Confidential

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

「共助アプリを横断したトラスト形成エコシステム」

大日本印刷株式会社

2024年03月15日

大日本印刷株式会社
ABセンター事業開発ユニット

DNP

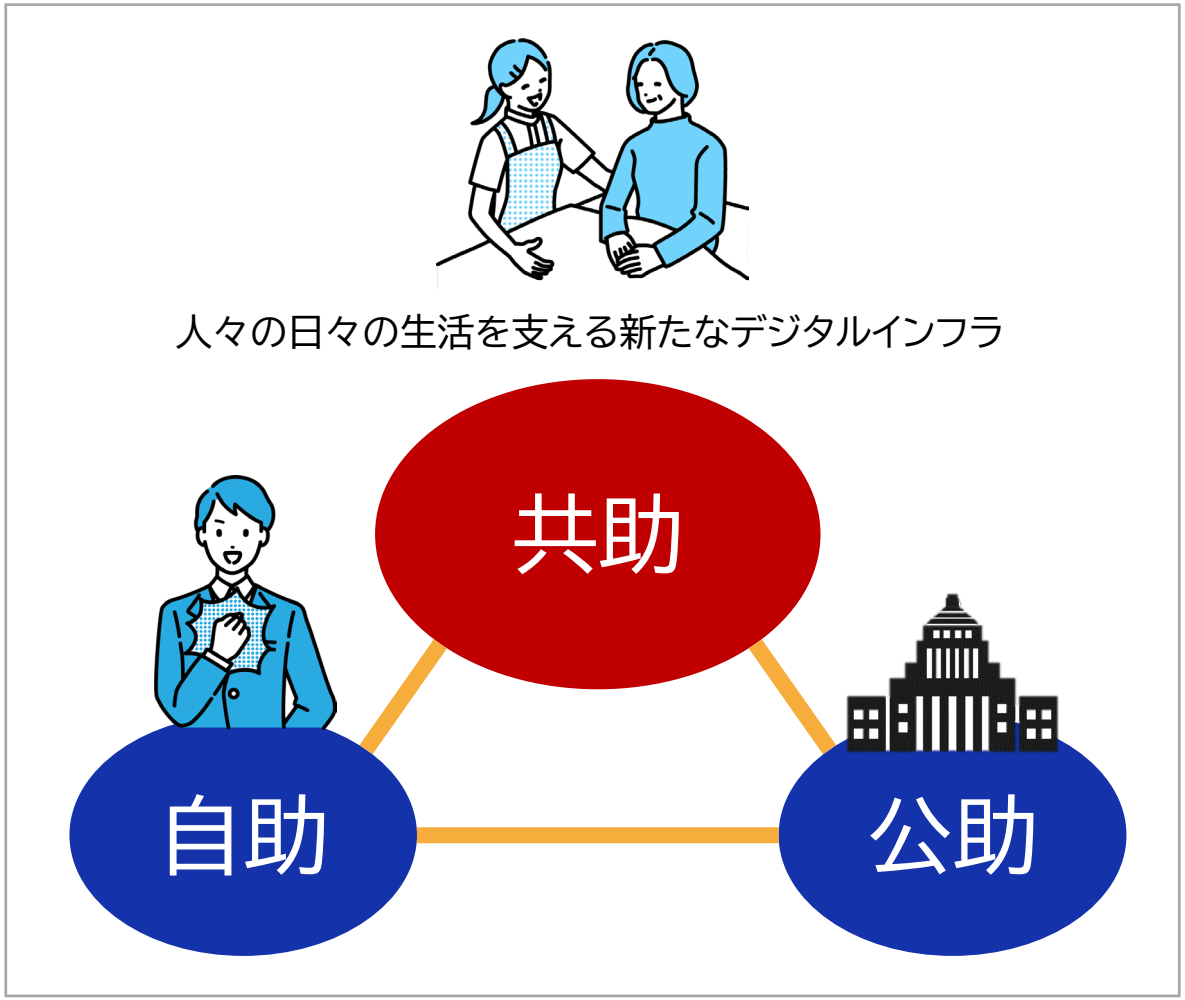
目次

Confidential DNP

1. 背景・目的

共助

現在、日本では地域社会の高齢化・過疎化が問題となっている。自助や公助だけではカバーしきれない問題を解決する手段として注目されているのが「共助」です。



1. 背景・目的

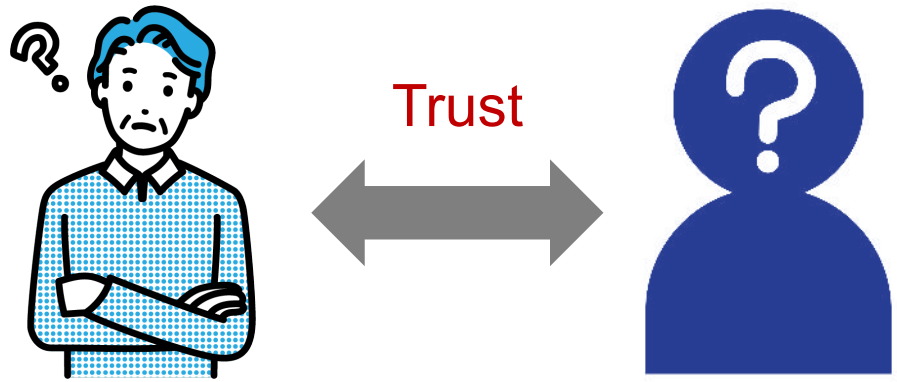
「共助アプリ」
（C to Cマッチングによる社会課題の解決）

子育てシェア　地域互助　コミュニティ通貨

視覚遠隔支援　スキルシェア

買い物難民支援　移動支援

共助アプリは見知らぬ他人とのマッチングすることが多いため、ユーザートラストの検証が重要な課題になっていることが昨年度実証のベンダーヒアリングで判明。



共助実績を見える化することで、サポーターにインセンティブを与えて共助活動への参加を促したいというニーズも確認できた。

1. 背景・目的
「令和4年 Trusted Web の実現に向けたユースケース実証事業」

Confidential

DNP

【May ii】

大日本印刷株式会社

【まちのコイン】

株式会社カヤック

共助実績をデジタル証明書として共有。

【子育てシェア】

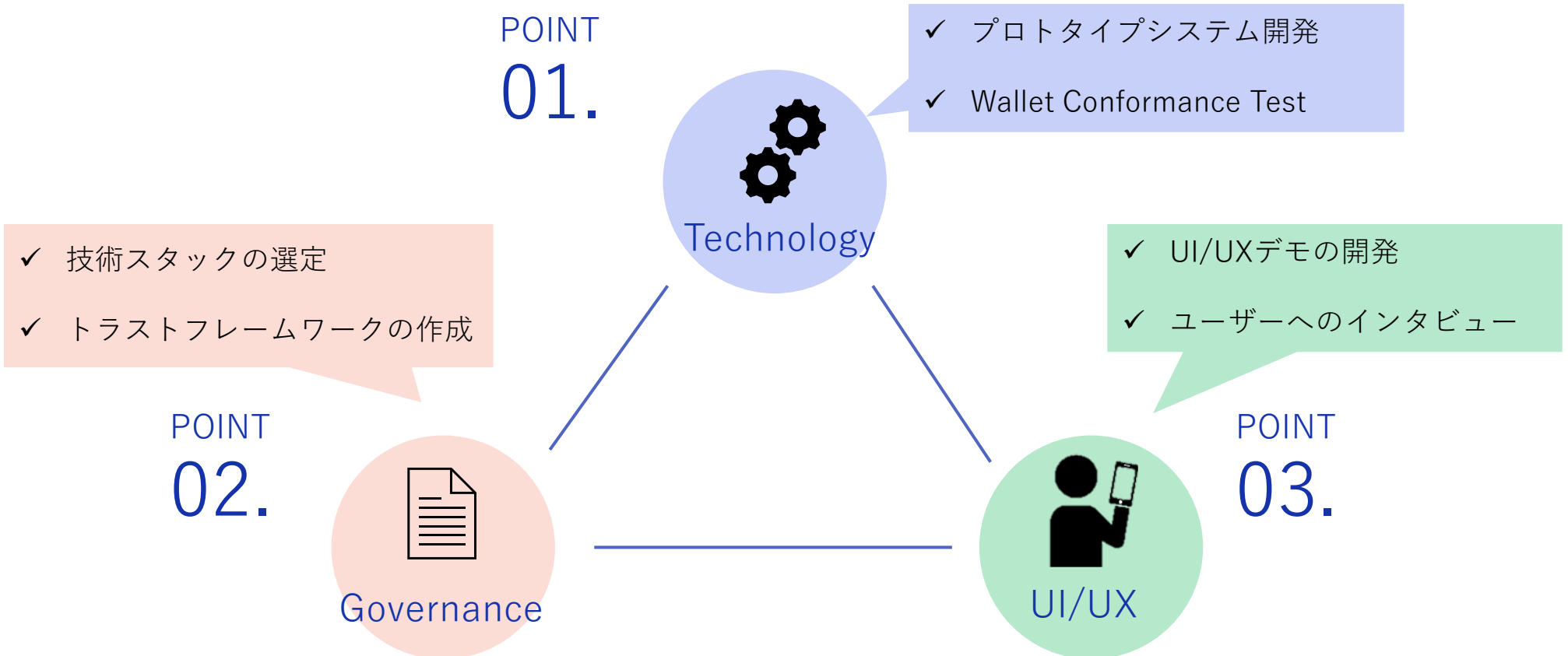
株式会社AsMama

【Sketter】

株式会社プラスロボ

1.背景・目的

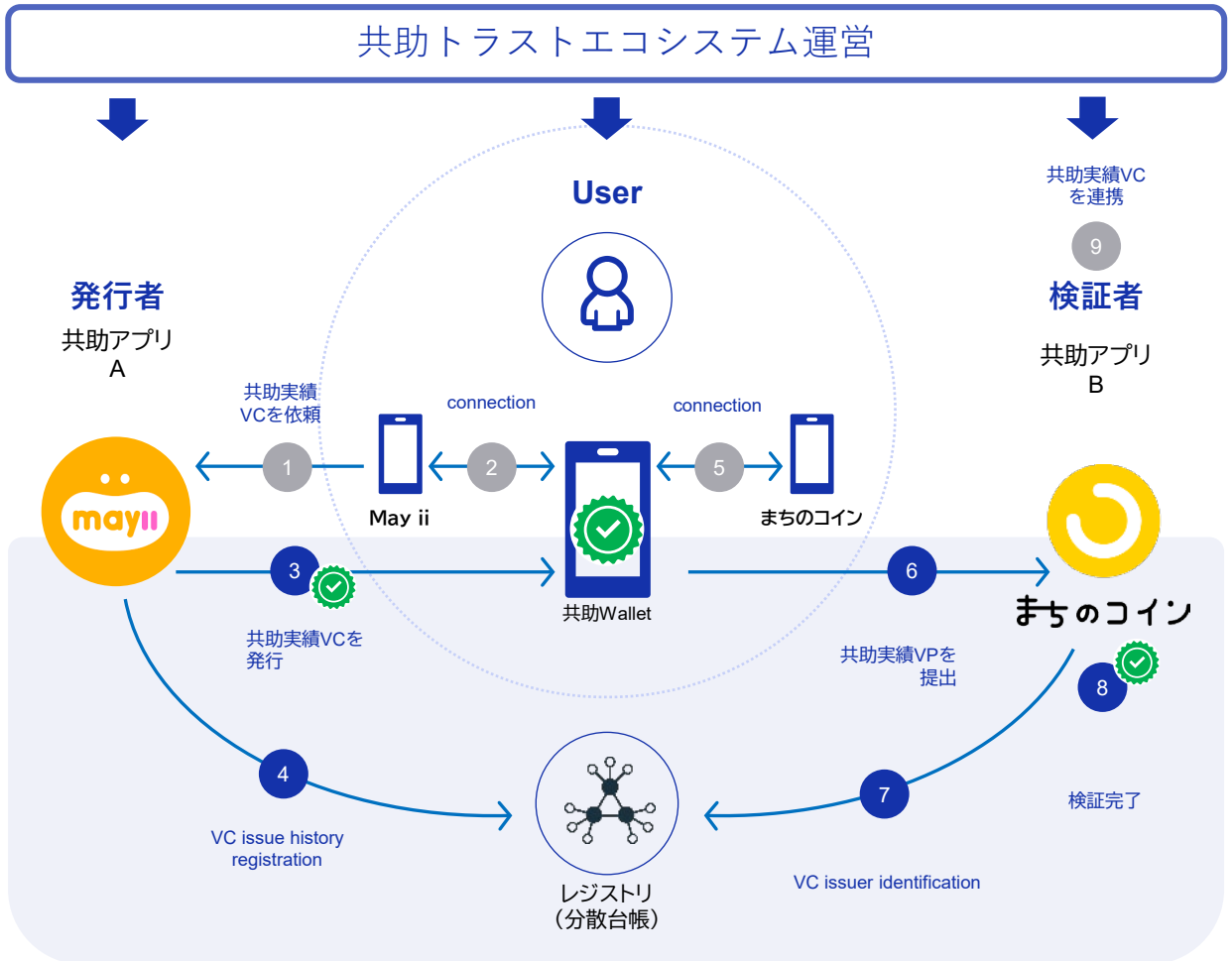
UI/UX、テクノロジー、ガバナンスの3つの観点で社会実装に向けた課題検討を実施。



2. 事業の概要

2.1. 登場する主体と概要

Confidential DNP



ステークホルダー	役割
共助トラスト エコシステム運営	• コンソーシアムの運営 • トラストフレームワーク作成 • 共助Walletの発行 • 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Userに発行 • トラストフレームワークに準拠した共助実績証明書を発行する
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
3rd party企業 （検証者）	• 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（検証者）	• 共助アプリを通じてサポートを依頼 • サポーターの共助実績を確認

2.2. 現状の課題を解決する事業スキーム案

Confidential

DNP

現在の課題（ペインポイント）

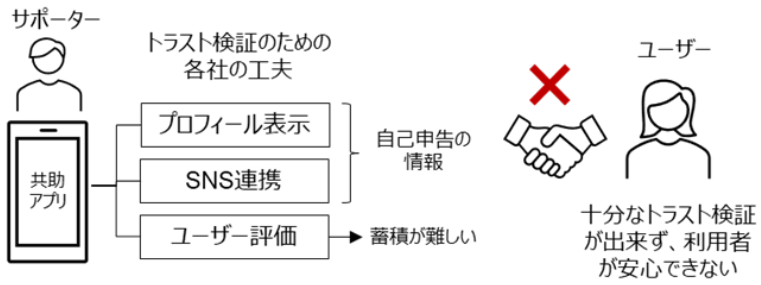
① 共助アプリ（保育・子育て支援、地域互助アプリなど）にとってトラスト検証（本人確認など）はトラブル回避のためにも重要である一方で、プライバシーとの両立やユーザー情報を登録する手間が増える等の課題がある

② 現状、プロフィール表示やSNS連携を通してユーザー同士で確認可能とするなど、トラストの拡大を図っているが、あくまでユーザーの自己申告に基づくものであり、内容の信ぴょう性を検証する方法がない

③ アプリ内のユーザー評価によってトラスト検証を促す場合もあるが、利用者が少ない共助アプリも存在するため、単体で十分な実績を蓄積できる規模がないサービスも多い

課題解決前のスキーム図（As-Is）

共助実績が蓄積されない→共助アプリ内でトラスト検証できない→ユーザーが安心して利用できない→利用者が増えない、という悪循環が形成され、事業撤退を迫られる可能性もある。



Trusted Webの実現により解決する内容

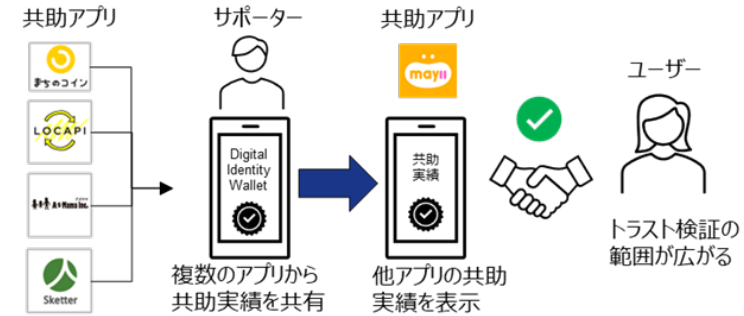
① ユーザーが自身でデータを第三者に提示できるようになり、プライバシーに配慮しながらも情報入力の手間を大きく増やすことなくトラスト検証の範囲が広がる可能性がある

② デジタル証明書として発行された共助実績が連携されることで、ユーザーは単なる自己申告の情報よりも信頼できる情報を基にマッチングするサポーターを選べる。

③ 共助アプリを含めて300以上存在するシェアリングサービスを横断して情報連携することで、他アプリからの共助実績が蓄積され、トラスト検証に流用できる。また大学入試や就職活動でも共助実績を検証可能な仕組みにすることで、共助アプリサポーターへのインセンティブ強化に繋がる

本実証ユースケースのスキーム図（To-Be）

全ての共助アプリの関連情報を繋ぐ集中型のデータベースを中心に据えたエコシステム形成は実現性に乏しい。そのため今回は分散型IDシステムの技術を活用し、Verifiable Credential（VC）として共助実績を連携する方法を検討。



2.3. 社会・経済に与える影響・価値(1/2)

社会的・経済的な価値

政府のデジタル田園都市国家構想では、公共サービスや企業サービスの限界を解決する手段として「共助サービス」が注目されている。本実証では、安全で安心なユーザー体験を保証しつつ、「共助サービス」エコシステムの拡大を後押しするインフラ基盤を企画している。これにより、社会・経済に多面的な価値を生み出し、以下の3つの社会的インパクトが期待される。

1つ目は、共助の広がりによる経済的インパクトである。2025年には高齢者向け市場が101.3兆円に拡大すると予測 されており、共助サービスは超高齢化社会での持続可能な消費行動を促進し、多様な人材の社会参加を通じて企業の生産性向上やイノベーション創出につながる。

2つ目は、共助データを活用した自治体のデジタル変革(DX)の促進である。行政では、エビデンスに基づく政策推進(EBPM)の際にデータ収集の時間とコストが課題となっているが、共助履歴データは「住民課題の可視化」に有益であり、プライバシーに配慮したデータ利活用施策のモデルケースになり得る。

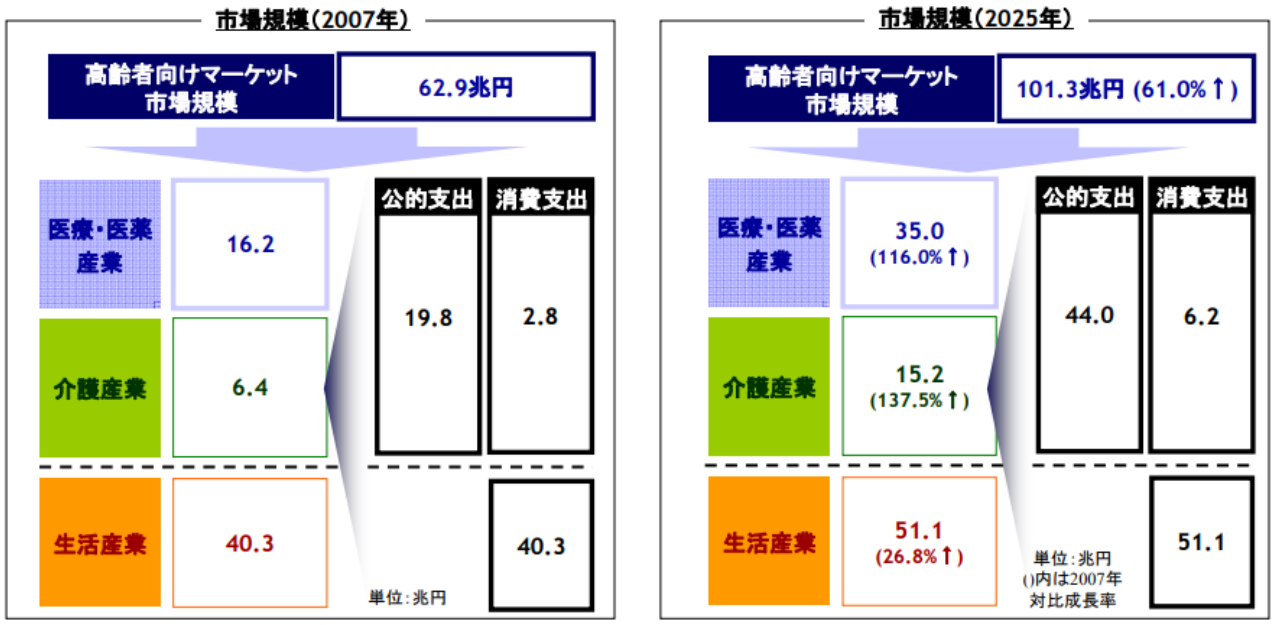
3つ目は、共助アプリ以外の他業界サービスとの連携である。共助アプリの利用を通じて蓄積された個人の信頼(トラスト)は、他業界のサービスからも有用なデータと認識される可能性があり、共助アプリ業界を超えた他業界ビジネスとの連携が視野

に入れられることで、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になる。

2.3. 社会・経済に与える影響・価値(2/2)

Confidential DNP

【図表Ⅲ－3－6】高齢者向け市場の将来推計



(出所)みずほコーポレート銀行産業調査部作成
(注)2025 年はみずほコーポレート銀行産業調査部予測

「みずほ産業調査Vol.39」
https://www.mizuhobank.co.jp/corporate/bizinfo/industry/sangyou/pdf/1039_03_03.pdf

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

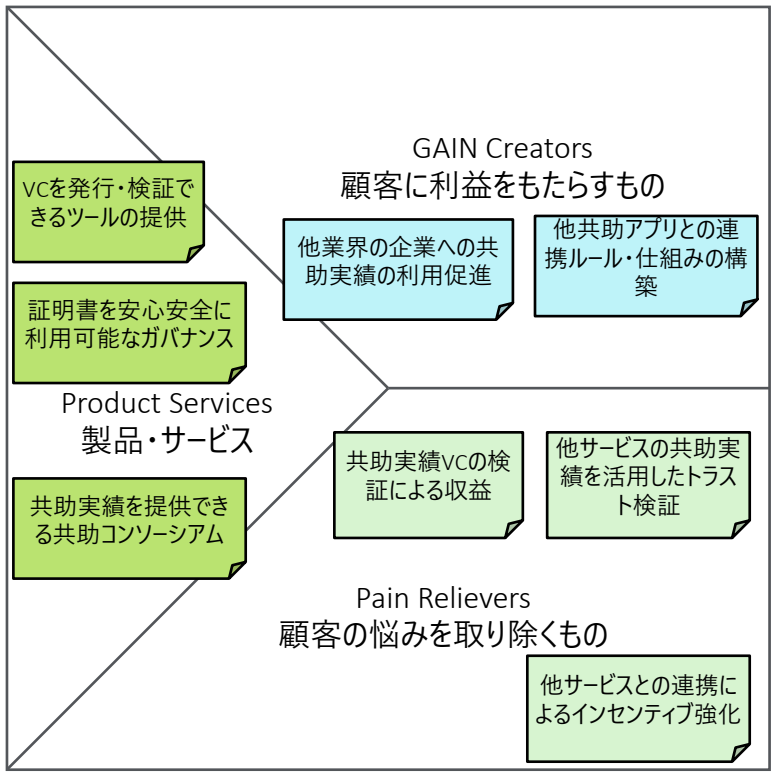
Confidential DNP

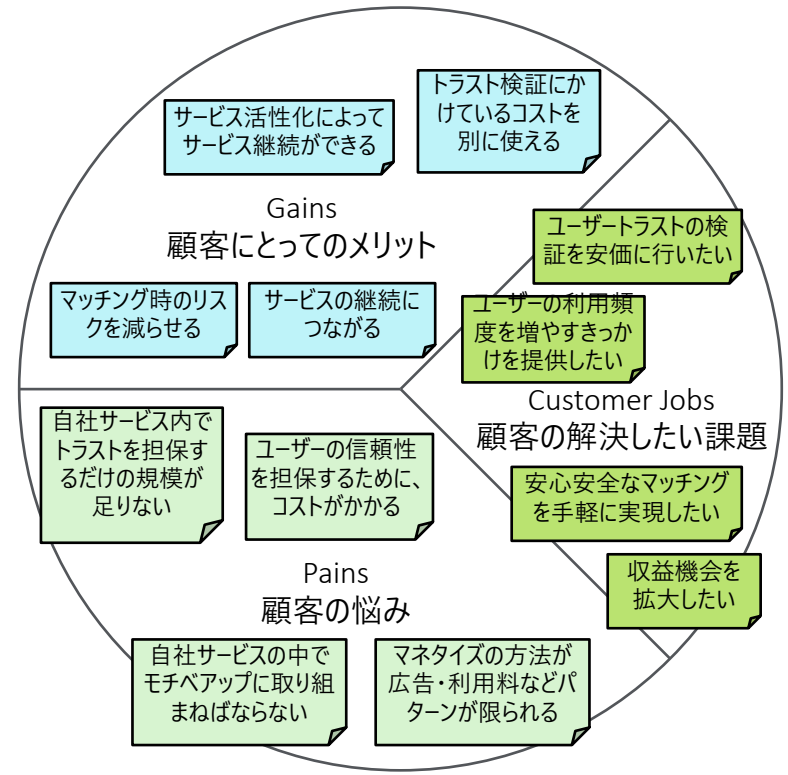
Value Proposition
企業が顧客に提供できる価値

- 他共助アプリの共助実績をユーザートラストの検証として利用化可能
- 共助実績を、共助以外のサービスとも連携可能

Customer's Segment
顧客セグメント

- 共助アプリベンダー





3. 本実証事業における検証計画

【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

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することで、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 Chain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。

