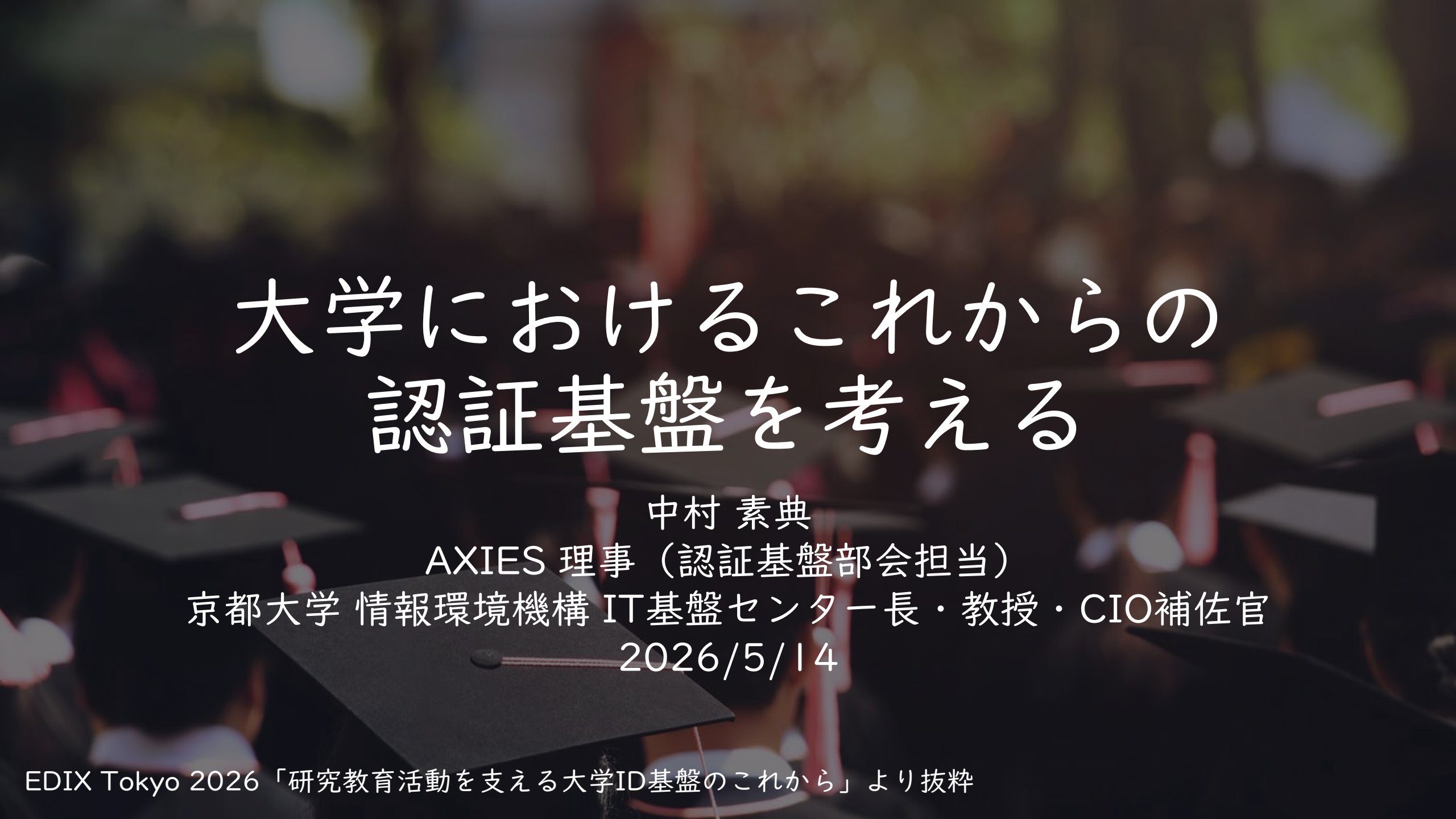


大学におけるこれからの認証基盤を考える

中村 素典
AXIES 理事（認証基盤部会担当）
京都大学 情報環境機構 IT基盤センター長・教授・CIO補佐官
2026/5/14

EDIX Tokyo 2026「研究教育活動を支える大学ID基盤のこれから」より抜粋

概要

大学の活動を支える認証基盤に関する2つのトピック

1. 認証（当人確認）技術の進化（パスキーへの流れ）
   - 大学における認証基盤の見直し

2. VC (Verifiable Credential)の時代へ
   - 大学はどのようにデジタル証明証をサポートすべきか

大学における認証の役割

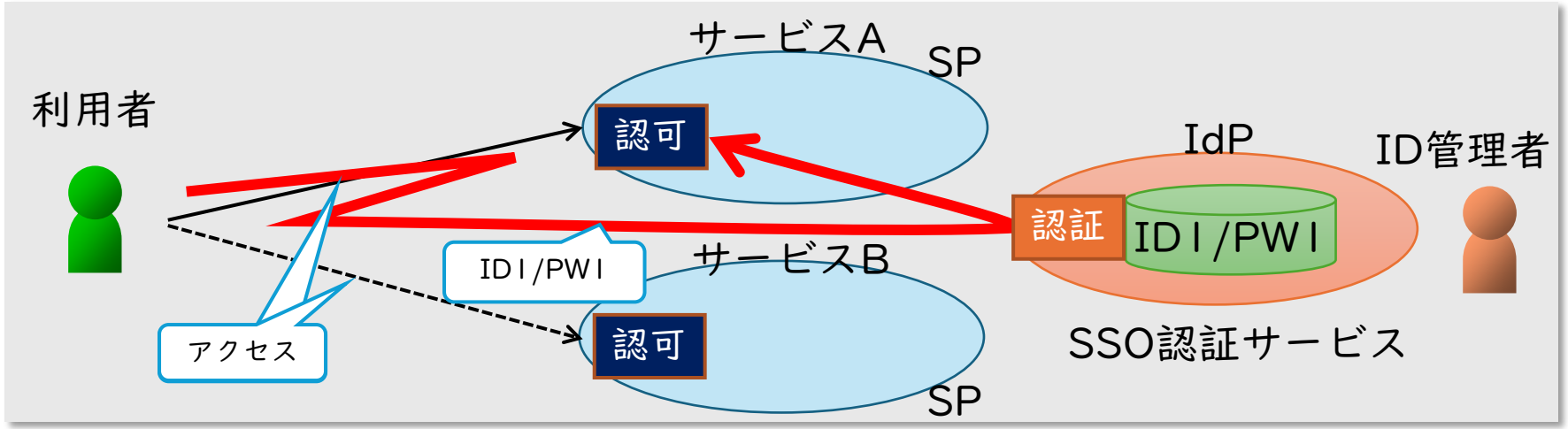
1. アカウントの発行とオンラインサービスへのアクセス
   各種手続きのオンライン化

2. ICカード（身分証）発行による物理サービスへのアクセス
   - 入退管理
   - 出席管理

- カード（物理）からモバイルデバイス（デジタル）へ
  - パスキーの普及で、すでにモバイルデバイス利用が前提化
  - モバイルデバイスにおける身分証の要件とは？

認証基盤の変遷 – ③ SSO（シングル・サイン・オン）

- 認証処理の部分もサービスから切り出して、IdPとして集約
  - デジタル署名技術を利用した「認証」と「認可」の分離
  - パスワードは、「サービス」には渡らない
- 「ワンストップ」認証
  - 認証済み状態を一定時間覚えることで、2回目以降の認証を省略
  - 認証機能をIdPに集約することで、多要素認証の導入も容易



に発展

SSOの仕組みとして、SAMLやOpenID Connectが利用される

IdP : ID Provider

SP : Service Provider

パスワードから多要素（MFA）へ

- パスワード（知識）による認証の限界
  - 複雑さより文字数が重要
  - 定期的に変更させるのはセキュリティ向上につながらない
  - 推測、フィッシング、中間者攻撃による被害の増加

- 物理トークン、マトリックス認証、SMS認証などの時代
  （1990年代）　（2000年代前半）　（2000年代後半）

- ワンタイムパスワード（OTP）の規格（計算方法）の統一 （2010年代）
  - OTP認証器（計算機）の所持による認証の方法として分類
  - Google Authenticatorをはじめ様々な認証器アプリが提供され、導入コストが低い

