研究教育活動を支える大学ID基盤のこれから

中村 素典 / 情報環境機構 IT基盤センター

EDIX Tokyo 2026

2026/5/13

ED-S8

質問用QRコード

自己紹介（経歴）

- 1989 京都大学 工学部情報工学科 卒業
- 1991 京都大学 大学院工学研究科修士課程 修了
- 1994 同 博士課程 単位修得退学
- 1994 立命館大学 理工学部 助手
- 1995 京都大学 経済学部 助教授
- 1999 京都大学 総合情報メディアセンター 助教授
- 2007 国立情報学研究所(NII) 学術NW研究開発センター 特任教授
- 2019 京都大学 情報環境機構 教授 / 国立情報学研究所 客員教授
- 2022 京都大学 情報環境機構 IT企画室長・CIO補佐官
- 2024 京都大学 情報環境機構 IT基盤センター長・CIO補佐官

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
   - 大学における認証基盤の見直し

2. VC (Verifiable Credential)の時代へ
   - 大学はどのようにサポートすべきか

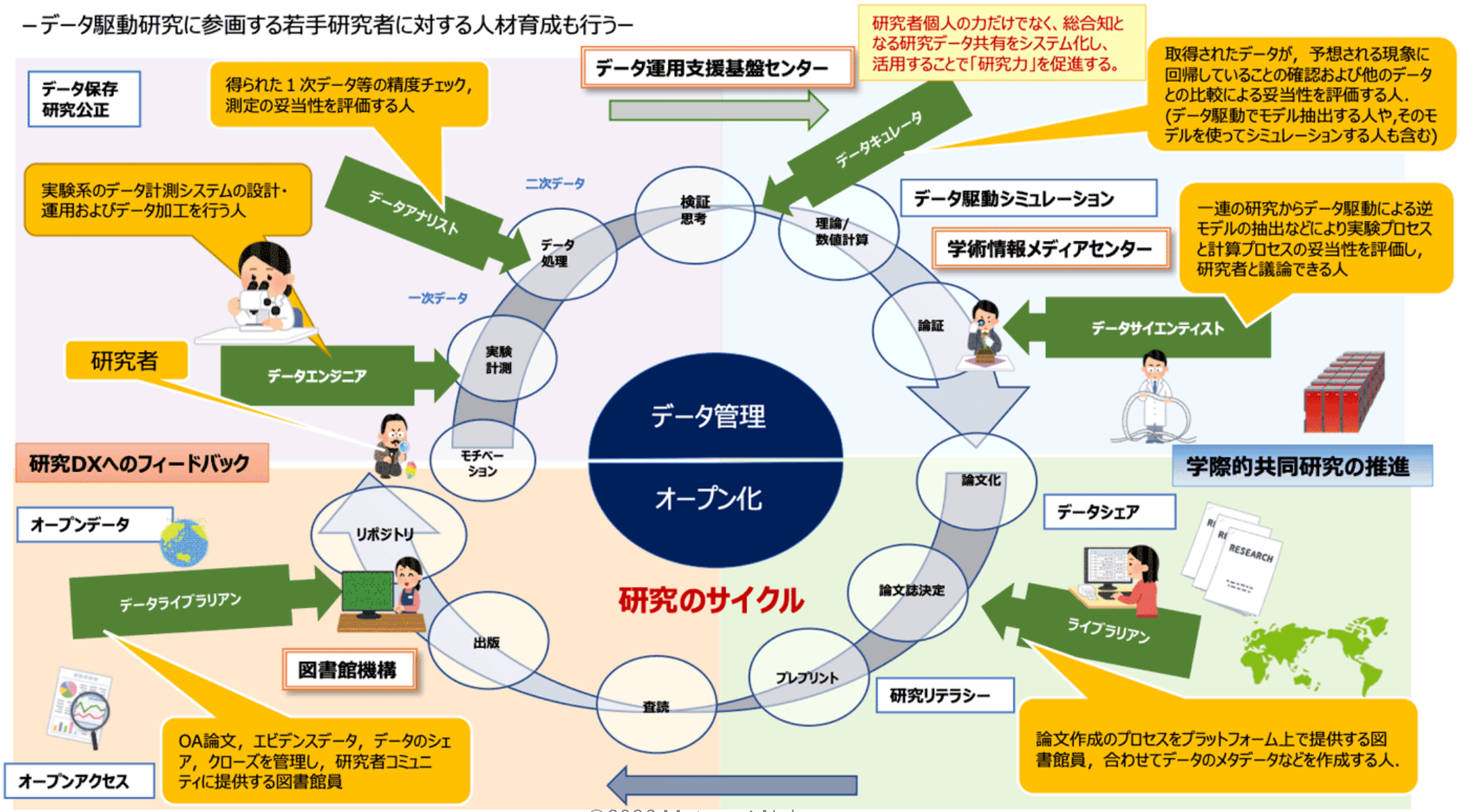
京都大学 の「認証」を支える体制の変化

- 1997/4: 総合情報メディアセンターを設置
  - 「情報処理教育センター（教育用計算機）＋工学部高度情報実験施設」を改組
- 2002/4: 学術情報メディアセンターを設置
  - 「総合情報メディアセンター+大型計算機センター+KUINS」を改組
- 2005/4: 情報環境機構を設置
  - 「情報部＋学術情報メディアセンター」の体制で基盤整備を行う
- 2009/4:情報部に統合認証センターを設置
  - ICカードの発行開始
- 2011/4: 情報環境機構にIT企画室を設置
  - 「情報部＋IT企画室＋学術情報メディアセンター」の体制に移行
- 2011/5: 統合認証センターを情報部から情報環境機構に移管
  - 教職員メール(2010-)＋学生用メール（2012に教育支援から移管）の発行管理
- 2014: 統合認証センターを廃止、情報基盤部門と情報環境支援センターが引き継ぐ（分割）
- 2024/1: 情報環境機構にIT基盤センターを設置
  - IT企画室を廃止
- 2024/1: 情報環境機構にデータ運用支援基盤センターを設置
  - 「情報部＋2センター＋学術情報メディアセンター」の体制に移行
- 2025/10: 教育支援グループ＋情報環境支援センターを統合して利用支援グループに改組
  - 認証システムを情報基盤グループから利用支援グループに移管（集約）

