IceWall SSOでグループアカウントを安全に利用

IceWall技術レポート

1. はじめに

お客様の環境によっては、Webメールシステム等において、個人アカウントとは別に、グループメールアカウント（通知サービスやイベント用等）・管理者アカウント（ユーザー管理やシステム管理等）など、複数の職員で1つの業務用アカウントを運用しているケースがありますが、これには様々な課題があります。
本技術レポートでは、そのようなシステムに対しても、IceWall SSOでグループアカウントを安全かつ便利に管理し、利用する方法をご紹介します。

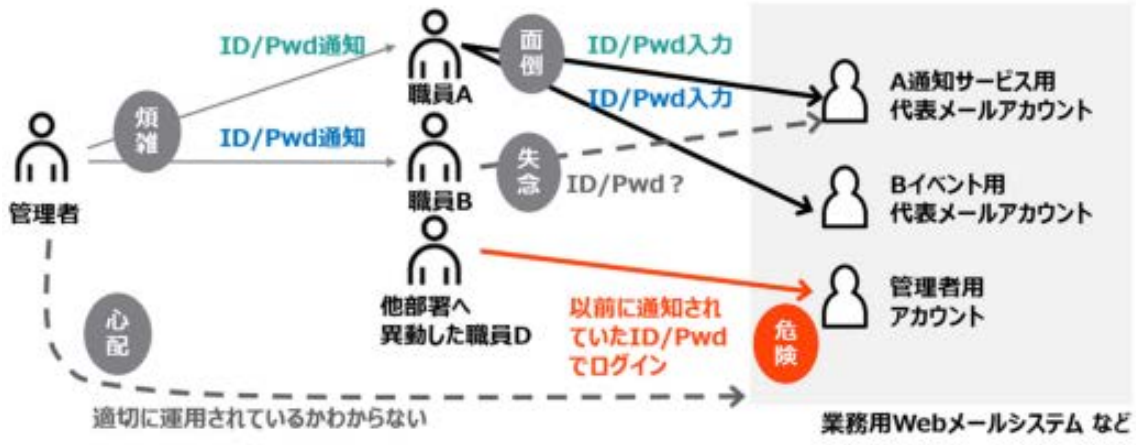
2. グループアカウントの課題

セキュリティ上、グループアカウントは利用しない事が推奨されていますが、現実的にはメールアカウントなど、業務の都合上、個人アカウントとは別に、グループアカウントを利用して複数の職員で特定の業務を行っているケースがあります。

例） グループメールアカウント（通知サービスやイベント等）
管理者アカウント（ユーザー管理やシステム管理等）

グループアカウントを利用するような運用においては、 ユーザーのログイン・ログアウト操作等が煩雑なだけでなく、セキュリティや管理の面でも様々な問題・リスクがあります。

