学認における属性の質の保証

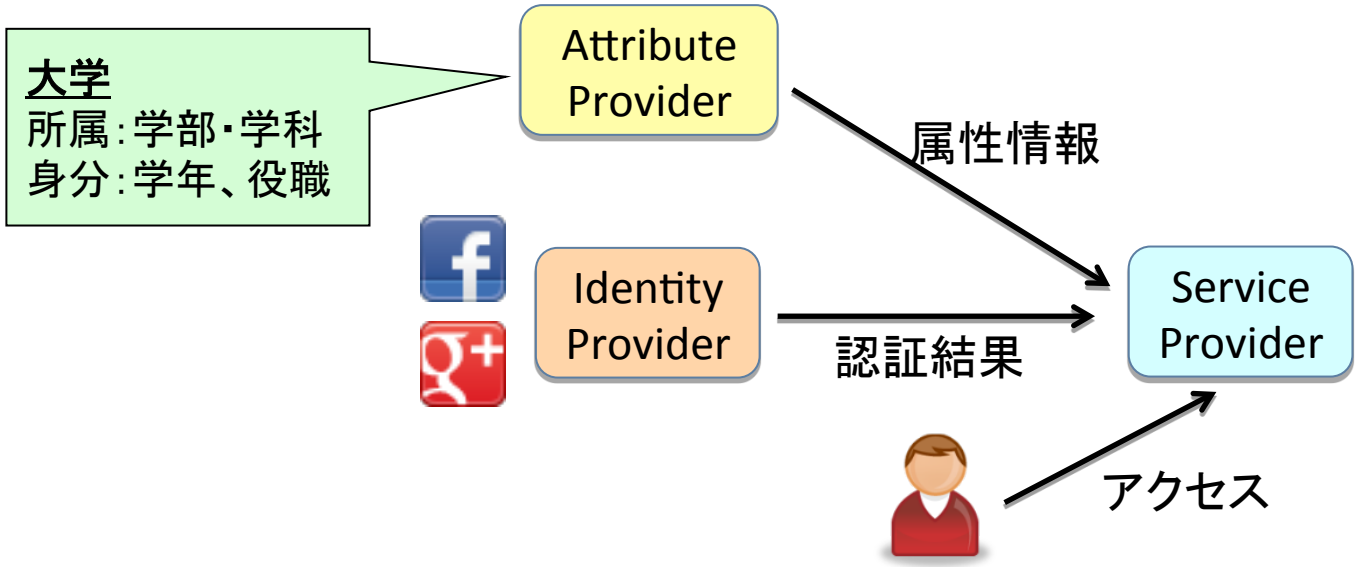
学認トラストチーム 島岡 政基 (セコム株式会社IS研究所)