研究サイクルの支援により研究DXを進めるデータ運用支援基盤センター

＜次世代研究を創造する研究サイクルのプラットフォームの構築＞

－データ駆動研究に参画する若手研究者に対する人材育成も行う－



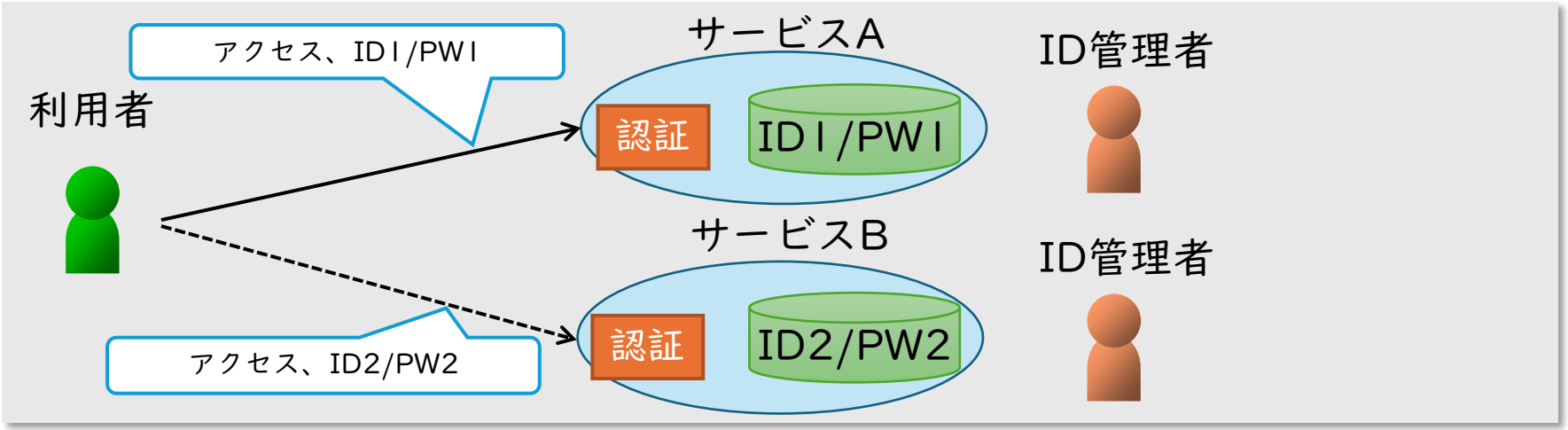
京都大学で扱う「ユーザ」

- 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

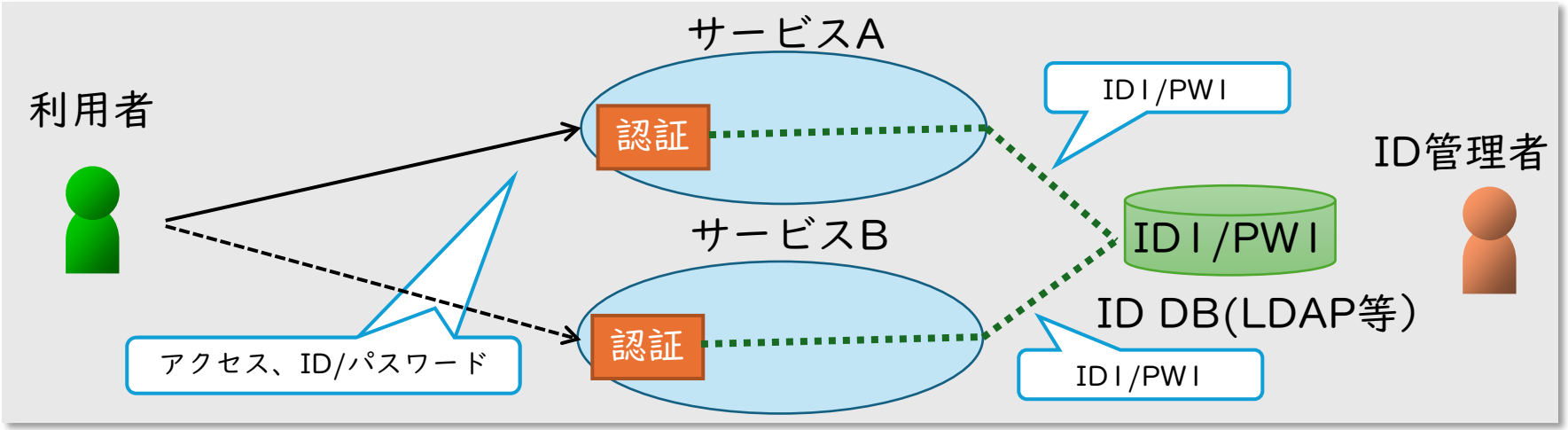
認証基盤の変遷 – ① 独立管理（～1990年代前半）

- ユーザ毎にIDを発行
- 異なるパスワード



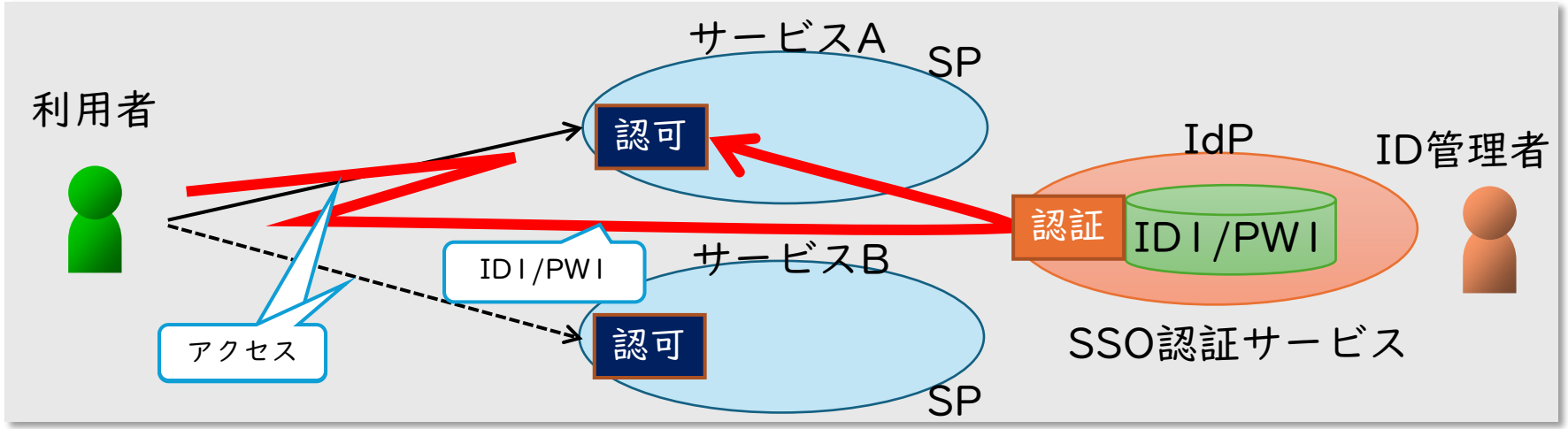
認証基盤の変遷 – ② ID統合　（～2000年代前半）

- ユーザ毎のID、パスワードを統一（IDデータベースを統合）
  - 管理の手間が減ってユーザも管理者も嬉しい
- パスワードは、従来通り各サービスに直接投入される
  - パスワード漏洩の危険性
  - パスワードのつかいわけ（つかいまわし？）



認証基盤の変遷 – ③ SSO（シングル・サイン・オン）　（2000年代後半～）

- 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



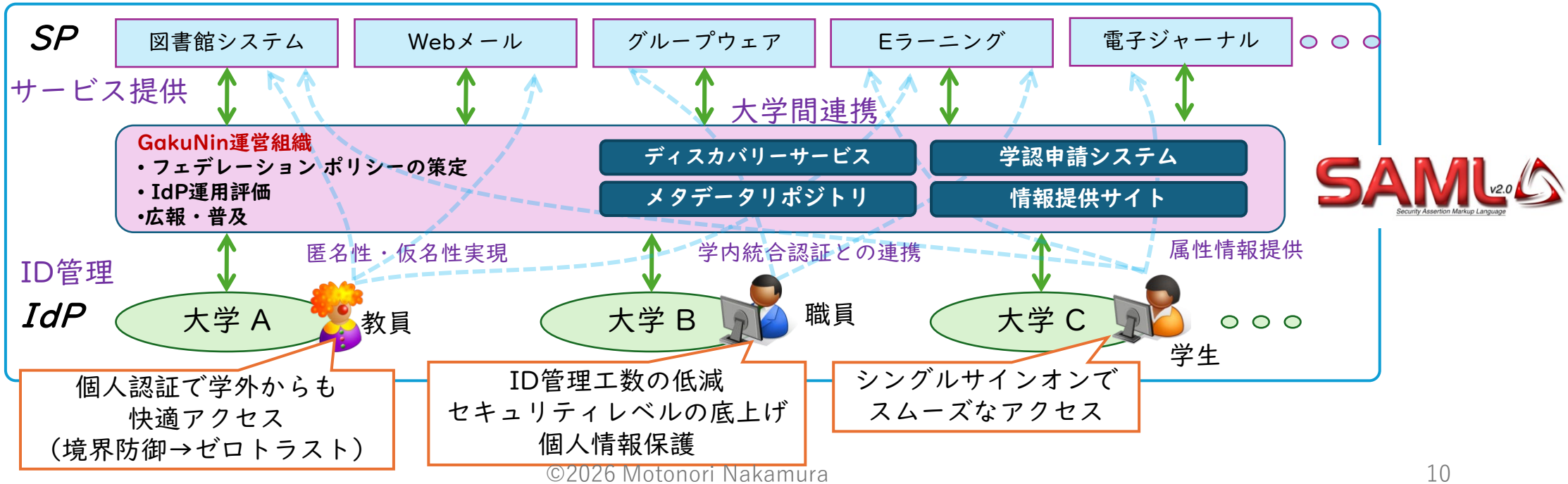
SSOの仕組みとして、SAMLやOpenID Connectが利用される

IdP : ID Provider

SP : Service Provider

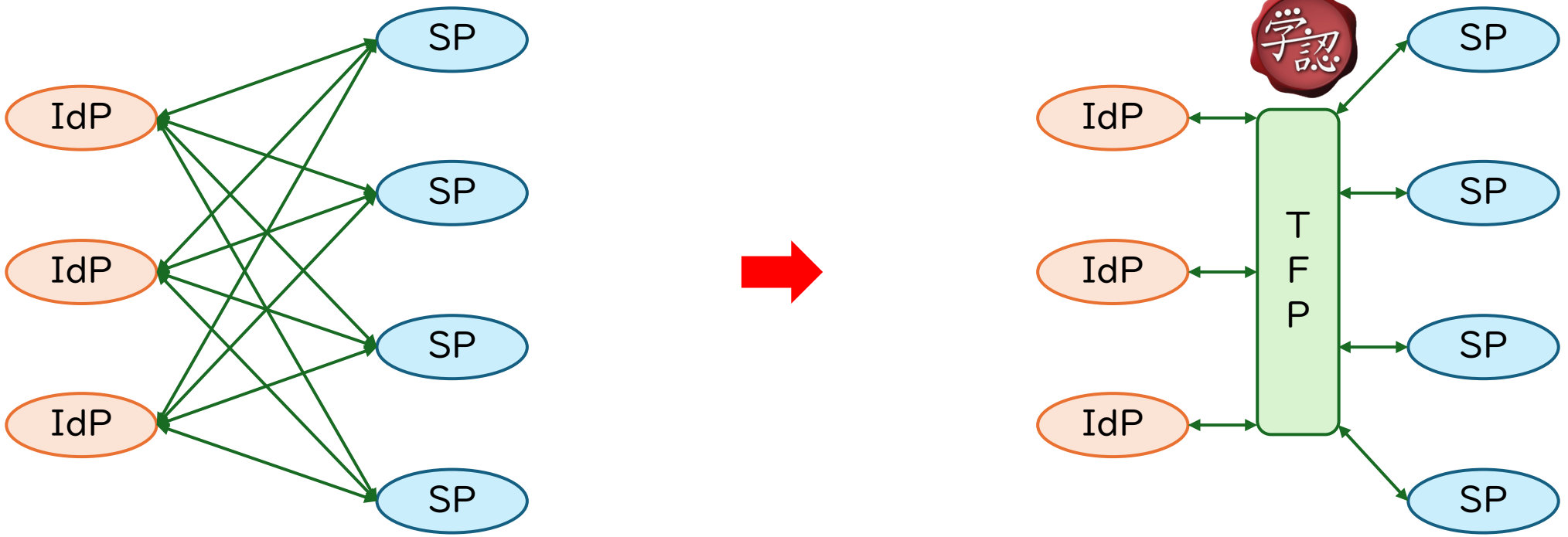
学術認証フェデレーション「学認」 by NII
– 学外サービスでの認証利用 –　（2009年～）

- シングルサインオン(SSO)技術に基づく学術研究支援IT基盤の構築
- IdP・SP相互の信頼を持続する信頼フレームワークの提供
- ID基盤のインフラ化による利便性向上、付加価値の実現、新サービスの創出
  - 大学間連携、産学連携、国際連携



フェデレーションの集約による効果

- 一律のポリシーに基づく信頼フレームワークの導入により、個別調整でのN×Mの関係が、N＋Mの関係に効率化



TFP: Trust Framework Provider

京都大学で「ユーザ」に付与する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
- 教育用計算機由来
  - 学生等向けサービス用（源泉：教務DB）
    - 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、…

