Trusted Web の実現に向けたユースケース実証事業
最終報告書 詳細版

ウォレットによるアイデンティティ管理とオンラインコミュニケーション

2024 年 3 月 15 日

株式会社 DataSign

目次

1. 背景と目的

1.1 背景・目的

【実証の背景】

結論として本ユースケースでは、令和 3 年度補正「Trusted Web の実現に向けたユースケース実証」分析レポート[1] および当社の 2022 年度 Trusted Web の実現に向けたユースケース実証、ヒアリングの結果を踏まえ、「特定の事業者に依存しない、安全で相互運用可能な、自己主権型の汎用的なアイデンティティウォレットとオンラインコミュニケーション基盤」を開発し、これらを国際標準やデファクトスタンダードとなり得る技術を用いて、オープンソースソフトウェアとして公開することとした。

また、これらの仕組みを運用・推進するためのコミュニティを形成し、アイデンティティウォレットやオンラインコミュニケーション基盤をベースとした多くの他ユースケースが創出・実装されることで、Trusted Web の社会実装/普及を推進していく。

（※オンラインコミュニケーションとは、オンラインにおける属性情報やメッセージのやり取りのことを指す。）

【問題意識】

オンラインマーケティングにおいて、生活者のメールアドレスや電話番号、Cookie やそれに紐づく行動履歴、位置情報などのパーソナルデータが本人の意思に関わらず様々な事業者によって収集されている。

パーソナルデータがいつの間にか知らない事業者に収集・利用され「気持ちが悪い」といった印象論だけではなく、リクナビ内定辞退率問題では、就職活動における採用判断に影響を与え、ケンブリッジ・アナリティカ事件では、Facebook のデータが第三者に不正に利用され、選挙の結果に影響を与えるなど、事業者により収集されたパーソナルデータが本人の意図しない利用をされることにより、本人の権利利益を害する事案が起きている。また、生活者のアイデンティティは一部の事業者によって管理され、自らのアイデンティティを証明する手段やコミュニケーションの相手方を検証する手段は提供されておらず、SNS での詐欺広告も横行しており、安心してオンラインでのコミュニケーションができない状況となっている。

これらの問題を解決するために、主に法的な対応を含めたガバナンスによって、個人の権利利益を保護するような動きは世界で活発化しており、欧州においては European Digital Identity[2]が実現しつつあるが、デジタルアイデンティティウォレットを用いた新たなコミュニケーションについての社会実装が進んでいるとは言えない。米国においてはモバイルドライバーズライセンスが一部の州で社会実装されているが、相互運用性の問題などが指摘されている。

また、昨年度のユースケース分析レポートでは、13 事業者中 11 事業者が Decentralized Identifiers（DID）や Verifiable Credentials（VC）の組み合わせを属性情報の検証の仕組みとして採用している一方、他の手法と比較評価をした上で採用しているケースはなく、また、その 11 事業

---

[1] 株式会社エヌ・ティ・ティ・データ経営研究所.「Trusted Web 共同開発支援事業に係る調査研究【報告書 別紙】（Trusted Web の実現に向けたユースケース実証分析レポート）」.
https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/2022seika/files/004_report_usecase.pdf

[2] European Commission. “European Digital Identity.” https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

者すべてが別々のウォレット実装を行っている。当社の昨年度実証でもウォレット実装を行ったが、汎用的なウォレットにはなっておらず、UI/UX の課題が残った。

Trusted Web の社会実装を行っていくためには、その基点となり得るウォレットの UI/UX や相互運用性が重要であり、ウォレットの実装のみならず、検証可能なデータのやり取りを誰でも簡単に実装できるようにすることが求められる。

これらを踏まえ、本ユースケースでは、属性情報の検証やデータのやり取りの仕組みを有識者の協力のもと、比較評価した上で、Trusted Web に適合するものを選定し、European Digital Identity Wallet（EUDIW）[3]や OpenWallet Foundation（OWF）[4]で採用が予定されている国際標準技術を組み合わせた、様々なユースケースに対応できる相互運用可能なアイデンティティウォレットを UI/UX デザインの専門家も交えて開発を行い、証明書の発行や検証のプロセスの実装についても開発し、オープンソースソフトウェアとして公開する。

また、エンティティ（人や法人）間のデータのやり取りにおいて、アイデンティティウォレットを基点にユーザ自身のコントロールのもとに検証可能な属性情報のやり取りを行ったとしても、エンティティ間でメールやメッセンジャー、SNS 等でのメッセージングを行う際に、それらの連絡先情報を共有することにより、やり取りするデータや相手方を検証できる仕組み等の新たな信頼の枠組の外側でデータのやり取りが発生してしまうこととなる。当社の昨年度実証においても、メールアドレスの提供を一部実証したが、結局メールアドレスやその他の連絡先情報を共有することにより、連絡先情報に紐づく自身の属性情報のコントロールはできず、特定のサービスへの依存や、メッセージのやり取りの相手先やメッセージ自体の検証、安全性の担保ができなくなってしまうことが課題となった。

また、現在利用されている、メールや SNS、法人向けコラボレーションツール等のオンラインでのメッセージングや属性データのやり取りは、マーケティング分野に限らず、CtoC、BtoC、BtoB、それぞれのケースで多くの課題があることが分かった。（「5.1.2 実証ユースケース概要・実施内容・手法」参照。）

① CtoC における課題

個人間のメッセージングにおいては、日本においては LINE が広く普及しており、他国においても、特定の事業者が独占的に提供するメッセージングサービスが普及している。

これらのサービスは特定の事業者を信頼（事実を確認せず信頼）することによって成り立っており、検証可能な範囲は狭く、アイデンティティの管理やメッセージの相手先や送信元の検証、メッセージの内容が End to End 暗号化されていることの検証はできない。

また、メッセージングサービスの利用登録に際し、電話番号の提供を必須とするサービスが多く、それらがターゲティング広告等の識別子やデータベースとの突合に利用される事例も散見され、特定の事業者

[3] European Digital Identity Wallet（EUDIW）：https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework

[4] Open Wallet Foundation（OWF）：https://openwallet.foundation/

が独占的にサービスを提供し、そのデータを商用に活用することによる不安から、そのようなサービスを利用しない生活者も存在している。

② BtoC における課題

事業者が生活者に対してメッセージを送ることは、マーケティングの一環として広く普及しており、メールマーケティングや SNS マーケティング等における顧客獲得に利用されている。

また、マーケティングメッセージを送信するために、メールアドレスや SNS の ID を簡便に取得するソーシャルログインを利用している事業者も多いが、意図せず自身に関する情報が取得されることに対し生活者は不安を持っていることも提案前のヒアリングにおいて分かった。（「5.1.2 実証ユースケース概要・実施内容・手法」参照。）

また、事業者が多数のソーシャルログインに対応することは、生活者がサービスを利用する際にログイン先の SNS の選択を迷うことになるため、UI/UX の観点においても好ましくない。

③ BtoB における課題

現在においてもメールが BtoB におけるオンラインでのメッセージングの主流となっているが、メッセージの内容が通常では暗号化されていないことにより、PPAP と呼ばれるパスワード付き zip ファイルを添付しパスワードを別送するという、UX 上煩雑で安全性も担保されていない方法が運用されており、メール自体の UI/UX にも課題がある。

他方、上記のメールにおける課題を一部解決する法人向けコラボレーションツールなどは普及しているが、各社が特定の事業者に依存しており、特に法人を跨ぐメッセージングにおいては、Slack, Teams, Chatwork 等複数のツールを常に確認するという UX 上の問題や、担当者が個人レベルで業務に利用してしまうシャドウ IT も問題になっている。

このようにオンラインコミュニケーションはインフラとして必要とされる一方、上記の①～③のようなケースにおいて課題が多く指摘され、アイデンティティウォレットのみならず、安全で使いやすく相互運用可能で特定の事業者に依存しないオンラインにおけるメッセージング基盤をオープンソースで提供することは、現在の社会における大きな課題を解決し、多くの人にその効果が及ぶことが期待される。

また、2022 年度 Trusted Web の実現に向けたユースケース実証の分析レポート[5]でも指摘されている通り、これらの仕組みを普及させるためには、オープンソースでコードを公開するだけではなく、社会実装するためのガバナンスやルールを含め、技術、ビジネス、法律、市民社会等の複数のステークホルダーが参加するコミュニティが運用を推進していくことが必要だと考えられる。

そのため、本実証事業では、既存のコミュニティの協力を得ながら、マルチステークホルダーが参加するコミュニティの形成を行い、ガバナンス・ルールの検討や社会実装/普及のための活動を推進していく。

---

[5] 3.2 実証結果 2）データコントロール・ガバナンスの考え方
「どのような内容をガバナンスで担保していく必要があるのか、そしてそのガバナンス・ルールの案を具体的に示していただくことが、今後の検討を有効に進めていく上で重要」

【実証の目的】

国際標準やデファクトスタンダードとなり得る技術をベースにユーザ自身が自らのアイデンティティを管理し、属性情報を他者と相互検証できるようにした上で、汎用的に利用できるアイデンティティウォレットをトラストおよび UI/UX を重視して開発し、オープンソースプロジェクトとしてコミュニティと連携しながら社会実装/普及を目指すことにより、アイデンティティウォレットをベースとした様々なユースケースで利用でき、かつ相互運用可能なデータのやり取りの実現を目指す。

また、アイデンティティウォレットで管理するアイデンティティを用いて、相互に検証可能で安全なメッセージングプロトコルを検討し、誰でも参加可能なメッセージングサービスを開発する。

2. 事業の概要

2.1 登場する主体と概要

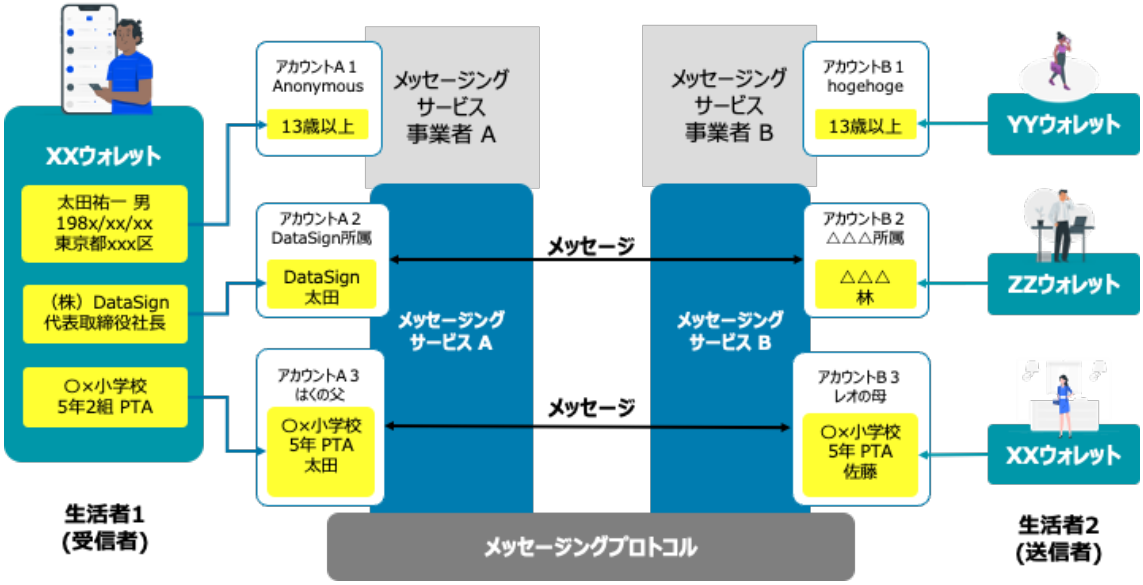

図 2-1-1：ユースケース概要

本実証では、「サービスへの会員登録」と「メッセージのやり取り」という 2 つの異なるユースケースの課題解決に取り組んだ。

サービスへの会員登録

このユースケースでは生活者はオンラインのメッセージングサービスに登録し、そのサービス事業者は登録する生活者を検証する役割がある。

従来の生活者はソーシャルログイン等の ID プロバイダに依存した情報の登録となるが、そのような場合は ID プロバイダにサービス利用状況が逐次分かるため、プライバシーの問題がある。また、サービス事業者に必要最小限の情報を提供することも難しい。さらに、サービス事業者の信頼性を確認できない問題もある。

一方で、従来のサービス事業者は自身が信頼できる事業者であることを生活者に容易に証明することは難しい。そして、生活者の登録情報が本当の情報かどうか、その信頼性をサービス事業者が検証することは難しく、ID プロバイダに登録されている情報を信頼するしかない。

メッセージのやり取り

このユースケースでは生活者 1（受信者）はメッセージングサービスで生活者 2（送信者）からメッセージを受け取る役割があり、生活者 2（送信者）は生活者 1（受信者）へメッセージを送信する役割がある。

従来のメッセージ受信者は、メッセージ送信者が本当に意図している属性を持った生活者 2 のアカウントかどうか検証がすることに課題がある。また、別の問題として従来のプラットフォーム事業者が提供する

メッセージングサービスを利用する場合、メッセージの安全性は特定のプラットフォーム事業者に依存することとなる。

従来のメッセージ送信者は、メッセージングサービス上のアカウントが本当に生活者 1 かどうか検証することは難しい。

2.2 現状の課題を解決する事業スキーム案

2.1.で記載した課題について Trusted Web を具現化することで解決できることが期待される。

具体的には、以下の解決が期待される。

- 生活者 1 は特定の事業者に依存せず、サービス事業者や生活者 2（友だち/取引先）に自分の意思で必要最小限の属性情報を渡すことができる。
- 生活者 1 は特定の事業者に依存せず、サービス事業者や生活者 2（友だち/取引先）と相互に属性情報を検証し、合意した範囲で安全なオンラインコミュニケーションができる。
- 生活者 2（友だち/取引先）も上記 2 つの生活者 1 と同様のことを実施することができる。
- サービス事業者は特定の事業者に依存せず、簡便に利用者の属性の確認・検証を行い、適切なサービス提供を行うことができる。

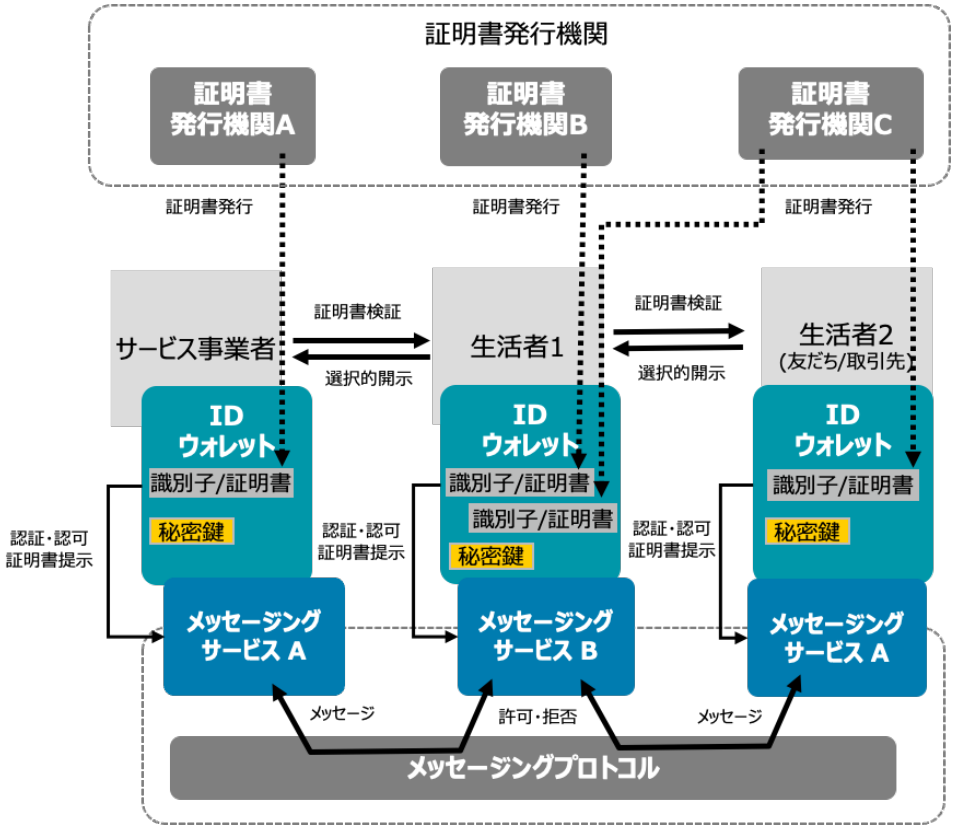

図 2-2-1：事業スキーム図

2.3 社会・経済に与える影響・価値

オープンソースとして公開するホワイトラベルのアイデンティティウォレットをベースに、様々なユースケースで相互運用可能な形で利用されることを想定したビジネス拡大を目指す。

【社会（業界の影響）】

- 国際標準やデファクトスタンダードとなり得る技術をベースにユーザが自身のアイデンティティを管理でき、汎用的に利用できるアイデンティティウォレットを UI/UX を重視して開発できるようになる。
- 相互に検証可能で安全なメッセージングプロトコルを検討し、誰でも参加可能なメッセージングサービスを開発できるようになる。
- アイデンティティウォレットをベースとした様々なユースケースで利用でき、かつ相互運用可能なデータのやり取りの実現を検討できるようになる。
- オープンソースプロジェクトとしてコミュニティと連携し、社会実装/普及を検討できるようになる。

本ユースケースを実現し、オープンソースとして公開することで、現在 ID プロバイダとしてサービスを提供しているプラットフォーマーや証明書の発行事業者、ウェブアプリケーションを提供するサービスプロバイダなど、様々な他のプレイヤーがデジタルアイデンティティウォレットのエコシステムに参入しやすくなり、Trusted Web の実現が推進されると考える。オープンソースの管理はコミュニティに引き継ぐことで、透明性および安全性の高いソフトウェアを様々なプレイヤーが使いやすい環境となる。

【経済的価値】

試算①

- 現在のオンラインコミュニケーション（オンラインにおける属性情報やメッセージのやり取り）の市場規模は、これらのビジネスモデルがパーソナルデータを用いた広告によって成り立っていることを鑑みると世界で約 63 兆円程度となる。[6]
- 2030 年頃までに Trusted Web がインターネット全体での実装することが推進される場合、少なくともオンラインコミュニケーションの 10%が Trusted Web に移行すると仮定すると、6.3 兆円程度の市場規模となる。

試算②

- BtoC サービスにおける広告型フリーミアムモデル（課金すると広告が出ない、YouTube プレミアム等）や広告型割引モデル（広告を視聴すると割引がある、Netflix 等）の採用例を参考にすると、BtoC サービスにおける 1 人当たりの売上はおよそ月額 200 円～1,000 円程度[7]である。

---

[6] statista. “ Programmatic advertising worldwide - statistics & facts.” https://www.statista.com/topics/2498/programmatic-advertising/#topicOverview

[7] DATAREPORTAL. “ DIGITAL 2022: GLOBAL OVERVIEW REPORT.” https://datareportal.com/reports/digital-2022-global-overview-report

- これは公募前に行ったヒアリングにおいて生活者が支払ってよいと考える金額と同程度であり、現在の SNS 利用者の 10%が移行すると仮定すると、46 億人[8]×10%×1,000 円×12 ヵ月 = 5.5 兆円程度の市場規模となる。

これらの試算を鑑みると、オンラインコミュニケーション市場において 10%が Trusted Web に移行すると仮定すると、世界で 5～6 兆円の市場規模が見込まれる。（世界における日本の GDP 割合から日本における市場規模は 3,500 億円と見込まれる）9

表 2-3-1：日本における市場規模予想

	2024 年	2025 年	2026 年	2027 年	2028 年
市場占有率（%）	2%	4%	6%	8%	10%
市場規模（億円）	700	1,400	2,100	2,800	3,500

[8] 総務省.「令和 5 年版 情報通信白書」.
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/nd247100.html

[9] 内閣府経済社会総合研究所.「GDP の国際比較」.
https://www.esri.cao.go.jp/jp/sna/data/data_list/kakuhou/files/2020/sankou/pdf/kokusaihikaku_20211224.pdf

2.4 ペイン・ゲインの整理　（Value Proposition Canvas）

Value Proposition Canvas による顧客セグメント整理と、本事業が顧客に提供できる価値を整理した。

初期的には顧客セグメントとしてビジネスパーソンを想定し、メッセージを送る相手や自分の属性（所属組織など）を必要最小限かつ簡単に検証・証明しつつメッセージのやり取りができることを目指す。中長期的には特定の事業者への依存度を減らし、相互運用可能なウォレットアプリとメッセージングサービスの普及を目指す。

