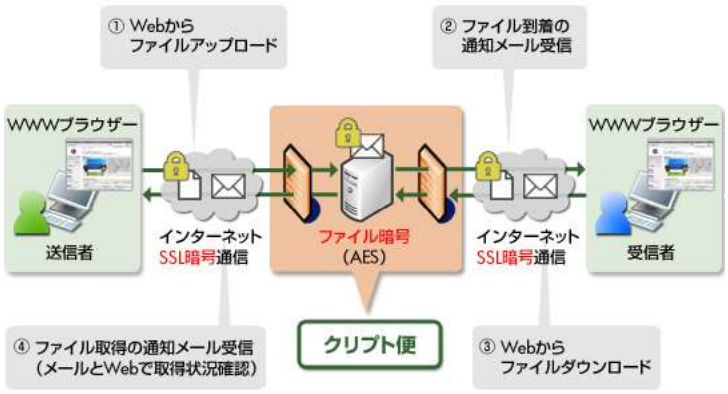
セキュアファイル送受信サービス「クリプト便」との認証連携

1. はじめに

このレポートでは、NRIセキュアテクノロジーズ株式会社（以下、NRIセキュア）のセキュアファイル送受信サービス「クリプト便」の認証に、HP IceWall Federation※1を使用して認証連携※2する場合についてご紹介します。
HP IceWall Federationを導入することにより、クリプト便のユーザーは、クリプト便固有のIDとパスワードを覚える必要がなくなります。また、管理者は、クリプト便上でのユーザーパスワード初期化作業を行う必要がなくなります。

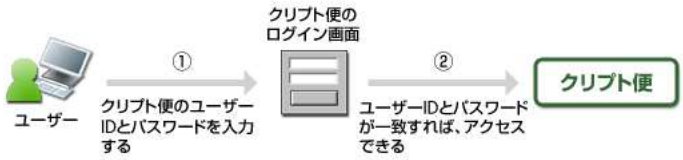
2. セキュアファイル送受信サービス「クリプト便」について

クリプト便とは、インターネットを介した電子ファイルのやり取りを、情報セキュリティベンダーであるNRIセキュアの高度なセキュリティ技術によって、安全かつ確実に実現するSaaS型ファイル交換サービスです。ファイルの送受信に必要なのは、Webブラウザーとインターネットに接続できる環境だけです。
NRIセキュアが提供する強固なセキュリティ機能の組み合わせで、送信者ー受信者間のセキュアなファイル交換を実現しています（下図）。また、株式会社アイ・エス・レーティングの情報セキュリティ格付けにおいて、SaaSとして最高レベルの「AAAis」を取得しています。クリプト便の詳細については、こちらをご参照ください。



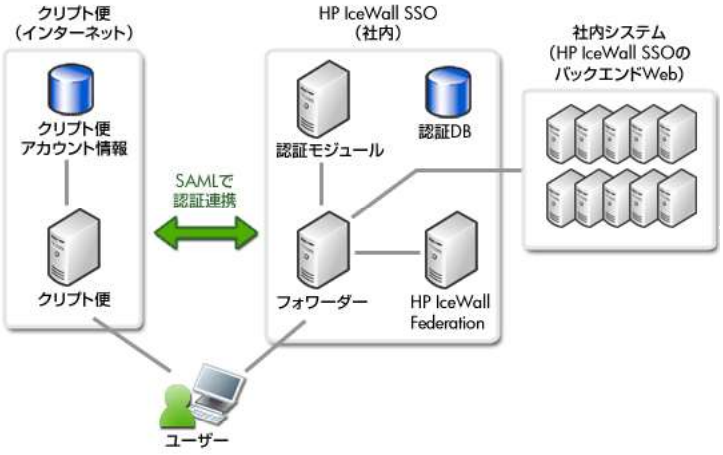
3. 一般的なログイン

クリプト便のユーザーは、ファイルを送受信（Webからファイルをアップロード、ダウンロード）する際、インターネット上にあるクリプト便の画面にログインする必要があります。ログインには、クリプト便専用のID とパスワードを入力します。



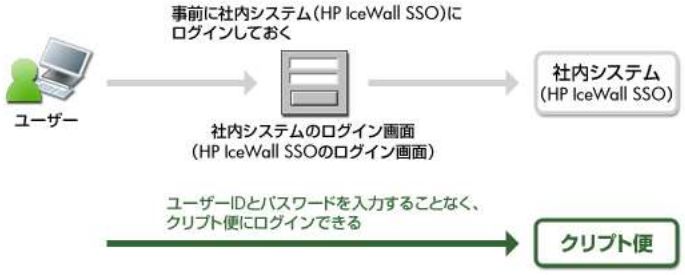
4. HP IceWall Federationによる認証連携の導入

クリプト便に、HP IceWall Federationを使用した認証連携を導入した構成例を以下に示します。HP IceWall SSOとサイト間認証連携製品「HP IceWall Federation」を導入し、クリプト便とHP IceWall Federation間を、SAML（Security Assertion Markup Language）で接続します。



