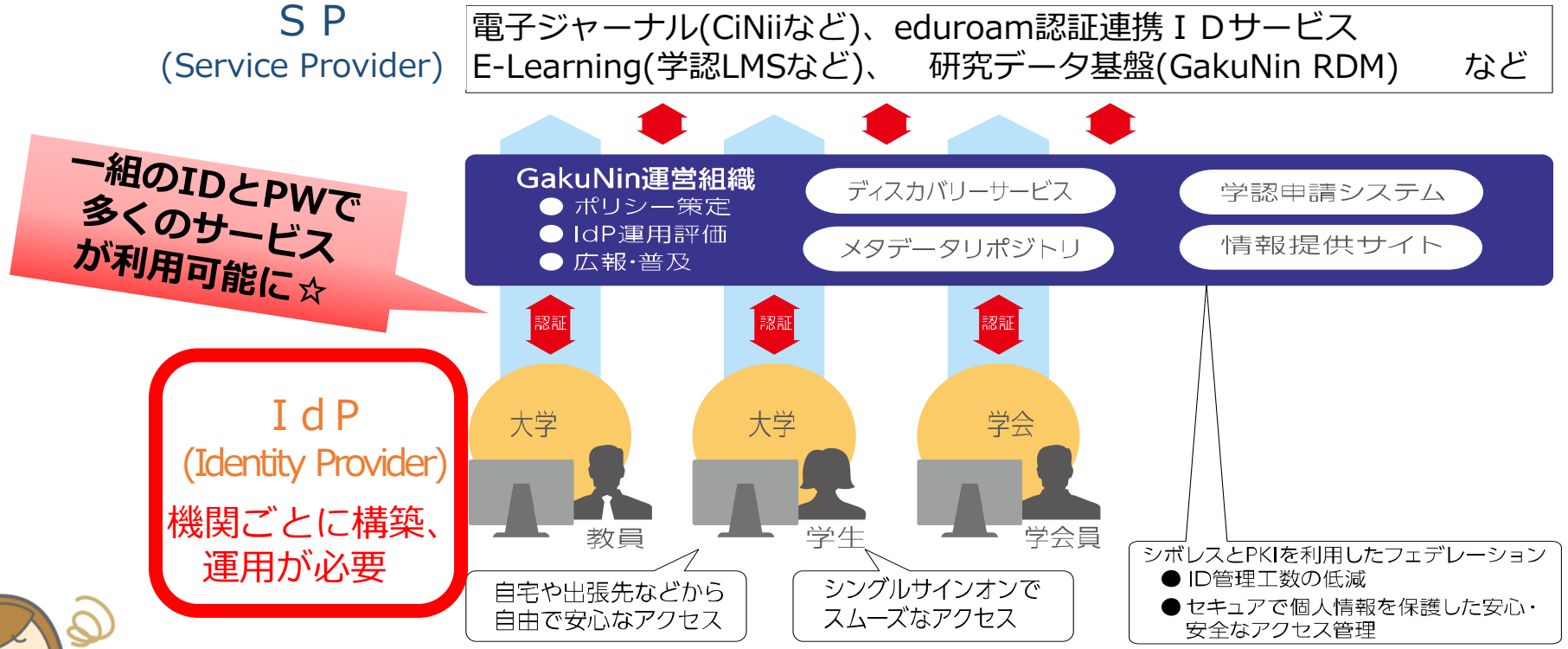
学認対応IdPホスティングサービス実証 実験から得られたID管理事情

清水　さや子

国立情報学研究所

学認とは

- 学術認証フェデレーション［学認］とは、所属機関が発行するアカウントを用いて学外の情報リソースにアクセスするための認証連携のフレームワーク

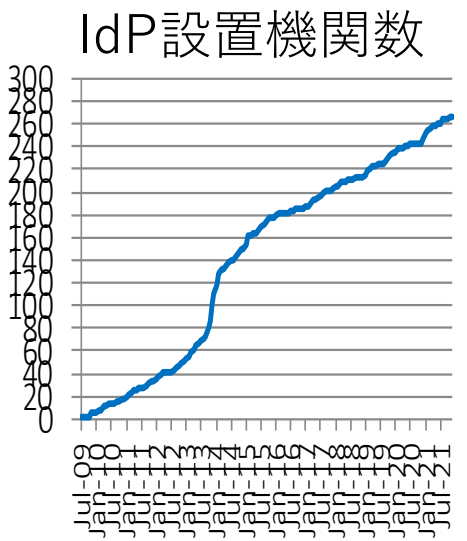


学認参加に向けた課題

- 現在、学認の参加機関は、約300機関（2023.12.1時点）
- 未参加機関の理由：

A) 人員的な問題（運用する人材、参加検討する人材の不足）（58件）
B) 技術的な問題（サーバの構築や運用ができないなど）（23件）
C) 金銭的な問題（20件）
D) 必要かどうかわからない（11件）
E) 委託業者が分からない（9件）
F) 現在は不要である（5件）　　などなど

