

# Trusted Web の実現に向けたユースケース実証事業 成果報告書

[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]

2023年03月20日（提出日）

代表機関：[大日本印刷株式会社]

[共助アプリトラストコンソーシアム]



# 目次

1	背景と目的	4
1.1	事業の背景	4
1.2	事業の目的	5
2	事業の概要	6
2.1	事業概要及び実証の範囲	6
2.2	社会・経済に与える価値・影響	6
2.3	コンソーシアムの体制	8
2.4	実証全体のスケジュール	9
3	実証内容	10
3.1	実証の実施事項、論点及び判断	10
3.1.1	プロトタイプサービス企画	10
3.1.2	システム要件定義	12
3.1.3	14	
3.1.4	共助アプリベンダーへのヒアリングの実施	16
3.1.5	海外のデジタルアイデンティティの取り組み調査	19
3.2	検証できる領域を拡大する仕組み	24
3.2.1	検証できる領域を拡大し、Trust を向上するために検証が必要な課題	24
3.2.2	データフロー	25
3.2.3	データフローに登場する主体とその概要	25
3.2.4	検証できる領域を拡大し、Trust を向上するために本システムで検証を行うデータ及びデータのやり取りの内容	26
3.2.5	本システムで形成を目指す合意とその履行のトレースの内容	26
3.3	6 構成要素との対応	27
3.3.1	検証可能なデータ	27
3.3.2	アイデンティティ	27
3.3.3	ノード	28
3.3.4	メッセージ	28
3.3.5	トランザクション	28
3.3.6	トランスポート	28
3.4	本実証で企画したシステムの概要	29
3.4.1	業務フロー	29
3.4.2	ユースケース図	32
3.4.3	操作画面 (UI)	32
3.4.4	機能一覧/非機能一覧	32

3.4.5	データモデル定義(VC データモデルを採用する場合)	35
3.4.6	実験環境	36
3.4.7	システムの構成要素	36
3.5	実証を通じて得られた主な成果	36
3.5.1	システムの企画・開発に関する実証内容・得られた主な成果	36
3.5.2	ビジネスモデルに関する実証内容・得られた成果	38
3.5.3	共助トラストフレームワーク策定の実証内容・得られた主な成果	40
4	実証終了後の社会実装に向けた見通し	42
4.1	社会実装時に想定しているビジネスモデル・ユーザーのメリット	42
4.2	実証を通じて判明したユースケースの課題とその解決方針	46
4.3	本ユースケースの社会実装に向けたマイルストーン	47
5	Trusted Web に関する考察	48
5.1	Trusted Web のアーキテクチャに関する課題と提言	48
5.2	その他 Trusted Web の課題と提言	48

## 1 背景と目的

### 1.1 事業の背景

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、Consumer to Consumer の共助を目的とした WEB マッチングサービスが開発されている。

【例：AsMama（保育・子育て）、Twidy（買い物）、ジモティー（地域互助）、エニタイム（スキル）、Be My Eyes（視覚障がい者支援）、まちのコイン（地域活性化）】

また、スーパーシティ等の自治体の取り組みにおいても、公助と自助ではカバーしきれない「特定多数の共同・共創」として地域内の共助が課題になっており、DX 実現に不可欠な要素として共助アプリの活用が推進されている。

当社としては 2019 年より「スマホがつなぐ、助け合いアプリ May ii（メイアイ）<sup>1</sup>」をサービス化。各自治体と共同で数多くの実証実験を実施し、2020 年 12 月には「バリアフリー・ユニバーサルデザイン推進功労者表彰」の内閣府特命担当大臣賞奨励賞を受賞。2022 年 7 月からは利用エリアを全国に拡大している。

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、現状は下記 3 点がエコシステム拡大に向けた課題であり、本取組によるプラットフォームを横断したトラスト形成が必要と考える。

#### ① 「安全性担保」と「ユーザー拡大」の両立

C2C のマッチング（特にリアル接触が発生する場合）においては、両ユーザーの安全性を担保することがプラットフォームの重要な役割と認識。各企業は対策として、ユーザーの本人確認、評価制度等を導入している。一方で、ユーザー数が増えるほど安全性担保の条件は厳しくなり、サービス登録フローが複雑化しているケースも多い。またアナログのユーザー検証（事前研修による認定等）を実施する事業者も多く、企業の運用負荷が大きいことが課題になっている。今後は低負荷でユーザー属性の検証精度を上げながら、UI/UX はユーザーフレンドリーなオンボーディングの仕組みが必要。

---

<sup>1</sup> (URL: <https://mayii.jp/>)

## ② 共助アプリのエコシステム形成

現状は各ユースケースでサービスがサイロ化されている。ユーザー（サポート側）も利用シーン毎にアプリを切り替えて登録作業が必要な状況。複数のプラットフォームを横断して自身の属性情報を再利用できるようにすることで、既存優良ユーザー（サポート側）の活躍の場を広げ、より細かいニーズに対応した地域互助エコシステムの形成が可能になる。

## ③ 社会における「共助アプリ」の価値向上

各企業が共助アプリを軸にしながら、啓発のため、ワークショップや研修を実施し、ユーザー（サポート側）の育成に取り組んでいる。共助アプリにおけるユーザーの評価、研修受講履歴等がプラットフォームに縛られず、個人の属性として蓄積されていけば、受験や就職等の場面で指標として活用される等、自身を社会にアピールする手段の一つになる可能性があり、今後、より多くのユーザーの参加を促進できる。

