IdP設定マニュアル

ユーザーがGakuNin RDMを利用するには、貴機関が運用するShibboleth IdPにおいて、ユーザーの属性値をGakuNin RDMのSPへ送出するための設定が必要となります。

前提条件

- IdPが学認（運用フェデレーション）に登録済みであることが必要です。運用フェデレーションへの参加登録が完了していない場合は別途ご相談ください。
- このドキュメントはIdPが学認技術ガイドに記載された手順で構築されていることを想定しています。IdPが貴機関固有の方法でインストールされている場合はファイルパス等を適宜読み替えてください。

概要

GakuNin RDMは次の3つのSPで構成されています。

- 基本機能 … 利用必須です。
- 管理機能 … 任意で利用できます。機関管理者が利用統計情報を参照したり、ユーザーに提供するGRDMの機能を制限したりする機能です。
- データ解析機能 … 任意で利用できます。ユーザーがNIIの計算機にJupyterHubの実行環境を構築する機能です。この機能は試行運用中です。

各SPのentityIDは次のとおりです。

entityID	機能
https://accounts.rdm.nii.ac.jp/shibboleth-sp	GakuNin RDM 基本機能
https://admin.rdm.nii.ac.jp/shibboleth-sp	GakuNin RDM 管理機能
https://jupyter.cs.rcos.nii.ac.jp/shibboleth-sp	GakuNin RDM データ解析機能

貴機関で利用する機能に応じて、各SPに必要な属性を送出してください。

属性	基本機能	管理機能	データ解析機能
eduPersonPrincipalName	**必須**	**必須**	**必須**
eduPersonEntitlement	任意	**必須** *1	任意
mail	任意	任意	**必須** *2
displayName	任意	任意	任意
organizationName	任意	任意	任意
organizationalUnitName	任意	任意	任意

*1: 属性値の中に「GakuNinRDMAdmin」を含めてください（後述）。

*2: 不正利用への対応に備えて必須としています。

管理機能を利用する場合

管理機能にアクセスできるユーザーは、eduPersonEntitlement属性値の中に「GakuNinRDMAdmin」という文字列が含まれるようにしてください。

このドキュメントは次の方法を想定しています。これ以外の方法を用いる場合は、後述のattribute-resolverの設定内容を適切に読み替えてください。

- ユーザー情報がLDAPで管理されている。
- ユーザーのレコードがeduPersonEntitlement属性を持つ。
- 管理機能にアクセスできるユーザーに限り、eduPersonEntitlement属性値が「GakuNinRDMAdmin」に設定されている。

なお、学認技術ガイドでは、LDAPの設定においてeduPersonPrincipalName属性 (ePPN) とeduPersonEntitlement属性を含むeduPersonスキーマの導入は必須とされていませんのでご注意ください。→ 参考: OpenLDAPの設定

設定手順

以下の手順でShibboleth IdPの設定を行います。詳細は学認技術ガイドを参照してください。

メタデータの更新

メタデータの自動更新が有効になっていない場合、以下の手順でメタデータのキャッシュファイルを更新します。

1. キャッシュファイルを見つけます。
    - キャッシュファイルのパスは、 /opt/shibboleth-idp/conf/metadata-providers.xml ファイルの中の MetadataProvider 要素の backingFile 属性で指定されています。
    - 学認技術ガイドの既定値は /opt/shibboleth-idp/metadata/gakunin-metadata-backing.xml となっています。
2. キャッシュファイルを開き、「https://jupyter.cs.rcos.nii.ac.jp/shibboleth-sp」という文字列を検索します。
3. 見つからない場合、 https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml から最新のメタデータを取得し、キャッシュファイルを置き換えます。

attribute-resolverの設定

attribute-resolver.xml ファイルの変更を参考に、以下の設定を行います。

1. /opt/shibboleth-idp/conf/attribute-resolver.xml を開きます。
2. 「id="eduPersonPrincipalName"」という文字列を検索し、次のXML要素が有効である（コメントアウトされていない）ことを確認します。→ 参考: eduPersonPrincipalName

```
<resolver:AttributeDefinition xsi:type="ad:Scoped" id="eduPersonPrincipalName" scope="%{idp.scope}" sourceAttributeID="uid">
    <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>
```

3. データ解析機能を利用する場合、「id="mail"」という文字列を検索し、次のXML要素が有効であることを確認します。→ 参考: mail

```
<resolver:AttributeDefinition xsi:type="ad:Simple" id="mail" sourceAttributeID="mail">
    <resolver:Dependency ref="myLDAP" />
    <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-def:mail" encodeType="false" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:0.9.2342.19200300.100.1.3" friendlyName="mail"
encodeType="false" />
</resolver:AttributeDefinition>
```

4. 管理機能を利用する場合、「id="eduPersonEntitlement"」という文字列を検索し、次のXML要素が無効である（コメントアウトされている）ことを確認します。※

```
<!--
<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>
-->
```

この直後に次の内容を追記します。→ 参考: eduPersonEntitlement

```
<resolver:AttributeDefinition xsi:type="ad:Simple" id="eduPersonEntitlement" sourceAttributeID="eduPersonEntitlement">
    <resolver:Dependency ref="myLDAP" />
    <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>
```

もし、※の時点で見つかったXML要素が有効である（コメントアウトされていない）場合は、別のサービスに対してeduPersonEntitlement属性を送出するよう設定されている可能性があります。別途NII担当者にご相談ください。

attribute-filterの設定

attribute-filter.xml ファイルの変更を参考に、以下の設定を行います。

1. /opt/shibboleth-idp/conf/attribute-filter.xml を開き、「</AttributeFilterPolicyGroup>」という文字列を検索します。
2. 見つかったタグの直前に次のXML要素を追加します。

```
<AttributeFilterPolicy id="PolicyforGakuNinRDM">
    <PolicyRequirementRule xsi:type="Requester" value="https://accounts.rdm.nii.ac.jp/shibboleth-sp" />
    <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
</AttributeFilterPolicy>
```

3. データ解析機能を利用する場合、次のXML要素も追加します。

```
<AttributeFilterPolicy id="PolicyforGakuNinFCS">
    <PolicyRequirementRule xsi:type="Requester" value="https://jupyter.cs.rcos.nii.ac.jp/shibboleth-sp" />
    <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="mail">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
</AttributeFilterPolicy>
```

4. 管理機能を利用する場合、次のXML要素も追加します。

```
<AttributeFilterPolicy id="PolicyforGakuNinRDMAdmin">
    <PolicyRequirementRule xsi:type="Requester" value="https://admin.rdm.nii.ac.jp/shibboleth-sp" />
    <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonEntitlement">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
</AttributeFilterPolicy>
```

設定完了

1. Shibboleth IdP サービスを再起動します。
2. 再起動が完了したら、**NII担当者 <rdm_support@nii.ac.jp> にメールでお知らせください。**
3. NII側でembeddedDSの設定を行います。NII担当者からの連絡をお待ち下さい。

動作確認

1. https://rdm.nii.ac.jp/ にアクセスします。画面右上のプルダウンメニューから機関名を選択し、ログインできることを確認します。
2. データ解析機能を利用する場合、https://jupyter.cs.rcos.nii.ac.jp/ にアクセスします。画面中央のプルダウンメニューから機関名を選択し、ログインできることを確認します。
3. 管理機能を利用する場合、https://admin.rdm.nii.ac.jp/ にアクセスします。画面中央のプルダウンメニューから機関名を選択し、ログインできることを確認します。
4. 確認できましたら、NII担当者 <rdm_support@nii.ac.jp> にメールでお知らせください。