HP IceWall技術レポート:

SECUREMASTER/EnterpriseAccessManagerと HP IceWall SSO＋HP IceWall Federationの認証連携

1.はじめに

本技術レポートでは、NEC製品であるシングルサインオンソフトウェア「SECUREMASTER/EnterpriseAccessManager」（以降SECUREMASTER/EAMと記述）とHP IceWall SSO+HP IceWall Federationとの認証連携方法と、その検証結果に関して記述します。

連携効果

HP IceWall SSO+HP IceWall FederationとSECUREMASTER/EAMが連携することで、どちらか一方のシステムで認証されたユーザーは他方のシステムで再認証することなくしシステム利用が可能となります。これにより、IceWall導入済の企業様は、IceWallによって企業内で認証済であれば、今後NECが提供していく認証連携対応のクラウドサービスをそのままご利用頂くことが出来ます。

2. SECUREMASTER/EnterpriseAccessManagerについて

SECUREMASTER/EAMは、シングルサインオン機能を提供するソフトウェアです。オプション製品の「SECUREMASTER/フェデレーション」を利用することで、SAML2.0、OpenIDの標準仕様に基づくサービスとの認証連携が可能です。

SECUREMASTER/EnterpriseAccessManagerの特徴

- シングルサインオンにより利用者の利便性を向上
  システム毎のユーザー認証が不要となり、全従業員の利便性、生産性を向上します。ログオン情報を一元管理し、ユーザーの権限に応じたアクセスコントロールにより、セキュリティも向上します。

- 簡単かつセキュアなアクセス制御ポリシー管理機能を提供
  管理対象システム全体のアクセス制御ポリシーの統合管理機能（Web-GUI）を提供します。また、管理者がアクセス制御ポリシー設定を行うことができる対象を限定することができます。

SECUREMASTER/フェデレーションの特徴

- 社内システムとクラウドサービス間のシングルサインオンを実現
  SAML2.0、OpenIDの標準仕様に基づく認証連携によりクラウドサービスも含めたセキュアなシングルサインオン環境を実現します。

