SiteMinder

実装ガイド

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。

- CA RiskMinder<tm>（旧 CA Arcot RiskFort）
- CA AuthMinder®（旧 CA Arcot WebFort）
- CA SiteMinder® Federation
- CA Directory
- CA DataMinder®（旧 CA DLP） Content Classification Service
- 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

以下のドキュメントの更新は、本書の最新のリリース以降に行われたものです。

- 定期的なメンテナンス タスク (P. 230) - XPS スイーパ ユーティリティを実行するためのガイダンスの更新 (169270、168658、21175885:01)。

目次

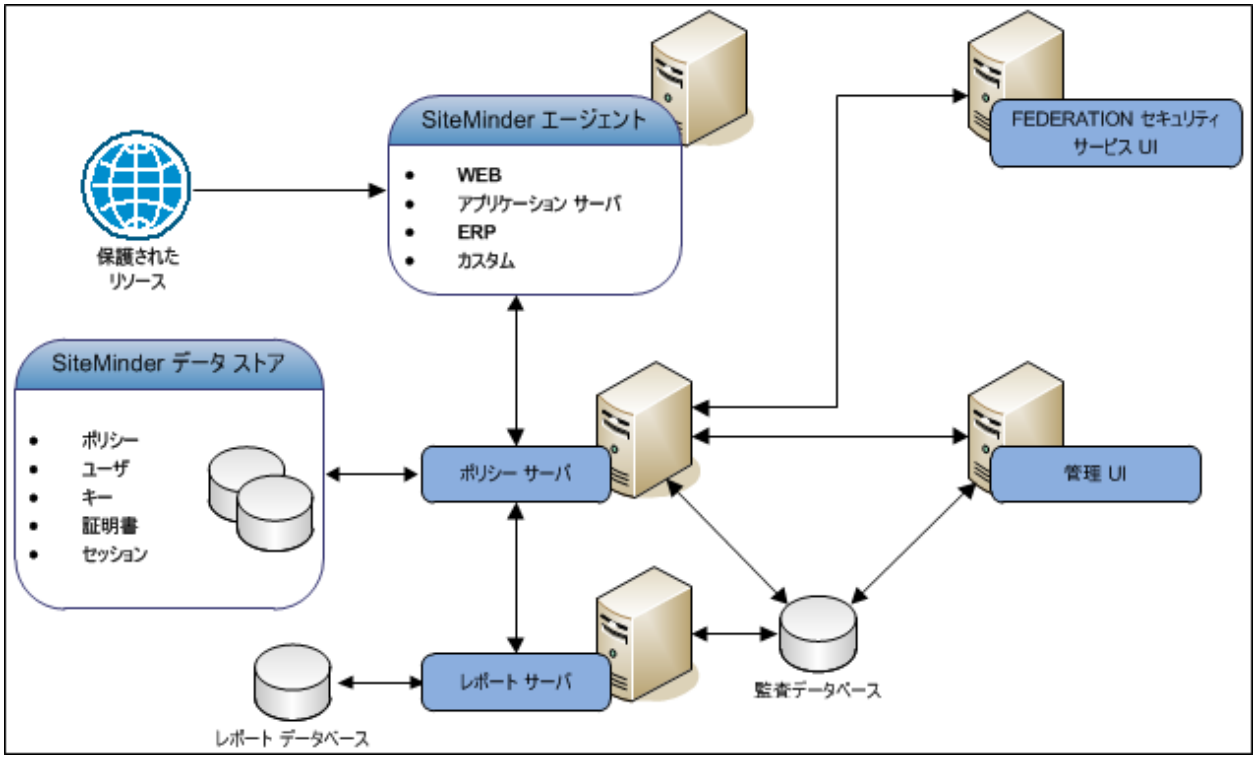
第 1 章: SiteMinder コンポーネントおよびストア

コンポーネントおよびストア

SiteMinder 環境には複数のコンポーネントが含まれます。コンポーネントのなかにはリソースを保護するために必要なものもありますが、オプションのものや、特定の機能を実装するためにのみ必要なものもあります。これらのコンポーネントは、組織内のリソース、アプリケーション、ディレクトリ、およびデータベースと連携して、企業ネットワーク内のリソースへの安全なアクセスを提供します。

すべての SiteMinder コンポーネントは、さまざまなオペレーティング環境上でサポートされています。 SiteMinder の実装は、それを展開する環境に大きく依存します。 実装については、必ずしも以下の図の通りである必要はありません。 以下の図は、SiteMinder 環境の主要コンポーネントとそれら相互の一般的な関係を示すことを目的とするものです。

図 1: 製品コンポーネント概要



このマニュアルで詳述されているアーキテクチャの問題を検討する場合のリソースとして、上図および以下のコンポーネントの説明を使用してください。

ポリシー サーバ

（必須）SiteMinder ポリシー サーバ（ポリシー サーバ）は、ポリシー決定ポイント（PDP）として働きます。 ポリシー サーバの目的は、アクセス制御ポリシーを評価および実行することです。その際、ポリシー サーバは SiteMinder エージェントと通信します。ポリシー サーバは、以下を提供します。

- ポリシー ベースのユーザ管理
- 認証サービス
- 認可サービス
- パスワード サービス
- セッション管理
- 監査サービス

ポリシー サーバは、これらのタスクを実行するために他のすべての主要コンポーネントと交信します。

SiteMinder エージェント

（必須）SiteMinder エージェントは、Web サーバ、J2EE アプリケーション サーバ、Enterprise Resource Planning（ERP）システムまたはカスタム アプリケーション上に存在することができます。 エージェントは、リソース用ユーザ リクエストをインターセプトし、リソースが保護されるかどうか決定するためにポリシー サーバと通信して、ポリシー実行ポイント（PEP）として機能します。

リソースが保護されない場合、エージェントはアクセスを許可します。リソースが保護されている場合、エージェントはユーザを認証および認可するためにポリシー サーバとの通信を続行します。 認可が正しく行われると、エージェントはリソース リクエストをサーバに送るよう要求されます。 さらにエージェントは以下のような働きをします。

- コンテンツのパーソナライズを有効にするために、Web アプリケーションに情報を提供します。
- 認証されたユーザおよび保護されたリソースに関する情報をキャッシュして、リソースへのより迅速なアクセスを可能にします。
- シングル サインオン（SSO）の有効化

eTrust SOA Security Manager エージェント

（eTrust SOA Security Manager に必要） eTrust SOA Security Manager （WSS）エージェントは、以下のプラットフォームで動作するポリシー実行ポイント（PEP）として機能します。

- Web サーバ
- J2EE アプリケーション サーバ
- カスタム アプリケーション

WSS エージェントは、「大きな」（SOAP 基づく）Web サービスのリクエストをインターセプトします。その後、WSS エージェントはポリシー サーバと通信して、リソースが保護されているかどうかを判断します。

注: JBoss 用の SiteMinder エージェントには SiteMinder *および*WSS エージェントの機能が含まれます。 .

リソースが保護されない場合、エージェントはアクセスを許可します。リソースが保護されている場合、エージェントはユーザを認証および許可するためにポリシー サーバとの通信を続行します。 認可が正しく行われると、エージェントはリソース リクエストをサーバに送るよう要求されます。

また、エージェントは以下の他の機能を実行します。

- 認証されたユーザおよび保護されたリソースに関する情報をキャッシュして、リソースへのより迅速なアクセスを可能にします。
- シングル サインオン（SSO）の有効化

CA Business Intelligence

（オプション）CA Business Intelligence は、レポーティングおよび分析ソフトウェアのセットです。情報の提示およびビジネス意思決定をサポートするために、さまざまな CA 製品により使用されます。CA 製品は、CA Business Intelligence を使用して、さまざまなレポート オプションによって、効果的な企業 IT 管理に必要な情報を統合、分析、および表示します。

CA Business Intelligence には、情報管理、レポート、クエリ、および解析用の各ツールからなる完全なスイートである SAP BusinessObjects Enterprise が含まれています。 CA Business Intelligence は、スタンドアロン コンポーネントとして SAP BusinessObjects Enterprise をインストールします。 このガイドでは、このスタンドアロン コンポーネントをレポート サーバと呼びます。 レポート サーバのインストールは全体的な SiteMinder インストール プロセス内の独立した手順です。SiteMinder 固有のコンポーネントとは別にレポート サーバをインストールすると、他の CA 製品が同じ Business Intelligence Services を共有できるようになります。

レポート サーバは SiteMinder 環境の分析を助けるためにレポートをコンパイルします。 このコンポーネントの目的は、以下のタイプのレポートを作成することです。

- 監査
- ポリシー分析

レポート サーバは、レポートを編集するために以下のコンポーネントと通信します。

- 集中管理サーバ（CMS）データベース（レポート データベース）
- 管理 UI
- ポリシー サーバ
- SiteMinder 監査データベース

データ ストア

SiteMinder の実装には複数のデータ ストアが含まれます。ストアによっては必須のものがありますが、その他はオプション、または特定の機能を実装する場合にのみ必要です。

以降では、以下について説明します。

- ストアが必須またはオプションの場合
- ストアの目的

ポリシー ストア

（必須）SiteMinder ポリシー ストア（ポリシー ストア）は、LDAP ディレクトリ サーバまたは ODBC データベース内に存在する資格情報ストアです。 このコンポーネントの目的は、以下を含むすべてのポリシー関連のオブジェクトを格納することです。

- SiteMinder が保護しているリソース
- それらのリソースを保護するために使用されるメソッド
- それらのリソースにアクセス可能またはアクセス不可能な、ユーザまたはグループ
- ユーザが保護されたリソースへのアクセスを許可または拒否されたときに実行されるべきアクション

ポリシー サーバは、エンタープライズ ポリシー管理（EPM）アプリケーションまたは SiteMinder ポリシーと総称されるこの情報を使用して、リソースを保護するかどうか、そして認証されたユーザによるリクエストされたリソースへのアクセスを許可するかどうかを決定します。

ユーザ ストア

（必須）SiteMinder ユーザ ストア接続（ユーザ ストア接続）は、企業ネットワーク内の既存のユーザ ディレクトリまたはデータベースへの接続です。 独自の SiteMinder ユーザ ストアを使用する必要はありません。 ユーザ ストア接続の目的は、ユーザ データをポリシー サーバで使用可能にすることです。それには以下が含まれます。

- 組織の情報
- ユーザおよびグループの属性
- パスワードなどのユーザ認証情報
- 名と姓などのユーザ属性

ポリシー サーバはこれらの接続を使用して、以下を実行します。

- エージェントが保護されたリソースへのリクエストをサブミットするときに、ユーザ認証情報を確認する
- 特定のユーザ データを必要とする SiteMinder 機能用のユーザ属性を取得する

注: ユーザ ストア接続の設定の詳細については、ドキュメント ロードマップを参照してください。

外部管理ユーザ ストア

（オプション）デフォルトでは、管理 UI は SiteMinder 管理者認証情報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により、ポリシー ストアの設定および 管理 UI のインストール直後から環境を管理することができます。 ポリシー ストアの設定時に、デフォルトの SiteMinder スーパーユーザ アカウント（siteminder）が作成されます。 このアカウントには最大のシステム権限があり、初めて 管理 UI にアクセスする場合、および追加の SiteMinder 管理者を作成する場合に使用されます。

たとえばコーポレート ディレクトリのような外部管理ユーザ ストアを使用するために、管理 UI を設定することができます。 外部管理ユーザ ストアは、エンタープライズ ネットワーク内の LDAP ディレクトリ サーバまたは ODBC データベースへの接続です。以下の点について考慮してください。

- 管理 UI は単一の外部管理ユーザ ストアにのみ接続できます。
- 複数のポリシー サーバを管理するように 管理 UI を設定できます。 管理 UI が複数のポリシー サーバを管理するためには、外部管理者ユーザ ストアへの接続が必要です。
- 高可用性用のために複数の 管理 UI を設定する場合、同じ外部管理ユーザ ストアによってすべての管理者が各 管理 UI を使用できるようになります。

注: SiteMinder 管理者および外部管理ユーザ ストアの設定の詳細については、ドキュメント ロードマップを参照してください。

キーストア

（必須）このコンポーネントの目的は、機密データを暗号化するためにポリシー サーバとエージェントが使用する暗号化キーを格納することです。キーには以下のものが含まれます。

- SiteMinder Cookie を暗号化するためにエージェントが使用するキー
- ポリシー ストアの機密情報を暗号化するためにポリシー サーバが使用するキー。管理者パスワードなどがあります。
- 認証情報およびユーザ セッションに関連するその他情報が含まれる SiteMinder セッション チケットを暗号化するためにポリシー サーバが使用するキー

キー ストアをポリシー ストアと連結させることができます。または、個別のディレクトリまたはデータベースに暗号化キーを格納できます。 個別のキー ストアを展開する必要があるかどうかは以下によって決まります。

- ポリシー サーバおよびポリシー ストアをどのように実装するか。
- シングル サインオン要件

注: ポリシー サーバ設定ウィザードを使用してポリシー ストアを設定する場合、キー ストアがポリシー ストアと自動的に連結されます。

証明書データ ストア

（オプション） SiteMinder 証明書データ ストア（CDS）によって、以下のコンポーネントおよび機能を SiteMinder 環境で利用できるようになります。

- 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（CRL）
- OCSP 破棄チェック

注: SiteMinder フェデレーション機能は証明書データ ストアを使用します。X.509 証明書認証方式が認証に使用するユーザ証明書は、証明書データ ストアに格納されません。 これらのユーザ証明書は LDAP/AD ユーザ ディレクトリまたは ODBC ストアに格納されます。

デフォルトでは、証明書データ ストアは、自動的に設定され、ポリシー ストアと同じ場所に格納されます。 結果は、以下のようになります。

- 別個の外部ストアは不要です。
- 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破棄リストにアクセスできます。
- 同じポリシー ストアを管理する SiteMinder 管理者はすべて、管理 UI を使用して、証明書データ ストアを集中管理できます。

SiteMinder 監査データベース

（オプション）デフォルトでは、ポリシー サーバは監査イベントをテキスト ファイルに書き込みます。これはポリシー サーバ ログとして知られています。監査ログの目的は、以下を含むすべてのユーザ アクティビティに関する情報を追跡することです。

- すべての成功した認証
- すべての失敗した認証
- すべての成功した認可試行

- すべての失敗した認可試行
- すべての管理ログイン試行
- 管理者パスワードの変更、ポリシー ストア オブジェクトの作成およびポリシー ストア オブジェクトの変更といった、すべての管理アクション

ただし、スタンドアロン SiteMinder 監査データベース (監査データベース) を設定することができます。 監査イベントの格納場所を決定するときは、以下を考慮します。

- レポート サーバは、監査ベースのレポートを作成するために監査データベースへの接続を必要とします。レポート サーバは、テキスト ファイルに書き込まれたポリシー サーバ ログから監査ベースのレポートを作成することはできません。
- テキスト ファイルに情報を記録するよりも、監査ログをデータベースに格納する方が安全です。
- サポートされている場合は、ポリシー ストアは監査データベースとしても機能することができます。

注: 監査データベースの設定する詳細については、ドキュメント ロードマップを参照してください。

セッション ストア

（オプション）SiteMinder がユーザを認証するときに、ポリシー サーバはセッション チケットを発行します。 セッション チケットには、ユーザの基本情報およびユーザの認証情報が含まれます。 デフォルトでは、SiteMinder は非永続セッションによってセッション管理を実装します。非永続セッションが有効な場合、エージェントはユーザのブラウザ上の Cookie にセッション チケットを書き込みます。ただし、SiteMinder 機能によっては永続セッションが必要な場合があります。

永続セッションが有効な場合、エージェントはスタンドアロン データベースにセッション チケットを書き込む必要があります。

以下の主な理由により、SiteMinder セッション ストア（セッション ストア）を展開します。

- SiteMinder のログオフ URI が実装された場合、セッション ストアは、ユーザのログオフ後に SiteMinder セッションが再度使用されることを防ぎます。
- 永続ユーザ セッションを必要とする機能をサポートします。

エージェントはこの情報を使用してユーザを識別し、ポリシー サーバにセッション情報を提供します。

注: セッション ストアの設定の詳細については、ドキュメント ロードマップを参照してください。

SiteMinder 管理 UI

（必須）SiteMinder 管理 UI（管理 UI）は、ポリシー サーバから独立してインストールされる Web ベースの管理コンソールです。 管理 UI は、アクセス制御、レポートおよびポリシー分析に関連するすべてのタスクを管理することを目的としています。

第 2 章: アーキテクチャの考慮事項

このセクションには、以下のトピックが含まれています。

エンタープライズ環境

SiteMinder の実装は、それらを展開する環境に大きく依存します。 実装をエンタープライズにとって意味のある手順に分けるように計画することをお勧めします。 展開を計画する際には、検討すべき多くの質問があります。

これらの質問に対する回答は SiteMinder 実装の計画に不可欠です。

オペレーティング システム

SiteMinder コンポーネントは複数のプラットフォームにわたってサポートされています。詳細については SiteMinder プラットフォーム サポート マトリックスを参照してください。 以下のどのオペレーティング システムによってエンタープライズを展開しますか。

- Microsoft® Windows®
- Oracle® Solaris™
- Red Hat® Enterprise Linux®
- Novell® SUSE® Linux
- Hewlett–Packard Company UNIX （HP-UX）
- IBM® AIX®
- IBM z/OS®

注: サポートされているオペレーティング システムの具体的なバージョンについては、SiteMinder プラットフォーム サポート マトリックスを参照してください。

以下の表を使用して、エンタープライズが展開されたオペレーティング システムが、必要な SiteMinder コンポーネントで現在サポートされているかどうかを判断できます。

コンポーネント	必要ですか。	オペレーティング システム
ポリシー サーバ	はい	
エージェント	はい	
管理 UI	はい	
レポート サーバ	いいえ	

注: さらにプラットフォーム以外の要件もこれらのコンポーネントごとに存在します（たとえば最小メモリ要件）。 ポリシー サーバ、管理 UI およびレポート サーバのプラットフォーム以外の要件の詳細については、「*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。 エージェントのプラットフォーム以外の要件の詳細については、該当する SiteMinder エージェントのドキュメントを参照してください。

Web サーバ ベンダー

SiteMinder エージェントをインストールおよび設定して Web サーバ上のリソースを保護できます。 サポートされている以下のどのサーバ ベンダーによってエンタープライズを展開しますか。

- Apache™ HTTP Server
- Apache Tomcat
- Hewlett–Packard Company (HP) Apache
- IBM HTTP Server
- IBM Lotus® Domino
- Microsoft IIS
- Oracle® HTTP Server
- Red Hat Apache
- Sun Java™ System

注: サポートされている Web サーバの具体的なバージョンについては、SiteMinder プラットフォーム サポート マトリックスを参照してください。

ここで一覧表示されていない他の Web サーバを使用する場合は、これらの Web サーバ上のリソースを保護するために CA SiteMinder for Secure Proxy Server の使用を検討してください。

アプリケーション サーバ ベンダー

SiteMinder エージェントをインストールおよび設定して J2EE アプリケーション サーバ上のリソースを保護できます。 サポートされている以下のどのサーバ ベンダーによってエンタープライズを展開しますか。

- Oracle WebLogic®
- IBM WebSphere®
- RedHat JBoss®

注: サポートされているアプリケーション サーバの具体的なバージョンについては、SiteMinder プラットフォーム サポート マトリックスを参照してください。

Enterprise Resource Planning システム

エージェントをインストールおよび設定して ERP システム上のリソースを保護できます。 サポートされている以下のどの ERP ベンダーによってエンタープライズを展開しますか。

- Oracle PeopleSoft®
- Oracle Siebel®
- SAP®

注: サポートされている ERP システムの具体的なバージョンについては、SiteMinder プラットフォーム サポート マトリックスを参照してください。

ディレクトリ サーバおよびデータベース

SiteMinder データ ストアは複数のディレクトリ サーバおよびデータベースにわたってサポートされています。 サポート対象のベンダー製品がエンタープライズに展開されていることを確認してください。

注: 詳細については、プラットフォーム サポート マトリックスを参照してください。

以下の表を使用して、エンタープライズが展開されたディレクトリ サーバおよびデータベースのタイプが実装に必要なコンポーネントで現在サポートされているかどうかを判断できます。

コンポーネント	必須	LDAP	データベース
ポリシー ストア	はい		
ユーザ ストア接続	はい		
管理ユーザ ストア	いいえ		
監査データベース	いいえ	該当なし	
キーストア	いいえ		
セッション ストア	いいえ	該当なし	

アーキテクチャ ユース ケース

以下のユース ケースの目的は、高可用性およびパフォーマンスの点から SiteMinder アーキテクチャについて考慮していただくことです。 ユース ケースは単純な展開から始まり、より複雑なシナリオに進みます。各ケースは、SiteMinder コンポーネントの論理的な「ブロック」の考えに基づき、環境に複数のブロックを含めて以下のアーキテクチャの考慮事項に対応する方法について説明します。

- 冗長性
- フェールオーバ
- 容量およびスケール
- 複数の Cookie ドメイン

これらのケースから以下のために必要なインフラストラクチャを推定します。

- SiteMinder コンポーネント間の冗長性および高可用性の実装方法を決定する
- 複数のデータ センターの実装方法を決定する
- 容量計画から収集する使用メトリックをサポートする
- 実装時の考慮事項をサポートする
- 環境を調整するパフォーマンスの反復プロセスを開始する

詳細情報:

容量計画が導入されました (P. 107)
導入されたパフォーマンス調整 (P. 157)
冗長性および高可用性 (P. 38)

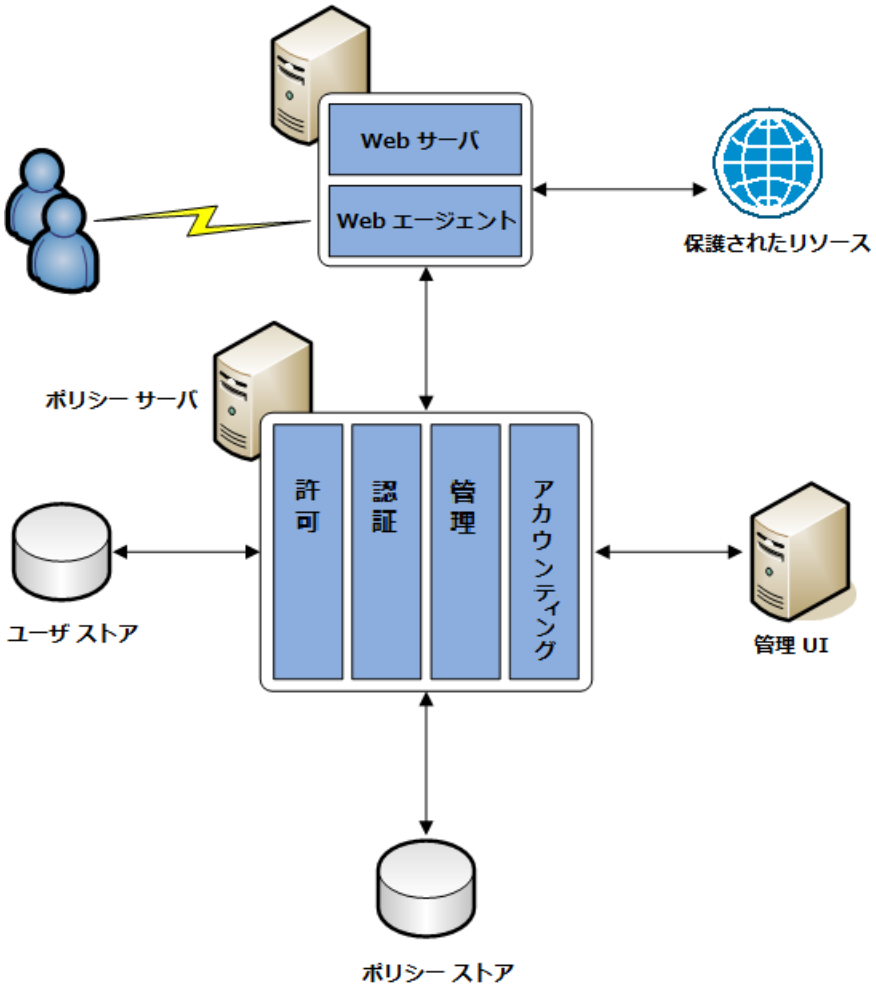
単純な展開

最も単純な SiteMinder 展開には、コンポーネントの 1 つの「ブロック」が必要です。 コンポーネントのブロックは以下を含む依存コンポーネントの論理的組み合わせです。

- Web エージェント
- ポリシー サーバ
- ユーザ ストア
- ポリシー ストア
- 管理 UI

少なくとも 1 つのブロックの展開により Web ベースのリソースを保護します。

以下の図では単純な展開を示します。



各コンポーネントにはリソース保護を含む特定のロールがあります。

注: 各コンポーネントの主な目的の詳細については、「SiteMinder コンポーネント」を参照してください。

オプションのコンポーネントによる単純な展開

オプションの SiteMinder コンポーネントを使用して、単純な展開の機能を拡張できます。 オプション コンポーネントの実装は、企業内で必要とされる SiteMinder 機能によって決定されます。 例：

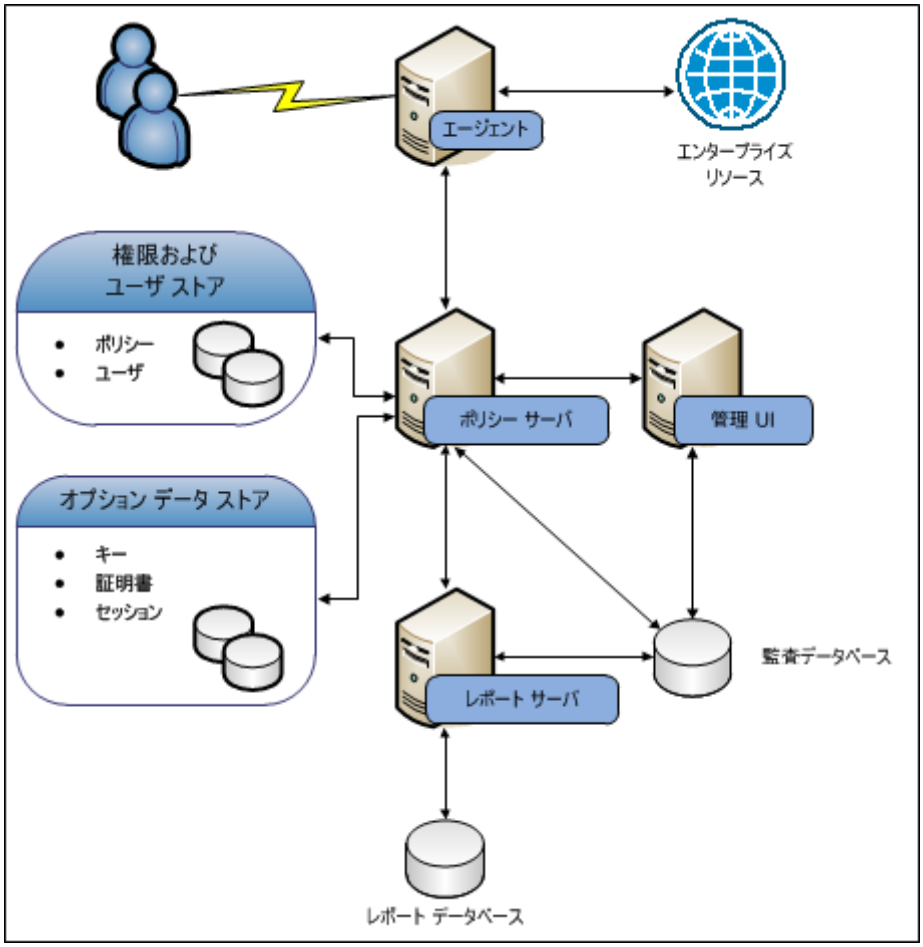
- フェデレーション ベースの機能の実装を計画している場合、その環境は証明書データ ストアおよびセッション ストアを必要とします。
- 監査ベースのレポートの作成を計画している場合、その環境はレポート サーバと監査データベースを必要とします。

以下の図に、オプションのコンポーネントと必要な依存関係を示します。

- レポート サーバ
- レポート データベース
- 監査データベース
- キー ストア

- セッション ストア
- 証明書データ ストア

図 2: オプションのコンポーネントによる単純な展開



各コンポーネントには、リソース保護における特定の役割があります。

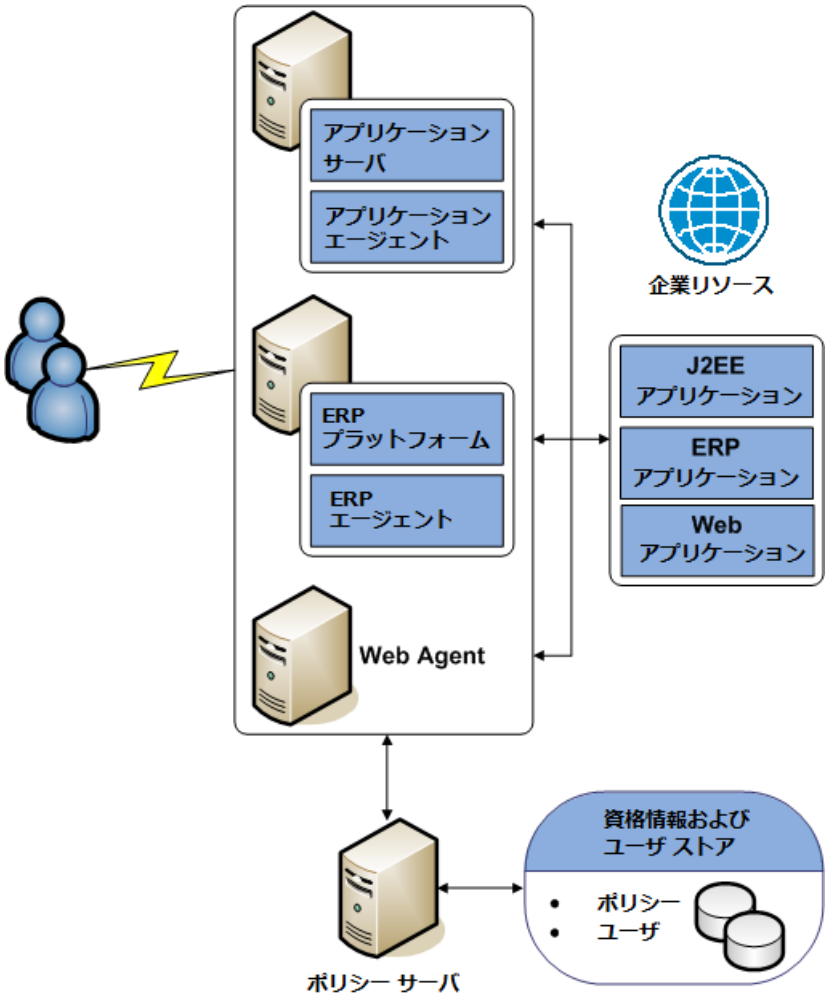
注: 各コンポーネントの主な目的の詳細については、「SiteMinder コンポーネント」を参照してください。

オプションのエージェントを含む単純な展開

環境の単純な展開の機能を拡張して Web サーバ上に存在しないリソースを保護できます。 たとえば、環境の次の場所でリソースがホストされている場合：

- アプリケーション サーバ上のリソースの場合、アプリケーション サーバ エージェントを実装してそれらを保護できます。
- ERP システム上のリソースの場合、ERP エージェントを実装してそれらを保護できます。

以下の図ではオプションのエージェントを示します。



各コンポーネントにはリソース保護を含む特定のロールがあります。

注: 各コンポーネントの主な目的の詳細については、「SiteMinder コンポーネント」を参照してください。

運用継続性管理のための複数コンポーネント

以下のユース ケースでは、以下のメソッドを使用して、環境に冗長性とフェールオーバを組み込むために、どのようにコンポーネントの複数ブロックを実装できるかを示します。

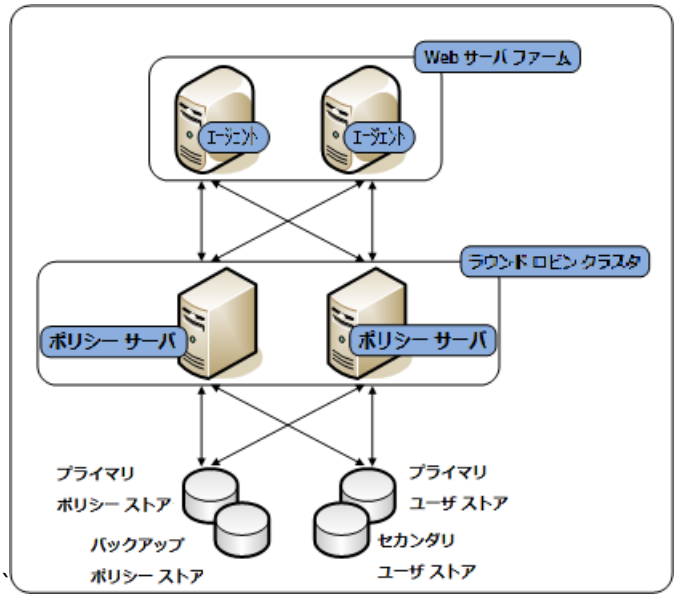
- SiteMinder ラウンド ロビン ロード バランシング
- ハードウェア ロード バランサ

SiteMinder ロード バランシングを使用した運用継続性管理のための複数コンポーネント

SiteMinder ラウンド ロビン ロード バランシングを使用して、環境に冗長性とフェールオーバを組み込むために、コンポーネントの複数ブロックを実装できます。 このユース ケースでは、単純な展開を使用して、運用継続性管理についてどのように考慮していくかを説明します。 以下の図では次のことを示します。

- ユーザ リクエストをインターセプトする複数のエージェント インスタンス。 図に示すように、各エージェントは初期化されて、プライマリ ポリシー サーバと通信し、2 番目のポリシー サーバにフェールオーバされるように設定されます。
- アクセス制御ポリシーを評価して適用するポリシー サーバ クラスタ。 負荷は、クラスタ内の各ポリシー サーバ間で動的に分散されます。
- 複数のユーザ ストア接続。 それぞれのポリシー サーバは、プライマリ ユーザ ストアと通信するように設定されます。 プライマリ ユーザ ストア接続は、セカンダリ ユーザ ストア接続と共に設定されます。ポリシー サーバは、両方の接続にまたがるユーザ情報に対しリクエストを負荷分散させます。 プライマリ接続が利用不能になると、ポリシー サーバはセカンダリ接続にフェールオーバされます。

- 単一のポリシー ストア インスタンス。それぞれのポリシー サーバは、ポリシー情報の共通ビューが得られるように同じポリシー ストアに接続します。 プライマリ ポリシー ストア接続は、ポリシー サーバがフェールオーバできるセカンダリ接続と共に設定されます。



各コンポーネントにはリソース保護を含む特定のロールがあります。

注: 各コンポーネントの主な目的の詳細については、「SiteMinder コンポーネント」を参照してください。 SiteMinder 冗長性および高可用性の詳細については、「冗長性と高可用性」を参照してください。

詳細情報:

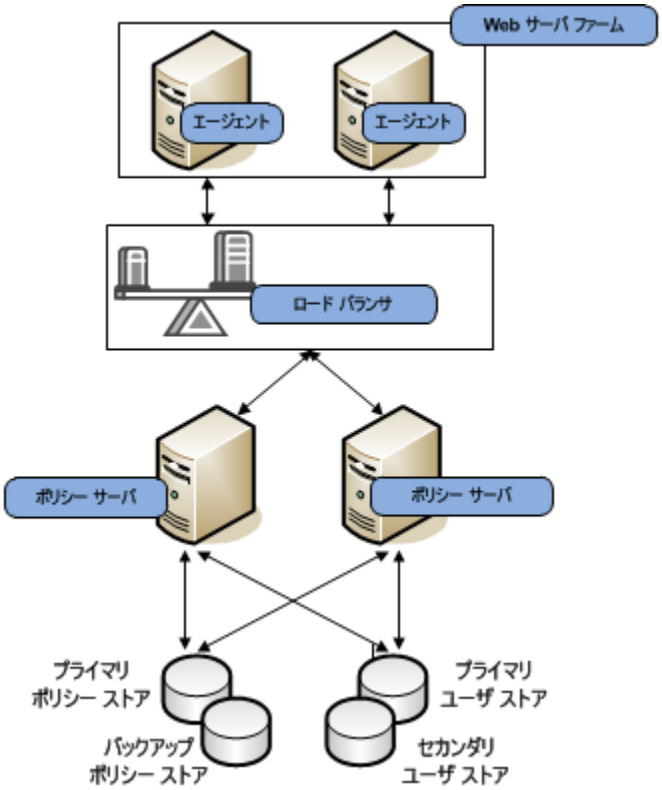
冗長性および高可用性 (P. 38)

ハードウェア ロード バランシングを使用した運用継続性管理のための複数コンポーネント

ハードウェア ロード バランシングを使用して、環境に冗長性とフェールオーバを組み込むために、コンポーネントの複数ブロックを実装できます。このユース ケースでは、単純な展開を使用して、運用継続性管理についてどのように考慮していくかを説明します。 以下の図では次のことを示します。

- ユーザ リクエストをインターセプトする複数のエージェント インスタンス。 図に示すように、各エージェントは初期化されて、プライマリ ポリシー サーバと通信し、2 番目のポリシー サーバにフェールオーバされるように設定されます。
- 仮想 IP アドレス（VIP）によって複数のポリシー サーバを表示するように設定されたハードウェア ロード バランサ。 ハードウェア ロード バランサは、その VIP と関連付けられたすべてのポリシー サーバ間で負荷を動的に分散させます。
- アクセス制御ポリシーを評価して適用する複数のポリシー サーバ。
- 複数のユーザ ストア接続。 それぞれのポリシー サーバは、プライマリ ユーザ ストアと通信するように設定されます。 プライマリ ユーザ ストア接続は、セカンダリ ユーザ ストア接続と共に設定されます。ポリシー サーバは、両方の接続にまたがるユーザ情報に対しリクエストを負荷分散させます。 プライマリ接続が利用不能になると、ポリシー サーバはセカンダリ接続にフェールオーバされます。

- 単一のポリシー ストア インスタンス。それぞれのポリシー サーバは、ポリシー情報の共通ビューが得られるように同じポリシー ストアに接続します。 プライマリ ポリシー ストア接続は、ポリシー サーバがフェールオーバできるセカンダリ接続と共に設定されます。



各コンポーネントにはリソース保護を含む特定のロールがあります。

注: 各コンポーネントの主な目的の詳細については、「SiteMinder コンポーネント」を参照してください。 SiteMinder 冗長性および高可用性の詳細については、「冗長性と高可用性」を参照してください。

詳細情報:

冗長性および高可用性 (P. 38)

スケール用のクラスタ化コンポーネント

スループットを拡張するためにスケールを調整した場合に、高いパフォーマンス レベルを維持しやすいように追加のクラスタを実装できます。 このユース ケースでは、運用継続性管理ユース ケースの複数のコンポーネントを使用して、スケールの面でアーキテクチャについてどのように考慮していくかを説明します。

この図の「初期展開」セクションでは次の内容を説明しています。

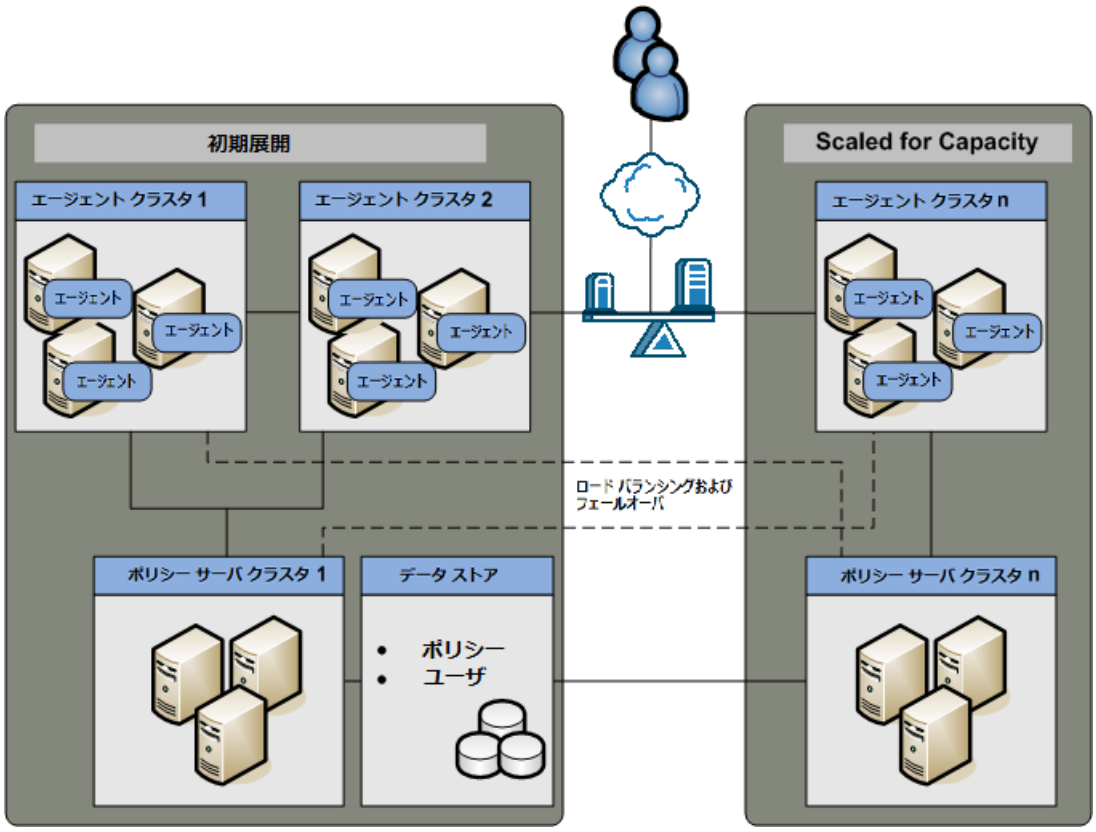
- 複数のエージェント クラスタでのユーザ リクエストを分散させるロード バランサ。
- 特定のアプリケーション用にユーザ リクエストをインターセプトする複数のエージェント インスタンス。各エージェントは初期化されて、クラスタ内のプライマリ ポリシー サーバと通信するように設定されます。 クラスタ内で十分なポリシー サーバを利用できない場合は、エージェントが別のポリシー サーバ クラスタにフェールオーバします。

  注: エージェントとポリシー サーバの冗長性および高可用性の詳細については、「冗長性と高可用性」を参照してください。
- アクセス制御ポリシーを評価して適用するポリシー サーバ クラスタ。負荷は、クラスタ内の各ポリシー サーバ間で動的に分散されます。
- 複数のユーザ ストア接続。 それぞれのポリシー サーバは、プライマリ ユーザ ストアに接続するように設定されます。 プライマリ ユーザ ストア接続は、セカンダリ ユーザ ストア接続と共に設定されます。ポリシー サーバは、両方の接続にまたがるユーザ情報に対しリクエストを負荷分散させます。 プライマリ接続が利用不能になると、ポリシー サーバはセカンダリ接続にフェールオーバされます。

  注: ポリシー サーバとユーザ ストアの冗長性および高可用性の詳細については、「冗長性と高可用性」を参照してください。

- 単一のポリシー ストア インスタンス。 クラスタ内のそれぞれのポリシー サーバは、ポリシー情報の共通ビューが得られるように同じポリシー ストアに接続します。 プライマリ ポリシー ストア接続は、ポリシー サーバがフェールオーバできるセカンダリ接続と共に設定されます。

  注: ポリシー サーバとポリシー ストアの冗長性の詳細については、「冗長性と高可用性」を参照してください。



各コンポーネントにはリソース保護を含む特定のロールがあります。

注: 各コンポーネントの主な目的の詳細については、「SiteMinder コンポーネント」を参照してください。

図の「キャパシティに合わせたスケール設定」セクションでは、別のコンポーネント ブロックを詳述し、次の内容について説明しています。

- 新しいエージェント クラスタにリクエストを分散させるロード バランサ。
- ユーザ リクエストをインターセプトする複数のエージェント インスタンス。 クラスタ 内のポリシー サーバへの各接続に加えて、環境内の任意のポリシー サーバにフェールオーバするようにそれぞれのエージェントを設定することもできます。 点線で示すように、エージェント クラスタ 内のエージェントは、ポリシー サーバ クラスタ 1 内のポリシー サーバにフェールオーバするように設定されます。
- アクセス制御ポリシーを評価して適用するポリシー サーバ クラスタ。 点線に示すように、それぞれのポリシー サーバ クラスタは、フェールオーバしきい値で設定されます。利用可能なポリシー サーバの数が指定されたしきい値よりも少なくなると、失敗したポリシー サーバで処理されることになっていたすべてのリクエストが別のクラスタに転送されます。

  注: ポリシー サーバ クラスタのフェールオーバしきい値の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

詳細情報:

冗長性および高可用性 (P. 38)
SiteMinder ロード バランシングを使用した運用継続性管理のための複数コンポーネント (P. 32)
ハードウェア ロード バランシングを使用した運用継続性管理のための複数コンポーネント (P. 34)

冗長性および高可用性

SiteMinder コンポーネントの論理ブロック間の冗長性と高可用性を設定し、システムの可用性とパフォーマンスを維持します。

エージェントとポリシー サーバ間の通信

SiteMinder エージェントを設定すると、ホスト設定ファイル（デフォルトでは SmHost.conf という名前）はホスト サーバ上で作成されます。 エージェントは、このホスト設定ファイル内の接続情報を使用して、ポリシー サーバとの初期接続を作成します。

初期接続が確立された後、エージェントはポリシー サーバ上のホスト設定オブジェクト (HCO) から以後のポリシー サーバ接続情報を取得します。

複数のポリシー サーバを含めるように HCO を設定し、複数のポリシー サーバ間でリクエストを分散させるのにエージェントが使用するメソッドを指定できます。

SiteMinder エージェントは以下の方法を使用して、複数のポリシー サーバ間でリクエストを分散させることができます。

- フェールオーバ
- ラウンド ロビン ロード バランシング
- ポリシー サーバの 1 つ以上のクラスタ上で行われるラウンド ロビン ロード バランシング

または、複数のポリシー サーバを表示するためにハードウェア ロード バランサ上で設定された単一の仮想 IP アドレスを含めるように HCO を設定できます。 この場合は、エージェント ソフトウェアではなくロード バランサがフェールオーバとロード バランシングに対応します。

詳細情報:

SiteMinder エージェント (P. 13)

フェールオーバ

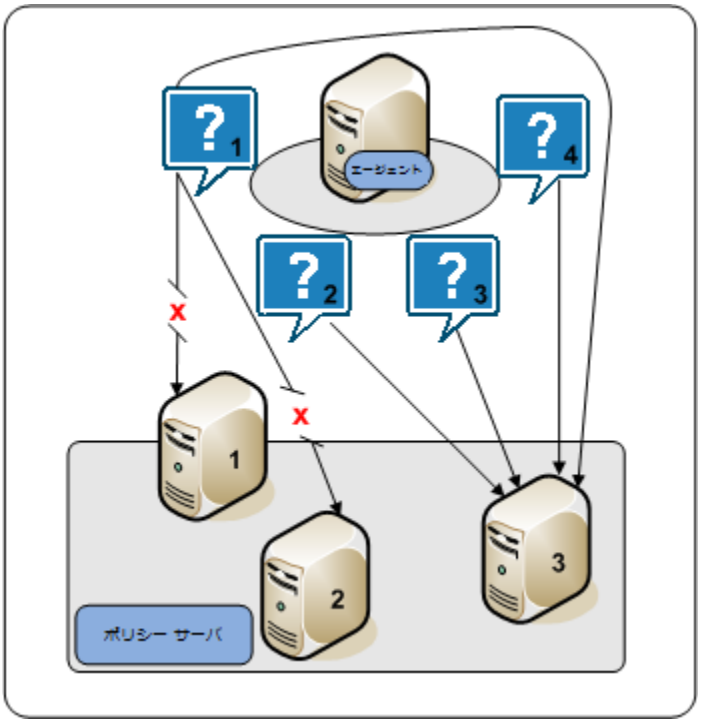
フェールオーバはデフォルトの HCO 設定です。 フェールオーバ モードの場合、SiteMinder エージェントは HCO が一覧表示する最初のポリシー サーバにすべてのリクエストを送り、以下を続行します。

1. 最初のポリシー サーバが応答しない場合、エージェントはそれを使用不可能であるとみなして、そのリクエストおよびすべての後続リクエストを HCO が一覧表示する次のポリシー サーバにリダイレクトします。
2. 最初の 2 つのポリシー サーバが応答しない場合、エージェントはそれら両方を使用不可能であるとみなして、そのリクエストおよびすべての後続リクエストを HCO が一覧表示する次のポリシー サーバにリダイレクトします。

注: 複数のポリシー サーバを含む HCO 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。

定期的なポーリングによって、無応答のポリシー サーバが回復したとエージェントが判断した場合、ポリシー サーバは自動的に HCO リスト内の元の場所に返され、すべてのエージェント リクエストの受信を開始します。

以下の図ではエージェント フェールオーバ プロセスを示します。



ラウンド ロビン ロード バランシング

ラウンド ロビン ロード バランシングはオプションの HCO 設定です。ラウンド ロビン ロード バランシングでは、リクエストが一連のポリシー サーバに均等に分散されて、以下が発生します。

- ユーザの認証および許可がより効率的になる
- 1 つのポリシー サーバにエージェント リクエストが集中するのを防ぐ

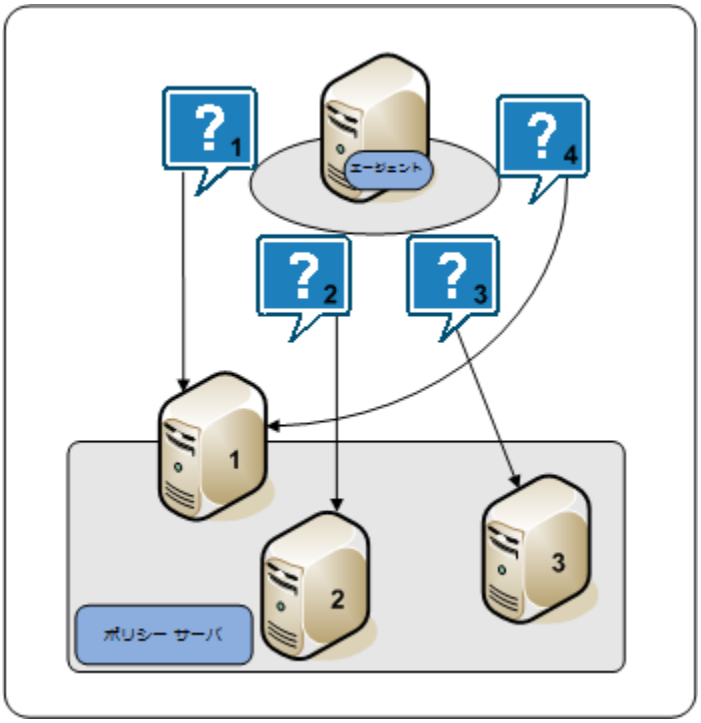
注: ラウンド ロビン ロード バランシング用に HCO を設定する詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

ラウンド ロビン モードでは、エージェントは HCO が一覧表示するすべてのポリシー サーバにリクエストを分散します。 エージェントによって以下が実行されます。

1. HCO が一覧表示する最初のポリシー サーバにリクエストを送信します。
2. HCO が一覧表示する 2 番目のポリシー サーバにリクエストを送信します。
3. HCO が一覧表示する 3 番目のポリシー サーバにリクエストを送信します。
4. このように、エージェントがすべての使用可能なポリシー サーバにリクエストを送信するまで、リクエストの送信を続けます。 すべての使用可能なポリシー サーバにリクエストを送信したら、エージェントは最初のポリシー サーバに戻って、再度このサイクルを開始します。

ポリシー サーバが応答しない場合、エージェントは HCO が一覧表示する次のポリシー サーバにリクエストをリダイレクトします。 定期的なポーリングによって、無応答のポリシー サーバが回復したとエージェントが判断した場合、ポリシー サーバは自動的に HCO リスト内の元の場所に復元されます。

以下の図ではラウンド ロビン プロセスを示します。



ポリシー サーバ クラスタ

ラウンド ロビン ロード バランシングでは、HCO が一覧表示するすべてのポリシー サーバに SiteMinder エージェント リクエストを均等に分散します。 システム可用性および応答時間を改善する効率的な方法ですが、以下の点を考慮してください。

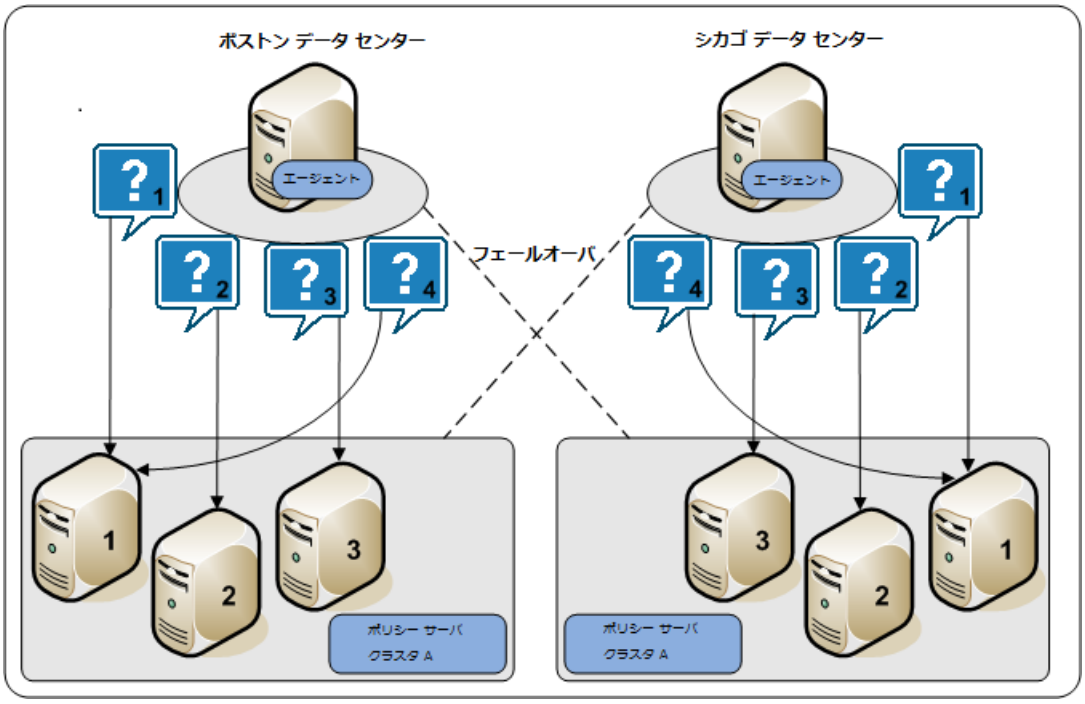
- ラウンド ロビン ロード バランシングは、計算容量が異なる可能性がある異機種環境では最も効率的な分散方法ではありません。 各ポリシー サーバは、容量にかかわらず、同数のリクエストを受信します。
- 異なる地理的位置にあるポリシー サーバへのラウンド ロビン ロード バランシングによって、パフォーマンスが低下する場合があります。 エージェント リクエストを一定の地域外のポリシー サーバに送信すると、ネットワーク通信のオーバーヘッドおよびネットワークの輻輳を増加させる場合があります。

ポリシー サーバ クラスタとは、エージェントがリクエストを分散できるポリシー サーバのグループです。 ポリシー サーバ クラスタには、ラウンドロビン ロードバランシングにはない次のような利点があります。

- 特定のデータ センターにのみポリシー サーバを含めるようにクラスタを設定できます。 個別のポリシー サーバ クラスタでエージェントをグループ化することにより、離れた地域間のロード バランシングに関連するネットワーク オーバーヘッドを回避します。 ネットワーク オーバーヘッドは、エージェントが別のポリシー サーバ クラスタにフェールオーバする場合にのみ発生します。
- クラスタは、ポリシー サーバ のフェールオーバのしきい値に基づいて別のクラスタにフェールオーバできます。
- エージェントは、リクエストを均等に配分するのではなく、レスポンス時間に基づいてすべてのポリシー サーバに動的にリクエストを配分します。

注: ポリシー サーバ クラスタ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。

以下の図では 2 つのポリシー サーバ クラスタを示します。各クラスタは、ラウンド ロビン ロード バランシングに関連する場合があるネットワーク オーバーヘッドを回避するために、地理的に離れています。

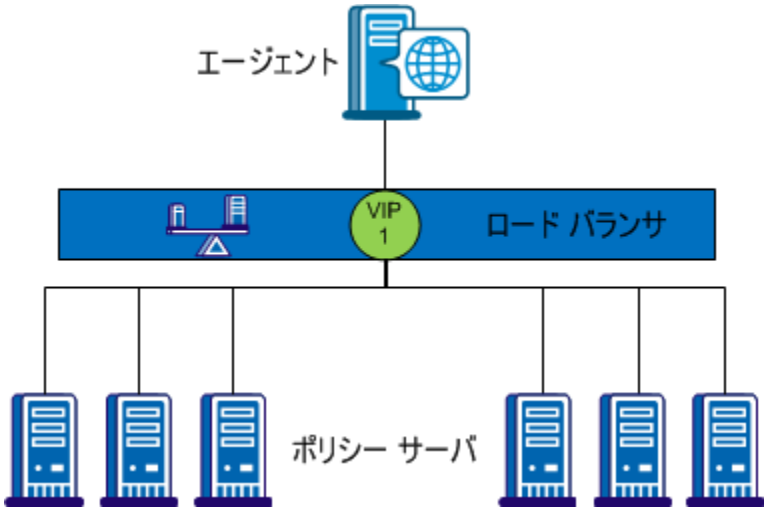


ハードウェア ロード バランシング

SiteMinder では、1 つ以上の仮想 IP アドレス（VIPs）によって複数のポリシー サーバを表示するように設定されたハードウェア ロード バランサを使用できます。 ハードウェア ロード バランサは、その VIP と関連付けられたすべてのポリシー サーバ間でリクエストの負荷を動的に分散させます。 以下のハードウェア ロード バランシング設定がサポートされています。

