旧: 属性管理（登録、変換、リリース方法）

属性管理（登録、変換、リリース方法）

Shibboleth（シボレス）には、基本的には多くの属性をLDAPやDBから取得してリリースするための設定が既に入っており、これらのコメントアウトを解除して有効化するだけで実行することができます。
また、属性の変換機能として、”@nii.ac.jp”といったスコープの付与、値の変換、固定値の割り当てや、スクリプトを利用した変換等が可能です。
さらに、リリース制御では、サイトとしてのポリシー、各個人のポリシーによる制御や、各SPに対応したリリース制御等が可能です。

以下では、新たなIDや属性の追加、そのリリースの方法について説明します。

IDの追加方法

以下の利用者をLDAPへ登録する例を示します。

uid	userPassword	ou	eduPersonAffiliation
test004	test004	technology	student

1. ldifファイル(sample1.ldif)の作成

```
dn: ou=technology,o=test_o,dc=ac,c=JP
objectClass: organizationalUnit
ou: technology


# test004, technology, test_o, ac, JP
dn: uid=test004,ou=technology,o=test_o,dc=ac,c=JP
objectClass: eduPerson
objectClass: inetOrgPerson
ou: technology
sn: test_sn_4
cn: test_cn_4
uid: test004
userPassword: test004
eduPersonAffiliation: student
```

2. 上記1のldifファイルを用いた登録

```
# ldapadd -x -h localhost -D ”cn=olmgr,o=test_o,dc=ac,c=JP” -w csildap -f sample1.ldif
```

属性の追加方法

利用者に「displayName」属性を追加する例を示します。

1. ldifファイル(sample2.ldif)の作成

```
dn: uid=test004,ou=technology,o=test_o,dc=ac,c=JP
changetype: modify
add: displayName
displayName: Test4
```

2. 上記1のldifファイルを用いた登録

```
# ldapmodify -x -h localhost -D "cn=olmgr,o=test_o,dc=ac,c=JP" -w csildap -f sample2.ldif
```

属性のリリース方法

先に追加した「displayName」属性をSPへリリースする例を示します。

1. スキーマの確認

・/etc/openldap/schema配下にスキーマファイルがあります。
・「displayName」属性は、/etc/openldap/schema/inetorgperson.schemaにて以下のように定義されています。赤字で示されている部分がdisplayName の oid です。

```
 (中略)
# displayName
# When displaying an entry, especially within a one-line summary list, it
# is useful to be able to identify a name to be used.  Since other attri-
# bute types such as 'cn' are multivalued, an additional attribute type is
# needed.  Display name is defined for this purpose.
attributetype ( 2.16.840.1.113730.3.1.241
        NAME 'displayName'
        DESC 'RFC2798: preferred name to be used when displaying entries'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        SINGLE-VALUE )
 (中略)
```

2. /opt/shibboleth-idp/conf/attribute-resolver.xmlへの登録

```
<AttributeResolver
        xmlns="urn:mace:shibboleth:2.0:resolver"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:mace:shibboleth:2.0:resolver http://shibboleth.net/schema/idp/shibboleth-attribute-resolver.xsd">

 (中略)

    <AttributeDefinition xsi:type="Simple" id="displayName">
        <InputDataConnector ref="myLDAP" attributeNames="displayName"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:displayName" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.16.840.1.113730.3.1.241" friendlyName="displayName" encodeType="
false" />
    </AttributeDefinition>  ←"displayName" の AttributeDefinition を追加（SAML2Stringのnameでは1.で確認したoidを指定）

 (中略)

</AttributeResolver>
```

※ 途中のSAML1Stringについては、URNとして登録されていない属性の場合はこの行自体を削除してください。

3. /opt/shibboleth-idp/conf/attribute-filter.xmlへの登録

```
<AttributeFilterPolicyGroup id="..."
        xmlns="urn:mace:shibboleth:2.0:afp"

 (中略)

    <AttributeFilterPolicy id="...">
 (中略)

        <AttributeRule attributeID="displayName" permitAny="true" />

            ↑ "displayName" の AttributeRule を追加
 (中略)
    </AttributeFilterPolicy>
 (中略)
 </AttributeFilterPolicyGroup>
```