グループ管理機能高度化について

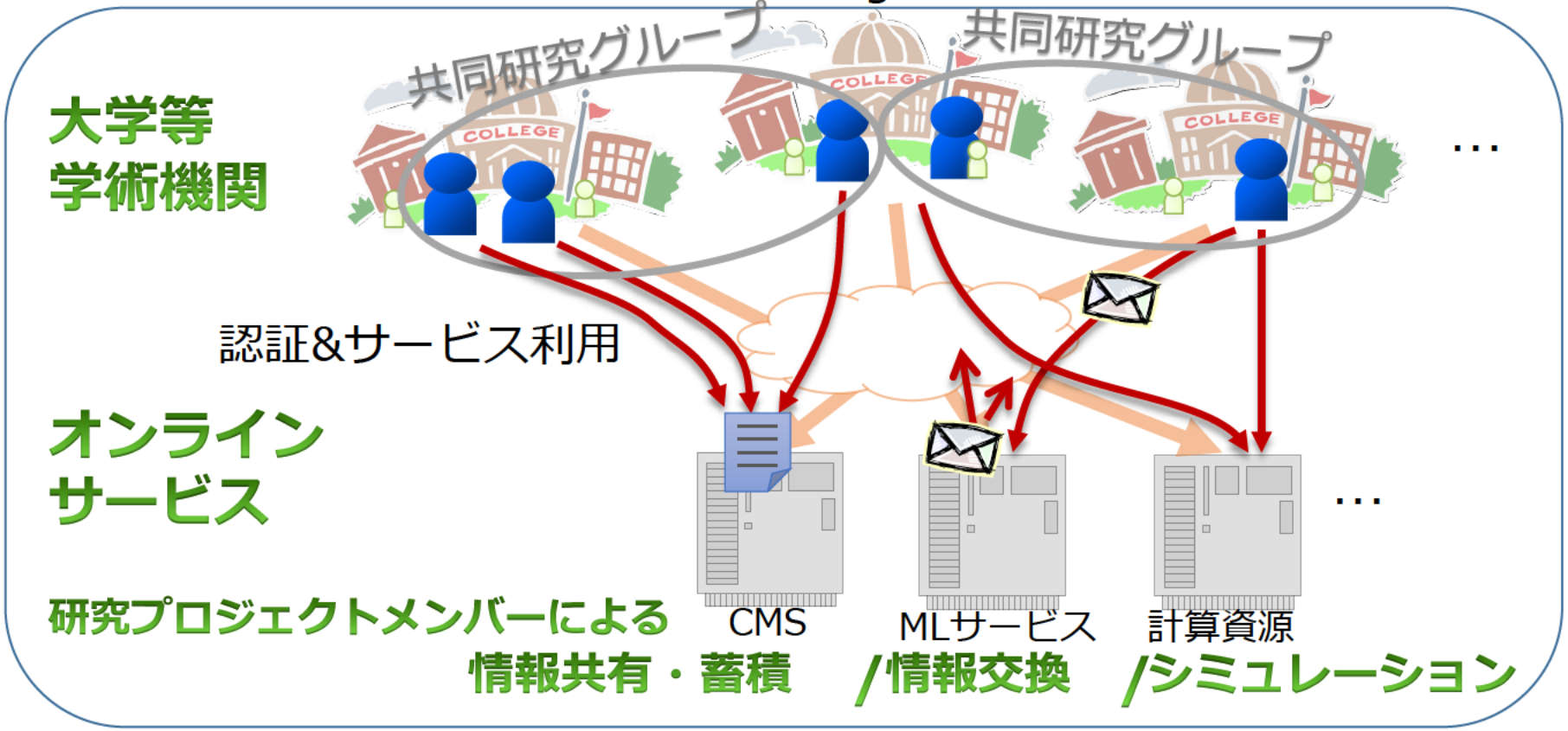
2023.5.30 NII学術情報基盤オープンフォーラム2023

国立情報学研究所　西村健

学認グループ機能の目指すところ：研究教育活動を支援するサイバースペースの提供

研究教育活動支援の各種オンラインサービスが簡単に利用できる場

- 研究活動/教育活動 - 例えば
  - 研究プロジェクトの推進（情報共有、情報交換、スケジューリング、計算資源利用）
  - 論文作成（文献検索、文献閲覧、収集・蓄積）
  - 講義の実施（履修登録、資料提供、e-Learning）

