SECUREMASTER/EnterpriseIdentityManagerと HP IceWall SSOの連携

はじめに

本技術レポートでは、NEC製品である統合ID管理ソフトウェア「SECUREMASTER/EnterpriseIdentityManager」(以降EIMと記述)を、HP IceWall SSOのユーザー管理基盤として利用する場合の連携方法と連携ポイント、および検証結果を記述します。

1.SECUREMASTER/EnterpriseIdentityManagerについて

EIMは、業務システムのユーザー情報や権限情報を一元管理し、運用コスト削減と統制強化を実現する統合ID管理ソフトウェアです。

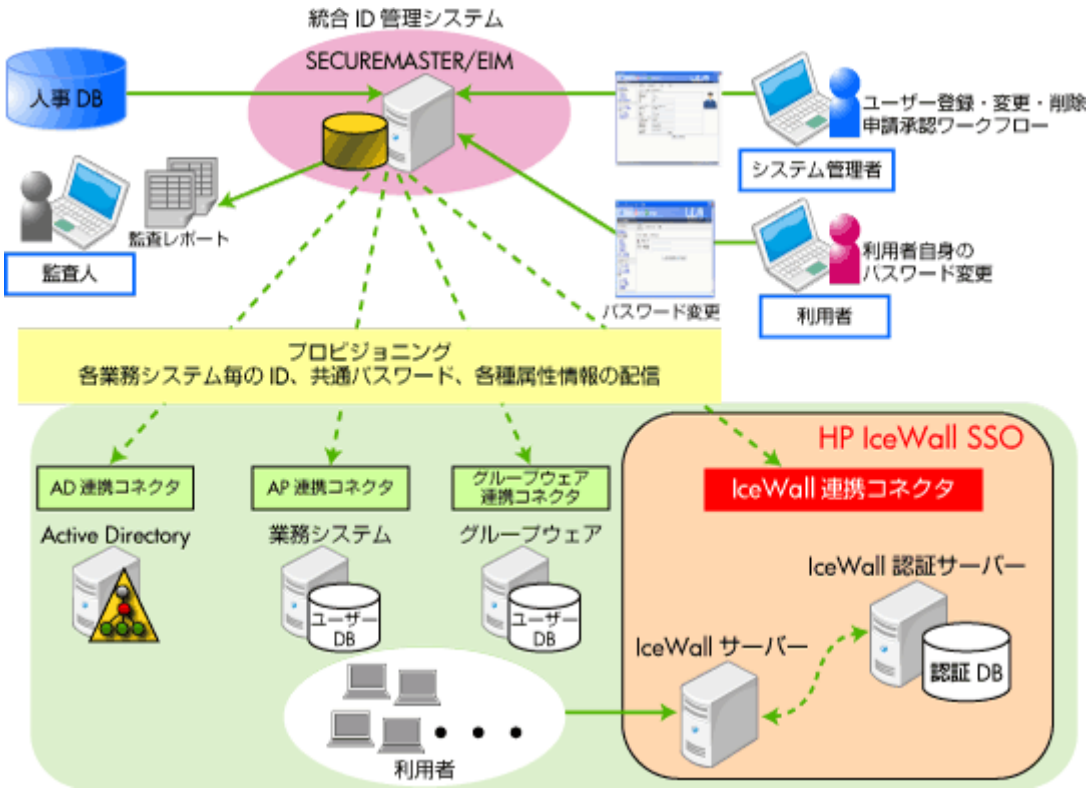
SECUREMASTER/EnterpriseIdentityManagerの特徴

1. ID管理に必要な申請承認ワークフロー機能、プロビジョニング機能、ユーザー管理データベースを1パッケージで提供。
   別途、ワークフロー製品や、データベース製品を購入することなく安価にID管理システムの構築が可能です。
2. 標準搭載のアプリケーション専用テンプレートにより、複雑な連携ルールの設計や開発を行わずに、導入することが可能。導入コストだけでなく、システム追加時の拡張コストも抑えることが可能です。
3. IDの整合性チェック(ID棚卸し)や、証跡取得、監査レポート生成など、監査対応機能を提供。
   これまで人手に頼っていた監査対応のコストを大幅に削減することが可能です。

