これからの次世代学術認証 パネルディスカッション （Orthros・グループ管理）

京都大学 情報環境機構
古村隆明

京都大学

KYOTO UNIVERSITY

京都大学の認証基盤の紹介

2008年 統合認証基盤の運用開始

- 学生アカウント:　教育用コンピュータシステムのアカウント
  IDの例: a0123456
- 教職員アカウント: グループウェアのアカウント
  IDの例: taro123kyoto

学内外の約100のSPとSAML連携、約40のサービスとLDAP連携。

学生・教職員が利用する多くのサービス（Microsoft365, Google Workspace などクラウドサービスを含む）を学内IdPで認証して利用可能。

京都大学の統合認証基盤の課題

- 学生と教職員のIDの統合
  - 名寄せの精度も不十分なので、IDが変わると同一人物のトレースが困難
- 利用者ごとのサービス利用可否の制御
  - 学生、教職員などの大雑把な判定だけでサービス利用可否をしている
  - 利用する必要の無いサービスにまでアカウントが登録されてしまう
    （ライセンス数不足や価格上昇を招く）
- 共同研究者として学外利用者の登録
  - サービス利用可否の制御が不十分なため、統合認証基盤に入れづらい
- 兼務に関する情報拡充
  - 複数の身分を持つときの情報が不十分、制約多い

身分・所属組織が変化しても個人を特定できる識別子

学内での話
[現状]
- 学生と教職員とでアカウント体系が分離
- 学生→教職員、学生→OB、教職員→OB などの身分変更でID変更

→ 身分に因らない「学内統合ID」（検討中）

組織を越えた話
- 転職するとID・アカウント変更
- （学内のように）統合IDを作るのは難しい

→ 異なるIdPの異なるIDで認証しても、
OrthrosのIDと紐付けることで同一人物の識別子（ePPN）を同一に

複数の身分・所属組織への対応が必要

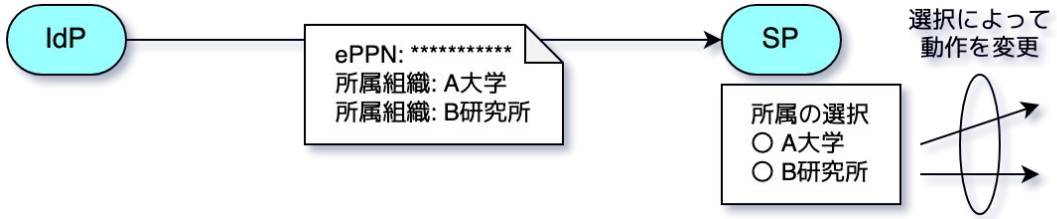
身分・所属組織が変化しても同じ識別子で特定できる環境を構築すると、
身分・所属組織を同時に複数持つアカウントに対応する必要がある
（例）

- TA・RA・OA など（学生であり、給与支払対象者）
- 兼務などによる複数の身分
- 兼業による複数の所属組織

課題1: 権限の選択

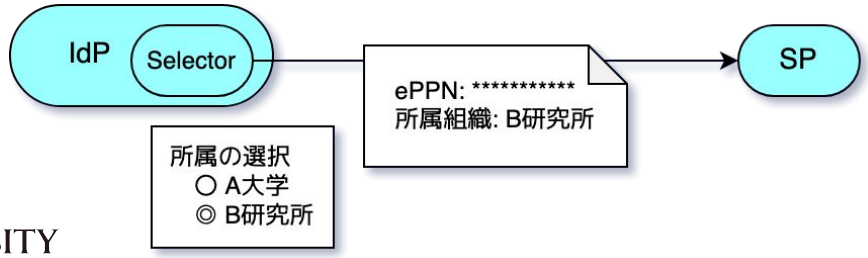
複数の身分・所属組織を持つときに、サービス(SP)をどの権限で利用するか？

- SP側で複数の権限を切り替え可能ならSPに任せる



- 複数の権限を扱えないSPが多い

→ IdP側でどの権限(どの身分・どの所属)で使うか選択したい

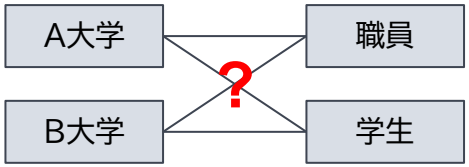


課題2: 複数の身分・所属組織などの情報管理

複数の身分・所属組織を扱うときに、どのように属性情報を管理するか

[現状]

```
organization: A大学
organization: C大学
eduPersonAffiliation: 職員
eduPersonAffiliation: 学生
```



正しい組み合わせが分からない。

[提案]

```
eduPersonEntitlement: A大学:職員
eduPersonEntitlement: C大学:学生
```

組み合わせて管理する必要があるのではないか？

AARC Blueprint Architecture "Guidelines on expressing group membership and role information (201710)" で `eduPersonEntitlement` 属性での利用が提案されている
https://aarc-community.org/wp-content/uploads/2017/11/AARC-JRA1.4A-201710.pdf

課題3: Orthros利用前後の紐付け

組織のIdPで直接認証しても、Orthros経由で認証しても、
SPで同一アカウントだと認識できる属性情報を送って欲しい