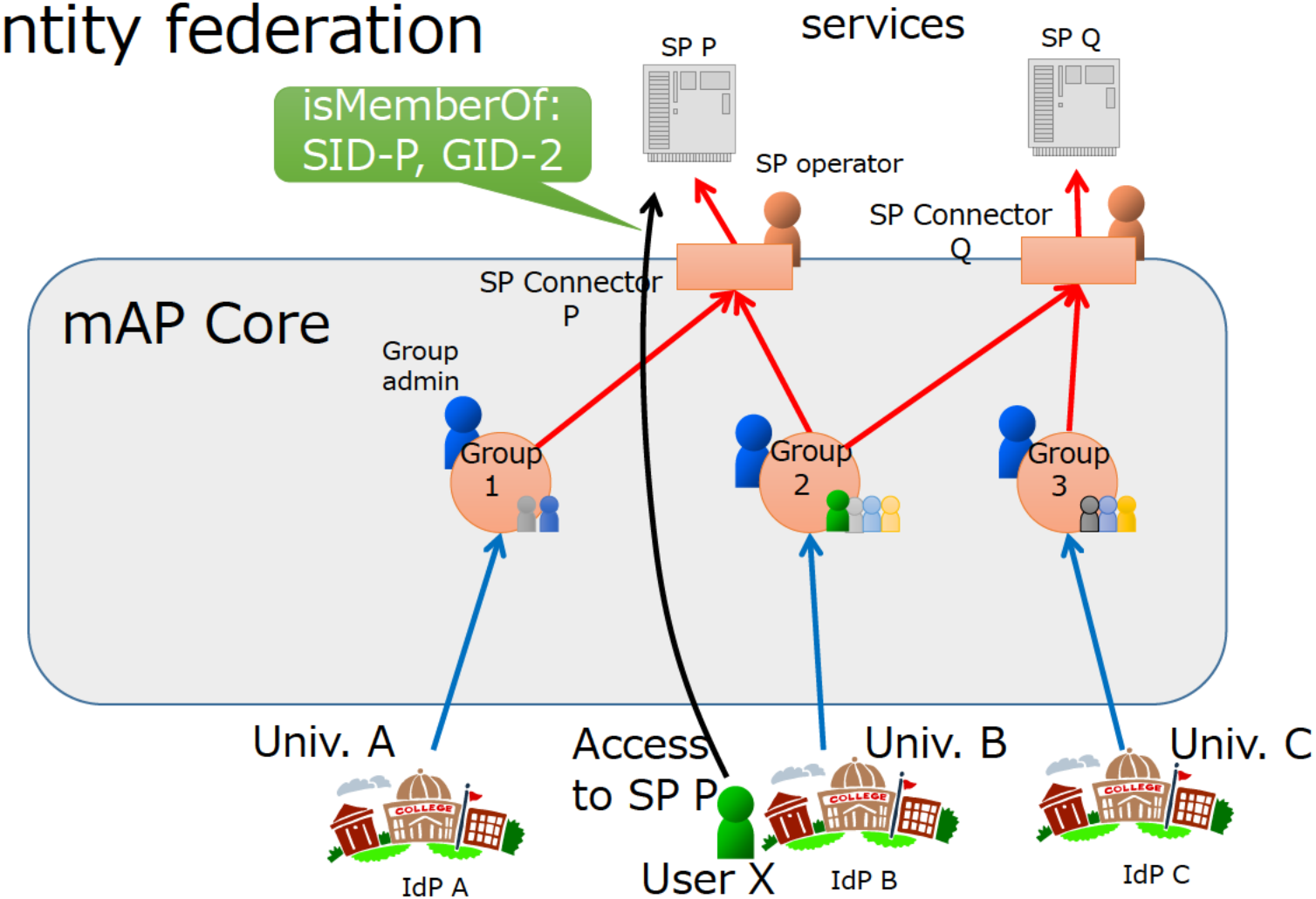


学認のグループ機能の変遷

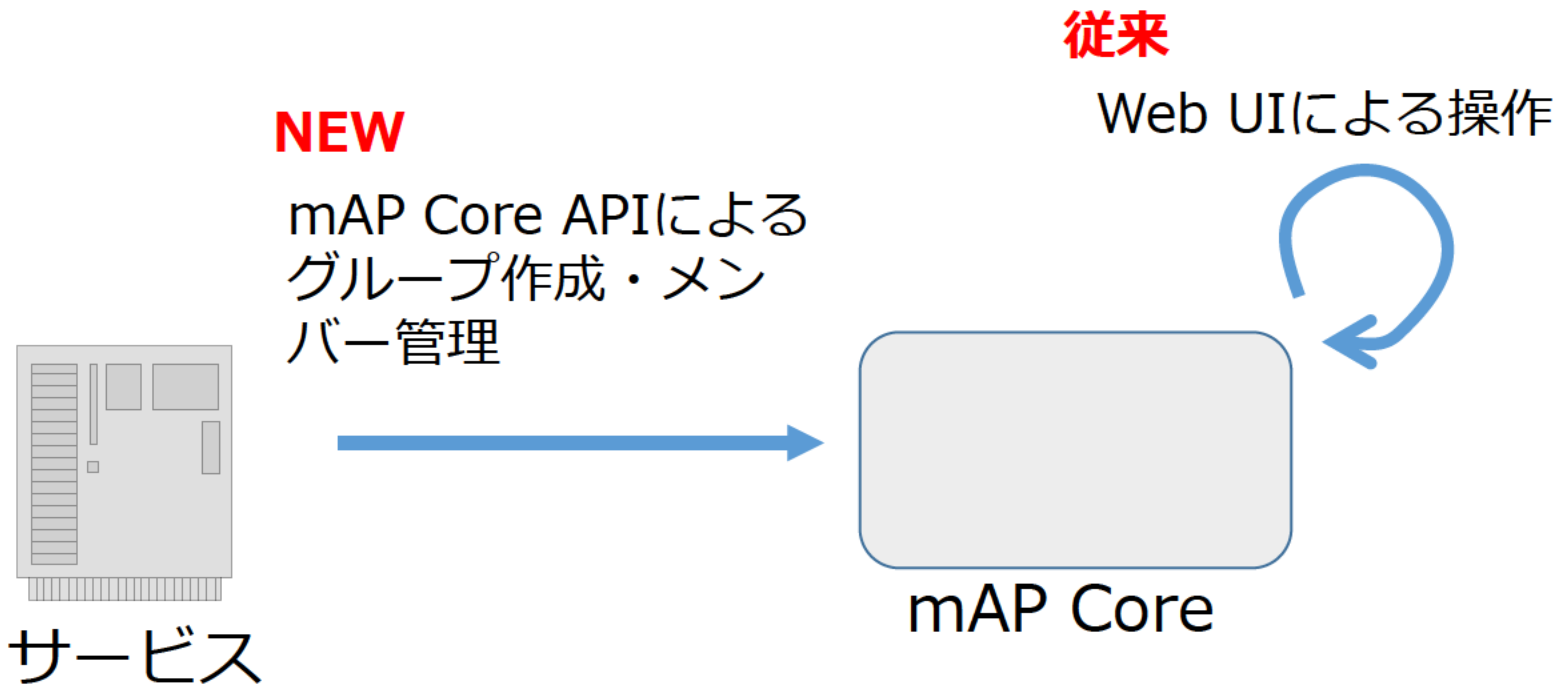
- 今回の内容は以下を包含します
  - GakuNin mAP
  - 学認クラウドゲートウェイサービスのグループ機能
  - mAP Core
  - （今後）
- グループ機能：共同研究グループなど学認のIDの任意の集合を「グループ」として扱い学認参加SPに対してグループ情報・メンバー情報を提供する
  - 利用例：
    - グループ機能対応Wiki
    - グループ機能対応メーリングリストサービス
    - 実習システム
    - GakuNin RDM
    - 大学Moodle
  - 全てのSPが全ての情報を取得できるわけではなく、グループが利用するSPを選択しそのSPに限って情報提供する（情報の保護）

学認のグループ機能の現状：mAP Core

- provides membership information of groups to services within an identity federation

