

# attribute-resolver.xml ファイルの変更 (IdPv3)

## attribute-resolver.xml ファイルの変更

### 0. 事前準備

デフォルトの /opt/shibboleth-idp/conf/attribute-resolver.xml をテンプレートで差し替え、下記にしたがい修正してください。

### 1. 属性の定義部分を、以下の例に従い有効にします

各属性の定義方法は[ここ](#)を参照下さい。

#### (1) eduPersonPrincipalNameを有効とする例：

```
<!-- Attribute Definition for eduPersonPrincipalName -->
<!-- --> ← コメント終了を追加して、以下を有効にします
<resolver:AttributeDefinition xsi:type="ad:Scoped" id="eduPersonPrincipalName" scope="%{idp.scope}" sourceAttributeID="uid">
  ← scopeはidp.propertiesを参照するので設定不要です。
  sourceAttributeIDにLDAP内の属性名を設定します。
  <resolver:Dependency ref="myLDAP" />
  <resolver:AttributeEncoder xsi:type="enc:SAML1ScopedString" name="urn:mace:dir:attribute-def:eduPersonPrincipalName"
  encodeType="false" />
  <resolver:AttributeEncoder xsi:type="enc:SAML2ScopedString" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" friendlyName="
  eduPersonPrincipalName" encodeType="false" />
</resolver:AttributeDefinition>
<!-- --> ← コメント開始を追加して、上記を有効にします
```

#### (2) eduPersonEntitlementのurn:mace:dir:entitlement:common-lib-termsを有効とする例：

```
<!-- Attribute Definition for eduPersonEntitlement -->
<!-- --> ← コメント終了を追加して、以下を有効にします
<resolver:AttributeDefinition xsi:type="ad:Simple" id="eduPersonEntitlement" sourceAttributeID="eduPersonEntitlement">
  <resolver:Dependency ref="staticEntitlementCommonLibTerms" />
  <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-def:eduPersonEntitlement" encodeType="
  false" />
  <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" friendlyName="
  eduPersonEntitlement" encodeType="false" />
</resolver:AttributeDefinition>
<!-- --> ← コメント開始を追加して、上記を有効にします
<!-- Static Connector for eduPersonEntitlement (common-lib-terms) -->
<!-- --> ← コメント終了を追加して、以下を有効にします
  <resolver:DataConnector id="staticEntitlementCommonLibTerms" xsi:type="dc:Static">
    <dc:Attribute id="eduPersonEntitlement">
      <dc:Value>urn:mace:dir:entitlement:common-lib-terms</dc:Value>
    </dc:Attribute>
  </resolver:DataConnector>
<!-- --> ← コメント開始を追加して、上記を有効にします
```

※属性値としてcommon-lib-terms以外を送信する場合は、しかるべき人にそのような値を生成するDataConnectorを用意し、上記5行目にDependencyとして追加してください。

### 2. 利用するコネクタを設定します

現在学認で配布しているバージョンでは [ldap.properties](#) を参照するようになっていまして、LDAP URLやbaseDN等を直接記述する必要はありません。ただし `returnAttributes` を指定している場合もしくは `useStartTLS=true` もしくは `useSSL=true` としている場合はテンプレートファイル中のコメントに従って修正してください。また後者の場合は `ldap.properties` の `idp.authn.LDAP.sslConfig` が `certificateTrust` もしくはコメントアウトされていることを確認してください。他の設定では意図した動作をしません。

LDAPコネクタが有効化されていない場合は有効化してください。

```

<!--Example LDAP Connector -->
<!--
  Add the following configuration below the </dc:FilterTemplate> line
  in order to reduce the LDAP attributes to be retrieved using
  idp.attribute.resolver.LDAP.returnAttributes in conf/ldap.properties:

  <dc:ReturnAttributes>{%idp.attribute.resolver.LDAP.returnAttributes}</dc:ReturnAttributes>
-->
<!--
  Add the following configuration above the </resolver:DataConnector>
  line in order to use StartTLS
  (i.e. idp.attribute.resolver.LDAP.useStartTLS in conf/ldap.properties
  is true):

  <dc:StartTLSTrustCredential id="LDAPtoIdPCredential" xsi:type="sec:X509ResourceBacked">
    <sec:Certificate>{%idp.attribute.resolver.LDAP.trustCertificates}</sec:Certificate>
  </dc:StartTLSTrustCredential>
-->
<!-- --> ← コメント終了を追加して、以下を有効とします
<resolver:DataConnector id="myLDAP" xsi:type="dc:LDAPDirectory"
  ldapURL="{idp.attribute.resolver.LDAP.ldapURL}"
  baseDN="{idp.attribute.resolver.LDAP.baseDN}"
  principal="{idp.attribute.resolver.LDAP.bindDN}"
  principalCredential="{idp.attribute.resolver.LDAP.bindDNCredential}"
  useStartTLS="{idp.attribute.resolver.LDAP.useStartTLS:true}">
  <dc:FilterTemplate>
    <![CDATA[
      {%idp.attribute.resolver.LDAP.searchFilter}
    ]]>
  </dc:FilterTemplate>
</resolver:DataConnector>
<!-- --> ← コメント開始を追加して、上記を有効とします

```

※ attribute-resolver.xmlに記述する内容に '&' や '<' を含む場合は '&amp;' や '&lt;,' のように記述してください。逆にldap.propertiesに記述する場合はそのまま記述してください。

→ [meatwiki:GakuNinShare:トラブルシューティング](#)

ComputedIdやStoredIdのコネクタも同様ですが、sourceAttributeやsaltは saml-nameid.properties ファイルを参照するようになっていますので、そちらで設定してください。また、直上の {%idp.persistentId.sourceAttribute} という疑似属性定義も有効化することを忘れないでください。その他詳細はテンプレートファイル中のコメントをご参照ください。