令和3年度補正予算Trusted Web共同開発支援事業費
「Trusted Webの実現に向けたユースケース実証事業」
最終報告書概要版

学修歴等の本人管理による人材流動の促進

SSI/FIDOコンソーシアム

2023年3月24日

目次

01

背景・目的

1.1　背景・目的

背景

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・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。特にマイクロクレデンシャルの運用に関する計画の具体化を図っているところである。また、ヤフー株式会社と東京大学は、FIDOに関する共同研究において、FIDO Notaryという仕組みを考案し、FIDO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。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。
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。そこで、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活用することを考えた。

目的

学習者の本人認証を強化することにより、学習歴証明が学習者本人に発行される確度と、企業等が学習歴証明等の属性情報を学習者本人から取得できる確度を高める。
学習者が企業等に開示した学修歴証明を企業等が検証する際に大学等に照会する必要をなくす。

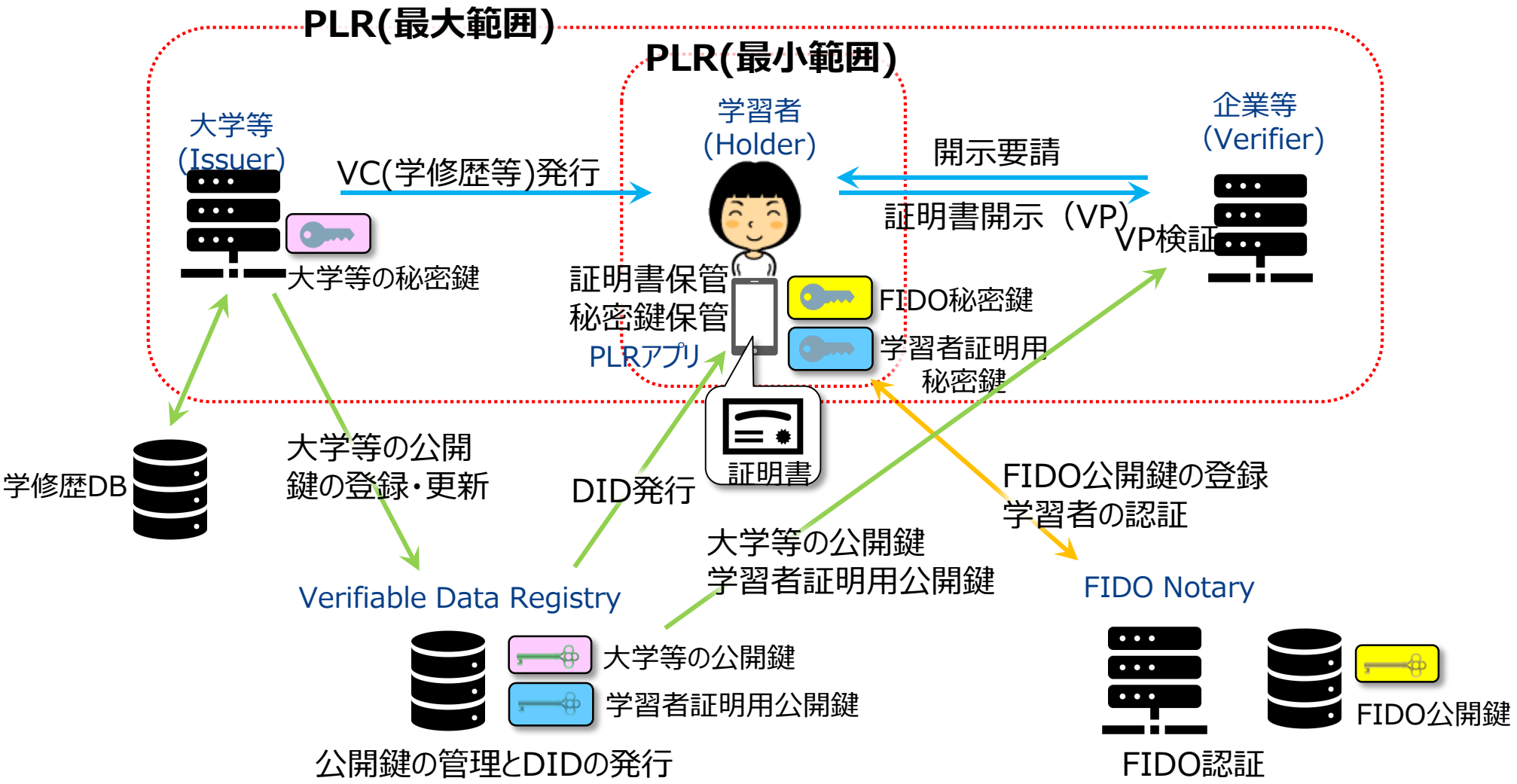
学習者が就職先や転職先の候補である企業等を選ぶ際に学修歴証明等の属性情報を他者に開示せずに活用できるようにする。

02

実証の概要

2.1　実証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。この仕組みにより労働市場の流動性を高めることを目指して、パーソナルAI (PAI)が就職や転職を支援するサービスを運用するための基盤を整備する。



