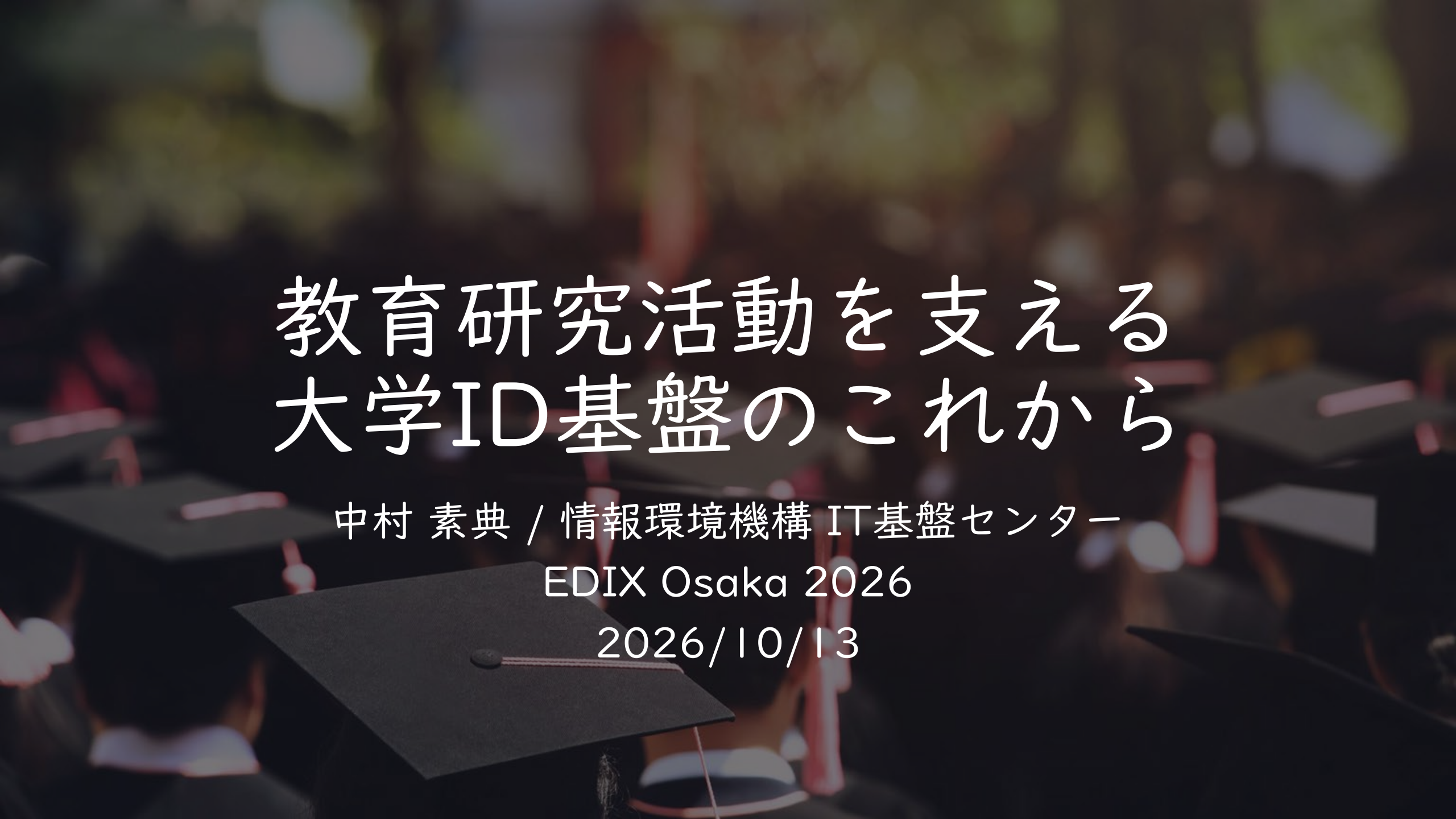


教育研究活動を支える大学ID基盤のこれから

中村 素典 / 情報環境機構 IT基盤センター

EDIX Osaka 2026

2026/10/13

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

©2026 Motonori Nakamura

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
   - **同期パスキーの普及とその管理**

2. VC (Verifiable Credential) の時代へ
   - 円卓会議・パブコメを経た整理
   - **大学として今から何を準備しておくべきか**

©2026 Motonori Nakamura

京都大学で扱う「ユーザ」

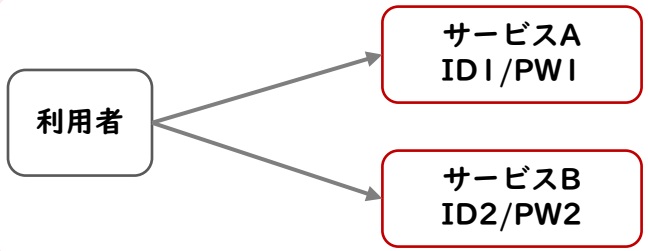
- 常勤教職員　　約7,500名
- 非常勤教職員　　約4,400名
  - うち附属病院所属　　約3,500名

- 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

©2026 Motonori Nakamura

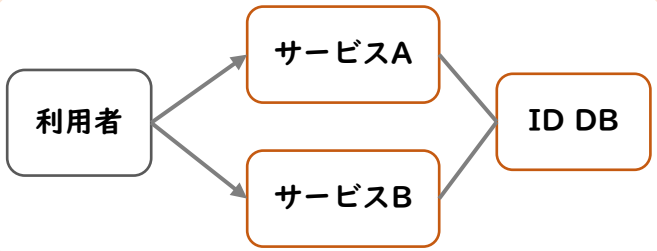
認証基盤の変遷

① 独立管理
～1990年代前半



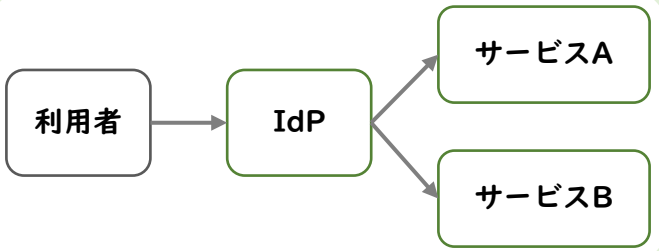
- サービスごとにIDを発行
- サービスごとに異なるパスワード

② ID統合
～2000年代前半



- ID・パスワードを統一（LDAP等）
- パスワードは各サービスに直接渡る → 漏洩・使い回しの危険

③ SSO
2000年代後半～



- IdPに認証を集約、パスワードはサービスに渡らない
- **クラウドサービス時代**の要請：多数のサービスを同じIDで
- 学認（2009～）、多要素認証の導入も容易
- IdP自体もクラウド（IDaaS）で選べる時代に

SSOで認証を一か所に集めていたことが、多要素認証・パスキーへの移行を容易にした

©2026 Motonori Nakamura

大学アカウントは今も「踏み台」に

2026年も相次ぐ報道（6～9月だけで複数大学）

- フィッシング等でIDとパスワードが盗まれ、海外からログイン
- 迷惑メールの大量送信：**1件の事案で1万7千通超**の例も
- メールボックスの閲覧による個人情報漏えいの可能性 → 個人情報保護委員会・文部科学省へ報告
- 学生・卒業生・教職員のいずれも被害に（卒業後も残るアカウントも狙われる）
- 事後に「学外からのログインに多要素認証を必須化」する例も

それでも多要素認証の必須化が進まなかった理由

- 方式の選択肢が多い：SMS・メールによるOTP（One-Time Password）、TOTP（時刻ベースのOTP）、プッシュ通知…優劣の検討から
  - TOTPはGoogle Authenticatorが主流に。スマホがなくてもブラウザ拡張で使えるが、移行・バックアップなど**利用者による扱いが難しい**
- 大学ごとに独自のシステムを構築・維持
- 利用者が多様で入れ替わりが多い：毎年の新入生、非常勤、卒業生
- 登録・機種変更・紛失時のユーザサポート

出典：Security NEXT 等の報道（2026年6～9月）をもとに一般化

多要素認証は急務。求められるのは、導入・運用コストの低い方式

©2026 Motonori Nakamura

本学の多要素認証とパスキーの導入

FIDO Alliance設立（2012）→ FIDO2/WebAuthn がW3C標準に（2018）→ マルチデバイス対応の「パスキー」（2022）

2020　教職員向けMFA

- 対象：Google Workspace、財務会計、出張旅費、就業管理、Zoom
- PW＋（TOTP／メールOTP／パスキー）
- まずはTOTP（Google Authenticator）を設定してもらう
- 導入当初からFIDOにも対応

2024　学生向けMFA

- 対象：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）
- まずはメールOTP（リカバリーにも使用）、次にTOTP
- パスキーに本格対応（Windows Helloの不具合解消、Appleの同期パスキー）

2025～　パスキーが本命に

- Googleの同期パスキーも利用可能に（2025秋頃）
- OTPによるMFAでもフィッシング被害
- 証券口座の不正取引が数千億円規模に → 警察庁・金融庁がパスキーの普及を推進

OTPでは防げないフィッシングへの答えとして、パスキーへ

©2026 Motonori Nakamura

パスキーはフィッシングに強い

攻撃の手口	パスワード	OTP（SMS・TOTP等）	パスキー
偽サイトに誘導して入力させる	盗まれる	盗まれる	**偽サイトには応答しない**
偽サイトが本物にリアルタイム中継（AiTM）	突破される	突破される	**突破されない**（接続先に紐づく署名）
盗んだ情報を後で使う	使える	短時間なら使える	使えない（秘密鍵は送られない）
サーバからの情報漏えい	パスワード（ハッシュ）	OTPの生成シード	公開鍵のみ（悪用できない）

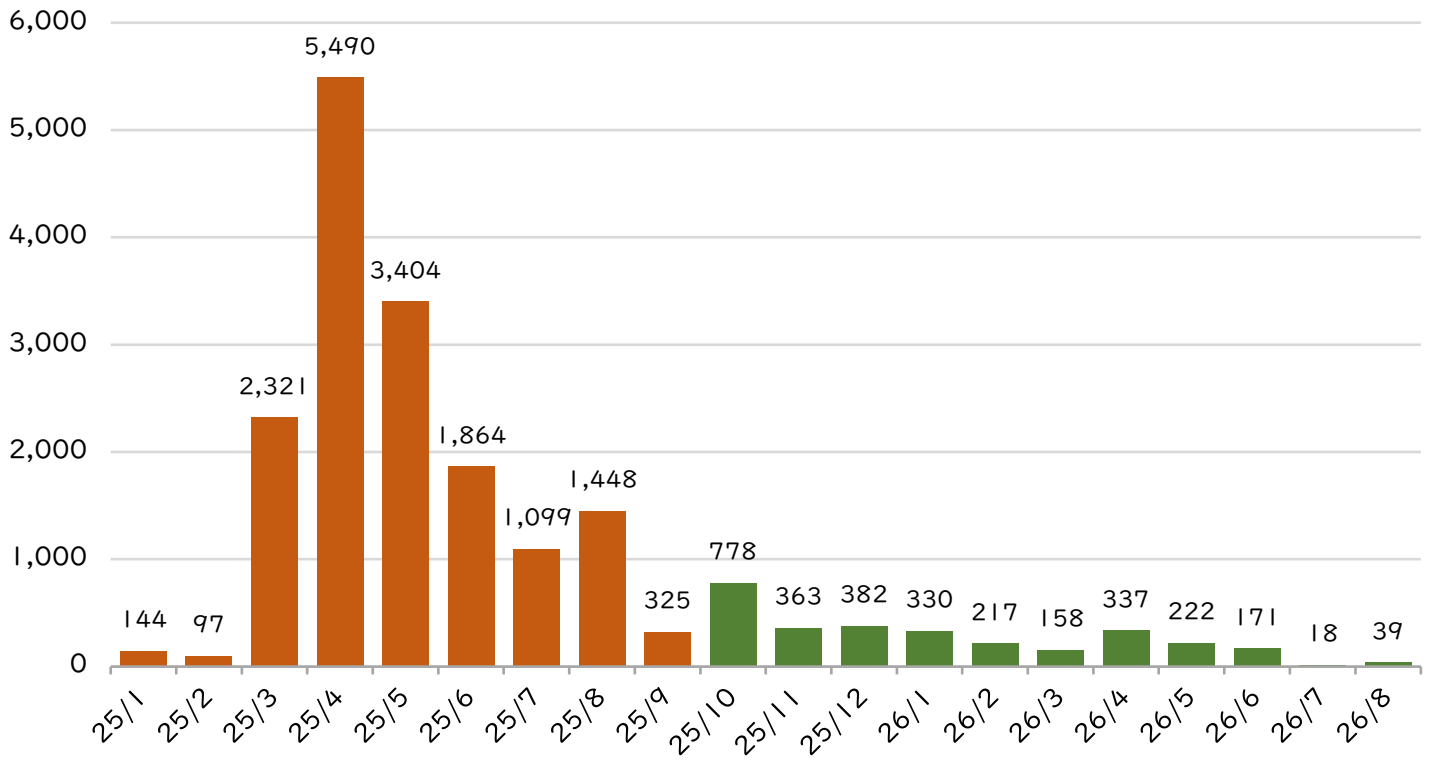
- 証券口座の事案では、OTPによる多要素認証の必須化後も被害が続いた（リアルタイムフィッシングでOTPを中継）
- NIST SP800-63B-4：AAL2でフィッシング耐性のある選択肢の提供を求め、AAL3では必須

