認証プロキシ Orthros とグループ管理 mAP Core

西村 健・坂根 栄作
国立情報学研究所

第14回 統合認証シンポジウム
2022/03/10


認証


認可

Orthros

認証

認可

mAP Core

National Institute of Informatics

認証プロキシサービス
Orthros

National Institute of Informatics

次世代認証連携への要望（研究コミュニティ視点）

- IdP を持たない利用者の認証
  - 利用者は、必ずしも学認に参加する IdP のアカウントを所有しているわけではない
  - 信頼に足る本人確認を行っている IdP に依拠したい
- 認証強度の把握
  - Id & Password か 多要素か
  - 多要素認証を経た利用者のみにサービスを提供する、のようなフィルタリング

- 複数組織に所属する利用者の同定
- 組織異動における利用者の同一性の担保
  - 組織間異動があっても情報資産利活用の継続性を担保したい
    - GakuNin RDM 上の資産を継続的に利用したい

- 用途に応じた属性の提供
  - 例：居住者か非居住者かを把握したい（輸出管理）

IdP 拡大の取組

- 適切な IdP がない利用者をどのように認証するか
  - 学術機関の利用者
    - 所属機関の学認参加を支援
  - 企業の利用者

- 一方で、一般社会には様々な Id 基盤が存在する
  - gBizID, ORCID, Google/Microsoft, SNS, 公的個人認証, 携帯事業者, …
  - これらのプロバイダと連携することで、SP に認証情報を送信

- 利用者は、適切な IdP を選択して SP の認証に利用できるようになる

IdP 強化の取組

- より強い認証に向けて
  - 本人確認の保証度（Identity Assurance Level: IAL）
  - 認証強度（Authenticator Assurance Level: AAL）

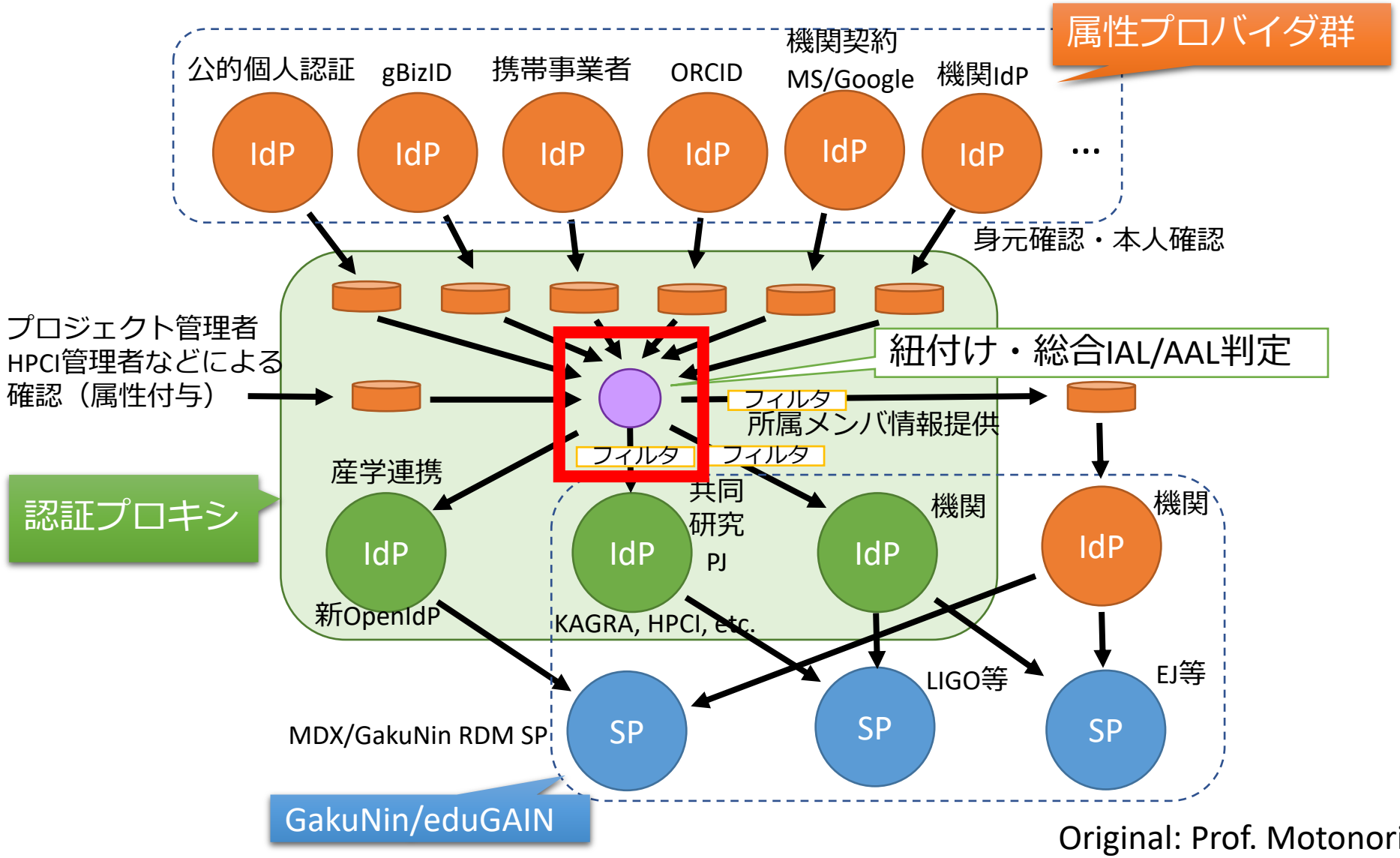
- 本人確認の保証度
  - IdP の IAL 評価基準と認定手続きの確立
  - 単一の IdP で IAL 要件を満たさない場合に、複数 IdP の組み合わせにより IAL を上げる仕組みの検討
- 認証強度
  - 多要素認証の技術支援（導入・運用）
  - 単一の IdP で AAL 要件を満たさない場合に、AAL を上げる仕組みの検討

