

グループ管理機能の高度化

NII オープンフォーラム2025

2025.6.17

国立情報学研究所

トラスト・デジタルID基盤研究開発センター

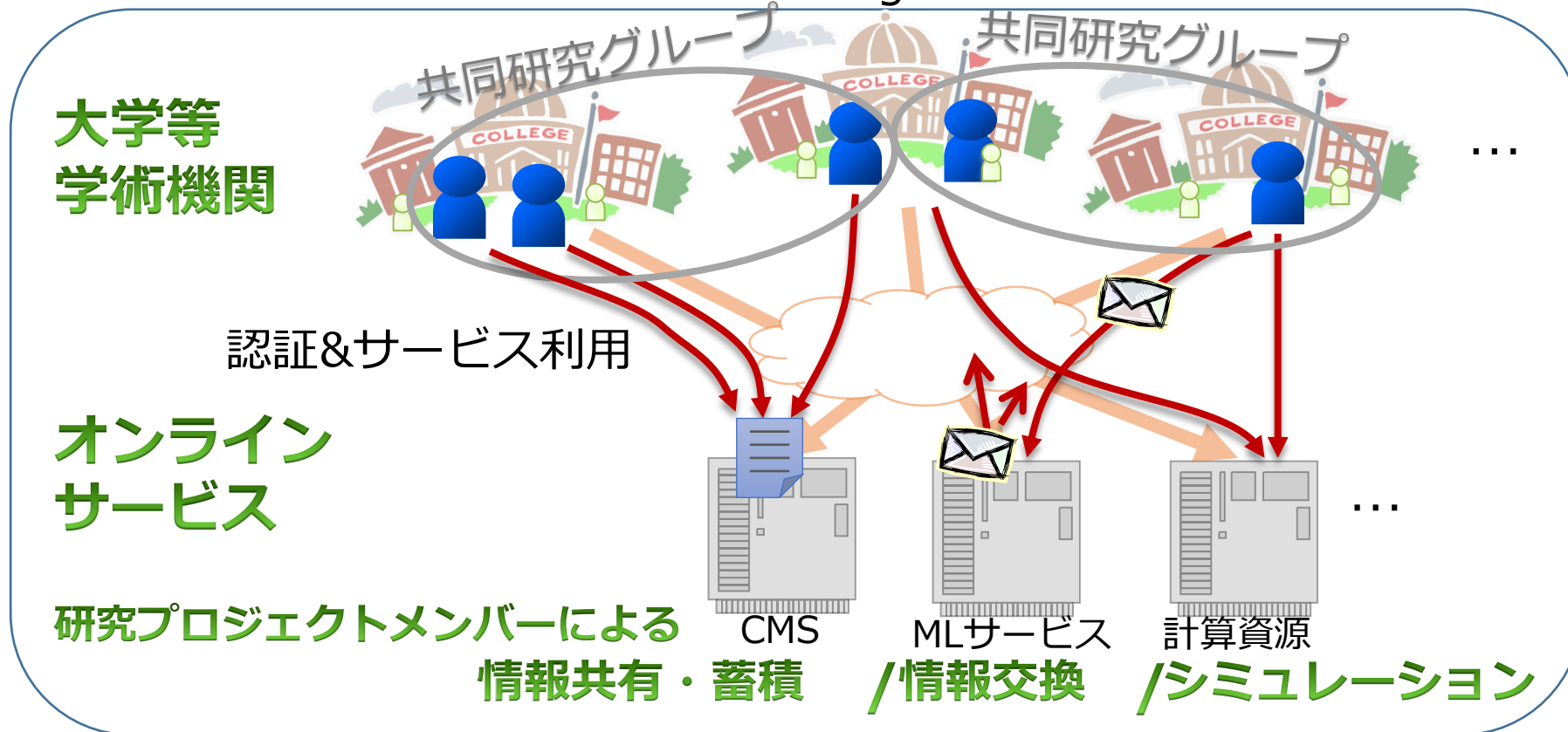
学術基盤推進部 学術基盤課 学術認証推進室

鈴木 彦文

グループ機能の利用例： 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）

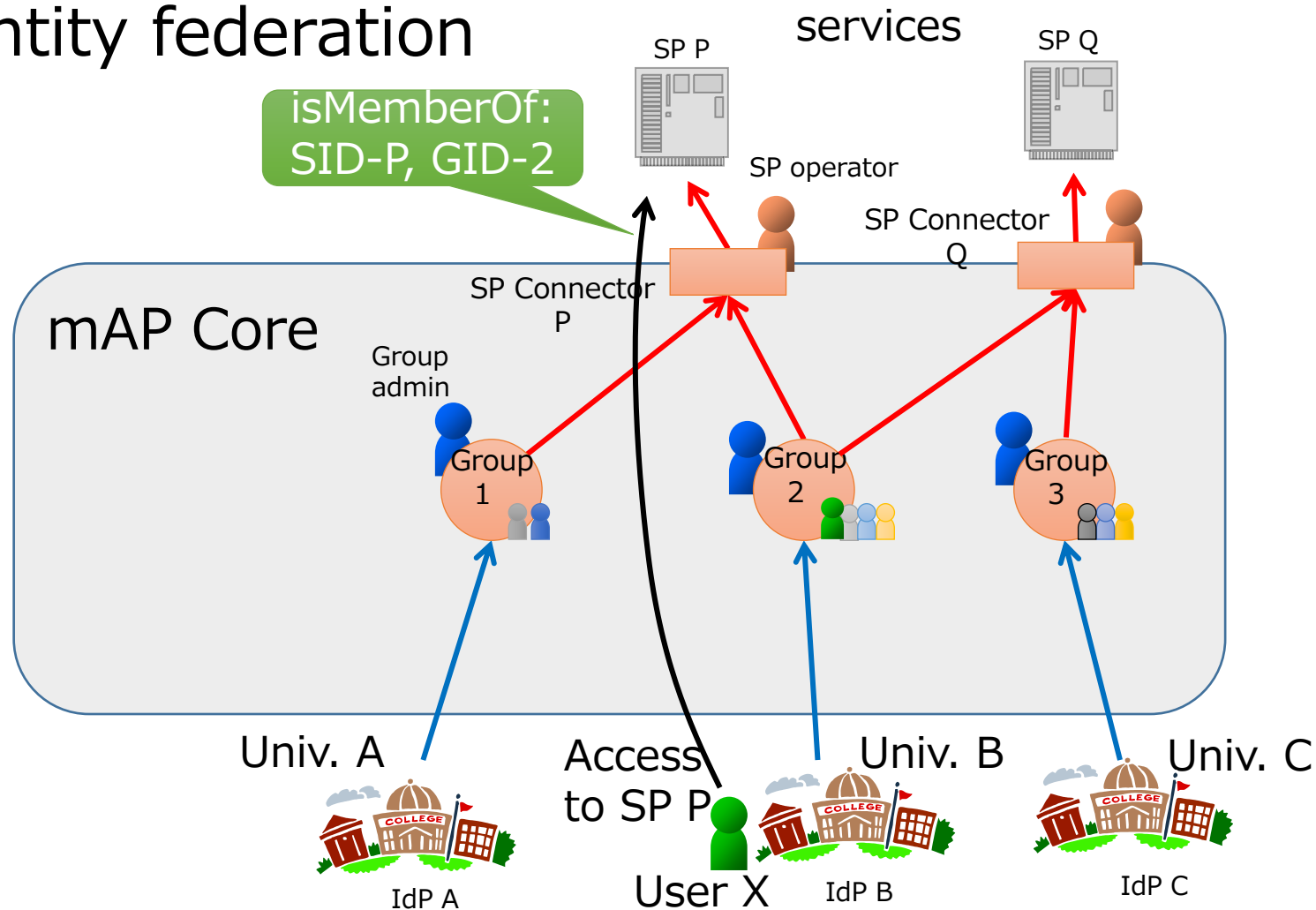


学認のグループ機能の変遷

- 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
- 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：
 - しぼすけ: スケジューリングサービス
 - 学認LMS: e-Learningシステム
 - meatwiki: グループ機能対応Wiki
 - meatmail / meatmail-lite: グループ機能対応メールリングリストサービス
 - クラス向け実習システム
 - 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）

