京都大学における認証基盤の次世代化に向けた取り組み

中村 素典 / 情報環境機構 IT基盤センター

AIXES認証基盤部会セミナー

2026/3/25

京都大学で扱う「ユーザ」

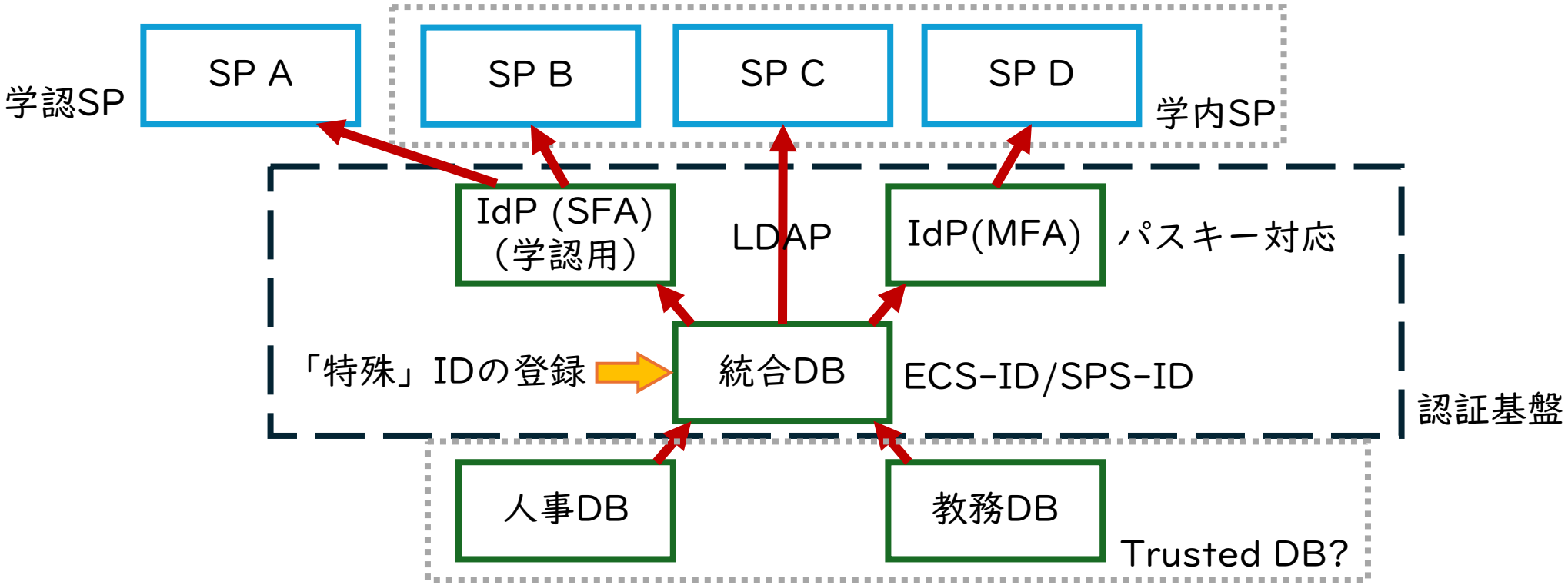
- 常勤教職員　　約7,500名
- 非常勤教職員　　約4,400名
  - うち附属病院所属　　約3,500名

- 学部学生　　約13,000名
- 大学院生　　約9,600名
- 研究生、聴講生等　　約50名
- 学振研究員等　　約750名

「ユーザ」に付与するID

- SPS-ID：教職員グループウェア由来
  - 教職員等向けサービス用（源泉：人事DB）
    - グループウェア、財務会計、人事給与、就業管理など
- ECS-ID：教育用計算機由来
  - 学生等向けサービス用（源泉：教務DB＋「特殊」）
    - 教務情報、LMS
  - 共通サービス
    - ネットワーク利用、安否確認、電子ジャーナル
    - Google Workspace（SPS-ID/ECS-IDで別テナント）
    - Microsoft 365（SPS-ID/ECS-IDで別ドメイン）
    - Zoom（GWS経由認証:SPS-ID＋TAのECS-ID）
    - GakuNin: 学認RDM、学認LMS、…
- その他
  - スパコン、附属病院、生涯メール、…

