Trusted Web の実現に向けたユースケース実証事業

成果報告書

仮想現実空間におけるサービス利用資格と提供データの Trust 検証

2023 年 2 月 17 日（提出日）

仮想空間サービス×自己主権型 ID コンソーシアム

代表機関：[NRI デジタル]

目次

1　背景と目的 1
2　事業の概要 1
2.1　事業概要及び実証の範囲 1
2.2　社会・経済に与える価値・影響 2
2.3　コンソーシアムの体制 4
2.4　実証全体のスケジュール 5
3　実証内容 7
3.1　実証の実施事項、論点及び判断 7
3.1.1　プロトタイプの企画・開発 7
3.1.2　国際標準規格の調査 10
3.2　検証できる領域を拡大する仕組み 10
3.2.1　データフロー 10
3.2.2　データフローに登場する主体とその概要 11
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 12
3.2.3.1 Issuer 自身の正当性 12
3.2.3.2 本人資格情報の正当性 13
3.2.3.3 ウォレット(Holder)の正当性 13
3.2.3.4 本人資格情報の正当性 14
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 15
3.3　6 構成要素との対応 15
3.3.1　検証可能なデータ 15
3.3.2　アイデンティティ 15
3.3.3　ノード 16
3.3.4　メッセージ 16
3.3.5　トランザクション 16
3.3.6　トランスポート 16
3.3.7　仮想空間サービス特有の示唆 17
3.3.8　VR ゴーグルを利用したケースの Trust 観点での示唆 17
3.4　本実証で企画・開発したシステムの概要 18
3.4.1　業務フロー 18
3.4.2　ユースケース図 22
3.4.3　操作画面（UI） 23
3.4.4　機能一覧/非機能一覧 23

3.4.5 データモデル定義 24
3.4.6 実験環境 25
3.4.7 システムの構成要素 25
3.5 実証を通じて得られた主な成果 26
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 26
3.5.2 ビジネスモデルに関する実証内容・得られた成果 27
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） 28
4 実証終了後の社会実装に向けた見通し 28
4.1 社会実装時に想定しているビジネスモデル・利用者のメリット 28
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 29
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 30
5 Trusted Web に関する考察 30
5.1 Trusted Web のアーキテクチャに関する課題と提言 30
5.2 その他 Trusted Web の課題と提言 30
5.3 仮想空間サービス観点特有の示唆 31

1　背景と目的

- 背景

・仮想現実空間、いわゆるメタバース等の仮想空間サービ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。
・仮想空間サービスにおいては、既存の Web サービス利用とは異なる仮想現実空間ならではの課題（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）がある。
・さらに複数仮想現実空間の間、複数サービスの間のシームレスな移動を実現するためには自己主権での属性情報等の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。

2　事業の概要

2.1　事業概要及び実証の範囲

- 事業概要

上記のとおり仮想現実空間においては、Trust を確保した上でのサービス利用・提供が難しい現状がある。仮想現実空間上にて、資格情報発行サービス、資格情報検証サービス、資格情報保管サービスを、仮想現実空間の利用者およびサービス提供者向けに提供することで、仮想現実空間上の安心安全なサービス利用・提供を実現する。

仮想現実空間ならではの課題として、「没入感を維持した UI/UX による Trust 検証をどう実現するか」という課題があるが、本ユースケースを通じてその点についても解決を試みる。下記に示す事業シナリオのような UI/UX を想定し実証を行う。

- 実証の範囲

本実証事業では、下記に示す事業シナリオのうち、①②⑤⑥のやり取りを実現するプロトタイプシステムの企画・開発を行う。

なお今回対象としない③④については必須のシナリオでなく、オプションサービスの位置付けとなる。「サービス利用者の意思により、サービス利用者が Verifiable Credential(以下、VC。今回のケースでは VC は学生証などの資格情報を指す)を資格情報保管事業者が保管し、資格情報保管事業者からサービス提供事業者へ直接連携することもできる」という前提のもと企画・開発を行う。

＜事業シナリオ＞

① サービス利用者が、契約にあたりサービス利用者の情報や資格など、利用者関連情報の正当性

を保証してもらうため、資格情報発行事業者に VC 発行を依頼する。
→例えば、通信契約者証明の発行、デジタル学生証の発行を想定

② 資格情報発行事業者は VC を発行する。

③ サービス利用者は資格情報保管事業者に発行された VC の保管を依頼する。

④ サービス利用者はサービス提供者のサービス利用時、サービス提供者へ資格情報保管事業者によって保管されていた VC を貸し出す。

⑤ サービス提供者は VC の検証を資格情報検証事業者に依頼する。または自ら VC を検証する。

⑥ サービス提供者はサービス利用者の情報や資格など VC の検証結果から、利用者関連情報の正当性を確認後適切なサービスを提供する。
→例えば、通信契約者専用サービスや専用仮想現実空間利用時の認証、学生向け割引適用時の確認などでの利用を想定

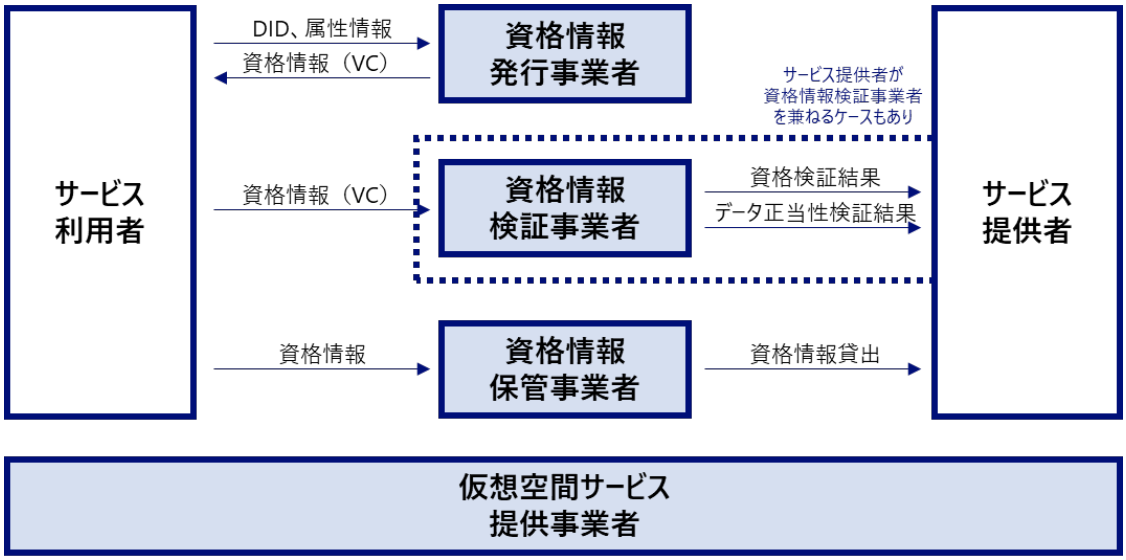

図 2.1.1 実証範囲

2.2 社会・経済に与える価値・影響

世界の仮想現実空間市場の市場規模は、2020 年に 6.2 兆円に上ると推計されており、通信・ネットワーク技術が発展していく中で、今後も多様な用途への広がりが期待できる。Emergen Research 社

によると 2028 年には 108 兆円になると推計されている[1]。

一方で、仮想現実空間においては、利用者（アバター）、サービス提供者間の売買契約などにおける利用者の資格情報の真正性を保証する手段が整っていない。本ユースケースは、仮想現実空間において、この利用者の資格情報の真正性を保証するサービスを想定しており、下記補足の通り約 200 億円の市場規模を創出するサービスとなる。

