デジタル証明書と大学のあり方

中村 素典 / 情報環境機構 IT基盤センター

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』
2026/6/26

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
- 2024 京都大学 情報環境機構 IT基盤センター長・CIO補佐

本講演の概要

- これからの大学の活動を支える情報基盤として
  - ID管理基盤に加えて
  - デジタル証明書発行管理基盤が重要に

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

- 大学における情報基盤を整備・運用する立場からの課題整理
  - 証明書発行システムが用途ごとにサイロ化しても良いのか？

京都大学 の「認証」を支える体制の変化

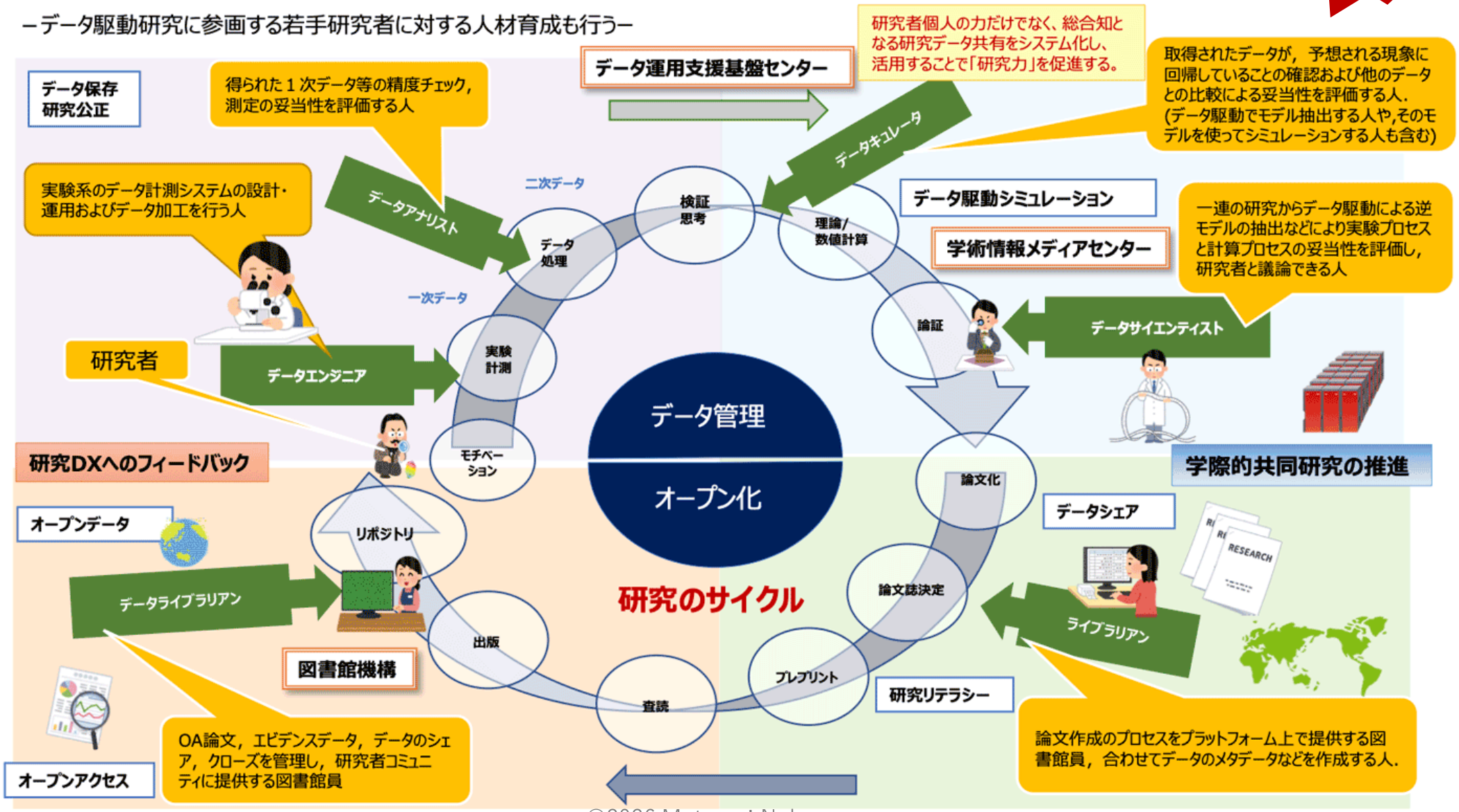
- 1997/4: 総合情報メディアセンターを設置
  - 「情報処理教育センター（教育用計算機）＋工学部高度情報実験施設」を改組
- 2002/4: 学術情報メディアセンターを設置
  - 「総合情報メディアセンター+大型計算機センター+KUINS」を改組
- 2005/4: 情報環境機構を設置
  - 「情報部＋学術情報メディアセンター」の体制で基盤整備を行う
- 2009/4:情報部に統合認証センターを設置
  - ICカードの発行開始
- 2011/4: 情報環境機構にIT企画室を設置
  - 「情報部＋IT企画室＋学術情報メディアセンター」の体制に移行
- 2011/5: 統合認証セ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

RDM

＜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－



大学における認証の（これまでの）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
  - スマートフォンの社会インフラ化
  - パスキーの急速な普及（当人確認(AAL)の信頼性向上の流れ）
  - アカウント情報と身分証情報の統合（身元確認(IAL)の信頼性向上の流れ）

- 従来の身分証機能をどのように引き継ぐか？

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
- オンラインサービスの高度化と並行して、物理媒体だった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
  - 身元確認、当人確認の高信頼化

