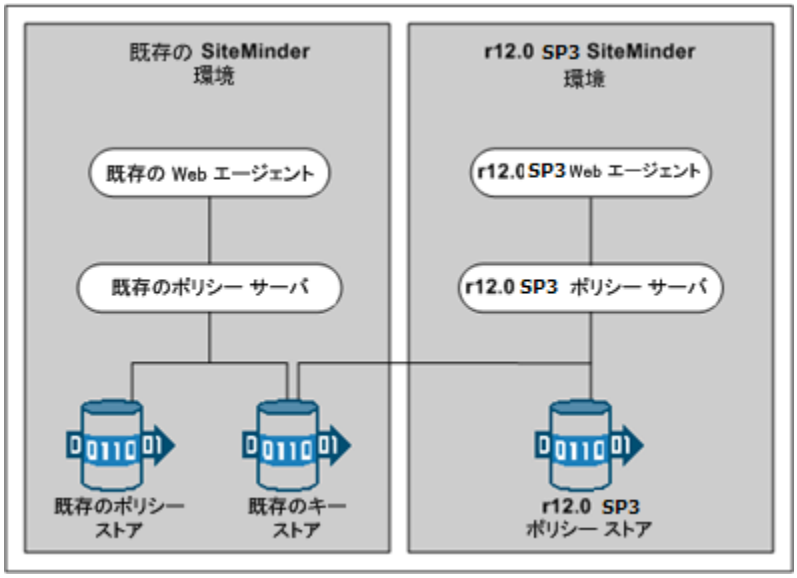


並行アップグレード

並行アップグレードは、既存の環境と同時に r12.0 SP3 環境を設定する処理です。並行アップグレードの設定は、以下の作業中に行う複数の手順で構成されます。

- 既存の環境は変更しないでください。
- r12.0 SP3 環境の設定
- 共通キー ストアまたは複数のキー ストアを使用して、両方の環境間でシングル サインオンを有効にします。

以下の図は、並行アップグレードの概念を示しています。r6.x または r12.x から並列アップグレードを完了する方法の詳細については、対応する章を参照してください。



移行を計画する方法

複雑な SiteMinder 環境を移行するには、環境のアップグレード前に多くのコンポーネントをアップグレードする必要があります。移行を効率よく完了して、機密リソースをセキュリティリスクにさらしたり、ダウンタイムが発生しないようにするため、移計画が不可欠です。

移行計画は、以下の内容で構成できます。

- テスト環境

  処理に精通するためにテスト移行を実行します。テスト移行は、実稼働環境を移行するときに、ミッション クリティカルなリソースをダウンさせる可能性のある問題を識別、トラブルシューティング、および回避するのに役立ちます。

- 現在のサードパーティ製品およびハードウェア

  r12.0 SP3 が現在のサードパーティ製品およびハードウェアをサポートするかどうかを判断します。

  注: サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカル サポート サイトの SiteMinder r12.0 SP3 プラットフォームのサポート マトリックスを参照してください。

- サイト分析

  SiteMinder 環境の現在の状態と、各コンポーネントを更新する最適な時間を判断します。

- SiteMinder コンポーネント

  アップグレードを計画する個々の SiteMinder コンポーネントを一覧表示し、各コンポーネントがホストされている場所を識別します。

- 回復計画

  移行中に問題が発生した場合に備えて、既存のコンポーネントをバックアップします。

- アップグレード パス

  移行によりサポートされる個々のコンポーネントのアップグレード パスを調べます。

- 混在モード サポート

  混在モード サポートについての理解を深めます。

- パフォーマンス テスト

  移行の完了時に環境のパフォーマンス テストを実行する計画を立てます。

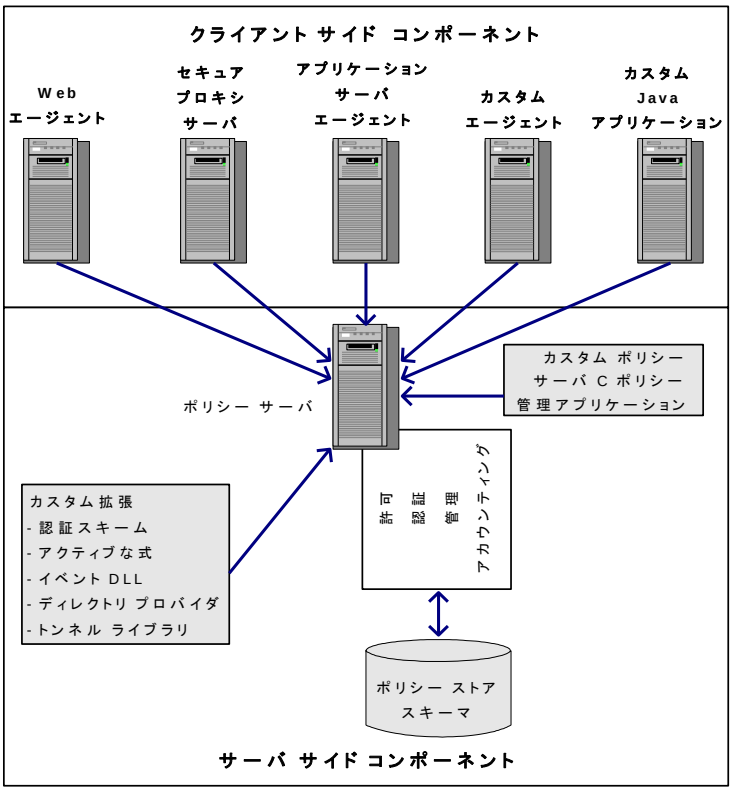
SiteMinder 環境の分析

SiteMinder 環境を分析して、移行の複雑さを調べます。以下の質問について考慮します。

質問	推奨される手順
環境で実行されているポリシー サーバおよびエージェントはいくつあるか。	ポリシー サーバ監査ログを使用して数を調べます。
ポリシー サーバおよびエージェントのバージョンは何か。	ポリシー サーバ監査ログを使用してバージョンを調べます。
どのポリシー サーバがどの Web エージェントと通信しているか。	ポリシー サーバ監査ログを使用してこの情報を調べます。
各サイトの最もトラフィックが少ない時間帯はいつか。	Web サーバ ログとポリシー サーバ監査ログを調べます。

質問	推奨される手順
Web エージェントがフェールオーバまたはラウンドロビン モードで動作しているか。	フェールオーバとラウンドロビンを維持するには、「混在 SiteMinder 環境」を参照してください。
SiteMinder 環境全体でシングル サインオンを使用しているか。	シングル サインオンの維持の詳細については、このガイドを参照してください。
認証方式に認証情報コレクタを使用しているか。	混在環境で認証情報コレクタを使用する方法の詳細については、「Web エージェント設定ガイド」を参照してください。
r12.0 SP3 は使用中のサードパーティ ハードウェアおよびソフトウェアをサポートするか。	テクニカル サポート サイトで SiteMinder r12.0 SP3 プラットフォーム サポート マトリックスを参照します。
プロフェッショナル サービスがカスタマイズした SiteMinder ソフトウェアがあるか。	カスタマ サポートに問い合わせます。
以前のバージョンの SiteMinder マニュアルにアクセスできるか。このガイドは、以前の SiteMinder マニュアルを参照しています。	テクニカル サポート サイトで、SiteMinder マニュアルを探します。
アップグレードにより上書きされる可能性がある、カスタマイズされたファイルがあるか。	移行を開始する前に、カスタマイズされたファイルをバックアップします。

以下の図は、アップグレード前に考慮する必要がある SiteMinder コンポーネントを示しています。



復旧計画

元の設定に戻ることができる回復計画を実行します。コンポーネント アップグレードまたは移行から戻ることはできません。

重要 各ポリシー サーバおよび Web エージェント ホストのイメージ全体をバックアップすると、最も徹底的な回復計画になります。この方法をお勧めします。

各システムのイメージ全体をバックアップしない場合は、以下の手順を実行します。

- すべての Web エージェントおよびポリシー サーバ バイナリをバックアップします。これらのファイルの大部分は、ポリシー サーバおよび Web エージェントをインストールした bin サブディレクトリにあります。
- Web エージェント設定ファイル（WebAgent.conf）をバックアップします。

  r12.0 SP3 ポリシー サーバからエージェントを集中管理する予定の場合、ポリシー サーバ管理者にエージェント設定ファイルを渡します。管理者は、エージェント設定オブジェクトを作成するためにこのファイルが必要です。

  注: Web エージェントの集中管理の詳細については、「ポリシー サーバ設定ガイド」を参照してください。
- r6.x から移行する場合は、smobjexport ユーティリティを使用してポリシー ストアをクリア テキストでファイルにエクスポートします。

  ポリシー ストアをクリア テキストでエクスポートすると、共有秘密キーなどの暗号化された情報を記録できます。この情報は、問題をトラブルシュートするために使用できます。キー ストアがポリシー ストアに存在する場合は、smobjexport ユーティリティで -k オプションを使用します。このオプションには、エクスポートされる情報と共にキーが含まれます。
- r12.0 SP1 から移行する場合は、XPSExport ユーティリティを使用してポリシー ストアをファイルにエクスポートします。
- r6.x または r12.x のインストール スクリプト、ホット フィックス、およびサービス パックをコピーして、必要な場合に再インストールできるようにします。テクニカル サポート サイトからコピーをダウンロードできます。

アップグレード パスの決定

以下のコンポーネントの組み合わせがサイトに存在している場合は、移行可能です。

- r6.x および r12.0 SP3 コンポーネント
- r12.0 SP1 および r12.0 SP3 コンポーネント

以下の表は、r12.0 SP3 への移行でサポートされるポリシー サーバのアップグレード パスを示しています。

ポリシー サーバのバージョン	アップグレード先
r6.0	r12.0 SP3
r6.0 SP1	r12.0 SP3
r6.0 SP2	r12.0 SP3
r6.0 SP3	r12.0 SP3
r6.0 SP4	r12.0 SP3
r6.0 SP5	r12.0 SP3
r6.0 SP6	r12.0 SP3
r12.0 SP1	r12.0 SP3
r12.0 SP2	r12.0 SP3

以下の表は、r12.0 SP3 への移行でサポートされる Web エージェントのアップグレード パスを示しています。

Web エージェントのバージョン	アップグレード先
r6.0	r12.0 SP3
r6.x QMR 1	r12.0 SP3
r6.x QMR 2	r12.0 SP3
r6.x QMR 3	r12.0 SP3
r6.x QMR 4	r12.0 SP3
r6.x QMR 5	r12.0 SP3
r6.x QMR 6	r12.0 SP3
r12.0 SP1	r12.0 SP3
r12.0 SP2	r12.0 SP3

注: フォームまたは SSL 認証情報コレクタとして機能している Web エージェントは、最後にアップグレードしてください。

以下の表は、r12.0 SP3 への移行でサポートされる 管理 UI のアップグレード パスを示しています。

管理 UI のバージョン	アップグレード先
r12.0 SP1	r12.0 SP3
r12.0 SP2	r12.0 SP3

以下の表は、r12.0 SP3 への移行でサポートされるレポート サーバのアップグレード パスを示しています。

レポート サーバのバージョン	アップグレード先
r12.0	r12.0 SP3
r12.0 SP1	r12.0 SP3
r12.0 SP2	r12.0 SP3

SiteMinder 混在環境

r12.0 SP3 に移行するとき、複数バージョンの SiteMinder コンポーネントの組み合わせを環境に含めることができます。さらに、すべてのコンポーネントを r12.0 SP3 にアップグレードする必要はありません。一部のコンポーネントを現在のバージョンとして残すことができます。以下の点について考慮してください。

- r6.x コンポーネントの組み合わせが環境に含まれる場合、r12.0 SP3 ポリシー サーバは r6.x ポリシー ストアとの通信を続行できます。
- お使いの環境に r12.0 SP1 または r12.0 SP2 コンポーネントの組み合わせが存在する場合、r12.0 SP3 ポリシー サーバは r12.0 SP1 または r12.0 SP2 ポリシー ストアとの通信を続行できます。
- ポリシー サーバのバージョンが混在している場合、ユーザはリソースに引き続きアクセスでき、r6.x QMR x、r12.0 SP1 または r12.0 SP2 エージェントを使用して同じ操作を行うことができます。
- 混在環境ではシングル サインオンをサポートできます。

混在モードのサポート

混在モード サポートでは、移行中に r12.0 SP3 ポリシー サーバが r6.x、r12.0 SP1 または r12.0 SP2 ポリシー ストアと通信できます。ポリシー サーバをアップグレードすると、ポリシー サーバ インストーラによりそのポリシー ストア バージョンが検出されます。ポリシー ストアが以前のバージョンで動作している場合、インストーラによりポリシー サーバがアップグレードされ、混在(互換性)モードが有効になります。

注: 混在モードをオフにすることはできません。

ポリシー サーバ管理コンソールでは、r12.0 SP3 ポリシー サーバが使用しているポリシー ストアのバージョンを参照できます。

ポリシー ストアのバージョンを識別する方法

1. ポリシーサーバー管理コンソールを起動します。
2. [データ]タブをクリックします。
3. [ヘルプ]-[バージョン情報]を選択します。

   ポリシー サーバ管理コンソールのバージョン情報の画面が表示されます。ポリシー サーバのバージョンが一覧表示されます。

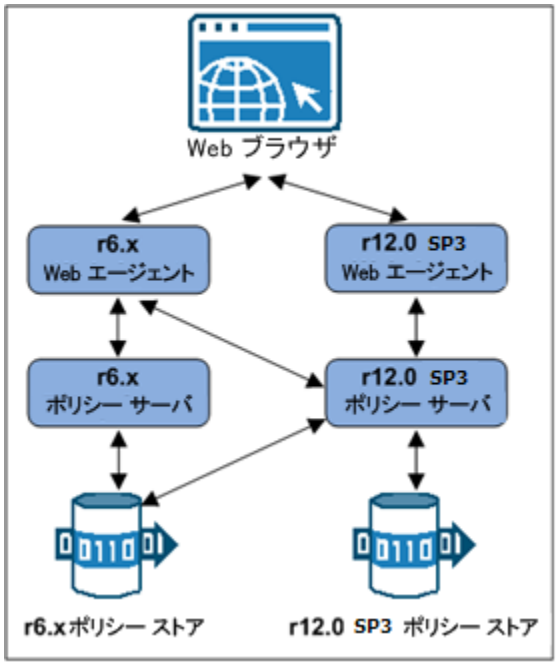
注: ポリシー ストアのバージョンも一覧表示されます。ポリシー ストアのバージョンは、ポリシー サーバのバージョンと一致しません。

6.x 混在モード サポート

r6.x から r12.0 SP3 に移行するときは、以下の点を考慮します。

- r6.x ポリシー サーバは、r12.0 SP3 ポリシー ストアと通信できません。
- r12.0 SP3 ポリシー サーバは、r6.x ポリシー ストアと通信できます。
- r6.x および r12.0 SP3 ポリシー サーバは、同じキー ストアを共有できます。
- r6.x および r12.0 SP3 ポリシー サーバは、同じセッション ストアを共有できます。
- r6.x Web エージェントは、r12.0 SP3 ポリシー サーバと通信できます。

以下の図は、r6.x 混在モード サポートを詳細に示しています。



6.x 混在環境の制限

r12.0 SP3 ポリシー サーバは、r6.x ポリシー ストアと通信できますが、r6.x ポリシー サーバは r12.0 SP3 ポリシー ストアに接続できません。このため、既存の r6.x 機能はすべて混在環境で使用できますが、r12.0 SP3 固有の機能は使用できません。

以下の表は、これらの機能の一覧です。

機能	説明	混在モードで使用可能
FIPS（Federal Information Processing Standard）140-2 のサポート **注**: FIPS は、AES（Advanced Encryption Standard: 高度暗号化標準）に適合する暗号モジュールを信用するために使用される米国政府のコンピュータ セキュリティ標準です。	FIPS 140-2 準拠のアルゴリズムの使用	いいえ

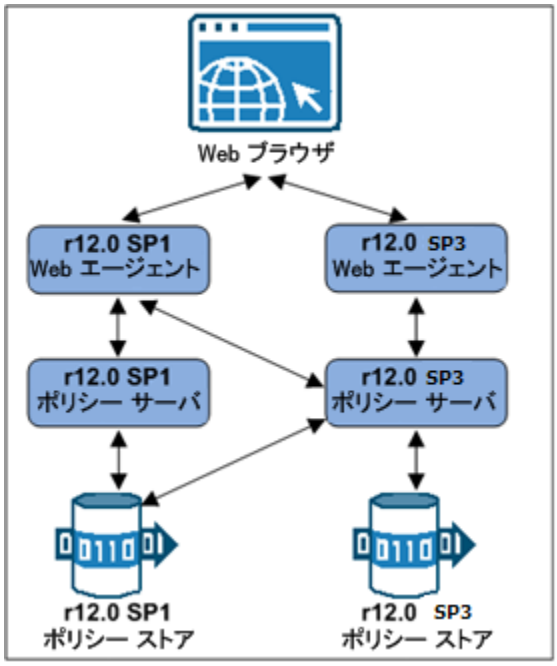
機能	説明	混在モードで使用可能
エンタープライズ ポリシー管理（EPM）	EPM は、アプリケーション中心でポリシーを作成する方法です。r12.0 SP3 管理 UI が必要です。	いいえ
IPv6 のサポート	IPv6 TCP/IP プロトコルの使用	いいえ

r12.0 SP1 および SP2 混在モードのサポート

r12.0 SP1 または r12.0 SP2 から r12.0 SP3 に移行するときは、以下の点を考慮します。

- r12.0 SP1/r12.0 SP2 ポリシー サーバは、r12.0 SP3 ポリシー ストアと通信できません。
- r12.0 SP3 ポリシー サーバは、r12.0 SP1/r12.0 SP2 ポリシー ストアと通信できます。
- r12.0 SP1/r12.0 SP2 ポリシー サーバは、r12.0 SP3 ポリシー サーバと同じキー ストアを共有できます。
- r12.0 SP1/r12.0 SP2 ポリシー サーバは、r12.0 SP3 ポリシー サーバと同じセッション ストアを共有できます。
- r12.0 SP1/r12.0 SP2 Web エージェントは、r12.0 SP3 ポリシー サーバと通信できます。

以下の図は、混在モード サポートを詳細に示しています。



r12.0 SP1/r12.0 SP2 混在環境の制限

r12.0 SP3 ポリシー サーバは、r12.0 SP1/r12.0 SP2 ポリシー ストアと通信できます。このため、既存の r12.0 SP1/r12.0 SP2 機能はすべて混在環境で使用できます。

注: 混在環境は r12.0 SP3 機能に影響を与えません。

並行アップグレードを計画する方法

既存の環境の並行 SiteMinder 環境を設定するには、以下のものをインストールする必要があります。

- 1 つ以上のポリシー サーバ
- ポリシー ストア
- 管理 UI

- 1 つ以上の Web エージェント
- CA Business Intelligence（レポート サーバ）

注: このガイドでは、両方の環境間でシングル サインオンを確立するための要件を一覧に示します。ポリシー サーバ、ポリシー ストア、管理 UI、およびレポート サーバのインストールの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。Web エージェントのインストールの詳細については、「*Web エージェント インストール ガイド*」を参照してください。

単純なテスト環境をアップグレードする方法

シングル サインオンまたはフェイルオーバーを維持する必要がある場合のみ、このガイドで説明するアップグレード パスに従います。

テスト環境でフェイルオーバーが必要でない場合は、以下の方法で最も効率的にアップグレードできます。

1. r12.0 SP3 ポリシー サーバをインストールします。

   注: 必ず、新しいポリシー サーバをインストールしてください。既存のポリシー サーバはアップグレードしないでください。ポリシー サーバのインストールの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

2. 以下のいずれかの操作を行います。

   - r6.x からアップグレードする場合は、smobjexport を使用して、r6.x ポリシー ストアからデータをエクスポートします。
   - r12.x からアップグレードする場合は、XPSExport を使用して、r12.x ポリシー ストアからデータをエクスポートします。

   注: これらのユーティリティの使用の詳細については、「*ポリシー サーバ管理ガイド*」を参照してください。

3. 以下のいずれかの操作を行います。
   - r6.x からアップグレードする場合は、smobjimport を使用して、r6.x ポリシー ストア データを r12.0 SP3 ポリシー ストアにインポートします。
   - r12.x からアップグレードする場合は、XPSImport を使用して、r12.x ポリシー ストア データを r12.0 SP3 ポリシー ストアにインポートします。

   注: これらのユーティリティの使用の詳細については、「*ポリシー サーバ管理ガイド*」を参照してください。
4. SiteMinder r6.x または r12.x のアンインストール

アップグレードまたはポリシー移行の一環として SiteMinder ポリシーをある環境から別の環境に移動させる場合、環境に固有の一部のオブジェクトがエクスポート ファイルに含まれます。これらのオブジェクトにはたとえば以下のものがあります。

- トラステッド ホスト
- HCO ポリシー サーバ設定
- 認証方式 URL
- パスワード サービス リダイレクト
- リダイレクト レスポンス

XPSExport を使用するときに選択したモードによって、これらのオブジェクトは新しい環境に追加されるか、または既存の設定を上書きします。オブジェクトをインポートする際は、環境設定を誤って変更することがないよう注意が必要です。

共通の SiteMinder 環境

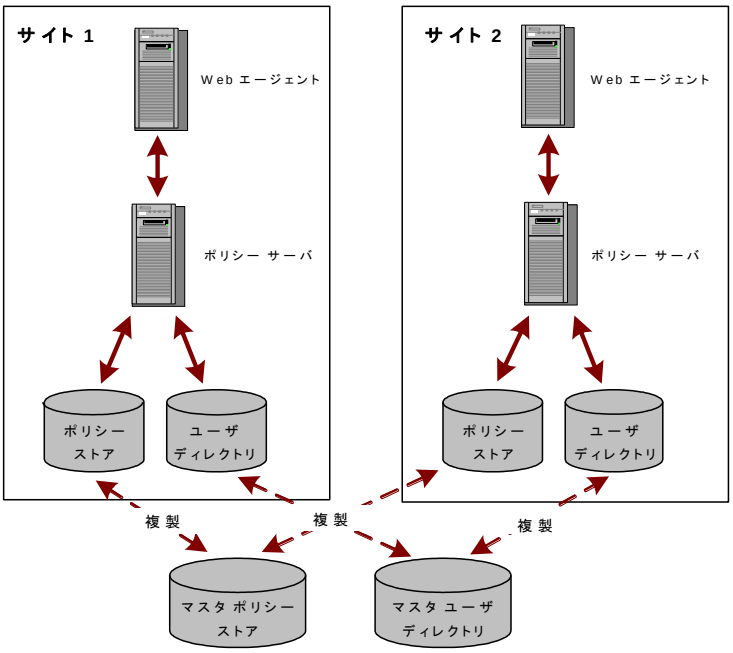
r12.0 SP3 にアップグレードする前に、いくつかの共通 SiteMinder 環境について考慮します。サイトが以下のいずれかと一致するかどうかを確かめます。

- 単一ポリシー ストア、複数ポリシー サーバ、および Web エージェント (P. 29)
- クラスタ環境 (P. 29)
- 共有ユーザ ディレクトリ環境 (P. 30)

単一ポリシー ストア、複数ポリシー サーバ、および Web エージェント

この SiteMinder 環境には、世界中に配置された 20 ～ 100 台のポリシー サーバによって使用される 1 つのポリシー ストアが存在します。パフォーマンス上の理由から、各ポリシー サーバが最も近いレプリケーション バージョンと通信するように、ポリシー ストアおよびユーザ ディレクトリは自動的にレプリケートされます。各ポリシー サーバ、50 ～ 300 の Web エージェントと通信します。

以下の図は、この環境を縮小して示しています。



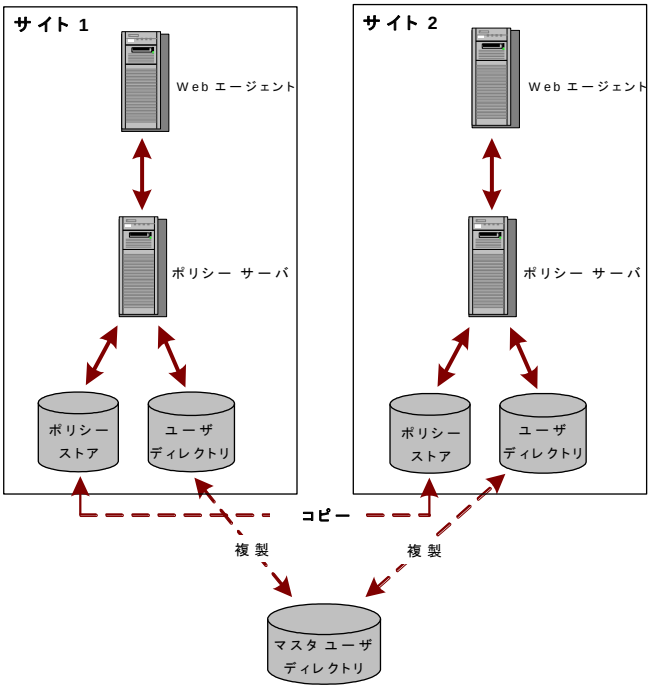
この環境をアップグレードするには、このガイドで概説する手順を使用します。

クラスタ環境

クラスタ環境は、1 つのポリシー ストアと複数の Web エージェントおよびポリシー サーバを備えた SiteMinder 環境に似ています。ただし、クラスタでは、ポリシー ストアはレプリケートされるのではなくコピーされます。コピーされたストアは、特定の時点でのポリシー ストアのスナップショットであり、動的に更新されない点が異なります。レプリケートされたストアは自動的に更新されます。通常、変更はプライマリ データベースに加えられてから、セカンダリ データベースに伝達されます。