【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

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。昨年度は深堀できなかった「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。

【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。

3.1. 実証事業で明らかにする論点への導出・経緯

Confidential DNP

検証課題･論点	初期仮説	論点解決に向けた検証概要
【プロトタイプシステム開発】 社会実装上、セキュリティやプライバシーの観点で問題のないシステムアーキテクチャーをどのように実現可能か。	• Hyperledger Indy/Ariseのフレームワークを活用することによってVerifiable Credentialsの発行～所持～検証の一連の流れを実装できる。 • Walletと発行者・検証者間のAPIについて、Open ID for VCI/VPを使うことでセキュアに送受信できる。 • Walletの秘密鍵管理について、バックアップをクラウド上に保管することで、Wallet紛失時のリカバリーが可能になる。	• Hyperledger Indy/Ariesを使って構築したプロトタイプシステムについて、技術的な課題やセキュリティ上の懸念点を洗い出す。 • 相互運用性の検討において、OpenID for VCI/VPを使うことができるのか調査を実施。実装時の課題を明らかにする。 • Walletのリカバリー方法について、セキュリティ上の問題がない方法で実現可能か検証する。 • 共助実績は点数など一次元の評価ではなく多次元の評価にして、選択的開示ができるようにする
【プロトタイプシステム開発】 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。	• W3CやEUDIWの仕様を読み解き、グレーゾーン箇所の洗い出しが必要。 • 標準仕様として共助エコシステム内で活用できるように落とし込み、準拠しているかテスト可能な環境の構築が必要。	• 現状のW3CやEUDIWの仕様においてグレーゾーン部分を洗い出し、適切な実装方法について検討する。対象の標準化の取り組みを絞り込む際の基準やフレームワーク、考え方を記録する。
【Wallet Conformance Test】 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及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。	• Walletの相互運用性をテストするためには、データフォーマットと通信プロトコルに関する技術プロファイルを定め、コンフォーマンスに参加する企業で合意することが必要。 • 技術提供を行うベンダーが複数存在することを想定して、各社が相互運用性のテストを実施しやすくするためのWallet Conformance Testサイトを設置することで、エコシステム拡張に寄与する。	• 共助アプリWalletについてDNP以外が実装することも想定して、Wallet間の相互運用性をテストできる環境（Wallet conformance test）の構築に向けて検証が必要な項目を検討する。 • テストを実施企業とのやり取りをファクトとして記録し、最終報告で共有する。 • 海外ベンダーにヒアリングを実施し、国外のボランティア実績等のデジタル証明書との相互運用性について検討を実施する。

3.1. 実証事業で明らかにする論点への導出・経緯

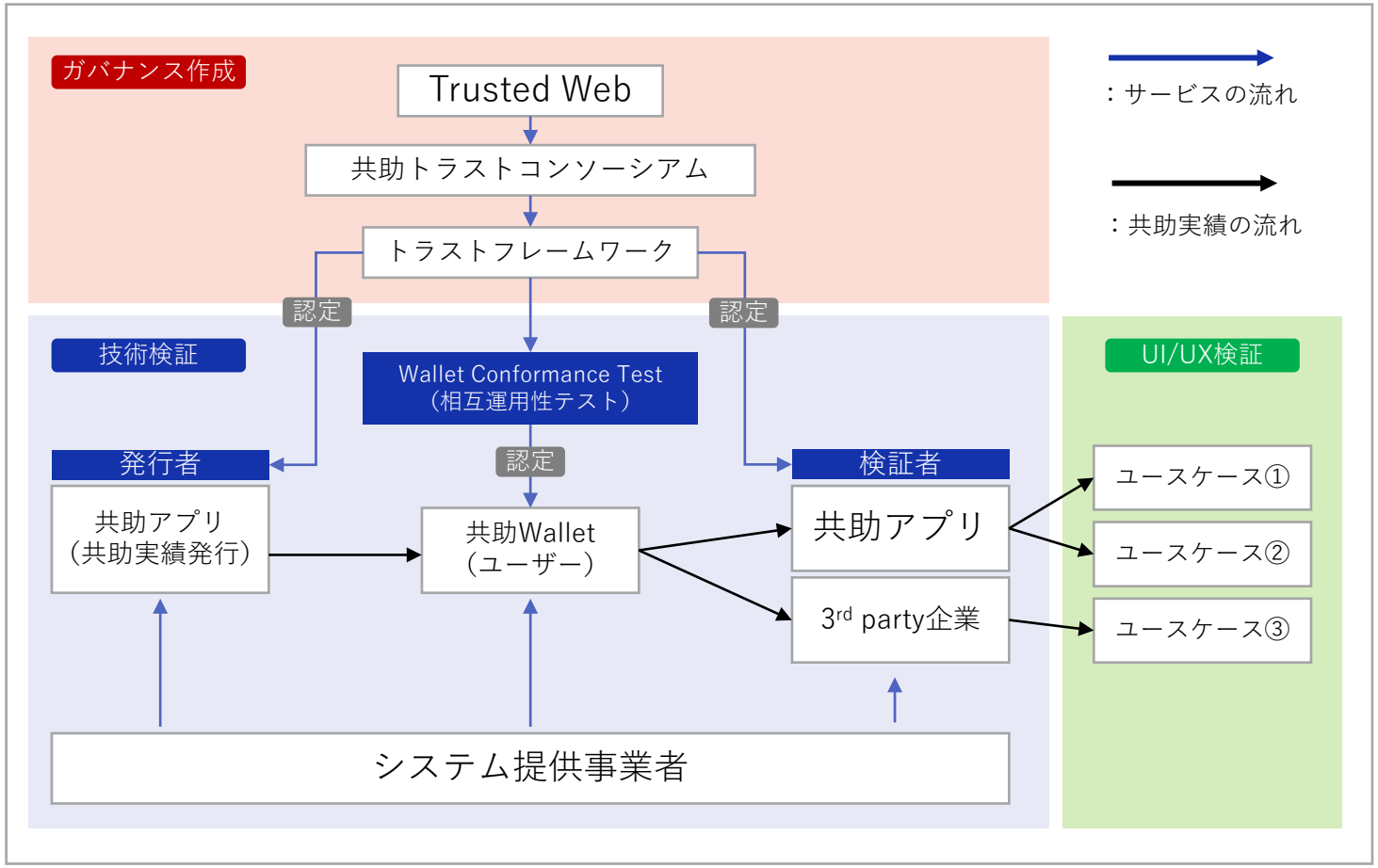
Confidential DNP

検証課題･論点	初期仮説	論点解決に向けた検証概要
【ガバナンス】 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ーの責任分界点を明らかにする。	• 共助エコシステムにおいて、政府と民間企業でそれぞれの役割を果たすことでユーザーが安全に利用することのできるTrusted Webの実現に寄与する。	• 共助実績の発行～保持～検証の一連の流れにおける各ステークホルダーの責任範囲を整理。トラストに関するどのような課題があるのかを洗い出す。 • IIW等の国際的なイベントに参加し、専門家の意見をヒアリングする。
【ガバナンス】 複数の共助ベンダーが合意できるトラストフレームワークをどのように作成可能か。	• 昨年度作成したトラストフレームワークを土台として、各項目を作成しながらブラッシュアップする。 • トラストマーク（発行者の信頼）の認定について、既存の認証制度（「シェアリングエコノミー認証制度」）を参考にしながら共助アプリベンダー間で合意を形成する。	• OIXトラストフレームワーク等を参照しながら、実際の運用を見据えた共助トラストフレームワークを作成する。 • 一定の基準を満たして認定された発行者や検証者のみがエコシステム内で活動できる仕組み（トラストリスト）を作ることで、ガバナンス上の信頼の起点を明確にできるか検証する。
【UI/UX】 共助実績の活用について、ステークホルダーが価値を感じるユースケースを作ることができるか。	• 共助実績を活用することで個人のトラストを向上したり、現状は可視化できていない属性情報に価値を付与することが出来るのではないか。 • 共助実績を3rd party企業が活用してインセンティブを提供することで、共助エコシステムの活性化を実現することができないか。	• 共助実績の活用シーンを共助ベンダーとディスカッションしながら検討。各ステークホルダーの視点でメリットが出るユースケースを抽出する。 • ユースケースを可視化するためのモックアップデモを作成。Digital Identity WalletのUI/UXとユースケースの実現性を検討する。
【UI/UX】 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の調査	• 生活者が必要性を強く感じる体験を設計し、モックアプリを作成しユーザーへヒアリングを行う	• 各共助アプリから5名程度のユーザーを紹介いただき、モックアプリを操作いただき、インタビューやアンケートを行う
【ビジネスモデル】 社会実装可能なビジネスモデル調査	• 海外事例を参考にビジネスモデル、実現までのプロセスなどを調査する。	• 台湾のTuring Space社に運用している海外ボランティアの事例をヒアリングする。

3.2. 本事業におけるスコープ

Confidential DNP

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
- IIWでガバナンス関連ワークショップ実施
- OIX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

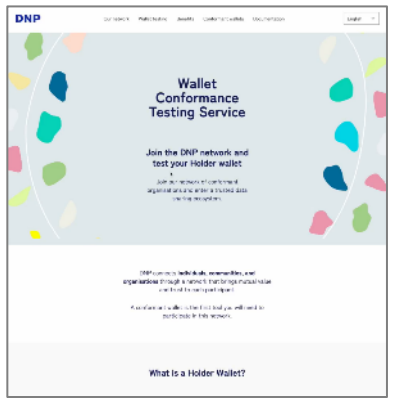
Confidential

DNP

プロトタイプ システム開発

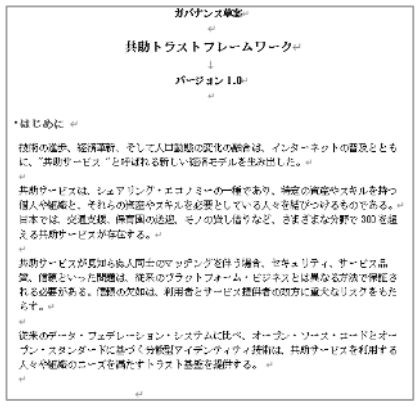
- ✓ 要件定義書
- ✓ 共助Walletアプリ
- ✓ 共助Walletバックエンド
- ✓ 発行、検証バックエンド

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

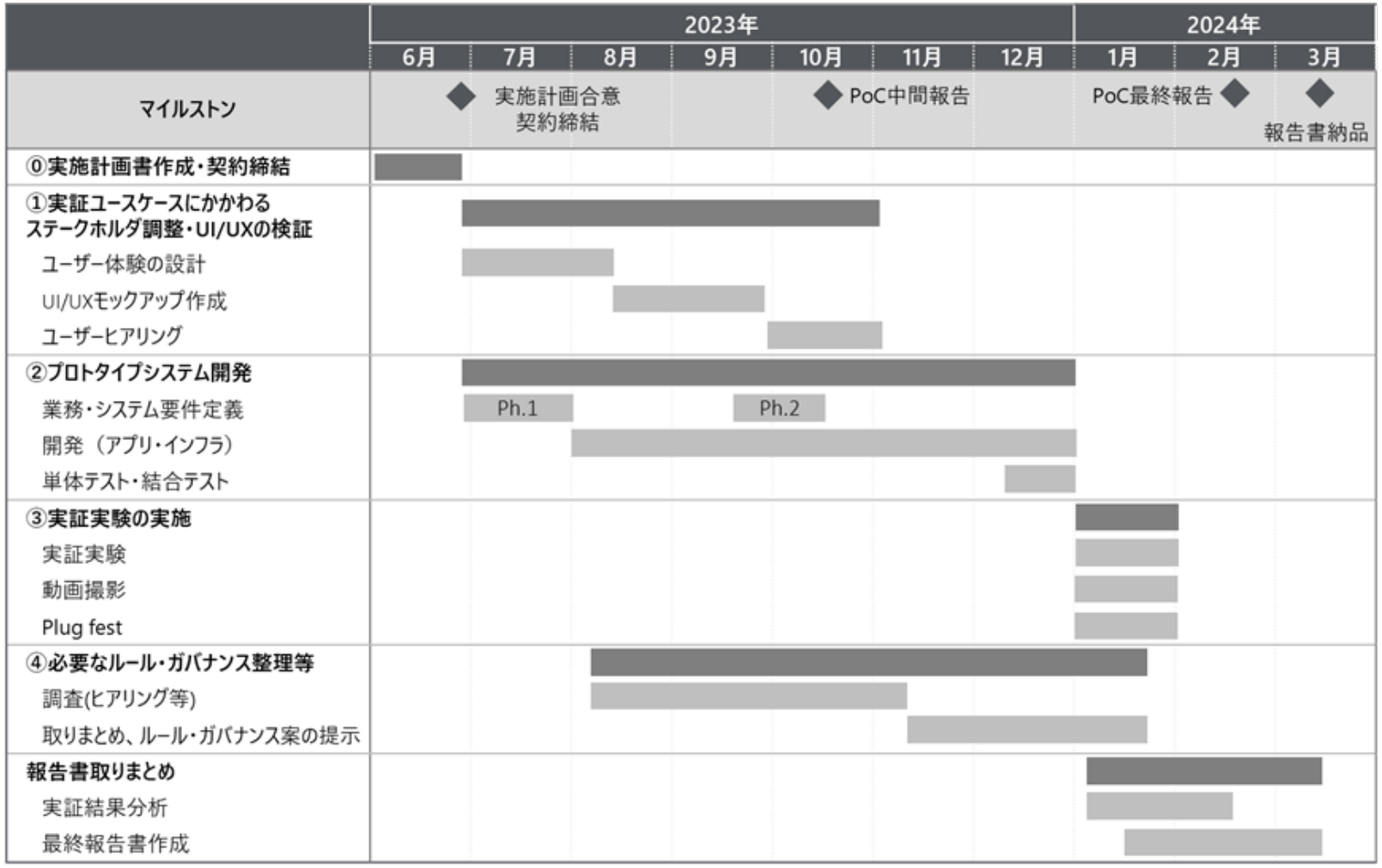
UI/UXモックアップ

- ✓ 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 調査

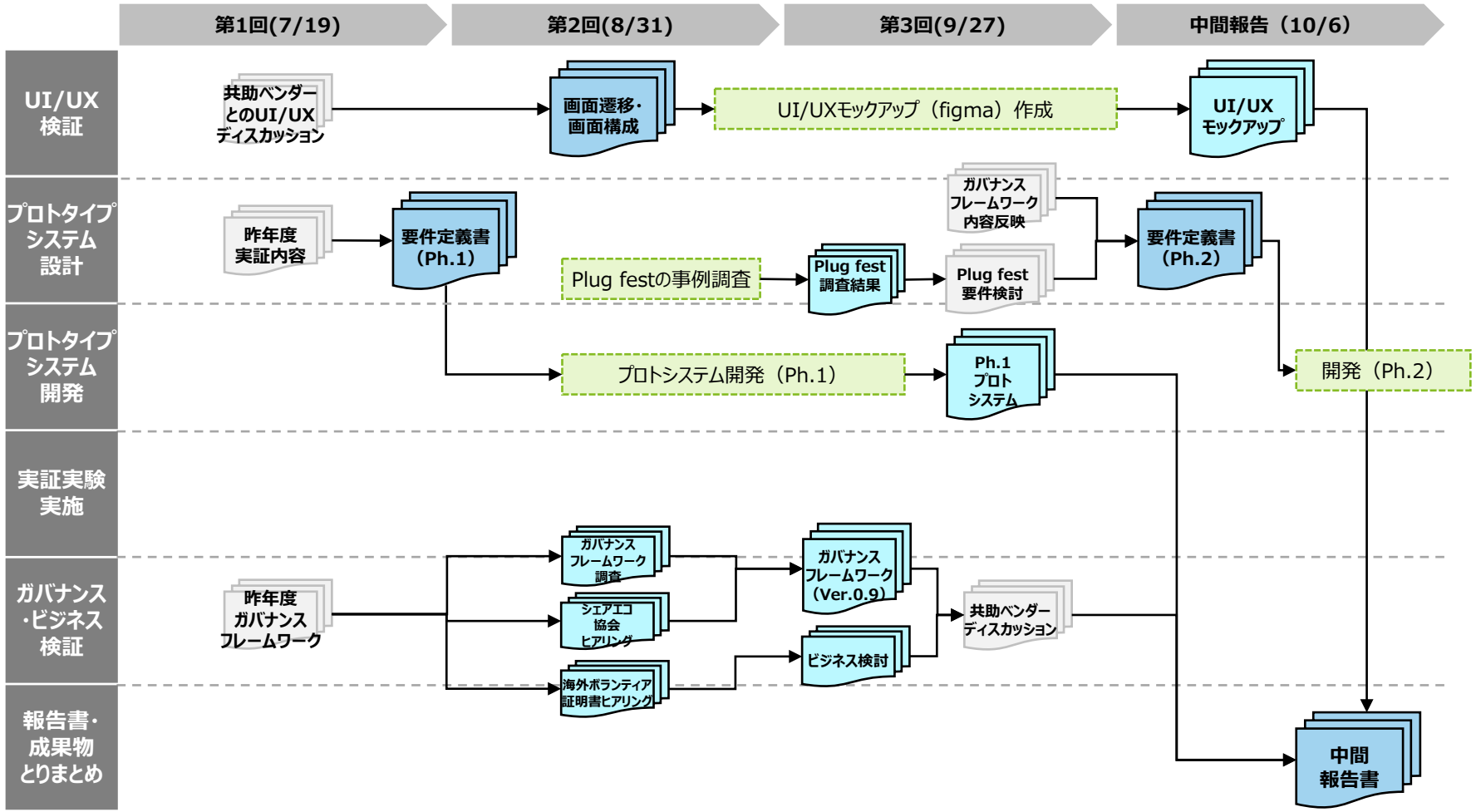
- ➢ UI/UXに関するユーザーヒアリングの結果レポート

3.4.　スケジュール
3.4.1.　全体スケジュール

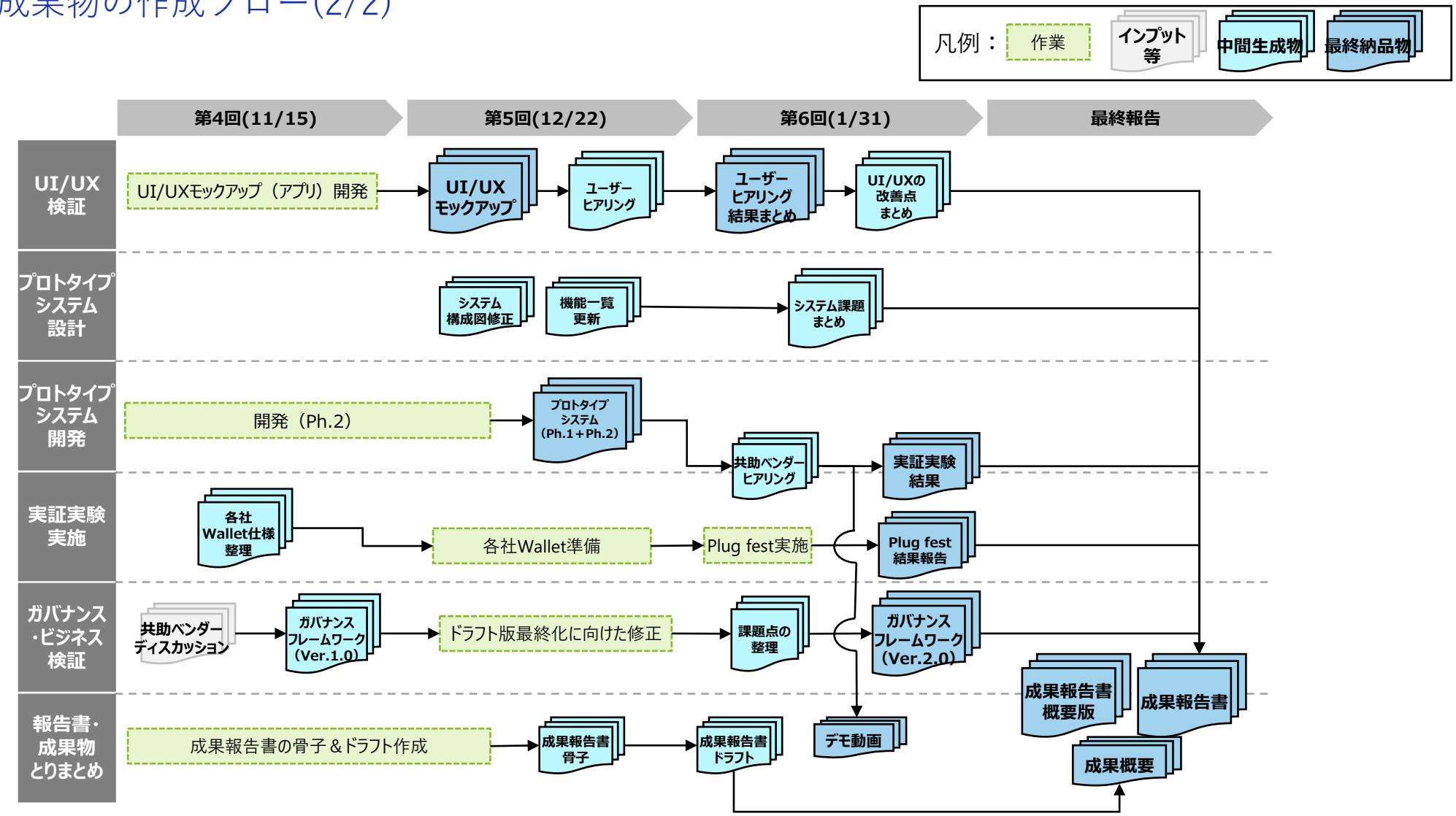


3.4.　スケジュール
3.4.2.　成果物の作成フロー(1/2)

Confidential DNP

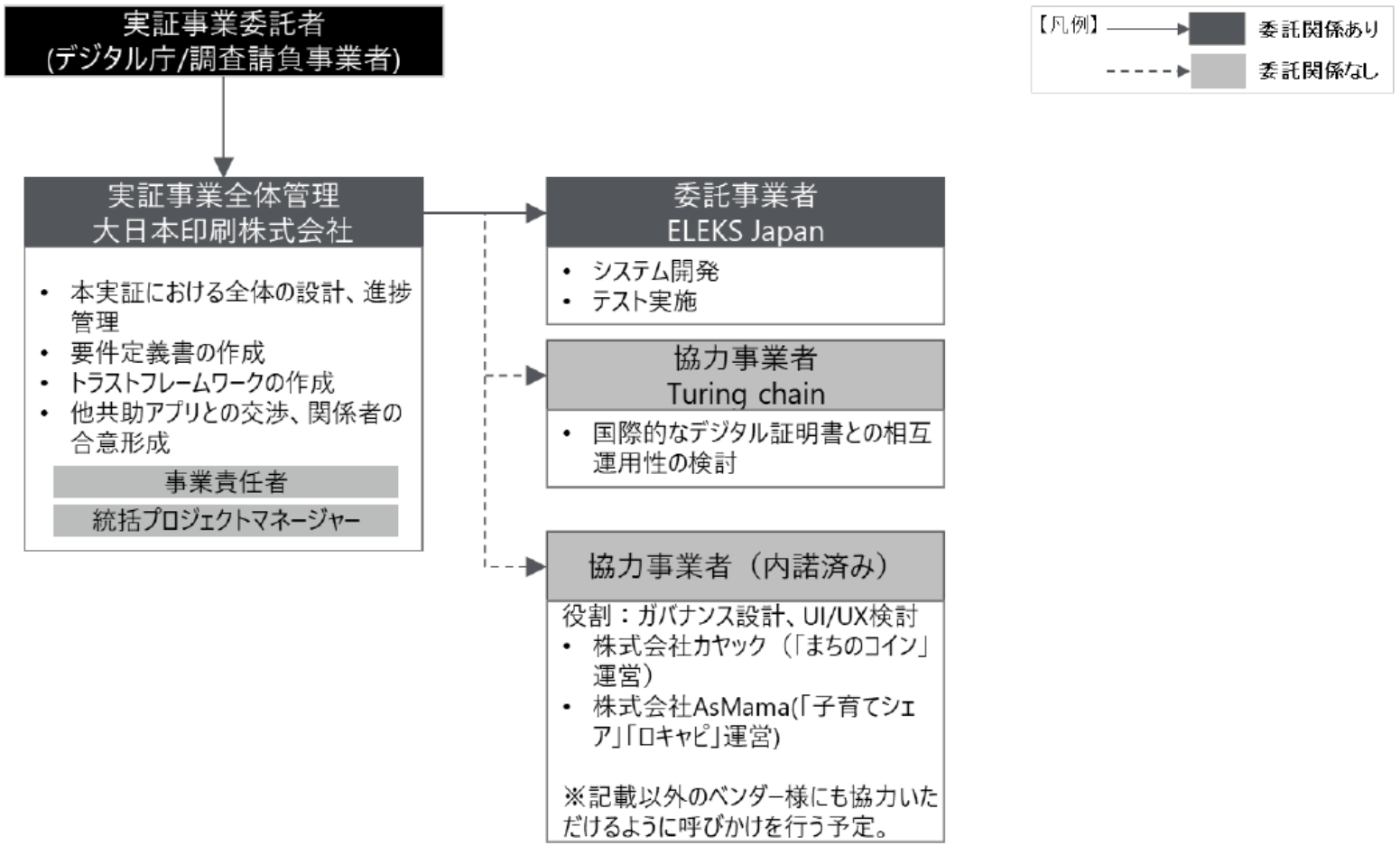


3.4. スケジュール
3.4.2. 成果物の作成フロー(2/2)

