



# 学認が目指す認証高度化

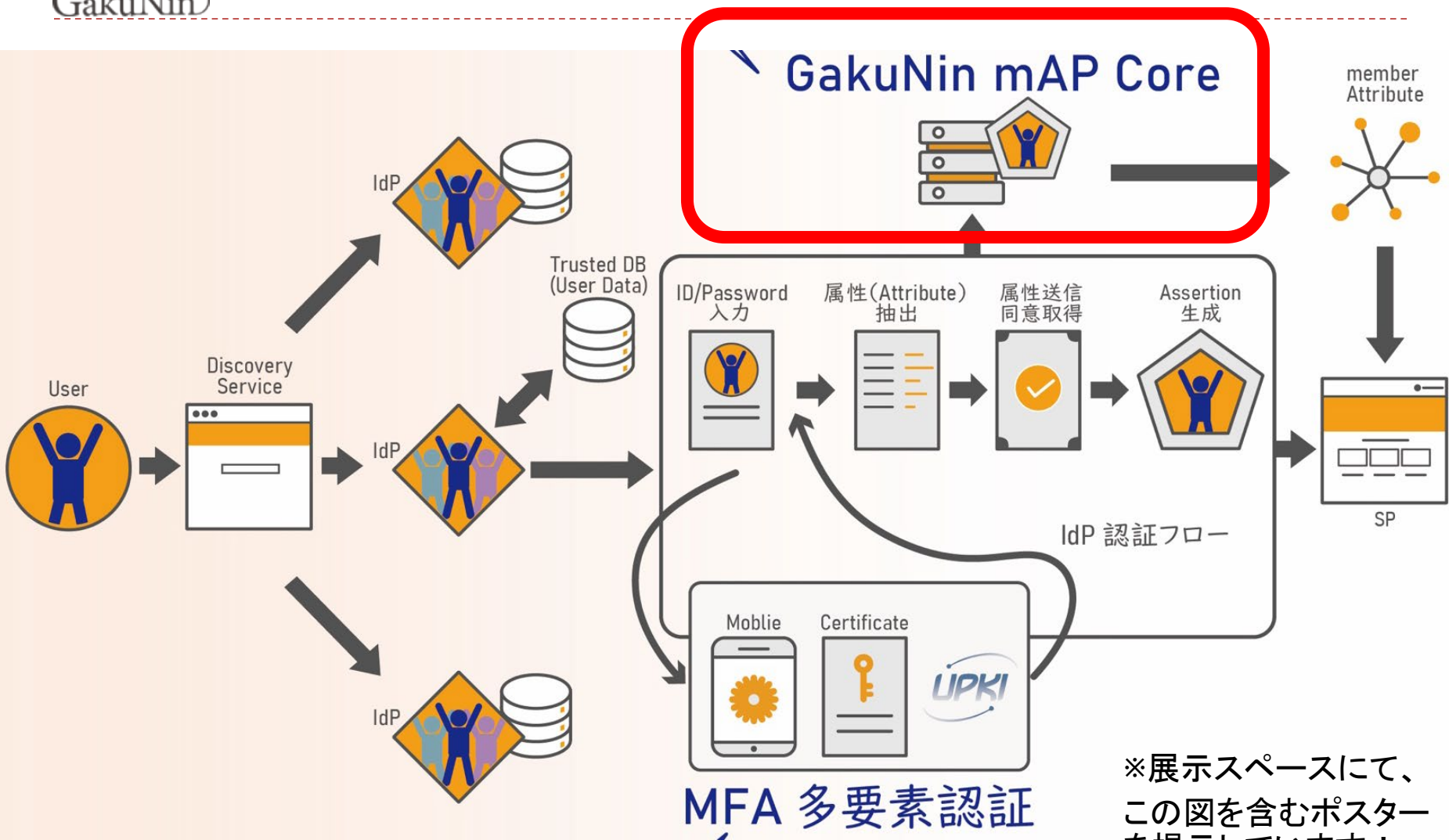
2019.12.12 AXIES2019  
国立情報学研究所 西村 健

- ① mAP Coreによるコラボレーション
- ② MFAの推進



# 認証高度化①:mAP Coreによるコラボレーション

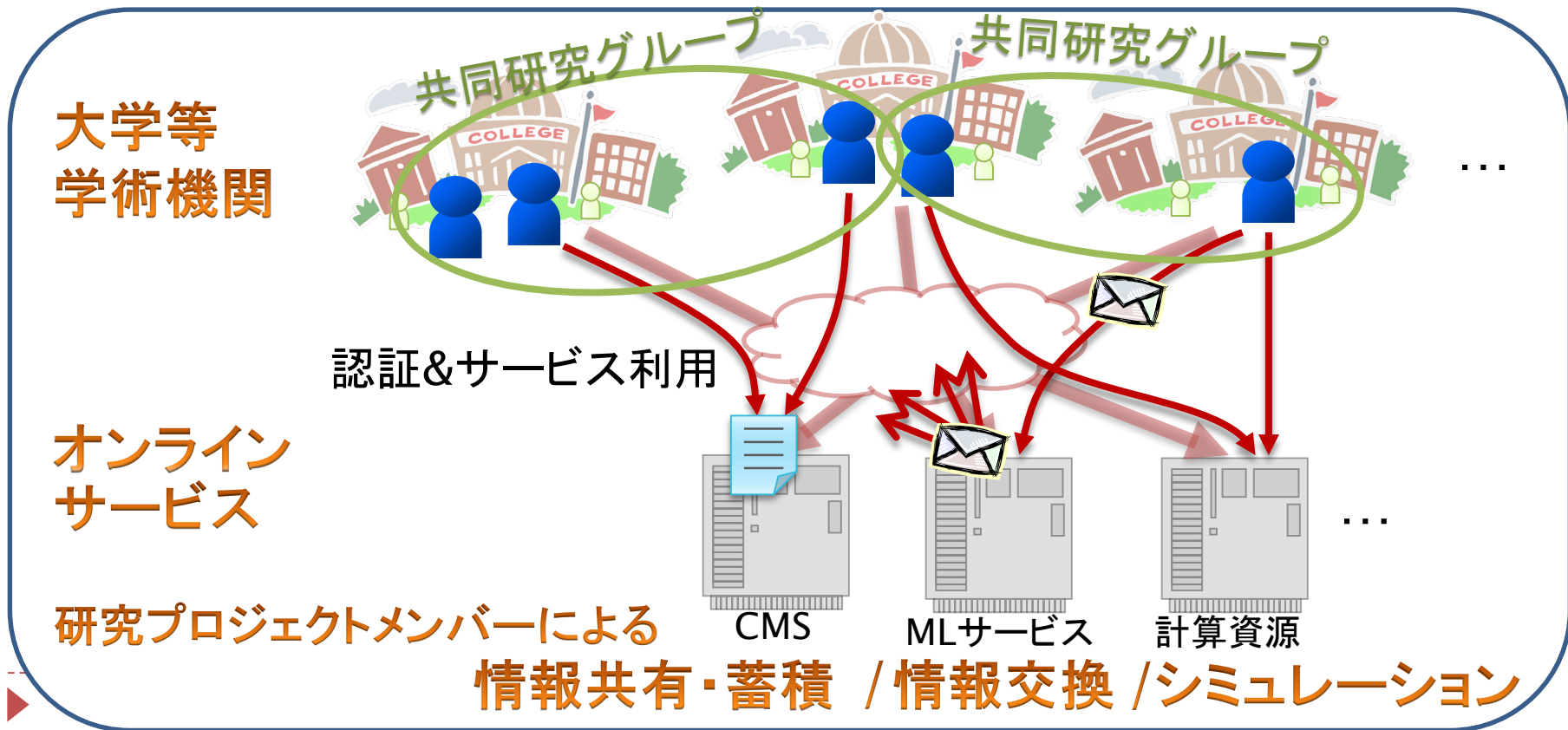
GakuNin



※展示スペースにて、この図を含むポスターを掲示しています！

# mAP Coreの目指すところ: 研究教育活動を支援するサイバースペースの提供

- ▶ 研究活動/教育活動におけるコラボレーション - 例えば
  - ▶ 研究プロジェクトの推進(情報共有、情報交換、スケジューリング、計算資源利用)
  - ▶ 講義の実施(履修登録、資料提供、e-Learning)