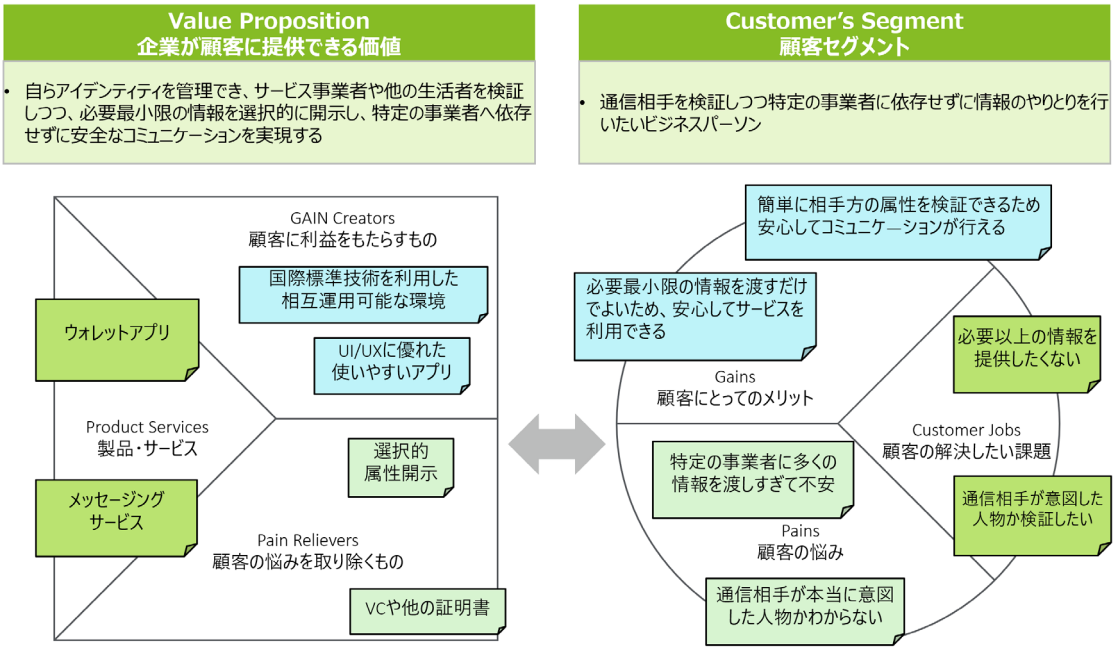

図 2-4-1：Value Proposition Canvas

3. 本実証事業における検証計画

3.1 実証事業で明らかにする論点への導出・経緯

本実証では、ビジネスモデル、UI/UX、機能と業務の整合性、非機能要件、必要な規制・ガイドライン対応といった 5 つの観点において、明らかにする論点を設定し、各論点解決に向けた検証を行った。

ビジネスモデルの観点では、国際標準技術に対応したグローバルに相互運用可能なオープンソースプロジェクトがないといった背景から、本実証で提案するシステムアーキテクチャを広く普及させるためには、どのような進め方がよいかという論点を設定した。論点解決に向けた検討としては、各業界団体やコミュニティと連携して実装・公開するオープンソースのグローバルな普及を目指し、新たなルール・ガバナンスおよびコミュニティ形成を検討することや、グローバルでのデータのやり取りを前提として、本ユースケースにおけるデータの越境移転に対するトラスト関連のルールや論点等についてコミュニティを通じて専門家へヒアリングを実施することとした。

UI/UX の観点では、使いやすいウォレットアプリが不在であることや、メッセージの相手先を確認して安全にメッセージを送る UX の課題があることから、システムの全体でどのような UX を実現すべきかという論点を設定した。論点解決に向けた検討としては、各標準仕様で考えられている UX のフローを参考としつつ、実際にデザインプロトタイプを用いた UX リサーチを実施して、利用者にとって扱いやすくかつ意味を理解しやすい UX となるように検証を行うこととした。

機能と業務の適合性の観点では、外部依存性が低く、相互運用可能で特定の事業者に依存しない識別子/証明書を管理できる仕組みがないといった背景から、生活者、サービス事業者は識別子/証明書をどのように管理して自身を証明すべきかという論点を設定した。論点解決に向けた検討としては、DID や VC のみではなくその他の技術利用 （X.509 証明書等） も広く検討すること、ウォレットの実装や利用する技術に関して OWF や EUDIW の動向を踏まえて決定し実証を行うこと、および秘密鍵のバックアップ・復元方法の検証を行うこととした。

もう 1 つ機能と業務の適合性の観点として、従来の技術や新しい証明書技術を網羅的に比較検討し、現状におけるユースケースに最適な検証技術が整理されていないといった背景から、生活者、サービス事業者はどのように証明書を検証すべきかという論点を設定した。論点解決に向けた検討としては、ウォレットアプリを利用した VC の検証のみではなく、従来の技術 （X.509 証明書等）が利用された場合の検証方法を広く検討すること、および OP や BIMI が分散型メッセージングプロトコル上で利用可能かどうか、またこれら以外の送信者の検証技術についても検討することとした。

非機能要件の観点では、属性情報の一部のみを開示できない、また Unlinkable な仕組みがない、自身において識別子や証明書の提示先の管理ができないといった背景から、プライバシーバイデザインをどのように取り入れたアーキテクチャを実現できるかという論点を設定した。論点解決に向けた検討としては、OID4VP や SD-JWT などの標準仕様を利用した場合に、従来の方法よりプライバシーバイデザインの考え方に従ったアーキテクチャとなっているか検証を行うこととした。

必要な規制・ガイドライン対応の観点では、従来の技術や新しい証明書技術を網羅的に比較検討し、現状におけるユースケースに最適な証明書発行技術が整理されていないことや、証明書発行におけるガバナンスやルールが整理されていないといった背景から、証明書発行機関は生活者、サービス事業者にどのように証明書を発行すべきかという論点を設定した。論点解決に向けた検討としては、従来の公開鍵基盤で利用されている技術の検討も幅広く実施すること、実装した際の技術的に困難な点を確認

し、必要に応じて標準化団体にフィードバックすること、NIST SP 800-63 等を参考に安全性の向上や身元確認レベルの検討を図ること、発行機関や発行時の審査方法のトラストをどのように担保するか検討を行うこと、および選択的開示の概念等を鑑み実施方法を検討することとした。

3.2 本事業におけるスコープ

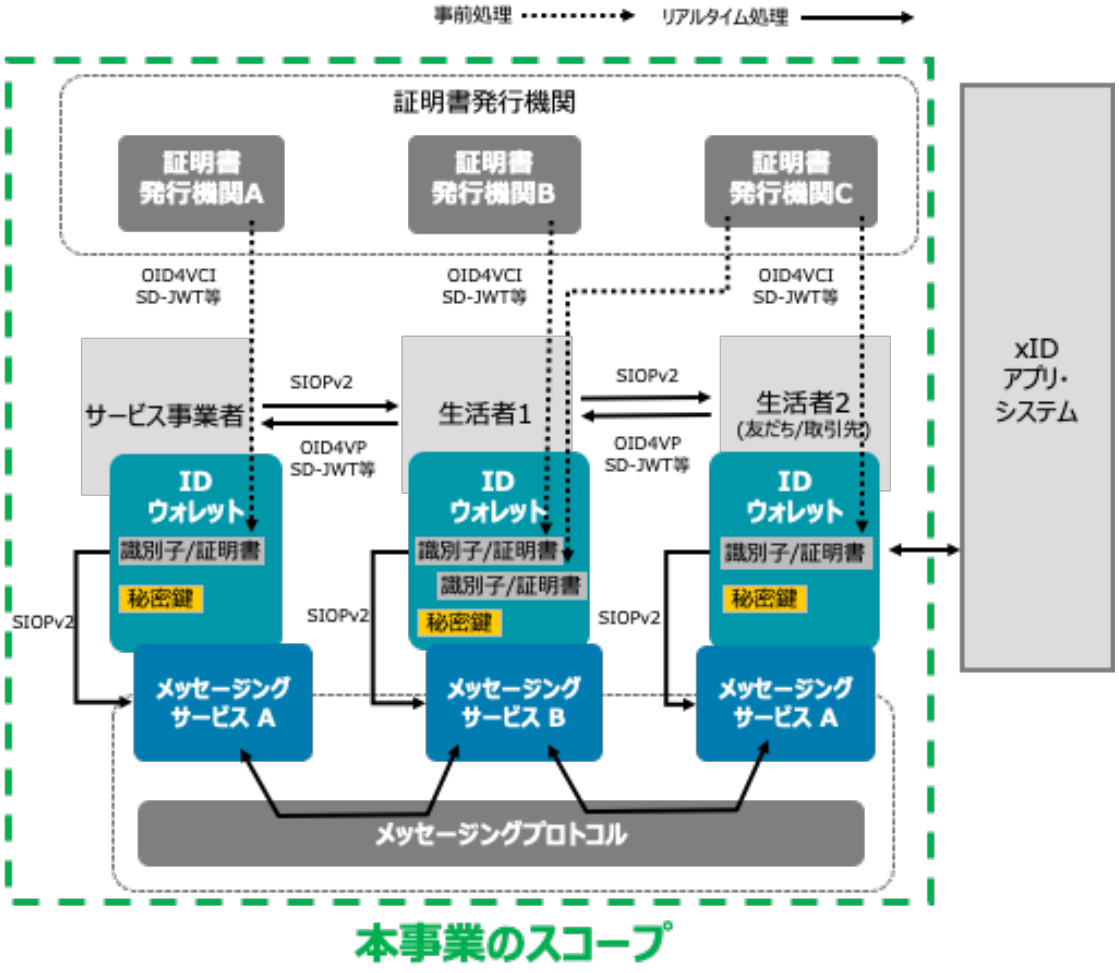

図 3-2-1：事業スコープ図

本実証では、属性情報のやり取りのプロトコルとして、OpenID for Verifiable Credential Issuance（以降「OID4VCI」）、OpenID for Verifiable Presentations（以降「OID4VP」）、Self-Issued OpenID Provider v2（以降「SIOPv2」）に対応することを想定しており、これらの標準技術を用いて Issuer が証明書を発行するためのコード、および Verifier が属性情報の検証を行うためのコードを含めてオープンソースとして公開を行うことで、それぞれのステークホルダーが特定の事業者に依存することなく、これらの実装が行えるようにする。

証明書については、xID 株式会社の協力のもと、xID 社が発行する X.509 形式の本人確認情報を、選択的開示ができる形式（Selective Disclosure for JWTs、以降「SD-JWT」）にした上で、相互運用可能な形で実装する。

メッセージングサービス・プロトコルは分散型で相互運用が可能な Matrix（クライアントアプリのベースは Element）を採用する。

- 事業シナリオ

ウォレットによるアイデンティティ管理とオンラインコミュニケーションとして、以下のシナリオを検証する。

事前準備

- 生活者 1/生活者 2 は xID 本人確認 API を用いて本人確認を行い、ウォレットにマイナンバーカード情報（基本 4 情報/マイナンバーは含まない）を SD-JWT 形式で保有している。
- 生活者 1/生活者 2 は自身の所属を証明する証明書を所属機関から SD-JWT 形式で発行され、ウォレットアプリで保有している。

シナリオ 1：生活者 1 のメッセージングサービスへの会員登録

① 生活者 1 はメッセージングサービスに会員登録するため、PC のブラウザ上に表示された QR コードをスマートフォンのウォレットアプリで読み取る。
② 生活者 1 のウォレットアプリが起動し、サービス事業者が会員登録に必要な情報項目（必須および任意）と用途、サービス事業者自体の検証可能な情報が表示される。
③ 生活者 1 はウォレットアプリ上で情報項目および用途を確認し、問題なければ、「同意」等のボタンを押し、メッセージングサービスに識別子（ペアワイズ識別子を想定）および証明書にある選択された任意の属性証明（例：13 歳以上であるという証明）を送信する。
④ 生活者 1 はメッセージングサービスに自身の属性証明を渡すために PC のブラウザ上に表示された QR コードをウォレットアプリで読み取り、メッセージングサービスに所属証明書（例：〇〇イベントに参加したものであるという証明）を提示する。

シナリオ 2：生活者 2 のメッセージングサービスへの会員登録

① 生活者 2 はメッセージングサービスに会員登録するため、PC のブラウザ上に表示された QR コードをスマートフォンのウォレットアプリで読み取る。
② 生活者 2 のウォレットアプリが起動し、サービス事業者が会員登録に必要な情報項目（必須および任意）と用途、サービス事業者自体の検証可能な情報が表示される。
③ 生活者 2 はウォレットアプリ上で情報項目および用途を確認し、問題なければ、「同意」等のボタンを押し、メッセージングサービスに識別子（ペアワイズ識別子を想定）および証明書にある選択された任意の属性証明（例：13 歳以上であるという証明）を送信する。
④ 生活者 2 はメッセージングサービスに自身の属性証明を渡すために PC のブラウザ上に表示された QR コードをウォレットアプリで読み取り、メッセージングサービスに所属証明書（例：DataSign の社員であるという証明）を提示する。

シナリオ 3：生活者 1 と生活者 2 のオンラインコミュニケーション

① 生活者 1 はメッセージングサービスで生活者 2 の所属証明を確認する。
② 生活者 1 は生活者 2 の所属が検証されれば、生活者 2 とのメッセージを開始する。
③ 生活者 2 はメッセージングサービスで生活者 1 からのメッセージ開始依頼を確認し、生活者 1 の所属証明を確認する。

④　生活者 2 は生活者 1 の所属が検証されれば、生活者 2 とメッセージを開始する。

3.3 実施事項・成果物一覧

本実証事業での実施事項を大きく 5 つに類型化し、①システムの設計、②システムの開発、③実証実験の実施、④コミュニティ形成・ヒアリングの実施、⑤報告書・成果物取りまとめとした。

① システムの設計

(ア) 要件定義・基本設計（DataSign/xID/有識者/デザイン事務所）

本実証では、ウォレットとメッセージングサービスのユースケースで、選択的開示および属性証明を行うことを想定して要件定義を行った。また要件や UI/UX デザインをもとに基本設計を実施した。

(イ) UI/UX デザイン（DataSign/デザイン事務所）

スマートウォンアプリ、ウェブアプリの UI/UX デザインの実績があるデザイン事務所の協力のもと、上記要件や UX リサーチの結果をもとに画面デザインを実施した。

② システムの開発

(ア) 開発（アプリ・インフラ）（DataSign/xID）

要件定義、基本設計および画面デザインをもとにウォレットアプリ（Android、iOS）、メッセージングサービス（ウェブアプリ）、証明書発行機関（認証認可サーバ）の開発を行った。本人確認情報の取得は xID アプリと連携した。

(イ) ユーザテスト（DataSign）

ウォレットアプリを公開し、ユーザテストを実施した。

③ 実証実験の実施

(ア) 実証実験・記録（DataSign）

本ユースケースについてイベントに参加した生活者・サービス事業者の協力を得て、実証実験を実施した。

(イ) 利用者アンケート（DataSign）

実証実験の参加者に対してアンケート調査を実施した。

④ コミュニティ形成・ヒアリングの実施

(ア) 実証期間中ヒアリング（DataSign）

生活者およびサービス事業者へは UX リサーチの観点で、証明書発行機関へはフィージビリティ、ビジネスモデルの観点でヒアリングを行った。

(イ) ルール・ガバナンス机上検討（DataSign/デザイン事務所）

OWND Project と名付けたコミュニティを形成し、ルール・ガバナンスを検討した。その内容をもとにホワイトペーパーを作成した。

⑤ 報告書・成果物取りまとめ

(ア) 最終報告書作成（DataSign）

最終報告書の内容を取りまとめ、報告書を作成した。

(イ) 成果物取りまとめ（DataSign）

納品物となる成果物を取りまとめ対応した。

3.4 スケジュール

3.4.1　全体スケジュール

本実行事業の全体スケジュールを下図に示す。

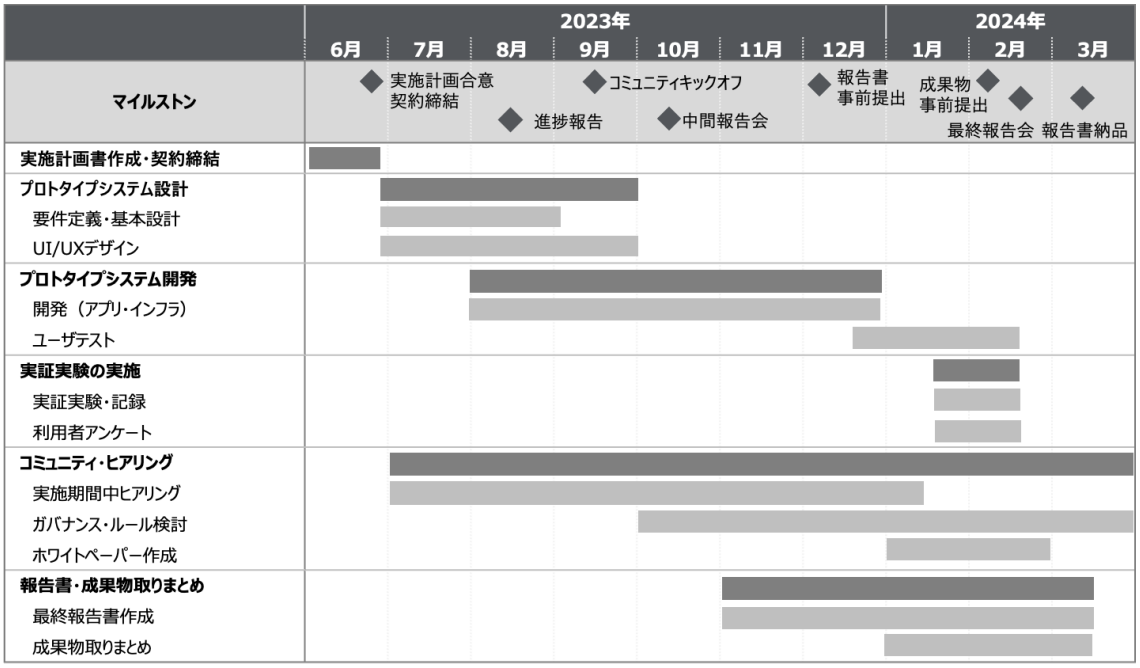

図 3-4-1：全体スケジュール

3.4.2　成果物の作成フロー

月次進捗会議では内閣官房、デジタル庁、事務局、ユースケース担当委員と、毎月の成果物や報告事項で確認いただきたい点についてご意見をいただき、発生した課題について対応をしつつプロジェクトの進め方への反映や、最終的な成果物への反映を行った。

