HP IceWall SSO と ベリサイン VIP（ワンタイムパスワード）との連携

1.はじめに

認証を強化する一つの方法として、ワンタイムパスワードの導入があります。このレポートでは、HP IceWall SSOにワンタイムパスワードによる認証機能を追加する方法についてご紹介します。ワンタイムパスワードによる認証には、ベリサイン社のVeriSign Identity Protection（VIP）オーセンティケーションサービスを使用します。

VIPオーセンティケーションサービスの詳細については、こちらをご参照ください。

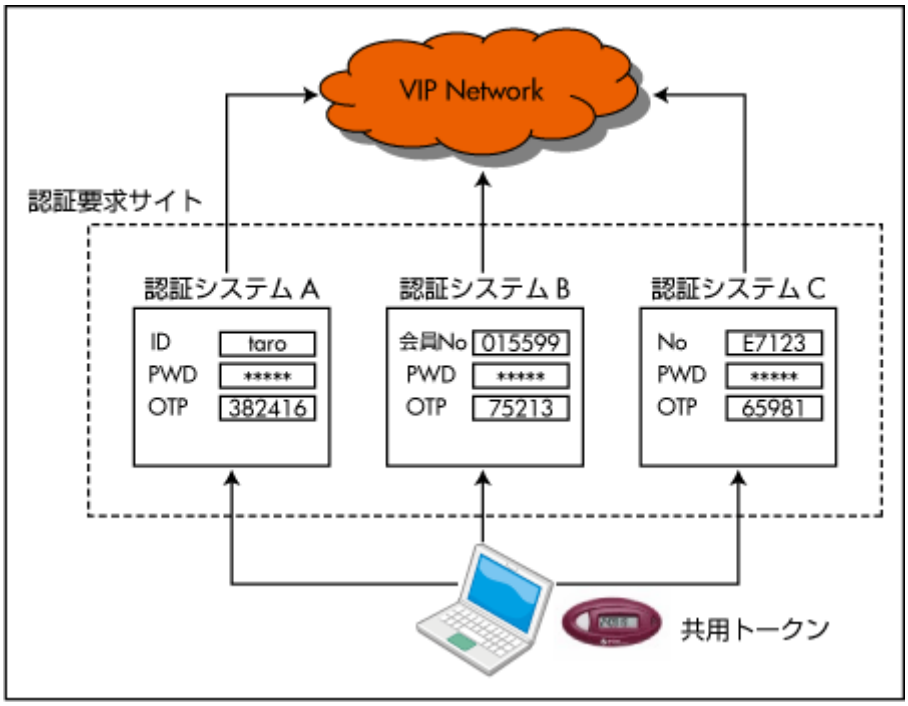
このレポートでは以降、ワンタイムパスワード（One Time Password）を「OTP」、VIPオーセンティケーションサービスを「VIP」と表記します。

2.VeriSign Identity Protection（VIP）

2.1 概要

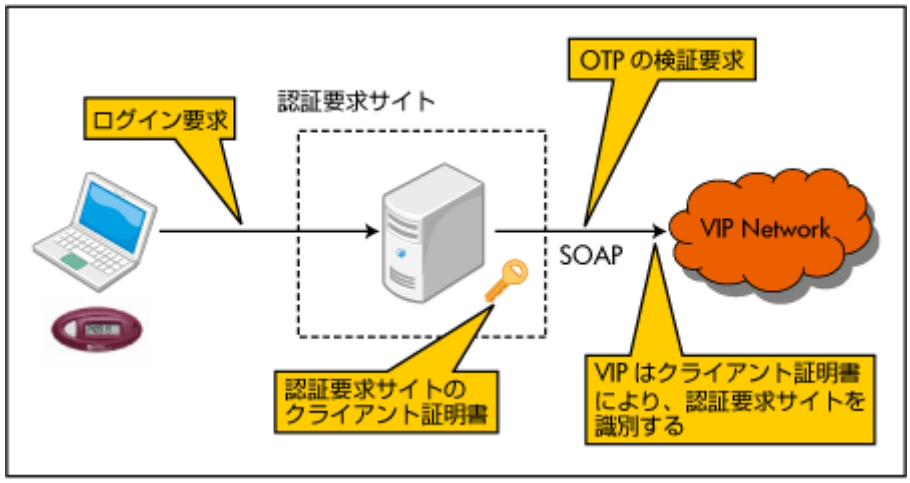
VIPは、認証要求サイトからOTPの検証要求を受けると、その検証結果を認証要求サイトに返すセキュリティサービスです※1。VIPはOTPの検証を、SaaS（Software as a Service）として提供します。（下図参照）

