テストフェデレーションメタデータ署名用証明書移行手順 (Shibboleth SP向け)

SPの設定変更手順

新しいテストフェデレーションメタデータ署名用証明書の公開後に、本手順に従い順次設定変更を実施してください。証明書切り替え期日（2020年12月17日）前に実施することを想定していますが、切り替え後に実施する場合は手順2.以外を実施してください。

> ⚠ 学認技術ガイドに従って設定した標準的なSP(バージョン3.1.0)の場合の設定です。 異なるバージョン、設定の場合には適宜置き換えて読んでください。

> ⓘ 本ページに記載している署名検証用証明書URLおよびそのフィンガープリントは次のページで公開されているものです。
>
> https://www.gakunin.jp/join/test/rule

手順:

- 1. 新しい検証用証明書の取得
- 2. 事前設定変更 (2020年12月17日 10:00以前に実施)
- 3. 証明書切り替え後の設定変更 (2020年12月17日 10:00以降に実施)

1. 新しい検証用証明書の取得

新しい検証用証明書を以下のURLからダウンロードして「/etc/shibboleth/cert/gakunin-test-signer-2020.cer」に配置します。

- https://metadata.gakunin.nii.ac.jp/gakunin-test-signer-2020.cer

> ⚠ **証明書のフィンガープリント確認**
>
> ダウンロードした署名検証用証明書のフィンガープリントを確認し、以下と一致するか確認してください。
>
> **SHA256 Fingerprint=FA:11:11:5B:EC:13:4D:55:85:AF:60:32:E1:6C:01:01:EF:9C:A0:6B:17:8C:8B:9C:7F:2B:69:41:EB:68:30:1E**
>
> OpenSSLコマンドでは以下のように確認します。
> **> openssl x509 -in gakunin-test-signer-2020.cer -fingerprint -sha256 -noout**

2. 事前設定変更 (2020年12月17日 10:00以前に実施)

/etc/shibboleth/shibboleth2.xml 内に記載のテストフェデレーション用の<MetadataProvider>を以下のように修正し、検証用証明書として新旧両証明書を併記します。

差分（unified diff形式）

```
         <MetadataProvider type="XML" validate="true"
               url="https://metadata.gakunin.nii.ac.jp/gakunin-test-metadata.xml"
               backingFilePath="federation-metadata.xml" maxRefreshDelay="7200">
             (...略...)
-            <MetadataFilter type="Signature" certificate="cert/gakunin-test-signer-2011.cer" verifyBackup="false"/>
+            <MetadataFilter type="Signature" verifyBackup="false">
+                <CredentialResolver type="Chaining">
+                    <CredentialResolver type="File" certificate="cert/gakunin-test-signer-2011.cer"/>
+                    <CredentialResolver type="File" certificate="cert/gakunin-test-signer-2020.cer"/>
+                </CredentialResolver>
+            </MetadataFilter>
             (...略...)
         </MetadataProvider>
```

shibdを再起動し、設定を再読み込みします。

```
## (CentOS 7の場合)
$ sudo systemctl restart shibd
## (CentOS 6の場合)
$ sudo service shibd restart
```

再読み込み後、エラーログ（/var/log/shibboleth/shibd_warn.log）に以下のように記録されている場合は署名検証に失敗しておりますので、shibboleth2.xmlの証明書ファイルの指定が正しいかどうか確認してください。

```
2020-11-30 14:30:36 WARN OpenSAML.MetadataFilter.Signature : filtering out group at root of instance after failed signature check: CredentialResolver did not supply any candidate keys.
```

⚠ 2020年12月17日 10:00以降に、下記の「証明書切り替え後の設定変更」を忘れずに実施してください。

3. 証明書切り替え後の設定変更 (2020年12月17日 10:00以降に実施)

/etc/shibboleth/shibboleth2.xml 内に記載のテストフェデレーション用の<MetadataProvider>を以下のように修正し、検証用証明書として新証明書のみを残します。

差分（unified diff形式）

```
        <MetadataProvider type="XML" validate="true"
              url="https://metadata.gakunin.nii.ac.jp/gakunin-test-metadata.xml"
              backingFilePath="federation-metadata.xml" maxRefreshDelay="7200">
            (...略...)
-           <MetadataFilter type="Signature" verifyBackup="false">
-               <CredentialResolver type="Chaining">
-                   <CredentialResolver type="File" certificate="cert/gakunin-test-signer-2011.cer"/>
-                   <CredentialResolver type="File" certificate="cert/gakunin-test-signer-2020.cer"/>
-               </CredentialResolver>
-           </MetadataFilter>
+           <MetadataFilter type="Signature" certificate="cert/gakunin-test-signer-2020.cer" verifyBackup="false"/>
            (...略...)
        </MetadataProvider>
```

⚠ 事前設定変更をしていない場合は、検証用証明書を新証明書に直接切り替えてください。

差分（unified diff形式）

```
        <MetadataProvider type="XML" validate="true"
              url="https://metadata.gakunin.nii.ac.jp/gakunin-test-metadata.xml"
              backingFilePath="federation-metadata.xml" maxRefreshDelay="7200">
            (...略...)
-           <MetadataFilter type="Signature" certificate="cert/gakunin-test-signer-2011.cer" verifyBackup="false"/>
+           <MetadataFilter type="Signature" certificate="cert/gakunin-test-signer-2020.cer" verifyBackup="false"/>
            (...略...)
        </MetadataProvider>
```

shibdを再起動し、設定を再読み込みします。

```
## (CentOS 7の場合)
$ sudo systemctl restart shibd
## (CentOS 6の場合)
$ sudo service shibd restart
```

再読み込み後、エラーログ（/var/log/shibboleth/shibd_warn.log）に以下のように記録されている場合は署名検証に失敗しておりますので、shibboleth2.xmlの証明書ファイルの指定が正しいかどうか確認してください。

```
2020-11-30 14:30:36 WARN OpenSAML.MetadataFilter.Signature : filtering out group at root of instance after failed signature check:
CredentialResolver did not supply any candidate keys.
```

以上