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

仮想空間サービスにおけるサービス利用資格と提供データのTrust検証

メタバース×自己主権型IDコンソーシアム

代表機関：NRIデジタル株式会社

参加団体：KDDI株式会社、KDDIデジタルデザイン株式会社、株式会社野村総合研究所

2023年2月17日

目次

01

背景・目的

1.1 背景･目的

背景

- 仮想空間サービス、いわゆるメタバースが急速に広まりつつあるが、利用者（アバター）、サービス提供者間の**売買契約などにおける利用者の資格情報を保証する手段が整っていない**
- 既存のWebサービス利用とは異なる**仮想空間サービスならではの課題**（没入感を維持したままでのTrust検証、視覚認識する対象者に対するTrust検証など）がある
- 仮想空間サービスの間、サービス間のシームレスな移動を実現するためには**web3の自己主権によるコントロールが重要**となる

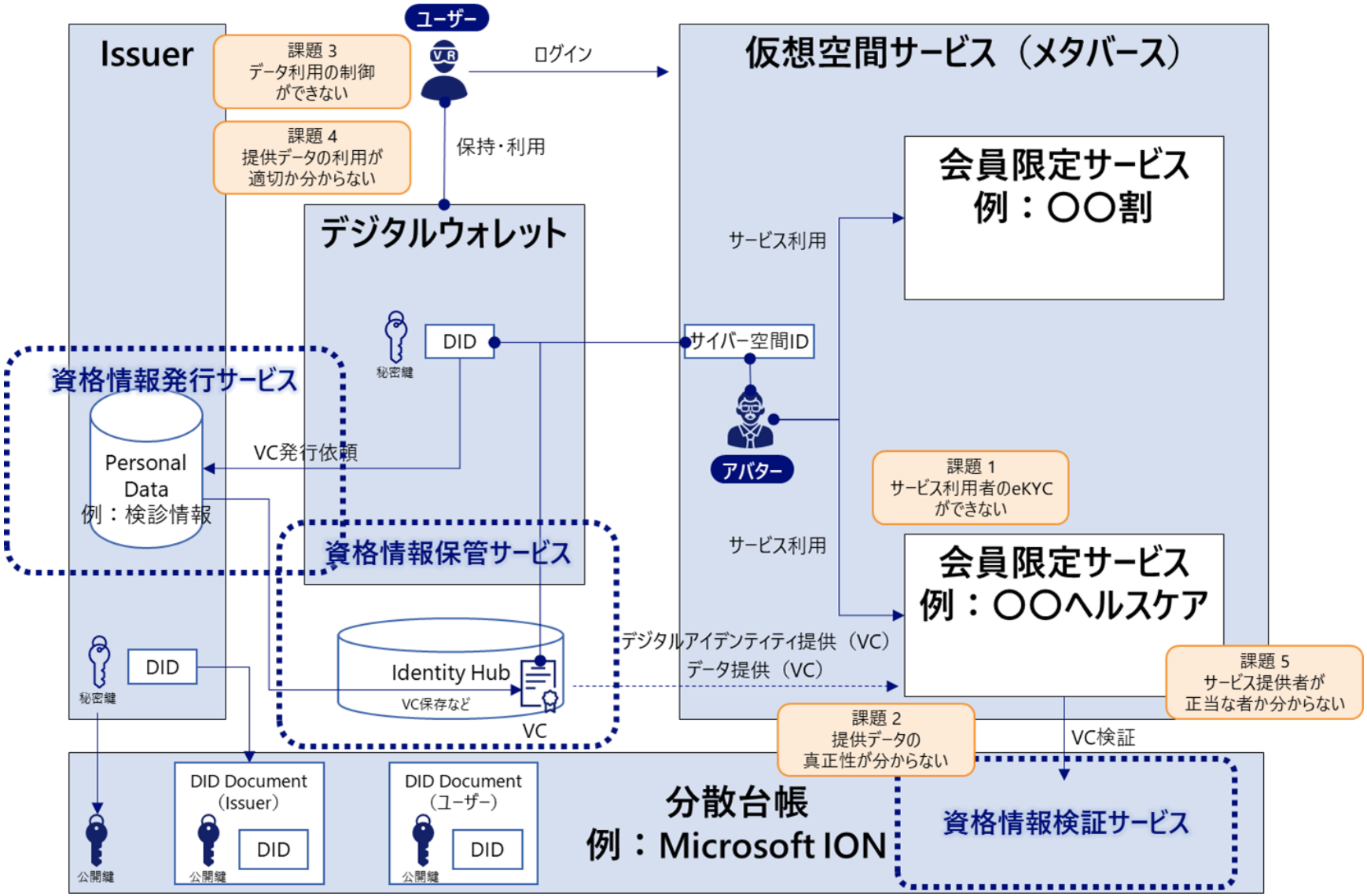
目的

- 仮想現実空間上のサービスを安心安全に利用できるようにすることで、仮想現実空間に関連するサービス利用を促進し、新たな市場を創出する。

02

実証の概要

2.1 実証概要及び実証の範囲



2.1 実証概要及び実証の範囲

プロトタイプシステムの企画・開発の内容

① デジタルウォレットを利用したDID/VC発行

- web3時代のB2Cビジネスにおいて、サービス利用者の属性情報および利用者関連情報を消費者起点で連携し制御するため、デジタルウォレットが重要。
- 当実証ではデジタルウォレットを利用して、DID/VCを発行し自己主権でのIDおよび関連データをコントロールできる仕組みを構築する。 ★⇒要件１へ対応
- サービス利用時にVC検証を行うことでサービス利用者の属性情報および利用者関連情報の正当性を証明でき、仮想空間サービス上のサービスを安心して利用できることを実証する。 ★⇒要件２へ対応

② VC提供に対する動的な合意形成とトレース

- サービス利用者の指示、合意によってVCがサービス提供者に渡され検証できる仕組み（Consent Management System）を構築する。 ★⇒要件３へ対応
- 合意破棄により速やかにデータ連携などを停止できる仕組みを作ることで、動的な合意形成の実現性を実証する。 ★⇒要件３へ対応
- 合意後のデータ利用情報についても利用者他が確認できる仕組みを実装することで、合意の履行がトレースできることを実証する。 ★⇒要件４へ対応

2.2 社会･経済に与える価値･影響

社会･経済に与える価値･影響

- 世界の仮想空間サービス市場の市場規模は、2020年に6.2兆円 に上ると推計されている。
- 今後も多様な用途への広がりが期待でき、Emergen Research社によると2028年には108兆円と推計される※。

- 仮想空間サービスにおいては、利用者（アバター）、サービス提供者間の売買契約などのTrust保証手段がない。本ユースケースは、Trustを保証するサービスを想定し、**約200億円の市場規模**を創出できると想定。
- 本ユースケースではリアル空間のユースケース、リアルと仮想現実を連携させたユースケースもサービス提供可能。それらをターゲットに含めると市場規模は、倍の約400億円を優に超えると想定。

- 日常的に複数仮想空間サービス、仮想空間サービス上の複数サービスを利用するようになった際には、複数仮想空間サービスの間、複数サービスの間のシームレスなデータ連携（利用者属性情報の移動）のニーズが高まることが想定され、それには自己主権での属性情報等のコントロールが重要。
- 本ユースケースは、自己主権での属性情報等のコントロールを実現することによって、仮想空間サービス自体の市場拡大にも寄与する。

※Emergen Research 「2028年に8,289億5,000万米ドルに達する世界のメタバース市場規模」
https://prtimes.jp/main/html/rd/p/000000041.000082259.html　1ドル130円換算

2.2 社会･経済に与える価値･影響

（補足）市場規模200億円の推計方法

推計方法は以下のとおり。ボトムアップ推計120億円とトップダウン推計271億円の平均である約200億円を採用

ボトムアップ推計
ユーザー数×本人確認サービス利用者割合×利用回数×単価 ＝ 3,000万人×80%×10回×50円 ＝ 120億円

ユーザー数：日本では約3,000万人 （人口の1/4がユーザーになるby Gartner）
本人確認サービス利用者割合：80%（大半のユーザが利用する想定）
利用回数：10回/年（月に1回程度利用する想定）
単価：50円 （金融機関のeKYCは数百円であることから妥当）

トップダウン推計
世界の本人確認市場×仮想現実上の市場割合×世界GDPの日本シェア ＝ 166.5億ドル×130円換算×1/4×5%
＝ 約271億円

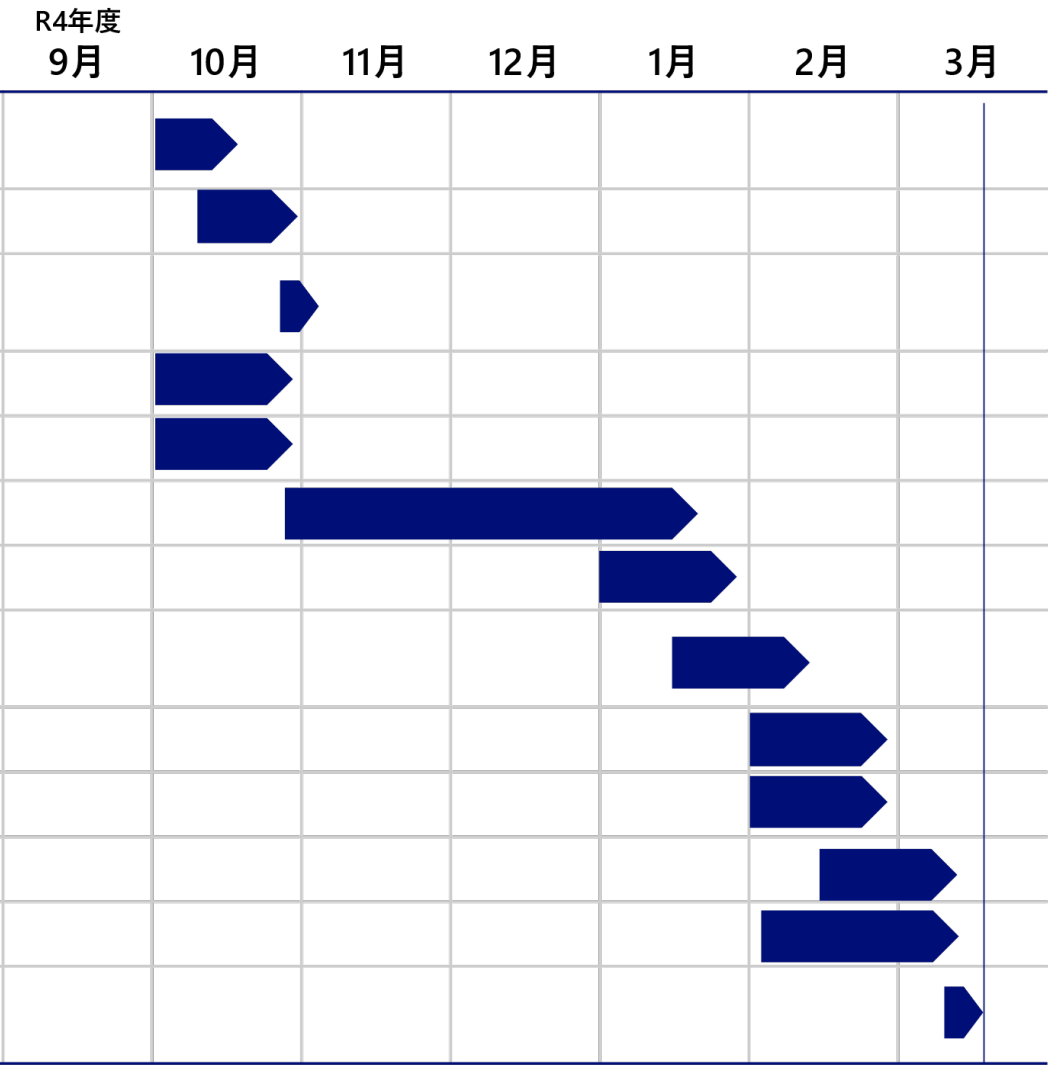
世界の本人確認市場：2026年までに166.5億米ドルに達すると予測
（https://www.mordorintelligence.com/ja/industry-reports/identity-verification-market）
仮想現実上の市場割合：1/4（想定）
世界GDPの日本シェア：5%