※1　認証以外に、トークンの状態管理サービスも提供します。また、VeriSign Identity Protectionは、ワンタイムパスワード以外にもさまざまなセキュリティサービスを提供します。詳細についてはこちらをご参照ください。



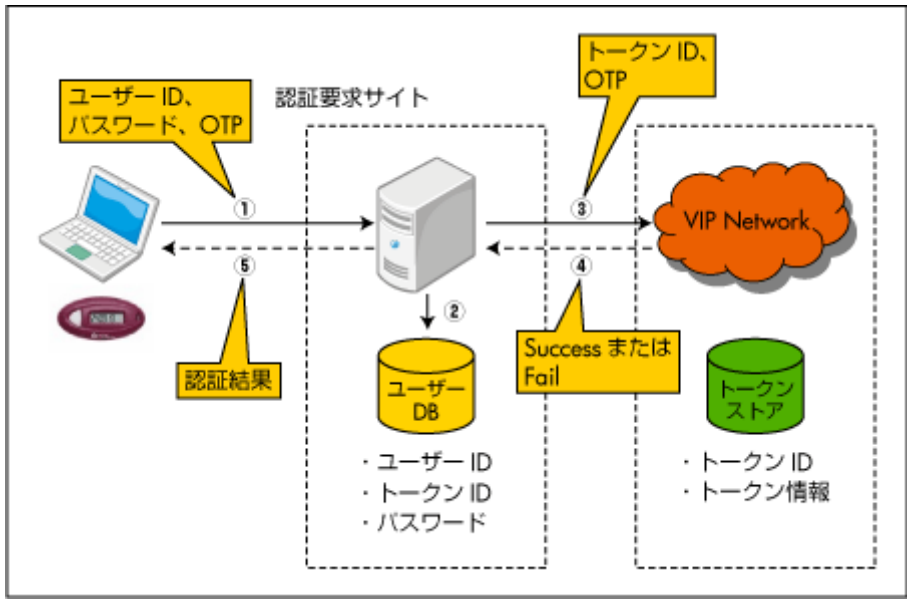
2.2 VIPへの接続方法

VIPを使用するサイト（認証要求サイト）は、VIPへSOAPを使用して接続します。また、VIPへの接続にはクライアント証明書を使用します。（下図参照）



2.3 認証時のシーケンス

認証要求サイトは、ユーザーが入力したユーザーIDからトークンIDを取得し、OTPと共にVIPへ認証リクエストを送信します。VIPはOTPの検証結果を返します。



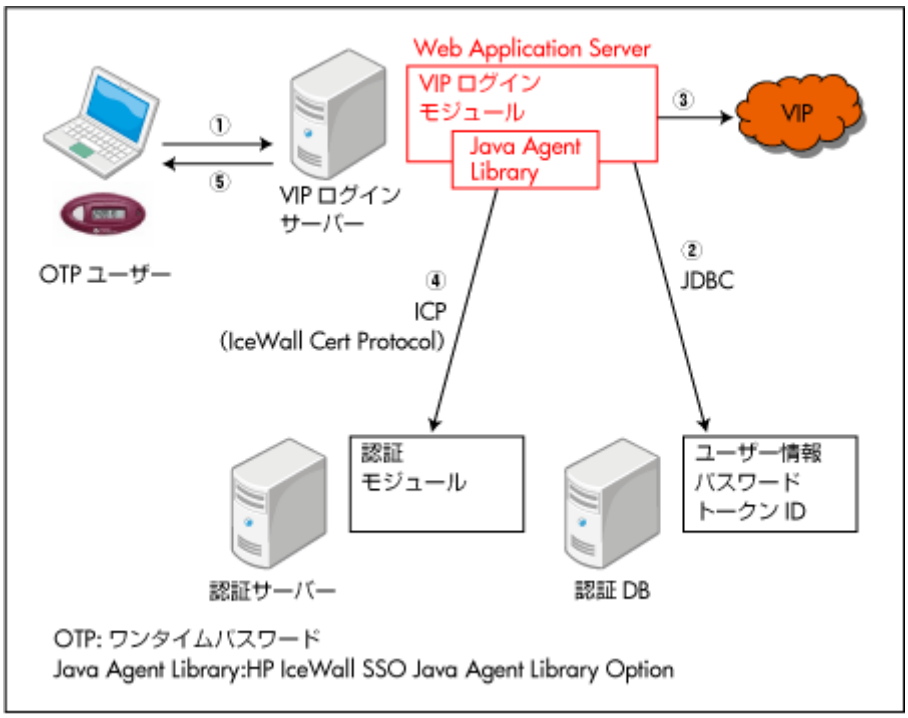
No	内容
①	ユーザーは、ユーザーID・パスワード・OTPを送信します。
②	認証要求サイトは、DBからユーザーIDに結びつくトークンIDを取得します。
③	認証要求サイトは、VIPへトークンID・OTPを送信します。
④	VIPはOTPを検証し、その検証結果を返します。
⑤	認証要求サイトは、OTPの検証結果が正しいことを確認します。また、ユーザーが入力したパスワードが正しいことを確認します。認証要求サイトは、OTPとパスワードの両方の検証が正しかった場合、認証結果をユーザーに返します。

3.HP IceWall SSOにOTPによる認証機能を追加する方法

3.1 概要

VIPを使用して、HP IceWall SSOにOTPによる認証機能を追加することができます。そのためには、HP IceWall SSOに「2.3認証時のシーケンス」を処理するモジュールを追加する必要があります。以降では、この機能を持つモジュールを作成する場合のキーとなるポイントについて説明します。
以降では、このモジュールを「VIPログインモジュール」と記述します。