2.2　社会・経済に与える価値・影響

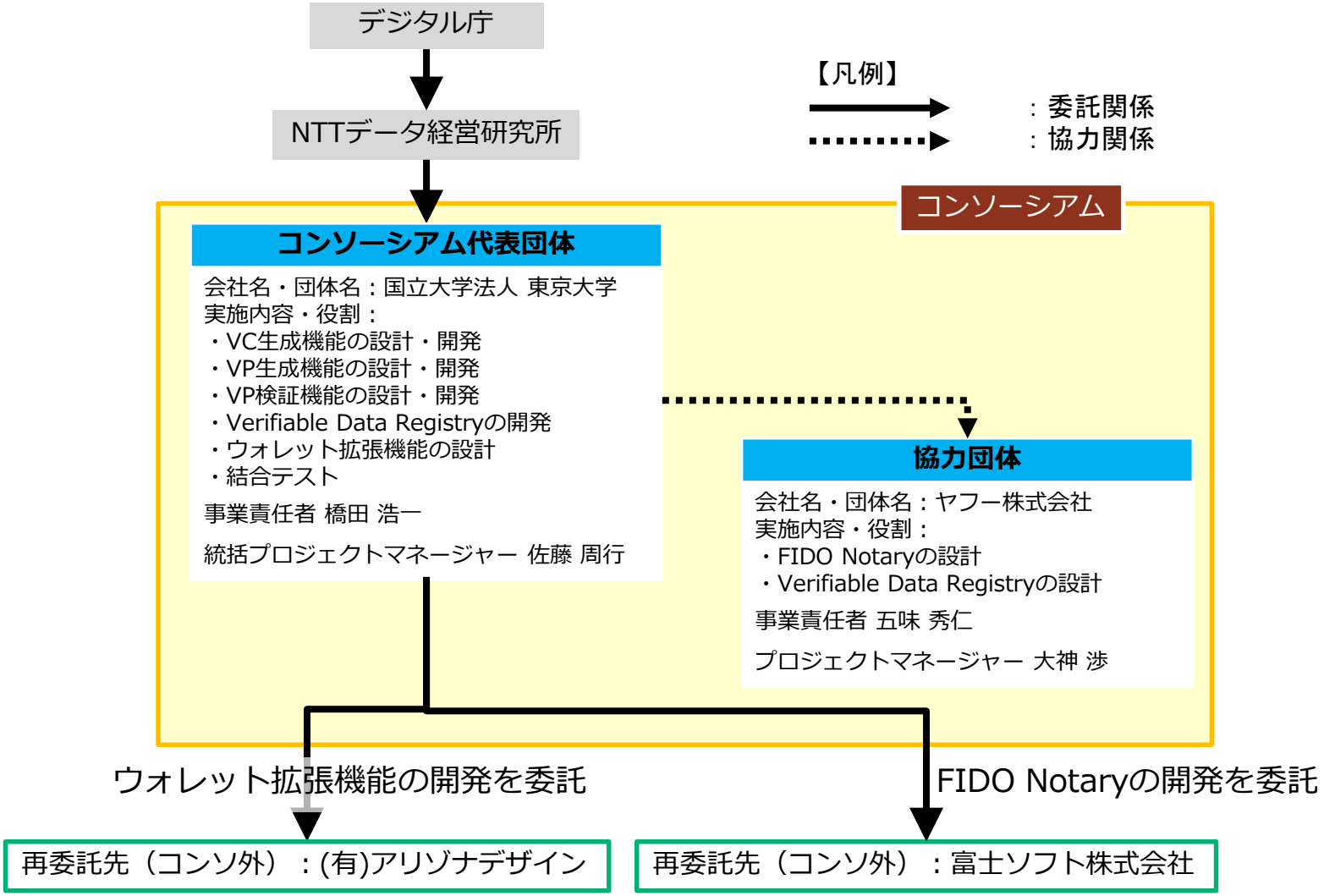
国内で利用できる学修歴証明サービスがすでにいくつかある。たとえば(一社)オープンバッジ・ネットワークが提供する学修歴証明サービスは50万円/年の利用料で使い放題、Digitary社の学修歴証明サービスは基本料金が年間480万円で証明書を6万回利用でき、それを越えると証明書利用1回につき80円かかる。前者はマクロクレデンシャルだけでなくマイクロクレデンシャルの運用にも適する可能性がある。後者はマイクロクレデンシャル用には高すぎるのではないか。以上より各証明書発行者の年間利用料を100～500万円とすれば、国内での潜在的利用者が3万団体として潜在市場規模は300億～1,500億円と推計される。

一方、パーソナルAI (PAI)が属性情報を他者に開示せずに就職や転職を支援する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(9兆円以上)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PAIによる就職や転職の支援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。

ただし、学修歴証明の市場は国内ではまだ確立していない。学修歴証明のニーズが明確になるためには、ジョブ型雇用や労働市場の国際的流動化などの社会環境が必要であり、逆にその社会環境を整えるためには学修歴証明の運用が必要という「鶏と卵」の状態にある。さらに、学修歴証明の本質は、TrustedWebで論じているような電子署名の検証等の技術ではなく、証明される内容の質を保証することであり、この質保証は学修歴証明発行者を含む社会システムに対するトラストに基づく。本事業が社会・経済に大きな価値をもたらすには、この状況を打開する必要があるが、その見通しはまだ立っていない。

一方、PAIの用途は就職や転職だけでなく他のサービスや商品および一般的な行動支援にも拡張でき、その潜在的な市場規模はGDPの25%程度と期待される。

2.3　コンソーシアムの体制



2.4　実証全体のスケジュール

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													

03

実証内容

3.1　実証の実施事項、論点及び判断（1/3）

プロトタイプシステムの企画・開発

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。
	Personary	PLRを組み込んだアプリ。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の開示要請とHolderによる開示の自動判断を可能にした。
	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。
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。

