学内システムとして構築する場合の設定

学内システムとして構築する場合の設定

本技術ガイドでは、フェデレーションに参加して連携する設定を説明していますが、ここでは、所属機関内のみで使用するSPを構築した場合など、特定のIdP・特定のSPの間でのみ連携する設定に変更する方法を説明します。

SP側shibboleth2.xmlとIdP側metadata-providers.xmlを編集し、以下のように設定します。

1. SPは、DSを経由せず、特定のIdPのみ信頼する
2. IdPは、特定のSPのみ信頼する

---

shibboleth2.xmlの設定

IdPのメタデータを別途取得している場合はそのメタデータファイルを用いてください。そうでない場合は以下の手順に従ってIdPメタデータを取得してください。

> もしIdPが学認の運用フェデレーションに参加している場合は、代わりに学認メタデータからIdPメタデータを自動抽出して利用することもできます。詳しくは以下をご参照ください。
> ⇒GakuNinShare:設定・運用・カスタマイズ#メタデータ中の特定のIdPのみ利用を許可する方法
>
> この設定を行った場合、DSの参照設定無効化から続きを実行してください。

- テストフェデレーションに登録済みのIdPを利用する場合、学認申請システム(テストfed)にログインして該当IdPの詳細画面で「以下の内容のエンティティメタデータを取得」ボタンでメタデータを取得します。
- テストフェデレーションに参加していない場合でも、学認申請システム(テストfed)を用いてIdPメタデータを取得することが可能です。

○学認申請システム(テストfed)にアクセスして、「新規IdP申請」をクリックします。

〇右側の入力に以下の必須情報を入力します。
entityID → 指定するIdPのentityID。 例: https://idp.example.ac.jp/idp/shibboleth
機関名称 → 入力例: フェデレーション大学 / The University of Federation
スコープ → SPがIdPを識別するための情報。 例: nii.ac.jp
証明書 → IdPの証明書をファイルで指定するか、もしくは MII… で始まる中身を貼り付けます。
IdP名称 → 他のIdP/SPと区別できる名称。
機関情報URL → IdP運用機関のウェブサイトURL。
連絡先 → 種別は「技術的問い合せ先(technical)」を選択して連絡先を入力してください。

〇入力後、申請せずに、「以下の内容でエンティティメタデータ生成」ボタンをクリックしてください。当該IdPのメタデータが生成されます。

IdPのメタデータを取得したら、それをSP上に配置します。端末上にある場合は、当該ファイルの中身を表示し全てコピーし、SP上でvi等を実行し挿入できる状態にした上で、貼り付けてください。

- 取得したIdPのメタデータをSPの /etc/shibboleth/ （もしくは /etc/shibboleth/metadata/）に配置します。配置したIdPのメタデータファイルを参照する設定を追加し、フェデレーションのメタデータ設定を外します。

```
(省略)
   <!-- Example of locally maintained metadata. -->
   <!-- コメントアウト解除 -->
   <MetadataProvider type="XML" validate="true" path="メタデータファイル名"/>
   <!-- コメントアウト解除 -->

   <!-- Example of remotely supplied batch of signed metadata. -->
   <!-- コメントアウト

   <MetadataProvider type="XML" validate="true"
            url="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml"
            backingFilePath="federation-metadata.xml" maxRefreshDelay="7200">
      <MetadataFilter type="RequireValidUntil" maxValidityInterval="1296000"/>
      <MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/gakunin-signer-2017.cer" verifyBackup="false"/>
      <DiscoveryFilter type="Exclude" matcher="EntityAttributes" trimTags="true"
         attributeName="http://macedir.org/entity-category"
         attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
         attributeValue="http://refeds.org/category/hide-from-discovery" />
      <TransportOption provider="CURL" option="64">1</TransportOption>
      <TransportOption provider="CURL" option="81">2</TransportOption>
      <TransportOption provider="CURL" option="10065">/etc/pki/tls/certs/ca-bundle.crt</TransportOption>
   </MetadataProvider>

   コメントアウト -->

(省略)
```

