学認申請システムを使ってテストフェデレーションに参加する

1. はじめに

本メニューでは、IdP・SPを学認申請システム（テストFed）を使用して、実際にテストフェデレーションへ登録します。
テストフェデレーションに関して、詳しくは「テストフェデレーションルール」を参照してください。

---

2. 実習セミナーでは

以下のような設定で行います。
手順書と照らし合わせながら、作業を進めてください。

・アカウント作成時のメールアドレスについて

```
ここで設定したメールアドレスに申請システムからの確認メールが届くので、
必ず使用可能なメールアドレスを設定してください。
```

・申請（IdP）entityID

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

・申請（SP）entityID

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

・スコープについて

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

・申請(IdP)証明書

```
# cat /opt/shibboleth-idp/credentials/server.crt
```

・申請(SP)証明書

```
# cat /etc/shibboleth/cert/server.crt
```

・DSからのリターンURL

```
https://ex-sp-testXX.gakunin.nii.ac.jp/Shibboleth.sso/DS
```

・連絡先

```
ここに限りませんがメタデータとして公開されますので、個人メールアドレス等公開して問題のある情報を入力することは避けてください。身の回りに公開メールアドレス等適当なものがなければ、ご相談ください。
```

・その他の項目について

各自の名前、所属機関などを設定してください。

3.手順書

以下の手順書を参照し、作業を行います。

- 学認申請システム利用マニュアル（テストFed）
  1. はじめに
  2. 学認申請システムの利用のフロー
  3. 初回の利用方法（新規IdP/SP申請）

---

4. 動作確認

以下の動作確認手順は、IdP・SPの両方を参加させた場合です。

・構築SPとテストフェデレーションテスト用IdPの間での接続テスト

① 構築したSPの/etc/shibboleth/shibboleth2.xmlにて、DSをテストフェデレーションのものに変更します。

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

 （省略）

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

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

    <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>

</Sessions>
```

② テストフェデレーションメタデータ検証用の証明書を
https://metadata.gakunin.nii.ac.jp/gakunin-test-signer-2020.cer からダウンロードします。

```
cd /etc/shibboleth/cert wget https://metadata.gakunin.nii.ac.jp/gakunin-test-signer-2020.cer
```

③ shibboleth2.xmlのメタデータダウンロード元と証明書を変更します。

```
<!--
Allows overriding of error template information/filenames. You can
also add your own attributes with values that can be plugged into the
templates, e.g., helpLocation below.
-->
<Errors supportContact="root@localhost"
    helpLocation="/about.html"
    styleSheet="/shibboleth-sp/main.css"/>

（省略）

<!-- Example of remotely supplied batch of signed metadata. -->
<!-- -->

<MetadataProvider type="XML" validate="true"
      url="https://metadata.gakunin.nii.ac.jp/gakunin-test-metadata.xml"
      backingFilePath="federation-metadata.xml" reloadInterval="7200">
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="1296000"/>
    <MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/gakunin-test-signer-2020.cer" verifyBackup="false"/>
    <DiscoveryFilter type="Blacklist" 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>
<!-- -->

<!-- Example of remotely supplied "on-demand" signed metadata. -->
<!--
<MetadataProvider type="MDQ" validate="true" cacheDirectory="mdq"
```

④ shibdおよびhttpdを再起動します。

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

⑤ テストフェデレーションDSから接続テスト用IdPを選択します。
・各自構築したSP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/
```

・ログインボタンをクリックします。

・テストフェデレーションDSが表示されるので、所属している機関リストから関東カテゴリの**「GakuNin テスト IdP」**
(英語表示の場合はKantoカテゴリの「GakuNin Test IdP」)を選択します。

・ログイン画面が表示されるので、**ユーザtest001**、**パスワードtest001**を入力して認証を行います。

・正しく属性受信の確認ページが表示されます。
(IdPエンティティIDが”https://test-idp1.gakunin.nii.ac.jp/idp/shibboleth”となっていることを確認してください)

・構築IdPとテストフェデレーションテスト用SPの間での接続テスト

① 構築IdPにて、テストフェデレーションメタデータ検証用の証明書を
https://metadata.gakunin.nii.ac.jp/gakunin-test-signer-2020.cer からダウンロードします。

```
cd /opt/shibboleth-idp/credentials wget https://metadata.gakunin.nii.ac.jp/gakunin-test-signer-2020.cer
```

② /opt/shibboleth-idp/conf/metadata-providers.xmlのメタデータ自動ダウンロード設定を変更します。

```
<?xml version="1.0" encoding="UTF-8"?>
<MetadataProvider id="ShibbolethMetadata" xsi:type="ChainingMetadataProvider"

（省略）

<!--
Example HTTP metadata provider.  Use this if you want to download the metadata
from a remote source.

（省略）

<!-- -->
<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" certificateFile="%{idp.home}/credentials/gakunin-test-signer-2020.cer" />
   <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P15D"/>
    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
    </MetadataFilter>
</MetadataProvider>
<!-- -->
```

③ jettyを再起動します。

```
systemctl restart jetty
```

④ テストフェデレーションの接続テスト用SP https://test-sp1.gakunin.nii.ac.jp にアクセスします。

・ログインボタンをクリックします。

・テストフェデレーションDSの所属している機関から「**各自の構築したIdP名称**」があるかどうかを確認し、選択をします。

（※ここで選択するIdPは **GakuNin テスト IdPではありません**）

・IdPのログイン画面が表示されるので、**ユーザtest001**、**パスワードtest001**を入力して認証を行います。

・正しく属性受信の確認ページが表示されることを確認してください。（本確認についてのみ、属性が全"NOT RECEIVED"になっていても問題ありません。そうなっていることを確認した上で次の確認に進んでください。）

・構築SPと構築IdPとの間での接続テスト

① 各自構築したSP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 テストフェデレーションDSの所属している機関から「**各自の構築したIdP名称**」を選択します。

④ IdPのログイン画面が表示されるので、**ユーザtest001**、**パスワードtest001**を入力して認証を行います。

⑤ 正しく属性受信の確認ページが表示されることを確認してください。