

Oracle Identity Federation

Oracle ホワイト・ペーパー
2006 年6 月

はじめに	3
Identity Federation について	3
Web ドメイン間でのシングル・サインオン	4
業界標準	5
ORACLE IDENTITY FEDERATION	6
Oracle Identity Federation のアーキテクチャ	6
異機種間サポート	7
複数プロトコルのサポートと相互運用性	7
データ・リポジトリ	9
容易な管理	10
フェデレーション配備に関する考慮事項	10
Oracle Identity Federation の DMZ 配備	11
SSL と証明書ベースの認証	11
結論	12

はじめに

Oracle Identity Federation は、スタンドアロン・アプリケーションの使いやすさと移植性を兼ね備えた、内蔵型のフェデレーション・ソリューションです。また、スケーラブルで、実績ある標準ベースの相互運用性アーキテクチャを備えています。ビジネスがグローバル化し、パートナー、サプライヤ、および顧客との密接な関係を持つビジネス・モデルへ向かうにつれて、安全で密接な取引関係を確立するという難題が持ち上がりました。ユーザーが連携 ID を利用することで、ビジネス・パートナーとの信頼関係からメリットを得ることができます。連携 ID は、通信、金融サービス、製造など複数の業界において、非常に重要な部分を占めるようになりました。連携 ID を使用したビジネス・プロセス統合は、廉価かつシンプルで、より安全なものになります。

Identity Federation について

アイデンティティ・フェデレーションは、標準、テクノロジー、および信託契約で構成されており、さまざまなセキュリティ・ドメインへのアイデンティティと属性の移植を可能にします。

アイデンティティ・フェデレーションは、セキュリティ・ドメイン間で、ID とその関連エンタイトルメントを伝播するインフラストラクチャを提供します。このドメインには、組織内に存在するドメインと、組織間に存在するドメインがあります。アイデンティティ・フェデレーションの概念には、連携関係の確立に必要なすべての標準、テクノロジー、および契約が含まれます。フェデレーションおよび SAML のコンテキスト内で一般に使用されている、知っておくべき用語は次のとおりです。

- **Assertion (アサーション)** - オーソリティによって本物と証明された 1 文または複数の文。SAML 仕様において、アサーションは、認証、属性、および認可に関する文として定義されています。
- **Identity Provider (アイデンティティ・プロバイダ IdP)** - ユーザー認証を行い、宛先サイトまたはサービス・プロバイダにアサーションを送信するサイト。
- **Service Provider (サービス・プロバイダ SP)** - アサーションに従ってユーザーのエンタイトルメントを特定し、要求リソースに対するアクセスを許可または拒否するサイト。
- **Circle of Trust (トラスト・サークル COT)** - 信頼関係を確立するサービス・プロバイダ、および/またはアイデンティティ・プロバイダのグループ。
- **Federation (フェデレーション)** - トラスト・サークル内のプロバイダ間におけるユーザー・アカウントのリンク。

- **Name Identifier (名前識別子)** - フェデレーション・プロトコル・メッセージ内で使用されるユーザー識別子 (電子メールアドレス、DN、内部文字列)。

アクセス管理とシングル・サインオン (SSO) の進化において、次の段階となるアイデンティティ・フェデレーションは、相互運用可能なソリューションであり、サービスを提供する企業が、組織やセキュリティ・ドメインの外部ユーザーのアイデンティティ情報を確実に受信し、処理します。利点のひとつとして、エンドユーザーのエクスペリエンス向上があげられます。ユーザーは、セッション内で、個々のアプリケーションや Web サイトへログインする必要はありません。また、これによって、ユーザーは多数のユーザー名とパスワードの組み合わせを覚える必要がなくなります。その結果、ヘルプデスクのコールとチケット数が減少することで、IT コストを大幅に削減できます。さらに、トラスト・サークルを確立することによって、組織はパートナーや顧客のユーザー・ベースを管理する必要がなくなり、ユーザー・アクションによる責任の所在をアサーションの提供者に置くことで、認証に関わるリスクを軽減できます。

アイデンティティ・プロバイダやソース・サイトによってユーザー・アカウントが無効化される場合、即座にそのユーザーはサービス・プロバイダのアプリケーションや宛先サイトから自動的にロック・アウトされます。

