デジタルアイデンティティとトラスト

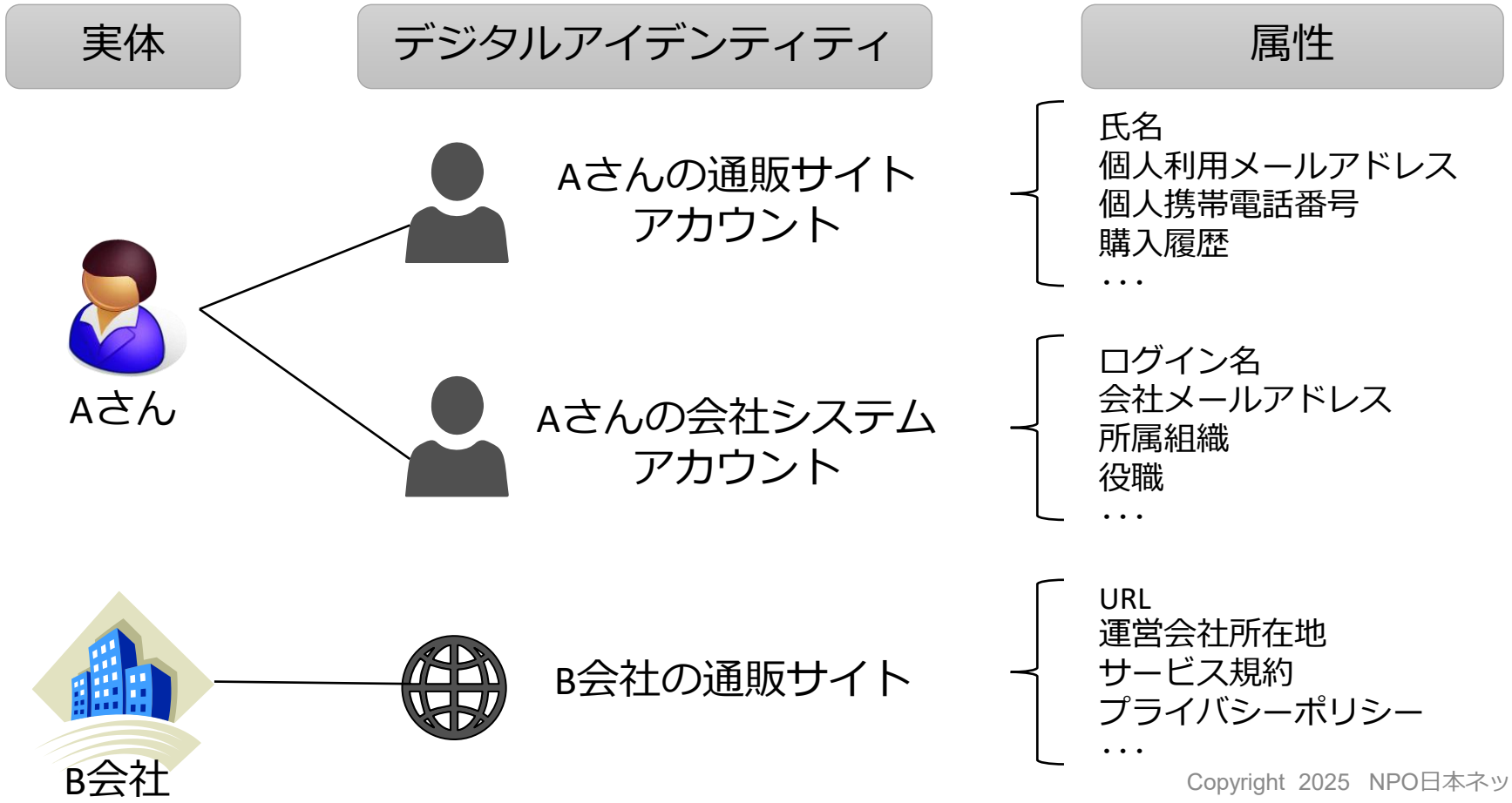
デジタルアイデンティティワーキンググループ
貞弘　崇行

本資料の構成

- デジタルアイデンティティとは
  - デジタルアイデンティティとは何か
  - デジタルアイデンティティを信じるには
- どうやって担保するのか
  - トラストフレームワーク
- フェデレーションからIHVモデルへ
  - IHVモデルにおけるトラストフレームワーク例