パスキー/FIDOの導入
(Fast IDentity Online)

2012 FIDO Alliance設立
2013（iPhoneでTouch ID開始）
2018 FIDO2/WebAuthnリリース
（W3C標準）
2022 マルチデバイス対応を機に
「パスキー」として展開

- 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）
  - スマートフォン等のモバイル端末の普及が後押し
  - ワンタイムパスワードによる多要素認証でもフィッシング被害に遭う
    - 2025年の証券口座不正取引被害額が数千億円規模
    - 警察庁、金融庁などがパスキーの積極的な普及活動に乗り出す

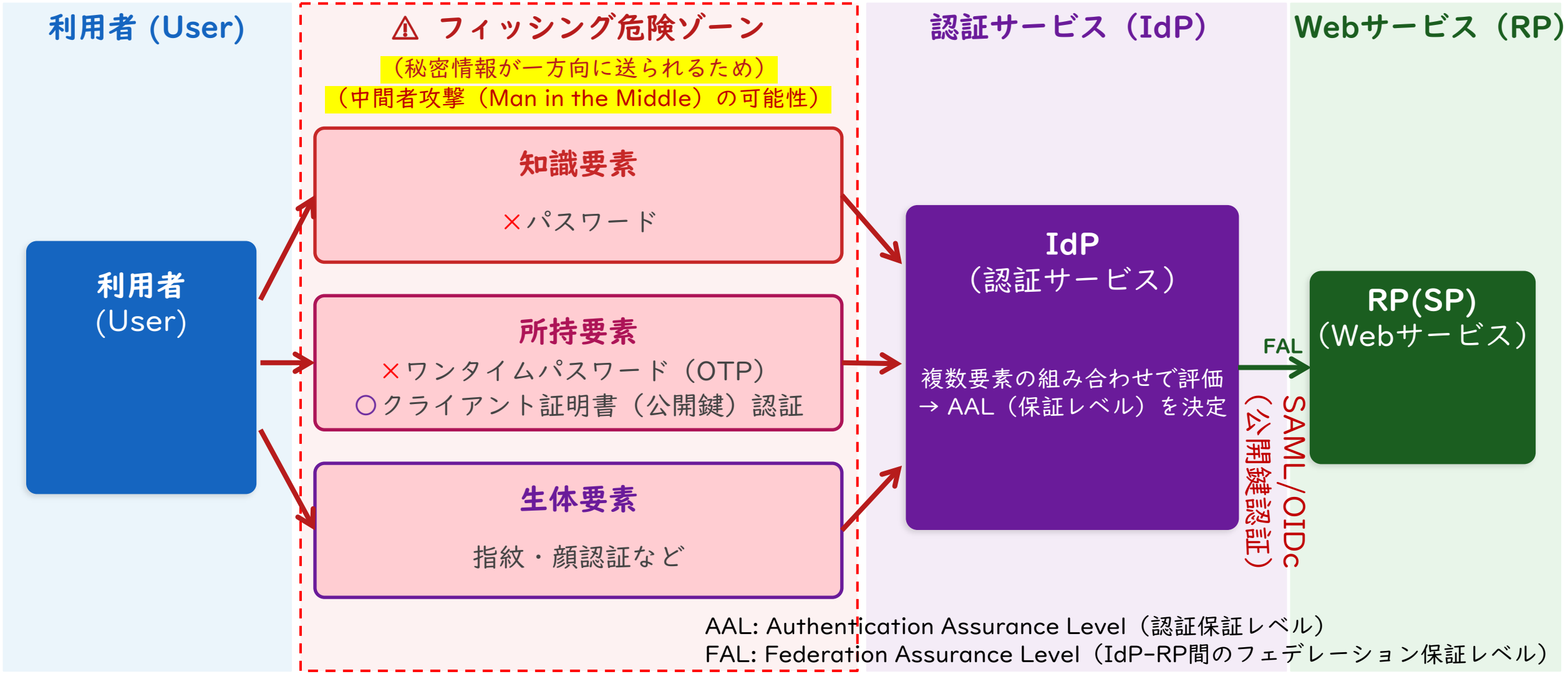
多要素認証の変遷

～ 従来の多要素認証（MFA）から FIDO・同期パスキーへ ～

「ユーザが秘密情報をサーバに送る」時代から「デバイスが署名する」(BYOD)時代へ

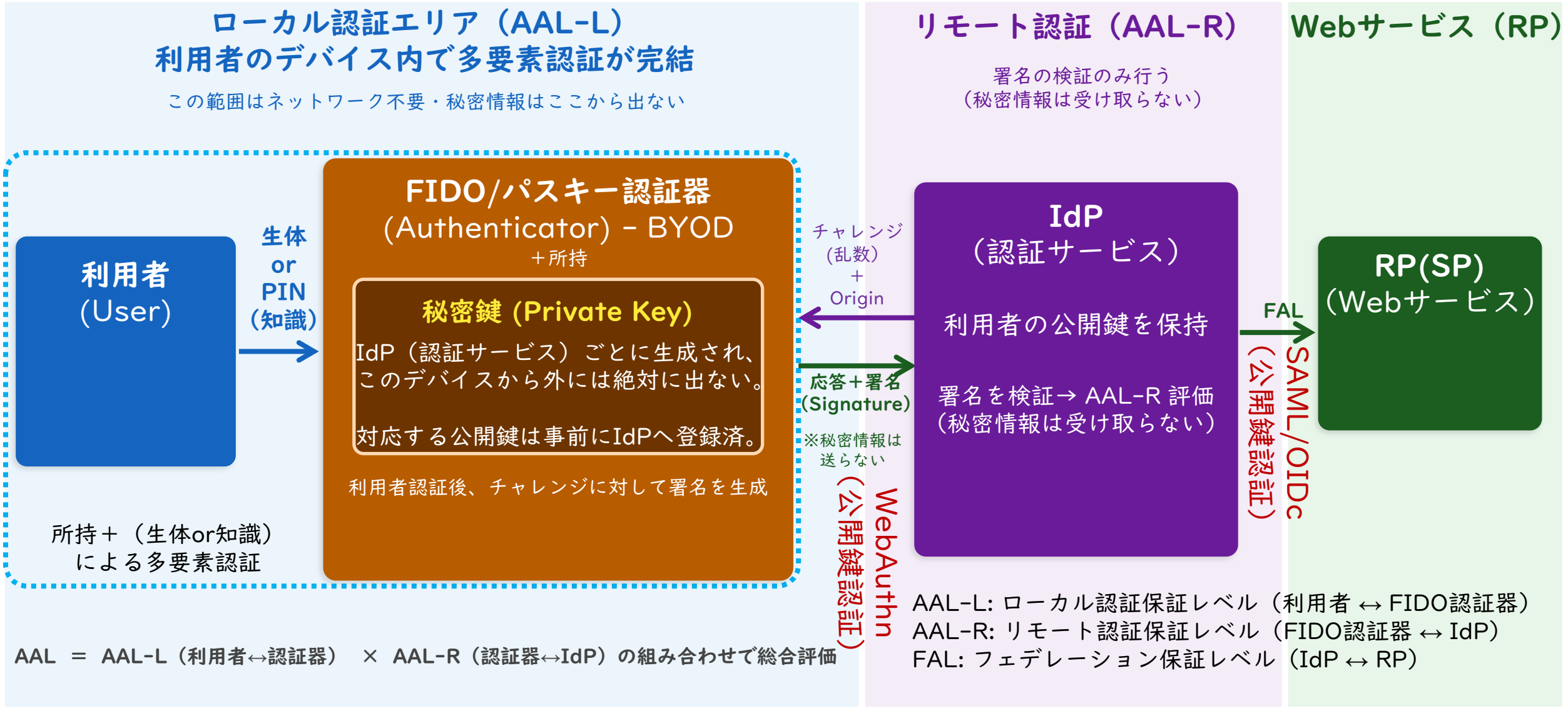
FIDO/パスキーは、クライアント証明書の利用上の問題（安全な配布・管理）を
利用者が所有するデバイス（スマートフォン等）で解決し、多要素認証の安全性構造を根本から変えた。

