

# 学認クラウドゲートウェイサービスと ガバナンス

2025年6月18日  
NII学術情報基盤オープンフォーラム2025

国立情報学研究所  
クラウド基盤研究開発センター／クラウド支援室  
西村 健

# 学認クラウドゲートウェイサービス ～大学・研究機関の認証基盤とクラウドの橋渡し～

- 一言でいえば、アクセス者が利用できるサービスを一覧にしたポータル
- 所属機関で利用可能なサービスが一覧できる
  - 機関毎のカスタマイズ（契約・連携しているサービスの指定/入力）
  - 個人毎のカスタマイズ（並び順の変更や個人利用サービスの追加）



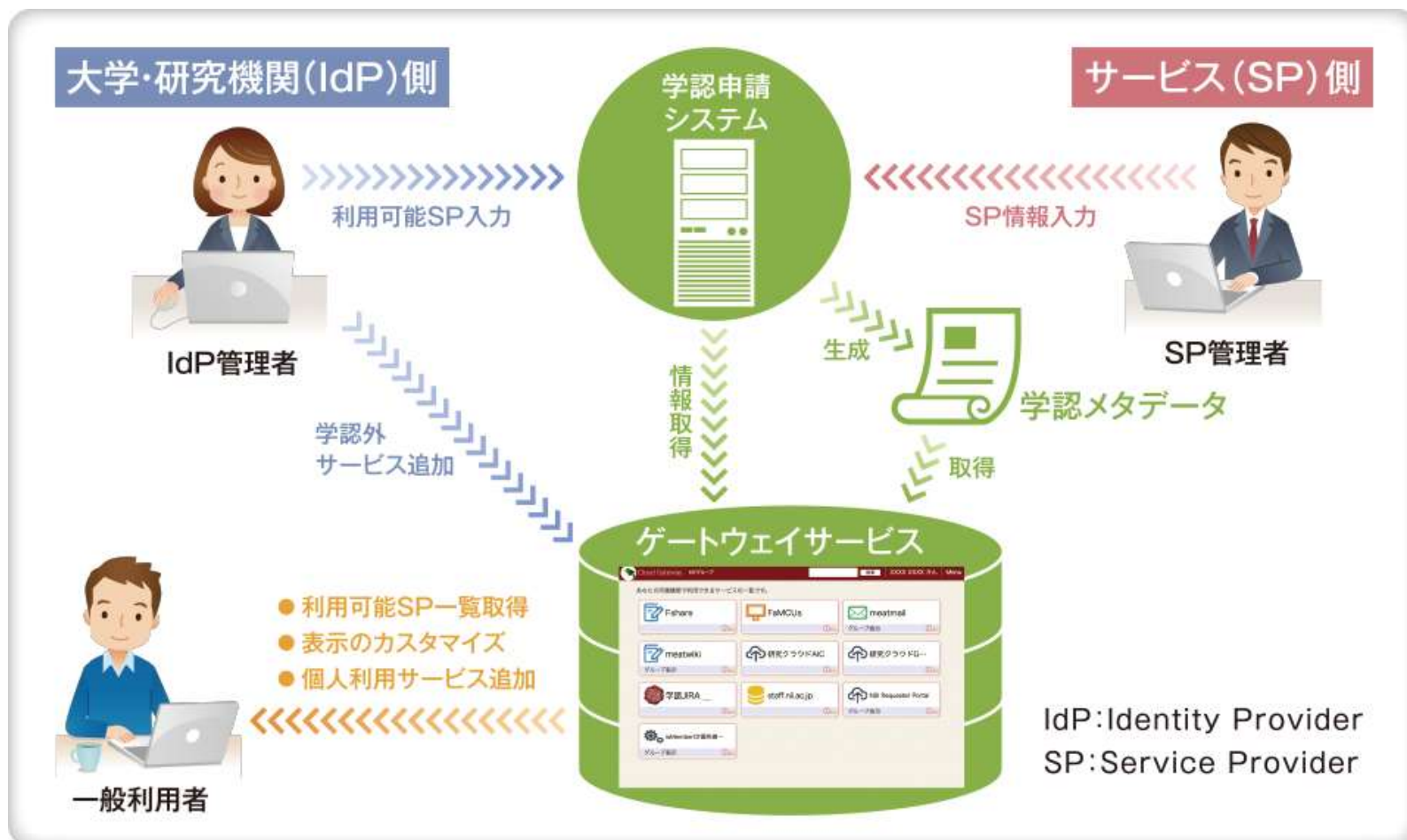
# 利用者のアクセス例

- 利用者は、ゲートウェイサービスを経由してe-Learningサイトやe-Journalサイトにアクセス



- ゲートウェイサービスに表示されているサービスは利用可能である  