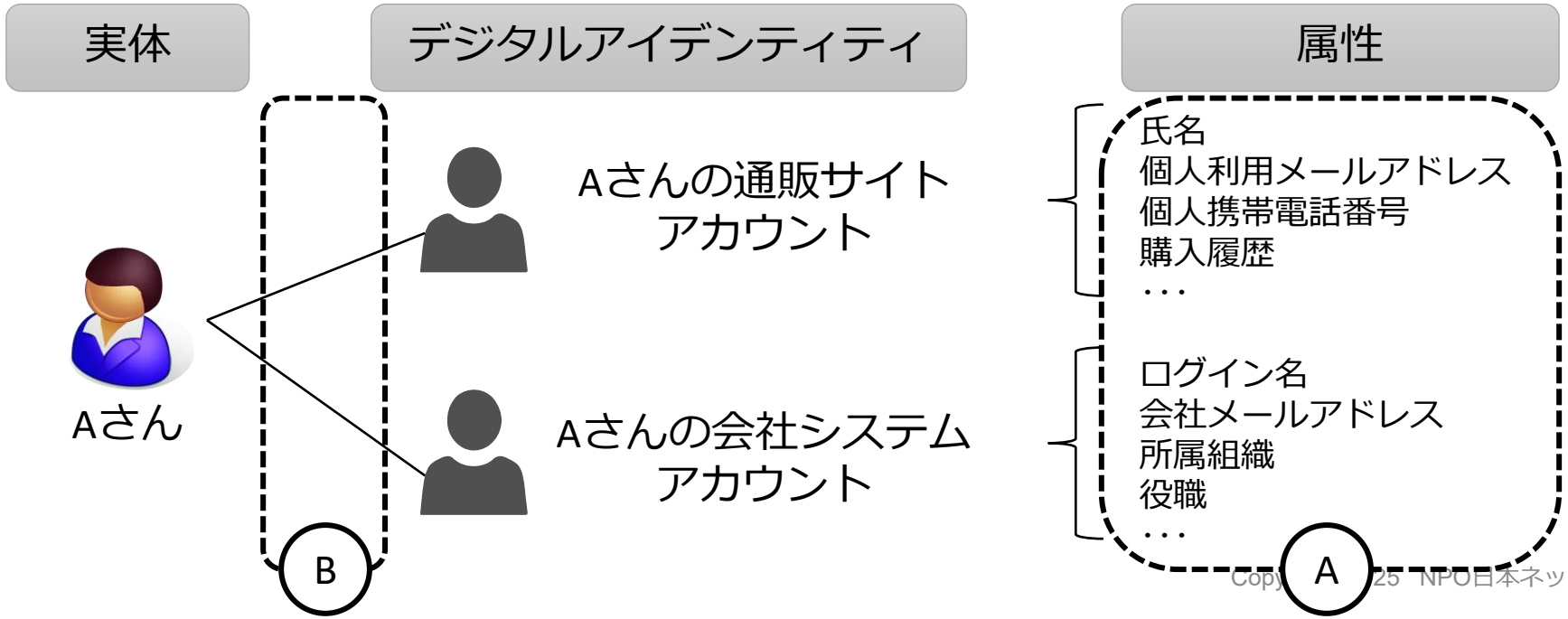
デジタルアイデンティティとは

- デジタルアイデンティティ（デジタルID）
  ＝実体に関する属性の集合体



デジタルIDを信じるには

- 属性は、本当にその実体に関する属性なのか？
  - A) デジタルIDの属性値
    ：そのデジタルIDは、その実体の属性と合致しているか？
  - B) デジタルIDとその実体の紐付け
    ：そのデジタルIDは、その実体によって使われているか？



デジタルIDを信じるには

- On the Internet, nobody knows you're a dog

引用：On the Internet, nobody knows you're a dog
https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

