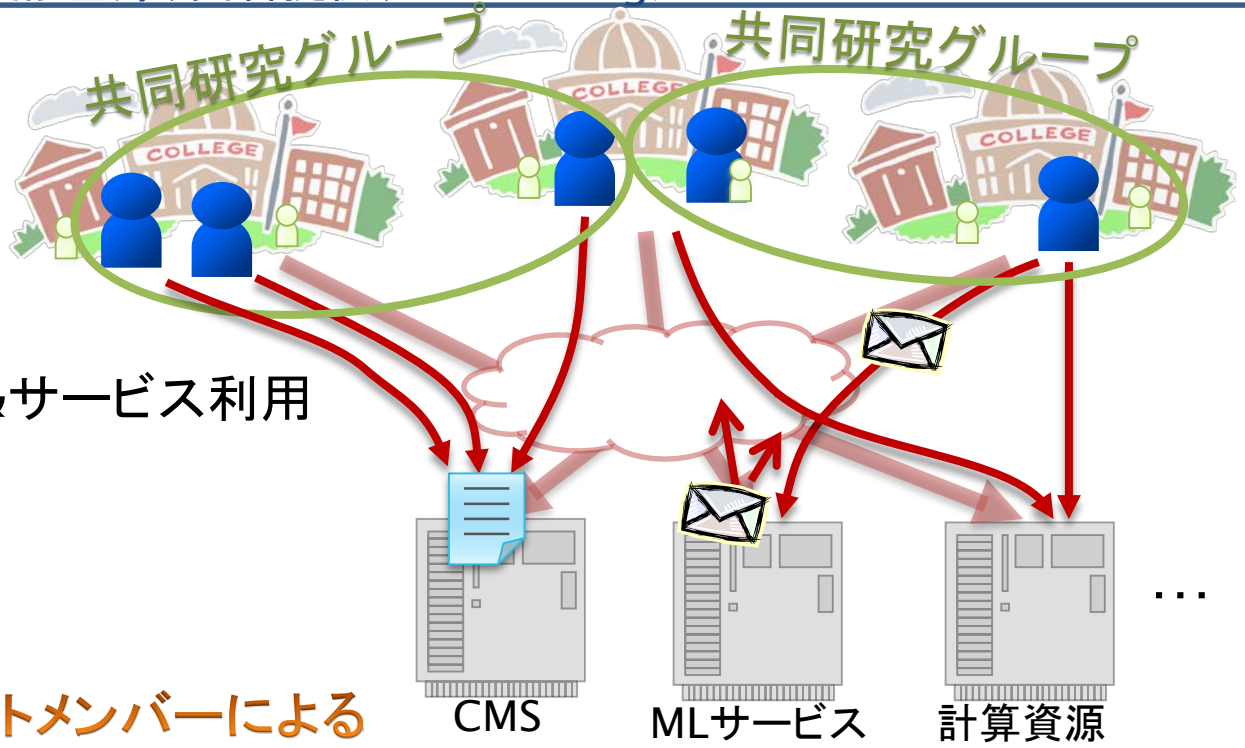
次世代学認サービスメニュー：グループ機能 mAP Core

2022年3月10日　第14回統合認証シンポジウム
国立情報学研究所　西村健

mAP Core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

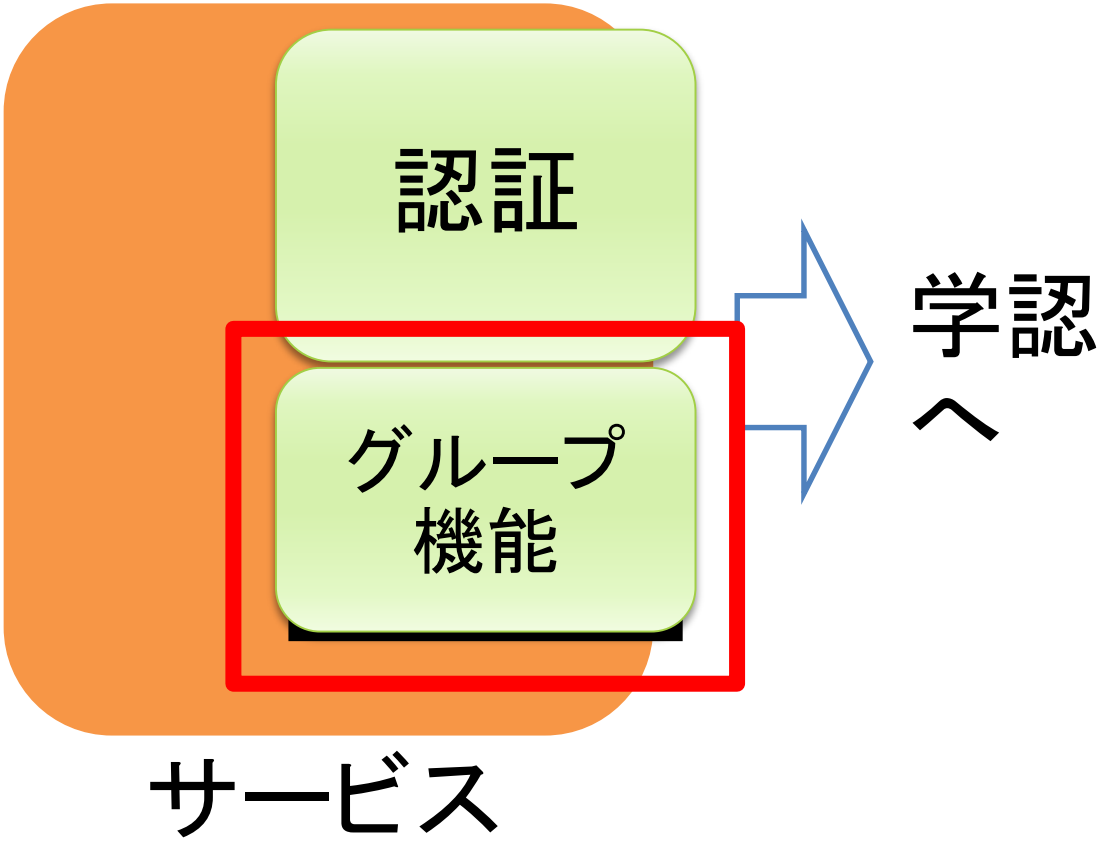
研究教育活動支援の各種オンラインサービスが簡単に利用できる場

- 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）



イメージ

- サービスの中の機能の一部を外出し・共有