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

多要素認証（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。

SSOが導入済みなので、多要素認証への対応もスムーズ

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

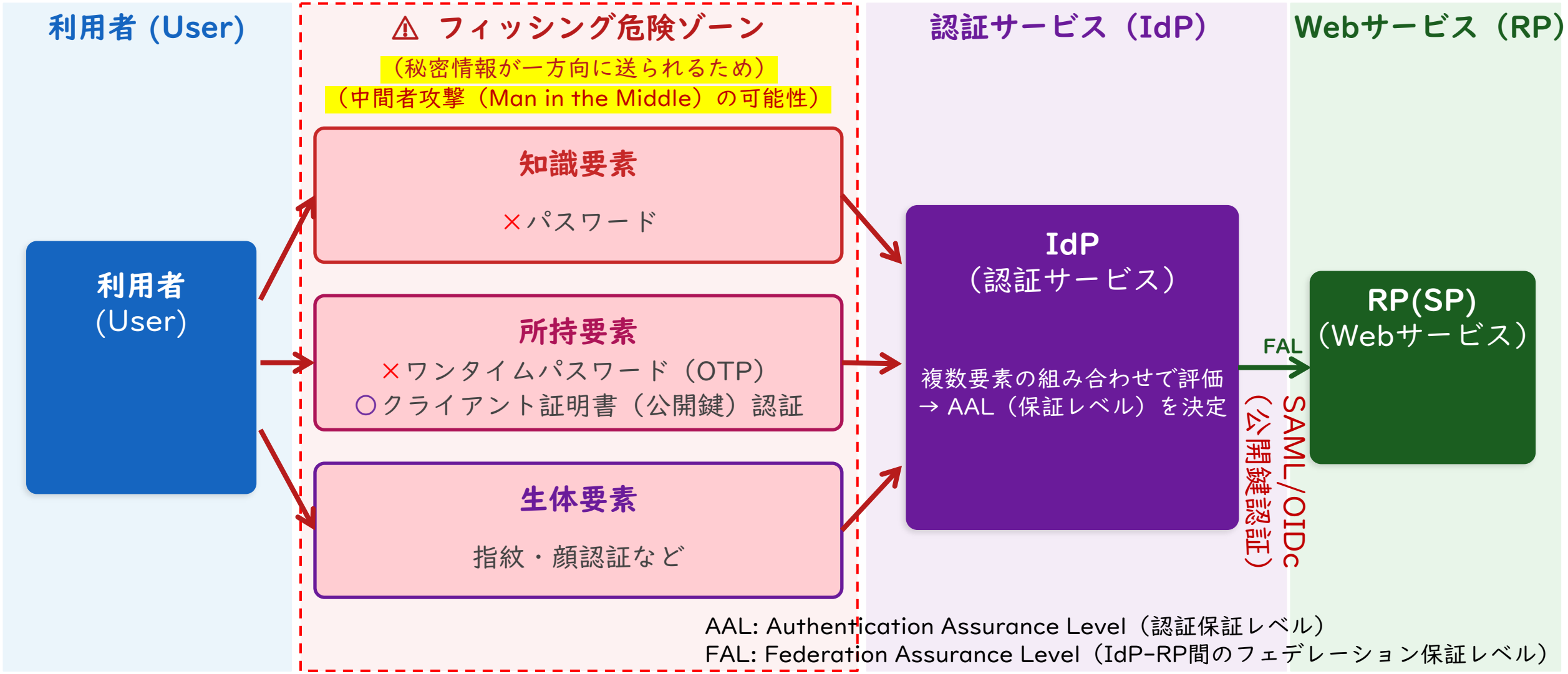
多要素認証の変遷

～ 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」時代へ

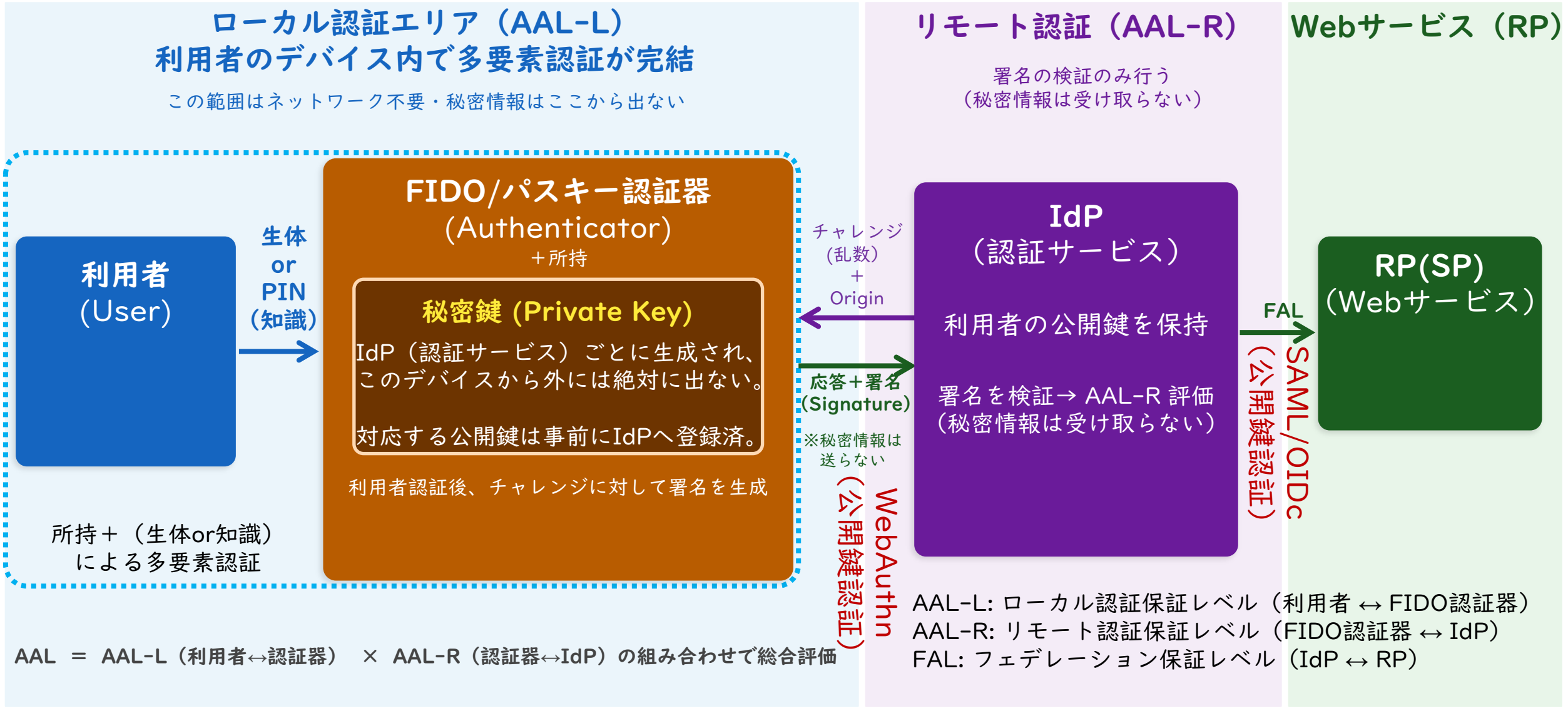
FIDO/パスキーは、クライアント証明書の利用上の問題（安全な配布・管理）を
利用者が所有するデバイス（スマートフォン等）で解決し、多要素認証の安全性構造を根本から変えた。

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



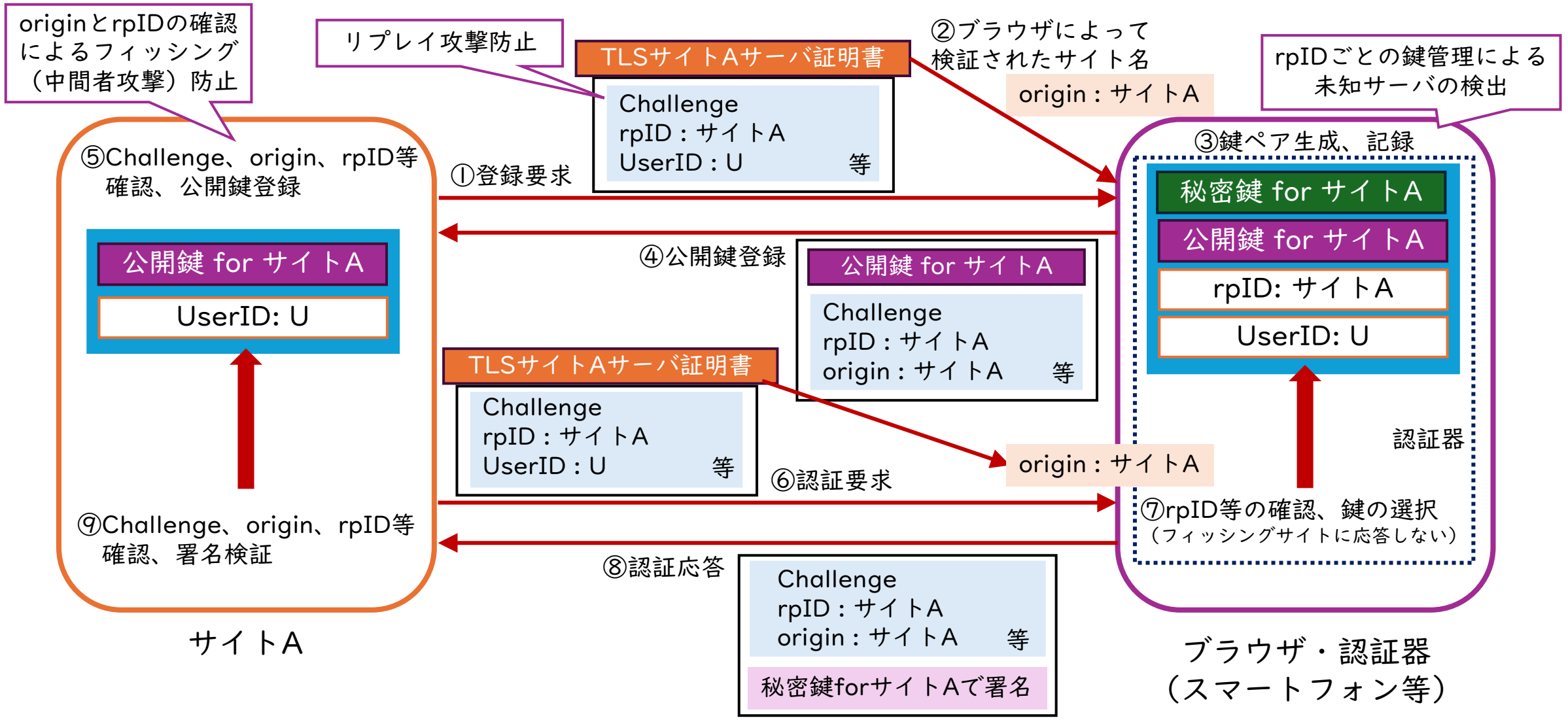
⚠ 課題：パスワード・OTP などの「秘密情報」が毎回ネットワークを経由してサーバに一方的に送られる仕組みであるため、
攻撃者が偽サイト（フィッシングサイト）を用意してユーザを誘導するだけで情報を盗める。
中間者攻撃に強い「クライアント証明書認証方式」は以前から選択肢にあったが、証明書を利用者が安全に管理する手段が確立されておらず普及しなかった。

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



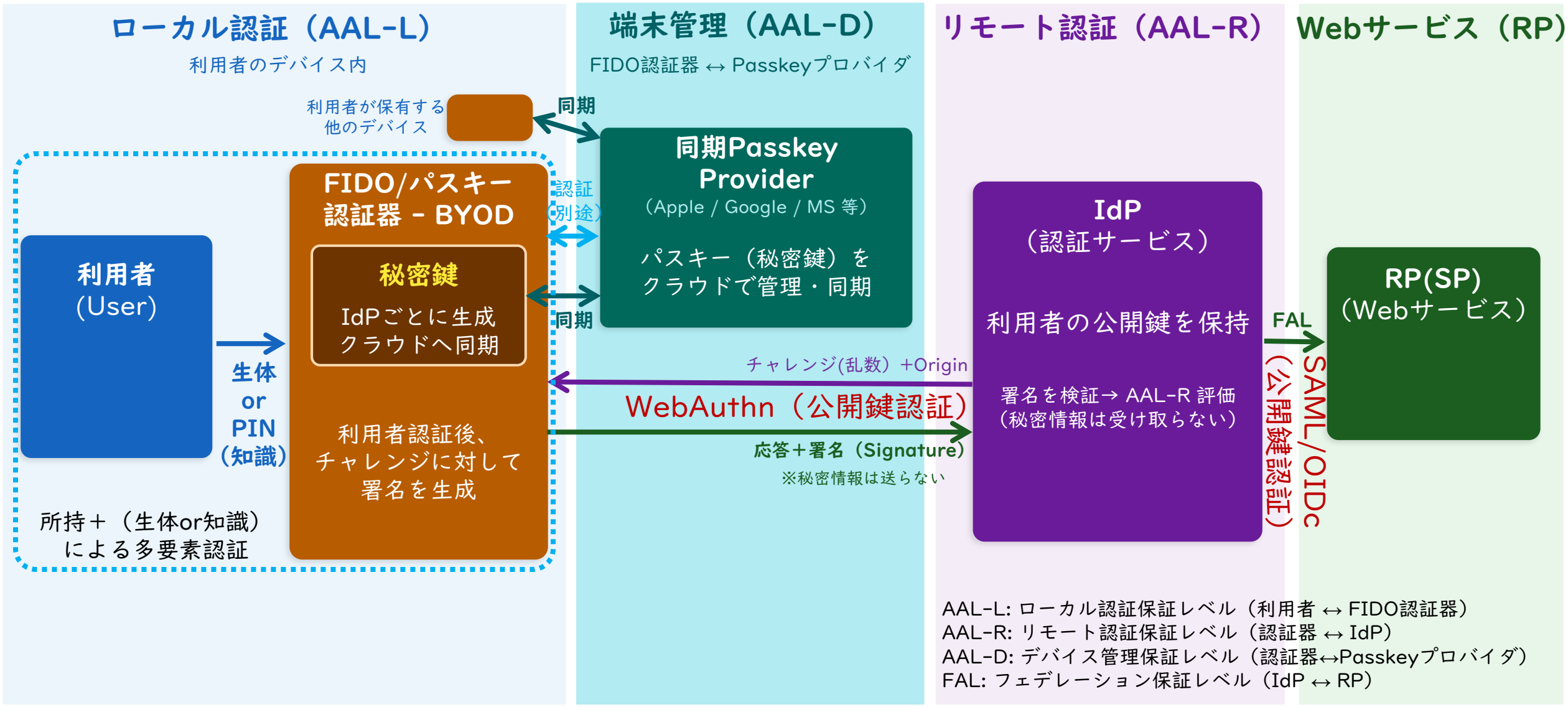
✅ ポイント：秘密鍵はFIDO認証器の外に出ない。接続先情報（Origin）を署名に封印したチャレンジ・レスポンス方式。
偽サイトへ誘導されても、チャレンジは偽サイトのオリジンに紐付くため攻撃者は正規サイトへの署名が得られない（フィッシング耐性の本質）。