利用者の注意力に頼らず、仕組みでフィッシングを防ぐ

©2026 Motonori Nakamura

証券口座乗っ取りとパスキー

不正アクセス件数の推移（月別、発生日ベース）



緑：主要証券会社がパスキーの提供を始めた2025年10月以降

出典：金融庁「インターネット取引サービスでの不正アクセス・不正取引の被害状況」（2026/9/9更新）

約7,400億円

2025年の不正な売買金額（売却＋買付）

5,490件 → 39件

月間の不正アクセス件数（2025/4 → 2026/8）

業界の対応

- 日本証券業協会がログイン時等の「フィッシング耐性のある多要素認証」を必須化（2025年7月に改正案公表）
- 各社がパスキーを導入し、順次必須化
- 楽天証券：利用者の約7割がパスキーを利用、2026年6月から段階的に必須化

©2026 Motonori Nakamura

パスキーは「使いやすさ」でも優位

FIDO Passkey Index（2025年10月、Google・Microsoft・LINEヤフー・NTTドコモ等9社）

93% vs 63%
サインイン成功率（パスキー vs その他）

8.5秒 vs 31.2秒
サインインにかかる時間（73%短縮）

81%減
ログイン関連のヘルプデスク対応

Microsoft（個人向けMicrosoftアカウント 数億人規模の実績）

99%
登録の成功率

95% vs 30%
サインイン成功率（対 従来方式）

3秒 vs 69秒
約14倍速い（対 パスワード＋MFA）

安全性と利便性を両立できる数少ない認証手段 → 利用者サポートの負担も軽くなる

©2026 Motonori Nakamura

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 ～

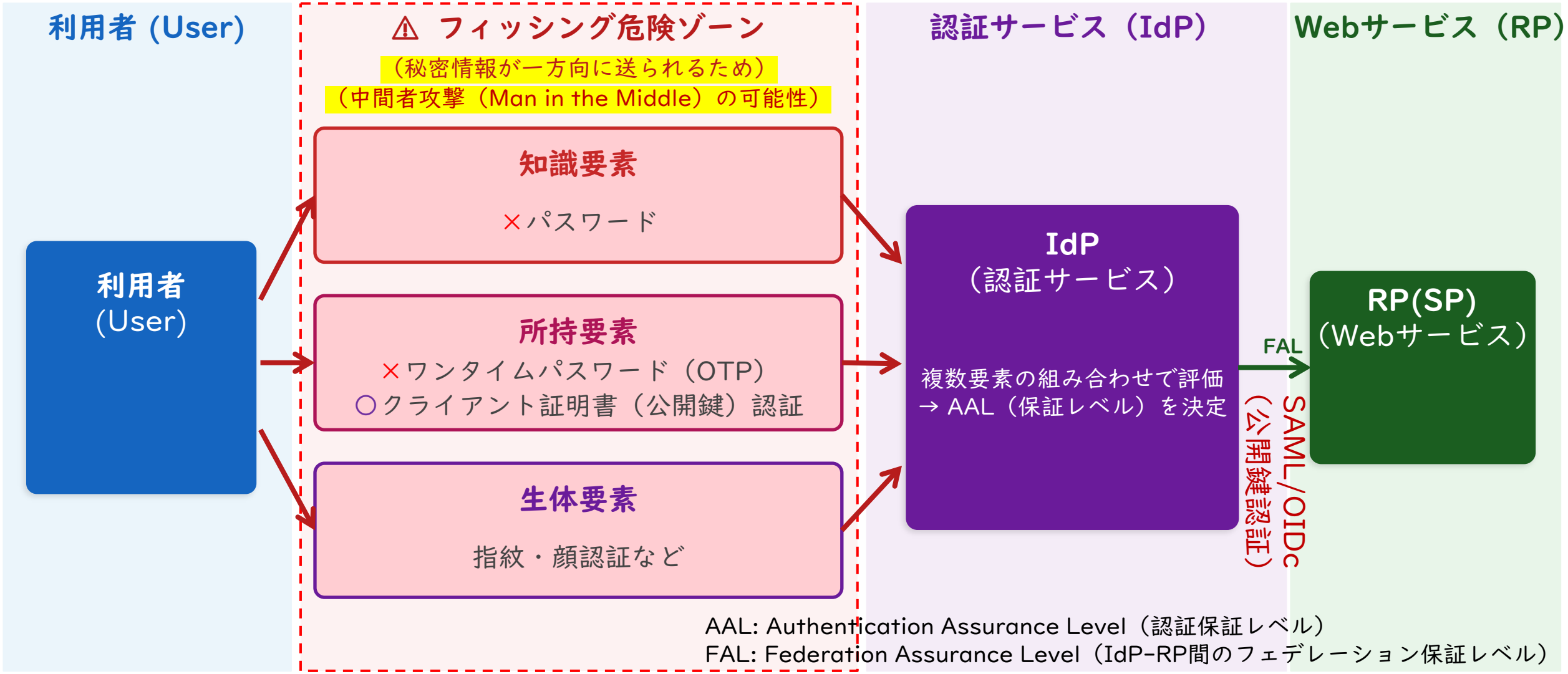
「ユーザが秘密情報をサーバに送る」時代から「デバイスが署名する」時代へ

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。



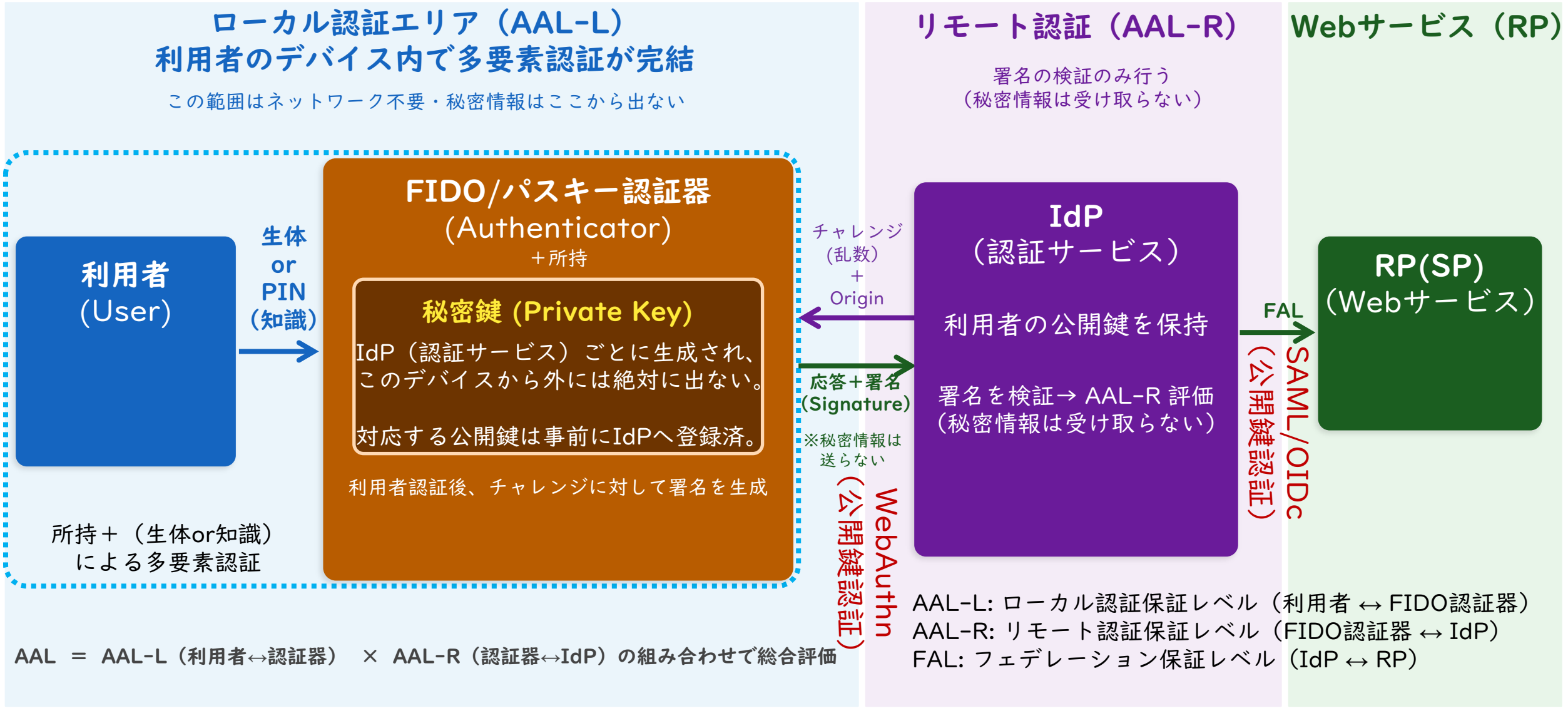
©2026 Motonori Nakamura

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



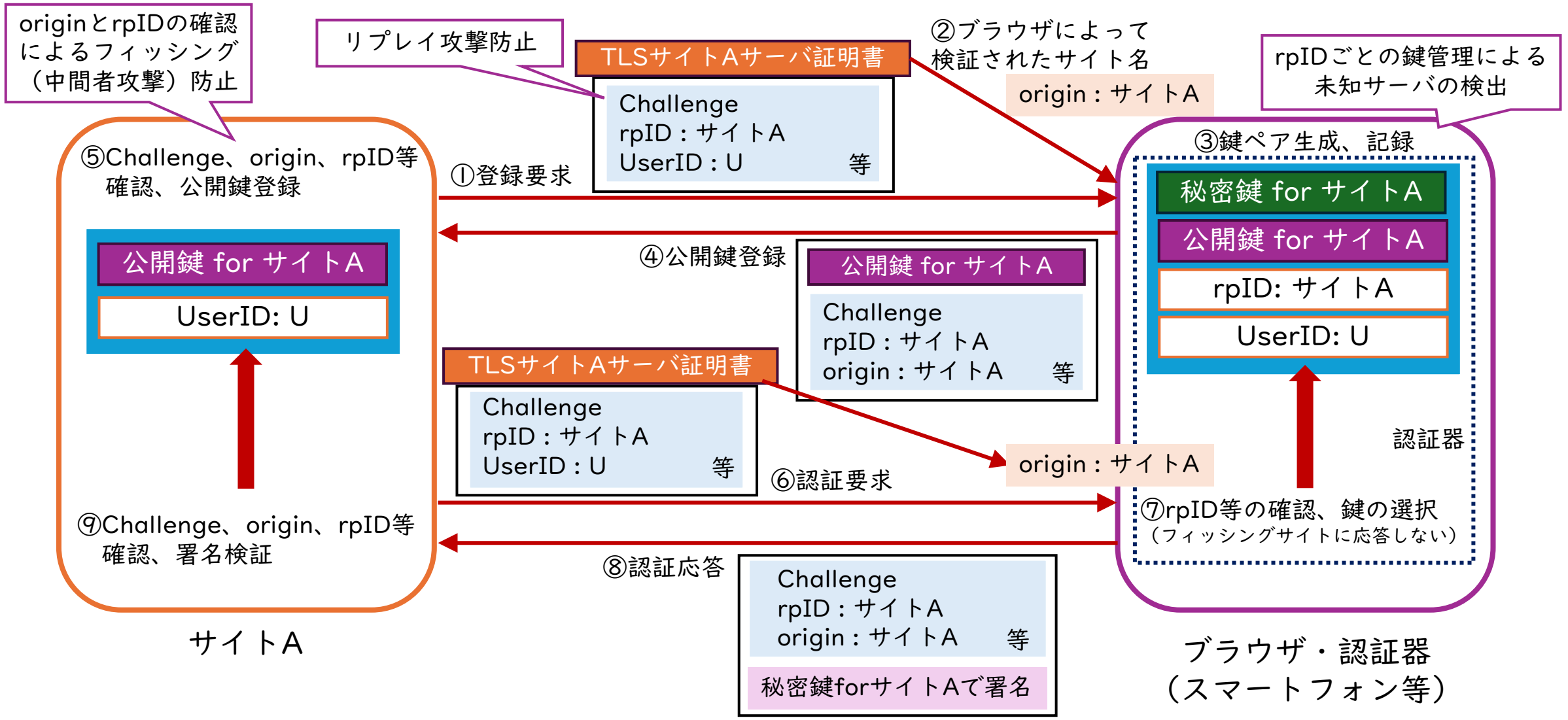
⚠ 課題：パスワード・OTP などの「秘密情報」が毎回ネットワークを経由してサーバに一方的に送られる仕組みであるため、
攻撃者が偽サイト（フィッシングサイト）を用意してユーザを誘導するだけで情報を盗める。
中間者攻撃に強い「クライアント証明書認証方式」は以前から選択肢にあったが、証明書を利用者が安全に管理する手段が確立されておらず普及しなかった。

