Microsoft® Active Directory Rights Management サービスとHP IceWall SSOとの連携効果

0.はじめに

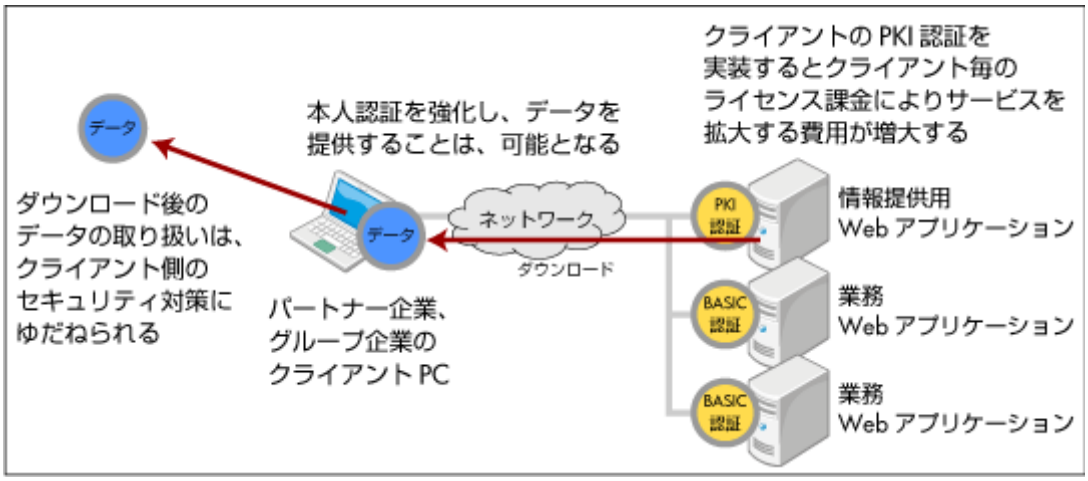
本レポートでは、Active Directory® Rights Management サービス(AD RMS)をMicrosoft Office Share Point™ Service(MOSS) ＋Information Rights Management(IRM)フレームワークで使用し、その環境をHP IceWall SSOを配下にする場合の効果と構成例、技術的な注意点を記述します。

1.連携の背景

・従来、パートナー企業、グループ企業との情報の提供手段として、PKIを利用した情報提供方法が主流となっていました。

下記の問題点があります。

- 年間の運用費用が高い。すべてのWebアプリケーションに適用が難しい
- クライアントとの認証は強化できるが、ダウンロード後のファイルに対するセキュリティ対策がクライアント側にゆだねられるため、情報提供をした後の漏えい対策ができない

