

メンバー属性プロバイダー

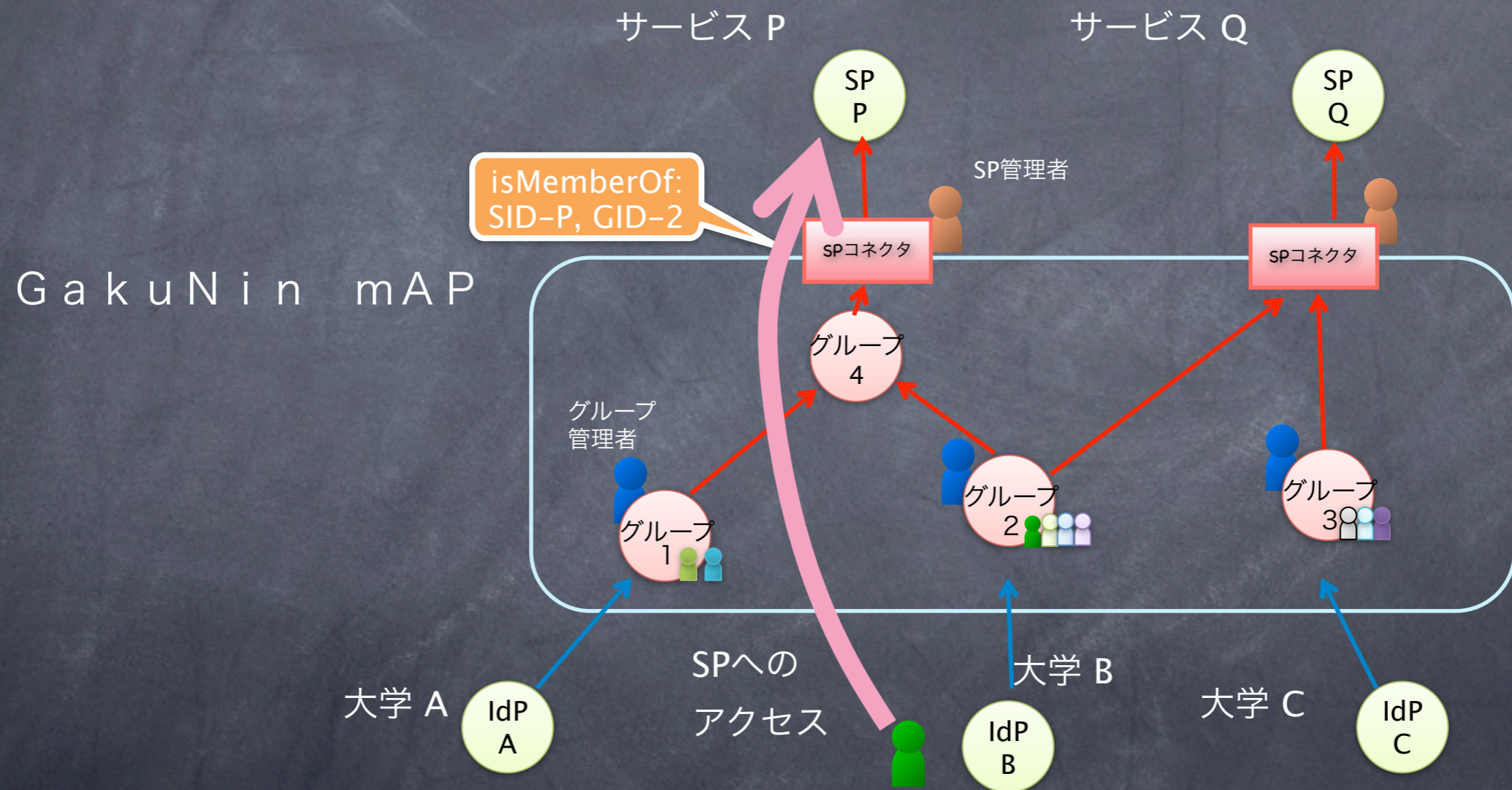
# GakuNin mAPの紹介

2011.9.14 学認CAMP

西村 健

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

# GakuNin mAPのアーキテクチャ



# 利点は？

- 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
- コラボレーションを目的とするサービスにグループ機能の作り込みが不要になるだけでも...
  - 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

