GakuNin RDM 接続用IdP設定マニュアル

利用申請機関が管理するShibboleth IdP(以下IdP)を利用してGakuNin RDM(以下GRDM)にログインをおこなう際に必要な設定について記述しています。
IdPは学認技術ガイド(https://www.gakunin.jp/technical/)に記載の手順で構築されていることを想定しています。固有の方法でインストールされている場合はファイルのパス等を適宜読み替えてください。

設定に必要な情報のまとめ

GRDMのshibboleth SPのentityID

- https://accounts.rdm.nii.ac.jp/shibboleth-sp
    - 通常のサービスの利用
- https://admin.rdm.nii.ac.jp/shibboleth-sp
    - 管理画面(後述)の利用

GRDMのSPに対してIdPから送出していただく属性値

- **eduPersonPrincpalName(ePPN)**
    - （必須）ユーザーの識別子として利用します。
- **eduPersonEntitlement**
    - （任意）管理画面を利用する際には必須
    - 管理機能の設定で「GakuNinRDMAdmin」をeduPersonEntitlement属性に記述してください。

以下の属性値は今後のGRDMの機能拡張において参照する可能性があります。

- **displayName**
    - （任意）
- **mail**
    - （任意）
- **organizationName**
    - （任意）
- **organizationalUnitName**
    - （任意）

上記について確認し、設定に問題なければご連絡ください。

弊所側で必要な設定を行ない、疎通が可能になり次第ご連絡を差し上げます。

GRDMのサービスを利用する際のIdPへの設定内容

GRDMのメタデータ取り込み

2019/02/22 現在公開されている学認運用フェデレーションのメタデータはGRDMのメタデータを含んでいます。
学認技術ガイドのIdPカスタマイズ設定に従いメタデータの自動更新が有効になるよう設定されている場合は特別な設定は必要ありません。
自動更新が有効になっていない場合はローカルのキャッシュファイルの確認が必要です。

ローカルのキャッシュファイルは通常
/opt/shibboleth-idp/metadata/gakuni-metadata.xml
として保存されています。

このファイルの中にhttps://accounts.rdm.nii.ac.jp/shibboleth-sp の文字列が含まれているかを確認してください。
含まれていれば問題ありません。無い場合はファイルの更新が必要です。

https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml
最新の学認運用フェデレーションのメタデータは上記URLから取得可能です。

属性送出の設定

GRDMのサービスを利用するためにはhttps://accounts.rdm.nii.ac.jp/shibboleth-sp のentityIDに対してeduPersonPrincipalName (ePPN)が送出されている必要があります。

/opt/shibboleth-idp/conf/attribute-resolver.xml の設定

ePPNの定義が有効であることを確認してください。

‘id=”eduPersonPrincipalName”’ の文字列を検索します。
学認技術ガイドの手順どおりの構築であれば以下のような記述が見付かるはずです。

```
<!-- Attribute Definition for 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>
<!-- -->
```

resolver:AttributeDefinitionのタグがコメント解除されていれば問題ありません。
(参考) 学認技術ガイド「attribute-resolver.xml ファイルの変更（IdPv3）」https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=20021642

/opt/shibboleth-idp/conf/attribute-filter.xmlの設定

ファイル末尾の</AttributeFilterPolicyGroup>タグの直前に以下の内容を追加してください。

```
<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>
```

設定を反映するためにIdPのサービスを再起動してください。
弊所での処理が完了しましたら、GRDMトップページhttps://rdm.nii.ac.jp/ 画面右肩のEmbedded DSのプルダウンメニューに機関名が表示されるようになります。
こちらからログインが可能であるかの確認をいただけるようお願いします。

管理画面のサービスを利用する際のIdPへの設定内容

GRDMでは利用機関のネットワーク管理者が、機関のユーザーに対して利用可能なGRDMの機能に対し一部制限をおこなう、また利用統計情報を参照する等の機能を利用するための管理画面を用意しています。
こちらを利用になるためには通常のサービスとは別に設定をいただく必要があります。

