# 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

共助アプリを横断したトラスト形成エコシステム

2024 年 3 月 15 日

大日本印刷株式会社

# 目次

# 1．背景と目的

## 1.1 背景・目的

【実証の背景】

昨今、ICT を活用した包括的社会の実現を目指して、移動支援、保育、高齢者見守り等の様々な分野において、生活者同士の共助を目的とした WEB マッチングサービス（共助アプリ）が開発されている。

一方、共助アプリでは見知らぬ他者同士のマッチングが行われることが多く、利用者のトラストをどのように検証して安全な顧客体験を実現するのか、各共助アプリプラットフォーマーにとっての大きな課題になっている。

2022 年度の「Trusted Web 実現に向けたユースケース実証事業」において、大日本印刷（DNP）は上記課題を解決するために共助エコシステムのサービス企画を実施し、共助アプリベンダー3 社（AsMama 社、カヤック社、プラスロボ社）と共にトラストフレームワークを検討しながら、共助実績を発行・検証するための分散型 ID システムの要件定義を行った。その結果、本ユースケースに関する共助アプリベンダーのニーズと、実現に向けた課題を確認できた。

【実証の目的】

人の個性が多様化する社会において、価値あるコミュニケーションによって人々を繋ぐためにも、今後、共助アプリのニーズは高まっていくことが予想される。一方で、現状は下記 3 点が共助エコシステムの社会実装に向けた課題であり、本取組によるプロトタイプシステム開発を通じてさらなる検証が必要であると考える。

① 【テクノロジー観点】相互運用可能な分散型 ID システムの構築

本ユースケースでは共助アプリ間の実績共有だけではなく、人的資本（大学入試や就職活動時のスキルやキャリアの証明）活用も見据えているため、異なるステークホルダ間でのシステムの相互運用性が重要。現状、W3C や EU Digital Identity Wallet（DIW）の仕様に関してはグレーゾーンが多く、システム構成において実装ベンダーに依存する範囲が大きいことが問題となっている。本取組では、オープンソースのフレームワークを使って分散型 ID のシステムを開発し、セキュリティやプライバシー保護の観点で検証することを想定。技術面における相互運用性の課題を抽出し、共助エコシステム内外で参照できる標準仕様の策定を目指す。

② 【ガバナンス観点】実運用を見据えたトラストフレームワークの設計

2022 年度の実証「共助アプリにおけるプラットフォームを超えたユーザートラストの共有」を通じて、適切なトラスト形成のためにはエコシステム内のガバナンス設計が重要であるとの結論に至った。共助実績が価値ある証明書として活用されるためには、発行者の認定（トラストマーク）やデータ項目の共通化が必要となる。本取組では、先行する共助アプリの認定制度（「シェアリングエコノミー認定制度」等）を参考にしながら、複数のステークホルダ間で合意可能なトラストフレームワークの策定を実施する想定である。2022 年度は深掘りできなかった「監査」や「法的規則」の項目も含め、実運用を見据えた制度設計を行う。

③　【UI/UX 観点】生活者にとって分かりやすいメリットの訴求

本ユースケースが社会で普及するためには、トラスト検証の範囲が広がることを生活者が実感できる体験設計が重要になる。本取組では共助実績を蓄積する Wallet のデモ画面を作成し、ユーザヒアリングを通して UI/UX を検証していく想定。具体的には、共助実績の表示方法や連携方法について共助アプリベンダーと議論しながら、より直感的なユーザー体験によるメリット訴求の方法を検討する。

# 2. 事業の概要

## 2.1 登場する主体と概要

### 2.1.1 ユースケースの概要

生活者同士のマッチングによる手助けを促進する共助アプリにおいて、ユーザーが安心してサポーターを選ぶ判断ができるように、複数の共助アプリを横断して共助実績を管理・検証できるシステムを開発することで、ユーザーのトラスト検証範囲を広げ、より安全な共助体験の実現を目指す。

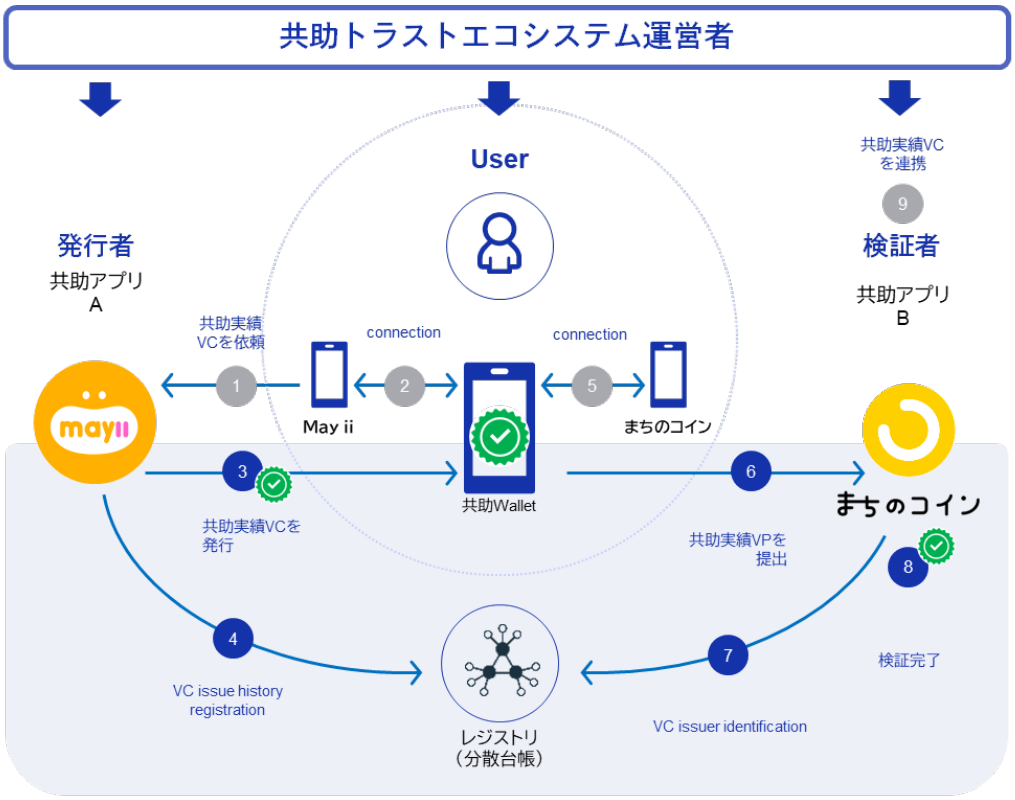



**図 2-1-1：ユースケース概要図**

### 2.1.2　事業スキームにおける各主体の役割

■ 共助トラストエコシステム運営者
- コンソーシアムの運営
- トラストフレームワーク作成・更新・運用
- 共助 Wallet の提供
- 他ベンダーの Wallet の認定

■ 共助 Wallet ユーザー（User）
- 共助アプリでサポートを実施
- 共助 Wallet を利用して共助実績を蓄積、管理
- 共助実績を別の共助アプリや 3rd party 企業に連携

■ 共助アプリベンダー（発行者）
- 共助実績証明書を共助 Wallet ユーザー（User）に発行
- 共助トラストフレームワークに準拠した証明書を発行する

■ 共助アプリベンダー（検証者）
- User へ検証リクエストを送信
- 共助実績証明書の署名を検証し、サービスを提供
- トラストフレームワークに準拠して共助実績証明書を取り扱う

■ 3rd party 企業
- User へ検証リクエストを送信
- 共助実績を検証してサービスを提供
- トラストフレームワークに準拠して共助実績証明書を取り扱う

■ 共助アプリの依頼主
- 共助アプリを通じてサポートを依頼
- 共助 Wallet ユーザー（User）の共助実績を確認

2.1.3　事業スキームにおける各主体の課題・本ユースケースを通じて解決できること

**表 2-1-1：事業スキームにおける各主体の課題と解決できること**

| 主体 | 課題 | 本ユースケースを通じて解決できること |
|---|---|---|
| 共助アプリベンダー（発行者） | サポーターになる生活者に、対外的に使えるインセンティブを渡して登録を促進したい | 本人確認 VC や共助実績 VC 等の属性証明を発行し、ユーザーの資産として蓄積・活用することを可能にする |
| | 収益機会を増やしたい | 発行した VC を他サービスや他共助アプリが活用した場合、検証手数料等の新たな収益機会となり得る |
| | 自分たちの共助アプリの認知を高めたい | 保有する VC をもとに活躍できる共助領域を提案することで、他共助アプリのサポーター化を促進する |
| | 利用者の安全性担保と、オンボーディングの UX 向上というトレードオフを解消したい | 他の共助アプリで証明済みの事項を VC として受領することで、安全性の担保を代替できる |
| 共助アプリの依頼主 | 相手となるサポーターが信頼できるか分からない | 共助実績 VC 等により従来可視化されていなかった信用度を担保できる |
| | サポートをする共助アプリユーザーが少なく、マッチングしない。 | 共助実績証明書の発行がサポートする共助アプリユーザーに対するインセンティブとなり、共助エコシステムへの参加者が増えることにより、マッチングが成立しやすくなる。 |
| サポート側の共助 Wallet ユーザー（User） | 複数の共助アプリを利用する場合、その都度個人情報の登録や事前教育を受ける必要がある | 本人確認 VC や共助実績等を他のアプリにも連携すれば、共助マインドのあるユーザーが容易に様々な共助アプリ上で活躍する機会を得られる |
| | 共助アプリ外での成果やスキル、修了事項（例：研修受講を大学入試の面接で提示したい） | VC として発行された「外部での成果や修了事項」を証明事項としてアピールが可能 |
| | 共助アプリ内での成果（例：共助履歴やユーザー評価など）を自分の活動履歴として証明したい | 共助アプリ内での成果を VC として発行し、検証者側となる学校や企業は VC を検証することでサポーターの活動成果を評価できる |

## 2.2 現状の課題を解決する事業スキーム案

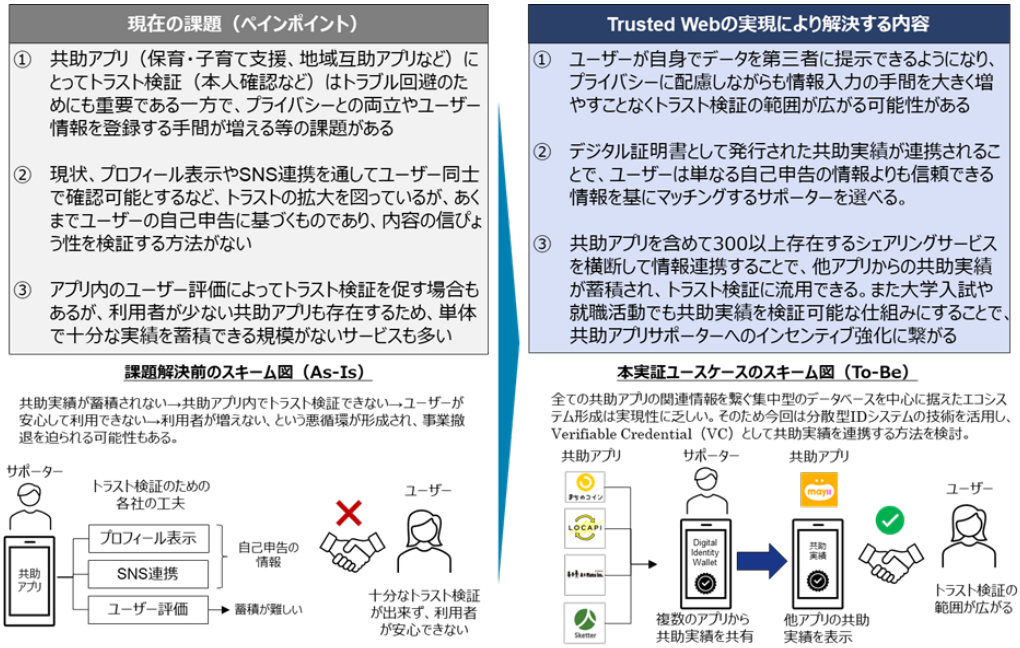



**図 2-2-1：事業スキーム案**

共助実績を Verifiable Credentials（VC）としてプラットフォーム横断で共有できるシステムを開発、そのシステム利用料に基づき運営を行っていく。DNP が運営する共助アプリ「May ii」と連携して本システム開発を進め、他社の共助アプリ運営者にも協力を呼び掛けながら本事業の詳細を検討していく予定である。

■ 事業シナリオ

共助アプリを横断した生活者の属性情報のやり取りとして、以下のシナリオを想定する。

① 共助アプリ（発行者）での活動を通じて、共助アプリサポーターは実績を蓄積する。
② 共助アプリ（発行者）は共助アプリサポーターに対して共助実績 VC を発行する。
③ 共助アプリサポーターは共助実績 VC を共助トラストフレームワーク運営者が発行している Wallet の中で保管・管理を行う。
④ 共助アプリサポーターは別の共助アプリ（検証者）を利用するときに、共助実績 VC を連携する。
⑤ 共助アプリ（検証者）は共助実績 VC の真正性を検証し、問題がなければ共助アプリサポーターのプロフィール欄に共助実績を表示する。
⑥ 共助アプリユーザーは共助アプリサポーターの共助実績を確認し、マッチングするユーザーを選ぶことができ、安心して共助アプリを活用できる。
⑦ 共助アプリサポーターは自らの共助実績を大学入試や就職活動時に証明書として提示できる。

■ 費用を負担する主体

本ユースケースにおいて想定しているビジネスモデルでは、「共助アプリトラストフレームワーク運営者」が Wallet の提供者となり、共助アプリ（発行者）および共助アプリ（検証者）からの登録手数料を徴収

してマネタイズを図る。

## 2.3 社会・経済に与える影響・価値

【社会（業界への影響）】

政府が掲げるデジタル田園都市国家構想においても「国が整備するデジタル基盤の上に、共助の力を引き出し、各地域で全体最適を目指したエコシステムを構築する。」[1]との記載がある通り、公共サービス、企業サービスの限界による「超高齢社会」「サービス業の人員不足」「地域交流の希薄化」等の様々な社会問題を解決する手段として「共助サービス」が注目されている。

本実証において企画する DIW/VC を活用したインフラ基盤は、ユーザーの安全安心な体験を担保しつつ、「共助サービス」エコシステムのスケール拡大を後押しすることで、多様な側面から社会・経済に価値を生み出すことができる。

【経済的価値】

「プラットフォームを横断した共助エコシステムのトラスト形成」の実現により、主に下記 3 点の社会的インパクトがあると考えられる。

① 共助の広がりによる経済的インパクト

高齢者（ここでは 65 歳以上と定義）向けの市場規模（「医療・医薬」「介護」「生活産業」）は、2025 年には 101.3 兆円に拡大すると言われており、その中でも生活産業の市場が過半数を占めている[2]。当社が運営する May ii は、サポートする側への「心のバリアフリー[3]（様々な心身の特性や考え方を持つすべての人々が、相互に理解を深めようとコミュニケーションをとり、支え合うこと） 」の意識醸成を重視して教育や行動促進するアプリを展開しており、高齢者が行政サービスや有償の事業者サービスを利用するだけではなく、周囲の人からのちょっとしたサポートで高齢者の経済活動（移動や消費）を活性化することを目指している。

このような共助サービスは、今後さらなる急激な超高齢社会において、持続可能な消費行動を促すインフラ基盤となる。また保育・子育て、障がい者支援、スキル提供の共助サービスも存在。共助エコシステムの拡大により多様な人材の社会参加が促進され、企業の生産性向上やイノベーション創出に繋がる[4]。

② 共助データを活用した自治体 DX の促進

---

[1] デジタル庁.「デジタル田園都市国家が目指す将来像について」.
https://www.cas.go.jp/jp/seisaku/digital_denen/dai2/siryou2-1.pdf

[2] みずほ産業調査部.「みずほ産業調査 Vol.39」.
https://www.mizuhobank.co.jp/corporate/bizinfo/industry/sangyou/m1039.html

[3] 国土交通省.「心のバリアフリー」.
https://www.mlit.go.jp/sogoseisaku/barrierfree/sosei_barrierfree_tk_000014.html

[4] 内閣府.「内閣府労働市場の多様化が経済に与える影響」.
https://www5.cao.go.jp/j-j/wp/wp-je19/h02-03.html

行政は、現場の課題を客観的なデータに基づき把握し施策を打つ EBPM の推進が求められているが、こうしたデータの収集は時間とコストがかかり、迅速な施策検討・実施が課題の 1 つとなっている。

地域における共助履歴のデータは「住民課題の可視化」に繋がることから、行政・自治体としても有益なデータになる可能性が高い。共助エコシステムで助け合いが活発な領域を抽出して分析することにより、「政策分析精度の向上、住民サービスの向上、行政職員の生産性の向上 [5]」等の効果を見込む。例えば、May ii で手助けのリクエストが多い場所は、移動困難者にとってバリアフリーではない場所とも言えるため、都市のバリアフリー改善のためのデータとして活用できる。

また本取組は「個人のデータを生活者自身が管理するエコシステム」であることから、プライバシーに配慮した自治体のデータ利活用施策として今後のモデルケースになり得る。

③　共助アプリ以外の他業界サービスとの連携

共助アプリの利用を通して蓄積された個人のトラストは、他業界のサービスからも有用なデータとして認められる可能性が高い。例えば、金融業界におけるローンの貸し出しや決済時の信用担保の場面では、個人の経済的信頼度だけではなく、社会的信頼度を評価する指標として活用することが考えられる。また不動産業界、保険業界等でも同様のユースケースが考えられ、社会的信用の担保が必要な領域で、個人のエンパワーメントに繋がることが想定される。

