AXIES2023

次世代認証連携における認証器レジストリの取り組み

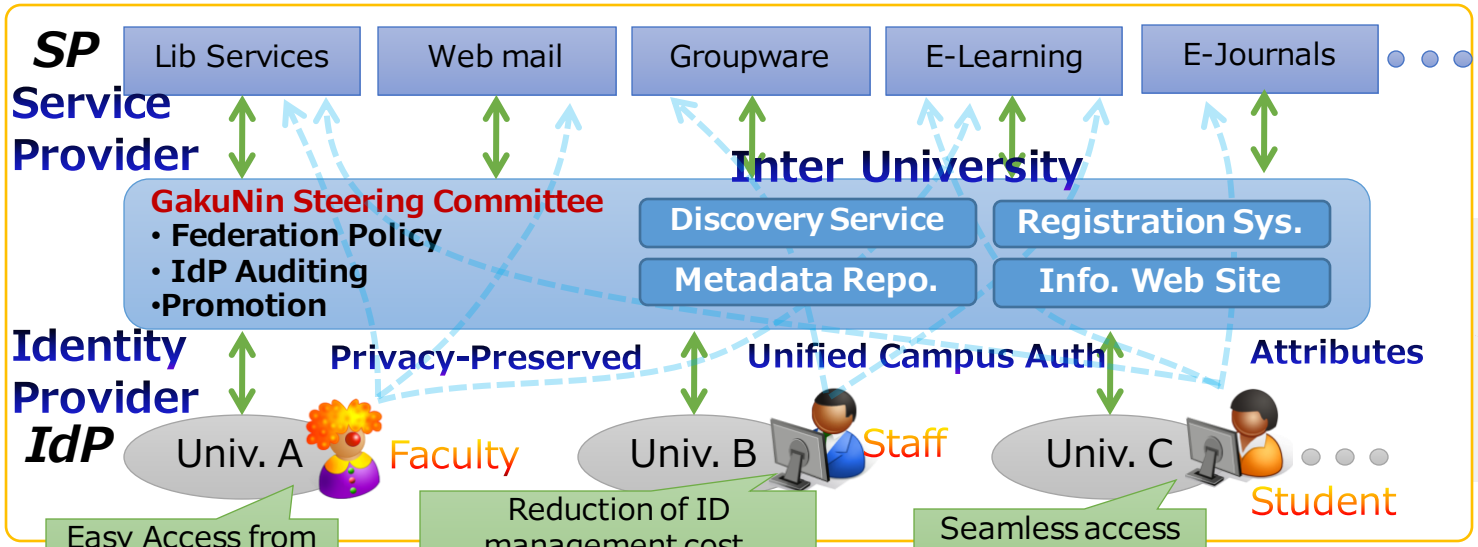
学術認証推進室 水元明法

自己紹介

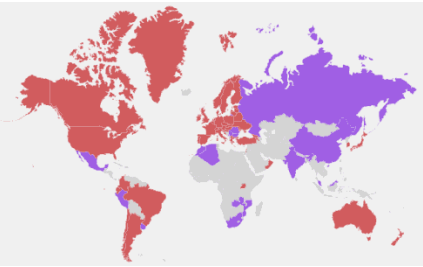
- 名前
  - 水元 明法(MIZUMOTO, Akinori)
- 所属
  - 国立情報学研究所(NII) 学術基盤研究員
- 出身地
  - 石川県
- 経歴
  - NII 学術支援技術専門員
  - 物質・材料研究機構(NIMS) NIMSエンジニア を経て現職
- 現在の活動
  - 学認
  - 次世代認証連携（認証器レジストリ）

