Trusted Web の実現に向けたユースケース実証事業
成果報告書

学修歴等の本人管理による人材流動の促進

2023 年 3 月 24 日（提出日）

代表機関：東京大学

SSI/FIDO コンソーシアム

内容

1　背景と目的

東京大学では、国内・国外にわたる入進学、留学、就職等に係る手続きの精度と効率と利便性を高めるため、学修歴(マイクロクレデンシャルおよびマクロクレデンシャル)の電子証明の必要性を認識し、全学 DX の一環として、大学の構成員(学生、教職員など)および他の関係者(卒業生や名誉教授)を認証する仕組み等とともに検討してきた。マイクロクレデンシャルは個々の科目の履修等に関する証明、マイクロクレデンシャルは卒業証明や全科目の成績の証明であり、生涯学習等のサービスにはマイロクレデンシャル、留学や就職に係る事務にはマクロクレデンシャルが用いられるが、大学にとってはいずれも重要であり、両方の実運用に関する検討を進めている。

また、ヤフー株式会社と東京大学は、FIDO (Fast Identity Online) 認証に関する共同研究において、FIDO Notary (後述)という仕組みを考案し、FIDO 認証と検証可能属性証明(Verifiable Credentials, VC)との組み合わせによる自己主権 ID(SSI)の実装等について検討してきた。その検討結果を上記の学内での取り組みに生かして学修歴証明の実運用に貢献することを目指している。

そこで本事業では、大学等が発行した検証可能な学修歴を学習者本人が管理し、企業等の要請に応じてそれを開示し、企業等がそれを検証して選考等に用いる、という一連のワークフローを実現することを目的とする。

一方、検証可能でないものを含むさまざまな属性情報を本人が他者に開示せず安全にフル活用すること(分散マッチング)によって個人の属性情報の最大の付加価値が生み出されると期待される。たとえば、学習者が就職先・転職先の候補である企業等を選ぶ際に学修歴等を他者に開示せずに企業のカタログと手もとでマッチングすることが考えられる。本事業はこのような分散マッチングに基づく事業の準備に当たる。

2　事業の概要

2.1　事業概要及び実証の範囲

学修歴等の属性情報を学習者本人が自ら管理し大学等や企業等とやりとりすることにより、進学・就職・転職・昇進等における安全で公正なデータの利活用を促進する。この仕組みにより、進学や留学の際の手続きを容易にするとともに労働市場の流動性を高めることを目的とする。この目的に対し、業界標準に則りながら、Verifiable Credential (VC), Verifiable Presentation (VP) を核として、大学等を発行者、採用企業等を検証者として、学習者本人が検証者の要請する属性を含む VP を、大学等が発行した VC から作成して開示するシステムを構築し、PoC を行う。このシステムは企業等からの開示要請に対する学習者の同意の自動化を含み、PoC はこれを含めた全体のワークフローを検証する。

2.2　社会・経済に与える価値・影響

学修歴証明サービスは学修歴の発行者から利用料を徴収するものが多い。たとえば(一社)オープンバッジ・ネットワークが提供する学修歴証明サービスは 50 万円/年の利用料で証明書を発行し放題、Digitary 社の学修歴証明サービスは基本料金が年間 480 万円で証明書を 6 万回発行でき、それを越えると証明書の発行 1 回につき 80 円かかる。前者はマクロクレデンシャルだけでなくマイクロクレデンシャルの運用にも適する可能性があるが、署名用秘密鍵をサービス運用事業者が管理するので証明書の

真正性に疑義を生ずるリスクがあるなど改善すべき点がある。後者は発行者にとってマイクロクレデンシャルを運用するコストが大きすぎるのではないか。以上より各証明書発行者の年間利用料を 100～500 万円とすれば、国内での潜在的利用者が 3 万団体(国内の小学校が約 2 万校、中学校が約 1 万校、大学が約 790 校、専門学校が約 2800 校)として潜在市場規模は 300 億～1,500 億円と推計される。

一方、就職・転職等に関する分散マッチング(属性情報を他者に開示しないマッチング)に基づく人材仲介サービスは従来のサービスよりも安全で使い勝手が良く労働市場の流動性を高めると期待されるので、その潜在市場規模は現在の市場規模(2021 年度の人材派遣、人材紹介、再就職支援の市場規模は合計約 9.5 兆円で、そのほとんどが人材派遣である。cf. 人材派遣ー労基旬報 2022-11-09: https://roukijp.jp/?p=3655)を上回ると考えられる。

このように、学修歴等の属性情報を学習者本人に集約することにより、安全で利便性の高い学修歴証明サービスが実現できるだけでなく、そのサービスを就職・転職等に関する分散マッチングに拡張することにより、労働市場の流動性を高めることができると考えられる。また、分散マッチングは就職や転職にとどまらず他のサービスや物販にも拡張できる。

2.3　コンソーシアムの体制

本コンソーシアムは、東京大学を代表機関として、同大学とヤフー株式会社から構成される。東京大学は実証全体の統括及び VC と Verifiable Presentation (VP)の生成・検証機能、Verifiable Data Registry (VDR)、およびウォレットの開発と結理テストの役割を担う。ヤフー株式会社は FIDO Notary および VDR の設計を担う。ウォレットと FIDO Notary の開発はそれぞれ(有)アリゾナデザインと富士ソフト(株)に委託する（図 2.3-1）。