# グループ

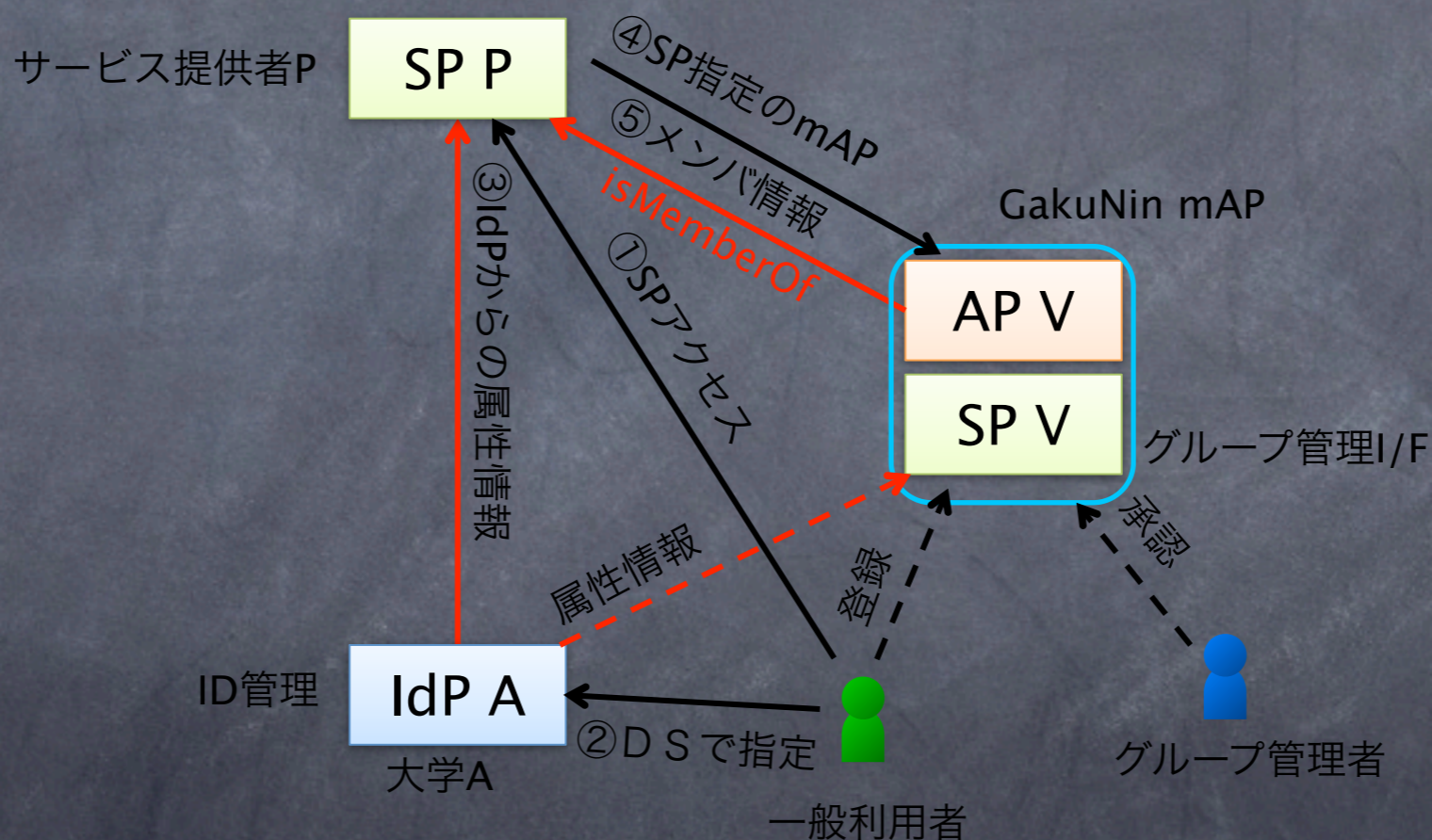
- いわゆる「グループ」  
任意の「学認IDの集合」を表すもの
- メンバーの構築方法
  - 管理者（作成者）からの招待（招待メール）
  - 利用者がグループを指定して入会申請する
  - 利用者が自由入会する — コミュニティ的なもの

