MOSS、ISAとHP IceWall SSOの接続・その効果と注意点

本技術レポートでは、Microsoft® Office SharePoint Server（以下、MOSS)とHP IceWall SSOを組み合わせる場合の構成例と効果、技術的な注意点を記述します。
また、Internet Security & Acceleration（以下、ISA）Server を併用した場合の構成、及びその効果についても記述します。

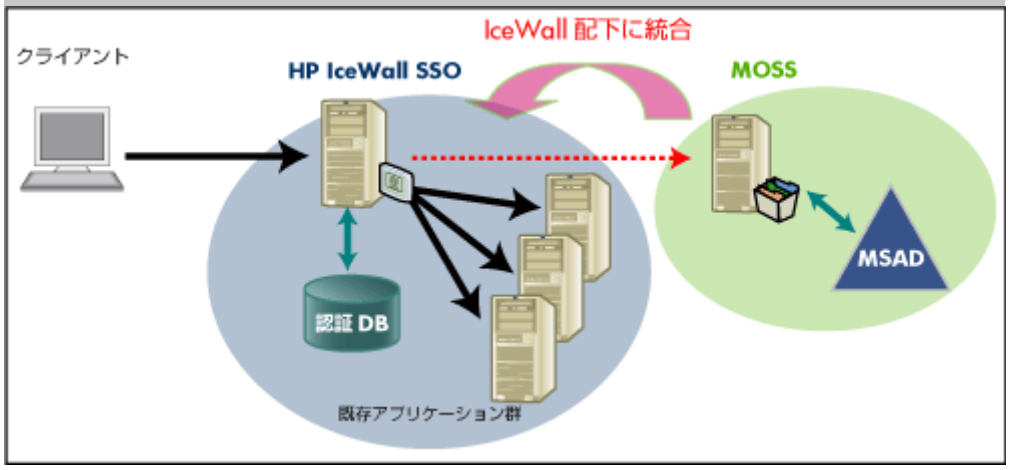
1.どのような時にMOSSとHP IceWall SSOを組み合わせるか

通常、MOSSもイントラネット環境の一部としてWindows統合認証下にて動作しますが、例えば以下の様な状況でHP IceWall SSOと組み合わせる必要があります。

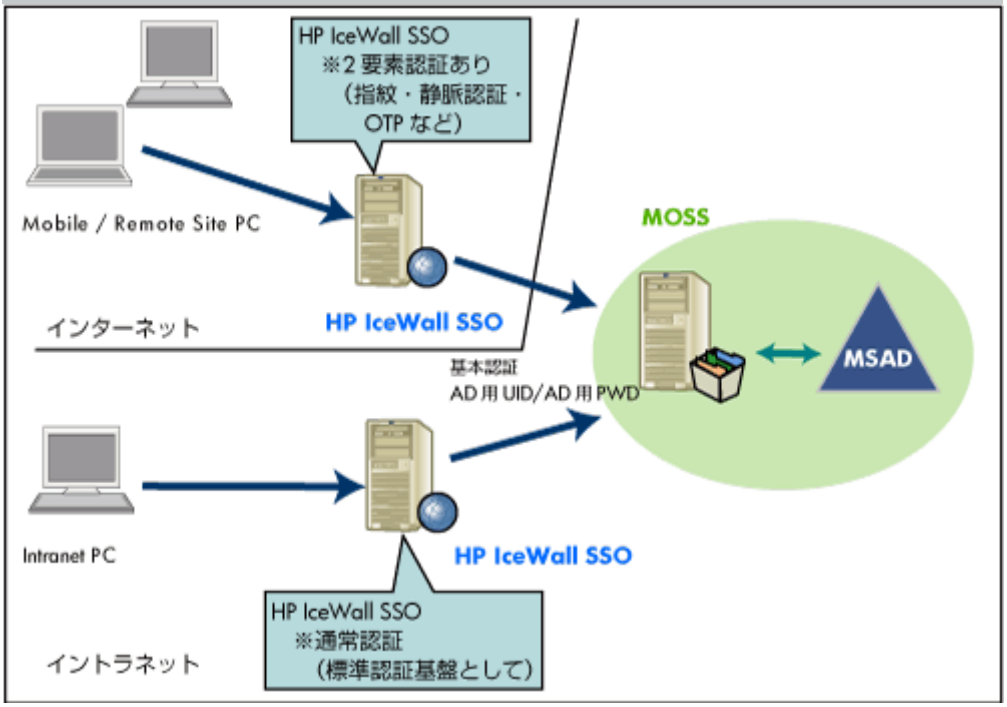
- 既にイントラネットのアプリケーションをHP IceWall SSOの認証下で統合しており、この環境にMOSSを導入する場合。もしくは既存のMOSSを含むアプリケーション群の認証をHP IceWall SSOを導入して統合したい場合。
- インターネット・イントラネットからのMOSSへのアクセスに対して、HP IceWall SSOが提供する2要素認証等の強力な認証を適用したい場合。

