電子ブックサービスを支援するための グループ管理システム GakuNin mAP

2011年3月7日

国立情報学研究所　西村　健

この発表の前提

- 認証は、電子ブック閲覧・ダウンロード時に利用者に対して行う
- 電子ブック利用は提供側との利用契約を前提とする

サービス（SP）の分類

- 契約ベース
  - 大学側（大学単位もしくは大学内組織単位）と個別に契約がある
    - 電子ジャーナル
- 自由登録・自由利用
  - 学認のID全てが対象となり、自由に利用できる
    - テレビ会議予約システム、ファイル共有、…

契約に沿ったアクセス制御のための情報は誰が持つ？

- SP？
  - 当然ながら大学単位の契約であればSPが持てば十分
  - ○○学部、△△学科、××研究室が契約者の場合は？
    - SPがどうやって把握する？→全てのIDを含むデータベースを持つ？
- IdP？
  - 学部単位くらいまでならそれも可能
    - しかしバックエンドのDB管理者が大変
    - 情報更新時期の問題
  - どうやってSPに伝える？
    - OU？レベルごとに新たな属性を追加する？
  - 大学をまたがる組織の場合にはどうにもならない

→ その悩み、mAPが解決します！

メンバー属性プロバイダー mAP

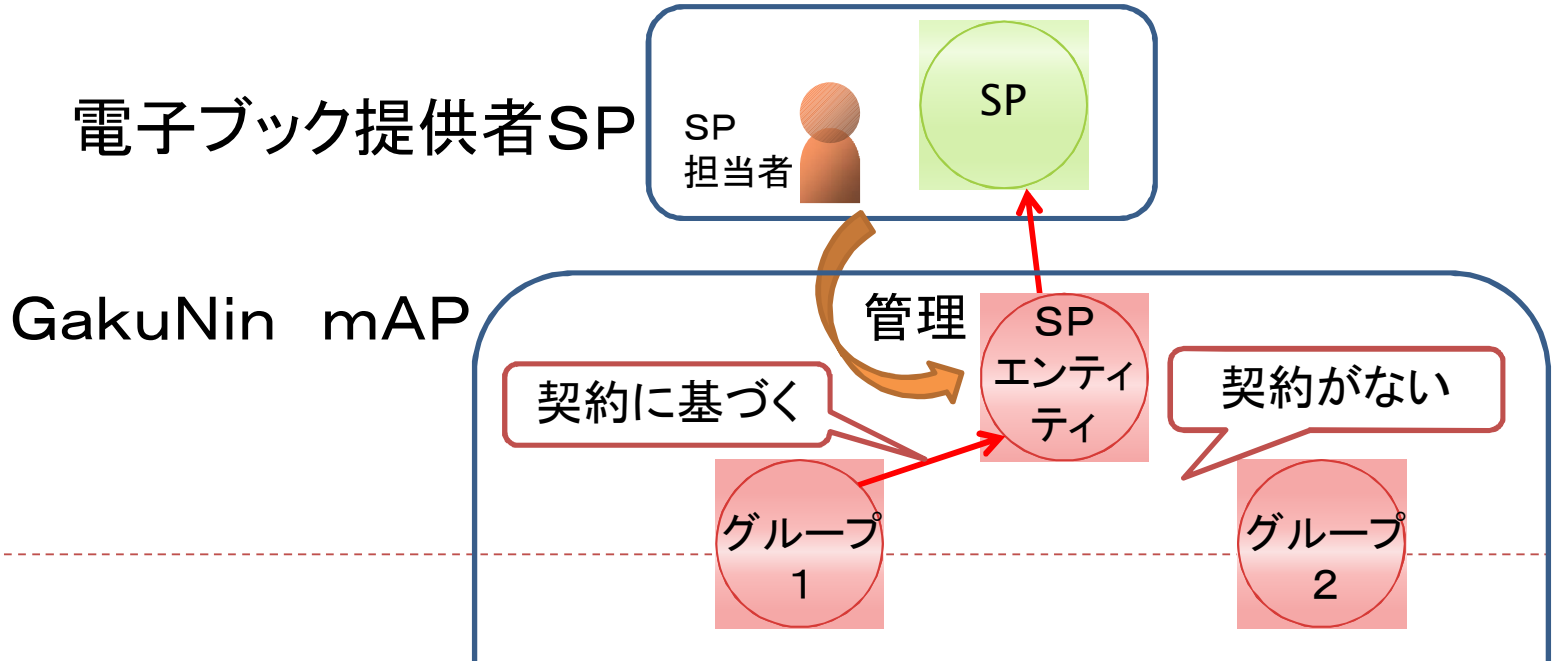
- IdP、SPに加えてmAPというエンティティを導入する
- mAPが各種グループを管理する
- 新たにisMemberOf属性を定義し、IdPからの属性情報に付加して「その人がどのグループに属するか」をSPに伝える
  - 加える属性は一つだけ！
- グループの管理については、SP側、IdP側がそれぞれの役割で行う（後述）

