次世代認証連携への学認の取り組み
認証プロキシサービスの試み

坂根 栄作

国立情報学研究所

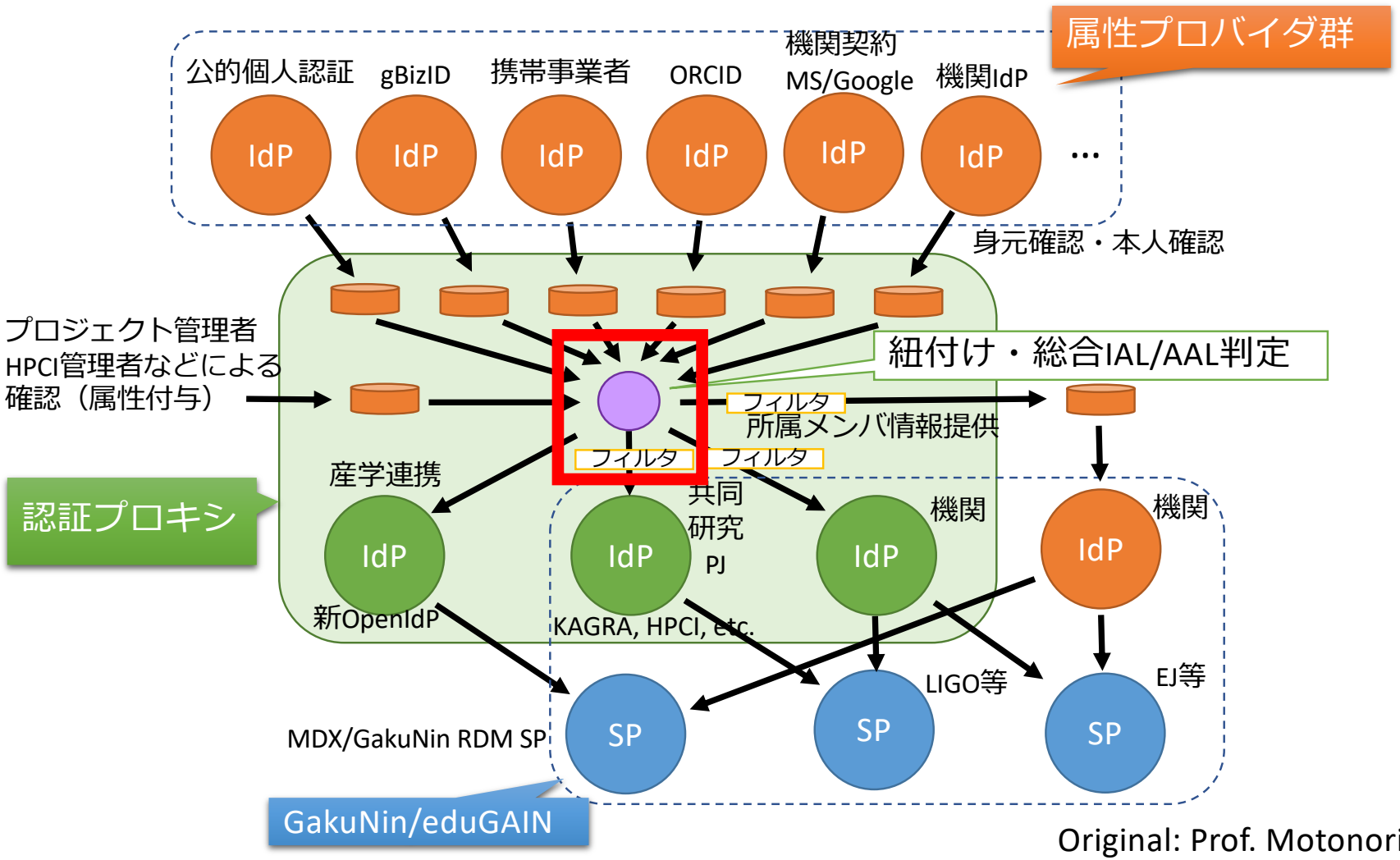
2021/12/17

認証プロキシサービスの研究開発

- 背景
  - 研究コミュニティは独自のトラストフレームワークをもつ。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 との調整は煩雑（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
  - 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
- 方法
  - OpenIdP をはじめとする各種既存 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