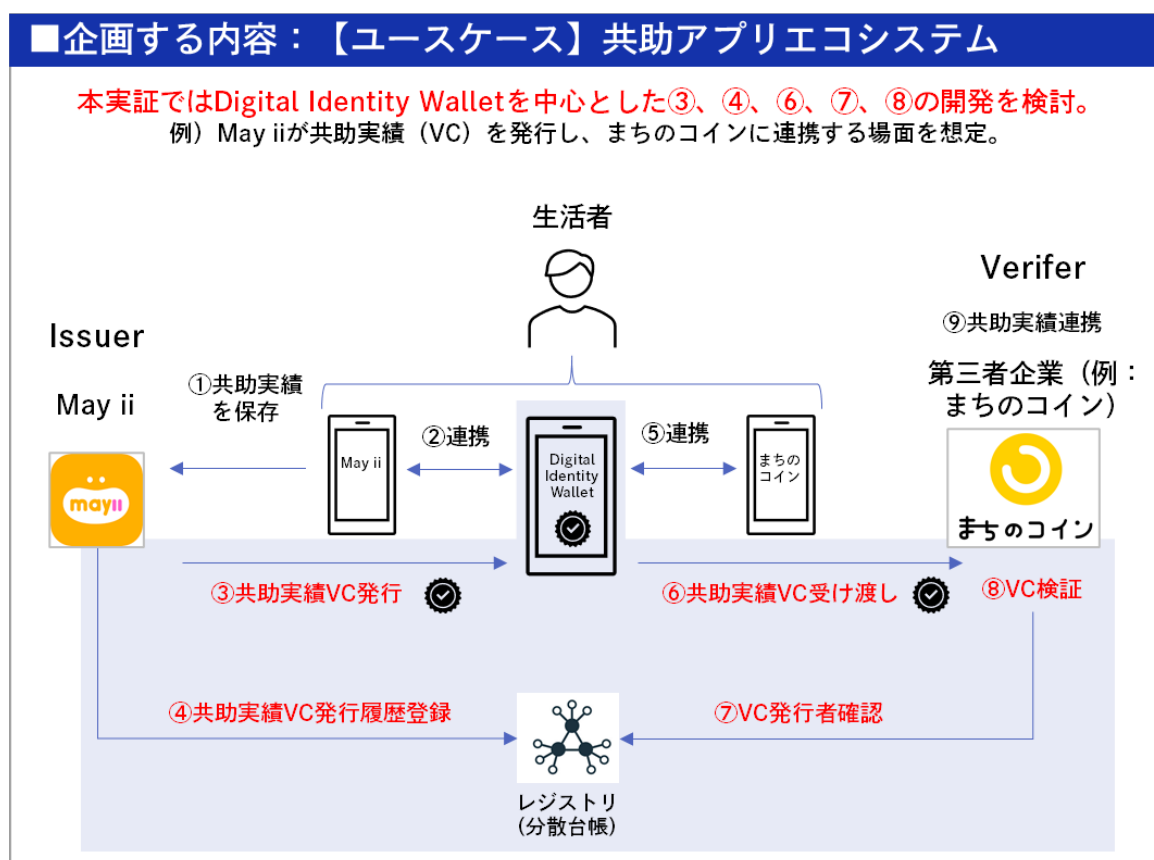
## 1.2 事業の目的

移動支援及び、保育、高齢者見守り等の各種分野における、Consumer to Consumer マッチングによる助け合いを目的とした共助アプリが対象。本取組では、現状アプリ毎にサイロ化して管理されているユーザーのトラストを、プラットフォーム横断で検証可能なインフラとして構築することで、安全安心で持続可能な共助エコシステムの活性化を目指す。

## 2 事業の概要

### 2.1 事業概要及び実証の範囲

ユーザーのトラストを共助実績 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。当社の共助アプリ「Mayii」運営チームと連携して本システム企画を進め、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。



### 2.2 社会・経済に与える価値・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。」<sup>2</sup>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「高齢化社会」「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 DID/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

<sup>2</sup> 出所) 「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](https://www.cas.go.jp/jp/seisaku/digital_denen/dai2/siryou2-1.pdf)

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。

「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<sup>3</sup>。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（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化社会において、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<sup>4</sup>。

### **② 共助データを活用した自治体 DX の促進**

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お金がかかり、迅速な施策の検討・実施が課題の一つとなっている。

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<sup>5</sup>」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。

---

<sup>3</sup> 出所) 「みずほ産業調査 Vol.39」

<https://www.mizuhobank.co.jp/corporate/bizinfo/industry/sangyou/m1039.html>

<sup>4</sup> 出所) 「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>

<sup>5</sup> 出所) 「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](https://www.soumu.go.jp/main_content/000620315.pdf)



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なく、社会的信頼度を評価する指標として活用できる。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。

## 2.3 コンソーシアムの体制

コンソーシアムの体制は、「May ii」を運営する DNP を代表機関とし、参画機関として本実証において様々なご意見を頂戴した「株式会社 AsMama」、「株式会社カヤック」、「株式会社プラスロボ」の 3 社にご参画いただいた。

