HP IceWall SSOとRSA SecurIDの連携による Webシングルサインオンソリューション

ーワンタイムパスワード 認証の実現ー

1. はじめに

Webシングルサインオン製品であるHP IceWall SSOによって使用できる認証方式には、標準のID/パスワードによる認証とオプションのクライアント証明書による認証があります。それ以外の認証方式、例えば指紋認識などの生体認証、ICカードによる認証等は、サードパーティの認証装置またはシステムと連携して実現することが可能*1です。
HP IceWall SSOには、他のソリューションと組み合わせて様々な機能を提供できる柔軟さを持ち合わせている、大きな特長があります。

今回の記事では、この特長を生かしたソリューションとして、RSAセキュリティ株式会社のRSA SecurIDとHP IceWall SSOと連携したワンタイムパスワード認証の実現について説明します。

*1 以下の製品とHP IceWall SSOとの連携がすでに行われています。

- 日立ソフトウェアエンジニアリング株式会社の指静脈認証「静紋」と連携したソリューション「HP IceWall SSO－日立ソフト静紋連携ソリューション」
  ≫ 詳細はこちら(日本ヒューレット・パッカード外サイトへ)
  ≫ ニュースリリースはこちら(日本ヒューレット・パッカード外サイトへ)
- 株式会社ソリトンシステムズSmartOnによるICカード認証とHP IceWall SSOの連携によるWebシングルサインオンのソリューション
  ≫ 詳細はこちら
- ソフトバンクBB社の多次元マルチ認証プラットフォームSyncLockとHP IceWall SSOとの連携による携帯電話を使用した多次元認証ソリューション
  ≫ 詳細はこちら
- RSAセキュリティ社のRSA Adaptive Authentication for WebとHP IceWall SSOと連携によるオンラインセキュリティ強化ソリューション
  ≫ 詳細はこちら

2. RSA SecurID

ワンタイムパスワードは一回きりでしか使えない「使い捨てパスワード」のことです。通常のID/パスワードの認証では、端末からサーバへアクセスする際にネットワーク上でパスワードを盗聴される危険性があります。
ワンタイムパスワードは1回きりしか有効でないため、たとえ盗聴されても再利用できず安全です。

RSAセキュリティ株式会社のRSA SecurID*2はワンタイムパスワード の代表的な製品です。RSA SecurIDは、トークンと呼ばれるパスコード生成器から生成されるパスコードと、ユーザ固有のPIN (Personal Identification Number) と組み合わせた一見ランダムな数字をワンタイムパスワードとして使用します。

*2 RSA SecurIDの詳細はこちら(日本ヒューレット・パッカード外サイトへ)

3. RSA SecurIDのコンポーネント

HP IceWall SSOと連携するために必要な、RSA SecurIDのコンポーネントは以下のとおりです。

- RSA SecurIDトークン
  ワンタイムパスワードの基となるパスコードを生成する小型機器です。

- RSA Authentication Agent
  各プラットフォーム、デバイスなどをアクセスから保護するエージェントソフトウェアで、ユーザが入力

したユーザIDとトークンによって生成されたパスコードから作られたワンタイムパスワードを受け取り、認証を行うためにRSA Authentication Managerに渡します。

RSA Authentication Agentはプラットフォーム毎にモジュール*3が用意されています。
今回のHP IceWall SSOとの連携には、RSA Authentication Agent for Web (Web Agent) を使用します。

- RSA Authentication Manager（旧名 RSA ACE/Server）
RSA SecurIDの認証サーバです。Authentication Agentから受け取ったユーザIDとワンタイムパスワードで認証を行います。

これらのコンポーネントの中で、HP IceWall SSOとの連携にはWeb Agentが特に重要です。
Web AgentはWeb サーバに組み込まれて動作するPlug-inプログラムです。Apacheサーバで言うモジュールに相当します。Web AgentをWebサーバに組み込むと、ワンタイムパスワードによる認証が成功した後にWebサイト全体または一部のコンテンツにアクセスすることができます。(図1)

