2011年度「SINET＆学認説明会」
学認最新R&D報告

国立情報学研究所

作成日：2011年10月20日

トピック

学認の利便性向上、プライバシー配慮、新規サービス開拓等のために研究・開発しているソフトウェアのご紹介

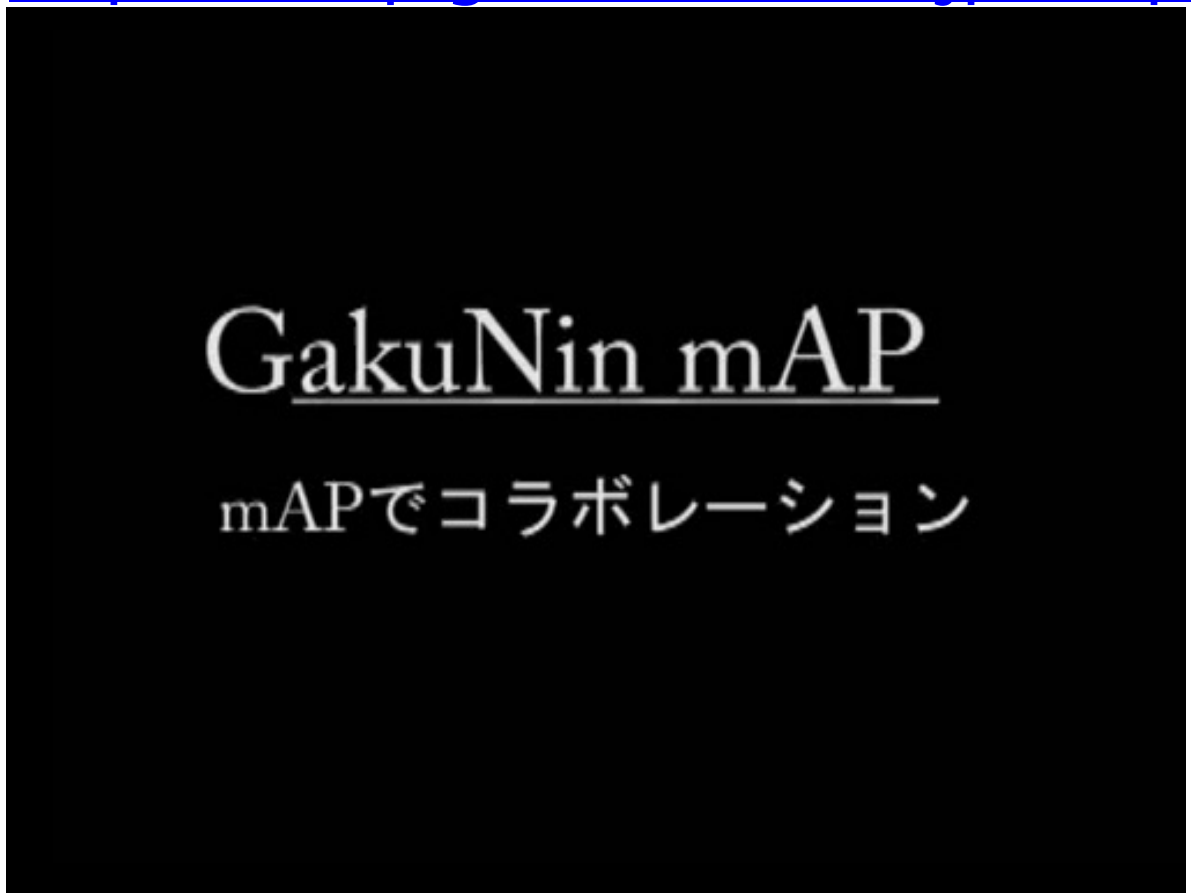
- グループ管理システム (GakuNin mAP)
- IdP機関のためのユーザ同意機構 (uApprove.jp)
- OpenIdP（特定組織に属さないIdP）