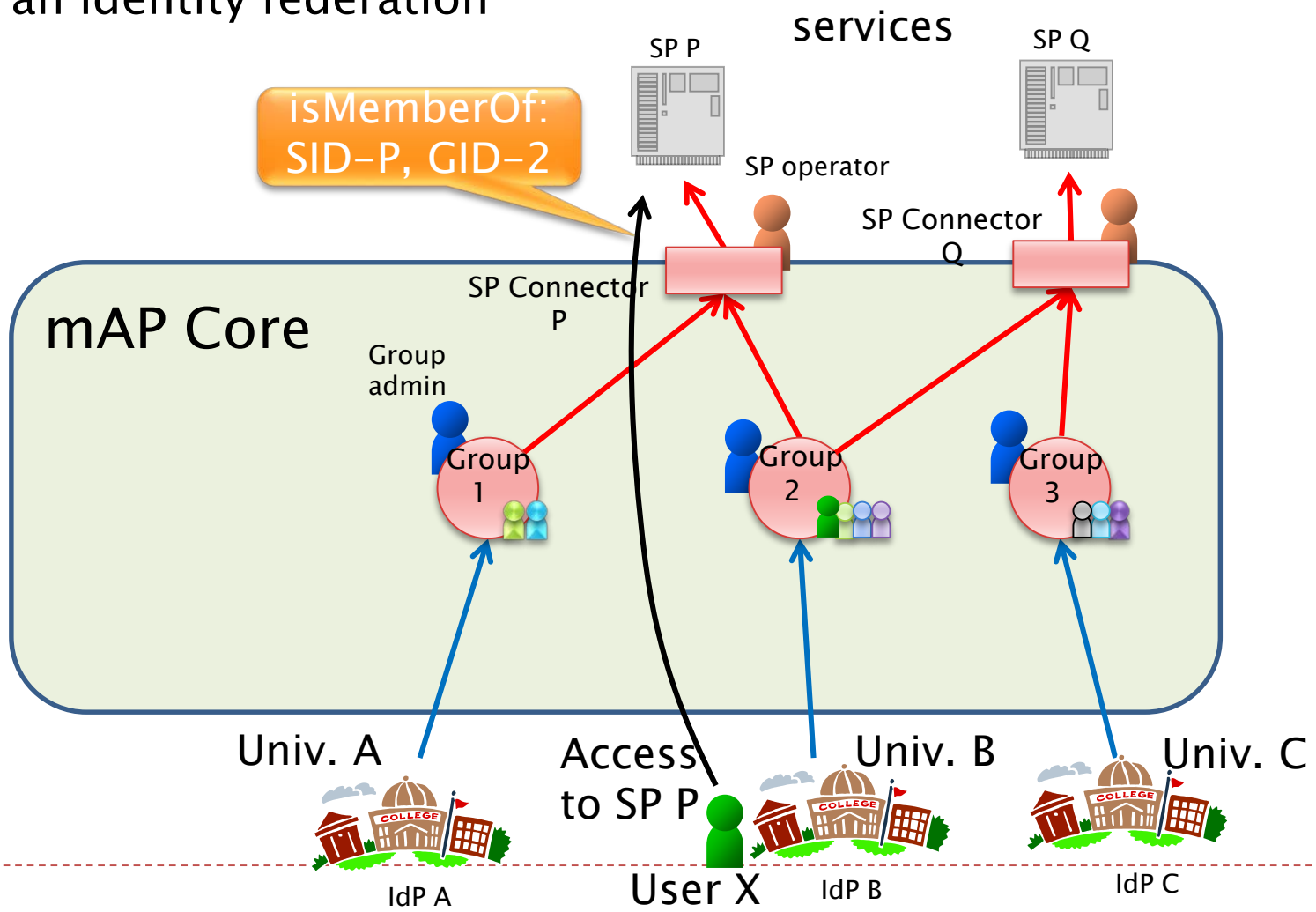


概要と経緯

- 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
- 改めて学認のグループ機能を「mAP Core」と命名。
- 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
  - 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）

mAP Core overview

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



mAP Coreの外部とのインターフェース