共助アプリ業界を超えた他業界ビジネスとの連携を視野に入れることで、社会における共助エコシステムの位置づけはさらに重要なものになる。

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

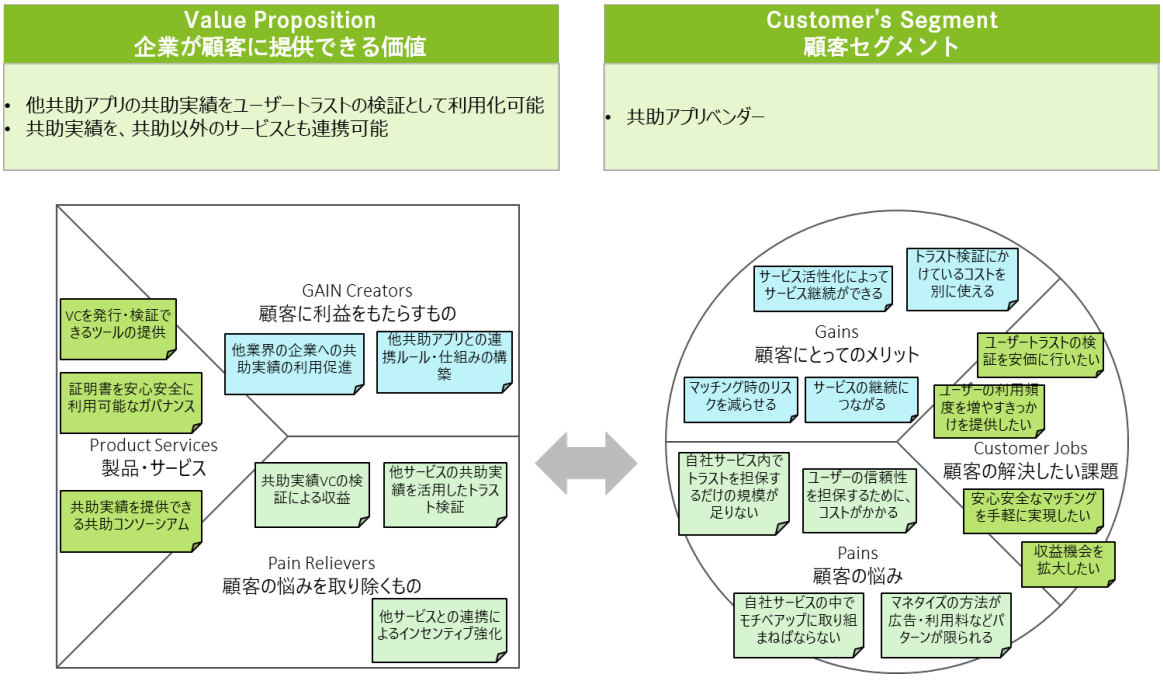



**図 2-4-1：ペイン・ゲインの整理**

[5] 総務省.「総務省地方公共団体におけるデータ活用の意義・必要性」.
https://www.soumu.go.jp/main_content/000620315.pdf

# 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

論点①：【テクノロジー観点】プロトタイプ開発と国際間連携の技術的なテスト実施

導出・経緯：昨年度机上で検討した技術仕様でプロトタイプシステムを実装し、セキュリティやプライバシーの観点で問題がないことを確認する。また共助トラストエコシステムの拡張のためには、複数の技術ベンダーが参加した場合の相互運用性を担保する仕組みづくりの想定が重要。本実証では台湾でボランティア証明書を発行している Turing Space 社と技術プロファイルを定め、Digital Identity Wallet のコンフォーマンステストを行い、データフォーマットや通信プロトコルの実装時の相互運用性における課題を検討する。

論点②：【ガバナンス観点】実運用を見据えたトラストフレームワークの設計

導出・経緯：昨年度の実証を通じて、適切なトラスト形成のためにはエコシステム内のガバナンス設計が重要であるとの結論に至った。共助実績が価値ある証明書として活用されるためには、発行者の認定（トラストマーク）やデータ項目の共通化が必要となる。

本取組では、先行する共助アプリの認定制度（「シェアリングエコノミー認定制度」等）を参考にしながら、複数のステークホルダ間で合意可能なトラストフレームワークの策定を実施する想定である。2022 年度は深掘りできなかった「Issuer/Verifier の要件」や「運営規則」の項目も含め、実運用を見据えた制度設計を行う。

論点③：【UI/UX 観点】生活者にとって分かりやすいメリットの訴求

導出・経緯：本ユースケースが社会で普及するためには、トラスト検証の範囲が広がることを生活者が実感できる体験設計が重要になる。

本取組では共助実績を蓄積する Wallet のデモ画面を作成し、ユーザーヒアリングを通して UI/UX を検証していく想定。具体的には、共助実績の表示方法や連携方法について共助アプリベンダーと議論しながら、より直感的なユーザー体験によるメリット訴求の方法を検討する。

## 3.2 本事業におけるスコープ

本事業のスコープは以下の 3 点に集約される。

① 技術検証：共助実績の発行、保管、検証のプロトタイプシステム開発と、国際間連携を見据えた Wallet 間の相互運用性テスト
② ガバナンス検討：複数ステークホルダ間で合意可能な共助トラストフレームワークの策定と、実運用に向けたコンソーシアム設立の検討
③ UI/UX 検証：共助実績の活用による具体的なユーザー体験を可視化し、ヒアリングを通じて課題抽出とビジネスモデル検討を実施

これらの検証を通じて、共助アプリ間でのトラスト検証範囲拡大を実現するためのシステム開発、ガバナンス設計、UI/UX デザインを包括的に行うことが本事業のスコープとなる。

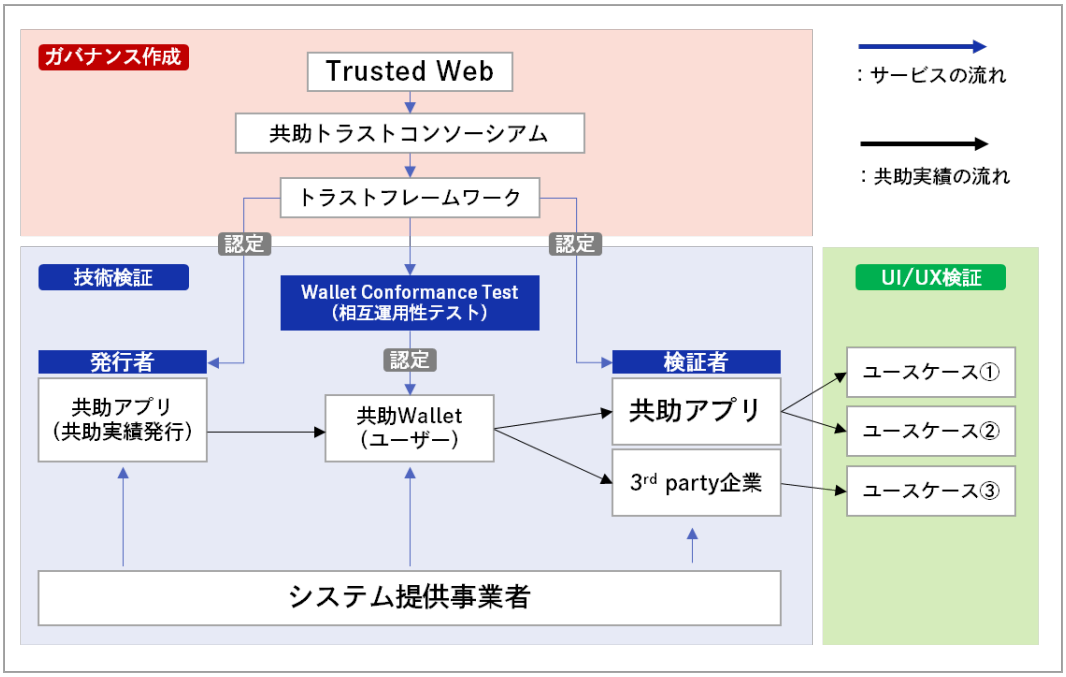



**図 3-2-1：本事業のスコープ図**

また各国の有識者とのディスカッションや実際のターゲットとなる生活者へのインタビューを通じ、本実証に対する客観的な意見を取り入れた。

【技術検証のポイント】

- 共助実績の発行、保管、検証のプロトタイプシステム開発
- 技術仕様の比較と選定
- Wallet Conformance Test 実施（国際間連携）

【ガバナンス作成のポイント】

- 共助トラストフレームワークの作成
- Internet Identity Workshop でガバナンス関連ワークショップ実施
- Open Identity Exchange へのヒアリング調査の実施

【UI/UX 検証のポイント】

- 3 つのユースケースの UI/UX デモ開発
- ユーザーインタビュー、アンケート調査実施
- ビジネスモデル、マネタイズ案の作成

## 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 |
|---|---|---|---|---|
| ①実証ユースケースにかかわるステークホルダ調整 | 実証参加者調整・説明会実施 | • 実証協力事業者に対して説明会の実施、協力内容について認識すり合わせを行う<br>(1社1回/月程度を想定) | • DNP | • 説明会資料 |
| | 実証参加者との契約・合意 | • 実証協力事業者に対して共助トラストエコシステム構築に関する合意契約を締結 | • DNP | • 協業契約書 |
| | UI/UXモックアップ | • 共助WalletのUI/UXを体験できるモックアップを作成し、ユーザーにヒアリングを行う。 | • DNP | • モックアップ<br>• ヒアリング結果 |
| ②プロトタイプシステム開発 | 業務・システム要件定義 | • ユースケースをもとにビジネス要件を定義<br>• 上記ビジネス要件をもとにシステム要件定義 | • DNP<br>• ELEKS | • 業務フロー<br>• 画面遷移図<br>• 機能一覧<br>• システム構成図 |
| | 開発（アプリ・インフラ） | • システム要件定義をもとに開発 | • ELEKS | • アプリ・システム |
| | 単体テスト・結合テスト | • テストケース策定のもとテスト実施 | • ELEKS | • テスト結果 |
| ③実証実験の実施 | 実証実験 | • 共助実績の発行・所有・検証のユースケースについて各共助ベンダーとユーザーの協力の元実証実験実施 | • DNP | • 実証実験結果 |
| | 動画撮影 | • 実証実験の様子・アプリ利用の様子を動画撮影 | • DNP | • 動画 |
| | Plug festの検証結果報告 | • 他社のWalletとの相互運用テストを実施し、結果や課題を報告 | • DNP | • 検証結果 |
| ④必要なルール・ガバナンス整理 | 調査 | • シェアリングエコノミー認証制度等のヒアリングを通じて調査。 | • DNP | • 調査結果 |
| | 取りまとめ、ルール・ガバナンス案の提示 | • 検証論点・調査をインプットにあるべきルール・ガバナンス案の提示 | • DNP | • あるべきルール・ガバナンス(案) |
| 報告書取りまとめ | 実証結果分析 | • 事前に定義した論点の検証結果分析 | • DNP | • 論点検証結果 |
| | 最終報告書作成 | • 開発アプリ・アンケート・調査・検証結果分析等の取りまとめ | • DNP | • 最終報告書 |

**図 3-3-1：実施項目・想定成果物一覧（計画書提出時）**

【プロトタイプシステム開発】

- ✓ 要件定義書
- ✓ 共助 Wallet アプリ
- ✓ 共助 Wallet バックエンド
- ✓ 発行、検証バックエンド

【国際間相互運用性テスト】

- ✓ 技術仕様ドキュメント
- ✓ Turing Space 社（台湾）による Wallet 相互運用性テストの実施
- ✓ テスト結果レポート

【トラストフレームワーク】

- ✓ 共助トラストフレームワークのドキュメント

【UI/UX モックアップ】

- ✓ UI/UX モックアップアプリ

【ユースケース】

- ① 信頼できるプロフィール
- ② 飲料メーカー連携
- ③ 子育てシェア実績連携

【ユーザーヒアリング】

- ✓ UI/UX に関するユーザーヒアリングの結果レポート

## 3.4 スケジュール

### 3.4.1　全体スケジュール

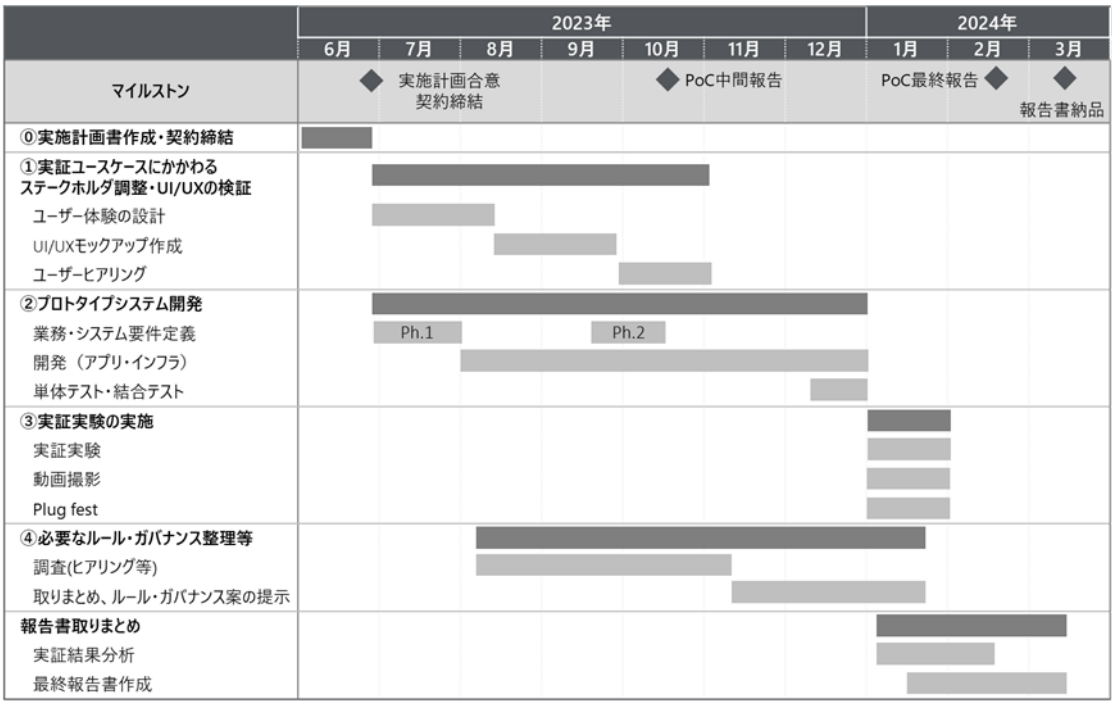
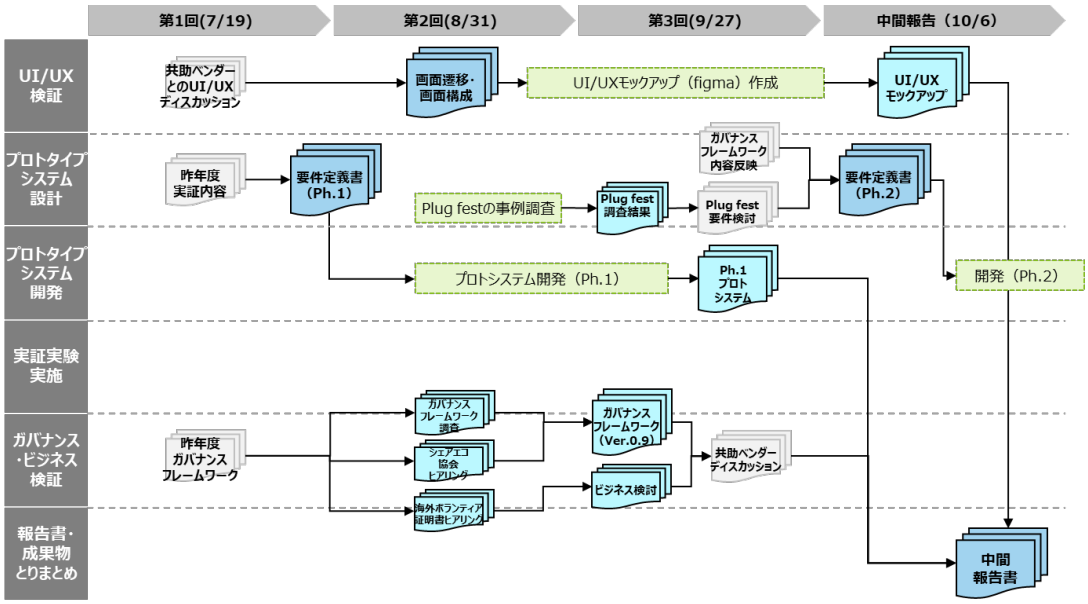



**図 3-4-1：全体スケジュール**

### 3.4.2　成果物の作成フロー




17

**図 3-4-2：成果物作成フロー（前半）**

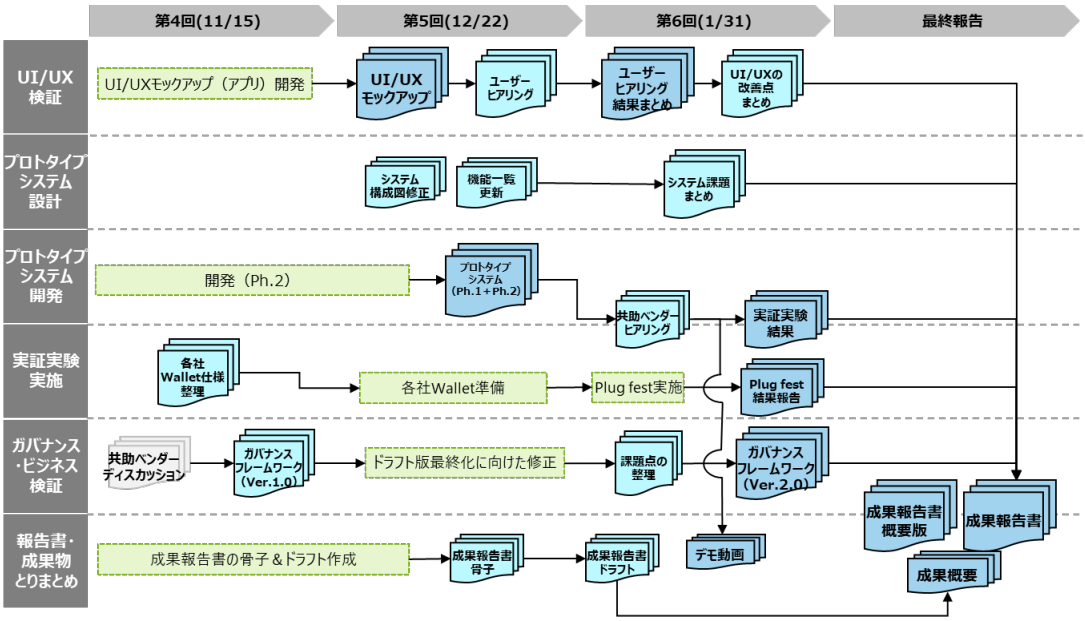



**図 3-4-3：成果物作成フロー（後半）**

## 3.5 実施体制

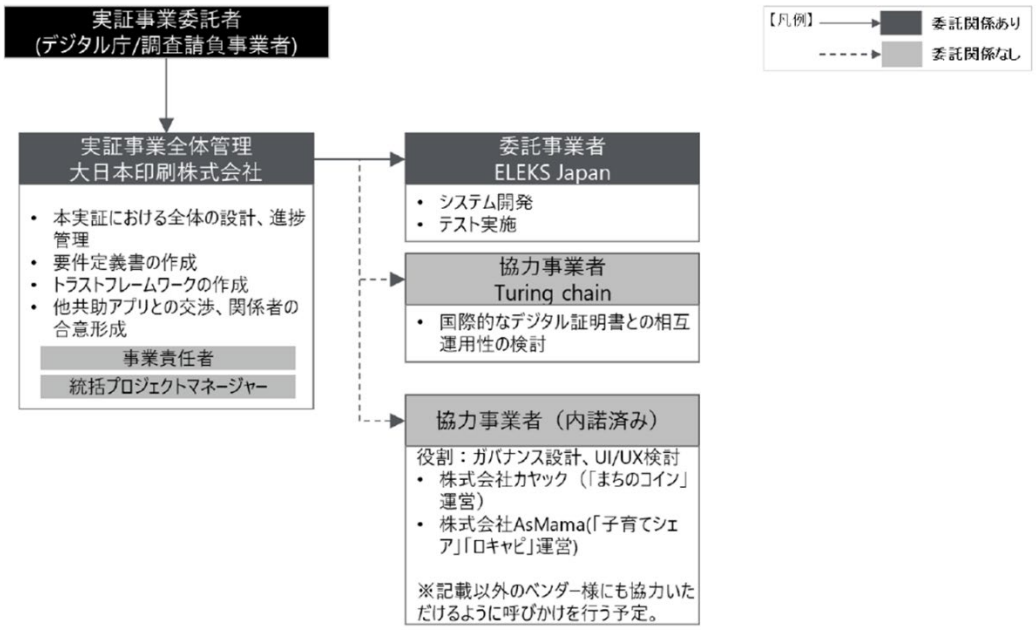



**図 3-5-1：実施体制図**

# 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

2022 年度に検討したシステムアーキテクチャー設計に基づき、Hyperledger Indy/Aries のオープンソースを用いてプロトタイプシステムを開発した。