さらに、1 つのクラスタ サイトを他のクラスタ サイトとは別個にアップグレードして、それらの間で 1 つのサインオンを維持することもできます。

以下の図に、クラスタ環境を小さい縮尺で示します。

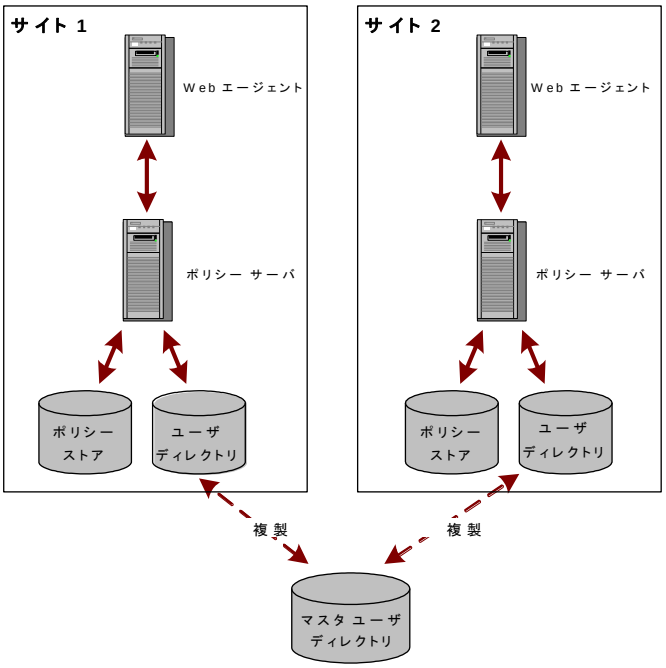


この環境をアップグレードするには、このガイドで概説する手順を使用します。

共有ユーザ ディレクトリ環境

この環境では、2 つのサイトに複数の Web エージェントと複数のポリシー サーバが存在しますが、2 つの別個のポリシー ストア内に格納されたポリシー セットがそれぞれ維持されています。これらのサイトでは、同じマスタ ユーザ ディレクトリをレプリケートすることで、1 つのサインオンが維持されます。

以下の図に、共有ユーザ ディレクトリ環境を小さい縮尺で示します。



この環境をアップグレードするには、このガイドで概説する手順を使用します。

第 2 章: r6.x からのアップグレード

このセクションには、以下のトピックが含まれています。

サポートされているアップグレード パス

アップグレードは、既存の SiteMinder 環境への r12.0 SP3 コンポーネントの展開で構成されます。r12.0 SP3 へのアップグレードすは、以下の 2 つの方法で実行できます。

- 移行を完了する。
- 既存の環境と並行する r12.0 SP3 環境を設定する。どちらの環境でも、1 つ以上のキー ストアを使用してシングル サインオンが維持されます。

r6.x からアップグレードする場合、どちらのアップグレード パスもサポートされます。

移行に関する考慮事項

r6.x から移行する場合は、移行の開始前に以下の点を考慮します。

ポリシー サーバ オプション パック サポート

PSOP（Policy Server Option Pack、ポリシー サーバ オプション パック）機能は、核となるポリシー サーバ機能の一部です。PSOP 機能を使用する r6.x 環境を移行する場合は、以下の点を考慮します。

- PSOP には、個別のアップグレードは必要なくなりました。
- ポリシー サーバ インストーラにより PSOP 設定ファイルがバックアップされ、ポリシー サーバのアップグレード時に PSOP がアンインストールされます。
- ポリシー サーバ インストーラにより、ポリシー サーバのアップグレード時に最新のバージョンの PSOP がインストールされます。

注: PSOP 機能を使用する r6.x 環境の移行の詳細については、「r6.x から移行する方法」を参照してください。

ポリシー サーバ オプション パック機能の管理

2 つのグラフィカル ユーザ インターフェース（GUI）を使用して、特定の SiteMinder ポリシー オブジェクトを管理できます。以下の点について考慮してください。

- **SiteMinder 管理 UI**（管理 UI）- 管理 UI は、ポリシー サーバから独立してインストールされる Web ベースの管理コンソールです。管理 UI は、認証および許可ポリシー、EPM（Enterprise Policy Management ）、レポートおよびポリシー分析のようなアクセス制御に関連するほとんどのタスクを設定するためのツールです。

  Federation セキュリティ サービス に関連するオブジェクトを除くすべてのポリシー サーバ オブジェクトを表示、変更、および削除するには、管理 UI を使用します。フェデレーション関連の設定タスクはすべて FSS 管理 UI を使用して管理できます。

- **SiteMinder Federation セキュリティ サービスの管理 UI**（FSS 管理 UI）- FSS 管理 UI は、ポリシー サーバと同時にインストールされるアプレットベースのアプリケーションです。Federation セキュリティ サービス コンポーネントは、アフィリエイト（コンシューマ、サービス プロバイダ、リソース パートナー）と、2 つのパートナー間のフェデレーション通信をサポートするために設定する SAML 認証方式で構成されます。

FSS 管理 UI は、SiteMinder Federation セキュリティ サービスを管理するために用意されています。以前のバージョンの SiteMinder ポリシー サーバのユーザ インターフェースと異なり、すべての SiteMinder オブジェクトが FSS 管理 UI に表示されることがわかります。表示されないオブジェクトは、EPM（Enterprise Policy Management）およびレポートに関連するオブジェクトだけです。FSS 管理 UI を使用すると、SiteMinder オブジェクトを管理できます。FSS 管理 UI を使用しているときに情報が必要となった場合は、FSS 管理 UI オンライン ヘルプ システムを調べます。

組織とパートナーとの間でフェデレーションが実現していない場合、FSS 管理 UI の使用は必須ではありません。コアのポリシー サーバ アップグレードの一部に含まれていますが、FSS 管理 UI を使用するにはポリシー サーバに登録する必要があります。FSS 管理 UI の登録は、管理 UI を通して行います。そのため、FSS 管理 UI を登録する前に 管理 UI をインストールして設定する必要があります。

注: 移行時にこれらの各ユーザ インターフェースをインストールおよび設定する方法の詳細については、「r6.x から移行する方法」を参照してください。

r12.0 SP3 内の SiteMinder キー データベース パスワード

データベースに格納されたキーおよび証明書データの暗号化に使用される SiteMinder キー データベース（smkeydatabase）パスワードは、FIPS 準拠のアルゴリズムを使用して暗号化されます。FIPS は、AES（Advanced Encryption Standard: 高度暗号化標準）に適合する暗号モジュールを信用するために使用される米国政府のコンピュータ セキュリティ標準です。移行を計画するときは、以下の点を考慮します。

- r12.0 SP3 ポリシー サーバは、r12.0 SP3 キー データベースとのみ通信できます。キー データベースは、互換モードでは動作しません。
- ポリシー サーバのアップグレード時にパスワードを変更することで、キー データベースをアップグレードできます。パスワードを変更すると、FIPS 準拠のアルゴリズムを使用して、データベース パスワードおよび既存の暗号化データが再暗号化されます。
- ポリシー サーバのアップグレード時に r12.0 SP3 キー データベースを作成し、既存のキーおよび証明書データを新しいインスタンスに移行できます。

このガイドでは、キー データベースをアップグレードする手順について詳述します。r12.0 SP3 キー データベースを作成して、既存のキーおよび証明書データを新しいインスタンスに移行する場合は、以下の手順を実行します。

1. smkeytool ユーティリティを使用して、キーおよび証明書データをエクスポートします。

   注: smkeytool の使用の詳細については、「*Federation Security Services Guide*」を参照してください。

2. ポリシー サーバのアップグレード時に、r12.0 SP3 キー データベースを作成します。

   注: ポリシー サーバ設定ウィザードを使用して、キー データベースを作成できます。ポリシー サーバ設定ウィザードの使用の詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

3. smkeytool ユーティリティを使用して、キーおよび証明書データをインポートします。

r12.0 SP3 内の AM キー ストア データ

r6.0、r6.0 SP1、r6.0 SP2、r6.0 SP3、または r6.0 SP4 から Federation セキュリティ サービス 環境を移行する場合、AM キー ストア（AM.keystore）データを移行するには PKI インフラストラクチャの変更が必要です。

移行では、コンシューマ権限の Web エージェントにある AM.keystore 内のデータを、コンシューマ権限の r12.0 SP3 SiteMinder キー データベース（smkeydatabase）に移行する必要があります。

注: PKI インフラストラクチャの変更の詳細については、「*Federation Security Services Guide*」を参照してください。AM.keystore データを r12.0 SP3 SiteMinder キー データベースにいつ移行するかの詳細については、「r6.x から移行する方法」を参照してください。

12.x の Crystal Reports

r12.0 SP3 ポリシー サーバ インストーラには、Crystal Reports 9.0 と互換性があるレポート ファイル（.rpt）は含まれなくなりました。SiteMinder レポートは、r12.0 SP3 管理 UI に統合されました。レポート サーバのインストールには、別個のインストーラを使用できます。レポート サーバは、r6.x で使用可能なレポートを含む、レポートのスケジュールおよび表示に必要です。

以下の点について考慮してください。

- 引き続き、Crystal Reports サーバでレポート ファイルを使用して、移行時にレポートをスケジュールおよび表示できます。 r12.0 SP3 ポリシー サーバは、r6.x 監査ログ データベースと通信できます。
- ポリシー サーバのアップグレードにより、r6.x レポート データ ソースが削除されます。r6.x レポート データ ソースのバックアップを作成します。
- 移行の最後の手順として、管理 UI をインストールし、r6.x ポリシー サーバ ユーザ インターフェースの使用を中断します。移行を完了すると、レポート ファイルにアクセスすることができません。さらに、r6.x ポリシー サーバ ユーザ インターフェースからレポート ファイルを使用して作成されたレポートにアクセスすることができません。これらのレポートにアクセスする必要がある場合、r6.x ポリシー サーバ ユーザ インターフェースの使用を中断する前にそれらをバックアップすることをお勧めします。
- r6.x で使用できたレポートは、r12.0 SP3 管理 UI を使用してスケジュールおよび表示できます。

注: レポート サーバのインストールの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。レポートのスケジュールおよび表示の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

管理者認証

SiteMinder を使用して外部管理者ユーザ ストアを保護している場合は、以下の点を考慮します。

- ポリシー サーバのアップグレード時、ポリシー サーバ ユーザ インターフェースが FSS 管理 UI にアップグレードされます。引き続き、SiteMinder を使用して FSS 管理 UI を保護できます。既存の外部接続は、FSS 管理 UI でも有効です。
- デフォルトでは、管理 UI はポリシー ストアを管理者アイデンティティのソースとして使用します。このデフォルト設定では、管理 UI のインストール直後から環境を管理することができます。ただし、外部ユーザに格納された既存の r6.x 管理者は、管理 UI では使用できません。管理 UI から外部管理者ストア接続を設定して、r6.x 管理者を使用できるようにします。

  注: SiteMinder を使用して 管理 UI を保護することはできません。管理 UI ログイン画面では、ユーザ名とパスワードのみ求められます。外部管理者ストア接続の設定の詳細については、「ポリシー サーバ設定ガイド」を参照してください。

シングル サインオン

r12.0 SP3 への移行時に、シングル サインオンを維持できます。以下の点について考慮してください。

- r12.0 SP3 ポリシー サーバは、r6.x ポリシー ストアおよび r6.x キー ストアと通信できます。
- r12.0 SP3 ポリシー サーバは、r6.x セッション ストアと通信できます。

ポリシー ストア破損の回避

ポリシー ストア破損を回避するためポリシー ストアをホストしているサーバが、UTF-8 形式でオブジェクトを格納するように設定してください。

注: UTF-8 形式でオブジェクトを格納するサーバ設定の詳細については、使用しているベンダーから発行されたマニュアルを参照してください。

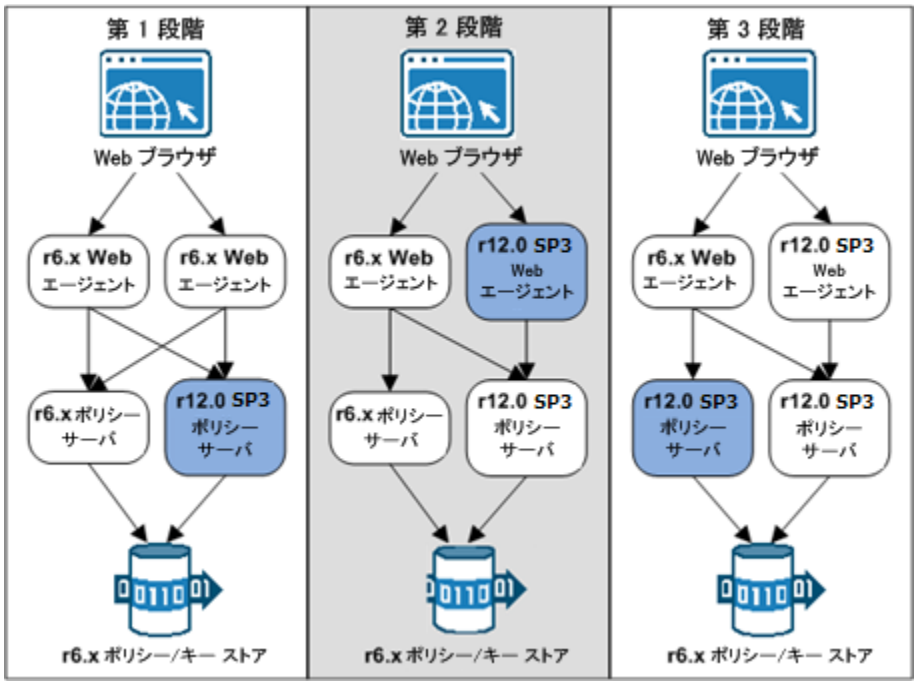
r6.x の移行の仕組み

複数のポリシー サーバおよび Web エージェントが存在する SiteMinder 環境をアップグレードするには、SiteMinder 環境からポリシー サーバおよび Web エージェントのうち 1 つを削除します。これらのコンポーネントはアップグレードされますが、残りのポリシー サーバおよび Web エージェントはリソースを保護し続行けます。すべてのコンポーネントがアップグレードされるまで SiteMinder コンポーネントの削除およびアップグレードを続行するか、互換性のある混在モードで動作を続行します。

以下の図は、単純な r6.x 環境と詳細を示しています。

- 既存のコンポーネントがアップグレードされる順序
- 新しいコンポーネントがインストールされる順序

注: 図はそれぞれ 1 つのポリシー/キー ストアを示しています。環境では、別個のポリシーおよびキー ストアを使用できます。



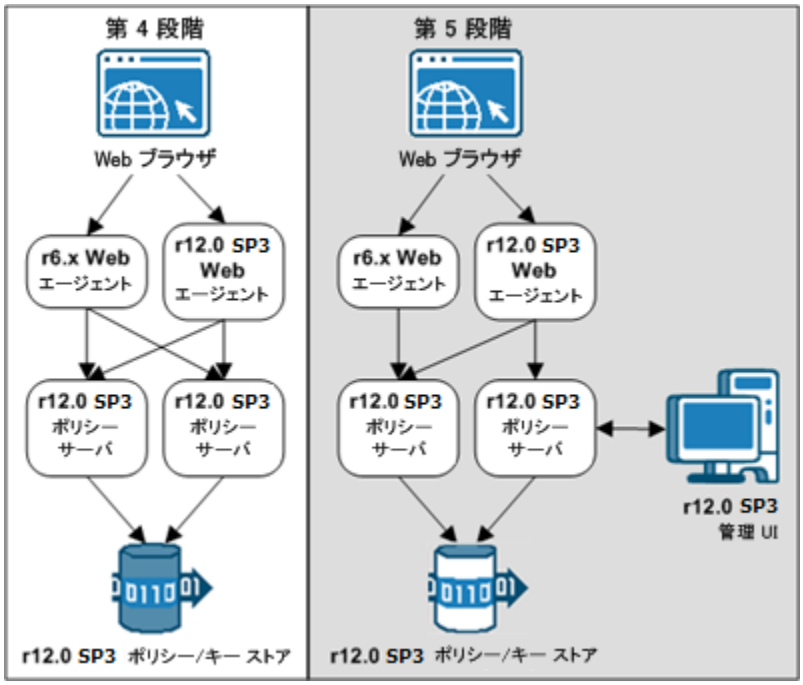
1. 第 1 段階では、r6.x ポリシー サーバが r12.0 SP3 にアップグレードされます。r12.0 SP3 ポリシー サーバは互換モードで動作します。以下の点について考慮してください。

   - r6.x Web エージェントは、r12.0 SP3 ポリシー サーバと通信し続けます。
   - r12.0 SP3 ポリシー サーバは、r6.x ポリシーおよびキー ストアと通信し続けます。
   - r6.x ポリシー サーバは、6.x ポリシーおよびキー ストアと通信し続けます。引き続き、r6.x ポリシー サーバ ユーザ インターフェースを使用して、r6.x ポリシー サーバ経由で r6.x ポリシー ストアを管理できます。

   重要: ポリシー サーバ インストーラにより、アップグレード時に r6.x ポリシー サーバ ユーザ インターフェースが FSS 管理 UI に置き換えられます。r12.0 SP3 ポリシー サーバは、引き続きアクセス制御を提供し、監査情報を含むログ ファイルを生成します。ただし、管理 UI がインストールされるまで、r12.0 SP3 ポリシー サーバ経由で r6.x ポリシー ストアを管理することはできません。

2. 第 2 段階では、r6.x Web エージェントが r12.0 SP3 にアップグレードされます。以下の点について考慮してください。
   - r6.x Web エージェントは、r6.x および r12.0 SP3 ポリシー サーバと通信し続けます。
   - r12.0 SP3 Web エージェントは、r12.0 SP3 ポリシー サーバのみと通信します。
3. 第 3 段階では、残りのポリシー サーバが r12.0 SP3 にアップグレードされます。r12.0 SP3 ポリシー サーバは、r6.x ポリシーおよびキー ストアとの互換モードで動作します。

   重要 ポリシー サーバはリソースの保護を続行するため、ポリシー サーバ管理コンソールにアクセスできますが、ポリシー サーバを管理することはできません。ポリシー サーバ インストーラにより、アップグレード時にポリシー サーバ ユーザ インターフェースが FSS 管理 UI に置き換えられました。r12.0 SP3 管理 UI をインストールするまで、ポリシー ストアにレコード ポリシー情報を記録することはできません。移行を計画するときは、この時間を考慮に入れてください。



4. 第 1 段階では、r6.x ポリシーおよびキー ストアが r12.0 SP3 にアップグレードされます。

5. 第 5 段階では、管理 UI がインストールされ、ポリシー サーバに登録されます。以下の点について考慮してください。
   - ポリシー ストアをアップグレードする前に、管理 UI をインストールできます。ただし、ポリシー ストアがアップグレードされるまで 管理 UI を登録することはできません。ポリシー ストアのアップグレード前に 管理 UI をインストールすると、ポリシー ストアが 管理 UI を使用できない時間が最小限に抑えられます。
   - r6.x Web エージェントは、混在モード互換の例として示されています。
6. （オプション）最終段階は、図には示されていませんが、以下の手順が含まれます。
   - 対応するポリシー サーバに各 FSS 管理 UI を登録します。FSS 管理 UI は 管理 UI を使用して登録されます。
   - レポート サーバをインストールして登録します。

     注: FSS 管理 UI の登録およびレポート サーバのインストールの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

r6.x から移行する方法

r6.x から r12.0 SP3 への移行を完了するには、以下の手順を完了します。

1. 「ポリシー サーバのアップグレード前の確認事項」の内容を確認します。
2. r6.x ポリシー サーバを r12.0 SP3 にアップグレードします。

   注: 以下の点について考慮してください。
   - ポリシー サーバ インストーラにより、アップグレード時に r6.x ポリシー サーバ ユーザ インターフェースが FSS 管理 UI に置き換えられます。r12.0 SP3 ポリシー サーバは、引き続きアクセス制御を提供し、監査情報を含むログ ファイルを生成します。ただし、管理 UI をインストールしないと r12.0 SP3 ポリシー サーバ経由で r6.x ポリシー ストアを管理することはできません。

- r12.0 SP3 ポリシー サーバは、r12.0 SP3 キー データベースとのみ通信できます。Federation セキュリティ サービス 環境をアップグレードする場合は、以下のいずれかを実行します。
  - 既存の SiteMinder キー データベースを r12.0 SP3 にアップグレードします。
  - 既存のキーおよび証明書を r12.0 SP3SiteMinder キー データベースに移行します。

  ポリシー サーバ インストーラでは、キー データベースを r12.0 SP3 にアップグレードしたり、ポリシー サーバのアップグレード時に r12.0 SP3 キー データベースを作成することができます。

3. 「ポリシー サーバをアップグレードした後」の内容を確認します。
4. (オプション) AM キー ストア (AM.keystore) データを r12.0 SP3 SiteMinder キー データベースに移行します。

   注: この手順は、r6.0、r6.0 SP1、r6.0 SP2、r6.0 SP3、および r6.0 SP4 Federation セキュリティ サービス 環境をアップグレードする場合のみ必要です。
5. r6.x Web エージェントを r12.0 SP3 にアップグレードします。
6. 残りの r6.x ポリシー サーバおよび r6.x Web エージェントをそれぞれ r12.0 SP3 にアップグレードします。

   重要 ポリシー サーバはリソースの保護を続行するため、ポリシー サーバ管理コンソールにアクセスできますが、ポリシー サーバを管理することはできません。ポリシー サーバ インストーラにより、アップグレード時にポリシー サーバ ユーザ インターフェースが FSS 管理 UI に置き換えられました。r12.0 SP3 管理 UI をインストールするまで、ポリシー ストアにレコード ポリシー情報を記録することはできません。移行を計画するときは、この時間を考慮に入れてください。

   注: r6.0、r6.0 SP1、r6.0 SP2、r6.0 SP3、または r6.0 SP4 Federation セキュリティ サービス 環境をアップグレードする場合は、AM.keystore データを r12.0 SP3SiteMinder キー データベースに移行します。
7. r6.x ポリシーおよびキー ストアを r12.0 SP3 にアップグレードします。

   注:既存の r6.x ポリシー ストア スキーマは、変更されていません。r12.0 SP3 の移行では、ポリシー ストア スキーマをアップグレードして、r12.0 SP3 によって必要とされるオブジェクトのポリシー ストアを拡張する必要があります。
8. r12.0 SP3 管理 UI をインストールします。

9. (オプション) 各 FSS 管理 UI を対応するポリシー サーバに登録します。
10. (オプション) レポート サーバをインストールします。

    注: FSS 管理 UI の登録およびレポート サーバのインストールの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

r6.x ポリシー サーバのアップグレード

以下のセクションでは、Windows と UNIX の r6.x UNIX ポリシー サーバをアップグレードする方法について詳述します。

アップグレード前の注意事項

ポリシー サーバをアップグレードする前に、以下の点を考慮します。

- テクニカル サポート サイトのインストール メディアを使用して、ポリシー サーバをアップグレードします。

  注: オペレーティング システムごとのインストール メディア名のリストについては、「*Policy Server Release Notes*」のインストールおよびアップグレードの考慮事項を参照してください。

- (Linux) 必要な Linux ライブラリがポリシー サーバのホスト システムにインストールされていることを確認します。詳細については、Required Linux Libraries を参照してください。

- 5.1 Sun ONE ディレクトリ サーバとポリシー サーバが同じ Windows 2003 システムにインストールされている場合、LDAP SDK を 5.0.8 (2002 年 7 月 17 日付) 以降にアップグレードします。 LDAP SDK のアップグレードに失敗すると、ポリシー サーバが不安定になります。

  注: LDAP SDK は、Sun ONE ディレクトリ サーバを使用しているかどうかにかかわらずアップグレードしてください。

- アップグレードするポリシー サーバを環境から削除します。ポリシー サーバを削除すると、アップグレード中に Web エージェントがポリシー サーバに接続することがなくなります。

- ポリシー サーバ管理コンソールのすべてのインスタンスをシャットダウンします。

- (UNIX) アクセス権によっては、以下のコマンドを実行することでインストール メディアへの実行アクセス権を追加する必要があります。

  ```
  chmod +x installation_media
  ```

  installation_media

  ポリシー サーバのインストール実行可能ファイルを指定します。

- (UNIX) 別のサブネットにまたがってポリシー サーバ インストーラを実行した場合、クラッシュすることがあります。インストーラは、ポリシー サーバ ホスト システム上で直接実行してください。
- ドキュメントをインストールします。SiteMinder ドキュメントは、ポリシー サーバと同時にはインストールされません。ポリシー サーバをアップグレードする前にドキュメントをインストールすることをお勧めします。

注: r6.0 SP6 および r12.0 SP2 のマニュアル選択メニューはテクニカル サポート サイトで提供されています。これらのバージョン用のインストール キットもありますが、ドキュメントのインストールは必須ではありません。マニュアル選択メニューはテクニカル サポート サイトから表示およびダウンロードできます。

詳細情報:

インストール メディアの検索 (P. 156)
SiteMinder のドキュメント (P. 9)

必要とされる Linux ライブラリ

このコンポーネントの Linux バージョンをインストールまたはアップグレードしている場合、ホスト システム上で以下が必要になります。

```
compat-libstdc++-33.3.2.3-patch_version.i386.rpm
```

この rpm をインストールして、お使いのオペレーティング システム用の適切な 32 ビット C ランタイム ライブラリが使用できることを確認してください。

Windows

ポリシー サーバをアップグレードする方法

1. 実行中のすべてのアプリケーションを終了します。
2. *installation_media* をダブルクリックします。

   installation_media

   ポリシー サーバのインストール実行可能ファイルを指定します。

   ポリシー サーバ インストーラが起動します。

   注: オペレーティング システムごとのインストール メディア名のリストについては、「*Policy Server Release Notes*」のインストールおよびアップグレードの考慮事項を参照してください。
3. インストーラを実行するときは、以下の点を考慮します。
   - インストーラにより、SiteMinder コンポーネントの選択が求められます。コンポーネントを選択する場合
     - 以前に環境に設定されたコンポーネントを再設定します。必ず、対応するコンポーネントを選択してください。
     - Federation セキュリティ サービス 環境をアップグレードする場合か、SiteMinder Information Card 認証方式を使用する予定の場合は、SM キー データベースの作成/SM キー データベース パスワードの変更のチェック ボックスをオンにします。
     - 新しいポリシーストアを設定しない場合は、ポリシー ストアのチェック ボックスをオフにします。既存のポリシー ストア設定を再設定する必要はありません。アップグレードされたポリシー サーバに、ポリシー ストア設定が保持されます。既存のポリシー ストアを手動でアップグレードします。
   - SM キー データベースの作成/SM キー データベース パスワードの変更のチェック ボックスをオンにした場合は、以下の手順を実行します。
     - 既存のキー データベース データをこのリポジトリに移行する場合は、r12.0 SP3 キー データベースを作成します。
     - 既存のキー データベースをアップグレードする予定の場合は、パスワードを変更します。パスワードを変更すると、FIPS 準拠のアルゴリズムを使用して、データベース パスワードおよび既存の暗号化データが再暗号化されます。
   - パス情報を切り取ってウィザードに貼り付ける場合は、文字を入力して［次へ］ボタンを有効にします。

4. インストール設定を確認し、[インストール]をクリックします。

   ポリシー サーバがアップグレードされます。選択したコンポーネントは、ポリシー サーバで使用できるように設定されます。

   注: FSS 管理 UI は、ポリシー サーバのアップグレード時にインストールされました。FSS 管理 UI は、Federation セキュリティ サービスを管理するためのものです。ポリシー ストアをアップグレードして 管理 UI をインストールした後、ポリシー サーバに FSS 管理 UI を登録します。FSS 管理 UI の登録の詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