- 利用者は、適切な保証度の認証で SP を利用できるようになる

認証プロキシサービスの研究開発

- 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できる
- 方法
  - 既存 Id 基盤 (OpenIdP, gBizID, …) と各種 SP との間に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

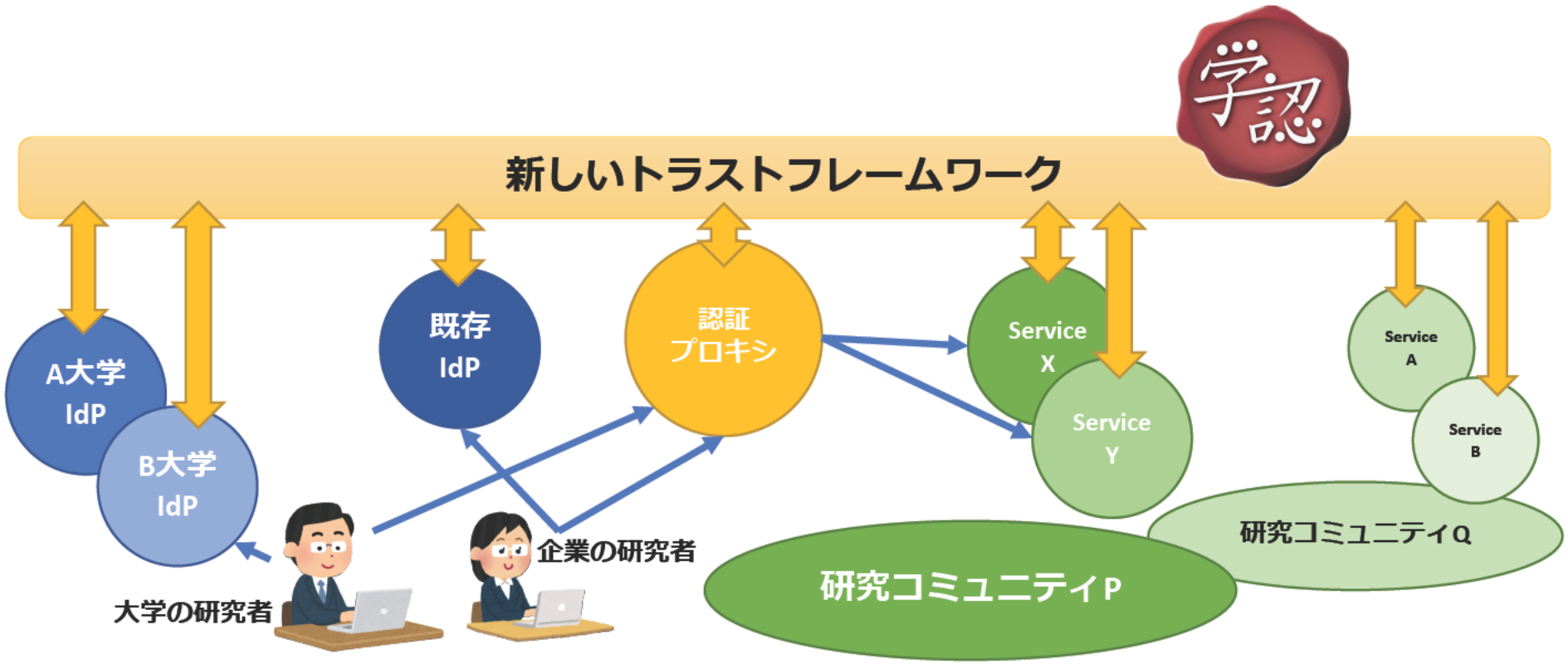
認証プロキシのデザイン案



Original: Prof. Motonori Nakamura

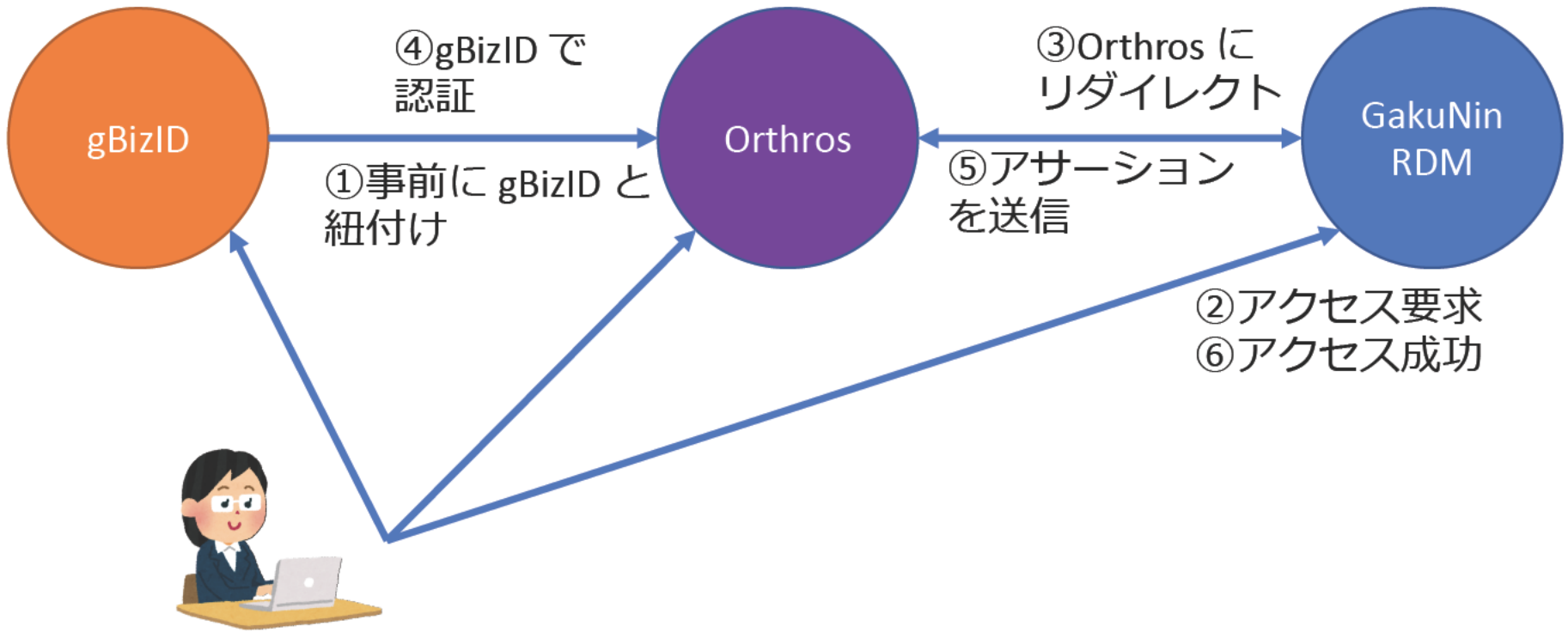
認証プロキシサービスの展開

- 新しいトラストフレームワークにより、関係者間のポリシマッチングの議論が効率的に行える
- 認証プロキシサービスが、研究コミュニティ (SP) と、利用者の所属機関による IdP との橋渡しを行う