デジタルIDを信じるには

- そのデジタルIDは、その実体の属性と合致しているか？
  - デジタルIDのライフサイクル管理

    ：右図に示すデジタルIDのライフサイクルに沿って、デジタルIDの属性（有効・無効などの状態も属性の一つ）を最新に保つこと

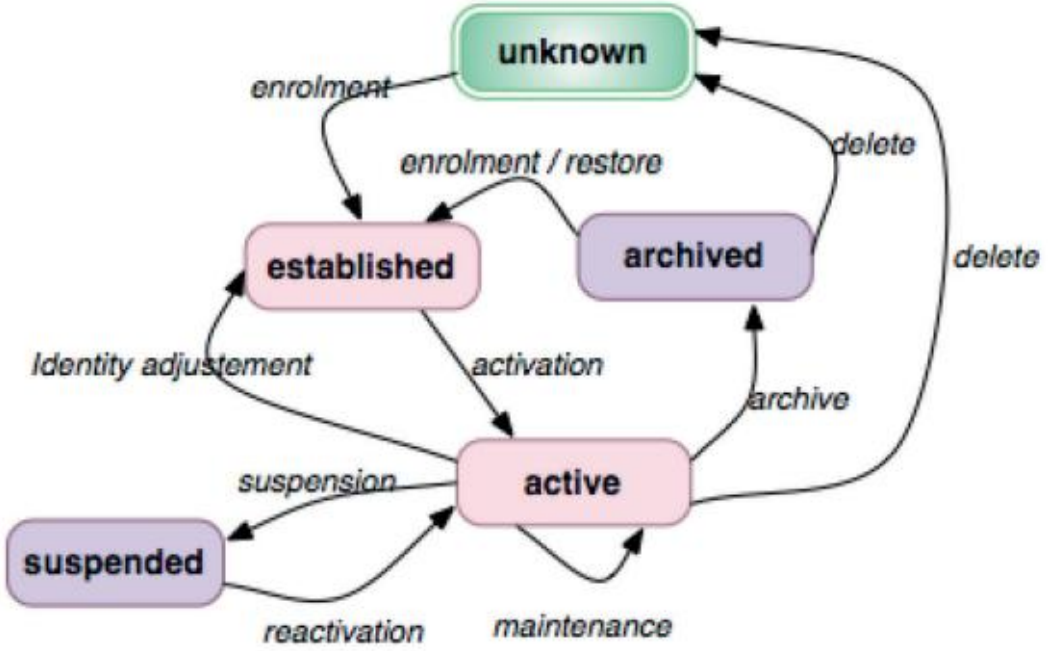


Figure 1 — Identity lifecycle

出典：ISO 24760-1 IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts

デジタルIDを信じるには

- そのデジタルIDは、その実体によって使われているか？
  - 認証

    ：デジタルIDと結合された認証器を保持し、制御できることを示し、そのデジタルIDに関連付けられた個人であることを示すこと

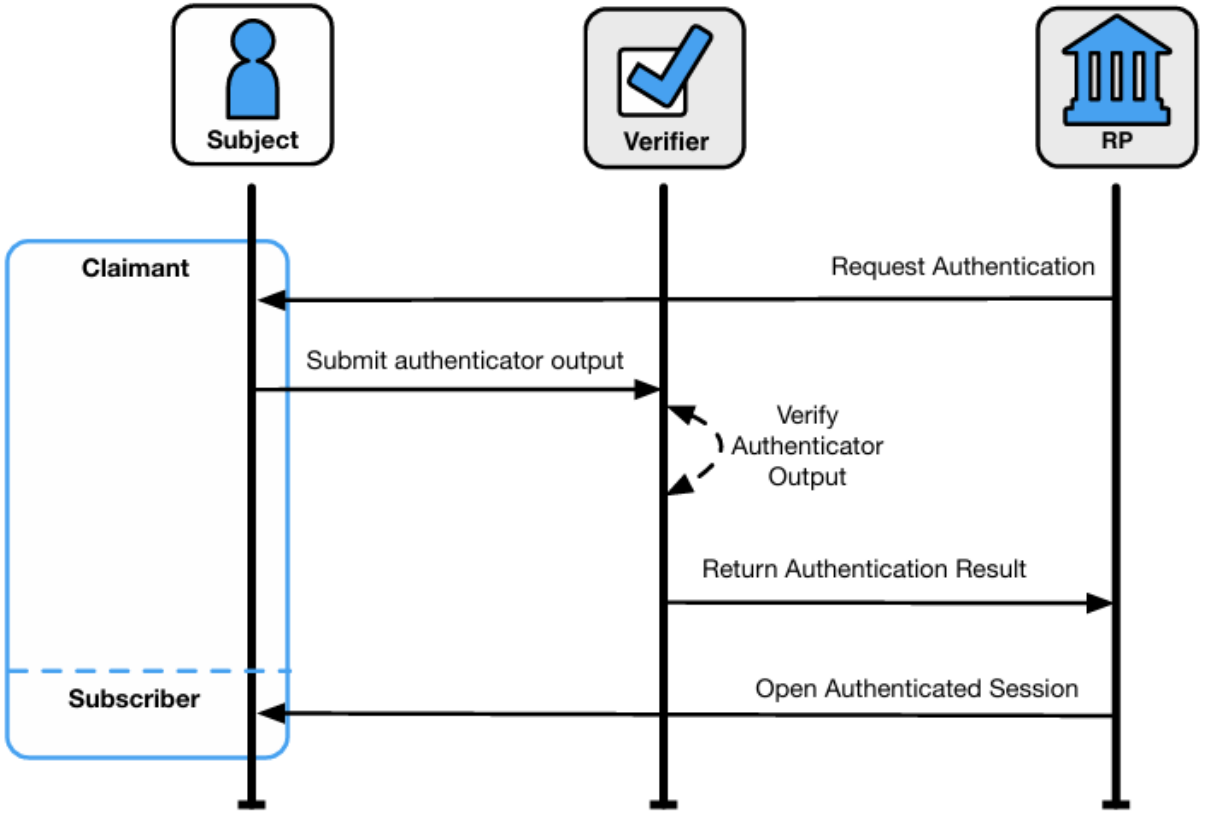


Fig. 2. Sample Authentication Process

出典：NIST Special Publication NIST SP 800-63-4 Digital Identity Guidelines

デジタルIDを信じるには

- ライフサイクル管理の保証度レベル：
  - 身元確認のレベル：NIST 800-63-4 IAL
  - 鮮度維持のレベル：普及したモノは無し

レベル	信頼度	本人確認の方法
IAL1	基本的	自己申告 or 信頼できる証拠を用いて確認。リモートまたは対面可
IAL2	高い	追加証拠の収集、強固な検証。リモートまたは対面可
IAL3	非常に高い	対面で訓練を受けた職員による対面確認＋生体情報の収集

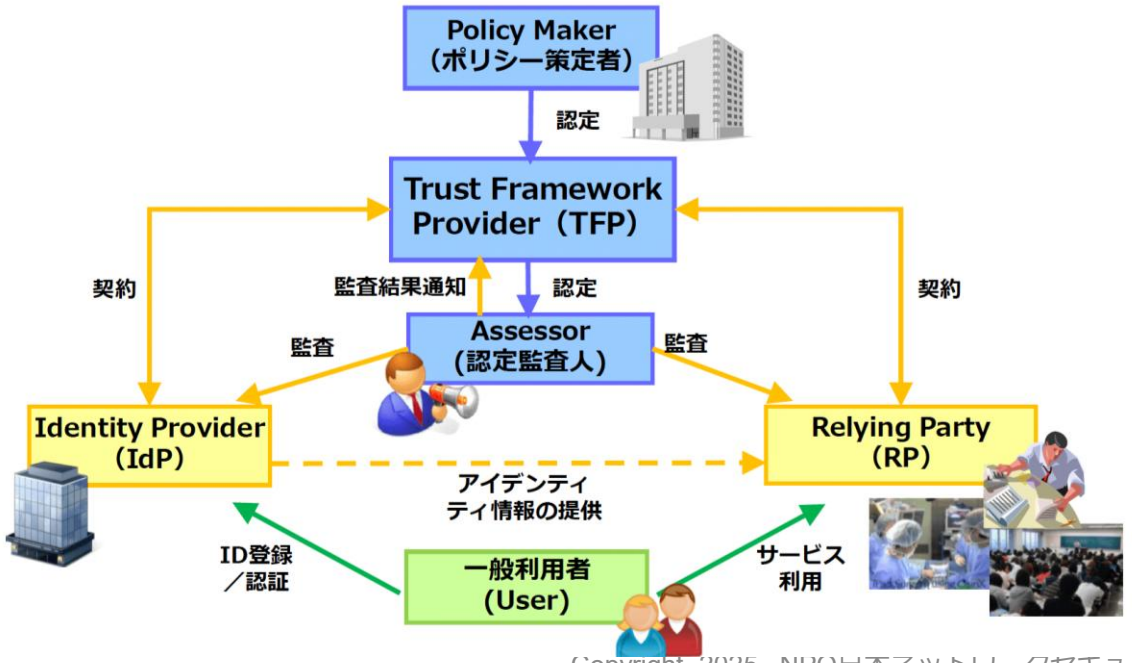
- 認証の保証度レベル： NIST 800-63-4 AAL

レベル	信頼度	認証器例
AAL1	基本的	パスワード / SMS / TOTP / Oauth
AAL2	高い	パスワード＋TOTP / パスワード＋ハードウェアトークン
AAL3	非常に高い	（フィッシング耐性あり）FIDO2 / WebAuthn セキュリティキー

どうやって担保するのか

- トラストフレームワーク
  ：各システムが一定のルールに従っていることを担保する仕組み

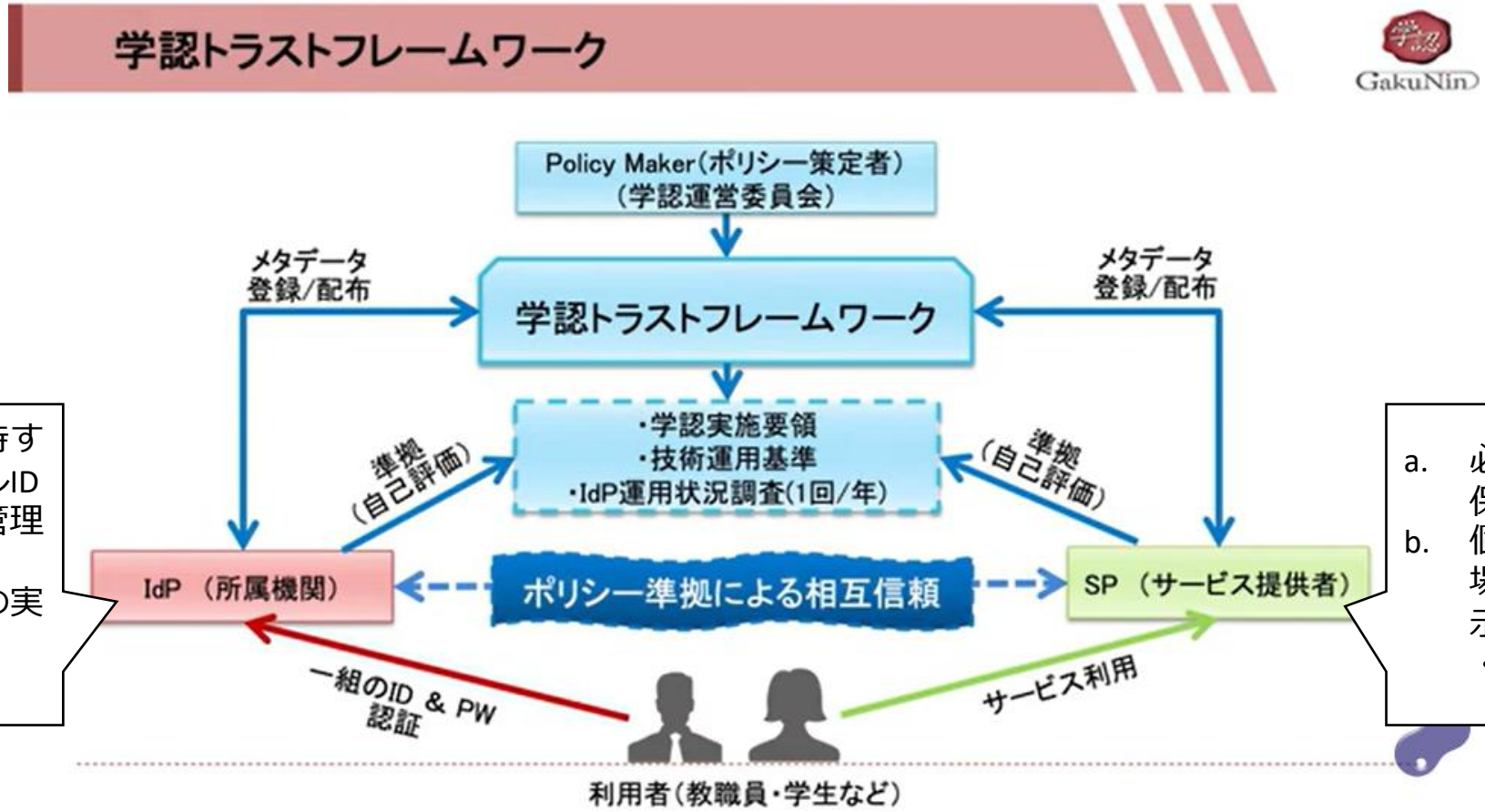
- トラストフレームワークの登場人物とその役割
  - （例　学生のデジタルID）



