HP IceWall技術レポート:

HP IceWall Federationを用いたパブリッククラウドサービスへの シングルサインオン(認証連携)- Salesforce編 -

1. はじめに

近年、企業は業務を遂行するために、社内システム以外にSalesforceなどのパブリッククラウドサービス(SaaS)を利用する事例が増えてきました。一方、IT環境としては、社内ITサービスとこれらのクラウドサービスが混在し、複雑化することで、セキュリティの確保と利便性の両立が大きな課題になっています。
その解決策の1つとして、大きな注目を浴びているのが、「認証連携」もしくは「フェデレーション」と呼ばれるソリューションです。

認証連携ソリューションを使用すると、ユーザーは社内システムもしくはクラウドサービスのいずれかで一度ログインすれば、いずれのサービスもシームレスに使用することができます。すなわち、通常、各々のサービスを使用する度に求められる都度のログイン/認証は不要となり、社内システムとクラウドサービスの間でシングルサインオンを実現することで、複雑なIT環境においてもセキュリティの確保と利便性を両立することができるのです。

本レポートではHP IceWall SSOと認証連携ソリューション製品であるHP IceWall Federationを用いてSalesforceとの認証連携を導入することによってもたらされるメリットと、Salesforceが提供するユーザープロビジョニングツールである「ジャストインタイムプロビジョニング」を利用した、容易なアカウント情報の登録方法についてご紹介します。

2. HP IceWall Federation導入によるメリットと認証連携シナリオ

HP IceWall Federationによる認証連携を導入していない状態では、ユーザーがHP IceWall SSOのバックエンドにあるWebサーバーへアクセスする場合(図1①)も、Salesforceにアクセスする場合(図1②)も、それぞれにユーザーIDとパスワードを入力し、ログインする必要があります。

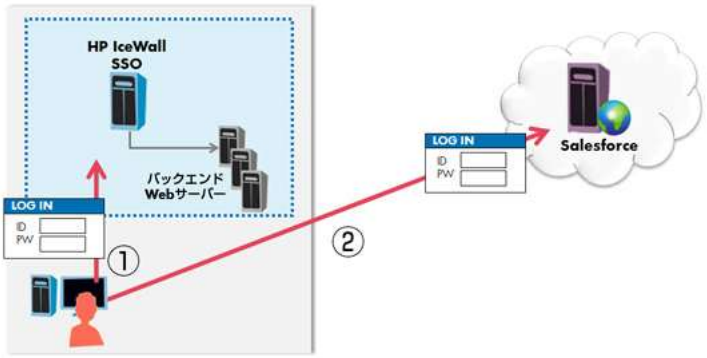

図1 HP IceWall Federation 導入前の利用フロー

① バックエンドWebサーバーにアクセスする場合、HP IceWall SSOのユーザーID・パスワードを入力してログインします。
② ユーザーは、Salesforceにアクセスする場合、Salesforceのユーザー ID・パスワードを入力してログインします。

HP IceWall Federationを導入すると、HP IceWall SSOへのログインにより、バックエンドWebサーバーへのアクセスと同様にSalesforceにもユーザーIDとパスワードを入力することなくアクセスできます。

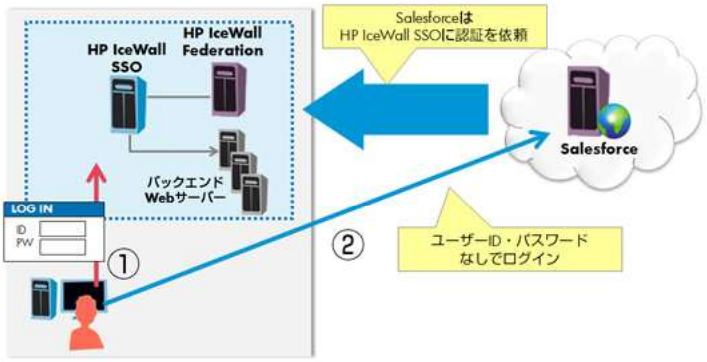

図2 HP IceWall Federation 導入後の利用フロー

① ユーザーは、バックエンドWebサーバーにアクセスする場合、HP IceWall SSOのユーザーID・パスワードを入力してログインします。
② ユーザーは、すでにHP IceWall SSOにログイン済みならばSalesforceにはユーザーID・パスワードなしでログインできるようになります。

