SiteMinder

ユーザのエンタープライズでのフェデレーション

12.52 SP1

ca technologies

CA Technologies 製品リファレンス

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

- SiteMinder
- CA SiteMinder® Web エージェント オプション パック
- CA SiteMinder for Secure Proxy Server

CA への連絡先

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

マニュアルの変更点

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

- SAML アフィリエイト エージェントへの参照をすべて削除しました。このエージェントはサポートされなくなりました。
- フェデレーション ユース ケースおよびソリューション (P. 11) - フェデレーション パートナーシップの概念をより明確に反映するために、ユース ケースが更新されました。
- フェデレーション トランザクション プロセス フロー (P. 85) - 新規チェックポイント ログ メッセージを含めるために、トランザクション ダイアグラムおよびフローが改訂および更新されました。

目次

第 1 章: SiteMinder フェデレーション展開

フェデレーション展開モデル

CA SiteMinder Federation には 2 つの展開モデルがあります。

- パートナーシップ フェデレーション

  パートナーシップ フェデレーションは、フェデレーション標準に基づく企業間のパートナーシップの設定に基づいています。 パートナーシップ モデルはドメイン、レルムおよびポリシーなどの SiteMinder 固有のオブジェクトを必要としません。 このモデルは SiteMinder Federation を使用した新しい設定に推奨されます。

- レガシー フェデレーション

  レガシー フェデレーション（以前のフェデレーション セキュリティ サービス）。

  レガシー フェデレーションは、アフィリエイト ドメイン、認証方式、フェデレーション リソースを保護するポリシーなど SiteMinder オブジェクトの設定に基づいています。 このモデルは、主に古い展開との下位互換性を維持するためのものです。

両方の展開は SAML アサーションの形式でユーザ認証データを提供します。 アサーションを消費するエンティティは、ユーザを識別するためにアサーションを使用します。 認証に成功すると、消費エンティティが要求されたリソースを利用可能にします。 結果はユーザのシームレスな操作性です。

両方のモデルを使用するために SiteMinder ポリシー サーバ、管理 UI および Web エージェント オプション パック をインストールします。

注: フェデレーションは、SiteMinder とは別にライセンスされます。

フェデレーション仕様

SiteMinder は次のフェデレーション仕様をサポートします。

SAML （Security Assertion Markup Language）

SAML （Security Assertion Markup Language）は、OASIS （構造化情報標準促進協会）によって策定された標準です。 この業界標準では、認証および許可情報を交換するための XML フレームワークが定義されています。

SAML はエンティティ間でユーザに関するセキュリティ情報を渡す手段としてアサーションを定義します。 SAML アサーションは、ユーザなど特定の対象について説明する XML ドキュメントです。 アサーションには、認証、許可および属性に関するいくつかの別の内部ステートメントを含めることができます。

SAML は、シングル サインオンを実行するためにパートナー間で SAML アサーションがどのように渡されるか指定する、2 つのブラウザ ベースのプロトコルを定義します。

プロファイルは次のとおりです。

- ブラウザ/Artifact プロファイル -- SAML アサーションへの参照として SAML Artifact を定義します。
- ブラウザ/POST プロファイル -- アサーションが含まれる応答を返します。

注: SAML 2.0 では、Artifact プロファイルおよび POST プロファイルは HTTP バインディングと呼ばれます。

SAML の仕様および SAML プロファイルの情報については、**エラー! ハイパーリンクの参照に誤りがあります。**の Web サイトを参照してください。

SiteMinder は以下の SAML 標準およびプロファイルをサポートします。

- SAML 1.0 Artifact プロファイルのみ（レガシー フェデレーション のみ）
- SAML 1.1 Artifact および POST プロファイル
- SAML 2.0 Artifact および POST プロファイル

WS-フェデレーション

ADFS（Active Directory フェデレーション サービス）は、フェデレーション シングル サインオン（SSO）のための Microsoft の Web サービス ベースのソリューションです。 ADFS は Windows サーバ上で実行され、セキュリティ保護されたネットワークを介してパートナーとユーザの識別情報およびアクセス権限を共有することで、SSO を実行します。ADFS はインターネット アプリケーションに SSO 機能を拡張して、ユーザが組織の Web ベース アプリケーションにアクセスする際にシームレスな Web SSO 操作を提供します。

ADFS は通信に WS-フェデレーション仕様を使用します。WS の仕様およびバックグラウンド ドキュメント、および ADFS プロファイルに関する情報については、**エラー! ハイパーリンクの参照に誤りがあります。**を参照してください。

フェデレーション ネットワークのエンティティ

フェデレーション ネットワークでは、1 つのエンティティが、SAML アサーションまたはアサーションを含む WS-フェデレーション トークンを生成します。 アサーションには、アサーションを生成するサイトでその ID がローカルに保守されるユーザに関する情報が含まれています。 もう一方のエンティティは、アサーションを使用してユーザを認証し、ユーザのセッションを確立します。

プロトコルに応じて、これらの 2 つのエンティティには違った指定が行われます。しかし、それらが提供する機能は同じです。

プロトコル	アサーションの生成	アサーションの消費
SAML 1.0 および 1.1	プロデューサ	コンシューマ
SAML 2.0	アイデンティティ プロバイダ（IdP）	サービス プロバイダ（SP）
WS-フェデレーション（パートナーシップ）	アイデンティティ プロバイダ（IP）	リソース パートナー（RP）
WS-フェデレーション（レガシー）	アカウント パートナー（AP）	リソース パートナー（RP）

単一サイトは、アサーティング パーティおよび依存パーティになることができます。

第 2 章: フェデレーションのユース ケースおよびソリューション

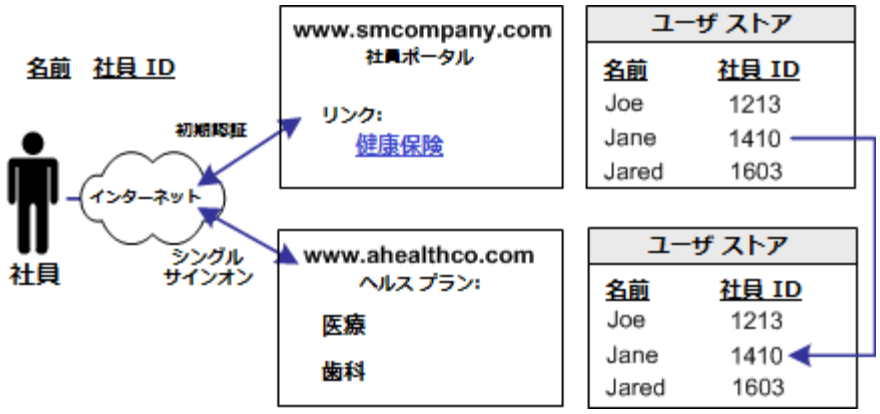
このセクションには、以下のトピックが含まれています。

ユース ケース: アカウント リンクに基づくシングル サインオン

このユース ケースでは、smcompany.com は、社員の健康保険を管理するために、パートナー企業 ahealthco.com と契約します。

smcompany.com の社員は自社の Web サイトの社員ポータル smcompany.com で認証を行い、リンクをクリックして ahealthco.com にある自分の健康保険情報を表示します。社員は ahealthco.com の Web サイトに移動し、このサイトにサインオンしなくても正しい健康保険情報が表示されます。

次の図はこのユース ケースを示しています。

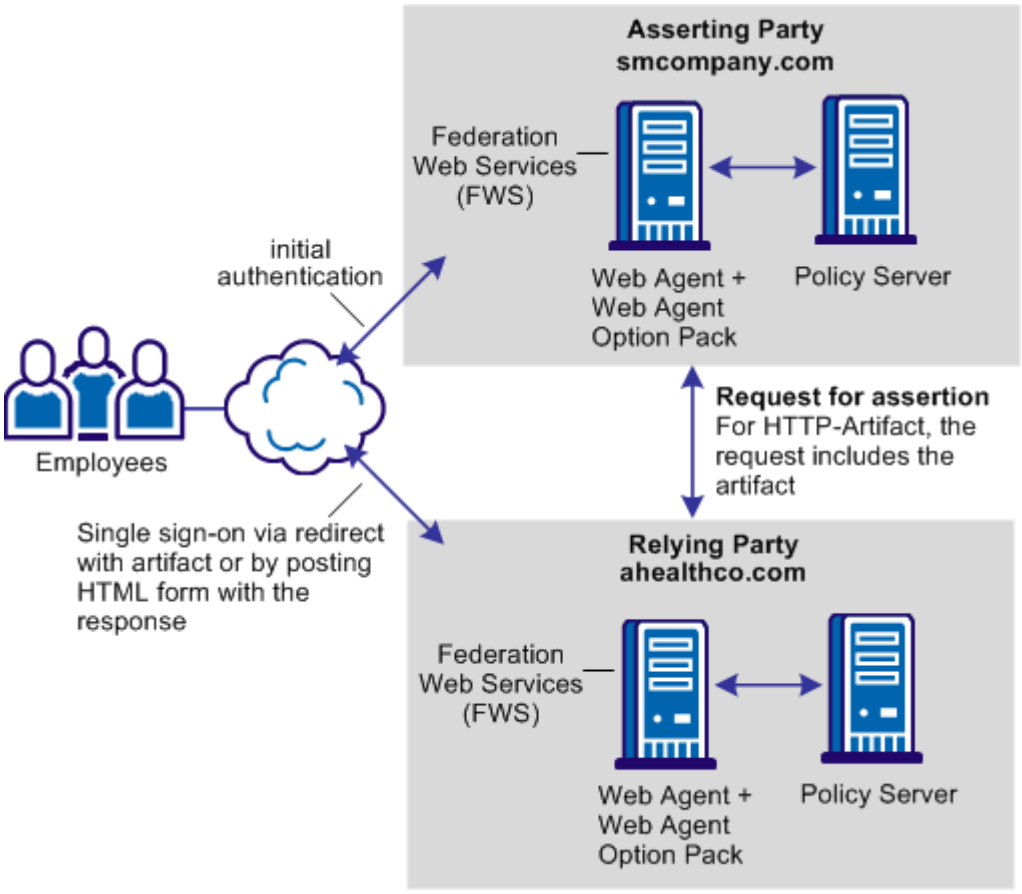


アカウント リンクはブラウザ ベースのシングル サインオンに使用できます。パートナーはそれぞれ、同じユーザの個別のユーザ アカウントを保守管理します。アカウント リンクでは SAML アサーションを使用し、パートナーでローカル ID とフェデレーション ID を関連付けます。

このユース ケースで、ahealthco.com は、smcompany.com ですべての従業員の健康関連情報およびユーザ ID をすべて保守管理します。smcompany.com の社員が ahealthco.com にアクセスすると、その社員の識別子が安全な方法で smcompany.com から ahealthco.com に渡されます。この識別子によって、ahealthco.com はそのユーザが誰かを特定し、また、そのユーザに対して許可するアクセス レベルを判別できます。

ソリューション: アカウント リンクに基づくシングル サインオン

smcompany.com および ahealthco.com でフェデレーションを展開すると、「ユース ケース： アカウント リンクに基づくシングル サインオン (P. 11)」を解決できます。



SiteMinder は両方のサイトで展開します。 1 つの Web サーバシステムに Web エージェント オプション パックと共に Web エージェントがインストールされ、また、別のシステムにポリシー サーバがインストールされます。これらのインストールは smcompany.com および ahealthco.com で同じです。

FWS アプリケーションは、HTTP-Artifact プロファイル用のアサーションを取得し、アサーションを消費するサーブレットを提供します。

注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

アカウント リンク ソリューション: SAML 1.1 HTTP-Artifact プロファイル

この例で、smcompany.com はプロデューサです。 smcompany.com の管理者は、smcompany.com と ahealthco.com の間に SAML 1.1 プロデューサ - コンシューマ パートナーシップを設定します。このパートナーシップでは、シングル サインオンのために HTTP-Artifact プロファイルが使用されます。

smcompany.com のパートナーシップには以下の情報があります。

- ahealthco.com でのアサーション コンシューマ サービスの場所。
- 一意の名前 ID。
- アサーションに追加されるアサーション属性。

smcompany.com の従業員は会社サイトにログインすると、最初に Web エージェントによって認証されます。 smcompany.com の従業員が従業員ポータル Web サイトにアクセスすると、次のイベント シーケンスが発生します。

1. 従業員が ahealthco.com にある健康保険情報を表示するために、smcompany.com でリンクをクリックします。リンクは smcompany.com でサイト間転送サービスに要求を出します。

2. サイト間転送サービスはポリシー サーバを呼び出し、ポリシー サーバによるアサーションおよびアーティファクトの生成を要求するリクエストを送信します。ポリシー サーバは、アサーションを生成し、アサーションをセッション ストアに置きます。ポリシー サーバはまた、サービスへのアーティファクトを生成し、返します。
3. Web エージェントが SAML Artifact によってユーザを ahealthco.com にリダイレクトします。

ahealthco.com はコンシューマ サイトです。 ahealthco.com の管理者が smcompany.com とのコンシューマ - プロデューサ パートナーシップを設定します。 このパートナーシップでは、シングル サインオンのために HTTP-Artifact プロファイルが使用されます。

パートナーシップ設定には以下の情報が含まれます。

- smcompany.com でのアーティファクト検索サービスの場所。
- ユーザ ディレクトリにユーザを置く場合に使用する、アサーション内の属性。
- ローカル ディレクトリ内でユーザ レコードを特定する検索文字列。このレコードはアサーション内の値と一致する必要があります。
- ターゲット リソース。

ahealthco.com がアサーションを受信します。以下のイベント シーケンスが発生します。

1. ブラウザが SAML 認証情報コレクタ URL への応答をポストします。
2. サービスが SAML Artifact により、smcompany.com のアサーション取得サービスに要求を送信します。 アサーション取得サービスは、アーティファクトからセッション ID を抽出します。
3. アサーション取得サービスは、セッション ストアからアサーションを取得します。 アサーション取得サービスは、アサーションをアーティファクト レスポンスとして ahealthco.com の SAML 認証情報コレクタに送信します。
4. SAML 認証情報コレクタはアサーションを検証します。 ポリシー サーバがセッションを作成し、ahealthco.com ドメイン用のブラウザにセッション Cookie を配置します。
5. SAML 認証情報コレクタが ahealthco.com のターゲット リソースにユーザをリダイレクトします。

アカウント リンク ソリューション: SAML 1.x POST プロファイル

この例で、smcompany.com はプロデューサです。 smcompany.com の管理者がプロデューサ - コンシューマ パートナーシップを設定します。パートナーシップはシングル サインオンで SAML 1.x POST プロファイルを使用します。

パートナーシップ設定には以下の情報が含まれます。

- ahealthco.com でのアサーション コンシューマ サービスの場所。
- 一意の名前 ID。
- アサーションに追加されるアサーション属性。

smcompany.com の従業員が従業員ポータル サイトにアクセスすると、以下のイベント シーケンスが発生します。

1. Web エージェントが初期認証を提供します。
2. 従業員が ahealthco.com にある健康保険情報を表示するために、smcompany.com でリンクをクリックします。リンクは smcompany.com でサイト間転送サービスに要求を出します。
3. サイト間転送サービスがアサーション生成プログラムを呼び出します。このプログラムは SAML アサーションを作成し、SAML 応答に署名します。
4. 署名された応答は Auto-POST HTML フォームで配置され、ユーザのブラウザに送信されます。
5. ブラウザは、ahealthco.com のアサーション コンシューマ サービスへのレスポンスが含まれるフォームをポストします。

ahealthco.com はコンシューマ サイトです。 ahealthco.com の SAML 認証情報コレクタ サービスが SAML 応答を処理します。 ahealthco.com の管理者は、シングル サインオン用に SAMl 1.1 HTTP-POST プロファイルを使用する smcompany.com とのコンシューマ - プロデューサ パートナーシップを設定します。

パートナーシップ設定には以下の情報が含まれます。

- smcompany.com でのアーティファクト検索サービスの場所。
- ユーザ ディレクトリにユーザを置く場合に使用する、アサーション内の属性。
- ローカル ディレクトリ内でユーザ レコードを特定する検索文字列。このレコードはアサーション内の値と一致する必要があります。
- ターゲット リソース。

イベント シーケンスを以下に示します。

1. SAML 認証情報コレクタがプロデューサからアサーションを受信します。
2. SAML 認証情報コレクタが ahealthco.com のポリシー サーバを呼び出します。
3. ポリシー サーバがアサーションの署名を検証し、それを使用してユーザを認証します。
4. 認証に成功した後、ポリシー サーバは SMSESSION Cookie を作成し、それをブラウザ内に配置します。
5. ブラウザはユーザを ahealthco.com のターゲット リソースにリダイレクトします。

アカウント リンク ソリューション: SAML 2.0 Artifact プロファイル

この例で、smcompany.com はアイデンティティ プロバイダです。smcompany.com の管理者は、ahealthco.com との IdP から SP へのパートナーシップをリモート SP として設定します。

パートナーシップ設定には以下の情報が含まれます。

- ahealthco.com でのアサーション コンシューマ サービスの場所。
- 一意の名前 ID。
- アサーションに追加されるアサーション属性。

従業員が従業員ポータル サイトにアクセスすると、以下のイベント シーケンスが発生します。

1. Web エージェントが初期認証を提供します。
2. ユーザが ahealthco.com にある健康保険情報を表示するためにリンクをクリックします。要求はアイデンティティ プロバイダで開始されるので、要求によって未承認応答がトリガされます。
3. フェデレーション Web サービス（FWS）がポリシー サーバに SAML Artifact を要求します。
4. ポリシー サーバは、SAML アサーションおよびアーティファクトを生成します。 ポリシー サーバは、アサーションをセッション ストアに格納し、アーティファクトを URL パラメータとして格納します。
5. ポリシー サーバは、SAML Artifact が含まれる応答を FWS に返します。
6. Web エージェントがユーザを SAML Artifact によって ahealthco.com にリダイレクトします。

ahealthco.com はサービス プロバイダです。 ahealthco.com の管理者は、smcompany.com との SP から IdP へのパートナーシップを設定します。これにはアーティファクト プロファイルが使用されます。 パートナーシップ設定には以下の情報が含まれます。

- smcompany.com でのシングル サインオン サービスの場所。
- ユーザ ディレクトリにユーザを置く場合に使用する、アサーション内の属性。
- ローカル ディレクトリ内でユーザ レコードを特定する検索文字列。このレコードはアサーション内の値と一致する必要があります。
- ターゲット リソース。

イベント シーケンスを以下に示します。

1. アサーション コンシューマ サービスがアーティファクトを受信します。サービスは、smcompany.com での Artifact 解決サービスの場所を、そのパートナーシップ設定から取得します。
2. アサーション コンシューマ サービスは、smcompany.com の Artifact 解決サービスをバック チャネルで呼び出します。
3. ポリシー サーバはセッション ストアからアサーションを取得し、ahealthco.com のアサーション コンシューマ サービスに応答を返します。

4. アサーション コンシューマ サービスは応答を検証し、ahealthco.com に対してセッションを作成します。セッション Cookie がブラウザに書き込まれます。
5. ブラウザはユーザを ahealthco.com のターゲット リソースにリダイレクトします。

アカウント リンク ソリューション: SAML 2.0 POST プロファイル

この例で、smcompany.com はアイデンティティ プロバイダです。smcompany.com の管理者は、IdP から SP へのパートナーシップを設定します。 パートナーシップはシングル サインオンで SAML 2.0 HTTP-POST プロファイルを使用します。

パートナーシップ設定には以下の情報が含まれます。

- ahealthco.com でのアサーション コンシューマ サービスの場所。
- 一意の名前 ID。
- アサーションに追加されるアサーション属性。

smcompany.com の従業員が従業員ポータル サイトにログインします。

初期認証が成功すると、以下のシーケンスが発生します。

1. smcompany.com の Web エージェントによってまずユーザが認証されます。
2. 従業員が健康保険情報を表示するために ahealthco.com へのリンクをクリックします。ポリシー サーバが SAML 2.0 SP 設定を読み取ります。

   アイデンティティ プロバイダが要求を開始し、これによって未承認応答がトリガされます。
3. 要求は smcompany.com でシングル サインオン（SSO）サービスに送信されます。
4. SSO サービスは、選択したプロファイルに基づいて SAML 2.0 アサーション/アーティファクトを生成するように、ポリシー サーバに対して要求を発行します。HTTP-POST の場合は、ポリシー サーバが SAML アサーションを生成します。
5. SSO サービスが、選択したプロファイルのアサーション応答を受信します。

6. 署名された応答が自動 POST HTML フォームで配置され、ブラウザに送信されます。
7. ブラウザは、ahealthco.com のアサーション コンシューマ サービスに応答をポストします。

ahealthco.com はサービス プロバイダです。 ahealthco.com の管理者は、smcompany.com との SP から IdP へのパートナーシップを設定します。 設定では SAML 2.0 HTTP-POST プロファイルをシングル サインオンに使用します。

パートナーシップ設定には、以下の情報が含まれます。

- smcompany.com でのアーティファクト検索サービスの場所。
- ユーザ ディレクトリにユーザを置く場合に使用する、アサーション内の属性。
- ローカル ディレクトリ内でユーザ レコードを特定する検索文字列。このレコードはアサーション内の値と一致する必要があります。
- ターゲット リソース。

ahealthco.com でのイベントのシーケンスを以下に示します。

1. アサーション コンシューマ サービスがポスト データから応答メッセージを取得します。
2. アサーション コンシューマ サービスは、ターゲット URL を取得するために IdP 設定を読み取ります。
3. アサーション コンシューマ サービスは署名された SAML 応答を認証情報として ahealthco.com のポリシー サーバへ渡します。
4. ポリシー サーバは署名を検証し、次に、ユーザを認証します。
5. ログインに成功します。
6. ポリシー サーバは、ahealthco.com ドメイン用の SMSESSION Cookie を作成し、Cookie をブラウザに配置します。
7. ブラウザはユーザを ahealthco.com のターゲット リソースにリダイレクトします。

アカウント リンク ソリューション: WS-フェデレーション パッシブ リクエスタ プロファイル

この例で、smcompany.com はアイデンティティ プロバイダです。smcompany.com の管理者は WSFED IP-RP パートナーシップを設定します。このパートナーシップでは WS-フェデレーション パッシブ リクエスタ プロファイルをシングル サインオンに使用します。このユース ケースでは、リソース パートナーシップである ahealthco.com がシングル サインオンを開始します。

SAML トークン タイプは SAML 1.1 です。 IP エンティティ設定のこの部分。

パートナーシップ設定には以下の情報が含まれます。

- ahealthco.com のセキュリティ トークン コンシューマ サービスの場所。
- 一意の名前 ID。
- アサーションに追加されるアサーション属性。

smcompany.com の従業員が従業員ポータルにアクセスすると、以下のイベント シーケンスが発生します。

1. ユーザが ahealthco.com の非保護サイト選定ページにアクセスします。Web エージェントが初期認証を提供します。
2. ユーザが smcompany.com のシングル サインオン サービスを指すリンクをクリックします。 ブラウザがユーザを smcompany.com にリダイレクトします。
3. SSO サービスがポリシー サーバを呼び出します。ポリシー サーバがアサーションを生成します。
4. ポリシー サーバは、リクエスト セキュリティ トークン レスポンスのアサーション エレメントに署名し、応答を返します。
5. ブラウザが ahealthco.com のセキュリティ トークン コンシューマ サービスへの自動 POST HTML 形式の応答をポストします。

ahealthco.com はリソース パートナーです。

パートナーシップ設定には以下の情報が含まれます。

- smcompany.com でのシングル サインオン サービスの場所。
- ユーザ ディレクトリにユーザを置く場合に使用する、アサーション内の属性。
- ローカル ディレクトリ内でユーザ レコードを特定する検索文字列。このレコードはアサーション内の値と一致する必要があります。
- ターゲット リソース。

イベント シーケンスを以下に示します。

1. セキュリティ トークン コンシューマ サービスがセキュリティ トークン コンシューマ応答からアサーションを抽出します。
2. サービスはターゲット リソースを確定します。
3. セキュリティ トークン コンシューマ サービスは、署名されたアサーションを認証情報として ahealthco.com のポリシー サーバへ渡します。
4. ポリシー サーバは署名を検証し、次に、ユーザを認証します。
5. 認証が成功したら、セキュリティ トークン コンシューマ サービスは SMSESSION Cookie を作成します。
6. その後、サービスはブラウザに cookie を配置し、ahealthco.com のターゲット リソースにユーザをリダイレクトします。

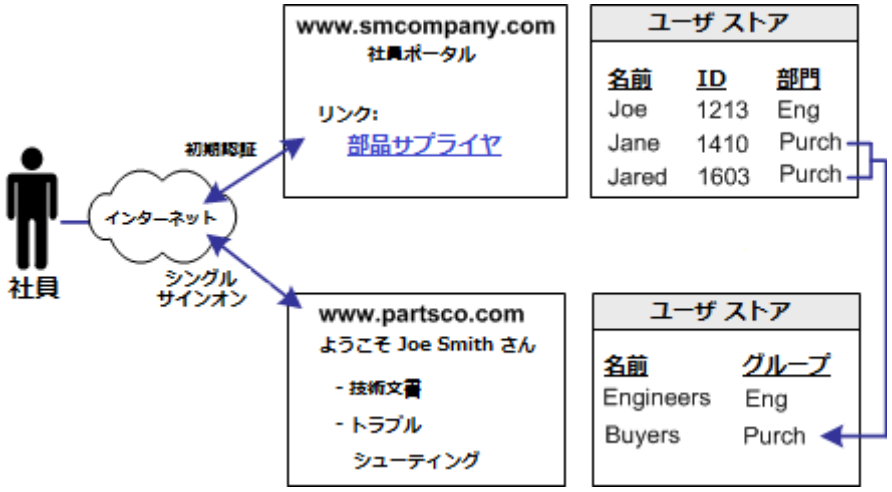
ユース ケース: ユーザ属性に基づいたシングル サインオン

ユース ケース 2 では、smcompany.com はビジネス パートナーである partsco.com から部品を購入します。

エンジニアは smcompany.com で認証を行い、リンクをクリックして partsco.com の情報にアクセスします。 smcompany.com のエンジニアとして、ユーザは partsco.com の Web サイトにログインせずとも、このサイトの「仕様書」部分に直接移動できます。

smcompany.com の購入者は認証を行い、partsco.com のリンクをクリックします。 購入者は partsco.com Web サイトの「部品リスト」部分に直接移動できます。 購入者はログインする必要がありません。

以下の画像は、2 つのパートナーの関係を示しています。



ユーザ名などの他の属性が smcompany.com から partsco.com に渡されると、個々のユーザに合わせてインターフェースがカスタマイズされます。

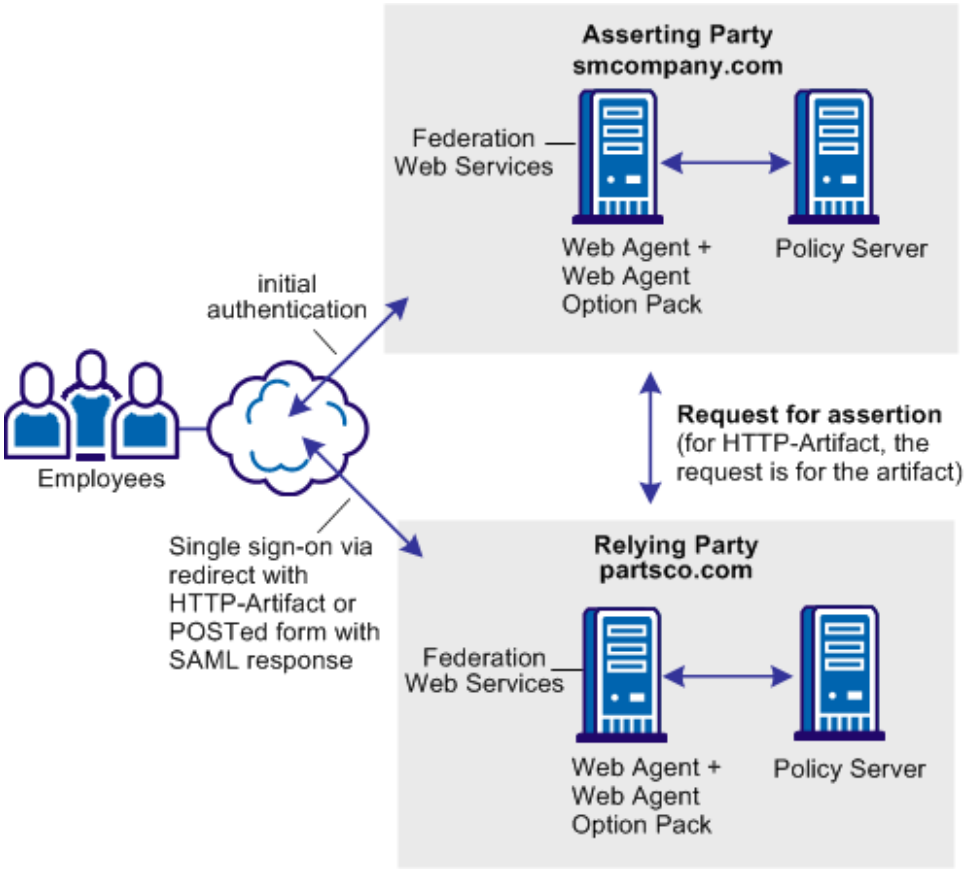
partsco.com は、smcompany.com 全社員のユーザ ID を保持する必要はありませんが、Web サイトの機密部分へのアクセスを制御する必要があります。アクセスを制御するために、partsco.com は smcompany.com のユーザについて、限られた数の ID を保有します。 エンジニア用に 1 つの ID、購入者用に 1 つの ID が保持されます。

smcompany.com の社員が partsco.com にアクセスすると、smcompany.com は partsco.com に安全な方法でユーザ属性を送信します。 partsco.com は、属性を使用して、ユーザのアクセスを制御する識別子を特定します。

ソリューション: ユーザ属性に基づいたシングル サインオン

smcompany.com および ahealthco.com でフェデレーションを展開すると、「ユース ケース： ユーザ属性プロファイルに基づくシングル サインオン (P. 22)」を解決できます。

図は、SAML 1.1、SAML 2.0、および WS-Federation の場合、類似しています。



SiteMinder は両方のサイトで展開します。ユーザと各サイトの間のインタラクションはどれも似ています。この場合、partsco.com が依存パーティとして機能します。フェデレーション Web サービス アプリケーションには、トランザクションを処理するために必要なサーブレットがすべてを含まれます。

注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

イベント シーケンスは、次の項目を除き、「アカウント リンクに基づくシングル サインオン (P. 13)」のソリューションの場合に似ています。

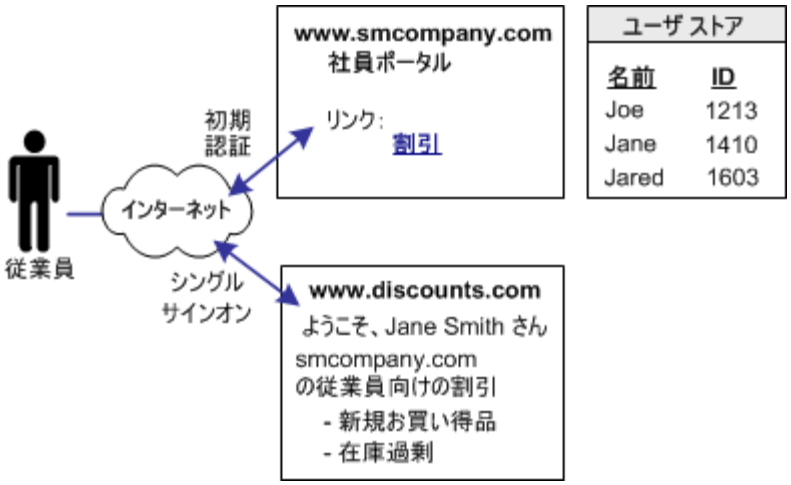
- smcompany.com の管理者が partsco.com とのパートナーシップを定義します。
- パートナーシップ設定には、*部門*という名前のアサーション属性が含まれます。 この属性では、ユーザが属するグループが指定されます。ポリシー サーバでは、要求しているユーザに対して生成するアサーションにこの属性を含みます。
- 管理者が partsco.com の Web サイトへのアクセスを許可されている部門ごとに 1 つのユーザ レコードを定義します。
- partsco.com の管理者が smcompany.com とのパートナーシップを定義します。
- アサーション コンシューマ サービスがアサーションから部門属性を抽出します。ポリシー サーバが、部門属性の値が一致しているユーザ レコードを求めて、partsco.com のユーザ ディレクトリを検索します。

ユース ケース: ローカル ユーザ アカウントなしのシングル サインオン

このユース ケースでは、smcompany.com が discounts.com とのパートナーシップを確立して社員割引を提供します。

社員が smcompany.com で認証を行い、discounts.com へアクセスするリンクをクリックします。 社員が discounts.com の Web サイトに移動すると、smcompany.com の社員に利用可能な割引が表示されます。discounts.com の Web サイトにはログインする必要はありません。

