SiteMinder

アップグレード ガイド

12.52 SP1

ca technologies

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。

- SiteMinder
- eTrust SOA Security Manager （CA SOA Security Manager）
- CA Security Command Center
- CA 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。

マニュアルの変更点

SiteMinder の旧リリースで発見された問題の結果として、12.52 のドキュメントに以下の更新が行われました。

- アサーション属性のログ記録に対応するために監査ストアをアップグレードする方法 -- DB2 用手順の改訂。 アップグレード スクリプトは NULL 値を正しく追加するようになり、アップグレード スクリプトの手動での編集はもう必要なくなりました。
- 並列環境の設定方法 (P. 126) - 手順および XPSImport コマンド スイッチを変更しました。
- このガイドのコンポーネント バージョン — r12.5 からのアップグレードのサポートを示す r12.5 への参照を追加しました。
- Linux で Korn シェル（ksh）パッケージが必要 (P. 58) - ポリシー サーバのアップグレードに必要なライブラリを記述するために追加されました。

- バック チャネル ユーザ名が各 SAML パートナーシップで一意であることの確認 (P. 106) - (同じプロトコルの) 既存のパートナーシップが同じ受信バック チャネル ユーザ名を持つことができないというアップグレード要件を説明するトピックを追加しました。 CQ 177179 を解決します。
- 12.x 移行の仕組み (P. 97) - ポリシー ストアあがアップグレードされるまで、12.52 SP1 Web エージェントはインストールされず、12.52 SP1 ポリシー サーバで設定されるという旨の注を削除しました。ポリシー ストアがアップグレードされる前の 12.52 SP1 Web エージェントのインストールに関するガイダンスを改訂する注を追加しました。

このガイドの第 2 版では、以下の点が変更されています。

ドキュメントのみの変更

- r6.x ポリシーの移行 (P. 91) -- Oracle Directory Server の移行手順を修正するためにトピックが更新されました。 ドキュメントは 12.52 SP1 で更新されています。 この変更によって、CQ 182636 および STAR 21697346-1 が解決されます。
- SiteMinder と CA Arcot WebFort および CA Arcot RiskFort との統合 (P. 97) -- SiteMinder と CA Arcot WebFort および CA RiskFort との統合において <stmdnr> をアップグレードする方法を説明するためにトピックが追加されました。

目次

第 1 章: SiteMinder の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。

コンポーネント バージョンおよびアップグレードのサポート

12.52 SP1 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 SP5 CR32
- r6.0 SP5 J
- r12.0 SP2
- r12.0 SP3
- r12.0 SP3 J
- r12.5
- r12.51
- r12.52

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 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 SP2、r12.0 SP3、r12.5、r12.51、および r12.52 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 SP5 を指します。
  - r12.x は、r12.0 SP2、r12.0 SP3、r12.5、r12.51、および r12.52 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 cr3 以下の r12 SP2 および r12.0 SP3 を指します。

    注: r12.0 SP3 cr4 以降のレポート サーバをインストールし、設定する場合は、アップグレードの必要はありません。
- 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.x QMR 5 を指します。
  - r12.x は、r12.0 SP2、r12.0 SP3、r12.5、r12.51、および r12.52 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 12.52 SP1 コンポーネントの展開で構成されます。 12.52 SP1 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 12.52 SP1 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

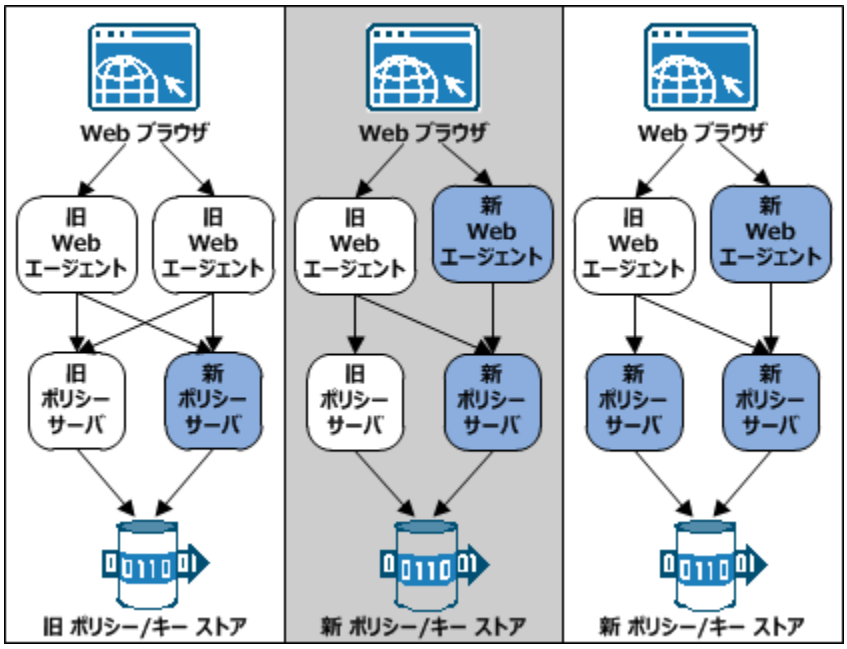
移行は、環境が 12.52 SP1 で動作するまで個々の SiteMinder コンポーネントをアップグレードする処理です。 個々のコンポーネントのアップグレードは、以下の作業中に行う 1 つ以上の手順で構成されます。

- 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.x 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。

図 1: シンプルな移行の概要



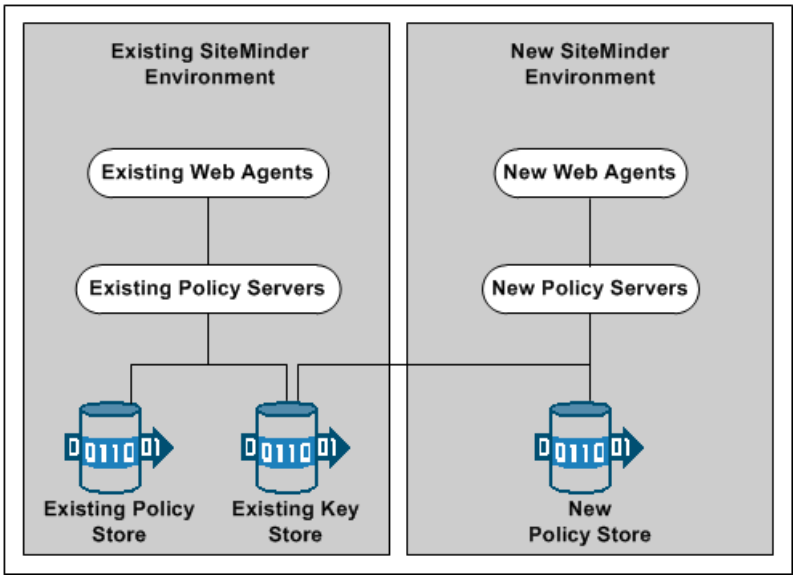
並行アップグレード

並行アップグレードは、既存の環境と同時に 12.52 SP1 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。
- 12.52 SP1 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。

図 2: 並行アップグレードの概要



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

  12.52 SP1 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 12.52 SP1 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。

ポリシー サーバ リリース ノート

ポリシー サーバ リリース ノートにはインストールとアップグレードの考慮事項が含まれます。 移行を開始する前に、これらの内容を確認することをお勧めします。

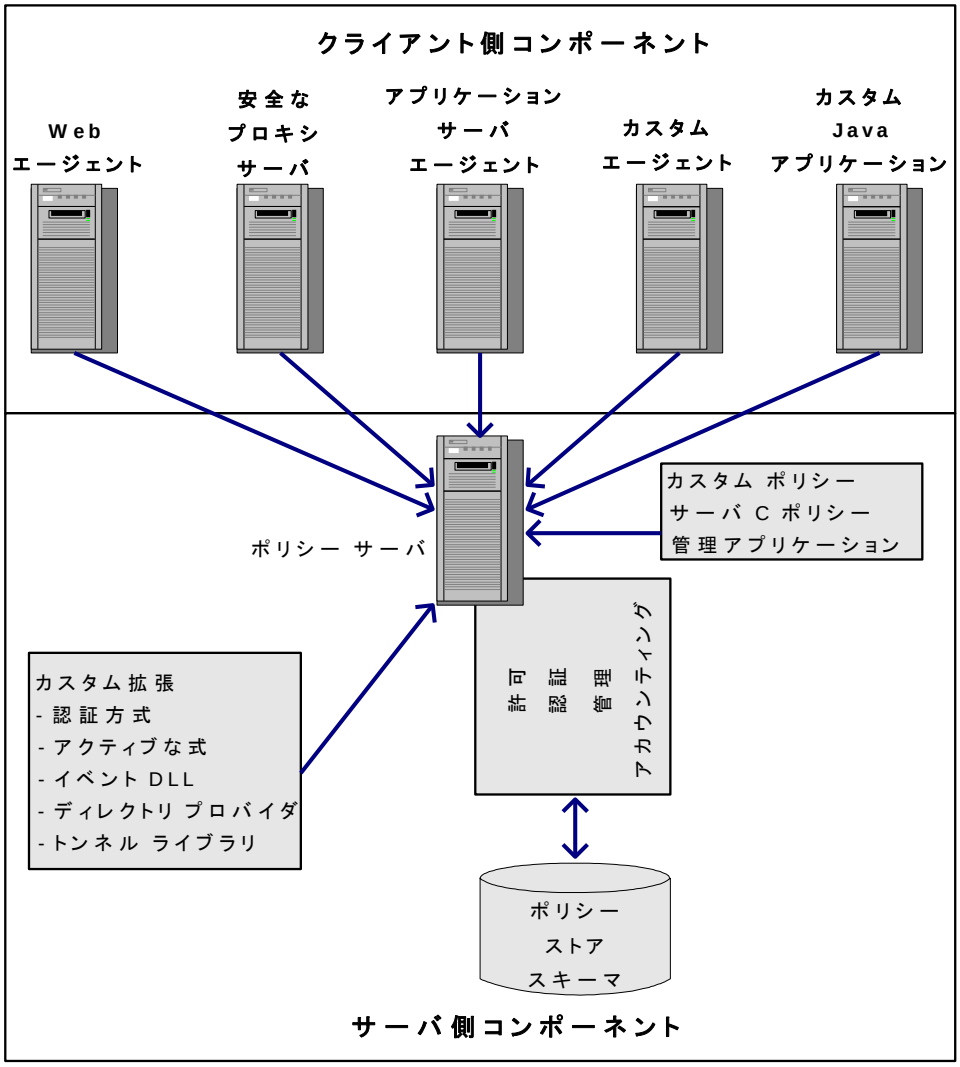
SiteMinder 環境の分析

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。

Question	推奨
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。
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。
12.52 SP1 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 12.52 SP1 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。

Question	推奨
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

元の設定に復帰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。

  12.52 SP1 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.x 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。

SiteMinder 混在環境

12.52 SP1 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 12.52 SP1 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。 以下の点を考慮します。

- 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、12.52 SP1 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。
- 12.x コンポーネントの組み合わせが環境に含まれる場合、12.52 SP1 ポリシー サーバは r12.x 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 QMR6、r12.0 SP2 または r12.0 SP3 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 12.52 SP1 ポリシー サーバが r6.x または r12.x 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。 混在モードのサポートは無効にできません。

ポリシー サーバ管理コンソールでは、12.52 SP1 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。

以下の手順に従います。

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］を選択して、ポリシー サーバ バージョンを表示します。

   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

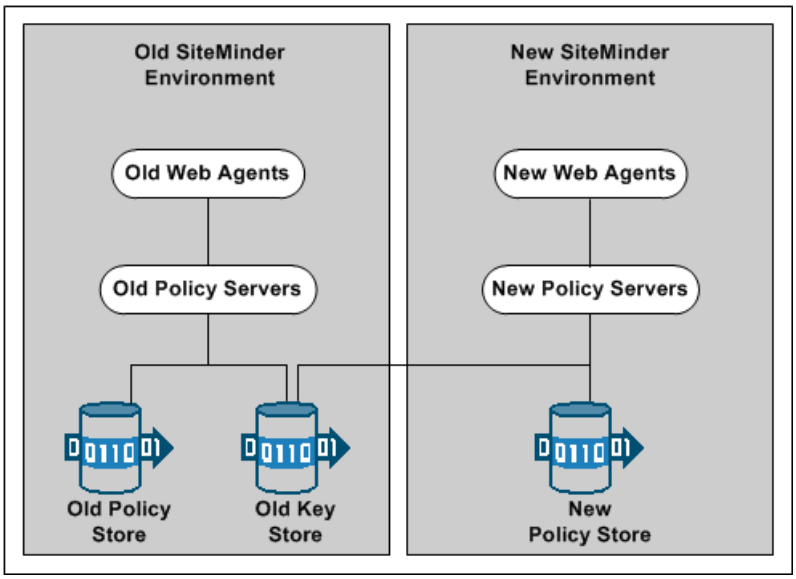
r6.x から 12.52 SP1 に移行するときは、以下の点を考慮します。

- r6.x ポリシー サーバは、12.52 SP1 ポリシー ストアと通信できません。
- 12.52 SP1 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 12.52 SP1 ポリシー サーバは、キー ストアを共有できます。

- r6.x および 12.52 SP1 ポリシー サーバは、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、12.52 SP1 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。

図 3: r6.x の共通キー ストアの展開



6.x 混在環境の制限

12.52 SP1 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 12.52 SP1 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.x および 12.52 SP1 固有の機能は使用できません。

注: r12.x および 12.52 SP1 の機能の詳細については、リリース ノートを参照してください。

r12.x 混在モードのサポート

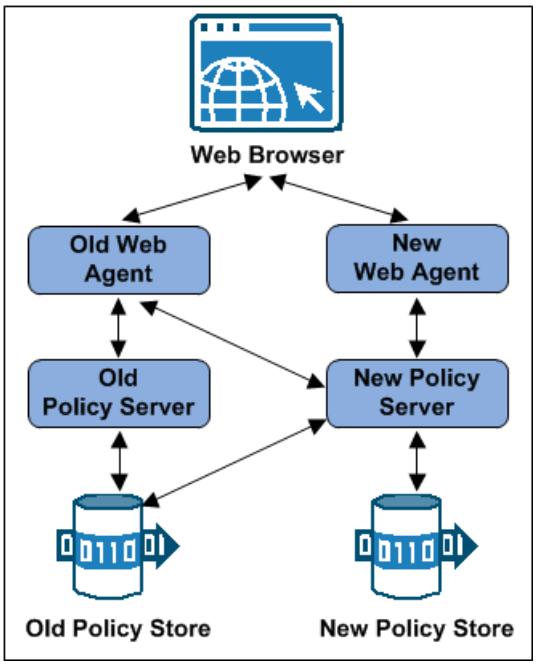
r12.0 SP1 または r12.0 SP2 から 12.52 SP1 に移行するときは、以下の点を考慮します。

- r12.x ポリシー サーバは、12.52 SP1 ポリシー ストアと通信できません。
- 12.52 SP1 ポリシー サーバは、12.52 SP1 ポリシー ストアと通信できます。

- r12.x ポリシー サーバは 12.52 SP1 ポリシー サーバとキー ストアを共有できます。
- r12.x ポリシー サーバは 12.52 SP1 ポリシー サーバとセッション ストアを共有できます。
- r12.x Web エージェントは、12.52 SP1 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。

図 4: r12.x 混在モードのサポート



r12.x 混在環境の制限

12.52 SP1 ポリシー サーバは、r12.x ポリシー ストアと通信できますが、r12.x ポリシー サーバは 12.52 SP1 ポリシー ストアに接続できません。 このため、既存の r12.x 機能はすべて混在環境で使用できますが、12.52 SP1 固有の機能は使用できません。

注: 12.52 SP1 の機能の詳細については、リリース ノートを参照してください。

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。

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. 12.52 SP1 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 12.52 SP1 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 12.52 SP1 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

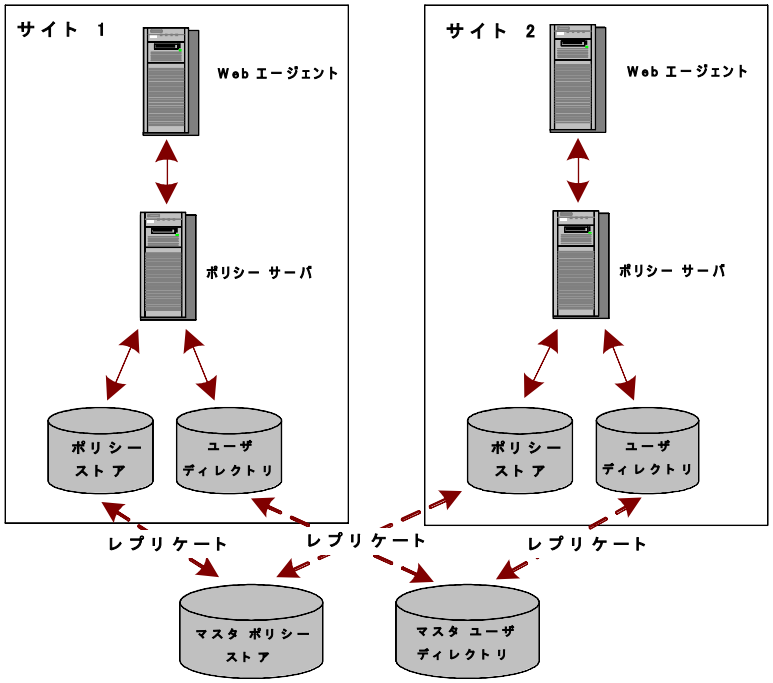
12.52 SP1 にアップグレードする前に、いくつかの共通 SiteMinder 環境について考慮します。 サイトが以下のいずれかと一致するかどうかを確かめます。

- 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. 25)
- クラスタ環境 (P. 26)
- 共有ユーザ ディレクトリ環境 (P. 27)

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。



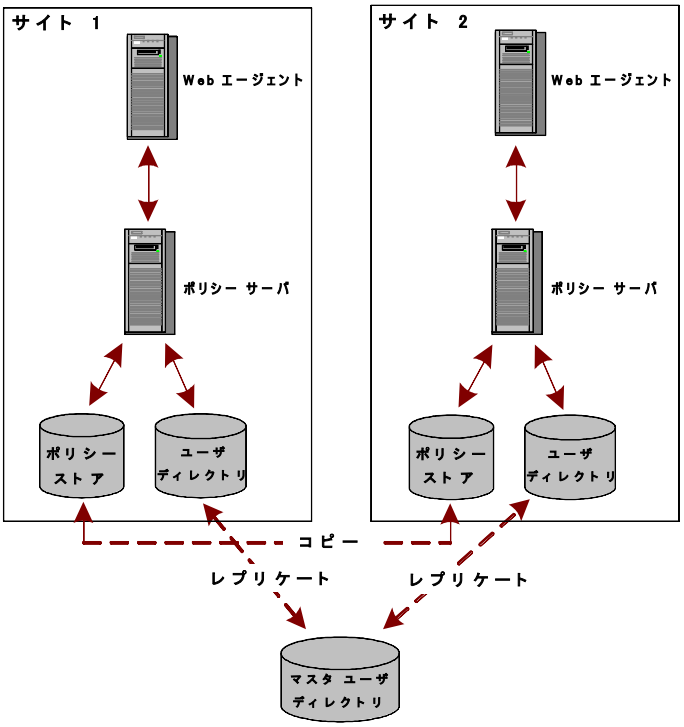
この環境をアップグレードするには、このガイドで概説する手順を使用します。

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。

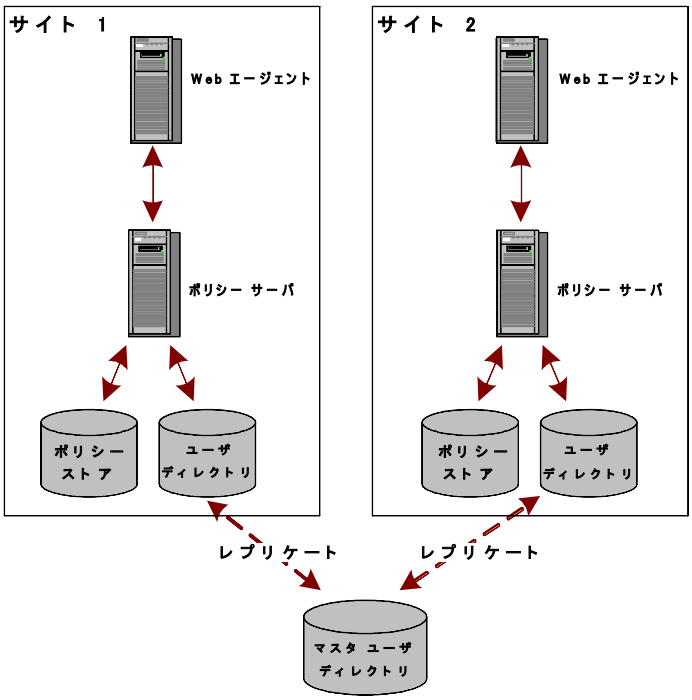


この環境をアップグレードするには、このガイドで概説する手順を使用します。

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: SiteMinder 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。