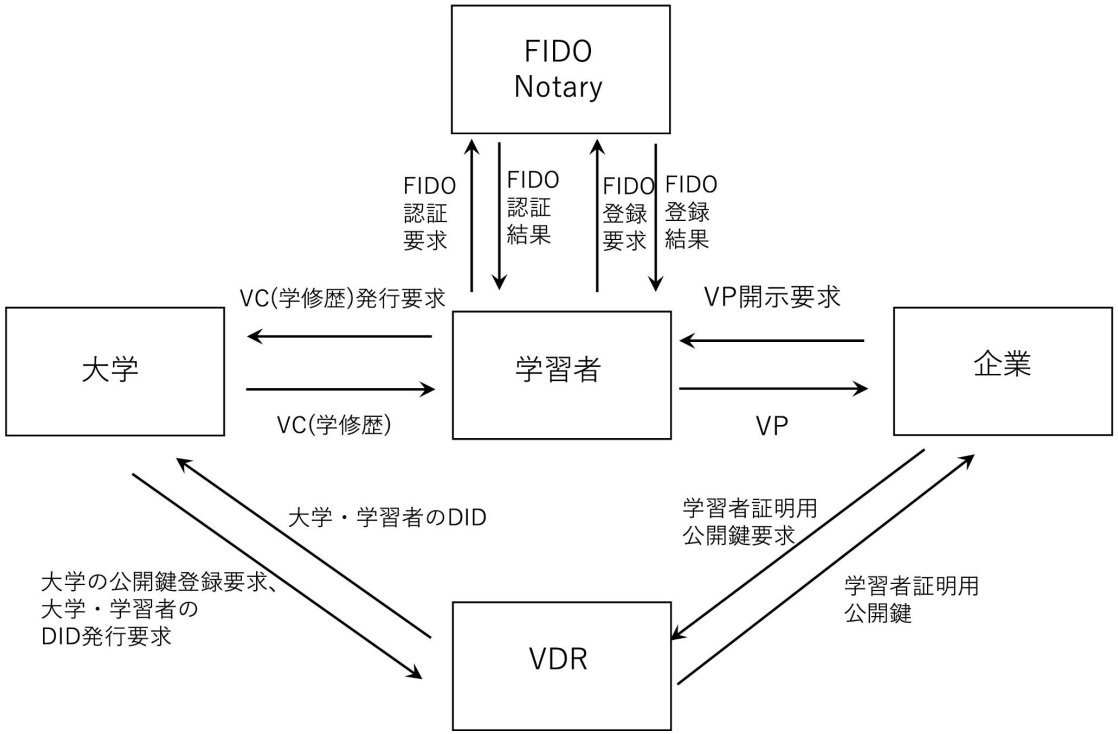
3.1　実証の実施事項、論点及び判断（2/2）

国際標準規格の調査

調査事項	調査対象機関	調査結果
検証可能な証明書に関する動向・仕様について標準仕様を調査	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（Verifiable Data Repository）にて登録することを想定。
	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・に関する手法の動向について確認するため標準仕様を調査	OASIS/ITU-T (SAML)	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。
認証に関する標準化仕様を調査	FIDO・W3C (FIDO・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、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という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（1/3）

データスキーム図



データへのアクセス

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。

登場する主体とその概要

主体	役割・設定
学習者	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	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	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 検証できる領域を拡大する仕組み（2/3）

本システムで検証を行う課題及びデータのやり取り等の内容

要検証の課題	検証対象	検証方法	検証者	保有者	発行者	データ置き場	アクセスコントロールの手法	成果・留意点
IDの使い分け	DID	VDRによるDID発行(またはPLRによる複数IDの使用)	大学等や企業等	学習者	VDR	学習者のPLRとVDR	大学等がVC(成績データ等)を発行する際はDIDで本人確認。	他者とPLR以外でつながる場合(またはPLRで複数のIDを使う場合)は名寄せされない。複数の大学等に応じて複数のDIDを使い分けることが可能。
データの開示とその停止	VP/VCとチャネル	PLRアプリ(ウォレット)	企業等	学習者	—	学習者のPLR	学習者が大学等から取得したデータを企業等に開示しその開示を停止することができる。	データを特定して他者に開示し、その開示を停止
本人認証強化	学習者の本人性	大学等 + FIDO Notary (署名検証)	大学等	学習者	大学等→FIDO Notary→VDR	学習者のPLR	FIDO認証に基づき学習者証明用公開鍵を含むDIDを生成してVDRに登録し学習者がPLRに保管して大学等に提示して認証に用いる。	PLRに依存しない強力な本人認証
本人認証	学習者の本人性	DID + VC (署名検証)	企業等	学習者	VDR	学習者のPLRとVDR	学習者がVPに含まれるDIDを企業等に開示する。	VPを開示した学習者の本人性を企業等が検証

3.2 検証できる領域を拡大する仕組み（2/3）

本システムで検証を行う課題及びデータのやり取り等の内容(続)

要検証の課題	検証対象	検証方法	検証者	保有者	発行者	データ置き場	アクセスコントロールの手法	成果・留意点
VPの分散的検証	VP/VC	VDR (署名検証)	企業等	学習者	学習者	学習者のPLR	学習者がVPを企業等に開示する。	大学等のトラストと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してVPを検証
VP開示の自動化	VPの開示	PLRアプリ	学習者	学習者	—	学習者のPLR	学習者が企業等からデータ開示要請を受け取り、自らの開示条件と整合する要請に自動的に同意して開示。学習者が手動でその開示を停止することもできる。	データ開示要請が開示条件を満たすか否かの判断、満たす場合の開示を自動化; 開示条件の変更に応じた開示および開示停止は自動化せず
表現	開示条件	データ型での条件の表現	学習者	学習者	—	学習者のPLR	学習者の開示条件は他者に開示しない。	将来は量や使用法も条件に含めるよう拡張したい
トレース	開示履歴	PLRアプリ	学習者と企業等	学習者	学習者と企業等	学習者のPLR	開示履歴タイムラインを学習者が検証者(就職先の企業や留学先の大学)に開示。検証者はその開示履歴タイムラインに開示要請だけを書き込める。	学習者と企業等データ開示に関するやり取りの履歴を共有。そこに企業等がデータ開示要請を書き込み、学習者のPLRアプリがその開示要請に対する同意/非同意とデータ開示を記録。
簡単化	トレース	PLRアプリ	学習者	学習者	—	学習者のPLR	学習者が企業等に開示したデータを企業等が第三者に開示しない。	第三者提供を制限することによってトレースが簡単になる

3.2 検証できる領域を拡大する仕組み（3/3）

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

合意の主体	合意の対象	合意の条件	トレースの対象	トレースの主体	トレースの手法	合意取り消しの可否・方法
学習者と企業等	学習者の属性情報の企業等への開示	学習者が予め設定した開示条件と企業等の開示要請を両方とも満たす属性情報である	学習者の開示履歴タイムライン(開示要請、合意、開示の履歴)	学習者と企業等	開示履歴タイムラインの閲覧	手動により可能