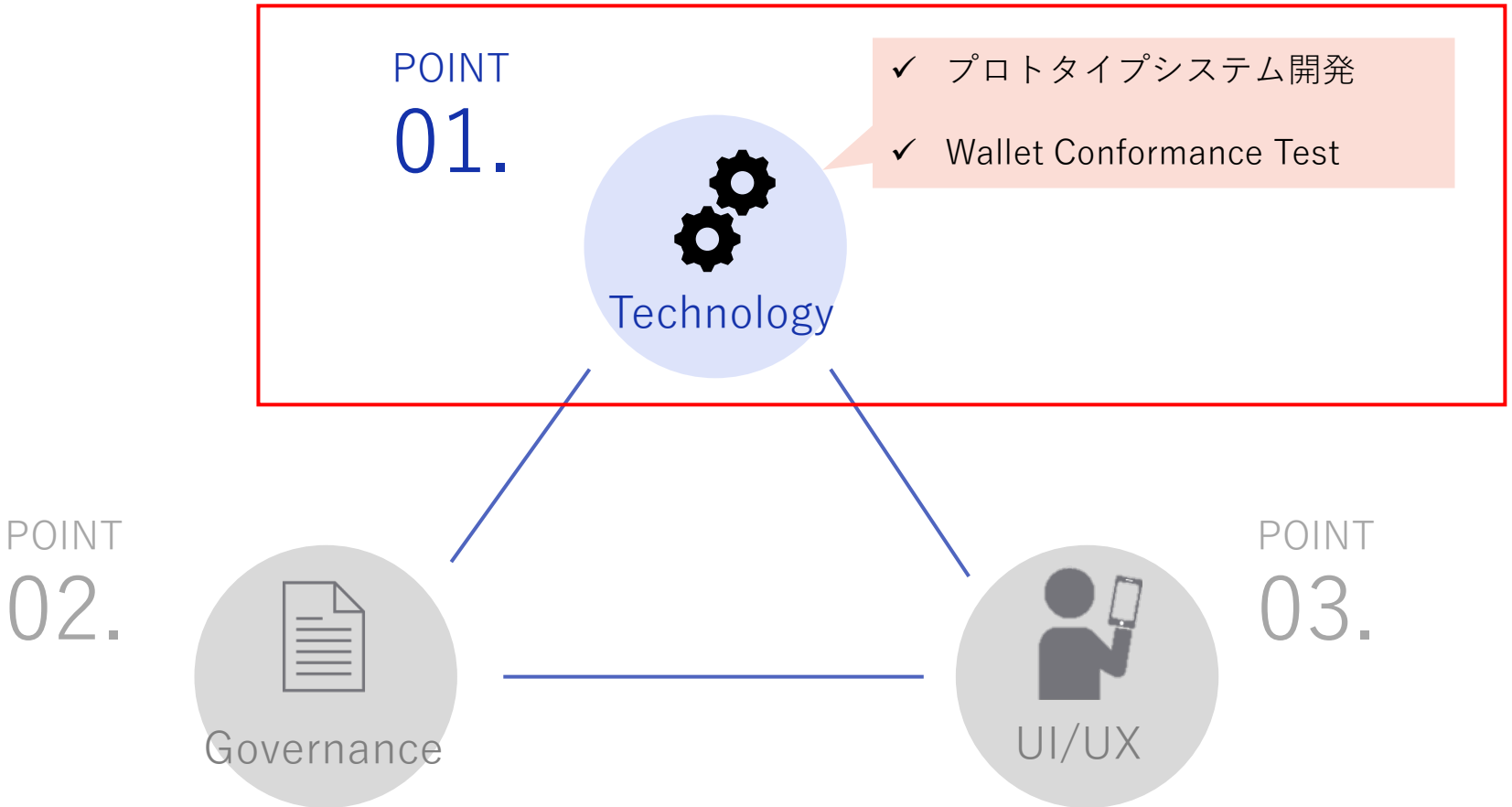


3.5. 実施体制

Confidential DNP

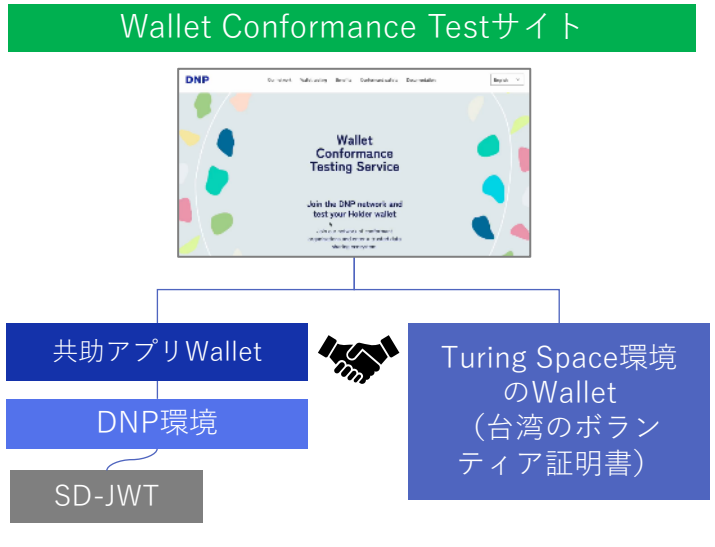


4. 実証（プロトタイプ開発）



4.1. 実施概要
4.1.1. プロトタイプ開発で明らかにする論点とその結果

セキュリティーとプライバシーを考慮したプロトタイプシステム開発と、他社Walletとの技術的な相互運用性の検証を実施。

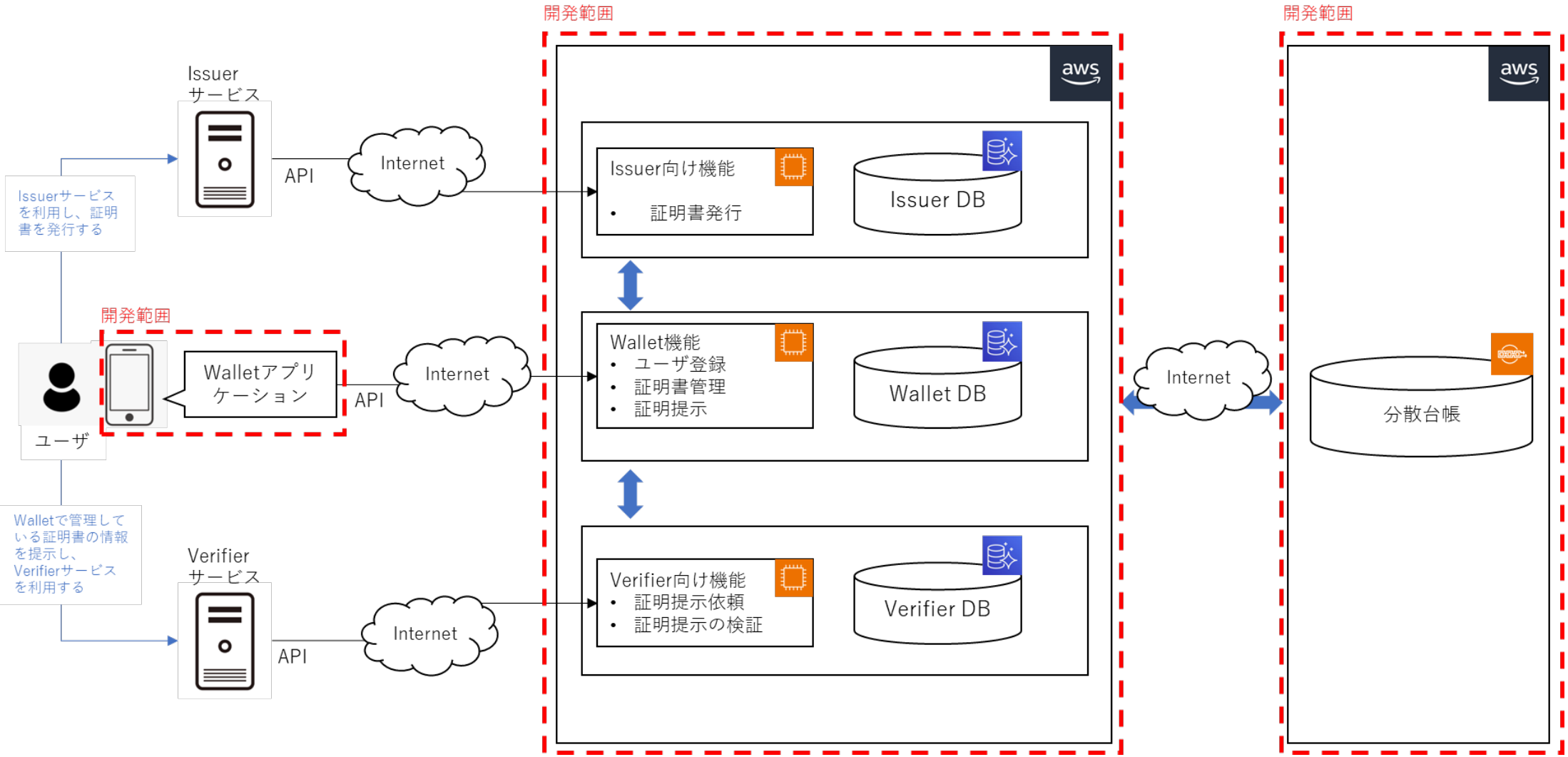
	Ph.1 プロトタイプシステム実装	相互運用性テストの検討	Ph.2 Walletの相互運用性テスト実施
論点	➢ 社会実装上、セキュリティやプライバシーの観点で問題のないシステムアーキテクチャーをどのように実現可能か。	➢ 共助トラストエコシステムにおいて相互運用性を見据えた標準仕様を策定するためにはどのような施策を実施すべきか。	➢ 共助エコシステムの形成において、技術的な相互運用性を担保するための技術プロファイルの作成及びそのテストを実施するために、どのような施策が必要か。
実施概要			
結果	✓ 共助ユースケースを想定したWalletアプリのフロントエンドと、VCの発行～検証を行うバックエンドの仕組みを開発して連携することができた。 ✓ AnonCredsを使ってPredicateの実装も行なった。	✓ 相互運用性の観点を重視した実装のためにSD-JWT、OID4VCI/VPを技術プロファイルとして設定。 ✓ 複数のクレデンシャル形式の切り替えは開発コストが高いため、別環境を用意。	✓ 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。Walletのテストができる環境を用意。 ✓ Turing Space社のWalletにて一定条件下でのテスト合格。

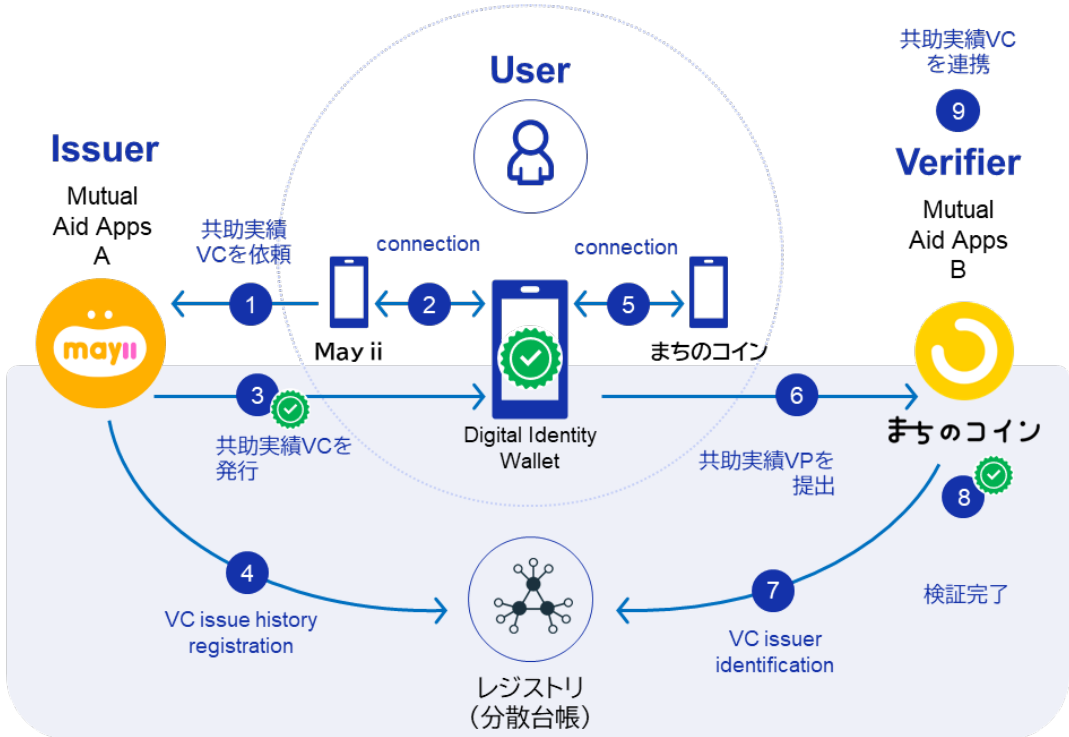
プロトタイプシステム開発のための技術検討の調査で、実装しているユースケースの多かったHyperledger Indy/Ariesを選択。

組織名	SITA	IDunion	Instnt	BRITISH COLUMBIA	DICE ID
ユースケース	Happy Traveler Card - Health credential solution in Aruba	an open ecosystem for decentralized identity management	Instnt Access - Portable KYC Solution	Energy & Mines Digital Trust	Decentralized Identity and Credential Exchange
プロジェクト	➢ Hyperledger Indy ➢ Hyperledger Aries	➢ Hyperledger Indy ➢ Hyperledger Aries	➢ Hyperledger Indy ➢ Hyperledger Aries	➢ Hyperledger Indy ➢ Hyperledger Aries	➢ Hyperledger Indy ➢ Hyperledger Aries
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。	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。	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。	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。	Hyperledger IndyとAriesを利用するDICE IDは、ユーザー所有のIDウォレットに保存された、自己検証可能で改ざん防止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。
Webサイト	https://www.sita.aero/resources/videos/happy-traveler-card/	https://idunion.org/?lang=en	https://www.instnt.org/access	https://digital.gov.bc.ca/learning/case-studies/energy-mines-digital-trust-pilot/	https://www.diceid.com/
追加日	2022/5/15	2022/8/23	2023/3/18	2023/7/3	2024/2/6

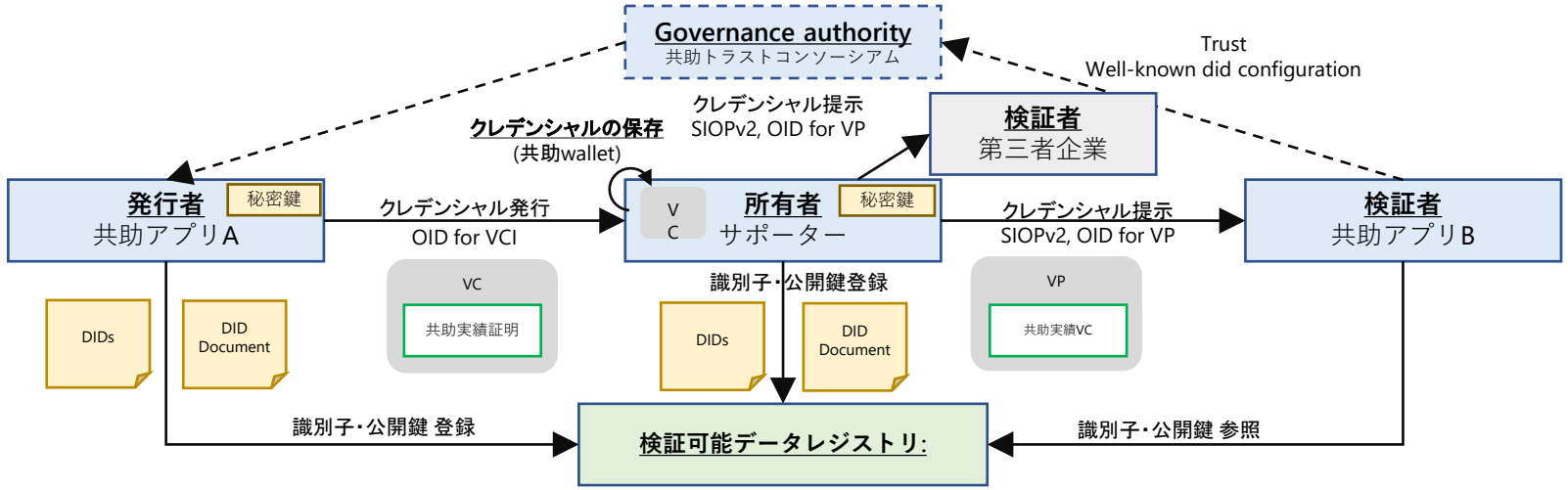
https://www.hyperledger.org/learn/use-case-tracker

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





ペイン：ユーザーのトラスト検証について	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)
プロフィール表示やSNS連携など工夫を行っているが、ユーザーの自己申告に基づくものであり、内容の信ぴょう性を検証する方法がない。	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	分散型IDシステム	全ての共助アプリの関連情報を繋ぐ集中型のデータベースを中心に据えたエコシステム形成は実現性に乏しい。分散型IDシステムの技術を活用し、Verifiable Credential（VC）として共助実績を連携する
アプリ内のユーザー評価システムによってトラスト検証を促す場合もあるが、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。			



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
共助実績の共有	共助実績の内容	VCの署名検証	共助アプリB	サポーター	共助アプリA	Cloud Wallet	FIDOの生体認証によって本人のみがアクセスできるように制御	• サポーターのトラストを向上 • 共助アプリの種類ごとにジャンル分けして実績を表示
本人確認＋αの情報付与	共助アプリでの実績や受講履歴	VCの署名検証	共助アプリB	サポーター	共助アプリA	Cloud Wallet	FIDOの生体認証によって本人のみがアクセスできるように制御	• サポーターのトラストを向上

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

Confidential DNP

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 ①共助実績の内容が改ざんされていないことの確認 ②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・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）
保有者のデータの置き場所	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。

証明書名称	説明
記載情報（クレーム）	・発行日、有効期限 ・発行者 ・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 ・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）の署名検証及び、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。 • 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形式でリクエストが可能とする。 • 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。）
識別子	
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。 • 検証者は、識別子からVDRの発行者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。

【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】

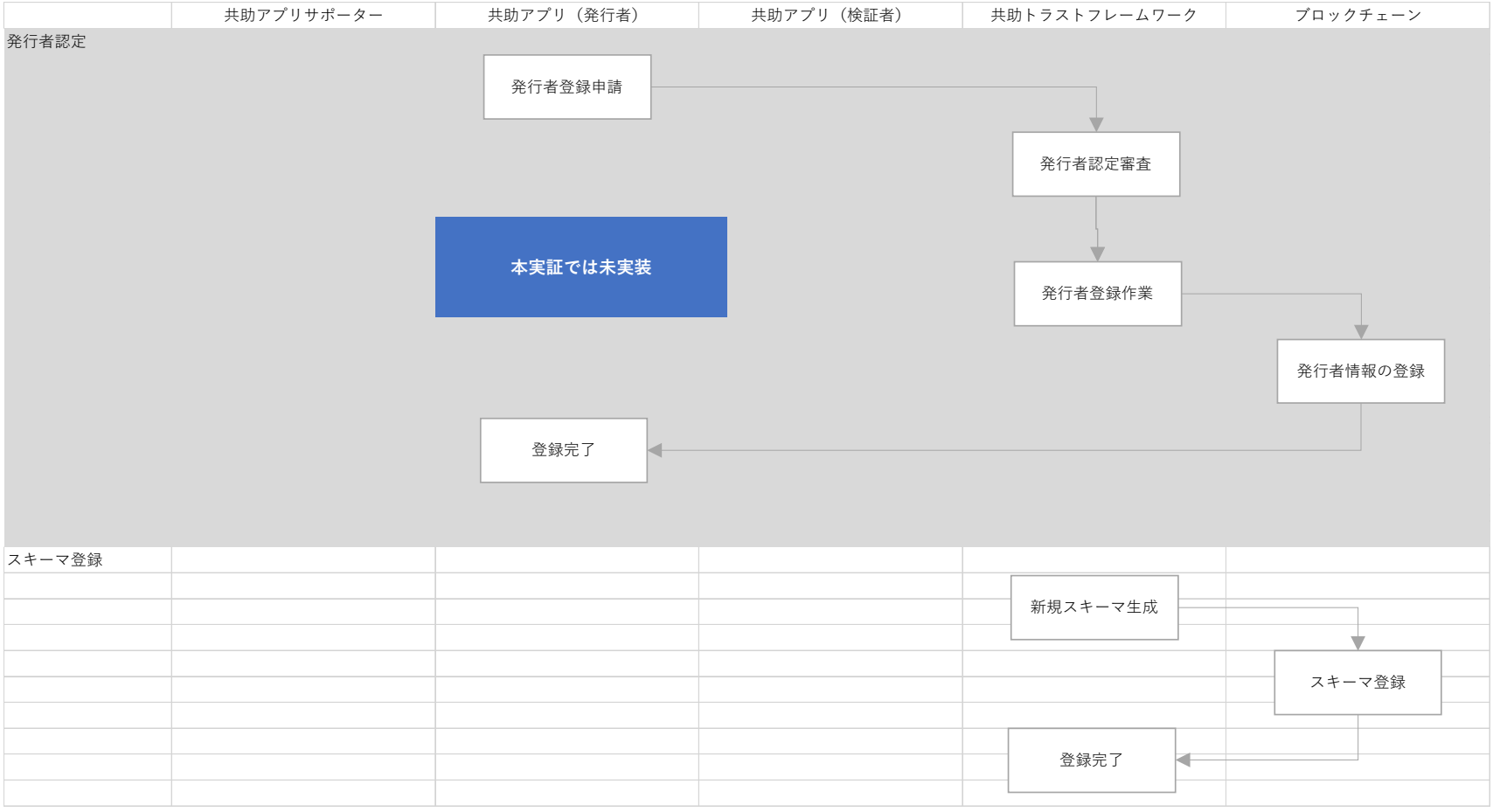
項目	説明	
	no.1	no.2
合意の主体	共助アプリ（発行者）と共助アプリサポーター	共助アプリサポーターと共助アプリ（検証者）
合意の対象	サポーターが実施した共助実績情報（VC）	サポーターが実施した共助実績情報（VP）
合意の条件	共助アプリ（発行者）がVCとして発行する共助実績VCの内容をWalletアプリを通じて共助アプリサポーターへ提示し、共助アプリサポーターが承認することで合意されたとする	共助アプリ（検証者）が要求する情報を提示し、共助アプリサポーターが開示する内容を選択、VPの共有を承認することで合意されたとする
トレースの対象	共助アプリ（発行者）と共助アプリサポータ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。

・合意内容のトレース（確認）は、合意主体のみが可能であり、第三者が単独で確認する手段は用意されていない。
・第三者が合意内容を確認するためには、各主体の許諾のもと、システムのログを確認する必要がある。
・しかし、本システムでは、ログに対する耐改ざん性が担保されておらず、現時点では法的根拠が薄いと考えられる。