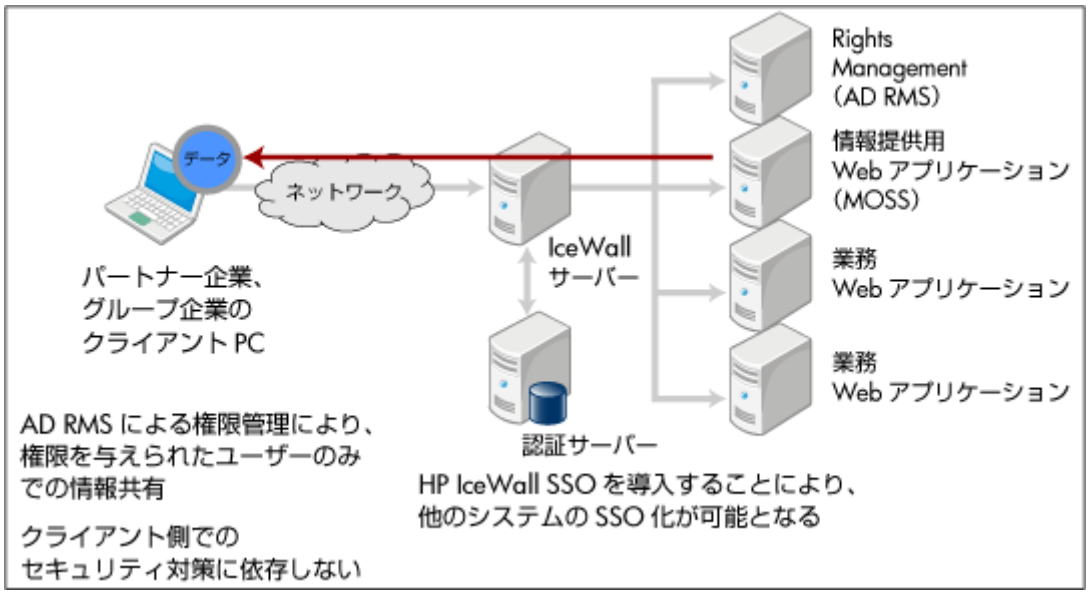


2.連携による効果

・HP IceWall SSOとマイクロソフト社のRights Managementソリューションであ AD RMSとMOSSとの組み合わせにより、情報漏えい対策と認証の拡張も可能となります。

これにより下記の効果があります。

- PKIを利用したクライアント認証よりもコストを抑えられます。
- SSOソリューションを導入することにより、認証機能の統合と将来OpenID等の認証連携機能も実装が可能となります。
- Rights Managementソリューションを導入することにより、情報提供後の情報漏えい対策を行うことが可能となります。

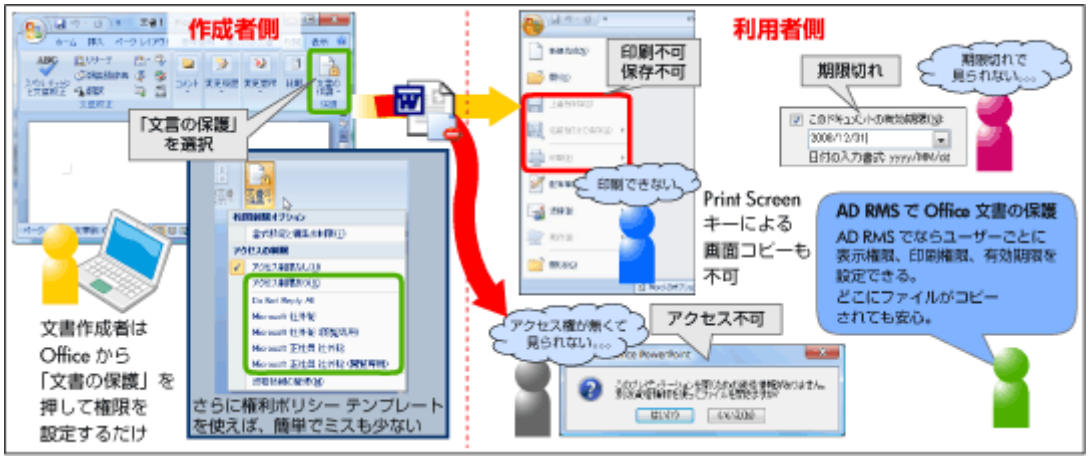


3.各ソリューションの説明

■ Active Directory Rights Management サービス

Windows Server® 2008 の Active Directory Rights Management サービス (AD RMS) は、電子メールやファイル、コンテンツなどの情報漏えいを防ぐデータ保護基盤を提供します。情報を暗号化で保護し、ユーザー権限に基づいて転送や参照、コピー、編集、印刷などの操作を制限することが可能です。この制御ポリシーは、情報の形式がドキュメント、スプレッド シート、プレゼンテーション、電子メール メッセージのいずれでも、どこに移動し、どこに格納されても、情報と共に保持されます。

AD RMS は、Active Directory フォレストに導入することができ、RMS クライアントおよび IRM 対応アプリケーションを実行するクライアントから保護機能を利用できます。RMS クライアントは、Windows Vista 以降に標準搭載されており、Windows® XP 以前の場合は Windows RMS Client SP2 を利用できます。IRM 対応アプリケーションとしては、Office 2003、Office 2007、XPS ビューアーおよび Rights Management Internet Explorer アドオンがあります。