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



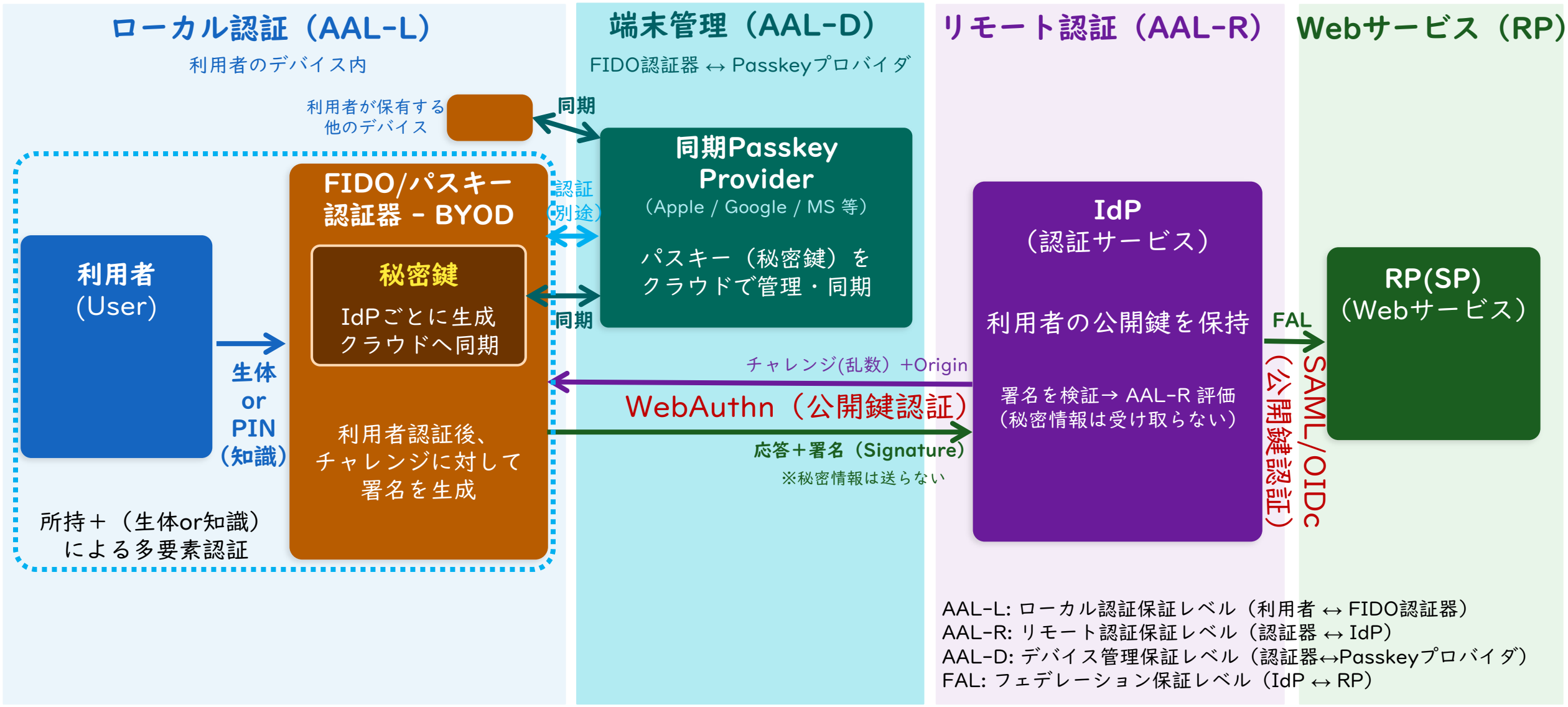
✅ ポイント：秘密鍵はFIDO認証器の外に出ない。接続先情報（Origin）を署名に封印したチャレンジ・レスポンス方式。
偽サイトへ誘導されても、チャレンジは偽サイトのオリジンに紐付くため攻撃者は正規サイトへの署名が得られない（フィッシング耐性の本質）。

（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

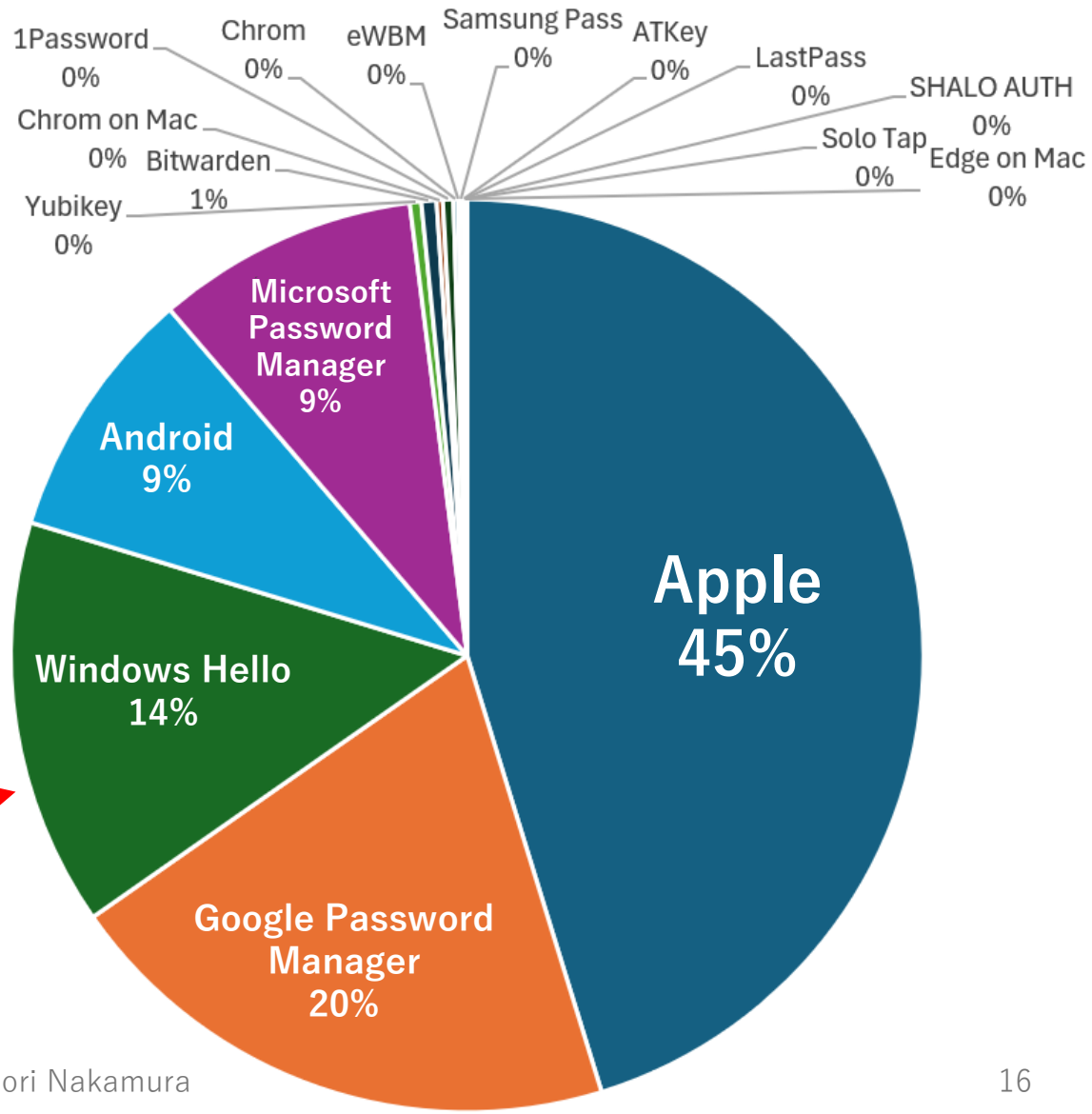


✅ 同一Passkeyを複数デバイスで利用可能
スマートフォン紛失時も容易に復元できる

⚠ 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10月5日時点の利用状況
  - 登録者数：3647
    - 認証器登録数
      - 1台 – 2308人
      - 2台 – 1013人
      - 3台 – 250人
      - 4台 – 58人
      - 5台 – 13人
      - 6台 – 3人
      - 9台 – 1人
      - 11台 – 1人
  - 登録認証器数：5418
    - AAGUID調べ
      - Authenticator Attestation Global Unique IDentifier



©2026 Motonori Nakamura

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

コスト高

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？

コスト低？

  - 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認証アプリ（複製可能）と同様

©2026 Motonori Nakamura

ユーザサポートの負担はむしろ減る

81%減
ログイン関連のヘルプデスク対応
（FIDO Passkey Index）

約35%減
カスタマーサポートへの問い合わせ
（KDDI）

32%減
パスワード再設定の要求
（Aflac）

大学で問い合わせが多い場面とパスキー

よくある問い合わせ	パスキーでは
パスワード忘れ・再設定	**同期パスキーなら**原則として発生しない（端末固定型は、端末を失うと再登録が必要）
機種変更・紛失時のTOTP再設定	同期パスキーは新しい端末に引き継がれる（Google Authenticatorも2023年から同期に対応。ただし利用者の設定次第）
OTPの入力ミス・時刻ずれ・メール遅延	生体認証・PINで完結

本学の状況
- 多要素化で不便を感じた学生が**自ら登録**
- 4月 2,107人 → 10月 3,647人
- うち約4割弱が2台以上を登録（機種変更・紛失への備えに）

パスキーでも、リカバリーに備えて複数の認証手段を登録しておくことを常識に

出典：FIDO Alliance「Passkey Index」（2025/10）、「世界パスキーの日2025 導入事例」（2025/5）、本学のAAGUID集計

©2026 Motonori Nakamura

つまずきやすい場面と備え

場面	備え
機種変更・端末の紛失	同期パスキーを基本に、複数の認証器の登録を勧める
演習室・共用PC	スマートフォンによるクロスデバイス認証（QRコード、PC側にBluetoothが必要）
スマートフォンを持たない・持ち込めない	パスキーはスマホ以外でも使える：PC（Windows Hello、Mac）やUSB／NFCのセキュリティキー（大学からの貸与・配布も）
保存先の取り違え	大学用プロファイルで登録するよう案内（→ 保存先の分離）
すべての認証手段を失った	本人確認を伴うリカバリー手続き（パスワードだけに戻さない → BAL）