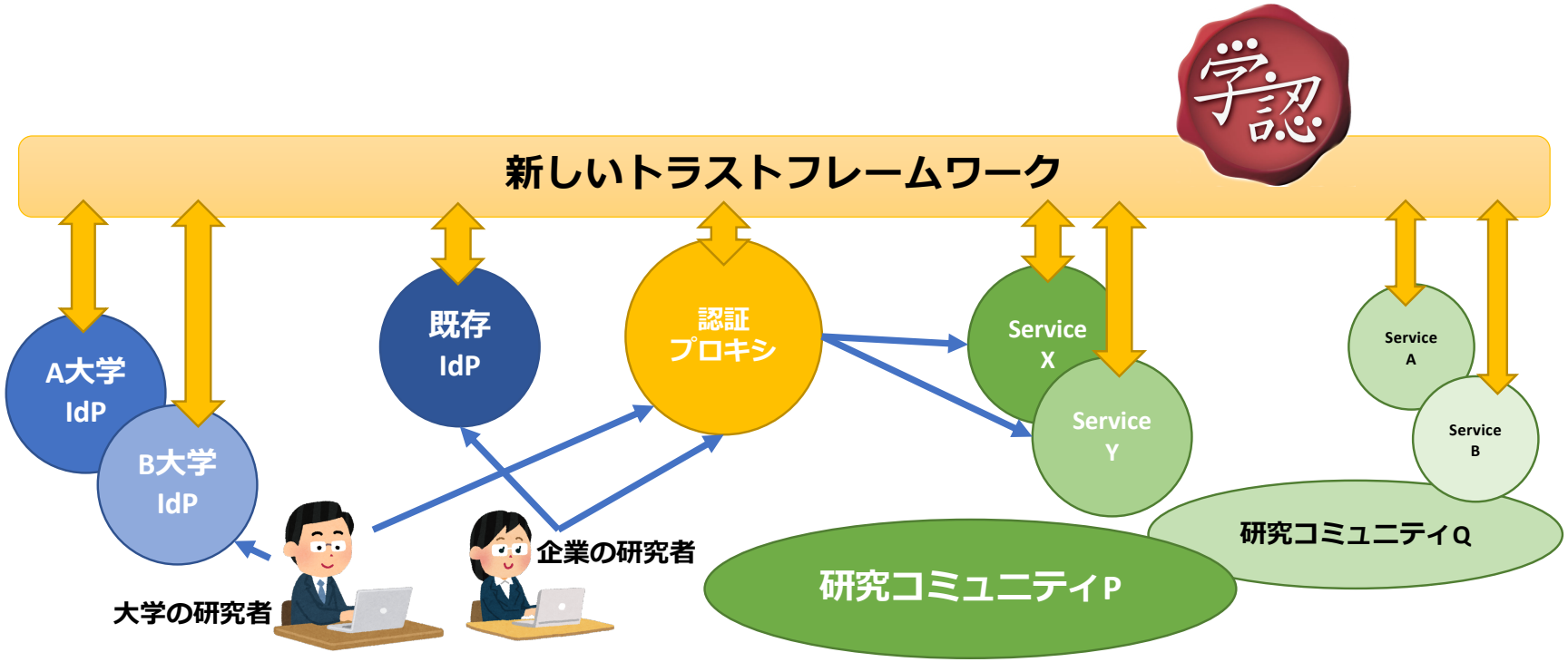
認証プロキシのデザイン案



Original: Prof. Motonori Nakamura

認証プロキシサービスの適用例

- 新しいトラストフレームワークにより、関係者 (Participants) 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



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、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