EIMとHP IceWall SSOが連携することにより、HP IceWall SSOのユーザー管理を効率化し、「適正」な人の管理を可能とする信頼性の高いシングルサインオン環境を実現することが可能になります。また、内部統制等の監査対応コストを削減することが可能になります。

EIMの詳細については、下記をご覧ください。
≫ NEC　WebSAM SECUREMASTER

EIMとHP IceWall SSOの連携イメージ



2.EIM連携方式

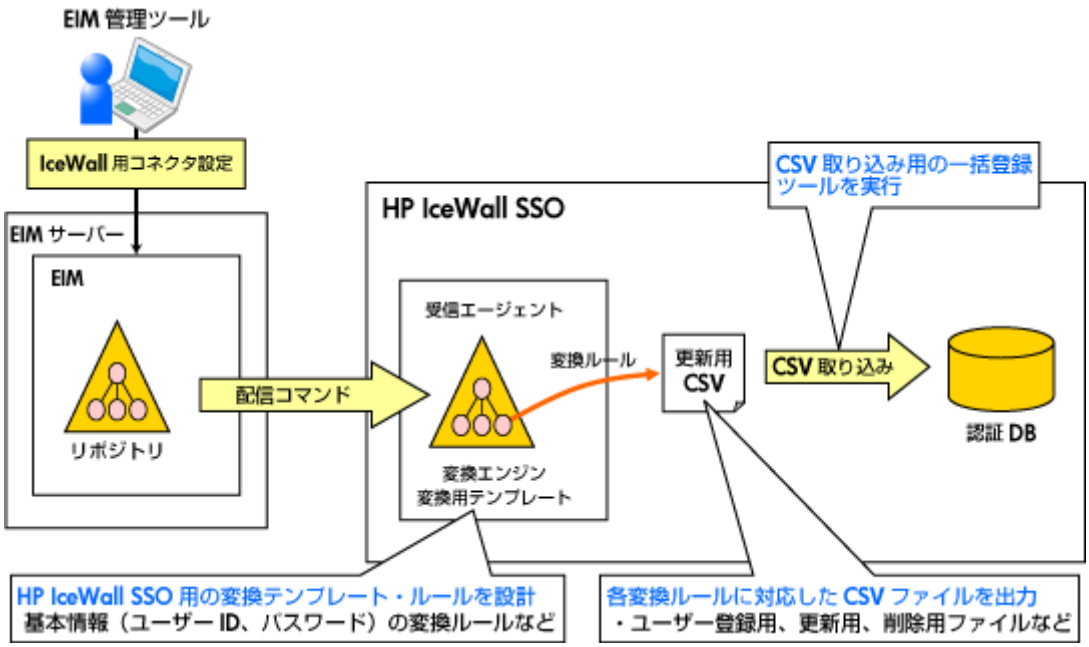
EIMとHP IceWall SSO を連携するIceWall連携コネクタは、HP IceWall SSOが利用するユーザー情報管理データベース（以降、認証DB）の種類により、2つの接続方式(LDAP連携、受信エージェント連携)があります。ご利用環境に合わせて選択願います。

1. LDAP連携

   認証DBがLDAPの場合に使用します。EIMでの変更が直接連携先DBに反映されます。
2. 受信エージェント連携

   認証DBがLDAP以外の場合に使用します。受信エージェントにより、更新用CSVファイル作成＋HP IceWall SSO一括登録ツールを実行し、リアルタイムに連携します。

受信エージェント連携の仕組み



3.検証項目と検証結果

EIMとHP IceWall SSOの連携に関する検証項目は以下の通りです。
ユーザーの登録/変更/削除および、変更したユーザー情報で正しくアクセスできることを確認しました。検証環境については、「参考.検証構成」を ご参照ください。

