NII 学術情報基盤オープンフォーラム 2023
認証トラック３

認証プロキシサービス Orthros

坂根 栄作

国立情報学研究所
アーキテクチャ科学研究系／学術認証推進室

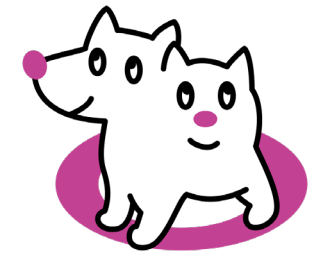
2023/05/30

認証プロキシサービスの研究開発

- 産学連携を念頭においた SP へのアクセスにおいて、必要なID保証の担保やID連携、属性保証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できる

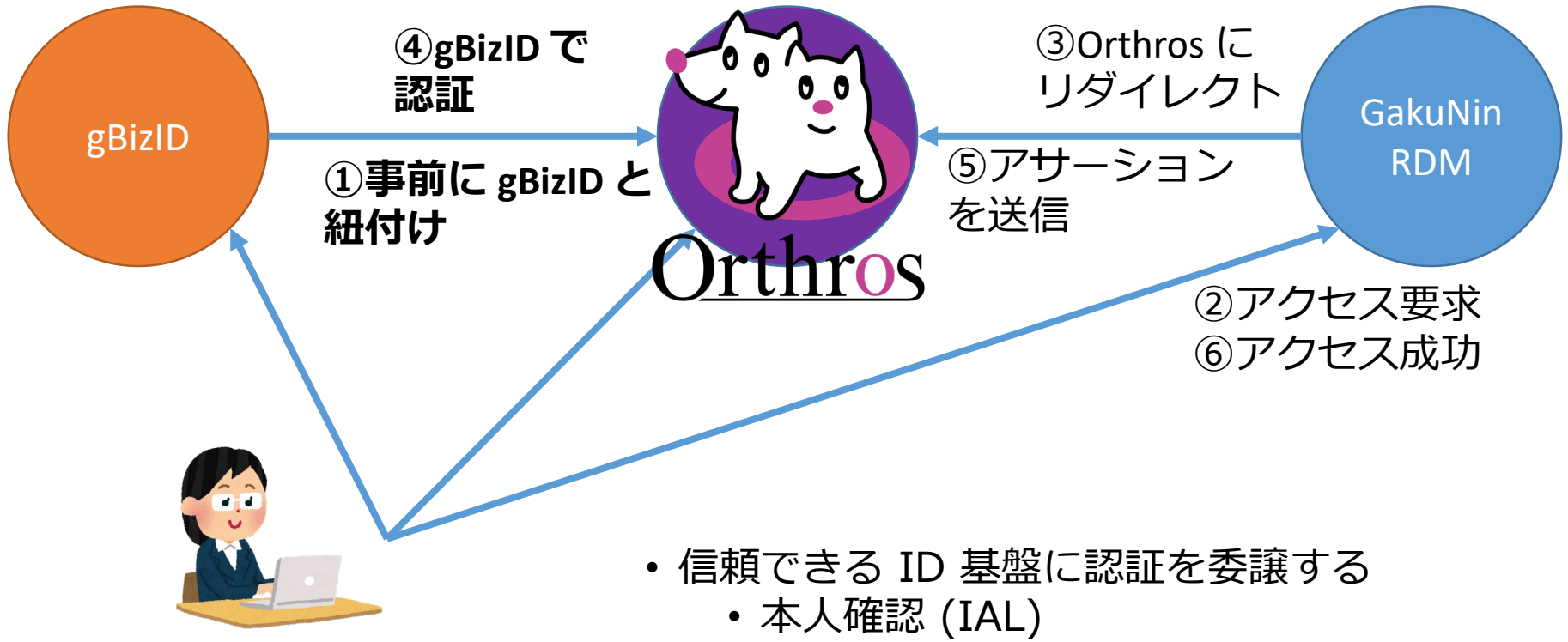
- 認証プロキシサービス “Orthros”