結果として、共助ユースケースを想定した Wallet アプリのフロントエンドと、VC の発行～検証を行うバックエンドの仕組みを開発して連携することができた。また Anoncreds の Predicate を実装することにより、ユーザーが必要最低限の情報のみを選択して検証者に提示できるようにすることで、生活者のプライバシーを保護しながらクレデンシャルの検証が可能になった。

一方で Anoncreds の実装を通じて、既存のオープンソースのドキュメント整備の課題やデータフォーマット自体の構造の複雑性から実装難易度が高いことが判明した。共助トラストエコシステムにおいて、相互運用性を見据えた標準仕様を策定するために、Wallet Conformance Test では SD-JWT、OID4VCI/VP を技術プロファイルとして指定した。

台湾の Turing Space 社との Wallet 相互運用性テストについては、上記の技術プロファイルを用いて検証を行った。

【論点と検討の経緯】

論点①社会実装を見据えた上で、プライバシーの観点からユーザーが最低限の情報だけを検証者に提示可能なシステムアーキテクチャーをどのように実現できるか、また机上のユースケースで想定したフローにおいて技術的な制約のために実装が困難なシステムとなっていないか（技術的な実現性の検証）。

- 本実証では Wallet アプリをインストールし、端末の持ち主と Wallet アプリの所有者を紐づけ、所有者が自らの Wallet で証明書一覧を確認できるフロントエンドアプリケーションを開発。Wallet アプリに対して共助実績を発行し、また Wallet から提示された共助実績を Verifiable presentation（VP）として検証できるバックエンドシステムと統合した。（システムの機能一覧については 4.4.4 に記載）

- プライバシー保護の観点では、ユーザーが VP を検証者に提示する際に必要最低限の情報だけを共有できるように Anoncreds による Predicate を実装した。これによりユーザーのプライバシーを保護しながらのクレデンシャルの提示が可能になり、検証範囲の拡大とユーザーのプライバシーを両立するシステムとなった。

- また正当なユーザー以外が VC を提示した際に検証できる機能がないと悪用されてしまう可能性があるというセキュリティ上の問題に対しても、Anoncreds に実装されているホルダーバイディングを活用することで VC を発行された正しいユーザーしか利用できないようにした。

- 一方で、当初のユースケースの想定が技術的制約により実装できないという課題も発見した。実現したいユースケースとしては、下図のような“Key”,”value”が点数,1 というクレームを作り、様々な共助アプリから点数を持ち寄り加算するというユースケースを想定。しかし、システム上は

Verifier からの VP のリクエストの際に holder の持っているすべての VC を提示させるようなリクエストが出せない、という問題が生じた。このような技術的制約も存在するため、あらかじめ共助アプリ間でのスキーマに対するルール作りが重要になることが分かった。

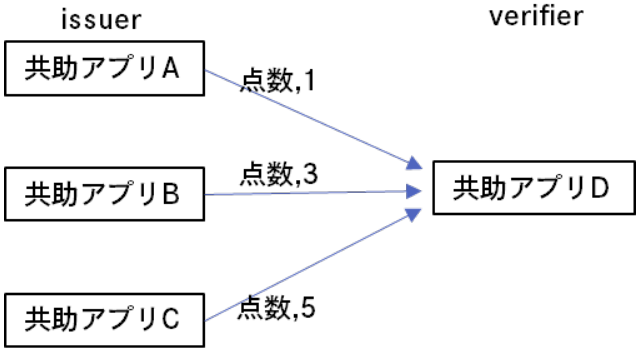



**図 4-1-1：ユースケースの想定**

論点②共助トラストエコシステムにおいて相互運用性を見据えた標準仕様を策定するためにはどのような施策を実施すべきか？

- 本実証では実装しやすい技術であることを重視して技術プロファイルを策定。今後のエコシステム拡大のために参入のしやすさを考慮した。データフォーマットとしては Anoncreds と SD-JWT を比較。下記の通り検討し、現時点で相互運用性の観点を重視する場合には、シンプルな SD-JWT の実装の方がベンダー負担は軽くなるという結論に至った。

【Anoncreds】

- ZKP 暗号を利用したプライバシー保護機能に優れた VC 形式のフォーマットである。
- （検討時点において）既に PoC 等の実装事例があり、他の方式に比べて進んでいた。
- 署名アルゴリズムが、NIST で採択されていない CL 署名を採用しており、セキュリティ面で課題が残る。
- Anoncreds 自体の構造が非常に複雑であることやドキュメントの整備状況に課題をかかえており、実装難易度が高い。限られた事業者内でシステム運営する場合は成立するが、様々な事業者間で証明書のやり取りを想定すると相互運用性の面でハードルが高くなると考えられる。
- Anoncreds ではスキーマごとに少なくとも 1 つの署名鍵が必要になる。基本となるスキーマは存在するが、ユースケースが増加することによりスキーマの種類が増える可能性があり、それに伴い署名鍵も増加する。事業者ごとに鍵管理をしなくてはならず、この管理が負担になると考える。

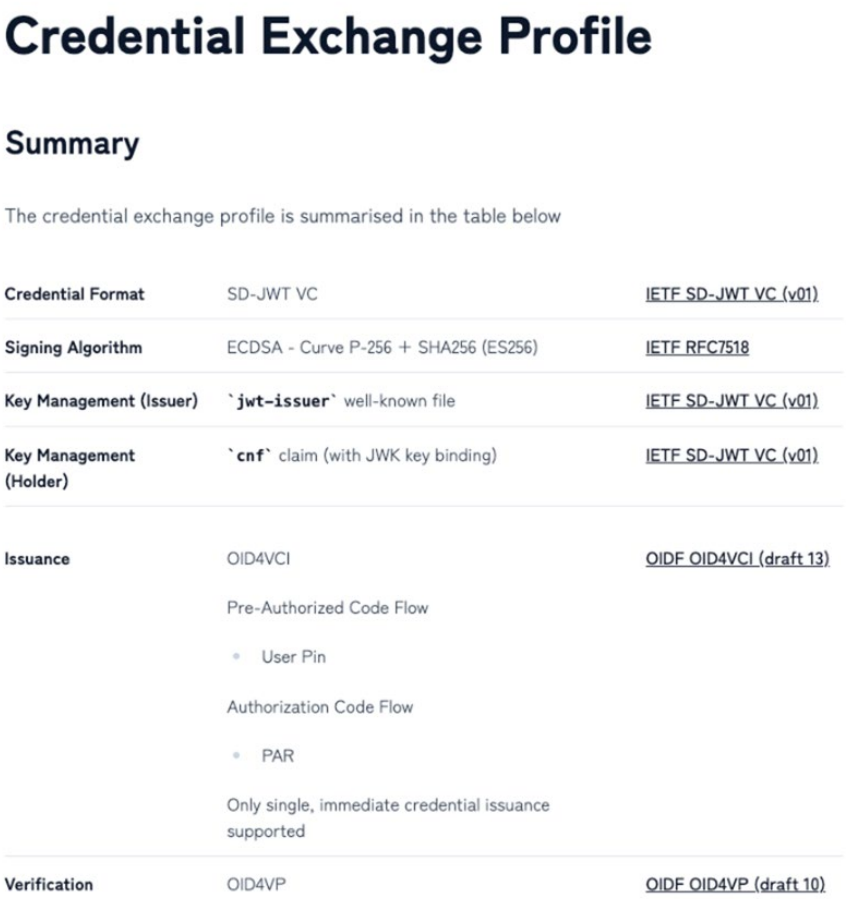
【SD-JWT】

- 構造や検証の仕組みが非常にシンプルであるため、相互運用性の面でのハードルは低いと考えられる。
- 既存の PKI の仕組みを活用した SD-JWT ではスキーマがごとに署名鍵を生成する必要が無いのでこの負担が軽減されると考える。
- EUDIW 等で必須のフォーマットになっており、国際的な相互運用を考えると重要度が高まっている。

（EUDIW のアーキテクチャはあくまでドラフトで今後も変わる可能性がある。）

- 毎回、同一の SD-JWT を検証者に渡すことになるので名寄せが起こる可能性があり、プライバシー面で課題が残る。

上記の比較の結果、下図の通り共助トラストエコシステムの技術プロファイルを策定した。



# Credential Exchange Profile

## Summary

The credential exchange profile is summarised in the table below

| | | |
|---|---|---|
| **Credential Format** | SD-JWT VC | IETF SD-JWT VC (v01) |
| **Signing Algorithm** | ECDSA - Curve P-256 + SHA256 (ES256) | IETF RFC7518 |
| **Key Management (Issuer)** | `jwt-issuer` well-known file | IETF SD-JWT VC (v01) |
| **Key Management (Holder)** | `cnf` claim (with JWK key binding) | IETF SD-JWT VC (v01) |
| **Issuance** | OID4VCI<br>Pre-Authorized Code Flow<br>• User Pin<br>Authorization Code Flow<br>• PAR<br>Only single, immediate credential issuance supported | OIDF OID4VCI (draft 13) |
| **Verification** | OID4VP | OIDF OID4VP (draft 10) |

**図 4-1-2：技術プロファイル**

論点③共助エコシステムの形成において、技術的な相互運用性を担保するための技術プロファイルの作成およびそのテストを実施するために、どのような施策が必要か？

- 本実証では、Wallet の相互運用性をテストするために、共助トラストエコシステムの技術プロファイルを策定し、Wallet のテストができる環境を用意した。

- Turing Space 社の Wallet で OID4VCI の Pre-Authorized Code Flow と Authorization Code Flow、OID4VPのテストをクリア（Same device）。VCの受け取りと提示において、DNP が実装している Wallet との相互運用性を確認することができた。

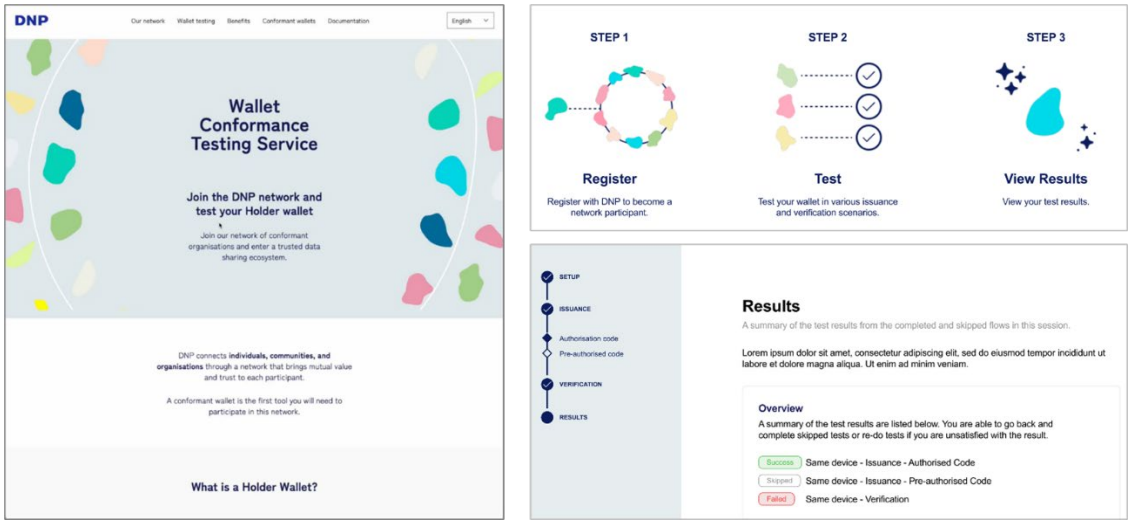



**図 4-1-3：Wallet Conformance サイト**

- Wallet Conformance サイトはネイティブアプリの Wallet を想定していたが、Turing Space 社の Wallet がブラウザ Wallet であったために Cross device でのテストでは挙動が上手くいかなかった。

- 今回のテストで一定の技術的な相互運用性が確認できたため、今後は台湾のデジタルボランティア証明書と日本の共助実績を連携させたユースケース創出を検討していく。

4.1.2 プロ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

プロトタイプシステム開発のための技術検討の調査で、実装しているユースケースの多かった Hyperledger Indy/Aries を選択した。実際に Hyperledger Indy/Aries を使って実装したユースケースは以下の通り[6]。

組織名：SITA

- ユースケース：Happy Traveler Card - Health credential solution in Aruba
- 概要：ハッピー・トラベラー・カードは、Hyperledger Indy、Aries、Ursa を活用し、健康情報を保存・検証するための改ざん防止された分散型システムを構築する。これにより、物理的な書類が不要になり、詐欺やエラーのリスクが軽減される。
- 追加日：2022/5/15

組織名：IDunion

- ユースケース：an open ecosystem for decentralized identity management
- 概要：IDunion 組織の目的は、分散型 ID 管理のためのオープン・エコシステムを構築することである。すべての人（自然人だけでなく法人や物も含む）が、自分の ID 情報を自分で管理し、この情報をいつ誰と共有するかを決定できることを目指す。

[6]「Hyperledger ユースケーストラッカー」https://www.hyperledger.org/learn/use-case-tracker

- 追加日：2022/8/23

組織名：Instnt

- ユースケース：Instnt Access - Portable KYC Solution
- 概要：Instnt Access は、Instnt のプラットフォームの上に構築され、W3C VC フレームワークと Hyperledger の Indy、Aries Mobile Agent、AFJ、ACA-PY、URSA を活用して、パスワード不要のログインとポータブルな認証情報を提供する。
- 追加日：2023/3/18

組織名：BRITISH COLUMBIA

- ユースケース：Energy & Mines Digital Trust
- 概要：Energy & Mines Digital Trust（EMDT）は、カナダのブリティッシュ・コロンビア州政府が TELUS と共同で開始したプロジェクト。EMDT の主な目的は、天然資源部門（特に鉱業）にデジタル・トラスト・ソリューションを提供し、企業が持続可能性の実践を証明できるようにすることである。
- 追加日：2023/7/3

組織名：DICE ID

- ユースケース：Decentralized Identity and Credential Exchange
- 概要：Hyperledger Indy と Aries を利用する DICE ID は、ユーザー所有の ID Wallet に保存された、自己検証可能で改ざん防止措置がなされたデジタル認証情報の発行と検証を可能にすることで、ユーザーに個人データの管理権限を与える。
- 追加日：2024/2/6

### 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

- 共助アプリユーザー（生活者）

  【役割】

  - 共助アプリを利用してサポーターを選び、自らの困りごとを解決してもらう。サポートを受けた後はサポーターを評価する場合もある。

  【実証事業において設定した要求事項】

  - 共助アプリを通じて自身の困りごとを解決したい生活者。マッチングするサポーターを選ぶために、様々な情報を基にサポーターのトラストを検証する。

- 共助 Wallet ユーザー（所有者）

  【役割】

  - 共助実績証明書を自らの Wallet で管理し、別の共助アプリを使う際に Wallet から共助実績を連携する。

  【実証事業において設定した要求事項】

  - 共助実績証明書を別の共助アプリに連携したり、共助エコシステム外の第三者に提示したりことにより、従来は可視化されていなかった自身の共助実績が可視化され、新たなインセンティブを獲得することができる。

- 共助アプリ（発行者）

  【役割】

  - 共助アプリを通じてユーザーをサポートする生活者。プロフィール欄にアピールポイントを記載し、ユーザーが選択しやすくなるように情報を提供する。マッチング後はユーザーに対してサポートを実施する。

  【実証事業において設定した要求事項】

  - 共助実績証明書をサポーターに発行することで、生活者同士で手助けをするインセンティブを与え、共助を促進したい。

- 共助アプリ（検証者）

  【実証事業において設定した要求事項】

  - 他の共助アプリで蓄積された実績データを流用することで、サポーターのトラストを向上させ、自社の共助アプリユーザーが安心してサービスを利用できる状況にしたい。

- 共助トラストエコシステム運営者（Wallet 提供者）

  【役割】

  - Wallet を提供し、トラストフレームワークが適切に運営されているかを管理する。Wallet に蓄積される共助実績の価値を高めたい。

  【実証事業において設定した要求事項】

- Wallet アプリを開発し、共助アプリサポーターに提供する。また共助実績を発行・検証する機能を SDK として各共助アプリに提供し、エコシステムを形成する。