■ AD RMS とSharePoint テクノロジとの連携

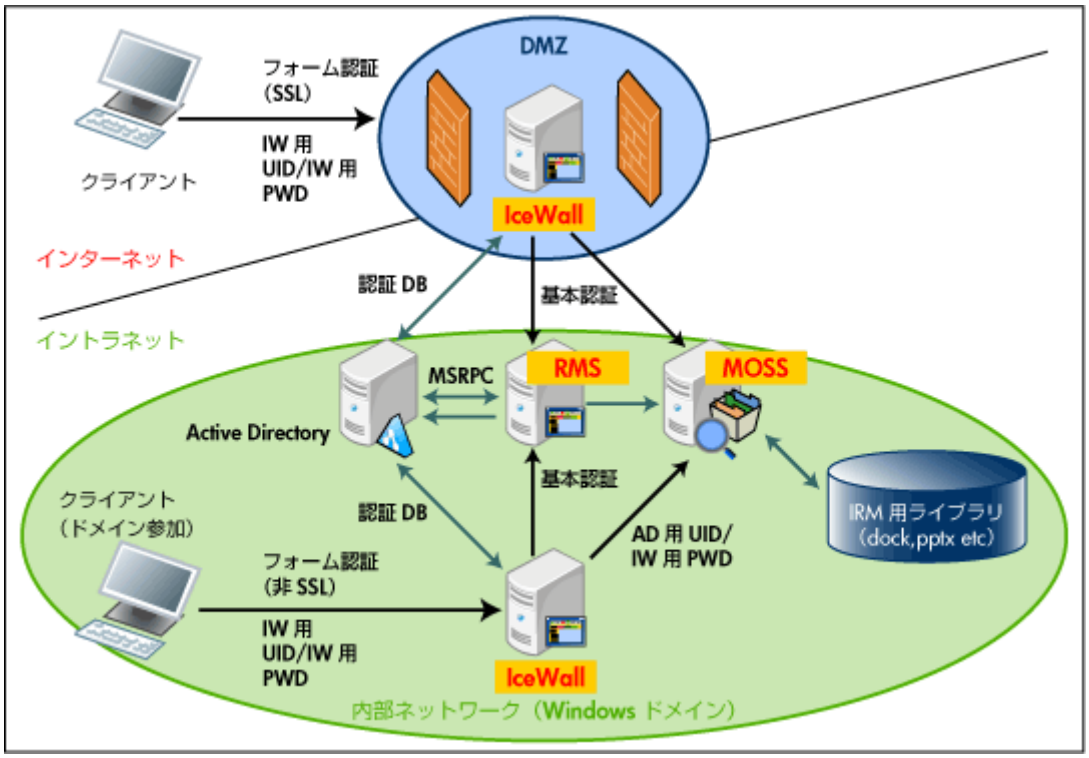
Microsoft Office SharePoint Server (MOSS) 2007 は、AD RMS/IRM の保護テクノロジと統合でき、イントラネット コンテンツの保護を強化できます。MOSS のドキュメント ライブラリでAD RMS/IRM との統合機能を有効化すると、ユーザーはそこにコンテンツを保存するだけで、閲覧、編集、コピー、印刷などの操作権限が自動的に設定されます。この統合により、SharePoint の強力な全文検索機能をユーザーに提供しながら、コンテンツがSharePoint からダウンロードされた際も、高度なセキュリティで保護されます。

4.RMS+MOSS IRM と HP IceWall SSOの構成と注意点

AD RMS + MOSS IRMをHP IceWall SSOのバックエンドとして使用する場合の推奨される構成、注意点などを記述します。

4-1 システム構成

RMS+MOSS IRM+ HP IceWall SSOの推奨するシステム構成を以下に示します。



4-2 HP IceWall SSOについて

HP IceWall SSOの構成では、以下の点について考慮します。

(1) 認証方法

MOSS,RMSへの代行認証は基本認証にて行うよう設定を行います。

(2) 認証データベース

認証データベースはMOSS、RMSが参照するADを使用します。

※他の認証データベースを使用する場合は、ADとユーザーの同期が行われている必要があります。

(3) MOSS,RMSへの接続方式について

MOSS、RMSとの接続は、URL変換機能を使用せずに、「オリジナルURL方式」を推奨します。

(4)セッションCookie

HP IceWall SSOのセッションクッキーは永続化クッキーを使用します。

※HP IceWall SSOとMOSSの連携時の注意点を記載した技術レポート「MOSS、ISAとHP IceWall SSOの接続・その効果と注意点」も合わせてご確認ください