4.4. 企画・開発物
4.4.1. 業務フロー①

Confidential

DNP



4.4. 企画・開発物
4.4.1. 業務フロー②

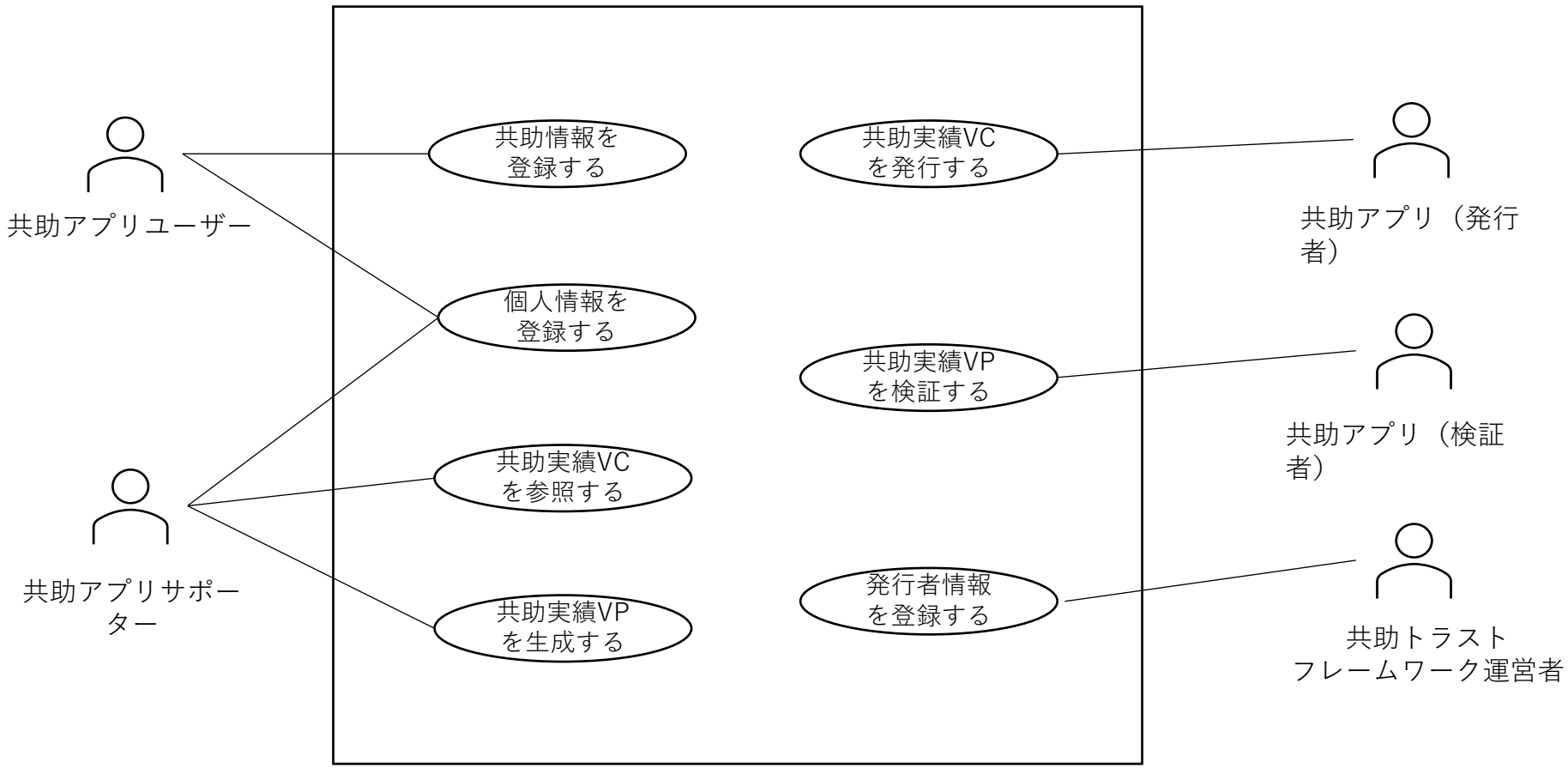
Confidential

DNP

4.4. 企画・開発物
4.4.1. 業務フロー③

Confidential

4.4. 企画・開発物
4.4.2. ユースケース図

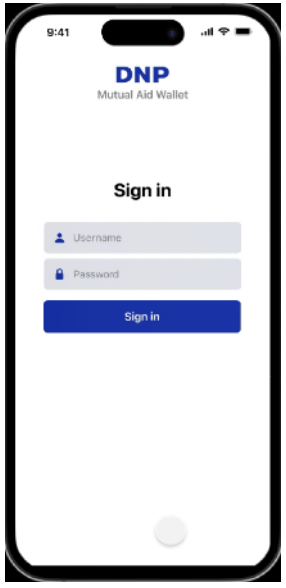


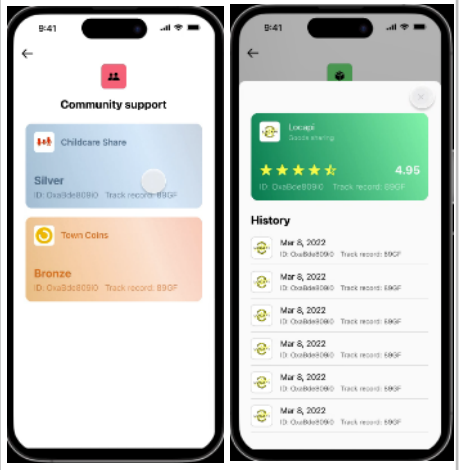
4.4. 企画・開発物
4.4.2. ユースケース図

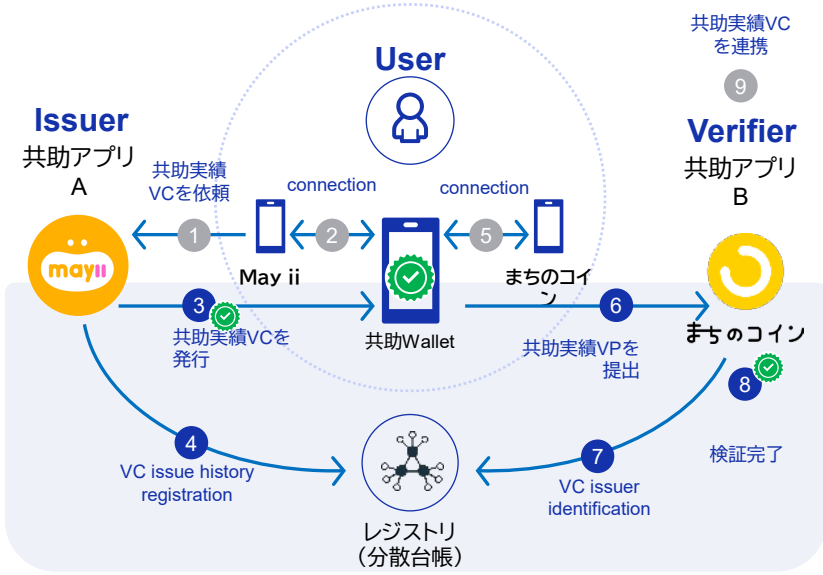
Hyperledger Indy/Ariseのフレームワークで証明書の発行～所持～検証のプロトタイプシステムを開発。

プロトタイプシステム開発を実施したシーンのイメージ

シーン0	シーン1	シーン2	シーン3
Walletアプリをインストールした際、端末の持ち主とWalletアプリの所有者を紐づける	Walletで証明書一覧を確認する	共助アプリから共助実績VCを発行し、Walletに保存する	共助アプリへWalletから共助実績VPを連携して、VPを検証する







4.4. 企画・開発物
4.4.3. 操作画面（UI）

Confidential DNP

ログイン → 証明書一覧 → 証明書詳細

証明書追加オファー一覧 → 証明書追加オファー詳細

Issuerから証明書発行の許可依頼（オファー）が送付されると、Wallet上に表示される。

ユーザはWallet上でオファーの内容を確認し、承認すると証明書が発行される。

証明リクエスト一覧 → 証明リクエスト詳細 → Claim選択 → Claim選択確認 → VP提示完了

Verifierから証明リクエスト（VPの提示要求）が送付されると、Wallet上に表示される。

ユーザはWallet上で証明リクエストの内容を確認。

所有している証明書から提示したい属性（Claim）を選択するとVPが生成され、Verifierに送付される。

送付されたVPは検証され、ステータスが更新される。

4.4. 企画・開発物
4.4.4. 機能一覧/非機能一覧

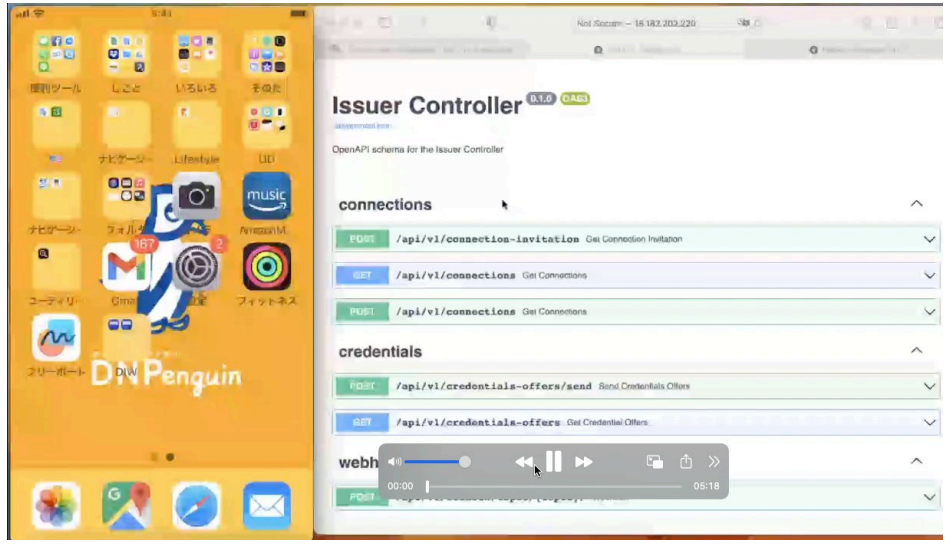
ログイン	ログイン	ユーザID/PWを入力してログインする このフェーズでは新規会員登録機能は実装せず、DBに直接登録する
	ログアウト	ログアウトし、ログイン画面に遷移する
資格証明書	証明書一覧参照	自分の保有している証明書を一覧で表示する 証明書を選択すると証明書詳細画面に遷移する
	証明書詳細参照	選択した証明書の詳細を表示する
	証明書削除	選択した証明書を削除する 証明書詳細画面から操作し、削除前には確認のメッセージを表示する
オファー	オファー一覧	Issuerからの証明書発行の許可依頼（オファー）を一覧で表示する オファーを選択するとオファー詳細画面に遷移する
	オファー詳細	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 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 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 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 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 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 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 証明リクエストのステータスを「却下」に変更する

4.4. 企画・開発物
4.4.4.1 デモ動画

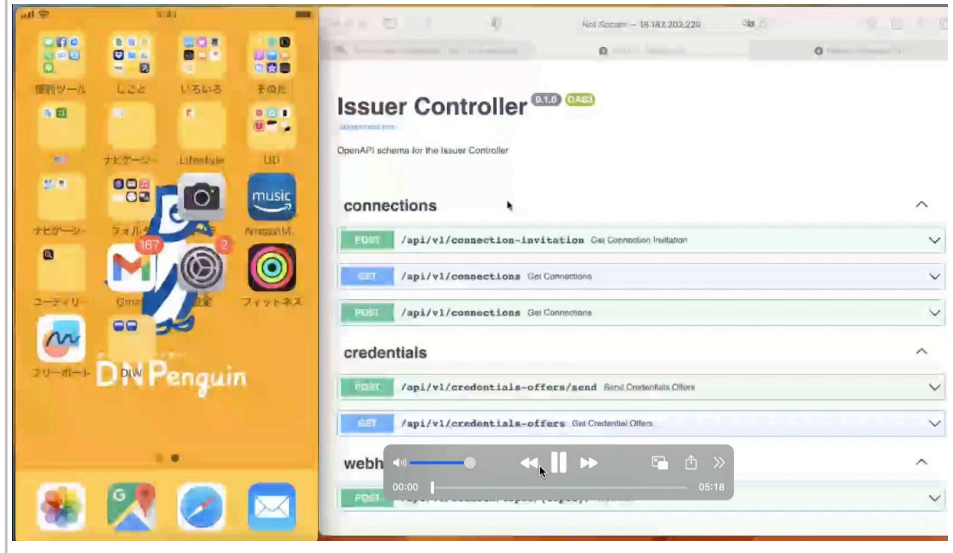
共助ユースケースを想定したWalletアプリのフロントエンドと、VCの発行～検証を行うバックエンドの仕組みを開発して連携。
ZKP暗号を用いたクレデンシャル提示・検証を実装することで、ユーザーのプライバシーに配慮したシステムを実現した。

ログイン

発行～証明書受け取り



検証



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

Confidential DNP

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。	• AnonCredにはホルダーバイ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つながる。	• 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、ステークホルダーからサービス（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することが可能。
■ 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. 企画・開発物
4.4.4.3. (非機能要件)大規模・商用・社会実装時のシステム・運用方針

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。 AnonCredではスキーマごとにすくなくとも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いけず、この管理が負担になると考える。 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。
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。

DNP

共助実績証明書
基本となるスキーマ

- ID
- Issued Date
- Expiration Date
- Issuer / service operator
- Service Category
- Service Signup Date
- Description
- Support Task Completions
- Total Support Hours
- User Binding Attributes
  -Name
  -Financial Institution ID

ディスカッションとなったポイント

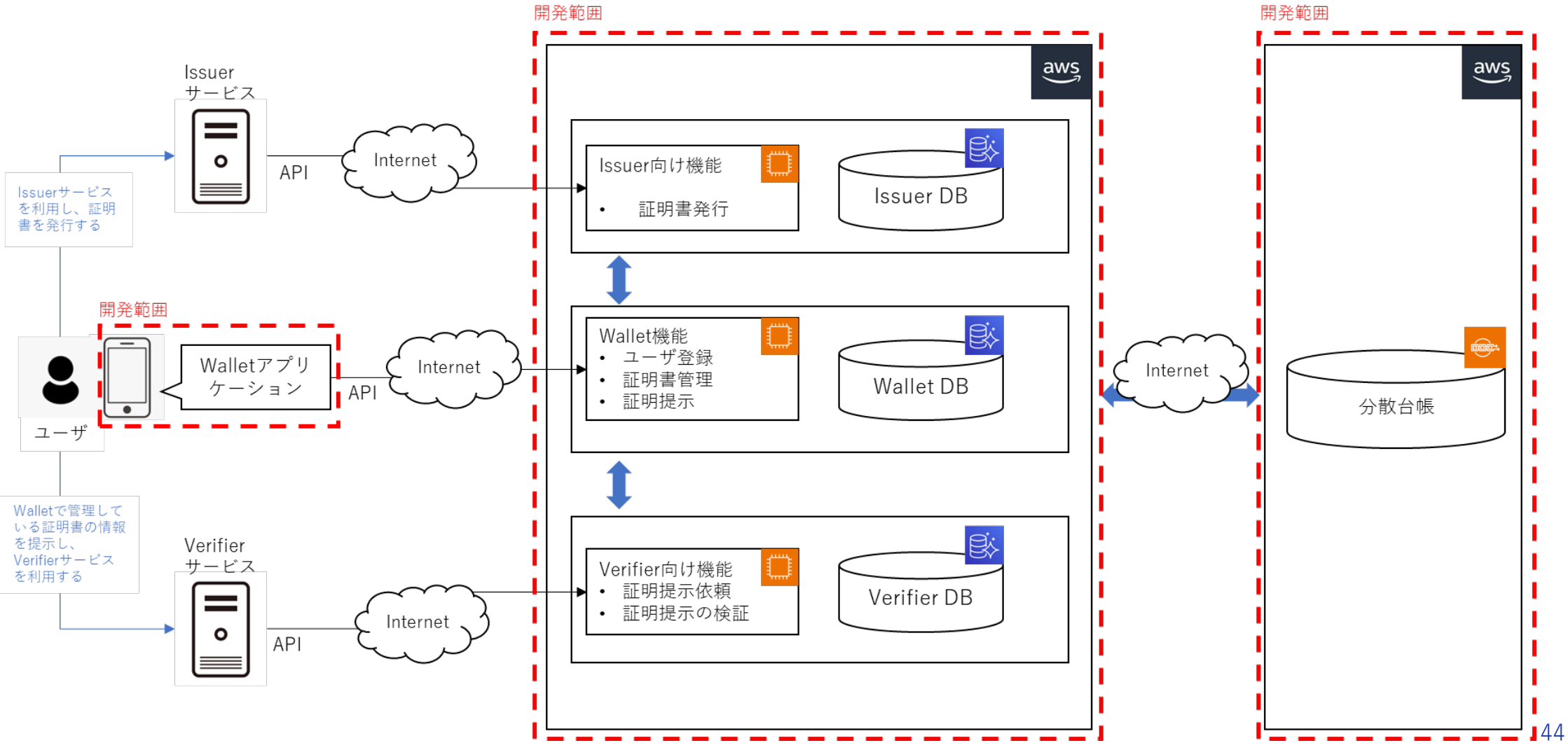
■ 検証者は何を重視するか？
➢ 検証者にとって、証明書の発行日が新しいことはトラストを検証する上で重要である。スキーマの中にも証明書の発行日を明示し、新しい証明書かどうかが分かりやすいようにする。

■ 証明書の無効化について
➢ 発行者が任意のタイミングで無効化？使用期限を設ける？
➢ 前者は実装が複雑になるため、使用期限を設ける仕様に決定。
➢ 日数については、ユースケースごとに策定（議論を継続）

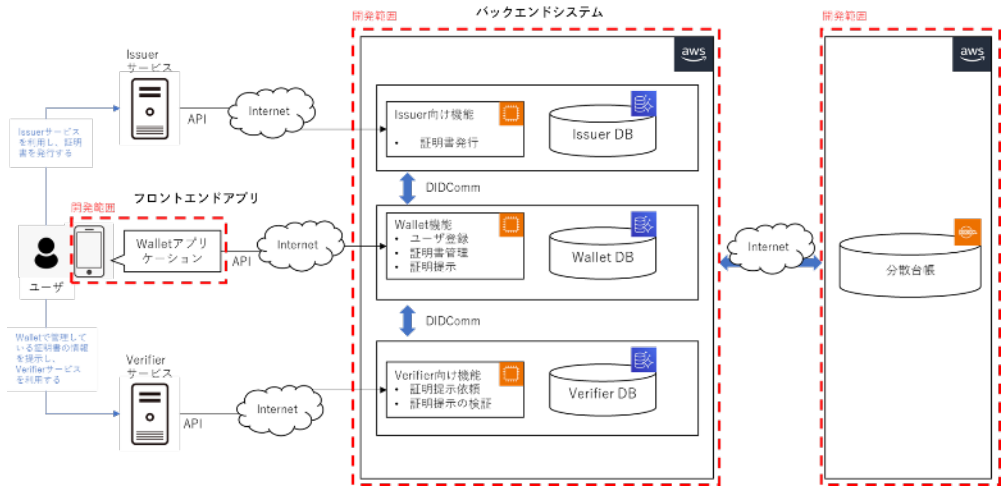
■ 悪意のあるユーザーの対策
➢ 低評価がついた場合に、別アカウントを作成して新たに実績を作ろうとする人への対策をどうするか？
➢ アカウントの作成日を入れて、経験の浅いユーザーには簡単に証明書を発行しないようにする。（発行に必要な最低継続日数を設定）

■ 本人とクレデンシャルの紐付け（※今後実装の方法については要検討）
➢ ①本人情報と共助実績の紐付け or ②別のVCと共助実績を紐付け
➢ ①についてはマイナンバーカードを使って紐付け
➢ 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

4.4. 企画・開発物
4.4.6. 実験環境



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)
Hyperledger Indy/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.



ユーザーが必要な情報のみを検証者に提示できるシステムの実装に成功。一方で、技術面だけでは解決が困難な課題もあった。

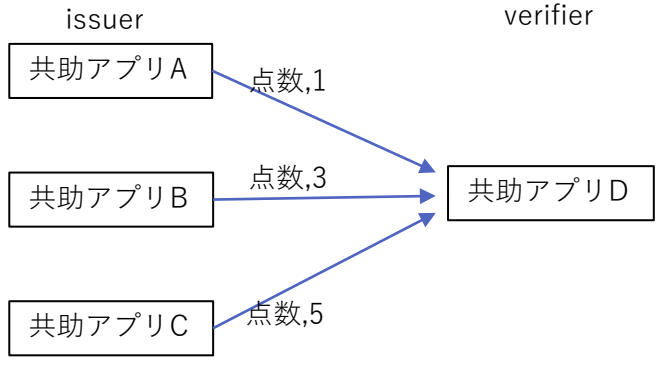
成果

- 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を使ってPredicateも実装でき、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提示が可能になった。
- 一方でAnoncredsの実装を通じて、構造の複雑性やドキュメント整備の課題から実装難易度が高いことが判明した。

技術的な課題

ユースケースの想定（やりたかったこと）

“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考えていた。



実装可能なこと

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。

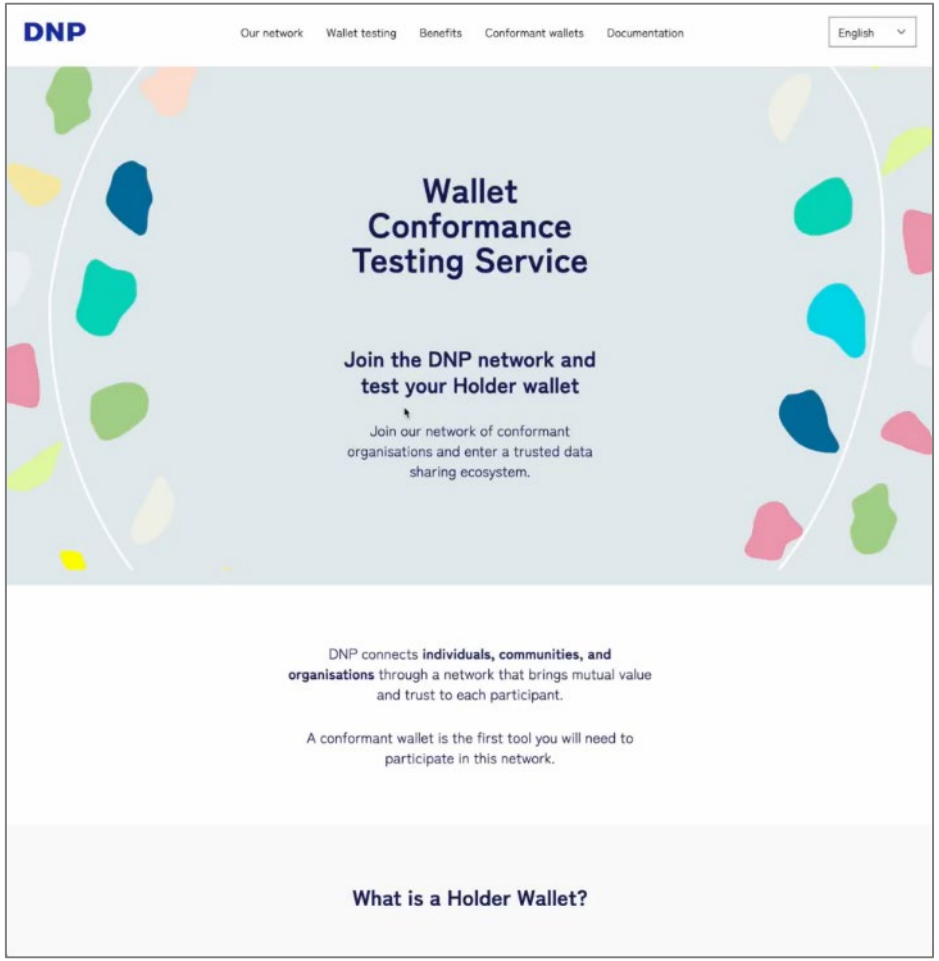
評価値の合算や平均は、不可。⇒VC/VPの受け渡しの仕組みの外側で実装しなければならない。

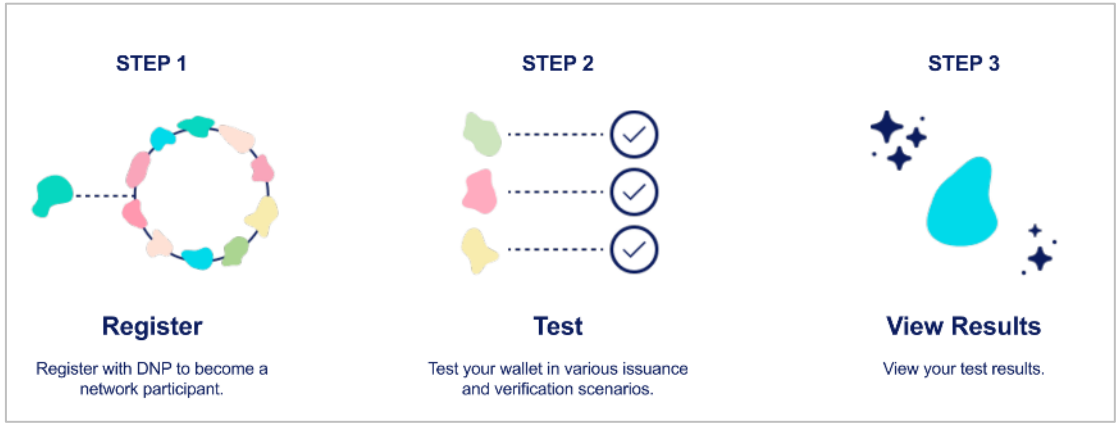
点数の意味も1/100点なのか1/10点なのかなど、アプリによって意味合いが違うので、統一する必要がある。

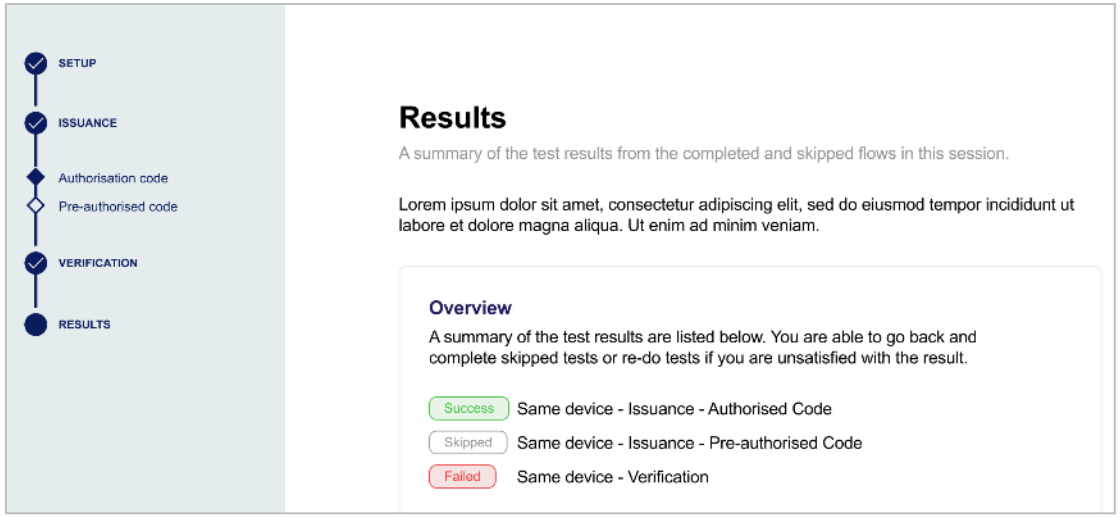
上記のような理由で、共助アプリ間でのスキーマに対するルール作りが必要となる。コンソーシアムの必要性、重要性がより明確になった。

4.4. 企画・開発物
4.4.9. Ph2.相互運用性のテスト

指定された技術仕様に準拠しているか、Walletの相互運用性をテストすることができるConformance Testサイトを用意。







4.4. 企画・開発物
4.4.10. Wallet Conformance Test テスト項目

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。

Documentation

This document describes the Wallet Conformance credential exchange profile.