現在の認証基盤の構成概略



MFAの導入

- 教職員向けシステムへの導入（2020）
  - Google Workspace、財務会計、出張旅費、就業管理、Zoom (Google経由認証)
  - PW+(TOTP / メールOTP / パスキー）
    - TOTPはGoogle Authenticator（スマホアプリ、ブラウザプラグイン）
    - とにかくTOTPを設定してもらう。メールOTPはオプション。
- 学生向けシステムへの導入（2024）
  - Microsoft 365、LMS、教務システム、電子ジャーナル
  - PW+(メールOTP / TOTP / パスキー）
    - とにかくメールOTPを設定してもらう（リカバリーにも使用）。
そのうえでTOTP。

パスキー/FIDOの導入

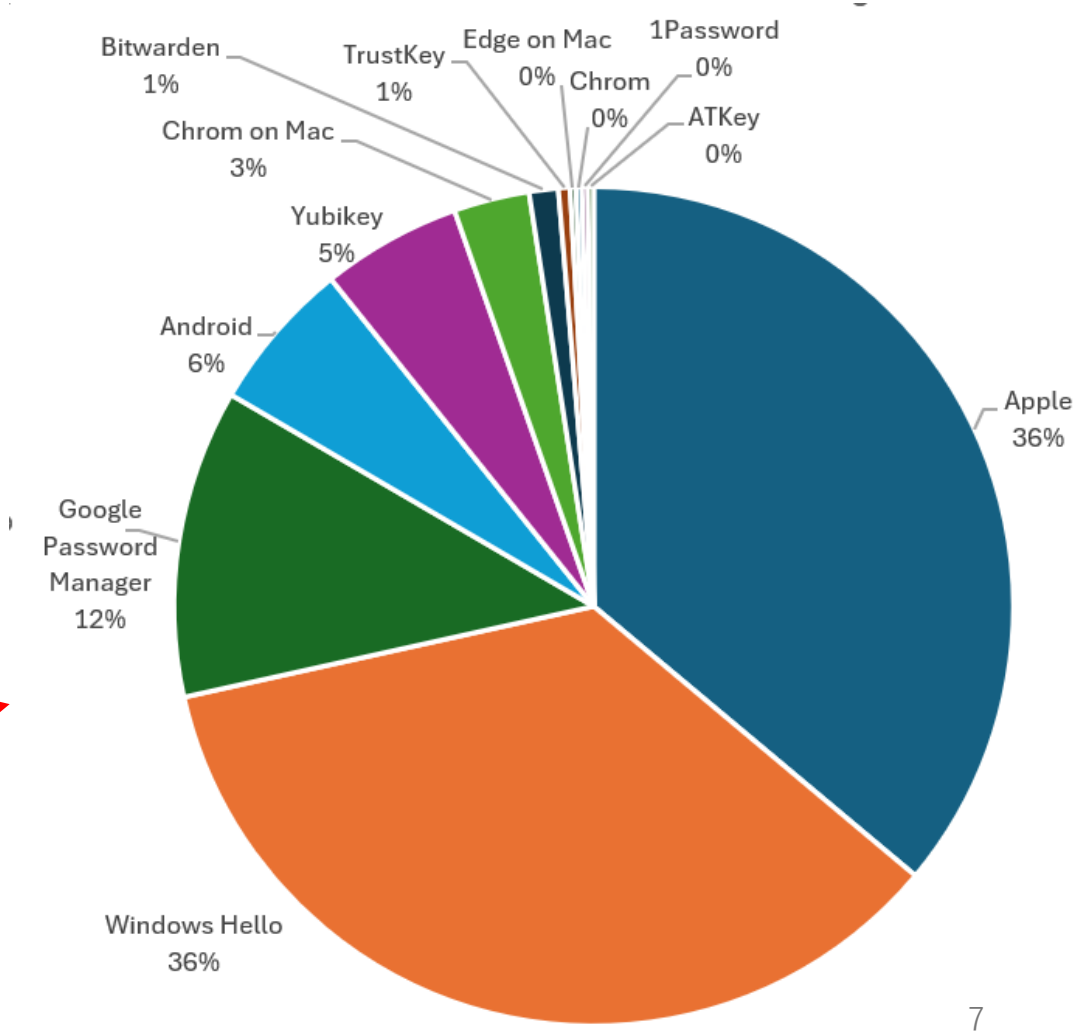
- 教職員向けMFA導入時点（2020）からFIDOに対応
  - SAME (Secioss Access Manager Enterprise)による機能