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

納期 3/15

#			担当
1	アプリ企画	要件定義	KDDI/NRId/KDI
2		基本設計	NRId
3		レビュー	KDDI/KDI/NRI
4	環境構築	サーバ環境構築	NRId
5		開発環境構築	NRId
6	アプリ開発	プログラミング	NRId
7		テスト	NRId
8	アプリ検証	仮想空間サービスへの組み込み	KDDI
9		機能検証	KDDI/NRId
10		ユーザUX検証	KDDI/NRId
11	成果報告作成	動画作成	NRId
12		ドキュメント作成	NRId
13		レビュー	KDDI/KDI/NRI



03

実証内容

3.1 実証の実施事項、論点及び判断（1/2）

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	本人の資格証明を行うための規格は何にするのか？	• メタバースでは様々な事業者がサービス提供を行う。そのため、情報提供スコープなどの事前取り決めが少ない、DID/VCを用いることとした • VPNなどの閉域NW内でしか発行できない本人証明が必要になる可能性があるため、DID/VCを用いることが良いと考えた
	DIDの連携プロトコルは何にするのか？	• OIDCを利用しているプレイヤーが多いと考えたためOIDCベースである、OIDC For VCI、SIOPを利用することが良いと考えた
	VCのデータプロトコルは何にするのか？	• 上記と同様の理由により、OIDC For VPを利用することが良いと考えた。
基本設計	ウォレットに相対するサーバは用意するのか？	• 企業の個人への影響を極力排除することが良いのではと考え、アプリ相対サーバは利用しないことが良いと考えた
	秘密鍵の管理はどうするのか？	• ユーザビリティを考え、バックアップサービスとして管理することが良いと考えた。 • バックアップサービスは利用者がアカウント登録し、そのアカウントを事業者が一括管理するため、自己主権型ウォレットとは切り離した別サービスとしてたてつけることが良いと考えた。
	発行されるVCはどこに格納するのか？	• 「ウォレットアプリがインストールされたスマートフォン内のストレージ」、「パブリックに公開されるブロックチェーン」、「IPFS」の候補から選択することとした。 • ブロックチェーンやIPFSはデータ削除が困難であるため除外した。 • バックアップサービスを提供するためデバイス紛失やデバイスの交換に起因する懸念は払しょくされるためスマートフォン内ストレージを選択した。

3.1 実証の実施事項、論点及び判断（1/2）

プロトタイプシステムの企画・開発

実施事項	論点	判断
基本設計	DIDメソッドは何にするか？	• 世界で最も利用されているのは「did:web」メソッドだが、本メソッドは公開鍵情報を各DID発行主体(HolderやIssuer)へ取得しに行く必要がある。本メソッドでは、自己主権型の検討の中で議論されるような、紛争が起きた国での人権保護の利用などに耐えられず、世界的な展開やスタンダード作成には向かないと考えた。 • 「did:web」の次に利用されているのは「did:ion」であり、「did:ion」の場合はIONノード上にDID Documentを格納するため、Issuer自体がなくなってもIONノード上に保存されているDID Documentを利用することで過去発行されたVCを検証することができるため、「did:ion」を選択した
システム開発	ウォレットアプリをインストールするデバイスは何にするのか？	• 今回の実証では仮想空間サービスへの導入を対象としているが、本来Verifierは仮想空間サービス以外にも存在し得る。今後Verifierがリアル空間のサービスになることもあると考えたため、スマートフォンをウォレットのデバイスにする方がユーザの日常利用にふさわしいと考えた。 • コンソーシアム内の関係者に通信キャリア企業がいるため、今後のサービス展開の強みになると考えスマートフォンを選択した。

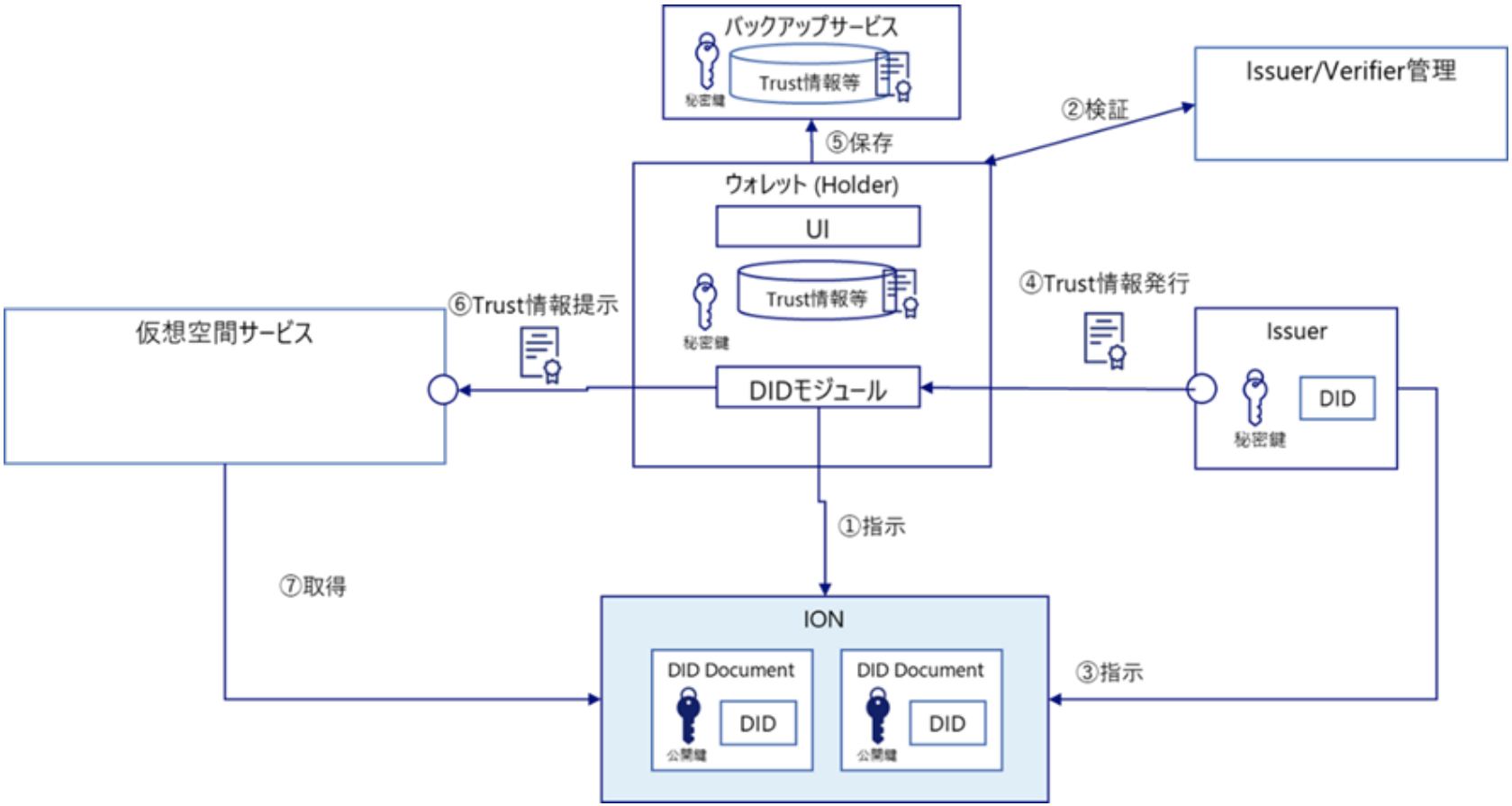
3.1 実証の実施事項、論点及び判断（２/２）

国際標準規格の調査

調査事項	調査対象機関	調査結果
DID/VCの仕様決定をするためにDID/VCに関する標準化機関を対象に調査を実施	W3C	「DIDs/VCs」について調査を実施した。 ・データモデルや項目定義、取りうるデータパターンについては定義されている内容を利用することができる。 ・各項目についてどんな値を入れるのか、どう使うのかについては明確な指示はない。 ・EXAMPLEとして記載されている内容から読み取らなければならない点も多い。 ・今回は限られたメンバーで認識が合えば利用できるため、規定されていない点や標準のEXAMPLEから読み取れた内容については、関係者間で認識齟齬が無いように定義して進めることとした。
	OpenIDFoundation	「OIDC For VCI、SIOP、OIDC For VP」について調査を実施した。 ・シーケンスについては定義されている内容で問題ない。 ・各シーケンスで利用するリクエストパラメータおよびレスポンスパラメータについて、項目定義がされている。ただし、任意項目が多く、どういうユースケースでどういう任意項目が必要になるのかが定義されていない。 ・OIDFの中で議論しているサポート対象は様々なユースケースを想定しているため、例えばオブジェクト自体が任意として指定されている項目がある。今回の実証実験では必要最低限の項目のみを設定することとして仕様策定を進めた。 ・クライアントIDの発行については、事業者の選択に任されている部分があったため、今回は事前取り決めが必要ないDynamic Client Registrationを併用することが良いと判断した。

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



3.2 検証できる領域を拡大する仕組み（1/3）

登場する主体とその概要

主体	役割・設定
ウォレット (Holder)	利用者が利用するウォレット。ウォレットの利用時には利用者とウォレットプロバイダーとの間で利用契約を締結する。
Issuer （＝本人資格情報提供者)	本人資格情報の管理者。依頼された本人資格情報をVCとして提示する。
仮想空間サービス （＝Verifier）	VPとして提示された本人資格情報を検証する。
バックアップサービス	ウォレットで発行したDIDの秘密鍵や発行されたVCをバックアップする。 ※今回の実証対象ではない
Issuer/Verifier管理者 （＝運営者）	IssuerおよびVerifierの正当性をチェックする。これは運営者の利益を追求するための仕組みではないため、公平に審査ができるように運営者は1社での運営ではなく、コンソーシアムでの運営が望ましい。 IssuerやVerifierから申請をもらい審査を行う。 ※今回の実証対象ではない

