学認参加IdP・SPがeduGAINメタデータを読み込む手順

（更新情報2024-02-06）
eduGAINメタデータURLを学認でホストされたものに更新しました。

（更新情報2022-04-28）
eduGAIN側のメタデータ署名用証明書更新に伴い証明書フィンガープリントを更新しました。

（更新情報2021-04-05）
eduGAIN側のメタデータ署名用証明書更新に伴い証明書フィンガープリントを更新しました。ただし公開鍵は同一ですので以前の設定のままのIdP/SPがあっても問題になることはないと思われます。

（更新情報2020-09-02）
IdPの設定手順に確認方法を追記しました。

（更新情報2019-06-13）
eduGAIN側のメタデータ署名用証明書更新に伴い証明書およびダウンロードURLを更新しました。ただし公開鍵は同一ですので以前の設定のままのIdP/SPがあっても問題になることはないと思われます。

（更新情報2018-11-05）
eduGAINメタデータの取得にsamlbits.netを使うように更新されております。こちらを用いることにより安定性を向上させることができますので、すでに設定済みのIdP/SPについても今一度ご確認ください。

IdPの設定方法

学認に参加しているIdPでeduGAINメタデータを読み込む手順です。技術ガイド metadata-providers.xml ファイルの変更 の手順に従って、学認の運用フェデレーションメタデータを読み込んでいる前提で説明します。

eduGAINメタデータはサイズが大きいため、読み込むには多くのメモリが必要です。事前に十分なメモリが割り当てられていることを確認してください。技術ガイドの手順に"-Xmx1500m"(1.5GB)の指定がありますが、"-Xmx2g"(2GB)以上が指定されていれば大丈夫なようです。

eduGAINメタデータを検証するための証明書（https://technical.edugain.org/mds-v2.cer）をダウンロードして、任意のディレクトリに置き、そのパスを設定します。（以下では「/opt/shibboleth-idp/credentials/」に置いたものとして説明しています）

ダウンロードした検証用証明書のフィンガープリントが下記と一致するか確認してください。

- SHA-256

```
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
```

eduGAINメタデータを自動的にダウンロードする設定を行います。/opt/shibboleth-idp/conf/metadata-providers.xml ファイルで、学認の運用フェデレーションメタデータを読み込む設定の直下に下記の設定を追加してください。

```
    <MetadataProvider id="HTTPMetadata-eduGAIN"
                      xsi:type="FileBackedHTTPMetadataProvider"
                      backingFile="%{idp.home}/metadata/edugain-backing.xml"
                                    ↑ eduGAINメタデータは上記のファイル名で保存されます。必要に応じて調整してください。
                      metadataURL="https://metadata.gakunin.nii.ac.jp/edugain-v2.xml">


        <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
                        certificateFile="%{idp.home}/credentials/mds-v2.cer"/>
        <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>
                                                                    ↑ 9日間を設定します。
        <!-- MetadataFilter xsi:type="SchemaValidation"/ -->
        <MetadataFilter xsi:type="EntityRoleWhiteList">
            <RetainedRole>md:SPSSODescriptor</RetainedRole>
        </MetadataFilter>
    </MetadataProvider>
```

上記設定でSignatureValidationをコメントアウトしていますが、これは意図的なものです。有効にすると以下を含むエラーが記録され起動しません。(2017年1月6日時点)

```
Caused by: net.shibboleth.utilities.java.support.resolver.ResolverException: Error filtering metadata from http://mds.edugain.org/edugain-v1.xml
        at org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver.processNonExpiredMetadata(AbstractReloadingMetadataResolver.java:430)
Caused by: org.opensaml.saml.metadata.resolver.filter.FilterException: Incoming metadata was not schema valid
        at org.opensaml.saml.metadata.resolver.filter.impl.SchemaValidationFilter.filter(SchemaValidationFilter.java:121)
Caused by: org.xml.sax.SAXParseException: cvc-elt.4.2: Cannot resolve 'fed:ApplicationServiceType' to a type definition for element 'md:RoleDescriptor'.
        at com.sun.org.apache.xerces.internal.util.ErrorHandlerWrapper.createSAXParseException(ErrorHandlerWrapper.java:198)
```

設定を更新しIdPに反映後の動作確認は、IdP単体で行うならIdPのサービス動作状況の確認（IdP）に記載の方法（もしくは同等の/opt/shibboleth-idp/bin/status.sh）で可能です。

```
        metadata source: HTTPMetadata-eduGAIN
        last refresh attempt: 2017-09-07T06:34:25Z
        last update: 2017-09-07T06:34:25Z
```

のように出力される部分に"last error: ..."のような行がなければ、eduGAINメタデータの読み込みは成功していると考えられます。

さらに、eduGAIN参加後のIdP挙動のチェックについては、eduGAINのサービスである「eduGAIN Connectivity Check Service」もご利用いただけます。これはすでにeduGAINに参加している全IdPについて定期的に設定内容をチェックしているサービスです。
https://technical.edugain.org/eccs/index.php
こちらにIdPのentityIDを入れて検索すると、チェック結果が表示されます。当該エントリが緑背景でCurrent ResultがOKとなっていれば正常です。

SPの設定方法

学認に参加しているSPでeduGAINメタデータを読み込む手順です。技術ガイド shibboleth2.xml ファイル の手順に従って、学認の運用フェデレーションメタデータを読み込んでいる前提で説明します。

eduGAINメタデータを検証するための証明書（https://technical.edugain.org/mds-v2.cer）をダウンロードして、任意のディレクトリに置き、そのパスを設定します。（以下では「 /etc/shibboleth/cert/」に置いたものとして説明しています）

ダウンロードした検証用証明書のフィンガープリントが下記と一致するか確認してください。

- SHA-256

```
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
```

eduGAINメタデータを自動的にダウンロードし、検証するための設定を行います。/etc/shibboleth/shibboleth2.xml ファイルで、学認の運用フェデレーションメタデータを読み込む設定の直下に下記の設定を追加してください。

```
        <!-- for eduGAIN -->
        <MetadataProvider type="XML"
              url="https://metadata.gakunin.nii.ac.jp/edugain-v2.xml"
              backingFilePath="edugain-backing.xml" maxRefreshDelay="7200">
                                ↑ eduGAINメタデータは上記のファイル名で保存されます。必要に応じて調整してください。
            <MetadataFilter type="RequireValidUntil" maxValidityInterval="777600"/>
                                                                    ↑ 9日間（777600秒）を設定します。
            <MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/mds-v2.cer"/>
            <DiscoveryFilter type="Blacklist" matcher="EntityAttributes" trimTags="true"
              attributeName="http://macedir.org/entity-category"
              attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
              attributeValue="http://refeds.org/category/hide-from-discovery" />
        </MetadataProvider>
```

ローカルのバッキング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はSignature MetadataFilterの末尾に verifyBackup="false" を追加してください。起動時のメタデータ読み込み時にバッキングファイルの署名検証がスキップされ起動が速くなります。（バージョン2.6およびそれ以降で対応）

```
<MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/mds-v2.cer" verifyBackup="false"/>
```

他のMetadataProviderと比較して、validate="true"が削除されていることにご注意ください。

参考情報

- https://technical.edugain.org/metadata
- https://wiki.edugain.org/Republish_eduGAIN_Metadata
- https://www.switch.ch/aai/support/presentations/shibboleth-training-2015/T3P18-New_Challenges_with_Interfederation.pdf