Orthros

ユースケース１ – credential bridging

- 企業の研究者が、既存IDの認証により GakuNin RDM を利用する

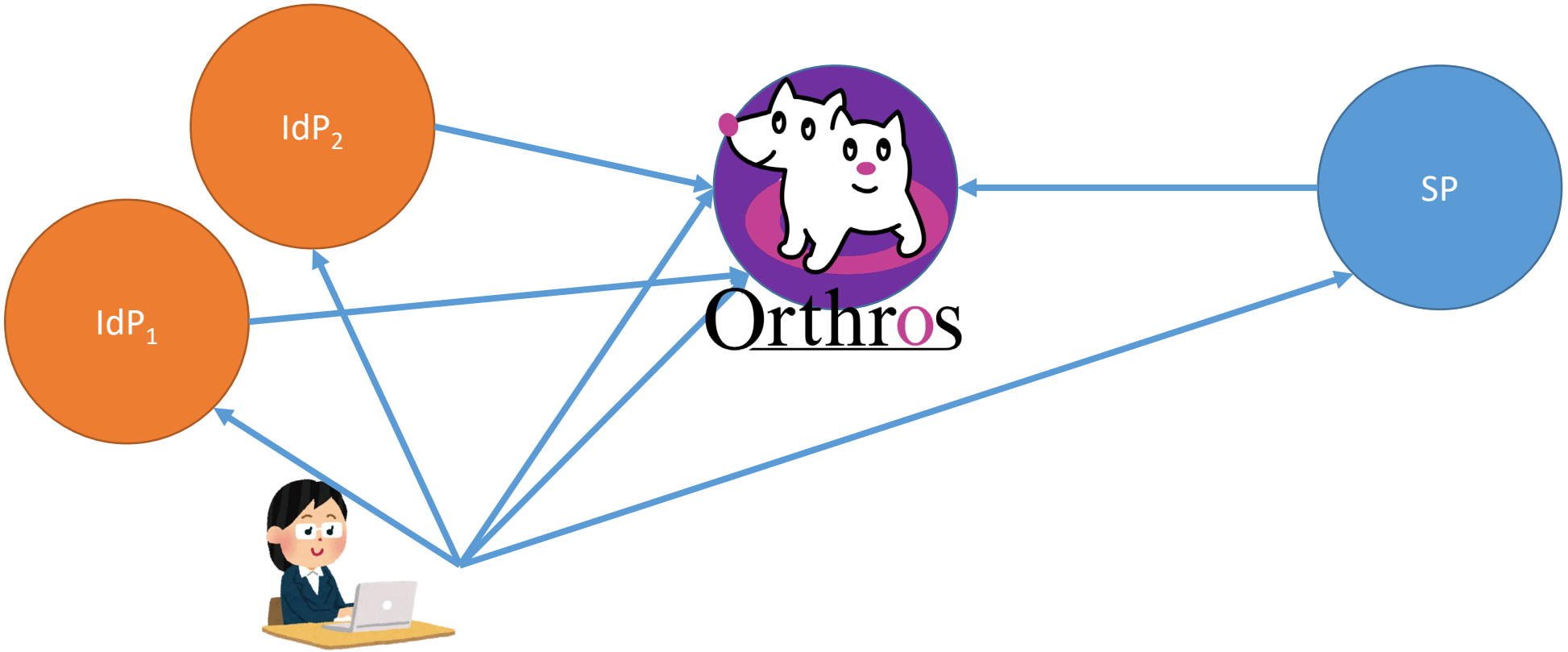


- 信頼できる ID 基盤に認証を委譲する
  - 本人確認 (IAL)
  - 認証クレデンシャル (AAL)