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。

12.x の Crystal Reports

12.52 SP1 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、12.52 SP1 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。 12.52 SP1 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、12.52 SP1 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

このリリースでは、ポリシー サーバ ユーザ インターフェースを SiteMinder 管理 UI で置き換えます。

管理 UI のデフォルト設定は以下のとおりです。

- 管理者 ID のソースとしてポリシー ストアを使用します。

  このデフォルト設定では、管理 UI をインストールすると直ちに環境を管理することができます。ただし、外部ユーザ ストアに格納された既存の r6.x 管理者は、管理 UI で使用できません。

- ユーザ名とパスワードのみ入力を求めるメッセージが表示されます。SiteMinder は 管理 UI を保護しません。

外部管理者ストア接続を設定して以下を可能にします。

- r6.x 管理者を 管理 UI で利用できるようにします。
- SiteMinder で 管理 UI を保護します。

  注: 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。

証明書データの管理

証明書データ ストアは SiteMinder キー データベース（smkeydatabase）を置換します。 使用する環境で 1 つ以上の smkeydatabases を展開する場合は、以下の点を考慮します。

- 証明書データ ストアは 12.52 SP1 ポリシー ストアと連結されます。 単一の証明書データ ストアによって、各ポリシー サーバ ホスト システム上の個別の smkeydatabase インスタンスが不要になります。
- ポリシー サーバのアップグレードの一部として、すべての smkeydatabase コンテンツが自動的にバックアップされ、証明書データ ストアに移行されます。

- 12.52 SP1 ポリシー サーバは証明書データ ストアとのみ通信できます。12.52 SP1 ポリシー サーバおよびそれぞれのローカル smkeydatabase は、互換モードで作動しません。 ただし、アップグレードされていないポリシー サーバはすべて、smkeydatabase のローカル バージョンとの通信を継続します。

  重要: smkeydatabase の移行が失敗した場合、ポリシー サーバを環境に戻さないでください。移行が失敗した後でポリシー サーバを戻すと、証明書データを必要とするトランザクションはすべて失敗します。

- 移行を開始する前に smkeydatabase インスタンスをすべて同期します。すべてのインスタンスを同期することによって、データの衝突を防ぎます。 データの衝突が発生すると、移行が正常に実行されません。
- 同じポリシー ストアに共通のビューを共有するポリシー サーバはすべて、同じキー、証明書および証明書廃棄リスト（CRL）にアクセスできます。
- 証明書データ ストアの目的は、smkeydatabase の目的と変わりません。このストアによって以下が SiteMinder 環境で利用可能になります。
  - 認証機関（CA）の証明書
  - 公開キーおよび秘密キー
  - 証明書破棄リスト
- 証明書データ ストアの管理に、SiteMinder キー ツールを引き続き使用できます。 ただし、いくつかのオプションが非推奨になります。

  注: 詳細については、「ポリシー サーバ リリース ノート」を参照してください。

- CRL が LDAP ディレクトリ サービスに格納される場合、以下の点を考慮します。
  - SiteMinder では、CRL の発行元と、対応するルート証明書の発行元が同一の CA である必要がなくなりました。
  - SiteMinder はこの確認を実行しなくなりました。 この動作はテキスト ベースの CRL の要件と一致しています。

フェデレーションの統合

このリリースではポリシー サーバ ユーザ インターフェースを 管理 UI に置き換えます。 Federation Security Services を管理していた場合、この機能は レガシー フェデレーション と呼ばれます。

管理 UI にはパートナーシップ フェデレーションも含まれます。 これは、CA SiteMinder® Federation によって使用可能になるパートナーシップ ベースのフェデレーション固有の機能です。

シングル サインオン

12.52 SP1 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。

- 12.52 SP1 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。
- 12.52 SP1 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。

拡張パスワード サービス

ユーザが Advanced Password Services を展開している場合、ポリシー サーバ アップグレードは LANG （翻訳）、CFG （設定）およびメール ファイルをすべて保持します。 ファイルのデフォルト 12.52 SP1 バージョンは *siteminder_home*¥samples にインストールされます。

siteminder_home

ポリシー サーバのインストール パスを指定します。

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。

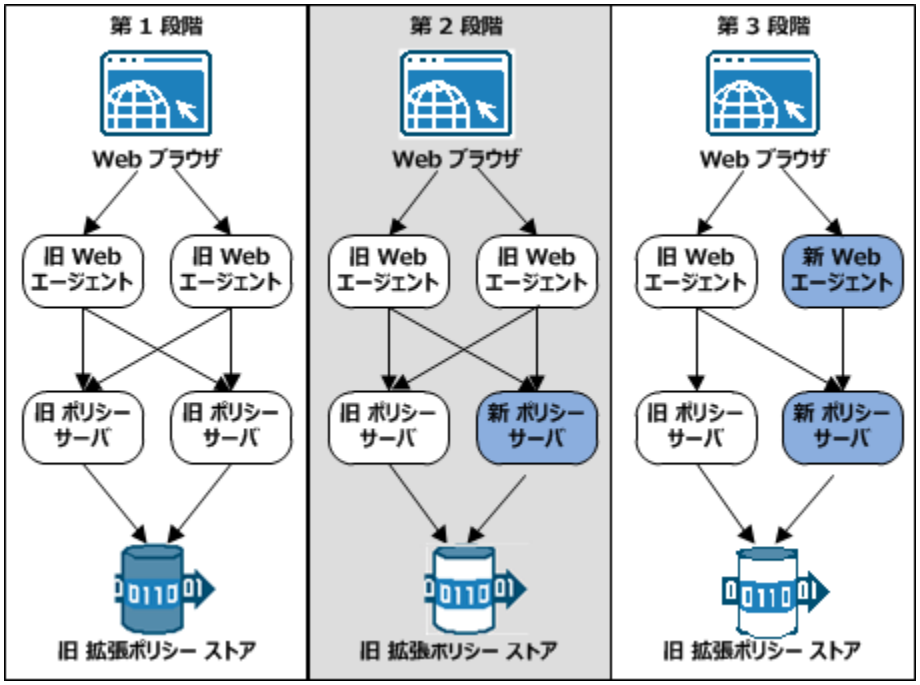
すべてのコンポーネントがアップグレードされるまで SiteMinder コンポーネントの削除およびアップグレードを続行するか、互換性のある混在モードで動作を続行します。

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 ストアを示しています。 このポリシー ストアにはキー ストアが含まれます。 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。

図 5: r6 SP5 移行。 第 1 段階～第 3 段階。



1. 第 1 段階で、r6.x ポリシー ストア スキーマが拡張されます。

   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。 12.52 SP1 の移行には、12.52 SP1 が必要とするオブジェクト用ポリシー ストアのポリシー ストア スキーマを拡張することが必要です。

   smkeydatabase を配置した場合は、最初のポリシー サーバをアップグレードする前にポリシー ストア スキーマを拡張します。 スキーマの拡張は、ポリシー サーバのアップグレード中に証明書データ ストアへの smkeydatabase 移行に対してポリシー ストアを準備します。 スキーマの拡張は互換モードに影響しません。 ポリシー ストアは、r6.x の場合と同様、引き続き機能します。

   smkeydatabase を配置しなかった場合は、ポリシー ストア アップグレード処理の一部としてスキーマを拡張します。

2. 第 2 段階では、r6.x ポリシー サーバが 12.52 SP1 にアップグレードされます。 12.52 SP1 ポリシー サーバは互換モードで動作します。 以下の点を考慮します。

   - r6.x Web エージェントは、12.52 SP1 ポリシー サーバと通信し続けます。
   - 12.52 SP1 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 ストアとの通信を継続します。 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。
   - 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削除されます。 12.52 SP1 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、12.52 SP1 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。

- 12.52 SP1 ポリシー サーバは、12.52 SP1 証明書データベースとのみ通信できます。 レガシー フェデレーション 環境をアップグレードしている場合、ポリシー サーバ インストーラにより既存の smkeydatabase コンテンツすべてが証明書データ ストアに移行するように試行されます。

  重要: smkeydatabase の移行が失敗した場合、ポリシー サーバを環境に戻さないでください。 移行が失敗した後でポリシー サーバを戻すと、証明書データを必要とするトランザクションはすべて失敗します。

3. 第 3 段階では、r6.x Web エージェントが 12.52 SP1 にアップグレードされます。 以下の点を考慮します。

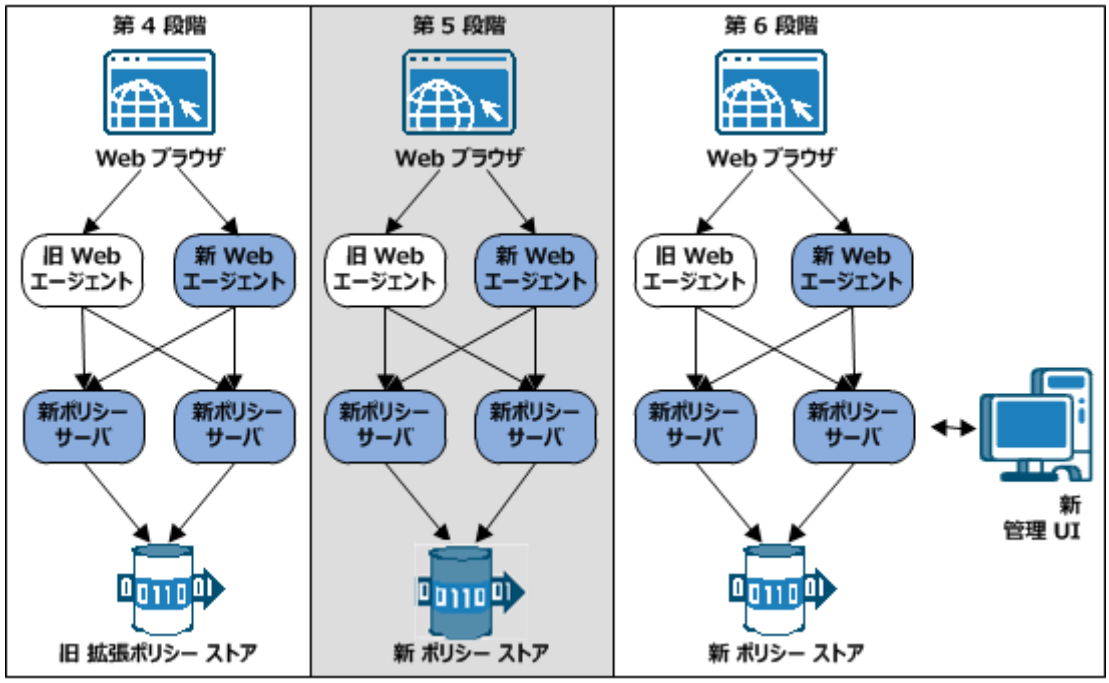
   - r6.x Web エージェントは、r6.x および 12.52 SP1 ポリシー サーバとの通信を継続します。
   - 12.52 SP1 Web エージェントは、12.52 SP1 ポリシー サーバのみと通信します。

     注: ポリシー ストアが 12.52 SP1 にアップグレードされない限り、12.52 SP1 ポリシー サーバで新規の 12.52 SP1 エージェントを設定できません。

4. 第 4 段階では、残りのポリシー サーバが 12.52 SP1 にアップグレードされます。 12.52 SP1 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: すべてのポリシー 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削除されました。 12.52 SP1 管理 UI をインストールするまで、ポリシー ストアのポリシー情報を管理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。

図 6: r6 SP^ 移行。 第 4 段階～第 6 段階。



5. 第 5 段階では、r6.x ポリシーおよびキー ストアが 12.52 SP1 にアップグレードされます。

6. 第 6 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。 以下の点を考慮します。
   - 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、混在モードの互換の一例として示されています。
7. （オプション）最終手順は、図には示されていませんが、レポート サーバのインストールおよび登録です。

r6.x から移行する方法

r6.x から 12.52 SP1 への移行を完了するには、以下の手順に従います。

1. 「*ポリシー サーバ リリース ノート*」のインストールおよびアップグレードの考慮事項を確認します。
2. ポリシー ストア スキーマ ファイルをダウンロードします。
3. r6.x ポリシー ストア スキーマを拡張します。
4. 使用する環境に複数の smkeydatabase インスタンスが含まれる場合は、それらを同期します。 ポリシー サーバのアップグレード時に、インストーラにより smkeydatabase 内のコンテンツすべてが証明書データ ストアに移行するように試行されます。
5. 「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。
6. r6.x ポリシー サーバを 12.52 SP1 にアップグレードします。
7. 「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。
8. r6.x Web エージェントを 12.52 SP1 にアップグレードします。
9. 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 12.52 SP1 にアップグレードします。
10. r6.x ポリシーおよびキー ストアを 12.52 SP1 にアップグレードします。

11. 12.52 SP1 管理 UI をインストールします。
12. （オプション）レポート サーバをインストールします。

    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。

ポリシーストア スキーマ ファイルのダウンロード

ポリシー ストア スキーマの拡張に必要なファイルは、ポリシー サーバのインストール zip のルートにあります。

12.52 SP1 のベース リリースにアップグレードする場合、次の手順に従ってください:

1. CA 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「SiteMinder」と入力し、Enter キーを押します。
4. ［Select a Product Page］リストの下の［Downloads］をクリックします。
5. ［Select a Product］リストの［Use］で特定の SiteMinder 製品を探し、ご使用の SiteMinder 製品を指定します。 名前をクリックします。
6. リリースと gen レベルを選択し、［Go］をクリックします。
7. ポリシー サーバのインストール zip をローカルに保存し、一時的な保存場所にキットを解凍します。

   ポリシー ストア スキーマ ファイルは policy_store_schema_ext.zip に含まれています。

12.52 SP1 の累積リリース（cr）にアップグレードする場合、次の手順に従ってください:

1. CA 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「SiteMinder」と入力し、Enter キーを押します。
4. ［Select a Product Page］リストの下の［Recommended Reading］をクリックします。

5. ［Recommend Reading］リスト内の［SiteMinder Hotfix/Cumulative Release Hot Index］をクリックします。
6. SiteMinder Web Access Manager をクリックします。
7. 使用する累積リリースをクリックします。
8. 累積リリースをダウンロードします。
9. ポリシー サーバのインストール zip をローカルに保存し、一時的な保存場所にキットを解凍します。

   ポリシー ストア スキーマ ファイルは policy_store_schema_ext.zip に含まれています。

ポリシー ストア スキーマの拡張

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。 12.52 SP1 の移行には、12.52 SP1 が必要とするオブジェクト用ポリシー ストアのポリシー ストア スキーマを拡張することが必要です。

smkeydatabase を配置した場合は、最初のポリシー サーバをアップグレードする前にポリシー ストア スキーマを拡張します。 スキーマの拡張は、ポリシー サーバのアップグレード中に証明書データ ストアへの smkeydatabase 移行に対してポリシー ストアを準備します。スキーマの拡張は互換モードに影響しません。ポリシー ストアは、r6.x の場合と同様、引き続き機能します。

smkeydatabase を配置しなかった場合は、ポリシー ストア アップグレード処理の一部としてスキーマを拡張します。

Active Directory サーバ用のポリシー ストア スキーマの拡張

次の手順に従ってください:

1. ポリシー サーバ ホスト システムに以下の zip ファイルをコピーし、それを一時的な保存場所に解凍します。

   `policy_store_schema_ext.zip`
2. 以下のディレクトリに移動します。

   `schema_extension¥db¥Active Directory`

3. ActiveDirectory.ldif ファイルを開き、ポリシー ストア スキーマの場所を表す DN（ドメイン名）で <RootDN> の各インスタンスを手動で置き換えます。 ポリシー ストア オブジェクトの場所は使用しません。

   例： 以下のルート DN がポリシー ストア オブジェクトを表す場合、

   `ou=policystore,dc=domain,dc=com`

   <RootDN> の各インスタンスを以下の DN で置き換えます。

   `dc=domain,dc=com`

4. ファイルを保存します。
5. コマンド ウィンドウから *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。

6. 以下のコマンドを実行します。

   `smldapsetup ldmod -f`*`path`*`/ActiveDirectory.ldif`

   path

   スキーマ ファイルへのパスを指定します。

   ポリシー ストア スキーマが拡張されます。

Active Directory LDS サーバ用のポリシー ストア スキーマの拡張

次の手順に従ってください:

1. ポリシー サーバ ホスト システムに以下の zip ファイルをコピーし、それを一時的な保存場所に解凍します。

   `policy_store_schema_ext.zip`

2. 以下のディレクトリに移動します。

   `schema_extension¥db¥Active Directory LDS`

3. ADLDS.ldif ファイルを開き、{guid} の各インスタンスを、かっこで囲まれた guid の実際の値で置き換えます。

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

4. ファイルを保存します。
5. コマンド ウィンドウから *siteminder_home*/bin に移動します。

   siteminder_home

   ポリシー サーバ インストール パスを指定します。

6. 以下のコマンドを実行します。

   ```
   smldapsetup ldmod -fpath/ADLDS.ldif
   ```

   path

   スキーマ ファイルへのパスを指定します。

   ポリシー ストア スキーマが拡張されます。

CA ディレクトリ サーバ用のポリシー ストア スキーマの拡張

次の手順に従ってください:

1. CA ディレクトリ ホスト システムに以下の zip ファイルをコピーし、一時的な保存場所にそれを解凍します。

   ```
   policy_store_schema_ext.zip
   ```

2. 以下のディレクトリに移動します。

   ```
   schema_extension¥db¥CA Directory
   ```

3. 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
   ```

4. 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"
   ```

5. 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 ディレクトリ 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従って、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;
```

6. DSA のデフォルト DXC ファイル（default.dxc）を開き、以下のセクションを探します。

```
# 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。

7. 以下の設定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。

8. JXplorer を使用して、ポリシー ストア DSA にアクセスします。
9. ルート エレメントを探し、次に、以下のベース ツリー構造を探します。

   Netegrity、SiteMinder、PolicySvr4

10. 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

11. 以下のコマンドで DSA（DSA ユーザとして）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ます。

IBM DB2 サーバ用のポリシーストア スキーマの拡張

次の手順に従ってください:

1. IBM DB2 ホスト システムに以下の ZIP ファイルをコピーし、一時的な保存場所にそれを解凍します。

   policy_store_schema_ext.zip

2. 以下のディレクトリに移動します。

   schema_extension¥db¥IBM DB2

3. 以下のファイルを見つけます。
   DB2.sql

4. 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。
   db2 -td@ [-v] -f *path*¥DB2.sql

   path

   DB2 設定ファイルへのパスを指定します。

   ポリシー ストア スキーマが拡張されます。

IBM Tivoli Directory Server 用のポリシー ストア スキーマの拡張

次の手順に従ってください:

1. IBM Tivoli Directory Server 管理ツールを使用してポリシー ストアのベース ツリー構造を更新します。
   ou=Netegrity,ou=SiteMinder,ou=PolicySvr4 の下に、以下のルート ノードを作成します。

   ou=XPS

2. IBM Directory Server ホスト システムに以下の zip ファイルをコピーし、一時的な保存場所にそれを解凍します。

   policy_store_schema_ext.zip

3. 以下のディレクトリに移動します。

   schema_extension¥db¥IBM Tivoli Directory Server

4. 以下のファイルを見つけます。

   IBMDirectoryServer.ldif

5. IBM Directory Server 構成ツールを使用して、スキーマ設定の［Manage Schema Files］セクションに以下のファイルを追加します。

   IBMDirectoryServer.ldif

6. ディレクトリ サーバを再起動します。

   ポリシー ストア スキーマが拡張されます。

Novell eDirectory サーバ用のポリシー ストア スキーマの拡張

次の手順に従ってください:

1. ポリシー サーバ ホスト システムに以下の zip ファイルをコピーし、それを一時的な保存場所に解凍します。

   policy_store_schema_ext.zip

2. 以下のディレクトリに移動します。

   schema_extension¥db¥Novell eDirectory

3. 以下のファイルを見つけて、開きます。

   Novell.ldif

4. コマンド ウィンドウから *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。

5. 以下のコマンドを実行します。

   ldapsearch -h*host* -p*port* -b*container* -s*sub* -D*AdminDN* -w*AdminPW* objectclass=ncpServer dn

   例：

   ldapsearch -h*192.168.1.47* -p*389* -b*o=nwqa47container* -s*sub* -d*cn=admin,o=nwqa47container* -w*password* objectclass=ncpServer dn

   Novell サーバ DN が表示されます。

6. 表示されたスキーマ ファイルを編集します。 すべての <ncpserver> 変数を Novell サーバ DN（ドメイン名）の値に置き換えます。

   例： Novell サーバ DN の値が cn=servername,o=servercontainer の場合は、<ncpserver> のすべてのインスタンスを以下の値に置き換えます。

   ```
   cn=servername,o=servercontainer
   ```

7. スキーマ ファイルを保存して閉じます。
8. 以下のコマンドを実行します。

   ```
   smldapsetup ldmod -fpath¥Novell.ldif
   ```

   -f*path*

   スキーマ ファイルへのパスを指定します。

   ポリシー ストア スキーマが拡張されます。

OpenLDAP サーバ用のポリシー ストア スキーマの拡張

次の手順に従ってください:

注: この手順は、OpenLDAP サーバが /usr/local/etc/openldap にあり、スキーマ ファイルが schema サブディレクトリにあることを前提としています。

1. ポリシー ストアのベース ツリー構造を更新します。
   ou=Netegrity,ou=SiteMinder,ou=PolicySvr4 の下に、以下のルート ノードを作成します。

   ```
   ou=XPS
   ```

2. OpenLDAP ホスト システムに以下の zip ファイルをコピーし、一時的な保存場所にそれを解凍します。

   ```
   policy_store_schema_ext.zip
   ```

3. 以下のディレクトリに移動します。

   ```
   schema_extension¥db¥OpenLDAP
   ```

4. 以下のスキーマ ファイルを見つけます。

   ```
   openldap_attribute_XPS.schema
   openldap_object_XPS.schema
   ```

5. OpenLDAP インストール ディレクトリ内のスキーマ フォルダに、手順 4 で見つけたスキーマ ファイルをコピーします。

6. slapd 構成ファイルの include セクションに、以下のエントリを入力します。

```
....
.....
include /usr/local/etc/openldap/schema/openldap_attribute_XPS.schema
include /usr/local/etc/openldap/schema/openldap_object_XPS.schema
```

ポリシー ストア スキーマが拡張されます。

Oracle Internet Directory Server 用のポリシー ストア スキーマの拡張

次の手順に従ってください:

1. Oracle Internet Directory ホスト システムにログインします。
2. Oracle カタログ コマンド ライン ツールを使用して、以下の属性にインデックスを付けます。 属性にインデックスを付けることで、デフォルトのポリシー ストア オブジェクトをインポートする際のエラー発生を防止します。

   `modifyTimestamp`

   以下のコマンドを実行します。

   oracle_home`/ldap/bin/catalog connect=`*conn_str* `add=TRUE attribute=modifyTimestamp`

   oracle_home

   Oracle Internet Directory のインストール パスを指定します。

   conn_str

   ディレクトリ データベース接続文字列を指定します。 tnsnames.ora ファイルを設定している場合、ファイルに指定されたネット サービス名を入力します。

   注: カタログ コマンド ライン ツールの詳細については、Oracle ドキュメントを参照してください。
3. ポリシー サーバ ホスト システムに以下の zip ファイルをコピーし、それを一時的な保存場所に解凍します。

   `policy_store_schema_ext.zip`
4. 以下のディレクトリに移動します。

   `schema_extension¥db¥Oracle Internet Directory`

5. 以下のファイルを見つけます。

   OID_10g.ldif

6. コマンド ウィンドウから *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。

7. 以下のコマンドを実行します。

   ldapmodify -h*host* -p*port* -d*AdminDN* -w*AdminPW*
   -c -f*path*¥OID_10g.ldif
   -Z -P*cert*

   -h*host*

   LDAP ディレクトリ サーバの IP アドレスを指定します。

   例： 123.123.12.12

   -p*port*

   LDAP ディレクトリ サーバのポート番号を指定します。

   例： 3500

   -d*AdminDN*

   LDAP スキーマを作成する権限を持つ LDAP ユーザの名前を指定します。

   -w*AdminPW*

   -d オプションで指定する管理者のパスワードを指定します。

   -c

   連続モードを指定します（エラーで停止しません）。

   -f*path*

   解凍したスキーマ ファイルへのパスを指定します。

   -Z

   SSL で暗号化される接続を指定します。

-P*cert*

SSL クライアント証明書データベースファイル（cert7.db）があるディレクトリのパスを指定します。

例：

cert7.db が app/siteminder/ssl に存在する場合は、以下を指定します。

```
-Papp/siteminder/ssl
```

ポリシー ストア スキーマが拡張されます。

Red Hat Directory Server 用のポリシー ストア スキーマの拡張

次の手順に従ってください:

1. ポリシー サーバ ホスト システムに以下の zip ファイルをコピーし、それを一時的な保存場所に解凍します。

   ```
   policy_store_schema_ext.zip
   ```

2. 以下のディレクトリに移動します。

   ```
   schema_extension¥db¥Red Hat Directory Server
   ```

3. 以下のファイルを見つけます。

   ```
   RedHat_7_1.ldif
   ```

4. コマンド ウィンドウから *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。

5. 以下のコマンドを実行します。

   ```
   smldapsetup ldmod -fpath/RedHat_7_1.ldif
   ```

   path

   解凍したスキーマ ファイルへのパスを指定します。

   ポリシー ストア スキーマが拡張されます。

Siemens DirX Server 用のポリシー ストア スキーマの拡張

次の手順に従ってください:

1. DirXmanage ツールを使用してポリシー ストアのベース ツリー構造を更新します。 以下の既存のルート パスで

   `ou=Netegrity、ou=SiteMinder、ou=PolicySvr4`

   以下のルート ノードを作成します。

   `ou=XPS`

2. zip ファイル、policy_store_schema_ext.zip を Siemens DirX ホスト システムにコピーし、以下の 一時的な保存場所にそれを解凍します。

3. 以下のディレクトリに移動します。

   `schema_extension¥db¥Siemens DirX`

4. 以下の解凍したファイルを見つけ、それらを *DirX_install_path*¥scripts¥security¥Netegrity¥SiteMinder にコピーします。

   - bind.tcl
   - GlobalVar.tcl
   - l-bind.cp
   - schema_ext_for_XPS.adm

   DirX_install_path

   DirX のインストール パスを指定します。

   例： C:¥program files¥siemens¥dirx

5. 解凍したファイル dirxabbr-ext.XPS を見つけ、それを *DirX_install_path*¥client¥conf にコピーします。

6. DirX サービスを停止し、再起動します。

7. GlobalVar.tcl ファイルを編集して、DirX スクリプトが参照するグローバル変数を更新します。

   デフォルト値：

   - LDAP ポート： 389
   - ルート DN： o=pqr

- 管理者ユーザ名： cn=admin、o=pqr
- 管理者パスワード： dirx

注: 値を修正して、それらの値が既存のセットアップに適用されるようにします。

8. *DirX_install_path*¥scripts¥security¥CA¥SiteMinder に移動します。
9. 以下のコマンドを実行します。

   ```
   dirxadm schema_ext_for_XPS.adm
   ```

10. DirXmanage ユーティリティを使用して、DSA に再バインドします。

    注: エラーに注意してください。

    ポリシー ストア スキーマが拡張されます。

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

次の手順に従ってください:

1. ポリシー サーバ ホスト システムに以下の zip ファイルをコピーし、それを一時的な保存場所に解凍します。

   ```
   policy_store_schema_ext.zip
   ```

2. 以下のディレクトリに移動します。

   ```
   schema_extension¥db¥Sun Java System Directory Server
   ```

3. 以下のファイルを見つけます。

   ```
   OracleDirectoryServer.ldif
   ```

4. コマンド ウィンドウから *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。

5. 以下のコマンドを実行します。

   ```
   smldapsetup ldmod -fpath¥OracleDirectoryServer.ldif
   ```

   -f*path*

   解凍したスキーマ ファイルへのパスを指定します。

   ポリシー ストア スキーマが拡張されます。

Microsoft SQL Server 用のポリシー ストア スキーマの拡張

次の手順に従ってください:

1. SQL Server ホスト システムに以下の zip ファイルをコピーし、一時的な保存場所にそれを解凍します。

   `policy_store_schema_ext.zip`

2. 以下のディレクトリに移動します。

   `schema_extension¥db¥Microsoft SQL Server`

3. 以下のファイルを見つけます。

   `SQLServer.sql`

4. 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。

5. クエリ アナライザを起動します。

6. 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。

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

8. スキーマをクエリに貼り付け、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ます。

MySQL サーバ用のポリシー ストア スキーマの拡張

次の手順に従ってください:

1. MySQL ホスト システムに以下の zip ファイルをコピーし、一時的な保存場所にそれを解凍します。

   `policy_store_schema_ext.zip`

2. 以下のディレクトリに移動します。

   `schema_extension¥db¥MySQL`

3. 以下のファイルを見つけます。

   `MySQL.sql`

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

5. クエリへファイルの内容を貼り付けます。
6. クエリを実行する MySQL コマンド ライン ツールを使用します。

   ポリシー ストア スキーマが拡張されます。

Oracle サーバ用のポリシー ストア スキーマの拡張

次の手順に従ってください:

1. Oracle ホスト システムに以下の zip ファイルをコピーし、一時的な保存場所にそれを解凍します。

   `policy_store_schema_ext.zip`
2. 以下のディレクトリに移動します。

   `schema_extension¥db¥Oracle`
3. 以下のファイルを見つけます。

   `Oracle.sql`
4. ポリシー ストア データベースを管理するユーザとして、sqlplus または別の Oracle ユーティリティで Oracle サーバにログインします。

   注: SYS ユーザや SYSTEM ユーザで 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、SMOWNER などの Oracle ユーザを作成し、そのユーザでスキーマを作成します。
5. r6.x データベースのインスタンスにファイルをインポートします。

   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。

   ポリシー ストア スキーマが拡張されます。

キー データベース インスタンスの同期

新バージョンへの移行を開始する前に smkeydatabase インスタンスをすべて同期します。

注: smkeytool ユーティリティを使用して、smkeydatabases を同期し、smkeydatabase インスタンス間でのデータの不整合をすべて解決します。smkeytool 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。

SiteMinder の旧バージョンでは、証明書データの格納にローカルな smkeydatabase を使用していました。 各ポリシー サーバにそれぞれの smkeydatabase が必要でした。バージョン 12.52 SP1 では、一元化された証明書データ ストアがローカルな smkeydatabases に置き換えられています。

ポリシー サーバのアップグレードの一部として、インストーラは自動的にローカル smkeydatabase をバックアップし、証明書データ ストアにコンテンツをすべて移行しようとします。 このプロセスのなかで、移行開始前に両方のストアが比較されます。

重要: smkeydatabase の移行が失敗した場合、ポリシー サーバを環境に戻さないでください。 移行が失敗した後でポリシー サーバを戻すと、証明書データを必要とするトランザクションはすべて失敗します。

smkeydatabases におけるデータの整合性を確認および解決するために、以下のガイドラインを使用します。

- 認証機関-の各証明書が、すべてのインスタンスの証明書破棄リストを参照することを確認する。

  例： 証明機関-の証明書は、LDAP ディレクトリ サービス内の証明書失効リストを一貫して参照します。
- すべてのインスタンスで defaultentpriseprivatekey エイリアスが同じ秘密キー/証明書のペアを表すことを確認する。
- 同じエイリアスが同一の証明書またはキー/証明書に対応することを確認する。
- 同じ認証機関-の証明書が同一の証明書廃棄リストに対応することを確認する。
- 無効または有効期限が切れている証明書が存在しないことを確認する。
- すべての CRL 情報が有効であることを確認する。

重要: データの不整合をすべて解決した後も、移行がすべて完了するまで smkeydatabase を変更しないことをお勧めします。

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。

- 環境に複数の smkeydatabase インスタンスが含まれる場合は、必ずコンテンツをすべて同期します。同期することで不整合なデータを処理し、ポリシー サーバ インストーラがコンテンツを証明書データ ストアに移行できない問題を防ぎます。
- （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。
- 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インスタンスをすべてシャットダウンします。
- アップグレード中に、既存のポリシー ストアを保持しておくために、設定ウィザードでポリシー ストア チェック ボックスをオフのままにしておきます。 ただし、設定ウィザードによって、Advanced Authentication Server 用の暗号化キーの入力を促されます。このキーは各ポリシー サーバに格納されますが、すべてのポリシー サーバで同じキーが必要です。
- （UNIX）ポリシー サーバをアップグレードするユーザ アカウントは、インストール メディアが含まれるディレクトリに対して実行権限を持っている必要があります。ユーザ アカウントにこれらの権限がない場合は、以下のコマンドを実行します。

  ```
  chmod +x installation_media
  ```

  installation_media

  ポリシー サーバのインストール実行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。

必要とされる Linux ライブラリ

Linux オペレーティング環境上で動作するコンポーネントには、特定のライブラリ ファイルが必要です。 正しいライブラリをインストールしないと、以下のエラーを引き起こす場合があります。

```
java.lang.UnsatisfiedLinkError
```

このコンポーネントの Linux バージョンをインストール、設定、またはアップグレードする場合は、ホスト システム上で以下のパッケージが必要になります。

Red Hat 5.x

- compat–gcc-34-c++-3.4.6-*patch_version*.l386
- libstdc++-4.x.x-x.el5.i686.rpm
- libidn.so.11.rpm
- ncurses

Red Hat 6.x

- libstdc++-4.x.x-x.el6.i686.rpm
- libidn-1.18-2.el6.i686
- libXext.i686.rpm
- libXrender.i686.rpm
- linXtst.i686.rpm
- libidn.so.11.rpm
- ncurses

Red Hat 6.x（64 ビット）の場合はさらに以下：

注: 64 ビット Red Hat 6.x に必要な RPM パッケージはすべて、*32* ビットのパッケージです。

- libXau-1.0.5-1.el6.i686.rpm
- libxcb-1.5-1.el6.i686.rpm
- compat-db42-4.2.52-15.el6.i686.rpm
- compat-db43-4.3.29-15.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm
- libXrender-0.9.5-1.el6.i686.rpm
- libexpat.so.1（expat-2.0.1-11.el6_2.i686.rpm により提供）
- libfreetype.so.6（freetype-2.3.11-6.el6_2.9.i686.rpm により提供）
- libfontconfig.so.1（fontconfig-2.8.0-3.el6.i686.rpm により提供）
- libICE-1.0.6-1.el6.i686.rpm
- libuuid-2.17.2-12.7.el6.i686.rpm
- libSM-1.1.0-7.1.el6.i686.rpm
- libXext-1.1-3.el6.i686.rpm
- compat-libstdc++-33-3.2.3-69.el6.i686.rpm
- compat-db-4.6.21-15.el6.i686.rpm
- libXi-1.3-3.el6.i686.rpm
- libXtst-1.0.99.2-3.el6.i686.rpm
- libXft-2.1.13-4.1.el6.i686.rpm
- libXt-1.0.7-1.el6.i686.rpm

- libXp-1.0.0-15.1.el6.i686.rpm
- libstdc++.i686.rpm
- compat-libtermcap.rpm
- libidn.i686.rpm
- ncurses

Linux 上で Korn シェル（ksh）パッケージが必要

Linux プラットフォームでのポリシー サーバのインストールおよびアップグレードに、ksh Korn シェルが必要です。ユーザの Linux 環境に適したバージョンがインストールされていることを確認します。

Red Hat 5.x（32 ビット）

ksh-20100621-12.el5.i386.rpm

Red Hat 5.x（64 ビット）

ksh-20100621-12.el5.x86_64.rpm

Red Hat 6.x（32 ビット）

ksh-20100621-16.el6.i686.rpm

Red Hat 6.x（64 ビット）

ksh-20100621-16.el6.x86_64.rpm

Windows

次の手順に従ってください:

1. 実行中のすべてのアプリケーションを終了します。
2. アップグレードするポリシー サーバを停止します。
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ファイルを指定します。
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、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
     - 環境に対して以前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。

- アップグレード中に、既存のポリシー ストアを保持しておくために、設定ウィザードでポリシー ストア チェック ボックスをオフのままにしておきます。 既存のポリシー ストアを手動でアップグレードします。 ただし、設定ウィザードによって、Advanced Authentication Server 用の暗号化キーの入力を促されます。 このキーは各ポリシー サーバに格納されますが、すべてのポリシー サーバで同じキーが必要です。
- 別の（n 番目の）ポリシー サーバをアップグレードしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。

- インストーラは smkeydatabase を検出すると、以下を実行します。
  - smkeydatabase をバックアップする。
  - 証明書データ ストアへのコンテンツの移行を試行する。

  重要: smkeydatabase の移行が失敗した場合、ポリシー サーバを環境に戻さないでください。 移行が失敗した後でポリシー サーバを戻すと、証明書データを必要とするトランザクションはすべて失敗します。
- 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。

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。
6. アップグレードしているポリシー サーバに対して、Advanced Authentication Server を有効にします。

UNIX GUI

次の手順に従ってください:

1. 実行中のすべてのアプリケーションを終了します。
2. アップグレードするポリシー サーバを停止します。
3. 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: ピリオドの間に必ずスペースを入れてください。
4. 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。

5. 以下のコマンドを入力します。

   ./installation_media

   installation_media

   ポリシー サーバのインストール実行ファイルを指定します。

6. 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。
     - アップグレード中に、既存のポリシー ストアを保持しておくために、設定ウィザードでポリシー ストア チェック ボックスをオフのままにしておきます。 既存のポリシー ストアを手動でアップグレードします。 ただし、設定ウィザードによって、Advanced Authentication Server 用の暗号化キーの入力を促されます。 このキーは各ポリシー サーバに格納されますが、すべてのポリシー サーバで同じキーが必要です。
       - 別の（n 番目の）ポリシー サーバをアップグレードしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
   - インストーラは smkeydatabase を検出すると、以下を実行します。
     - smkeydatabase をバックアップする。
     - 証明書データ ストアへのコンテンツの移行を試行する。

     重要: smkeydatabase の移行が失敗した場合、ポリシー サーバを環境に戻さないでください。 移行が失敗した後でポリシー サーバを戻すと、証明書データを必要とするトランザクションはすべて失敗します。
   - 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。

7. 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。

8. ［終了］をクリックします。
9. 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: ピリオドの間に必ずスペースを入れてください。
10. アップグレードしているポリシー サーバに対して、Advanced Authentication Server を有効にします。

UNIX コンソール

次の手順に従ってください:

1. 実行中のすべてのアプリケーションを終了します。
2. アップグレードするポリシー サーバを停止します。
3. 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: ピリオドの間に必ずスペースを入れてください。
4. 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。
5. 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ファイルを指定します。
6. 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に、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。

- アップグレード中に、既存のポリシー ストアを保持しておくために、設定ウィザードでポリシー ストア チェック ボックスをオフのままにしておきます。 既存のポリシー ストアを手動でアップグレードします。 ただし、設定ウィザードによって、Advanced Authentication Server 用の暗号化キーの入力を促されます。 このキーは各ポリシー サーバに格納されますが、すべてのポリシー サーバで同じキーが必要です。
- 別の（n 番目の）ポリシー サーバをアップグレードしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。

- インストーラは smkeydatabase を検出すると、以下を実行します。
  - smkeydatabase をバックアップする。
  - 証明書データ ストアへのコンテンツの移行を試行する。

  重要: smkeydatabase の移行が失敗した場合、ポリシー サーバを環境に戻さないでください。 移行が失敗した後でポリシー サーバを戻すと、証明書データを必要とするトランザクションはすべて失敗します。

7. 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。

8. Enter キーを押します。
9. ［終了］をクリックします。
10. 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: ピリオドの間に必ずスペースを入れてください。

11. アップグレードしているポリシー サーバに対して、Advanced Authentication Server を有効にします。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべて*オフ*のままにします。
3. ［次へ］をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。

   注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

   Advanced Authentication Server が有効になります。

カスタマイズされたファイルの変更

ポリシー サーバのアップグレード中に、インストーラは特定のファイルの新規バージョンを作成します。 インストーラは、*policy_server_home*/config ディレクトリに、以下のファイルを作成します。