データへのアクセス

- 本システムでは、VCの元となる本人資格情報はIssuerが管理
- 利用者が利用するウォレットを介してIssuerに対して、本人資格情報を要求する
- Issuerは情報要求者の確認および開示範囲をウォレットへ提示したうえで、本人資格情報をVCとして発行する。
- VCとして発行された本人資格情報はウォレットに格納する。また、利用者の希望に応じてバックアップサービスでバックアップを行う。
- 仮想空間サービスはウォレットに、本人資格情報を要求する。
- ウォレットは要求された本人資格情報に対して、VCを選択し、開示条件を確認したうえで提示を行う。
- 仮想空間サービスは提示されたVCの検証を行う。

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データ及びデータのやり取りの内容

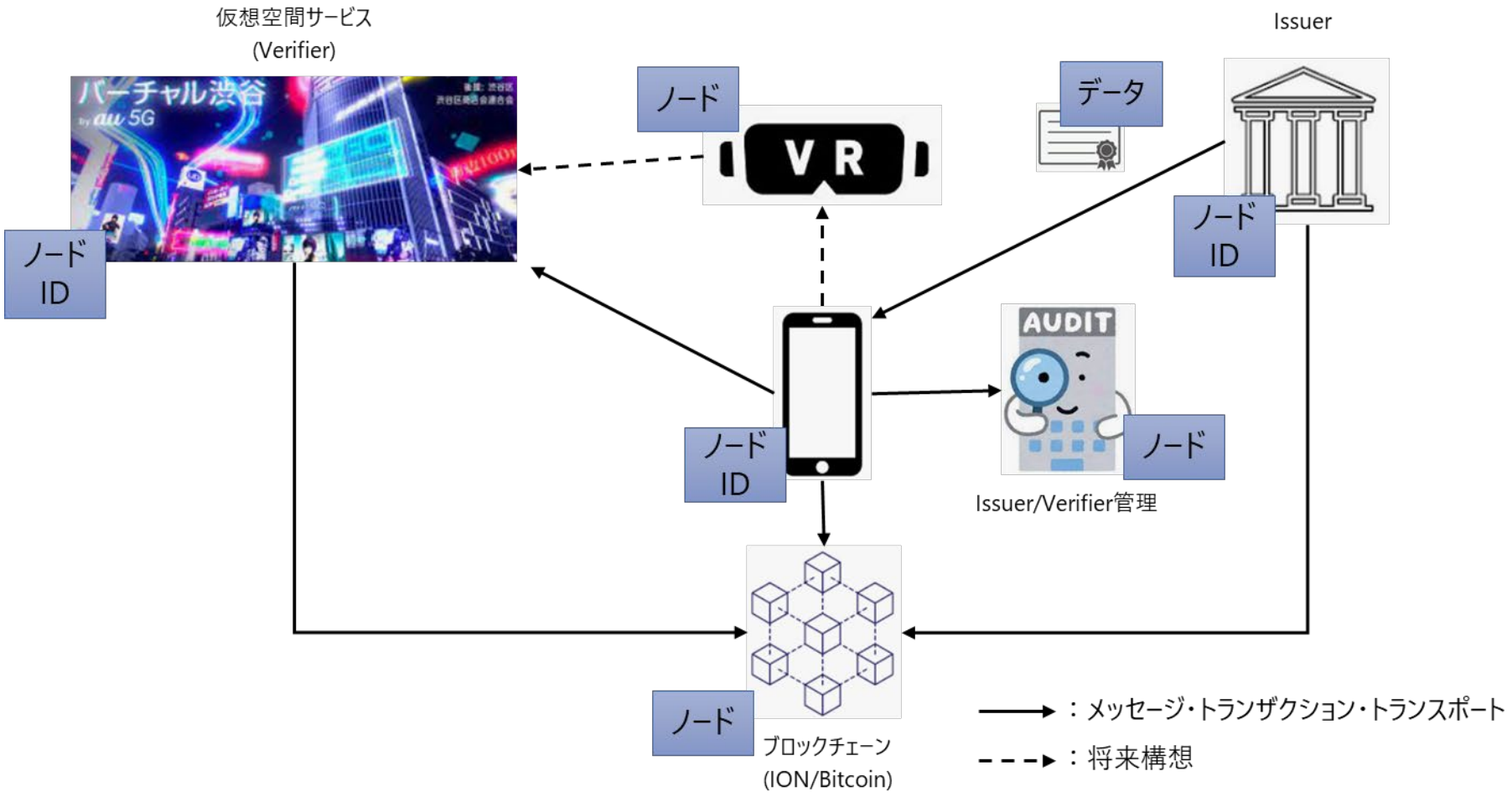
要検証の課題	検証対象	検証方法	検証者	保有者	発行者	データの置き場	アクセスコントロールの手法	成果・留意点
Issuer自身の真正性	Issuer自身	運営者による審査	運営者	Issuer	Issuer	なし ※強いて言うなら登記等	行政にならう	Issuer管理機能を具備する。 運営者の成り手が誰なのかが課題。
本人資格情報の真正性	本人資格情報	運営者による審査	運営者	Issuer	Issuer	Issuer 内ストレージ	Issuerのみアクセス可。	Issuerが持つ本人資格情報と発行した本人資格情報が一緒であることを第三者が審査する必要がある。
ウォレット(Holder)利用者の真正性	ウォレット自身	DIDの署名検証	・Issuer ・仮想空間サービス	ウォレット利用者(Holder)	ウォレッ利用者ト(Holder)	IONノード上	DID ResolverでのIONノードからのDID Document取得	OIDC For VCI/SIOPなどのプロトコル規定に従った検証
本人資格情報の真正性	本人色覚情報	VCの署名検証	仮想空間サービス	ウォレッ利用者ト(Holder)	Issuer	ウォレット格納デバイス(スマートフォン)の特定領域	スマートフォンの操作者によるPWD認証などのスマートフォンのロック解除	OIDC For VCI/SIOPなどのプロトコル規定に従った検証

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
ウォレット利用者とIssuer	学生証などの本人資格情報の発行	• これからVCとして発行する本人資格情報の内容を利用者へ許諾として表示し、利用者が許諾する	履行された左記の合意	ウォレット利用者	VC発行履歴として、ウォレット内に表示	• 考慮不要
ウォレット利用者と仮想空間サービス提供事業者	学生証などの本人資格情報の提供内容および利用用途	• 要求する本人資格情報の内容および利用用途について許諾として表示し、利用者が許諾しVC提供する	履行された左記の合意	ウォレット利用者	VC提示履歴として、ウォレット内に表示	• 合意の取り消しはシステム的な機能を整備するよりも、Issuer/Verifier管理(運営者)による監査や規定整備を行う方が効果的

3.3 6構成要素との対応



3.3 6構成要素との対応

#	要素	該当箇所	見解(課題含む)	備考
1	検証可能データ	ウォレットーIssuer間	・本人資格情報 ・ウォレット内に格納する	
2	アイデンティティ	Issuer 仮想空間サービス ウォレット	・DIDを発行するIssuer、仮想空間サービス、ウォレットが該当	
3	ノード	Issuer/Verifier管理 仮想空間サービス Issuer VRゴーグル ウォレット ION	・システムが存在するものにはすべてノードが存在する。	
4	メッセージ	ウォレットとIONのノード間	・DID Documentの格納のメッセージ(リクエスト・レスポンス) ・VC発行したIssuerの署名検証のためのIssuerのDID Documentの取得のメッセージ(リクエスト・レスポンス)	
5	トランザクション	ウォレットとIONのノード間	・OIDC For VCIプロトコルにより担保される	
6	トランスポート	ウォレットとIONのノード間	・HTTPSでの通信	
7	メッセージ	ウォレットと Issuer/Verifier管理	・Issuer管理の正当性チェック依頼のメッセージ(リクエスト・レスポンス)	
8	トランザクション	ウォレットと Issuer/Verifier管理	・1つのメッセージで完結するため、トランザクションとして担保する必要があるものはない	
9	トランスポート	ウォレットと Issuer/Verifier管理	・HTTPSでの通信	
10	メッセージ	IssuerとIONのノード間	・DID Documentの格納のメッセージ(リクエスト・レスポンス) ・ウォレットの署名検証のためのウォレットのDID Documentの取得のメッセージ(リクエスト・レスポンス)	

3.3 6構成要素との対応（続き）

#	要素	該当箇所	見解(課題含む)	備考
11	トランザクション	IssuerとIONのノード間	・OIDC For VCIプロトコルにより担保	
12	トランスポート	IssuerとIONのノード間	・HTTPSでの通信	
13	メッセージ	仮想空間サービスとIONのノード間	・VC発行したIssuerの署名検証のためのIssuerのDID Documentの取得のメッセージ(リクエスト・レスポンス) ・ウォレットの署名検証のためのウォレットのDID Documentの取得のメッセージ(リクエスト・レスポンス)	
14	トランザクション	仮想空間サービスとIONのノード間	・SIOPプロトコルにより担保	
15	トランスポート	仮想空間サービスとIONのノード間	・HTTPSでの通信	
16	メッセージ	ウォレットとIssuerのノード間	・本人資格情報の発行のメッセージ(リクエスト・レスポンス)	
17	トランザクション	ウォレットとIssuerのノード間	・OIDC For VCIプロトコルにより担保	
18	トランスポート	ウォレットとIssuerのノード間	・HTTPSでの通信	
19	メッセージ	ウォレットと仮想空間サービスのノード間	・本人資格情報の提供のメッセージ(リクエスト・レスポンス)	
20	トランザクション	ウォレットと仮想空間サービスのノード間	・SIOPプロトコルにより担保	
21	トランスポート	ウォレットと仮想空間サービスのノード間	・HTTPSでの通信	

3.3 6構成要素との対応（続き）

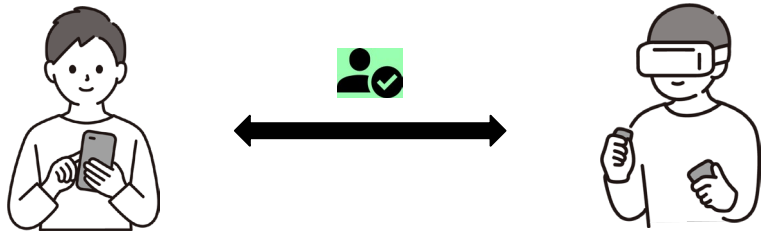
＜VRゴーグルを利用したケースのトラスト観点での示唆＞

実現すべき事項：

VRゴーグルを利用している「利用者の本人認証」を「没入感を維持したまま」実現すること

その際の要件：

- **端末仕様に依存しない**　（＝内部カメラの有無、Bluetoothの有無などに依存しない）
- **第三者から見ても分からない**　（＝本人認証時の知識情報が外部に漏れない）
- **外部のデバイスを触ることがない**　（＝没入感の維持）