このような場合、HP IceWall SSO のリバースプロキシ機能を経由して、MOSSがアクセスするように構成する必要があります。

HP IceWall SSO 認証配下にMOSSを統合する



インターネット・イントラネットからMOSSへアクセスする



2.MOSS と HP IceWall SSOを組み合わせる場合の方式と注意点

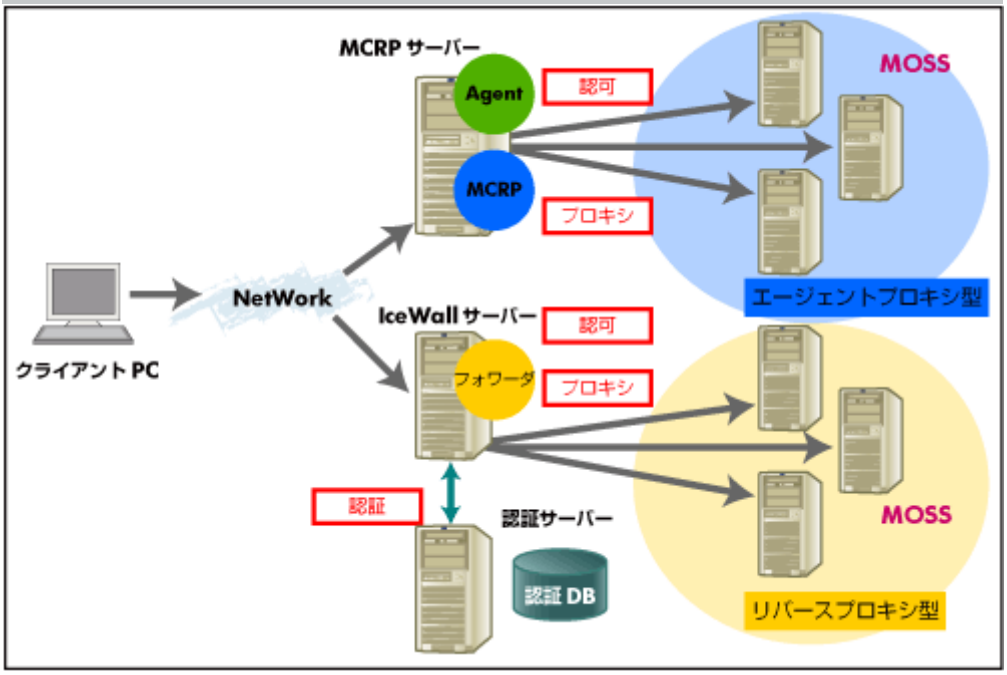
HP IceWall SSOのバックエンドサーバーとしてMOSSを使用する場合は様々な方式が可能です。ここでは、使用するテクノロジー毎に推奨される構成、注意点などを記述します。

2.1.リバースプロキシ製品の選択

HP IceWall ファミリーのリバースプロキシ製品には、CGIタイプの製品であるHP IceWall SSO(フォワーダ)と、Apacheのモジュールとして動作するHP IceWall MCRPがあります。MOSSをバックエンドサーバーとして接続する場合は、このどちらでも使用できます。ただし、HP IceWall MCRPには認証認可(アクセスコントロール)機能がありませんので、認証認可をさせる場合は、HP IceWall MCRP に加えてHP IceWall SSO と、HP IceWall SSO エージェントオプションが必要となります。