以下にVIPログインモジュールのシステム構成を示します。



3.2 VIPログインモジュールに必要な機能

VIPログインモジュールには、以下の機能が必要です。

1. リクエスト受信機能

   ユーザーが入力したユーザーID、パスワード(PWD)、OTP、最終目的URLを受信します。

2. DB検索機能

   テーブルからユーザーIDを検索キーにしてトークンIDを取得します。

3. SOAP送信機能

   トークンIDとOTPをVIPへ送信し、VIPが返す検証結果(SuccessまたはFail)を受信します。

4. 認証モジュールログイン要求機能

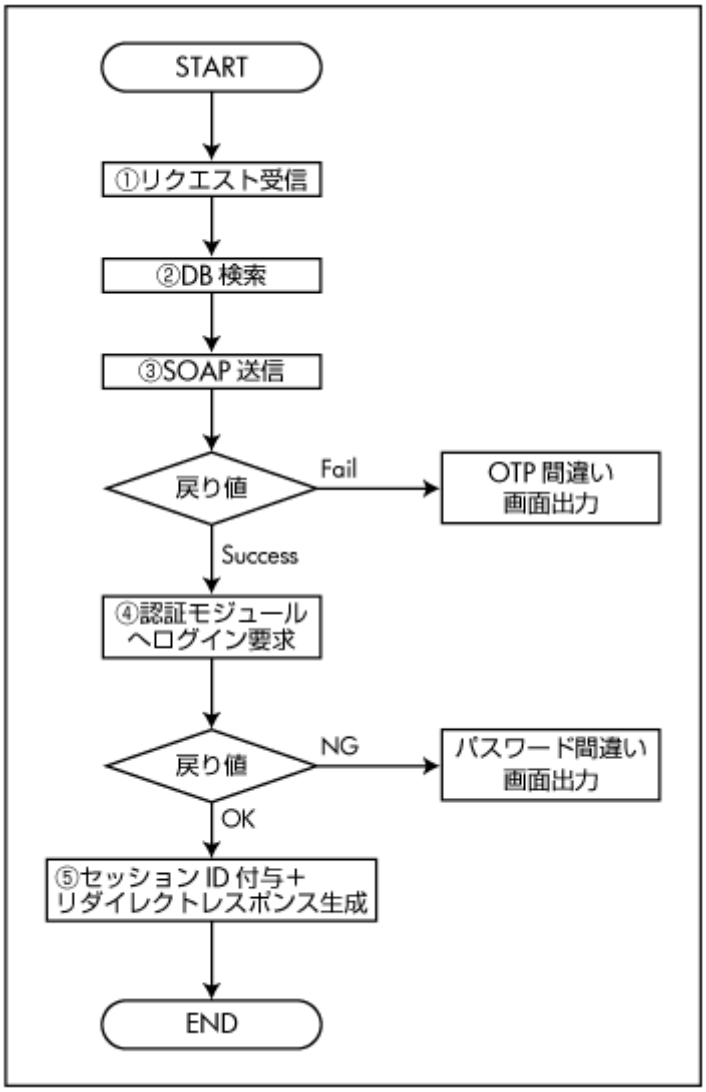
   Java Agent Library(HP IceWall SSO Java Agent Library Option)を使用して、認証モジュールへログイン要求を送信します。次に、認証モジュールが発行したセッションIDを受信します。(Java Agent LibraryはHP IceWall SSOのオプション製品で購入が必要です。Java Agent Libraryは、Javaプログラムから認証モジュールへの接続機能を提供します。)