FY21 エンハンス事項一覧

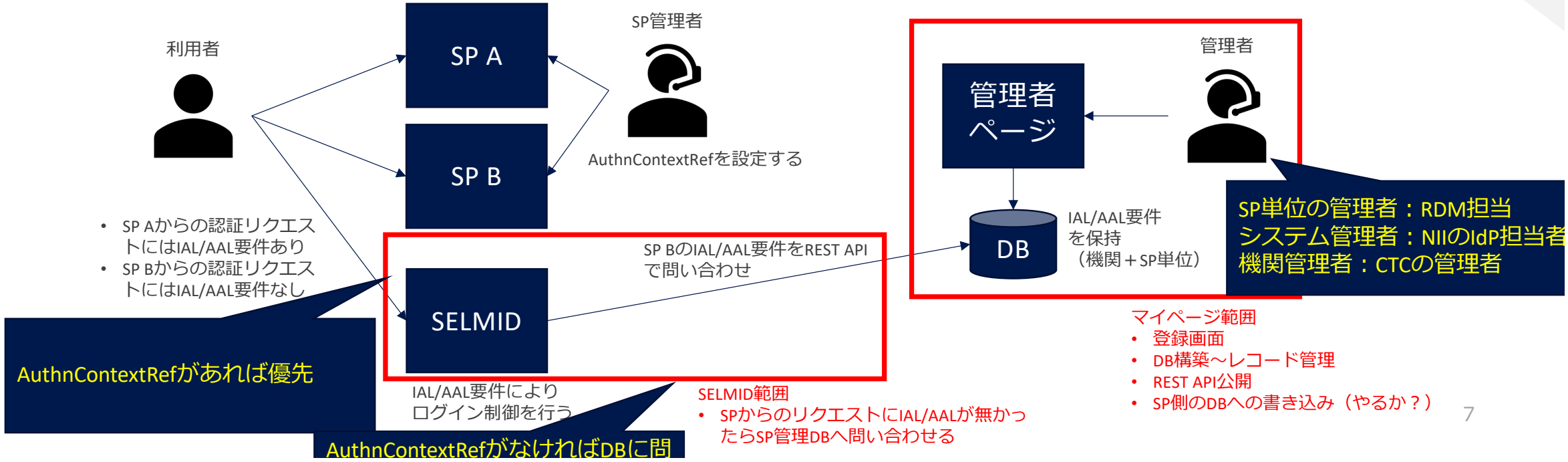
SELMID

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

次のスライドから現在開発中のもの
を含みますのでご留意ください

1. SP管理機能

- 管理者向けSP管理ページからSP毎に要求するIAL/AALを設定する
- 設定したIAL/AALはデータベースへ保持（マイページDB and/or SP側DB）
- 利用者がSPへログインする際にSELMIDで対象SPのIAL/AAL要件をチェックし必要な制御を行う



仕様案

- SPからの認証コンテキスト要求（AuthnContextClassRef）に設定する値
  - 一つの文字列しか設定できないのでIAL/AALの組み合わせ文字列の設定が必要
  - 例）IAL2_AAL2（強度の順番を決める必要あり）
- データベースとのI/F（REST API）
  - メソッド：GET/POSTのみ
  - 認証：Bearerトークン、BASIC認証、クライアント証明書認証
  - SELMID⇒APIへのパラメータの渡し方
    - QueryString、Urlの一部（https://xxx.example.com/{username}）、Form、JSON、ヘッダ
  - API⇒SELMIDへのレスポンス
    - HTTPコード：200 or 4xx
    - JSONをボディで返却

参考）https://docs.microsoft.com/ja-jp/azure/active-directory-b2c/restful-technical-profile

成功

```
{
  “displayname": “Naohiro Fujie",
  “email": “hoge@example.com"
}
```

失敗

```
{
  "version": "1.0.0",
  "status": 409,
  "code": "API12345",
  "requestId": "50f0bd91-2ff4-4b8f-828f-00f170519ddb",
  "userMessage": "Message for the user",
  "developerMessage": "Verbose description of problem and how to fix it.",
  "moreInfo": "https://restapi/error/API12345/moreinfo"
}
```

仕様案

- SP管理データベースの構造
  - SP共通
    - SPのID（SAMLRequest内のProviderNameと同じ値）
    - AuthnContextClassRefの初期値
    - 初期値以下のレベルの設定の許可・不許可フラグ
  - 機関単位
    - SPのID（SAMLRequest内のProviderNameと同じ値）
    - 機関名（SELMIDに持つ所属組織名と同じ値）
    - AuthnContextClassRef
  - AuthnContextClassRefの値（SAMLRequestに入るものと同じ値）