次の図はこのユース ケースを示しています。

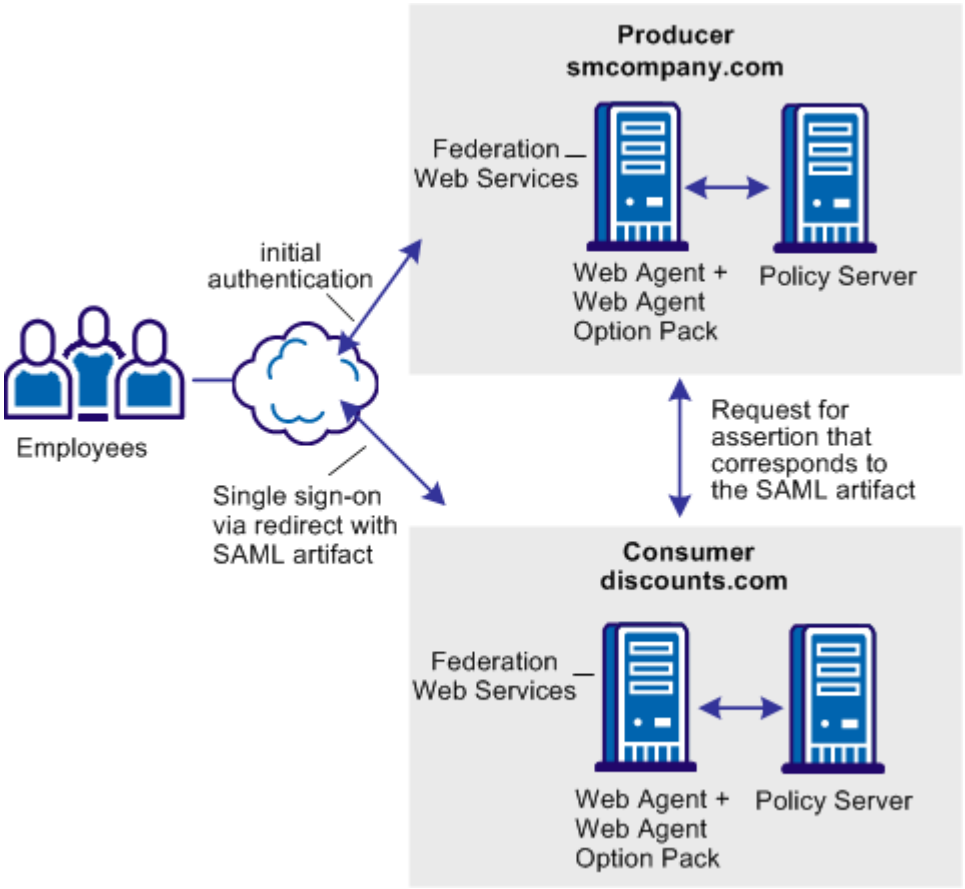


discounts.com は、smcompany.com の社員の ID を保守しません。 smcompany.com のすべての社員は、smcompany.com で認証を行う限り discounts.com へのアクセスが許可されます。 smcompany.com は、アクセスが許可されるように、リソースをリクエストしているユーザに関する認証情報を安全な方法で discounts.com に送信します。

ソリューション: ローカル ユーザ アカウントなしのシングル サインオン

smcompany.com と discounts.com でフェデレーションを展開して、「ユース ケース： ローカル ユーザ アカウントなしのシングル サインオン (P. 26)」を解決します。

次の図は、ローカル ユーザ アカウントなしのシングル サインオンを示しています。 SAML 1.1 は使用中の SSO プロファイルです。



注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

この展開では、SiteMinder は両方のサイトにあります。 smcompany.com は SAML 1.1 プロデューサです。smcompany.com の管理者が、discounts.com を表すリモート エンティティが含まれる SAML 1.1 パートナーシップを設定します。パートナーシップで設定されている属性はいずれも、アサーションに取り込まれます。

このソリューションがうまくいくためには、すべてのユーザをそれぞれ単一のユーザ アカウントにマップし、単一ユーザを本質的に匿名のユーザとする必要があります。

smcompany.com の従業員が従業員ポータルにアクセスすると、以下プロセスが発生します。

1. まず、Web エージェントによって認証が行われます。
2. 従業員が、discounts.com での取り引きにアクセスするためにリンクをクリックします。 このリンクは、ユーザを別のサイトに転送することになるため、サイト間転送 URL と呼ばれます。
3. サイト間転送 URL が Web エージェントに要求を出します。 この URL には、SAML 認証情報コレクタの場所と、コンシューマ サイトのターゲット URL が含まれています。
4. smcompany.com の Web エージェントがポリシー サーバを呼び出します。ポリシー サーバは、アサーションおよびアーティファクトを生成し、そのアサーションをセッション ストアに格納します。
5. ポリシー サーバは FWS アプリケーションにアーティファクトを返し、それによって応答が作成されます。
6. ブラウザは、アーティファクト応答によって、discounts.com にユーザをリダイレクトします。

discounts.com はコンシューマ サイトです。 discounts.com の管理者は、SP から IdP へのパートナーシップを設定します。パートナーシップ設定では、smcompany.com のアサーション検索サービスの場所と、保護されているターゲット リソースが指定されます。

パートナーシップのユーザ識別設定では、単一ユーザを検索する場合に使用するカスタム ユーザ検索仕様を指定する必要があります。 たとえば、ユーザ ディレクトリが LDAP である場合、検索指定は uid=user1 です。

重要: すべてのユーザをいずれも単一ユーザにマップするには、discounts.com のユーザ ディレクトリが存在する必要があります。 このユーザ ディレクトリには単一ユーザ レコードが含まれる必要があります。同じユーザ レコードを返すポリシー サーバ API を使用してユーザ ディレクトリを作成するという方法もあります。

以下のプロセスが発生します。

1. ブラウザが SAML 認証情報コレクタに応答をポストします。これにより、smcompany.com のアサーション検索サービスの場所が取得されます。
2. SAML 認証情報コレクタはバックチャネルで smcompany.com のアサーション検索サービスを呼び出します。 セッション ID が Artifact から抽出されます。
3. ポリシー サーバがセッション ストアからアサーションを取得し、discounts.com の SAML 認証情報コレクタにそれを返します。
4. SAML 認証情報コレクタは SAML アサーションを検証し、ブラウザにセッション Cookie を発行します。
5. ブラウザはユーザを discounts.com のターゲット リソースにリダイレクトします。

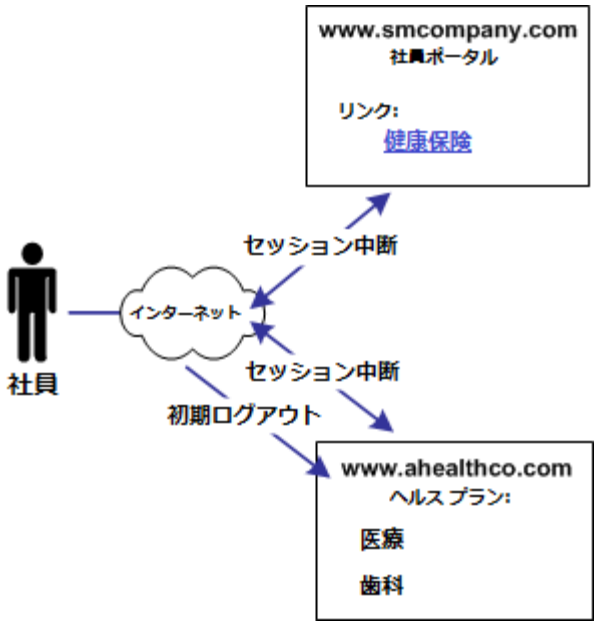
ユース ケース: SAML の 2.0 シングル ログアウト

このユース ケースでは、smcompany.com の社員が社員ポータルで認証を行い、リンクを選択して、ahealthco.com にある健康保険情報を表示します。 社員は ahealthco.com の Web サイトに自動的に移動し、サイトにログインしなくても、健康保険情報が表示されます。

社員が ahealthco.com からログアウトした後、サイトは ahealthco.com および smcompany.com でのユーザ セッションの終了を確認する必要があります。 両方のセッションを終了させることで、許可されていない社員による、既存のセッションを利用した smcompany.com のリソースへの不正アクセスや、許可された社員の健康保険情報の不正表示を防止できます。

注: この場合、初期ログアウトが ahealthco.com で発生し、結果、両方のセッションが終了します。

次の図はこのユースケースを示しています。



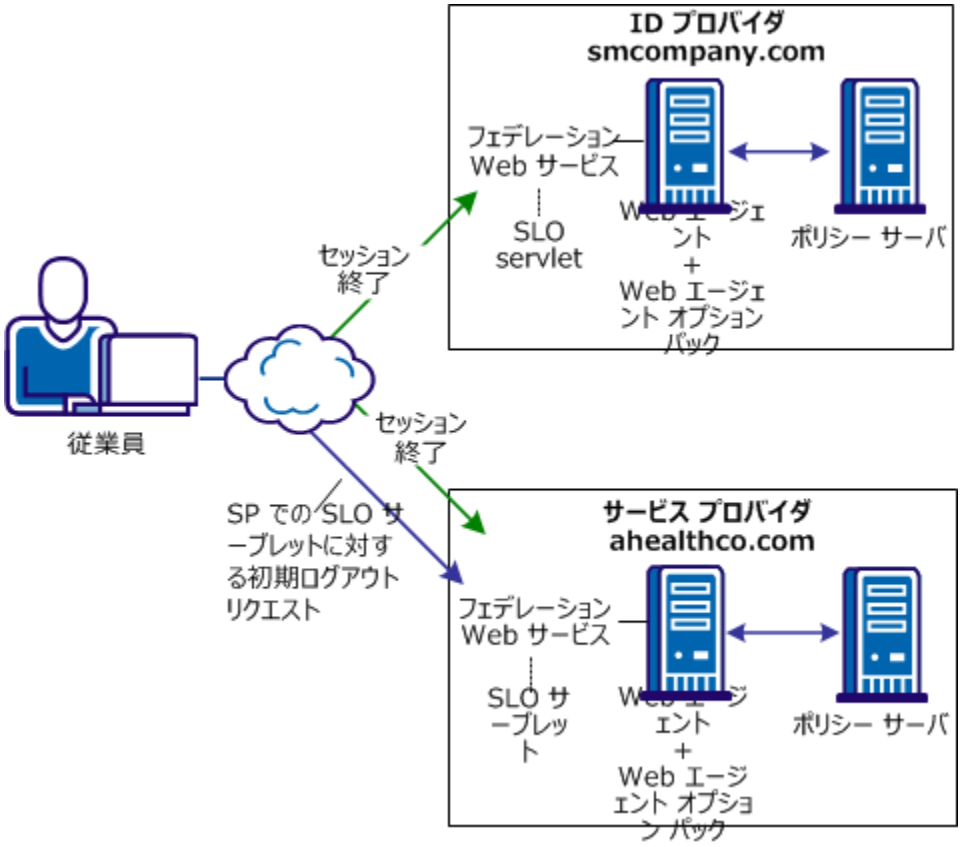
ソリューション: SAML 2.0 シングル ログアウト

フェデレーションを使用して「ユース ケース：SAML 2.0 シングル ログアウト (P. 29)」を解決できます。

このソリューションは以下のように展開します。

- smcompany.com はアイデンティティ プロバイダです。
- ahealthco.com はログアウト要求を開始するサービス プロバイダです。
- シングル ログアウトはアイデンティティ プロバイダおよびサービス プロバイダで有効です。

次の図は、シングル ログアウトのためのソリューションを示しています。



注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

SP で開始されるシングル ログアウトの場合、以下のイベント シーケンスが発生します。

1. 従業員が smcompany.com で認証を行い、フェデレーション シングル サインオンによって ahealthcom.com の健康保険情報にアクセスします。 smcompany.com は、そのセッション ストアに ahealthco.com に関する情報を配置します。 ahealthco.com は、そのセッション ストアに smcompany.com に関する情報を配置します。
2. 従業員は健康保険の閲覧を終了し、ahealthco.com のログアウト リンクをクリックします。 ブラウザがシングル ログアウト サーブレットにアクセスします。
3. ahealthco.com の FWS アプリケーションが、既存の SMSESSION Cookie の名前を SESSIONSIGNOUT に変更して、ユーザの現在のセッションを無効にします。
4. ユーザ セッションは ahealthco.com で終了します。

   注: 終了によりセッション ストアからセッションが削除されるわけではなく、セッションの状態は LogoutInProgress に設定されます。
5. ポリシー サーバが、smcompany.com のユーザ セッションを無効にするためにログアウト リクエストを生成します。 ポリシー サーバはまた、smcompany.com のプロバイダ ID を返します。
6. ブラウザは、ログアウト リクエストを smcompany.com のシングル ログアウト サーブレットにリダイレクトします。ログアウトメッセージがクエリ パラメータとして追加されます。
7. FWS アプリケーションは、ログアウト リクエスト メッセージを受信し、SMSESSION Cookie を SESSIONSIGNOUT に名前変更します。
8. FWS は、ユーザ セッションに関連付けられているすべてのサービス プロバイダからのユーザ セッションを無効にします。唯一の例外は、ログアウト リクエストを開始した ahealthco.com のセッションです。
9. すべてのサービス プロバイダがログアウトを確認した後、smcompany.com がセッション ストアからユーザ セッションを削除します。 FWS は SESSIONSIGNOUT Cookie を削除します。

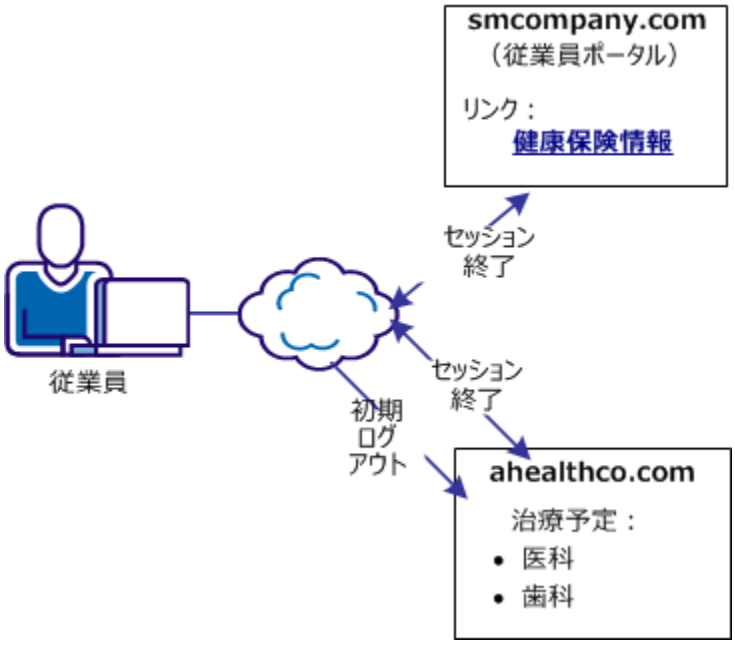
   注: 他のサービス プロバイダは図で識別されていません。
10. Smcompany.com が、開始サービス プロバイダである ahealthco.com にログアウト応答メッセージを返します。ユーザ セッションがそのセッション ストアから削除されます。
11. ユーザは最終的に ahealthco.com の SLO 設定ページにリダイレクトされます。

ユース ケース: WS-フェデレーション サインアウト

このユース ケースでは、smcompany.com の社員が社員ポータルで認証を行います。 社員は、リンクを選択して、ahealthco.com にある健康保険情報を表示します。 社員は ahealthco.com のサイトに移動し、このサイトにサインオンしなくても健康保険情報が表示されます。

社員がログアウトすると、ahealthco.com はそのサイトおよび smcompany.com のユーザ セッションを終了させる必要があります。 両方のセッションを終了させることで、許可されていない社員による、既存のセッションを利用した smcompany.com や ahealthco.com のリソースへの不正アクセスを防止できます。

次の図はこのユースケースを示しています。



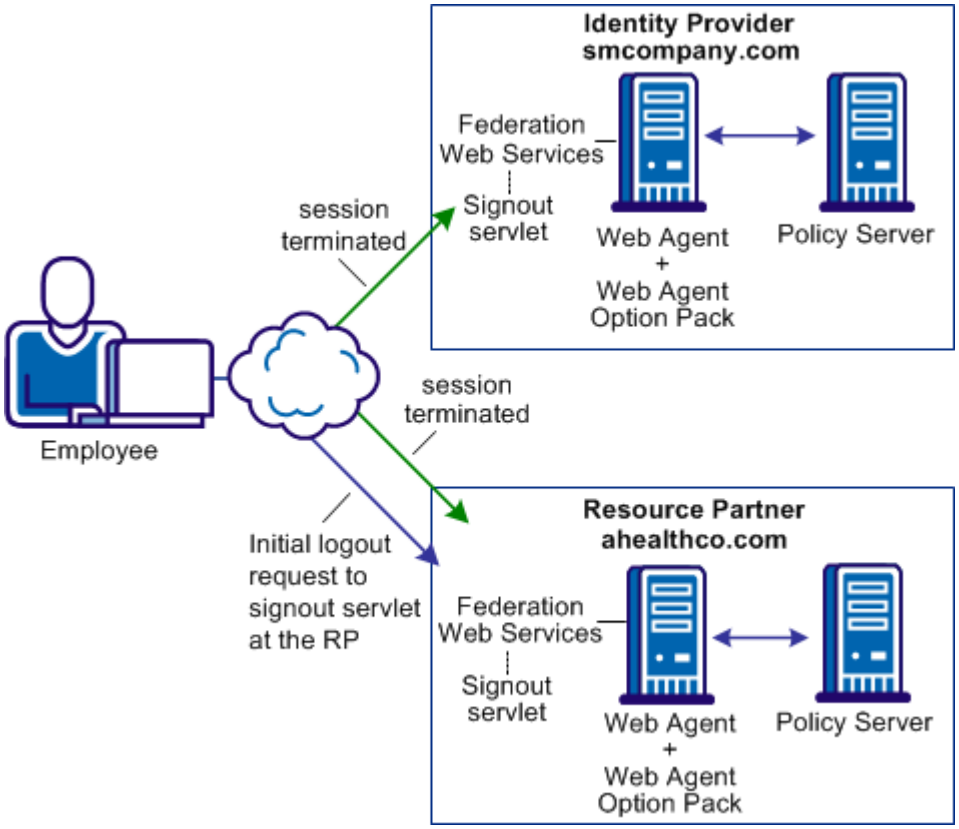
ソリューション: WS-フェデレーション サインアウト

以下のフェデレーション実装によって、「ユース ケース: WS-フェデレーション サインアウト (P. 33)」が解決されます。

このソリューションは以下のように展開します。

- smcompany.com はアイデンティティ プロバイダです。
- ahealthco.com はリソース パートナーであり、サインアウト リクエストを開始します。
- シングル サインオンを有効にするために、smcompany.com と ahealthco.com の間で WSFED IP-RP パートナーシップが設定されます。
- アイデンティティ プロバイダとリソース パートナーで、HTTP バインディングを使用する WS-フェデレーション サインアウトが有効になります。

次の図は、WS-フェデレーション サインアウトを示しています。



注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

以下のイベント シーケンスが発生します。

1. 従業員は smcompany.com で認証を行ってから、ahealthco.com と連携してその健康封建情報を表示します。 トランザクションの間、smcompany.com はセッション ストアに ahealthco.com に関する情報を配置します。 ahealthco.com は、そのセッション ストアに smcompany.com に関する情報を配置します。
2. 従業員は健康保険情報の閲覧を終了し、ahealthco.com のログアウト リンクをクリックします。 サインアウト サービスがサインアウト リクエストを受信します。
3. サインアウト サービスは、SMSESSION Cookie からのセッション情報を取得し、ユーザ セッションに関連付けられているアイデンティティ プロバイダを特定します。
4. サインアウト サービスは、ポリシー サーバを呼び出してセッションを無効にします。
5. サインアウト サービスはサインアウト リクエストを生成し、そのサインアウト リクエストを smcompany.com のサインアウト URL に転送します。
6. smcompany.com のサインアウト サービスがリクエストを受信します。
7. サインアウト サービスは、SMSESSION Cookie からのセッション情報を取得し、ユーザ セッションに関連付けられているリソース パートナーを特定します。
8. サインアウト サービスは、ポリシー サーバを呼び出してセッションを無効にします。

9. サインアウト サービスはサインアウト リクエストを生成し、サインアウト メッセージおよび複数の RP-SignoutCleanup の場所を、ポスト データとして SignoutConfirmURL JSP にポストします。

   SignoutConfirm ページによってフレーム ベースの HTML ページが生成されます。各フレームには、ユーザ セッションに関連付けられている各リソース パートナーのサインアウト クリーンアップ URL が含まれます。

10. ahealthco.com は、ユーザ セッションに関連付けられている任意のリソース パートナーにサインアウト リクエストを転送します。 各 RP で、セッション ストアからのセッションが終了します。

11. 各 RP は、サインアウト クリーンアップ URL ahealthco.com にブラウザを開始パートナーとしてリダイレクトして、サインアウトを完了します。

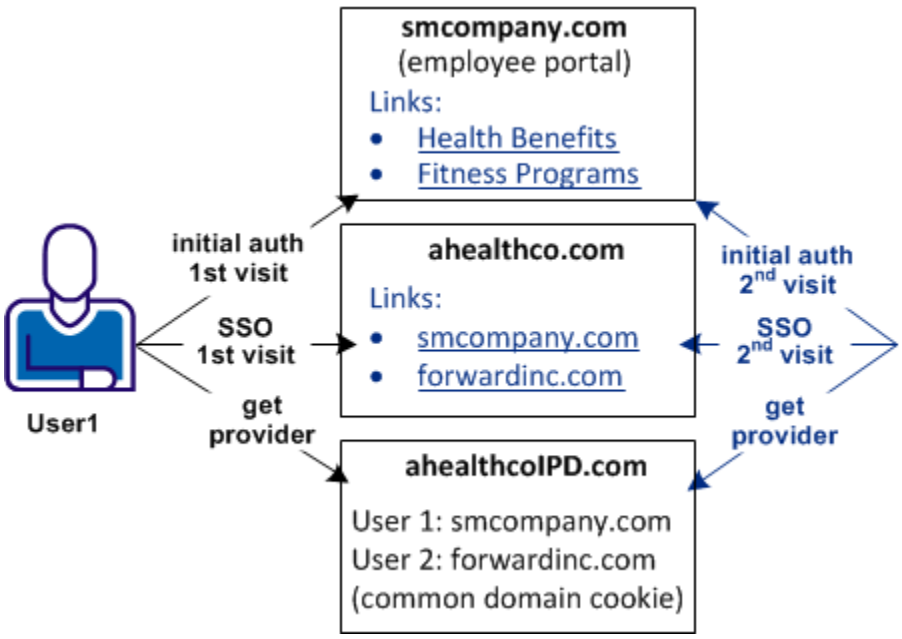
ユース ケース: アイデンティティ プロバイダ ディスカバリ プロファイル

このユース ケースでは、いくつかの会社が、ahealthco.com と健康保険管理契約を結びます。 ユーザは自分の健康保険情報を表示するために ahealthco.com にログオンします。 ahealthco.com は、特定のユーザについて、認証リクエストをどのアイデンティティ プロバイダに送信するか決定する必要があります。

IdP ディスカバリは、複数のパートナーがアサーションを提供するフェデレーション ネットワークで役立ちます。このプロファイルは、必要なユーザ レコードが存在するアイデンティティ プロバイダをサービス プロバイダが特定できるように、動的な方法を提供します。

次の図は、アイデンティティ プロバイダ ディスカバリ プロファイルが使用されているネットワークを示しています。

注: すべてのサイトがアイデンティティ プロバイダ ディスカバリ サービスと対話するように、このネットワークのサイト間では前もって業務提携契約が結ばれています。



この例では、User1 は ahealthco.com に到達します。ahealthco.com は、User1 が smcompany.com から来たと断定します。aheathco.com は、ahealthco.com の共通のドメイン Cookie 内に smcompany.com の Cookie を設定します。forwardinc.com などの他の会社は、健康保険給付サイトとして ahealthco.com を使用する別のアイデンティティ プロバイダです。 ユーザが forwardinc.com から ahealthco.com に移動すると、共通のドメイン Cookie にも Cookie が設定されます。

ソリューション: アイデンティティ プロバイダ ディスカバリ プロファイル

フェデレーションによって「ユース ケース: アイデンティティ プロバイダ ディスカバリ プロファイル (P. 36)」を解決できます。

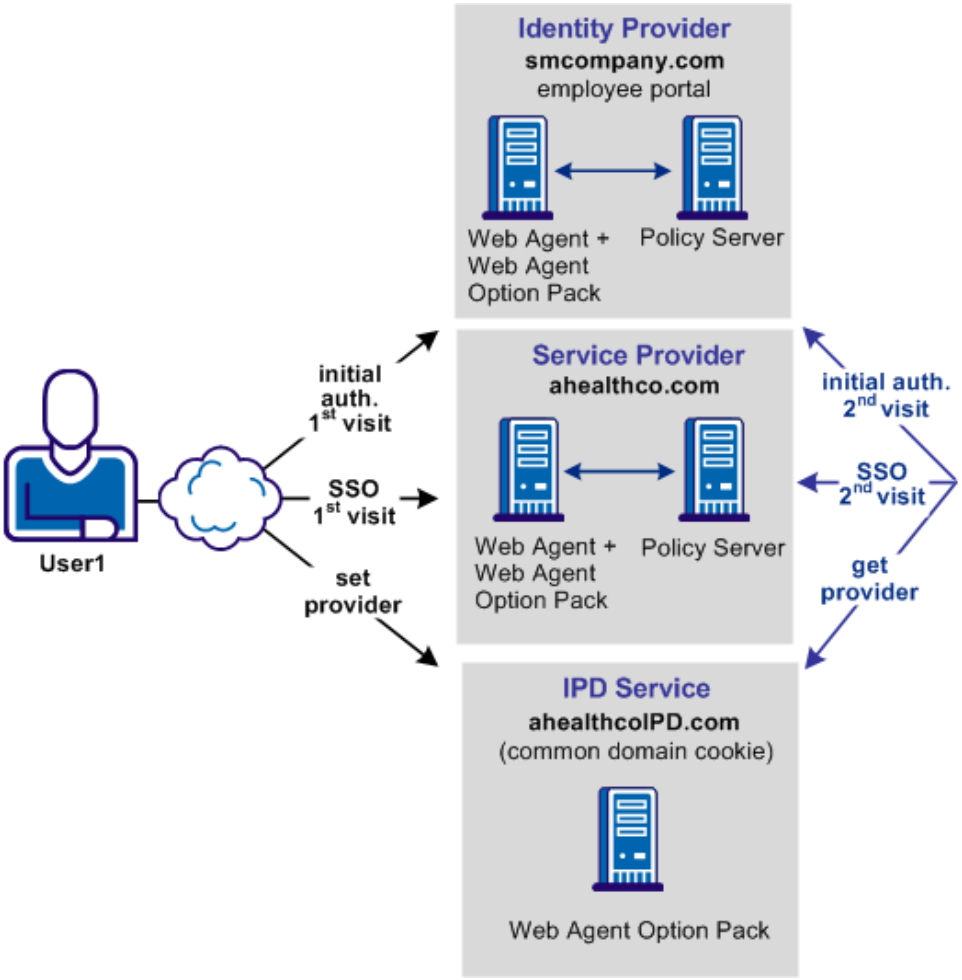
IdP ディスカバリ プロファイル (SAML 2.0 のみ) は、2 つのフェデレーション パートナーに共通の Cookie ドメインを使用して実装されます。 合意されたドメインの Cookie には、そのユーザがアクセスしたことがある IdP のリストが含まれています。

注: サービス プロバイダの認証を受けるユーザは、アイデンティティ プロバイダへのアクセスおよび認証を完了してからサービス プロバイダにアクセスする必要があります。

このソリューションは以下のように展開します。

- smcompany.com は、User 1 用のアサーションを発行し、そのサービス プロバイダとして ahealthco.com を設定します。
- ahealthco.com は smcompany.com 用のサービス プロバイダです。 このサイトの SAML 2.0 SP-IdP パートナーシップは、そのサービスを使用する各アイデンティティ プロバイダで設定されています。
- ahealthcoIPD.com は ahealthco.com 用のアイデンティティ プロバイダ ディスカバリ サービスです。 Web エージェント オプション パックでインストールされたフェデレーション Web サービス アプリケーションは IPD サービスを提供します。 このサービスは共通ドメイン Cookie を読み取ります。この Cookie には ahealthco.com に関連するアイデンティティ プロバイダがすべて含まれます。

次の図は、このソリューションのフェデレーション ネットワークを示しています。



注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

トランザクション フローを以下に示します。

1. ユーザ 1 はまず、smcompany.com にログインして認証します。 次に、ユーザは再認証の必要なしに、ahealthco.com と連携します。

   smcompany.com と ahealthco.com の間には、ahealthcoIPD.com を IPD サービスとして使用するための許諾契約が存在します。

2. smcompany.com の FWS アプリケーションは、アイデンティティ プロバイダ ID を渡すことにより、ポリシー サーバにアイデンティティ プロバイダ ディスカバリ プロファイル（IPD）設定を要求します。

3. ポリシー サーバが、IPD 設定（IPD サービス URL、共通ドメイン cookie、および共通ドメイン cookie の永続性情報など）を返します。

4. smcompany.com の FWS アプリケーションは、ユーザを IPD サービス URL にリダイレクトし、共通のドメイン Cookie を設定します。 smcompany.com のアイデンティティ プロバイダ ID が IPD サービスの共通ドメイン Cookie に書き込まれます。

5. IPD サービスは smcompany.com のシングル サインオン サービスにユーザをリダイレクトします。 リダイレクトには認証リクエストが含まれます。

6. smcompany.com の FWS アプリケーションはポリシー サーバにアサーションを要求します。ポリシー サーバは、保持している ahealthco.com 用のパートナーシップ設定に基づいてアサーションを生成します。

7. FWS アプリケーションは ahealthco.com にアサーション応答を返します。

8. これで、ユーザ 1 は、ahealthco.com に正常にログオンし、健康保険情報を見ることができます。 ユーザは健康保険情報の閲覧を終了しログアウトします。

9. 別の日に異なるトランザクションで、ユーザ 1 は、ahealthco.com に直接ログインします。ユーザ 1 は、健康保険情報を再度閲覧するために、リンクをクリックします。 ahealthIPD.com には、ユーザ 1 がアクセスしたすべてのアイデンティティ プロバイダの Cookie があります。 ahealthco.com は、IPD 検出サービスを呼び出して、アイデンティティ プロバイダ ID を取得します。

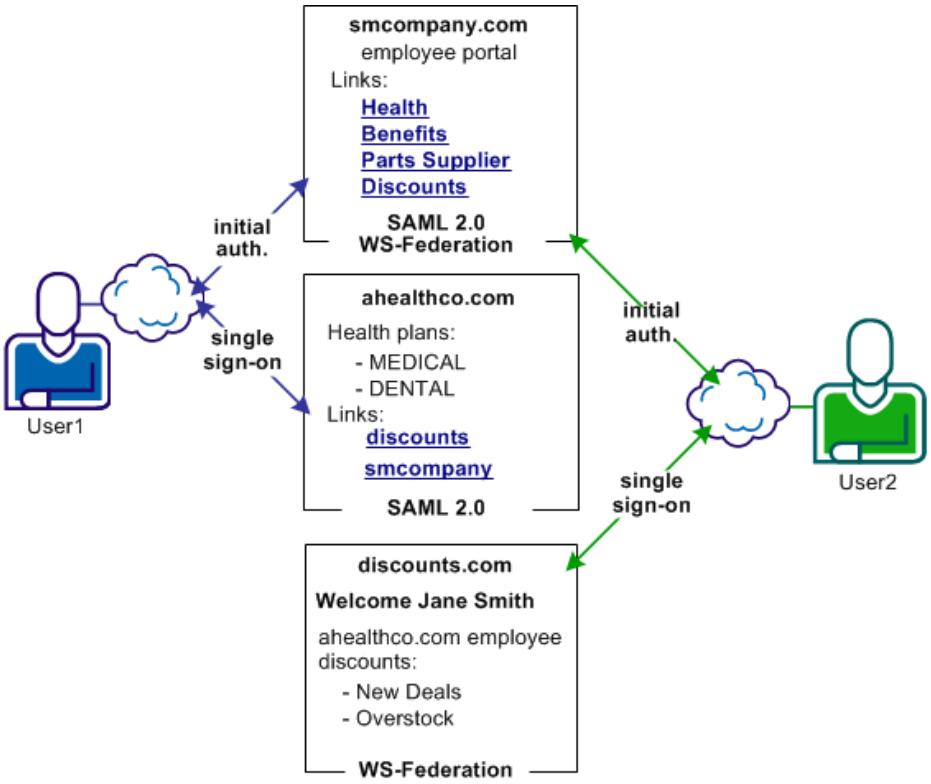
10. ahealthco.com では、認証可能な会社を選択できるように、ユーザ 1 にサイト選定ページを提供します。ユーザ 1 は smcompany.com を選択します。

11. ahealthco.com は smcompany.com に認証リクエストを送信します。 smcompany.com のポリシー サーバはアサーションを生成し、それを ahealthco.com のアサーション コンシューマ サービスに送信します。
12. ユーザは正常にログインすると、リクエストしたリソースにリダイレクトされます。