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

ペイン：ユーザーのトラスト検証には、現在の方法ではユーザーの自己申告に基づいており、内容の信ぴょう性を検証する方法がないという問題がある。また、共助サービスの中には、アプリ内のユーザー評価システムを利用してトラスト検証を行っているものもあるが、単体で十分な実績を提供できるほどの規模がない共助サービスも多い。

解決方法：この問題を解決するための仮説として、アプリを横断して共助実績データを蓄積し、ユーザーのトラストの検証範囲を拡大する。

活用する企画・技術：この際に活用する規格・技術としては、分散型 ID システムが選ばれている。
技術選定理由：集中型のデータベースを中心にしたエコシステム形成は実現性に乏しいため、分散型 ID システムの技術を活用し、共助実績を Verifiable Credential（VC）として連携する。

**表 4-2-1：ペインと解決方法**

| ペイン | 解決方法 |
|---|---|
| 【holder】<br>共助アプリ内の活動履歴の証明が自己申告を基にしているため、信頼される証明にならない | 共助アプリ内の活動内容を検証可能な証明書（VC）形式で発行することで、検証者となる他の共助アプリや他業界のサービスにおいて VC を検証することができ、信頼できるデータとして認められる可能性が高い。 |
| 【verifier】<br>提示された活動履歴の内容が共助アプリサポーターの活動を正しく反映していない可能性がある（サポーターの都合のよい情報しか提示していない可能性がある） | 共助トラストフレームワーク（コンソーシアム）において、各共助アプリベンダーが共通で使用する共助実績スキーマを設計し、検証者が検証しやすいクレームを検討する。 |
| 【holder】<br>適切な相手に対して、適切な範囲の属性情報を共有できるようにしたい | Anoncreds 形式の VC を利用することで、属性情報の開示範囲や開示の可否を自身でコントロールできるようになり、適切な範囲の属性情報を共有できるようになる。 |

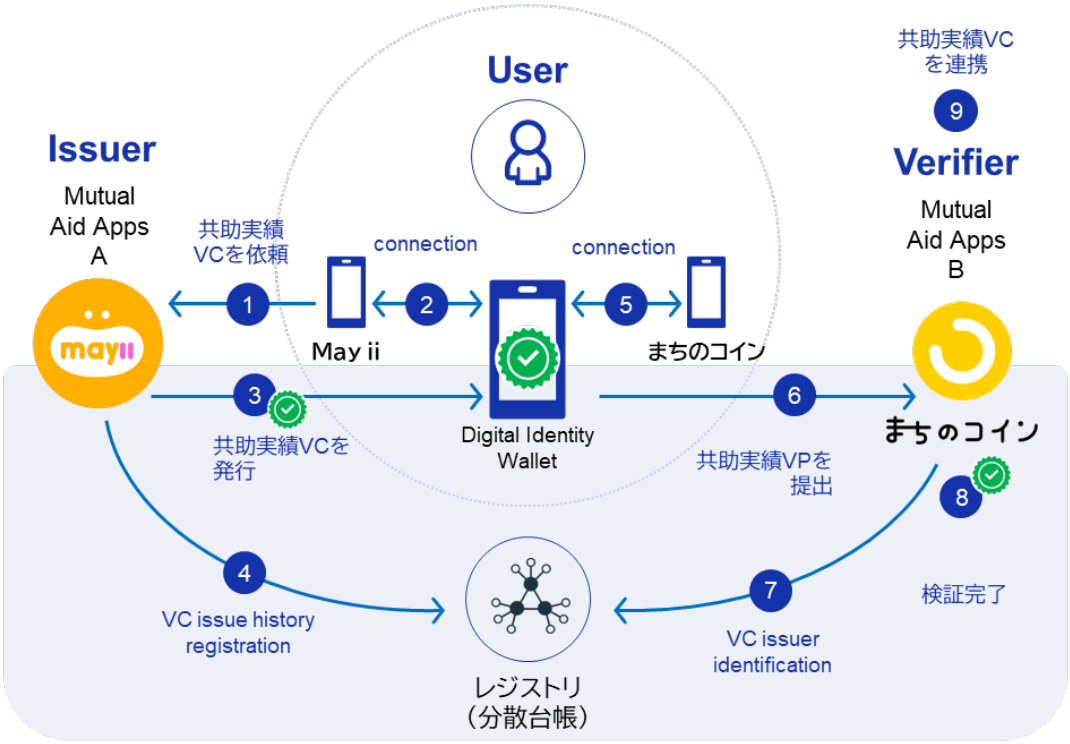



**図 4-2-1：共助アプリエコシステムイメージ**

### 4.2.3　Verify するデータ一覧

共助実績 VC にかかる検証概要について以下表にて示す。

**表 4-2-2：verify データ一覧**

| 項目 | 説明 |
|---|---|
| 検証によって解決したい課題 | 共助サービスを横断したトラストレベルが高い共助実績の連携を実現するため、下記の内容を確認する。<br>• 共助実績の内容が改ざんされていないことの確認<br>• コンソーシアムに所属している正当な発行者から発行された共助実績であることの確認 |
| 検証対象のデータ・そのやり取り | 共助アプリ（発行者）は共助アプリ（発行者）サービスでの活動を通じて蓄積した実績情報をもとに生成した共助実績 VC を共助アプリサポーターの Wallet アプリに発行する。 |
| 検証方法 | 共助アプリサポーターから提示された共助実績 VP の署名を検証し、改ざんされていないことを確認するとともに、発行者や有効期限切れでないかといったクレームの妥当性を検証する。 |
| 検証者 | 共助アプリ（検証者） |
| データの保有者 | 共助アプリサポーター |
| 発行者 | 共助アプリ（発行者） |
| データの置き場所 | 共助アプリサポーターのみがアクセス可能な Cloud Wallet |
| アクセスコントロールの手法 | Wallet アプリ起動時の本人認証（PIN 入力） |
| 成果・留意点 | サポーターの共助実績に関するトラスト検証範囲の拡大やトラストレベル向上が期待できる。 |

4.2.4　証明書要件・識別子要件

**表 4-2-3：証明書要件**

| | 説明 |
|---|---|
| 証明書の名称 | 共助実績証明書（VC） |
| 証明書に記載されている情報 | • 発行日、有効期限<br>• 発行者（Credential Definition に紐づいた ID）<br>• サービスカテゴリ、サポート活動完了件数、サポート活動総時間、サービスアカウント作成日<br>• ユーザーバインディング情報 |
| 要件 | • 本 VC は Anoncreds を採用し、VC を発行した共助アプリ（発行者）の署名検証および、共助アプリサポーターが提示した VP の署名検証により、真正性が確認できる。<br>• サポート活動完了件数、サポート活動総時間の情報は、～件以上、～時間以上活動しているかのような predicate 形式でリクエスト可能とする。<br>• 有効期限の情報により、検証者が失効管理を行う。（有効期限内か否かを判定するロジックは本システムに実装していない。） |

**表 4-2-4：識別子要件**

| 識別子 | 説明 |
|---|---|
| 共助アプリ（発行者）ID | • 発行者を識別する ID で、共助実績証明書（VC）の発行者クレームに記載される。<br>• 検証者は、識別子から VDR に置かれている署名検証用の公開鍵を取得でき、共助アプリサポーターが提示した VP の署名検証を行うことができる。 |

4.3 合意形成・トレースの仕組み

**表 4-3-1：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**

| 項目 | 説明 | |
|---|---|---|
| | No.1 | No.2 |
| 合意の主体 | 共助アプリ（発行者）と共助アプリサポーター | 共助アプリサポーターと共助アプリ（検証者） |
| 合意の対象 | サポーターが実施した共助実績情報（VC） | サポーターが実施した共助実績情報（VP） |
| 合意の条件 | 共助アプリ（発行者）が VC として発行する共助実績 VC の内容を Wallet アプリを通じて共助アプリサポーターへ提示し、共助アプリサポーターが承認することで合意されたこととする。 | 共助アプリ（検証者）が要求する情報を提示し、共助アプリサポーターが開示する内容を選択、VP の共有を承認することで合意されたこととする。 |
| トレースの対象 | 共助アプリ（発行者）と共助アプリサポーターとの間でやり取りした VC に関する合意 | 共助アプリサポーターと共助アプリ（検証者）との間でやり取りした VP に関する合意 |
| トレースの主体 | 共助アプリ（発行者）と共助アプリサポーター | 共助アプリサポーターと共助アプリ（検証者） |
| トレースの手法 | 共助アプリ（発行者）は、VC 発行システムのログ機能により、また共助アプリサポーターは、Wallet アプリの VC 受領ログを確認することで、2 者間で合意した内容（VC 発行履歴）を確認することができる。 | 共助アプリサポーターは Wallet アプリの VP 提示ログを、共助アプリ（検証者）は VP 検証システムログ機能を確認することで、2 者間で合意した内容（VP提示履歴）を確認することができる。 |
| 合意取消の可否・方法 | 可能。hyperledger Aries の revocation 機能により VC を無効化することは技術的に可能であるが、本システムでは実装していない。 | 不可。 |