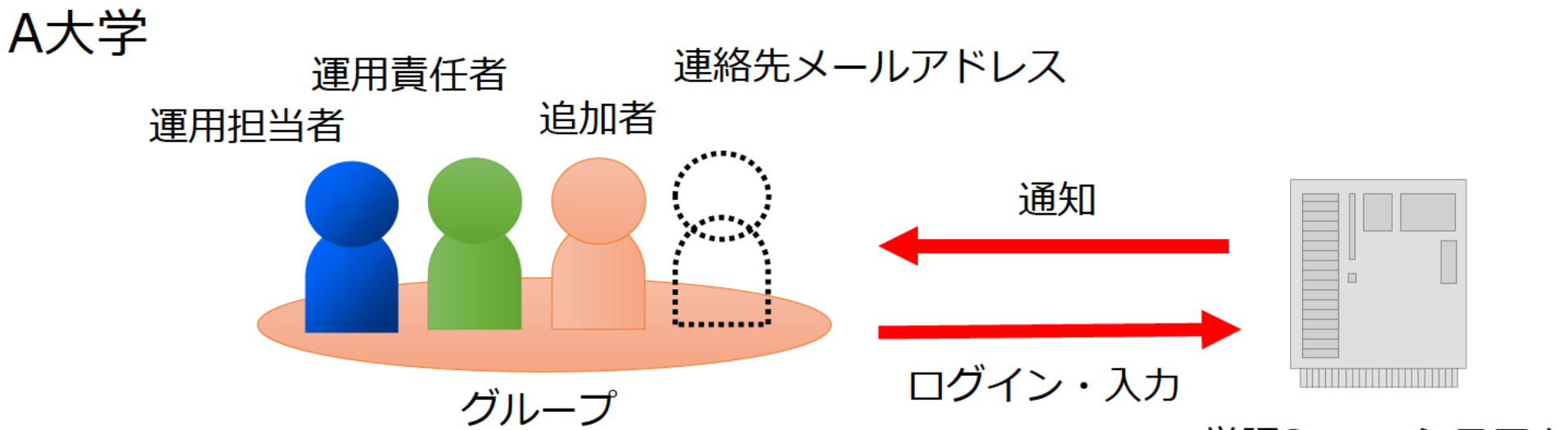


mAP Core API


従来
Web UIによる操作
NEW
mAP Core APIによる
グループ作成・メン
バー管理
サービス
mAP Core

接続例：学認Surveyシステム

- 各参加機関の担当者（運用担当者・運用責任者）に対して調査
  - ・アンケートを行うシステム
  - 担当者をグループとして、認証した上で入力させる
  - 適格者を自分で追加・削除することが可能
  - 通知先メールアドレスを追加可能
  - 例年行っている学認参加IdP運用状況調査に利用