アップグレード中に問題が発生した場合、*siteminder_home*\siteminder\install_config_info にポリシー サーバのインストール ログ ファイルがあります。

siteminder_home

ポリシー サーバのインストール パスを指定します。

UNIX GUI

ポリシー サーバをアップグレードする方法

1. 実行中のすべてのアプリケーションを終了します。
2. SiteMinder インストール ディレクトリから ksh シェルで以下のスクリプトを実行します。

   ```
   ../ca_ps_env.ksh
   ```

   注: スクリプトを実行するときは、ピリオドの間にスペースを入れてください (. .)。
3. シェルを開き、インストール実行可能ファイルに移動します。
4. 以下のコマンドを入力します。

   ```
   ./installation_media gui
   ```

   installation_media

   ポリシー サーバのインストール実行可能ファイルを指定します。

   ポリシー サーバ インストーラが起動します。

   注: オペレーティング システムごとのインストール メディア名のリストについては、「*Policy Server Release Notes*」のインストールおよびアップグレードの考慮事項を参照してください。

5. インストーラを実行するときは、以下の点を考慮します。

   - インストーラにより、SiteMinder コンポーネントの選択が求められます。コンポーネントを選択する場合
     - 以前に環境に設定されたコンポーネントを再設定します。必ず、対応するコンポーネントを選択してください。
     - Federation セキュリティ サービス 環境をアップグレードする場合か、SiteMinder Information Card 認証方式を使用する予定の場合は、SM キー データベースの作成/SM キー データベース パスワードの変更のチェック ボックスをオンにします。
     - 新しいポリシーストアを設定しない場合は、ポリシー ストアのチェック ボックスをオフにします。既存のポリシー ストア設定を再設定する必要はありません。アップグレードされたポリシー サーバに、ポリシー ストア設定が保持されます。既存のポリシー ストアを手動でアップグレードします。
   - SM キー データベースの作成/SM キー データベース パスワードの変更のチェック ボックスをオンにした場合は、以下の手順を実行します。
     - 既存のキー データベース データをこのリポジトリに移行する場合は、r12.0 SP3 キー データベースを作成します。
     - 既存のキー データベースをアップグレードする場合は、パスワードを変更します。パスワードを変更すると、FIPS 準拠のアルゴリズムを使用して、データベース パスワードおよび既存の暗号化データが再暗号化されます。
   - パス情報を切り取ってウィザードに貼り付ける場合は、文字を入力して［次へ］ボタンを有効にします。

6. インストール設定を確認し、［インストール］をクリックします。

   ポリシー サーバがアップグレードされます。選択したコンポーネントは、ポリシー サーバで使用できるように設定されます。

   注: アップグレードには数分かかる場合があります。

7. ［完了］をクリックし、システムを再起動します。

   注: FSS 管理 UI は、ポリシー サーバのアップグレード時にインストールされました。FSS 管理 UI は、Federation セキュリティ サービス を管理するためのものです。ポリシー ストアをアップグレードして 管理 UI をインストールした後、ポリシー サーバに FSS 管理 UI を登録します。FSS 管理 UI の登録の詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

アップグレード中に問題が発生した場合、*siteminder_home*/siteminder/install_config_info にポリシー サーバのインストール ログ ファイルがあります。

siteminder_home

ポリシー サーバのインストール パスを指定します。

UNIX コンソール

ポリシー サーバをアップグレードする方法

1. 実行中のすべてのアプリケーションを終了します。
2. SiteMinder インストール ディレクトリから ksh シェルで以下のスクリプトを実行します。

   ```
   ../ca_ps_env.ksh
   ```

   注: スクリプトを実行するときは、ピリオドの間にスペース を入れてください (. .)。
3. シェルを開き、インストール実行可能ファイルに移動します。
4. 以下のコマンドを入力します。

   ```
   ./installation_media -i console
   ```

   installation_media

   ポリシー サーバのインストール実行可能ファイルを指定します。

   ポリシー サーバ インストーラが起動します。

   注: オペレーティング システムごとのインストール メディア名のリストについては、「*Policy Server Release Notes*」のインストールおよびアップグレードの考慮事項を参照してください。

5. インストーラを実行するときは、以下の点を考慮します。

   - インストーラにより、SiteMinder コンポーネントの選択が求められます。各コンポーネントには、数字のプレフィックスが付きます。1 つ以上のコンポーネントを選択するため、数字をカンマ(,)で区切って入力します。どの機能も選択しない場合は、カンマのみを入力します。コンポーネントを選択する場合

     - 以前に環境に設定されたコンポーネントを再設定します。必ず、対応するコンポーネントを選択してください。
     - Federation セキュリティ サービス 環境をアップグレードする場合か、SiteMinder Information Card 認証方式を使用する予定の場合は、SM キー データベースの作成/SM キー データベース パスワードの変更のチェック ボックスをオンにします。
     - 新しいポリシーストアを設定する場合は、ポリシー ストアのみ選択します。既存のポリシー ストア設定を再設定する必要はありません。アップグレードされたポリシー サーバに、ポリシー ストア設定が保持されます。既存のポリシー ストアを手動でアップグレードします。

   - SM キー データベースの作成/SM キー データベース パスワードの変更のチェック ボックスをオンにした場合は、以下の手順を実行します。

     - 既存のキー データベース データをこのリポジトリに移行する場合は、r12.0 SP3 キー データベースを作成します。
     - 既存のキー データベースをアップグレードする場合は、パスワードを変更します。パスワードを変更すると、FIPS 準拠のアルゴリズムを使用して、データベース パスワードおよび既存の暗号化データが再暗号化されます。

6. インストール設定を確認し、Enter キーを押します。

   ポリシー サーバがアップグレードされます。選択したコンポーネントは、ポリシー サーバで使用できるように設定されます。

   注: アップグレードには数分かかる場合があります。

7. Enter キーを押し、システムを再起動します。

   注: FSS 管理 UI は、ポリシー サーバのアップグレード時にインストールされました。FSS 管理 UI は、Federation セキュリティ サービス を管理するためのものです。ポリシー ストアをアップグレードして 管理 UI をインストールした後、ポリシー サーバに FSS 管理 UI を登録します。FSS 管理 UI の登録の詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

アップグレード中に問題が発生した場合、*siteminder_home*/siteminder/install_config_info にポリシー サーバのインストール ログ ファイルがあります。

siteminder_home

ポリシー サーバのインストール パスを指定します。

ポリシー サーバをアップグレードした後

ポリシー サーバ監査ログが、ポリシー ストア オブジェクトの管理者による変更が含まれるように設定されている場合は、以下の点を考慮します。

- ポリシー サーバ管理コンソールを初めて開くと、この種類の管理者監査を無効にするように求めるメッセージが表示されます。
- このメッセージは、この種類の管理者イベントをポリシー サーバ監査ログに含める方法に変更があったために表示されます。この種類の管理者イベントを監査ログに含めるには、ポリシー サーバ管理コンソールではなく XPSConfig ユーティリティを使用します。デフォルトでは、XPSConfig ユーティリティを使用するとポリシー ストア オブジェクトへの管理者による変更のロギングが有効になります。

[ログ]タブにある、ポリシー ストア オブジェクトに対して管理者が行った変更の設定を、イベントのログを記録しないように変更するまでは、メッセージが表示され続けます。変更後、設定は無効になったように見えますが、ポリシー ストア オブジェクトへの管理者による変更はログに記録され続けます。

ポリシー サーバ監査ログからこの種類の管理者イベントを除外する場合は、XPSConfig ユーティリティを使用して無効にします。

注: XPSConfig ユーティリティの使用の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

AM キー ストア データの SiteMinder キー データベースへの移行

r6.0、r6.0 SP1、r6.0 SP2、r6.0 SP3、または r6.0 SP4 から Federation セキュリティ サービス 環境をアップグレードする場合、PKI インフラストラクチャを変更するには、AM キー ストア（AM.keystore）に現在格納されているデータを r12.0 SP3 SiteMinder キー データベース（smkeydatabase）に移行する必要があります。

AM.keystore データは、migratekeystore ユーティリティを使用して SiteMinder キー データベースに移行します。

注: migratekeystore ユーティリティの使用の詳細については、「*Federated Security Services Guide*」を参照してください。

r6.x Web エージェントをアップグレードします。

Web エージェントのアップグレードは、移行処理の第 2 段階です。

SiteMinder r6.x Web エージェントは、r12.0 SP3 ポリシー サーバと通信できます。このため、Web エージェントを r12.0 SP3 にアップグレードする前に、ポリシー サーバを r12.0 SP3 にアップグレードします。

r6.x Web エージェントのアップグレード前の確認事項

Web エージェントをアップグレードする前に、以下の点を確認してください。

- （UNIX）Web エージェントのインストールに使用したのと同じアカウントを使用して、Web エージェントをアップグレードします。別のアカウントを使用した場合、アップグレードに失敗する場合があります。
- WAOP（Web Agent Option Pack、Web エージェント オプション パック）設定ファイルをバックアップし、WAOP をアンインストールします。

  注: WAOP のアンインストールの詳細については、「*Web Agent Option Pack Guide*」を参照してください。
- ポリシー サーバが設定されていることを確認します。
- 必要な管理者およびポリシー サーバ オブジェクト名を識別します。
- Web エージェント要件を識別します。

ポリシー サーバが設定されていることを確認します。

Web エージェントをアップグレードする前に、以下の手順を実行します。

- ポリシー サーバが、Web エージェント ホスト システムに接続できることを確認します。
- トラステッド ホストを登録する前に、ポリシー サーバが実行されていることを確認します。ポリシー サーバ管理コンソールの[ステータス]タブでポリシー サーバを起動します。

必要な管理者名およびポリシー サーバ オブジェクト名の識別

Web エージェントをアップグレードするには、ポリシー サーバ管理者から以下の情報を入手必要があります。

- ホストの登録権限を持つ SiteMinder 管理者の名前。
- ホスト設定オブジェクトの名前。
- エージェント設定オブジェクトの名前。

Web エージェントの要件の識別

パッチおよび他の Web エージェントの要件の詳細については、「*Web エージェント インストール ガイド*」を参照してください。

r6.x Web エージェントをアップグレードします。

r12.0 SP3 Web エージェント インストーラを使用して、Windows または UNIX の r6.x Web エージェントをアップグレードします。

注: オプション パック機能が必要なエージェントは、r12.0 SP3 Web エージェント オプション パックをインストールする前に r12.0 SP3 にアップグレードする必要があります。Web エージェントのアップグレードの詳細については、「*Web エージェント インストール ガイド*」を参照してください。r12.0 SP3 Web エージェント オプション パックのインストールの詳細については、「*Web Agent Option Pack Guide*」

r6.x ポリシー ストアをアップグレードします。

ポリシーおよびキー ストアのアップグレードは、移行処理の第 3 段階です。以下のセクションでは、r6.x ポリシーおよびキー ストアを r12.0 SP3 にアップグレードする方法について詳述します。

ポリシー ストアのアップグレードのオプション

r6.x ポリシー ストアを r12.0 SP3 にアップグレードするには、2 つのパスがあります。以下の方法が可能です。

- 既存のポリシーおよびキー ストアを r12.0 SP3 にアップグレードします。
- r12.0 SP3 ポリシーおよびキー ストアを作成し、既存のポリシーおよびキー ストア データを新しいインスタンスにインポートします。

このガイドでは、既存のポリシーおよびキー ストアをアップグレードする手順について詳述します。

r12.0 SP3 ポリシーおよびキー ストアを作成する場合

1. 適切なバージョンの smobjexport を使用して、ポリシーおよびキー ストア データをエクスポートします。

   注: r6.x バージョンの smobjimport の詳細については、r6.x の「ポリシー サーバ インストール ガイド」を参照してください。

2. r12.0 SP3 ポリシーおよびキー ストアを作成します。

   注: r12.0 SP3 ポリシーおよびキー ストアの作成の詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

3. r12.0 SP3 バージョンの smobjimport を使用して、ポリシーおよびキー ストア データを r12.0 SP3 ポリシーおよびキー ストアにインポートします。

   注: r12.0 SP3 バージョンの smobjimport の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

r6.x ポリシー ストアをアップグレードする方法

r12.0 SP3 へのアップグレードに、新しいポリシーストアは必要ありません。既存のポリシー ストアを r12.0 SP3 にアップグレードできます。

ポリシー ストアをアップグレードするには、以下の手順を完了します。

1. ポリシー ストア スキーマを拡張します。

   注:既存の r6.x ポリシー ストア スキーマは、変更されていません。r12.0 SP3 の移行では、ポリシー ストア スキーマをアップグレードして、r12.0 SP3 によって必要とされるオブジェクトのポリシー ストアを拡張する必要があります。

2. ベース ポリシー ストア オブジェクトをインポートします。

   注: Federation セキュリティ サービス 環境をアップグレードする場合、ポリシー サーバ オプション パック(PSOP)スキーマは変更されません。ポリシー ストアの ampolicy.smdif ファイルにデフォルト オブジェクトがすでに含まれている場合、ファイルを再インポートする必要はありません。

3. ポリシー ストア データ定義をインポートします。

注: SiteMinder プラットフォームのサポート マトリックスに記載された SiteMinder ストアを設定またはアップグレードしようとして、このガイドの手順が見つからない場合は、「*Directory Configuration Guide*」を参照してください。

Active Directory ポリシー ストア スキーマの拡張

ポリシー ストア スキーマを拡張して、r12.0 SP3 で導入されたオブジェクトを格納します。既存の r6.x ポリシー ストア スキーマは、変更されていません。

Active Directory ポリシー ストア スキーマを拡張する方法

1. *policy_server_home*\xps\db に移動し、ActiveDirectory.ldif ファイルを開きます。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. <RootDN> の各インスタンスを、ルート DN の実際の値に手動で置き換えます。

   例: dc=domain,dc=com

3. コマンド ウィンドウから *policy_server_home*/bin に移動します。
4. 以下のコマンドを実行します。

   ```
   smldapsetup ldmod -fpolicy_server_home/xps/db/ActiveDirectory.ldif
   ```

   ポリシー ストア スキーマが拡張され、r12.0 SP3 により導入されたオブジェクトが格納されます。

   重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ADAM ポリシー ストア スキーマの拡張

ポリシー ストア スキーマを拡張して、r12.0 SP3 で導入されたオブジェクトを格納します。既存の r6.x ポリシー ストア スキーマは、変更されていません。

ADAM ポリシー ストア スキーマを拡張する方法

1. *policy_server_home*/xps/db に移動し、ADAM.ldif ファイルを開きます。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. {guid} の各インスタンスを、かっこの guid の実際の値に置き換え、ファイルを保存します。

   例: {CF151EA3-53A0-44A4-B4AC-DA0EBB1FF200}

3. コマンド ウィンドウから *policy_server_home*/bin に移動します。
4. 以下のコマンドを実行します。

   ```
   smldapsetup ldmod -fpolicy_server_home/xps/db/ADAM.ldif
   ```

   ポリシー ストア スキーマが、r12.0 SP3 によって必要とされるオブジェクト用に拡張されます。

   重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

CA Directory ポリシー ストア スキーマの拡張

ポリシー ストア スキーマを拡張して、r12.0 SP3 で導入されたオブジェクトを格納します。既存の r6.x ポリシー ストア スキーマは、変更されていません。

CA Directory ポリシー ストア スキーマを拡張する方法

1. 以下のファイルを CA Directory の DXHOME\config\schema ディレクトリにコピーします。

   etrust.dxc

   注: etrust.dxc ファイルは、ポリシー サーバと同時に *policy_server_home*\xps\db にインストールされます。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. CA Directory DXHOME\bin ディレクトリに以下のファイルをコピーします。

   - etrust_schema.txt
   - schema.txt

   注: etrust_schema.txt ファイルは、ポリシー サーバと同時に *policy_server_home*\xps\db にインストールされます。schema.txt ファイルは、ポリシー サーバと共に *policy_server_home*\eTrust にインストールされます。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

3. SiteMinder スキーマ ファイル(.dxg)を開き、ファイルの末尾に以下の行を追加します。

```
#CA Schema
source "netegrity.dxc"
source "etrust.dxc"
```

4. ファイルの末尾に以下の行を追加することで、DSA の DXI ファイルを編集します。

   - **r12**

     ```
     # cache configuration
     set max-cache-size = 100;
     set cache-attrs = all-attributes;
     set cache-load-all = true;
     set ignore-name-bindings = true;
     ```

     注: DXI ファイルは DXHOME\config\servers にあります。最大キャッシュ サイズのエントリは、合計キャッシュ サイズ(MB 単位)です。CA Directory サーバで利用可能な合計メモリとポリシー ストアの合計サイズに基づいてこの値を調整します。

   - **r12 SP1 以降**

     ```
     # cache configuration
     #set max-cache-size = 100;
     #set cache-attrs = all-attributes;
     #set cache-load-all = true;
     set ignore-name-bindings = true;
     ```

5. DSA のデフォルト DXC ファイル(default.dxc)を開き、以下を探します。

   ```
   # size limits
   set max-users = 255;
   set credits = 5;
   set max-local-ops = 100;
   set max-dsp-ops = 100;
   set max-op-size = 200;
   set multi-write-queue = 20000;
   ```

   注: デフォルト DXC ファイルは、DXHOME\dxserver\config\limits にあります。

6. 以下の内容と一致するように設定を編集し、DXC ファイルを保存します。

```
# size limits
set max-users = 1000;
set credits = 5;
set max-local-ops = 1000;
set max-dsp-ops = 1000;
set max-op-size = 4000;
set multi-write-queue = 20000;
```

注: サイズ制限設定を編集すると、キャッシュ サイズ エラーが CA Directory ログ ファイルに表示されなくなります。

重要: 複数の書き込みキュー設定は、テキスト ベースの設定でのみ使用できます。DSA が DXmanager でセットアップされる場合は、この設定を省略します。

7. JXplorer を使用して、ポリシー ストア DSA にアクセスします。
8. ルート エレメントの下で、以下のベース ツリー構造を見つけます。

   Netegrity, SiteMinder, PolicySvr4

9. PolicySvr4 の下に以下の名前の組織単位(ルート エレメント)を作成します。

   XPS

10. DSA ユーザとして、以下のコマンドを使用して DSA を停止して再起動します。

    `dxserver stop DSA_Name`

    `dxserver start DSA_Name`

    DSA_Name

    ポリシー ストア DSA の名前を指定します。

    ポリシー ストア スキーマが拡張され、r12.0 SP3 により導入されたオブジェクトが格納されます。

Sun Java System Directory Server ポリシー ストア スキーマの拡張

ポリシー ストア スキーマを拡張して、r12.0 SP3 で導入されたオブジェクトを格納します。既存の r6.x ポリシー ストア スキーマは、変更されていません。

Sun Java System Directory Server ポリシー ストア スキーマを拡張する方法

1. コマンド ウィンドウを使用して、*policy_server_home*/bin に移動します。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   ```
   smldapsetup ldmod -fpolicy_server_home/xps/db/SunOne.ldif
   ```

   ポリシー ストア スキーマが拡張され、r12.0 SP3 により導入されたオブジェクトが格納されます。

   重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

MS SQL Server ポリシー ストア スキーマの拡張

ポリシー ストア スキーマを拡張して、r12.0 SP3 で導入されたオブジェクトを格納します。既存の r6.x ポリシー ストア スキーマは、変更されていません。

Microsoft SQL Server ポリシー ストア スキーマを拡張する方法

1. ポリシー サーバ データベース情報を管理するユーザとして SQL Server にログインします。
2. クエリ アナライザを起動します。
3. データベース リストからポリシー ストア データベース インスタンスを選択します。

4. テキスト エディタで SQLServer.sql を開き、ファイル全体の内容をコピーします。

   注: SQLServer.sql ファイルは *policy_server_home*\xps\db にあります。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

5. SQLServer.sql からクエリにスキーマを貼り付けて、クエリを実行します。

   ポリシー ストア スキーマが拡張され、r12.0 SP3 により導入されたオブジェクトが格納されます。

Oracle ポリシー ストア スキーマの拡張

ポリシー ストア スキーマを拡張して、r12.0 SP3 で導入されたオブジェクトを格納します。既存の r6.x ポリシー ストア スキーマは、変更されていません。

Oracle ポリシー ストア スキーマを拡張する方法

1. sqlplus または他の Oracle ユーティリティを使用して、ポリシー サーバ データベース情報を管理するユーザとして Oracle にログインします。

   注: SYS ユーザや SYSTEM ユーザには、SiteMinder スキーマを作成しないことをお勧めします。必要な場合は、SMOWNER などの Oracle ユーザを作成し、そのユーザにスキーマを作成します。

2. 以下の r12.0 SP3 スクリプトを 6.x データベース インスタンスにインポートします。

   $NETE_PS_ROOT/xps/db/Oracle.sql

   注: sqlplus を使用する場合は、@ 記号を使用してスキーマを実行してください。

   sqlplus の例: <@NETE_PS_ROOT>/xps/db/Oracle.sql

   sqlplus 以外の例: <$NETE_PS_ROOT>/xps/db/Oracle.sql

   ポリシー ストア スキーマが拡張され、r12.0 SP3 により導入されたオブジェクトが格納されます。

ベース ポリシー ストア オブジェクトのインポート

デフォルトの SiteMinder オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがアップグレードされます。デフォルトの SiteMinder オブジェクトは、ポリシー ストアにポリシー情報を格納するために必要です。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home\db\smdif\upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

upgrade_smdif_file_name

インポート ファイルの名前を指定します。

- **r60 から r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
- **r60 SP1 から r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
- **r60 SP2 から r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
- **r60 SP3 から r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r60 SP4 から r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
- **r60 SP5 から r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r60 SP6 から r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト出力: stdout

-f

重複するポリシー ストア オブジェクトを、r12.0 SP3 のもので上書きします。

引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

Windows の例: smobjimport

```
-i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
-wPassword -v
```

UNIX の例: smobjimport

-i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v

ベース ポリシー ストア オブジェクトがインポートされます。

2. 以下のコマンドを実行します。

重要: ampolicy.smdif が以前にポリシー ストアにインポートされている場合は再インポートしないでください。

```
smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

-policy_server_home

インポート ファイルのパスと名前を指定します。

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-f

重複するオブジェクトを上書きします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

注: ampolicy.smdif をインポートすると、SiteMinder から別々にライセンスされるフェデレーション セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能を使用する予定の場合は、ライセンス情報について CA ジャパン ダイレクトに問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*\xps\dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

管理ユーザ インターフェースのインストール

旧バージョンの SiteMinder とは異なり、ポリシー サーバ ユーザ インターフェースはポリシー サーバと同時にインストールされません。r12.0 SP3 管理 UI は別個にインストールする必要があります。

注: 管理 UI のインストールの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

FSS 管理 UI の登録

FSS 管理 UI は、ポリシー サーバと同時にインストールされ、Federation セキュリティ サービス の管理に使用されるアプレットベースのアプリケーションです。Federation セキュリティ サービス コンポーネントは、アフィリエイト(コンシューマ、サービス プロバイダ、リソース パートナー)と、2 つのパートナー間のフェデレーション通信をサポートするために設定する SAML 認証方式で構成されます。

ポリシー サーバに FSS 管理 UI を登録して、両方のコンポーネント間の通信が FIPS で暗号化(AES 暗号化)されるようにします。

FSS 管理 UI は、SiteMinder Federation セキュリティ サービス を管理するために用意されています。以前のバージョンの SiteMinder ポリシー サーバのユーザ インターフェースと異なり、すべての SiteMinder オブジェクトが FSS 管理 UI に表示されることがわかります。表示されないオブジェクトは、EPM(Enterprise Policy Management)およびレポートに関連するオブジェクトだけです。FSS 管理 UI を使用すると、SiteMinder オブジェクトを管理できます。FSS 管理 UI を使用しているときに情報が必要となった場合は、FSS 管理 UI オンライン ヘルプ システムを調べます。

組織とパートナーとの間でフェデレーションが実現してしない場合、ポリシー サーバに登録しなくても FSS 管理 UI をポリシー サーバ マシンに安全に残すことができます。

注: FSS 管理 UI の登録の詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

r6.x セッション サーバのアップグレード

r12.0 SP3 セッション サーバ スキーマは、r6.0 SP5 以降変わっていません。r6.0 SP5 以降のセッション サーバを使用している場合、スキーマをアップグレードする必要はありません。

注: セッション ストア スキーマのインポートの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

セッション サーバをアップグレードするには、以下の .sql スキーマ スクリプトのいずれかを既存のセッション ストア データベースにインポートします。以下のスクリプトは、*policy_server_home*\db\SQL にあります。

- sm_mssql_ss_upgrade_60_to_R12sp3.sql

  SQL Server セッション ストアをアップグレードし、新しい Expiry Data テーブルをセッション ストアに追加します。

- sm_oracle_ss_upgrade_60_to_R12sp3.sql

  Oracle セッション ストアをアップグレードし、新しい Expiry Data テーブルをセッション ストアに追加します。

policy_server_home

ポリシー サーバのインストール パスを指定します。

注: SiteMinder プラットフォームのサポート マトリックスに記載された SiteMinder ストアを設定またはアップグレードしようとして、このガイドの手順が見つからない場合は、「*Directory Configuration Guide*」を参照してください。

r6.x Audit ログ データベースのアップグレード

SiteMinder 用 iRecorder を使用すると、SCC（Security Command Center）は、SiteMinder SQL Server または Oracle ログ データベースのセキュリティ関連ロギング データを読み取ることができます。

注: SiteMinder 用 iRecorder の詳細については、「*eTrust Audit iRecorder Reference Guide*」を参照してください。監査ログ スキーマのインポートの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

統合するには、監査ログ データベースのスキーマをアップグレードする必要があります。そのためには、*policy_server_home*\db\SQL にある sm_mssql_logs_eaudit_upgrade.sql スクリプトまたは sm_oracle_logs_eaudit_upgrade.sql スクリプトをインポートします。このスクリプトは、SiteMinder と SCC を統合する場合のみインポートします。

policy_server_home

ポリシー サーバのインストール パスを指定します。

注: SiteMinder と SCC の統合は、DB2 ロギング データベースでは機能しません。

監査ログ データベースをアップグレードするには、以下のスキーマ スクリプトのいずれかを既存の SiteMinder 監査ログ データベースにインポートします。

sm_mssql_logs_eaudit_upgrade.sql

SQL Server 監査ログ データベースを r6.x から r12.0 SP3 にアップグレードします。

sm_oracle_logs_eaudit_upgrade.sql

Oracle 監査ログ データベースを r6.x から r12.0 SP3 にアップグレードします。

注: SiteMinder プラットフォームのサポート マトリックスに記載された SiteMinder ストアを設定またはアップグレードしようとして、このガイドの手順が見つからない場合は、「*Directory Configuration Guide*」を参照してください。