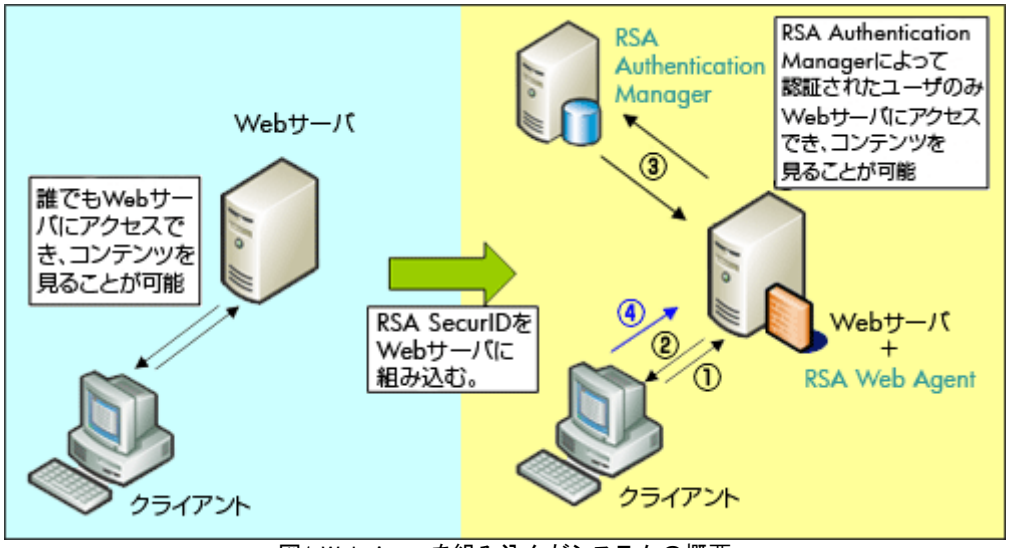

図1 Web Agentを組み込んだシステムの概要

Web Agentを組み込んだWebサーバへのアクセス手順は、以下のとおりです。

1. クライアントからWebサーバへアクセスします。
2. 指定されたURLが認証の対象の場合、Web Agentのログイン画面がクライアントに表示されます。
3. ログイン画面に入力されたユーザIDとワンタイムパスワードがRSA Authentication Managerに送られます。ユーザIDとワンタイムパスワードの照合・認証が行われ、結果がWeb Agentに通知されます。
4. 認証に成功した場合はWebサーバのコンテンツがアクセスでき、失敗した場合はWeb Agentからのエラー画面が表示されます。

詳細は、RSA SecurIDのドキュメントを参照してください。

*3 Webサーバ版の他に、Windows版、UNIX/LINUX版が用意されています。

4. RSA SecurIDとHP IceWall SSO との連携

RSA SecurIDはワンタイムパスワードによる強力な認証を提供する製品です。一方、HP IceWall SSOはコンテンツへのアクセス認可機能、シングルサインオン機能、リバースプロキシ機能、アクセスログ監査等の豊富な機能を提供していますが、認証機能については前述のID/パスワードによる認証とクライアント証明書による認証の機能のみで、ワンタイムパスワードによる認証機能は持っていません。

そこで、HP IceWall SSOの認証機能部分をRSA SecurIDと連携させて、認証機能の強化を図ります。

次章にRSA SecurIDとHP IceWall SSOとの連携例を説明します。

5. HP IceWall SSO とRSA SecurID Web Agentとの連携例（二要素認証）

図 2は、HP IceWall SSOを使ってWebアプリケーションにアクセスする典型的なシステム構成です。
Webアプリケーションは2つのグループに分けられ、セキュリティを強固にする必要がないWebアプリケーション

のグループ1は、従来どおりHP IceWall SSOのID/パスワードでアクセスします。そしてWebアプリケーションのグループ2に対して、RSA SecurID を導入しセキュリティを強固にするケースを想定します。