- 学生向けMFA導入時点（2024）に本格対応
  - Windows Helloにおける不具合の解消
  - Appleの同期パスキーが利用可能
  - Googleの同期パスキーも気が付けば利用可能に（2025秋頃）
    - Google側の仕様変更？

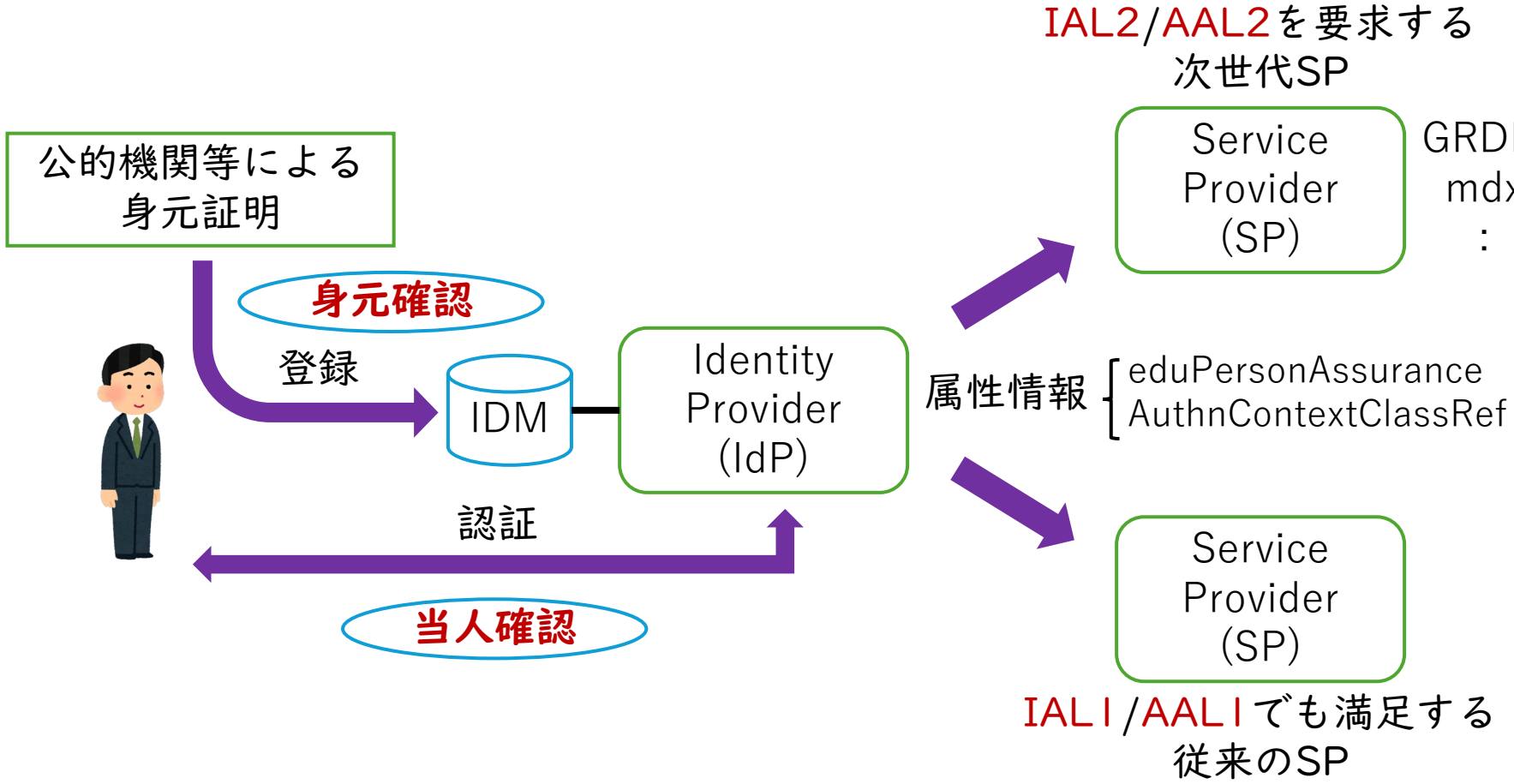
- フィッシング耐性のある認証手段として広く普及へ（2025）
  - 警察庁、金融庁などによる積極的が普及活動

