

HP IceWall SSO

技術レポート: アイデンティティマネジメント特集



変化するビジネス環境にも柔軟に対応するソリューションを提供 - HP IceWall Identity Manager のご紹介 -

今回の技術トピックスは、前回に引き続き「Identity Management」を特集します。
弊社HPは、2005年2月1日に、効率的かつセキュアに個人情報を管理するソフトウェア「HP IceWall Identity Manager Ver.3.0」の販売を開始致しました。
今回は、このIdentity Managerの特長と、そこから生まれる新たなソリューションをご紹介します。

- » ユーザの個人情報管理に関する問題
- » フレームワーク化により新機能も充実。進化を続ける HP IceWall Identity Manager
- » カスタムアプリケーションを使用したアプリケーションセントリックなアクセス制御例

ユーザのアイデンティティ(個人情報)管理に関する問題

「システムの拡張に伴って管理するデータベースが増え、管理者の工数が増大している。」
「組織が複雑でユーザデータに余計な二重管理が発生している。」
「複数のデータベースを管理できるツールが欲しい。」
変化の激しいビジネス環境の中で、このような問題を抱えるシステム管理者も増えているのではないのでしょうか。
HP IceWall Identity Managerは、複雑な環境にまたがる個人情報を、Webベースで手軽かつ安全に管理できます。そして、効率的に管理できるだけでなく、各企業の組織・アプリケーションに適した個人情報管理システムに容易にカスタマイズできます。
また、HP IceWall SSOと組み合わせる場合、アカウントロック解除などの基本的な機能以外に、カスタマイズして、アプリケーションセントリックなアクセス制御を行えるなど、さらに柔軟な管理が可能となり、複雑で変化の激しいシステムにもスピーディーに対応します。

フレームワーク化により、新機能も充実。進化を続ける HP IceWall Identity Manager

HP IceWall Identity Managerは、新バージョン3.0へとアップし、より一層機能の進化を遂げました。
バージョン3.0の最大の特長は、ソフトウェアの構造を再設計し、拡張性・再利用性に優れたアプリケーションフレームワークへと生まれ変わったことです(図1参照)

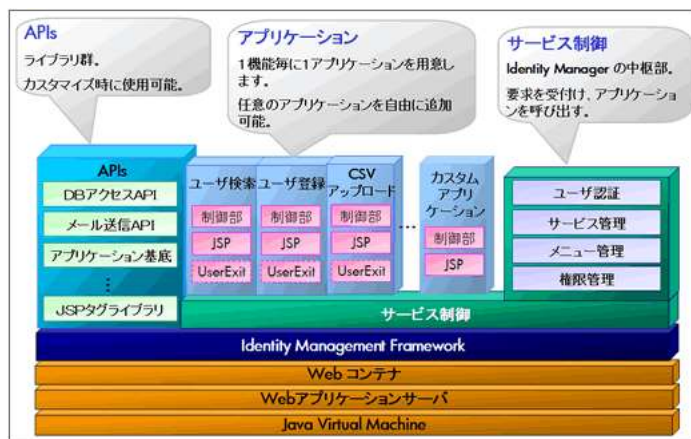


図1 HP IceWall Identity Manager構成図 (Identity Management Framework)

今回は、このフレームワーク構造にフォーカスしてHP IceWall Identity Managerの特長をご紹介します。

■ HP IceWall Identity Managerの構成

HP IceWall Identity Managerは、Webアプリケーションサーバ上で動作するWebアプリケーションフレームワークとして構成されています。
「Identity Management Framework」から上層がHP IceWall Identity Managerが提供するモジュール、それより下層が、Webアプリケーションサーバが提供する実行環境です。
フレームワークは以下の3部構成になっています。

- ・ サービス制御
ユーザからのリクエストを受け付けて、認証やアプリケーションの呼び出しを行う。
- ・ アプリケーション
リクエストに応じて検索・一覧や登録などを実際に行う。
- ・ APIs
DBアクセスやメール送信など、各種機能を提供する。

また、「Identity Management Framework」はMVCモデルに基づいて設計されています。サービス制御が「コントローラ(C)」、アプリケーションの制御部が「モデル(M)」、JSPが「ビュー(V)」に相当します。