出典：「信頼フレームワーク」セミナー Vol.2 学生向けトラストフレームワーク資料より抜粋
https://www.slideshare.net/slideshow/student-identity-trust-framework-motonori-nakamura-shingo-yamanaka/12975967#7

どうやって担保するのか

- トラストフレームワーク事例としての学認



a. 一定の鮮度を維持する学生のデジタルIDライフサイクル管理実施
b. 一定強度の認証の実施
・・・

a. 必要最低限の情報の保持
b. 個人情報を保持する場合にはその旨の明示
・・・

出典：より「安全」で「効率的」な認証基盤を提供　学術認証フェデレーション
https://www.youtube.com/watch?v=KYLcH9-8e94

どうやって担保するのか

- トラストフレームワーク事例としてのGビズID

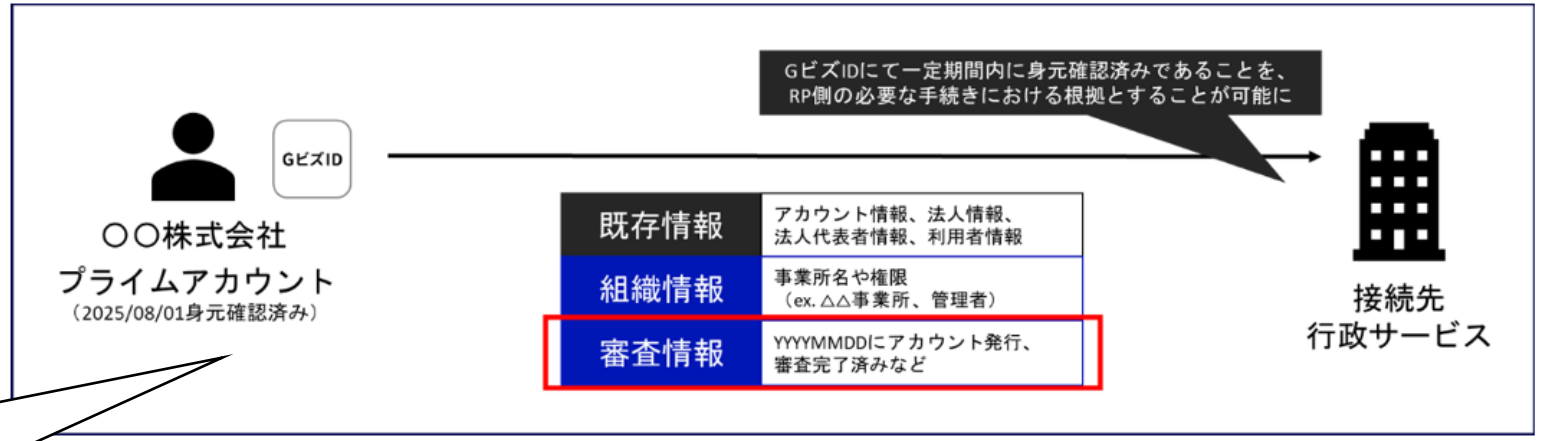


図 接続先行政サービスとの本人確認情報連携

（オンライン申請の場合）

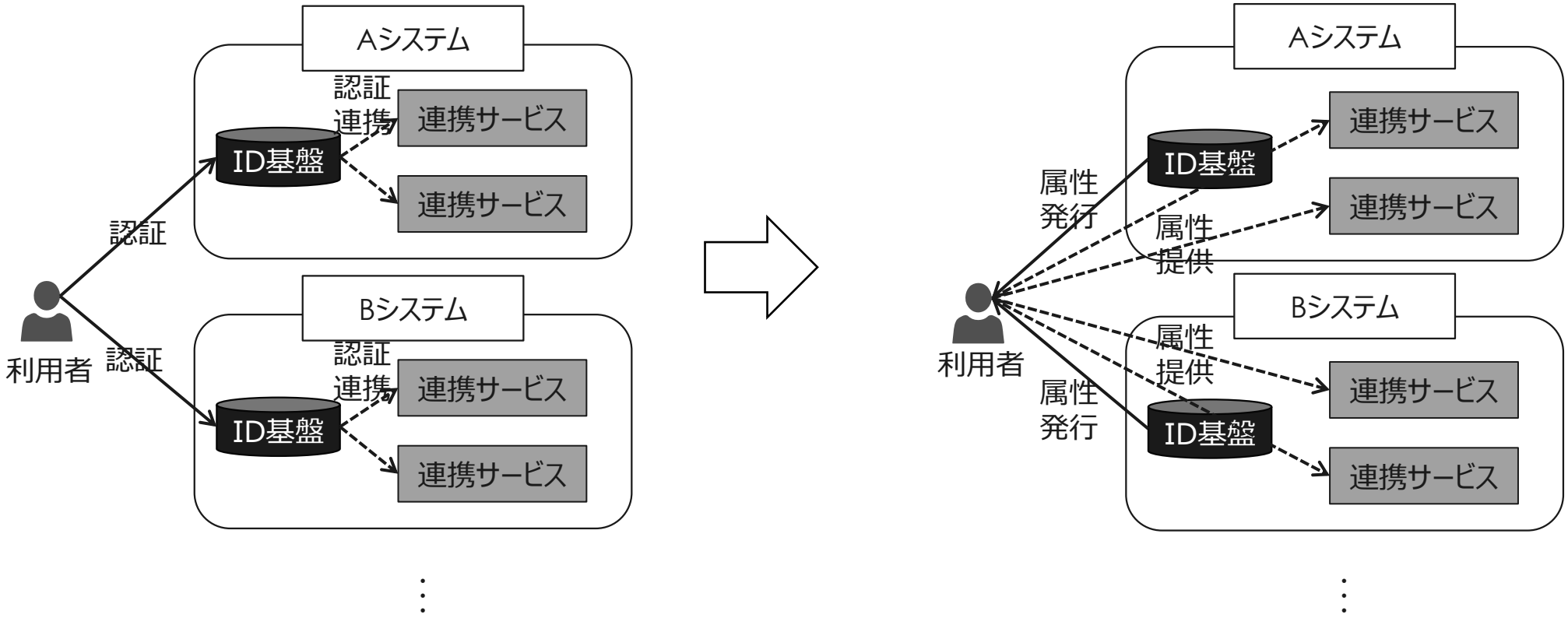
a. 法人代表者（＝プライム）アカウント登録時
    1. マイナンバーカードで個人の実在性確認
    2. 法務省管轄の登記情報システムで法人の実在性と代表者の一致確認