段階的に進める：任意 → 推奨 → 必須。移行期間は既存の方式を併存させる

例：楽天証券は利用率が約7割に達した段階で必須化へ／Berkeley Labは3か月の試行後、部門ごとに展開

サポートの焦点は「日々のログイン」から「登録とリカバリー」へ移る

©2026 Motonori Nakamura

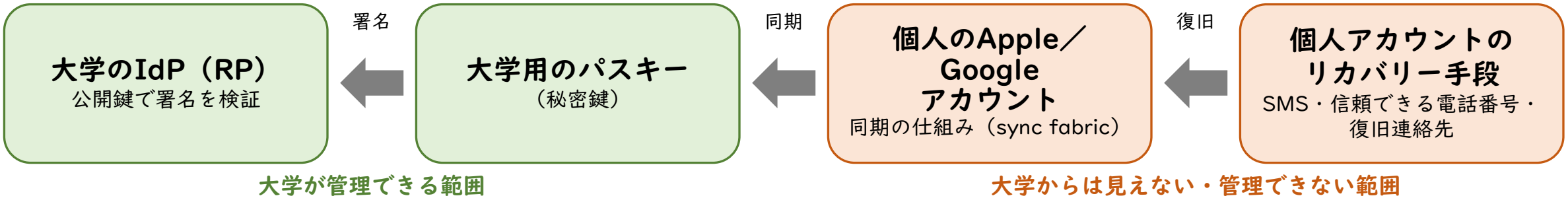
同期パスキーの普及

- 主要プラットフォームが同期パスキーを標準で提供
  - Apple（iCloudキーチェーン）、Google（パスワードマネージャー）、Microsoft（Edge／パスワードマネージャー）、サードパーティ製パスワード管理ツール
  - Microsoft Entra ID：同期パスキーとパスキープロファイルを既定で有効化（2026年3月～順次）
- パスキーの「持ち運び」も標準化へ
  - FIDO Credential Exchange（CXP／CXF）：プロバイダ間でのパスキーの移行
- NIST SP800-63B-4（2025）での位置づけ
  - 同期可能な認証器は**AAL2まで**（鍵のエクスポート不可の要件を満たさず、AAL3は不可）
  - 同期の仕組み（sync fabric）へのアクセスに**AAL2相当の多要素認証**を要求
- 本学でも登録された認証器の大半は同期型（AAGUID調べ）

パスキーは「端末に閉じた鍵」から「アカウントに紐づいて同期される鍵」へ

©2026 Motonori Nakamura

個人アカウントの保護＝組織の保護



- 個人のApple／Googleアカウントが乗っ取られると、大学のパスキーも攻撃者の端末に同期される
  - フィッシング耐性があっても、この経路は防げない
  - 個人アカウントのリカバリー手段が、実質的な**最も弱い環**になる
- 個人アカウントの保護は、メールOTP（個人メール宛て）の時代から本来必要だったこと
  - 同期パスキーによって、そのことが明確になり**共通認識**になってきた
- 大学としてできること
  - 情報セキュリティ教育で**個人アカウントの保護**を明示的に扱う（パスキー化、リカバリー設定の点検、共有しない）
  - 大学アカウントへのパスキー登録・削除を本人に通知し、登録一覧を本人が確認できるように
  - 登録・削除などの設定変更にはAAL2を要求（→ 後述のBAL）

©2026 Motonori Nakamura

パスキーをどこに保存するか

同期パスキーの保存先は、ブラウザ／OSが「いまどのアカウントで動いているか」で決まる

Chrome／Edge：プロファイル単位で同期

- プロファイルごとに同期先のアカウントが異なる
  - 個人のGoogle／Microsoftアカウントのプロファイル
  - 大学のGoogle Workspace／Microsoft 365アカウントのプロファイル
- **大学用のパスキーを個人プロファイルに保存**
  - 卒業・退職後も個人側に残り、個人アカウント乗っ取りの影響を受ける
- 逆に、**個人用のパスキーを大学プロファイルに保存**
  - 卒業・退職で大学アカウントが消えると、個人のサービスにログインできなくなる

Apple：iCloudキーチェーン

- 個人端末には組織アカウントがない（Managed Apple Accountを除く）
- 保存先は基本的に個人のiCloudキーチェーン
  - 保存先で迷わない分、**まだわかりやすい**
- その分、個人のApple Accountの保護が直接効いてくる

分離を意識した運用：大学用のパスキーは大学のプロファイルに、個人用は個人のプロファイルに

（対応状況はブラウザ・アカウント種別により異なるため、利用者向け案内で具体的に示す）

©2026 Motonori Nakamura

同期パスキーはもはや禁止できない

- アテステーション：認証器の機種・性質をRP（IdP）に証明する仕組み
  - FIDO Allianceの認定制度とメタデータサービス（MDS）で裏付ける仕組み（ただし、そのガバナンスがどこまで効いているかは未知数）
- 同期パスキーでは原則として提供されない
  - AAGUID、BE（同期可能）／BS（同期済み）フラグは**認証器の自己申告**
  - 本学のAAGUID集計も、厳密には「申告値」の分布
  - Entra IDでも同期パスキーはアテステーション非対応
- Appleの場合
  - iCloudキーチェーンのパスキーは常に同期型で、端末固定型を選べない
  - MDMによるパスキーアテステーションはManaged Apple Accountが前提で、鍵はその管理対象アカウントのiCloudキーチェーンに同期される
  - 外部（RP）から「この端末に固定されている」ことは**判別できない**

アテステーションに頼れない
→ 同期型かどうかを技術的に見分けて禁止することはできない

本学の登録の約45%はApple（常に同期型）。禁止すれば多くの利用者が使えなくなる

同期パスキーの利用を前提に、端末固定が必要な場面は別の手段で担保する

©2026 Motonori Nakamura

端末固定が必要な場面の現実解

対象	方式	担保の仕組み
一般の学生・教職員	同期パスキーを許容	登録・リカバリー手続きの厳格化 登録通知、個人アカウント保護の啓発
大学支給の管理端末	MDM＋組織アカウントの同期領域 （Managed Apple Account 等）	同期先の制限 条件付きアクセスで端末の準拠状態を別に確認
特権アカウント 機微な業務（入試・人事・医療・輸出管理 等）	大学が配布するセキュリティキー （アテステーションを検証可能）	配布と登録の場面を大学が管理 AAGUIDの許可リスト

NIST SP800-63B-4：連邦システムでは、MDM等により許可されていない端末・同期先への同期や共有を防ぐことを要求

鍵の性質で判別できないなら、「配布経路」と「登録手続き」で担保する

©2026 Motonori Nakamura

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も増加
- **社会全体でも「オンラインでの確かな本人確認」が求められるように**
  - 特殊詐欺・口座の不正利用対策：犯収法の改正（非対面での本人確認書類の画像送信方式を廃止）
  - マイナンバーカードの公的個人認証が普及（スマートフォンへの搭載：Android 2023年、iPhone 2025年）
  - 国際的な指標も改訂：NIST SP800-63-4（2025）

©2026 Motonori Nakamura

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

©2026 Motonori Nakamura

「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

©2026 Motonori Nakamura

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

©2026 Motonori Nakamura

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）

窓口に来なくても、本人だけで解決できる

- パスワードを忘れても、窓口での対面の本人確認が不要に
- マイナンバーカード（デジタル認証アプリ）で本人確認し、オンラインで再設定
- 本人確認の確かさを保ちつつ、**窓口対応のコストを削減**



©2026 Motonori Nakamura

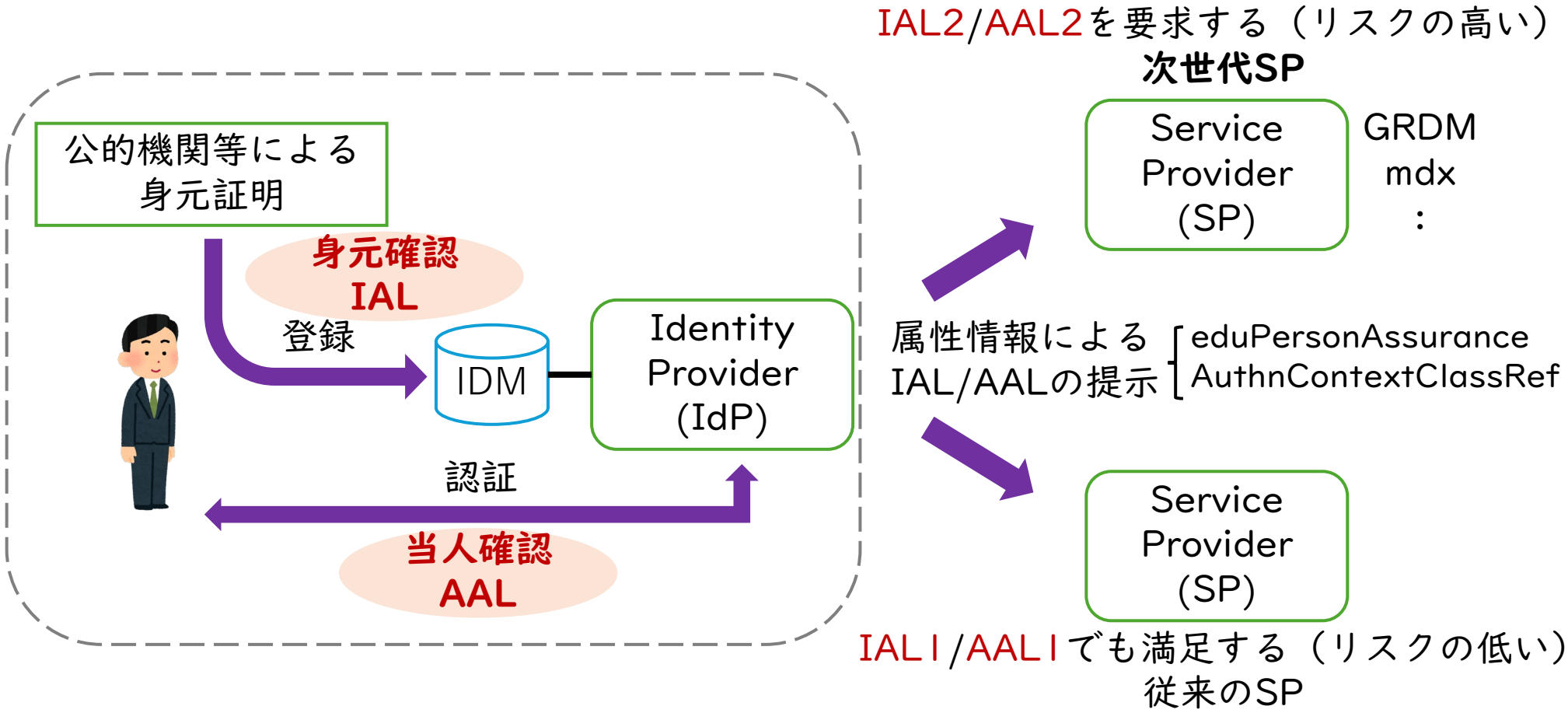
様々な保証レベル

- 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

©2026 Motonori Nakamura

認証連携における
身元確認(IAL)と当人確認(AAL)



©2026 Motonori Nakamura

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/

©2026 Motonori Nakamura

新入生アカウント発行フロー（例）

	経路①：郵便（住所）	経路②：連絡用メール
1. 受験出願　生年月日・連絡用メールアドレスの登録、出願番号・受験番号の取得	住所を登録	アドレスを登録
2. 合格通知　アカウント取得方法を郵送	取得方法を郵送	
3. ID発行サイト　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	出願番号・受験番号	
4. 有効化キー送付　連絡用メールアドレス（非表示）に有効化キーを送付		有効化キー
5. アカウント有効化　ログインIDと有効化キーを入力し、パスワードを設定	ログインID	有効化キー
6. 多要素認証の設定　続けて設定。やり直しには有効化キーが必要、完了すると有効化キーは無効化		有効化キー→完了で無効

以降のログイン　パスワード（知識）＋ 多要素認証（所持・生体）

パスワード ＋ 多要素認証 ＝ 2要素

郵便とメールの両方の経路を通らないと設定できない ＆ パスワードのみでログインできる瞬間を作らない

©2026 Motonori Nakamura

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
  - モバイルデバイスの普及が、認証のパスキー化を後押しした
  - 同じ流れが、身分証のデジタル化にも広がろうとしている
  - モバイルデバイスにおける身分証の要件とは？

©2026 Motonori Nakamura

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）

©2026 Motonori Nakamura

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的： 組織による一括証明	Web 3.0的： 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）