■ フレームワーク化のメリット

フレームワーク化することで、以下のようなメリットを得ることができます。

- ・ 複雑な組織やビジネスの変化に柔軟に対応
フレームワークが提供する便利なAPIを使用して、容易に機能を追加できるようになりました(カスタマイゼーションの実現)。それにより、企業毎の個別要求やビジネスの変化に迅速かつ柔軟に対応できます。
フレームワークが提供するカスタマイゼーションには、「画面カスタマイズ」、「基本組み込み機能の一部処理変更」、「新機能の追加(カスタムアプリケーション)」があります。これらのカスタマイズは、フレームワークが提供する豊富なAPIを利用することで、短時間で容易に実現できます。また、DBアクセス機能が汎用化され、HP IceWall SSOの認証DBだけでなく、様々なDBを統合管理できます。このように、カスタマイズの柔軟性が備わったことにより、企業に散らばるシステムの個人情報を一元管理できます。
- ・ 開発コストの削減
MVCモデルを採用していることにより、各機能の役割分担は明確化されています。

機能を拡張する場合は、「サービス制御」で提供しているユーザ認証や権限管理などの処理を新たに作成する必要はありません。必要な機能部分のみを「アプリケーション」として追加するだけです。

- ・ 開発精度の均質化
カスタマイズも視野に入れた堅牢で安定した基盤を提供しているため、均質な開発精度を保つことができます。

■ HP IceWall Identity Managerのその他の特長

他にもHP IceWall Identity Managerには、以下のような特長があります。

- ・ 効率的な個人情報管理
 - 管理者の階層化管理
 - 一般ユーザのセルフサービス機能
- ・ 生産性の向上
 - パスワードの自動生成、メール自動送信機能
 - CSVアップロード・ダウンロード、パスワード初期化、複数ユーザー一括更新機能
- ・ セキュアな個人情報管理
 - ロールに基づいた権限管理
 - 監査ログ、エラーログ、トレースログの収集、保存

このように、HP IceWall Identity Managerは、個人情報管理を行うための様々な機能を持っています。「開発時には、低コストかつ迅速に企業独自の機能を追加。運用時には、セキュアで効率的な管理」。まさに、HP IceWall Identity Managerはビジネスに求められる「低コスト・スピーディー・セキュア」を導入から運用までトータルに実現した製品なのです。

それでは、具体的な例として、HP IceWall Identity ManagerとHP IceWall SSOを連携したアクセス制御の例をご紹介します。

カスタムアプリケーションを使用したアプリケーションセントリックなアクセス制御例

近年、ユーザセントリックにアクセス制御を設定するのではなく、アプリケーションセントリックなアクセス制御を実現したいというニーズが高まっています(図2)。

HP IceWall Identity Managerのカスタムアプリケーションを使用すれば、そのようなニーズも容易に実現することができます。

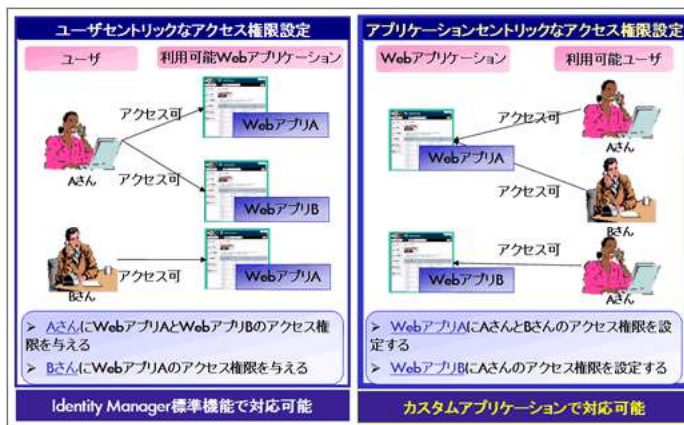


図2 アクセス権限設定の2パターン

■ アプリケーションセントリックなアクセス制御を実現するカスタムアプリケーション

アプリケーションセントリックなアクセス制御を実現するため、以下のカスタムアプリケーションを用意します(図4)。

- ・ アクセス権限設定アプリケーション
アクセス権を設定するアプリケーション。Webアプリケーション毎にグループやユーザを割り当てます。
- ・ アクセス権限シミュレーションアプリケーション
アクセス権をシミュレーションするアプリケーション。指定したユーザがどのWebアプリケーションにアクセス可能かを確認します。

カスタムアプリケーション作成手順

1. アプリケーション基底APIを継承して、「アクセス権限設定アプリケーションクラス」、「アクセス権限シミュレーションアプリケーションクラス」を用意する。
2. 作成したそれぞれのクラスに業務ロジックを追加する。DB接続などの基本的な機能はAPIで提供しているDBアクセスクラスなどを利用する。
3. 作成したそれぞれのクラスをHP IceWall Identity Managerモジュールに追加し、再コンパイルして新たにモジュールを生成する。