Kintoneによる発行試行

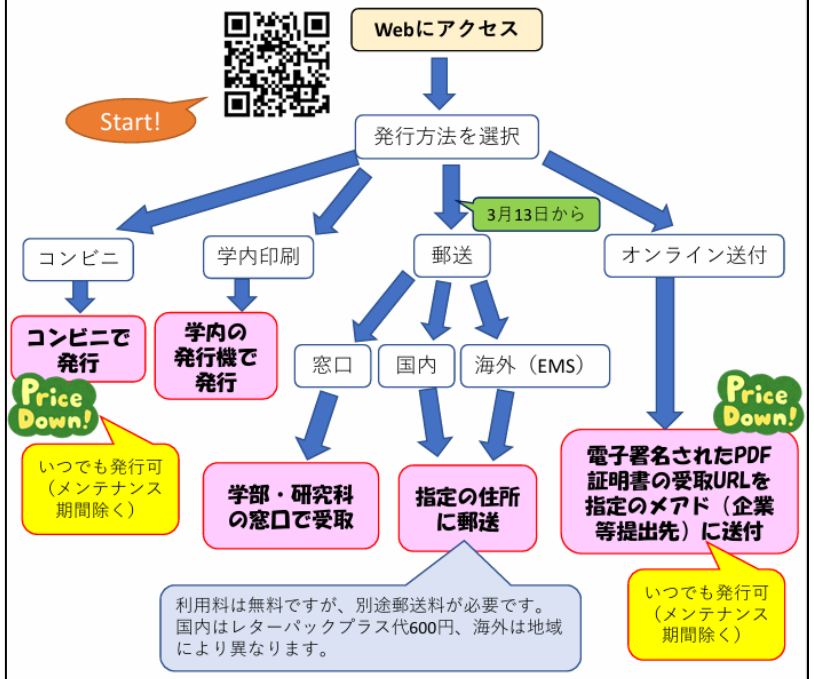
証明書発行のいま

（共通認証を用いた
教学部によるサービス）

学生各位

証明書の発行方法いろいろ

自動発行機以外にも、いろいろな証明書の発行方法がありますので、ぜひご活用ください。



Price Down! 在学生のコンビニ発行とオンライン送付にかかる手数料を、2025年3月13日以降は300円に値下げします（従前は400円）。

※コンビニ発行は別途1通60円の印刷代が必要です。

デジタル署名つきPDFにもさまざまな課題

- 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）
- 機械可読でない → 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　　（どちらかというとリテラシー問題？）
  - 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

→VC化の検討

認証エコシステムの広がり

大学の認証基盤は、
これらの機能を支える
共通基盤であるべき

- サービス内・組織内だけで通用するローカルアカウント
- 組織を越えて利用可能な認証フェデレーション（Worldwide）

- 組織内だけで通用する身分証 – デジタル化
- 組織を越えて利用可能な身分証（以前から）
  - 学割、入館（図書館等の施設相互利用） – 目視

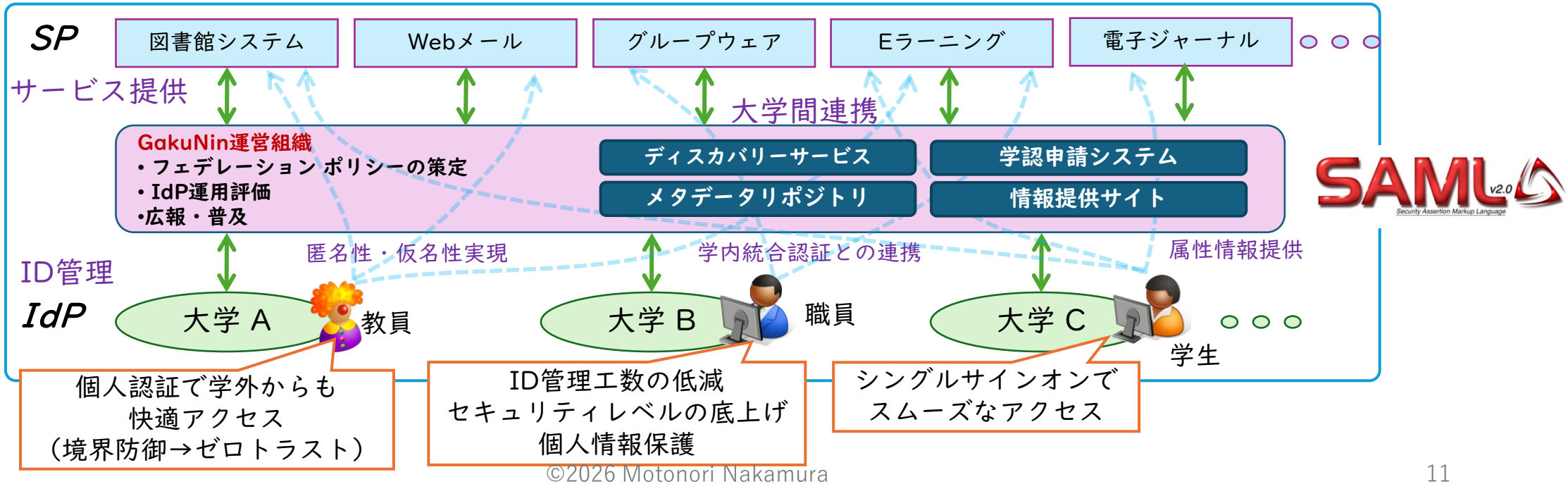
従来からの、発行者の制度的権威への信頼と、善意確認者の法的保護（偽造罪等による抑止）といった、あいまいな信頼構造の限界

- 卒業証明などの経歴証明
  - もともと他組織に対する証明機能 – 目視（偽造問題）

より信頼でき相互運用可能な仕組み（デジタル証明書）

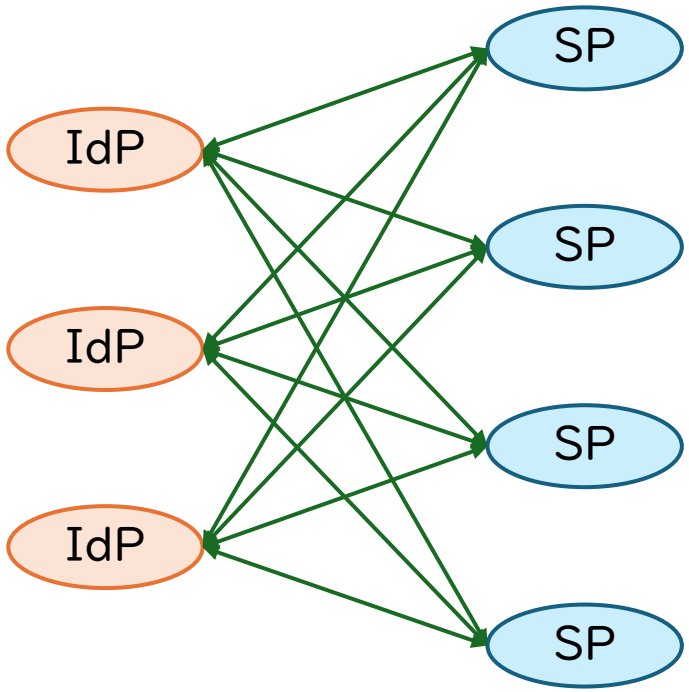
学術認証フェデレーション「学認」 by NII
– 学外サービスでの認証利用 –　（2009年～）