- ひとまず、学認が提供する1つのmAP（GakuNin mAP, GNAP）のみが存在するモデルを想定する
  （複数のmAPを扱うモデルは今後の課題）

SP側から見たmAP管理

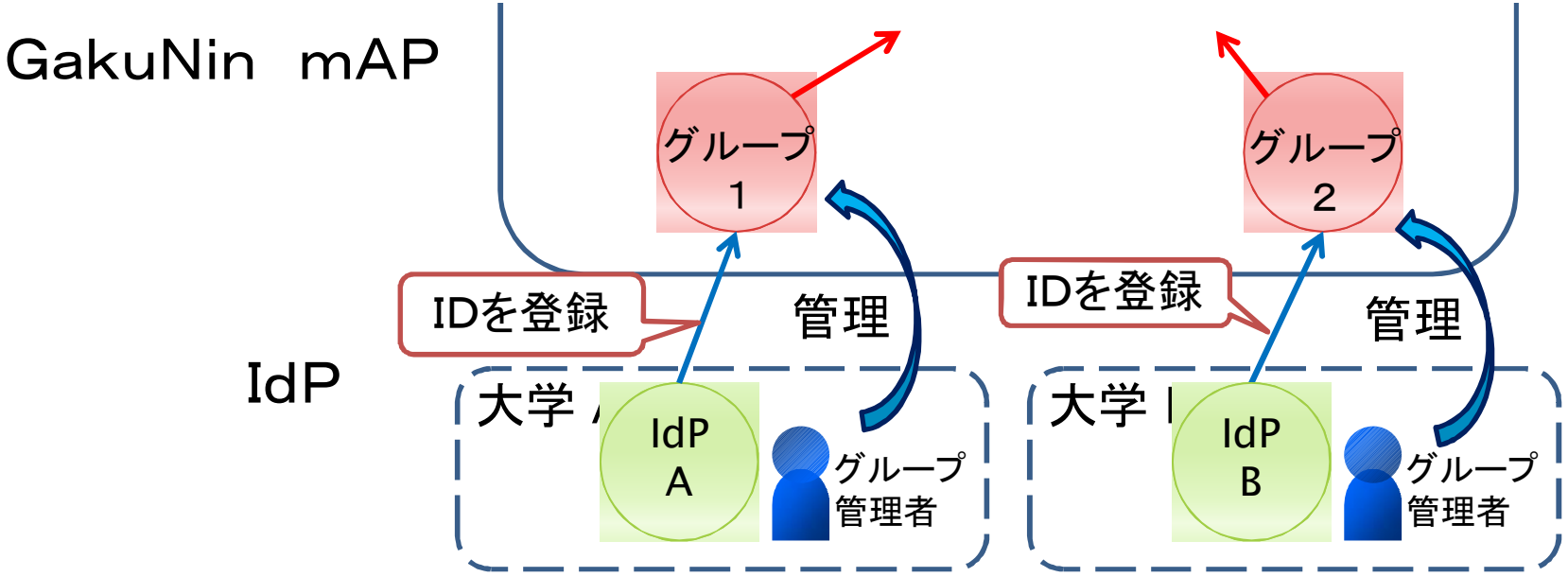
- mAP内のグループが契約対象かどうかの管理
  これだけ！
- Shibboleth SPの設定は、
  - 付加的にmAPを参照するようにして、
  - 各利用者のisMemberOf属性をチェックするだけ。