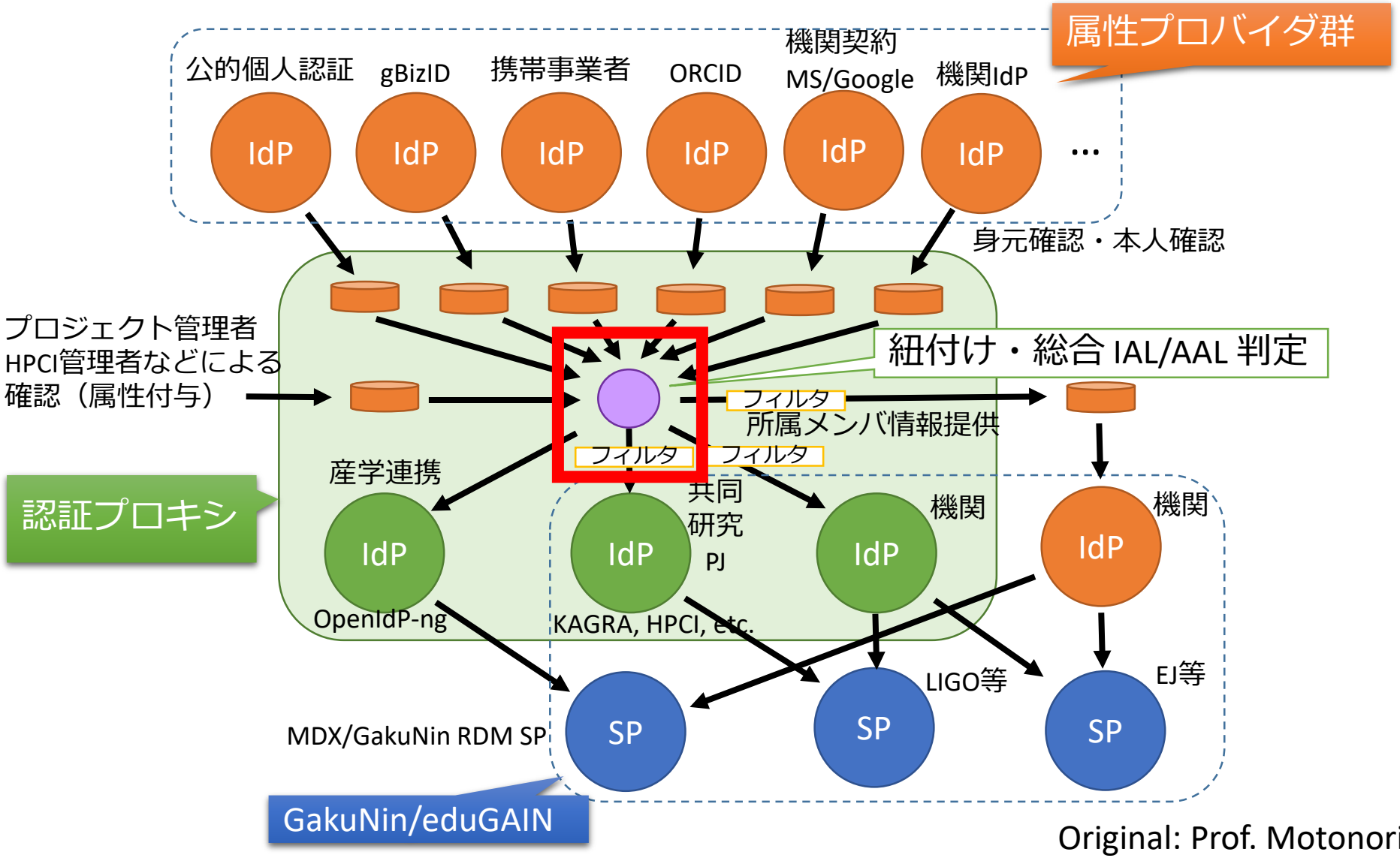
このようなID連携の実現を目指す

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



認証プロキシのデザイン



Original: Prof. Motonori Nakamura

認証プロキシサービス Orthros の設計・実装

- 認証プロキシコア部 (IDaaS) – **SELMID** https://ctc-insight.com/selmid
- 各種機能設定インターフェイス部 (マイページ機能) – 内製

- 基本機能
  - ID 管理、ログイン、ID 紐付け、ID 紐付け管理、属性更新
- 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
- 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
- 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）

Orthros の設計・実装（続き）

- 更なる機能強化
  - メールアドレス変更時の通知機能
  - アカウント停止機能
  - マイページ上に連携済みIdPの情報を表示する機能
  - パスワードの強制リセット機能

- 外部IdPの追加
  - 接続済み：LINE, Google, Yahoo! JAPAN, Facebook, Twitter
  - 調整中：gBizID, ORCiD

- SP の追加
  - meatwiki, GakuNin RDMステージング環境

デモンストレーション

FY2023 整備・開発

- Orthros 本格運用に向けて
  - OpenIdP 移行環境としての機能整理、基盤整備
  - OpenIdP からのユーザ移行準備・支援
  - 本格運用に向けた体制・手順整備
    - 運用ポリシ・運用規程策定

- FY2023 以降
- Orthros 拡張機能開発 – 次世代認証連携対応
  - 外部IdP（GビズID、ORCID）連携
  - SP単位の送出属性選択
  - 異動に伴うHome IdP Binding対応
  - 学認IAL2/AAL2ポリシー対応
  - 認可属性の取り扱い強化