ユース ケース: 複数の SSO プロファイルによるフェデレーション

このユース ケースでは、smcompany.com が ahealthco.com および discounts.com 向けのアサーションを発行します。 ahealthco.com は SAML 2.0 プロファイルを使用します。discounts.com は WS-フェデレーション プロファイルを使用します。 発行するアサーションは、依存パーティがアサーションを使用できるように、適切なプロファイルに従って生成する必要があります。

次の図は、マルチプロトコルのユース ケースを示しています。



ソリューション: 複数の SSO プロファイルによるフェデレーション

以下のフェデレーション展開により、「ユース ケース： 複数の SSO プロファイルによるフェデレーション (P. 41)」が解決されます。

注: このソリューションのシングル サインオン トランザクションは、アカウント リンク トランザクションの使用に似ています。

このソリューションは以下のように展開します。

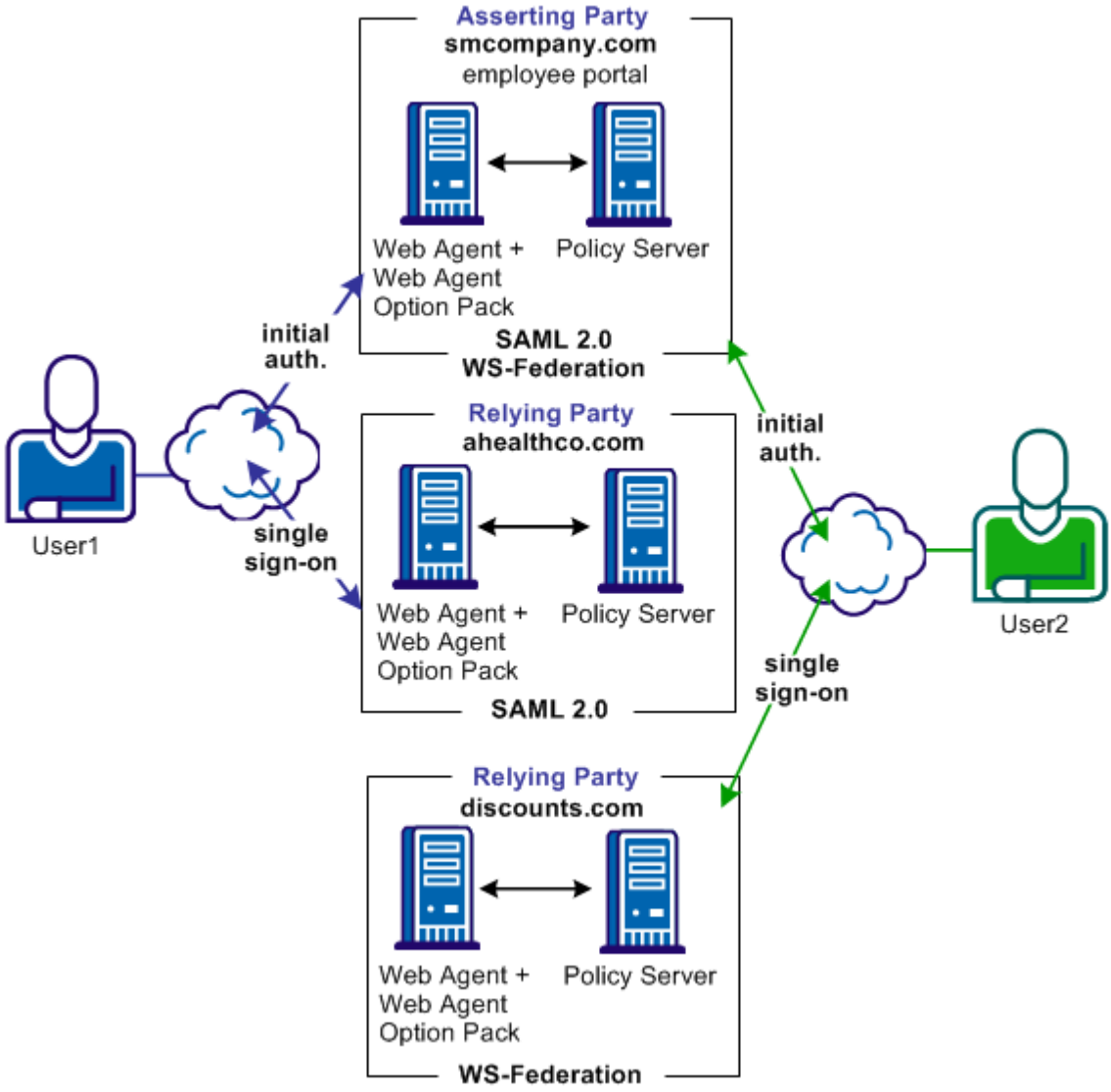
ユーザ 1

- smcompany.com は ahealthco.com の SAML 2.0 アイデンティティ プロバイダです。
- ahealthco.com は SAML 2.0 サービス プロバイダです。

ユーザ 2

- smcompany.com は discounts.com の WS-フェデレーション アイデンティティ プロバイダです。
- discounts.com は WS-フェデレーション リソース パートナーです。

以下の図は、マルチプロトコル サポートを実装したフェデレーション ネットワークを示しています。



注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

このマルチプロトコル ソリューションでは、さまざまな SSO プロファイル用のシングル サインオン トランザクションのフローがアカウント リンク SSO トランザクションに似ています。

- smcompany.com は、ユーザ 1 が ahealthco.com のリソースにアクセスする場合に SAML 2.0 アサーションを発行できます。
- smcompany.com はまた、ユーザ 2 が discounts.com で認証する場合に SAML 1.1 アサーションが含まれるトークン応答を発行できます。 アサーションの SSO プロファイルは、パートナーシップ設定によって、および初期認証中に設定されるセッション Cookie に基づいて確定されます。

この解決策のために、以下のパートナーシップが smcompany.com で設定されます

- IdP から SP へのパートナーシップ。smcompany.com がローカル IdP で、ahealthco.com がリモート SP です。
- IP から RP へのパートナーシップ。smcompany.com がローカル IP で、discounts.com がリモート RP です。

以下のパートナーシップが ahealthco.com で設定されます。

- SP から IdP へのパートナーシップ。ahealthco.com がローカル SP で、smcompany.com がリモート IdP です。

以下のパートナーシップが discounts.com で設定されます。

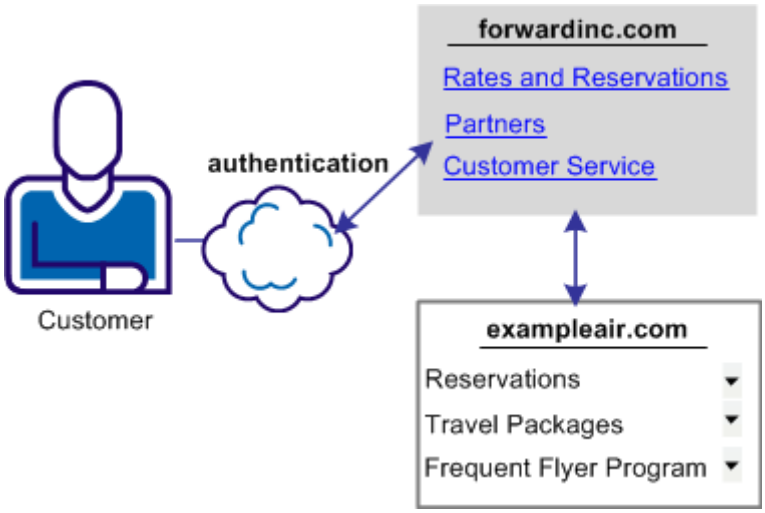
- RP から IP へのパートナーシップ。discounts.com がローカル RP で、smcompany.com がリモート IP です。

ユース ケース: ユーザ属性に基づく SAML 2.0 ユーザ認証

このユース ケースでは、forwardinc.com はレンタカー サービスであり、exampleair.com は旅行代理店です。

forwardinc.com の顧客は forwardinc.com でログインして認証を行い、リンクをクリックしてレンタカーの見積もりをとります。 forwardinc.com の顧客プロファイルには、exampleair.com 用の顧客のマイレージ会員番号が含まれます。 マイレージ会員アカウントによって、forwardinc.com でのステータス レベルが決定されます。 ステータス レベルによって顧客に適用するレンタカー割引が決定されます。

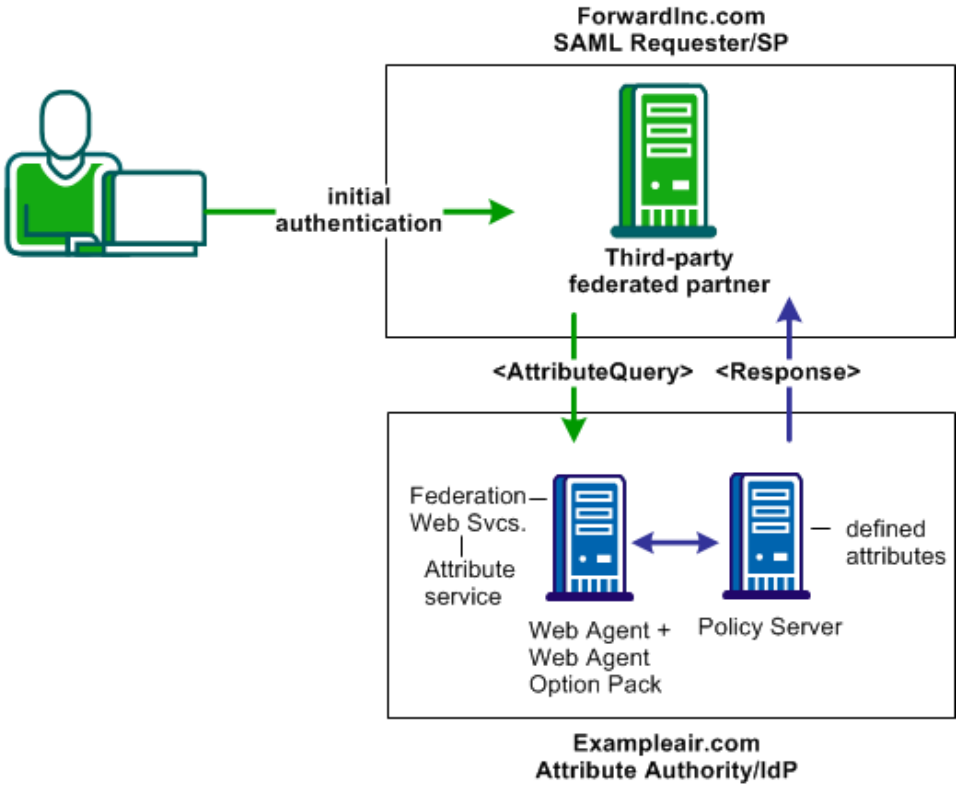
次の図はこのユース ケースを示しています。



forwardinc.com は適切な割引情報を顧客に提示します。 ただし、forwardinc.com は、顧客がまず exampleair.com にログインして認証を行い、次に再度自社のサイトにログインしなくても済むようにします。

ソリューション: ユーザ属性に基づく SAML 2.0 ユーザ認可

SAML 2.0 属性クエリ/レスポンス プロファイルで、「ユース ケース: ユーザ属性に基づく SAML 2.0 ユーザ認可 (P. 44)」を解決できます。



注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

この展開は以下のようになります。

- SiteMinder は、IdP/属性機関である example.air でのみ展開します。Web エージェント オプション パックのある Web エージェントが 1 つのシステムにインストールされ、ポリシー サーバが別のシステムにインストールされます。

  注: SiteMinder は属性クエリ プロファイルを実装するために IdP として機能する必要があります。 つまり、SiteMinder は属性権限になり、属性クエリに応答することができます。SiteMinder は SP として機能できず、属性クエリを送信できません。

- forwardinc.com は、属性クエリ/レスポンス プロファイルを使用するように設定される、サードパーティのサービス プロバイダです。

forwardinc.com は SAML リクエスタとして機能します。 顧客がこのサイトでログインすると、以下のイベント シーケンスが発生します。

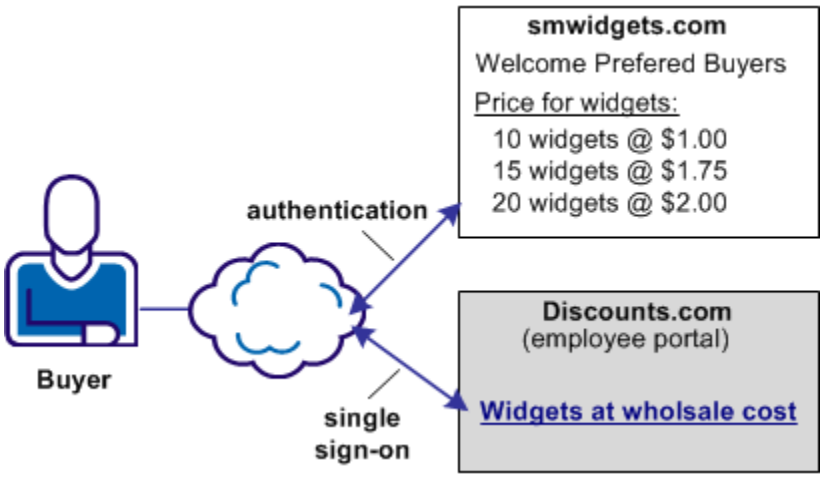
1. ユーザが forwardinc.com にログインし、認証されます。
2. ユーザは自動車を借りるためにリンクをクリックします。 forwardinc.com は未解決のマイレージ会員属性を識別します。
3. forwardinc.com は、ローカル ユーザ ディレクトリでユーザを検索することにより属性の解決を試みますが、ユーザ属性変数を解決できません。
4. forwardinc.com は属性クエリを IdP/属性機関 exampleair.com に SOAP リクエストとして送信します。クエリ リクエストには、マイレージ会員属性が含まれます。
5. exampleair.com はユーザに関する自社のユーザ ディレクトリ レコードを参照して、マイレージ会員属性を解決します。 exampleair.com はアサーションを SOAP レスポンスとして forwardinc.com に返します。そのアサーションにはリクエストされた属性が含まれます。
6. SAML リクエスタは属性を解決し、リクエストされたリソースのユーザを認可します。
7. ユーザはターゲット リソースにリダイレクトされます。

ソリューション: IdP での名前 ID のないシングル サインオン

このユース ケースでは、discounts.com が smwidgets.com からウィジェットを購入します。

discounts.com の購入者は、リンクをクリックして smwidgets.com にあるウィジェットの最新の価格表にアクセスします。 購入者は smwidgets.com の Web サイトに移動し、discounts.com の Web サイトにログインしなくても価格表が表示されます。

次の図はこのユース ケースを示しています。



discounts.com にローカルに格納された購入者 ID はありません。 したがって、discounts.com は、smwidgets.com で購入者の ID を取得します。 discounts.com は smwidgets.com に認証リクエストを送信します。 smwidgets.com はリクエストを受信しますが、名前 ID 属性の値を見つけることはできません。 smwidgets.com は、購入者の一意の永続的な ID を生成し、この ID をアサーションに追加します。 discounts.com はこの一意の識別子を使用して、購入者がリクエストされたリソースにアクセスできるようにします。

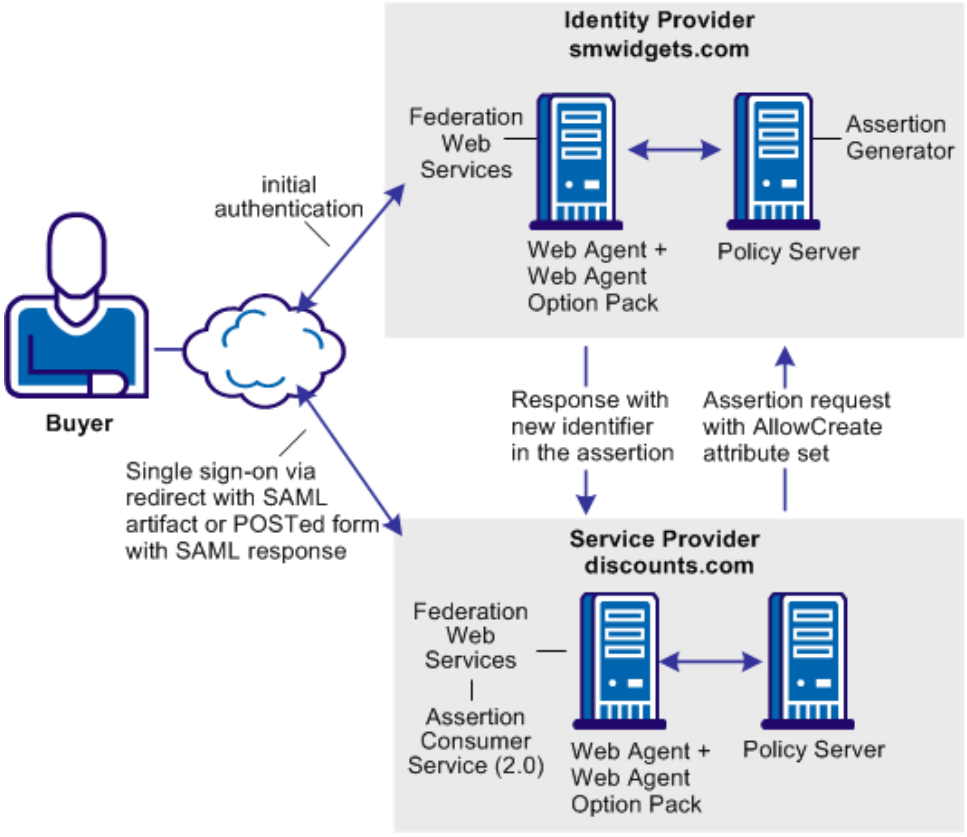
ソリューション: IdP での名前 ID のないシングル サインオン

許可/作成属性を使用することで、「ユース ケース： IdP での名前 ID なしでのシングル サインオン (P. 48)」が解決されます。

注: このソリューションには SAML 2.0 プロファイルが必要です。

フェデレーションは discounts.com と smwidgets.com で展開されます。1 つのシステムに Web エージェントと Web エージェント オプション パックがインストールされ、別のシステムにはポリシー サーバがインストールされます。

次の図で、smwidgets.com はアイデンティティ プロバイダであり、discounts.com はサービス プロバイダです。



注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

アイデンティティ プロバイダでユーザ ID なしで 2 つのサイト間のシングル サインオンを有効にするために、以下のイベント シーケンスが発生します。

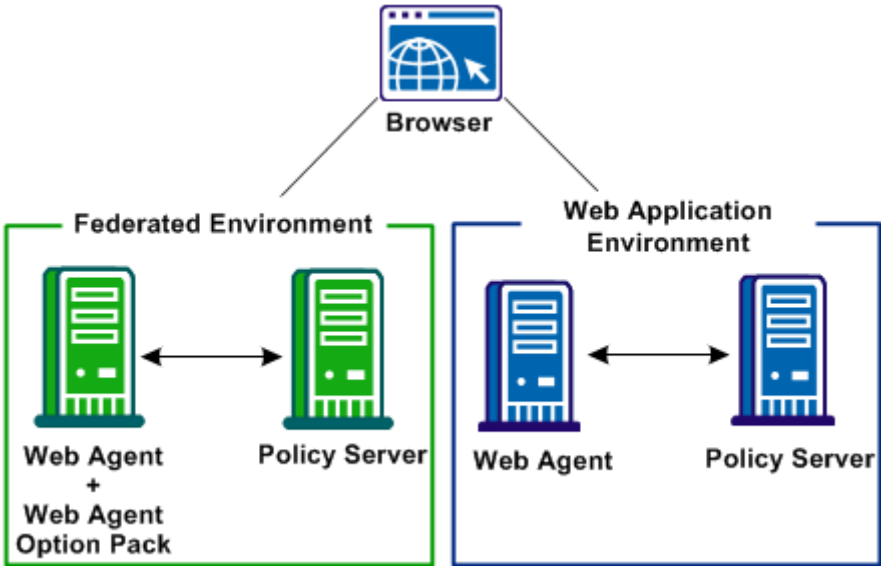
1. ユーザ（この場合は購入者）が discounts.com で認証を行います。 このリンクによって認証リクエストが開始されます。
2. discounts.com のポリシー サーバが、設定内に［許可/作成］オプションが存在するかどうか確認します。 このオプションは、discounts.com の SP から IdP へのパートナーシップで有効にされます。

3. AllowCreate という名前の属性が認証リクエストに含まれます。ローカル Web エージェントのフェデレーション Web サービス アプリケーションが認証リクエストを smwidgets.com にリダイレクトします。
4. smwidgets.com のポリシー サーバはアサーションを生成します。 アサーションの生成中に、ポリシー サーバは、リソースをリクエストしているユーザのユーザ レコード内で名前 ID 属性を検索します。 ユーザ レコードに名前 ID の値はありません。
5. ポリシー サーバは、AllowCreate オプションに対する設定を検証します。ポリシー サーバはまた、認証リクエストを調べて、検索対象の AllowCreate 属性があるかどうかを確認します。
6. ポリシー サーバは、認証リクエスト内と自身の設定内に AllowCreate 属性が存在するので、一意の永続的な識別子を生成します。 ポリシー サーバは、ユーザ ストアに識別子を配置します。
7. ポリシー サーバは discounts.com のアプリケーションでフェデレーション Web サービスにアサーションを返します。 フェデレーション Web サービス アプリケーションは、discounts.com でアサーション コンシューマ サービスにアサーション レスポンスを含む自動ポスト フォームを送信します。
8. discounts.com のサービス プロバイダは、認証情報としてこの応答を使用し、ポリシー サーバにログインするための応答メッセージを使用します。
9. ポリシー サーバはそのユーザ ストア内で名前 ID を探すことにより、応答を検証します。 ポリシー サーバはユーザを特定し、ユーザにログインします。
10. Web エージェントが、discounts.com ドメインの SMSESSION cookie を生成します。
11. Web エージェントはブラウザに cookie を配置し、ユーザをターゲット宛先にリダイレクトします。

ユース ケース: セキュリティーゾーンを使用した SSO

このユース ケースでは、CompanyA は非フェデレーション Web アプリケーションを保護し、フェデレーション シングル サインオンをサポートします。SiteMinder 展開では、Web アプリケーション環境からフェデレーション環境に移動する 1 人のユーザに対して 2 つのセッションが存在することはできません。 ユーザが各環境間を移動する場合、セッション cookie は互いに上書きします。

以下は、フェデレーション環境と Web アプリケーション環境を組み合わせたサイトを示しています。

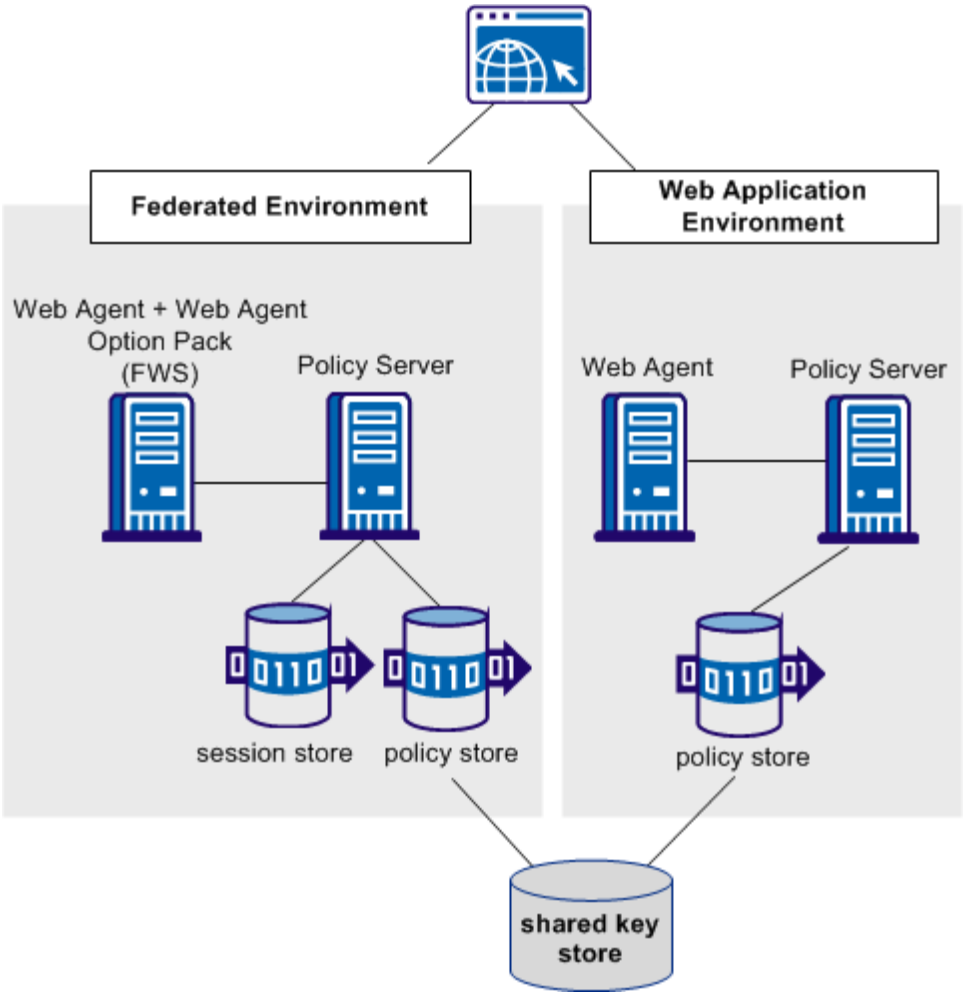


ソリューション: セキュリティーゾーンを使用した SSO

このソリューションでは、「[ユース ケース：セキュリティーゾーンを使用した SSO (P. 52)」を解決するために、セキュリティ ゾーンによって並列 Web アプリケーションとフェデレーションの環境をセットアップする方法を示します。

セキュリティ ゾーンは 1 つの cookie ドメインのセグメントで、アプリケーションを分割する場合に使用されます。 各ゾーンへ別のセキュリティ要件を割り当てることができます。 セキュリティ ゾーンを使用することにより、ポリシー サーバは、環境ごとに 1 人のユーザに対して異なるセッション cookie を生成できます。 一意の名前が付けられた 2 つのセッション cookie は生成されますが、各 cookie は Web アプリケーションおよびフェデレーション環境にわたって同じセッションを表します。 アサーティング パーティの Web エージェントは、セキュリティ ゾーンを適用します。

次の図は、1 つのアサーティング パーティで 2 つの異なる環境を使用する展開を示しています。1 つの環境はフェデレーション機能向けです。また、他方は Web アプリケーション保護向けです。



注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

この図は、次の設定を表しています。

Web アプリケーション環境

エージェント設定オブジェクトまたはローカル設定ファイル

DefaultAgent

信頼されたセキュリティ ゾーン

SM （デフォルト ゾーン）

ゾーンに対して Web エージェント が読み取る cookie

DefaultAgent 設定では、Web エージェントによるデフォルトのセッション cookie、SMSESSION の読み書きが有効です。

フェデレーション環境

エージェント設定オブジェクトまたはローカル設定ファイル

FedWA

信頼されたセキュリティ ゾーン

- Fed （デフォルト ゾーン）
- SM

ゾーンに対して Web エージェント が読み取る cookie

FedWA 設定によって、Web エージェントは、SMSESSION Cookie の読み書きが可能になります。

注: このソリューションが機能するためには、各環境にそれ自身のエージェント設定オブジェクトが必要です。

以下のイベント シーケンスが発生します。

1. ユーザがフェデレーション環境にログインします。
2. フェデレーション環境の Web エージェントは、認証 URL に対してユーザ セッションを確立するように要求を転送します。

   ユーザには、Web アプリケーション環境に前の認証の SMSESSION cookie がすでにあります。
3. フェデレーション環境で Web エージェントは SMSESSION cookie を読み取ります。 ポリシー サーバは、新しいフェデレーション セッション Cookie を生成し、Web エージェントはこの新しいセッション cookie を書き込みます。 新しいフェデレーション セッション Cookie は、SMSESSION Cookie に基づいています。

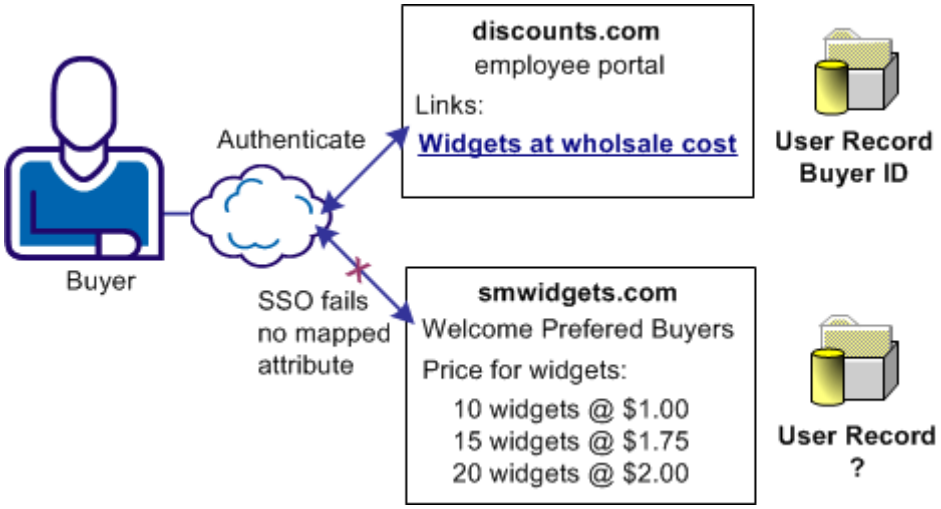
   フェデレーションでは、セッション ストアに格納される永続的なセッションを必要とします。Web アプリケーション環境から読み取られる SMSESSION Cookie は永続的ではありません。ポリシー サーバがフェデレーション Cookie を生成すると、その Cookie は変更され、セッションは永続的な Cookie にアップグレードされます。
4. フェデレーション環境内の FWS アプリケーションは、フェデレーション Cookie を読み取り、リソースに対する要求を正常に処理します。

ユース ケース: SP での動的アカウント リンクによる SSO

このユース ケースでは、IdP （discounts.com）に、特定のユーザを識別する buyerID という名前の属性が含まれています。 購入者 ID 値は名前 ID としてアサーションに入力されます。 ただし、購入者 ID に対するマップされた ID は smwidgets.com にありません。 購入者が認証され、保護されたリソースにアクセスできるようにするため、smwidgets.com は、適切なユーザ レコードに属性を作成する必要があります。

smwidgets.com の管理者は、動的なアカウント リンクを使用してマッピングを確立します。 このマッピングにより、smwidgets は購入者を認証してリソースへのアクセスを許可することができます。 discounts.com の購入者が、smwidgets.com のウィジェット上の最新の価格表にアクセスするためのリンクを選択すると、購入者は再認証する必要なしにログインできます。

次の図はこのユース ケースを示しています。



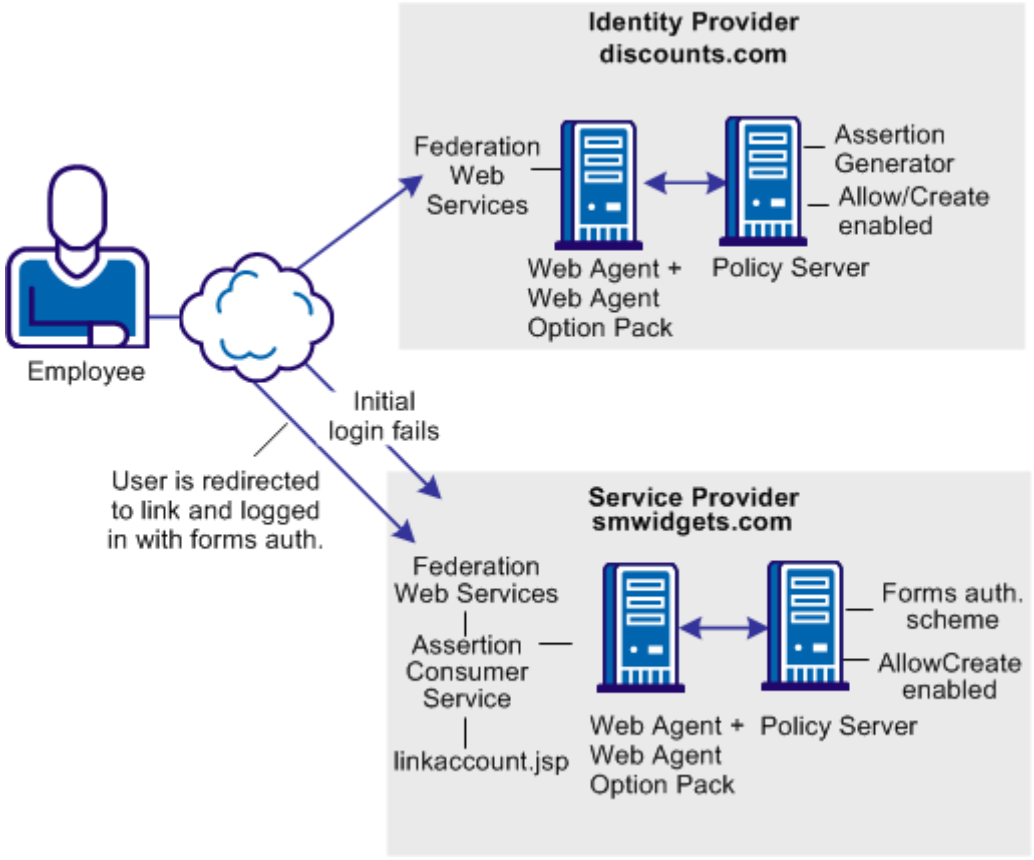
ソリューション: SP での動的アカウント リンクによる SSO

フェデレーションを IdPA.com および SPB.com に配置することで、「ユース ケース： SP での動的アカウント リンクによる SSO (P. 55)」を解決できます。