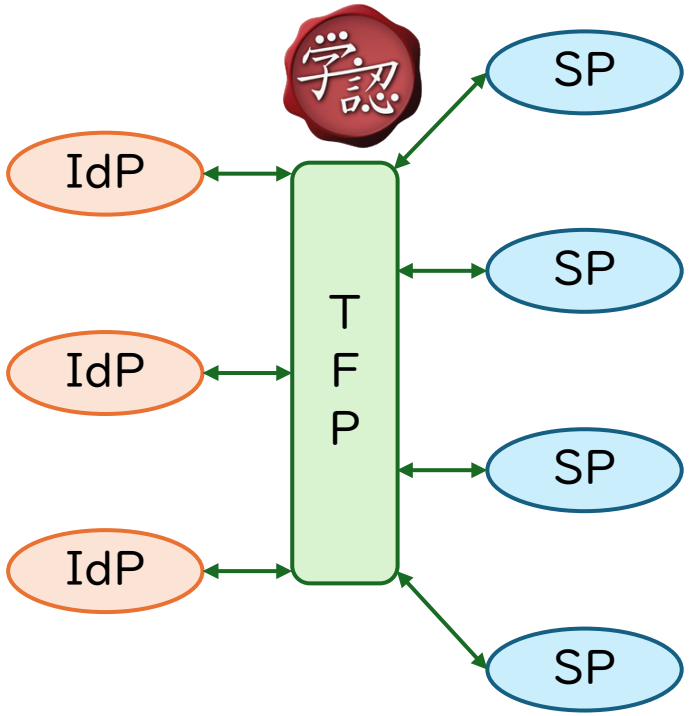
- シングルサインオン(SSO)技術に基づく学術研究支援IT基盤の構築
- IdP・SP相互の信頼を持続する信頼フレームワークの提供
- ID基盤のインフラ化による利便性向上、付加価値の実現、新サービスの創出
  - 大学間連携、産学連携、国際連携



フェデレーションによる集約効果

- 一定のポリシーに基づく信頼（トラスト）フレームワーク
- 個別調整でのN×Mの関係が、N＋Mの関係に効率化



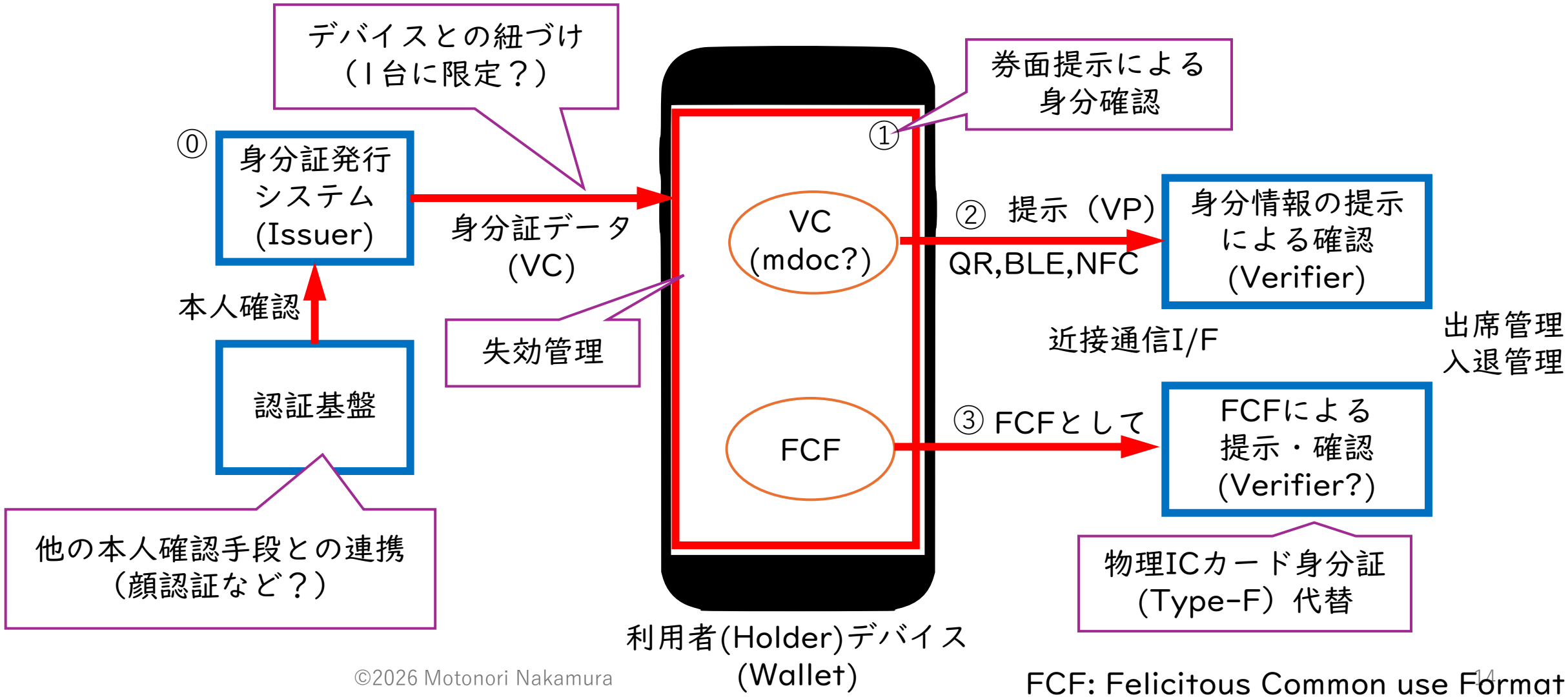


TFP: Trust Framework Provider

デジタル身分証発行のための技術的課題整理

- 様々な要素技術の組み合わせによる実現（スマホアプリ）
  - 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

