

API

現在連携SPが学認クラウドゲートウェイサービスで利用できるAPIは3種類あります。前二者はOpenSocialおよびVOOT 1.0をベースとしたフォーマットでレスポンスはJSON形式です。最後のものは呼び出しが逆向きです。

- [People API](#)
グループを指定してそのメンバーに関する情報を取得するためのAPI
- [Groups API](#)
SPコネクタに接続しているグループに関する情報を取得するためのAPI
- [New Group API](#)
新たなグループから接続があった場合に学認クラウドゲートウェイサービスから呼び出されるSPのAPI

いずれも、認証は学認におけるSPメタデータに記載されている証明書を用いたTLSクライアント証明書認証により行います。証明書の extended Key Usage (eKU) に clientAuth が記載されていなければなりません。
また、学認クラウドゲートウェイサービスが提示する証明書も学認におけるSPメタデータに記載されているものとなりますので、SP側で適切に検証してください。

People API

グループを指定してそのメンバーに関する情報を取得するためのAPI

リクエストURL

- メンバーのみを取得
`https://cg.gakunin.jp/api/people/@me/グループentityIDorID[?lang=言語]`
- 管理者のみを取得
`https://cg.gakunin.jp/api/people/@me/グループentityIDorID%2Fadmin[?lang=言語]`

グループentityIDorID には グループentityID もしくは グループID を指定します。

グループentityID は、isMemberOfで取得することができる値をURLエンコードした値です。

例えば、isMemberOfで取得した値が下記の場合は、

(元の値) `https://cg.gakunin.jp/gr/GakuNinTF`

URLエンコード後は、下記となります。

(変換後の値) `https%3A%2F%2Fcg.gakunin.jp%2Fgr%2FGakuNinTF`

※ %3A、%2Fのアルファベットは小文字も許容します。

また、グループentityIDの短縮形の グループID を利用することも可能です。
isMemberOfが上記の(元の値)とした場合、短縮形のグループIDは、**GakuNinTF**となります。

管理者を取得する場合は、グループentityIDもしくはグループIDに %2Fadmin を付与します。
~~SPコネクタのグループentityIDもしくはグループIDに %2Fadmin を付与すると、SP管理者が取得できます。~~

設定値と取得できる値をまとめたものを以下に示します。

グループentityID/ID	%2Fadmin	取得値
グループを指定	無	グループメンバー一覧
〃	有	グループ管理者一覧
SPコネクタを指定	無	仕様外
〃	有	仕様外

言語 はオプション項目であり、レスポンスで返す言語を指定します。
指定できるTYPEは、en と ja で、下記の優先順位でレスポンスを返します。

リクエストURLの言語指定 > 英語入力 > 日本語入力

なお、英語、日本語とも学認クラウドゲートウェイサービスに登録がなければ、当該属性自体が存在しない状態で返します。

認可: 認証に用いた証明書に紐づくSPを対象SPとするSPコネクタについて、当該SPコネクタと指定したグループが接続している場合のみメンバー情報を取得することができます。なお、グループentityID/IDとして指定できるのは、SPコネクタに直接接続しているグループのみです。

下記に例を示します。
学認クラウドゲートウェイサービスに、氏名「日／英」、自己紹介「英」、所属「日／英とも空欄」で登録されていた場合、
リクエストの言語指定が「ja」であった場合は、氏名「日」、自己紹介「英」、所属「無し」を、
リクエストの言語指定が「en」であった場合は、氏名「英」、自己紹介「英」、所属「無し」を、
リクエストの言語指定がない場合は、氏名「英」、自己紹介「英」、所属「無し」を返します。

項目	日本語の登録	英語の登録	lang=ja	lang=en	言語指定なし
----	--------	-------	---------	---------	--------

氏名	有	有	日本語	英語	英語
自己紹介	-	有	英語	英語	英語
所属	-	-	-	-	-

レスポンス

上記リクエストのレスポンスを以下に示します。（見易くなるように整形しています）

```
{
  "totalResults" : <ユーザ数>,
  "entry" : [
    {
      "id" : "<学認クラウドゲートウェイサービスのeduPersonTargetedID>",
      "displayName" : "<氏名>",
      "aboutMe" : "<自己紹介>",
      "emails" : [
        { "type" : "email", "value" : "<学認クラウドゲートウェイサービスに登録したメールアドレス>" }
      ],
      "languagesSpoken" : [
        { "type" : "languageSpoken", "value" : "<学認クラウドゲートウェイサービスに登録した使用言語>" }
      ],
      "organizations" : [
        { "type" : "organization", "value" : { "name" : "<学認クラウドゲートウェイサービスに登録した所属>" } }
      ],
      "map_IdPEntityIDs" : [
        { "type" : "map_IdPEntityID", "value" : "https://xxxxxx/idp/shibboleth" },
        ...
      ],
      "eduPersonPrincipalNames" : [
        { "type" : "eduPersonPrincipalName", "value" : "<所属機関IdPから送信されたeduPersonPrincipalName>" },
        ...
      ],
    },
    ...
  ]
}
```