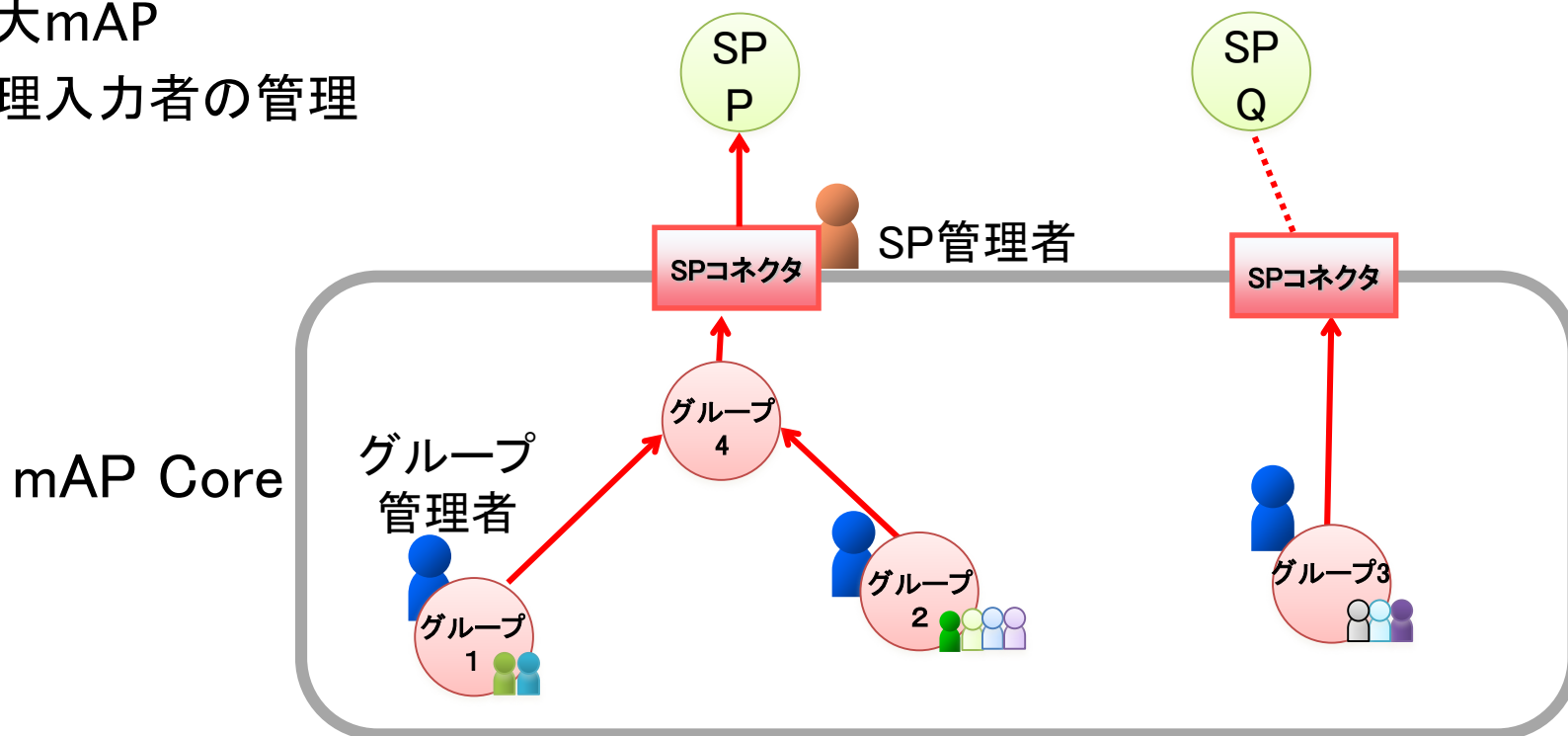







## mAP Coreの特長