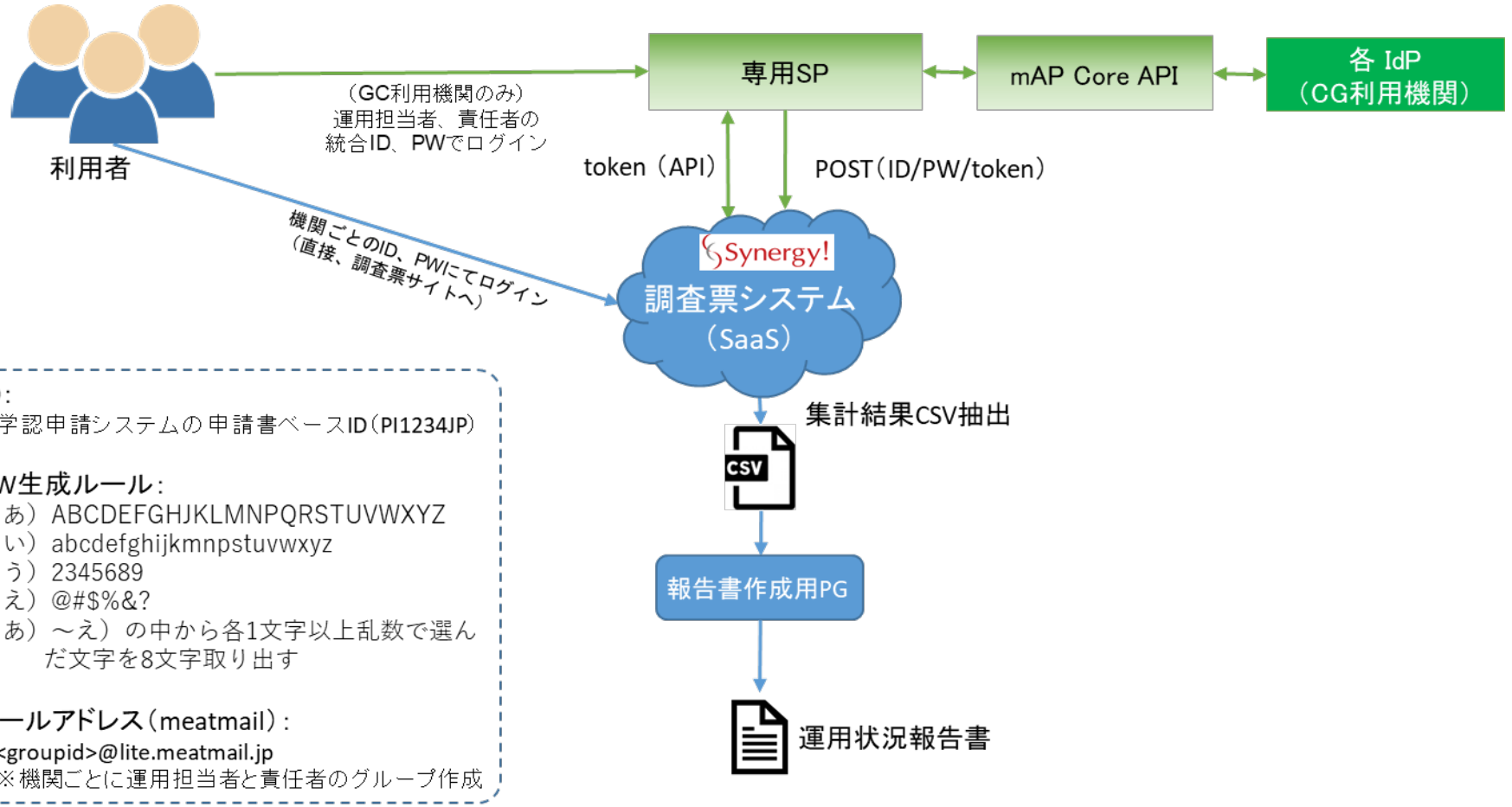


学認Surveyシステム（続き）

- mAP Core上に機関の数だけグループを作成する
- 通知には既存MLサービスであるmeatmailが利用できる
- 認可のためのグループ情報をmAP Core APIで取得する