学術認証フェデレーション

- 学認は、サイバー空間における円滑な学術活動を支援すべくトラストフレームワーク（ポリシ、技術、評価）を提供
  - 全学的なサービスに対してうまく機能

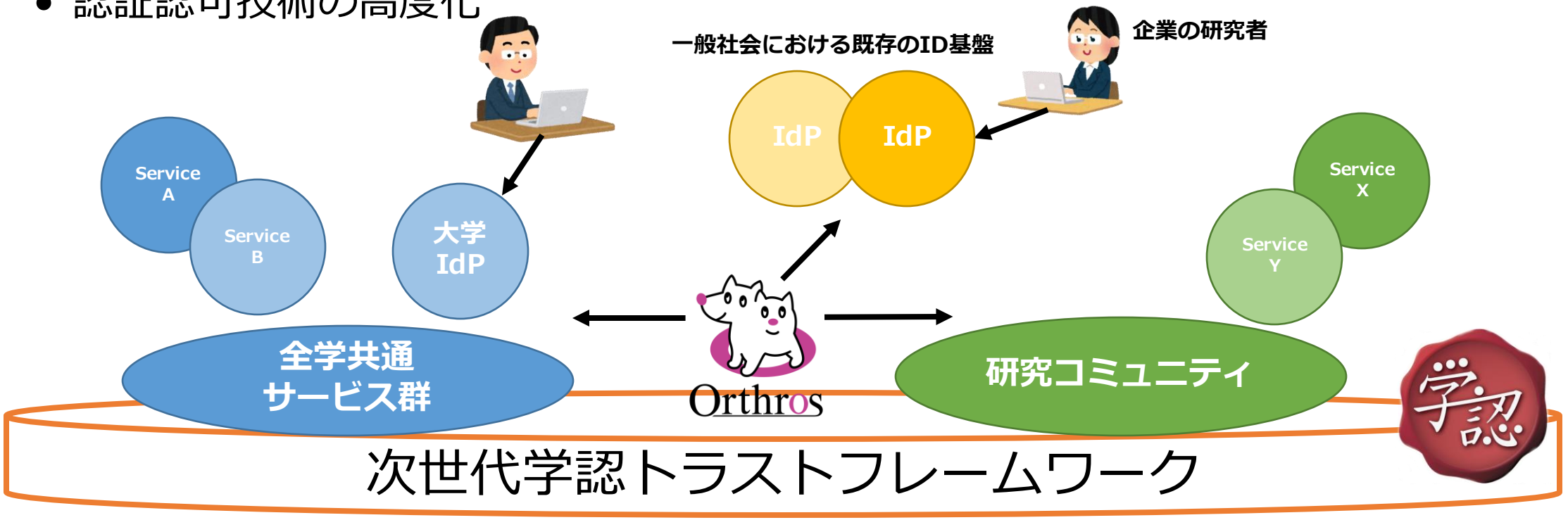


Academic Federations have been established per country basis



次世代認証基盤研究開発の必要性

- 学術の研究・教育DX推進には、研究・教育データ流通の加速が必須
- データ流通の加速には、多種多様なサービスの円滑な利活用が鍵
  - 異種サービス間、異種コミュニティ間でのデータ共有
- **研究・教育DXを推進する新しいトラストフレームワークの確立**
  - 認証ポリシの相互運用性（IAL, AAL, FAL）
  - 認証認可技術の高度化



新しいトラストフレームワーク

参加IdP数の更なる拡大

認可機能の高度化
・グループ機能

IdPs

IdP-SP 仲介
・IAL/AAL マッチング
・既存ID基盤連携

SPs

認証器の利活用

本人確認の保証度、認証強度の明確化
・どの程度の本人確認が実施されているのか
・どの程度の認証強度なのか

次世代認証連携における主要構成要素

学認IAL/AAL

- 本人確認の保証度、認証強度について規定

IdPとSPが参照することにより統一的かつ効率的な議論が可能となり、また、各機関が遵守することにより学認全体のトラストを担保できる

認証器レジストリ

- 学認AALに基づく認証器の評価

認証器を評価、結果を公開し、大学・研究機関のIdPの多要素認証対応を促進する

認証プロキシサービス "Orthros"

- IAL/AAL matching, Credential bridging, Attribute coordination

SPからの要求を仲介しIdPと連動することで、IAL, AALの担保が可能となる

IdPホスティングサービス

- 大学、研究機関のIdP構築運用の課題を議論

大学・研究機関のIdP構築運用の負荷を軽減、様々な運用形態のなかから機関に適したものを選択し、すべての機関がIdPを運用できるようになる

グループ管理機能の高度化

- より高度な認可要求に対応

所属などの基本属性に加えて一般的なIdPが扱わない属性に基づいたグループ管理を実現し、SPの認可管理が効率化できる

認証器レジストリとは？

- 学認が提供する、学認AAL2対応認証器と関連する情報が登録されたレジストリ
  - 学認は「認証器」の性能を調査し、当該認証器がAAL2の認証に利用できるか？がわかるレジストリを用意する
  - 学認参加機関の求めに応じて認証器の審査・認定を行った場合、その結果を登録して定期的に更新する