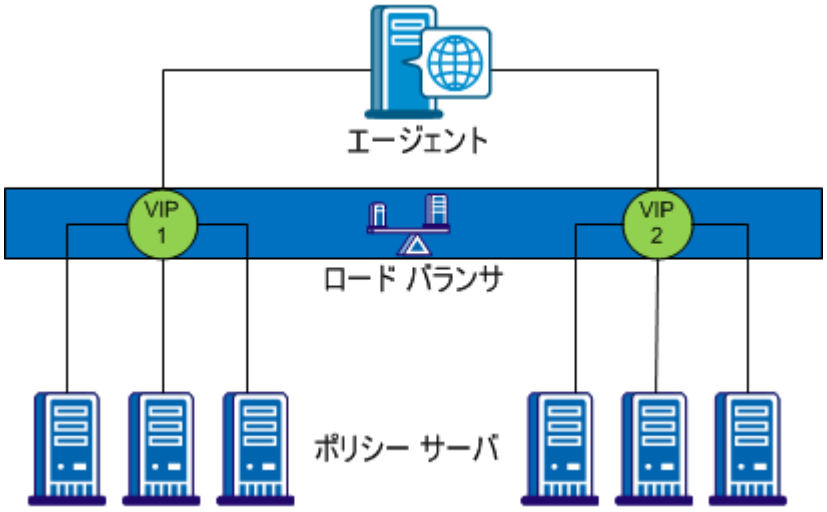
- 単一の VIP と各 VIP によって表示される複数のポリシー サーバ
- 複数の VIP と各 VIP によって表示される複数のポリシー サーバ

単一の VIP と VIP ごとの複数のポリシー サーバ



前の図に示した設定で、ロード バランサは単一の VIP を使用して、複数のポリシー サーバを表示します。このシナリオは、VIP を処理するロード バランサが失敗した場合の単一障害点を示しています。

複数の VIP と VIP ごとの複数のポリシー サーバ



前の図に示した設定で、ポリシー サーバのグループは 1 つ以上のロード バランサによって個別の VIP として表示されます。 複数のロード バランサが使用される場合は、ロード バランサ間のフェールオーバになるため、単一障害点は除去されます。 ただし、主要なすべてのハードウェア ロード バランサ ベンダーは、単一の VIP のみが必要となるように、複数の同様なロード バランサ間のフェールオーバを内部的に処理しています。 したがって、同じベンダーからの冗長なロード バランサを使用している場合は、単一の VIP でエージェントとポリシー サーバ間の通信を設定して、堅牢なロード バランシングとフェールオーバを維持できます。

注: ハードウェア ロード バランサを使用して複数の仮想 IP アドレス（VIP）としてポリシー サーバを公開している場合は、それらの VIP をフェールオーバ設定に設定することを推奨します。 ハードウェア ロード バランサが同じ機能をより効率よく実行するため、ラウンド ロビン負荷分散は不必要です。

ポリシー サーバからユーザ ストアへの通信

ポリシー サーバは複数の LDAP または ODBC ユーザ ストアにクエリを分散して、以下を有効にすることができます。

- フェールオーバ
- ラウンド ロビン ロード バランシング

注: ユーザ ストア接続の設定の詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

詳細情報:

ユーザ ストア (P. 17)

フェールオーバ

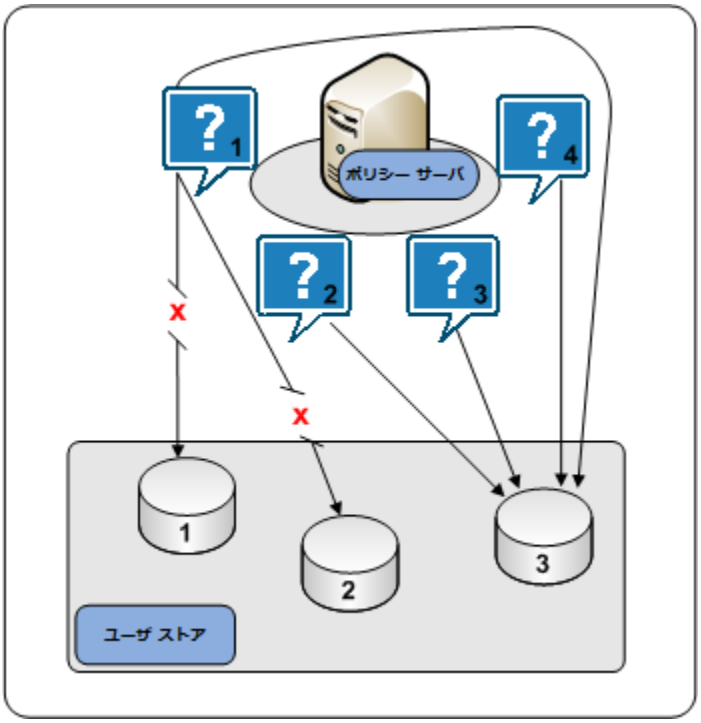
フェールオーバは SiteMinder ユーザ ストア オブジェクトのオプション設定です。 フェールオーバ モードでは、ポリシー サーバはすべてのリクエストをプライマリ ユーザ ストアに分散して、以下を続行します。

1. プライマリ ユーザ ストアが応答しない場合、ポリシー サーバはそれら両方を使用不可能であるとみなして、SiteMinder ユーザ ストア オブジェクトが一覧表示する次のユーザ ストアに、そのリクエストおよびすべての後続リクエストをリダイレクトします。
2. 1 番目と 2 番目のユーザ ストアが応答しない場合、ポリシー サーバはそれら両方を使用不可能であるとみなして、SiteMinder ユーザ ストア オブジェクトが一覧表示する次のユーザ ストアに、そのリクエストおよびすべての後続リクエストをリダイレクトします。

注: ユーザ ストア フェールオーバ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。

無応答のユーザ ストアが回復した場合、ユーザ ストアは自動的にフェールオーバ リスト内の元の場所に返され、すべてのポリシー サーバ リクエストの受信を開始します。

以下の図ではユーザ ストア フェールオーバ プロセスを示します。



ラウンド ロビン ロード バランシング

ラウンド ロビン ロード バランシングはオプションの SiteMinder ユーザ ストア オブジェクト設定です。ラウンド ロビン ロード バランシングでは、リクエストが一連のユーザ ストアに均等に分散されて、以下が発生します。

- ユーザ ストア クエリがより効率的になる
- 1 つのユーザ ストアにポリシー サーバ リクエストが集中しなくなる

注: 以下の点について考慮してください。

- LDAP ユーザ ストア間のロード バランシング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。
- 管理 UI には、ODBC ユーザ ストア間のラウンド ロビン ロード バランシングを設定するための設定は含まれていません。 ただし、ポリシー サーバ インストールには以下が含まれます。
  - SiteMinder Oracle ワイヤ プロトコル。 このプロトコルは、複数の Oracle ストアにわたるロード バランシングをサポートします。 データ ソース レベルで Oracle ユーザ ストアのロード バランシングを設定できます。
  - SQL Server または SQL Server Cluster Enterprise の設定に使用できる SiteMinder SQL Server ワイヤ プロトコル。 データベース レベルで SQL Server ユーザ ストアのロード バランシングを設定できます。

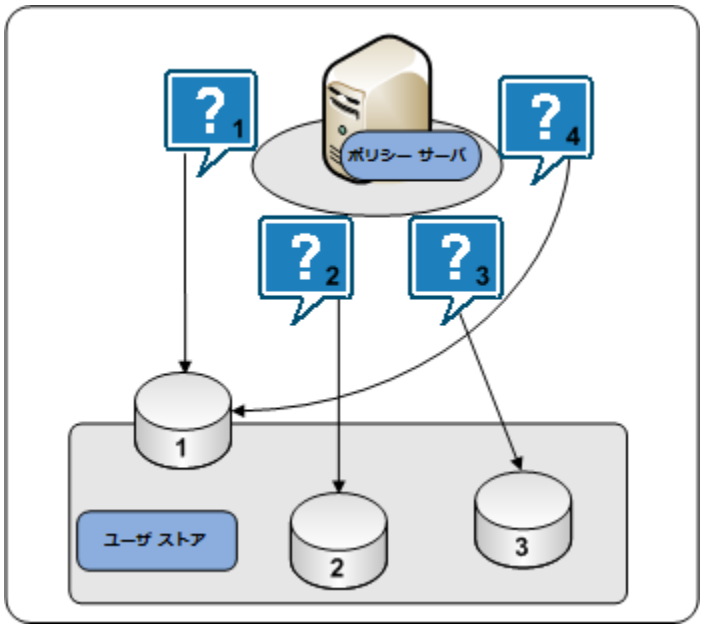
ラウンド ロビン モードでは、ポリシー サーバは SiteMinder ユーザ ストア オブジェクトが一覧表示するすべてのユーザ ストアにリクエストを分散します。 ポリシー サーバによって以下が実行されます。

1. ユーザ ストア オブジェクトが一覧表示する最初のユーザ ストアにリクエストを送信します。
2. ユーザ ストア オブジェクトが一覧表示する 2 番目のユーザ ストアにリクエストを送信します。
3. ユーザ ストア オブジェクトが一覧表示する 3 番目のユーザ ストアにリクエストを送信します。

4. このように、ポリシー サーバがすべての使用可能なユーザ ストアにリクエストを送信するまで、リクエストの送信を続けます。 すべての使用可能なユーザ ストアにリクエストを送信したら、ポリシー サーバは最初のユーザ ストアに戻って、再度このサイクルを開始します。

注: ユーザ ストア障害発生時には、フェールオーバと共にロード バランシングを設定して冗長性を追加します。 ロード バランシングとフェールオーバ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。

以下の図ではユーザ ストア ラウンド ロビン プロセスを示します。



ポリシー サーバからポリシー ストアへの通信

すべてのポリシー サーバは、ポリシー情報の共通のビューのために同じポリシー ストアに接続する必要があります。 ただし、ポリシー サーバがフェールオーバできる複数の「ホット」ポリシー ストアを展開に含めることをお勧めします。

ポリシー ストアのフェールオーバ シナリオを以下に示します。

- レプリケーション バージョンで設定されたマスタ ポリシー ストア
- マルチマスタ ポリシー ストア

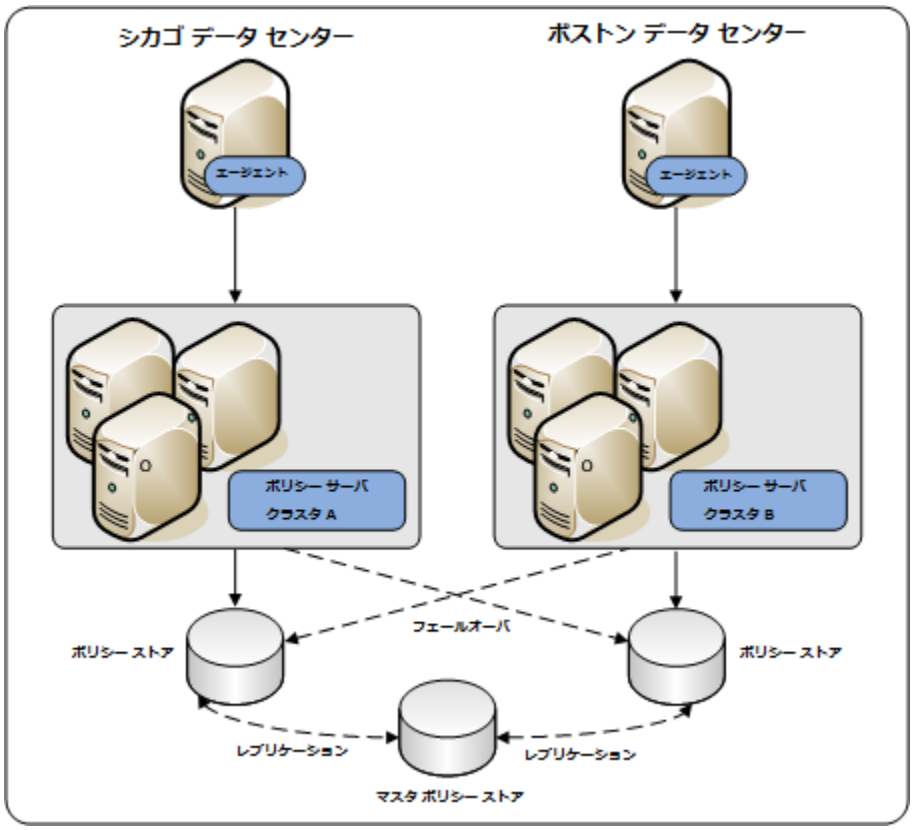
マスタ ポリシー ストア

レプリケーション バージョンによるマスタ ポリシー ストアの展開は、ポリシー ストアの冗長性を実現します。 1 つのマスタ ポリシー ストアによって各ポリシー サーバは最も近いレプリケーション バージョンと通信できます。 この通信方法については以下のとおりです。

- 地理的に離れたポリシー サーバのパフォーマンスを向上させます。ポリシー サーバ リクエストを一定の地域外のポリシー ストアに送信すると、ネットワーク通信のオーバーヘッドおよびネットワークの輻輳を増加させる場合があります。
- フェールオーバを可能にします。 プライマリ ポリシー ストアが失敗すると、ポリシー サーバはセカンダリ ストアにフェールオーバします。

注: レプリケーションの設定の詳細については、ベンダー固有のマニュアルを参照してください。 ポリシー ストア フェールオーバ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。

以下の図では単一のマスタ ポリシー ストアの環境を示します。



マルチマスタ ポリシー ストア

マルチマスタ技術の使用による LDAP ディレクトリの展開は、ポリシー ストアの冗長性を実現します。 マルチマスタ ポリシー ストアによって各ポリシー サーバは最も近いレプリケーション バージョンと通信できます。この通信方法については以下のとおりです。

- 地理的に離れたポリシー サーバのパフォーマンスを向上させます。ポリシー サーバ リクエストを一定の地域外のポリシー ストアに送信すると、ネットワーク通信のオーバーヘッドおよびネットワークの輻輳を増加させる場合があります。
- フェールオーバを可能にします。 プライマリ ポリシー ストアが失敗すると、ポリシー サーバはセカンダリ ストアにフェールオーバします。

マルチマスタ モードで LDAP ポリシー ストアを設定する場合は、以下の設定が推奨されます。

- 1 つのマスタをすべての管理に使用します。
- 1 つのマスタをキーのストレージに使用します。

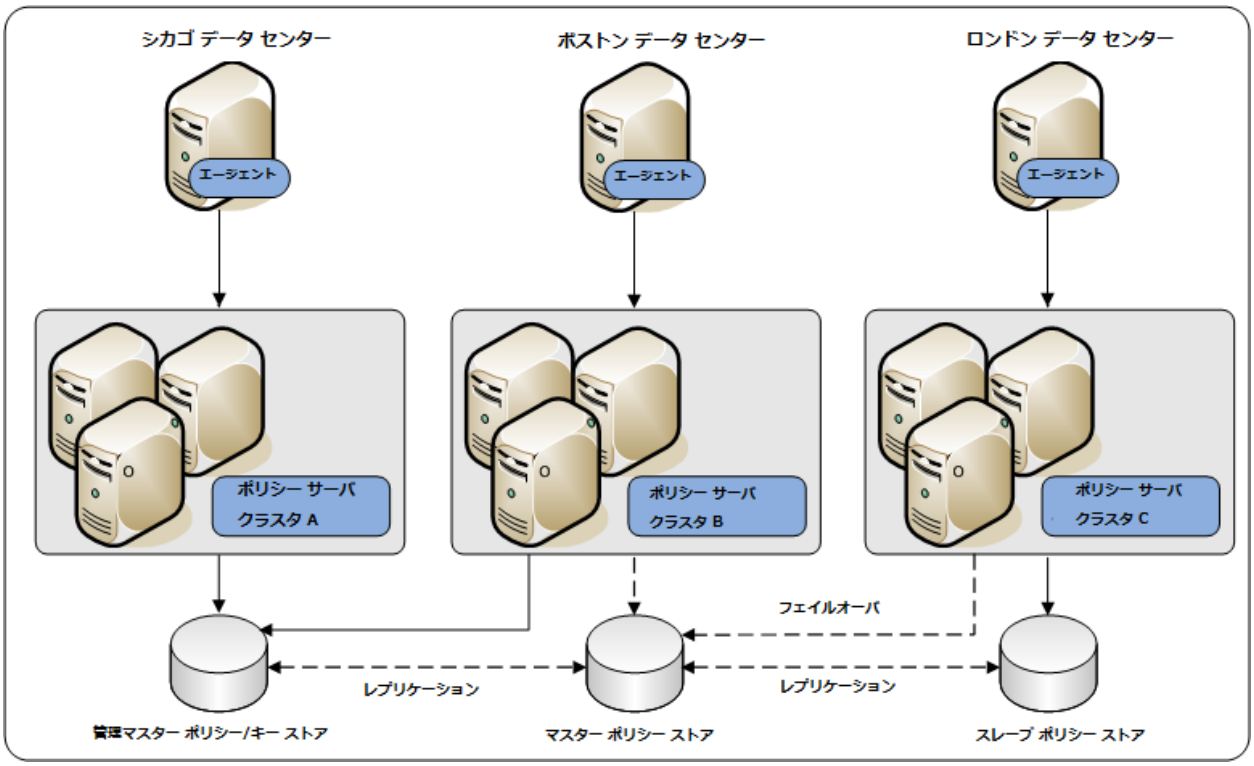
  このマスタは、管理に使用されるマスタと同じである必要はありません。ただし、キーと管理の両方に同じマスタ ストアを使用することをお勧めします。 この設定では、すべてのキー ストア ノードがレプリカではなくマスタを参照している必要があります。

  注: キー ストレージに管理用マスタ以外のマスタを使用する場合、すべてのキー ストアで同じキー ストア値を使用する必要があります。キー ストアは、ポリシー ストアおよびキー ストアの両方として機能するよう設定することはできません。
- ほかのすべてのポリシー ストア マスタは、フェールオーバ モードに設定する必要があります。

同期の問題が発生する可能性があるため、これ以外の設定では、ポリシー ストアが破損したりエージェント キーが同期されなくなったりと、不整合な結果が生じる場合があります。

他の設定については、SiteMinder サポートまでお問い合わせください。

以下の図ではマルチマスタ ポリシー ストアの環境を示します。



ポリシー サーバから監査ストアへの通信

デフォルトでは、各ポリシー サーバはそれぞれの監査情報をテキスト ファイルに格納します。 このテキスト ファイルは、ポリシー サーバ ログと呼ばれます。 監査データをデータベースに直接記録するようにポリシー サーバを設定できます。

通常 SiteMinder 監査ログは、監査およびコンプライアンスに使用されます。以下の点について考慮してください。

- すべてのポリシー サーバに、全データを一度に問い合わせることができる一元化された監査ストアへの書き込みを実行させることをお勧めします。 一元化された監査ストアを展開する場合は、高可用性展開をお勧めします。

  注: 監査ストアの設定の詳細については、「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。フェールオーバ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。

  重要: 同期監査を有効にする場合は、監査ストアの停止によってすべてのポリシー サーバ認証および許可が停止することを防ぐように、フェールオーバを設定することをお勧めします。 ポリシー サーバは、レコードが監査データベースに保存されるまで、エージェントの認証リクエストおよび許可リクエストの結果を返しません。 レコードが保存されるまで、ユーザは認証または許可されません。 フェールオーバ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。

- 展開でポリシー サーバが一元化された監査ストアに書き込めない場合、smauditimport ユーティリティを使用して個別のポリシー サーバ ログを一元化された監査ストアにインポートできます。

  注: ポリシー サーバ ログ記録および smauditimport ツールの詳細については、「*ポリシー サーバ管理ガイド*」を参照してください。

詳細情報:

SiteMinder 監査データベース (P. 19)

ポリシー サーバからセッション ストアへの通信

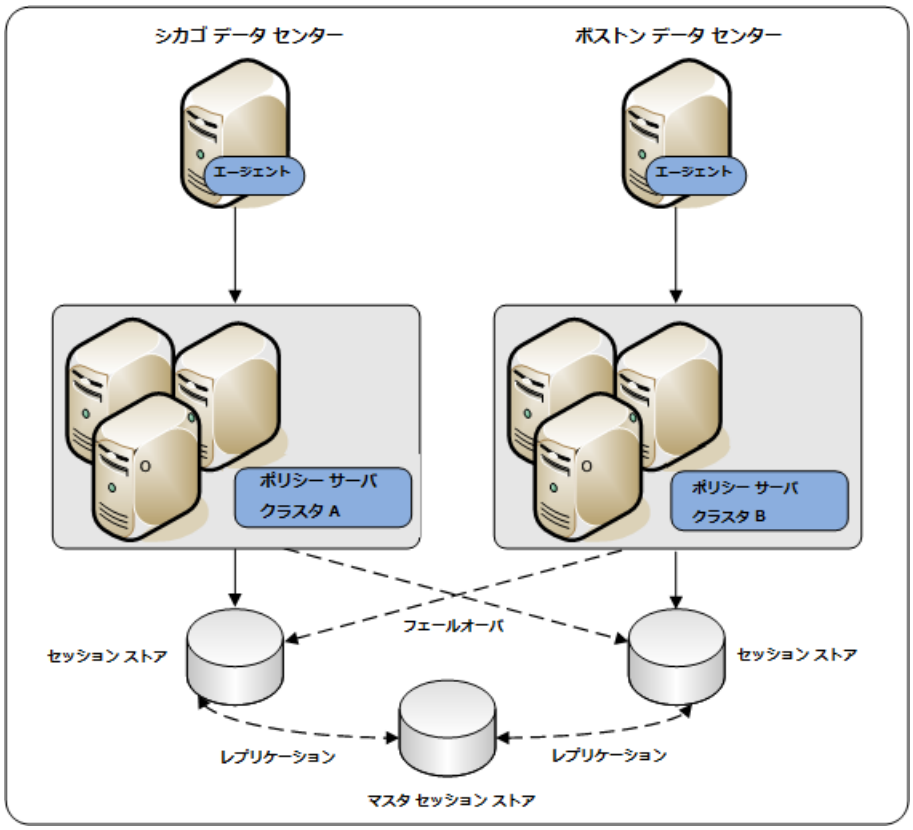
セッション ストアを展開する場合、環境内のすべてのポリシー サーバは同じセッション ストア データベースを使用する必要があります。

マスタ セッション ストアの展開は、セッション ストアの冗長性を実現します。マスタ セッション ストアによって各ポリシー サーバは最も近いレプリケーション バージョンと通信できます。 この通信方法については以下のとおりです。

- 地理的に離れたポリシー サーバのパフォーマンスを向上させます。ポリシー サーバ リクエストを一定の地域外の一元化されたセッション ストアに送信すると、ネットワーク通信のオーバーヘッドおよびネットワークの輻輳を増加させる場合があります。
- フェールオーバを可能にします。 プライマリ セッション ストアが失敗すると、ポリシー サーバはセカンダリ セッション ストアにフェールオーバします。

注: レプリケーションの設定の詳細については、ベンダー固有のマニュアルを参照してください。 セッション ストア フェールオーバ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。

以下の図では、セッション ストアへの共通のビューを共有するすべてのポリシー サーバを示します。



詳細情報:

セッション ストア (P. 21)

拡張されたセッション保証アーキテクチャおよびパフォーマンスの考慮事項

拡張されたセッション保証機能によって、セッションのハイジャックおよび再生を防ぎます。 ユーザがログインすると、DeviceDNA™チェックが実行され、エンドユーザ デバイスのフィンガープリントが取得されます。デバイスはデフォルトでは 5 分間隔でフィンガープリントによる検証が行われ、新規フィンガープリントがログイン時に取得された元のフィンガープリントと比較されます。

最初のフィンガープリント取得とそれ以降の再チェックによって、SiteMinder アーキテクチャへの要求が増大します。 特に、SiteMinder ポリシー サーバ、および拡張されたセッション保証フロー アプリケーションを実行する CA SiteMinder for Secure Proxy Server のインスタンスは影響を受けます。 フィンガープリントの再検証が必要な場合、ユーザの認証時間が増加すると、リソースへのアクセス許可に要する時間も増加します。認証時にどの程度の遅延が発生するかは、ネットワーク接続速度、サーバの性能、およびエンドユーザのデバイスなど、多数のパラメータに応じて異なります。 内部テストは、拡張されたセッション保証で設定されたアプリケーションの認証時の遅延が 60% 増加する可能性があることが示されました。 これは、DeviceDNA™ のコレクションおよび計算用の追加のリダイレクトおよび処理時間によるものです。 各環境での実際の増加の割合は、現在の認証遅延、ネットワーク、およびリソースにアクセスしているコンピュータの速度に応じて変わります。 さらに、トランザクションが拡張されたセッション保証を使用しなかった場合、拡張されたセッション保証トランザクションに参加する SiteMinder ファミリ コンポーネントをホストするシステムのリソース（たとえば CPU 使用率）はより高くなります。

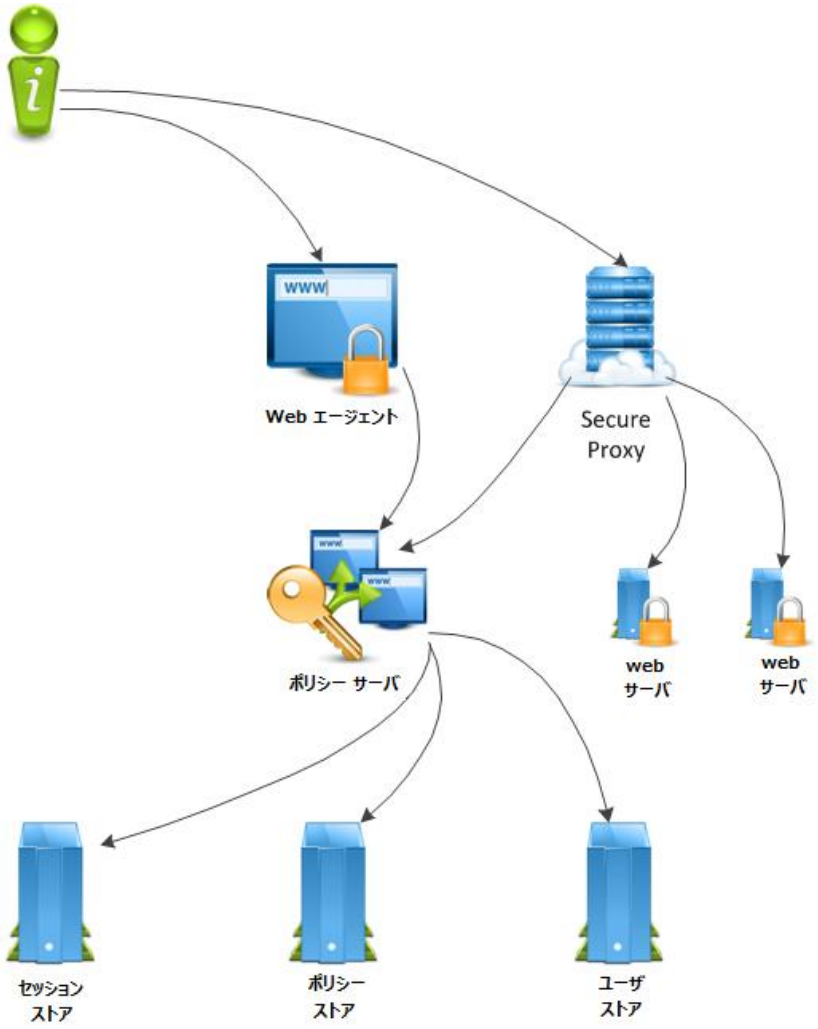
DeviceDNA チェックを実行するアプリケーションは CA SiteMinder for Secure Proxy Server インスタンスでホストされます。インスタンスは、Web プロキシまたは SAML フェデレーション機能などの標準 CA SiteMinder for Secure Proxy Server 機能を実行する CA SiteMinder for Secure Proxy Server インスタンス、または、拡張されたセッション保証トランザクション処理専用の別のスタンドアロン CA SiteMinder for Secure Proxy Server インスタンスである場合があります。 また、CA SiteMinder for Secure Proxy Server プラットフォームのパフォーマンスは、1 秒あたりの認証および許可トランザクション数、環境内の認証と許可の割合、ユーザ セッション長、および再検証の頻度など、多くのパラメータに依存します。

このセクションでは、SiteMinder の拡張されたセッション保証の展開に使用されるさまざまなアーキテクチャについて説明し、ユーザの環境でこの機能を使用しない既存の SiteMinder アプリケーションに対するパフォーマンスの影響を最小化するための選択肢の概要を説明します。

展開するアーキテクチャにかかわらず、拡張されたセッション保証を段階的に導入することは非常に重要です。 ベスト プラクティスは、拡張されたセッション保証を開発環境にインストールし、パフォーマンスに対する影響を測定する一方で、異なるアプリケーションやレルムに対してこの機能を段階的に有効にして、環境に対する影響をテストすることです。

基本的なアーキテクチャ

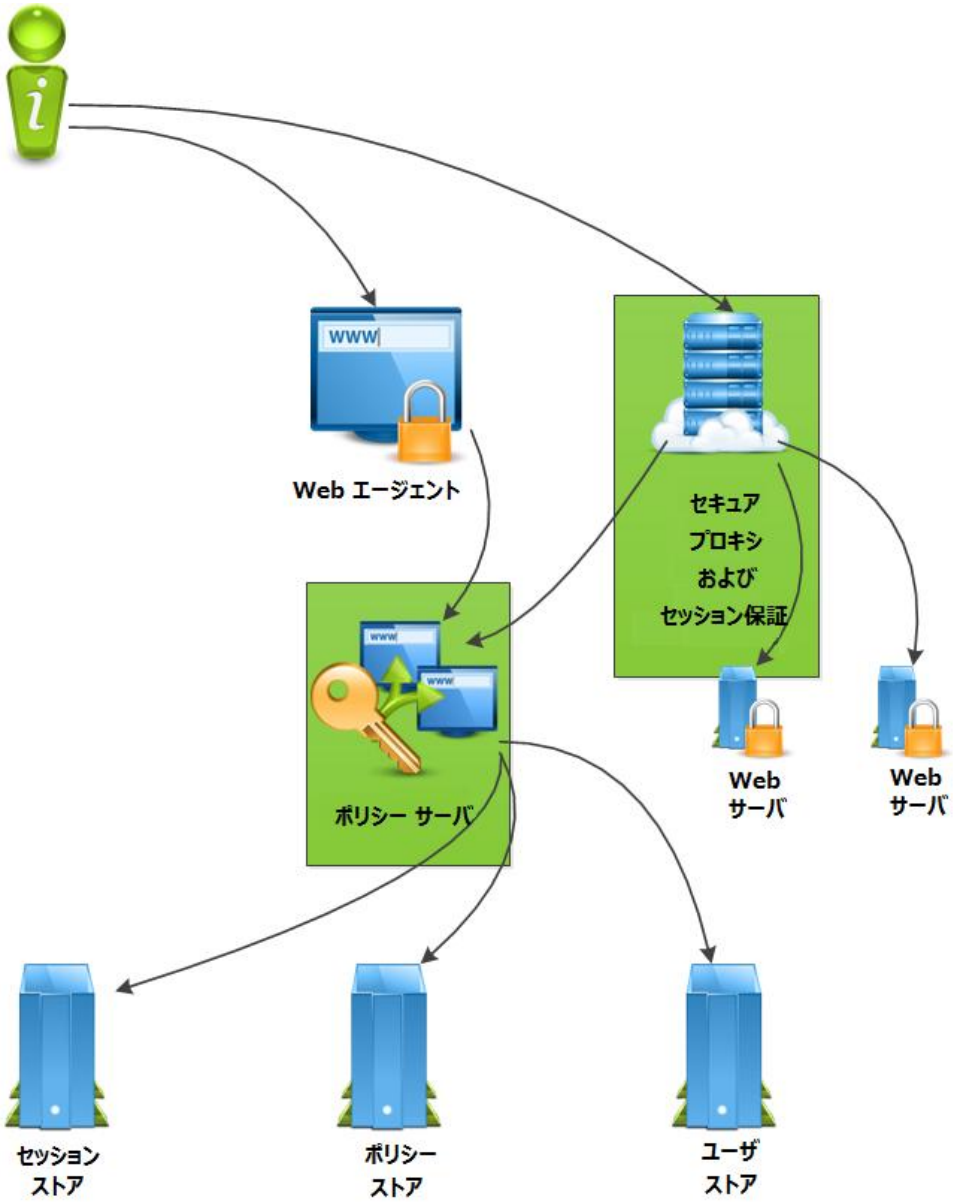
以下の図は、拡張されたセッション保証を使用しない、基本的な SiteMinder のアーキテクチャの簡略図です。



このアーキテクチャでは、他の Web アプリケーションへのプロキシに Web エージェントと CA SiteMinder for Secure Proxy Server の両方を使用しています。

可能なアーキテクチャ 1 - 既存コンポーネントの使用

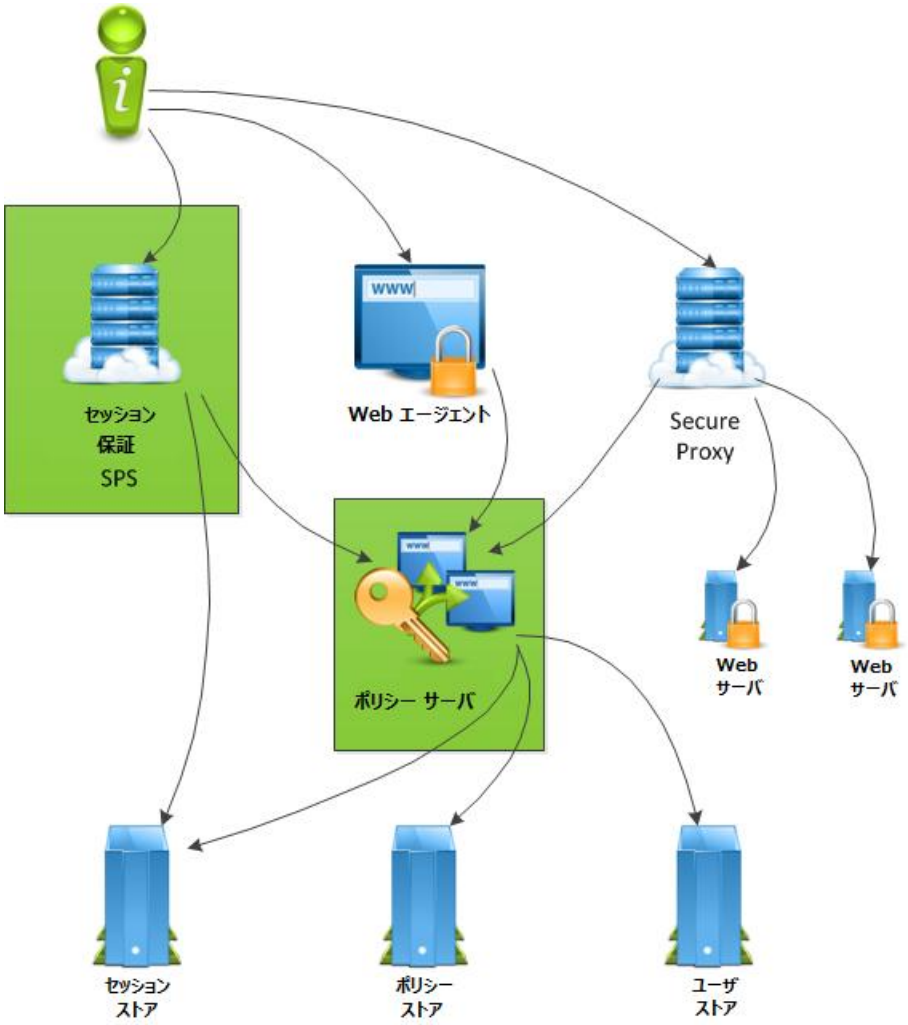
以下の図は、拡張されたセッション保証の展開に既存のコンポーネントを使用する SiteMinder アーキテクチャを示しています。



このアーキテクチャで、緑で強調表示されているポリシー サーバと CA SiteMinder for Secure Proxy Server は拡張されたセッション保証に使用できます。 既存のポリシー サーバと CA SiteMinder for Secure Proxy Server の使用は、この機能の展開に追加のハードウェアが必要ないことを意味します。ただし、このアーキテクチャで、拡張されたセッション保証の負荷が増加するにつれて、ポリシー サーバと CA SiteMinder for Secure Proxy Server の CPU 使用率も増加します。いずれかのコンポーネントのスレッドの使用率が 100 % になるか、CPU が負荷に対応できなくなるまで負荷が増加すると、SiteMinder のトランザクションはすべて、拡張されたセッション保証を使用するように設定されているかどうかにかかわらず、その影響を受けます。

可能なアーキテクチャ 2 - 既存のポリシー サーバの使用

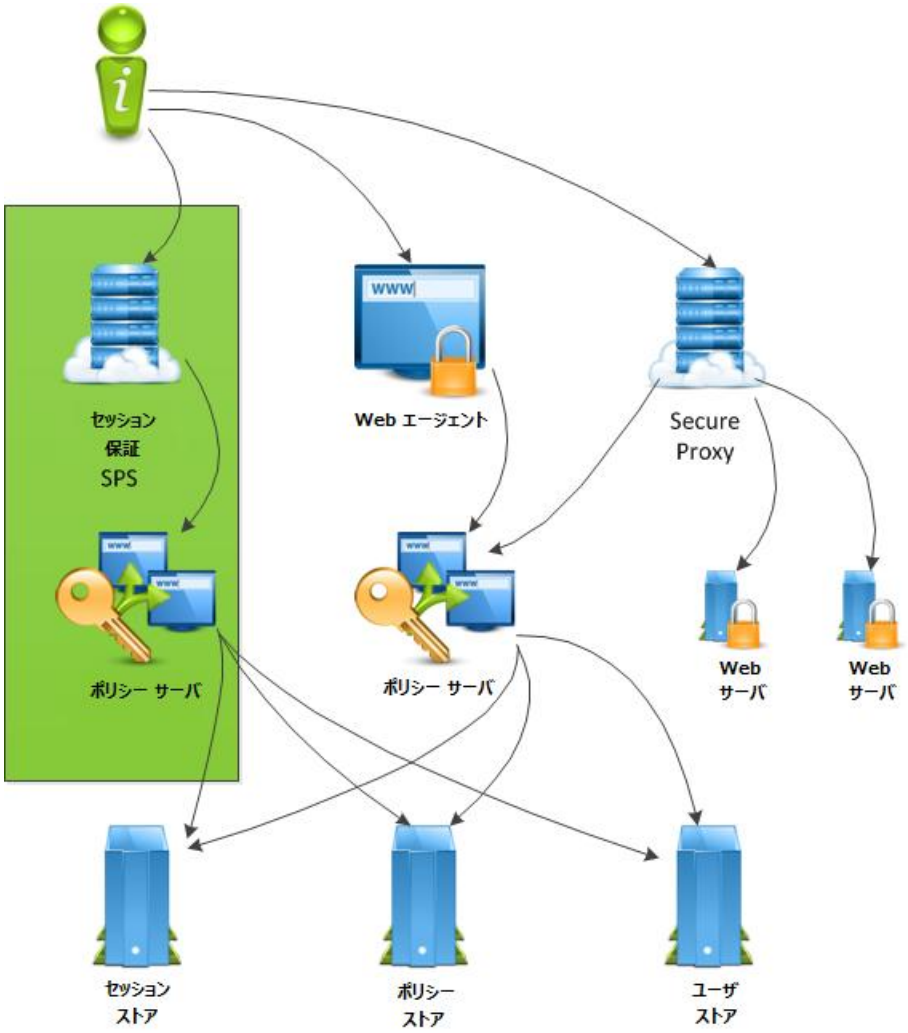
以下の図は、拡張されたセッション保証の展開に新しい CA SiteMinder for Secure Proxy Server インスタンスを使用する SiteMinder アーキテクチャを示しています。



このアーキテクチャでは、新しい CA SiteMinder for Secure Proxy Server が緑で強調表示されて導入されています。 この CA SiteMinder for Secure Proxy Server は、増加した CPU 使用率またはバックエンド Web サーバへのリクエストをプロキシするために使用される別の CA SiteMinder for Secure Proxy Server インスタンスのパフォーマンスの低下を回避するために、拡張されたセッション保証タスクをすべて実行します。 ただし、拡張されたセッション保証フロー アプリケーションを実行する CA SiteMinder for Secure Proxy Server インスタンスとその他のエージェントおよび CA SiteMinder for Secure Proxy Server インスタンスの両方で同じポリシー サーバを共有することで、ポリシー サーバの使用要求がその能力を越えて増加すると、アプリケーションおよびエージェントからの SiteMinder トランザクションはすべて影響を受けます。

可能なアーキテクチャ 3 - セッション保証コンポーネントの完全な分離

以下の図は、拡張されたセッション保証を展開するために、新しいポリシー サーバおよび CA SiteMinder for Secure Proxy Server を使用する可能な SiteMinder アーキテクチャを示しています。



このアーキテクチャでは、新しい CA SiteMinder for Secure Proxy Server インスタンスは拡張されたセッション保証をホストするためだけに展開されます。 新しい CA SiteMinder for Secure Proxy Server は新しいポリシー サーバと通信します。 このアーキテクチャでは環境内のハードウェアが増えますが、それれによって既存のポリシー サーバの負荷およびパフォーマンスが、基本的なアーキテクチャに可能な限り近いレベルに維持されます。

このアーキテクチャは、拡張されたセッション保証の迅速な展開が求められる、大規模な組織向けに推奨されます。 これは、拡張されたセッション保証による CPU 使用率の増加や、リクエストの一般処理に必要なスレッドの占有を最小限にするのに役立ちます。

第 3 章: SiteMinder 実装の計画

実装計画概要

どのように SiteMinder を実装するかに関連する決定は以下のものに依存します。

- アプリケーションを SiteMinder アクセス管理モデルにマッピングする方法
- 使用する SiteMinder 機能
- どのようにして SiteMinder ポリシー サーバおよびエージェントの管理を計画するか

SiteMinder を展開および設定する前に、このセクションの情報について考慮することをお勧めします。

ポリシー管理モデル

SiteMinder ポリシー管理モデルによって、Web リソースおよびそれぞれのユーザ群にアクセス許可を定義できます。 ポリシー管理モデルは以下を確立します。

- 保護されるリソース。
- リソースにアクセスできるユーザ。
- ユーザ群に付与されるアクセス権限のタイプ。
- SiteMinder がリソースへのアクセスを許可した場合に発生する状況。
- SiteMinder がリソースへのアクセスを拒否した場合に発生する状況。

すべての SiteMinder 機能は使用するモデルにかかわらず利用可能です。モデル間の主な違いはそれぞれの設定に必要な SiteMinder の知識のレベルです。 以下の 管理 UI オブジェクトはポリシー管理モデルを表します。

- アプリケーション
- ポリシー ドメインおよびドメイン オブジェクト

注: 以下の SiteMinder コア オブジェクトが、アプリケーション オブジェクトまたはドメイン ポリシーの設定に必要です。

- ホスト設定オブジェクト
- エージェント設定オブジェクト
- エージェント オブジェクト
- ユーザ ディレクトリ オブジェクト

  注: これらのオブジェクトの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

アプリケーション オブジェクトを使用するポリシー管理

アプリケーション オブジェクトは、Web アプリケーション、Web サイト、または Web サービスのための完全なセキュリティ ポリシーを定義する直観的な方法を提供します。アプリケーションは、どのユーザがどのリソースにアクセスできるか決める資格ポリシーを指定するために、リソースとユーザ ロールを関連付けます。

注: アプリケーション オブジェクトはポリシー情報を定義します。この情報はポリシー ドメインおよびそのサブオブジェクトでも設定できます。これには、レルム、ルール、ルール グループ、レスポンス、およびポリシーが含まれます。 以下の表に、この関係の概要を示します。

アプリケーション ダイアログとグループ ボックス	同等ドメイン コンポーネント
一般設定	保護されたリソースのポリシー ドメインおよびルートの場所。
コンポーネント	レルム、および同じセキュリティ要件を共有するアプリケーション内のリソースの場所。
リソース	ルールおよび必要な認証または許可アクション。
アプリケーション ロール	ユーザ ディレクトリの検索。

注: アプリケーションを使用したポリシー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。

ポリシードメインおよびドメイン オブジェクトを使用したポリシー管理

SiteMinder r12.0 よりも以前は、ポリシー ドメインおよびドメイン オブジェクト（レルム、ルール、レスポンス、ポリシーなど）がリソースを保護する唯一の方法でした。それら、ポリシー ドメイン、ドメイン オブジェクトに満足しているポリシー サーバ管理者は、リソースのセキュリティ ポリシーを設定できます。

SiteMinder ポリシーは以下の個別の SiteMinder オブジェクトで構成されます。

- ドメイン
- ドメイン内の 1 つ以上のレルム
- ドメイン内の 1 つ以上のルールまたはルール グループ
- （オプション）ドメイン内の 1 つ以上のレスポンスまたはレスポンス グループ

ポリシー オブジェクトはこれらのコア オブジェクトをバインドして、リソース、ユーザ群、および SiteMinder がリソースへのアクセスを許可または拒否するときに必要なアクションを特定します。 そのため、SiteMinder ポリシーを設定するには、各オブジェクトについて理解している必要があります。

注: これらの各オブジェクトおよびそれぞれの SiteMinder ポリシー ロールの詳細については、「ポリシー サーバ設定ガイド」を参照してください。

保護するアプリケーションの識別

どのアプリケーションを保護しますか。 アプリケーションをどのように SiteMinder アクセス管理モデルにマッピングしますか。

組織内の個別のアプリケーション、および同じ保護レベルを必要とする各アプリケーション内の個別のリソース（URL）について検討することから始めます。 以下の指定をお勧めします。

- 1 つ以上のユーザ群に関連付けられるリソースの論理グループ（個別のアプリケーションである場合が多い）。 これらの論理グループは、SiteMinder ポリシー ドメインまたは EPM アプリケーションのリソース フィルタにマップします。SiteMinder ポリシー ドメインまたは EPM アプリケーションのリソース フィルタは、アプリケーションのルートの場所を表します。
- 同じセキュリティ（認証および許可）要件を含むアプリケーション内の個別のリソース（URL）のセット。 同じセキュリティ要件を共有するリソースのセットは、SiteMinder ポリシー レルムまたは EPM アプリケーション コンポーネントのいずれかにマッピングされます。

このようにリソースをグループ化することによって、アプリケーションを SiteMinder アクセス管理モデルにマッピングできます。

各アプリケーションに関する情報を収集するときは、以下のようなリソースの表を使用して組織情報に役立てます。

リソース	ドメイン/アプリケーション リソース フィルタ	レルム/コンポーネント リソース フィルタ
例： Corporate Portal	**例：** パフォーマンス管理アプリケーション	**例：** Manager リソース

注: 保護が必要なアプリケーションの特定は容量計画にも役立ちます。

詳細情報:

容量計画が導入されました (P. 107)
拡張パラメータの無視 (P. 174)

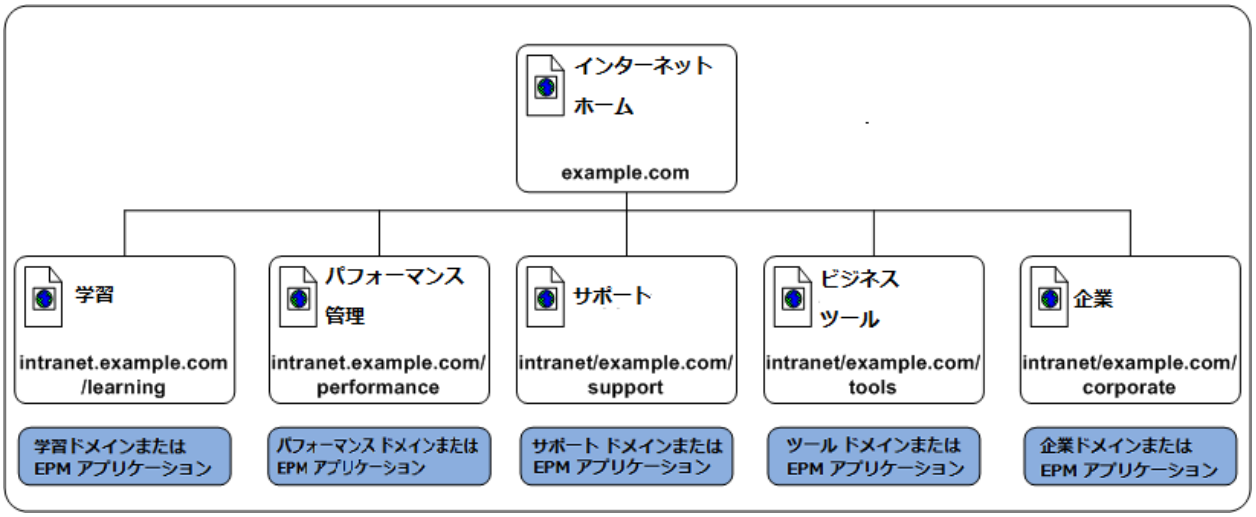
ドメインまたは EPM アプリケーションへのリソースのグループ化

SiteMinder ポリシー ドメインまたは EPM アプリケーションの定義は、1 つ以上のユーザ群に関連付けられるリソースの論理グループ（個別のアプリケーションである場合が多い）の特定に依存します。このレベルでリソースをグループ化することによって、同じセキュリティ要件を共有するアプリケーション内の個別のリソース（URL）のセットを特定できます。

注: SiteMinder ポリシー ドメインまたは EPM アプリケーションの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

これらの要件を決定するための戦略として、組織のサイトマップを確認することがあります。

たとえば、ある架空会社には、以下のサイトマップが表す企業イントラネットがあります。



この例では、企業ポータルは以下のリソースの論理グループに分割されています。

- 学習
- パフォーマンス管理
- サポート
- ビジネス ツール
- 企業

企業イントラネット用のリソースの表は以下のようになります。

リソース	ドメイン/EPM アプリケーション フィルタ	レルム/コンポーネント フィルタ
企業イントラネット	intranet.example.com	該当なし
学習	intranet.example.com/learning	該当なし
パフォーマンス管理	intranet.example.com/performance	該当なし
サポート	intranet.example.com/support	該当なし
ビジネス ツール	intranet.example.com/tools	該当なし
企業	intranet.example.com/corporate	該当なし

詳細情報:

ドメインおよび認証パフォーマンス (P. 192)

レルムまたは EPM コンポーネントへの複数のリソースのグループ化

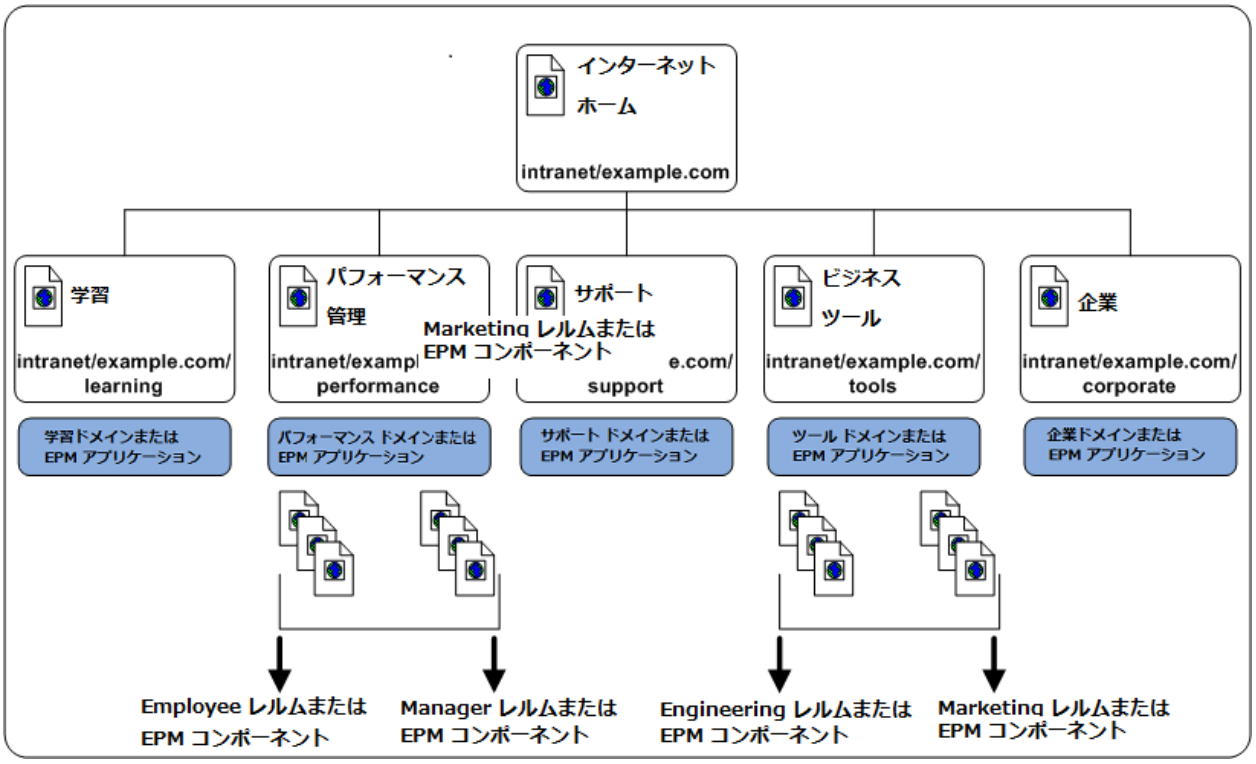
SiteMinder ポリシー レルムまたは EPM コンポーネントの定義は、SiteMinder ポリシー ドメインまたは EPM アプリケーション内の同じセキュリティ要件またはパーソナライズ要件を共有する個別のリソース（URL）のセットの特定に依存します。 レルムの内容または EPM コンポーネントは同じ認証方式を共有します。 その結果、プロセスの初期にこれらのリソースを特定することは、個別のセキュリティ要件を満たすために必要な認証方式の決定に役立ちます。

注: SiteMinder ポリシー レルムおよび EPM コンポーネントの詳細については、「ポリシー サーバ設定ガイド」を参照してください。

たとえば、Performance Management アプリケーションおよび Business Tools アプリケーションのそれぞれによって、特定のユーザ群はアプリケーションのルートにアクセスできますが、各アプリケーションには、リソースに適したセキュリティまたはパーソナライズのレベルを提供する追加の SiteMinder ポリシー レルムまたは EPM コンポーネントが含まれます。

- パフォーマンス管理アプリケーションには、正社員のみがアクセスできるリソース、およびマネージャのみがアクセスできるリソースが含まれます。
- Business Tools アプリケーションには、研究開発の社員のみがアクセスできるリソース、およびマーケティングの社員のみがアクセスできるリソースが含まれます。

注: 図には示されていませんが、特定の Web エージェント、認証および許可イベントを制御するために SiteMinder ポリシー ルールおよび EPM リソースが使用されます。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。



アプリケーション用のリソースの表は以下のようになります。

リソース	ドメイン/EPM アプリケーション フィルタ	レルム/コンポーネント フィルタ
企業イントラネット	intranet.example.com	該当なし
学習	intranet.example.com/learning	該当なし
パフォーマンス管理	intranet.example.com/performance	/employee /manager
サポート	intranet.example.com/support	該当なし
ビジネス ツール	intranet.example.com/tools	/engineering /marketing
企業	intranet.example.com/corporate	該当なし

ユーザ ストアの特定

SiteMinder は、企業ネットワーク内の既存のユーザ ストアへの 1 つ以上の接続によってユーザを認証および許可できます。 保護するアプリケーション (P. 68)を特定したら、以下の質問を検討してください。

- アプリケーションは、一元化されたユーザ ストアまたは個別のユーザ ストアのどちらを認証に使用しますか。
- アプリケーションが個別のストアを使用する場合、このプロジェクトには、ユーザ ID を単一のストアに一元化するタスクが含まれていますか。
- アプリケーションは、ユーザの認証および許可に同じストアを使用しますか。 または、個別のストア（複数可）が許可に使用されますか。

各アプリケーションが使用するストアを特定すると、以下の場合に役立ちます。

- SiteMinder 管理者が、リソースを保護するために SiteMinder ポリシー ドメインで設定する必要があるユーザ ストア接続を特定します。

  注: ドメイン内のユーザ ストア接続の設定の詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

- SiteMinder ディレクトリ マッピング機能が必要な環境であるかどうかを判断します。 デフォルトでは、SiteMinder によって、ユーザは同じユーザ ストア（複数可）に対して認証および許可されているとみなされます。 ただし、1 つ以上のストアに対して認証し、その他に対して許可するように SiteMinder ポリシー ドメインを設定できます。

  注: ディレクトリ マッピングの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

各アプリケーションに関する情報を収集するときは、以下のような表を使用して情報を整理します。

ユーザ ストア名	ユーザ ストア タイプ	認証?	許可?