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）

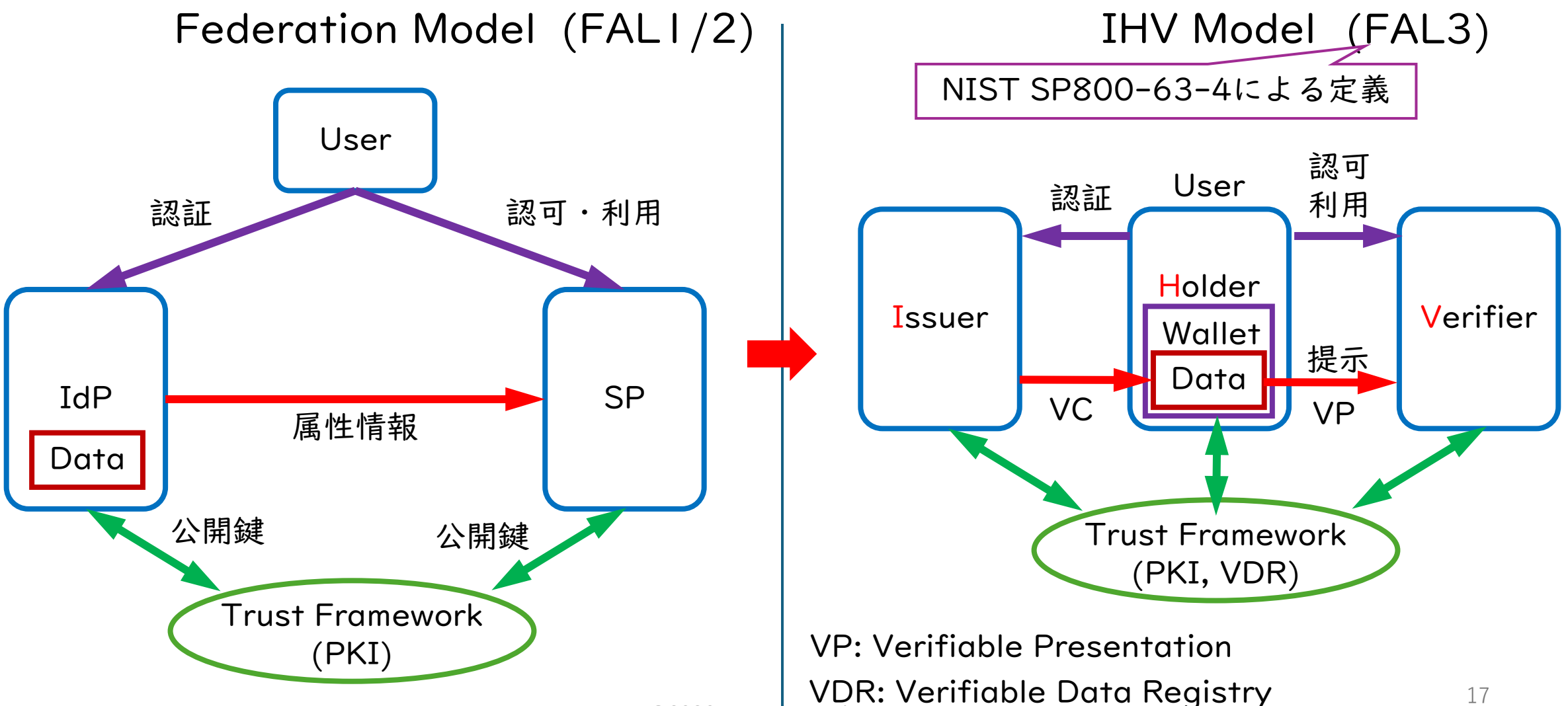
社会的背景：Web 2.0からWeb 3.0へ
情報の信頼と制御のパラダイムシフト

	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？

モバイルの普及によるモデルの変化：
フェデレーションモデルとIHVモデル



VP: Verifiable Presentation

VDR: Verifiable Data Registry

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

細部は異なるが、技術的基本構造は同じ　⇒　基盤の共通化による効率化・コスト削減

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

（公社）2025年日...
EXPO 2025 デジ...

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）

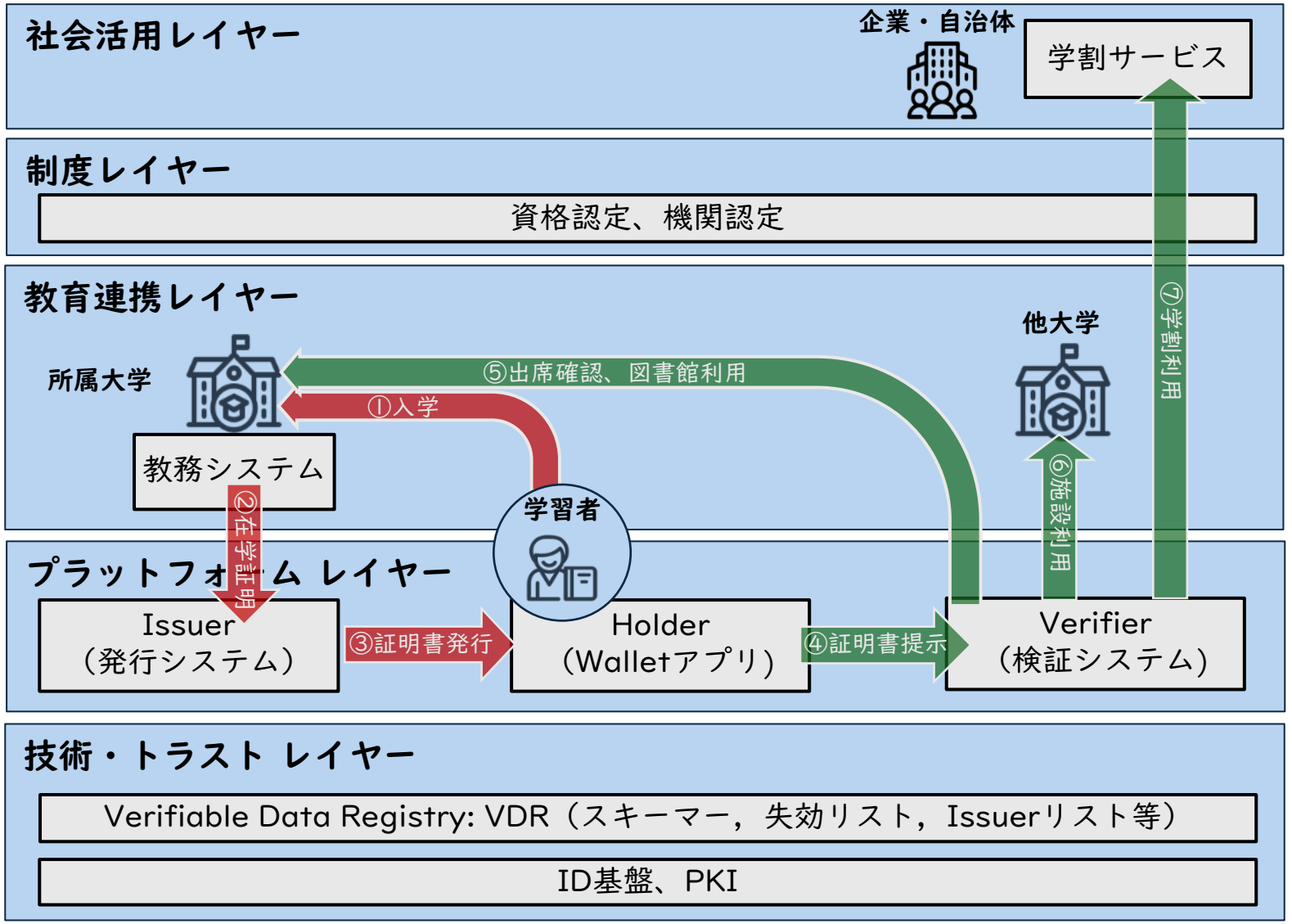
学内認証	**学割**	**国際流動性**	**就職・採用**	**生涯学習**
入退室	通学定期	留学・研修	学位証明	マイクロ資格
出欠・図書館	美術館・映画館	単位互換	インターン	スキル証明
期末試験	各種施設		資格証明	学習ポートフォリオ

デジタル身分証の実現に向けた課題

- 国際的な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）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