本ユースケースはデジタルウォレットを利用した利用者の資格情報の真正性保証サービスを想定しており、リアルのユースケースにおいても、リアルと仮想現実を連携させたユースケースにおいても、同様にサービス提供が可能である。リアル、リアルと仮想現実の連携までをサービスターゲットに含めると、デジタルウォレットを利用した利用者の資格情報の保証サービスの市場規模は、仮想現実上の市場割合を 1/4 と想定すると、約 400 億円を優に超えると考えられる。

また、日常から複数仮想現実空間、仮想現実空間上の複数サービスを利用するような社会になった際には、複数仮想現実空間の間、複数サービスの間のシームレスなデータ連携（利用者属性の情報連携）のニーズが高まることが想定されるが、それを実現するためには今回提案する自己主権での属性情報等のコントロールが重要となる。本ユースケースは、自己主権型の属性情報等のコントロールを実現することによって、仮想現実空間自体の市場拡大にも寄与するものである。

（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

利用者数×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

利用者数：日本では約 3,000 万人 （人口の 1/4 が利用者になる by Gartner）

本人確認サービス利用者割合：80%（大半の利用者が利用する想定）

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

[1] Emergen Research「2028 年に 8,289 億 5,000 万米ドルに達する世界の仮想空間サービス市場規模」
https://prtimes.jp/main/html/rd/p/000000041.000082259.html 1 ドル 130 円換算

（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

- 実施体制図

仮想現実空間においてサービス利用者の利用者の資格情報を保証・検証できるサービスを開発する。大手通信キャリア KDDI 社と NRI デジタルが共同検討する中で生まれたサービスアイデアであり、KDDI 社は本実証実験において、仮想現実空間の提供を行う。資格情報発行事業者・資格情報検証事業者・資格情報保管事業者なども、将来的には KDDI 社によるサービス提供を想定（排他的なサービス提供でなく、他社によるサービス提供も想定）する。当該事業を推進するためのシステム提供および運用は NRI デジタルにて担う。

図 2.3.1　コンソーシアム体制図

- 各団体のタスクと役割

各団体のタスクと役割については表 2.3.1 の通りとなる。

表 2.3.1　各団体のタスク

事業者	役割	タスク
NRI デジタル	・全体統括 ・システムアーキテクチャ検討 ・システム実装 ・デジタルウォレット提供	・当実証案件の全体統括および推進 ・システムアーキテクチャの全体設計 ・Decentralized Identity(以下、DID)システム/Blockchain(以下、BC)基盤の実装 ・デジタルウォレット機能の提供
KDDI	・仮想現実空間提供 ・仮想現実空間への接続部分実装 ・仮想現実空間でのサービス提供(Verifier 機能の実装)	・仮想現実空間(実証実験環境)の提供 ・仮想現実空間への接続部分の実装 ・仮想現実空間サービス提供
KDDI デジタルデザイン	・事業化アドバイス	・事業化に向けた戦略アドバイス
野村総合研究所	・事業化アドバイス	・事業化に向けた戦略アドバイス ・Trusted Web、Web3 のノウハウ提供

2.4　実証全体のスケジュール

10 月から要件定義等のアプリ企画を行い、同時に環境構築を行う。その後 2 月中旬までアプリ開発および仮想空間サービスへの組み込みを行う。2 月中に実装した機能を検証する。

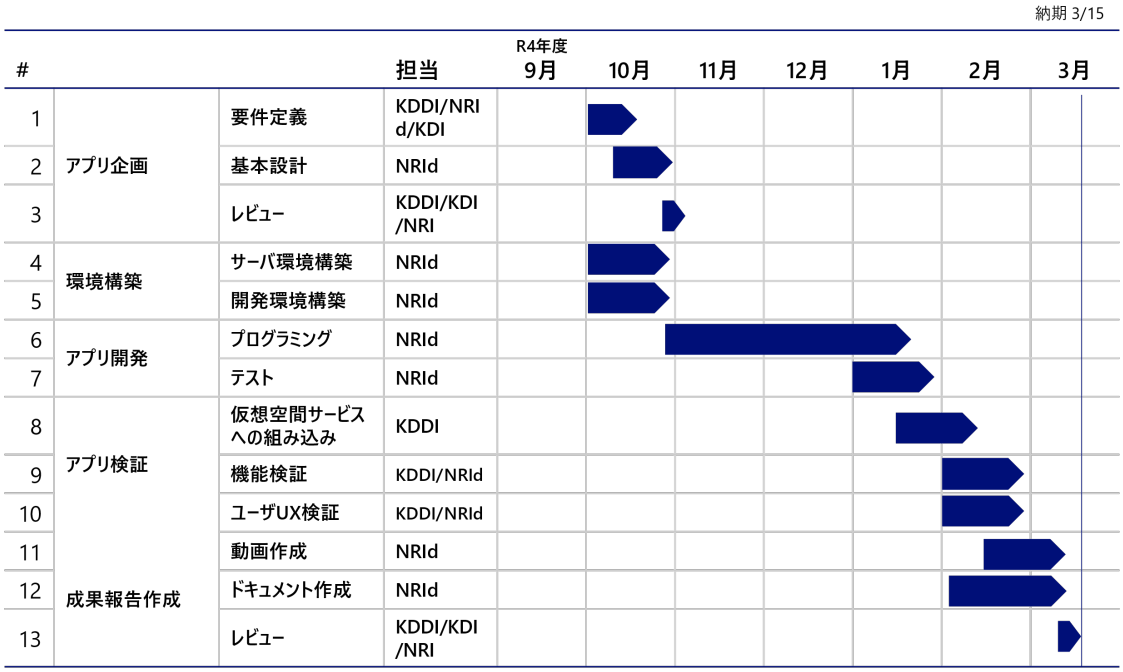

図 2.4.1　実証スケジュール

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

（１） 要件定義

- ユースケースのコンセプトを再検討する際に、ユースケースに用いる技術に関して議論を行った。論点となったのは以下の 3 点。
  A：本人の資格証明を行うための規格は何にするのか
  B：DID の連携プロトコルは何にするのか
  C：VC のデータプロトコルは何にするのか
- A については、以下の 2 つの理由により DID/VC を利用することが良いと判断した
  - 仮想空間サービスでは様々な事業者がサービス提供を行う。従来から利用されている OpenID Connect[2](以下、OIDC)では、事前に情報提供スコープの取り決めやクライアント ID のやり取りを行い、ID 連携を行い、本人資格情報の授受が必要である。事業者が多くいる仮想空間サービスの場合は、事前取り決めおよび ID 連携が必要な技術を選ぶよりも、事前の情報提供スコープの決定などの取り決めが少ない分 VC の提示による資格情報の授受を行う方が効果的と考え、DID/VC を用いることとした。
  - 本人資格情報は通常セキュリティの高い領域で管理されている。例えば、企業の場合、社員情報などは企業が管理しており、社内ネットワークからでないとアクセスできないようにしている企業が多い。従来から利用されている OIDC では、Identity Provider（以下、IdP）と Relying Party(以下、RP)が相互に到達性があることを前提に作られているため、インターネットと社内ネットワークといったネットワークの隔たりがある場合には利用できない。DID/VC の場合は、ネットワークの隔たりがあっても、VC 発行、提示、検証の時だけオンラインであればよく、Issuer/Verifier/Holder が常にオンラインである必要はない。仮想空間サービスでは、本人資格情報として学生証や社員証といった VPN などの閉域 NW 内でしか取り扱いできない情報を用いる可能性があるため、DID/VC を用いることが良いと考えた。
- B については、以下の理由により OIDC ベースのプロトコルを用いることが良いと判断した
  - コンシューマー向けに ID 連携サービスを提供する Apple や Google を初めとする IdP は OIDC を利用して ID 連携および情報授受を行っている。今後の拡大を見据えると現在主流である OIDC をベースとした、OpenID Connect for Verifiable Credential Issuance[3] (以下、OIDC For VCI)、Self-Issued OpenID Provider v2[4] (以下、SIOP)を利用することが良いと考えた。