現状の例



---

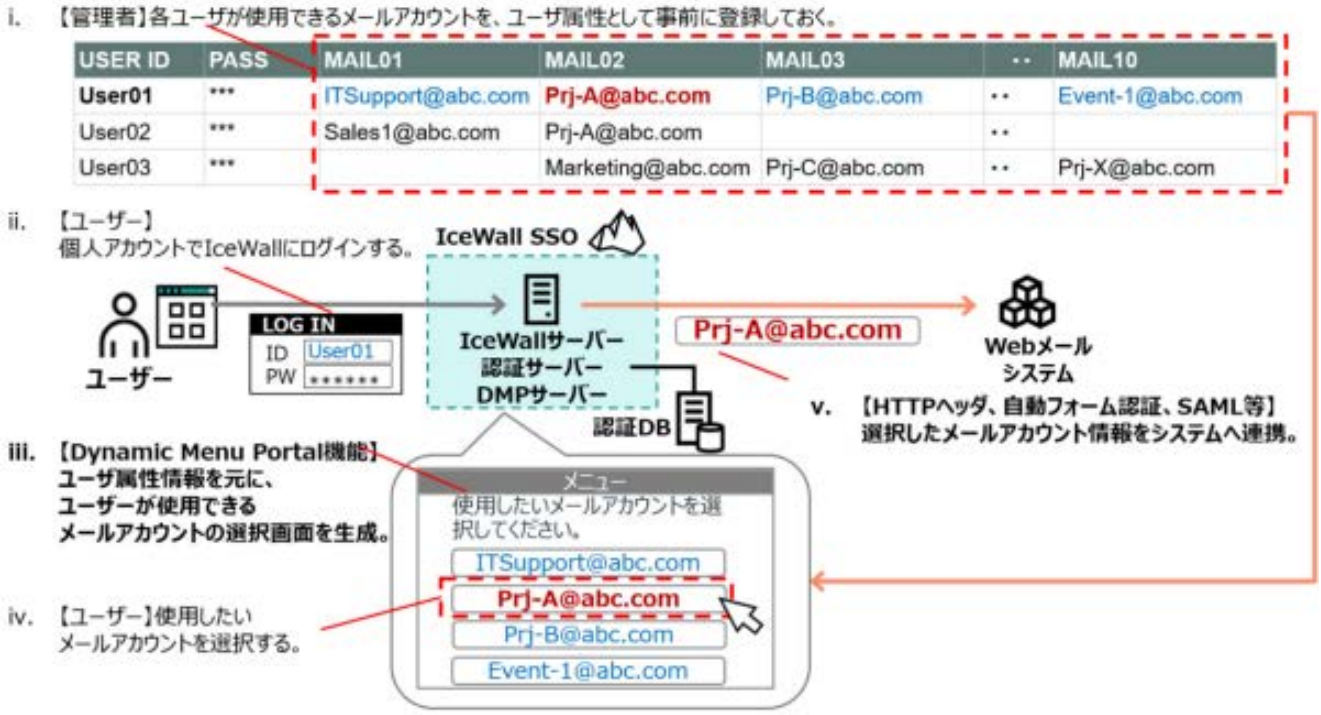
3. IceWallによる解決

前述のような課題に対して、IceWall SSOによる認証基盤の配下にシステムを配置し、IceWall SSOの機能でグループアカウントの利用を制御する実装を行うことにより、以下のように解決することができます。

#	課題	リスク	IceWallによる解決
①	管理者は、各職員にグループアカウントのID/パスワードをメールで周知している。	■ 必要な範囲やタイミングで周知するのが難しい。 ■ パスワード変更時の連絡にも手間がかかる。	職員に周知する必要がない。管理者がグループアカウントへのアクセス権を職員に付与するだけ。