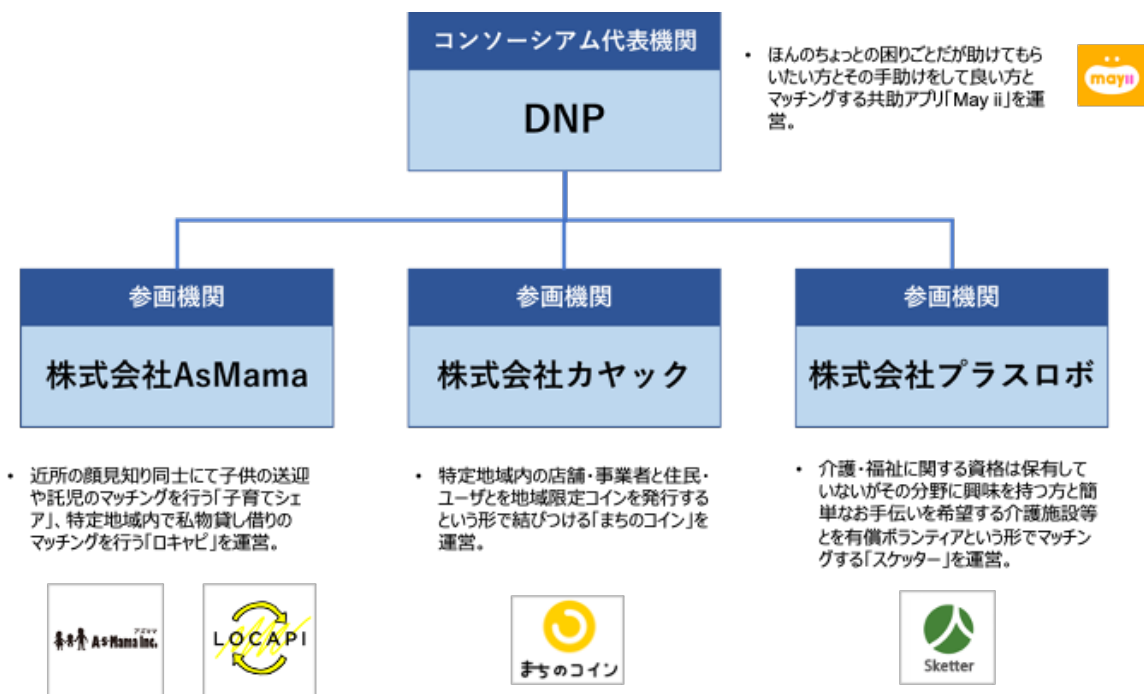


図 2.3 実施体制図

## 2.4 実証全体のスケジュール

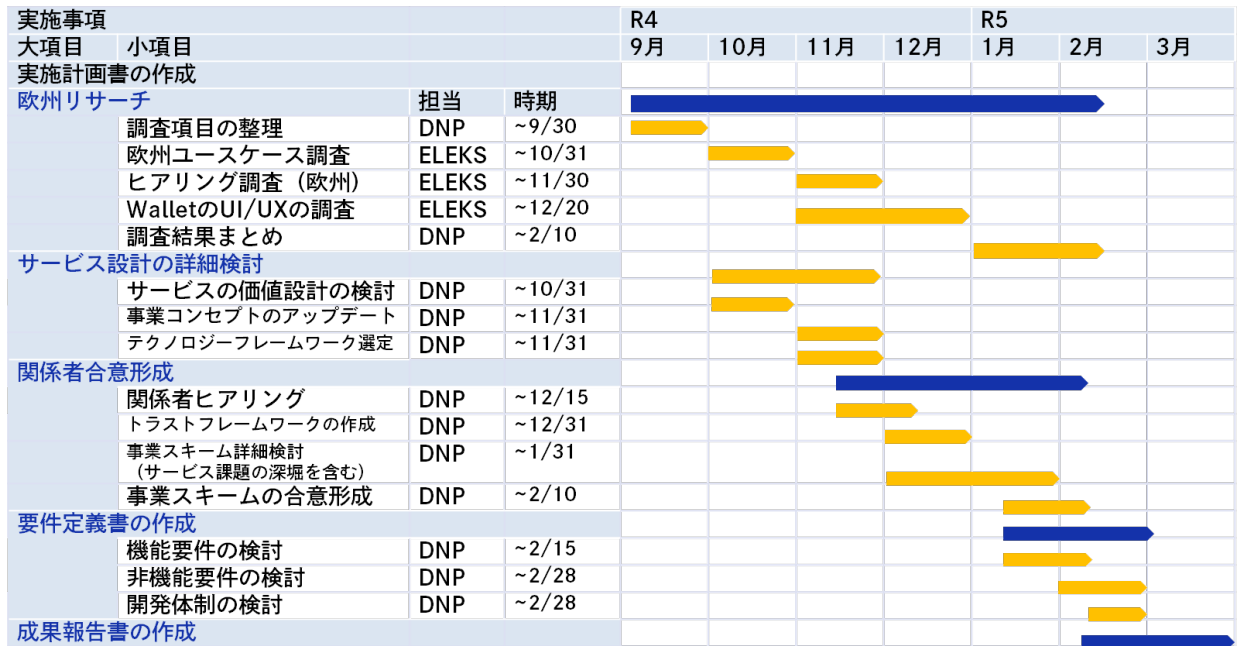


図 2.4 実証全体スケジュール

### 3 実証内容

#### 3.1 実証の実施事項、論点及び判断

##### 3.1.1 プロトタイプサービス企画

- カヤック（まちのコイン）、AsMama（子育てシェア、ロキャピ）、プラスロボ（スケッター）、DNP（May ii）へのヒアリングを実施し、共助アプリのトラスト形成に関するニーズや現状の課題について抽出した。論点となったのは、以下の3点。なお、下記に関わるヒアリングの詳細は、P16の「3.1.4 共助アプリベンダーへのヒアリングの実施」に記載している。

A：現状の共助アプリにおけるトラスト検証方法の整理

B：ユースケースの選定について

C：本取り組みによる効果について

- Aについては、各共助アプリでトラスト検証の方法を工夫しており、現状、KYCによるトラスト検証をしていない共助アプリも多いことが分かった。

利用者の安全確保のニーズの高い「子育てシェア」においては、サポーター認定をコミュニティにおける対面での実施に限定しており、高いレベルのトラスト検証を行っている。

一方で、「子育てシェア」と同じく AsMama が運営するモノの貸し借りアプリ「ロキャピ」では、決済サービスを導入していることから犯罪収益移転防止法<sup>6</sup>に準拠した eKYC を導入している。ユーザーのトラストを検証する仕組みとして、SNS 連携も実施しており、ユーザーがサポーターの情報を確認できるようになっている。

