Design and Implementation of Portal System for Subscribed Cloud Services in Identity Federation

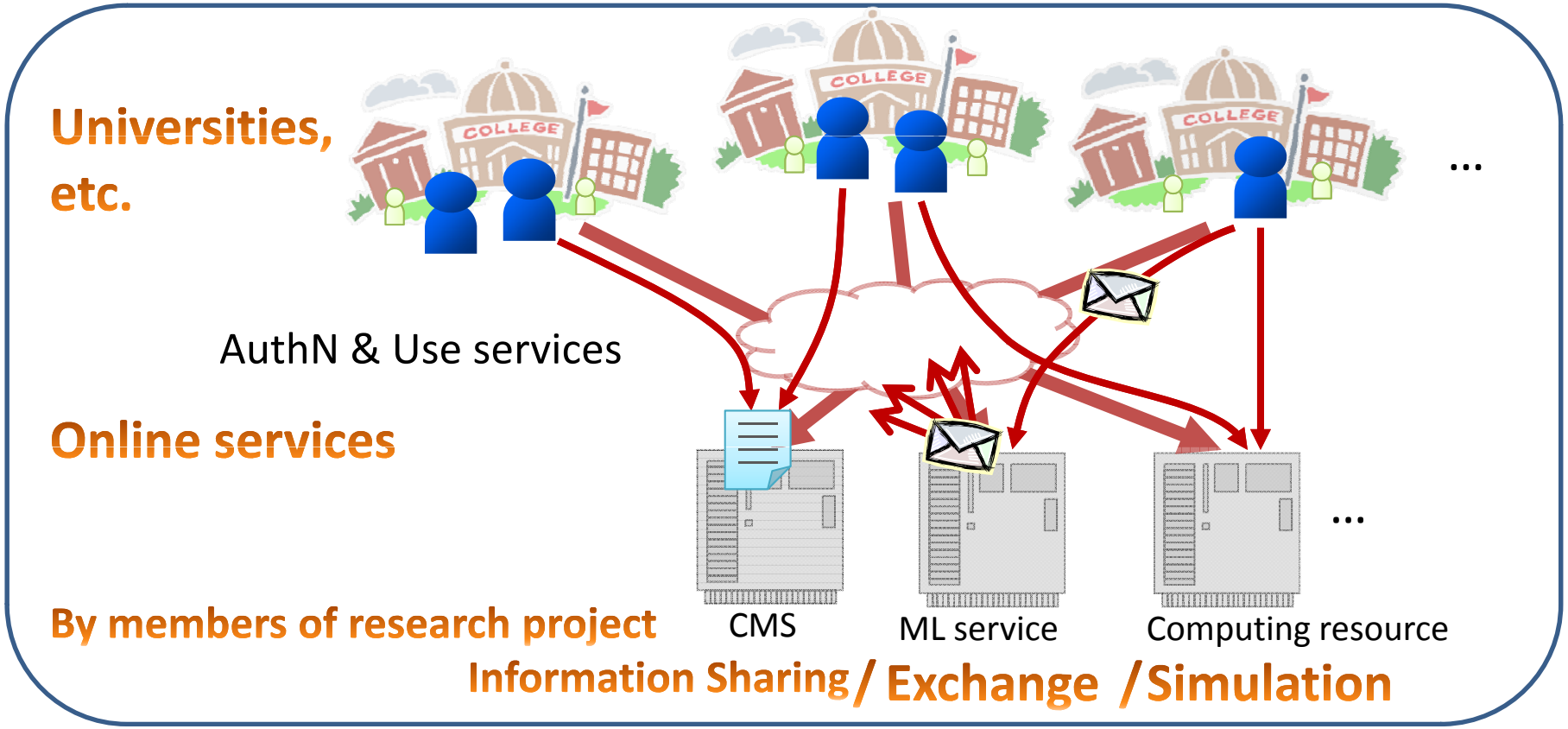
National Institute of Informatics

Takeshi Nishimura

Background: Supporting R&E and Importance of AuthN Technology

GOAL: Platform to ease to use various cloud services supporting research & education (R&E)

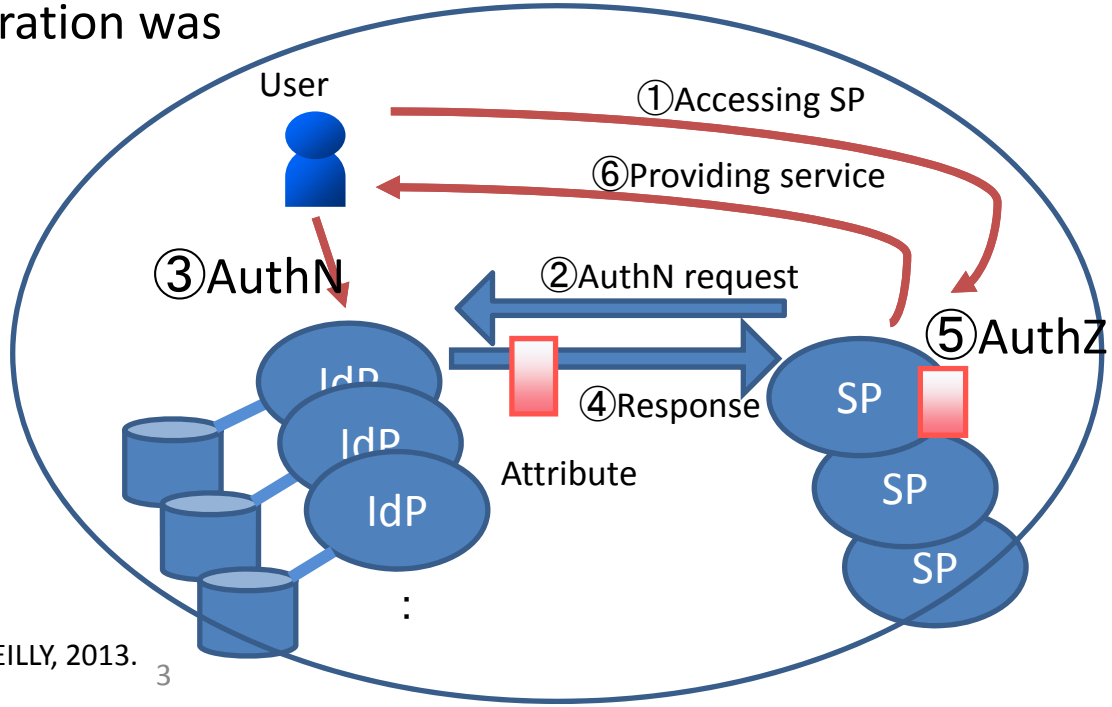
- Research & Education, for example
  - Promoting research project (information sharing, exchange, scheduling)
  - Writing papers (searching papers, viewing papers, collection)