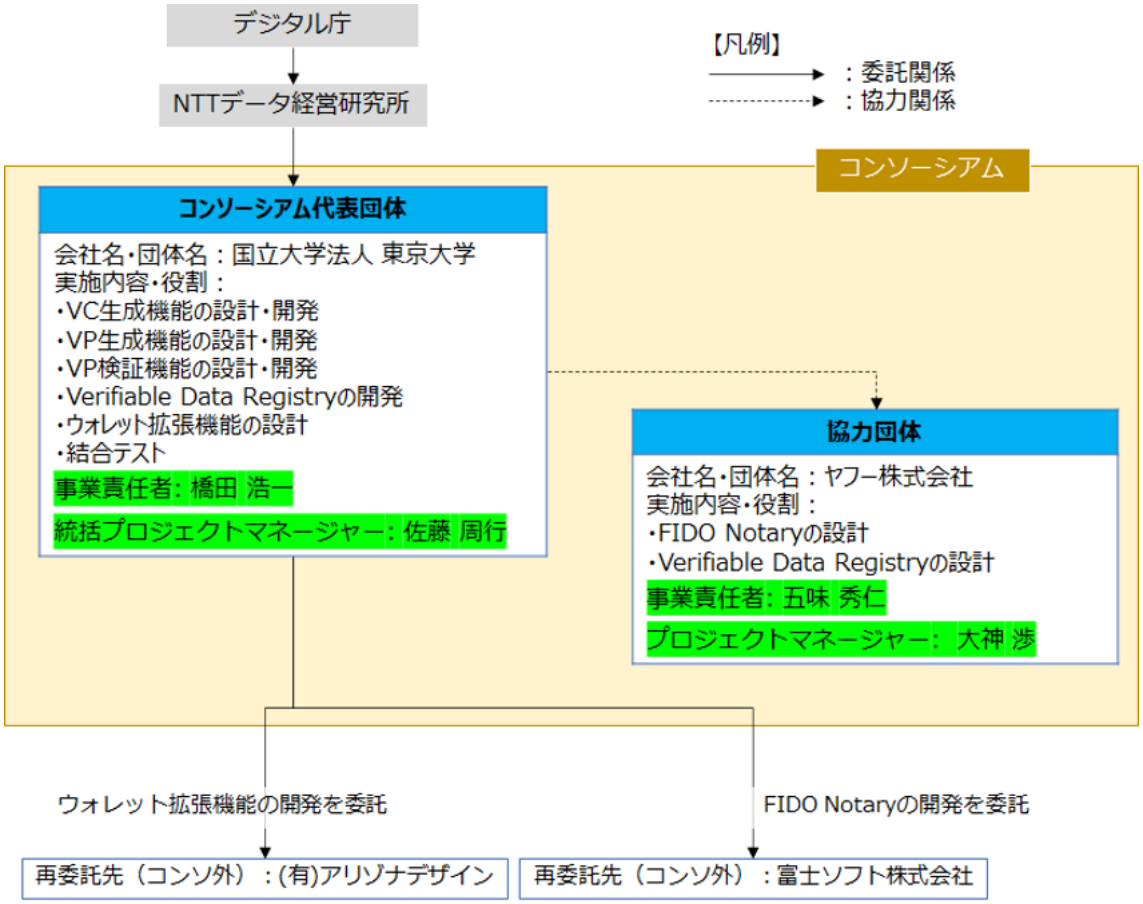
デジタル庁
NTTデータ経営研究所
【凡例】
：委託関係
：協力関係
コンソーシアム
コンソーシアム代表団体
会社名・団体名：国立大学法人 東京大学
実施内容・役割：
・VC生成機能の設計・開発
・VP生成機能の設計・開発
・VP検証機能の設計・開発
・Verifiable Data Registryの開発
・ウォレット拡張機能の設計
・結合テスト
事業責任者: 橋田 浩一
統括プロジェクトマネージャー: 佐藤 周行
協力団体
会社名・団体名：ヤフー株式会社
実施内容・役割：
・FIDO Notaryの設計
・Verifiable Data Registryの設計
事業責任者: 五味 秀仁
プロジェクトマネージャー: 大神 渉
ウォレット拡張機能の開発を委託
FIDO Notaryの開発を委託
再委託先（コンソ外）：(有)アリゾナデザイン
再委託先（コンソ外）：富士ソフト株式会社

図 2.3-1 実施体制図

2.4　実証全体のスケジュール

図 2.4-1 に本事業全体のスケジュールを示す。

実施事項			R4								R5				
大項目	小項目	担当	9月		10月		11月		12月		1月		2月		3月
実施計画書の作成															
アプリケーション企画															
	要件定義	東大+ヤフー													
	基本設計	東大+ヤフー													
開発環境の構築															
	クラウドサーバの設定	東大													
アプリケーション開発															
	VC生成機能	東大													
	VP生成機能	東大													
	VP検証機能	東大													
	Verifiable Data Registry	東大													
	FIDO Notary	富士ソフト													
	ウォレット拡張機能	アリゾナデザイン													
	機能の結合テスト														
デモ動画の制作															
	動画シナリオの作成	東大													
	撮影（キャプチャ）	東大													
成果報告書の作成		東大+ヤフー													

図 2.4-1 実証全体のスケジュール

3　実証内容

3.1　実証の実施事項、論点及び判断

✧　　3.1.1 プロトタイプの企画・開発

東京大学とヤフー株式会社は、FIDO 認証に関する共同研究において、FIDO Notary という仕組み(FIDO 認証の機能の一部をマイクロサービス化したもの)を考案し、FIDO 認証と検証可能属性証明(VC)との組み合わせによる自己主権 ID(SSI)の実装等について検討してきた。また、東京大学では分散 PDS ライブラリである PLR (Personal Life Repository)を開発してきており、それを属性証明用のウォレットとして用いる構造を兼ねてより持っていた。本実証実験では、図 3.1.1-1 に示すように、FIDO Notary で FIDO 認証を SSI に導入し、全体のサービスを PLR の形で学習者に提供する。具体的な実施事項、論点とその判断を表 3.1.1-1 にまとめる。

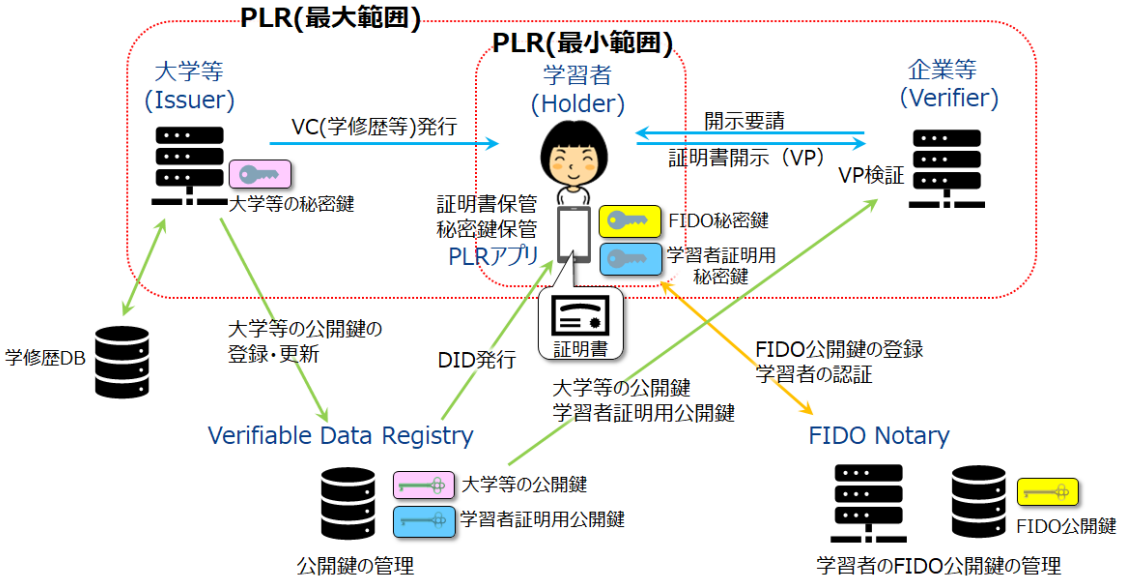

図 3.1.1-1 構築するプロトタイプの全体像

表 3.1.1-1 実施事項、論点とその判断

実施事項	論点	判断
要件定義	FIDO Notary	FIDO 認証トラストモデル(認証サーバの origin のみが認証要求し、認証に成功したユーザしか秘密鍵にアクセスできない)を採用しつつ、VC のトラスト性を高めるため、大学等とは別の主体として学習者を認証する主体として採用。
	エンティティの実現	Issuer、 Verifier、Holder の間で属性情報の安全なやり取りをサポートするためのウォレットとして PLR を採用。VDR (Verifiable Data Registry)として今回はパブリックチェーンに対応する必要がないため、公開を前提としたRDB (関係データベース)及び WEB API、VP 署名検証形式(BBS+)に対応した署名機能を提供する