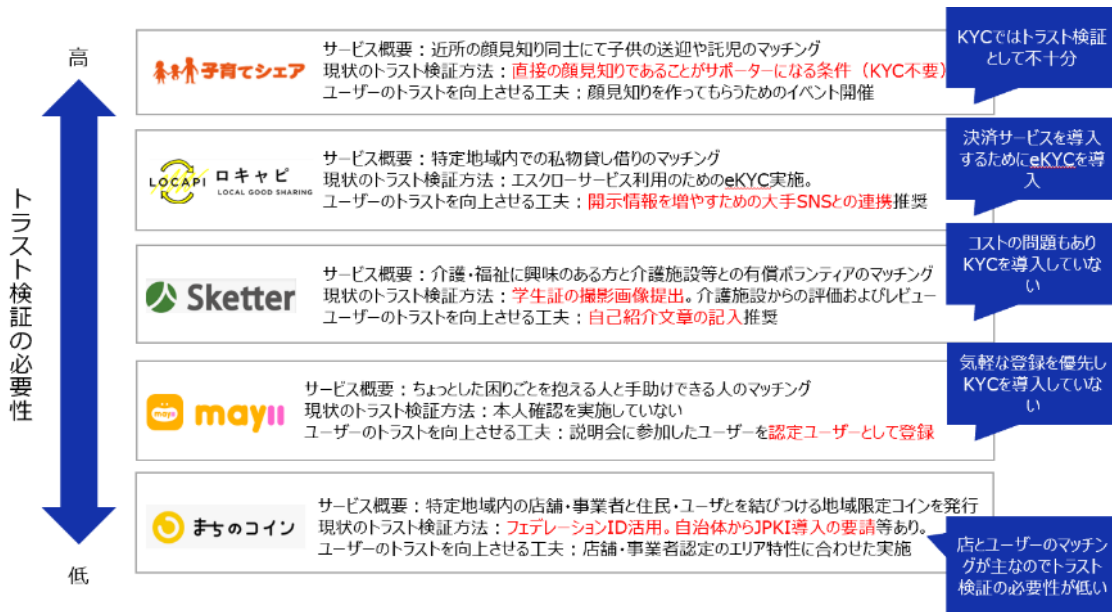
「May ii」や「スケッター」では、利用登録時に KYC を顧客に求めた場合、ユーザビリティが犠牲になり途中離脱率が上がってしまう可能性が高いことから、現状は本人確認を実施していない（スケッターについては学生証の撮影画像の提出はあり）。また KYC を導入する場合の費用もボトルネックになっており、アプリの初期フェーズにおいては KYC 導入を見送る判断をしている。ただし、利用中のプロフィール画面や評価システムの導入によって、サポーターの情報をユーザーが確認できるように設計されている。

「まちのコイン」については、現状 KYC は実施していないが、自治体から利用者のトラスト検証を理由にアプリ登録時の JPKI の導入を要請されるケースも出てきており、対応を検討中である。

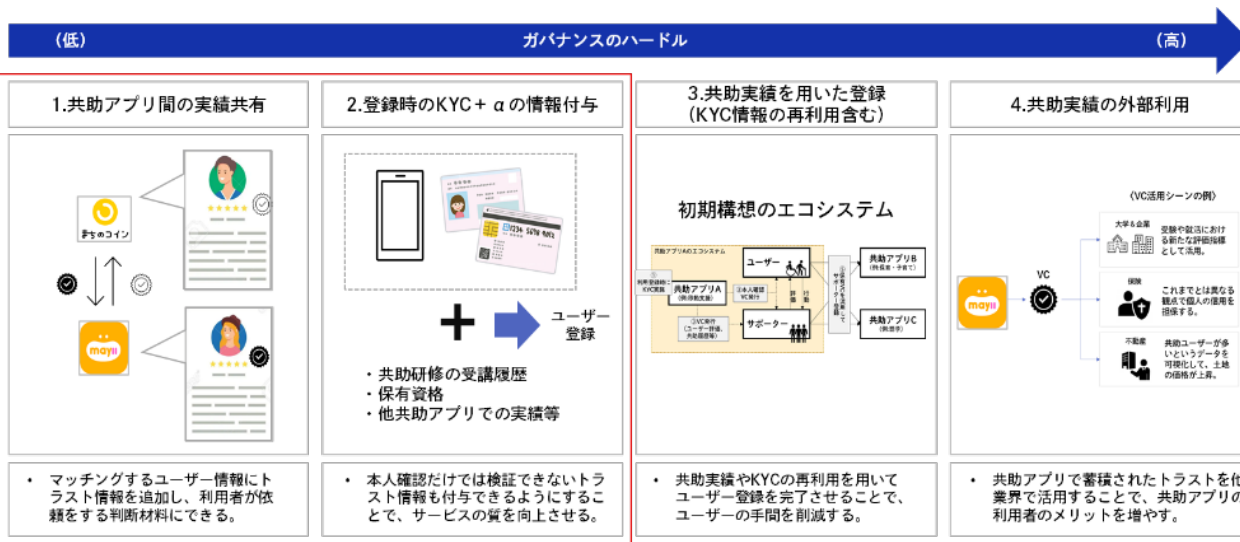
---

<sup>6</sup> 「犯罪収益移転防止法」が根拠となり、金融機関などの特定事業者には、口座開設などの特定取引の際に「本人確認手続き」が義務付けられている。

各共助アプリへのヒアリング結果、トラスト検証について以下の通り整理した。



- Bの本取り組みにおけるユースケースの選定については、当初 KYC 情報の再利用によりトラスト形成の簡易化を行うことを想定していた。しかしベンダーヒアリングを通して、共助アプリにおいては、各社が独自の方法でトラスト検証の工夫を行っており、KYC 実施率がそこまで高くないことが判明した。一方、それぞれの共助アプリでの活動実績や評価を、ユーザーのトラスト形成や新たな価値創出に繋げることについては意義を見出すベンダーが多かった。具体的には、各共助アプリの実績データをプラットフォームを超えて連携することで、コストを抑えながらユーザーの検証可能性を広げ、より安心できるサービス体験を提供することについてのニーズが確認できた。上記を踏まえて本取り組みにおいては、共助実績や研修受講履歴をクレデンシャルとして活用するユースケースを深堀するという結論に至った。



「ユーザーの検証範囲を今よりも拡張」する施策。  
 まずはこの領域から  
 共助アプリベンダーと検討を開始。

- C の本取り組みよる効果については、共助アプリベンダーへのヒアリングを基に現状の課題を整理し、本取り組みによる効果を検討した。その結果、「安全性：コスト最低限で検証の範囲を拡大できる」と「利用継続：共助実績データの活用でユーザーにインセンティブを提供できる」の 2 点において価値が高いとの結論に至った。現状の課題とメリットの詳細については、3.5.2 に記載する。