5. セッションID付与＋リダイレクト生成機能

   認証モジュールが発行したセッションIDを、Cookieを使用してブラウザに渡します。その際、このCookieがフォワーダにも届くように、Cookieのpath属性を設定します。また、最終目的URLへリダイレクトするようにレスポンスヘッダーを設定します。

3.3 VIPログインモジュールのフローチャート

VIPログインモジュールのフローチャートを以下に示します。



3.4 HP IceWall SSOに必要な設定

HP IceWall SSOに以下の設定が必要です。

1. フォワーダが表示するログイン画面の変更

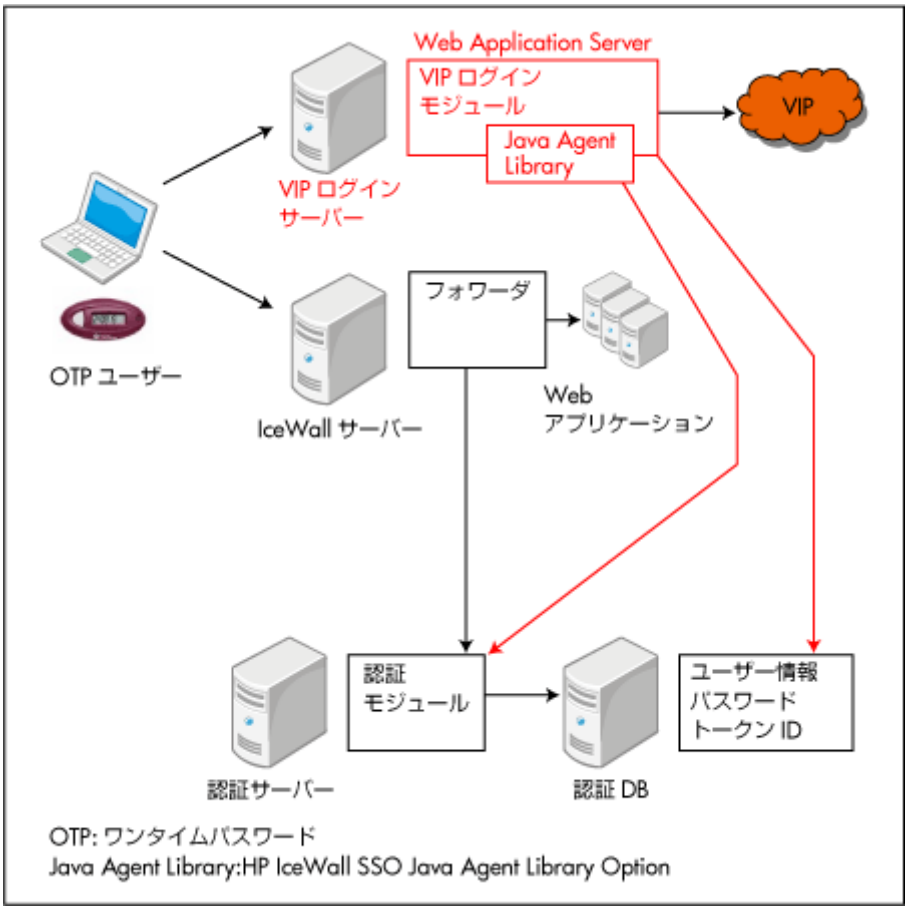
   フォワーダが表示するログイン画面（login.html）において、サブミットボタン押下時のPOST先をVIPログインモジュールに変更します。これにより、ユーザーは、入力したユーザーID、PWD、OTP、最終目的URLなどを、フォワーダではなくOTP認証モジュールへ送信します。