# SPコネクタ

- SPとグループの間で接続関係を管理するもの
  - グループは、SPコネクタに接続しなければ一切情報は流されない！（プライバシー配慮）
- SPコネクタには2種類ある
  - SP（サービス）の利用形態をそのまま表したもの
    - 契約ベース — SP側による完全コントロール
    - 自由利用 — グループ側から自由に接続できる

# グループ属性送信のプロトコル

- 所属グループの情報は、Shibbolethの属性の一つ(isMemberOf属性)として、IdP認証と同時に取得される



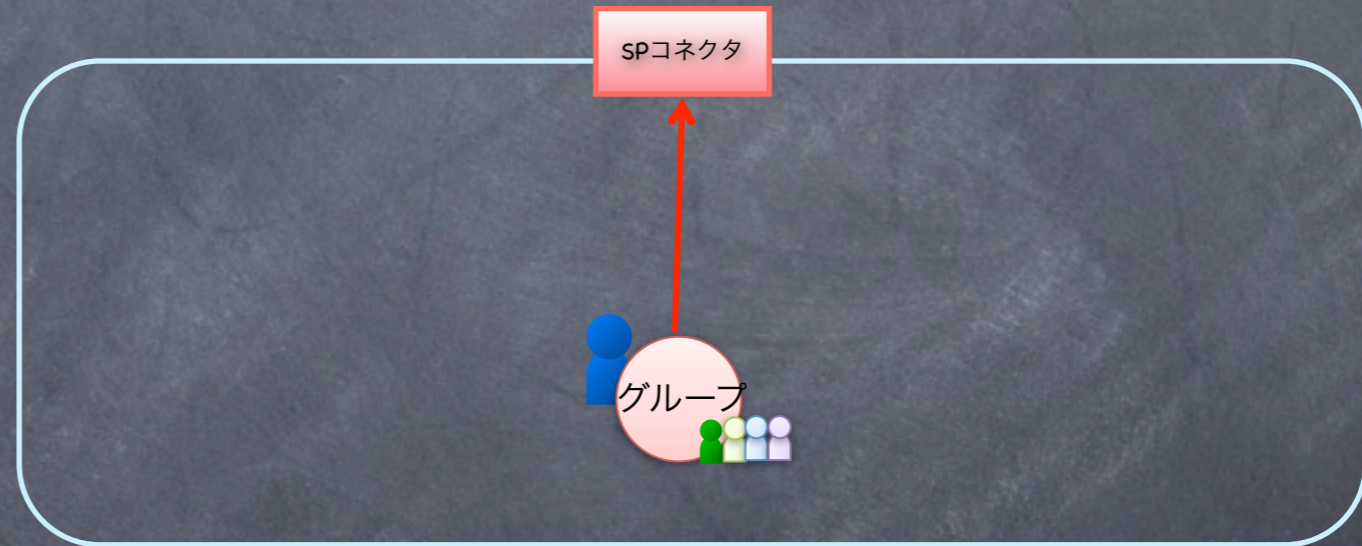
既存のShibboleth SPの機能を利用しているので

安心！

# ケース1 (一般的)

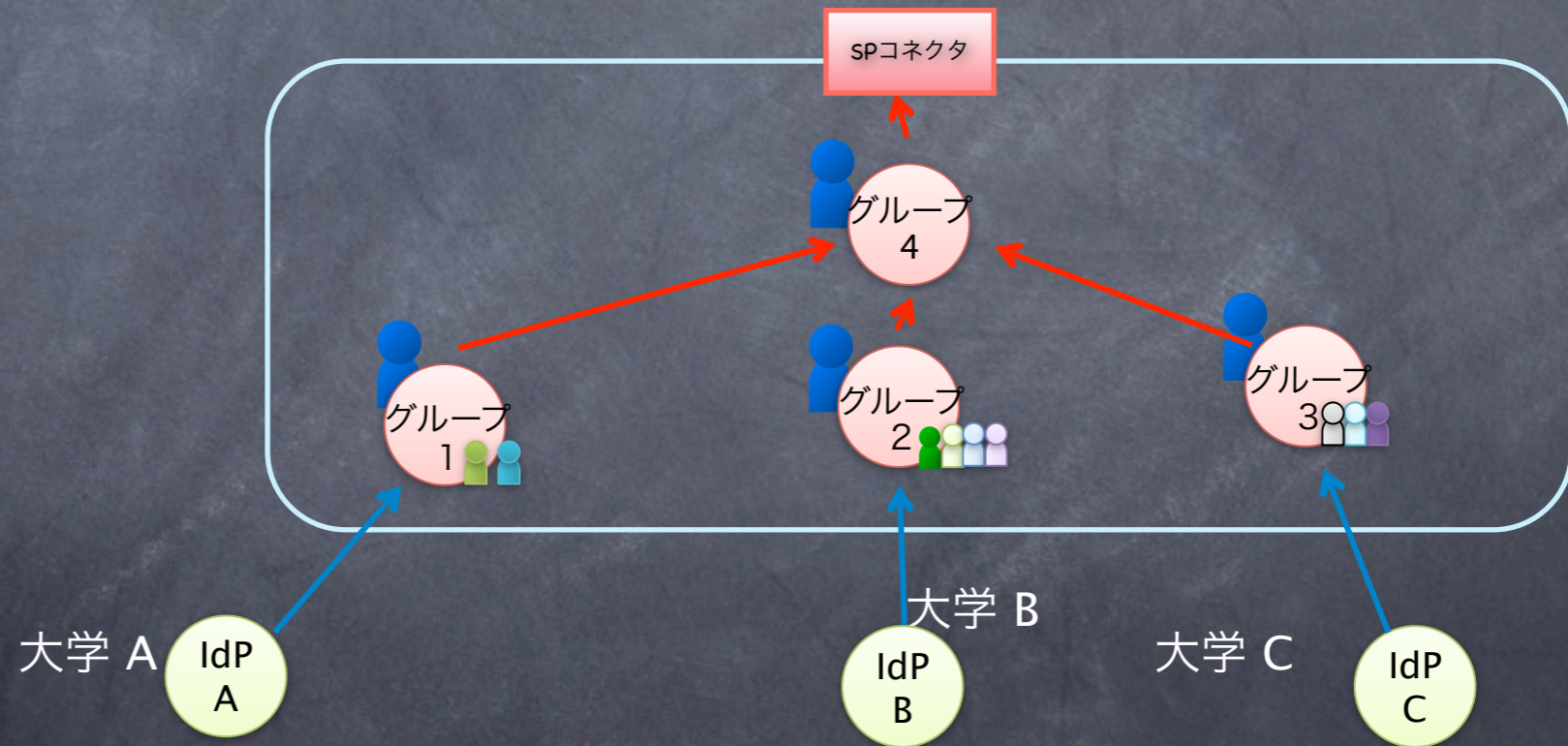
- 独立グループと呼ぶ

(ケース2,3は非独立グループ)