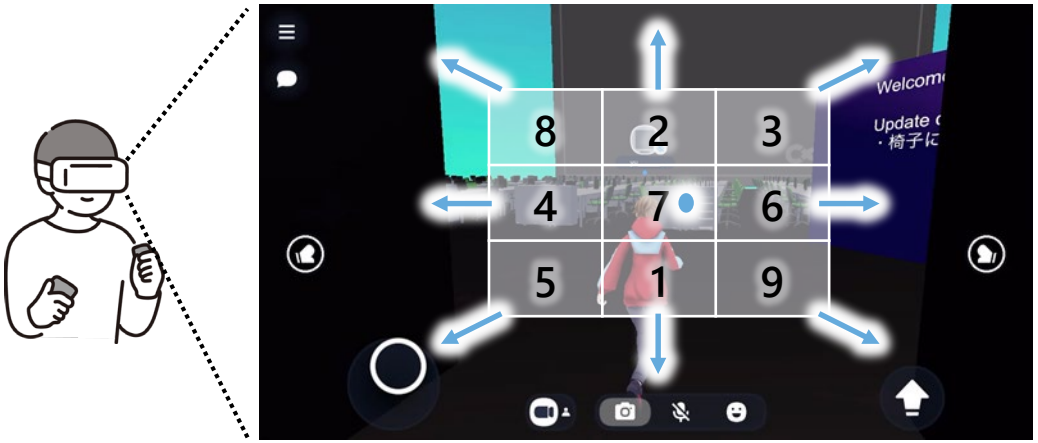
3.3 6構成要素との対応（続き）

各要件に対して、次のような解決方針を検討した。

No	要件	解決方針
1	利用者の本人認証	知識情報による認証（PINコード入力など）
2	端末仕様に依存しない	端末独自機能を利用しない（ジェスチャーなどVR内操作で実現）
3	第三者から見ても分からない	認証操作のランダム生成（認証パターンを都度ランダム生成）
4	外部のデバイスを触ることがない	外部デバイスを利用しない（ジェスチャーなどVR内操作で実現）