4-3 MOSSについて

MOSSの構成では、以下の点について考慮します。

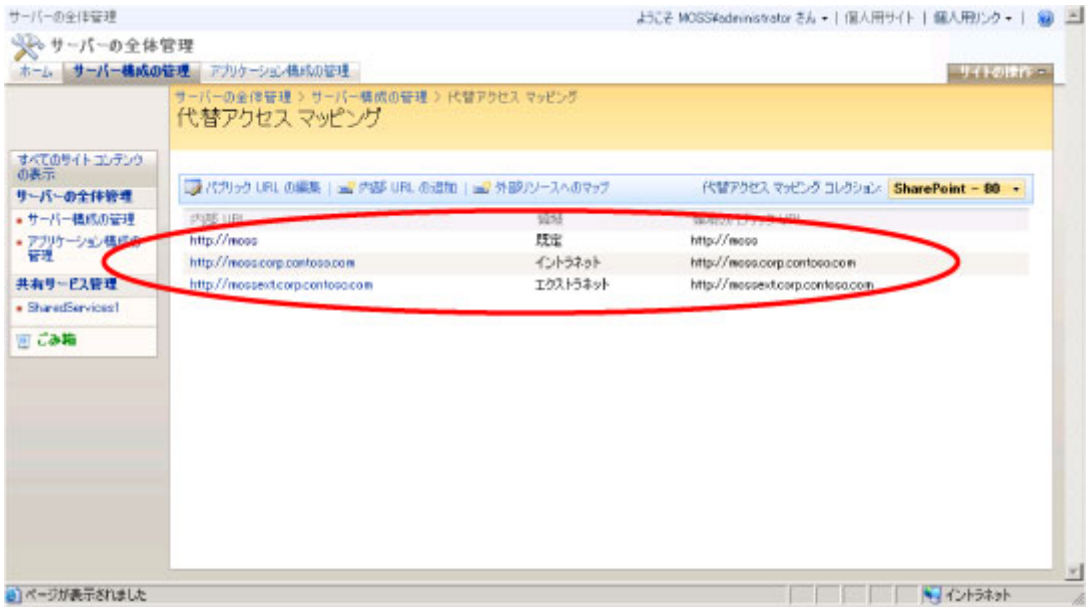
(1)認証方法の変更

Webアプリケーション(IIS)の認証方法を基本認証に設定します。

(2)代替アクセスマッピング

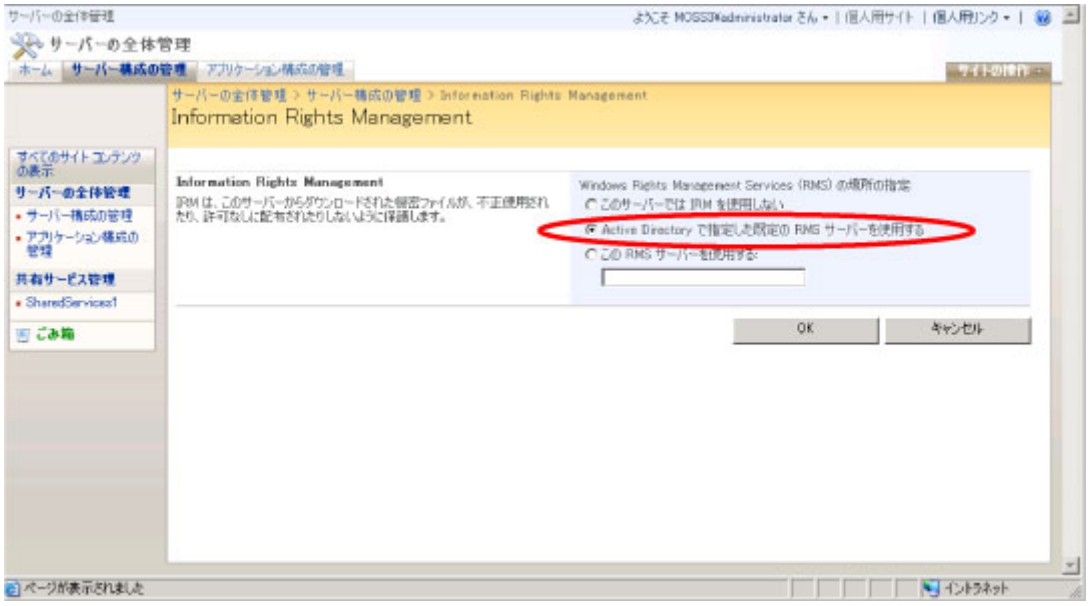
HP IceWall SSO経由でアクセスするURLを代替アクセスマッピングに追加します。

