旧: Shibboleth IdP の設定をVer3形式に変換

1. はじめに

本メニューでは、IdPをカスタマイズします。
IdP Ver2からVer3にアップグレードを行い設定ファイルがコンバートされた環境に対して実施します。アップグレード直後の状態でも動作しますが、以降のカスタマイズで支障が出ますので適当なタイミングで下記手順を行うことをお勧めします。
Ver3形式にすると、送信属性同意機能が有効となるなど、IdP Ver3の全ての機能を使うことができるようになります。（以下に無効化の手順も示してあります）

設定ファイルをVer3形式に修正し、認証確認まで行います。

---

2. 実習セミナーでは

以下の手順で作業を進めてください。

・idp.propertiesの修正

/opt/shibboleth-idp/conf/idp.propertiesに、参照している証明書・秘密鍵の情報を設定します。

```
idp.signing.key= %{idp.home}/credentials/server.key
idp.signing.cert= %{idp.home}/credentials/server.crt
idp.encryption.key= %{idp.home}/credentials/server.key
idp.encryption.cert= %{idp.home}/credentials/server.crt
```

・credentials.xmlの確認

/opt/shibboleth-idp/conf/credentials.xmlが存在することを確認してください。
存在しなければ、以下のようにcredentials.xml.distをコピーして作成します。

```
lsコマンドを使ってファイルが存在するかを確認します。（以下、見つからない場合）
# ls /opt/shibboleth-idp/conf/credentials.xml
ls: cannot access /opt/shibboleth-idp/conf/credentials.xml: そのようなファイルやディレクトリはありません



# cp /opt/shibboleth-idp/dist/conf/credentials.xml.dist /opt/shibboleth-idp/conf/credentials.xml
```

このファイル（テンプレート）は上記idp.propertiesの変更部分を参照しているだけなので、ファイル内容の修正は不要です。

・relying-party.xmlの置き換え

/opt/shibboleth-idp/dist/conf/relying-party.xml.distでVer2からコンバートされたrelying-party.xmlを置き換えます。

特定のSPに対してSAML1アサーションに属性情報を含める、のようにrelying-party.xmlをカスタマイズしている場合は、その部分が失われますので置き換え後のrelying-party.xmlに対して修正・追加を行ってください。

```
# cp /opt/shibboleth-idp/dist/conf/relying-party.xml.dist /opt/shibboleth-idp/conf/relying-party.xml

cp: `/opt/shibboleth-idp/conf/relying-party.xml' を上書きしてもよろしいですか(yes/no)? y[Enter]
```

上書きしたrelying-party.xmlテンプレートに送信属性同意機能有効化が含まれています。無効にしたい場合は以下の赤字部分を削除してください。

```
...
    <bean parent="Shibboleth.SSO" p:postAuthenticationFlows="attribute-release" />
...
    <bean parent="SAML2.SSO" p:postAuthenticationFlows="attribute-release" />
...
```

・metadata-providers.xmlの置き換えと修正

アップグレード直後のmetadata-providers.xmlの内容はアップグレード前のrelying-party.xmlと同内容です。

まず、現在の設定内容を確認します。

```
# grep metadataURL= /opt/shibboleth-idp/conf/metadata-providers.xml
                        metadataURL="https://metadata.gakunin.nii.ac.jp/gakunin-test-metadata.xml" ←このURLを記録してください
# grep -A 2 id=.shibboleth.MetadataTrustEngine /opt/shibboleth-idp/conf/metadata-providers.xml
    <security:TrustEngine id="shibboleth.MetadataTrustEngine" xsi:type="security:StaticExplicitKeySignature">
        <security:Credential id="MyFederation1Credentials" xsi:type="security:X509Filesystem">
            <security:Certificate>/opt/shibboleth-idp/credentials/gakunin-test-signer-2011.cer</security:Certificate> ←このファイル名を記録してください
```

/opt/shibboleth-idp/dist/conf/metadata-providers.xml.distでVer2からコンバートされたmetadata-providers.xmlを置き換えます。

追加でローカルSPのメタデータを読み込んでいるなど<MetadataProvider>の部分をカスタマイズしている場合は、置き換え後にバックアップ(/opt/shibboleth-idp/conf.v2/relying-party.xml)を参照しながら必要なものを反映してください。

```
# cp /opt/shibboleth-idp/dist/conf/metadata-providers.xml.dist /opt/shibboleth-idp/conf/metadata-providers.xml
上書きします。
cp: `/opt/shibboleth-idp/conf/metadata-providers.xml' を上書きしてもよろしいですか(yes/no)? y[Enter]
```

また、以下のように確認した設定内容を復元します。metadataURL= の部分と certificateFile= の部分は上で確認したURLおよびファイル名で置き換えてください。また読み込むメタデータを追加している場合はここに追加してください。

```
The EntityRoleWhiteList saves memory by only loading metadata from SAML roles
that the IdP needs to interoperate with.
-->

<!-- --> ← コメントアウト解除

<MetadataProvider id="HTTPMetadata"
                  xsi:type="FileBackedHTTPMetadataProvider"
                  backingFile="%{idp.home}/metadata/gakunin-metadata-backing.xml"
                  metadataURL="https://metadata.gakunin.nii.ac.jp/gakunin-test-metadata.xml">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
                    certificateFile="%{idp.home}/credentials/gakunin-test-signer-2011.cer">

<!-- ← 公開鍵をファイルで指定するのでコメントアウト
         <PublicKey>
             MIIBI.....
         </PublicKey>
--> ← 公開鍵をファイルで指定するのでコメントアウト

    </MetadataFilter>
    <MetadataFilter xsi:type="metadata:RequiredValidUntil" maxValidityInterval="P15D"/>
                                ↑この部分を削除します
     <MetadataFilter xsi:type="EntityRoleWhiteList">
             <RetainedRole>md:SPSSODescriptor</RetainedRole>
     </MetadataFilter>
</MetadataProvider>
<!-- --> ← コメントアウト解除
```

・services.propertiesの修正

Ver3の形式で読み込むように/opt/shibboleth-idp/conf/services.propertiesを修正します。

```
#idp.service.relyingparty.resources= shibboleth.LegacyRelyingPartyResolverResources
idp.service.relyingparty.resources= shibboleth.RelyingPartyResolverResources  ※Legacyを削除した値を設定します。
```

・Tomcatの再起動

Tomcatを再起動して、Ver3形式に変換した設定ファイルを読み込ませます。

```
# service tomcat7 restart
```

---

3. 手順書

以下は、英語での情報が記載されたwiki.shibboleth.netのURLです。手順の詳細にご興味がある方はご参照ください。

参考: Installation

---

4. 動作確認

作業前と同様に動作することを確認します。

① 各自が使用するSPの接続確認用ページにアクセスします。

```
例）1番を割り振られた場合
https://ex-sp-test01.gakunin.nii.ac.jp/
```

② ログインボタンをクリックします。

③ DSの所属機関の選択画面が表示されるので、各自が使用するIdPを選択します。

④ IdPのログイン画面が表示されます。

⑤ Username/Passwordを入力して認証を行います。

⑥ 送信属性同意画面が表示される事を確認します。

⑦ 正しく属性受信の確認ページが表示される事を確認してください。

BACK TOP NEXT