アジェンダ

- なぜ属性の話?
- 属性交換がもたらす安全・安心
- 3つのアプローチ
- 学認における取り組み
- 参加機関に期待したいこと

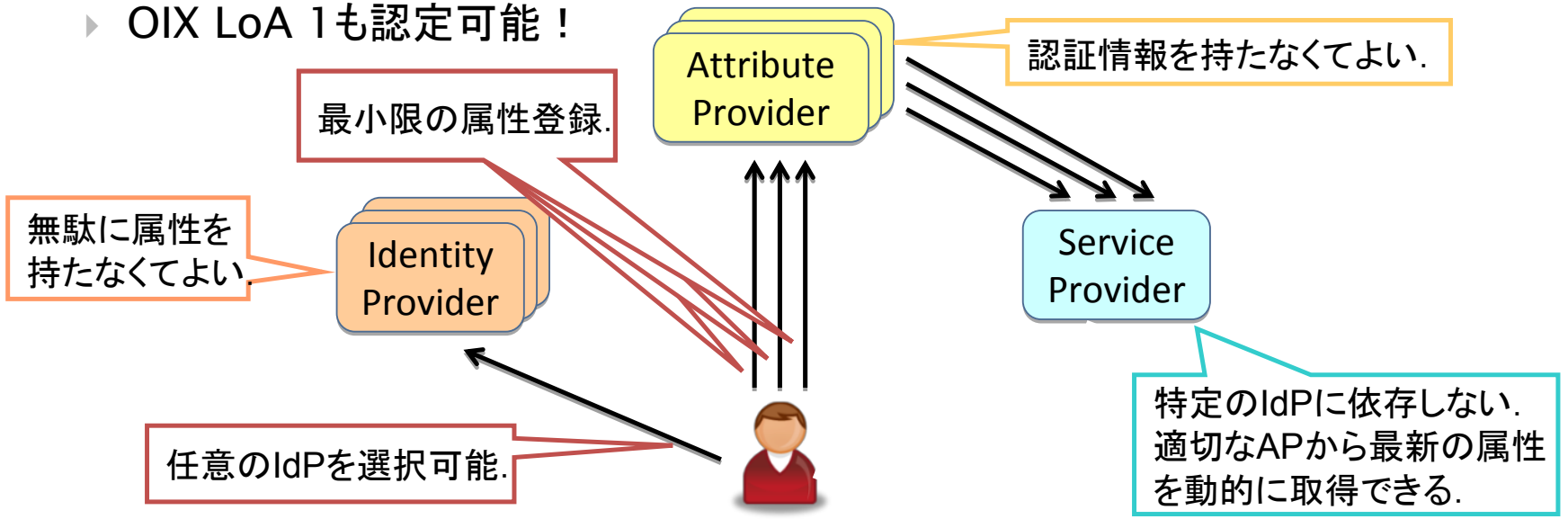
ID連携から属性交換へ

- Student Identity Trust Framework
  - OpenIDファウンデーション・ジャパンとの共同研究
  - 研究者中心だった学認の門戸を学生にも拡大する
  - 学認を活用，プライバシーに配慮したオンライン学割ビジネス
  - 民間IdPを利用し，大学IdPは属性提供者として振る舞う



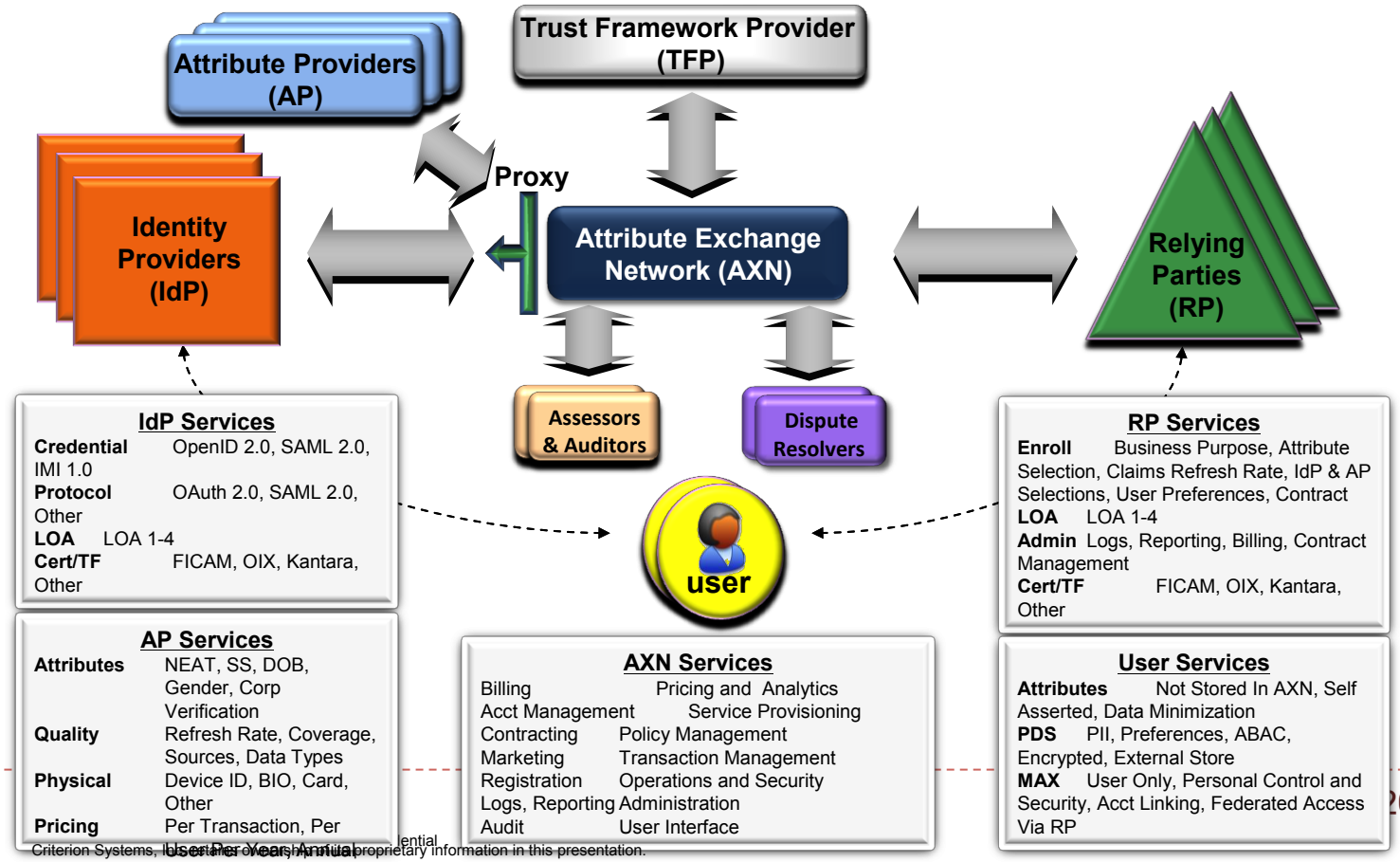
属性交換がもたらす安全・安心

- APとしての大学
  - 学績情報などを信頼できる形で提供できる**唯一の機関**
- IdPとしての大学
  - 学術サービス以外に対するIdPの可能性
  - 信頼されたIdPとして
    - 日本唯一のトラストフレームワーク
    - OIX LoA 1も認定可能！