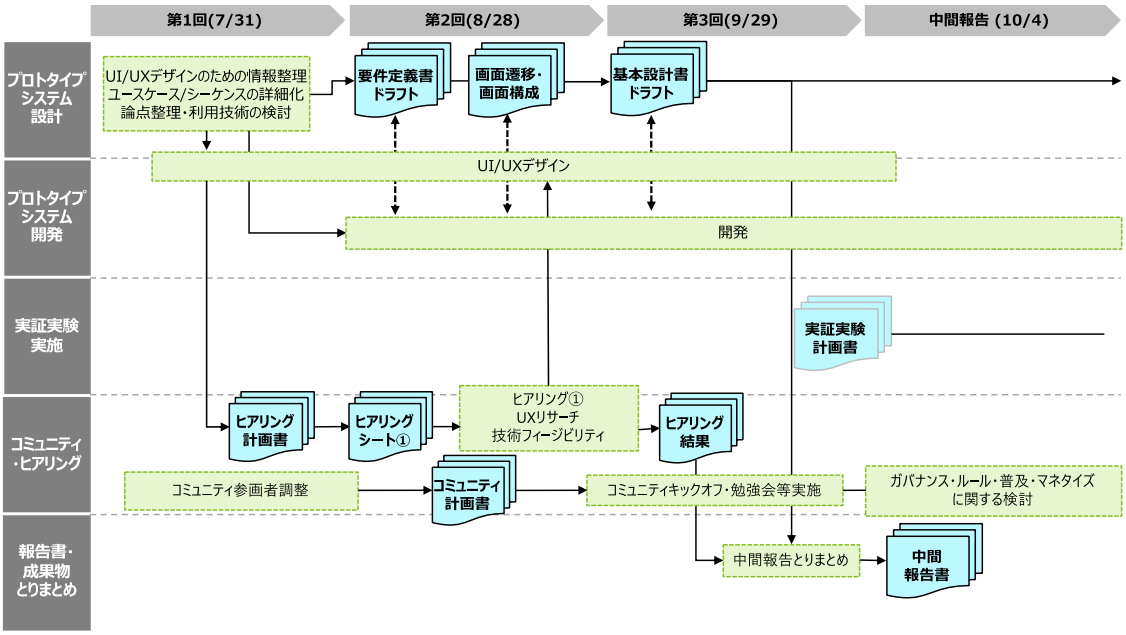

図 3-4-2 （a）：成果物の作成フロー（前半）

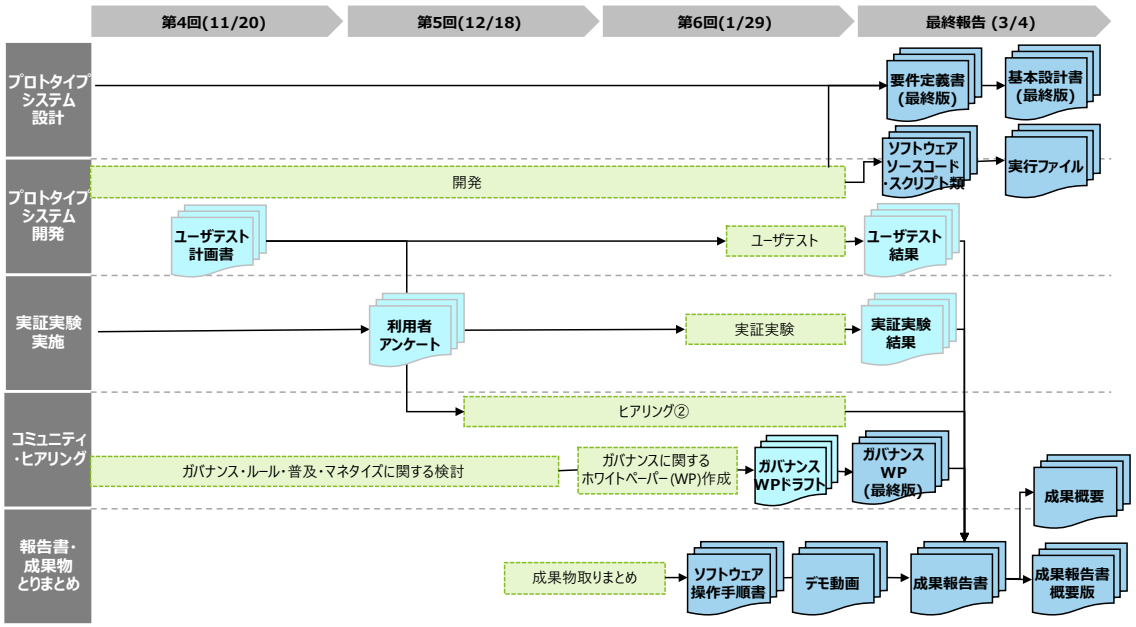

図 3-4-2 （b）：成果物の作成フロー（後半）

3.5 実施体制

本実証事業では、事業企画、プロジェクト推進、設計・開発、テスト、実証実験を DataSign で行う。ウォレットのユースケース実証にあたり、本人確認 API は事業者 A と協業、また UI・UX デザインに関しては事業者 B と協業する。また暗号技術や国際標準技術に関するアドバイスをいただくため、外部有識者 2 名にご協力いただく。さらに証明書発行やサービス展開に関して 3 事業者、コミュニティ形成に関して 2 団体と協力する。

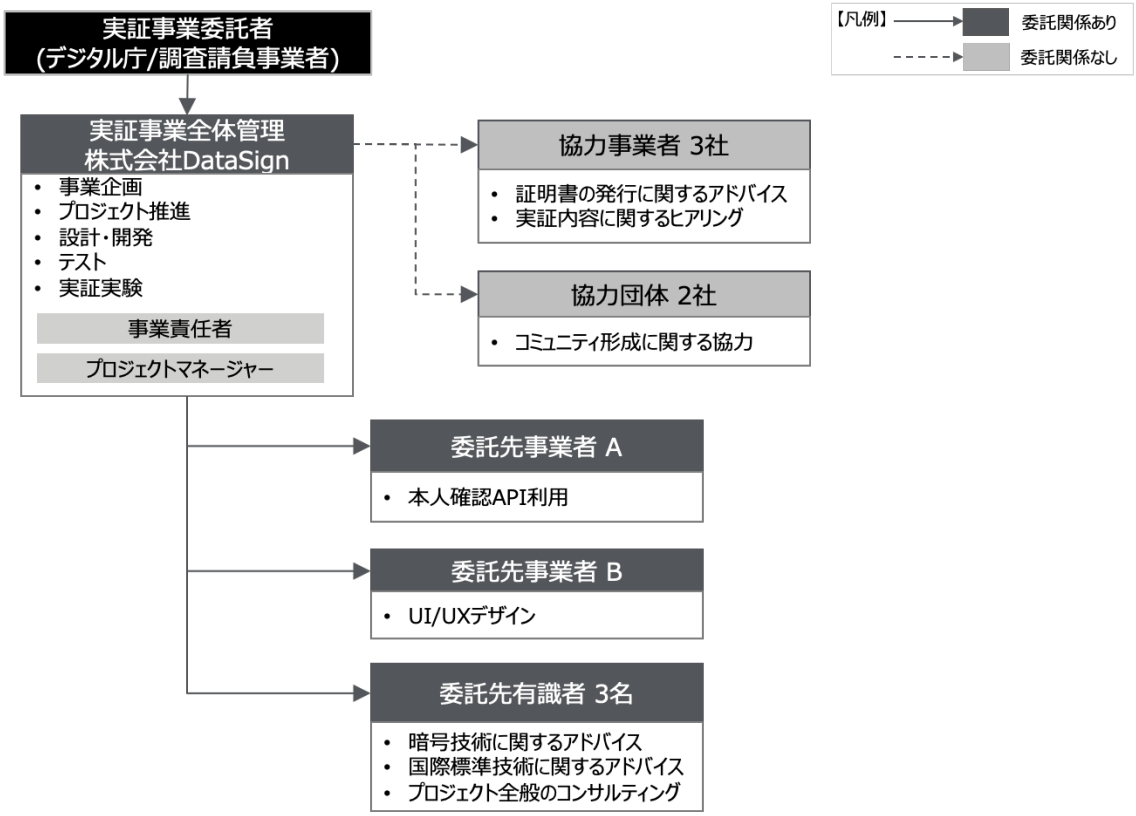

図 3-5-1：実施体制

4. 実証検証（企画・プロトタイプ開発）

4.1 実施概要

4.1.1 企画・プロトタイプ開発で明らかにする論点とその結果

論点①：証明書発行機関は生活者、サービス事業者にどのように証明書を発行すべきか

検討結果とその経緯：証明書形式の比較を選択的開示への対応状況や実装難易度、国際動向を踏まえて議論して、有識者 MTG でのレビューを行い決定した。比較の結果、本実証では SD-JWT を利用することとした。JSON-LD BBS+等その他の証明書形式への対応は実証後にコミュニティによる開発として実施予定である。本人確認情報としては xID 社のサービスと連携し、マイナンバーカードの基本 4 情報の証明書を発行する。発行機関のガバナンスはコミュニティで議論を行いホワイトペーパーにまとめた [10]。

論点②：生活者、サービス事業者は識別子/証明書をどのように管理して自身を証明すべきか

検討結果とその経緯：本実証のユースケースをもとに識別子および証明書形式の比較を選択的開示への対応状況や実装難易度、国際動向を踏まえて議論して、有識者 MTG でのレビューを行い決定した。比較の結果、本実証では Holder（ウォレット）の識別子は認証プロトコルに SIOPv2 を利用することから JWK Thumbprint、証明書形式は SD-JWT を利用することとした。JSON-LD BBS+等その他の証明書形式への対応は実証後にコミュニティによる開発として実施予定である。また、本実証のユースケースをもとに OWF や EUDIW の動向を踏まえてプロトコルの選定を行い、OID4VCI, OID4VP, SIOPv2 を利用することとした。秘密鍵のバックアップ・復元方法は HD ウォレットの仕組みを利用することとし、バックアップはファイルで扱い、ウォレットにエクスポート・インポート機能を実装する。

論点③：生活者、サービス事業者はどのように証明書を検証すべきか

検討結果とその経緯：本実証のユースケースをもとに証明書形式の比較を選択的開示への対応状況や実装難易度、国際動向を踏まえて議論して、有識者 MTG でのレビューを行い決定した。JSON-LD BBS+等その他の証明書形式への対応は実証後にコミュニティによる開発として実施予定である。またメッセージングプロトコルとしては Matrix を採用する。 VC の Issuer を検証する目的としては、サーバ証明書（ただし、Organization Validation 以上の認証レベルであること）を用いる。 VC の具体的な形式は、JWT（SD-JWT）を想定しており、サーバ証明書はその中の x5c ヘッダーに記載することとする。OP や BIMI・vLEI 等の技術への対応は比較検討の結果、技術の普及状況が本要件に現状では合致しないと判定したが、実証後のコミュニティによる開発で引き続き検討を進める。

論点④：生活者、サービス事業者はどのように特定の事業者に依存せず、簡単かつ安全にメッセージをやり取りできるか

検討結果とその経緯：比較検討の結果として、Matrix プロトコルを採用した。 AT プロトコルや Nostr 等の他の分散型メッセージングプロトコルと比較して、仕様内容やその変更に関する手続きが明

[10] OWND Project. “Whitepaper （ドラフト）.” https://github.com/OWND-Project/whitepaper/blob/docs/%231_draft_whitepaper/whitepaper.md

確に定義されており、長く維持されているためである。また、メールと比較して暗号化機能にすぐれており、LINE 等と比較して特定の企業への依存は抑えられる。1 対 1 から複数人のメッセージへの切り替えは、新たな人物がメッセージのやり取りに参加した時に、過去のメッセージを複合できるかどうかで制御される。過去のメッセージを複合できなければ過去に個別送信した VC は表示できない。新しい人物が過去のメッセージの複合を許可するかどうかは Matrix/Element の機能として実装されている。

論点⑤：システムの全体でどのような UX を実現すべきか

検討結果とその経緯：デザインの専門家とともにウォレットアプリ/メッセージングサービスの UI/UX デザインを実施し、デザインプロトタイプ（Figma 機能）を利用したユーザビリティテスト/UX リサーチを実施し、ユーザが理解しにくい箇所、分かりにくい箇所の問題を画面デザインにフィードバックして、最終的な画面デザインを完成させた。

論点⑥：プライバシーバイデザインをどのように取り入れたアーキテクチャを実現するか

検討結果とその経緯：プライバシーへの配慮も考えられている EUDIW ARF Type 1 に準拠することを念頭に、まずは SD-JWT ならびにそれに関する技術（OID4VCs）を実装した。一方で、SD-JWT は署名値が同じになるという仕組み上プライバシーに関する課題（リンカビリティ）が残るため、将来的に JSON-LD BBS+等さらにプライバシー耐性のある証明書形式への対応をコミュニティで継続して検討する。

論点⑦：提案するシステムアーキテクチャを広く普及させるためには、どのような進め方がよいか

検討結果とその経緯：OWND Project と名付けたコミュニティを発足し、MyDataJapan、OIDF-J、DIF Japan SIG、Code for Japan 等からの参加を募集した。開発 WG ではオープンソースとして公開するウォレットアプリ、メッセージングサービスの継続的なメンテナンスを普及活動として実施した。ガバナンス WG ではトラストモデルやデータ越境移転等の議論ならびに専門家へのヒアリングを行い、ホワイトペーパーを発行した。

4.1.2　企画・プロトタイプ開発に用いる技術・標準等を選定した理由および背景

本実証事業では、グローバルに相互運用可能な Issuer – Holder – Verifier モデルに対応したウォレットを開発するため、OID4VCI、OID4VP、SIOPv2 の標準規格を活用することとした。理由としては、EUDIW ARF においても対応が言及されており、今後の標準として普及する見込みのためである。

Holder の識別子をペアワイズ ID とすることや、VDR などの外部依存を避けるため、識別子の規格は JWK Thumbprint を採用した。理由としては、JWK Thumbprint は IETF で標準化されており既に広く使われている、かつ SIOPv2 で利用可能なためである。

プライバシーバイデザインの観点から、選択的属性開示を実施するため、SD-JWT の標準規格を採用した。理由としては、実装が比較的容易でありかつ、EUDI ARF の Type 1 としての実装が必須であることから、将来的な普及が見込めるためである。

証明書発行機関などの事業者の実在性を検証するため、OV 証明書 （X.509） の標準規格を採用した。理由として、既にサーバ証明書として普及している技術であり、安価かつ信頼性が高く証明書の発行機関の実在を証明できるためである。

特定の事業者に依存せず、簡単かつ安全なメッセージのやり取りを実現するため、オープンな分散型メッセージングプロトコルの規格である Matrix を採用した。理由として、他の分散型メッセージングプロトコルと比較して、仕様内容やその変更に関する手続きが明確に定義されており、長く維持されているためである。

4.2 Verify できる領域を拡大する仕組み

4.2.1 登場主体・要求事項整理

生活者 1 （Holder/Client）の役割は、エンドユーザ向けオンラインサービスを利用するために、オンラインサービス事業者に会員登録を行う者、会員登録後に、オンラインサービス事業者および信頼できる相手先である生活者 2（友だち/取引先）からのメッセージを受信する者、である。

実証事業において設定した要求事項としては以下の通り。

- オンラインでの情報収集やオンラインサービスの利用をオンラインで行いたい。
- オンラインサービスを利用するために自身の情報を登録する必要があり、オンラインサービス事業者が信頼できるか確認して登録する情報や手段を判断したい。
- サービス事業者や生活者 2 （友だち/取引先） からのオンラインでの連絡（メッセージの送受信）を承諾するためにサービス事業者や生活者 2 （友だち/取引先） が正当かどうか検証したい。

生活者 2 （Holder/Client）の役割は、生活者 1 へのメッセージの送信する者である。

実証事業において設定した要求事項としては以下の通り。

- 友だちまたは取引先担当者である生活者 1 と連絡を取りたい。
- 生活者 1 に連絡を取るため生活者 1 が本人かどうか検証したい。

サービス事業者 （Verifier） の役割は、生活者 1 にオンラインサービスを提供する者である。

実証事業において設定した要求事項としては以下の通り。

- 生活者 1 にオンラインサービスを提供したい。
- 自身が信頼できる事業者であることを生活者 1 に証明する必要があり、生活者 1 の情報を取得するため、できるだけ簡便な方法で生活者 1 の情報登録（例：年齢等）を行ってもらいたい。

証明書発行機関 （Issuer） の役割は、サービス事業者、生活者 1、生活者 2 への証明書を発行する者である。

実証事業において設定した要求事項としては以下の通り。

- 各エンティティ（サービス事業者、生活者 1、生活者 2）の属性を証明し、それぞれに対し検証可能な選択的開示に対応した証明書を発行する必要がある。

4.2.2　企画・プロトタイプシステムの開発におけるペインの解決方法

- 生活者（Holder）は必要最小限の情報提供ができないというペインがあり、選択的属性開示が可能な証明書形式である SD-JWT を利用することで解決できると考えた。SD-JWT は EUDIW ARF Type1 で要求されており、今後の国際標準になる見込みのため、相互運用性にも資する。Holder から Verifier に提供する識別子はプライバシーの課題（リンカビリティ）に配慮し Pairwise ID （JWK Thumbprint） とした。
- 従来の特定の事業者を利用した認証連携では、生活者（Holder）およびサービス提供者（Verifier）は、情報の信頼性が特定の事業者に依存しているというペインがあり、相互運用可能なプロトコル （OID4VCI, OID4VP, SIOPv2） を採用することで解決できると考えた。これらのプロトコルは EUDIW ARF で言及されており、今後の標準として普及する見込みである。
- サービス提供者（Verifier）は生活者の登録した情報が本当の情報であるかを検証できない、特定の事業者を信頼するしかないというペインがあり、また生活者同士の通信であっても、相手先が意図した相手かどうか （〇〇会社所属の△△さん等） を検証できないというペインがある。これらは検証可能な証明書形式を利用することで解決できると考え、SD-JWT を採用することとした。
- 生活者同士はメッセージのやり取りが特定のサービス事業者に依存しているというペインがあり、分散型のメッセージングプロトコルである Matrix を採用することで解決できると考えた。Matrix は他のメッセージングサービスとの連携、E2E 暗号化の実装、鍵管理の仕組み等にも強みがある。

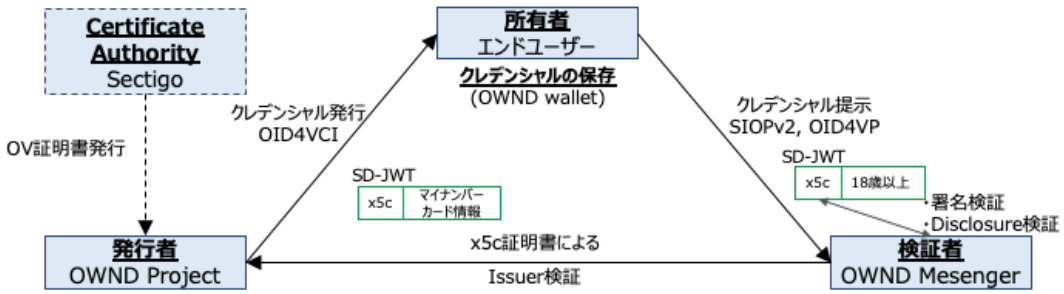

図 4-2-1：検証フロー図

4.2.3　Verify するデータ一覧

- 生活者本人の確認
  - ➢ 生活者がサービスを利用する際に自身の証明を行うために、マイナンバーカード情報を選択的開示可能な Verifiable Credential（SD-JWT） にて検証。xID 社の API を用いてマイナンバーカード情報を取得する。証明書は生活者のウォレットにて管理し、13 歳以上の年齢証明など必要に応じた属性情報を提供する。証明書のアクセスにあたってはウォレットを格納しているデバイス生体認証にてコントロールを行う。
- 証明書発行機関やサービス事業者の実在性

- 証明書発行機関やサービス事業者の実在性を証明するために第三者機関（Sectigo）による審査を行い、OV 証明書を発行する。VCI（OWND Project）のサーバ証明書として設置することにより、通信の暗号化と証明書発行機関としての実在性を担保する。

- メッセージ送受信相手の正当性
  - OWND Messenger にてメッセージを送受信する際に証明書を用いて、送信相手に対して自身の正当性を証明する。社員証をメッセージングサーバに格納して表示することにより、送信相手に対して自身の所属証明を行う。

4.2.4　証明書要件・識別子要件

【証明書】

- マイナンバーカード（※マイナンバーは含まれない）

  主な記載情報は基本 4 情報、13 歳以上証明、15 歳以上証明と 20 歳以上証明。この情報は xID の API を経由して発行されるものとする。記載情報のうち、本証明書は、機微であるため本人の意思で選択的情報開示を可能とする。メッセージングサービスにサインアップする際に 13 歳以上であることを証明することができる。

- 社員証

  主な記載情報は会社名、部署名、社員番号、姓名。この情報は社員証発行サーバ（VCI）から発行される。記載情報のうち、メッセージングサービスでメッセージの送信相手に自身の所属を証明することができる。

- イベント参加証

  主な記載情報は説明、終了日、場所、イベント名、主催者、主催者 URL、開始日、イベント URL。この情報はイベント証発行サーバ（VCI）から発行される。該当のイベントに参加したことを証明することができる。

【識別子】

- Issuer

  発行者（Issuer）を識別するものとする。VC に issuer の URL を記載、/.well-known/jwks.json に公開鍵を配置、kid で指定。選定理由は Verifiable Credentials Data Model v2.0 に準じて。

- Sub

  エンドユーザ（Holder）を識別するものとする。Holder が Verifier に VP を渡すときの識別子。
  - SIOPv2 + OID4VP で渡す場合は ID トークンの sub
  - OID4VP で渡す場合は holder プロパティの値

  選定理由は OpenID Connect に準じて。

- aud

  検証者（Verifirer）を識別するものとする。V SIOP/OID4VP における Verifier の識別子。選定理由は OpenID Connect に準じて。