認証方法の特定

SiteMinder は、リソースが必要とする保護レベルの変化に対応できるよう複数の認証方式をサポートします。

- 基本
- フォームベースのユーザ ID およびパスワード
- RSA® ACE/SecurID® などのハードウェアおよびソフトウェア トークンベース
- 統合 Windows 認証（IWA）
- Microsoft Windows CardSpace などの情報カード認証方式（ICAS）
- MIT Kerberos
- RADIUS および SafeWord などのサーバベース
- X.509 証明書ベース
- SiteMinder SDK を使用して作成されたカスタム認証方式

推奨しているように、同じセキュリティ要件を共有するリソース（URL）のセットを特定して、保護するアプリケーション (P. 68)を特定したら、以下の質問を検討してください。

- 組織が特定のタイプのリソースに対して満たすべき認証ガイドライン、規制または法規がありますか。
- 情報の機密性と重要性はどの程度か
- どのようなタイプのユーザがこの情報にアクセスするか
- どのタイプのセキュリティをユーザが期待していますか。

これらのような質問の回答は、以下の点で役立ちます。

- 環境に必要な認証方法を特定します。
- 特定のリソースを保護するために SiteMinder 管理者が設定する必要がある認証方式を特定します。

  注: 認証方式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。

各リソースに関する情報を収集するときは、保護する予定のアプリケーションによって情報を整理することをお勧めします。 たとえば、以下の表では、保護するアプリケーション (P. 68)で説明したとおりに、アプリケーションが個別のドメインおよびレルムにグループ化されていると仮定しています。

リソース	URL	レルム	認証方法

パスワード管理オプションの特定

セキュリティ ポリシーには、組織によるユーザ パスワードの管理が必要ですか。 今後ユーザ パスワードを管理することが見込まれますか。

SiteMinder パスワード ポリシーを使用して企業のパスワード要件を適用できます。 パスワード ポリシーは、パスワードを受理する前に以下のタイプの特性に対してユーザ パスワードを検証できます。

構成

パスワードの最小または最大文字数、使用可能な文字のタイプ、およびそれらの文字をあるパスワード中で再度使用することが可能かどうか、またはどれくらいの頻度で繰り返し使用できるかを確認します。

年齢

同じパスワードをどれくらい長い時間使用できるか、パスワードの変更が必要になるまでにどのくらい長い時間非アクティブであることが可能か、および、期限切れパスワードはどのくらい長い時間を経て、またはどのくらいの頻度で再利用できるか、これらの時間制限を確認します。 期限切れパスワードを持つユーザに対して、次のいずれかのレスポンスを指定できます。

- そのユーザ アカウントを無効にする
- 強制的にパスワードを変更させる

試行

ユーザが以前に不正なパスワードを入力した回数を記録し、その回数が制限を超えたときに次のいずれかのアクションを講じます。

- ユーザ アカウントを無効にする。
- 指定した期間の待機後に 1 回のログイン試行を許可するか、再度アカウントを有効にする。

注: 詳細については、「*SiteMinder ポリシー サーバ設定ガイド*」を参照してください。

パスワード ポリシーの考慮事項

企業内にパスワード ポリシーを実装する予定の場合は、以下を考慮します。

- SiteMinder には、パスワードおよびパスワード関連情報を格納するディレクトリ内にあるいくつかの属性の独占的使用を含む、ユーザ ディレクトリへの読み取り/書き込みアクセス権限が必要です。
- パスワード ポリシーは、パスワードを検証するために、ユーザ ディレクトリの追加検索が必要になるため、SiteMinder のパフォーマンスに影響を及ぼす可能性があります。 ディレクトリ全体ではなく、ユーザ ディレクトリの一部のみを検索するように設定されたパスワード ポリシーも、パフォーマンスに影響を及ぼす可能性があります。
- ユーザ ディレクトリにネイティブ パスワード ポリシーがある場合、このポリシーは以下の条件を満たす必要があります。
  - SiteMinder パスワード ポリシーよりも制限が少ないか、または
  - 無効

  上記を満たさない場合、ネイティブ パスワード ポリシーは、SiteMinder に通知することなくパスワードを許可または拒否します。 その結果、SiteMinder はこれらのパスワードを管理できなくなります。
- デフォルトでは、パスワードを変更するときにユーザが間違った情報を入力した場合、SiteMinder は一般的な失敗メッセージを返します。このメッセージは失敗理由を明示しません。 デフォルト動作を変更し、パスワードの変更に失敗した理由をユーザに明示的に伝えるには、DisallowForceLogin レジストリ キーを作成し、有効にします。
- 複数のポリシー サーバ上でパスワード ポリシーを使用する場合は、すべてのサーバのシステム時刻を同期します。 時刻を同期することにより、アカウントやパスワードの強制変更が途中で無効になるのを防ぐことができます。

  注: 詳細については、「*SiteMinder ポリシー サーバ設定ガイド*」を参照してください。

Web エージェントの管理者の指定

Web エージェントは起動時にポリシー サーバに接続します。 ポリシー サーバには、関連付けられた Web エージェントをその設定パラメータの場所に送るエージェント設定オブジェクト（ACO）が含まれます。

アプリケーションが組織全体にどのように展開するかは、SiteMinder Web エージェントの設定パラメータを格納する最も効率的な方法を決定するのに役立ちます。 以下の質問について考慮します。

1. ほとんどの Web アプリケーションを同じセキュリティ要件で大規模なサーバ ファーム上に展開していますか。
2. ほとんどの Web アプリケーションが一元化された担当者またはグループによって管理されていますか。
3. ほとんどの Web アプリケーションが別々のセキュリティ要件で個別の Web サーバ上に展開していますか。
4. ほとんどの Web アプリケーションが異なる部門または物理的に異なる場所の異なる担当者によって管理されていますか。

上記のリストの 1 つまたは 2 つの質問にはいと答えた場合は、以下の設定方法を試してください。

- 中央設定

  ポリシー サーバにあるエージェント設定オブジェクト（ACO）から 1 つ以上のエージェントのパラメータを管理します。中央エージェント設定では、複数のエージェントのパラメータ設定を一度に更新できます。通常、個々の Web アプリケーションはそれぞれ個別の ACO を使用します。それらの設定は、Web アプリケーションを保護するすべてのエージェントで共有されます。 たとえば、1 つの会計アプリケーションを保護する 5 つのエージェントがある場合、そのアプリケーションの設定で 1 つの ACO を作成できます。 5 つのエージェントはすべて、同じ ACO のパラメータ設定を使用します。

  別のアプリケーションについては、個別のエージェント設定オブジェクトを使用することをお勧めします。 たとえば、より厳密なセキュリティ要件を持つ人事アプリケーションを保護する場合は、その人事アプリケーション用に別の ACO を作成します。

  エージェントが起動すると、関連する ACO の AllowLocalConfig パラメータ値を読み取ります。 値が no に設定されている場合、エージェントは ACO のパラメータ設定を使用します（エージェント ログおよびトレース ファイル設定を除く）。 エージェント ログ ファイルおよびトレース ファイルは、ACO 設定にかかわらず、常にローカルに制御できます。

  注: エージェント設定およびメンテナンスが簡略化されるので、（可能な限り）中央エージェント設定を使用することを推奨します。

上記のリストの 3 つまたは 4 つの質問にはいと答えた場合は、以下の設定方法を試してください。

- ローカル設定

  Web サーバ自体にインストールされたファイルを使用して、各 Web エージェントを個別に管理します。 Web エージェントが開始すると、関連付けられたエージェント設定オブジェクト（ACO）の AllowLocalConfig パラメータの値を読み取ります。 値が yes に設定されている場合、Web エージェントは Web サーバ上の LocalConfig.conf ファイルのパラメータ設定を使用します。ローカル ファイル内のパラメータ設定は、ポリシー サーバのエージェント設定オブジェクトに格納されているすべての設定に優先します。

以下の質問は、ローカル エージェント設定で企業のニーズをより満たすことができる別の状況の特定に役立ちます。

- リバース プロキシ サーバに一部の Web エージェントを展開しますか。

  たとえば、少数の場所にリバース プロキシ サーバを実装しているとしても、Web エージェントの大規模なグループを持つ内部リソースを保護する必要があります。 ローカル設定を使用してリバース プロキシ Web エージェントを管理できます。

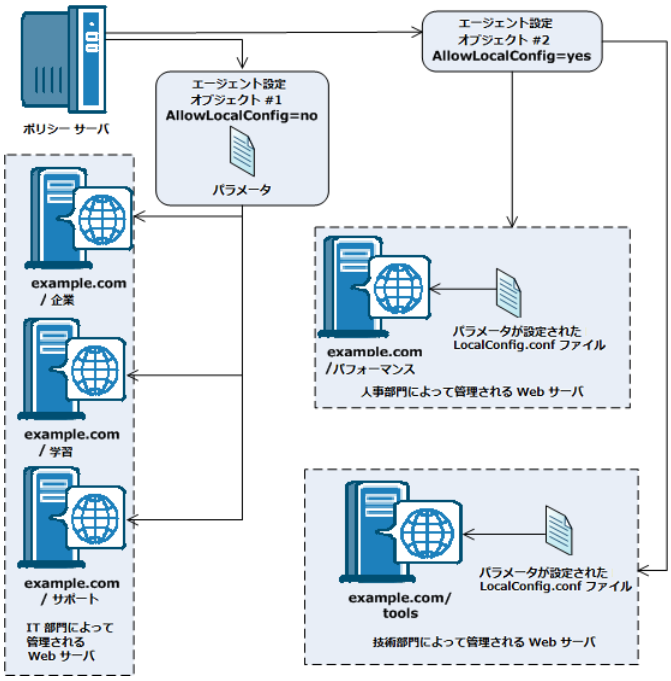
- ローカル Web サーバ管理者が一部の Web エージェント設定のみを変更することを許可しますか。

  たとえば、組織は SiteMinder を使用してセキュリティ ポリシーを管理および適用しますが、リモート オフィスの Web サーバ管理者にログオンおよびログオフ ページのカスタマイズを許可します。 ACO の AllowLocalConfig パラメータの値に個別のパラメータを追加して、カスタマイズされたページのそれらの設定のみ変更することを管理者にのみ許可できます。

  注: 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。

中央設定とローカルの設定の組み合わせ

ニーズに合わせて中央設定およびローカル設定の組み合わせを使用することもできます。 たとえば、中央設定で 3 つの類似した Web サーバを管理しながら、ローカル設定で別の 2 つのサーバを管理できます。以下の図に例を示します。



データ センターの特定

後ほど説明する複数の要因が、複数のデータ センターにわたる SiteMinder コンポーネントの実装を決定する方法に影響を及ぼす場合があります。SiteMinder 環境に合うデータ センターおよび目的をそれぞれ特定することによって、SiteMinder コンポーネントの実装方法を判断するときに情報に基づく決定を行えます。 以下の質問について考慮します。

- 展開にはどれだけのデータ センターが含まれ、各センターはどこにありますか。
- 複数のデータ センターがある場合
  - それらのすべてがアクティブですか、または一部はディザスタ リカバリまたはバックアップ専用ですか。
  - 保護されている各アプリケーションは単一のデータ センターに存在しますか、または複数のセンターにわたって存在しますか。
  - フェールオーバをデータ センター レベルで設定しますか、またはデータ センターにわたって設定しますか。
  - データ センター間の帯域幅およびスループットはどれくらいですか。

各データ センターに関する情報を収集するときは、以下のようなリソースの表を使用して結果を整理します。

データ センター名	場所	目的

詳細情報:

複数のデータ センター (P. 136)

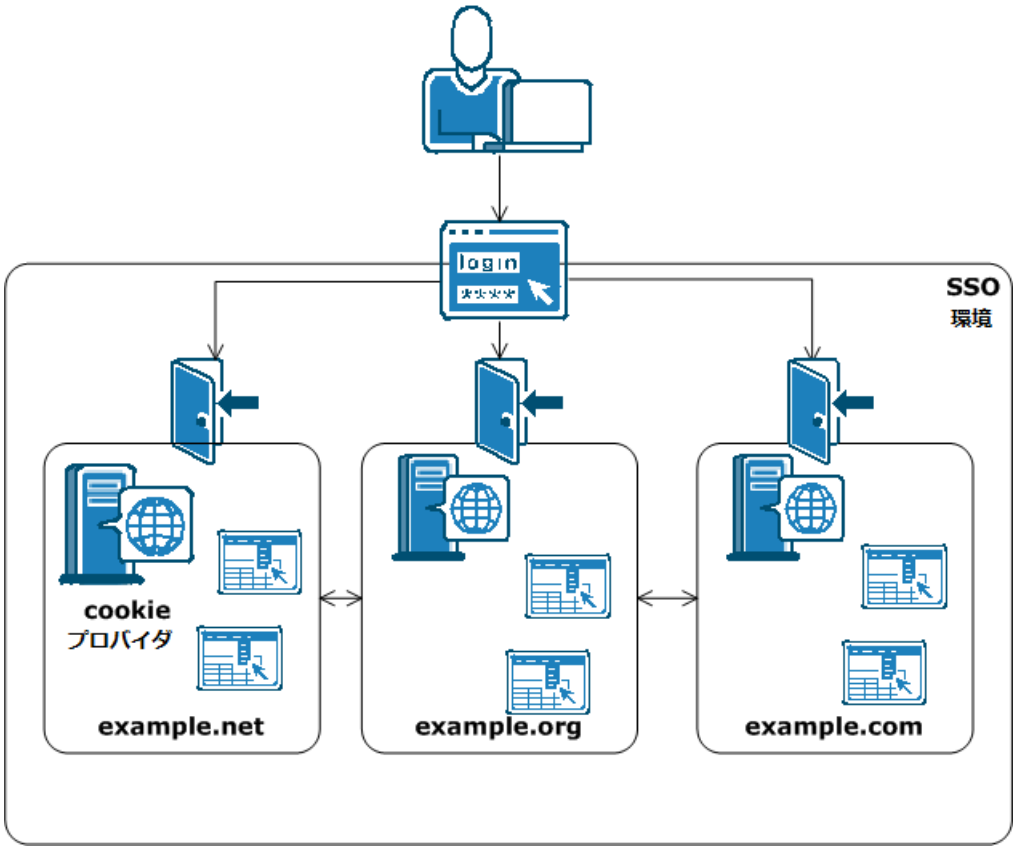
複数の cookie ドメインで保護するリソースを識別する

企業内のシングル サインオン環境は複数の Cookie ドメインにまたがりますか。

SiteMinder では、cookie プロバイダとして設定された SiteMinder Web エージェントを使用して、複数の cookie ドメインにおけるシングル サインオンを実装します。

cookie プロバイダの Web エージェントが存在する cookie ドメインのことを、cookie プロバイダ ドメインといいます。 シングル サインオン環境において、他の cookie ドメインにあるその他すべての Web エージェントは、1 つの cookie プロバイダを参照しています。

以下の図では、複数の Cookie ドメインを使用する SSO 環境の例を示します。

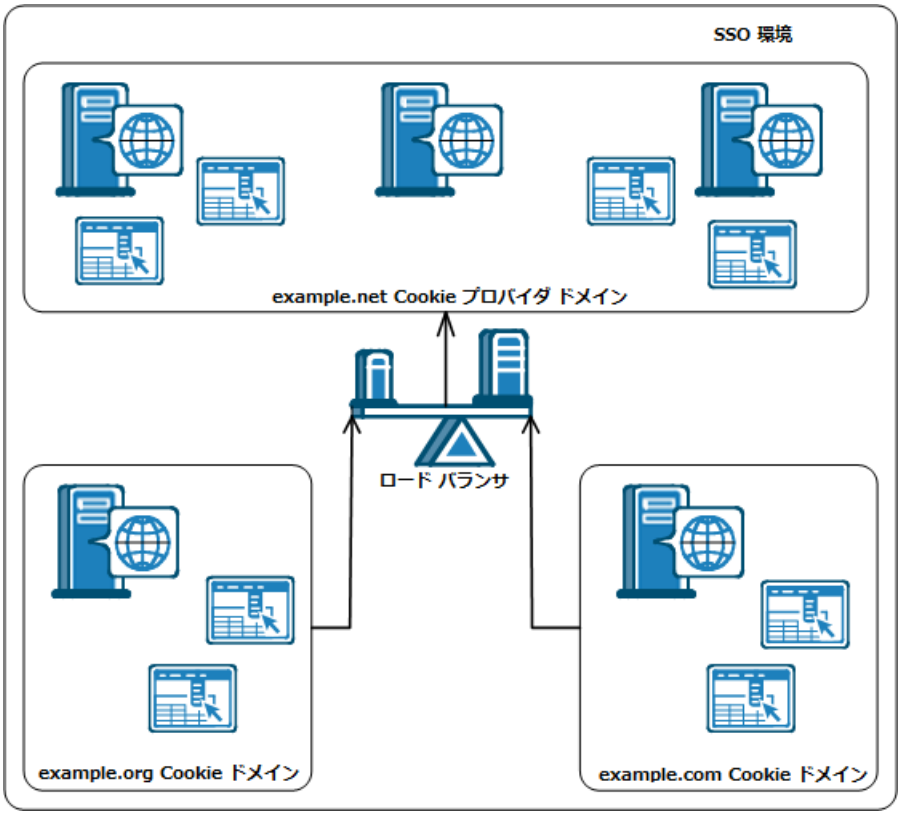


注: Cookie プロバイダの詳細については、「*Web エージェント設定ガイド*」を参照してください。

Cookie プロバイダ ドメインと他の Cookie ドメイン間での SSO 負荷分散

シングル サインオン環境内のエージェントは負荷分散を使用するか。

SSO 環境内のエージェントはすべて一つの Cookie プロバイダ ドメインを参照する必要があります。 Cookie プロバイダ ドメインの Web サーバと SSO 環境内の他の Cookie ドメインの間にロード バランサを追加します。以下の図に例を示します。



example.org Cookie ドメイン内の Web エージェント、および example.com Cookie ドメイン内の Web エージェントは両方とも、example.net の同じ Cookie プロバイダ ドメインを参照しています。 ロード バランサは、example.net Cookie プロバイダ ドメイン内のすべての Web サーバ間でトラフィックを均等に分散させます。

パートナーシップに CA SiteMinder® Federation が必要であるかどうかを判断する

既存のまたは予定された企業間（B2B）パートナーシップには、組織がパートナーと安全にアイデンティティ情報を共有することが必要ですか。

CA SiteMinder® Federation では、アイデンティティ フェデレーションを有効にすることによりパートナー サイトに対して SiteMinder 機能を拡張できます。CA SiteMinder® Federation は 2 つの展開オプション（レガシー フェデレーション と パートナーシップ フェデレーション）を提供します。

パートナー組織間のフェデレーション トランザクションによって、エンタープライズは以下を実行できます。

- 安全な方法によりパートナー間でユーザ識別情報を交換します。
- パートナーのユーザ ID と社内のユーザ ID の間にリンクを確立します。
- 複数ドメインのパートナー Web サイト全体でシングル サインオンを有効にします。
- すべてのパートナー Web サイト間、または各パートナー Web サイトの個別のセッション間でのシングル ログアウトなど、パートナー サイト間の異なるユーザ セッション モデルを処理します。
- パートナーから送られるユーザ情報に基づいてリソースへのアクセスを制御します。
- 異種環境間の相互運用性を許可します。

CA SiteMinder® Federation により、エンタープライズはアサーションを生成または消費できます。 CA SiteMinder® Federation は以下の標準およびプロトコルをサポートします。

- SAML 1.0 （レガシー フェデレーション のみ）
- SAML 1.1 および 2.0
- Microsoft ADFS/WS-Federation （レガシー フェデレーション のみ）

- SAML ブラウザ アーティファクト プロトコル
- SAML POST プロトコル
- WS-Federation Passive Requestor Profile プロトコル（レガシー フェデレーション のみ）

注: CA SiteMinder® Federation は SiteMinder から別々にライセンスを付与されます。 ライセンスの詳細については、CA アカウント担当者に問い合わせてください。 フェデレーションの詳細については、「*CA SiteMinder® Federation レガシー フェデレーション ガイド*」または「*CA SiteMinder® Federation パートナーシップ フェデレーション ガイド*」を参照してください。

組織がフェデレーションの実装を計画する場合は、以下のような表を使用してパートナー、およびアイデンティティ フェデレーションを有効にするための方法を特定します。

パートナー	標準	プロトコル

Advanced Encryption Standard が必要かどうか判断する

組織は、Federal Information Processing Standard （FIPS） 140-2 準拠のアルゴリズムを使用する必要がありますか。

Advanced Encryption Standard （AES）の SiteMinder 実装は FIPS 140-2 標準をサポートしています。 FIPS とは、AES に適合する暗号モジュールの認定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。

ポリシー サーバは、FIPS 140-2 準拠の認証された暗号ライブラリを使用します。 これらの暗号ライブラリにより、SiteMinder 環境で AES 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

注: SiteMinder が使用する暗号ライブラリ、および FIPS 専用モードで機密データを暗号化するために使用される AES アルゴリズムの詳細については、「ポリシー サーバ管理ガイド」を参照してください。FIPS の動作モードおよびポリシー サーバのインストール時にどちらを使用するかの詳細については、「*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。

FIPS 専用モードによって AES 暗号化を実装する場合は、以下の点について考慮してください。

- ディレクトリ サーバ、データベース、およびドライバを含むすべてのサードパーティ コンポーネントを FIPS 準拠のアルゴリズムをサポートするように設定する必要があります。

  注: FIPS 140-2 標準をサポートするベンダー機能の詳細については、ベンダー固有のマニュアルを参照してください。

- X.509 クライアント証明書認証方式が使用される環境の場合は、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てください。

- ポリシー サーバが SSL を使用してポリシー ストアまたはユーザ ストアに接続する場合は、ポリシー サーバおよびディレクトリ ストアが FIPS 準拠の証明書を使用することを確認してください。
- SiteMinder r12.x 付属のすべての Web エージェントは FIPS 準拠です。他のエージェントが FIPS 準拠であるかどうかを判断するには、エージェント固有のマニュアルを参照してください。

重要: FIPS 専用モードで実行されている環境は、以前のバージョンの SiteMinder で動作することはできず、上位互換性はありません。この要件には、すべてのエージェント、エージェント API の旧バージョンを使用するカスタム ソフトウェア、および PM API またはポリシー サーバが公開する他の API を使用するカスタム ソフトウェアが含まれます。そのようなソフトウェアをすべて対応する SDK の現行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。

仮想化が使用されるかどうかの判断

SiteMinder は仮想環境に実装されますか。

仮想環境に SiteMinder を実装する前に、以下の点について考慮してください。

- 仮想化上の CA ポリシーを確認してください。
- 以下を確認してください。
  - 仮想環境、およびホスト システムがアプリケーションに課すことができるパフォーマンス オーバーヘッドを把握します。
  - 仮想環境を調整して、可能な限りパフォーマンスのオーバーヘッドを除去します。

    注: 仮想環境のパフォーマンス チューニングの詳細については、各ベンダーのドキュメントを参照してください。
- CPU、ディスク領域およびメモリが仮想環境で使用できるサイズであることを確認してください。各 SiteMinder インストール ガイドに詳述されているシステム要件を使用して、システム全体に展開するコンポーネント数を決定します。
- クロック同期および複数のオペレーティング システムに関する問題に注意してください。非同期のクロックによって予期しない SiteMinder 動作が生じる場合があります。

- コンポーネントを展開する場所について検討する場合については以下のとおりです。
  - 仮想環境にポリシー サーバを展開することをお勧めします。 ポリシー サーバに自身のイーサネット ポートがあることをお勧めします。 専用ポートは、使用できる帯域幅の他の仮想ホストとの競合によって、SiteMinder がリクエストを失わないようにします。
  - 仮想化された Web サーバに Web エージェントを展開することをお勧めします。
  - すべての SiteMinder データ ストアを物理ハードウェアおよびオペレーティング システムに展開することをお勧めします。 ディレクトリ サーバおよびデータベースは、リソースにかなり依存する場合があります。 仮想化された環境に展開した場合、この依存性によりパフォーマンスが低下する可能性があります。

ポリシー サーバの管理方法の決定

個々の業務部門がポリシー サーバを管理する必要がありますか。または、すべてのポリシー サーバを単一の業務部門で集中的に管理できますか。

ローカル ポリシー サーバ管理

個々の業務部門がポリシー サーバおよびポリシー ストアをローカルに管理する場合は、ローカル ポリシー サーバ管理について以下の点を考慮してください。

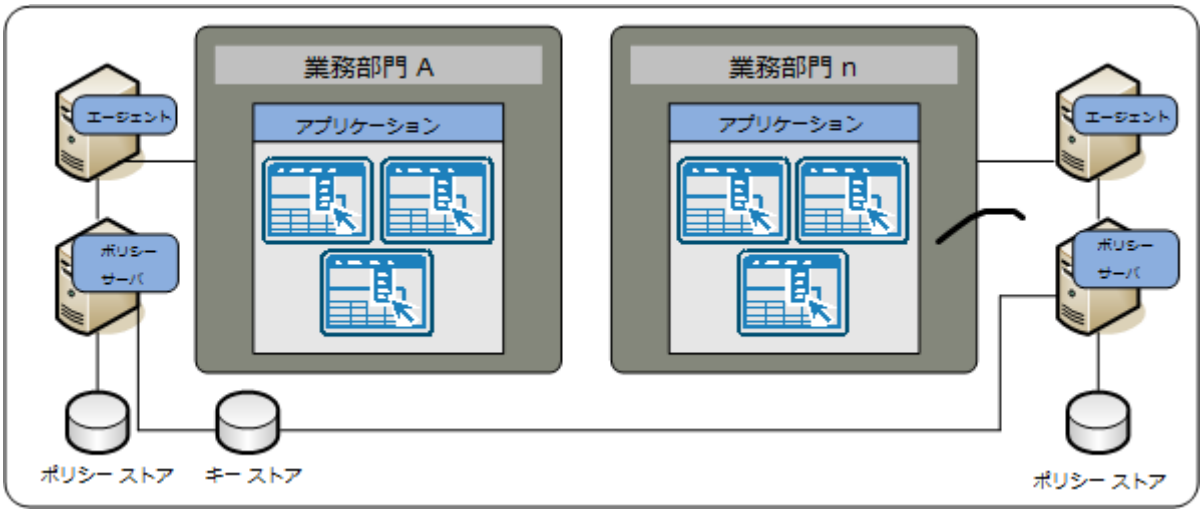
- 各業務部門は、個別のニーズに基づいてセキュリティ要件を管理できます。
- 以下のように SiteMinder インフラストラクチャがより複雑になる場合があります。
  - ローカル ポリシー サーバ管理によって、管理およびアップグレードが必要なポリシー サーバおよびポリシー ストアが増加する場合があります。

- シングル サインオンが要件である場合、ローカル ポリシー サーバ管理によって追加の SiteMinder 設定が必要になります。 示されているように、両方の業務部門のポリシー サーバはキー ストアを共有し、SiteMinder エージェントが同じキーを共有できるようにする必要があります。

  注: 図は、シングル サインオン要件を表す共有キー ストアを示しています。共有キー ストアはシングル サインオンを実装する唯一の方法ではなく、他の要件もあります。 シングル サインオンを促進するキー管理シナリオの詳細については、「*ポリシー サーバ管理ガイド*」を参照してください。

- SiteMinder 管理者が異なる業務部門に存在するため、SiteMinder コア オブジェクト、ポリシー、および EPM アプリケーションの一貫した実装および管理がより難しくなる場合があります。

以下の図では、ポリシー サーバをローカルに管理する 2 つの業務部門について説明します。



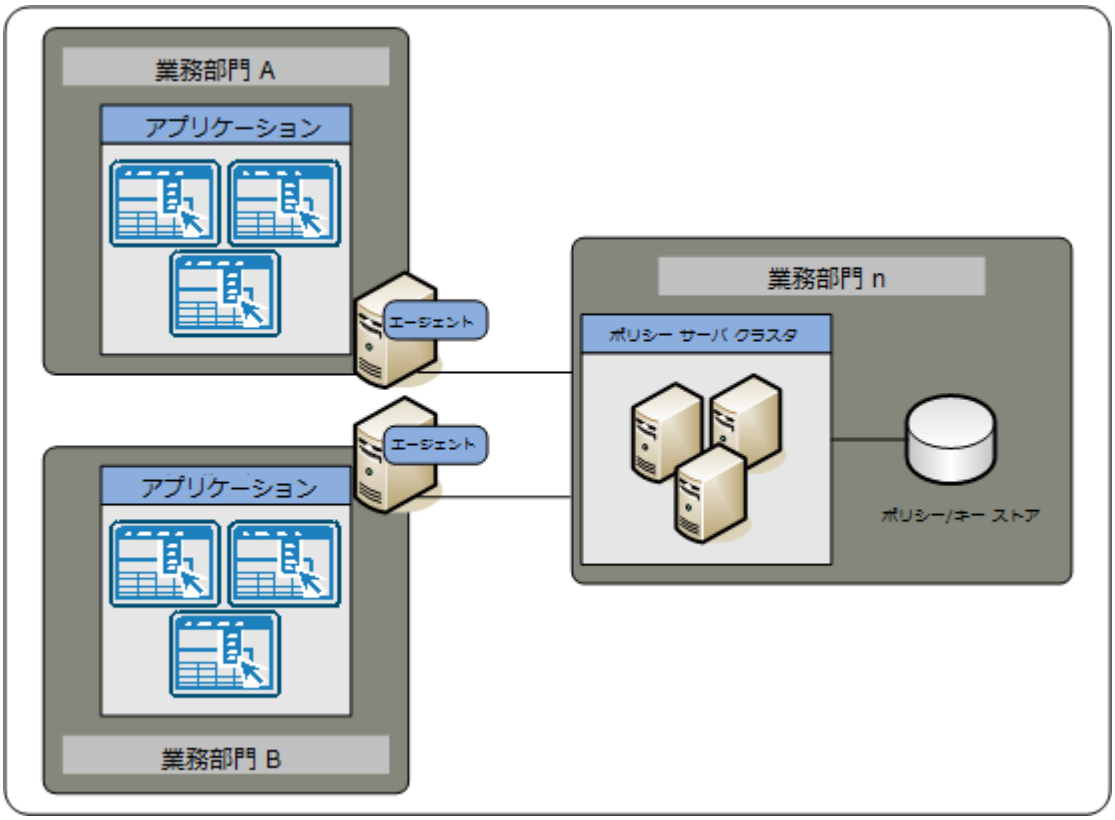
中央ポリシー サーバ管理

1 つの業務部門がポリシー サーバを一元的に管理する場合は、中央ポリシー サーバ管理について以下の点を考慮してください。

- すべての SiteMinder 管理者が同じ業務部門に存在するので、SiteMinder コア オブジェクト、ポリシー、および EPM アプリケーションの一貫した実装が容易になる場合があります。
- すべての SiteMinder 管理者が同じ業務部門に存在するので、これらのオブジェクトの管理が容易になる場合があります。

  注: 示されているように、個々の業務部門はアプリケーションを保護している SiteMinder エージェントの管理を続行できます。
- SiteMinder インフラストラクチャを簡略化する場合があります。 集中管理によって、管理およびアップグレードが必要なポリシー サーバおよびポリシー ストアを減らすことができます。
- 管理者は SiteMinder のパフォーマンスを一元的に監視できます。

以下の図では、すべてのポリシー サーバを管理する単一の業務部門について説明します。



Web エージェントの管理方法の決定

同じように設定される複数の Web エージェントがある場合、ポリシー サーバ上でエージェント設定オブジェクトを使用することによって、Web エージェントの管理がより容易になります。1 つのエージェント設定オブジェクトを共有できる Web エージェントの数に制限はありません。 ポリシー サーバ上で行われた設定変更は、設定オブジェクトを使用するすべての Web エージェントに自動的に適用されます。

注: 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。

第 4 章: eTrust SOA Security Manager 実装の計画

ポリシー管理モデル

eTrust SOA Security Manager アクセス管理モデルによって、アプリケーションおよびそれぞれのユーザ群にアクセス許可を定義できます。 アクセス管理モデルは以下を確立します。

- 保護されるリソース。
- リソースにアクセスできるユーザ。
- ユーザ群に付与されるアクセス権限のタイプ。
- SiteMinder がリソースへのアクセスを許可した場合に発生する状況。
- SiteMinder がリソースへのアクセスを拒否した場合に発生する状況。

ほとんどすべての eTrust SOA Security Manager 機能は使用するモデルにかかわらず利用可能です。 モデル間の主な違いはそれぞれの設定に必要な SiteMinder の知識のレベルです。 以下の 管理 UI オブジェクトはポリシー管理モデルを表します。

- アプリケーション オブジェクト
- ポリシー ドメインとポリシー オブジェクト

注: 以下の SiteMinder コア オブジェクトが、アプリケーション オブジェクトまたは SiteMinder ドメイン ポリシーの設定に必要です。

- ホスト設定オブジェクト
- エージェント設定オブジェクト
- エージェント オブジェクト
- ユーザ ディレクトリ オブジェクト

  これらのオブジェクトの詳細については、「ポリシー サーバ設定ガイド」を参照してください。

アプリケーション オブジェクトを使用するポリシー管理

eTrust SOA Security Manager 環境の新しいセキュリティ ポリシーの作成と管理に対する推奨される方法は、1 つ以上の関連する Web サービスを表すアプリケーション オブジェクトを定義した後、関連する WSDL ファイルから保護するものを定義するコンポーネントおよびリソースの設定を生成することです。

注: アプリケーション オブジェクトは可変オブジェクトを使用するポリシー式をサポートしません。変数を使用するコンテンツ ベースの許可を、ポリシー ドメインおよびポリシーを使用して実装する必要があります。

ポリシー ドメインとポリシーを使用したポリシー管理

CA SOA Security Manager または SiteMinder に満足しているポリシー サーバ管理者は、ポリシー ドメインおよびドメイン オブジェクト（レルム、ルール、レスポンス、ポリシーなど）を使用するポリシー管理を引き続き使用して、Web サービス リソースのセキュリティ ポリシーを手動設定できます。

以下の状況ではドメインおよびドメイン オブジェクトも使用する必要があります。

- 従来どおり作成され、以前の CA SOA Security Manager 展開から移行されたポリシーを変更する。
- 変数を使用してコンテンツ ベースの許可を実装する。

保護する Web サービスの識別

どの Web サービスを保護しますか。 それらをどのように eTrust SOA Security Manager ポリシー管理方法にマッピングしますか。

組織内の個別の Web サービス、および同じ保護レベルを必要とする各 Web サービス内の操作のセットについて検討することから始めます。 以下の指定をお勧めします。

- 1 つ以上のユーザ群に関連付けられる、個別の Web サービスによって提供される場合が多い、リソースの論理グループ。
- 同じセキュリティ（認証および許可）要件を含む Web サービス内の個別の操作のセット。

注: 保護が必要な Web サービスの特定は容量計画にも役立ちます。

詳細情報:

導入された eTrust SOA Security Manager 容量計画 (P. 123)

ユーザ ストアの特定

SiteMinder は、企業ネットワーク内の既存のユーザ ストアへの 1 つ以上の接続によってユーザを認証および許可できます。 保護する Web サービスを特定したら、以下の質問を検討してください。

- Web サービスは、一元化されたユーザ ストアまたは個別のユーザ ストアのどちらを認証に使用しますか。
- Web サービスが個別のストアを使用する場合、このプロジェクトには、ユーザ ID を単一のストアに一元化するタスクが含まれていますか。
- Web サービスは、ユーザの認証および許可に同じストアを使用しますか。 または、個別のストア（複数可）が許可に使用されますか。

各 Web サービスが使用するストアを特定すると、以下の場合に役立ちます。

- SiteMinder 管理者が、リソースを保護するために SiteMinder ポリシー ドメインで設定する必要があるユーザ ストア接続を特定します。

  注: ドメイン内のユーザ ストア接続の設定の詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

- SiteMinder ディレクトリ マッピング機能が必要な環境であるかどうかを判断します。 デフォルトでは、SiteMinder によって、ユーザは同じユーザ ストア（複数可）に対して認証および許可されているとみなされます。 ただし、1 つ以上のストアに対して認証し、その他に対して許可するように SiteMinder ポリシー ドメインを設定できます。

  注: ディレクトリ マッピングの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

各 Web サービスに関する情報を収集するときは、以下のような表を使用して情報を整理します。

ユーザ ストア名	ユーザ ストア タイプ	認証?	許可?

詳細情報:

保護する Web サービスの識別 (P. 94)

認証方法の特定

eTrust SOA Security Manager は、リソースが必要とする保護レベルとタイプの変化に対応できるよう 4 つの認証方式をサポートします。

XML ドキュメント認証情報コレクタ

ユーザ ディレクトリ内のフィールドにドキュメント内のフィールドをマップすることにより、メッセージ自体から収集された認証情報を使用して XML メッセージを検証します。

XML デジタル署名

有効な X.509 証明書でデジタル署名された XML ドキュメントを検証します。

WS-セキュリティ

受信メッセージの SOAP エンベロープ内の WS-Security ヘッダから収集された認証情報を使用して、XML メッセージを検証します。

eTrust SOA Security Manager は WS-Security トークンを作成および消費できます。そのため、WS-Security 認証方式を使用して連携サイトで複数の Web サービスの実装を展開できます。

SAML セッションチケット

メッセージの HTTP ヘッダ、SOAP エンベロープ、または Cookie に設定された eTrust SOA Security Manager 同期セッション SAML アサーション（暗号化された CA SiteMinder セッション チケットおよび CA SiteMinder ユーザ公開キーのセットを含む）から取得した認証情報を使用して、XML メッセージを検証します。

eTrust SOA Security Manager は SAML セッション チケット アサーションを生成および消費できます。 これによって、1 つのポリシー サーバ ドメイン内に複数の Web サービスの実装を展開するために SAML セッション チケット認証方式を使用できます。

推奨しているように、同じセキュリティ要件を共有する Web サービス操作を特定して、保護する Web サービスを特定したら、以下の質問を検討してください。

- 組織が特定のタイプのリソースに対して満たすべき認証ガイドライン、規制または法規がありますか。
- 情報の機密性と重要性はどの程度か

- どのようなタイプのユーザがこの情報にアクセスするか
- どのタイプのセキュリティをユーザが期待していますか。

これらのような質問の回答は、以下の点で役立ちます。

- 環境に必要な認証方法を特定します。
- 特定のリソースを保護するために SiteMinder 管理者が設定する必要がある認証方式を特定します。

  注: 認証方式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。

詳細情報:

保護する Web サービスの識別 (P. 94)

SiteMinder WSS エージェントの管理者の指定

SiteMinder WSS エージェント は起動時にポリシー サーバに接続します。ポリシー サーバには、関連付けられた SiteMinder WSS エージェント をその設定パラメータの場所に送るエージェント設定オブジェクト（ACO）が含まれます。

Web サービスが組織全体にどのように展開するかは、SiteMinder WSS エージェントの設定パラメータを格納する最も効率的な方法を決定するのに役立ちます。 以下の質問について考慮します。

1. ほとんどの Web サービスを同じセキュリティ要件で大規模なサーバ ファーム上に展開していますか。
2. ほとんどの Web サービスが一元化された担当者またはグループによって管理されていますか。
3. ほとんどの Web サービスが別々のセキュリティ要件で個別のサーバ上に展開していますか。
4. ほとんどの Web サービスが異なる部門または物理的に異なる場所の異なる担当者によって管理されていますか。

eTrust SOA Security Manager は以下のいずれかのメソッドを提供します。

中央設定

前のリストの質問 1 または 2 に「はい」と答えた場合、ポリシー サーバに存在するエージェント設定オブジェクト（ACO）から 1 つ以上の SiteMinder WSS エージェントが管理される中央設定を試します。 中央設定では、複数の SiteMinder WSS エージェント のパラメータ設定を一度に更新できます。通常、個々の Web サービスはそれぞれ個別の ACO を使用します。それらの設定は、Web サービスを保護するすべての SiteMinder WSS エージェントで共有されます。 たとえば、1 つの会計 Web サービスを保護する 5 つの SiteMinder WSS エージェントがある場合、その Web サービスの設定で 1 つの ACO を作成できます。5 つの SiteMinder WSS エージェントはすべて、同じ ACO のパラメータ設定を使用します。

別のアプリケーションについては、個別のエージェント設定オブジェクトを使用することをお勧めします。 たとえば、より厳密なセキュリティ要件を持つ人事 Web サービスを保護する場合は、その人事 Web サービス用に別の ACO を作成します。

SiteMinder WSS エージェントが開始すると、関連付けられた ACO の AllowLocalConfig パラメータの値を読み取ります。 値が no に設定されている場合、SiteMinder WSS エージェントは ACO のパラメータ設定を使用します。

注: エージェント設定およびメンテナンスが簡略化されるので、（可能な限り）中央エージェント設定を使用することを推奨します。

ローカル設定

前のリストの質問 3 または 4 に「はい」と答えた場合は、各 SiteMinder WSS エージェントがサーバ自体にインストールされたファイルを使用して個別に管理されるローカル設定を試します。 SiteMinder WSS エージェント が起動すると、関連付けられたエージェント設定オブジェクト（ACO）の AllowLocalConfig パラメータの値を読み取ります。値が yes に設定されている場合、SiteMinder WSS エージェント はアプリケーションまたは Web サーバ上の LocalConfig.conf ファイルのパラメータ設定を使用します。 ローカル ファイル内のパラメータ設定は、ポリシー サーバのエージェント設定オブジェクトに格納されているすべての設定に優先します。上記のリストの 3 つまたは 4 つの質問にはいと答えた場合は、以下の設定方法を試してください。

注: アプリケーションまたは Web サーバ上の LocalConfig.conf ファイルの場所の詳細については、対応する SiteMinder WSS エージェント ガイドを参照してください。

ニーズに合わせて中央設定およびローカル設定の組み合わせを使用することもできます。 たとえば、中央設定で 3 つの類似した Web サーバを管理しながら、ローカル設定で別の 2 つのサーバを管理できます。

以下の質問は、ローカル エージェント設定で企業のニーズをより満たすことができる別の状況の特定に役立ちます。

- XML ゲートウェにカスタム SiteMinder WSS エージェントを展開しますか。

  たとえば、少数の場所に XML ゲートウェイを実装しているとしても、SiteMinder WSS エージェントの大規模なグループを持つ内部リソースを保護する必要があります。 XML ゲートウェイ上のカスタム SiteMinder WSS エージェント を管理するためにローカル設定を使用できます。

- ローカル サーバ管理者が一部の SiteMinder WSS エージェント 設定のみを変更することを許可しますか。

  たとえば、組織は SiteMinder を使用してセキュリティ ポリシーを管理および適用しますが、リモート オフィスのアプリケーションおよび Web サーバ管理者にログオンおよびログオフ ページのカスタマイズを許可します。 ACO の AllowLocalConfig パラメータの値に個別のパラメータを追加して、カスタマイズされたページのそれらの設定のみ変更することを管理者にのみ許可できます。

データ センターの特定

後ほど説明する複数の要因が、複数のデータ センターにわたる SiteMinder コンポーネントの実装を決定する方法に影響を及ぼす場合があります。 SiteMinder 環境に合うデータ センターおよび目的をそれぞれ特定することによって、SiteMinder コンポーネントの実装方法を判断するときに情報に基づく決定を行えます。 以下の質問について考慮します。

- 展開にはどれだけのデータ センターが含まれ、各センターはどこにありますか。
- 複数のデータ センターがある場合
  - それらのすべてがアクティブですか、または一部はディザスタ リカバリまたはバックアップ専用ですか。
  - 保護されている各アプリケーションは単一のデータ センターに存在しますか、または複数のセンターにわたって存在しますか。

- フェールオーバをデータ センター レベルで設定しますか、またはデータ センターにわたって設定しますか。
- データ センター間の帯域幅およびスループットはどれくらいですか。

各データ センターに関する情報を収集するときは、以下のようなリソースの表を使用して結果を整理します。

データ センター名	場所	目的

詳細情報:

複数のデータ センター (P. 136)

Advanced Encryption Standard が必要かどうか判断する

組織は、Federal Information Processing Standard （FIPS） 140-2 準拠のアルゴリズムを使用する必要がありますか。

Advanced Encryption Standard （AES）の SiteMinder 実装は FIPS 140-2 標準をサポートしています。 FIPS とは、AES に適合する暗号モジュールの認定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。

ポリシー サーバは、FIPS 140-2 準拠の認証された暗号ライブラリを使用します。 これらの暗号ライブラリにより、SiteMinder 環境で AES 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 専用

注: SiteMinder が使用する暗号ライブラリ、および FIPS 専用モードで機密データを暗号化するために使用される AES アルゴリズムの詳細については、「ポリシー サーバ管理ガイド」を参照してください。FIPS の動作モードおよびポリシー サーバのインストール時にどちらを使用するかの詳細については、「*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。

FIPS 専用モードによって AES 暗号化を実装する場合は、以下の点について考慮してください。

- ディレクトリ サーバ、データベース、およびドライバを含むすべてのサードパーティ コンポーネントを FIPS 準拠のアルゴリズムをサポートするように設定する必要があります。

  注: FIPS 140-2 標準をサポートするベンダー機能の詳細については、ベンダー固有のマニュアルを参照してください。

- X.509 クライアント証明書認証方式が使用される環境の場合は、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てください。

- ポリシー サーバが SSL を使用してポリシー ストアまたはユーザ ストアに接続する場合は、ポリシー サーバおよびディレクトリ ストアが FIPS 準拠の証明書を使用することを確認してください。

- SiteMinder 12.x 付属のすべての SiteMinder WSS エージェントは FIPS 準拠です。他のエージェントが FIPS 準拠であるかどうかを判断するには、エージェント固有のマニュアルを参照してください。

重要: FIPS 専用モードで実行されている環境は、以前のバージョンの SiteMinder で動作することはできず、上位互換性はありません。この要件には、すべてのエージェントおよび以前のバージョンの eTrust SOA Security Manager SDK を使用するカスタム ソフトウェアが含まれます。そのようなソフトウェアをすべて SDK の現行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。

仮想化が使用されるかどうかの判断

SiteMinder は仮想環境に実装されますか。

仮想環境に SiteMinder を実装する前に、以下の点について考慮してください。

- 仮想化上の CA ポリシーを確認してください。
- 以下を確認してください。
  - 仮想環境、およびホスト システムがアプリケーションに課すことができるパフォーマンス オーバーヘッドを把握します。
  - 仮想環境を調整して、可能な限りパフォーマンスのオーバーヘッドを除去します。

    注: 仮想環境のパフォーマンス チューニングの詳細については、各ベンダーのドキュメントを参照してください。
- CPU、ディスク領域およびメモリが仮想環境で使用できるサイズであることを確認してください。各 SiteMinder インストール ガイドに詳述されているシステム要件を使用して、システム全体に展開するコンポーネント数を決定します。
- クロック同期および複数のオペレーティング システムに関する問題に注意してください。 非同期のクロックによって予期しない SiteMinder 動作が生じる場合があります。
- コンポーネントを展開する場所について検討する場合については以下のとおりです。
  - 仮想環境にポリシー サーバを展開することをお勧めします。 ポリシー サーバに自身のイーサネット ポートがあることをお勧めします。 専用ポートは、使用できる帯域幅の他の仮想ホストとの競合によって、SiteMinder がリクエストを失わないようにします。
  - 仮想化された Web サーバに Web エージェントを展開することをお勧めします。
  - すべての SiteMinder データ ストアを物理ハードウェアおよびオペレーティング システムに展開することをお勧めします。 ディレクトリ サーバおよびデータベースは、リソースにかなり依存する場合があります。 仮想化された環境に展開した場合、この依存性によりパフォーマンスが低下する可能性があります。

ポリシー サーバの管理方法の決定

個々の業務部門がポリシー サーバを管理する必要がありますか。または、すべてのポリシー サーバを単一の業務部門で集中的に管理できますか。

ローカル ポリシー サーバ管理

個々の業務部門がポリシー サーバおよびポリシー ストアをローカルに管理する場合は、ローカル ポリシー サーバ管理について以下の点を考慮してください。

- 各業務部門は、個別のニーズに基づいてセキュリティ要件を管理できます。
- SiteMinder インフラストラクチャの複雑さが増大する可能性があります。ローカル ポリシー サーバ管理によって、管理およびアップグレードが必要なポリシー サーバおよびポリシー ストアが増加する場合があります。
- SiteMinder 管理者が異なる業務部門に存在するため、SiteMinder コア オブジェクト、ポリシー、およびアプリケーション オブジェクトの一貫した実装および管理がより難しくなる場合があります。

中央ポリシー サーバ管理

1 つの業務部門がポリシー サーバを一元的に管理する場合は、中央ポリシー サーバ管理について以下の点を考慮してください。

- すべての SiteMinder 管理者が同じ業務部門に存在するので、SiteMinder コア オブジェクト、ポリシー、およびアプリケーション オブジェクトの一貫した実装が容易になる場合があります。
- すべての SiteMinder 管理者が同じ業務部門に存在するので、これらのオブジェクトの管理が容易になる場合があります。

  注: 示されているように、個々の業務部門はアプリケーションを保護している SiteMinder エージェントの管理を続行できます。
- SiteMinder インフラストラクチャを簡略化する場合があります。 集中管理によって、管理およびアップグレードが必要なポリシー サーバおよびポリシー ストアを減らすことができます。
- 管理者は SiteMinder のパフォーマンスを一元的に監視できます。

SiteMinder WSS エージェント の管理方法の決定

同じように設定される複数の SiteMinder WSS エージェントがある場合、ポリシー サーバ上でエージェント設定オブジェクトを使用することによって、エージェントの管理がより容易になります。 1 つのエージェント設定オブジェクトを共有できる SiteMinder WSS エージェントの数に制限はありません。 ポリシー サーバ上で行われた設定変更は、設定オブジェクトを使用するすべての SiteMinder WSS エージェント に自動的に適用されます。

注: エージェント関連のオブジェクトを設定する方法に関する詳細については、「*eTrust SOA Security Manager ポリシー設定ガイド*」および SiteMinder WSS エージェントの種類の SiteMinder WSS エージェント ガイドを参照してください。

第 5 章: SiteMinder 容量計画

このセクションには、以下のトピックが含まれています。

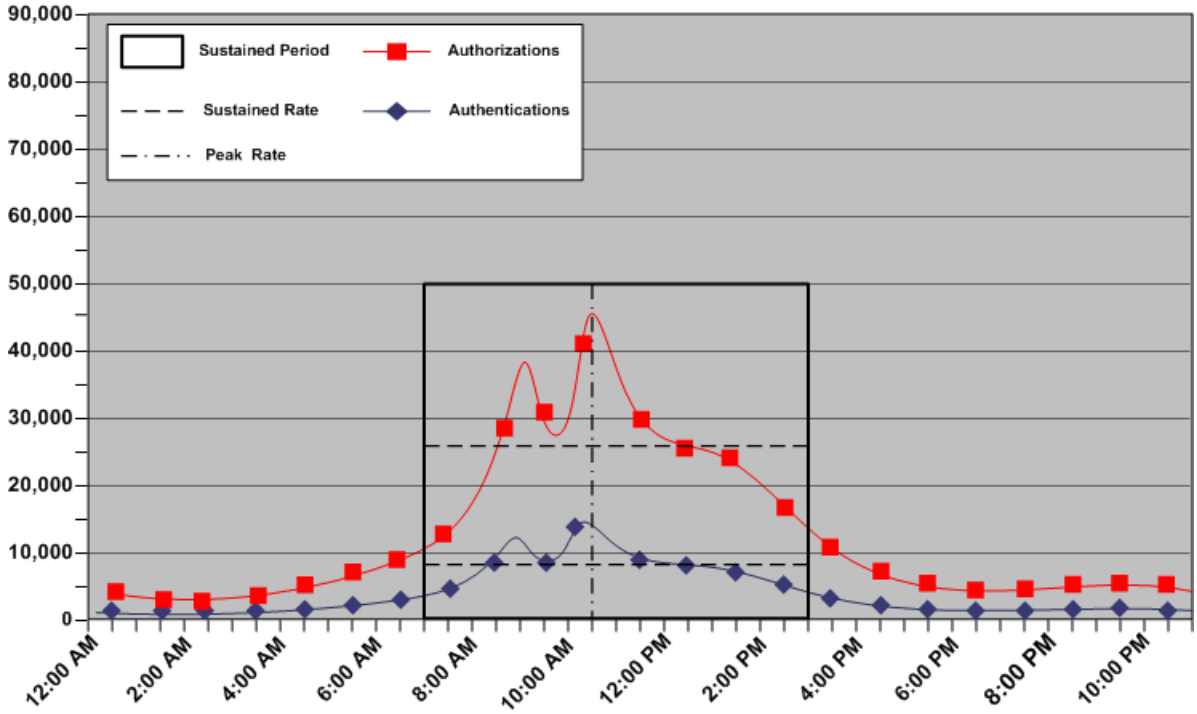
容量計画が導入されました

パフォーマンスを考慮した SiteMinder 展開の計画は、高い企業可用性および性能基準を維持するための第一歩です。SiteMinder が アプリケーションごとに処理する必要がある認証および許可の予測数を概算することをお勧めします。以下の一般的な要因が SiteMinder のパフォーマンスに影響します。

- 持続認証レートおよび許可レート。ユーザがアプリケーションに認証し、保護されているリソースをリクエストするレートは、営業日の全体にわたって変動します。期間によっては比較的少数の認証リクエスト、およびそれに伴って比較的少数の許可リクエストが生成される場合がありますが、一方で他の期間ではより多くのリクエストが生成されます。 持続認証レートおよび許可レートは、SiteMinder が平均数の認証および許可リクエストを処理する必要がある持続期間を表します。
- ピーク認証レートおよび許可レート。アクティビティの持続期間中に、ユーザ アクティビティが急増する場合があります。ピーク認証レートおよび許可レートは、SiteMinder が最も多くの認証および許可リクエストを処理する必要がある期間を表します。

  注: 他の複数の要因が、パフォーマンス 調整およびネットワーク帯域幅などの SiteMinder のパフォーマンスに影響を及ぼす場合がありますが、前述の要因はポリシー サーバおよびエージェントを実装するとき、および既存ユーザ ストアが予期される SiteMinder の作業負荷を処理できるかどうかを判断するときに、情報に基づく決定を行うために役立ちます。

以下の図では、認証および許可のレートの、1 日を通した変動、特定の期間の保持、その期間内のピークを示します。



注: ユーザの認証および許可によって、ユーザ ストアに対する複数の読み取りが生じ、パスワード ポリシーが有効な場合は、ユーザ ストアへの書き込みが必要になります。持続レートおよびピーク レートの特定は、ユーザ ストアがポリシー サーバ リクエストの処理のために動作する必要があるロードの決定に役立ちます。

詳細情報:

導入されたパフォーマンス調整 (P. 157)

ユース ケース: 容量計画

以下のユース ケースの目的は、架空の組織がアプリケーションの使用状況をモデル化することにより、容量計画に取り組む方法を示すことです。このユース ケースは例として本章の全体にわたって参照されます。

会社は SiteMinder の展開を計画しています。 会社には 1 つのユーザ ストア内に 100,000 のユーザがいます。パスワード サービスはこのストアに対して有効です。

ポータル アプリケーションに 1 日に 1 回ログインするユーザもいれば、1 日に 3 回もログインするユーザもいます。

持続認証レートの概算方法

アプリケーションの持続認証レートの概算は、以下のことを決定するプロセスです。

- 認証リクエストの総数は営業日全体でどのように変動するか。
- 認証リクエストは毎秒どのようにリクエストに変換されるか。

アプリケーションの持続認証レートを概算するには、以下の手順に従います。

1. 日単位の認証を概算します。
2. 持続認証レートを概算します。

日単位の認証の概算

アプリケーションの日単位の認証の概算数はいくつですか。

ユーザ数は日単位の認証（認証ロード）に直接影響します。 ユーザはアプリケーションにログインするときに SiteMinder によって認証されます。従って、アプリケーションの認証ロードは 1 日あたりの総ログイン数であると考えてください。

注: 認証ロードの特定時には、24 時間間隔の評価から始めることをお勧めします。 ただし、企業の要件に応じて、数週間または数か月の期間にわたって日単位の結果を比較し、年間を通じた使用状況を詳細に把握できます。

すべてのユーザが毎日アプリケーションにログインするとは考えにくいので、総ログイン数の概算は、以下に示すように 1 日に 1 回ログインするユーザの割合の特定から始まります。

(*total_users* * *percentage_users*) * (*number_of_logins*) = *daily_logins*

total_users

アプリケーションへのアクセス権を持つユーザの総数を表します。

percentage_users

1 日あたりのログイン回数が同じユーザの割合を表します。

number_of_logins

特定のユーザ集団がログインする回数を表します。

daily_logins

特定のユーザ集団が作成するログイン数を表します。

例 1： 会社には 100,000 人のユーザがいて、その内の 75 パーセントが 1 日に 1 回ログインします。

（100,000 * 0.75） x （1） = 75,000 ログイン

ただし、一部のユーザは 1 日に複数回アプリケーションにログインする可能性があります。

例 2： 会社には 100,000 人のユーザがいて、その内の 5 パーセントが 1 日に 2 回ログインし、1 パーセントが 1 日に 3 回ログインします。

（100,000 * 0.05） x （2） = 10,000 ログイン

（100,000 * 0.01） x （3） = 3,000 ログイン

1 日の総ログイン数は各ログイン計算の合計です。

例 3： 会社には 100,000 人のユーザがいて、割合は以下のとおりです。

- 75 パーセントが 1 日に 1 回ログインするので、75,000 ログインです。
- 5 パーセントが 1 日に 2 回ログインするので、10,000 ログインです。
- 1 パーセントが 1 日に 3 回ログインするので、3,000 ログインです。

ポータル アプリケーションの認証ロードは 88,000 ログインです。

注: すべてのユーザが毎日アプリケーションにログインするとは限らないので、ログインするユーザの割合が 100 パーセントである必要はありません。

以下の表は、前述の各例を示しています。

ユーザ総数	ユーザ総数の割合	1 日当たりログイン数	ログイン数
100,000	75	1	75,000
100,000	5	2	10,000
100,000	1	3	3,000
認証ロード			**88,0000**

会社は、認証ロードを使用して持続認証レートを概算します。

持続認証レートの概算

アプリケーションの持続認証レートはどれくらいですか。

持続認証レートは認証ロードに基づきます。特に、いつ、どのようなレートで認証が発生するかを示します。 認証ロードが営業日中に均一に分散される可能性はあまりありません。 さらに、リクエストが発生するレートは、持続期間の最低レベルと最高（ピーク）レベルの間で変動します。持続認証レートの概算は、システムが平均数の認証リクエストを処理する持続期間を特定するプロセスです。

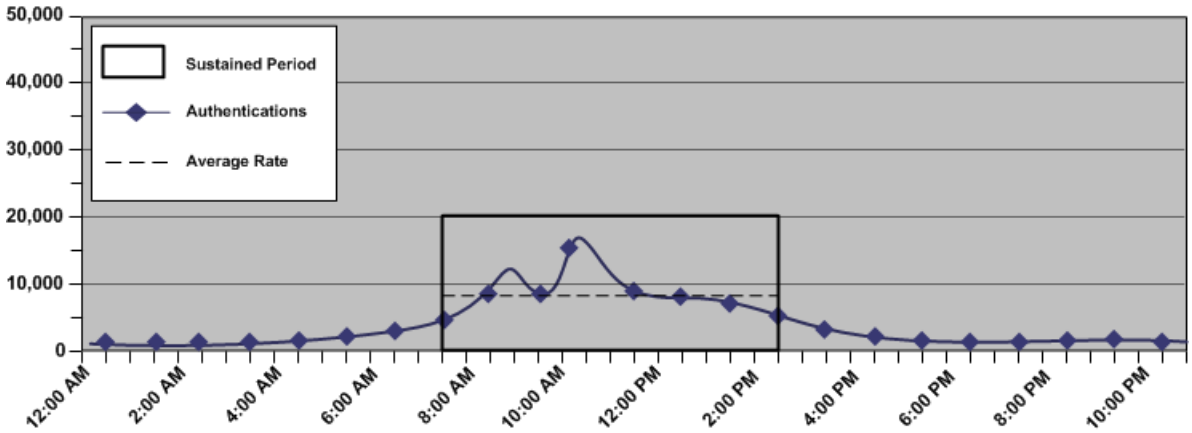
持続認証レートの概算時には、日単位の認証ロードを使用して以下を特定することをお勧めします。