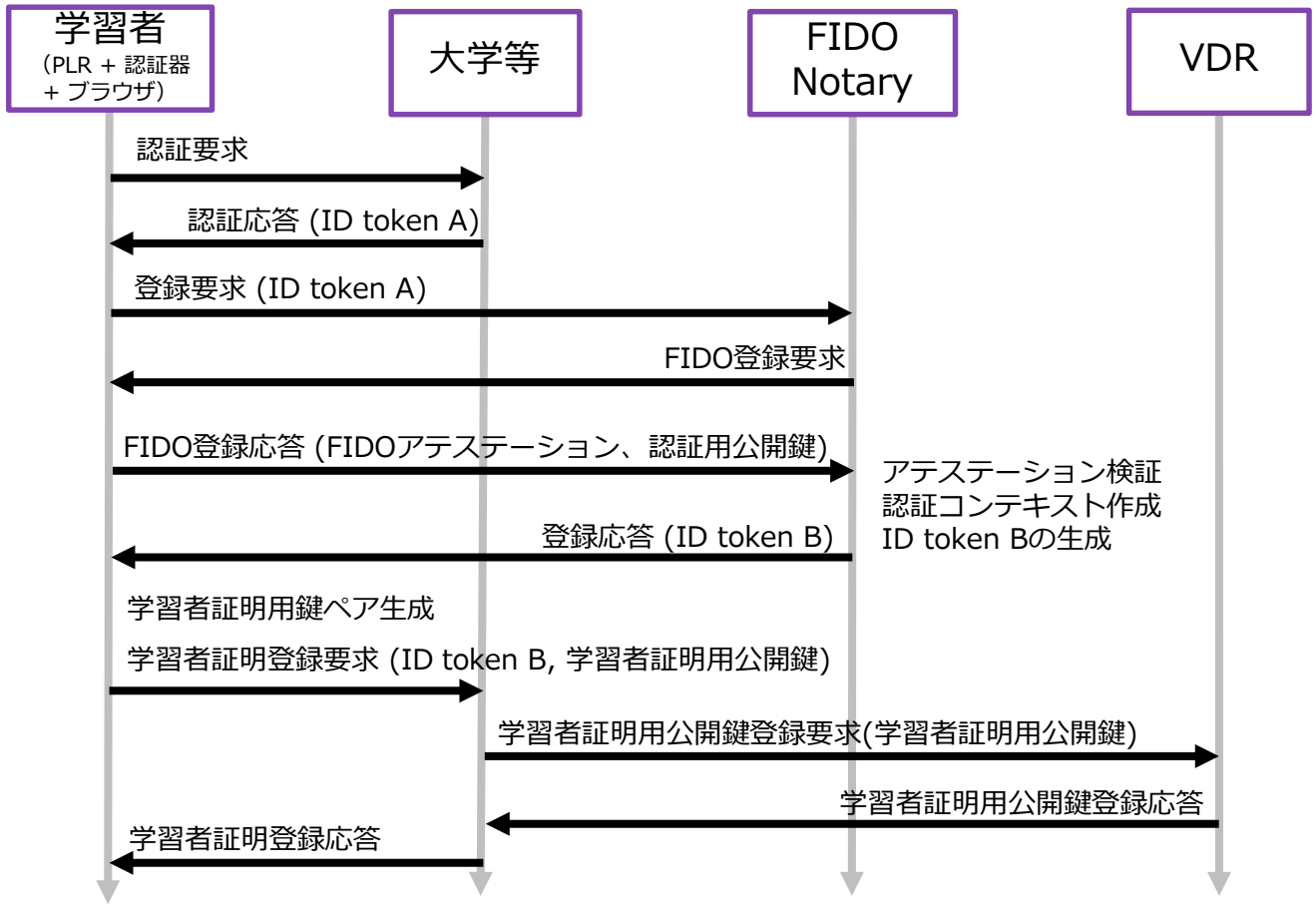
3.3 6構成要素との対応

6構成要素	6構成要素との当てはめ	
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	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（1/6）