並行アップグレードの仕組み

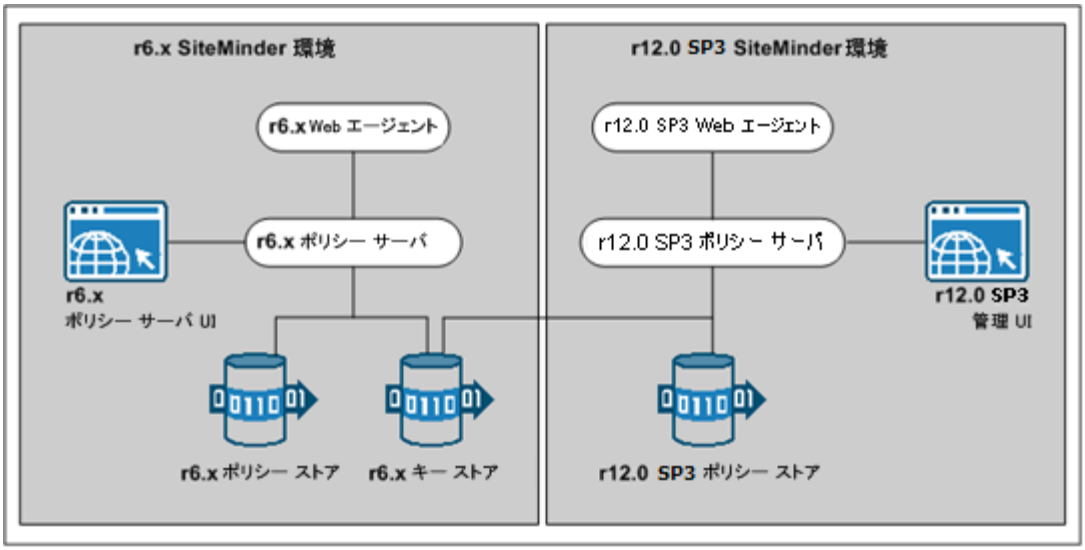
既存の r6.x 環境を r12.0 SP3 に移行する必要はありません。むしろ、既存の展開の並行 r12.0 SP3 環境を設定できます。

以下の図は、単純な並列アップグレードおよび詳細を示しています。

- 既存のリソースの保護を続行する r6.x 環境。
- r6.x ポリシー ストアの SiteMinder オブジェクトの管理に使用される r6.x ポリシー サーバ ユーザ インターフェース。
- 新しいリソースを保護する r12.0 SP3 環境。

- r12.0 SP3 ポリシー ストアの SiteMinder オブジェクトの管理に使用される r12.0 SP3 管理 UI。
- 共通 r6.x キー ストア。共通キー ストアにより、両方の環境でシングル サインオンが有効になります。

  注: 図には示されまていませんが、複数のキー ストアを使用して両方の環境でシングル サインオンを有効にできます。



並行環境を設定する方法

並行環境を設定するには、以下の手順を実行します。

1. 並行環境のキー管理オプションを確認して、シングル サインオンを実装する方法を調べます。
2. r12.0 SP3 環境を作成します。
3. 以下のいずれかを行います。
   - 両方の環境が共通キー ストアのシングル サインオン要件を満たすようにしてください。
   - 両方の環境が複数キー ストアのシングル サインオン要件を満たすようにしてください。
4. (オプション) r6.x ポリシー ストア データを移行します。
5. ユーザ ディレクトリのシングル サインオン要件を確認します。

並行環境のキー管理オプション

並行アップグレードを成功させるには、SiteMinder キーを管理して既存の環境と r12.0 SP3 環境の間でシングル サインオンを維持する必要があります。2 つの SiteMinder キー管理オプションを使用できます。展開するオプションは、両方の環境間で 1 つ以上のキー ストアを実装する方法によって決まります。オプションは、以下のとおりです。

- 共通のキーストアがある複数のポリシーストア
- 個別のキーストアがある複数のポリシーストア

共通キー ストアの展開

すべてのポリシー サーバは、キー ロールオーバーに 1 つのキー ストアを使用できます。以下の図は、次のものを表しています。

- r6.x ポリシー ストアに接続する r6.x ポリシー サーバ。
- r12.0 SP3 ポリシー ストアに接続する r12.0 SP3 ポリシー サーバ。
- すべてのポリシー サーバのキー データを維持する共通 r6.x キー ストア。共通キー ストアを使用すると、すべてのポリシー サーバに関連付けられたエージェントでキーを共有できます。キーを共有すると、両方の環境間でシングル サインオンが有効になります。

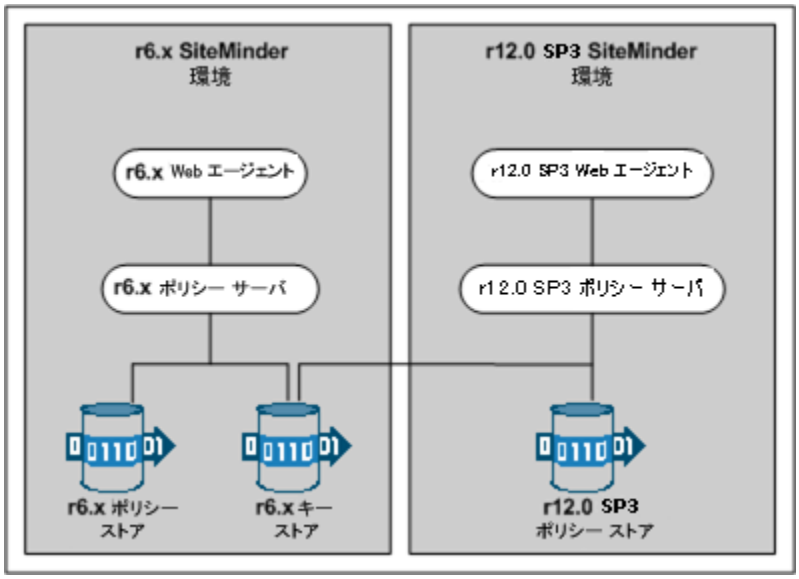
  重要: r6.x キー ストアは、r6.x ポリシー ストアとは別個に設定する必要があります。

- 共通キー ストアに接続して新しいキーを取得するすべてのポリシー サーバ。

  重要: r12.0 SP3 ポリシー サーバは、r6.x キー ストアを使用して設定する必要があります。r6.x ポリシー サーバは、r12.0 SP3 キー ストアと通信できません。

- 対応するポリシー サーバをポーリングして新しいキーを取得するすべての Web エージェント。

注: 図には示されていませんが、ポリシーストアとストアデータは、フェイルオーバーのために複製することができます。データベースまたはディレクトリ サーバのタイプにより、データの複製方法が決まります。マスタ/スレーブ環境でのキー管理の詳細については、「ポリシー サーバ管理ガイド」を参照してください。 データの複製の詳細については、使用しているベンダーから発行されたマニュアルを参照してください。



複数キー ストアの展開

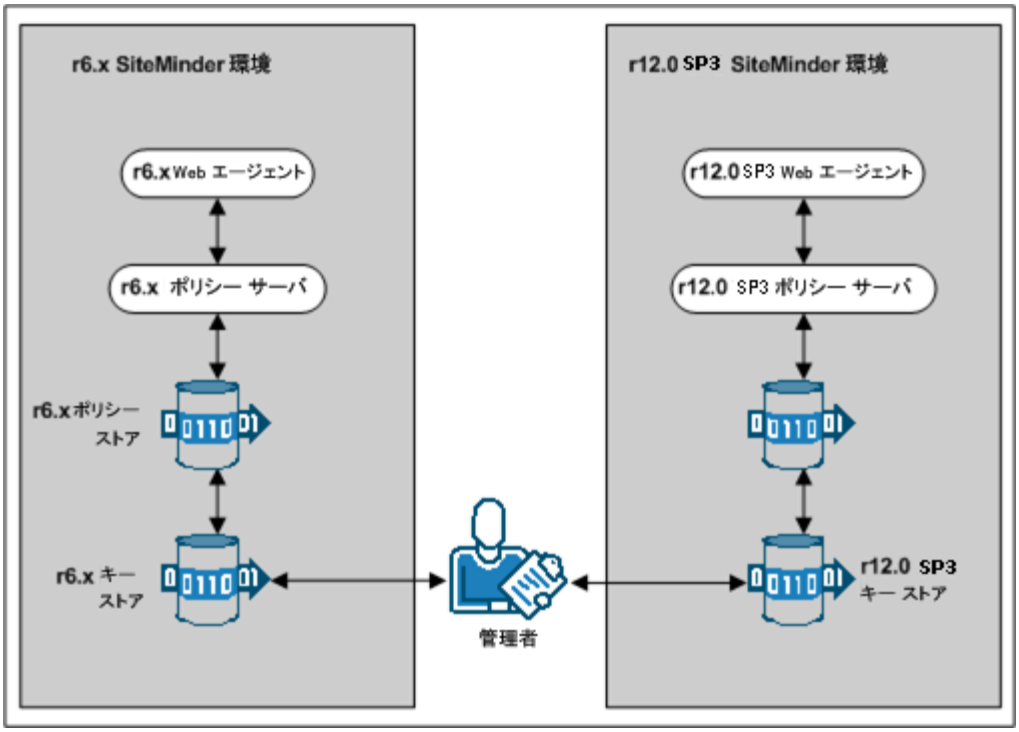
既存の r6.x ポリシー サーバは、キー ロールオーバーに r6.x キー ストアを使用できますが、r12.0 SP3 ポリシー サーバはキー ロールオーバーに r12.0 SP3 キー ストアを使用できます。以下の図は、次のものを表しています。

- r6.x ポリシー ストアに接続する r6.x ポリシー サーバ。
- r12.0 SP3 ポリシー ストアに接続する r12.0 SP3 ポリシー サーバ。
- r6.x キー ストアに接続して新しいキーを取得する r6.x ポリシー サーバ。

- r12.0 SP3 キー ストアに接続して新しいキーを取得する r12.0 SP3 ポリシー サーバ。
- 管理 UI を使用して各キー ストアの静的エージェントおよびセッション キーを設定する SiteMinder 管理者。

  重要: すべてのキー ストアで同じエージェントとセッション キーが使用されるわけではない場合、シングル サインオンに失敗します。
- 対応する r6.x ポリシー サーバをポーリングして新しいキーを取得する r6.x Web エージェント。
- 対応する r12.0 SP3 ポリシー サーバをポーリングして新しいキーを取得する r12.0 SP3 Web エージェント。

注: 図には示されていませんが、ポリシーストアとストアデータは、フェイルオーバーのために複製することができます。データベースまたはディレクトリ サーバのタイプにより、データの複製方法が決まります。マスタ/スレーブ環境でのキー管理の詳細については、「ポリシー サーバ管理ガイド」を参照してください。データの複製の詳細については、使用しているベンダーから発行されたマニュアルを参照してください。



r12.0 SP3 環境の作成

既存の環境から独立した r12.0 SP3 環境を設定できます。r12.0 SP3 コンポーネントを以下の順序でインストールして設定します。

1. 1 つ以上のポリシー サーバ。

   重要 共通キー ストアを使用してシングル サインオンを維持する場合、すべてのポリシー サーバが同じ暗号化キーを使用する必要があります。暗号化キーの値がわからない場合、ポリシー ストアの r6.x 値をリセットできます。r12.0 SP3 ポリシー サーバをインストールするときに新しい値を使用します。

   注: ポリシー ストア暗号化キーのリセットの詳細については、「ポリシー サーバ管理ガイド」を参照してください。

2. ポリシー ストア。
3. 管理 UI。
4. 1 つ以上の Web エージェント。
5. レポート サーバ

注: ポリシー サーバ、ポリシー ストア、管理 UI、およびレポート サーバのインストールの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。Web エージェントのインストールの詳細については、「*Web エージェント インストール ガイド*」を参照してください。

共通キー ストアのシングル サインオン要件

共通キー ストアを展開する場合は、以下の手順を実行します。実行しない場合、シングル サインオンに失敗します。

- r6.x ポリシーおよびキー ストアは必ず別個に設定してください。

  注: キー ストアの設定の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

- キー ストアのバージョンを r6.x のままにします。r12.0 SP3 ポリシー サーバは r6.x キー ストアと通信できますが、r6.x ポリシー サーバは r12.0 SP3 キー ストアと通信できません。
- すべてのポリシー サーバが共通の r6.x ポリシーストアを使用するように設定します。

- すべてのポリシー サーバが必ず同じ暗号化キーを使用するようにしてください。暗号化キーの値がわからない場合、ポリシー ストアの r6.x 値をリセットできます。r12.0 SP3 ポリシー サーバをインストールするときに新しい値を使用します。

  注: ポリシー ストア暗号化キーのリセットの詳細については、「ポリシー サーバ管理ガイド」を参照してください。

- 1 つのポリシー サーバを指定して、動的なエージェント キーを生成します。残りのポリシー サーバのエージェント キー生成を無効にします。

  注: エージェント キーの動的な生成の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

複数キー ストアのシングル サインオン要件

複数キー ストアを展開する場合は、以下の手順を実行します。実行しない場合、シングル サインオンに失敗します。

- すべてのポリシー サーバの動的エージェント キー生成を無効にします。
- SiteMinder 管理者が、必要なポリシー サーバ ユーザ インターフェースと、r6.x および r12.0 SP3 キー ストアで同じ静的エージェント キーと同じセッション チケットを指定する 管理 UI アクセス権を持っているようにしてください。

  注: 管理者権限の委任の詳細については、「ポリシー サーバ設定ガイド」を参照してください。

- **重要** r6.x および r12.0 SP3 キー ストアで同じ静的エージェント キーと同じセッション チケットが設定されるようにしてください。

  注: 静的エージェント キーとセッション チケットの設定の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

r6.x ポリシーの移行

r12.0 SP3 展開を使用して r6.x リソースを保護する予定の場合、ポリシー ストア データを r12.0 SP3 ポリシー ストアに移行することをお勧めします。

必須ではありませんが、r12.0 SP3 ポリシー ストアの管理を開始する前にポリシー ストア データを移行した場合、重複するオブジェクトに関連する競合の可能性を回避できます。

ポリシーを移行する方法

1. 以下のいずれかの操作を行います。
   - r6.x 環境でエンタープライズ ポリシー管理アプリケーションを使用している場合は、r6.x バージョンの XPSExport ユーティリティを使用して r6.x ポリシー ストア データをエクスポートします。
   - r6.x 環境でエンタープライズ ポリシー管理アプリケーションを使用していない場合は、r6.x バージョンの smobjimport ユーティリティを使用して r6.x ポリシー ストア データをエクスポートします。

   注: r6.x バージョンの smobjimport ユーティリティの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。r6.x バージョンの XPSExport ユーティリティの詳細については、「ポリシー サーバ管理ガイド」を参照してください。

2. 以下のいずれかの操作を行います。

   - r6.x 環境でエンタープライズ ポリシー管理アプリケーションを使用している場合は、r12.0 SP3 バージョンの XPSImport ユーティリティを使用して r12.0 SP3 ポリシー ストア データをインポートします。
   - r6.x 環境でエンタープライズ ポリシー管理アプリケーションを使用していない場合は、r12.0 SP3 バージョンの smobjimport ユーティリティを使用して r12.0 SP3 ポリシー ストア データをインポートします。

   注: r12.0 SP3 バージョンの smobjimport ユーティリティと XPSImport ユーティリティの詳細については、「ポリシー サーバ管理ガイド」を参照してください。

アップグレードまたはポリシー移行の一環として SiteMinder ポリシーをある環境から別の環境に移動させる場合、環境に固有の一部のオブジェクトがエクスポート ファイルに含まれます。これらのオブジェクトにはたとえば以下のものがあります。

- トラステッド ホスト
- HCO ポリシー サーバ設定
- 認証方式 URL
- パスワード サービス リダイレクト
- リダイレクト レスポンス

XPSExport を使用するときに選択したモードによって、これらのオブジェクトは新しい環境に追加されるか、または既存の設定を上書きします。オブジェクトをインポートする際は、環境設定を誤って変更することがないよう注意が必要です。

注: エクスポートの XPSExport モードの詳細については、ポリシー サーバ管理ガイド を参照してください。

ユーザ ディレクトリのシングル サインオン要件

両方の環境で作成する SiteMinder ユーザ ディレクトリ オブジェクトが同じ名前になるようにしてください。異なる名前を使用して r6.x および r12.0 SP3 ポリシー サーバを同じユーザ ストアにポイントした場合、シングル サインオンに失敗します。

第 3 章: r12.x からのアップグレード

このセクションには、以下のトピックが含まれています。

サポートされているアップグレード パス

アップグレードは、既存の SiteMinder 環境への r12.0 SP3 コンポーネントの展開で構成されます。r12.0 SP3 へのアップグレードすは、以下の 2 つの方法で実行できます。

- 移行を完了する。
- 既存の環境と並行する r12.0 SP3 環境を設定する。どちらの環境でも、1 つ以上のキー ストアを使用してシングル サインオンが維持されます。

r12.0 からアップグレードする場合、サポートされるアップグレード パスは並行アップグレードのみです。r12.0 SP1 以降からアップグレードする場合、どちらのアップグレード パスもサポートされます。

詳細情報:

移行 (P. 14)
並行アップグレード (P. 15)

移行に関する考慮事項

r12.0 SP1 以降から移行する場合は、移行の開始前に以下の点を考慮します。

ポリシー サーバ オプション パックのサポート

r12.0 SP1 からは、PSOP（Policy Server Option Pack、ポリシー サーバ オプション パック）に関連する機能は核となるポリシー サーバ機能と見なされるようになりました。PSOP 機能を使用する r12.0 SP1 環境を移行する場合は、以下の点を考慮します。

- PSOP には、個別のアップグレードは必要なくなりました。PSOP は、ポリシー サーバのアップグレード時にアップグレードされます。
- オプション パック機能が必要な r12.x エージェントは、r12.0 SP3 WAOP（Web Agent Option Pack、Web エージェント オプション パック）をインストールする前に r12.0 SP3 にアップグレードする必要があります。

注: Web エージェントのアップグレードの詳細については、「*Web エージェント インストール ガイド*」を参照してください。WAOP のインストールの詳細については、「*Web Agent Option Pack Guide*」を参照してください。

ポリシー サーバ オプション パック機能の管理

2 つのグラフィカル ユーザ インターフェース（GUI）を使用して、特定の SiteMinder ポリシー オブジェクトを管理できます。以下の点について考慮してください。

- **SiteMinder 管理 UI**（管理 UI）- 管理 UI は、ポリシー サーバから独立してインストールされる Web ベースの管理コンソールです。管理 UI は、認証および許可ポリシー、EPM（Enterprise Policy Management ）、レポートおよびポリシー分析のようなアクセス制御に関連するほとんどのタスクを設定するためのツールです。

  Federation セキュリティ サービス に関連するオブジェクトを除くすべてのポリシー サーバ オブジェクトを表示、変更、および削除するには、管理 UI を使用します。フェデレーション関連の設定タスクはすべて FSS 管理 UI を使用して管理できます。

- **SiteMinder Federation セキュリティ サービスの管理 UI**（FSS 管理 UI）- FSS 管理 UI は、ポリシー サーバと同時にインストールされるアプレットベースのアプリケーションです。Federation セキュリティ サービス コンポーネントは、アフィリエイト（コンシューマ、サービス プロバイダ、リソース パートナー）と、2 つのパートナー間のフェデレーション通信をサポートするために設定する SAML 認証方式で構成されます。

  FSS 管理 UI は、SiteMinder Federation セキュリティ サービス を管理するために用意されています。以前のバージョンの SiteMinder ポリシー サーバのユーザ インターフェースと異なり、すべての SiteMinder オブジェクトが FSS 管理 UI に表示されることがわかります。表示されないオブジェクトは、EPM（Enterprise Policy Management）およびレポートに関連するオブジェクトだけです。FSS 管理 UI を使用すると、SiteMinder オブジェクトを管理できます。FSS 管理 UI を使用しているときに情報が必要となった場合は、FSS 管理 UI オンライン ヘルプ システムを調べます。

Federation セキュリティ サービス コンポーネント

r12.0 SP1 環境を移行する場合で、Federation セキュリティ サービス の使用を予定している場合は、以下の点を考慮します。

- SiteMinder キー データベース（smkeydatabase）は、必須のコンポーネントです。ポリシー サーバのアップグレード時に、キー データベースを作成できます。ポリシー サーバをアップグレードした後、ポリシー サーバ設定ウィザードを使用して、キー データベースを作成することもできます。

  注: フェデレーション環境でキー データベースが果たす役割の詳細については、「*Federation Security Services Guide*」を参照してください。

- 登録された FSS 管理 UI は、必須のコンポーネントです。FSS 管理 UI は、核となる r12.0 SP1 環境の一部ですが、使用するにはポリシー サーバに登録する必要があります。SiteMinder Federation セキュリティ サービス を管理する予定の場合は、ポリシー ストアおよび 管理 UI のアップグレード後に FSS 管理 UI を登録します。

- フェデレーション環境を展開するには、追加の SiteMinder コンポーネントが必要です。

  注: 必要な Federation セキュリティ サービス コンポーネントの詳細については、「*Federation Security Services Guide*」を参照してください。

管理 UI アップグレード オプション

このリリースでは、簡略化された 管理 UI インストールが導入されました。これには、組み込みオブジェクト ストアおよび組み込み SiteMinder 管理 UI サービス（JBoss）が含まれています。r12.0 SP3 に移行する場合、管理 UI をアップグレードする以下の 2 つのオプションがあります。

- r12.0 SP1/r12.0 SP2 の 管理 UI を r12.0 SP3 にアップグレードできます。管理 UI をアップグレードした場合、引き続き以下のものを使用できます。
  - 既存の外部オブジェクト ストア。
  - 既存の外部管理者ユーザ ストア。
  - 既存のポリシー サーバ接続。
  - 管理 UI にアクセスする既存の URL。

  注: 管理 UI のアップグレードの詳細については、「r12.x から移行する方法」を参照してください。
- 既存の 管理 UI をアンインストールし、スタンドアロン インストール オプションを使用して r12.0 SP3 管理 UI をインストールできます。r12.0 SP3 管理 UI をインストールした場合、次のものを使用します。
  - 外部オブジェクト ストアの代わりに組み込みオブジェクト ストア。r12.0 SP3 管理 UI では、外部オブジェクト ストアが必要ありません。
  - 既存のアプリケーション サーバ インフラストラクチャの代わりに埋め込みアプリケーション サーバ。
  - 既存の外部管理者ユーザ ストアへの接続を設定する管理認証ウィザード。
  - 管理 UI にアクセスする新しい URL。r12.0 SP3 URL は //*host*:*port*/iam/siteminder/adminui です。

  注: r12.0 SP1/r12.0 SP2 管理 UI のアンインストールの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。管理 UI のインストールの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。外部管理者ユーザ ストアへの接続の設定の詳細については、「ポリシー サーバ設定ガイド」を参照してください。

シングル サインオン

r12.0 SP3 への移行時に、シングル サインオンを維持できます。以下の点について考慮してください。

- r12.0 SP3 ポリシー サーバは、r12.0 SP1/r12.0 SP2 ポリシー ストア、および r12.0 SP1/r12.0 SP2 キー ストアと通信できます。
- r12.0 SP3 ポリシー サーバは、r12.0 SP1/r12.0 SP2 セッション ストアと通信できます。

ポリシー ストア破損の回避

ポリシー ストア破損を回避するためポリシー ストアをホストしているサーバが、UTF-8 形式でオブジェクトを格納するように設定してください。

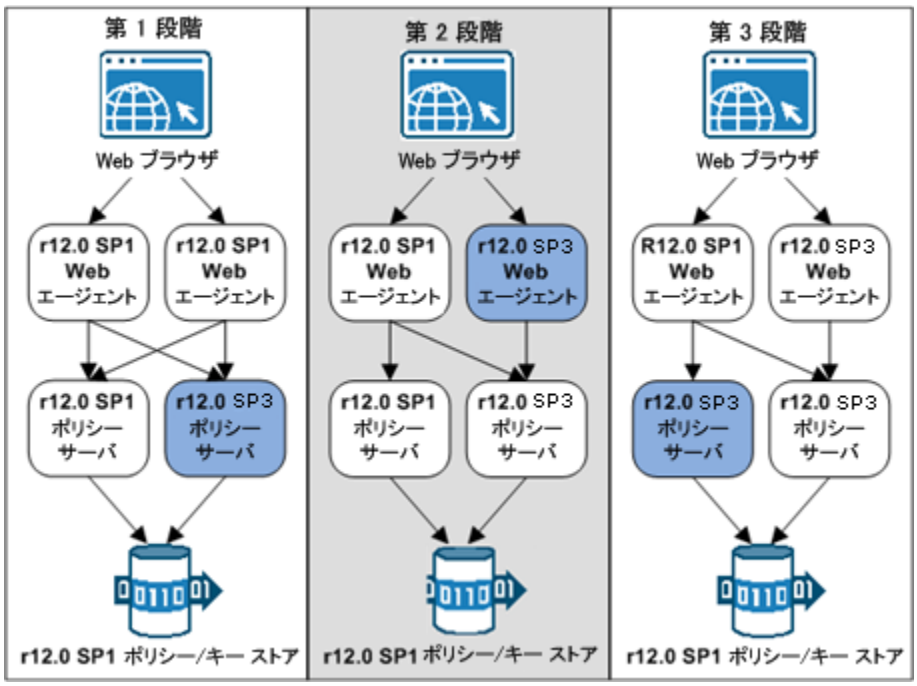
注: UTF-8 形式でオブジェクトを格納するサーバ設定の詳細については、使用しているベンダーから発行されたマニュアルを参照してください。

r12.x の移行の仕組み

複数のポリシー サーバおよび Web エージェントが存在する SiteMinder 展開を移行するには、SiteMinder 環境からポリシー サーバおよび Web エージェントのうち 1 つを削除します。これらのコンポーネントはアップグレードされますが、残りのポリシー サーバおよび Web エージェントはリソースを保護し続行けます。すべてのコンポーネントがアップグレードされるまで SiteMinder コンポーネントの削除およびアップグレードを続行するか、互換性のある混在モードで動作を続行します。