本学でのパスキーの利用状況

- まだ積極的に案内していない段階
- 2025年12月時点の利用状況
  - 登録者数：297
    - 認証器登録数
      - 1台 - 242人
      - 2台 - 51人
      - 3台 - 13人
      - 4台 - 3人
      - 5台 - 6人
      - 9台 - 1人
      - 12台 - 1人
  - 登録認証器数：446
    - AAGUID調べ
      - Authenticator Attestation Global Unique IDentifier



認証連携における
身元確認(IAL)と当人確認(AAL)



BAL (Binding Assurance Level)

- AAL2って多要素認証を採用してさえいればOKなのか？
  - AAL1（パスワードのみ）→AAL2（多要素認証）ってどうしてます？
  - AAL1の瞬間があれば、そこでなりすまされて多要素認証の登録がなされてしまうかも？
- AAL1である瞬間を作らない工夫
  - 身元確認（IAL2）のフローの中でAAL2の設定まで完了させる
    - あるいは、先にAAL2を設定した状態から身元確認
    - アカウント発行時から多要素を意識する
  - 認証関係の設定変更（MFA設定の追加・削除等）にはAAL2を要求
    - まさかのとき（リカバリー）のために、MFAは複数登録すべき
      - リカバリー手続きの中で単要素を許容すべきではない

参考: https://nat.sakimura.org/2025/12/10/on-nist-sp800-63-4-and-the-binding-level-of-assurance-and-account-hijack-possibilities/

学部新入生アカウント発行フロー

1. 合格通知とともにアカウント取得方法を郵送
2. ECS-ID案内サイトに受験番号、インターネット出願番号、生年月日を入力し、合致したらログインID（ECS-ID、学生番号とは異なる）を表示
3. さらに「送信」ボタンを押すことで、インターネット出願時に登録したメールアドレス（非表示）に有効化キーを送付
4. アカウント有効化サイトにログインIDと有効化キーを入力し、パスワードを設定
5. 続けて多要素認証の設定に進む（多要素認証の設定をやりなおす場合は、有効化キーが必要）

パスワードのみでログインできる状況を作らない

AAL2/IAL2対応(次世代学認)に向けて

- AAL2
  - IdPとしては多要素認証（AAL2）に対応済み（前述）
  - SPごとにAAL2対応に移行中
    - まだ未移行のものが残っている：学認など
  - AuthnContextClassRef対応を進めたい
    - SPからの要求に基づいてAAL1/AAL2認証を切り替える仕組み
    - パスキーの普及でAAL2が当たり前になる可能性もある
    - パスワードレス認証にも対応したいかも
- IAL2
  - 身分ごとに、アカウント申請時（人事DBへの登録時）にどのような身元確認を行っているかを整理
    - 身元確認が不十分な場合は、追加で確認するフローを検討（IAL2への昇格）
  - ユーザごとにeduPersonAssuranceLevelでIALを送出したい