HP IceWall SSO(フォワーダ)を使用した場合(リバースプロキシ型)と、HP IceWall MCRPを使用した場合(エージェントプロキシ型)のシステム構成図を以下に示します。

リバースプロキシ製品の選択による違い



2.2.リバースプロキシでのアクセスURL変換方式

通常リバースプロキシを介してWebアプリケーションにアクセスする場合は、クライアントからのアクセス先URLが変化します。これはクライアントからアクセスされるサーバーが直接バックエンドサーバーではなく一度リバースプロキシを経由するため、アクセス先のホスト名がリバースプロキシサーバーになるためです。この事はバックエンドサーバーが出力し、クライアントに送信されるコンテンツの内容に、アクセス先のURLが含まれている場合に問題となります。
この事へ対応する一つの方法としてHP IceWall SSOのフォワーダやHP IceWall MCRPには、バックエンドサーバーから送られたコンテンツをクライアントに送信する際に、コンテンツ内のURLをリバースプロキシ経由のURLに変換する機能があります。しかしMOSSから出力されるコンテンツは多岐に渡るため、コンテンツに含まれる全てのURLを変換することがとても難しくなります。
このため、MOSSをバックエンドサーバーとする場合には、HP IceWall SSOのフォワーダやHP IceWall MCRPが提供するURL変換の機能を使用せずに、「オリジナルURL方式」※1にて接続して下さい。

※1 「オリジナルURL方式」についての詳細はこちらの技術レポート記事をご参照ください

2.3.MOSSの認証方式に合わせたHP IceWall SSOの認証情報継承機能の使用

HP IceWall SSOでは、ログインユーザーのIDとパスワードや認証DB内に格納されているユーザーの属性情報をバックエンドサーバーに引き渡すことが出来ます。この際に使用できる認証方式としては、基本認証(Basic認証)とフォーム認証がありますが、MOSSとの接続を行う場合は基本認証を使用して下さい。
また、これに合わせてMOSS側の認証方式を基本認証に設定する必要があります。

なお、基本認証を使った場合でも、Kerberos認証設定でアカウントの委任を構成するのと同様に、2ホップの認証を行うことができ、Excel Services や Business Data Catalogなどの外部のリソースへアクセスする場合で

も、同じユーザー権限を利用することが可能です。また基本認証では、パスワード情報が平文でネットワーク上を流れることになります。このため、リバースプロキシとMOSS間のネットワークはHTTPSを使って通信を暗号化するか、プライベートなセグメントとし、一般ユーザーから直接アクセスができないようにする事をお勧めします。なおMOSSへアクセスできるクライアントを制限する方法としては、MOSSのサービスをホストするIIS Webサイトにて、IPアドレス制限を構成し、IceWallとのみ通信を許可します。

また、リバースプロキシ経由以外でのアクセス経路が必要な場合は、MOSSのWebアプリケーションの拡張を行い、Windows統合認証を使ったIIS Web サイトを、特定のホストヘッダーと関連づけて別途構成します。

基本認証使用時の注意点

2.4.HP IceWall SSOセッションクッキーの保存方式

HP IceWall SSOはセッションをクッキーにて保存します。通常のWebブラウザではクッキーはオンメモリでも問題はありませんが、MOSSではクライアントとしてWebブラウザ以外の(Office関連製品)も使用します。これらにセッション情報を引き継ぐため、クッキーの保存場所をメモリ上だけでなく、一度「Temporary Internet Files」フォルダ内のファイルクッキーとする必要があります。

このようにHP IceWall SSOフォワーダやHP IceWall MCRPを構成する際には、以下のように設定してください。

認証モジュールの設定ファイル(cert.conf) にて以下を設定します。
COOKIEEXP=1、LOMETHOD=0

LOMETHOD=0を設定できない場合は、
HP IceWall SSOフォワーダの場合は「フォワーダ設定ファイル」(dfw.conf)、
HP IceWall MCRPとHP IceWall SSO エージェントオプションを使用している場合は「エージェント設定ファイル」(agent.conf)において COOKIEATTR項目に「Thu, 1-Jan-2030 00:00:00 GMT」など未来の日付を設定する。