- conapi.conf
- JVMOptions.txt
- profiler_templates
- siteminder.conf
- SMocsp.sample.conf
- SmSWEC.cfg
- smtracedefault.txt
- snmp.conf
- snmptrap.conf
- trace.conf

インストーラは、*policy_server_home*/properties ディレクトリに、以下のファイルを作成します。

- AMAssertionGenerator.properties
- AssertionGeneratorFramework.properties
- cdslog4j.properties
- EntitlementGenerator.properties
- FederationAttributeConfig.properties
- InfoCard.properties
- JSAMLAssertionStrings.properties
- JSAMLProtocolStrings.properties
- log4j.properties
- LoggerConfig.properties
- logging.properties
- openformatexpression.conf
- scriptActiveExpConfig.properties
- smkeydatabase.properties
- WebServiceConfig.properties
- xsw.properties

これらの 12.52 SP1 ファイルは .new という拡張子を使用します。たとえば、旧バージョンからの JVMOptions.txt ファイルはそのままになります。インストーラは JVMOptions.txt ファイルの 12.52 SP1 バージョンを作成し、それは「JVMOPtions.new」と命名されます。

元のファイルにカスタマイズされた設定が含まれていた場合は、必ずカスタマイズされた設定で .new ファイルを変更します。 元のファイルの拡張子で .new ファイルの名前を変更します。

たとえば、JVMOptions.txt ファイル内にカスタム設定があった場合は、それらの変更を JVMOptions.txt.new へコピーします。 名前を JVMOptions.txt.new から JVMOptions.txt へ変更します。

サーバ側のカスタム コードの要件

ポリシー サーバのオペレーティング システムは、サーバ側のカスタム コードの再コンパイルが必要かどうかを判断します。 以下の表を使用して、要件を識別してください。

オペレーティング システム	必要ですか。
Microsoft Windows および UNIX	いいえ。カスタム コードの再コンパイルはオプションです。
Red Hat Linux	はい。 SDK をアップグレードし、GCC 3.4 を使用してカスタム コードを再コンパイルします。

ポリシー サーバ アップグレードのトラブルシュート

アップグレード中に問題が発生した場合、以下を参照します。

- *siteminder_home*¥siteminder¥install_config_info にあるポリシー サーバ インストール ログ ファイルを参照できます。

  siteminder_home

  ポリシー サーバのインストール パスを指定します。

- *siteminder_home*¥log にある smkeydatabase 移行ログ（smkeydatabaseMigration.log）を参照できます。

  注: ポリシー サーバのアップグレードと smkeydatabase の移行は別個のプロセスです。 smkeydatabase の移行が失敗しても、ポリシー サーバのアップグレードは失敗しません。

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。

r6.x Web エージェントのアップグレード

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、12.52 SP1 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 12.52 SP1 にアップグレードする前に、ポリシー サーバを 12.52 SP1 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 エージェントのアップグレード

12.52 SP1 Web エージェント インストーラを使用して、r6.x Web エージェントをアップグレードします。 以下の点を考慮します。

- オプション パック機能が必要なエージェントは、12.52 SP1 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 12.52 SP1 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。 12.52 SP1 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。

- Advanced Password Services を展開した場合、Web エージェント アップグレードは LANG（変換）ファイルおよび CFG（設定）ファイルをすべて保持してます。 ファイルのデフォルト 12.52 SP1 バージョンは *agent_home*¥samples にインストールされます。

  agent_home

  Web エージェントのインストール パスを指定します。

- r6 の起動スクリプトを使用していた場合、「nete_wa…」のインスタンスをすべて「ca_wa…」に置き換えます。

カスタム エージェントの要件

カスタム エージェントを再コンパイルする必要があるかどうかを判断するには、以下の表を使用します。

エージェント タイプ	必要ですか。
SiteMinder エージェント	オペレーティング システムによって異なります。 エージェントのオペレーティング システムのサポートが終了している場合、カスタム エージェントを再コンパイルする必要があります。 SiteMinder SDK をアップグレードし、サポートされているオペレーティング システム上でエージェントを再コンパイルします。
サードパーティ エージェント	ベンダーによって異なります。 エージェントがサポートされているかどうかを確認するには、サードパーティ ベンダーに問い合わせてください。

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 12.52 SP1 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 12.52 SP1 にアップグレードするには、2 つのパスがあります。 以下の操作を行うことができます。

- 既存のポリシーおよびキー ストアを 12.52 SP1 にアップグレードします。
- 12.52 SP1 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。

12.52 SP1 ポリシーおよびキー ストアに既存のポリシー ストアを移行する場合は、以下の手順に従います。

1. r6.x 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: 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. 12.52 SP1 ポリシーおよびキー ストアを作成します。

   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. 12.52 SP1 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 12.52 SP1 ポリシーおよびキー ストアにインポートします。

   注: 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 ストアのアップグレードのオプション

r6.x キー ストアを 12.52 SP1 にアップグレードするには、2 つのパスがあります。 以下の操作を行うことができます。

- 既存のポリシーおよびキー ストアを 12.52 SP1 にアップグレードします。
- スタンドアロンの 12.52 SP1 キー ストアを作成し、新規インスタンスに既存のエージェント キーをインポートします。

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。

スタンドアロンの 12.52 SP1 キー ストアを作成する場合、以下の手順を実行します。

1. ポリシー ストアに格納されるエージェント キーのみをエクスポートするために smobjexport の r6.x バージョンを使用します。

   注: 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. デフォルト ポリシー ストア スキーマを使用して、12.52 SP1 キー ストアを作成します。

   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. smobjimport の 12.52 SP1 バージョンを使用して、12.52 SP1 キー ストアにエージェント キーをインポートします。

   注: 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. ポリシー サーバ管理コンソールを使用して、スタンドアロンのキー ストアにポリシー サーバを示します。

   注: 詳細については、ポリシー サーバ管理コンソールのヘルプ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

r6.x ポリシー ストアを 12.52 SP1 にアップグレードするには、以下の手順に従います。

1. ポリシー ストアと通信しているすべてのポリシー サーバを停止します。
2. ポリシー サーバのアップグレード中に smkeydatabase 移行のためにポリシー ストア スキーマを拡張しなかった場合は、スキーマを拡張します。
3. ポリシー ストア データ定義をインポートします。
4. デフォルトのポリシー ストア オブジェクトをインポートします。

   注: レガシー フェデレーション 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。
5. FSS 管理 UI を使用して、r6.x レガシー フェデレーション 環境を管理している場合は、レガシー フェデレーション オブジェクトの移行を完了するために XPS スイーパ ユーティリティを実行します。
6. ポリシー ストアと通信しているすべてのポリシー サーバを開始します。

すべてのポリシー サーバの停止

ポリシー ストアと通信しているすべてのポリシー サーバを停止すると、アップグレード中のポリシー ストアの破損を防ぐのに役立ちます。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のいずれかの操作を実行します。
   - （Windows）
     a. ポリシー サーバ管理コンソールを開き、［停止］をクリックします。
     b. ［OK］をクリックしてコンソールを閉じます。

- （UNIX）以下の提供されたスクリプトを使用します。
  install_path/siteminder/stop-all

  install_path

  ポリシー サーバのインストール パスを指定します。

3. ポリシー ストアと通信している各ポリシー サーバに対して、この手順を繰り返します。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home*¥xps¥dd 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。

2. 以下のコマンドを実行します。

   XPSDDInstall SmMaster.xdd

   XPSDDInstall

   必要なデータ定義をインポートします。

デフォルトのポリシー ストア オブジェクトのインポート

デフォルトのポリシー ストア オブジェクトをインポートすると、管理 UI とポリシー サーバで使用するポリシー ストアが設定されます。

デフォルトのポリシー ストア オブジェクトは以下の XML ファイルにあります。

- smpolicy.xml
- smpolicy-secure.xml

smpolicy-secure.xml ファイルは smpolicy.xml ファイルより限定的なセキュリティ設定を提供します。 デフォルトのポリシー ストア オブジェクトをインポートするには、上記ファイルの *1* つのみを選択してください。

いずれのファイルも新規ポリシー ストアを設定し、既存のストアをアップグレードします。 アップグレードの一部としてインポートされた場合、ファイルは変更された既存のデフォルト オブジェクトを上書き *しません*。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト（ACO）テンプレート内のデフォルト セキュリティ設定が含まれます。

いずれのファイルをインポートしても、レガシー フェデレーション および Web サービス変数機能は利用可能になります。 これらの機能は別々にライセンスされています。 Web サービス変数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 アカウント担当者までお問い合わせください。

次の手順に従ってください:

1. コマンド ライン ウィンドウを開き、*siteminder_home*¥db に移動します。
2. 以下のファイルの *いずれか*をインポートします。
   - smpolicy.xml をインポートするには、以下のコマンドを実行します。

     ```
     XPSImport smpolicy.xml -npass
     ```

   - smpolicy-secure.xml をインポートするには、以下のコマンドを実行します。

     ```
     XPSImport smpolicy-secure.xml -npass
     ```

   -npass

   パスフレーズが必要ではないことを指定します。 デフォルト ポリシー ストア オブジェクトには暗号化されたデータが含まれていません。デフォルト ポリシー ストア オブジェクトのインポートにパスフレーズは不要です。

   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。

レガシー フェデレーション オブジェクトを 管理 UI で利用可能にする

ポリシー サーバ UI を使用して、フェデレーション セキュリティ サービス（レガシー フェデレーション）オブジェクトを管理している場合は、管理 UI にこれらのオブジェクトを移行するために XPS スイーパ ユーティリティを実行します。

次の手順に従ってください:

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て、管理 UI に対して レガシー フェデレーション オブジェクトを利用可能にします。

   XPSSweeper

   ポリシー サーバ UI を使用して作成された レガシー フェデレーションはすべて、管理 UI で利用可能です。

   アップグレード処理の次の段階に進む準備ができたら、管理 UI をアップグレードします。

すべてのポリシー サーバの起動

すべてのポリシー サーバを開始すると、すべてのポリシー サーバとアップグレードされたポリシー ストアの間の通信が再開します。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のいずれかの操作を実行します。
   - （Windows）
     a. ポリシー サーバ管理コンソールを開き、［開始］をクリックします。
     b. ［OK］をクリックしてコンソールを閉じます。
   - （UNIX）以下の提供されたスクリプトを使用します。
     install_path/siteminder/start-all

     install_path

     ポリシー サーバのインストール パスを指定します。
3. ポリシー ストアと通信している各ポリシー サーバに対して、この手順を繰り返します。

ポリシー ストアがアップグレードされます。

r6.x からの移行での管理ユーザ 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。 12.52 SP1 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。

r6.x セッション ストアのアップグレード

セッション ストアのアップグレードは必須ではありません。 12.52 SP1 セッション ストア スキーマは、r6.0 SP5 以降変更されていません。

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 12.52 SP1 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 12.52 SP1 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。

r6.x 並行アップグレードの仕組み

既存の r6.x 環境を 12.52 SP1 に移行する必要はありません。 代わりに、既存の展開との並行 12.52 SP1 環境を設定できます。

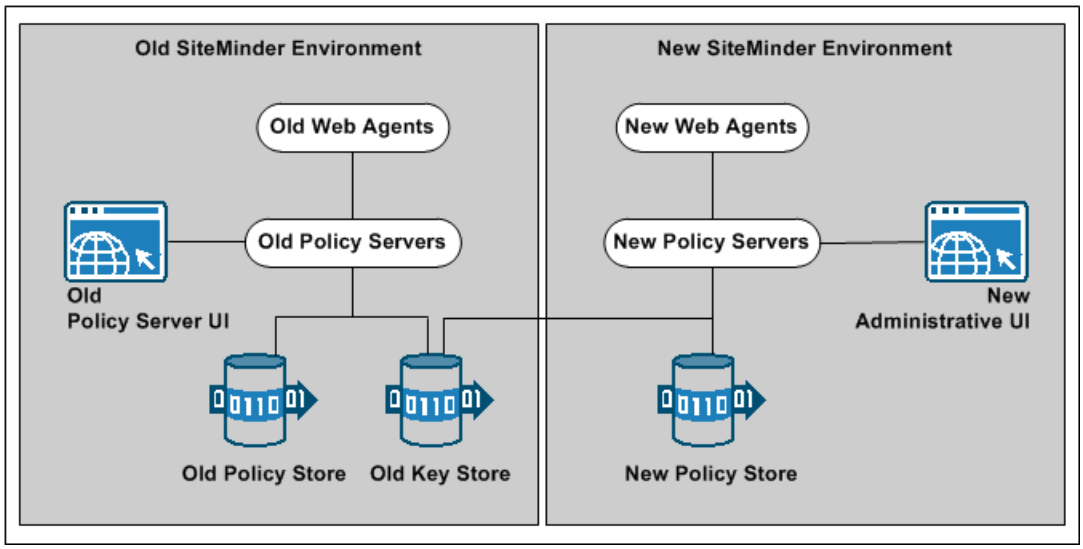
以下の図は、単純な並列アップグレードおよび詳細を示しています。

- 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 12.52 SP1 環境。

- 12.52 SP1 ポリシー ストアの SiteMinder オブジェクトの管理に使用される 12.52 SP1 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。

図 7: r6.x 並行アップグレードの概要



r6.x 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. 12.52 SP1 環境を作成します。
3. 以下のいずれかの操作を実行します。
   - 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. ユーザの r6.x 環境に smkeydatabases が含まれる場合、以下を実行します。
   a. すべてのインスタンスを同期する。
   b. 12.52 SP1 証明書データ ストアに smkeydatabase のコンテンツを移行する。
5. r6.x 環境で レガシー フェデレーション （フェデレーション セキュリティ サービス）オブジェクトを管理している場合は、アサーション発行者 ID を移行します。
6. （オプション）r6.x ポリシー ストア データを移行します。
7. 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 12.52 SP1 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。
- 12.52 SP1 ポリシー ストアに接続する 12.52 SP1 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 ストアを使用することにより、すべてのポリシー サーバに関連付けられる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。

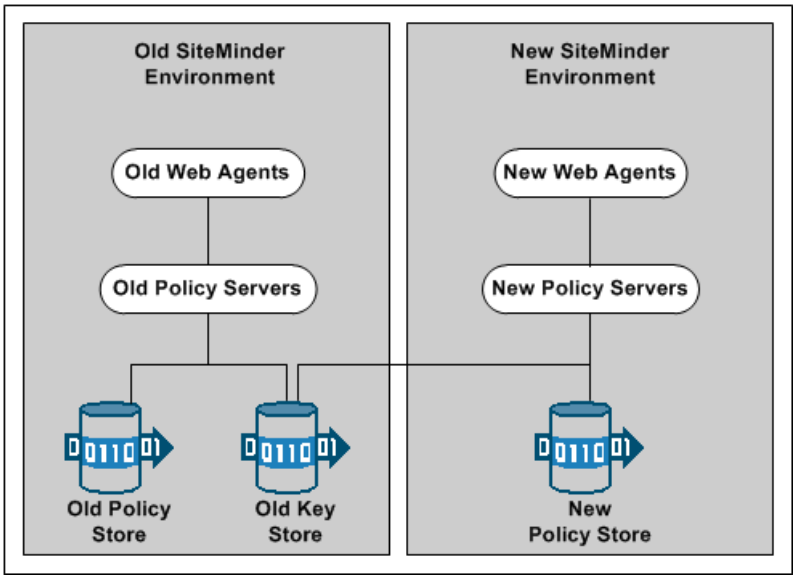
- 共通キー ストアに接続して新しいキーを取得するすべてのポリシー サーバ。

  重要: 12.52 SP1 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、12.52 SP1 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、フェールオーバ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。

図 8: r6.x の共通キー ストアの展開



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、12.52 SP1 ポリシー サーバはキー ロールオーバーに 12.52 SP1 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。

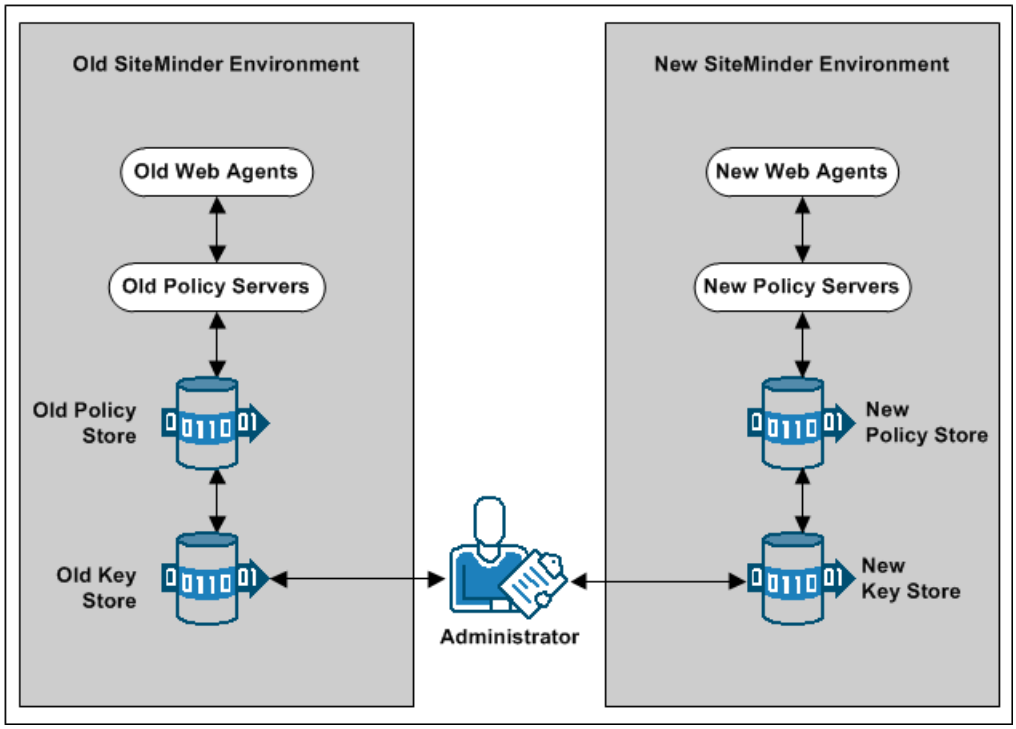
12.52 SP1 ポリシー ストアに接続する 12.52 SP1 ポリシー サーバ。

- 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。
- 12.52 SP1 キー ストアに接続して新しいキーを取得する 12.52 SP1 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 12.52 SP1 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 12.52 SP1 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、フェールオーバ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。

図9: r6.x の複数キー ストアの展開



12.52 SP1 環境の作成

既存の環境から独立した 12.52 SP1 環境を設定できます。 12.52 SP1 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。 12.52 SP1 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。
  - r6.x 環境で別個にキー ストアが設定されている場合は、キー ストアのバージョンを r6.x のままにします。12.52 SP1 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 12.52 SP1 キー ストアと通信できません。
  - ポリシーとキー ストアが連結して設定されている r6.x 環境の場合、r6.x キーを別個の r6.x キー ストアに分けます。
- 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。12.52 SP1 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。

ポリシー ストアからキー ストアを分ける方法

ポリシー ストアからキー ストアを分けるには、以下の手順を実行します。

1. セットアップ ポリシー サーバをインストールするか、見つけます。セットアップ ポリシー サーバは、ポリシーとキー ストアが連結して設定されないポリシー サーバのことです。
   - ポリシーとキー ストアが連結して設定されているポリシー サーバの場合、それを使用して新しいキー ストア インスタンスを設定できません。ポリシー サーバ ホスト システムで利用できる必要な SiteMinder ユーティリティは、連結したストアを管理するように設定されます。
   - セットアップ ポリシー サーバは、必要なユーティリティの個別のセットを利用可能にします。個別のセットを使用することにより、連結されたストアを妨げずにキー ストアを設定できます。
2. セットアップ ポリシー サーバ ホスト システムを使用して、個別の r6.x キー ストア インスタンスを作成します。 以下の点を考慮します。
   - キー ストアはデフォルトのポリシー ストア スキーマのみを必要とします。デフォルトのポリシー ストア スキーマのインポートに関する詳細については、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。
   - キー ストアについては、以下の処理は不要です。
     - SiteMinder スーパーユーザ パスワードを設定します。
     - デフォルトのポリシー ストア オブジェクトをインポートします。