		VCS(Verifiable Credential Services)を採用。VCS の機能はその機能が Issuer や Holder が信頼できるものとして仮定し、特定の認証認可を実施せず WEB API として機能を利用する形態で検討した。
基本設計	FIDO と DID の組合せによる本人認証の強化	FIDO 認証における本人認証用の鍵を使わずに、FIDO 認証後に検証目的の鍵を DID (Decentralized Identifier) と紐づけて生成し公開する方法を採用。
	ウォレットとしての PLR	PLR は、多様な種類やサイズのデータの開示・共有およびそれに基づく人間同士のほぼあらゆる種類の共同作業をサポートする分散 PDS ライブラリである。そのような一般的な機能を持つウォレットとして PLR を用いて VC と VP を含む属性情報を保管する。
	Open Badge 3.0 および W3C の VC/VP の規格に準拠	1EdTech が策定した Open Badge 3.0 は業界標準である Open Badge 2.0 の後継であり、W3C の VC/VP に対応していることから、これを前倒しして採用する。
システム開発	FIDO Notary	OSS で公開されており、FIDO 認定製品でもある LINE OSS をベースに標準的な FIDO サーバを開発後、FIDO Notary に必要な ID トークンの検証・発行機能などと合わせて外部 ID の取り入れに必要な機能を実装。
	PLR	FIDO Notary との結合に必要な ID トークンの発行・検証機能を実装し、属性情報のやり取りの他、VP 生成機能を実装。Verifier が開示を要求し、Holder によって開示の判断を可能にした。
	VCS/VDR	VCS に BBS+の署名機能を実装し、DID に紐づく BBS 鍵の登録・公開機能を VDR に実装した。また、学修歴証明書に合わせた VP 作成時の開示属性の組み合わせを検討し、実装した。公開鍵の保管や DID の登録に用いる VDR は、運用コスト低減のためブロックチェーンを使わず通常の集中管理型サーバにおいて実装。
ユーザーテスト	FIDO Notary	FIDO の標準プロトコルについてメジャーOS（Android, Windows, iOS, MacOS)/ブラウザ(Chrome, Firefox, (Apple 製品のみ)Safari)の組み合わせで、端末に標準装備された認証器（主に指紋や顔）で検証。
	結合テスト	パラメータやデータの授受について不備がないか、エラーの通知とエラーハンドリングについてそれぞれ検証。

3.1.2 国際標準規格の調査

本事業に関係する国際標準規格を表 3.1.2-1 に挙げる。これらは事業実施に先立って採用を検討し参考にしたものである。

調査事項	調査対象機関	調査結果

検証可能な証明書	W3C（VC Data Model)	Issuer と Verifier というロールが分離され、DID の活用が想定した分散モデルを採用している。データの「コンテナ」フレームワークを提供し、データ形式やプロトコルは実装依存である。データの検証は、公開鍵暗号技術を使った署名検証を基本技術として想定。そのための公開鍵を公開情報として VDR にて登録。
	1EdTech (OpenBadge)	OpenBadge は学修歴証明の標準規格。3.0 版は上記 VC に準拠。
アイデンティティ管理・に関する手法	OASIS/ITU-T (SAML)	SAML (Security Assertion Markup Language) は、セキュリティに関するユーザ情報の交換のためのプロトコル・フレームワークである。IdP（Identity Provider）と SP（Service Provider）という 2 つのエンティティとユーザを含めた 3 者を跨ってユーザ個人のデータを配付・流通する。ユーザのプライバシーに配慮する（トラッキングを防止する）モデルを採用しており、分散環境におけるユーザ情報の参照方法に関して先駆的な取り組みである。
	OpenID Foundation (OpenID Connect)	上記 SAML とプロトコルは異なるが、3 者を跨る分散形態において、ユーザ情報を配付する仕組みとして類似している。
認証に関する標準	FIDO アライアンス・W3C (FIDO2 ・ WebAuthn)	FIDO アライアンスで策定、W3C にて標準化が進められている認証仕様であり、公開鍵ベースの認証をサポートする。ユーザのデバイス（スマートフォンや PC 等）のローカルにある認証器というデバイス機能を用いて、ユーザを生体認証等を利用して認証した結果に対して認証器で保管するユーザの秘密鍵を用いて署名を生成し、認証サーバに予め保管する公開鍵を用いて署名検証する。セキュリティ上の目的で、前記 FIDO トラストモデルを採用している。

3.2　検証できる領域を拡大する仕組み

3.2.1 データフロー

システム全体のデータフローを図 3.2.1-1 に示す。

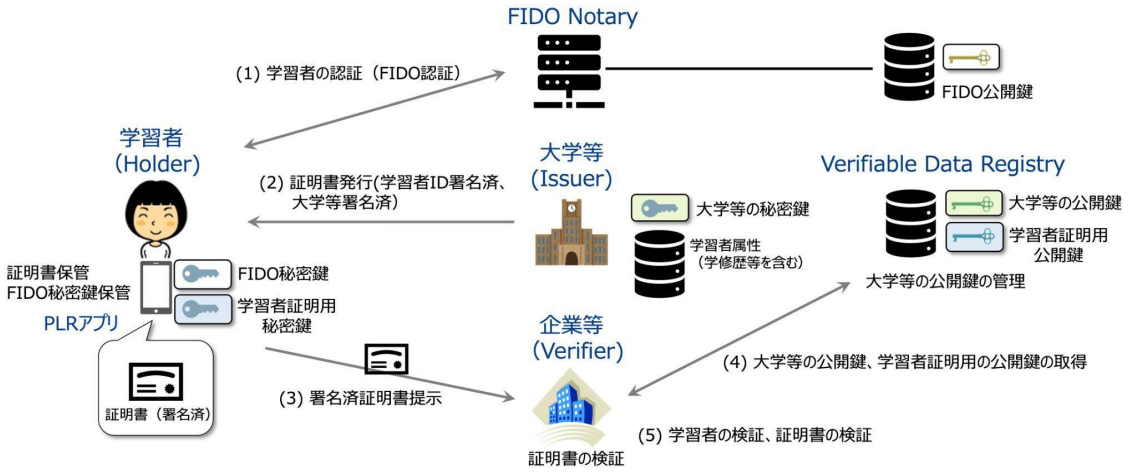

図 3.2.1-1 データフロー

学習者(Holder)は FIDO 認証を経て大学等(Issuer)から VC 等の属性情報を取得し、それをウォレット(PLR)で管理し、企業等(Verifier)の開示要請を（自動的に）確認した上で VP を生成して開示する。開示する情報の範囲は学習者が開示条件の設定により主体的に選択できる。企業等は大学等に直接照会することなくその VP が大学等によって発行されたことを検証できる。

3.2.2 データフローに登場する主体とその概要

- 学習者(Holder)
  - 必要な学修歴証明を取得するため、大学等に VC の発行を依頼する。発行された VC に対する所有権を持ち、自分の属性情報をウォレットで管理し、企業等の要請に応じて、合意形成された必要な属性情報のみ選択的に企業等に提示する。

- 大学等(Issuer)
  - 各種形式の学修歴証明の発行を学習者から依頼され、学習者のアイデンティティを確認したうえで、学修歴証明を VC として発行する。