GRDMのメタデータ取り込み

2019/02/22 現在公開されている学認運用フェデレーションのメタデータはGRDMのメタデータを含んでいます。
学認技術ガイドのIdPカスタマイズ設定に従いメタデータの自動更新が有効になるよう設定されている場合は特別な設定は必要ありません。
自動更新が有効になっていない場合はローカルのキャッシュファイルの確認が必要です。

ローカルのキャッシュファイルは通常
/opt/shibboleth-idp/metadata/gakuni-metadata.xml
として保存されています。

このファイルの中にhttps://accounts.rdm.nii.ac.jp/shibboleth-sp の文字列が含まれているかを確認してください。
含まれていれば問題ありません。無い場合はファイルの更新が必要です。

https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml
から取得できる最新の学認運用フェデレーションのメタデータを利用してください。

属性送出の設定

管理画面のサービスを利用するためにはhttps://admin.rdm.nii.ac.jp/shibboleth-sp のentityIDに対してeduPersonPrincipalName (ePPN)とeduPersonEntitlementが送出されている必要があります。
管理画面にアクセスが可能なユーザーのeduPersonEntitlement属性はその値の中に**GakuNinRDMAdmin**の文字列を含む必要があります。
管理画面にアクセスを許可するユーザーにのみこの値が付与されるようにしてください。

以下の例ではユーザー情報を収めたLDAP上の当該ユーザーのレコードがeduPersonEntitlement属性を持っており、管理画面にアクセス可能なユーザーに対してはGakuNinRDMAdminの値が設定されていることを期待しています。
eduPersonEntitlement属性はedupersonスキーマに含まれます。学認技術ガイドでは導入は選択となっておりますのでご注意ください。

(参考) https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=20021639
eduPersonEntitlementの算出に別の方法を用いられる場合はattribute-resolver.xmlの設定を適切に変更してください。

/opt/shibboleth-idp/conf/attribute-resolver.xml の設定

ePPNが有効であることを確認してください。

‘id=”eduPersonPrincipalName”’ の文字列を検索します。

学認技術ガイドの手順どおりの構築であれば以下のような記述が見付かるはずです。

```
<!-- Attribute Definition for 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>
<!-- -->
```

resolver:AttributeDefinitionのタグがコメント解除されていれば問題ありません。

eduPersonEntitlementの設定を追加します。

‘id="eduPersonEntitlement"’ の文字列を検索します。
学認技術ガイドの手順どおりの構築であれば以下のような記述が見付かるはずです。

```
<!-- Attribute Definition for eduPersonEntitlement -->
<!--
<AttributeDefinition xsi:type="Simple" id="eduPersonEntitlement" sourceAttributeID="eduPersonEntitlement">
    <Dependency ref="staticEntitlementCommonLibTerms" />
    <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:eduPersonEntitlement" encodeType="false" />
    <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" friendlyName="eduPersonEntitlement" encodeType="
false" />
</AttributeDefinition>
-->
```

AttributeDefinitionのタグがコメントアウトされている事を確認してください。

コメントアウトされていない場合は現在別のサービスに対するeduPersonEntitlement属性の送出設定がされている可能性があります。この手順書の範疇を超えると思われますので別途ご相談ください。
上記の引用箇所の直後に以下の内容を追記してください。

```
<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>
```

(参考) 学認技術ガイド「attribute-resolver.xml ファイルの変更（IdPv3）」https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=20021642

/opt/shibboleth-idp/conf/attribute-filter.xmlの設定

ファイル末尾の</AttributeFilterPolicyGroup>タグの直前に以下の内容を追加してください。

```
<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>
```

設定を反映するためにIdPのサービスを再起動してください。

再起動が完了しましたらご連絡ください。

弊所での処理が完了しましたら、GRDM管理画面ページhttps://admin.rdm.nii.ac.jp 画面中央のembeddedDSのプルダウンメニューに機関名が表示されるようになります。

こちらからログインが可能であるかの確認をいただけるようお願いします。ログインが確認できましたらその旨をメールにてお知らせください。