2. フォワーダから認証モジュールへのログインリクエストを停止

   認証モジュールのコンフィグ（request.acl）を設定し、認証モジュールが、フォワーダからのログインリクエストを受信しないようにします。

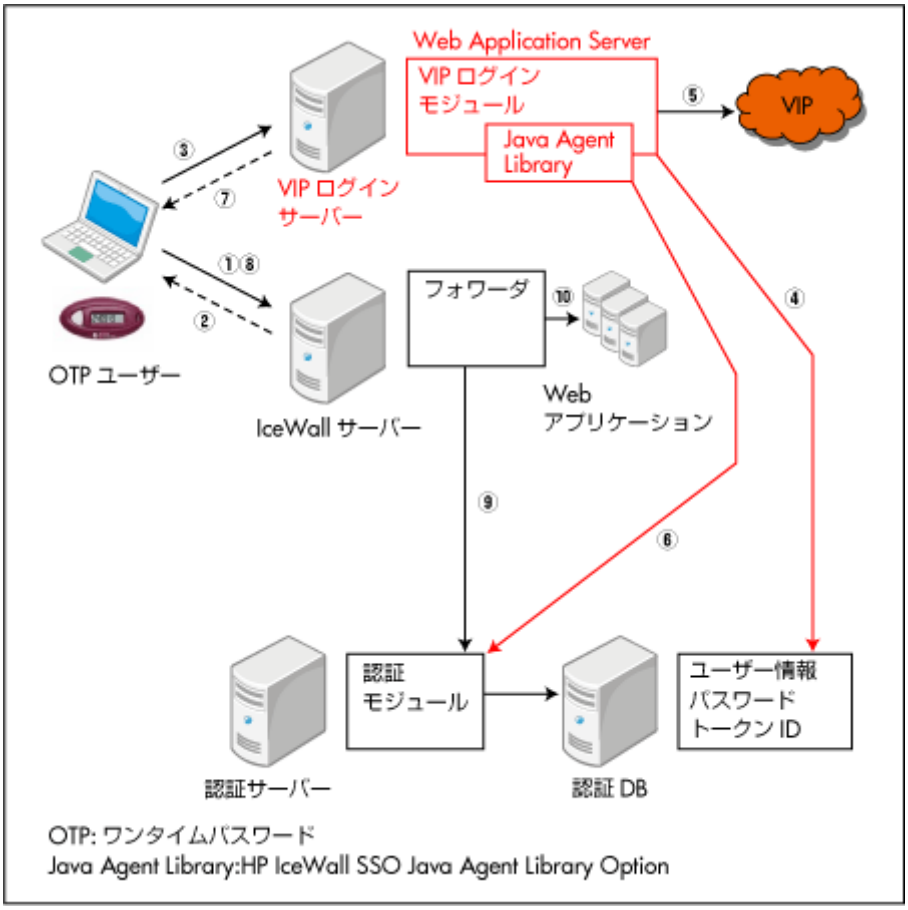
3.5 システム構成

HP IceWall SSOシステムに、VIPログインモジュールを入れたVIPログインサーバーを追加する必要があります。以下に、システム構成を示します。赤い部分は、HP IceWall SSOをOTPに対応するために、追加した部分を示します。