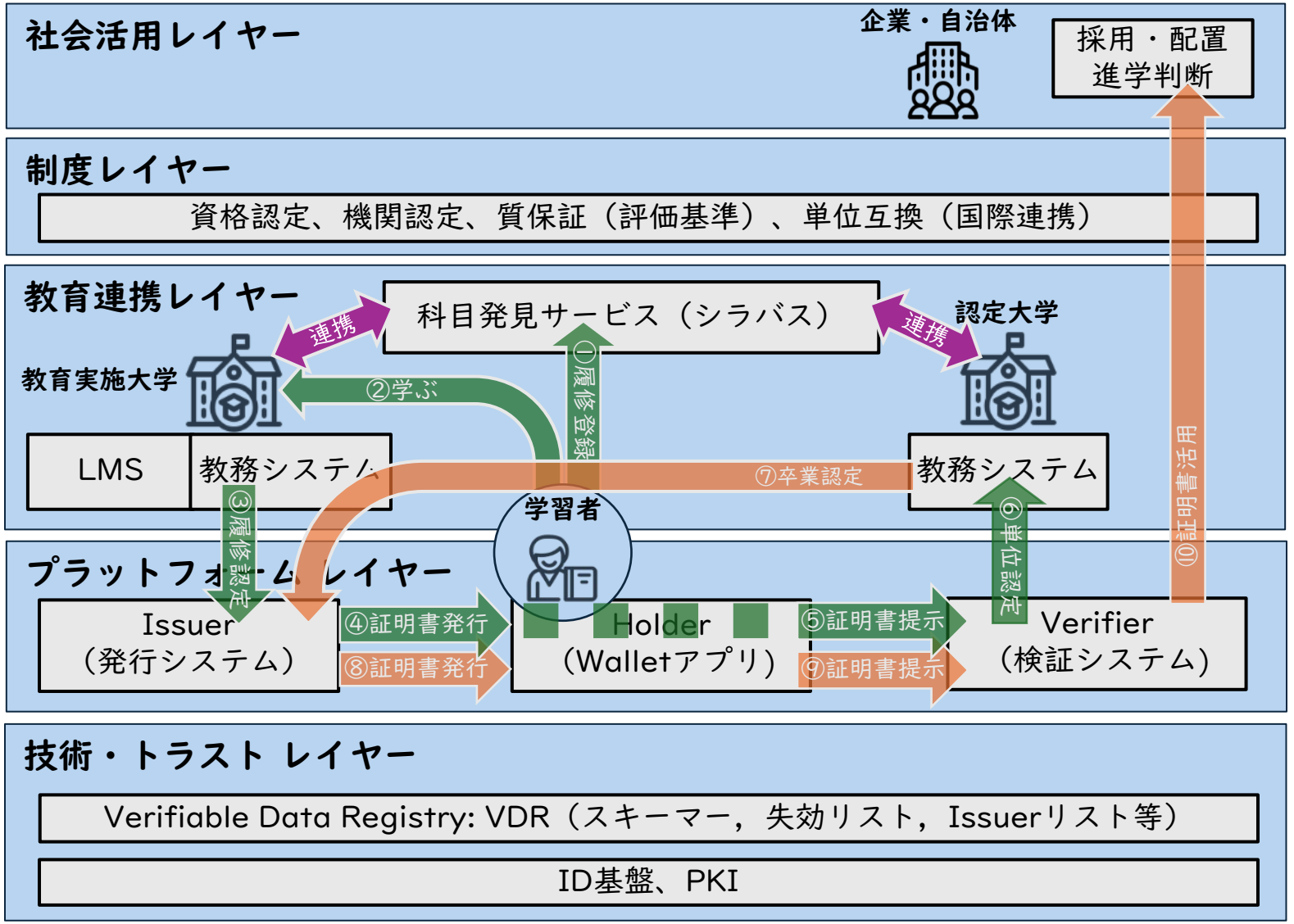
IHV型学術デジタル証明書基盤の事例－１

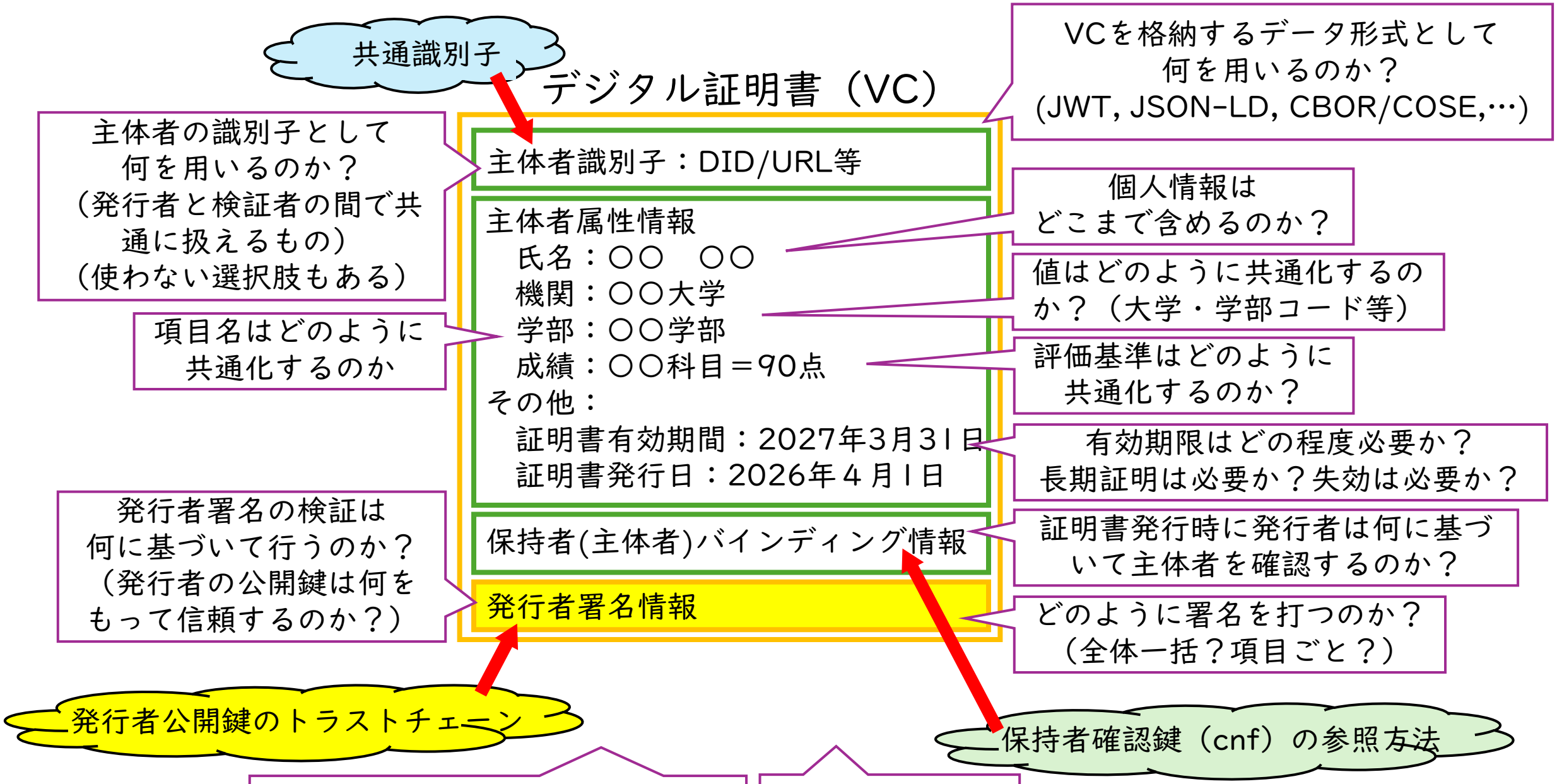
デジタル身分証を実現する基盤



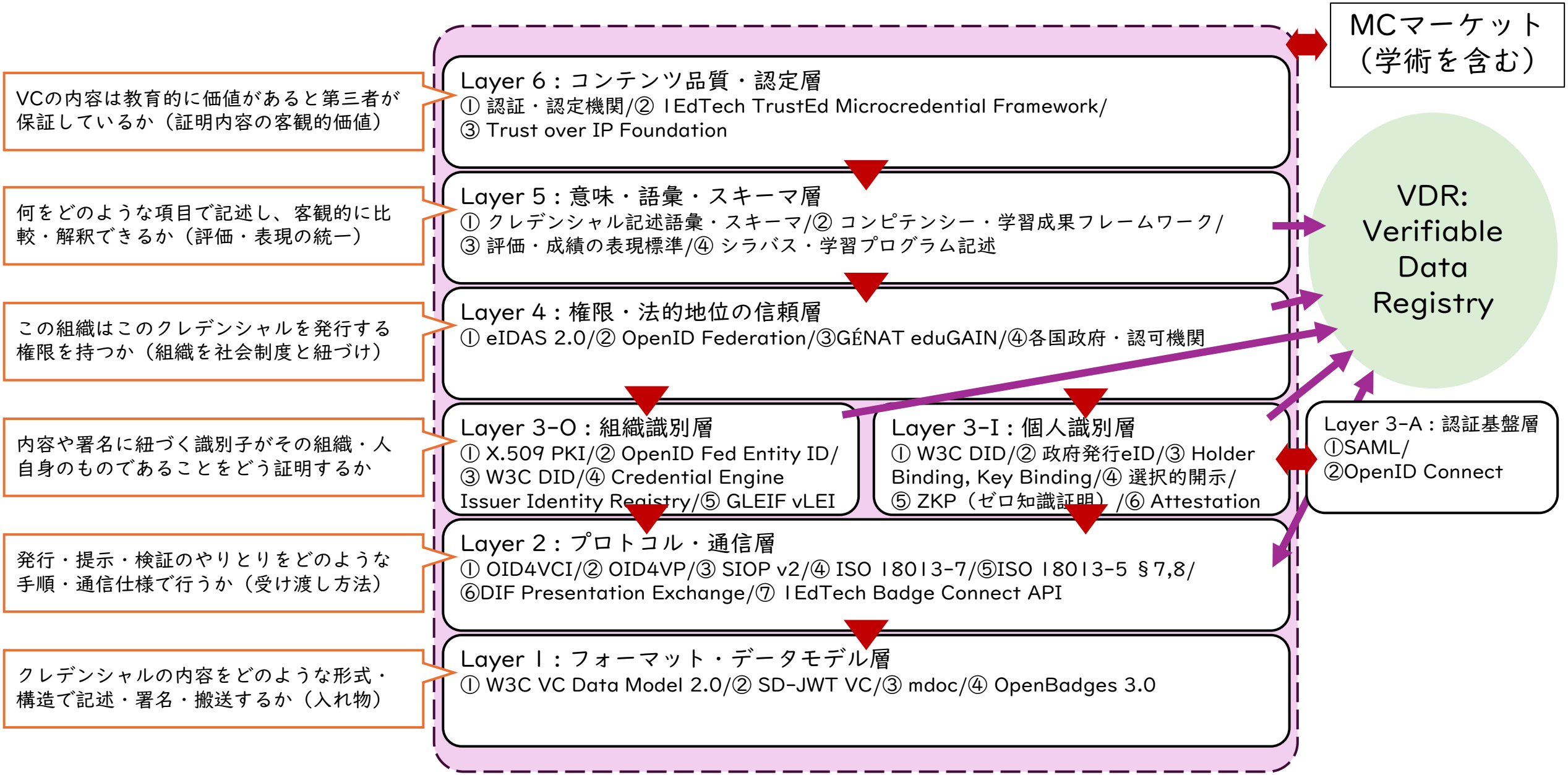
IHV型学術デジタル証明書基盤の事例-２

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？
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？）
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）