➡IdPサーバの構築、運用がネックになっている場合が多い



（件数は、2022年10月のアンケート結果（複数回答可）、対象72機関より）
参考URL　https://www.gakunin.jp/document/684
アンケートにご協力いただきました皆様、誠にありがとうございました。

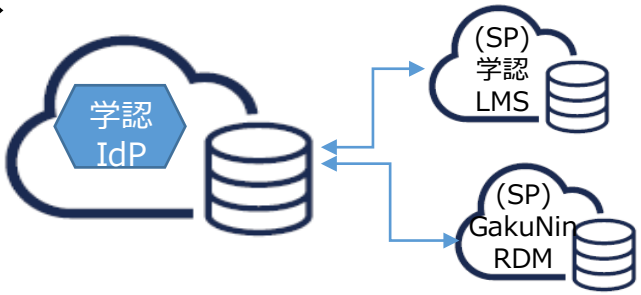
- 次世代学認では、全ての人が認証できるようにしたい、認証レベルを上げたい
- もっと多くの機関に学認参加していただきたい

学認参加の際の障壁を下げるため、障壁の一つであると考えられるIdPを、NIIで貸し出すためのサービス（学認対応IdPホスティングサービス）を検討開始

学認対応IdPホスティングサービス実証実験

- 実証実験の目的：提供サービスの内容と参加機関における課題の分析を行う

- 実証実験の内容：
  - **対象機関は、学認への参加を予定または検討中であり、IdPの構築、運用に課題がある機関、または、既に学認に参加しIDaaSへの移行を検討している機関、約10機関**
  - **学認対応のIdPサーバをクラウドサービス（IDaaS）として提供**
  - 実証実験の期間は、2023年3月～2024年4月の約1年間
  - 単なるIDaaSとして提供するだけでなく、**各種支援も提供**
    - ✓ 学認への参加手続きに関する支援
    - ✓ IdPホスティングサービスへの初回アカウント登録支援（２回目以降は機関側で対応）
    - ✓ IdPホスティングサービスの設定操作の支援
    - ✓ 学認に関するメタデータの登録支援
    - ✓ SP接続時の設定支援（5つまで。 6SP以降は機関側にて対応）
    - ✓ 学認参加IdP運用状況調査の一部回答サポート　など



参考 https://www.gakunin.jp/node/687

- 募集の流れ：
  - 2023年1月　協力いただける機関（実証実験参加機関）の募集
    - 想定を上回る多くの機関様からご希望、お問合せをいただきまして、誠にありがとうございました。
  - 2023年2月末　参加機関の決定
    - ご希望いただいた全機関にヒアリングを行い、NII側であらかじめ設定していた基準に基き、選定させていただきました。

実証実験参加機関について

- 実証実験参加機関数：10機関、合計約20,000アカウント

		アカウント数
1	S大学	1700（教職員＋全学生）
2	B大学	7500（教職員＋通学課程学生）
3	H院	100（教職員）
4	K館	100（教職員）
5	K所	350（研究者＋職員）
6	T大学	2000（教職員＋全学生）
7	A大学	1600 (教職員＋全学生)
8	K大学	1000 (教員のみ)
9	S大学	450 (教職員のみ)
10	K大学	6400（教職員＋全学生）

