旧: メタデータの作成と提出(IdPv4)

メタデータの作成と提出

1.メタデータの作成

メタデータテンプレートは、初期設定で「/root/GETFILE」に取得したidp-metadata.xmlを使用します。

rootのホームディレクトリに「**ex-idp-test??.xml**」のファイル名でコピーします。(??は各自、割り振られた番号に置き換えてください)

```
# cp /root/GETFILE/idp-metadata.xml /root/ex-idp-test??.xml
                                                    ↑ ホスト名
```

/root/ex-idp-test??.xmlの設定を行います。

証明書部分には、/opt/shibboleth-idp/credentials/server.crtの内容を使用します。）

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://ex-idp-test??.gakunin.nii.ac.jp/idp/shibboleth">
                                                                                ↑ ホスト名
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:mace:shibboleth:1.0 urn:oasis:names:tc:SAML:
2.0:protocol">
    <Extensions>
      <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" regexp="false">nii.ac.jp</shibmd:Scope>
                                                                                ↑ 構築したIdPのスコープ（SCOPEをnii.ac.jpに設定）
      <mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
        <mdui:DisplayName xml:lang="ja">実習セミナーIdPテストXX</mdui:DisplayName>
        <mdui:DisplayName xml:lang="en">Ex-IdP-TestXX</mdui:DisplayName>
                                        ↑ IdP名称（英/日）、DSに表示されます。
```

```
                                        XXは、割り当てられた番号に置き換えてください。
        <mdui:Keywords xml:lang="en">category:location:seito category:organizationType:others</mdui:Keywords>
                                        ↑ 地域                  ↑ IdPカテゴリ
      </mdui:UIInfo>
    </Extensions>
    <KeyDescriptor>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
MIIFITCCBAmgAwIBAgIIBpAaVBrt6kMwDQYJKoZIhvcNAQEFBQAwfTELMAkGA1UE
BhMCSlAxETAPBgNVBAcTCEFjYWRlbWUyMSowKAYDVQQKEyFOYXRpb25hbCBJbnN0
aXR1dGUgb2YgSW5mb3JtYXRpY3MxDTALBgNVBAsTBFVQS0kxIDAeBgNVBAsTF05J
（中略）
kBFfvNBdrux4CkIsKhpYQXCAIEuy12CFZUXEtHB5XxeBkntbs2lfP/rWbg2J1Ige
zZc6shCn3VdrL2douVFjaAXlc8zwys/KIpLzNSxOOGwJdKxFTaIzH/emcqKj93Jd
DC1rrFMhoPE=
↑ 設定した証明書に変更（/opt/shibboleth-idp/credentials/server.crt）
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
    <SingleSignOnService Location="https://ex-idp-test??.gakunin.nii.ac.jp/idp/profile/Shibboleth/SSO" Binding="urn:mace:shibboleth:
1.0:profiles:AuthnRequest"/>
                                        ↑ ホスト名
    <SingleSignOnService Location="https://ex-idp-test??.gakunin.nii.ac.jp/idp/profile/SAML2/POST/SSO" Binding="urn:oasis:names:tc:
SAML:2.0:bindings:HTTP-POST"/>
                                        ↑ ホスト名
    <SingleSignOnService Location="https://ex-idp-test??.gakunin.nii.ac.jp/idp/profile/SAML2/Redirect/SSO" Binding="urn:oasis:names:
tc:SAML:2.0:bindings:HTTP-Redirect"/>
                                        ↑ ホスト名
  </IDPSSODescriptor>
  <AttributeAuthorityDescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">

    <Extensions>
      <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" regexp="false">nii.ac.jp</shibmd:Scope>
                                                                    ↑ 構築したIdPのスコープ（SCOPEをnii.ac.jpに設定）
    </Extensions>
    <KeyDescriptor>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
MIIFITCCBAmgAwIBAgIIBpAaVBrt6kMwDQYJKoZIhvcNAQEFBQAwfTELMAkGA1UE
BhMCSlAxETAPBgNVBAcTCEFjYWRlbWUyMSowKAYDVQQKEyFOYXRpb25hbCBJbnN0
aXR1dGUgb2YgSW5mb3JtYXRpY3MxDTALBgNVBAsTBFVQS0kxIDAeBgNVBAsTF05J
（中略）
kBFfvNBdrux4CkIsKhpYQXCAIEuy12CFZUXEtHB5XxeBkntbs2lfP/rWbg2J1Ige
zZc6shCn3VdrL2douVFjaAXlc8zwys/KIpLzNSxOOGwJdKxFTaIzH/emcqKj93Jd
DC1rrFMhoPE=
↑ 設定した証明書に変更（/opt/shibboleth-idp/credentials/server.crt）
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <AttributeService Location="https://ex-idp-test??.gakunin.nii.ac.jp:8443/idp/profile/SAML1/SOAP/AttributeQuery" Binding="urn:
oasis:names:tc:SAML:1.0:bindings:SOAP-binding"/>
                                        ↑ ホスト名
    <AttributeService Location="https://ex-idp-test??.gakunin.nii.ac.jp:8443/idp/profile/SAML2/SOAP/AttributeQuery" Binding="urn:
oasis:names:tc:SAML:2.0:bindings:SOAP"/>
                                        ↑ ホスト名
    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
  </AttributeAuthorityDescriptor>
  <Organization>
    <OrganizationName xml:lang="en">Training Seminar University</OrganizationName>
    <OrganizationName xml:lang="ja">実習セミナー大学</OrganizationName>
                                      ↑ 機関名称（英/日）
    <OrganizationDisplayName xml:lang="en">Ex-IdP-TestXX</OrganizationDisplayName>
    <OrganizationDisplayName xml:lang="ja">実習セミナーIdPテスト??</OrganizationDisplayName>
                                        ↑ IdP名称（英/日）、DSに表示されます。
```

```
                                                    XXは、割り当てられた番号に置き換えてください。
    <OrganizationURL xml:lang="en">http://YourHomePage/</OrganizationURL>
  </Organization>
  <ContactPerson contactType="technical">
    <GivenName>Your GivenName</GivenName>
    <SurName>Your SurName</SurName>
    <EmailAddress>mailto:admin@example.org</EmailAddress>
  </ContactPerson>
</EntityDescriptor>
```

作成したメタデータは**学認申請システムではなく、実習セミナー内のDSサーバに転送**します。

```
# scp /root/ex-idp-test??.xml uploader@ex-ds.gakunin.nii.ac.jp:METADATA
                                    ↑「??」には割り振られた番号を記述
ex-idp-test??.xml                   100% 7072     6.9KB/s   00:00
                                                ↑100%で転送完了
```

ヒント

転送したメタデータは、1分周期で他のメタデータとマージ処理を行い、実習セミナー内のフェデレーションメタデータが更新されます。
※1分周期で行う為、最大約1分登録までに時間がかかります。