---

[2] サービス間で、利用者の合意に基づき ID 情報を流通するための標準仕様
https://openid.net/connect/

[3] https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

[4] https://openid.net/specs/openid-connect-self-issued-v2-1_0.html

- C については、以下の理由により OIDC ベースのプロトコルを用いることが良いと判断した
  - コンシューマー向けに ID 連携サービスを提供する Apple や Google を初めとする IdP は OIDC を利用して ID 連携および情報授受を行っている。今後の拡大を見据えると現在主流である OIDC をベースとした、OpenID for Verifiable Presentations[5] (以下、OIDC For VP)を利用することが良いと考えた。

（２） 基本設計

- 基本設計を行う際に、アーキテクチャに関して議論を行った。論点となったのは以下の４点。
  A：ウォレットに相対するサーバは用意するのか
  B：秘密鍵の管理はどうするのか
  C：発行される VC はどこに格納するか
  D：DID メソッドは何にするか
- A については、以下の理由によりアプリ相対サーバは用意しないと判断した
  - 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。
  - アプリ相対サーバがないとネイティブアプリですべてのデータを保持する必要が出てしまうが、今回の実証実験で使うウォレットではデータ保管すべき内容は VC のみであるため、大量データの処理は必要ないと判断した。一方で、ネイティブアプリのみにデータ保存してしまうと端末に問題があった場合にデータが消えてしまう。そのため、バックアップサーバというものを用意し、そこに DID や VC などの必要なデータは保存する形とした。
  - バックアップサーバを持つ場合は、事業者の都合でバックアップサーバを停止することができ、またそのサーバに保管されていたデータも消失してしまう。自己主権型のサービスを目指し、事業者のバックアップサーバに依存しないデータのコントロールの機能を利用者に提供することで、プラットフォーマーが運営することによる利用者のネガティブなイメージを払拭することが良いと考えた。
- B については、以下の 2 つの理由によりバックアップサービスで管理することが良いと判断した
  - 利用者が鍵管理する仕組みよりも、事業者が責任をもって利用者から鍵を預かる形とする方がユーザビリティは良いと判断し、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の建付けにすることが良いと考えた。
- C については、以下の 3 つの理由によりウォレット内部ストレージに格納することが良いと判断した
  - 自己主権型ウォレットを実現するためには、ウォレットプロバイダーによる管理を避けられることが理想的だと考えた。その考えに基づくと候補となるのは、「データが利用者の操作するスマートフォンの中に格納されるウォレット内部ストレージ」、「パブリックで管理者がいないブロックチェーン」、「パブリックで管理者がいない IPFS」だと考えた。
  - ブロックチェーンや IPFS に VC を格納した場合、データ削除が困難であるため、例えば利用者

[5] https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

から削除したいという要望が来た場合に対応が困難であると考えた。また、パブリックなブロックチェーンや IPFS は格納データが公開される。そのため、いかに VC を暗号化したとしても量子コンピューターの発展により一般的に利用される公開鍵暗号方式による暗号化を破られてしまい [6]、VC が流出してしまうリスクがあると考え、一般的に格納データが公開されるブロックチェーンおよび IPFS には格納しない方針とした。

- ◆ ウォレット内部ストレージに VC を格納する場合デバイス紛失やデバイスの交換により VC が消失してしまう。格納データを公開しないバックアップサービスを提供することで、流出リスクを抑え、デバイス紛失やデバイス交換時にバックアップサービスよりデータ復元ができるため本懸念は払しょくされると考えた。

- ➢ D については、以下の 2 つの理由により「did:ion」のメソッドを利用することが良いと判断した
  - ◆ 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 ID の検討の中で議論されるような、Issuer が廃止されたりしてもサービス全体が停止されないためユーザーの主権が守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。そのため、Issuer が廃止されたりしてもサービス全体が停止されないためユーザーの主権が守られ、世界的な展開やスタンダード作成に向いていると考えた。

（３） システム開発

- ➢ 開発工程を行う際に、利用者利用環境について議論を行った。論点となったのは以下の 1 点。
  A：ウォレットをインストールするデバイスを何にするか
- ➢ A については、以下の理由によりスマートフォンの使用想定した
  - ◆ 候補となったデバイスは PC とスマートフォン、VR ゴーグルである。
  - ◆ VR ゴーグルについてはユーザへの普及率が低いことと VR ゴーグルの規格統一が図られておらず、仮想空間サービスは VR ゴーグル以外にも PC やスマートフォンへのサービス提供も行っているため候補から除外した。
  - ◆ 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、スマートフォンにウォレットアプリをインストール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おり、将来のサービス実現に向けて強みを生かすことができるため、スマートフォンをベースとして考えた。

[6] https://www.soumu.go.jp/main_content/000655118.pdf

3.1.2 国際標準規格の調査

W3C[7]および DIF[8]で標準化の検討が行われている「DIDs/VCs」について調査を実施した。

調査結果は以下の通りとなる。

・データモデルや項目定義、採りうるデータパターンについては標準で定義されている内容を本ユースケースで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標準で明確な指示はない。

・標準で 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、標準で規定されていない点や 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定義して進めることとした。

Open ID Foundation(以下、OIDF)で DID/VC を OIDC の拡張プロトコルとして適用する検討が行われている「OIDC For VCI、SIOP、OIDC For VP」について調査を実施した。

調査結果は以下の通りとなる。

・シーケンスについては各標準で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[9]を併用することが良いと判断した。クライアントと認可サーバがやり取りするためにはクライアント情報が必要になるが、Dynamic Client Registration を利用すると動的にクライアント情報を登録することができる。

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

- データスキーム図
  - 本システムでは、VC の元となる本人資格情報は Issuer が管理する。
  - 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 VC の発行を要求する。
  - 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。

---

[7] World Wide Web Consortium の略称。Web 技術の標準化を行う非営利団体。

[8] Decentralized Identity Foundation の略称。分散 ID 連携に関する各種仕様の検討を行うための団体。

[9] https://openid.net/specs/openid-connect-registration-1_0.html

- VCとして発行された本人資格情報はウォレット（ユーザーのスマートフォンストレージ）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。