業務フロー

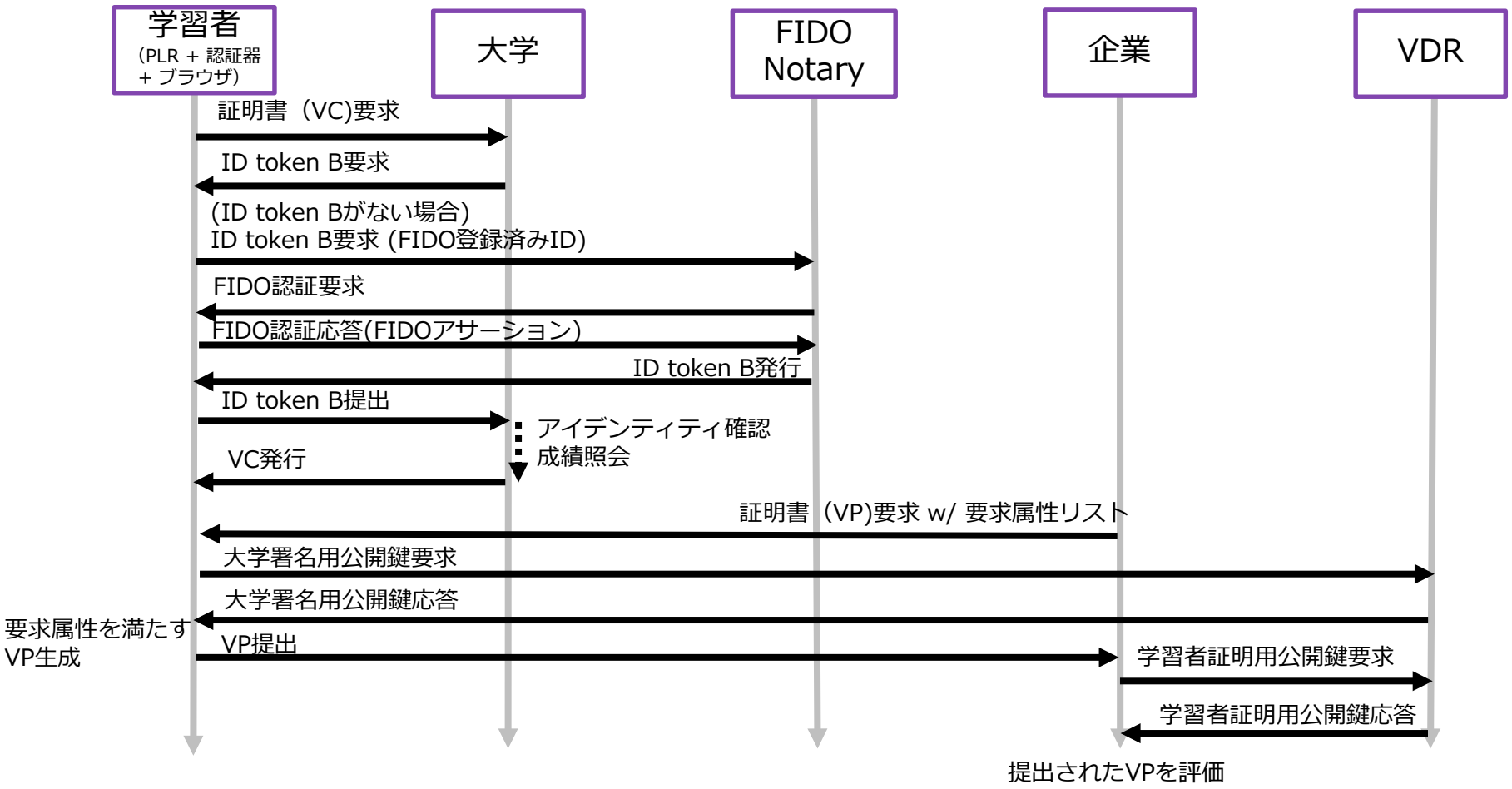
FIDO・DID登録



3.4 本実証で企画・開発したシステムの概要（1/6）

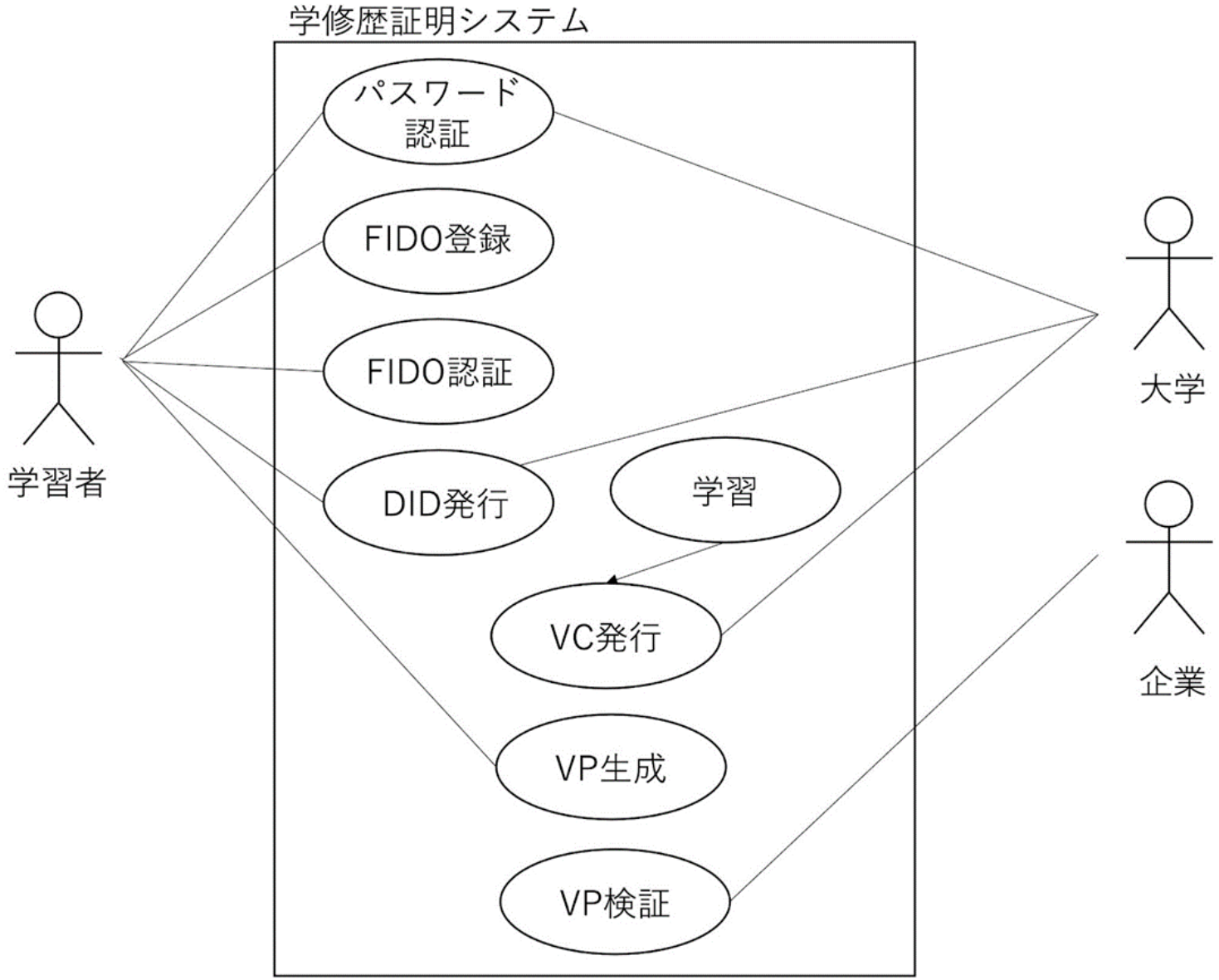
業務フロー

VC発行・VP提示



3.4 本実証で企画・開発したシステムの概要（2/6）

ユースケース図



3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）(1/3)