Current Status of GakuNin Group Function: mAP Core

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



mAP Core の外部とのインターフェイス

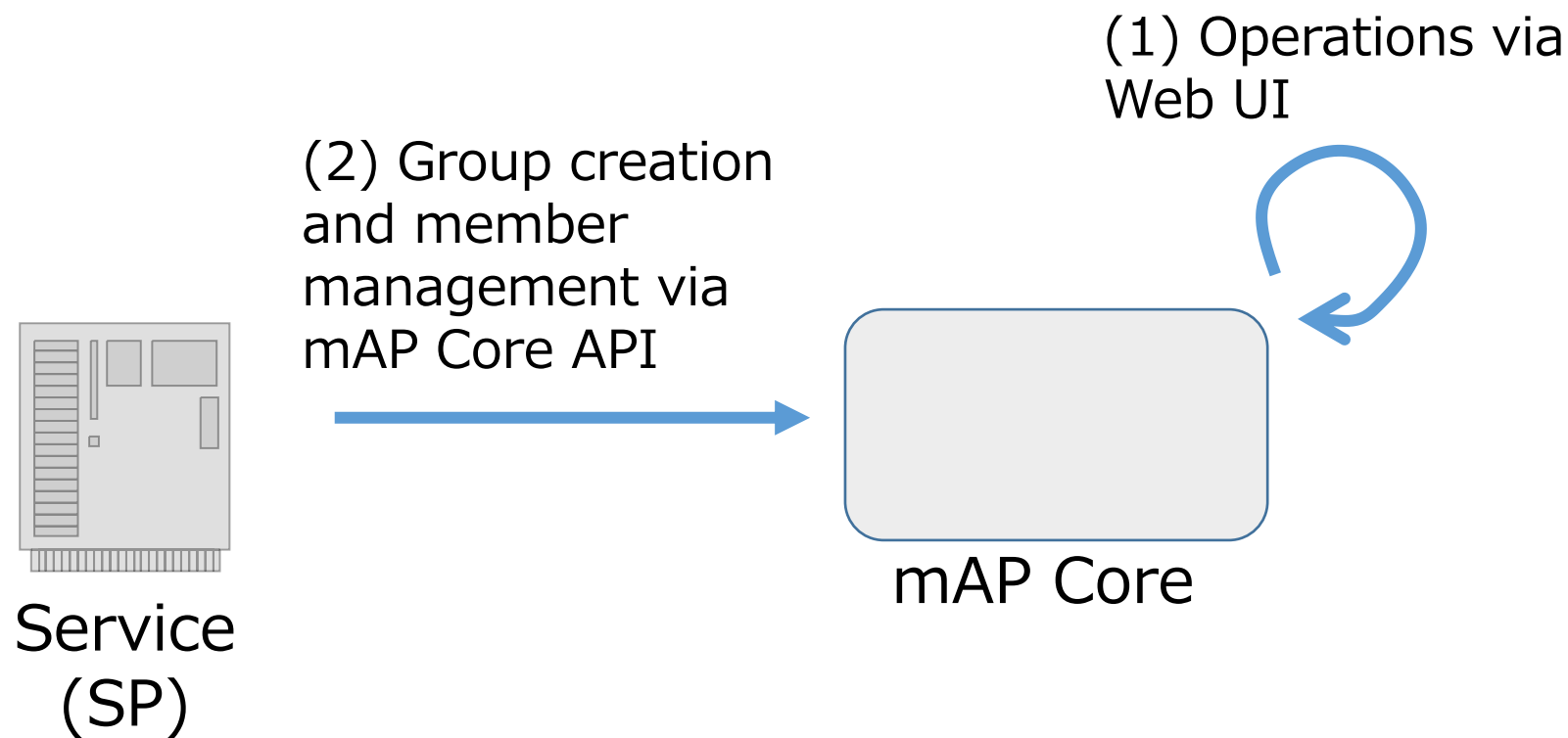
mAP Core が提供するグループ管理のインターフェイス・API(ユーザに対するUIを除く)

