学認クラウドゲートウェイサービス連携のための情報

IdP管理者に必要な情報

学認参加IdPが学認クラウドゲートウェイサービスを利用するために必要な情報をまとめます。

まず、学認クラウドゲートウェイサービス (entityID: `https://cg.gakunin.jp/shibboleth-sp`) に対して以下の属性を送信するようにしてください。

ePPN (eduPersonPrincipalName)	必須
~~eduPersonTargetedID~~	~~任意~~
jao	任意
o	任意
jaDisplayName	任意
displayName	任意
mail	任意
~~eduPersonAffiliation~~	~~任意~~

~~eduPersonTargetedID~~/eduPersonAffiliationを除いた各任意属性は、学認クラウドゲートウェイサービス上でのアカウント登録時にユーザ情報を初期入力するために使用されます。ユーザ情報の「所属」は日本語および英語がそれぞれjaoおよびoに対応します。ユーザ情報の「氏名」は日本語および英語がjaDisplayNameおよびdisplayNameに対応します。

~~eduPersonAffiliationは、faculty/staffであれば当該利用者が管理者となっているグループのメンバーに対する招待なし入会・属性送信同意のオプションが加わります。詳しくはお問い合わせください。~~（現在無効化されています。「お知らせ一覧#2019/08/27掲載」をご参照ください）

学認クラウドゲートウェイサービスへの属性送信の設定例は以下を参照してください。設定例となっていますので、所属機関IdPで送信可能な属性への変更してご利用ください。

```
<!-- Policy for GakuNin Cloud Gateway Service -->
<AttributeFilterPolicy id="PolicyforGakuNinCloudGatewayService">

    <PolicyRequirementRule xsi:type="Requester" value="https://cg.gakunin.jp/shibboleth-sp" />

    <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>

    <AttributeRule attributeID="jaOrganizationName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>

    <AttributeRule attributeID="organizationName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>

    <AttributeRule attributeID="jaDisplayName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>

    <AttributeRule attributeID="displayName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>

    <AttributeRule attributeID="mail">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>

</AttributeFilterPolicy>
```

そして、学認クラウドゲートウェイサービスと連携しているサービス(SP)に対しても、必要な属性を送信していないとIdPの利用者は当該サービスが利用できませんのでご注意ください。

API

連携するIdPが利用できる、ゲートウェイトップ画面で表示される利用可能サービスの情報を取得するためのAPIを以下に示します。
⇒API(IdP)

SP管理者に必要な情報

SP管理者が提供しているサービスを学認クラウドゲートウェイサービスと連携させるためには以下の手順に従って設定を行ってください。

⚠ 以下の手順でisMemberOf属性を取得するためにはあらかじめIdPからeduPersonPrincipalName(ePPN)を取得していなければなりません。

- グループメンバー情報を取得できるようにする
  以下のようにShibboleth SPの設定ファイルを変更してください。動作確認は Shibboleth SP 2.6 で行っています。
  a. 学認クラウドゲートウェイサービス (IdP)のメタデータを次のリンクから取得して /etc/shibboleth/metadata/ に保存してください。
     cgidp-metadata.xml

     2017年2月22日以前に設定されたかたは、アクセス先が変わっておりますので、最新のメタデータを用いてください。

     以前、Gakunin mAP連携のためにshibboleth2.xmlに以下の1行を追加している場合は **削除** してください。

```
    <ProtocolProvider type="XML" validate="true" reloadChanges="false" path="protocols.xml"/>

    <TransportOption provider="CURL" option="81">0</TransportOption>
</SPConfig>
```

     なお、メタデータ取得時のサーバ証明書検証（初期値ではいずれにしろ不完全です）については以下でご案内しておりますので、もし設定がまだのようであれば別途ご検討いただければと思います。
     shibboleth2.xml ファイル　の<TransportOption>の3行

b. **shibboleth2.xmlの編集**
/etc/shibboleth/shibboleth2.xml を編集します。

- 学認クラウドゲートウェイサービス (IdP)メタデータの読み込み
  a.でダウンロードしたメタデータを読み込むように設定します。他の<MetadataProvider>の後に下記を追加してください。

```
<MetadataProvider type="XML" file="/etc/shibboleth/metadata/cgidp-metadata.xml"/>
```