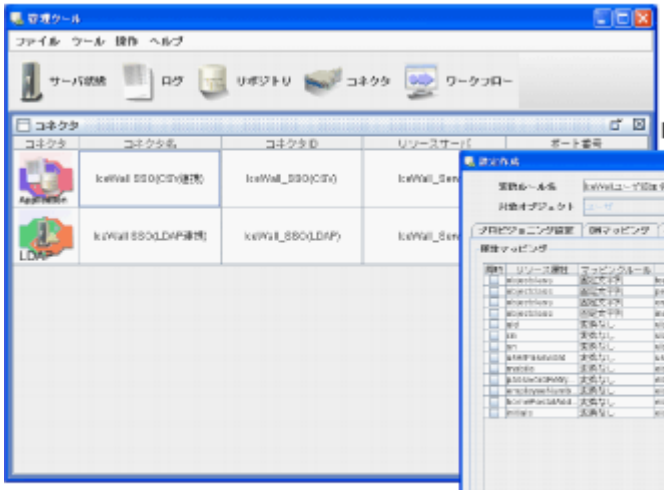
- ユーザー情報登録
- ユーザー情報登録(証明書利用)
- ユーザー情報更新
- ユーザー更新(証明書利用)
- パスワード変更
- パスワードロック解除
- アカウントロック設定/解除
- ユーザー削除

4.連携のポイント

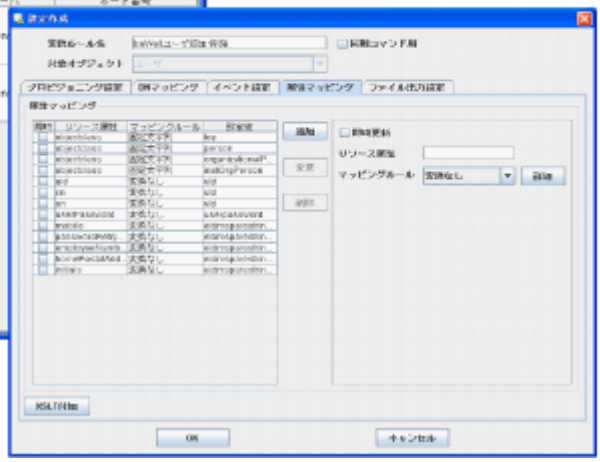
EIMと連携（LDAP連携および受信エージェント連携）する場合のポイントは以下の通りです。

（1）IceWall連携テンプレートによる連携ルールの設定
HP IceWall SSOと連携するための属性情報マッピングルールやCSV出力情報（カラム定義、設定項目など）はEIMが提供するIceWall用の標準テンプレートを利用できます。設定情報のカスタマイズも可能です。

HP IceWall SSO 連携設定画面

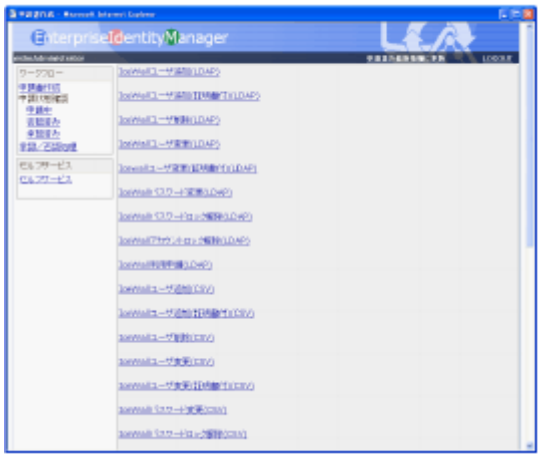


HP IceWall SSO 属性マッピングルール設定画面

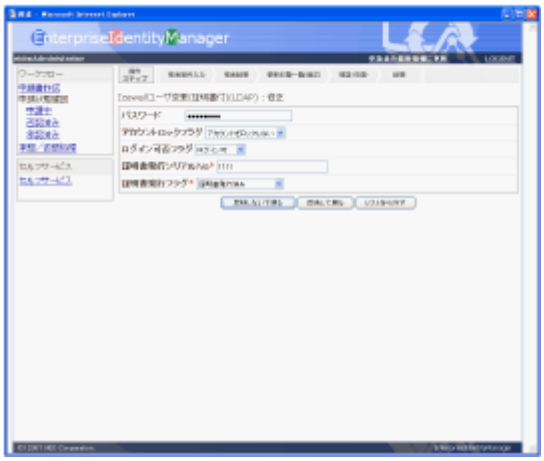


(2)GUI、コマンドによるHP IceWall SSOのユーザー管理
ユーザーID情報の更新やパスワード管理はEIMの管理端末より、GUIを用いた支援ツールで行います。

