IdPのメタデータ署名証明書移行手順

本ページは2017年に行われたメタデータ署名用証明書の切り替えの際に作成されたものです。内容が古くなっている可能性がありますのでご注意ください。

IdPの設定変更手順

新しい署名鍵で署名されたフェデレーションメタデータおよび新しい検証用証明書が公開されておりますので、本手順に従い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およびそのフィンガープリント、メタデータ公開URLは次のページで公開されているものです。
https://meatwiki.nii.ac.jp/confluence/display/GakuNinShibInstall/signer
上記ページURLは学認技術運用基準7.3)にて規定されております。
学認技術運用基準：https://www.gakunin.jp/document/80

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3.3.2)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。

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-signer-2017.cer」に置きます。
https://metadata.gakunin.nii.ac.jp/gakunin-signer-2017.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表示し、以下と一致するか確認してください。

SHA256 Fingerprint=5E:D6:A8:C5:E9:30:49:3F:B4:BA:77:54:6A:FB:66:BA:14:7D:CB:50:5B:EF:0F:D9:7C:26:04:C2:D9:36:FD:81

OpenSSLコマンドでは以下のように確認します。
> openssl x509 -in gakunin-signer-2017.cer -fingerprint -sha256 -noout

/opt/shibboleth-idp/conf/metadata-providers.xml を以下のように編集します。

1. <MetadataProvider>のmetadataURLに指定するメタデータダウンロードURLを以下の通り、末尾に ?generation=2 を付加します。

差分（unified diff形式）

```
  <MetadataProvider id="HTTPMetadata"
 (...略...)
-     metadataURL="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml">
+     metadataURL="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml?generation=2">
 (...略...)
```

2. <MetadataFilter>のcertificateFileに指定する署名検証用証明書のファイル名を以下の通り、2010 の部分を 2017 に修正します。

差分（unified diff形式）

```
  <MetadataProvider id="HTTPMetadata"
 (...略...)
     metadataURL="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml?generation=2">

-     <MetadataFilter xsi:type="SignatureValidation" certificateFile="%{idp.home}/credentials/gakunin-signer-2010.cer" />
+     <MetadataFilter xsi:type="SignatureValidation" certificateFile="%{idp.home}/credentials/gakunin-signer-2017.cer" />
 (...略...)
 </MetadataProvider>
```

変更後、**悪影響があることが判明していますので保存されたメタデータファイル(backingFile)を削除してから、**以下のコマンドで設定を再読み込みします。

```
$ sudo rm /opt/shibboleth-idp/metadata/gakunin-metadata-backing.xml
$ /opt/shibboleth-idp/bin/reload-service.sh -id shibboleth.MetadataResolverService
```

新しい署名鍵で署名されたメタデータがダウンロードされているか、保存されたメタデータファイル（/opt/shibboleth-idp/metadata/gakunin-metadata-backing.xml もしくはmetadata-providers.xmlのbackingFileで指定されたパス）を確認してください。
まず、ファイルの更新日時を確認し、上記再読み込みコマンド実行より後であることを確認してください。
次に、メタデータファイルの先頭から検索し、最初にマッチする</ds:X509Certificate>の直前の行が以下のようになっていれば成功です。

```
コマンド例：
$ grep -B 1 ”</ds:X509Certificate>” /opt/shibboleth-idp/metadata/gakunin-metadata-backing.xml | head -n 2
```

```
nwU/H9ROp1cl
</ds:X509Certificate>
```

以下のようになっている場合は古い署名鍵で署名されたものですので、ログ（/opt/shibboleth-idp/logs/idp-process.log）でメタデータのダウンロードが行われているか、ダウンロードURLが ?generation=2 付きになっているかを確認してください。

```
7NVe3mIUWLcYEtdbC8Ip5OA2TXvA
</ds:X509Certificate>
```

また、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の証明書ファイルの指定が -2017 のほうになっているか、および上述の証明書のフィンガープリントを今一度確認してください。

```
2017-11-16 13:44:23,237 - WARN [org.apache.xml.security.signature.XMLSignature:760] - Signature verification failed.
2017-11-16 13:44:23,237 - ERROR [org.opensaml.saml.metadata.resolver.filter.impl.SignatureValidationFilter:420] - Signature trust establishment failed for metadata entry GakuNin
2017-11-16 13:44:23,240 - WARN [org.opensaml.saml.metadata.resolver.filter.impl.SignatureValidationFilter:251] - Saw fatal error validating metadata signature(s), metadata will be filtered out
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:421)
```