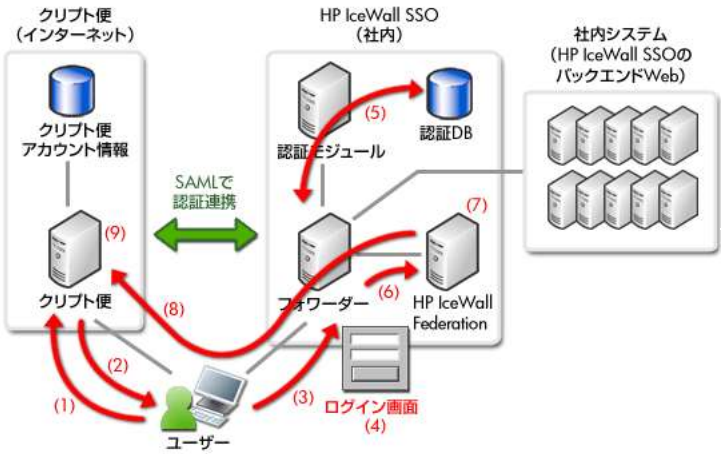
5. 認証連携を導入した後のログイン

クリプト便のユーザーは、事前に、社内システム（HP IceWall SSO）にログインしておきます。クリプト便のユーザーは、ファイルを送受信（Webからファイルをアップロード、ダウンロード）する際、すでに社内システム（HP IceWall SSO）にログイン済みならば、ユーザーID とパスワードを入力することなくクリプト便のシステムにログインできます。



6. 認証連携時の処理の流れ

認証連携時の処理の流れを以下に示します。



番号	内容
(1)	ユーザーは、クリプト便にアクセスを試みます。
(2)	クリプト便は、SAMLの認証リクエストを(ユーザーのブラウザーを経由して)HP IceWall SSOへ送信します。
(3)	ユーザーのブラウザーは、(2)で受信したSAMLの認証リクエストをHP IceWall SSOへ送信します。
(4)	HP IceWall SSOは、ユーザーが未認証の場合、ログイン画面を表示して、ユーザーに認証を求めます。 ユーザーは、ログイン画面に、社内システム用(HP IceWall SSO用)のユーザーIDとパスワードを入力します。
(5)	HP IceWall SSOは、ユーザーが入力したユーザーIDとパスワードが正しいことをチェックします(認証)
(6)	フォワーダーは、ブラウザーからのリクエスト(SAMLの認証リクエスト)をHP IceWall Federationへ転送します。
(7)	HP IceWall Federationは、SAMLの認証レスポンスを発行し、これを(ユーザーのブラウザーを経由して)クリプト便へ送信します。
(8)	ユーザーのブラウザーは、SAMLの認証レスポンスをクリプト便へ送信します。
(9)	クリプト便は、SAMLの認証レスポンスを受信し、ユーザーがHP IceWall SSOで認証済みであることを確認します。確認できた場合、ユーザーからクリプト便へのアクセスを許可します。

7. 認証連携の導入によるユーザーのメリット

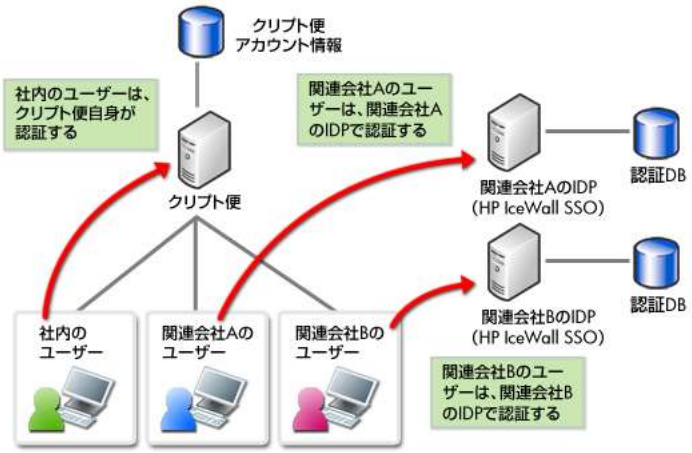
認証連携の導入による、ユーザーのメリットを以下に示します。

- 社内システムとは別に、クリプト便用のユーザーIDとパスワードを管理する必要がない。(ユーザーは、社内システムのユーザーID とパスワードだけを管理するだけでよい)
- 一度、社内システムにログインしておけば、クリプト便を利用する際に、再度ユーザーIDとパスワードを入力する必要がない。

8. 認証連携の導入によるシステム管理者のメリット

認証連携の導入による、システム管理者のメリットを以下に示します。

- クリプト便のセキュリティポリシー(パスワード長や有効期限など)を、社内システムのポリシーと統合して一元管理できる。
- クリプト便のアカウントを、社内システムと統一できる。
  例えば、退職者のアカウントを社内システムから削除することで、クリプト便の利用も停止できる。
- クリプト便へのアクセスを社内環境からのアクセスに限定して、インターネットからの不正アクセスを制限できる。
- SAMLで連携する情報は、クリプト便のユーザーIDだけで、社内のユーザーIDやパスワードはインターネット側にあるクリプト便には送信されない。
- クリプト便の認証を、ユーザーが所属する組織に委譲できる。
  例えば、ユーザーが所属する会社ごとにIDP(Identity Provider。このケースではHP IceWall SSOとHP IceWall Federation)を用意する。認証は、ユーザーが所属するそれぞれのIDPに委譲する。(下図)



認証をユーザーの組織に委譲したケース

9. 認証連携を導入する際の注意事項

クリプト便が使用するユーザーのアカウント情報は、クリプト便の管理者画面よりアカウ ントー括・個別登録機能を利用して、事前に登録しておく必要があります。

10. まとめ

このレポートでは、NRIセキュアのクリプト便の認証に、HP IceWall Federation※1を使用した認証連携をご紹介しました。また、認証連携の導入によるメリットを説明しました。HP IceWall Federationをクリプト便のセキュリティ強化と利便性向上のシステムとして、是非、導入をご検討ください。HP IceWall Federationでは、これからも多くのクラウドサイトと接続を検証していく予定です。

※1: 認証連携には、HP IceWall SSOとそのオプション製品であるHP IceWall Federationが必要です。
※2: 認証連携とは、異なるサイト間(この場合は、クリプト便とHP IceWall SSOが管理する社内システム)でシングルサインオンすることです。

2011.12.12 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　テクニカルコンサルタント　米川和利