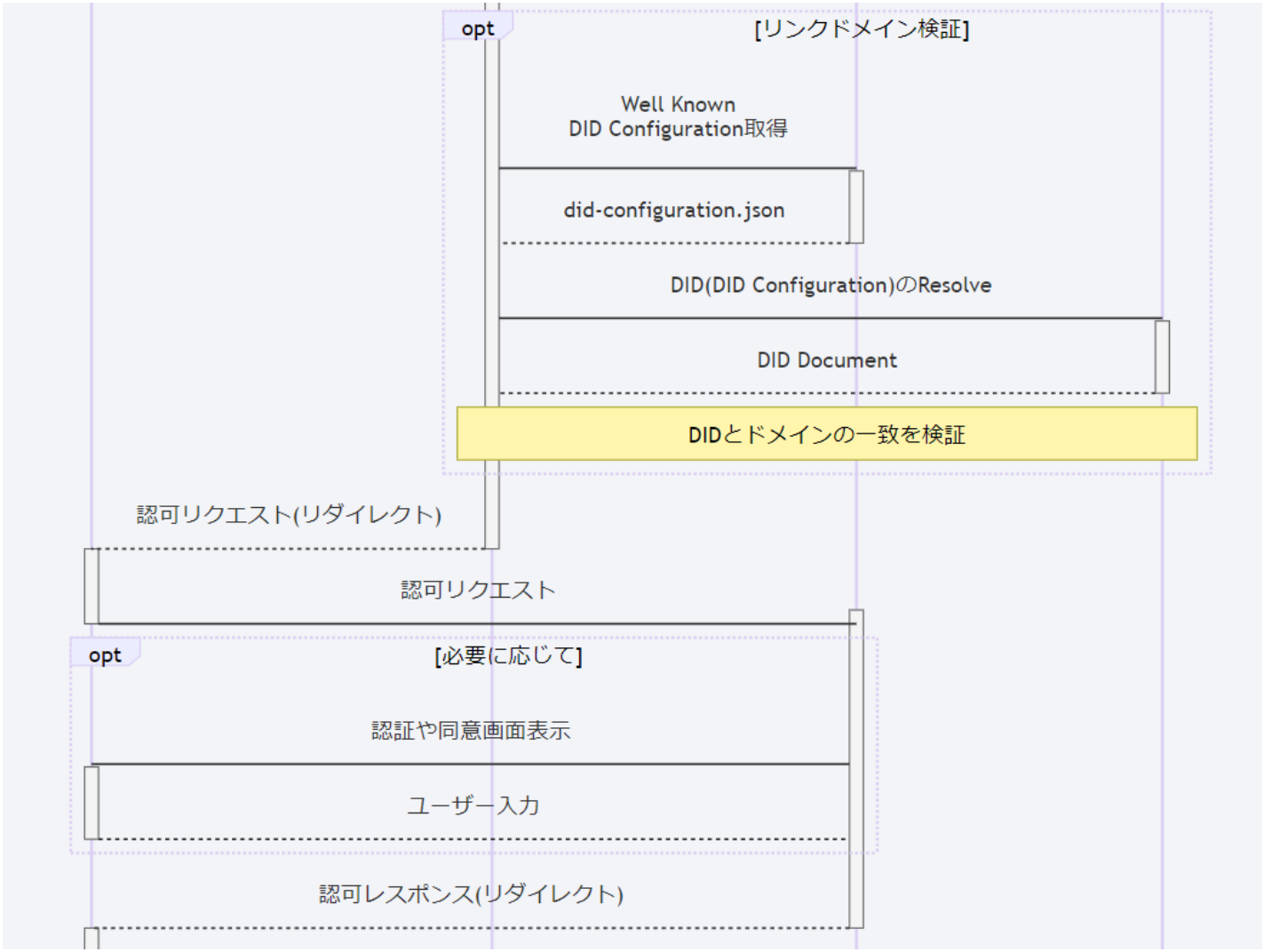
実現イメージ例

- 予めPINコードを決定
- 認証タイミングでVR空間に認証機能表示
- ジェスチャーで矢印方向を入力
- 数字の位置は毎回ランダム生成



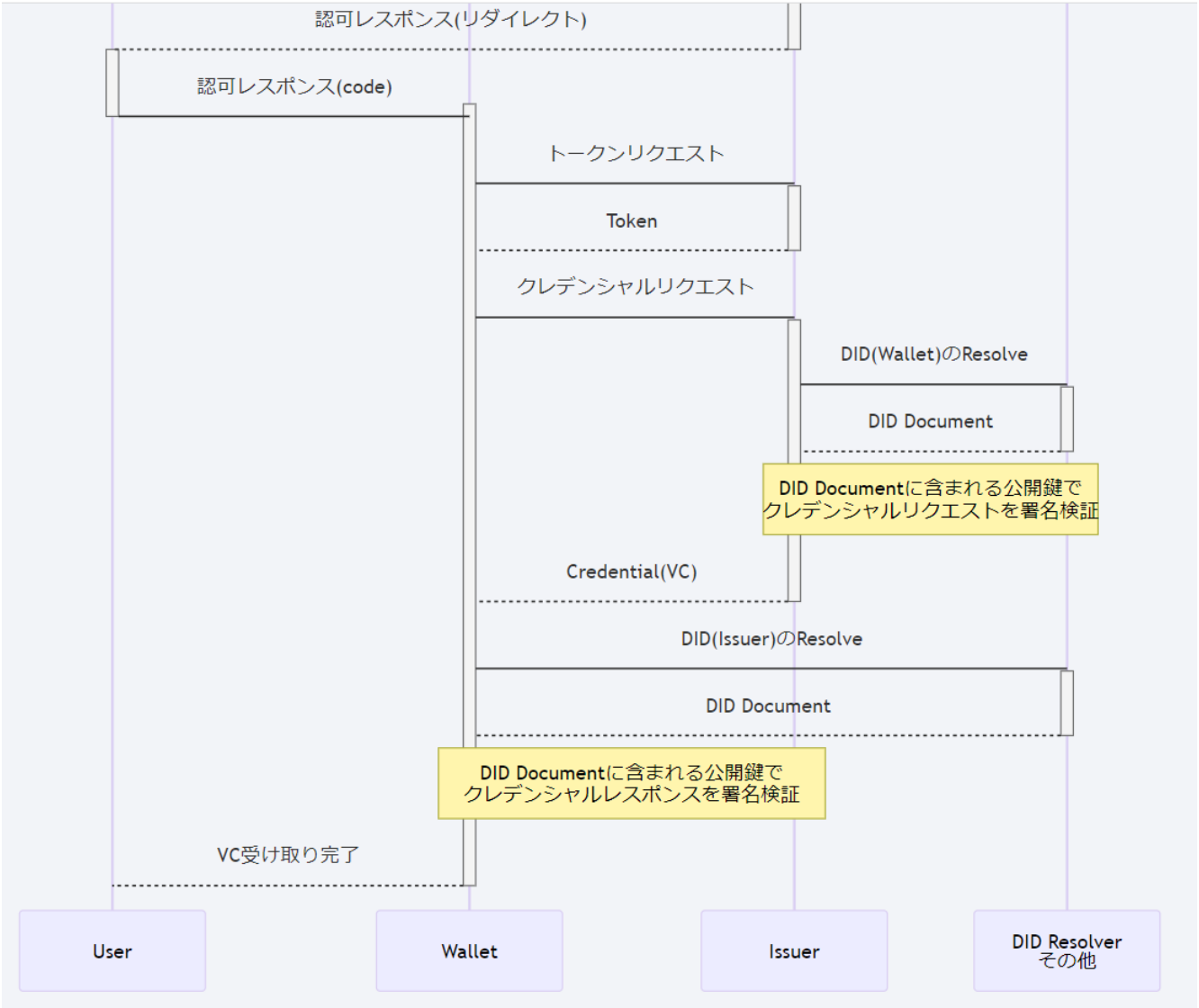
3.4 本実証で企画・開発したシステムの概要（1/6）

業務フロー



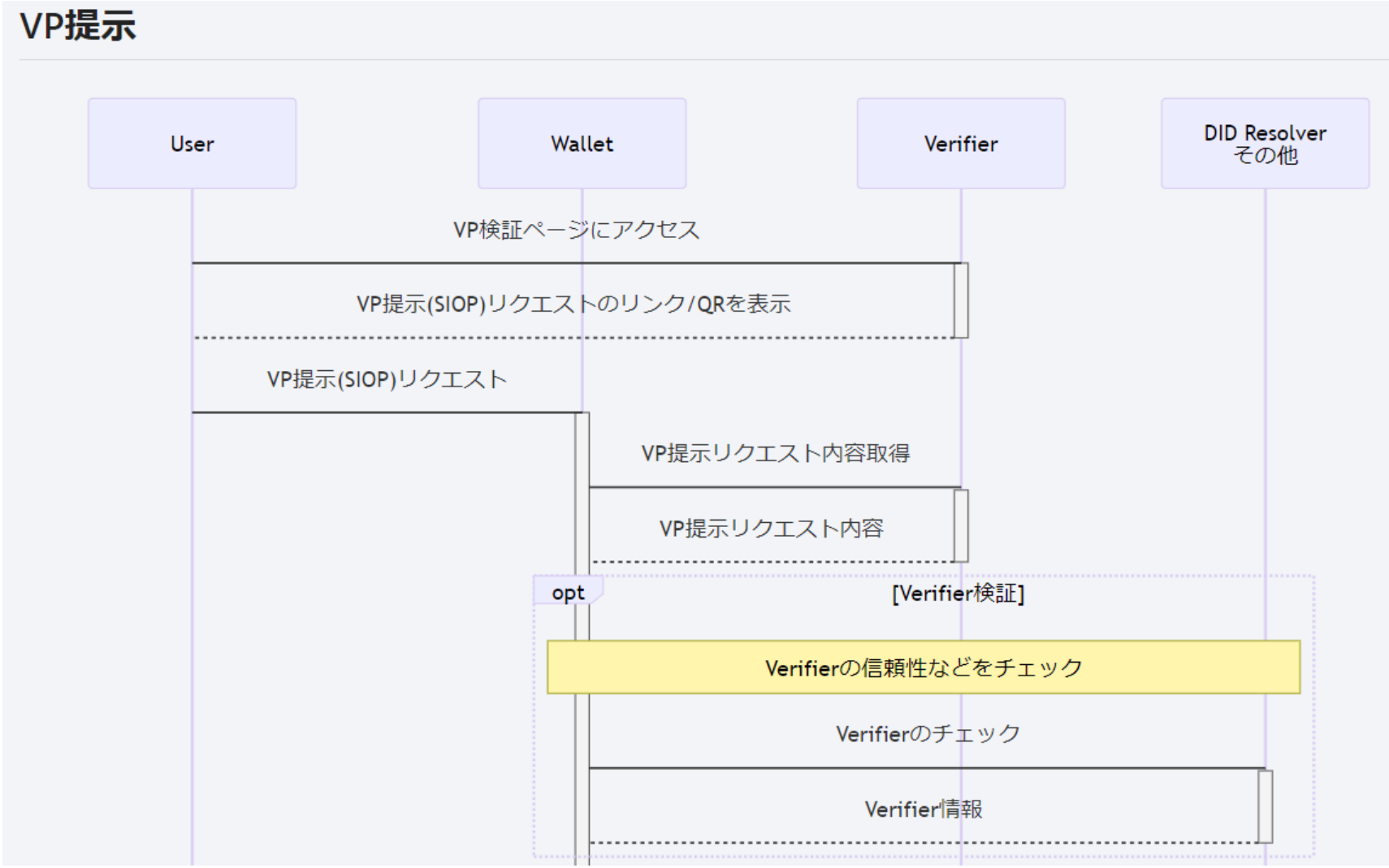
3.4 本実証で企画・開発したシステムの概要（1/6）

業務フロー



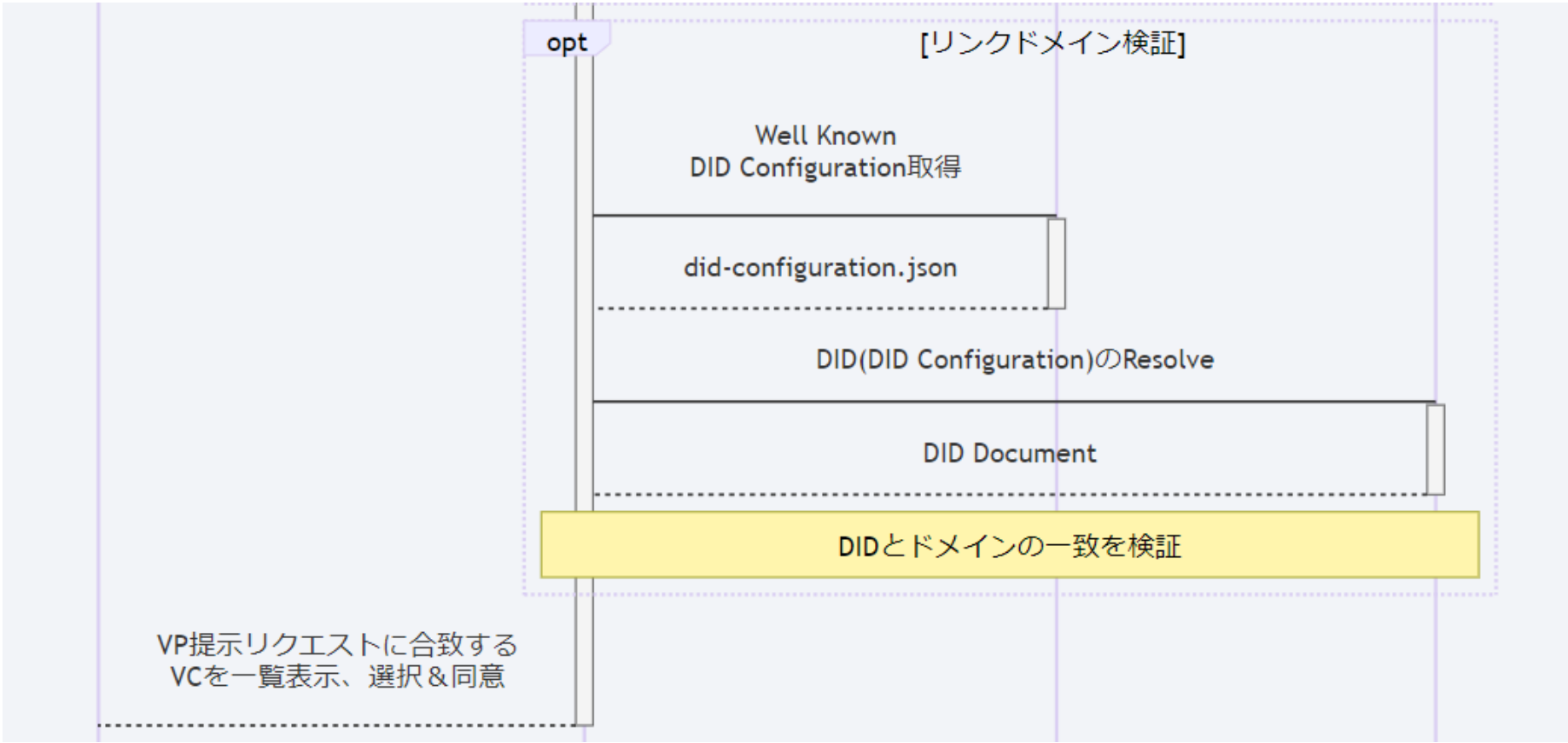
3.4 本実証で企画・開発したシステムの概要（1/6）

業務フロー



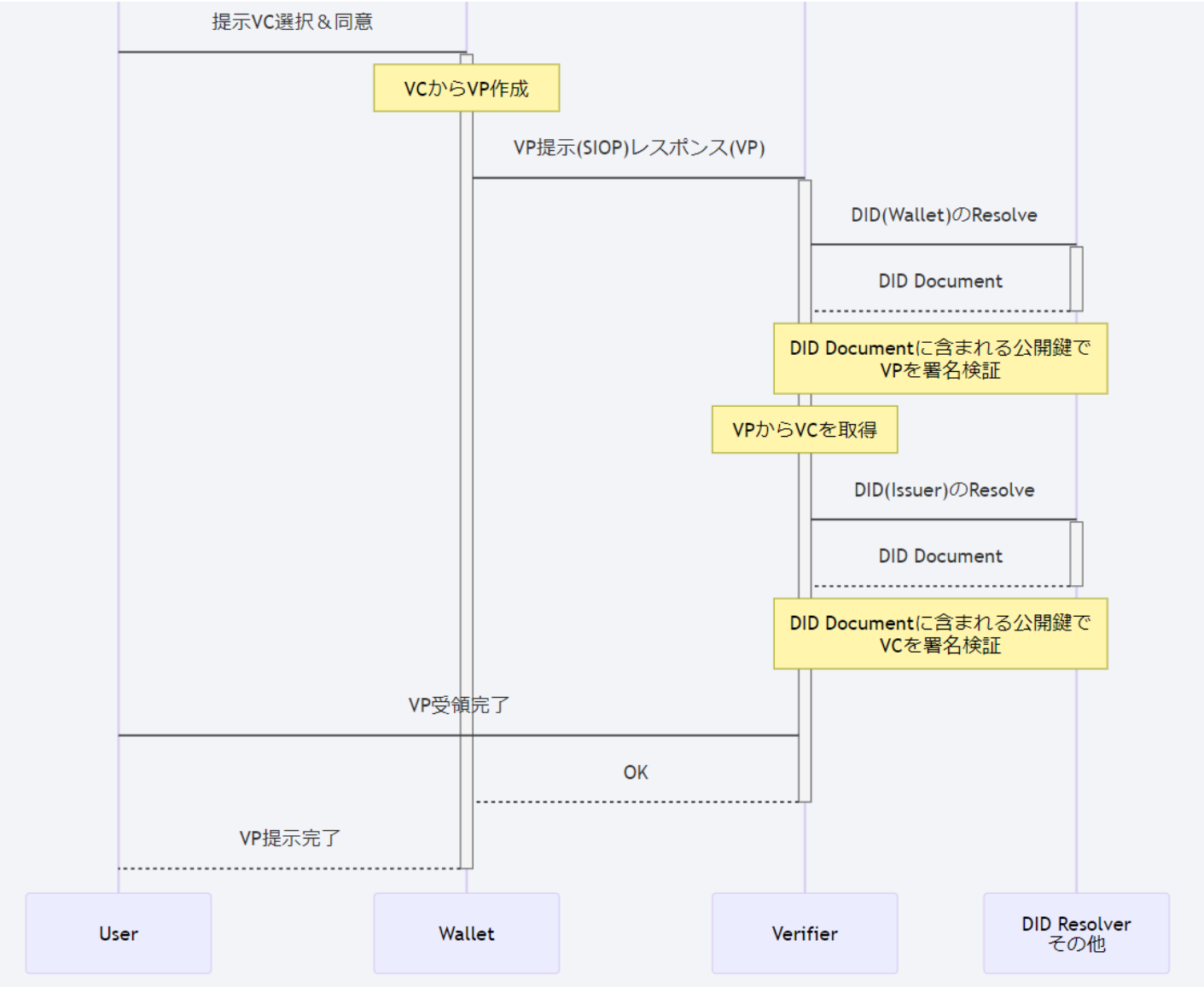
3.4 本実証で企画・開発したシステムの概要（1/6）

業務フロー



3.4 本実証で企画・開発したシステムの概要（1/6）

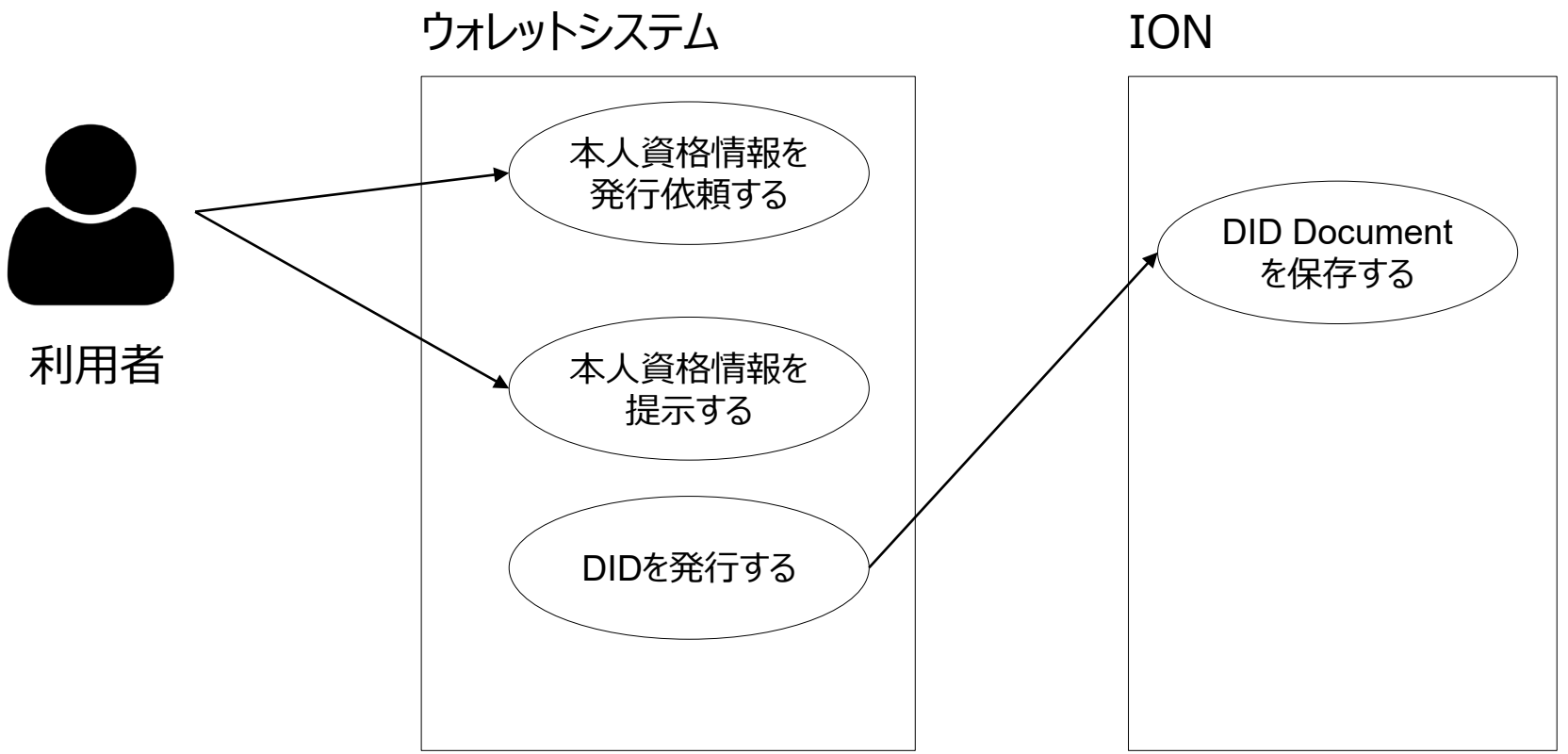
業務フロー



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

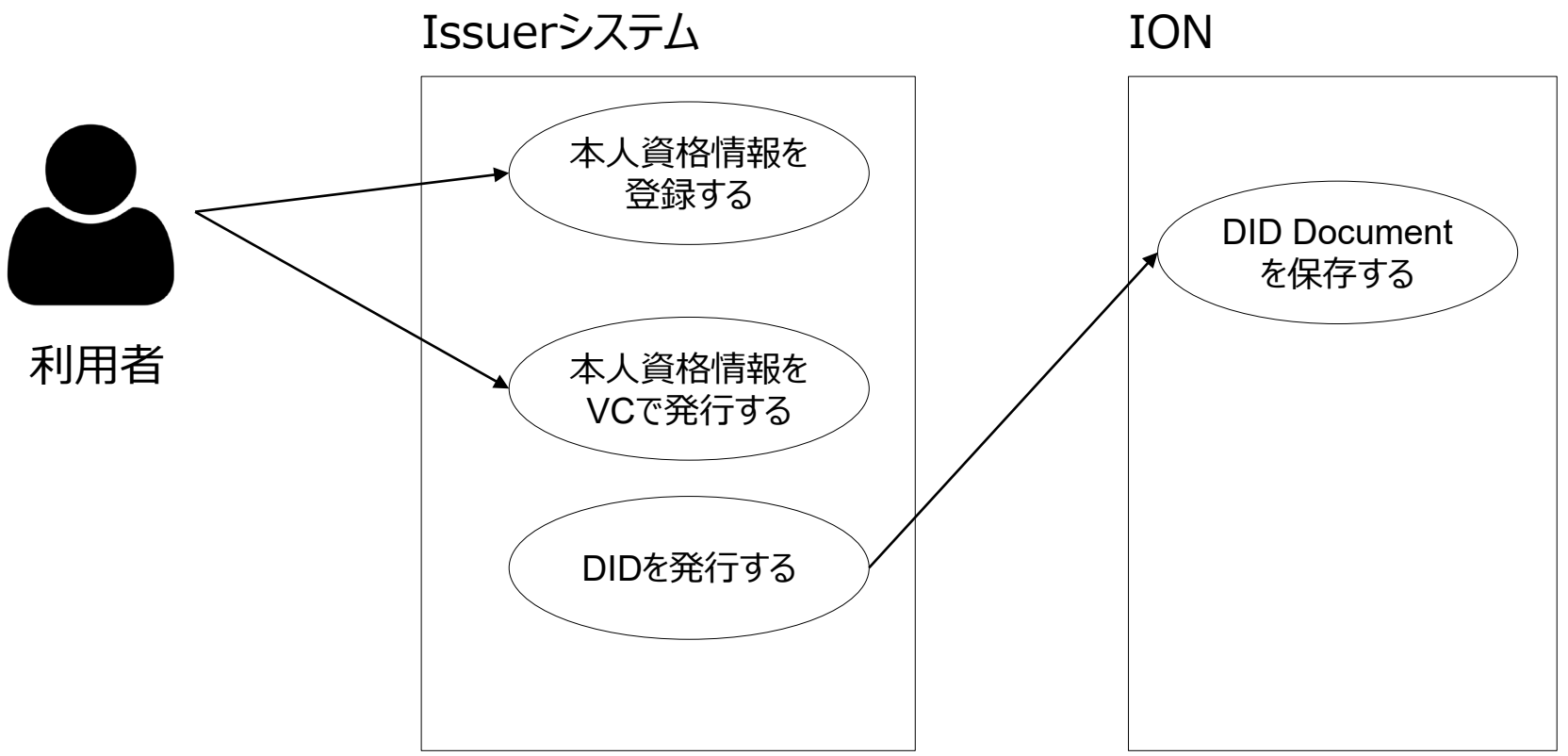
ウォレットシステム利用ケース



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

