HP IceWall SSO

HP IceWall技術レポート：HP IceWall SSOとICカードとの連携（クライアント証明書を格納したICカードとの連携）

はじめに

本レポートでは、HP IceWall SSOとICカード、クライアント証明書を連携させる方法についてご紹介いたします。

本検証では、大日本印刷株式会社（以降、DNP社と表記）にもご協力いただき、以下のプロダクトを使用しました。

認証認可（シングルサインオン）システム：HP IceWall SSO　及び　クライアント証明書オプション
ICカード連携システム：DNP社　TranC’ert Enterprise
ICカード：DNP社　接触型ICカード　（上記のクライアント証明書をICチップ内に格納）
接触型ICカードリーダライタ：USBタイプカードリーダ
デジタル証明書：マイクロソフト株式会社のエンタープライズCA（Windows Server標準機能）が発行したデジタル証明書

本検証で連携したDNP社　TranC’ertについてのご紹介

TranC’ert はICカードとPKI技術を使用したセキュリティソフトウェアです。
リーダライタを介して接続されたICカードを使用して、下記のような各種セキュリティ機能を使用できます。

- パソコン起動制御
- デバイス制御
- 無線LANやVPN使用時のネットワーク認証

以下の表に、TranC’ertの詳細機能（一例）をまとめました。

クライアント機能	管理サーバ機能	管理者機能
■ ICカードログオン認証 / スクリーンロック	■ 権限情報、認証情報管理	■ 各種ポリシー作成 / 管理
■ PC利用者制限	■ ポリシー配信	■ ICカード / ユーザ / PC管理
■ SSFC連携	■ オンラインアップデート	■ ヘルプデスク
■ デバイスロック	■ 操作ログ(簡易)収集	■ 操作ログ権限
■ 簡易パスワード自動入力		■ 管理者権限の委譲・分散
■ 電子証明書(PKIの使用)		
■ 操作ログ送信		

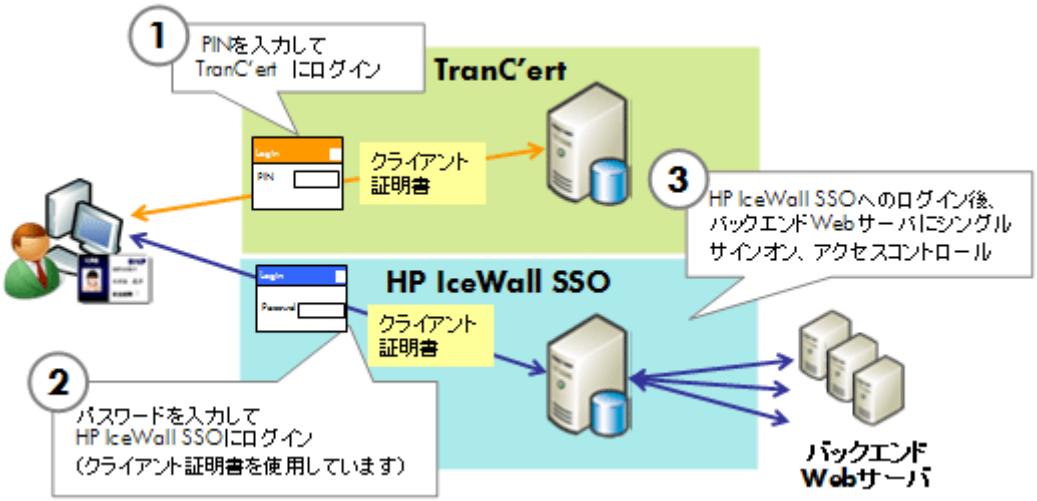
本検証では、HP IceWall SSOとICカードの連携に、TranC’ertの電子証明書機能を活用しました。

検証の内容と結果

検証内容

本レポートでは、以下の動作を確認しました。

- ICカードをリーダにセットし、PIN入力を行うことによりTranC’ ertにログインします。(スマートカード ログオン)
- HP IceWall SSO管理下のバックエンドWebサーバにアクセスする際、初回アクセス時には、HP IceWall SSOへのログインを行います。この際に、ICカード内のクライアント証明書を使用します。
  ユーザは、パスワードの入力のみ行います。
- HP IceWall SSOへのログイン後は、HP IceWall SSOの通常の動作として、シングルサインオンとアクセスコントロールを行います。



検証結果

上記の検証内容において、稼動を確認しました。

検証環境の設定内容

本検証の環境について以下に補足します。

HP IceWall SSO

- 標準構成のHP IceWall SSOとクライアント証明書オプションを使用し、特に大きな注意点はありませんでした。
- 認証データベースには、クライアント証明書オプションの使用に必要となる以下の情報を登録しました。
  - ユーザID
  - パスワード
  - クライアント証明書の発行時シリアル番号
  - クライアント証明書の発行時発行者名称

TranC'ert

- ICカードの使用環境やTranC’ ertに関しても、標準構成で構築しました。
- クライアント証明書は、「スマートカードユーザ」テンプレートで発行したものを使用しました。

両システムのデータベースに登録するユーザ情報について

- TranC’ ertのローカルデータベースとHP IceWall SSOの認証データベースには、同一のユーザ情報を登録しました。

HP IceWall SSOとICカード、TranC’ ertの連携メリットや応用について

本連携のメリットや、今後の応用例については以下などがあげられます。

●利便性の向上

- ユーザのID入力が不要となります。ユーザが管理するものは、ICカード、PIN、パスワードのみです。
- HP IceWall SSOへの追加プログラムを個別に開発することにより、パスワードの入力を省略させるといった対応も検討可能です。□ユーザは、ICカードとPINを覚えておくだけで、セキュアにWebシステムにアクセスできます。

●セキュリティの向上

- HP IceWall SSOのみによるID/パスワードでのログインと比較し、ICカードの所持が前提となるためセキュリティが向上します。
- 従来のICカードとHP IceWall SSOの連携と比較し、クライアント証明書が発行されていること、その証明書が使用されること、という前提が付加されるため、セキュリティが向上します。
- HP IceWall SSOを使用させるユーザを、「ICカードを所持・提示する者に限定させる」ことが可能です。
- HP IceWall SSOのクライアント証明書オプションを使用した従来のモデルでは、PCにクライアント証明書をインストールする必要がありました。
  本検証のモデルでは、クライアント証明書はICカード内に格納されているため、ユーザは異なるPCからでも自分のクライアント証明書を使用してアクセスが可能です。
- ICカードを使用してHP IceWall SSOにログインする場合と、ICカードは使用せずIDとパスワードを入力してHP IceWall SSOにログインする場合を混在させることも可能です。□それぞれのログインパターンでアクセス権を変えることも可能です。

●個別ニーズに合わせて柔軟に拡張可能

- ICカード及びTranC' ertを使用して、PCログオン、ActiveDirectoryへのドメインログオンをセキュアに行い、HP IceWall SSOのWindows統合認証機能と連携させることも可能です。
- DNP社ではWindows Serverで発行できるデジタル証明書を大量に一括生成できるツールが用意されています。
- DNP社としてはその証明書をICカードに格納するサービスも提供しています。
  ≫「大日本印刷　MS Active Directoryと連携した電子証明書大量生成ツールを開発」

おわりに

今回の検証では、HP IceWall SSOとICカードを連携しました。
イントラネットへのセキュリティ強化と利便性向上のツールとして、是非ご検討ください。

2009.3.4
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　平野　宜敬、木田　智子
大日本印刷株式会社　IPS事業部 セキュリティソリューション開発部　中村　聡志　氏
≫ 大日本印刷株式会社セキュリティソリューションホームページ