APIを利用した学認Surveyシステムとの連携

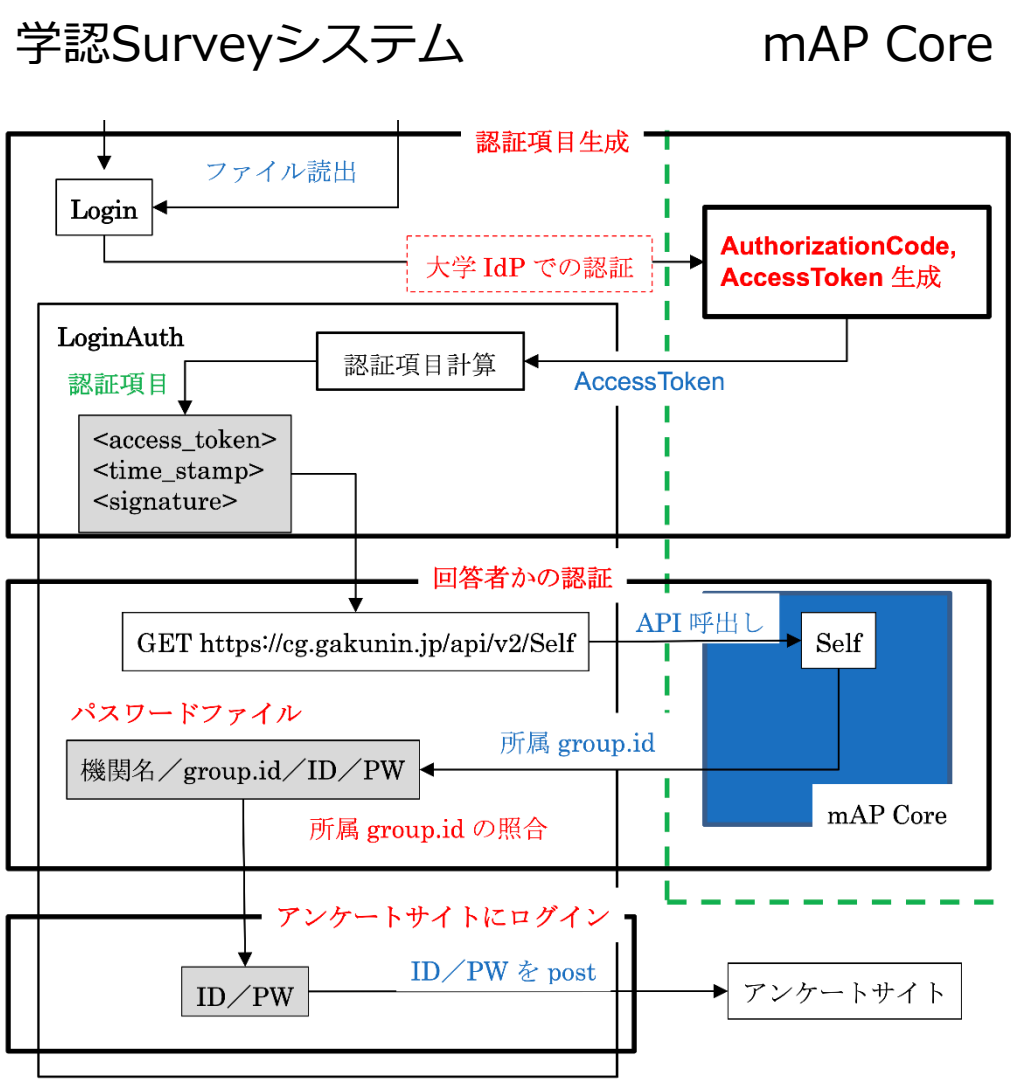
- 調査票システムはSaaS
- 専用SPが仲介となる



APIを利用した学認Surveyシステムとの連携（続き）

- 専用SP自身はIdPから属性をもらわない
  - mAP Coreで認証を行う
  - 専用SPはmAP Coreからグループ情報をもらうのみ

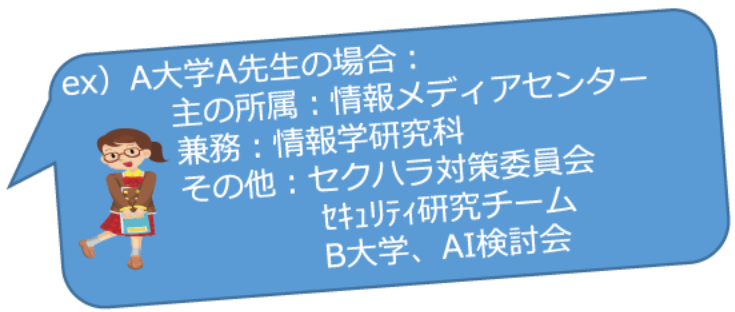
⇒新たな連携方法の可能性



グループ機能の拡張に向けた背景と課題

- 課題１：グループ管理者のメンバ管理の負担を軽減したい
  - mAP Core（少人数の研究などのグループ向け）では、メンバ情報は個々に管理が必要
  - メンバを個々に管理する場合、グループ管理者の作業負担大
    - メンバの追加、削除漏れ等の可能性大

- 課題２：所属などの属性を基にしたグループを容易に作成し、認可に使用したい
  - SP側で、学部、学科、センター等（もしくはもっと小単位）の単位で認可が求められるようになってきた
  - mAP Coreでは、所属などの属性を用いたグループ作成を行うことが難しい
    - そもそもIdPには認可に使用できる所属などの属性情報を持っていない
    - （ただし、IdPは組織単位での認可は可能）