- 企業等(Verifier)
  - 学修歴証明の開示を学習者に要請し、それに応じて開示された学修歴証明を検証して選考等に用いる。

3.2.3 検証できる領域を拡大し、Trust を向上するために本システムで検証を行うデータ及びデータのやり取りの内容

本システムでは、学習者のアイデンティティが DID として与えられる。DID と本人の結びつきの強化が、学修歴証明(VC)を大学が発行したこと、およびその VC が学習者に関するものであることに関する企業等(Verifier)の信頼を強化する。ここでは、主としてこれらの信頼をトラストと呼ぶ。そのトラストは FIDO 登録/認証を司る FIDO Notary へのトラストに依存する。本システムのトラストが従来システムのものと比べてどう強化されているかを以下にまとめる。

学習者の本人認証を強化するため、以下の手順により、大学等におけるリアルな認証と FIDO 認証

を経て学習者の DID を生成する。

1. 大学等が学習者のリアルな認証に基づき ID トークン A を生成して学習者に渡す。
2. 学習者が ID トークン A を FIDO Notary に渡す。
3. FIDO Notary が ID トークン A を検証した後に新たな ID トークン B を生成し FIDO 登録/認証を経て B を学習者に渡す。
4. 学習者が学習者証明用公開鍵と B を大学等に渡して DID の発行を依頼する。
5. 大学等が B を検証したうえで VDR に学習者証明用公開鍵を渡す。
6. VDR が学習者証明用公開鍵を含む ID を発行・登録して大学等に渡す。
7. 大学等がその DID を学習者に渡す。
8. 学習者が DID を PLR に保管する。

このようにして作られた DID は、大学等でのリアルな認証に基づき、FIDO 認証によって特定の端末と紐付けられるので、学習者の本人認証を強化すると考えられる。このような DID を学習者が後ほど大学等または企業等に提示したとき、大学等または企業等は、FIDO Notary へのトラストを前提することによって学習者の本人性を高い確度で検証することができる。

また本事業では学修歴証明(VP)も運用・検証可能にする。1EdTech が策定し W3C の VC/VP に準拠している Open Badge 3.0 に基づき、大学等と VDR のトラストを前提として、企業等が大学等に直接照会せず VDR から大学等の公開鍵を取得することにより VP を大学等が発行したことを検証できる。

3.2.4 本システムで形成を目指す合意とその履行のトレースの内容

学習者と企業等が学習者の何らかの属性情報を企業等に開示することについて合意する。その際、学習者が予め設定してあった開示条件と企業等が示した開示要請とを両方とも満たす属性が自動的に選択され開示される。その開示要請とそれに対する同意/非同意および同意した場合の開示を表わすデータを学習者が開示履歴タイムラインとして保管し、企業等も開示履歴タイムラインを閲覧してトレースすることができる。学習者は合意を手動で取り消すことができるが、属性情報の開示後に開示条件を変更した場合には開示状態は変わらない。なお、企業等は開示要請を学習者の開示履歴タイムラインに書き込むことによって学習者に開示要請を送るが、他の情報を開示履歴タイムラインに書き込むことはできない。

開示履歴タイムラインの中のデータには学習者と企業等の電子署名を付けることによって不正な改竄を防ぐことが望ましいが、そのための開発は招来の課題である。

3.3 6 構成要素との対応

表 3.3-1 に Trusted Web の 6 構成要素と本事業の対応を示す。

表 3.3-1 6 構成要素と本事業の対応

6 構成要素	6 構成要素との当てはめ	6 構成要素
検証可能なデータ	検証対象	①学習者の本人性 ②VP
	署名者	①大学等+FIDO Notary ②大学等
アイデンティティ	アイデンティティとして想定されるものが何か	大学等、学習者、企業等
	アイデンティティ管理システム（外部）は何を利用しているか	FIDO Notary による FIDO ID の生成、VDR による DID の生成
	アイデンティティグラフとして想定されるのはなにか	学習者の ID: 大学等が付与→FIDO Notary が付与→VDR が付与(DID) 企業等からは大学等が付与した ID と FIDO Notary が付与した ID が見えない
ノード	Wallet か否か	学習者は PLR アプリをウォレットとして用いる。大学等と企業等もそうして良いが、そうである必要はない。
	合意形成がされているか、されているならその手段	学習者の開示条件と企業等の開示要請が整合するかどうかをウォレットで自動的に判断する
	データのやりとりをどこに記録するか	ウォレット
メッセージ	コネクションオリエンテッドかメッセージオリエンテッドか	学修歴等の属性データを授受するための PLR と他のシステムとのやり取りは常時接続ではなくメッセージの授受に伴って生ずるのでメッセージオリエンテッド
トランザクション	データのやり取りを記録するか	学習者のウォレットに大学等および企業等とのやり取りを記録
	データのやり取りの検証はできるか	各エンティティがデータの作成者に都度直接照会せずに検証できる
トランスポート	トランスポートのプロトコルは何か	学習者が大学等および企業等とのやり取りする場合、相手も PLR を用いる場合は PLR クラウド(さしあたり Google ドライブ)の API、そうでない場合は相手のシステムの API