3. r6.x 環境で動的エージェント キー生成を無効にします。

   注: 利用している環境がスタティック キーを使用する場合、この手順は必要ありません。ただし、ポリシー ストアからキーをエクスポートした後 SiteMinder 管理者がランダムなエージェント キーを生成しないことを確認してください。

4. r6.x ポリシー/キー ストアからエージェント キーをエクスポートします。
5. r6.x キー ストアにエージェント キーをインポートします。
6. すべてのポリシー サーバを設定して、個別のキー ストアを使用します。
7. 動的エージェント キーの生成を無効にした場合は、それを再度有効にします。

動的エージェント キー生成の無効化

キー ストアの個別化を完了していない場合、r6.x 環境では以下のように 2 種類のキー ストアで動作しています。

- 一部のポリシー サーバは連結されたポリシー/キー ストアでエージェント キーを使用します。
- 一部のポリシー サーバは個別のキー ストアでエージェント キーを使用します。

動的エージェント キーの生成を無効にすると、個別のストアに対してエクスポートした後、ポリシー サーバがキーを生成しません。ポリシー サーバがキーを生成しないと、キーがすべてのストアで同期されない場合に生じるシングル サインオンの問題を回避します。

以下の手順に従います。

1. r6.x ポリシー サーバのユーザ インターフェースにログインします。
2. ［ツール］-［キーの管理］を選択します。
3. ［スタティック エージェント キーを使用］オプションを選択します。
4. ［Apply］をクリックします。

   ポリシー サーバはスタティック キーを使用するように設定されます。ポリシー サーバはキーを自動的に生成しません。

エージェント キーのエクスポート

連結されたポリシー/キー ストアからキーをエクスポートして、それらを個別のキー ストアに利用できるようにします。

以下の手順に従います。

1. r6.x ポリシー サーバ ホスト システムにログインします。 このポリシー サーバが、連結されたポリシー/キー ストアで設定されていることを確認します。
2. 以下のコマンドを実行して、ポリシー ストアからキーのみをエクスポートします。

   ```
   smobjectexport -ffile_name -x
   ```

   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する前に、管理者権限でコマンド ライン ウィンドウを開きます。 アカウントに管理者権限がある場合でも、このようにコマンド ライン ウィンドウを開きます。

   注: これらのモードと引数の詳細については、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。

   例 :

   ```
   smobjexport -fagentkeys -x
   ```

   エージェント キーが連結されたポリシー/キー ストアからエクスポートされます。
3. セット アップ ポリシー サーバ ホスト システムに、エージェント キーを含むファイルをコピーします。

エージェント キーのインポート

連結されたポリシー/キー ストアからキーをインポートして、それらを個別のキー ストアに利用できるようにします。

以下の手順に従います。

1. r6.x セットアップ 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て、個別のキー ストアにエージェント キーをインポートします。

   ```
   smobjimport -ffile_name -k
   ```

   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する前に、管理者権限でコマンド ライン ウィンドウを開きます。 アカウントに管理者権限がある場合でも、このようにコマンド ライン ウィンドウを開きます。

   注: これらのモードと引数の詳細については、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。

   例 :

   ```
   smobjimport -fagentkeys -k
   ```

   エージェント キーが個別のキー ストアにインポートされます。

すべてのポリシー サーバを設定して、キー ストアを使用します。

並列の環境ですべてのポリシー サーバを設定して共通の r6.x キー ストアを使用すると、両方の環境でシングル サインオンを維持します。

以下の手順に従います。

1. エージェント キーを動的に生成する際に指定されるポリシー サーバを特定します。 このポリシー サーバをキー ストアで最後に設定します。
2. 環境内の他のすべてのポリシー サーバに対して、以下の手順を実行します。
   a. ポリシー サーバ ホスト システムにログインします。
   b. ポリシー サーバ管理コンソールを開きます。
   c. ［データ］タブをクリックします。
   d. ［データベース］リストから［キー ストア］を選択し、［ポリシー ストアを使用］データベース オプションをクリアします。

e. ［ストレージ］リストからキー ストアのタイプを選択します。

f. 以下のいずれかを実行します。

   a. （LDAP）［LDAP キー ストア］セクションに必要な接続情報を入力します。

   b. （ODBC）［データ ソース情報］セクションにデータ ソース情報を入力します。

g. 接続をテストします。

h. ［OK］をクリックします。

i. ポリシー サーバを再起動して、キー ストアを使用するようにポリシー サーバを設定します。

3. キー ストアを使用するためにエージェント キーの生成に指定されるポリシー サーバを設定します。

動的エージェント キー生成の再有効化

動的エージェント キー生成を無効にした場合は、エージェント キーの生成に指定されるポリシー サーバの機能を再度有効にします。 環境内のすべてのポリシー サーバが新規キー ストアを使用するように設定した後でのみ、この手順を実行します。

以下の手順に従います。

1. r6.x ポリシー サーバのユーザ インターフェースにログインします。
2. ［ツール］-［キーの管理］を選択します。
3. ［動的エージェント キーを使用］オプションを選択します。
4. ［Apply］をクリックします。

   指定されたポリシー サーバはキーを動的に生成するために有効にされます。

ポリシー ストアからキー ストアを分けるために必要な処理が完了しました。

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 12.52 SP1 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 12.52 SP1 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。

キーと証明書の移行

環境に 1 つ以上の smkeydatabases が含まれる場合は、12.52 SP1 証明書データ ストアにそれらのコンテンツを移行します。

以下の手順に従います。

1. すべての r6.x smkeydatabases は必ず同期します (P. 53)。
2. r6.x ポリシー サーバ ホスト システムにログインし、以下のディレクトリに移動します。

   siteminder_home¥config¥properties

   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. 以下のファイルをコピーします。

   smkeydatabase.properties

4. 12.52 SP1 ポリシー サーバ ホスト システムにログインし、以下の手順を実行します。
   a. 以下の場所に移動します。

      siteminder_home¥config¥properties

   b. smkeydatabase プロパティ ファイルの 12.52 SP1 バージョンの名前を以下の値に変更します。

      newsmkeydatabase.properties

   c. プロパティ ファイルの r6.x バージョンをディレクトリに追加します。
   d. テキスト エディタで 12.52 SP1 および r6.x プロパティ ファイルを開きます。
   e. r6.x バージョンのデータベースのパスを編集して、12.52 SP1 バージョンのパスに一致させます。

      例：

      r6.x ファイルは以下のパスを参照します。

      DBLocation=C¥:/Program Files/netegrity/siteminder/smkeydatabase

      12.52 SP1 ファイルは以下のパスを参照します。

      DBLocation=C:/Program Files/CA/siteminder/smkeydatabase

      r6.x ファイルを更新して以下のパスを参照するようにします。

      DBLocation=C¥:/Program Files/CA/siteminder/smkeydatabase

   f. r6.x プロパティ ファイルを保存し、12.52 SP1 プロパティ ファイルを閉じます。
   g. ポリシー サーバ インストールのルートで以下のディレクトリを作成します。

      smkeydatabase

      例：

      C:¥Program Files¥CA¥SiteMinder¥smkeydatabase

5. r6.x ポリシー サーバ ホスト システムに戻り、smkeydatabase ディレクトリの内容をコピーします。

   注: このファイルのデフォルトの場所は *siteminder_home* です。

6. 12.52 SP1 ポリシー サーバ ホスト システムに戻り、以下の手順を実行します。
   a. 作成した 12.52 SP1 smkeydatabase ディレクトリに、r6.x smkeydatabase ディレクトリの内容を追加します。
   b. 以下の移行ユーティリティを使用して、smkeydatabase を証明書データ ストアに移行します。

      ```
      smmigratecds
      ```

   c. 移行が成功したら、smkeydatabase プロパティ ファイルおよび smkeydatabase ディレクトリを削除します。

   これで移行は完了です。

詳細情報:

手動による SiteMinder キー データベースの移行 (P. 189)

アサーション発行者 ID の移行

r12.x 環境で レガシー フェデレーション（フェデレーション セキュリティ サービス）オブジェクトを管理している場合は、r12.x プロデューサ から 12.52 SP1 プロデューサ にアサーション発行者 ID を移行します。ID の移行により、SAML 1.1 トランザクションがサービス プロバイダで失敗するのを防ぎます。

以下の手順に従います。

1. r6.x ポリシー サーバ ホスト システムにログインし、以下のディレクトリに移動します。

   siteminder_home¥config¥properties

   siteminder_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のファイルをコピーします。

   AMAssertionGenerator.properties

3. 12.52 SP1 ポリシー サーバ ホスト システムにログインし、以下のディレクトリに移動します。

   siteminder_home¥config¥properties

4. アサーション ジェネレータのプロパティ ファイルの 12.52 SP1 バージョンの名前を以下の値に変更します。

   `newAMAssertionGenerator.properties`

5. プロパティ ファイルの r6.x バージョンをディレクトリに追加します。

   これで移行は完了です。

r6.x ポリシーの移行

12.52 SP1 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 12.52 SP1 ポリシー ストアに移行することをお勧めします。

12.52 SP1 ポリシー ストアの管理を開始する前に、ポリシー ストア データを移行することで、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。

次の手順に従ってください:

1. smobjexport ユーティリティの r6.x バージョンを使用して、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 smobjexport ユーティリティの詳細については、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. smobjimport ユーティリティの 12.52 SP1 バージョンを使用して、ポリシー データを 12.52 SP1 ポリシー ストアへインポートします。

   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

3. Oracle Directory Server の場合は、インデックスをすべて再作成します。

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 12.52 SP1 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: SiteMinder 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。

移行に関する考慮事項

r12.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。

管理 UI アップグレード パス

以下のアップグレードに関する考慮事項を確認します。

- 既存のアプリケーション サーバ上の 管理 UI は、12.5 よりも前のバージョンから 12.52 SP1 にアップグレードできません。 代わりに、以下の手順を実行します。
  a. 管理 UI の r12.x バージョンをアンインストールします。
  b. SiteMinder がサポートするアプリケーション サーバをインストールします。
  c. 新しい 12.52 SP1 管理 UI をインストールします。

  注: 管理 UI をインストールする詳細については、「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。

- 既存のアプリケーション サーバ インフラストラクチャ上の 管理 UI は、バージョン 12.5 からのみ 12.52 SP1 にアップグレードできます。
- JBoss の組み込みバージョンを使用する r12.x 管理 UI を 12.52 SP1 にアップグレードできます。

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 (P. 100)」および「r12.x 管理 UI のアップグレード (P. 118)」の手順を参照してください。

SiteMinder の 管理 UI の保護

SiteMinder の 12.52 SP1 管理 UI を保護できます。 管理 UI を保護するには、以下の手順に従う必要があります。

1. リバース プロキシ サーバで機能するエージェントを設定します。

   注: リバース プロキシ サーバ の設定の詳細については、「Web エージェント設定ガイド」を参照してください。

2. 外部管理者ストアを設定します。ストアを設定するとき、SiteMinder 認証を有効にします。

   注: 外部管理者ストア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。

外部管理者ストアで r12.x 管理 UI を設定しており、SiteMinder 認証を有効にする場合は、以下の手順に従います。

1. リバース プロキシ サーバで機能するエージェントを設定します。
2. 必要なエージェントの設定で外部管理者ストアを再設定します。

重要: ストアを再設定する場合、管理 UI は設定を保持しません。 接続を再設定する前に、接続を表示して設定を記録しておくことをお勧めします。

シングル サインオン

12.52 SP1 への移行時に、シングル サインオンを維持できます。 以下の点を考慮します。

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

証明書データの管理

証明書データ ストアは SiteMinder キー データベース（smkeydatabase）を置換します。 使用する環境で 1 つ以上の smkeydatabases を展開する場合は、以下の点を考慮します。

- 証明書データ ストアは 12.52 SP1 ポリシー ストアと連結されます。 単一の証明書データ ストアによって、各ポリシー サーバ ホスト システム上の個別の smkeydatabase インスタンスが不要になります。
- ポリシー サーバのアップグレードの一部として、すべての smkeydatabase コンテンツが自動的にバックアップされ、証明書データ ストアに移行されます。
- 12.52 SP1 ポリシー サーバは証明書データ ストアとのみ通信できます。 12.52 SP1 ポリシー サーバおよびそれぞれのローカル smkeydatabase は、互換モードで作動しません。 ただし、アップグレードされていないポリシー サーバはすべて、smkeydatabase のローカル バージョンとの通信を継続します。

  重要: smkeydatabase の移行が失敗した場合、ポリシー サーバを環境に戻さないでください。移行が失敗した後でポリシー サーバを戻すと、証明書データを必要とするトランザクションはすべて失敗します。
- 移行を開始する前に smkeydatabase インスタンスをすべて同期します。 すべてのインスタンスを同期することによって、データの衝突を防ぎます。 データの衝突が発生すると、移行が正常に実行されません。
- 同じポリシー ストアに共通のビューを共有するポリシー サーバはすべて、同じキー、証明書および証明書廃棄リスト（CRL）にアクセスできます。
- 証明書データ ストアの目的は、smkeydatabase の目的と変わりません。 このストアによって以下が SiteMinder 環境で利用可能になります。
  - 認証機関（CA）の証明書
  - 公開キーおよび秘密キー
  - 証明書破棄リスト
- 証明書データ ストアの管理に、SiteMinder キー ツールを引き続き使用できます。 ただし、いくつかのオプションが非推奨になります。

  注: 詳細については、「ポリシー サーバ リリース ノート」を参照してください。

- CRL が LDAP ディレクトリ サービスに格納される場合、以下の点を考慮します。
  - SiteMinder では、CRL の発行元と、対応するルート証明書の発行元が同一の CA である必要がなくなりました。
  - SiteMinder はこの確認を実行しなくなりました。 この動作はテキスト ベースの CRL の要件と一致しています。

フェデレーションの統合

r12.xFSS 管理 UI で利用可能なフェデレーション セキュリティ サービス機能はすべて、管理 UI に移動しました。 フェデレーション環境 を管理していた場合、この機能は レガシー フェデレーション と呼ばれます。

管理 UI にはまたパートナーシップ フェデレーションが含まれます。 これは、CA SiteMinder® Federation によって使用可能になるパートナーシップ ベースのフェデレーション固有の機能です。

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。

拡張パスワード サービス

ユーザが Advanced Password Services を展開している場合、ポリシー サーバ アップグレードは LANG （翻訳）、CFG （設定）およびメール ファイルをすべて保持します。 ファイルのデフォルト 12.52 SP1 バージョンは *siteminder_home*¥samples にインストールされます。

siteminder_home

ポリシー サーバのインストール パスを指定します。

SiteMinder と CA Arcot WebFort および CA Arcot RiskFort との統合

CA Arcot Adapter を使用して、SiteMinder リリース 12.5 以前と CA Arcot WebFort および CA RiskFort を統合した場合に、SiteMinder を 12.52 以降にアップグレードする場合は、以下の手順を実行します。

1. AFM_HOME¥conf ディレクトリに移動します。
2. adaptershim.ini ファイルのバックアップを作成します。
3. SiteMinder をアップグレードします。
4. バックアップの adaptershim.ini ファイルを ARCOT_HOME¥conf ディレクトリにコピーします。

r12.x の移行の仕組み

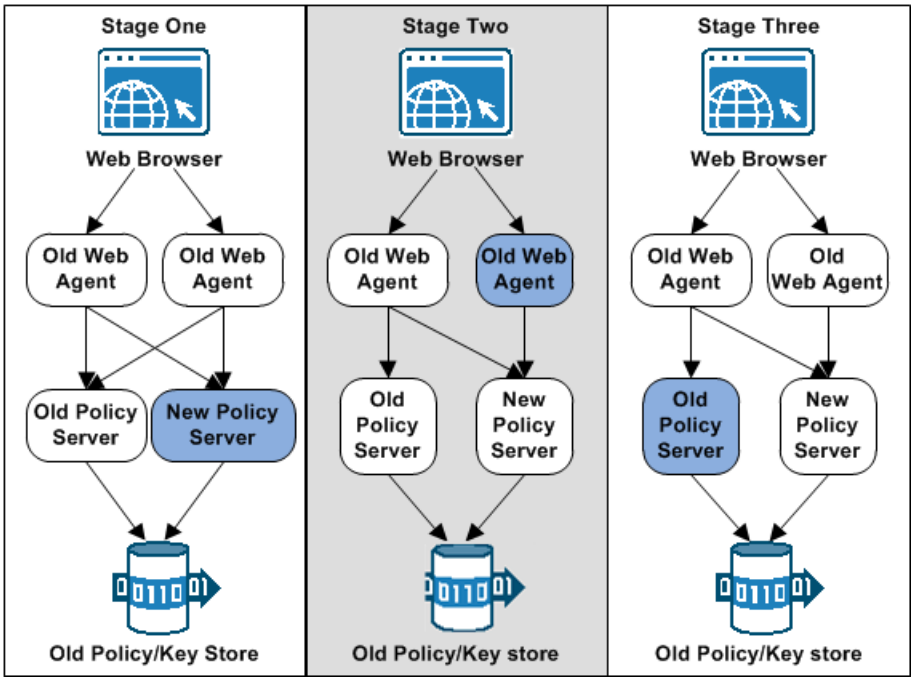
複数のポリシー サーバおよび Web エージェントが存在する SiteMinder 展開を移行するには、SiteMinder 環境からポリシー サーバおよび Web エージェントのうち 1 つを削除します。 これらのコンポーネントはアップグレードされますが、残りのポリシー サーバおよび Web エージェントはリソースを保護し続行けます。

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.x 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。

図 10: r12.x 移行の概要。



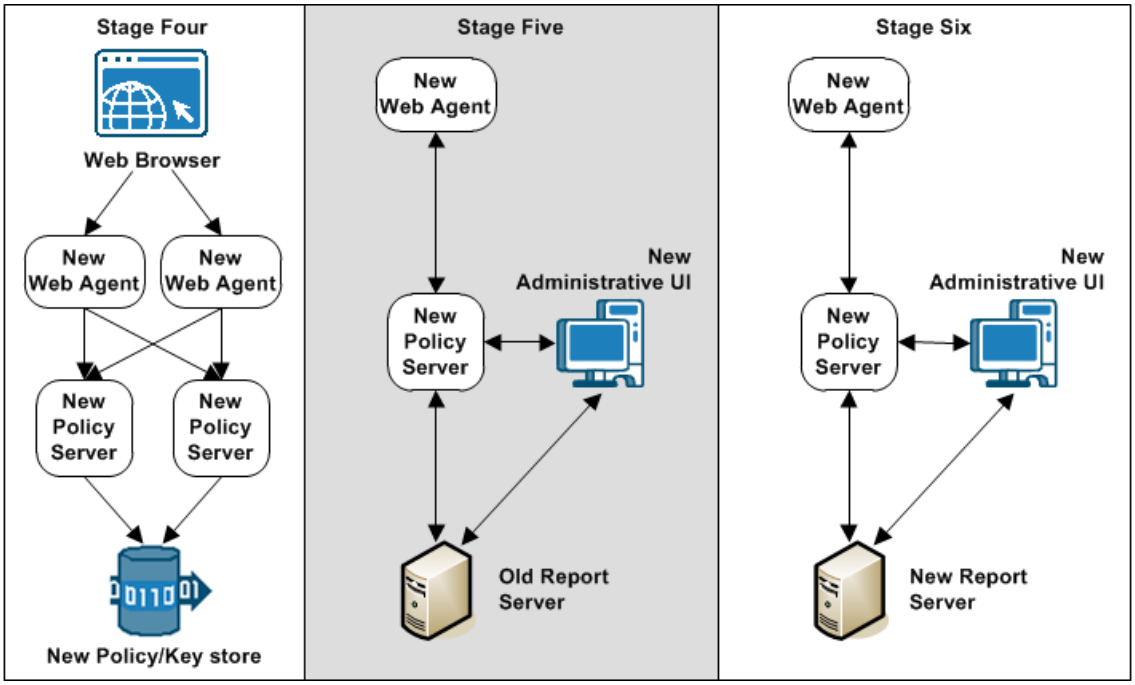
1. 第 1 段階では、r12.x ポリシー サーバがアップグレードされます。12.52 SP1 ポリシー サーバは互換モードで動作します。 以下の点を考慮します。

   - r12.x Web エージェントは、12.52 SP1 ポリシー サーバと通信し続けます。
   - 12.52 SP1 ポリシー サーバは、r12.x ポリシーおよびキー ストアと通信し続けます。
   - r12.x ポリシー サーバは、r12.x ポリシーおよびキー ストアと通信し続けます。
   - r12.x 管理 UI が 12.52 SP1 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.x ポリシー ストアのオブジェクトを管理し続けます。
   - r12.x レポート サーバが 12.52 SP1 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.x Web エージェントが 12.52 SP1 にアップグレードされます。
   - r12.x Web エージェントは、r12.x および 12.52 SP1 ポリシー サーバと通信し続けます。
   - 12.52 SP1 Web エージェントは、12.52 SP1 ポリシー サーバのみと通信します。