EIM による HP IceWall SSO ユーザー管理画面

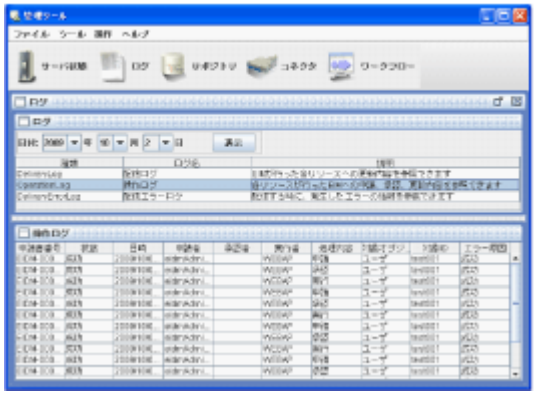


EIM による HP IceWall SSO ユーザー変更画面

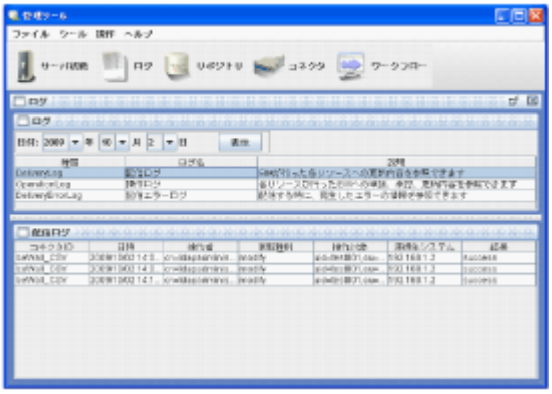


(3)監査証跡、レポート
ユーザーの申請、承認、ユーザープロビジョニング(配信)の証跡をEIM管理ツールで参照することができます。また、HP IceWall SSO登録ユーザーのID棚卸しや監査レポートの作成が可能です。

ユーザーの申請・承認履歴



IceWall へのユーザー情報配信履歴



まとめ

本技術レポートでは、SECUREMASTER/EnterpriseIdentityManagerとHP IceWall SSOの連携について、構成例と検証結果、連携ポイントを説明しました。

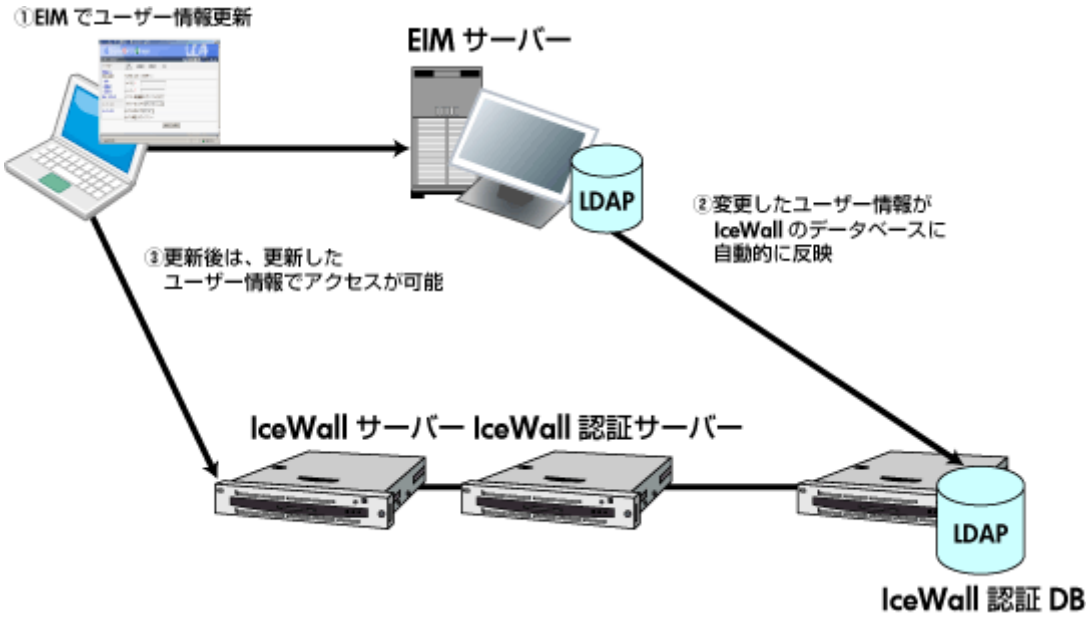
SECUREMASTER/EnterpriseIdentityManagerにより、複雑な連携ルール設計を行うことなく統合ID管理と連携し、HP IceWall SSOのユーザー管理を効率よく行うことができます。また、監査対応の証跡採取や監査レ