このとき、イントラネット、エクストラネットで使用するURLの構成をそれぞれ追加します。

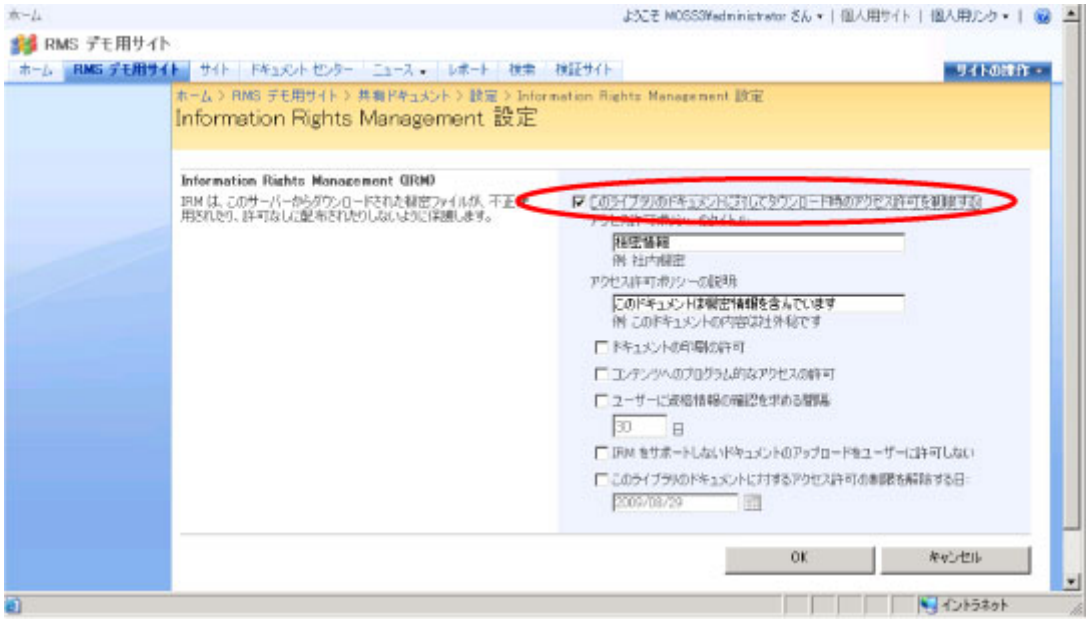


(3)IRMライブラリの有効化

IRM機能の有効化を行います。



(4)ドキュメントライブラリのIRM利用設定
IRM機能を利用するドキュメントライブラリで、IRM機能を有効化します。

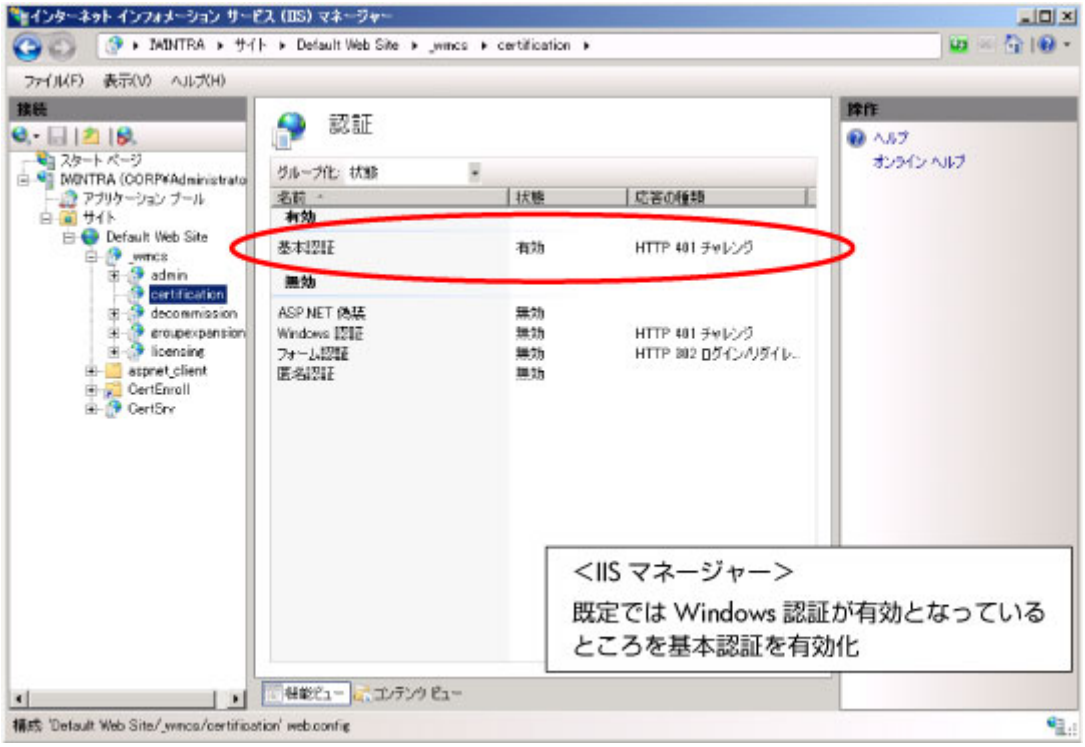


4-4 RMSについて