この設定によりブラウザ以外からのアクセスにもセッションが引き継がれるようになります。

2.5.セッションタイムアウト設定

MOSSをバックエンドサーバーに設定する場合、HP IceWall SSOのセッションタイムアウトの長さにも注意が必要です。セキュリティ リスクと利便性のトレードオフとなりますが、再認証が煩雑にならないように数十分から数時間のタイムアウトを設定します。

2.6.補足： Active Directory®内のユーザーIDについて

HP IceWall SSOにてActive Directory®を認証データベースとして使用する際には、ユーザーのcn(ユーザー名)と、ユーザーのWindowsログイン名が同一であり、ASCII文字列であることが必須となりますのでご注意下さい。

3.Internet Security & Acceleration Server との連携

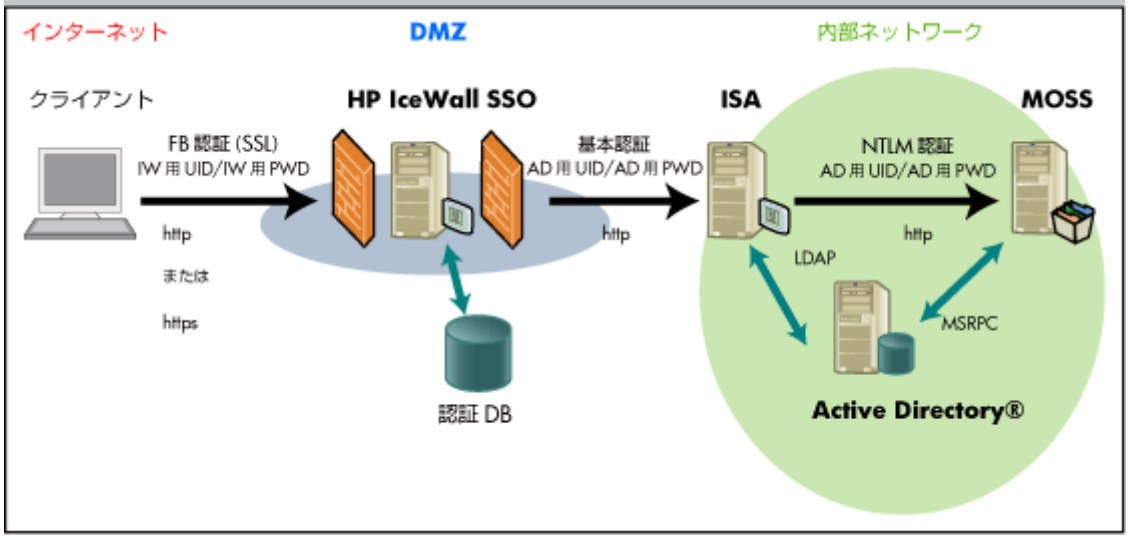
まずISA Serverとは、ファイアウォール機能を備えたマイクロソフトのセキュリティゲートウェイ製品です。ここでは、HP IceWall SSOとMOSSの環境へISA Serverの追加が有効となるシナリオを紹介します。

≫ Microsoft® Internet Security & Acceleration Server製品サイト

(1) HP IceWall SSO導入時に既存MOSS環境への変更を最小化

前述の通り、MOSSをHP IceWall SSOの統合認証環境へ組み込む際には、MOSS側の認証方式を基本認証に設定する必要があります。例えば、ネットワークとMOSSの管理者が異なる場合、その変更は容易に行えないことも考えられます。そこで、HP IceWall SSOとMOSSとの間にISA Serverを設置すれば、MOSS側は従来のWindows統合認証モードのままで環境を構築することができます。後述の検証結果にある通り、Excel ServiceでMOSSからバックエンドのデータベースを参照するなど、Kerberosチケットを用いた資格情報の委任が必要な利用形態にも対応可能です。