注: 動的なアカウント リンクは SAML 2.0 でのみサポートされています。

SiteMinder は両方のサイトで展開します。 各サイトでは、1 つのシステムに Web エージェントおよび Web エージェント オプション パックが、別のシステムにポリシー サーバがインストールされます。

以下の図は、サービス プロバイダでの動的アカウント リンクによるシングル サインオンを示しています。



注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

以下のイベント シーケンスが発生します。

1. 社員が最初に、discounts.com でログインし、認証を行います。 Discounts.com が社員のアサーションを作成します。 Discounts.com はアサーションをポストする（POST バインディング）か、または Artifact により smwidgets.com のアサーション コンシューマ サービスに、ユーザをリダイレクト（Artifact バインディング）します。 このアサーションには、buyerID という名前の属性が含まれます。
2. smwidgets.com のアサーション コンシューマ サービスは、ユーザを認証しようとしますが、buyerID 属性はローカル ユーザ レコードにマップしていません。 認証は失敗します。
3. smwidgets.com でのパートナーシップ設定の一部としてリダイレクト URL が定義されています。これは、ディレクトリ *web_agent_home*/affwebservices/linkaccount.jsp を指しています。 社員はこの URL にリダイレクトされます。

   注: linkaccount.jsp ファイルは保護されているレルムの一部である必要があります。 このファイルのデフォルトの場所は http://*sp_home*/affwebservices/public/ です。 この場所から保護されているレルムにファイルをコピーします。
4. フォーム認証方式によりローカル ユーザを認証する Web エージェントは、この linkaccount.jsp URL を保護します。 認証が成功したら、smwidgets.com でセッションが確立され、SMSESSION cookie が社員のブラウザに配置されます。
5. linkacount.jsp はブラウザでロードされ、ユーザに対してはサービス プロバイダ アカウントにリンクするためのメッセージが表示されます。アカウント リンクを許可するボタンをクリックします。
6. ユーザはアサーション コンシューマ サービスにリダイレクトされます。ここで、社員のブラウザはアサーションを SMSESSION cookie に提示します。
7. アサーション コンシューマ サービスはアサーションから名前 ID を抽出し、新しく作成された buyerID 属性に名前 ID 値を挿入します。 buyerID 属性は社員の既存ユーザ レコードにあります。 SMSESSION cookie の UserDN がユーザを識別するので、アサーション コンシューマ サービスは、どのユーザ レコードをマップするか知っています。

   SAML 2.0 パートナーシップに設定された検索の仕様は、どの属性が名前 ID にマップされるかを示します。この場合、検索仕様は buyerID=%s です。

8. 属性がマップされたら、アサーションに基づいてユーザが認証されます。 新しいユーザ セッションが確立されます。

   次回に同じユーザが購入者 ID を持つアサーションを提示したときには、このユーザは要求したリソースへのアクセスを正常に取得します。

SP での動的アカウント リンクの設定

サービス プロバイダで以下のコンポーネントを設定して、動的アカウント リンクを有効にします。

注: 動的なアカウント リンクは SAML 2.0 でのみサポートされています。

- AllowCreate 機能

  既存ユーザ ストアでの属性の作成を有効にします。

- リダイレクト URL

  認証が失敗した場合に、ユーザを linkaccount.jsp ファイルにリダイレクトします。認証方式によりリダイレクト URL が保護されます。認証方式はユーザに対し、ログインしてセッションを作成するよう要求します。

- Web エージェントのポスト保存

  サービス プロバイダ Web エージェントで有効である必要があります。

- 検索仕様

  アサーションの名前 ID がどの属性を置換するかを示します

サービス プロバイダで SAML 2.0 POST または Artifact シングル サインオンの動的アカウント リンクを有効化する

次の手順に従ってください:

1. linkaccount.jsp ファイルについては、以下の手順に従います。
   - （オプション）linkaccount.jsp ファイルをカスタマイズして、ユーザが認証の試行に失敗した後にリダイレクトされるときに、カスタム ユーザ操作性を提供します。 このファイルは、**accountlinking** パラメータおよび **samlresponse** パラメータをアサーション コンシューマ サービス URL に再度ポストする必要があります。

     注: accountlinking を［yes］（accountlinking=yes）に設定する必要があります。

     このファイルのデフォルトの場所は http://*sp_home*/affwebservices/public/ です。
   - SiteMinder フォーム認証方式（POST 保護をサポート）により linkaccount.jsp ファイルを保護します。ユーザがサービス プロバイダでローカルにログインした後、アサーションが含まれる SAML 応答がアサーション コンシューマ サービスにポストされます。ローカル認証処理の間ずっと、SAML 応答の POST データを保護します。

     認証方式によりリソースを保護するには、「ポリシー サーバ設定ガイド」の認証方式に関する情報を参照してください。
2. サービス プロバイダで許可/作成機能を有効にします。
3. サービス プロバイダの Web エージェントでは、［POST 保持］パラメータを「yes」に設定します。 この設定は、保護される SAML 応答の POST データを有効にします。
4. 認証が失敗した場合に linkaccount.jsp ファイルにユーザを送るリダイレクト URL を設定します。このファイルにのみユーザをリダイレクトします。

   リダイレクト URL は、サービス プロバイダの SAML 2.0 認証方式設定の一部です。

以下のフィールドに次の値を入力します。

ユーザが見つからなかった状態のためのリダイレクト URL

http://*sp_home*/*protected_realm*/linkaccount.jsp

例： http://smwidgets.com/partner_resources/linkaccount.jsp

linkaccount.jsp ファイルのデフォルトの場所は http://*sp_home*/affwebservices/public/ です。このディレクトリから保護されているレルムとして設定されるディレクトリにファイルをコピーします。

モード

HTTP POST

5. SAML 認証方式の検索仕様を設定します。 たとえば、アサーションの名前 ID が buyerID を置換すれば、検索仕様は buyerID=%s になります。

第 3 章: フェデレーション展開の考慮事項

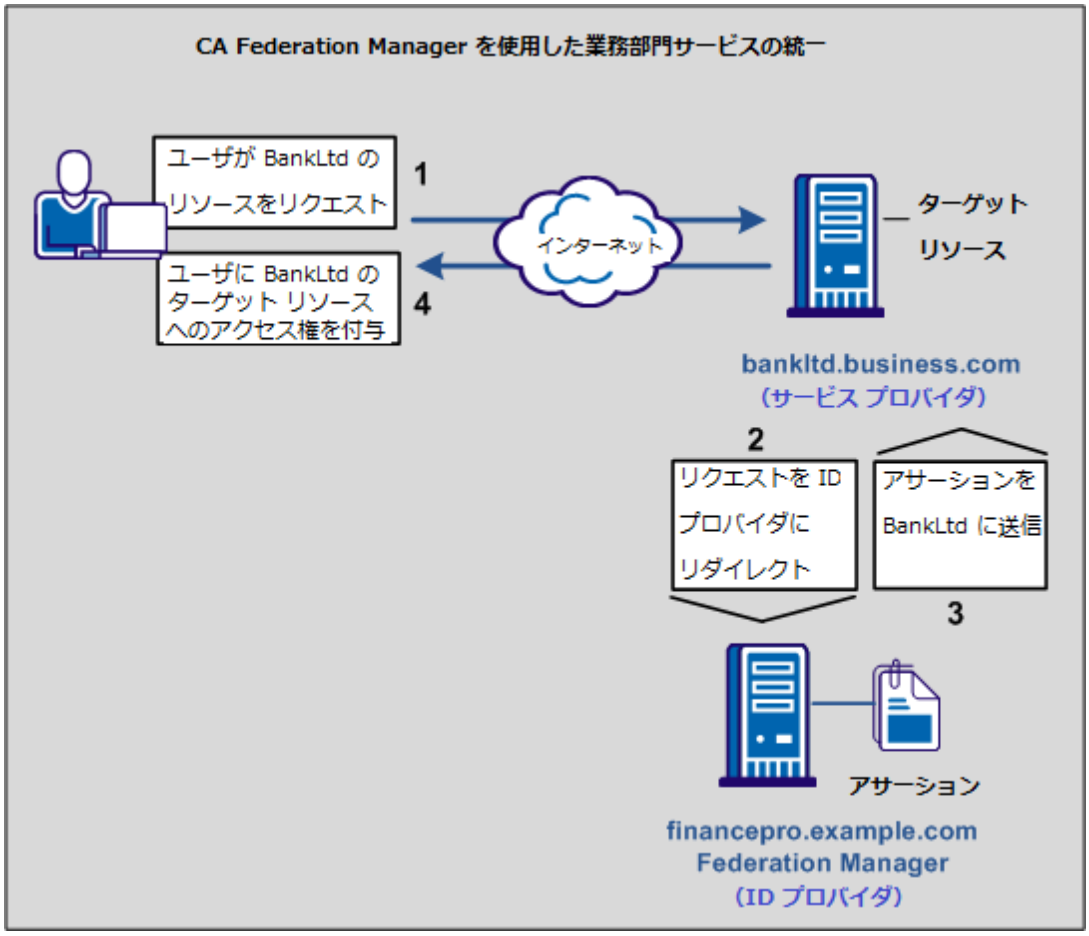
フェデレーション ビジネス ケース

サンプル ビジネス ケースは、一般的なビジネスの問題を CA SiteMinder® Federation が解決できる方法を最適に示します。

このビジネス ケースで、Financepro は、クライアントにプライベート バンキングを提供するために最近 BankLtd 銀行を買った投資コンサルタントです。 これらの 2 つの会社には異なる情報インフラがあります。しかし、これを顧客の目には 1 つの会社と映るようにしたいと考えています。この問題を解決するために、彼らはフェデレーション パートナーシップを築きました。

フェデレーション関係を確立することにより、2 つの会社はシングル サインオンを使用して、顧客にシームレスな操作性を提供できます。 顧客は何度も認証画面が表示されることなく、Financepro と BankLtd の間を行き来できます。 さらに、顧客 ID および顧客情報の共有はユーザの操作性をいっそうカスタマイズし、各パートナーの金融商品の販売促進を相乗的に行うことができます。

以下の図は、Financepro と BankLtd 間のフェデレーション パートナーシップを示しています。通信の流れは SAML 2.0 サービス プロバイダにより開始されるシングル サインオンに基づいています。



この図では、以下の情報の流れについて説明します。

1. ユーザが、BankLtd でフェデレーション リソースにアクセスしようとします。
2. このユーザは認証のために Financepro にリダイレクトされ、また、アサーションが生成されます。
3. アサーションは BankLtd に渡されます。
4. SAML HTTP-Artifact または HTTP-POST のいずれかに基づいてシングル サインオンが発生します。ユーザはターゲット リソースにアクセスします。

このパートナーシップが機能するには、フェデレーションを使用して関係を実装する前に、パートナーシップがどのように機能するかを決定します。

検討すべき問題には次のものがあります。

- ユーザがパートナーシップにおいて識別される方法。
- アサーションで送信する属性とその目的。
- 使用するフェデレーション バインディング（SAML POST または Artifact、WS-フェデレーション）。

ユーザの決定は、ビジネス パートナーシップの構築を支援します。

パートナーシップにおけるユーザ識別

取引先企業にはそれぞれのユーザ ストアでユーザ ID を定義する独自の方法があります。 ユーザがどのように識別されるかで、ある提携先が別の提携先にそのユーザをマップできる方法が決まります。

次のようなシナリオを考慮する必要があります。

- ユーザ ID が各サイトのユーザ ストアで同じである。

  アカウント リンクがユーザの識別法です。

- ユーザ ID が各サイトのユーザ ストアで一意である。

  ID マッピングがユーザの識別法です。 FinancePro で顧客は JohnDoe と識別されますが、BankLtd ではこの同じ顧客が DoeJ と識別されます。パートナーは、ID マッピングに使用するユーザ属性プロファイルに同意する必要があります。

- ユーザ ID が依存側に存在しない。

  アカウント プロビジョニングがユーザの識別法です。アカウントのプロビジョニングには、ユーザ アカウントの作成が必要な場合や、単純に既存のユーザ アカウントへ SAML アサーションの情報を入力することが必要な場合があります。

ユーザの識別法を決定することで、アサーションでどんな情報がユーザ ID として送信されるかが決まります。

ユーザ マッピング

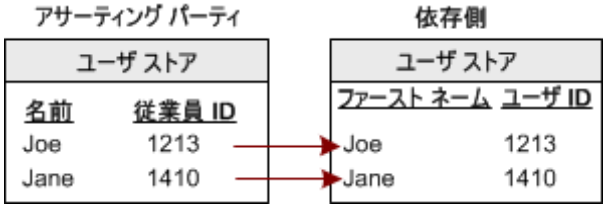
ユーザ マッピングは、ある企業でのユーザ ID と別の企業でのユーザ ID の関係を確立する機能です。 アサーティング パーティのリモート ユーザを依存パーティのローカル ユーザにマップします。

マッピングのタイプは次のとおりです。

- 1 対 1 マッピングは、生産権限の一意リモート ユーザ ディレクトリ エントリを、消費権限の一意のユーザ エントリにマップします。

  1 対 1 マッピング（アカウント リンク）は、アサーティング パーティのアカウントを依存パーティのアカウントにリンクします。

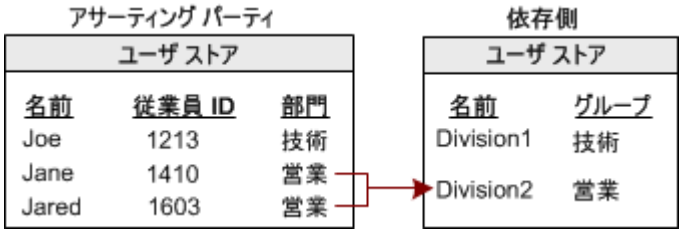
  次の図は、1 対 1 マッピングを示しています。



- N 対 1 マッピングは、リモート ユーザ ディレクトリ エントリのグループを単一のローカル プロファイル エントリにマップします。

  N 対 1 マッピングでは、生産権限の複数のユーザ レコードを、消費権限のユーザ レコードまたはプロファイルにマップできます。依存パーティの管理者は、各リモート ユーザのレコードをメンテナンスせずに、リモート ユーザのグループに対して N 対 1 マッピングを使用できます。

  次の図は、N 対 1 マッピングを示しています。



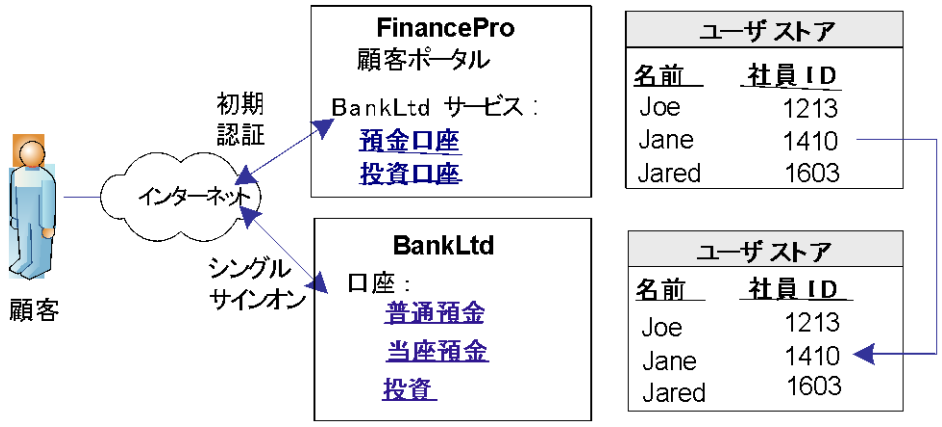
レガシー フェデレーション では、ユーザ マッピングがフェデレーション認証方式の一部として設定されています。 パートナーシップ フェデレーション では、ユーザ マッピングが名前 ID および属性設定の一部として設定されます。

フェデレーション ID を確立するアカウント リンク

FinancePro の顧客が BankLtd のリソースにアクセスする場合は、アサーションに必ず名前 ID があります。 この識別子によって、BankLtd はその顧客が誰か、また、その顧客に対して許可するアクセス レベルを決定できます。

各提携先のユーザ ストアが、同じ ID を使用する同じ方式でユーザを識別したときに、名前 ID はフェデレーション ID を確立できます。

次の図は同じ社員 ID を使用した各サイトのユーザ ストアを示しています。



CA SiteMinder® Federation では、パートナーシップ設定プロセスの一部としてアカウント リンクを設定できます。 ユーザは名前 ID の形式および名前 ID のタイプを指定します。これにより、名前を定義する値のタイプが決まります。特定の名前 ID タイプを、静的属性、ユーザ属性、またはユーザ ディレクトリの DN 属性と関連付けます。 CA SiteMinder® Federation によりアサーションに組み込まれる名前 ID は、ユーザが定義する設定に一致します。

依存パーティがアサーションを受信すると、BankLtd ではユーザの特定プロセスが発生します。 このプロセスは、アサーションの名前 ID 値をそのユーザ ストアのレコードにリンクします。

フェデレーション ID を確立する ID マッピング

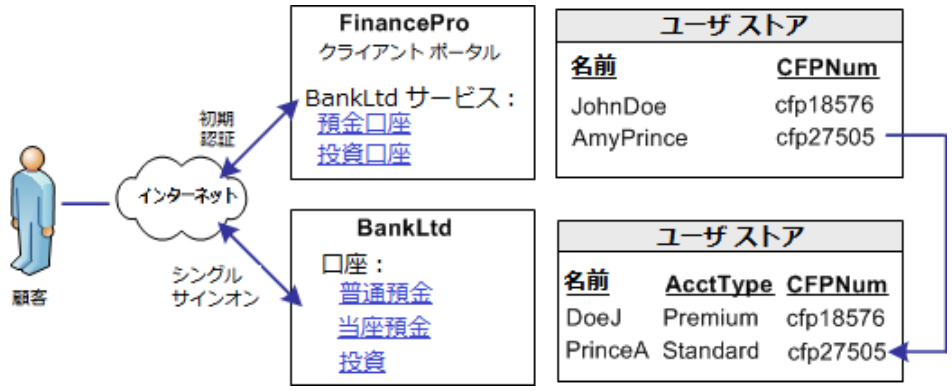
Financepro の投資者が認証を行い、BankLtd のアクセス情報へのリンクを選択します。この投資者はサインオンしなくても BankLtd Web サイトのアカウント領域に直接移動します。

BankLtd は、Financepro のすべての顧客に対してユーザ ID を保守しますが、BankLtd の ID は FinancePro での ID と異なります。たとえば、FinancePro では JohnDoe は顧客です。BankLtd では、この同じ顧客は DoeJ として識別されます。いずれにせよ、BankLtd は会社の Web サイトの機密部分に対するアクセスを制御する必要があります。 フェデレーション ID を確立するために、両社はどちらのサイトでも 1 人の顧客に対して適切な ID にマップする属性に合意します。

両社は、帯域外の情報交換中に使用する属性に関して合意します。これは、この合意がチャネルを介した任意のメッセージの任意の通信の一部ではないことを意味します。 この例の場合、両社が合意した属性は、公認投資コンサルタント認可番号（各ユーザ ストアの CFPNum）です。

顧客が BankLtd でフェデレーション リソースへのアクセスを試行すると、その要求がシングル サインオン プロセスのトリガになります。FinancePro で生成されるアサーションには CFPNum 属性が含まれます。 BankLtd がアサーションを受信するときに、そのサイトのアプリケーションはユーザ明確化プロセスを実行する必要があります。 どのプロファイル ID を要求に使用するかをプロセスが決定するのは、属性に依存します。

次の図は、同じユーザが各社でどのように違って識別されるかを示しています。



SiteMinder フェデレーションでは、パートナーシップ設定プロセスの一部として ID マッピングを設定できます。 名前 ID および属性の設定について、CFPID と呼ばれる属性を定義します。 この属性をユーザ属性 CFPNum （各社のユーザ ストアの属性の名前）と関連付けます。

SiteMinder Federation はアサーションに属性を組み込みます。BankLtd がアサーションを受信すると、ユーザ明確化プロセスはアサーションの属性をそのユーザ ストアの適切なレコードにリンクします。

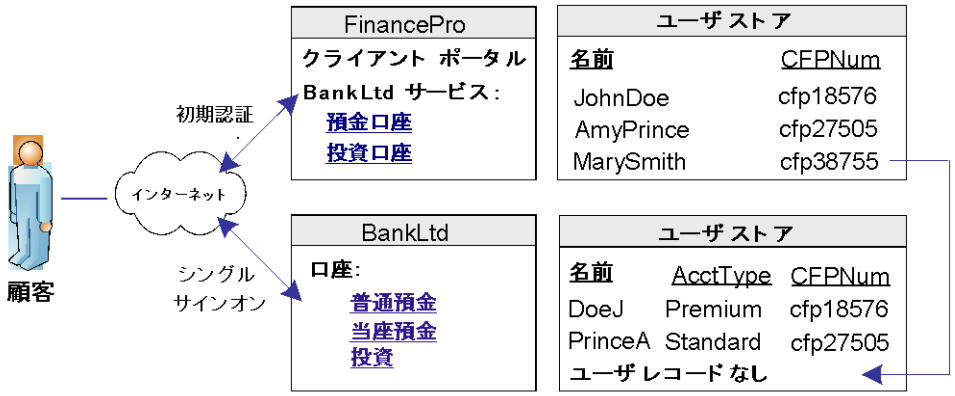
フェデレーション ID を確立するためのユーザ プロビジョニング（パートナーシップ フェデレーション のみ）

パートナーシップ フェデレーションは ID を確立するために依存パーティでプロビジョニング アプリケーションと連携できます。

Financepro のクライアント、メアリー スミスが認証を行い、リンクをクリックして BankLtd の情報にアクセスします。最初、BankLtd ではメアリー スミスのユーザ アカウントが見つかりません。 BankLtd は、新しい顧客を許可する一方で、Web サイトの機密部分は保護したいと考えます。

BankLtd は、メアリー スミスの新しいフェデレーション ID を確立するプロビジョニングを実装するようにフェデレーションを設定しました。SiteMinder は BankLtd のプロビジョニング サーバにメアリー スミスをリダイレクトします。プロビジョニング アプリケーションは、フェデレーション ID 情報を使用して、ユーザ ストアにユーザ アカウントを作成します。

次の図は、FinancePro と BankLtd のユーザ ストアを示しています。



フェデレーションでは、依存パーティでパートナーシップ設定の一部としてプロビジョニングを設定できます。 この例で、ユーザはリモート プロビジョニングを選択し、アサーション データを BankLtd のプロビジョニング サーバに届ける方法を決定します。 この設定により、ユーザ ストアでユーザ エントリを動的に作成できるようになります。

アプリケーションをカスタマイズするための属性

CA SiteMinder® Federation は、ターゲット アプリケーションをカスタマイズするために属性を使用する 2 つの方法を提供しています。

アサーティング パーティのアサーションに追加された属性

アプリケーションをカスタマイズする目的でユーザを識別するために、アサーションにユーザ ストア レコードの属性を含めることができます。

サーブレット、Web アプリケーションおよび他のカスタム アプリケーションは、カスタマイズされたコンテンツを表示したり、他のカスタム機能を有効あるいは無効にするために、属性を使用できます。 属性を Web アプリケーションと共に使用すると、ターゲット サイトでのユーザ アクティビティを制限することにより、きめの細かいアクセス制御を実装できます。 たとえば、Account Balance という名前の属性変数を送信し、これに、BankLtd のユーザの口座保有高を反映させるように設定します。

属性の形式は、名前/値のペアになっています。依存パーティはアサーションを受け取ると、その属性値をアプリケーションで使用できるようにします。

依存パーティでの属性マッピング

依存パーティは一連のアサーション属性を受信します。この属性を、ターゲット アプリケーションに配信される一連のアプリケーション属性にマップできます。

たとえば、FinancePro にはアサーション属性 CellNo=5555555555 が含まれます。 BankLtd で、この属性名がアプリケーション属性 Mobile=5555555555 に変換されます。 属性名は変換されますが、値は同じままです。

複数のアサーション属性も単一のアプリケーション属性に変換できます。たとえば、FinancePro は、属性 Acct=Savings および Type=Retirement を持つ受信アサーションを送信し、BankLtd で FundType= Retirement Savings へ変換しました。

シングル サインオンのフェデレーション プロファイル

SAML または WS フェデレーションをパートナーシップに使用するかどうかの判断は、それぞれの側がサポートするバインディングによって異なります。

新しい連携では、どちらの会社にもレガシー要件がありません。したがって、シングル サインオンに使用する推奨 SAML プロファイルは、SAML 2.0 POST プロファイルです。 SAML 2.0 POST プロファイルは、アサーション データの安全な転送を提供します。また、設定プロセスは SAML Artifact プロファイルより単純です。 ただし、2 社間の契約により SAML Artifact が必要な場合は、このバインディングも実装できます。

展開には、Active Directory フェデレーション サービス (ADFS) を使用して、WS フェデレーションを設定します。

各 CA SiteMinder® Federation モデルとの連携

レガシー フェデレーション または パートナーシップ フェデレーション モデルでは、Financepro と BankLtd の間のフェデレーション パートナーシップを確立できます。フェデレーションを使用して、ユーザは各社の間を、それらが 1 つの会社であるかのように移動します。

パートナーシップ フェデレーション モデル

パートナーシップ ウィザードに従って、管理 UI にパートナーシップ モデルを設定します。 パートナーシップ オブジェクトは、シングル サインオンを実行するために、パートナーシップの作成およびパートナーシップの両関係者を識別することに焦点を当てます。

パートナーシップ ウィザードのこれらの手順には以下のものが含まれます。

1. パートナーシップの設定

   パートナーシップに名前を付け、そのパートナーシップを構成する 2 つのエンティティを識別します。

2. フェデレーション ユーザ/ユーザ ID の確立

   アサーティング パーティがアサーション/トークンを生成し、依存パーティが認証するユーザを識別します。

3. 名前 ID と属性

   フェデレーション ID を確立する方法を決定し、識別する属性の追加とアサーション内容のカスタマイズを可能にします。

   名前 ID と属性を使用すると、依存パーティで適切な情報がアプリケーションに利用可能かどうかを確認できます。名前 ID と属性は、アカウント リンクおよび ID マッピングを設定する段階で使用されます。

4. SSO と SLO またはサインアウト

   依存パーティでアサーションを消費するサービスの場所を含む、シングル サインオン バインディングを定義します。SAML 2.0 については、シングル ログアウト（SLO）、認証コンテキスト、機能強化クライアントまたはプロキシ（ECP）プロファイル、およびアイデンティティ プロバイダ ディスカバリ プロファイルなどの追加機能を設定できます。WS-フェデレーションでは、サインアウトを設定できます。

5. AuthnContext （SAML 2.0 のみ）

   サービス プロバイダを有効にして、認証プロセスに関する情報を取得し、信頼性を確立します。 また、この機能は、アサーションに認証コンテキストを含めるためにアイデンティティ プロバイダも有効にします。

6. 署名と暗号化

   安全なデータ交換のための署名および暗号化オプションを定義します。以下のものがあります。

   - アサーション
   - 認証リクエスト
   - SAML 2.0 シングル ログアウト要求および応答
   - WS-フェデレーション サインアウト レスポンス。

7. アプリケーション統合

   ユーザによるターゲット アプリケーションへのリダイレクト設定を可能にし、ユーザ レコードのプロビジョニング設定と依存パーティの属性マッピングの定義ができるようにします。 また、ユーザ認証失敗時のリダイレクトを設定できます。

レガシー フェデレーション モデル

レガシー フェデレーション モデルは、ドメイン、レルム、ルール、認証方式、およびポリシー オブジェクトに焦点を当てています。

SiteMinder がアサーティング パーティである場合、設定手順には次のものが含まれます。

1. アフィリエイト ドメインのエンティティの設定

   アサーティング パーティがアサーションを生成するパートナーを指名します。

2. フェデレーション ユーザの確立

   アサーティング パーティがアサーションを生成し、依存パーティが認証するユーザ ディレクトリを指定します。

3. トランザクション用のプロファイル（SAML または WS-フェデレーション）の選択

   フェデレーション ID がどのように確立されるかを決定します。 プロファイルの設定では、アサーションのコンテンツを識別しカスタマイズするために属性を追加します。

   名前 ID と属性を使用すると、依存パーティで適切な情報がアプリケーションに利用可能かどうかを確認できます。 プロファイル設定は、アカウント リンクおよび ID マッピングを指定する場所です。

   プロファイルの一部として、シングル サインオンを設定します。SAML 2.0 については、シングル ログアウト（SLO）、機能強化クライアントまたはプロキシ（ECP）プロファイル、およびアイデンティティ プロバイダ ディスカバリ プロファイルなどの追加機能を設定できます。WS-フェデレーションでは、サインアウトを設定できます。

4. 署名処理および暗号化（SAML 2.0）

   アサーション、認証リクエスト、およびシングル ログアウト リクエストとレスポンスの安全な交換のための署名オプションを定義します。

SiteMinder が依存パーティである場合、設定手順には次のものが含まれます。

1. SAML および WS-フェデレーション認証方式の設定

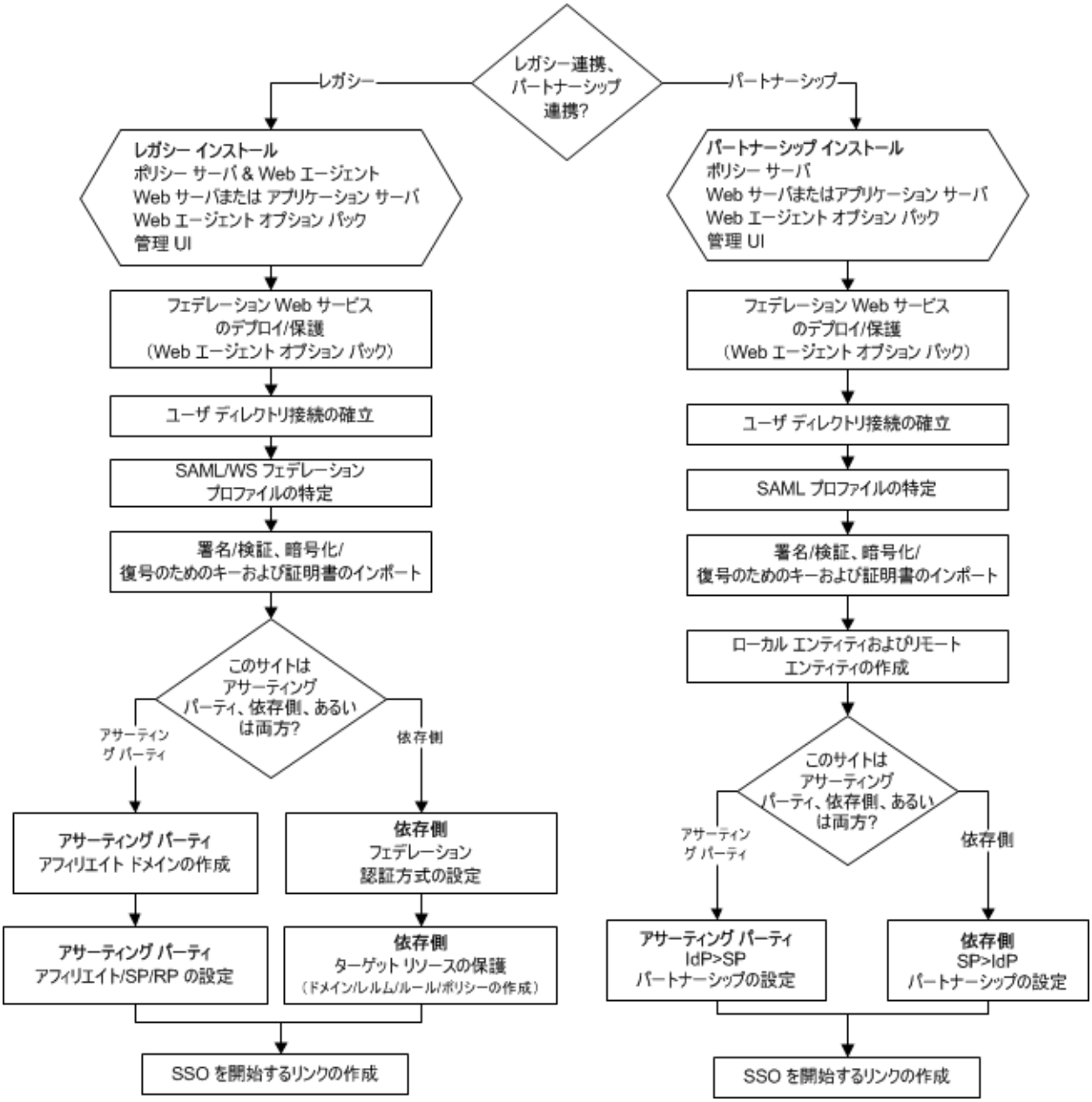
   ユーザによるターゲット アプリケーションへのリダイレクト設定を可能にし、ユーザ レコードのプロビジョニング設定と依存パーティの属性マッピングの定義ができるようにします。