## 4.4 企画・開発物

### 4.4.1 業務フロー

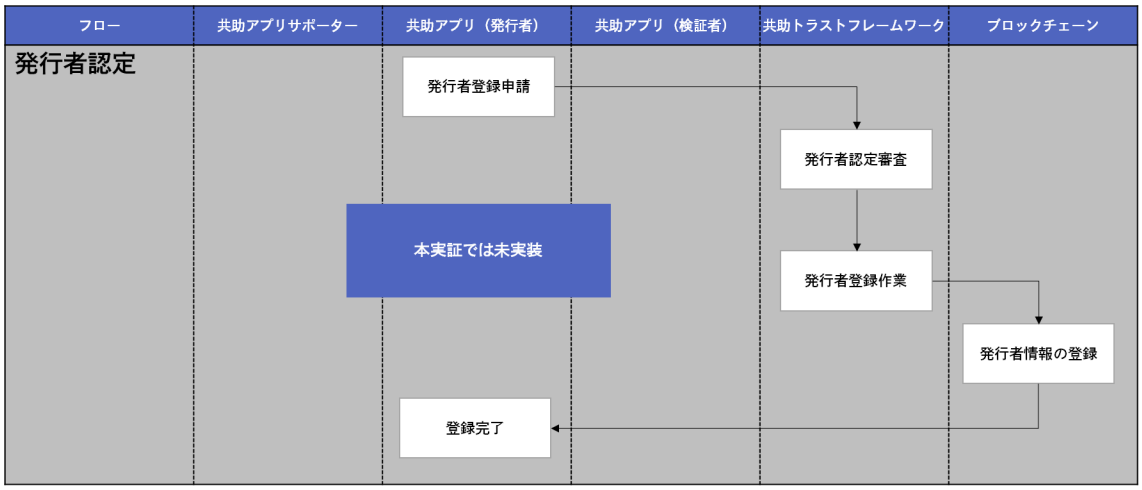



**図 4-4-1：業務フロー（発行者認定）**

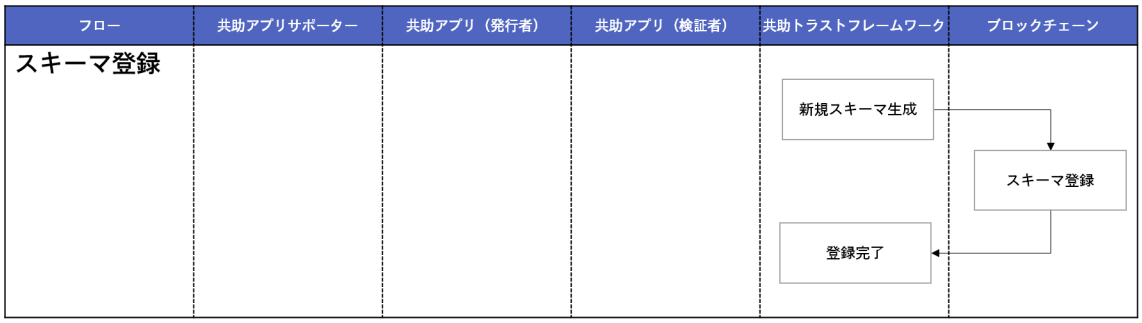



**図 4-4-2：業務フロー（スキーマ登録）**

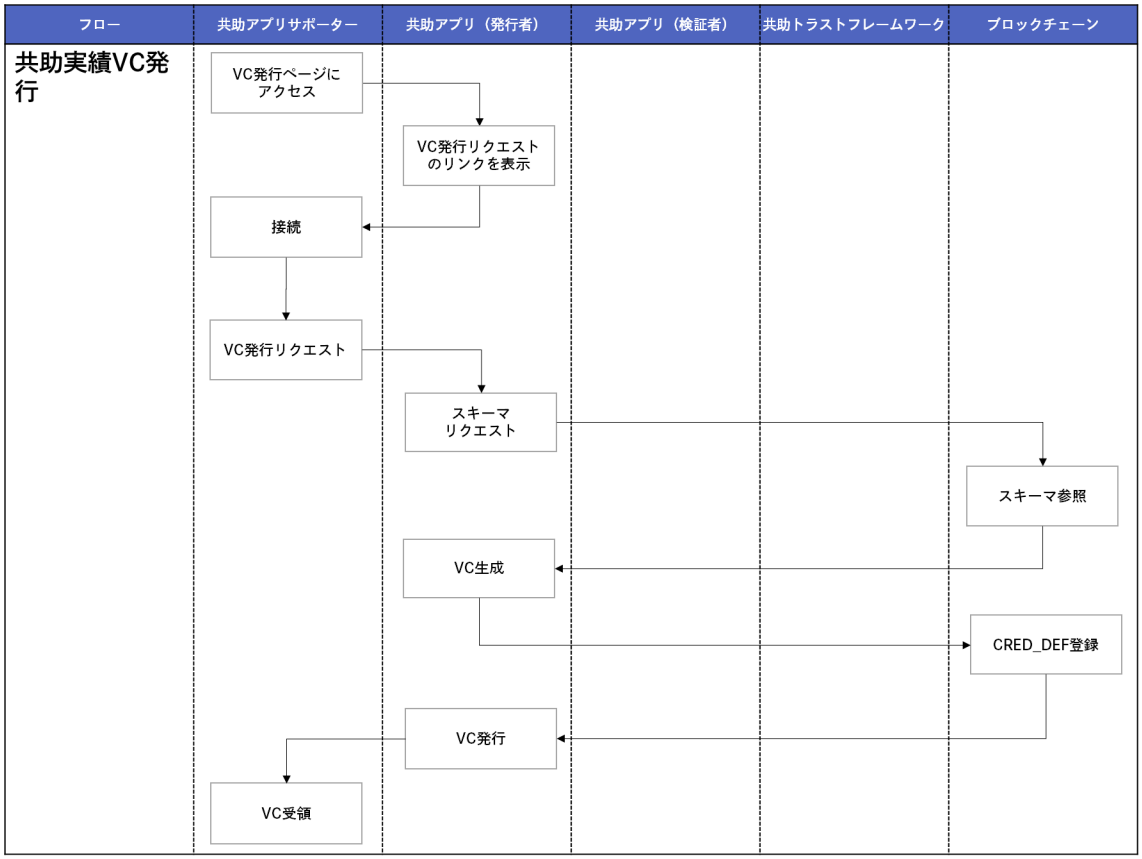



**図 4-4-3：業務フロー（共助実績 VC 発行）**

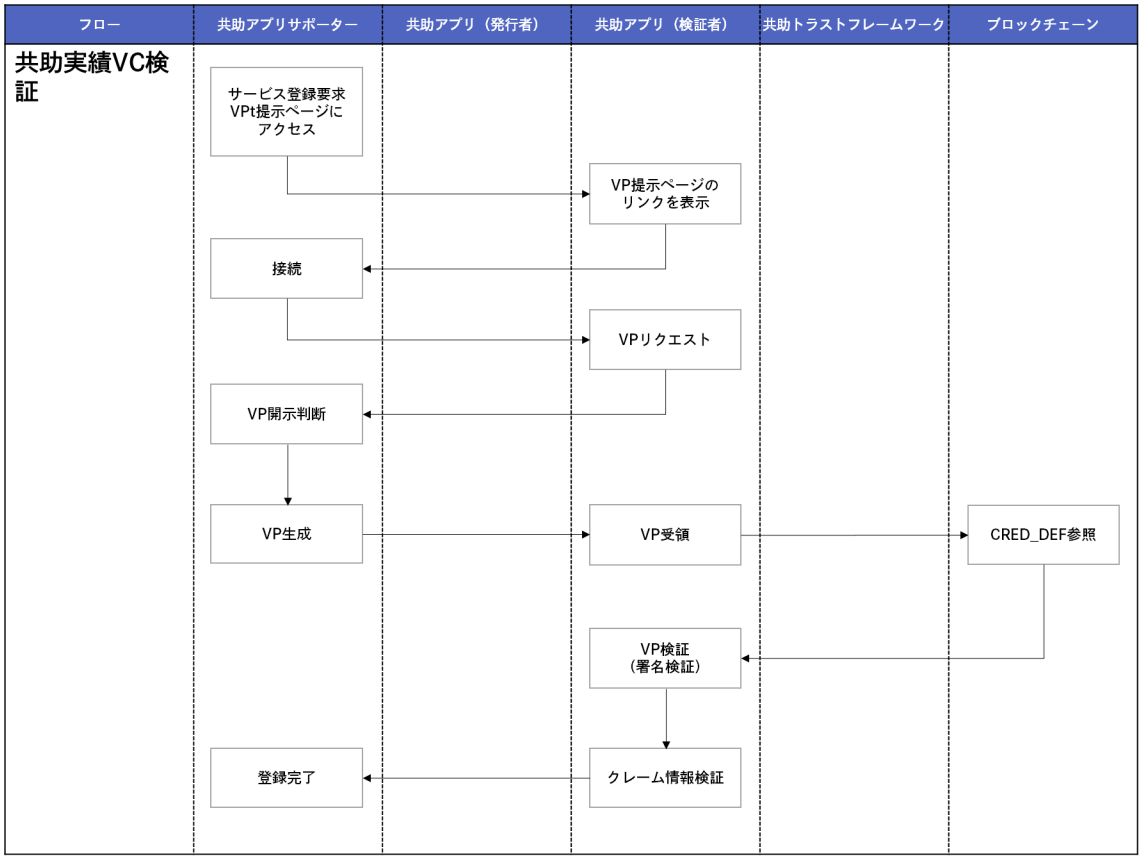



**図 4-4-4：業務フロー（共助実績 VC 検証）**

### 4.4.2　ユースケース図

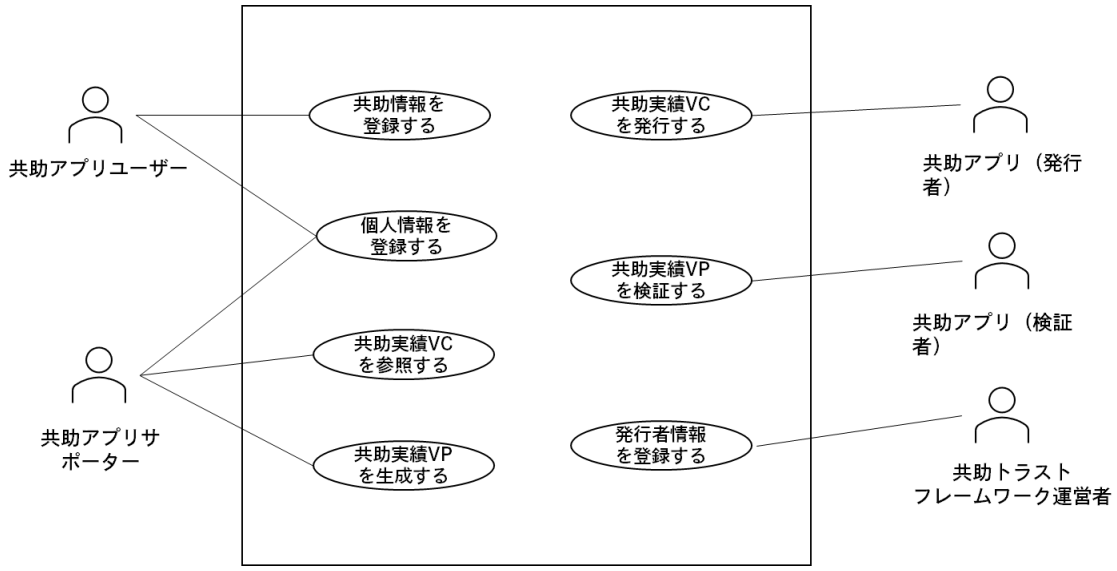



**図 4-4-5：ユースケース図**

### 4.4.3　操作画面（UI）


**図 4-4-6：操作画面（UI）**

4.4.4　機能一覧/非機能一覧

**表 4-4-1：機能一覧**

| | | |
|---|---|---|
| ログイン | ログイン | • ユーザーID/PW を入力してログインする。(このフェーズでは新規会員登録機能は実装せず、DB に直接登録する。) |
| | ログアウト | • ログアウトし、ログイン画面に遷移する。 |
| 資格証明書 | 証明書一覧参照 | • 自分の保有している証明書を一覧で表示する。<br>• 証明書を選択すると証明書詳細画面に遷移する。 |
| | 証明書詳細参照 | • 選択した証明書の詳細を表示する。 |
| | 証明書削除 | • 選択した証明書を削除する。<br>• 証明書詳細画面から操作し、削除前には確認のメッセージを表示する。 |
| オファー | オファー一覧 | • Issuer からの証明書発行の許可依頼（オファー）を一覧で表示する。<br>• オファーを選択するとオファー詳細画面に遷移する。 |
| | オファー詳細 | • 選択したオファーの詳細を表示する。 |
| | オファー承認 | • オファーを承認し、証明書を発行する。<br>• オファーのステータスを「承認済み」に変更する。 |
| | オファー却下 | • オファーを却下し、証明書発行を受け付けない。<br>• オファーのステータスを「却下」に変更する。 |
| 証明リクエスト | 証明リクエスト一覧 | • Verifier からの証明提示リクエストを一覧で表示する。<br>• リクエストを選択すると証明リクエスト詳細画面に遷移する。 |
| | 証明リクエスト詳細 | • 選択した証明リクエストの詳細を表示する。 |
| | Claim 選択 | • 証明リクエストに対して、保有している証明書から Verifier に提示する Claim を選択する。 |
| | VP 提示 | • 選択した Claim に基づいて VP を生成し、Verifier に提示する。<br>• 提示された VP を検証し、検証結果に基づいて証明リクエストのステータスを「成功」または「却下」に更新する。 |
| | 任意項目設定 | • 証明リクエストの任意項目については、対象の Claim の選択有無に関わらず VP を生成する。<br>例）リクエスト内で Claim「性別」が任意項目に設定されていた場合、ユーザーは「性別」を含めない VP を提示できる。 |
| | 条件項目設定 | • 証明リクエストの条件項目については、選択した Claim がその条件を満たすか否かの bool 値のみを提示する。<br>例）リクエスト内で「合計サポート時間＞2」の条件が設定されていた場合、ユーザーは「合計サポート時間」の値を Verifier に渡さず、2 より大きいかの判定結果（True/False）のみを Verifier に提示する。 |

| | | |
|---|---|---|
| | 証明リクエスト却下 | • 証明リクエストを却下し、VP を提示しない。<br>• 証明リクエストのステータスを「却下」に変更する |

**表 4-4-2：非機能一覧**

| | | |
|---|---|---|
| サービス可用性 | システムの提供時間（稼働時間） | • 本システムは実証期間中、メンテナンス期間を除いた 24 時間 365 日をサービス提供時間とする。ただし、実証期間外はシステムの稼働を停止する |
| | サービス停止について | • 実証中においてメンテナンスの必要が生じた場合、システム停止を計画・実施する。 |
| | 目標復旧時間 | • 原則、AWS の SLA レベルに準拠するが、AWS に依存しない部分の障害は 2 営業日以内の復旧を目標とする |
| | 目標稼働率 | • 実証期間中において、オンライン系の処理については 90.0%（実証期間が 30 日の場合は累計停止時間 72 時間目標） ※ただし、AWS の障害やメンテナンスは除く |
| | 耐障害性（冗長性） | • プロトタイプシステムのため、耐障害性を考慮した冗長構成は対象外とする（コスト削減を優先する） |
| | AWS サービスリソース構成可用性 | • プロダクト化する際は以下を実施して可用性を高める<br>• 同機能の AWS 構成リソースを異なる Availability Zone に分散配置する |
| | データベース可用性 | • プロダクト化する際は以下を実施して可用性を高める<br>• Aurora Replica を異なる Availability Zone に分散配置する<br>• 障害が発生した場合や AWS 側の都合によるメンテナンスが発生した場合、フェイルオーバー（予備のものに切り替え）には数十秒程度で完了する構成で作成する。 |
| | 災害対策 | • プロトタイプシステムのため、分散配置等による災害時への対策は対象外とする<br>• プロダクト化する際は AWS の構成をマルチ Availability Zone 構成にし、分散配置することで災害時の影響を分散させる。 |
| データ要件 | 個人情報 | • プロトタイプシステムのため、個人情報は扱わない。<br>• DB および Credential の定義上は個人情報に相当する項目の定義を行うが、実証ではダミーデータを使用する。 |
| | クライアント利用環境 | • 利用環境としては以下のデバイス、OS を推奨環境とする<br>デバイス：iPhone<br>OS：iOS 16.x |
| | データベースのバックアップ | • データベース上のデータは Amazon Aurora 標準機能によるバックアップが取得する。 |

| | | |
|---|---|---|
| | データ削除 | • 実証期間が終了した時点でデータを一括削除する提示された VP を検証し、検証結果に基づいて証明リクエストのステータスを「成功」または「却下」に更新する。 |
| システム性能要件 | データ容量 | • 実証期間において Credential Schema の定義は 1 種類とする<br>• 実証期間中の想定容量は以下を想定する<br>➢ Holder 数：1000<br>➢ Holder あたりの Credential 数：100<br>➢ Offer テンプレート種類：100<br>➢ Proof Request テンプレート種類：100 |
| | 業務処理要件 | • 実証期間における業務処理量は以下を想定する<br>【VC 発行数】<br>・定常時：200 件/日 ※VC 作成数＋作成済み最大 Holder 数の 1%の利用を想定<br>・ピーク時：120 件/時 ※VC 作成数のピーク時の 1.2 倍を想定<br><br>【VC 検証数】<br>・定常時：1,000 件/日 ※最大 Holder 数の 10%と仮定<br>・ピーク時：333 件/時　※定常時の 1 日分の件数の 1/3 がピークの 1 時間に集中想定 |
| システムセキュリティ要件 | アクセス管理 | • 必要最低限のアクセス制限、IP アドレス・ポート開放により、実証に必要な最低限の通信のみ許可するアクセス制御を行う<br>• 外部ネットワークから AWS のバックエンドまでの経路については暗号化通信（TLS1.2, TLS1.3 を使用する） |
| | 開発時のセキュリティ | • プロトタイプシステムのため、脆弱性検査等は対象外とする。 |

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）

**表 4-4-3：非機能検討一覧**

| サービス利用にかかるリスク | 影響度 | 発生可能性 | 対応方針 |
|---|---|---|---|
| Wallet アプリが格納されたデバイスの紛失 | 悪意のあるユーザーに Wallet アプリにログインされ悪用されてしまう可能性がある。 | Wallet アプリはスマートフォンなどのデバイスは日常的に持ち運ぶものなので、置き忘れなど発生する可能性がある。 | ログイン時には PIN 入力で本人確認をすることで、登録したユーザー以外ログインをすることができない。 |

| | | | |
|---|---|---|---|
| VC の改ざん | 改ざんされた VC を提示することで、実績のないユーザーが評価され、エコシステムの信頼が低下する可能性がある。 | 改ざんされていないことを検証できる機能がないと、VC の内容を簡単に変えることができてしまう可能性がある。 | デジタル署名の検証を行うことで、証明書の完全性を検証する。 |
| VC の盗難 | 悪意のあるユーザーに VC が奪われ、悪用されてしまう可能性がある。 | 正当なユーザー以外が VC を提示した際に検証できる機能がないと悪用されてしまう可能性がある。 | Anoncreds にはホルダーバインディングが実装されているので、VC を発行された正しいユーザーしか利用できない。 |
| 検証者（共助アプリ、学校、企業）による VP に含まれる個人情報の不適切利用・データコピー | ユーザーの個人情報の漏洩などが発生する可能性があり、ユーザーのプライバシー侵害に繋がる。 | システム外での VC/VP 情報の取扱いはトレースできないため、不正利用やデータコピーされてしまう可能性がある。 | システム外に波及したデータトレースは困難であるため、検証者に対して、利用規約の同意を行うことや、教育・啓蒙活動をコンソーシアム等を通じて行うことが必要になると考えられる。 |
| 不正な共助実績の形成 | 不正が発生することで、ステークホルダからサービス（実績情報）に対する信頼が低下する可能性がある。 | 同じサービスに登録している複数のユーザーが協力関係にあると、実施していない不正な共助実績や不正な評価を登録できてしまう可能性がある。 | 共助サービス側で共助について監視を行い不正検出することで、ある程度のリスクは抑制できる。 |
| 発行者（共助アプリ）の身元確認 | 不正な発行者から不正な VC が発行され、コミュニティ内で流通すると、このコミュニティ内の VC/VP に対する信頼が低下する可能性がある。 | 誰でも発行者になることができてしまうと、不正な発行者が不正な VC を発行してしまう可能性がある。 | コンソーシアム等で発行者を認定するなどすることで、ユーザーや検証者は認定発行者からの VC か否かを判断できるようになる。 |

#### 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】**

今後の社会実装時には相互運用性を重視し、Hyperledger Indy/Aries のオープンソースを使った Anoncreds ではなく、シンプルな構造の SD-JWT のフォーマットの実装を優先することを想定している。

またシェアリングアプリを含む共助アプリ提供会社は日本において 300 社以上存在しており、本実証の

共助トラストエコシステムについても将来的には数十万人～数百万人のユーザー数をカバーできるシステムの実装が求められる。プロトタイプシステムの開発を通じて想定する規模感へのスケーリングのためには下記課題があることが分かった。

**表 4-4-4：Anoncreds の社会実装時の課題**

| 課題 | 説明 |
|---|---|
| 署名鍵の増加 | エコシステムの参加者が増加し、それに伴い事業者も増加すると、VC を発行する際に必要な署名鍵の数が膨大になる可能性がある。<br><br>Anoncreds ではスキーマごとに少なくとも 1 つの署名鍵が必要になる。<br>基本となるスキーマは存在するが、ユースケースが増加することによりスキーマの種類が増える可能性があり、それに伴い署名鍵も増加する。<br>事業者ごとに鍵管理をしなくてはならず、この管理が負担になると考える。<br><br>SD-JWT ではスキーマごとに署名鍵を生成する必要が無いのでこの負担が軽減されると考える。 |
| 処理時間 | 事業者が増えると、台帳に書き込まれる DID document が増えるため、DID を解決する時間が増加し、検証に時間がかかる恐れがある。 |

### 4.4.5　データモデル定義

**表 4-4-5：データモデル**

| 属性値（日） | 属性値（英） |
|---|---|
| ID | ID |
| 発行日 | Issued Date |
| 有効期限 | Expiration Date |
| 発行者／サービス運営者 | Issuer / service operator |
| サービス区分 | Service Category |
| サービス契約日 | Service Signup Date |
| サービス内容 | Description |
| サポートタスク完了数 | Support Task Completions |
| 総サポート時間 | Total Support Hours |
| ユーザーバインディング属性 | User Binding Attributes |
| -名前 | -Name |
| -金融機関 ID | -Financial Institution ID |

### 4.4.6　実験環境

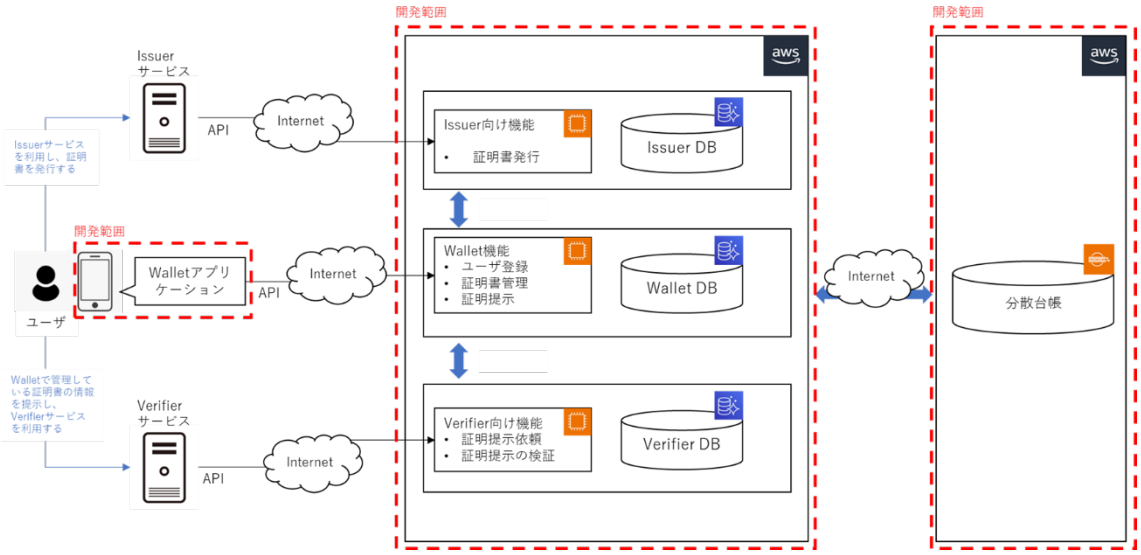



**図 4-4-7：実験環境**

4.4.7　システムの構成要素

**表 4-4-6：システム構成要素**

| コンポーネント名称<br>(システム・ライブラリ名) | 開発区分<br>(新規/既存) | 開発先/<br>権利の帰属先(OSS) | 型式名・ライセンス名/OSS 名 |
|---|---|---|---|
| Hyperledger Indy<br>/Aries | ― | OSS | Linux Foundation |
| 外部ストレージ | クラウド環境等 | 各ベンダーが権利を保有 | 各ベンダー |
| モバイルデバイス | Android | Google 社が権利を保有 | Google Inc. |
| モバイルデバイス | iOS | Apple 社が権利を保有 | Apple Inc. |

# 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

共助トラストフレームワークのドキュメントを作成。各国の有識者との議論を通じ、ステークホルダの責任分解点を整理した。

論点①：共助トラストフレームワークにどのような項目を含めるべきか。

結果：

- トラストフレームワークの内容を共助アプリベンダーとともにディスカッション。最終的に OIX[7]のホワイトペーパーとも整合性のある項目に整理した。

論点②：エコシステム内のリスクを最に抑えるためにどのようなルールを検討すべきか。

結果：

- Issuer/Verifier の要件を定め、ユーザーが安心して利用できるエコシステム形成を目指した。
- エコシステムの運営方針に関しても組織形態や権限について定めた。

論点③：エコシステム外のステークホルダ（政府）の役割は何か。

結果：

- 各国の有識者との議論を通じ、エコシステムにおける政府の役割を整理。リスクを抑えるためのガイドライン作成が政府に求められていることが明らかになった。

論点④：トラストフレームワークの運用における各ステークホルダの責任分界点を明らかにする。

結果：

- エコシステム内外のステークホルダを整理し、それぞれの責任分界点について図式化した。
- 各フェーズで起き得るトラストの問題についても可視化した。

### 5.1.2 実証ユースケース概要・実施内容・手法

共助トラストエコシステムを運営するためのトラストフレームワークを作成。3 つのポイントに留意して、下記項目に落とし込んだ。

ポイント①：シンプルで再現性のある項目設計

OIX が世界各地のトラストフレームワークを研究して共通項を抽出した「General Policy Rules」を参考に本実証のトラストフレームワークの項目を検討した。他のエコシステムでも参考にできるように可能なシンプルで再現性の高い設計を目指した。

ポイント②：Issuer/Verifier の要件を設定

[7] The Open Identity Exchange

共助実績の発行者と検証者の要件を設定し、ユーザーが安心して利用できるエコシステム形成を目指した。発行者の要件については、シェアリングエコノミープラットフォーマーに対する ISO の規格を援用することで、事業者が遵守すべき事項を明示した。

