eduGAINメタデータ署名用証明書移行手順(Shibboleth SP向け)

本件はeduGAIN参加機関向け、eduGAINのメタデータ署名検証用証明書更新に伴うIdP/SP設定変更のお願いです。

eduGAINのメタデータの署名に用いている証明書が更新され、それに伴いメタデータダウンロードURLも更新されました。従来のメタデータダウンロードURLでの提供は**6月末まで**とのことですので、eduGAIN参加のみなさまにおかれましては期日までに設定変更を行なっていただけますようよろしくお願いいたします。

SPの設定変更手順

新しい署名鍵で署名されたeduGAIN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。

技術ガイド 学認参加IdP・SPがeduGAINメタデータを読み込む手順 の手順に従って、eduGAINメタデータを読み込んでいる前提で説明します。

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://technical.edugain.org/metadata

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/mds-v2.cer」に配置します。

- https://technical.edugain.org/mds-v2.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=BD:21:40:48:9A:9B:D7:40:44:DD:68:05:34:F7:78:88:A9:C1:3B:0A:C1:7C:4F:3A:03:6E:0F:EC:6D:89:99:95

OpenSSLコマンドでは以下のように確認します。
> openssl x509 -in mds-v2.cer -fingerprint -sha256 -noout

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

- <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、v1の部分をv2に修正します。

差分（unified diff形式）

```
         <!-- for eduGAIN -->
         <MetadataProvider type="XML"
-              url="http://edugain.cdn.samlbits.net/edugain-v1.xml"
+              url="http://edugain.cdn.samlbits.net/edugain-v2.xml"
             (...略...)
```

- <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、v1の部分をv2に修正します。

差分（unified diff形式）

```
         <!-- for eduGAIN -->
         <MetadataProvider type="XML"
             (...略...)
               backingFilePath="edugain-backing.xml" maxRefreshDelay="7200">
             <MetadataFilter type="RequireValidUntil" maxValidityInterval="777600"/>
-            <MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/mds-v1.cer"/>
+            <MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/mds-v2.cer"/>
             (...略...)
```

shibdを再起動し、設定を再読み込みします。

```
$ sudo systemctl restart shibd
```

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の証明書ファイルおよびダウンロードURLの指定が正しいかどうか確認してください。

```
2022-03-30 10:13:31 WARN OpenSAML.MetadataFilter.Signature : filtering out group at root of instance after failed signature check:
CredentialResolver did not supply any candidate keys.
```

以上

参考情報

- IdPの設定変更手順
- eduGAINに関する情報
- eduGAINに参加する