フィールド名	内容	備考
totalResults	ユーザ数（全ての属性が許可されない場合そのユーザ分は差し引く）	Required
id	学認クラウドゲートウェイサービスのeduPersonTargetedID	
displayName	氏名	
aboutMe	自己紹介	未有効化
emails	メールアドレス	
languagesSpoken	使用言語	"en"もしくは"ja" 未有効化
organizations	所属	未有効化
map_IdPEntityIDs	認証に利用するIdP（entityID）	複数可 未有効化
eduPersonPrincipalNames	所属機関IdPから送信されたeduPersonPrincipalName	複数可

※ Required以外のフィールドは、利用者が同意したフィールドのみ送られます。また、全てのフィールドが存在しない（同意されていないもしくはSPが要求していない）場合はオブジェクトごと無くなります。

※ id には、学認クラウドゲートウェイサービスが発行する永続的な識別子のJavaScriptでの表現が入ります。SP毎に異なる値になりますが、同一SPに対しては同一ユーザについて常に同じ値を返します。

例: "https://cg.gakunin.jp/idp/shibboleth!https://sp.example.ac.jp/shibboleth-sp!S8Xi7R5Wf1pd8k8lq9eoiXyCtmw="

※ ここで送信される id と、ユーザ認証時にSimpleAggregationで学認クラウドゲートウェイサービスから送信されるeduPersonTargetedIDは一致します。

※ 特に、文字列中にUnicodeのコード表記（例:\u3042）の形式の文字を含む可能性があります。

※ 指定されたグループに下位グループが存在する場合、下位グループのメンバーも含まれます。

※ 未有効化のフィールドについては現状利用できません。受信を希望するフィールドがございましたら学認クラウドゲートウェイサービスサポートまでご連絡ください。

※ People APIで取得できる属性については [FAQ#学認クラウドゲートウェイサービスとIdPから得られる情報の違いについて](#) も合わせてご参照ください。

Groups API

SPコネクタに接続しているグループに関する情報を取得するためのAPI

リクエストURL

- SPコネクタに接続しているグループ情報の取得
- https://cg.gakunin.jp/api/groups/@me[?lang=言語]
- https://cg.gakunin.jp/api/groups/SPコネクタentityIDorID[?lang=言語]

SPコネクタentityIDorID には SPコネクタentityID もしくは SPコネクタID を指定します。

SPコネクタID は、SPコネクタ作成時に入力した任意の文字列、もしくは自動生成されたUUID形式の値となっており、SPコネクタの管理者メニューの「SPコネクタの修正」から値を確認できます。

SPコネクタentityID は、「https://cg.gakunin.jp/sp/」とSPコネクタIDと組み合わせてURLエンコードした値です。

例えば、SPコネクタIDが **GakuNinTF** の場合は、
（元の値）https://cg.gakunin.jp/sp/GakuNinTF
URLエンコード後は、下記となります。
（変換後の値）https%3A%2F%2Fcg.gakunin.jp%2Fsp%2FGakuNinTF
※ %3A、%2Fのアルファベットは小文字も許容します。

SPコネクタとして @me が指定された場合は、認証に用いた証明書に紐づくSPを対象SPとする全てのSPコネクタと解釈され、いずれかのSPコネクタに接続しているグループ情報を返します。

言語 はオプション項目で、レスポンスで返す言語を指定します。
指定できるTYPEは、enとjaであり、下記の優先順位でレスポンスを返します。
リクエストURLの言語指定 > 英語入力 > 日本語入力
なお、英語、日本語とも学認クラウドゲートウェイサービスに登録がなければ、当該属性自体が存在しない状態で返します。

認可: 指定されたSPコネクタは、認証に用いた証明書に紐づくSPを対象SPとするSPコネクタでなければなりません。

下記に例を示します。
学認クラウドゲートウェイサービスに、グループ名「日／英」、紹介文「日」で登録されていた場合、
リクエストの言語指定が「ja」であった場合は、グループ名「日」、紹介文「日」を、
リクエストの言語指定が「en」であった場合は、グループ名「英」、紹介文「日」を、
リクエストの言語指定がない場合は、グループ名「英」、紹介文「日」を返します。

項目	日本語の登録	英語の登録	lang=ja	lang=en	言語指定なし
グループ名	有	有	日本語	英語	英語
紹介文	有	-	日本語	日本語	日本語

レスポンス

上記リクエストのレスポンスを以下に示します。（見易くなるように整形しています）

```
{
  "totalResults" : <グループ数>,
  "entry" : [
    {
      "id" : "<グループentityID>",
      "title" : "<グループ名>",
      "description" : "<グループの紹介>",
      "map_totalMembers" : <グループのメンバー数>
    },
    ...
  ]
}
```