- Summary
- Credential Format
  - Key Management
    - Issuer Key Management
    - Holder Binding
  - OpenID4VC Credential Format Profile
    - Format Identifier
    - Credential Issuer Metadata
    - Verifier Metadata (Provisional)
- Signing Algorithm
- OpenID for Verifiable Credential Issuance
  - Generic Flow
  - Pre-Authorized Code Flow
    - Detailed Flow
  - Authorization Code Flow
    - Detailed Flow
  - Credential Offer
  - Authorization Endpoint
  - Token Endpoint
  - Credential Endpoint
- OpenID for Verifiable Presentation
    - Detailed Flow
  - Authorization Request
    - Universal link
    - Authorization Request URI
    - Self-Issued OP Request Object
    - Self-Issued OP Request Parameters
    - Verifier/RP Registration Metadata
    - Presentation Definition
  - Authorization Response
- Self-Issued OP v2
- Privacy & Security Considerations
- Normative References
- Informative References
- Appendix A
  - JSON Schema for supported Presentation Definition

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 Pre-Authorized Code Flow • User Pin Authorization Code Flow • PAR Only single, immediate credential issuance supported	OIDF OID4VCI (draft 13)
Verification	OID4VP	OIDF OID4VP (draft 10)

Anoncreds

評価	ポイント
○	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、）すでに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。
×	AnonCredではスキーマごとにすくなくとも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いけず、この管理が負担になると考える。

現在、Hyperledger Ariesのコミュニティ内でも相互運用性を見据えたSD-JWT、OIDFの規格への適応の議論が進みつつある。

SD-JWT

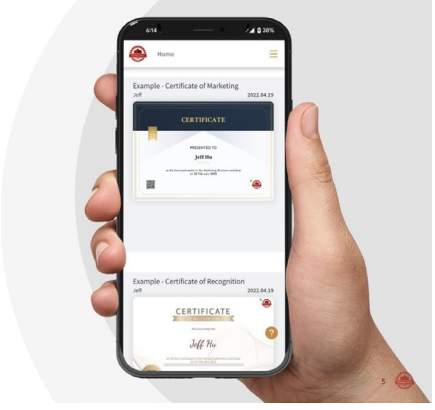
評価	ポイント
○	構造や検証の仕組みが非常にシンプルであるため、相互運用性の面でのハードルは低いと考えられる。
○	既存のPKIの仕組みを活用したSD-JWTではスキーマごとに署名鍵を生成する必要が無いのでこの負担が軽減されると考える。
△	EUDIW等で必須のフォーマットになっており、国際的な相互運用を考えると重要度が高まっている。（EUDIWのアーキテクチャはあくまでドラフトで今後も変わる可能性がある。）
×	毎回、同一のSD-JWTを検証者に渡すことになるので名寄せが起こる可能性があり、プライバシー面で課題が残る。

現時点で相互運用性の観点を重視する場合は、シンプルなSD-JWTを使った実装の方がベンダーの負担が軽くなる想定。
ただし現在VCの仕様がW3CとIETFで割れる等、今後の展開については不透明な状況。

Confidential DNP

TURING SPACE

TrustTechを核心としたサービスで、様々な業界での認証問題の解決、
ボーダーレスな信用ネットワークの創造を行う台湾のテクノロジーベンダー。

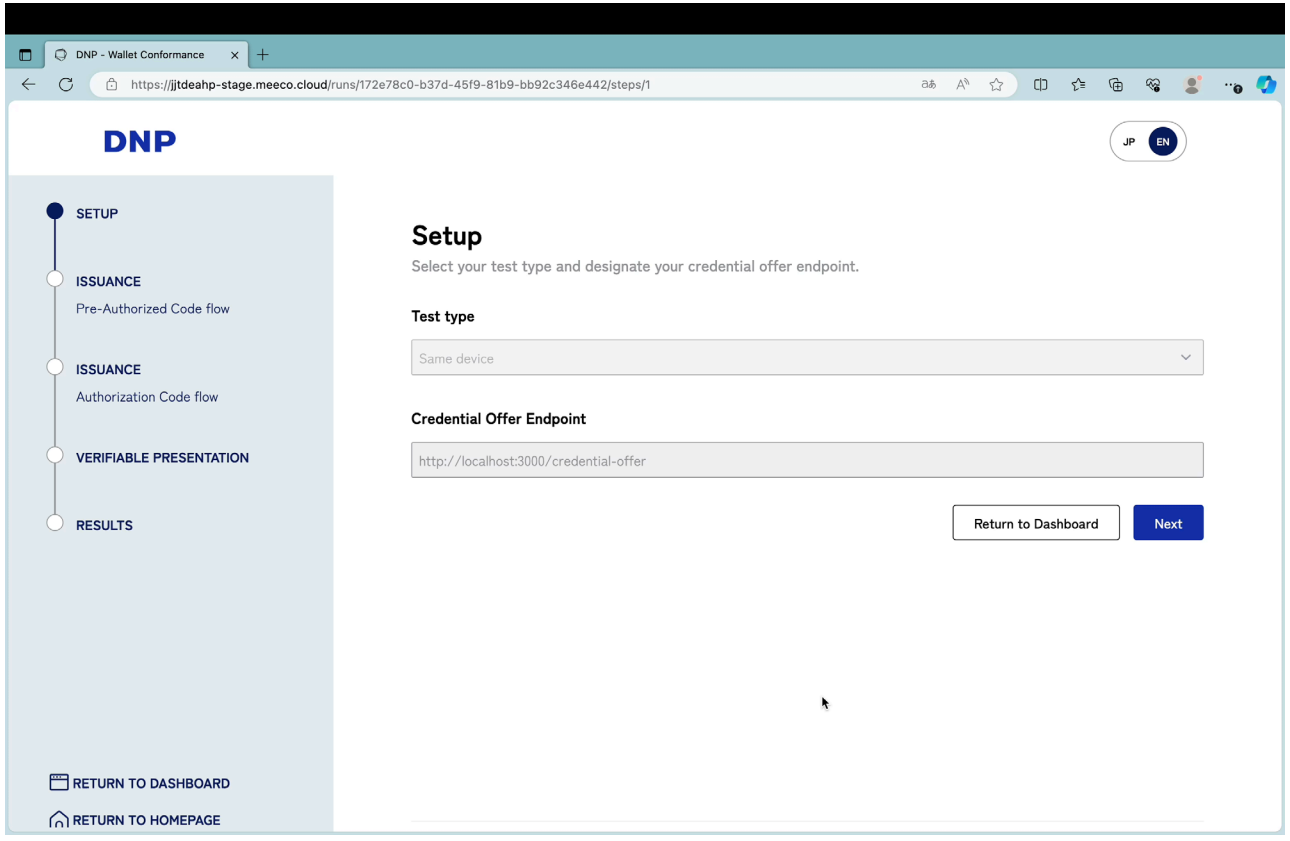


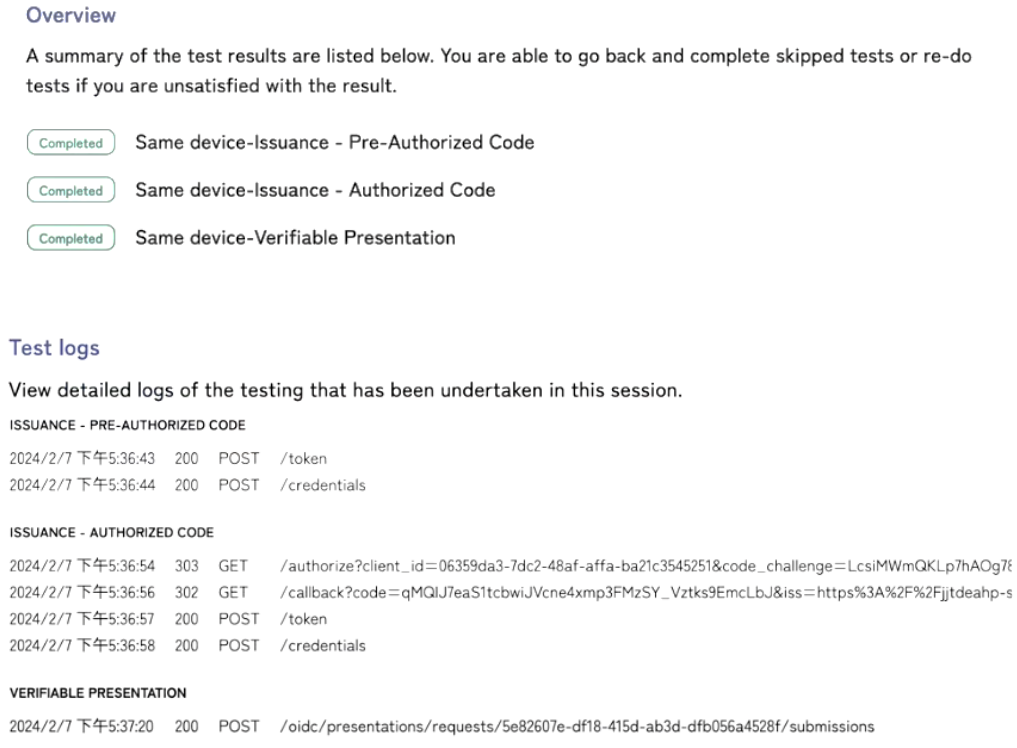
機関名	取り組み内容
台湾デジタル発展部	• 台湾国内優良企業認定証発行 • 電子証明書活用示範プロジェクト（医療機関より開始）
台湾経済部標準検験局	• 国家再生可能エネルギーレコード発行
台湾工業研究院	• 台湾全土の法人履歴書全部事項発行
中小企業総会	• T大使トレーニング証明書発行
資訊工業策進会	• 企業エネルギー履歴書発行
台北市/台北市教育局	• 台北市全体の高校生の卒業証明書発行
桃園市	• ボランティア参加証明書発行
新竹市	• 新竹市全体の高校生の卒業証明書発行 • ボランティア参加証明書発行

4.4. 企画・開発物
4.4.13. 相互運用性テストのデモ

Confidential DNP

Turing SpaceのWalletでOID4VCIのPre-Authorized Code FlowとAuthorization Code Flow、OID4VPのテストにクリア（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。





4.4. 企画・開発物
4.4.14. Ph2の結果・成果

Turing Space社のWalletで相互運用性のテストをクリア。テスト設定が原因で一部完了できていない項目もあるため、今後改良していく。

成果

- 共助エコシステムの拡大を見据えて、実装のしやすさを重視した技術プロファイルを策定。Turing Space社のWalletで相互運用性テストを実施したところ、Same deviceでは成功を確認できた。
- 今後のTrusted webのエコシステムを検討するにあたって、技術的な相互運用性を確認するためのWallet Conformance Testのあり方を提示することができた。

今後の課題

■ Wallet Conformance Test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。

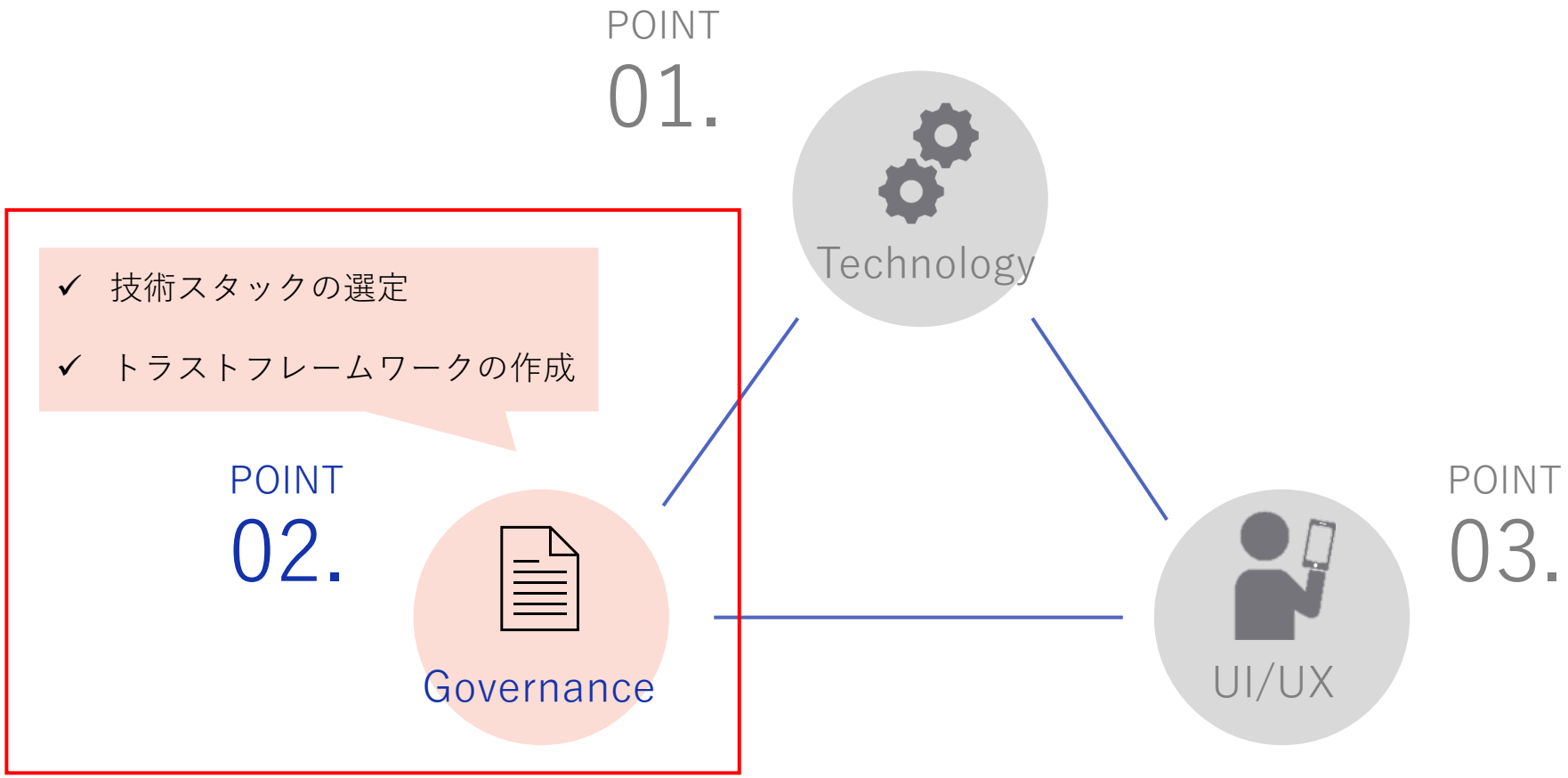
台湾のデジタルボランティア証明書

■背景
従来、ボランティア証明書は紙切符で発行され、生活者は張り付けた手帳を、大学などに提出していた。そのため、手帳で管理する中で紙切符の汚損や紛失、大学側の受領業務の煩雑さが課題となっていた。

■解決
紙切符で発行していた証明書をデジタル化し、データ管理や提出業務の簡易化・効率化を行った。桃園市、台北市で導入。

■用途
国際及び国内双方のボランティア参加者に対して日時、時間数を掲載したボランティア証明書の発行にご活用。
証明書の時間数をポイント換算し地方自治体の定める場所で景品と交換。ボランティア証明書の提示によっては地方自治体の施設などで優待を受けることが可能。

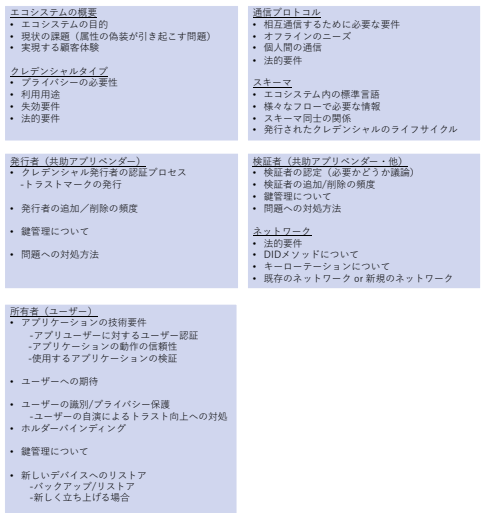
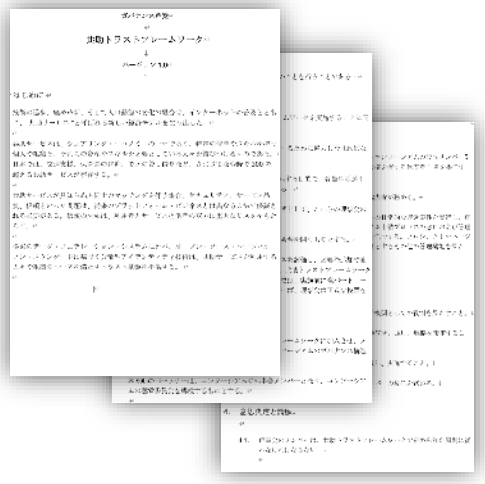
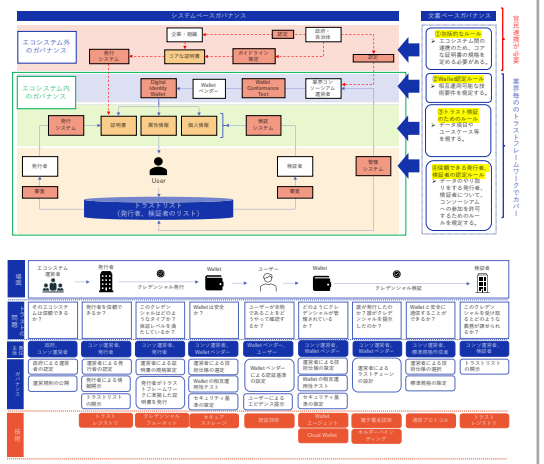
5. 実証（事業実現に向けたガバナンス・コミュニティ等の検討）



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、ステークホルダーの責任分解点を整理した。

	項目整理	トラストフレームワーク作成	IIWセッション・OIXとの議論	ステークホルダーの責任分解点整理
論点	➢ 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。	➢ エコシステム内のリスクを最小限に抑えるためにどのようなルールを検討すべきか。	➢ エコシステム外のステークホルダー（政府）の役割は何か。	➢ 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ーの責任分界点を明らかにする。
実施概要				
結果	✓ トラストフレームワークの全体を５つのブロックに分けて内容を検討。最終的にOIXのホワイトペーパーとも生合成のある項目に整理した。	✓ 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。	✓ 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。	✓ エコシステム内外のステークホルダーを整理し、それぞれの責任分解点について図式化した。各フェーズで起きうるトラストの問題についても可視化した。

5.1. 実施概要
5.1.2. 実施内容・手法：ガバナンス整理

トラストフレームワークの全体を5つのブロックに分けて内容を検討。
現在、各項目のディスカッションを行い、それを基にトラストフレームワークに落とし込む作業を行なった。

エコシステムの概要
- エコシステムの目的
- 現状の課題（属性の偽装が引き起こす問題）
- 実現する顧客体験

クレデンシャルタイプ
- プライバシーの必要性
- 利用用途
- 失効要件
- 法的要件

通信プロトコル
- 相互通信するために必要な要件
- オフラインのニーズ
- 個人間の通信
- 法的要件

スキーマ
- エコシステム内の標準言語
- 様々なフローで必要な情報
- スキーマ同士の関係
- 発行されたクレデンシャルのライフサイクル

所有者（ユーザー）
- アプリケーションの技術要件
  -アプリユーザーに対するユーザー認証
  -アプリケーションの動作の信頼性
  -使用するアプリケーションの検証
- ユーザーへの期待
- ユーザーの識別/プライバシー保護
  -ユーザーの自演によるトラスト向上への対処
- ホルダーバインディング
- 鍵管理について
- 新しいデバイスへのリストア
  -バックアップ/リストア
  -新しく立ち上げる場合

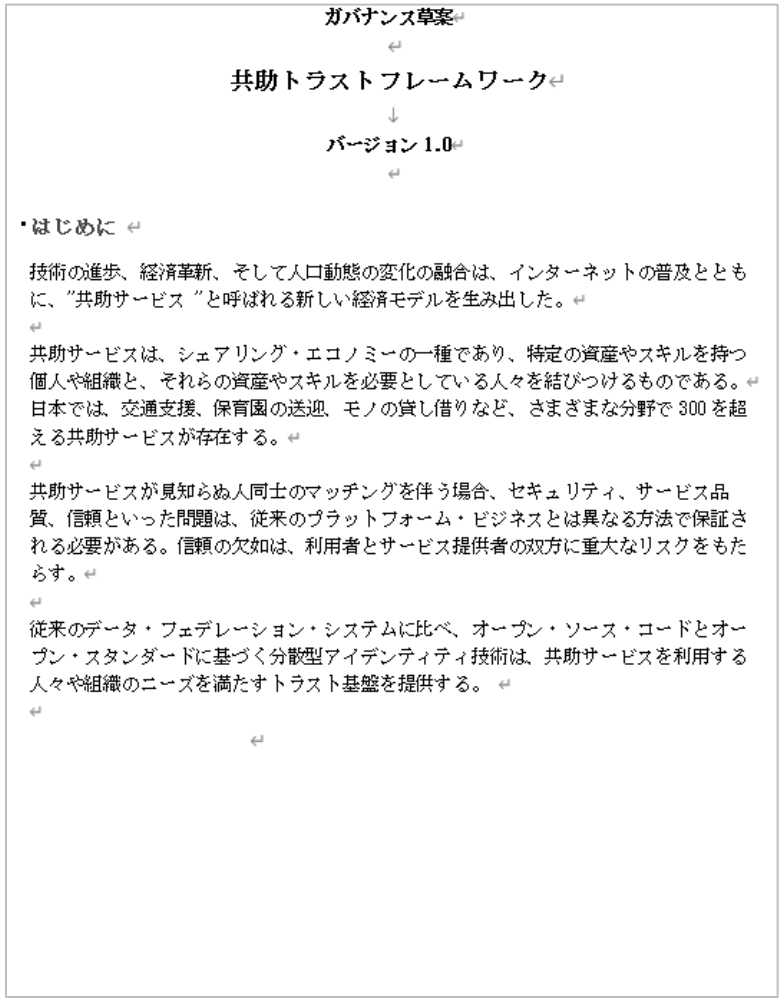
発行者（共助アプリベンダー）
- クレデンシャル発行者の認証プロセス
  -トラストマークの発行
- 発行者の追加／削除の頻度
- 鍵管理について
- 問題への対処方法