認証器レジストリの目的

- 学認AAL2の認定と運用のためには、多数ある認証器の評価が必要
- 市場に流通する認証器ごとに、学認参加機関が各自でAAL2準拠を評価することは、合理的ではない
  - この認証器はどのタイプに該当するのか？
  - この認証器は学認AAL2基準のチェック項目を満たすか？
  - この認証器は単体で単要素か？多要素か？
  - 運用上の問題点は？
  - セキュリティリスクにはどんなものがあるか？
- 認証器の性能を調査し、AAL2基準を満たす認証に利用可能かを判定し、結果を公開する認証器レジストリが重要な役割をもつ

利便性・セキュリティ水準の向上、運用の効率化

- 種類や仕組みなど、認証器に関する情報を提供
  - 自らに適した認証器を選択しやすくなる
  - 認証器のセキュリティリスクを理解し、適切な対策を講じることができる
  - 管理者は認証器の運用方法を適切に検討しやすくなる
- 設定方法や使い方など、認証器の利用方法に関する情報を提供
  - 認証器をスムーズに導入して利用できるようになる
  - 利用者は認証器を適切に利用し、セキュリティを向上させることができる
  - 管理者は認証器の運用を効率化できる

AAL2として認められる認証器

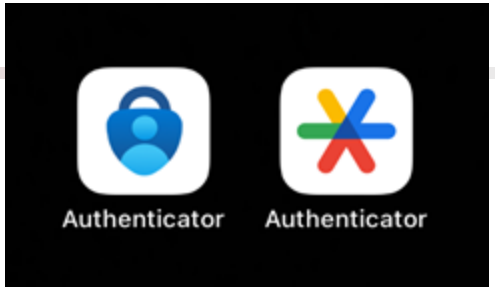
- NIST SP800−63
  - AAL2の認証では,
    - 一つの多要素認証器 または
    - 2つの単一要素認証器の組み合わせ（同時）
      のどちらかを利用するものとする(SHALL)
  - →AAL2では「二要素認証」が必須（AAL1では何をつかってもよい）
- Kantara KIAF1440
  - 「多要素認証器１個またはパスワード認証に所持要素に基づく認証器を組み合わせたもの」
    をAAL2に対応する認証器の要件としている。
- 学認AAL2では、KIAF1440と同様の要件を求めることとする

認証器の種類

- Single-Factor OTP Device（単要素OTPデバイス）
- Multi-Factor OTP Device（多要素OTPデバイス）
- Single-Factor Cryptographic Software（単要素暗号ソフトウェア）
- Multi-Factor Cryptographic Device（多要素暗号ソフトウェア）
- Single-Factor Cryptographic Device（単要素暗号デバイス）
- Multi-Factor Cryptographic Device（多要素暗号デバイス）
- Look-Up Secret（参照シークレット）
- Out-of-Band Device（経路外デバイス）
- Memorized Secret（記憶シークレット）

評価対象の認証器

- 現在（2023年度）評価実施中の認証器
  - OTPデバイス
    - Microsoft Authenticator
    - Google Authenticator
  - 暗号デバイス
    - FIDO認定を取得した認証器
      - 学認（NII）はLiaison Partners としてFIDO Alliance と協同
  - 暗号ソフトウェア
    - UPKI電子証明書発行サービスのクライアント証明書



認証器の運用

- 学認AAL2基準を満たすために、認証器それ自体の選定に加え、運用面での評価も必要。
  - 適切に運用できるIdPは何か？
    - Shibboleth IdP
  - 適切に運用できるIDaaS・ID管理製品はあるか？
    - 学認参加実績有りのIDaaS・ID管理製品
- 学認AAL2は、認証器が要件を満たし、またその認証器を用いた認証システムの実装と運用が適切に行われてはじめて基準を充足する

まとめ

- 学術認証フェデレーション「学認」の現在について
  - 円滑な学術活動を支援すべくトラストフレームワーク（ポリシ、技術、評価）を提供
- 次世代の学認について
  - より信頼性の高い本人確認の保証度、認証強度を規定し、その実現に向けた活動を実施中
- 認証器レジストリについて
  - 利用者の利便性の向上、セキュリティの向上、運用の効率化など、さまざまなメリットをもたらす

きいてみたいこと

- 認証器を無くした！→どうやってリカバリする？
- 認証器に求める性能
  - コスト面やフィッシング耐性など
- 多要素認証の運用に際して、大学側として知りたいこと
- 導入を検討している認証器

次世代認証連携実現に向けて…

- 学認の取り組みを随時公開して参ります
  - NII Open Forum 2024

GakuNin