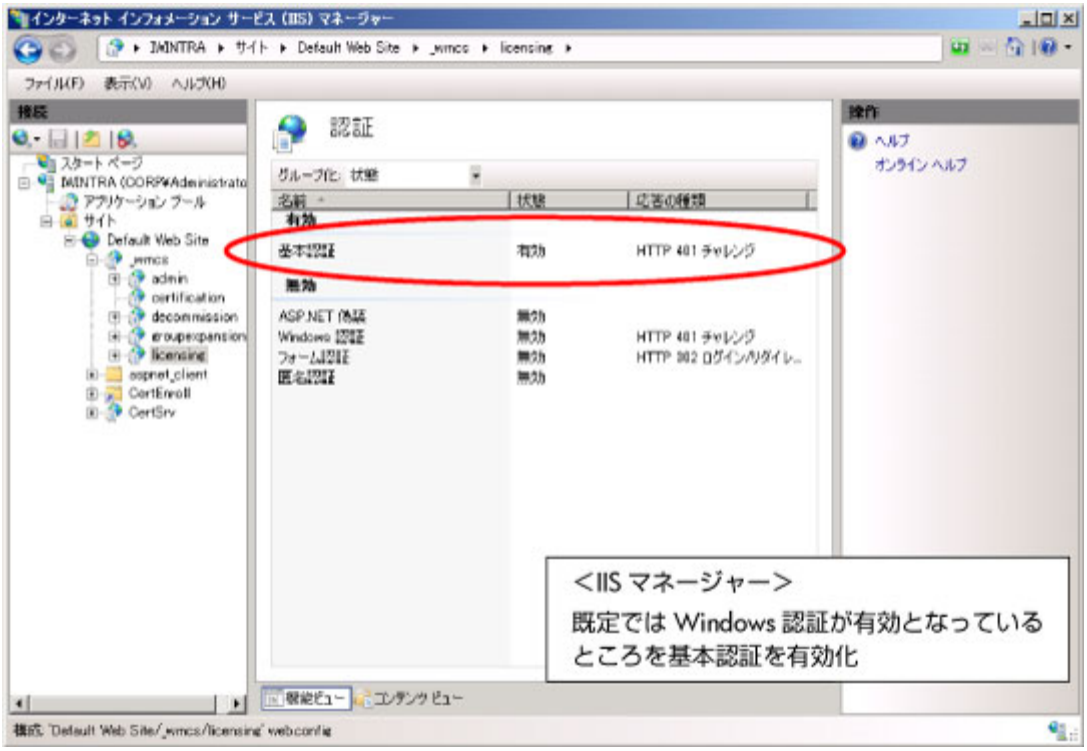
RMSの構成では、以下の点について考慮します。

(1) AD RMS サーバーで基本認証を構成
AD RMS の証明書発行プロセスで利用される認証方式を基本認証に変更します。
・構成方法
基本認証モジュールを役割サービスから追加します。
標準では AD RMS 構成時に基本認証モジュールはインストールされませんので、以下について基本認証を有効化します。
/_wmcs/certification
/_wmcs/licensing