グループ管理システム
GakuNin mAP

GakuNin mAP とは

- 学認利用者のグループを管理するためのシステム

https://map.gakunin.nii.ac.jp/map/

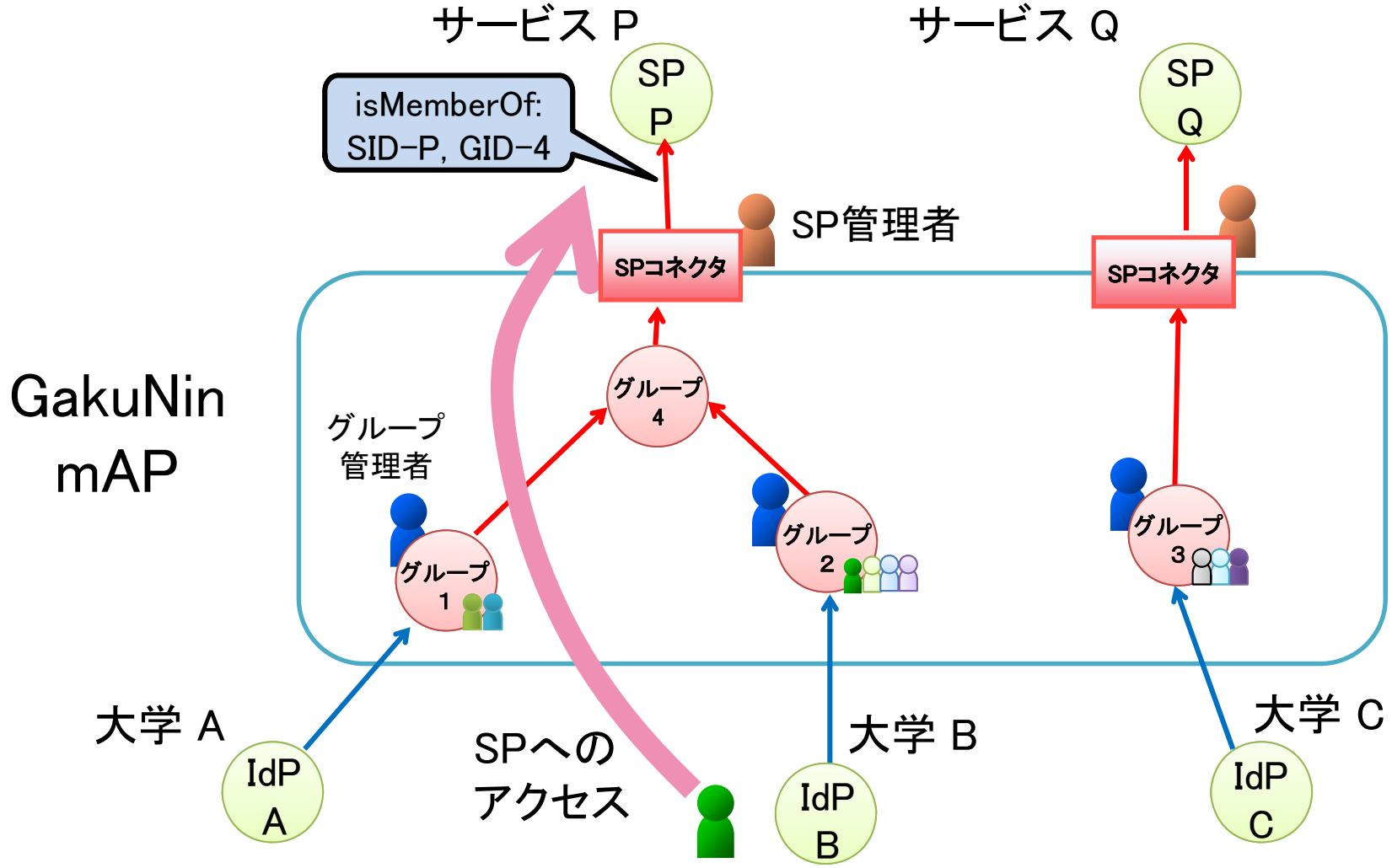


利点は？

- IdP側（大学側、利用者側）の視点では…
  グループ情報を特定のサービスから独立させる
  - サービス毎に管理する手間の削減／
    ロックインされないオープンな環境を提供

- SP側（サービス提供者）の視点でも…
  コラボレーションを目的とするサービスにグループメンバー管理機能の作り込みが不要になる
  - 思い付いたアイデアを手軽に実現できる
  - サービス開発の迅速化

