旧: Active DirectoryにおけるeduPersonスキーマ（拡張スキーマ）の利用（成城大学提供）

Active DirectoryにおけるeduPersonスキーマの利用（成城大学提供）

[検証内容]

Shibboleth IdP で Windows Server 2003 R2 の Active Directory を直接データソースとして利用する際の設定方法を検証する．尚，ここでは UPKI イニシアティブ学術認証フェデレーションで公開されている技術ガイド（以下「技術ガイド」という）を基に，Active Directory 用の設定部分のみに言及し，他の設定については省略する．

---

1. UPKI フェデレーションで利用するスキーマの導入

Active Directory 用 eduPerson スキーマを以下の URL からダウンロードする．
https://spaces.internet2.edu/display/macedir/Active+Directory+eduPerson
コマンドプロンプトで，ldifde.exe を実行してスキーマを拡張する．log を c:\tmp に出力して，ssotest.seijo.ac.jp ドメインに対してスキーマ拡張するにはパラメータを以下のように与える．

```
ldifde -i -f eduPerson.adschema.ldif -j c:¥tmp¥log.txt -c "DC=X" "DC=ssotest,DC=seijooo,DC=ac,DC=jp"
```

その後，MMC の Active Directory スキーマ スナップインで追加した属性を選択してプロパティを開き，[グローバル カタログにこの属性をレプリケートする] にチェックを入れる．
＊この設定をしないとグローバルカタログに問い合わせた際に属性値が参照できなくなる．詳細については後述する．

---

2. テストデータの作成

PowerShell を使ってユーザー作成時に拡張属性に値を設定する．以下のスクリプトでは eduPersonAffiliation 属性の値を staff に設定している．

```
$strOU = "ou=mnc,dc=ssotest,dc=seijooo,dc=ac,dc=jp"
$prinStr = "@ssotest.seijo.ac.jp"

$Password = Read-Host "Password" -asSecureString
$oOU = [ADSI]"LDAP://$strOU"

$name = "zazu"
$kname = "座図"
$cnx = "cn=" + $name
$snx = "sn=" + $kname

$oUser = $oOU.Create("user", $cnx)
$oUser.Put("sAMAccountName", $name)
$oUser.Put("userPrincipalName", $name+$prinStr)
$oUser.Put("sn", $kname)
$oUser.setInfo()

$oUser.SetPassword($Password.ToString())
$oUser.Put("userAccountControl","66176")
$oUser.Put("eduPersonAffiliation","staff")  # ← eduPersonAffiliation 値の追加
$oUser.setInfo()
```

---

3. login.config ファイルの編集

https://wiki.shibboleth.net/confluence/display/SHIB2/IdPADConfigIssues に Active Directory 設定時の注意点が解説されており，Port 3268 を使ってグローバルカタログへ接続すると Referral 問題を回避できる．以下はグローバルカタログを持つホスト mncssotad.seijooo.ac.jp に ldapadm ユーザーで接続するサンプル設定である．Active Directory の場合 userField は sAMAccoutName を使用する．

```
ShibUserPassAuth {
   edu.vt.middleware.ldap.jaas.LdapLoginModule required
      host="mncssotad.seijooo.ac.jp"
      port="3268"
      base="dc=ssotest,dc=seijooo,dc=ac,dc=jp"
      ssl="false"
      userField="sAMAccountName"
      serviceUser="ldapadm@ssotest.seijo.ac.jp"
      serviceCredential="ldapadm のパスワード"
      subtreeSearch="true";
};
```