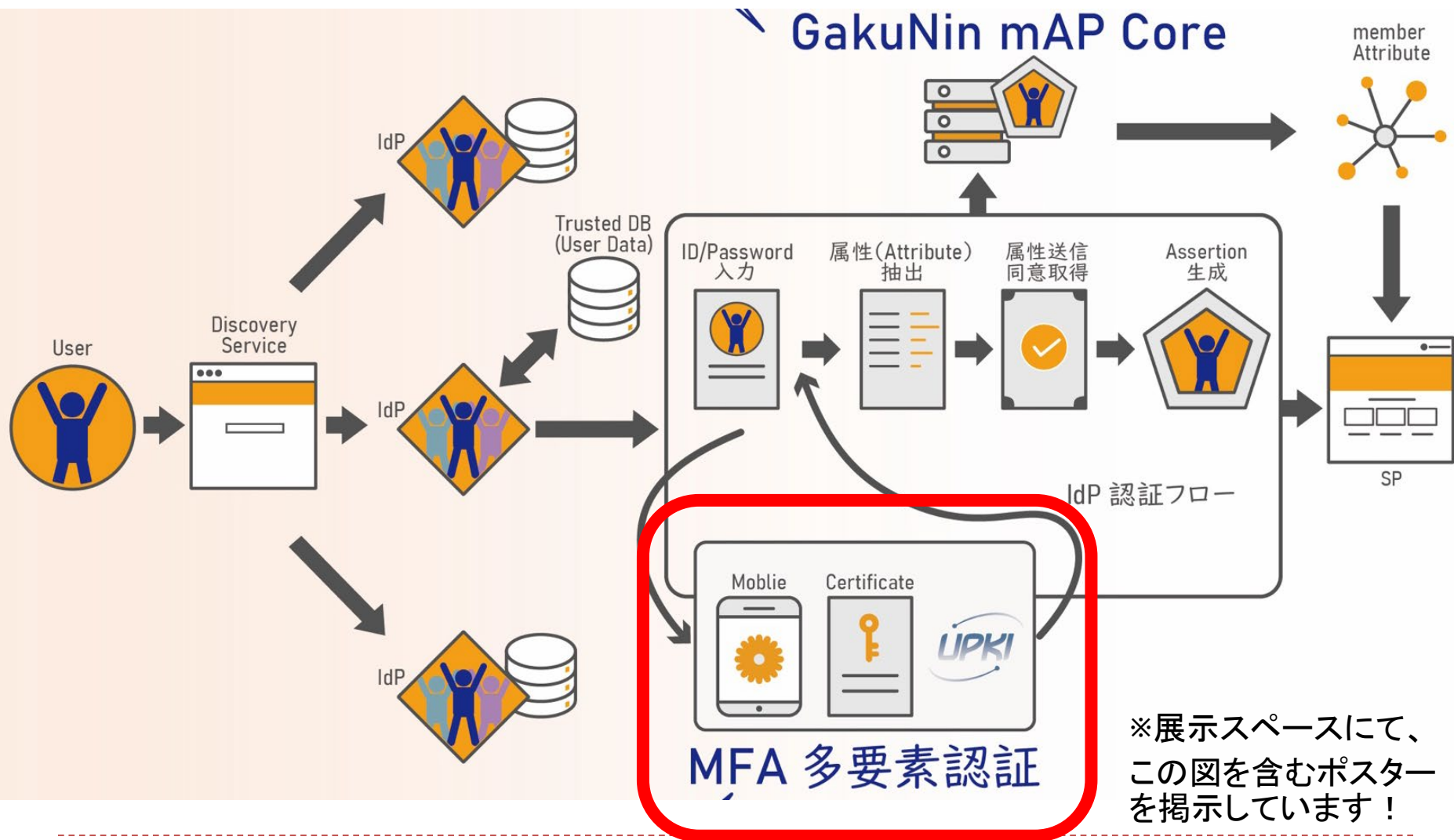
- ▶ 同意ベースの属性送信
- ▶ 2階層のグループ
- ▶ 誰でもグループを作れる
  