双方を考慮したハイブリッド プラットフォームに収束？

©2026 Motonori Nakamura

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

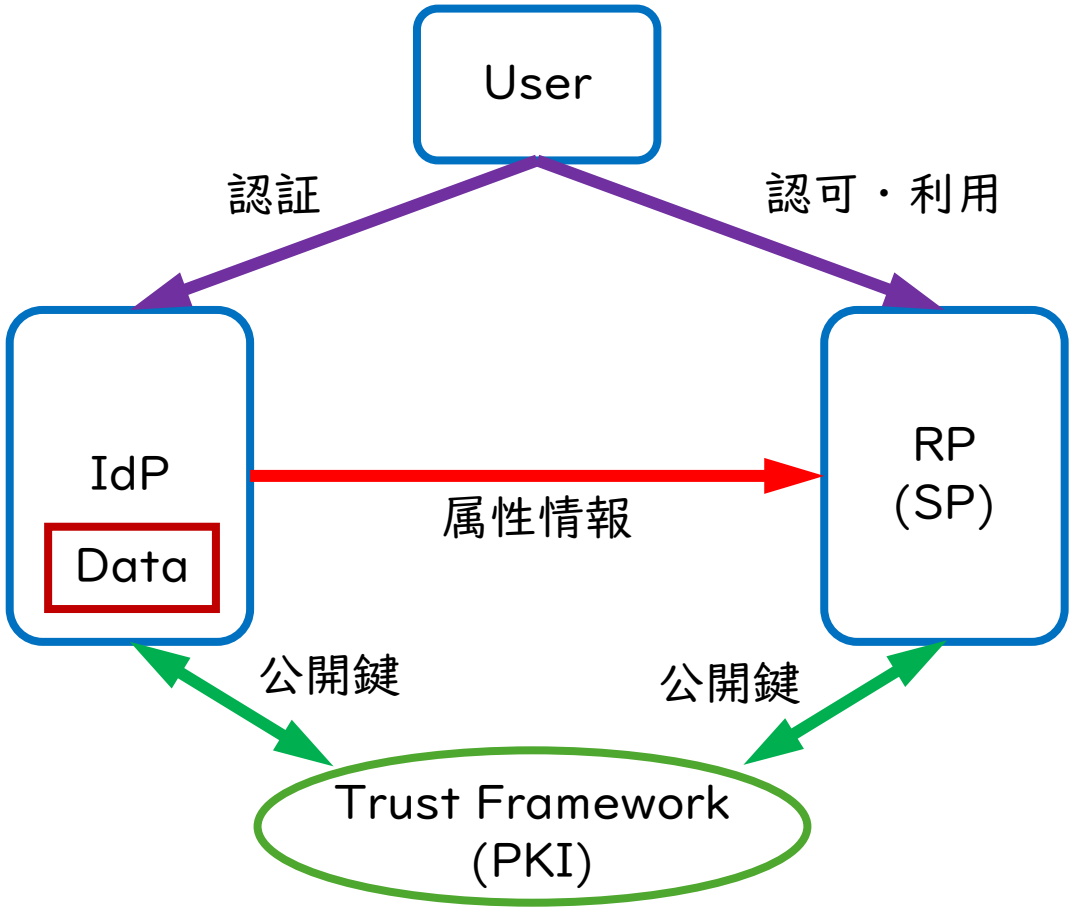
- ワクチン接種証明（2021年～2024年）
  - SMART Health Card（SHC）という健康証明用の規格
  - 海外事例
    - EUデジタルCOVID証明書（EU DCC）
    - WHO世界デジタル健康認証ネットワーク
- mDL（2022年～）
  - オーストリア、ルイジアナ州などが先行
- OpenBadges 3.0 （2024年～）
  - 2.0までの画像ベースと異なり、VCに対応した機械可読版に再設計
- EUDI Wallet（EU Digital Identity Wallet）
  - eIDAS 2.0に基づき、2026年までに欧州各国がサポート予定
- 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



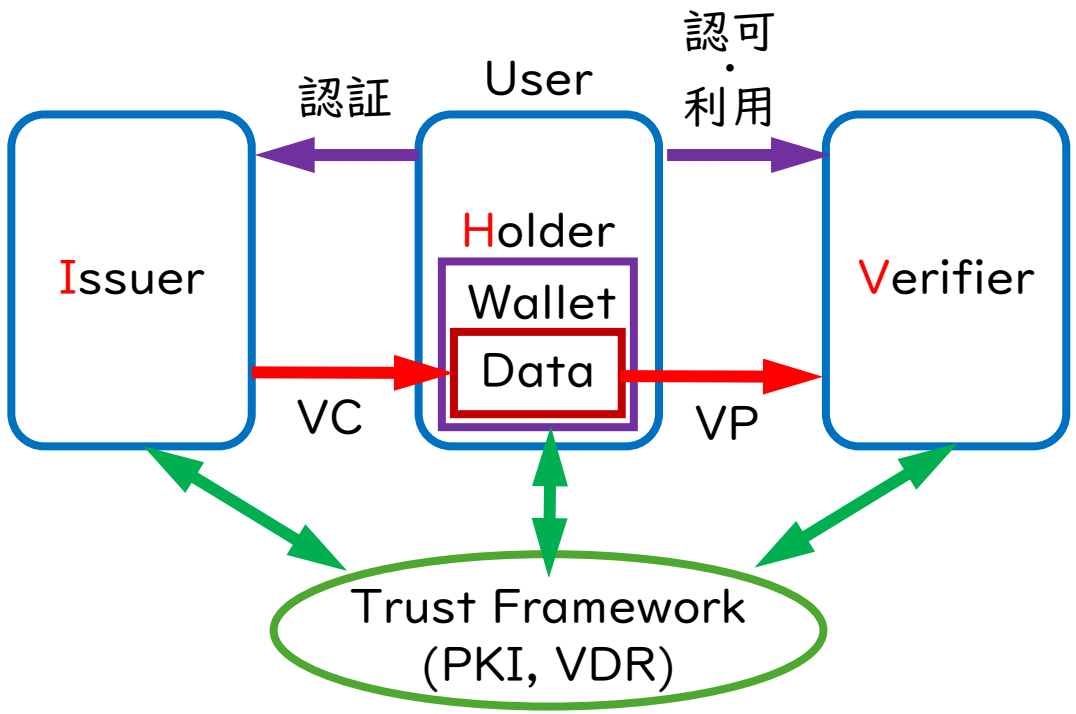
©2026 Motonori Nakamura

SSOモデルとIHVモデル

SSO Model (FAL1/2)



IHV Model (FAL3)



VP: Verifiable Presentation

VDR: Verifiable Data Registry

©2026 Motonori Nakamura

学術デジタル証明書の２つの用途

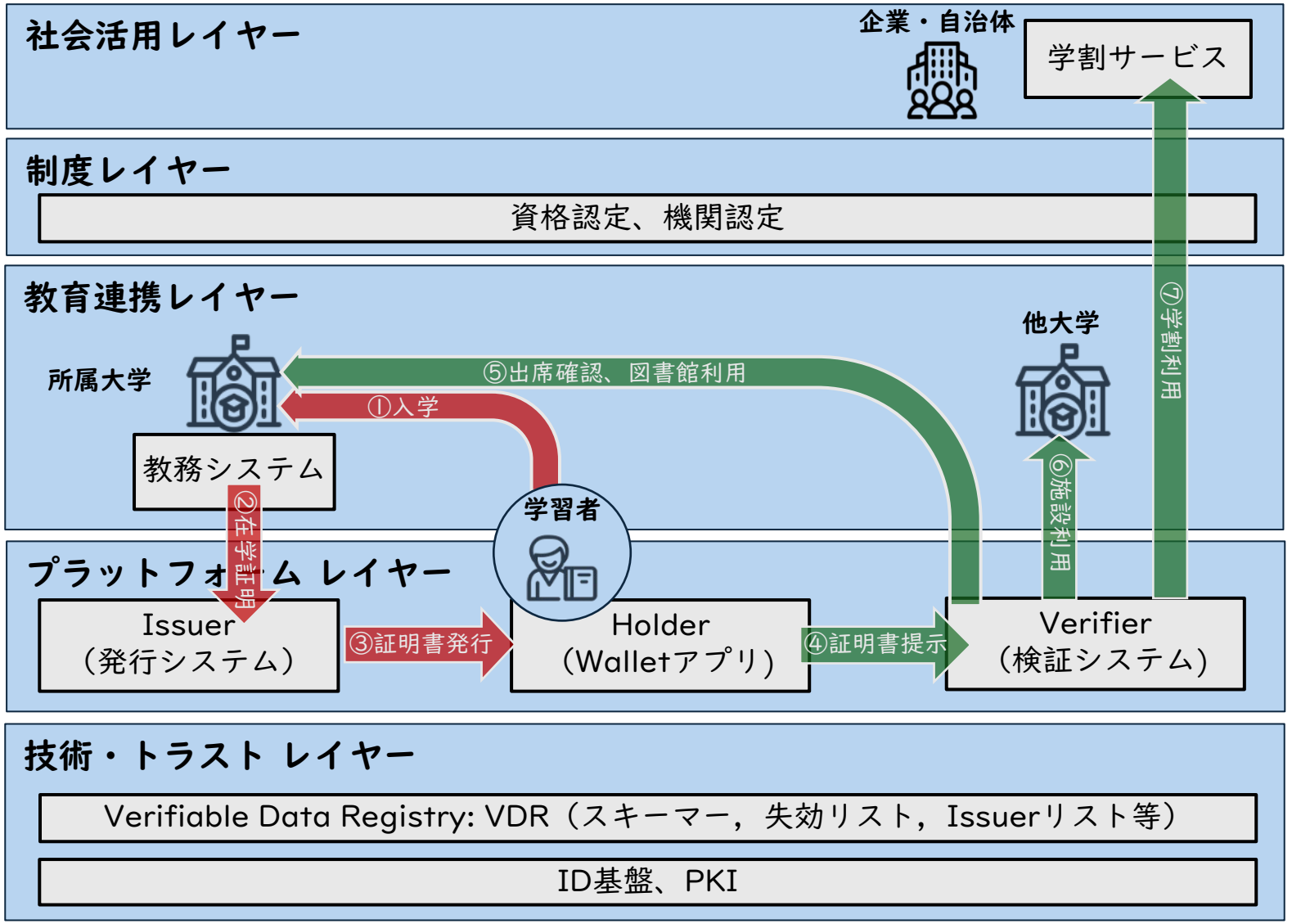
- 身分証明
  - 学生証、教職員証
  - 在学証明書、在籍証明書
  - ユーザに関する**現時点の属性**を証明する