- 営業日全体で認証リクエストが発生するレート。

  注: 1 時間のインクリメントに分割した 24 時間の評価期間で始めることをお勧めします。 ただし、企業の要件に応じて、数週間または数か月の期間にわたって日単位の結果を比較し、年間を通じた使用状況を詳細に把握できます。

- システムが平均数の認証リクエストを処理する持続期間。
- 持続期間に発生する認証リクエストの概数。

以下の図はこれらのメトリックの例です。



これらのメトリックの特定は、ユーザが認証する平均レートを維持するために SiteMinder が 1 秒あたりに処理する必要がある認証リクエスト数の概算に役立ちます。以下にこれを示します。

(*authentication_load* * *percentage_of_authentication_requests*) / *number_of_sustained_hours* / 3600 = *sustained_authentication_rate*

authentication_load

アプリケーションの日単位の認証数を表します。

percentage_of_authentication_requests

システムが持続レベルで動作しているときに発生する認証リクエストの割合を表します。

例： 認証ロードが 50,000 ログインで、持続期間に 32,000 ログインが発生する場合、この値は 64 パーセント（0.64）です。

number_of_sustained_hours

システムが持続レベルで動作する時間数を表します。

注: 3,600 は 1 時間の秒数を表します。

sustained_authentication_rate

SiteMinder が持続アクティビティの期間中に 1 秒あたりに処理する必要がある認証リクエスト数を表します。

例: 持続認証レートの概算

会社は、アプリケーション ポータルに 88,000 ログインの認証ロードがあることを特定しました。 顧客は、毎日 24 時間アプリケーション ポータルを使用できます。 システム アクティビティ レポートを使用して典型的な 1 日を分割すると、以下のメトリックになります。

- システムは、持続レベルで約 5 時間（午前 9:00 - 午後 2:00）動作します。
- 持続レベルの間、1 時間に約 9,000 の認証リクエストが発生します。
- 約 45,000 （9,000 * 5）の認証リクエストまたは日単位の認証ロードの 51 パーセント（45,000/88,000）がこの時間内に発生します。

（88,000 * 0.51）/5/3600 = 毎秒 2.49 認証。

ポータル アプリケーションには毎秒 2.49 認証の持続認証レートがあります。

ピーク認証レートの概算

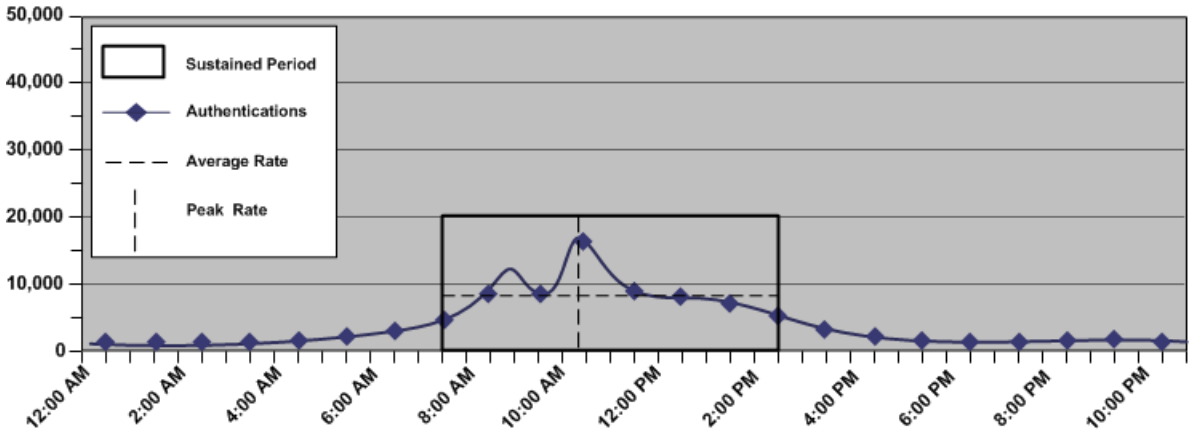
アプリケーションのピーク認証レートはどれくらいですか。

ピーク認証レートは、持続認証レート（特に、システムがピーク レベルで動作する時期およびレート）に基づきます。 ピーク認証レートの概算は、システムが認証リクエストの最高レベルを処理する時期を特定するプロセスです。

ピーク認証レートの概算時には、持続認証レートの特定時に得たメトリックを使用して以下を特定することをお勧めします。

- システムが最も多くの認証リクエストを処理する時間帯
- この期間に発生する認証リクエストの概数。

以下の図はこれらのメトリックの例です。



これらのメトリックの特定は、ユーザが認証するピーク レートを維持するために SiteMinder が 1 秒あたりに処理する必要がある認証リクエスト数の概算に役立ちます。以下にこれを示します。

(*authentication_load* x *percentage_of_transactions*) / *number_of_hours* / 3600 = *peak_authentication_rate*

注: このレートは最繁時の 1 時間に基づきます。ピーク認証レートが時間単位の計算を超える期間がある場合があります。

authentication_load

アプリケーションの日単位の認証数を表します。

percentage_of_transactions

システムがピーク レベルで動作しているときに発生するトランザクションの割合を表します。

number_of_hours

システムがピーク レベルで動作する時間数を表します。

注: 3,600 は 1 時間の秒数を表します。

peak_authentication_rate

アプリケーションのピーク認証レートを表します。

例: ピーク認証レートの概算

会社は、ポータル アプリケーションに 88,000 ログインの日単位の認証ロードがあることを特定しました。 システム アクティビティ レポートには、最繁時の 1 時間に 18,000 の認証リクエストが発生することが詳述されます。 この数は、認証ロードの約 20 パーセントに相当します。

18,000/1/3600 = 毎秒 5 認証

ポータル アプリケーションには毎秒 5 認証のピーク認証レートがあります。

注: この例は最繁時の 1 時間に基づきます。 この時間内のピーク認証レートが毎秒 5 認証を超える期間がある場合があります。

詳細情報:

エージェントに対して使用できるソケット量の増加 (P. 164)

持続許可レートの概算方法

アプリケーションの持続許可レートの概算は、以下のことを特定するプロセスです。

- 許可リクエストの総数は営業日全体でどのように変動するか。
- 許可リクエストは毎秒どのようにリクエストに変換されるか。

アプリケーションのピーク許可レートを概算するには、以下の手順に従います。

1. 日単位の許可を概算します。
2. 持続許可レートを概算します。

日単位の許可の概算

アプリケーションの日単位の許可の概算数はいくつですか。

認証された各ユーザによる総ログイン数（認証ロード）およびページの「ヒット」数は、日単位の許可数（許可ロード）に直接影響します。 通常、Web ページの「ヒット」には許可が必要です。 したがって、アプリケーションの許可ロードは 1 日あたりの総許可数であると考えてください。

注: 許可ロードの概算時には、24 時間間隔の評価から始めることをお勧めします。 ただし、企業の要件に応じて、数週間または数か月の期間にわたって日単位の結果を比較して、年間を通じた使用状況を詳細に把握できます。

すべてのユーザが 1 回のログインで同数のページをリクエストするとは考えにくいので、総許可数の計算は、以下に示すように 1 件のページ ヒットを発生させるログインの割合の特定から始めます。

*authentication_load * percentage_of_authenticated_users * page_visits = daily_authorizations*

authentication_load

アプリケーションの日単位の認証の概算数を表します。

percent_of_authenticated_users

ログイン後に同数のページにアクセスする認証されたユーザの割合を表します。

page_visits

特定の認証されたユーザ集団がログイン後にアクセスするページ数を表します。

注: ページには複数のオブジェクトが含まれるので、複数の GET/POST が生じる場合があります。 1 ページあたりの総許可数は、GET リクエストの数に POST リクエストの数を加えて、Web エージェントが無視する拡張子の数を引いた数です。本書では、以下の各例で、1 回のページ アクセスにつき 1 つの GET/POST が生成されることを前提としています。ポリシーを確認せずに特定のリソース タイプへのアクセスを許可するように Web エージェントを設定する詳細については、「Web エージェント設定ガイド」を参照してください。

daily_authorizations

特定の認証されたユーザ集団が必要とする許可数を表します。

例 1: 日単位の許可の概算

「日単位の認証の概算 (P. 109)」で詳述したとおり、ポータル アプリケーションには 88,000 ログインの認証ロードがあります。その内の 25 パーセントがログイン後に 1 つのページにアクセスします。

88,000 * 0.25 * 1 = 22,000 許可

ただし、ログインによっては複数のページ ヒットが発生する可能性がありそうです。

例 2: 日単位の許可の概算

ポータル アプリケーションには 88,000 ログインの認証ロードがあり、割合は以下のとおりです。

- 50 パーセントがログイン後に 10 ページにアクセスします。
- 25 パーセントがログイン後に 15 ページにアクセスします。

88,000 * 0.5 * 10 = 440,000 許可

88,000 * 0.25 * 15 = 330,000 許可

1 日あたりの総許可数（許可ロード）は許可の各計算の合計です。

例 3: 日単位の許可の概算

ポータル アプリケーションには 88,000 ログインの認証ロードがあり、割合は以下のとおりです。

- 25 パーセントがログイン後に 1 件のページ ヒットを発生させるので、22,000 許可です。
- 50 パーセントがログイン後に 10 件のページ ヒットを発生させるので、440,000 許可です。
- 25 パーセントがログイン後に 15 件のページ ヒットを発生させるので、330,000 許可です。

注: 認証された各ユーザが少なくとも 1 件のページ ヒットを発生させるので、認証されたユーザの割合は 100 パーセントになる必要があります。

したがって、ポータル アプリケーションの許可ロードは 792,000 です。

以下の表は、前述の各例を示しています。

ページのヒット数	総ログイン数の割合	認証ロード	許可
1	25	88,000	22,000
10	50	88,000	440,000
15	25	88,000	330,000
許可ロード			**792,000**

会社は、許可ロードを使用して持続許可レートを概算します。

持続許可レートの概算

アプリケーションの持続許可レートはどれくらいですか。

持続許可レートは、許可ロード（特に、許可が発生する時期およびレート）に基づきます。 許可ロードが営業日中に均一に分散される可能性はあまりありません。 さらに、リクエストが発生するレートは、持続期間の最低レベルと最高（ピーク）レベルの間で変動します。 持続許可レートの概算は、システムが平均数の許可リクエストを処理する持続期間を特定するプロセスです。

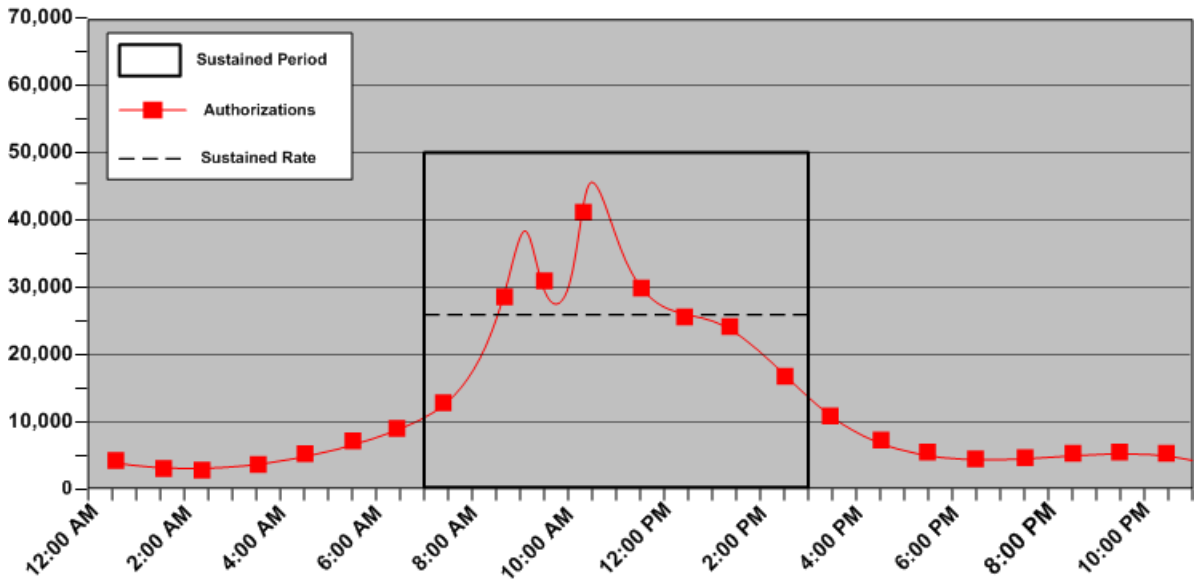
持続許可レートの概算時には、日単位の許可ロードを使用して以下を特定することをお勧めします。

- 営業日全体で許可リクエストが発生するレート。

  注: 1 時間のインクリメントに分割した 24 時間の評価期間で始めることをお勧めします。 ただし、企業の要件に応じて、数週間または数か月の期間にわたって日単位の結果を比較し、年間を通じた使用状況を詳細に把握できます。

- システムが平均数の許可リクエストを処理する持続期間。
- 持続期間に発生する許可リクエストの概数。

以下の図はこれらのメトリックの例です。



これらのメトリックの特定は、許可リクエストが発生する平均レートを維持するために SiteMinder が 1 秒あたりに処理する必要がある許可リクエスト数の概算に役立ちます。以下にこれを示します。

(*authorization_load* * *percentage_of_authorization_requests*) / *number_sustained_hours* / 3600 = *sustained_authorization_rate*

authorization_load

アプリケーションの日単位の許可数を表します。

percentage_of_authorization_requests

システムが持続レベルで動作しているときに発生する許可リクエストの割合を表します。

例： 許可ロードが 500,000 リクエストで、持続期間に 320,000 リクエストが発生する場合、この値は 64 パーセント（0.64）です。

number_of_sustained_hours

システムが持続レベルで動作する時間数を表します。

注: 3,600 は 1 時間の秒数を表します。

sustained_authentication_rate

SiteMinder が持続アクティビティの期間中に 1 秒あたりに処理する必要がある許可リクエスト数を表します。

例: 持続許可レートの概算

「日単位の許可の概算 (P. 116)」で詳述したとおり、ポータル アプリケーションには 792,000 の許可ロードがあります。 顧客は、毎日 24 時間アプリケーション ポータルを使用できます。システム アクティビティ レポートを使用して典型的な 1 日を分割すると、以下のメトリックになります。

- システムは、持続レベルで約 5 時間（午前 9:00 ～午後 2:00）動作します。
- 持続レベルの間、1 時間に約 75,000 の許可リクエストが発生します。
- 約 375,000 （75,000 * 5）の許可リクエストまたは日単位の認証ロードの 47 パーセント（375,000/792,000）がこの時間内に発生します。

（762,000 * 0.47）/5/3600 = 毎秒 19.90 許可

ポータル アプリケーションには毎秒 19.90 許可の持続許可レートがあります。

ピーク許可レートの概算

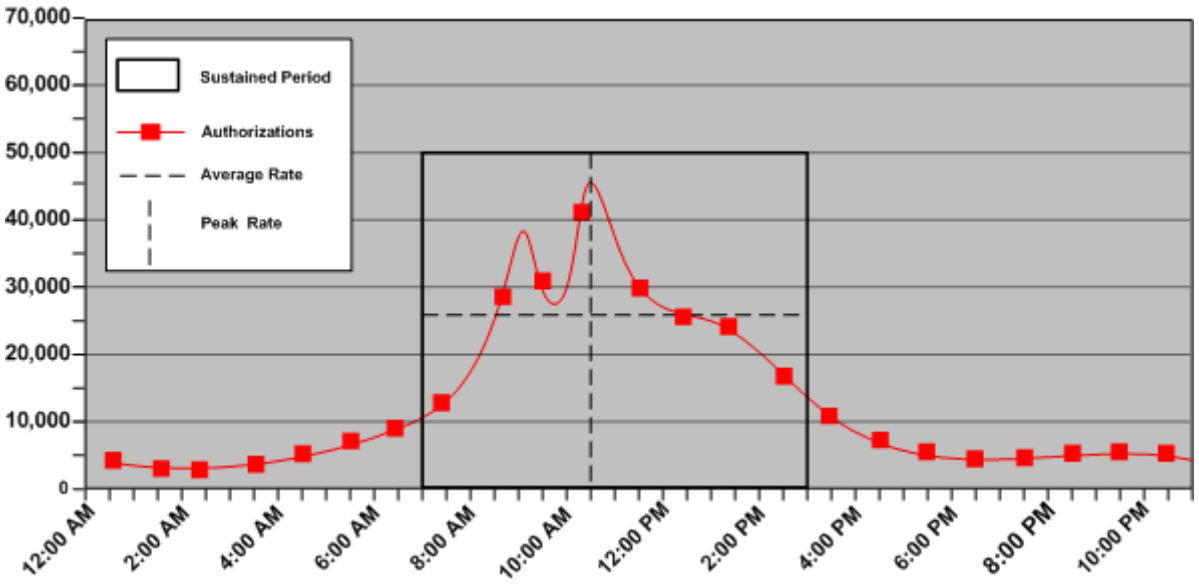
アプリケーションのピーク認証レートはどれくらいですか。

ピーク許可レートは、持続許可レート（特に、システムがピーク レベルで動作する時期およびレート）に基づきます。 ピーク許可レートの概算は、システムが許可リクエストの最高レベルを処理する時期を特定するプロセスです。

ピーク許可レートの概算時には、持続許可レートの特定時に得たメトリックを使用して以下を特定することをお勧めします。

- システムが最も多くの許可リクエストを処理する時間帯
- この期間に発生する許可リクエストの概数。

以下の図はこれらのメトリックの例です。



これらのメトリックの特定は、ユーザが認証するピーク レートを維持するために SiteMinder が 1 秒あたりに処理する必要がある認証リクエスト数の概算に役立ちます。以下にこれを示します。

(*authorization_load* * *percentage_of_transactions*) / *number_of_hours* / 3600 = *peak_authorization_rate*

注: このレートは最繁時の 1 時間に基づきます。 ピーク許可レートが時間単位の計算を超える期間がある場合があります。

authorization_load

アプリケーションの日単位の許可数を表します。

percentage_of_transactions

システムがピーク レベルで動作しているときに発生するトランザクションの割合を表します。

number_of_hours

システムがピーク レベルで動作している時間数を表します。

peak_authorization_rate

アプリケーションのピーク許可レートを表します。

例: ピーク許可レートの概算

「日単位の許可の概算 (P. 116)」で詳述したとおり、ポータル アプリケーションには 792,000 の許可ロードがあります。 システム アクティビティ レポートには、最繁時の 1 時間に 260,000 の許可リクエストが発生することが詳述されます。 この数は、許可ロードの約 33 パーセントに相当します。

（792,000 * 0.33）/1/3600 = 毎秒 72.6 許可

ポータル アプリケーションには毎秒 72.6 許可のピーク認証レートがあります。

第 6 章: eTrust SOA Security Manager 容量計画

このセクションには、以下のトピックが含まれています。

導入された eTrust SOA Security Manager 容量計画

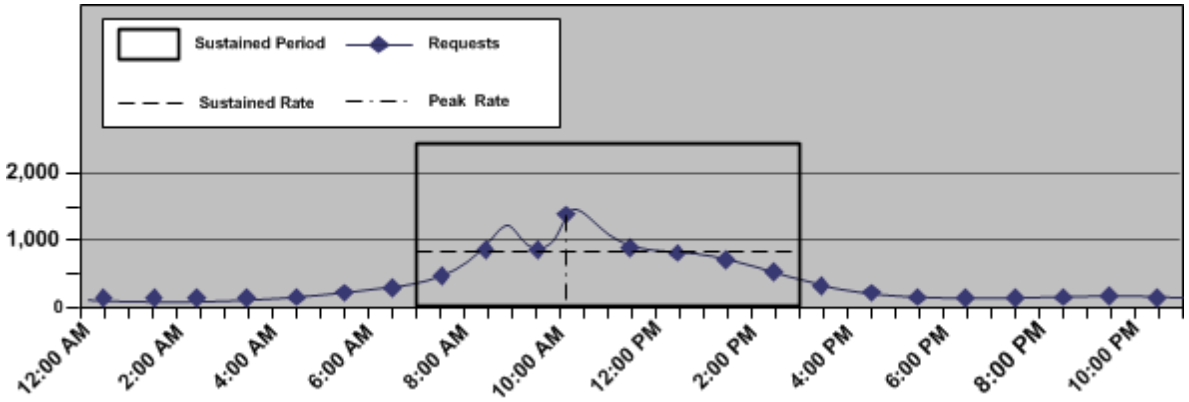
パフォーマンスを考慮した eTrust SOA Security Manager 展開の計画は、高い企業可用性および性能基準を維持するための第一歩です。SiteMinder が Web サービスごとに処理する必要があるリクエストの予測数を概算することをお勧めします。以下は、SiteMinder のパフォーマンスに影響する最も重要な要因です。

- 持続リクエスト レート。 Web サービス クライアントが保護されている Web サービス リソースにリクエストを送信するレートは、営業日の全体にわたって変動します。期間によっては比較的少数のリクエストが生成され、それに伴って比較的少数の認証と許可が必要な場合がありますが、一方で他の期間ではより多くのリクエストが生成されます。 持続リクエスト レートは、SiteMinder が平均数の認証および許可リクエストを処理する必要がある持続期間を表します。

  注: 各 Web サービス リクエストは、1 つの認証イベントと 1 つの許可イベントをトリガします。

- ピーク リクエスト レート。アクティビティの持続期間中に、Web サービス クライアント アクティビティが急増する場合があります。 ピーク リクエスト レートは、SiteMinder が最も多くの認証および許可リクエストを処理する必要がある期間を表します。

以下の図では、リクエストのレートの、1 日を通した変動、特定の期間の保持、その期間内のピークを示します。



注: リクエストの認証および許可によって、ユーザ ストアからの読み取りが多数発生します。 持続レートおよびピーク レートの特定は、ユーザ ストアがポリシー サーバ リクエストの処理のために動作する必要があるロードの決定に役立ちます。

詳細情報:

導入されたパフォーマンス調整 (P. 157)

ユース ケース: 容量計画

以下のユース ケースの目的は、処理サービス組織である example.com が注文処理 Web サービスの使用状況をモデル化することにより、容量計画に取り組む方法を示すことです。 このユース ケースは例として本章の全体にわたって参照されます。

会社は、Web サービスを保護するために eTrust SOA Security Manager を展開することを計画しています。 会社には 1 つのユーザ ストア内に 10,000 のユーザがいます。

一部の Web サービス クライアントは、Web サービスのインベントリ操作に単一のステータス リクエストを 1 日に 1 回送信します。その一方で、ほかの Web サービス クライアントは、処理操作に 1 日あたり 4 つのバッチ化された要求リクエストを送信している場合があります。

持続リクエスト レートの概算方法

Web サービスの持続リクエスト レートの概算は、以下のことを特定するプロセスです。

- リクエストの総数は営業日全体でどのように変動するか。
- リクエストは、どのように秒単位のリクエストに変換されるか。

Web サービスの持続リクエスト レートを概算するには、以下の手順に従います。

1. 日単位リクエストの概算
2. 持続リクエスト レートの概算

日単位リクエストの概算

Web サービスの日単位のリクエストの概算数はいくつですか。

Web サービス クライアントの数は日単位のリクエスト（リクエスト ロード）に直接影響します。 Web サービス クライアントが Web サービスにリクエストを送信すると、SiteMinder がそれらを認証します。 したがって、Web サービスのリクエスト ロードは 1 日あたりの総リクエスト数であると考えてください。

注: リクエスト ロードの特定時には、24 時間間隔の評価から始めることをお勧めします。 ただし、企業の要件に応じて、数週間または数か月の期間にわたって日単位の結果を比較し、年間を通じた使用状況を詳細に把握できます。

すべての Web サービス クライアントが毎日 Web サービスにリクエストを送信するとは考えにくいので、総リクエスト数の概算は、以下に示すようにリクエストを 1 日に 1 回送信する Web サービス クライアントの割合の特定から始まります。

(*total_clients* * *percentage_clients*) * (*number_of_requests*) = *daily_logins*

total_clients

アプリケーションへのアクセス権を持つクライアントの総数を表します。

percentage_clients

1 日あたりのリクエスト送信回数が同じクライアントの割合を表します。

number_of_requests

特定のクライアント集団がリクエストを送信する回数を表します。

daily_logins

特定のクライアント集団が作成するログイン数を表します。

例

会社には 10,000 人のユーザがいて、その内の 60 パーセントが 1 日に 1 回インベントリ ステータス リクエストを送信します。

（10,000 * 0.6） x （1） = 6,000 ログイン

さらに、30 パーセントのユーザは 1 日当たり 1 つの注文処理要求を送信し、20 パーセントのユーザは 1 日当たり 2 つの注文処理要求を送信し、10 パーセントは 1 日に 3 つの注文処理要求を送信し、10 パーセントは 1 日に 4 つの注文処理要求を送信します。

（10,000 * 0.3） x （1） = 3,000 ログイン

（10,000 * 0.2） x （2） = 4,000 ログイン

（10,000 * 0.1） x （3） = 3,000 ログイン

（10,000 * 0.1） x （4） = 4,000 ログイン

1 日あたりの総リクエスト数はリクエストの各計算の合計です。したがって、処理 Web サービスのリクエスト ロードは 20,000 ログインです。

注: すべてのクライアントが毎日、サービスに必ずリクエストを送信するとは限らないので、リクエストを行うクライアントの割合が 100 パーセントである必要はありません。

会社は、リクエスト ロードを使用して持続リクエスト レートを概算します。

持続リクエスト レートの概算

Web サービスの持続リクエスト レートはどれくらいですか。

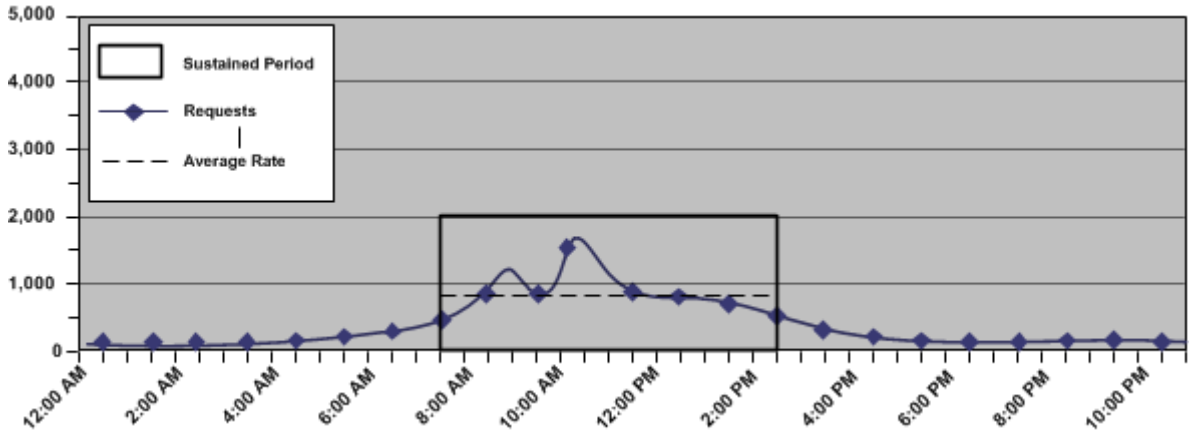
持続リクエスト レートはリクエスト ロードに基づきます。 特に、いつ、どのようなレートでリクエストが発生するかを示します。 リクエスト ロードが営業日中に均一に分散される可能性はあまりありません。 さらに、リクエストが発生するレートは、持続期間の最低レベルと最高（ピーク）レベルの間で変動します。 持続リクエスト レートの概算は、システムが平均数のリクエストを処理する持続期間を特定するプロセスです。

持続リクエスト レートの概算時には、日単位のリクエスト ロードを使用して以下を特定することをお勧めします。

- 営業日全体でリクエストが発生するレート。

  注: 1 時間のインクリメントに分割した 24 時間の評価期間で始めることをお勧めします。 ただし、企業の要件に応じて、数週間または数か月の期間にわたって日単位の結果を比較し、年間を通じた使用状況を詳細に把握できます。
- システムが平均数のリクエストを処理する持続期間。
- 持続期間中に発生するリクエストの概数です。

以下の図はこれらのメトリックの例です。



これらのメトリックの特定は、ユーザが認証する平均レートを維持するために SiteMinder が 1 秒あたりに処理する必要があるリクエスト数の概算に役立ちます。以下にこれを示します。

(*request_load* * *percentage_of_requests*) / *number_of_sustained_hours* / 3600 = *sustained_request_rate*

request_load

アプリケーションの日単位のリクエスト数を表します。

percentage_of_requests

システムが持続レベルで動作しているときに発生するリクエストの割合を表します。

例： リクエスト ロードが 5,000 ログインで、持続期間に 3,000 ログインが発生する場合、この値は 64 パーセント（0.64）です。

number_of_sustained_hours

システムが持続レベルで動作する時間数を表します。

注: 3,600 は 1 時間の秒数を表します。

sustained_request_rate

SiteMinder が持続アクティビティの期間中に 1 秒あたりに処理する必要があるリクエスト数を表します。

例: 持続リクエスト レートの概算

会社は、Web サービスに 2,000 ログインのリクエスト ロードがあることを特定しました。 顧客は、毎日 24 時間 Web サービスを使用できます。 システム アクティビティ レポートを使用して典型的な 1 日を分割すると、以下のメトリックになります。

- システムは、持続レベルで約 5 時間（午前 9:00 - 午後 2:00）動作します。
- 持続レベルの間、1 時間に約 2,500 のリクエストが発生します。
- 約 1,250 （250 * 5）のリクエストまたは日単位のリクエスト ロードの 62.5 パーセント（1,250/2,000）がこの時間内に発生します。

（2,000 * 0.625）/5/3600 = 0.0694 リクエスト/秒。

処理 Web サービスには、毎秒 0.694 リクエストの持続リクエスト レートがあります。

ピーク リクエスト レートの概算

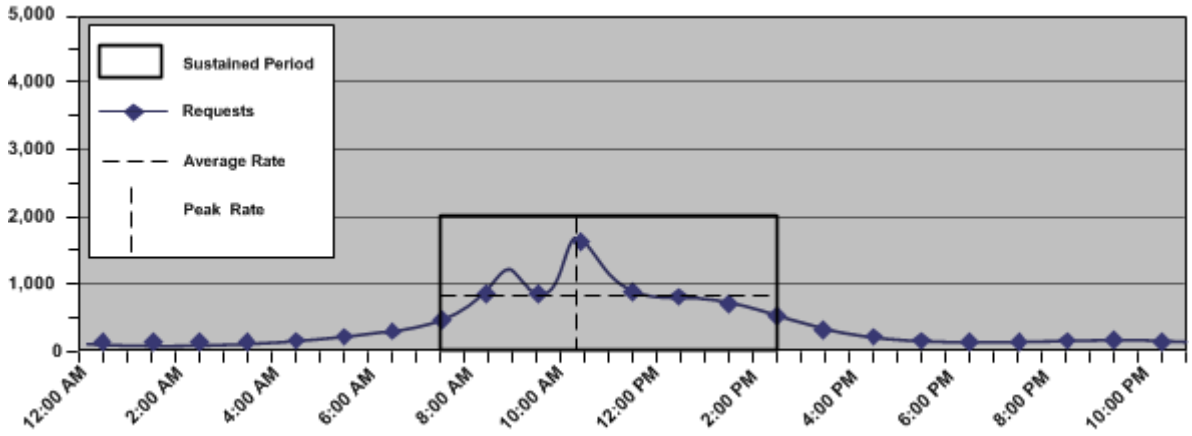
Web サービスのピーク リクエスト レートはどれくらいですか。

ピーク リクエスト レートは、持続リクエスト レート（特に、システムがピーク レベルで動作する時期およびレート）に基づきます。 ピーク リクエスト レートの概算は、システムがリクエストの最高レベルを処理する時期を特定するプロセスです。

ピーク リクエスト レートの概算時には、持続リクエスト レートの特定時に得たメトリックを使用して以下を特定することをお勧めします。

- システムが最も多くのリクエストを処理する時間帯
- この期間に発生するリクエストの概数。

以下の図はこれらのメトリックの例です。



これらのメトリックの特定は、Web サービス クライアントが認証するピーク レートを維持するために SiteMinder が 1 秒あたりに処理する必要があるリクエスト数の概算に役立ちます。以下にこれを示します。

(*request_load* x *percentage_of_transactions*) / *number_of_hours* / 3600 = *peak_request_rate*

注: このレートは最繁時の 1 時間に基づきます。 ピーク リクエスト レートが時間単位の計算を超える期間がある場合があります。

request_load

Web サービスの日単位のリクエスト数を表します。

percentage_of_transactions

システムがピーク レベルで動作しているときに発生するトランザクションの割合を表します。

number_of_hours

システムがピーク レベルで動作する時間数を表します。

注: 3,600 は 1 時間の秒数を表します。

peak_request_rate

アプリケーションのピーク リクエスト レートを表します。

例: ピーク リクエスト レートの概算

会社は、Web サービスに 1 日に 8,800 のリクエスト ロードがあることを特定しました。 システム アクティビティ レポートには、最繁時の 1 時間に 1,800 リクエストが発生することが詳述されます。 この数は、リクエスト ロードの約 20 パーセントに相当します。

1,800 / 1 / 3600 = 毎秒 0.5 リクエスト

処理 Web サービスには、毎秒 5 リクエストのピーク リクエスト レートがあります。

注: この例は最繁時の 1 時間に基づきます。この時間内のピーク リクエスト レートが毎秒 5 リクエストを超える期間がある場合があります。

詳細情報:

エージェントに対して使用できるソケット量の増加 (P. 164)

容量計画時に考慮する他の要因

リクエスト レートは、eTrust SOA Security Manager 容量計画を決定する最も重要な要因ですが、その他の要因も SiteMinder のパフォーマンスに影響します。その中には、特に Web サービスの保護に使用する認証方式があります。

また、容量計画プロセスでのパフォーマンス調整とネットワーク帯域幅を考慮します。

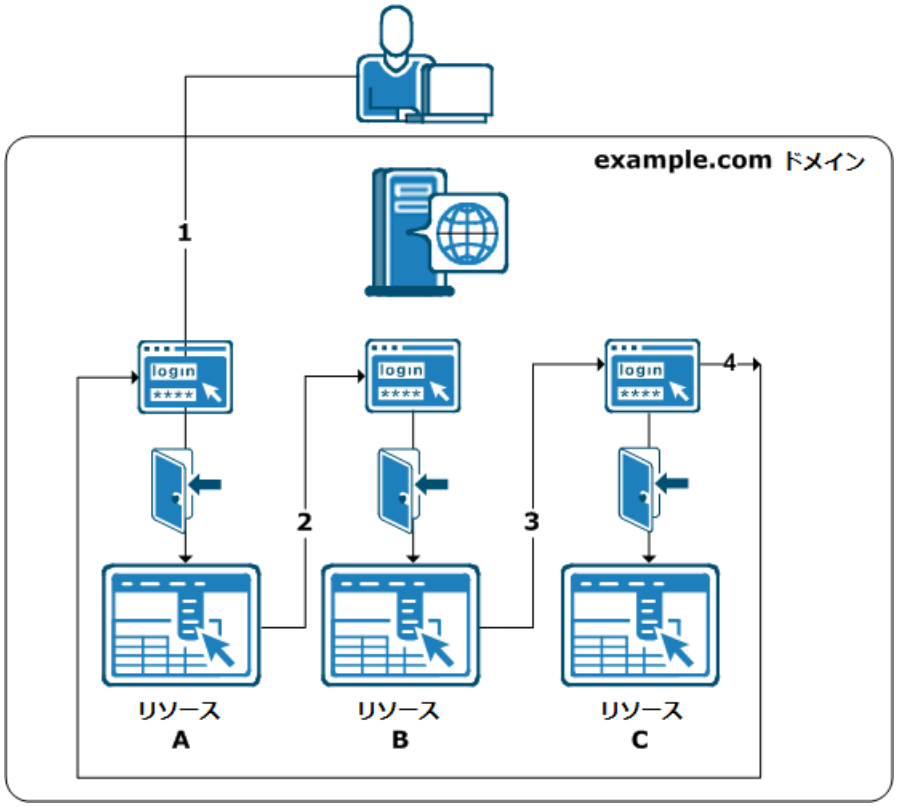
第 7 章: 設定時の考慮事項

このセクションには、以下のトピックが含まれています。

セキュリティ ゾーン

セキュリティ ゾーンは、SiteMinder Web エージェントにより保護される単一の Cookie ドメイン内のリソースのグループです。ユーザは一度認証し、その後、再認証なしで（許可されている）ゾーン内の他のリソースにアクセスできます。

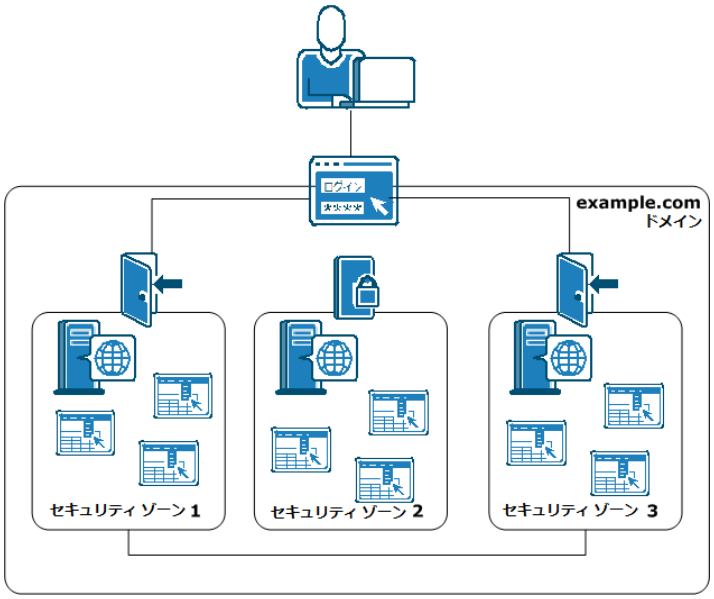
セキュリティ ゾーンがない場合、ユーザは同じ Cookie ドメイン内の保護されたリソースにアクセスする度に、（Cookie ドメイン内の別のリソースの SiteMinder によって以前に認証されていたとしても）認証される可能性があります。 以下の図に例を示します。



以下の状況でのセキュリティ ゾーンの実装を検討してください。

- Cookie ドメイン内には複数のリソースがありますが、それらのリソースには異なるアクセス制限を適用する必要があります。
- 同じ Cookie ドメインの異なるリソース間の SSO を有効にする必要があります。
- 複数の Cookie ドメインにまたがるリソース グループを作成して、それらの間で SSO を許可する必要があります。
- 単一の Cookie ドメインを持つ大規模な組織があり、SiteMinder の複数のインスタンスを使用して組織内のリソースを保護します。 セキュリティ ゾーンによって、リソースを分割して単一の Cookie ドメイン内のアクセスを制御できます。 セキュリティ ゾーンがない場合は、Cookie ドメイン名が両方のインスタンスに対して同じであるため、1 つの SiteMinder インスタンスによって使用される Cookie が、別の SiteMinder インスタンスの Cookie を上書きする可能性があります（Cookie ストンプ）。

以下の図では、シングル ログインのみがセキュリティ ゾーン 1 および 3 のリソースへのユーザ アクセスを許可するが、セキュリティ ゾーン 2 の無許可のリソースへのアクセスを拒否するようにセキュリティ ゾーンを使用する方法を示します。



注: 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。

複数のデータ センター

SiteMinder は、グローバル展開を同一大陸内の複数のデータ センターと同様に処理します。そのため、SiteMinder 以外の要因は、マルチデータ センター展開のパフォーマンスに影響します。 以下の主要因には次のものが含まれます。

- ネットワーク遅延
- 回復力

マルチデータ センター展開を計画するときには、以下の外部要因を考慮することをお勧めします。

- ネットワーク インフラストラクチャ
- アプリケーションの場所
- ユーザの場所
- ユーザ ストア ベンダー、および許可されているマスタ数などの制限

ベスト プラクティス

データ センターの設定時には、以下の点について考慮してください。

- 各データ センター内の以下のコンポーネントを連結することによって、ネットワーク遅延および回復力が SiteMinder のパフォーマンスに与える影響を減少させることができます。
  - SiteMinder エージェント
  - ポリシー サーバ
  - ユーザ ストア

    注: パスワード サービスなどの SiteMinder 機能が書き込み可能のストアを必要とする場合は、各データ センターに書き込み可能のストアを含めることをお勧めします。
- すべてのコンポーネントを同じデータ センターに含められない場合は、少なくとも同じデータ センター内のポリシー サーバおよびユーザ ストアを連結することをお勧めします。

アーキテクチャの考慮事項

SiteMinder データ センターの計画時には、以下のアーキテクチャの要因を考慮してください。

- SiteMinder パスワード サービスは、すべての認証でユーザ アカウントへの LDAP 書き込みの実行を試行します。

  注: パスワード サービスの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

- 読み取り専用のコンシューマ ディレクトリと通信する場合、SiteMinder は LDAP 書き込みリフェラルに従います。

- レプリケーション バージョンでマスタ ポリシー ストアを展開する場合は、ポリシー サーバ ホスト システム (LDAP) のローカル ホスト ファイルまたは ODBC データ ソースを使用して、ポリシー サーバをローカル ポリシー ストアに向けることを検討してください。 この方法を使用することにより、すべてのポリシー サーバが同じポリシー ストアを共有でき、すべてのポリシー サーバが広域ネットワーク（WAN）を介してポリシー ストアと通信する必要があるときに発生する可能性がある遅延を回避します。

- マスタ/コンシューマ ユーザ ストアを展開する場合は、ポリシー サーバ ホスト システム（LDAP）のローカル ホスト ファイルまたは ODBC データ ソース名（DSN）を使用して、ポリシー サーバをローカル コンシューマに向けることを検討してください。 この方法を使用することにより、すべてのポリシー サーバが同じユーザ ストアを読み取ることができ、すべてのポリシー サーバが WAN を介してユーザ アカウント情報を読み取る必要があるときに発生する可能性がある遅延を回避します。

例: ポリシー サーバをローカル コンシューマ ユーザ ストアに向けるローカル ホスト ファイル

地理的に分離された 2 つのデータ センターには、myusers という名前のコンシューマ ユーザ ストアを指しているポリシー サーバが含まれます。

- データ センター 1 のローカル コンシューマは 111.11.111.1 で使用できます
- データ センター 2 のローカル コンシューマは 222.22.222.2 で使用できます

ポリシー サーバをローカル コンシューマに向ける方法

1. データ センター 1 のポリシー サーバ ホスト システムから、ローカル ホスト ファイルを使用して myusers を 111.11.111.1 にマッピングします。
2. データ センター 2 のポリシー サーバ ホスト システムから、ローカル ホスト ファイルを使用して myusers を 222.22.222.2 にマッピングします。

複数のデータ センター ユース ケース

以下のユース ケースの目的は、ネットワーク遅延および回復力の点から SiteMinder データ センターについて考慮していただくことです。 ユース ケースは単純な展開から始まり、より複雑なシナリオに進みます。

これらのユース ケースは、グローバル アーキテクチャの一部として使用できる方法の特定を目的としており、最終アーキテクチャは想定されていません。 これらのケースから必要なインフラストラクチャを推定して、組織のニーズに最適なデータ センターを設定します。

1 つのデータ センター内のすべてのコンポーネント

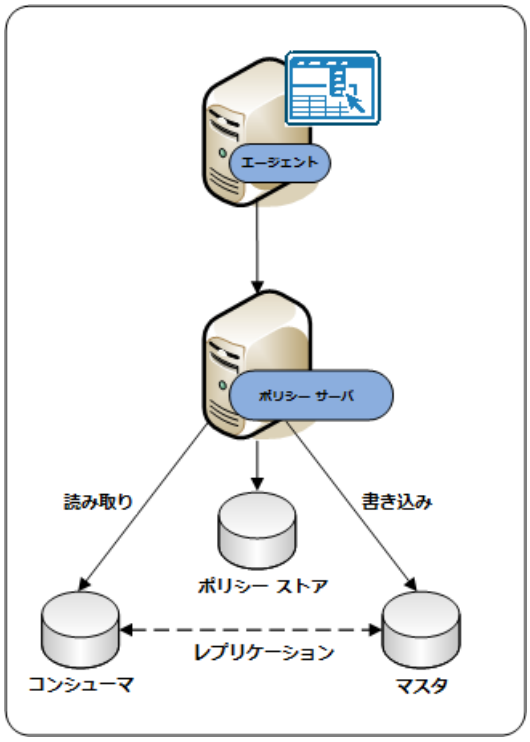
最も単純な展開では、すべての必要な SiteMinder コンポーネントが単一のデータ センターに含まれます。

以下の図では次のことを示します。

- 単一のデータ センター内のすべてのアプリケーション。
- マスタ ユーザ ストアに書き込むポリシー サーバ。 SiteMinder パスワード サービスは、すべての認証でユーザ アカウントへの LDAP 書き込みの実行を試行します。

  重要: マルチマスタ LDAP ユーザ ストア サポート制限の詳細については、「ポリシー サーバ リリース ノート」を参照してください。

- コンシューマ ユーザ ストアを読み取る SiteMinder。



以下の点について考慮してください。

- 図には示されていませんが、SiteMinder は、書き込みおよび読み取り専用トランザクション用に設定されているデータベース クラスタをサポートします。
- 運用継続性、冗長性および高可用性のために、1 つのデータ センターに複数のコンポーネントを設定できます。

詳細情報:

冗長性および高可用性 (P. 38)

複数のデータ センター内のすべてのコンポーネント

複数のデータ センターの展開によって SiteMinder 環境を拡張します。 以下の要因が、複数のデータ センターの実装を決定する際に影響する場合があります。

- ネットワーク インフラストラクチャ
- アプリケーションの場所
- ユーザの場所

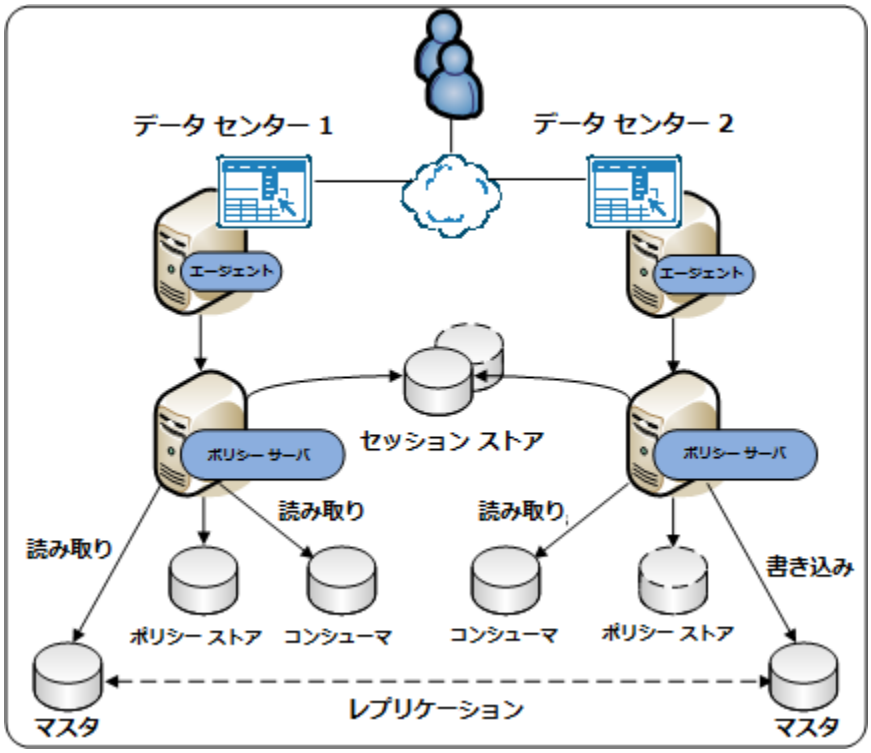
以下の図では次のことを示します。

- 複数のデータ センター内のアプリケーション
- 自身のポリシー ストアを使用する各データ センター。 データ センター 1 にはプライマリ ポリシー ストアが含まれます。 データ センター 2 には、点線で示されるように、レプリケーション バージョンが含まれています。

  注: 展開内のすべてのポリシー サーバは同じポリシー ストアへの共通のビューを共有する必要があります。ポリシー ストアの冗長性の詳細については、「ポリシー サーバからポリシー ストアへの通信 (P. 48)」を参照してください。
- 自身のマスタ/コンシューマ ユーザ ストアを使用する各データ センター。

  重要: マルチマスタ LDAP ユーザ ストア サポート制限の詳細については、「ポリシー サーバ リリース ノート」を参照してください。

- すべてのアプリケーション間のシングル サインオンを有効にする一元化されたレプリケーション セッション ストア。



詳細情報:

ポリシー サーバからポリシー ストアへの通信 (P. 48)
1 つのデータ センター内のすべてのコンポーネント (P. 138)

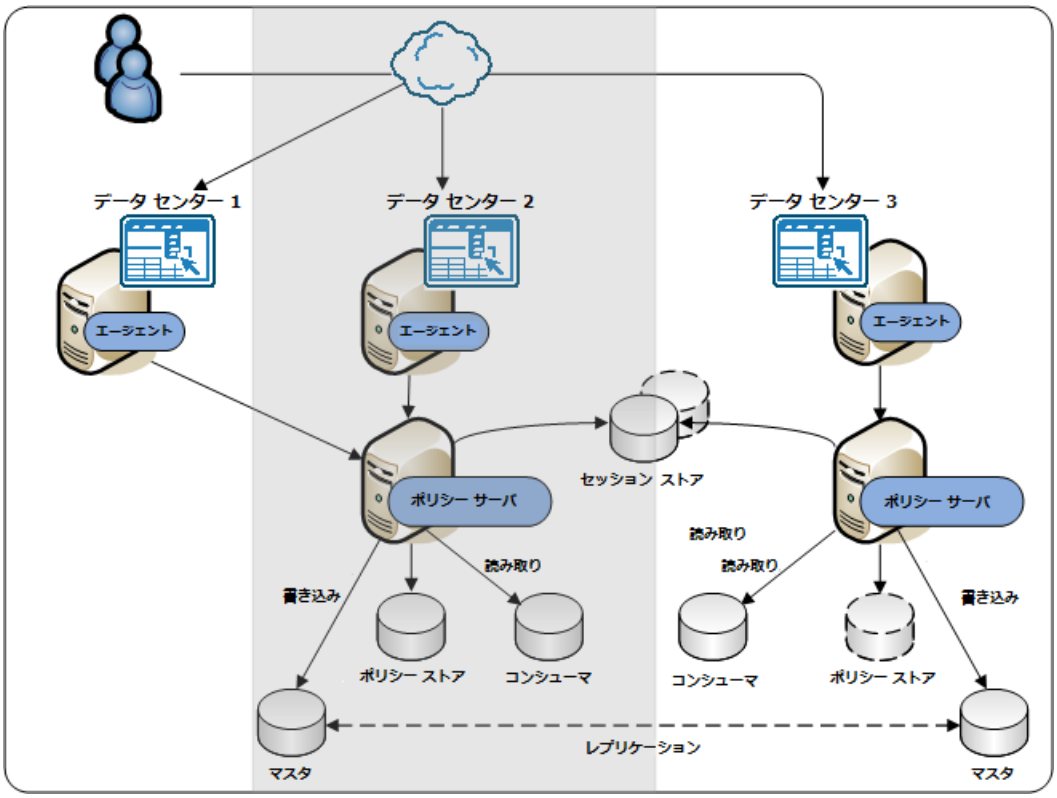
データ センターを介して通信する SiteMinder エージェント

すべてのコンポーネントを同じデータ センターに含められない場合は、少なくとも同じデータ センター内のポリシー サーバおよびユーザ ストアを連結することをお勧めします。

以下の図では次のことを示します。

- 複数のデータ センター内のアプリケーション。
- SiteMinder エージェントが存在する Web サーバを含むデータ センター 1。 エージェントは広域ネットワークを介してデータ センター 2 のポリシー サーバと通信します。

- データ センター 2 および 3 については以下のとおりです。
  - マスタ/レプリケーション ポリシー ストア (P. 49)によってポリシー ストアへの共通のビューを共有する。
  - 自身のマスタ/コンシューマ ユーザ ストア (P. 138)を使用する。
  - 一元化されたレプリケーション セッション ストアを使用して、すべてのアプリケーション間のシングル サインオンを有効にする。



詳細情報:

ポリシー サーバからポリシー ストアへの通信 (P. 48)

データ センターを介して通信するポリシー サーバ

すべてのコンポーネントを同じデータ センターに含められない場合は、少なくとも同じデータ センター内のポリシー サーバおよびユーザ ストアを連結することをお勧めします。

以下の図では次のことを示します。

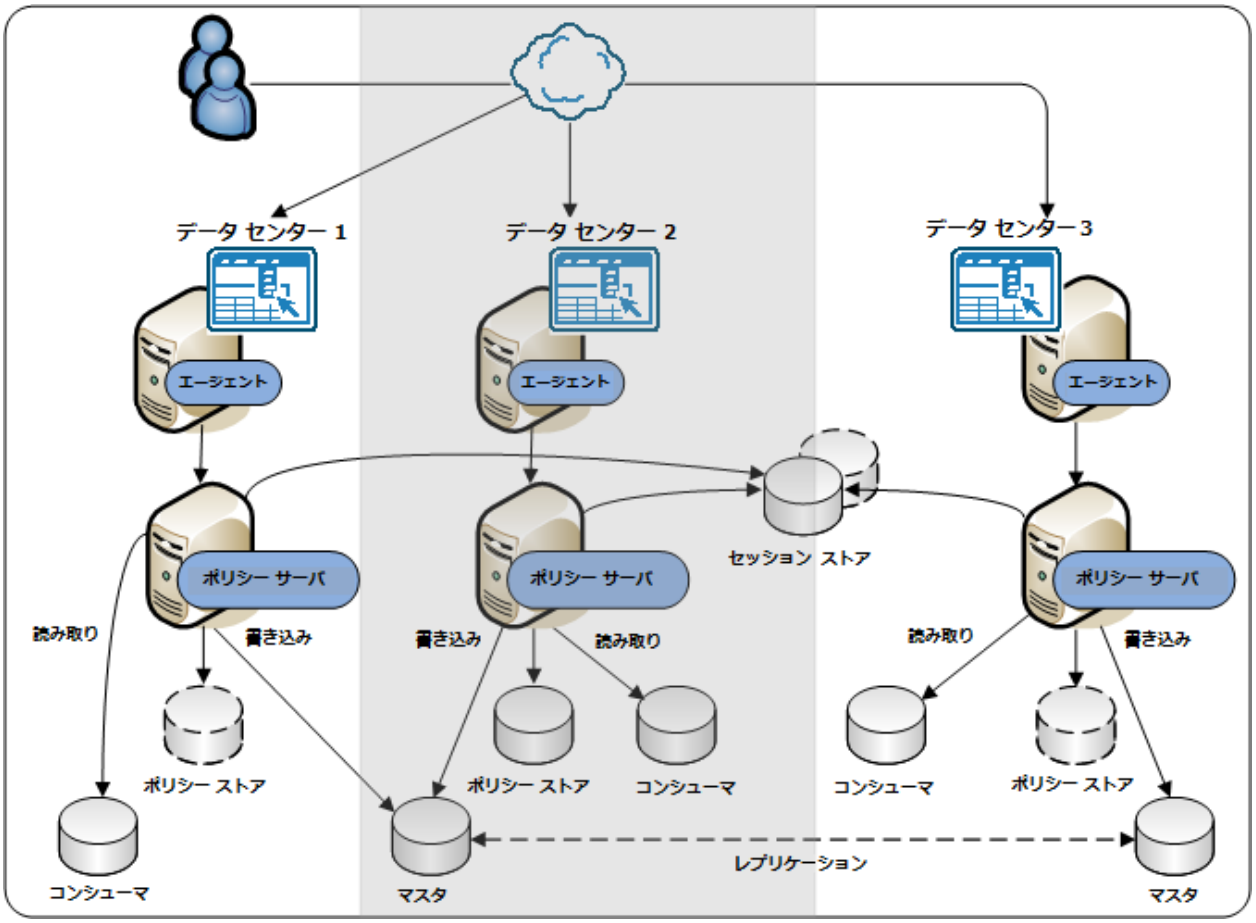
- 複数のデータ センター内のアプリケーション。
- エージェントおよびポリシー サーバのみを含むデータ センター 1。ポリシー サーバは、ワイド エリア ネットワークのみを使用して通信し、データ センター 2 のマスタ ユーザ ストアへの LDAP 書き込みを実行します。

  重要: 広域ネットワークを介して通信し LDAP 読み取りおよび書き込みを実行するようにポリシー サーバを設定することはお勧めしません。

- すべてのデータ センターについては以下のとおりです。
  - マスタ/レプリケーション ポリシー ストア (P. 49)によってポリシー ストアへの共通のビューを共有する。
  - 一元化されたレプリケーション セッション ストアを使用して、すべてのアプリケーション間のシングル サインオンを有効にする。

- 自身のマスタ/コンシューマ ユーザ ストア (P. 138) を使用するデータ センター 2 および 3。

  重要: マルチマスタ LDAP ユーザ ストア サポート制限の詳細については、「ポリシー サーバ リリース ノート」を参照してください。



詳細情報:

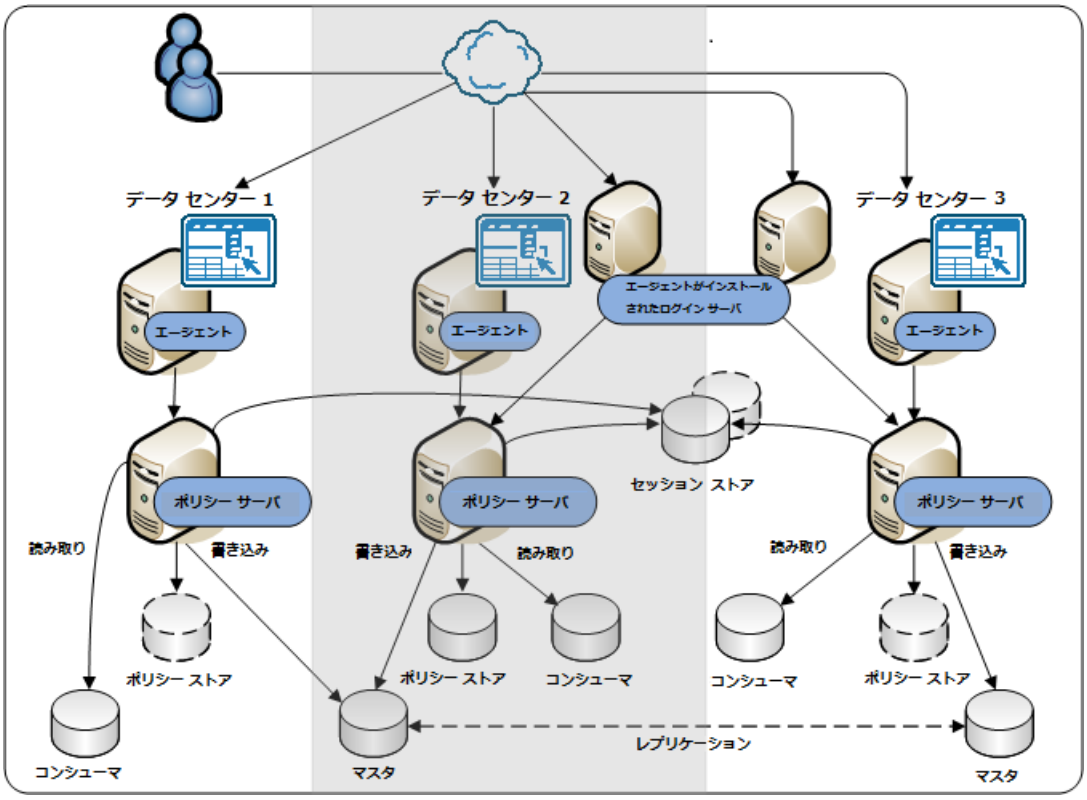
ポリシー サーバからポリシー ストアへの通信 (P. 48)
マスタ ポリシー ストア (P. 49)
1 つのデータ センター内のすべてのコンポーネント (P. 138)

ユーザ ストア書き込みを制御するログイン サーバ

LDAP 書き込み可能なマスタの場所では、SiteMinder 展開が制限される場合があります。 各データ センターの書き込み可能なマスタの要件を除去するために、1 つ以上の一元化されたログイン サーバの使用を検討してください。

以下の図では次のことを示します。

- 以下の場合の複数のデータ センター展開。
  - データ センター 1 のポリシー サーバは、WAN を介して通信し LDAP 書き込みを実行します (P. 143)。
  - すべてのコンポーネント (P. 140)を含む残りのデータ センター。
- データ センター2 およびデータ センター 3 のログイン サーバ。



ユーザがデータ センター 1 の保護されている URL へのアクセスをリクエストする場合は、以下のとおりです。

1. Web エージェントは、リクエストをデータ センター 2 のログオン サーバにリダイレクトします。 リダイレクトは、リソースを保護している認証方式に基づきます。

   注: 認証方式の詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

2. データ センター 2 のポリシー サーバはユーザを認証し、マスタ ユーザ ストアに書き込みます。

3. ポリシー サーバは SiteMinder セッション チケットを作成し、元の保護されている URL に渡します。

   注: ユーザ セッションの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

4. Web エージェントは SiteMinder セッション チケットを Cookie に配置します。以下のいずれかが発生するまで、Web エージェントは Cookie を使用して、データ センター内の後続の認証および許可リクエストを処理します。

   - ユーザは、追加のクレデンシャルを必要とする別のリソースをリクエストします。
   - セッションが失効します。

認証および一元化されたログイン サーバ

SiteMinder 展開には、通常、異なる認証（ログイン）要件が存在するアプリケーションが含まれます。 これらの要件は、個別のアプリケーション所有者による管理を必要とする多数のログイン ページをもたらす場合があります。 これらのログイン ページの管理は、認証操作全体に影響する可能性があるページ設計およびエラー メッセージの表示などの不整合をローカルに引き起こす場合があります。

以下を実行するために、ログイン ページを一元的に管理することをお勧めします。

- 複数のアプリケーション全体にわたる整合性を実現します。 単一の SiteMinder チームがすべてのログイン ページを所有する場合、チームはそれらを一貫して実装し、より簡単に管理することができます。
- ログイン ページの数を最小限にします。アプリケーションへのエントリ ポイントの数を最小限にすることによって、ユーザが個別のアプリケーションではなく一元化されたインフラストラクチャにログインしているような状態になります。

ログイン ページの設定時には、以下の点について考慮してください。

- 同じ認証要件を共有し、同じログイン ページを再利用するアプリケーションを特定します。
- 一元化されたログイン サーバを使用して、すべてのログイン ページをホストします。
- 以下の場合にユーザに通知するようにログイン ページを設定します。
  - 有効な認証情報を入力していません。
  - 試行回数が多すぎるため認証に失敗しました。

ログイン ページの一元化

アプリケーション ログイン要件は、ユーザ名/パスワードの基本認証からフォーム ベースの認証、デジタル証明書にまで及ぶ場合があります。 可能ならば、以下をお勧めします。

- 中央ログイン サーバからすべてのログイン ページを管理して、すべての Web アプリケーション上の重複を回避する。
- パスワード サービス ページ、エラー ページおよび条件ページなど他のすべてのシステム全体のリソースを中央サーバから管理する。

注: 認証方式の詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

ログイン ページを一元的に管理することは、同じログイン要件を共有するアプリケーションを特定するプロセスです。 認証の設定時には、以下の点について考慮してください。

- 各アプリケーション用に個別のログイン ページを作成しないようにします。 SiteMinder 導入の増加に伴い、すべてのアプリケーション用のログイン ページの管理を持続できない場合があります。
- 同じ認証要件を共有するアプリケーションを特定します。 可能であれば、これらのアプリケーションへのエントリ ポイントとして単一のログイン ページを使用します。

以下のような表を使用して、認証要件によってアプリケーションをグループ化します。

認証方式名	タイプ	ログイン ページ サーバ	ログイン ページ URL

例: 認証要件によるアプリケーションのグループ化

SiteMinder 環境は 10 のアプリケーションを保護します。

- 5 つのアプリケーションにはフォーム ベースの認証が必要です。
- 3 つのアプリケーションには Windows ベースの認証が必要です。
- 2 つのアプリケーションにはユーザ名/パスワードの基本認証が必要です。

同じ認証要件を共有するアプリケーションを特定することにより、以下の表で詳述されるように、3 つのログイン ページによって 8 つが不要になります。

認証方式名	タイプ	ログイン ページ サーバ	ログイン ページ URL
Auth1	フォーム	login.acme.com	/login.asp
Auth2	Windows	login.acme.com	/smgetcrd.ntc
Auth3	基本	login.acme.com	該当なし

ベスト プラクティス

ログイン ページの設定時には、以下の点について考慮してください。

- ユーザが認証に失敗すると、エラー メッセージが表示されます。
- ログインの試行回数を超過したというメッセージを表示するページにユーザをリダイレクトします。
- ユーザのリダイレクトにはフォーム ベースの認証を使用することをお勧めします。 フォーム ベースの認証を使用できない場合は、SiteMinder の OnAuthAttempt および OnAuthReject レスポンスを使用してユーザをリダイレクトできます。

  注: レスポンスの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

- フォーム ベースの認証を設定する場合は、login.asp などの動的なページを作成して既存のインフラストラクチャとのより緊密な統合を作成することを考えます。
- 動的なページを作成できない場合は、Web エージェント インストールの一部として含まれているサンプル ログイン FCC ファイル（login.fcc）を使用して、ログイン FCC ファイルを設定します。 サンプル ファイルのデフォルトの場所は *web_agent_home*¥samples_default¥forms です。 フォーム ディレクトリは、フォーム クレデンシャル コレクタ（FCC）が処理するファイルのデフォルトの場所です。

  web_agent_home

  Web エージェントのインストール パスを指定します。

  注: フォーム ベースの認証に適用されるログイン FCC 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。Web エージェントによるログイン FCC の設定、および FCC プロセスによるリクエスト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。

- Web エージェント ホスト システム上ですべてのログイン ページ用に個別のディレクトリを作成することをお勧めします。フォーム ディレクトリ以外の場所を使用すると、サンプル ファイルが誤って上書きされるのを防ぐのに役立ちます。
- ユーザが正常にログアウトすると、カスタム ログオフ ページが表示されます。

  注: ログオフ ページ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。

ログイン ページ ユース ケース

以下のユース ケースの目的は、SiteMinder 認証について考慮していただくことです。

これらのユース ケースはベスト プラクティスを反映し、グローバル アーキテクチャの一部として使用できる方法の特定を目的としています。 これらのユース ケースで最終アーキテクチャは想定されていません。 これらのケースから必要なインフラストラクチャを推定して、組織のニーズに最適なログイン ページを設定します。

スタンドアロン ログイン ページ

このユース ケースでは、ユーザが保護されたリソースをリクエストすると、SiteMinder はスタンドアロン ログイン ページにユーザをリダイレクトします。 具体的な内容は次のとおりです。

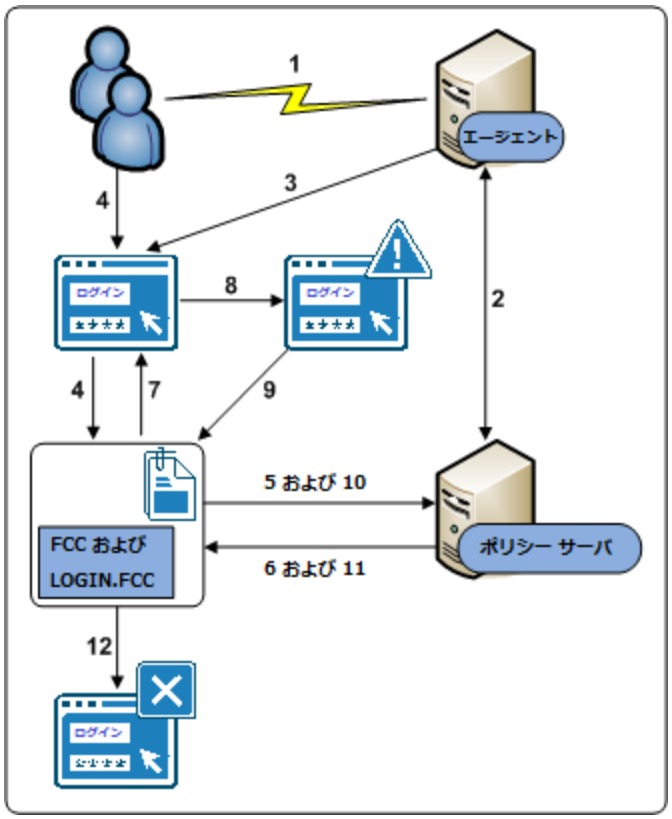
- 動的ログイン ページ（login.asp）は Web エージェント ホスト システムに展開されます。
- 動的なログイン ページは、以下の目的でコード化されます。
  - ログイン FCC ファイル（login.fcc）にポストします。
  - SMTRYNO Cookie がユーザの Web ブラウザに存在する場合に、エラー メッセージを表示します。

    注: SMTRYNO cookie に関する詳細は、「*Web エージェント設定ガイド*」を参照してください。
- ログイン FCC ファイルには、認証試行が 2 回失敗した後でユーザを認証失敗ページ（login.unauth）にリダイレクトする @directive（@smretries）が設定されています。

  注: @directives を含む FCC ファイル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。
- SiteMinder 管理者は、Auth1 という名前のフォーム ベースの認証方式を設定しました。 Auth1 のターゲットは login.asp です。

  注: 認証方式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。

以下の図ではこのユース ケースの認証プロセスを示します。



1. ユーザが保護されたリソースをリクエストします。
2. Web エージェントはポリシー サーバに問い合わせ、ポリシー サーバはリソースが保護されていると判断します。
3. Web エージェントはユーザ リクエストを login.asp にリダイレクトします。
4. ユーザは無効な認証情報をサブミットします。 認証情報は login.fcc ファイルにポストされ、FCC によって処理されます。
5. FCC は認証情報をポリシー サーバに転送します。
6. ポリシー サーバは、認証情報が無効であると判断して FCC に通知します。
7. FCC は SMTRYNO Cookie をユーザの Web ブラウザに挿入して、ユーザをログイン ページにリダイレクトします。

8. ログイン ページはエラー メッセージでリフレッシュされます。 エラー メッセージには、無効な認証情報が入力されたこと、および再試行が示されます。
9. ユーザは無効な認証情報をサブミットします。 認証情報は login.fcc ファイルにポストされ、FCC によって処理されます。
10. FCC は認証情報をポリシー サーバに転送します。
11. ポリシー サーバは、認証情報が引き続き無効であると判断して FCC に通知します。
12. ユーザは認証試行失敗の最大回数を超過してしまい、認証失敗メッセージが表示されるページにリダイレクトされます。

Web ポータル上の埋め込まれたフォーム

このユース ケースでは、フォームは Web ポータル ホーム ページに埋め込まれています。 ユーザは認証情報をフォームに入力し、認証時に保護されたリソースにリダイレクトされます。 具体的な内容は次のとおりです。

- Web ポータル ホーム ページ（portal.asp）には、ユーザにクレデンシャルを要求する埋め込みフォームが含まれます。ホーム ページについては以下のとおりです。
  - 保護されたリソースを指す目標変数を含みます。
  - ログイン FCC ファイル（login.fcc）にポストします。
- スタンドアロン ログイン ページ（login.asp）は Web エージェント ホスト システムに展開されます。ユーザが保護されたリソースに直接アクセスしようとすると、このページによって認証情報をリクエストされます。 ログイン ページ：
  - ログイン FCC ファイルにポストします。
  - SMTRYNO Cookie がユーザの Web ブラウザに存在する場合、エラー メッセージを表示します。

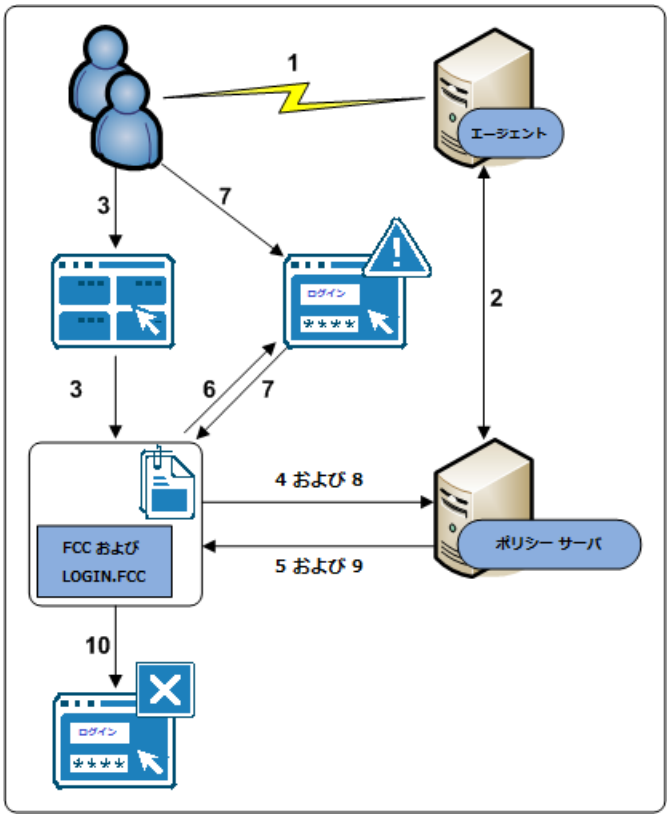
    注: SMTRYNO cookie に関する詳細は、「*Web エージェント設定ガイド*」を参照してください。
- ログイン FCC ファイルには、認証試行が 2 回失敗した後でユーザを認証失敗ページ（login.unauth）にリダイレクトする @directive（@smretries）が設定されています。

  注: @directives を含む FCC ファイル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。

- SiteMinder 管理者は、Auth1 という名前のフォーム ベースの認証方式を設定しました。 Auth1 のターゲットは login.asp です。

  注: 認証方式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。

以下の図ではこのユース ケースの認証プロセスを示します。



1. ユーザは Web ポータル ホーム ページに移動します。
2. Web エージェントはポリシー サーバに問い合わせ、ポリシー サーバはリソースが保護されていないと判断します。
3. ユーザは無効な認証情報をサブミットします。 認証情報は login.fcc ファイルにポストされ、FCC によって処理されます。
4. FCC は認証情報をポリシー サーバに転送します。
5. ポリシー サーバは、認証情報が無効であると判断して FCC に通知します。

6. FCC は SMTRYNO Cookie をユーザの Web ブラウザに挿入して、ユーザをログイン ページにリダイレクトします。 ログイン ページにエラー メッセージが表示されます。エラー メッセージには、無効な認証情報が入力されたこと、および再試行が示されます。

   注: 図には示されていませんが、ユーザが保護されたリソースに直接アクセスした場合、Web ブラウザには SMTRYNO Cookie が含まれていないので、ログイン ページにエラー メッセージは表示されません。

7. ユーザは無効な認証情報をサブミットします。 認証情報は login.fcc ファイルにポストされ、FCC によって処理されます。

8. FCC は認証情報をポリシー サーバに転送します。

9. ポリシー サーバは、認証情報が引き続き無効であると判断して FCC に通知します。

10. ユーザは認証試行失敗の最大回数を超過してしまい、認証失敗メッセージが表示されるページにリダイレクトされます。

第 8 章: パフォーマンス調整

このセクションには、以下のトピックが含まれています。

導入されたパフォーマンス調整

ポリシー サーバは、以下の 3 つの基本的なリクエストを処理することによって、アクセス制御ポリシーを評価および実行します。

- IsProtected -- リクエストされたリソースは保護されていますか。
- IsAuthenticated -- リソースをリクエストするユーザは ID を確立するために認証情報を示しましたか。
- IsAuthorized -- 認証されたユーザは、保護されているリソースを表示することを認められますか。

これらの各リクエストを処理することによって、SiteMinder コンポーネント間のトランザクションが作成されます。SiteMinder のパフォーマンス 調整は、以下によってスループットを増やして遅延を減らす反復プロセスです。

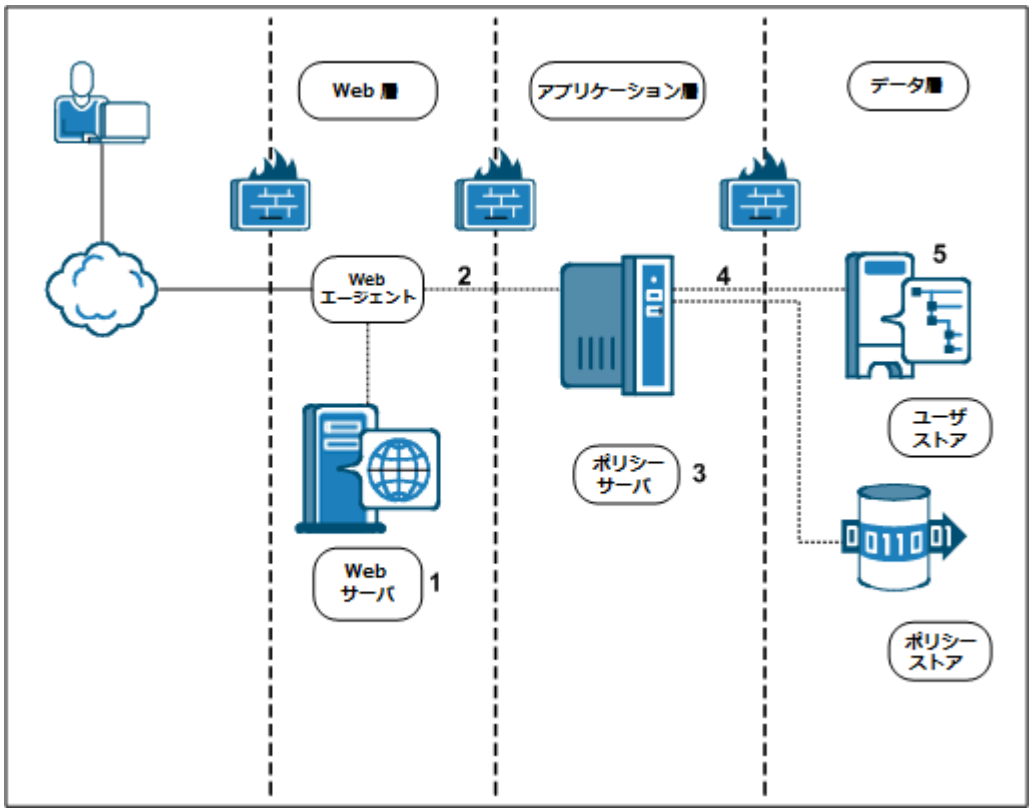
- これらのトランザクションが発生する場所ととき
- パフォーマンスに影響する SiteMinder 設定および機能を特定する
- サードパーティおよび SiteMinder のツールを使用してパフォーマンスを測定し、インフラストラクチャ ボトルネックを特定する

よい戦略は、Web、アプリケーション、およびデータ層でパフォーマンス要因を検討することです。

注: SiteMinder はミドルウェアであり、単独で展開されません。 以下のセクションでは、実際の Web、アプリケーションまたはデータ層自身の調整方法ではなく、Web およびアプリケーション層の SiteMinder コンポーネントの調整に焦点を当てます。 お使いの環境の Web サーバ、ディレクトリサーバおよびデータベースの調整の詳細については、ベンダー固有のマニュアルを参照してください。

パフォーマンス調整のロードマップ

パフォーマンス調整は反復プロセスであるため、Web、アプリケーションおよびデータ層を個別に処理して、それぞれがどのようにパフォーマンス全体に影響する可能性があるかを理解することが重要です。 SiteMinder エージェント、ポリシー サーバ、または SiteMinder ポリシー オブジェクト自体の設定を変更することで、パフォーマンスが向上することがよくあります。 以下の図では標準的な展開を示し、パフォーマンスの中心となる個別のコンポーネントについて詳述します。



1. 環境内に展開された Web サーバおよびアプリケーション サーバのタイプが、SiteMinder エージェントとポリシー サーバの通信方法に影響する場合があります。
2. 使用できるソケット数が、エージェントとポリシー サーバの通信効率に影響する場合があります。
3. SiteMinder ポリシー設計が、ポリシー サーバによる認証リクエストおよび許可リクエストの処理効率に影響する場合があります。
4. ポリシー サーバは一連のサービスを実行して、ユーザを認証および許可します。 これらのサービスによって、リクエストと総称されるユーザ ディレクトリへの読み取りおよび書き込みが生じます。 SiteMinder のパフォーマンスに関与する要因によって、ユーザ ディレクトリが操作の持続期間およびピーク期間にこの作業負荷を処理できるかどうかが決定します。
5. ユーザ ディレクトリ自身が SiteMinder のパフォーマンスに影響する場合があります。

詳細情報:

ユーザ ストア容量計画 (P. 206)
SiteMinder ポリシー設計およびパフォーマンス (P. 182)
サーバのパフォーマンス (P. 161)
エージェントとポリシー サーバ間のトラフィックの低減 (P. 167)
データ層ガイドライン (P. 203)
Web 層ソケットの使用 (P. 163)

Web 層のパフォーマンス

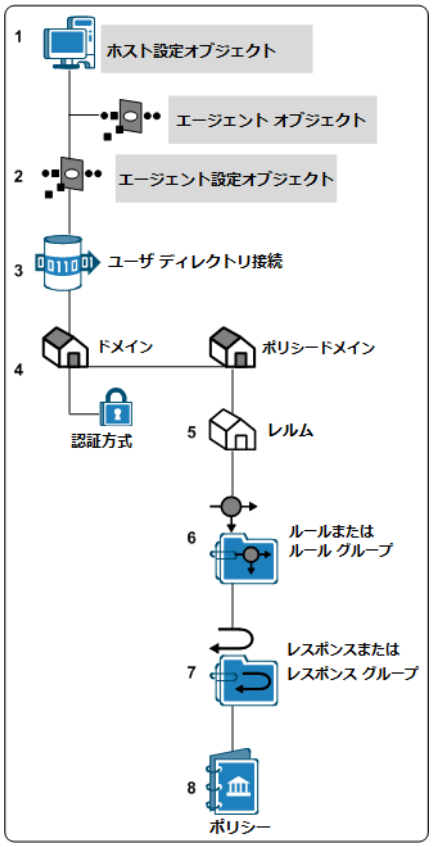
SiteMinder エージェントが Web サーバまたはアプリケーション サーバに送信されたリクエストをインターセプトする場合、エージェントは SiteMinder ポリシー サーバに以下の呼び出しを行います。

- isProtected
- isAuthenticated
- isAuthorized

これらの各呼び出しによって、Web 層のエージェントとアプリケーション層のポリシー サーバの間でトラフィックが生成されます。 以下の設定によって、Web 層のパフォーマンスを調整できます。

- ポリシー サーバ リクエストのタイムアウト間隔を変更します。
- エージェントがポリシー サーバ接続に使用できるソケットの数を変更します。
- エージェント キャッシュを使用して、エージェントが ポリシー サーバに対して行う呼び出しの数を減らします。

以下の図でグレー表示された項目には、Web 層のパフォーマンスに影響する設定が含まれます。



サーバのパフォーマンス

SiteMinder エージェントは、多くのサポートされている Web サーバおよびアプリケーション サーバにインストールできます。 ホスト サーバのパフォーマンスにより、SiteMinder Web 層のパフォーマンスが決まります。以下のアイテムは、SiteMinder での Web サーバのパフォーマンスに影響します。

- Web サーバのプロセッサ速度
- Web サーバのメモリ量

SiteMinder エージェントのパフォーマンス

以下の要因が SiteMinder Web エージェントのパフォーマンスに影響します。

- Web サーバまたはアプリケーション サーバの CPU および使用可能なメモリ。
- ポリシー サーバの遅延（ポリシー サーバがエージェントのリクエストに応答する速さ）。

リクエスト数を処理するために使用できる Web サーバが少なすぎる場合、以下のタイプの問題が発生する場合があります。

- ユーザのログインが遅延する、またはできません。
- 要求したリソースを受け取るユーザ側で遅延が発生します。
- CPU 使用率が最大容量、またはそれに近くなります。

ピーク時に各 Web サーバまたはアプリケーション サーバによってサービスされるリクエスト数の予想は、SiteMinder 環境の Web サーバの理想的な数を判断するのに役立ちます。

以下のいずれかの方法を使用してリクエスト数を概算します。

- 容量計画作業を実行します。
- 環境内の各エージェントの SiteMinder アクティビティ レポートを生成します。
- Web サーバ用にパフォーマンス レポートを生成します。

  注: 詳細については、Web サーバ ベンダーによって提供されているマニュアルを参照してください。

詳細情報:

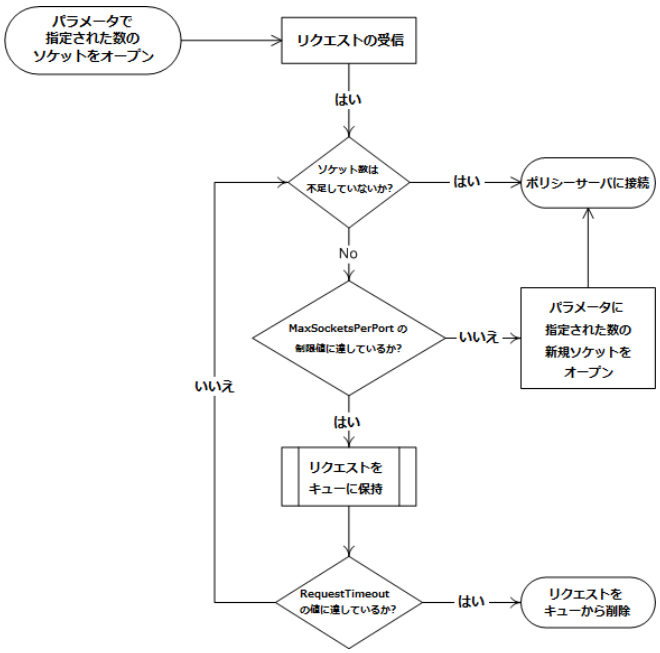
ピーク認証レートの概算 (P. 113)
ピーク許可レートの概算 (P. 121)

Web 層ソケットの使用

SiteMinder エージェントの起動時に、ポリシー サーバ上のホスト設定オブジェクト内の MinSocketsPerPort パラメータによって指定された数のソケットが開きます。 受信されるリクエストが多い場合、最大ソケット数に達するまで、エージェントは指定された数の新しいソケットを接続プールに追加します。 すべてのソケットが使用されると、以下のいずれかのイベントが発生するまで、その他のリクエスト（300 まで）はキューに保持されます。

- ソケット ペアが使用可能になり、リクエストがポリシー サーバに送信される。
- リクエストがタイムアウトになり、ユーザはリソースへのアクセスを再試行する必要があります。

以下の図では、このプロセスについて説明します。



ポリシー サーバ上のホスト設定オブジェクトには、使用されるソケット数を制御するパラメータが含まれます。

高負荷時のリクエストのタイムアウト間隔の増加

ネットワークが以下のいずれかの状況である場合、SiteMinder エージェントからのリクエストがポリシー サーバのキューで保持される期間の延長を検討してください。

- 過剰トラフィック
- 遅い接続

ポリシー サーバ上のホスト設定オブジェクト内の RequestTimeout パラメータは、エージェントがポリシー サーバからの応答を待つ期間を制御します。 間隔が短すぎる場合、リクエストはタイムアウトになり、ユーザはエラー メッセージを受信します。

注: 詳細については、「*SiteMinder ポリシー サーバ設定ガイド*」を参照してください。

エージェントに対して使用できるソケット量の増加

容量計画の概算によって、SiteMinder エージェントごとのユーザ リクエスト数が一定期間に 60 を超える（20 のリクエストが処理中で 40 がキュー内にある）ことが確認された場合は、MaxSocketsPerPort パラメータの値を増やします。

管理 UI 内の MaxSocketsPerPort パラメータの値を増やした後で、ポリシー サーバ管理コンソールの［最大接続数］設定が、SiteMinder 環境のすべてのエージェント プロセスに対応するために十分であることを確認します。この設定によって、特定のポリシー サーバに対して使用できる最大接続数が決まります。

注: マルチプロセス Web サーバ（pre-fork モードの Apache ベース サーバなど）については、このソケット数を 1 に減らすことができます。 各プロセスが SiteMinder ポリシー サーバ と通信するために使用するのは 1 スレッドのみなので、必要なソケットは 1 つのみです。

詳細情報:

ピーク リクエスト レートの概算 (P. 129)

NewSocketStep 設定の増加

SiteMinder エージェントがピーク期間に接続プールからの追加のソケットを必要とする場合、NewSocketStep パラメータによって各回に取得するソケット数が決まります。

NewSocketStep パラメータの値の設定が低すぎる場合、エージェントがソケット接続の作成に余分な時間をとるので、ピーク期間の応答時間に影響します。

遅い応答時間を回避するには、容量計画の概算を使用してエージェントが処理するリクエスト数を判断し、NewSocketStep パラメータの値をそれに応じて増やします。

このパラメータの理想的な数は、Web またはアプリケーション サーバの負荷が増加するときに、リクエスト用のソケット作成にエージェントが時間を使い過ぎることを防ぐために十分な大きさの数です。

SiteMinder 環境で最適に動作する設定を見つけるまで、様々な設定での試行をお勧めします。

注: マルチプロセス Web サーバ（pre-fork モードの Apache ベース サーバなど）については、このソケット数を 1 に減らすことができます。各プロセスが SiteMinder ポリシー サーバ と通信するために使用するのは 1 スレッドのみなので、必要なソケットは 1 つのみです。

詳細情報:

ピーク認証レートの概算 (P. 113)
ピーク リクエスト レートの概算 (P. 129)

ポートあたりの最小ソケット数設定

SiteMinder エージェントの起動時に、ポリシー サーバ上のホスト設定オブジェクト内の MinSocketsPerPort パラメータによって指定された数のソケットが開きます。 これらのソケットによりポリシー サーバへの常時接続が維持されます。

ほとんどのタイプの Web およびアプリケーション サーバ（ワーカー モードの Apache ベースのサーバを含む）については、このパラメータをデフォルト設定のままにすることをお勧めします。 このパラメータを増やすと、エージェントがリソースに対するリクエストを受信していないときでもソケットを開いたままにすることによって、不必要にソケットを占有します。

注: マルチプロセス Web サーバ（pre-fork モードの Apache ベース サーバなど）については、このソケット数を 1 に減らすことができます。 各プロセスが SiteMinder ポリシー サーバ と通信するために使用するのは 1 スレッドのみなので、必要なソケットは 1 つのみです。

ソケット設定間の関係の例

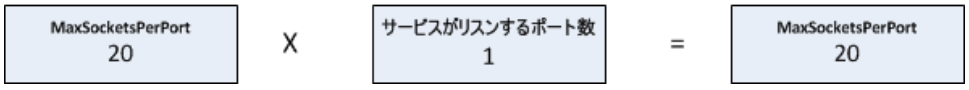
使用している Web サーバのタイプによって、ポリシー サーバ上のソケット割り当てパラメータ間の関係が決まります。

単一プロセス複数スレッドの Web サーバは複数プロセス単一スレッドの Web サーバとは異なる動作をするので、ポリシー サーバ上のソケットの割り当ては Web サーバの各タイプによって異なります。

注: このタイプを判断するには、各 Web サーバのベンダーのマニュアルを参照してください。

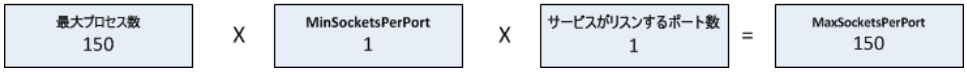
以下の図では、単一プロセス、複数スレッドの Web サーバの式について説明します。

シングルプロセス/マルチスレッドの Web サーバにおけるソケット設定の公式



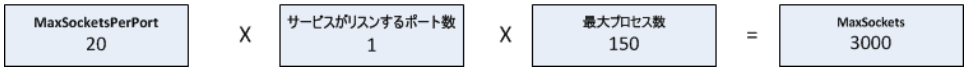
以下の図では、複数プロセス、単一スレッドの Web サーバの式について説明します。

マルチプロセス/シングルスレッドの Web サーバにおけるソケット設定の公式



以下の図では、複数プロセス、複数スレッドの Web サーバの式について説明します。

マルチプロセス/マルチスレッドの Web サーバにおけるソケット設定の公式



ソケット設定を調整するときに、前述のいずれかの式をガイドとして使用します。

エージェントとポリシー サーバ間のトラフィックの低減

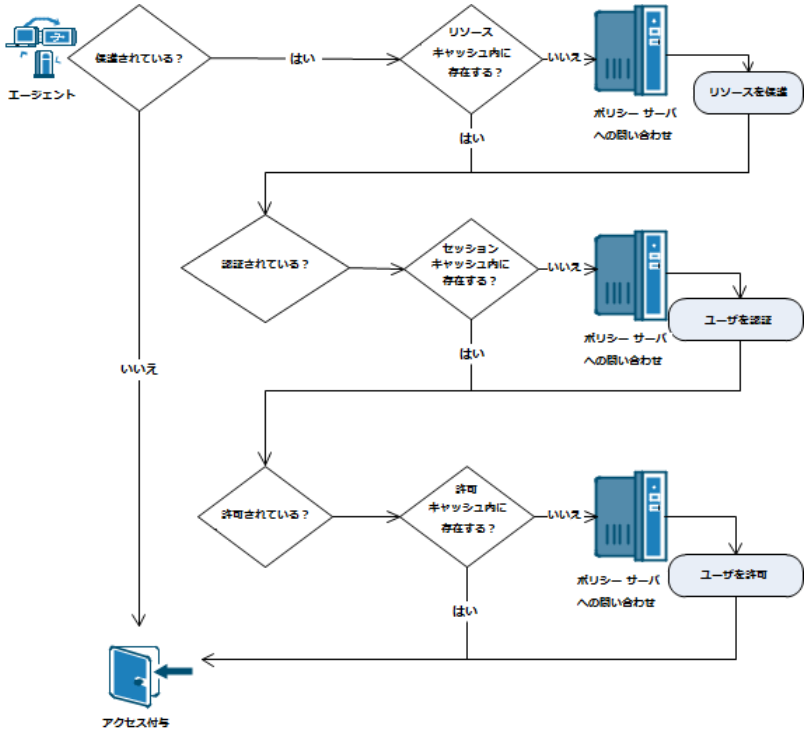
エージェントとポリシー サーバ間のトラフィック量を減らすために併用できる SiteMinder エージェントの複数のキャッシュおよび設定パラメータ。 一般的に、これらの設定は、ポリシーおよび URI が通常は静的なままである SiteMinder 環境で最も効率的です。

エージェント キャッシュが動作する仕組み

SiteMinder エージェントは、SiteMinder ポリシー サーバに問い合わせる前に必要な情報のために以下のキャッシュを検索します。

- リソース キャッシュ
- セッション キャッシュ
- 許可キャッシュ

キャッシュからの情報の取得はポリシー サーバへの問い合わせより迅速なので、パフォーマンスが向上します。 以下の図では、このプロセスについて説明します。



リソース キャッシュ

SiteMinder エージェントはそれぞれ、ポリシー サーバから一時的に受信する以下の情報を格納するためにリソース キャッシュを使用します。

- リソースが保護されているかどうか
- ポリシーに含まれる任意の追加レスポンス属性

エージェントはポリシー サーバに問い合わせる前に、リソースが保護されているかどうかを決定するためにリソース キャッシュを検索します。リソースがキャッシュに存在する場合、エージェントはポリシー サーバへ IsProtected 呼び出しを行わないので、ポリシー サーバへのトラフィックが軽減されます。

2 つのエージェント設定パラメータがリソース キャッシュに影響します。SiteMinder の配置を計画する際には、以下の点を考慮します。

リソース キャッシュのタイムアウト

キャパシティ計画テストの結果に基づいたエージェント リソース キャッシュのタイムアウト間隔をお勧めします。タイムアウト間隔が短すぎると、リソース キャッシュの有効性が制限されます。エージェント設定の ResourceCacheTimeout パラメータの値が、リソース キャッシュのタイムアウト間隔を決定します。

リソース キャッシュのサイズ

ユーザからの要求が予想される URI の最大数の 10 パーセント増しのリソース キャッシュを使用することをお勧めします。 動的 URL（クエリ文字列を持つ URL など）を使用するアプリケーションを保護している場合は、リソース キャッシュのサイズを調整する代わりに IgnoreQueryData パラメータを使用することを検討してください。MaxResourceCacheSize エージェント設定パラメータの値は、リソース キャッシュのサイズを決定します。

注: 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。

リソース キャッシュおよび URL クエリ文字列

URL クエリ文字列を使用するアプリケーションを保護する場合、クエリ文字列内のデータを無視するように Web エージェントを設定することにより、今までどおりリソース キャッシュを利用できます。クエリ文字列データが無視されると、省略された URL がリソース キャッシュに格納されます。 クエリ文字列は、Web エージェント設定で IgnoreQueryData パラメータの値を設定することにより無視されます。

重要: URL クエリ データに依存するポリシーがある場合は、この設定を有効にしないでください。

次の表では、URL 内のクエリ文字列を無視することにより、リソース キャッシュのアイテムを使用するか、または代わりに Web エージェントがポリシー サーバに問い合わせるかを決定する方法を示しています。

クエリ文字列を持つ要求された URL	切り捨てられた URL（キャッシュに格納）	キャッシュされたアイテム（使用中）	問い合わせ先ポリシー サーバ
/exampleapplication/page1.html?user=firstuser	/exampleapplication/page1.html	いいえ	はい
/exampleapplication/page1.html?user=seconduser		はい	いいえ
/exampleapplication/page2.html?user=seconduser	/exampleapplication/page2.html	いいえ	はい

注: 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。

セッション キャッシュ（認証）

各 SiteMinder エージェントは、セッション キャッシュを使用してポリシー サーバがすでに認証したユーザの認証情報を格納します。

エージェントはセッション キャッシュを検索して、ポリシー サーバに認証を問い合わせる前に、ユーザが認証済みであるかどうかを判断します。セッション キャッシュによって、ポリシー サーバへの認証呼び出しの数を減らすことにより、パフォーマンスが向上します。

以下のいずれかのイベントが発生すると、ユーザの認証は終了します。

- ユーザがログアウトします。
- ユーザに関連付けられたセッションが期限切れになります。
- キャッシュ内の項目の経過時間が 60 分を超えます。

認証情報はセッション キャッシュから削除され破棄されます。

許可キャッシュ

各 SiteMinder エージェントは、許可キャッシュを使用してポリシー サーバがすでに許可したユーザの許可識別を格納します。

エージェントは許可キャッシュを検索して、ポリシー サーバに許可を問い合わせる前に、ユーザが許可済みであるかどうかを判断します。 許可キャッシュによって、ポリシー サーバへの許可呼び出しの数を減らすことにより、パフォーマンスが向上します。

以下のいずれかのイベントが発生すると、ユーザの許可は終了します。

- ユーザがログアウトします。
- ユーザに関連付けられたセッションが期限切れになります。

許可識別はキャッシュから削除され破棄されます。

セッション キャッシュおよび許可キャッシュの設定

ポリシー サーバ設定とエージェント設定パラメータの組み合わせによってセッション キャッシュおよび許可キャッシュを制御します。 容量計画の結果を参考にして、SiteMinder 展開内の以下の設定に最適な値を決定します。

セッション タイムアウト

次のようにセッション タイムアウトを設定することをお勧めします。

- 保護されているアプリケーションに最大数のユーザがアクセスしている持続時間に合わせて最大セッション タイムアウトを設定します。
- アイドル セッション タイムアウトを、次のすべての基準を満たす間隔に設定します。
  - 作業中にユーザがログアウトしないために十分に長い。
  - アプリケーションが使用されていないとき（ユーザがログアウトせずに、コンピュータを離れる場合など）に、ユーザを自動的にログアウトさせるために十分に短い。

ポリシー サーバの設定がタイムアウト間隔を決定する。

セッション キャッシュのサイズ

このキャッシュのサイズは、セッション タイムアウト間隔中の持続期間にリソースへのアクセスが予想されるユーザ数に基づいて決定します。サイズの見積もりには、セッション タイムアウト期間中にログアウトして再びログインするユーザも含めます。 サイズの見積もりには、ほとんど要求を行わないと予想されるユーザは含めないでください（こうしたユーザはセッション キャッシュおよび許可キャッシュにわずかの影響しか及ぼさないからです）。 MaxSessionCacheSize という名前の Web エージェント設定パラメータは、セッション キャッシュと許可キャッシュの両方のサイズを決定します。

詳細情報:

持続認証レートの概算方法 (P. 109)

キャッシュおよび匿名ユーザ

SiteMinder によって提供される匿名認証方式は、それらが保護するリソースへのアクセスを制御*しません*。 匿名認証方式は、ネットワーク上の未確認のユーザに対して以下を許可します。

- ユーザがサイトに戻る頻度を追跡します。
- 特定のユーザがサイトにアクセスしている間に実行することを追跡します（アクセス中にユーザが表示したページなど）。
- 特定のユーザに対してパーソナライズされたコンテンツを表示します。

ユーザが匿名認証方式によって保護されたリソースをリクエストすると、ポリシー サーバは GUID （グローバル一意識別子）を割り当てて、関連するユーザのブラウザに格納します。 SiteMinder は、この GUID を使用してユーザを識別します。

匿名認証方式を使用する場合は、以下のアイテムを実装すると、SiteMinder 環境のパフォーマンスが向上する可能性があります。

- 匿名のリクエストを処理する個別の Web サーバ。
- それぞれの Web サーバ上で Web エージェントを設定し、CacheAnonymous パラメータを設定することによって匿名のリクエストをキャッシュします。

個別の Web サーバおよび Web エージェントを匿名のユーザに対して使用することにより、保護されたリソースに対するリクエストを処理する他の Web サーバ上のキャッシュが頻繁にフラッシュされないようにします。

注: 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。

Web エージェントのパフォーマンスに影響する他のパラメータ

以下のパラメータも Web エージェントのパフォーマンスに影響します。

- PSPollInterval
- IgnoreExt
- IgnoreURL

ポリシー サーバのポーリング間隔パラメータ

SiteMinder エージェントは定期的にポリシー サーバに問い合わせて、更新されたポリシーまたは暗号化キーを受信します。 ポリシー サーバに問い合わせる時間間隔は、PSPollInterval エージェント設定パラメータの変更によって調整できます。

時間間隔を増やすことで、エージェントとポリシー サーバの間の不要なトラフィックを低減できます。SiteMinder 環境に以下のいずれかの特徴がある場合は、間隔の増加を検討してください。

- 多数のエージェントがあります。
- ほとんどの SiteMinder ポリシーは静的であり、頻繁に変わることはありません。

  注: 詳細については、各エージェントの「エージェント設定ガイド」または「エージェント ガイド」を参照してください。

重要: PSPollInterval パラメータを増加させると、Web エージェントで SiteMinder ポリシー変更が提供されるタイミングにも影響があります。たとえば、勤務が終了した従業員のアクセスを無効にするため、10:30 にポリシーを変更し、PSPollInterval パラメータの値が 3600 （1 時間の秒数）であるとします。 この場合、Web エージェントでは、変更されたポリシーを 11:30 まで適用しません。

拡張パラメータの無視

SiteMinder で保護するリソースに保護*しない*多くのイメージまたはファイルが含まれる場合、特定のファイル拡張子を無視するように Web エージェントを設定することにより、Web エージェントとポリシー サーバの間のトラフィックを低減できます。

Web エージェントはポリシー サーバに対して次の呼び出しを行わ*ない*ため、パフォーマンスが向上します。

- IsProtected
- IsAuthenticated
- IsAuthorized
- ログイン

関連付けられたリソースの要求は Web サーバに直接渡され、ユーザはアクセスを付与されます。

最初に保護するリソースを特定すると、Web エージェントに無視させるファイル拡張子があれば、その決定に役立つ場合があります。

無視するすべてのファイル拡張子を Web エージェント設定の IgnoreExt パラメータに追加します。

注: 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。

詳細情報:

保護するアプリケーションの識別 (P. 68)

URL パラメータの無視

特定のサブディレクトリのリソースを非保護のままにする場合、特定の URI （Uniform Resource Identifier）を無視するように Web エージェントを設定できます。

たとえば、各 Web サーバに pictures という名前のサブディレクトリがあり、それらのディレクトリを非保護のままにする場合、Web エージェント設定で IgnoreURL パラメータを設定できます。

Web エージェントはポリシー サーバに対して次の呼び出しを行わないため、パフォーマンスが向上します。

- IsProtected
- IsAuthenticated
- IsAuthorized
- ログイン

関連付けられたリソースの要求は Web サーバに直接渡され、ユーザはアクセスを付与されます。

ロード バランシングによるエージェント パフォーマンスの向上

複数の SiteMinder エージェントとポリシー サーバがあるときは、ダイナミック ロード バランシングによって遅延が軽減され、スループットが向上します。これはエージェントがすべてのポリシー サーバ間でリクエストを分散させるためです。 ダイナミック ロード バランシングを使用すると、エージェントはポリシー サーバに迅速にアクセスできるようになり、認証および許可の効率が向上します。

SiteMinder は、複数のポリシー サーバとのその通信でソフトウェア ベースのフェールオーバおよびロード バランシングを提供します。 ［ホスト設定オブジェクト］の EnableFailover パラメータでは、以下のいずれかの値を使用して、Web エージェント接続の処理方法を決定します。

- 値が yes に設定されていると、エージェントは常に、［ホスト設定オブジェクト］でリスト表示された（左から右に）最初のポリシー サーバに接続しようとします。複数のポリシー サーバがある場合、すべてのエージェントは最初のポリシー サーバへの接続を試行します。リスト内の最初のサーバが利用不能でない限り、リスト内の他のサーバはアクセスされません。高ボリューム環境では、この設定はロード バランシングよりも効率が低くなります。これは一部のポリシー サーバで多くの接続を処理する一方で、他のポリシー サーバで少ない接続（存在する場合）が処理されるためです。
- 値が no に設定されていると、ロード バランシングが有効になります。エージェントは、［ホスト設定オブジェクト］にリストされているすべてのポリシー サーバ間で、ラウンド ロビン方法によりそれらのリクエストを負荷分散させます。複数のポリシー サーバを使用するときにスループットが向上するので、この設定をお勧めします。ロード バランシング ポリシー サーバの 1 つが利用不能になると、引き続きフェールオーバが行われます。

  注: 詳細については、「*SiteMinder ポリシー サーバ設定ガイド*」を参照してください。

また、SiteMinder は、SiteMinder エージェントとポリシー サーバの間の接続の高度なダイナミック ロード バランシングを提供するためにハードウェア ロード バランサの使用をサポートします。仮想 IP アドレスによって複数のポリシー サーバを表示するように設定すると、ハードウェア ロード バランサはその仮想アドレスと関連付けられたすべてのポリシー サーバ間の負荷の分散を処理します。 エージェントはフェールオーバまたはロード バランシングを処理する必要がないので、SiteMinder ロード バランシングを無効にするために EnableFailover パラメータを yes に設定します。 ［ホスト設定オブジェクト］内のポリシー サーバのグループを表示する VIP（複数可）のみを設定します。

マルチスレッド Web およびアプリケーション サーバの場合の SiteMinder フェールオーバおよびロード バランシング

マルチスレッド Web およびアプリケーション サーバ（Sun Java System、IIS、worker モードの Apache ベース サーバまたは WebSphere Application Server など）上で実行される SiteMinder エージェントは、起動時にポリシー サーバに対して最小数のソケットを開きます。

使用している環境で、ポリシー サーバ間のフェールオーバまたはロード バランシングを設定すると、エージェントは、起動時に最小数のソケットを開きます。 負荷分散されたポリシー サーバへの接続は同じ方法で行われますが、それぞれのポリシー サーバに対しより少ないソケットが開かれます。これはそれぞれがリクエストの合計の半分のみを取得するためです。

フェールオーバを設定している場合、エージェントとプライマリ ポリシー サーバの間に通信エラーが発生すると、フェールオーバ ポリシー サーバへの接続が使用されます。 フェールオーバはサーバごとに行われるため、プライマリ ポリシー サーバへの接続とフェールオーバ ポリシー サーバへの接続が同時にアクティブになることがあります。 プライマリ ポリシー サーバが復旧しても、フェールオーバ サーバに対するソケットは開いたままです。 新しいソケットはすべて、プライマリ ポリシー サーバに対して開かれます。

詳細情報:

Apache ベースの Web サーバ ワーカー モードを使用する Web エージェントとポリシー サーバの通信 (P. 180)

マルチプロセス Web およびアプリケーション サーバの場合の SiteMinder フェールオーバおよびロード バランシング

マルチプロセス Web またはアプリケーション サーバ（pre-fork モードで実行される Apache ベース サーバなど）上で実行される SiteMinder エージェントは、フェールオーバが行われるかどうかにかかわらず、すべての設定済みポリシー サーバに対し同数の接続を開きます。

フェールオーバは、それぞれの子から独立して行われます。これは、それぞれの子プロセスにポリシー サーバに対する独自の接続が存在するためです。このため、フェールオーバの実行によって、各ソケットに関する 500 エラーが発生します。 プライマリ ポリシー サーバの復旧後に、フェールオーバ サーバに対するソケットは開いたままです。 新しいソケットはすべて、プライマリ ポリシー サーバに対して開かれます。

詳細情報:

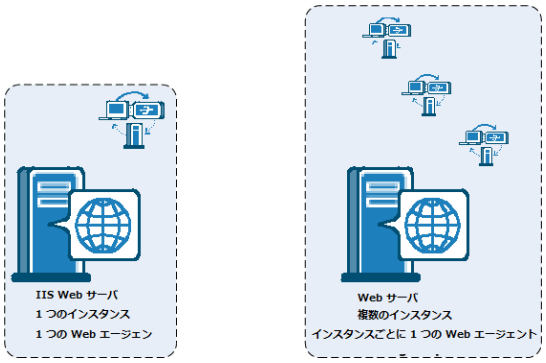
Apache ベースの Web サーバ プリフォーク モードを使用する Web エージェントとポリシー サーバの通信 (P. 180)

Web サーバ、Web エージェント、および Web サーバ プロセス

各 SiteMinder エージェントには、専用の Web サーバ インスタンスが必要です。 たとえば、IIS Web サーバはインストールされたコンピュータの単一のインスタンスを使用して動作します。 IIS エージェント数は IIS Web サーバ数と同じです。

1 台のコンピュータにつき複数のインスタンスをサポートするその他の Web サーバの場合は、各インスタンスに対して 1 つの SiteMinder エージェントをインストールおよび設定できます。 たとえば、1 台のコンピュータで 3 つの個別の Web サーバ インスタンスを実行することができます。 各インスタンスには、専用のエージェントがあります。 そのため、1 台のコンピュータが 3 つの SiteMinder エージェントを操作します。

以下の図に例を示します。



Apache Web サーバの場合、以下のマルチ処理モジュール（MRM）が、SiteMinder エージェント プロセスのポリシー サーバへの接続方法に影響します。

プリフォーク モード

子プロセスを作成して追加のリクエストを処理します。

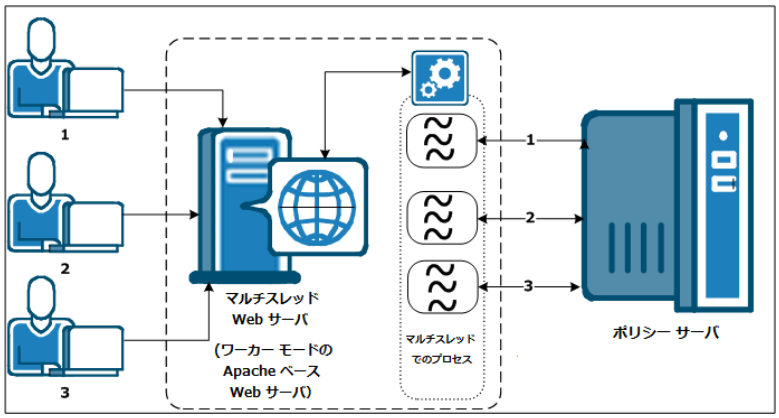
ワーカー モード

接続プールから追加のスレッドを取得して、追加のリクエストを処理します。

Apache ベースの Web サーバ ワーカー モードを使用する Web エージェントとポリシー サーバの通信

ワーカー モードの Apache ベースの Web サーバは、スレッドを使用して SiteMinder ポリシー サーバへの接続を処理します。スレッドは必要に応じて接続プールから取得されて、高負荷時にポリシー サーバへの追加の接続を作成します。

以下の図では、このプロセスについて説明します。



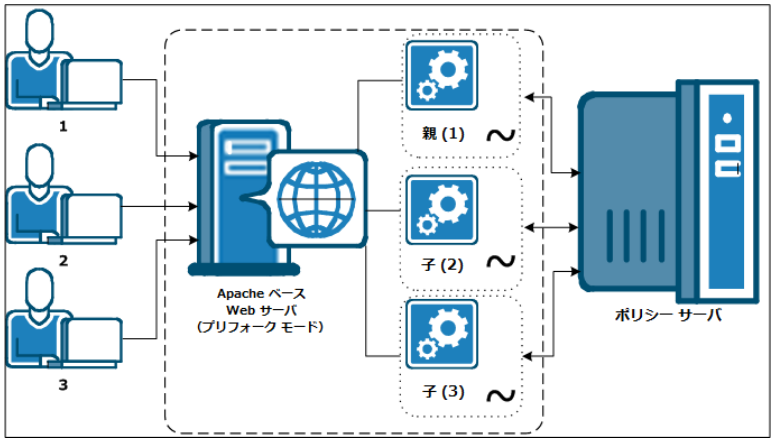
詳細情報:

マルチスレッド Web およびアプリケーション サーバの場合の SiteMinder フェールオーバおよびロード バランシング (P. 177)

Apache ベースの Web サーバ プリフォーク モードを使用する Web エージェントとポリシー サーバの通信

プリフォーク モードの Apache ベースの Web サーバがリクエストを受信すると、Web サーバは子プロセスを生成して SiteMinder ポリシー サーバと通信します。 受け取るリクエストが多いほど、それらを処理するためにスポーンされる子プロセスが多くなります。 Apache ベースの Web サーバによって生成された各子プロセスは、それぞれ独立して SiteMinder ポリシー サーバに接続します。

以下の図では、このプロセスについて説明します。



Apache ベースの Web サーバの場合は、（httpd.conf ファイルの）MaxClients パラメータの値によって、Web サーバで生成される子プロセスの数が決まります。 Apache ベースの Web サーバの親プロセスによって子プロセスが生成されると、子プロセスは SiteMinder ポリシー サーバへの初期接続を開始します。

Web エージェントの数と Web エージェント プロセスの数の間には重要な違いが存在します。各 Web エージェントにはそれ自身の Web サーバ インスタンスが必要です。 たとえば、IIS Web サーバは単一のインスタンスとしてのみ動作するので、IIS Web エージェント数は IIS Web サーバ数と同じです。 他のタイプのサーバの場合、1 つの物理 Web サーバ内の異なるポートで複数のサーバ インスタンスがリスニングすることが可能です。

Apache ベースの Web サーバから SiteMinder ポリシー サーバに対して開かれるソケットの最大数は、Web エージェント プロセスの数を乗算した MaxClients パラメータの値です。 たとえば、サーバの MaxClients パラメータの値が 150 に設定され、5 つの Web エージェント プロセスがある場合、開くことができるソケットの最大数は 750 です。

マルチプロセス Web サーバの使用は、SiteMinder 環境のポリシー サーバに対する Web エージェント プロセスの割合に影響します。 制限要因は、多くの場合に毎秒のトランザクション数ではなく、 Web エージェント プロセスとポリシー サーバの間の接続数になります。

Web エージェントを展開する前に、リクエストを受信する SiteMinder ポリシー サーバが、関連する Web サーバが開くことができる接続の最大数を処理できることを確認します。

詳細情報:

マルチプロセス Web およびアプリケーション サーバの場合の SiteMinder フェールオーバおよびロード バランシング (P. 178)

アプリケーション層のパフォーマンス

ポリシー サーバは、アプリケーション層のポリシー、およびデータ層のユーザ認証情報および属性を評価してリソースを保護します。 アプリケーション層を調整するパフォーマンスに対する以下のガイドラインを考慮してください。

- ユーザの認証に必要なシステム リソースの量はパフォーマンスに影響します。
- ユーザの許可に必要なシステム リソースの量はパフォーマンスに影響します。
- 認証および許可中の SiteMinder ユーザ ディレクトリへのポリシー サーバ リクエストの数はパフォーマンスに影響します。

SiteMinder ポリシー設計およびパフォーマンス

SiteMinder ポリシーによって、ユーザがリソースと対話する方法が定義されます。管理 UI で SiteMinder ポリシーを作成すると、ユーザ、リソース、リソースに関連するアクションを識別するさまざまなオブジェクトが結び付けられます（バインドされます）。

特定の SiteMinder コンポーネントを設定する方法で、またはオプション機能を有効にすることによって、パフォーマンスを向上または低下させる場合があります。 パフォーマンス戦略には以下が含まれます。

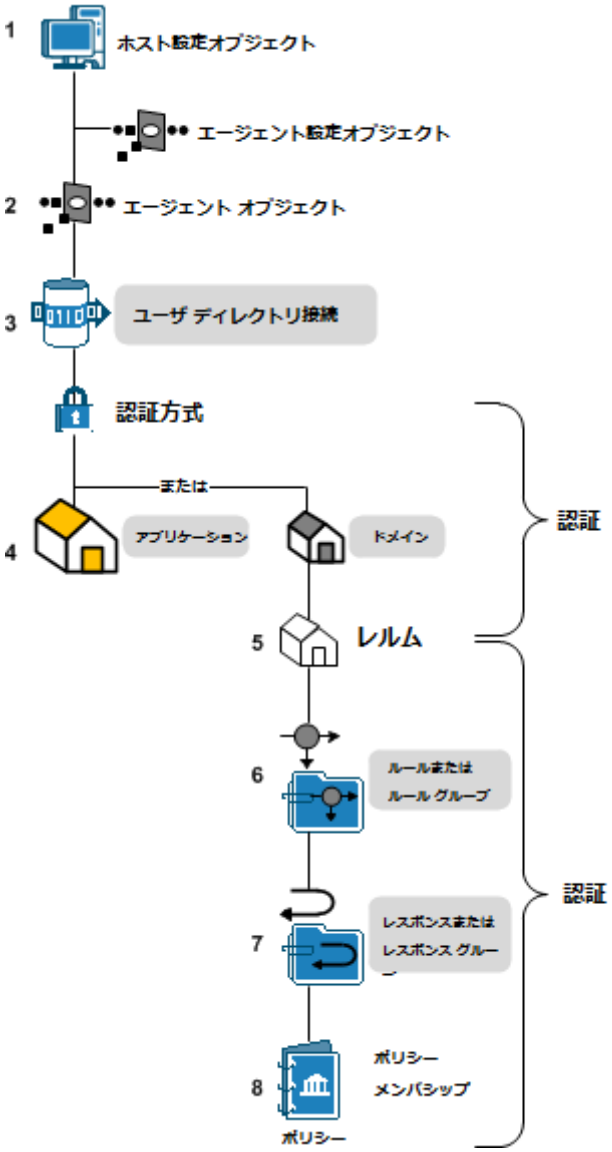
- パフォーマンスに影響する可能性がある SiteMinder ポリシー オブジェクトを特定する
- ユーザ認証に影響する SiteMinder パラメータおよび機能の特定
- ユーザ許可に影響する SiteMinder パラメータおよび機能の特定

最終的には企業のビジネス ルールおよびセキュリティ要件によって SiteMinder ポリシー設計を指定する必要があります。以下のガイドラインは、これらの要件を満たすと同時に SiteMinder のパフォーマンスのバランスを保つために役立ちます。

SiteMinder ポリシー オブジェクトおよびパフォーマンス ロードマップ

SiteMinder では、特定の順序でコア SiteMinder ポリシー オブジェクトを設定する必要があります。 以下の図にこの順序を一覧表示します。グレー表示された項目は、ユーザ認証または許可中のパフォーマンスに影響するオブジェクトを表します。

注: ホスト設定オブジェクト（HCO）およびエージェント設定オブジェクト（ACO）は、Web 層のパフォーマンスに影響します。



詳細情報:

Web 層のパフォーマンス (P. 160)

アプリケーション

アプリケーションの設定方法によって、認証および許可中のパフォーマンスを向上または低下させる場合があります。

アプリケーションは、1 つ以上の関連する Web サービスの完全なセキュリティ ポリシーを定義するポリシー サーバ オブジェクトです。アプリケーションは、Web サービス リソースをユーザ ロールと関連付けて、どの Web サービス ユーザがどの Web サービス アプリケーション リソースにアクセスできるかを決める資格ポリシーを指定します

アプリケーションを作成すると、それをポリシー サーバがユーザ認証を試行する 1 つ以上のユーザ ディレクトリ接続にバインドします。 そのため、ディレクトリ接続の数、およびそれらがリストされている順序は、認証中の SiteMinder のパフォーマンスに直接影響します。

アプリケーションで保護されたリソースとして定義されている Web サービス ポートおよび操作の数は、許可中の SiteMinder のパフォーマンスに相関します。

リソースは 1 つ以上のレスポンスにバインドできます。リソースにアクセスすると、関連するレスポンスがユーザ属性、DN 属性、静的なテキスト、またはカスタマイズされたアクティブなレスポンスなどの情報をエージェントに返します。

Web サービス リソースにバインドするレスポンスのタイプは、許可中の SiteMinder のパフォーマンスと直接相関します。

ドメイン

ドメインを設定する方法によって、認証中のパフォーマンスを向上または低下させる場合があります。

SiteMinder ポリシードメインは、1 つ以上のユーザ ディレクトリに関連したリソースの論理グループです。 ドメインの作成時に、1 つ以上のユーザ ディレクトリ接続をドメインにバインドします。

ポリシー サーバは、これらのディレクトリ接続を使用して、ユーザの認証を試行します。 そのため、ディレクトリ接続の数、およびそれらが一覧表示されている順序は、認証中の SiteMinder のパフォーマンスと直接相関します。

注: ドメイン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。

詳細情報:

ドメインまたは EPM アプリケーションへのリソースのグループ化 (P. 69)
ドメインおよび認証パフォーマンス (P. 192)

レルム

レルムを設定する方法によって、認証中のパフォーマンスを向上または低下させる場合があります。

ドメインのリソースを 1 つ以上のレルムにグループ化します。レルムとは、共通のセキュリティ（認証）要件を持つリソース（URL）のセットです。定義するリソース フィルタおよび選択する認証方式は、認証中のパフォーマンスと直接相関します。

- リソース フィルタは保護されたリソースのルートとして機能します。ポリシー サーバは、リソース フィルタを評価してリクエストされたリソースが保護されているかどうかを判断する必要があります（IsProtected?）。
- レルムに関連付けられた認証方式によって、ユーザがレルム内のリソースへのアクセス権を取得するために示す必要がある認証情報のタイプが決まります（IsAuthenticated?）。

レルム設定によって、以下のことも決定します。

- SiteMinder によるユーザ セッションの処理方法。 SiteMinder は、ユーザが認証されたレルムのコンテキストでユーザ セッションを作成します。
- 認証中にアクションを制御するためにレルムを使用できるかどうか。

注: レルムの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。 認証方式の詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

詳細情報:

レルムまたは EPM コンポーネントへの複数のリソースのグループ化 (P. 70)
レルムおよび認証パフォーマンス (P. 193)

ルールおよびルール グループ

レルムを設定する方法によって、許可中のパフォーマンスを向上または低下させる場合があります。

レルムのコンテキストでルールまたはルール グループを作成します。
ルール

- 保護を必要とするレルム内の特定のリソースを識別する
- 特定の認証または許可イベントに基づいて、リソースへのアクセスを許可または拒否するために使用される場合があります。

ルールで定義するリソース フィルタ（その前にはレルム フィルタが付いている）は、保護を必要とするリソースを識別します。

ポリシー サーバはルールを評価して、リクエストされたリソースに一致するリソース フィルタを決定します。 一致に際して、ポリシー サーバはルールがバインドされたポリシーを起動して、ユーザがリソースへのアクセスを許可されているかどうかを判断します。

レルム内のルールの数および各リソース フィルタの定義方法は、許可の間の SiteMinder のパフォーマンスと直接関係します。

注: ルールの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

詳細情報:

ルールおよび許可パフォーマンス (P. 195)

レスポンス

レスポンスを設定する方法によって、許可中のパフォーマンスを向上または低下させる場合があります。

レスポンスまたはレスポンス グループは特定のルールまたはルール グループにバインドされます。 ルールの起動時に、レスポンスは以下を実行できます。

- ユーザ セッションが有効である期間をカスタマイズします。
- ユーザをほかのリソースにリダイレクトします。
- ユーザ ディレクトリに含まれる属性に基づいて、ユーザが受信するコンテンツをカスタマイズします。
- スタティック テキスト、ユーザ属性、DN 属性、カスタマイズされたアクティブ レスポンス、または定義された変数のランタイム値をポリシー サーバから SiteMinder エージェントに渡します。
- WS-Security ヘッダおよび SAML セッション チケットを生成するように SiteMinder WSS エージェント に指示します。

ポリシー ルールは 1 つ以上のレスポンスにバインドできます。SiteMinder ポリシー ルールにバインドするレスポンスのタイプは、許可中の SiteMinder のパフォーマンスと直接相関します。

注: レスポンスの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

詳細情報:

レスポンスおよび許可パフォーマンス (P. 196)

認証ガイドライン

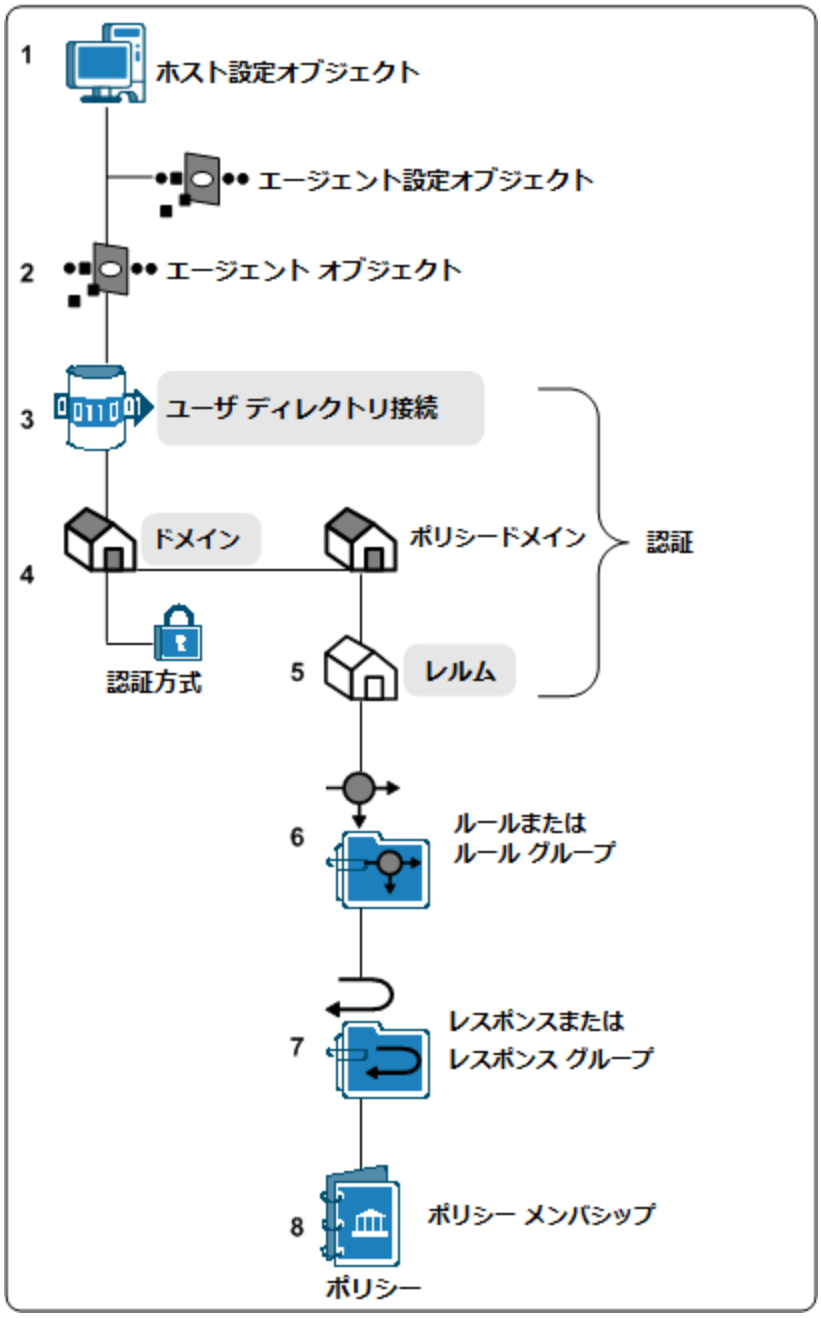
通常、認証（IsAuthenticated?）手順中の SiteMinder パフォーマンスは以下と相関します。

- 認証リクエストの処理に使用されるシステム リソース
- ポリシー サーバが認証リクエストを処理するために SiteMinder ユーザ ディレクトリに対して行う読み取り/書き込み（リクエストと総称される）の数

SiteMinder ポリシー オブジェクトおよびパフォーマンス ロードマップ

特定の SiteMinder ポリシー オブジェクトの設定方法に応じて、またはそれらのオブジェクトに関連付けられたオプション機能を有効にすることによって、認証パフォーマンスが向上または低下する場合があります。

SiteMinder では、特定の順序でコア SiteMinder ポリシー オブジェクトを設定する必要があります。 以下の図にこの順序を一覧表示します。グレー表示された項目は、ユーザ認証中のパフォーマンスに影響するオブジェクトを表します。


1
ホスト設定オブジェクト
エージェント設定オブジェクト
2
エージェント オブジェクト
3
ユーザ ディレクトリ接続
4
ドメイン
ポリシードメイン
認証
認証方式
5
レルム
6
ルールまたは
ルール グループ
7
レスポンスまたは
レスポンス グループ
8
ポリシー メンバシップ
ポリシー

ユーザ ディレクトリおよび認証パフォーマンス

ドメインの設定では、1 つ以上のユーザ ディレクトリ接続をドメインにバインドする必要があります。 ポリシー サーバはユーザ ディレクトリ接続で指定する検索条件を使用して、認証手順中にユーザ認証情報を確認します。

注: ユーザ ディレクトリ接続の設定の詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

以下の要因がディレクトリ レベルでユーザ認証のパフォーマンスに影響します。

- 式およびクエリの検索 -- LDAP 式または ODBC クエリが複雑であるほど、ポリシー サーバが条件を解決してユーザを認証するために時間がかかります。
- パスワード サービス -- パスワード ポリシーを SiteMinder ユーザ ディレクトリに適用できます。パスワード ポリシーの実装前に以下の点について考慮してください。
  - ポリシー サーバはパスワード ポリシーに関連する属性を読み取り、それらを更新する必要がある場合があります。 属性の更新には、ポリシー サーバによるユーザ ディレクトリへの書き込みが必要です。
  - ログイン詳細を追跡するようにパスワード ポリシーが設定されている場合、すべての認証で追加のユーザ ディレクトリ書き込みが必要です。
  - ポリシー サーバが、ディレクトリ全体ではなく、ディレクトリ内の特定のユーザ グループにのみ適用されるパスワード ポリシーを解決する場合に、より時間がかかります。

eTrust SOA Security Manager 認証方式および認証パフォーマンス

eTrust SOA Security Manager 認証方式によって、オーバーヘッドを処理する WSS エージェントのレベルが異なります。 これは WSS エージェントのタイプによっても変わる場合があります。

一般的に、認証のスループットは、デジタル署名の検証やペイロードの機密性を必要としない認証方式に対して高くなります。

デジタル署名の検証は、Web サーバの WSS エージェントで CPU に負担がかかり、データ量が多くなりますが、アプリケーション サーバの WSS エージェントにも多少影響を与えます。

ドメインおよび認証パフォーマンス

以下の要因が、ドメイン（またはアプリケーション オブジェクト）レベルでユーザ認証のパフォーマンスに影響します。

- ドメイン内のディレクトリ接続数 -- ユーザ認証情報を検証できるまで、ポリシー サーバはドメイン内の各ユーザ ディレクトリを検索します。ユーザ ディレクトリ接続数が多いほど、ポリシー サーバによるユーザの認証に時間がかかる場合があります。

  ドメイン内のディレクトリ接続数を減らす方法を評価して、不要なポリシー サーバ リクエストを防止します。 以下について考慮してください。

  - ドメイン内のリソースをリクエストしているユーザ、およびそれらの情報が格納されているディレクトリ
  - 組織を SiteMinder 展開に追加するときのユーザ ディレクトリの組み合わせ

- ユーザ ディレクトリ接続が一覧表示される順序 -- ポリシー サーバは、ドメインによって一覧表示される順にユーザ ディレクトリを検索します。 接続の順序を決定するときに、認証優先度を評価します。 以下について考慮してください。

  - ユーザの大半が特定のディレクトリ（複数可）からアプリケーションにアクセスするかどうか
  - 認証優先度が高い小規模なユーザ グループが存在するかどうか

レルムおよび認証パフォーマンス

以下の要因はレルム（またはアプリケーション オブジェクト コンポーネント）レベルでユーザ認証のパフォーマンスに影響します。 レルムを設定する際に、以下のそれぞれを考慮してください。

- 認証情報コレクション -- レルムは特定の認証方式に関連付けられ、その一部は認証情報コレクタの使用を必要とします。 これらのタイプの認証方式でリソースを保護するエージェントは、認証情報を収集するためにユーザを認証情報コレクタにリダイレクトします。 認証情報の収集により、認証プロセスに手順が追加されます。

  注: 認証方式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。 認証情報コレクタ使用の詳細については、「*Web エージェント設定ガイド*」を参照してください。

- 永続セッション -- SiteMinder がユーザを認証するときに、ポリシー サーバはセッション チケットを発行します。 セッション チケットには、ユーザの基本情報およびユーザの認証コンテキストが含まれます。デフォルトでは、SiteMinder は、非永続セッション（エージェントはそのセッション チケットをユーザの Web ブラウザの Cookie に書き込む）によってセッション管理を実装します。

  SiteMinder 機能によっては永続セッションが必要な場合があります。永続セッションに対してレルムを設定できます。 このレルムのリソースを保護するエージェントはセッション チケットを SiteMinder セッション ストアに書き込み、それにより各認証でセッション ストアに追加のリクエストが発生します。

  重要: 永続セッションはパフォーマンスに重大な影響を及ぼす場合があります。

  注: ユーザ セッションの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

- 認証イベント -- デフォルトでは、レルムは［認証イベントの処理］に設定されます。 この設定によって、ユーザが認証するとき、または認証に失敗するときに起動するルールを定義できます。 ポリシー評価ロジックは、認証イベントを処理するように設定されたすべてのレルムに適用されます。 このロジックはシステム リソースを消費し、ユーザ ディレクトリ リクエストをもたらす場合があります。

  ユーザがリソースへのアクセスを取得するために認証する場合に発生するイベント アクションの必要性を評価します。認証アクションを必要としない場合は、レルムに対して認証イベントを無効にして、認証手順を促進します。

  注: レルムの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

許可ガイドライン

通常、許可手順中の SiteMinder パフォーマンスは以下と相関します。

- 許可リクエストの処理に使用されるシステム リソース。
- ポリシー サーバが許可リクエストを処理するために SiteMinder ユーザ ディレクトリに対して行う読み取り/書き込み（リクエストと総称される）の数。

SiteMinder ポリシー設計の複雑さは、これらの各領域に影響します。

ポリシー オブジェクトおよびパフォーマンス

特定の SiteMinder ポリシー オブジェクトの設定方法によって、またはそれらのオブジェクトと関連付けられたオプション機能を有効にすることによって、認証のパフォーマンスを向上または低下させる場合があります。以下のポリシー オブジェクトは、ユーザの許可中にパフォーマンスに影響を与える場合があります。

- ルール（P. 195）
- レスポンス（P. 196）
- ポリシー メンバシップ（P. 197）

ルールおよび許可パフォーマンス

以下の要因がルール（またはアプリケーション オブジェクト リソース）レベルでユーザ許可のパフォーマンスに影響します。

- 単一のレルム内の多数のルールによって許可決定が遅くなる場合があります。 ユーザが特定のレルムに対して認証される場合、ポリシー サーバはレルム内のすべてのルールを評価して、ユーザがリクエストしている特定のリソース（URL）に一致するリソース フィルタを決定する必要があります。
- リソース フィルタのタイプは、ポリシー サーバがリソース一致を評価する速さに影響します。

注: ルールの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

以下のフィルタが、パフォーマンスに及ぼす影響が小さい順に一覧表示されます。

- 完全一致 -- 特定のリソースによるリソース フィルタの定義がパフォーマンスに及ぼす影響は最小です。 ポリシー サーバは、リソース フィルタとリクエストされたリソースの URL との比較のみを行う必要があります。

  例： ある会社はカスタマ レルム（/customer）を作成し、ポータル アプリケーションの特定のページ（lending_home.html）でルールを指定します。 この結果、リソース フィルタは /customer/lending_home.html です。 リクエストされたリソースとルールの一致を評価するために必要なことは、ポリシー サーバがリクエストされたリソースをリソース フィルタと比較してそれが一致するかどうかを判断することのみです。

- 完全なプレフィックス -- プレフィックスでリソース フィルタを定義すると、完全一致よりパォーマンスへの影響が大きくなります。ポリシー サーバは、リクエストされたリソースがリソースのルート（レルム）内に含まれているかどうかを判断する必要があります。

  例： ある会社は従業員レルム（/employee）を作成し、「*.html」でルールを指定します。 * プレフィックスは、従業員レルムのすべての html ファイルが保護されることを指定します。 この結果、リソース フィルタは /employee /*.html です。 リクエストされたリソースとリソース フィルタの一致を評価するには、リクエストされたリソースが従業員ディレクトリの一部で、HTML ファイルであるかどうかをポリシー サーバが評価する必要があります。

- 正規表現 -- 正規表現によるリソース フィルタの定義はパフォーマンスに最大の影響を及ぼします。 ポリシー サーバは式を評価し、その結果をリクエストされたリソースと比較する必要があります。式の複雑さはさらにパフォーマンスに影響します。

レスポンスおよび許可パフォーマンス

SiteMinder ポリシーのルールにバインドされたレスポンス属性のタイプは、パフォーマンスに影響します。以下のレスポンス タイプが、パフォーマンスに及ぼす影響が小さい順に一覧表示されます。

- スタティック -- スタティック属性を定義すると、不変のデータを返します。
- ユーザ属性 -- ユーザ属性を定義すると、ユーザ ディレクトリのユーザのエントリからプロファイル情報を返します。

  注: このタイプのレスポンスには、ポリシー サーバによるユーザ ディレクトリの検索が必要です。

- DN 属性 -- DN 属性を定義すると、ユーザが関連するディレクトリ オブジェクトに関連付けられた情報を返します。 ユーザが所属するグループ、およびユーザ DN の一部である組織単位（OU）は、属性を DN 属性として扱うことのできるディレクトリ オブジェクトの例です。

  注: このタイプのレスポンスには、ポリシー サーバによるユーザ ディレクトリの検索が必要です。

SiteMinder ポリシー メンバシップおよび許可パフォーマンス

ポリシー メンバシップは、ポリシーに適用されるユーザを指定する SiteMinder ポリシーの一部です。 SiteMinder ポリシーがドメインに格納されるため、フィルタを使用して、ドメインにバインドされたユーザ ディレクトリに格納されたいずれかまたはすべてのユーザに SiteMinder ポリシー メンバシップを適用します。 定義するフィルタのタイプによって、ポリシー サーバが SiteMinder ポリシー メンバシップを評価する方法が決まります。

注: SiteMinder ポリシーへのユーザの追加の詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

以下のフィルタが、パフォーマンスに及ぼす影響が小さい順に一覧表示されます。

- すべて -- 「すべて」がパフォーマンスに及ぼす影響は最小です。

  SiteMinder がユーザを認証するときに、ポリシー サーバはセッション チケットを発行します。セッション チケットによって、ユーザが格納されているユーザ ディレクトリが識別されます。 ポリシー サーバは、ポリシーがユーザに適用されることを判断するために、SiteMinder ポリシーにバインドされたディレクトリとセッション チケットの比較のみを行う必要があります。

  注: ユーザ セッションの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

- 識別名 -- 識別名（dn）は、「すべて」より大きな影響をパフォーマンスに及ぼします。

  認証されたユーザの dn を含む組織または組織単位は、セッション チケットに格納されます。 ポリシー サーバはセッション チケット情報を SiteMinder ポリシー メンバシップ フィルタと比較して、ポリシーがユーザに適用されるかどうかを判断する必要があります。

- グループ メンバシップまたは検索式 -- これらのタイプのフィルタは、識別名より大きな影響をパフォーマンスに及ぼします。グループ メンバシップおよび検索式はシステム リソースをさらに消費し、ユーザ ディレクトリ検索をもたらします。ポリシー サーバは以下を実行する必要があります。

  a. グループ メンバシップまたは検索式を解決します。

  b. ユーザ ディレクトリを検索して、SiteMinder ポリシーがユーザに適用されるかどうかを判断します。

- ネストされたグループ -- ネストされたグループによる SiteMinder ポリシー メンバシップの定義はパフォーマンスに最大の影響を及ぼします。

  ポリシー サーバは、ディレクトリの各ユーザ グループおよびすべてのサブグループを検索して SiteMinder ポリシーがユーザに適用されるかどうかを判断する必要があります。

  重要: グループ階層が深いディレクトリは、ポリシー サーバがポリシー メンバシップを評価するためにかかる時間に著しい影響を及ぼす場合があります。

注: ユーザ許可キャッシュを有効にして、ポリシー メンバシップを解決するためにポリシー サーバがユーザ ディレクトリに対して行うリクエスト数を減らすことができます。

詳細情報:

ユーザ許可キャッシュ (P. 198)

ユーザ許可キャッシュ

ユーザ許可キャッシュは、ユーザとポリシーの関係を格納することにより SiteMinder ポリシー メンバシップを判断するためのユーザ ディレクトリ リクエストの数を減らします。

注: ユーザ許可キャッシュは、ユーザに関するデータおよびユーザ属性値を格納せず、ユーザ エントリのキャッシュも行いません。

たとえば、3 つのポリシーが「管理者」グループ（ユーザ A が属する）に適用されるように設定されています。ポリシー サーバが最初に SiteMinder ポリシー メンバシップを評価するときに、各 SiteMinder ポリシーが適用されることを判断するために、グループ メンバシップを解決してユーザ ディレクトリに 3 つのリクエスト（ポリシーごとに 1 つ）を行う必要があります。

ポリシー サーバはこれらの結果をユーザ許可キャッシュに書き込みます。後続のポリシー評価では、ポリシー サーバがユーザ ディレクトリ リクエストを行う必要がありません。 その代わりに、ポリシー サーバはキャッシュされた許可情報を使用して、ポリシー メンバシップを判断します。

注: ポリシー サーバは、ポリシー更新に対して定期的にポーリングします。デフォルトの間隔は 60 秒です。 ポリシー メンバシップが変更する場合、ポリシー サーバはポリシーを再ロードして、更新されたポリシーに関連するキャッシュ エントリを削除します。

詳細情報:

SiteMinder ポリシー メンバシップおよび許可パフォーマンス (P. 197)

ユーザ許可キャッシュ効率

ユーザ許可キャッシュは次の場合に最も効果的です。

- セッション中のすべてのユーザ リクエストが、同じサーバに一貫して送信（持続）されます。
- すべての SiteMinder エージェントはラウンド ロビン ロード バランシングではなくポリシー サーバ フェールオーバに対して設定されます。

これらの要因に適合しない場合、ユーザ許可キャッシュの有効性は低下します。

例: ラウンド ロビン方式で負荷分散するように設定されたユーザ許可キャッシュおよびエージェント

SiteMinder エージェント ラウンド ロビン プール内のポリシー サーバが多いほど、ユーザ許可キャッシュの効率が下がる可能性が高くなります。

単一の SiteMinder エージェントが 2 つのポリシー サーバ間でラウンド ロビンするように設定されている場合、保護されたリソースへの最初のリクエストによっていずれかのポリシー サーバのユーザ許可キャッシュ エントリが生じます。 キャッシュ エントリがないポリシー サーバが 2 番目のリクエストを処理する必要がある可能性は、約 50 パーセントです。 ただし、両方のポリシー サーバは後のリクエスト用にデータをキャッシュしています。

では、10 のポリシー サーバ間でラウンド ロビンするように設定された単一のエージェントの影響について考えてみましょう。 ポリシー サーバがユーザを許可して、その結果を許可キャッシュに入力した後、同じポリシー サーバが次のリクエストを処理する可能性は 10 パーセントのみです。この設定では、キャッシュ ヒットの可能性が 50 パーセントになる前に、必ずキャッシュ ミスが 5 回発生します。

注: ポリシー サーバ クラスタは、ラウンドロビン ロード バランシングがユーザ許可キャッシュに対して持っている効果を低下させることがあります。

ユーザ許可キャッシュのサイズの概算

ユーザ許可キャッシュのデフォルト サイズは 10 MB です。 ユーザ許可キャッシュに必要な容量を概算し、ポリシー サーバ管理コンソールを使用してデフォルト サイズを調整できます。

ユーザ許可キャッシュのサイズを概算する方法

1. 以下の式を使用してキャッシュ エントリの数を概算します。

   *expected_users * number_of_policies_per_session = entries*

   expected_users

   SiteMinder が保護しているアプリケーションに対して認証するユーザの総数を指定します。

   number_of_policies_per_session

   セッション中にユーザに適用される SiteMinder ポリシーの平均数を指定します。

   注: 各 SiteMinder ポリシーは、ユーザ許可キャッシュに一意のエントリを入力する可能性があります。

   エントリ

   許可によって作成できるキャッシュ エントリの数を指定します。

2. 以下の式を使用してキャッシュのサイズを概算します。

   （*エントリ* * .000062） + 1

   注: .000062 は、MB でキャッシュ エントリの近似サイズを表します。

監査およびパフォーマンス

デフォルトでは、ポリシー サーバはポリシー サーバ ログと呼ばれるテキスト ファイルに監査イベントを書き込みます。 オプションで、監査データベースにイベントをログ記録するようにポリシー サーバを設定できます。

注: 監査データベースにイベントをログ記録するためのポリシー サーバ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。監査データベースの設定の詳細については、「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。

イベントを監査データベースにログ記録する場合は、以下の要因を考慮してください。

- SiteMinder は認証および許可に関するすべての決定をデータベースに記録するので、認証および許可に関連するパフォーマンスが影響を受けます。
- （オプション）同期ログ記録 -- レルム レベルで同期ログ記録を設定できます。 これを設定した場合、レコードが監査データベースに保存されるまで、ポリシー サーバは各認証および許可リクエストの結果を防止します。 レコードが保存されるまで、ユーザは認証または許可されません。

アプリケーション層の負荷分散

さまざまな SiteMinder エージェント パラメータを調整したり SiteMinder ポリシー設計ガイドラインに従っても、ポリシー サーバが認証および許可リクエストを処理するためにかかる時間はほとんど改善しません。

複数のエージェントおよびポリシー サーバがある場合は、エージェントがすべてのポリシー サーバ間でリクエストを分散させるので、ダイナミック ロード バランシングによって遅延が軽減されてスループットが向上します。

詳細情報:

冗長性および高可用性 (P. 38)

データ層のパフォーマンス

SiteMinder データ ストアに関連する貧弱なパフォーマンス（特にユーザ ディレクトリ）は、SiteMinder のパフォーマンスを低下させる最も一般的な原因の 1 つです。データ層のパフォーマンスは、通常以下の 2 つの一般的な領域と相関します。

- データ層自体。正しく調整されていない、またはシステム リソースが十分でないユーザ ディレクトリは、SiteMinder のパフォーマンスを低下させる場合があります。
- ユーザ ディレクトリが動作する容量。 SiteMinder 認証および許可サービスによって、ユーザ ディレクトリへの複数の読み取りおよび書き込み（リクエストと総称される）が生じます。ユーザ ディレクトリ自体で容量計画作業を実行して、ユーザ ディレクトリが SiteMinder 作業負荷を処理できることを確認します。

パフォーマンス戦略には以下が含まれます。

- データ層自体が、貧弱なパフォーマンスの主な原因ではないことを確定する。
- SiteMinder が指定された期間に処理する必要がある認証および許可の数を特定する。

  注: ユーザ認証および許可が発生する持続レートおよびピーク レートを算出できます。
- 各ユーザ認証および後続の許可によって作成されるユーザ ディレクトリ リクエストの数を概算する。

詳細情報:

容量計画が導入されました (P. 107)
導入された eTrust SOA Security Manager 容量計画 (P. 123)

データ層ガイドライン

ポリシー サーバは標準プロトコルを使用してデータ層と対話します。 パフォーマンスを最大化するようにディレクトリ サーバおよびデータベースを標準クライアントで調整すると、これらの変更によって SiteMinder のパフォーマンスが向上する場合があります。

注: 調整の詳細については、ベンダー固有のマニュアルを参照してください。

SiteMinder のパフォーマンスの向上については、ユーザ ディレクトリのパフォーマンスに関連するので、いくつかの一般的な考慮事項があります。以下の領域を検査します。

- ユーザ ディレクトリに使用できるシステム リソースおよびそれらのリソースに対して競合する可能性がある外部リソース
- Secure Socket Layer の使用
- SiteMinder がユーザ ディレクトリを検索できる効果
- スタティック IP アドレスの使用
- レプリケーションの使用

システム リソース

ユーザ ディレクトリに使用できるシステム リソースは、SiteMinder のパフォーマンスと直接相関します。 ユーザ ディレクトリが高レベルの使用率で動作している場合、SiteMinder を調整してもパフォーマンスを向上できません。

ユーザ ディレクトリをホストするシステムが、以下によってパフォーマンスを低下させないことを確認してください。

- 遅い CPU または I/O システム
- メモリの不足
- 正しく設定されていないバッファ キャッシュ
- ディスク領域不足または断片化

Secure Socket Layer およびユーザ ディレクトリ

SiteMinder 環境への SSL の実装を計画している場合は、以下の点について考慮してください。

- SSL を介して通信するようにポリシー サーバおよび LDAP ユーザ ディレクトリを設定すると、パフォーマンスが低下します。 セキュリティ要件を確認して、SSL が必須であるかどうかを判断します。
- SSL を設定する場合は、ポリシー サーバとディレクトリ サーバの間に SSL アクセラレータを配置しないでください。 さもないと、ポリシー サーバはディレクトリの単一のインスタンスを使用します。 これにより、アクセラレータの背後にある複数のユーザ ディレクトリにわたって不整合な書き込みが発生する場合があります。

スタティック IP アドレスおよびユーザ ディレクトリ

管理 UI でユーザ ディレクトリ接続を設定する場合は、ホスト名ではなくスタティック IP アドレスを使用することを検討してください。 ポリシー サーバによるホスト名の解決にかかる時間は無視できますが、スタティック IP アドレスの使用によって、DNS （Domain Naming Services）依存関係が除去されます。

ユーザ ディレクトリの検索

確実に SiteMinder が効率的にユーザ ディレクトリを検索できるようにすることは、パフォーマンスと直接相関します。 以下の点について考慮してください。

- ディレクトリ インデックスを使用して SiteMinder の検索結果を向上します。
  - LDAP -- 検索で使用される他のすべての属性に加えて、objectClass 属性にもインデックスを付ける必要があります。

    注: Microsoft は objectClass の代わりに objectCategory 属性の使用を推奨しています。 Active Directory 内の objectClass 属性にインデックスを付けられないと、パフォーマンスが著しく低下する場合があります。
  - ODBC -- SiteMinder スキーマ クエリで検索条件として定義されたすべてのフィールドにインデックスを付ける必要があります。

    注: インデックス付けの詳細については、ベンダー固有のマニュアルを参照してください。

- 管理しやすいユーザ グループのセットを返すようにクエリを設計します。

  注: クエリを最適化できない場合は、最大の検索結果パラメータを設定して、全体的なパフォーマンスが低下しないように大規模な結果セットを制限します。

- 標準的な SQL アナライザで ODBC の SQL クエリ方式を最適化します。

レプリケーション

レプリケーションは、以下の状況でパフォーマンスを低下させる場合があります。

- マスタ レプリカがマスタ スレーブ レプリケーションで書き込みリクエストのみを許可する場合。 パスワード サービスでは、通常、各認証のパスワード BLOB 属性の更新が必要です。 マスタ レプリカのみが書き込みを処理できる場合、各書き込みリクエストはマスタにリダイレクトされます。

  リダイレクトによって、認証手順でさらに時間がかかるようになり、マスタ レプリカは書き込みが発生するレートに対応できない場合があります。

- LDAP リフェラルが有効な場合。 各リクエストがディレクトリへの複数のリクエストに影響する可能性があるので、LDAP リフェラルによってパフォーマンスが低下する場合があります。

ユーザ ストア容量計画

ポリシー サーバは一連のサービスを実行して、ユーザを認証および許可します。これらのサービスによって、リクエストと総称されるユーザ ディレクトリへの読み取りおよび書き込みが生じます。SiteMinder のパフォーマンスに著しく関与する要因によって、ユーザ ディレクトリが操作の持続期間およびピーク期間にこの作業負荷を処理できるかどうかが決定します。

以下の一般的な要因が SiteMinder のパフォーマンスに影響します。

- 合計操作数および持続ユーザ ディレクトリ検索レート -- 合計操作数は、認証および許可リクエストの処理時に、ポリシー サーバが処理する必要があるリクエストの合計数です。 これらの操作が発生するレートは営業日を通して変動します。

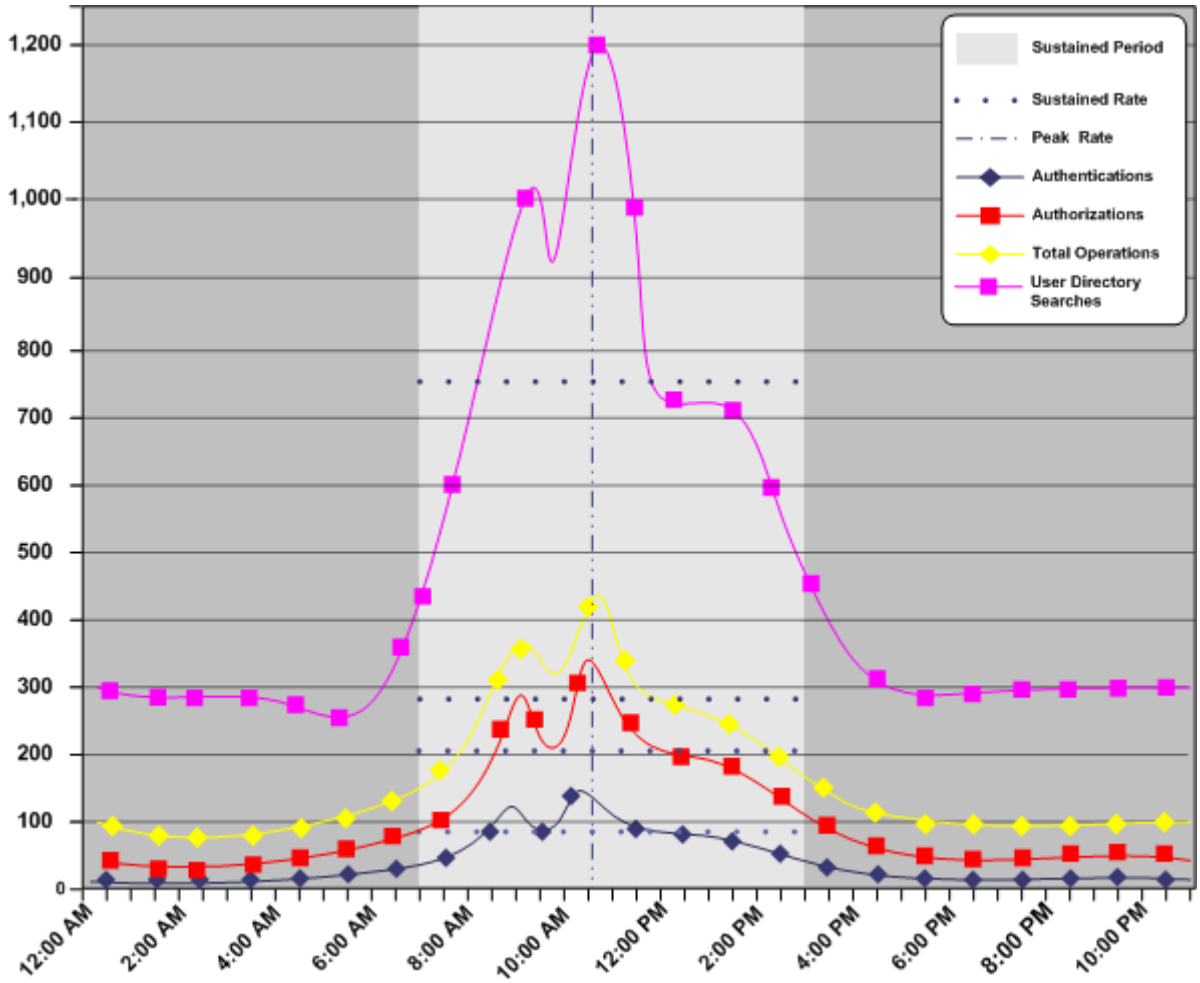
  同様に、ポリシー サーバがユーザ ディレクトリ リクエストを行って操作を処理するレートは変動します。 一部の期間では比較的少数のユーザ ディレクトリ リクエストが生成されますが、その他の期間ではより多くのリクエストが生成されます。

  持続ユーザ ディレクトリ検索レートは、ポリシー サーバが平均数のユーザ ディレクトリ リクエストを行い、平均数の操作を処理する期間を表します。

- 合計操作数およびピーク ユーザ ディレクトリ検索レート -- アクティビティの持続期間中に、ユーザ アクティビティが急増する場合があります。 ピーク ユーザ ディレクトリ検索レートは、ポリシー サーバが最も多くのユーザ ディレクトリ リクエストを行い、最大数の操作を処理する期間を表します。

以下のグラフでは次のことを示します。

- 合計操作数とユーザ ディレクトリ検索レートの関係。
- 各レートが 1 日の間に変動し、特定の期間持続してその期間内にピークに達する様子。



ユーザ ディレクトリが操作する必要があるロードを概算するために以下のガイドラインを使用することをお勧めします。 いったんロードを概算すると、すべての標準ツールを使用してディレクトリでロードを作成し、その結果を追跡できます。

注: 多くの要因によって必要数の獲得に失敗する場合があります。調整の詳細については、ベンダー固有のマニュアルを参照してください。

詳細情報:

ポリシー サーバ (P. 13)
持続認証レートの概算方法 (P. 109)
持続許可レートの概算方法 (P. 115)

ユーザ ストア容量計画のチェックリスト

ポリシー サーバが認証および許可リクエストを処理するために行う必要があるユーザ ディレクトリ リクエスト数の概算には、特定の情報が必要です。 ユーザ ストア容量計画を開始する前に以下の情報を収集します。

- ☐ アプリケーションの日単位の認証総数（認証ロード）。
- ☐ アプリケーションの日単位の許可総数（許可ロード）。
- ☐ ユーザがアプリケーションに対して認証し、保護されたリソースをリクエストする持続期間およびピーク期間。

  注: 容量計画作業は、認証ロード、許可ロード、およびユーザ アクティビティの持続レベルとピーク レベルに関連するメトリックの識別に役立ちます。
- ☐ 有効なポリシーの総数。 各 SiteMinder ポリシーについて、以下の点を判断します。
  - SiteMinder ポリシー メンバシップ フィルタによって 1 つ以上のユーザ ディレクトリ検索が生じるかどうか。
  - SiteMinder ポリシーにバインドされたレスポンスによって 1 つ以上のユーザ ディレクトリ検索が生じるかどうか。

詳細情報:

容量計画が導入されました (P. 107)
SiteMinder ポリシー メンバシップおよび許可パフォーマンス (P. 197)
レスポンスおよび許可パフォーマンス (P. 196)

持続ユーザ ディレクトリ検索レートの概算方法

持続ユーザ ディレクトリ検索レートの概算は、以下のことを特定するプロセスです。

- ユーザ ディレクトリ リクエストの総数は営業日全体でどのように変動するか。
- 持続期間中にユーザ ディレクトリ リクエストが毎秒どのようにリクエストに変換されるか。

以下の手順を実行して、持続ユーザ ディレクトリ検索レートを概算します。

1. 認証ガイドラインを使用して、認証ロードが作成するユーザ ディレクトリ リクエスト数を概算します。
2. 許可ガイドラインを使用して、許可ロードが作成するユーザ ディレクトリ リクエスト数を概算します。
3. 持続ユーザ ディレクトリ検索レートを概算します。

認証ガイドラインの使用によるディレクトリ検索の概算

ポリシー サーバは複数のユーザ ディレクトリ リクエストを行って、各認証リクエストを処理します。 ユーザ ディレクトリ リクエストによっては必須のものがありますが、その他は回避できます。

以下のガイドラインを使用して、各認証が作成するポリシー サーバ リクエスト数を概算します。

（必須）各ユーザを認証する 2 つの検索。

- ユーザを識別するためのストアごとに 1 つの検索/クエリ
- ユーザ認証情報を確認するための 1 つの検索/クエリ

（オプション）ポリシーの設計方法に応じて、およびパスワード サービスを有効にする場合は、さらに検索が必要になる場合があります。

- ユーザが認証されると発生するルール（OnAuth ルール）にバインドされる各 SiteMinder ポリシーの 1 つの検索/クエリ。

  注: ルール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。ルールと SiteMinder ポリシーとの関係の詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

- ユーザ属性を返すレスポンスにバインドされる各 SiteMinder ポリシーの 1 つの検索/クエリ。

  注: レスポンスおよびルールとの関係の詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

- パスワード サービスに対して有効にされたユーザ ストアごとに 1 つの書き込み/更新。パスワード サービスが SiteMinder ポリシー ドメイン内のユーザ ディレクトリに適用されない場合、書き込み/更新は必要ありません。

  注: パスワード サービスの詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

以下のユース ケースでは、各ガイドラインを使用して認証ロードが作成するユーザ ディレクトリ検索の総数を特定する方法を説明します。

ケース 1: ユーザ認証およびディレクトリ リクエスト

ある会社の場合

- バンキング アプリケーションに 1 つのユーザ ディレクトリを展開しました。
- 容量計画作業を実行しました。その結果はユーザが 88,000 ログインの認証ロードを作成することを示します。

会社は以下の式を使用して、ポリシー サーバが認証ロードを処理するためにユーザ ディレクトリに送信するリクエスト数の概算を開始します。

*authentication_load * 2 * number_of_user_stores = requests_for_authentication*

authentication_load

アプリケーションの日単位の認証数を指定します。

注: 2 は定数です。 ユーザの認証によって 2 つのリクエストが発生します。 ユーザを識別するための 1 つの検索と、クレデンシャルを検証するための 1 つのバインド。

number_of_user_stores

実装内のユーザ ストアの数を指定します。

requests_for_authentication

認証ロードが作成するユーザ ディレクトリ リクエストの数を指定します。

結果： 88,000 * 2 * 1 = 176,000 リクエスト

会社はこの概算を使用して、日単位の認証ロードを処理するために必要なユーザ ディレクトリ リクエストの総数を判断します。

ケース 2: ポリシー設計およびユーザ ディレクトリリ クエスト

ある会社は、4 つのポリシーをアプリケーション ポータルを保護するように設定しました（その内の 1 つは認証成功時に起動するルールにバインドされています）。

会社は以下の式を使用して、ポリシー サーバが認証ロードを処理するためにユーザ ディレクトリに送信するリクエスト数の概算を続行します。

authentication_load * (*percent_of_policies* * *number_of_searches*) = *requests_for_authentication*

authentication_load

アプリケーションの日単位の認証数を指定します。

percent_of_policies

有効なポリシーの総数をパーセンテージで指定します。有効なポリシーについては以下のとおりです。

- onAuth ルールにバインドされています
- 同数のユーザ ディレクトリ検索を作成します

例： 4 つの有効な SiteMinder ポリシーが存在します。 1 つは OnAuth ルールにバインドされています。 このポリシーは、1 つのユーザ ディレクトリ検索を生成してポリシー メンバシップを判断します。有効なポリシーの 25 パーセントは認証時に起動して、1 つのユーザ ストア検索を生成します。 残りのポリシーは、認証中に起動しません。

number_of_searches

SiteMinder ポリシーが認証された各ユーザに適用されるかどうかを判断するためにポリシー サーバが行うリクエストの数を指定します。

requests_for_authentication

認証ロードが作成するユーザ ディレクトリ リクエストの数を指定します。

結果： 88,000 * 0.25 * 1 = 22,000 リクエスト

会社はこの概算を使用して、日単位の認証ロードを処理するために必要なユーザ ディレクトリ リクエストの総数を判断します。

ケース 3: レスポンスおよびユーザ ディレクトリ リクエスト

ある会社は、OnAuth ルールを持つ 1 つの SiteMinder ポリシーを定義しました。 このポリシーでは、起動時に共通名（cn）属性レスポンスが返される必要があります。 会社は、この値を返す Web エージェント レスポンスを定義して、SiteMinder ポリシー ルールにバインドします。

会社は以下の式を使用して、ポリシー サーバが認証ロードを処理するためにユーザ ディレクトリに送信するリクエスト数の概算を続行します。

*authentication_load * percent_of_policies * number_of_responses_per_policy = requests_for_authentication*

authentication_load

アプリケーションの日単位の認証数を指定します。

percent_of_policies

ユーザ属性を返す特定の数のレスポンスにバインドされている有効なポリシーの総数をパーセンテージで指定します。

例： 4 つの有効なポリシーがあり、その内の 1 つがレスポンスを使用してユーザ属性を返す場合、ポリシーの 25 パーセントにはユーザ ディレクトリ検索が必要です。

number_of_responses_per_policy

SiteMinder ポリシーにバインドされたレスポンスの数を指定します。

requests_for_authentication

認証ロードが作成するユーザ ディレクトリ リクエストの数を指定します。

結果： 88,000 * 0.25 * 1 = 22,000 リクエスト

会社はこの概算を使用して、日単位の認証ロードを処理するために必要なユーザ ディレクトリ リクエストの総数を判断します。

ケース 4: パスワード サービスおよびディレクトリ リクエスト

ある会社は、ユーザ ストア用のパスワード サービスを有効にしました。会社は以下の式を使用して、ポリシー サーバが認証ロードを処理するためにユーザ ディレクトリに送信するリクエスト数の概算を続行します。

authentication_load * 1 = *requests_for_authentication*

authentication_load

アプリケーションの日単位の認証数を表します。

注: 1 は定数です。 ユーザ ログイン詳細の追跡には、認証ごとにユーザ ディレクトリへの 1 回の書き込みが必要です。

requests_for_authentication

認証ロードが作成するユーザ ディレクトリ リクエストの数を表します。

結果： 88,000 * 1 = 88,000 リクエスト

会社はこの概算を使用して、日単位の認証ロードを処理するために必要なユーザ ディレクトリ リクエストの総数を判断します。

ケース 5: 認証に対するディレクトリ リクエスト総数

ある会社は、各ユース ケースからのそれぞれの合計を使用して、ポリシー サーバが認証ロードを処理するためにユーザ ストアに送信するリクエストの総数を判断します。

- 88,000 人の一意のユーザおよびそれらのクレデンシャルを識別するための 176,000 のリクエスト
- OnAuth SiteMinder ポリシーがそれらのユーザに適用されるかどうかを判断するための 22,000 のリクエスト
- 認証時に共通名属性を返すための 22,000 のリクエスト
- パスワード ポリシーに対する 88,000 のリクエスト

結果： 176,000 + 22,000 + 22,000 + 88,000 = 322,080 リクエスト

会社は、この結果および許可ロードに基づく結果を使用して、ユーザ ストアがポリシー サーバ リクエストを処理する必要がある持続レートを概算します。

許可ガイドラインの使用によるディレクトリ検索の概算

ポリシー サーバは、複数のユーザ ディレクトリ リクエストを行ってユーザを許可します。 ユーザ ディレクトリ リクエストによっては SiteMinder ポリシー メンバシップを判断するために必須のものがありますが、その他は SiteMinder ポリシー設計によって異なります。以下のガイドラインを使用して、各許可が作成するポリシー サーバ リクエスト数を概算できます。

- ポリシー ドメイン内の各 SiteMinder ポリシーの 1 つの検索/クエリ。

  注: このガイドラインは、メンバシップ フィルタが 1 つ以上のユーザ ディレクトリ リクエストをもたらすポリシーにのみ適用されます。SiteMinder ポリシー メンバシップとユーザ ディレクトリ リクエストの関係の詳細については、「ポリシー メンバシップおよび許可リクエスト」を参照してください。

- ユーザ属性を返すレスポンスにバインドされる各ポリシーの 1 つの検索/クエリ。

  注: レスポンスとユーザ ディレクトリ リクエストの関係の詳細については、「レスポンスおよび許可パフォーマンス」を参照してください。

以下のユース ケースでは、各ガイドラインを使用して許可ロードが作成するユーザ ディレクトリ検索の総数を特定する方法を説明します。

注: ユーザ許可キャッシュは、ユーザ ディレクトリへの許可関連のリクエスト数を大幅に減らす場合があります。

詳細情報:

SiteMinder ポリシー メンバシップおよび許可パフォーマンス (P. 197)
レスポンスおよび許可パフォーマンス (P. 196)
ユーザ許可キャッシュ (P. 198)

ケース 1: ポリシー メンバシップおよびユーザ ディレクトリ リクエスト

ある会社は、ポータル アプリケーションを保護する 3 つのポリシーを有効にしました。

- ポリシー A では、SiteMinder ポリシー メンバシップを判断するために 1 つのユーザ ディレクトリ リクエストが必要です。
- ポリシー B では、SiteMinder ポリシー メンバシップを判断するために最大 2 つのユーザ ディレクトリ リクエストが必要な場合があります。
- ポリシー C では、SiteMinder ポリシー メンバシップを判断するために最大 3 つのユーザ ディレクトリが必要な場合があります。

さらに、容量計画作業の結果により、アプリケーションには 726,000 の許可ロードがあることが示されます。

会社は以下の式を使用して、ポリシー サーバが許可ロードを処理するためにユーザ ディレクトリに送信するリクエスト数の概算を開始します。

authorization_load x *percent_of_policies* * *number_of_searches* = *daily_authorization_requests*

authorization_load

アプリケーションの日単位の許可数を指定します。

percent_of_policies

SiteMinder ポリシー メンバシップを判断するために、同数のユーザ ディレクトリ リクエストをもたらす可能性がある有効なポリシーの数をパーセンテージで指定します。

注: パーセンテージの合計が 100 パーセントになる必要があります。

number_of_searches

SiteMinder ポリシー メンバシップを判断するために、ポリシー サーバが行う可能性があるユーザ ディレクトリ リクエストの数を指定します。

daily_authorization_requests

許可リクエストを処理するためのユーザ ディレクトリ リクエストの数を指定します。

結果：

- ポリシー A -- 792,000 * 0.33 * 1= 261,360 リクエスト
- ポリシー B および C -- 792,000 * 0.66 * 2= 1,045,440 リクエスト
- ユーザ ディレクトリ リクエスト総数 - 158,000 + 1,045,440= 1,306,880 リクエスト

会社はこの概算を使用して、日単位の許可ロードを処理するために必要なユーザ ディレクトリ リクエストの総数を判断します。

詳細情報:

ユーザ許可キャッシュ (P. 198)

ケース 2: レスポンスおよびユーザ ディレクトリ検索

ある会社は、ポータル アプリケーションを保護する 3 つのポリシーを有効にしました（その内の 2 つは、ユーザ属性を返すレスポンスにバインドされています）。

- ポリシー A は起動時に 1 つのユーザ属性を返します。
- ポリシー B は起動時に 2 つのユーザ属性を返します。
- ポリシー C はユーザ属性を返すレスポンスにバインドされていません。

会社は以下の式を使用して、ポリシー サーバがユーザ属性を返すレスポンスを解決するために行うユーザ ディレクトリ リクエストの数を概算します。

*authorization_load * percent_of_policies * number_of_responses= daily_authorization_requests*

authorization_load

アプリケーションの日単位の許可数を指定します。

percent_of_policies

ユーザ属性を返すレスポンスのために同数のユーザ ディレクトリ リクエストをもたらす有効なポリシーの数をパーセンテージで指定します。

注: パーセンテージの合計が 100 パーセントになる必要があります。

number_of_responses

SiteMinder ポリシーにバインドされたレスポンスの数を指定します。

daily_authorization_requests

許可リクエストを処理するためのユーザ ディレクトリ リクエストの数を指定します。

結果：

- ポリシー A -- 792,000 * 0.2 x 1= 158,000
- ポリシー B -- 792,000 * 0.2 x 2= 316,800
- ポリシー C -- 792,000 * 0.6 x 0= 0
- ユーザ ディレクトリ リクエスト総数 -- 158,000 + 316,800 + 0= 526,000

会社はこの概算を使用して、日単位の許可ロードを処理するために必要なユーザ ディレクトリ リクエストの総数を判断します。

ケース 3: 許可に対するディレクトリ リクエスト総数

会社は、各ユース ケースからのそれぞれの合計を使用して、ポリシー サーバが許可ロードを処理するためにユーザ ディレクトリに送信するリクエストの総数を判断します。

- SiteMinder ポリシー メンバシップを解決するための 1,203,440 のリクエスト。
- レスポンスに関連付けられたユーザ属性を返すための 526,000 のリクエスト。