2. 認証方式に含まれる、フェデレーション固有の設定（シングル サインオン、シングル ログアウト、サインアウト、暗号化、および復号化）の設定。

フェデレーションのフローチャート

フェデレーション パートナーシップを正常に確立するためにコンポーネントを設定します。 これらのコンポーネントのほとんどは 管理 UI を使用して設定可能です。

以下のフローチャートは、レガシー フェデレーション および パートナーシップ フェデレーション の一般的なプロセスに焦点を当てています。



必要なコンポーネントおよび設定手順上の詳細については、以下のガイドを参照してください：

パートナーシップ フェデレーション

パートナーシップ フェデレーション ガイド

パートナーシップ フェデレーションとは、フェデレーションのパートナーシップ モデルのことです。

レガシー フェデレーション

レガシー フェデレーション ガイド

レガシー フェデレーションは、Federation Security Services という製品を参照します

第 4 章: シングル サインオンについてのフェデレーションと Web アクセス管理の比較

フェデレーションと Web アクセス管理の利点

フェデレーションおよび Web アクセス管理（WAM）は、シングル サインオンに対して異なる利点を提供します。 フェデレーション シングル サインオンまたは WAM シングル サインオンをいつ使用するかの決定は、ユーザ側の展開に左右されます。

フェデレーションでは、ユーザが WAM 機能上で展開でき、機能を置き換えることはありません。

フェデレーションには次の長所があります。

- SAP、SharePoint、WebLogic など多くのアプリケーションでは、すぐにフェデレーションを直接処理できます。 これらのアプリケーションはアサーションを受け入れます。
- 中央サーバへの直接接続が不要です。 フェデレーション要求は生成されたアサーションを取得するために、必ずアサーティング パーティを通過します。 ユーザは 1 つのサーバ上のコンテンツへのアクセスを取得した後、フェデレーション ハブに戻り、次のサーバにリダイレクトされます。ハブでユーザ セッションがタイムアウトになった場合にのみ、再認証が必要です。
- SiteMinder フェデレーションには 2 つのモデルがあります。 パートナーシップ フェデレーションは取引先との関係に重点を置いた、ビジネス中心のモデルです。レガシー フェデレーションはプロトコル中心で、プロトコル仕様をよりカスタマイズできます。

これらの利点により、パートナーシップ フェデレーションは、各サイトがリモート環境であったり、アクセス不能であったり、または第三者の管理下に置かれている環境に、より適したものになっています。

SiteMinder WAM シングル サインオンには次の長所があります。

- ブラウザのリダイレクトが少ない分、トランザクションはより速くなります。
- SiteMinder は一元化された権限および監査を提供します。
- アサーション生成のためにユーザに一元化されたハブを通過させることなく、ネットワーク内のある Web サーバから別の Web サーバに直接のリンクが存在できます。
- SiteMinder はタイムアウト管理を提供します。
- アプリケーションはリモートで開始されたトランザクションに依存しません。

これらの利点により、WAM シングル サインオンは社内のデータ センターなど、ユーザの管理下に置かれたサイトのある環境に、より適したものになっています。

フェデレーションを好む展開

フェデレーションは会社がサーバを制御しないネットワークで有利です。たとえば、サードパーティは Web サーバを所有し、ユーザが Web エージェントをサーバにインストールすることを許可しません。 また、Web エージェントとポリシー サーバ間に高いネットワーク遅延がある場所に、リモート サーバが置かれる場合があります。 ユーザがターゲット サーバに対するコントロールを持っていない場合、SAML アサーションは ID 情報を渡す理想的な方法です。

フェデレーション ネットワークのパートナーは、通信で使用されるプロトコルについて特定の基準に従います。この共通基準により、アサーションの生成と消費が共通化されます。 その結果、アサーティング パーティのベンダーであるか依存パーティのベンダーであるかはもとより、各ベンダーの場所がリモート ロケーションであるかどうかも重要でなくなります。

タイムアウトが主な関心事ではなく、ID 情報取得が目標である場合、最終的にフェデレーションが優れたソリューションとなります。 外部の権限チェックはフェデレーションの目的ではありません。

Web アクセス管理を好む展開

WAM シングル サインオンは、ユーザが各 Web サイトに対するコントロールを持っている環境で最適に機能します。 Web サイトまたは他の社内シングル サインオン環境と同じデータ センターの中に SiteMinder があることは、Web アクセス管理に適した展開です。 また、各 Web サイトの制御は、ネットワーク パフォーマンスの監査とタイムアウト問題のモニタリングにとっても重要です。

WAM シングル サインオンでは、WAM セッション経由でアプリケーションと統合できます。 また、WAM 実装環境では、フェデレーション固有のパフォーマンス問題の一部が軽減されます。 たとえば、ユーザが要求を出すためにリンクを選択した後、アサーティング パーティによって開始されるトランザクションはいくつかのリダイレクトを必要とする場合があります。

第 5 章: フェデレーション Web サービス

フェデレーション Web サービスの概要

フェデレーション Web サービス（FWS）アプリケーションは、ポリシー サーバへの接続をしているサーバに、Web エージェント オプション パックと共にインストールされます。 フェデレーション Web サービスおよび Web エージェントは、以下の Web ブラウザ シングル サインオン プロファイルをサポートしています。 これらのプロファイルは標準的なブラウザを介して、あるサイトから別のサイトに情報を伝えます。

サポートされているプロファイルは以下のとおりです。

- SAML Artifact プロファイル 1.0 （レガシー フェデレーション のみ）
- SAML Artifact プロファイル 1.1 および 2.0（レガシー フェデレーション および パートナーシップ フェデレーション）
- SAML POST Artifact 1.x および 2.0 （レガシー フェデレーション および パートナーシップ フェデレーション）
- WS-フェデレーション パッシブ リクエスタ プロファイル（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）

SAML 1.x Artifact および POST プロファイル

SAML 1.x Artifact および POST プロファイルの場合、フェデレーション Web サービス アプリケーションは次のサービスを使用します。

アサーション取得サービス（SAML 1.x Artifact のみ）

プロデューサ側コンポーネント。このサービスは、SiteMinder セッション ストアからアサーションを取得することにより SAML Artifact に相当するアサーションの SAML リクエストを処理します。 SAML 仕様は、アサーション取得リクエストおよびレスポンス動作を定義します。

注: SAML Artifact プロファイルのみがアサーション取得サービスを使用します。

SAML 認証情報コレクタ（SAML 1.x）

埋め込み SAML 応答により SAML Artifact または HTTP フォームを受信し、対応する SAML アサーションを取得する、コンシューマ側コンポーネント。 認証情報コレクタは、ユーザのブラウザへ SiteMinder Cookie を発行します。

サイト間転送サービス（SAML 1.x）

SAML POST プロファイル用のプロデューサ側コンポーネント。 サイト間転送サービスはプロデューサ サイトからコンシューマ サイトにユーザを転送します。 SAML Artifact プロファイルの場合は、Web エージェントがサイト間転送サービスと同じ機能を実行します。

SAML 2.0.x Artifact および POST プロファイル

SAML 2.0.x Artifact および POST プロファイルの場合、フェデレーション Web サービス アプリケーションは次のサービスを使用します。

Artifact **解決サービス**（SAML 2.0 Artifact **のみ**）

HTTP Artifact バインディングを使用した、SAML 2.0 認証に相当するアイデンティティ プロバイダ側のサービス。 このサービスは、アイデンティティ プロバイダの SiteMinder セッション ストアに格納されたアサーションを取得します。

注: HTTP Artifact バインディングのみが Artifact 決サービスを使用します。

アサーション コンシューマ サービス（SAML 2.0）

SAML Artifact または埋め込み SAML レスポンスを含む HTTP フォームを受信し、対応する SAML アサーションを取得する サービス プロバイダ コンポーネント。 アサーション コンシューマ サービスは、ブラウザに対して SiteMinder cookie を発行します。

注: アサーション コンシューマ サービスは、0 の AssertionConsumerServiceIndex 値を持つ AuthnRequest を受け入れます。この設定の他のすべての値は拒否されます。

認証リクエスト サービス（SAML 2.0）

このサービスは SAML 2.0 が使用するために展開されます。 サービス プロバイダは、クロスドメイン シングル サインオンのためにユーザを認証する <AuthnRequest> メッセージを生成できます。このメッセージには、アイデンティティ プロバイダで、フェデレーション Web サービス アプリケーションがシングル サインオン サービスにブラウザをリダイレクトできるようにする情報が含まれます。 AuthnRequest サービスは POST および Artifact シングル サインオンに使用されます。

シングル サインオン サービス（SAML 2.0）

シングル サインオン サービスは、アイデンティティ プロバイダが AuthnRequest メッセージを処理できるようにします。 また、このサービスはアサーション生成プログラムを呼び出し、サービス プロバイダに送信するアサーションを作成します。

シングル ログアウト サービス（SAML 2.0）

このサービスは、シングル ログアウト機能の処理を実行します。この機能はアイデンティティ プロバイダまたはサービス プロバイダが開始できます。

アイデンティティ プロバイダ ディスカバリ サービス（SAML 2.0）

SAML 2.0 アイデンティティ プロバイダ ディスカバリ プロファイルを実装し、共通ドメイン cookie を設定し、取得します。 IdP は、プリンシパルを認証した後に共通ドメイン cookie の設定を要求します。SP は、プリンシパルがどのアイデンティティ プロバイダを使用しているかを検出するために、共通ドメイン cookie の取得を要求します。

WS-フェデレーション プロファイル

WS-フェデレーション プロファイルの場合、フェデレーション Web サービス アプリケーションは以下のサービスを使用します。

セキュリティトークン コンシューマ サービス

セキュリティ トークンを受信し、対応する SAML アサーションを抽出するリソース パートナー コンポーネント。 セキュリティ トークン コンシューマ サービスは、ブラウザに対して Cookie を発行します。

シングル サインオン サービス

アイデンティティ プロバイダがユーザを認証するために、サインオン メッセージを処理し、必要なリソース パートナー情報を収集できるようにします。 また、このサービスはアサーション生成プログラムを呼び出し、リソース パートナーに送信するアサーションを作成します。

サインアウト サービス

サインアウト サーブレット経由でシングル サインアウト トランザクションの処理を実装します。 アイデンティティ プロバイダまたはリソース パートナーが、サインアウトを開始できます。

第 6 章: フェデレーション トランザクション プロセス フロー

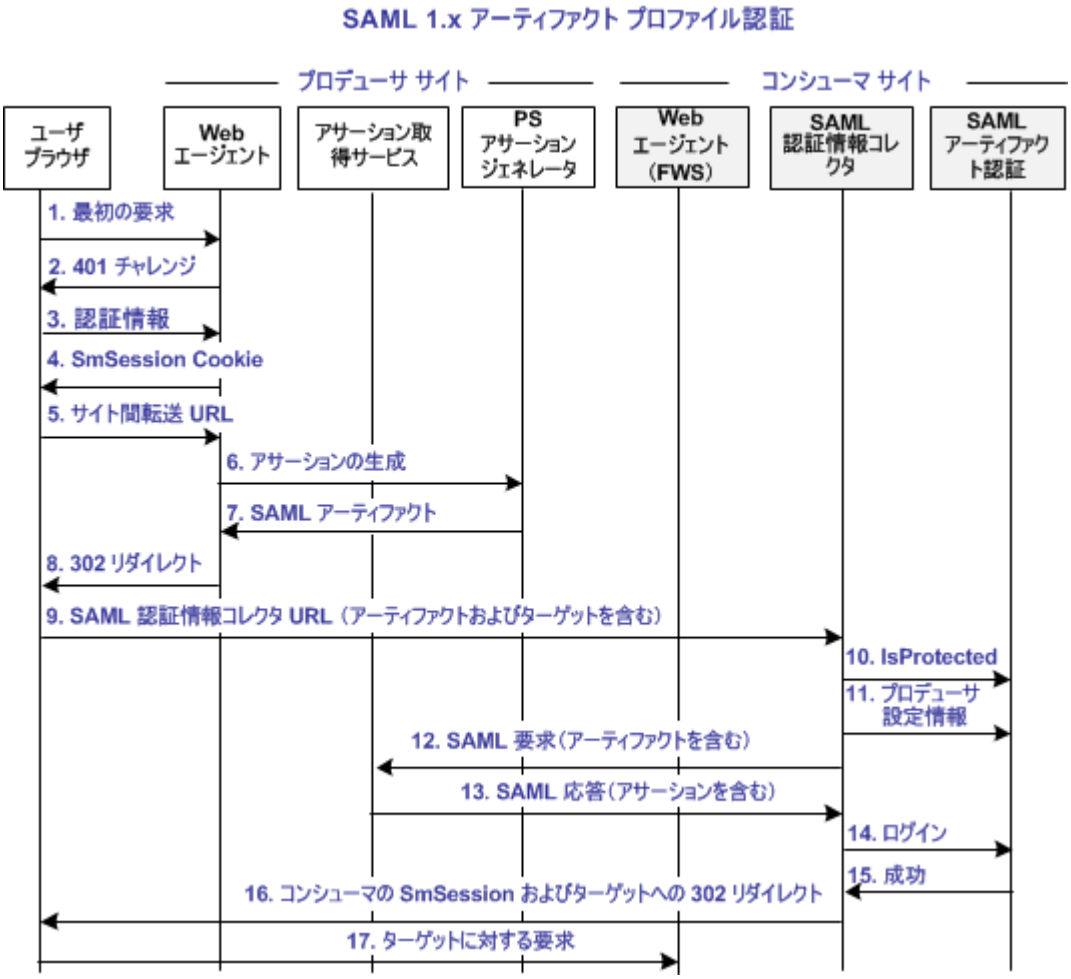
SAML 1.x Artifact SSO トランザクション フロー（プロデューサで開始された）

以下の図は、プロデューサ サイトおよびコンシューマ サイトでのユーザとフェデレーション コンポーネント間のフローを示しています。 このフローでは、SAML アサーションを処理する方法として SAML 1.x Artifact プロファイルを使用したサイト間のシングル サインオンを示します。

このフローチャートでは以下の情報を想定しています。

- プロデューサはトランザクションを開始します。
- 各サイトで認証および許可が正常に行われます。
- 各パートナーでプロセスを参照できるように、SiteMinder はプロデューサおよびコンシューマのみとして表示されます。 SiteMinder が環境内のプロデューサである場合は、テーブル内のプロデューサ アクティビティを確認します。 SiteMinder がコンシューマである場合は、テーブル内のコンシューマ アクティビティを確認します。

以下の図は、SAML 1.x Artifact SSO トランザクション フローを示しています。



注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 フロー図では、Web エージェント ブロックは SPS フェデレーション ゲートウェイに組み込まれた Web エージェントになります。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

イベント シーケンスを以下に示します。

アクター	トランザクション プロセス
ユーザ エージェント（ブラウザ）	1. ユーザが、プロデューサ サイトの保護されているページに対して最初のリクエストを行います。
プロデューサとしての **SiteMinder**	2. プロデューサ サイトの Web エージェントは、ユーザの認証情報に対して 401 チャレンジで応答します。
	3. ユーザは、Web エージェントへユーザ名やパスワードなどの認証情報をサブミットします。
	4. Web エージェントは、プロデューサ サイト ドメインに対して SMSESSION Cookie をブラウザに発行し、ローカル ページへのアクセスを許可します。 **ログ メッセージ：** Session cookie does not exist, redirecting to authentication url. **チェックポイント コード：** [SSOSAML11_AUTHENTICATIONURL_REDIRECT]
	5. ユーザは、コンシューマ サイトにアクセスするためにローカル ページ上でリンクをクリックします。このリンクは、サイト間の転送 URL です。 サイト間転送 URL は、プロデューサ サイトで Web エージェントにリクエストを出します。 Web エージェントは、IsProtected コールをポリシー サーバに転送します。この URL には、SAML 認証情報コレクタの場所と、コンシューマ サイトのターゲット URL が含まれています。 **ログ メッセージ：** SAML11 Consumer Configuration is not in cache. Requesting to get from policy server. **チェックポイント コード：** [SSOSAML11_CONSUMERCONFFROMPS_REQ]
	6. Web エージェントは、アサーションを生成するためにポリシー サーバにリクエストします。 **ログ メッセージ：** Request to policy server for generating saml11 assertion/artifact based on selected profile. **チェックポイント コード：** [SSOSAML11_GENERATEASSERTIONORARTIFACT_REQ]

アクター	トランザクション プロセス
	7. ポリシー サーバは、アサーションを生成し、セッション ストアにそれを配置し、アサーションに対して SAML Artifact を返します。 ログ メッセージ： Policy server generates the saml11 assertion. チェックポイント コード： [SSOSAML11_PSGENERATEASSERTION_RSP] ログ メッセージ： Policy server stores the assertion in session store チェックポイント コード： [SSOSAML11_PSSTOREASSERTIONINSSTORE_REQ] ログ メッセージ: Policy server returns the wrappedassertion/artifact(based on profile selected) in response message チェックポイント コード： [SSO_PSWRAPPEDASSERTION_RSP]
	8. Web エージェントが、コンシューマ側の SAML 認証情報コレクタへ 302 リダイレクトで応答します。リダイレクトには、Artifact およびターゲット URL がクエリ パラメータとして含まれています。 ログ メッセージ： Sending artifact to credential collector service url. チェックポイント コード： [SSOSAML11_SENDARTIFACTTOCONSUMERURL_RSP]
ユーザ エージェント（ブラウザ）	9. ブラウザがコンシューマ サイトの SAML 認証情報コレクタの URL にリクエストを出します。
コンシューマとしての **SiteMinder**	10. SAML 認証情報コレクタは、プロデューサに関する情報についてポリシー サーバに対する isProtected コールを作成します。 ログ メッセージ： IsProtected call to policy server for producer configuration チェックポイント コード： SSOSAML11_ISPROTECTEDCALLTOGETPRODUCERCONF_REQ
	11. ポリシー サーバは、プロデューサ設定情報を返します。
	12. SAML 認証情報コレクタは、プロデューサ設定情報を使用して、プロデューサ側のアサーション取得サービスに対する SAML リクエストを行います。 ログ メッセージ： Reading producer configuration from property. チェックポイント コード： SSOSAML11_GETPRODUCERCONFFROMPROPERTY_REQ ログ メッセージ： Backchannel call to resolve the artifact チェックポイント コード： [SSOSAML11_RESOLVEARTIFACT_REQ]

アクター	トランザクション プロセス
プロデューサとしての **SiteMinder**	13. プロデューサのアサーション取得サービスが、セッション ストアから SAML アサーションを取得します。 サービスは、SAML アサーションが含まれる SAML 応答で応答します。アサーションはコンシューマに送信されます。 **ログ メッセージ：** Retrieving assertion from session store **チェックポイント コード：** [SSOSAML11_RETREIVEASSERTIIONFROMSSTORE_REQ] **ログ メッセージ：** Received the assertion from session store. **チェックポイント コード：** [SSOSAML11_RECEIVEDASSERTIONFROMSSTORE_RSP] **ログ メッセージ：** Sending assertion as artifact response. **チェックポイント コード：** SSOSAML11_SENDARTIFACTRESPONSE_RSP
コンシューマとしての **SiteMinder**	14. SAML 認証情報コレクタは、ポリシー サーバにログイン コールを送信し、SAML アサーションを認証情報として渡します。 **ログ メッセージ：** Obtained the SAML11 assertion as response from artifact resolve call **チェックポイント コード：** [SSOSAML11_GOTARTIFACTRESPONSE_RSP] **ログ メッセージ：** Passing response message through login call **チェックポイント コード：** [SSO_RESPONSEMESSAGEINLOGIN_REQ]
	15. コンシューマはアサーションを検証します。ユーザはユーザ レコード内で検索されます。 ポリシー サーバは成功を返答します。 **ログ メッセージ：** Login successful **チェックポイント コード：** [SSO_LOGINSUCEESS_RSP] SAML アサーションが有効でない場合、またはユーザ レコードが見つからない場合、失敗の返答が返されます。 **ログ メッセージ：** Login failure. **チェックポイント コード：** [SSO_LOGINFAILURE_RSP]

アクター	トランザクション プロセス
コンシューマとしての **SiteMinder**（続き）	16. 成功返答が返された場合、SAML 認証情報コレクタはブラウザに対してコンシューマ ドメインの SMSESSION Cookie を発行します。 また、SAML 認証情報コレクタは、ターゲット URL への 302 リダイレクトを発行します。 **ログ メッセージ：** Creating the smsession cookie for SP domain. **チェックポイント コード：** [SSO_SMSESSIONFORSPDOMAIN_REQ] **ログ メッセージ：** Placing smsession in browser. **チェックポイント コード：** [SSO_PLACESMSSESSIONTOBROWSER_REQ] 失敗返答が返された場合、SAML 認証情報コレクタは 302 リダイレクトを非アクセス URL に対して発行します。
ユーザ エージェント（ブラウザ）	17. ブラウザは Web エージェントが保護しているコンシューマ サイトのターゲット URL にリクエストを出します。

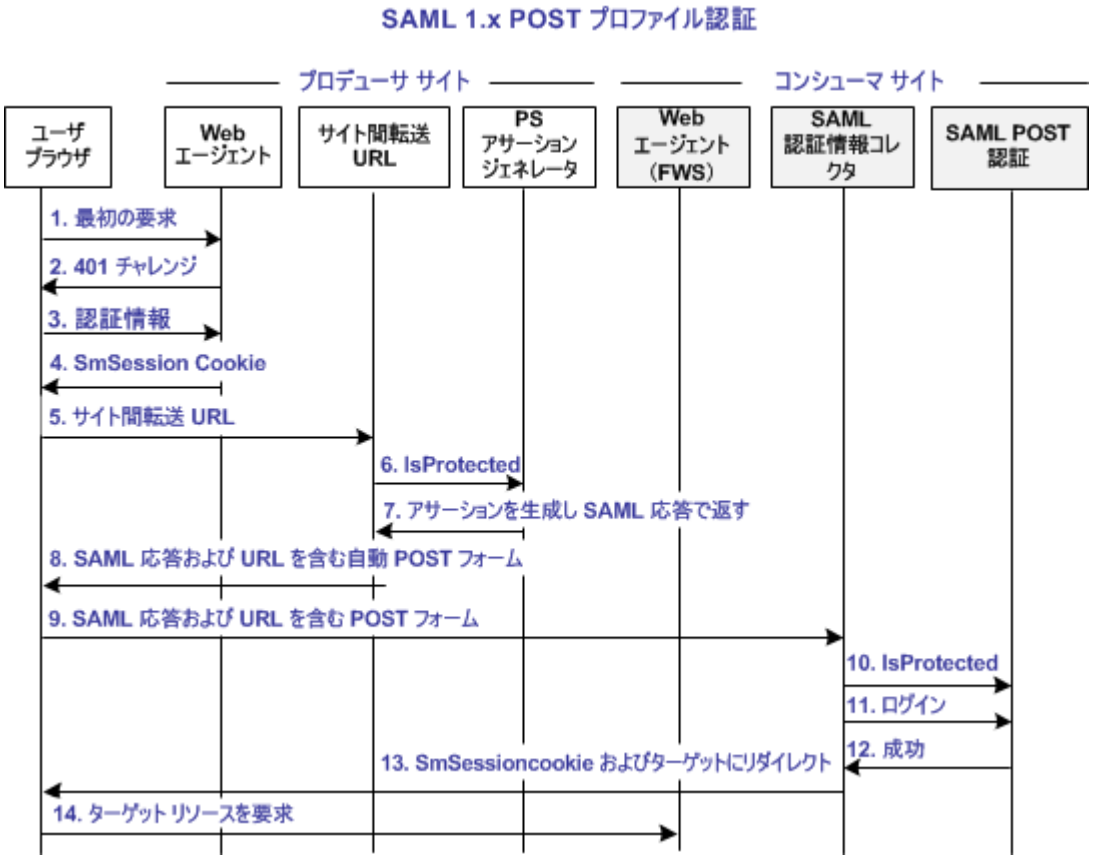
SAML 1.x POST SSO トランザクション フロー（プロデューサで開始された）

以下の図は、プロデューサ サイトおよびコンシューマ サイトでのユーザとフェデレーション コンポーネント間のフローを示しています。 このフローでは、SAML アサーションを処理する方法として SAML 1.x Artifact プロファイルを使用したサイト間のシングル サインオンを示します。

このフローチャートでは以下の情報を想定しています。

- プロデューサはトランザクションを開始します。
- 各サイトで認証および許可が正常に行われます。
- 各パートナーでプロセスを参照できるように、SiteMinder はプロデューサおよびコンシューマのみとして表示されます。 SiteMinder が環境内のプロデューサである場合は、テーブル内のプロデューサ アクティビティを確認します。 SiteMinder がコンシューマである場合は、テーブル内のコンシューマ アクティビティを確認します。

SAML 1.x POST プロファイルのプロセス フローチャートは次のようになります。



注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 フロー図では、Web エージェント ブロックは SPS フェデレーション ゲートウェイに組み込まれた Web エージェントになります。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

イベント シーケンスを以下に示します。

アクター	トランザクション プロセス
ユーザ エージェント（ブラウザ）	1. ユーザが、プロデューサ サイトの保護されているページに対して最初のリクエストを行います。

アクター	トランザクション プロセス
プロデューサとしての **SiteMinder**	2. プロデューサ サイトの Web エージェントは、ユーザの認証情報に対して 401 チャレンジで応答します。 **ログ メッセージ**： SMSESSION cookie does not exist, redirecting to Authentication URL. **チェックポイント コード**： [REDIRECT_AUTH_URL]
	3. ユーザは、Web エージェントへユーザ名やパスワードなどの認証情報をサブミットします。
	4. Web エージェントは、プロデューサ サイト ドメインに対して SMSESSION Cookie をブラウザに発行し、ローカル ページへのアクセスを許可します。
	5. ユーザは、コンシューマ サイトにアクセスするためにローカル ページ上でリンクをクリックします。 このリンクは、サイト間の転送 URL です。これによりユーザを別のサイトに転送します。サイト間転送 URL は、プロデューサ サイトで Web エージェントにリクエストを出します。 この URL には、コンシューマの名前、SAML 認証情報コレクタの場所、コンシューマ サイトのターゲット URL についてクエリ パラメータが含まれています。 **ログ メッセージ**： SAML11 Consumer Configuration is not in cache. Requesting to get from policy server. **チェックポイント コード**： [SSOSAML11_CONSUMERCONFFROMPS_REQ]
	6. サイト間転送サービスは、ポリシー サーバに対して、リソースの IsProtected コールを行います。 この URL には、一意にコンシューマを識別する名前クエリ パラメータが含まれます。 **ログ メッセージ**： Request to policy server for generating saml11 assertion/artifact based on selected profile. **チェックポイント コード**： [SSOSAML11_GENERATEASSERTIONORARTIFACT_REQ]
	7. ポリシー サーバは、アサーションを生成し、デジタル署名された SAML レスポンス メッセージで返します。 その後、ポリシー サーバは、サイト間転送 URL に対して応答を返します。 **ログ メッセージ**： Policy server generates the saml11 assertion. **チェックポイント コード**： [SSOSAML11_PSGENERATEASSERTION_RSP]

アクター	トランザクション プロセス
	8. サイト間転送 URL サービスは、フォーム変数としてエンコードされた SAML 応答とターゲット URL が含まれる、Auto-POST フォームを生成します。 サービスがブラウザにフォームを送信します。 **ログ メッセージ：** Adding response in form for HTTP post. **チェックポイント コード：** [FWSBASE_POSTDATAFORM_ADD]
ユーザ エージェント（ブラウザ）	9. ブラウザは HTML フォームをコンシューマ サイトの SAML 認証情報コレクタにポストします。 この URL は、サイト間の転送 URL サービスが送信した SAML 応答から読み取られます。
コンシューマとしての **SiteMinder**	10. SAML 認証情報コレクタは、ポリシー サーバに対して isProtected をコールします。 **ログ メッセージ：** IsProtected call to policy server for producer configuration. **チェックポイント コード：** SSOSAML11_ISPROTECTEDCALLTOGETPRODUCERCONF_REQ
	11. SAML 認証情報コレクタは、リクエストされたターゲット リソースについてポリシー サーバに対してログインをコールし、アサーションを認証情報として渡します。 **ログ メッセージ：** Reading the configuration to get the target url. **チェックポイント コード：** [SSOSAML11_READTARGETURL_REQ]
	12. ログインが成功した場合、SAML 認証情報コレクタはコンシューマ サイト ドメインの SMSESSION Cookie を生成します。 **ログ メッセージ：** Login successful **チェックポイント コード：** [SSO_LOGINSUCEESS_RSP] **ログ メッセージ：** Creating the smsession cookie for SP domain. **チェックポイント コード：** [SSO_SMSESSIONFORSPDOMAIN_REQ]
	13. SMSESSION Cookie はブラウザに配置され、ユーザをターゲット リソースにリダイレクトします。 **ログ メッセージ：** Placing smsession in browser. **チェックポイント コード：** [SSO_PLACESMSSESSIONTOBROWSER_REQ]
	14. ブラウザは、コンシューマ側の Web エージェントが保護しているターゲット リソースをリクエストします。 ブラウザには、コンシューマ ドメインの SMSESSION Cookie があるので、Web エージェントはユーザを認証しません。

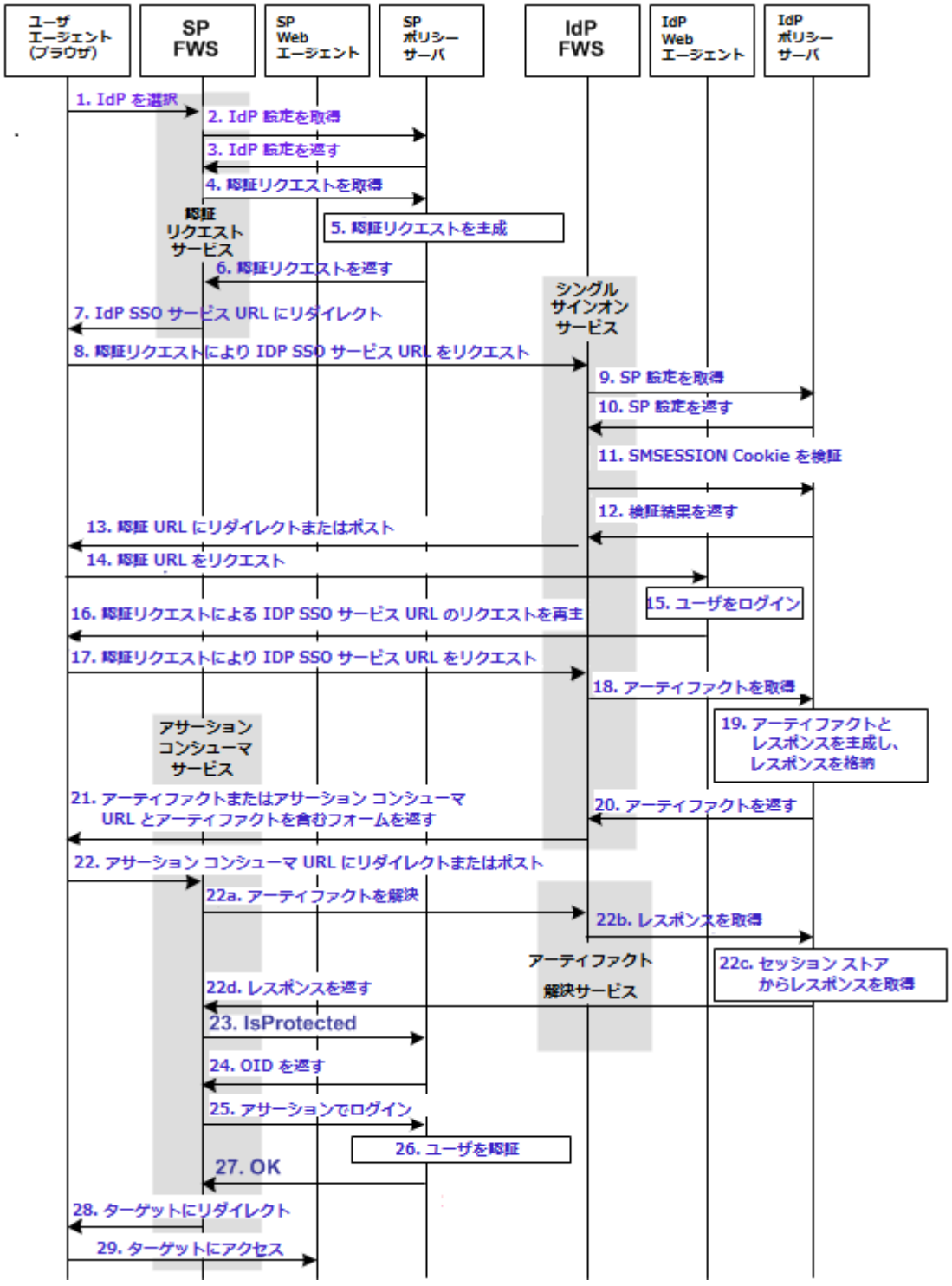
SAML 2.0 Artifact SSO トランザクション フロー（SP で開始された）

次の図は、アイデンティティ プロバイダのユーザとサービス プロバイダのコンポーネント間の詳細なフローを示しています。 このフローでは、SAML アサーションを処理する方法として SAML 2.0 Artifact プロファイルを使用したサイト間のシングル サインオンを示します。