Web ドメイン間でのシングル・サインオン

フェデレーションは、どのように機能するのでしょうか。2つのビジネス・パートナーがそれぞれのアプリケーションをリンクし、ユーザーが追加のログインなしで外部アプリケーションにアクセスできるようにしたいという、シンプルなシナリオがあるとします。このシナリオにおいて、アイデンティティ・プロバイダは、ユーザーが各自のプロファイルを管理できるカスタム・ポータルを有しており、また、企業とパートナーに対するサービスを提供しています。これらのユーザーが使用できるサービスのうちの1つとして、パートナーであるサービス・プロバイダの販売調査レポートを表示する機能があげられます。これらのレポートへのアクセスは、2つのパートナー間で定められた契約によって制限されます。ユーザーがアイデンティティ・プロバイダにログインし、レポートを表示するリンクをクリックすると、サービス・プロバイダのアプリケーションが起動します。いったんアイデンティティ・プロバイダによって認証されたユーザーは、別のログインをする必要はなく、会社側もパスワード、ID、またはプロファイルを同期する必要はありません。

裏側では、両社の連携アイデンティティ管理ソリューションが、このシンプルなフェデレーション・シナリオを可能にするために必要なステップを、ユーザーに気づかれることなく管理しています。下の例では、SAML を利用して、2つの環境間でアイデンティティ・データを共有しています。次に、このプロセスがどのように機能するかを示します。

ステップ 1: 認証用の ID とパスワードを使用して、アイデンティティ・プロバイダにログインします。いったんユーザーが認証されると、ブラウザ内にセッション Cookie が保存されます。

ステップ 2: サービス・プロバイダ上のアプリケーションを表示するリンクをクリックします。IdP は、ユーザーのブラウザ内の Cookie に基づいて SAML アサーションを作成し、アサーションにデジタル署名を付加して、SP へリダイレクトします。

ステップ3: SPはSAMLアサーションを受信し、ユーザーのアイデンティティ情報を抽出して、ユーザーを宛先サイト上のローカル・ユーザー・アカウントにマッピングします。

ステップ4: 認可チェックが実行され、認可に成功すると、ユーザーのブラウザは保護リソースにリダイレクトされます。SPはユーザーの受信と検証に成功すると、ユーザーのブラウザ内に独自のCookieを保存し、ユーザーが追加のログインなしで両方のドメインをナビゲートします。

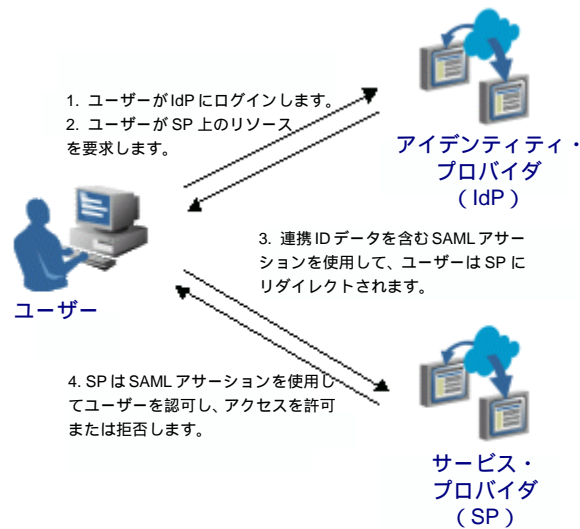


図 1.1 ドメイン間でのシングル・サインオン

業界標準

OASIS SAML2.0は、OASIS SAML 1.1、Liberty Alliance Identity Federation Framework (ID-FF) 1.2、および Internet2 Shibboleth 標準を統合したものです。

標準への準拠は、アイデンティティ・フェデレーション・ソリューションの重要な一面です。これらの標準は、プロトコル、処理ルール、およびセマンティクスを定義して、多様な実装、アイデンティティ、およびアクセス管理インフラストラクチャの相互運用を可能にします。ドメイン間のSSOに関する要求に応じて、OASIS 組織は最初のフェデレーション標準である SAML 仕様を策定しました。