デジタル証明エコシステムの実現には、ガバナンス構造の構築が重要

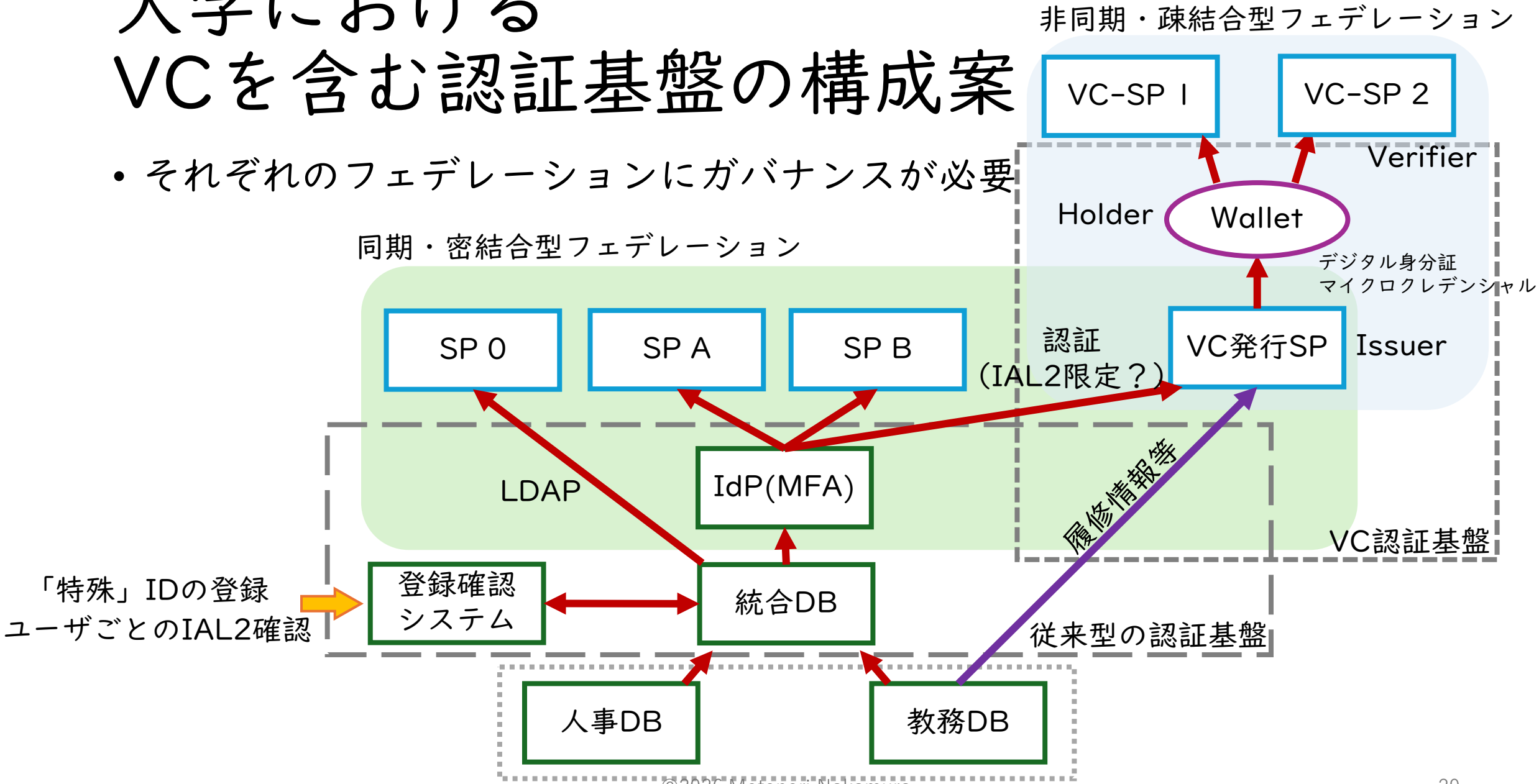
- 従来からの、発行者の制度的権威の具体的な表現（Issuerとしての正当性）と、その確実な検証（Verifier）の仕組みを実現することで、信頼構造がデジタル空間に移行できる。

  - 組織としての認定
  - 身分や資格の定義、共通化
  - 評価基準の統一、合意
  - VCフォーマットの統一、互換定義
  - トラストチェーンの設計
  - データ（個人情報）の制御設計（プライバシー保護など）
  - 識別子設計

  など

大学における 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



大学における共通VC基盤に向けた整理

外部エコシステム連携層 外部Verifier（他大学、企業、行政） / Trust Registry, eduID / 外部Issuer（他大学、民間資格） / Wallet
プロトコル・トランスポート層 VC発行 / VP提示・検証 / 委任型IHV,IV
クレデンシャルフォーマット抽象化層 フォーマット別モジュール / フォーマット間ブリッジ、クロスフォーマット同時提示
コアVC管理層 VC発行・失効管理、アルゴリズム / 同意・委任管理 / スキーマ・ポリシー管理
鍵・識別子管理層 鍵管理（HSM、更新、旧鍵保管） / 識別子管理（名寄せ、マッピング）
データソース統合層 在籍管理系システム連携 / 教務系システム連携 / データ変換・正規化 / 発行条件, データ正確性
インフラ・セキュリティ基盤層 PKI基盤 / データベース基盤 / 高可用性構成 / セキュリティ監視