学習者が大学等とやり取りして端末を登録

「Trusted Web Test」チャネル(仮称)の設定に応じて、各ステップの操作は自動化が可能。次ページ以降も同様。

3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）

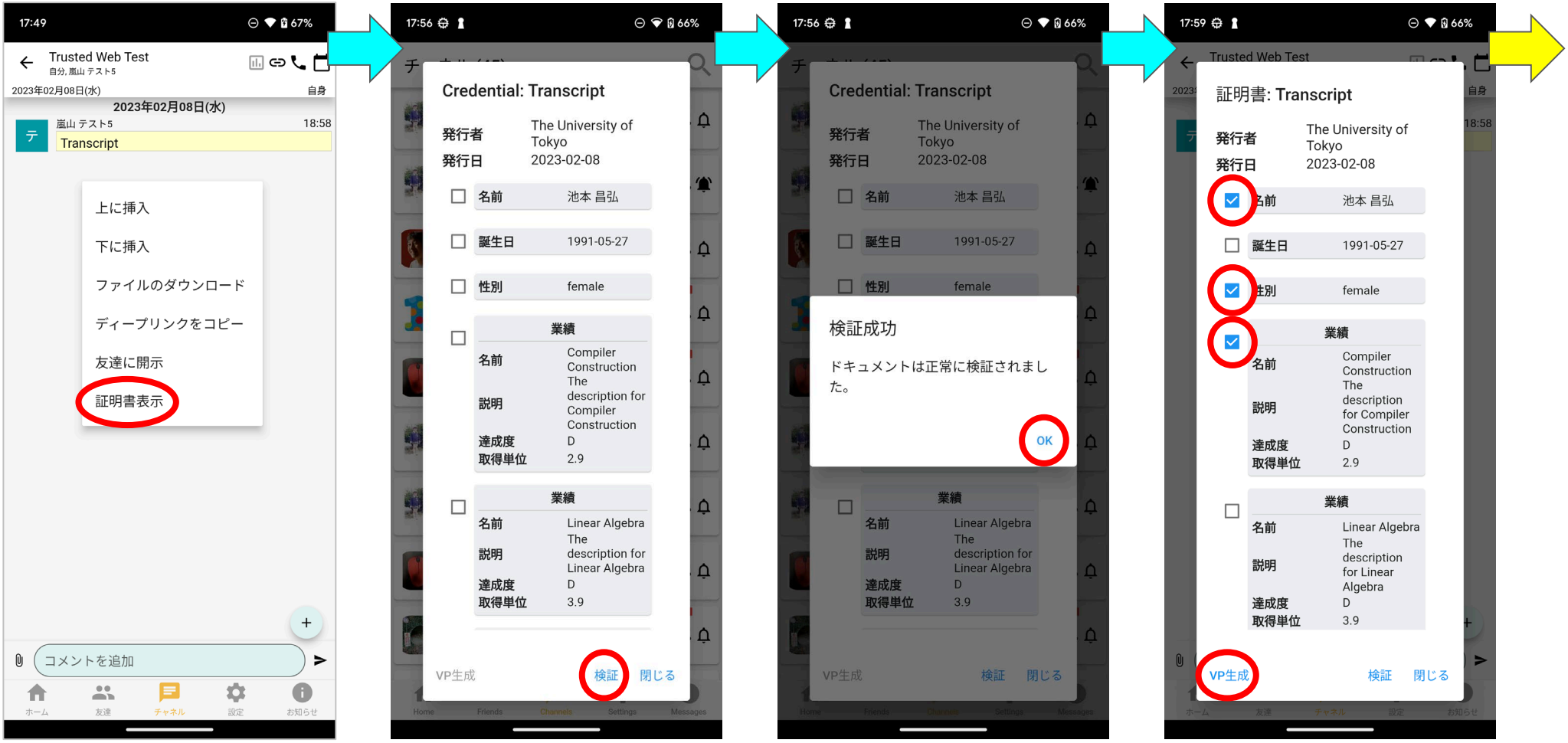
学習者がVDRからDIDを取得

学習者が大学等から成績証明書を取得

3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）

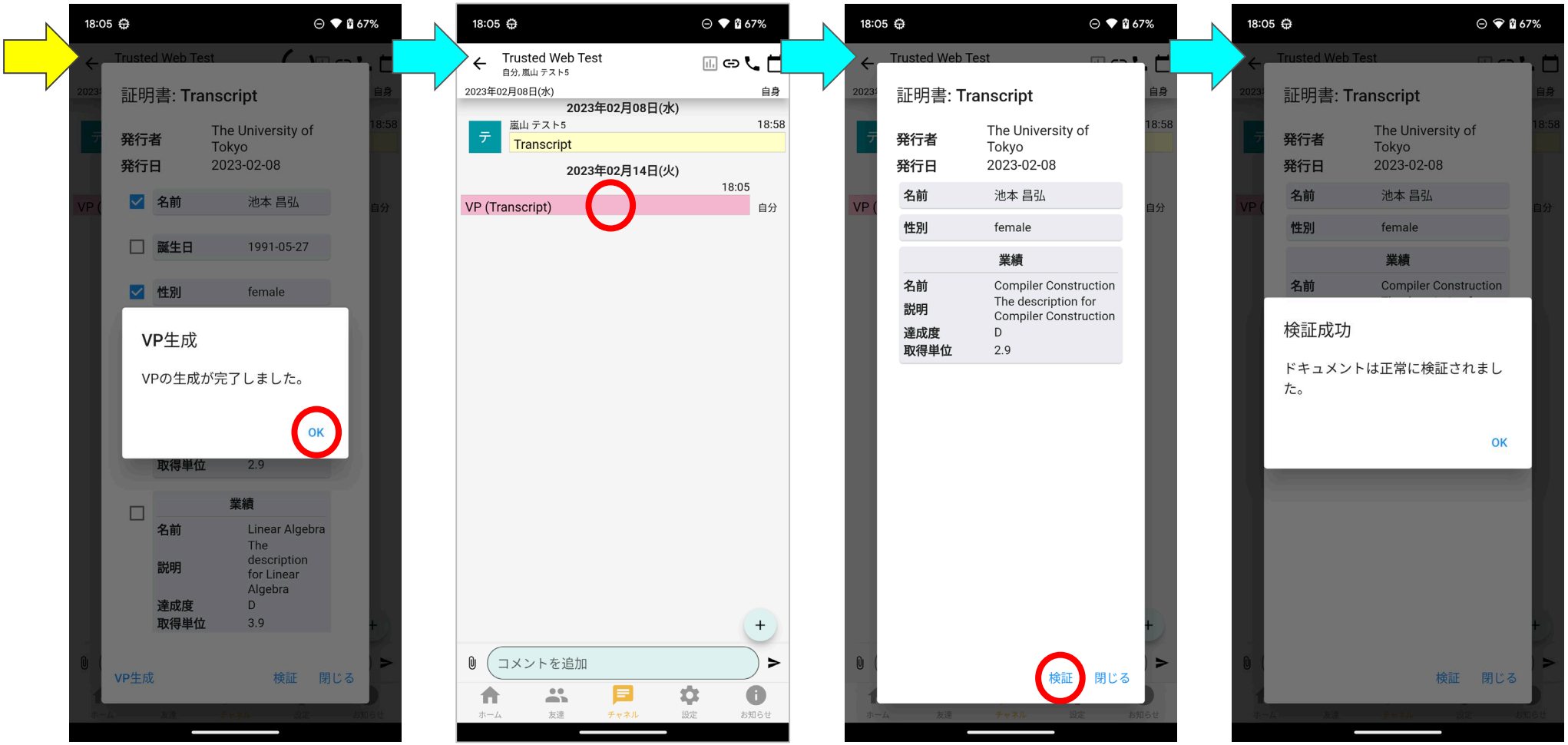
学習者がVCを表示して検証し、手動でVPを生成(実際には企業等からの開示要請に応じてVPを自動生成)