b. 法人代表者アカウント認証時
    a. パスワードのみ
    b. パスワード＋所有物
    ・・・

出典：法人共通認証基盤における トラストフレームワーク
https://gbiz-id.go.jp/top/trust_framework/trust_framework.pdf

フェデレーションからIHVモデルへ

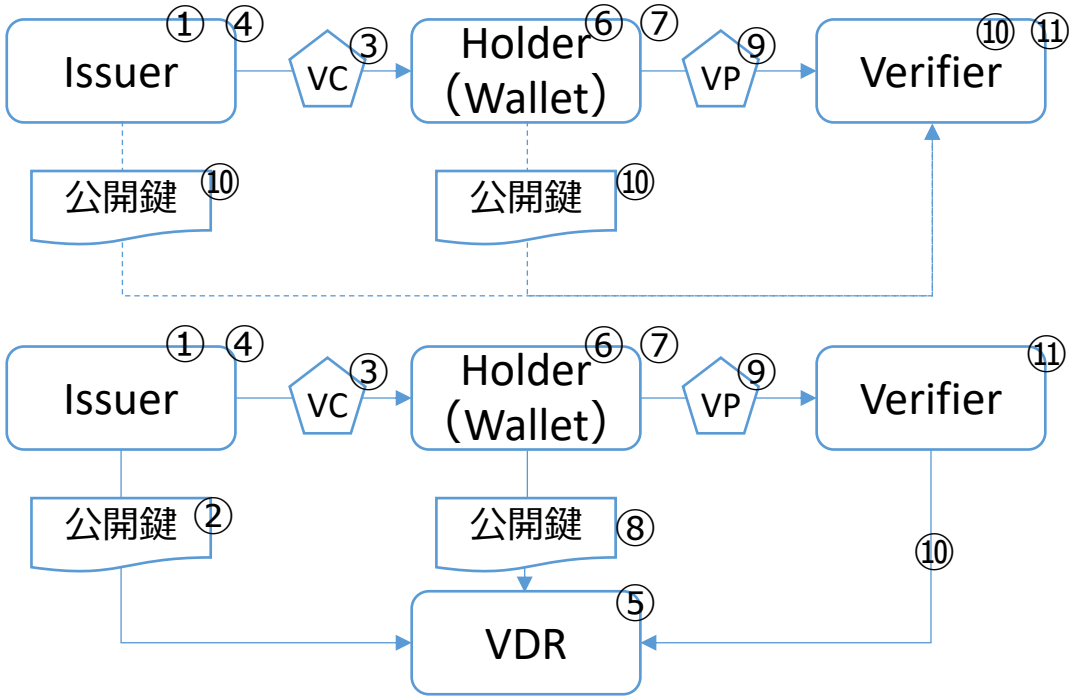
- 連携エコシステムの乱立・サイロ化を招くフェデレーションモデル
- 再利用可能な属性情報を利用し、サービス間の連携を促進するIHVモデル



フェデレーションからIHVモデルへ

- Verifiable Credentialに属性を載せる
  ：改ざんが検知可能、その発行者（作成者）が暗号的に検証可能

VC利用プロセス



VC利用プロセスの各アクション例

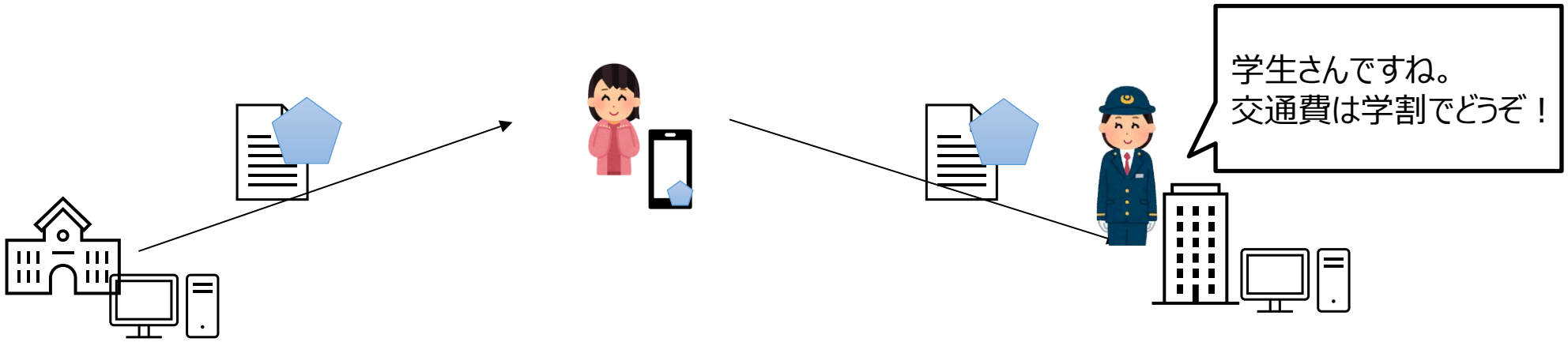
① Issuerが、適切な情報に基づき、VCを作成
② Issuerが、VDRに公開鍵を登録
③ Issuerが、Holderに対してVCを発行
④ Issuerが、発行済みのVCに対し、更新・失効等の管理を実施
⑤ VDRが、登録された鍵を保管・管理
⑥ Holderが、発行されたVCを保管・管理
⑦ Holderが、VCに署名しVPを作成
⑧ Holderが、VDRに公開鍵を登録
⑨ Holderが、VerifierにVP/VCを提示
⑩ Verifierが、受け取ったVP/VCをIssuer/Holderの公開鍵で検証
⑪ Verifierが、受け取ったVP/VCを保管・破棄