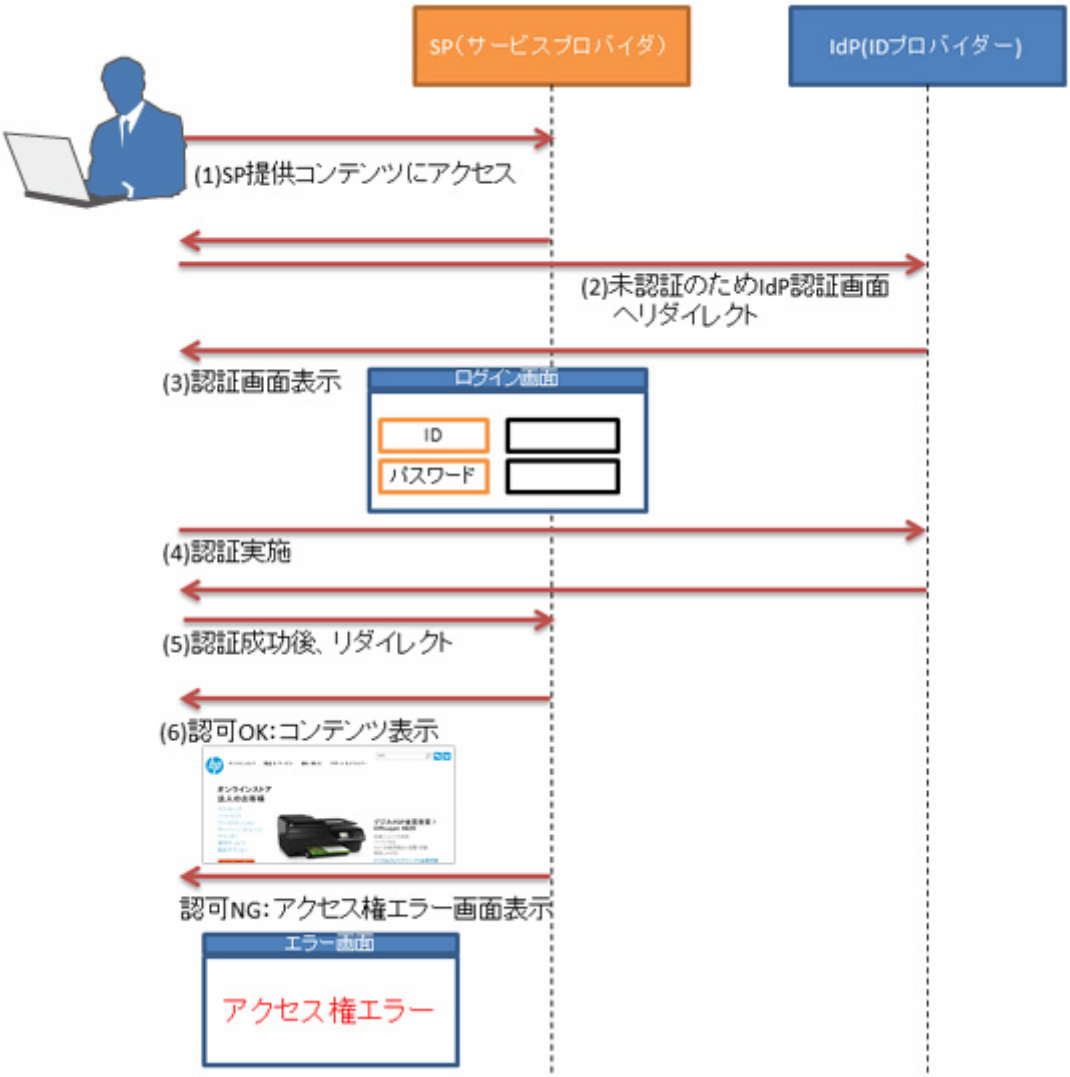
3. SECUREMASTER/EAMとの検証内容と検証結果

以下の組み合わせにて、認証連携が正しく行われることを確認しました。

IDプロバイダ（IdP）	サービスプロバイダ（SP）	連携プロトコル
HP IceWall SSO+HP IceWall Federation	SECUREMASTER/EAM	SAML2.0

確認した内容は以下の通りです。

1. 保護コンテンツへのアクセス
2. 未認証のため、IdP認証画面へのリダイレクト
3. 認証画面表示
4. 認証実施
5. 認証成功後、コンテンツへリダイレクト。
6. 認可OKの場合:コンテンツ表示
   認可NGの場合:アクセス権エラー画面表示



4. SECUREMASTER/EAMとの連携方法

4.1 IdP:HP IceWall SSO+HP IceWall Federation、SP:SECUREMASTER/EAM

IdPをHP IceWall SSO + HP IceWall Federation、SPをSECUREMASTER/EAM＋SECUREMASTER/フェデレーションとし、SAML2.0で認証連携を行います。
（赤字部分について追加・編集を行います。）
（青字部分はSECUREMASTERと連携する上での注意点です。）

注意事項:

- SECUREMASTER/フェデレーションはNEC WebOTX Application Serverへインストールすることを前提としているため、Tomcatを利用する場合は設定ファイル中の以下の文字列をすべて置換してください。
  /opt/WebOTX/domains/domain1/applications/j2ee-modules
  →/usr/share/tomcat6/webapps
  /opt/WebOTX/domains/domain1/logs
  →/usr/share/tomcat6/logs

- すべてのサーバーは正しく時刻が設定されている必要があります。

4.1.1 構成

今回確認した構成は以下の通りです。

1. IdP:HP IceWall SSO+HP IceWall Federation
   ・ホスト名:idp.iwfed.hp.com

ソフトウェア名	バージョン

RedHat Enterprise Linux (OS)	ES 6.2
HP IceWall SSO フォワーダ(dfw)	Ver10.0
HP IceWall SSO 認証モジュール(certd)	Ver10.0
HP IceWall Federation ※SPとの連携ではHP IceWall Federation Agent連携モジュールを使用	Ver3.0
NEC SECUREMASTER/ EnterpriseDirectoryServer (LDAPサーバー)	Ver7.0