このフローチャートでは以下の情報を想定しています。

- SP がリソースのリクエストを開始します。
- IdP サイトと SP サイトで認証および許可が正常に行われます。
- 各パートナーでプロセスを参照できるように、SiteMinder は IdP および SP として表示されます。SiteMinder が環境内の SP である場合は、テーブル内の SP アクティビティを確認します。 SiteMinder が IdP である場合は、テーブル内の IdP アクティビティを確認します。

以下の図は、SAML 2.0 Artifact SSO トランザクション フローを示しています。



注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 フロー図では、Web エージェント ブロックは SPS フェデレーション ゲートウェイに組み込まれた Web エージェントになります。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

イベント シーケンスを以下に示します。

アクター	トランザクション プロセス
SP としての SiteMinder	1. ユーザは、特定の IdP で認証するために SP でリンクを選択します。 このリンクには、選択した IdP を表すプロバイダ ID が含まれている必要があります。
	2. SP FWS がローカル ポリシー サーバの IdP 設定情報を要請します。 **ログ メッセージ:** SAML2.0 IDP Configuration is not in cache. Requesting to get from policy server. **チェックポイント コード：** [SSOSAML2_IDPCONFFROMPS_REQ]
	3. ローカル ポリシー サーバは、SP FWS アプリケーションに IdP 設定情報を返します。 FWS はこの情報をキャッシュします。 **ログ メッセージ：** Policy server returns SAML2.0 IDP Configuration **チェックポイント コード：** [SSOSAML2_IDPCONFFROMPS_RSP]
	4. SP FWS はプロバイダ ID を渡すことにより、ローカル ポリシー サーバからの AuthnRequest メッセージをトンネル コールを通じてリクエストします。このリクエストには、ProtocolBinding エレメント値に Artifact プロファイルが含まれています。 **ログ メッセージ：** Get authentication request from policy server **チェックポイント コード：** [SSOSAML2_GETAUTHENTICATIONREQFROMPS_REQ]
	5. SP ポリシー サーバは AuthnRequest メッセージを生成し、SP FWS アプリケーションにそれを返します。
	6. ローカル ポリシー サーバは、HTTP リダイレクト バインディングで SP FWS へ AuthnRequest メッセージを返します。 **ログ メッセージ：** Policy server returns authentication request. **チェックポイント コード：** [SSOSAML2_GETAUTHENTICATIONREQFROMPS_RSP]

アクター	トランザクション プロセス
	7. SP FWS アプリケーションは、ユーザを IdP シングル サインオン サービス URL にリダイレクトします。この URL は AuthnRequest メッセージにより設定情報から取得されます。 **ログ メッセージ：** Service redirecting to SSO URL **チェックポイント コード：** [SSOSAML2_SSOURL_REDIRECT]
ユーザ エージェント（ブラウザ）	8. ブラウザが IdP シングル サインオン サービス URL をリクエストします。
IdP としての SiteMinder	9. IdP FWS は、ローカル IdP ポリシー サーバから SP 設定情報をリクエストします。 **ログ メッセージ：** SAML2.0 SP configuration is not in cache. Requesting to get from policy server. **チェックポイント コード：** [SSOSAML2_SPCONFFROMPS_REQ]
	10. ローカル ポリシー サーバは設定を返し、FWS アプリケーションはこれをキャッシュします。 **ログ メッセージ：** Policy server returns SAML2.0 SP Configuration **チェックポイント コード：** [SSOSAML2_SPCONFFROMPS_RSP]
	11. IdP FWS アプリケーションは、この IdP ドメインに対して SMSESSION Cookie を取得します。 FWS は、次にポリシー サーバを呼び出してこれを検証します。 SMSESSION Cookie がない場合、FWS アプリケーションは認証 URL にリダイレクトするか、ポストします。 **ログ メッセージ**: Session cookie does not exists. Redirecting to authentication URL **チェックポイント コード：** [SSOSAML2_AUTHENTICATIONURL_REDIRECT]
	12. ポリシー サーバは、SMSESSION Cookie を検証し、結果を返します。 **ログ メッセージ：** Request to validate the session. **チェックポイント メッセージ：** [SSOSAML2_SESSIONCOOKIEVALIDATE_REQ]
	13. SMSESSION Cookie が有効な場合、IDP FWS はローカル ポリシー サーバの SAML 2.0 Artifact をリクエストします（手順 18 を参照）。 SMSESSION Cookie が存在しないか有効でない場合、IDP FWS は認証 URL にリダイレクトするか、ポストします。 **ログ メッセージ：** Session cookie does not exists, redirecting to authentication url. **チェックポイント コード：** [SSOSAML2_AUTHENTICATIONURL_REDIRECT]

アクター	トランザクション プロセス
ユーザ エージェント（ブラウザ）	14. SMSESSION Cookie が有効でない場合、ブラウザは IdP Web エージェントによって保護されている認証 URL をリクエストします。
IdP としての SiteMinder	15. IdP Web エージェントは、ユーザをログインさせ、SMSESSION Cookie を設定し、リクエストを認証 URL に渡します。 **ログ メッセージ：** Service redirecting to SSO URL **チェックポイント コード：** [SSOSAML2_SSOURL_REDIRECT]
	16. 認証 URL は redirect.jsp ファイルです。これは、AuthnRequest メッセージにより IdP シングル サインオン サービスへのリクエストを再生します。
ユーザ エージェント（ブラウザ）	17. ブラウザが IdP シングル サインオン サービス URL をリクエストします。 このリクエストは手順 8 のリクエストと同じですが、今度はユーザには有効な SMSESSION Cookie があります。
IdP としての SiteMinder	18. IdP FWS がローカル ポリシー サーバの SAML 2.0 Artifact をリクエストします。 FWS は設定情報から取得したレルムへの許可呼び出しを通じて AuthnRequest を渡します。 **ログ メッセージ：** Request to policy server for generating saml2 assertion/artifact based on selected profile. **チェックポイント コード：** [SSOSAML2_GENERATEASSERTIONORARTIFACT_REQ]
	19. ポリシー サーバが Artifact および対応する応答メッセージを生成します。メッセージは、サービス プロバイダ設定から形成されます。ポリシー サーバがセッション ストアに応答を格納します。 メッセージはセッション変数として格納され、Artifact メッセージ ハンドルの文字列表記を使用して指定されます。 **ログ メッセージ：** Policy server generates the artifact for the assertion. **チェックポイント コード：** [SSOSAML2_PSGENERATEARTIFACT_REQ] **ログ メッセージ：** Policy server stores the assertion in session store. **チェックポイント コード：** [SSOSAML2_PSSTOREASSERTIONINSSTORE_REQ]
	20. ポリシー サーバが IdP FWS に Artifact を返します。 **ログ メッセージ：** Policy server returning the wrappedassertion/artifact based on profile selected in response message. **チェックポイント コード：** [SSO_PSWRAPPEDASSERTION_RSP]

アクター	トランザクション プロセス
	21. ポリシー サーバは SP 設定情報を返します。 **ログ メッセージ：** Policy server returns SAML2.0 SP Configuration **チェックポイント コード：** [SSOSAML2_SPCONFFROMPS_RSP] この情報に基づき、IdP FWS は次のいずれかのアクションを実行します。 ■ SP のアサーション コンシューマ URL へブラウザをリダイレクトします。 URL エンコードされた Artifact は URL パラメータです。 **ログ メッセージ：** Sending artifact to assertion consumer as url parameter. **チェックポイント コード：** [SSOSAML2_SENDINGARTIFACTASURLPARAM_RSP] ■ ユーザにフォームを返します。 このフォームには、ブラウザでフォームを自動ポストするための JavaScript、応答メッセージ、アサーション コンシューマ URL が含まれています。 **ログ メッセージ：** Adding response in form for HTTP post. **チェックポイント コード：** [FWSBASE_POSTDATAFORM_ADD] **注**: アサーション ジェネレータは、現在のセッションの認証レベルが低すぎることを示すことがあります。 レベルが低すぎる場合、IdP FWS はステップアップ認証を促すために認証 URL へリダイレクトします。
ユーザ エージェント（ブラウザ）	22. ブラウザは、SP のアサーション コンシューマ URL に応答メッセージをポストします。
IdP としての SiteMinder	23. Artifact が URL の一部として送信された場合、ブラウザはユーザを Artifact によりアサーション コンシューマ URL にリダイレクトします。 Artifact がフォームで返された場合は、ブラウザはその Artifact をアサーション コンシューマ URL にポストします。 **ログ メッセージ：** Browser posting the response to assertion consumer url. **チェックポイント コード：** [SSOSAML2_POSTASSERTIONTOCONSUMERURL_RSP] SP FWS アサーション コンシューマ サービスは、Artifact を取得するために IdP FWS Artifact 解決サービスに対してバックチャネルをコールします。手順 23a ～ 23d はバックエンド チャネルに関するものです。

アクター	トランザクション プロセス
	23a. SP FWS は、IdP FWS がブラウザをリダイレクトするためにどのように設定されているかに応じて、GET または POST データから Artifact を取得します。FWS は次に IdP 設定の Artifact 解決サービスの SOAP エンドポイントを取得します。 ソース ID は Artifact の一部です。 SOAP エンドポイントが取得された後、SP FWS は Artifact をレスポンス メッセージに解決するために IdP FWS Artifact 解決サービスに対してバックチャネルをコールします。 **ログ メッセージ：** Backchannel call to resolve the artifact. **チェックポイント コード：** [SSOSAML2_RESOLVEARTIFACT_REQ] **ログ メッセージ：** Obtained response message from post data for artifact binding. **チェックポイント コード：** SSOSAML2_READRESPONSEARTIFACTDATA_RSP
	23b. IdP FWS はローカル ポリシー サーバの応答メッセージをリクエストします。 Java エージェント API を使用して、セッション変数として格納されるメッセージがリクエストされます。セッション ID が Artifact から抽出されます。セッション変数名は Artifact メッセージ ハンドルの文字列表記です。 **ログ メッセージ：** Extracting session id from artifact. **チェックポイント コード：** [SSOSAML2_EXTRACTSESSIONIDFROMARTIFACT_REQ]
	23c. ローカル ポリシー サーバは、セッション ストアからアサーション レスポンス メッセージを取得します。 ポリシー サーバは、Artifact 取得後にそれを削除します。 **ログ メッセージ：** Retrieving assertion from session store. **チェックポイント コード：** [SSOSAML2_RETREIVEASSERTIIONFROMSSTORE_REQ]
	23d. ローカル ポリシー サーバは、アサーションを取得し、Artifact レスポンスを IdP FWS に返します。 IdP FWS は、Artifact レスポンスを SP FWS アサーション コンシューマ サービスに返します。 **ログ メッセージ：** Obtained the SAML2 asserion as response from artifact resolve call. **チェックポイント コード：** [SSOSAML2_GOTARTIFACTRESPONSE_RSP] **ログ メッセージ：** Sending assertion as artifact response. **チェックポイント コード：** [SSOSAML2_SENDARTIFACTRESPONSE_RSP] これでバックチャネル呼び出しが終了します。

アクター	トランザクション プロセス
SP としての SiteMinder	24. SP FWS が、POST データから応答メッセージを取得します。 その後、サービスは設定からターゲット リソースを決定し、ターゲット リソースのポリシー サーバへ isProtected 呼び出しを行います。 **ログ メッセージ：** Reading the configuration to get the target URL. **チェックポイント コード：** [SSOSAML2_READTARGETURL_REQ] **ログ メッセージ：** IsProtected call to policy server for target resource realm **チェックポイント コード：** [SSOSAML2_ISPROTECTEDCALLTOPS_REQ] アサーションが暗号化されている場合、FWS はトンネル コールを行います。 このコールは暗号化されたアサーションを取得し、プレーン テキストでアサーションを返します。 **ログ メッセージ：** Tunnel call to decrypt the assertion. **チェックポイント コード：** [SSOSAML2_DECRYPTASSERTION_REQ]
	25. ポリシー サーバが、ターゲット リソースのレルム OID を返します。 **ログ メッセージ：** Policy server returns the realm OID for target resource. **チェックポイント コード：** [SSOSAML2_REALMOIDFORTARGETFROMPS_RSP]
	26. SP FWS はローカル ポリシー サーバに、ログイン呼び出しを通じて応答メッセージを渡します。 応答メッセージは認証情報として機能します。また、レルム OID は isProtected 呼び出しから取得されます。 **ログ メッセージ：** Passing response message through login call. **チェックポイント コード：** [SSO_RESPONSEMESSAGEINLOGIN_REQ] SAML 2.0 認証方式は認証情報として応答メッセージを使用し、ユーザをログインさせます。 **ログ メッセージ：** Policy server logs in the user using SAML 2 auth scheme. **チェックポイント コード：** [SAML2_AUTH_COMPLETE]
	27. ローカル ポリシー サーバは、SP FWS に OK を返します。

アクター	トランザクション プロセス
	28. 成功返答が返された場合、SP FWS は SP ドメインの SMSESSION Cookie を作成します。 サービスは Cookie をブラウザに配置します。 **ログ メッセージ：** Login successful **チェックポイント コード：** [SSO_LOGINSUCEESS_RSP] **ログ メッセージ：** Creating the smsession cookie for SP domain **チェックポイント コード：** [SSO_SMSESSIONFORSPDOMAIN_REQ] ブラウザは、ユーザをターゲット URL にリダイレクトします。この URL は設定情報から取得されます。 **ログ メッセージ：** Redirecting user to target url. **チェックポイント コード：** [SSOSAML2_REDIRECTUSERTARGETURL_REQ] ログインが失敗した場合、SP FWS はユーザを非アクセス URL にリダイレクトします。 **ログ メッセージ：** Login failure **チェックポイント コード：** [SSO_LOGINFAILURE_RSP]
ユーザ エージェント（ブラウザ）	29. ブラウザは、リクエストをターゲット URL に送信します。これは SP 側の Web エージェントによって保護されています。 ブラウザに SMSESSION Cookie があるので、Web エージェントはユーザの認証を行いません。ユーザはリソースにアクセスできます。

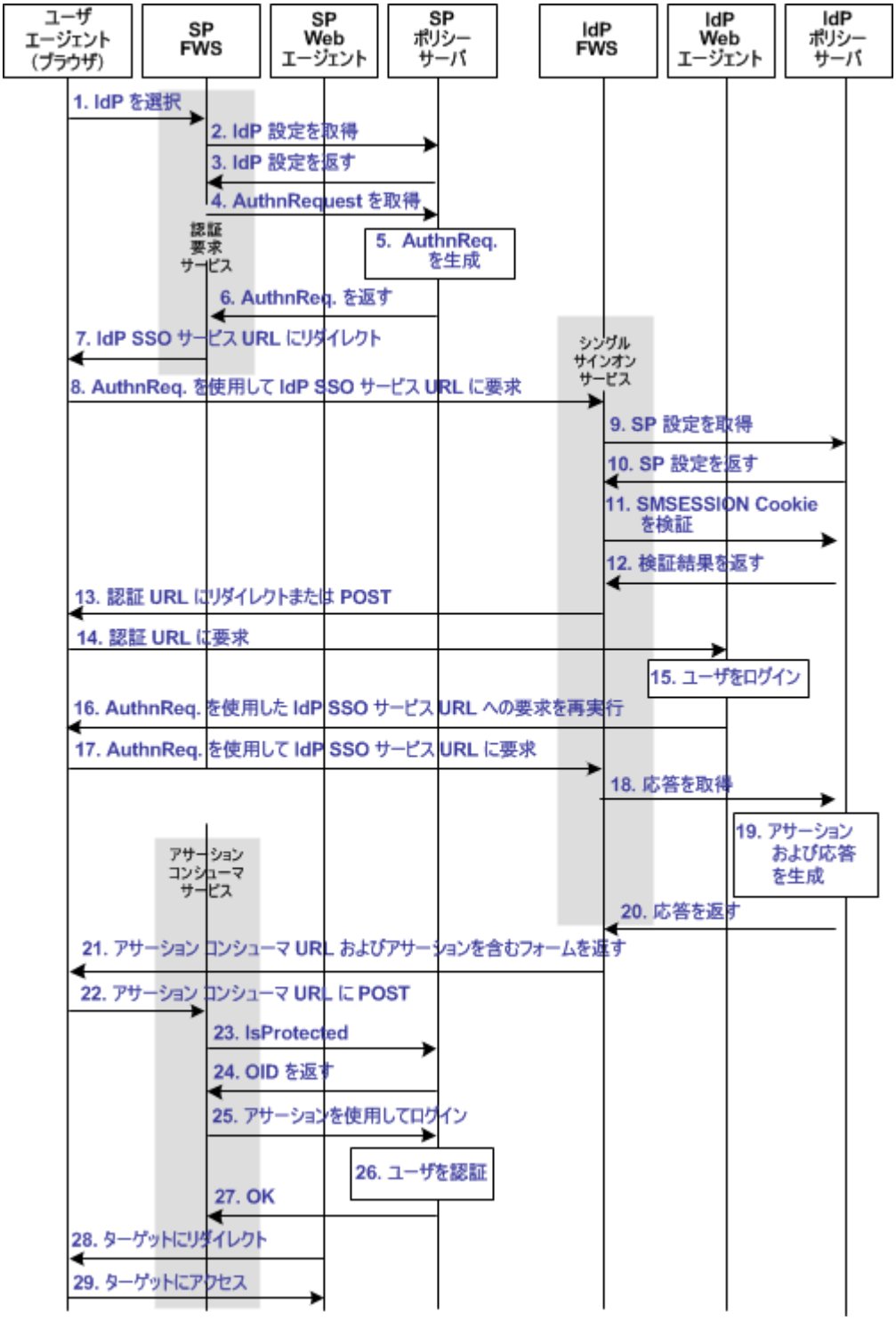
SAML 2.0 POST SSO トランザクション フロー（SP で開始された）

以下の図は、SiteMinder アイデンティティ プロバイダ（IdP）サイトおよびサービス プロバイダ（SP）サイトに展開されたコンポーネントとユーザ間の詳細なフローを示しています。 このフローでは、SAML アサーションを処理する方法として SAML 2.0 POST プロファイルを使用したサイト間のシングル サインオンを示します。

このフローチャートでは以下の情報を想定しています。

- アサーションに対して SP でリクエストが開始されました。
- IdP サイトと SP サイトで認証および許可が正常に行われます。
- 各パートナーでプロセスを参照できるように、SiteMinder は IdP および SP のみとして表示されます。 SiteMinder が環境内の SP である場合は、テーブル内の SP アクティビティを確認します。 SiteMinder が IDP である場合は、テーブル内の IdP アクティビティを確認します。

以下の図は、SAML 2.0 POST SSO トランザクション フローを示しています。



注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 フロー図では、Web エージェント ブロックは SPS フェデレーション ゲートウェイに組み込まれた Web エージェントになります。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

イベント シーケンスを以下に示します。

アクター	トランザクション プロセス
SP としての SiteMinder	1. ユーザは、特定の IdP で認証するために SP でリンクを選択します。このリンクには、選択した IdP を表すプロバイダ ID が含まれる必要があります。
	2. SP FWS は、ローカル ポリシー サーバから IdP 設定をリクエストします。 **ログ メッセージ：** SAML2.0 IDP Configuration is not in cache. Requesting to get from policy server **チェックポイント コード：** [SSOSAML2_IDPCONFFROMPS_REQ]
	3. ポリシー サーバは、IdP 設定を SP FWS アプリケーションに返します。FWS アプリケーションはこの情報をキャッシュします。 **ログ メッセージ：** Policy server returns SAML2.0 IDP Configuration **チェックポイント コード：** [SSOSAML2_IDPCONFFROMPS_RSP]
	4. SP FWS アプリケーションは、ローカル SP ポリシー サーバからの AuthnRequest メッセージをトンネル コールを通じてリクエストし、プロバイダ ID を渡します。 **ログ メッセージ：** Get authentication request from policy server **チェックポイント コード：** [SSOSAML2_GETAUTHENTICATIONREQFROMPS_REQ]
	5. SP ポリシー サーバは AuthnRequest メッセージを生成し、SP FWS アプリケーションにそれを返します。

アクター	トランザクション プロセス
	6. SP FWS アプリケーションは、HTTP リダイレクト バインディングで AuthnRequest レスポンスを取得します。 **ログ メッセージ：** Policy server returns authentication request. **チェックポイント コード：** [SSOSAML2_GETAUTHENTICATIONREQFROMPS_RSP]
	7. SP FWS アプリケーションは、ユーザを IdP シングル サインオン サービス URL にリダイレクトします。 **ログ メッセージ：** Service redirecting to SSO URL **チェックポイント コード：** [SSOSAML2_SSOURL_REDIRECT]
ユーザ エージェント（ブラウザ）	8. ブラウザが IdP シングル サインオン サービス URL をリクエストします。
IdP としての SiteMinder	9. IdP FWS は、ローカル IdP ポリシー サーバから SP 設定をリクエストします。 **ログ メッセージ：** SAML2.0 SP configuration is not in cache. Requesting to get from policy server. **チェックポイント コード：** [SSOSAML2_SPCONFFROMPS_REQ]
	10. ローカル ポリシー サーバは設定を返し、FWS アプリケーションはこれをキャッシュします。 **ログ メッセージ：** Policy server returns SAML2.0 SP Configuration **チェックポイント コード：** [SSOSAML2_SPCONFFROMPS_RSP]
	11. IdP FWS アプリケーションは、この IdP ドメインに対して SMSESSION Cookie を取得します。 FWS アプリケーションは、次にポリシー サーバを呼び出して、これを検証します。 SMSESSION Cookie がない場合、アプリケーションは認証 URL にリダイレクトされるか、認証 URL にポストされます。 **ログ メッセージ：** Session cookie does not exists. Redirecting to authentication URL **チェックポイント コード：** [SSOSAML2_AUTHENTICATIONURL_REDIRECT]
	12. ポリシー サーバは、SMSESSION Cookie を検証し、結果を返します。 **ログ メッセージ：** Request to validate the session. **チェックポイント メッセージ：** [SSOSAML2_SESSIONCOOKIEVALIDATE_REQ]

アクター	トランザクション プロセス
	13. SMSESSION Cookie が有効な場合、IdP FWS は手順 18 にスキップします。 SMSESSION Cookie が有効でないか存在しない場合、IdP FWS は認証 URL にリダイレクトされるか、認証 URL にポストされます。 **ログ メッセージ：** Session cookie does not exists, redirecting to authentication url. **チェックポイント コード：** [SSOSAML2_AUTHENTICATIONURL_REDIRECT]
ユーザ エージェント（ブラウザ）	14. SMSESSION Cookie が有効でない場合、ブラウザは IdP Web エージェントによって保護されている認証 URL をリクエストします。
IdP としての SiteMinder	15. IdP Web エージェントは、ユーザをログインさせ、SMSESSION Cookie を設定し、リクエストを認証 URL に渡します。 **ログ メッセージ：** Service redirecting to SSO URL **チェックポイント コード：** [SSOSAML2_SSOURL_REDIRECT]
	16. 認証 URL は redirect.jsp ファイルです。これは、AuthnRequest メッセージにより IdP シングル サインオン サービスへのリクエストを再生します。
ユーザ エージェント（ブラウザ）	17. ブラウザが IdP シングル サインオン サービス URL をリクエストします。このリクエストは手順 8 のリクエストと同じですが、今度はユーザには有効な SMSESSION Cookie があります。
IdP としての SiteMinder	18. IdP FWS がポリシー サーバに SAML 2.0 アサーションをリクエストします。AuthnRequest は、設定から取得されたレルムへの許可呼び出しを行います。 **ログ メッセージ：** Request to policy server for generating saml2 assertion/artifact based on selected profile. **チェックポイント コード：** [SSOSAML2_GENERATEASSERTIONORARTIFACT_REQ]
	19. ポリシー サーバは、SP の設定情報に基づいてアサーションを生成し、署名して、レスポンス メッセージでラップしてアサーションを返します。 **ログ メッセージ：** Policy server generates the saml2 assertion. **チェックポイント コード：** [SSOSAML2_PSGENERATEASSERTION_RSP]

アクター	トランザクション プロセス
	20. 応答メッセージが IdP FWS に返されます。 **ログ メッセージ:** Policy server returns the wrappedassertion/artifact(based on profile selected) in response message. **チェックポイント コード：** [SSO_PSWRAPPEDASSERTION_RSP]
	21. IdP FWS はフォームをユーザに返します。 このフォームには、レスポンス メッセージ、アサーション コンシューマ URL、およびフォームをサブミットするための JavaScript が含まれています。 **ログ メッセージ：** Adding response in form for HTTP post. **チェックポイント コード：** [FWSBASE_POSTDATAFORM_ADD] **注**: ポリシー サーバが現在のセッションの認証レベルが低すぎることを指摘した場合、IdP FWS は、ステップアップ認証を容易に行うために、手順 13 に示されているように、認証 URL にリダイレクトされます。
ユーザ エージェント（ブラウザ）	22. ブラウザは、SP でレスポンスをアサーション コンシューマ URL にポストします。
SP としての SiteMinder	23. SP FWS が、POST データから応答メッセージを取得します。 その後、FWS は設定からターゲット リソースを決定し、ターゲット リソースのポリシー サーバへ isProtected 呼び出しを行います。 アサーションが暗号化されている場合、FWS はトンネル コールを行います。 この呼び出しは暗号化されたアサーションを取得し、プレーンテキストでアサーションを返します。 **ログ メッセージ：** Reading the configuration to get the target url. **チェックポイント コード：** [SSOSAML2_READTARGETURL_REQ] **ログ メッセージ：** Get realm oid for target resource from property **チェックポイント コード：** [SSOSAML2_REALMOIDFORTARGETFROMPROPERTY_RSP] **ログ メッセージ：** Tunnel call to decrypt the assertion. **チェックポイント コード：** [SSOSAML2_DECRYPTASSERTION_REQ]
	24. ポリシー サーバが、ターゲット リソースのレルム OID を返します。 **ログ メッセージ：** Policy server returns the realm oid for target resource. **チェックポイント コード：** [SSOSAML2_REALMOIDFORTARGETFROMPS_RSP]

アクター	トランザクション プロセス
	25. SP FWS はローカル ポリシー サーバに、ログイン呼び出しを通じて応答メッセージを渡します。 FWS は、認証情報としての応答メッセージと isProtected 呼び出しから取得されされたレルム OID を使用します。 **ログ メッセージ：** Passing response message through login call. **チェックポイント コード：** [SSO_RESPONSEMESSAGEINLOGIN_REQ]
	26. ポリシー サーバは、応答メッセージを認証情報として使用してユーザをログインさせます。 **ログ メッセージ：** Policy server logs in the user using SAML 2 auth scheme. **チェックポイント コード：** [SAML2_AUTH_COMPLETE]
	27. ローカル ポリシー サーバは、SP FWS に OK を返します。 **ログ メッセージ：** Login successful **チェックポイント コード：** [SSO_LOGINSUCEESS_RSP]
	28. 成功返答が返された場合、SP FWS は SP ドメインに対して SMSESSION Cookie を作成します。 FWS アプリケーションはブラウザに Cookie を配置し、ユーザをターゲット URL にリダイレクトします。 **ログ メッセージ：** Redirecting user to target url **チェックポイント コード：** [SSOSAML2_REDIRECTUSERTARGETURL_REQ] ログインが失敗した場合、SP FWS はユーザを非アクセス URL にリダイレクトします。 **ログ メッセージ：** Login failure **チェックポイント コード：** [SSO_LOGINFAILURE_RSP]
ユーザ エージェント（ブラウザ）	29. ブラウザは、リクエストをターゲット URL に送信します。これは SP 側の Web エージェントによって保護されています。 ブラウザに SMSESSION Cookie があるので、Web エージェントはユーザの認証を行いません。 ユーザはリソースにアクセスできます。

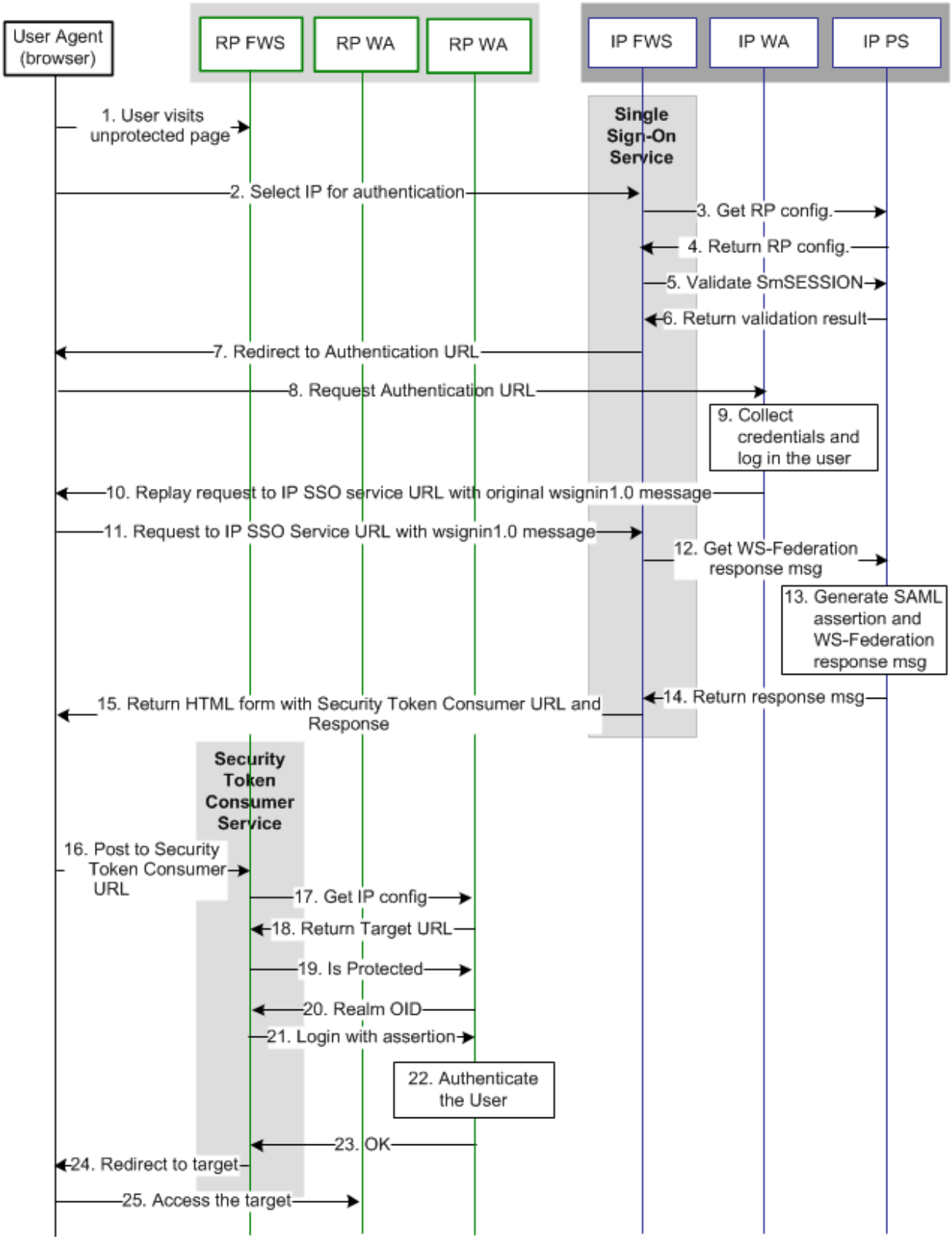
WS-フェデレーション SSO トランザクション フロー（RP で開始された）

以下の図は、アイデンティティ パートナー（IP）サイトとリソース パートナー（RP）サイトでのユーザとフェデレーション コンポーネント間の詳細なフローを示しています。 このフローでは、SAML アサーションを処理する方法として WS-フェデレーション パッシブ リクエスタ プロファイルを使用したサイト間のシングル サインオンを示します。

このフローチャートでは以下の情報を想定しています。

- リソース パートナーがリソースのリクエストを開始します。
- 各サイトで認証および許可が正常に行われます。
- 各パートナーでプロセスを参照できるように、SiteMinder は IP および RP のみとして表示されます。 SiteMinder が環境内の IP である場合は、テーブル内の IP アクティビティを確認します。 SiteMinder が RP である場合は、テーブル内の RP アクティビティを確認します。

以下の図は、WS-フェデレーション SSO トランザクション フローを示しています。


User Agent (browser)
RP FWS
RP WA
RP WA
IP FWS
IP WA
IP PS
Single Sign-On Service
1. User visits unprotected page
2. Select IP for authentication
3. Get RP config.
4. Return RP config.
5. Validate SmSESSION
6. Return validation result
7. Redirect to Authentication URL
8. Request Authentication URL
9. Collect credentials and log in the user
10. Replay request to IP SSO service URL with original wsignin1.0 message
11. Request to IP SSO Service URL with wsignin1.0 message
12. Get WS-Federation response msg
13. Generate SAML assertion and WS-Federation response msg
14. Return response msg
15. Return HTML form with Security Token Consumer URL and Response
Security Token Consumer Service
16. Post to Security Token Consumer URL
17. Get IP config
18. Return Target URL
19. Is Protected
20. Realm OID
21. Login with assertion
22. Authenticate the User
23. OK
24. Redirect to target
25. Access the target