OASIS による SAML 仕様に基づいて、Liberty Alliance (連携ネットワーク・アイデンティティ標準の開発を行うコンソーシアム) は、Liberty Identity Federation Framework (ID-FF) 仕様を策定しました。この仕様では、アカウントのリンクや導入などの概念を取り入れています。同様に、Internet2 グループによって、おもに高等教育で使用されるオープン・ソース仕様の Shibboleth が規定されました。Shibboleth は、属性ベースで連携アイデンティティを認証および認可するインフラストラクチャであり、SAML 1.0 および 1.1 標準に基づいています。並行して、Web サービス指向アプリケーションに対する認証と認可の標準に関する作業が進められており、WS-Federation 標準の開発へと至りました。WS-Federation 標準は、Web サービス指向環境のドメイン間におけるアイデンティティ、認証、および認可の連携をモデル化したものです。

これらの標準組織の参入と、それに続く仕様の策定にともない、ドメイン間で SSO

アプリケーションを配備する際に、どのフェデレーション・プロトコルを採用するかという選択が問題になりました。OASIS SAML 2.0 標準は、いくつかのフェデレーション・プロトコル (SAML 1.1、Liberty ID-FF、Shibboleth) を集約して統合したものであり、フェデレーション・ソリューションを配備する企業に、強力で安定した仕様を提供します。

ORACLE IDENTITY FEDERATION

企業がそのビジネス・プロセスをインターネットへ移行するにつれて、これらのアプリケーションに対して顧客やパートナーをリンクさせたり、アクセスを提供したりする必要性が優先事項となってきました。既存のアイデンティティ管理ソリューションおよびアクセス管理ソリューションが配備されているため、フェデレーション製品はサード・パーティ・ベンダーの製品との相互運用や、本番環境における既存のアイデンティティ・インフラストラクチャとの統合に対応する必要があります。Oracle Identity Federation 独自の柔軟なアーキテクチャは、標準準拠のフェデレーション・ソリューション、ディレクトリ、データベース、アクセス管理製品との統合、および相互運用を可能にします。

Oracle Identity Federation のアーキテクチャ

Oracle Identity Federation は、スタンドアロンのフェデレーション・サーバーであり、J2EE コンテナ (Oracle Application Server) や Web サーバー (Oracle HTTP Server) を含む、配備に必要なすべてのコンポーネントを備えています。このサーバーは、サービス・プロバイダおよびアイデンティティ・プロバイダの両方として配備することができ、トラスト・サークル内の複数プロトコルのハブとして機能します。

イベント・ベースのモデルを使用することによって、Oracle Identity Federation は、HTTP や SOAP ベースのメッセージの受信、処理、および応答を行います。アサーションを受信した場合、フェデレーション・サーバーはそのコア・プロトコルとビジネス・ロジックを使用して、アサーションを処理します。認証と認可の決定を行うため、Oracle Identity Federation は、AAA エンジンやユーザー・データ・リポジトリ (LDAP、RDBMS など) といった、サード・パーティによるアイデンティティ管理システムおよびアクセス管理システムと統合します。