以下、3つのシナリオに沿って、HP IceWall FederationとSalesforceの認証連携を解説します。

2.1.[シナリオ1] 社内ポータルなどのリンクからSalesforceにアクセス

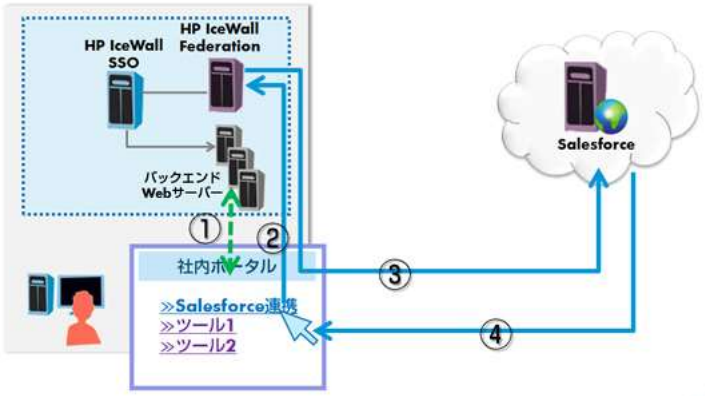

図3 社内ポータルからアクセス

イントラネットにログインしている状態で、社内ポータルサイト内のリンクをクリックして、Salesforceへ認証連携する利用形態を見てみましょう。ユーザーはHP IceWall SSOにはログイン済み、Salesforceには未ログインだとします（図3①）。HP IceWall SSOのバックエンドWebアプリケーションの1つとして構築されたHP IceWall Federationに、「salesforce連携」のリンクからアクセスします（図3②）。
HP IceWall SSOにログイン済みなので、HP IceWall FederationはSalesforceとの認証連携を行い（図3③）、SalesforceユーザーIDとパスワードを入力することなく利用できるようになります（図3④）。

2．2．[シナリオ2] メールのリンクをクリックしてSalesforceにアクセス

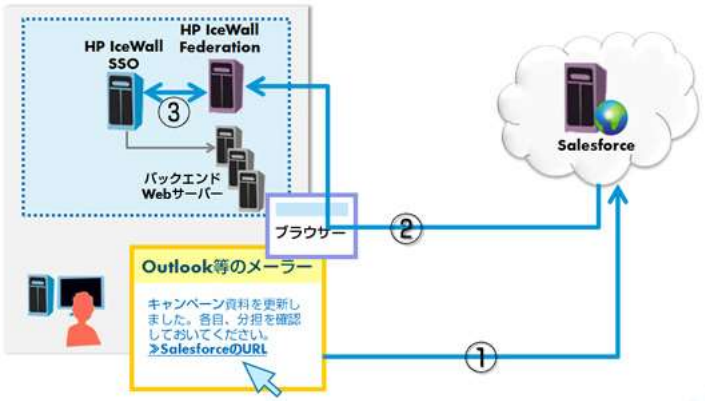

図4-1 メールのリンクからアクセス：ログイン前のアクセス時

イントラネットのユーザーが、まだHP IceWall SSOにもSalesforceにもログインしておらず、ユーザーが受信したメールにSalesforceへのリンクを埋め込んでいる場合を想定しています。ユーザーがメール内のリンクをクリックしてSalesforce側にアクセスしようとすると（図4-1①）、Salesforceは、HP IceWall Federationに認証を求めるため、ユーザーにリダイレクトレスポンスを返します（図4-1②）。リダイレクト先のHP IceWall Federationは、ユーザーがHP IceWall SSOにログインしていないことを確認し（図4-1③）、HP IceWall SSOへのログインを求めます（図4-2④）。

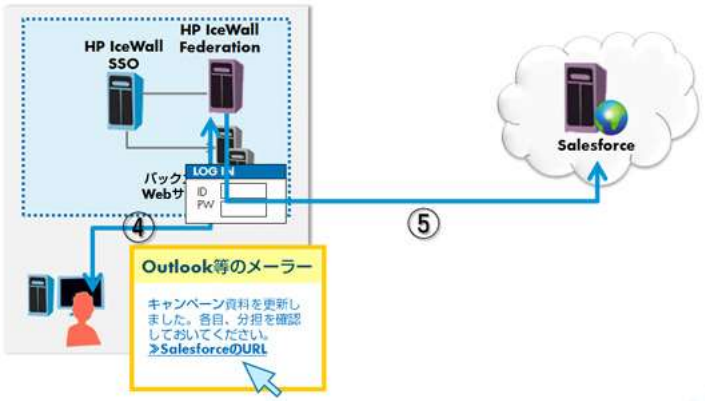

図4-2 メールのリンクからアクセス：HP IceWall SSOへのログインと認証連携

HP IceWall SSOにログインすると、HP IceWall Federationが認証連携を実行し、SalesforceではユーザーIDとパスワードを入力することなく、メールのリンク先へアクセスできます（図4-2⑤）。以上のシナリオにより、HP IceWall SSOのユーザーIDとパスワードの入力でSalesforceへアクセスできます。

2．3．[シナリオ3] SalesforceのURLに直接アクセス

イントラネットのユーザーが、まだHP IceWall SSOにもSalesforceにもログインしておらず、ブックマークなどでSalesforce側のURLにアクセスする場合を想定しています。

