認証プロキシサービス Orthros

坂根 栄作
国立情報学研究所

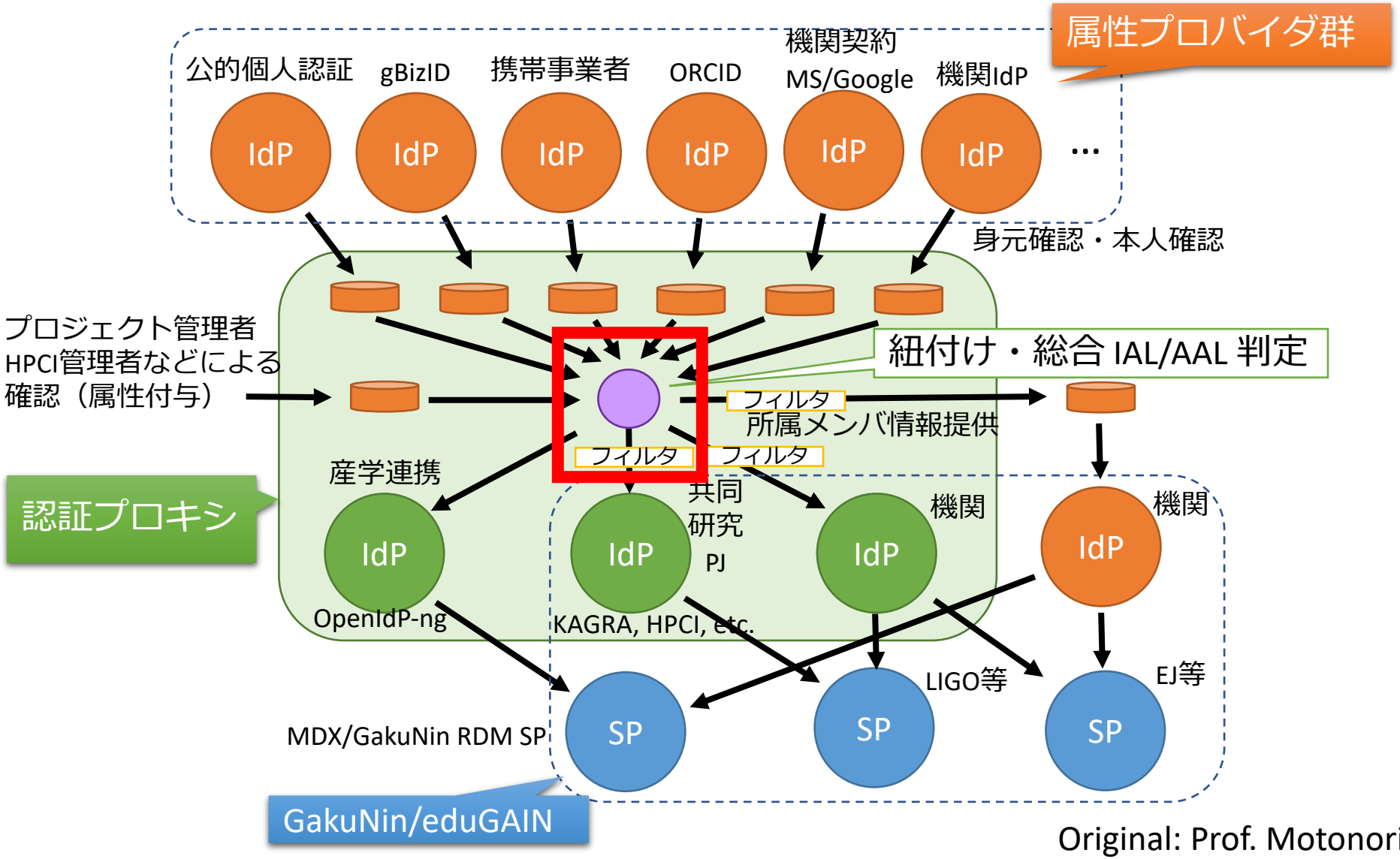
2022/01/18

認証プロキシサービスの研究開発

- 背景
  - 既に独自のトラストフレームワークをもつ研究コミュニティやプロジェクトが存在する。国家規模での認証エコシステム構築にむけて、たとえば IdP の機能を、大学・研究機関の IdP に置き換えるのは容易ではない
    - ポリシ・マッチングが自明ではない
    - 大学・研究機関 IdP と研究コミュニティ SP との調整が煩雑（両者の視点から）
  - 研究コミュニティでは産学連携は特別なものでない

