FAQ

学認クラウドゲートウェイサービス利用に関してよくあるご質問 (FAQ)

- WAYFless URLを持つSPをプライベートサービスに登録するには？
- meatwiki等の連携SPにて学認クラウドゲートウェイサービスで設定したグループ権限でアクセスできない
    - IdPから連携SPへ必要な属性が送信されていない
    - ePPN属性の値が変更になった
    - IdPから送信されるePPNがSPごとに異なっている
- 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
- 必須属性が送られていないときの学認クラウドゲートウェイサービスの挙動について
- IdPで認証時にブラウザに「SAML response reported an IdP error」というエラーが出力されます
- 学認クラウドオンデマンド構築サービスをサービス一覧に表示したい

※ 学認クラウドゲートウェイサービス利用申請などその他のよくあるご質問はこちら⇒学認クラウドウェブサイト

WAYFless URLを持つSPをプライベートサービスに登録するには？

SPによってはディスカバリーサービス(DS)のIdPリストから所属機関を選択して認証する方法のほかに、所属機関ごとに用意されるWAYFless URLを用いてログインする方法が提供される場合があります。WAYFless URLは所属機関ごとに異なるURLが発行されるため、学認クラウドゲートウェイサービスの利用可能サービスとして表示するためにはプライベートサービスを活用する必要があります。

あなたが所属機関のIdP管理者である場合には、プライベートサービスを機関グループに接続することで、機関に所属するユーザが利用可能なサービスとして公開することができます。プライベートサービスを使ったWAYFless URLのサービス追加について以下に設定例を記載します (事前に プライベートサービス のドキュメントをご一読ください)。

- 学認クラウドゲートウェイサービス (https://cg.gakunin.jp/) にログインしてください。
- ゲートウェイトップ画面右上のドロップダウンメニューから「プライベートサービスの登録」をクリックしてください。
- 「プライベートサービスの登録」で以下を設定してください。
    - **サービス名称　　：**任意の名前を設定することができます。所属機関のユーザに見せることを考えると学認の IdP・SP一覧 と同じ名前にしておくほうが混乱が少ないと考えられますが、サービス名称は学認クラウドゲートウェイサービス内で一意でなくてはならないという制約があります。「同一のグループ名が存在します」というエラーが表示される場合はサービス名称を修正してください。
    - **接続するグループ：**所属する機関グループを選択します。
    - **サービスアイコン：**任意のアイコンを選択してください。もしくは上記 IdP・SP一覧 にロゴが表示されている場合はその画像をアップロードすることもできます。
    - **サービスURL　　：**SPから指定されたWAYFless URLを設定してください。SPごとの具体的な設定例を以下に記載します

meatwiki等の連携SPにて学認クラウドゲートウェイサービスで設定したグループ権限でアクセスできない

meatwikiをはじめとした学認クラウドゲートウェイサービス連携SPでは「MYグループ」で設定したグループ情報に基づいて、SPごとに定められた処理（アクセス権の付与など）が行われています。グループ情報の登録が学認クラウドゲートウェイサービス上では正しくなされているにも関わらず、連携SP側に正しいグループ情報が渡っていない（許可されているはずのページが表示されない、スペースが表示されないなど）の場合には次の原因が考えられます。

IdPから連携SPへ必要な属性が送信されていない

学認クラウドゲートウェイサービスへ必要な属性を送信しているのと同様に、連携SPへもそれが要求している属性を送信してください。特にePPN (eduPersonPrincipalName) を連携SPへも送信しないとグループ情報が渡らない原因となります。

ePPN属性の値が変更になった

以前はアクセスできていたものがメンバー変更等を行っていないのにアクセスできなくなった場合、IdP側の設定変更でePPN属性の値が変更になった可能性があります。連携SPはePPNをユーザのIDとしていますのでこれが変更になっていると別人として扱われ、必要な権限が得られません。さらに学認クラウドゲートウェイサービスもePPNをユーザのIDとしているため、旧ePPNでグループのメンバーだったという情報が新ePPNには引き継がれません。このようになってしまった場合はグループ管理者に依頼して新ePPNのアカウントを改めてグループメンバーにしてもらう必要があります。その後、連携SPにアクセスし再度ログインすれば、グループメンバーとして正しく認識されるはずです。

詳しくは所属機関のIdP管理者にお問い合わせください。これはスコープが変更になった場合も同様です。

IdPから送信されるePPNがSPごとに異なっている

IdPから学認クラウドゲートウェイサービスと連携SPにそれぞれ異なるePPN (eduPersonPrincipalName) が送信されていることが原因で正しいグループ情報が渡らず、結果として意図した動作ができないという場合があります。これは連携SPがePPNをキーとして学認クラウドゲートウェイサービスへ問い合わせを行うために、SPごとにそれぞれ異なるePPNが送信されている場合には別の人物として取り扱われるためです。

ePPNの送信に関しては、フェデレーションに参加する全てのSPに対して同じ値を送信する必要があることが学認の属性リスト (eduPersonPrincipalName) にも明記されています。

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

学認クラウドゲートウェイサービスではグループID(isMemberOf)のほかに学認クラウドゲートウェイサービス上に保持する属性として eduPersonTargetedID (ePTID)、メールアドレス(mail)、氏名(displayName)等を保持しており、これらを利用者の同意に基づいて対応SPへ送信することが可能です。
また、同時にこれらの情報は所属機関IdPで属性の送信を許可している場合にはIdPから情報を得ることも可能となっています。