※ <グループentityID> は、isMemberOfで取得することができるURL形式の値（のJavaScriptでの表現）

例: "https://cg.gakunin.jp/gr/GakuNinTF"

※ このAPIで取得できるグループはSPコネクタに直接接続しているもののみです。上位グループ経由で接続している下位グループのグループ情報は含まれません。

※ <グループのメンバー数> には、管理者のみの人（管理者であるがメンバーでない人）は含まれません。また、属性送信に同意しているかどうかに関わらずカウントされますので、people APIを通して取得した数より大きい可能性があります。

※ 特に、文字列中にUnicodeのコード表記（例:\u3042）の形式の文字を含む可能性があります。

New Group API

SPに新たなグループから接続があった場合に学認クラウドゲートウェイサービスから呼び出されるコールバックタイプのAPIです。

コールバックURL

- URLのフォーマットは特に定めません。SPコネクタの設定項目の一つである「New Group API」欄にSP側のAPIのURLを登録してください。
- URLに以下の変数を含めると、API呼び出し時に当該部分が学認クラウドゲートウェイサービスが持つ情報で置換されます。

変数名	置換される値
SgroupID	グループID（グループentityIDの短縮形）
SadminEmail	接続を行ったグループ管理者のメールアドレス（つまり当該グループに管理者が複数人いても1つのみ渡されます）

- 例えばmeatmailでは以下のように登録しており、

```
https://meatmail.nii.ac.jp/meatmail-api/newList/$groupID/$adminEmail
```

実際の呼び出し例は以下のようになります。

```
https://meatmail.nii.ac.jp/meatmail-api/newList/TestGroup/user%40example.jp
```

- 当該URLへのアクセスをソースIPアドレスで制限している場合には、少なくとも学認クラウドゲートウェイサービスからのアクセスを許可してください。アクセス元は natgw1.cg.gakunin.jp, natgw2.cg.gakunin.jp (52.192.180.249, 52.199.121.28) となります。学認クラウドゲートウェイサービスがURLへアクセスできない場合には「SPコネクタとは接続できません」とのエラーメッセージが出力されます。



グループ管理者の操作によって、同じリクエストが複数あることがあります。そのため、問題がない場合はOKを返すようにしてください。

例えば、メーリングリストの作成リクエストの1回目は実際にメーリングリストを作成し、2回目は既に作成されているのでそのままOKを返します。

レスポンス

上記コールバックのレスポンスを以下に示します。SP側では下記のようなJSON形式で、学認クラウドゲートウェイサービスにレスポンスを返す必要があります。

成功時

```
{
  "result": "OK",
  "message": "メッセージ"
}
```

失敗時

```
{
  "result": "NG",
  "message": "メッセージ"
}
```

項目	必須	説明
result	○	成功時はOK、失敗時はNGを設定します。
message	○	成功時、失敗時ともメッセージを入れてください。現状これは学認クラウドゲートウェイサービスのログに記録されるのみです。

HTTPステータス

HTTPステータス	説明
200	学認クラウドゲートウェイサービスからのコールバックを受け付けた場合、ステータスを200で返してください

※ HTTPステータスが200以外の場合、および上記resultがNGの場合は、接続したグループ管理者に対して「meatmailへのAPI呼び出しが失敗しました」のように画面にメッセージが表示されます。

サーバ認証およびクライアント認証

学認クラウドゲートウェイサービスからのリクエストではTLSクライアント証明書認証を使います。
学認フェデレーションのメタデータにある学認クラウドゲートウェイサービス（entityID:https://cg.gakunin.jp/idp/shibboleth）の証明書を使いSPにリクエストします。
SP側ではリクエストを受け取った際に、学認クラウドゲートウェイサービスの証明書であることを確認してください。

また、学認クラウドゲートウェイサービス側はTLSサーバ証明書認証によりリクエスト先の正当性確認を行ないます。登録したURLのスキームがHTTPSであること、および当該URLのサーバ証明書がSPメタデータに記載されたものと一致することをご確認ください。

エラーレスポンス（共通）

HTTPステータス	原因
400	APIのURL不正
403	・提示された証明書が学認参加SPのものでない場合 ・セレクトア(@me)が未設定の場合 ・指定されたグループが対象となるSPコネクタと接続していない場合
404	指定されたグループがない場合

※ @meはクライアント証明書認証に用いた証明書に紐づくSPを対象SPとする0個以上のSPコネクタと解釈されます。該当する学認参加SPが存在する場合は、学認クラウドゲートウェイサービス上に対応するSPコネクタが存在しない場合でもエラーにはなりません。
※ レスポンスに返すデータが0件の場合は空配列のentryを返します。