- ▶ 京大mAP
- ▶ 代理入力者の管理



# mAP Core APIの提供

- ▶ 従来(学認クラウドゲートウェイサービスのグループ機能)提供するグループ管理機能はWeb UIで操作する形態
    - ▶ メンバーの一括追加・削除が面倒
    - ▶ 情報源がSP側や機関側にある場合にその反映が手間
- 
- ▶ グループ管理機能をREST APIとして提供します
    - ▶ SPが利用者の権限でAPI呼び出しを行う想定
  - ▶ クローズドベータ版として一部のSPに提供中
    - ▶ ドキュメント整備でき次第公開予定

# 認証高度化②: 多要素認証(MFA)の推進



※展示スペースにて、この図を含むポスターを掲示しています！





## MFA: 多要素認証導入の推進

---

- ▶ 学認は、ID・Passwordのみより強固な認証として、多要素認証の普及を勧奨しています
  - ▶ もちろん、いくつかの学認参加機関ではすでに様々な形態で導入され、ユーザ情報の保護が実現しています
- ▶ 今後、多要素認証を必須とするSPの増加が予想されます
  - ▶ IdPは、「このユーザは多要素で認証された者である」と保証する必要に迫られるでしょう



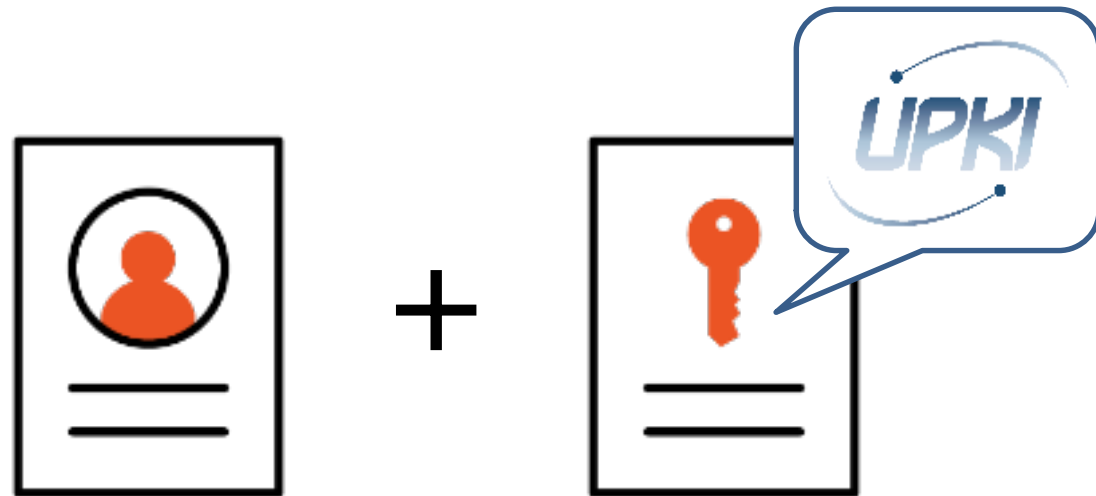
## 学認多要素認証プロフィールの制定

- ▶ 学認ではこの認識に立ち、  
統一的な基準を定めようとしています
- ▶ 学認多要素認証プロフィール
  - ▶ Assertionに含める値を定義するプロフィール
    - この者は多要素で認証されたユーザであると明示し、保証します
  - ▶ REFEDSのプロフィールをもとに作成
    - 学認のプロフィールとイコールではありませんが、条件を満たそうとしたときに、余分な処理が必要ないように考慮しています
    - 将来的には、eduGAINでの利用を考慮しています