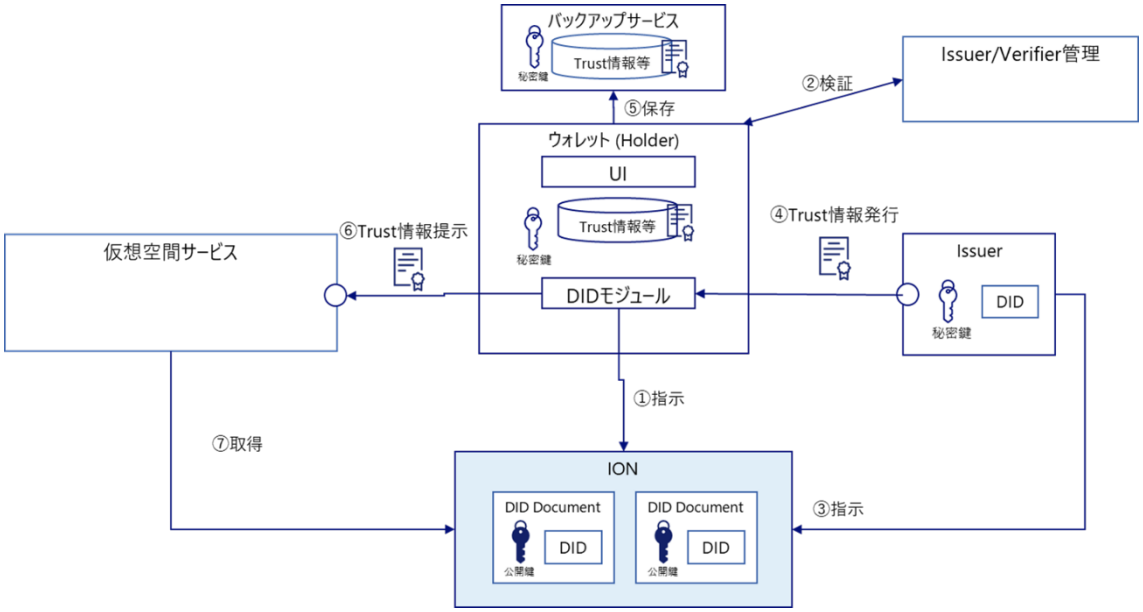

図 3.2.1.1　データスキーム図

3.2.2　データフローに登場する主体とその概要

- 登場する主体とその概要

本ユースケースのデータフローに登場する主体は、「利用者が利用するウォレット(Holder)」、「本人資格情報を管理し VC 発行を行う Issuer」、「本人資格情報 VC の検証を行う Verifier の役割を担う仮想空間サービス」、「利用者への利便性および秘密鍵の紛失/流失を防ぐバックアップサービス」、「Issuer および Verifier の正当性をチェックする Issuer/Verifier の管理者（＝運営者）」となる。

表 3.2.2.1　主体と役割

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	本人資格情報の管理者。依頼された本人資格情報を VC として提示す

（＝本人資格情報提供者）	る。
仮想空間サービス （＝Verifier）	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。

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

3.2.3.1 Issuer 自身の真正性

- 背景
  仮想空間サービス上のサービス提供者が、利用者から提示された VC が信頼できる資格情報発行者が発行したものなのかを確認する必要がある。
- ペインポイント
  サービス提供者から見て Issuer が信頼できるかどうかを判断することができない。
- 検証できる領域
  Issuer 自身の真正性。
- 検証方法
  運営者による審査。
- 検証者
  運営者。
- 保有者
  Issuer。
- 発行者
  Issuer。
- データの置き場所
  なし。（強いて言うなら登記簿）
- アクセスコントロール手法
  行政にならう。
- 成果および留意点
  Issuer/Verifier 管理者である運営者による審査を行うことで、Trusted Web に参加している団

体が Issuer を信頼することができる。
ただし、運営者の成り手には課題があり、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に一企業がなることは望ましくなく、コンソーシアムでの運営が望ましい。

3.2.3.2 本人資格情報の真正性

- 背景
  仮想空間サービス上のサービス提供者が、利用者から提示された VC は資格情報発行者が正しい情報をもとに発行したものなのかを確認する必要がある。
- ペインポイント
  サービス提供者から見て VC の内容自体が信頼できるかどうかを判断することができない。
- 検証できる領域
  本人資格情報の真正性。
- 検証方法
  運営者による審査。
- 検証者
  運営者。
- 保有者
  Issuer。
- 発行者
  Issuer。
- データの置き場所
  Issuer 内ストレージ。
- アクセスコントロール手法
  Issuer のみアクセス可能。
- 成果および留意点
  本課題は、システム考慮で解消できる課題ではない。そのため、Issuer が持つ本人資格情報と発行した本人資格情報が一致していることを運営者が審査する必要がある。

3.2.3.3 ウォレット(Holder)利用者の真正性

- 背景
  仮想空間サービス上のサービスを利用するために、サービス利用者が自身のデジタルアイデンティティを証明する必要がある。
- ペインポイント
  仮想空間サービス上のサービス提供者に提示された VC が正しいウォレットから提供されたものであることを検証できない。

・ 検証できる領域
ウォレット利用者の真正性。
・ 検証方法
ウォレット利用者が発行した DID の署名検証。
・ 検証者
仮想空間サービス提供事業者。
・ 保有者
ウォレット利用者。
・ 発行者
ウォレット利用者。
・ データの置き場所
ION ノード上。
・ アクセスコントロール手法
DID Resolver での ION ノードからの DID Document 取得。
・ 成果および留意点
本実証実験で採用した SIOP のプロトコル規定に従ってウォレットの署名が入った VC の検証を行い、ウォレットのアイデンティティを証明することができる。

3.2.3.4 本人資格情報の真正性

・ 背景
仮想空間サービス上のサービス提供者が、利用者から提示された VC は Issuer が発行してから改ざんされていないことを確認する必要がある。
・ ペインポイント
仮想空間サービス上のサービス提供者に提示された VC が改ざんされていないことを検証できない。
・ 検証できる領域
本人資格情報の真正性。
・ 検証方法
VC の署名検証。
・ 検証者
仮想空間サービス。
・ 保有者
ウォレット。
・ 発行者
Issuer。
・ データの置き場所
ウォレットアプリをインストールしたスマートフォン内のストレージ。

・　アクセスコントロール手法

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。

・　成果および留意点

本実証実験で採用した OIDC For VCI および SIOP のプロトコル規定に従って VC の署名検証を行うことで VC が改ざんされていないことを確認することができる。

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

本実証では、本人資格情報 VC を Issuer がウォレットに対して発行し、ウォレットから仮想空間サービスへ提供することを想定している。そのため、「ウォレット利用者と Issuer」と「ウォレット利用者と仮想空間サービス提供事業者」のそれぞれの合意形成が必要となる。

ウォレット利用者と Issuer 間での合意については、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表示し、ウォレット利用者が許諾することで合意形成が行われる。

ウォレット利用者と仮想空間サービス提供事業者間での合意については、要求する本人資格情報の内容および利用用途について表示し、利用者が開示する範囲を選択し表示された許諾に承諾後、VC 提供することで合意形成が行われる。

履行された合意事項を、VC 発行/提示履歴としてウォレットアプリケーションに表示・確認できることで合意情報のトレースが可能と考えた。

ウォレット利用者と Issuer 間での合意内容は、VC 発行依頼があったデータ内容が正しいかという確認となるため、合意の取り消し自体が不要と考えた。

ウォレット利用者と仮想空間サービス提供事業者間での合意の取り消しについては、本実証内ではシステム構築はできていない。本ユースケースでは、VC 提供後のデータの取り扱いまでは実証範囲に含めていなかったため、システム構築のは行わず、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だと考えた。

3.3 6 構成要素との対応

3.3.1 検証可能なデータ

（1）　検証対象

①　Issuer が発行する本人資格情報

（2）　検証者

①　仮想空間サービス

3.3.2 アイデンティティ

（1）　アイデンティティとして想定されるもの

Issuer、ウォレット、仮想空間サービス

（2）　アイデンティティ管理システム

Issuer、ウォレット、仮想空間サービスそれぞれで自身の DID を管理する。
管理システムは問わない。

3.3.3 ノード

（1） Wallet の使用有無

Holder である利用者が操作するウォレットにおいては、NRI デジタルが保有するアセットを利用している。
本ウォレットは、OIDC For VCI/SIOP のプロトコルに対応したウォレットである。

（2） 合意形成がされているか、されている場合その手段

ウォレット上に要求する本人資格情報の内容および利用用途を表示し、ユーザがその内容について承諾することで合意形成が行われる。

（3） データのやり取りの記録場所

- Issuer のサーバー
- ウォレットアプリケーションをインストールしたデバイス

3.3.4 メッセージ

（1） 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

- 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)
- 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)
- 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)
- 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)
- 本人資格情報の提示のメッセージ(リクエスト・レスポンス)