What is Identity Federation

- **Identity federation** is a set of IdP and SP [1]
  - IdP…Identity management system belonging to a organization
  - SP…Service that utilize authN result
  - Separation of authN and authZ, centralized authN
    - AuthN…Identifying and confirming who the accessing user is
    - AuthZ…Permit accessing or not for the user
  - IdP sends **attributes** and SP utilizes them to authZ.
  - Historically academic federation was built in each country.

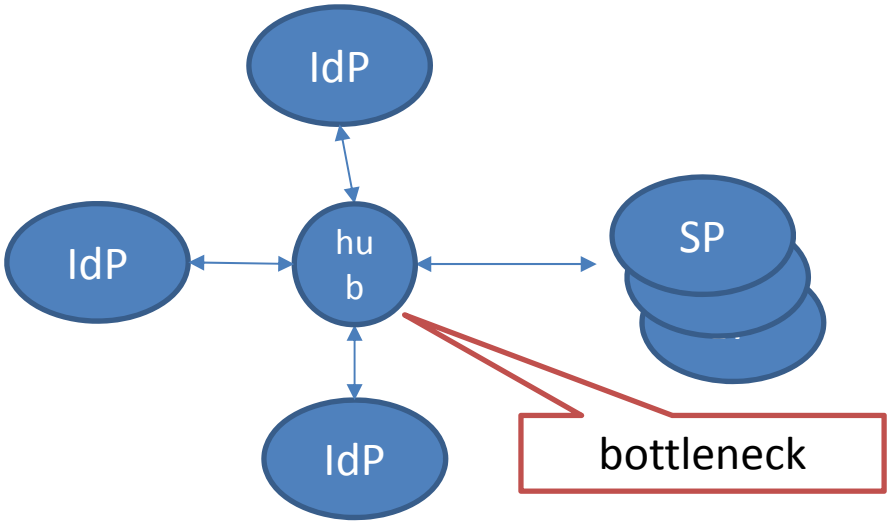
Identity Federation



[1] Phillip J. Windley, "Digital Identity," O'REILLY, 2013.

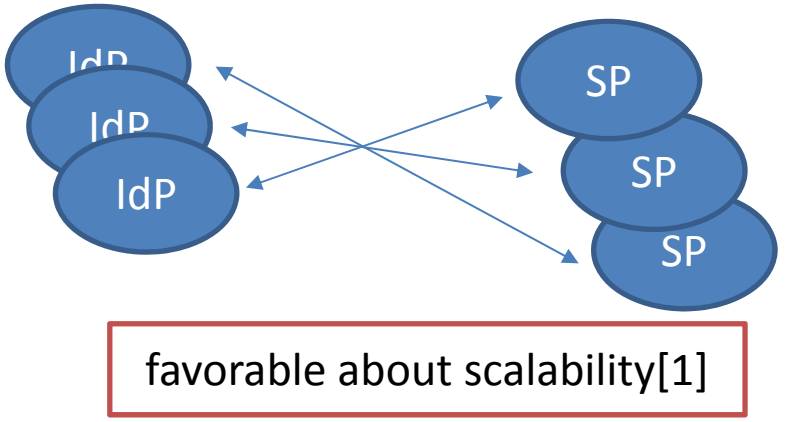
Topology of Federation

hub-and-spoke



Example: SURFconext, WAYF.dk, …

full-mesh



Example: GakuNin, InCommon, UK Fed., …

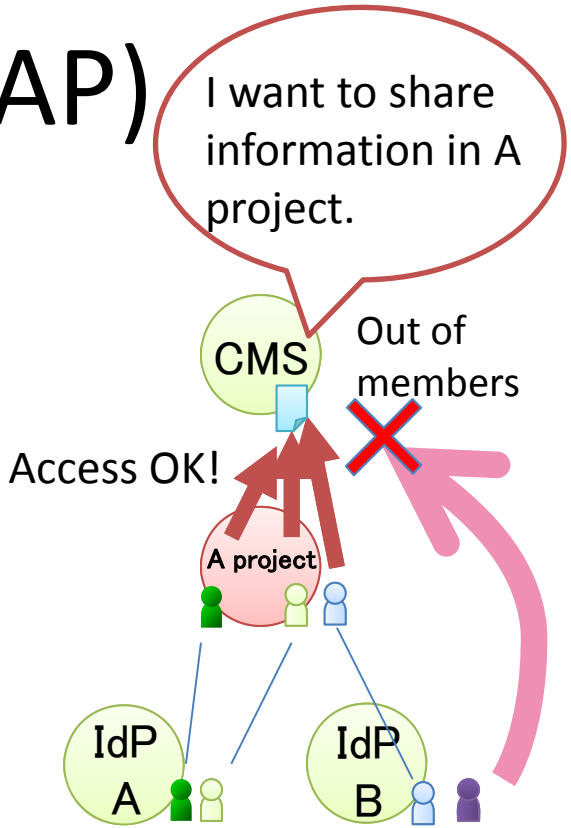
- Our research focuses on full-mesh, which is capable of large-scale federations.