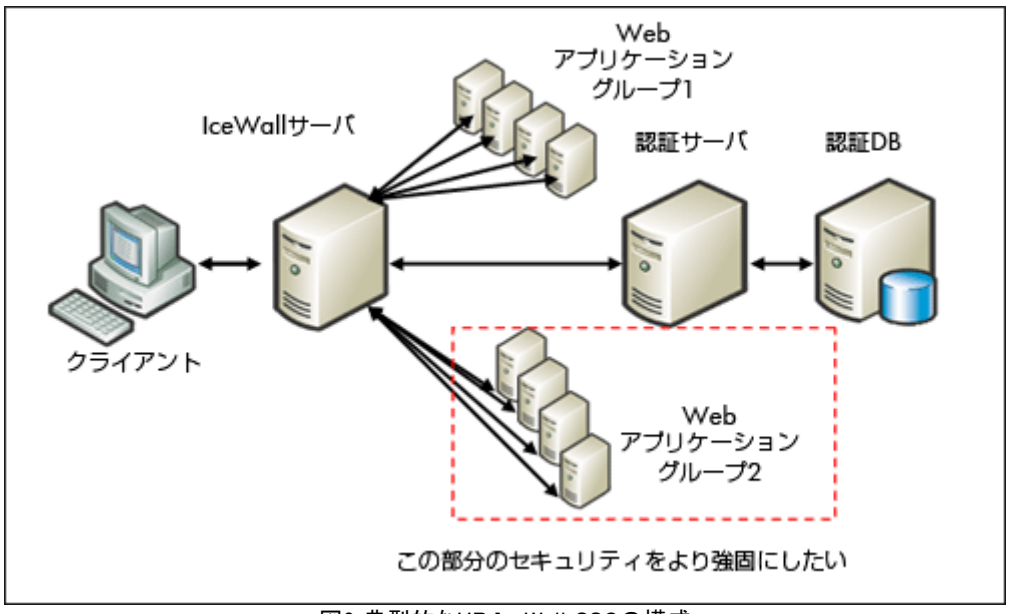

図2 典型的なHP IceWall SSOの構成

セキュリティを高める手段として、二つの異なる要素の認証方式を組み合わせて認証する二要素認証があります。図 3は、HP IceWall SSO のID/パスワードによる認証とRSA SecurIDのワンタイムパスワードによる認証の、二つ異なる要素を組み合わせた二要素認証システムの例です。ここではHP IceWall MCRPを使用しています。HP IceWall MCRPは、リバースプロキシ機能に特化したIceWall製品群のひとつです。
図 3では、IceWall サーバとWebアプリケーションのグループ2との間にWeb AgentとHP IceWall MCRPを組み込んだWebサーバを設置することでセキュリティを強化しています。
クライアントがWebアプリケーションのグループ2にアクセスすると、最初にIceWallサーバでID/パスワードによる認証が行われ、次にWeb Agentでワンタイムパスワードによる認証が行われます。これら二つの要素の認証の照合が成功した後にWebアプリケーションのグループ2へアクセスできます。

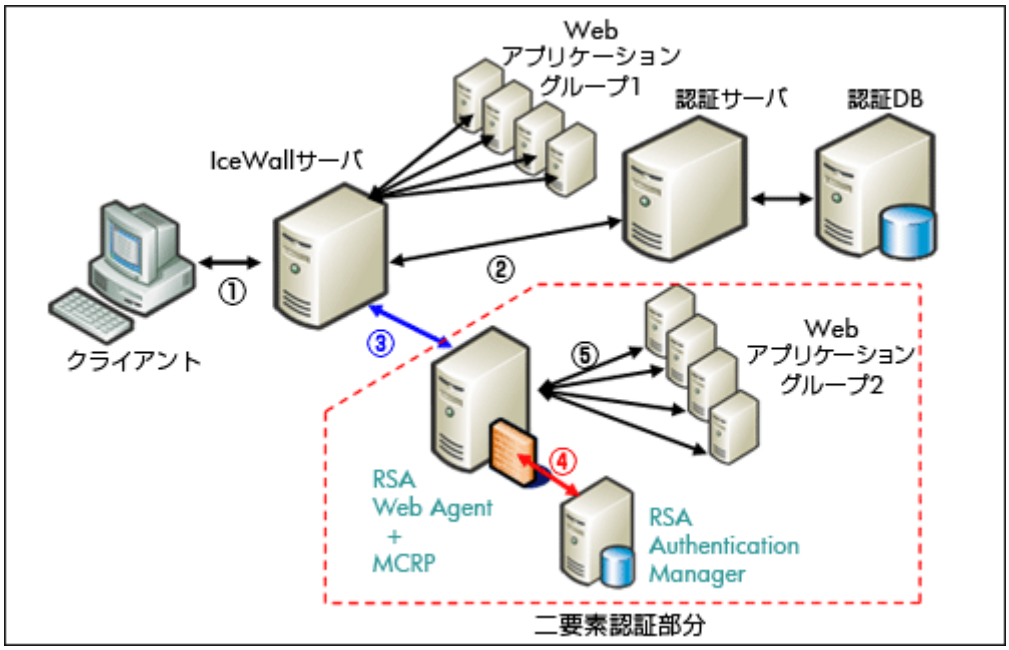

図3 HP IceWall SSOとRSA SecurIDとの連携による二要素認証

クライアントからWebアプリケーショングループ2へアクセス可能になるまでの認証・アクセス認可の流れは以下のとおりです。

1. IceWallサーバ経由でWebアプリケーショングループ2へアクセスしようとします。ユーザがまだ認証されていない場合はIceWallサーバからログイン画面が表示され、ユーザIDとパスワードが入力されます。
2. 入力されたユーザIDとパスワードはIceWallサーバから認証サーバへ送られ、照合・認証が行われます。認証成功後、アクセス先のURLパスに対するアクセス認可許否が行なわれます。
3. アクセス認可成功後、Web Agentのログイン画面が表示され、ユーザIDとワンタイムパスワードが入力されます。