① 従来の多要素認証（MFA）：ユーザが「秘密情報」をネットワーク経由で送る方式



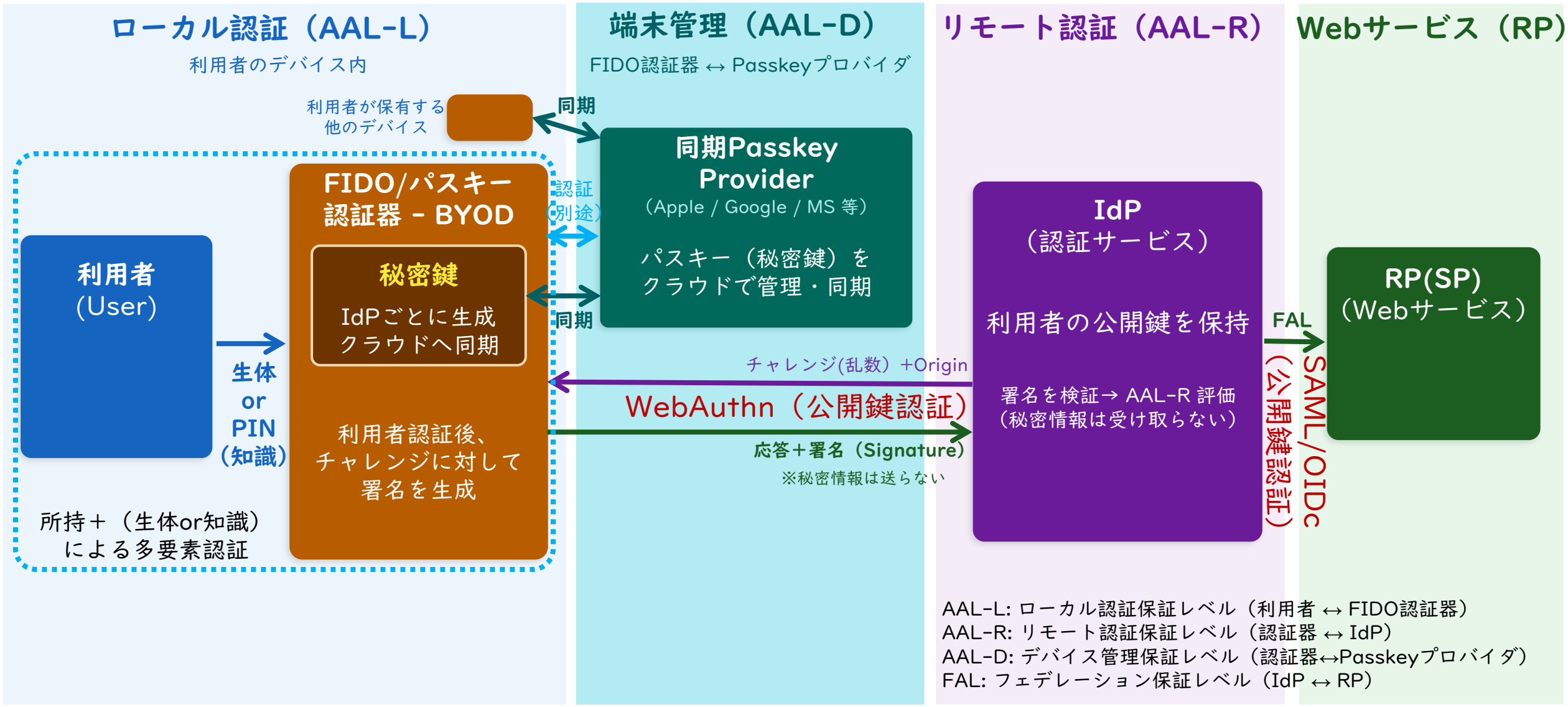
⚠ 課題：パスワード・OTP などの「秘密情報」が毎回ネットワークを経由してサーバに一方的に送られる仕組みであるため、
攻撃者が偽サイト（フィッシングサイト）を用意してユーザを誘導するだけで情報を盗める。
中間者攻撃に強い「クライアント証明書認証方式」は以前から選択肢にあったが、証明書を利用者が安全に管理する手段が確立されておらず普及しなかった。

② FIDO/パスキー（ハードウェア認証器）： 秘密鍵がデバイス外に出ない・フィッシング耐性あり



✅ ポイント：秘密鍵はFIDO認証器の外に出ない。接続先情報（Origin）を署名に封印したチャレンジ・レスポンス方式。
偽サイトへ誘導されても、チャレンジは偽サイトのオリジンに紐付くため攻撃者は正規サイトへの署名が得られない（フィッシング耐性の本質）。

③ 同期パスキー ：クラウド同期でマルチデバイス対応に進化。認証が「サービス（AaaS）」に

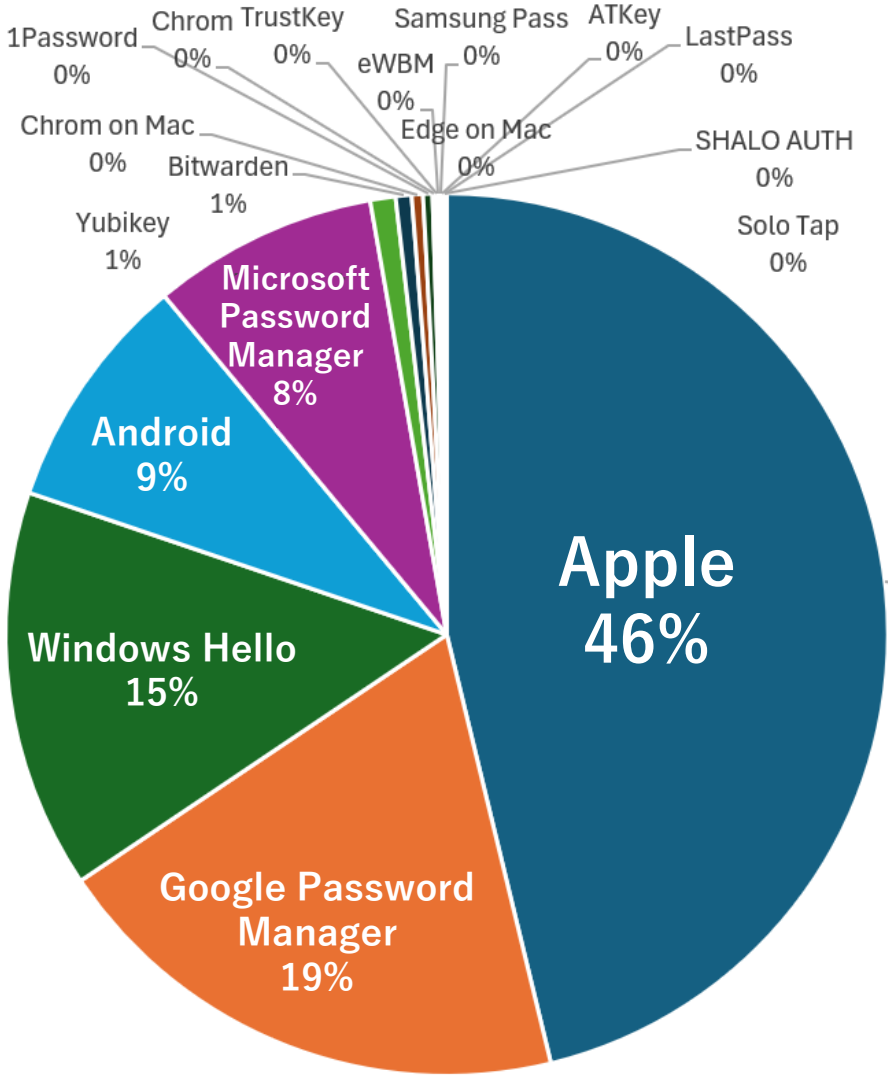


✅ 同一Passkeyを複数デバイスで利用可能
スマートフォン紛失時も容易に復元できる

⚠ 新たな課題：IdPはAAL-L・AAL-Rに加え、AAL-DとしてEnrollment・Recovery・クレデンシャルの保管・共有方法・デバイス認定などを総合的に評価し、最終的なAALを判断する必要がある。