[1] Phillip J. Windley, “Digital Identity,” O’REILLY, 2013.

Attribute Provider (AP)

- **Individual attribute** is not enough for supporting R&E.
  - Example: sharing information in A project
  - New attribute for authZ in SP
    - it indicates "The user is a member of X group"

    = **Set attribute**
- IdP cannot provide all of set attributes
  - labo. member, joint project member, society member, …

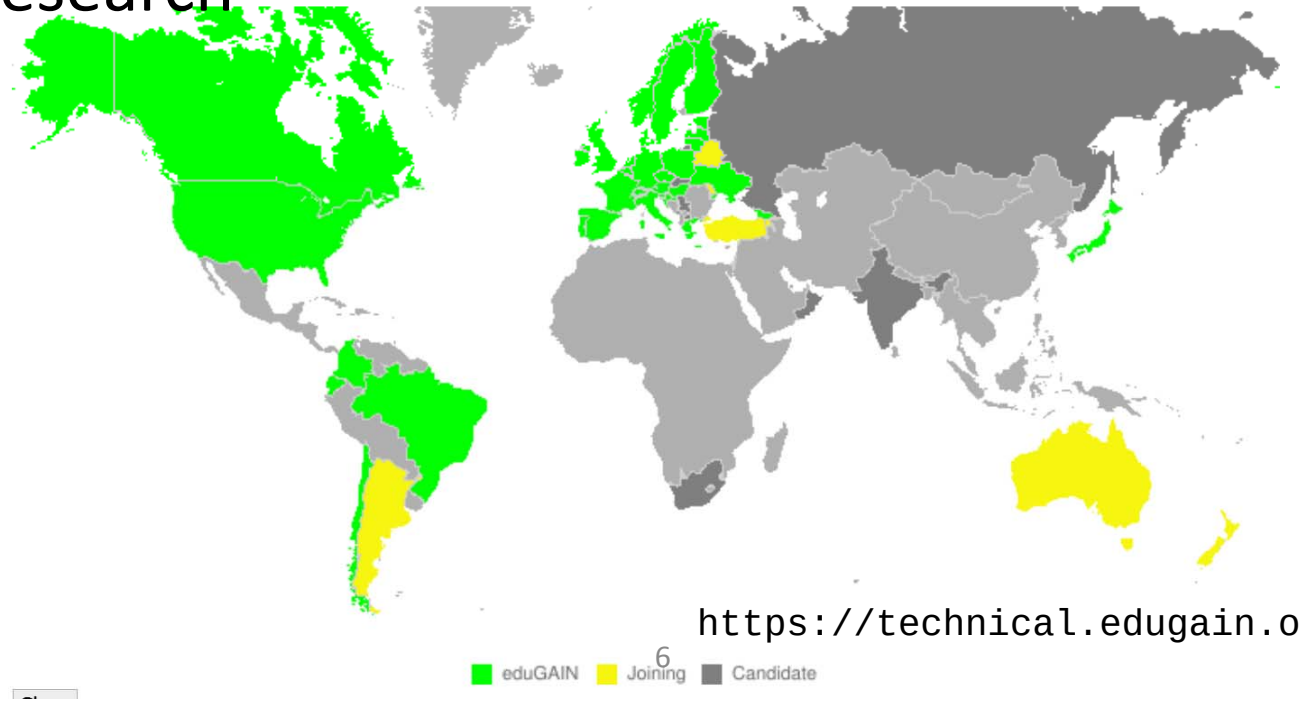


- To solve this problem, some federations operate independent **Attribute Provider** (AP), which manages set attributes for federated identities.[2]

[2] M. PROCHÁZKA, S. LICEHAMMER, and L. MATYSKA, "Perun – Modern Approach for User and Service Management," Michal , IST-Africa Conference Proceedings, pp.1-11 (2014)

Coping with inter-national cooperation

- Inter-federation framework is spreading. It is called “eduGAIN”.
  - Users can use SPs in the world – international joint research



https://technical.edugain.org/status.php

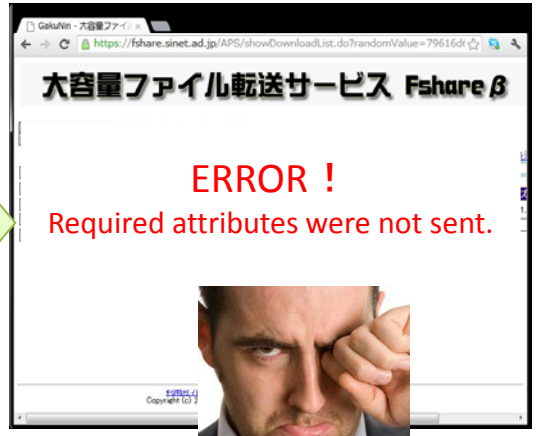
Problem

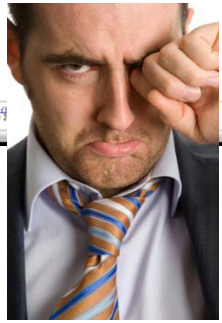
According to increase of SPs and presence of AP, it is difficult to grasp accessible services by himself.

- For example, someone may know that the service is inaccessible, after entering his password.