注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 フロー図では、Web エージェント ブロックは SPS フェデレーション ゲートウェイに組み込まれた Web エージェントになります。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

イベント シーケンスを以下に示します。

アクター	トランザクション プロセス
RP としての SiteMinder	1. ユーザがリソース パートナーで非保護のサイト選定ページにアクセスします。
	2. ユーザはリンクをクリックして、IP で認証を行います。 このリンクは IP の シングル サインオン サービスを指しています。 このリンクには、RP のプロバイダ ID が含まれる必要があり、wctx パラメータなどのオプションのパラメータを含めることができます。
	3. IP FWS は、ローカル ポリシー サーバの RP 設定をリクエストします。 **ログ メッセージ：** Trying to fetch Wsfed Resource Partner Configuration from cache **チェックポイント コード：** [SSOWSFED_RESOURCEPARTNERCONFFROMCACHE_REQ] **ログ メッセージ：** Wsfed Resource Partner Configuration is not in cache. Requesting to get from policy server. **チェックポイント コード：** [SSOWSFED_RESOURCEPARTNERCONFFROMPS_REQ]
	4. ローカル ポリシー サーバは設定を返します。 **ログ メッセージ：** Policy server returns Wsfed Resource Partner Configuration **チェックポイント コード：** [SSOWSFED_RESOURCEPARTNERCONFFROMPS_RSP]

アクター	トランザクション プロセス
	5. IP FWS は、IP ドメインの SMSESSION Cookie を取得し、それを検証するためにポリシー サーバを呼び出します。 SMSESSION Cookie がない場合、IP FWS は手順 7 にスキップします。 **ログ メッセージ：** Request to validate the session **チェックポイント コード：** [SSOWSFED_SESSIONCOOKIEVALIDATE_REQ]
	6. ポリシー サーバは SMSESSION Cookie を検証し、FWS アプリケーションに結果を返します。
	7. SMSESSION Cookie が存在しないか有効でない場合、IP FWS はユーザを RP 設定情報から取得された認証 URL にリダイレクトします。 SMSESSION Cookie が有効な場合、IP FWS は手順 12 にスキップします。 **ログ メッセージ：** Session cookie does not exists, redirecting to authentication url **チェックポイント コード：** [SSOWSFED_AUTHENTICATIONURL_REDIRECT]
ユーザ エージェント（ブラウザ）	8. ブラウザは、IP Web エージェントが保護する認証 URL をリクエストします。
IP としての SiteMinder	9. IP WA がユーザを認証し、SMSESSION Cookie を設定します。 IP WA によって、リクエストが認証 URL に渡されます。
	10. 認証 URL は、元の wsignin メッセージにより IP SSO サービスへのリクエストを再生します。
ユーザ エージェント（ブラウザ）	11. ブラウザが IP SSO サービス URL をリクエストします。このリクエストは手順 2 のリクエストと同じですが、今度は、ユーザには有効な SMSESSION Cookie があります
IP としての SiteMinder	12. IP FWS は、設定から取得したレルムに対する許可コールを通じて、ポリシー サーバからの WS-フェデレーション <RequestSecurityTokenResponse> をリクエストします。 **ログ メッセージ：** Request to policy server for generating Wsfed assertion. **チェックポイント メッセージ：** [SSOWSFED_GENERATEASSERTION_REQ]
	13. ポリシー サーバは、RP の設定に基づいて SAML1.1 アサーションを生成します。 **ログ メッセージ：** Policy server generates the samlxx assertion for wsfed12. **チェックポイント コード：** [SSOWSFED12_PSGENERATESAML11ASSERTION_RSP]

アクター	トランザクション プロセス
	14. ポリシー サーバはアサーションに署名し、それを <RequestSecurityTokenResponse> メッセージで IP FWS アプリケーションに返します。 **ログ メッセージ：** Policy server signs the Assertion element of the RequestSecurityTokenResponse **チェックポイント コード：** SAML プロトコルに応じて異なります。 [SSOWSFED10_PSGENERATELEGACYASSERTION_RSP] [SSOWSFED12_PSGENERATESAML12ASSERTION_RSP] [SSOWSFED_PSSIGNASSERTION_RSP]
	15. IP FWS は、ユーザにフォームを返します。このフォームには、URL がエンコードされた <RequestSecurityTokenResponse> メッセージ、セキュリティ トークン コンシューマ サービス URL、wsignin メッセージ内のオプションの wctx、およびフォームを自動サブミットするための JavaScript が含まれます。 元の wsignin リクエストに wreply パラメータが含まれている場合、その値はセキュリティ トークン コンシューマの URL になります。 wreply の値が URL になるのは、セキュリティ トークン コンシューマ の URL 設定が RP 設定にない場合のみです。 RP 設定内のセキュリティ トークン コンシューマ URL は wreply パラメータに優先します。 **注**: ポリシー サーバは、現行セッションの認証レベルが低すぎることを指摘することがあります。 レベルが低すぎる場合、IP FWS アプリケーションは、ステップアップ認証を容易に行うために、手順 7 に示されているように、ブラウザを認証 URL へリダイレクトします。 **ログ メッセージ：** Received the assertion response. **チェックポイント コード：** [SSOWSFED_RECEIVEDASSERTION_RSP]
ユーザ エージェント（ブラウザ）	16. ブラウザは、<RequestSecurityTokenResponse> メッセージおよび wctx を、RP でセキュリティ トークン コンシューマ URL にポストします。

アクター	トランザクション プロセス
RP としての SiteMinder	17. RP FWS アプリケーションは POST データから <RequestSecurityTokenResponse> メッセージおよび wctx を取得します。RP FWS アプリケーションは、ローカル ポリシー サーバの IP 設定をリクエストします。 **ログ メッセージ：** Browser posting the response to security token consumer service url. **チェックポイント コード：** [SSOWSFED_POSTASSERTIONTOSECURITYTOKENCONSUMER_RSP] **ログ メッセージ：** Extracting the assertion from security token consumer response **チェックポイント コード：** [SSOWSFED_EXTARCTASSERTIONFROMSECURITYTOKENRESPONSE_REQ]
	18. RP FWS は、ローカル ポリシー サーバの IP 設定からターゲット リソースを決定します。 ターゲット リソースが IP 設定の一部ではなく、wctx パラメータが POST データで見つかる場合、wctx の値がターゲット リソースになります。 **ログ メッセージ：** Request to get the target url realm. **チェックポイント コード：** [SSOWSFED_GETTARGETURLREALM_REQ]
	19. FWS が、ターゲット リソースのポリシー サーバに対して isProtected 呼び出しを行います。
	20. ポリシー サーバが、ターゲット リソースのレルム OID を返します。
RP としての SiteMinder （続き）	21. RP FWS アプリケーションは、ログイン コールを通じて <RequestSecurityTokenResponse> メッセージをローカル ポリシー サーバに 渡します。 isProtected コールで取得された <RequestSecurityTokenResponse> メッセージおよびレルム OID は、認証情報として機能します。
	22. RP FWS アプリケーションは、<RequestSecurityTokenResponse> メッセージを認証情報として使用して、ユーザをログインさせます。
	23. ローカル ポリシー サーバは、RP FWS アプリケーションへ OK ステータス メッセージを返します。

アクター	トランザクション プロセス
	24. RP FWS アプリケーションは、RP ドメインの SMSESSION Cookie を生成します。 FWS は Cookie をブラウザに配置し、ユーザをターゲット URL、または wctx POST データにリダイレクトします。 ログインが失敗した場合、FWS アプリケーションはユーザを非アクセス URL にリダイレクトします。 **ログ メッセージ：** Redirecting user to target url. **チェックポイント コード：** [SSOWSFED_REDIRECTUSERTARGETURL_REQ]
ユーザ エージェント（ブラウザ）	25. ユーザ エージェントは、RP 側の Web エージェントが保護するターゲット URL をリクエストします。ブラウザに RP ドメインの SMSESSION Cookie があるので、Web エージェントはユーザに対してチャレンジを行う必要はありません。

WS-フェデレーション SSO トランザクション フロー（IP で開始された）

IP で開始されたシングル サインオンは、RP で開始されたトランザクションに類似しています。 主な違いは、ユーザが RP に送信される前に、IP で発生するわずかのアクションです。

IP で、以下のアクションが発生します。

1. ユーザは特定のパートナー サイトのリンクを選択します。このリンクは IP の HTML コンテンツの一部です。これには、別の RP サイトへのサイト間の転送リンクが含まれています。
2. このリンクは Web ブラウザを IP SSO サービス URL にダイレクトします。
3. SSO サービスはブラウザを RP にリダイレクトします。RP での残りの処理は、RP で開始された SSO トランザクション フロー (P. 109)で指定されたものと同じです。

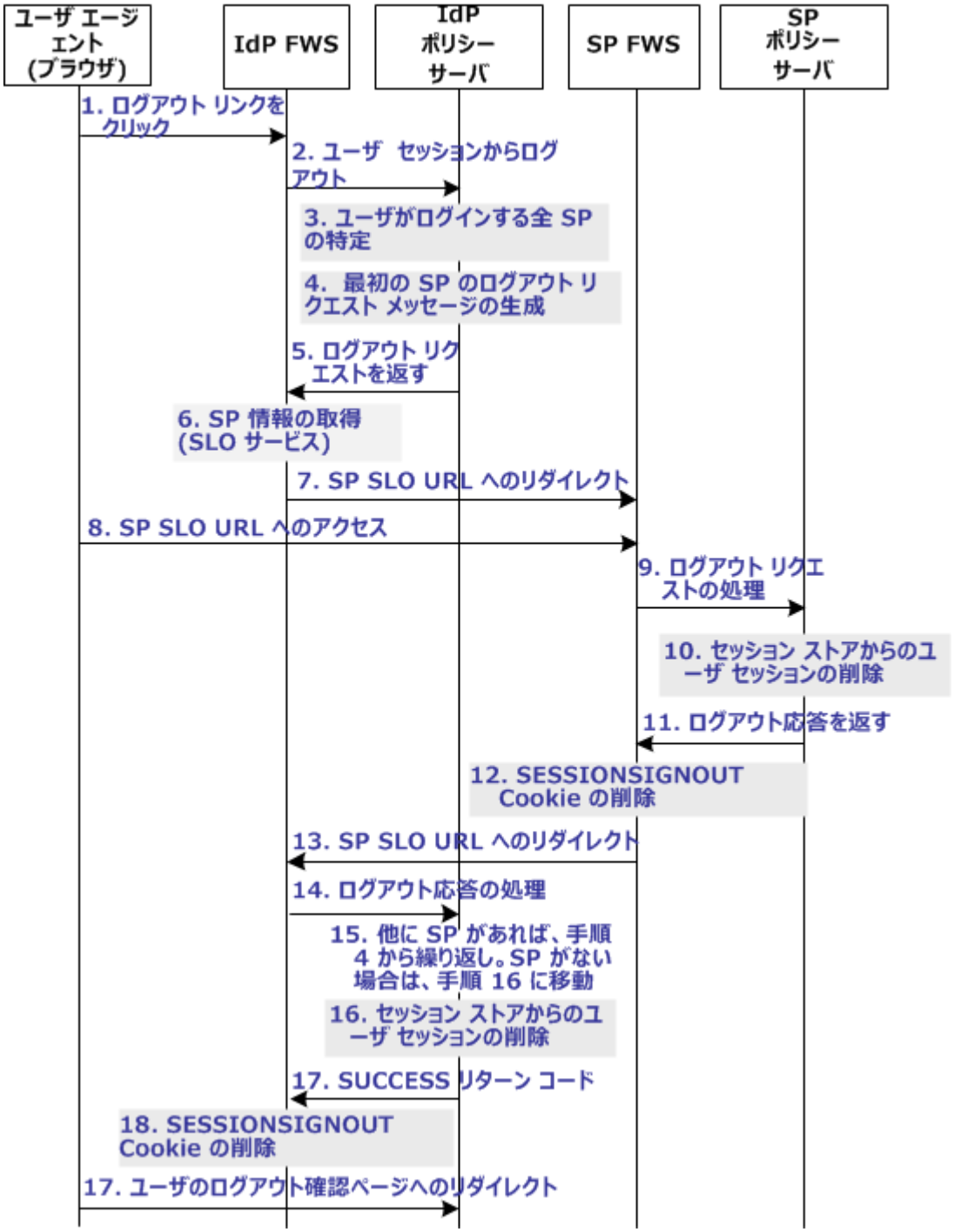
SAML 2.0 シングル ログアウト トランザクション フロー（IdP で開始された）

以下の図は、ユーザと SiteMinder アイデンティティ プロバイダ（IdP）およびサービス プロバイダ（SP）で展開されているコンポーネントの間のシングル ログアウト（SLO）リクエストの詳細なフローを示しています。 このフローは、特定のユーザとセッションを行うすべてのエンティティのシングル ログアウトを示しています。

このフローチャートでは以下の情報を想定しています。

- IdP はログアウト リクエストを開始します。
- HTTP-Redirect バインディングは使用中です。
- 各パートナーでプロセスを参照できるように、SiteMinder は IdP および SP のみとして表示されます。 SiteMinder が環境内の SP である場合は、テーブル内の SP アクティビティを確認します。 SiteMinder が IDP である場合は、テーブル内の IdP アクティビティを確認します。

以下の図は、SLO トランザクション フローを示しています。 IdP が SLO を開始すると、いくつかの SP は SLO リクエストを受信できます。


ユーザ エージェント (ブラウザ)
IdP FWS
IdP ポリシー サーバ
SP FWS
SP ポリシー サーバ
1. ログアウト リンクをクリック
2. ユーザ セッションからログアウト
3. ユーザがログインする全 SP の特定
4. 最初の SP のログアウト リクエスト メッセージの生成
5. ログアウト リクエストを返す
6. SP 情報の取得 (SLO サービス)
7. SP SLO URL へのリダイレクト
8. SP SLO URL へのアクセス
9. ログアウト リクエストの処理
10. セッション ストアからのユーザ セッションの削除
11. ログアウト応答を返す
12. SESSIONSIGNOUT Cookie の削除
13. SP SLO URL へのリダイレクト
14. ログアウト応答の処理
15. 他に SP があれば、手順 4 から繰り返し。SP がない場合は、手順 16 に移動
16. セッション ストアからのユーザ セッションの削除
17. SUCCESS リターン コード
18. SESSIONSIGNOUT Cookie の削除
17. ユーザのログアウト確認ページへのリダイレクト

注: SPS フェデレーション ゲートウェイは、Web エージェントおよび Web エージェント オプション パックを置き換えて、FWS アプリケーション機能を提供することができます。SPS フェデレーション ゲートウェイのインストールおよび設定の詳細については、「*CA SiteMinder Secure Proxy Server Administration Guide*」を参照してください。

イベント シーケンスを以下に示します。

アクター	トランザクション プロセス
IdP としての SiteMinder	1. ユーザは IdP でログアウト リンクをクリックします。ブラウザは IdP でシングル ログアウト サーブレットにアクセスします。 IdP FWS アプリケーションは、SMSESSION Cookie の名前を SESSIONSIGNOUT に変更して、現在のユーザ セッションを無効にします。 **ログ メッセージ：** Renaming session cookie to sessionsignout cookie. **チェックポイント コード：** [SLO_SESSION_RENAME]
	2. IdP FWS アプリケーションは SESSIONSIGNOUT Cookie から SessionID 値を読み取り、ユーザ セッションを終了するために IdP ポリシー サーバにリクエストを送信します。 **ログ メッセージ：** Fetching session details from cookie. **チェックポイント コード：** [SLO_SESSION_FETCH] リクエスト タイプ（GET または POST）に応じて、対応するチェックポイント メッセージの 1 つがログに記録されます。 **ログ メッセージ：** Receiving request at SAML2 SLO Logout URL through GET method. **チェックポイント コード：** [SLOSAML2_LOGOUTSERVICEGET_RECEIVE] または **ログ メッセージ：** Receiving request at SAML2 SLO Logout URL through POST method. **チェックポイント コード：** [SLOSAML2_LOGOUTSERVICEPOST_RECEIVE]
	3. IdP ポリシー サーバは、ユーザがログインした SP をすべて特定します。

アクター	トランザクション プロセス
	4. セッション ストア情報に基づいて、リスト内の最初の SP のユーザ セッション ステータスが LogoutInProgress 状態に変更されます。 ポリシー サーバが、SP でユーザ セッションを無効にする、LogoutRequest リクエストを生成します。 **ログ メッセージ：** Generating SAML LogoutRequest. **チェックポイント コード：** [SLO_LOGOUTREQUEST_GEN]
	5. ポリシー サーバが IdP FWS に LogoutRequest リクエストを返します。また、ポリシー サーバは、SP のプロバイダ ID およびプロバイダ タイプを返します。 **ログ メッセージ：** Generating SAML LogoutRequest. **チェックポイント コード：** [SLO_LOGOUTREQUEST_GEN]
	6. IdP FWS アプリケーションは、ポリシー サーバから SP のプロバイダ設定データを取得します。このデータには、SP での SLO サービス URL が含まれます。 **ログ メッセージ：** Fetching provider information. **チェックポイント コード：** [SLOSAML2_PROVIDERINFO_FETCH]
	7. IdP FWS アプリケーションは、LogoutRequest メッセージがクエリ パラメータとして追加された SP SLO サービスにユーザをリダイレクトします。 **ログ メッセージ：** Redirecting to service providers single logout service url. **チェックポイント コード：** [SLOSAML2_SPSLOSERVICEURL_FORWARD]
ユーザ エージェント（ブラウザ）	8. ブラウザが SP の SLO サービスにアクセスします。

アクター	トランザクション プロセス
SP としての SiteMinder	9. SP FWS アプリケーションは LogoutRequest メッセージを受信し処理します。 **ログ メッセージ：** Receiving request at SAML2 SLO Logout URL through GET method. **チェックポイント コード：** [SLOSAML2_LOGOUTSERVICEGET_RECEIVE] または **ログ メッセージ：** Receiving request at SAML2 SLO Logout URL through POST method. **チェックポイント コード：** [SLOSAML2_LOGOUTSERVICEPOST_RECEIVE] SP は、SMSESSION Cookie の名前を SESSIONSIGNOUT へ変更します。 **ログ メッセージ：** Renaming session cookie to sessionsignout cookie. **チェックポイント コード：** [SLO_SESSION_RENAME]
	10. SP はセッション ストアからユーザ セッションを削除します。 **ログ メッセージ：** Logging out session cookie. **チェックポイント コード：** [SLO_SESSIONCOOKIE_LOGOUT] **ログ メッセージ：** Terminating user session from session store. **チェックポイント コード：** [SLO_USERSESSION_TERMINATE]
	11. SP ポリシー サーバは、署名された LogoutResponse メッセージを SP FWS アプリケーションへ返します。 このレスポンスには、IdP のプロバイダ ID およびプロバイダ タイプが含まれています。 ポリシー サーバは、またユーザ セッションがセッション ストアにもうないことをアプリケーションに伝えます。 **ログ メッセージ：** Generating SAML LogoutResponse. **チェックポイント コード：** [SLO_LOGOUTRESPONSE_GEN]
	12. ユーザ セッションがセッション ストアから削除されたことを知ると、SP FWS アプリケーションは SESSIONSIGNOUT Cookie を削除します。 **ログ メッセージ：** Terminating user session from session store. **チェックポイント コード：** [SLO_USERSESSION_TERMINATE]

アクター	トランザクション プロセス
	13. SP FWS アプリケーションは、LogoutResponse メッセージがクエリ パラメータとして追加された IdP SLO サービスにユーザをリダイレクトします。 ブラウザは IdP の SLO サービスにアクセスします。 サービス プロバイダは署名された LogoutResponse メッセージを処理します。 **注**: LogoutResponse メッセージに SUCCESS 以外のリターン コードが含まれる場合、SP は SIGNOUTFAILURE Cookie を発行します。 base 64 でエンコードされたパートナー ID は、Cookie 値に追加されます。 Cookie に複数の ID がある場合は、スペース文字で区切られます。 **ログ メッセージ：** Redirecting to identity provider single logout service url. **チェックポイント コード：** [SLOSAML2_IDPSLOSERVICEURL_FORWARD]
IdP としての SiteMinder	14. IdP ポリシー サーバは LogoutResponse メッセージを受信し、処理します。
	15. SP ポリシー サーバがセッション ストアからユーザ セッションを削除します。 **ログ メッセージ：** Terminating user session from session store. **チェックポイント コード：** [SLO_USERSESSION_TERMINATE]
	16. IdP ポリシー サーバは追加の SP があるか確認します。 追加の SP がある場合、フローは手順 4 から繰り返されます。 それ以外の場合、プロセスは次の手順に移動します。
	17. セッションがセッション ストアから削除された後、IdP ポリシー サーバは FWS アプリケーションに SUCCESS リターン コードを送信します。 ポリシー サーバは最後の LogoutResponse メッセージに SP ID を含めます。
	18. 処理する LogoutRequest または LogoutResponse のメッセージがそれ以上ない場合、IdP FWS アプリケーションは SESSIONSIGNOUT Cookie を削除します。
	19. ブラウザはユーザを SP のログアウト確認ページにリダイレクトします。 **ログ メッセージ：** Redirecting to SLO confirmation URL. **チェックポイント コード：** [SLOSAML2_LOGOUTCONFIRMURL_REDIRECT] **ログ メッセージ：** Displaying local logout message / URL. **チェックポイント コード：** [SLO_LOCALLOGOUT_DISPLAY]

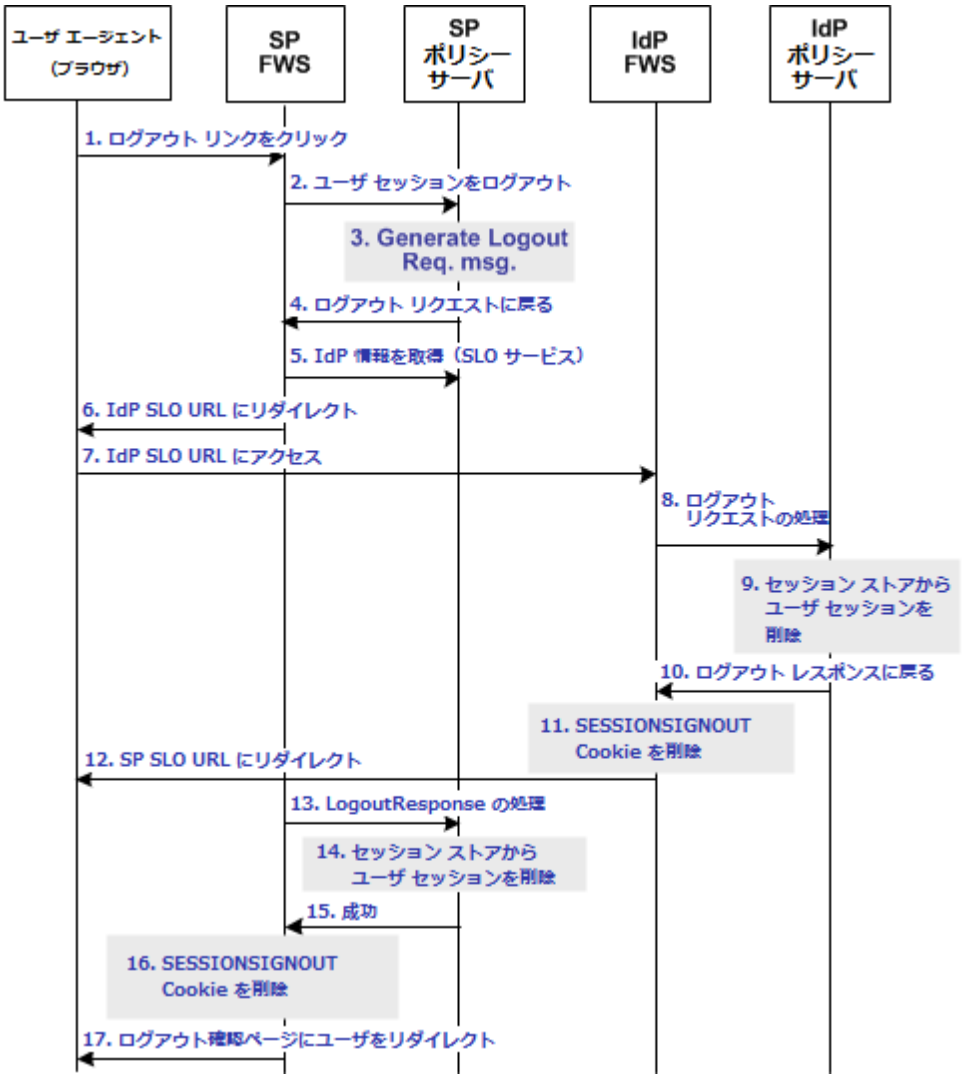
SAML 2.0 シングル ログアウト トランザクション フロー（SP で開始された）

以下の図は、ユーザと SiteMinder アイデンティティ プロバイダ（IdP）およびサービス プロバイダ（SP）で展開されているコンポーネントの間のシングル ログアウト（SLO）リクエストの詳細なフローを示しています。 このフローは、特定のユーザとセッションを行うすべてのエンティティのシングル ログアウトを示しています。

このフローチャートでは以下の情報を想定しています。

- SP はログアウト リクエストを開始します。
- HTTP-Redirect バインディングは使用中です。
- 各パートナーでプロセスを参照できるように、SiteMinder は IdP および SP のみとして表示されます。 SiteMinder が環境内の SP である場合は、テーブル内の SP アクティビティを確認します。 SiteMinder が IDP である場合は、テーブル内の IdP アクティビティを確認します。

以下の図は、SLO トランザクション フローを示しています。



注: SPS フェデレーション ゲートウェイは、Web エージェントおよび Web エージェント オプション パックを置き換えて、FWS アプリケーション機能を提供することができます。SPS フェデレーション ゲートウェイのインストールおよび設定の詳細については、「*CA SiteMinder Secure Proxy Server Administration Guide*」を参照してください。

イベント シーケンスを以下に示します。

アクター	トランザクション プロセス
SP としての SiteMinder	1. ユーザは SP でログアウト リンクをクリックします。 ブラウザは SP でシングル ログアウト サーブレットにアクセスします。 SP FWS アプリケーションは、SMSESSION Cookie の名前を SESSIONSIGNOUT に変更して、現在のユーザ セッションを無効にします。 **ログ メッセージ：** Renaming session cookie to sessionsignout cookie. **チェックポイント コード：** [SLO_SESSION_RENAME]
	2. FWS アプリケーションは SESSIONSIGNOUT Cookie から SessionId 値を読み取り、ユーザ セッションを終了するためにポリシー サーバにリクエストを送信します。 **ログ メッセージ：** Fetching session details from cookie. **チェックポイント コード：** [SLO_SESSION_FETCH] リクエスト タイプ（GET または POST）に応じて、対応するチェックポイント メッセージの 1 つがログに記録されます。 **ログ メッセージ：** Receiving request at SAML2 SLO Logout URL through GET method. **チェックポイント コード：** [SLOSAML2_LOGOUTSERVICEGET_RECEIVE] または **ログ メッセージ：** Receiving request at SAML2 SLO Logout URL through POST method. **チェックポイント コード：** [SLOSAML2_LOGOUTSERVICEPOST_RECEIVE]
	3. セッション ストア情報に基づき、ユーザ セッションのステータスは LogoutInProgress 状態に変更されます。 ポリシー サーバは、IdP から受信されたアサーションに基づいてユーザ セッションが作成されたと判断します。 ポリシー サーバが、IdP でユーザ セッションを無効にする、LogoutRequest リクエストを生成します。 **ログ メッセージ：** Generating SAML LogoutRequest. **チェックポイント コード：** [SLO_LOGOUTREQUEST_GEN] **ログ メッセージ：** Identifying providers associated with user session for single logout. **チェックポイント コード：** [SLO_PROVIDERFORLOGOUT_IDENTIFY]

アクター	トランザクション プロセス
	4. ポリシー サーバが SP FWS に LogoutRequest リクエストを返します。また、ポリシー サーバは、IdP のプロバイダ ID およびプロバイダ タイプを返します。 **ログ メッセージ：** Generating SAML LogoutRequest. **チェックポイント コード：** [SLO_LOGOUTREQUEST_GEN]
	5. SP FWS アプリケーションは、ポリシー サーバから IdP のプロバイダ設定データを取得します。 このデータには、IdP での SLO サービス URL が含まれています。 **ログ メッセージ：** Fetching provider information. **チェックポイント コード：** [SLOSAML2_PROVIDERINFO_FETCH]
	6. SP FWS アプリケーションは、SAML LogoutRequest メッセージがクエリ パラメータとして追加された SLO サービスにユーザをリダイレクトします。 **ログ メッセージ：** Redirecting to identity provider single logout service url. **チェックポイント コード：** [SLOSAML2_IDPSLOSERVICEURL_FORWARD]
ユーザ エージェント（ブラウザ）	ブラウザは IdP の SLO サービスにアクセスします。
IdP としての SiteMinder	7. IdP FWS アプリケーションは LogoutRequest メッセージを受信します。 リクエスト タイプ（GET または POST）に応じて、対応するチェックポイント メッセージの 1 つがログに記録されます。 **ログ メッセージ：** Receiving request at SAML2 SLO Logout URL through GET method. **チェックポイント コード：** [SLOSAML2_LOGOUTSERVICEGET_RECEIVE] または **ログ メッセージ：** Receiving request at SAML2 SLO Logout URL through POST method. **チェックポイント コード：** [SLOSAML2_LOGOUTSERVICEPOST_RECEIVE] IdP は、SMSESSION Cookie の名前を SESSIONSIGNOUT へ変更します。 **ログ メッセージ：** Renaming session cookie to sessionsignout cookie. **チェックポイント コード：** [SLO_SESSION_RENAME]

アクター	トランザクション プロセス
IdP としての SiteMinder （続き）	8. IdP は署名された LogoutRequest メッセージを処理します。 その後、IdP は、そのセッションの間セッション ストアで指定された、すべての SP のユーザ セッションの無効化を試行します。 無効にされないただ一つの SP は、元の LogoutRequest を送信した SP です。 **注**: 各 SP でユーザをログアウトさせる処理は、手順 2 から手順 7 で同じです。 **ログ メッセージ：** Logging out session cookie. **チェックポイント コード：** [SLO_SESSIONCOOKIE_LOGOUT]
	9. すべての関連する SP のユーザ セッションを終了した後に、IdP はセッション ストアからユーザ セッションを削除します。 **ログ メッセージ：** Terminating user session from session store. **チェックポイント コード：** [SLO_USERSESSION_TERMINATE] 10. IdP ポリシー サーバは、署名された LogoutResponse メッセージを IdP FWS アプリケーションへ返します。 このレスポンスには、SP のプロバイダ ID およびプロバイダ タイプが含まれています。 IdP ポリシー サーバは、またユーザ セッションがセッション ストアにもうないことをアプリケーションに伝えます。 **ログ メッセージ：** Generating SAML LogoutResponse. **チェックポイント コード：** [SLO_LOGOUTRESPONSE_GEN]
	11. ユーザ セッションがセッション ストアから削除されたことを知ると、IdP FWS アプリケーションは SESSIONSIGNOUT Cookie を削除します。
	12. IdP FWS は、ユーザを LogoutResponse メッセージがクエリ パラメータとして追加されている SP のシングル ログアウト サービスにリダイレクトします。 ブラウザは SP の SLO サービスにアクセスします。サービス プロバイダは署名された LogoutResponse メッセージを処理します。 **注**: LogoutResponse メッセージに SUCCESS 以外のリターン コードが含まれる場合、SP は SIGNOUTFAILURE Cookie を発行します。また、Base 64 エンコード形式のパートナー ID が Cookie 値に追加されます。 Cookie に複数の ID がある場合は、スペース文字によって区切られます。 **ログ メッセージ：** Redirecting to service providers single logout service url. **チェックポイント コード：** [SLOSAML2_SPSLOSERVICEURL_FORWARD]
SP としての SiteMinder	13. SP ポリシー サーバは FWS アプリケーションから LogoutResponse メッセージを受信し、処理します。

アクター	トランザクション プロセス
SP としての SiteMinder （続き）	14. SP ポリシー サーバがセッション ストアからユーザ セッションを削除します。 **ログ メッセージ：** Terminating user session from session store. **チェックポイント コード：** [SLO_USERSESSION_TERMINATE]
	15. セッションがセッション ストアから削除された後、ポリシー サーバは FWS アプリケーションに SUCCESS リターン コードを送信します。 ポリシー サーバは最後の LogoutResponse メッセージに SP ID を含めます。
	16. 処理する LogoutRequest または LogoutResponse メッセージがそれ以上ない場合、SP FWS アプリケーションは SESSIONSIGNOUT Cookie を削除します。
	17. FWS はユーザを SP のログアウト確認ページにリダイレクトします。 **ログ メッセージ：** Redirecting to SLO confirmation URL. **チェックポイント コード：** [SLOSAML2_LOGOUTCONFIRMURL_REDIRECT] **ログ メッセージ：** Displaying local logout message / URL. **チェックポイント コード：** [SLO_LOCALLOGOUT_DISPLAY]

