AXIES認証基盤部会・学認合同企画セッション

2023/5/30
10:00～11:30

部会主査 中村素典（京都大学）

認証強度の強化と ID管理の信頼性向上に向けて

- 概要紹介
- 東京大学における認証基盤の取り組み
- FIDO2対応Yubikeyがグローバルで選ばれる理由とパスキーの展開
- 認証基盤サーバ・サービス等の紹介
  - HCNET
  - Exgen
  - サイオステクノロジー
  - Netspring

Day2 認証トラック3 (14:30～)

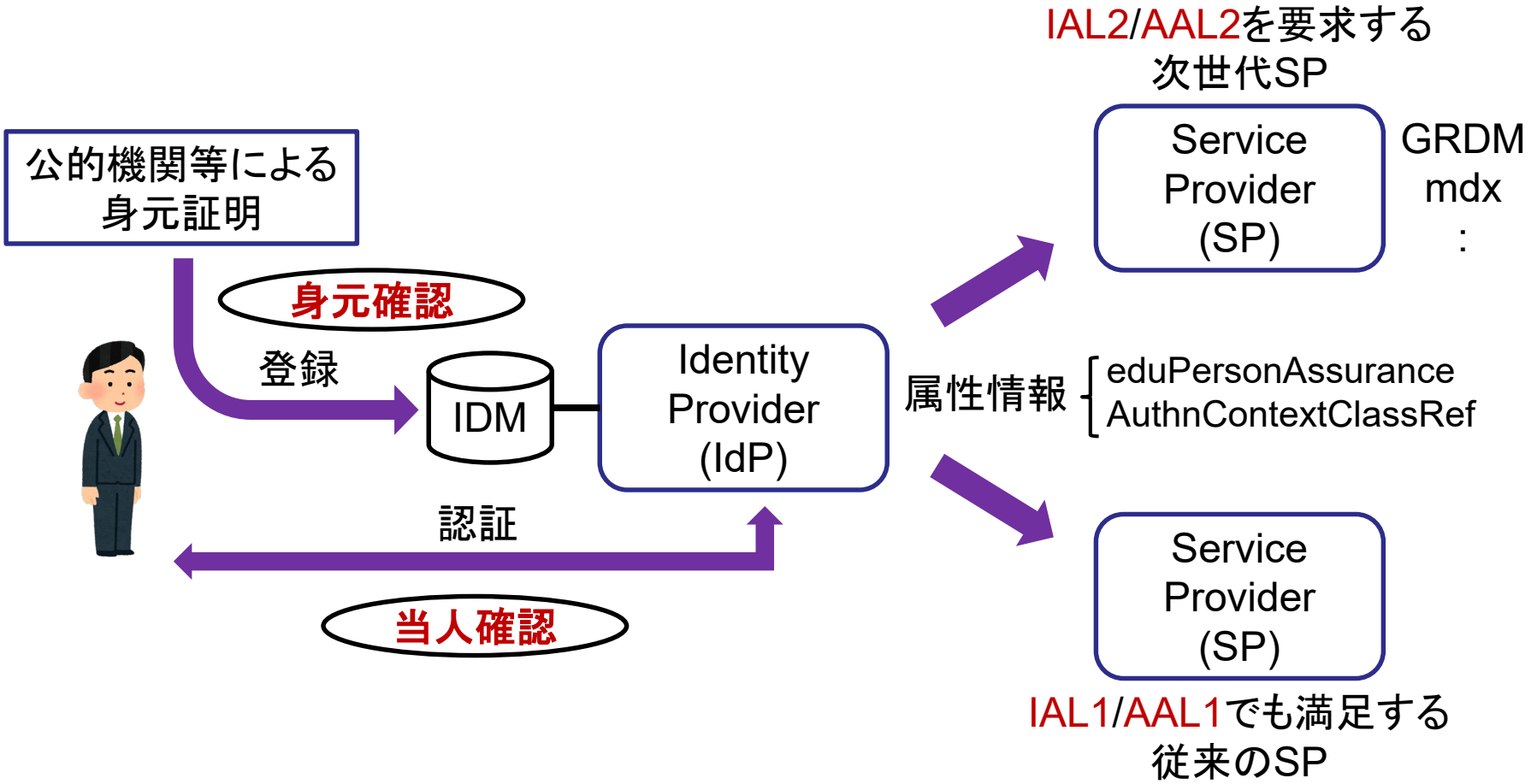
「次世代認証連携を実現する技術開発の今とサービス事業展開に向けて」

- 学認が目指す次世代認証連携
- 認証器レジストリについて
- 認証プロキシサービスOrthrosについて
- 学認対応 IdP ホスティングサービスについて
- （仮）グループ管理機能高度化について