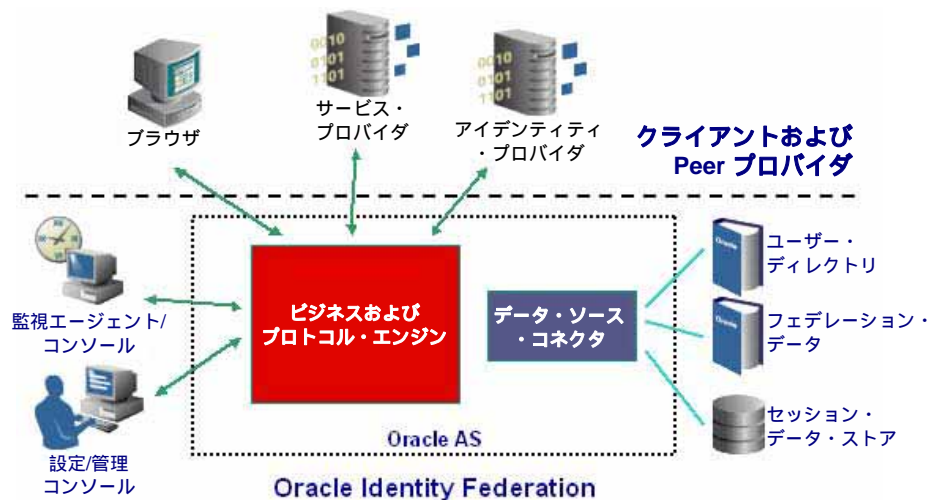


図 1.2 Oracle Identity Federation のアーキテクチャ

異機種間サポート

Oracle Identity Federation は、サード・パーティのアイデンティティ管理ソリューションおよびアクセス管理ソリューションと統合可能であるため、組織は既存のインフラストラクチャを利用できます。アイデンティティ・プロバイダとして機能する Oracle Identity Federation は、LDAP ディレクトリやデータベースに対するユーザー認証を行います。また、Oracle Identity Federation は、これらのリポジトリからユーザー属性を取得する際、パフォーマンスを向上させるためにダイレクト・コールを行います。サポートされる認証システムまたは認可システムをすでに利用している場合、Oracle Identity Federation はそのシステムを利用して、ユーザーを認証し、パートナ・アプリケーションに渡す認証アサーションを作成します。サービス・プロバイダの役割を果たす Oracle Identity Federation は、サポートされる認証システムまたは認可システムと通信を行い、認証ユーザーのアクセス権限を特定し、データ・リポジトリからユーザーの属性を取得します。

複数プロトコルのサポートと相互運用性

Oracle Identity Federation は、主要なフェデレーション・プロトコルをサポートしており、いくつかの相互運用性および適合性に関するイベントに参加しています。また、Liberty ID-FF や SAML 2.0 に対する Liberty Alliance 認証を取得しています。Oracle Identity Federation は、OASIS SAML 2.0、Liberty Alliance ID-FF 1.1 および 1.2、OASIS SAML 1.0 および 1.1、WS-Federation をサポートします。

標準ベースの相互運用性を実現するために、Oracle Identity Federation は、オープン・スタンダード・グループによって定義されたプロファイルを実装することで、他ベンダーによるソリューションとのメッセージ交換をすばやく正確に実行します。Oracle Identity Federation は、以下のプロファイルをサポートします。

SAML Browser Artifact Profile - これは SAML および Liberty ID-FF のプロファイルであり、SAML リファレンスや "artifact" を使用して、SSO の SAML アサーションをアイデンティティ・プロバイダからサービス・プロバイダへ渡します。そして、artifact は安全なバック・チャンネル交換 (SSL など) を介して逆参照され、アイデンティティ・プロバイダからの参照アサーションがプルされます。次に、ブラウザ Artifact プロファイルを使用したシングル・サインオンのステップについて説明します。

はじめに、ユーザーは IdP の役割を果たす Oracle Identity Federation にログインします。認証が行われると、SSO Cookie が生成されてユーザーのブラウザ内に設定されます。次に、ユーザーは SP ドメイン内のリソースに対するアクセスを要求します。IdP からの転送サービスを介して、シングル・サインオンが開始されます。このサービスによって生成される artifact には、IdP 識別子とアサーション本体に対するハンドルが含まれます。URL のクエリー文字列に含まれる artifact を使用して、ユーザーのブラウザは SP の受信サービスへリダイレクトされます。SP の受信サービスは、artifact、IdP 識別子、およびアサーション・ハンドルを含む関連情報を抽出し、安全なバック・チャンネル通信を使用して、アサーション本体に対するリクエストを IdP へ送信します。IdP の応答サービスはリクエストを処理し、当該アサーションを SP へ送信します。

アサーションは SP に処理され、ローカルのユーザー・アカウントへマッピングされます。最後に、すべてのユーザー情報がそろった段階で、SP はリソースへのユーザー

ザー・アクセスを許可するかどうかを決定することができます。

SAML Browser POST Profile - これは SAML および Liberty ID-FF のプロファイルであり、SSO の SAML アサーションを SP へ渡します。バック・チャンネル通信は必要ありません。SAML アサーションは、IdP によって SP へプッシュされます。次に、POST プロファイルを使用したシングル・サインオンのステップについて説明します。

はじめに、ユーザーは IdP として機能している Oracle Identity Federation にログインします。認証が行われると、シングル・サインオンのセッション Cookie が設定されます。ユーザーは、SP 上にある保護リソースへのリンクにアクセスし、IdP がそのユーザーに対するアサーションを生成します。アサーションには、ユーザー・ディレクトリ（例：LDAP ディレクトリ）内にあるユーザー属性に基づいたコンテンツが含まれます。IdP は、アサーションと SP を含む応答を送信します。そして、応答にデジタル署名が付加されます。