以下の図は、単純な r12.0 SP1 環境を示しており、既存のコンポーネントがアップグレードされる順序を詳細に示しています。

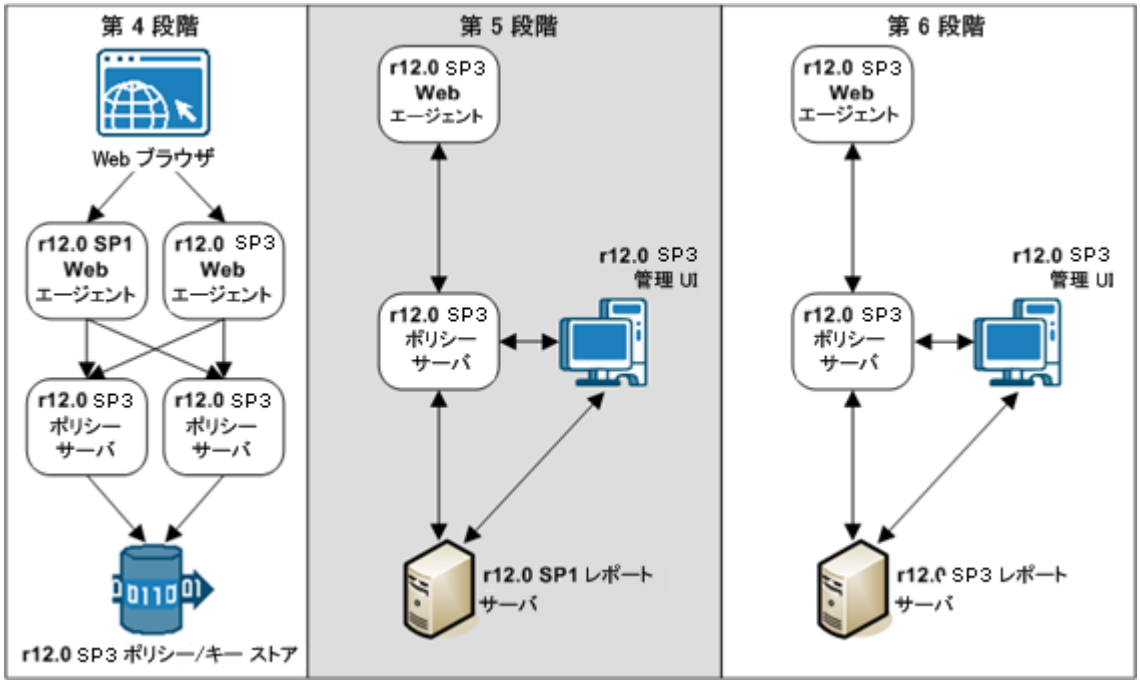
注: 図はそれぞれ 1 つのポリシー/キー ストアを示しています。環境では、別個のポリシーおよびキー ストアを使用できます。それぞれの図は r12.0 SP1 コンポーネントを示します。r12.0 SP1 以降からの移行がサポートされています。



1. 第 1 段階では、r12.0 SP1 ポリシー サーバがアップグレードされます。r12.0 SP3 ポリシー サーバは互換モードで動作します。以下の点について考慮してください。

   - r12.0 SP1 Web エージェントは、r12.0 SP3 ポリシー サーバと通信し続けます。
   - r12.0 SP3 ポリシー サーバは、r12.0 SP1 ポリシーおよびキー ストアと通信し続けます。
   - r12.0 SP1 ポリシー サーバは、r12.0 SP1 ポリシーおよびキー ストアと通信し続けます。
   - r12.0 SP1 管理 UI が r12.0 SP3 ポリシー サーバを使用して設定される場合、管理 UI はポリシー サーバと通信して、r12.0 SP1 ポリシー ストアのオブジェクトを管理し続けます。
   - r12.0 SP1 レポート サーバが r12.0 SP3 ポリシー サーバを使用して設定される場合、レポート サーバはレポートを作成し続けます。

2. 第 2 段階では、r12.0 SP1 Web エージェントが r12.0 SP3 にアップグレードされます。
   - r12.0 SP1 Web エージェントは、r12.0 SP1 および r12.0 SP3 ポリシー サーバと通信し続けます。
   - r12.0 SP3 Web エージェントは、r12.0 SP3 ポリシー サーバのみと通信します。
3. 第 3 段階では、残りのポリシー サーバが r12.0 SP3 にアップグレードされます。r12.0 SP3 ポリシー サーバは、r12.0 SP1 ポリシーおよびキー ストアとの互換モードで動作します。



4. 第 4 段階では、r12.0 SP1 ポリシーおよびキー ストアが r12.0 SP3 にアップグレードされます。
5. 第 5 段階では、管理 UI がアップグレードされます。
6. 第 6 段階では、r12.0 SP1 レポート サーバがアンインストールされます。r12.0 SP3 レポート サーバがインストールされ、ポリシー サーバに登録され、管理 UI に接続されます。

r12.x から移行する方法

r12.0 SP1 または r12.0 SP2 から r12.0 SP3 に移行するには、以下の手順を実行します。

1. 「ポリシー サーバのアップグレード前の確認事項」の内容を確認します。
2. r12.x ポリシー サーバを r12.0 SP3 にアップグレードします。
3. r12.x Web エージェントを r12.0 SP3 にアップグレードします。
4. 残りの r12.x ポリシー サーバおよび Web エージェントをそれぞれ r12.0 SP3 にアップグレードします。
5. r12.x ポリシーおよびキー ストアを r12.0 SP3 にアップグレードします。
6. r12.x 管理 UI をアップグレードします。
7. 必要に応じて、管理 UI を使用して既存のレポートをローカルに保存し、r12.x レポート サーバおよびレポート データベースを環境から削除します。r12.0 SP3 レポーティング環境を構築する最もシンプルな方法は、新しいレポート サーバおよびレポート データベースをインストールして設定することです。

重要: r12.0 SP2 以前のリリースからの移行は、サポートされるアップグレード パスではありません。r12.0 SP2 以前のリリースからアップグレードしている場合は、並列の環境を設定してください。

r12.x ポリシー サーバのアップグレード

以下のセクションでは、Windows および UNIX 上の r12.0 SP1/r12.0 SP2 ポリシー サーバをアップグレードする方法について詳述します。

アップグレード前の注意事項

ポリシー サーバをアップグレードする前に、以下の点を考慮します。

- テクニカル サポート サイトのインストール メディアを使用して、ポリシー サーバをアップグレードします。

  注: オペレーティング システムごとのインストール メディア名のリストについては、「*Policy Server Release Notes*」のインストールおよびアップグレードの考慮事項を参照してください。

- (Linux) 必要な Linux ライブラリがポリシー サーバのホスト システムにインストールされていることを確認します。詳細については、Required Linux Libraries を参照してください。

- 5.1 Sun ONE ディレクトリ サーバとポリシー サーバが同じ Windows 2003 システムにインストールされている場合、LDAP SDK を 5.0.8 (2002 年 7 月 17 日付) 以降にアップグレードします。 LDAP SDK のアップグレードに失敗すると、ポリシー サーバが不安定になります。

  注: LDAP SDK は、Sun ONE ディレクトリ サーバを使用しているかどうかにかかわらずアップグレードしてください。

- ポリシー サーバを環境から削除します。ポリシー サーバを削除すると、アップグレード中に Web エージェントがポリシー サーバに接続することがなくなります。

- ポリシー サーバ管理コンソールのすべてのインスタンスをシャットダウンします。

- (UNIX) アクセス権によっては、以下のコマンドを実行することでインストール メディアへの実行アクセス権を追加する必要があります。

  ```
  chmod +x installation_media
  ```

  installation_media

  ポリシー サーバのインストール実行可能ファイルを指定します。

- (UNIX) 別のサブネットにまたがってポリシー サーバを実行した場合、クラッシュすることがあります。ポリシー サーバ インストーラは、ホスト システム上で直接実行してください。

- (UNIX) 少なくともポリシー サーバをインストールしたユーザと同じアクセス権を持つアカウントを使用すてポリシー サーバをアップグレードします。たとえば、root ユーザがポリシー サーバをインストールした場合は、root ユーザを使用してポリシー サーバをアップグレードします。
- ドキュメントをインストールします。SiteMinder ドキュメントは、ポリシー サーバと同時にはインストールされません。ポリシー サーバをアップグレードする前にドキュメントをインストールすることをお勧めします。

注: r6.0 SP6 および r12.0 SP2 のマニュアル選択メニューはテクニカル サポート サイトで提供されています。これらのバージョン用のインストール キットもありますが、ドキュメントのインストールは必須ではありません。マニュアル選択メニューはテクニカル サポート サイトから表示およびダウンロードできます。

詳細情報:

インストール メディアの検索 (P. 156)
SiteMinder のドキュメント (P. 9)

必要とされる Linux ライブラリ

このコンポーネントの Linux バージョンをインストールまたはアップグレードしている場合、ホスト システム上で以下が必要になります。

`compat-libstdc++-33.3.2.3-`*`patch_version`*`.i386.rpm`

この rpm をインストールして、お使いのオペレーティング システム用の適切な 32 ビット C ランタイム ライブラリが使用できることを確認してください。

Windows

ポリシー サーバをアップグレードする方法

1. 実行中のすべてのアプリケーションを終了します。
2. インストール メディアに移動します。
3. *installation_media* をダブルクリックします。

   installation_media

   ポリシー サーバのインストール実行可能ファイルの名前を指定します。

   ポリシー サーバ インストーラが起動します。

   注: オペレーティング システムごとのインストール メディア名のリストについては、「*Policy Server Release Notes*」のインストールおよびアップグレードの考慮事項を参照してください。

4. インストーラを実行するときは、以下の点を考慮します。

   - インストーラにより、コンポーネントの選択が求められます。コンポーネントを選択する場合
     - 以前に環境に設定されたコンポーネントを再設定します。必ず、対応するコンポーネントを選択してください。
     - 新しいポリシーストアを設定する予定でない場合は、ポリシー ストアのチェック ボックスをオフにします。既存のポリシー ストア設定を再設定する必要はありません。アップグレード後も、ポリシー サーバにポリシー ストア設定が保持されます。既存のポリシー ストアを手動でアップグレードします。
   - 以下の場合は、SM キー データベースの作成/SM キー データベース パスワードの変更のチェック ボックスをオンにします。
     - Federation セキュリティ サービス に関連する機能の使用を計画している。
     - SiteMinder Information Card 認証方式の使用を計画している。たとえば、Microsoft CardSpace をサポートするために SiteMinder Information Card 認証方式を使用できます。

   注: SiteMinder キー データベースを作成した場合、インストーラによりデフォルト CA 証明書のインストールが求められます。CA のデフォルト証明書をインポートのチェック ボックスをオンのままにし、証明書をインストールします。アップグレード後、追加の証明書および秘密キーをキー データベースに追加できます。

5. インストール設定を確認し、[インストール]をクリックします。

   ポリシー サーバがアップグレードされます。選択したコンポーネントは、ポリシー サーバで使用できるように設定されます。

アップグレード中に問題が発生した場合、*siteminder_home*\siteminder\install_config_info にポリシー サーバのインストール ログ ファイルがあります。

siteminder_home

ポリシー サーバのインストール パスを指定します。

UNIX GUI

ポリシー サーバをアップグレードする方法

1. 実行中のすべてのアプリケーションを終了します。
2. SiteMinder インストール ディレクトリから ksh シェルで以下のスクリプトを実行します。

   ```
   ../ca_ps_env.ksh
   ```

   注: スクリプトを実行するときは、ピリオドの間にスペース を入れてください (. .)。
3. シェルを開き、インストール実行可能ファイルに移動します。
4. 以下のコマンドを入力します。

   ```
   ./installation_media gui
   ```

   installation_media

   ポリシー サーバのインストーラ実行可能ファイルの名前を指定します。

   ポリシー サーバ インストーラが起動します。

   注: オペレーティング システムごとのインストール メディア名のリストについては、「*Policy Server Release Notes*」のインストールおよびアップグレードの考慮事項を参照してください。
5. インストーラを実行するときは、以下の点を考慮します。
   - インストーラにより、コンポーネントの選択が求められます。コンポーネントを選択する場合
     - 以前に環境に設定されたコンポーネントを再設定します。必ず、対応するコンポーネントを選択してください。
     - 新しいポリシーストアを設定しない場合は、ポリシー ストアのチェックボックスをオフにします。既存のポリシー ストア設定を再設定する必要はありません。アップグレードされたポリシー サーバに、ポリシー ストア設定が保持されます。既存のポリシー ストアを手動でアップグレードします。

- 以下の場合は、SM キー データベースの作成/SM キー データベース パスワードの変更のチェック ボックスをオンにします。
  - Federation セキュリティ サービス に関連する機能の使用を計画している。
  - SiteMinder Information Card 認証方式の使用を計画している。たとえば、Microsoft CardSpace をサポートするために SiteMinder Information Card 認証方式を使用できます。

注: キー データベースを作成した場合、インストーラによりデフォルト CA 証明書のインストールが求められます。CA のデフォルト証明書をインポートのチェック ボックスをオンのままにし、証明書をインストールします。アップグレード後、追加の証明書および秘密キーをキー データベースに追加できます。

6. インストール設定を確認し、[インストール]をクリックします。

   ポリシー サーバがアップグレードされます。選択したコンポーネントは、ポリシー サーバで使用できるように設定されます。

アップグレード中に問題が発生した場合、*siteminder_home*\siteminder\install_config_info にポリシー サーバのインストール ログ ファイルがあります。

siteminder_home

ポリシー サーバのインストール パスを指定します。

UNIX コンソール

ポリシー サーバをアップグレードする方法

1. 実行中のすべてのアプリケーションを終了します。
2. SiteMinder インストール ディレクトリから ksh シェルで以下のスクリプトを実行します。

   ```
   ../ca_ps_env.ksh
   ```

   注: スクリプトを実行するときは、ピリオドの間にスペース を入れてください (. .)。

3. シェルを開き、インストール実行可能ファイルに移動します。
4. 以下のコマンドを入力します。

   ```
   ./installation_media -i console
   ```

   installation_media

   ポリシー サーバのインストーラ実行可能ファイルの名前を指定します。

   ポリシー サーバ インストーラが起動します。

   注: オペレーティング システムごとのインストール メディア名のリストについては、「*Policy Server Release Notes*」のインストールおよびアップグレードの考慮事項を参照してください。

5. インストーラを実行するときは、以下の点を考慮します。

   - インストーラにより、SiteMinder コンポーネントの選択が求められます。各コンポーネントには、数字のプレフィックスが付きます。1 つ以上のコンポーネントを選択するため、数字をカンマ(,)で区切って入力します。どの機能も選択しない場合は、カンマのみを入力します。コンポーネントを選択する場合
   - 以前に環境に設定されたコンポーネントを再設定します。必ず、対応するコンポーネントを選択してください。
   - 新しいポリシーストアを設定する場合は、ポリシー ストアのみ選択します。既存のポリシー ストア設定を再設定する必要はありません。アップグレードされたポリシー サーバに、ポリシー ストア設定が保持されます。既存のポリシー ストアを手動でアップグレードします。
   - 以下の場合は、SM キー データベースの作成/SM キー データベース パスワードの変更のチェック ボックスをオンにします。
     - Federation セキュリティ サービス に関連する機能の使用を計画している。
     - SiteMinder Information Card 認証方式の使用を計画している。たとえば、Microsoft CardSpace をサポートするために SiteMinder Information Card 認証方式を使用できます。

   注: キー データベースを作成した場合、インストーラによりデフォルト CA 証明書のインストールが求められます。CA のデフォルト証明書をインポートのチェック ボックスをオンのままにし、これらの証明書をインストールします。アップグレード後、追加の証明書および秘密キーをキー データベースに追加できます。

6. インストール設定を確認し、Enter キーを押します。

   ポリシー サーバがアップグレードされます。選択したコンポーネントは、ポリシー サーバで使用できるように設定されます。

アップグレード中に問題が発生した場合、*siteminder_home*\siteminder\install_config_info にポリシー サーバのインストール ログ ファイルがあります。

siteminder_home

ポリシー サーバのインストール パスを指定します。

r12.0 SP1 Web エージェントのアップグレード前の確認事項

Web エージェントをアップグレードする前に、以下の点を確認してください。

- （UNIX）Web エージェントのインストールに使用したのと同じアカウントを使用して、Web エージェントをアップグレードします。別のアカウントを使用した場合、アップグレードに失敗する場合があります。
- ポリシー サーバが設定されていることを確認します。
- 必要な管理者およびポリシー サーバ オブジェクト名を識別します。
- Web エージェント要件を識別します。

ポリシー サーバが設定されていることを確認します。

Web エージェントをアップグレードする前に、以下の手順を実行します。

- ポリシー サーバが、Web エージェント ホスト システムに接続できることを確認します。
- トラステッド ホストを登録する前に、ポリシー サーバが実行されていることを確認します。ポリシー サーバ管理コンソールの[ステータス]タブでポリシー サーバを起動します。

必要な管理者名およびポリシー サーバ オブジェクト名の識別

Web エージェントをアップグレードするには、ポリシー サーバ管理者から以下の情報を入手必要があります。

- ホストの登録権限を持つ SiteMinder 管理者の名前。
- ホスト設定オブジェクトの名前。
- エージェント設定オブジェクトの名前。

Web エージェントの要件の識別

パッチおよび他の Web エージェントの要件の詳細については、「*Web エージェント インストール ガイド*」を参照してください。

r12.x Web エージェントのアップグレード

r12.0 SP3 Web エージェント インストーラを使用して、Windows または UNIX 上の r12.0 SP1/r12.0 SP2 Web エージェントをアップグレードします。

注: オプション パック機能が必要なエージェントは、r12.0 SP3 Web エージェント オプション パックをインストールする前に r12.0 SP3 にアップグレードする必要があります。Web エージェントのアップグレードの詳細については、「*Web エージェント インストール ガイド*」を参照してください。Web エージェント オプション パックのインストールの詳細については、「*Web Agent Option Pack Guide*」を参照してください。

r12.x ポリシー ストアをアップグレードする方法

r12.0 SP1 または r12.0 SP2 ポリシー ストアを r12.0 SP3 にアップグレードするには、以下の手順を実行します。

1. ベース ポリシー ストア オブジェクトをインポートします。
2. ポリシー ストア データ定義をインポートします。

   注: ポリシー ストア データ定義に関連付けられたアップグレード ファイルはありません。各ファイルを再インポートして、データ定義をアップグレードします。

ベース ポリシー ストア オブジェクトのインポート

デフォルトの SiteMinder オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがアップグレードされます。デフォルトの SiteMinder オブジェクトは、ポリシー ストアにポリシー情報を格納するために必要です。

ベース ポリシー ストア オブジェクトをインポートするには、以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home\db\smdif\upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

upgrade_smdif_file_name

アップグレード ファイルの名前を指定します。

- sm_upgrade_R12sp1_to_R12sp3.smdif
- sm_upgrade_R12sp2_to_R12sp3.smdif

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト出力: stdout

-f

重複するポリシー ストア オブジェクトを、r12.0 SP3 のもので上書きします。

引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

Windows の例: smobjimport

```
-i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
-wPassword -v
```

UNIX の例: smobjimport

-i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v

ベース ポリシー ストア オブジェクトがインポートされます。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*\xps\dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。
2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

r12.x 管理 UI のアップグレード

以下のセクションでは、Windows と UNIX 上で 管理 UI をアップグレードする方法について詳述します。

重要: r12.0 からの 管理 UI のアップグレードはサポートされていません。

アップグレード前の注意事項

管理 UI をアップグレードする前に、以下の点を考慮します。

- テクニカル サポート サイトのインストール メディアを使用して、管理 UI をアップグレードします。

  注: オペレーティング システムごとのインストール メディア名のリストについては、「*Policy Server Release Notes*」のインストールおよびアップグレードの考慮事項を参照してください。

- (Linux) 必要な Linux ライブラリが 管理 UI ホスト システムにインストールされていることを確認します。詳細については、Required Linux Libraries を参照してください。

- **重要**: インストール zip には、インストール メディアと同じレベルに layout.properties ファイルおよび Framework フォルダが含まれています。インストール zip を展開した後にインストール メディアを移動した場合、以下のものを同じ場所に移動しないと、インストールに失敗します。

  - layout.properties ファイル
  - Framework フォルダ

- **重要**: (UNIX) アクセス権によっては、以下のコマンドを実行することでインストール メディアが存在するディレクトリへの実行アクセス権を追加する必要があります。

  ```
  chmod -R+x directory
  ```

  directory

  インストール メディアが存在するディレクトリを指定します。

- (UNIX) 別のサブネットにまたがって 管理 UI インストーラを実行した場合、クラッシュすることがあります。管理 UI インストーラは、ホスト システム上で直接実行してください。

詳細情報:

インストール メディアの検索 (P. 156)

必要とされる Linux ライブラリ

このコンポーネントの Linux バージョンをインストールまたはアップグレードしている場合、ホスト システム上で以下が必要になります。

```
compat-libstdc++-33.3.2.3-patch_version.i386.rpm
```

この rpm をインストールして、お使いのオペレーティング システム用の適切な 32 ビット C ランタイム ライブラリが使用できることを確認してください。

Windows

管理 UI をアップグレードする方法

1. 実行中のすべてのアプリケーションを終了します。
2. 管理 UI をホストしているアプリケーション サーバを停止します。

   注: アプリケーション サーバの停止の詳細については、r12.0 SP1 の「ポリシー サーバ インストール ガイド」を参照してください。

3. 管理 UI インストール実行可能ファイルに移動します。

   重要 インストール zip には、管理 UI 実行可能ファイルと同じレベルに layout.properties ファイルおよび Framework フォルダも含まれています。インストール zip を展開した後に 管理 UI 実行可能ファイルを移動した場合、以下のものを 管理 UI 実行可能ファイルと同じ場所に移動しないと、アップグレードに失敗します。

   - layout.properties ファイル
   - Framework フォルダ

4. *installation_media* をダブルクリックします。

   installation_media

   管理 UI インストール実行可能ファイルを指定します。

   注: オペレーティング システムごとのインストール メディア名のリストについては、「*Policy Server Release Notes*」のインストールおよびアップグレードの考慮事項を参照してください。

   管理 UI インストーラが起動します。

5. プロンプトに従って、インストーラが 管理 UI をアップグレードできることを確認します。

6. インストール設定を確認し、[インストール]をクリックします。

   インストーラにより、管理 UI がインストールされたことが確認されます。

7. 管理 UI をホストしているアプリケーション サーバを起動します。

   注: アプリケーション サーバの起動の詳細については、r12.0 SP1 の「ポリシー サーバ インストール ガイド」を参照してください。

   管理 UI がアップグレードされました。

UNIX GUI

管理 UI をアップグレードする方法

1. 実行中のすべてのアプリケーションを終了します。
2. 管理 UI をホストしているアプリケーション サーバを停止します。

   注: アプリケーション サーバの停止の詳細については、r12.0 SP1 の「ポリシー サーバ インストール ガイド」を参照してください。

3. シェルを開き、インストール実行可能ファイルに移動します。

   重要 インストール zip には、管理 UI 実行可能ファイルと同じレベルに layout.properties ファイルおよび Framework フォルダが含まれています。インストール zip を展開した後に 管理 UI 実行可能ファイルを移動した場合、以下のものを 管理 UI 実行可能ファイルと同じ場所に移動しないと、アップグレードに失敗します。

   - layout.properties ファイル
   - Framework フォルダ

4. 以下のコマンドを入力します。

   ```
   ./installation_media gui
   ```

   installation_media

   管理 UI インストール実行可能ファイルを指定します。

   インストーラが起動します。

   注: オペレーティング システムごとのインストール メディア名のリストについては、「*Policy Server Release Notes*」のインストールおよびアップグレードの考慮事項を参照してください。

5. プロンプトに従って、インストーラが 管理 UI をアップグレードできることを確認します。

6. インストール設定を確認し、[インストール]をクリックします。

   インストーラにより、管理 UI がインストールされたことが確認されます。

7. 管理 UI をホストしているアプリケーション サーバを起動します。

   注: アプリケーション サーバの起動の詳細については、r12.0 SP1 の「ポリシー サーバ インストール ガイド」を参照してください。

   管理 UI がアップグレードされました。

UNIX コンソール

管理 UI をアップグレードする方法

1. 実行中のすべてのアプリケーションを終了します。
2. 管理 UI をホストしているアプリケーション サーバを停止します。

   注: アプリケーション サーバの停止の詳細については、r12.0 SP1 の「ポリシー サーバ インストール ガイド」を参照してください。

3. シェルを開き、インストール実行可能ファイルに移動します。

   重要 インストール zip には、管理 UI 実行可能ファイルと同じレベルに layout.properties ファイルおよび Framework フォルダが含まれています。インストール zip を展開した後に 管理 UI 実行可能ファイルを移動した場合、以下のものを 管理 UI 実行可能ファイルと同じ場所に移動しないと、アップグレードに失敗します。

   - layout.properties ファイル
   - Framework フォルダ

4. 以下のコマンドを入力します。

   ```
   ./installation_media -i console
   ```

   installation_media

   管理 UI インストール実行可能ファイルを指定します。

   インストーラが起動します。

   注: オペレーティング システムごとのインストール メディア名のリストについては、「*Policy Server Release Notes*」のインストールおよびアップグレードの考慮事項を参照してください。

5. プロンプトに従って、インストーラが 管理 UI をアップグレードできることを確認します。

6. インストール設定を確認し、Enter キーを押します。

   インストーラにより、管理 UI がインストールされたことが確認されます。

7. 管理 UI をホストしているアプリケーション サーバを起動します。

   注: アプリケーション サーバの起動の詳細については、r12.0 SP1 の「ポリシー サーバ インストール ガイド」を参照してください。

   管理 UI がアップグレードされました。

r12.x レポート サーバのアップグレード

r12.0 SP3 レポーティング環境を構築する最もシンプルな方法は、r12.x レポート環境をアンインストールし、r12.0 SP3 レポート コンポーネントをインストールして設定することです。

レポート サーバは、ポリシー ストアおよび SiteMinder 監査データベース内のデータを使用して、ポリシー分析および監査ベースのレポートをまとめます。レポート データベースには、これらのレポートで必要とされる情報は含まれません。そのため、r12.x レポート データベースから r12.0 SP3 レポート データベースへの移行は必要ありません。

以下の手順に従って、r12.0 SP3 レポート コンポーネントをインストールおよび設定します。

1. (オプション) 既存のレポートをエクスポートします。

   重要: 既存のレポートはレポート データベースに格納されています。既存のレポートを履歴目的で保存しておく必要がある場合は、管理 UI を使用してレポートを表示し、一時的な場所にそれらをエクスポートします。レポートの表示の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