次世代の認証連携基盤とは

- 背景
  - 機微な情報を扱う機会の増加
  - 不正アクセスの増加、攻撃の高度化
  - クラウド化の進展に伴うサービス間連携の多様化
  - 共同研究など機関をまたいだ活動の支援
- 対策（要請）
  - より厳密な身元（属性）の保証
  - より厳密な当人性（認証強度）の保証

認証連携における
(1)身元確認と(2)当人確認



(1)身元確認

- Enrollment and Identity Proofing
  - IAL: Identity Assurance Level
  - 参考: NIST SP 800-63A (-4)

- いわゆるKYCやeKYCにあたる手続き
  - (electronic) Know Your Customer

- 大学で発行するアカウント
  - 人事部や教務部由来のもの
    - 便宜上Trusted DBとみなしているが、本当にTrustedか？
  - それ以外（個別申請など）

大学におけるアカウント発行時の身元確認はどうなっているか？

- 様々な種別の構成員（一例）
  - センター試験（共通テスト）を経て入学する学生
  - 編入生、聴講生、研究生、…
  - 常勤教職員、非常勤教職員
    - 給与の支払いがあればマイナンバーでたどれる？
  - （直接）雇用されていない者
    - 共同研究員、名誉教授などの称号付与
    - 派遣職員、業務委託、…

「人事部・学務部まかせ」ではすまなくなってきている

理想のIAL管理に向けて

- IAL (SP800-63A-3での定義、ざっくりと)
  1：検証なし (63A-4では0)
  2：検証あり (63A-4では1)
    - 機微な情報へのアクセスにはIAL2以上が要求される
- 個人ごとのIAL管理
  - 大学全体としてIAL2を保証することは困難
  - 確認できたアカウントを1から2に昇格させる？
    - 初期登録時のIAL2の確認を省略した場合
- アカウントには多数の属性情報が紐づいている
  - 場合によっては、属性情報の項目ごとに信頼度の管理が必要となる（自己申告のもの、確認済みのもの）

(2)当人確認

- Authentication and Lifecycle Management
  - AAL: Authentication Assurance Level
  - 参考: NIST SP 800-63B (-4)

- 多要素認証
  - “Something you know” （知識）
  - “Something you have”（所有）
  - “Something you are”（生体、行動を含む）

  これらのうち複数の組み合わせによる認証強化

理想のAAL管理に向けて

- AAL（ざっくりとした分類）
  1：何らかの認証（技術基準を満たしていること）
  2：多要素認証
  3：ハードウェア認証器利用（大学では不要？）
- 大学に求められること
  - 広く利用可能な認証方式（認証器）の選定
  - アカウント発行（登録、配付）手続きの整理
    - 受け入れに責任を持つ者がアカウントも責任を持つ？

大学におけるアカウント発行時の受け渡し等はどうなっているか？

- 最終的に多要素認証が実現されていても、途中に脆弱な瞬間があるならば、そのアカウントは本当に信頼に値するのか？
  - 入学時（合格時）等のアカウント情報の通知方法
  - 初期パスワードからの変更方法
  - 多要素認証の設定方法
  - パスワード忘れ時等の再設定方法
- 従来のパスワードのみ認証からの移行では問題なかったかもしれないが
  - 将来は最初から高いAALが求められるようになる？

脆弱と思われる事例

- アカウント有効化が単一認証
- 多要素認証の設定が完了するまでに単要素で（設定画面に）アクセスできる瞬間がある
- 多要素認証の再設定が単要素で可能
- メールの到達性確認が、送信したリンク（URL）をクリックするのみ
- パスワードリセット等の際に送るメールの宛先アドレスが任意に指定可能（メールアドレスの指定が単要素認証の状態で可能）

本セッションを通じて

次世代認証連携を支える認証基盤のありかたを考える

- 各大学が個別に高度なID管理・認証基盤を構築・維持するのは高コスト
  - 統一規格に基づく認証基盤（オンプレ、クラウド、IDaaSなど）の普及・活用が必要
- 大学特有のKYC（≠eKYC）のサポート
  - 継続的に対面する関係による信頼の構築？

（オンラインで確認できるアカウントの信頼性ではなく、その向こうに居る実際の人に対する信頼性）