OK, I select my org. “NII” …

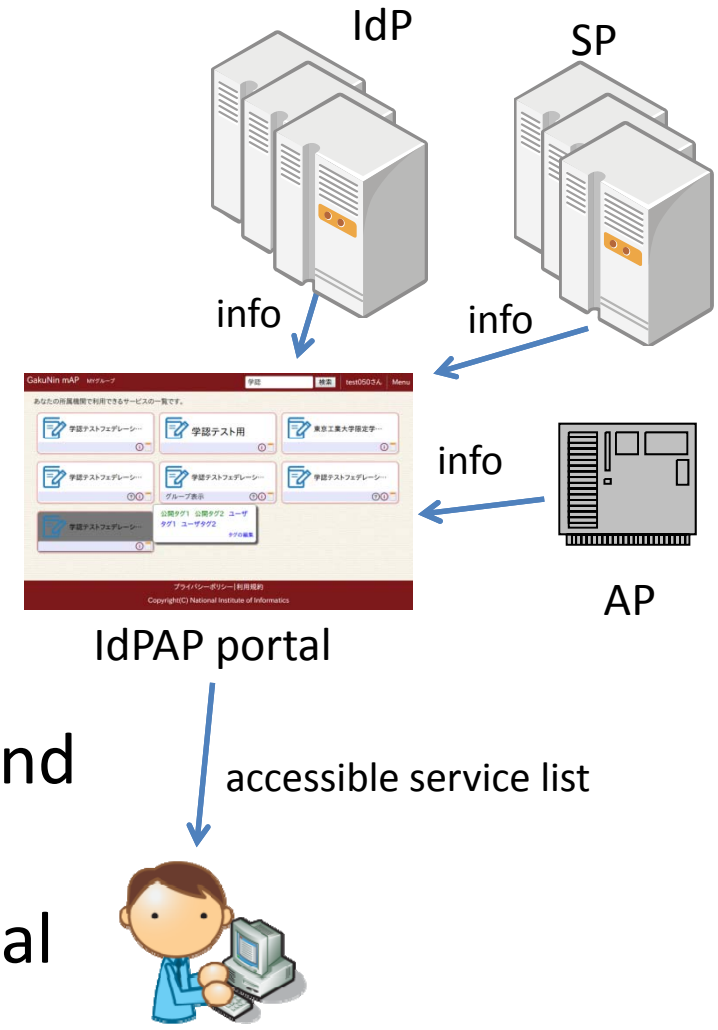
Entering my password …





Purpose of this research

- We propose service accessibility determination mechanism, which enable users to know accessible services on the portal.
  - Information gathering mechanism based on authN and authZ model
  - Implementation of IdPAP portal



Related work and system（1/2）

- Portal services to show accessible services
  - e.g. Azure AD[3], Google Apps Marketplace[4]

- These services collect information from IdP. But, there is no consideration of “AP”.

- The proposed system also incorporates AP’s information to show AP-dependent services.

[3] https://azure.microsoft.com/ja-jp/services/active-directory/
[4] https://apps.google.com/marketplace/

Related work and system (2/2)

- Several APs supporting R&E, such as Perun[2], have a portal functionality.
- There is no consideration of IdP, so it must be inaccurate about users' accessibility.
  - It also excludes AP-independent services, such as e-Journal, which has contract with organizations.

- The proposed system collect IdP information as well as AP's, so that it can show IdP-dependent services as well.

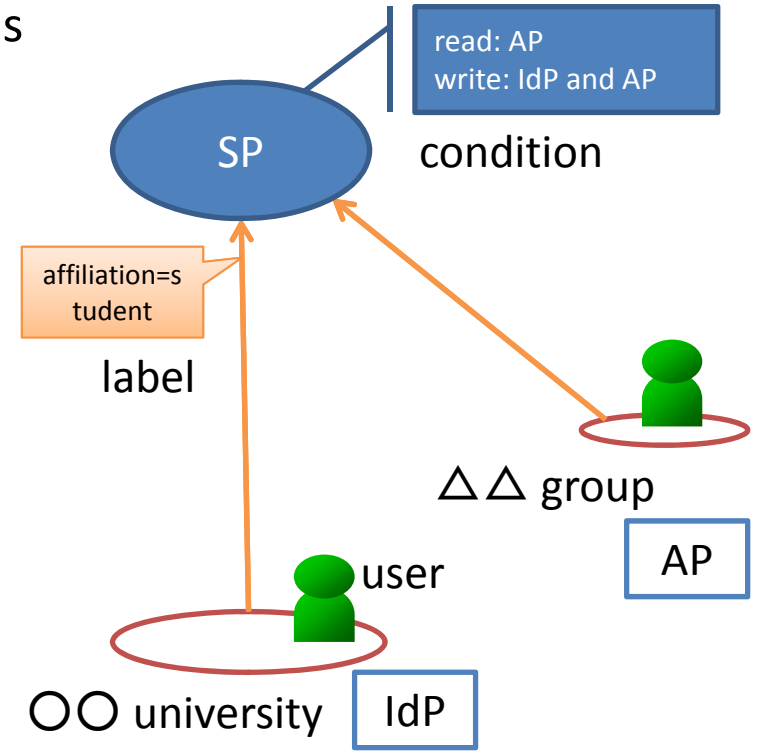
[2] M. PROCHÁZKA, S. LICEHAMMER, and L. MATYSKA, "Perun – Modern Approach for User and Service Management," Michal , IST-Africa Conference Proceedings, pp.1-11 (2014)

Proposed AuthN and AuthZ Model (1/2)

The proposed model collects information from both IdPs and APs to find accessible services.

① Graph representation of authN and authZ [5]:

- The graph consists of: users, nodes and edges
- **User**
  - is registered by one or more IdPs, and joins zero or more groups.
- **Node**: is one of IdP, group, SP
  - IdP: provides individual attributes to SP
  - group: provides set attributes to SP
  - SP: authZ by combination of attributes
    - condition: per functionality in service
- **Edge**
  - means IdP or AP sends the attributes to SP
  - label = in case of authZ by attribute values, such as “student only”