3.6 処理の流れ

ログイン画面を下図に示します。



No	内容
①	ユーザーは、フォワーダの後段にあるWebアプリケーションにアクセスを試みます。
②	フォワーダはユーザーが未認証の場合、ログイン画面を表示します。フォワーダは、このログイン画面にhidden属性で最終目的URL(WebアプリケーションのURL)を埋め込みます。
③	ユーザーは、ユーザーID・パスワード・OTPをフォームに入力後、「ログイン」ボタンを押します。これらの値と最終目的URLは、VIPログインモジュールに送信されます。
④	VIPログインモジュールは、受信したユーザーIDを検索キーにしてトークンIDを取得します。
⑤	VIPログインモジュールは、③で受信したOTPと、④で取得したトークンIDをVIPへ送信します。VIPはOTPを検証し、その検証結果を返します。
⑥	VIPログインモジュールは、⑤の検証結果が「Success」の場合、認証モジュールにログイン要求(③で受信したユーザーID、パスワード)を送信します。認証モジュールは、パスワードを検証し、パスワードが正しい場合はセッションIDを発行して返します。
⑦	OTP検証サーバーは、以下のHTTPレスポンスを返します。 ・⑥で取得したセッションIDをSet-Cookieするヘッダー ・③で受信した最終目的URLへリダイレクトするLocationヘッダー
⑧	ブラウザはLocationヘッダーに従い、最終目的URLへリダイレクトします。また、セッションIDを保持するCookieヘッダーを送信します。
⑨	フォワーダは、受信したセッションIDが有効か、認証モジュールに問い合わせます。認証モジュールは、セッションIDが有効な場合「OK」を返します。
⑩	フォワーダは、セッションIDが有効な場合、リクエストをWebアプリケーションに転送します。

3.7 注意点

HP IceWall SSOからVIPログインモジュールを使用する場合の、注意点を以下に示します。

- OTP検証処理を追加しているため、パスワード認証時と比べてログイン時の応答時間が長くなる場合があります。
- HP IceWall SSOのURL Cookie方式には対応していません。このため、ブラウザにはCookie機能が必須となります。
- HP IceWall SSOのPOSTデータ継承機能について考慮する必要があります。

- VIPログインモジュール⇔認証モジュール間、およびフォワーダ⇔認証モジュール間との接続にはICP2.0を使用する必要があります。

- 認証モジュールを二重化している場合、VIPログインモジュールからプライマリ認証モジュールの接続に失敗するとセカンダリの認証モジュールへフェールオーバーする機能が必要です。

- 認証DBを二重化している場合、認証モジュールとVIPログインモジュールが接続する認証DBを一致させるなどの考慮が必要です。

3.8 管理機能

ここまでは認証機能について説明しました。実際の運用では、以下のユーザー情報とトークン情報の管理も必要です。

1. ユーザー情報

   DBに格納したユーザー情報を管理する機能が必要です。これらはHP IceWall SSOでは範囲外の機能であるため、このレポートでは説明しません。ユーザーデータの管理には、HP IceWall Identity Managerが使用できます。

2. トークン情報

   VIP上のトークン情報を管理する機能が必要です。これは、トークン管理用SOAPリクエストをVIPへ送信することで実現します。

4.まとめ

このレポートでは、VIPとHP IceWall SSOを連携することで、HP IceWall SSOでOTPによる認証を実現できることを説明しました。また、その構成例と注意点についても説明しました。

※RSA SecurIDとの連携については、こちらをご参照ください。
※VASCO DIGIPASSとの連携については、こちらをご参照ください。

2011.5.10 日本ヒューレット・パッカード　テクノロジーサービス統括本部　テクニカルコンサルタント　米川 和利