令和4年度補正Trusted Web 開発等推進事業に係る調査研究
Trusted Web ユースケース実証事業
最終報告書 概要版

「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」

株式会社DataSign

2024年3月15日

目次

1．背景・目的

2．事業の概要

2.1．登場する主体と概要

2.2．現状の課題を解決する事業スキーム案

2.3．社会・経済に与える影響・価値

2.4．ペイン・ゲインの整理

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

3.2．本事業におけるスコープ

3.3．実施事項・成果物一覧

3.4．実施スケジュール

4．実証（企画・プロトタイプ開発）

4.1．実施概要

4.2．Verifyできる領域を拡大する仕組み

4.3．合意形成・トレースの仕組み

4.4．企画・開発物

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

5.2．実証検証結果

6．調査検証

6.1．実施概要

6.2．調査検証結果

7．実証終了後の社会実装に向けた実現案

7.1．残課題への対応方針

7.2．将来的なユースケース実現モデル

7.3．実現に向けたアクション・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

8.2．Trusted Web のガバナンスに関する課題と提言

8.3．Trusted Web のアーキテクチャに関する課題と提言

8.4．その他Trusted Web の課題と提言

1. 背景･目的

1. 背景・目的

背景

- UI/UXに優れた汎用的なデジタルアイデンティティウォレットがないという課題
  - European Digital Identity Wallet（EUDIW）やOpen Wallet Foundation（OWF）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ウォレットがない
  - プライバシーに配慮して選択的属性開示が可能なウォレットがない
- 現状のコミュニケーションに対する課題
  - 個人における課題
    - プラットフォーマーへの依存度が高く、メッセージの暗号化や相手先の検証についてはプラットフォーマーを信じるしかない
    - プラットフォーマーの管理するアイデンティティやメールアドレス、電話番号を用いた認証が多く、これらの情報が広告の識別子として第三者と共有されるリスクがある
  - 法人における課題
    - メールではEnd to End暗号化できないことによりPPAPと呼ばれる煩雑なやり取りでファイルの送受信が行われている
    - 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

1. 背景・目的

目的

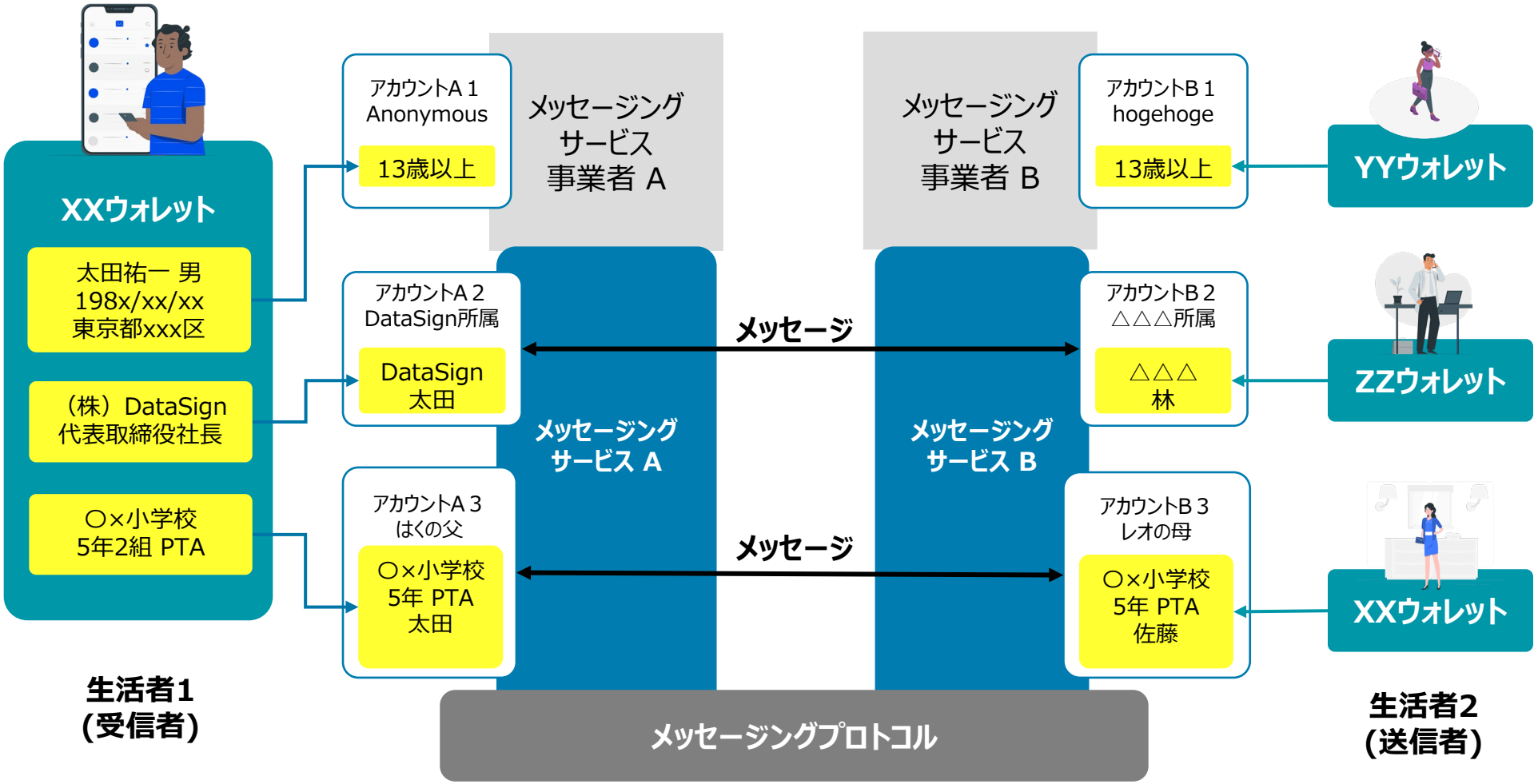
- ユーザ自身が自らのアイデンティティを管理し、属性情報を他者と相互検証できるようにした上で、特定のサービスに依存しないよう、相互運用性を確保したデータのやり取りや安全なメッセージングを行うことができるようにすることで、オンラインコミュニケーションのTrustおよびUI/UXを向上させることを目指す。

- European Digital Identity Wallet（EUDIW）やOpen Wallet Foundation（OWF）で採用が予定されている国際標準技術を用いて開発を行い、成果物はオープンソースソフトウェアとして公開することで、コミュニティの構築を目指す。

- 公開されたソースコードを誰でも利用できるようにすることで、さまざまなユースケースやビジネスモデルが創出され、よりトラストできるオンラインコミュニケーションが普及することでTrusted Webの社会実装を目指す。

2. 事業の概要

2.1. 登場する主体と概要



2.1. 登場する主体と概要

ユースケース	主体	役割	課題
サービスへの会員登録	生活者	• サービス事業者のサービスへ会員登録を行う	• IDプロバイダに依存した情報の登録となる • **必要最小限の情報提供ができない** • サービス事業者の信頼性を確認できない
	サービス事業者	• 生活者にオンラインサービス(メッセージングサービス)を提供する事業者	• 自信が信頼できる事業者であることを生活者に証明できない • **生活者の登録情報の信頼性を検証できない**
メッセージのやり取り	生活者1 (受信者)	• メッセージングサービスの利用者で生活者2からメッセージを受け取る	• **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2かどうか検証できない** • 特定の事業者に依存せずに安全に通信できない
	生活者2 (送信者)	• メッセージングサービスの利用者で生活者1へメッセージを送る	• 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かどうか検証できない • **特定の事業者に依存せずに安全に通信できない**

2.2. 現状の課題を解決する事業スキーム案

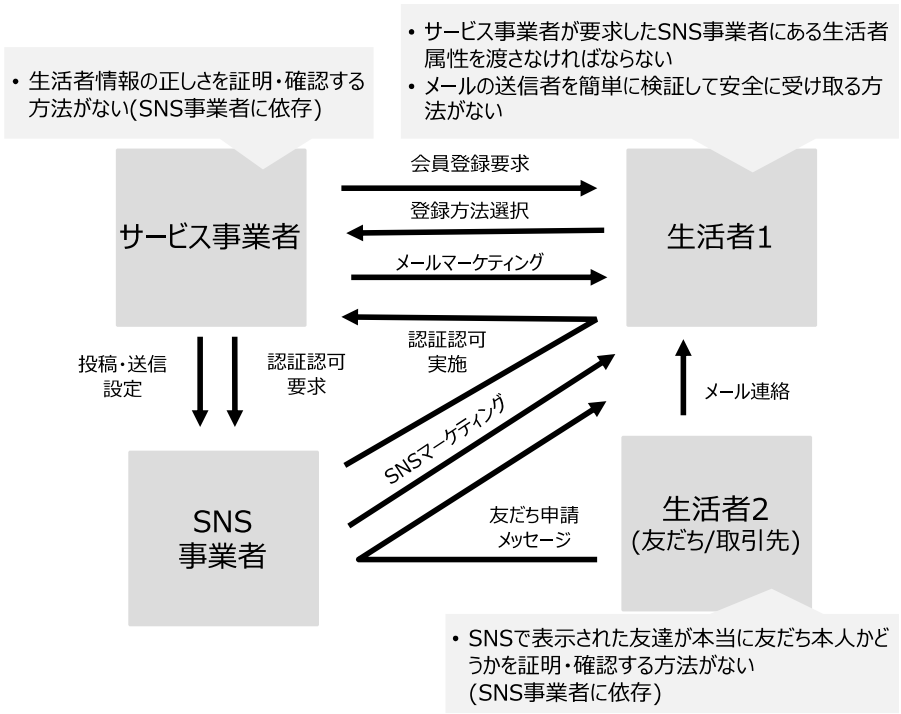
現在の課題（ペインポイント）

- 生活者1はSNS事業者のログイン機能を使うと便利だが、よく知らないサービス事業者にSNS事業者が管理する属性情報を渡したくない
- 生活者1は特定のSNSを用いてメッセージを送ろうとすると、生活者2(友だちや取引先)もその特定のSNSを利用していないとメッセージが送信できない。メールは送信者の検証ができず安全ではない
- サービス事業者は利用者の属性の確認・検証を行いたいが、本人確認はコストが高く、利用者のUXを阻害してしまう
- サービス事業者は生活者に簡便な会員登録方法を提供したいが、複数のSNSに対応すると、逆にUXを阻害してしまう

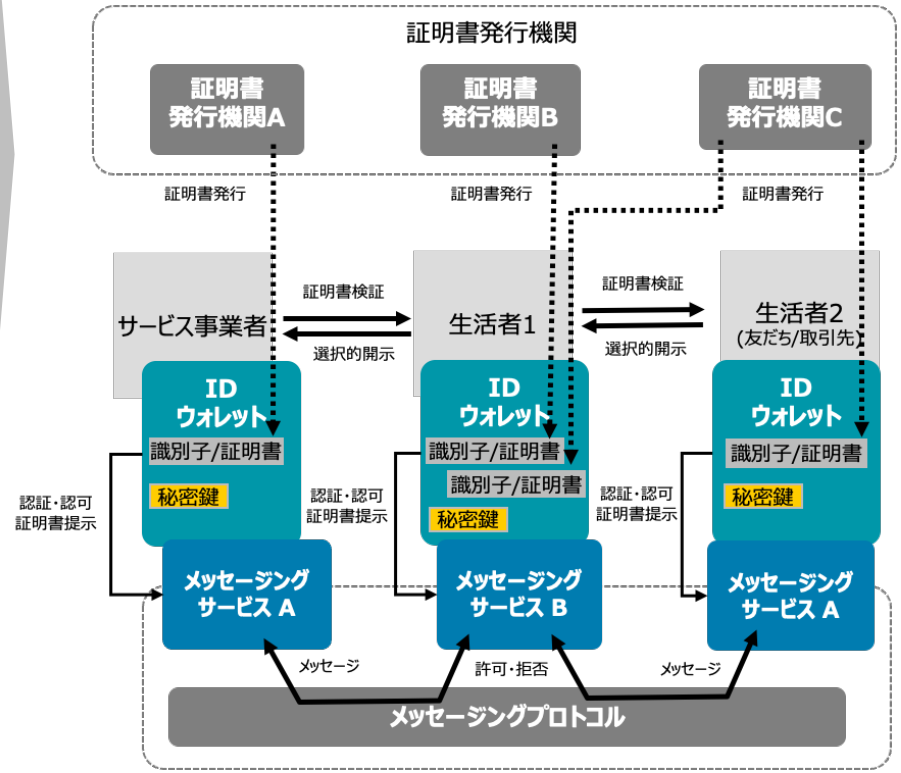
Trusted Webの実現により解決する内容

- 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

課題解決前の事業スキーム図（As-Is）



創出するユースケースの事業スキーム図（To-Be）



2.3. 社会・経済に与える影響・価値(1/2)
社会への影響・価値について

**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**

本実証で実施する内容

- 国際標準やデファクトスタンダート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
- 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の開発
- アイデンティティウォレットをベースとしたさまざま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
- 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