出典：Verifiable Credential (VC/VDC) の活用におけるガバナンスに関する有識者会議「VCに関連する各種制度等について」に基づき改変
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5a5c145f-85f4-41a5-bc51-4e442c6154b8/4c7ac849/20250310_meeting_verifiable-credential-governance_outline_04.pdf

フェデレーションからIHVモデルへ

- 以下は担保されていない
  - VCの発行元が適切であること
  - VCの格納先が適切であること
  - VCの発行先が適切であること

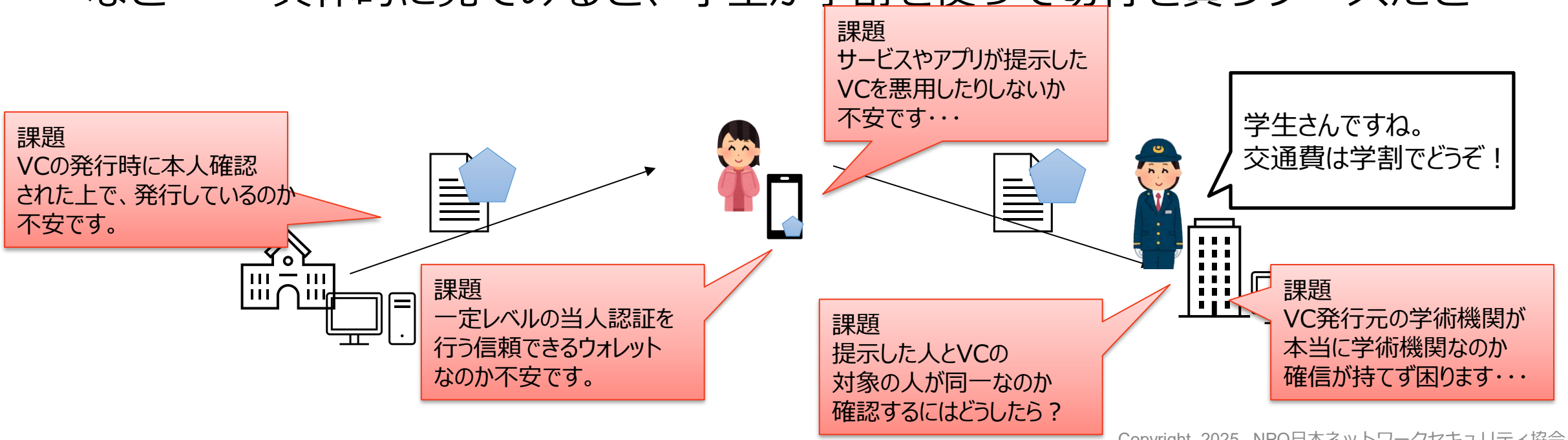
  など･･･　具体的に見てみると、学生が学割を使って切符を買うケースだと



フェデレーションからIHVモデルへ

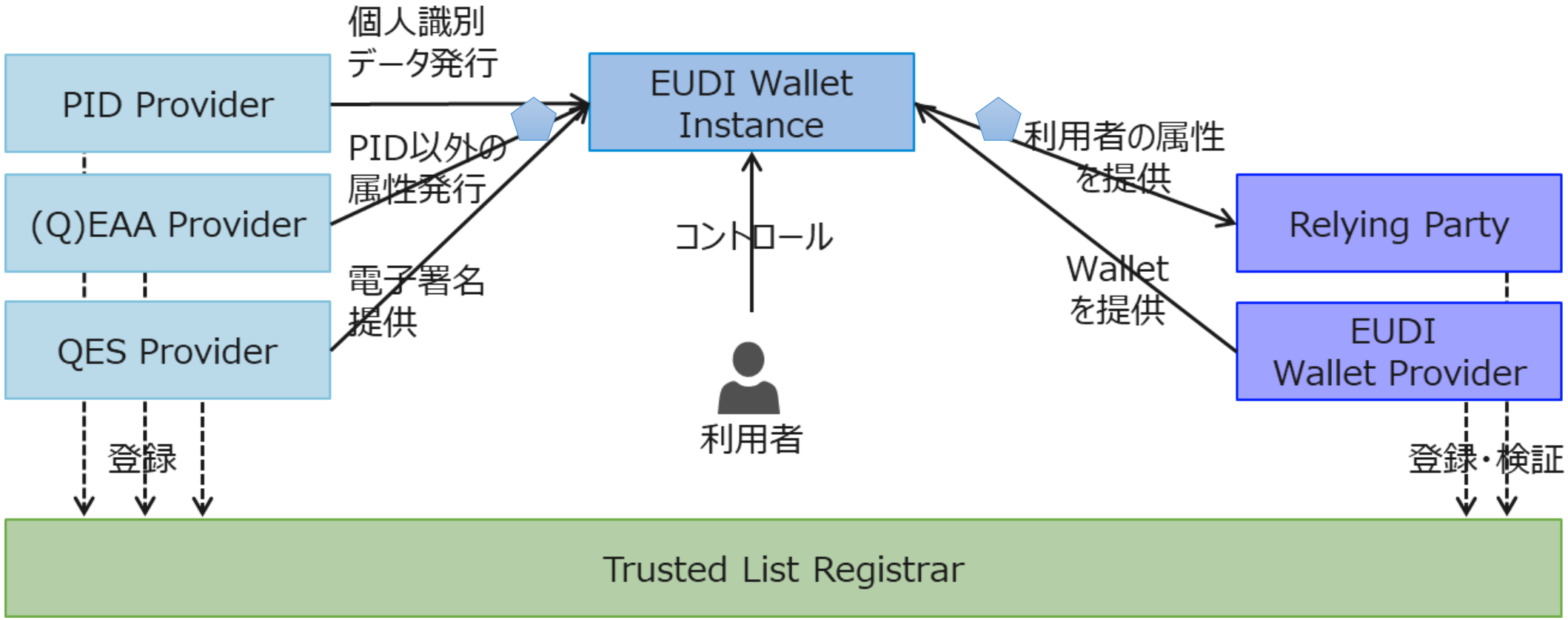
- 以下は担保されていない
  - VCの発行元が適切であること
  - VCの格納先が適切であること
  - VCの発行先が適切であること