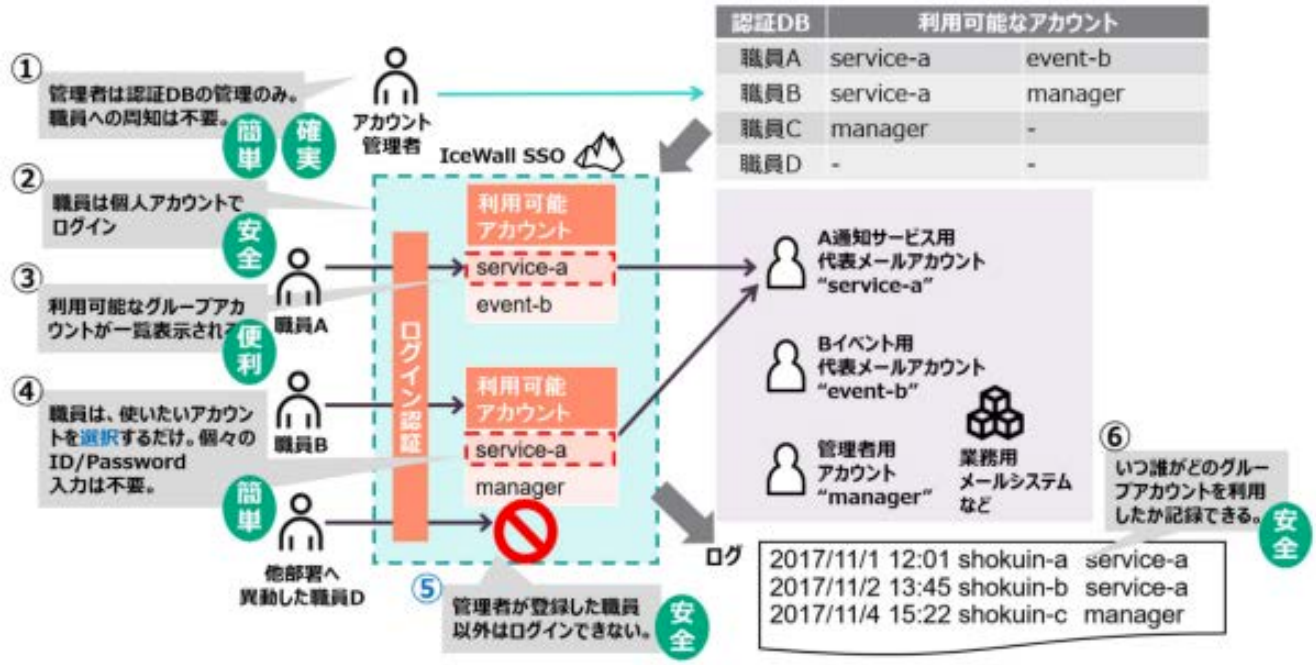
#	課題	リスク	IceWallによる解決
②	全員でパスワードを共有し、それぞれがグループアカウントにログインしている。	■ パスワード漏洩のリスクが高まる。 ■ パスワード漏洩時の影響が大きい（アカウントの一時停止、調査、パスワード再設定と周知）。	ログインは個人アカウントで行い、その後は個別のログインなくグループアカウントへアクセスできる。
③	職員は複数のID/パスワードを覚える必要があるが、利用可能なグループアカウントが増えるほど正確に覚えるのは難しくなる。	■ 職員の記憶に依存し、組織として管理が難しい。 ■ グループアカウントのID/パスワードを複数回間違えてアカウントロック。運用者の管理負担が増大。	各自が利用可能なグループアカウントが一覧表示される。（未許可のアカウントは表示されない）
④	利用の都度ログイン作業が必要で面倒。	■ 職員は多くのグループアカウントのID/パスワードを覚えられないためノートで管理している。ID/パスワード漏洩のリスクが高まる。	職員は選択画面に表示される利用可能なグループアカウントを選択するだけでシステムを利用可能。
⑤	アクセス権限を失効させる必要がある職員もグループアカウントを利用出来る。（別の部署へ異動した職員や退職者など）	■ アクセス権限を失効させる必要がある職員からの不正アクセスのリスクがある。	退職者が発生しても、グループアカウントのパスワード変更なしに、確実に利用を抑止できる。
⑥	いつ誰がグループアカウントにアクセスしたのか記録が残らない。	■ 万が一セキュリティ事故が発生しても、いつ誰がアクセスしたのか調査できない。	いつ・誰が・どのグループアカウントを利用したかログに記録できる。

本実装の処理の流れ



事前に、認証データベース上のユーザー属性に当該ユーザーの利用可能なメールアカウント名を登録しておきます（複数ある場合は、複数のユーザー属性欄に登録）。
ユーザーがWebメールにアクセスした際には、IceWallに個人アカウントでログイン（※既にログイン済みの場合はシングルサインオンによりログイン操作なし）した後、そのユーザーの利用可能なメールアカウントが一覧表示されるメニュー画面が表示され、選択するとそのメールアカウントのWebメール画面が表示される形となります。