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、さまざま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さまざまなプレイヤーが使いやすい環境となる。

2.3. 社会・経済に与える影響・価値(2/2)
経済への影響・価値について

- 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[1]
  - 2030年ごろまでに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サービスにおける一人当たりの売上はおよそ月額200円～1000円程度である[2]
  - これはヒアリング[3]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Trusted Webに移行すると仮定すると、46億人[4]×10%×1000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3500億円が見込まれる） [5]

日本における市場規模予想

	2024年	2025年	2026年	2027年	2028年
市場普及率(%)	2%	4%	6%	8%	10%
市場規模(億円)	700	1400	2100	2800	3500

[1] statista, https://www.statista.com/topics/2498/programmatic-advertising/#topicOverview
[2] DATAREPORTAL, https://datareportal.com/reports/digital-2022-global-overview-report
[3] DataSignによる事前の生活者ヒアリング（詳細は最終報告書をご参照ください）
[4] 総務省, https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/nd247100.html
[5] 内閣府, https://www.esri.cao.go.jp/jp/sna/data/data_list/kakuhou/files/2020/sankou/pdf/kokusaihikaku_20211224.pdf

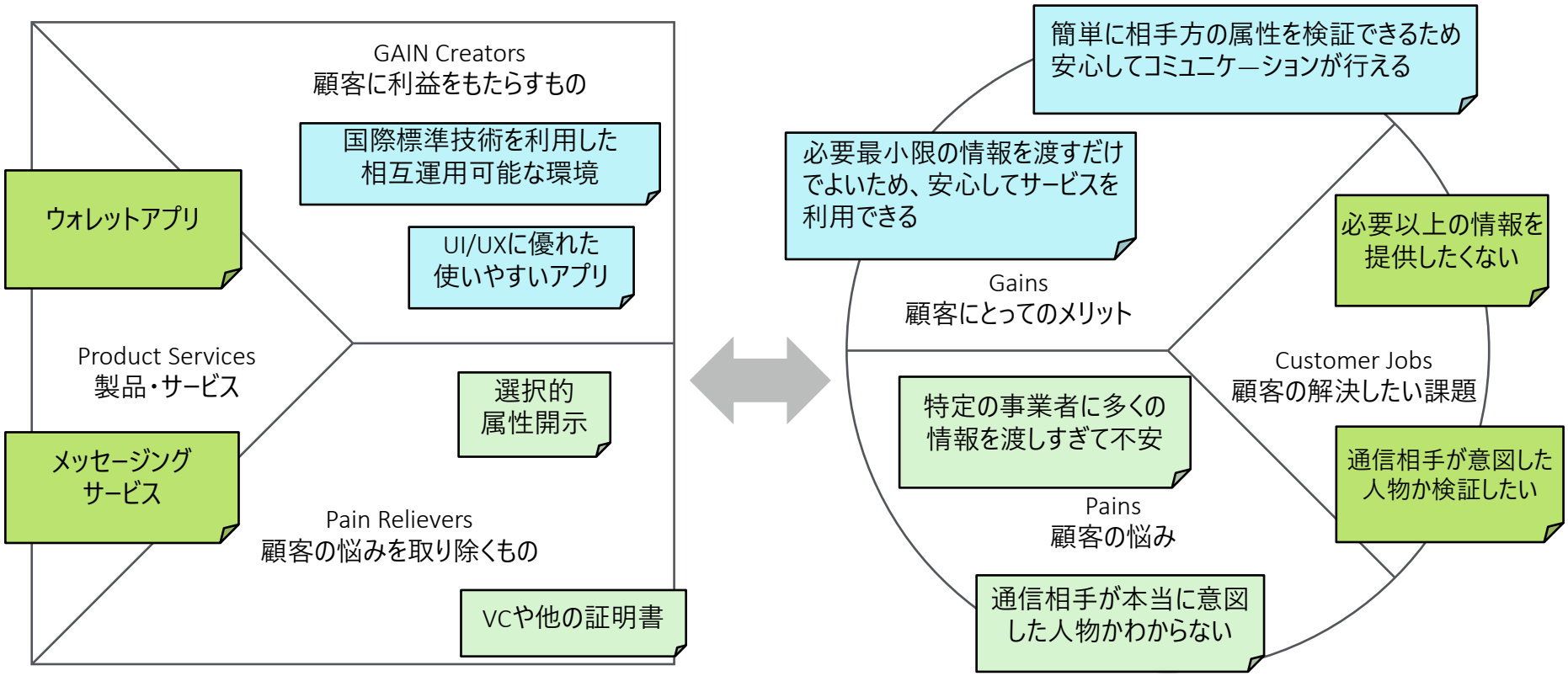
2.4. ペイン･ゲインの整理 （Value Proposition Canvas)

Value Proposition
企業が顧客に提供できる価値

- 自らアイデンティティを管理でき、サービス事業者や他の生活者を検証しつつ、必要最小限の情報を選択的に開示し、特定の事業者へ依存せずに安全なコミュニケーションを実現する

Customer’s Segment
顧客セグメント

- 通信相手を検証しつつ特定の事業者に依存せずに情報のやり取りを行いたいビジネスパーソン



3. 本実証事業における検証計画

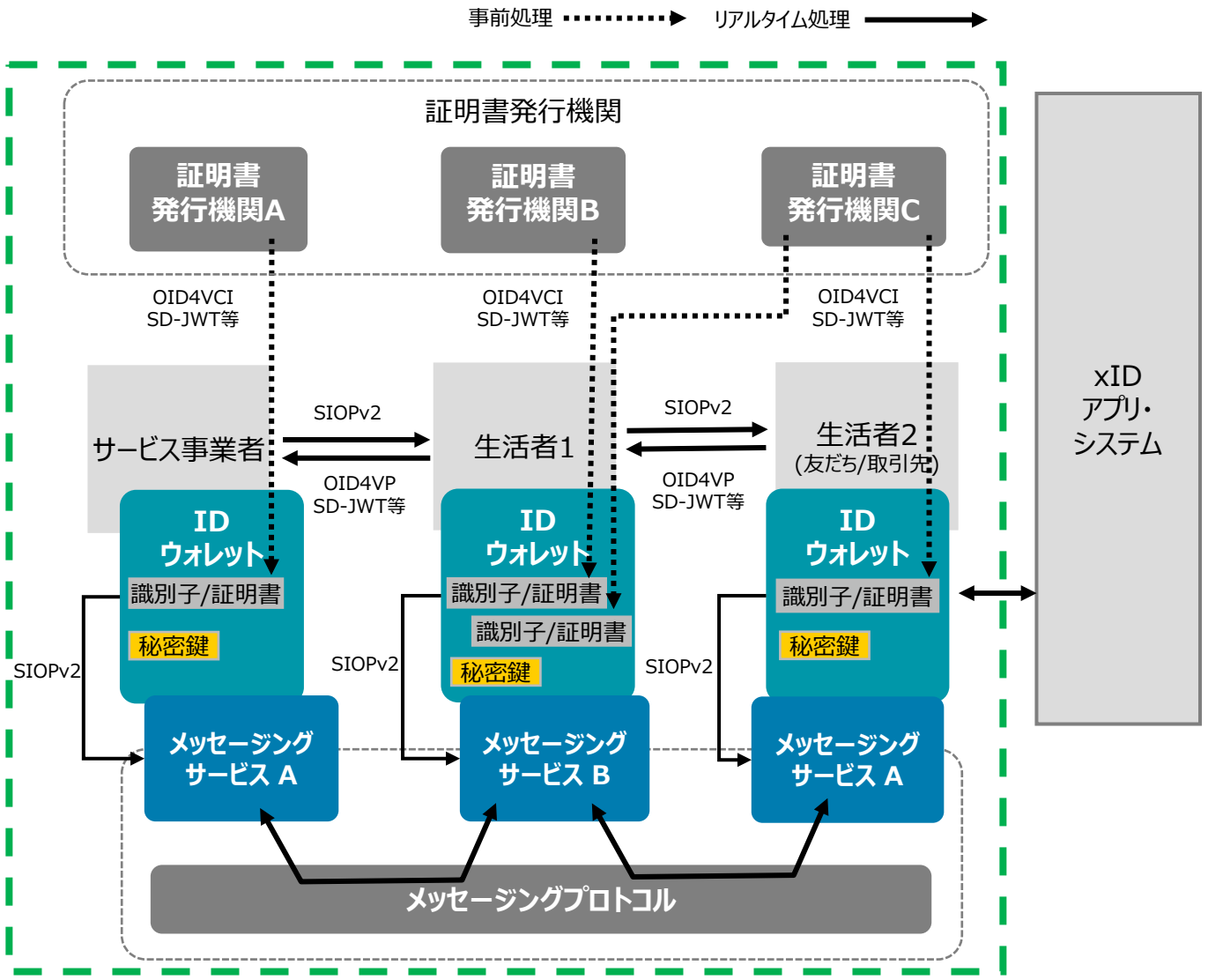
3.1. 実証事業で明らかにする論点への導出・経緯 (1/2)

観点	明らかにする論点		論点設定の背景	論点解決に向けた検証概要
ビジネスモデル	1	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	• 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の不在	• 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 • 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
UI/UX	1	システムの全体でどのようなUXを実現すべきか	• 使いやすいウォレットアプリが不在 • 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	• 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
機能と業務の適合性	1	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	• 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	• DIDやVCのみでなくその他の技術利用 （X.509証明書等） も広く検討する • 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 • 秘密鍵のバックアップ・復元方法の検証を行う

3.1. 実証事業で明らかにする論点への導出・経緯 (2/2)

観点	明らかにする論点		論点設定の背景	論点解決に向けた検証概要
機能と業務の適合性	2	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	• 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の整理の不在	• 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 • ウォレットアプリを利用したVCの検証のみでなく、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 • 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
非機能要件	1	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	• 属性情報の一部のみを開示できない • Unlinkableな仕組みの不在 • 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	• 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
必要な規制・ガイドライン対応	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	• 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の整理の不在 • 証明書発行におけるガバナンスやルールの整理の不在	• 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 • 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 • 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 • 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 • 本人確認については現状ではX.509証明書を発行しているが、選択的開示の概念等を鑑み、その方法やプロトコルはxID社と協議を行い、実施方法を検討する