- 認証要求先のIdPを設定し、DSの参照設定を無効にします。

```
(省略)

   <Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
             checkAddress="false" handlerSSL="false" cookieProps="http">

       <!--
       Configures SSO for a default IdP. To allow for >1 IdP, remove
       entityID property and adjust discoveryURL to point to discovery service.
       (Set discoveryProtocol to "WAYF" for legacy Shibboleth WAYF support.)
       You can also override entityID on /Login query string, or in RequestMap/htaccess.
       -->
       <SSO entityID="https://test-idp1.gakunin.nii.ac.jp/idp/shibboleth"
                      ↑IdPを設定 (metadataに設定されているentityID)
            discoveryProtocol="SAMLDS" discoveryURL="https://ds.example.org/DS/WAYF">
         SAML2 SAML1
       </SSO>

(省略)

       <!-- Session diagnostic service. -->
       <Handler type="Session" Location="/Session" showAttributeValues="false"/>

       <!-- JSON feed of discovery information. -->
       <Handler type="DiscoveryFeed" Location="/DiscoFeed"/>

       <!-- コメントアウト
       <SessionInitiator type="Chaining" Location="/DS" isDefault="true " id="DS">
           <SessionInitiator type="SAML2" template="bindingTemplate.html"/>
           <SessionInitiator type="Shib1"/>
           <SessionInitiator type="SAMLDS" URL="https://test-ds.gakunin.nii.ac.jp/WAYF"/>
       </SessionInitiator>
       コメントアウト -->
   </Sessions>

(省略)
```

※端末のサイズによっては表記がずれる可能性がございます。画面を広くしてご覧ください。

設定変更後、httpdとshibdを再起動します。

```
systemctl restart httpd
systemctl restart shibd
```

```
service httpd restart
service shibd restart
```

※DSを経由する設定にshibboleth2.xmlを戻したい場合は、こちらを参照してください。

---

metadata-providers.xmlの設定

SPのメタデータを別途取得している場合はそのメタデータファイルを用いてください。そうでない場合は以下の手順に従ってSPメタデータを取得してください。

- テストフェデレーションに登録済みのSPを利用する場合、学認申請システム(テストfed)にログインして該当SPの詳細画面で「以下の内容のエンティティメタデータを取得」ボタンでメタデータを取得します。
- テストフェデレーションに参加していない場合でも、学認申請システム(テストfed)を用いてSPメタデータを取得することが可能です。

  〇学認申請システム(テストfed)にアクセスして、「新規SP申請」をクリックします。

  〇右側の入力に以下の必須情報を入力します。
  entityID → 指定するSPのentityID。 例: https://sp.example.ac.jp/shibboleth-sp
  機関名称 → 入力例: フェデレーション大学 / The University of Federation
  証明書 → SPの証明書をファイルで指定するか、もしくは MII… で始まる中身を貼り付けます。
  DSからのリターンURL → DSからの戻り先となるURL。例: https://sp.example.ac.jp/Shibboleth.sso/DS
  SP名称 → 他のIdP/SPと区別できる名称。
  機関情報URL → SP運用機関のウェブサイトURL。
  連絡先 → 種別は「技術的問い合せ先(technical)」を選択して連絡先を入力してください。

  〇入力後、申請せずに、「以下の内容でエンティティメタデータ生成」ボタンをクリックしてください。当該SPのメタデータが生成されます。

SPのメタデータを取得したら、それをIdP上に配置します。端末上にある場合は、当該ファイルの中身を表示し全てコピーし、IdP上でvi等を実行し挿入できる状態にした上で、貼り付けてください。

- 取得したSPのメタデータをIdPの /opt/shibboleth-idp/metadata/ に配置します。配置したSPのメタデータファイルを参照する設定を追加し、フェデレーションのメタデータ設定を外します。

```
    （省略）

    The EntityRoleWhiteList saves memory by only loading metadata from entity types
    that you will interoperate with.
-->
<!-- ← 学認メタデータの自動ダウンロードを使用しないのでコメントアウト
<MetadataProvider id="HTTPMetadata"
                  xsi:type="FileBackedHTTPMetadataProvider"
                  backingFile="%{idp.home}/metadata/gakunin-metadata-backing.xml"
                  metadataURL="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml"
                  failFastInitialization="false">

<MetadataFilter xsi:type="SignatureValidation" certificateFile="%{idp.home}/credentials/gakunin-signer-2017.cer" />
   <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P15D" />
   <MetadataFilter xsi:type="EntityRoleWhiteList">
       <RetainedRole>md:SPSSODescriptor</RetainedRole>
   </MetadataFilter>
</MetadataProvider>
-->

<MetadataProvider id="SPMD" xsi:type="FilesystemMetadataProvider" metadataFile="%{idp.home}/metadata/"/>

    （省略）
```

※端末のサイズによっては表記がずれる可能性がございます。画面を広くしてご覧ください。

学認参加IdPが個別の学内SPとも連携したい場合など、フェデレーションのメタデータ設定をコメントアウトせずにSPメタデータ設定を追加すれば、どちらのSPとも連携できます。

設定変更後、Jettyを再起動します。

```
systemctl restart jetty
```

```
service tomcat7 restart
```

※フェデレーションのメタデータの参照設定を行った設定にmetadata-providers.xmlを戻す場合は、こちらを参照してください。

利用するSPにアクセスし、DSを経由せず、設定したIdPに直接アクセスすること、およびIdPで認証してSPに接続できることを確認してください。