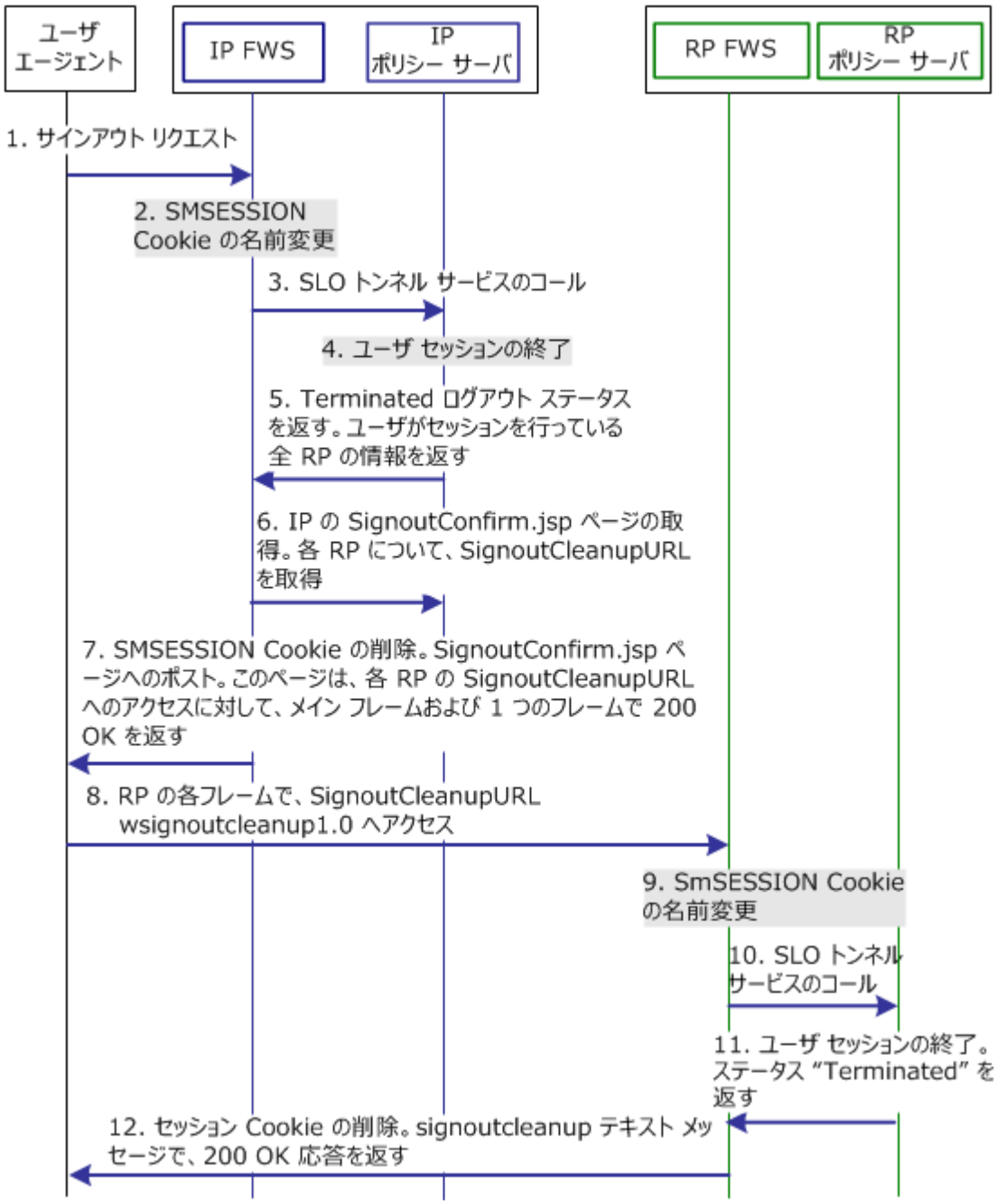
WS-フェデレーション サインアウトトランザクション フロー（IP で開始された）

以下の図は、ユーザとアイデンティティ プロバイダ（IP）およびリソース パートナー（RP）で展開されたコンポーネントの間のサインアウト リクエストのフローを示しています。このフローは、特定のユーザとセッションを行っているすべての WS-フェデレーション エンティティのサインアウト トランザクションを示します。

このフローチャートでは以下の情報を想定しています。

- IP はサインアウト トランザクションを開始します。
- 各パートナーでプロセスを参照できるように、SiteMinder は IP および RP として表示されます。SiteMinder が環境内の IP である場合は、テーブル内の IP アクティビティを確認します。 SiteMinder が RP である場合は、テーブル内の RP アクティビティを確認します。

以下の図は、WS-フェデレーション トランザクション フローを示しています。



注: SPS フェデレーション ゲートウェイは、Web エージェントおよび Web エージェント オプション パックを置き換えて、FWS アプリケーション機能を提供することができます。SPS フェデレーション ゲートウェイのインストールおよび設定の詳細については、「*CA SiteMinder Secure Proxy Server Administration Guide*」を参照してください。

サインアウトがアイデンティティ プロバイダで開始される場合、イベントのシーケンスは以下のとおりです。

アクター	トランザクション プロセス
IP としての SiteMinder	1. ユーザは、グローバル セッションを終了するために、IP でリンクをクリックします。 ブラウザは IP のサインアウト サーブレットに HTTP ベースの wsignout リクエストを送信します。
	2. IP FWS アプリケーションは、SMSESSION Cookie の名前を SESSIONSIGNOUT に変更して、現在のユーザ セッションを無効にします。 **ログ メッセージ：** Renaming session cookie to sessionsignout cookie. **チェックポイント コード：** [SLO_SESSION_RENAME]
	3. IP FWS は SESSIONSIGNOUT Cookie から SessionId 値を読み取り、ユーザ セッションを終了するために SLO Tunnel Service API を呼び出します。 **ログ メッセージ：** Fetching session details from cookie. **チェックポイント メッセージ：** SLO_SESSION_FETCH **ログ メッセージ：** Performing tunnel call for WSFED signout. **チェックポイント コード：** [SLOWSFED_TUNNEL_REQUEST]
	4. SLO Tunnel Service API はセッション ストアでユーザのセッション ステータスを「Terminated」に設定します。 また、サービスは、そのユーザ セッションと関連付けられているすべての RP 参照を削除します。 **ログ メッセージ：** Setting session to inactive assuming a cleanup state. **チェックポイント コード：** [SLOWSFED_INACTIVESTATE_SET]
	5. SLO Tunnel Service API は FWS サインアウト サーブレットにログアウト ステータス「Terminated」 を返します。 さらに、Tunnel ライブラリは、ユーザ セッションと関連付けられたすべての RP の RP providerID および providerType を返します。 **ログ メッセージ：** Terminating user session from session store. **チェックポイント コード：** [SLO_USERSESSION_TERMINATE]
	6. IP FWS は、FWS がメンテナンスするプロバイダのキャッシュから RP のプロバイダ設定データを取得します。この情報には、サインアウト クリーンアップ URL が含まれます。 **ログ メッセージ：** Validate GET request for necessary parameters. **チェックポイント コード：** [SLOWSFED_GETREQUEST_VALIDATE]

アクター	トランザクション プロセス
	7. IP FWS は SESSIONSIGNOUT Cookie を削除してから、IP サインアウト メッセージおよび複数の RP-SignoutCleanup ロケーションを、POST データとして SignoutConfirmURL JSP へポストします。 **ログ メッセージ：** Logging out session cookie. **チェックポイント コード：** [SLO_SESSIONCOOKIE_LOGOUT] SignoutConfirmURL JSP はさまざまなポスト変数を解析し、フレーム ベースの HTML ページを作成します。 この HTML ページのメイン フレームには、IP-SignOut メッセージが表示されます。残りの各フレームは、ユーザ セッションと関連付けられた個別の RP の SignoutCleanupURL にアクセスします。 **ログ メッセージ**: Sending signout message to Identity Provider (Account Partner). **チェックポイント コード：** [SLOWSFED_IDPSIGNOUTMSG_SEND] **ログ メッセージ**: Redirecting to signout confirmation URL **チェックポイント コード：** [SLOWSFED_LOGOUTCONFIRMURL_REDIRECT]
ユーザ エージェント（ブラウザ）	8. ブラウザは RP の SignoutCleanup サービスにアクセスします。
RP としての SiteMinder	9. RP FWS アプリケーションが wsignoutcleanup リクエストを受信すると、SMSESSION Cookie の名前を SESSIONSIGNOUT へ変更します。その後、FWS は、wsignoutcleanup リクエストを処理するために SLO Tunnel Service API を呼び出します。 **ログ メッセージ：** Renaming session cookie to sessionsignout cookie. **チェックポイント コード：** [SLO_SESSION_RENAME] **ログ メッセージ：** Receiving signout request at WSEFD through GET method **チェックポイント コード：** [SLOWSFED_LOGOUTSERVICEGET_RECEIVE]
	10. SLO トンネル ライブラリは wsignoutcleanup リクエストを処理し、セッション ストアからユーザ セッションを終了します。 **ログ メッセージ：** Terminating user session from session store. **チェックポイント コード：** [SLO_USERSESSION_TERMINATE]
	11. SLO トンネル ライブラリは、ユーザ セッションがセッション ストアに存在しなくなったことを示す "Terminated" ステータス メッセージと共に FWS を返します。 **ログ メッセージ：** Logging out session cookie. **チェックポイント コード：** [SLO_SESSIONCOOKIE_LOGOUT]

アクター	トランザクション プロセス
	12. FWS サインアウト サーブレットが SESSIONSIGNOUT Cookie を削除し、フレームで 200 OK 応答を返します。 **ログ メッセージ：** Displaying local logout message / URL. **チェックポイント メッセージ：** [SLO_LOCALLOGOUT_DISPLAY]

注: 手順 8 ～ 12 は、同じ HTML ページの異なるフレームで、個々の RP に対して同時に繰り返されます。

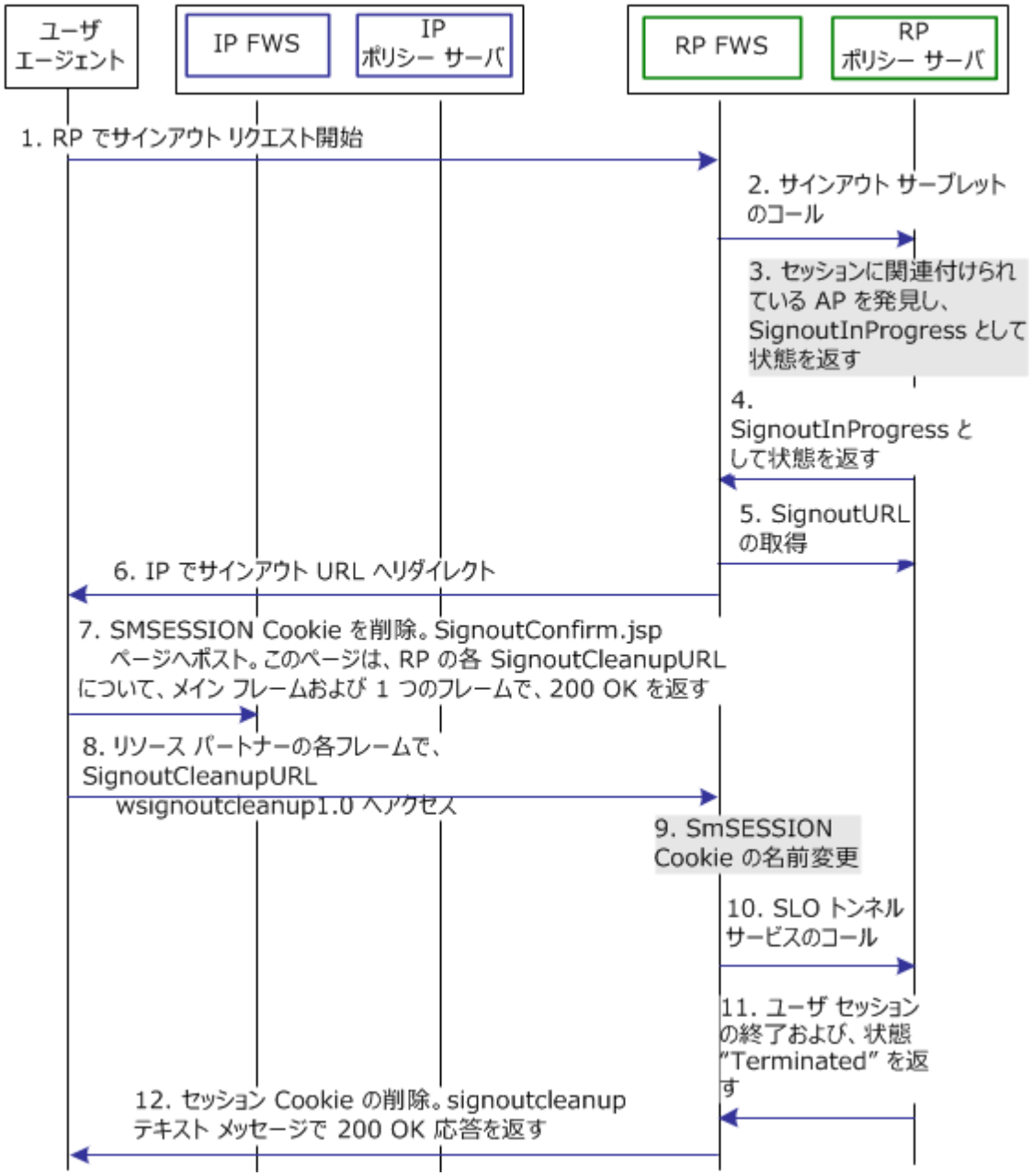
WS-フェデレーション サインアウト トランザクション フロー（RP で開始された）

以下の図は、ユーザとアイデンティティ プロバイダ（IP）およびリソース パートナー（RP）で展開されたコンポーネントの間のサインアウト リクエストのフローを示しています。このフローは、特定のユーザとセッションを行っているすべての WS-フェデレーション エンティティのサインアウト トランザクションを示します。

このフローチャートでは以下の情報を想定しています。

- RP はサインアウト トランザクションを開始します。
- 各パートナーでプロセスを参照できるように、SiteMinder は IP および RP として表示されます。SiteMinder が環境内の IP である場合は、テーブル内の IP アクティビティを確認します。 SiteMinder が RP である場合は、テーブル内の RP アクティビティを確認します。

以下の図は、サインアウト リクエスト トランザクション フローを示しています。



注: SPS フェデレーション ゲートウェイは、Web エージェントおよび Web エージェント オプション パックを置き換えて、FWS アプリケーション機能を提供することができます。SPS フェデレーション ゲートウェイのインストールおよび設定の詳細については、「*CA SiteMinder Secure Proxy Server Administration Guide*」を参照してください。

サインアウトがリソース パートナーで開始される場合、そのプロセス フローは以下のとおりです。

アクター	トランザクション プロセス
RP としての SiteMinder	1. ユーザは、グローバル セッションを終了するためにリソース パートナーでリンクをクリックします。 ブラウザがアカウント パートナーの Signout サーブレットに HTTP ベースの wsignout リクエストを送信します。 **注**: RP サイトは wsignoutcleanup メッセージではなく wsignout メッセージを受信しています。
	2. RP FWS アプリケーションは SMSESSION Cookie から SessionId 値を読み取ります。 アプリケーションは SMSESSION Cookie の名前を SESSIONSIGNOUT へ変更し、wsignout リクエストで SLO トンネル ライブラリをコールします。 **ログ メッセージ：** Renaming session cookie to sessionsignout cookie. **チェックポイント コード：** [SLO_SESSION_RENAME] **ログ メッセージ：** Performing tunnel call for WSFED signout. **チェックポイント コード：** [SLOWSFED_TUNNEL_REQUEST]
	3. セッション ストアの情報に基づいて、トンネル ライブラリはユーザ セッションに関連付けられた IP を判別します。 SLO トンネル ライブラリはユーザ セッションの状態を SignoutInProgress に設定しますが、これを終了しません。 **ログ メッセージ：** Sending signout message and awaiting response from ap for cleanup. **チェックポイント コード：** [SLOWSFED_AWAITINGRESPONSE_SEND]
	4. トンネル ライブラリは SignoutInProgress 状態メッセージ、IP providerID および providerType を返します。 **ログ メッセージ：** Performing tunnel call for WSFED signout. **チェックポイント コード：** [SLOWSFED_TUNNEL_REQUEST]
	5. RP FWS アプリケーションは IP 設定データを取得します。このデータには、FWS キャッシュまたはポリシー サーバからのサインアウト URL が含まれています。

アクター	トランザクション プロセス
	6. RP FWS アプリケーションは、ブラウザをサインアウト URL へリダイレクトします。 RP FWS（Signout サーブレット）が wsignoutcleanup リクエストを受信すると、SMSESSION Cookie の名前を SESSIONSIGNOUT へ変更します。その後、サービスは wsignoutcleanup リクエストを処理するために SLO Tunnel Service API を呼び出します。 **ログ メッセージ：** Redirecting to signout confirmation URL. **チェックポイント コード：** [SLOWSFED_LOGOUTCONFIRMURL_REDIRECT]
IP としての SiteMinder	7. IP FWS アプリケーションは SESSIONSIGNOUT Cookie を削除してから、IP サインアウト メッセージおよび複数の RP-SignoutCleanup ロケーションを、POST データとして SignoutConfirmURL JSP へポストします。 SignoutConfirmURL JSP はさまざまなポスト変数を解析し、フレーム ベースの HTML ページを作成します。 この HTML ページのプライマリ フレームに IP-SignOut メッセージが表示されます。 残りの各フレームは、ユーザ セッションと関連付けられた個別の RP の SignoutCleanupURL にアクセスします。 **ログ メッセージ：** Sending signout message and awaiting response from ap for cleanup. **チェックポイント コード：** [SLOWSFED_AWAITINGRESPONSE_SEND] **ログ メッセージ：** Sending signout cleanup message. **チェックポイント コード：** [SLOWSFED_CLEANUPMESSAGE_SEND]
ユーザ エージェント（ブラウザ）	8. ブラウザが個々のフレームで、リソース パートナー サイトの SignoutCleanup サービスにアクセスします。
RP としての SiteMinder （続き）	9. RP FWS（Signout サーブレット）が wsignoutcleanup リクエストを受信すると、SMSESSION Cookie の名前を SESSIONSIGNOUT へ変更します。その後、サービスは wsignoutcleanup リクエストを処理するために SLO Tunnel Service API を呼び出します。 **ログ メッセージ：** Renaming session cookie to sessionsignout cookie. **チェックポイント コード：** [SLO_SESSION_RENAME]

アクター	トランザクション プロセス
	10. SLO トンネル ライブラリは wsignoutcleanup リクエストを処理し、セッション ストアからユーザ セッションを終了します。 **ログ メッセージ：** Terminating user session from session store. **チェックポイント コード：** [SLO_USERSESSION_TERMINATE] 11. その後、SLO トンネル ライブラリは、ユーザ セッションがセッション ストアに存在しなくなったことを示す「Terminated」ステータス メッセージにより FWS を返します。 **ログ メッセージ：** Redirecting to signout confirmation URL. **チェックポイント コード：** [SLOWSFED_LOGOUTCONFIRMURL_REDIRECT]
	12. FWS サインアウト サーブレットが SESSIONSIGNOUT Cookie を削除し、フレームで 200 OK 応答を返します。 **ログ メッセージ：** Displaying local logout message / URL. **チェックポイント メッセージ：** [SLO_LOCALLOGOUT_DISPLAY]

注: 手順 8 ～ 12 は、同じ HTML ページの異なるフレームで、個々の RP に対して同時に繰り返されます。

アイデンティティ プロバイダ ディスカバリ トランザクション フロー

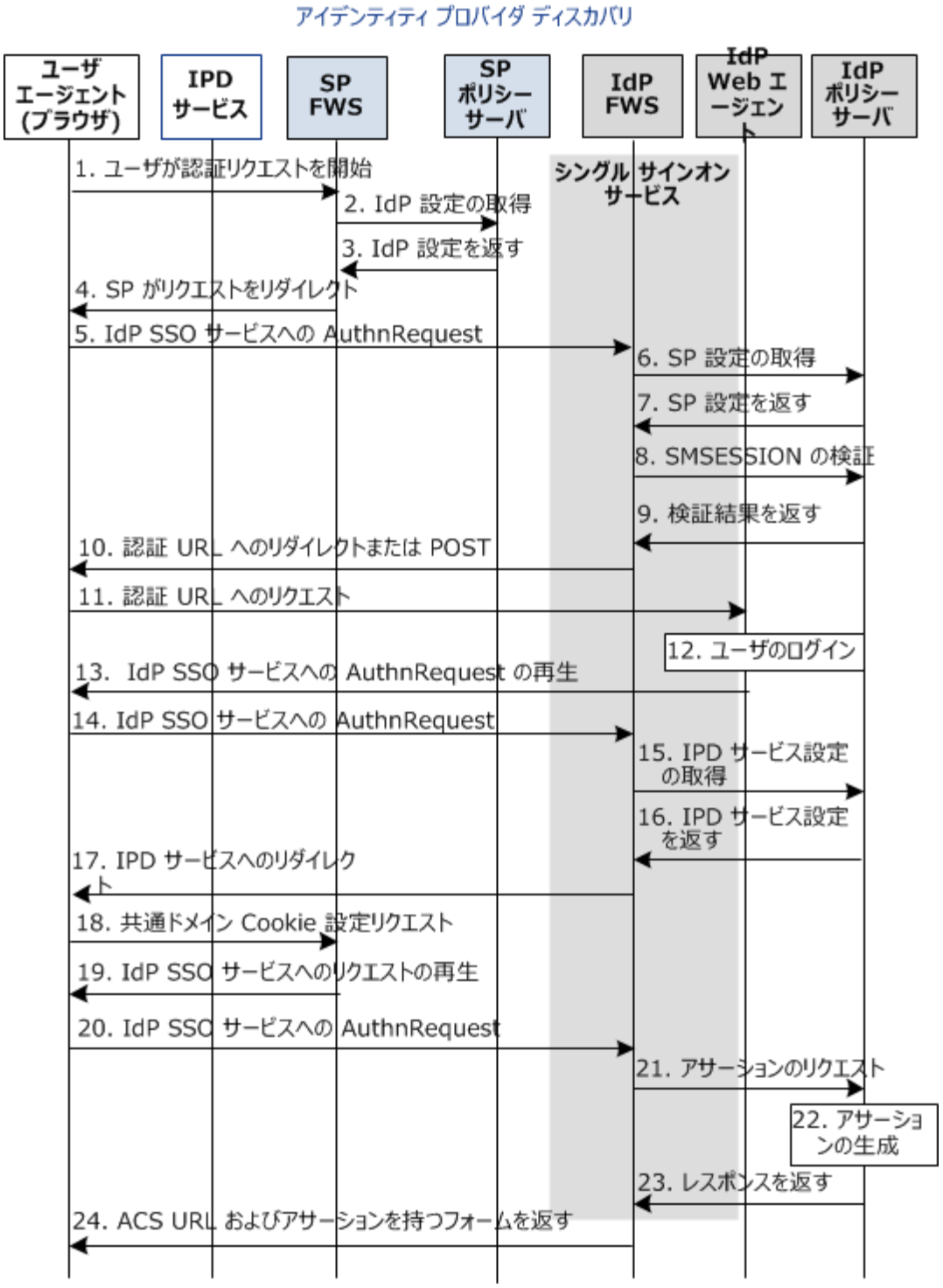
以下の図は、アイデンティティ プロバイダ ディスカバリ プロファイルを使用した、シングル サインオン トランザクションのフローを示しています。 アイデンティティ プロバイダ ディスカバリ（IPD）プロファイルは、共通の検出サービスを提供し、これを使用して、サービス プロバイダが認証用の固有の IdP を選択できます。パートナー間では前もって業務提携契約が確立され、ネットワーク内のすべてのサイトがアイデンティティ プロバイダ ディスカバリ サービスとやり取りできるようになります。

この図で、アイデンティティ プロバイダ ディスカバリ サービスは、SiteMinder アイデンティティ プロバイダでユーザとフェデレーション コンポーネントの間に位置します。このフローは、共通のドメイン Cookie を設定するために、アイデンティティ プロバイダからアイデンティティ プロバイダ ディスカバリ サービスにリクエストをリダイレクトします。

このフローチャートでは以下の情報を想定しています。

- SP FWS は、トランザクションを開始するために、ユーザを IdP SSO サービス URL にリダイレクトします。
- SAML 2.0 HTTP POST はシングル サインオン プロファイルです。
- 各パートナーでプロセスを参照できるように、SiteMinder は IdP として表示されます。

以下の図は、アイデンティティ プロバイダ ディスカバリ トランザクションのフローを示しています。


アイデンティティ プロバイダ ディスカバリ
ユーザ エージェント (ブラウザ)
IPD サービス
SP FWS
SP ポリシー サーバ
IdP FWS
IdP Web エージェント
IdP ポリシー サーバ
シングル サインオン サービス
1. ユーザが認証リクエストを開始
2. IdP 設定の取得
3. IdP 設定を返す
4. SP がリクエストをリダイレクト
5. IdP SSO サービスへの AuthnRequest
6. SP 設定の取得
7. SP 設定を返す
8. SMSESSION の検証
9. 検証結果を返す
10. 認証 URL へのリダイレクトまたは POST
11. 認証 URL へのリクエスト
12. ユーザのログイン
13. IdP SSO サービスへの AuthnRequest の再生
14. IdP SSO サービスへの AuthnRequest
15. IPD サービス設定の取得
16. IPD サービス設定を返す
17. IPD サービスへのリダイレクト
18. 共通ドメイン Cookie 設定リクエスト
19. IdP SSO サービスへのリクエストの再生
20. IdP SSO サービスへの AuthnRequest
21. アサーションのリクエスト
22. アサーションの生成
23. レスポンスを返す
24. ACS URL およびアサーションを持つフォームを返す

注: SPS フェデレーション ゲートウェイは、Web エージェント Web エージェント オプション パックを置き換えて、フェデレーション Web サービス アプリケーション機能を提供できます。 フロー図では、Web エージェント ブロックは SPS フェデレーション ゲートウェイに組み込まれた Web エージェントになります。 SPS フェデレーション ゲートウェイをインストールするおよび設定する詳細については、「*Secure プロキシ サーバ管理ガイド*」（Secure Proxy Server Administration Guide）を参照してください。

アイデンティティ プロバイダ ディスカバリ プロセスを以下に示します。

アクター	トランザクション プロセス
ユーザ エージェント（ブラウザ）	1. ユーザは、認証リクエストを開始するためにリンクをクリックします。
SP としての SiteMinder	2. SP FWS がローカル ポリシー サーバの IdP 設定情報をリクエストします。 **ログ メッセージ：** Reading SAML 2.0 IDP Configuration **チェックポイント コード：** [SSOSAML2_IDPCONFREAD_REQ]
	3. ローカル ポリシー サーバが設定情報を返します。 **注**: SP FWS アプリケーションは設定情報をキャッシュできます。 **ログ メッセージ：** Policy server returns SAML2.0 IDP Configuration **チェックポイント コード：** [SSOSAML2_IDPCONFFROMPS_RSP]
	4. SP FWS は、リクエストをブラウザへリダイレクトします。
ユーザ エージェント（ブラウザ）	5. ユーザ エージェント（ブラウザ）は IdP SSO サービスをリクエストします。
IdP としての SiteMinder	6. IdP FWS がローカル ポリシー サーバの SP 設定情報をリクエストします。 **ログ メッセージ：** SAML2.0 SP Configuration is not in cache. Requesting to get from policy server. **チェックポイント コード：** [SSOSAML2_SPCONFFROMPS_REQ]
	7. ローカル ポリシー サーバが設定情報を返します。 **注**: IdP FWS アプリケーションは設定情報をキャッシュできます。 **ログ メッセージ：** Policy server returns SAML2.0 SP Configuration. **チェックポイント コード：** [SSOSAML2_SPCONFFROMPS_RSP]

アクター	トランザクション プロセス
	8. IdP FWS は、IdP ドメイン用 SMSESSION Cookie を取得し、それを検証するためにポリシー サーバを呼び出します。 SMSESSION Cookie がない場合、IdP FWS は手順 6 にスキップします。 **ログ メッセージ：** Request to validate the session. **チェックポイント コード：** [SSOSAML2_SESSIONCOOKIEVALIDATE_REQ]
	9. ポリシー サーバは、SMSESSION Cookie を検証し、結果を返します。
	10. SMSESSION Cookie が存在しないか有効でない場合、IdP FWS は設定から取得した認証 URL へリダイレクトするか、ポストします。 SMSESSION Cookie が有効な場合、IdP FWS は手順 18 にスキップします。 **ログ メッセージ：** Session cookie does not exists. redirecting to authentication url **チェックポイント コード：** [SSOSAML2_AUTHENTICATIONURL_REDIRECT]
ユーザ エージェント（ブラウザ）	11. ブラウザは認証 URL をリクエストします。 IdP Web エージェントが認証 URL を保護します。
IdP としての SiteMinder	12. IdP Web エージェントは SMSESSION Cookie を設定してユーザをログインさせ、リクエストを認証 URL に渡します。
	13. 認証 URL は、AuthnRequest メッセージで IdP SSO サービスへのリクエストを再生します。 **ログ メッセージ：** Policy server returns the authentication request **チェックポイント コード：** [SSOSAML2_GETAUTHENTICATIONREQFROMPS_RSP] **ログ メッセージ：** Service redirecting to SSO URL **チェックポイント コード：** [SSOSAML2_SSOURL_REDIRECT]
ユーザ エージェント（ブラウザ）	14. ブラウザは IdP SSO サービスをリクエストします。 このリクエストは手順 8 のリクエストと同じですが、今度はユーザには有効な SMSESSION Cookie があります。
IdP としての SiteMinder	15. IdP FWS はアイデンティティ プロバイダの ID を渡すことにより、ポリシー サーバにアイデンティティ プロバイダ ディスカバリ プロファイル（IPD）設定をリクエストします。 **ログ メッセージ：** Request for IPD configuration **チェックポイント コード：** [SSOIPD_READIPDCONF_REQ]

アクター	トランザクション プロセス
	16. ポリシー サーバは、IPD 設定（IPD サービス URL、共通ドメイン Cookie、および共通ドメイン Cookie の永続性情報など）を返します。 **ログ メッセージ：** Reading IPD service URL from configuration **チェックポイント コード：** [SSOIPD_READIPDSERVICEURL_REQ] **ログ メッセージ：** Reading common domain cookie from configuration **チェックポイント コード：** [SSOIPD_READCOMMONDOMAINCOOKIE_REQ] **ログ メッセージ：** Reading persistence information of the common domain cookie **チェックポイント コード：** [SSOIPD_READPERSISTENCEINFOFORCOMMONCOOKIE_REQ]
	17. IdP FWS はコールを IPD サービス URL にリダイレクトします。 **ログ メッセージ：** Redirecting to IPD service URL **チェックポイント コード：** SSOIPD_REDIRECTTOIPDURL_REQ
ユーザ エージェント（ブラウザ）	18. ブラウザは、共通ドメイン Cookie を設定するために、ユーザを IPD サービスへリダイレクトします。
アイデンティティ プロバイダ ディスカバリ サービス	19. IPD Service はアイデンティティ プロバイダの ID を使用して、共通ドメイン Cookie を設定または更新します。 IPD Service はユーザ エージェントを、Set Request を受信した IdP FWS に再度リダイレクトします。 **ログ メッセージ：** IPD service setting common domain cookie with identity provider id **チェックポイント コード：** [SSOIPD_SETCOMMONDOMAINCOOKIE_REQ]
ユーザ エージェント（ブラウザ）	20. ブラウザは IdP SSO サービスにリクエストを行います。
IdP としての SiteMinder	21. IdP FWS は AuthnRequest を設定から得られたレルムへ、許可呼び出しを通じて渡すことにより、ポリシー サーバの SAML 2.0 アサーションをリクエストします。 **ログ メッセージ：** Request to policy server for generating saml2 assertion/artifact based on selected profile. **チェックポイント コード：** [SSOSAML2_GENERATEASSERTIONORARTIFACT_REQ]

アクター	トランザクション プロセス
	22. ポリシー サーバがサービス プロバイダの設定情報に基づいアサーションを生成します。 ポリシー サーバはアサーションに署名し、応答メッセージでアサーションを返します。 **ログ メッセージ：** Policy server generates the saml2 assertion **チェックポイント コード：** [SSOSAML2_PSGENERATEASSERTION_RSP] **ログ メッセージ：** Policy server signs saml2 assertion **チェックポイント コード：** [SSOSAML2_PSSIGNASSERTION_RSP]
	23. 応答メッセージが Idp FWS に返されます。 **ログ メッセージ：** Received the assertion/artifact response based on profile selected. **チェックポイント コード：** [SSOSAML2_RECEIVEDASSERTION_RSP]
	24. IdP FWS はユーザに、応答メッセージ、設定から取得されるアサーション コンシューマ URL およびフォームをサブミットするための Javascript が含まれるフォームを返します。 **ログ メッセージ：** Browser posting the response to assertion consumer url **チェックポイント コード：** SSOSAML2_POSTASSERTIONTOCONSUMERURL_RSP **注**: ポリシー サーバは、現行セッションの認証レベルが低すぎることを指摘できます。 レベルが低すぎる場合、IdP FWS はステップアップ認証を促すために認証 URL へリダイレクトします。

図の最終手順の後、ユーザ エージェントは、サービス プロバイダのアサーション コンシューマ URL へ応答メッセージをポストします。