= 安心してアクセスできる
- ふらっと、あるサービス(e-Learning B)にアクセスして、  
利用できなくて困る、ということがなくなる

# ゲートウェイサービスの登場人物と役割



※学認 - 大学・研究機関の認証基盤と商用・非商用のオンラインサービスの間のSSOのための枠組み

# 各種ソースからの情報を統合表示



Gateway Service MYグループ

あなたの所属機関( )で利用できるサービスの一覧です。

Elsevier: ScienceDir... Web of Science meatwiki

John Wiley & Sons ... Gmail

グループ表示

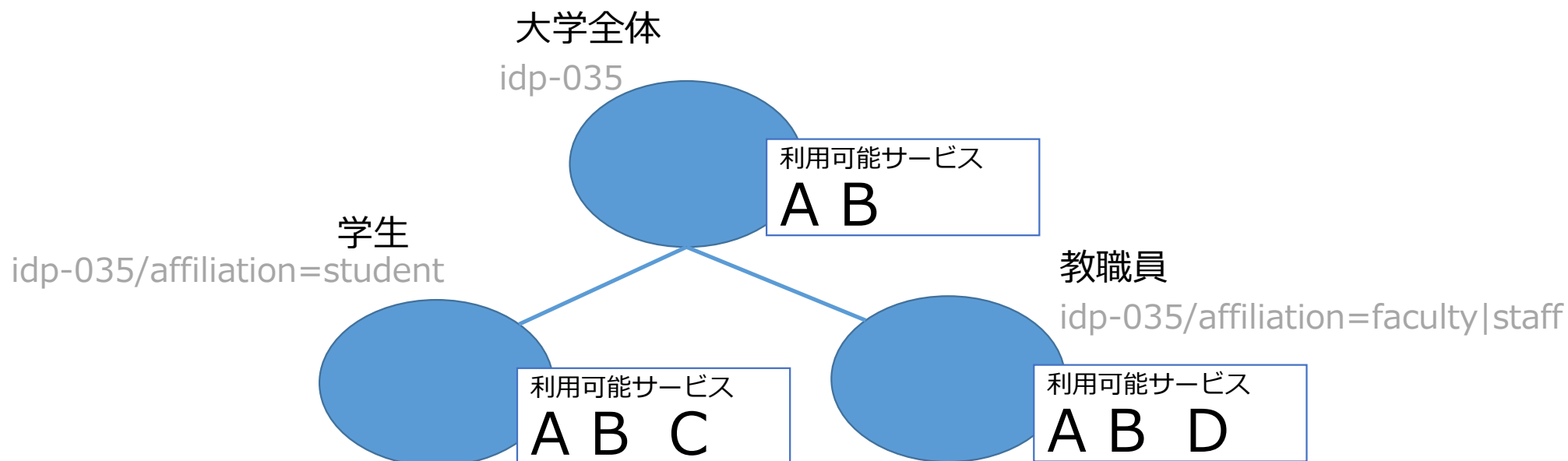
- 次世代mAP
- 学認クラウド参加大学・研究機関
- NII クラウド支援室
- uApprove Jet Pack開発