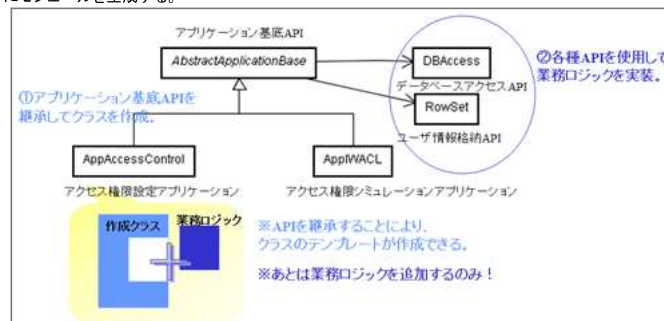


図3 カスタムアプリケーション作成クラスイメージ

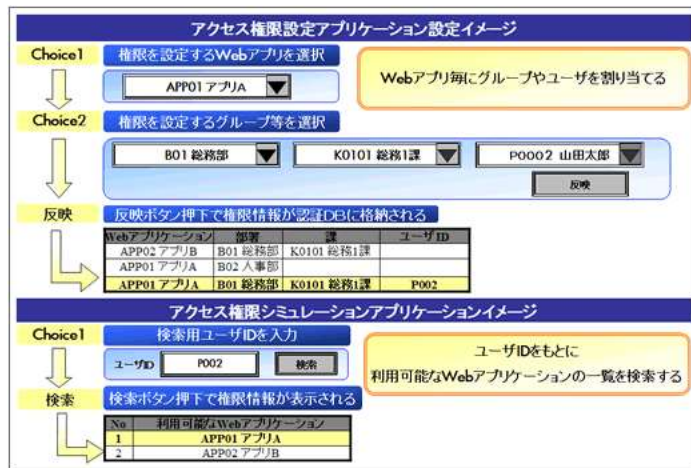


図4 各カスタムアプリケーション利用イメージ

上記のカスタムアプリケーションは、デモ用に弊社コンサルタントが開発したところ、約3日間で完成しました。このように、フレームワークが提供するAPIを利用してカスタムアプリケーションを作成すれば、企業毎に応じた業務アプリケーションを容易に作成することができます。

■ HP IceWall SSOと連携し、アイデンティティ&アクセスマネージメントを実現

日本におけるアクセスコントロール製品シェアNo.1であるHP IceWall SSOと連携することにより、ユーザの個人情報管理のみならず、バックエンドのWebアプリケーションのアクセス権限設定までを視野に入れたトータルな管理を実現します。

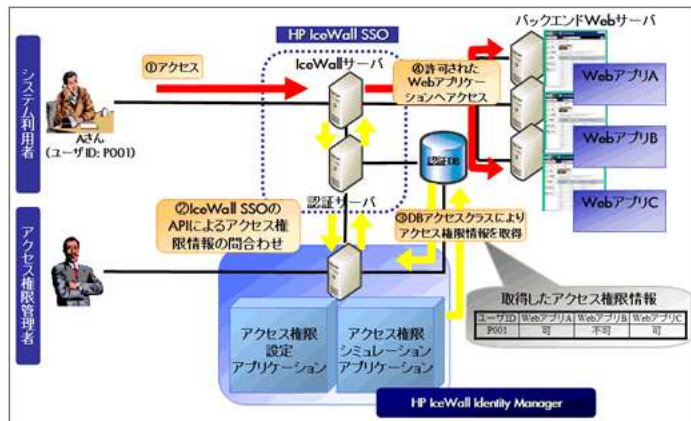


図5 アクセス制御を実現するシステム全体イメージ

アクセス制御フロー

※アクセス権限管理者が、アクセス権限設定アプリケーションを使用して事前にシステム利用者の権限を設定しておきます(アクセス権限設定イメージは図4を参照)。

1. システム利用者がブラウザからHP IceWall SSOへアクセスする。
2. HP IceWall SSOからHP IceWall Identity Managerにアクセス権限情報を問い合わせる。
3. HP IceWall Identity Managerのアクセス権限シミュレーションアプリケーションを使用して、システム利用者のアクセス権限情報を取得する。
4. HP IceWall SSOが、HP IceWall Identity Managerよりアクセス権限情報を受け取る。システム利用者は、許可されたWebアプリケーションへのアクセスが可能となる。

これは、HP IceWall SSOとHP IceWall Identity Managerを連携したトータルソリューションのほんの一例です。HP IceWall SSOとHP IceWall Identity Managerの組み合わせが提供するアイデンティティ&アクセスマネージメントソリューションで、企業が求める様々なニーズをトータルに支えます！

いかがでしたでしょうか。HP IceWall Identity Managerは、拡張性・柔軟性のあるフレームワーク構造を持ち、変貌するビジネス環境にスピーディーに対応するための様々な機能を提供しています。ご興味を持たれた方は、是非お問い合わせください！