3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）

VPの生成と検証



3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）

企業等が学習者の開示履歴タイムラインに属性の開示要請を作成

3.4 本実証で企画・開発したシステムの概要（4/6）

機能/非機能一覧

機能/非機能	(非)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。

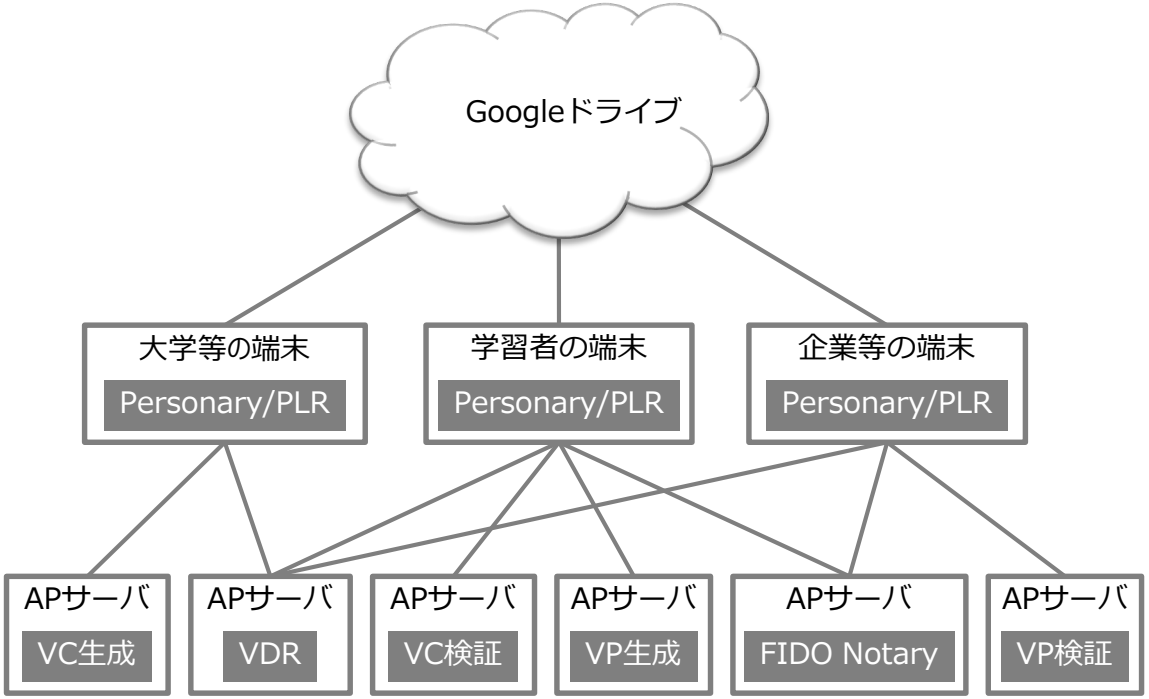
3.4 本実証で企画・開発したシステムの概要（5/6）

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 本実証で企画・開発したシステムの概要（6/6）

実験環境



システムの構成要素

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	—	OSS	Apache-2.0

3.5 実証を通じて得られた主な成果

システムの企画・開発に関する成果

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。

ビジネスモデルに関する成果

- 学修歴証明に関して日本は他の先進国や中国に比べてかなり遅れているので、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。学習者(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、社会的認知が非常に重要であることを再認識した。
- 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。
- 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

- 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。

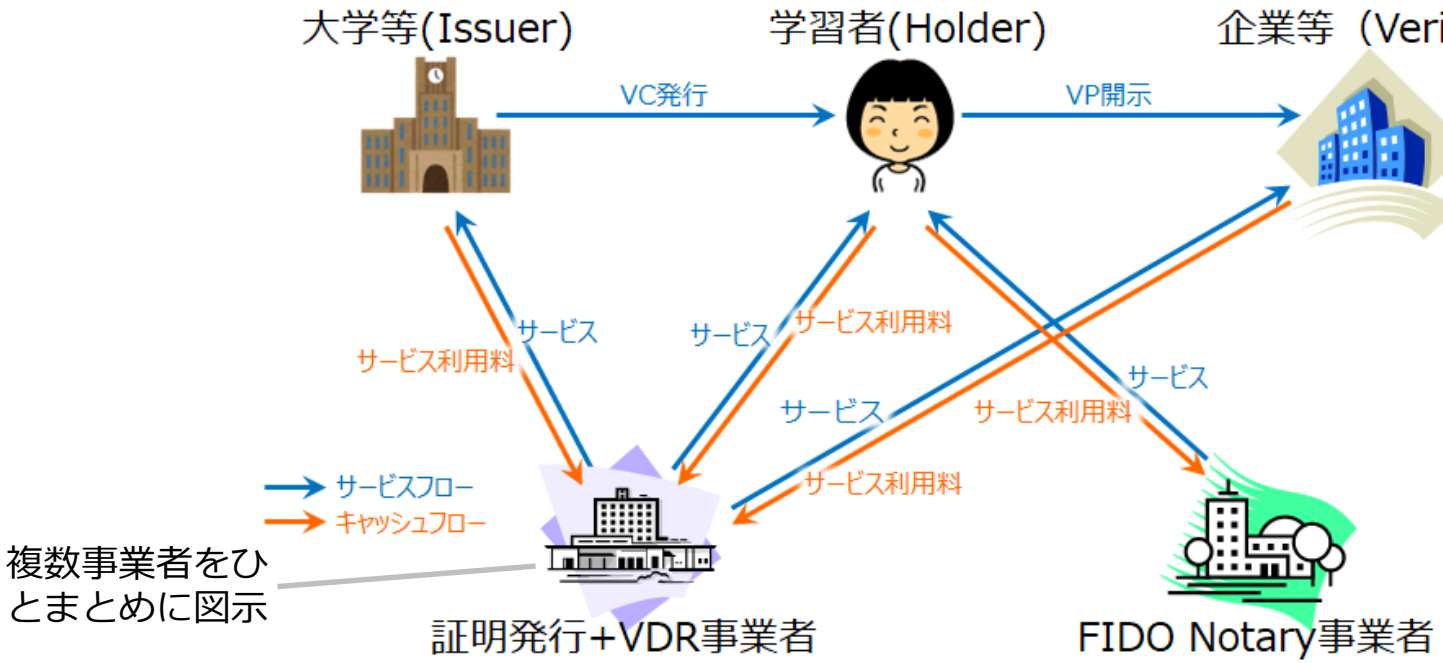
- 上記プロトタイプシステムのうちPersonaryはアセンブローグ社が権利を持つPLRライブラリを組み込んでいるが、商用でなければ無料で利用可能である。