機関契約 個人利用 グループ利用

- 「機関契約」「グループ利用」「個人利用」を統合して表示
- 個人がよく使うサービスを上部に配置することが可能
- この画面を起点として各種サービスにアクセスできる
- 他の利用者への案内(「ゲートウェイサービスから〇〇をクリックしてください」)が容易に

## 利用者の属性で分類し異なるサービスリストを提供 (機関内分類機能)

- 例えば、学生は利用するが教員は利用しないサービス（例:履修登録）、およびその逆のようなサービスへの対応
- 「〇〇向けポータル」のイメージ
- 利用者の分類（サブグループ）は、IdPからの属性を元に自動分類
  - 特定部局特有のサービスなど、部局毎メニューもカバーできる（）
- 定義した分類に合致しない場合は従来通り「大学全体」に登録されたサービスが表示される



# 機関内でのガバナンスを効かせるには

- 「ガバナンス」
  - 多種多様な同種のクラウドサービスがある中で特定のサービスを使ってもらう
  - 機関が契約しているサービスに誘導する
  
- そのサービスをゲートウェイサービスに登録してください
  - 学認に参加していないサービスであっても「プライベートサービス」として登録できます
  
- ゲートウェイサービスを常用している構成員は自然とそのリンクから利用を開始する
- 「人の目に留まらせる」ことが大事

# パブリッククラウドへのSSO(1/2)

- パブリッククラウド(IaaS)の中にはSAML対応しているものがあり、コンソールにSSOできる（以下例としてAWS）
- ただし機関IdPがAWSの要求を満たすには困難が伴う
  - 学認で規定されない特殊な属性を要求している
  - “誰”としてサインインしたいかは人により異なるが、その情報を属性として贈らなければならない
    - 同一人物でも複数の役割を持つ場合もある



- 機関IdPで認証した上でゲートウェイサービスIdPが必要な属性をAWSに送信する
  - 必要な情報はグループ管理者が自由に設定できる
    - 同一グループのメンバーには同一の権限を与えるモデル
- ※ AWS側にも若干の設定が必要

# パブリッククラウドへのSSO(2/2)



## ■ 通称AWS連携 休止中

ゲートウェイサービスを介してアクセスすることで、機関IdPには手を入れることなく、機関IdPからAWSマネジメントコンソールへSSOできるようになります

手順書：<https://meatwiki.nii.ac.jp/confluence/x/9Yp6Ag>

/ 学認クラウドゲートウェイ拡張属性ドキュメント整備 📄 🗨

### ゲートウェイサービスからAWSマネジメントコンソールへシングルサインオンするための情報

作成者 KUROSAKA Shoichi, 最終変更日2019/05/17

#### 目次

- 1 概要
- 2 AWSマネジメントコンソールの設定
- 3 グループの設定
- 4 ゲートウェイサービスからAWSマネジメントコンソールへシングルサインオン

#### 概要

学認クラウドゲートウェイサービス（以下、ゲートウェイサービス）に登録されているAWSマネジメントコンソールSPコネクタに任意のグループを接続することで、ゲートウェイサービス経由でAWSマネジメントコンソールへサインオンするための手順を示します。

AWSマネジメントコンソールはすでに利用可能な状態でご契約されていることを前提とします。

⚠️ AWSマネジメントコンソールのロール設定において、権限ポリシーの選択や eduPersonEntitlementで指定する利用グループが適切に設定されない場合、意図しない権限がメンバーに付与される。⚠️ 事前にAWSマネジメントコンソールが利用されるおぼえの事故

# 課題

- 世の中の多種多様なサービスそれぞれについて各大学が作成するのは大変
  - 作成したプライベートサービスを他機関でも参照できるようにする仕組みの提供検討
    - 「半公開サービス」？
  - もちろんNIIとしても半公開サービスの提供に協力します
  - 「こういう方向性で作成すればよい」というガイドラインの提供検討
  
- 本提案によって「機関内でガバナンスを効かせる」ことの一助になるでしょうか？