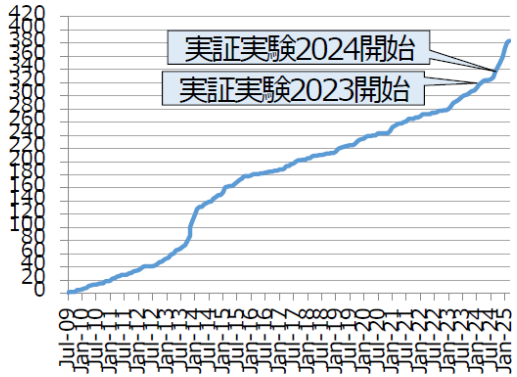
分散（フルメッシュ）型基盤整備の是非

- 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？

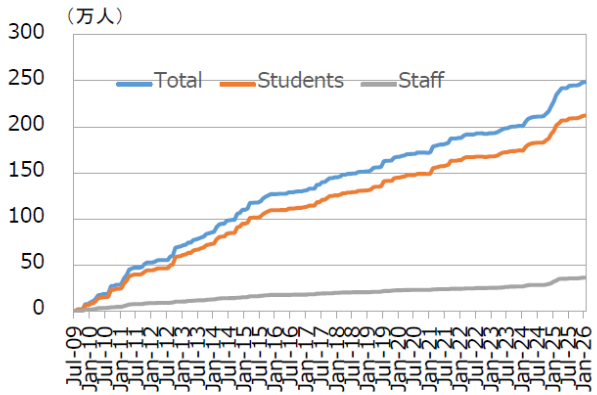
学認参加状況　（2026年1月末時点）

GakuNin

IdP機関数：398



ユーザ数（推計）：249万



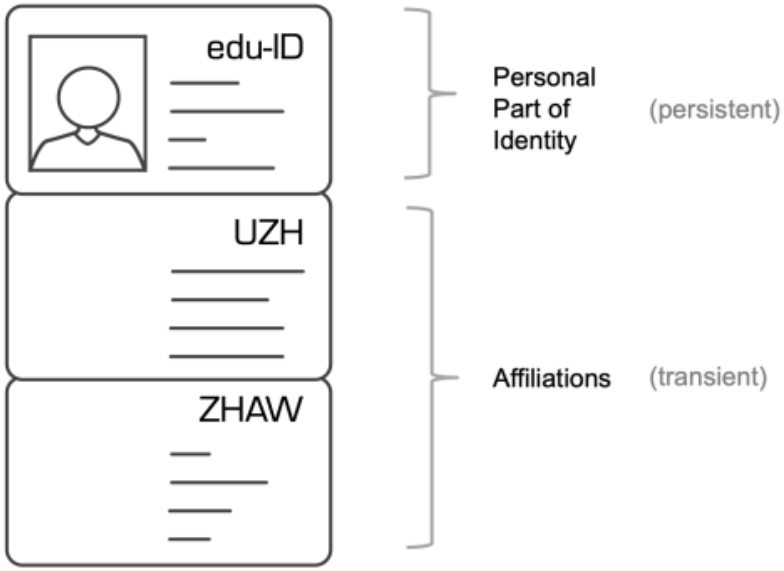
（IdP機関内訳）

	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

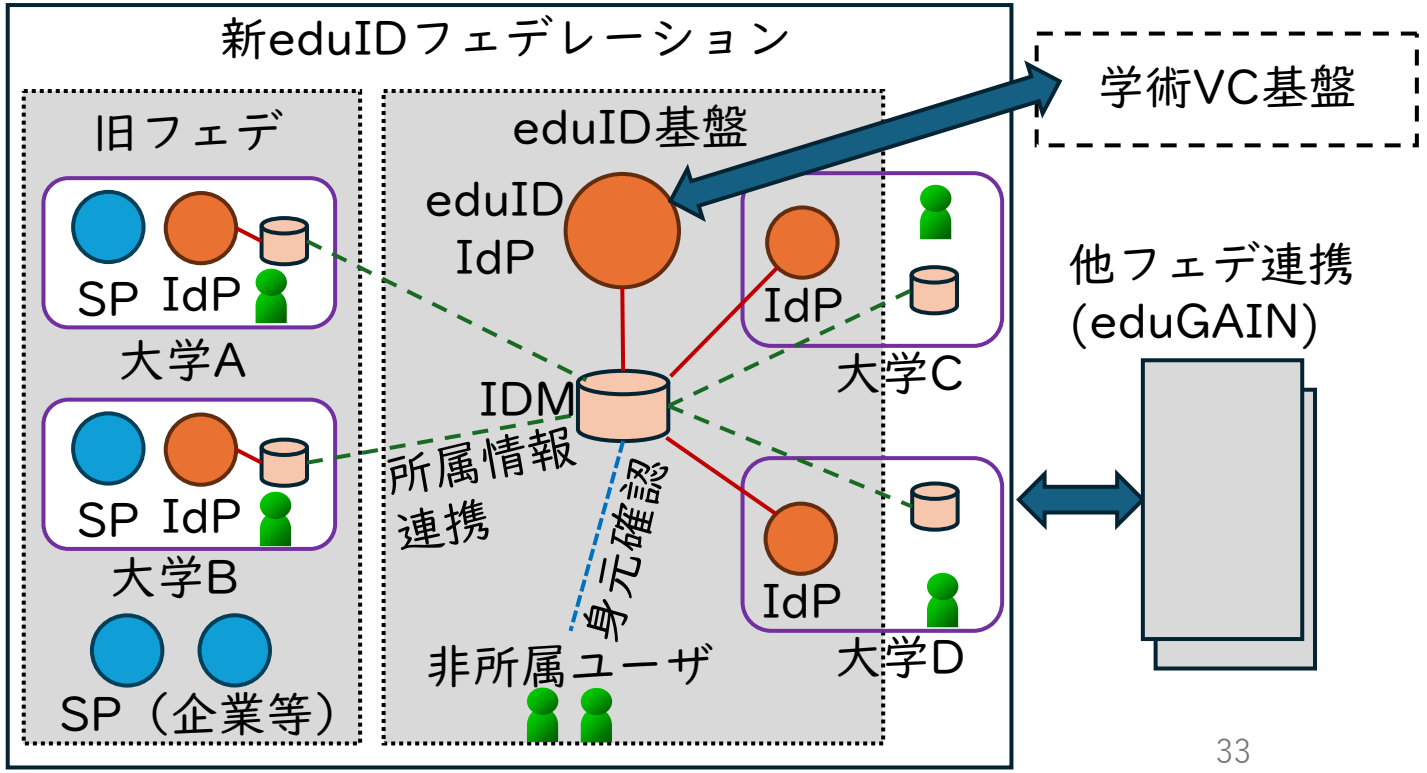
- 教育機関の枠を超えて個人に付与される永続的識別子
  - スイスやオランダ等においてeduIDとして基盤を構築・運用
  - 欧州学生ID（ESI）とリンク
- 特徴
  - 卒業後も維持される
    - 同窓会活動にも寄与する？
  - 本人管理のID＋機関から付与される属性
    - 国内や欧州域内等で有効な識別子として利用
  - VC/マイクロクレデンシャルと親和性が高い
    - というか、VC基盤の構築において重要



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

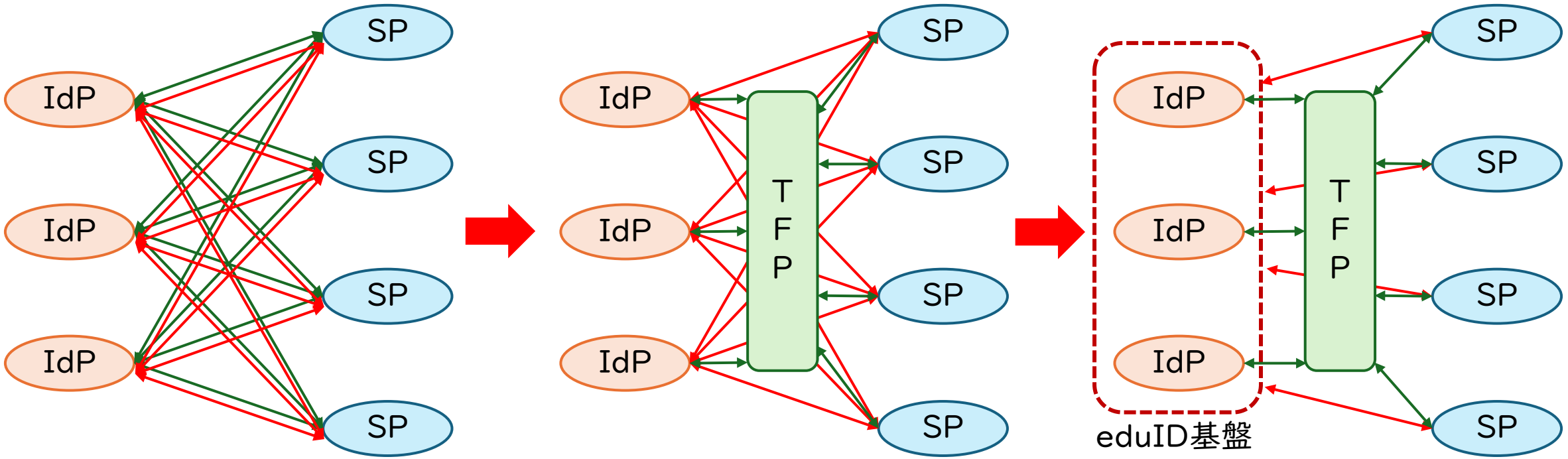
学認eduIDという方向性

- 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への期待

- 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

まとめ

- 大学の多様な活動を支える、これからの認証基盤

- 身分証・学修証明のデジタル化を支える基盤の役割

  - 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）