IIS – /_wmcs/certification の構成



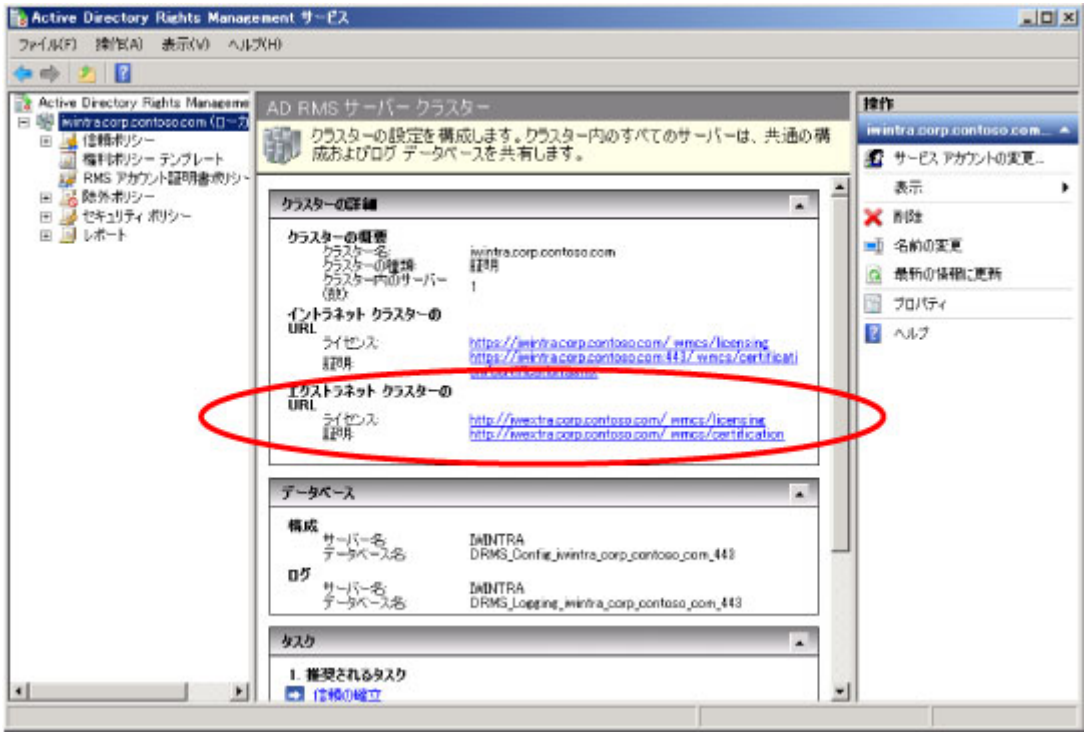
IIS –/_wmcs/licensing の構成



(2)クラスター URL の構成

AD RMS 管理コンソールより、エクストラネット クラスター URLの設定を行います。

詳細設定はAD RMS サーバープロパティにて行います。

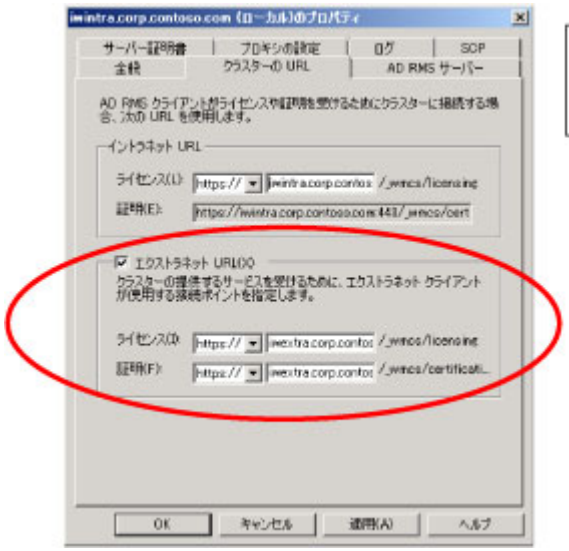


AD RMS サーバープロパティの「クラスター URL」では以下を設定します。

・AD RMS のサービスを提供している場所に関する設定

・イントラネット クラスター URL(社内アクセス) とエクストラネット クラスター URL (社外アクセス)