（参考）　フィッシングを防止するWebAuthnの仕組み



従来のパスワードやOTP認証は、相手が正しいサーバかどうかにかかわらず情報を送ってしまうためフィッシングに遭う。

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

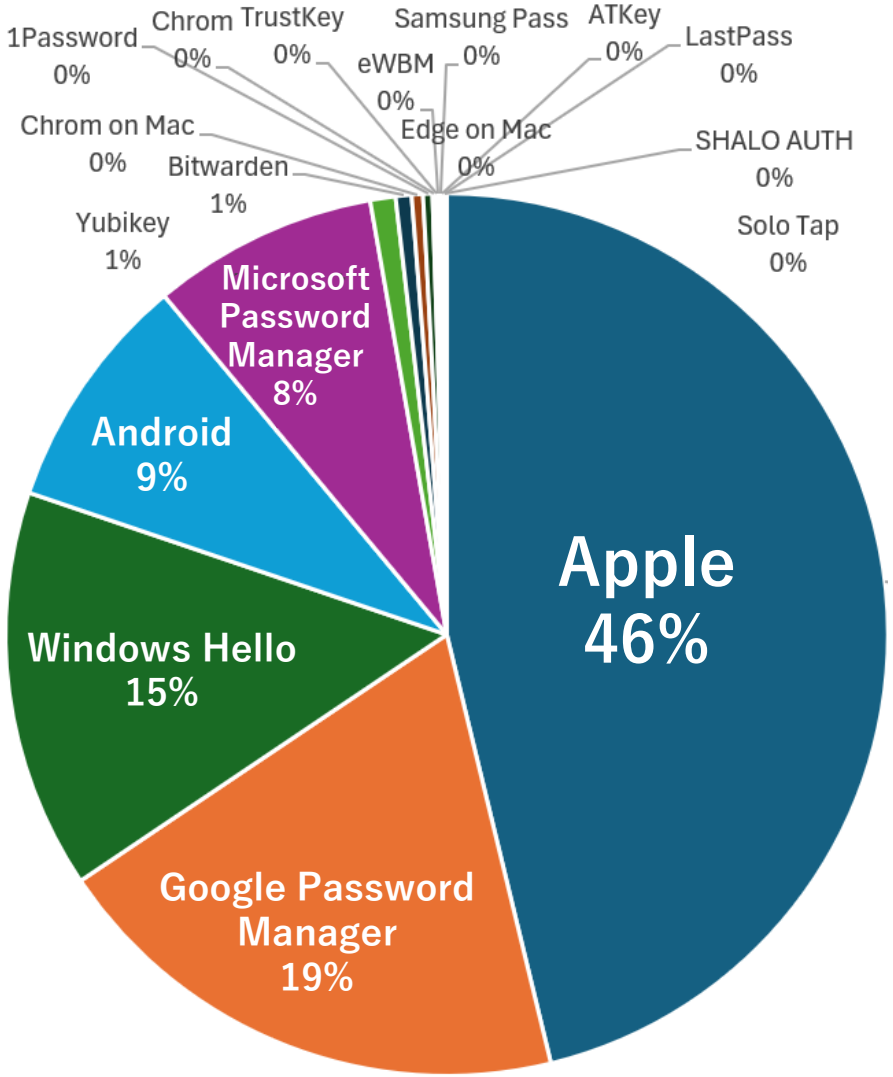


✅ 同一Passkeyを複数デバイスで利用可能
スマートフォン紛失時も容易に復元できる

⚠ 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



パスキー(WebAuthn)のメリット

- これまで：機関ごとに導入する認証方式を検討し実装する時代
  - 様々な多要素認証方式の優劣の検討
  - 独自システムの維持と新方式への対応
  - 独自のユーザサポートとそのコスト

AaaS: Authentication as a Service

- これから：WebAuthn統一APIによる認証機能の切り出し
  - 認証機能の実装は認証サービスプロバイダーに依存
    - 新方式対応コストの低減
    - ユーザサポートコストの低減？

  - BYODを含む端末管理に対するガバナンスがより重要に
    - 特に同期パスキーの場合、同期するすべての端末の管理が必須（AAL3では不可）
      - とはいえ、メールOTP（個人メール利用）やOTP認証器（複製可能）と同様

身元確認（IAL）の必要性

- 昔は、多くの関係は対面（オフライン）で構築されてきた
- 大学等の教育機関では、継続的な関係の中で教育サービスが提供され、その中で相互の信頼関係が構築される（原則）

そうは言っても、

- 短期的な関係、オンラインのみの関係も急速に増加
- 不正（なりすまし）の手口も巧妙化
- 機微情報のオンラインでの取り扱いの増加

厳格な身元確認が求められる状況の例

- 先端技術・安全保障輸出管理へのアクセス
- 臨床研究および電子カルテの参照
- 遺伝子組み換え・動物実験等の倫理審査申請
- 高価・特殊な研究施設の利用と機器操作
- 競争的研究資金の管理・執行権限
- 知的財産・特許申請プロセスへの関与
- 情報セキュリティ委員会や法務監査への参画
- 学内キャッシュレス決済・ICカードへの職能付与
- 卒業生への証明書オンライン発行サービス

「ユーザ」の多様性

- 名誉教授
- 客員教員、客員研究員
- 非常勤講師
- 派遣職員
- 入学予定者
- 保護者
- 高大連携
- 科目等履修生
- 短期留学生
- 研究生（非正規）
- 実験協力者
- 入居スタートアップ・ベンチャー関係者
- リカレント教育・公開講座などの受講者
- 寄付者
- 委託業者
- 卒業生・同窓生

など

身分ごとに身元確認の方法（有無）が異なる

犯罪収益移転防止法（犯収法）の改正

- アナログな本人確認書類の限界
  - 特殊詐欺の携帯電話契約で、運転免許証による本人確認の７割が偽造

- 非対面での「本人確認書類の画像情報の送信を受ける方法」や「本人確認書類の写しの送付を受ける方法」の廃止（2025年6月施行）

- 対面・非対面にかかわらず、マイナンバーカードによる公的個人認証、ICチップの利用へ

マイナンバーカードでの身元確認

- マイナンバーカード（2016～）の普及
- 主務大臣認定事業者（PF事業者）による公的個人認証サービスに加えて、デジタル認証アプリ（デジタル庁）の提供
- 東大でのアカウントリカバリーでの利用例↓

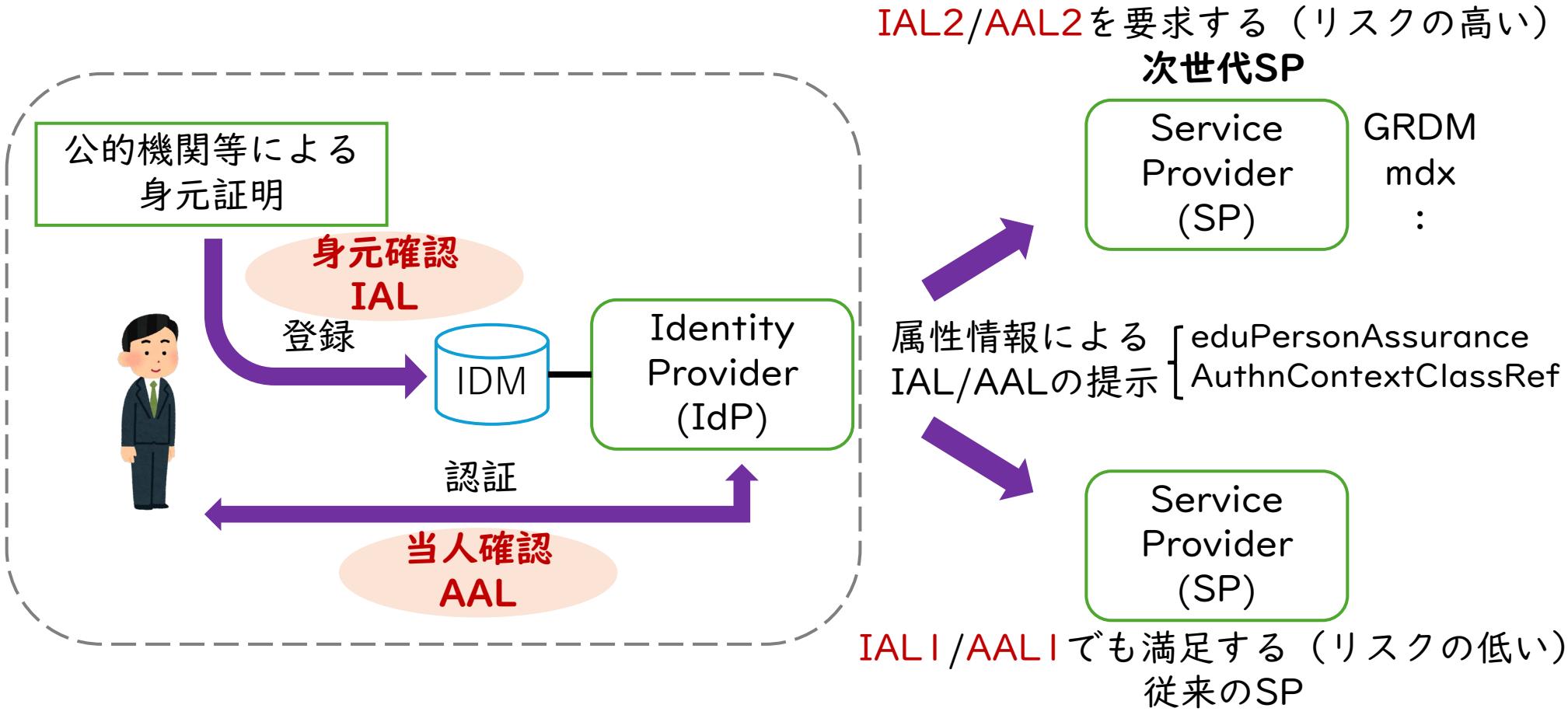
（パスワード忘れ対応）

様々な保証レベル

- NIST SP800-63による国際的な指標（第4版/2025）
  - NIST:米国国立標準技術研究所が発行するガイドライン

- AAL (Authentication Assurance Level)
  - 当人確認の強度：AAL1-単要素、AAL2-多要素　（ざっくりとした説明）
- IAL (Identity Assurance Level)
  - 身元確認の強度：IAL1-自己申告、IAL2-根拠の確認
- FAL (Federation Assurance Level)
  - 認証連携の強度：FAL1-署名のみ、FAL2-暗号化・事前合意、FAL3-Holder Binding (VC)対応