ポートの作成により、監査対応コストを削減することができます。
統合ID管理と連携した管理コスト削減、監査対応コスト削減に是非ご活用下さい。

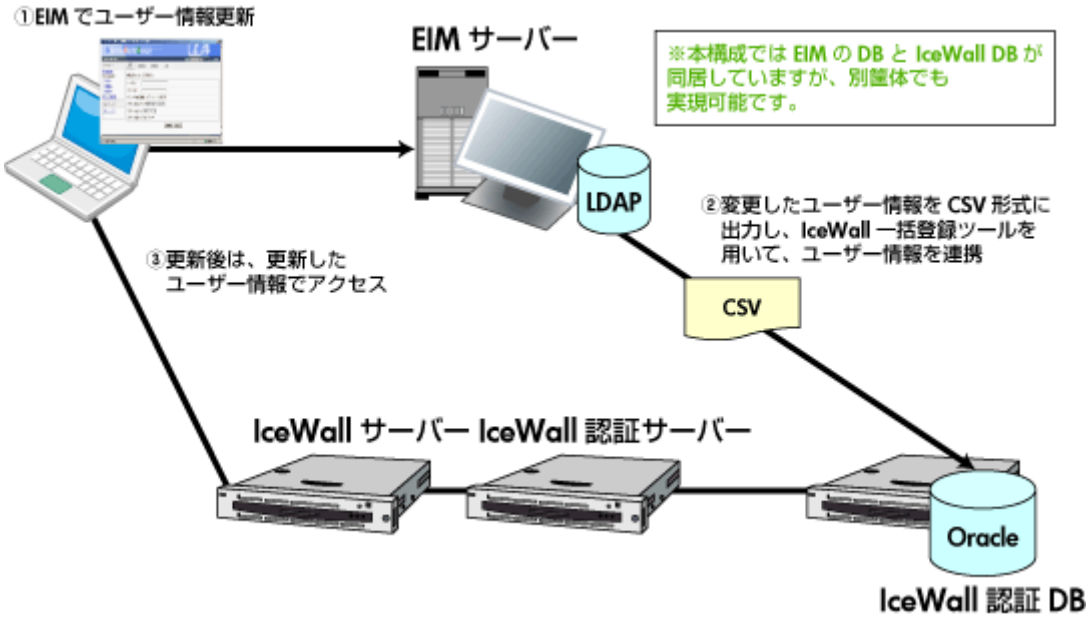
ご参考.検証構成

EIM連携の検証構成は以下の通りです。

(1)LDAP連携



(2)受信エージェント連携



検証構成詳細

サーバー、PC	製品	OS
EIMサーバー	SECUREMASTER/EnterpriseIdentityManager Ver3.0 Windows版	Windows Server 2003 StandardEdition SP2
IceWallサーバー	HP IceWall SSO 8.0 R3	Red Hat Enterprise Linux 4.0
IceWall認証サーバー	HP IceWall SSO 8.0 R3	Red Hat Enterprise Linux 4.0
IceWall認証DB (LDAP連携)	SECUREMASTER/EnterpriseDirectory Server v6.0	Red Hat Enterprise Linux 4.0
(受信エージェント連携)	Oracle 10g	Windows Server 2003 StandardEdition SP2

クライアント	WindowsXP	Internet Explorer 6.0 SP2

お問い合わせ
日本電気株式会社 スマートネットワーク事業部
E-Mail:info@security.jp.nec.com

2009.11.12 新規掲載

執筆者　　日本電気株式会社