2024年11月8日

SAMLAuthnConfiguration機能による

SAMLプロキシの実現

国立情報学研究所

教育研修事業

**目次**

[**1. はじめに 2**](#_heading=h.486mtdvy58z)

[**2. 実習セミナーでは 2**](#_heading=h.tauevnjjbosw)

[**3. 動作確認 5**](#_heading=h.7zrt2eifjiro)

# **はじめに**

SAML Proxyを利用することで、Shibboleth IdPはユーザーを認証するプロセスを別のIdPに委譲することができます。

# **実習セミナーでは**

以下のような設定で行います。

|  |
| --- |
| SPから認証要求を直接受け取るIdPを「SAML Proxy IdP」とし、  そのEntityIDは以下のとおりです。  "https://ex-idp-test??.gakunin.nii.ac.jp/idp/shibboleth"  SAML Proxy IdPが認証委譲する先のIdPを「アップストリーム IdP」とし、  そのEntityIDは以下のとおりです。  "https://ex-idp.gakunin.nii.ac.jp/idp/shibboleth"  どちらのIdPもShibboleth IdPを利用します。  アップストリーム IdPはメタデータ以外既に設定済みです。 |

* SPメタデータの作成・提出

SAML ProxyではShibboleth IdPはSPとして振る舞い、アップストリーム IdPに認証要求を行うため、SPとしてのメタデータを作成し、アップストリーム IdPに提供します。以下の内容で /root/ex-idp-test??.xml というファイルを作成してください。

|  |
| --- |
| <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://ex-idp-test??.gakunin.nii.ac.jp/idp/shibboleth" >  SAML Proxy IdPのホスト名↑  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">  <KeyDescriptor>  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  <ds:X509Data>  <ds:X509Certificate>  MIIHQjCCBiqgAwIBAgIQQsAPav4/uCrWMDHZXvM5oDANBgkqhkiG9w0BAQsFADBa  MQDVQQGEwJVDT00gVHJKUDElswCQYMCMGA1UEChMcU01c3QgU3lzdGVtcyBDTy4s  (省略)  LbzM7Jwo+QIJ68THd97BjA8Do+EcKpsmog3qKMEAxAJP7K1j508JVNnjYVmv6EF/  QbXkQerkU7PBdrtmtmPHr/KlpYWVHrGs89tOHP3CmnMyDbOBzg=  </ds:X509Certificate>  </ds:X509Data>  </ds:KeyInfo>  </KeyDescriptor>  <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  Location="https://ex-idp-test??.gakunin.nii.ac.jp/idp/profile/Authn/SAML2/POST/SSO" index="0"/>  SAML Proxy IdPのホスト名↑  </SPSSODescriptor>  </EntityDescriptor> |

以下のコマンドで実習セミナーフェデレーションへ提出してください。自動的にアップストリームIdPに読み込まれます。

|  |
| --- |
| # scp /root/ex-idp-test??.xml uploader:METADATA |

* アップストリーム IdPのメタデータ登録

/opt/shibboleth-idp/metadata/upstream-idp-metadata.xmlファイルを新規作成し、以下のアップストリーム IdPのメタデータ情報を記載します。「アップストリームIdPの証明書」の部分は、実習セミナーフェデレーションメタデータ

<https://ex-ds.gakunin.nii.ac.jp/fed/ex-fed-metadata.xml>

からentityIDで検索し適切に切り出してください。

※ 今回簡略化のためアップストリームIdPメタデータを手作業で作成していますが、適切に切り出せば上記フェデレーションメタデータ等から切り出したメタデータを利用可能です。