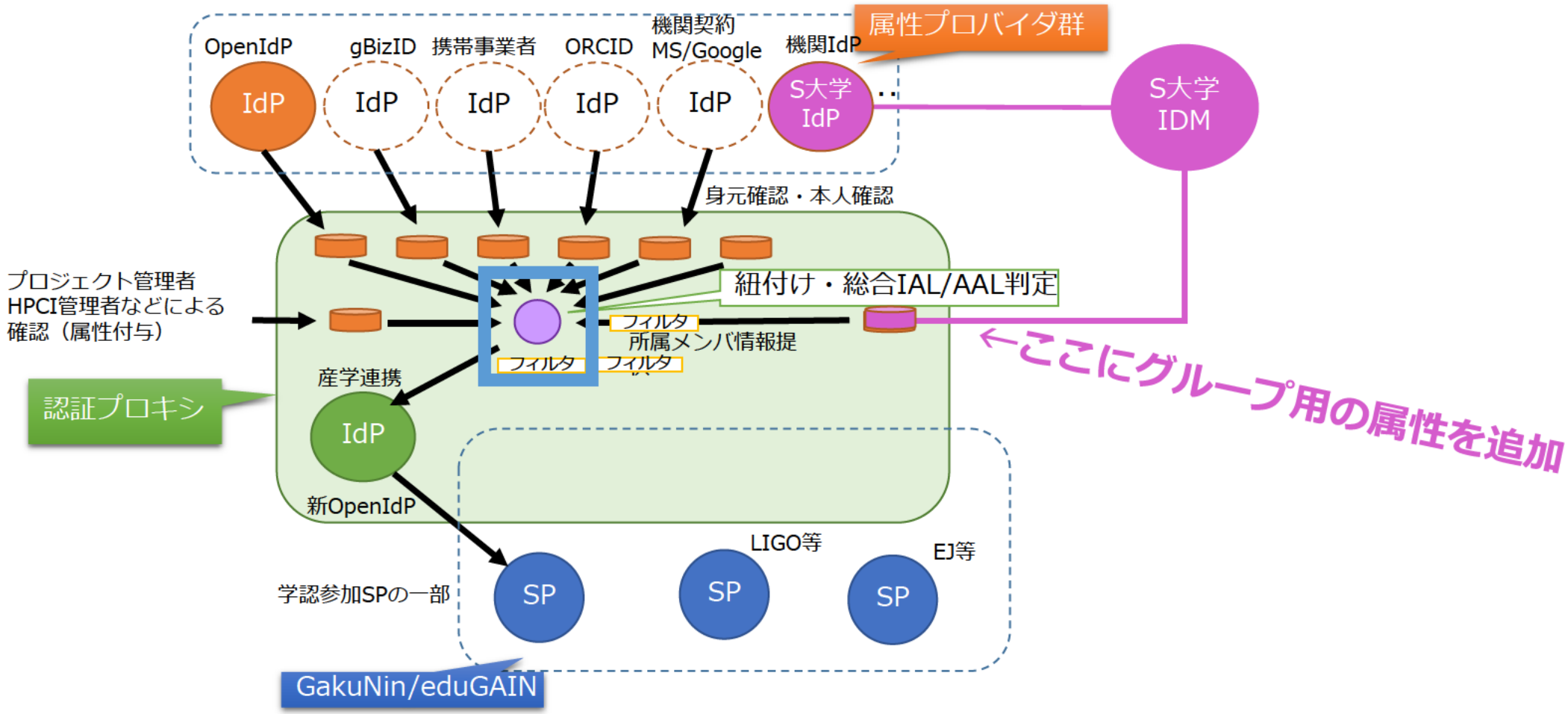


  - 人は様々なグループに所属しており、全てを管理するのは困難
    - 認証基盤DBでは主の所属のみ管理されている場合が多い
    - 実際は主の所属以外の単位で動くことが多い（A先生は授業は情報学研究科で行うなど）
    - 組織(事務)として、把握が難しいグループがある（A先生はセキュリティ研究チームに参加しているなど）
    - 組織外のグループに所属している場合もあり

課題解決に向けて

- まずは、SPが求める利用範囲（学部、学科、センター等 （もしくはもっと小単位） の単位）をグループとして作成し、認可に使用できるようにする
  - ただし、グループは、複数のSPで使いまわせるグループとする
    - 単一のSPしか使わないグループは、SP内で認可情報の管理を行えばよいと考える
- 作成するグループは、なんらかの属性から導かれるものとし、グループ管理者のメンバ管理を軽減する
  - 原則は、属性は既存情報（学内のDBなど何らかの形で管理されている情報）を用いる
  - ただし、兼務などの情報も柔軟に対応できる仕組みにする
- SP側にあまり手を入れずに認可できる仕組みとする
  - IdPで認証時にグループ情報を一緒に渡せるようにするとよい
    - Orthrosにグループ情報を持たせると、グループ情報付きの認可ができるようになる