mAP Coreが提供するグループ管理のインターフェース・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、しぼ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がプロキシして学内情報との連携を実施した実績あり

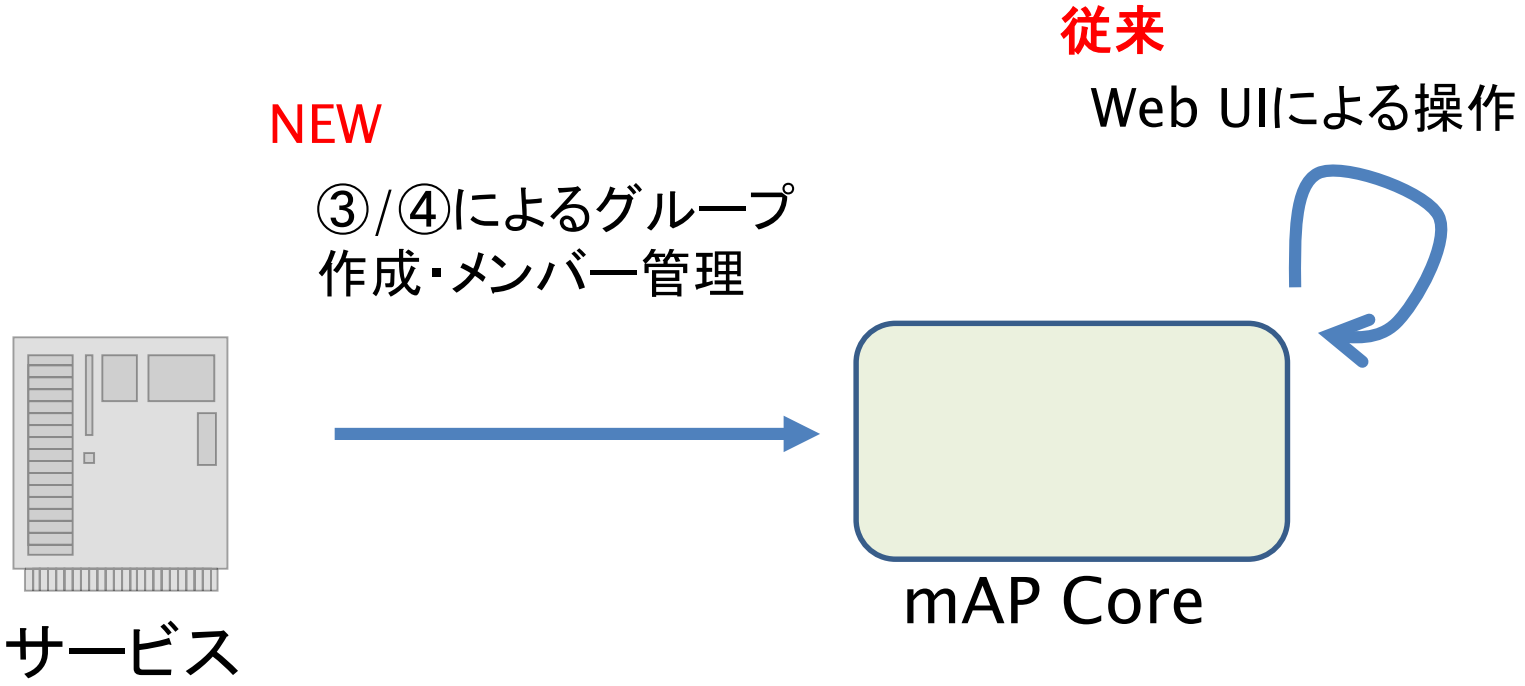
② 情報取得API（Groups API / People API）
- グループ情報・メンバー情報取得のためのAPI
- `https://meatwiki.nii.ac.jp/confluence/x/lwic`
- VOOTベースだが認証は独自
- MLサービスで利用