身分証

- 身分証は、券面表示のみのものから、磁気ストライプを備えたものを経て、ICカードを備えたものに変遷してきた
- 学内における教職員および学生等のアイデンティティを示すものとして、アカウントとともに身分証は重要な役割を持つ
  - アカウント：オンラインサービスで利用するアイデンティティ
  - 身分証：オフラインサービスで利用するアイデンティティ

デジタル身分証

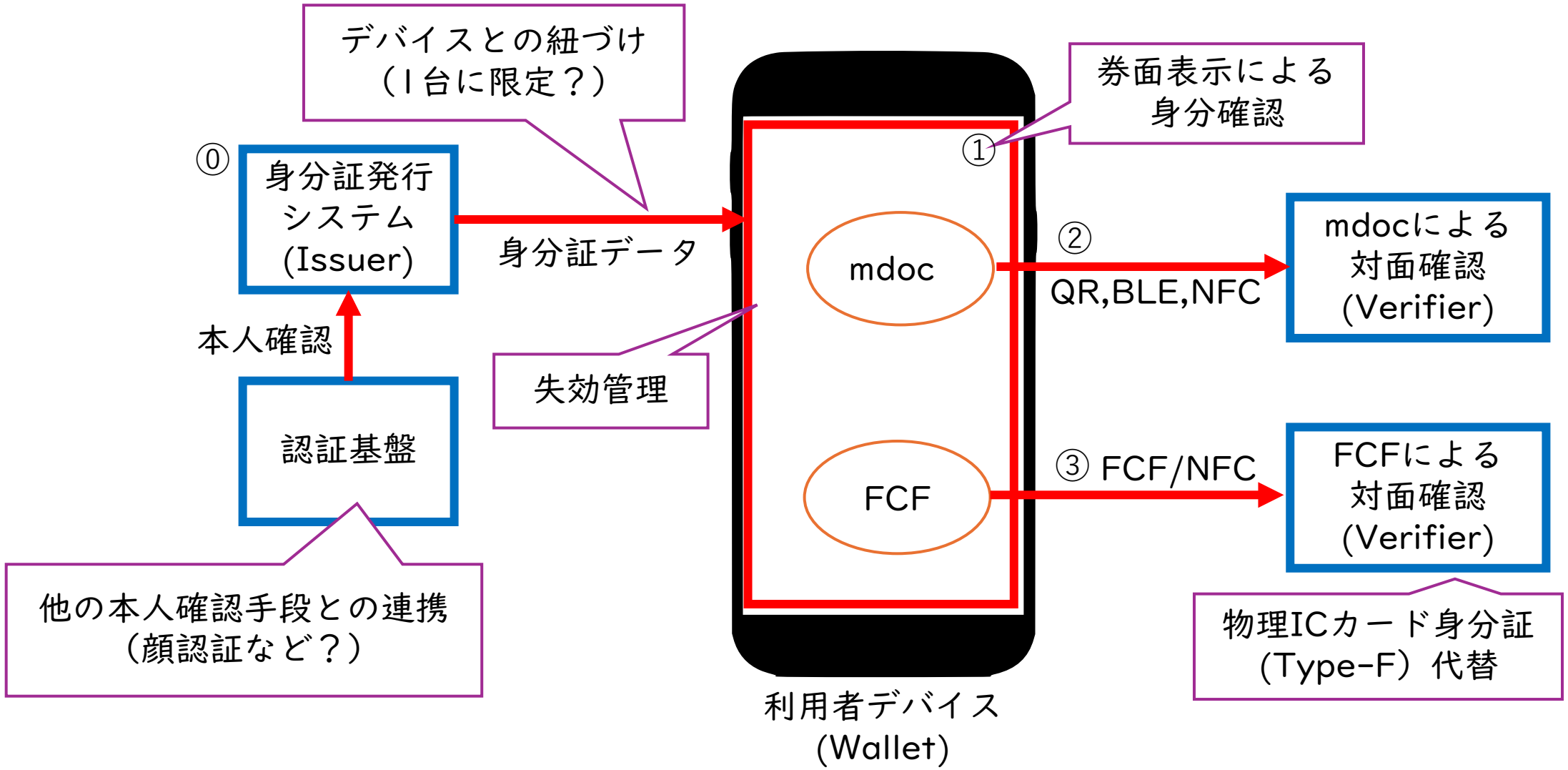
- オンラインサービスの高度化と並行して、物理媒体による身分証の高度化についても検討が必要
  - スマートフォン等の高度化したデジタル端末の普及
  - 発行・配付コストの削減、入退管理システム等の更新コスト削減