4. Web Agentから送られたユーザIDとワンタイムパスワード によって、RSA Authentication Managerによる照合・認証が行われます。
5. Authentication Managerによる認証成功後、HP IceWall MCRPを経由したWeb アプリケーションへのアクセスが可能になります。

次に、図 3の構成を実際に構築する際のポイントについて説明します。

- ユーザIDの統一（RSA SecurID、HP IceWall SSO 両方にて設定）
  ユーザIDなどの認証ユーザの情報はSecurID, HP IceWall SSO別々に用意します。
  ただしユーザID自体は共通で使えるように同じものを用意します。

- IceWallサーバのホスト設定ファイル（HP IceWall SSOにて設定）
  Web AgentのサーバがIceWallサーバのバックエンドWebサーバとなるため、IceWallサーバにおいてURLパスの変換が行われますが、IceWallサーバのデフォルトの設定ではWeb Agentが表示するHTMLページの中に記述されている一部のURLパスが変換できません。そのため、IceWallサーバのホスト設定ファイルにキーワード変換の設定を入れる必要があるため以下のように設定します。

  REPKEY=location.replace(″/,location.replace(″$DFW/$ALIAS/

- Web Agentのログイン画面HTMLテンプレートファイルの修正（RSA SecurIDにて設定）
  前述した認証の流れでは、IceWallサーバとWeb Agentの二つのログイン画面が表示され、ユーザIDを二重に入力する手間があります。これを軽減させるために、Web AgentのログインHTMLテンプレートファイルを修正して、ユーザIDの入力を省略し、ワンタイムパスワードのみを入力させることができます。そのためには以下のようにします。

修正前
```
<TABLE class=″form″ cellspacing=″0″>
<TR>
<TD class=″label″>User ID:</TD>
<TD class=″field″><INPUT TYPE=TEXT NAME=″username″ VALUE=″″ MAXLENGTH=32>
</TD>
</TR>
```

修正後
```
<p>$USER_ID のワンタイムパスワードを入力してください ←特殊キーワード変換
<INPUT TYPE=HIDDEN NAME=″username″ VALUE=″$USER_ID″> ←特殊キーワード変換
```

入力フィールドをテキストフィールドからHIDDENタイプに変更します。そして、IceWallサーバの特殊キーワード変換の機能を利用し、フォワーダを通過した時に$USER_IDの部分を認証されたユーザ名に置き換えます。
置き換えによりユーザIDの入力が省略されます。

修正後のログイン画面は、以下の図 4の例のようになります。

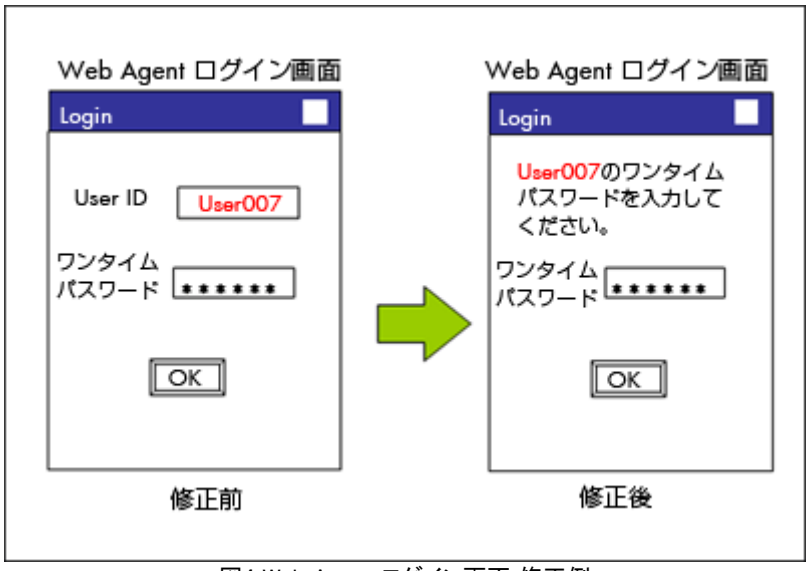

図4 Web Agent ログイン画面 修正例

6. 最後に

本記事では、HP IceWall SSOとRSA SecurIDとの連携例を紹介しました。この例以外でも様々な連携の構成が考えられます。

HP IceWall SSO製品は、他社の認証製品や認証デバイス製品と連携できる柔軟性を持ち合わせています。
さらに他の認証関連製品との連携について、機会があれば皆様にご紹介したいと考えております。

2008.2.29

日本ヒューレット・パッカード コンサルティング・インテグレーション統括本部 セキュリティスペシャリスト CISSP-ISSJP　藤波 勉