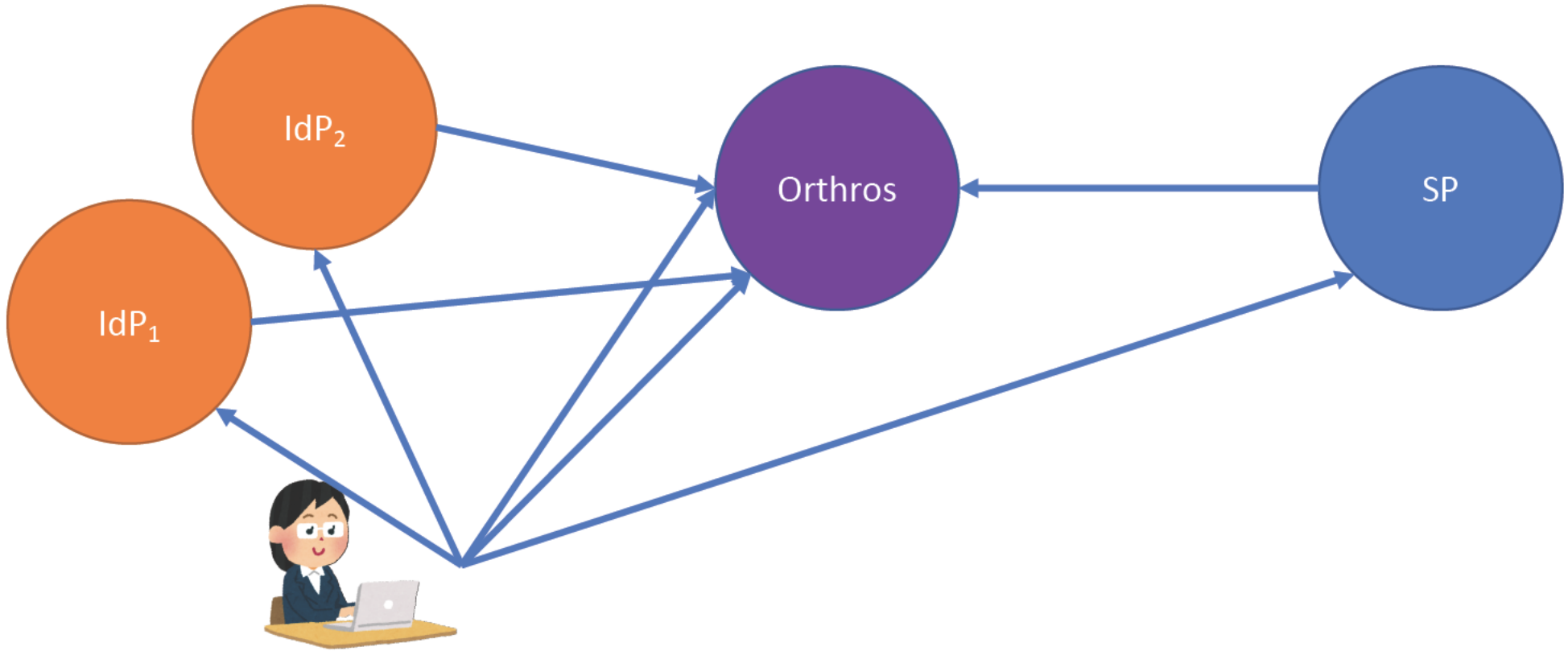
ユースケース１ - credential bridging

- 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) – B2C 事業者向け IDaaS : **SELMID** https://ctc-insight.com/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）

- 今年度の開発目標
  - GakuNin RDM での実運用を目指す
  - 機能要件定義
  - 産学連携研究プロジェクトを想定した認証フローの検証
    - 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

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

まとめ：認証プロキシサービス Orthros

- 認証プロキシサービスの研究開発
  - 実運用に向けた主要機能の実装完了
  - 外部 IdP 接続
    - 接続済 : LINE, Google, Yahoo! Japan, Twitter, Facebook
    - 対応中 : ORCID
- 来年度計画