ポイント③：エコシステム運営組織のガバナンス

共助トラストフレームワークを社会実装して運用することを想定し、ガバナンスの運営組織の形態と各ステークホルダの権限についても議論した。初期のボードメンバーを運営の中心に据えつつ、今後のエコシステムへの参加者増加を視野に入れた運営方針を取りまとめた。

また Open Identity Exchange の最新のホワイトペーパー『Digital ID DNA Interoperability across Trust Frameworks』[8]（2023.10.25）ではトラストフレームワークに含まれている項目が「General Policy Rules」と「Identity Assurance Policy」の 2 軸で整理されている。本実証で作成した共助トラストフレームワークの項目と比較した結果、General Policy Rules の検討項目では大きな乖離はなかった。
一方で、Identity Assurance Policy については、より複雑な議論が包含されており、今後の検討で深堀する必要があることことが分かった。『Digital ID DNA Interoperability across Trust Frameworks』の General Policy Rules は下記の通り。

【General Policy Rules】
・Roles ：各ステークホルダーの役割
・Governance Approach ：エコシステムの目的及び原則
・Trustmark ：トラストマークを発行するかどうか、誰がそれを表示する必要があるか
・Inclusion / Equity / Accessibility ：包括性／公平性／アクセシビリティの方針
・User Account Management ：アカウントの閉鎖や一時停止のトリガー、不正行為の処理方法等
・Liability ：エラーや不正行為に対して誰が責任を負うか
・Complaints and Disputes ：苦情や紛争が起きた時のプロセス
・Data Management ：データ保護とプライバシーポリシーのアプローチ
・Record Keeping ：データ保持についての方針
・Risk and Incident Management ：リスクとインシデント管理について
・Fraud Management ：不正対策の方法について
・Relying Party Requirements ：検証者の要件について
・Prohibitions ：禁止事項
・Technical and Security Policy ：エコシステムで標準的に使われる技術スタックについて
・Trust Registry ：証明書の検証に関する方針
・Credential Standards ：クレデンシャルのフォーマット・失効について

[8]『Digital ID DNA Interoperability across Trust Frameworks』（2023.10.25）
https://openidentityexchange.org/networks/87/item.html?id=708

Identity Assurance Policy は下記プロセスでの検討検討が推奨されている。Identity Assurance Policy に関しては、各ユースケースで求められる保証レベルがどの程度か議論する必要があり、より複雑な検討となるため本実証のスコープからは外し、今後の課題として整理した。

| STEP | 詳細 |
|---|---|
| Accepted Credentials | 証明書の検証のプロセスの一環として、どのような証明書やエビデンスが認められるかを記載する。 |
| Validation Methods | 証明書を発行するためのエビデンスが真正であることを確認するために、どのような検証方法が認められているかを記載する。 |
| Validation Method Combinations | 証明書のエビデンスの信頼性を高めるために、検証方法をどのように組み合わせるかを記載する。 |
| Verification Methods | 正しい個人と証明書が紐づいていることを確認するために、どの検証方法が認められるかを記載する。 |
| Verification Method Combinations | 証明書のエビデンスの検証方法が組み合わせによって保証レベルを上げるのと同様に、本人確認のエビデンスを組み合わせることで、より高い信頼性を担保する方法について記載する。 |
| Assurance Combinations | 保証レベルを決定するために、各エビデンスがどのように使用され、どのように組み合わされるのかを記載する。<br>・エビデンスの「重み」または強さ<br>・証明書のエビデンスに適用される検証技法の組み合わせ。<br>・本人確認のエビデンスに適用される検証技法の組み合わせ。 |

【共助トラストフレームワークについて】

各共助アプリベンダーと議論をしながら、共助トラストフレームワークの項目を作成。各項目についてポイントとなった箇所についてまとめて記載をする。

【共助トラストフレームワーク項目】

- 用語定義
- 目的
- ローカライゼーション
- 法的地位
- スコープ
- 手続き
- 原則
- 方針
    1. 通信プロトコルと標準規格の管理方針
    2. プライバシーポリシー
    3. 証明書の発行に関する方針
    4. 識別子に関する方針
    5. 共助実績証明書に関する方針
    6. スキーマ管理方針
    7. 技術の活用方針
    8. クレデンシャルの有効期限に関する方針
    9. クレデンシャル失効に関する方針
    10. エコシステム参加者に関する方針
    11. ユーザーに関する方針
    12. Wallet に関する方針
    13. 証明書の検証に関する方針
    14. ガバナンスの運営に関する方針
    15. ガバナンス文書の管理方針
    16. 改定に関する方針

【目的と原則について】

ガバナンスの基本方針となる目的と原則を設定し、本ユースケースとテクノロジーの関係性について記載した。

■ 目的（なぜそのような価値観を持っているのか？）

インターネットの普及、技術の発展、経済モデルの革新、人口動態の変化などが相まって、「共助サービス」と呼ばれる新しい経済モデルが注目されている。共助サービスとは、何らかの困りごとがある人と、それ

を解決できる資産やスキルを持つ個人や組織を結びつけるシェアリングエコノミーの形態の 1 つである。日本には移動支援、保育園の送り迎え、モノの貸し借り、コミュニティ活動等の様々なジャンルで 300 を超える共助アプリが存在する。

一方で、見知らぬ人同士がマッチングする共助サービスでは、セキュリティ、サービス品質、トラストといった問題は、従来のプラットフォームビジネスとは異なる方法で保障される必要がある。特にトラストの欠如に関する課題は、利用者だけではなくサービス提供者にとっても大きなリスクになる。

このトラストフレームワークの目的は、共助アプリにおけるユーザーのトラスト検証範囲を拡張することである。その結果、共助アプリで安全安心な顧客体験を提供できるようにプラットフォーマーを支援するとともに、ユーザー自身が蓄積した実績やトラストを用いて新たな価値を創出できる社会を目指す。

■　原則（共助アプリのトラスト問題を解決するテクノロジーは？）

共助アプリ Wallet ユーザーは、自分だけのデジタル ID を使って、自身の共助実績を管理・活用することができる。共助実績はユーザーの信頼性を向上させる情報として、様々なサービス間で連携可能なものである。

このデジタル ID は、標準化されたデータ形式や技術に基づいて開発される必要がある。これにより、共助アプリ同士の連携がスムーズになるだけではなく、共助アプリ以外の第三者ともデータのやり取りが容易になる。結果、利用可能なユースケースが増え、ユーザーの共助実績の価値を向上させることができる。

またプライバシー保護の観点から、データの共有にはユーザーの同意が必要であり、ステークホルダ間の通信はセキュアな環境で行われなければならない。

分散型 ID の技術は、従来のデータ連携システムと比較して、標準仕様に基づいたオープンな技術であり、プライバシーとセキュリティを保ちつつ、組織間のシームレスなデータ連携を実現できる。

【Issuer/Verifier の要件について】

Issuer の認定基準としてシェアリングエコノミープラットフォーマーに対する ISO の規格を活用できるか検討した。

テーマ１ ：Issuer の認定

論点： Issuer と Verifier はどのようステップで参加メンバーとして認定されるか？

- 方向性：

  Step1：コンソーシアム内でサービスのレビューを行う。（ISO/TS 42501 を参考に基準を設ける）

  Step2：コンフォーマンステストにより技術検証を行う。

  Step3：ガバナンスメカニズム（Issuer リスト）に追加。
- 現時点での結論：

  Issuer の認定については、ISO/TS 42501 が基準として参考になるか検討する。またシェアリングエコノミー協会に加入していれば、オンボーディングが簡単になる等の方法を取れば、参加者を募りやすくなるため、併せて検討する。

※ ISO/TS 42501 について
「シェアリングエコノミー デジタルプラットフォーマーに対する一般的な信頼性と安全性の要件」
信頼性と安全性の確保のため、プラットフォーマーが遵守すべき事項が記載されている。

テーマ２： Issuer/Verifier の資格停止

論点： Issuer/Verifier の資格を停止するステップはどうするか？

- 方向性：
  ルール違反により削除の判断をする。削除をする前に事前警告を行い、改善しない場合は Issuer リストから削除する流れ。削除と同時にユーザーへの共有を行う。
- 現時点での結論：
  削除の判断基準としては、ISO/TS 42501 に沿った安全なプラットフォーム運営ができているか、MAC の保証レベルに準拠した措置を取っているか等から判断する。

【ガバナンスの運営方針について】

ガバナンスの基本事項として、トラストフレームワークの運営組織や共助アプリベンダーの参加形態について議論した。

テーマ１：ガバナンス運営組織の形態

論点：ガバナンス・ルールの運営組織をどのように立ち上げるか？

- 方向性：
  ① 理念に賛同する企業と緩やかな連携のために non-binding MOU を策定し、内容が固まった段階でコンソーシアムを立ち上げる。
  ② 最初からコンソーシアムを立ち上げ、賛同者を募る。
- 現時点の結論：
  方向性①を選択。いきなりコンソーシアムを立ち上げるのではなく、トライアルプロジェクトとして策定したガバナンスが Issuer の賛同を得ることができるかテストをするところから開始する。

テーマ２：参加者数の想定

論点：どのくらいの共助アプリベンダーがエコシステムに参加する想定か？

- 方向性：
  現在 4 社で検討中。シェアリングエコノミー協会の参加者数が 300 社であるため、初期のターゲットとしては 100 社程度を目標にする。
- 現時点の結論：
  シェアリングエコノミー協会の協力も得ながら、本エコシステムへの賛同者を募っていく。

テーマ３：コンソーシアムの参加者にどの程度権限を持たせるか

論点：参加者はどの程度意見を述べたり、ガバナンス・ルールを変えたりすることができるか？

- 方向性：

① 初期 4 つの共助アプリ（May ii、まちのコイン、子育てシェア、ロキャピ）以外はガバナンスの変更権限は持たない。

② 今後賛同企業が増えた場合は、ガバナンスに干渉できる権限も付与する。

➢ 現時点の結論：

方向性①を選択。ガバナンスについてはステークホルダが増えるほど調整が困難になることが予測されるため、初期参加の 4 つの共助アプリで決めたルールに賛同する企業がエコシステムに参加する形式を取る。

【ガバナンスの整理】

ガバナンスルールを記載した文書をもとにした、システムベースのガバナンスへの落とし込みが重要である。エコシステム全体でトラストを担保できる仕組みの構築を検討する必要がある。

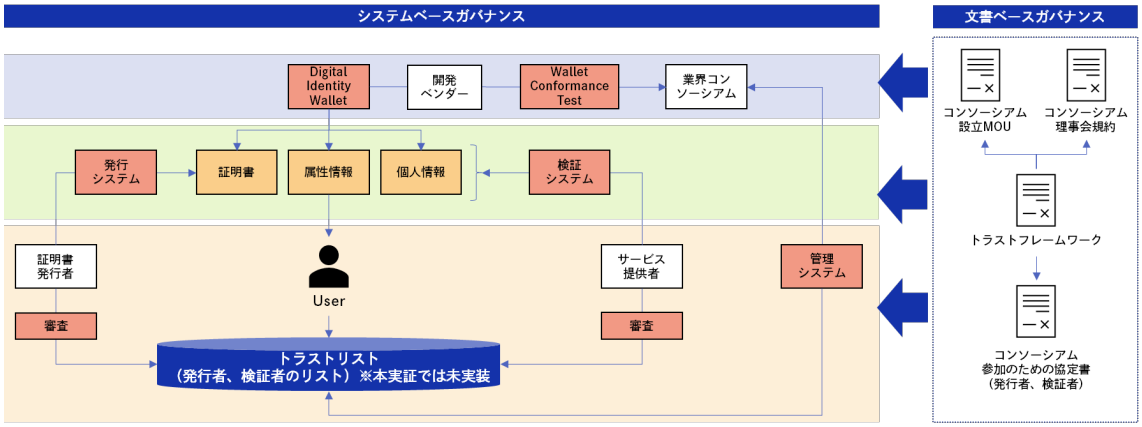



**図 5-1-1：ガバナンス全体像**

【ガバナンスの課題】

現状、業界コンソーシアムがエコシステムの信頼の起点になっているが、User がどのコンソーシアムを信頼できるか判断することは困難。また発行者と検証者から見た User と Wallet の紐づけも弱い。

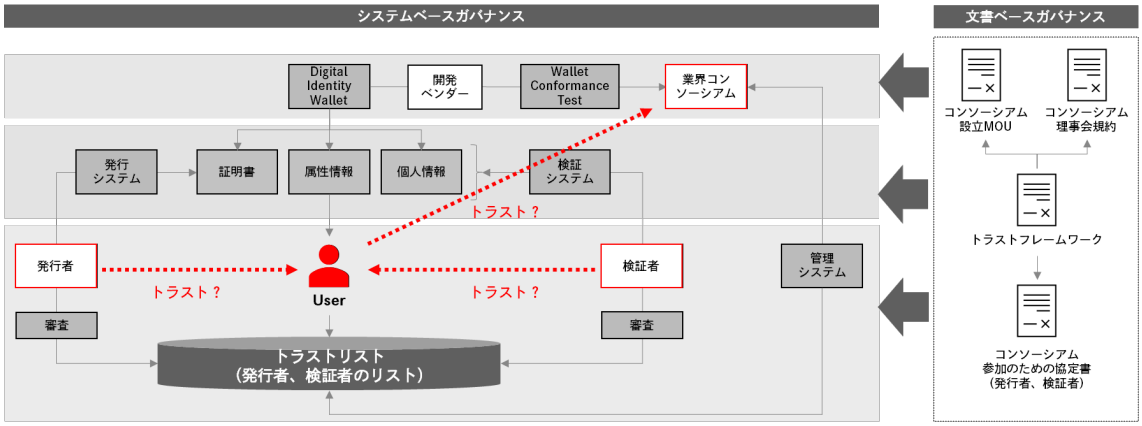



**図 5-1-2：ガバナンスの課題**

【Internet Identity Workshop（IIW）への参加】

上記ガバナンスの課題を踏まえ、2023 年 10 月開催の IIW へ参加し、分散型 ID コミュニティにおい

て政府はどのような役割を果たすべきかについてセッションを実施した。

政府が Verifiable Credentials Ecosystem で果たすべき役割を明確にするため、政府および民間が行うべきことをブレインストーミングした上で、各国の状況をまとめ、共通で各国政府がすべきことをリストアップした。

日本、アメリカ、カナダ、インドの政府/民間企業より合計約 15 名が参加。

参加者：BC 州政府、Digital Impact Alliance(DIAL)、Accenture、DFINITY、Trusted Web 推進協議会など


**図 5-1-3：セッション内容**

| | | | |
|---|---|---|---|
| SPACE **F** | Browser API Wallet Query Lang / Sam Gogo | Access Notes Form | Not yet |
| SPACE **G** | Should Governments be involved in VC ecosystems? / Naoki Yagita and Rintaro Okamoto | Access Notes Form | YES! |
| SPACE **H** | Secure Organizational Identity / Lance Byrd & Rodo & Alex Andrei | Access Notes Form | yes |

**図 5-1-4：セッション項目**

IIW 参加の結果、下図のようなエコシステム外のガバナンスについて、政府がガイドライン等を策定することでリスクを軽減する必要があるとの結論に至った。

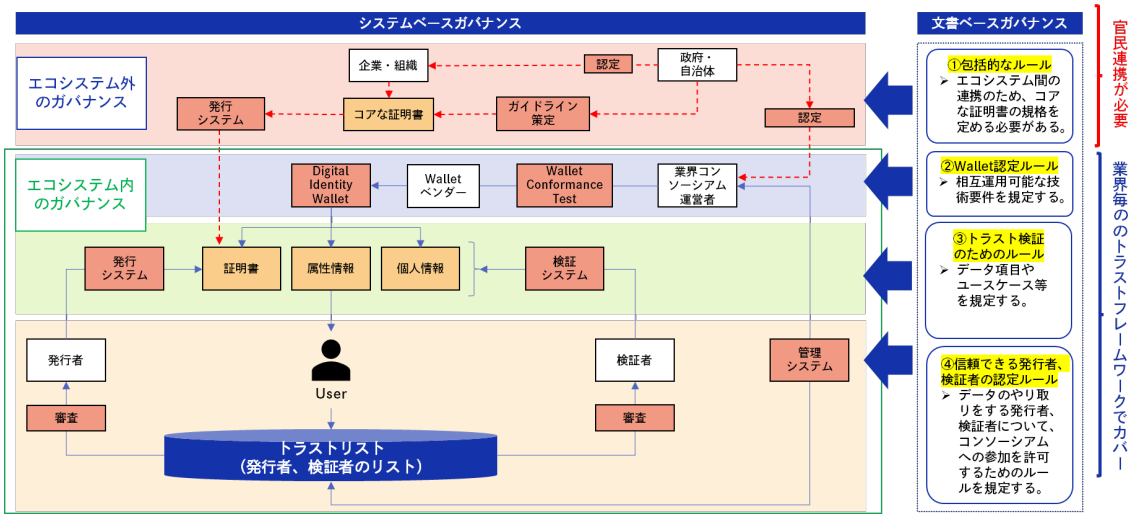



**図 5-1-5：ガバナンス全体像（更新版）**

# 6. 調査検証

## 6.1 実施概要

### 6.1.1 事業実現に向けた UI/UX における論点とその結果

【UI/UX の検討の流れ】

以下の流れで UI/UX の検討を行った。

① ユースケース検討

論点：共助実績の活用について、ステークホルダが価値を感じるユースケースを作れるか。

結果：AsMama 株式会社、カヤック株式会社、アサヒ飲料株式会社とのディスカッションを通じ、共助実績の活用ユースケースを 3 つ作成。それぞれのユーザージャーニーを整理した。

② UI/UX モックアップ開発

論点：技術に深く精通していなくても直感的に利便性を体感できる UI/UX を調査できるか。

結果：検討した 3 つのユースケースについて、具体的な体験を UI/UX モックアップとして可視化し、共助実績の活用によってオンライン上のトラストが拡大する体験を作り出した。

③ ユーザーインタビュー

論点：技術に精通していなくても直感的に利便性を体感できる UI/UX を調査できるか。

結果：保育園申請ユースケースについて、実際のユーザーに対してインタビューとワークショップを実施し、ユースケースに対する共感や UI/UX に対する課題について調査した。