     注: 移行中に、12.52 SP1 ポリシー サーバを持った新しい 12.52 SP1 Web エージェントを設定できます。 ただし、12.52 SP1 コンポーネントは、ユーザのポリシー ストアの現在のバージョンでサポートされている機能のみをサポートします。
3. 第 3 段階では、残りのポリシー サーバが 12.52 SP1 にアップグレードされます。 12.52 SP1 ポリシー サーバは、r12.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。

図 11: rr12.x 移行の概要。



4. 第 4 段階では、r12.x ポリシーおよびキー ストアが 12.52 SP1 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.x レポート サーバがアンインストールされます。12.52 SP1 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。

   注: r12.0 SP3 cr4 以上のレポート サーバをインストールし、設定した場合は、この手順は必要ありません。

r12.x から移行する方法

r12.x から 12.52 SP1 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 リリース ノート*」のインストールおよびアップグレードの考慮事項を確認します。
2. （オプション）使用している環境に smkeydatabase の複数のインスタンスが含まれる場合は、インスタンスをすべて同期します。 ポリシー サーバ アップグレードの一部として、証明書データ ストアに smkeydatabase の内容をすべて移行することも含まれます。
3. 「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。
4. r12.x ポリシー サーバを 12.52 SP1 にアップグレードします。
5. r12.x Web エージェントを 12.52 SP1 にアップグレードします。
6. 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 12.52 SP1 にアップグレードします。
7. r12.x ポリシーおよびキー ストアを 12.52 SP1 にアップグレードします。
8. r12.x 管理 UI をアップグレードします。
9. 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。12.52 SP1 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。

キー データベース インスタンスの同期

新バージョンへの移行を開始する前に smkeydatabase インスタンスをすべて同期します。

注: smkeytool ユーティリティを使用して、smkeydatabases を同期し、smkeydatabase インスタンス間でのデータの不整合をすべて解決します。smkeytool 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。

SiteMinder の旧バージョンでは、証明書データの格納にローカルな smkeydatabase を使用していました。 各ポリシー サーバにそれぞれの smkeydatabase が必要でした。バージョン 12.52 SP1 では、一元化された証明書データ ストアがローカルな smkeydatabases に置き換えられています。

ポリシー サーバのアップグレードの一部として、インストーラは自動的にローカル smkeydatabase をバックアップし、証明書データ ストアにコンテンツをすべて移行しようとします。 このプロセスのなかで、移行開始前に両方のストアが比較されます。

重要: smkeydatabase の移行が失敗した場合、ポリシー サーバを環境に戻さないでください。 移行が失敗した後でポリシー サーバを戻すと、証明書データを必要とするトランザクションはすべて失敗します。

smkeydatabases におけるデータの整合性を確認および解決するために、以下のガイドラインを使用します。

- 認証機関-の各証明書が、すべてのインスタンスの証明書破棄リストを参照することを確認する。

  例： 証明機関-の証明書は、LDAP ディレクトリ サービス内の証明書失効リストを一貫して参照します。
- すべてのインスタンスで defaultentpriseprivatekey エイリアスが同じ秘密キー/証明書のペアを表すことを確認する。
- 同じエイリアスが同一の証明書またはキー/証明書に対応することを確認する。
- 同じ認証機関-の証明書が同一の証明書廃棄リストに対応することを確認する。
- 無効または有効期限が切れている証明書が存在しないことを確認する。
- すべての CRL 情報が有効であることを確認する。

重要: データの不整合をすべて解決した後も、移行がすべて完了するまで smkeydatabase を変更しないことをお勧めします。

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 と UNIX の r12.x 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。

- （オプション）環境に複数の smkeydatabase インスタンスが含まれる場合は、必ずコンテンツをすべて同期します。 同期することでポリシー サーバ インストーラがコンテンツを証明書データ ストアに自動的に移行できないというデータ不整合の問題を解決します。
- 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。
- （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。
- 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 SiteMinder 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）ポリシー サーバをアップグレードするユーザ アカウントは、インストール メディアが含まれるディレクトリに対して実行権限を持っている必要があります。ユーザ アカウントにこれらの権限がない場合は、以下のコマンドを実行します。

  `chmod +x installation_media`

  installation_media

  ポリシー サーバのインストール実行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。

必要とされる Linux ライブラリ

Linux オペレーティング環境上で動作するコンポーネントには、特定のライブラリ ファイルが必要です。 正しいライブラリをインストールしないと、以下のエラーを引き起こす場合があります。

```
java.lang.UnsatisfiedLinkError
```

このコンポーネントの Linux バージョンをインストール、設定、またはアップグレードする場合は、ホスト システム上で以下のパッケージが必要になります。

Red Hat 5.x

- compat–gcc-34-c++-3.4.6-*patch_version*.I386
- libstdc++-4.x.x-x.el5.i686.rpm
- libidn.so.11.rpm
- ncurses

Red Hat 6.x

- libstdc++-4.x.x-x.el6.i686.rpm
- libidn-1.18-2.el6.i686
- libXext.i686.rpm
- libXrender.i686.rpm
- linXtst.i686.rpm
- libidn.so.11.rpm
- ncurses

Red Hat 6.x（64 ビット）の場合はさらに以下：

注: 64 ビット Red Hat 6.x に必要な RPM パッケージはすべて、*32* ビットのパッケージです。

- libXau-1.0.5-1.el6.i686.rpm
- libxcb-1.5-1.el6.i686.rpm
- compat-db42-4.2.52-15.el6.i686.rpm
- compat-db43-4.3.29-15.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm
- libXrender-0.9.5-1.el6.i686.rpm
- libexpat.so.1（expat-2.0.1-11.el6_2.i686.rpm により提供）
- libfreetype.so.6（freetype-2.3.11-6.el6_2.9.i686.rpm により提供）
- libfontconfig.so.1（fontconfig-2.8.0-3.el6.i686.rpm により提供）
- libICE-1.0.6-1.el6.i686.rpm
- libuuid-2.17.2-12.7.el6.i686.rpm
- libSM-1.1.0-7.1.el6.i686.rpm
- libXext-1.1-3.el6.i686.rpm
- compat-libstdc++-33-3.2.3-69.el6.i686.rpm
- compat-db-4.6.21-15.el6.i686.rpm
- libXi-1.3-3.el6.i686.rpm
- libXtst-1.0.99.2-3.el6.i686.rpm
- libXft-2.1.13-4.1.el6.i686.rpm
- libXt-1.0.7-1.el6.i686.rpm

- libXp-1.0.0-15.1.el6.i686.rpm
- libstdc++.i686.rpm
- compat-libtermcap.rpm
- libidn.i686.rpm
- ncurses

ポリシー サーバのアップグレード前のシグネチャ ラッピングのチェックの無効化

サービス プロバイダでポリシー サーバをアップグレードした後、SiteMinder Federation（レガシーまたはパートナーシップ）展開で SAML 2.0 Artifact トランザクションが失敗します。

以下の場合、トランザクションは失敗します。

- SiteMinder Federation がサービス プロバイダ サイトで展開されている。
- SAML 2.0 HTTP-Artifact SSO が設定されている。
- サービス プロバイダでの署名の検証がアサーションまたは Artifact 解決レスポンスに対して設定されている。
- XML シグネチャ ラッピング攻撃を防ぐポリシー サーバ設定が有効になっている。

ポリシー サーバが Artifact レスポンスの署名を検証しようとすると、SSO トランザクションは失敗します。

Artifact SSO が失敗するのを防ぐには、署名の脆弱性のチェックを一時的にオフにします。サービス プロバイダ サイトでポリシー サーバをアップグレードした後、ポリシー サーバを稼働させる前に、チェックを無効にします。

次の手順に従ってください:

1. xsw.properties ファイルに移動します。以下のディレクトリにあるファイルを確認します。

   siteminder_install_dir¥config¥properties¥xsw.properties

   siteminder_install_dir はポリシー サーバをインストールした場所です。
2. テキスト エディタでファイルを開き、DisableXSWCheck を true に設定します（DisableXSWCheck=true）。 この値を true に設定すると、脆弱性のチェックが無効になります。

3. 展開全体がバージョン 12.52 SP1 になり、ポリシー サーバが実行されたら、DisableXSWCheck 設定を false に戻します（DisableXSWCheck=false）。この値を false に設定すると、署名の脆弱性のチェックが有効になります。

バック チャネル ユーザ名が各 SAML パートナーシップで一意であることを確認する

HTTP-Artifact シングル サインオン トランザクション中に、アサーティング パーティは保護されたバック チャネルを介して依存パーティにアサーションを返します。 バック チャネルへのアクセスを認証するためにエンティティを要求できます。 バック チャネル用の認証方式として基本認証を選択している場合は、ユーザ名が必要です。

アップグレードする前に、同じ SAML プロファイル内のフェデレーション パートナーシップが、それぞれ一意のユーザ名を受信バック チャネルに使用していることを確認します。 複数の SAML 2.0 または SAML 1.x パートナーシップでは、受信バック チャネル ユーザ名を共有できません。

注: SAML 1.x と SAML 2.0 のパートナーシップでは受信バック チャネル ユーザ名を共有できますが、推奨されません。

受信バック チャネル ユーザ名を共有する同じプロトコルのパートナーシップがある場合は、アップグレードする前に以下の手順に従います。

1. パートナーシップの 1 つを非アクティブにします。
2. そのパートナーシップで定義されているバック チャネル ユーザ名を変更します。
3. リモート パートナーに変更を伝えます。
4. パートナーシップを再度アクティブ化します。

Windows のポリシー サーバのアップグレード

次の手順に従ってください:

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。

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。
     - アップグレード中に、既存のポリシー ストアを保持しておくために、設定ウィザードでポリシー ストア チェック ボックスをオフのままにしておきます。ただし、設定ウィザードによって、Advanced Authentication Server 用の暗号化キーの入力を促されます。 このキーは各ポリシー サーバに格納されますが、すべてのポリシー サーバで同じキーが必要です。
     - 別の（n 番目の）ポリシー サーバをアップグレードしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
   - インストーラは smkeydatabase を検出すると、以下を実行します。
     - smkeydatabase をバックアップする。
     - 証明書データ ストアへのコンテンツの移行を試行する。

     重要: smkeydatabase の移行が失敗した場合、ポリシー サーバを環境に戻さないでください。 移行が失敗した後でポリシー サーバを戻すと、証明書データを必要とするトランザクションはすべて失敗します。
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。

UNIX での GUI を使用したポリシー サーバのアップグレード

次の手順に従ってください:

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: ピリオドの間に必ず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

   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。
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。
     - アップグレード中に、既存のポリシー ストアを保持しておくために、設定ウィザードでポリシー ストア チェック ボックスをオフのままにしておきます。 既存のポリシー ストアを手動でアップグレードします。 ただし、設定ウィザードによって、Advanced Authentication Server 用の暗号化キーの入力を促されます。 このキーは各ポリシー サーバに格納されますが、すべてのポリシー サーバで同じキーが必要です。 既存のポリシー ストアを手動でアップグレードします。
     - 別の（n 番目の）ポリシー サーバをアップグレードしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
   - インストーラは smkeydatabase を検出すると、以下を実行します。
     - smkeydatabase をバックアップする。
     - 証明書データ ストアへのコンテンツの移行を試行する。

     重要: smkeydatabase の移行が失敗した場合、ポリシー サーバを環境に戻さないでください。 移行が失敗した後でポリシー サーバを戻すと、証明書データを必要とするトランザクションはすべて失敗します。
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。

7. ［終了］をクリックします。
8. 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: ピリオドの間に必ずスペースを入れてください。

コンソールを使用した UNIX でのポリシー サーバのアップグレード

次の手順に従ってください:

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: ピリオドの間に必ず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。
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とき、以下の点を考慮します。
     - 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。

- アップグレード中に、既存のポリシー ストアを保持しておくために、設定ウィザードでポリシー ストア チェック ボックスをオフのままにしておきます。 既存のポリシー ストアを手動でアップグレードします。 ただし、設定ウィザードによって、Advanced Authentication Server 用の暗号化キーの入力を促されます。 このキーは各ポリシー サーバに格納されますが、すべてのポリシー サーバで同じキーが必要です。
- 別の（n 番目の）ポリシー サーバをアップグレードしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。

- インストーラは smkeydatabase を検出すると、以下を実行します。
  - smkeydatabase をバックアップする。
  - 証明書データ ストアへのコンテンツの移行を試行する。

  重要: smkeydatabase の移行が失敗した場合、ポリシー サーバを環境に戻さないでください。 移行が失敗した後でポリシー サーバを戻すと、証明書データを必要とするトランザクションはすべて失敗します。

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。

7. ［終了］をクリックします。
8. 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: ピリオドの間に必ずスペースを入れてください。

カスタマイズされた JVMOptions ファイルの変更

ポリシー サーバ アップグレード中に、既存の JVMOptions.txt ファイルの名前が JVMOptions.txt.backup に変更されます。新しい JVMOptions.txt ファイルが作成されます。

元のファイルにカスタマイズされたパラメータが含まれていた場合、これらのカスタム パラメータが含まれるよう、作成されたファイルを変更する必要があります。

Apache ベースのエージェントの場合は、以下の例のように、SiteMinder/resources ディレクトリを JVMOptions.txt ファイル内の CLASSPATH に追加します。

```
-Djava.class.path=C:/Program Files (x86)/CA/siteminder/resources;
```

サーバ側のカスタム コードの要件

ポリシー サーバのオペレーティング システムは、サーバ側のカスタム コードの再コンパイルが必要かどうかを判断します。 以下の表を使用して、要件を識別してください。

オペレーティング システム	必要ですか。
Microsoft Windows および UNIX	いいえ。カスタム コードの再コンパイルはオプションです。
Red Hat Linux	はい。 SDK をアップグレードし、GCC 3.4 を使用してカスタム コードを再コンパイルします。

ポリシー サーバ アップグレードのトラブルシュート

アップグレード中に問題が発生した場合、以下を参照します。

- *siteminder_home*¥siteminder¥install_config_info にあるポリシー サーバ インストール ログ ファイルを参照できます。

  siteminder_home

  ポリシー サーバのインストール パスを指定します。

- *siteminder_home*¥log にある smkeydatabase 移行ログ（smkeydatabaseMigration.log）を参照できます。

  注: ポリシー サーバのアップグレードと smkeydatabase の移行は別個のプロセスです。 smkeydatabase の移行が失敗しても、ポリシー サーバのアップグレードは失敗しません。

r12.x Web エージェントのアップグレード

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 r12.x Web エージェントは、12.52 SP1 ポリシー サーバと通信できます。 したがって、Web エージェントを 12.52 SP1 にアップグレードする前に、ポリシー サーバを r12.5 にアップグレードします。

r12.x Web エージェントのアップグレード前

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

12.52 SP1 Web エージェント インストーラを使用して、Web エージェントをアップグレードします。

- オプション パック機能が必要なエージェントは、12.52 SP1 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 12.52 SP1 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。 12.52 SP1 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。

- Advanced Password Services を展開した場合、Web エージェント アップグレードは LANG（変換）ファイルおよび CFG（設定）ファイルをすべて保持してます。 ファイルのデフォルト 12.52 SP1 バージョンは agent_home¥samples にインストールされます。

  agent_home

  Web エージェントのインストール パスを指定します。

カスタム エージェントの要件

カスタム エージェントを再コンパイルする必要があるかどうかを判断するには、以下の表を使用します。

エージェント タイプ	必要ですか。
SiteMinder エージェント	オペレーティング システムによって異なります。 エージェントのオペレーティング システムのサポートが終了している場合、カスタム エージェントを再コンパイルする必要があります。 SiteMinder SDK をアップグレードし、サポートされているオペレーティング システム上でエージェントを再コンパイルします。
サードパーティ エージェント	ベンダーによって異なります。 エージェントがサポートされているかどうかを確認するには、サードパーティ ベンダーに問い合わせてください。

r12.x ポリシー ストアをアップグレードする方法

r12.0 SP1 ポリシー ストアを 12.52 SP1 にアップグレードするには、以下の手順に従います。

1. ポリシー ストアと通信しているすべてのポリシー サーバを停止します。
2. ポリシー ストア データ定義をインポートします。
3. デフォルトのポリシー ストア オブジェクトをインポートします。
4. FSS 管理 UI を使用して、r12.x レガシー フェデレーション 環境を管理している場合は、レガシー フェデレーション オブジェクトの移行を完了するために XPS スイーパ ユーティリティを実行します。
5. ポリシー ストアと通信しているすべてのポリシー サーバを開始します。

すべてのポリシー サーバの停止

ポリシー ストアと通信しているすべてのポリシー サーバを停止すると、アップグレード中のポリシー ストアの破損を防ぐのに役立ちます。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のいずれかの操作を実行します。
   - （Windows）
     a. ポリシー サーバ管理コンソールを開き、［停止］をクリックします。
     b. ［OK］をクリックしてコンソールを閉じます。
   - （UNIX）以下の提供されたスクリプトを使用します。
     install_path/siteminder/stop-all

     install_path

     ポリシー サーバのインストール パスを指定します。
3. ポリシー ストアと通信している各ポリシー サーバに対して、この手順を繰り返します。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home*¥xps¥dd 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。
2. 以下のコマンドを実行します。

   XPSDDInstall SmMaster.xdd

   XPSDDInstall

   必要なデータ定義をインポートします。

デフォルトのポリシー ストア オブジェクトのインポート

デフォルトのポリシー ストア オブジェクトをインポートすると、管理 UI とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず *siteminer_home*¥bin への書き込みアクセス権があることを確認してください。インポート ユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

  siteminder_home

  ポリシー サーバのインストール パスを指定します。

- 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する前に、管理者権限でコマンド ライン ウィンドウを開きます。 アカウントに管理者権限がある場合でも、このようにコマンド 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。

以下の手順に従います。

1. コマンド ウィンドウを開き、*siteminder_home*¥db に移動します。
2. 以下のファイルのいずれかをインポートします。
   - smpolicy.xml をインポートするには、以下のコマンドを実行します。

     ```
     XPSImport smpolicy.xml -npass
     ```

   - smpolicy-secure.xml をインポートするには、以下のコマンドを実行します。

     ```
     XPSImport smpolicy-secure.xml -npass
     ```

   注: いずれかのファイルを使用して、新規ポリシー ストアの設定、および既存のストアのアップグレードを行います。 アップグレードの一部としてインポートされた場合、ファイルは変更された既存のデフォルト オブジェクトを上書きしません。 両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。 これらのオブジェクトにはデフォルトのエージェント設定オブジェクト（ACO）テンプレート内のデフォルト セキュリティ設定が含まれます。 secure ファイルはより制限の厳しいセキュリティ設定を提供します。

-npass

パスフレーズが必要ではないことを指定します。 デフォルト ポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

デフォルトのポリシー ストア オブジェクトがインポートされます。

XPS スイーパ ユーティリティの実行

FSS 管理 UI を使用して、フェデレーション セキュリティ サービス（レガシー フェデレーション）のオブジェクトを管理した場合は、XPS スイーパ ユーティリティ（XPSSweeper）を実行して、これらのオブジェクトの移行を完了します。

以下の手順に従います。

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て、管理 UI に対して レガシー フェデレーション オブジェクトを利用可能にします。

   XPSSweeper

   FSS 管理 UI を使用して作成された レガシー フェデレーション はすべて、管理 UI で利用可能です。

すべてのポリシー サーバの起動

すべてのポリシー サーバを開始すると、すべてのポリシー サーバとアップグレードされたポリシー ストアの間の通信が再開します。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のいずれかの操作を実行します。
   - （Windows）
     a. ポリシー サーバ管理コンソールを開き、［開始］をクリックします。
     b. ［OK］をクリックしてコンソールを閉じます。