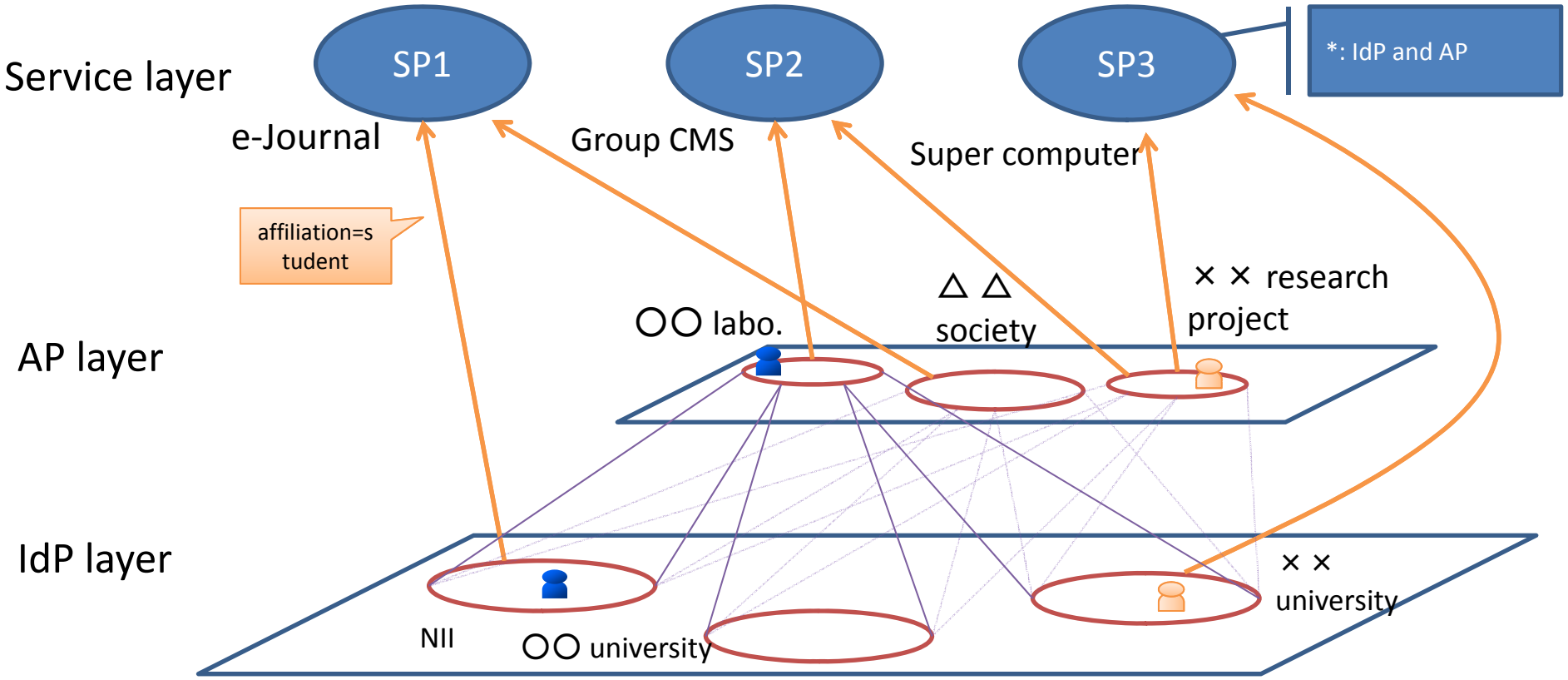


[5] 西村健, 坂根 栄作, 合田 憲人, "個人属性と集合属性が共存する認証認可モデル," 電子情報通信学会技術研究報告, vol. 114, no. 216, pp. 19-24, 2014年9月.

Proposed AuthN and AuthZ Model (2/2)

② Nodes are classified into three layers.
- Service layer – provides services
- AP layer – provides set attributes
- IdP layer – provides individual attributes

③ The proposed model finds accessible services by traversing the graph.