APIとしてはレコードが存在しなかったら初期値を返却

複合キー

仕様案

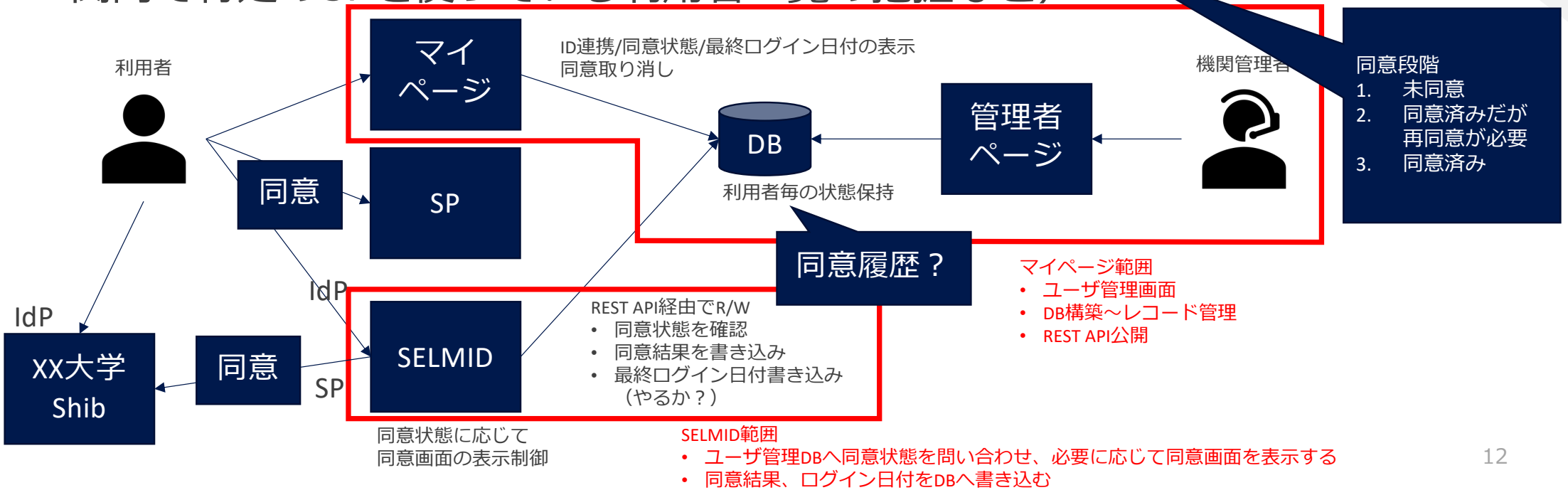
- 認証コンテキストの優先順位（SELMID内の処理）
  1. SPからの認証要求
  2. ユーザ認証（IAL、所属情報の取得）
  3. 認証要求内にAuthnContextClassRefがある
     - コンテキストに応じたユーザ評価（IALを満たさない場合はブロックor追加IAL要求）
  4. 認証要求内にAuthnContextClassRefがない
     - SP、所属情報（機関名）を使ってデータベースからAuthnContextClassRefを取得
     - コンテキストに応じたユーザ評価（IALを満たさない場合はブロックor追加IAL要求）
  5. AALの要求レベルに応じて多要素認証の強制

仕様案

- 管理機能の利用範囲
  - SP管理者
    - AuthnContextClassRefの初期値設定
    - 初期値以外の値を機関管理者が設定可能かどうかのフラグ設定
      - すべての機関に対して許可
      - 特定の機関に対して許可
    - 初期値を下回る値を機関管理者が設定可能かどうかのフラグ設定
      - すべての機関に対して許可
      - 特定の機関に対して許可
  - 機関管理者
    - SP管理者が設定を許可していない場合
      - 設定値の閲覧
    - SP管理者が設定を許可した場合
      - 初期値以外の値を設定
  - システム管理者
    - SP管理者、機関管理者の替わりに設定可能