2. SP:SECUREMASTER/EAM

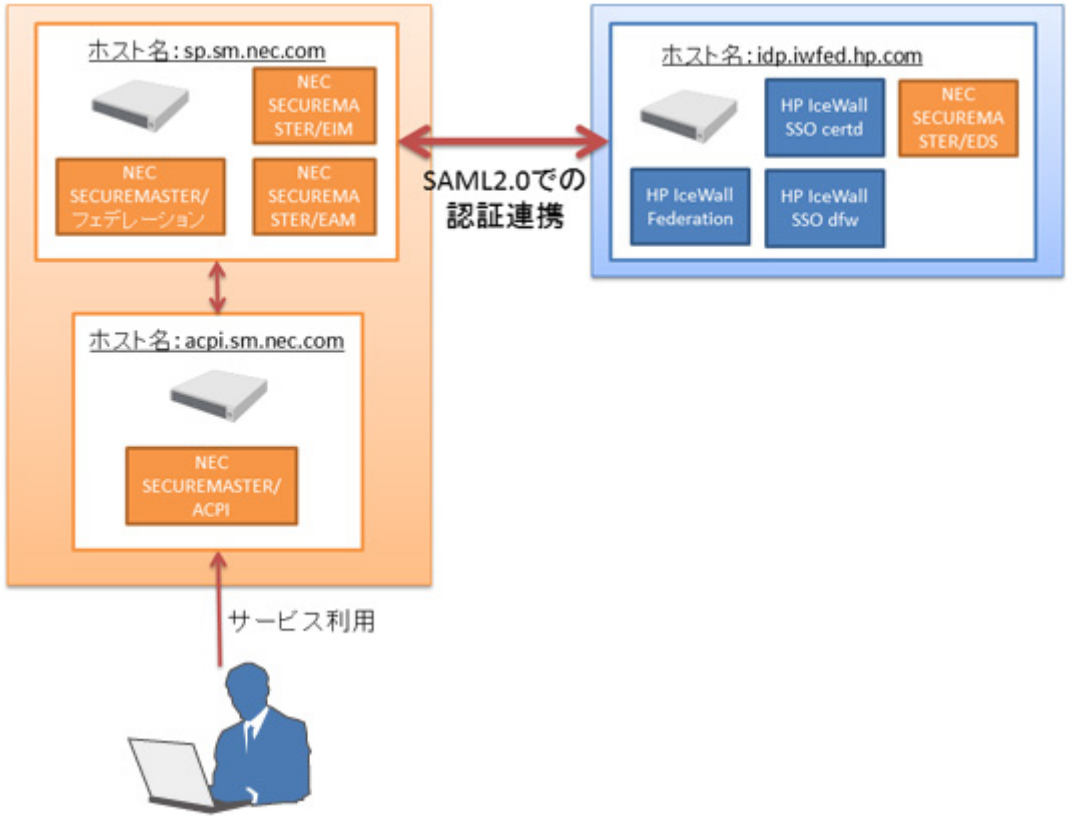
・ホスト名:sp.sm.nec.com

ソフトウェア名	バージョン
RedHat Enterprise Linux (OS)	ES 6.2
SECUREMASTER/EnterpriseAccessManager	Ver7.0
SECUREMASTER/EnterpriseIdentityManager	Ver5.0
SECUREMASTER/フェデレーション	Ver7.0
Apache Tomcat	Ver6.0.24

・ホスト名:acpi.sm.nec.com

ソフトウェア名	バージョン
RedHat Enterprise Linux (OS)	ES 5.8
SECUREMASTER/AccessControlPlugIn	Ver7.0
Apache HTTP Server	Ver2.2.23

構成図:



4.1.2 HP IceWall Federationの設定

HP IceWall Federationをインストール後、以下の設定を行います。

※/opt/icewall-federation/以下にインストールしています。

※SECUREMASTERとの連携についてはHP IceWall Federation Agent連携モジュールを利用します。

1. SAMLレスポンステンプレートの編集
以下のファイルを編集します。
/opt/icewall-federation/config/iwidp/SamlResponseTemplate.xml

```
13行目 ： <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"

          NameQualifier="{ISSUER}">{NAME_ID}</NameID>
```