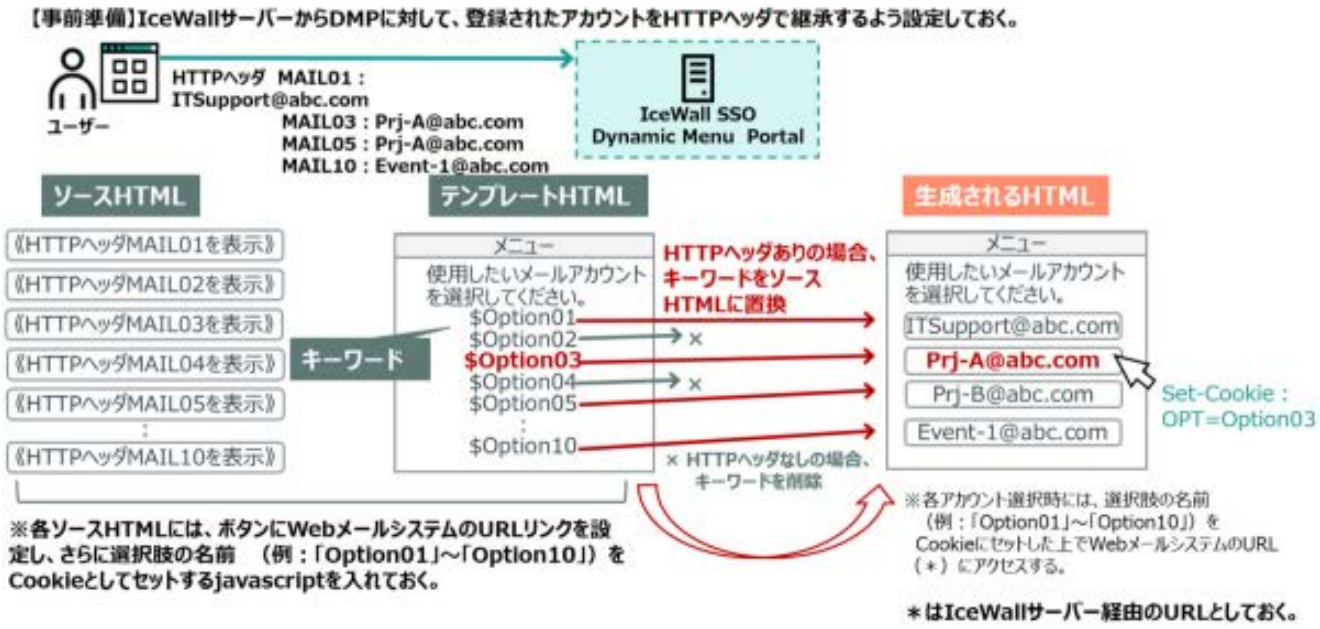
解決例



4. 実装のポイント

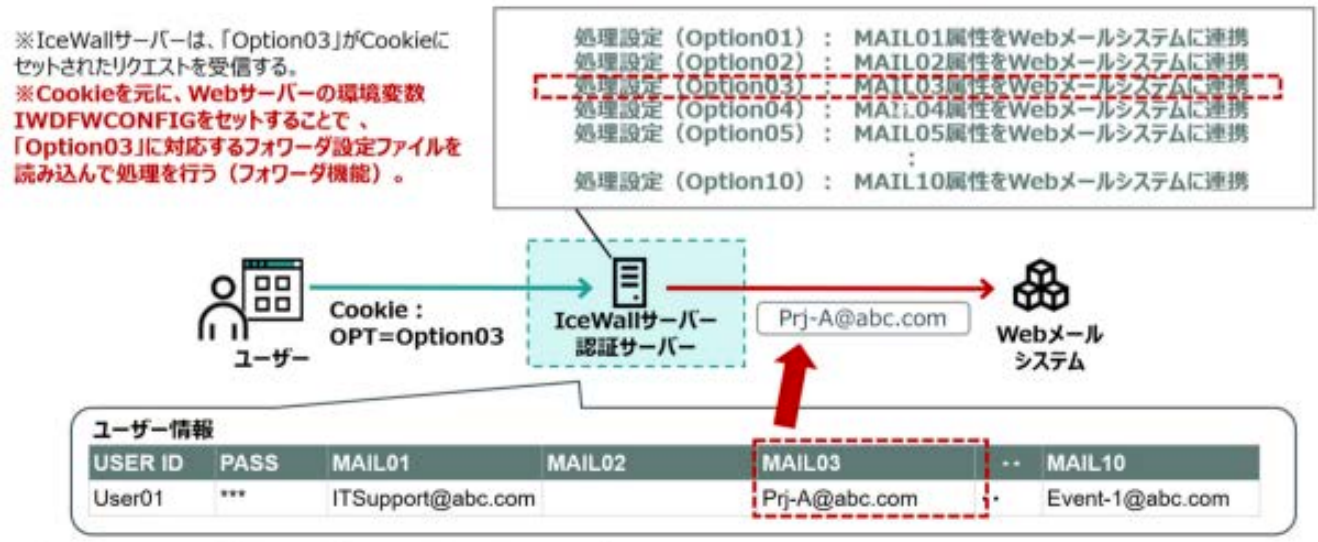
メニュー表示

「処理の流れ」のイメージにおけるメニュー画面の生成には、IceWall SSOのDynamic Menu Portal機能（ポータル画面生成機能。※IceWall SSOライセンスに無償バンドル）を使用します。
本機能では、事前に用意した画面のテンプレートHTML内に記述するキーワードを、ログインユーザーが特定の条件を満たした場合に指定したコンテンツに置き換えた画面HTMLを生成・表示することが可能です。特定の条件としては、HTTPヘッダーの条件を使用できますので、IceWall経由でDynamic Menu Portal機能にアクセスする際に、認証データベース上のユーザー属性情報（メールアカウント名）をHTTPヘッダーで送信するようにし、ユーザー属性の条件によってメニュー画面が生成・表示されるようにします。
メニュー画面に表示される選択肢のボタンには、Webメールシステムへのアクセスリンクを設定し、さらに選択肢の名前をCookieとしてセットするjavascriptを入れておきます。



アカウント選択後

「処理の流れ」のイメージにおけるアカウント選択後のWebメールシステムへの情報連携には、Webサーバーの環境変数によるIceWallサーバーの処理設定の切替とバックエンドシステムへの情報継承／認証連携機能（※IceWall SSO標準機能）を使用します。
ユーザーが先程のメニュー画面でボタンをクリックすると、IceWallサーバーに対し、Cookieに選択肢の名前がセットされた上で、Webメールシステムへのアクセスリクエストが届きます。そのCookieをWebサーバーの環境変数にセットすることで、IceWallサーバーに選択肢に応じた処理設定でバックエンドシステムへの情報継承／認証連携を行わせることができます。