本学でのパスキーの利用状況

- KULASIS/KULMSの多要素化で不便を感じた学生が登録（4月）
- 2026年4月21日時点の利用状況
  - 登録者数：2107
    - 認証器登録数
      - 1台 – 1482人
      - 2台 – 501人
      - 3台 – 93人
      - 4台 – 21人
      - 5台 – 7人
      - 6台 – 1人
      - 10台 – 1人
      - 11台 – 1人
  - 登録認証器数：2909
    - AAGUID調べ
      - Authenticator Attestation Global Unique IDentifier



「学修証明のデジタル化」の流れ

- 静的ドキュメントのデジタル化（1990年代～）
  - PDFの登場（1993～）、電子署名のサポート（1999～）
- オープンバッジ発表（Mozilla, 2011～）
  - 「マイクロ」の概念、 画像による表現
  - MozillaからIMS Global （現1EdTech）が引き継ぐ（2016)
  - OpenBadges 2.0 （2018、画像にJSON-LD等の埋め込み）
- VCへの統合（2020～）
  - W3C Verifiable Credential Data Model （2019）
  - OpenBadges 3.0 （2023、W3C VCベース）

VC事例

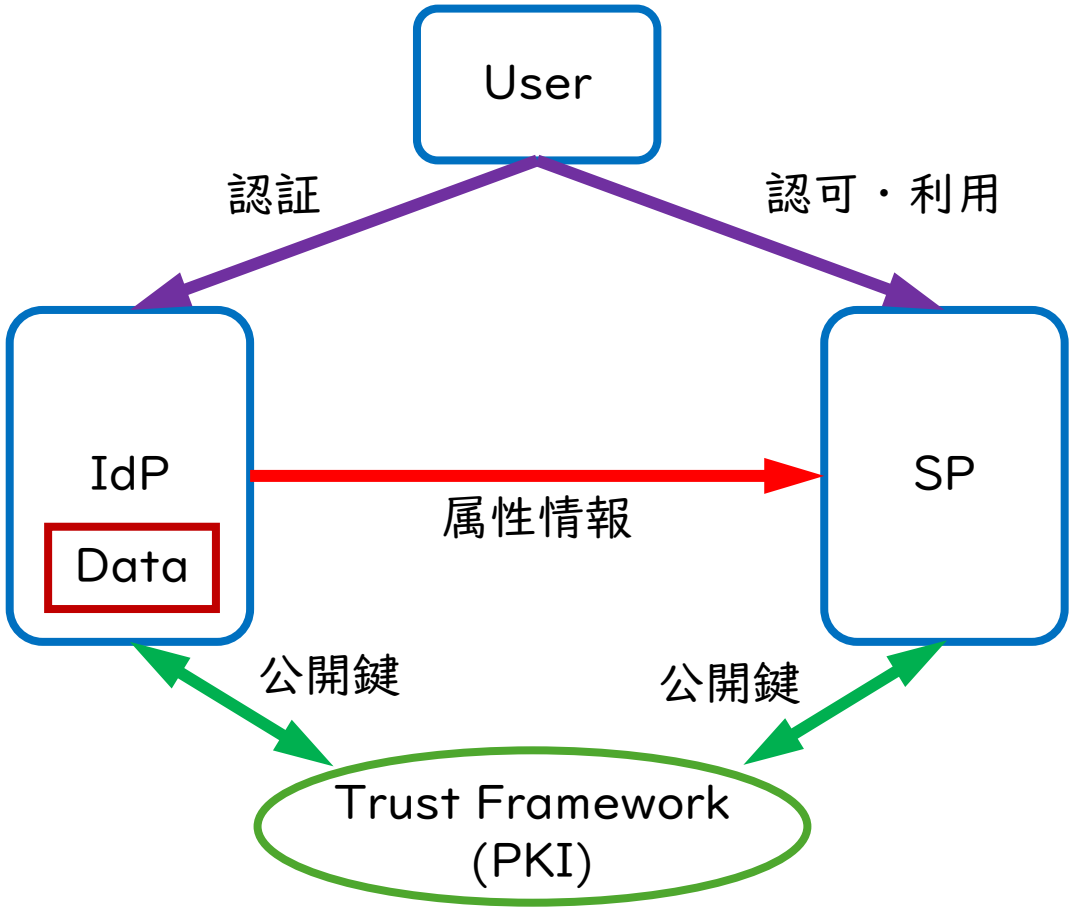
https://www.ipsj.or.jp/CITP/openbadge.html

(Open Badges 2.0 / VCでない)
- オンライン検証
- 限定的Holder Binding

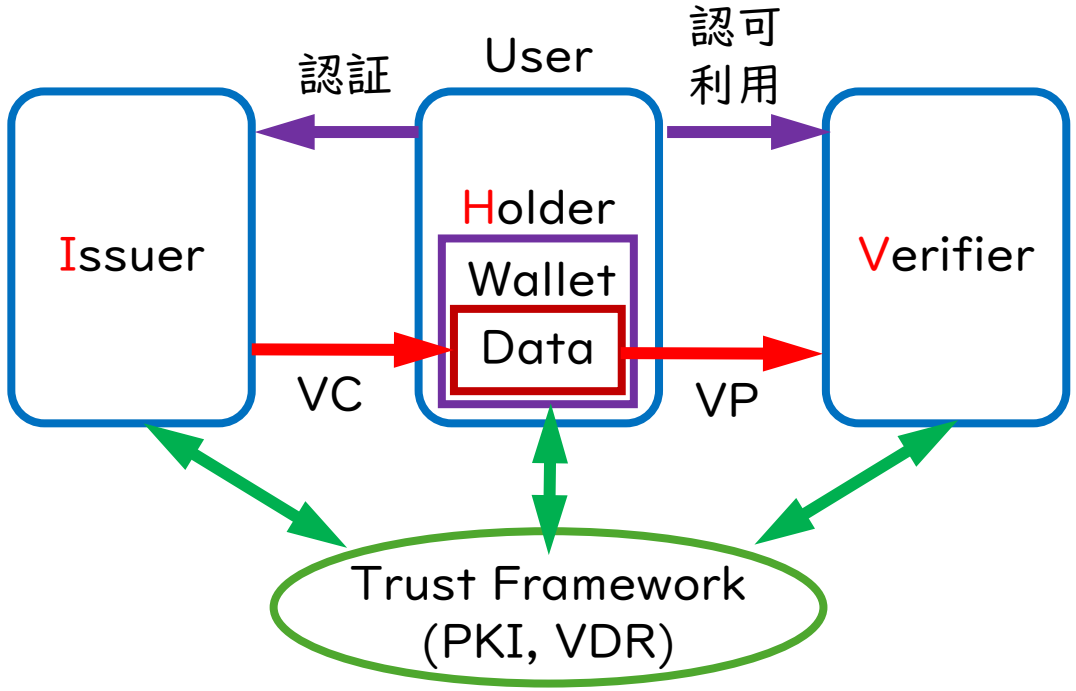
- ワクチン接種証明（2021年～2024年）
  - SMART Health Card（SHC）という健康証明用の規格
  - 海外事例
    - EUデジタルCOVID証明書（EU DCC）
    - WHO世界デジタル健康認証ネットワーク
- mDL（2022年～）
  - オーストリア、ルイジアナ州などが先行
- OpenBadges 3.0 （2024年～）
  - 2.0までの画像ベースと異なり、VCに対応した機械可読版に再設計
- EUDI Wallet
  - eIDAS 2.0に基づき、2026年までに欧州各国がサポート予定
- 大阪関西万博「ミャクーン！」NFT（参考：VCではない）
  - SBT（Soulbound Token）によるブロックチェーン上の永続的な証明