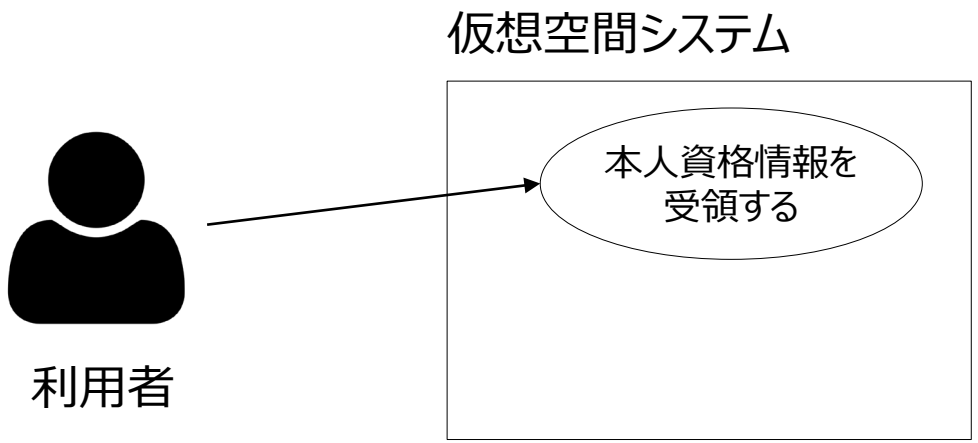
Issuerシステム利用ケース



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

仮想空間システム利用ケース



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)

①ユーザーがTrust情報発行事業者(Issuer)にVC発行を依頼

a. ユーザーがIssuerシステムにログイン
b. ユーザーがIssuerのVC発行ページにアクセス
c. ユーザーがVC発行リンクをクリック → Walletに遷移
d. Walletのユーザー認証
e. WalletがIssuerからメタデータ取得
f. WalletがIssuerの信頼性を検証(ドメインとDIDの紐づけ確認)
g. WalletはIssuerからトークンを取得
h. Walletはトークンを用いてIssuerにVC発行をリクエスト

②Trust情報発行事業者はVCを発行

a. Issuerは分散台帳からWalletの公開鍵を取得し、Walletからのリクエストの署名を検証
b. IssuerはWalletにVCを発行
c. Walletは分散台帳からIssuerの公開鍵を取得し渡されたVCの署名を検証する。
(VCの受け取り完了)

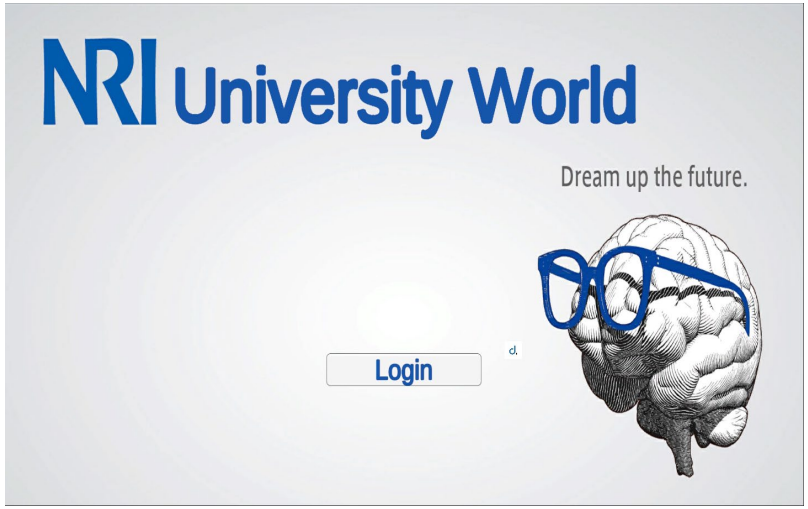
3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI） (2/3)