- 目的
  - 産学連携を念頭においた SP への Id 連携時に必要な Id 保証の担保などに柔軟に対応する
    - IAL, AAL matching, AL enhancement
    - credential bridging (e.g., OAuth access token -> SAML assertion)
  - 既存の研究コミュニティのもつトラストフレームワークにおいて、Id 基盤部分を外だしできるようにする
    - 本人確認手続きを外部に依拠する
- 方法
  - 既存 IdP や gBizID 等と各種 SP の間に配置する認証プロキシサービス (IDaaS) を導入する
- 基本機能要件
  - 利用者と Id の紐付けできること（複数の Id にも対応：Id 連携）
  - 総合 IAL/AAL 判定できること
  - 属性保証ができること
  - それぞれの関係者が必要な設定を行えること

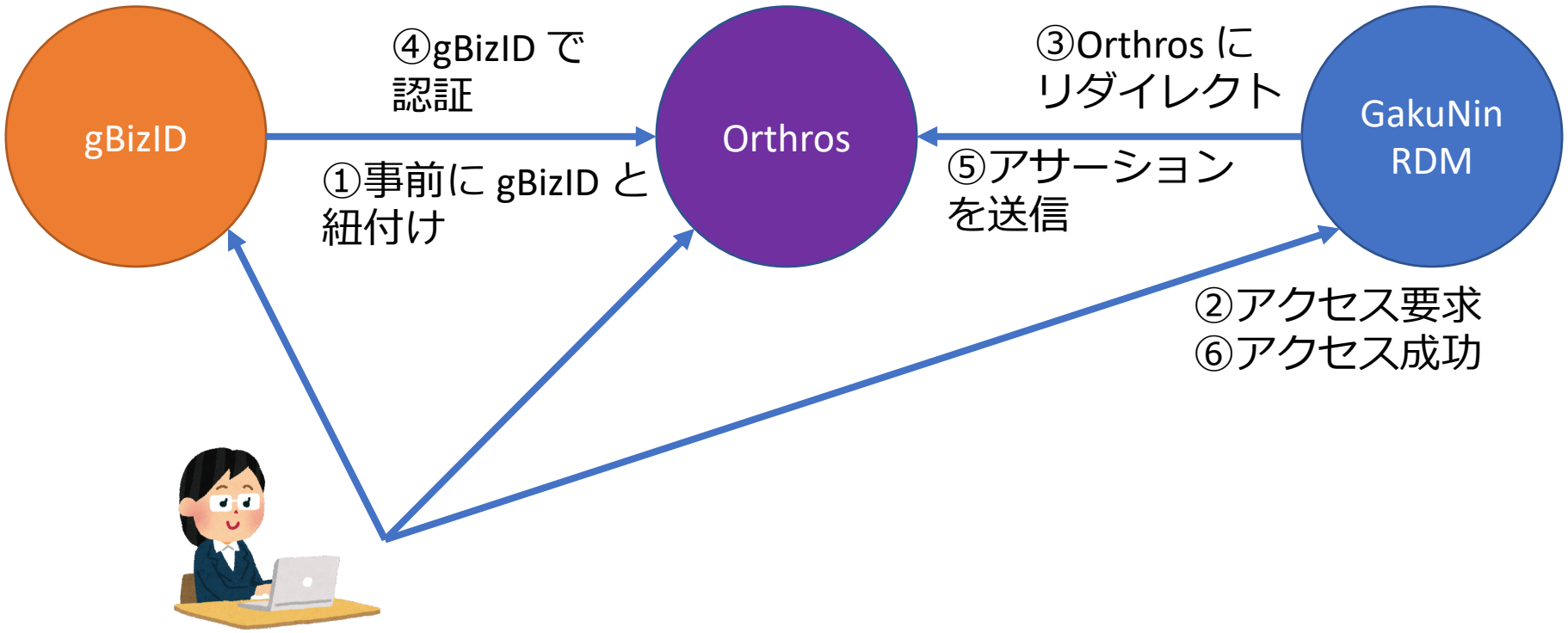
認証プロキシのデザイン案



Original: Prof. Motonori Nakamura

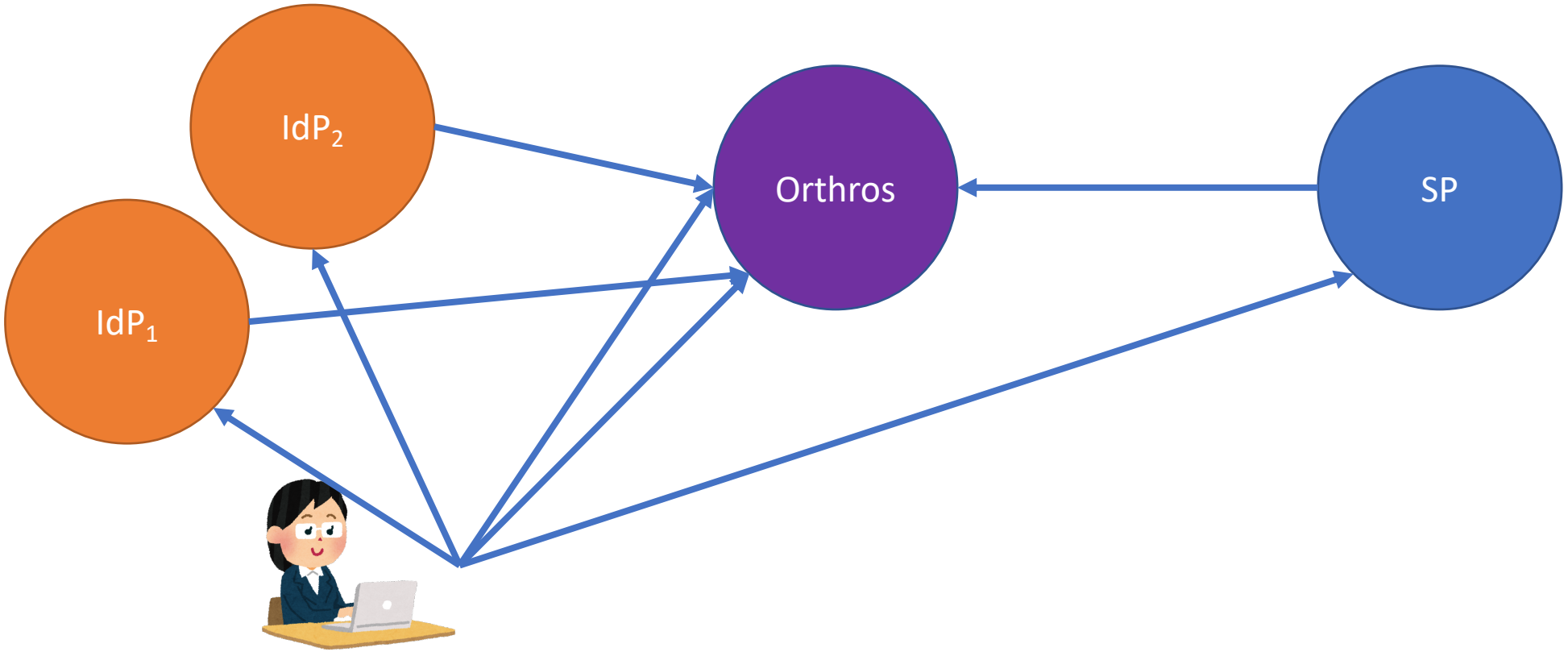
ユースケース１ - credential bridging

- 企業の研究者が GakuNin RDM を利用する



ユースケース２ - IAL enhancement

- 複数の Id を紐づけることにより、SP の要求 IAL, AAL に対応する