|  |
| --- |
| <md:EntityDescriptor entityID="https://ex-idp.gakunin.nii.ac.jp/idp/shibboleth"  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">  <md:KeyDescriptor>  <ds:KeyInfo>  <ds:X509Data>  <ds:X509Certificate>  MIIHgDCCBmigAwIBAgIQMXVPXxYaNC6EPpnqMPZOojANBgkqhkiG9w0BAQsFADBa  (省略) ← アップストリームIdPの証明書  2wBiBA==  </ds:X509Certificate>  </ds:X509Data>  </ds:KeyInfo>  </md:KeyDescriptor>  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://ex-idp.gakunin.nii.ac.jp/idp/profile/SAML2/SOAP/ArtifactResolution" />  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign" Location="https://ex-idp.gakunin.nii.ac.jp/idp/profile/SAML2/POST-SimpleSign/SSO" />  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://ex-idp.gakunin.nii.ac.jp/idp/profile/SAML2/Redirect/SSO" />  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://ex-idp.gakunin.nii.ac.jp/idp/profile/SAML2/POST/SSO" />  </md:IDPSSODescriptor>  </md:EntityDescriptor> |

/opt/shibboleth-idp/conf/metadata-providers.xmlに以下を追加します。

|  |
| --- |
| <MetadataProvider id="ShibbolethMetadata" (省略) >  (省略)  <MetadataProvider id="UpstreamIdPMetadata" xsi:type="FilesystemMetadataProvider" metadataFile="%{idp.home}/metadata/upstream-idp-metadata.xml"/>  (省略)  </MetadataProvider> |

* 認証フローの設定

/opt/shibboleth-idp/conf/authn/authn.propertiesのidp.authn.flowsとidp.authn.SAML.proxyEntityIDを以下のように設定します。

|  |
| --- |
| idp.authn.flows = SAML  (省略)  ~~#~~ idp.authn.SAML.proxyEntityID = https://ex-idp.gakunin.nii.ac.jp/idp/shibboleth  ↑コメントアウトを削除 |

* 属性フィルタの更新

アップストリーム IdPから受け取る属性の設定をします。

実習セミナーではアップストリーム IdPから「uid」属性を受け取るよう設定します。

/opt/shibboleth-idp/conf/attribute-filter.xmlに以下を追加します。

|  |
| --- |
| <AttributeFilterPolicyGroup id="ShibbolethFilterPolicy" (省略) >  (省略)  <!-- For SAML Proxy -->  <AttributeFilterPolicy id="saml-proxy-pass-through">  <PolicyRequirementRule xsi:type="Issuer" value="https://ex-idp.gakunin.nii.ac.jp/idp/shibboleth" />  <AttributeRule attributeID="uid" permitAny="true" />  </AttributeFilterPolicy>  </AttributeFilterPolicyGroup> |

* C14Nの設定

/opt/shibboleth-idp/conf/c14n/subject-c14n.xmlの以下の行のコメントアウトをはずします。

|  |
| --- |
| ~~<!-~~  <bean id="c14n/attribute" parent="shibboleth.PostLoginSubjectCanonicalizationFlow" />  ~~..>~~  ↑コメントアウトを削除 |

/opt/shibboleth-idp/conf/c14n/subject-c14n.propertiesを以下のように設定します。

|  |
| --- |
| ~~#~~ idp.c14n.attribute.attributeSourceIds = uid  ~~#~~ idp.c14n.attribute.resolveFromSubject = true  ↑コメントアウトを削除 |

* Jetty再起動

jettyを再起動します。

|  |
| --- |
| # systemctl restart jetty |

# **動作確認**

① 接続確認用SPにアクセスします。  
　テストフェデレーションの場合: <https://test-sp1.gakunin.nii.ac.jp/>

② ログインボタンをクリックします。

③ DSの設定を行っている場合、所属機関の選択画面が表示されるので、各自が使用するIdPを選択します。

④ アップストリーム IdPの認証画面が表示されます。

⑤ Username/Passwordを入力して次に進みます。

⑥ アップストリームIdPの送信属性同意画面が表示されます。そのまま設定値を送信します。

⑦ SAML Proxy IdPの送信属性同意画面が表示されます。そのまま設定値を送信します。

⑧ 認証後、正しく属性受信の確認ページが表示される事を確認してください。