Microsoft Outlook® Web AccessとHP IceWall SSOとの接続

はじめに

本技術レポートでは、前回の技術レポート「MOSS、ISAとHP IceWall SSOの接続・その効果と注意点」に引き続き、マイクロソフト製品であるExchange ServerのOutlook® Web Access機能を、HP IceWall SSOの配下で使用した場合の接続について検証結果と共に記述します。
Outlook® Web Access(以下OWA)を使用するメリットはさまざまありますが、他のWebアプリケーションと同様に認証が必要となります。OWAをHP IceWall SSOの配下に入れることより、よりセキュアな環境が構築でき、他のWebアプリケーションとのシングルサインオン化が可能となります。

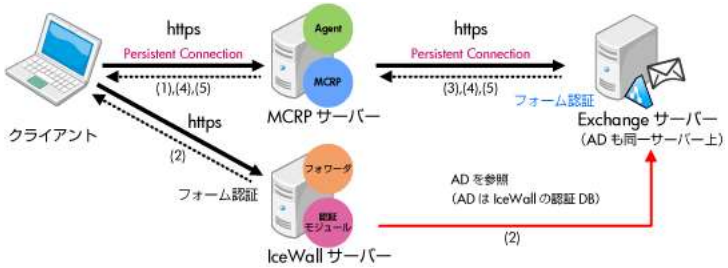
Microsoft® Office Outlook® Web Access について

Microsoft® Office Outlook® Web Access を利用すれば、自宅からでも宿泊先のホテルからでも外出中でも、ネットワークに接続できる環境があればいつでもどこからでも Exchange Server にアクセスし電子メール メッセージの送受信ができるようになります。
また、OWAを介して、Outlook で作業しているときと同じタスクの多くを実行することができます。
たとえば、次の操作が可能です。

- 電子メール、カレンダー、連絡先、およびその他の Outlook フォルダを確認する。
- 電子メール メッセージおよび会議出席依頼を送信する。
- 電子メール メッセージを受信トレイから別のフォルダに移動する。
- ファイル、オーディオ クリップ、およびビデオ クリップをメッセージに添付する。
- 新しい電子メール メッセージが届いたときに通知を受け取る。
- 会議の通知を受信する。

1.検証環境の構成

検証を行ったシステム構成は次の図のとおりです。



処理フロー概要
(1) クライアントはMCRP経由でExchangeサーバーへアクセスを行います。
※未認証の場合は、AgentはIceWallサーバーへのリダイレクトを発行します。
(2) 未認証時はIceWallサーバーのフォワーダにてログイン画面を出力し、その認証を認証モジュールにて行います。
※認証モジュールは、ユーザーIDとパスワードを認証DBであるADへ参照し認証を行います。
(3) HP IceWall SSOの認証後、クライアントがMCRP経由でExchangeサーバーへアクセスを行います。
※MCRPサーバーのAgentでは、認可の処理が毎回行われます。
(4) Exchangeサーバーより認証画面が返される場合は、MCRPの代行認証処理で認証を行います。
※本検証では間接送信方式の自動フォーム認証設定を行っています。
(5) クライアントは、IceWallサーバー, Exchangeサーバーの認証完了後はMCRP経由でExchangeサーバーへアクセスを行います。

2.検証環境の詳細

■HP IceWall SSO
OS: Red Hat Enterprise Linux 5.2
Version: 8.0 R3
■HP IceWall MCRP
OS: Red Hat Enterprise Linux 5.2
Version: 2.1 SP2
■HP IceWall SSO エージェントオプション
OS: Red Hat Enterprise Linux 5.2
Version: 8.0 2007 Update Release2
■OWA
OS: Windows Server 2003 R2 SP2
Version: Microsoft Exchange Server 2007 SP1
■クライアント(ブラウザ)
Internet Explorer 6.0 SP2
Internet Explorer 8.0

3.構成のポイント

この構成でポイントとなる点を以下に記述します。

1. OWAとの接続方式

   MOSSの場合と同様に、OWAをバックエンドサーバーとする場合には、URL変換機能を使用せずに、「オリジナルURL方式」または「オリジナルPATH方式」(※技術レポート掲載予定)にて接続を行なってください。本検証では、「オリジナルPATH方式」にて検証を行いました。

2. Persistent Connection (KeepAlive接続)

   KeepAlive接続を使用しない場合でもOWAとの接続は可能ですが、パフォーマンス向上の為に、MCRPを使用する場合は、KeepAlive接続にすることが可能です。MCRPのホスト設定ファイルにてKEEPALIVEパラメータを1に設定してください。