ユーザーのブラウザは、SP の受信サービスにフォームをポストします。応答はデコードされ、アサーションが IdP によって発行された元のアサーションと一致するかどうかを検証されます。検証が行われると、アサーションは SP ドメイン内のユーザーにマッピングされます。SP ユーザーのログインが行われ、シングル・サインオンの Cookie が割り当てられます。ここで、SP はユーザー・アクセスを許可するかどうかを決定することができます。

SAML X.509 Attribute Sharing Profile - これは、SAML 2.0 のプロファイルであり、X.509v3 証明書ベースの認証を使用した分散認可をサポートします。ユーザー認証は、SSL のクライアント証明書認証を使用して、SP によって行われます。ここで、ユーザーは SSL ハンドシェイクを確立するための X.509v3 証明書を提示します。認証が行われると、SP はユーザーのアイデンティティが管理されている IdP に SAML リクエストを送信し、認可に関する決定を行うためのユーザー属性情報を要求します。次に、このプロファイルを使用した場合のステップについて説明します。

ユーザーは、SP 上の保護リソースにブラウザからアクセスしようとします。SP は、認証の資格証明を要求します。そして、ユーザーはこの資格証明を X.509v3 証明書の形式で提示します。SSL クライアント認証を使用して、認証が行われます。ユーザー認証が行われ、SP は署名付きのユーザー属性用 SAML アサーションを IdP に送信します。SP はアサーションを送信する IdP を決定するために、ユーザーの証明書の識別名 (DN) を利用します。

IdP がアサーションを受信して SP の妥当性を検証した後、適切なユーザー属性を含む署名付きの応答が SP へ送信されます。この情報によって、保護リソースへのアクセスを許可するかどうかを決定することができます。

Single Logout Profile - これは SAML 2.0 および Liberty ID-FF のプロファイルであり、グローバル・ログアウトをサポートします。IdP は、ユーザー認証が行われたすべての SP のリストを保持します。ユーザーがグローバル・ログアウトをリクエストすると、IdP によりユーザーがログインしたそれぞれの SP に対して、ユーザーをログアウトする要求が送信されます。次に、このプロファイルを使用した場合のステップについて説明します。

ユーザー（または信頼できるプロバイダ）が、グローバル・ログアウトを要求します。IdP は、ユーザーがログインしている SP または IdP のうちの 1 つに対して、ログアウト要求を送信します。次に、IdP は、メッセージを送信したプロバイダからのログアウト応答を受信します。IdP は、ユーザー認証が行われる次のプロバイダに対して、次のログアウト要求を送信し、ログアウト応答を待ちます。この処理は、ユーザー認証が行われたすべてのプロバイダからのログアウト応答を、IdP が受信するまで繰り返されます。そして、IdP はローカルでユーザーをログアウトして、ログアウト画面を表示します。Oracle Identity Federation は、IdP が開始するシングル・ログアウトと、SP が開始するシングル・ログアウトの両方をサポートします。

NameIdentifier Profile - これらは SAML 2.0 および Liberty ID-FF のプロファイルであり、あるプロバイダにおいて共通ユーザーの名前識別子を更新する必要がある場合に、プロバイダ間で通信する方法を定義します。これらのプロファイルでは、サービス・プロバイダまたはアイデンティティ・プロバイダのいずれも、ユーザーの名前識別子を指定または登録できます。

Federation Termination Profile - これらは SAML 2.0 および Liberty ID-FF のプロファイルであり、アイデンティティ・プロバイダとサービス・プロバイダがフェデレーションの終了要求を処理する方法を定義します。SP が開始したプロファイルと、IdP が開始したプロファイルの両方がサポートされます。

Passive Requestor Profile - これは WS-Federation のプロファイルであり、受動リクエスト（HTTP をサポートする Web ブラウザなど）を含む、フェデレーション・サービス・クライアントのコンテキスト内での仕様における使用方法を定義します。

データ・リポジトリ

Oracle Identity Federation は、アイデンティティ・リポジトリと直接通信を行い、ユーザー・データ、フェデレーション・データもしくはプロバイダ・データ、セッション・データもしくは非永続データ、構成データの 4 つのデータ・タイプを処理します。ユーザー・データに関して、Oracle Identity Federation はさまざまなユーザー・データ・リポジトリに接続して、ユーザーのアイデンティティ情報および属性にアクセスします。フェデレーション・サーバーがアイデンティティ・プロバイダの役割を果たす場合、LDAP や RDBMS に対する認証を直接行うように設定できます。フェデレーション・データは、ユーザーが信頼できるプロバイダに対して定義した永続的なフェデレーション（アカウントのリンクなど）に関連するデータです。このデータの情報は、LDAP に保存されます。