GakuNin mAPのアーキテクチャ



グループ

- いわゆる「グループ」
  ＝任意の「学認IDの集合」を表すもの

- メンバーの登録方法
  - 管理者（作成者）からの招待（招待メール）
  - 利用者がグループを指定して入会申請する
    - 入会審査あり
    - 入会審査なし＝利用者が自由入会する（コミュニティ的なもの）

eScienceプラットフォームとしての応用

一連の流れ（デモ）

- グループ管理者の操作
  1. グループを作成
  2. SPコネクタに接続
  3. メンバーを招待
- メンバーの操作
  4. 招待に同意
  5. SPにログイン

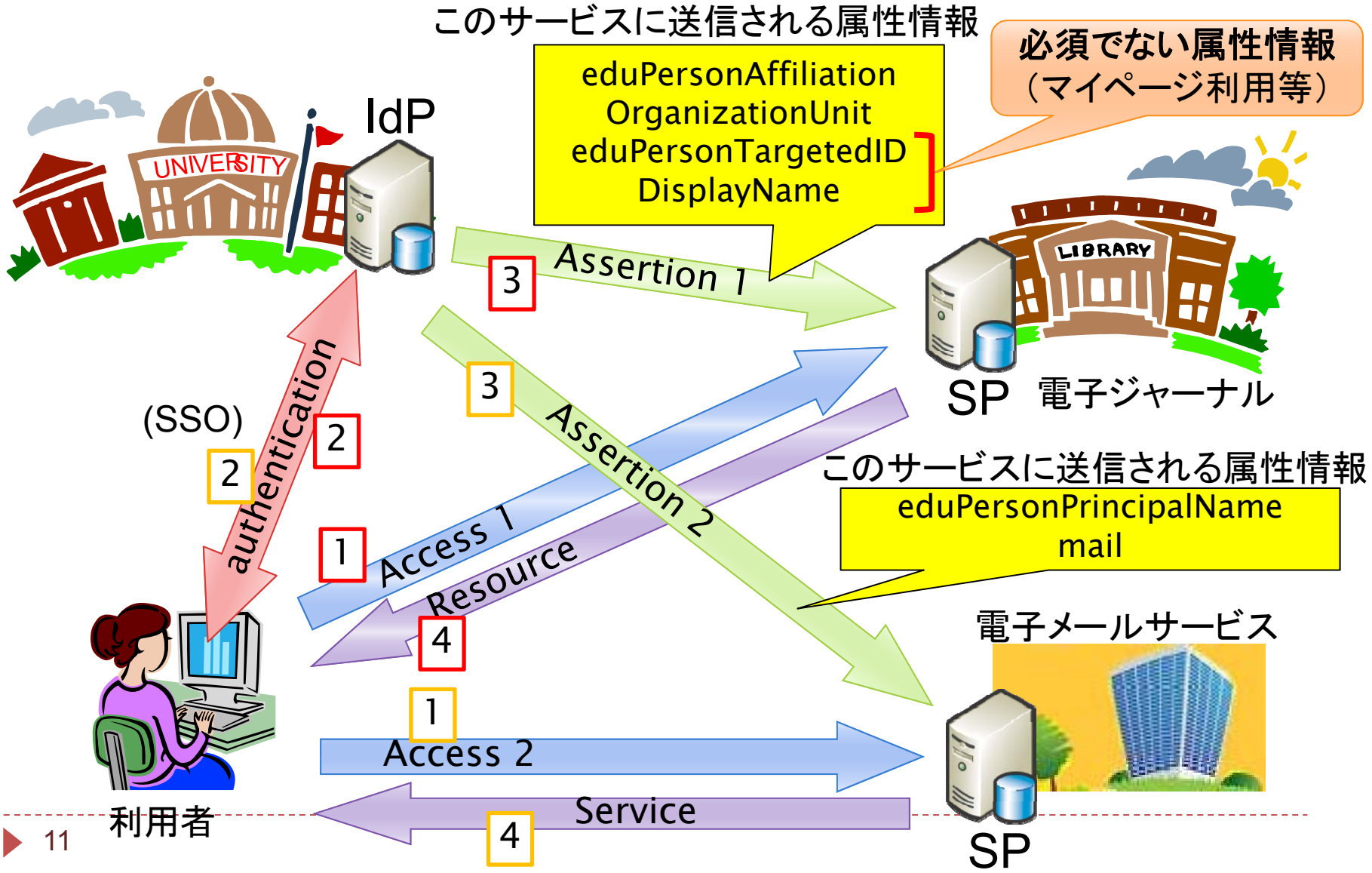
- mAP連携SP例： meatwiki
  - グループを作成してSPコネクタに接続すれば、そのグループのメンバーだけが読み書きできるWikiスペースが提供されるサービス