3.2. 本事業におけるスコープ



本実証では、属性情報のやり取りのプロトコルとして、下記3技術に対応することを想定している。

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。

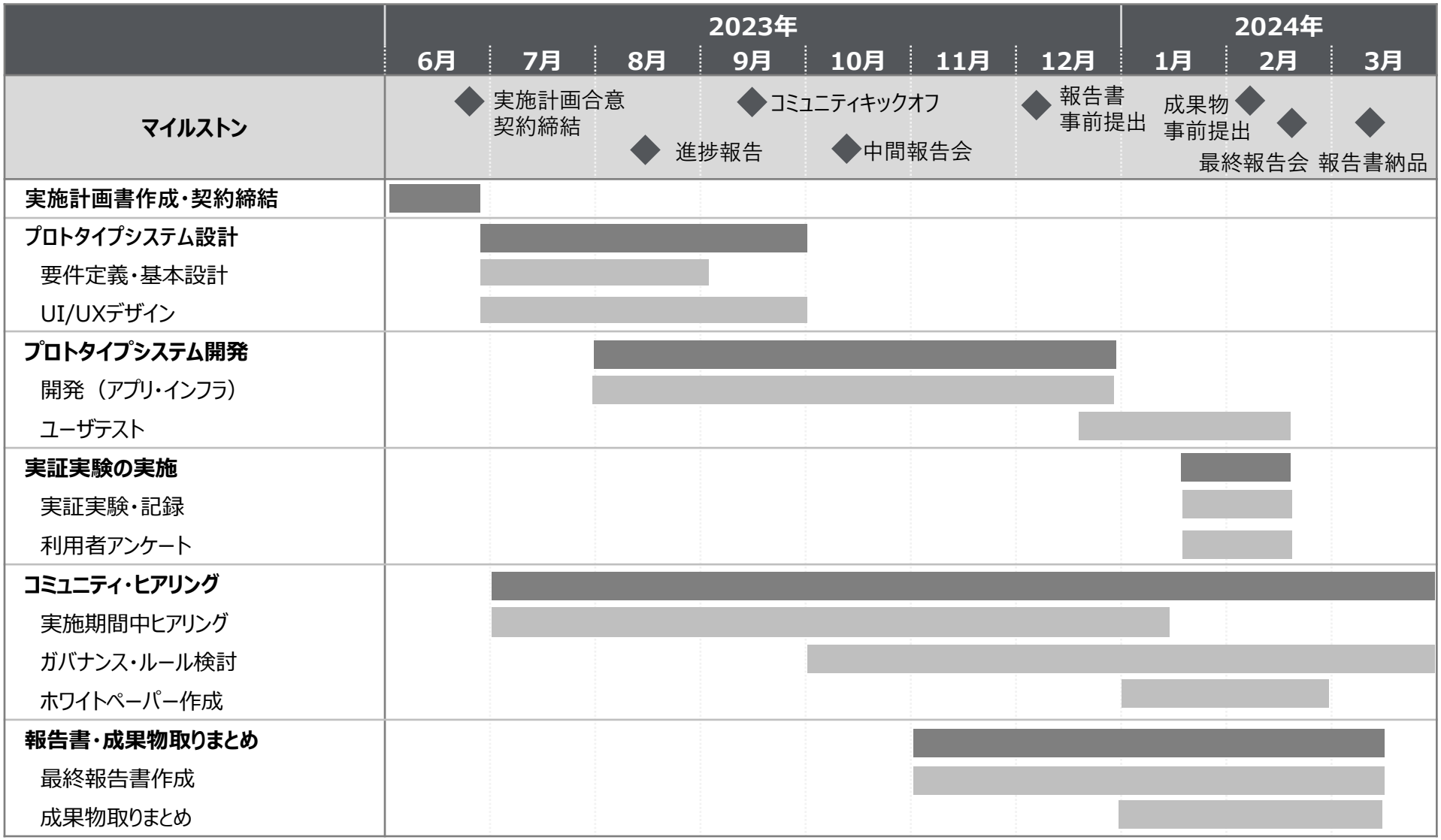
- OpenID for Verifiable Credential Issuance
  （以降、OID4VCI）
- OpenID for Verifiable Presentations
  （以降、OID4VP）
- Self-Issued OpenID Provider v2
  （以降、SIOPv2）

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。

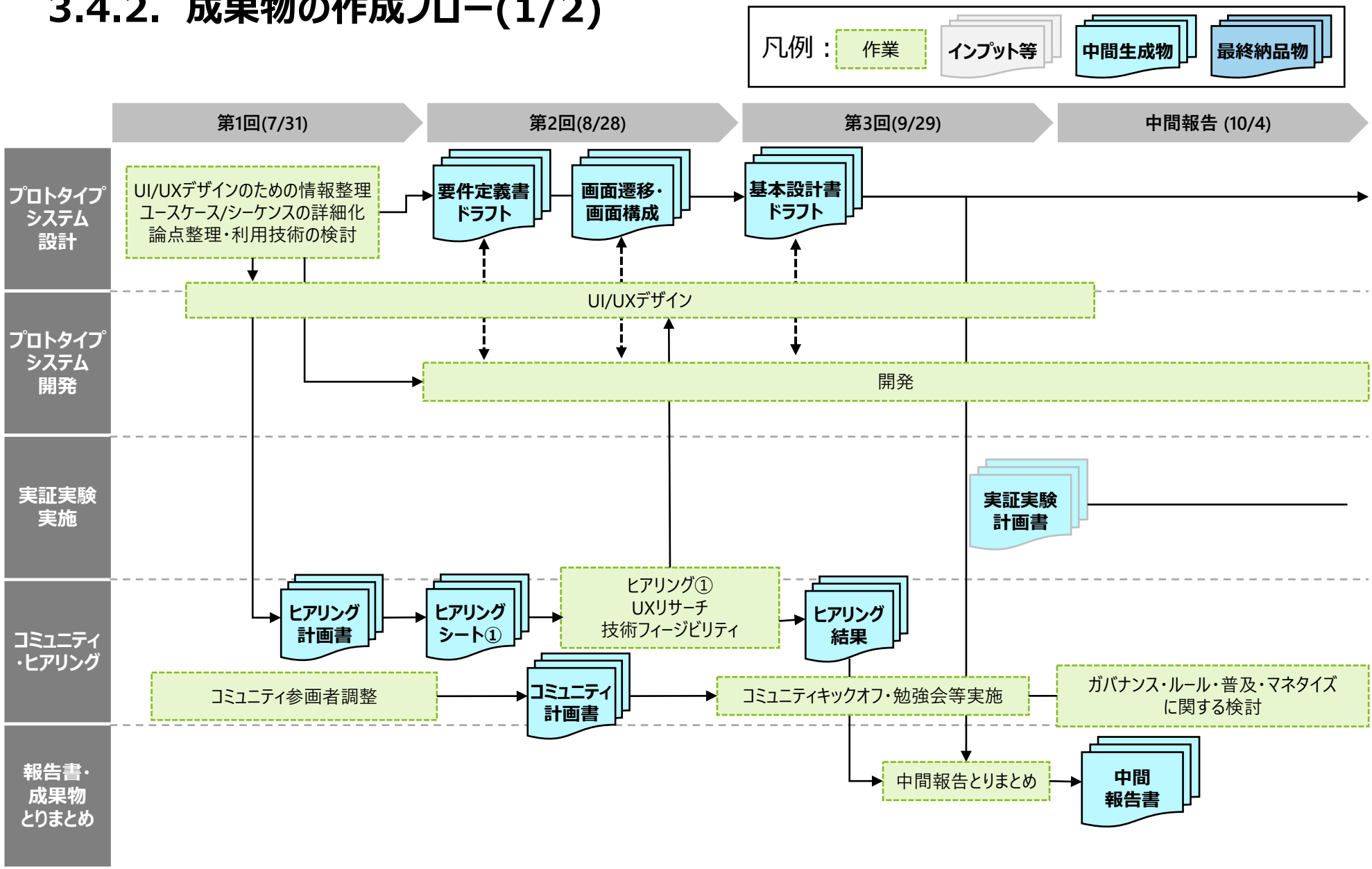
3.3. 実施事項・成果物一覧

実施項目		具体的な作業内容	担当(会社名)	想定成果物
本システムの設計	要件定義・基本設計	• ユースケースをもとに要件定義を実施 • 上記要件やUI/UXデザインをもとに基本設計を実施	• DataSign/xID/有識者/デザイン事務所	• 要件定義/基本設計書（ユースケース定義書）
	UI/UXデザイン	• 上記要件や実施期間中ヒアリングをもとにUI/UXデザインを実施	• DataSign/デザイン事務所	• 画面遷移 • 画面構成
本システムの実装	開発（アプリ・インフラ）	• 要件定義・基本設計をもとに開発	• DataSign/xID	• ソースコード • 実行ファイル
	ユーザテスト	• プロトタイプアプリを公開し、ユーザテストを実施	• DataSign	• テスト結果
実証実験の実施	実証実験・記録	• 本ユースケースについてサービス事業者、生活者の協力の元実証実験を実施	• DataSign	• 実証実験結果
	利用者アンケート	• 実証実験参加者に対してアンケートを実施	• DataSign	• アンケート
コミュニティ形成・ヒアリングの実施	実施期間中ヒアリング	• ユースケースにおけるUXリサーチの観点でヒアリングを実施	• DataSign/デザイン事務所	• 調査結果
	ルール・ガバナンス机上検討	• コミュニティにおいて、有識者へのヒアリングを元にルール・ガバナンスを検討し、ホワイトペーパーを作成	• DataSign/コミュニティ	• ガバナンスに対するホワイトペーパー
報告書・成果物取りまとめ	最終報告書作成	• 報告書内容の取りまとめと執筆	• DataSign	• 最終報告書
	成果物取りまとめ	• 開発アプリや納品物の取りまとめ	• DataSign	• 納品物一式