Kintoneによる発行試行

デジタル身分証発行のための整理

- 様々な要素技術の組み合わせによる実現
  - 汎用モジュール化の活用
  - スーパーアプリは利便性が高そうだが、（連携していれば）必ずしも一つのアプリで実現される必要はない
- 構成要素
  - スマホにインストール可能な身分証情報を発行する仕組み(Issuer)
  - 発行された身分証情報(VC)を保持するWalletアプリ
  - 券面表示（スクリーンショット等の不正対策）
  - 対面提示連携
    - QR、BLE、NFCなどによる提示
  - FCF準拠ICカード機能（既存の入退館・出席管理の活用）
- ユースケース検討
  - スマートフォンを所有しない者の考慮

デジタル身分証を構成する要素



デジタル身分証発行機能⓪

- 大学のID管理システムとの連携
  - 本人確認
  - 発行したデジタル身分証のスマホ（Wallet）へのインストール
  - 発行システムは複数大学共用にできるとコスト削減が図れる？
    - そのためには大学間の仕様の共通化が必要
    - VCへの署名（Issuer）は大学ごと？
- 失効処理
  - 発行されたデジタル身分証の有効期限はいつまでとするか
    - TLSサーバ証明書は短い有効期間と頻繁な更新
  - 退職・退学等を考慮した有効性確認の仕組みは必要か
- 不正利用防止対策
  - 複数のスマホへのインストールの防止（短期的な端末変更の防止）
  - FCF物理ICカード(Type-F)身分証との区別は必要か

共通仕様・共通発行システム

券面表示機能①

- 何を記載するか

- 券面表示の確認をするユースケースは何か
  - 学割等の際の学生であることの証明
  - 他大学等での施設利用
  - ほかには？

- スクリーンショット等の対策は必要か
  - 目視による真正性の確認？
    - アニメーション、時刻情報
  - 大学共通ルールが必要

VC対応機能②③

- デジタル身分証の情報を安全にスマートフォンに格納するための世界標準仕様として期待される
- 情報を選択的に提示することが可能
- 提示インタフェース
  - QR（BLE、NFCの補助）
  - BLE
  - NFC (Type-B?)
- mdocはフェリカネットワークスの事例がある
  - SDKの提供など