- 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

©2026 Motonori Nakamura

IHV型学術デジタル証明書基盤の事例–身分

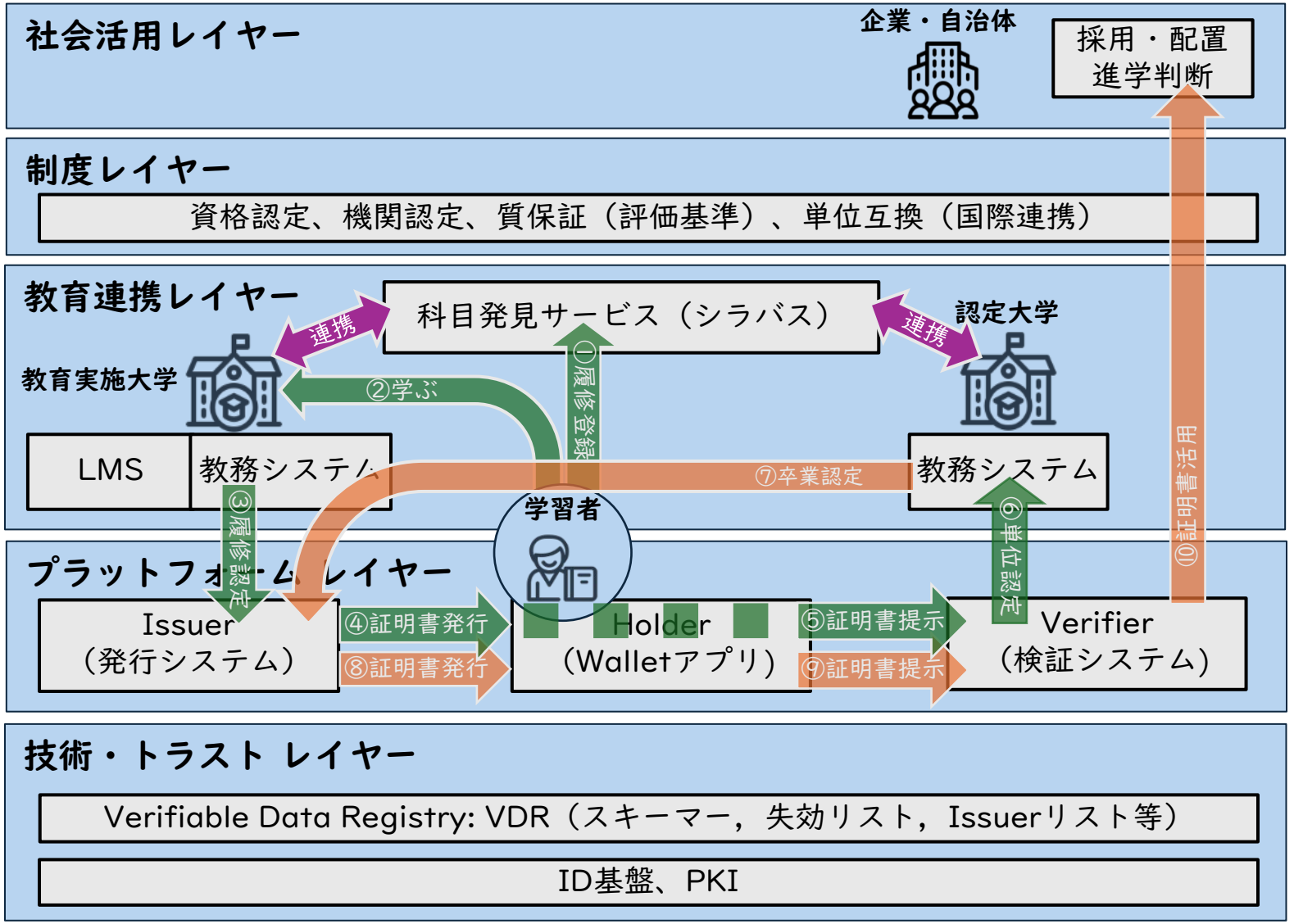
デジタル身分証を実現する基盤



©2026 Motonori Nakamura

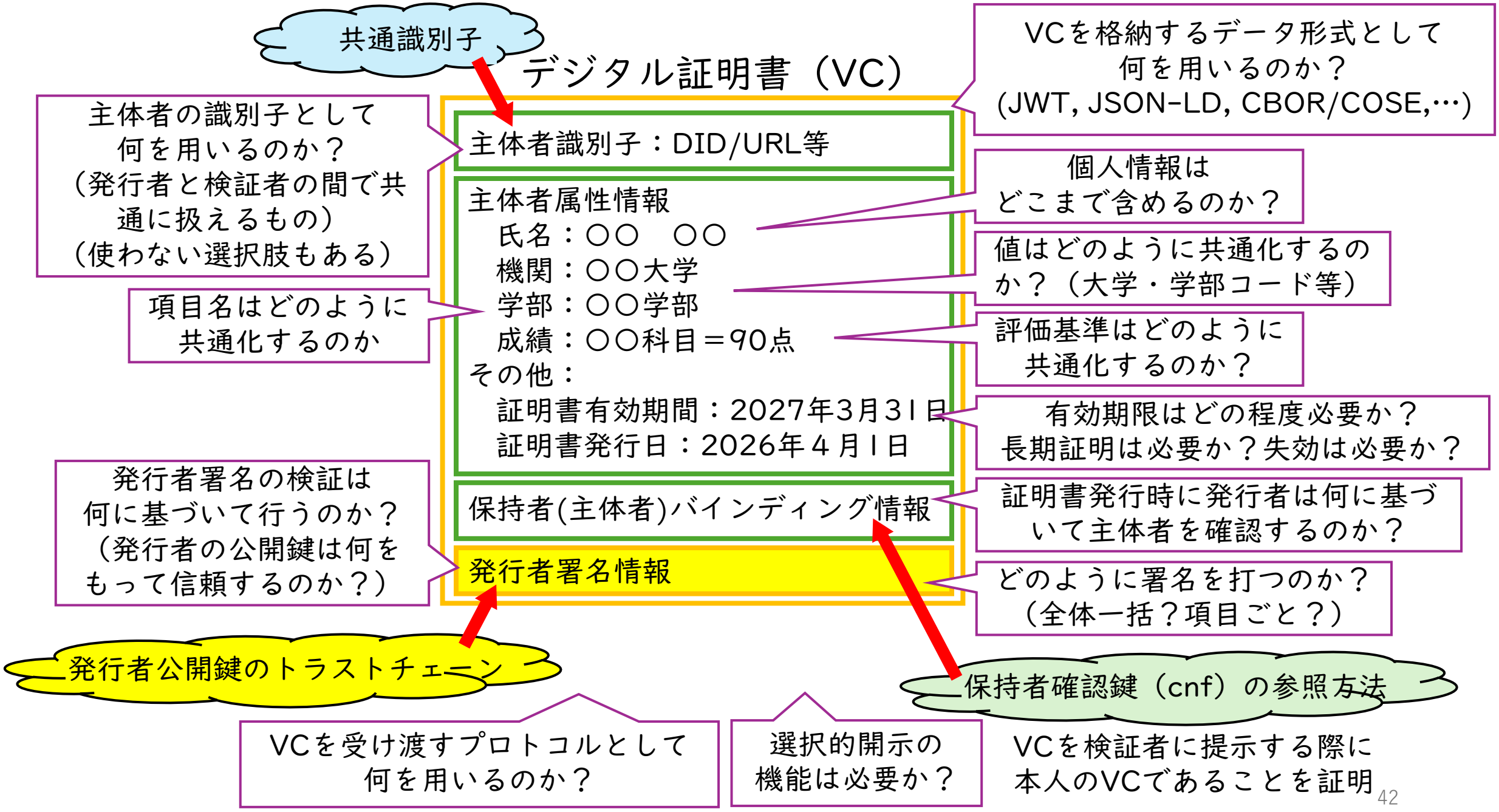
IHV型学術デジタル証明書基盤の事例–経歴

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



©2026 Motonori Nakamura

IHVモデル(VC)は自由度が非常に大きく、決めるべき事項が膨大



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）

©2026 Motonori Nakamura

この夏の動き（2026年7～9月）

学術デジタル・クレデンシャル円卓会議2026

2026年7月15日開催、OpenID Foundation Japan主催

- 標準動向／マイクロ・マクロクレデンシャル／大学事例／ベンダー／パネル
- 複数の団体・ベンダーが個別に進める検討を俯瞰
- 産学の役割分担と、機関が関与すべき「共通領域」を議論

JMICRO 質保証・承認審査制度案

2026年7月から意見募集

- 認定機関／非認定機関の区分
- 審査観点：MCを含む内部質保証規程、自己点検の対象化、フレームワーク・記述子への適合、デジタル発行ガイドライン・メタデータへの適合
- 承認は原則4年、レジストリで公表

AXIESでも部会を新たに立ち上げ、検討が始まろうとしている

整理が進んだこと

- 関係者の**役割分担と関係性の再認識**（標準化団体・質保証機関・大学・ベンダー）
- 発行側：質保証と発行者の信頼の枠組み（承認・レジストリ）

これから

- 「消費」側の立場も含めた**エコシステムのデザイン**
- 誰が（企業・他大学・本人）、何に（採用・単位認定・入学審査）、どう使うか（検証方法・業務システムとの接続）の整理

円卓会議：https://openid.connpass.com/event/393175/　JMICRO：https://www.micro-credentials.jp/ova_doc/public_comment202607/

©2026 Motonori Nakamura

オープンバッジの課題：「消費」の設計



仕組みは整ってきた

受け取った側がどう使うかが設計されていない

- 検証は「画像やURLを人が見る」、発行プラットフォームの検証ページ頼み
- 提示しているのが本人かを確認する仕組み（Holder Binding）がない
- 標準的な提示・検証プロトコルが使われていない（OB 3.0はVCベースだが実装はこれから）
- 採用・入学審査・単位認定などの業務システムが機械的に取り込む想定がない
- 発行プラットフォームの存続に依存する

大学が今、考えるべきこと

技術（形式・プロトコル）も運用（誰がどう検証し活用するか）が、まだ決まっていない

→ だからこそ、どちらにも左右されない源泉（データ）の整備から始める

©2026 Motonori Nakamura

持ち出せる源泉データの整備

JMICRO「マイクロクレデンシャル内容記載シート」の項目を、学内の源泉で分類すると

区分	記載シートの項目	学内の源泉
プログラム（科目）の記述	名称、内容、学修成果、授業言語、授業の方法、学習量、評価の方法、質保証、レベル、単位／その他の認定、前提条件、積み上げ可能性	シラバス、カリキュラム 内部質保証の記録
個人の達成記録	学習者を識別する情報、発行日（＋評価の結果）	教務システム、LMS
発行者	発行機関、発行国／地域	機関の情報、署名鍵

- 特定の形式に依存しない構造化データとして、年度・版を管理して保持する
- OB 3.0、W3C VC、SD-JWT VC、mdoc、署名付きPDF … は出口での変換

発行形式は「出口」にすぎず、源泉データこそが大学の資産

©2026 Motonori Nakamura

持ち出すための「ID」の整理

どのIDを使うかの運用標準はまだ定まっていない（整理の途中）

IDの種類	論点	現状の候補
人（学習者）	学籍番号は学内限定、進学で変わり、卒業後は使えない 記載シートでは「学習者を識別する情報」が必須	学籍番号、メールアドレス、ePPN、eduID、ウォレットの鍵（DID 等）
機関（発行者）	発行者の真正性と、鍵の信頼の起点	大学コード、ドメイン、OpenID Federation Entity ID、DID
科目・プログラム	年度をまたいだ同一性と版の管理	科目ナンバリング、シラバスID
証明（記録）	失効・訂正のための個別の識別	証明書ID、失効リスト

標準が決まる前にできること

学内のIDと外部のIDの対応表を管理できる状態にしておく

©2026 Motonori Nakamura

まずは従来型の単位互換の枠組みから

- 将来に向けた整理（JMICRO、AXIESの新部会）と並行して、**既存の制度の中で始められる**ことがある

- 単位互換・大学間連携には、すでに制度と運用がある
  - 協定、科目の対応付け、成績のやり取り、単位認定
  - 現状は紙・PDF・個別の表計算での処理が中心

- 既存業務のデジタル化として、VCの要件を具体化できる
  - 誰が発行し、誰が検証し、何に使うか（「消費」側）が明確
  - 必要なIDとデータ項目が実務から決まる

大学間で個別に科目を対応付け

N × M

科目の提供元 N校 × 受入先 M校
組み合わせごとに対応表が必要

共通の参照枠にマッピング

N ＋ M

提供元・受入先がそれぞれ1回ずつ対応付け
シラバス・学修成果の構造化が前提
（学認のIdP・SP連携と同じ構図）

©2026 Motonori Nakamura

身分証

- 身分証は、券面表示のみのもの（紙）から、磁気ストライプを備えたものを経て、ICチップ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