04

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

ビジネスモデル



ユーザーのベネフィット

ステークホルダ	ベネフィット	負担するコスト
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

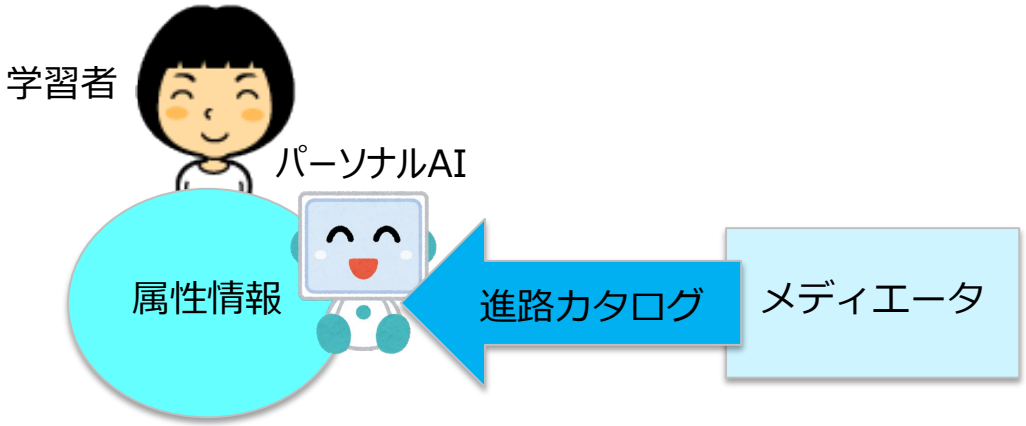
企業等がいったん取得した属性情報を所期の目的以外に使い回さないように、使用履歴が管理されることが必要である。分散台帳による履歴管理手法がいくつか提案されているが、使用履歴の台帳への登録を企業等に強制する手段がなければ有効でない。

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、労働市場の流動化等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。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、学習者に専属するパーソナルAI (PAI)がPLRに保管する本人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。
- 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。



05

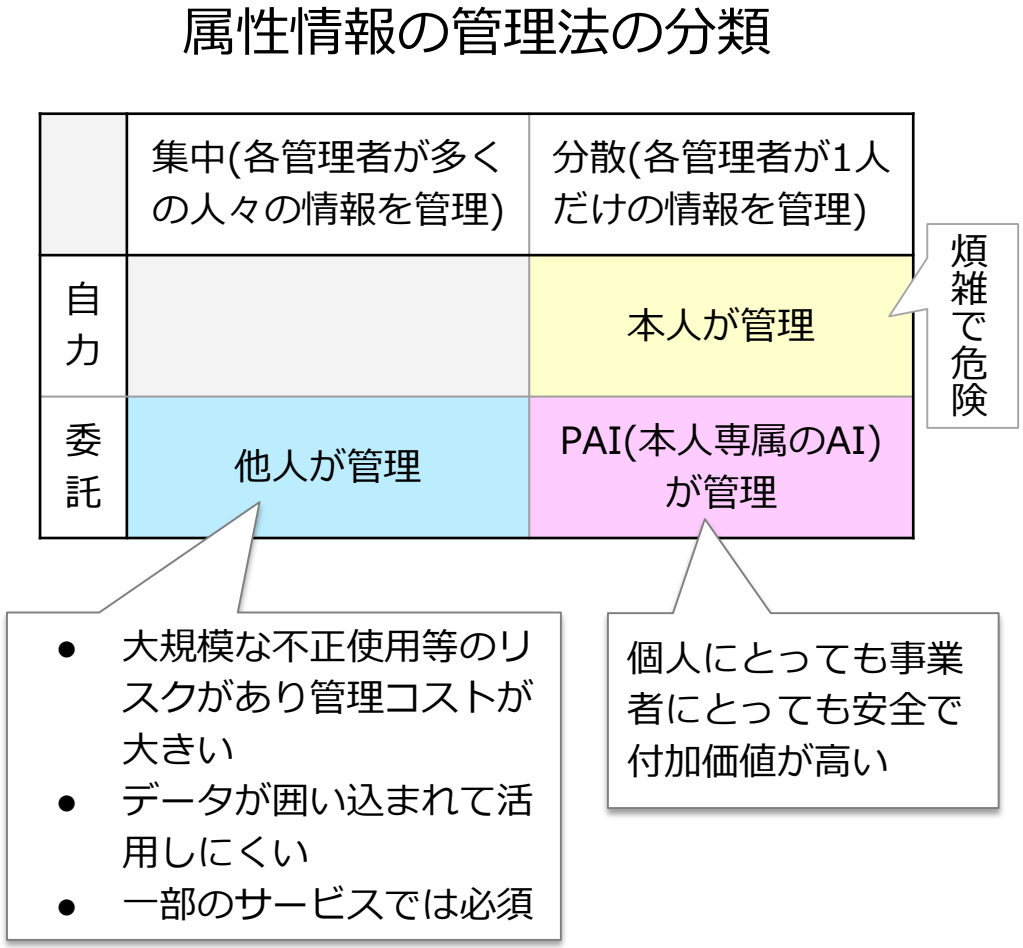
Trusted Webに関する考察

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。
- 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。

5.2　その他Trusted Webの課題と提言

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。属性情報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)に属性情報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。属性情報の管理は創造性を要しないので、AIが担うことはすでに十分可能である。



5.2　その他Trusted Webの課題と提言(続)

- 一般に検証すべき対象は多様であり、署名の検証だけでは不十分であることが多い。特にデータの内容の真正性や精度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。このような考察によって、Trusted Webにおける署名検証の有効範囲とTrustedWeb以外に必要な取り組みが明確になる。
- 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、データに関連づけて検証用の新規公開鍵を作成しDIDに紐付けてVDRから入手可能にする方法を考案した。これは他のユースケースにも広く応用できると考える。

5.2　その他Trusted Webの課題と提言(続)

- 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。
  - そのため、複数IDを束ねて運用するPLRの機能を設計中
- 検証(広義)可能な範囲を広げるとともに、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。
  - 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。

5.2 その他Trusted Webの課題と提言(続)

- 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
- 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

改善法の改善/メタガバナンス
設計・監査者同士のピアレビュー
や熟議(**分権的なガバナンス**)による
トラストの醸成

サービスの改善/ガバナンス
- PAI・サービスの改善/ガバナンス
- 人間や社会に関する研究
- 商品やサービスの開発
- 政策の立案と検証
- …

個別サービス
PDを本人に集約し
それをPAIがフル活用して
本人に介入