3.3.5 トランザクション

（1） データのやり取りの記録・検証はできるか

- 全ての[リクエスト＋レスポンス]はトランザクションたり得る

3.3.6 トランスポート

（1） トランスポートのプロトコル

- OIDC For VCI プロトコル
- SIOP プロトコル

3.3.7　仮想空間サービス特有の示唆

仮想空間サービスは、同一プラットフォーム上に複数の空間(ワールド)を構築することができる。

仮想空間サービスでは、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、トランザクションの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の整合性を担保する必要がある。

3.3.8　VR ゴーグルを利用したケースの Trust 観点での示唆

本ユースケースでは、デバイスとして VR ゴーグルを想定していないが、VR ゴーグルを利用する場合、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」実現することが必要である。この実現には、「内部カメラの有無、Bluetooth の有無などの VR ゴーグルの端末仕様に依存しないこと」、「VR ゴーグル利用者以外の第三者に本人認証時の知識情報が外部に漏れないこと」、「VR ゴーグル以外の外部デバイスを触ることがないこと」を同時に満たす必要がある。

各要件に対して、下記の表のとおりの解決方針を検討した。

表 3.3.8.1　解決方針

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
2	端末仕様に依存しない	端末独自機能を利用しない
3	VR ゴーグル利用者以外の第三者に知識情報が漏れない	認証操作のランダム作成
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

本解決方針を踏まえた実現方針として、予め PIN コードを設定し、認証タイミングで VR 空間に認証画面表示、ジェスチャーによる矢印方向入力で解決できると考えた。数字の位置は毎回ランダム生成することで第三者から見てもわからない形にできると考えた。

