HP IceWall技術レポート:

UNIADEX SecureSuiteVによる 多要素認証で強化された統合認証基盤

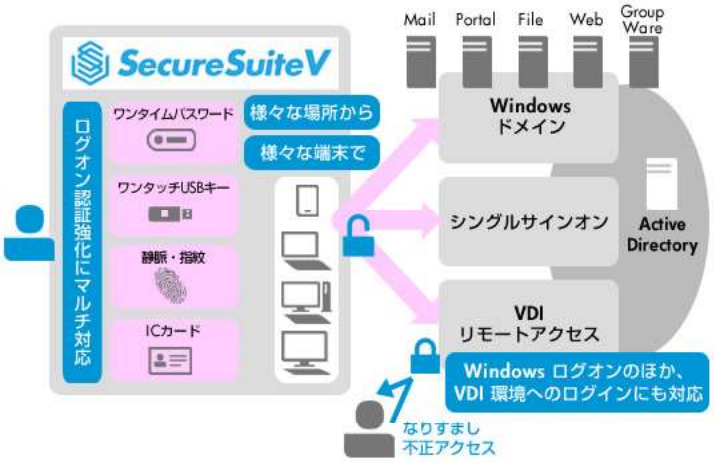
1. はじめに

『なりすまし』による不正侵入は、セキュリティ対策である『アクセス制御』や『アクセスログによる追跡』を無効化します。それを防ぐには生体認証やICカードを併用した多要素認証ソリューションの導入が有効です。シングルサインオンと組み合わせて導入することで強固で便利な認証基盤を構築することが可能になります。本書では、シングルサインオンのHP IceWall SSOに加えてユニアデックスの多要素認証ソリューション SecureSuiteVを組み合わせた利用方法をご紹介します。

2. UNIADEX SecureSuiteV とは

PCのドメインログオンに対して、静脈や指紋等の生体情報やICカードやワンタイムパスワードトークンといった持ち物による多要素認証機能を提供します。各種認証要素は組み合わせて使うことができ、『ICカード＋パスワード』、『ICカード＋静脈』、『指紋またはICカード＋パスワード』等の様々な認証方式が可能となります。また、クライアントベースのシングルサインオン機能も有しています。

» 詳細はこちら



3. 連携システムの紹介

3. 1 概要

ユーザーは静脈認証でWindowsドメインにログオンします。その後のWebアプリとクライアントサーバーアプリには再ログオン無しで利用が可能となります。また、ユーザー情報は人事システムから出力されたCSVファイルをID管理システムで取り込み、情報を付加して各システムに配信します。

3. 2 システム構成

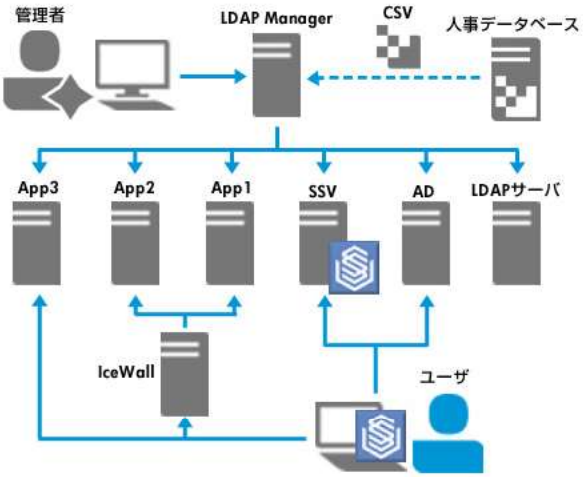


図1 全体図

構成システム	略称	備考
人事データベース	ー	ユーザー情報の元データ
LDAP Manager	ー	ID管理システム
LDAPサーバー	ー	付加されたユーザー情報の格納場所
Active Directory	AD	Windowsドメインの認証サーバー
SecureSuiteV	SSV	静脈認証、クライアントサーバーアプリの認証代行
HP IceWall SSO	IceWall	Webシングルサインオン
Webアプリ1	App1	独自認証データベースを持つ
Webアプリ2	App2	認証はADで照合する
クライアントサーバーアプリ	App3	独自認証データベースを持つ

3．3　各製品の役割

1）SecureSuiteV（ユニアデックス株式会社）

- Windowsドメインへのログオンを静脈認証に変換します。
- クライアントサーバーアプリのログイン画面にID/パスワードを投げ込みます。

2）HP IceWall SSO（日本ヒューレット・パッカード株式会社）

- HP IceWall SSOの統合Windows認証機能（Domain Gateway オプション）により、Windowsログオンしたユーザーは自動的にHP IceWall SSOにもログインできます。
- SecureSuiteVがHP IceWall SSOのログイン画面にID/パスワードを投入することもできます。