### 3.1.2 システム要件定義

- 海外事例の調査を実施し、システム構築のための要件や懸念事項を抽出した。論点となったのは、以下の 2 点。
  - A：分散型 ID フレームワークの選定
  - B：セキュリティ面の懸念と対応策について

A については、Private Ethereum for enterprise、Hyperledger Indy、Hyperledger Fabric で比較。フレームワークの選定にあっては、ユーザーのプライバシー保護への配慮を重視して調査を行った。スマートコントラクトを使う Private Ethereum for enterprise と Hyperledger Fabric については、実装方法が各社独自のものである場合が多く、プライバシーに配慮しながら、相互運用性を保つことが難しいと判断。一方、Hyperledger Indy のコミュニティ内ではフレームワークの実装方法がある程度整っており、プライバシーに配慮した設計がなされていた。具体的には、ユーザーの DID が分散台帳で公開されると、それと紐づいた VC に関連するデータが名寄せされる可能性があり、プライバシーリスクが高まる懸念があった。以上を踏まえ、今回はユーザーの DID を分散台帳等で公開しない方法で整理されている Hyperledger Indy での構築事例 (IDunion) を参照することに決定した。

フレームワーク	Private Ethereum for enterprise	Hyperledger Indy	Hyperledger Fabric
設立	2015	2017	2017
プログラミング言語	Solidity、NodeJs	Python	Go、Java、Javascript
スマートコントラクト	YES (Solidity)	NO (ただし、別途プラグインを開発することは可能)	YES (Go、NodeJs)
ゼロ知識証明	スマートコントラクトを使って実装可能	Anoncred (DID が分散台帳等で公開されない)	スマートコントラクトを使って実装可能
実装上の利点	古くから実装方式が検討されているため、開発経験者が多い。	コミュニティ内で、プライバシーに配慮した選択的開示やゼロ知識証明の実装方法が整理されている。	スマートコントラクトを使った柔軟な実装方法を検討することができる。
実装上の懸念事項	スマートコントラクトを使った実装の仕組みは各社各様で、相互運用性を保つのが難しい可能性がある。	コミュニティ内の実装方式に縛られ、柔軟な要件変更が出来ない可能性がある。	スマートコントラクトの複雑なロジックとネットワークの設定の両方を熟知した開発者が必要。

図 3.1.2 フレームワーク比較表

- B のセキュリティ面での懸念事項について、ガバナンス面と技術面で対策を検討した。詳細については、3.5.1 に記載する。

## 共助トラストフレームワークの策定

### 3.1.3

- 分散型 ID 技術を用いて、共助実績データを相互に共有可能なエコシステムを構築するためには、ガバナンスを機能させるための統一のルールが必要であると判断。先行するトラストフレームワーク（GAIN Trust Framework<sup>7</sup>、OIX Guide to Trust Frameworks for Smart Digital Identity<sup>8</sup>）を参考に共助版のトラストフレームワーク策定について検討した。下記 2 点が論点になった。

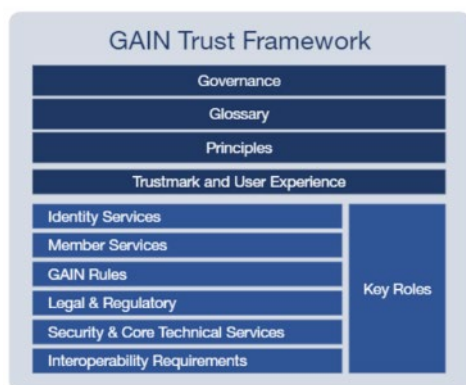
A：参考にするトラストフレームワークの選定

B：トラストマークについて

- Aについては、当初、Linux Foundation がデジタルアイデンティティの標準化を実現するためのコンソーシアムである「Trust Over IP」のガバナンスフレームワークを参考に検討を進めていたが、記載されている内容の抽象度が高く、具体的なユースケースへの落とし込みが困難であったため、別のトラストフレームワークを参考にすることにした。結果として、本実証の取り組みと近いユースケースであった GAIN Trust Framework（KYC 情報の再利用）と、GAIN でも参考にされている OIX Guide to Trust Frameworks for Smart Digital Identity をベースとしながら、共助トラストフレームワークを策定した。詳細は、P40 の「3.5.3 共助トラストフレームワーク策定の実証内容・得られた主な成果」に記載している。

## ■ GAIN Trust Framework

Global Assured Identity Networkホワイトペーパーより



<https://gainforum.org/GAINWhitePaper.pdf>

### GAIN Trust Framework

トラストフレームワークは、マルチパーティシステムを管理する法的強制力のある仕様と規則を定めたものです。GAINトラストフレームワークは、以下のことを保証するために設立されます。

1. エンドユーザーは、自分に関するデータの安全性と信頼する当事者の正当性を信頼することができます。
2. RPは、デジタルIDデータを安心して利用できる。
3. すべての関係者が、この論文で明示された利益を実現する。