（特徴）

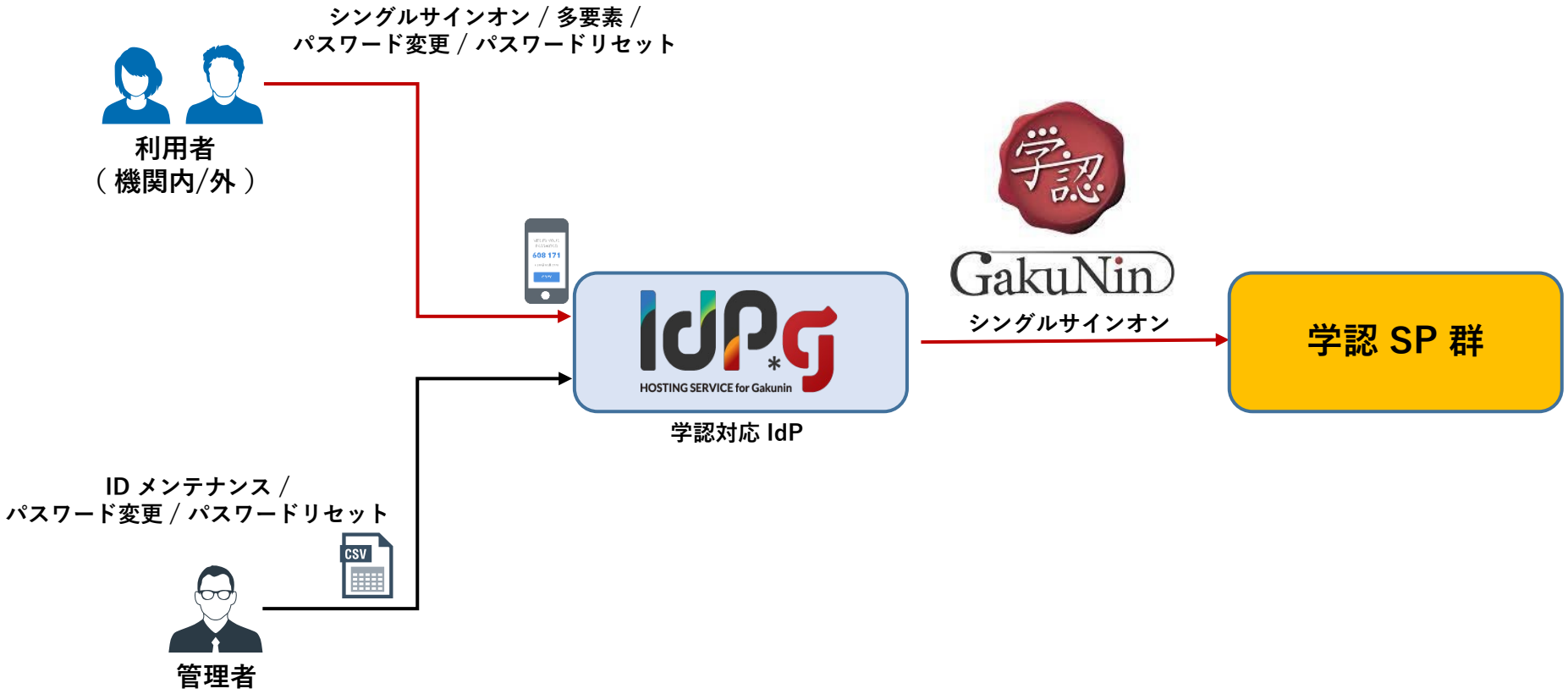
- 既にUPKI を利用していた機関は7機関
- 学認参加済機関は0機関
  - 10機関とも学認未参加