# ケース2 (メタグループ)

- 大学をまたがるコンソーシアムなど
  - SPには1,2,3全てのメンバーが4のメンバーに見える

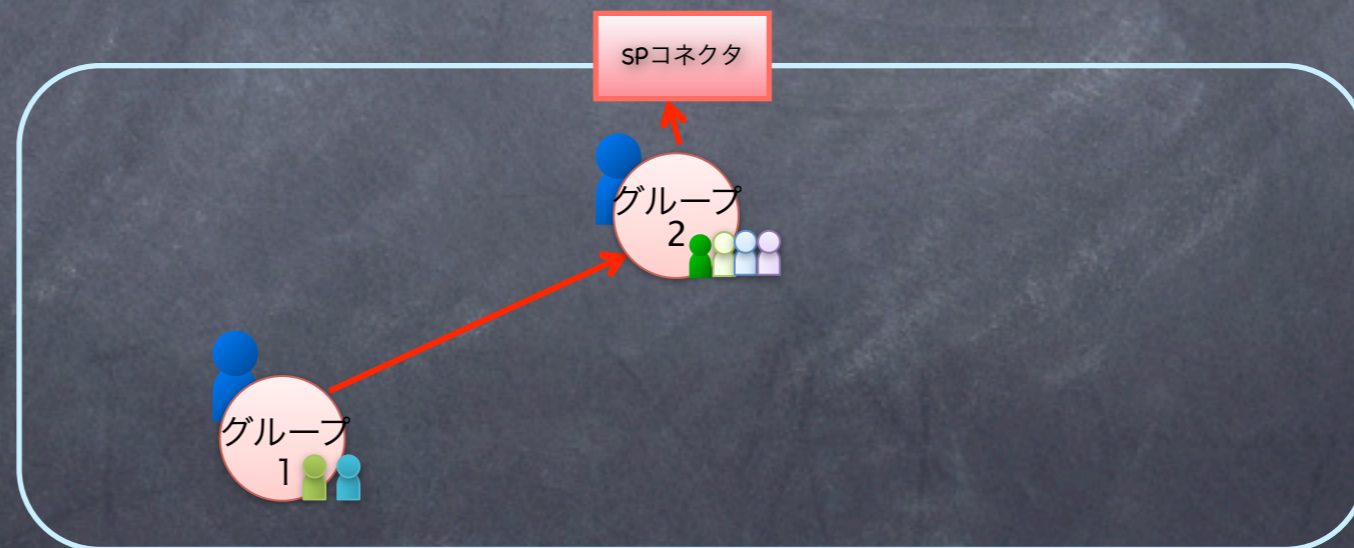




# ケース3

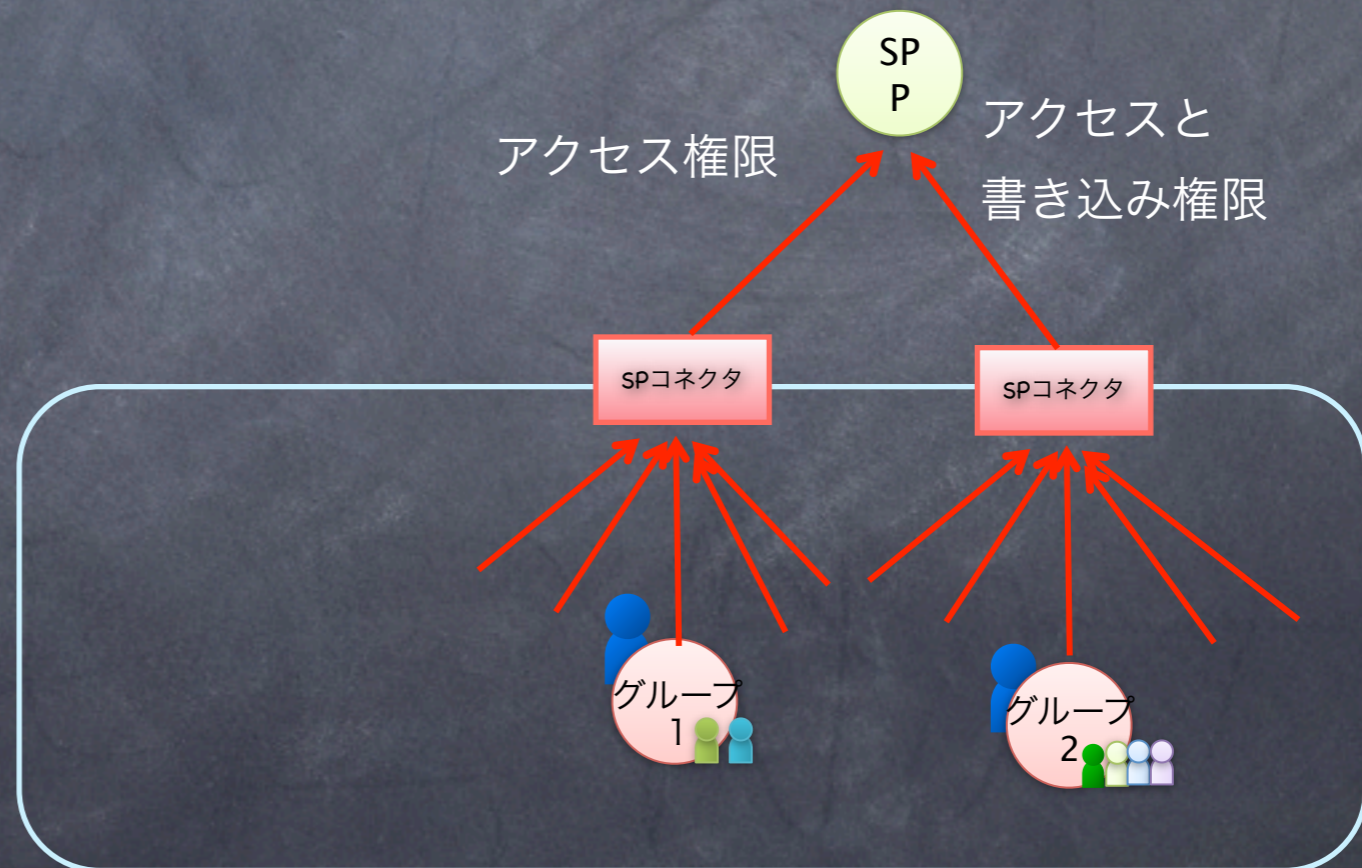
- 一部のメンバーの管理を他人に任せる場合など
  - 応用例：学部と学科の関係

(学部メンバー ⊃ 学科メンバー なので)



# ケース4 (SPコネクタ複数)

- SP側で権限の違うグループを扱いたい場合、SPコネクタを複数用意して同じSPに接続します



# GakuNin mAP FAQ

● GakuNin mAPがIdPになるの？

NO

● グループ階層の下のグループはサブグループ？

NO サブグループはグループの中で  
作るもので概念が違う

● グループ階層は組織の階層を表すの？

NO 単なるメンバーの包含関係を表すのみ

(=上位グループは下位グループのメンバーを  
含む)

# 連携例 1 : meatwiki

- GakuNin mAP対応のWiki

- グループメンバーのみが読み書きできるスペースを提供する

- グループ内の情報共有 / 情報交換に使える

- ピュアな連携例

# 連携例 2 : meatmail (開発中)

- GakuNin mAP対応メーリングリストサービス

- ピュアな実装ではメンバーのメールアドレスをIdPから取得しなければならない

- 全てのメンバーがMLサービスにアクセスしてからでないとMLとして機能しない？



- 連携APIが必要

- SPからグループIDで問い合わせる

- mAPがメンバーのメールアドレス一覧を返す