  など･･･　具体的に見てみると、学生が学割を使って切符を買うケースだと



IHVモデルでのトラストフレームワーク例

- EUDIW ARF* 簡易構成



*：EU Digital Identity Wallet Architecture Reference Framework

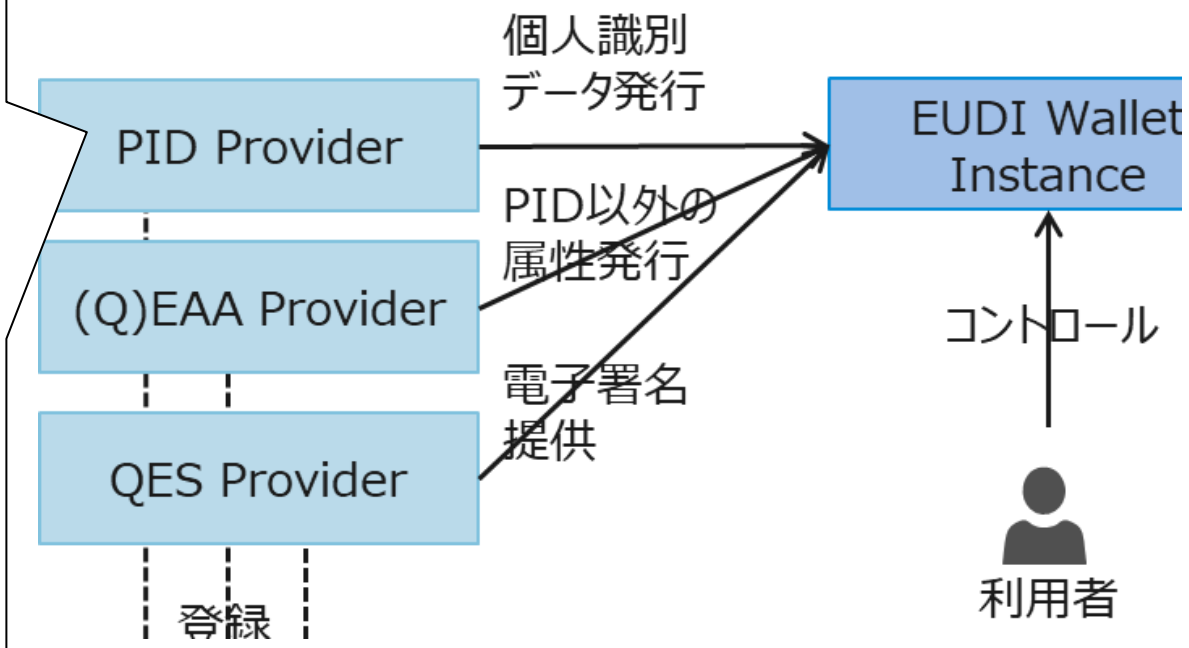
IHVモデルでのトラストフレームワーク例

- EUDIW ARF 簡易構成

#	コンポーネント	名称	説明
1	PID Provider	Personal Identification Data Provider	以下を行う主体。 ・高保証度でEUDI Walletの利用者や法人のアイデンティティを検証 ・共通フォーマットで個人識別情報（PID）をEUDIWに発行 （日本で言うところのデジタルマイナンバーカード的なモノ） ・PIDの有効性をRelying Partyが検証するための情報を提供
2	(Q)EAA Provider	(Qualified) Electric Attestation of Attribute Provider	EUDIWの利用者についての属性を発行する主体。より厳格な管理要件を満たす場合には「Qualified」が付く。
3	QES Provider	(Qualified) Electric Signature/Seal Provider	リモート電子署名を生成する主体
4	Relying Party	–	自然人もしくは法人。EUDIWに格納されたPIDやEAAといった属性を利用してサービス提供する主体
5	EUDI Wallet Provider	–	EUメンバー国、もしくは、そのメンバー国によってEUDI walletを作成することになった組織
6	Trusted List Registrar	–	Wallet ProviderやPID Providerなどの公開鍵と識別子の組み合わせの形でトラストアンカーを提供するTrusted Listの維持と発行を担う主体。

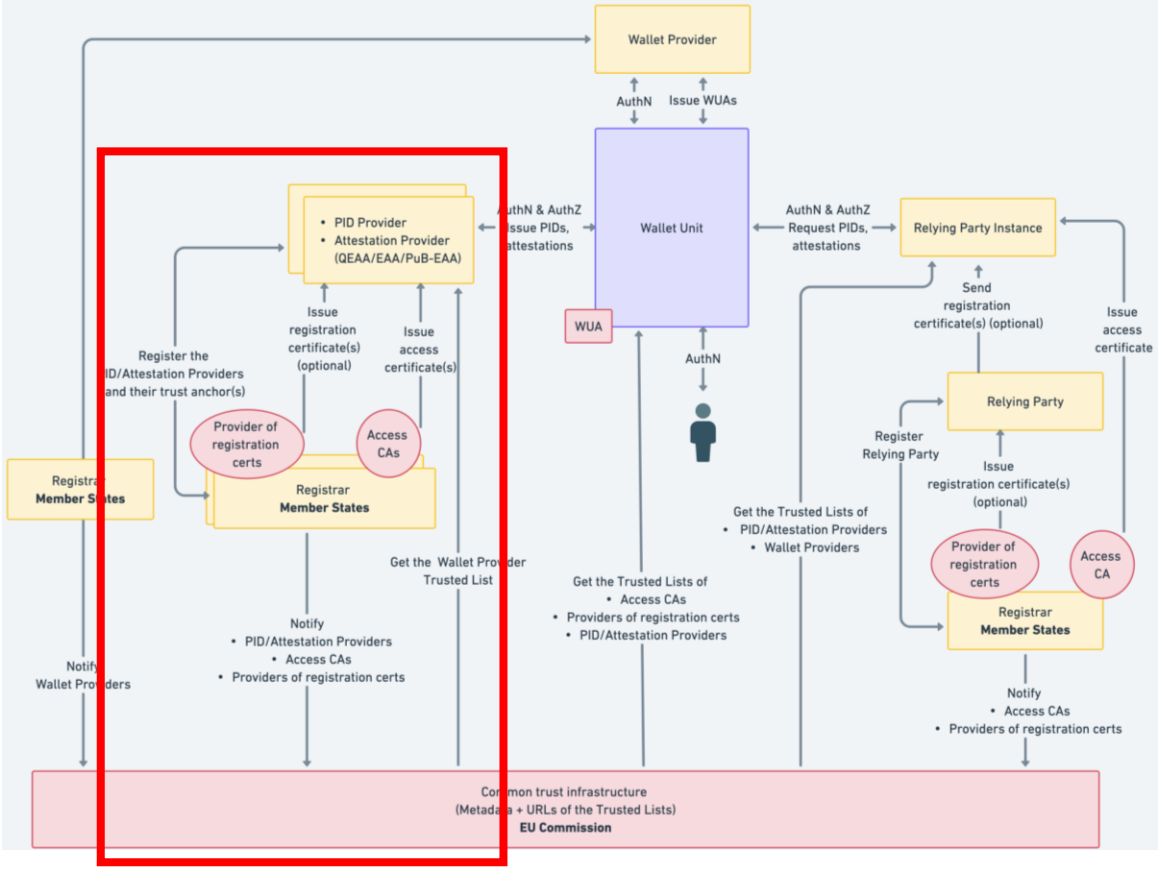
IHVモデルでのトラストフレームワーク例

- PID Providerが遵守すべき項目
  - （EUDIW PID rulebook、高レベル要件より）
  - PIDに含めるべき情報
    - 必須属性：姓、名、誕生日･･･
    - 任意属性：住所、居住国、顔写真･･･
    - 必須メタデータ：有効期日、発行者、発行国
      ･･･
  - PID Providerとして果たすべき役割
    - ISO 18013-5, SD-JWT VC両方の形式で発行出来なくてはならない
    - 発行対象となる人を高い保証度で本人確認しなくてはならない
    - 別途定められる仕様に沿って、発行したPIDの失効ステータスを公開する
    - 発行したPIDは、ウォレットとbindされていなくてはならない
      ･･･