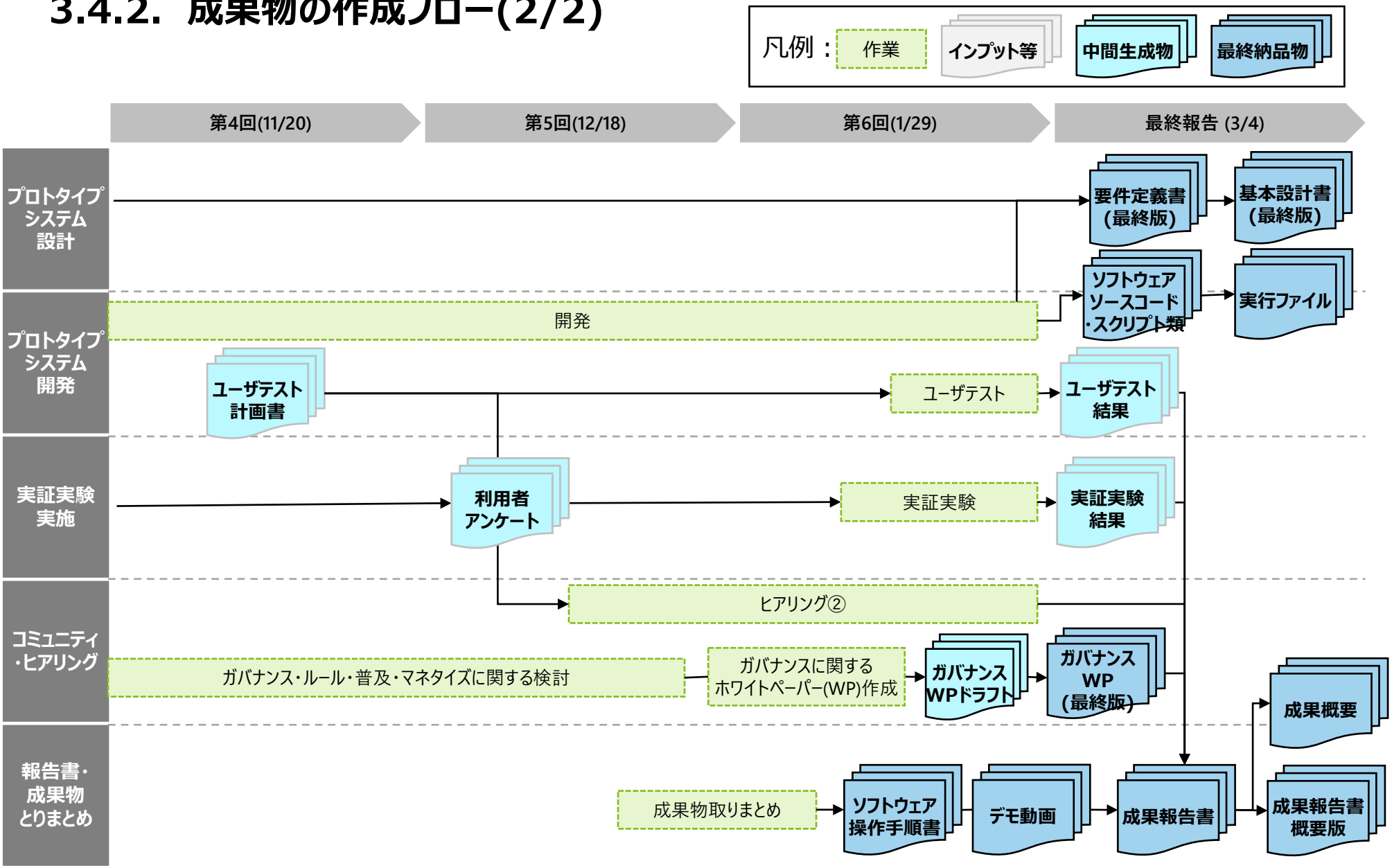
3.4. スケジュール
3.4.1. 全体スケジュール



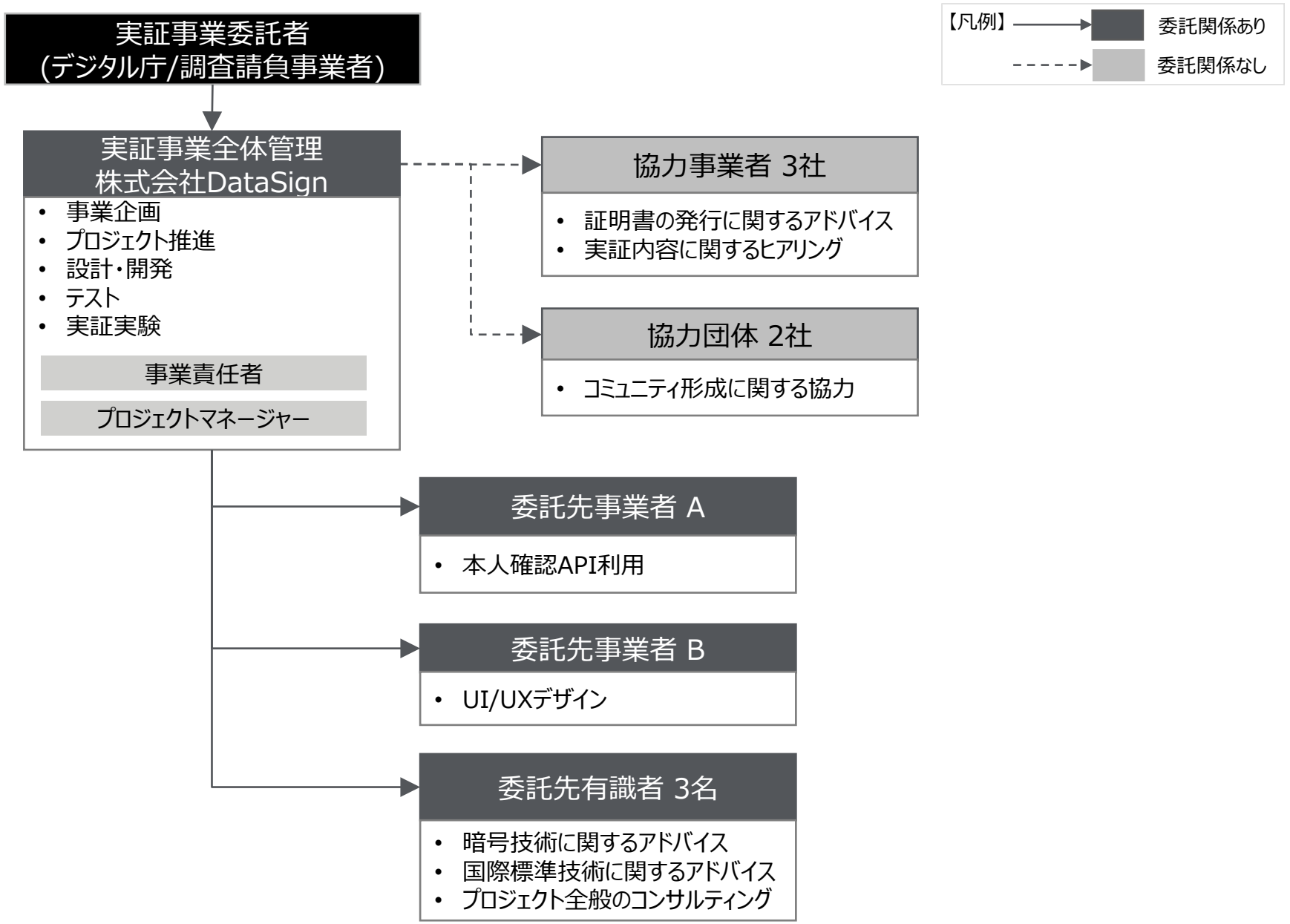
3.4. スケジュール
3.4.2. 成果物の作成フロー(1/2)



3.4. スケジュール
3.4.2. 成果物の作成フロー(2/2)



3.5. 実施体制


【凡例】
委託関係あり
委託関係なし
実証事業委託者
(デジタル庁/調査請負事業者)
実証事業全体管理
株式会社DataSign
• 事業企画
• プロジェクト推進
• 設計・開発
• テスト
• 実証実験
事業責任者
プロジェクトマネージャー
協力事業者 3社
• 証明書の発行に関するアドバイス
• 実証内容に関するヒアリング
協力団体 2社
• コミュニティ形成に関する協力
委託先事業者 A
• 本人確認API利用
委託先事業者 B
• UI/UXデザイン
委託先有識者 3名
• 暗号技術に関するアドバイス
• 国際標準技術に関するアドバイス
• プロジェクト全般のコンサルティング

4. 実証（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

No.	論点	検討結果とその経緯
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	• 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。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メーパーにまとめた。
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	• 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。
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	• 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。 証明書の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。証明書の具体的な形式は、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、技術の普及状況や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。

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

No.	論点	検討結果とその経緯
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	• 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。
5	• システムの全体でどのようなUXを実現すべきか	• 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、わ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。
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	• 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。
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	• WND 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。

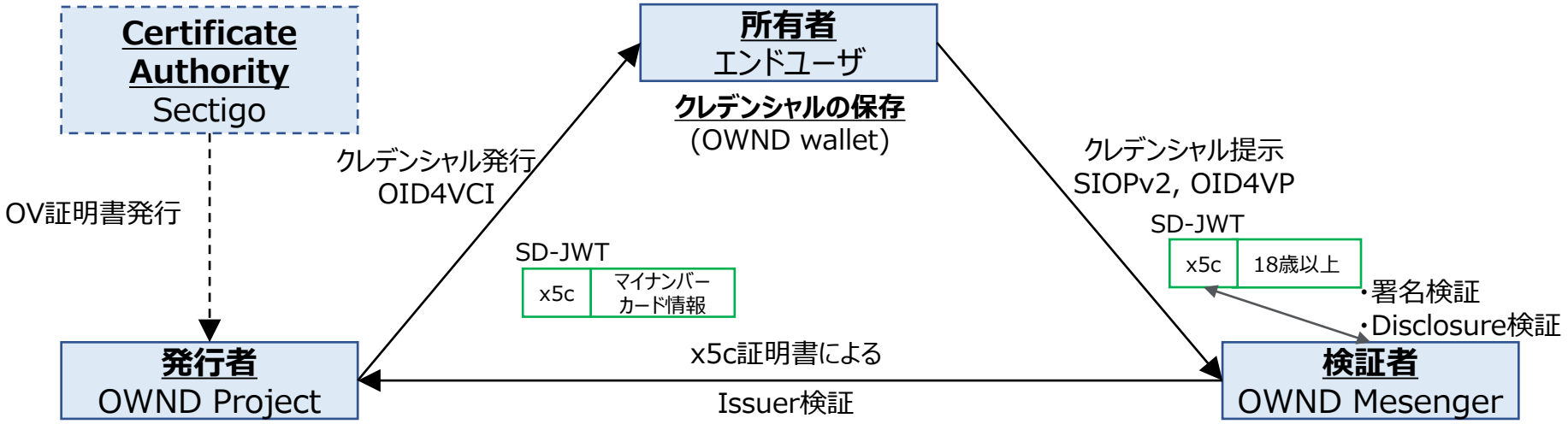
4.1. 実施概要
4.1.2. 企画・プロトタイプ開発に用いる技術・標準等を選定した理由及び背景

No.	活用技術・規格	実現したい要件	選定理由とその経緯
1	• OID4VCI • OID4VP • SIOPv2	• 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	• 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。
2	• JWK Thumbprint	• Holderの識別子としてペアワイズ可能である • VDRなどの外部依存を避ける	• 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。 • またVDR非依存なため。
2	• SD-JWT	• 選択的開示によりプライバシー・バイ・デザインを実現する	• 実装が比較的容易であり且つ、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。
3	• OV(EV)証明書	• 証明書の発行機関を検証する	• すで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。
4	• Matrix	• 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する	• 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。

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)	• 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	• 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 • また、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)	• 生活者１へのメッセージの送信する者	• 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)	• 生活者１にオンラインサービスを提供する者	• 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）を行ってもらう必要がある
証明書発行機関 (Issuer)	• 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	• 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. Verifyできる領域を拡大する仕組み
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



ペイン	ペインの解決方法(仮説)	活用する規格・技術	技術選定理由(仮説)
必要最小限の情報提供ができない	選択的属性開示が可能な証明書形式を利用する。	SD-JWT	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なため。
情報の信頼性が特定の事業者に依存している	相互運用可能なプロトコルを採用する。	OID4VCI OID4VP SIOPv2	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のため。
登録、通信相手が意図した人物か検証したい	検証可能な証明書形式を利用する。	SD-JWT	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なため。
メッセージのやり取りが特定の事業者に依存している	分散型のプロトコルを採用する。	Matrix	特定の事業者に依存しない構造、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強みがあるため。

4.2. Verifyできる領域を拡大する仕組み
4.2.3. Verifyするデーター一覧

課題	Verifyの対象	Verify方法	検証者(verifier)	データの保有者(ownership)	発行者(issuer)	データの置き場所(storage)	アクセスコントロール(access control)	成果・留意点
生活者の本人確認	生活者本人の実在性	検証可能な選択的開示(SD-JWT等)に対応した証明書の検証	サービス事業者(メッセージングサービス)	生活者	J-LIS → xID → OWND Project	アイデンティティウォレット	ウォレット格納デバイスでの生体認証	本実証ではxID社のAPIを用いてマイナンバーカードを用いた本人確認を実施。
生活者の属性確認	生活者本人の属性（13歳以上であること等）	検証可能な選択的開示(SD-JWT)に対応した証明書の検証	サービス事業者(メッセージングサービス)	生活者	J-LIS → xID → OWND Project	アイデンティティウォレット	ウォレット格納デバイスでの生体認証	本実証ではxID社のAPIを用いてマイナンバーカードを用いた情報の取得を実施。
証明書発行機関の実在性・正当性	事業者の審査結果	第三者機関による審査（OV証明書）	生活者 サービス事業者	証明書発行機関	Sectigo(CA事業者)	証明書発行機関サーバ	サーバのセキュリティ対策	利用技術について比較検討の上、OV証明書を利用することに決定。
サービス事業者の実在性・正当性	事業者の審査結果	第三者機関による審査（OV証明書）	生活者	サービス事業者(メッセージングサービス)	Sectigo(CA事業者)	サービス事業者サーバ	サーバのセキュリティ対策	利用技術について比較検討の上、OV証明書を利用することに決定。
メッセージ送信者の正当性	送信者の属性（当該組織所属であること）	検証可能な選択的開示(SD-JWT等)に対応した証明書の検証	生活者1(受信者)	生活者2(送信者)	DataSign(もしくは他社)	サービス事業者サーバ	サーバのセキュリティ対策	メッセージングサービスに社員証を提示して利用。
メッセージ受信者の正当性	受信者の属性（当該組織所属であること）	検証可能な選択的開示(SD-JWT等)に対応した証明書の検証	生活者2(送信者)	生活者1(受信者)	DataSign(もしくは他社)	サービス事業者サーバ	サーバのセキュリティ対策	メッセージングサービスに社員証を提示して利用。

4.2. Verifyできる領域を拡大する仕組み
4.2.4. 証明書要件・識別子要件

証明書要件

証明書名	記載情報	要件	活用する規格	規格選定理由
マイナンバーカード情報 ※ マイナンバーは含まれない	・基本4情報 ・13歳以上証明 ・18歳以上証明 ・20歳以上証明	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。	SD-JWT	選択的開示を行うため。
社員証	・会社名 ・部署名 ・社員番号 ・性名	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。	SD-JWT	選択的開示を行うため。
イベント参加証	・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	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。	JWT_VC_JSON	開示を行うため。

識別子要件

識別子名	何を識別しているか	要件	活用する規格	規格選定理由
Issuer	発行者(Issuer)	VCにissuerのURLを記載、/.well-known/jwks.json に公開鍵を配置、kidで指定。	url	Verifiable Credentials Data Model v2.0に準じて選定。
sub	エンドユーザ(Holder)	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	JWK Thumbprint	OpenID Connectに準じて選定。
aud	検証者(Verifier)	SIOP/OID4VPにおけるVerifierの識別子。	url	OpenID Connectに準じて選定。
id	エンドユーザ(Holder)	HolderがWalletを使うときのHolderの識別子。	HD wallet	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(1/2)