セッション・データは、ブラウザ・セッションまたはプロトコル・ステートに関する一時的なデータです。軽量配備オプションの場合、このデータはメモリに保存されます。高可用性、クラスタリング、およびロード・バランシング構成の場合、セッション・データは RDBMS に保存されます。構成データは、管理コンソールに抽象化された XML ファイル内で管理されます。この Web ベースの GUI を使用して、管理者はサーバー・プロパティやプロトコル・プロパティなどを設定できます。

容易な管理

Oracle Identity Federation は、フェデレーション管理を簡素化する次の機能を提供します。

- *Bulk Federation Utility* - 管理者がユーザーのフェデレーション・レコードをバルク・ロードするためのコマンド・ライン・ユーティリティ。既存のアイデンティティの共有プロセスとリンク・プロセスを円滑にします。
- *Automatic account linking* - アイデンティティ・プロバイダとサービス・プロバイダの既存アカウントをシームレスかつ自動的にリンクします。これによって、ユーザー自身によるアカウントの管理およびリンクを可能にしました。
- *Federation Termination* - プロトコル・ベースのプロファイル。プロバイダは、このプロファイルを使用して、共通のユーザーまたは名前識別子に割り当てられたフェデレーションを終了します。
- *Web based graphical user interface* - サポートされるプロトコルのコンテキスト内で、ユーザーのフェデレーション・データ、信頼できるプロバイダ、サーバー・プロパティの管理と設定を行います。

フェデレーション配備に関する考慮事項

"ハブ・アンド・スポーク"モデル、および"Peer-to-Peer"モデルは、Oracle Identity Federation の一般的な2つの配備モデルです。ハブ・アンド・スポーク・モデルは、サービス・プロバイダ("ハブ")が、アイデンティティ・プロバイダ("スポーク")のユーザーに対して、アプリケーションやリソースを提供する連携システムです。スポークまたは IdP によって、ローカルのユーザー認証が行われます。ユーザーはローカルのポータルを介してログインします。ユーザーが適切な資格証明を持っており、そのアカウントがフェデレーション済みである場合、いったん認証が行われると、そのユーザーはハブのリソースにアクセスできます。このフェデレーション・モデルにおける一番のビジネス要因は、サービス・プロバイダのリソースとアイデンティティ・プロバイダのユーザー間の密な統合です。

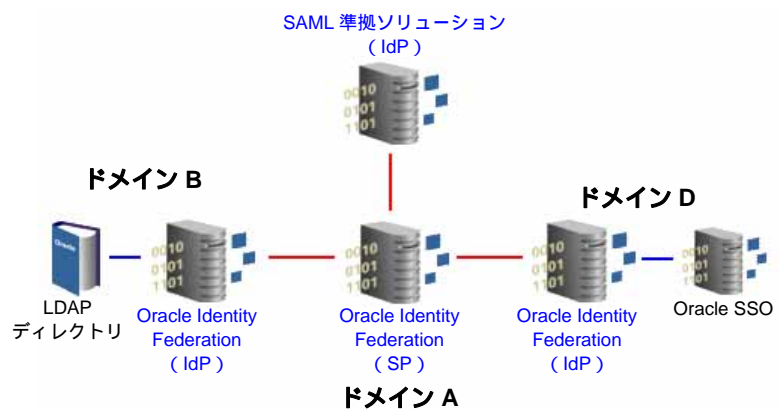


図 1.3 ハブ・アンド・スポーク・モデル

Peer-to-Peer モデルの場合、複数ドメインがハブの役割を果たします。それぞれのハブは、サービス・プロバイダとして配備することも、アイデンティティ・プロバイダとして配備することもできます。さらに、それぞれのハブを信頼できるプロバイダの SP または IdP として機能させることができます。