検証者（共助アプリベンダー・他）
- 検証者の認定（必要かどうか議論）
- 検証者の追加/削除の頻度
- 鍵管理について
- 問題への対処方法

ネットワーク
- 法的要件
- DIDメソッドについて
- キーローテーションについて
- 既存のネットワーク or 新規のネットワーク

5.1. 実施概要
5.1.3. 検証結果：ガバナンス整理

Confidential DNP



ガバナンス草案

共助トラストフレームワーク

バージョン 1.0

・はじめに

技術の進歩、経済革新、そして人口動態の変化の融合は、インターネットの普及とともに、"共助サービス "と呼ばれる新しい経済モデルを生み出した。

共助サービスは、シェアリング・エコノミーの一種であり、特定の資産やスキルを持つ個人や組織と、それらの資産やスキルを必要としている人々を結びつけるものである。日本では、交通支援、保育園の送迎、モノの貸し借りなど、さまざまな分野で 300 を超える共助サービスが存在する。

共助サービスが見知らぬ人同士のマッチングを伴う場合、セキュリティ、サービス品質、信頼といった問題は、従来のプラットフォーム・ビジネスとは異なる方法で保証される必要がある。信頼の欠如は、利用者とサービス提供者の双方に重大なリスクをもたらす。

従来のデータ・フェデレーション・システムに比べ、オープン・ソース・コードとオープン・スタンダードに基づく分散型アイデンティティ技術は、共助サービスを利用する人々や組織のニーズを満たすトラスト基盤を提供する。

用語定義
目的
用語解説
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
7. 暗号技術の活用方針
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に関するポリシー
13. 証明書の検証に関する方針
14. ガバナンスの実行に関するポリシー
15. ガバナンス文書の管理方針
16. 改定に関する方針

変更履歴

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。他のエコシステムでも参考にできるように可能な限りシンプルで再現性の高い設計を目指した。

ポイント②Issuer/Verifierの要件を設定

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ーの権限についても議論。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いれた運営方針を取りまとめた。

悪意のある第三者を想定して、共助実績のデータに含めるべき項目について共助ベンダーと合意した。

共助実績証明書
基本となるスキーマ

- ID
- Issued Date
- Expiration Date
- Issuer / service operator
- Service Category
- Service Signup Date
- Description
- Support Task Completions
- Total Support Hours
- User Binding Attributes
  - -Name
  - -MyNumberCard ID
  - -Financial Institution ID

ディスカッションとなったポイント

■ 検証者は何を重視するか？
- ➢ 検証者にとって、証明書の発行日が新しいことはトラストを検証する上で重要である。スキーマの中にも証明書の発行日を明示し、新しい証明書かどうかが分かりやすいようにする。

■ 証明書の無効化について
- ➢ 発行者が任意のタイミングで無効化？使用期限を設ける？
- ➢ 前者は実装が複雑になるため、使用期限を設ける仕様に決定。
- ➢ 日数については、ユースケースごとに策定（議論を継続）

■ 悪意のあるユーザーの対策
- ➢ 低評価がついた場合に、別アカウントを作成して新たに実績を作ろうとする人への対策をどうするか？
- ➢ アカウントの作成日を入れて、経験の浅いユーザーには簡単に証明書を発行しないようにする。（発行に必要な最低継続日数を設定）

■ 本人とクレデンシャルの紐付け（※今後実装の方法については要検討）
- ➢ ①本人情報と共助実績の紐付け or ②別のVCと共助実績を紐付け
- ➢ ①についてはマイナンバーカードを使って紐付け
- ➢ 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

5.1. 実施概要
5.1.3. 検証結果：ガバナンス整理

ガバナンスの基本方針となるValue（価値観）とPrinciple（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。

■ Value（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一つである。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。

■ Principles（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、データの共有はユーザーの同意が必要であり、ステークホルダー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。

5.1. 実施概要
5.1.3. 検証結果：ガバナンス整理

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。

	テーマ	論点	方向性	現時点の結論
1	ガバナンス運営組織の形態	• 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？	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。	• 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。
2	参加者数の想定	• どのくらいの共助アプリベンダーがえこしすてむに参加する想定か？	• 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。	• 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。
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	• 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？	① 初期の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。	• 方向性①を選択。ガバナンスについてはステークホルダー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。

5.1. 実施概要
5.1.3. 検証結果：ガバナンス整理

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中。
ISOの規格化に携わった有識者であるシェアリングエコノミー協会委員からのアドバイスも頂く予定。

■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 」
信頼性と安全性を確保するため、プラットフォーマー（シェア事業者）が遵守すべき事項が記載されている。

- 一般的な要求事項
  -完全性、透明性、説明責任
- 取引における要求事項
  -情報提供、決済、評価・レビュー
- 管理業務における要求事項
  -本人確認、利用規約、苦情処理・紛争処理、情報セキュリティ

	テーマ	論点	方向性	現時点の結論
1	Issuerの認定	• 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？	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。	• 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。
2	Issuer/Verifierの資格停止	• Issuer/Verifierの資格を停止するステップはどうするか？	• 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。	• 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出来ているか、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。

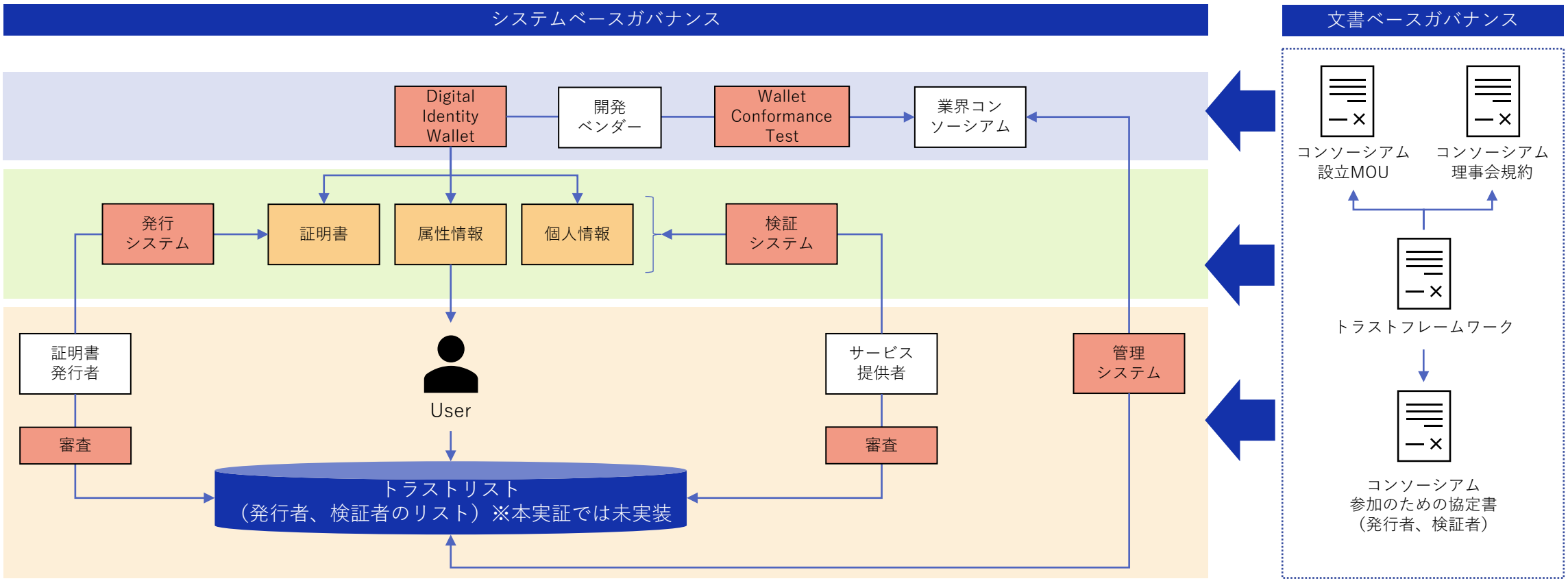
5.1. 実施概要
5.1.3. 検証結果：ガバナンス整理

ユーザーのプライバシー保護の観点からVerifierに対する制限事項についてディスカッション。
Verifierによる共助実績の二次利用はできないようなガバナンスルールにしていくことを想定。

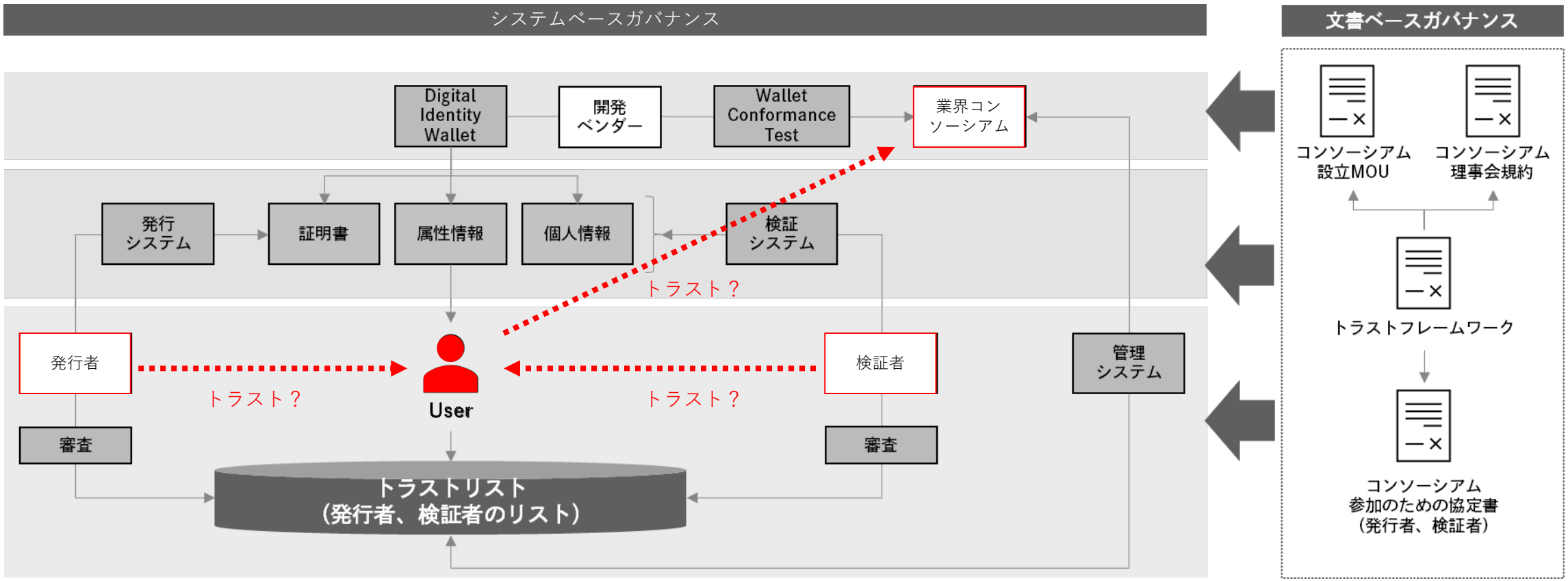
	テーマ	論点	方向性	現時点の結論
3	Verifierの制限事項	• Verifierによる共助実績の使い方で何か制限事項が存在するか？	① Verifierはユーザーから受け取ったVCを限られた文脈のためだけに利用することを想定しており、VCを蓄積したり流用したりすることはできないようにルールに定める。 ② 情報利用の期限等を設定し、その範囲内であればVerifierがパートナーと共助実績を共有することができる。（ユーザー同意は必須）	• 方向性①を選択。ユーザーのプライバシー保護の観点から、Verifierがユーザーの情報の流用や蓄積はできないようにする。
4	共助エコシステム内におけるユーザー同意について	• 共助実績をVerifierに渡す際にどこまで同意が必要か？	① Verifierへ連携する際に、ユーザーが共助実績のデータを１つ１つ細かく確認して同意する必要がある。 ② エコシステムの概要説明をして、共助walletを利用開始するにデータ活用に関する全体的な同意を得る。（共助エコシステムへのユーザーの参加を同意とみなす）	• 方向性②を選択。現状のユースケースは共助実績の複雑な利用を想定しておらず、Verifierに連携される情報も限られるので、共助Walletの利用開始時に簡単な同意画面を用意する。 • 将来的に新たなユースケースが追加された時に、さらに細かなユーザー同意が必要になる可能性はある。
5	共助エコシステム外のVerifierへの共助実績の共有について	• 共助エコシステム外のVerifierに証明書を渡し際に、新たにユーザーの同意を得る必要はあるか？	• 飲料メーカー等の共助エコシステム外の企業が共助実績を活用してサービスを提供する場合、Verifierに共助実績を渡す際に別途ユーザー同意が必要になる。	• 共助アプリエコシステム外の企業に共助実績を共有する場合は、別途ユーザー同意を得ることにする。 • 共助アプリ以外の企業でも共助実績を活用したユースケースが増えていくことで、ユーザーへのインセンティブも高まっていくため、共助エコシステム外の企業への連携方法についての標準化を進める。

5.1. 実施概要
5.1.4. 検証結果：ガバナンス整理（論点整理）

ガバナンスルールを記載した文書をもとに、システムベースのガバナンスへの落とし込みが重要。
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。



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。



5.1. 実施概要
5.1.6. 成果：DNPによるSessionの主催 “Should governments be involved in VC systems?”

Trusted Webユースケース実証でも重要な論点になっているガバナンスにテーマを絞ってセッション準備を行った。

Should governments be involved in VC system? (DNP from Japan)

■Purpose
To make it clear what governments should do in Verifiable Credentials ecosystems.

■Goal
List up common things governments should do accelerate governments’ rule making.
For that, I’d like government officials and trust framework professionals to participate.

■Timetable
1.Intro 5min
2.Brainstorm what governments(Green) or Privates(Yellow) should do to minimize risks 10min
3.Group things above 10min
4.List up Current governments roles in each countries against above things 15min
5.Make lists of common things governments should do based on matrix 10min

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

■事前準備
Trusted Web推進協議会の委員(松尾氏、佐古氏、崎村氏、安田氏等)との事前ディスカッションを実施して内容を検討。

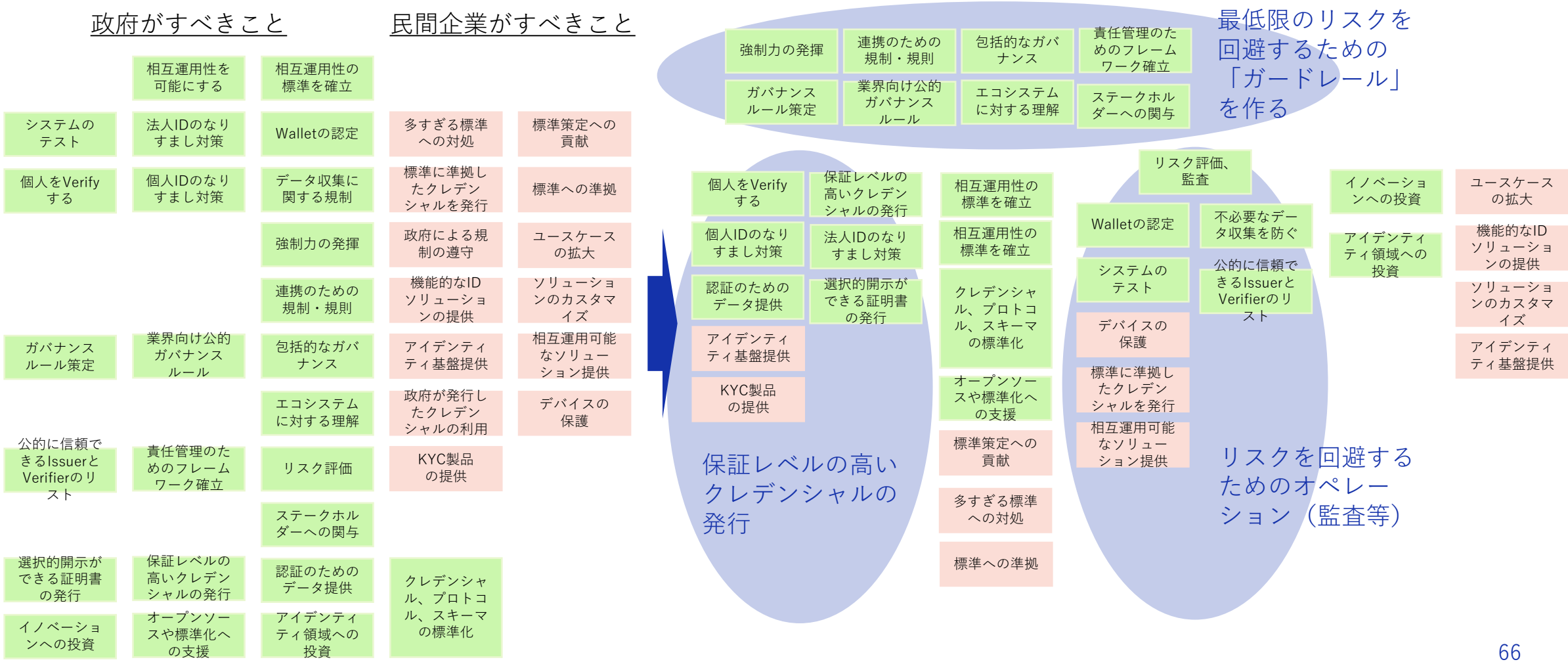
業界のホットトピックであるガバナンスのテーマを設定し、参加者を集った上で1時間のセッションを執り行った。

■セッションの目的
政府がVerifiable Credentials Ecosystemで果たすべき役割を明確にするため、政府及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する。

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

5.1. 実施概要

5.1.6. **成果：DNPによるSessionの主催 “Should governments be involved in VC systems?”**



5.1.7.　**成果：**OIXとの面談結果

Confidential　DNP

Open Identity Exchange　：Nick Mothershow氏との打ち合わせを実施

政府の役割について

- 政府はルールメイキングをして、その実行は民間企業に任せなければスピードが出ない。
- 保証レベルの高いクレデンシャルの定義は政府がドキュメントで定めるが、その発行は政府に認定された民間事業者がやるべき。イギリスにおいては40の認定された事業者が、保証レベルの高いクレデンシャルの発行を行なっている。
- 政府が直接的に発行者になるわけではなく、政府の定めたルールに従ってトラストアンカーを認定する。
- 国際標準に従ったグローバルスタンダード（ISO、W3C、ICAO等）のクレデンシャル定義を政府が定めることが重要。　　国がこの部分を決めないと、技術とポリシーのギャップが広がってしまい、責任分解点におけるグレーゾーンが生まれてしまう。
- コアのクレデンシャル（ゴールデンクレデンシャル）については、政府が技術仕様をどこに準拠するか決めるべき。
  ※ゴールデンクレデンシャルにはナショナルIDカード、パスポート、銀行アカウント、運転免許証、電話アカウントが含まれる。

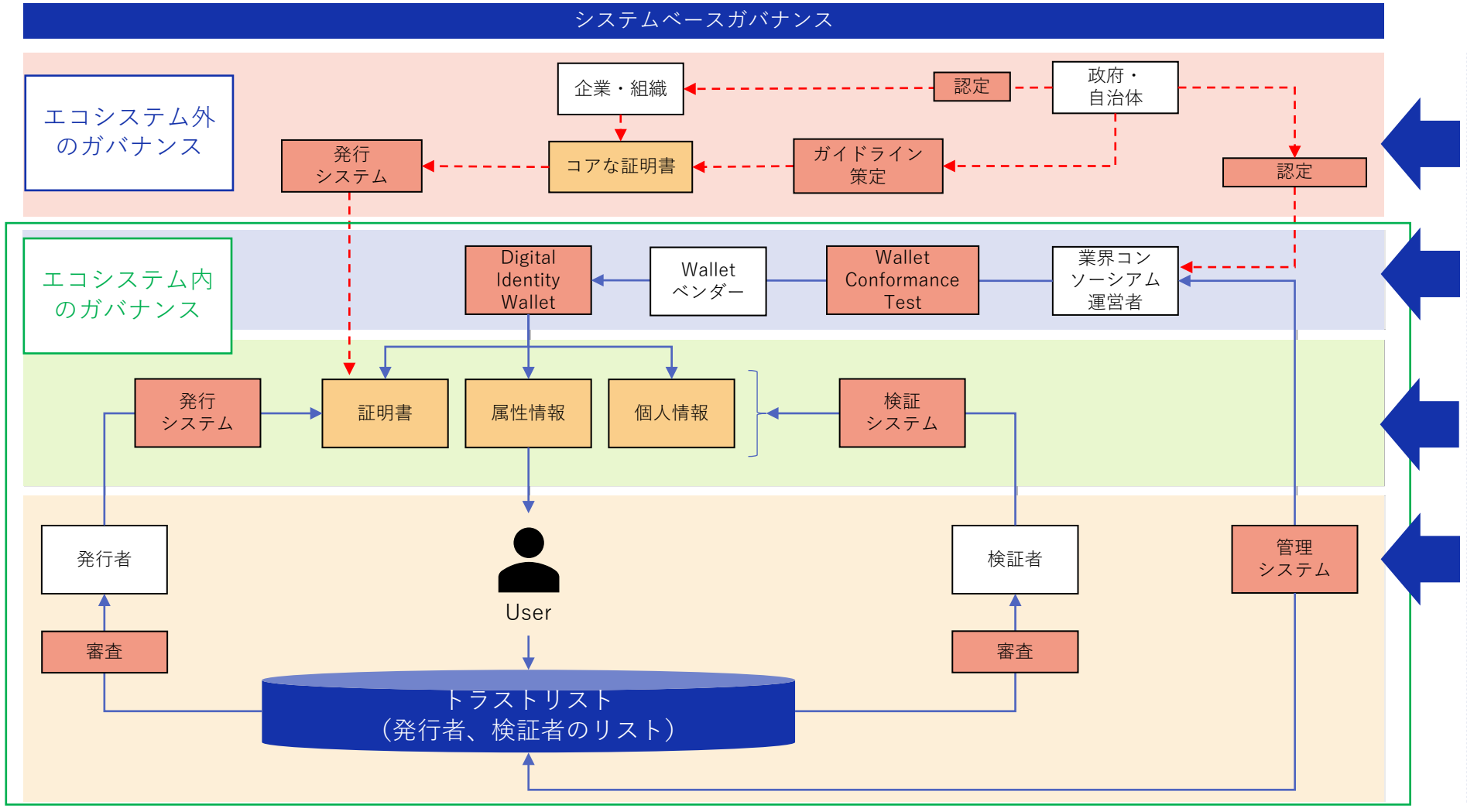
トラストフレームワークに含める項目について

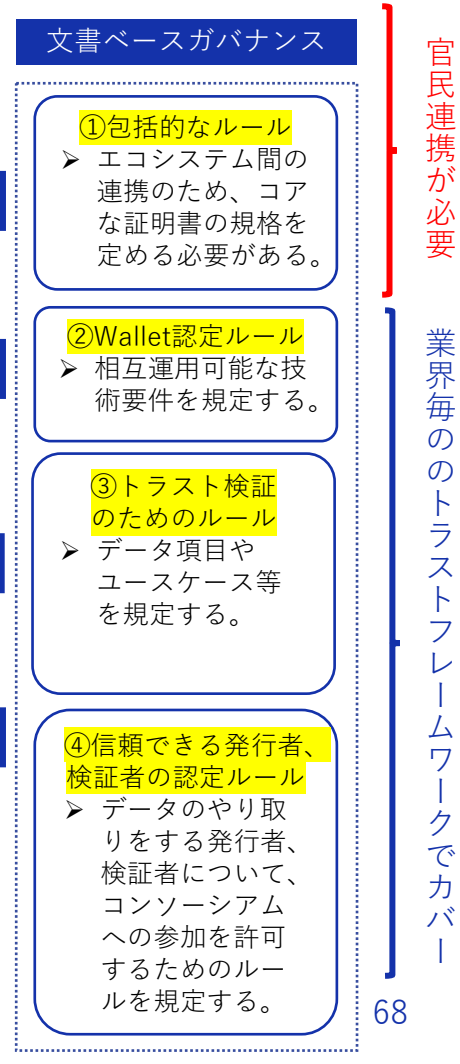
- OIXはトラストフレームワーク間の相互運用性を高めることに注力している。
- General rulesはできるだけシンプルに項目を埋めていくことが重要。エコシステム内のガバナンス形成はこれでカバーできる。
- 他のエコシステムとの相互運用性で重要になるのが、Identity Assuarance Policy（LoA）の話。
- LoAとはどの程度の保証レベルのクレデンシャルかを定めることであり、General Policy rulesより階層が深く、複雑になる。
- OIXではLoAを相互運用可能にするためのツール開発を進めている。EUとUSでもLoAの相互運用性を議論し始めている。