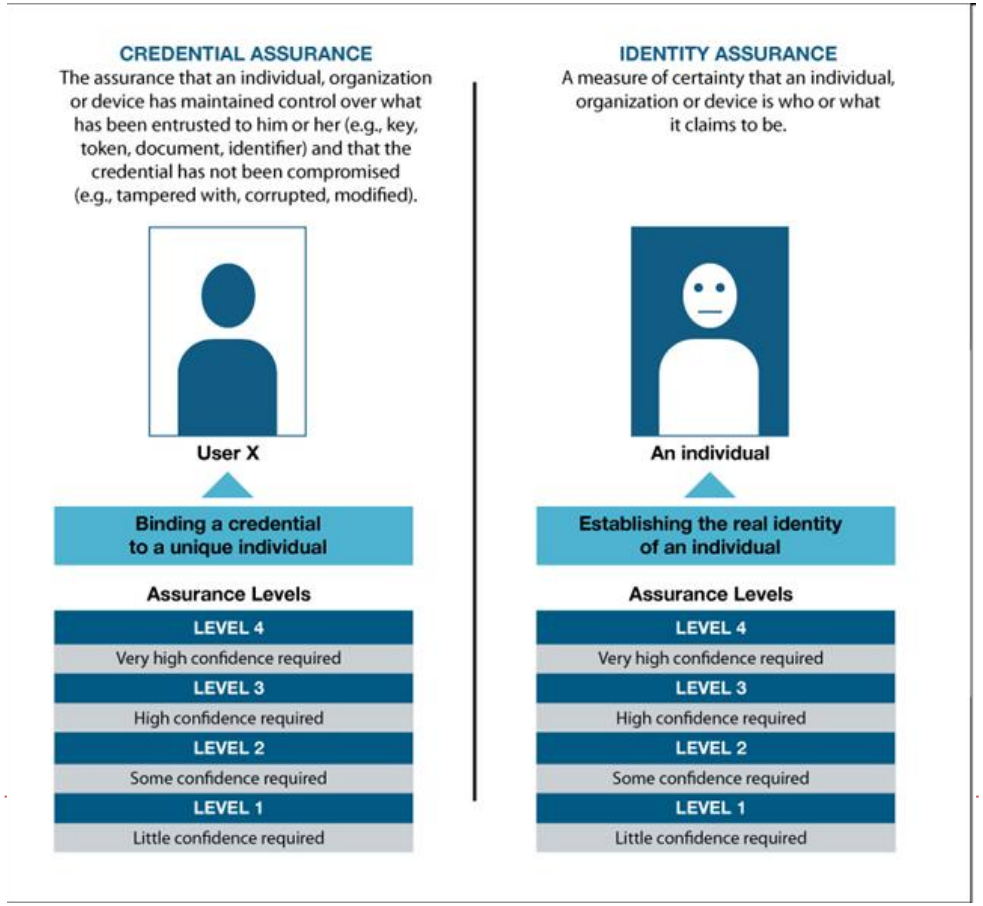
属性交換に関する海外動向(1)

- Attribute eXchange Network [1]
  - 米連邦政府ICAMにおける属性交換の仕組み
  - IdP/APとSPの間にプロクシを置くことでプライバシーに配慮