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

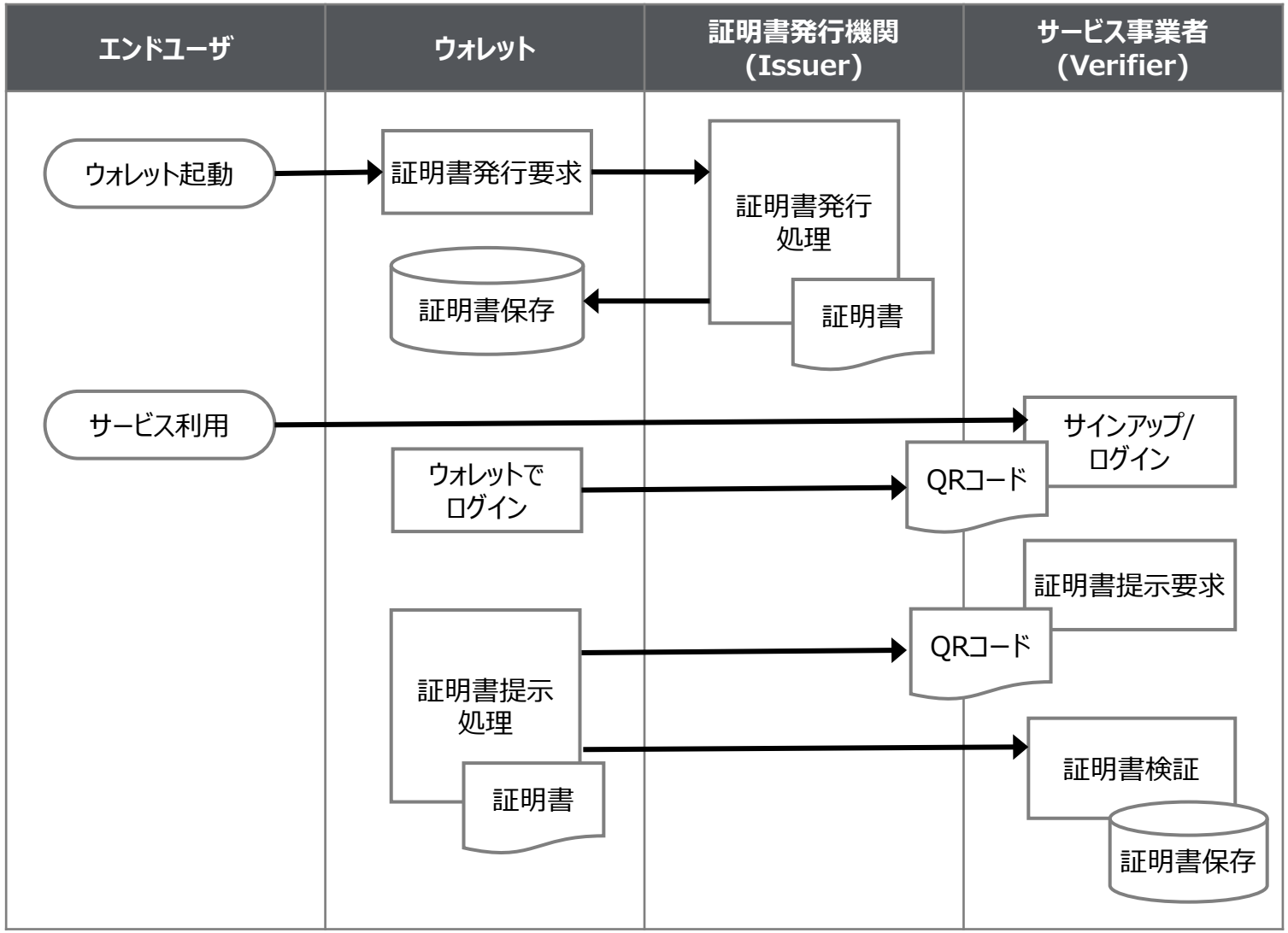
合意の主体	合意の対象	合意の条件	トレースの対象	トレースの手法	合意取消の可否・方法
エンドユーザと OWND Project	マイナンバー基本4情報と年齢情報(13歳、18歳、20歳以上)の取得	OWND ProjectがxIDアプリから左記の情報を取得して証明書にすることをエンドユーザ許可する	履行された左記の合意	OWND Wallet内の証明書として照会	可能 Walletからクレデンシャルの削除
DataSign社員と DataSign	社員証の取得	DataSign社員がDataSignに対して社員証の発行を要求してDataSignが許可する	履行された左記の合意	OWND Wallet内の証明書として照会	可能 Walletからクレデンシャルの削除
PbDLとPbDLが主催したイベントの参加者	イベント参加証明の取得	参加者がPbDLに対し参加証明の発行を要求	履行された左記の合意	OWND Wallet内の証明書として照会	可能 Walletからクレデンシャルの削除
エンドユーザと OWND Messenger	13歳以上の証明	OWND Messengerが要求した13歳以上ということの証明提供をエンドユーザが許可する	履行された左記の合意	Elementの画面にて照会	可能
エンドユーザと OWND Messenger	DataSign社員の証明	OWND Messengerが要求した所属組織証明提供をエンドユーザが許可する	履行された左記の合意	Elementの画面にて照会	可能
エンドユーザと OWND Messenger	PbDLイベント参加の証明	OWND Messengerが要求したイベント参加証明提供をエンドユーザが許可する	履行された左記の合意	Elementの画面にて照会	可能
エンドユーザとエンドユーザ	メッセージング所属証明	OWND MessengerがエンドユーザがDataSign社員に対してDMの送受信を行う許可	履行された左記の合意	Elementの画面にて照会	一度相手に送信されたメッセージを削除することは不可

4.3. 合意形成・トレースの仕組み(2/2)

第三者が確認する情報一覧

トレース情報	トレース手法	第三者が確認することのリスク・対応方針
クレデンシャルを取得した際の記録	クレデンシャルを発行した記録をVCIがログとしてAWSに保存	ログ自体が第三者から閲覧できない環境にある上、提供した事実のみを記録しているので個別の属性内容は記録されない
クレデンシャル	JWT形式のクレデンシャルより、発行者の署名でJWTを生成	JWT_VC_JSON、SD-JWTともにlinkabilityが発生し、verifireの結託によりクレデンシャルの持ち主が同一人物だということがわかってしまう
エンドユーザがOWND Messengerに開示した情報	クレデンシャルはsynapseのデータベースに保存され、保存された記録はAWSのログに保存	データベース、ログともに第三者からは閲覧不可

4.4. 企画・開発物
4.4.1. 業務フロー



4.4. 企画・開発物
4.4.2. ユースケース図

- 以下の項目のユースケース図を作成し設計を実施

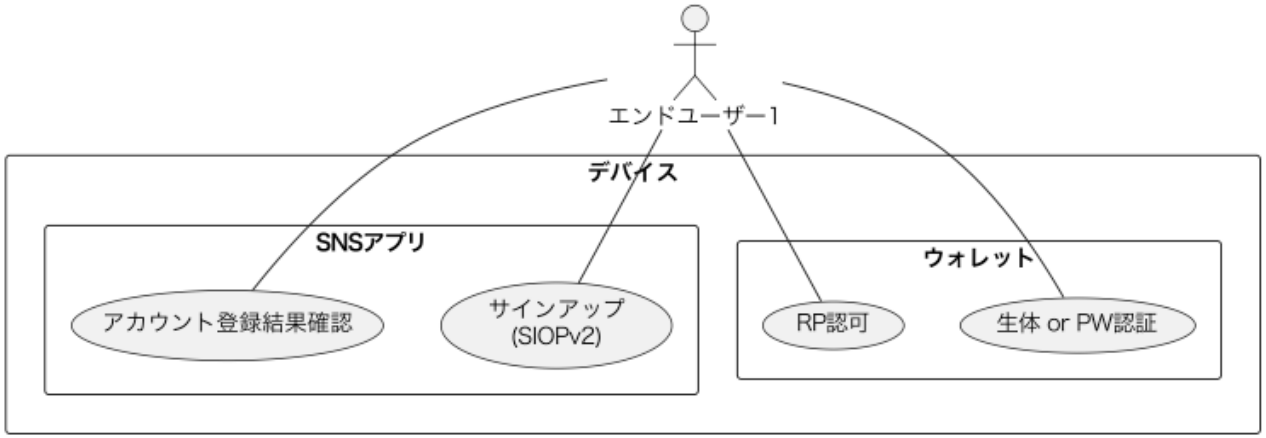
ウォレット

- 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

メッセージングサービス サインアップ (例)



※ 詳細は「別紙_ユースケース設計書.pdf」を参照。

4.4. 企画・開発物
4.4.3. 操作画面（ウォレット①）

※ 詳細は、OWND Project UI Components をご参照ください。

証明書新規追加

※ マイナンバーは含まれない

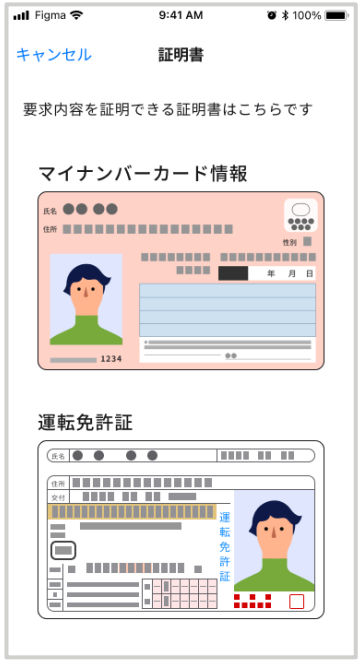
データ取得や第三者に共有するための画面上でのポイント

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わかるように工夫している。

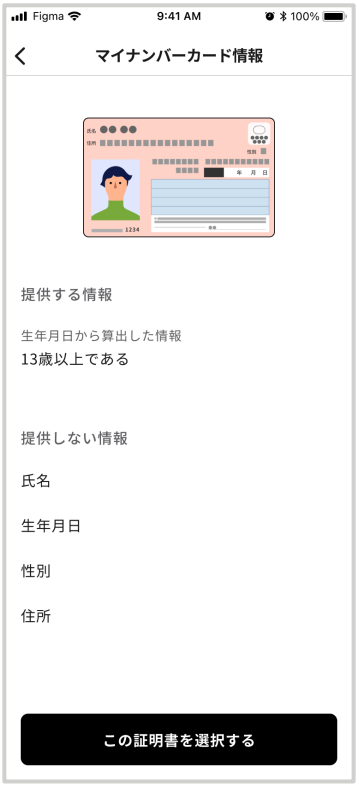
4.4. 企画・開発物
4.4.3. 操作画面（ウォレット②）

※ 詳細は、OWND Project UI Components をご参照ください。

証明書の提示



※ マイナンバーカード情報に
マイナンバーは含まれない



データ取得や第三者に共有するための画面上でのポイント

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」が明確にわ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。

4.4. 企画・開発物
4.4.3. 操作画面（メッセンジャー）

※ 詳細は、OWND Project UI Components をご参照ください。

メッセージの送信先の検証（送信元画面）

メッセージの送信元の検証（送信先画面）

データ取得や第三者に共有するための画面上でのポイント

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. 企画・開発物
4.4.4. 機能一覧/非機能一覧

機能/非機能	機能名	機能概要
機能	[ウォレット]初期設定	簡易かつ安全にウォレットの利用を開始できる
機能	[ウォレット]マイナンバーカード情報取得	OID4VCIのCredentialOfferのプロトコル上で基本４属性を持つVC発行を要求できること
機能	[ウォレット]サインアップ(属性情報提供)	OID4VPのプロトコル上でのクレデンシャル提供要求を受け付けられること
機能	[ウォレット]提供属性情報選択	提供要求のメタデータに従って対象の属性を明示できること
機能	[ウォレット]メッセージングサービスサインイン	SIOPv2プロトコルでサインアップできること
機能	[ウォレット]バックアップリカバリ	バックアップしたリカバリーフレーズにてマスターアカウントが復旧できること
機能	[Issuer]キーペア生成	指定されたキーIDと暗号曲線で新しいキーペアを生成し、データベースに保存できること 暗号曲線名は指定されたリストから選択される必要がある
機能	[Issuer]xID連携	マイナンバーカード情報発行する際にxIDと連携して証明書情報を提供できること
機能	[Issuer]証明書発行	特定の形式でクレデンシャルを発行する（JWT VC JSON, vc+sd-jwtなど）
機能	[Verifier]サインアップ	QRコードを表示してWalletからのサインアップを提供できること Walletでのサインアップが完了するとブラウザもサインアップが完了し、画面が遷移する
機能	[Verifier]属性情報提供	QRコードを表示してWalletから属性情報を提供ができること(OID4VP)
機能	[Verifier]バックアップリカバリ	暗号鍵を再生成するためのセキュリティーキーをダウンロードできること ダウンロードしたセキュリティキーからリカバリできること
機能	[Verifier]メッセージ送信	身元を検証した結果、送信先に対して暗号化されたメッセージを送信が可能であること