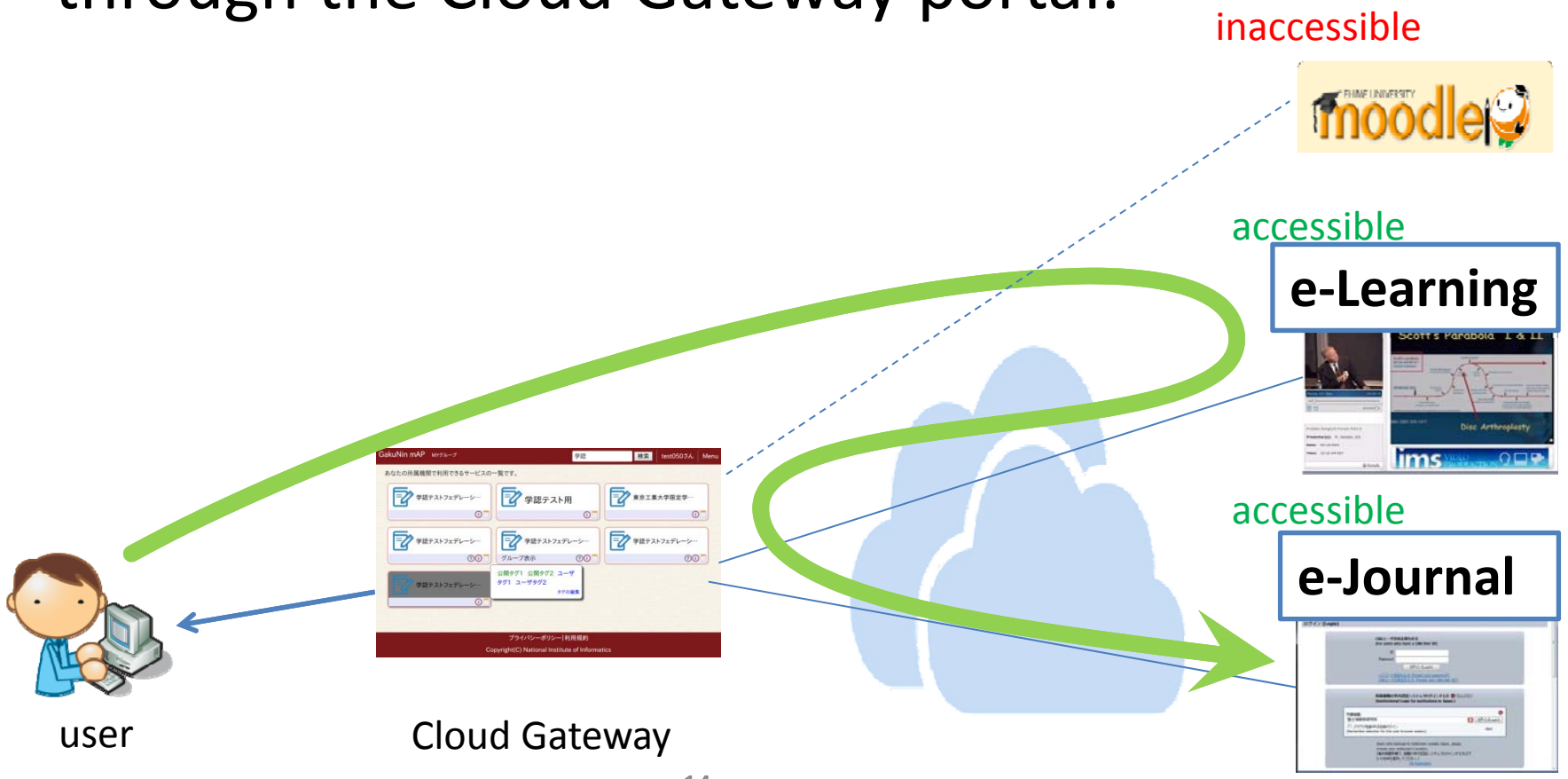


Portal System – Cloud Gateway

- Based on the proposed authN and authZ model, we implemented a portal system for federated identity called “Cloud Gateway”.
  - The portal presents accessible services for accessing user.
    - Permitted through the organization
    - Permitted through the group
  - The user is no longer confused about service accessibility.

Example

- User can access e-Learning and e-Journal through the Cloud Gateway portal.

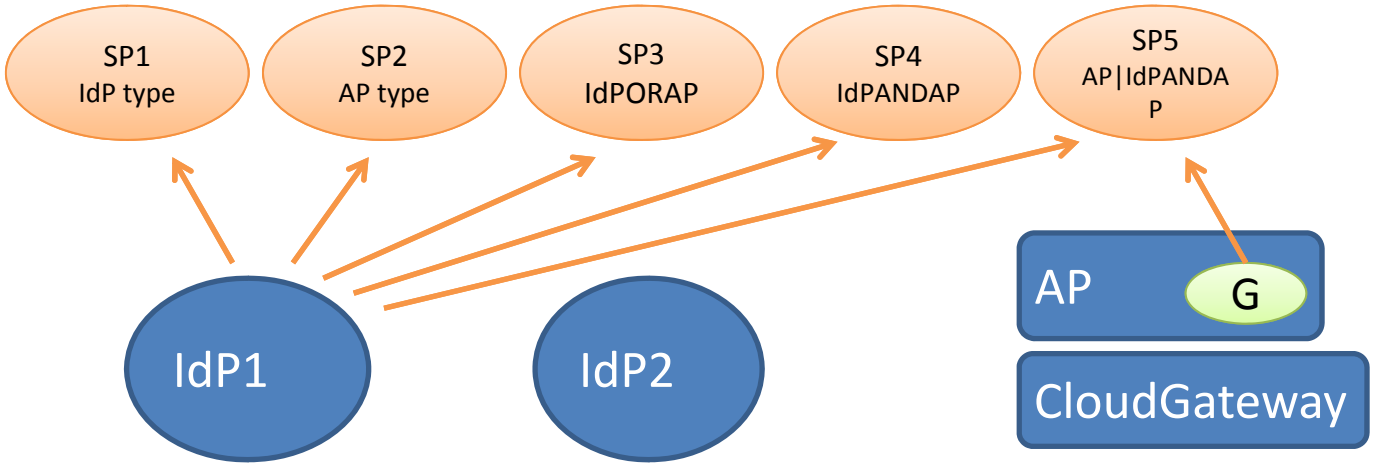


Experiment (1/2)

We run experiments with 5 settings of SPs, IdPs, AP and IDs.

Experimental Environment：

- Virtual machines on Xen（1.5GB memori, 20GB disk）
  - CloudGateway, IdP x 2, SP x 5



Experiment (2/2)

- We confirmed that the portal system selectively displays usable services by collecting proper information.

	IdP type	AP type	IdPORAP	IdPANDAP	AP|IdPANDAP
IdP1/id1	○	○	○	○	○
IdP1/id2	○	×	○	×	×
IdP2/id1	×	○	○	×	Read-only
IdP2/id2	×	×	×	×	×

DEMO

Summary & Future Work

Summary:

- We proposed service accessibility determination mechanism on identity federation containing AP.
- We implemented a portal system for federated identity called “Cloud Gateway”.
- Cloud Gateway portal helps users to find accessible services.

Future work:

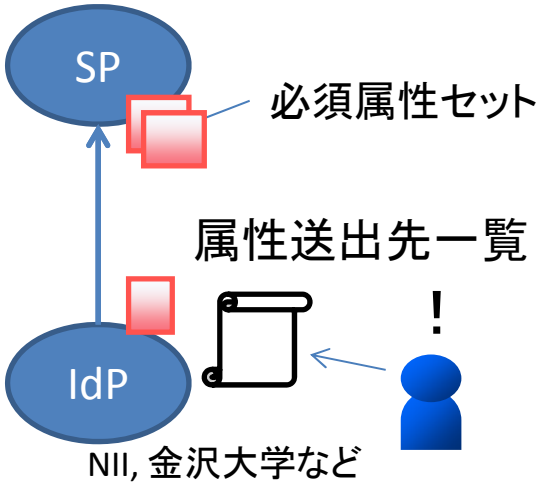
- Large-scale deployment

技術的観点からの問題点の考察

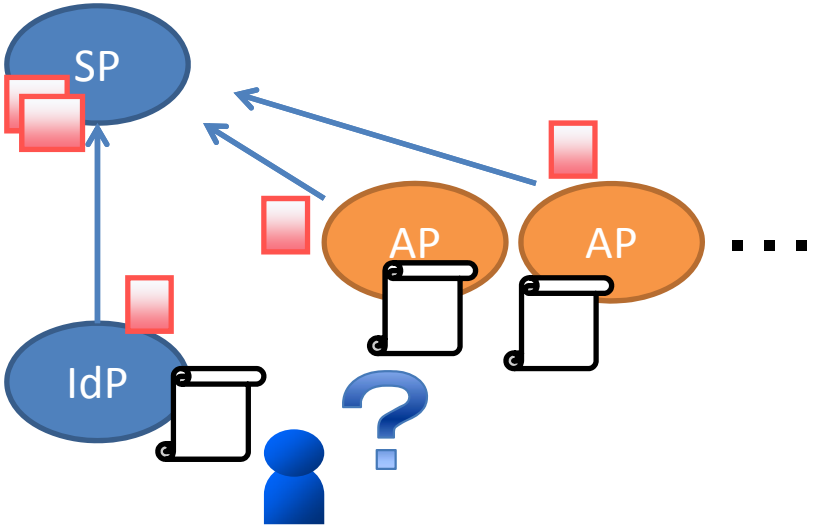
- 属性送出するのがIdPのみであればIdPが属性を送出するかどうかを調べられればよい
  – ポータル

- APからの属性を必要とする場合、それぞれの情報を調べて判断するのは現実的でない
  - SPは必須属性セットを公開していない

従来



今後



サービス利用可否を判定するための方法が必要

提案モデルの検証

SPの必須属性セットのパターンは以下の5つに分類できる。特に後半の3つについて、具体的なユースケースを設定し提案モデルで表現できることを検証する。

1. IdPからの属性のみ必要とする
2. APからの属性のみ必要とする

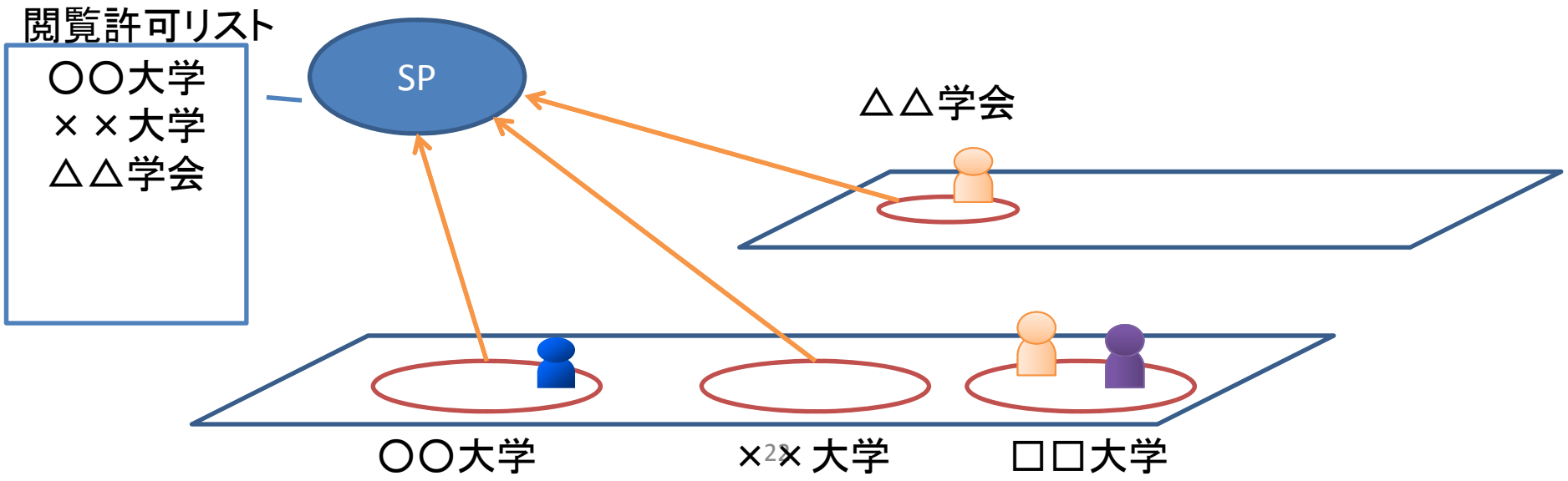
3. IdPからもしくはAPからの属性があれば利用可能
   - 学会のメンバーが電子ジャーナルを閲覧する。