3.4 本実証で企画・開発したシステムの概要

3.4.1 業務フロー

図 3.4.1-1 に初期の FIDO 登録、図 3.4.1-2 に VC 発行のフローを示す。

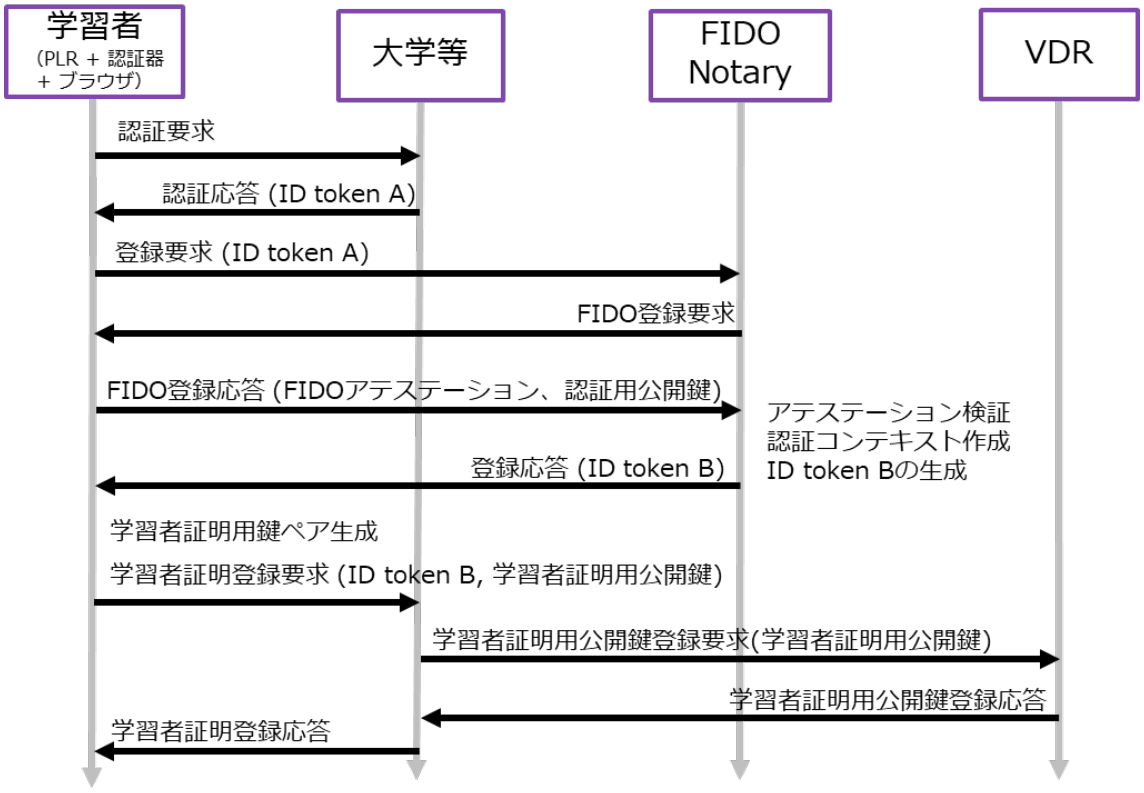

図 3.4.1-1 初期の FIDO 登録のフロー

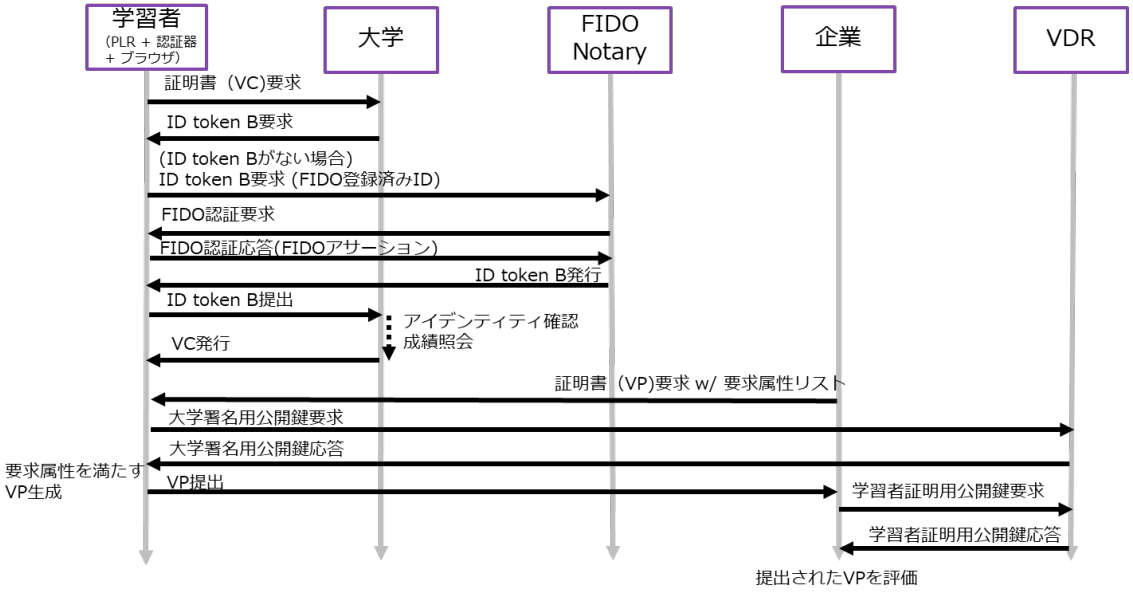

図 3.4.1-2 VC 発行のフロー

3.4.2 ユースケース図

図 3.4.2.1 に本システムのユースケース図を示す。

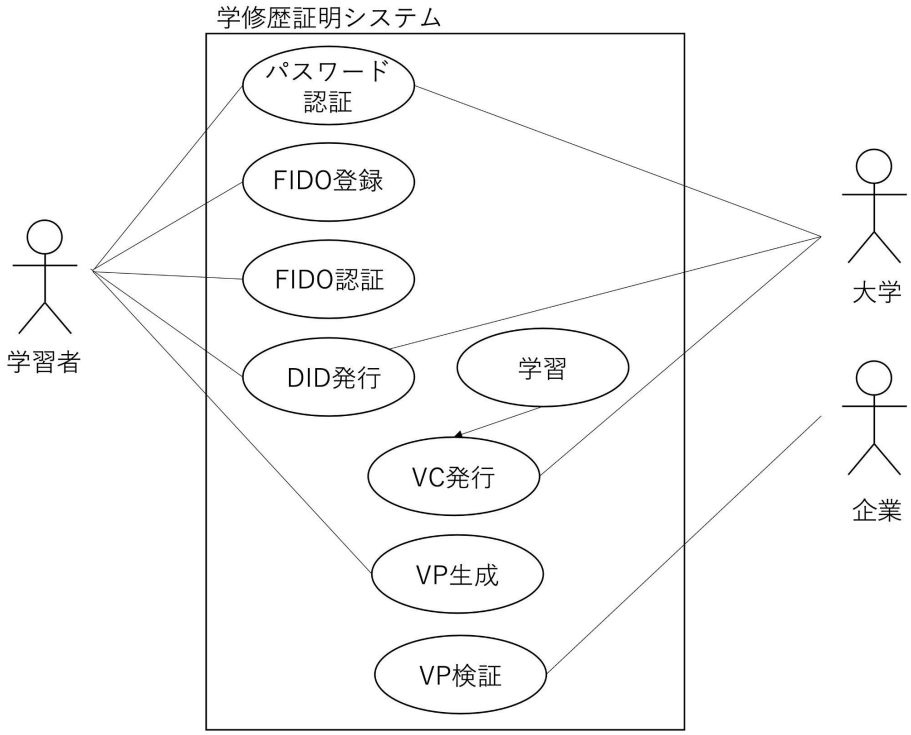

図 3.4.2.1 ユースケース図

3.4.3 操作画面（UI）

操作画面は成果報告書概要版に記載する。

3.4.4 機能一覧/非機能一覧

機能と非機能の一覧を表 3.4.4-1 に示す。

表 3.4.4-1 機能/非機能一覧

機能/非機能	機能名	機能概要
機能	FIDO 登録/認証	学習者が Personary で FIDO Notary を呼び出して FIDO 登録/認証を行なう。
機能	DID 発行の依頼	学習者が DID 発行を大学等に Personary で依頼する。さらに、大学等が DID の発行を VDR に依頼する。
機能	DID 発行	VDR が DID を発行し登録する。
機能	VC 発行の依頼	学習者が VC 発行を大学等に Personary で依頼する。
機能	VC 発行	大学等が学習者の FIDO 登録/認証を確認した上で VC を発行する。
機能	VC 検証	学習者が VC の署名を検証する。

機能	開示条件の作成	学習者が属性情報を開示する条件を作成する。
機能	開示要請の作成・投稿	企業等が属性情報の開示要請を作成し学習者の開示履歴タイムラインに投稿する。
機能	開示の判断	学習者の Personary が開示条件と開示要請を満たす属性情報を自動的に抽出する。
機能	VP 作成	学習者の Personary が開示すべき属性情報からなる VP を作成する。
機能	VP 開示	学習者の Personary が上記の判断に基づいて VP を企業等に開示する。
機能	VP 検証	企業等が VP を検証する。
非機能	可用性	学習者がオフラインでも自分の属性情報と開示履歴にアクセスできる。
非機能	スケーラビリティ	10 億以上の利用者にサービス提供可能。

3.4.5 データモデル定義(VC データモデルを採用する場合)

属性値は OpenBadge 3.0 の context に従う。以下、本事業でテストとして用いたものについて、属性値と取得元を合わせて表 3.4.5-1 に示す。