©2026 Motonori Nakamura

デジタル身分証

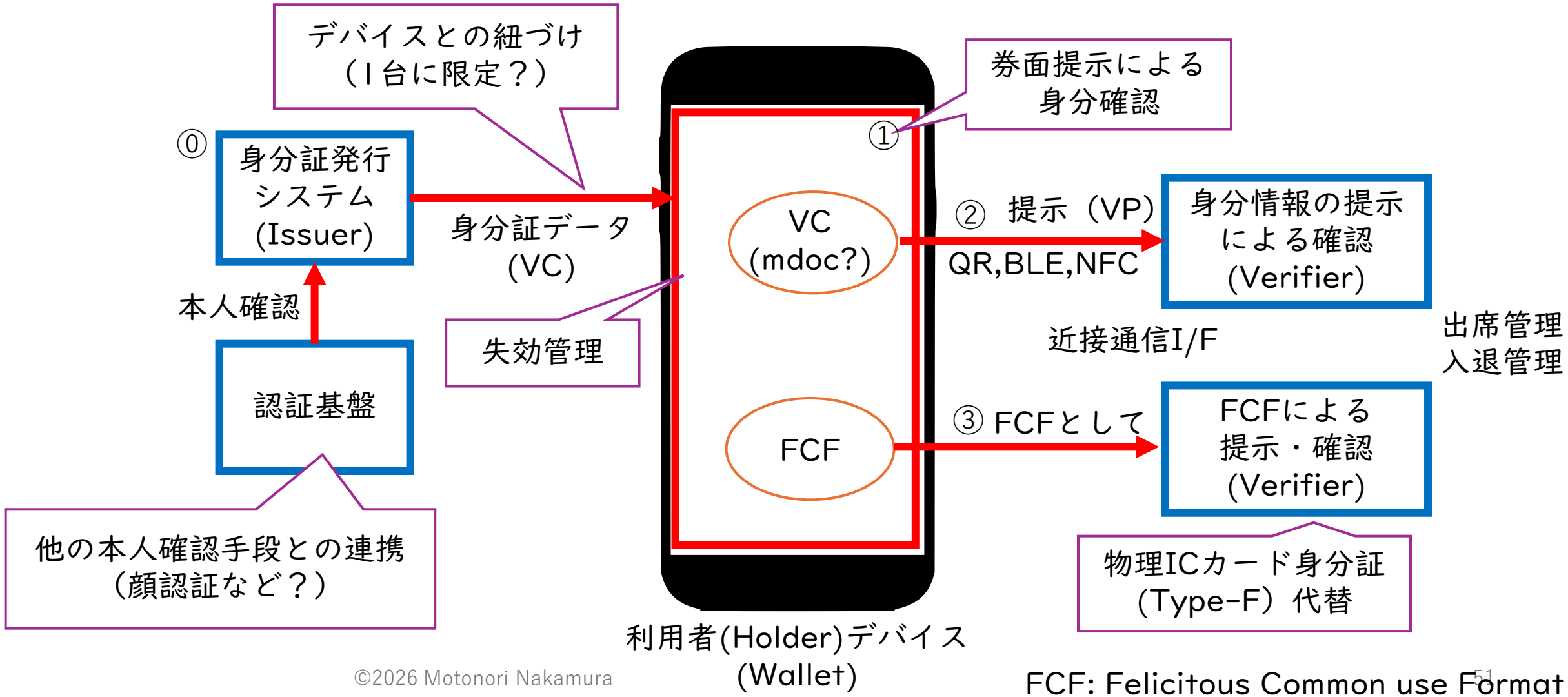
- オンラインサービスの高度化と並行して、物理媒体による身分証の高度化についても検討が必要
  - スマートフォン等の高度化したデジタル端末の普及
  - 発行・配付コストの削減、入退管理システム等の更新コスト削減



Kintoneによる発行試行

©2026 Motonori Nakamura

デジタル身分証を構成するハードウェア要素



©2026 Motonori Nakamura

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 出欠・図書館 期末試験	通学定期 美術館・映画館 各種施設	留学・研修 単位互換	学位証明 インターン 資格証明	マイクロ資格 スキル証明 学習ポートフォリオ

©2026 Motonori Nakamura

デジタル学生証：方式の乱立

方式	利点	課題
QRコード （静的／ダイナミック）	導入が容易、多くのベンダーが採用	**身分証としての統一規格がない**（ベンダーごとの独自形式） スクリーンショット対策と応答性の両立 FeliCaリーダーからの機器更新
NFC （スマートフォンのウォレット）	利便性・安全性が高い	プラットフォーム依存、リーダー側の対応 OSによる差
モバイルFCF	既存のFCF（FeliCa）設備を活用できる	当面はAndroid中心 iPhoneへの対応が課題
mdoc （ISO/IEC 18013-5）	国際標準、本人の端末であることの確認、選択的開示	国内標準プロファイルを策定中 普及はこれから

例：フェリカネットワークス「学生証プラットフォーム」（mdoc、NIIと連携、2026年4月開始）、大阪大学での実証（2025年）

決め手がない今は、方式に依存しない発行元データ・ID・失効管理の整備を優先

©2026 Motonori Nakamura

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
  - EUDI Wallet（EUデジタルIDウォレット）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

©2026 Motonori Nakamura

定期試験がモバイル学生証の壁になる

学生証に載っている機能

身分証明（本人確認）

入館・入退室

図書館の利用

証明書の発行

決済

衝突するのは
端末操作を禁じた場面での本人確認
学生証を机上に置き、監督者が巡回して照合する方式では、全員に物理カードが必要

機能を分ければ、道はある：試験の本人確認を別の手段に

方式	内容	留意点
入室時の確認	開始前に端末で提示し、その後は電源を切って収納	入室に時間がかかる **バッテリー切れ**への代替が必要
座席QRの読取り	机に貼ったQRを端末で読み取ってから電源を切る	共通テスト会場などでは**QRを常置できない** バッテリー切れへの代替が必要
写真付きの名簿	大学が保有する写真で監督者が照合	写真の取扱いに注意
受験票	試験ごとに紙の受験票を発行	印刷と配付の手間

ただし、試験の本人確認の方法は教務の所管
情報基盤の側でどれだけ整えても、試験の運営方法が変わらなければ物理カードは全員に必要なまま
→ 学生証のモバイル化は、情報部門だけでは進められない

©2026 Motonori Nakamura

費用は消えず、部署をまたいで移る

方式	費用が生じる場所	主に負担する部署
物理カードを全員に発行	カードの発行・再発行	学生支援・情報部門
写真付きの名簿	教務システムの改修、監督時の照合の手間	教務・教員
入室時の確認	試験監督の増員	教務・教員
受験票	印刷と配付	教務

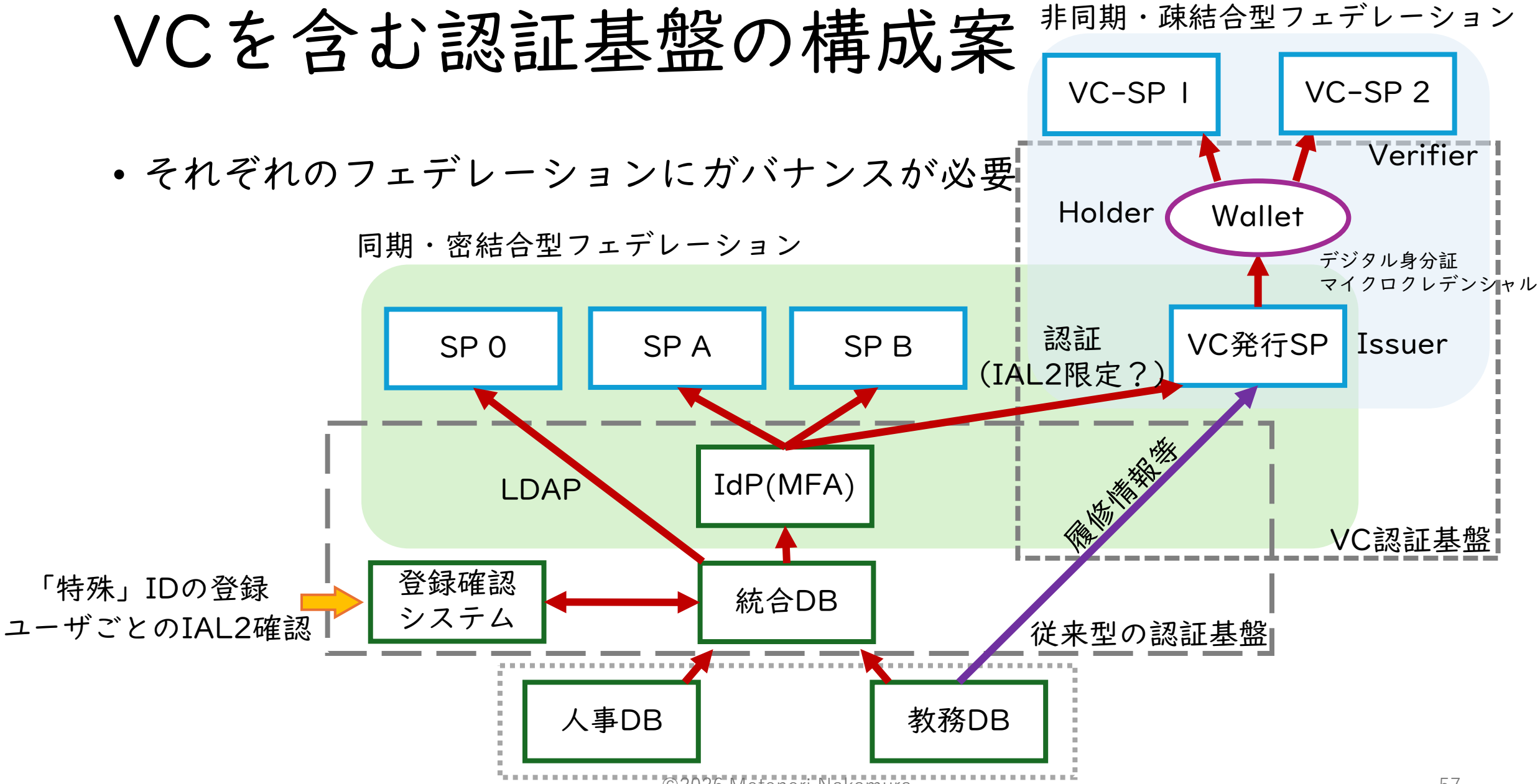
- モバイル化でカード費を減らしても、その分が**試験運営の側に移る**可能性が高い
  - 定期試験は学期ごと・科目ごとに実施され、多くは担当教員が監督 → 手間が頻度の分だけ積み重なる（年1回・専任体制の共通テストとは事情が違う）
- 情報部門だけで計画すると、カード費の削減だけが見えて試験運営の負担増が見えない