4. IdPおよびAP双方からの属性を必要とする
   - 研究プロジェクトで利用申請したスーパーコンピュータをメンバーが利用する。

5. SP内の機能によって異なる必須属性セットを持つ
   - 研究プロジェクト内での情報共有のためのグループ利用CMS{を閲覧する|に書き込む}。

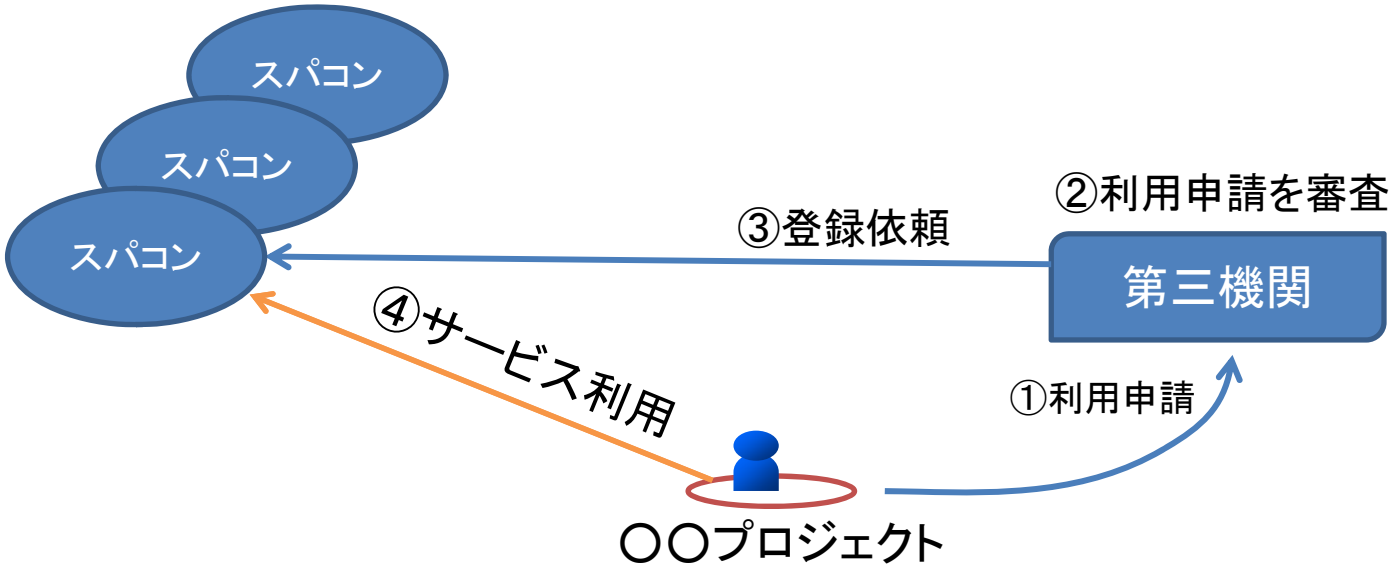
3.IdPからもしくはAPからの属性があれば利用可能

- パターン3.のユースケース
  - 複数の学会から発行論文誌の委託を受ける**電子ジャーナルプラットフォーム**がある。
    - 例：応用物理学会がIOP Publishingに委託
  - 発行学会メンバーおよびサイトライセンス契約のある大学向けに電子ジャーナルの閲覧を許可する。
- サービスが利用可能な条件:
  - 利用者が発行学会のメンバー
    OR 利用者の所属大学がサイトライセンス契約を結んでいる
- 本ユースケースのモデル化



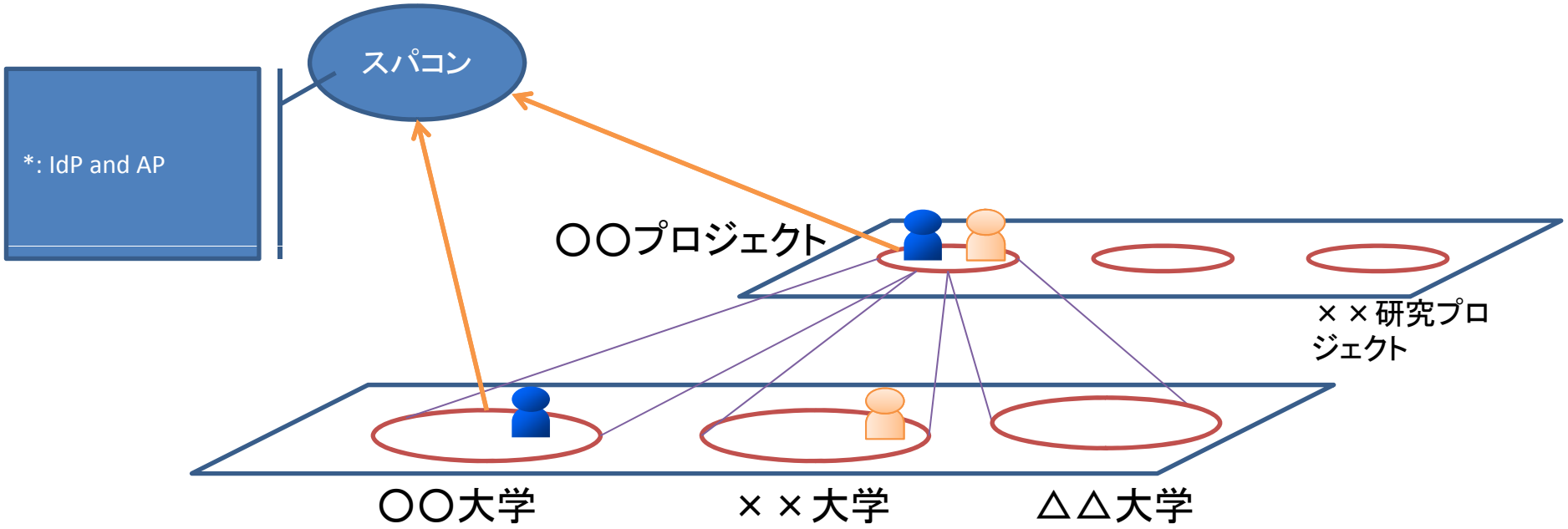
4.IdPおよびAP双方からの属性を必要とする（1/2）

- パターン4.のユースケース
  1. 利用者が、利用したい共用スパコンに対して第三機関に利用申請する。
  2. 利用申請が承認されたら第三機関が利用スパコンに対して登録を依頼する。
     - 例: HPCI
- サービスが利用可能な条件：
  - 承認されたグループのメンバー AND 所属IdPが身元保証（ID属性を送信）する



4.IdPおよびAP双方からの属性を必要とする(2/2)

- パターン4ユースケースのモデル化



5. SP内の機能によって異なる必須属性セットを持つ

- パターン5.のユースケース
  - グループ内のあるメンバーが情報を書き込む。グループ内で情報を共有し蓄積する。
  - 書き込み時にはIdPからのID属性が必須（書き込み者の記録のため）
  - 閲覧時にはプライバシー保護のためID属性は不要とする
- サービスが利用可能な条件:
  - 閲覧: ユーザが××プロジェクトに所属している
  - 書き込み:（閲覧条件）AND 所属大学がID属性を送信する
- 本ユースケースのモデル化