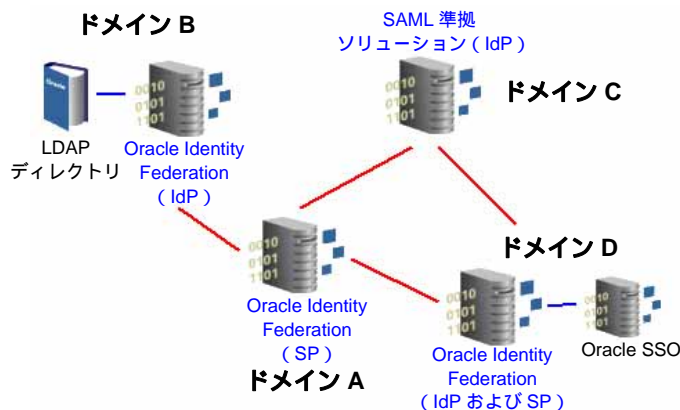


図 1.4 Peer-to-Peer モデル

Oracle Identity Federation の DMZ 配備

企業において、Oracle Identity Federation Server を配備する際、どのコンポーネントを DMZ 内に配置し、インターネットからアクセス可能にするかについて検討する必要があります。サーバーがファイアウォール内に存在する場合、外部ネットワークからサーバーに対する透過的なアクセスを可能にするには、プロキシ・サーバーを使用して要求と応答を Oracle Identity Federation に転送する必要があります。また、ロード・バランシング環境において、フェデレーション・サーバーをシームレスに負荷分散する目的においても、プロキシ・サーバーを使用できます。

プロキシ・サーバーの設定は、プロファイルによって異なります。たとえば、Browser POST プロファイルは HTTPS を使用するため、アイデンティティ・プロバイダとサービス・プロバイダの両方が、これらのポートを使用して通信するように設定する必要があります。SP の通信には、通常 DMZ 内のプロキシ・サーバーを使用します。Browser Artifact プロファイルが実装されている場合、アイデンティティ・プロバイダとサービス・プロバイダの両方でプロキシ・サーバーを使用するか、または両方ともプロキシ・サーバーを使用しないように設定する必要があります。プロキシ・サーバーが配備されている場合、これは SAML artifact 交換における要求サービスおよび応答サービスの役割を果たします。

SSL と証明書ベースの認証

セキュリティは、すべてのエンタープライズ・アーキテクチャにとって必要不可欠な要素であり、デジタル証明は、検証および認証における重要な一部分をなします。Oracle Identity Federation は、Secure Socket Layer (SSL) テクノロジーと証明書ベースの認証を使用して、安全な通信を実現する機能を提供します。SSL オプションを使用すると、サポートされる仕様において説明したとおり、信頼できるプロバイダ間の"バック・チャンネル"通信を保護します。

また、信頼できるプロバイダは、検証のために証明書を利用できます。Oracle Identity Federation は、デジタル署名と暗号化に対する X.509 証明書をサポートする、証明書の検証ストアを提供します。これによって、管理コンソール内の使いやすいインターフェースを使用して、信頼できる認証局 (CA) と証明書失効リスト (CRL) を管理できます。管理者は、送信 SAML アサーションに対する署名および暗号化と、信頼できるプロバイダからの受信メッセージの検証および認証を行うことができます。

結論

Oracle Identity Federation は、スケーラブルで標準ベースのアーキテクチャを備えた、スタンドアロンのフェデレーション・サーバーです。異機種間モデルへの配備が可能であるため、組織は既存インフラストラクチャを利用してフェデレーション・サーバーを配備することができ、結果として、迅速な本番ロールアウトを実現します。Oracle Identity Federation プラットフォームを利用すると、パートナーはそれぞれのロケーションにアイデンティティ・プロファイルをコピーすることなく、ユーザー・アイデンティティやセキュリティ情報を複数の独立組織で共有できます。企業は、顧客やビジネス・パートナーとの融合を進めるとともに、プライバシーおよびセキュリティに関する規制への準拠を強化できます。

ORACLE FUSION MIDDLEWARE

Oracle Identity Federation
2006年6月
著者： Howard Bae

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

お問合せ：
電話： +1.650.506.7000
ファクシミリ： +1.650.506.7200
oracle.com

Copyright © 2006, Oracle. All rights reserved.

本文書は情報提供のみを目的として提供されており、ここに記載される内容は予告なく変更されることがあります。

本文書は一切間違いがないことを保証するものではなく、さらに、口述による明示または法律による黙示を問わず、特定の目的に対する商品性もしくは適合性についての黙示的な保証を含み、いかなる他の保証や条件も提供するものではありません。オラクル社は本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクル社の書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

Oracle、JD Edwards、PeopleSoft、および Retek は、オラクル社およびその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標です。