- id

  エンドユーザ（Holder）を識別するものとする。Holder が Wallet を使うときの Holder の識別子。選定理由はペアワイズ ID 格納のため。

4.3 合意形成・トレースの仕組み

【本システムで目指す合意形成とその履行のトレースの内容】

- エンドユーザの OWND Wallet でのマイナンバー情報の取得において、OWND Project に対してエンドユーザがクレデンシャルとして取得することを許可する。トレースは Wallet 内から可能で、合意の取り消しについても Wallet 内のクレデンシャル削除を行うことで可能である。
- エンドユーザ OWND Wallet での社員証・イベント参加証の取得において企業・イベント主催者がエンドユーザに対してクレデンシャルとして取得することを許可する。トレースは Wallet 内から可能で、合意の取り消しにおいても Wallet 内のクレデンシャル削除を行うことで可能である。
- エンドユーザの OWND Messenge での自身の属性証明（13 歳以上の証明、組織への所属証明、イベント参加証明）を行うにあたり、ユーザが OWND Messenger に対して属性証明のクレデンシャル提供を許可する。トレースは Messenger アプリ内から可能で、合意の取り消しについてもアプリ内でのクレデンシャル削除を行うことで可能である。
- OWND Messenger にてメッセージ送信者がメッセージ受信者との間でメッセージの送受信を許可するために、メッセージ受信者が所属証明を提供する。Messenger アプリ内にてトレースは可能だが、一度相手に送信されたメッセージの取り消しはできない。

【第三者が確認する情報一覧】

- クレデンシャル取得は VCI サーバのログとして AWS に保存される。ログ自体は第三者から閲覧できない環境にある上、提供した事実のみが記録されており、クレデンシャルの内容は保存されない。
- クレデンシャルに関しては JWT 形式であるため、発行者の署名からトレースが可能である。JWT_VC_JSON、SD-JWT ともにリンカビリティが発生し、verifier の結託によりクレデンシャルの持ち主が同一人物ということが推測可能になってしまう。
- エンドユーザが OWND Messenger に提供したクレデンシャルは、Messenger サーバに保存される。クレデンシャルはデータベースに、提供の記録はログとして AWS に保存される。データベース、ログともに第三者からは閲覧できない。

4.4 企画・開発物

4.4.1 業務フロー

本実証の業務フローとしては、エンドユーザがウォレットを利用して証明書発行機関（Issuer）から証明書を取得すること、ならびにサービス事業者（Verifier）へウォレットを利用してサインアップやログインを行い、ウォレットが保持している任意の証明書をサービス事業者に提示してサービスを享受するという流れがある。基本的な業務フロー図を図 4-4-1 に示す。

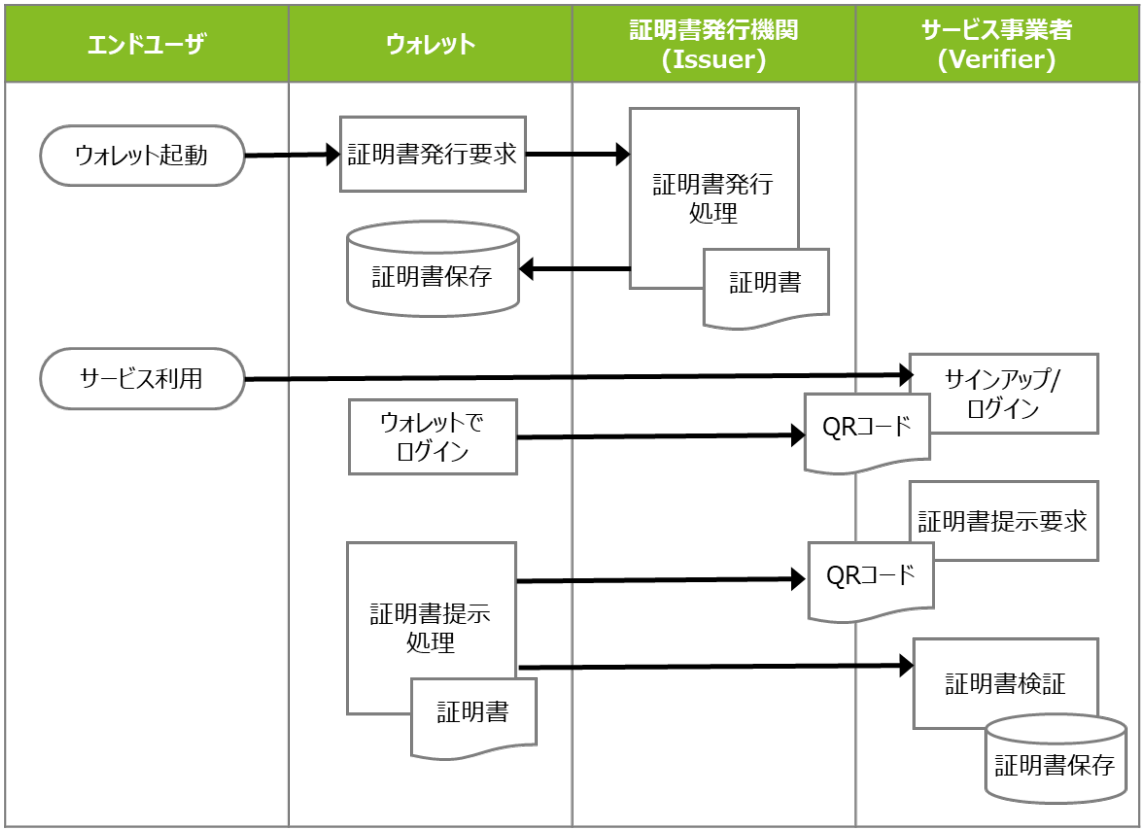

図 4-4-1：業務フロー図

4.4.2 ユースケース図

本実証事業では、以下の項目のユースケースが存在する。それぞれのユースケース図を作成した。

ウォレット

- ウォレット利用開始
- ウォレット認証
- Issuer 公開鍵登録
- 証明書取得
  - マイナンバーカード （xID 連携）
  - 社員証
- 属性情報提供
- 属性情報提供管理

- バックアップ/復元

メッセージングサービス

- サインアップ
- 属性情報提供
- メッセージ送信

例えば、メッセージングサービスへのサインアップは以下のようなユースケース図となる。その他のユースケース図は別紙のユースケース設計書 [11]を参照されたい。

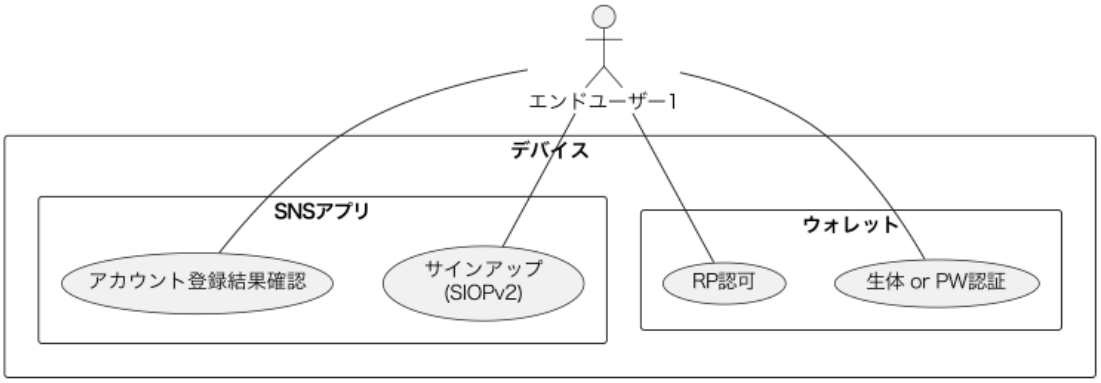

図 4-4-2：メッセージングサービスサインアップのユースケース図

[11] ユースケース設計書
https：//drive.google.com/file/d/1p-DWLv6Jke5osqD2dlKrt94PDyNJ8oKv/view?usp=drive_link

4.4.3　操作画面（UI）

主な操作画面の UI イメージを次の通り示す。

① ウォレット（証明書新規追加）

図 4-4-3：ウォレット（証明書新規追加）

データ取得・共有におけるポイントとして、ウォレットに証明書をインストールするまでは、ウォレットで個人情報を取り扱わないため、ウォレット新規開始時の個人情報に関する説明はシンプルに記載し、証明書発行時に取得する目的と項目が明確に分かるように工夫している。なお、マイナンバーカード情報に含まれるものは基本 4 情報（氏名、生年月日、性別、住所）および生年月日から算出した 13 歳以上、18 歳以上、20 歳以上のような属性情報のみであり、マイナンバーは含まれない。

② ウォレット（証明書提示）

図 4-4-4：ウォレット（証明書提示）

データ取得・共有におけるポイントとして、外部のサービスへの証明書提示時には、「提供する情報」と「提供しない情報」が明確に分かるように表示を工夫した。また、提供先の信頼性確認のため、提供先情報も明示的に記載した。なお、マイナンバーカード情報に含まれるものは基本 4 情報（氏名、生年月日、性別、住所）および生年月日から算出した 13 歳以上、18 歳以上、20 歳以上のような属性情報のみであり、マイナンバーは提供されない。

③　メッセンジャー（証明書提示）

(a) メッセージの送信先の検証（送信元画面）　　(b) メッセージの送信元の検証（送信先画面）

図 4-4-5：メッセンジャー

データ取得・共有におけるポイントとして、ウォレットから証明書を提示することにより、メッセージ送信時に送信先のプロフィールで所属等を確認し、メッセージを始めることができる。また、メッセージ開始時に送信元の検証された属性も確認することができる。

4.4.4　機能一覧/非機能一覧

- ウォレットはクレデンシャル（マイナンバーカード、社員証、イベント参加証）を取得し、基本的操作（取得・表示・削除）を行うことができる。OID4VP プロトコルの提供要求を受け付けることができ、OWND Messenger へのサインアップを行うことができる。また、ウォレット自体のバックアップ・リカバリ機能の提供を行う。
- Issuer はキーペアを生成して OID4VCI プロトコルでクレデンシャルの要求を受け付け生成した鍵を用いて署名し発行することができる。マイナンバーカードの要求に対しては xID と連携することでマイナンバーカード情報をクレデンシャルとして提供することができる。
- Verifier は QR コードを表示して Wallet からのサインアップ・サインインの受け付けを行ったり、OID4VP の属性情報の提供フローを実施したりする。身元を検証した結果送受信者の間で暗号化されたメッセージングサービスを提供する。暗号鍵を再生成するためのセキュリティキーをダウンロードさせリカバリできる機能を提供することができる。

4.4.4.1 非機能検討（リスク分析とセキュリティ対応方針）

本サービス・アプリを利用するにあたってリスク分析・対応方針の整理を行い、うち大きく 2 点を挙げた。

1 点目は、Linkability の発生によるプライバシーの侵害や同意なしの情報使用。悪意ある Verifier 同士が結託してクレデンシャルの名寄せを行うことで可能になってしまう。その結果、Linkability が発生し、選択開示した以外の情報が流出してしまう可能性がある。本リスクについては、SD-JWT や JWT_VC_JSON の機能では回避できないため、BBS+署名などの技術を用いて防止するように検討する必要がある。

2 点目は、Holder 識別子に JWK Thumbprint を使用することによる鍵のローテーション問題。公開鍵そのものが識別子となるため鍵のローテーションに対応できない。鍵の危殆化等への対処を行った場合、更新によって識別子が変化してしまい、アカウントの復旧ができなくなってしまう。今後もペアワイズ可能な識別子を調査する。

4.4.4.2 非機能検討（大規模・商用・社会実装時の対応方針）

【社会実装時に想定する利用規模】

- 日本における SNS 利用者を 1 億 200 万人 [12]とし、そのうちの 10%が OWND Project に係る VCI 発行を実施するとし、VC が 3 クレデンシャルある場合、年間 3,060 万枚の発行と想定される。
- メッセンジャーは 1,020 万人が利用することとし、5 件/日のトランザクションが発生すると、年間 186 億 1,500 万トランザクションが発生すると予想される。

【対応方針】

- VCI、homeserver（matrix）ともに一般的な web サービスと同等のスケーラビリティーを備えていれば可用性に関して問題はないと想定する。

[12] 総務省.「令和 5 年版 情報通信白書」.
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/nd247100.html

4.4.5　データモデル定義

証明書のデータモデルは表 4-4-1 の通りである。

表 4-4-1：データモデル定義

属性値	属性取得元	属性値 （VC 内）
発行元	Issuer	iss
発行日	Issuer	iat
有効期限	Issuer	Exp
証明書形式	Issuer	Typ
アクセストークン	Issuer	accessToken
x5c	Issuer	x5c
x5u	Issuer	x5u
証明書種類	Issuer	Vct
属性情報	Issuer	_sd

4.4.6　実験環境

実験環境を図 4-4-6 に示す。クライアント側はスマートフォンアプリである OWND Wallet およびウェブアプリである OWND Messenger である。サーバ側は AWS 上に Matrix Home Server や各種証明書発行エンドポイントを構築している。

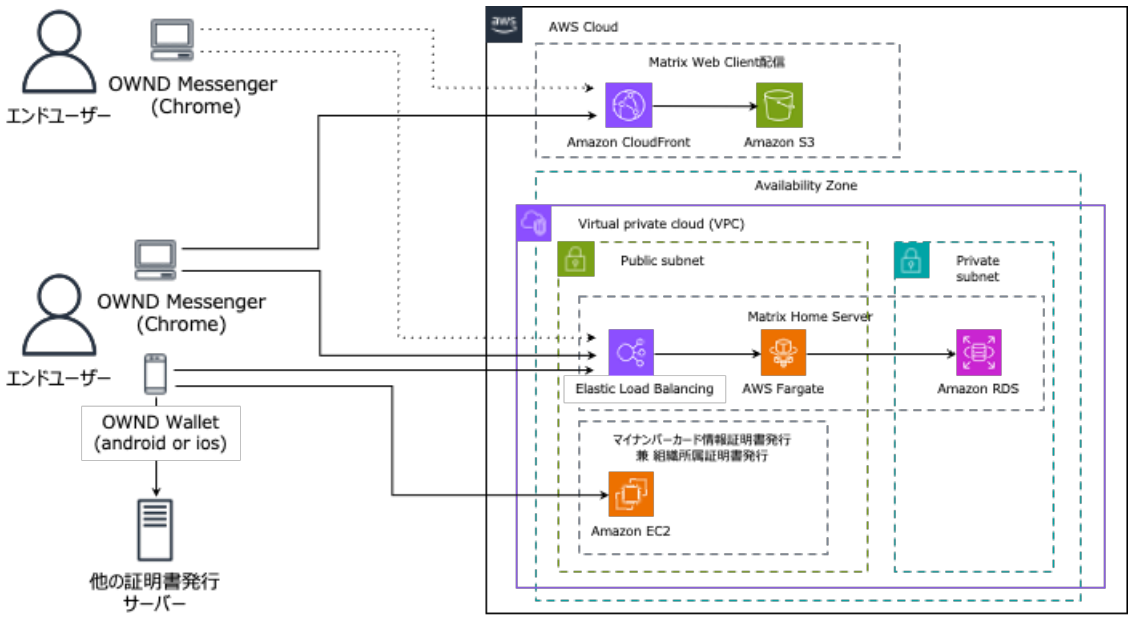

図 4-4-6：クライアントおよびサーバサイドのネットワーク構成図

4.4.7　システムの構成要素

システムの構成要素は表 4-4-2 の通りである。

表 4-4-2：システムの構成要素

コンポーネント名称（システム・ライブラリ名）	開発区分（新規/既存）	開発先/権利の帰属先（OSS）	型式名・ライセンス名（製品の場合）/ OSS 名（OSS の場合）
証明書発行システム（証明書発行モジュール、本人確認 API）	新規開発	OWND Project（OSS）	OWND Project VCI
アイデンティティウォレット	新規開発	OWND Project（OSS）	OWND Wallet iOS/Android
メッセージングプロトコル（認証認可・証明書検証モジュール）	既存オープンソースコードの改変（synapse）	OWND Project（OSS）	OWND Messenger Server
メッセージングプロトコルフロントエンド SDK	既存オープンソースコードの改変（matrix-react-sdk）	OWND Project（OSS）	OWND Messenger React SDK
メッセージングプロトコルフロントエンド	既存オープンソースコードの改変（element）	OWND Project（OSS）	OWND Messenger Client

5. 実証（事業実現に向けたガバナンス・コミュニティ等の検討）

5.1 実施概要

5.1.1 事業実現に向けたガバナンス・コミュニティ等における論点とその結果

ビジネスフィージビリティについて、生活者がサービス事業者の会員登録を行う際の課題、生活者がサービス事業者や他の生活者とメッセージをやり取りする際の課題、サービス事業者が生活者の会員登録を受ける際の課題、本ユースケースを実現した時の期待感・課題解決時に支払ってよい費用、技術への期待感および技術採用時の影響をどう考えるか等を論点として取り上げた。

検討結果としては、公募前のヒアリング時点で、ソーシャルログイン利用時の SNS 事業者の信頼性が気になりログイン利用をためらうという声や、SNS ログイン利用の事後管理に課題があるという声があったため、事業者の信頼性や属性提供の事後管理に関する機能のウォレットへの搭載を検討した。また、初めてのメッセージ送信相手は複数の情報を総合的に判断して検証すること、ビジネス利用ではシャドーITやフィッシングの懸念がある等トラストが確立されていない課題が確認されるため、簡便な送信相手の属性検証方法と安全なメッセージングプロトコルの採用を検討した。さらに、ソーシャルログイン提供事業者による不明瞭な利用停止や不正確な登録情報への懸念が確認されており、特定の事業者に依存せずかつ正確な情報提供が可能な仕組みの検討や、ウォレット、メッセージングサービスが求められている。これらのサービスが利便性の高い機能がある場合や真にセキュリティが確保されている場合であれば、月数百円程度（200 円以上 1,000 円以下程度）であれば支払ってもよいという意見を確認できており、さらなるビジネスモデルの検討をコミュニティで実施した。証明書発行事業者の観点では、既に広く利用されている認証基盤製品が本ユースケースで採用する標準技術を採用するのであれば期待できるという意見や、発行事業者に情報が渡らないという点はビジネスではマイナス面という意見があったが、本実証後も引き続き業界の動向の観察し採用する技術を増やす方向で検討を進める。

ガバナンス・ルール整理について、本ユースケースの社会実装/普及に係るガバナンスモデルはどのようなものが妥当か、本システムの開発・運用に参画する場合にはどのようなルールが妥当か等を論点として取り上げた。

検討結果としては、オープンソースソフトウェアコミュニティのガバナンスモデルを参考として、既存のコミュニティから意見をいただきつつ、開発・運用のコミュニティに参画するルールを Code of Conduct として策定し、階層型のトラスト・ガバナンスモデルの検討を進め、ホワイトペーパーにまとめた。

コミュニティ形成について、本ユースケースの成果物を持続的に普及促進していくためにはどのようなコミュニティを形成すべきか等を論点として取り上げた。

検討結果としては、オープンソースソフトウェアコミュニティのガバナンスモデルを参考として、既存のコミュニティから意見をいただきつつ、持続的に普及促進してくためのコミュニケーション基盤を Matrix 上に整備した。

5.1.2 実証ユースケース概要・実施内容・手法

ビジネスフィージビリティについて、主に IT 業界、出版業界の生活者や事業者へヒアリングを実施した。また、技術への期待感や技術採用への影響の観点で標準化有識者へヒアリングを実施した。

生活者がサービス事業者に会員登録を行う際にどのような課題があるかという論点に関して、公募前の事前ヒアリングでは次のような意見を得た。

- サービス事業者が信頼できるかどうかで直接登録する、もしくは SNS 事業者のログイン機能を利用する、SNS 事業者のログイン機能を利用するとしてもサービス事業者の信頼度合によっても利用する SNS 事業者を選ぶという意見があり、サービス事業者の信頼と会員登録方法に課題があることを確認した。
- 上記おいて信頼できないサービス事業者に必要以上に SNS に登録している情報を渡したくないという意見があった。
- また登録時の必須情報に電話番号などの容易に変更できない識別子があると、登録に抵抗を感じるという意見もあった。
- さらにどのサービス事業者にどの SNS でログインしているか、どのような情報を登録しているか管理できておらず、誤って同じサービス事業者に複数の SNS でログインをしてしまったという意見もあり、生活者が自身の会員登録を管理することに課題があることを確認した。