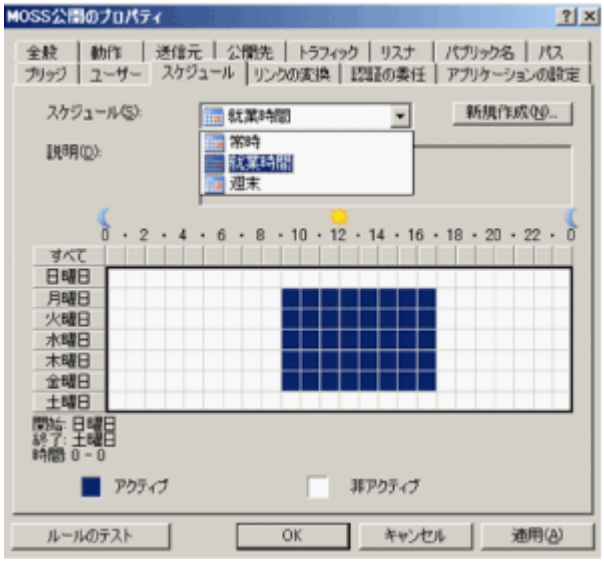
ISAによる 基本認証->Kerberos認証の変換



(2) インターネット経由でイントラネットのMOSSへアクセス

自宅や外出先からも社内のMOSSへアクセスさせるためには、インターネットへMOSSを安全に公開する必要があります。

ISA ServerにはMOSS専用に「公開ウィザード」が用意され、10ステップ程度でMOSSをHP IceWall SSO経由でインターネットへ簡単に公開することができ、MOSSの利用可能な時間帯を設定することもできます。

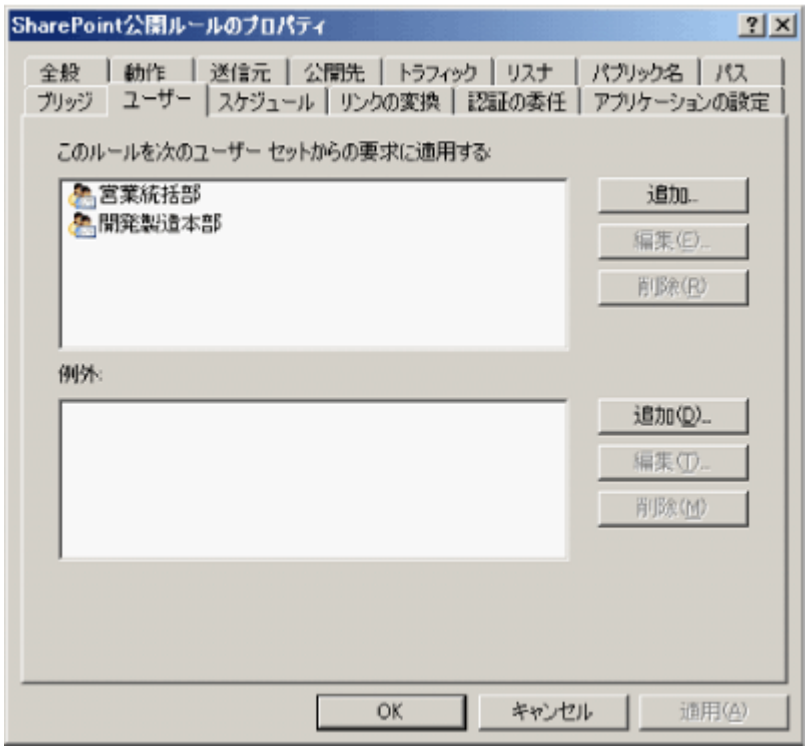


この公開用ウィザードは、Internet Information Services（以下、IIS）やExchange Server （Outlook® Web Access）用にも提供されています。

(3) Windows環境のアクセス管理を集約

異種混在プラットフォーム環境において、認証をHP IceWall SSOで統合しながら、例えばISA Server配下にMOSS、IIS、Exchange Serverを設置し、マイクロソフトサーバー製品群の認可管理を容易に集中化することができます。