IHVモデルでのトラストフレームワーク例

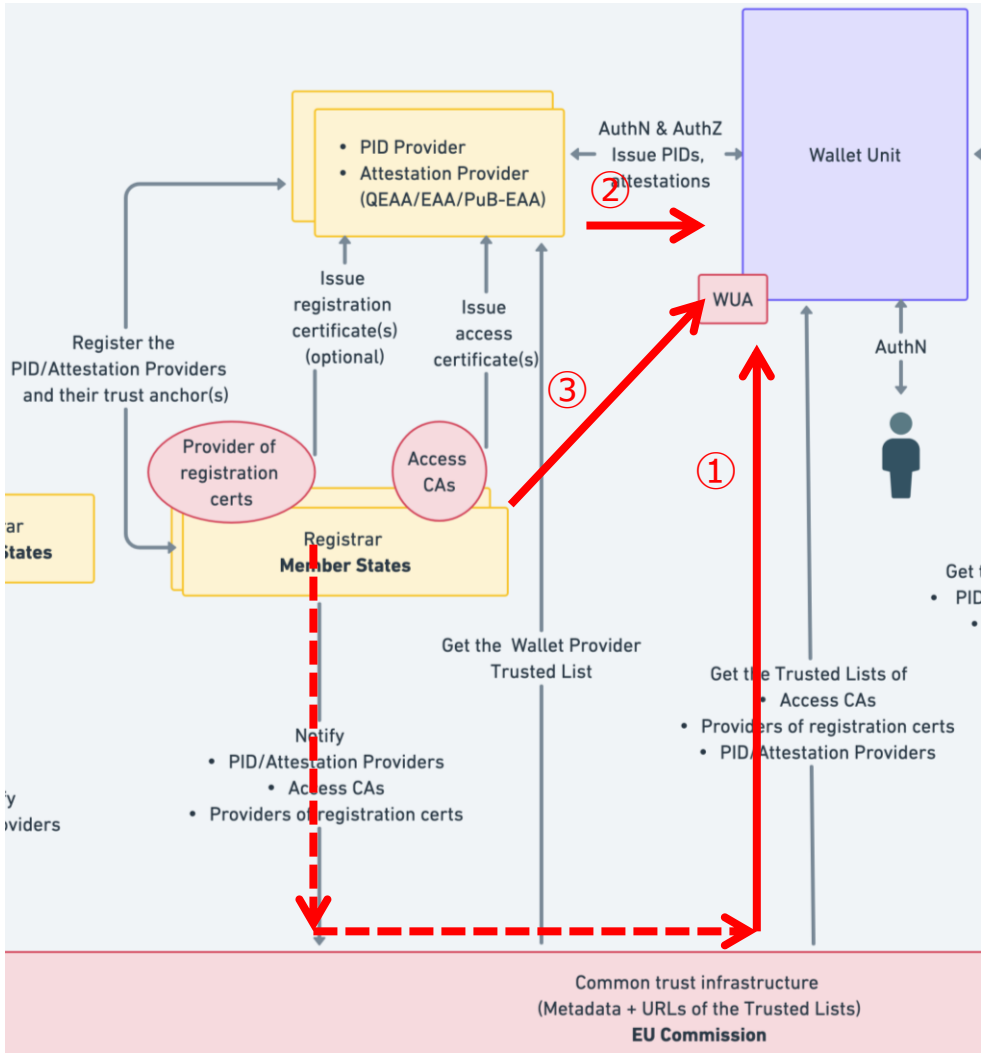
- ウォレットインスタンスがPID ProviderやEAA Providerを認証する仕組み
- 加盟国における信頼リストレジストラがPID ProviderやEAA ProviderをTrusted Listsへ登録し、欧州委員会への通知が終わると以下が生じる
  - 登録と通知は右図赤枠部分
  - PID ProviderやEAA Providerについての情報が登録される（例　発行できるEAAの種類）
  - PID ProviderやEAA Providerは、アクセス証明書と登録証明書を受け取る
  - PID ProviderやEAA Providerのトラストアンカー（＝公開鍵＋識別子）はTrusted Listに登録される



出典：EUDIW Architecture and Reference Framework, figure 11から抜粋

IHVモデルでのトラストフレームワーク例

- ウォレットインスタンスがPID ProviderやEAA Providerを認証する仕組み
  - ①　（前提として）ウォレットインスタンスはTrusted Listからアクセス証明書の証明局Trusted Listを取得しておく
  - ②　（PIDやEAAを取得する前に）ウォレットインスタンスはPID ProviderやEAA Providerが提示するアクセス証明書を発行者メタデータから取得
  - ③　ウォレットインスタンスは提示されたアクセス証明書の発行元証明局が、信頼リストに含まれることを確認
  - PID ProviderやEAA Providerは、Registrarが登録したPID ProviderやEAA Providerである
  - 信頼のルート
    - 加盟国での信頼リストレジストラでの登録
    - 欧州委員会での登録された情報の通知と発行



出典：EUDIW Architecture and Reference Framework, figure 11から抜粋

IHVモデルでのトラストフレームワーク例

- EUDIW ARFが規定するのは一部のみ
  - PID Provider
    - PIDは加盟国の自然人あるいは法人のデジタルアイデンティティ
    - 発行時の手続きやステータス管理についてはARFにもある程度明記されている
    - VCの利用者側はこれらの事項が遵守されていることを信頼できる
  - （Q）EAA Provider
    - 業界や業種ごとに必要なライフサイクル管理や認証の強度は異なる
    - ARFには特に定めは無い
    - 業界や業種ごとに追加のトラストフレームワークが必要

まとめ

- デジタルアイデンティティとは、実体の属性の集合
- デジタルアイデンティティを信じるには、以下が必要
  - デジタルアイデンティティの属性が実体に沿っていること
  - デジタルアイデンティティが実体によって使われていること

- 上記を担保する仕組みとして、トラストフレームワークがある
  - トラストフレームワーク内のシステムが一定のルールに従っていることを担保

- デジタルアイデンティティ利用はフェデレーションからIHVモデルへ
  - IHVモデルにおいてもトラストフレームワークは適用可能