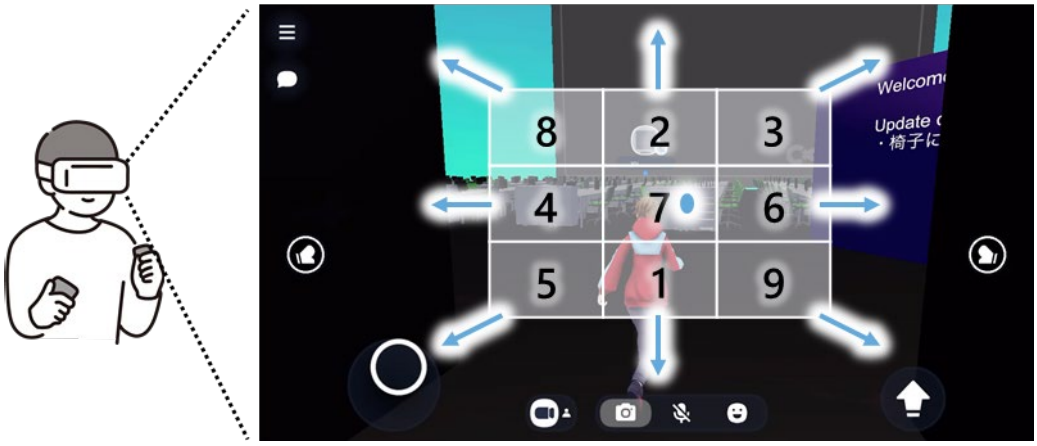

図 3.3.8.1　ジェスチャーによる認証

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

VC 発行では、OIDC For VCI を採用したため、それを元にした下記の図に示す処理とした。

VC発行

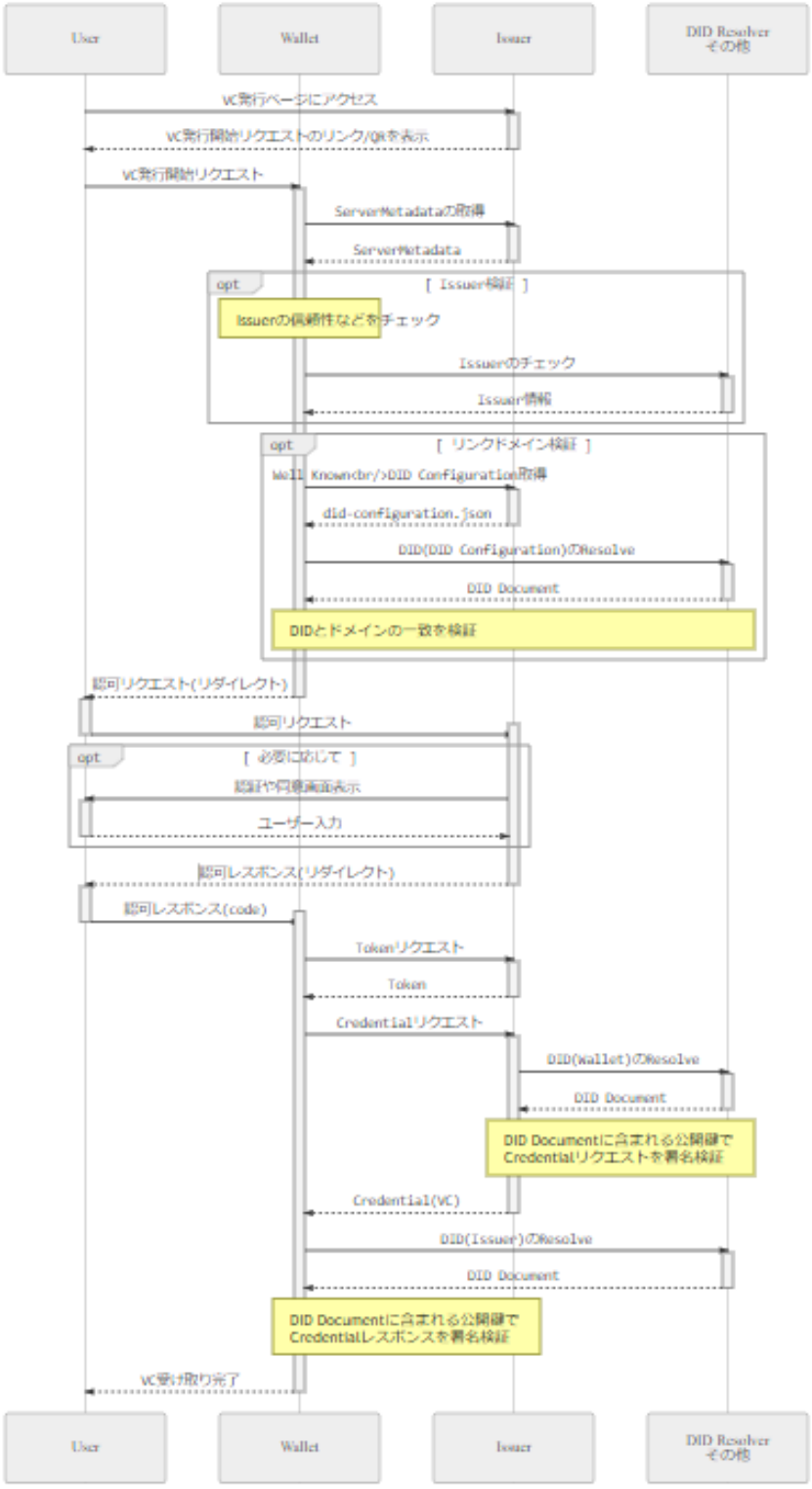

図 3.4.1.1 VC 発行フロー

VC 提示では、SIOP を採用したため、それを元にした下記の図に示す処理とした。

VP提示

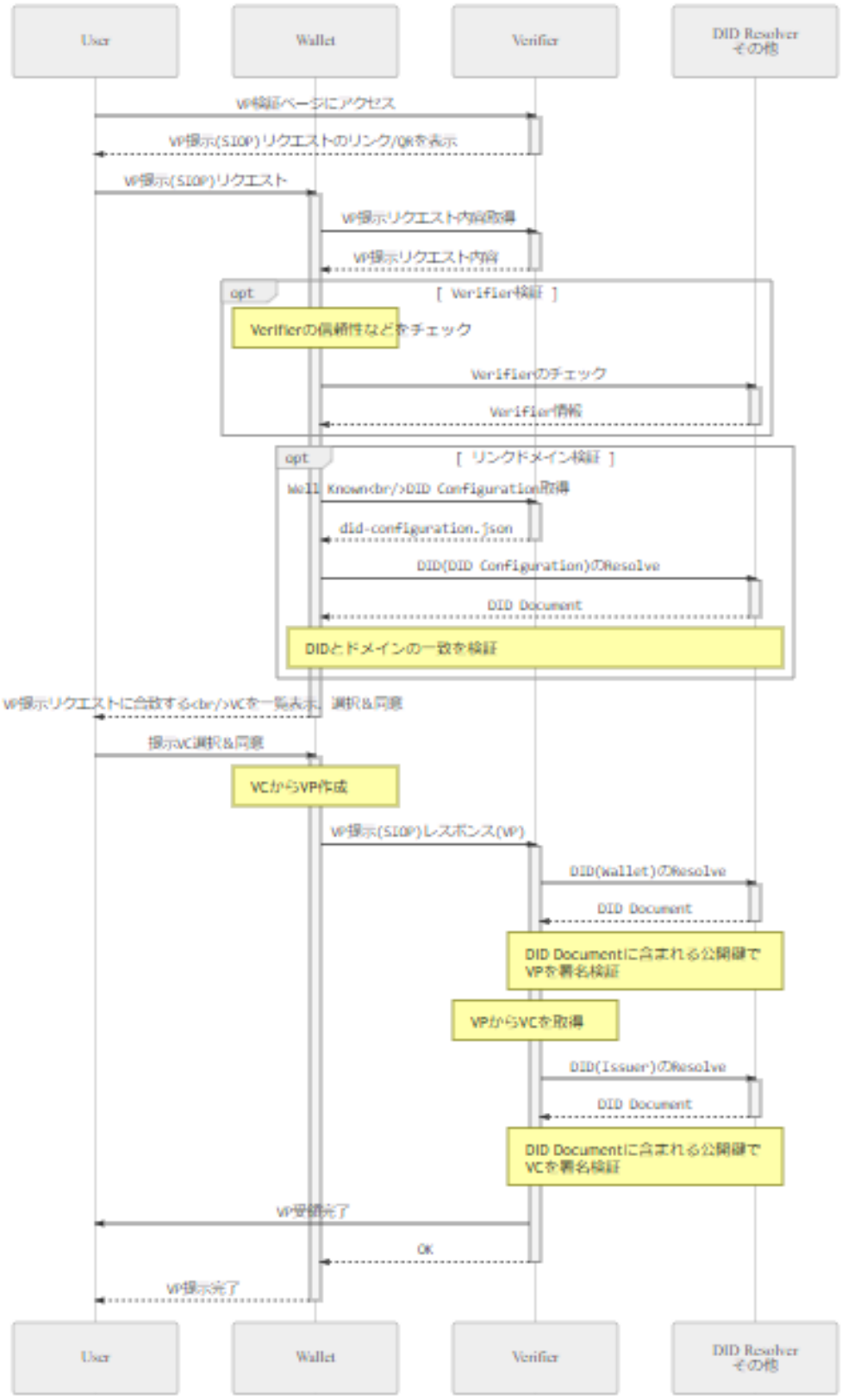
User
Wallet
Verifier
DID Resolver
その他
VP検証ページにアクセス
VP提示(SIOP)リクエストのリンク/QRを表示
VP提示(SIOP)リクエスト
VP提示リクエスト内容取得
VP提示リクエスト内容
opt
[Verifier検証]
Verifierの信頼性などをチェック
Verifierのチェック
Verifier情報
opt
[リンクドメイン検証]
Well Known
DID Configuration取得
did-configuration.json
DID(DID Configuration)のResolve
DID Document
DIDとドメインの一致を検証
VP提示リクエストに合致する
VCを一覧表示、選択&同意
提示VC選択&同意
VCからVP作成
VP提示(SIOP)レスポンス(VP)
DID(Wallet)のResolve
DID Document
DID Documentに含まれる公開鍵で
VPを署名検証
VPからVCを取得
DID(Issuer)のResolve
DID Document
DID Documentに含まれる公開鍵で
VCを署名検証
VP受領完了
OK
VP提示完了
User
Wallet
Verifier
DID Resolver
その他

図 3.4.1.2 VC 提示フロー

3.4.2ユースケース図

利用者はまずウォレットを利用して DID の発行を行う。また、ウォレットを用いて本人資格情報の発行依頼および本人資格情報の提示を行う。

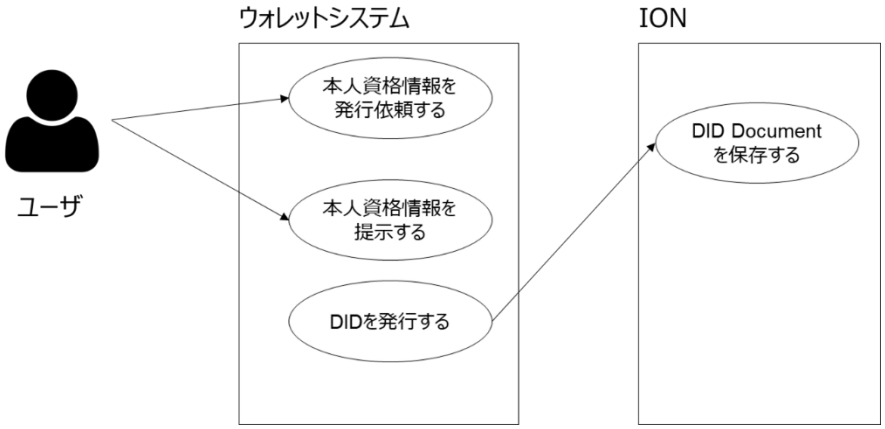

図 3.4.2.1 ウォレット利用ユースケース図

Issuer は事前に自身の DID を発行し、ION へ DID Document を保存しておく。その後、利用者からの VC 発行依頼に基づいて本人資格情報を VC として発行する。