認証連携における
身元確認(IAL)と当人確認(AAL)



IAL（身元確認）とAAL（当人確認）の連携

- 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（多要素認証導入時の検討事項）
  - 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

→BAL (Binding Assurance Level) by Sakimura

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

新入生アカウント発行フロー（例）

1. 受験出願
   - 生年月日、連絡用メールアドレスの登録
   - インターネット出願番号、受験番号の取得

2. 合格通知
   - アカウント取得方法を郵送

3. ID発行サイト
   - インターネット出願番号、受験番号、生年月日を入力
   - ログインID（学生番号とは異なる）を表示

4. 連絡用メールアドレス（非表示）に有効化キーを送付

5. 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

6. 続けて多要素認証を設定
   - 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
   - 多要素認証の設定が完了すると有効化キーは無効化

パスワードのみでログインできる瞬間を作らない

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？

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）

Web 2.0からWeb 3.0へ
情報の信頼と制御のパラダイムシフト

	Web 2.0： 組織による一括証明	Web 3.0： 個人による自律的証明
署名主体と権限	組織主導 プラットフォームが発行・署名 （「証明してもらう」立場）	個人主導 組織署名 ＋ 個人の署名 （「自ら証明する」立場）
制御の粒度	一括・ファイル単位 文書（PDF等）を丸ごと提示 （不要な情報の散在）	個別・属性単位 必要なデータ項目のみ提示検証 （選択的開示）
信頼の性質	組織の静的な信頼 発行元の組織を信頼	個人を含めた動的な信頼 本人の意思による提示と検証
技術モデル	フェデレーション	ウォレット（IHVモデル）

IAL（組織による身元保証）　AAL（当人自身による保証）

ハイブリッドによるプラットフォームに収束？

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）

VC事例

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

- 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

(Open Badges 2.0 / VCでない)

- オンライン検証
- 限定的Holder Binding

似たようなものとして

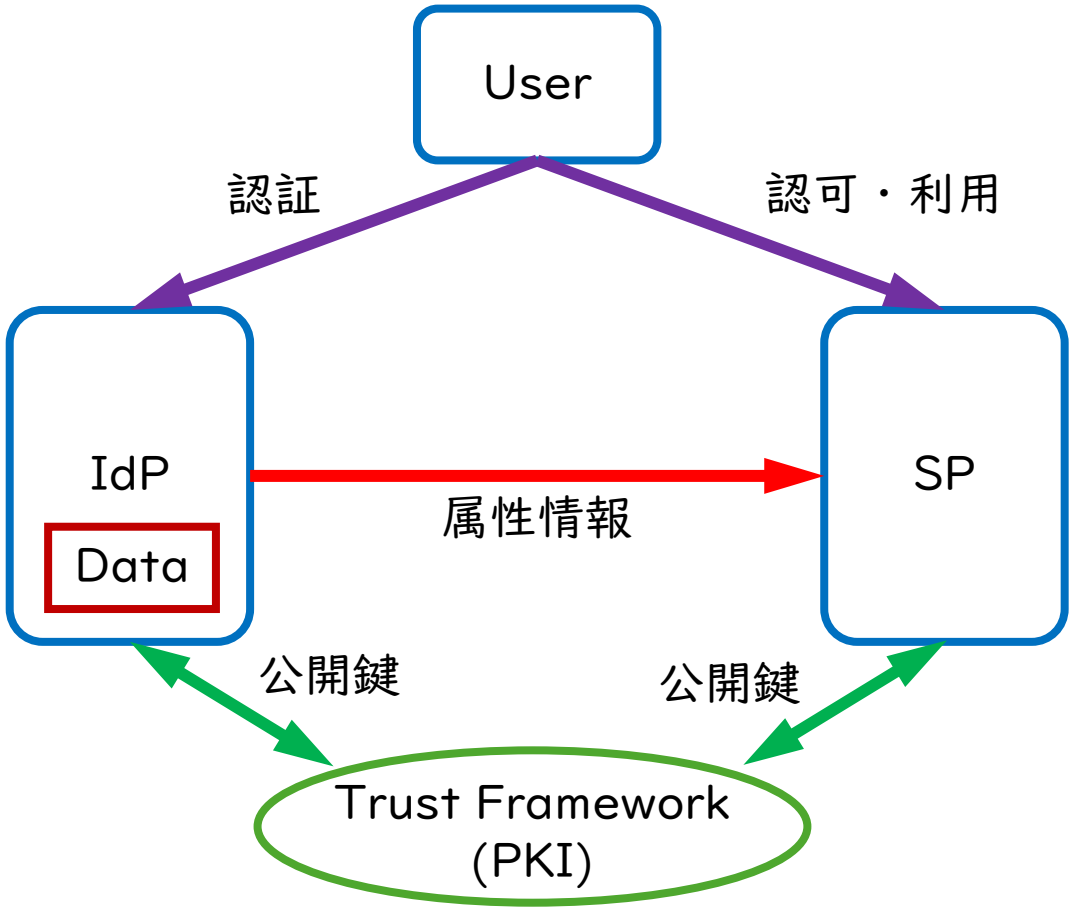
デジタル署名つきPDF

- PDF用署名鍵のトラストリスト
  - AATL (Adobe Approved Trust List)、EUTL (European Union Trust List)
- 署名サービス
  - DocuSign、クラウドサイン、Adobe Sign（署名代行＋証跡管理）
- 機械可読情報付加の検討
  - XMLやVCの埋め込み
- 住民票の（署名なし）PDF交付に対する議論
  - デジタル技術を活用した効率的・効果的な住民基本台帳事務等のあり方に関するワーキンググループ中間とりまとめ（2025/6/30）
    - https://www.soumu.go.jp/main_content/001018670.pdf
  - 容易に複製でき、原本との区別が困難
  - 複製を防止する安価な方法がない
  - 本人確認書類として利用され、なりすまし契約される
    - そもそも本人確認書類としての利用が想定されていない?
    - 犯罪収益移転防止法では「住民票の原本＋記載住所への転送不要郵便の受け取り」が定義
  - 提出により不必要な個人情報が提供されてしまう