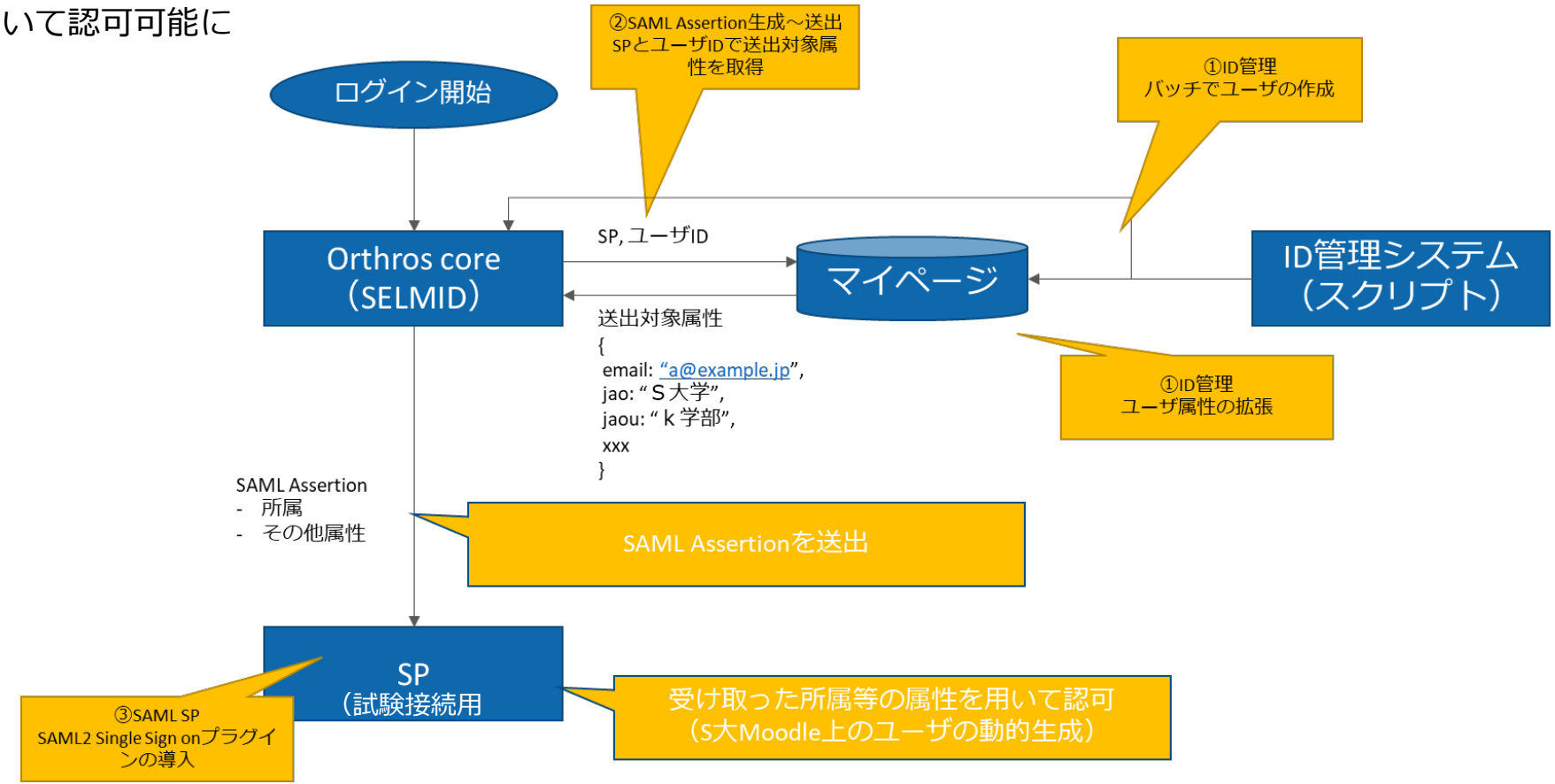
認証プロキシOrthros上で実装するイメージ図



認証プロキシのデザイン案
Original: Prof. Motonori Nakamura

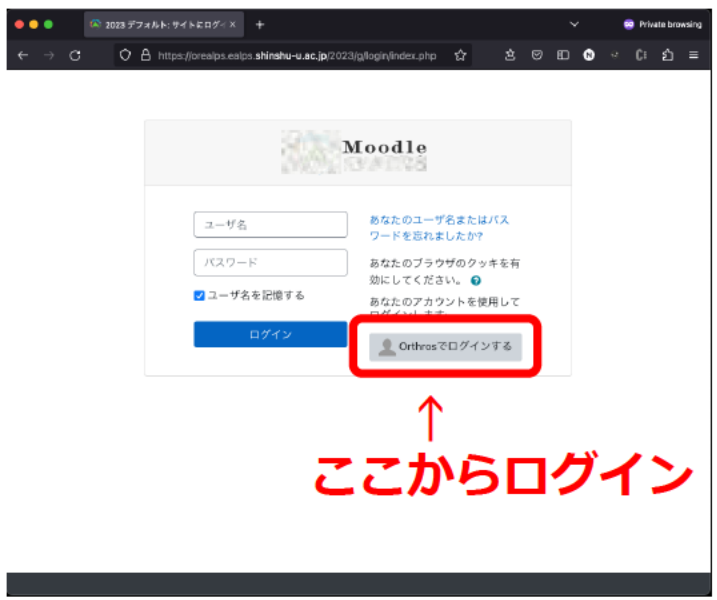
今回実装したシステム概要図
～OrthrosにおけるS大Moodle（SP）連携～

- Orthros上で追加開発した主な機能
  - ID管理（属性情報の追加、管理）
  - SAML Assertion生成～送出
- SP側（元々はLDAP認証）で追加開発した内容
  - SAML2 Single Sign onプラグインを導入・設定
  - 受け取った属性を用いて認可可能に



試験接続用SP

- 試験接続用SPは、S大のMoodleとした
  - S大Moodleの特徴：
    - 利用者は、学内者（S大IdPに登録）と学外者（S大IdPに未登録）の両方を含む
    - 主にS大学生が授業で利用するが、一般公開授業で、学外者も利用
    - 利用者（授業の受講者）は教務担当が一元管理
- 利用者には、Orthros上でS大Moodleの属性を付与、管理
- S大Moodle側には、SAML2 Single Sign-Onプラグインを導入・設定
- S大Moodleのログイン画面を改修



現在の状況：
- 2023年3月末に試験用システムの開発済
- S大Moodleによる試験運用中
- 課題の整理中

今後について：
- 試験接続用SPを拡大
  - 学認LMS、GakuNin RDMなど
- さらなる課題を洗い出し、認可機能の充実に