4.4. 企画・開発物
4.4.4.1. (非機能要件)リスク分析とセキュリティ対応方針

サービス(アプリ)利用にかかるリスク	影響度 (機密性・完全性・可用性への影響)	発生可能性 (どのような悪意的な攻撃が考えられるか)	左記リスクへの対応方針・攻撃防止の根拠
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	• VerifierがほかのVerifierと結託することによりLinkabilityが発生し、選択開示した以外の情報が流出	• 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	• 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
JWK ThumbprintをHolder識別子に使用することにより 鍵のローテーションに対応できない	• 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

4.4. 企画・開発物
4.4.4.2. (非機能要件)大規模・商用・社会実装時のシステム・運用方針

社会実装時に想定する利用規模

- 「2.3. 社会・経済に与える影響・価値(2/2)」に準ずる規模を以下の通り想定
- 日本におけるSNS利用者を1億200万人[1]とすると、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3060万枚の発行と想定
- メッセンジャーは1020万人が利用するとし、5件/日のトランザクションが発生すると、年間186億1500万トランザクションが発生すると予想

システム・運用方針

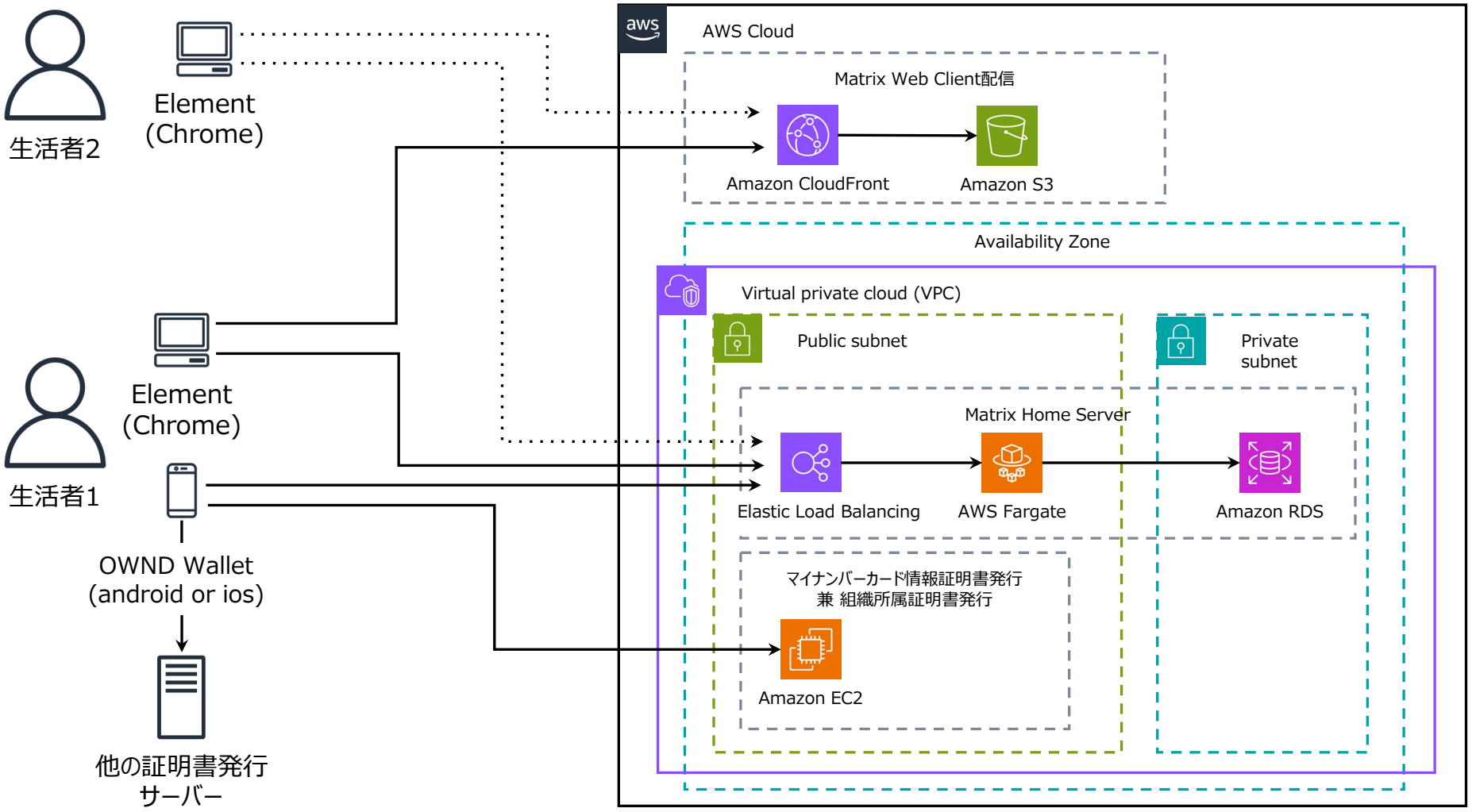
- VCI、homeserver(matrix)ともに一般的なwebサービスと同等のスケーラビリティーを備えていれば可用性に関して問題はない想定

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

4.4. 企画・開発物
4.4.5. 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. 企画・開発物
4.4.6. 実験環境



4.4. 企画・開発物
4.4.7. 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 (1/2)

No.	論点	検討結果とその経緯
1	ビジネスフィージビリティ① • 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	• 公募前の事前ヒアリングでは、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。
2	ビジネスフィージビリティ② • 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	• 公募前の事前ヒアリングでは、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していたり、ビジネス利用ではシャドーITやフィッシングの懸念が示されており、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。
3	ビジネスフィージビリティ③ • 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	• 公募前の事前ヒアリングでは、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を検討した。
4	ビジネスフィージビリティ④ • 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	• 公募前の事前ヒアリングでは、ウォレット、メッセージングサービスは、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。
5	ビジネスフィージビリティ⑤ • 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	• すで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いか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、本実証では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を検討する。

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 (2/2)

No.	論点	検討結果とその経緯
6	ガバナンス・ルール整理① • 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	• 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、階層型のトラスト・ガバナンスモデルを検討し、ホワイトペーパーにまとめた。
7	ガバナンス・ルールの整理② • 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	• 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として策定した。
8	コミュニティ形成 • 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	• 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. 実施概要
5.1.2. 実施内容・手法：ビジネスフィージビリティ検証 (1/2)

No.	論点	事前ヒアリング結果
1	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	• 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、登録に抵抗感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。
2	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	• SNSで友だち申請があった場合、申請元をさまざまなコンテキスト（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さまざま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をつかったり、メールをつか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合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。

5.1. 実施概要
5.1.2. 実施内容・手法：ビジネスフィージビリティ検証 (2/2)

No.	論点	事前ヒアリング結果
3	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	• 多数のソーシャルログインが存在するが、UX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、導入は二種類にとどめた。 • 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。
4	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	• ウォレット、メッセージングサービスは基本的に無料が良いが、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いただいた。 • 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いただいた。 • 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いただいた。 • 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いただいた。
5	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	• 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いただいた。 • 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いただいた。 • 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いただいた。

5.1. 実施概要
5.1.2. 実施内容・手法：ガバナンス整理

No.	論点	実施内容
1	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	• 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在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）
2	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	• 上記討議結果に応じた、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）

5.1. 実施概要
5.1.2. 実施内容・手法：コミュニティ形成

No.	論点	実施内容	想定参加者
1	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	コミュニティ定例会を開催し、以下取組を推進 • 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～）	• 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 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

5.2. 検証結果

5.2.1. オープンソースコミュニティの設立

※ 詳細は、https://github.com/OWND-Project/ を参照ください。

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プロジェクトをオープンソースコミュニティ形式で設立。

成果概要

- 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（3月予定）
- Wallet/Messenger関連のソースコードをオープンソースとして公開（3月予定）

5.2. 検証結果
5.2.2. ホワイトペーパーの作成

OWND Project WhitePaper 目次

- 1. イントロダクション
  - 1.1 OWND Project の概要
  - 1.2 この Whitepaper の役割
  - 1.3 Trusted Webとの関係
- 2. ビジョン、ミッション、コアバリュー
  - 2.1 未来に対するビジョン
  - 2.2 プロジェクトのミッション
  - 2.3 コアバリュー
- 3. 現状認識と考慮事項
  - 3.1 現状のデジタルアイデンティティ
  - 3.2 新しいアプローチに対する考慮事項
- 4. 課題の解決に向けて
  - 4.1 主な課題の特定
  - 4.2 OWND Projectの提案する解決策
- 5. 提供する価値
  - 5.1 個人にとっての価値
  - 5.2 企業にとっての価値
  - 5.3 競争上の優位性
- 6. ガバナンス構造
  - 6.1 ガバナンスの考え方
  - 6.2 OWND Project のガバナンス
  - 6.3 参加と貢献のためのインセンティブ
- 7. 技術的アーキテクチャ
  - 7.1 OWND Wallet のアーキテクチャ
  - 7.2 OWND Messenger のアーキテクチャ
  - 7.3 Trusted Web アーキテクチャとの関係
- 8. ロードマップとマイルストーン
  - 8.1 開発フェーズ
  - 8.2 マイルストーンとタイムライン
- 9. ユースケース
  - 9.1 年齢確認
  - 9.2 イベント参加証
  - 9.3 デジタル社員証
- 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（UXリサーチとトラストの考察）

※ 詳細は、2024年12月に論文発表を行った
「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」を参照ください。

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

No.	論点	検討結果とその経緯
1	• 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	• 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、抵抗感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	• 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	• 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ない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の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	• 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	• 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わからない」「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。
4	• 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	• 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考え、上記の調査結果を踏まえて机上検討を行った。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. 実施概要
6.1.2. 実施内容・手法

3つのシナリオ(タスク)に関して、Figmaのプロトタイプ画面を操作いただき、論点に対応するインタビュー調査を実施した。

No.	論点	シナリオ(タスク)	インタビュー内容
1	• 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	• ウォレットへマイナンバーカード情報を登録	• タスク1では、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？
2	• 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	• 架空のSNSサービスへウォレットで会員登録	• タスク2では、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？
3	• 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	• ウォレットでSNSサービスに提供した情報の確認	• タスク3では、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？

実験参加者に関して

- 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。

No.	論点	テーマ	主な発見
1	• 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	• ウォレットアプリやウォレット事業者の信頼	• 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
		• マイナンバーカードへの親しみ	• 証明書を提示するという行為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	• 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	• 新しい体験への移行	• 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
		• 理解の深まりによる安心感	• 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	• 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	• 確認したいが方法がわからない	• 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、確認方法がわからないために確認できないことが示唆された • 後から確認する時には提供した情報について忘れてしまっていたり、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
		• 管理したいが面倒で諦めてしまう	• どこに何を提供したかを管理したいと思っているが、めんどうなので諦めている • 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

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 (1/4)

No.	残課題（指摘事項含む）	対応方針
1	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。	本実証では、シンプルな仕様であり且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。
2	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)	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。
3	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。	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）
4	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。	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。
5	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。	OID4VP overBLE(ドラフト)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。https://openid.net/specs/openid-4-verifiable-presentations-over-ble-1_0.html

7.1. 残課題対応方針一覧 (2/4)

No.	残課題（指摘事項含む）	対応方針
6	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。	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。
7	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。	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。
8	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。	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、業界標準となりう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。
9	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。	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。
10	VCIのKey Binding問題、あらかじ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毎の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)	発行時点でHolderとVCを結びつける構成の場合は、提供先毎に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。
11	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。その為悪意のある者が、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。	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。

7.1. 残課題対応方針一覧 (3/4)

No.	残課題（指摘事項含む）	対応方針
12	No.1に挙げたように、連結性への対処の為に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無い。	RP毎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。その為には、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。
13	SIOPv2のdirect postを行なった後に、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。	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。
14	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。	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。
15	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）	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。
16	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。	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。

7.1. 残課題対応方針一覧 (4/4)