【ユースケース検討】

AsMama 株式会社、カヤック株式会社、アサヒ飲料株式会社とのディスカッションを通じ、共助実績の活用ユースケースを３つ作成。それぞれのユーザージャーニーを整理した。

ユースケース①：オンライン上で信頼できるプロフィール

- ペルソナ：（地域に）移住してきたばかりの子育て世代
- 提供内容：まちのコインの活動実績をオンラインで連携し、SNS アプリのプロフィール情報に活用する。
- 提供価値：今まで築き上げてきたコミュニティの活動実績を SNS アプリ上におけるユーザー同士の信頼性担保に活用できる。


**図 6-1-1：ユースケース①オンライン上で信頼できるプロフィール**

ユースケース②：飲料メーカーへの共助実績の連携

- ペルソナ：共助アプリユーザー
- 提供内容：May ii アプリの利用証明をオンラインで連携し、飲料メーカーのキャンペーンでクーポン交換の条件に活用する。
- 提供価値：共助アプリユーザーはインセンティブにより共助アプリ利用のモチベーションが増加する。飲料メーカーなど企業にとって顧客層の拡大や社会貢献（CSR）を通じた共助促進を図ることができる。

**図 6-1-2：ユースケース②飲料メーカーへの共助実績の連携**

ユースケース③：保育園の入園申込におけるデジタル証明書活用

- ペルソナ：転居を検討している子育て世代
- 提供内容：子育てシェアアプリの利用証明をオンラインで連携し、保育園の入園申込の調整指数への加点に活用する。
- 提供価値：子育て世代には転居する際に保育園入園の不利を軽減することができる。自治体には地域活動へのインセンティブ付与とオンライン申請の効率化を実現する。


**図 6-1-3：ユースケース③保育園の入園申込におけるデジタル証明書活用**

6.1.2　実施内容・手法

調査検証として、「ユースケース③：保育園の入園申込におけるデジタル証明書活用」に対して「コンセプトの受容性評価」「UX 評価」を実施した。

コンセプトの受容性評価では、統計学的に、対象ユーザーの母集団全体の受容性を検証するには約 385 人の評価を得れば母集団規模に関わらず高い精度（※）で検証できるが、今回は UX 課題抽出作業と同時に受容性を確認する程度に留めた。

※高い精度：許容誤差 5%、信頼レベル 95%。今回は許容誤差。

許容誤差：得られた結果が母集団の実態から、どの程度ずれている可能性があるか。

信頼レベル：抽出したサンプルの 1 つが、どのくらいの確率で許容誤差内の結果となるか。

また、UX 評価では、ストーリーボードに沿った達成目標をユーザーに提示し、モックアップを操作していただいて感じたことを評価する手法を選択し、ヒアリングの人数は、一般論として「5 人を対象にテストすれば 85%の課題が発見できる」と言われていることから、5 名でのテストを行った。

6.2 調査検証結果

6.2.1　実施概要

実施日：2024 年 1 月 27 日(土) 13:00～15:00

場所：神奈川県横浜市栄区 某所

対象者：下記要件で 5 名を事前リクルーティング

**表 6-2-1 リクルーティング要件**

| 必須 | 任意 |
|---|---|
| ● 保育園に子供を預けている or 過去預けていた、共働きのママ/パパ<br>● 地域ぐるみの子育てへの共感と興味あり（経験の有無は問わない） | ● 産育休から復帰済み<br>● 保育園通園中に転居予定あり or 将来転居したい、もしくは自治体を飛び越えての転居経験あり<br>● 子育てシェアユーザー（頼る側） |

調査内容：リクルーティング対象者に対して、下記の観点および下図のフローで「受容性評価」「UX 評価」を実施した。

受容性評価：コンセプトや提供価値、ユーザー体験を紹介し、ターゲットユーザーの立場から見て受容できるサービス体験かどうかを評価する。

UX 評価：ストーリーボードに沿った達成目標をユーザーに提示し、モックアップを操作して感じたことを評価する。

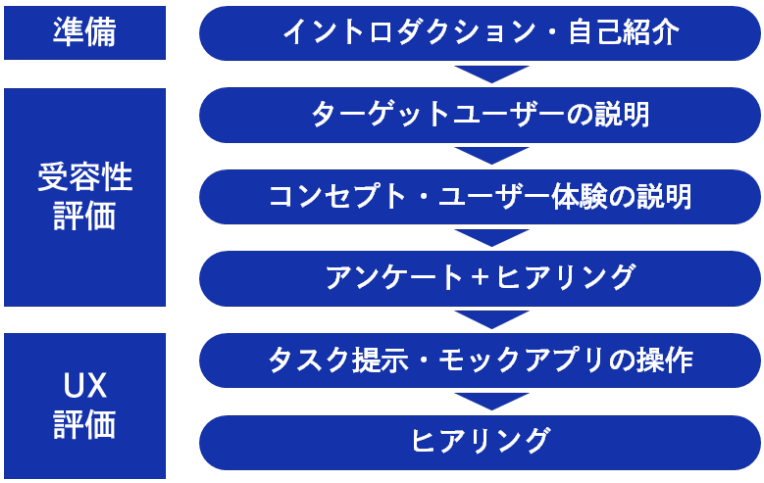



**図 6-2-1：ヒアリングの当日フロー**

### 6.2.2　実施結果

下図のように、リクルーティング対象者にモックアップアプリを体験してもらい気づいた内容を集約した。


**図 6-2-2：ヒアリング実施の状況**

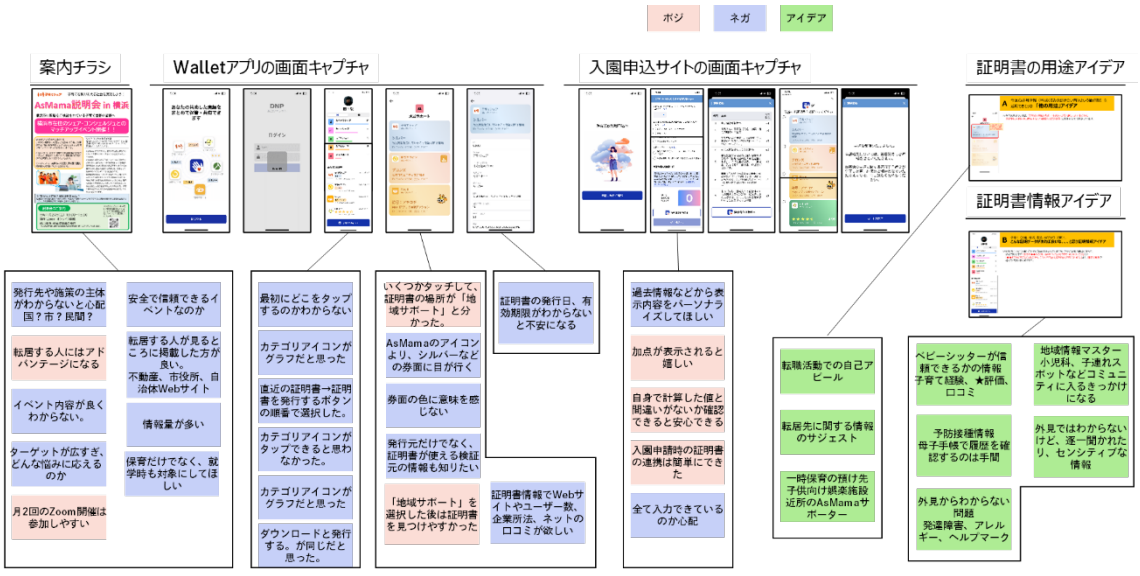



**図 6-2-3：調査結果の整理**

リクルーティング対象者にヒアリングを実施し、以下のような結果を得られた。

総論：ユースケースに対する評価

- 「地域で育児を助け合う」という価値が証明され、保育支援などに活かされる社会は本当にありがたい。
- 転居のハードルは本当に高く、本制度・サービスが実現したらすぐにでも利用したい。
- 一方で、調整点数制度の仕組み上、入園が保証されるわけではないのでその点は不安が残る。

Wallet アプリで証明書を管理することついて

- ネガティブなイメージはないが、セキュリティが担保されることが大前提である。
- スマホアプリの場合、スマホ容量を考慮する必要があり、ひっ迫していると削除することがある。
- 過去にコロナワクチン接種の履歴をデジタルで管理した経験が、ネガティブイメージ払しょくに繋がっている。

Wallet アプリの UI について

- 選択するボタンやアイコンについて説明が必要であり、一目見て理解できる UI をより配慮する必要がある。
- 証明書を確認する際に、格納されているカテゴリと証明書の関連性をイメージできる工夫が必要である。
- 証明書の発行日や有効期限が分からないと不安に感じる。

証明書のトラストについて

- 本ユースケースのように制度に合わせた証明書発行の場合、生活者が安心して証明書を利用するには、発行元だけではなく、制度の主体など検証元もあわせて信頼できる必要がある。

証明書情報のアイデア

- 子供の予防接種情報が証明書化されれば、急に確認されたときに母子手帳を持っていなくても証明でき便利である。

# 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

**表 7-1-1：残課題対応方針一覧**

| テーマ | 残課題 | 対応方針 |
|---|---|---|
| 技術 | Issuer/Verifier 側へのアプリケーションの組み込み検討 | まちのコイン、子育てシェア、May ii の各アプリに対して共助実績証明書の発行・検証の機能を付与する場合の開発方法を検討する。 |
| | 実運用を見据えた運用体制の構築 | 共助実績に名前や本人に紐づく ID 情報等を含むことを想定し、セキュリティ基準の高いレベルでの運用体制の構築を検討する。 |
| | Issuer/Verifier の相互運用性テストの検討 | Wallet Conformance Test サイトを拡張する形で Issuer/Verifier の相互運用性をテストする環境を構築する。 |
| ガバナンス | 共助トラストフレームワークに対するステークホルダ間の合意と、共助トラストエコシステム運営の立ち上げ | カヤック、AsMama、DNP を共助トラストエコシステム運営のボードメンバーとし、まずはトライアルプロジェクトとして non-binding MOU の締結を実施する。 |
| | 本人とクレデンシャルの紐付け方法についての検討 | 本人とクレデンシャルの紐づけ（※今後実装の方法については要検討）<br>■ ①本人情報と共助実績の紐づけ or ②別の VC と共助実績を紐づけ<br>■ ①についてはマイナンバーカードを使って紐付け<br>■ ②については A:暗号鍵を使って異なる VC 同士をバインディング、B：アトリビュートの共通項目との突合（社員 ID、メールアドレス等）のパターンあり |
| | 国際間連携のための共助実績の Identity assurance policy の検討 | OIX のホワイトペーパーを参考に、現状の共助トラストフレームワークの項目でカバーできていない領域について検討を進める。 |
| UI/UX | ユーザーヒアリングの結果を受けた UI/UX の改善 | 共助 Wallet の UI/UX について、ユーザーが操作を迷った点を洗い出して改善策を検討する。 |
| | 各ユースケースのビジネスモデル検討 | ユースケース毎のビジネスモデルの検討と並行し、地域の様々な課題を共助で解決する「地域 Wallet」としての構想を検討する。 |
| | 台湾のデジタルボランティア証明書との連携ユースケース検討 | 既に台湾でデジタルボランティア証明書を発行してユースケースを作っている Turing Space 社と連携して、国際間連携のユースケース創出を目指す。 |

## 7.2 ユースケース実現モデル

### 7.2.1 ビジネスモデル案

ビジネスモデル案①：共助アプリ間の連携

概要：共助実績の発行、検証を行うためのエコシステムへの登録のために発行者、検証者、技術ベンダーは登録手数料をエコシステム運営者へ支払う。

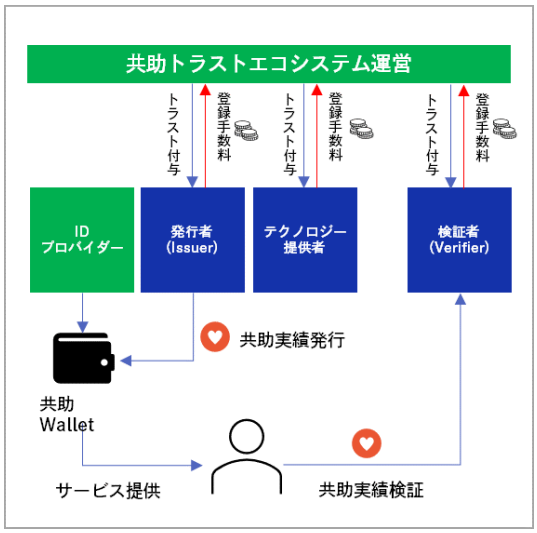



**図 7-2-1：ビジネスモデル案①：共助アプリ間の連携**

ビジネスモデル案②：3rd Party 企業との連携

概要：共助実績をエコシステム外の 3rd Party 企業へ連携することで、共助アプリユーザーへ新たなインセンティブを付与し、利用を促進する機会を創出する。

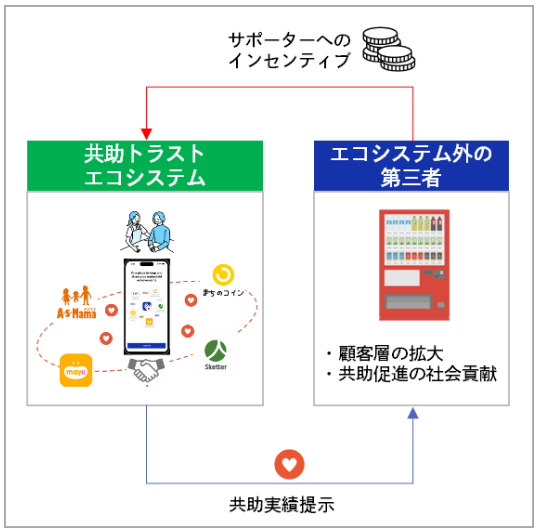



**図 7-2-2：ビジネスモデル案②：3rd Party 企業との連携**

ビジネスモデル案③：国際間連携

概要：今後更なる増加を見込むインバウンド顧客に対し、地域の共助アプリ利用をする際のトラスト形成手段として共助実績を活用。共助アプリの決済手段と連携する。

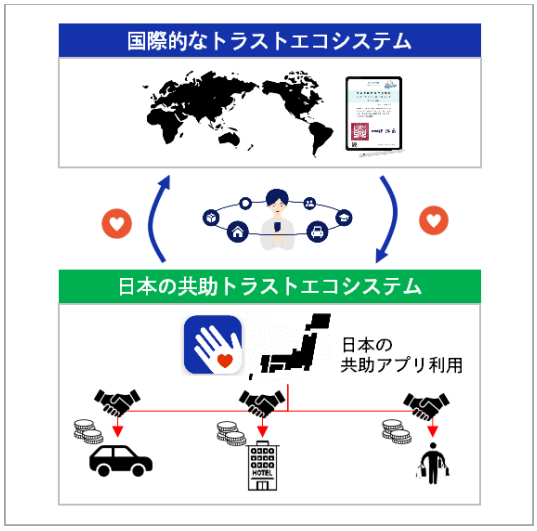



**図 7-2-3：ビジネスモデル案③：国際間連携**

### 7.2.2　アプリ・システム案

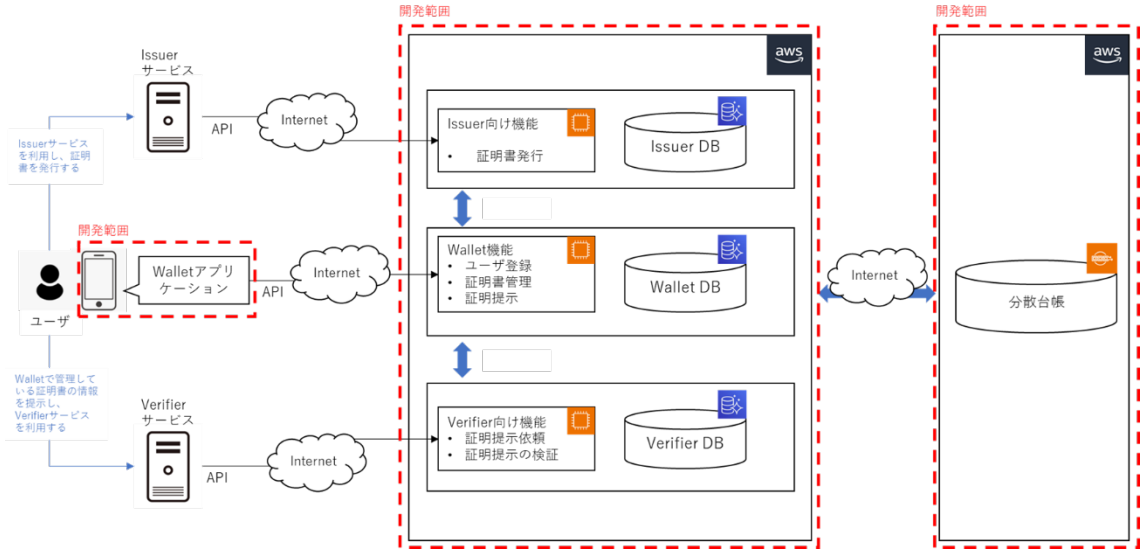



**図 7-2-4：アプリ・システム案**

本実証においては、ユーザーが保持するクレデンシャルのリカバリーが可能なシステムを実現するために、クラウド Wallet でのプロトタイプ開発を行った。

### 7.2.3　ガバナンス・ルール案

ガバナンス・ルールを記載した文書を作成した。

- 共助トラストフレームワーク：

本エコシステムのガバナンス・ルールの中心となるトラストフレームワークを作成した。トラストフレームワークの目的、準拠すべき技術的なプロファイル等を記載している。

- 共助トラストコンソーシアム設立に向けた MOU（基本合意書）：
  本コンソーシアム設立の初期段階として、現在検討を続けている共助アプリベンダーとの MOU 締結のための文書を作成した。本 MOU の中でコンソーシアムの構造をさらに具体化していく想定である。
- 共助トラストコンソーシアム理事会 規約：
  共助トラストコンソーシアムのボードメンバー向けの規約を作成した。理事会の目的、トラストフレームワークの変更等に関わるガバナンス・ルールについて記載している。
- 共助トラストコンソーシアム協定書：
  共助トラストコンソーシアムの参加メンバー向けの協定書を作成した。コンソーシアムの目的、参加者の役割について記載している。今後、持続的なコンソーシアム運営のためのマネタイズモデルの検討が必要である。