---

4. attribute-resolver.xml ファイルの編集

eduPersonPrincipalName を有効にする場合は，sourceAttributeID にsAMAccountNameを指定する．

```
  <!-- Attribute Definition for eduPersonPrincipalName -->
    <resolver:AttributeDefinition id="eduPersonPrincipalName" xsi:type="Scoped" xmlns="urn:mace:shibboleth:2.0:resolver:ad"
        scope="seijo.ac.jp" sourceAttributeID="sAMAccountName">
        <resolver:Dependency ref="myLDAP" />
        <resolver:AttributeEncoder xsi:type="SAML1ScopedString" xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
            name="urn:mace:dir:attribute-def:eduPersonPrincipalName" />
        <resolver:AttributeEncoder xsi:type="SAML2ScopedString" xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
            name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" friendlyName="eduPersonPrincipalName" />
    </resolver:AttributeDefinition>
```

eduPersonAffiliation を有効にする場合は，コメント記述子を外すだけでよい．

```
   <!-- Attribute Definition for eduPersonAffiliation -->
    <resolver:AttributeDefinition id="eduPersonAffiliation" xsi:type="Simple" xmlns="urn:mace:shibboleth:2.0:resolver:ad"
        sourceAttributeID="eduPersonAffiliation">
        <resolver:Dependency ref="myLDAP" />
        <resolver:AttributeEncoder xsi:type="SAML1String" xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
            name="urn:mace:dir:attribute-def:eduPersonAffiliation" />
        <resolver:AttributeEncoder xsi:type="SAML2String" xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
            name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1" friendlyName="eduPersonAffiliation" />
    </resolver:AttributeDefinition>
```

LDAP Connector を Port 3268 で設定する．FilterTemplate タグ中でもsAMAccountName を指定する．

```
    <resolver:DataConnector id="myLDAP" xsi:type="LDAPDirectory" xmlns="urn:mace:shibboleth:2.0:resolver:dc"
        ldapURL="ldap://mncssotad.seijooo.ac.jp:3268"
        baseDN="dc=ssotest,dc=seijo,dc=ac,dc=jp"
        principal="ldapadm@ssotest.seijooo.ac.jp"
        principalCredential="ldapadm のパスワード">
        <FilterTemplate>
            <![CDATA[
                (sAMAccountName=$requestContext.principalName)
            ]]>
        </FilterTemplate>
    </resolver:DataConnector>
```

その他 Shibboleth Idp の設定については技術ガイドの通り行う．

---

5. 接続テスト

https://test-sp00.gakunin.nii.ac.jp/ に接続し，eduPersonAffiliation 属性が表示されていることが確認できる．

6.その他

LDAP Connector が取得した値を確認するには，logging.xml で，以下のようにLog Level を DEBUG に変更し，idp-proccess.log を参照する．

```
    <logger name="edu.internet2.middleware.shibboleth">
        <level value="DEBUG" />
    </logger>
```

グローバルカタログに eduPerson スキーマをレプリケートするよう設定してあれば，idp-proccess.log で以下のように結果が表示される．

```
18:59:48.397 - DEBUG [edu.vt.middleware.ldap.Ldap:566] - Search with the following parameters:
18:59:48.397 - DEBUG [edu.vt.middleware.ldap.Ldap:567] -   dn = dc=ssotest,dc=seijooo,dc=ac,dc=jp
18:59:48.397 - DEBUG [edu.vt.middleware.ldap.Ldap:568] -   filter = (sAMAccountName=zazu)
18:59:48.399 - DEBUG [edu.vt.middleware.ldap.Ldap:569] -   filterArgs =
18:59:48.399 - DEBUG [edu.vt.middleware.ldap.Ldap:571] -     none
18:59:48.400 - DEBUG [edu.vt.middleware.ldap.Ldap:575] -   retAttrs =
18:59:48.400 - DEBUG [edu.vt.middleware.ldap.Ldap:577] -     all attributes
18:59:48.400 - TRACE [edu.vt.middleware.ldap.Ldap:582] -   config = {java.naming.provider.url=ldap://mncssotad.seijooo.ac.jp:3268,
java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory}
18:59:48.403 - DEBUG [edu.internet2.middleware.shibboleth.common.attribute.resolver.provider.dataConnector.LdapDataConnector:882] -
Found the following attribute: uSNChanged=[33134]
18:59:48.403 - DEBUG [edu.internet2.middleware.shibboleth.common.attribute.resolver.provider.dataConnector.LdapDataConnector:882] -
Found the following attribute: eduPersonAffiliation=[staff]
```