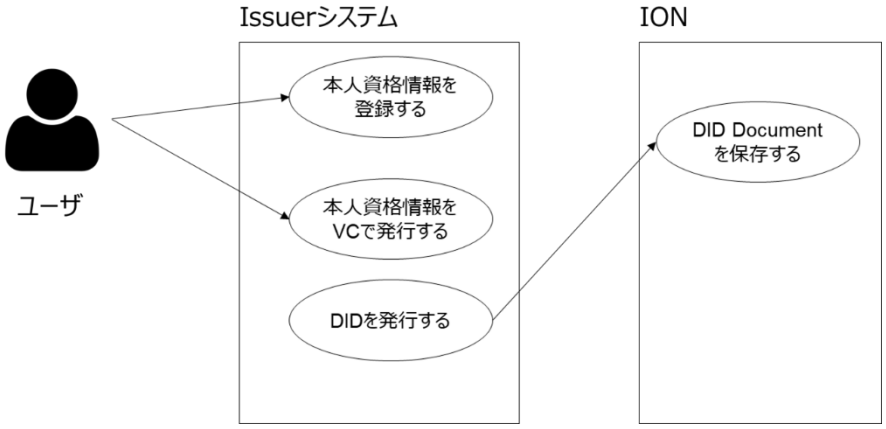

図 3.4.2.2 Issuer システム利用ユースケース図

仮想空間サービスは利用者へ本人資格情報の要求を行う。

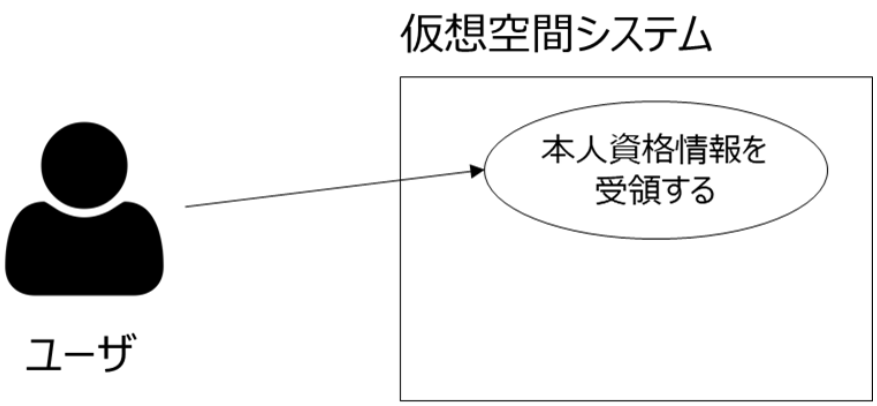

図 3.4.2.3 仮想空間システム利用ユースケース図

3.4.3 操作画面（UI）

操作画面については成果報告書概要版にて記載する。

システムへのログイン

3.4.4 機能一覧/非機能一覧

- 機能一覧表

今回の実証では非機能に関しての検討は行っていない。

機能としては、以下を開発した。

- ウォレットが自身の DID 発行を行い、Issuer により本人資格情報を VC として発行する機能
- ウォレットで Issuer および仮想空間サービスと合意した事項を閲覧する機能
- ウォレットが仮想空間サービスへ本人資格情報 VC を提示する機能

表 3.4.4.1 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 ノードへ格納する
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 がウォレットに対して VC 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	合意済み許諾事項一覧確認	合意した許諾事項の一覧を確認する
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

3.4.5 データモデル定義

VC のデータモデルについては W3C　VCs で定義されている内容をもとに定義を行った。

具体的な定義は下記の表のとおりである。

今回の実証実験では学生証を資格情報として扱うことを想定した。

表 3.4.5.1 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	ナンス	nonce		○	クレデンシャルエンドポイント リクエストで受けた nonce
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 URL
17	クレデンシャルス	type		○	クレデンシャルステータスのタイ

	テータスタイプ				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
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
20	利用規約	termsOfUse	Object[]	△	利用規約情報
21	利用規約タイプ	type		○	利用規約タイプ

3.4.6 実験環境

- 環境構成図

本実証では、ウォレットはスマートフォンの中のアプリとして組み込み、Issuer、バックアップサービス、Issuer/Verifier 管理（＝運営者）、仮想空間サービスについては AWS 上にサーバを用意し、環境構築した。Issuer/Verifier 管理については、システム化の検討は行ったが実際の構築までは行っていない。

ION ノードについては、Microsoft 社が開放しているβ版のノードを利用し環境構築した。

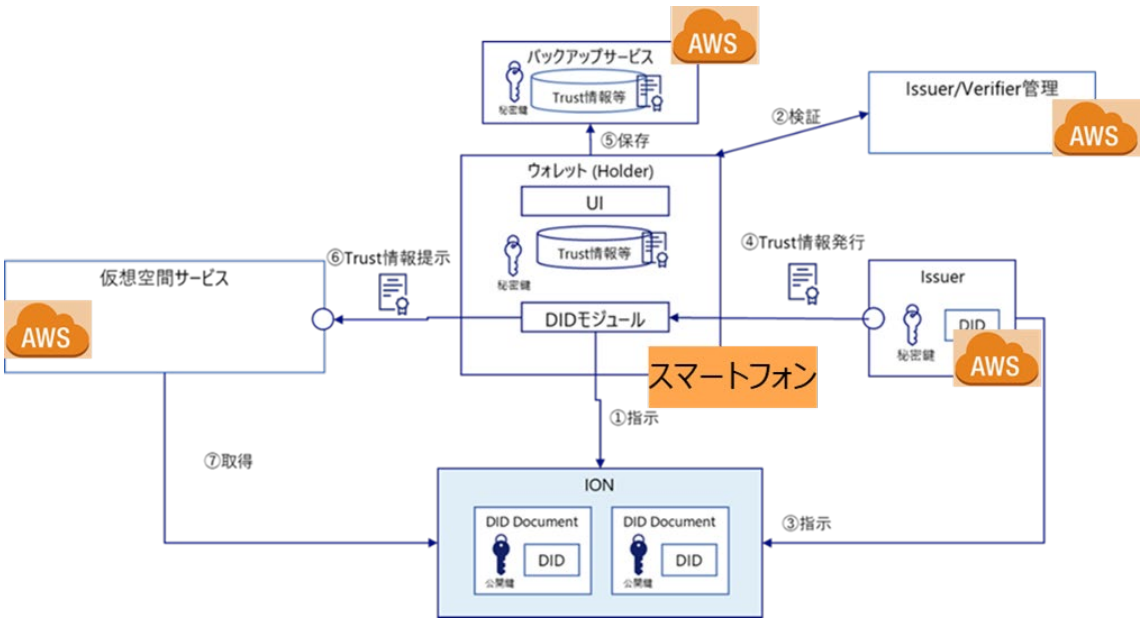

図 3.4.6.1 環境構成図

3.4.7 システムの構成要素

本実証では、KDDI、NRI デジタルが従前から持っているアセットを活用し、それに本実証の内容であ

る本人資格情報 VC の発行および提示の機能を組み込んだ。

具体的には、ウォレットについては NRI デジタルが保有しているものを活用、仮想空間サービスについては KDDI が保有しているものを活用した。

NRI デジタルが保有するウォレットは、did:ion メソッドが利用でき、OIDC For VCI/SIOP のプロトコルに対応しているアプリケーションである。

KDDI が保有する仮想空間サービスについては、KDDI 独自で開発した仮想空間サービス基盤となる。ただし、第三者による本実証実験の再現には特定の仮想空間サービスを利用する必要はないため、Cluster などの仮想空間サービス基盤に今回の SIOP のプロトコルを組み込み、ウォレットと接続することで再現が可能となる。

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
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

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

- 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、仮想空間サービス内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、仮想空間サービス内で業務を完結することができるようになった。