ISA Server側で認可情報をActive Directory®のグループオブジェクトを用いて設定すれば、MOSSの前段にあるISA で事前にActive Directory® のグループ(ユーザー)によるアクセス制御が可能となります。また、組織変更によるグループメンバシップ情報の変更がISA Server側へも自動で適用されます。



この様に、HP IceWall SSO(MCRP)とISAサーバーの連携は、Windowsドメイン環境とのHP IceWall SSO連携に強力なソリューションとなります。

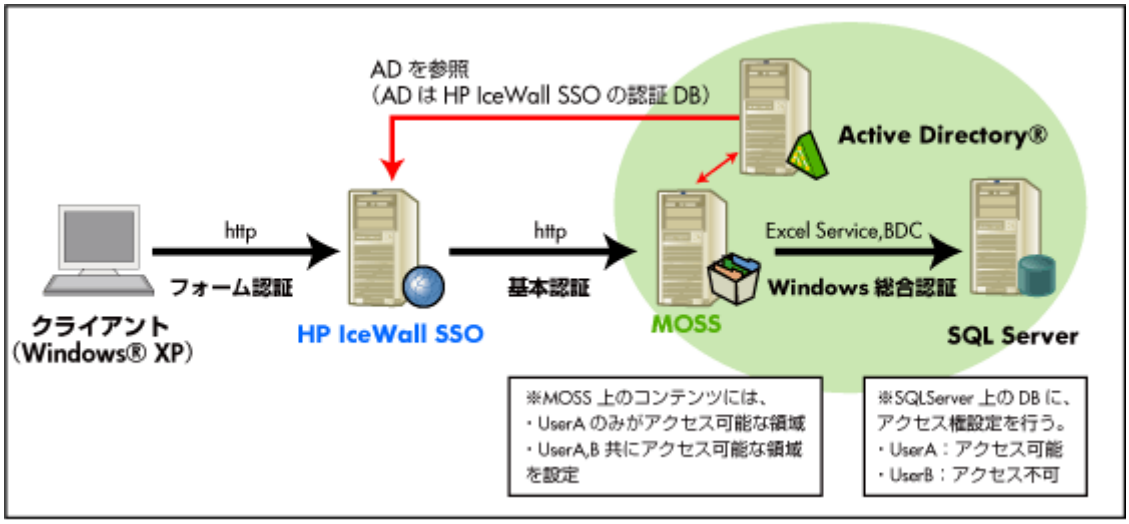
4.接続検証

これまで述べました「MOSS + HP IceWall SSO」、「ISA + MOSS + HP IceWall SSO」の接続について、実際の環境で接続検証を行いました。その内容と結果を説明します。