デモ内容

グループをSPコネクタに接続しなければ、一切SPに情報は渡されない！
（利用者主体の情報コントロール）

IdP機関のためのユーザ同意機構
uApprove.jp

サービス利用時の個人情報送信



学認で利用されている属性情報

Name (abbreviation)	Description
OrganizationName (o)	組織名
jaOrganizationName (jao)	組織名（日本語）
OrganizationalUnit (ou)	部門名
jaOrganizationalUnit (jaou)	部門名（日本語）
eduPersonPrincipalName (eppn)	フェデレーション内で固有の個人識別子
eduPersonTargetedID	SP毎に固有の個人識別子（匿名識別子）
eduPersonAffiliation	Staff, Faculty, Student, Member
eduPersonScopedAffiliation	Staff, Faculty, Student, Member（@scopeつき）
eduPersonEntitlement	SP毎に固有の付加情報
SurName (sn)	名字
jaSurName (jasn)	名字（日本語）
GivenName	名前
jaGivenName	名前（日本語）
displayName	表示用氏名
jaDisplayName	表示用氏名（日本語）
mail	E-mail アドレス
gakuninScopedPersonalUniqueCode	学生番号、職員番号（@scopeつき）

個人情報

学認参加以前に収集した個人情報は目的外利用となるため本人同意が必要

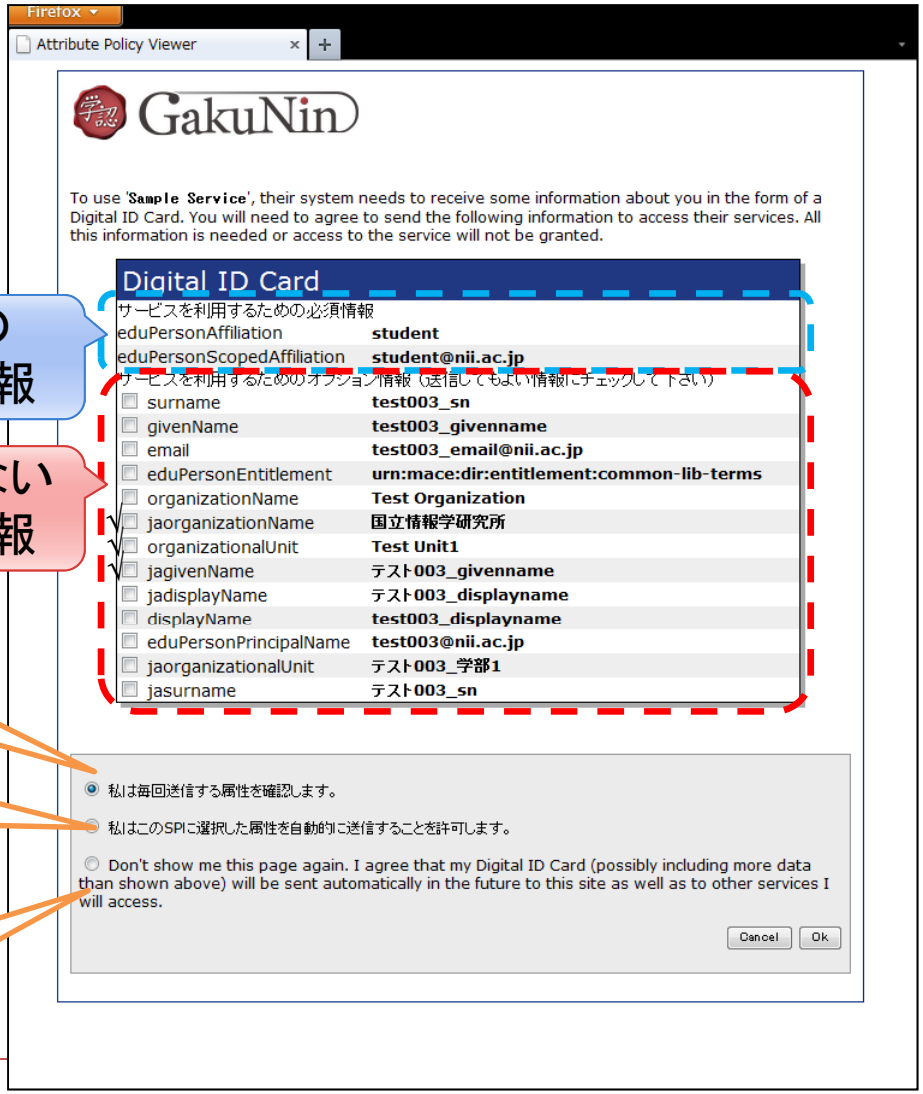
個人情報保護法

- 個人情報の保護に関する法律（平成15年5月30日法律第57号）
  - 私立大学

- 独立行政法人等の保有する個人情報の保護に関する法律（平成15年5月30日法律第59号）
  - 国立大学（公立大学もこちらに準じる）
  - 利用目的以外の目的での保有個人情報の提供には、本人の同意が必要
    - 全てのSP（将来の追加を含む）に対する包括的な同意
    - SPごとの個別の同意

ユーザに選択権を与える拡張：uApprove.jp

- 送信が必須でない属性情報に関して、ユーザが送信の可否を個別に選択できる
- 将来の挙動について指定できる



(*) SWITCH（スイス）のuApproveを元に開発
http://www.switch.ch/aai/support/tools/uApprove.html