- SimpleAggregationの追加
  通常の認証フローの後にeppnを手がかりとして学認クラウドゲートウェイサービス (IdP)からisMemberOf属性を取得するよう、SimpleAggregation設定を行います。
  既存の<AttributeResolver>の後に以下の記述を追加します。

```
<AttributeResolver type="SimpleAggregation" attributeId="eppn" format="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">
    <Entity>https://cg.gakunin.jp/idp/shibboleth</Entity>
    <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:
1.3.6.1.4.1.5923.1.5.1.1" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="
isMemberOf"/>
</AttributeResolver>
```

c. **attribute-map.xmlの編集**
/etc/shibboleth/attribute-map.xmlにてisMemberOf属性の設定を確認します。
以下の記述がない場合、最終行の</Attributes>の直前に追加してください。

```
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.5.1.1" id="isMemberOf"/>
```

d. **attribute-policy.xmlの編集**
他のIdPからのisMemberOf属性を拒否し、学認クラウドゲートウェイサービスからのisMemberOfのみを利用する設定を行ないます。

> *<!-- Catch-all that pases everything else through unmolested. -->*

の直前に以下の記述を追加してください。

```
<afp:AttributeRule attributeID="isMemberOf">
    <afp:PermitValueRule xsi:type="AttributeIssuerString"
        value="https://cg.gakunin.jp/idp/shibboleth"/>
</afp:AttributeRule>
```

.

- 取得したisMemberOf属性を利用するようにサービスを変更する
  例えば、isMemberOf属性には下記のような値が入ります。全てURI形式です。

> *https://cg.gakunin.jp/sp/SPCID　←　SPコネクタ名*
> *https://cg.gakunin.jp/gr/GROUPID　←　ユーザが参加しているグループ名*
> *https://cg.gakunin.jp/gr/GROUPID/admin　←　ユーザが当該グループの管理者の場合*

後者2つは、SPコネクタの設定で「グループ情報も取得する」を選択した場合のみ取得できます。

取得したisMemberOf属性のホスト部をチェックしているプラグインを使用している等で属性値が https://map.gakunin.nii.ac.jp/gr/... でないと支障がある場合は、shibboleth2.xmlに以下2箇所を追加してください。

a. 既存の<ApplicationDefaults> より前に記述を追加。

```
<OutOfProcess>
    <Extensions>
        <Library path="plugins.so" fatal="true"/>
    </Extensions>
</OutOfProcess>
```

b. 既存の<AttributeResolver> の後に記述を追加。

```
<AttributeResolver type="Transform" source="isMemberOf">
    <Regex match="^https://cg.gakunin.jp/gr/(.+)$">https://map.gakunin.nii.ac.jp/gr/$1</Regex>
</AttributeResolver>
```

- SPに対応するSPコネクタを作成する

本項目の操作には適切に権限が付与されている必要があります。権限付与を希望する学認参加SPの運用担当者の方は学認クラウドゲートウェイサービスのページ下にある「問い合わせ先」（要ログイン）からサービスサポートまでご連絡ください。

グループの接続先となるSPコネクタを作成します。グループが当該SPコネクタに接続した場合のみSPはそのグループに関する情報を取得できます。SPコネクタ作成の詳細は、mAP利用マニュアルの「SPコネクタを作成する」の章をご参照ください。

.

API

連携するSPが利用できる、利用者のグループ情報等を取得するためのAPIを以下に示します。
⇒API

SP連携のトラブルシューティング

1. isMemberOf属性が取得できない

以下2つの条件を満たす場合にはisMemberOf属性が取得できません。

- SP側の設定ファイルshibboleth2.xmlのApplicationDefaultsに *encryption="true"* と指定されている
- ダウンロードしたメタデータcgidp-metadata.xmlの *KeyDescriptor use="signing"*（2か所）が設定されている （以前配布していたメタデータには *use="signing"* を設定していました）

上記でisMemberOf属性が取得できない原因はAttributeQueryのNameIDが暗号化されているためによるものですが、NameIDを暗号化したままisMemberOf属性を取得するためには、最新のメタデータcgidp-metadata.xmlをダウンロードし直すか（最新のメタデータでは *use="signing"* を削除済み）、以前ダウンロードしたメタデータの use="signing"（2か所）を削除してください。