2. レポート サーバと 管理 UI の間の接続を削除します。

   注: 詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

3. r12.x レポート サーバをアンインストールします。

   注: 詳細については、r12 SP2 の「ポリシー サーバ インストール ガイド」を参照してください。レポート サーバをアンインストールしてもレポート データベース内のテーブルは削除されません。レポート データベースにアクセスし、すべてのテーブルを手動で削除します。

4. r12.0 SP3 レポートをインストールおよび設定します。これには以下が含まれます。

   a. レポート サーバのインストール。

   b. SiteMinder レポート テンプレートのインストール。

   c. レポート サーバの登録。

   d. レポート サーバと SiteMinder 監査データベースの間の接続の設定。

   注: 詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

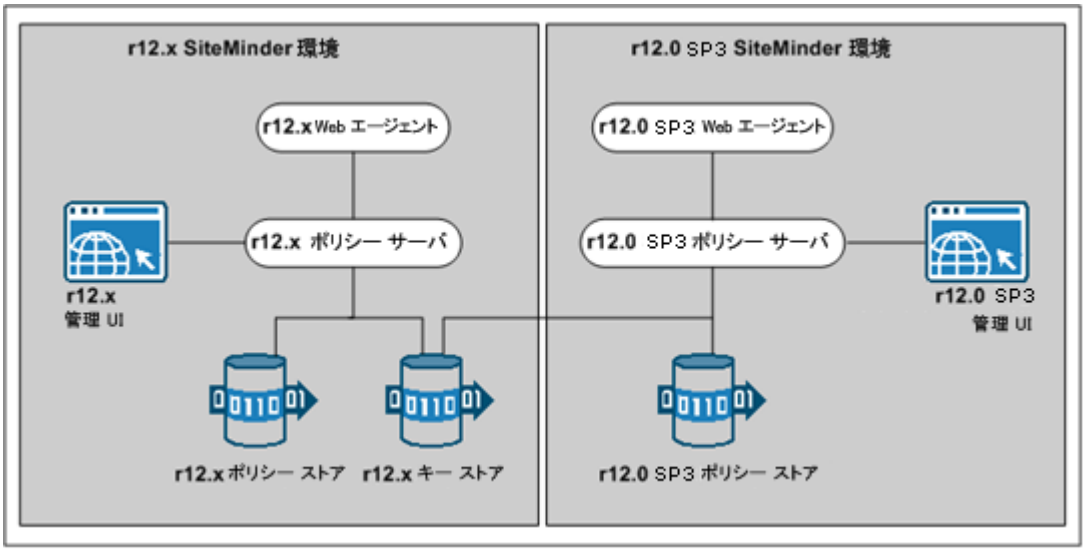
並行アップグレードの仕組み

既存の r12.x 環境を r12.0 SP3 に移行する必要はありません。むしろ、既存の展開の並行 r12.0 SP3 環境を設定できます。

以下の図は、単純な並列アップグレードおよび詳細を示しています。

- 既存のリソースの保護を続行する r12.x 環境。
- r12.x ポリシー ストアの SiteMinder オブジェクトの管理に使用される r12.x 管理 UI。
- 新しいリソースを保護する r12.0 SP3 環境。
- r12.0 SP3 ポリシー ストアの SiteMinder オブジェクトの管理に使用される r12.0 SP3 管理 UI。
- 共通 r12.x キー ストア。共通キー ストアにより、両方の環境でシングル サインオンが有効になります。

  注: 図には示されまていませんが、複数のキー ストアを使用して両方の環境でシングル サインオンを有効にできます。



並行環境を設定する方法

並行環境を設定するには、以下の手順を実行します。

1. 並行環境のキー管理オプションを確認して、シングル サインオンを実装する方法を調べます。
2. r12.0 SP3 環境を作成します。
3. 以下のいずれかの操作を行います。
   - 両方の環境が共通キー ストアのシングル サインオン要件を満たすようにしてください。
   - 両方の環境が複数キー ストアのシングル サインオン要件を満たすようにしてください。
4. （オプション）r12.x ポリシー ストア データを移行します。
5. ユーザ ディレクトリのシングル サインオン要件を確認します。

並行環境のキー管理オプション

並行アップグレードを成功させるには、SiteMinder キーを管理して既存の環境と r12.0 SP3 環境の間でシングル サインオンを維持する必要があります。2 つの SiteMinder キー管理オプションを使用できます。展開するオプションは、両方の環境間で 1 つ以上のキー ストアを実装する方法によって決まります。オプションは、以下のとおりです。

- 共通のキーストアがある複数のポリシーストア
- 個別のキーストアがある複数のポリシーストア

共通キー ストアの展開

すべてのポリシー サーバは、キー ロールオーバーに 1 つのキー ストアを使用できます。以下の図は、次のものを表しています。

- r12.x ポリシー ストアに接続する r12.x ポリシー サーバ。
- r12.0 SP3 ポリシー ストアに接続する r12.0 SP3 ポリシー サーバ。
- すべてのポリシー サーバのキー データを維持する共通 r12.x キー ストア。共通キー ストアを使用すると、すべてのポリシー サーバに関連付けられたエージェントでキーを共有できます。キーを共有すると、両方の環境間でシングル サインオンが有効になります。

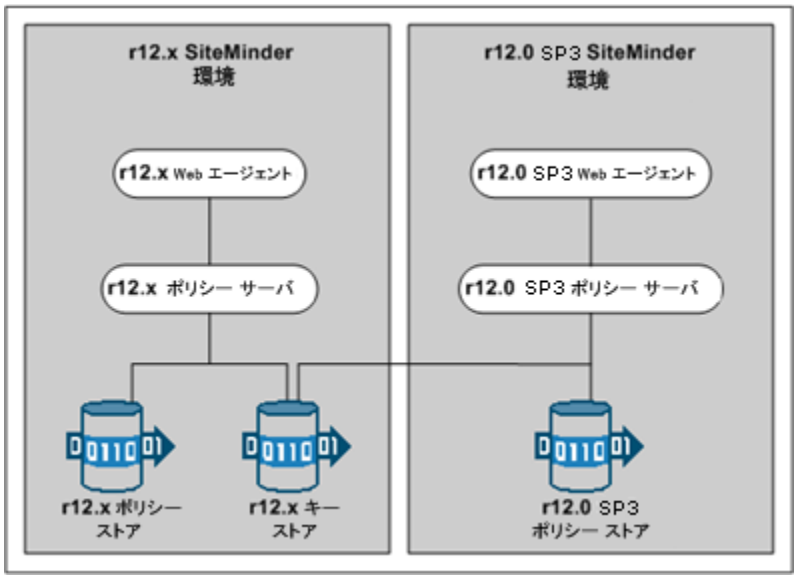
  重要: r12.x キー ストアは、r12.x ポリシー ストアとは別個に設定する必要があります。

- 共通キー ストアに接続して新しいキーを取得するすべてのポリシー サーバ。

  重要: r12.0 SP3 ポリシー サーバは、r12.x キー ストアを使用して設定する必要があります。r12.x ポリシー サーバは、r12.0 SP3 キー ストアと通信できません。

- 対応するポリシー サーバをポーリングして新しいキーを取得するすべての Web エージェント。

注: 図には示されていませんが、ポリシーストアとストアデータは、フェイルオーバーのために複製することができます。データベースまたはディレクトリ サーバのタイプにより、データの複製方法が決まります。マスタ/スレーブ環境でのキー管理の詳細については、「ポリシー サーバ管理ガイド」を参照してください。 データの複製の詳細については、使用しているベンダーから発行されたマニュアルを参照してください。



複数キー ストアの展開

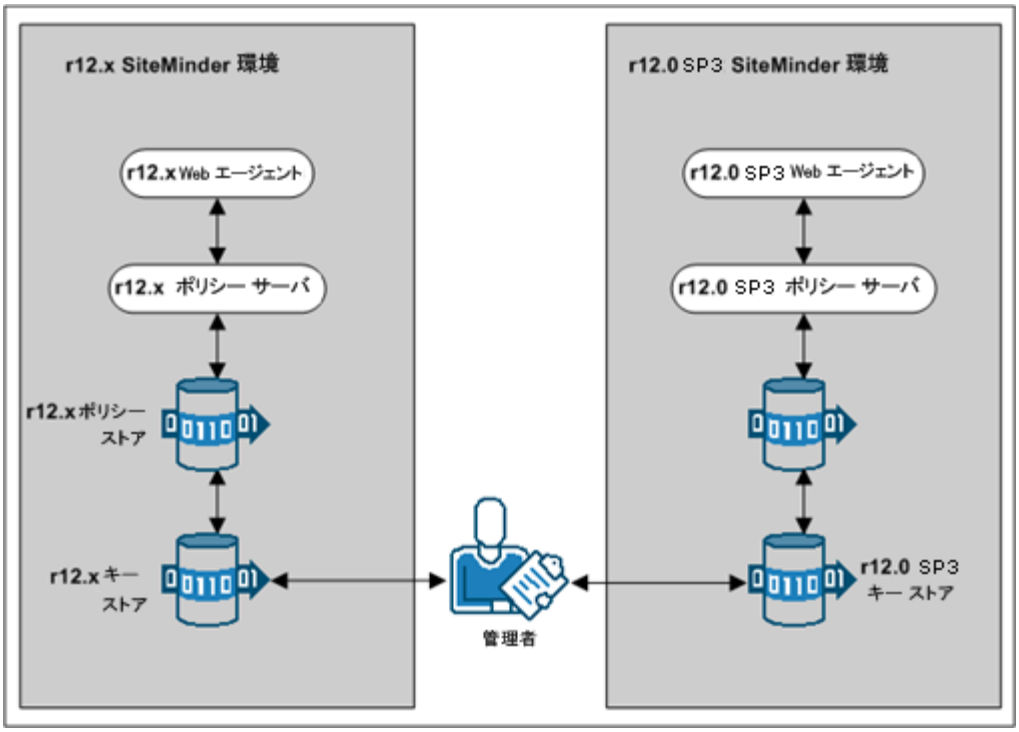
既存の r12.x ポリシー サーバは、キー ロールオーバーに r12.x キー ストアを使用できますが、r12.0 SP3 ポリシー サーバはキー ロールオーバーに r12.0 SP3 キー ストアを使用できます。以下の図は、次のものを表しています。

- r12.x ポリシー ストアに接続する r12.x ポリシー サーバ。
- r12.0 SP3 ポリシー ストアに接続する r12.0 SP3 ポリシー サーバ。
- r12.x キー ストアに接続して新しいキーを取得する r12.x ポリシー サーバ。

- r12.0 SP3 キー ストアに接続して新しいキーを取得する r12.0 SP3 ポリシー サーバ。
- 管理 UI を使用して各キー ストアの静的エージェントおよびセッション キーを設定する SiteMinder 管理者。

  重要: すべてのキー ストアで同じエージェントとセッション キーが使用されるわけではない場合、シングル サインオンに失敗します。
- 対応する r12.x ポリシー サーバをポーリングして新しいキーを取得する r12.x Web エージェント。
- 対応する r12.0 SP3 ポリシー サーバをポーリングして新しいキーを取得する r12.0 SP3 Web エージェント。

注: 図には示されていませんが、ポリシーストアとストアデータは、フェイルオーバーのために複製することができます。データベースまたはディレクトリ サーバのタイプにより、データの複製方法が決まります。マスタ/スレーブ環境でのキー管理の詳細については、「ポリシー サーバ管理ガイド」を参照してください。データの複製の詳細については、使用しているベンダーから発行されたマニュアルを参照してください。



r12.0 SP3 環境の作成

既存の環境から独立した r12.0 SP3 環境を設定できます。r12.0 SP3 コンポーネントを以下の順序でインストールして設定します。

1. 1 つ以上のポリシー サーバ。

   重要 共通キー ストアを使用してシングル サインオンを維持する場合、すべてのポリシー サーバが同じ暗号化キーを使用する必要があります。暗号化キーの値がわからない場合、ポリシー ストアの r12.x 値をリセットできます。r12.0 SP3 ポリシー サーバをインストールするときに新しい値を使用します。

   注: ポリシー ストア暗号化キーのリセットの詳細については、「ポリシー サーバ管理ガイド」を参照してください。

2. ポリシー ストア。
3. 管理 UI。
4. 1 つ以上の Web エージェント。
5. レポート サーバ

注: ポリシー サーバ、ポリシー ストア、管理 UI、およびレポート サーバのインストールの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。Web エージェントのインストールの詳細については、「*Web エージェント インストール ガイド*」を参照してください。

共通キー ストアのシングル サインオン要件

共通キー ストアを展開する場合は、以下の手順を実行します。実行しない場合、シングル サインオンに失敗します。

- r12.x ポリシーおよびキー ストアは必ず別個に設定してください。

  注: キー ストアの設定の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

- キー ストアのバージョンを r12.x のままにします。r12.0 SP3 ポリシー サーバは r12.x キー ストアと通信できますが、r12.x ポリシー サーバは r12.0 SP3 キー ストアと通信できません。
- すべてのポリシー サーバが共通の r12.x ポリシーストアを使用するように設定します。

- すべてのポリシー サーバが必ず同じ暗号化キーを使用するようにしてください。暗号化キーの値がわからない場合、ポリシー ストアの r12.x 値をリセットできます。r12.0 SP3 ポリシー サーバをインストールするときに新しい値を使用します。

  注: ポリシー ストア暗号化キーのリセットの詳細については、「ポリシー サーバ管理ガイド」を参照してください。

- 1 つのポリシー サーバを指定して、動的なエージェント キーを生成します。残りのポリシー サーバのエージェント キー生成を無効にします。

  注: エージェント キーの動的な生成の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

複数キー ストアのシングル サインオン要件

複数キー ストアを展開する場合は、以下の手順を実行します。実行しない場合、シングル サインオンに失敗します。

- すべてのポリシー サーバの動的エージェント キー生成を無効にします。
- SiteMinder 管理者が、r12.x および r12.0 SP3 キー ストアで同じ静的エージェント キーと同じセッション チケットを指定するのに必要な 管理 UI アクセス権を持っているようにしてください。

  注: 管理者権限の委任の詳細については、「ポリシー サーバ設定ガイド」を参照してください。

- r12.x および r12.0 SP3 キー ストアで同じ静的エージェント キーと同じセッション チケットが設定されるようにしてください。

  注: 静的エージェント キーとセッション チケットの設定の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

r12.x ポリシーの移行

r12.0 SP3 展開を使用して r12.x リソースを保護する予定の場合、ポリシー ストア データを r12.0 SP3 ポリシー ストアに移行することをお勧めします。

必須ではありませんが、r12.0 SP3 ポリシー ストアの管理を開始する前にポリシー ストア データを移行した場合、重複するオブジェクトに関連する競合の可能性を回避できます。

ポリシーを移行する方法

1. r12.x バージョンの XPSExport ユーティリティを使用して r12.x ポリシー ストア データをエクスポートします。*注:* r12.x バージョンの XPSExport の詳細については、r12.x の「ポリシー サーバ管理ガイド」を参照してください。
2. r12.0 SP3 バージョンの XPSImport ユーティリティを使用して r12.0 SP3 ポリシー ストア データをインポートします。r12.0 SP3 バージョンの XPSImport の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

アップグレードまたはポリシー移行の一環として SiteMinder ポリシーをある環境から別の環境に移動させる場合、環境に固有の一部のオブジェクトがエクスポート ファイルに含まれます。これらのオブジェクトにはたとえば以下のものがあります。

- トラステッド ホスト
- HCO ポリシー サーバ設定
- 認証方式 URL
- パスワード サービス リダイレクト
- リダイレクト レスポンス

XPSExport を使用するときに選択したモードによって、これらのオブジェクトは新しい環境に追加されるか、または既存の設定を上書きします。オブジェクトをインポートする際は、環境設定を誤って変更することがないよう注意が必要です。

注: エクスポートの XPSExport モードの詳細については、ポリシー サーバ管理ガイド を参照してください。

ユーザ ディレクトリのシングル サインオン要件

両方の環境で作成する SiteMinder ユーザ ディレクトリ オブジェクトが同じ名前になるようにしてください。異なる名前を使用して r12.x および r12.0 SP3 ポリシー サーバを同じユーザ ストアにポイントした場合、シングル サインオンに失敗します。

第 4 章: FIPS 準拠アルゴリズムの使用

このセクションには、以下のトピックが含まれています。

FIPS 140-2 移行の概要

ポリシー サーバは、FIPS（Federal Information Processing Standard）140-2 準拠の認定暗号ライブラリを使用します。FIPS は、AES（Advanced Encryption Standard: 高度暗号化標準）に適合する暗号モジュールを信用するために使用される米国政府のコンピュータ セキュリティ標準です。 これらのライブラリにより、SiteMinder 環境で FIPS 準拠のアルゴリズムのみを使用して機密データを暗号化する場合に、FIPS 動作モードが実現されます。SiteMinder 環境は、以下のいずれかの FIPS 動作モードで動作できます。

- FIPS 互換
- FIPS 移行
- FIPS 専用

デフォルトでは、r12.0 SP3 にアップグレードされた SiteMinder 環境は、FIPS 互換モードで動作しています。FIPS 互換モードの環境は、機密データを暗号化するために以前のバージョンの SiteMinder に存在していたアルゴリズムを使用し、以前のバージョンの SiteMinder と互換性があります。組織が FIPS 準拠のアルゴリズムの使用を要求していない場合、ポリシー サーバはそれ以外の設定を行わなくても FIPS 互換モードで動作できます。

FIPS 準拠のアルゴリズムのみを使用するように環境を移行するには、2 つの段階が必要です。

1. **既存の機密データの暗号化** - 第 1 段階では、FIPS 移行モードで動作するように環境を設定します。FIPS 移行モードでは、FIPS 互換モードで実行されている r12.0 SP3 環境を FIPS 専用モードに移行できます。FIPS 移行モードでは、r12.0 SP3 環境は、FIPS 準拠のアルゴリズムを使用して既存の機密データを再暗号化するときは、既存の SiteMinder 暗号化アルゴリズムを引き続き使用します。
2. **FIPS 専用モードの設定** - 第 2 段階では、FIPS 専用モードで動作するように環境を設定します。FIPS 専用モードでは、環境は FIPS 準拠のアルゴリズムのみを使用して機密データを暗号化します。

   重要 FIPS 専用モードで実行されている環境は、以前のバージョンの SiteMinder と相互運用することはできず、上位互換性はありません。これには、すべてのエージェント、以前のバージョンのエージェント API を使用しているカスタム ソフトウェア、および PM API またはポリシー サーバが公開する他の API を使用しているカスタム ソフトウェアが含まれます。そのようなソフトウェアをすべて対応する SDK の r12.0 SP3 バージョンと再リンクして、FIPS 専用モードの必要なサポートを実現します。

注:使用されている FIPS 認定モジュールおよびアルゴリズム、保護されているデータおよび、SiteMinder 暗号境界の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

FIPS 140-2 の移行要件

FIPS 準拠のアルゴリズムのみ使用するように環境を移行する前に、環境が最小要件を満たすことを確認します。以下を印刷してチェックリストとして使用できます。

- ☐ SDK を含む SiteMinder 環境全体が r12.0 SP3 にアップグレードされていることを確認します。
- ☐ 環境にカスタム エージェントが含まれている場合は、それらが対応する SDK に再リンクされていることを確認します。

  注: カスタム エージェントの再リンクの詳細については、「*API Reference Guide for C*」および「*API Reference Guide for Java*」を参照してください。

- ☐ 環境内の少なくとも 1 つのポリシー サーバで、エージェント キー生成が有効に設定されていることを確認します。

  注: エージェント キー生成の有効の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

- ☐ 環境で X.509 クライアント証明書認証方式が使用される場合は、ユーザ証明書が FIPS 準拠のアルゴリズムのみを使用して生成されることを確認します。
- ☐ ポリシー サーバが SSL を介してポリシー ストアやユーザ ストアに接続する場合、ポリシー サーバにより使用される証明書と接続用のディレクトリ ストアが FIPS 準拠であることを確認します。

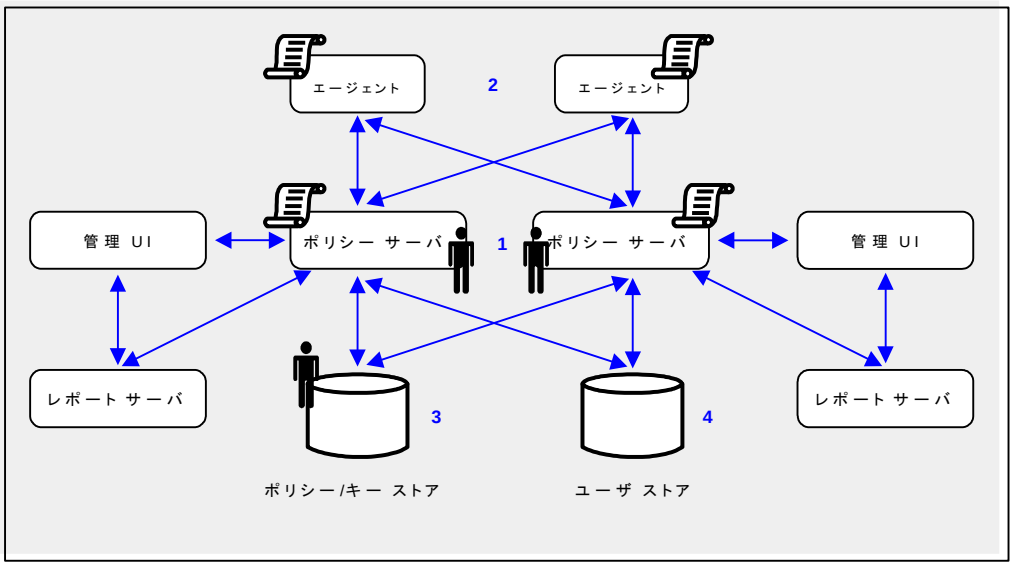
移行のロードマップ - 機密データの暗号化

環境が FIPS 専用モードで動作するには、以下の手順を実行する必要があります。

- 特定のコンポーネントを、FIPS 移行モードで動作するように設定します。
- FIPS 準拠のアルゴリズムを使用して、既存の機密データを再暗号化します。

以下の図に、サンプル r12.0 SP3 環境および詳細を示します。

- FIPS 移行モードで動作するコンポーネントを設定する順序
- 再暗号化する必要がある既存の機密データ



1. 環境内の各ポリシー サーバが、FIPS 移行モードで動作するように設定されます。

   - EncryptionKey.txt ファイルにあるポリシー ストア キーは、FIPS 準拠ではないアルゴリズムを使用して暗号化されます。環境を FIPS 専用モードに設定する前に、環境内のポリシー サーバごとにこのキーを再暗号化します。
   - ポリシー ストア管理者パスワードは、FIPS 準拠ではないアルゴリズムを使用して暗号化されます。環境を FIPS 専用モードに設定する前に、このパスワードを再暗号化します。

     重要 キー ストア、監査ログ、トークン データ、またはセッション サーバに別個のデータベースを設定している場合、これらのパスワードは FIPS 準拠ではないアルゴリズムを使用して暗号化されます。環境を FIPS 専用モードに設定する前に、これらのパスワードを再暗号化します。

   - SiteMinder スーパー ユーザ パスワードは、FIPS 準拠ではないアルゴリズムを使用して暗号化されます。環境を FIPS 専用モードに設定する前に、このパスワードを再暗号化します。

     注: これは、デフォルト SiteMinder 管理者アカウントのパスワードです。このアカウントは、管理 UI への直接アクセスを必要としないすべての管理タスクに使用されます。これは、スーパー ユーザ権限を持つ 管理 UI 管理者アカウントのパスワードではありません。

2. 環境内の各 SiteMinder Web エージェント(カスタム エージェントを含む)は、FIPS 移行モードで動作するように設定されます。

   ポリシー サーバおよびエージェントが暗号化通信チャネルの確立に使用する共有秘密キーは、FIPS 準拠ではないアルゴリズムを使用して暗号化されます。環境を FIPS 専用モードに設定する前に、共有秘密キーを再暗号化します。

3. キーおよび機密ポリシー ストア データが再暗号化されます。

   注: 上の図では、1 つのデータベース インスタンスがポリシー/キー ストアとして表されています。お使いの環境では、ポリシー ストアおよびキー ストアに別々のデータベース インスタンスが使用されている場合があります。

   ポリシー ストアまたはポリシーおよびキー ストアに格納された機密データは、FIPS 準拠ではないアルゴリズムを使用して暗号化されます。環境を FIPS 専用モードに設定する前に、キーおよび機密ポリシー ストア データを再暗号化します。

4. （オプション）環境で基本パスワード サービスが使用されている場合、FIPS 移行モードで動作しているポリシー サーバは、対応するユーザが認証を求められたときに FIPS 準拠のアルゴリズムを使用して各パスワード BLOB を再暗号化します。ユーザがパスワード履歴を失ってロックアウトされることがないようにするには、ポリシー サーバが再暗号化しなかったパスワード BLOB を識別し、ログインするか、パスワードを変更する必要があることをユーザに通知します。

   注: パスワード ポリシーの設定方法により、ポリシー サーバがいつパスワード BLOB を再暗号化するかが決まります。

   - パスワード ポリシーがログインの成功と失敗を追跡するように設定されている場合、ポリシー サーバはユーザのログイン時にパスワード BLOB を再暗号化します。
   - パスワード ポリシーがログインを追跡するように設定されていない場合、ポリシー サーバはユーザがパスワードを変更したときにパスワード BLOB を再暗号化します。

既存の機密データを再暗号化する方法

FIPS 準拠のアルゴリズムを使用して既存の機密データを再暗号化するには、以下の手順を実行します。

1. 環境情報を集めます。
2. すべてのポリシー サーバを FIPS 移行モードに設定します。
3. ポリシー ストア キーを再暗号化します。
4. ポリシー ストア管理者パスワードを再暗号化します。
5. SiteMinder スーパー ユーザ パスワードを再暗号化します。
6. すべてのエージェントを FIPS 移行モードに設定します。
7. ポリシーおよびキー ストア データを再暗号化します。
8. （オプション）環境で基本パスワード サービスが使用されている場合、パスワード BLOB が再暗号化されていることを確認します。

環境情報の収集

ポリシー サーバが FIPS 移行モードで動作しているときに既存の機密データを再暗号化するには、特定の環境情報が必要です。

注: FIPS 情報ワークシートは、機密データの再暗号化前に情報を収集して記録するために用意されています。このワークシートを印刷して、必要な情報を記録するために使用できます。