ここに示す提案は、Open Identity Exchange (OIX) の2017年ガイドで示されたベストプラクティスに従って整理されている。

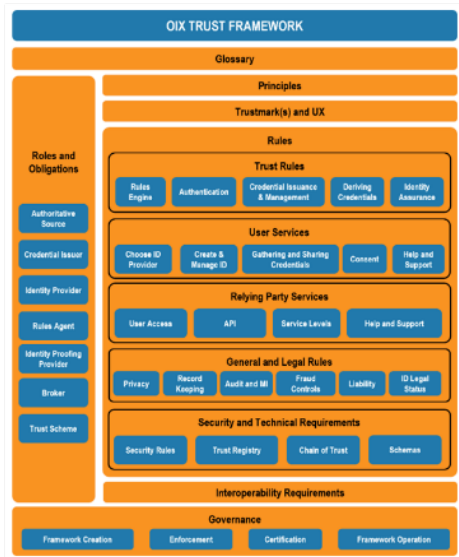
1. 用語解説と主な役割
2. ガバナンス、原理・原則、トラストマーク
3. トラストマークとユーザーエクスペリエンス
4. アイデンティティサービス
5. 会員サービス
6. 共助トラストルール
7. 参加するための基礎知識
8. 技術的な基礎知識
9. モニタリングとコンプライアンスの基礎
10. 主な法的側面
  - a. 責任
  - b. データ保護とポリシー
  - c. 規制のフレームワークと要件
  - d. 課金・清算の規則
  - e. 共助トラストメンバーの規制対象サービス
  - f. 相互運用性要件
  - g. 方針と手順
  - h. データ・メタデータ
  - i. プロトコル
11. コア技術サービス

<sup>7</sup> <https://gainforum.org/GAINWhitePaper.pdf>

<sup>8</sup> <https://openidentityexchange.org/a-guide-to-trust-frameworks-for-smart-digital-id?page=digital-identity-trust-framework>

## ■ OIX Guide to Trust Frameworks for Smart Digital Identity

OIX Guide to Trust Frameworks for Smart Digital Identity v1.2 June 2022



序文より～

このガイドは、スマートデジタルIDを実現するためのトラストフレームワークのあるべき姿について、その主要な構成要素である原則、内容、役割、責任について詳述し、専門家の見解を提供することを目的としています。

これは、世界中で受け入れられ、信頼のためのルールと基準を定義するグローバルな組織で使用されるベンチマークガイドとなった、OIX 2017の論文「Trust Frameworks for Identity Systems」を基に作成されたものです。この新しいガイドには、ヨーロッパのeIDAS、イギリスのVerify、カナダのPCTF、インドのAadhaarなど、既存の国内外フレームワークから学んだ教訓が盛り込まれています。

OIXは、トラストフレームワークを以下のような文脈で定義することにより、トラストフレームワークのすべての潜在的な構成要素について、実際の事例とともに、実務に基づいた包括的な説明を提供します。

- 原則とトラストマーク
- 信頼ルール（例：証明、認証、アイデンティティ保証）
- ユーザーサービス（例：Consent、Multiplicity、ID作成など）
- 組織的なサービス（例：ユーザーアクセス、責任、SLA）
- 一般的・法的規則（例：データ管理、記録保持、不正管理）
- セキュリティと技術要件（例：スキーマ、信頼の連鎖）
- ガバナンス（認証、登録、運用など）
- インターオペラビリティ

<https://openidexchange.org/a-guide-to-trust-frameworks-for-smart-digital-id?page=digital-identity-trust-framework>



- B のトラストマークについては、ガバナンスの観点から、正当な Issuer を認定するトラストマークを発行することが先行事例では一般的であるものの、トラストマークの定義や内容が曖昧であった。下記の通り整理して検討した。

■トラストマークとは何か？

トラストマークとはトラストフレームワークに準拠していると認定された組織を判別することができるシボル。人々が容易に識別できるようなフレーズ、単語、ロゴなどがトラストマークになる。トラストフレームワークの運営主体は、定められたルールに従って参加メンバーを審査し、問題がなければトラストマークを付与する。

■トラストマークはどこでどのように提示されるのか？

ユーザーが共助アプリベンダーを安心して選択できるように、アプリのダウンロード画面や紹介ページに掲載することが推奨される。

■トラストマークにはどのような情報が含まれるのか？

- ・ どのような背景・運営主体がバックに存在するか。
- ・ 誰がどのような基準に基づいてトラストマークの審査したのか。
- ・ どのような場面で共助実績を利用することができるか。
- ・ 困ったことがあったときの窓口はどこか。

### 3.1.4 共助アプリベンダーへのヒアリングの実施

共助アプリを運営する3社に対して、トラスト形成、トラストフレームワーク、サービス企画の観点でヒアリングを実施した。

(1) ヒアリング概要（合計9回のヒアリングを実施）

- 10月中旬 カヤック社へ現状のトラスト形成の課題についてヒアリング
- 11月上旬 AsMama 社へ現状のトラスト形成の課題についてヒアリング
- 11月下旬 プラスロボ社へ現状のトラスト形成の課題についてヒアリング
- 1月上旬 AsMama 社へトラストフレームワークについてヒアリング
- 1月上旬 カヤック社へトラストフレームワークについてヒアリング
- 1月中旬 プラスロボ社へトラストフレームワークについてヒアリング
- 1月下旬 AsMama 社へサービス企画の内容についてヒアリング
- 1月下旬 カヤック社へサービス企画の内容についてヒアリング
- 2月上旬 プラスロボ社へサービス企画の内容についてヒアリング

#### ■ヒアリング内容のポイント

- ・ 各社それぞれにユーザー同士のマッチングを安全に行うための工夫（対面でのサポーター認定、評価システム導入、SNS 連携等）をしている一方で、KYC によるユーザーのトラスト検証を行っている共助アプリは多くなかった。ユーザーのトラスト検証が共助アプリサービス運営の根幹に関わるテーマであるという認識については一致していた。
- ・ 現状の共助アプリのトラスト検証において抱える問題点としては、対面によるサポーター認定の負荷（子育てシェア）、SNS 連携によるサポーターの信頼向上とプライバシー保護のバランス（ロキャピ）、eKYC 導入による登録途中脱率アップへの懸念（May ii）、プロフィールに記載されている内容の信ぴょう性（May ii、スケッター、ロキャピ）等が挙げられた。
- ・ アプリのスケール前の利用者数であればトラスト検証は問題にならないが、徐々に利用者数が増えるにつれて性善説での対応に限界が来るとの意見も多く出た。
- ・ 共助アプリを横断した実績データ共有により検証可能性を拡大することについては、各社とも前向きな回答があった。ベンダー側のメリットとしては、ユーザーマッチングの安全性向上、サービス領域の拡大（例：現状は企業と生活者のマッチングサービスに限定しているが、生活者同士のマッチングも可能なサービスに拡大する等）、ユーザーへのインセンティブ等が挙げられた。特に、蓄積された共助実績がユーザー自身のトラスト向上に繋がり、別の価値を生む可能性があることについては、意義を見出すベンダーが多かった。
- ・ 近年の就職活動や大学入試では、学力以外にボランティア活動等の経験を話す機会も増えており、共助アプリ利用者から「ボランティア参加証明」のようなものを求められることもあるとのこと。共助実績もそのような場面で活用できるかもしれないとの意見も出た。