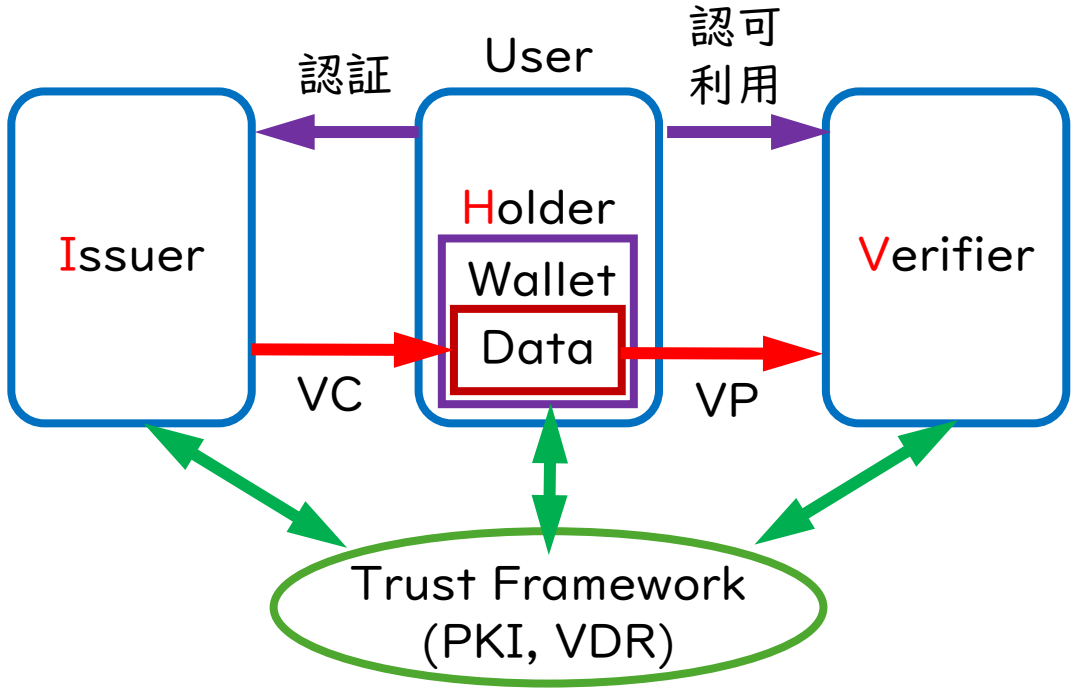
（どちらかというとリテラシー問題？）

フェデレーションモデルとIHVモデル

Federation Model（FAL1/2）



IHV Model（FAL3）

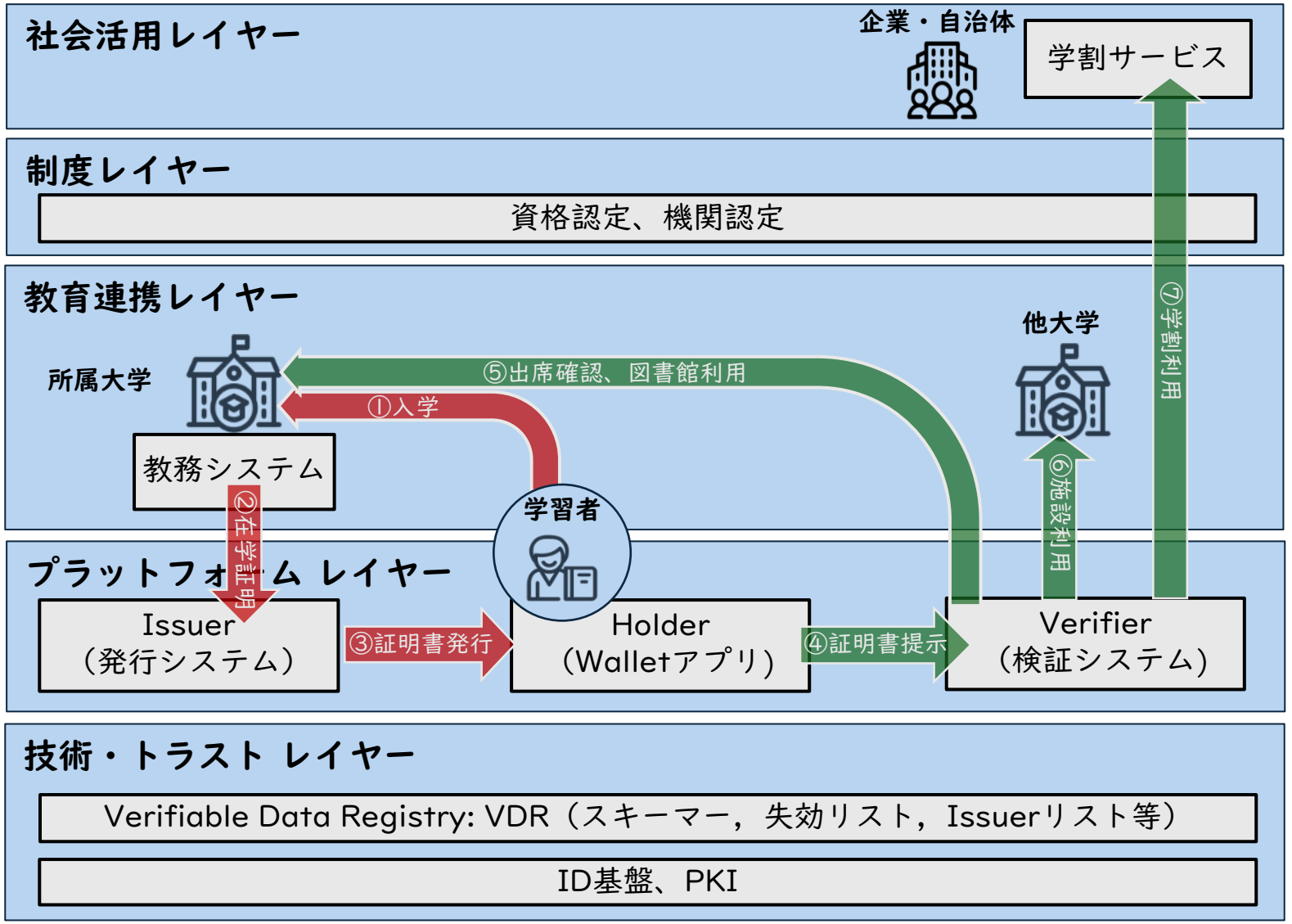


VP: Verifiable Presentation

VDR: Verifiable Data Registry

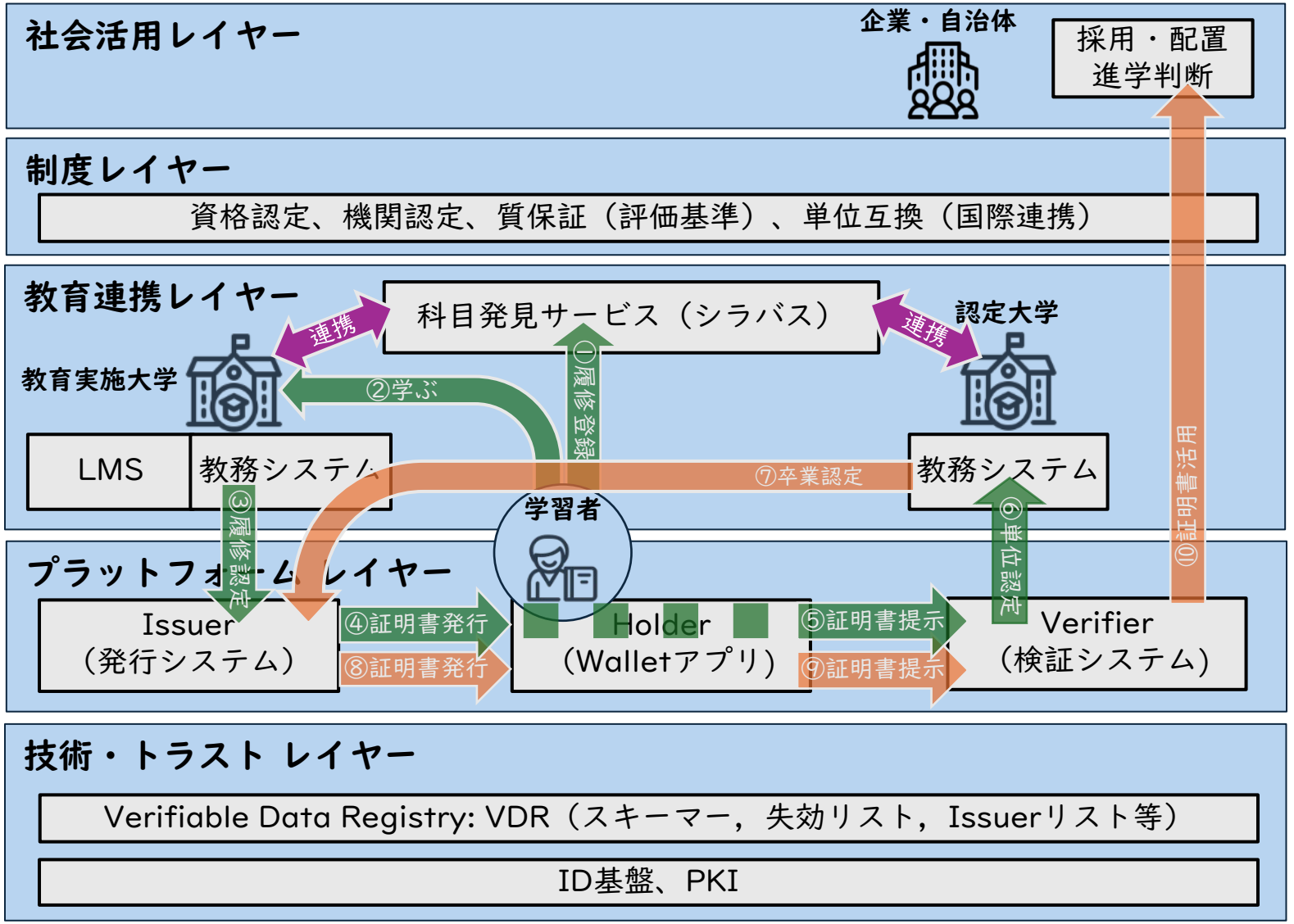
IHV型学術デジタル証明書基盤の事例－１

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

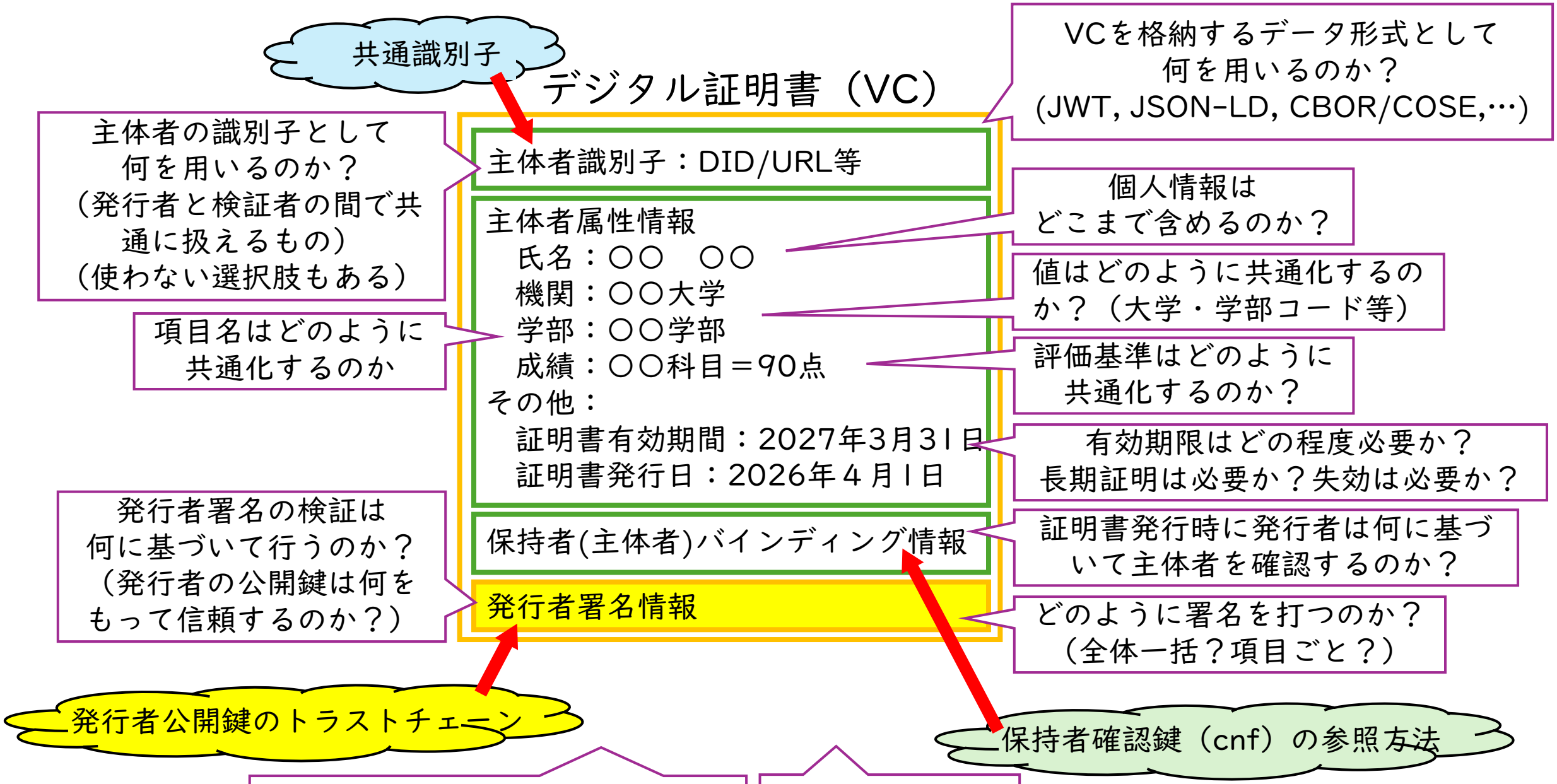
教育連携・成績証明・社会接続（就職・人材配置）を同一基盤で実現



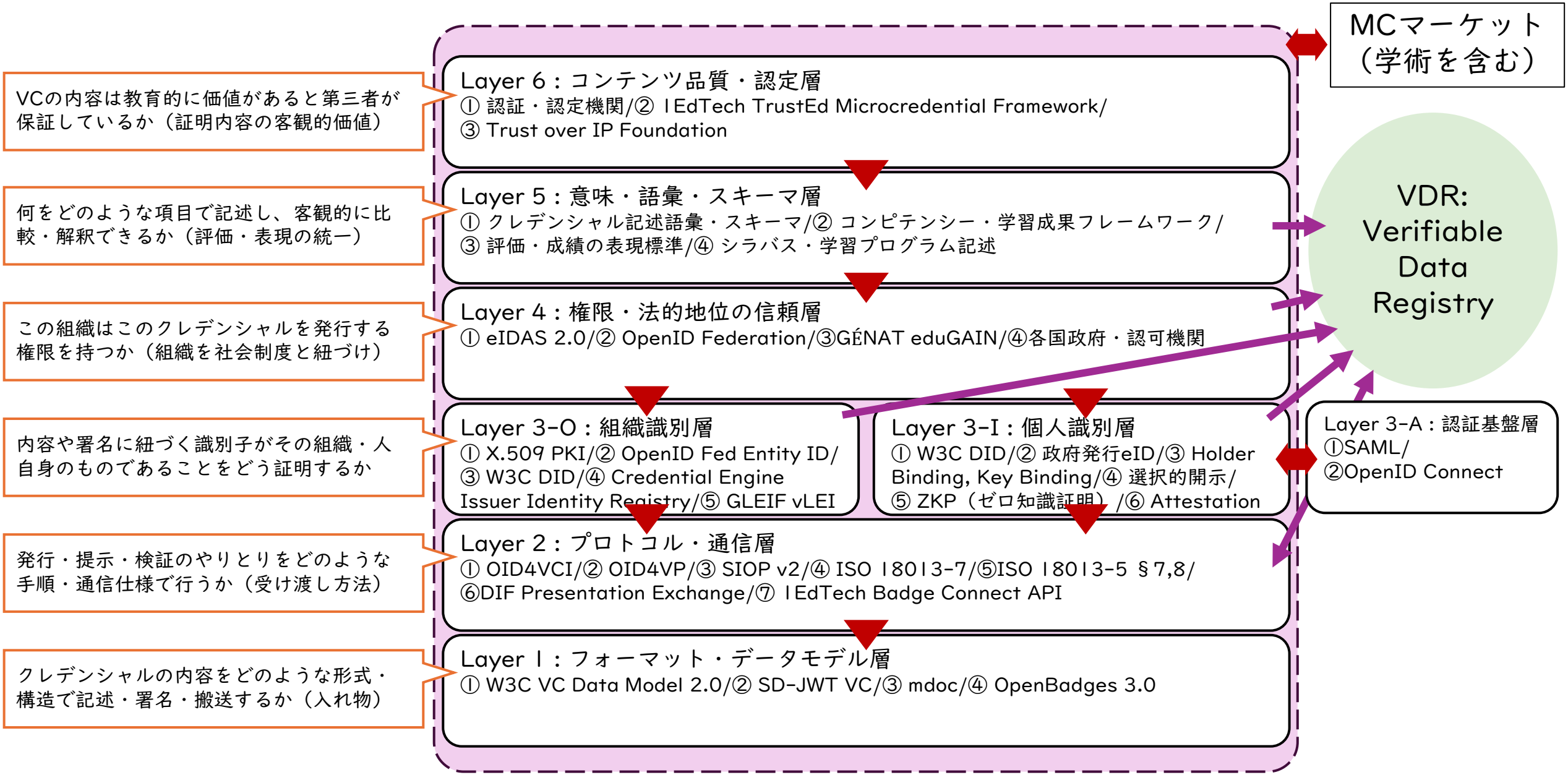
学術デジタル証明書の２つの用途

- 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


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）

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
  - FCF Campus Card（フェリカカード）が国内では主流
- 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

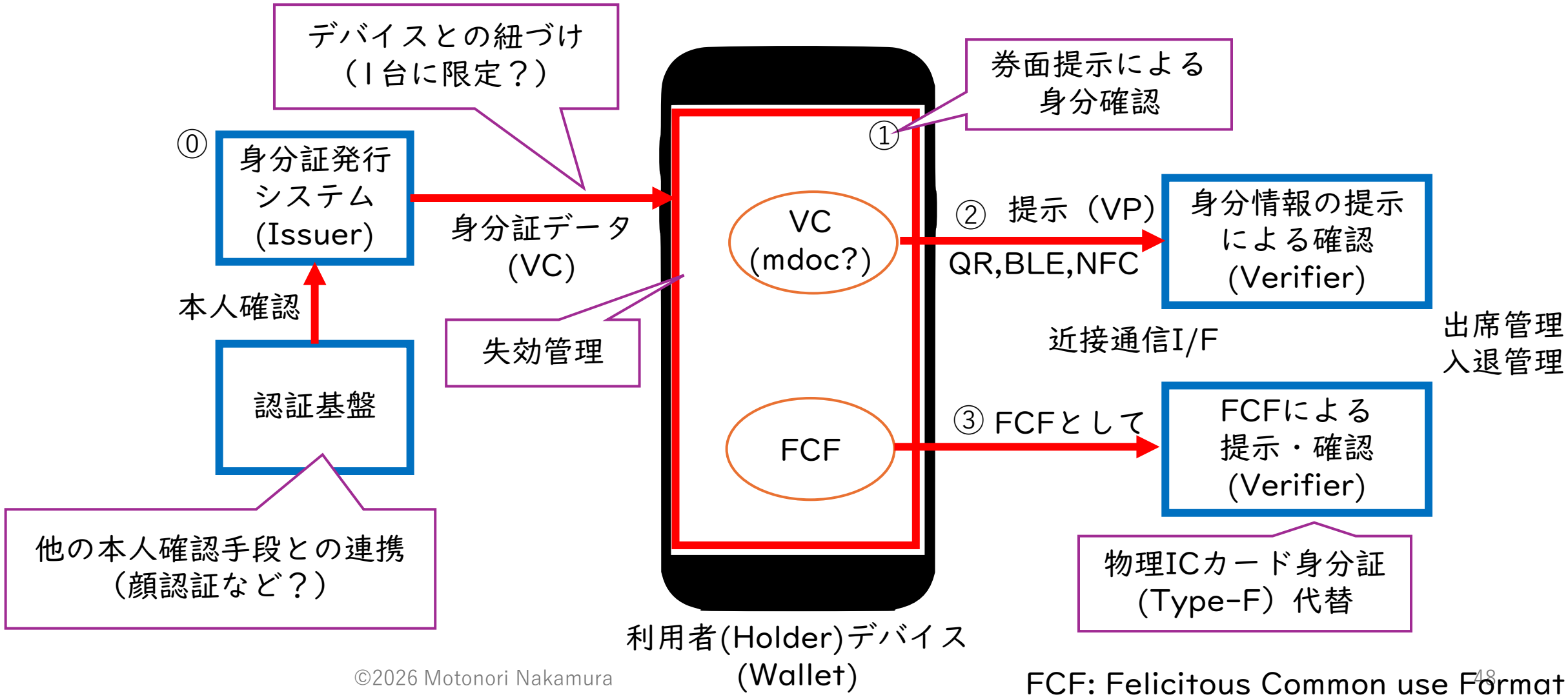