当面は物理カードを残し、モバイルを付加価値として加える
一本化を目指すなら、部署を横断した場で全体の費用を比べて判断する

©2026 Motonori Nakamura

VCを含む認証基盤の構成案

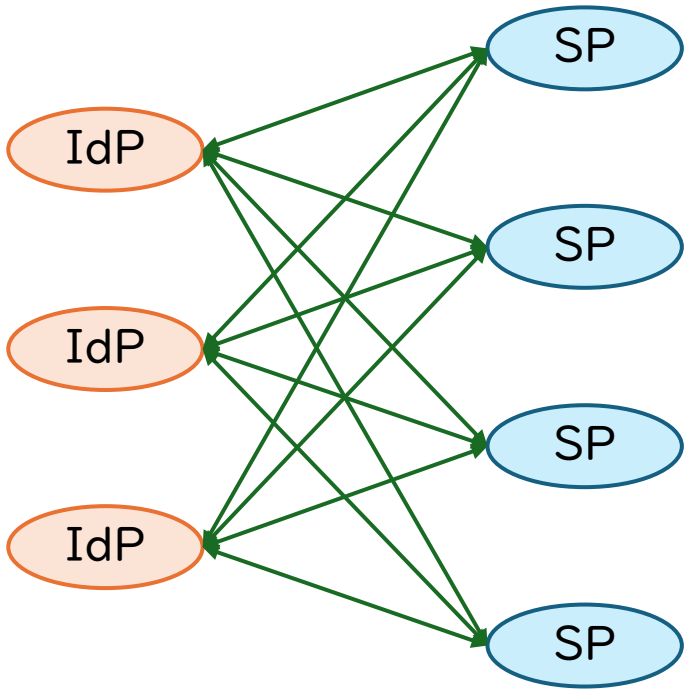
- それぞれのフェデレーションにガバナンスが必要

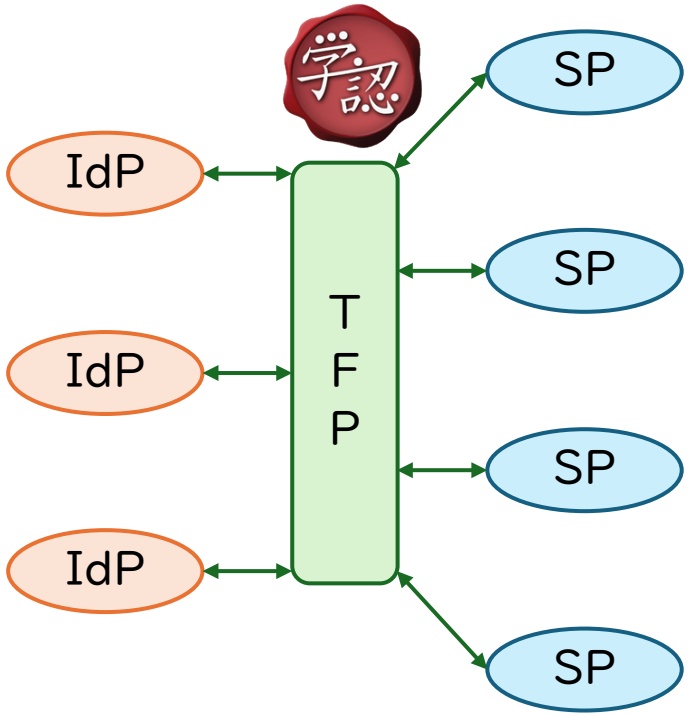


©2026 Motonori Nakamura

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

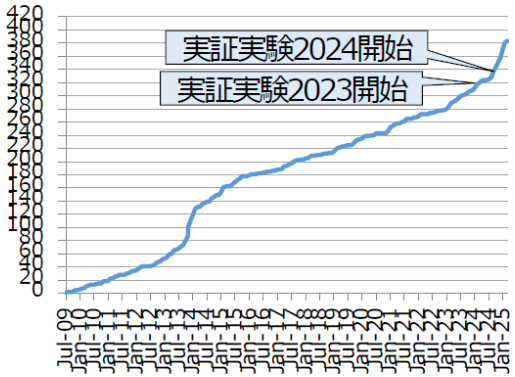
©2026 Motonori Nakamura

分散（フルメッシュ）型基盤整備の是非

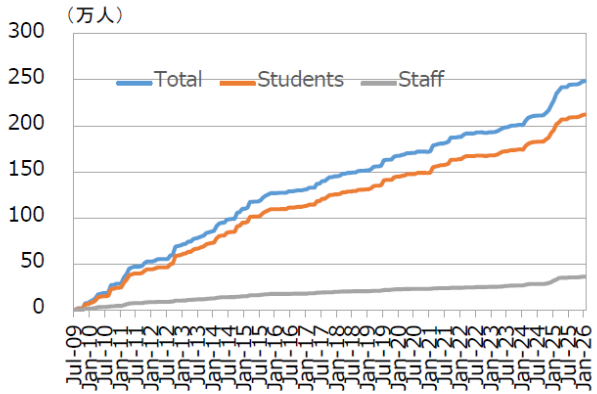
- 各機関の自主的な整備にまかせていて良いか？
  - 大学数規模などから米国の学術フェデレーションをモデルに構築
  - 小規模機関における導入の困難さ
  - 同じことをVCでも繰り返す？
  - 欧州のeduIDが参考になるか？

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）

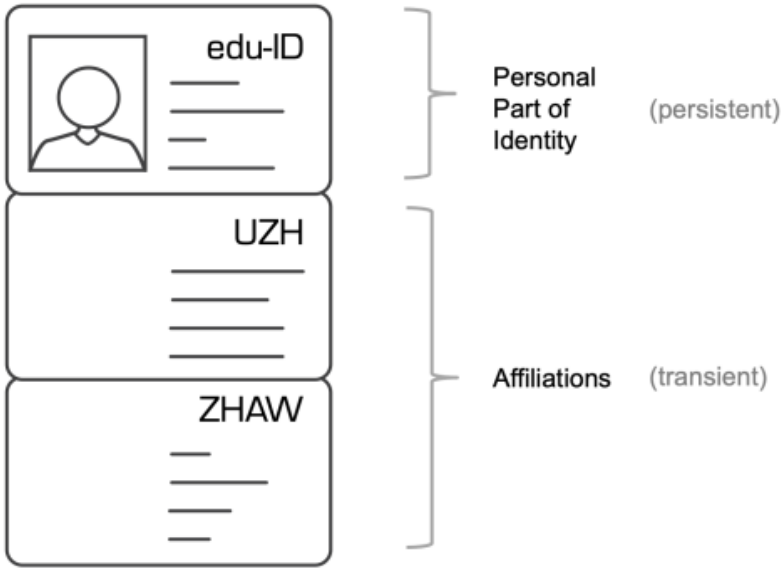
	国立大学	公立大学	私立大学	短期大学	高等専門学校	大学共同利用機関	その他
学認利用数	85	45	180	12	53	7	31
総数	85	103	624	292	58		
カバー率	100%	44%	29%	4%	91%		

※ 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

©2026 Motonori Nakamura

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

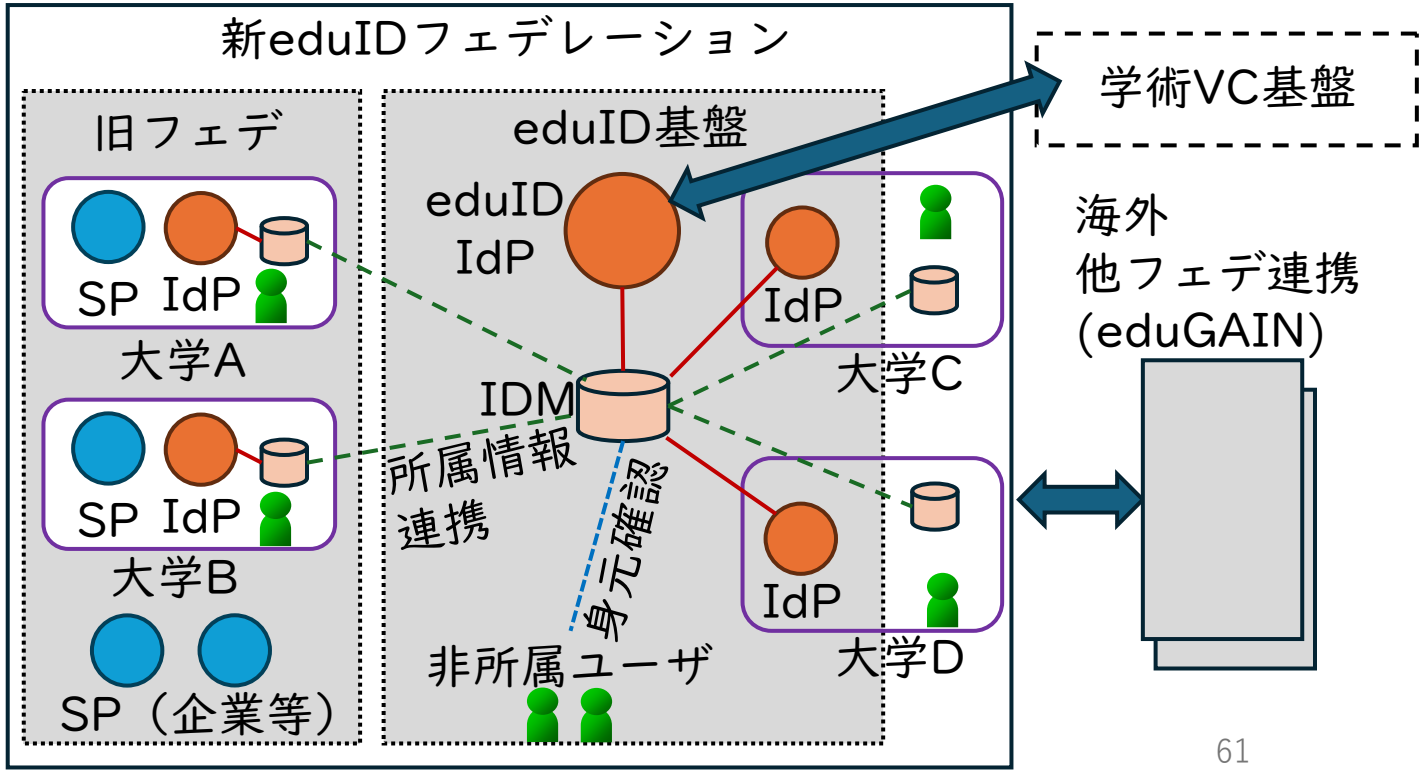


Source: https://help.switch.ch/eduid/docs/unis/architecture/

©2026 Motonori Nakamura

学認eduIDという方向性

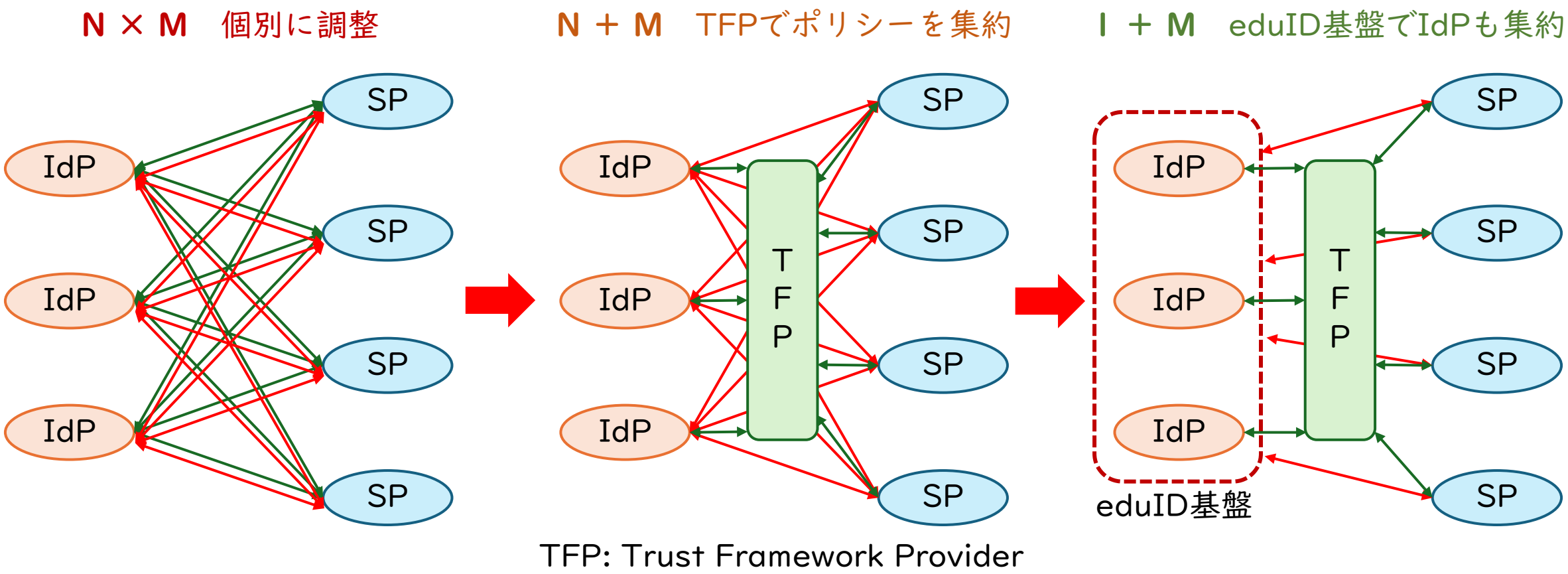
- 教育機関の枠を超えて個人に付与される永続的識別子とその認証基盤
  - 統合IdPシステムと分散管理によるコスト削減、機関参加率向上
  - 大学ごとの学外者アカウント管理の省力化
  - SP連携管理のコスト削減
  - SP参入コストの削減
  - 永続的なVC実現の基盤
  - VC規格の変遷への効率的な対応



©2026 Motonori Nakamura

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

©2026 Motonori Nakamura

大学が今から準備しておくこと

認証基盤

1. 同期パスキーを前提にした運用ルール（保存先の分離、登録通知、設定変更はAAL2で）
2. 個人アカウントの保護を含むセキュリティ教育
3. 特権アカウント・機微な業務向けに、端末固定型の認証器の配布と登録管理
4. 卒業生・学外者を含む身元確認（IAL2）とアカウント基盤

学修証明・身分証

1. 源泉データ（シラバス・学修成果・成績）を、形式に依存しない構造化データで
2. 人・機関・科目・証明のIDと、学内外のIDの対応表
3. MCを内部質保証規程の対象に（JMICROの認定機関区分の前提）
4. 単位互換など既存の大学間連携から小さく始める
5. 調達では標準への準拠とデータの持ち出しやすさを要件に

©2026 Motonori Nakamura

まとめ

- 大学の多様な活動を支える、これからの認証基盤
  - AAL・IALの整理と、多要素認証への移行時の脆弱性（BAL）の点検
  - 同期パスキーの時代：**個人アカウントの保護が組織の保護に**
  - 保存先の分離と、配布経路・登録手続きによる端末固定の担保

- 身分証・学修証明のデジタル化
  - 「消費」のデザインはこれから → **技術に依存しない準備**を先に
  - 持ち出せる源泉データと、ID（人・機関・科目・証明）の整理
  - 単位互換など既存の枠組みから始め、共通基盤（eduID等）へ

ID基盤は、大学ごとに特色や最適化を求めるものから共通の基盤へ

→ 大学のIT基盤整備の役割は、その上での教育・研究を支えるサービスの充実へ

©2026 Motonori Nakamura