表 3.4.5-1 データモデル定義

属性値	**属性取得元**	**属性名 (vc 内)**
Holder の識別子	Holder	identifier
単位情報(学位・単位別)	Issuer	achievementType
単位情報(学位・単位名)	Issuer	name
成績情報	Issuer	creditsEarned
発行元	Issuer	issuer
発行日	Issuer	issuanceDate

3.4.6 実験環境

本実証で企画・開発したシステムの実証環境の概要を図 3.4.6-1 に示す。

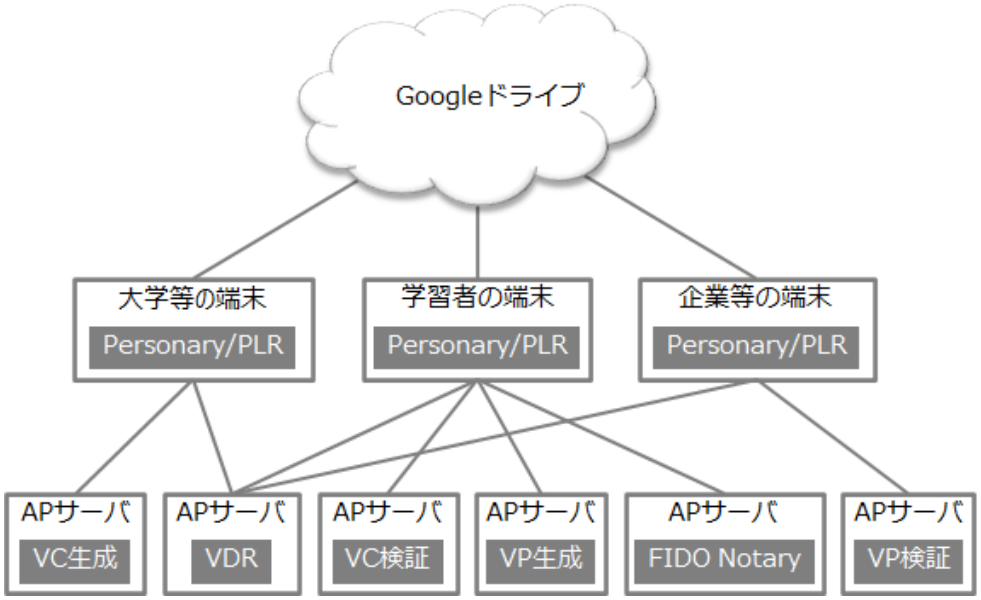

図 3.4.6-1 実験環境

3.4.7 システムの構成要素

本実証で企画・開発したシステムで用いた主な製品・ライブラリを表 3.4.7-1 に示す。

表 3.4.7-1 主要な製品・ライブラリ一覧

コンポーネント名称	型式（製品の場合）	OSS か否か	ライセンス
PLR ライブラリ	—	アセンブローグ社が権利を保有	非商用は無料
Personary	—	OSS	Apache-2.0
FIDO Notary	LINE OSS	OSS	Apache-2.0
VDR	MySQL	OSS	GNU GPL

3.5 実証を通じて得られた主な成果

3.5.1 システムの企画・開発に関する実証内容・得られた主な成果

- FIDO Notary というコンポーネント(ロール)を導入し、FIDO 認証のトラストモデルを踏襲し学習者(Holder)の本人認証を強化すると同時に、企業等(Verifier)が検証者として学生(Holder)の本人性を検証可能とする VC 形式の学修歴証明書を発行するシステムを開発し、動作を検証した。上記において、汎用的に認証に用いる FIDO 鍵とは異なる本人証明用の鍵ペアを生成し、その公開鍵を学習者の DID と共に VDR に配備することによって企業等が学習者の本人性を検証することができた。BBS 署名を実装することで、学習者が自らの好みやポリシーに応じて複数の VC から必要な情報をのみを抽出して記載した VP を改竄なく生成し、企業等に提示できるようになった。

3.5.2 ビジネスモデルに関する実証内容・得られた成果

- 学修歴証明については日本は他の先進国や中国に比べてかなり遅れており、一部の大学で導入を

検討中だが、学生の就職先である企業等には積極的な動きがない。したがって、さしあたり最も有効な価値提案は事務コスト削減と考えられる。大学等(Issuer)と企業等(Verifier)は事務コスト削減のため有料サービスを使う可能性がある。学生(Holder)には無料でサービスを提供するのが良いだろう。しかし、本事業のようなサービスの規模が一定以上になるには、社会的な認知が本質的に必要であることを再認識した。本事業で実証した選択的開示により、プライバシーに配慮したデータ流通が可能になっている。国際化対応を含め、大学や企業の意識が前向きになる動機付けを与えることが重要である。

- 学修歴証明に関するサービスを事業化するための本質的な課題は、署名の検証による技術的なトラストではなく、学修歴データの内容に関するトラスト(質保証)である。そのための社会環境が整うには、少子化対策、働き方改革、ジョブ型雇用、リスキリングなどの進展が必要であり、逆にそれらの進展を促すために学修歴証明の普及が必要とされる、という鶏と卵の状態にある。
- 属性証明に関するサービスを早期に事業化するには、属性データの内容に関するトラストが既に成立しているユースケースを対象にする必要がある。学校での成績の評価の方法は標準化されていないので、大学等の学修歴によって他の大学や企業が学習者の能力を評価するためには、多数の大学等の間で学修歴を比較するための質保証の仕組みが必要だが、国内にはそのような仕組みがない。これに対してたとえば検査値などの客観的なデータは(センサのキャリブレーション等ができていれば)信頼できるので、そのような医療データに医療機関や検査センターの電子署名を施す仕組みがあれば、バイオバンク等のサービスが有望と考えられる。

3.6 本実証で開発したシステムの第三者による再現可能性（A 類型のみ）

- 本実証事業で企画・開発するプロトタイプシステムは全てオープンソースで構築し、そのソースコードを GitLab 上に公開することで、第三者が再構築し再現することができる。
- 上記プロトタイプシステムのうち Personary はアセンブローグ社が権利を持つ PLR ライブラリを組み込んでいるが、PLR ライブラリは非商用なら無料で利用できるので、Personary も同様に利用可能である。

4　実証終了後の社会実装に向けた見通し

4.1　社会実装時に想定しているビジネスモデル・ユーザーのメリット

本事業では、学習者の知識と技能を証明する卒業証明書や成績証明書を発行する大学等、それらを用いて学習者の採用の選考を行う企業等が、学習者とともに一つのエコシステムを構成することを想定している。本事業では構築した技術的な仕組みによって、学習者は、各種の学修歴証明を主体的に管理してプライバシーを守り、教育を受けたことを証明することができる。また企業等は、学修歴証明の真正性が保証されることにより、成績の質を評価することに注力できる。

日本の労働市場の流動化は従前と比較して進んでいるものの、スキルとジョブ要件のミスマッチが解消されているとは言い難い。しかし、大学等が発行する学修歴証明をプライバシーに配慮した形で流通させる技術的な仕組みが本事業で構築されたことにより、上記ミスマッチを解消するために学修歴証明を利用できるようになり、大学等も学習者も企業等もそのメリットを享受できる。

想定されるビジネスモデルを図 4.1-1 に示す(「証明発行+VDR 事業者」は実際には複数ある事業者を簡単のためひとまとめに図示してある)。大学等は教育に対応して学修歴証明を発行するが、それによって学習者の就職や留学が促進されて大学等の評価が高まるのであれば、そのコストを負担すると考えられる。学習者も自らの就職や留学に学修歴証明が有用である度合に応じてコストを負担するのが妥当である。同じく企業等も学修歴証明が人材の獲得に有効であれば相応のコストを負担するだろう。