・HTTP or HTTPS による構成に関する設定

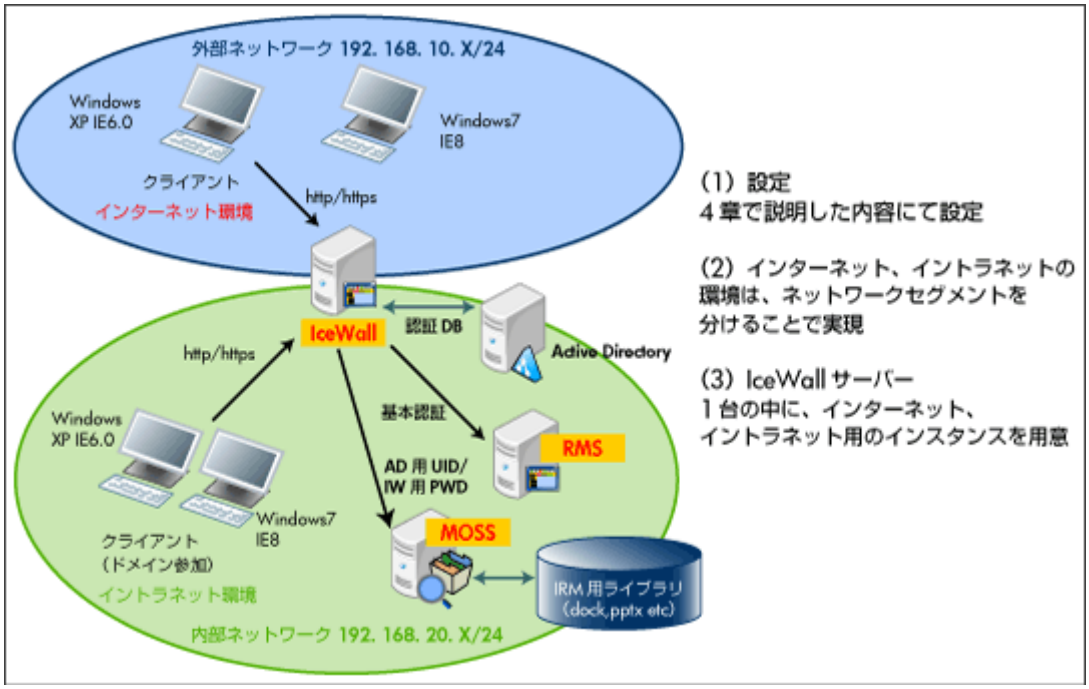


5.接続検証

これまで述べました「RMS + MOSS IRM + 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。

5-1 システム構成

下記の構成で検証を行いました。



5-2 使用した製品のVersionについて

■HP IceWall SSO
OS: Red Hat Enterprise Linux 5.2
Version: 8.0 R3
■MOSS
OS: Windows Server 2003 R2 SP2
Version: Office SharePoint Server 2007
■RMS
OS: Windows Server 2008 R2
■クライアント(ブラウザ)
Windows XP SP3 Internet Explorer 6.0 SP2 (RMS v1 SP2)
Windows 7 Internet Explorer 8.0 (RMS v2.0)

5-3 検証確認項目と結果

検証を行った項目とその結果です。下記の通りとなりました。

確認項目	結果 ※1 IE6 SP2,IE8 両ブラウザの結果 ※2 イントラネット、インターネット両環境から確認
IRM ライブラリのファイルを開く（docx,pptx,xlsx）	ライブラリのファイルを問題なく開くことができることを確認。
開いたファイルの制御内容を確認	RMS にて制御されている内容に従い、制御できることを確認。 ※権限のない操作はできないことを確認。
編集 / 保存	開いたファイルの編集、保存をすることができることを確認。

6.まとめ

本技術トピックスでは、Active Directory Rights Management サービスをMOSS＋IRMフレームワークで使用し、その環境をHP IceWall SSOを配下にする場合の効果と構成例、技術的な注意点を説明しました。
パートナー企業、グループ企業との情報の提供手段として、本ソリューションを是非ご活用ください。

2010.4.16 日本ヒューレット・パッカード テクノロジーコンサルティング統括本部　スペシャリスト　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

Microsoft Active Directory Rights Management サービスとHP IceWall SSOとの連携効果（本レポート）