FCF Campus Card対応機能④

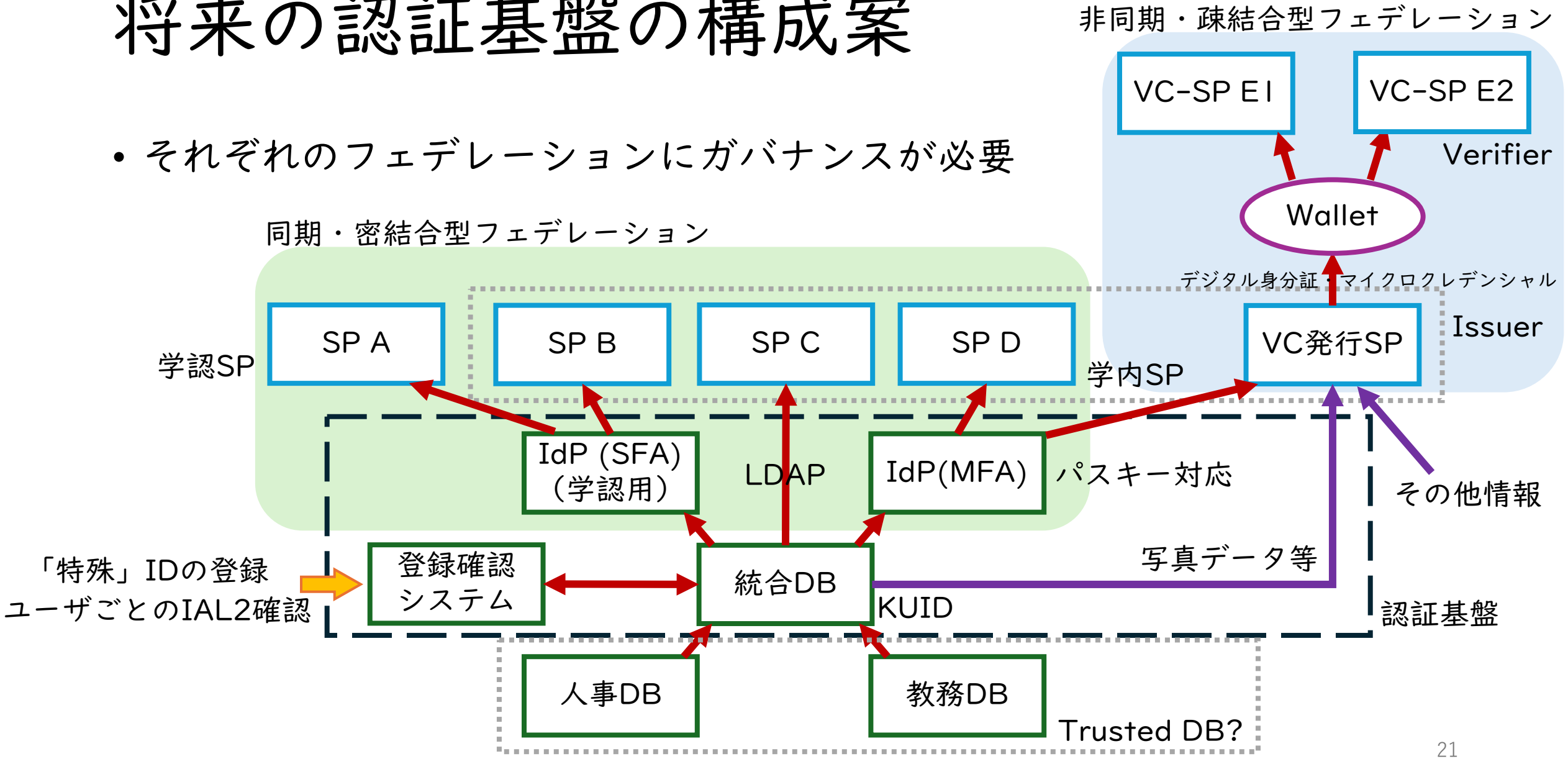
- FCF (フェリカ共通フォーマット) 準拠のIC身分証が多くの学術機関に普及している (Version 2, 3)
  - 出席確認や入退管理で利用されている
  - 過去の設備投資を無駄にしないためにも、FCFが当面継続的に利用できることが望ましい
- スマートフォンへの搭載については、FCF推進フォーラムにおいて検討が進められている
  - 物理カードとともにFCF Version 3への移行は必要か？
  - ICカード版とのコンパチビリティ？
  - 全てのスマートフォンが利用可能？
  - ライセンスコスト？

その他の検討事項

- VCの複数発行や複製を認めるのか？
- スマートフォンを所有しない者への対応
- 試験におけるスマートフォンの持ち込み禁止対応
  - 物理学生証を廃止した場合の対応
- 交通機関等における学割利用
  - 対面での券面確認
  - 事業者側の認証基盤との連携？
- 大学生協等との連携

将来の認証基盤の構成案

- それぞれのフェデレーションにガバナンスが必要



まとめ

- 京都大学における認証基盤の改善
- デジタル身分証の実現と応用の検討