一度設定すれば運用中に一切変更する必要なし。



IdP側から見たmAP管理

- グループのメンバー管理
- お願いします！



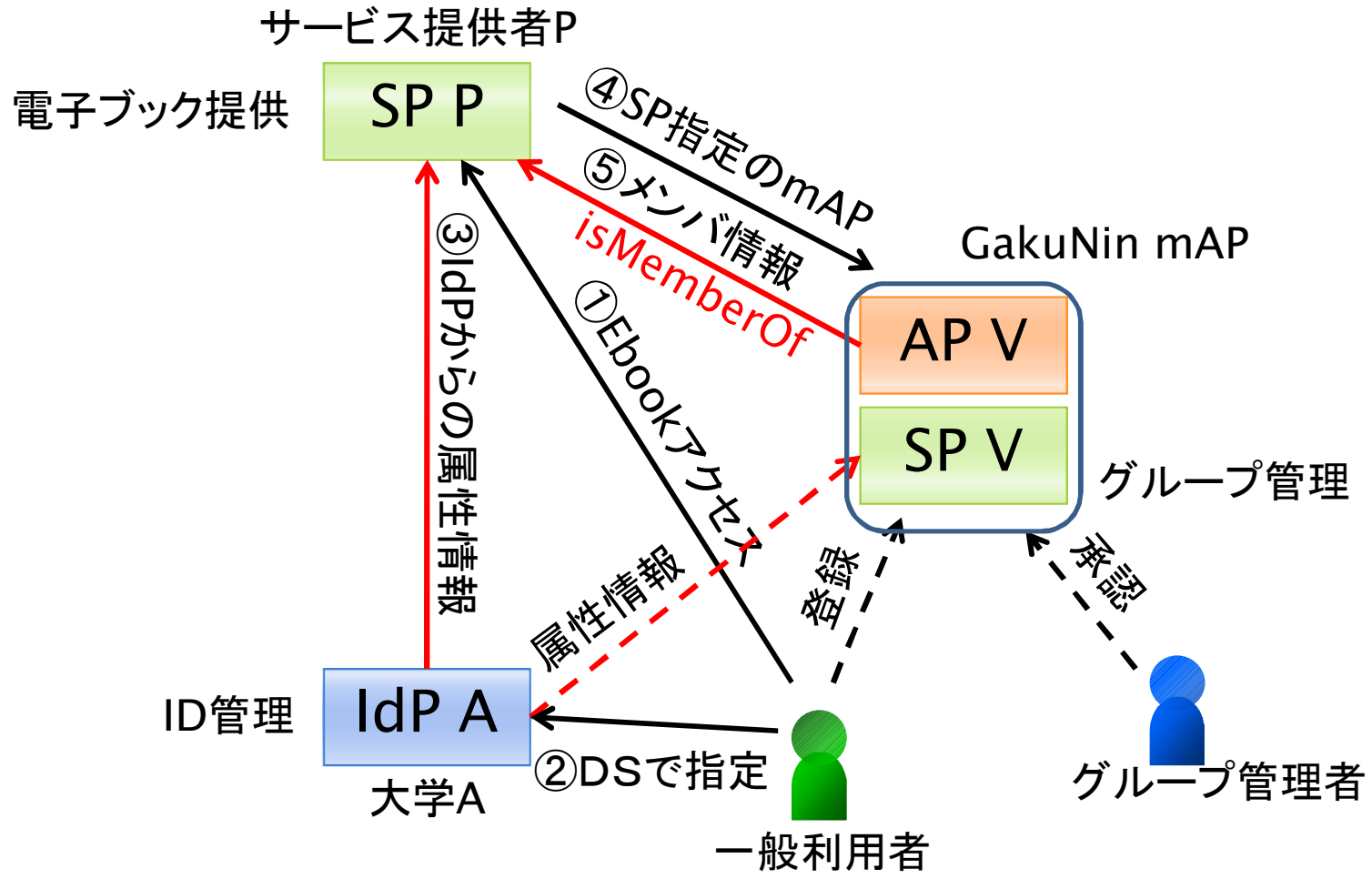
Q. 電子ブック用なの？
A. いいえ、そんなことはありません

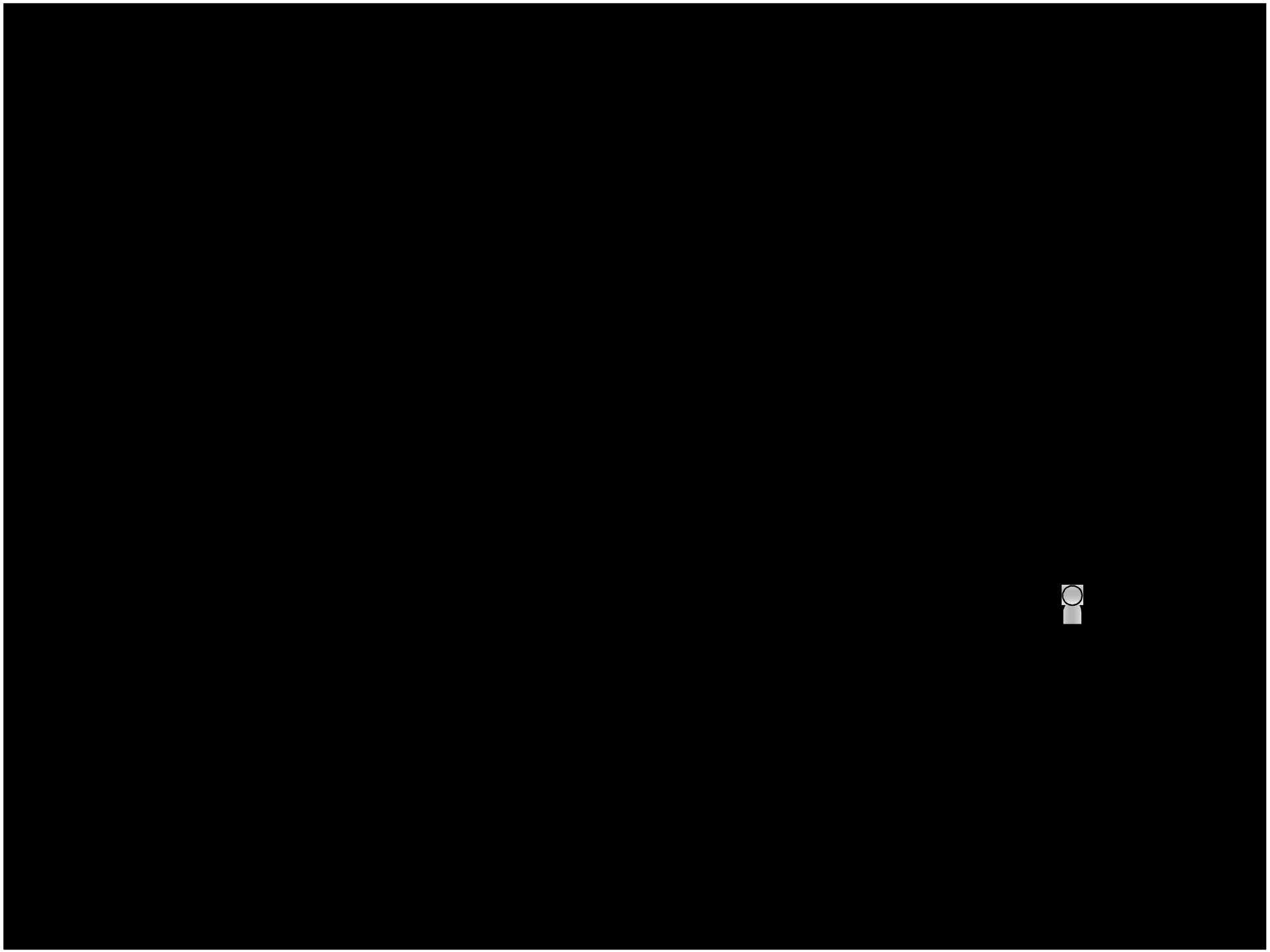
複数のSPに共通な「グループ」を一元管理

- 契約ベースのサービスのみならず、
「グループ」の概念があるサービスには普遍的に利用可能
- 例えば…
  - 学科、研究室単位で協調して使いたいサービス（グループウェア等）に利用可能
  - 大学をまたがるプロジェクト、共同研究についても、含まれるIDをグループとして登録しておけば利用可能になる

- 他の卑近な例で言うとグループはメーリングリスト（ML）のようなもの
  - メンバー固定のクローズドなML
  - 管理者の承認が必要なML
  - 参加自由のオープンなML
  - など用途・形態・規模がさまざま

isMemberOf 属性送信のプロトコル





認証連携のその先へ

- 利用者個人を特定サービスから解き放つもの　…
  認証連携
  ↓
  グループ情報やその他の認可判断情報を特定サービスから解き放つもの　…　mAP！

- 企業内SSOが提供する機能を組織横断型SSOへ

- 必要なのは、それらの情報をしまう箱、そしてプロトコル標準。 －　GakuNin　mAPにはどちらもあります！

まとめ

- 電子ブックサービス（SP）で契約の範囲を明示するために利用できる、メンバー属性プロバイダー（mAP）の仕組みを解説
- mAPは電子ブックのみならず、グループの概念を持つSPで利用可能！

- IdP管理者のみなさま、サービス提供者のみなさま、ご意見ご要望等ありましたら学認まで！