2. SP単位の同意管理機能

- 利用者がSPに初回ログイン時にID連携に関する同意を取得する
- 利用者がマイページから自身のID連携/同意状態の確認、取り消しが出来る
- 管理者が自機関に所属する利用者のID連携/同意状態の確認が出来る（自機関内で特定のSPを使っている利用者一覧の把握など）



仕様案

- 同意管理データベースの構造
  - ユーザID（ePPN※SP側に出力するID）
  - SP（ProviderName）

  } 複合キー

  - 同意状態（1/未同意、2/同意済みだが再同意が必要、3/同意済み）
  - 同意済みの規約バージョン
  - 同意日付
  - 最終ログイン日付
- 要決定事項
  - 同意履歴を持つかどうか
- DBとのI/F
  - 前述と同様

仕様案

- 同意規約バージョンの管理
  - 規約を変更した場合はSELMIDにHTMLの設定、規約バージョンを更新する
  - ユーザの同意済みバージョンと最新規約バージョンを比較し、再度同意を求めるかどうかを判断する
- SELMID内の処理
  - SPからの認証要求
  - ユーザ認証
  - APIでDBから同意状態を取得
    - 同意バージョンの比較：同意バージョンが古ければ再同意を求める
    - 同意状態の比較：未同意、同意済みだが再同意が必要なら同意を求める
  - 同意の取得
    - 規約の表示、同意状態保存の選択（毎回同意させるかどうか）
  - APIでDBへ同意状態を保存

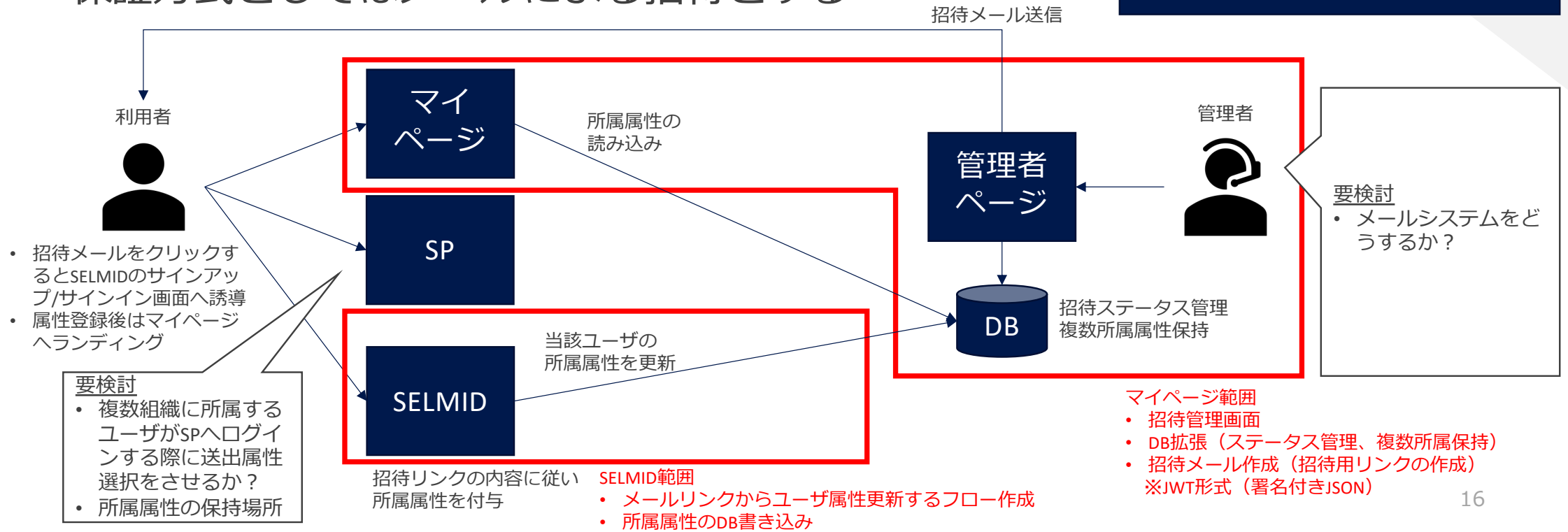
仕様案

- 管理者機能
  - 機関管理者
    - 自機関に属するユーザのSP利用状況を一覧表示、ダウンロード
      - 検索時点でSPに同意済みのユーザ一覧
        - 同意フラグ状態、同意日付、同意対象規約、最終ログイン日付
- 利用者向け機能
  - 自身が利用しているSP一覧の表示
    - 同意済みSP一覧
      - 同意フラグ状態、同意日付、同意対象規約、最終ログイン日付
  - SPへの同意状態の変更
    - 同意フラグの再選択
      - 未同意、同意済みだが毎回再同意、同意済み