## 2要素目に何を用いるか？

- ▶ 導入コストを抑えられるよう、UPKIのクライアント証明書を用いた形態を考えています
- ▶ ID・Password + UPKIクライアント証明書





- ▶ **学認MFAクライアント証明書運用基準**
  - ▶ IdPとして参加する機関が、クライアント証明書を多要素認証の1要素として用いるための基準です
  - ▶ 「学認多要素認証プロファイル」に定めるSAMLアサーションをIdPから送出する場合、本稿の基準を満たす必要があります
    - ▶ 学認参加IdP運用状況調査でも、監査を意図した質問が追加される可能性があります



## ガイドラインの制定

- ▶ 学認MFAクライアント証明書運用ガイド
  - ▶ IdPでの認証においてクライアント証明書を多要素認証の1要素として用いる場合のガイドラインです
  - ▶ 本ガイドラインは、「学認MFAクライアント証明書運用基準」に基づいてクライアント証明書を多要素認証の1要素として運用できるように設計しています
  - ▶ したがって、本ガイドラインにそってクライアント証明書を運用すると、「学認多要素認証プロフィール」に定めるSAMLアサーションをIdPから送出手続きの資格を満たすことができます
- ▶ 実際にMFAを導入しようと思ったとき、下記を1から整備するのはとても大変ですが、これらを高速・容易に構築できるよう企図しています
  - ▶ IdPを構成
  - ▶ 証明書発行体制の整備
  - ▶ 機関内証明書利用ルールの整備



## プロフィール、運用基準、運用ガイドの関係

- ▶ 2要素目として用いる要素ごとに、運用基準と運用ガイドを策定する必要があります
- ▶ 学認多要素認証プロフィール
  - ▶ 2要素目としてクライアント証明書を利用
    - ▶ 学認MFAクライアント証明書運用基準
    - ▶ 学認MFAクライアント証明書運用ガイド
- ▶ いずれ2要素目としてクライアント証明書以外を用いた運用基準と運用ガイドを策定する必要があると認識しています



- ▶ 以下のプラグイン開発・設定手順書の提供
  - ▶ 証明書認証
  - ▶ TigrShib
  - ▶ TOTP
  - ▶ Shibboleth MFA
    - ▶ 各種認証を要素(ログインフロー)として取り扱う
    - ▶ 組み合わせ自由自在



## まとめ - 学認が目指す認証高度化

---

- ① mAP Coreによるコラボレーション
- ② MFAの推進





# SIRTFI: Security Incident Response Trust Framework for Federated Identity

認証連携基盤におけるセキュリティインシデント対応のための責任ある運用管理体制の要請

- ▶ すでに、
  - ▶ Trusted DBなどに基づくID管理
  - ▶ セキュリティインシデント対応のためのCSIRT体制などが構築・実施されていれば、メタデータを登録すればよい
  
- ▶ 要件
  - ▶ 基本的なセキュリティ対策(パッチの適用など)
  - ▶ トレースのためのログ管理
  - ▶ 窓口情報の提供、迅速な応答、個人情報の適正な管理
  - ▶ 責任ある措置(アカウントの停止・失効、利用者への連絡など)
  
- ▶ メタデータへの登録
  - ▶ セキュリティコンタクト情報
  - ▶ Sirtfi Entity Attribute (Sirtfi Complianceでることの宣言)



## R&S (REFEDS Research and Scholarship)

---

- ▶ wikis, blogs, project and grant management toolsなどR&Sサービスの効果的な利用のための枠組み
- ▶ R&Sとして承認審査を受けたSPに対して、IdPは以下の属性情報をまとめて提供
  - ▶ Personal identifiers: email address, person name, eduPersonPrincipalName
  - ▶ Pseudonymous identifier: eduPersonTargetedID
  - ▶ Affiliation: eduPersonScopedAffiliation (オプション)
- ▶ IdPにおいて個別に追加登録しなくても、すぐに利用できるようにすることで、eduGAINの活用を促進