5.1. 実施概要

5.1.8. **成果：**ガバナンス全体像の設計（更新版）

エコシステム外の政府がガイドライン策定等を通じて、エコシステム内のガバナンスのリスクを最小限に抑えることが重要。

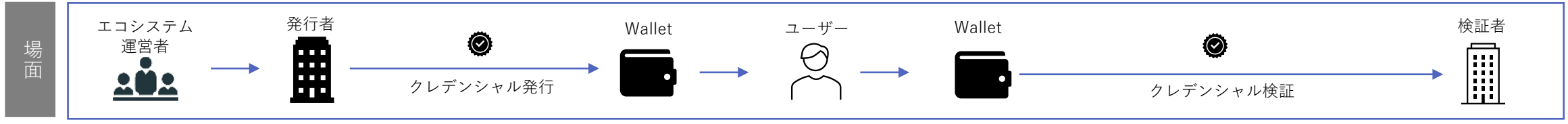




5.1.9. **成果：**エコシステム内のトラスト問題における責任分界点の整理（ドラフト版）

DNP

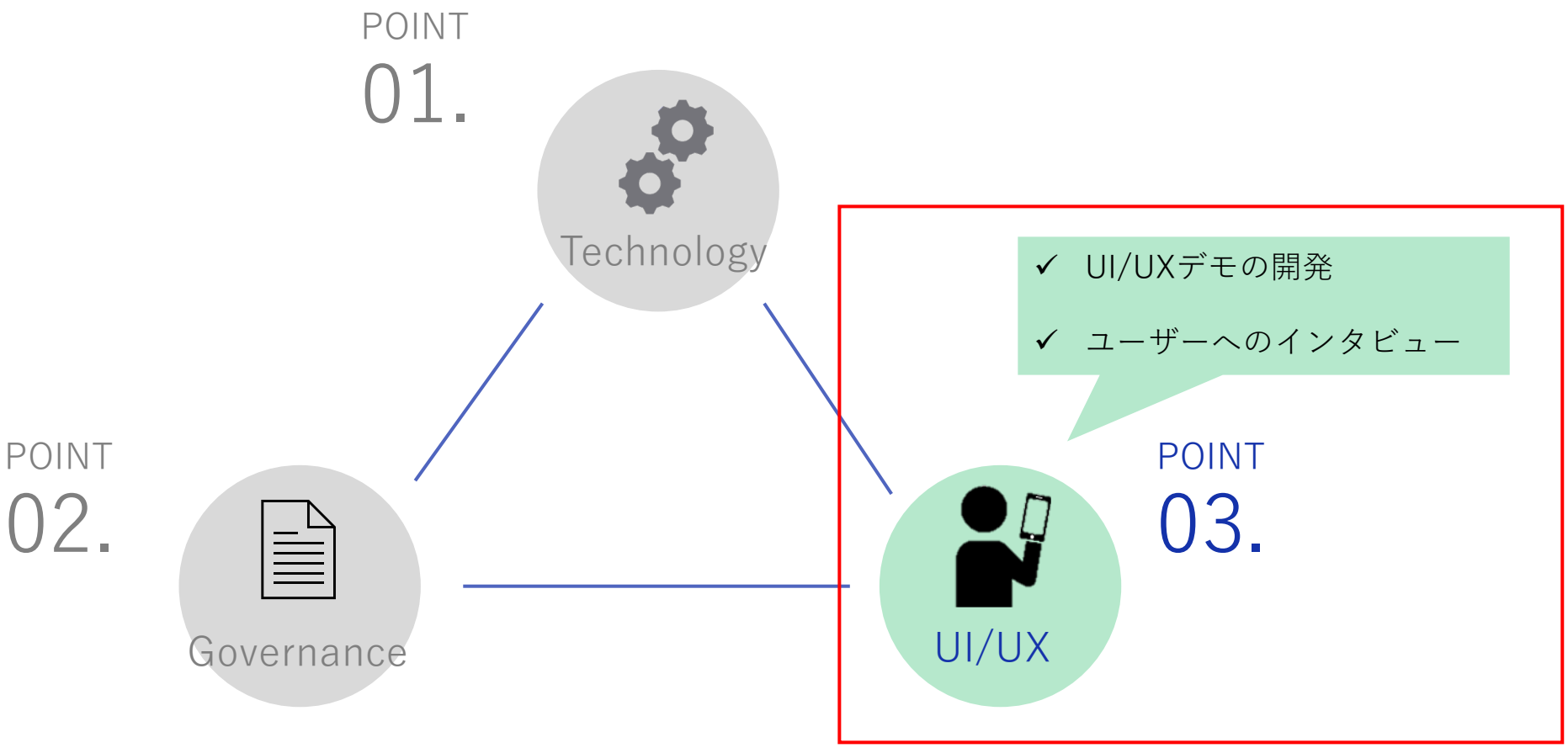
証明書の発行～保持～検証の一連の流れにおけるトラストの責任分界点について整理。
コンソーシアム運営者に高度な技術的知見とトラストチェーン全体の設計が求められる。
今後さらに責任主体毎に責任事項・免責事項・責務（道義的、善管注意義務的なもの）等に分解していく。



トラストの問題	そのエコシステムは信頼できるか？	発行者を信頼できるか？	このクレデンシャルはどのようなタイプか？保証レベルを満たしているか？	Walletは安全か？	ユーザーが本物であることをどうやって確認するか？	どのようにクレデンシャルが管理されているか？	誰が発行したのか？誰がクレデンシャルを提示したのか？	Walletと安全に通信することができるか？	このクレデンシャルを受け取るとどのような義務が課せられるか？
主体責任	政府、コンソ運営者	コンソ運営者、発行者	コンソ運営者、発行者	コンソ運営者、Walletベンダー	Walletベンダー、ユーザー	コンソ運営者、Walletベンダー	コンソ運営者、Walletベンダー	コンソ運営者、標準規格作成者	コンソ運営者、検証者
ガバナンス 政府	政府による運営者の認定	個人情報保護法		参照可能なアーキテクチャの策定		セキュリティガイドラインの策定			個人情報保護法
ガバナンス 業界ルール	運営規則の公開	運営者による発行者の認定	運営者による証明書の規格策定	運営者による技術仕様の選定	Walletベンダーによる認証基準の設定	運営者による技術仕様の策定	運営者によるトラストチェーンの設計	標準規格の策定（標準化団体）	トラストリストの開示
		トラストリストの開示	発行者がトラストフレームワーク準拠の証明書を発行	Walletの相互運用性テスト		Walletの相互運用性テスト		運営者による技術仕様の選択	
ガバナンス 契約				ユーザーの同意	ユーザーによるエビデンス提示		ユーザーの同意		
技術		トラストレジストリ	クレデンシャルフォーマット	セキュアストレージ	認証技術	Walletエージェント Cloud Wallet	電子署名技術 ホルダーバインディング	通信プロトコル	トラストレジストリ

6. 調査（UI/UXの検討）

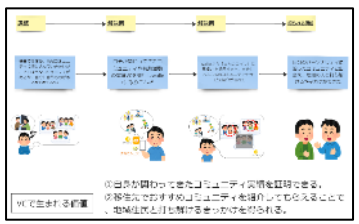
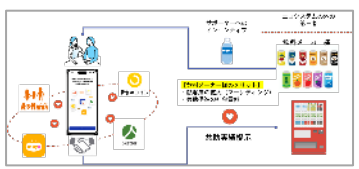
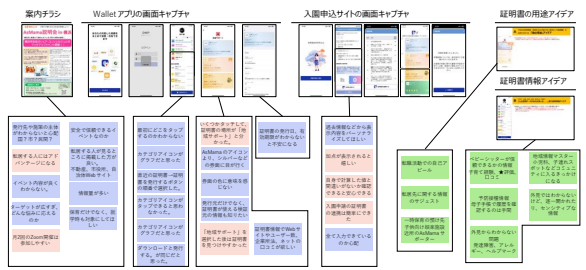
6.1.実施概要


POINT
01.
Technology
POINT
02.
Governance
UI/UX
POINT
03.
✓ UI/UXデモの開発
✓ ユーザーへのインタビュー

6.1. 実施概要

6.1.1. 事業実現に向けたUI/UXおける論点とその結果

共助実績を活用してトラスト範囲が向上する顧客体験ユースケースを検討。ユーザーヒアリングを通じ、体験価値を確認した。

	ユースケース検討	UI/UXモックアップ開発	ユーザーインタビュー
論点	➢ 共助実績の活用について、ステークホルダーが価値を感じるユースケースを作ることができるか。	➢ 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の調査	➢ 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の調査
実施概要	まちのコイン  A-SMama  Asahi アサヒ飲料 		  
結果	✓ カヤック様、Asmama様、アサヒ飲料様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。	✓ 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。 ✓ 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。	✓ 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。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。

「共助アプリの“信頼”を共有できる」分散型IDを活用した共助トラストエコシステム

ー分散型IDを活用した「共助トラストエコシステム」について教えてください。

中川：共助トラストエコシステムは、異なる共助アプリ間で実績を連携させ、ユーザーの信頼を向上させる仕組みです。DNPは信頼できるデータを流通させる分散型IDの基盤システムを制作しています。アプリやサービスを跨いで、利用実績などのユーザーの信頼を連携できる基盤システムです。

以前からDNPでは共助アプリの一つである「May ii」の活動を通じ、ユーザーのデジタル上の活動において信頼情報が重要であることを意識していました。特に、生活者同士の共助やシェアリングサービスのマッチングをする際の信頼が、これからの社会で重要な役割になると感じ、共助アプリにおける分散型IDの活用に着目しました。

ー今回のカヤックとの共創の経緯を教えてください。

中川：現在、共助トラストエコシステムの取組みにご賛同いただける共助アプリ事業者を探しています。カヤックが運営する「まちのコイン」は、May iiと同じく地域における共助を目指していることから、はじめにお声がけさせていただきました。

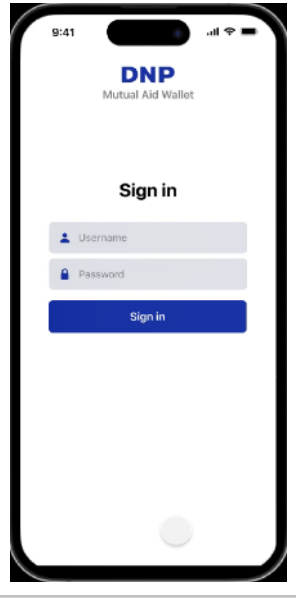
May iiも含め、多くの共助アプリは無償のサポーターで成り立つサービスです。しかし、現状は無償のサポーターが参加するメリットやインセンティブを十分には提供できていません。サポート実績の証明書を発行することがサポーターのメリットになり、共助サービスのビジネスモデルへの一助になるのではないかと議論をしています。

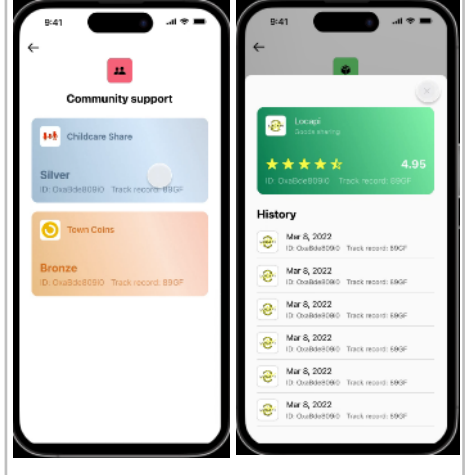
https://www.dnp-innovationport.com/news/3334/

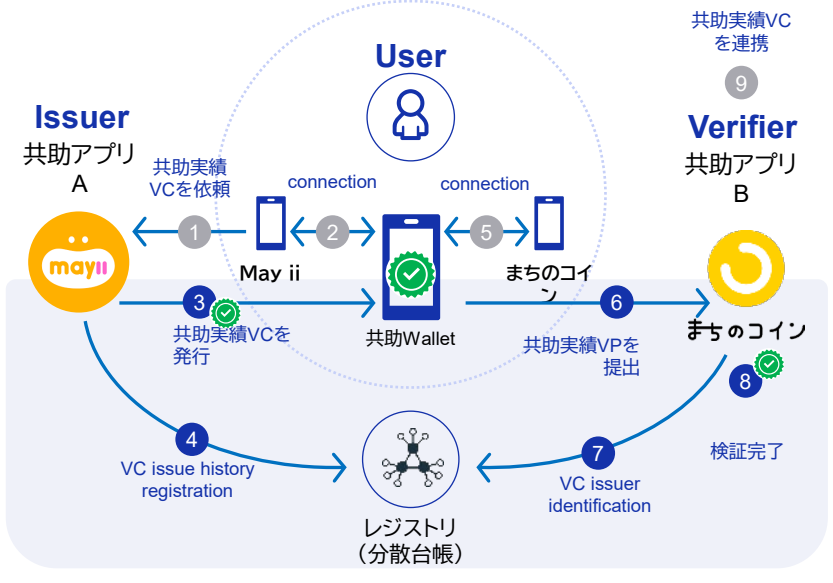
6.1. 実施概要
6.1.1.2. 共助アプリWalletのユーザー体験

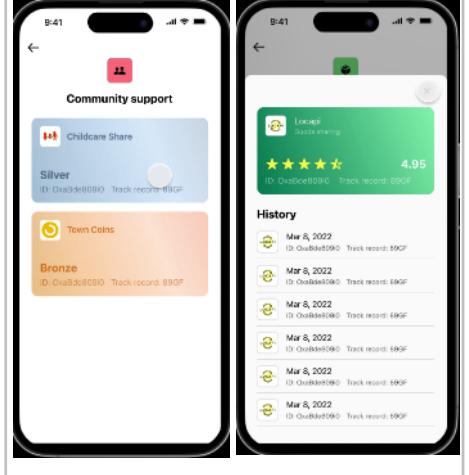
生活者の体験に繋がるUI/UXについて、各共助アプリベンダーと検討。
生活者が本実証のメリットを体感できるユースケースとなることを重視。

プロトタイプシステム開発するシーンのイメージ				UI/UXモックアップ
シーン0	シーン1	シーン2	シーン3	シーン4
Walletアプリをインストールした際、端末の持ち主とWalletアプリの所有者を紐づける	Walletで証明書一覧を確認する	共助アプリから共助実績VCを発行し、Walletに保存する	共助アプリへWalletから共助実績VPを連携して、VPを検証する	共助実績を検証することによるユーザーメリット・顧客体験









6.1. 実施概要

6.1.1.3. 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

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。
SNSアプリ上におけるユーザー同士の信頼性担保の一助として活用する。

SNSアプリ画面　プロフィールの確認　デジタル証明書を連携　プロフィールに追加　証明書の詳細確認

6.1. 実施概要

6.1.1.4. ユースケース②飲料メーカーへの共助実績の連携

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。
飲料メーカーだけでなく、様々な企業が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。

キャンペーンサイトにアクセス

キャンペーンの確認

デジタル証明書を連携

クーポンの取得

6.1. 実施概要

6.1.1.5. 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

子育てシェアアプリの利用証明をオンラインで連携し、保育園申込の調整指数への加点に活用。
自治体における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。

オンライン申し込み画面

調整指数の加算点数を確認

調整指数の条件を確認

デジタル証明書を連携

調整指数が加点

共助Wallet

グループチャット

飲料メーカー

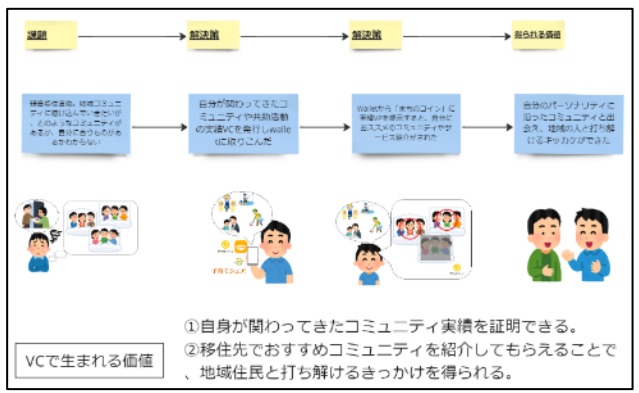
保育園申請

現在、下記3つのユースケースの検証課題についてユーザーインタビュー、アンケートを実施。

①信頼できるプロフィール

■内容
まちのコインの活動実績を、グループチャットのプロフィール情報に連携。

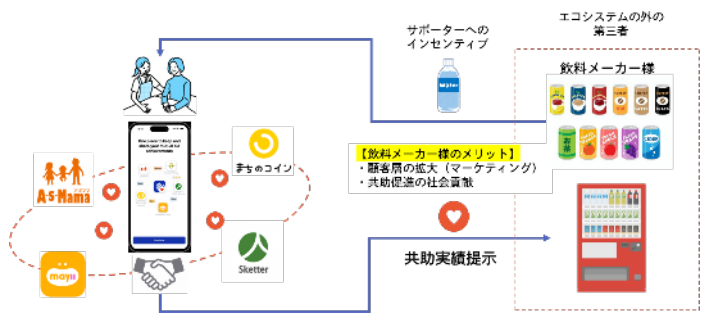
■検証する課題
見知らぬ他人が多いグループチャット内で第三者によるお墨付き実績を連携することで、ユーザー同士のトラスト範囲は拡大するか？



②飲料メーカー連携

■内容
May iiアプリの利用証明を、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。

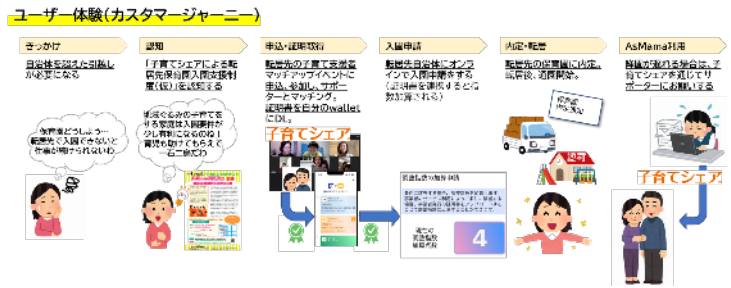
■検証する課題
共助実績をエコシステム外の第三者に連携することで、新たなユーザーインセンティブを作ることができないか？



③子育てシェア実績連携

■内容
子育てシェアアプリの利用証明を、保育園申込の調整指数への加点に活用。

■検証する課題
これまで証明することのできなかった実績（トラスト）が可視化され、オンライン上で第三者に連携可能になることでユーザーの体験を向上させることができるか？



①受容性の把握

・想定しているターゲットペルソナにとって、提供するサービス体験／技術の受容可能性を把握する
・本体験を享受するために支払うことができるコストについて把握する
※ユーザーの支払いコストが無い想定の体験については、感情的な価値を収集する

No	カテゴリ	観点	検証ステップ
1	**ユーザーの欲求**	ユーザーの不満、インサイトが正しいか	コンセプト検証
2	**体験の受容性**	本サービス体験を通じた「提供価値」が理解できるか	コンセプト検証
3		想定ペルソナの抱える「不満」が解決できるか	コンセプト検証
4		想定ペルソナにとっての体験価値の程度とその理由	コンセプト検証
5		ターゲットユーザーにとっての体験価値の程度とその理由	コンセプト検証
6	**技術的受容性（アイデンティティWallet）**	自分の技能・特性・経験などが、改ざん不能なデータ形式で「アイデンティティ」として発行され、自身のスマートフォンで保持・管理するという体験が理解できるか	UX検証
7		発行された「アイデンティティ」の活用機会についてイメージできるか	UX検証
8	**優位性**	不満を解決するための競合体験はないか（本手法でなければ解決できないことを把握するため	総評 or 事後アンケ

②UX課題の抽出

・提供したい体験を実現するための一連の繋がりを体験し、主要な導線への課題を明確にする
・自分が同シチュエーションに置かれた時に、本UXで体験を享受可能かどうかを把握する

No	シーン（CJM）	観点	検証ステップ
1	**きっかけ**	同状況に置かれた際に、まずどのような行動をとるか？	UX検証
2	**認知**	**案内チラシ（orバナー）を見ての反応は？**	UX検証
3		案内チラシ（orバナー）の提供場所として適切な場所はどこか？	UX検証
4	**申込・証明取得（イベントに参加したテイ）**	**ミッション①：発行された証明書を確認できるか？**	UX検証
5		証明書発行フローにおける障壁は？	UX検証
6		ペルソナの不安はどの程度軽減できるか？	UX検証
7	**入園申請**	**ミッション②：入園申請を独力で遂行できるか？**	UX検証
8	**内定・転居**	自治体横断での転居において、転園において不安に感じることは？	UX検証
9	**利用**	-（AsMama自体のサービス体験として評価外）	UX検証

6.1.　実施概要
6.1.2.　実施内容・手法：ビジネスフィージビリティ検証

1：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。

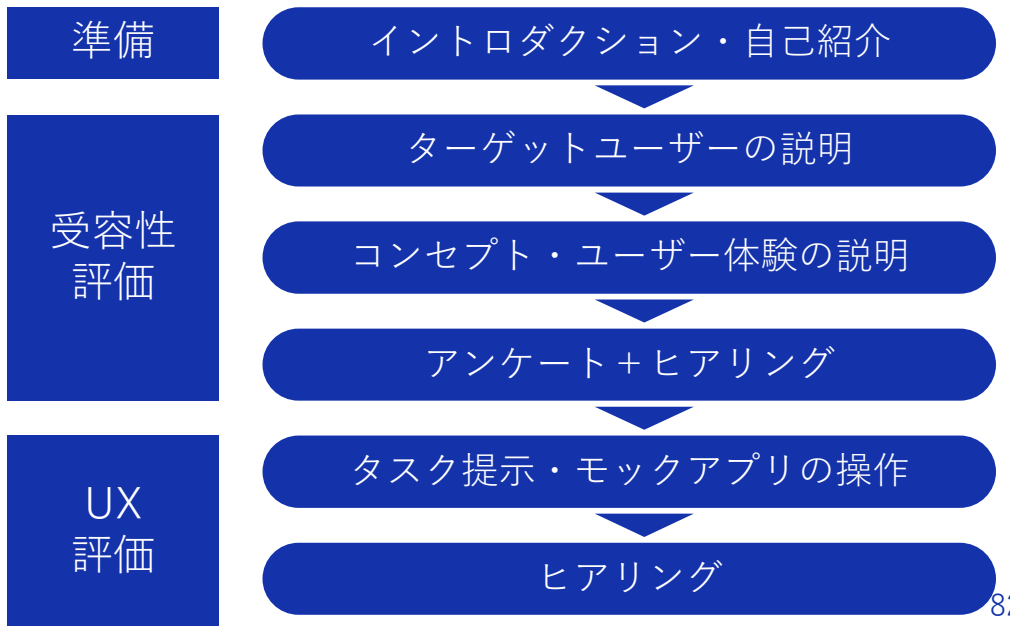
2：UX評価
ストーリーボードに沿った達成目標をユーザーに提示し、モックアップを操作して感じたことを評価する。

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

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 ・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 ・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 ・子育てシェアユーザ（頼る側）

内容：下記フローで実施



6.1. 実施概要
6.1.2. 実施内容・手法：ビジネスフィージビリティ検証


カメラによる録音、記録者席を用意


気づきを付箋に記載


デモアプリの体験


付箋に書いた気づきを関連する画面に貼付け


付箋記載内容の深堀


ヒアリング終了後、アイデア出しを実施

6.2. 調査検証結果

ポジ　ネガ　アイデア　Confidential　DNP

案内チラシ

- 発行先や施策の主体がわからないと心配　国？市？民間？
- 安全で信頼できるイベントなのか
- 転居する人にはアドバンテージになる
- 転居する人が見るところに掲載した方が良い。不動産、市役所、自治体Webサイト
- イベント内容が良くわからない。
- 情報量が多い
- ターゲットが広すぎ、どんな悩みに応えるのか
- 保育だけでなく、就学時も対象にしてほしい
- 月2回のZoom開催は参加しやすい

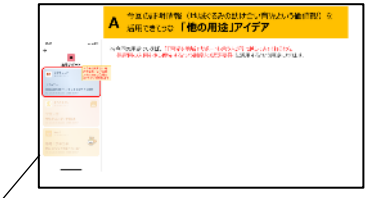
Walletアプリの画面キャプチャ

- 最初にどこをタップするのかわからない
- カテゴリアイコンがグラフだと思った
- 直近の証明書→証明書を発行するボタンの順番で選択した。
- カテゴリアイコンがタップできると思わなかった。
- カテゴリアイコンがグラフだと思った
- ダウンロードと発行する。が同じだと思った。
- いくつかタッチして、証明書の場所が「地域サポート」と分かった。
- AsMamaのアイコンより、シルバーなどの券面に目が行く
- 券面の色に意味を感じない
- 発行元だけでなく、証明書が使える検証元の情報も知りたい
- 「地域サポート」を選択した後は証明書を見つけやすかった
- 証明書の発行日、有効期限がわからないと不安になる
- 証明書情報でWebサイトやユーザー数、企業所法、ネットの口コミが欲しい

入園申込サイトの画面キャプチャ

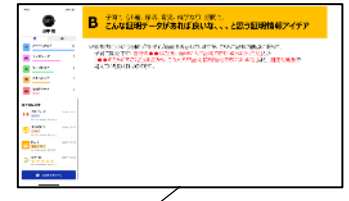
- 過去情報などから表示内容をパーソナライズしてほしい
- 加点が表示されると嬉しい
- 自身で計算した値と間違いがないか確認できると安心できる
- 入園申請時の証明書の連携は簡単にできた
- 全て入力できているのか心配