フェデレーションモデルとIHVモデル

Federation Model（FAL1/2）



IHV Model（FAL3）



VP: Verifiable Presentation

VDR: Verifiable Data Registry

VC (Verifiable Credential)標準化への流れ

- PKI / フェデレーション型Identity時代（1990-2000年代）を経て
- 個人を中心とする考え方の萌芽（2010年前後）
  - SSI: Self-Sovereign Identity（自己主権型アイデンティティ）
  - Open Badgesの発案（2011）
- ブロックチェーンとDIDの登場（2016年～2017年）
  - DID（Decentralized Identifier）
  - W3C Credentials Community Group (2014年～)
    - この頃は、Claims、Credentialsなどと呼ばれる
- 標準化
  - W3C Verifiable Credentials Data Model 1.0勧告（2019年）
    - W3C Verifiable Claims Working Group （2017年～）
    - Verifiable Credentialsという用語が正式に定義され、WGも名称変更
  - mDL/mdoc (ISO/IEC 18013-5)発行（2021年）
  - 欧州における政府IDとの統合: EUDI Wallet / eIDAS 2.0（2022年）
  - W3C VCDM 2.0勧告（2025年）
  - OpenID for Verifiable Credential Issuance 1.0 [OID4VCI] final等（2025年）

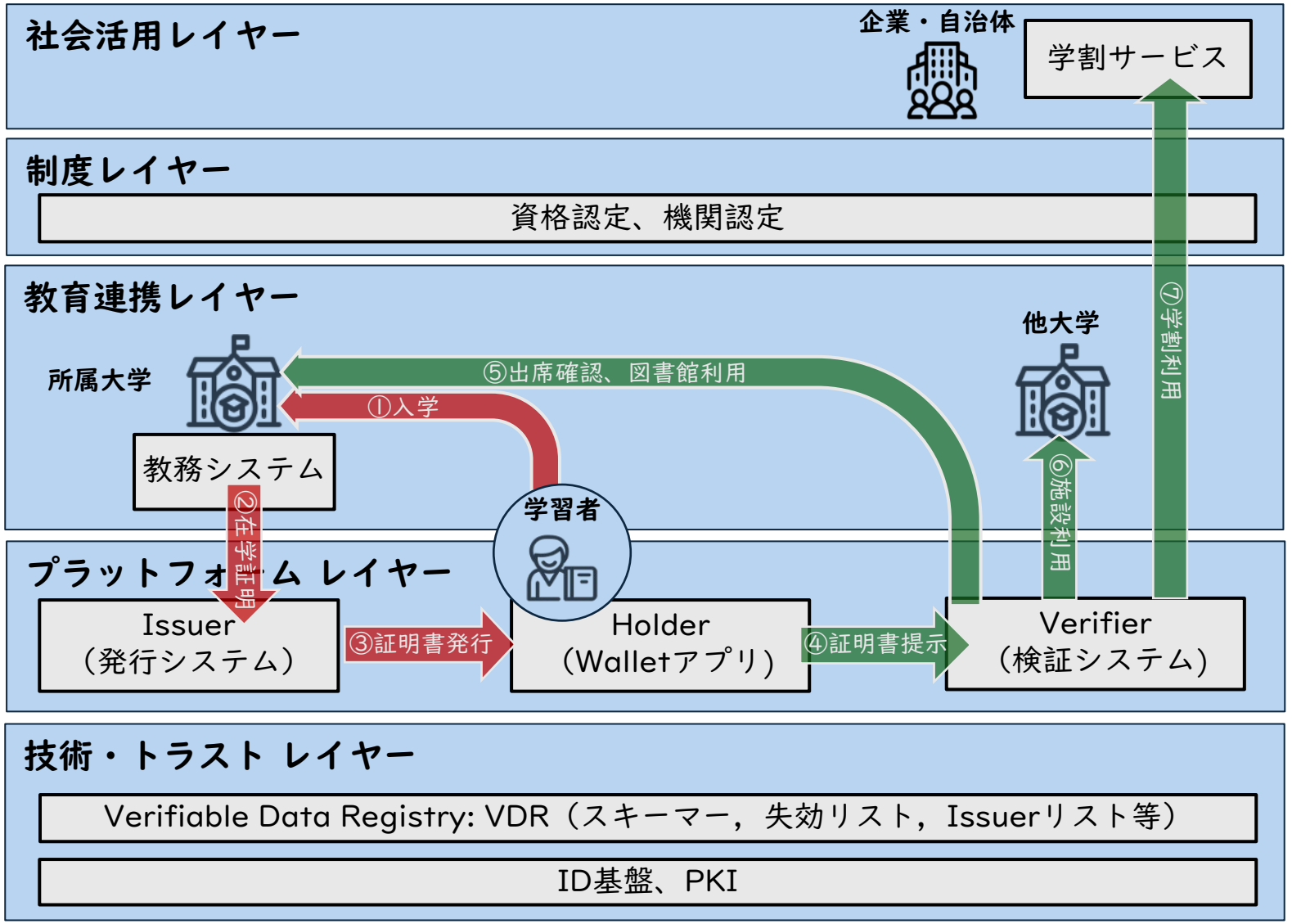
学術デジタル証明書の２つの用途

- 身分証明
  - 学生証、教職員証
  - 在学証明書、在籍証明書
  - ユーザに関する現時点の属性を証明する

- 経歴証明
  - 卒業・修了証明書、学位証明書（マクロクレデンシャル）
  - 単位取得証明書（マイクロクレデンシャル）
  - ユーザに関する過去の属性を証明する

