IdP-アプリケーション間で受け渡す属性の追加方法

IdP-アプリケーション間で受け渡す属性の追加方法

/etc/shibboleth/attribute-map.xml内に、該当する属性があるか確認してください。ほとんどの属性が attribute-map.xmlにて定義されています。ただし、Shibboleth SPをインストールした直後の当該ファイルは一部の属性を除いてコメントアウトされていますので注意してください。attribute-map.xmlで定義されていてかつ有効な属性は、IdPがリリースすると、そのままアプリケーションに渡されます。

> 学認では、学認が規定する属性をコメントアウト解除・追加したattribute-map.xmlのテンプレートを提供しています。学認に参加するSPを構築する場合はまずはこちらをお使いください。⇒技術ガイド#テンプレート

attribute-map.xmlで定義されていない場合については、以下に「displayName」属性をマッピングする例で示します。

1. スキーマの確認

・LDAPサーバ上の/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。

```
 (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. /etc/shibboleth/attribute-map.xmlへの登録

```
<Attributes xmlns="urn:mace:shibboleth:2.0:attribute-map"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 (中略)
<Attribute name="urn:mace:dir:attribute-def:displayName" id="displayName"/>
<Attribute name="urn:oid:2.16.840.1.113730.3.1.241" id="displayName"/> ←1のoid
 (中略)
</Attributes>
```