- （UNIX）以下の提供されたスクリプトを使用します。
  install_path/siteminder/start-all

  install_path

  ポリシー サーバのインストール パスを指定します。

3. ポリシー ストアと通信している各ポリシー サーバに対して、この手順を繰り返します。

ポリシー ストアがアップグレードされます。

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。

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。

- **重要**: 管理 UI アップグレード パス (P. 93) を確認します。
- 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: インストール メディア名のリストについては、「ポリシー サーバ リリース ノート」を参照してください。
- （組み込み JBoss インストールのみ）必須インストーラの内容を 管理 UI インストーラの内容を展開したのと同じディレクトリに展開します。各インストーラ zip ファイルの内容は layout.properties ファイルと同じ場所にある必要があります。 管理 UI インストール zip に含まれている layout.properties ファイルは、常に両方の実行可能ファイルと同じ場所に配置する必要があります。配置しないと、インストールは失敗します。
- （Windows） 管理 UI ホスト システムからインストーラを実行します。マップされたネットワーク共有または UNC パスからインストーラを実行しないでください。
- （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**:（UNIX）権限に応じて、以下のコマンドを実行し、実行可能権限をインストール メディアが含まれるディレクトリに追加します。

  ```
  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。

必要とされる Linux ライブラリ

Linux オペレーティング環境上で動作するコンポーネントには、特定のライブラリ ファイルが必要です。 正しいライブラリをインストールしないと、以下のエラーを引き起こす場合があります。

```
java.lang.UnsatisfiedLinkError
```

このコンポーネントの Linux バージョンをインストール、設定、またはアップグレードする場合は、ホスト システム上で以下のパッケージが必要になります。

Red Hat 5.x

- compat–gcc-34-c++-3.4.6-*patch_version*.l386
- libstdc++-4.x.x-x.el5.i686.rpm
- libidn.so.11.rpm
- ncurses

Red Hat 6.x

- libstdc++-4.x.x-x.el6.i686.rpm
- libidn-1.18-2.el6.i686
- libXext.i686.rpm
- libXrender.i686.rpm
- linXtst.i686.rpm
- libidn.so.11.rpm
- ncurses

Red Hat 6.x（64 ビット）の場合はさらに以下：

注: 64 ビット Red Hat 6.x に必要な RPM パッケージはすべて、*32* ビットのパッケージです。

- libXau-1.0.5-1.el6.i686.rpm
- libxcb-1.5-1.el6.i686.rpm
- compat-db42-4.2.52-15.el6.i686.rpm
- compat-db43-4.3.29-15.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm
- libXrender-0.9.5-1.el6.i686.rpm
- libexpat.so.1（expat-2.0.1-11.el6_2.i686.rpm により提供）
- libfreetype.so.6（freetype-2.3.11-6.el6_2.9.i686.rpm により提供）
- libfontconfig.so.1（fontconfig-2.8.0-3.el6.i686.rpm により提供）
- libICE-1.0.6-1.el6.i686.rpm
- libuuid-2.17.2-12.7.el6.i686.rpm
- libSM-1.1.0-7.1.el6.i686.rpm
- libXext-1.1-3.el6.i686.rpm
- compat-libstdc++-33-3.2.3-69.el6.i686.rpm
- compat-db-4.6.21-15.el6.i686.rpm
- libXi-1.3-3.el6.i686.rpm
- libXtst-1.0.99.2-3.el6.i686.rpm
- libXft-2.1.13-4.1.el6.i686.rpm
- libXt-1.0.7-1.el6.i686.rpm

- libXp-1.0.0-15.1.el6.i686.rpm
- libstdc++.i686.rpm
- compat-libtermcap.rpm
- libidn.i686.rpm
- ncurses

Windows での 管理 UI のアップグレード

次の手順に従ってください:

1. （組み込み JBoss セットアップのみ）。 管理 UI インストーラ zip を展開したのと同じディレクトリへ必須インストーラ zip を展開したことを確認します。 管理 UI インストール zip に含まれている layout.properties ファイルは、両方の実行可能ファイルと同じディレクトリに配置する必要があります。

   注: zip を展開した後に必須または 管理 UI インストール実行可能ファイルを移動する場合は、同じ場所に layout.properties ファイルを移動します。

2. 実行中のすべてのアプリケーションを終了します。
3. 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: 組み込みの JBoss アプリケーション サーバの停止および起動については、r12.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。 既存のアプリケーション サーバの停止については、ベンダー固有のドキュメントを参照してください。

4. 組み込み JBoss インストールの場合のみ、以下の実行可能ファイルを実行し、インストーラのプロンプトに従います。 その他の場合は、次の手順に進んでください。

   `adminui-pre-req-`*`version`*`-`*`cr`*`-win32.exe`

5. 以下の実行可能ファイルを実行します。

   ca-adminui-*version*-*cr*-win32.exe

6. インストーラのプロンプトに従い、管理 UI のアップグレードを確認します。
7. 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。
8. 既存のアプリケーション サーバについては、インストールが完了した後、アプリケーション サーバを再起動します。

   注: 組み込み JBoss アプリケーション サーバは、インストールが完了した後、自動的に再起動します。

管理 UI がアップグレードされました。

UNIX での 管理 UI のアップグレード

UNIX プラットフォームで、GUI モードまたはコンソール モードを使用して 管理 UI をインストールできます。

次の手順に従ってください:

1. （組み込み JBoss セットアップのみ）。 管理 UI インストーラ zip を展開したのと同じディレクトリへ必須インストーラ zip を展開したことを確認します。 管理 UI インストール zip に含まれている layout.properties ファイルは、両方の実行可能ファイルと同じディレクトリに配置する必要があります。

   注: zip を展開した後に必須または 管理 UI インストール実行可能ファイルを移動する場合は、同じ場所に layout.properties ファイルを移動します。

2. 実行中のすべてのアプリケーションを終了します。
3. 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: 組み込みの JBoss アプリケーション サーバの停止および起動については、r12.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。 既存のアプリケーション サーバの停止については、ベンダー固有のドキュメントを参照してください。

4. 組み込み JBoss インストールの場合のみ、必須インストーラを実行します。 その他の場合は、次の手順に進んでください。

   a. シェルを開き、以下のいずれかの必須インストール実行可能ファイルに移動します。
   ```
   adminui-pre-req-version-cr-linux.bin
   adminui-pre-req-version-cr-sol.bin
   ```

   b. 適切なモードでコマンドを入力します。

   GUI モード
   ```
   ./prerequisite_installation_media
   ```
   コンソール モード
   ```
   ./prerequisite_installation_media –i console
   ```

   c. 必須インストーラのプロンプトに従います。

5. シェルを開き、以下のいずれかのインストール実行可能ファイルに移動します。

   ```
   ca-adminui-version-cr-linux.bin
   ```

   ```
   ca-adminui-version-cr-sol.bin
   ```

6. 適切なモードでコマンドを入力します。

   GUI モード

   ```
   ./installation_media
   ```

   コンソール モード

   ```
   ./installation_media –i console
   ```

7. プロンプトに従い、管理 UI のアップグレードを確認します。

8. 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。

9. 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: 組み込みの JBoss アプリケーション サーバの停止および起動については、r12.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。 既存のアプリケーション サーバの停止については、ベンダー固有のドキュメント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 CR4 より前のバージョンのレポート サーバを使用している場合、12.52 SP1 レポート環境への最も単純なパスは、インストールされているバージョンをアンインストールし、12.52 SP1 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 r12.0 SP3 CR4 以降を使用している場合、アップグレードは必須ではありません。 ただし、ローカライズされたレポートが必要な場合は、12.52 SP1 レポート テンプレートが必要です。 そのため、レポート テンプレートをインストールするために、12.52 SP1 バージョンのレポート サーバ設定ウィザードを実行します。

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 12.52 SP1 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、12.52 SP1 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. 12.52 SP1 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。

r12.x 並行アップグレードの仕組み

既存の r12.x 環境を 12.52 SP1 に移行する必要はありません。代わりに、既存の展開との並行 12.52 SP1 環境を設定できます。

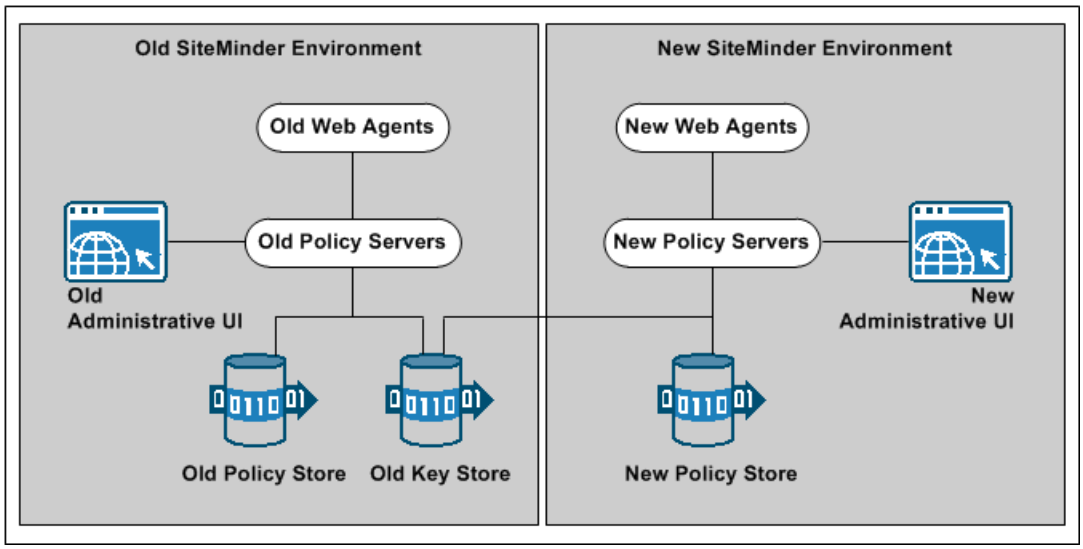
以下の図は、単純な並列アップグレードおよび詳細を示しています。

- 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 12.52 SP1 環境。

- 12.52 SP1 ポリシー ストアの SiteMinder オブジェクトの管理に使用される 12.52 SP1 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。

図 12: r12.x 並行アップグレードの概要



r12.x 並行環境を設定する方法

並行環境を設定するには、以下の手順を完了します。

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. 12.52 SP1 環境を作成します。
3. 以下のいずれかを実行します。
   - 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. r12.x ポリシー ストア データを移行します。以下のコマンドを使用し、XPSImport ユーティリティの 12.52 SP1 バージョンを使用して、12.52 SP1 のデフォルト ポリシー オブジェクトを 12.x ポリシー ストアにインポートします。

   ```
   XPSImport smpolicy.xml –npass
   ```

5. r12.x 環境に smkeydatabases が含まれる場合、以下を実行します。
   a. すべてのインスタンスを同期する。
   b. 12.52 SP1 証明書データ ストアに smkeydatabase のコンテンツを移行する。
6. r12.x 環境で レガシー フェデレーション（フェデレーション セキュリティ サービス）オブジェクトを管理している場合は、アサーション発行者 ID を移行します。
7. 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。

詳細情報:

証明書データの管理 (P. 31)
キー データベース インスタンスの同期 (P. 53)

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 12.52 SP1 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。
- 12.52 SP1 ポリシー ストアに接続する 12.52 SP1 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 ストアを使用することにより、すべてのポリシー サーバに関連付けられる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。

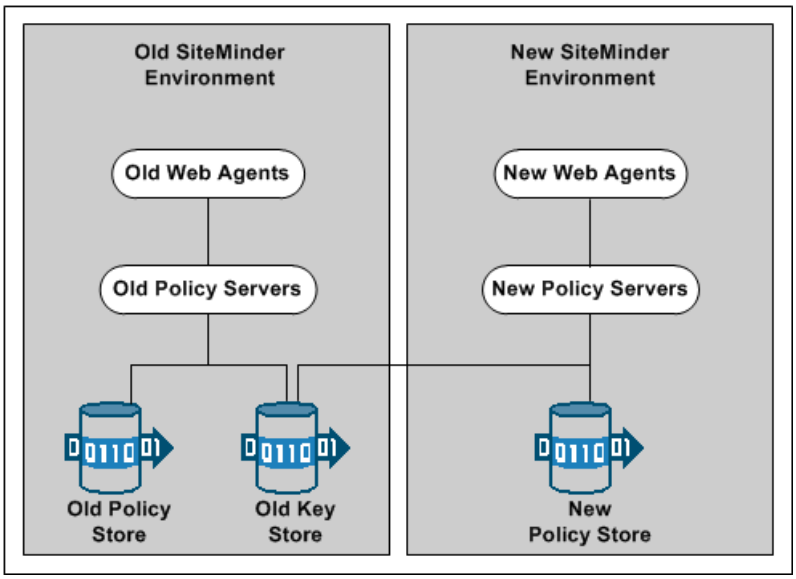
- 共通キー ストアに接続して新しいキーを取得するすべてのポリシー サーバ。

  重要: 12.52 SP1 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、12.52 SP1 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、フェールオーバ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。

図 13: r12.x の共通キー ストアの展開



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、12.52 SP1 ポリシー サーバはキー ロールオーバーに 12.52 SP1 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。
- 12.52 SP1 ポリシー ストアに接続する 12.52 SP1 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。
- 12.52 SP1 キー ストアに接続して新しいキーを取得する 12.52 SP1 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。

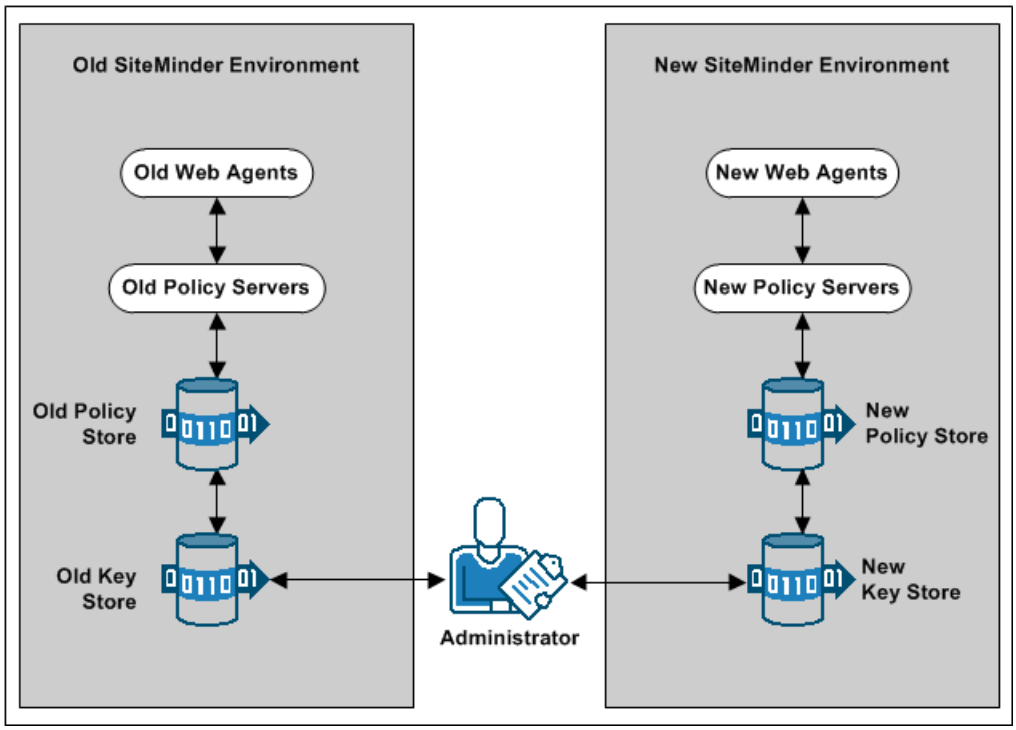
  重要: すべてのキー ストアで同じエージェントとセッション キーが使用されるわけではない場合、シングル サインオンに失敗します。

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 12.52 SP1 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 12.52 SP1 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、フェールオーバ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。

図 14: r12.x の複数キー ストアの展開



12.52 SP1 環境の作成

既存の環境から独立した 12.52 SP1 環境を設定できます。 12.52 SP1 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。 12.52 SP1 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。
  - 個別にキー ストアが設定されている r12.x 環境の場合は、キー ストアのバージョンを r12.x のままにします。 12.52 SP1 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 12.52 SP1 キー ストアと通信できません。
  - ポリシーとキー ストアが連結して設定されている r12.x 環境の場合、r12.x キーを別個の r12.x キー ストアに分けます。

- キー ストアのバージョンを r12.x のままにします。 12.52 SP1 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 12.52 SP1 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。 12.52 SP1 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。

ポリシー ストアからキー ストアを分ける方法

ポリシー ストアからキー ストアを分けるには、以下の手順を実行します。

1. セット アップ ポリシー サーバをインストールするか、見つけます。 セット アップ ポリシー サーバは、ポリシーとキー ストアが連結して設定されないポリシー サーバのことです。
   - ポリシーとキー ストアが連結して設定されているポリシー サーバの場合、それを使用して新しいキー ストア インスタンスを設定できません。ポリシー サーバ ホスト システムで利用できる必要な SiteMinder ユーティリティは、連結したストアを管理するように設定されます。
   - セット アップ ポリシー サーバは、必要なユーティリティの個別のセットを利用可能にします。個別のセットを使用することにより、連結されたストアを妨げずにキー ストアを設定できます。

2. セットアップ ポリシー サーバ ホスト システムを使用して、個別の r12.x キー ストア インスタンスを作成しします。 以下の点を考慮します。
   - キー ストアはデフォルトのポリシー ストア スキーマのみを必要とします。個別のキー ストアを設定する詳細については、r12.0 SP3 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。
   - キー ストアについては、以下の処理は不要です。
     - SiteMinder スーパーユーザ パスワードを設定します。
     - デフォルトのポリシー ストア オブジェクトをインポートします。
3. r12.x 環境の動的エージェント キー生成を無効にします。

   注: 利用している環境がスタティック キーを使用する場合、この手順は必要ありません。ただし、ポリシー ストアからキーをエクスポートした後 SiteMinder 管理者がランダムなエージェント キーを生成しないことを確認してください。
4. r12.x ポリシー/キー ストアからエージェント キーをエクスポートします。
5. r12.x キー ストアにエージェント キーをインポートします。
6. すべてのポリシー サーバを設定して、個別のキー ストアを使用します。
7. 動的エージェント キーの生成を無効にした場合は、それを再度有効にします。

動的エージェント キー生成の無効化

キー ストアの個別化を完了していない場合、r12.x 環境では以下のように 2 種類のキー ストアで動作しています。

- 一部のポリシー サーバは連結されたポリシー/キー ストアでエージェント キーを使用します。
- 一部のポリシー サーバは個別のキー ストアでエージェント キーを使用します。

動的エージェント キーの生成を無効にすると、個別のストアに対してエクスポートした後、ポリシー サーバがキーを生成しません。ポリシー サーバがキーを生成しないと、キーがすべてのストアで同期されない場合に生じるシングル サインオンの問題を回避します。

以下の手順に従います。

1. r12.x 管理 UI にログインします。
2. ［管理］-［ポリシー サーバ］をクリックします。
3. ［キー管理］-［エージェント キー管理］をクリックします。
4. ［スタティック エージェント キーを使用］オプションを選択します。
5. ［サブミット］をクリックします。

   ポリシー サーバはスタティック キーを使用するように設定されます。ポリシー サーバはキーを自動的に生成しません。

エージェント キーのエクスポート

連結されたポリシー/キー ストアからキーをエクスポートして、それらを個別のキー ストアに利用できるようにします。

以下の手順に従います。

1. r12.x ポリシー サーバ ホスト システムにログインします。 このポリシー サーバが、連結されたポリシー/キー ストアで設定されていることを確認します。
2. 以下のコマンドを実行して、ポリシー ストアからキーのみをエクスポートします。

   ```
   smkeyexport -dadministrator -wpassword -ofile_name
   ```

   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する前に、管理者権限でコマンド ライン ウィンドウを開きます。 アカウントに管理者権限がある場合でも、このようにコマンド ライン ウィンドウを開きます。

   注: ユーティリティの詳細については、r12.x の「*ポリシー サーバ管理ガイド*」を参照してください。

   例：

   ```
   smkeyexport -dsuperuser -wpassword -oagentkeys
   ```

   エージェント キーが連結されたポリシー/キー ストアからエクスポートされます。
3. セットアップ ポリシー サーバ ホスト システムに、エージェント キーを含むファイルをコピーします。

エージェント キーのインポート

連結されたポリシー/キー ストアからキーをインポートして、それらを個別のキー ストアに利用できるようにします。

以下の手順に従います。

1. r12.x セットアップ 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て、個別のキー ストアにエージェント キーをインポートします。

   `smobjimport -f`*`file_name`* `-k`

   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する前に、管理者権限でコマンド ライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンド ライン ウィンドウを開きます。

   注: これらのモードと引数の詳細については、r12.x の「*ポリシー サーバ管理ガイド*」を参照してください。

   例 :

   ```
   smobjimport -fagentkeys -k
   ```

   エージェント キーが個別のキー ストアにインポートされます。

すべてのポリシー サーバを設定して、キー ストアを使用します。

並列の環境ですべてのポリシー サーバを設定して共通の r12.x キー ストアを使用すると、両方の環境でシングル サインオンを維持します。

以下の手順に従います。

1. エージェント キーを動的に生成する際に指定されるポリシー サーバを特定します。 このポリシー サーバをキー ストアで最後に設定します。
2. 環境内の他のすべてのポリシー サーバに対して、以下の手順を実行します。
   a. ポリシー サーバ ホスト システムにログインします。
   b. ポリシー サーバ管理コンソールを開きます。
   c. ［データ］タブをクリックします。

d. ［データベース］リストから［キー ストア］を選択し、［ポリシー ストアを使用］データベース オプションをクリアします。

e. ［ストレージ］リストからキー ストアのタイプを選択します。

f. 以下のいずれかの操作を実行します。

- （LDAP）［LDAP キー ストア］セクションに必要な接続情報を入力します。
- （ODBC）［データ ソース情報］セクションにデータ ソース情報を入力します。

g. 接続をテストします。

h. ［OK］をクリックします。

i. ポリシー サーバを再起動して、キー ストアを使用するようにポリシー サーバを設定します。

3. キー ストアを使用するためにエージェント キーの生成に指定されるポリシー サーバを設定します。

動的エージェント キー生成の再有効化

動的エージェント キー生成を無効にした場合は、エージェント キーの生成に指定されるポリシー サーバの機能を再度有効にします。 環境内のすべてのポリシー サーバが新規キー ストアを使用するように設定した後でのみ、この手順を実行します。

以下の手順に従います。

1. r12.x 管理 UI にログインします。
2. ［管理］-［ポリシー サーバ］をクリックします。
3. ［キー管理］-［エージェント キー管理］をクリックします。
4. ［動的エージェント キーを使用］オプションを選択します。
5. ［サブミット］をクリックします。

   指定されたポリシー サーバはキーを動的に生成するために有効にされます。

ポリシー ストアからキー ストアを分けるために必要な処理が完了しました。

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 12.52 SP1 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 12.52 SP1 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。

キーと証明書の移行

環境に 1 つ以上の smkeydatabases が含まれる場合は、12.52 SP1 証明書データ ストアにそれらのコンテンツを移行します。

以下の手順に従います。

1. 必ずすべての r12.x smkeydatabases を同期します (P. 53)。
2. r12.x ポリシー サーバ ホスト システムにログインし、以下のディレクトリに移動します。

   siteminder_home¥config¥properties

   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. 以下のファイルをコピーします。

   smkeydatabase.properties

4. 12.52 SP1 ポリシー サーバ ホスト システムにログインし、以下の手順を実行します。
   a. 以下の場所に移動します。

      siteminder_home¥config¥properties

   b. smkeydatabase プロパティ ファイルの 12.52 SP1 バージョンの名前を以下の値に変更します。

      newsmkeydatabase.properties

   c. プロパティ ファイルの r12.x バージョンをディレクトリに追加します。
   d. テキスト エディタで 12.52 SP1 および r12.x プロパティ ファイルを開きます。
   e. r12.x バージョンのデータベースのパスを編集して、12.52 SP1 バージョンのパスに一致させます。

      例：

      r12.x ファイルは以下のパスを参照します。

      DBLocation=C¥:/Program Files/netegrity/siteminder/smkeydatabase

      12.52 SP1 ファイルは以下のパスを参照します。

      DBLocation=C:/Program Files/CA/siteminder/smkeydatabase

      r12.x ファイルを更新して以下のパスを参照するようにします。

      DBLocation=C¥:/Program Files/CA/siteminder/smkeydatabase

   f. r12.x プロパティ ファイルを保存し、12.52 SP1 プロパティ ファイルを閉じます。
   g. ポリシー サーバ インストールのルートで以下のディレクトリを作成します。

      smkeydatabase

      例：

      C:¥Program Files¥CA¥SiteMinder¥smkeydatabase

5. r12.x ポリシー サーバ ホスト システムに戻り、smkeydatabase ディレクトリの内容をコピーします。

   注: このファイルのデフォルトの場所は *siteminder_home* です。

6. 12.52 SP1 ポリシー サーバ ホスト システムに戻り、以下の手順を実行します。
   a. 作成した 12.52 SP1 smkeydatabase ディレクトリに、r12.x smkeydatabase ディレクトリの内容を追加します。
   b. 以下の移行ユーティリティを使用して、smkeydatabase を証明書データ ストアに移行します。

      ```
      smmigratecds
      ```

   c. 移行が成功したら、smkeydatabase プロパティ ファイルおよび smkeydatabase ディレクトリを削除します。

   これで移行は完了です。

詳細情報:

手動による SiteMinder キー データベースの移行 (P. 189)

アサーション発行者 ID の移行

r12.x 環境で レガシー フェデレーション（フェデレーション セキュリティ サービス）オブジェクトを管理している場合は、r12.x プロデューサ から 12.52 SP1 プロデューサ にアサーション発行者 ID を移行します。ID の移行により、SAML 1.1 トランザクションがサービス プロバイダで失敗するのを防ぎます。

以下の手順に従います。

1. r12.x ポリシー サーバ ホスト システムにログインし、以下のディレクトリに移動します。

   siteminder_home¥config¥properties

   siteminder_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のファイルをコピーします。

   AMAssertionGenerator.properties

3. 12.52 SP1 ポリシー サーバ ホスト システムにログインし、以下のディレクトリに移動します。

   siteminder_home¥config¥properties

4. アサーション ジェネレータのプロパティ ファイルの 12.52 SP1 バージョンの名前を以下の値に変更します。

   newAMAssertionGenerator.properties

5. プロパティ ファイルの r12.x バージョンをディレクトリに追加します。

   これで移行は完了です。

r12.x ポリシーの移行

12.52 SP1 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 12.52 SP1 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、12.52 SP1 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. 12.52 SP1 バージョンの XPSImport ユーティリティを使用して 12.52 SP1 ポリシー ストア データをインポートします。 12.52 SP1 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 12.52 SP1 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、12.52 SP1 にアップグレードされた環境は、FIPS 互換モードで動作します。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。ユーザの組織で FIPS 互換アルゴリズムを使用する必要がない場合、環境はそれ以上の設定を行わなくても、FIPS 互換モードで動作します。

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 12.52 SP1 環境を FIPS 専用モードに移行できます。FIPS 移行モードでは、12.52 SP1 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、以下を含め、12.x より前のバージョンの SiteMinder と相互運用することはできず、後方互換性もありません。

   - すべてのエージェント
   - 古いバージョンのエージェント API を使用するカスタム ソフトウェア
   - PM API、またはポリシー サーバが表示するその他の API を使用するカスタム ソフトウェア

   そのようなソフトウェアをすべて対応する SDK の 12.52 SP1 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。

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 12.52 SP1 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。

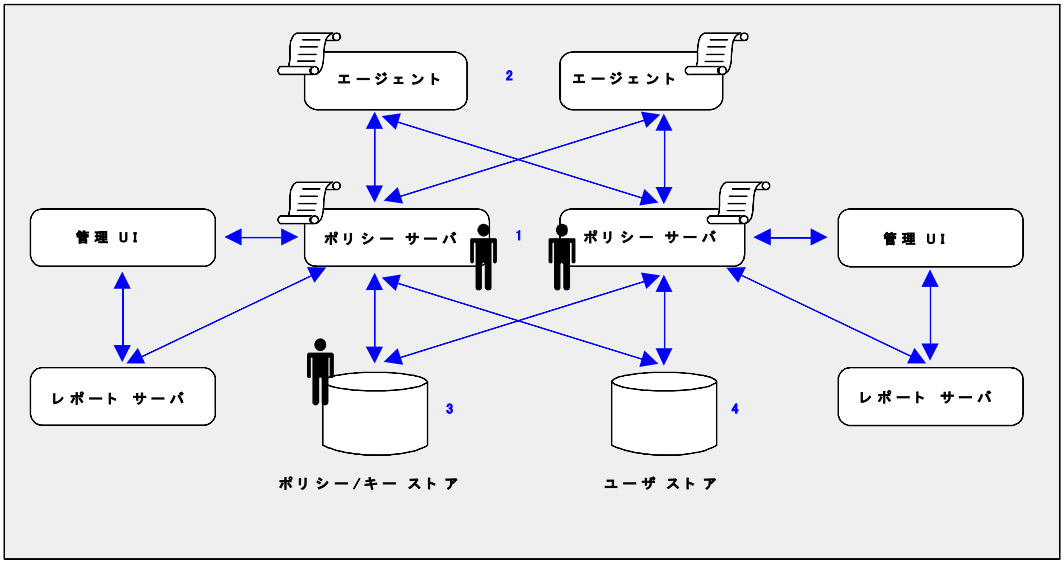
移行のロードマップ - 機密データの暗号化

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 12.52 SP1 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。

   - 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 キーは EncryptionKey.txt ファイルにあります。
   - 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 ストア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: パスワードは、デフォルト SiteMinder 管理者アカウントのパスワードです。 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。 パスワード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 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、ユーザにログインするか、パスワードを変更するように通知します。

   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または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。

- **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。

- **スーパー ユーザ アカウントの名前とパスワード** - 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。

以下の手順に従います。

1. ポリシー サーバをホストしているコンピュータでコマンド 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 サーバの停止と開始についての詳細は、「*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実行します。
   - 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、システムを再起動します。
   - 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、以下の手順に従います。
     a. ポリシー サーバの起動に使用されるユーザとしてログインします。
     b. コマンド プロンプトを開きます。
     c. *policy_server_home*/config に移動します。
     d. 以下のコマンドを実行します。

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

以下の手順に従います。

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開始についての詳細は、「*ポリシー サーバ管理ガイド*」を参照してください。

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 ストアの 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 ストア

   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。

パスワード

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。以下の操作を行うことができます。

- 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 12.52 SP1 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 12.52 SP1 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. 12.52 SP1 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 -xe -xp -pass <passphrase> -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

   -xe

   実行環境に関連付けられるオブジェクト タイプをエクスポートします。

   -xp

   ポリシーに関連付けられるオブジェクト タイプをエクスポートします。

-pass <passphrase>

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 -pass <passphrase> -vT -vI -vW -vE -vF -l log_path
```