※SECUREMASTER/EAMではNameQualifer要素が必須のため、テンプレートを拡張します。

2. 鍵・証明書の生成
以下のコマンドを実行します。

```
# cd  /opt/icewall-federation/config/iwidp

# keytool -genkey -keystore  keystore.jks -storepass password -alias myrsa ¥
 -keypass password -keyalg rsa -keysize 1024 -validity  3650 -dname "CN=idp.iwfed.hp.com"
# keytool -exportcert -rfc -keystore  keystore.jks -storepass password ¥
 -alias  myrsa -file public.pem
```

※-storepass、-alias、-keypassについては任意のものに変更します。

3. IdP設定ファイルの変更
以下のファイルを編集します。
/opt/icewall-federation/config/iwidp/iwidp.conf

```
18行目 : KEY_ALIAS=myrsa #(2)の-aliasの値
19行目 : KEY_PASSWORD=password #(2)の-keypassの値
20行目 : KEY_STORE_PASSWORD=password #(2)の-storepassの値
40行目 : ISSUER=http://idp.iwfed.hp.com
46行目 : ACS_URL=http://sp.sm.nec.com:8080/SamlSPLite/AssertionReceiver
47行目 : SP_ENTITY_ID=http://sp.sm.nec.com
```

4. IdPメタファイルの編集
以下のファイルを編集します。
<ds:X509Certificate>については(3)で作成したpublic.pemファイルの文字列をコピーします。
/opt/icewall-federation/config/iwidp/idp-meta.xml

```
2行目 : <md:EntityDescriptor  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
        entityID="http://idp.iwfed.hp.com" cacheDuration="PT1800S">

7~16行目 : <ds:X509Certificate>
            [(3)で作成したpublic.pemの文字列をコピー]
           </ds:X509Certificate>
20行目 : <md:SingleSignOnService  Binding=
          "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
          Location="http://idp.iwfed.hp.com/fw/dfw/tc/iwidp/sso"/>
```

※SECUREMASTER/EAMではcacheDuration要素が必須のため、メタファイルを拡張します。

5. SECUREMASTER/EAMへのIdPメタファイル配置
(4)で編集したidp-meta.xmlをSECUREMASTE/フェデレーションの以下のディレクトリに配置します。
/usr/share/tomcat6/webapps/SamlSPLite/WEB-INF/metadata/smidp-metadata.conf

4.1.3 SECUREMASTER/EAMの設定

SECUREMASTER/EAM、SECUREMASTER/フェデレーションをインストール後、以下の設定を行います。
※SECUREMASTER/フェデレーションは/usr/share/tomcat6/webapps/SamlSPLite以下にデプロイしています。

1. AuthnRequestテンプレートの編集
   以下のファイルを編集します。
   /usr/share/tomcat6/webapps/SamlSPLite/WEB-INF/authnreq/default.authnreq

```
2行目：<samlp:AuthnRequest
        AssertionConsumerServiceURL="
        http://sp.sm.nec.com:8080/SamlSPLite/AssertionReceiver"
9行目：<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        http://sp.sm.nec.com
       </saml:Issuer>
```

2. SP設定ファイルの編集
   以下のファイルを編集します。
   /usr/share/tomcat6/webapps/SamlSPLite/WEB-INF/sm_sp_conf.xml

```
26～35行目：
<item  id="VERIFYRESPONSE" valueType="2">
        <simpleItem>
                <name>SAMLレスポンス署名検証フラグ</name>
                <!--
                        true  ： 署名検証実施
                        false ： 署名検証スキップ
                -->
                <valueBool>false</valueBool>
        </simpleItem>
</item>
```

   ※HP IceWall SSOのSAMLレスポンスは未署名のため"false"（署名検証をスキップ）とします。

3. IdPリストファイルの編集
   以下のファイルを編集します。
   /usr/share/tomcat6/webapps/SamlSPLite/WEB-INF/sm_idp_list.xml

```
15～16行目：
<name>IdPのAuthnRequest送信先URLリスト</name>
<valueStr>http://idp.iwfed.hp.com/fw/dfw/tc/iwidp/sso</valueStr>
21～26行目：
<name>AuthnRequest圧縮形式リスト</name>
        <!--
                1: RFC1950準拠
                2: RFC1951準拠
        -->
<valueInt min="1" max="2">2</valueInt>
```

