eduGAINメタデータ署名用証明書移行手順(Shibboleth IdP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。

IdP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「/opt/shibboleth-idp/credentials/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

`/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、v1の部分をv2に修正します。

差分（unified diff形式）

```
     <MetadataProvider id="HTTPMetadata-eduGAIN"
                       xsi:type="FileBackedHTTPMetadataProvider"
                       backingFile="%{idp.home}/metadata/edugain-backing.xml"
-                      metadataURL="http://edugain.cdn.samlbits.net/edugain-v1.xml">
+                      metadataURL="http://edugain.cdn.samlbits.net/edugain-v2.xml">
     (...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、v1の部分をv2に修正します。

差分（unified diff形式）

```
     <MetadataProvider id="HTTPMetadata-eduGAIN"
     (...略...)
                       metadataURL="http://edugain.cdn.samlbits.net/edugain-v2.xml">

         <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
-                        certificateFile="%{idp.home}/credentials/mds-v1.cer"/>
+                        certificateFile="%{idp.home}/credentials/mds-v2.cer"/>
     (...略...)
```

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
```


今回のようにメタデータのダウンロード等の処理に時間がかかると、reload-service.shのコマンド実行時に以下のようなHTTP 502エラーが返ってくることがあります。

```
$ /opt/shibboleth-idp/bin/reload-service.sh -id shibboleth.MetadataResolverService
(http://localhost/idp/profile/admin/reload-service?id=shibboleth.MetadataResolverService) Server returned HTTP response
code: 502 for URL: http://localhost/idp/profile/admin/reload-service?id=shibboleth.MetadataResolverService
```

この場合はログ（/opt/shibboleth-idp/logs/idp-process.log）を確認して、再読み込みが正常に完了していることを確認してください。
以下のように"New metadata successfully loaded for ..."のログが記録されていれば、再読み込みは正常に完了しています。

```
2022-05-20 15:18:42,252 - 127.0.0.1 - INFO [org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:592]
- Metadata Resolver FileBackedHTTPMetadataResolver HTTPMetadata-eduGAIN: New metadata successfully loaded for
'http://edugain.cdn.samlbits.net/edugain-v2.xml'
2022-05-20 15:18:42,253 - 127.0.0.1 - INFO [org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:397]
- Metadata Resolver FileBackedHTTPMetadataResolver HTTPMetadata-eduGAIN: Next refresh cycle for metadata provider
'http://edugain.cdn.samlbits.net/edugain-v2.xml' will occur on '2022-05-20T06:18:47.252219Z' ('2022-05-20T15:18:47.252219+09:
00[Asia/Tokyo]' local time)
2022-05-20 15:18:42,845 - 127.0.0.1 - INFO [net.shibboleth.ext.spring.service.ReloadableSpringService:421] - Service
'shibboleth.MetadataResolverService': Completed reload and swapped in latest configuration for service 'shibboleth.
MetadataResolverService'
2022-05-20 15:18:42,862 - 127.0.0.1 - INFO [net.shibboleth.ext.spring.service.ReloadableSpringService:428] - Service
'shibboleth.MetadataResolverService': Reload complete
2022-05-20 15:18:42,865 - 127.0.0.1 - INFO [Shibboleth-Audit.Reload:282] - 127.0.0.1|2022-05-20T06:17:51.554252Z|2022-05-
20T06:18:42.865541Z|||||||||||||||||Java/11.0.15
```

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の証明書ファイルおよびダウンロードURL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 http://edugain.org/
2020-11-30 14:05:32,410 -  - ERROR [org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:537] - Metadata
Resolver FileBackedHTTPMetadataResolver HTTPMetadata-eduGAIN: Error filtering metadata from http://edugain.cdn.samlbits.net/edugain-
v2.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)
```

最後に、証明書移行とは無関係ながら、現在のeduGAINメタデータを読み込むのにメモリ量設定が足りないのではないかという報告がございます。メモリに余裕がありましたらJettyのメモリ使用設定を1.5GBから2GBに増量することもご検討ください。

/opt/jetty-base/start.d/start.ini:

-Xmx1500m → -Xmx2g

以上

参考情報

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