※別のメールアカウントを利用したい場合は、一旦ブラウザセッションを終了します。

5. まとめ

本技術レポートでは、IceWall SSOの標準機能を使用して、グループアカウントを利用するような運用のシステムに対しても、統合された個人アカウントでのシングルサインオンを可能にすると共にセキュリティや管理面の向上も図れる実装方法をご紹介しました。バックエンドシステムのシングルサインオン対応の１つのパターンとして、本実装方法を是非ご検討ください。

2017/12/28 新規掲載

執筆者　：日本ヒューレット・パッカード株式会社

Pointnext事業統括　IceWallソフトウェア本部 認証コンサルティング部

谷垣 敦

技術レポート一覧へ →

検索のサポート

ご購入方法

製品サポート

営業へのお問い合わせ

お問い合わせ先一覧

企業情報

会社情報

アクセス

お問い合わせ

採用情報

HPEについて

インクルージョン & ダイバーシティ

サステナビリティと企業責任

経営幹部

お知らせ

ニュースルーム

イベント・セミナー

新着情報

重要なお知らせ

パートナー

パートナープログラム

認定資格制度

OEMソリューション

サポート

製品サポート

ソフトウェア & ドライバー

標準保証確認

オペレーショナルサポート

教育とトレーニング

製品リサイクル

機器部品の妥当性確認

コミュニティ

HPE Japan ブログ

リソース

お客様事例

ご購入方法

オンラインストア

HPE Customer Center

Eメール登録

ドキュメントライブラリ

Resource Library

ビデオギャラリー

金融サービス

日本 (ja)