表 4.1-1 に各ステークホルダのベネフィットと想定される利用料を示す。ただし、労働市場の流動化やジョブ型雇用の普及が十分に進んでいない現状においては、学修歴証明の価値は事務コストの削減に留まるだろう。表 4.1-1 に示す利用料は事務コストの削減のみに対する金額である。

東京大学とヤフー株式会社との共同研究は令和 5 年以降も継続するので、その一環としてこのビジネスモデルの洗練や他のビジネスモデルへの展開について検討を続ける予定である。

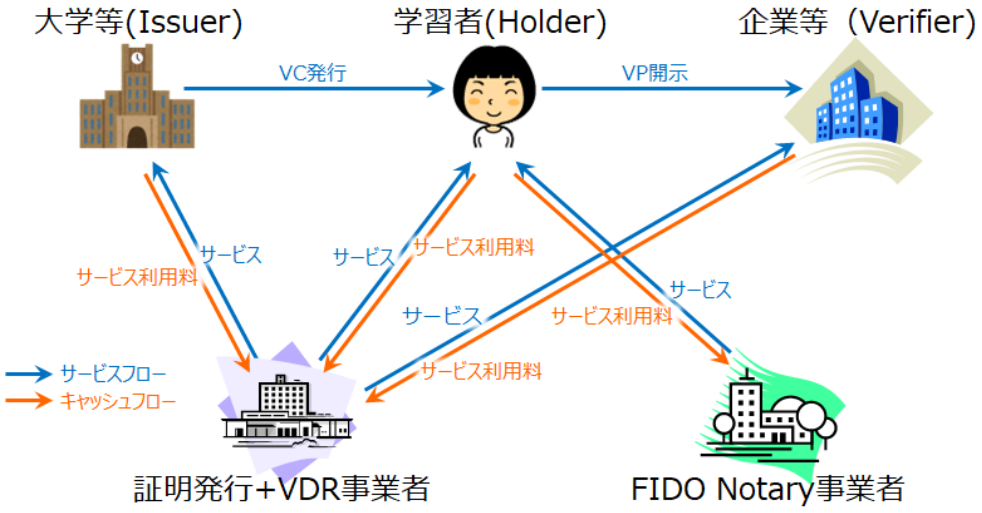

図 4.1-1 ビジネスモデル

表 4.1-1　各ステークホルダのベネフィット及び想定している利用料

ステークホルダ	ベネフィット	利用料

大学等	証明発行および企業等からの照会等に係る事務コストの削減、紙の証明書の印刷費用の削減、学習者の就職・留学の促進による社会的評価の向上	証明発行 1 件につき 50 円 →証明発行+VDR 事業者
学習者	証明書の取得や開示に係る事務コストの削減、就職・留学の機会の拡大	年額 100 円 →FIDO Notary 事業者
企業等	証明の取得や真正性検証に係る事務コストの削減、人材獲得の効率向上	証明検証 1 件につき 50 円 →証明発行+VDR 事業者

4.2　実証を通じて判明したユースケースの課題とその解決方針

課題① データ最小化

学習者のプライバシー保護のため、企業等に開示する属性情報は、選考など所期の目的のために必要最小限のものでなければならないが、現状ではそれをチェックする仕組みがない。各個人がそのようなチェックをすることは一般には不可能と考えられるので、企業等の開示要請の最小性をチェックする外部サービスが必要と考えられる。学修歴の管理だけでなく医療データ等の管理においても同様である。

課題② 属性情報使用の履歴管理

企業等がいったん取得した属性情報を所期の目的以外に使い回さないように、使用履歴が管理されることが必要である。分散台帳による履歴管理手法がいくつか提案されているが、使用履歴の台帳への登録を企業等に強制する手段がなければ有効でない。

課題③ 大学側の内容の質保証

大学等が発行する学修歴証明は、本事業の枠組ではそれを特定の大学等が発行したことが保証されるだけであり、その内容の質が保証されるわけではない。教育の質保証は日本社会全体での今後の大きな課題である。

4.3　成果の社会実装に関する展望

4.1 のビジネスモデルは、働き方改革や労働市場の流動化の進展によりステークホルダのニーズが顕在化するにつれて普及すると期待される。東京大学でも学修歴証明の導入を具体的に検討しており、おそらく既存の学修歴証明サービスを利用して証明の発行を開始することになるだろう。既存のサービスによって証明を発行する場合でも、本事業で開発した仕組みの大部分は既存サービスと組み合わせて運用できるので、前記のビジネスモデルの普及が進むことを前提として新たなビジネスモデルの実現を目指す。

新しいビジネスモデルにおいては、図 4.3-1 のように、学習者に専属するが専属するパーソナル AI (PAI)が PLR に保管された学習者の属性情報を他者に開示せずに就職先や進学先の候補とマッチング

することによって学習者の進路選択を支援する。就職や進学に関する知識を集約した「進路カタログ」を多くの個人の PAI に提供する事業者をメディエータと呼ぶ。メディエータと PAI ベンダーは学習者の就職等を仲介して手数料を取る事業を運営する。

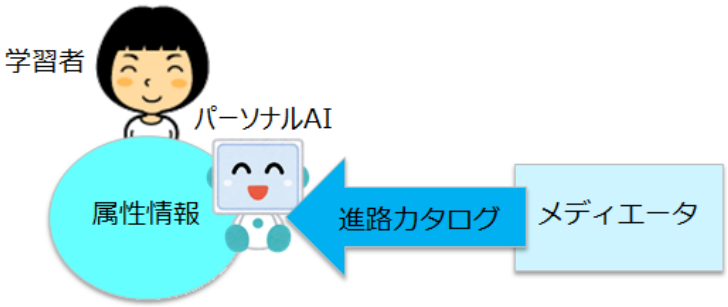

図 4.3-1 パーソナル AI による進路選択の支援

進路カタログはさしあたり GPT などの生成型 AI モデルとして実現されると考えられる。GPT-4 や LLaMa など既存の生成型 AI はすでに大量の知識を学習しているが、その知識は今後ますます充実して行くに違いない。PAI はそのような大量の知識を用いて利用者本人と対話することにより就職や進学を支援することになるだろう。

この PAI サービスを実現するには、PAI の開発に加えて、学習者の PLR に本人の属性情報を集約することと、メディエータが進路カタログを作成・保守することが必要である。属性情報の本人への集約は学修歴の電子化によって進むだろう。一方、進路カタログを生成型 AI として作成・保守する技術は 5 年ほどで実用化できそうである。さらには、就職や進学に限らない多様な知識を持つ生成型 AI をメディエータが PAI に提供してプライバシーを守りながら個人にさまざまな支援を提供することもおそらく数年のうちに可能であり、そのような PAI の活用が学修歴証明の普及を含む DX を促すことになるだろう。

4.2 の課題①は他者に開示する属性情報を PAI が必要最小限に絞ることによって達成されるだろう。それに必要な知識もメディエータが提供する生成型 AI モデルに含まれる。課題②の完全な解決は不可能と考えられるが、後述のオープン市民科学によって属性情報の不正使用を防ぐことはある程度可能だろう。課題③は学修歴の電子化が進むにつれて達成されると考えられる。①は各事業者が取り組むべき課題であり、②と③は社会全体の課題であるが、多くの事業者が①に取り組むことによって②と③も達成される。