3）LDAP Manager（エクスジェン・ネットワークス株式会社）

- 人事データベースから出力したCSVからユーザー情報をLDAPサーバーに取り込みます。さらにADや各システムにユーザー情報（ID/パスワード等）を配信します。

3．4　動作の流れ

1）認証（静脈認証とシングルサインオン）

1. ユーザーはPCのWindowsドメインログオン時にSecureSuiteVによる静脈認証を行います。
2. HP IceWall SSO Domain Gateway オプションによりHP IceWall SSOの認証を完了します。
3. Webアプリ1、Webアプリ2に対してはHP IceWall SSOによるシングルサインオンを実現します。
4. クライアントサーバーアプリに対してはSecureSuiteVによるシングルサインオンを実現します。

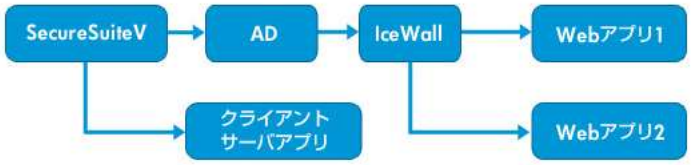


図2 シングルサインオンの関係性

2）ユーザー情報、パスワードの連携

1. 人事データベースにてユーザー情報をCSVファイルにエクスポートします。
2. LDAP ManagerでCSVファイルを取り込み、LDAPサーバーに格納します。
3. 不足する属性情報を付加し、LDAPサーバーに格納します。
4. LDAP Managerにて各システムのパスワードを個別にランダム生成します。
5. LDAP Managerにて各システムにID/パスワードを登録します。

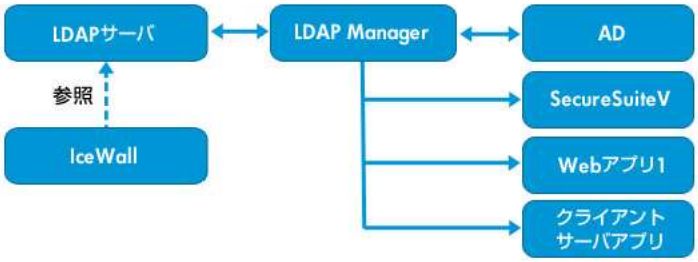


図3 ユーザー情報の連携

3．5　本システムのメリット

1）セキュリティ
PCログオンに静脈認証を採用することにより『なりすまし』による不正ログオンを防止します。アプリケーションの認証はシングルサインオン化されておりユーザーはパスワードの記憶や入力が不要です。そのためパスワードをメモしたり、教えたりすることができないためパスワード情報が漏洩するリスクが小さくなります。また、各システムのパスワードはランダム化したものを生成し定期的に更新しており、ひとつのパスワードが盗まれたとしても連鎖的な不正侵入を防止できます。

2）ユーザー利便性
PCログオンは静脈認証としており、その他はシングルサインオンとしていることから、パスワードの入力が不要です。パスワードが不要なため記憶、入力、変更の運用が全て不要になり利便性が大幅に向上します。

3）メンテナンス性
ユーザーの認証が統合されパスワードの入力が不要になることから、パスワード忘れによるリセットなどの対応コストが削減できます。また、ID管理システムにより、定期的なパスワード変更、ユーザーの増減、異動に対しても、自動でシステムに反映できるため管理者の運用負荷が軽減できます。

3．6　連携のテスト

HP IceWall SSOとSecureSuiteVの連携方法として2通りのテストを実施しました。

1）SecureSuiteVによるドメインログオンと、HP IceWall SSOのDomain Gateway オプションによりADのKerberos認証を介して連携する。
2）HP IceWall SSOのログオン画面にSecureSuiteVがID/パスワードを自動投入する。

両方式において、動作の確認が取れました。
※HP IceWall SSO、SecureSuiteV、Windowsのバージョンや設定によって動作しない場合もありますので、導入の際には各環境に応じて動作検証していただくようお願いします。

4．まとめ

SecureSuiteVとHP IceWall SSO、LDAP Managerの組み合わせで、効率的かつ、より強固な認証基盤が構築できることを紹介しました。今回は、静脈認証としていますが、ICカード等の組み合わせでも利用することが可能です。多要素認証による『なりすまし』対策ソリューションとしてご検討ください。

本ソリューションに関するお問い合わせ

ユニアデックス株式会社
≫ 製品やサービスについてのお問い合わせ・見積ご依頼