3. 属性保証（旧機関管理）

- 機関管理者がユーザの属性を保証するための機能
- 本ステップでは自機関に所属していることを保証する
- 保証方式としてはメールによる招待とする

継続検討？
来歴管理も持つ？
アカウント選択？
⇒ミニマム・オプションのパターン



仕様案

- 要検討事項
  - 複数組織からの招待を受けるか
  - シンプル実装にするなら後勝ちで所属をシングルバリューで持たせる形
  - 将来的には機関単位で所属を持てるようにするべき？
  - 複数組織に登録できる場合、IALとの関係は？（誰がその人のIALに責任を持つのか）
    - SP単位、組織単位でIAL/AAL要求があった場合は特に
- 導入ステップ案
  1. **まずは単一組織からスタート**
     - この時点では基本は組織単位でアカウントを使い分けてもらう想定
     - ePPNは変えずにメールアドレスを付け替えてもらうことでSP側でのデータ保全
  2. 複数組織からの招待を同一メールアドレスで受けられるようにエンハンス
     - SPへ連携する場合、どの組織の構成員としてアクセスするか選択できる画面が必要
     - 同時に同意状態（どの組織として同意したか）、などの整理も必要
  3. ePPNの複数化、IALの調整
     - ePPNと組織とIALのセットをDB管理
     - 外部IdP（GビズIDなど）でIALをセットする際もどの組織に所属している人として保証されるか選択

仕様案

SELMID

- 要決定事項
  - 機関名、機関コードの払い出し、マスタ管理？
    - 誰が最初に機関名を決定するのか？
      - 例）最初にアカウントを作った管理者がNIIに申請し、NII管理者が対象アカウントに機関を割り当てる
  - 利用するメールシステム
    - NIIのメールシステムを使えるか？
    - 送信APIでメールを送信する仕組みが存在するか？（SendGridのようなメール送信APIがあるか？）

仕様案

SELMID

- 一連のフロー
  - 機関管理者
    - 招待対象者のメールアドレスをデータベースから検索
      - 既に存在する場合
        - 自機関に所属している場合：操作不要
        - 自機関に所属していない場合：
          - 現所属の表示（確認のため）
          - 招待の送信　⇒招待中フラグを管理DBにたてる
      - 存在しない場合
        - 招待の送信　⇒管理DBにレコードを作成し、招待中フラグをたてる
  - 利用者
    - 招待メールを受け取りURLをクリック
      - 既にOrthorosにアカウントがある場合
        - ログイン⇒　id_token_hint内に設定されたメールアドレスとログインした人の一致をチェック
      - アカウントがない場合
        - サインアップ⇒　対象者のメールアドレスにワンタイムコードを飛ばしアドレス所有確認
    - ログイン・サインアップした利用者の所属属性にid_token_hint内の機関コードが設定される
      - 設定が完了したら管理DBの招待完了フラグをたてる

招待メール内のリンク
https://{SELMIDのアドレス}?id_token_hint={エンコード/署名されたJSON}

Id_token_hintの内容（抜粋）
{
“id”: “{対象者のメールアドレス}”,
“organization”: “{招待する機関コード}”
“exp”: “{有効期限}”
}
⇒このJSONをエンコードしデジタル署名する（ライブラリ有）

仕様案

SELMID

- 管理DBの構造（基本はユーザDBへのカラム拡張）
  - 招待状態（招待中、完了）
  - 招待日付
  - 完了日付

まとめ

- 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 Id 連携時に必要な Id 保証の担保などに柔軟に対応する
  - 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

- 2022年度 Open Forum にてデモンストレーションを予定！

Orthros