5　Trusted Web に関する考察

5.1　Trusted Web のアーキテクチャに関する課題と提言

各エンティティの複数個のアイデンティティの使い分けについて議論を深める必要がある。たとえばメタバースの最も重要な応用は教育(メタバースの恥はかき捨て：現実世界でやらかすと致命的であるような失敗を仮想世界でしてその失敗から学ぶこと)だと考えられるが、それには仮想世界での自分のアバターと現実世界の自分との名寄せが他者にできないようにアイデンティティを管理する必要がある。

5.2 その他 Trusted Web の課題と提言

一般論として、トラストとセキュリティまたはプライバシーとの関連性に関して注意する必要がある。トラストにフォーカスされているがゆえに、トラストを高めることを強調し優先すると、セキュリティまたはプライバシーが損なわれるリスクがある。実用的なシステムの実装のためには、トラストの要件のみならず、セキュリティとプライバシー要件も含めた総合的な設計が必要と考える。

厳密な自己情報コントロールは不可能であり、全面的な集中管理も非現的である。次世代医療基盤法の改正の議論も自己情報コントロールではなくデータ利用者の責任に関するガバナンスを指向している。そのように(VC 等を含む)パーソナルデータの管理を他者に委ねるのが現実的であることと、セキュリィとプライバシーのためには分散管理が望ましいことを併せて考えると、本人専属の AI (パーソナル AI)にパーソナルデータの管理運用を委ねる(もちろん本人の意思も管理に反映される)必要があると考えられる。

表 5.2-1 パーソナルデータの管理方法の分類

	集中(各管理者が多くの人々の PD を管理)	分散(各管理者が 1 人だけの PD を管理)
自力		本人が管理 ● 煩雑で危険
委託	他人が管理 ● リスクとコストが大きい ● データが囲い込まれて利用しにくい ● ある種のサービスには必須	PAI(本人専属の AI)が管理 ● 個人にとっても事業者にとっても安全で付加価値が高い

一般に検証すべき対象は多様であり、データ検証だけで十分ではないことが多い。特にデータの内容の真正性(データが正しいか)や精度(データがどの程度確からしいか)の検証には他の手段が必要である。たとえば学修歴証明の本質は電子署名の検証などの技術というよりは証明内容の正しさの保証である。それは学修歴証明の発行者である大学等を含む社会システムに対するトラストに基づくが、そのトラストの根拠は電子署名の検証などではなく社会的相互作用の蓄積である。これはもちろん学修歴証明に限らない。また、ブロックチェーン上の DID が検証できても、一般に利用者のアイデンティティ(属性情報等)の検証には十分ではない。この考察は、TrustedWeb として提案されたトラストモデルが暗黙裡に仮定していた条件を明らかにしたと思われる。TrustedWeb をトラストモデルの視点から精緻化し、

TrustedWeb 以外に必要な取り組みを明確にする必要がある。

署名検証などの既存技術によりデータの改竄は検出できる。しかし、それに必要な情報（署名検証の場合には公開鍵）を検証者が入手可能とは限らない。データのトラストを高めることを優先するあまり、元々入手できないデータの開示を迫るような構想にならないように配慮いただきたい。

データ検証のための公開鍵が入手できない場合にも検証を実現するために、データに関連づけて検証用の新規公開鍵を作成して DID に紐付けて VDR から入手可能にする方法を考案した。具体的には個人に紐づく FIDO 鍵と DID をバインドするために登録時にトークンを発行、交換する仕組みであり、セキュアなバインディングが可能になっている（図 3.4.1-1 参照）。これは汎用的な仕組みであり、他のユースケースにも適用可能である。

ウォレットは個人間の共同作業等をサポートできることが望ましい。共同作業には常時オンラインのサーバが必要と考えられるが、ペルソナ(ID)の使い分け(複数 ID の他者による名寄せの防止)にはそのサーバに複数 ID でログインしてウォレットでそれらの ID を束ねる必要がある。そこで、複数 ID を束ねて運用する PLR の機能を設計中である。

検証可能な範囲を広げるだけでなく、検証が必要な範囲を狭める(わざわざ広げない)ことも重要である。たとえば、マイナポータルの API を使えるのはサーバだけということになっているが、個人アプリが直接 API を使えるようにしてサーバをなくした方が検証すべき範囲が狭くなりリスクとコストが小さくなる。

集中管理の範囲内がトレース可能であるには管理者のトラストが必要である。分散管理におけるデータに基づくチェック&バランス(民主的ガバナンス)がトラストを醸成する。

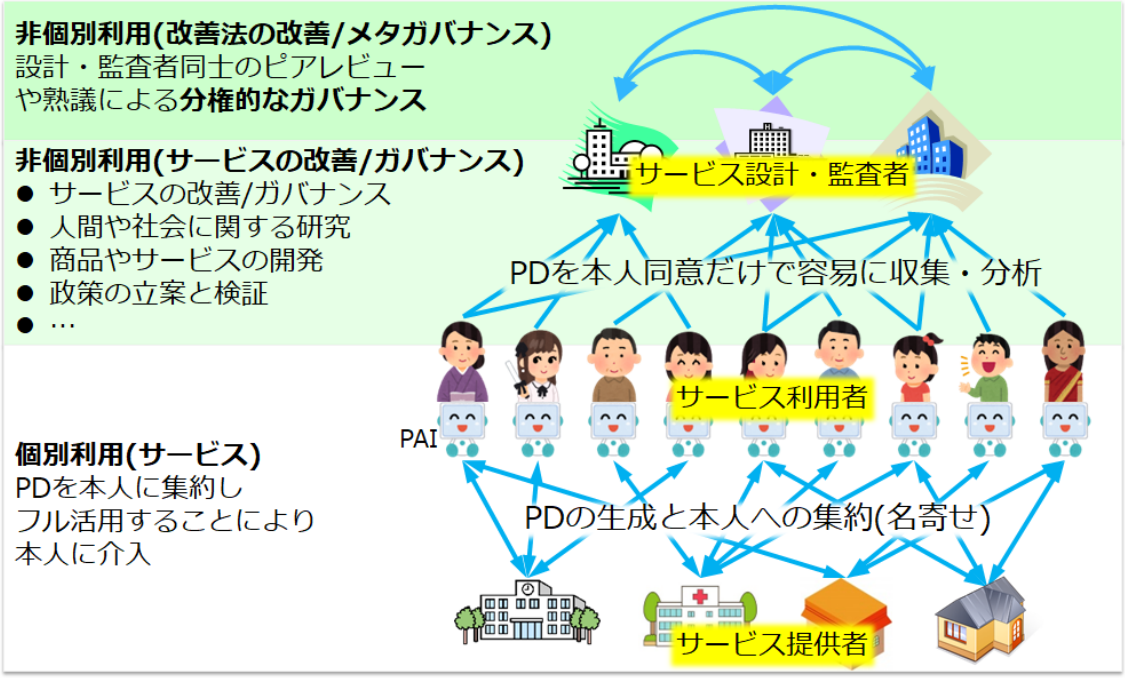

図 5.2-1 オープン市民科学