- **ポリシー ストア キー** - 環境内のポリシー サーバごとに、EncryptionKey.txt ファイルからポリシー ストア暗号化キーをコピーし、コピー可能な 1 箇所に保存します。EncryptionKey.txt ファイルは *policy_server_home*\bin にあります。

  policy server home

  ポリシー サーバのインストール パスを指定します。

- **SiteMinder スーパー ユーザ アカウントの名前とパスワード** - SiteMinder スーパー ユーザ アカウントの名前とパスワード。データの再暗号化に使用する SiteMinder ツールには、この情報が必要です。

  注: このアカウントは、管理 UI への直接アクセスを必要としないすべての管理タスクに使用されます。スーパー ユーザ権限を持つ 管理 UI 管理者アカウントの資格情報ではありません。

- **ポリシー ストア管理者のパスワード** - ポリシー ストア管理者のパスワードを識別します。これは、ポリシー ストアとポリシー サーバの間の接続を設定したときに指定されたパスワードです。

ポリシー サーバの FIPS 移行モードへの設定

ポリシー サーバを FIPS 移行モードに設定すると、FIPS 準拠のアルゴリズムを使用して既存の機密データを再暗号化するときに、環境で既存の SiteMinder 暗号化アルゴリズムを使用し続けることができます。

ポリシー サーバを FIPS 移行モードに設定する方法

1. ポリシー サーバをホストしているコンピュータからコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   setFIPSmigration
   ```

   コマンド ウィンドウ内に MIGRATION と表示されます。

2. ポリシー サーバを停止します。

   注: ポリシー サーバの停止および起動の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

3. 以下のいずれかの操作を行います。

   a. ポリシー サーバが Windows システムにインストールされている場合は、マシンを再起動します。

   b. ポリシー サーバが UNIX システムにインストールされている場合は、ポリシー サーバの起動に使用されたユーザとしてログインします。

4. ポリシー サーバを起動します。

5. smps.log ファイルを開き、以下の行があることを確認します。

   従来の SiteMinder から FIPS-140 暗号化アルゴリズムに移行するポリシー サーバ。

6. ログ ファイルを閉じます。

   ポリシー サーバが、FIPS 移行モードで動作するように設定されます。

7. 環境内のポリシー サーバごとに上の手順を繰り返します。

これで、環境内のポリシー サーバごとにポリシー ストア キーを再暗号化できるようになりました。

ポリシー ストア キーの再暗号化

ポリシー ストア キーを再暗号化して、既存のキーを、FIPS 準拠のアルゴリズムを使用して暗号化されたバージョンに置き換えます。

ポリシー ストア キーを再暗号化する方法

1. ポリシー サーバをホストしているコンピュータからコマンド プロンプトを開き、以下のコマンドを実行します。

   `smreg -cf MIGRATE -key key_value`

   -cf MIGRATE

   smreg を FIPS 移行モードで実行するように指定します。

   注: smreg が FIPS 移行モードで実行されると、ポリシー ストア キーは FIPS 準拠のアルゴリズムを使用して再生成されます。

   -key *key value*

   現在のポリシー ストア キーを指定します。

   smreg は新しいポリシーストア キーを生成し、FIPS 準拠のアルゴリズムを使用して暗号化します。

2. EncryptionKey.txt ファイルを開き、新しい暗号化キーが存在し、FIPS 準拠のアルゴリズムによってプレフィックスが付いていることを確認します。

   プレフィックスの例: {AES}

   ポリシー ストア キーが再暗号化されます。

3. 環境内のポリシー サーバごとに後述の手順を繰り返します。

これで、ポリシー ストア管理者のパスワードを再暗号化できるようになりました。

ポリシー ストア管理者パスワードの再暗号化

ポリシー ストア管理者パスワードを再暗号化して、データが FIPS 準拠のアルゴリズムを使用して暗号化されるようにします。

ポリシー ストア管理者パスワードを再暗号化する方法

1. ポリシー サーバ管理コンソールを起動し、[データ]タブをクリックします。

   注: ポリシー サーバ管理コンソールの起動の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

   ポリシー ストアの接続情報が表示されます。

2. [パスワード]フィールドに管理者パスワードを再入力し、[適用]をクリックします。

   管理者パスワードが、FIPS 準拠のアルゴリズムを使用して暗号化されます。

3. (オプション) 以下の 1 つ以上の別個のデータベースを設定している場合、それぞれの管理者パスワードを再暗号化します。

   - キーストア
   - 監査ログ
   - トークンデータ
   - セッション サーバ

   重要 FIPS 専用モードで動作するポリシー サーバは、FIPS に準拠しないアルゴリズムで暗号化されたままのデータベース パスワードを復号化できません。

これで、SiteMinder スーパー ユーザのパスワードを再暗号化できるようになりました。

SiteMinder スーパー ユーザ パスワードの再暗号化

SiteMinder スーパー ユーザ パスワードを再暗号化して、データが FIPS 準拠のアルゴリズムを使用して暗号化されるようにします。

注: これは、デフォルト管理者アカウントのパスワードです。このアカウントは、管理 UI への直接アクセスを必要としないすべての管理タスクに使用されます。これは、スーパー ユーザ権限を持つ 管理 UI 管理者アカウントのパスワードではありません。

SiteMinder スーパー ユーザ パスワードをリセットするには、コマンド プロンプトを開き、以下のコマンドを実行します。

```
smreg -cf MIGRATE -su password
```

-cf MIGRATE

smreg を FIPS 移行モードで実行するように指定します。

注: smreg が FIPS 移行モードで実行されると、既存のスーパー ユーザ パスワードは FIPS 準拠のアルゴリズムを使用して保存されます。

password

既存のスーパー ユーザ パスワードを指定します。

注: 新しいパスワードを指定する必要はありません。同じパスワードを入力して、データが FIPS 準拠のアルゴリズムを使用して暗号化されるようにします。

SiteMinder スーパー ユーザ パスワードが、FIPS 準拠のアルゴリズムを使用して暗号化されます。

これで、環境内の各エージェントを FIPS 移行モードに設定できるようになりました。

エージェントの FIPS 移行モードへの設定

エージェントを FIPS 移行モードに設定すると、FIPS 準拠のアルゴリズムを使用して機密データを再暗号化するときに、環境で既存の SiteMinder 暗号化アルゴリズムを使用し続けることができます。

エージェントの FIPS モードを変更する方法

1. SmHost.conf ファイルをテキスト エディタで開きます。

   以下の行がファイルに存在します。

   ```
   fipsmode="COMPAT"
   ```

2. この行を次のように編集します。

   ```
   fipsmode="MIGRATE"
   ```

3. ファイルを保存して閉じます。

4. エージェントをホストしているマシンを再起動します。

   エージェントは FIPS 移行モードで動作しています。

5. 環境内のトラステッド ホストが登録されたマシンごとに、前の手順を繰り返します。

これで、エージェント共有秘密キーを暗号化できるようになりました。

クライアント共有秘密キーの再暗号化

エージェント共有秘密キーを再暗号化して、既存の秘密キーを、FIPS 準拠のアルゴリズムを使用して暗号化された秘密キーに置き換えます。以下のいずれかの方法で、共有秘密キーを再暗号化します。

- 管理 UI から共有秘密キーを手動でロールオーバーします。
- smreghost を FIPS 移行モードで使用します。

  注: トラステッド ホストの登録時にエージェントが共有秘密キーをロールオーバーできるように設定されなかった場合、smreghost を使用するだけでかまいません。

管理 UI を使用した共有秘密キーの再暗号化

管理 UI から共有秘密キーをロールオーバーする方法

1. 管理 UI にログインし、[管理]-[ポリシー サーバ]、[共有秘密キーのロールオーバー]をクリックします。

   [共有秘密キーのロールオーバー]ペインが表示されます。

2. [指定周期による共有秘密キーのロールオーバー]ラジオ ボタンをオンにします。

   [今すぐロールオーバーを実行]がアクティブになります。

3. [今すぐロールオーバーを実行]をクリックします。

   ポリシー サーバは、共有秘密キーのロールオーバーの有効化が設定されているすべてのトラステッド ホストについて、共有秘密キーをロールオーバーします。

これで、ポリシー ストア内の機密ポリシーおよびキー データを再暗号化できるようになりました。

smreghost を使用した共有秘密キーの暗号化

smreghost を使用して共有秘密キーを再暗号化する方法

1. コマンド プロンプトを開き、以下のコマンドを実行します。

```
smreghost -i policy_server_ip_address -u administrator_user_name
-p administrator_password -hn hostname_for_registration -hc host_config_object
-f path_to_host_config_file -o -cf MIGRATE
```

-i *policy server ip address*

トラステッド ホストが登録されているポリシー サーバの IP アドレスを指定します。

-u *administrator user name*

トラステッド ホストを登録する権限を持つ SiteMinder 管理者の名前を指定します。

-p *administrator password*

トラステッド ホストの登録を許可された管理者のパスワードを指定します。

-hn *hostname for registration*

登録されたホストの現在の名前を指定します。

-hc *host configuration object*

ポリシー サーバで設定されたホスト設定オブジェクトを指定します。

-f *path to host config file*

登録データが含まれているファイルへの完全パスを指定します。デフォルトのファイル名は、SmHost.conf です。

注: ファイル パスを指定しない場合、smreghost を実行している場所に更新されたファイルが保存されます。

-o

既存のトラステッド ホストに上書きします。この引数を使用しない場合、管理 UI を使用して既存のトラステッド ホストを削除する必要があります。この引数を使用して smreghost を使用することをお勧めします。

-cf MIGRATE

smreghost が FIPS 移行モードで実行されるように指定します。

注: smreghost が FIPS 移行モードで実行されると、共有秘密キーは FIPS 準拠のアルゴリズムを使用して作成および暗号化されます。

smreghost は、トラステッド ホストを再登録し、FIPS 承認のアルゴリズムを使用して暗号化された新しい共有秘密キーを作成します。

2. トラステッド ホスト登録データが含まれるファイルを開き、新しい共有秘密キーが存在しており、FIPS 承認のアルゴリズムによってプレフィックスが付けられていることを確認します。

   共有秘密キーは、FIPS 準拠のアルゴリズムを使用して暗号化されます。

   プレフィックスの例: {AES}

これで、ポリシー ストア内の機密ポリシーおよびキー データを再暗号化できるようになりました。

ポリシーおよびキー ストア データの再暗号化

ポリシーおよびキー ストア データを再暗号化して、既存の SiteMinder アルゴリズムを使用して暗号化された機密データが FIPS 準拠のアルゴリズムを使用して暗号化されるようにします。

ポリシーおよびキー ストア データの再暗号化のオプション

ポリシーおよびキー ストア データを再暗号化する方法は、3 つあります。以下の方法が可能です。

- 既存のポリシー ストア内のポリシーおよびキー ストア データを再暗号化します。
- 既存のポリシー ストア内のポリシー データと、既存のキー ストア内のキー データを再暗号化します。
- ポリシーおよびキー ストア データを再暗号化し、データを新しい r12.0 SP3 ポリシー ストア、またはポリシーおよびキー ストアにそれぞれ移行します。

このガイドでは、既存のストアのポリシーおよびキー ストア データを再暗号化する手順について詳述します。

新しい r12.0 SP3 ポリシー ストア、またはポリシーおよびキー ストアを作成する場合

1. smkeyexport を使用して、キー データをエクスポートします。

   注: XPSExport は、ポリシーまたはキー ストアに格納されているキーをエクスポートしません。smkeyexport の使用の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

2. XPSExport を使用して、ポリシー ストア データをエクスポートします。

   注: XPSExport の使用の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

3. r12.0 SP3 ポリシー ストア、またはポリシーおよびキー ストアを作成します。

   注: ポリシーおよびキー ストアの作成の詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

4. smkeyimport を使用して、キー データを新しいポリシー ストアに、または作成されている場合は新しいキー ストアにインポートします。

   注: smkeyimport の使用の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

5. XPSImport を使用して、ポリシー ストア データを新しいポリシーストアにインポートします。

   注: XPSImport の使用の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

ポリシーまたはキー ストアに格納されたキーの再暗号化

ポリシーまたはキー ストアに格納されたキーを再暗号化して、既存のキーを FIPS 準拠のアルゴリズムを使用して暗号化されたバージョンに置き換えます。

ポリシーまたはキー ストアに格納されたキーを再暗号化する方法

1. ポリシー サーバをホストしているコンピュータからコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   smkeyexport -dadmin_name -wadmin_password -ooutput_file_name -l -v -t -cf
   ```

   -d*admin_name*

   SiteMinder 管理者アカウントの名前を指定します。

   -w*admin_password*

   SiteMinder 管理者アカウントのパスワードを指定します。

-o*output_file_name*

(オプション)エクスポートされたファイルの名前を指定します。ファイルを指定しない場合、デフォルトのファイル名は stdout.smdif です。

注: ファイル名に .smdif 拡張子が含まれる確認してください。

例: pskeys.smdif

-l

ログ ファイルの作成を指定します。

-v

(オプション)トラブルシューティング用に詳細モードを有効にします。

-t

(オプション)トラブルシューティング用にトレースを有効にします。

-cf

smkeyexport が FIPS 移行モードで実行されるように指定します。

注: smkeyexport が FIPS 移行モードで実行されている場合、ポリシー ストアに格納されたキーがエクスポートされ、FIPS 準拠のアルゴリズムを使用して再暗号化されます。

smkeyexport は、再暗号化されたキーが含まれる smdif ファイルをエクスポートします。

2. 以下のコマンドを実行します。

```
smkeyimport -iinput_file_name -dadmin_name -wadmin_password -l -v -t -cf
```

-i*input_file_name*

作成したファイル出力ファイルの名前を指定します。

注: 指定するファイル名に .smdif 拡張子が含まれることを確認してください。

-d*admin_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*admin_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-l

ログ ファイルの作成を指定します。

-v

(オプション)トラブルシューティング用に詳細モードを有効にします。

-t

(オプション)トラブルシューティング用にトレースを有効にします。

-cf

smkeyimport が FIPS 移行モードで実行されるように指定します。

smkeyimport は、再暗号化されたキーを対応するストアにインポートします。

これで、ポリシー ストア データを再暗号化できるようになりました。

ポリシー ストア データの再暗号化

ポリシー ストア データを再暗号化する方法

1. ポリシー サーバをホストしているマシンからコマンド プロンプトを開き、ポリシー ストア データ ファイルをエクスポートする場所に移動します。
2. 以下のコマンドを実行します。

   `XPSExport` *`outputfile`* `-xa -passphrase` *`phrase`* `-vT -vI -vW -vE -vF -e file_name -l log_file`

   注: XPSExport を使用して 1 つ以上の個々のオブジェクトをエクスポートすることができますが、この手順ではポリシー ストア データすべてをエクスポートする引数について説明します。これにより、エクスポートにすべての機密データが確実に含まれるようになります。1 つ以上の個々のオブジェクトのエクスポートの詳細については、「ポリシー サーバ管理ガイド」を参照してください。

   outputfile

   XML 出力ファイルの名前を指定します。

   注: ファイル名は一意である必要があります。同じ名前のファイルが存在する場合、エクスポートは失敗します。

   例: psdata

   -xa

   すべてのポリシー データをエクスポートすることを指定します。

-passphrase *phrase*

機密データの暗号化に必要なパスフレーズを指定します。この値は、機密データをポリシー ストアにもう一度インポートするために必要なため、記録します。

制限: パスフレーズには、少なくとも以下の文字が含まれている必要があります。

- 8 文字
- 数字 1 字
- 大文字 1 字
- 小文字 1 字

注: パスフレーズにスペースが含まれている場合は、二重引用符(")で囲んでください。

-vT

(オプション)詳細レベルを TRACE に設定します。

-vI

(オプション)詳細レベルを INFO に設定します。

-vW

(オプション)詳細レベルを WARNING に設定します(デフォルト)。

-vE

(オプション)詳細レベルを ERROR に設定します。

-vF

(オプション)詳細レベルを FATAL に設定します。

-l *log_path*

(オプション)ログを指定されたパスに出力します。

-e *file_name*

(オプション)エラーと例外をログ記録するファイルを指定します。省略した場合、stderr が使用されます。

XPSExport は、ポリシー ストア データをエクスポートし、データ ファイルをツールを実行したディレクトリに配置します。

3. 以下のコマンドを実行します。

   `XPSImport input_file -passphrase phrase -vT -vI -vW -vE -vF -l log_path`

   input_file

   入力 XML ファイルを指定します。

   -passphrase *phrase*

   機密データの復号化に必要なパスフレーズを指定します。

   制限: フレーズは、エクスポート時に指定したフレーズと一致する必要があります。一致しない場合は暗号化に失敗します。

   -vT

   (オプション) 詳細レベルを TRACE に設定します。

   -vI

   (オプション) 詳細レベルを INFO に設定します。

   -vW

   (オプション) 詳細レベルを WARNING に設定します (デフォルト)。

   -vE

   (オプション) 詳細レベルを ERROR に設定します。

   -vF

   (オプション) 詳細レベルを FATAL に設定します。

   -l *log_path*

   (オプション) ログを指定されたパスに出力します。

   -e *file_name*

   (オプション) エラーと例外をログ記録するファイルを指定します。省略した場合、stderr が使用されます。

   XPSImport は、データをポリシー ストアにインポートします。機密データは、FIPS 準拠のアルゴリズムを使用して暗号化されます。

環境で基本パスワード サービスが使用されている場合、パスワード BLOB が FIPS 認定のアルゴリズムを使用して再暗号化されていることを確認できるようになります。

パスワード BLOB が再暗号化されていることを確認します。

ユーザがパスワード履歴を失って、パスワード サービスによってロックアウトされないようにするため、ポリシー サーバがユーザ ストア内のすべてのパスワード BLOB を再暗号化したことを確認します。

パスワード ポリシーのユーザ ストア接続を設定するとき、パスワード データのユーザ プロファイル属性を指定しました。この値は、パスワード BLOB がユーザ ストア内のどこに格納されているかを表しており、再暗号化されていないパスワード BLOB の識別に使用する値です。

パスワード BLOB が再暗号化されていることを確認する方法

1. ディレクトリ サーバまたはデータベース固有のツールを使用して、次のプレフィックスが付いていない Password Data エントリを検索します。

   {AES}

   例: ユーザ ストア接続の設定時に Password Data フィールドの値として「audio」を指定した場合、プレフィックス {AES} が付いていない「audio」に格納されているすべてのエントリを検索します。

2. パスワード BLOB にプレフィックス {AES} が付いていないユーザを識別します。ポリシー サーバは、これらのパスワード BLOB を再暗号化していません。

3. これらのユーザに、ログインするか、パスワードを変更する必要があることを通知します。

   注: パスワード ポリシーの設定方法により、ポリシー サーバがいつパスワード BLOB を再暗号化するかが決まります。

   - パスワード ポリシーがログインの成功と失敗を追跡するように設定されている場合、ポリシー サーバはユーザのログイン時にパスワード BLOB を再暗号化します。
   - パスワード ポリシーがログインを追跡するように設定されていない場合、ポリシー サーバはユーザがパスワードを変更したときにパスワード BLOB を再暗号化します。

重要 パスワード サービスは、ポリシー サーバが FIPS 専用モードで動作している場合、パスワード BLOB が再暗号化されていないユーザをロックアウトします。パスワード BLOB を削除し、無効なフラグをすべてクリアするまで、ユーザはアクセスを回復することができません。パスワード BLOB を削除すると、ユーザのパスワード履歴が失われます。

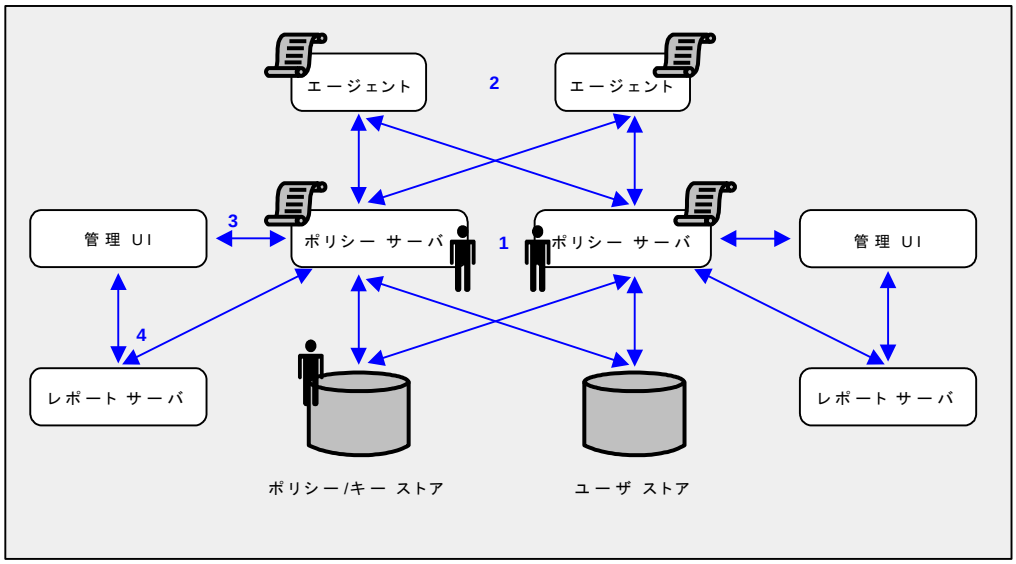
移行ロードマップ - FIPS 専用モードの設定

以下の図は、FIPS 移行モードで動作しているサンプル r12.0 SP3 環境と、FIPS 専用モードで動作するために各コンポーネントおよび接続を設定する順序を示しています。

グレー表示されたコンポーネントは、FIPS 認定のアルゴリズムを使用して再暗号化する必要がある機密データを表わしています。以下の作業が完了するまで、移行処理を続行しないでください。

- 環境内の各ポリシー サーバのポリシー ストア キーを再暗号化する。
- ポリシー ストア管理者パスワードを再暗号化する。
- SiteMinder スーパー ユーザ パスワードを再暗号化する。
- 環境内の各エージェントの共有秘密キーを再暗号化する。
- ポリシー ストア データを再暗号化する。
- 環境で基本パスワード サービスが使用されいている場合は、ポリシー サーバがユーザ ストア内のすべてのユーザ パスワード BLOB を再暗号化する。

  重要 パスワード サービスは、ポリシー サーバが FIPS 専用モードで動作している場合、パスワード BLOB が再暗号化されていないユーザをロックアウトします。パスワード BLOB を削除し、無効なフラグをすべてクリアするまで、ユーザはアクセスを回復することができません。パスワード BLOB を削除すると、ユーザのパスワード履歴が失われます。



1. 環境内の各ポリシー サーバが、FIPS 専用モードで動作するように設定されます。
2. 各 SiteMinder Web エージェント(カスタム エージェントを含む)が、FIPS 専用モードで動作するように設定されます。
3. 各 管理 UI と対応するポリシー サーバの間の既存の接続は、FIPS 準拠ではないアルゴリズムを使用して暗号化されます。各 管理 UI を対応するポリシー サーバに再登録して、FIPS 準拠のアルゴリズムを使用して接続を暗号化します。
4. レポート サーバとポリシー サーバの間の既存の接続は、FIPS 準拠ではないアルゴリズムを使用して暗号化されます。各レポート サーバを対応するポリシー サーバに再登録して、FIPS 準拠のアルゴリズムを使用して接続を暗号化します。

FIPS 専用モードを設定する方法

環境で FIP 順序のアルゴリズムのみを使用して機密データが暗号化されるようにするには、以下の手順を実行します。

1. 環境内の各エージェントを FIPS 専用モードに設定します。
2. 環境内の各ポリシー サーバを FIPS 専用モードに設定します。
3. 管理 UI を対応するポリシー サーバに再登録します。以下の点について考慮してください。
   - 管理 UI は、登録処理中は使用できません。ただし、ポリシー サーバは、この間もアクセス制御を続行し、監査情報を含むログ ファイルを生成します。

- 管理 UI は、内部管理者認証または外部管理者認証用を使用するように設定できます。
  - 内部認証を使用するように設定された 管理 UI は、ポリシー ストアを管理者認証情報のソースとして使用します。
  - 外部認証を使用するように設定された 管理 UI は、外部ユーザ ストアを管理者認証情報のソースとして使用します。

  管理 UI を再登録する処理は、SiteMinder 管理者の認証方法によって異なります。

注: すべての 管理 UI 接続が再登録されるまで、この手順を繰り返します。

4. レポート サーバを対応するポリシー サーバに再登録します。

   注: すべてのレポート サーバ接続が再登録されるまで、この手順を繰り返します。

エージェントの FIPS 専用モードへの設定

エージェントを FIPS 専用モードに設定して、エージェントが FIPS 準拠のアルゴリズムを使用して暗号化されたセッション キー、エージェント キー、共有秘密キーのみ受け入れるようにします。

エージェントを FIPS 専用モードに設定する方法

1. SmHost.conf ファイルをテキスト エディタで開きます。

   以下の行がファイルに存在します。

   ```
   fipsmode="MIGRATE"
   ```

2. この行を次のように編集します。

   ```
   fipsmode="ONLY"
   ```

3. ファイルを保存して閉じます。
4. エージェントをホストしているマシンを再起動します。

   エージェントは FIPS 移行モードで動作しています。

5. 環境内のトラステッド ホストとして登録されたマシンごとに、前の手順を繰り返します。

これで、ポリシー サーバを FIPS 専用モードで動作するように設定できるようになりました。

ポリシー サーバの FIPS 専用モードへの設定

ポリシー サーバを FIPS 専用モードに設定すると、ポリシー サーバが FIPS 準拠のアルゴリズムを使用して暗号化された情報のみ読み書きするように設定されます。

重要 パスワード サービスは、ポリシー サーバが FIPS 専用モードで動作している場合、パスワード BLOB が再暗号化されていないユーザをロックアウトします。パスワード BLOB を削除し、無効なフラグをすべてクリアするまで、ユーザはアクセスを回復することができません。パスワード BLOB を削除すると、ユーザのパスワード履歴が失われます。

注: 再暗号化されないパスワード BLOB の識別の詳細については、「パスワード BLOB が再暗号化されていることを確認する方法 (P. 129)」を参照してください。