- オンラインサービスの高度化と並行して、物理媒体による身分証の高度化についても検討が必要
  - スマートフォン等の高度化したデジタル端末の普及
  - 発行・配付コストの削減、入退管理システム等の更新コスト削減

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、定期試験時の机上提示

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（学生証）エコシステム実現に向けた整理

技術標準層　（グローバルなデータ形式・署名技術の標準・基盤 / 相互運用）

- W3C VC
  検証可能な資格情報
- ISO/IEC 18013-5
  mdoc / mDL の応用
- Open Badges 3.0
  マイクロクレデンシャル標準

制度・ウォレット層　（地域・国ごとのデジタルIDウォレットと制度実装 / 信頼の提供）－ 海外事例

- EU:EUDI Wallet
  eIDAS 2.0規則準拠
  全加盟国に展開（2026）
- 欧州学生証（ESC）
  Erasmus+ESCI
- 各国の取り組み
  US: mDL拡大
  AU: Digital ID Act
  IN: Aadhaar+VC

利用・サービス層　（学生等が実際に身分証を利用する場面）

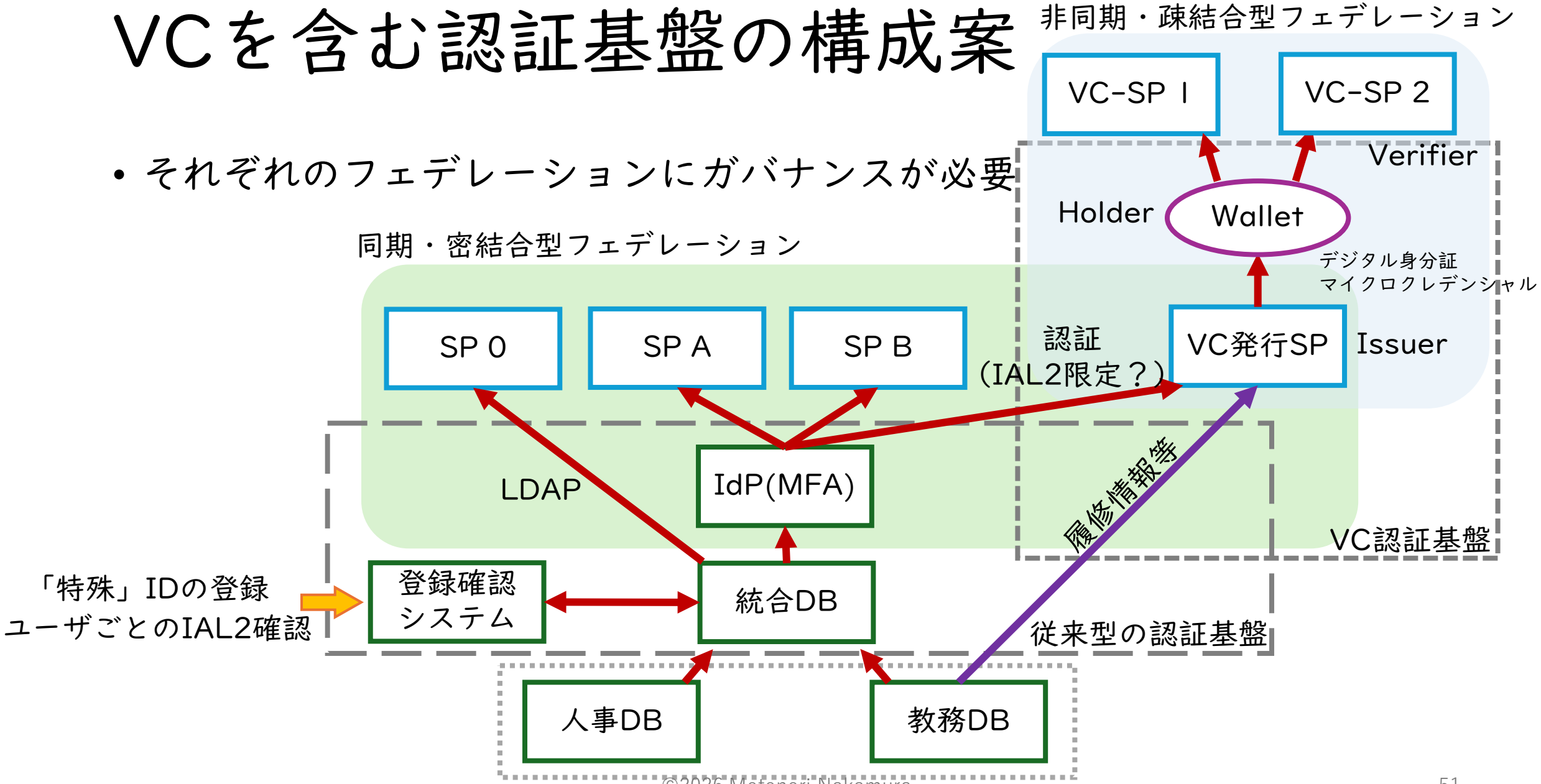
学内認証	**学割**	**国際流動性**	**就職・採用**	**生涯学習**
入退室	通学定期	留学・研修	学位証明	マイクロ資格
出欠・図書館	美術館・映画館	単位互換	インターン	スキル証明
期末試験	各種施設		資格証明	学習ポートフォリオ