結果： 1,203,440 + 526,000= 1,729,440 リクエスト

会社は、この結果および認証ロードに基づく結果を使用して、ユーザ ストアがポリシー サーバ リクエストを処理する必要がある持続レートを概算します。

持続ユーザ ディレクトリ検索レートの概算

持続ユーザ ディレクトリ検索レートは、合計操作数（認証ロードと許可ロード）に基づきます（特に、これらのリクエストが発生する時期およびレート）。 これらのリクエストが営業日中に均一に分散される可能性はあまりありません。 さらに、これらのリクエストが発生するレートは、持続期間の最低レベルと最高（ピーク）レベルの間で変動します。

持続ユーザ ディレクトリ検索レートの概算は、以下を識別するプロセスです。

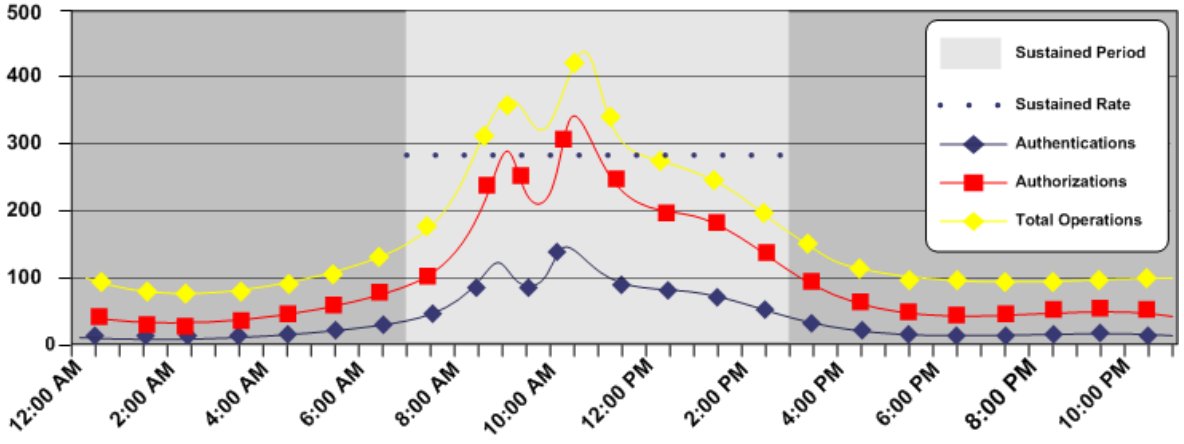
- システムが平均数の操作を処理する持続期間
- これらのリクエストがどのようにユーザ ディレクトリ検索に変換されるか。

持続ユーザ ディレクトリ検索レートの概算時には、日単位の認証ロードおよび許可ロードを使用して以下を特定することをお勧めします。

- 合計操作数が 1 日の間に発生するレート

  注: 1 時間のインクリメントに分割した 24 時間の評価期間で始めることをお勧めします。 ただし、企業の要件に応じて、数週間または数か月の期間にわたって日単位の結果を比較し、年間を通じた使用状況を詳細に把握できます。
- システムが平均数のリクエストを処理する持続期間
- 持続期間中に発生するリクエストの概数です。

以下の図はこれらのメトリックの例です。



ケース: 持続ユーザ ディレクトリ検索レートの概算

会社は以下を特定しました。

- アプリケーションの日単位の認証ロードおよび許可ロードによって、約 888,000 の合計操作数が生じます。
- 合計操作数によって約 2,051,520 のユーザ ディレクトリ リクエストが生じます。
- システムは、持続レベルで約 5 時間（午前 9:00 - 午後 2:00）動作します。
- 持続レベルの間、1 時間に約 84,000 の操作が発生します。
- 約 420,000 （84,000 * 5）の操作または合計操作数の 48 パーセント（420,000/880,000）がこの時間内に発生します。

会社は以下の式を使用して、持続ユーザ ストア検索レートを概算します。

(*total_user_directory_requests* * *percentage_of_requests*) / *number_of_hours* / 3600 = *sustained_user_directory_search_rate*

total_user_directory_requests

ポリシー サーバが認証および許可リクエストを処理するために、ユーザ ディレクトリに対して行う日単位のリクエスト数を表します。

percentage_of_requests

システムが持続レベルで動作しているときに発生する合計操作数の割合を表します。

number_of_hours

システムが持続レートで動作しているときの時間数を表します。

sustained_user_directory_search_rate

ポリシー サーバが操作の持続レートを維持するために、ユーザ ディレクトリに対して行う毎秒のリクエスト数を表します。

結果： （2,051,520 * 0.48）/5/3600 = 毎秒 54.7 ユーザ ディレクトリ リクエスト。

ポリシー サーバは、操作の持続レベル中に認証および許可リクエストを処理するときに、ユーザ ディレクトリに対して毎秒 54.7 のリクエストを行います。

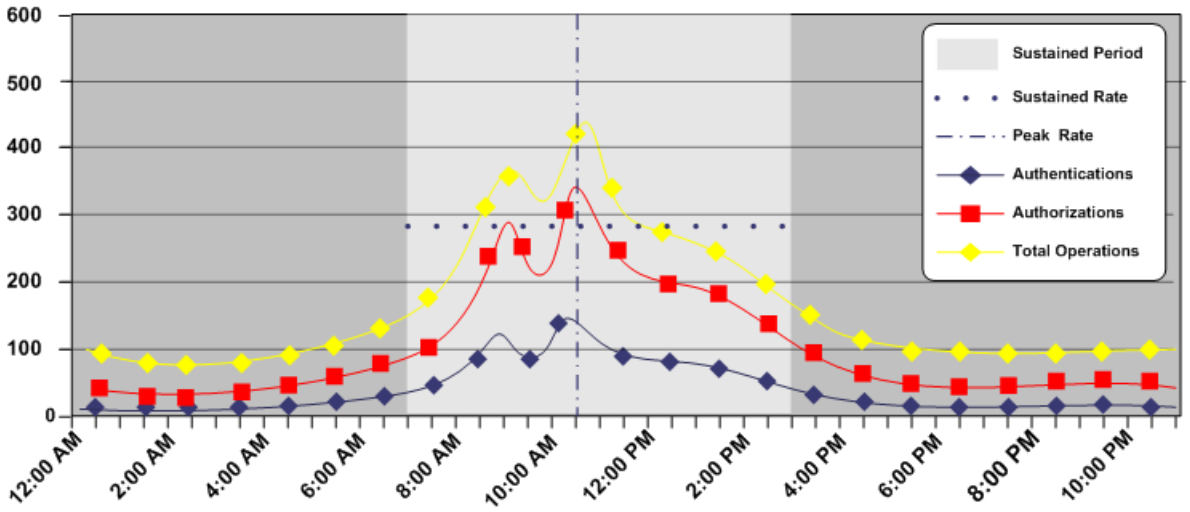
ピーク ユーザ ディレクトリ検索レートの概算

ピーク ユーザ ディレクトリ検索レートは、合計操作数（認証ロードと許可ロード）に基づきます（特に、システムがピーク レベルで動作する時期およびレート）。 ピーク ユーザ ディレクトリ検索レートの概算は、システムが操作の最高レベルを処理する時期、およびこれらのリクエストがどのようにユーザ ディレクトリ検索に変換されるかを特定するプロセスです。

ピーク許可レートの概算時には、持続許可レートの特定時に得たメトリックを使用して以下を特定することをお勧めします。

- システムが最も多くの操作を処理する時間帯。
- この期間に発生する操作の概数。

以下の図はこれらのメトリックの例です。



ケース: ピーク ユーザ ディレクトリ検索レートの概算

ある会社は、アプリケーションによって 1 日あたり合計 888,000 の操作が生じることを特定しました。 これらの操作によって約 2,051,520 のユーザ ディレクトリ検索が生じます。 会社は容量計画実行中に収集したメトリックを使用して、最繁時の 1 時間に約 278,000 の操作（または合計操作数の 31 パーセント）が発生したことを特定しました。

会社は以下の式を使用して、ピーク ユーザ ストア検索レートを概算します。

(*total_user_directory_requests* * *percentage_of_requests*) / *number_of_hours* / 3600 = *peak_authentication_request_rate*

total_authentication_requests

ポリシー サーバがユーザ ストアに送信するリクエストの総数を表します。

percentage_of_requests

システムがピーク レベルで動作しているときに発生する操作の割合を表します。

number_of_hours

システムがピーク レベルで動作する時間数を表します。

peak_user_directory_request_rate

ポリシー サーバがピーク認証レートを維持するために、ユーザ ストアに対して行う毎秒のリクエスト数を表します。

結果： （2,051,520 * 0.31）/1/3600 = 毎秒 176.6 リクエスト。

ポリシー サーバは、操作のピーク レベル中に認証および許可リクエストを処理するときに、ユーザ ディレクトリに対して毎秒 176.6 のリクエストを行います。

ユーザ ストア容量計画

ポリシー サーバは一連のサービスを実行して、Web サービス リクエスト メッセージを認証および許可します。 これらのサービスによって、リクエストと総称されるユーザ ディレクトリへの読み取りおよび書き込みが生じます。 eTrust SOA Security Manager のパフォーマンスに著しく関与する要因によって、ユーザ ディレクトリが操作の持続期間およびピーク期間にこの作業負荷を処理できるかどうかが決定されます。

以下の一般的な要因が eTrust SOA Security Manager のパフォーマンスに影響します。

- Web サービス リクエストの合計数および持続ユーザ ディレクトリ検索レート -- ポリシー サーバは、各受信 Web サービス リクエストの認証と許可の操作を処理する必要があります。 これらのリクエストが行われるレートは営業日を通して変動します。

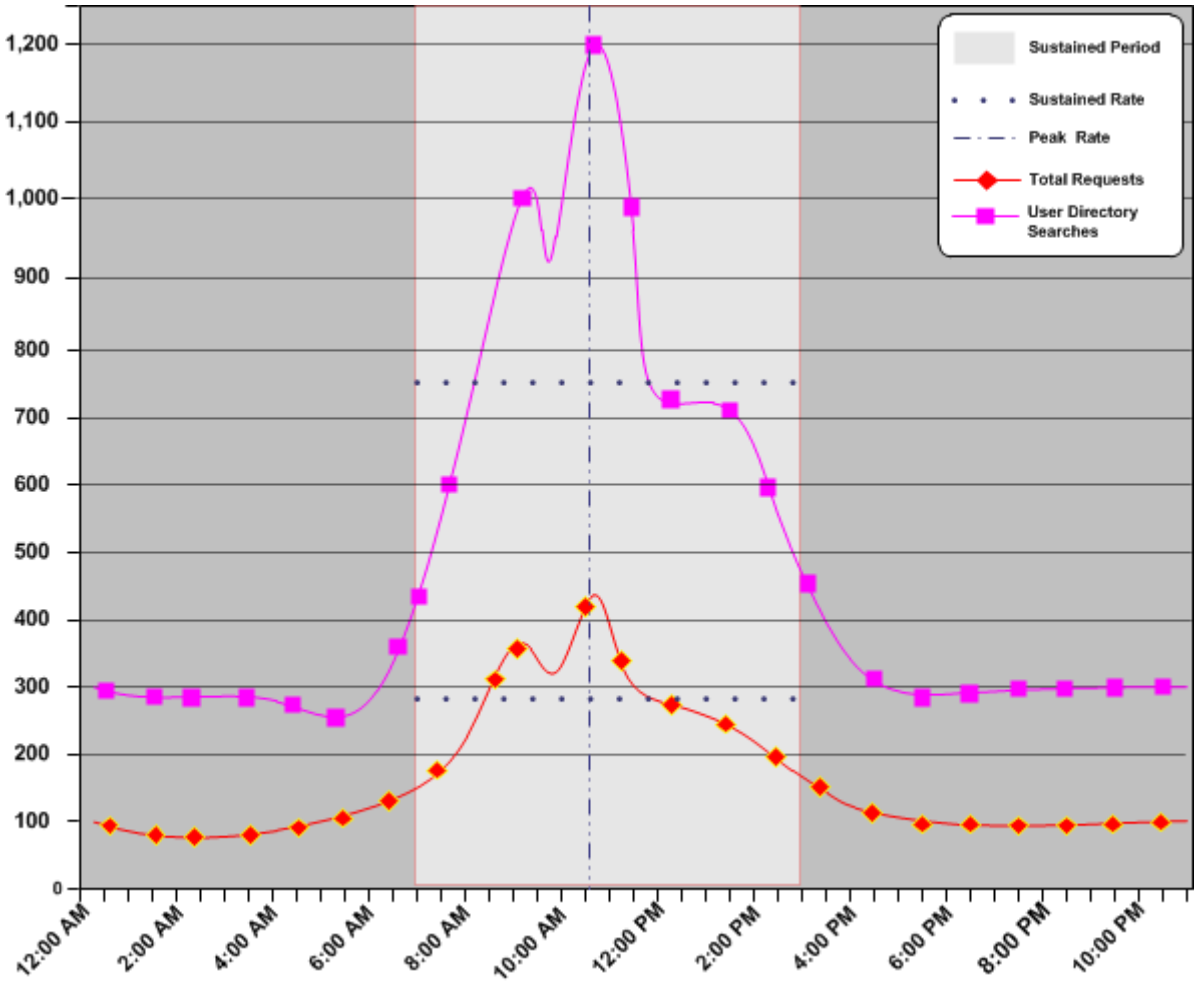
  同様に、ポリシー サーバがユーザ ディレクトリ リクエストを行って操作を処理するレートは変動します。 一部の期間では比較的少数のユーザ ディレクトリ リクエストが生成されますが、その他の期間ではより多くのリクエストが生成されます。

  持続ユーザ ディレクトリ検索レートは、ポリシー サーバが平均数のユーザ ディレクトリ リクエストを行い、平均数の操作を処理する期間を表します。

- 合計リクエスト数およびピーク ユーザ ディレクトリ検索レート -- アクティビティの持続期間中に、Web サービス リクエスト アクティビティが急増する場合があります。 ピーク ユーザ ディレクトリ検索レートは、ポリシー サーバが最も多くのユーザ ディレクトリ リクエストを行い、最大数の認証と許可操作を処理する期間を表します。

以下のグラフでは次のことを示します。

- 合計リクエスト数とユーザ ディレクトリ検索レートの関係。
- 各レートが 1 日の間に変動し、特定の期間持続してその期間内にピークに達する様子。



ユーザ ディレクトリが操作する必要があるロードを概算するために以下のガイドラインを使用することをお勧めします。 いったんロードを概算すると、すべての標準ツールを使用してディレクトリでロードを作成し、その結果を追跡できます。

注: 多くの要因によって必要数の獲得に失敗する場合があります。調整の詳細については、ベンダー固有のマニュアルを参照してください。

詳細情報:

ポリシー サーバ (P. 13)
持続リクエスト レートの概算方法 (P. 125)

ユーザ ストア容量計画のチェックリスト

ポリシー サーバが Web サービス リクエストを処理するために行う必要があるユーザ ディレクトリ リクエスト数の概算には、特定の情報が必要です。 ユーザ ストア容量計画を開始する前に以下の情報を収集します。

- ☐ Web サービスの日単位の Web サービス リクエスト（リクエスト ロード）の総数。
- ☐ Web サービス クライアントが Web サービスにリクエストを送信する持続期間およびピーク期間。
- ☐ 有効なポリシーの総数。 各 SiteMinder ポリシーについて、以下の点を判断します。
  - ポリシー メンバシップ フィルタによって 1 つ以上のユーザ ディレクトリ検索が生じるかどうか。
  - ポリシーにバインドされたレスポンスによって 1 つ以上のユーザ ディレクトリ検索が生じるかどうか。

詳細情報:

SiteMinder ポリシー メンバシップおよび許可パフォーマンス (P. 197)
導入された eTrust SOA Security Manager 容量計画 (P. 123)

持続ユーザ ディレクトリ検索レートの概算方法

持続ユーザ ディレクトリ検索レートの概算は、以下のことを特定するプロセスです。

- ユーザ ディレクトリ リクエストの総数は営業日全体でどのように変動するか。
- 持続期間中にユーザ ディレクトリ リクエストが毎秒どのようにリクエストに変換されるか。

以下の手順を実行して、持続ユーザ ディレクトリ検索レートを概算します。

1. 認証ガイドラインを使用して、認証ロードが作成するユーザ ディレクトリ リクエスト数を概算します。
2. 許可ガイドラインを使用して、許可ロードが作成するユーザ ディレクトリ リクエスト数を概算します。
3. 持続ユーザ ディレクトリ検索レートを概算します。

認証ガイドラインの使用によるディレクトリ検索の概算

ポリシー サーバは複数のユーザ ディレクトリ リクエストを行って、各認証リクエストを処理します。 ユーザ ディレクトリ リクエストによっては必須のものがありますが、その他は回避できます。

以下のガイドラインを使用して、各認証が作成するポリシー サーバ リクエスト数を概算します。

（必須）各ユーザを認証する 2 つの検索。

- ユーザを識別するためのストアごとに 1 つの検索/クエリ
- ユーザ認証情報を確認するための 1 つの検索/クエリ

（オプション）ポリシーの設計方法に応じて、さらに検索が必要になる場合があります。

- ユーザが認証されると発生するルール（OnAuth ルール）にバインドされる各 SiteMinder ポリシーの 1 つの検索/クエリ。

  注: ルール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。 ルールと SiteMinder ポリシーとの関係の詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

- ユーザ属性を返すレスポンスにバインドされる各 SiteMinder ポリシーの 1 つの検索/クエリ。

  注: レスポンスおよびルールとの関係の詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

許可ガイドラインの使用によるディレクトリ検索の概算

ポリシー サーバは、複数のユーザ ディレクトリ リクエストを行ってユーザを許可します。 ユーザ ディレクトリ リクエストによっては SiteMinder ポリシー メンバシップを判断するために必須のものがありますが、その他は SiteMinder ポリシー設計によって異なります。以下のガイドラインを使用して、各許可が作成するポリシー サーバ リクエスト数を概算できます。

- アプリケーションまたはポリシー ドメイン内の各 SiteMinder ポリシーの 1 つの検索/クエリ。

  注: このガイドラインは、メンバシップ フィルタが 1 つ以上のユーザ ディレクトリ リクエストをもたらすポリシーにのみ適用されます。SiteMinder ポリシー メンバシップとユーザ ディレクトリ リクエストの関係の詳細については、「ポリシー メンバシップおよび許可リクエスト」を参照してください。

- ユーザ属性を返すレスポンスにバインドされる各ポリシーの 1 つの検索/クエリ。

  注: レスポンスとユーザ ディレクトリ リクエストの関係の詳細については、「レスポンスおよび許可パフォーマンス」を参照してください。

注: ユーザ許可キャッシュは、ユーザ ディレクトリへの許可関連のリクエスト数を大幅に減らす場合があります。

詳細情報:

ユーザ許可キャッシュ (P. 198)

持続ユーザ ディレクトリ検索レートの概算

持続ユーザ ディレクトリ検索レートは、合計操作数（認証ロードと許可ロード）に基づきます（特に、これらのリクエストが発生する時期およびレート）。 これらのリクエストが営業日中に均一に分散される可能性はあまりありません。 さらに、これらのリクエストが発生するレートは、持続期間の最低レベルと最高（ピーク）レベルの間で変動します。

持続ユーザ ディレクトリ検索レートの概算は、以下を識別するプロセスです。

- システムが平均数の操作を処理する持続期間
- これらのリクエストがどのようにユーザ ディレクトリ検索に変換されるか。

持続ユーザ ディレクトリ検索レートの概算時には、日単位の認証ロードおよび許可ロードを使用して以下を特定することをお勧めします。

- 合計操作数が 1 日の間に発生するレート

  注: 1 時間のインクリメントに分割した 24 時間の評価期間で始めることをお勧めします。 ただし、企業の要件に応じて、数週間または数か月の期間にわたって日単位の結果を比較し、年間を通じた使用状況を詳細に把握できます。
- システムが平均数のリクエストを処理する持続期間
- 持続期間中に発生するリクエストの概数です。

ケース: 持続ユーザ ディレクトリ検索レートの概算

会社は以下を特定しました。

- アプリケーションの日単位の認証ロードおよび許可ロードによって、約 888,000 の合計操作数が生じます。
- 合計操作数によって約 2,051,520 のユーザ ディレクトリ リクエストが生じます。
- システムは、持続レベルで約 5 時間（午前 9:00 - 午後 2:00）動作します。
- 持続レベルの間、1 時間に約 84,000 の操作が発生します。
- 約 420,000 （84,000 * 5）の操作または合計操作数の 48 パーセント（420,000/880,000）がこの時間内に発生します。

会社は以下の式を使用して、持続ユーザ ストア検索レートを概算します。

(*total_user_directory_requests* * *percentage_of_requests*) / *number_of_hours* / 3600 = *sustained_user_directory_search_rate*

total_user_directory_requests

ポリシー サーバが認証および許可リクエストを処理するために、ユーザ ディレクトリに対して行う日単位のリクエスト数を表します。

percentage_of_requests

システムが持続レベルで動作しているときに発生する合計操作数の割合を表します。

number_of_hours

システムが持続レートで動作しているときの時間数を表します。

sustained_user_directory_search_rate

ポリシー サーバが操作の持続レートを維持するために、ユーザ ディレクトリに対して行う毎秒のリクエスト数を表します。

結果：（2,051,520 * 0.48）/5/3600 = 毎秒 54.7 ユーザ ディレクトリ リクエスト。

ポリシー サーバは、操作の持続レベル中に認証および許可リクエストを処理するときに、ユーザ ディレクトリに対して毎秒 54.7 のリクエストを行います。

ピーク ユーザ ディレクトリ検索レートの概算

ピーク ユーザ ディレクトリ検索レートは、合計操作数（認証ロードと許可ロード）に基づきます（特に、システムがピーク レベルで動作する時期およびレート）。 ピーク ユーザ ディレクトリ検索レートの概算は、システムが操作の最高レベルを処理する時期、およびこれらのリクエストがどのようにユーザ ディレクトリ検索に変換されるかを特定するプロセスです。

ピーク許可レートの概算時には、持続許可レートの特定時に得たメトリックを使用して以下を特定することをお勧めします。

- システムが最も多くの操作を処理する時間帯。
- この期間に発生する操作の概数。

ケース: ピーク ユーザ ディレクトリ検索レートの概算

ある会社は、アプリケーションによって 1 日あたり合計 888,000 の操作が生じることを特定しました。 これらの操作によって約 2,051,520 のユーザ ディレクトリ検索が生じます。 会社は容量計画実行中に収集したメトリックを使用して、最繁時の 1 時間に約 278,000 の操作（または合計操作数の 31 パーセント）が発生したことを特定しました。

会社は以下の式を使用して、ピーク ユーザ ストア検索レートを概算します。

(*total_user_directory_requests* * *percentage_of_requests*) / *number_of_hours* / 3600 = *peak_authentication_request_rate*

total_authentication_requests

ポリシー サーバがユーザ ストアに送信するリクエストの総数を表します。

percentage_of_requests

システムがピーク レベルで動作しているときに発生する操作の割合を表します。

number_of_hours

システムがピーク レベルで動作する時間数を表します。

peak_user_directory_request_rate

ポリシー サーバがピーク認証レートを維持するために、ユーザ ストアに対して行う毎秒のリクエスト数を表します。

結果： （2,051,520 * 0.31）/1/3600 = 毎秒 176.6 リクエスト。

ポリシー サーバは、操作のピーク レベル中に認証および許可リクエストを処理するときに、ユーザ ディレクトリに対して毎秒 176.6 のリクエストを行います。

定期的なメンテナンス タスク

以下のリストで、一般的な SiteMinder メンテナンスに対して実行できるタスクを詳述します。 通常 CA サービスの実装チームは、特定の環境に基づいたこれらのタスクの詳細を説明します。

- オペレーティング システム パッチを適用します。

  頻度： 月単位または必要に応じて

- SiteMinder 累積パッチを適用します。

  頻度： 月単位または必要に応じて

- SiteMinder OneView Monitor、CA Wily （または同等のツール）を使用して、SiteMinder のパフォーマンスを監視します。

  頻度： 継続的

- バックエンド リポジトリのパフォーマンスを監視します。

  頻度： 継続的

- ネイティブまたは SiteMinder のツールを使用してバックエンド リポジトリをバックアップします。

  頻度： 組織の要件に従って

- ネイティブ ツールを使用して、バックエンド リポジトリをメンテナンスします。 このメンテナンスの例には以下の項目が含まれます。

  - インデックス作成
  - ディスク領域の消費を削減するためのトランザクション ログのバックアップ。

  頻度： 組織の要件に従って

- XPSSweeper ユーティリティを実行して、ポリシー ストアから削除対象のオブジェクトを削除します。

  頻度： 24 時間ごと。 このスケジュールは、ポリシー ストアのサイズを縮小するのに役立ちます。

- SiteMinder ログ ファイルをアーカイブします。

  頻度： 組織の要件に従って

- SiteMinder ポリシーを監査し、必要に応じて調整および最適化します。

  頻度： 組織の要件に従って

- 認証および許可の失敗を監査します。 必要に応じてイベントをエスカレーションします。

  頻度： 継続的

第 9 章: 実装問題の診断

このセクションには、以下のトピックが含まれています。

導入された問題の診断

SiteMinder 実装中に発生する可能性がある問題はさまざまであり、各環境によって異なります。 問題は、環境の全体的なパフォーマンスへの各コンポーネントの展開に関連する場合があります。

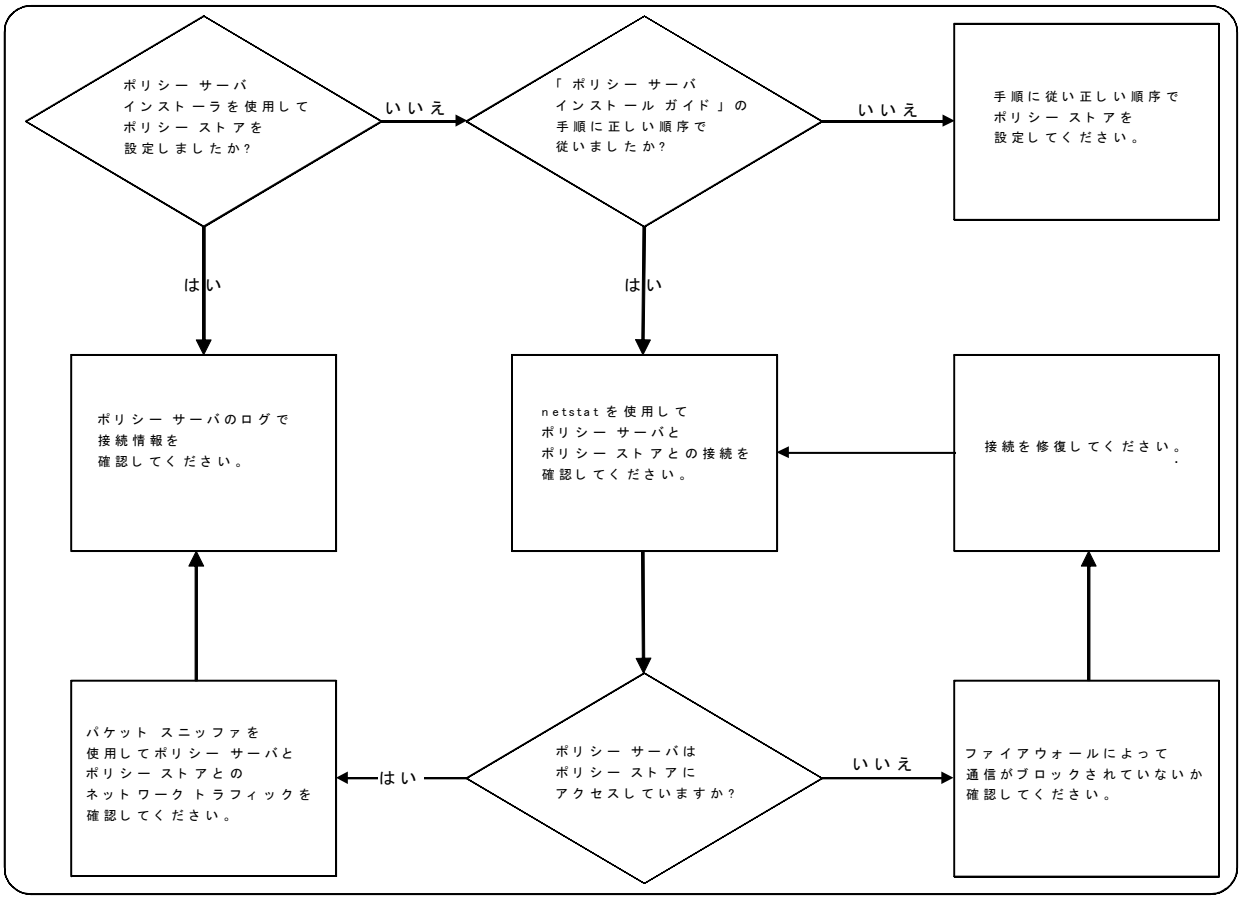
以降のセクションでは、以下について説明します。

- 一般的な実装問題の診断方法
- 問題を効率的に解決するためのサポートの利用方法
- 問題のトラブルシュートに役立つ他の SiteMinder ドキュメントがある場所
- SiteMinder パフォーマンスの測定に使用できるツール

ポリシー サーバ/ポリシーストア接続問題

さまざまな問題が、ポリシー サーバと適切に設定されたポリシー ストアとの接続に関連しています。 これらの問題は、正しく設定されていないポリシー ストアからネットワークとデータベースの接続にまで及ぶ場合があります。

以下のフローチャートを使用して問題を診断します。



以下の点について考慮してください。

- ポリシー サーバ ホスト システム上でパケット スニッファを使用することにより、ポリシー ストアがポリシー サーバに送信するエラー メッセージを記録できます。 接続リクエストに接続が拒否されたことを示すエラー メッセージが含まれる場合、ポリシー ストアとして機能するデータベースまたはディレクトリ サーバが接続を妨げています。

- ポリシー サーバ ログを確認すると、ポリシー サーバが試行している接続に関する情報を特定できます。 接続が失敗する一般的な理由には、以下が含まれます。
  - ポリシー サーバが、ポリシー ストアへのアクセスに無効な管理者認証情報を使用しています。
  - ポリシー サーバが使用している管理者アカウントに読み取りアクセス権がありません。

  注: ポリシー サーバ 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場所を示します。

サポートの利用

SiteMinder テクニカル サポートの支援が必要な場合は、サポート チケットを開くときに、特定の情報を収集して含めることができます。 可能な限り多くの情報を含めることによって、テクニカル サポートによる問題解決にかかる時間を短縮できます。

環境情報

サポート チケットを開くときに、以下の情報を可能な限り多く収集して含めます。

- ポリシー サーバがインストールされているオペレーティング システム（サービス パック レベルを含む）。

  例： Windows 2008 SP2
- SiteMinder エージェントがインストールされている Web サーバ。

  例： Windows 2008 SP2、IIS 7.0
- サービス パックおよび累積リリース（CR）を含むポリシー サーバのバージョン。

  例： r12.0 SP2 CR1
- ポリシー サーバと通信する SiteMinder エージェントのバージョン（サービス パックおよび CR を含む）。

  例： r12.0 SP2 CR1

- ポリシー ストア タイプ（LDAP/ODBC）および特定のベンダーやバージョン。

  例： Oracle 10g R2
- その他の SiteMinder データ ストアの特定のベンダーおよびバージョン。
- 他の CA 製品、または SiteMinder と統合されたサードパーティ製品（該当する場合）。
- 環境で展開されたカスタム コードまたはサードパーティの認証方式。カスタム コードには、GSE （Global Solutions Engineering）によって提供されるコードまたは組織によって開発されるコードが含まれます。
- アップグレードされた SiteMinder コンポーネントまたは新しいハードウェアなど、環境に対して最近行われた変更。
- 問題が発生した時期。

注: SiteMinder プラットフォーム サポート マトリックスを使用して、その問題が SiteMinder がサポートしていないオペレーティング システムまたはサードパーティ製品と関係がないことを確認できます。 詳細については、SiteMinder プラットフォーム サポート マトリックスを参照してください。

ログ ファイル

発生している問題に応じて、サポートが以下のログ ファイルの 1 つまたは複数をリクエストする場合があります。

コンポーネント	ファイル
ポリシー サーバ	■ ポリシー サーバ ログ（smps.log） ■ ポリシー サーバ プロファイラ ログ（smtracedefault.log） ■ 監査ログ（smaccess.log）
Web エージェント	■ Web エージェント ログ ■ Web エージェント トレース ログ ■ Web サーバ エラー ログ ■ Web サーバ アクセス ログ

コンポーネント	ファイル
WSS エージェント	■ WSS エージェント ログ ■ XML 処理メッセージ ログ ■ Web エージェント トレース ログ（Web サーバの WSS エージェントのみ） ■ アプリケーション サーバまたは Web サーバのエラー ログ ■ アプリケーション サーバまたは Web サーバのアクセス ログ

以下の点について考慮してください。

- すべてのポリシー サーバ ログは *ps_home*¥log にあります。

  ps_home

  ポリシー サーバのインストール パスを指定します。

  注: ポリシー サーバ プロファイラ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。監査の詳細については、「*ポリシー サーバ管理ガイド*」を参照してください。

- Web および WSS エージェント ログには、デフォルトの場所またはデフォルトの名前がありません。

  注: Web エージェント ログ記録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。WSS エージェント ログ記録の設定の詳細については、該当する WSS エージェント ガイドを参照してください。

ポリシー サーバ クラッシュ

ポリシー サーバがクラッシュした場合、以下に示す情報はサポートがさらに詳細を調査する際に役立ちます。 この情報はサポート チケットを開くためには必要ありませんが、サポートがリクエストする可能性が高い情報です。 この情報を最初に提供すれば、サポートによる問題解決にかかる時間が短縮される場合があります。

1. 環境情報を提供します。
2. 可能な限り詳細に問題を説明します。 例：
   - プロセスがクラッシュする頻度。
   - クラッシュが発生した回数。

- クラッシュ時にサーバ上で発生したことの説明。
- クラッシュを再現する手順。

3. UNIX コア ファイルまたは Windows ダンプ ファイルを添付します。これらのファイルを添付する場合は、以下の点について考慮してください。
   - （UNIX）可能であれば、パッケージ化されたコアを提供してください。
   - （Windows）このファイルが、プログラム エラー デバッグ ツールによって作成されたミニ ダンプではなく完全なダンプ ファイルであることを確認してください。
4. ポリシー ストア データを添付します。
5. ポリシー サーバ ログおよびポリシー サーバ監査ログを添付します。
6. ポリシー サーバ トレース ログ出力を変更します。
7. ポリシー サーバ プロファイラ ログを添付します。

   注: ログ ファイルを添付する場合は、ファイルのセットが一致していることを確認してください。 また、すべてのファイルが、問題の発生時と同じ時間のものであることを確認します。

詳細情報:

環境情報 (P. 235)
ログ ファイル (P. 236)

ポリシー ストア データの添付

サポートは、ポリシー ストア データの検討によって問題をより効率的に特定できます。ポリシー ストアをエクスポートして、SiteMinder データ情報ファイル（smdif）をチケットに添付します。

注: ポリシー ストア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。

ポリシー サーバ トレース ログを変更します。

サポートは、ポリシー サーバ トレース ログの検討によって問題をより効率的に特定できます。ポリシー サーバがクラッシュする場合は、ポリシー サーバ プロファイラを使用して問題をキャプチャできます。

注: ポリシー サーバがハングする場合、問題をキャプチャできない場合があります。 ポリシー サーバ プロファイラを使用する代わりに、強制的にコア ダンプさせます。

ポリシー サーバ プロファイラはデフォルト設定ファイルを使用して、ポリシー サーバ アクションをトレース ログに記録します。デフォルト設定にはコンポーネントおよびデータに関する情報が含まれます。

- コンポーネントは、ポリシー サーバが実行するアクションの論理的なグループを表します。
- データは、ポリシー サーバがトレースする必要がある実際のデータを表します。

SiteMinder サポートは、デフォルト設定ファイルに含まれていないコンポーネントおよびデータの設定を使用して、トラブルシューティング プロセスを開始します。ポリシー サーバ トレース ログをサブミットする前にデフォルト設定を変更します。

注: ポリシー サーバ プロファイラ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。

例: 変更されるコンポーネント

デフォルト トレース設定を変更して以下のコンポーネントを含めます。

- サーバ

  サーバ コンポーネントには他のサブコンポーネントが含まれます。サーバ コンポーネントを追加した後、以下のサブコンポーネントを削除します。

  - Policy_Object
  - Policy_Object_Cache
  - 管理
  - Audit_Logging

- Tunnel_Service
- JavaAPI

例: 変更されるデータ型

デフォルト トレース設定を変更して以下のデータ型を含めます。

重要: データ型がリスト表示される順序で、データがログ記録される順序が決まります。 データ型が以下の順序で一覧表示されることを確認してください。

- Date
- Time
- Precise Time
- Pid
- Tid
- SrcFile
- Function
- AgentName
- TransactionName
- TransactionID
- Resource
- Realm
- Rule
- Domain
- Group
- Policy
- User
- Directory
- AgentType
- ReturnValue
- ErrorString
- ErrorValue

- AuthStatus
- AuthReason
- AuthScheme
- ClusterID
- RequestIPAddr
- Returns
- Result
- Message

エージェントのクラッシュ

エージェントがクラッシュしている場合に、サポートが詳細を調査するのに役立つ情報を以下に示します。 この情報はサポート チケットを開くためには必要ありませんが、サポートがリクエストする可能性が高い情報です。 この情報を最初に提供すれば、サポートによる問題解決にかかる時間が短縮される場合があります。

1. 環境情報を集めます。
2. 可能な限り詳細に問題を説明します。 例：
   - プロセスがクラッシュする頻度。
   - クラッシュが発生した回数。
   - クラッシュ時にサーバ上で発生したことの説明。
   - クラッシュを再現する手順。
3. UNIX コア ファイルまたは Windows ダンプ ファイルを添付します。 これらのファイルを添付する場合は、以下の点について考慮してください。
   - （UNIX）可能であれば、パッケージ化されたコアを提供してください。
   - （Windows）このファイルが、プログラム エラー デバッグ ツールによって作成されたミニ ダンプではなく完全なダンプ ファイルであることを確認してください。

4. エージェント ログおよび Web サーバまたはアプリケーション サーバのエラー ログを添付します。

   注: ログ ファイルを添付する場合は、ファイルのセットが一致していることを確認してください。 また、すべてのファイルが、問題の発生時と同じ時間のものであることを確認します。

5. Web サーバ バイナリ ディレクトリの tar または zip を添付します。

   注: この手順は、IIS Web サーバ上で実行するエージェントには適用されません。

6. Web サーバの Web エージェントまたは WSS エージェントについては、Web エージェント トレース ログおよび Web サーバ アクセス ログを添付します。

詳細情報:

環境情報 (P. 235)
ログ ファイル (P. 236)

リソース リーク

メモリ、ファイル ハンドル、ネットワーク接続、ソケットまたはディスク領域などのシステム リソースがリリースされていない場合、以下に示す情報はサポートがさらに詳細を調査する際に役立ちます。 この情報はサポート チケットを開くためには必要ありませんが、サポートがリクエストする可能性が高い情報です。 この情報を最初に提供すれば、サポートによる問題解決にかかる時間が短縮される場合があります。

1. 環境情報を集めます。
2. 可能な限り詳細に問題を説明します。少なくとも以下の情報を含めます。
   - リソース リークの頻度。
   - リソース リークのサイズ。 prstat などリソース割り当てを表示できるツールで、一定期間のリソース リークを測定します。
   - リソース リークの測定に使用したツール。

- リソース リークがシステムに及ぼす影響。

  例： システムがクラッシュまたはハングします。

- リソース リークの再現手順またはアプリケーション トラフィックに基づく再現テスト。

3. 以下のログを添付します。
   - （ポリシー サーバ）ポリシー サーバの問題が発生している場合は、ポリシー サーバ ログおよびポリシー サーバ監査ログを添付します。
   - （SiteMinder エージェント）エージェントの問題が発生している場合は、エージェント ログおよび Web サーバまたはアプリケーション サーバのエラー ログを添付します。

   注: ログ ファイルを添付する場合は、ファイルのセットが一致していることを確認してください。 また、すべてのファイルが、問題の発生時と同じ時間のものであることを確認します。

詳細情報:

環境情報 (P. 235)
ログ ファイル (P. 236)

機能上の問題

ドキュメントで詳述されるように、機能上の問題は SiteMinder が動作していない問題として定義されます。 機能上の問題が発生している場合、以下に示す情報はサポートがさらに詳細を調査する際に役立ちます。 この情報はサポート チケットを開くためには必要ありませんが、サポートがリクエストする可能性が高い情報です。 この情報を最初に提供すれば、サポートによる問題解決にかかる時間が短縮される場合があります。

1. 環境情報を集めます。
2. 問題の再現手順を含めて、可能な限り詳細に問題を説明します。

3. 以下のログを添付します。
   - （ポリシー サーバ）ポリシー サーバの問題が発生している場合は、ポリシー サーバ ログおよびポリシー サーバ監査ログを添付します。
   - （SiteMinder エージェント）エージェントの問題が発生している場合は、エージェント ログおよび対応する Web サーバまたはアプリケーション サーバのエラー ログを添付します。

   注: ログ ファイルを添付する場合は、ファイルのセットが一致していることを確認してください。 また、すべてのファイルが、問題の発生時と同じ時間のものであることを確認します。
4. ポリシー ストアを SiteMinder データ情報ファイル（smdif）にエクスポートして、そのファイルを添付します。

   注: ポリシー ストア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。
5. 以下のログを添付します。
   - （ポリシー サーバ）ポリシー サーバの問題が発生している場合は、ポリシー サーバ プロファイラ ログを添付します。
   - （SiteMinder エージェント）エージェントの問題が発生している場合は、すべてのエージェント ログおよび Web サーバまたはアプリケーション サーバのアクセス ログを添付します。

詳細情報:

環境情報 (P. 235)
ログ ファイル (P. 236)

ランダムな問題

ランダムな問題は、本質的に機能上ではあるが散発的に発生し、再生できるパターンがない問題として定義されます。 ランダムな問題が発生している場合、以下に示す情報はサポートがさらに詳細を調査する際に役立ちます。 この情報はサポート チケットを開くためには必要ありませんが、サポートがリクエストする可能性が高い情報です。 この情報を最初に提供すれば、サポートによる問題解決にかかる時間が短縮される場合があります。

1. 環境情報を集めます。
2. 可能な限り詳細に問題を説明します。 例：
   - 問題の開始時期。
   - 問題の頻度。
   - 問題がシステムに及ぼす影響。

     例： トランザクションに通常より多くの時間がかかります。
3. 以下のログを添付します。
   - （ポリシー サーバ）ポリシー サーバの問題が発生している場合については、以下のとおりです。
     - 障害発生ポイントを含むポリシー サーバ ログ、障害発生ポイントを含むポリシー サーバ監査ログおよび障害発生ポイントを含むポリシー サーバ プロファイラ ログを添付します。
     - 正しく機能するシステムを含むポリシー サーバ プロファイラ ログを添付します。
   - （SiteMinder エージェント）エージェントの問題が発生している場合については、以下のとおりです。
     - 障害発生ポイントを含むすべてのエージェント ログを添付します。
     - 正しく機能するシステムを含むすべてのエージェント ログを添付します。

   注: ログ ファイルを添付する場合は、ファイルのセットが一致していることを確認してください。 また、すべてのファイルが、問題の発生時と同じ時間のものであることを確認します。

詳細情報:

環境情報 (P. 235)
ログ ファイル (P. 236)

ナレッジ ベース記事の特定

SiteMinder マニュアル選択メニューは、使用できる唯一のリソースです。SiteMinder のナレッジ ベース（KB）記事は CA テクニカル サポート サイトで使用できます。これらの記事では、SiteMinder 環境の管理およびトラブルシューティングに関連するさまざまなトピックを扱っています。

SiteMinder の KB 記事を特定する方法

1. テクニカル サポート サイトにログインします。
2. ［Support By Product］をクリックします。

   ［Support by Product］ページが表示されます。
3. 製品リストで SiteMinder を見つけて、リンクをクリックします。

   SiteMinder 製品ページが表示されます。
4. ［Search Support］の下に検索条件を入力します。［Search Support］は画面の右側にあります。

   検索条件に一致する情報が表示されます。

SiteMinder パフォーマンスの測定

SiteMinder パフォーマンスの測定は、展開のさまざまなコンポーネントの動作方法に影響するメトリックの収集に関連する反復プロセスです。 各コンポーネント ペア間の往復回数を測定して、性能基準が満たされているかどうかを判断し、潜在的なボトルネックを特定することをお勧めします。

注: SiteMinder 展開を調整するための唯一の決定要因として、CPU 使用率など従来のパフォーマンス メトリックを使用しないようにしてください。たとえば、ポリシー サーバをホストするシステムはロード中に低い CPU 使用率で稼働する場合がありますが、この要因によって、ポリシー サーバが最適なパフォーマンスに達したことが確実になります。

SiteMinder パフォーマンスの測定に以下のツールを使用できます。

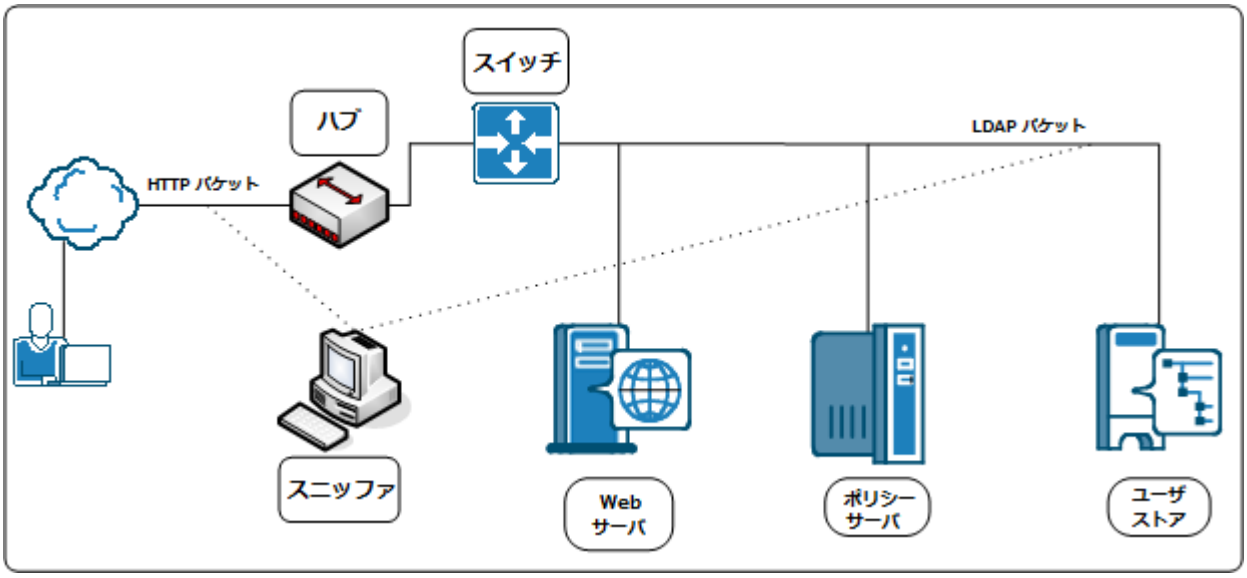
- ネットワーク スニッファ
- SiteMinder OneView Monitor
- SiteMinder テスト ツール
- ディレクトリ サーバ ユーティリティおよび SQL アナライザ

ネットワーク スニッファ

サードパーティのネットワーク スニッファを使用して、テスト結果に影響を及ぼさずに、暗号化されていないデータに対するリクエストのサイズおよびコンテンツを予測できます。 スニッファでは、送信される余分なパケット、ロード バランシング間の長期の遅延、およびログ単独ではキャプチャできないリダイレクト技術に対するアラートも使用できます。

注: ネットワークがスイッチング ハブ設定でセットアップされている場合は、クライアントとクライアント側ハブのサーバの間にスニッファを配置します。

以下の図では、標準的な SiteMinder 展開内のネットワーク スニッファを示します。



SiteMinder OneView Monitor

SiteMinder OneView Monitor を使用してパフォーマンス ボトルネックを特定し、SiteMinder 展開内のリソース使用状況に関するメトリックを収集できます。 さらに OneView Monitor は、以下の SiteMinder コンポーネントから動作データを収集することによって、コンポーネント障害などの特定のイベントが発生した場合にアラートを表示します。

- ポリシー サーバ
- SiteMinder エージェント

OneView Monitor では、以下のようなメトリックの使用により SiteMinder エージェントとポリシー サーバの間のパフォーマンス ボトルネックを特定できます。

- 平均認証試行回数およびユーザの認証にかかる平均時間。
- 平均許可試行回数およびユーザの許可にかかる平均時間。
- キャッシュ ヒット数およびキャッシュ ミス数。

注: OneView Monitor が提供できるデータ型の全リストについては、「ポリシー サーバ管理ガイド」を参照してください。 OneView Monitor 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。

SiteMinder テスト ツール

SiteMinder テスト ツール ユーティリティを使用して、SiteMinder エージェントとポリシー サーバ間の通信をテストできます。 テスト ツールは、ポリシー サーバのパフォーマンスの分離を可能にする Web エージェントをエミュレートします。

テスト ツールによって以下の 3 種類のテストを実行できます。

機能

ポリシーをテストして正しく設定されていることを確認します。

リグレッション

ポリシー ストアの移行や新機能の実装などの変更が、展開に影響するかどうかをテストします。

ストレス

複数のリクエストを受信したときのポリシー サーバのパフォーマンスをテストします。

注: テスト ツール ユーティリティの詳細については、「テスト ツール ヘルプ」を参照してください。

ディレクトリ サーバ ユーティリティおよび SQL アナライザ

ディレクトリ サーバ ユーティリティを使用して、クエリ遅延を分離するディレクトリ サーバまたはデータベースへのポリシー サーバ リクエストをシミュレートできます。 SQL アナライザを使用して、ポリシー サーバとユーザ ディレクトリ間の応答時間を分析することもできます。

第 10 章: 製品統合

このセクションには、以下のトピックが含まれています。

CA Arcot WebFort と RiskFort の統合

CA Arcot Adapter™ （Adapter）を使用して、CA Arcot WebFort の強力な認証ソリューションおよび CA Arcot RiskFort の順応性のある認証ソリューションのオンプレミスの実装と SiteMinder を統合します。

インストールを開始する前に、次の点を確認してください。

- 統合には Adapter および CA Arcot RiskFort の最小バージョンが必要です。
- 統合には CA Arcot WebFort の最小バージョンが必要です。

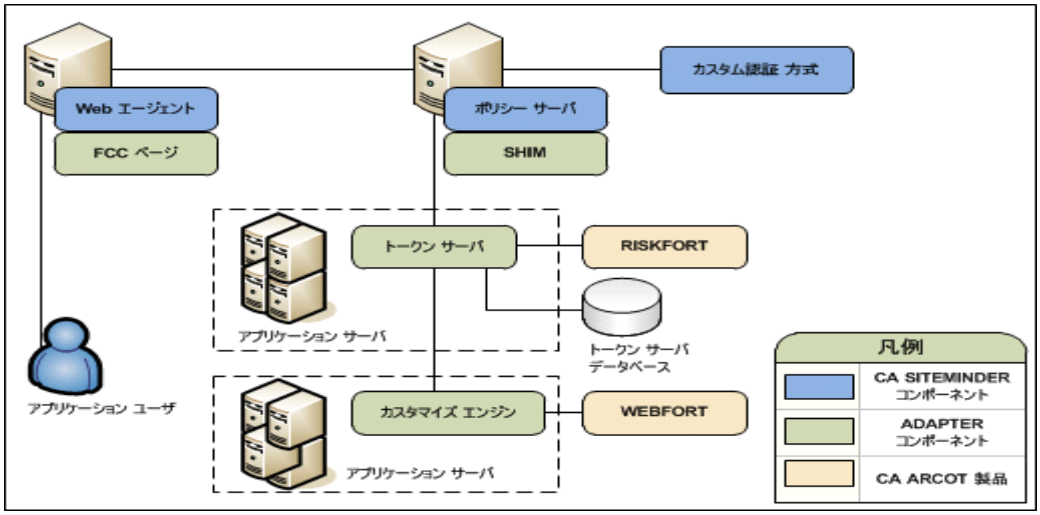
注: サポートされているバージョンの詳細については、SiteMinder プラットフォーム サポート マトリックスを参照してください。

以下の図の目的は次のとおりです。

- Adapter およびそのコンポーネントである CA Arcot RiskFort と CA Arcot WebFort を SiteMinder 環境に統合する方法を示します。
- 主要コンポーネントおよびそれらの一般的な関係を詳述します。 これはワークフロー図ではありません。

注: すべての CA Arcot コンポーネントのインストールおよび設定の詳細については、CA アルコットのマニュアルを参照してください。

図 3: CA SiteMinder および CA Arcot 統合アーキテクチャ



オンプレミス Arcot 統合での認証

CA Arcot は、認証（CA Arcot WebFort）およびリスク評価（CA Arcot RiskFort）プロセスに従って統合された環境での認証サービスを前提としています。認証プロセス中については以下のとおりです。

- CA Arcot WebFort は、SiteMinder で保護されたリソースをリクエストするユーザの ID が正当であることの確認に役立つ強力な認証を提供します。

  注: 強力な認証の詳細については、「CA Arcot WebFort インストールおよび展開ガイド」を参照してください。 サポートされている認証方式の設定の詳細については、「CA Arcot WebFort 管理ガイド」を参照してください。

- CA Arcot RiskFort は一連のデータを収集して、各トランザクションに関連付けられたリスクのレベルを特定するリスク評価を実行します。

  注: リスク評価およびリスク スコアの詳細については、「CA Arcot RiskFort インストールおよび展開ガイド」を参照してください。 リスク スコアリングの設定の詳細については、「CA Arcot RiskFort 管理ガイド」を参照してください。

リスク評価の結果は、リスク スコア、および認証の許可または拒否などの対応するアドバイス（推奨アクション）です。

CA Arcot は、必要に応じてアドバイスをポリシー サーバに転送し、許可サービスを続行します。

注: Adapter のワークフロー、および認証中の各 CA Arcot コンポーネントのロールの詳細については、「CA Arcot Adapter for CA SiteMinder インストールおよび設定ガイド」を参照してください。

信頼レベルおよび SiteMinder 許可

ポリシー サーバは統合環境で許可サービスを保持し、許可決定にリスク スコアを適用できます。 リスク スコアは認証プロセス (P. 252)中に作成されます。

ポリシー サーバは SiteMinder 信頼レベル（信頼レベル）としてリスク スコアを適用します。 信頼レベルはリスク スコアに基づいており、それ自体トランザクションが安全である可能性を表す整数です。

両方のアクセス管理モデルに信頼レベルを適用できます。

- ポリシーを持つリソースを保護している場合、以下のオブジェクトに信頼レベルを適用できます。
  - ポリシー レルム
  - アクティブなポリシー式
- EPM アプリケーションを持つリソースを保護している場合、以下のオブジェクトに信頼レベルを適用できます。
  - アプリケーション コンポーネント
  - SM_USER_CONFIDENCE_LEVEL SiteMinder が生成する属性を参照する名前付きの式で構成されるアプリケーション ロール。

注: ポリシー レルムまたはアプリケーション コンポーネントに信頼レベルを適用する場合、ユーザが信頼レベル サポートを有効にする (P. 256)必要があります。 信頼レベルを適用するアクティブなポリシー式またはアプリケーション ロールの使用は、以前のリリースからサポートされており、デフォルトで有効になります。 ポリシーとアプリケーションへの信頼レベル適用の詳細については、「ポリシー サーバ設定ガイド」を参照してください。

以下のワークフローの例では、両方の値の関係を詳述し、ポリシー サーバが許可決定にどのように信頼レベルを適用するか説明します。

1. ユーザが正常に認証された後、アダプタは以下の代数公式を使用して、リスク スコアを信頼レベルに変換します。

   （100-リスク スコア） * 10 = 信頼レベル

2. アダプタは SiteMinder セッション チケットに信頼レベルを挿入します。

   注: セッション チケットの詳細については、「ポリシー サーバ設定ガイド」を参照してください。

3. ユーザが保護されたリソースをリクエストすると、ポリシー サーバは、セッション チケット内の信頼レベルをポリシーまたはアプリケーションで設定された信頼レベルと比較します。

4. 以下の処理が行われます。

   - ポリシー ルールがアクセスを許可するように設定され、ユーザの信頼レベルが、ポリシー レルムまたはアクティブなポリシー式で設定された信頼レベル以上である場合、ポリシー ルールはトリガされます。

     注: ユーザの信頼レベルがポリシーで設定された信頼レベル未満である場合、SiteMinder はアクセスを拒否します。

   - ポリシー ルールがアクセスを拒否するように設定され、ユーザの信頼レベルが、ポリシー レルムまたはアクティブなポリシー式で設定された値未満である場合、ポリシー ルールはトリガされます。

   - ユーザの信頼レベルがアプリケーション ロールで設定された信頼レベル未満である場合、ユーザはロール メンバシップから除外されます。また、SiteMinder はアクセスを拒否します。

   - ユーザの信頼レベルがアプリケーション コンポーネントで設定された信頼レベル以上である場合、SiteMinder はアクセスを付与します。

詳細情報:

ポリシー管理モデル (P. 65)

リスク スコアと信頼レベルの比較

リスク スコアと信頼レベルは、両方ともトランザクションの安全を確認するのに役立ちますが、両方の値には違いがあります。 許可決定について計画を立てる場合は、以下の違いを考慮してください。

CA Arcot リスク スコア	SiteMinder 信頼レベル
数値スケール（0 ～ 100）はリスク スコアを表します。	数値スケール（0 ～ 1000）は信頼レベルを表します。
リスク スコアが低いほど、トランザクションが安全である可能性が大きくなります。	信頼レベルが高いほど、トランザクションが安全である可能性が大きくなります。 **注**: 値ゼロ (0) は信頼がないことを示します。信頼がないと、SiteMinder はリクエストされたリソースへのアクセスを拒否します。

以下のワークフローの例では、リスク スコアと信頼レベルの逆比例の関係を詳述します。

1. ユーザは SiteMinder によって保護されたリソースをリクエストし、認証のために CA Arcot に転送されます。
2. アダプタは認証とリスク分析を通じてユーザをガイドします。 CA Arcot の評価とスコアリング ルールに基づいて、ユーザは 30 のリスク スコアで認証されます。 リスク スコアが低いほど安全なトランザクションであることを示します。