#### （2）ヒアリング結果の詳細

##### ■カヤック社：

カヤックの運営する「まちのコイン」においては、現在フェデレーション ID でのログインを実施しているが、自治体等から本人確認の要請があり、今後はマイナンバーカードの JPKI 活用も検討中。

「まちのコイン」ユーザーの地域内におけるトラストを蓄積・可視化するサービスについては、ユーザーへのインセンティブになる可能性があるため、事業者として取り組む意義を感じるとのことだった。また現時点では、「まちのコイン」のサービスで個人間のやり取りは行われていないが、検証できるトラストが拡大することによって、判断基準を確立することが出来れば、個人間のやり取りを行うサービスもできるようになるかもしれないといった意見も出た。

■ AsMama 社 :

保育園の送り迎えのマッチングを行う「子育てシェア」では、ユーザーのトラスト形成について長年様々な試行錯誤をしており、現在はコミュニティ内で対面確認をした人だけをサポーターとして認定するようにしている。（「子育てシェア」の登録自体では KYC は実施していない。）一人ひとり対面での確認を行うため運用の負荷はかなり高いが、ユーザーが安心してサービスを利用できる環境を最優先にしている。

一方でモノの貸し借りをを行うマッチングサービスの「ロキャピ」も運用しており、SNS との連携でサポーターの情報を確認できる工夫する等の「子育てシェア」とは異なる観点でのトラスト形成にも取り組む。（「ロキャピ」では、物品のやりとりの中間に入り、代金決済等の取引の安全性を確保するエスクローサービスを利用しているため、登録時に eKYC が必須になっている）

SNS 連携によってユーザーがより多くの情報を見ながらマッチング相手を選択できる反面、住所バレによるトラブルなどのプライバシー侵害のリスクに関する懸念もある。

トラスト形成に関して長年のノウハウを持っている AsMama 社としても、ユーザーのトラストが可視化され、別の場面で活用できることに関する取り組みは興味があるとのことだった。

共助実績を流用する具体的なユースケースについても、「ロキャピ」においてユーザーが最初からトラストを高い状態にすることで物品の破損・汚損・紛失等の賠償責任保険適用の必要をなくしたり、プライバシーを保護しながらユーザーの質を検証するための方法として採用したりできる可能性等、様々な意見を聞くことができた。

■ プラスロボ社 :

介護福祉施設の人手不足解消を目的としたサポーターのマッチングサービスを行うプラスロボ社では、金銭問題や怪我・事故のリスクがある業務に関してのみ、学生証などの身分証の提示を実施している。

現状、ユーザーのトラストを判断する方法としては自己紹介文の記載等があるが、新規登録者の中には自己紹介文を記載していないユーザーも多く、受け入れ施設側が安心して判断できる基準がないという課題がある。本取り組みにより、ユーザーのトラスト検証の幅が広がれば、受け入れ施設側も判断材料の一つとすることができるため、今よりも安心できるサービスの提供につながる可能性があるとのこと。また新たなデータ連携を実施するために発生する開発費や、その検討に要するコミュニケーションコストが実施の課題になるという意見も出た。

■ DNP :

移動困難者のちょっとした困りごとを街なかのサポーターが解決するマッチングサービスを提供する「May ii」は、気軽な登録を優先し、ユーザー登録時の途中離脱を防ぐため、KYC を実施していない。

現状、ユーザーのトラストを向上する方法として、説明会や体験会などのイベントに参加したユーザーを認定ユーザーとして登録し、マッチング時に相手に表示している。

共助アプリ間で共助実績を連携することで、ユーザーのトラスト検証によりマッチング時の安全性が向上するほか、現状、サポーターにとってインセンティブがアプリ内ポイントのみのため、サポートの実績を外部利用できるようによって、新たなインセンティブとなることを期待する意見が出た。

### 3.1.5 海外のデジタルアイデンティティの取り組み調査

ドイツで実施されている SSI やデジタル ID Wallet の取り組みについて調査を実施。先行する実証において政府が力を入れている点や、課題になっていることをヒアリングして整理した。