   ※HP IceWall SSOはRFC1951準拠(「2」設定)のみ対応します。

4. SECUREMASTERサービス設定ファイルの編集
   以下のファイルを編集します。
   /usr/share/tomcat6/webapps/SamlSPLite/WEB-INF/sm_service_conf.xml

```
7～8行目：
<name>認証サーバーURL</name>
<valueStr  maxlen="1024">
        http://sp.sm.nec.com:8080/AuthServer/ExternalAuthRequest</valueStr>
13～14行目：
```

```
<name>デフォルトオリジナルリクエストURL</name>
<valueStr  maxlen="1024">http://acpi.sm.nec.com/index.html</valueStr>
40～41行目：
<name>IdPのIssuerリスト</name>
<valueStr>http://idp.iwfed.hp.com</valueStr>
```

5. 鍵の作成
   以下のコマンドを実行します。

```
# mkdir  /usr/share/tomcat6/webapps/SamlIdP/WEB-INF/keys
# cd /usr/share/tomcat6/webapps/SamlIdP/WEB-INF/keys
# keytool  -genkeypair -alias myrsa -keyalg RSA -validity 3650 -storetype JCEKS ¥


  -keypass password -storepass password -keystore  mykeystore
```

   ※-storepass、-keypassは同一のものとし、-storepass、-keypass、-keystoreは任意のものに変更します。

6. SAML2設定ファイルの編集
   以下のファイルを編集します。
   /usr/share/tomcat6/webapps/SamlSPLite/WEB-INF/classes/samlv2.xml

```
28行目：<File path="/usr/share/tomcat6/webapps/SamlSPLite/WEB-INF/keys/mykeystore"
          password="password"/>  <!--(5)の-keystore、-keypassの値-->
40行目：<Metadata skipsVerification="true" >
55行目：<ServiceProvider entityID="http://sp.sm.nec.com" />
```

   ※HP IceWall SSOのIdPメタファイルは未署名のため、skipsVerification=true（署名検証をスキップ）とします。

7. SPメタデータ作成テンプレートの編集
   以下のファイルを編集します。
   /usr/share/tomcat6/webapps/SamlSPLite/WEB-INF/metadata/sp.conf.sample

```
11行目：EntityDescriptor/@entityID = http://sp.sm.nec.com
45行目：SPSSODescriptor_1/AssertionConsumerService_1/@Location =
        http://sp.sm.nec.com:8080/SamlSPLite/AssertionReceiver
56行目：SPSSODescriptor_1/AssertionConsumerService_2/@Location =
        http://sp.sm.nec.com:8080/SamlSPLite/AssertionReceiver
```

8. SPメタデータの作成
   以下のコマンドを実行します。

```
cd /usr/share/tomcat6/webapps/SamlSPLite/WEB-INF/metadata
./makeMetadata.sh sp.conf.sample ../key/mykeystore password myrsa sp-metadata.xml
```

以上でIdP:HP IceWall SSO+HP IceWall Federation、SP:SECUREMASTERの認証連携設定は完了です。

5. まとめ

本技術レポートでは、HP IceWall SSO+HP IceWall FederationとSECUREMASTER/EAMの連携について、構成、検証結果、連携方法について記載しました。

両製品が連携することでパブリッククラウドだけでなく、各々の企業が持つサービスへの連携も可能となり、他企業のサービスを自企業のサービスとしてお客様にご提供することが出来ます。また、お客様にとっても認証が一度で済むというメリットがあります。
今後の認証基盤導入、企業間連携の拡大に是非ご活用ください。

※両製品の連携をご検討の場合は、製品の構成、連携内容に関して製品窓口までお問い合わせ頂きますようお願い致します。

お問い合わせ
日本電気株式会社 スマートネットワーク事業部
e-mail： info@security.jp.nec.com

2013.2.15　新規掲載

執筆者　　日本電気株式会社