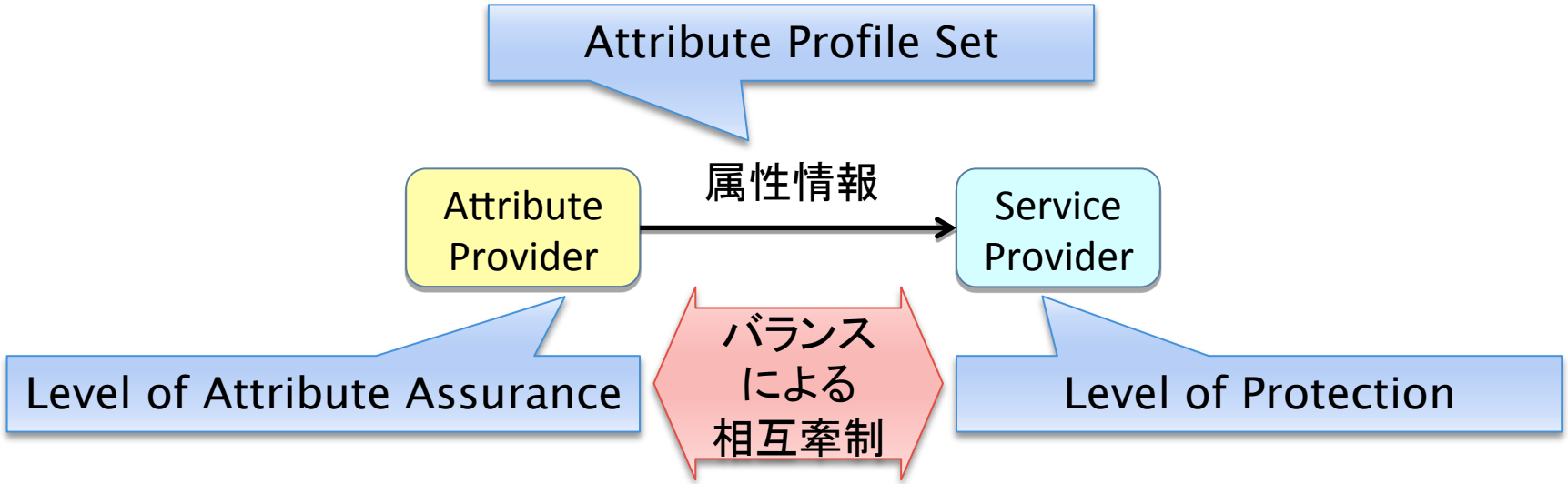
属性交換に関する海外動向(2)

- Pan-Canadian Assurance Model [2]
  - カナダ政府における属性の保証レベルの定義
  - 属性情報と認証情報を区別して保証レベルを定義している



属性交換3つのアプローチ

- 扱う属性の種類，内容(値)の定義が必要
- 属性プロファイルセット全体としてのLoAA



- SPは，APから提供される属性を信頼してよいものか?
- 提供する属性について，APは一定の保証を行う必要がある

- APは，属性を提供するSPを信頼してよいものか?
- 提供された属性に対して，SPは一定の安全管理義務を負う

学認における取り組み

- 属性プロファイルセットの策定
- Level of Attribute Assuranceの策定
- (Level of Protectionについてはこれから)

- まずはSITFをケーススタディとして取り組む
  - SITFで必要な属性をスコープとする
  - SITFで知見を集め，その後順次拡充させていく

属性プロファイルセット

≠studentのエンティティについては提供しなくてよい

- SITFで扱う属性は下記の2種類.
  - eduPersonAffiliation = student
  - Organization
- これら以外の属性を提供することも可能，ただし，その保証レベルについては対象外とする.

属性プロファイルセット(1)

- ‘student’(学生)の定義
  - 学生属性の定義は「(当該)***機関に在籍し、その機関の学務の管理対象になっているもの***」を基本とする。
    - あくまでも基本方針
    - 各大学に厳密にこれを適用することは難しい
      - 留学生，単科履修生など大学によって扱いが異なる
  - なお、学生属性を付与する対象は厳密には各機関によって異なるため、各機関は学生属性を付与する基準についてSPに明示しなければならない。
  - SPは、厳密な定義が機関によって異なることについて理解を示し、必要に応じて各機関の規程を確認した上で、学生属性の利用について同意しなければならない。

属性プロファイルセット(2)

- Organizationの値の定義
  - 機関が学認参加時に機関名として届け出た文字列とする

Level of Attribute Assurance

- 3つの軸でレベルを評価する
  - 鮮度(Freshness) →属性値の最終確認日
  - 正確度(Accuracy)
  - 認証情報との紐付け(Linkage of Attribute to Identifier)
- 例えばLevel 2を取得するには，すべての評価軸でLevel 2以上の規準を満たす必要がある
  - まずはOIX LoAと同様LoAA 1から始める予定

参加機関に期待したいこと

- 属性交換を積極的に行いたいと思った機関は，以下の準備を是非進めておいてください
  - 学生の定義の明文化とSPへの開示
    - SPだけがアクセスできればPublic Accessである必要はありません
  - 属性値の適切なライフサイクル管理(言わずもがな)
    - 卒業，退学などに応じて速やかに更新してください
  - 属性値の最終確認日の管理
    - 学務情報の最終更新日など
- 学認トラストチームが可能な限り支援します
- まずはご相談ください
  - gakunin-office@nii.ac.jp

参考資料

- [1] David Coxe, “Online Identity Attribute Exchange 2013 Initiatives” in part of Panel Discussion: Attribute Exchange and Information Sharing in Action, Federal ICAM Information Sharing Day and Vendor Expo, June 18, 2013.
- [2] Assurance, Identity and Trust Working Group, “Pan-Canadian Assurance Model”, March 3, 2010.