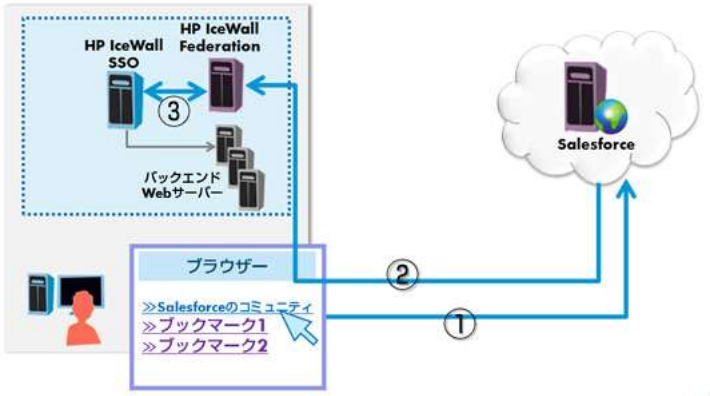

図5-1 ブックマークからアクセス：ログイン前のアクセス時

ユーザーがブラウザーのブックマークにあるSalesforceのコミュニティーページにアクセスしようとすると（図5-1①）、Salesforceは、HP IceWall Federationに認証を求めるため、ユーザーにリダイレクトレスポンスを返します（図5-1②）。

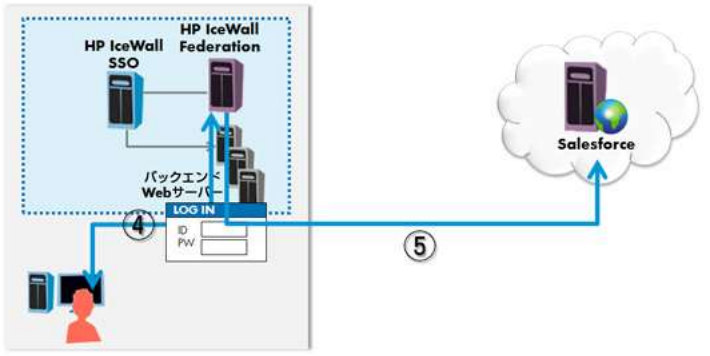

図5-2 ブックマークからアクセス：HP IceWall SSOへのログインと認証連携

以降はシナリオ2と同様、HP IceWall SSOにログインすると、HP IceWall Federationが認証連携を実行し、Salesforceではユーザーの IDとパスワードを入力することなく、Salesforceにもアクセスすることができるようになります（図5-1③、図5-2④、⑤）。

3. Salesforceへのユーザーアカウント情報の容易な登録方法

一般的には、クラウドサービスを使用する場合には、事前にクラウドサービスのユーザーIDを登録し、認証連携を行う社内のユーザーIDに紐付けを行っておく必要があります。
Salesforceは、この運用を軽減するために「ジャストインタイムプロビジョニング」というツールを提供しています。
ジャストインタイムプロビジョニングを使用すると、認証連携したシステムのユーザーIDで初めてSalesforceにアクセスした際、Salesforceのユーザー IDの自動登録を行うことができます。

以下に、HP IceWall Federationでジャストインタイムプロビジョニングを使用する場合の動作を説明します。
SalesforceがHP IceWall Federationと認証連携を行う際、HP IceWall Federationはユーザーの認証後、ユーザーのアカウントに対応したSalesforceのユーザーIDをSalesforceに返します。前章で解説したシナリオでは、そのSalesforceのユーザーIDやプロフィール情報（以下、アカウント情報）があらかじめSalesforce側にアカウント登録され、また、HP IceWall SSO側のユーザーのアカウント情報にSalesforceのユーザーIDを紐づけておく必要がありました。
ジャストインタイムプロビジョニングを利用すると、HP IceWall SSO側だけにアカウント情報を登録すれば、Salesforceが認証連携と同時にアカウント登録します。

まずHP IceWall SSOの認証データベースに事前に、認証連携を行うユーザーのSalesforceアカウント情報を登録しておきます（図6-1①）。以降の流れはSalesforceにはアカウント登録を行っていないuser2 を想定します。

図6-1 ジャストインタイムプロビジョニング：HP IceWall SSOの認証データベース設定

user2がSalesforceの所定のURLにアクセスしようとすると（図6-2②）、Salesforceは、HP IceWall Federationに認証を求めるため、user2のブラウザーにリダイレクトレスポンスを返します（図6-2③）。