No.	残課題（指摘事項含む）	対応方針
17	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元にエコシステムを設計すべきか。	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。
18	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。	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の対応べき課題として継続して検討を進める。
19	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。	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。
20	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コード読み取り時に、そのうちの一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。	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。
21	本実証ではわ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。	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。

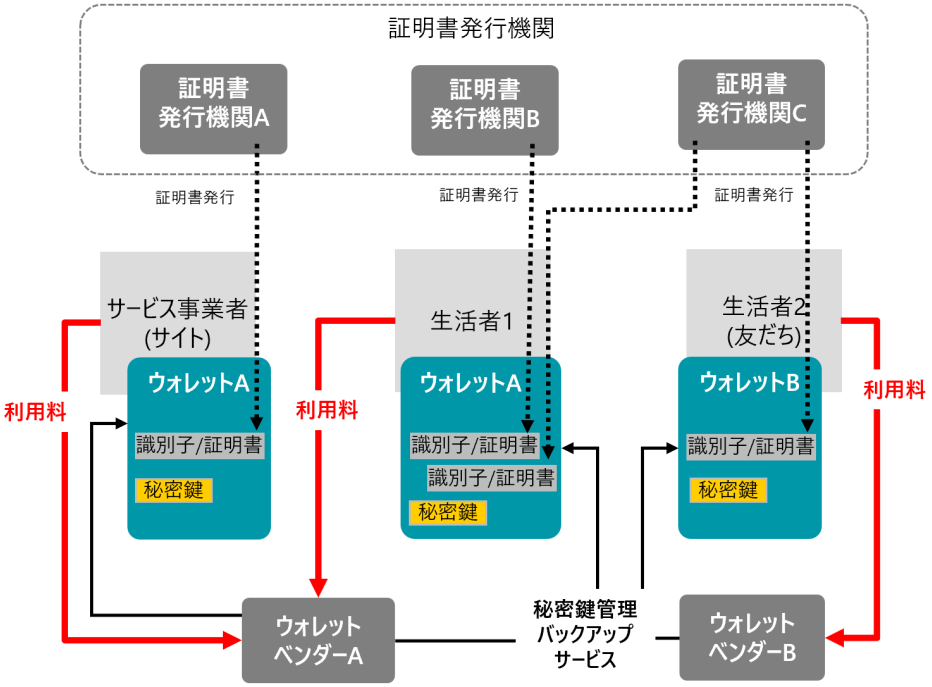
7.2. 将来的なユースケース実現モデル
7.2.1. ビジネスモデル案

ビジネスモデル	収益構造	対応方針
①ウォレット（秘密鍵管理サービス）	秘密鍵の管理はDIWにおいて大きな課題のひとつであり、OWND Walletにおいても、利用者自身の責任において秘密鍵を管理する構成としている（データ主体によるコントローラビリティを最大化するため）。この課題を解決するための秘密鍵管理サービスをDIW利用者に提供することにより、その管理料としてDIW利用者から収益を得る。	OWND Project（コミュニティの形成）によって相互運用可能なDIWをオープンソースで公開し、商用利用や改変を排除しないことにより、誰でも独自のウォレットサービスを提供できるようにする。また、秘密鍵の管理については、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が独自に管理サービスを提供できるような構成とする。
②証明書発行（企業向けPaas, Saasの提供）	各エンティティがトラストを担保するために証明書発行機関に対して審査費用等を支払うことは、現状も存在するビジネスモデルのため、証明書発行機関がDXの一環として証明書をデジタル（VC）で発行することが考えられる。OWND Projectの成果物をベースにそれらの発行するためのシステムを証明書発行機関にPaaSやSaaSとして提供することにより収益を得る。	OWND Project（コミュニティの形成）によって相互運用可能な証明書の発行システムをオープンソースで公開し、商用利用や改変を排除しないことにより、誰でも独自の証明書（VC）発行ビジネスを開始することができるようにする。
③メッセージング（企業向けPaas, Saasの提供）	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PaaSやSaaSとして提供することで、利用企業から収益を得る。既存のメールサーバ提供事業とビジネスモデルとしては同様。上記の証明書発行PaaSと組み合わせることにより、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。	OWND Project（コミュニティの形成）によって相互運用可能なメッセージングシステムをオープンソースで公開し、商用利用や改変を排除しないことにより、誰でもメッセージングビジネスを開始することができるようにする。
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。	OWND Project（コミュニティの形成）によって相互運用可能なメッセージングシステムをオープンソースで公開し、商用利用や改変を排除しないことにより、誰でもメッセージングビジネスを開始することができるようにする。

