メタデータの作成と設定（SP）2023

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sp-metadata.xmlを使用します。

rootのホームディレクトリに**「*"ドメインなしホスト名"*.xml」のファイル名でコピー**します。

```
# cp /root/GETFILE/sp-metadata.xml /root/ex-sp-test??.xml   ←??は割り振られた番号を設定してください

確認のため、lsを実行

# ls -l /root/ex-sp-test??.xml

-rw-r--r-- 1 root root 2777  7月  5 17:47 /root/ex-sp-test20.xml
```

「ex-sp-test??.xml」の**必要な項目を変更**します。

（なお、<ds:X509Certificate></ds:X509Certificate>で囲まれた証明書部分には、/etc/shibboleth/cert/server.crtの内容を使用します。）

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"  entityID="https://ex-sp-test??.gakunin.nii.ac.jp/shibboleth-sp">
                                                                                                ↑ ホスト名(??は割り振られた番号)
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol urn:oasis:names:tc:SAML:1.1:protocol">
    <Extensions>
      <idpdisc:DiscoveryResponse xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol"
          Location="https://ex-sp-test??.gakunin.nii.ac.jp/Shibboleth.sso/DS" index="1"
                                  ↑ ホスト名(??は割り振られた番号)
          Binding="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol"/>

      <mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
        <mdui:DisplayName xml:lang="ja">実習セミナーSPテストXX</mdui:DisplayName>← XXは割り振られた番号
        <mdui:DisplayName xml:lang="en">Ex-SP-TestXX</mdui:DisplayName>
                                              ↑ SP名称（英/日）、XXは割り振られた番号
      </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
DC1rrFWhoPE=
↑ 設定した証明書に変更（/etc/shibboleth/cert/server.crt）
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <AssertionConsumerService isDefault="true"
        Location="https://ex-sp-test??.gakunin.nii.ac.jp/Shibboleth.sso/SAML2/POST" index="1"
                                  ↑ ホスト名(??は割り振られた番号)
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
    <AssertionConsumerService
        Location="https://ex-sp-test??.gakunin.nii.ac.jp/Shibboleth.sso/SAML2/POST-SimpleSign" index="2"
                                  ↑ ホスト名(??は割り振られた番号)
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"/>
    <AssertionConsumerService
        Location="https://ex-sp-test??.gakunin.nii.ac.jp/Shibboleth.sso/SAML2/Artifact" index="3"
                                  ↑ ホスト名(??は割り振られた番号)
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"/>
    <AssertionConsumerService
        Location="https://ex-sp-test??.gakunin.nii.ac.jp/Shibboleth.sso/SAML/POST" index="4"
                                  ↑ ホスト名(??は割り振られた番号)
        Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"/>
    <AssertionConsumerService
        Location="https://ex-sp-test??.gakunin.nii.ac.jp/Shibboleth.sso/SAML/Artifact" index="5"
                                  ↑ ホスト名(??は割り振られた番号)
        Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"/>

  </SPSSODescriptor>
  <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-SP-TestXX</OrganizationDisplayName>
    <OrganizationDisplayName xml:lang="ja">実習セミナーSPテストXX</OrganizationDisplayName>
                                              ↑ SP名称（英/日）
    <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>
```

※ viで「↑ 設定した証明書に変更（/etc/shibboleth/cert/server.crt）」を実現する操作

viで他ファイルの読み込み（:r コマンド）

(1) 緑色部分を削除

```
      <ds:X509Certificate>
MIIFITCCBAmgAwIBAgIIBpAaVBrt6kMwDQYJKoZIhvcNAQEFBQAwfTELMAkGA1UE
BhMCSlAxETAPBgNVBAcTCEFjYWRlbWUyMSowKAYDVQQKEyFOYXRpb25hbCBJbnN0
（中略）
zZc6shCn3VdrL2douVFjaAXlc8zwys/KIpLzNSxOOGwJdKxFTaIzH/emcqKj93Jd
DC1rrFMhoPE=
      </ds:X509Certificate>
```

(2) **:r /etc/shibboleth/cert/server.crt** とreadコマンドを投入する

```
      <ds:X509Certificate>
←カーソル位置
      </ds:X509Certificate>



:r /etc/shibboleth/cert/server.crt   ←画面最下行
```

(3) すると、/etc/shibboleth/cert/server.crtの内容が読み込まれる

```
      <ds:X509Certificate>
-----BEGIN CERTIFICATE-----
MIIHQTCCBimgAwIBAgIQSG8djrJHs7bdgB4ELhMrwzANBgkqhkiG9w0BAQsFADBa
MQswCQYDVQQGEwJKUDElMCMGA1UEChMcU0VDT00gVHJ1c3QgU3lzdGVtcyBDTy4s

（中略）

6y4A48KtzQ3uWlyntM1URxAuvxM01b6IxR4wa81fapxTL325VlPjVIsRiD162Nqy
ARVL5AsYf4aeNnZO26dVpToGCrmX8HwoVmUXsVDIRciwctzO+w==
-----END CERTIFICATE-----
      </ds:X509Certificate>
```

(4) 「-----BEGIN CERTIFICATE-----」「-----END CERTIFICATE-----」を削除する

```
      <ds:X509Certificate>
MIIHQTCCBimgAwIBAgIQSG8djrJHs7bdgB4ELhMrwzANBgkqhkiG9w0BAQsFADBa
MQswCQYDVQQGEwJKUDElMCMGA1UEChMcU0VDT00gVHJ1c3QgU3lzdGVtcyBDTy4s

（中略）

6y4A48KtzQ3uWlyntM1URxAuvxM01b6IxR4wa81fapxTL325VlPjVIsRiD162Nqy
ARVL5AsYf4aeNnZO26dVpToGCrmX8HwoVmUXsVDIRciwctzO+w==
      </ds:X509Certificate>
```

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-sp-test??.xml  uploader:METADATA

                              ↑「??」には割り振られた番号を記述

ex-sp-test??.xml                    100% 7072     6.9KB/s   00:00

                                      ↑100%で転送完了
```

実習セミナー

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。