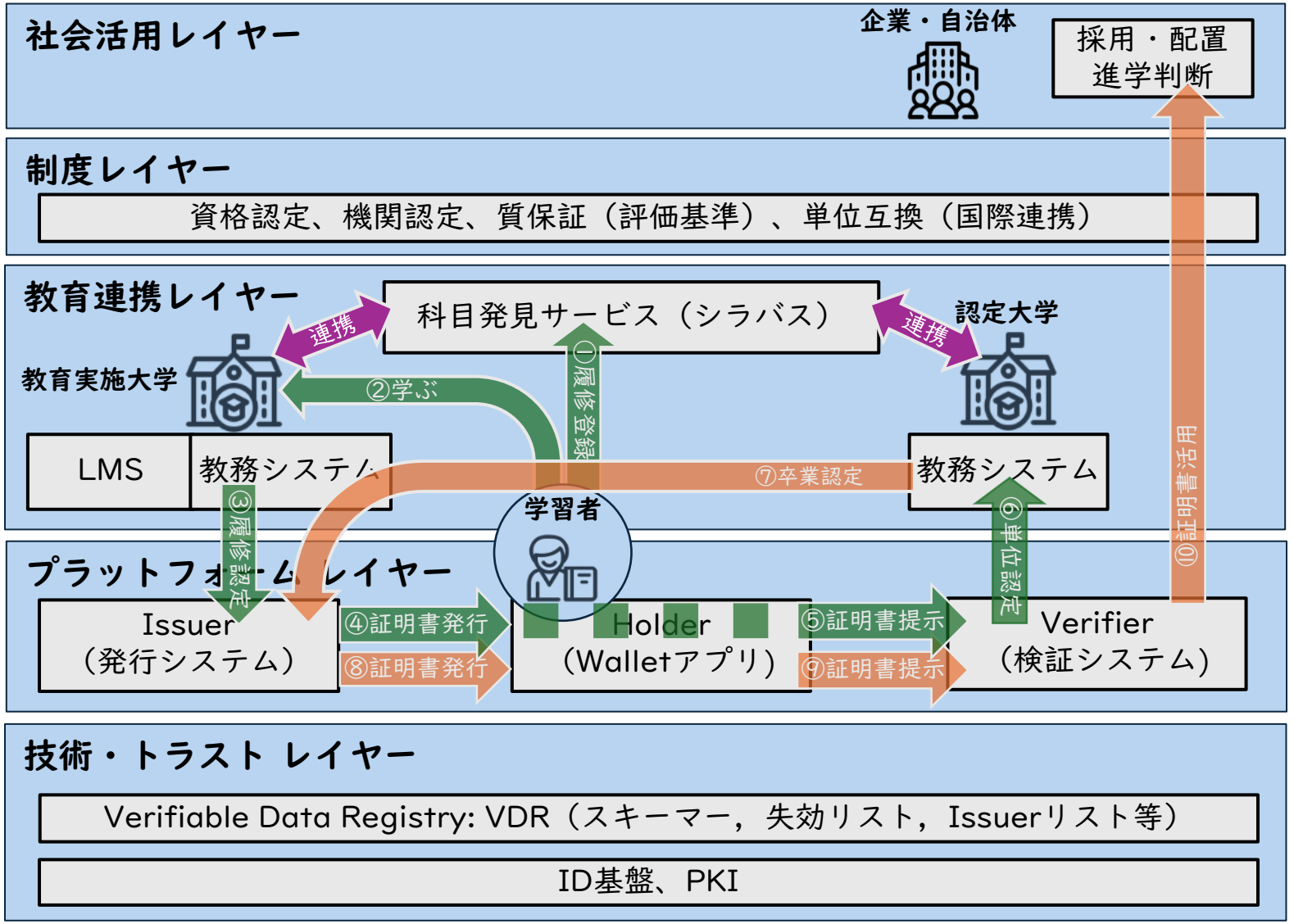
IHV型学術デジタル証明書基盤の事例－１

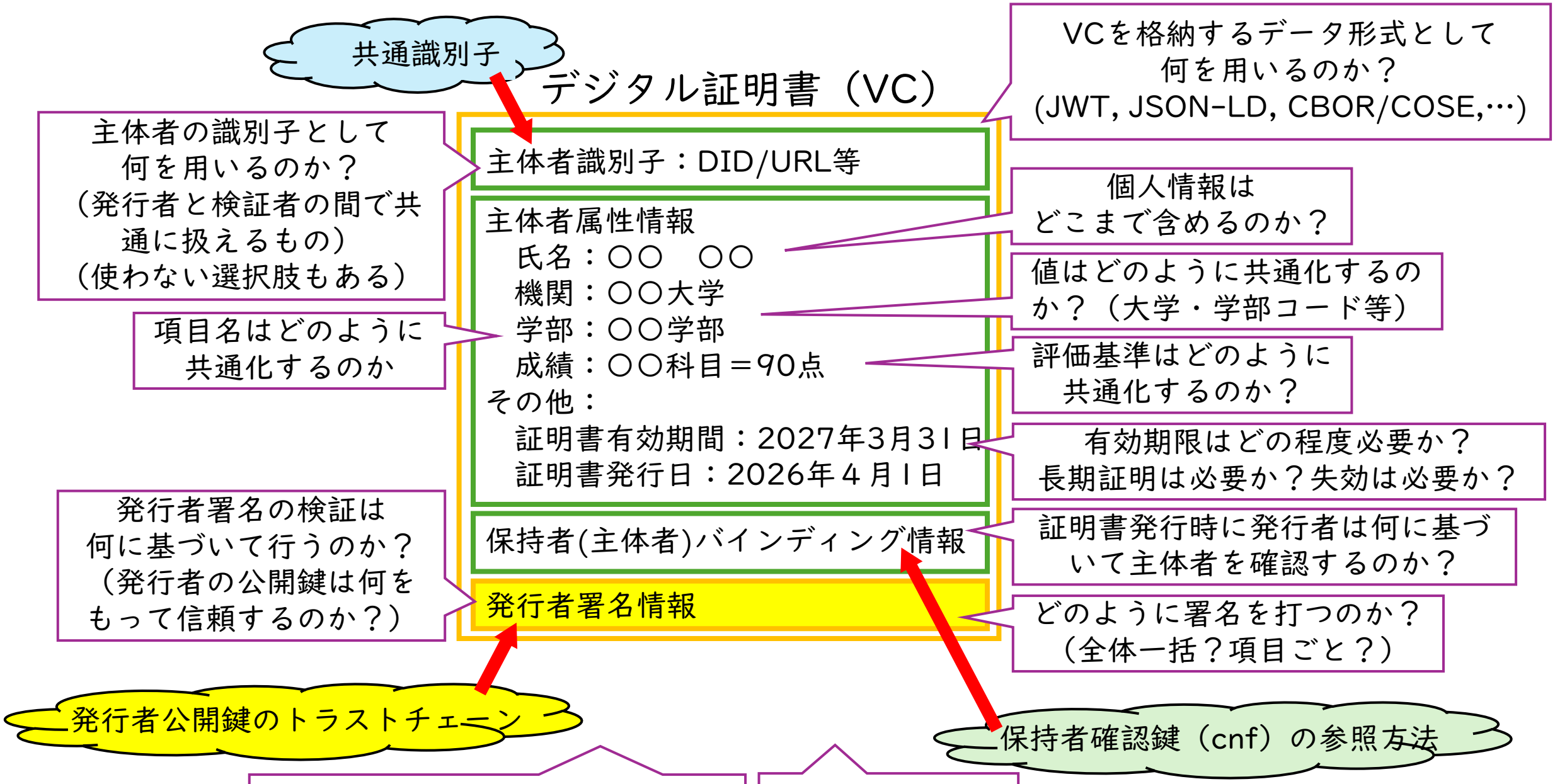
デジタル身分証を実現する基盤



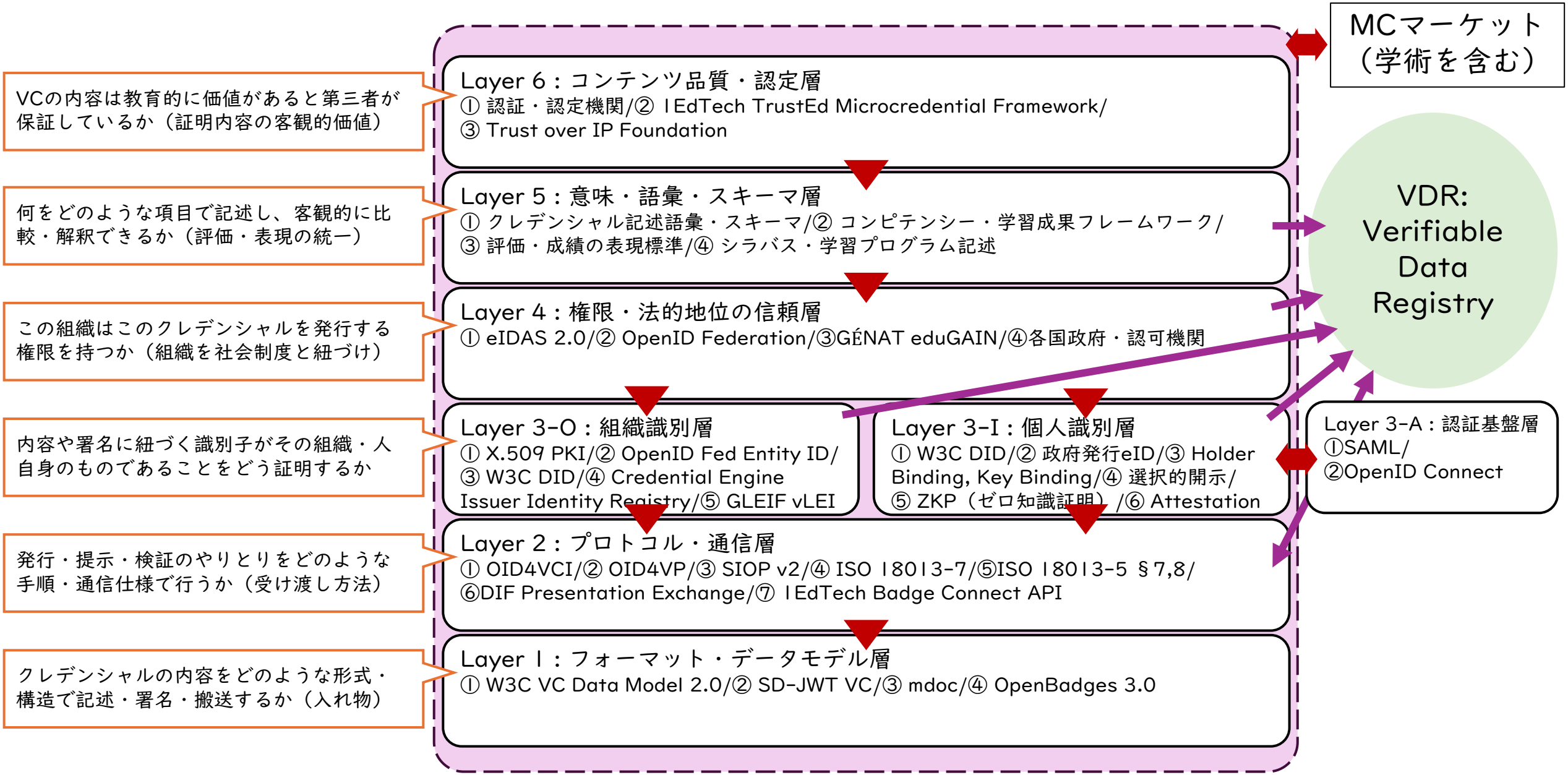
IHV型学術デジタル証明書基盤の事例-２

教育連携・成績証明・社会接続（就職・人材配置）を同一基盤で実現




共通識別子
デジタル証明書（VC）
VCを格納するデータ形式として
何を用いるのか？
(JWT, JSON-LD, CBOR/COSE,…)
主体者の識別子として
何を用いるのか？
（発行者と検証者の間で共
通に扱えるもの）
（使わない選択肢もある）
主体者識別子：DID/URL等
個人情報は
どこまで含めるのか？
主体者属性情報
氏名：〇〇　〇〇
機関：〇〇大学
学部：〇〇学部
成績：〇〇科目＝90点
その他：
証明書有効期間：2027年3月31日
証明書発行日：2026年４月１日
値はどのように共通化するの
か？（大学・学部コード等）
項目名はどのように
共通化するのか
評価基準はどのように
共通化するのか？
有効期限はどの程度必要か？
長期証明は必要か？失効は必要か？
保持者(主体者)バインディング情報
証明書発行時に発行者は何に基づ
いて主体者を確認するのか？
発行者署名の検証は
何に基づいて行うのか？
（発行者の公開鍵は何を
もって信頼するのか？）
発行者署名情報
どのように署名を打つのか？
（全体一括？項目ごと？）
発行者公開鍵のトラストチェーン
保持者確認鍵（cnf）の参照方法
VCを受け渡すプロトコルとして