- ID 管理システムを導入していた機関は3機関
  - すべてオンプレで導入
  - 該当の3機関は比較的大規模な組織

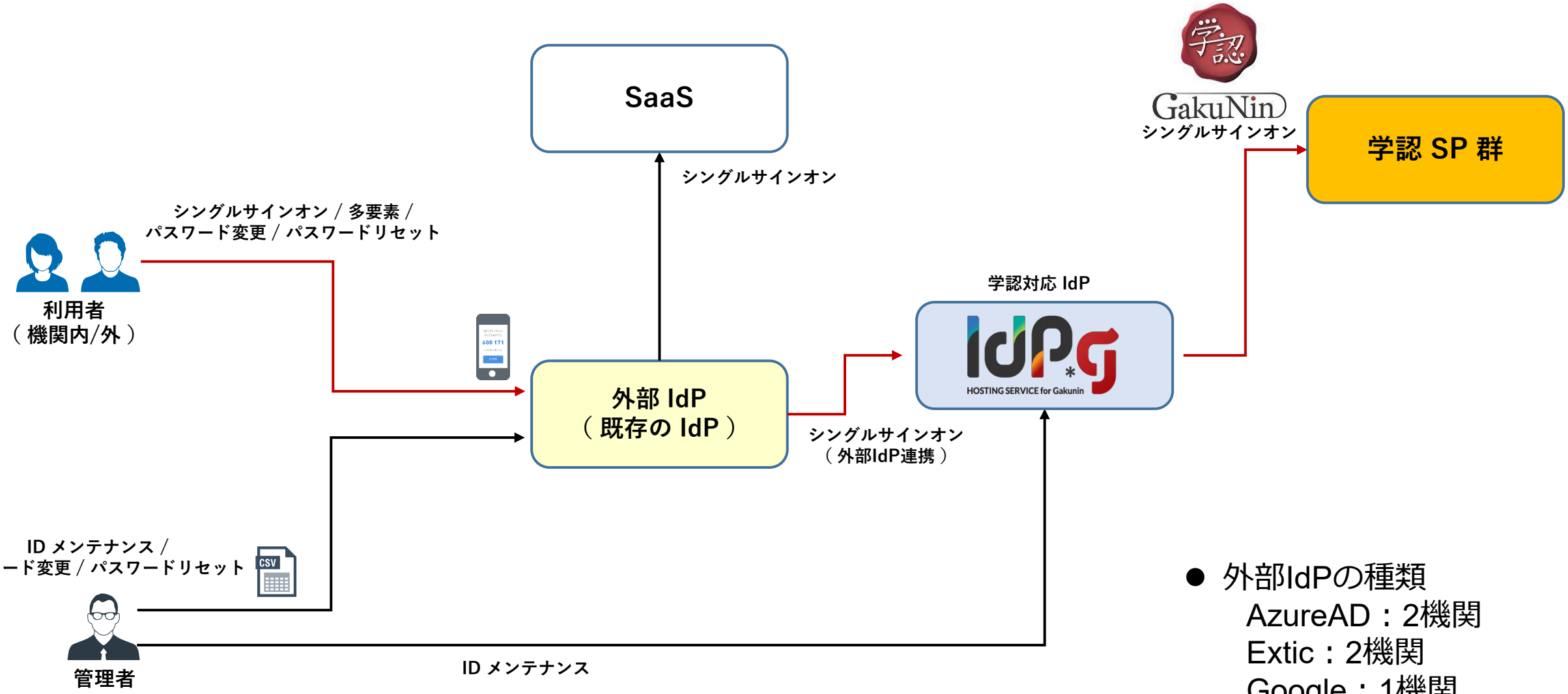
- 認証サーバにAzureAD を利用している機関は7機関

（実証実験開始時点、2023年4月）

実証実験の構成（スタンダード構成）



実証実験の構成（学認対応IdPの認証に外部IdPを利用した構成）



- 外部IdPの種類
  AzureAD：2機関
  Extic：2機関
  Google：1機関

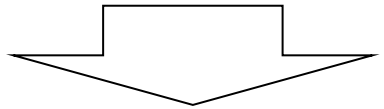
実証実験から出てきた課題

- 自組織に所属していないユーザの対応
  - 在籍者は、教職員、学生、 留学生、研究員、派遣契約社員、客員教員などなど・・
  - 身分や所属によって管理部局が異なる
  - これだけでも管理が大変
  - さらに他組織所属の共同研究者などが在籍している場合もあり

- 要望：自組織外の共同研究者と同じSP（具体的にはGakuNinRDM）を利用して研究データ管理などを行いたい
  - 具体的には、N院様、管理範囲にある研究データ基盤を共通化されたい
  - しかし、N院様の共同研究者は学認に参加していない組織の人が多い
  - 自組織所属でない共同研究者は、自組織のIdPに登録することが難しい
    - ライセンス、ID管理などが課題
    - 共同研究者は、研究代表者、研究分担者、研究協力者など範囲が広いため、すべてを自組織で管理することが難しい