生活者がメッセージをやり取りする際にどのような課題があるかという論点に関して、公募前の事前ヒアリングでは次のような意見を得た。

- SNS で友だち申請があった場合、申請元を様々なコンテキスト（別経路で申請するという連絡があったなど）で総合的に判断しているという意見があり、検証に課題があることを確認した。
- 上記において本名以外を SNS で利用している場合は、判断が困難であるという意見があった。
- メール連絡であっても外部の様々なコンテキストによってメールの信頼性を判断しているという意見があった。
- （BtoB）SNS のメッセージ機能を仕事で使うことがあるが、取引先に自分の SNS アカウントを知られてしまうのが嫌だという意見があった。
- （BtoB）各社利用しているコミュニケーション手段が異なるため、Slack を使ったり Teams を使ったり、メールを使ったりと非常に煩雑であり、かつ社内規定に違反して利用してしまっているという意見があった。
- （BtoB）ファイルなどの受け渡しの際、それぞれの企業で方法が異なり、PPAP での受け渡しや、最悪の場合、記憶媒体を郵送する、という方法になってしまうという意見があった。
- （BtoB）主にメールを用いているが、フィッシングや迷惑メールが絶えず、怖い。取引先を装ったメールで被害に遭うケースなども聞いているため防御が難しいという意見があった。

サービス事業者が生活者の会員登録を受ける際にどのような課題があるかという論点に関して、公募前の事前ヒアリングでは次のような意見を得た。

- 多数のソーシャルログインが存在するが、UX の観点で選択肢が多いことはユーザを迷わせてしまい、また、以前何を使ってログインしたかを忘れてしまうユーザが多いため、導入は 2 種類にとどめた。

- ユーザが簡単に会員登録できるように Facebook ログインに対応したが、Facebook の規約に違反していないのにも関わらず、アプリケーションが Facebook によって BAN され、Facebook ログインが一時利用不能になった。
- 登録情報の正確性や検証可能性に関してヒアリングを実施した結果、データをもとにした広告配信やデータそのもののマネタイズを進める場合に課題があることを確認した。
- キャンペーン特典取得のためだけに登録情報に不正確な情報を入力されることがあるという課題を確認した。

本ユースケースを実現した際にどれくらいの費用を払ってもよいかという論点に関して、公募前の事前ヒアリングでは次のような意見を得た。

- ウォレット、メッセージングサービスは基本的に無料がよいが、利便性の高い機能がある場合や真にセキュリティが確保されている場合であれば、月数百円程度（200 円以上 1,000 円以下程度）であれば支払ってもよいという意見を得た。
- また、発行できる証明書によって証明書発行機関に料金支払いが発生することは受け入れられるという意見を得た。
- 正確な情報が集まる方がありがたく、ユーザ分析の観点でも重要という意見を得た。
- またメッセージアプリでオンラインマーケティングを行うのであれば、マーケティング担当者は複数の生活者にメッセージを送る必要があるため、CRM のようなウェブアプリが必要という意見を得た。

証明書発行機関は本ユースケースで採用する技術への期待感および技術採用時の影響をどう考えるかという論点に関して、公募前の事前ヒアリングでは次のような意見を得た。

- SIOPv2、OID4VCI、OID4VP 対応のウォレットおよび Issuer 側、RP 側の実装を開発し OSS として公開することは非常に意義のあることであり、Issuer 側、RP 側の実装を特定の事業者に依存するケースが現在は多いため、OSS として公開されることはグローバルにも求められているという意見を得た。
- OID4VCI、OID4VP の実装方法にもいろいろな選択肢があるため、このユースケースで、実装方法を比較し、どのように実装していくかを検討することにも意義があるという意見を得た。
- コミュニティという観点では、今後 Open Wallet Foundation（OWF）においても同様の標準技術が採用されることが考えられ、OWF との連携も可能になるだろう。また、将来的には EUDIW、カリフォルニアの DIW との相互運用性も視野に入れることができるという意見を得た。

ガバナンスおよびルール整備について、本ユースケースの社会実装/普及に係るガバナンスモデルはどのようなものが妥当かという論点に関して、次の通り実証を進めた。

- コミュニティにおいて、本ユースケースの社会実装/普及に必要となる、法制度面などを含めたガバナンスのあり方について討議を行う（9 月～10 月）
- ガバナンスモデル、フレームワークの策定（11 月～12 月）
- ホワイトペーパーの作成（1 月～2 月）

また、本システムの開発・運用に参画する場合にはどのようなルールが妥当かという論点に関して、次の通り実証を進めた。

- ガバナンス討議結果に応じた、各ステークホルダー（証明書発行者・検証者・開発者・システム運用者等）に対する、参画・運用ルールの検討（12 月～2 月）
- 参画・運用ルールの整備（3 月）

コミュニティ形成について、本ユースケースの成果物を持続的に普及促進していくためにはどのようなコミュニティを形成すべきかという論点に関して、Code for Japan コミュニティメンバー、MyData Japan コミュニティメンバー、OpenID Foundation Japan コミュニティメンバー、有識者（技術・法律・標準化）、政府機関関係者・関連団体・事業者等を巻き込み、本実証独自に個人が主体となるデジタルアイデンティティーの社会実装を目指し、よりトラストできるコミュニケーションを実現するための非営利プロジェクトである「OWDN Project[13]」を立ち上げた。OWDN Project では毎月コミュニティ定例会を開催し、以下の取り組みを推進した。

- Trusted Web の勉強会（9 月）
- 本ユースケースの説明（9 月）
- 本ユースケースの社会実装に係る普及促進・運用に対するガバナンス・ルール等に対する討議（10 月～12 月）
- コミュニティにおけるユースケース・開発物に関する討議（1 月～2 月）
- 討議の結果に対する対応（運用ルールの策定や分散ノードの運営、一部機能のコミュニティ内での実利用等を想定）（2 月～）

5.2 実証検証結果

5.2.1 オープンソースコミュニティの設立結果

本実証事業の目的や論点および残課題への対応を、実証期間後も継続して有志により実施していくため、オープンソースコミュニティ OWND Project を設立した。実証期間中に実施した主な成果は次の通りである。

- 2023 年 9 月から毎月 1 回 Monthly Meeting を開催し、Wallet/Messenger の実装、ガバナンスのあり方をディスカッション
- Matrix 上にコミュニティルームを作成
- 開発 WG、ガバナンス WG を設立
- Code of Conduct の作成
- Wallet/Messenger の利用規約/プライバシーポリシーの作成
- ガバナンスのあり方やビジネスモデルをまとめたホワイトペーパーを発行
- Wallet/Messenger 関連のソースコードをオープンソースとして公開

[13] OWND Project
https : //github.com/OWND-Project/

5.2.2　ホワイトペーパーの作成結果

OWND Project コミュニティの成果として、OWND Project WhitePaper を作成し、GitHub で公開した[10]。詳細は公開しているホワイトペーパーをご参照いただき、本報告では目次のみを掲載する。

OWND Project WhitePaper 目次

10. ビジネスモデルの検討

10.1 有料サービスの提供

10.2 秘密鍵管理サービスの提供

10.3 Paas、Saas の提供

6. 調査検証

本章では、ウォレットの UI/UX およびプライバシーバイデザインに関する調査検証内容[14]を報告する。また調査結果を受けて、ウォレットのエコシステムではどのようなトラストモデルが考えられるか考察を行った。

6.1 実施概要

6.1.1 調査で明らかにする論点とその結果

本調査では主に 3 つの論点に関して、インタビュー調査を実施した。

1 つ目として、マイナンバーカード情報の証明書を登録することに抵抗感はあるかという論点に関して、マイナンバーカード情報のようなセンシティブな属性情報をあまり馴染みのないウォレットアプリに格納することは、ユーザにとって抵抗感があると仮説を立て、インタビュー調査を行った。分析の結果として、抵抗を感じるユーザは多く、「ウォレットアプリやウォレット事業者の信頼」や「マイナンバーカードへの親しみ」に依存することが示唆された。

2 つ目として、サービス事業者に証明書を提示するときの感情や認識はどのようなものかという論点に関して、ウォレットアプリを使って他サービスへログインする際など、他サービスへウォレット内の証明書を提示する UX が存在するため、ユーザの感情面や認識を調査した。分析の結果として、サービス事業者やサービスの種類でウォレットを利用するかどうか判断していることや、提供される/されない情報の表示によりポジティブな反応を得られることが示唆された。

3 つ目として、提供した属性情報に対するユーザの意識はどのようなものかという論点に関して、提供した属性情報に対して、提供後に確認できるという UX が与える影響を調査した。分析の結果、一定数のユーザは提供した情報を事後に気にしていることが示唆されるが、「確認したいが方法が分からない」「管理したいが面倒で諦める」といった現状の課題が明らかとなった。

また、上記調査を受けて、トラストモデルがウォレット利用の抵抗感の緩和に寄与するという示唆を得たため、ウォレットのエコシステムでどのようなトラストモデルが考えられるか、考察を行った。結果として、ウォレットアプリが標準技術を正しく実装し然るべき認定を受けていることや、既に信頼の基点となっていることが多い Issuer が証明書発行に値するウォレットかどうかを判断するモデルに言及した。

6.1.2 実施内容・手法

調査は 3 つの論点に対してそれぞれシナリオ（タスク）を用意し、実験参加者がタスクを実施した後にインタビュー調査を行った。具体的には Figma のプロトタイプ画面を実験参加者に操作していただき、以下の点についてインタビューを実施した。

1 つ目の論点である「マイナンバーカード情報の証明書を登録することに抵抗感はあるか」に関しては、ウォレットへマイナンバーカード情報を登録するというタスクを設定した。このタスクのインタビュー質問として「ウォレットアプリを初めて使い始めて、マイナンバーカードを登録しましたが、マイナンバーカードを登録することをどう感じましたか？」という内容を設定し調査した。

---

[14] 株式会社 DataSign.「デジタルアイデンティティウォレット利用者の心理的側面に関する初期調査とトラストに関する一考察」. http://id.nii.ac.jp/1001/00231339/

2 つ目の論点である「サービス事業者に証明書を提示するときの感情や認識はどのようなものか」に関しては、架空の SNS サービスへウォレットで会員登録するというタスクを設定した。このタスクのインタビュー質問として「SNS サービスにウォレットアプリで会員登録しましたが、ウォレットアプリから SNS サービスに情報を渡すことをどう感じましたか？」という内容を設定し調査した。

3 つ目の論点である「提供した属性情報に対するユーザの意識はどのようなものか」に関しては、ウォレットで SNS サービスに提供した情報の確認というタスクを設定した。このタスクのインタビュー質問として「ウォレットアプリから提供した情報を確認しましたが、普段の生活の中で提供した情報が気になることはありますか？」という内容を設定し調査した。

また、実験手法は次の通りである。

- 20 代～50 代、男性：3 名、女性 2 名 （計 5 名）
- Google Meet によるオンラインインタビュー
- 各参加者 1 時間程度
- 事前アンケート、同意取得後に実施

6.2 調査検証結果

6.2.1 検証結果

インタビュー結果に対して再帰的テーマティック分析（RTA）を行い、それぞれに対して 2 つずつテーマを作成した結果を示す。以下に示す内容は脚注にある論文 [15]の引用であり、詳しい内容は論文を参照されたい。

1 つ目の論点である「マイナンバーカード情報の証明書を登録することに抵抗感はあるか」に関しては、「ウォレットアプリやウォレット事業者の信頼」、「マイナンバーカードへの親しみ」という 2 つのテーマを作成した。「ウォレットアプリやウォレット事業者の信頼」という点では、主に以下のような発見があった。

- ウォレットアプリやウォレットアプリの提供事業者がどういったものか分からないという不安から、抵抗感を示すユーザが多いことが示唆された。
- ウォレットの利用者が多い、もしくは利用者にとって明確な便益があれば不安感や抵抗感が軽減されるだろうと言及した参加者も存在する。

また、「マイナンバーカードへの親しみ」という点では、主に以下のような発見があった。

- 証明書を提示するという行動は日常的に行われているが、運転免許証や健康保険証の方が利用経験が多く、マイナンバーカードの提示よりそれらを提示するというユーザが存在することが示唆された。

2 つ目の論点である「サービス事業者に証明書を提示するときの感情や認識はどのようなものか」に関しては、「新しい体験への移行」、「理解の深まりによる安心感」という 2 つのテーマを作成した。「新しい体験への移行」という点では、主に以下のような発見があった。

---

[15] 株式会社 DataSign.「デジタルアイデンティティウォレット利用者の心理的側面に関する初期調査とトラストに関する一考察」. http://id.nii.ac.jp/1001/00231339/

- 実験参加者はウォレットからデータを提供することにそこまで抵抗感はないが、既存のソーシャルログインとの比較から使い分けを検討していた。
- サービス事業者やサービスの種類でウォレットを利用するかどうかの判断が行われる。

また、「理解の深まりによる安心感」という点では、主に以下のような発見があった。

- ウォレットから提供される情報、提供されない情報を表示したユーザ体験から、ユーザの理解が深まり提供情報の自由度に対する関心の表れが起こった。
- 確認できることに対してポジティブな反応があり、それによって一定の安心感が生まれていると示唆される。

3 つ目の論点である「提供した属性情報に対するユーザの意識はどのようなものか」に関しては、「確認したいが方法が分からない」、「管理したいが面倒で諦めてしまう」という 2 つのテーマを作成した。「確認したいが方法が分からない」という点では、主に以下のような発見があった。

- サービス事業者に提供した情報を確認したいと思っているが、確認方法が分からないために確認できないことが示唆された。
- 後から確認するときには提供した情報について忘れる参加者や、後から確認するよりは提供時に確認した方がよいという参加者も存在する。

また、「管理したいが面倒で諦めてしまう」という点では、主に以下のような発見があった。

- どこに何を提供したかを管理したいと思っているが、面倒なので諦めている。
- 電話番号やメールアドレスを変更したときには、提供した情報も更新する必要があり、負荷を感じている。

以上の結果の中で、「ウォレットアプリやウォレット事業者への信頼」という点が、特に重要と位置付け、ウォレットのエコシステムでどのようなトラストモデルが考えられるか考察を実施した。

7. 実証終了後の社会実装に向けた実現案と今後の見通し

7.1 残課題対応方針一覧

本実証における検証を通じて残った課題や、検証を通じて新たに発見した課題、および有識者から指摘を受けた課題を取りまとめ、それぞれ今後取り得る対応方針を次の通り示す。

残課題 1

- 課題内容：SD-JWT を用いる場合、その署名値をキーとした連結性の課題が生じることとなる。欧州の業界団体の昨今の動向等に鑑みると、これを解消する BBS+等のアルゴリズムの採用を検討すべきである。
- 対応方針：本実証では、シンプルな仕様でありかつデファクトになり得る技術である SD-JWT を優先的に実装した。今後はオープンソースコミュニティ（OWND Project）において JSON-SD BBS+等のよりプライバシーへの配慮が可能な署名技術の適用を進める。

残課題 2

- 課題内容：VC 所有者の検証を SD-JWT の Key Binding JWT （KB-JWT） で実施することの是非について、Matrix 上で生活者が VC をやり取りするユースケースにおいては、VC の属性の一つとして Matrix ID を記載しておく方式も考えられる。（KB-JWT を用いない）
- 対応方針：引き続き OWND Project において、2 つの方式に対応できるよう改善予定である。1 つ目は、VC に Matrix の ID を記載しておく方式である。この方式では VC に記載の Matrix ID から有効な当該 VC を受信した場合は、所有者として適切と判断する。2 つ目は、KB-JWT を用いる方法である。社員証やマイナンバーカード情報 VC のユースケースを踏まえると、事前に Matrix ID を VC に記載しておくことは困難であるが、この方式であれば KB-JWT の検証（VC に記載の公開鍵の検証）で実現することができる。

残課題 3

- 課題内容：事業者（Issuer, Verifier）の検証方式において、X.509 形式の既存の Organization Validation（OV）証明書を用いた。しかしながら、金融業界の vLEI 等の新しい技術が利用できないか検討すべきである。
- 対応方針：引き続き OWND Project において、vLEI 等の方式が利用目的（VC の Issuer を検証する目的）に合致するか検証を進める。また、今回対応した OV 証明書では認証できる組織の情報が少ないという課題も生じたため、X.509 で扱える別の証明書への対応も併せて進めることで、組織の属性を適切に検証できるように進める。具体的には、次の証明書の認証項目を調査し検討する。（商業登記電子証明書、e シール等）

残課題 4

- 課題内容：バックアップ/リカバリ方法について、本実証では端末内に Zip ファイルでバックアップする方法を採用したが、よりよい方法を検討すべきである。

- 対応方針：秘密鍵の管理やバックアップ/リカバリについては、モジュール化を行うことにより、ウォレットサービス提供者や秘密鍵管理サービスに特化した第三者が独自に秘密鍵管理サービスを提供できるような構成とし、OWND Wallet 利用者が自身で利用サービスについて選べるように実装をしていくことを検討する。

残課題 5

- 課題内容：証明書を QR コードとして提示する際の所有者との Binding について、今後の標準仕様へのフィードバックも含め検討すべきである。
- 対応方針：OID4VP overBLE（ドラフト）16が策定中で、VP を BLE 通信で送信するプロトコルの標準化を期待できる。こちらが標準化された暁には、VP そのものは既存のプロトコルに従ったものとなるので、オフライン環境での固有の懸念事項ではなくなると考えられる。

残課題 6

- 課題内容：ユニバーサルデザインやバリアフリーの観点を含む、Wallet/Messenger の UI/UX の継続的な改善を検討すべきである。
- 対応方針：引き続き OWND Project において、ユニバーサルデザインやバリアフリーの観点を含む UI/UX の課題について検討を進める予定である。また、本実装の UI/UX 検討段階で、Messenger に Wallet を利用して複数の ID でログインすると、どの ID でログインしているか判断が困難になるという課題もあり、本課題への対応も進める。

残課題 7

- 課題内容：コミュニティやアプリの国際化について検討すべきである。
- 対応方針：引き続き OWND Project で検討を進め、まずは英語 GitHub やアプリ、関連コンテンツの英語対応を進める予定である。また、OWF 等の関連コミュニティへの情報提供を積極的に行い、連携を進める予定である。

残課題 8

- 課題内容：他サービスとの連携において、OWND Wallet で（OWND Messenger 以外の）他サービスへのログイン、OWND Messenger への他ウォレットでのログインが考えられるが、それらをどのように認定するか等、ガバナンスの観点で検討すべきである。
- 対応方針：OWND Messenger へ他ウォレットを用いてログインする件について、他ウォレットが予め認定を受けていることを要求する考えは現在のところない。一方で、他サービスに OWND Wallet を利用するに際しては、業界標準となり得る認定スキームの調査とそれへの対応を進めていくこととする。

[16] OpenID Connect. “OpenID for Verifiable Presentations over BLE - draft 00.” https://openid.net/specs/openid-4-verifiable-presentations-over-ble-1_0.html

残課題 9

- 課題内容：OWND Messenger （Matrix） において、Fediverse の観点から別プラットフォーム （Slack など） との接続について検討すべきである。
- 対応方針：本実証中に、Slack などとの接続方法について机上検討を実施したが、プラットフォームごとに特別なホスト用サーバを実装する必要があり、開発工数の関係で実施は見送った。プラットフォームごとにサードパーティライブラリは存在しているため、引き続き接続するプラットフォームを OWND Project で議論し、実装の検討を進める。

残課題 10

- 課題内容：VCI の Key Binding 問題、予め発行しておくかどうか。SD-JWT だとクレデンシャルに鍵が必要（BBS+は大元の署名値を秘匿したまま提供先ごとの VC を渡す仕組みであり、発行時点で対象の Holder の情報を含める仕組みではない）。
- 対応方針：発行時点で Holder と VC を結びつける構成の場合は、提供先ごとに VC を発行することになる（ウォレットから VC が盗難されても問題とならない）。VC 発行者による保有者の証明ではなく、提供時点での保有の証明ができれば OK という場合は BBS+を用いることで実現できると考えられる。

残課題 11

- 課題内容：Matrix へ Verifiable Presentation を行うユースケースにおいて、Session Fixation に関する配慮が現実装にはない。そのため悪意のある者が、VP の QR コードを取得し被害者に対応させれば被害者の属性を得ることができる。
- 対応方針：仕様上定義されている Session Fixation に関する機能実装を、引き続き OWND Project で検討を進める。