次世代認証連携における認証プロキシ実装

- 認証プロキシサービスの基本機能の設計・試作完了
  - 認証プロキシコア部 (IDaaS) - **SELMID**
    - ID 登録、ログイン、ID 紐付け、ID 紐付け解除、属性更新
  - 各種機能設定インターフェイス部（マイページ機能）

- 今年度の開発
  - 機能要件定義
    - GakuNin RDM での実運用
  - 産学連携研究プロジェクトを想定し、実証評価実験を実施
    - 企業の研究者の方が、認証プロキシサービスを利用してサービスにアクセス
    - 2022 Open Forum にてデモ実施予定
  - 接続 IdP
    - gBizID, ORCID
  - 現行 OpenIdP からの移行・切り替え
  - R04年度からパイロット運用

FY21 エンハンス事項一覧

SELMID

1. SP管理機能（管理者向け機能）
   - SP毎に要求するIALおよびAALを設定する機能
2. SP単位の同意管理機能
   - 利用者がSPに初回ログインする際に同意を取得する機能
   - 利用者が自身の同意状態の確認・取り消しが出来る機能
   - 管理者が機関内のユーザの同意状態を確認する機能
3. 属性保証（旧機関管理）
   - 管理者が管理対象ユーザの属性を保証する機能
   - 例）自機関に所属するユーザの所属属性を保証する（招待による確認～属性付与）
4. その他
   - 画面デザイン
   - 現 OpenIdP からの移行・切り替え