

SPのメタデータ署名証明書移行手順(Procedure for Transition of Metadata Signing Certificate for SPs)

 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。

 [English version is here.](#)

SP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://metawiki.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SP(バージョン2.6.1)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読み替えてください。

新しい検証用証明書を以下のURLからダウンロードして「/etc/shibboleth/cert/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確認し、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

/etc/shibboleth/shibboleth2.xml を次のように編集します。

1. <MetadataProvider>のuri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 type="XML" validate="true"
-   uri="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml"
+   uri="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml?generation=2"
   backingFilePath="federation-metadata.xml" reloadInterval="7200">
(.....)
```

2. <MetadataFilter>のcertificate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 type="XML" validate="true"
(.....)
   backingFilePath="federation-metadata.xml" reloadInterval="7200">
-   <MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/gakunin-signer-2010.cer"/>
+   <MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/gakunin-signer-2017.cer"/>
(.....)
</MetadataProvider>
```



バージョン2.6およびそれ以降をお使いの場合、万一設定ミスした場合もしくはダウンロードに失敗した場合の保険として、さらに`verifyBackup="false"`を追加していない場合は追加することをお勧めします。そうでなければ、後述の再起動時、旧署名証明書で署名されたバックアップファイルに対して新署名証明書で検証するため失敗し、当該バックアップファイルが効果を失います。ただし、バックアップファイルが他者によって変更されないことが確実な場合のみこれを行ってください。

差分 (unified diff形式)

```
<MetadataProvider type="XML" validate="true"
(.....)
    backingFilePath="federation-metadata.xml" reloadInterval="7200">
-   <MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/gakunin-signer-2017.cer"/>
+   <MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/gakunin-signer-2017.cer" verifyBackup="
false"/>
(.....)
</MetadataProvider>
```

もちろんバックアップファイルが新メタデータで上書きされた後は上記問題は起こりませんが、起動時にバックアップファイルが使われる場合署名検証がスキップされ起動が速くなりますのでいずれにしろお勧めです。

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
```

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 (`/var/cache/shibboleth/federation-metadata.xml` もしくは `shibboleth2.xml` の `<MetadataProvider>` の `backingFilePath` 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、上記再起動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>` の直前の行が以下ようになっていれば成功です。

```
$ grep -B 1 "/ds:X509Certificate" /var/cache/shibboleth/federation-metadata.xml | head -n 2
nwU/H9R0p1cl
</ds:X509Certificate>
```

以下のように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 (`/var/log/shibboleth/shibd.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。

```
7NVe3mIUWLCyEtdbC8Ip50A2TXvA
</ds:X509Certificate>
```

また、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 `-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 14:19:44 WARN OpenSAML.MetadataFilter.Signature : filtering out group at root of instance after failed signature check:
CredentialResolver did not supply any candidate keys.
```

Procedure for Changing the SP Configuration to Use New GakuNin Signing Certificate

As new federation metadata signed by a new signing key and corresponding certificate were released, please change the configuration according to the procedure outlined here.



TL;DR

If the SAML implementation of your SP differs from Shibboleth SP, all you need to change are the following 2 points:

1. GakuNin metadata URL
old: <https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml>
NEW: <https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml?generation=2>
2. GakuNin signer certificate
old: [gakunin-signer-2010.cer](#)
NEW: [gakunin-signer-2017.cer](#)

You can also skip the latter half of this document because it is Shibboleth specific.

Download the new signing certificate from the URL below and place it in: `/etc/shibboleth/cert/gakunin-signer-2017.cer`
<https://metadata.gakunin.nii.ac.jp/gakunin-signer-2017.cer>



Confirmation of certificate fingerprint

Please confirm that the fingerprint of the downloaded certificate matches the following:

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 command is as follows:

```
> openssl x509 -in gakunin-signer-2017.cer -fingerprint -sha256 -noout
```

Please check the locations of signing certificate and fingerprint in : <https://meatwiki.nii.ac.jp/confluence/x/F4W5>

The signing certificate URL and its fingerprint and federation metadata URL are stipulated in "System Administration Standards for the GakuNin".

System Administration Standards for the GakuNin : <https://www.gakunin.jp/document/299>

notice:The following description is diff format.



This manual is for the standard Shibboleth SP configuration set according to version 2.6.0. If you are using a different version or configuration, please replace and read it accordingly.

Edit `/etc/shibboleth/shibboleth2.xml` as follows:

1. Amend the metadata URL for `<MetadataProvider>` as follows:

```
<MetadataProvider type="XML" validate="true"
-   uri="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml"
+   uri="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml?generation=2"
  backingFilePath="federation-metadata.xml" reloadInterval="7200">
  (.....)
```

2. Amend the certificate for `<MetadataFilter>` as follows:

```
<MetadataProvider type="XML" validate="true"
  (.....)
  backingFilePath="federation-metadata.xml" reloadInterval="7200">
-   <MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/gakunin-signer-2010.cer"/>
+   <MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/gakunin-signer-2017.cer"/>
  (.....)
</MetadataProvider>
```

Restart shibd and refresh the configuration.

```
(For CentOS 7)
$ sudo systemctl restart shibd
(For CentOS 6)
$ sudo service shibd restart
```

After a sufficient amount of time, please make sure that the signed metadata with the new signing key is downloaded. It is success that just before the first match "</ds:X509Certificate>" of the GakuNin metadata backing file (/var/cache/shibboleth/federation-metadata.xml or similar) is as follows:

```
$ grep -B 1 "/ds:X509Certificate" /var/cache/shibboleth/federation-metadata.xml | head -n 2
nwU/H9R0p1cl
</ds:X509Certificate>
```

If it looks like as follows, it is the metadata with a signature by the OLD signing key. You should check the log file to confirm that a metadata was downloaded and also check your configuration of download URL has a query string "?generation=2".

```
7NVe3mIUWLCyEtDbC8Ip50A2TXvA
</ds:X509Certificate>
```

Furthermore, if your log file (/var/log/shibboleth/shibd_warn.log) has following lines, it failed signature verification. You should check that your configuration of certificate path contains "-2017" and also check the fingerprint of the certificate again.

```
2017-11-16 14:19:44 WARN OpenSAML.MetadataFilter.Signature : filtering out group at root of instance after failed signature check:
CredentialResolver did not supply any candidate keys.
```