残課題 12

- 課題内容：残課題 1 に挙げたように、連結性への対処のために BBS+のクレデンシャルも扱えるよう対応する見込みである。しかし、SD-JWT のクレデンシャルを扱う場合においては（ウォレットは様々な形式のクレデンシャルに対応するのが適当と思われる）、連結性が引き続き生じることに変わりない。
- 対応方針：RP ごとに渡す証明書を変えることで、署名値による連結を防ぐ方法がある。そのためには、ウォレット中に署名値違いのクレデンシャルを複数プールしておくことが考えられる。SD-JWT 形式のクレデンシャルの連結性を改善するためにこの機能を実装するか、引き続き OWND Project で検討を進める。

残課題 13

- 課題内容：SIOPv2 の direct post を行った後に、追加のユーザ側の作業（例：Matrix アカウント ID の決定）が必要となる場合のフローが仕様上明確ではなく、一部独自な実装を行っ

ている部分がある。具体的には、ウォレット上で操作を続ける（今回行った実装）かブラウザ上で操作を続けるかについてである。

- 対応方針：引き続き OWND Project で最新仕様や仕様検討の動向を確認し、必要に応じてフィードバックを行う。

残課題 14

- 課題内容：OS の仕様により意図した通りに動作しないこと（iOS により起動する DIW が勝手に選択される点）や特定の事業者に依存してしまう可能性のある部分（OS を介した Secure Element の利用）について、今後これらの事業者に対してどのようにアプローチを行っていくべきであるか。
- 対応方針：引き続き OWND Project において、各業界団体やコミュニティと連携して、国際標準規格や OS ベンダーに働きかけを実施する。その場合、政府機関からの働きかけが有効かどうかも含め検討を進める。

残課題 15

- 課題内容：OSS プロジェクトが公開しているコードを用いた第三者のアプリケーション開発に対して、理念の継承などを評価、認定等する枠組みはどのようなものがあるか、また、そのような評価や認定は必要か。（OpenID Certification program は似たような取り組みではあるが、技術的な部分のみの評価であるため）
- 対応方針：引き続き OWND Project において、ホワイトペーパーの理念やガバナンスモデルを継承していくためにはどのような取り組みが有効であるかを検討する。

残課題 16

- 課題内表：次に実装を進めるべきものは何か（mDL、BBS+、 Aries 系など）。BBS+の実装を優先的に検討しているが他にあれば追加検討すべきである。
- 対応方針：引き続き OWND Project において、JSON-LD BBS+の実装を検討しているが、国内やグローバルの動向に合わせて、優先的に実装すべき標準規格に関する追加検討を進める。

残課題 17

- 課題内容：Issuer, Holder, Verifier が独立性を担保し、結託せずにトラストモデルを維持するためにはどのようなガバナンスのもとにエコシステムを設計すべきか。
- 対応方針：次の 2 つのアプローチについて検討を深めることとする。1 点目は、各エンティティが定め公開すべきデータの取り扱い規則について、それへの準拠性審査を定期的に行い可視化することである。審査主体や可視化の方式（OpenID Federation の Trust Mark を想定）について詳細を深めることとする。2 点目は、各エンティティの運営事業者（Holder については、Wallet の開発事業者を想定する）の素性または関係性（関係会社であるか否か等）を明

示する仕組みの導入を検討し、結託等生活者が意図しないエンティティ間の繋がりに気づくための情報を提供できるようにする。

残課題 18

- 課題内容：ウォレットのトラストを確保できたとしても、ユーザにその信頼性を理解し納得して利用してもらうことには課題がある。ユーザとのコミュニケーションはどのように進めていくべきか。
- 対応方針：ウォレットアプリの信頼性に関する UX リサーチにおいても、OWDN Project の対応すべき課題として継続して検討を進める。

残課題 19

- 課題内容：選択的属性開示を実現しても、Verifier が多くの属性情報の提供を要求してきた場合、ユーザが適切に処理の継続や停止を判断することは難しい。Verifier の過度な属性情報の提供要求をどのように検知し制限することができるか。
- 対応方針：この課題は、OIDC のような従来の認証連携においても課題となっているため、OpenID ファウンデーション・ジャパン等と連携し、対応を進める。

残課題 20

- 課題内容：iOS 側の仕様で、複数のデジタルアイデンティティウォレットがスマホに入っている場合、QR コード読み込み時に、そのうちの 1 つが勝手に選ばれてウォレットを発行できないといった課題が実証実験で明らかとなった。
- 対応方針：引き続き問題の詳細な検証を OWND Project で実施し、標準化団体や OS ベンダーへのフィードバックを検討する。

残課題 21

- 課題内容：本実証では分かりやすさを重視するため、マイナンバーカードの含まれる基本 4 情報の証明書は「マイナンバーカード情報」という名称としたが、ユーザからするとマイナンバー自体が含まれてしまうのではないかという懸念や、公的機関から発行された身分証明書と誤解しないかという課題がある。
- 対応方針：引き続き OWND Project において、UI/UX の改善を進め、どのような機関が発行したものあるか、証明書にはどのような情報が含まれているか、Verifier に提示する際にはどのような情報が提示されるか、等がユーザにとって明確に理解できるように努める。

7.2 ユースケース実現モデル

7.2.1 ビジネスモデル案

① ウォレット（秘密鍵管理サービス）

デジタルアイデンティティウォレットにおいて、秘密鍵の管理は大きな課題の 1 つである。現状の OWND Wallet においては、アイデンティティを自分自身で管理するメリットと引き換えに、秘密鍵管理やバックアップは自己責任になるというトレードオフが発生している。

OWND Wallet では、秘密鍵を各デバイスのセキュアエレメントに保存しており、端末自体を紛失した場合には、事前にバックアップを手動で行っていない限り、情報が失われてしまう。

またバックアップデータに関しても、デバイスの紛失に対応する場合には、Google Drive 等のオンラインストレージに保存することになり、設定ミス等によりデータが漏えいしてしまうリスクが発生する。

また、複数のデバイスでデジタルアイデンティティウォレットを用いる場合には、デバイス間でのデータの自動的な同期が行われる等、利便性についても考慮する必要がある。

暗号資産で用いられているウォレットも、ノンカストディアルウォレット（秘密鍵を利用者自身で管理する）の場合は同様の課題を抱えている。

有名な Mt.Gox 事件や Coincheck 事件はいずれも、サーバに保管している秘密鍵に対して、第三者から不正なアクセスがあったことが原因である。そのため、暗号資産を安全に管理したい利用者は、秘密鍵を自分自身で管理するノンカストディアルウォレットに暗号資産を保管しておくことが一般的になっている。

暗号資産ウォレットで広く用いられている HD Wallet （Hierarchical Deterministic Wallet）は、12 個のランダムな単語を秘密鍵生成のシードとして利用する方法を用いて復元することができるようにすることで、秘密鍵の管理の簡略化に取り組んでいるが、12 単語を忘れないようにどこかに保管しておく必要は生じる。

ウォレット作成時に表示される 12 単語のスクリーンショットを保存したり、12 単語をコピーしてメモ帳アプリに保管したり、紙に書き写したりすることで保管している方が多いが、管理方法として適切であるとは言えない。

そのため、利用者が自分の信頼できる第三者に秘密鍵やバックアップデータの管理を委託することで、安全にこれらのデータを保管し、デバイス間同期などの利便性に対応するサービスを DIW 提供事業者やその他の第三者が有料で DIW 利用者に提供するビジネスが考えられる。
特に DIW 提供事業者ではなく、その他の第三者（銀行などの信頼性が高い企業）が上記のようなビジネスを行うことで、安全性だけでなく、ウォレット間の相互運用性にも対応する利便性の高いサービスが提供できると期待される。

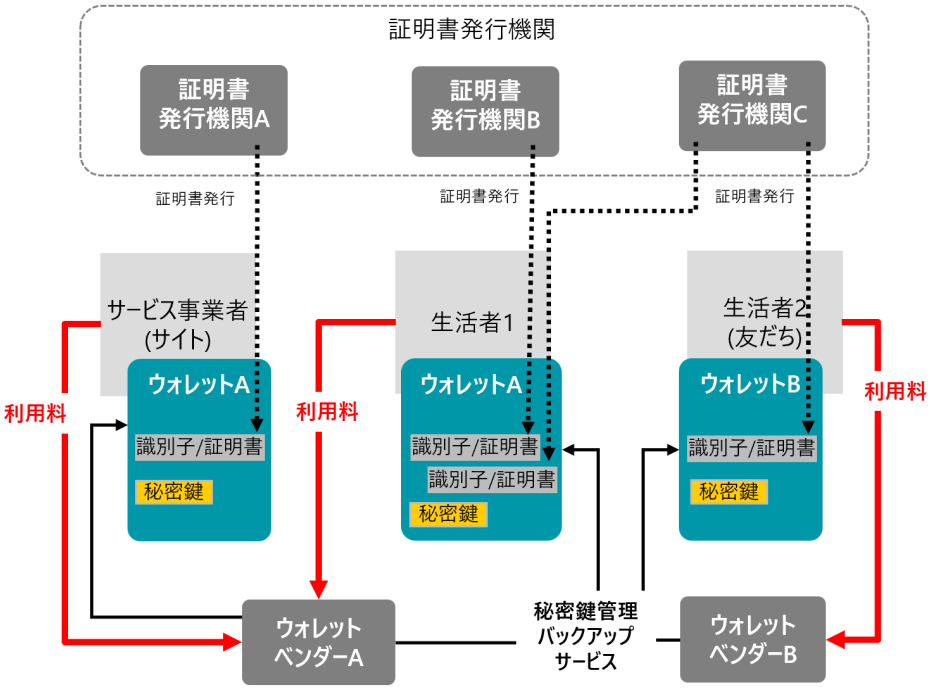

図 7-2-1：ウォレット（秘密鍵管理サービス）

② 証明書発行（企業向け Paas, Saas の提供）

学生証や社員証、TOEIC の点数証明、フィナンシャルプランナーの資格証明など、自身が保有する資格等を第三者に対して証明を行う必要がある場合には、学校や所属企業、検定事業者等が発行した、何らかの証明書を提示する必要がある。

現状においては、紙の証明書を提示することが多く、デジタルにおける証明や検証について課題があることは、現状の課題でも述べた通りである。またこれらをデジタル化するデジタル証明書発行サービスも存在はしているが、選択的開示には対応しておらず、例えば、TOEIC のデジタル証明書には顔写真や生年月日なども記載されており、不要な情報まで提示先に渡すことになる。また、デジタル証明書は Issuer のサーバにホストされており、本人によるコントローラビリティが確保されているとは言えず、デジタル証明書の Issuer が、証明書発行者ではなく、デジタル証明書発行サービスになっていることや、Issuer 自体を検証できないことなどにより、ガバナンスに関して課題が存在している。

OWND Project においては、Issuer 自身の検証を行えるよう X.509 証明書を用いた Issuer 自身の検証にも対応し、また、選択的開示にも対応することにより、上記の課題を解決したシステムを Issuer に対して提供できるよう構成している。これらのシステムを Issuer 自身がサーバを構築し運用することも可能であるが、学校や所属企業、検定事業者等の Issuer 自身がそれらのシステムを構築運用し続けることは難しいため、証明書発行システムの構築運用を行うサービスを SIer やホスティング事業者等が提供することが期待される。

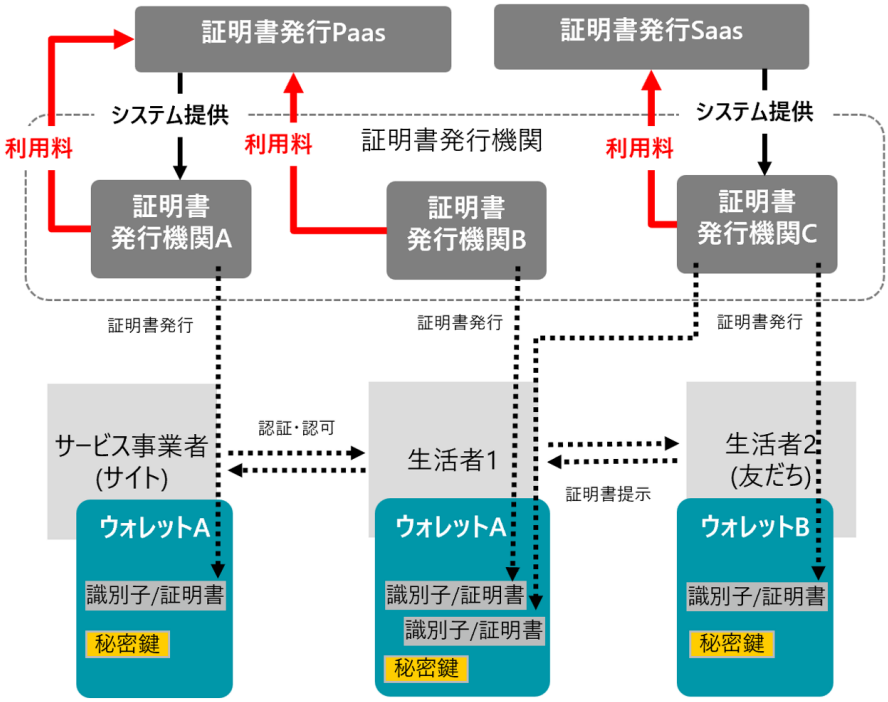

図 7-2-2：証明書発行（企業向け Paas, Saas の提供）

③ メッセージング（企業向け Paas, Saas の提供）

OWND Messenger では、特定の事業者に依存している Slack 等の企業向けメッセージングツールを代替するものとして、Matrix プロトコルに対応した相互運用可能なメッセージングアプリケーションをオープンソースで公開する。

これらのコードを利用し、各社が自社のメッセージングサーバを構築し、企業間でのメッセージのやり取りを、特定の事業者に依存せず、End-to-End 暗号化された環境で行うことで、課題の解決を行うことができる。

しかしながら、メールサーバにおいても、メールサーバを自社で独自に構築し運用しているケースはほとんど存在しておらず、メールサーバの Paas や Google Workspace や Office 365 等の Saas を利用し、その構築運用を委託しているケースがほとんどである。

E メールのケースと同様、メッセージングサーバについても、Home Server の Paas や Saas を提供するサービスが SIer やホスティング事業者等から提供されることが期待され、また、証明書発行インフラ提供サービスを組み合わせることで、企業間での所属証明等も可能なメッセージング環境を構築することが可能となる。

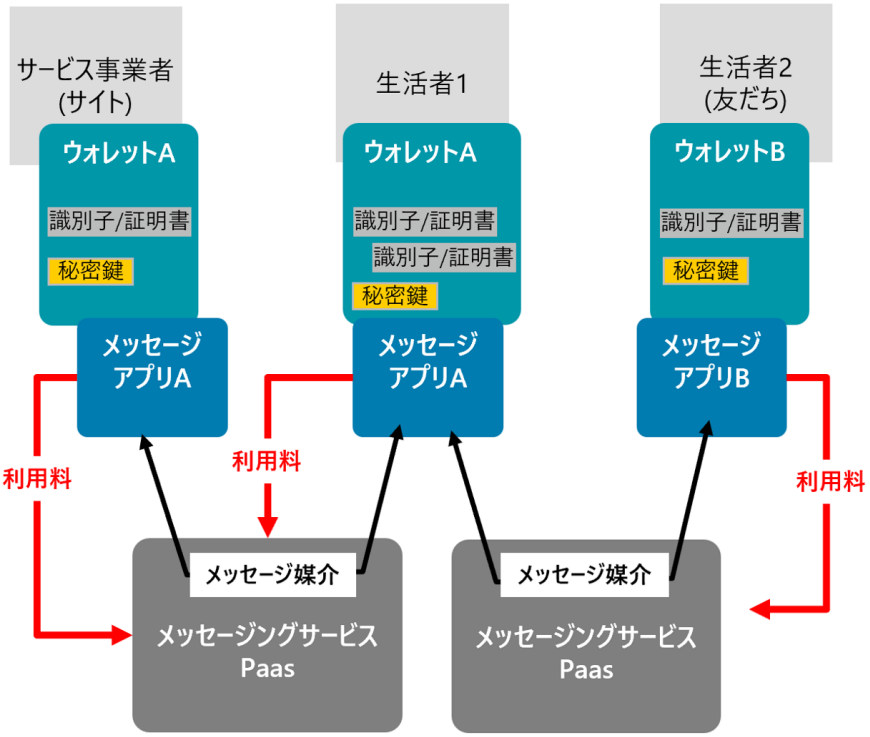

図 7-2-3：メッセージング（企業向け Paas, Saas の提供）

④ メディアサービス

特定の事業者に依存している LINE 等の個人向けメッセージングツールを代替するものとして、Matrix プロトコルに対応した相互運用可能なメッセージングアプリケーションを個人向けに提供することで、LINE 等と同様、メディア化（様々な情報を提供することにより、広告やデジタル商材等で収益を得る）することにより収益を得ることが可能となる。相互運用可能であることで、プラットフォーマーが独占的に運営している環境からの乗り換えが期待できる。

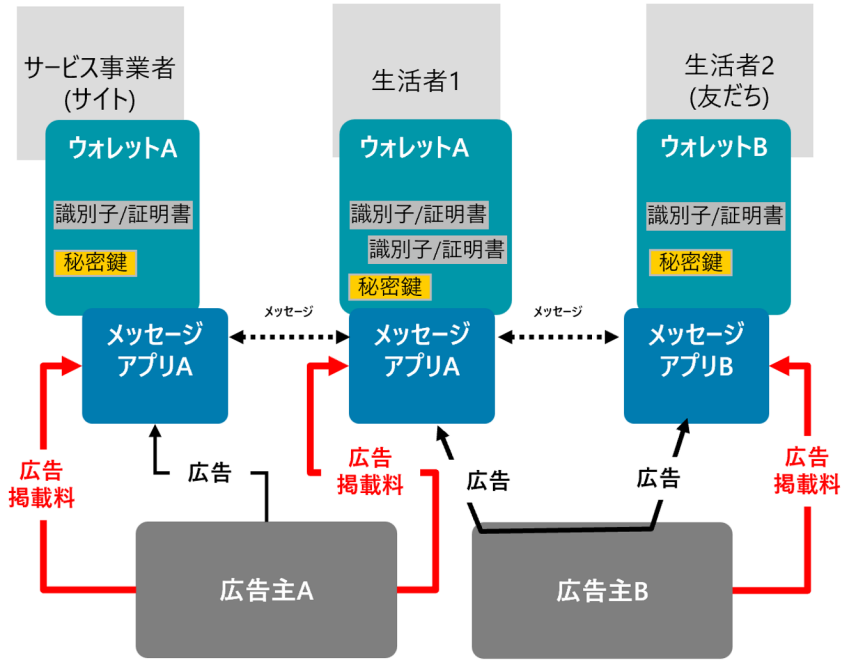

図 7-2-4：メディアサービス

7.2.2　システム案

Trusted Web ホワイトペーパーで示されている必要となる原則について、以下の観点から本実証における対応を表 7-2-1 で示す。

表 7-2-1：システム案

観点	対応
データ主体によるコントロール	OWND Wallet に関してはサーバ側では一切情報を保持せず、ユーザにすべて帰属する設計とし、データを受け取る際（VC 発行時）やデータを提示する際（SIOPv2 によるログイン時や VP 提示時）には、どのようなデータをやり取りするかを画面上に示し、特に提示する際には、提示されない情報も示すことにより、データ主体によるコントロール性を確保している。 OWND Messenger に関しては、自身の所属等を OID4VP によって提示することにより、データ主体が自らの意思で自身の属性を示すことができるようにしている。
ユニバーサル性	OWND Wallet に関しては、iOS および Android の両プラットフォームに対応し、OWND Messenger に関しては Web で公開することにより、できるだけ多くの人が利用できるように構成している。 ユニバーサルデザインやバリアフリーの観点については、課題が残っている。

ユーザ視点、相互運用性	OWND Wallet、OWND Messenger ともに、相互運用性を担保するための技術選定を行っており、OWND Project で公開するアプリケーションにロックインされない。 イベント参加証の実証実験においては、OID4VCI に対応している DIW であればどの DIW であっても発行可能なように対応した。現に VESS Wallet との相互運用性を確保している。 また、OWND Messenger は Element 他、matrix protocol によるメッセージングアプリケーションとの相互運用が可能である。
継続性、相互運用性	社員証やイベント参加証について、既存の Trust 手段（x.509 PKI）とフェデレーションを行う設計とした。具体的には、VC の内部に、OV 証明書を含めることにより、VC 発行組織の実在性の検証を行うことができる設計とした。