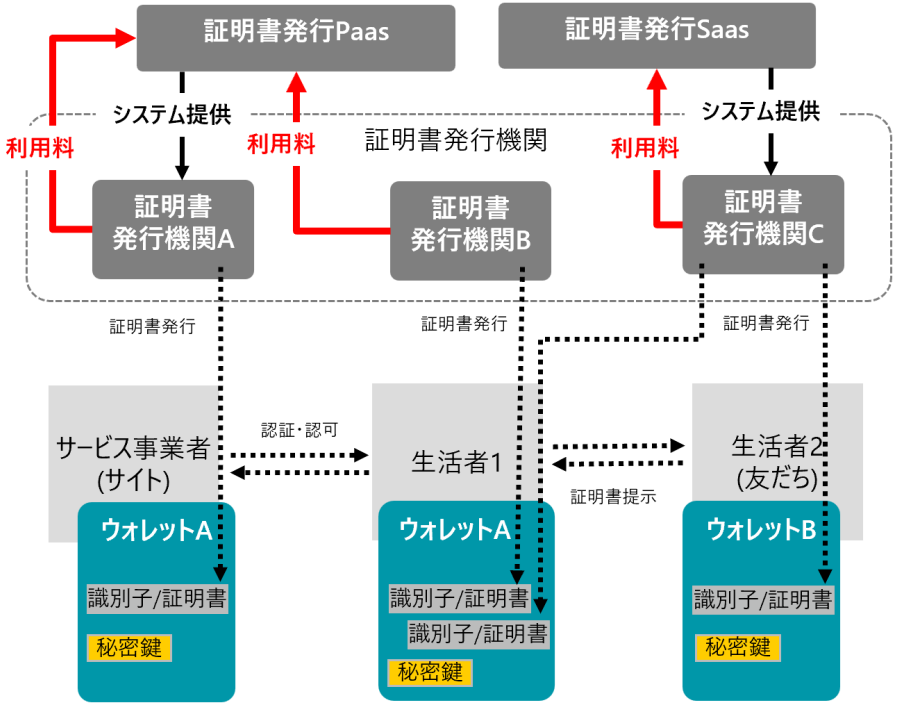
7.2. 将来的なユースケース実現モデル
7.2.1. ビジネスモデル案

：サービスの流れ
：情報の流れ
：お金の流れ

① ウォレット（秘密鍵管理サービス）



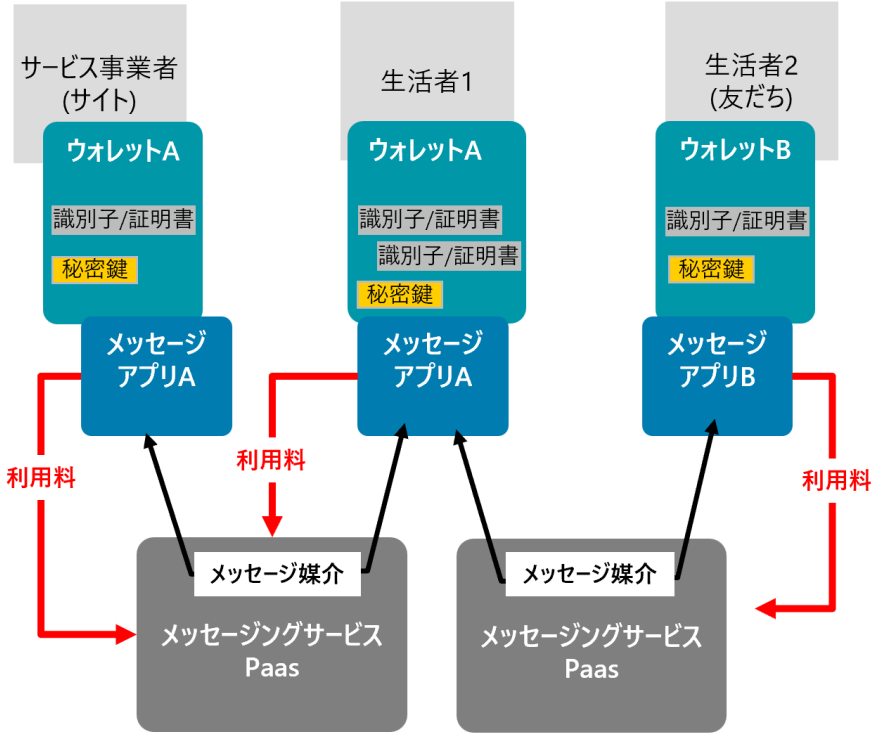
② 証明書発行（企業向けPaas, Saasの提供）



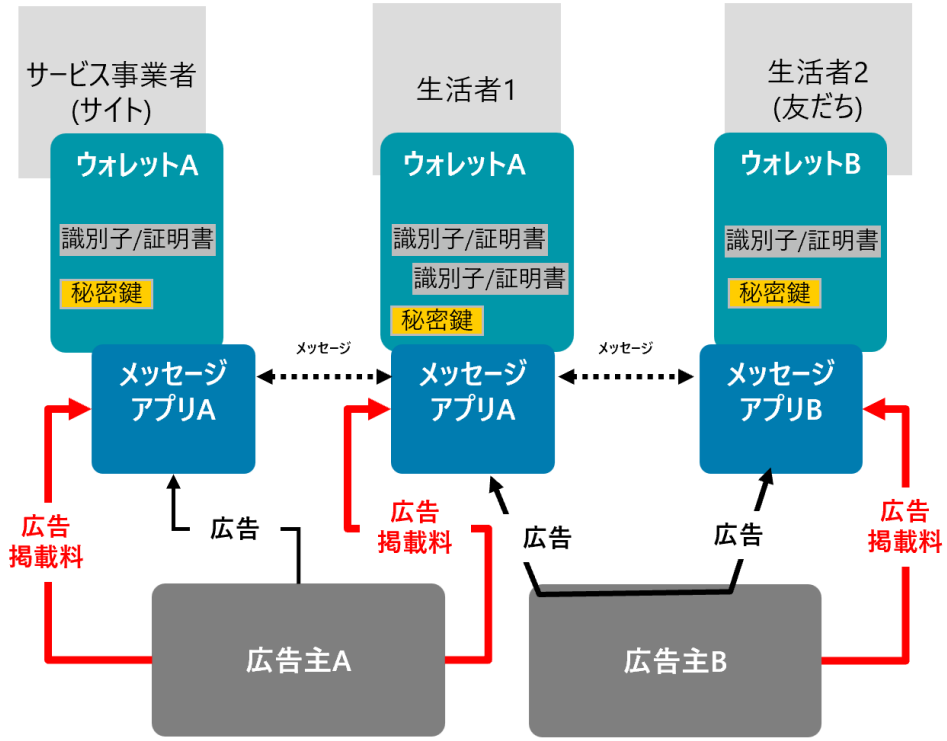
7.2. 将来的なユースケース実現モデル
7.2.1. ビジネスモデル案

：サービスの流れ
：情報の流れ
：お金の流れ

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



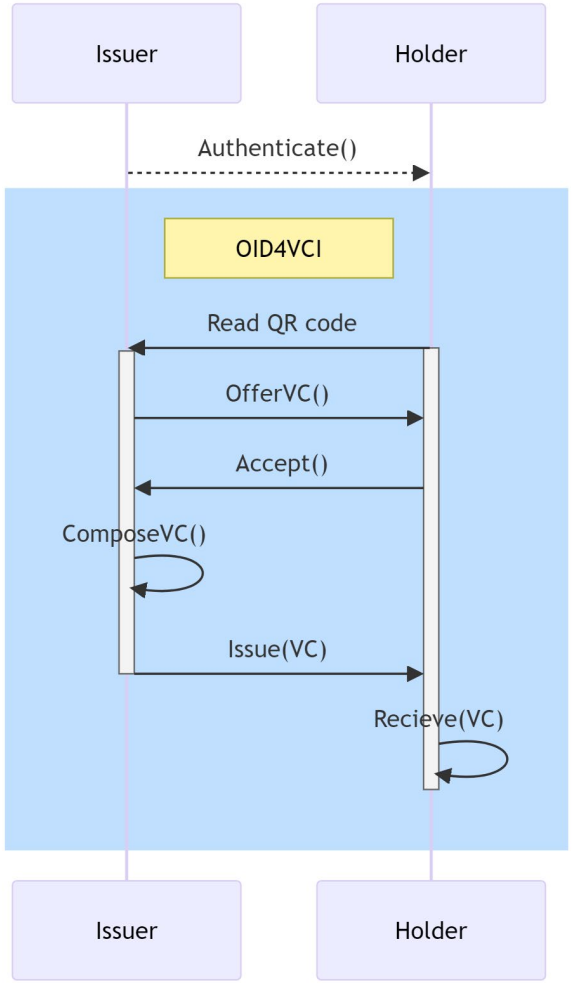
7.2. ユースケース実現案
7.2.2. アプリ・システム案

各観点への対応

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出来る設計とした。

7.2. ユースケース実現案
7.2.2. アプリ・システム案

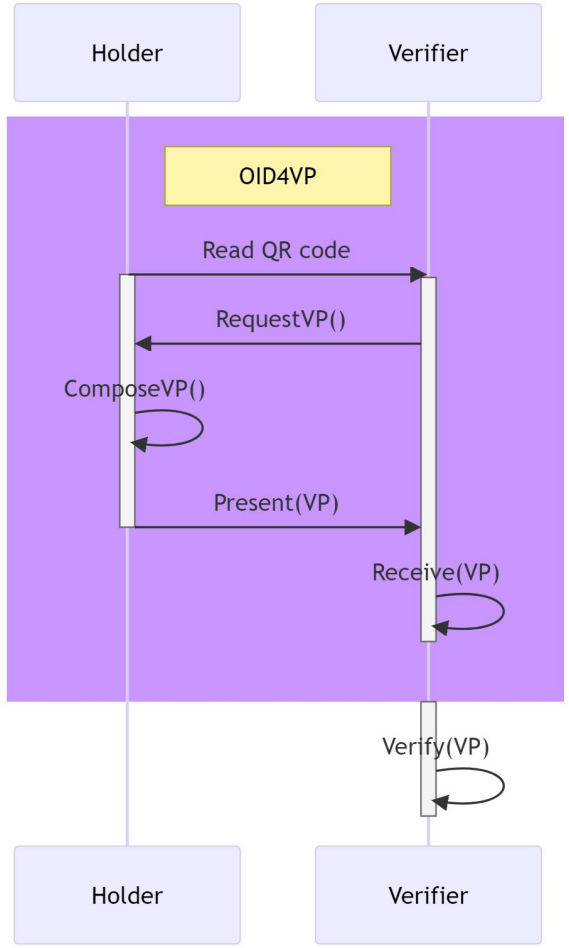
アプリ・システム構成（OID4VCI）



- 属性情報（画像の例では「マイナンバーカード情報」）をIssuerから発行するプロトコルとしてOID4VCIを採用しており、ウォレットに証明書を補完することができる。
- また、OID4VCIに対応しているIssuerやWalletとの相互運用が可能になっている。
- Issuerは証明書をSD-JWT形式で発行できるように構成し、また、画面上でどのような情報を含む証明書が発行されるのかを確認できるようにする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。

7.2. ユースケース実現案
7.2.2. アプリ・システム案

アプリ・システム構成（OID4VP）



- 属性情報（画像の例では「13歳以上であること」）をVerifierに提示するプロトコルとしてOID4VPを採用しており、ウォレットに保存されている証明書から自分の意思で属性情報を提示することができる。
- また、OID4VPに対応しているVerifierやWalletとの相互運用が可能になっている。
- Verifierにデータを提示する際には画像にあるように、画面上でどの証明書から何の情報が提供されるか示し、SD-JWTから必要な情報のみを提供できるようにすることよりデータ主体によるコントロール性を確保している。

7.2. ユースケース実現案
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次ページに示す。

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、Whitepaper内で宣言することとした。（OWND Project Whitepaperのドラフト）

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。

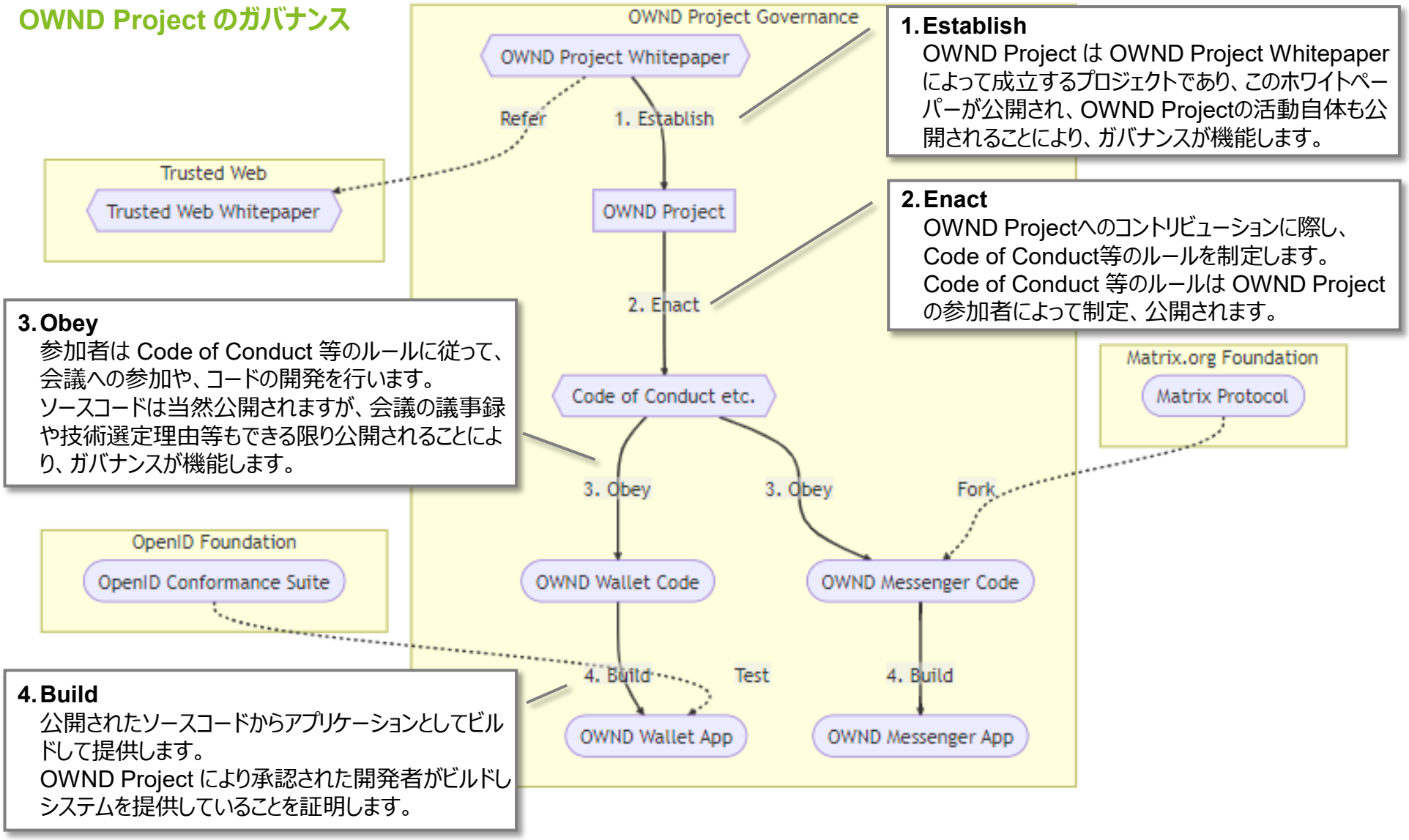
- **透明性**
  - 意思決定プロセスと、プロジェクトに関わる文書は公開されることで、透明性を担保
- **多様なステークホルダーによるコンセンサス**
  - 参加者を排除しないことにより、多様なステークホルダーによるコンセンサスを形成することで意思決定を行う。

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

7.2. ユースケース実現案
7.2.3. ガバナンス・ルール案

OWND Project のガバナンス



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、ガバナンスが機能します。

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

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、コードの開発を行います。
ソースコードは当然公開されますが、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、ガバナンスが機能します。

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します。
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します。

7.3. 実現に向けたアクションプラン・ロードマップ

タイムライン	マイルストーン	マイルストーン達成に向けて実施すること
2024年02月	実証実験	• 本ユースケース・システムの実証実験の実施
2024年03月	汎用ウォレット オープンソース化	• 本ユースケース開発物のオープンソース化、コミュニティでの継続的なアップデート • 汎用ウォレットをベースに用いた、営利企業によるウォレットの提供
2024年05月	メッセージング ベータサービスリリース 運用ノード募集開始	• メッセージングサービスのベータ版リリース • 参画・運用ルールを整備し、運用ノード募集開始
2024年07月	汎用ウォレットを用いた ユースケースの募集	• コミュニティによる汎用ウォレットを用いた他ユースケースの募集（地方自治体等を想定）
2024年12月	汎用ウォレットをベースとした複数 アプリケーションでの相互運用性の確認	• ユースケースの応じたデータの標準化を検討し、ウォレットアプリの相互運用性を確認
2025年04月	メッセージング 運用ノード増加	• メッセージング運用ノードが10ノードに拡大、利用者1万人越え

8. Trusted Web に関する考察

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

原則	自社取組との関連	アラインするうえでの課題
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	• 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無いと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
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	• OSSプロジェクトへの参加の敷居を下げ、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と感じている。
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。	

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

原則	自社取組との関連	アラインするうえでの課題
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はすべてコントロールすつ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を行っていくことで、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、それが排除につな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うえ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いなってしまうが、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。

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

原則	自社取組との関連	アラインするうえでの課題
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うこともある。
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ほうが機能拡張が容易な場合もある。

8. Trusted Web に関する考察
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うえでの課題
   - 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、技術的には連携可能だが、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、ガバナンスに参加するために有効な取組み・インセンティブにかかる示唆（各業界や行政などがどのように関与するか等）
   - 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 もその一つと考えられる）やGood Lobby Tracker のような取り組みが参考になると考えられる。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うえでの課題
   - それぞれのステークホルダーにガバナンスをかけるうえで、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。その基準を満たすコストがメリッ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。
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してほしい。WPv3.0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つながるかを明確にすることが難しい。

8. Trusted Web に関する考察
8.3. Trusted Web のアーキテクチャに関する課題と提言

No.	課題	提言
1	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、頻繁に使用が変更されてしまう。	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良いのではないか。
2	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。	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。
3	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。	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. Trusted Web に関する考察
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、現時点ではとくにないが、
引き続きOWND Project等の活動の中で議論を進める。

Appendix.

用語集 (1/2)

用語	内容
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とりのこと。
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と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。

用語集 (2/2)

用語	内容
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 Toke (JWT)n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) 自信がOpenID Provider (OP) となり認証連携を行う標準仕様。
Decentralized Identifiers（DID）	分散的に管理されたグローバルに一意な識別子。
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な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ホームサーバー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できる 。
  - 利用技術選定
  - https://docs.google.com/spreadsheets/d/1slgnsy94R3Ku3SEJPddlYciZ1bIDZcU2sHR8cSuSP-4/edit?usp=sharing
- 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 。
  - ユースケース設計書
  - https://drive.google.com/file/d/1p-DWLv6Jke5osqD2dlKrt94PDyNJ8oKv/view?usp=drive_link
- 本実証事業で開発したプロトタイプシステムは全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 。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。
  - https://github.com/OWND-Project/
- 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 。
  - https://www.ownd-project.com/
- 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

ヒアリング先	検証する課題論点	ヒアリング項目	回答
証明書発行機関 A社	✓ 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	➢ 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	➢ 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わかるとよいと意見をいただいた ➢ 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	✓ 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	➢ 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	➢ 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いただいた ➢ 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、合わせていくほかないという意見をいただいた
サービス事業者 C社	✓ 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	➢ 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	➢ 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意見をいただいた ➢ 既存のソーシャルログインと比べ、ウォレットの方が取れ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いただいた
サービス事業者 D社	✓ 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	➢ 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	➢ 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	✓ 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	➢ どういったインセンティブがあれば今後似たようなことをやってみようと思うか	➢ 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回答をいただいた ➢ 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増加を期待できるかというところがポイントと回答をいただいた