   注: リスク評価およびスコアリング ルールの詳細については、「CA Arcot RiskFort 管理ガイド」を参照してください。
3. アダプタ：
   a. 認証決定をポリシー サーバに転送します。
   b. 以下の代数公式を使用して、リスク スコアを信頼レベルに変換します。

      （100 - リスク スコア） * 10 = 信頼レベル

      この例で、アダプタは以下の代数公式を使用して、リスク スコアを信頼レベルに変換します。

      (100 - 30) * 10 = 700

      信頼レベルが高いほど安全なトランザクションであることを示します。

4. アダプタはユーザのセッション チケットに信頼レベルを挿入します。
5. ユーザは、少なくとも 700 の信頼レベルを必要とするポリシーまたはアプリケーションによって保護されたリソースをリクエストします。
6. ポリシー サーバはリソースへのアクセス許可を付与します。

認可決定のための信頼レベル サポートの有効化

オプションで許可決定に信頼レベルを適用できます。 以下の点を考慮します。

- 以下のオブジェクトに信頼レベルを適用できます。
  - ポリシー レルム
  - アクティブなポリシー式
  - アプリケーション コンポーネント
  - SM_USER_CONFIDENCE_LEVELSiteMinder で生成された属性を参照する名前付き式が含まれるアプリケーション ロール。

  注: ポリシーとアプリケーションへの信頼レベル適用の詳細については、「ポリシー サーバ設定ガイド」を参照してください。
- 信頼レベル サポートを有効にするだけで、レルムまたはアプリケーション コンポーネントに信頼レベルを適用できます。信頼レベルを適用するアクティブなポリシー式またはアプリケーション ロールの使用は、以前のリリースからサポートされており、デフォルトで有効になります。

以下の手順に従います。

1. SiteMinder 環境内の任意のポリシー サーバ ホスト システムにログインします。
2. XPSConfig ユーティリティを起動します。

   XPSConfig はオプションを要求します。
3. 「SM」と入力して Enter キーを押します。

   XPSConfig はオプションを要求します。
4. 「15」と入力して Enter キーを押します。

   ConfidenceLevelSupportEnabled パラメータが表示されます。

5. 「C」と入力して Enter キーを押します。

   パラメータの保留の値が True として表示されます。

6. XPSConfig ユーティリティを終了します。
7. ポリシー サーバを再起動します。

   信頼レベル サポートが有効になります。

CA Arcot 統合ユース ケース

以下のユース ケースでは、SiteMinder を CA Arcot の強力な認証およびリスク評価と統合する方法を説明します。 ユース ケースは単純な統合から始まり、より複雑なシナリオに進みます。

CA Arcot 認証およびリスク分析

最も単純な展開には、アダプタおよびすべての関連するコンポーネントの SiteMinder への統合が含まれます。

アダプタは、認証 (CA Arcot WebFort) およびリスク評価 (CA Arcot RiskFort) プロセスを通じてユーザをガイドし、認証中にリスク スコア (P. 252)を適用します。

以下の手順に従います。

1. CA Arcot RiskFort および CA Arcot WebFort を必ずインストールおよび設定してください。

   注: 詳細については、それぞれの CA Arcot インストールおよび展開ガイドを参照してください。

2. CA Arcot Adapter およびすべての関連するコンポーネントをインストールし、展開します。 これらのコンポーネントには一連のフォーム認証情報コレクタ ファイルが含まれます。 これらのファイルにより、ユーザはユーザ認証情報を収集するためにアダプタ HTML フォーム認証方式を使用できます。

   注: アダプタおよびすべての関連するコンポーネントのインストールと設定の詳細については、「CA Arcot Adapter for CA SiteMinder インストールおよび設定ガイド」を参照してください。

3. 以下の手順を実行します。

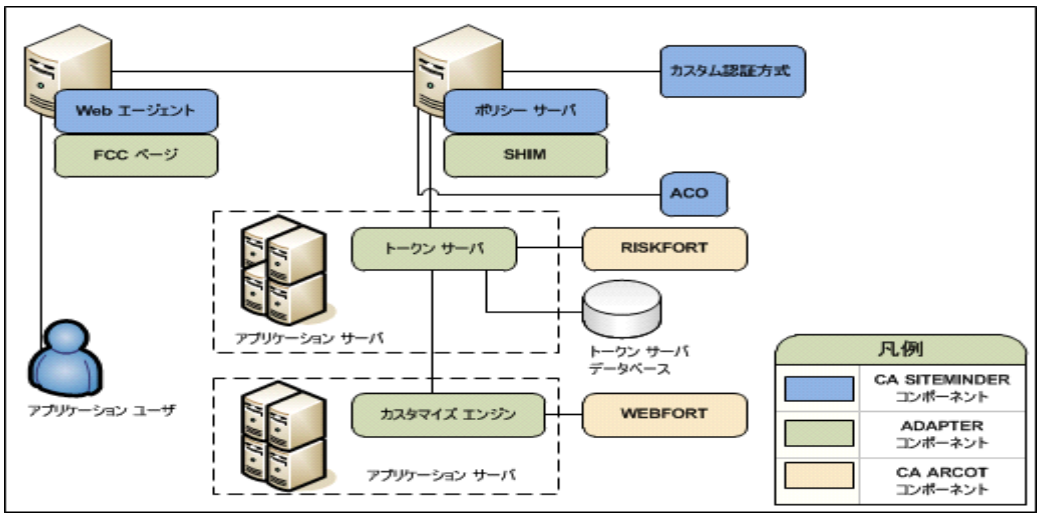
   a. アダプタ ライブラリを呼び出すために SiteMinder カスタム認証方式を設定します。

   b. どの Web エージェントが CA Arcot 統合に含まれるか決定します。統合をサポートするためにそれぞれのエージェント設定オブジェクト（ACO）を設定します。

   注: 必要なカスタム認証方式および ACO 設定の詳細については、「CA Arcot Adapter for CA SiteMinder インストールおよび設定ガイド」を参照してください。認証方式および ACO パラメータ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。

以下の図は、この展開シナリオを示しています。

図 4: CA Arcot 認証およびリスク分析



SiteMinder 認証および CA Arcot リスク分析

SiteMinder 認証方式の統合によってのみリスク評価用のアダプタを設定できます。統合の一部である SiteMinder 認証方式はバックアップ認証として知られています。

ユーザが認証のバックアップとして SiteMinder 認証方式を使用する場合、Shim は SiteMinder と SiteMinder 認証方式の間のインターフェースとして機能します。

注: 認証のバックアップの詳細については、「CA Arcot Adapter for CA SiteMinder インストールおよび設定ガイド」を参照してください。 すべての SiteMinder 認証方式でバックアップ認証がサポートされているとは限りません。 詳細については、SiteMinder プラットフォーム サポート マトリックスを参照してください。

次の手順に従ってください:

1. CA Arcot 認証およびリスク分析 (P. 257)でリスト表示された手順を完了します。

   重要: 統合には、SiteMinder カスタム認証方式の設定が必要です。 SiteMinder カスタム認証方式は必要なアダプタ ライブラリを呼び出します。 バックアップ認証を展開している場合でも、このライブラリは必要です。

2. 有効な CA Arcot パラメータを持つ SiteMinder カスタム認証方式を設定してください。 このパラメータは、バックアップ認証として機能している SiteMinder 認証方式をサポートするユーザ フローを表す必要があります。 ［パラメータ］フィールドにこの値を入力します。

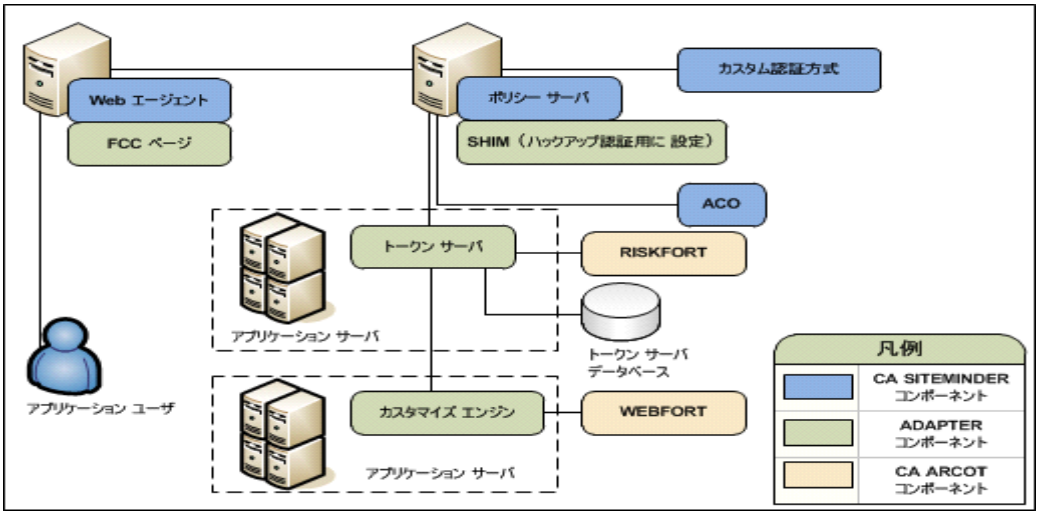
   注: ユーザ フローおよび対応するパラメータ値の詳細については、「CA Arcot Adapter for CA SiteMinder インストールおよび設定ガイド」を参照してください。 SiteMinder カスタム認証方式の設定の詳細については、「ポリシー サーバ設定ガイド」を参照してください。

3. ハックアップ認証として SiteMinder 認証方式を使用するために Shim を設定します。

   注: バックアップ認証方式設定の詳細については、「CA Arcot Adapter for CA SiteMinder インストールおよび設定ガイド」を参照してください。

以下の図は、この展開シナリオを示しています。

図 5: CA SiteMinder 認証および CA Arcot リスク分析



SiteMinder 許可および信頼レベル

両方のアクセス管理モデルへの信頼レベル (P. 253)の追加により、ポリシー サーバ許可サービスを拡張できます。

信頼レベルを追加すると、許可決定に CA Arcot リスク分析結果を適用できます。

以下の手順に従います。

1. CA Arcot 認証およびリスク分析 (P. 257) または SiteMinder 認証および CA Acrot リスク分析 (P. 258) の手順を完了します。
2. （オプション）ポリシー レルムまたはアプリケーション コンポーネントへの信頼レベルの適用を計画する場合は、信頼レベル サポートを有効 (P. 256) にします。 信頼レベルを適用するアクティブなポリシー式またはアプリケーション ロールの使用は、以前のリリースからサポートされており、デフォルトで有効になります。
3. 以下のいずれかを実行します。
   - リソースを保護するポリシーを使用している場合は、1 つ以上のポリシー レルムまたはアクティブなポリシー式に信頼レベルを追加します。

- リソースを保護するアプリケーションを使用している場合は、1 つ以上のアプリケーション コンポーネントまたはアプリケーション ロールに信頼レベルを追加します。

  注: ポリシーとアプリケーションへの信頼レベル適用の詳細については、「ポリシー サーバ設定ガイド」を参照してください。

詳細情報:

ポリシー管理モデル (P. 65)

ユーザ ストア考慮事項

統合が適用されるすべての SiteMinder ユーザを、CA Arcot WebFort データベースで使用できるようにする必要があります。

詳細については、CA Arcot サポートにお問い合わせください。

注: 問い合わせ先については、「CA Arcot Adapter for CA SiteMinder インストールおよび設定ガイド」を参照してください。

CA Arcot A-OK の統合

CA Arcot A–OK Adapter™ （A–OK Adapter）を使用して、SiteMinder をホストされた CA Arcot A–OK サービスと統合します。

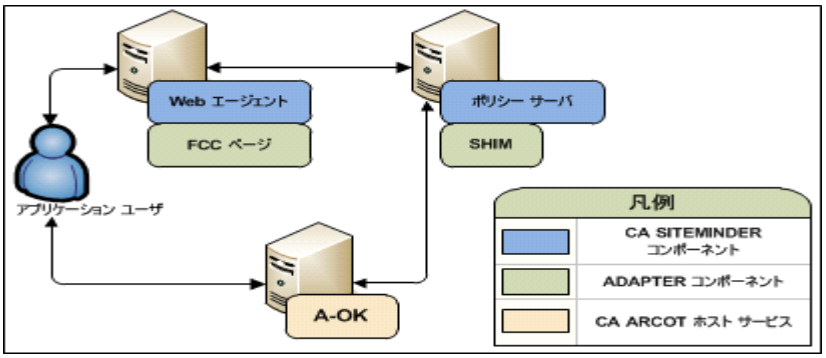
注: 統合には、A–OK Adapter の最小バージョンが必要です。 サポートされているバージョンの詳細については、SiteMinder プラットフォーム サポート マトリックスを参照してください。

以下の図の目的は次のとおりです。

- A–OK Adapter およびそのコンポーネントを SiteMinder 環境に統合する方法を示します。
- 主要コンポーネントおよびそれらの一般的な関係を詳述します。 これはワークフロー図ではありません。

注: A–OK Adapter のインストールおよび設定の詳細については、「CA Arcot A–OK Adapter for CA SiteMinder インストールおよび設定ガイド」を参照してください。

図 6: CA SiteMinder および CA Arcot A-OK 統合アーキテクチャ



ホストされた CA Arcot 統合での認証

CA Arcot A–OK は、認証およびリスク評価プロセスに従って統合された環境での認証サービスを前提としています。 CA Arcot A–OK は一連の SAML リクエストおよびレスポンスを使用して認証ワークフローを進めます。

注: 認証ワークフローの詳細については、「CA Arcot A–OK Adapter for CA SiteMinder インストールおよび設定ガイド」を参照してください。

リスク評価の結果は、リスク スコア、および認証の許可または拒否などの対応するアドバイス（推奨アクション）です。

CA Arcot A–OK は、必要に応じてアドバイスをポリシー サーバに転送し、許可サービスを続行します。

注: ユーザ認証情報の管理およびリスク評価プロセスに関連付けられたルールの設定の詳細については、「CA Arcot A–OK ユーザ管理ガイド」を参照してください。

信頼レベルおよび SiteMinder 許可

ポリシー サーバは統合環境で許可サービスを保持し、許可決定にリスク スコアを適用できます。 リスク スコアは認証プロセス (P. 262)中に作成されます。

ポリシー サーバは SiteMinder 信頼レベルとしてリスク スコアを適用します。信頼レベルはリスク スコアに基づいており、それ自体トランザクションが安全である可能性を表す整数です。

両方のアクセス管理モデルに信頼レベルを適用できます。

- ポリシーを持つリソースを保護している場合、以下のオブジェクトに信頼レベルを適用できます。
  - ポリシー レルム
  - アクティブなポリシー式
- EPM アプリケーションを持つリソースを保護している場合、以下のオブジェクトに信頼レベルを適用できます。
  - アプリケーション コンポーネント
  - SM_USER_CONFIDENCE_LEVEL SiteMinder が生成する属性を参照する名前付きの式で構成されるアプリケーション ロール。

注: ポリシー レルムまたはアプリケーション コンポーネントに信頼レベルを適用する場合、ユーザが信頼レベル サポートを有効にする (P. 265)必要があります。 信頼レベルを適用するアクティブなポリシー式またはアプリケーション ロールの使用は、以前のリリースからサポートされており、デフォルトで有効になります。 ポリシーとアプリケーションへの信頼レベル適用の詳細については、「ポリシー サーバ設定ガイド」を参照してください。

以下のワークフローの例では、両方の値の関係を詳述し、ポリシー サーバが許可決定にどのように信頼レベルを適用するか説明します。

1. ユーザが正常に認証された後、A–OK Adapter は以下の代数公式を使用して、リスク スコアを信頼レベルに変換します。

   （100-リスク スコア） * 10 = 信頼レベル

2. A–OK Adapter は SiteMinder セッション チケットに信頼レベルを挿入します。

   注: セッション チケットの詳細については、「ポリシー サーバ設定ガイド」を参照してください。

3. ユーザが保護されたリソースをリクエストすると、ポリシー サーバは、セッション チケット内の信頼レベルをポリシーまたはアプリケーションで設定された信頼レベルと比較します。

4. 以下の処理が行われます。

   - ポリシー ルールがアクセスを許可するように設定され、ユーザの信頼レベルが、ポリシー レルムまたはアクティブなポリシー式で設定された信頼レベル以上である場合、ポリシー ルールはトリガされます。

     注: ユーザの信頼レベルがポリシーで設定された信頼レベル未満である場合、SiteMinder はアクセスを拒否します。

   - ポリシー ルールがアクセスを拒否するように設定され、ユーザの信頼レベルが、ポリシー レルムまたはアクティブなポリシー式で設定された値未満である場合、ポリシー ルールはトリガされます。

   - ユーザの信頼レベルがアプリケーション ロールで設定された信頼レベル未満である場合、ユーザはロール メンバシップから除外されます。また、SiteMinder はアクセスを拒否します。

   - ユーザの信頼レベルがアプリケーション コンポーネントで設定された信頼レベル以上である場合、SiteMinder はアクセスを付与します。

リスク スコアと信頼レベルの比較

リスク スコアと信頼レベルは、両方ともトランザクションの安全を確認するのに役立ちますが、両方の値には違いがあります。 許可決定について計画を立てる場合は、以下の違いを考慮してください。

CA Arcot リスク スコア	SiteMinder 信頼レベル
数値スケール（0 ～ 100）はリスク スコアを表します。	数値スケール（0 ～ 1000）は信頼レベルを表します。
リスク スコアが低いほど、トランザクションが安全である可能性が大きくなります。	信頼レベルが高いほど、トランザクションが安全である可能性が大きくなります。 **注**: 値ゼロ (0) は信頼がないことを示します。信頼がないと、SiteMinder はリクエストされたリソースへのアクセスを拒否します。

以下のワークフローの例では、リスク スコアと信頼レベルの逆比例の関係を詳述します。

1. ユーザは SiteMinder によって保護されたリソースをリクエストし、CA Arcot A–OK の認証用に転送されます。
2. A–OK Adapter は認証とリスク分析を通じてユーザをガイドします。CA Arcot A–OK の評価とスコアリング ルールに基づいて、ユーザは 30 のリスク スコアで認証されます。 リスク スコアが低いほど安全なトランザクションであることを示します。

   注: ユーザ認証情報の管理およびリスク評価プロセスと関連付けられるルール設定の詳細については、「CA Arcot A–OK ユーザ管理ガイド」を参照してください。
3. A–OK Adapter：
   a. 認証決定をポリシー サーバに転送します。
   b. 以下の代数公式を使用して、リスク スコアを信頼レベルに変換します。

      （100 - リスク スコア） * 10 = 信頼レベル

      この例で、A–OK Adapter は以下の代数公式を使用して、リスク スコアを信頼レベルに変換します。

      (100 - 30) * 10 = 700

      信頼レベルが高いほど安全なトランザクションであることを示します。
4. A–OK Adapter はユーザのセッション チケットに信頼レベルを挿入します。
5. ユーザは、少なくとも 700 の信頼レベルを必要とするポリシーまたはアプリケーションによって保護されたリソースをリクエストします。
6. ポリシー サーバはリソースへのアクセス許可を付与します。

信頼レベル サポートの有効化

オプションで許可決定に信頼レベルを適用できます。 以下の点を考慮します。

- 以下のオブジェクトに信頼レベルを適用できます。
  - ポリシー レルム
  - アクティブなポリシー式

- アプリケーション コンポーネント
- SM_USER_CONFIDENCE_LEVELSiteMinder で生成された属性を参照する名前付き式が含まれるアプリケーション ロール。

注: ポリシーとアプリケーションへの信頼レベル適用の詳細については、「ポリシー サーバ設定ガイド」を参照してください。

- 信頼レベル サポートを有効にするだけで、レルムまたはアプリケーション コンポーネントに信頼レベルを適用できます。信頼レベルを適用するアクティブなポリシー式またはアプリケーション ロールの使用は、以前のリリースからサポートされており、デフォルトで有効になります。

以下の手順に従います。

1. SiteMinder 環境内の任意のポリシー サーバ ホスト システムにログインします。
2. XPSConfig ユーティリティを起動します。

   XPSConfig はオプションを要求します。
3. 「SM」と入力して Enter キーを押します。

   XPSConfig はオプションを要求します。
4. 「15」と入力して Enter キーを押します。

   ConfidenceLevelSupportEnabled パラメータが表示されます。
5. 「C」と入力して Enter キーを押します。

   パラメータの保留の値が True として表示されます。
6. XPSConfig ユーティリティを終了します。
7. ポリシー サーバを再起動します。

   信頼レベル サポートが有効になります。

CA Arcot A-OK 統合ユース ケース

以下のユース ケースでは、SiteMinder を CA Arcot A-OK の強力な認証およびリスク評価と統合する方法を説明します。 ユース ケースは単純な統合から始まり、より複雑なシナリオに進みます。

CA Arcot A–OK 認証およびリスク分析

最も単純な展開には A–OK Adapter およびすべての関連するコンポーネントの SiteMinder への統合が含まれます。

A–OK Adapter は、認証およびリスク評価プロセスを通じてユーザをガイドし、認証プロセス (P. 262)中にリスク スコアを適用します。

以下の手順に従います。

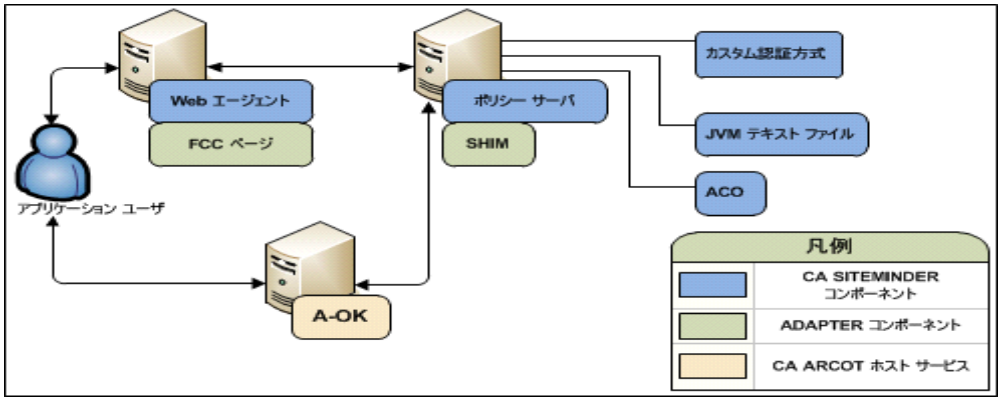
1. CA Arcot A–OK サービスは必ず利用可能にしてください。
2. A–OK Adapter およびすべての関連するコンポーネントをインストールし、展開します。 これらのコンポーネントには一連のフォーム認証情報コレクタ ファイルが含まれます。 これらのファイルにより、ユーザはユーザ認証情報を収集するために A–OK Adapter HTML フォーム認証方式を使用できます。

   注: A–OK Adapter およびすべての関連するコンポーネントのインストールおよび設定の詳細については、「CA Arcot A–OK Adapter for CA SiteMinder インストールおよび設定ガイド」を参照してください。
3. 以下の手順を実行します。
   a. A–OK Adapter ライブラリを呼び出すために SiteMinder カスタム認証方式を設定します。
   b. どの Web エージェントが CA Arcot A–OK 統合に含まれるか決定します。 統合をサポートするためにそれぞれのエージェント設定オブジェクト（ACO）を設定します。
   c. ポリシー サーバの Java Virtual Machine （JVM）ファイル（JVMOptions.txt）に A–OK Adapter JAR ファイル、証明書およびプロパティ ファイルを追加します。

   注: 必要なカスタム認証方式、ACO 設定、およびポリシー サーバ JVM ファイルへの編集の詳細については、「CA Arcot A–OK Adapter for CA SiteMinder インストールおよび設定ガイド」を参照してください。 認証方式および ACO パラメータ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。

以下の図は、この展開シナリオを示しています。

図 7: CA Arcot A-OK 認証およびリスク分析



SiteMinder 許可および信頼レベル

両方のアクセス管理モデルへの信頼レベル (P. 262)の追加により、ポリシー サーバ許可サービスを拡張できます。

信頼レベルを追加すると、許可決定に CA Arcot A–OK リスク分析結果を適用できます。

以下の手順に従います。

1. CA Arcot A–OK 認証およびリスク分析 (P. 267) の手順を完了します。
2. (オプション) ポリシー レルムまたはアプリケーション コンポーネントへの信頼レベルの適用を計画する場合は、信頼レベル サポートを有効 (P. 265) にします。 信頼レベルを適用するアクティブなポリシー式またはアプリケーション ロールの使用は、以前のリリースからサポートされており、デフォルトで有効になります。
3. 以下のいずれかの操作を実行します。
   - リソースを保護するポリシーを使用している場合は、1 つ以上のポリシー レルムまたはアクティブなポリシー式に信頼レベルを追加します。
   - リソースを保護するアプリケーションを使用している場合は、1 つ以上のアプリケーション コンポーネントまたはアプリケーション ロールに信頼レベルを追加します。

     注: ポリシーとアプリケーションへの信頼レベル適用の詳細については、「ポリシー サーバ設定ガイド」を参照してください。

詳細情報:

ポリシー管理モデル (P. 65)

ユーザ ストア考慮事項

統合が適用されるすべての SiteMinder ユーザを、CA Arcot A–OK のホストされたサービスで使用できるようにする必要があります。

詳細については、CA Arcot サポートにお問い合わせください。

注: 問い合わせ先については、「CA Arcot A–OK Adapter for CA SiteMinder インストールおよび設定ガイド」を参照してください。

[assign the value for dlp in your book] Content Classification Service の統合

SiteMinder を [assign the value for dlp in your book] Content Classification Service （CCS）と統合すると、ポリシー サーバは CCS コンテンツ評価を使用してコンテンツ認識の許可を判断できます。

事前に、以下の項目について考慮してください。

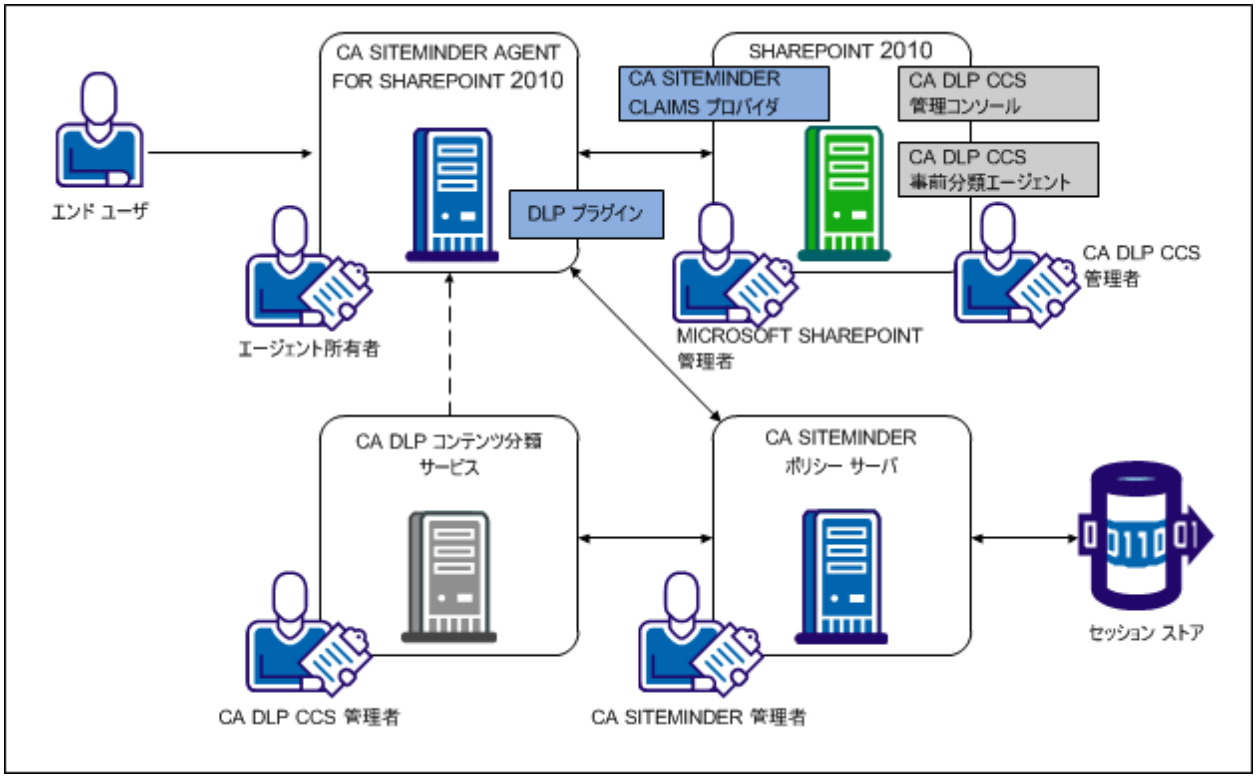
- 統合には、SiteMinder の最小バージョン、CCS および SiteMinder Agent for S 統合に対して SSL を有効にする SharePoint が必要です。

  注: 詳細については、SiteMinder プラットフォーム サポート マトリックスを参照してください。

- 統合を有効にするには複数の組織ロールが必要です。以下のユーザと統合を調整します。
  - CCS 管理者
  - SiteMinder 管理者
  - SharePoint 用 SiteMinder エージェントの所有者

以下の図の目的は次のとおりです。

- 統合環境内の CCS と SiteMinder コンポーネントの一般的な関係を示します。 この図は、ワークフロー、または統合環境で展開されるすべてのコンポーネントを表すものではありません。
- 必要なコンポーネントのインストールまたは設定を行う各担当者を関連付けています。



[assign the value for dlp in your book] Content Classfication Service

統合における CCS のロールは、事前定義されたコンテンツ分類を SiteMinder ポリシー サーバが使用できるようにすることです。分類は、企業環境によくあるドキュメント タイプに相当します。ポリシー サーバは、コンテンツ認識の許可の判断を行うために分類を使用します。

[assign the value for dlp in your book] Content Classification Service (P. 269) の点線が示すように、ポリシー サーバの許可の判断の時点でコンテンツ分類が使用できない場合、CCS はリソースを直接要求して分類または再分類できます。 CCS は以下を実行します。

- 許可の判断を行うポリシー サーバに結果を渡します。
- 今後の許可の判断のために結果を CCS 分類キャッシュに追加します。

注: CCS およびコンテンツ分類の詳細については、「*[assign the value for dlp in your book] Content Classification Service Integration Guide*」を参照してください。 このガイドは [assign the value for dlp in your book] Content Classification Service のマニュアル選択メニューに含まれています。

[assign the value for dlp in your book] Content Classification Service 事前分類エージェント

統合における [assign the value for dlp in your book] CCS 事前分類エージェントのロールは、SharePoint ドキュメントをオフラインでスキャンおよび分類することです。 ドキュメントをオフラインで分類することにより、ポリシー サーバの許可の判断の一部としてドキュメント分類を取得する必要がなくなります。

注: 事前分類エージェントおよび分類サービス スキャンの詳細については、「*[assign the value for dlp in your book] Content Classification Service Integration Guide*」を参照してください。 このガイドは [assign the value for dlp in your book] Content Classification Service のマニュアル選択メニューに含まれています。

SiteMinder ポリシー サーバ

統合における SiteMinder ポリシー サーバのロールは、ポリシー決定ポイント (PDP) として機能することです。ポリシー サーバは以下を実行します。

- 統合環境のすべての認証および許可サービスを維持します。
- SharePoint 用 SiteMinder エージェントと通信して、保護されているドキュメントのリソース情報を取得します。
- [assign the value for dlp in your book] CCS と通信して、保護されているドキュメントのコンテンツ分類を取得します。ポリシー サーバはコンテンツ認識の許可の判断を行うためにこの結果を使用します。

設定されていれば、ポリシー サーバは [assign the value for dlp in your book] CCS 用の使い捨てのセキュリティ トークンを作成できます。 [assign the value for dlp in your book] CCS はリソースを直接要求するためにトークンを使用します。 許可の判断の一部として分類または再分類する必要がある場合、CCS はリソースを要求します。

注: コンテンツ分類をエンタープライズ ポリシー管理アプリケーションに適用する詳細については、「*ポリシー サーバ設定ガイド*」を参照してください。

SharePoint 用 SiteMinder エージェント

統合における SharePoint 用 SiteMinder エージェントのロールは、ポリシー実行ポイント（PEP）として機能することです。 SharePoint 用エージェントは以下を実行します。

- SharePoint ドキュメントに対する要求をインターセプトします。
- ドキュメントのリソース情報を抽出します。
- リソース情報をポリシー サーバに渡します。

SiteMinder セッション ストア

SiteMinder セッション ストアのロールは、クラスタ環境のすべてのポリシー サーバが使い捨てのセキュリティ トークンを使用できるようにすることです。設定されていれば、ポリシー サーバは [assign the value for dlp in your book] CCS 用のセキュリティ トークンを作成します。 保護されているドキュメントへのアクセスが必要な場合に、トークンは [assign the value for dlp in your book] CCS 用の認証情報として機能します。

[assign the value for dlp in your book] CCS は、コンテンツ分類をポリシー サーバに提供できないときに、保護されているドキュメントにアクセスする必要があります。 リソースを要求すると CCS は以下を実行できます。

- ドキュメントを分類または再分類します。
- コンテンツ分類をポリシー サーバに提供します。
- 今後のポリシー サーバの許可要求のために、コンテンツ分類を [assign the value for dlp in your book] 分類キャッシュに追加します。

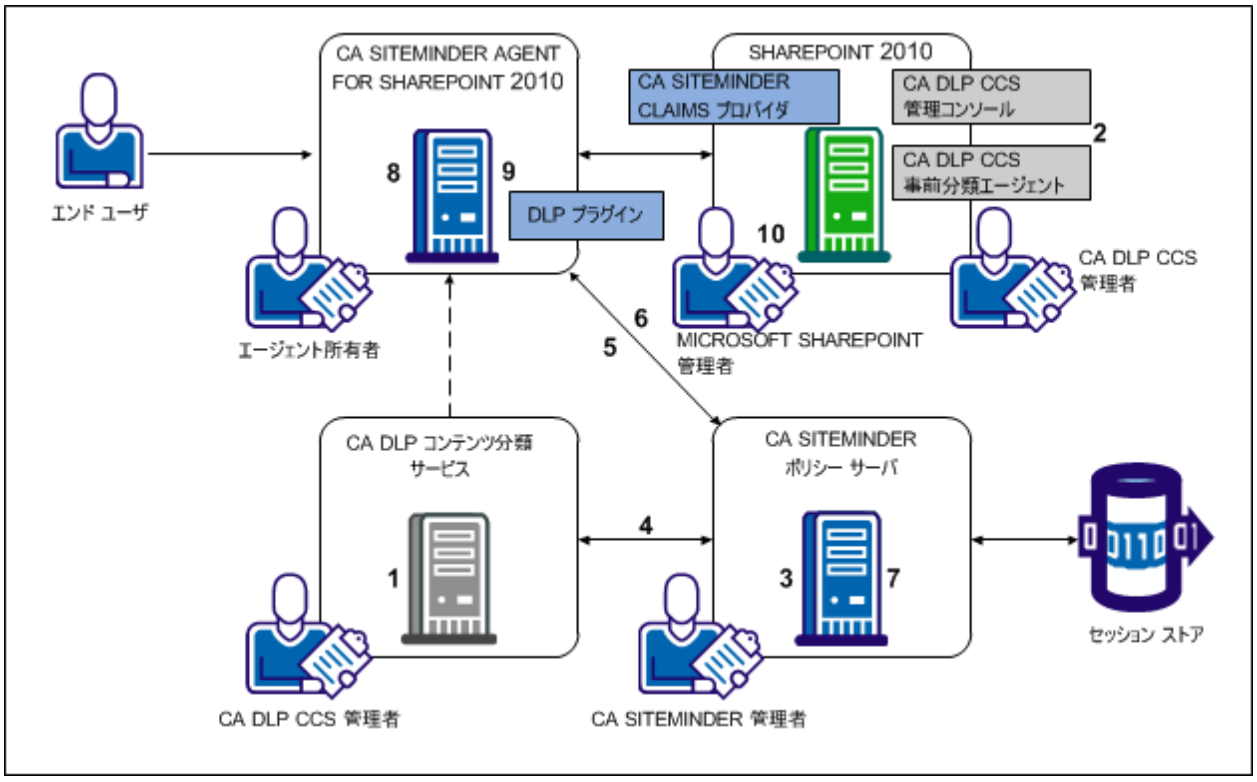
プロセスの一部として、SharePoint 用エージェントは、信頼性を検証するためにポリシー サーバにトークンを返します。SharePoint 用エージェントがトークンを作成しなかったポリシー サーバに検証要求を送信し、かつ環境が以下の場合は次のとおりです。

- 環境にセッション ストアが含まれている場合、ポリシー サーバはトークンを取得および検証して、[assign the value for dlp in your book] CCS を許可します。
- 環境にセッション ストアが含まれていない場合、ポリシー サーバはトークンを検証できず、許可要求を拒否します。

[assign the value for dlp in your book] Content Classification Service 統合ロードマップ

以下の図で示すものは次のとおりです。

- サンプル [assign the value for dlp in your book] および SiteMinder の統合を示します。
- 各コンポーネントがインストールおよび設定される順序を示します。



以下の表で、図に示した各手順およびタスクの各担当者を示します。

手順	アクション	担当者
1	SSL で通信するように [assign the value for dlp in your book] CCS をインストールおよび設定する (P. 274)。	[assign the value for dlp in your book] CCS 管理者
2	[assign the value for dlp in your book] 事前分類エージェントをインストールおよび設定する (P. 274)。	[assign the value for dlp in your book] CCS 管理者
3	統合に対して SSL を有効にする (P. 275)。	SiteMinder 管理者
4	[assign the value for dlp in your book] CCS への接続を設定する (P. 276)。	SiteMinder 管理者
5	SharePoint 用エージェントのエージェント設定オブジェクトを変更する (P. 277)。	SiteMinder 管理者
6	DLP 除外リスト パラメータを有効にする (P. 278)。	SiteMinder 管理者
7	許可失敗メッセージを有効にする (P. 279)。	SiteMinder 管理者
8	SharePoint マルチ認証のプロキシ ルールを変更する (P. 280)。	SharePoint エージェント所有者
9	DLP プラグインを有効にする (P. 283)。	SharePoint エージェント所有者
10	[assign the value for dlp in your book] CCS に SharePoint アプリケーションへの読み取りアクセス権を提供する (P. 284)。	SharePoint 管理者

[assign the value for dlp in your book] CCS 管理者タスク

[assign the value for dlp in your book] CCS 管理者は以下を実行します。

- 1 つ以上の [assign the value for dlp in your book] Content Classification Services をインストールして、各インスタンスを SSL で通信するように設定します。 統合では、[assign the value for dlp in your book] Content Classification Service および SiteMinder ポリシー サーバが安全に通信する必要があります。

SiteMinder 管理者には、ポリシー サーバ ホスト システム上で SSL を有効にするために CCS サーバ証明書ファイルが必要です。

重要: インスタンスを安全に通信するように設定するときには、すべての CCS インスタンスに対して同じ証明書およびパスワードを使用します。

- [assign the value for dlp in your book] CCS 事前分類エージェントを SharePoint 環境にインストールして、分類サービス スキャンをスケジュールします。[assign the value for dlp in your book] CCS 管理コンソールは事前分類エージェントと共にインストールされます。

注: 詳細については、「*[assign the value for dlp in your book] Content Classification Service Integration Guide*」を参照してください。このガイドは [assign the value for dlp in your book] Content Classification Service のマニュアル選択メニューに含まれています。

SiteMinder 管理者タスク

SiteMinder 管理者は統合用の SiteMinder 環境を有効にします。以下の順序で統合手順を実行します。

1. 統合に対して SSL を有効にする。
2. [assign the value for dlp in your book] CCS への接続を設定する。
3. SharePoint エージェント設定オブジェクトを変更する。
4. DLP 除外リスト パラメータを有効にする。
5. 許可失敗メッセージを有効にする。

統合に対する SSL の有効化

統合では、[assign the value for dlp in your book] CCS および SiteMinder ポリシー サーバが安全に通信する必要があります。

- [assign the value for dlp in your book] CCS 管理者は、すべての [assign the value for dlp in your book] CCS インスタンスを安全に通信するように設定する必要があります。 事前に、CCS サーバ証明書を [assign the value for dlp in your book] 管理者に要求します。統合に対する SSL の有効化にはサーバ証明書が必要です。
- SSL の有効化はローカル設定です。SharePoint ドキュメントを保護している各ポリシー サーバについては以下の手順に従います。

以下の手順に従います。

1. クライアント証明書チェーン ファイルを作成します。 チェーン ファイルは、証明書ファイルおよびそれぞれの秘密キーを含む単一のファイルです。

   重要: このファイルは PEM 形式である必要があります。

2. ポリシー サーバ ホスト システムにログインします。
3. CCS サーバ証明書およびクライアント証明書チェーン ファイルを展開します。
4. *siteminder_home*¥bin¥thirdparty¥axis2c に移動します。
5. 以下のファイルを開きます。

   `axis2.xml`

6. SERVER_CERT パラメータを見つけます。 サンプル値を CCS サーバ証明書ファイルへのパスに置換します。
7. KEY_FILE パラメータを見つけます。 サンプル値をクライアント証明書チェーン ファイルへのパスに置換します。
8. SSL_PASSPHRASE パラメータを見つけます。サンプル値をクライアント証明書チェーン ファイルの秘密キーの暗号化に使用するパスフレーズに置換します。
9. ファイルを保存します。

[assign the value for dlp in your book] Content Classification Service への接続の設定

ポリシー サーバは、以下を実行するために [assign the value for dlp in your book] CCS に接続する必要があります。

- 保護されているドキュメントのコンテンツ分類を取得します。
- コンテンツ分類を使用してコンテンツ認識の許可の判断を行います。

接続の設定はローカル設定です。 SharePoint ドキュメントを保護しているすべてのポリシー サーバについて、以下の手順を完了します。

以下の手順に従います。

1. スーパーユーザ管理者アカウントで 管理 UI にログインします。
2. ［ポリシー］-［DLP の設定］をクリックします。
3. ［SiteMinder DLP 統合有効］リストから「True」を選択します。

4. プライマリ [assign the value for dlp in your book] CCS の IP アドレスまたは完全修飾ドメイン名を入力します。
5. （オプション）追加の設定パラメータを入力します。

   注: パラメータの詳細については、［ヘルプ］をクリックしてください。
6. ［保存］をクリックします。
7. ポリシー サーバを再起動して、統合に対してポリシー サーバを有効化し、[assign the value for dlp in your book] CCS への接続を設定します。
8. 再起動されたポリシー サーバに登録されている任意の 管理 UI を再起動します。

SharePoint エージェント設定オブジェクトの変更

SharePoint エージェント設定オブジェクトを変更することにより、保護されているドキュメントからリソース情報を抽出するようにエージェントを設定します。 エージェントは許可プロセスの一部として情報をポリシー サーバに渡します。

以下の手順に従います。

1. 管理 UI にログインします。
2. ［インフラストラクチャ］-［エージェント設定オブジェクト］をクリックします。
3. SharePoint 2010 エージェント用のエージェント設定オブジェクトを見つけます。
4. 編集アイコンをクリックしてオブジェクトを開きます。
5. DLPSupportEnabled パラメータの以下の値を入力します。

   SHAREPOINT
6. ［サブミット］をクリックします。

   エージェント設定オブジェクトが統合に対して有効になります。
7. SharePoint 用エージェントの所有者に問い合わせます。 エージェント設定オブジェクトは、ポリシー サーバにおける Web エージェント設定ファイルに相当するものです。 SharePoint 用エージェントの統合を完了するには、個別の手順が Web 層上で必要です。 SharePoint 用エージェントの所有者がこのタスクを実行します。

DLP 除外リスト パラメータの有効化

SharePoint 2010 エージェント設定オブジェクトには DLP 除外リスト パラメータが含まれます。このパラメータには、ポリシー サーバが [assign the value for dlp in your book] CCS コンテンツ分類から除外するデフォルト リソースのセットが含まれます。 コンテンツ分類からリソースを除外すると、リソースを自動的に許可できることが SharePoint エージェントに示されます。

統合にはパラメータの有効化が必要です。

以下の手順に従います。

1. 管理 UI にログインします。
2. ［インフラストラクチャ］-[エージェント設定オブジェクト］をクリックします。
3. SharePoint 2010 エージェント用のエージェント設定オブジェクトを見つけます。
4. 編集アイコンをクリックしてオブジェクトを開きます。
5. 以下のパラメータを探します。

   `#DlpExclusionList`
6. 編集アイコンをクリックしてパラメータを開きます。
7. パラメータ名からポンド記号を削除します。
8. コンテンツ分類から追加リソースを除外する場合は、デフォルト セットに拡張子を追加します。

   注: 値はカンマで区切ります。
9. ［OK］をクリックします。
10. ［サブミット］をクリックします。

    エージェント設定オブジェクトが有効になります。

許可失敗メッセージの有効化

デフォルトでは、許可中に DLP コンテンツ チェックに失敗すると、ユーザは標準の HTTP 403 エラー メッセージにリダイレクトされます。

許可失敗メッセージを有効にして、別のわかりやすいメッセージを返します。

次の手順に従ってください：

1. テキスト ファイルまたは HTML ファイルのいずれかを使用して、カスタム エラー ページを作成します。 以下の点を考慮します。
   - ユーザをカスタム エラー ページにのみリダイレクトできます。アプリケーションはサポートされていません。
   - Internet Explorer を使用する環境で、カスタム HTML ファイルを展開する場合は、以下を含めます。
     - ヘッド要素内のスタイル要素。
     - 本文要素の末行。

     Internet Explorer がカスタム ページの代わりに標準エラー メッセージを表示することを防ぐために、HTML ファイルにはこれらのアイテムが必要です。
2. 管理 UI にログインします。
3. ［インフラストラクチャ］-［エージェント設定オブジェクト］をクリックします。
4. SharePoint 2010 エージェント用のエージェント設定オブジェクトを見つけます。
5. 編集アイコンをクリックしてオブジェクトを開きます。
6. 以下のパラメータを探します。

   `#DlpErrorFile`
7. 編集アイコンをクリックしてパラメータを開きます。
8. パラメータ名からポンド記号を削除します。
9. ［値］フィールドにカスタム エラー ページの場所を入力します。

   例：

   `C:¥custompages¥dlperror.txt`

10. ［OK］をクリックします。
11. ［サブミット］をクリックします。

    わかりやすいメッセージが有効になります。

CA Agent for SharePoint 所有者タスク

CA Agent for SharePoint 管理者は統合に対して SharePoint エージェント環境を有効にします。 以下の順序で統合手順を実行します。

1. SharePoint がマルチ認証モードに設定されている場合は、プロキシ ルールを変更します。
2. DLP プラグインを有効にします。

SharePoint マルチ認証のプロキシ ルールの変更

SharePoint がマルチ認証用に設定されている場合、[assign the value for dlp in your book] CCS が SharePoint リソースを正しく分類するように特定の CA SiteMinder Agent for SharePoint プロキシ ルールが必要です。

Sharepoint 管理者に問い合わせて、マルチ認証が設定されているかどうかを判断します。 マルチ認証が設定されている場合は、以下の手順に従います。

重要: SharePoint 環境がマルチ認証に対して設定されているときは、他のどのプロキシ ルールも使用しないでください。 リソースに対する [assign the value for dlp in your book] CCS リクエストでは、CA SiteMinder Agent for SharePoint が適切に転送するために HTTP ヘッダが使用されます。 CA SiteMinder Agent for SharePoint が以下のプロキシ ルールを使用してこれらのリクエストを適切に転送しない場合、保護されている情報の不正アクセスおよび漏えいが発生する可能性があります。

次の手順に従ってください:

1. CA SiteMinder Agent for SharePoint で以下のファイルを見つけます。

   Agent-for-SharePoint_home¥proxy-engine¥conf¥proxyrules.xml

2. 以下の例のような名前を使用して、上述のファイルの名前を変更します。

   proxyrules_xml_default.txt

3. テキスト エディタで CA SiteMinder Agent for SharePoint 上の以下のファイルを開きます。

   Agent-for-SharePoint_home¥proxy-engine¥examples¥proxyrules¥proxyrules_example2.xml

4. 上述のファイルを新規ファイルとして以下の場所に保存します。

   Agent-for-SharePoint_home¥proxy-engine¥conf¥proxyrules.xml

5. 更新された proxyrules.xml ファイルで以下のテキストを見つけます。

   :///$$PROXY_RULES_DTD$$"

6. 上述のテキストを以下のテキストに置換します。

   :///C:¥Program Files¥CA¥Agent-for-SharePoint¥proxy-engine¥conf¥dtd¥proxyrules.dtd"

7. 以下のテキストを見つけます。

   http://www.company.com

8. 上述のテキストを組織のドメインに変更します。以下の例を参考にしてください。

   http:www.example.com

9. 次の行を検索します。

   <nete:cond type="header" criteria="equals" headername="HEADER">

10. 以下の行と一致するように上述の行を編集します。

    <nete:cond type="header" headername="SMSERVICETOKEN">

11. 次の行を検索します。

    <nete:case value="value1">

12. 以下の行と一致するように上述の行を編集します。

    <nete:case value="DLP">

13. 上述の行の後に行を追加します。

14. 以下の XML 構文をコピーして新しい行に貼り付けます。

```
<nete:xprcond>

<nete:xpr>

<nete:rule>^/_login/default.aspx¥?ReturnUrl=(.*)</nete:rule>
<nete:result>http://sharepoint.example.com:port_number/_trust/default.aspx?tr
ust=siteminder_trusted_identity_provider&amp;ReturnUrl=$1</nete:result>
</nete:xpr>

<nete:xpr-default>

<nete:forward>http://sharepoint.example:port_number$0</nete:forward>

</nete:xpr-default>

</nete:xprcond>
```

15. 前述の **sharepoint.example:***port_number* の両方のインスタンスを以下の*いずれか*の値に置換します。
    - ハードウェア ロード バランサのホスト名、ドメインおよびポート番号。このハードウェア ロード バランサは CA SiteMinder Agent for SharePoint サーバと SharePoint サーバの間で動作します。
    - 単一の Web フロント エンドのホスト名、ドメインおよびポート番号。このコンテキストで、この Web フロント エンド (WFE) は「バック エンド」 SharePoint サーバの前で動作する Web サーバを参照します。
16. 前述の *siteminder_trusted_identity_provider* のインスタンスを SiteMinder 信頼済みのアイデンティティ プロバイダの名前に置換します。
17. ファイル内で以下の行を見つけます。

```
<nete:forward>http://home.company.com</nete:forward>
```

18. 上述の行の **home.company.com** を以下の*いずれか*の値に置換します。
    - ハードウェア ロード バランサのホスト名、ドメインおよびポート番号。このハードウェア ロード バランサは CA SiteMinder Agent for SharePoint サーバと SharePoint サーバの間で動作します。
    - 単一の Web フロント エンドのホスト名、ドメインおよびポート番号。このコンテキストで、この Web フロント エンド (WFE) は「バック エンド」 SharePoint サーバの前で動作する Web サーバを参照します。
19. ファイルを保存してテキスト エディタを閉じます。

    プロキシ ルールが設定されます。

DLP プラグインの有効化

DLP プラグインを有効にすると、保護されているドキュメントからリソース情報を抽出するようにエージェントが設定されます。 エージェントは許可プロセスの一部として情報をポリシー サーバに渡します。

重要: 統合を有効にするには、個別の手順がアプリケーション層で必要です。SharePoint エージェント設定オブジェクトを変更する前に、Web エージェント設定ファイルを変更しないでください。SiteMinder 管理者がこのタスクを実行します。

次の手順に従ってください:

1. CA SiteMinder Agent for SharePoint をホストするシステムへログインします。
2. 以下の場所に移動します。

   Agent-for-SharePoint_Home¥proxy-engine¥conf¥defaultagent

   Agent-for-SharePoint_Home

   CA SiteMinder Agent for SharePoint がインストールされているディレクトリを示します。

   デフォルト： （Windows） ［32 ビット］ C:¥Program Files¥CA¥Agent-for-SharePoint

   デフォルト： （Windows） ［64 ビット］ C:¥CA¥Agent-for-SharePoint
   デフォルト： （UNIX/Linux） /opt/CA/Agent-for-SharePoint
3. 以下のファイルを開きます。

   WebAgent.conf
4. 特定プラグインをロードする行をコメント解除 (左側の # 記号を削除) します。

   例： （Windows ［32 ビット］） LoadPlugin="C:¥Program Files¥CA¥Agent-for-SharePoint¥agentframework¥bin¥DisambiguatePlugin.dll"

   例： （Windows ［64 ビット］） LoadPlugin="C:¥CA¥Agent-for-SharePoint¥agentframework¥bin¥DisambiguatePlugin.dll"

   例： （UNIX/Linux） LoadPlugin="/opt/CA/Agent-for-SharePoint/agentframework/bin/DisambiguatePlugin.so"

5. ファイルを保存します。
6. Web サーバを再起動します。

   CA SiteMinder Agent for SharePoint が [assign the value for dlp in your book] 統合に対して設定されます。

Microsoft SharePoint 管理者タスク

SharePoint 管理者は、SiteMinder が保護している SharePoint アプリケーションへの読み取りアクセス権を [assign the value for dlp in your book] CCS に提供します。 [assign the value for dlp in your book] CCS が保護されているドキュメントに含まれるコンテンツの種類を確認するには、読み取りアクセス権が必要です。

[assign the value for dlp in your book] CCS への読み取りアクセス権の提供は各アプリケーションに対してローカルです。SiteMinder が保護しているすべてのアプリケーションについては以下の手順に従います。

以下の手順に従います。

1. CA SiteMinder クレーム プロバイダが設定されている場合は、SharePoint ループバック検索機能が必要です。 機能が有効になっていない場合は、以下の手順に従います。
   a. ［スタート］-［すべてのプログラム］-［Microsoft SharePoint 2010 製品］-［SharePoint 2010 管理シェル］をクリックします。
   b. 管理シェルを使用して以下のディレクトリに移動します。

      ```
      C:¥Program Files¥CA¥SharePointClaimsProvider¥scripts
      ```

   c. 以下のコマンドを入力します。

      ```
      .¥Set-SMClaimProviderConfiguration.ps1 -EnableLoopBackSearch
      ```

   d. ループバック検索が有効になります。
2. SharePoint Central Administration にログインします。
3. ［アプリケーション管理］セクションで［Web アプリケーションの管理］をクリックします。

   アプリケーションのリストが表示されます。
4. アプリケーションを選択し、［Web アプリケーション］リボンの［ユーザ ポリシー］をクリックします。

   ［Web アプリケーションのポリシー］ダイアログ ボックスが表示されます。

5. ［ユーザの追加］をクリックします。

   ［ユーザの追加］ウィザードが表示されます。

6. タイム ゾーンを選択して［次へ］をクリックします。

7. ［ユーザ］フィールドで参照アイコンをクリックします。

   ［ユーザとグループの選択 - Web ページ］ダイアログ ボックスが表示されます。

8. SiteMinder 信頼済みのアイデンティティ プロバイダを見つけます。信頼済みのアイデンティティ プロバイダの下で、関連する識別子クレームをクリックします。

9. ［検索］フィールドに以下の値を入力して検索アイコンをクリックします。

   caservice

10. 以下のユーザ アイコンをダブルクリックして［OK］をクリックします。

    caservice

    ［ユーザの追加］ダイアログ ボックスが表示されます。

11. 以下の許可を選択して［完了］をクリックします。

    完全な読み取り - 完全な読み取り専用アクセス権を持ちます。

    ［Web アプリケーションのポリシー］ダイアログ ボックスが表示されます。

12. ［OK］をクリックします。

    [assign the value for dlp in your book] CCS にはアプリケーションへの読み取りアクセス権があります。

Identity Manager ロールとアクセス制御

Identity Manager との統合により、Identity Manager ロールを使用したポリシー ベースのアクセス制御の実装が可能になります。これらのロールは、外部アプリケーション内のユーザ権限の集中的管理を可能にします。

注: 統合の設定に関しての詳細は、CA Identity Manager のマニュアルを参照してください。

統合の要件は次のとおりです。

- ポリシー サーバのインストールでは、以下の場所に CA Identity Manager の統合に必要なデータ定義が含まれます。

  siteminder_home¥xps¥dd

  siteminder_home

  ポリシー サーバのインストール パスを指定します。

- ファイル名は以下のとおりです。

  IdmSmObjects.xdd

  重要: Identity Manager の統合が完了するまで、このファイルをポリシー ストアにインポートしないでください。統合を完了しないうちにデータ定義をインポートした場合、ポリシー サーバは不確定状態になる可能性があります。 Identity Manager 管理者との統合を調整します。

- Identity Manager 管理者は Identity Manager 内の環境およびロールを管理して、SiteMinder で安全性を確保するアプリケーションへのユーザ アクセスを決定します。SiteMinder 管理 UI は IDM 環境としてこれらの環境を参照します。

  注: 環境およびロールの詳細については、Identity Manager のマニュアルを参照してください。

- SiteMinder 管理者は 管理 UI を使用して、1 つ以上の IDM 環境をポリシー ドメインおよびユーザ ディレクトリに関連付けます。 SiteMinder 管理者は IDM 環境を作成または管理することができません。

- SiteMinder 管理者は 管理 UI を使用して、ポリシーを作成し、かつ IDM 環境に利用可能な 1 つ以上のロールを関連付けます。 SiteMinder 管理者は CA Identity Manager ロールを作成または管理することができません。

  注: エンタープライズ管理アプリケーションに Identity Manager ロールを適用できません。

SiteMinder は、保護されたアプリケーションで Identity Manager ユーザが持つ権限付与に関する詳細情報も提供します。 以下の図が示すように、SiteMinder 管理者はポリシーでアクセス ルールとレスポンスを関連付けます。 レスポンスには、SiteMinder で自動的に生成されるユーザ属性を指定するレスポンス属性が含まれています。

SiteMinder で生成されるユーザ属性は、Identity Manager からタスク情報を取得します。 ポリシー サーバは HTTP ヘッダ変数または Cookie としてこの情報を Web エージェントへ渡します。 保護されたアプリケーションでは、Web エージェントを通じてこのヘッダ変数またはクッキーを利用して、きめ細かなアクセス制御を行うことができます。

図 8: CA Identity Manager ときめの細かいアクセス制御