【本システムに登場する各エンティティの役割】

- Certificate Authority

  Issuer および Verifier の信頼性担保のために Issuer と Verifier に対して証明書を発行する。
- Issuer

  Holder の認証を行い、Holder に対し、Holder の何らかの属性を証明するための Verifiable Credentials（VC） を発行する。Issuer は VC を発行するためのシステムを保持している。
- Holder

  Issuer から VC を発行してもらい、Verifiable Presentation（VP）を作成し、自分の属性を証明したい相手（Verifier）に提示する。Holder は Issuer から VC を受け取り、VP を Verifier に提示するための Wallet を保持している。また、Verifier（サービスプロバイダ）に対しアカウントの発行を行ってもらう主体である。
- Verifier

  Holder から確認したい属性の証明書が含まれた VP を受け取り、VP および VC を検証することで、Holder の属性および Issuer の信頼性を確認する。Verifier は Holder から VP を受け取り、検証するためのシステムを保持している。また、Holder に対して何らかのサービスを提供するサービスプロバイダとして、Holder にアカウントを発行する。

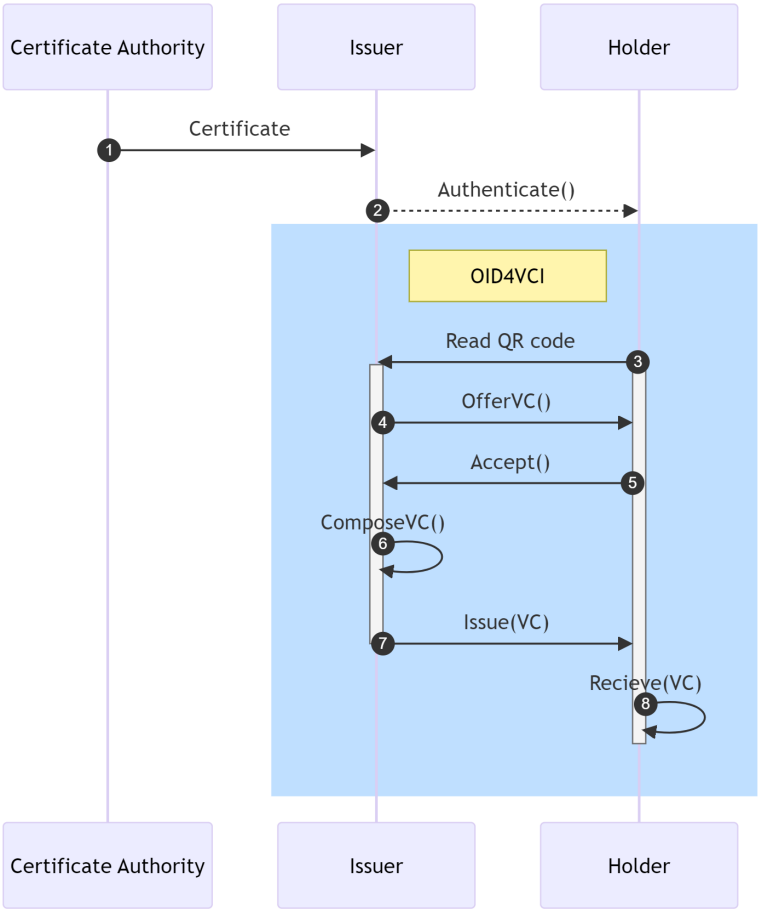

図 7-2-5：OID4VCI におけるシーケンス図

① Certificate – Certificate による Issuer への OV 証明書発行

Issuer の信頼性を担保するため、認証局が X.509 証明書を発行する。X.509 証明書は VC を発行する際に x5c ヘッダーに格納される。

OWND Project においては、既存の X.509 サーバ証明書のガバナンスに従って発行される OV（Organization Validation）証明書を利用し、Issuer の実在性の担保を行っているが、これに限らず、例えば日本においては、法務省が発行する X.509 証明書を用いることも考えられる。

将来的には X.509 に限らず、OpenID Federation 1.0 trust chain などの技術の採用も検討し、Issuer のメタデータ（ISMS 取得企業である等）の検証もできるように発展させていくことも考えられる。

② Authenticate（） - Issuer による Holder の認証

Issuer が VC を発行する主体である Holder を認証し、VC の発行に必要な QR コードを Holder に提示する。

OWND Project では、現状において Issuer による Holder の認証方法については検討の対象としていないため、例えば社員証を発行する際に Holder が社員であることをどのように認証するかについては、言及していない。

③ READ QR code - Holder による QR コードの読み取り

Holder が Wallet を用いて QR コードを読み取る。この際、Wallet を起動せず、カメラアプリ等から QR コードを読み取ることも可能であるが、QR コードから生成される Credential Offer は "openid-credential-offer：//" というスキーマで表現されるため、Wallet を指定することができず、"openid-credential-offer：//"に対応した複数の Wallet を保有している場合には目的の Wallet に VC が発行されない可能性がある。

Android においては、OS の機能として Wallet を選択する UI を備えている場合もあるが、iOS においてはどの Wallet が選択されるかは指定することはできず、目的の Wallet 以外の "openid-credential-offer：//"に対応したアプリケーションは端末から削除する必要がある。

④ Offer VC（） - Issuer による VC の発行オファー

Issuer が QR コードを読み取った Holder に対して VC の発行オファーを送信する。この際に Holder は識別子として、端末内に保持する秘密鍵に紐づく公開鍵が得られる識別子（公開鍵そのものやハッシュ化したもの、その他各種 DID の Holder が考えられる）を生成し、Issuer に提示する。

⑤ Accept（） - Holder による VC 発行の承認

OWND Wallet では、VC 発行前に、CA、Issuer、Issuer のプライバシーポリシー、発行する目的、発行する情報の項目を Wallet 内で Holder に対し提示するように構成しているが、VC 発行前にこれらの項目を Holder に対して提示することは、技術的な仕様として標準化されているわけではないため、今後発行時における Holder に対する情報提示のあり方については議論が必要だと考えられる。

⑥ ComposeVC（） - Issuer による VC の生成

Issuer は VC を生成する。この際に VC には、CA から Issuer に発行された X.509 証明書、Issuer の公開鍵、Holder の識別子、Holder の属性情報を含め、Issuer の保有する秘密鍵（X.509 証明書の発行時に用いたもの）で署名を行う。

⑦ Issue（VC） - Issuer による VC の発行

Issuer は生成した VC を Holder の Wallet に発行する。

⑧ Recieve（VC） - Holder による VC の受領

Holder は VC を受領し、Wallet 内に格納する。

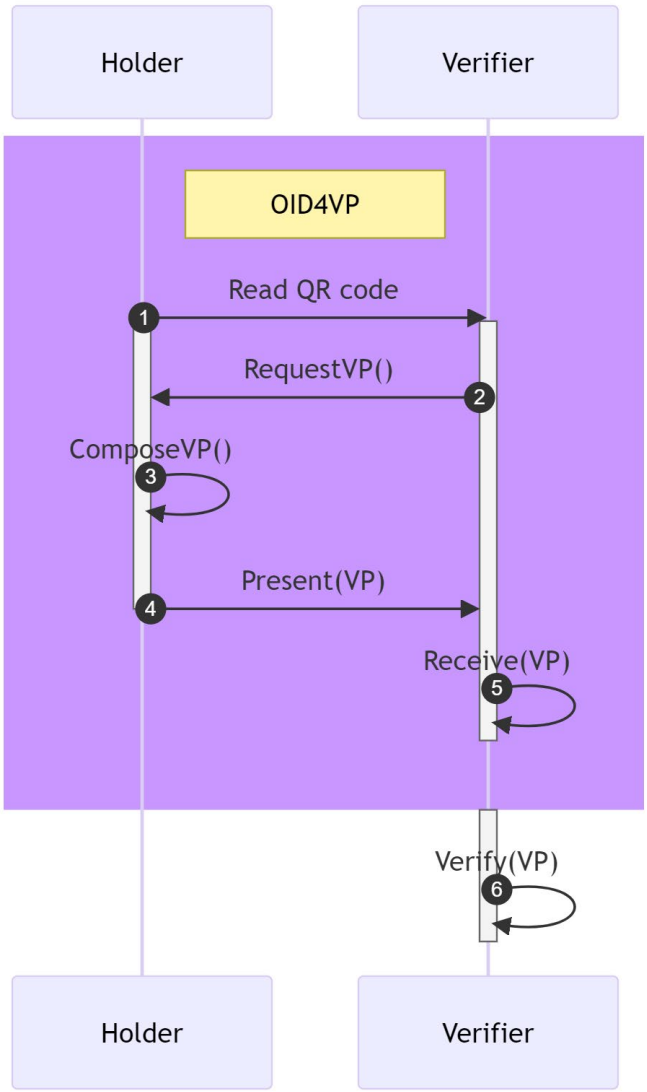

図 7-2-6：OID4VP におけるシーケンス図

① Read QR code - Holder による QR コードの読み取り

Holder は属性を提示したい Verifier の表示する QR を Wallet で読み取る。

② RequestVP（） - Verifier による属性の要求

Holder はどのような属性がどのような事業者から要求されているかを確認する。

この際 OWND Wallet では、提供する目的、提供する情報の項目を Wallet 内で Holder に対し提示するように構成しているが、これらの項目を Holder に対して提示することは、技術的な仕様として標準化されているわけではないため、今後情報提供時における Holder に対する情報提示の在り方については議論が必要だと考えられる。

③ ComposeVP（） - Holder による VP の生成

上記要求を受け、Holder は利用する証明書の選択を行い、選択した証明書と属性情報、Holder の識別子を格納し、Holder の秘密鍵によって署名することにより VP を生成する。

このとき、OWND Wallet では、Verifier の要求する項目が証明できる証明書が自動的に選

択可能な証明書一覧に表示されるよう構成されているが、Verifier の要求する項目の項目名と、Holder が保有する証明書の項目名が一致している必要がある。現状 OID4VP においては項目名についての標準化は行われていないため、今後ユースケースごとにスキーマや項目名の標準化が必要になってくると考えられる。

④ Present（VP） - Holder による VP の提示

OWND Wallet では、VP を提示する際に、提供される情報の項目だけでなく、上記で選択された証明書に含まれるが、提供されない情報の項目も提示するように構成し、また、提供先のアプリケーション名や提供先事業者名、提供先事業者の OV 証明書の内容、プライバシーポリシー等を表示することで、誰に何が提供され、何が提供されないかが分かりやすいように表示している。

これらの提供時に表示する情報についても標準化は行われていないため、今後 VP に情報を提供する際に Holder にどのような情報を提示すべきかについては議論が必要である。

⑤ Receive（VP） - Verifier による VP の受領

Verifier は Holder から VP を受け取る。

⑥ Verify（VP） - Verifier による VP の検証

Verifier は Holder の公開鍵を用いた VP の署名検証、Issuer の公開鍵を用いた VC の署名検証、VC の x5c ヘッダーに含まれる X.509 証明書の検証を行う。

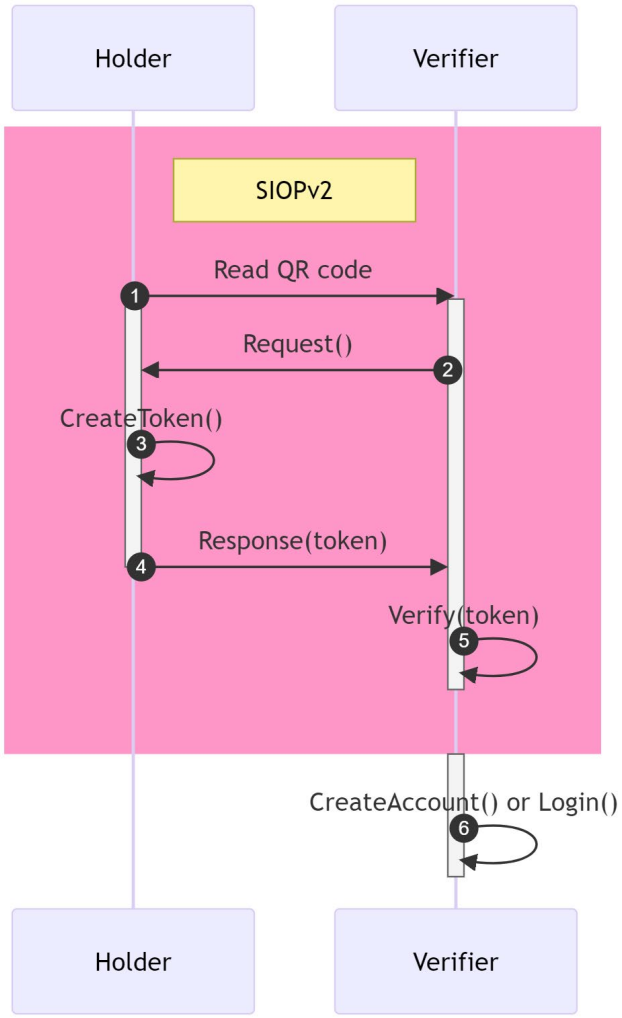

図 7-2-7：SIOPv2 におけるシーケンス図

① Read QR code - Holder による QR コードの読み取り

Holder はアカウントを作成したい Verifier（サービスプロバイダ）の表示する QR を Wallet で読み取る。

② Request（） - Verifier による認証の要求

Holder はどのような事業者から認証が要求されているかを確認する。

この際 OWND Wallet では、提供する目的、提供する情報の項目を Wallet 内で Holder に対し提示するように構成しているが、これらの項目を Holder に対して提示することは、技術的な仕様として標準化されているわけではないため、今後認証時における Holder に対する情報提示のあり方については議論が必要だと考えられる。

③ CreateToken（） - Holder による ID トークンの生成

上記要求を受け、Holder は Verifier に提供する識別子を生成し秘密鍵で署名することにより、ID トークンを生成する。

このとき、OWND Wallet では、提供する識別子による事業者間での名寄せを行えないようにするため、Verifier ごとに異なった識別子（JWK Thumprint）を生成している。

7.2.1 Verifiable Credentials を用いた属性証明において利用している Holder の識別子とは異なることに注意が必要である。

④ Respons（token） - Holder による ID トークンの提示

生成した ID トークンを Verifier に送信する。

⑤ Verify（token） - Verifier による ID トークンの検証

Verifier は Holder の公開鍵を用いた識別子および署名を検証する。

⑥ CreateAccount（）or Login（） - カウントの作成またはログイン

検証した結果、問題がなければ、アカウントの作成またはログインの処理を行う。

7.2.3 ガバナンス・ルール案

ガバナンスの検討にあたり、コミュニティ（OWND Project）におけるガバナンスモデルの検討を行った。

OWND Project のガバナンスの概念図を（図 7-2-8：OWND Project のガバナンス）に示す。

OWND Project のガバナンスは、第一階層として、Trusted Web の概念を継承することとし、OWND Project Whitepaper[17]内で宣言することとした。

第二階層として、OWND Project の活動、公開するソースコードおよび提供するアプリケーションが、Whitepaper の内容に沿って開発・運用されていることを担保するために以下の原則に基づいてガバナンスを構築することとした。

- 透明性

意思決定プロセスと、プロジェクトに関わる文書を公開することで、透明性を担保

- 多様なステークホルダーによるコンセンサス

参加者を排除しないことにより、多様なステークホルダーによるコンセンサスを形成することで意思決定を行う。

また、第二階層おいて、OpenID Foundation、Matrix.org Foundation などの外部コミュニティと連携し、それらのトラストフレームワークに準拠することで、OWND Project のガバナンスが強化されることを想定している。

第三階層として、他エンティティにおける OWND Project の成果物利用時のガバナンスが考えられるが、現時点では、ガバナンスの対象としていない。ただし、将来的に他エンティティが OWND Project の理念に適合しているかを評価する枠組みを提供する可能性を残している。

[17] OWND Project. “WhitePaper.” https://github.com/OWND-Project/whitepaper

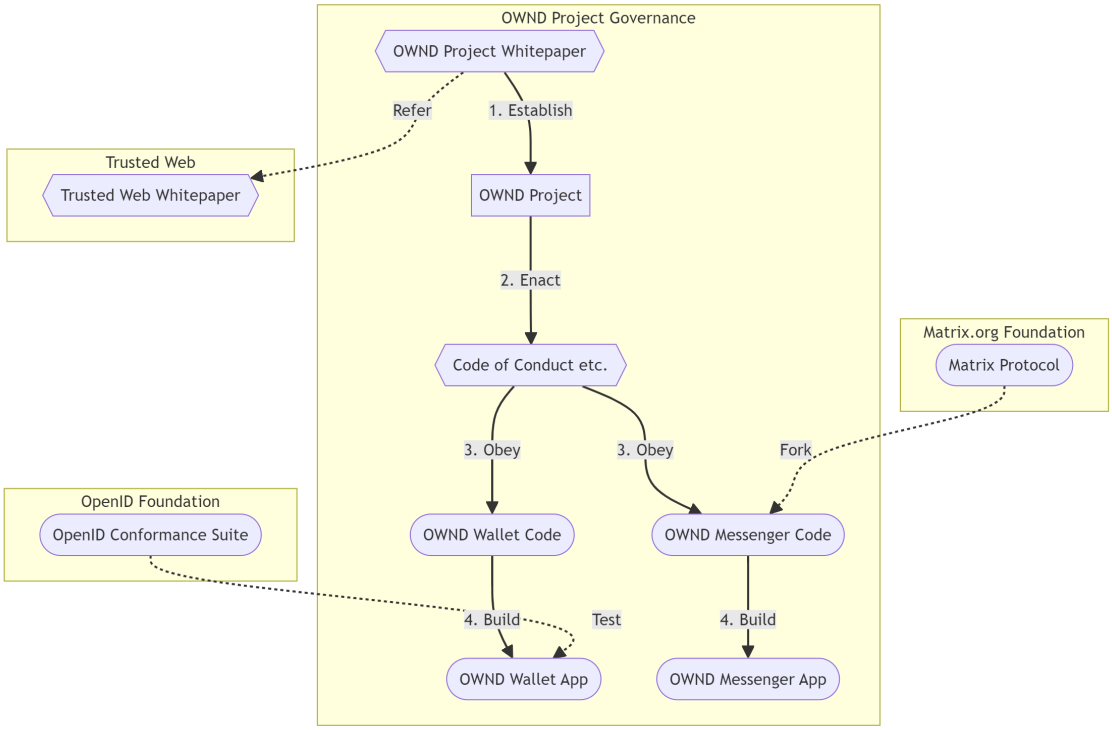

図 7-2-8：OWND Project のガバナンスモデル

1. Establish

   OWND Project は OWND Project Whitepaper によって成立するプロジェクトであり、このホワイトペーパーが公開され、OWND Project の活動自体も公開されることにより、ガバナンスが機能する。

2. Enact

   OWND Project へのコントリビューションに際し、Code of Conduct 等のルールを制定する。Code of Conduct 等のルールは OWND Project の参加者によって制定、公開される。

3. Obey

   参加者は Code of Conduct 等のルールに従って、会議への参加や、コードの開発を行う。ソースコードは当然公開されるが、会議の議事録や技術選定理由等もできる限り公開されることにより、ガバナンスが機能する。

4. Build

   公開されたソースコードからアプリケーションとしてビルドして提供する。OWND Project により承認された開発者がビルドしシステムを提供していることを証明する。

7.3 実現に向けたアクション・ロードマップ

図 7-3-1 に 2024 年 2 月以降において、OWND Project を中心に進めていくロードマップを示す。

図 7-3-1：ロードマップ

8. Trusted Web に関する考察

8.1 求める機能や Trusted Web ホワイトペーパーver.1.0 の原則に関する課題と提言

① 持続可能なエコシステム

(ステークホルダーがそれぞれの責任を分担し、責任を果たすインセンティブがあること)

OWND Project を OSS プロジェクトとして推進することにより、OSS エコシステムとして持続可能な形態となるよう多方面に働きかけを行い、OSS に貢献することがビジネスにおいても利益として還元がなされるようなインセンティブ設計を目指している。

OSS エコシステムとして持続可能であることがビジネス利用へのインセンティブに繋がるが、ビジネス利用へのインセンティブがないと OSS エコシステムとして持続可能にならない、という鶏卵問題をどのように解決するかが課題となる。

② マルチステークホルダーによるガバナンス

(マルチステークホルダーがガバナンスに関与し、ステークホルダーの責任が明確で、問題が発生したときに原因究明ができること)