- ① SAML 2.0 Attribute Query
 - ePPN(もしくはメールアドレス)をキーに、所属するグループIDを取得できる
 - 属性交換仕様として国際標準
 - Meatwiki、しばすけ他多くのグループ機能対応SPで利用
 - 大学にサーバーを立てて mAP Core がプロ棋士として学内情報との連携を実施した実績あり
- ② 情報取得 API (Groups API / People API)
 - グループ情報・メンバー情報取得のための API
 - <https://meatwiki.nii.ac.jp/confluence/x/lwic>
 - VOOT ベースだが認証は独自
 - ML サービスで利用
- ③ mAP Core API V1
 - グループ作成、メンバー管理を含めた REST API
- ④ mAP Core API V1
 - SCIM に準拠した汎用的な API

グループ機能が装備しておくべき機能

- 利用者がグループを作成、メンバーを設定できること
- サービスが利用者の所属グループを把握できること(①)
 - 個人のIDを知っていることが前提
 - SAML Attribute Query 他
- サービスが接続されたグループ情報メンバー情報を取得できること(②)
 - 利用者がログインしたタイミングでなくとも把握できる
 - 例：MLサービス
- サービスが利用者に成り代わってグループ作成・メンバー管理できること(③,④)
 - サービスが持つグループ情報を同期するなど