ポリシー サーバを FIPS 専用モードに設定する方法

1. ポリシー サーバをホストしているマシンからコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   setFIPSonly
   ```

   コマンド ウィンドウ内に ONLY と表示されます。

2. ポリシー サーバを停止します。

   注: ポリシー サーバの停止および起動の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

3. 以下のいずれかの操作を行います。

   a. ポリシー サーバが Windows システムにインストールされている場合は、マシンを再起動します。

   b. ポリシー サーバが UNIX システムにインストールされている場合は、ポリシー サーバの起動に使用されたユーザとしてログインします。

4. ポリシー サーバを起動します。

5. smps.log ファイルを開き、以下の行があることを確認します。

   ```
   FIPS-140 暗号アルゴリズムのみを使用するポリシー サーバ。
   ```

6. ログ ファイルを閉じます。

   ポリシー サーバが、FIPS 専用モードで動作するように設定されます。

7. 環境内のポリシー サーバごとに後述の手順を繰り返します。

これで、各 管理 UI を対応するポリシー サーバに再登録できるようになりました。

内部認証を使用するように設定された 管理 UI を再登録する方法

既存の SiteMinder アルゴリズムは、管理 UI およびポリシー サーバが暗号化接続の確立に使用する共有秘密キーを引き続き暗号化します。管理 UI を再登録すると、FIPS 準拠のアルゴリズムを使用して暗号化された新しい共有秘密キーが作成されます。

内部認証を使用するように設定された 管理 UI を再登録するには、以下の手順を実行します。

1. アプリケーション サーバを停止します。
2. 管理 UI データ ディレクトリを削除します。
3. 管理 UI 登録ウィンドウをリセットします。
4. アプリケーション サーバを起動します。
5. 管理 UI を登録します。

アプリケーション サーバを停止します。

アプリケーション サーバを停止する方法

1. 管理 UI ホスト システムにログインします。
2. 以下のいずれかを行います。
   - スタンドアロン インストール オプションを使用して 管理 UI をインストールした場合は、SiteMinder 管理 UI サービスを停止します。
   - 既存のアプリケーション サーバ インフラストラクチャに 管理 UI をインストールした場合は、アプリケーション サーバを停止します。

   注: アプリケーション サーバの停止の詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

管理 UI データ ディレクトリの削除

管理 UI とポリシー サーバの間の既存の信頼された接続を削除するには、管理 UI データ ディレクトリを削除します。

管理 UI データ ディレクトリを削除する方法

1. 管理 UI ホスト システムにログインします。
2. 以下のいずれかを行います。
   - (スタンドアロン) スタンドアロン インストール オプションを使用して 管理 UI をインストールした場合、*administrative_ui_home*/CA/SiteMinder/adminui/server/default に移動して、以下のフォルダを削除します。

     data

     administrative_ui_home

     管理 UI インストール パスを指定します。
   - (JBoss) 既存の JBoss インフラストラクチャに 管理 UI をインストールした場合、*JBoss_home*/server/default/data に移動します。

     JBoss_home

     JBoss のインストール パスを指定します。

     データ フォルダには、apacheds、derby、および siteminder フォルダが存在します。

     a. siteminder フォルダを削除します。

     b. apacheds フォルダを開き、siteminder フォルダを削除します。

     c. derby フォルダを開き、siteminder フォルダを削除します。
   - (WebLogic) 既存の WebLogic インフラストラクチャに 管理 UI をインストールした場合、*WebLogic_domain_folder* に移動して、以下のフォルダを削除します。

     data

     WebLogic_domain_folder

     管理 UI 用に作成された WebLogic ドメインへのパスを指定します。

- (WebSphere)既存の WebSphere インフラストラクチャに 管理 UI をインストールした場合、*WebSphere_home*/profiles/*profile* に移動し、以下のフォルダを削除します。

  data

  WebSphere_home

  WebSphere インストールの完全パスを指定します。

  profile

  管理 UI に使用するプロファイルの名前を指定します。

管理 UI データ ディクショナリが削除されます。

管理 UI 登録ウィンドウのリセット

ポリシー ストア内の任意のスーパー ユーザの認証情報をサブミットするには、登録ウィンドウをリセットします。ポリシー サーバは、これらの認証情報を使用して、登録リクエストが有効であることと、管理 UI とポリシー サーバの間の関係が信頼できることを確認します。

管理 UI 登録ウィンドウをリセットする方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のコマンドを実行します。

```
XPSRegClient siteminder_administrator[:passphrase] -adminui-setup -t timeout -r
retries -c comment -cp -l
log_path -e error_path -vT -vI -vW -vE -vF
```

siteminder_administrator

スーパー ユーザ アクセス権を持つ SiteMinder 管理者を指定します。

注: スーパー ユーザ アカウントを使用できない場合は、smreg ユーティリティを使用してデフォルト SiteMinder アカウントを作成します。

passphrase

SiteMinder 管理者アカウントのパスワードを指定します。

注: パスフレーズを指定しない場合、XPSRegClient でパスフレーズの入力と確認が求められます。

-adminui-setup

管理 UI がポリシー サーバに再登録されることを指定します。

-t *timeout*

(オプション) 管理 UI をインストールしてから、ログインしてポリシー サーバとの信頼関係を作成するまでの割り当て時間を指定します。タイムアウト値を超過すると、ポリシー サーバは登録リクエストを拒否します。

測定単位: 分

デフォルト: 240 (4 時間)

最小制限: 1

最大制限: 1440 (24 時間)

-r *retries*

(オプション) 管理 UI の登録時に許容される試行の失敗回数を指定します。管理 UI にログインして登録処理を完了するときに間違った SiteMinder 管理者認証情報をサブミットすると、登録に失敗することがあります。

デフォルト: 1

最大制限: 5

-c *comment*

(オプション) 指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注: コメントは引用符で囲んでください。

-cp

(オプション) 登録ログ ファイルに複数行のコメントが含まれることを指定します。ユーティリティにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注: コメントは引用符で囲んでください。

-l *log path*

(オプション) 登録ログ ファイルをエクスポートする必要がある場所を指定します。

デフォルト: *siteminder_home*¥log

siteminder_home

ポリシー サーバのインストール パスを指定します。

-e *error path*

(オプション) 例外を指定されたパスに送信します。

デフォルト: stderr

-vT

(オプション) 詳細レベルを TRACE に設定します。

-vI

(オプション) 詳細レベルを INFO に設定します。

-vW

(オプション) 詳細レベルを WARNING に設定します。

-vE

(オプション) 詳細レベルを ERROR に設定します。

-vF

(オプション) 詳細レベルを FATAL に設定します。

3. Enter キーを押します。

   XPSRegClient は、ポリシー サーバに管理者認証情報を提供します。ポリシー サーバは、管理 UI にログインするときにこれらの認証情報を使用して登録リクエストを検証します。

アプリケーション サーバの起動

アプリケーション サーバを起動する方法

1. 管理 UI ホスト システムにログインします。
2. 以下のいずれかの操作を行います。
   - スタンドアロン インストール オプションを使用して 管理 UI をインストールした場合は、SiteMinder 管理 UI サービスを起動します。
   - 既存のアプリケーション サーバ インフラストラクチャに 管理 UI をインストールした場合は、アプリケーション サーバを起動します。

   注: アプリケーション サーバの起動の詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

管理 UI の登録

管理 UI を登録し、FIPS 準拠のアルゴリズムを使用して暗号化された新しい共有秘密キーを作成します。

注: 管理 UI の登録の詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

外部認証を使用するように設定された管理 UI を再登録する方法

既存の SiteMinder アルゴリズムは、管理 UI およびポリシー サーバが暗号化接続の確立に使用する共有秘密キーを引き続き暗号化します。管理 UI を再登録すると、FIPS 準拠のアルゴリズムを使用して暗号化された新しい共有秘密キーが作成されます。

外部認証を使用するように設定された 管理 UI を再登録するには、以下の手順を実行します。

1. 管理 UI とポリシー サーバの間の既存の接続を削除します。
2. 管理 UI 登録ツールを実行します。
3. 登録情報を集めます。
4. 管理 UI とポリシー サーバの接続を設定します。
5. 前述のトラステッド ホストを削除します。

ポリシー サーバへの 管理 UI 接続の削除

接続を再登録することができるように、ポリシー サーバへの 管理 UI 接続を削除します。

ポリシー サーバへの 管理 UI 接続を削除する方法

1. 管理 UI にログインし、[管理]-[管理 UI]をクリックします。

   接続のタイプのリストが表示されます。
2. [ポリシー サーバ接続]-[ポリシー サーバ接続の削除]をクリックします。

   [ポリシー サーバ接続の削除]ペインが開きます。
3. 検索条件を入力し、[検索]をクリックします。

   条件と一致する接続が表示されます。

4. 削除する接続を選択し、[選択]をクリックします。

   要求を確認するメッセージが表示されます。

5. [はい]をクリックします。

   管理 UI とポリシー サーバの間の接続が削除されます。

登録ツールの実行

クライアント名とパスフレーズを作成するには、管理 UI 登録ツールを実行します。クライアント名とパスフレーズの組み合わせは、登録する 管理 UI を識別するためにポリシー サーバが使用する値です。登録処理を完了するには、管理 UI からクライアントとパスフレーズの値をサブミットします。

登録ツールを実行する方法

1. ポリシー サーバ ホスト システムからコマンド プロンプトを開きます。
2. 以下のコマンドを実行します。

   ```
   XPSRegClient client_name[:passphrase] -adminui -t timeout -r retries -c comment
   -cp -l log_path -e error_path
   -vT -vI -vW -vE -vF
   ```

   注: *client_name* と [:*passphrase*] の間にスペースを挿入すると、エラーが発生します。

   client_name

   登録する 管理 UI を識別します。

   制限: この値は一意である必要があります。たとえば、管理 UI の登録にすでに smui1 を使用している場合は、「smui2」と入力します。

   注: この値は記録しておいてください。この値は、管理 UI から登録処理を完了するときに使用します。

   passphrase

   管理 UI の登録の完了に必要なパスワードを指定します。

   制限:

   - パスフレーズは 6 文字以上にする必要があります。
   - パスフレーズには、アンパサンド (&) またはアスタリスク (*) を含めることができません。

- パスフレーズにスペースが含まれる場合、引用符で囲む必要があります。
- 管理 UI をアップグレードの一部として登録する場合、以前のパスフレーズを再利用できます。

注: この手順でパスフレーズを指定しない場合、XPSRegClient でパスフレーズの入力と確認が求められます。

重要: パスフレーズを記録して、後で参照できるようにします。

-adminui

管理 UI の登録を指定します。

-t *timeout*

(オプション) 管理 UI からの登録処理を完了する必要がある時間を指定します。タイムアウト値に到達すると、ポリシー サーバは登録リクエストを拒否します。

測定単位: 分

デフォルト: 240 (4 時間)

最小制限: 1

最大制限: 1440 (1 日)

-r *retries*

(オプション) 管理 UI からの登録処理を完了するまでに許容される試行の失敗回数を指定します。登録処理時にポリシー サーバに間違ったクライアント名またはパスフレーズをサブミットすると、登録に失敗することがあります。

デフォルト: 1

最大制限: 5

-c *comment*

(オプション) 指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注: コメントは引用符で囲んでください。

-cp

(オプション) 登録ログ ファイルに複数行のコメントが含まれることを指定します。登録ツールにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注: コメントは引用符で囲んでください。

-l *log_path*

(オプション)。登録ログ ファイルをエクスポートする場所を指定します。

デフォルト: *siteminder_home*¥log

siteminder_home

ポリシー サーバのインストール パスを指定します。

-e *error_path*

(オプション) 例外を指定されたパスに送信します。

デフォルト: stderr

-vT

(オプション) 詳細レベルを TRACE に設定します。

-vI

(オプション) 詳細レベルを INFO に設定します。

-vW

(オプション) 詳細レベルを WARNING に設定します。

-vE

(オプション) 詳細レベルを ERROR に設定します。

-vF

(オプション) 詳細レベルを FATAL に設定します。

登録ログ ファイルの名前が一覧表示され、パスフレーズが求められます。

3. Enter キーを押します。

登録ツールにより、クライアント名およびパスフレーズの組み合わせが作成されます。

これで、ポリシー サーバに 管理 UI を登録できるようになりました。管理 UI からの登録処理が完了しました。

登録情報の収集

管理 UI では、ポリシー サーバに関する特定の情報と、登録処理の実行時に作成したクライアント名およびパスフレーズが必要です。管理 UI にログインする前に、以下の情報を集めます。

- **クライアント名** - XPSRegClient ツールを使用して指定したクライアント名。
- **パスフレーズ** - XPSRegClient ツールを使用して指定したパスフレーズ。
- **ポリシー サーバ ホスト** - ポリシー サーバ ホスト システムの IP アドレスまたは名前。
- **ポリシー サーバの認証ポート** - ポリシー サーバが認証リクエストをリスニングするポート。

  デフォルト: 44442

注: ワークシートは、管理 UI の登録前に情報を収集して記録するために用意されています。

ポリシー サーバへの接続設定

SiteMinder 管理者が 管理 UI を使用してポリシー サーバ経由でポリシー情報を管理できるように、管理 UI およびポリシー サーバの接続を設定します。管理 UI からの接続を設定します。

管理 UI およびポリシー サーバの接続を設定する方法

1. サポートされる Web ブラウザを開いて、次のように入力します。

   http://*host.domain*/iam/siteminder/adminui

   管理 UI のログイン画面が表示されます。
2. スーパー ユーザとしてログインします。
3. [管理]-[管理 UI]をクリックします。
4. [ポリシー サーバ接続]-[ポリシー サーバ接続の登録]をクリックします。

   [ポリシー サーバ接続の登録]ペインが開きます。

   注:それぞれの要件および制限など、設定とコントロールの説明を参照するには、[ヘルプ]をクリックします。
5. [一般]グループ ボックスの[名前]フィールドに接続名を入力します。
6. [ポリシー サーバ ホスト]フィールドに、ポリシー サーバ ホスト システムの名前または IP アドレスを入力します。

7. [ポリシー サーバ ポート]フィールドに、ポリシー サーバ認証ポートを入力します。

   注: この値は、ポリシー サーバ管理コンソールの[設定]タブにある[認証ポート](TCP)フィールドの値と一致する必要があります。デフォルトの認証ポートは 44442 です。

8. [一般]グループ ボックスのフィールドに、登録ツールを使用して作成したクライアント名およびパスフレーズを入力します。
9. [FIPS のみのモード]ラジオ ボタンをオンにします。
10. [サブミット]をクリックします。

    管理 UI とポリシー サーバの間の接続が設定されます。管理 UI およびポリシー サーバが暗号化接続の確立に使用する共有秘密キーは、FIPS 認定のアルゴリズムを使用して暗号化されます。

管理 UI を再登録する処理が完了しました。

以前のトラステッド ホストの削除

ポリシー サーバに 管理 UI を再登録すると、新しいトラステッド ホストが作成されます。以前のトラステッド ホストは、必要でなくなったときに削除します。

トラステッド ホスト接続を削除する方法

1. 管理 UI にログインし、[インフラストラクチャ]-[ホスト]をクリックします。
2. [トラステッド ホスト]-[トラステッド ホストの削除]をクリックします。

   [トラステッド ホストの削除]ペインが表示されます。

3. 以前のトラステッド ホスト接続を検索して選択します。

   注: 管理 UI 登録処理の結果作成されるトラステッド ホストには、「Generated by XPSRegClient」という説明が付いています。

4. [選択]をクリックします。

   削除の確認を求めるメッセージが表示されます。

   重要 必ず、新しいトラステッド ホストではなく、前回 管理 UI を登録したときに作成されたトラステッド ホストを削除してください。

5. [はい]をクリックします。

   トラステッド ホスト接続が削除されます。

レポート サーバの接続を再登録する方法

レポート サーバを再登録すると、レポート サーバとポリシー サーバの間の接続が FIPS 承認のアルゴリズムを使用して暗号化されるようになります。

レポート サーバを再登録するには、以下の手順を実行します。

1. レポート サーバのクライアント名とパスフレーズを作成します。
2. 登録情報を集めます。
3. ポリシー サーバにレポート サーバを登録します。

クライアント名とパスフレーズの作成

XPSRegClient ユーティリティを実行すると、クライアント名とパスフレーズを作成できます。クライアント名とパスフレーズは、以下のような値です。

- 登録するレポート サーバを識別するためにポリシー サーバが使用する値
- ポリシー サーバにレポート サーバを登録するために XPSRegClient ツールで使用する値

登録ツールを実行する方法

1. ポリシー サーバ ホスト システムからコマンド ライン ウィンドウを開きます。
2. *siteminder_home*/bin に移動します。

   siteminder_home

   ポリシー サーバのインストール パスを指定します。
3. 以下のコマンドを実行します。

   ```
   XPSRegClient client_name[:passphrase] -report -t timeout -r retries
   -c comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   client_name

   登録するレポート サーバの名前を識別します。

   制限: 値は一意である必要があります。たとえば、すでに reportserver1 を使用している場合は、「reportserver2」と入力します。

   注: この値は記録しておいてください。この値は、レポート サーバ ホスト システムから登録処理を完了するときに必要です。

passphrase

レポート サーバ登録を完了するのに必要なパスワードを指定します。

制限: パスフレーズは

- 6 文字以上にする必要があります。
- パスフレーズには、アンパサンド(&)またはアスタリスク(*)を含めることができません。
- パスフレーズにスペースが含まれる場合、引用符で囲む必要があります。

この手順でパスフレーズを指定しない場合、XPSRegClient でパスフレーズの入力と確認が求められます。

注: この値は記録しておいてください。この値は、レポート サーバ ホスト システムから登録処理を完了するときに必要です。

-report

レポート サーバの登録を指定します。

-t *timeout*

(オプション)レポート サーバ ホスト システムからの登録処理を完了する必要がある時間を指定します。タイムアウト値に到達すると、ポリシー サーバは登録リクエストを拒否します。

測定単位: 分

デフォルト: 240(4 時間)

最小制限: 1

最大制限: 1440(1 日)

-r *retries*

(オプション)レポート サーバ ホスト システムからの登録処理を完了するまでに許容される試行の失敗回数を指定します。登録時に間違ったパスフレーズをサブミットすると、登録に失敗することがあります。

デフォルト: 1

最大制限: 5

-c *comment*

(オプション)指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注: コメントは引用符で囲んでください。

-cp

(オプション) 登録ログ ファイルに複数行のコメントが含まれることを指定します。登録ツールにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注: コメントは引用符で囲んでください。

-l *log path*

(オプション) 登録ログ ファイルをエクスポートする必要がある場所を指定します。

デフォルト: siteminder_home¥log。siteminder_home はポリシー サーバがインストールされている場所です。

-e *error path*

(オプション) 例外を指定されたパスに送信します。

デフォルト: stderr

-vT

(オプション) 詳細レベルを TRACE に設定します。

-vI

(オプション) 詳細レベルを INFO に設定します。

-vW

(オプション) 詳細レベルを WARNING に設定します。

-vE

(オプション) 詳細レベルを ERROR に設定します。

-vF

(オプション) 詳細レベルを FATAL に設定します。

登録ログ ファイルの名前が一覧表示されます。パスフレーズを指定しなかった場合、入力が求められます。

4. Enter キーを押します。

登録ツールにより、クライアント名とパスフレーズが作成されます。

これで、ポリシー サーバにレポート サーバを登録できるようになりました。レポート サーバ ホスト システムからの登録処理が完了しました。

登録情報の収集

レポート サーバとポリシー サーバの間で登録処理を完了するには、特定の情報が必要です。レポート サーバ ホスト システムから XPSRegClient ユーティリティを実行する前に、以下の情報を集めます。

- **クライアント名** - XPSRegClient ツールを使用して指定したクライアント名。
- **パスフレーズ** - XPSRegClient ツールを使用して指定したパスフレーズ。
- **ポリシー サーバ ホスト** - ポリシー サーバ ホスト システムの IP アドレスまたは名前。

ポリシー サーバにレポート サーバを登録します

ポリシー サーバにレポート サーバを登録して、両方のコンポーネント間に信頼関係を作成します。レポート サーバ登録ツールを使用して、レポート サーバ ホスト システムからの接続を設定します。

ポリシー サーバへの接続を設定する方法

1. レポート サーバ ホスト システムからコマンド ライン ウィンドウを開き、*report_server_home/external/scripts* に移動します。

   report_server_home

   レポート サーバのインストール場所を指定します。

   デフォルト:（Windows）C:¥Program Files¥CA¥SC¥CommonReporting

   デフォルト:（UNIX）/opt/CA/SharedComponents/CommonReporting

2. 以下のいずれかのコマンドを実行します。

   - （Windows）

     ```
     regreportserver.bat -pshost host_name -client client_name -passphrase passphrase
     -psport portnum -fipsmode 0|1
     ```

     重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

   - （UNIX）

     ```
     regreportserver.sh -pshost host_name -client client_name -passphrase passphrase
     -psport portnum -fipsmode 0|1
     ```

-pshost *host_name*

レポート サーバを登録するポリシー サーバ ホスト システムの IP アドレスまたは名前を指定します。

-client *client_name*

クライアント名を指定します。クライアント名は、登録するレポート サーバを識別します。

注: この値は、ポリシー サーバ ホスト システムでレポート サーバを登録したときに、XPSRegClient ユーティリティを使用して指定したクライアント名と一致する必要があります。

例: XPSRegClient ユーティリティを使用したときに「reportserver1」を指定した場合、「reportserver1」と入力します。

-passphrase *passphrase*

クライアント名とペアになるパスフレーズを指定します。 クライアント名は、登録するレポート サーバを識別します。

注: この値は、ポリシー サーバ ホスト システムでレポート サーバを登録したときに、XPSRegClient ユーティリティを使用して指定したパスフレーズと一致する必要があります。

例: XPSRegClient ユーティリティを使用したときに「SiteMinder」を指定した場合、「SiteMinder」と入力します。

-psport *portnum*

(オプション)ポリシー サーバが登録リクエストをリスニングしているポートを指定します。

fipsmode

レポート サーバとポリシー サーバの間の通信を暗号化する方法を指定します。

- 0 の場合、FIPS 互換モードを指定します。
- 1 の場合、FIPS のみのモードを指定します。

デフォルト: 0

3. Enter キーを押します。

登録が成功したことを示すメッセージが表示されます。ポリシー サーバへのレポート サーバの再登録が完了しました。レポート サーバとポリシー サーバの間の接続は、FIPS 準拠のアルゴリズムを使用して暗号化されます。

付録 A: アップグレードと FIPS ワークシート

以下のワークシートを使用すると、アップグレードに必要な情報を記録できます。

- ポリシー ストアとしてのサポートされる LDAP データベース
- ポリシー ストアとしてのサポートされるリレーショナル データベース
- 監査ログ データベース、キー ストア、トークン ストア、またはセッション ストアとしての個々のリレーショナル データベース

Active Directory 情報ワークシート

このワークシートを使用すると、Active Directory ディレクトリ サーバをポリシー ストアとして設定したり、既存のポリシー サーバをアップグレードするために必要な情報を集めることができます。

必要な情報	使用する値
ホスト情報	
ディレクトリ サーバのポート情報	
管理 DN	
管理パスワード	
ポリシー サーバのルート DN	
(オプション) SSL クライアント証明書	

CA Directory 情報ワークシート

このワークシートを使用すると、CA Directory データベースをポリシー ストアとして設定するために必要な情報を集めることができます。

必要な情報	使用する値
ホスト情報	

必要な情報	使用する値
CADSA ポート番号	
ベース DN	
管理 DN	
管理パスワード	

Oracle Directory Server 情報ワークシート

以下のワークシートを使用して、Oracle Directory Server Enterprise Edition（以前の Sun Directory Server Enterprise Edition）をポリシー ストアとして設定するか、または既存のポリシー ストアをアップグレードするために必要な情報を確認できます。

必要な情報	使用する値
ホスト情報	
ディレクトリ サーバのポート情報	
管理 DN	
管理パスワード	
ポリシー サーバのルート DN	
（オプション）SSL クライアント証明書	

Microsoft ADAM 情報ワークシート

このワークシートを使用すると、Microsoft ADAM ディレクトリ サーバをポリシー ストアとして設定したり、既存のポリシー サーバをアップグレードするために必要な情報を集めることができます。

必要な情報	使用する値
ホスト情報	
ディレクトリ サーバのポート情報	

必要な情報	使用する値
管理 DN	
管理パスワード	
ポリシー サーバのルート DN	
(オプション) SSL クライアント証明書	

管理 UI の登録ワークシート

このワークシートを使用すると、管理 UI のインストールに必要な登録情報を集めることができます。

必要な情報	使用する値
クライアント名	
パスフレーズ	
ポリシー サーバのホスト名	
ポリシ サーバのポート番号	

FIPS 情報ワークシート

このワークシートを使用すると、ポリシー サーバが FIPS 移行モードで動作しているときに、既存の機密データの再暗号化に必要な情報を集めることができます。

必要な情報	使用する値
SiteMinder スーパー ユーザ アカウント名およびパスワード	
ポリシー ストア管理者パスワード	

付録 B: プラットフォーム サポートおよびインストール メディア

このセクションには、以下のトピックが含まれています。

SiteMinder プラットフォーム サポート マトリックスへのアクセス

SiteMinder によりサポートされる CA およびサードパーティ コンポーネントの全体的なリストについては、テクニカル サポート サイトを参照してください。

サポート サイトからサポート マトリックスを参照する方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下で、[Support By Product]をクリックします。
3. [Select a Product Page]フィールドに「CA SiteMinder」を入力し、Enter キーを押します。

   CA SiteMinder 製品ページが表示されます。
4. [Product Status]セクションをスクロールし、CA SiteMinder Family of Products Platform Support Matrices をクリックします。

注: 最新の JDK および JRE バージョンは、Sun Developer Network でダウンロードできます。

マニュアル選択メニューの使用

SiteMinder マニュアル選択メニューはテクニカル サポート サイトで提供されています。

サポート サイトからサポート マトリックスを参照する方法

1. テクニカル サポート サイトにアクセスします。

   注: ログインする必要はありません。

2. (任意)[Get Support]タブが前面にない場合は、[Get Support]をクリックします。
3. [Find Product News and Support]の下で[Product Pages]をクリックします。

   [Support by Product]ページが表示されます。

4. [Select a Product Page]フィールドに CA SiteMinder を入力して Enter キーを押します。

   CA SiteMinder 製品ページが表示されます。

5. マニュアル選択メニューをクリックします。
6. 必要なリリースのリンクをクリックします。

   SiteMinder マニュアル選択メニューのメイン ページが表示されます。

インストール メディアの検索

SiteMinder インストール メディアの全体的なリストは、テクニカル サポート サイトで見つけることができます。

サポート サイトからサポート マトリックスを参照する方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下で、[Download Center]-[Products]をクリックします。

   [Download Center]画面が表示されます。

3. [Select a Product]フィールドに SiteMinder を入力します。
4. [Select a Release]リストからリリースを選択します。

5. ［Select a Gen Level］リストからサービス パックを選択します。
6. ［Go］をクリックします。

   ［Product Downloads］画面が表示されます。SiteMinder のインストール実行可能ファイルがすべて一覧表示されます。

索引

S

U

W

あ

か

さ

た

は

ま

や

ら