shibboleth2.xml ファイル設定

shibboleth2.xml ファイル

1. entityIDを設定します。

/etc/shibboleth/shibboleth2.xml ファイルを以下のように編集してください。

```
※「ApplicationDefaults entityID」を検索し、場所を特定してください。
    ??には、各自が割り振られたホスト名を設定してください。

<ApplicationDefaults entityID="https://ex-sp-test??.gakunin.nii.ac.jp/shibboleth-sp"
                                          ↑ホスト名変更                    ↑後ろに「-sp」追記
                     REMOTE_USER="eppn subject-id pairwise-id persistent-id"
```

2. DSサーバの参照設定を行います。

/etc/shibboleth/shibboleth2.xml ファイルを以下のように編集してください。

```
※「</Sessions>」の直前に行を挿入してください。
           <!-- 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://ex-ds.gakunin.nii.ac.jp/WAYF"/>
                                                                    ↑DSサーバの設定
            </SessionInitiator>
       </Sessions>
 (省略)
```

3. メタデータの自動更新設定を行います。

証明書を格納するディレクトリを作成します。

```
# mkdir /etc/shibboleth/cert
```

証明書は、初期設定で「/root/GETFILE」に取得したex-fed.crtを使用します。
「/etc/shibboleth/cert」配下にコピーしてください。

```
# cp /root/GETFILE/ex-fed.crt /etc/shibboleth/cert/
```

メタデータを自動的にダウンロードする設定を行います。

実習セミナー

・実習セミナーではフェデレーションメタデータはDSサーバにて公開していますので、
DSサーバよりメタデータを自動ダウンロードします。
参照先のuriには、以下を設定してください。（実習セミナー内の公開メタデータ）
https://ex-ds.gakunin.nii.ac.jp/fed/ex-fed-metadata.xml
・自動ダウンロードするメタデータの署名検証用の証明書を設定します。
先ほどコピーした、実習セミナー用の証明書「ex-fed.crt」を参照するように設定します。
/etc/shibboleth/cert/ex-fed.crt

/etc/shibboleth/shibboleth2.xml ファイルを以下のように編集してください。

```
        <!-- Example of remotely supplied batch of signed metadata. -->
        <!-- --> ←コメントアウト解除
        <MetadataProvider type="XML" validate="true"
                    url="https://ex-ds.gakunin.nii.ac.jp/fed/ex-fed-metadata.xml"
                                        ↑参照先のURLを設定
              backingFilePath="federation-metadata.xml" maxRefreshDelay="7200">
            <MetadataFilter type="RequireValidUntil" maxValidityInterval="1296000"/>
                                                                        ↑validUntilの検証設定
            <MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/ex-fed.crt" verifyBackup="false"/>
                                                        ↑自動更新メタデータの検証用証明書設定
        <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>
                                ↑ HTTPSサイトの証明書検証を有効化（メタデータのダウンロード時に利用）
        </MetadataProvider>
        <!-- -->  ←コメントアウト解除
```

※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。

※ 上記設定によってダウンロードされたメタデータは /var/cache/shibboleth/federation-metadata.xml に配置されます。

参考資料

- Shibboleth SP 3の設定ドキュメント
  https://wiki.shibboleth.net/confluence/display/SP3/ReloadableConfiguration
  https://wiki.shibboleth.net/confluence/display/SP3/MetadataProvider

TOP NEXT