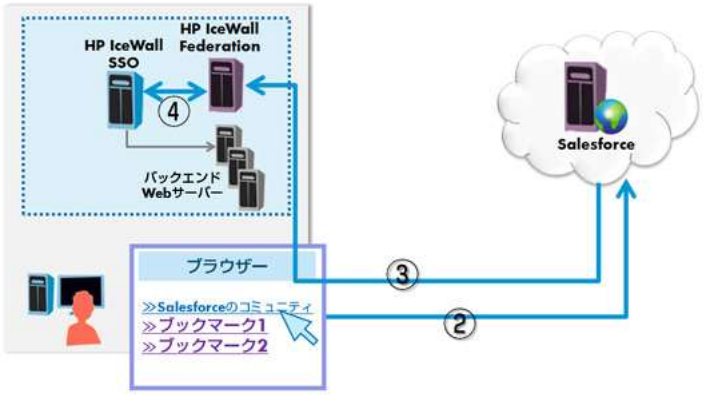

図6-2 ジャストインタイムプロビジョニング：ログイン前のアクセス時

リダイレクト先のHP IceWall Federationはuser2がHP IceWall SSOに認証されているかどうかを確認します（図6-2④）。未認証の場合、user2はHP IceWall SSOのユーザーIDとパスワードを入力してログインします（図6-3⑤）。

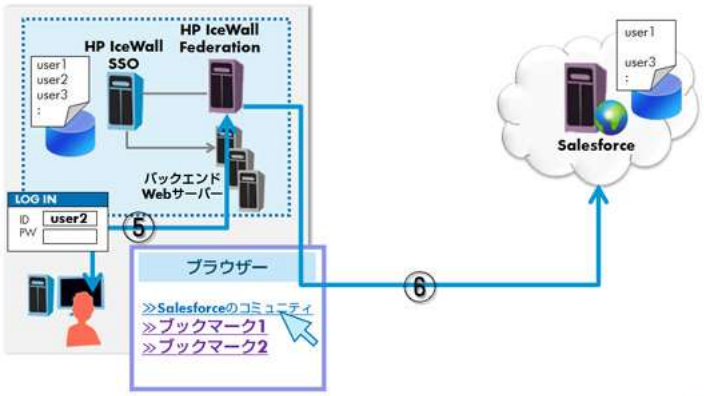

図6-3 ジャストインタイムプロビジョニング：HP IceWall SSOへのログインと認証連携

ここで、HP IceWall FederationはSAML※1レスポンス内に図6-1で設定したuser2のアカウント情報を埋め込み、ブラウザーにリダイレクトさせます（図6-3⑥）。

※1 Security Assertion Markup Language

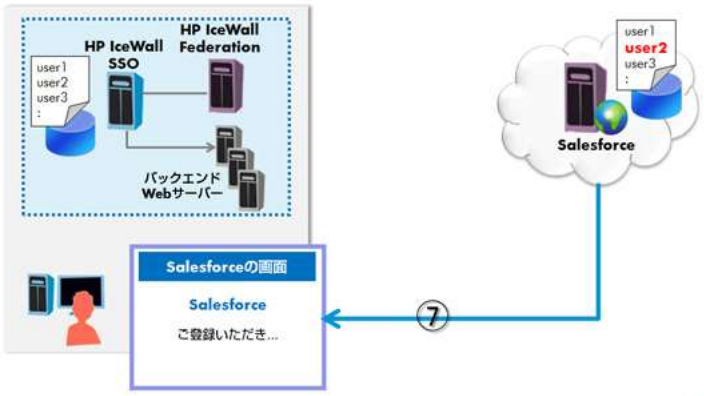

図6-4 ジャストインタイムプロビジョニング：ユーザ登録とログインの完了

Salesforceは、user2のアカウント情報を元に新たにuser2を登録し、ログイン後のページへアクセスさせます（図6-4⑦）。
初回アクセス時のメッセージが出るのでuser2が登録されたことが分かります。user2はHP IceWall SSOにログイン済みなので、アクセス権限が与えられているSalesforceのサービスにアクセスできます。
ここで説明したジャストインタイムプロビジョニングは、2.で挙げたどのシナリオでも活用できます。

4. おわりに

以上、HP IceWall Federationによる認証連携ソリューションを導入することによる3つの動作シナリオとメリットを解説しました。このように認証連携を導入することで、イントラネット内のシステムとクラウド上のSalesforceとのシングルサイオンを実現し、セキュリティの確保と利便性の両立をはかることができます。また、ジャストインタイムプロビジョニングを利用し、Salesforce側へのアカウント情報の登録を自動化することで、運用面の負荷を軽減することが可能です。

このようにHP IceWall製品は、システムのセキュリティの強化、運用負荷の軽減、およびユーザーへの利便性の提供を、今後も幅広くサポートしていきます。

なお、本技術レポートで取り上げたSalesforceとの認証連携機能はHP IceWall Federation 3.0 Patch Release 5にて提供される機能です。

2014.5.15　新規掲載

執筆者　日本ヒューレット・パッカード テクノロジーコンサルティング統括本部
セキュリティスペシャリスト CISSP

久下 哲男