3. 自動フォーム認証設定

   OWAに対しては、間接送信方式の自動フォーム認証設定を行います。
   以下は、検証で用いた設定です。

ホスト設定ファイル

```
FORM_HTML=FORMGRP,/opt/icewall-sso/iwproxy/config/autologin.html
FORM_DATA_PAGE=FORMGRP,NOENCVAL,DESTINATION,destination
FORM_DATA_PAGE=FORMGRP,NOENCVAL,FLAGS,flags
FORM_DATA_PAGE=FORMGRP,NOENCVAL,FORCEDOWNLEVEL,forcedownlevel
FORM_DATA_PAGE=FORMGRP,NOENCVAL,TRUSTED,trusted
FORM_DATA_HEAD=FORMGRP,NOENCVAL,ID,BKID
FORM_DATA_HEAD=FORMGRP,NOENCVAL,PASS,BKPASS
FORM_DATA_PAGE=FORMGRP,NOENCVAL,ISUTF8,isUtf8
```

ユーザーIDとパスワードはヘッダより取得するようにします。

テンプレートファイル(autologin.html)

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN">
<html lang="ja">
<head>
<meta http-equiv="content-type" content="text/html; charset=shift_jis">
<meta http-equiv="content-script-type" content="text/javascript">
<title>AutoLogin Page</title>
</head>
<body onLoad="document.logonForm.submit()">
<form action="owaauth.dll" method="post" name="logonForm">
<div>
<input type="hidden" name="destination" value="$DESTINATION">
<input type="hidden" name="flags" value="$FLAGS">
<input type="hidden" name="forcedownlevel" value="$FORCEDOWNLEVEL">
<input type="hidden" name="trusted" value="$TRUSTED">
<input type="hidden" name="username" value="$ID">
<input type="hidden" name="password" type="password" value="$PASS">
<input type="hidden" name="isUtf8" value="$ISUTF8">
</div>
</form>
</body>
</html>
```

4. OWAのセッションタイムアウト設定

OWAにてセッションタイムアウトが発生すると、MCRPによる代行認証処理が行われます。
代行認証が頻繁に行われないように、調整してください。
※1 OWAの既定では、ユーザーが OWAを 15 分間使用しないと、コンピュータ上の Cookieは自動的に期限切れになり、ユーザーはログオフされます。
※2 OWA Lightを使用していない場合、セッションタイムアウト時にHTTP Status 440 Login TimeOutがクライアントへ返されます。MCRPでは拡張されたStatusコードを返すことができない為、ホスト設定ファイルに、以下のようにキーワード変換の定義を行い回避します。

```
CTYPE=application/x-javascript
REPKEY=Status: 440 Login Timeout,Status: 408 Login Timeout
REPKEY=this.fST=(oXH.status==440),this.fST=(oXH.status==408)
REPKEY=oE.iEC==440,oE.iEC==408
```

5. HP IceWall SSOのセッションタイムアウト

OWAの既定(15 分間使用しないとログオフ)に合わせて、ログイン有効期限を15分とし、最終アクセスよりログイン有効期限を算出するように設定します。 cert.confの内容は以下のようになります。

```
COOKIETIME=15
LOMETHOD=1
```

※上記は自動フォーム認証にて「共有のコンピュータ」としてOWAへ代行認証を行った場合の時間です。フォーム認証設定にて「個人のコンピュータ」を選択してOWAへ代行認証をさせることも可能ですが、その場合、OWAの規定タイムアウト時間は24時間となります。

4.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 ※IE6 SP2, IE8 両ブラウザの結果
メッセージの送受信	メールの送受信が可能
予定表の参照	予定表の参照、書き込みが可能
アドレス帳検索	アドレス帳の検索が可能
メール検索	メールの検索が可能
パブリックフォルダの参照	パブリックフォルダの参照が可能
パスワード変更	パスワード変更が可能 ※パスワード変更後は強制的にログオフされる
OWA Light	OWA Lightの機能が使用可能
ログオフ	ログオフが可能 ※OWAのログオフを行うとClearAuthenticationCacheコマンドが実行される為、HP IceWall SSOの認証クッキーも削除される。 ClearAuthenticationCacheコマンドはIE6SP1から提供されるコマンドで、キャッシュに存在するすべての資格情報をフラッシュし、ユーザーが認証を必要とするリソースを要求すると、認証の確認が再度行われるようにする。

5.まとめ

本技術レポートでは、Outlook® Web AccessをHP IceWall SSOの配下で使用した場合のポイントと接続検証結果について記述しました。

例えば、外出先や自宅からも Exchange Server を利用可能とするシナリオでは、OWAをHP IceWall SSOの配下に入れることより、よりセキュアな環境が構築でき、他のWebアプリケーションとのシングルサインオン化が可能となります。

OWAとHP IceWall SSOを連携する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

» Outlook® Web Access の概要

» Outlook® Web Access のフォームベース認証の構成

» Exchange Server 2007 製品情報

» Outlook® Web AccessのISA Server 2006の使用

2009.9.14 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