input_file

入力 XML ファイルを指定します。

-pass <passphrase>

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。

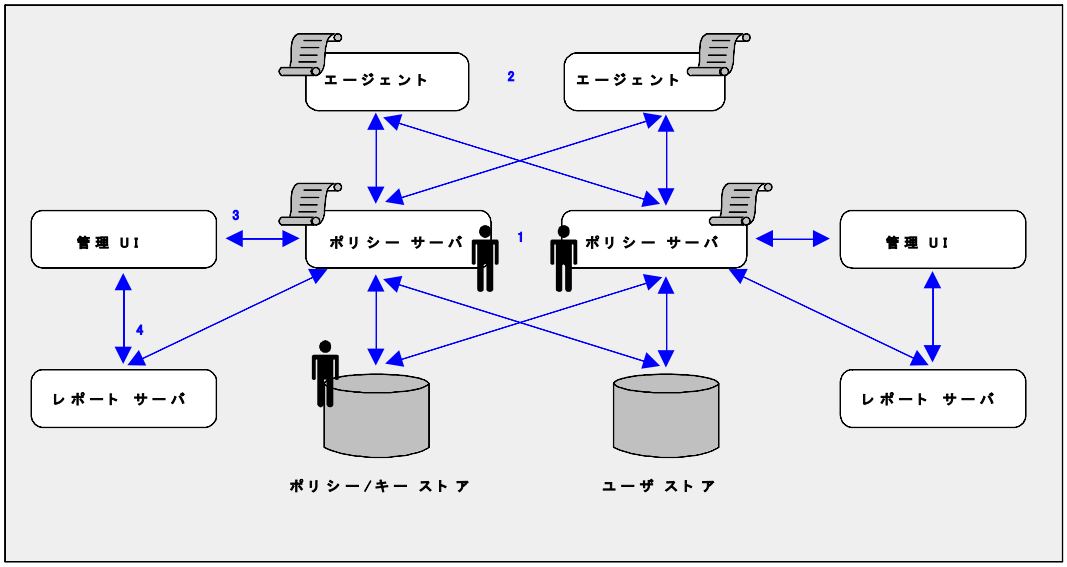
移行ロードマップ - FIPS 専用モードの設定

以下の図は、FIPS 移行モードで動作しているサンプル 12.52 SP1 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. 163)」を参照してください。

以下の手順に従います。

1. ポリシー サーバのホスト システムからコマンド 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 サーバの停止と開始についての詳細は、「*ポリシー サーバ管理ガイド*」を参照してください。

3. 以下のいずれかを実行します。

   - 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、システムを再起動します。
   - 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、以下の手順に従います。

     a. ポリシー サーバの起動に使用されるユーザとしてログインします。

     b. コマンド プロンプトを開きます。

     c. *policy_server_home*/config に移動します。

     d. 以下のコマンドを実行します。

     ```
     ./ca_ps_env.ksh
     ```

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. 以下のいずれかを実行します。
   - 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. 以下のいずれかを実行します。
   - （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。

     データ

     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。

  データ

  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。

  データ

  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*

（任意）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*

（任意）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*

（任意）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

（任意）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*

（任意）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*

（任意）例外を指定されたパスに送信します。

デフォルト： stderr

-vT

（任意）詳細レベルを TRACE に設定します。

-vI

（任意）詳細レベルを INFO に設定します。

-vW

（任意）詳細レベルを WARNING に設定します。

-vE

（任意）詳細レベルを ERROR に設定します。

-vF

（任意）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. 以下のいずれかを実行します。
   - 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。

管理 UI 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*

（任意）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

（任意）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*

（任意）例外を指定されたパスに送信します。

デフォルト： stderr

-vT

（任意）詳細レベルを TRACE に設定します。

-vI

（任意）詳細レベルを INFO に設定します。

-vW

（任意）詳細レベルを WARNING に設定します。

-vE

（任意）詳細レベルを ERROR に設定します。

-vF

（任意）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、ユーザがポリシー サーバに登録するために、登録処理に関する具体的情報が必要です。

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

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*

（任意）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

（任意）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*

（任意）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 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*

（任意）例外を指定されたパスに送信します。

デフォルト： stderr

-vT

（任意）詳細レベルを TRACE に設定します。

-vI

（任意）詳細レベルを INFO に設定します。

-vW

（任意）詳細レベルを WARNING に設定します。

-vE

（任意）詳細レベルを ERROR に設定します。

-vF

（任意）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¥CommonReporting3

デフォルト：（UNIX）/opt/CA/SharedComponents/CommonReporting3

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する前に、管理者権限でコマンド ライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンド ライン ウィンドウを開きます。

   - （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。

第 5 章: SiteMinder キー データベース移行のトラブルシューティング

SiteMinder キー データベースの移行の状況がわからない

症状：

ポリシー サーバがアップグレードされたことはわかります。 ただし、証明書データ ストアに smkeydatabase が問題なく移行されたか不確かです。

解決方法：

smkeydatabase 移行ユーティリティ（smmigratecds）を使用して、移行が成功したことを確認します。

注: このユーティリティのデフォルトの場所は *siteminder_home*¥bin です。

siteminder_home

ポリシー サーバのインストール パスを指定します。

以下の手順に従います。

1. smkeydatabase が連結されているポリシー サーバ ホスト システムにログインします。
2. 以下のいずれかを実行します。
   - （Windows）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。

     ```
     smmigratecds.bat –isComplete
     ```

     -isComplete

     前の移行が成功したことを確認します。
   - （UNIX）シェルを開き、以下のコマンドを実行します。

     ```
     smmigratecds.sh –isComplete
     ```

   移行が成功していた場合、システムで移行がすでに成功したことを示すメッセージが表示されます。 移行が失敗していた場合、システムで移行を実行する必要があることを示すメッセージが表示されます。

証明書データ ストアのエラーが表示される

症状：

証明書データ ストアが設定されていないことを示すメッセージが表示されました。

解決方法：

以下の手順に従います。

1. r6.x からアップグレードしている場合は、ポリシー ストア スキーマを拡張します (P. 40)。
2. ポリシー サーバ ホスト システムにログインします。
3. 以下のコマンドを実行します。

   ```
   XPSDDInstall CDSObjects.xdd
   ```

   ポリシー ストア スキーマが拡張されて、証明書データ ストアをサポートします。
4. 以下のいずれかを実行します。
   - （Windows）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。

     ```
     smmigratecds.bat –validateInstall
     ```

     validateInstall

     証明書データ ストアが正しくインストールされているかどうかを確認します。
   - （UNIX）シェルを開き、以下のコマンドを実行します。

     ```
     smmigratecds.sh -validateInstall
     ```

     証明書データ ストアが正しく設定される場合、インストールが有効であることを示すメッセージが表示されます。 証明書データ ストア のインストールが失敗した場合、インストールが有効ではないことを示すメッセージが表示されます。
5. SiteMinder キー データベースを手動で移行します。

詳細情報:

手動による SiteMinder キー データベースの移行 (P. 189)

移行失敗のエラーが表示される

症状:

smkeydatabase 移行が失敗したことを示すメッセージが表示されました。

解決方法:

移行ユーティリティ（smmigratecds）により、smkeydatabase のコンテンツが証明書データ ストアと比較され、1 つ以上のデータ不整合が検出されています。 データ不整合の一例として、別の証明書への同じエイリアスのマッピングがあります。

これらの不整合があると移行は成功しません。

以下の手順に従います。

1. smkeydatabase 移行ログ（smkeydatabaseMigration.log）を使用して、問題を特定します。

   ログは *siteminder_home*¥log にあります。

   siteminder_home

   ポリシー サーバのインストール パスを指定します。

2. アクセス レガシー キー ストア フラグ（–accessLegacyKS） を含む smkeytool ユーティリティを使用して、smkeydatabase にアクセスします。
3. 移行失敗の原因となったデータ不整合を解決します。

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

4. smkeydatabase を手動で移行します。

手動による SiteMinder キー データベースの移行

症状:

smkeydatabase 証明書データを証明書データ ストアに手動で移行する場合は、以下のようにします。

解決方法:

smkeydatabase 移行ユーティリティ（smmigratecds）を使用します。

以下の手順に従います。

1. 必ずすべての smkeydatabases インスタンスを同期します (P. 53)。
2. smkeydatabase が連結されているポリシー サーバ ホスト システムにログインします。
3. 証明書データ ストアが正しく設定されていることを確認するために、以下のいずれかの手順を実行します。
   - （Windows）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。

     ```
     smmigratecds.bat –validateInstall
     ```

     -validateInstall

     証明書データ ストアが正しくインストールされているかを検証します。
   - （UNIX）シェルを開き、以下のコマンドを実行します。

     ```
     smmigratecds.sh -validateInstall
     ```
4. 以下のいずれかの手順を実行して、smkeydatabase のコンテンツを証明書データ ストアと比較します。コンテンツの比較によって、移行の成功を妨げるデータの不整合が特定されます。
   - （Windows）以下のコマンドを入力します。

     ```
     smmigratecds.bat –validate -log log_file
     ```

     -validate

     smkeydatabase のコンテンツを証明書データ ストアと比較します。

     -log

     検証結果がログに送信されます。

     log_file

     ログ ファイルの名前と、それがユーティリティによって送信される送信先を指定します。

     例： -log "C:¥Progam Files¥Sample¥Logs"
   - （UNIX）以下のコマンドを入力します。

     ```
     smmigratecds.sh -validate -log log_file
     ```
5. （オプション）データの不整合が存在する場合は、ログ ファイルを使って問題を特定します。

6. 以下のいずれかの手順を実行して、移行を開始します。
   - （Windows）以下のコマンドを入力します。

     `smmigratecds.bat -migrate -log log_file`

     -migrate

     smkeydatabase を証明書データ ストアに移行します。

     -log

     移行の実行結果がログに送信されます。

     log_file

     ログ ファイルの名前と、それがユーティリティによって送信される送信先を指定します。

     例： -log "C:¥Progam Files¥Sample¥Logs"

   - （UNIX）以下のコマンドを入力します。

     `smmigratecds.sh -migrate -log log_file`

7. （オプション）移行が失敗した場合は、ログ ファイルを使用して原因を特定します。