対応SPでこれらの情報を利用する場合には正確性や入手容易性に関する次の特性をふまえ、属性値の利用を検討してください。

- IdPから送信される属性は学認技術運用基準 (https://www.gakunin.jp/join/production/) 等の定めにより、送信される属性がその機関によって保証されています。
  送信できる属性については各所属機関のIdP管理者によって設定されます（最終的にはIdP付属の機能やuApprove JP等によりユーザが属性送信に同意したものが送られますが、その範囲はIdP管理者が許可した範囲にとどまります）。また、属性送信可否の決定プロセスは各機関でまちまちですが、上位委員会の決定に従うところもあるようです。
- 学認クラウドゲートウェイサービスから送信される属性のうちePTIDを除く属性についてはユーザ自身が設定した値であり、入力された値の正確性の保証はされません。
  送信できる属性については各グループ管理者によって決定されます（最終的にはユーザが属性送信に同意したものが送られますが、その範囲はグループ管理者が許可した範囲にとどまります）。

必須属性が送られていないときの学認クラウドゲートウェイサービスの挙動について

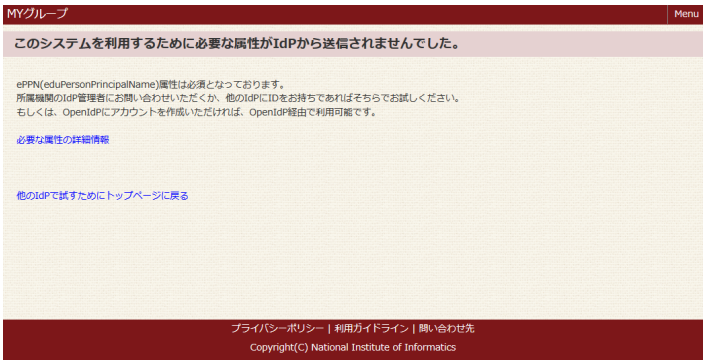
学認クラウドゲートウェイサービスの利用にはIdPから属性送信をしていただく必要があります。送信が必要な必須属性は 学認クラウドゲートウェイサービス連携のための情報#IdP管理者に必要な情報に示す通りです。

必須属性が送られていない場合には以下の挙動を示します。学認クラウドゲートウェイサービスに利用申請していただいていない機関の方はログイン後直接後者の画面が表示されます。また、招待メール記載のURLからログインした場合も後者の画面が表示されます。

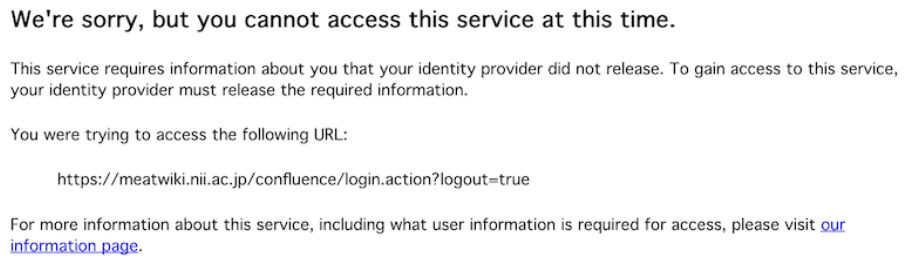
- ゲートウェイトップ画面（ゲートウェイサービス利用機関の方に対して、通常通り表示されます）

- MYグループ画面（以下のようなエラーメッセージが表示されます）

> このシステムを利用するために必要な属性がIdPから送信されませんでした。



なお、学認クラウドゲートウェイサービスから連携している他サービス(SP)を利用する場合、当該サービスに必要な属性を送信していないとサービスが利用できません。詳細は各サービスへお問い合わせください。例えばmeatwikiを利用するために必要な属性を送信していないと以下のような"We're sorry, but you cannot access this service at this time."で始まるエラー画面が表示されるようです。



IdPで認証時にブラウザに「SAML response reported an IdP error」というエラーが出力されます

アカウントの紐付けの処理において（認証時）、ブラウザに以下のエラーが出力される場合は、所属機関IdPでForce Authentication機能が無効もしくは非対応である可能性があります。IdPの設定情報等の詳細は所属機関のIdP管理者にお問い合わせください。

```
opensaml::FatalProfileException

The system encountered an error at Wed Dec 12 17:00:08 2018
To report this problem, please contact the site administrator at root@localhost.
Please include the following message in any email:
opensaml::FatalProfileException at (https://cg.gakunin.jp/Shibboleth.sso/SAML2/POST)
SAML response reported an IdP error.

Error from identity provider:
    Status: urn:oasis:names:tc:SAML:2.0:status:Requester
    Sub-Status: urn:oasis:names:tc:SAML:2.0:status:AuthnFailed
    Message: An error occurred.
```

学認クラウドオンデマンド構築サービスをサービス一覧に表示したい

オンデマンド構築サービスをゲートウェイサービスの1つのサービスとして登録していただくと、ゲートウェイサービスからオンデマンド構築サービスにアクセスできるようになります（オンデマンド構築サービスのユーザーインターフェースであるJupyterNotebookのみ）。
プライベートサービスの登録手順にて、オンデマンド構築サービスページ記載の「ご利用までの流れ」の「3. クライアント環境の準備」のステップでご用意いただいた Jupyter Notebook サーバの URL を登録いただきます。
その際、設定項目の1つ「接続するグループ」にて機関グループとして貴機関を選択すると構成員全員に表示されてしまいます。クラウド環境構築担当者など一部の人のみに表示したい場合は、あらかじめ対象者をメンバーにしたグループを作成した上で「接続するグループ」で当該グループを選択してください。
なお、「接続するグループ」で機関もしくはグループを選択できるのはそれぞれの管理者のみです。一般構成員もしくはグループメンバーで対象者に表示されるサービスを登録したい場合は管理者の方にその旨リクエストしてください。