プロジェクトへの参加のハードルを下げ、複数の団体や市民も含めて議論に参加することでマルチステークホルダーがガバナンスに関与し、コード（およびコード作成者）が公開されていることによる透明性により、信頼性を担保する。また理念や考え方を含めたホワイトペーパーに沿った運用を行うことで、参加者による目指すべき方向性の統一を図る。

マルチステークホルダーによる参加は可能となるが、OSS においてすべてのステークホルダーの責任を明確にするのは難しいことが課題となる。

③ オープンネスと透明性

(アーキテクチャ設計、実装とそのプロセスがオープンであり、透明性が高く相互に検証可能であること)

OSS プロジェクトとして、コード自体の透明性および検討段階における議論や検討資料も公開することで、なぜその技術を用いたかなど誰でも検証を行うことができるように取り組んでいる。

④ データ主体によるコントロール

(データへのアクセスのコントロールは、データ主体（個人・法人）に帰属すること)

OWND Project ではデータ主体によるコントロールを主眼に置いており、特定の事業者に依存するような方法ではなく、利用者自身が自分のデータを保持し、コントロールできるようなアーキテクチャとしている。

将来的にユースケース等が広がってくると、すべてのデータをデータ主体でコントロールすることが難しくなることは容易に想像できるため、データ主体によるコントロールを保証する代理人のような存在をどのように定義するかが課題となる。

⑤ ユニバーサル性

(誰も排除せず、弱い立場にある人を取り残さないこと。誰でも自由に参加できること)

誰でも参加できるOSSプロジェクトとして推進していくことで、弱い立場にある人に向けた機能改善や追加（例えばアクセスビリティ観点でのUIの改善等）を行えるようにする。

技術的な制約により対応しているスマホやPCを持っていない人は排除することになってしまうことは課題となる。

またDIWの利用は新しい体験となるため、使い方を理解してもらうためには現状においてはハードルがあると感じており、それが排除に繋がることが危惧される。

⑥ ユーザ視点

(ロックインフリーでユーザに選択肢があること。ユーザにとって分かりやすく安心して使えること)

国際標準仕様に準拠したプロトコル等を採用し、またライセンスフリーでソースコードを公開することにより、ロックインされることなく、ユーザ（企業含む）が自由に選択できる環境の構築を目指している。

また、分かりやすく安心して利用できるようにソースコードを公開するだけでなく、ビルドしたアプリケーションも運用責任者を明確にした上でエンドユーザに提供する。

上記のユニバーサル性と同じ視点になってしまうが、DIWの利用は新しい体験となるため、分かりやすく説明し、使い方やメリットを理解してもらうことに課題を感じている。

⑦ 継続性

(既存のインターネットアーキテクチャを基礎として、上位に構築することとし、transitionalな形で現行ウェブに付加されること。既存のトラスト手段とのフェデレーショ ンも考慮すること)

既に普及しているOpenIDConnectをベースとした仕様を採用し、トラストチェーンとして既存のサーバ証明書のPKIのエコシステムも取り込むことで、既存のシステムに大きな変更を加えることなく、構築することができるようにしている。

既存のトラストにおける課題を改善しようとすると、transitionalな形がとれない場合が発生したり、既存のトラスト手段とのフェデレーションをするために、トラストチェーンが複雑になってしまったりすることもある。

⑧ 柔軟性

(構成部品が疎結合で構成され、拡張可能なアーキテクチャであること)

特にIdentifierの採用においては、特定のDID等に依存することなく、OSS活用者が自由に選択できるような形態を目指している。

すべての構成部品を疎結合にすることは逆に効率性が失われることもあるため、どの程度の拡張性を持たせるかに課題がある。

⑨ 相互運用性

(技術のみだけでなく、法制度、ガバナンス、組織等の社会システム全体について異なるシステム間で連携可能であること)

OIDC等の国際標準仕様に準拠することで、技術的な相互運用性を担保する。

またガバナンスの一部にサーバ証明書の PKI のエコシステムも取り込むことで、異なるシステム間においてもガバナンスも相互運用可能となる。

法制度の相互運用性には課題がある。特に DIW の法制度で先行している EU の規制に準拠するためには、個人情報保護における十分制認定のような国家間の取り組みが必要となる。

⑩ 更改容易性・拡張性

(特定の技術に依存し過ぎず、中長期での利用を意識して継続的に機能拡張が容易でスケーラブルであること)

OSS プロジェクトとして進め、国際標準仕様に準拠することを目指しており、技術の選定においても特定の技術や VDR、暗号資産等に依存しないような選定を行っている。

現状 DIW の仕様については、仕様が決まっていないものが多いため、それに追従するための開発が機能拡張の容易性に対して悪影響を及ぼす場合もある。

また、特定の技術に依存した方が、機能拡張が容易な場合もある。

8.2 Trusted Web のガバナンスに関する課題と提言

① トラストフレームワークを新規に策定する/既存のルールとアラインする形で策定する上での課題

既に存在するトラストフレームワークが Trusted Web の原則に完全にアラインしているケースはあまり多くないと考えており、特にデータ主体によるコントロール等、既存のトラストフレームワークではあまり重視されていない部分について、準用した場合にはトレードオフが発生することとなる場合はあるのではないか。

また、本実証では、既存 X.509 サーバ証明書のトラストフレームワークを準用し、Issuer の実在性証明として活用を行い、技術的には x.509 署名書を SD-JWT VC の x5c ヘッダーに含めることは可能であったが、実在性のみの証明のため Issuer に必要となる信頼性の指標としては不足するものであった。一方、一定の信頼性の指標として ISMS 認証や P マークなどのトラストフレームワークを利用することが考えられるが、これらはデジタル証明書として発行されていないため、技術的な連携が難しいことが課題である。

② ガバナンスの実効性を担保することや、（例：透明性や継続性、原則との関係性等）ガバナンスに参加するために有効な取り組み・インセンティブに係る示唆（各業界や行政などがどのように関与するか等）

ガバナンスの実効性を担保し、参加するためのインセンティブを確保するためには、ビジネスの推進においてどのようなメリットがあるかを示していくことが有効であると考えられる。例えば ISMS においては、政府調達や大企業との取引の際に取得が求められることが多いため、特に日本において取得する事業者などが多い状況となっている。

また、政府が推進するイニシアティブとして一定の成果を挙げているものでは、スマートフォンプライバシーイニシアティブ（SPI）[18]が挙げられる。2012 年に公表したものであるが、その後 iOS アプリや Android アプリに求められるプライバシーポリシーの公表について、企業から参照されるものとして活用が行われ、主にはプラットフォーマー（AppStore 等）によるルール変更へ対応する際の指標となった。また、その後、電気通信事業法として一部ではあるが、イニシアティブで推奨されてきた内容が法的な義務となることで、法的なガバナンスの実効性の担保も行われるようになった。

ただし、特定の事業者に過度に依存しないという Trusted Web の原則に従ったビジネスを構築することは難しいため、SDGs に関連するような取り組み（Ouranos Ecosystem[19] もその一つと考えられる）や Good Lobby Tracker[20]のような取り組みが参考になると考えられる。

Good Lobby Tracker は、企業の政治的責任に関する主要な取り組みを包括的に評価し、その透明性、説明責任、行動可能性を高めることを目的としたイニシアティブであり、企業のロビー活動における透明性指標を提供している。

SPI や Good Lobby Tracker 等のイニシアティブに共通していることとして、各事業者や組織の実際の取り組みを評価し、定期的にレポートとして公表するという活動が行われており、特に Good Lobby Tracker については、投資判断の指標として採用されることにより、経済的なメリットに直結するように設計されている。

③ Issuer/Holder/Verifier 等の各主体にガバナンスをかける上での課題

それぞれのステークホルダーにガバナンスをかける上で、各ステークホルダーには一定の基準を満たすようなルールを策定する必要がある。その基準を満たすメリットがコストを上回るように設計しなければ、エコシステムとして機能しないと考えられる。例えば情報銀行の認定において、情報銀行の運営者、データ提供先やデータ提供元にガバナンスをかけるために様々なルールが設定されたが、情報銀行の運営をするメリット、データ提供先になるメリット、データ提供元になるメリットを明確にできておらず、情報銀行のエコシステムに参加するコストが上回っている状態が続いている。

例えば、通常の銀行のように、特定の業務を行うためには、当局による免許が必要となり、かつそのエコシステムに参加することで多くのステークホルダーに（金銭的な）メリットがあるというようなエコシステムを設計する必要がある。

④ トラストフレームワークを作成する上で必要な構成要素や、策定プロセスにおける課題・提言

そもそも Trusted Web 推進協議会におけるトラストがどのように担保されているかが明確ではないことは課題と感じているため、まずはこれを明確にしてほしい。

---

[18] スマートフォン プライバシー イニシアティブ（SPI）：https：//www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/smartphone_privacy.html

[19] Ouranos Ecosystem ：https：//www.meti.go.jp/policy/mono_info_service/digital_architecture/ouranos.html

[20] Good Lobby Tracker ：https：//www.thegoodlobby.eu/initiatives/tracker/

V3.0 では「官民コンソーシアムの組成なども今後の検討課題となってくる」としているが、現在進めているプロジェクトにおいて、どのように Trusted Web とのトラストチェーンが繋がるかを明確にすることが難しい。

8.3 Trusted Web のアーキテクチャに関する課題と提言

課題：アーキテクチャの実装が複雑で、高度な技術知識を要求される。また、実装に必要な技術は開発途上のものが多く、頻繁に仕様が変更されてしまう。

提言：X.509 などの具体的な使用例と同様に、Verifiable Identity、Verifiable Data、Verifiable Messaging に具体的な技術を交えたユースケースを追加してもよいのではないか。

課題：Verifiable Identity の互換性が不足しているため、アプリケーション、システム、プラットフォーム間でのインターオペラビリティが確保できていない。

提言：EUDIW や OWF と互換性のある Trusted Web における Verifiable Identity、Verifiable Data、Verifiable Messaging の仕様の策定が必要ではないか。

課題：Verifiable Identity コミュニティの範囲が不明瞭であるため、ガバナンスモデルの設計が困難である。

提言：Verifiable Identity は異なる背景を持つ多様なステークホルダー（個人、企業、非営利団体、政府機関など）から構成されるため、規模に応じたガバナンスモデルのユースケースの提示が必要ではないか。

8.4 その他 Trusted Web に関する課題と提言

アーキテクチャ・ガバナンス以外に関する Trusted Web の課題・提言は、現時点では特にないが、引き続き OWND Project 等の活動の中で議論を進める。

Appendix

用語集

本事業について正しく理解する上で必要な用語は表 9-1-1 の通りである。

表 9-1-1：用語一覧

用語	定義
エンティティ	実体として認識できるものの総称。例えば、自然人、法人、製品、サービスなどをエンティティと現すことが多い。
アイデンティティ	エンティティに関する属性情報の集合。（ISO/IEC 24765-1）
デジタルアイデンティティ	デジタル空間上のアイデンティティ。
属性情報	氏名、生年月日、住所などのアイデンティティを構成する情報。
デジタルアイデンティティウォレット （DIW）	デジタルアイデンティティを安全に保存、管理、共有するためのツールやアプリケーション。本書では単純にウォレットと表記する場合もある。
オンラインコミュニケーション	オンラインにおける属性情報やメッセージのやり取りのこと。
メッセージングサービス	メッセージやその他の情報のやり取りができるツールやアプリケーション。
メッセージングプロトコル	メッセージングサービスの基盤技術となるプロトコル。
アクター	ユースケースにおけるエンティティ。本書でのユースケースとしてはウォレットを扱うエンドユーザ （Holder）、証明書を発行する Issuer、証明書を検証する Verifier を想定している。
証明書	然るべき発行機関からエンティティへ発行されたアイデンティティの一部または全部を証明するもの。本書では電子署名技術を用いて証明可能なデジタル証明書の意味で用いる。
証明書署名要求 （CSR：Certificate Signing Request）	証明書への署名を要求するためのドキュメント。
キーペア（鍵ペア）	電子署名に用いられる秘密鍵（署名鍵）、公開鍵（検証鍵）のペア。
選択的属性開示	属性情報の一部もしくは属性情報から導き出される情報のみを選択的に提示でき、かつ前記の情報のみでも検証可能となる仕組み。
Decentralized Identifiers（DID）	分散的に管理されたグローバルに一意な識別子。
Verifiable Credentials （VC）	改ざん検出が容易なクレデンシャルであり、誰が発行したかを暗号学的に検証できるもの。
Selective Disclosure for JWTs （SD-JWT）	選択的属性開示を JSON Web Token（JWT）をベース技術として実現する標準仕様。
OpenID for Verifiable Credential Issuance （OID4VCI）	Issuer から Holder に証明書を発行する標準仕様。

OpenID for Verifiable Presentations （OID4VP）	Holder から Verifier に証明書を提示する標準仕様。
Self-Issued OpenID Provider v2（SIOPv2）	エンドユーザ （Holder） 自身が OpenID Provider （OP） となり認証連携を行う標準仕様。
階層型決定性 （HD：Hierarchical Deterministic） ウォレット	1 つのシードからマスターキーとなる秘密鍵を生成し、そこから木構造のように階層的に複数の派生秘密鍵と派生公開鍵（アドレス）を生成する鍵管理方法をとるウォレット。
Matrix	オープンソースの分散型メッセージングプロトコル。
Synapse	Matrix ホームサーバのオープンソースソフトウェア。
Element	Matrix クライアントのオープンソースソフトウェア。

本実証で開発したシステムの第三者による再現可能性

本実証事業で利用する技術の選定および、利用技術の決定理由は以下のスプレッドシートで公開している。第三者が選定理由を確認でき、今後の相互利用に向けた技術選定の参考とにできる [21]。また、基本設計で作成したユースケースおよびシーケンスも公開している [22]。

本実証事業で開発したプロトタイプシステムはすべてオープンソースソフトウェアとして GitHub に公開している [23]。具体的には、4.4.7 で示したコンポーネントを取得可能であり、第三者が利用することでシステムの再現が可能である。また、プロトタイプシステムのウォレットアプリ、メッセージングサービスは Google play、App store、ウェブアプリとして公開しており、OWND Project のウェブサイトから入手可能である [24]。

本実証で開発したプロトタイプシステムは、xID アプリと連携することでマイナンバーカード情報を取得している。xID アプリは xID 社の規約に従い利用可能である。

ヒアリング詳細・結果

実証期間中に証明書発行機関、サービス事業者、有識者へ実施したヒアリング結果について以下の通り記載する。

証明書発行機関 A 社

【論点】

---

[21] 利用技術選定
https : //docs.google.com/spreadsheets/d/1slgnsy94R3Ku3SEJPddlYciZ1bIDZcU2sHR8cSuSP-4/edit?usp=sharing

[22] ユースケース設計書
https : //drive.google.com/file/d/1p-DWLv6Jke5osqD2dlKrt94PDyNJ8oKv/view?usp=drive_link

[23] OWND Project （Github）
https : //github.com/OWND-Project/

[24] OWND Project
https : //www.ownd-project.com/

- 本ユースケースで採用する技術への期待感および技術採用時の影響をどう考えるか。

【ヒアリング項目】

- 利用を検討している OpenID4VCI, VP、SD-JWT 等を採用することは妥当か。
- これまで IdP を運用している中で、VC のモデルに変わったときにユーザのログイン情報などの行動を観測できなくなる点はどうか。

【回答】

- 選定技術は妥当という意見をいただいたが、普及している IDaaS や OSS が対応していることが重要という回答を得た。
- 相互運用性も重視しているという回答を得た。
- ログイン情報を観測できないというところはビジネス面ではマイナスだが、発行者も証明書利用数などの検証が必要なので、統計化された利用状況でも分かるとよいという意見を得た。
- 紙の証明書発行や中央集権的な仕組みはコストがかかるので、VC モデルはコスト削減も期待できるという意見も得た。

証明書発行機関 B 社

【論点】

- 本ユースケースで採用する技術への期待感および技術採用時の影響をどう考えるか。

【ヒアリング項目】

- 利用を検討している OpenID4VCI, VP、SD-JWT 等を採用することは妥当か。
- これまで IdP を運用している中で、VC のモデルに変わったときにユーザのログイン情報などの行動を観測できなくなる点はどうか。

【回答】

- 選定技術は妥当という意見をいただいたが、相互運用性があるとコモディティ化が進み、ビジネスが狭くなるという意見を得た。
- 自己主権の観点で欧州を中心に既存の IdP のモデルは許されなくなってきているため、合わせていく他ないという意見を得た。

サービス事業者 C 社

【論点】

- サービス事業者が生活者の会員登録を受ける際にどのような課題があるか。

【ヒアリング項目】

- サービス事業者として検証された属性提供があるとどのようなメリットがあるか。

【回答】

- 匿名であってもアルコール飲料や成人向けゲームなどの広告を検証された年齢属性のオーディエンスに配信できるメリットはあるという意見を得た。
- 既存のソーシャルログインと比べ、ウォレットの方が取得できるデータは少ないかもしれないが、幅広くその人の活動に関する属性を取得できる可能性があるという意見を得た。

サービス事業者 D 社

【論点】

- サービス事業者が生活者の会員登録を受ける際にどのような課題があるか。

【ヒアリング項目】

- サービス事業者として検証された属性提供があるとどのようなメリットがあるか。

【回答】

- 対面契約を基本としているサービスだと、VC モデルの利点を活かしきれないという意見をいただいた。問い合わせ、見積もりはオンラインであっても、契約は対面というサービスはまだまだ多く、契約が対面であるため、問い合わせ時に虚偽の情報を送信されるリスクは少ないという意見を得た。
- 個人情報の利用目的への再同意、新たな個人情報の取得など、契約後の継続的な確認のための方が、VC モデルを活かせるのではないかという意見を得た。

サービス事業者 E 社

【論点】

- 本ユースケースを実現した際にどれくらいの費用を払ってもよいか。

【ヒアリング項目】

- サービス事業者として検証された属性提供があるとどのようなメリットがあるか。

【回答】

- 実証実験のような仕組みを使うことで、人的コストが削減されるのであれば、それに見合う費用を払う価値はあるという回答を得た。
- イベントがない平日の夜など、閑散としている時にどれだけ集客効果を期待できるかというところがポイントという回答を得た。

有識者 X,Y,Z 氏

- ウォレットについて
    - ウォレットに関しては将来的に必要になるものだと感じたし、未来の UX はこのようになるんだということを実感できた。
    - **OV 証明書ではなく、法務省発行の証明書を用いることができるとよい。**

    - eIDAS2 のように、法務省発行の証明書への対応をブラウザに義務付ける方向性がよいのではないか。
    - SNS 等において、自分の年代や性別だけを公表して意見表明を行うようなユースケースに使えそう。
    - 有名人などが、自分自身の発信であること（なりすましではないこと）を示すために利用することもできそう。
    - 簡単に自分の属性を証明できるようになることで、逆になりすましが増えてしまいそうな印象を持った。
- メッセンジャーについて
    - Matrix というプロトコルは知らなかったが、鍵の交換や E2E 暗号化が不得意としているグループメッセージの仕組みが気になった。
    - ロシア人はほぼ Telegram を利用している。
    - **普及させるには、既存メッセージングサービスとの相互運用性が重要**ではないか。
    - **LINE のオープンチャットのように、匿名のままグループを作る際に、自分の属性を選択的に開示できることで、事故が減るのではないかと思われる。**
- ガバナンスについて
    - OSS プロジェクトをどう信頼するかについて、ソースコードが公開されていることは前提としてあるが、自分自身でソースコードをすべて確認するようなことはしていない。
    - 信頼に対する明確な指標はなく、みんな使ってそうとか、コミットが多いとか、複合的に判断して利用している。
    - **誰が（どんな人が）推進しているか、開発しているかが重要だが、既存の OSS ではあまり可視化されていないのは課題である。**
    - Ruby のまつもとゆきひろさんは宣教師として活動した経緯もあり、Ruby が世界的に利用される際に信頼を判断する基準となったのではないか。
    - Linux が普及した経緯として、linus torvalds という人物に対する信頼が厚かったことが普及に繋がった。
- 社会実装に向けて
    - **まずは、政府発行のマイナンバーカードや保険証、運転免許証などについての VC 化をデジタル庁が推進し、ウォレットを認可制にするべき。**
    - **法人番号検索サイトや登記情報提供サービスで法人の公開鍵がダウンロードできるようになるとよい。**