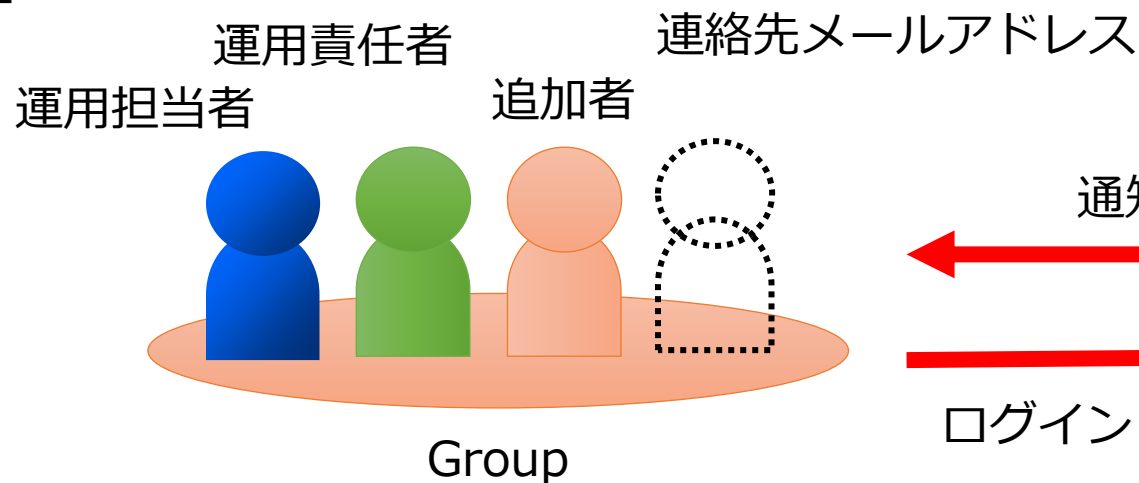
mAP Core API



API による接続例：学認Surveyシステム

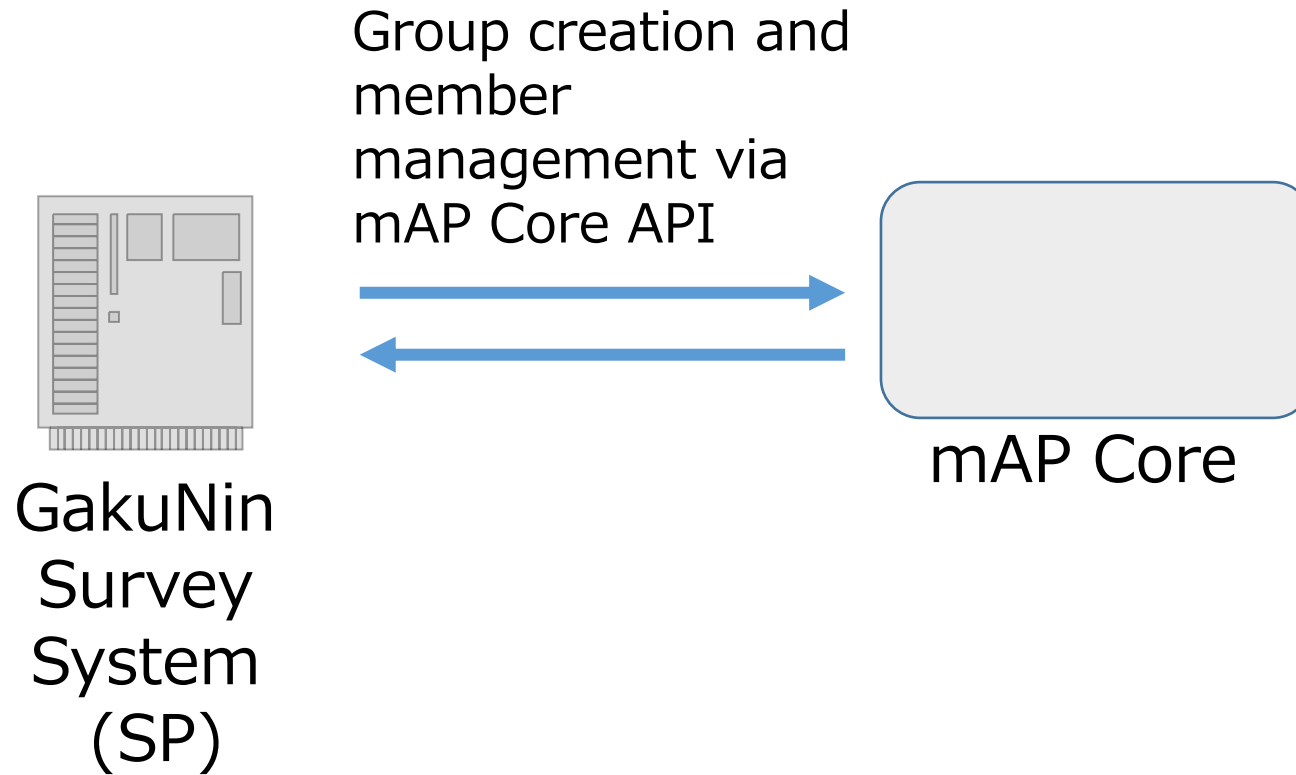
- 各参加機関の担当者（運用担当者・運用責任者）に対して調査・アンケートを行うシステム
 - 担当者が複数おりそれをグループとして、認証した上で入力させる
 - 適格者を自分で追加・削除することが可能
 - 通知先メールアドレスを追加可能
 - 学認で例年行っている学認参加IdP運用状況調査に利用

A大学



学認Surveyシステム

mAP Core API and GakuNin Survey System



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

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

ex) A大学A先生の場合：
主の所属：情報メディアセンター
兼務：情報学研究科
その他：セクハラ対策委員会
セキュリティ研究チーム
B大学、AI検討会



ユースケースの収集（募集中）

- サイエンスプロジェクト
 - MS (Moon Shot) の事例：多数の研究機関と研究者が関わるプロジェクトのグループ管理
 - 複数の計算資源・データ管理・論文管理システムにアクセスするグループの管理
- 高度人材育成
 - SPARC (高度人材育成事業)の事例：複数の地域大学が連携して、人材育成コンテンツを利用する際のグループ管理
 - 複数の教育システムに共通するグループの管理

中規模・大規模のユーザー、かつ、複数のSPで利用するグループの管理についてユースケースを分析しモデルを作成

グループ管理機能と属性プロバイダ

- デジタル証明書に必要となる情報を中心とした属性を創出するプロバイダについて現在検討中
- 様々な属性情報を取り扱うため、その一つとしてグループに関する情報が入る可能性を検討中(直ちにではありませんので、引き続き mAP Core をご利用ください)
- デジタル証明書に必要となる属性情報について公開中
パブリックコメント募集しております
トラスト・デジタルID基盤研究開発センター HP 標準化・規格化
<https://trustdigitalidcenter.jp/>