証明書の用途アイデア



- 転職活動での自己アピール
- 転居先に関する情報のサジェスト
- 一時保育の預け先
  子供向け娯楽施設
  近所のAsMamaサポーター

証明書情報アイデア



- ベビーシッターが信頼できるかの情報
  子育て経験、★評価、口コミ
- 地域情報マスター
  小児科、子連れスポットなどコミュニティに入るきっかけになる
- 予防接種情報
  母子手帳で履歴を確認するのは手間
- 外見ではわからないけど、逐一聞かれたり、センシティブな情報
- 外見からわからない問題
  発達障害、アレルギー、ヘルプマーク

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大きく、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。
- 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つながっている。

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わ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、発行元だけでなく、制度の主体など検証元も合わせて信頼できる必要がある。

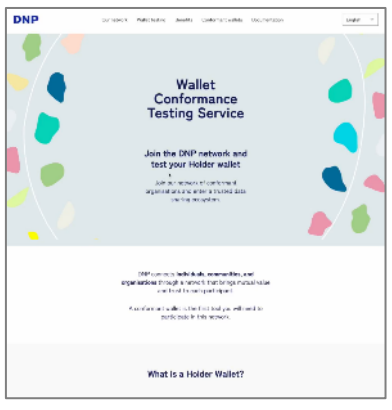
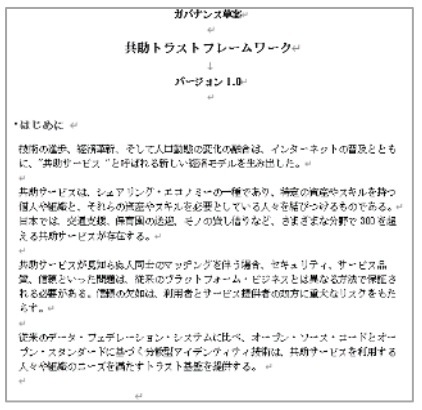
証明書情報のアイデア
- 子供の予防接種情情報が証明書化されれば、急に確認されたときに母子手帳を持っていなくても証明でき便利。

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. 本実証の成果

テクノロジー・ガバナンス・UI/UXの３領域を横断しながら検討を深め、社会実装を見据えた成果物への落とし込みを完了した。

テクノロジー　ガバナンス　UI/UX

プロトタイプ システム開発	国際間相互運用性 テスト	トラスト フレームワーク	UI/UXモックアップ	ユーザーヒアリング 調査
				
✓ 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	✓ 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	✓ 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	➢ UI/UXに関するユーザーヒアリングの結果レポート

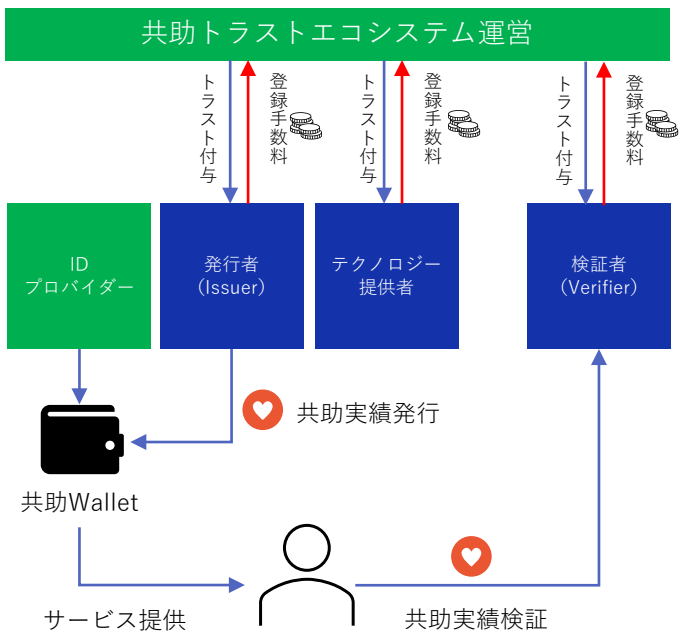
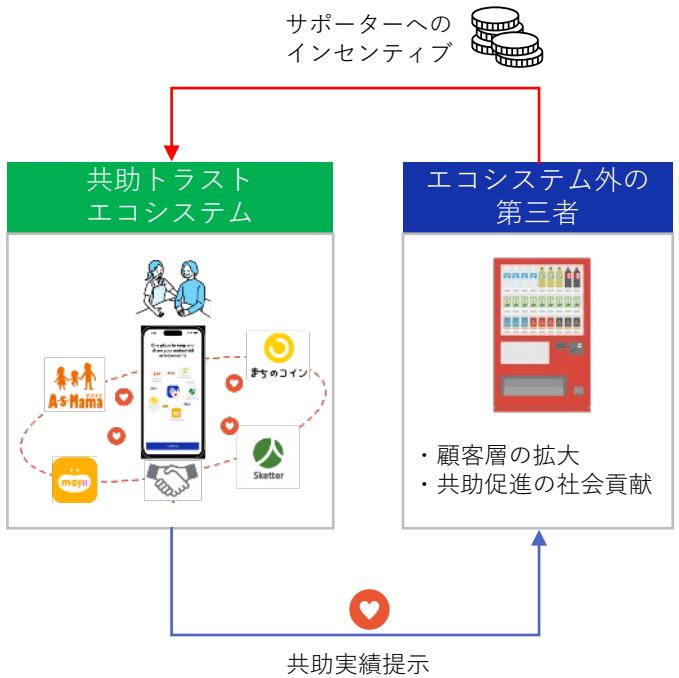
7.2. 残課題対応方針一覧

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ー間の合意と、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付け（※今後実装の方法については要検討） ➢ ①本人情報と共助実績の紐付け or ②別のVCと共助実績を紐付け ➢ ①についてはマイナンバーカードを使って紐付け ➢ 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。

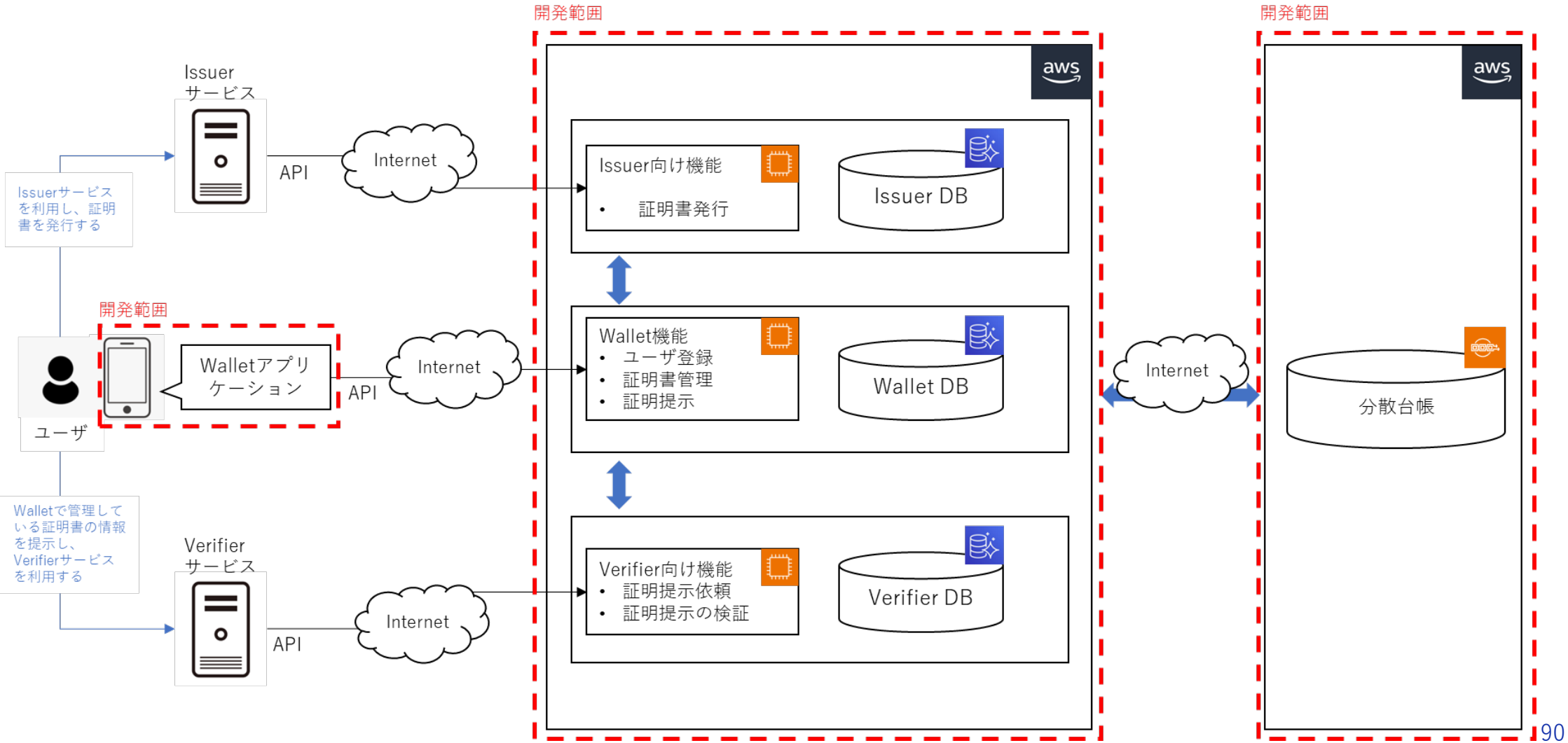
7.2. ユースケース実現案
7.2.1. ビジネスモデル案

Confidential DNP

共助実績を利活用するステークホルダーを拡大していくことで、マネタイズの機会を増やしていくことを想定。

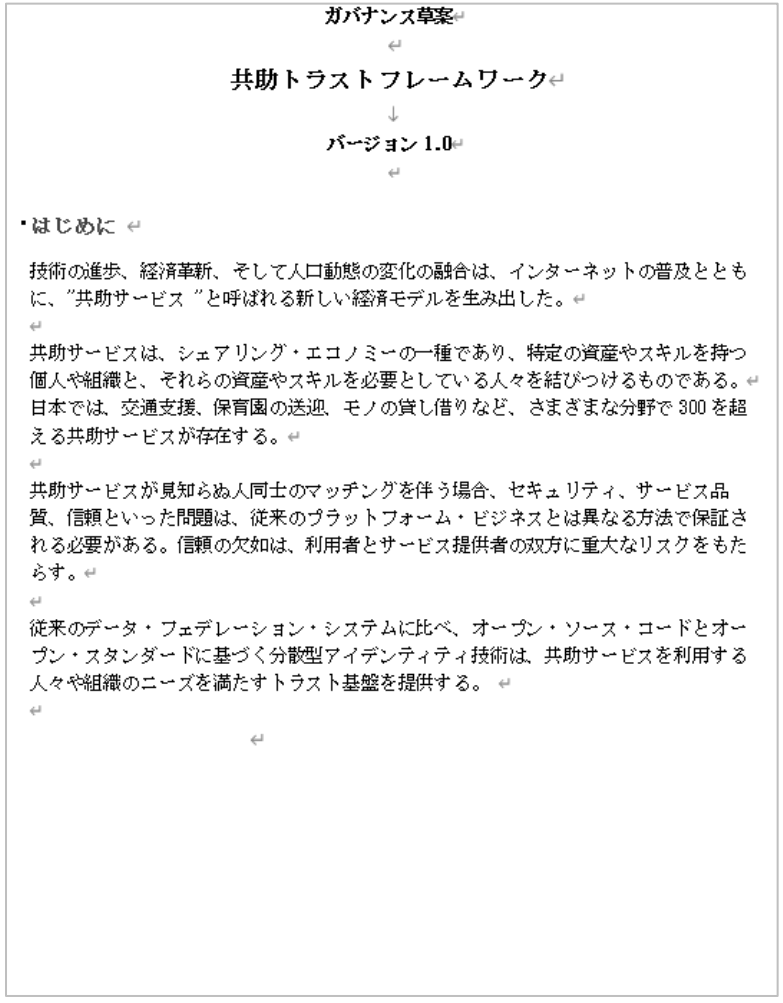
	共助アプリ間の連携	3rd Party企業との連携	国際間連携
概要	➢ 共助実績の発行、検証を行うためのエコシステムへの登録のために発行者、検証者、技術ベンダーは登録手数料をエコシステム運営者へ支払う。	➢ 共助実績をエコシステム外の3rd Party企業へ連携することで、共助アプリユーザーへ新たなインセンティブを付与し、利用を促進する機会を創出する。	➢ 今後更なる増加を見込むインバウンド顧客に対し、地域の共助アプリ利用をする際のトラスト形成手段として共助実績を活用。共助アプリの決済手段と連携する。
ビジネスモデル			

7.2. ユースケース実現案
7.2.2. アプリ・システム案



7.2. ユースケース実現案
7.2.3. ガバナンス・ルール案

Confidential DNP



ガバナンス草案

共助トラストフレームワーク

バージョン 1.0

・はじめに

技術の進歩、経済革新、そして人口動態の変化の融合は、インターネットの普及とともに、"共助サービス "と呼ばれる新しい経済モデルを生み出した。

共助サービスは、シェアリング・エコノミーの一種であり、特定の資産やスキルを持つ個人や組織と、それらの資産やスキルを必要としている人々を結びつけるものである。日本では、交通支援、保育園の送迎、モノの貸し借りなど、さまざまな分野で 300 を超える共助サービスが存在する。

共助サービスが見知らぬ人同士のマッチングを伴う場合、セキュリティ、サービス品質、信頼といった問題は、従来のプラットフォーム・ビジネスとは異なる方法で保証される必要がある。信頼の欠如は、利用者とサービス提供者の双方に重大なリスクをもたらす。

従来のデータ・フェデレーション・システムに比べ、オープン・ソース・コードとオープン・スタンダードに基づく分散型アイデンティティ技術は、共助サービスを利用する人々や組織のニーズを満たすトラスト基盤を提供する。

用語定義
目的
用語解説
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
7. 暗号技術の活用方針
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に関するポリシー
13. 証明書の検証に関する方針
14. ガバナンスの実行に関するポリシー
15. ガバナンス文書の管理方針
16. 改定に関する方針

変更履歴

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。他のエコシステムでも参考にできるように可能な限りシンプルで再現性の高い設計を目指した。

ポイント②Issuer/Verifierの要件を設定

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

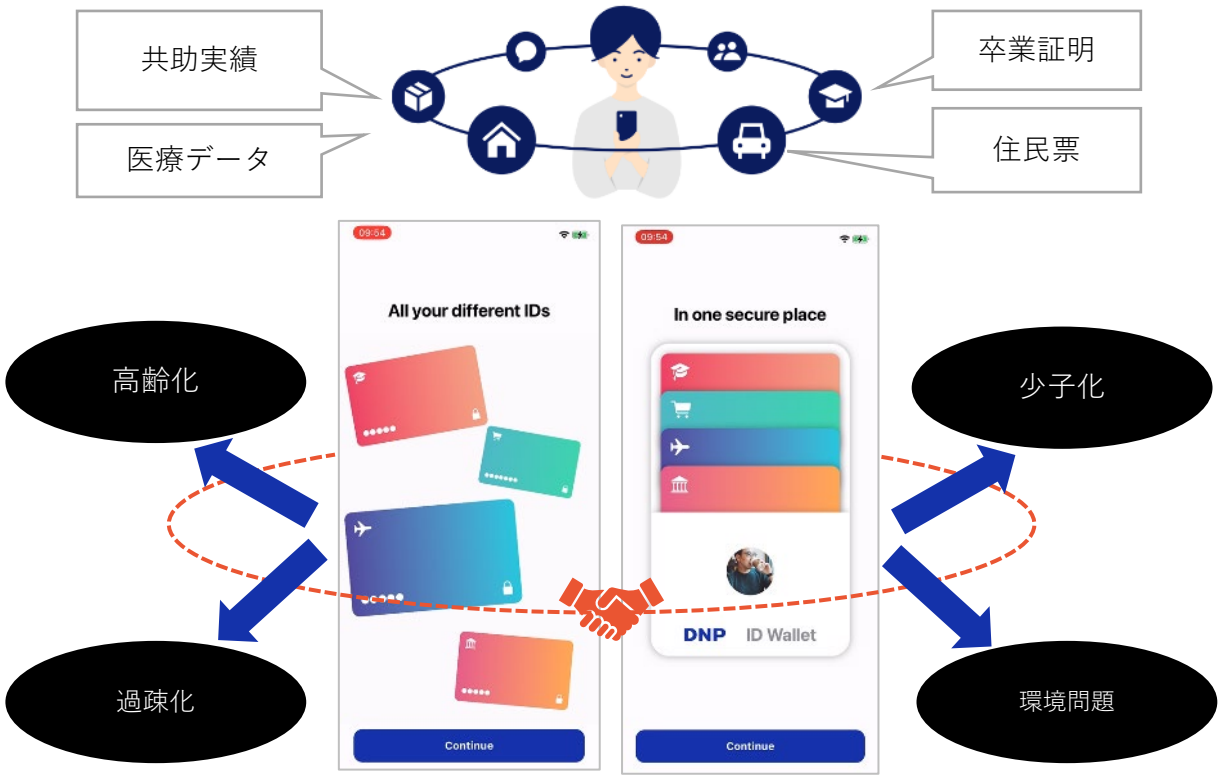
共助トラストフレームワークを社会実装して運用することを想定し、ガバナンスの運営組織の形態と各ステークホルダーの権限についても議論。初期のボードメンバーを運営の中心に据えつつ、今後のエコシステムへの参加者増加を視野にいれた運営方針を取りまとめた。

7.3　実現に向けてアクション・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。

SHARING ECONOMY ASSOCIATION JAPAN　A-S-Mama　まちのコイン　Sketter　mayu

2024	2025	2026	2027
PoC	商用化	エコシステムの拡大	
共助トラストフレームワークの構築			
UI/UX design	ユースケース拡大		
技術検証	相互運用性の確立		
	共助実績以外のデジタル証明書との連携		



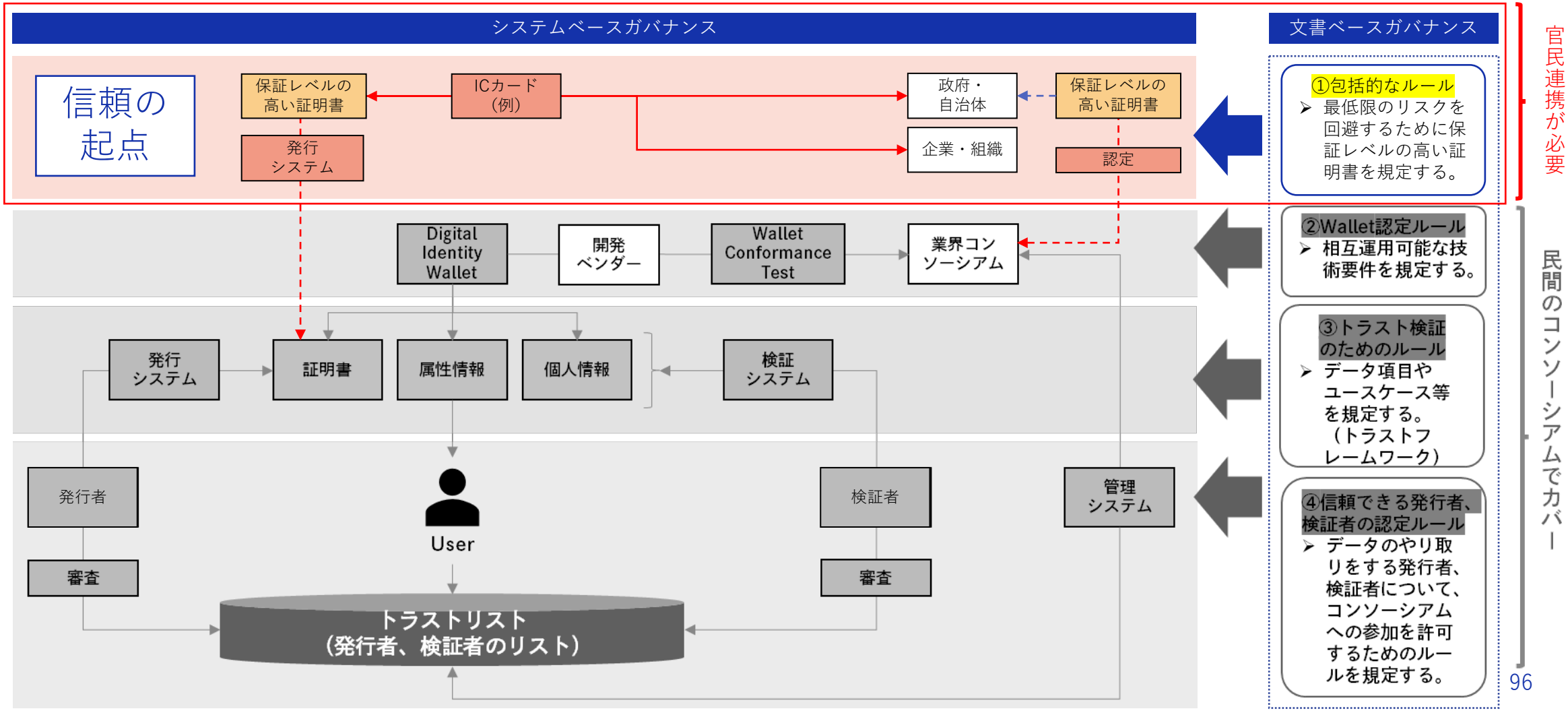
日本の地方自治体が抱える社会問題を解決

8. Trusted Webに関する考察

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 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。 ■原則10の更改容易性・拡張性について 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、 共助実績をステークホルダーを横断して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。 ■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。 ■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。 ■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）を参考にしながら各業界ごとに 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。 ■また参加するステークホルダー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。

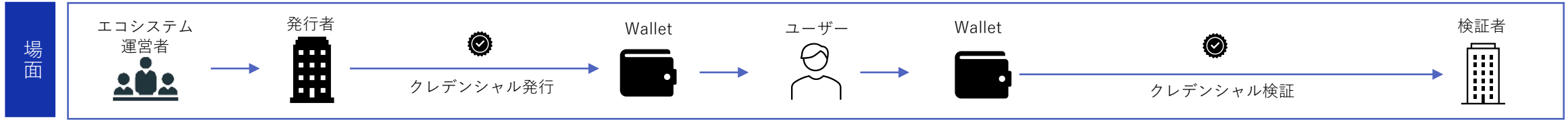
ガバナンスの実効性を担保するために有効な取組 （各業界や行政などへの働きかけ等）	■共助トラストフレームワークの立ち上げと賛同者を募るために、シェアリングエコノミー協会のネットワークを活用することを想定。既に運用されているコンソーシアムに協力いただきながら、トラストフレームワークを市場に浸透させるステップを踏むことで効率的にガバナンスの実効性を向上させることができる。 ■またトラストフレームワークそのものへの信頼性や、ユーザーのアイデンティティ保証レベルの確認のために、コンソーシアム外の第三者（政府や権威的な企業）がトラストアンカーになる必要がある。
トラストフレームワークを作成する上でプロセ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。 ■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。 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。 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。 ■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。

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発行を発行することで、信頼の起点を作る必要がある。



Confidential DNP

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。
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ことを想定。
（トラストの問題点についてはOIXのNick氏と議論して抽出）



トラストの問題	そのエコシステムは信頼できるか？	発行者を信頼できるか？	このクレデンシャルはどのようなタイプか？保証レベルを満たしているか？	Walletは安全か？	ユーザーが本物であることをどうやって確認するか？	どのようにクレデンシャルが管理されているか？	誰が発行したのか？誰がクレデンシャルを提示したのか？	Walletと安全に通信することができるか？	このクレデンシャルを受け取るとどのような義務が課せられるか？
主体責任	政府、コンソ運営者	コンソ運営者、発行者	コンソ運営者、発行者	コンソ運営者、Walletベンダー	Walletベンダー、ユーザー	コンソ運営者、Walletベンダー	コンソ運営者、Walletベンダー	コンソ運営者、標準規格作成者	コンソ運営者、検証者
ガバナンス	政府による運営者の認定 運営規則の公開	運営者による発行者の認定 発行者による情報開示 トラストリストの開示	運営者による証明書の規格策定 発行者がトラストフレームワークに準拠した証明書を発行	運営者による技術仕様の選定 Walletの相互運用性テスト セキュリティ基準の策定	Walletベンダーによる認証基準の設定 ユーザーによるエビデンス提示	運営者による技術仕様の策定 Walletの相互運用性テスト セキュリティ基準の策定	運営者によるトラストチェーンの設計	運営者による技術仕様の選択 標準規格の策定	トラストリストの開示
技術		トラストレジストリ	クレデンシャルフォーマット	セキュアストレージ	認証技術	Walletエージェント Cloud Wallet	電子署名技術 ホルダーバインディング	通信プロトコル	トラストレジストリ

8. Trusted Web に関する考察
8.3. 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。

8. Trusted Web に関する考察
8.3. その他 Trusted Web に関する課題と提言

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、政府へ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検討いただきたい。

未来のあたりまえをつくる。

DNP