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

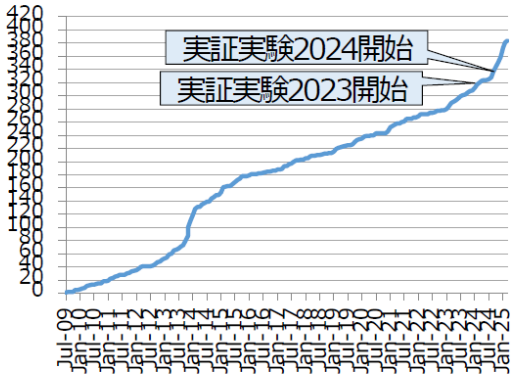


分散（フルメッシュ）型基盤整備の是非

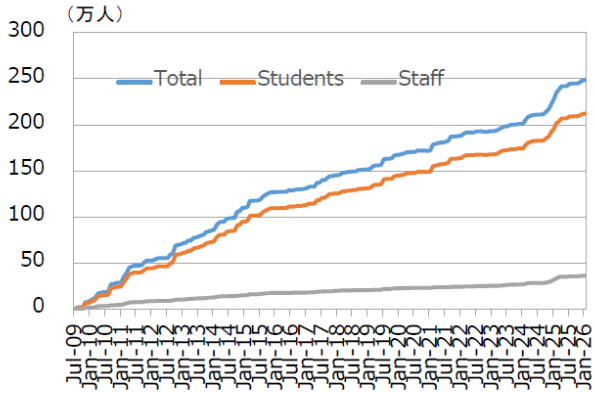
- 各機関の自主的な整備にまかせていて良いか？
  - 大学数規模などから米国の学術フェデレーションをモデルに構築
  - 小規模機関における導入の困難さ
  - 同じことをVCでも繰り返す？
  - 欧州のeduIDが参考になるか？

学認参加状況　（2026年1月末時点）

IdP機関数：398



ユーザ数（推計）：249万



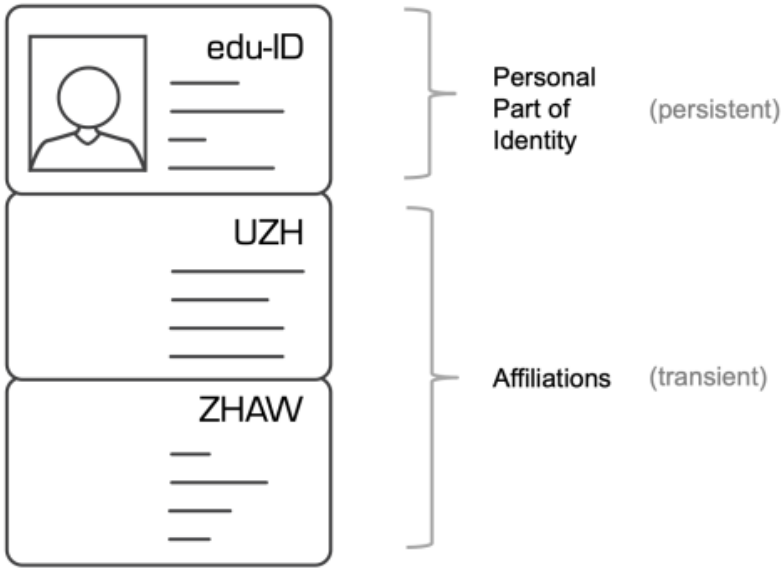
（IdP機関内訳）

	国立大学	公立大学	私立大学	短期大学	高等専門学校	大学共同利用機関	その他
学認利用数	85	45	180	12	53	7	31
総数	85	103	624	292	58		
カバー率	100%	44%	29%	4%	91%		

※ 1機関で複数校カバーするものがあるため合計はグラフと一致しない

eduID

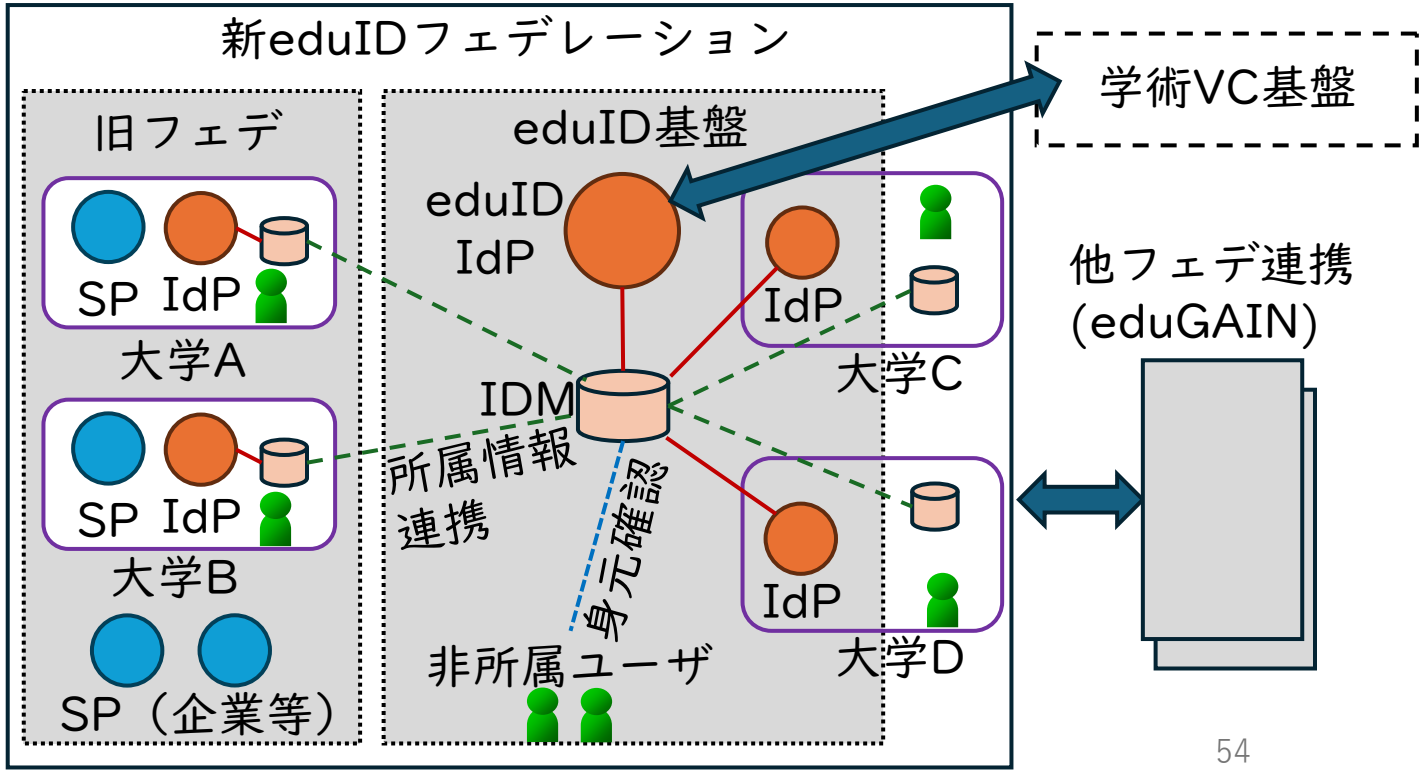
- 教育機関の枠を超えて個人に付与される永続的識別子
  - スイスやオランダ等においてeduIDとして基盤を構築・運用
  - 欧州学生ID（ESI）とリンク
- 特徴
  - 卒業後も維持される
    - 同窓会活動にも寄与する？
  - 本人管理のID＋機関から付与される属性
    - 国内や欧州域内等で有効な識別子として利用
  - VC/マイクロクレデンシャルと親和性が高い
    - というか、VC基盤の構築において重要



Source: https://help.switch.ch/eduid/docs/unis/architecture/

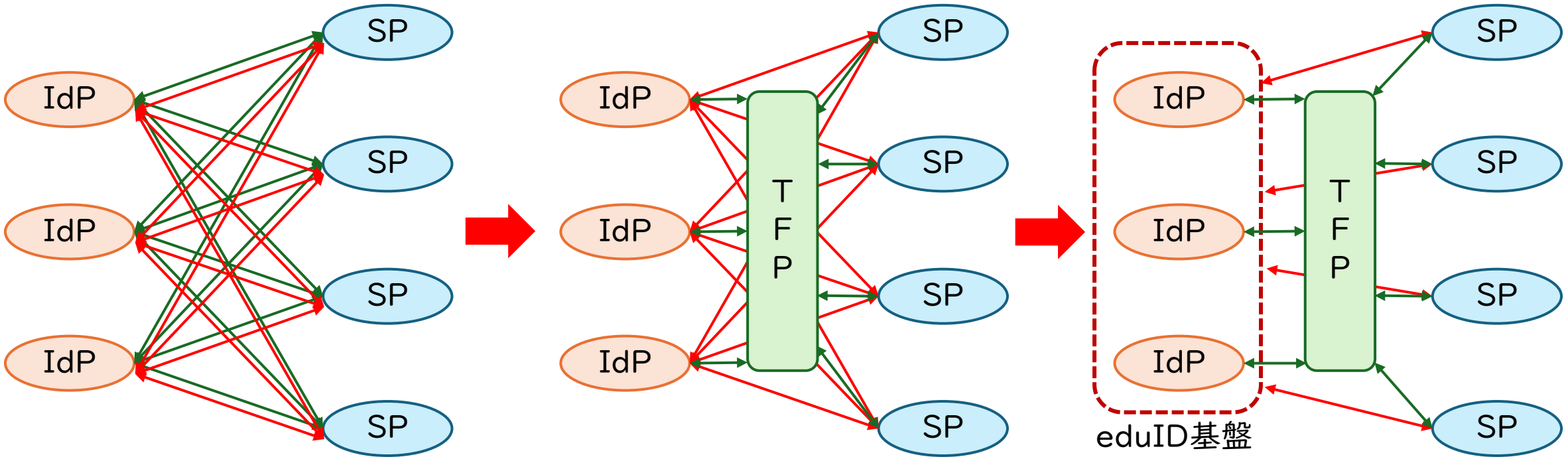
学認eduIDという方向性

- 教育機関の枠を超えて個人に付与される永続的識別子とその認証基盤
  - 統合IdPシステムと分散管理によるコスト削減、機関参加率向上
  - 大学ごとの学外者アカウント管理の省力化
  - SP連携管理のコスト削減
  - SP参入コストの削減
  - 永続的なVC実現の基盤
  - VC規格の変遷への効率的な対応



さらなる集約による効率化効果の向上

- ポリシーの集約だけでなく、運用コストの集約の可能性を模索



TFP: Trust Framework Provider

さらなる将来への認証の課題（キーワード）

- AIエージェントによる代理アクセスに対する権限管理
  - 複数AIエージェントの連鎖（分担）関係における再委任なども
- コンテンツの来歴証明
  - C2PA（Coalition for Content Provenance and Authenticity)
  - Originator Profile: 発信者の意図の表明と確認による信頼の構築
  - W3C Verifiable Credentials for Documents
- システム間のトラスト
  - IoT、クラウド、マイクロサービスにおけるシステム間認証
  - Attestation（端末来歴管理）
  - Signals（認証後の継続的なリスク評価：リスクベース認証の高度化）

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時の脆弱性（BAL）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）の整理
  - コスパの良いプラットフォームの在り方（eduID）

質問用QRコード
ED-S8

【予告】デジタルクレデンシャル円卓会議2026（参加無料）
2026/07/15(水) 14:00 ～ 19:30、一ツ橋講堂 中会議場（東京都千代田区）
https://openid.connpass.com/event/393175/