③ mAP Core API V1
- グループ作成、メンバー管理を含めたREST API
- 試験利用・提供中

④ mAP Core API V2 (2022年度提供予定)

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


従来
Web UIによる操作
NEW
③/④によるグループ
作成・メンバー管理
サービス
mAP Core

プライバシー・権限

- そもそも接続していないサービスにはグループ・メンバーの情報が流れない
- サービス利用開始にあたって各利用者から属性送信の同意を取得する
- REST APIでもこれを反映するよう各データと権限者のマトリクスを作成

attribute name	修正不可	未使用	必須	ユーザ本人	招待主	グループ管理者(所属グループ)	サービス管理者(利用中サービス)	組織(Id
.				rw	rwd	r	r	r
schemas[]	1			-	-	-	-	
id	1			r	r	r	r	
externalId	1		1	rw	rw	r	r	r
userName			1	rw	r	r	r	
displayName				rwd	rwd	r	r	rw
nickName				rwd	rwd	r	r	rw
profileUrl				rwd	rwd	r	r	rw
title		1		rwd	rwd	r	r	rw
userType		1		rwd	rwd	r	r	rw
preferredLanguage				rwd	rwd	r	r	rw
locale		1		rwd	rwd	r	r	rw
timezone		1		rwd	rwd	r	r	rw
password		1		-	-	-	-	
meta.resourceType				r	r	r	r	
meta.created	1			r	r	r	r	
meta.lastModified	1			r	r	r	r	
meta.location				r	r	r	r	
meta.createdBy	1			r	r	r	r	
name.familyName		1		rwd	r	r	r	rw
name.givenName		1		rwd	r	r	r	rw
name.middleName		1		rwd	r	r	r	rw

mAP Core APIの現状および計画

- 学認参加SP（もしくはIdP）から直接グループ管理できるようAPIを整備
- 現状、外部SPからグループ管理の最低限（作成・更新・メンバー追加削除）のAPIのみを提供している(mAP Core API V1)
  - NII内で試験利用・提供中
- SCIMに準拠した汎用的なAPI V2を来年度提供予定

海外事例：eduTEAMS

- https://eduteams.org/
- https://wiki.geant.org/display/eduTEAMS/eduTEAMS+Home
- GÉANTが提供しているVO(仮想組織)管理の仕組み。対象者はeduGAINのIDおよびSNS等（例：ORCID、Googleアカウント）のID。

3種の「eduTEAMS」

- eduTEAMS Service
  - 中小規模VO向け、マルチテナントのクラウドサービス
- eduTEAMS Dedicated
  - 希望するVOに対して、カスタマイズされたものをServiceとは別に提供する。運用はGEANTがやってくれる。
- eduTEAMS Bespoke
  - 各VOが運用も行うeduTEAMS。コンサルテーションも行う。

- SPとのI/FはIdP的。SCIMベースのものはない。

まとめ

- 学認のグループ機能 mAP Core を紹介しました