7.3 実現に向けたアクション・ロードマップ

将来的には共助実績と様々なクレデンシャルを組み合わせることで、地域課題を解決するソリューション化を目指す。

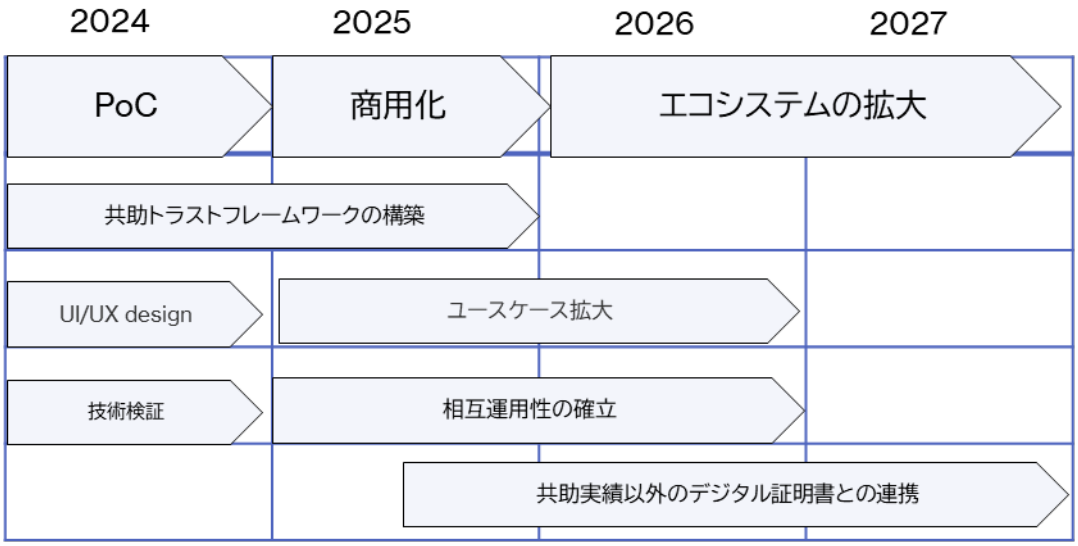



**図 7-3-1：アクション・ロードマップ**

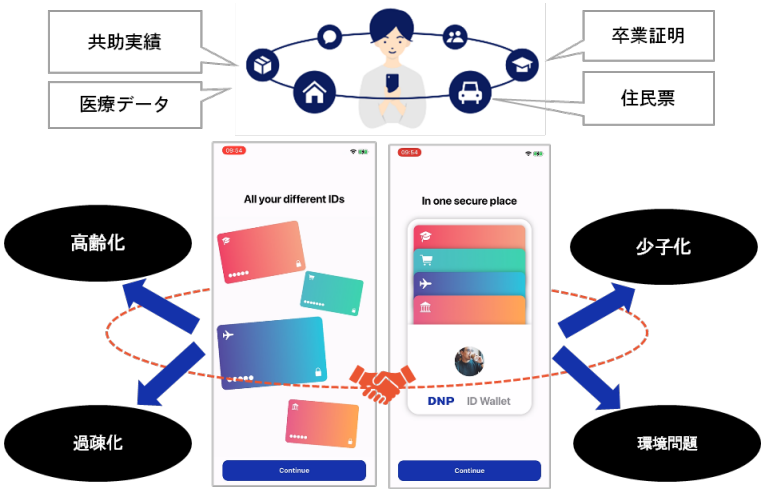



**図 7-3-2：ソリューション化イメージ**

# 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

【Trusted Web が目指すべき方向性】

目指すべき方向性と必要となる原則が示されており、Trusted Web の全体像を把握しやすいと感じる。今後付け加えるとすれば、実現に向けた道筋についてより具体的なマイルストーンや達成目標を示すことによって各ステークホルダの目線合わせができ、取り組みやすさが向上するのではないか。

【Trusted Web のアーキテクチャデザイン】

各構成要素の実装例をより充実させることにより、技術的な理解がさらに深まると考えられる。（例えば、Verifiable Messaging の具体的なユースケースや実装パターンなどを追加する等）さらにはアーキテクチャ全体像と実現方式の関係性をより明示的に説明することができれば、各ユースケースを本アーキテクチャに落とし込みしやすくなる。

【Trusted Web におけるガバナンス】

ガバナンスの必要性と課題、多層的なガバナンスモデルの全体像が示されており、ガバナンスを重視する Trusted Web の特徴が理解しやすい。一方で本実証においてもガバナンスについては様々なアップデートがあったと思われるので、その最新の事例を盛り込むことができれば今後議論を深めるべきポイントが明確になるのではないか。

【Trusted Web におけるセキュリティの考え方】

セキュリティの目標について論点を整理していただいたことにより、事業者として検討するポイントが理解できた。一方でより検討を具体化させるために、論点としてプロトコルのセキュリティ評価方法や鍵管理のモデル構築等の議論を深めていく必要があると感じる。

【今後の取組について】

国際連携の方向性について、単に欧米の議論に追従するだけではなく「日本が主導する（影響力を発揮する）」という観点も盛り込むことによって、国内のステークホルダが能動的に動く指針となり得るのではないか。

## 8.2 Trusted Web のガバナンスに関する課題と提言

**表 8-2-1：Trusted Web のガバナンスに関する課題と提言**

| テーマ | 課題・提言 |
|---|---|
| Ver.1.0 で設定した原則と照らし合わせたときに、現状の原則に対するフィードバックや改善要望 | • 「ガバナンス」の明確化について<br>Ver.1.0 の原則においていくつか「ガバナンス」の記載があるが、言葉の定義が曖昧であり（トラストフレームワークを指している？）、具体的なアクションに結びつけにくいため、「何のための」ガバナンスなのか明確にする必要があるのではないか。<br>• 原則 10 の更改容易性・拡張性について<br>特定の技術に依存しすぎることに問題があることは同意する一方で、実装レベルで相互運用性を確保するためには一定程度の道標となるガイドラインが必要。欧州の EU DIW の議論を参考に、Trusted Web 実現のためのアーキテクチャーフレームワークとしてデータ形式や通信プロトコルの明示に踏み込むことも見据え、既存の原則のアップデートが必要ではないか。 |
| ①業界で既に存在するトラストフレームワーク・ルールを準用したときに原則との関係性は問題ないか | • 現在、共助アプリ業界には既存のトラストフレームワークと呼ぶべきものは存在しないため、ステークホルダを横断して共助実績を連携するための共助トラストフレームワークの作成が必要となった。<br>• 新たなトラストフレームワークを作成する上で、シェアリングエコノミー国際規格（ISO/TS42501）を参考に共助実績の発行者、検証者の認定の基準を定めることにする等、一部既存の規格を準用した。<br>• 共助アプリ内のトラストフレームワークを構築する際に、相互運用性を確保するために技術的な要件を絞る必要があり、「柔軟性」や「更改容易性・拡張性」を制限せざるを得ない状況が出てきた。 |
| ②新規でガバナンスを作成した場合、他業界に横展開する上で効果的な取組は何かあるか | • 一般的なトラストフレームワークの内容については、OIX が提言している「General Policy Rules」を参照して作成することで、海外の先行事例で検討されている項目を網羅することができる。<br>• 一方で、 アイデンティティ保証のポリシーについては各国で基準が異なることがあるため、国内の検討状況（OIDF Japan の KYC ワーキンググループのホワイトペーパー等）を参考にしながら業界ごとに証明書のエビデンスの検証レベル等を定める必要がある。<br>• また参加するステークホルダが技術的なプロファイル要件を満たしているかどうか確認してリスト化するため、コンソーシアムごとにコンフォーマンステストサイトの実装が効果的であると考える。 |
| ガバナンスの実効性を担保するために有効な取組 | • 共助トラストフレームワークの立ち上げと賛同者を募るために、シェアリングエコノミー協会のネットワークを活用することを想定。既に運用されているコンソーシアムにご協力いただきながら、トラストフレームワークを市場に |

| | |
|---|---|
| （各業界や行政などへの働きかけ等） | 浸透させるステップを踏むことで効率的にガバナンスの実効性を向上させることができる。<br>• またトラストフレームワークそのものへの信頼性や、ユーザーのアイデンティティ保証レベルの確認のために、コンソーシアム外の第三者（政府や権威的な企業）がトラストアンカーになる必要がある。 |
| トラストフレームワークを作成する上でのプロセスにおける課題や提言 | • トラストフレームワークの運営組織の設計が重要。ガバナンス運営組織の形態、参加者の想定、参加者の権限設定についてなど、実際にトラストフレームワークを運用するための規約の作成が必要になる。<br>• 悪意のある第三者への対策という観点から、どのような情報をクレデンシャルに含めるべきか検討が必要。例えば証明書の発行日（新しい方が信頼できる）、アカウント作成日（古い方が信頼できる）、証明書の使用期限などをスキーマに含めることで、証明書自体の信頼性を高める工夫をすることができる。 |
| Trusted Web に概念に則ったガバナンスを効かせるための認定のメリットやデメリットについて事業者としてどう考えるか。<br>また、仮に認定が必要とされる場合、事業を進める上であるいは実装する上で、どのようなところ（例：トラストフレームワークや発信元の信頼性、システムの各構成要素等）に必要と考えるか。 | • エコシステム内のトラストチェーン（信頼の連鎖）を安定させるため、信頼の起点となるトラストアンカーの設置は必須。特にトラストフレームワークの運営主体、ユーザーと Wallet のアイデンティティ保証レベルに関しては信頼できる第三者によるお墨付きが重要であると考える。<br>クレデンシャルの発行者と検証者については、信頼できる第三者にお墨付きを与えられた運営主体が認定することで、エコシステム内のトラストチェーンの形成が可能になる。<br>• 共助アプリの場合はシェアリングエコノミー国際規格（ISO/TS42501）を準用することで、発行者と検証者の「事業者としての信頼性」は認定することを想定しているが、同時に「技術面」において発行・検証機能をトラストフレームワークに則って実装できているか認定することも重要。技術的な相互運用性を検証するコンフォーマンスサイトを実装することで、事業者側が自社のテクノロジーをテスト可能な環境を整備することができる。 |

## 8.3 Trusted Web のガバナンスに関する課題と提言

個人・法人に対して政府が保証レベルの高いクレデンシャルを発行することで、信頼の起点を作る必要がある。

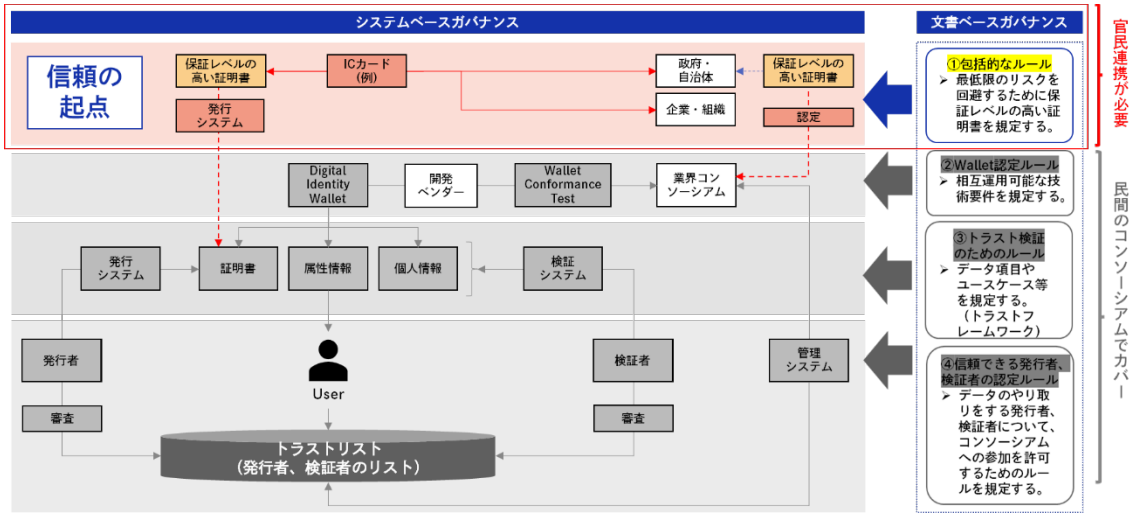



**図 8-3-1：ガバナンス運用に関する政府の役割提言**

証明書の発行～保持～検証の一連の流れにおけるトラストの責任分界点について整理し、コンソーシアム運営者に高度な技術的知見とトラストチェーン全体の設計が求められる。

今後さらに責任主体ごとに責任事項・免責事項・責務等に分解していく必要がある。

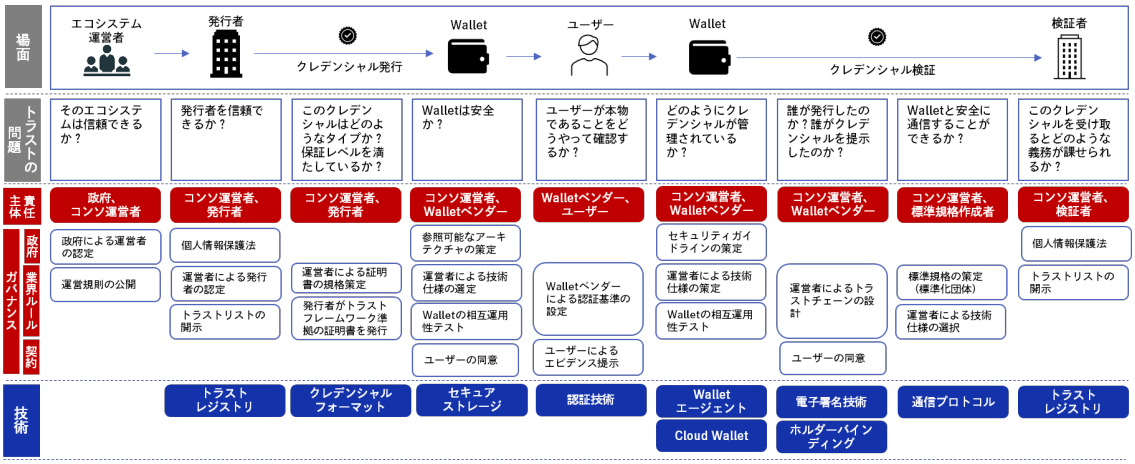



**図 8-3-2：トラストの責任分界点**

## 8.4 その他 Trusted Web に関する課題と提言

■ 技術選定について

- 現状、技術的な仕様については様々な選択肢が想定される状況。一方で相互運用を見据えた際にはできるだけシンプルな技術仕様でなければ、双方のコミュニケーションコストが高くなることが分かった。
- 相互運用性の議論をする際には、例えば EU DIW の参照アーキテクチャのようなものがあれば、認識統一が容易になるため、日本版の参照アーキテクチャ作成をご検討いただきたい。検討にあたっては実装を担うテクノロジーベンダーの意見も参考にする必要があると考える。

■ エコシステム間の技術的相互運用性について

- 本実証では Wallet conformance テストを実施し、Wallet 間の相互運用性を確認している。今後、様々な Wallet がエコシステム内で乱立した際には、このようなコンフォーマンステストの実施が必要になってくることが想定されるため、技術的な相互運用性確保の工夫の一つとして参考にしていただきたい。
- また将来的には発行者、検証者に向けたコンフォーマンステストの実施も必要であると認識している。

■ トラストフレームワークの項目について

- 本実証では OIX のホワイトペーパーを参照して、共助トラストフレームワークの項目を整理した。各項目については汎用的に通じることを意識して作成している。今後も他のエコシステムでトラストフレームワークの作成は必須になると想定されるため、検討時に参照可能な事例として Trusted Web ホワイトペーパーに記載することをご検討いただきたい。

■ 政府の役割について

- IIW への参加や OIX との面談を通じて、政府の役割としてエコシステム間の相互運用性を高めるためのガイドライン作成が求められていることが分かった。相互運用性を高めるための保証レベルの高いクレデンシャル（ゴールデンクレデンシャル）について、技術仕様を国際標準のどの規格を参照すべきか、また海外の同様なクレデンシャルと比べてどの程度の保証レベルが担保されるのか、OIX 等の国際標準化団体とも連携しながら日本政府としてのガイドライン策定が必要。

■ トラストフレームワーク運営者の負担について

- エコシステムを形成する運営者に対しては、高度な技術的知見と全体のトラストチェーン設計が求められるため大きな負荷が想定される。ガバナンス、技術の双方について、参照可能なドキュメント作成や情報発信を通じて運営者の負荷を下げる工夫が必要になる。官民連携のコンソーシアムを作り、トラストフレームワーク運営者の横の繋がりを作っていくこともご検討いただきたい。

# Appendix

用語集

**表 9-1-1：用語集**

| 用語 | 内容 |
|---|---|
| 共助アプリ | 生活者同士のマッチングによる手助けを促進するサービス。支援を必要とする人と支援できる人を繋ぐプラットフォームの役割を果たす。 |
| 共助実績 | 共助アプリ上でのユーザーの活動履歴や評価データ。信頼できる第三者によって検証可能な形式で記録される。 |
| 共助 Wallet | ユーザーが自身の共助実績を管理するためのアプリケーション。他の共助アプリとの連携や、第三者への共助実績の提示に使用される。 |
| 共助トラストフレームワーク | 共助エコシステム内での共助実績の発行、管理、検証に関するルールや技術要件を定めた枠組み。各ステークホルダの役割と責任を明確化する。 |
| 発行者 | 共助アプリベンダーが共助実績証明書をユーザーに発行する際の役割。トラストフレームワークに準拠して証明書を発行する。 |
| 検証者 | 共助アプリベンダーや第三者企業がユーザーの共助実績を検証する際の役割。トラストフレームワークに準拠して証明書を検証する。 |
| 共助トラストエコシステム運営者 | 共助トラストフレームワークの策定と運用を行う主体。コンソーシアムの運営、共助 Wallet の提供、参加ベンダーの認定等を行う。 |
| Verifiable Credential(VC) | 発行者が署名し、検証者が検証可能なデジタル証明書の標準フォーマット。共助実績の記録・共有に用いられる。 |

本実証で開発したシステムの第三者による再現可能性

本実証事業で開発したプロトタイプシステムはオープンソースで構築している。

Wallet アプリケーションはソースコード付随の README をもとに導入し、バックエンドシステムは CI/CD を使用して構築することで第三者による再現が可能である。