4.1.システム構成

4.1.1. MOSS + HP IceWall SSO

検証のシステム構成は次の図のとおりです。



この構成でポイントとなる点を以下に記述します。

(1) HP IceWall SSOへの認証はフォーム認証を使用

- HP IceWall SSOは認証ディレクトリとして、MOSSで実行しているADを参照

(2) MOSSの認証は基本認証を使用

- ユーザー名のみ(ドメイン名なし) のユーザー指定にて認証を通すために、MOSSのIISの設定である、既定のドメインの設定を行う。

(3) URL変換の方法

- HP IceWall SSOではURL変換は行わない
- MOSS側では代替アクセスマッピングを構成しない

(4) 永続化クッキー

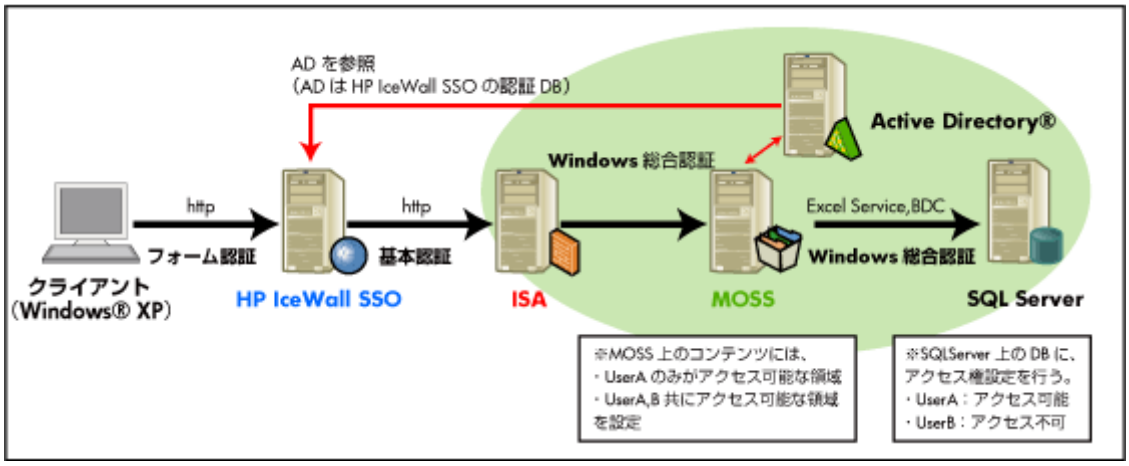
- HP IceWall SSOでは永続化クッキーを使用

(5) Excel Service, BDCのセキュリティ設定

- Windows統合認証を使用するように設定

4.1.2. ISA + MOSS + HP IceWall SSO

検証のシステム構成は次の図のとおりです。



この構成でポイントとなる点を以下に記述します。

(1) HP IceWall SSOへの認証はフォーム認証を使用

- HP IceWall SSOは認証ディレクトリとして、MOSSで実行しているADを参照

(2) MOSSの認証はKerberos認証を使用

(3) ISAの認証は基本認証を使用

(4) ISAの設定

- Kerberos認証を保持した形でMOSSを公開するよう設定
- MOSS側で2ホップでも認証情報を渡せるように、更新プログラムを適用し、Kerberos認証のフラグにチェックを入れるスクリプトを有効化する。
  (参考技術情報はこちら➡)

(5) URL変換の方法

- HP IceWall SSOではURL変換は行わない
- MOSS側では代替アクセスマッピングを構成しない
- ISA側ではURL変更を行わないように設定

(6) 永続化クッキー

- HP IceWall SSOでは永続化クッキーを使用

(7) Excel Service, BDCのセキュリティ設定

- Windows統合認証を使用するように設定

4.2.検証結果

検証結果は下記の通りとなりました。
※上記の2つ構成とも同じ結果

検証項目	検証結果
Office ドキュメントの参照	認証されることなくファイルを開くことが可能
Office ドキュメントの編集	直接保存することが可能
エクスプローラビューの動作確認	エクスプローラーで参照可能
外部DBを参照する Excel Serviceの動作確認	ユーザーの権限設定に応じた動作が可能 • UserAは、アクセス可能 • UserBは、アクセス不可 （UserBはSQL Serverへのアクセスを許可していないため想定された動作）
外部DBを参照する Business Data Catalogの動作確認	ユーザーの権限設定に応じた動作が可能 • UserAは、アクセス可能 • UserBは、アクセス不可 （UserBはSQL Serverへのアクセスを許可していないため想定された動作）
検索の動作確認	ユーザーの権限設定に応じた動作が可能 （各ユーザーが権限を保持するコンテンツのみ検索結果に表示される）
Form Serviceの動作確認	動作可能

5.まとめ

本技術レポートでは、MOSSとHP IceWall SSO 及び ISAサーバーとHP IceWall SSOの連携について、構成例とその効果、技術的な注意点を説明しました。
Windowsドメイン環境でHP IceWall SSOとの連携を行なう際には本ソリューションを是非ご活用ください。

6.参考URL

≫ Microsoft® Office SharePoint Server 2007 自習書 基本用語リファレンス
≫ ISA設定に関するTips

2009.6.10 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 コンサルタント 佐藤 義昭

関連技術レポート
≫ マイクロソフトソリューションとHP IceWallソリューションの連携
MOSS、ISAとHP IceWall SSOの接続・その効果と注意点（本レポート）
≫ Microsoft Active Directory Rights Management サービスと□HP IceWall SSOとの連携効果