課題に対する対応

- 自組織に所属していない（学認未参加機関に所属）ユーザが、同じSPを利用して研究データ管理など行えるようにする機能を、Orthrosで実現しようと検討中



「（仮）学認対応IdPホスティングサービスのOrthros連携」として検討中

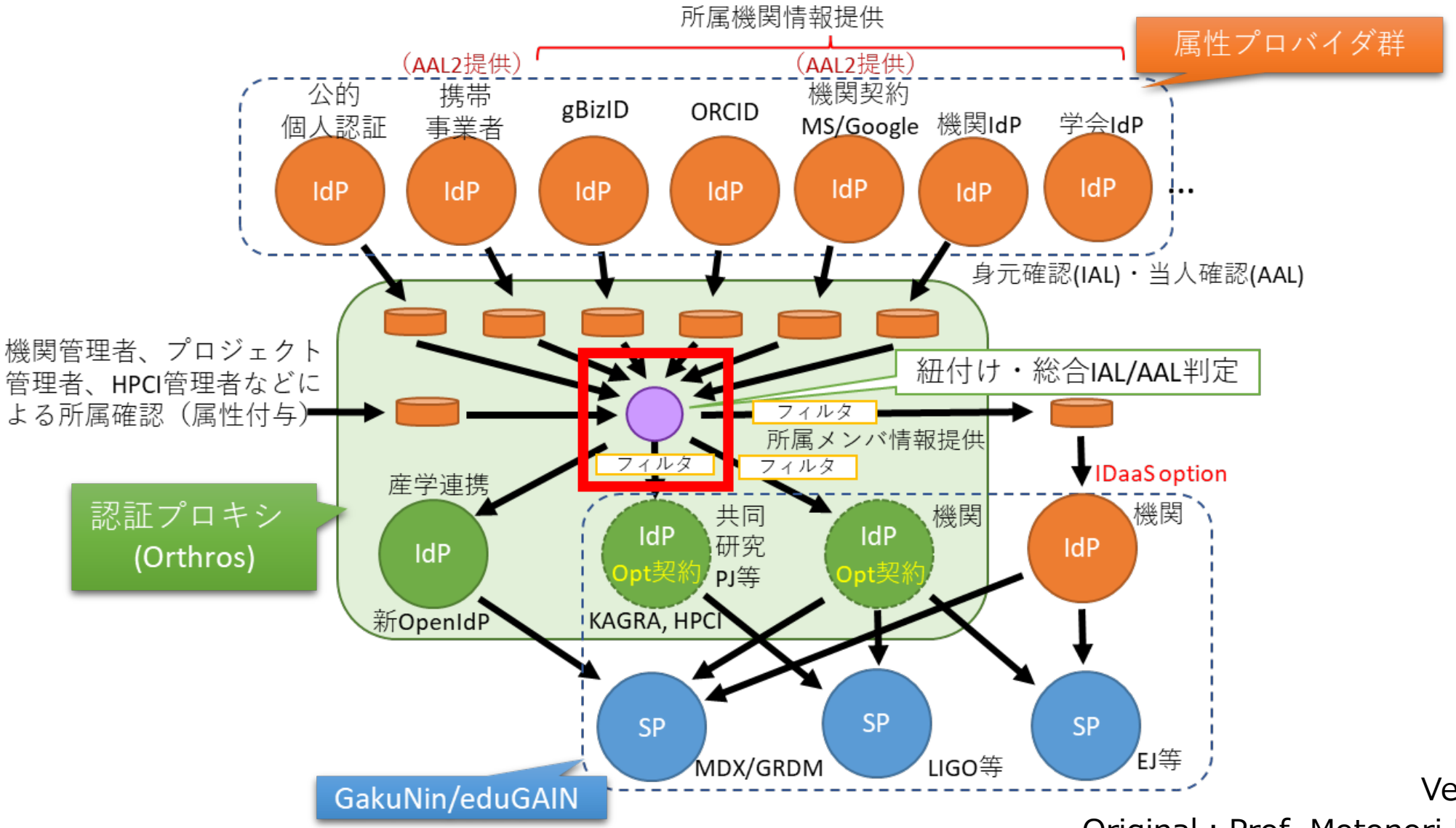
具体的に検討中の内容と今後

1. 運用ポリシーの取り決め
   - プロジェクト自体の運用、利用者管理を各機関N院様がどのように行うべきか、のルール・ポリシー策定
     - 例：プロジェクトの管理をどうするか？棚卸しの要否は？タイミングは？
       地方自治体など共通IDを使っているところをどうするか？
       機関に属していない人をどうするか？
       そもそも本人確認はどうするのか？　など
   - Orthrosを利用するにあたり、別途提供されるIdPホスティングサービスとの棲み分けを含むサービス提供範囲・内容に関する基準の策定

2. 属性を用いた認可の試験的な実装検討（GakuNinRDMとの接続）
   - Orthrosからプロジェクト属性の送出
   - GakuNinRDMとの接続（送出したプロジェクト属性を用いたGakuNinRDM側での認可処理の検討・実装）
   - GakuNinRDM以外のSPにおける対応可否の検討

➡ 学認対応IdPホスティングサービスのOrthros連携の実現に向けて～

【参考】　認証プロキシのデザイン



Ver.2023.12

Original : Prof. Motonori Nakamura