何を用いるのか？
選択的開示の
機能は必要か？
VCを検証者に提示する際に
本人のVCであることを証明

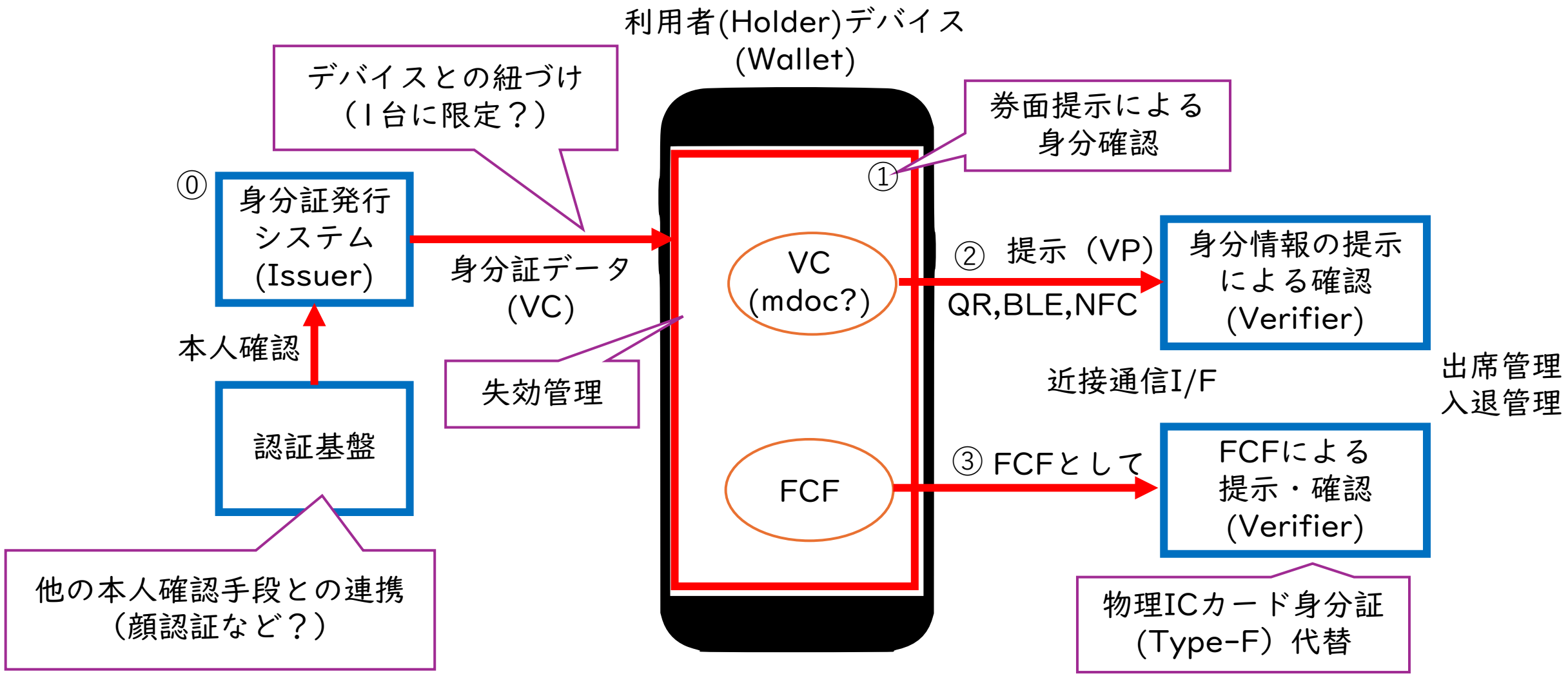
学術デジタル証明（MC/VC）を扱うための「技術」の関係整理



学術デジタル証明（VC）基盤実現のための「ガバナンス」関係整理

ガバナンス構造	対応する技術要素
実社会制度層 文部科学省等 / 教育機関認可制度 NIAD-QE・NIC（機関認定・質保証）	機関認定情報（Trust List）の法的根拠 発行機関レジストリへの権威付け 識別子制度（学籍番号・マイナ等）の定義
教育コンソーシアム層 マイクロクレデンシャル機構等 大学団体・学術認証フェデレーション	スキーマ語彙・項目名の標準化 評価基準・セマンティクスの合意 質保証フレームワーク
技術基盤コンソーシアム層 W3C / 1EdTech / OpenID Foundation IETF・技術仕様策定コミュニティ	VCフォーマット / クレデンシャル形式 トランスポートプロトコル（OID4VCI等） 署名アルゴリズム / 公開鍵Trust Chain
機関認定・登録管理層 発行機関レジストリ運営者 Wallet認定機関・認証局	発行者公開鍵の登録・Key Discovery 機関識別子・DIDの管理 Walletの認定・監査基準の適用
運用層 Issuer（大学等）/ Verifier（検証機関・企業）	VC発行・失効管理 / 検証システム 学籍・成績システムとの連携I/F
Holder層（学生） ウォレット / 同意・提示の主体	Wallet・VP提示・選択的開示 保持者バインディング（cnf）