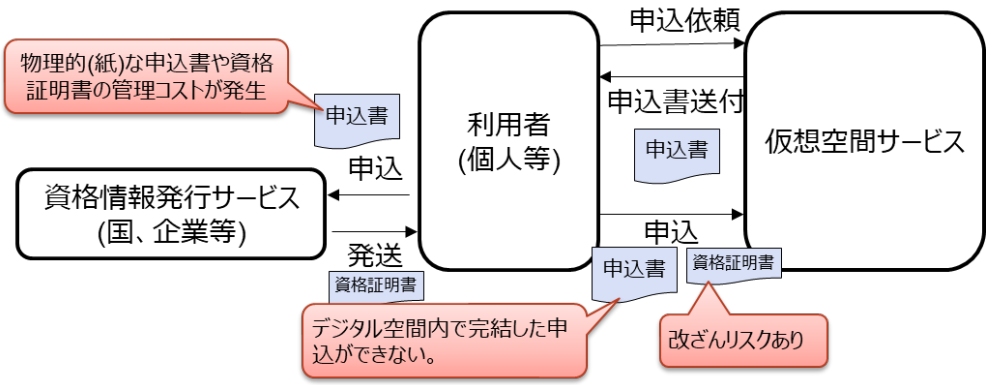

図 3.5.1.1　As Is（現状）のスキーム図

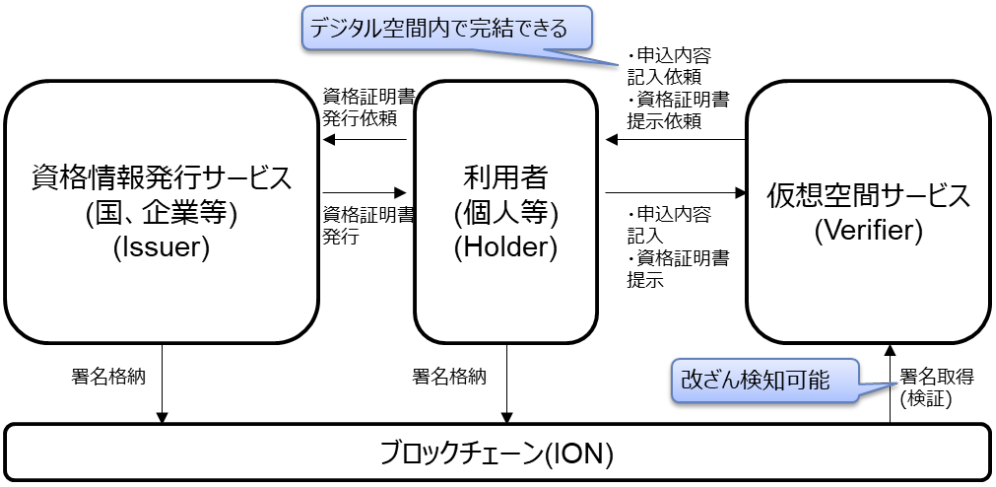

図 3.5.1.2　To Be（将来）のスキーム図

- 仮想空間サービ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
  - 仮想空間サービスの中で提供するサービスでは、特定の入場資格を持つ人しか入れないワールドがあるため、本人を識別し入場資格の検証を行う必要がある。
  - 一方で、仮想空間サービスではアバターの動きを実際の動きと同期させるといった扱える情報の多様性から不用意に本人識別されてしまい、プライバシーを侵害してしまう可能性がある（例：アバターの歩き方や癖のあるジェスチャーPIN コードの入力におけるジェスチャー）。
  - そのため、仮想空間サービスの中で本人識別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。

3.5.2 ビジネスモデルに関する実証内容・得られた成果

- 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 に収益が入るモデルを作る必要があると考える。

- 仮に Verifier から Issuer への一時的な情報利用料を渡したとしても、一度 VC としてウォレットに本人資格情報を発行してしまうと、ウォレットは自由に Verifier へ提示することができてしまう。また、Verifier がその他の事業者へ情報提供したことが検知できないと、Issuer が発行した本人資格情報が二次流通してしまう。そのため、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の信頼性を向上させたことに関しての収益が生まれない。

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）

- 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。

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・利用者のメリット

仮想空間サービス内の各事業者が VC の提示を受けるたびに情報提供料を Issuer へ支払うことを想定した。

仮想空間サービスは、自身で利用者の個人情報を収集/管理することがなくなり、管理コストの削減が見込める。

利用料については、各企業への個人情報管理やリスクにかかっているコストのヒアリングを行い、費用がが明確になれば算出可能と考える。ただし、実際には各企業によって大きな幅があると思われるため、固定の情報提供料の算出は難しいと考える。

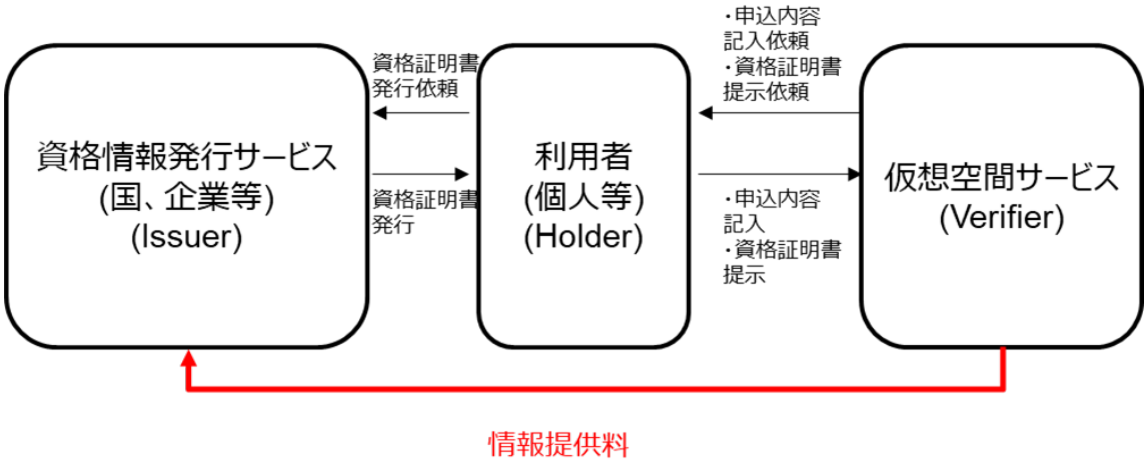

図 4.1.1 社会実装時に想定されるビジネスモデル

表 4.1.1 各ステークホルダーのベネフィット及び想定している利用料

ステークホルダー	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、標準に 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成立したたが、今後世界標準で様々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本ユースケースと同様に行う必要がある。こちらについては、今回採用したプロトコルを様々な事業者が一定のルールの元に利用できるように、標準化団体の実装フェーズを待つ他、各標準化団体への課題提起を行い解決していく予定である。
  - 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こととなる。
- 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である。
    - 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となる。
    - 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となる。

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。

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

- 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、Trusted Web 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、実装するためには規定（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、早期に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追跡可能な識別子を evidence フィールド内に埋め込むといった W3C VCs における 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。
- 今回の実証実験では、VC＝本人証明の資格情報という前提とし、署名検証ができればよいと考えていた。ただし、実際のサービスを考えた際には以下のようなケースにおいて、法令の解釈により展開できるサービスに制限があるのではないかと思われる。
  - 銀行口座開設を行う際に、犯収法の対応として免許証を提示する必要があるが、それは実際の免許証の提示ではなく、VC になった免許証でもよいのか。
-

5.3 仮想空間サービス観点特有の示唆

仮想空間サービスでは、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、DB 間でメッセージ間の整合性を担保する必要がある。

- 仮想空間サービスの特殊性とそれぞれの特殊性に関する考察
  - デバイスの特殊性
    - 仮想空間サービ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
  - デバイスの特殊性に関する考察

    VR ゴーグルはまだ出始めたばかりであるため、本人認証手段や安全なデータ連携プロトコルの発展に課題があるため、今後の技術革新が期待される。

表 5.3.1 デバイスの特殊性から考慮すべき事項

No	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	Trust 情報が入っているスマホ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、スマホ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、スマホなどのデバイスの画面自体をメタバース内のスマホ画面上に表示する
2	操作性課題	メタバース内に表示されたスマホ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	・音声によりスマホおよび 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 ゴーグルとスマホを 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

- プライバシーの保護と本人特定性
  - 仮想空間サービスはアバターを利用して活動する
  - 仮想空間サービ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
  - アバターと利用者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
  - 全身を使って仮想空間サービスで活動するデバイスが発表され、アバターの動きと利用者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
- プライバシーの保護と本人特定性、取扱可能なデータの多様性に関する考察
  プライバシー保護と本人特定性が同時に求められるのは仮想空間サービスの特徴だと考えられる。

表 5.3.2 本人識別性とプライバシーの保護の観点から考慮すべき事項

No	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