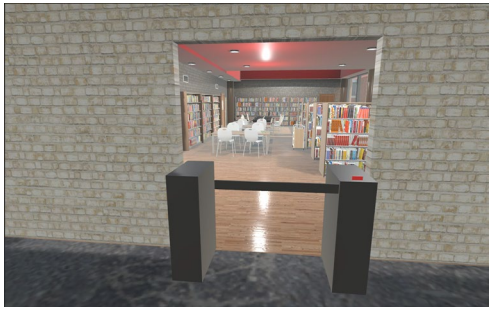
⑤サービス提供者がTrust情報発行事業者(Issuer)にVC検証を依頼

a. ユーザーが図書館の前に行く
b. ユーザーがPIN入力を行う → Walletを開く
c. ユーザーがWalletをゲートにかざす

d. IssuerはVCを検証(分散台帳に問い合わせる)
e. IssuerはVCの検証結果をサービス提供者に返す



⑤a



⑤b

⑤c

⑤de

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） (3/3)

⑥サービス提供

a. サービス提供者がVC提示完了の旨をユーザーに返す
b. ゲートオープン
c. ユーザーが図書館を利用できるようになる

⑥a

⑥b

⑥c

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	機能名	機能概要
機能	DID発行	ウォレットが自身のDIDを発行し、DID DocumentをIONへ格納する
機能	VC発行依頼	ウォレットがIssuerに対してVCを発行依頼する
機能	VC発行前許諾	IssuerがウォレットにVCを発行する前に、許諾取得を行う。
機能	Issuerチェック	Issuerの信頼性を確認する
機能	発行済みVC確認	ウォレット内で管理されているVCを確認する。
機能	合意済み許諾一覧確認	合意した許諾の一覧を確認する。
機能	VP提示	ウォレットが仮想空間サービスに対してVPを提示する。
機能	VP提示前許諾	仮想空間サービス提供事業者がウォレット利用者に対してVP提示前に、開示条件を提示し、許諾を取得する。

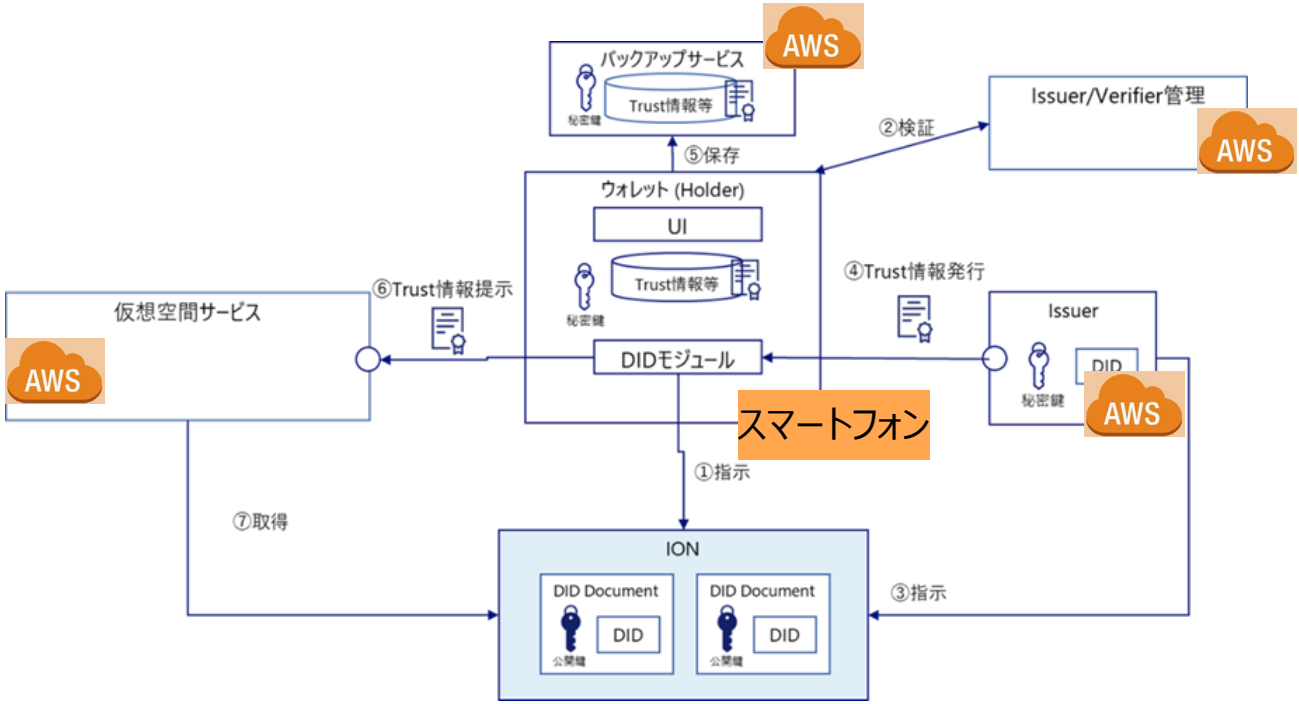
3.4 本実証で企画・開発したシステムの概要（5/6）

データモデル定義

No	項目名	要素名	属性	必須／任意	項目説明
1	JWT ID	jti		○	発行クレデンシャル識別子
2	発行者	iss		○	発行者DID
3	サブジェクト	sub		○	ホルダーDID
4	JWT発行日時	iat		○	クレデンシャル発行日時
5	有効開始日時	nbf		△	クレデンシャル有効開始日時
6	有効期限	exp		○	クレデンシャル有効期限
7	ノンス	nonce		○	クレデンシャルエンドポイント リクエストで受けた
8	クレデンシャルクレーム	vc	Object	○	クレデンシャルクレーム
9	構成コンテキスト	@context	Object[]	○	解析に必要な用語定義
10	クレデンシャル識別子	id		△	クレデンシャルステートメント（声明）を表すURI
11	タイプ	type	Object[]	○	クレデンシャルタイプ
12	クレデンシャルスキーマ	credentialSchema	Object[]	△	クレデンシャルクレームの構文チェックスキーマ
13	クレデンシャルスキーマ識別子	id		○	スキーマファイルを識別するURI／DID
14	クレデンシャルスキーマタイプ	type		○	スキーマタイプ／DIDスキーマ
15	クレデンシャルステータス	credentialStatus	Object	△	クレデンシャルのステータスを検証する方法を記載
16	クレデンシャルステータス識別子	id		○	クレデンシャルステータスのエンティティを取得する
17	クレデンシャルステータスタイプ	type		○	クレデンシャルステータスのタイプ
18	クレデンシャルサブジェクト	credentialSubject	Object Object[]	○	クレデンシャルサブジェクト 配列可
19	クレデンシャルサブジェクトクレーム	(Claims)		○	クレデンシャルタイプで定義されたClaim
23	利用規約	termsOfUse	Object[]	△	利用規約情報
24	利用規約タイプ	type		○	利用規約タイプ

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
ウォレット	—	NRIデジタルが保有	—
仮想空間サービス	—	KDDIが保有	—
Issuer	—	今回シミュレーターとして開発	—
ION	—	OSS	Apache License 2.0

3.5 実証を通じて得られた主な成果

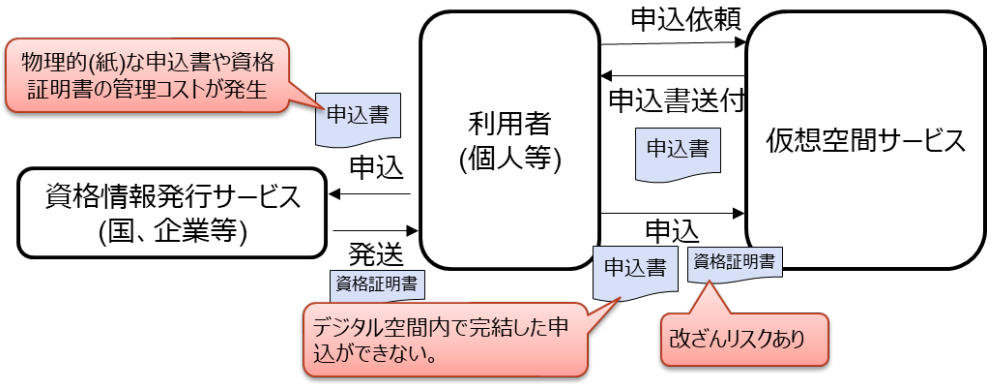
システムの企画・開発に関する成果

- 本人資格情報の授受のスキームについて
  - 課題解決前のスキームでは、本人資格情報を仮想空間サービスで利用しようとした場合、物理的な申込書を用いて、事業者へ郵送などで送る必要があった。そのため、仮想空間サービスで業務が完結することはなかった。
  - 本実装のスキームでは、本人資格情報をVCとすることで、改ざん検知をしつつ、仮想空間サービスで業務を完結することができるようになった。
- メタバースならではのプライバシー保護の観点の課題検討をした
  - メタバースの中で本人特定性とプライバシー保護の両者を満たす手段を検討する必要がある。

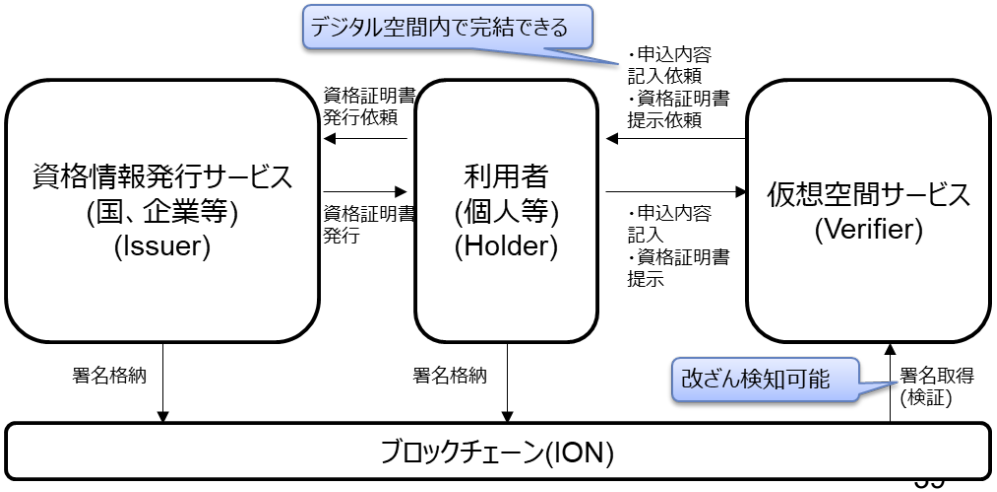
ビジネスモデルに関する成果

- Trusted Webが拡がるためのマネタイズ課題を検討した
  - 資格情報発行サービスであるIssuerは個人情報管理を行う必要があり、それに伴うセキュリティ対策などの継続的なコストが発生するため、Issuerにに収益が入るモデルを作る必要がある。
  - 仮にIssuerからVerifierへの一時的な情報利用料を渡したとしても、発行した資格情報に対してのデータトレーサビリティを確保できる仕組みがないと、Issuerはコストをかけて情報をTrust化したことに関しての収益が生まれない。