uApprove.jpの開発状況

- 試験実装公開中(IdP 2.1.3, 2.1.5, 2.2.0)
  - http://www.gakunin.jp/docs/fed/uapprove-jp

- 実運用に耐えるバージョンを公開予定(IdP 2.3.x)
  - IdPでは、IdP 2.3.2以降の利用を推奨
    - Vulnerability of OpenSAML library included in prior to version 2.3.2

特定組織に属さないIdP
OpenIdP

学認利用支援に向けて

- 学認は2010年度から本格運用を開始
  - IdPは30機関が構築し、ユーザ総数は概算で45万（2011年10月1日現在）
- 各機関での整備は進んでいるが、まだまだこれから
  - 日本国内の高等教育機関は1200以上、ユーザ総数は350万以上（文部科学省、平成23年度学校基本調査）
    - 大学 780校、学生290万人、教員36万人（兼務含む）
    - 短大 387校、学生15万人、教員6500人（兼務含む）
    - 高専 64校、学生6万人、教員5000人（兼務含む）
- 学認利用を支援・促進する仕組みが必要
  - IdPホスティング
  - OpenIdP

OpenIdP

- IdPの構築が完了していない機関ユーザ向けサービス
  - OpenIdPは学認には属さない
- 学認サービスの「一部」が利用可能
  - 大容量ファイル転送サービス Fshare β
  - Communications service for sharing academic information（山形大）
  - meatwiki
  - FaMCUs（テレビ会議用MCU）
  - など
- ac.jpのメールアドレスを持つユーザであれば自由に登録可
  - メールの到達性を確認
  - ac.jpドメイン以外にも対応可能
  - 登録可能ドメインの追加は openidp-admin@nii.ac.jp へ

おわりに

- 今回紹介した新機能
  - グループ管理システム (GakuNin mAP)
  - IdP機関のためのユーザ同意機構 (uApprove.jp)
  - OpenIdP（特定組織に属さないIdP）

- この他にも(開発中のものも含む)
  - 埋め込みDS (embedded DS)
  - 学認申請システムの改良
  - IdP選択、確認のためのブラウザプラグイン
  - 学認mAP対応メーリングリストサービス
  - OpenID連携プロキシ などなど

是非とも改善へのご意見ご要望をお寄せ下さい。