デジタル身分証を構成する要素



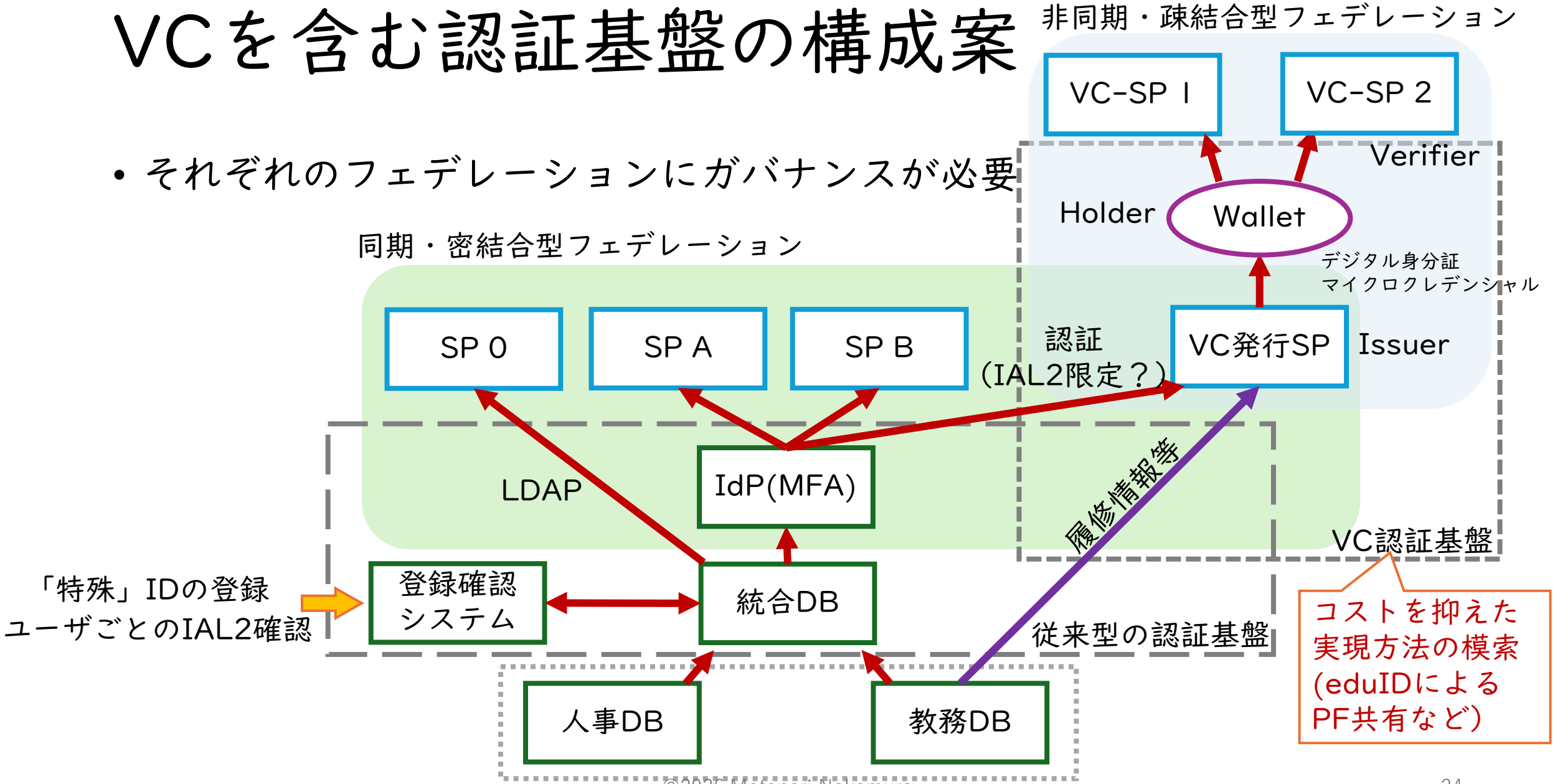
FCF: Felicitous Common use Format

デジタル身分証の実現に向けた課題

- 国際的統一標準がまだ存在（決定）していない
  - EUDIWにおける教育証明の義務化は未定
  - 「信頼フレームワーク」の構築はこれから
- デジタルでの対面検証インタフェースの標準化
  - 券面提示における真正性確認方法（学割、定期試験対応等）
  - NFC, QR, BLE, etc.
  - 入退等の既存のICカード利用システムからの移行方法
- 運用方法の検討
  - 有効期限設定、失効管理、複数発行可否、コスト削減
- スマートフォンを持たない者への対応

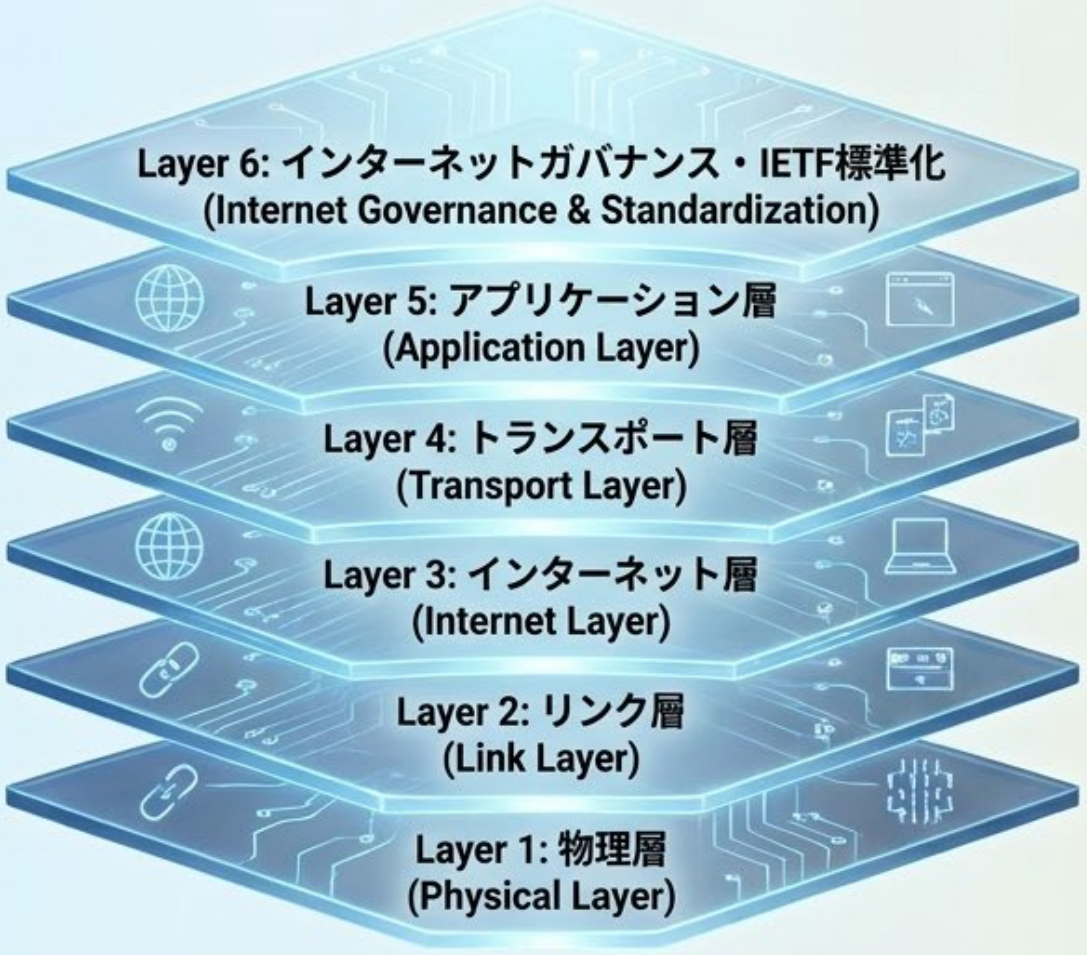
VCを含む認証基盤の構成案

- それぞれのフェデレーションにガバナンスが必要



コア・メタファー：「通信」のインターネットから、「トラスト」のインターネットへ

インターネットという全世界の通信環境の理想を共有し、協力して作り上げてきたように、
新しいアーキテクチャはトラストという視点での理想を共有し、協力してトラストインターネットを作り上げる。



インターネットの階層構造 (Internet Architecture)

トラストの階層構造 (VC/eduID Architecture)

まとめ

- 大学の多様な活動を支える、これからの認証基盤
  - 当人確認レベル（AAL）と身元確認レベル（IAL）の整理
  - 多要素認証への移行手順における脆弱性の点検
  - 同期パスキーの普及を見据えたBYOD運用ルールの検討

- 身分証・学修証明のデジタル化
  - VC (Verifiable Credentials)の導入と活用の検討
  - 既存システム（入退等）からの移行手順の整理
  - コスパの良いプラットフォームの在り方（eduID）

今後のイベントのご案内

1. TIESシンポジウム2026
   『みらいの教育を変えるマイクロクレデンシャル』
   - 2026年6月26日（金）
   - 大阪教育大学みらい教育共創館5階
   - 現地：一般5,000円/会員無料、リモート：無料
   - https://www.cties.jp/events/e20260626/

2. 『デジタルクレデンシャル円卓会議2026』
   - 2026年7月15（水）14:00 ～ 19:30
   - 一ツ橋講堂 中会議場（東京都千代田区）
   - 参加無料
   - https://openid.connpass.com/event/393175/