課題解決前のスキーム図（As-Is）



本実証ユースケースのスキーム図（To-Be）



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

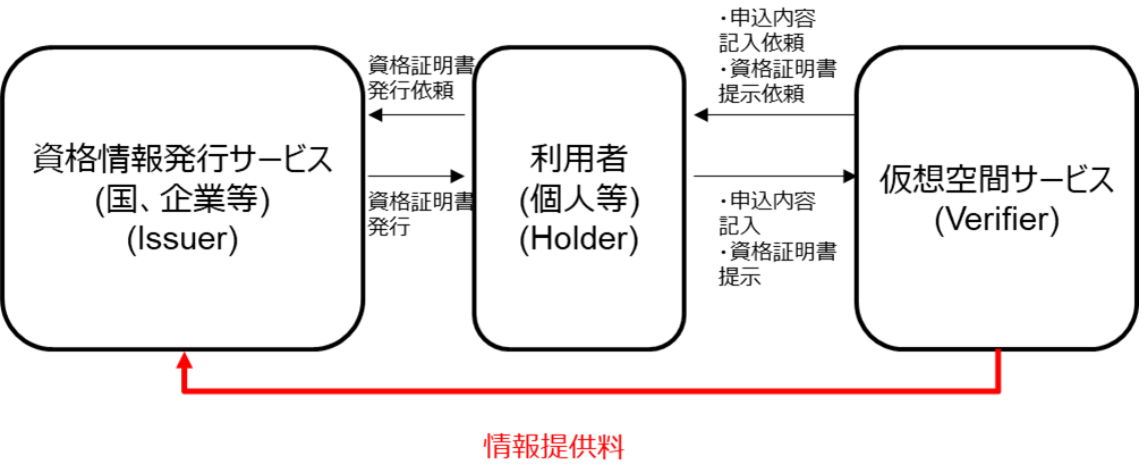
- ウォレットはNRIデジタル社が保有するシステムを利用しているが、OIDC For VCIおよびSIOPに対応するウォレットを利用することで第三者による再現が可能となる。
- 仮想空間サービスはKDDI社が保有するシステムを利用しているが、その他クラスターなどの仮想空間サービスにSIOPを組み込むことで第三者による再現が可能となる。

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・利用者ーのメリット

ビジネスモデル



利用者ーのベネフィット

ステークホルダ	ベネフィット	負担するコスト
Issuer	情報提供料の獲得	個人情報管理コスト
仮想空間サービス	利用者の個人情報を収集/管理することがなくなることによる管理コスト削減	VC提示を受けるたびの情報提供料

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

- 開発面の課題
  - 今回採用した国際標準化規格であるVC、OIDC For VCI、SIOP、OIDC For VPについて、EXAMPLEとして記載されている内容から読み取らなければならない点が多いことや任意項目の利用有無についてあいまいさが残っており、それらを定義して進める必要があった。今回は限られたメンバーで認識が合えばよかったが、今後世界標準で様様なステークホルダーと認識合わせする必要がある際には、これらのあいまいさの排除を行う必要がある。こちらについては、標準化団体のインプリフェーズを待つ他、各標準化団体への課題提起を行い解決していく予定。
  - VRゴーグルを利用した本人資格情報の連携には、スマートフォンとの接続が必須となるが、その際に安全に情報を授受できるプロトコルが存在していない。具体的にはBluetoothをベースとするセキュアな情報授受プロトコルがない。こちらについては、BluetoothベースでのOIDC拡張プロトコルの実装を待つ。
- ビジネス面の課題
  - 本実証では、想定するビジネスモデルを定義したが、そのモデル自体が成り立つのかを実際のIssuerおよび仮想空間サービス以外のVerifierにもヒアリングし、ビジネスモデル自体が成り立つのかを検討する必要がある。具体的には以下の2点のヒアリングが必要。
    - ✧ Issuerが本人資格情報を発行し、仮想空間サービス(Verifier)が提供を受けるたびに支払う情報提供料を仮想空間サービスが支払う価値があると考えるかどうかのヒアリングが必要。
    - ✧ Issuerが情報提供料をもらうだけで、本人資格情報を提供する価値があるかどうかのヒアリングが必要。

4.3 本ユースケースの社会実装に向けたマイルストーン

- 本ビジネスモデルの社会実装については、2024年度まで継続的な実証を行い、2025年度以降の商用化を想定している。
- 前述した開発面の課題については、参加するIssuerへの仕様開示にて解決しようと考えている。
- ビジネス面の課題については2024年度中にIssuerおよびVerifierになりえる企業へのヒアリングを行い、必要に応じてビジネスモデルの見直しを行う。
- 2025年度のサービス開始当初はKDDI社がIssuerになることを想定するが、その後Issuerの数を増やし、市場の拡大を目指す。

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

- Trusted Webを構成する要素として、Issuer自身やIssuerが発行した資格情報自体の真正性を監査する役割を担う運営基盤の観点が不足しているのではないかと思われる。
- VC化した資格情報は主に個人情報であることから、データの保管ルールの規定が必要だと思われる。
  - たとえば、ブロックチェーンやIPFS上に暗号化して格納するというパターンの場合は、削除ができないため暗号化を破られた場合に個人情報の流出につながる。
- Trusted Webで実現する未来が、利用者に対してどんな【実益】をもたらすのかを議論する必要がある。
  - サービス利用者は、常に最もセキュリティが高いサービスを利用し続けるというわけではなく、利便性や享受されるメリットを鑑みたうえで、利用するサービスを選択する。そのため、ただセキュリティが高まったというだけでは、TrustedWebが利用されない可能性があると考える。
  - 実益の例としては、VCとして検証可能データを持ち運ぶことができるため、本人確認書類の発行回数が減り、利用者が払うコストが低くなるといったことが考えられる。ただし、これが起きるとIssuerのマネタイズに課題が起きるため、全体最適化が必要となる。

5.2 その他Trusted Webの課題と提言

- 合意履行のトレースについては、合意履行状態だけではなく、VC提供後も含めたデータトレーサビリティの考慮も必要だと考える
  - 具体的には、Verifier側へ渡したデータが再利用されているのか、合意範囲外に利用されていないかなどを監査する仕組みが必要と考える。
- Issuerが発行する資格情報が個人情報である場合、Issuerが担保する本人確認レベルを定義し、Trusted Web内でその定義をVerifierや他Issuerが認識したうえで、情報連携をする必要がある。
- DIDおよびVCの実装規格にOpenID関連プロトコルを利用しているが、Implementするためには規定(明確化)されていない部分が多く存在することがわかった。そのため、様々な事業者がImplementして、課題を洗い出し、早期なプロトコル明確化をする必要があると考える。
- 要件4を完全に満たすためには、前述したようにデータトレーサビリティにも言及する必要があると考える。しかし、VCは最終的にテキストデータになるため、データトレーサビリティを向上させるためのメタデータの付与が難しい。今後テキストデータでもデータトレーサビリティを向上させるためにevidenceフィールドの活用の議論により今後の検討が進められると期待される。

5.3 メタバース観点特有の示唆

- メタバースでは、ワールドが異なる場合、ノード間でデータベースが異なる場合が存在する。
  その場合、トランザクションにアクセストークン検証などで、データベース間でメッセージ間の整合性を担保する必要がある。
- デバイスの特殊性
  - メタバースは従来デバイスのPCやスマートフォンだけではなく、VRゴーグルを利用する
  - VRゴーグルは没入感を出すため、着用時にはリアル世界の視覚情報を遮断する
- プライバシーの保護と本人特定性
  - メタバースはアバターを利用して活動する
  - メタバースは様々なワールドが存在し、ワールド別で活動することができる
  - アバターと自然人は必ずしも同一のアイデンティティを持つ必要はない
  - サービス提供には法令等により本人特定を必須とするケースがある
- 取扱可能なデータの多様性
  - 氏名や住所といった従来から扱われていた個人情報(本人情報)を扱う
  - 全身を使ってメタバースで活動するデバイスが発表され、アバターの動きと自然人の動きがリンクするようになり、生体情報(活動情報)も扱えるようになる
  - NFTにより唯一性を証明できるコンテンツがアバターの服やアクセサリーなどに広がっている

5.2 その他Trusted Webの課題と提言

デバイスの特殊性

- メタバースは従来デバイスのPCやスマートフォンだけではなく、VRゴーグルを利用する
- VRゴーグルは没入感を出すため、着用時にはリアル世界の視覚情報を遮断する

#	カテゴリ	課題概要	解決案(実現可能性は未考慮)
1	技術課題	資格情報が入っているスマートフォン等を操作してメタバース内にデータ連携を行う必要があるが、スマートフォン等を操作するためにはVRゴーグルを外して操作する必要がある。	・リモートデスクトップのようなもので接続し、スマートフォンなどのデバイスの画面自体をメタバース内のスマートフォン画面上に表示する
2	操作性課題	メタバース内に表示されたスマートフォンを操作しようとしても、VRゴーグルを利用した文字入力等は操作しづらい	・音声によりスマートフォンおよびVRゴーグルを操作することを前提とした機能実装を行う
3	技術課題	メタバース内にデータ連携するためにVRゴーグルとスマートフォンをBluetoothなどで接続する必要があるが、データ連携方式の安全性が確立できていない	・BluetoothベースのOpenIDConnectでのデータ連携などセキュアなデータ連携方式を利用する
4	セキュリティ課題	VRゴーグルを利用している自然人の本人認証手段が少ない	・VRゴーグルの中で虹彩認証を行う

5.2 その他Trusted Webの課題と提言

プライバシーの保護と本人特定性

- メタバースはアバターを利用して活動し、ワールド別で活動することができる
- アバターと自然人は必ずしも同一のアイデンティティを持つ必要はない
- サービス提供には法令等により本人特定を必須とするケースがある

取扱可能なデータの多様性

- 氏名や住所といった従来から扱われていた個人情報(本人情報)を扱う
- アバターの動きと自然人の動きがリンクするようになり、生体情報(活動情報)も扱えるようになる
- NFTにより唯一性を証明できるコンテンツがアバターの服やアクセサリーなどに広がっている

#	カテゴリ	課題概要	解決案(実現可能性は未考慮)
1	プライバシー保護	アバターと自然人を紐づけられないような情報連携やサービス提供が必要	・サービスを提供している企業から情報流出しないような厳重なセキュリティ対策 ・情報の匿名化を行ったうえでの情報連携
2	プライバシー保護	ワールド間でアバターを変更して活動してもアバター間が特定されないようにする	・情報の匿名化を行ったうえでの情報連携
3	プライバシー保護	NFTや動作の特徴(歩き方等)にから本人特定できないようにすることが必要	・NFTの一部情報隠蔽や動作の特徴へのノイズ付与
4	本人特定性	アバター間/サービス間での情報の引継ぎ犯収法により本人確認を行う必要がある	・DID/VCによる情報連携

プライバシー保護と本人特定性は相反する要件となるため、同時に満たす手段を検討する必要がある

⇒DID/VC/ゼロ知識証明を組み合わせることで一部は実現可能か？