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 IdP向け)

IdP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IdP(バージョン3.4.6)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。4.0.xは同じ手順で実施できます。

> ⚠ (※) - Shibboleth IdP 3.2.xおよび3.3.xについてはメタデータ署名検証に失敗すると直前に取得したメタデータ情報を破棄するという不具合があります。エラーを避けるためには、必ず証明書切り替え前に設定変更を実施してください。

> ⓘ 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

新しい検証用証明書を以下のURLからダウンロードして「/opt/shibboleth-idp/credentials/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)

/opt/shibboleth-idp/conf/metadata-providers.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 id="HTTPMetadata"
     (...略...)
                       metadataURL="https://metadata.gakunin.nii.ac.jp/gakunin-test-metadata.xml">

-        <MetadataFilter xsi:type="SignatureValidation" certificateFile="%{idp.home}/credentials/gakunin-test-signer-2011.cer" />
+        <MetadataFilter xsi:type="SignatureValidation">
+            <security:TrustEngine id="GTestTrustEngine" xsi:type="security:StaticExplicitKeySignature">
+                <security:Credential id="GTestCredential" xsi:type="security:X509ResourceBacked">
+                    <security:Certificate>%{idp.home}/credentials/gakunin-test-signer-2011.cer</security:Certificate>
+                </security:Credential>
+                <security:Credential id="GTestCredentialNew" xsi:type="security:X509ResourceBacked">
+                    <security:Certificate>%{idp.home}/credentials/gakunin-test-signer-2020.cer</security:Certificate>
+                </security:Credential>
+            </security:TrustEngine>
+        </MetadataFilter>
     (...略...)
     </MetadataProvider>
```

変更後、以下のコマンドで設定を再読み込みします。

```
$ /opt/shibboleth-idp/bin/reload-service.sh -id shibboleth.MetadataResolverService
```

再読み込み後、エラーログ（/opt/shibboleth-idp/logs/idp-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、metadata-providers.xmlの証明書ファイルが正しいかどうか確認してください。

```
2020-11-30 14:05:32,408 -  - WARN [org.apache.xml.security.signature.XMLSignature:777] - Signature verification failed.
2020-11-30 14:05:32,409 -  - ERROR [org.opensaml.saml.metadata.resolver.filter.impl.SignatureValidationFilter:419] - Signature trust
establishment failed for metadata entry GakuNin-test
2020-11-30 14:05:32,410 -  - ERROR [org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:537] - Metadata
Resolver FileBackedHTTPMetadataResolver HTTPMetadata: Error filtering metadata from https://metadata.gakunin.nii.ac.jp/gakunin-test-
metadata.xml
org.opensaml.saml.metadata.resolver.filter.FilterException: Signature trust establishment failed for metadata entry
        at org.opensaml.saml.metadata.resolver.filter.impl.SignatureValidationFilter.verifySignature(SignatureValidationFilter.java:
420)
```

⚠ 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)

/opt/shibboleth-idp/conf/metadata-providers.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 id="HTTPMetadata"
     (...略...)
                       metadataURL="https://metadata.gakunin.nii.ac.jp/gakunin-test-metadata.xml">

-        <MetadataFilter xsi:type="SignatureValidation">
-            <security:TrustEngine id="GTestTrustEngine" xsi:type="security:StaticExplicitKeySignature">
-                <security:Credential id="GTestCredential" xsi:type="security:X509ResourceBacked">
-                    <security:Certificate>%{idp.home}/credentials/gakunin-test-signer-2011.cer</security:Certificate>
-                </security:Credential>
-                <security:Credential id="GTestCredentialNew" xsi:type="security:X509ResourceBacked">
-                    <security:Certificate>%{idp.home}/credentials/gakunin-test-signer-2020.cer</security:Certificate>
-                </security:Credential>
-            </security:TrustEngine>
-        </MetadataFilter>
+        <MetadataFilter xsi:type="SignatureValidation" certificateFile="%{idp.home}/credentials/gakunin-test-signer-2020.cer" />
     (...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 id="HTTPMetadata"
     (...略...)
                       metadataURL="https://metadata.gakunin.nii.ac.jp/gakunin-test-metadata.xml">

-        <MetadataFilter xsi:type="SignatureValidation" certificateFile="%{idp.home}/credentials/gakunin-test-signer-2011.
cer" />
+        <MetadataFilter xsi:type="SignatureValidation" certificateFile="%{idp.home}/credentials/gakunin-test-signer-2020.
cer" />
     (...略...)
     </MetadataProvider>
```

変更後、以下のコマンドで設定を再読み込みします。

```
$ /opt/shibboleth-idp/bin/reload-service.sh -id shibboleth.MetadataResolverService
```

再読み込み後、エラーログ（/opt/shibboleth-idp/logs/idp-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、metadata-providers.xmlの証明書ファイルが正しいかどうか確認してください。

```
2020-11-30 14:05:32,408 -  - WARN [org.apache.xml.security.signature.XMLSignature:777] - Signature verification failed.
2020-11-30 14:05:32,409 -  - ERROR [org.opensaml.saml.metadata.resolver.filter.impl.SignatureValidationFilter:419] - Signature trust
establishment failed for metadata entry GakuNin-test
2020-11-30 14:05:32,410 -  - ERROR [org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:537] - Metadata
Resolver FileBackedHTTPMetadataResolver HTTPMetadata: Error filtering metadata from https://metadata.gakunin.nii.ac.jp/gakunin-test-
metadata.xml
org.opensaml.saml.metadata.resolver.filter.FilterException: Signature trust establishment failed for metadata entry
        at org.opensaml.saml.metadata.resolver.filter.impl.SignatureValidationFilter.verifySignature(SignatureValidationFilter.java:
420)
```

以上