調査内容：

#### ■ 概要

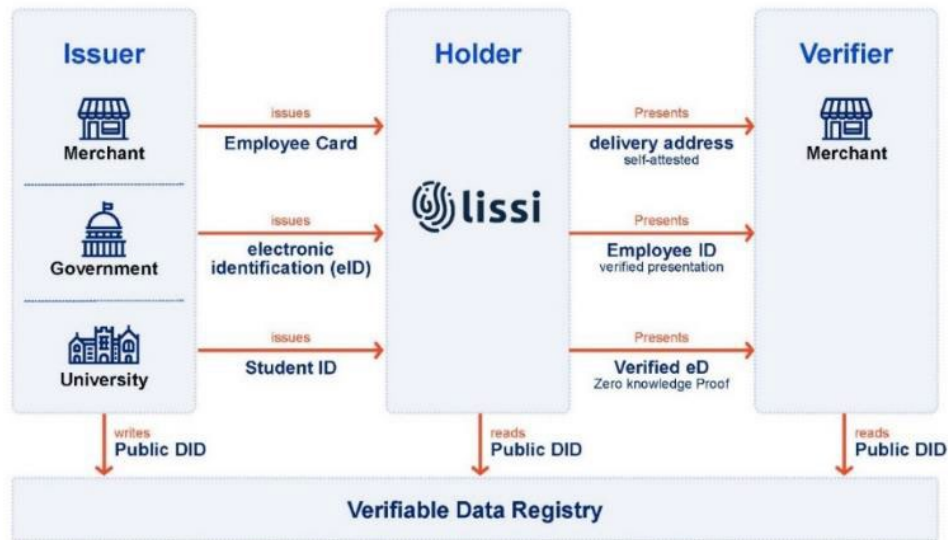
ドイツ連邦経済省は、行政、企業（特に中小企業）、国民にとって利用しやすく、信頼性が高く、経済的なドイツの eIDAS ソリューションの開発を目指し、2019 年にショーケース・プログラム「Secure Digital Identities」を開始。合計 4 つのプロジェクトが選ばれ、今後 3～4 年の間に、ドイツ国内のさまざまな都市やコミュニティで実証実験を行う予定になっている。選ばれたプロジェクトは、すべて SSI の分野であり、SSI アプリケーションの広範な PoC となっている。その目的は、ユーザーがモバイルデバイスを使って場所を問わずにデジタルで本人確認ができる、新しい ID エコシステムを構築すること。ヒトの認証、モノの認証、またはその両方の組み合わせに関連した PoC を予定している。プロジェクトのユースケースは、教育、医療、ホスピタリティ、観光、貿易、物流、モビリティ、エネルギー、インダストリー4.0、IoT、アクセス管理、行政、金融の 10 分野をカバーしている。

#### ■ 「Secure Digital Identities」の 3 つのプロジェクト

「Secure Digital Identities」の目的は、ヨーロッパ全域での使用に適し、SSI に基づいて人、機関、物のアイデンティティに等しく機能するインフラを構築することである。基本的にはスマートフォンをベースとし、検証可能な証明書はデジタルウォレットに保存される。現在、3 つのプロジェクトが実施段階に入っている。

#### ① IDunion

欧州の協同組合 Societas Cooperativa Europaea S.C.E をガバナンス当局とし、法人としてネットワークのルールとその実装を決定し、分散型の公開鍵基盤を実装している。また独自のウォレット（Lissi と esatus）とスマートフォンとクラウド間の通信を行うためのエージェントも開発している。



図：IDunion SSI プロジェクトのフレームワーク

### ②ONCE

行政、運輸、ホテル業界向けの安全なデジタル ID を開発・実装している。ONCE で使用されている ID システムは eIDAS に準拠しており、さまざまな分野のアプリケーションで要求されるセキュリティと信頼の要件に対応している。

### ③ID-ideal

W3C と DIF に基づく既存の SSI 標準を考慮したトラストフレームワークの開発に焦点を当てている。詳細については以下の調査結果に記載。

調査結果：

「Secure Digital Identities」の中から、特にトラストフレームワークの開発に焦点を当てている ID-ideal の取り組みを詳細に調査した。

A：ID-ideal の取り組みの深堀

B：ID-ideal の実証における課題についてのヒアリング

➤ A：ID-ideal の取り組みの深堀

ID-ideal プロジェクトは、ドイツ連邦経済・気候変動省（BMWK）が支援するイノベーションコンペティション「Secure Digital Identities Showcase」（SDIS）において資金提供されている。このコンペティションは、ドイツの eIDAS ソリューションが、ユーザーフレンドリーで、信頼性が高く、経済的なものになることを目的としている。

3 年間のプロジェクト期間中（2021-2024）、様々なプロジェクトの中でビジネスや行政におけるデジタル ID の取り扱いをより安全かつ容易にすることを旨とする。

■ ID-ideal プロジェクトの優先順位（下記の優先順位で検討を進めている）

● 相互運用性

ID-ideal は TrustNet と呼ばれる法的に安全なデジタル空間を作ることをビジョンにしている。TrustNet では、ステークホルダーは明確に識別可能であり、交換される情報は検証可能であり、取引は法的に安全である。同時に、すべてのステークホルダーに対してデータ主権が確保される。

● フレームワークの定義

このプロジェクトのもうひとつの優先課題は、トラストフレームワークを定義することである。一連のルールとして異なる ID サービスを調和させ、安全な証明書の交換のための基準を作成していく予定。

● ユーザーへのインセンティブ

上記の優先事項の中で、ID-ideal は、デジタル ID サービスの利用拡大につながるインセンティブを作り出すことも重視している。（例えば、日常生活との高い関連性、優れたユーザビリティ、および自己のデータを経済的に活用する可能性等）

④コミュニティの発展

デジタル ID ソリューションは、ユーザーと、デジタル ID サービスを提供しサポートするコミュニティからの幅広い支持があって初めて機能する。ID-Ideal の取り組みは、安全なデジタル ID 活用を促進するオープンコミュニティとして TrustNet イニシアチブを発展させることも目指す。

## ■ ID-ideal のユースケースについて（保育所における手続き管理）

ドイツでは、約 400 万人の子どもたちが保育所（KiTa）に通っている。保育所では、日々の生活の中で、子どもたち一人ひとりのために個別の手続きが必要。例えば、遠足や休日の登録・抹消、病気の診断書や健康診断書の提出、家族の送迎許可、子どものアレルギーの告知など、保護者は日々の生活の中で、子どもたち一人ひとりのために対応している。こうした事務手続きは、現在は印刷物や電子メールなどの書面によって行われている。

### ■ 現行システムの問題点

- ・登録に時間がかかる
- ・登録が紙ベースである
- ・書類の回収と登録は本人（保護者？保育士？）しかできない
- ・保育所の無料枠の有無について透明性がない。

この問題に取り組む ID-IDEAL のユースケースのひとつに、Mittweida 市でのプロジェクトがある。保育園への登録プロセスや情報提供プロセスを再設計し、すべての関係者にとってよりシンプルで便利、同時に安全なものにすることを目的としている。

この計画では分散型 ID の技術を使って、保育所の子どもの初期登録のための管理ソフトウェアを実装し、テストする予定。

例えば、デジタルウォレットから、子供の送迎の権限を第三者に発行し、再び撤回することができるようになることが想定されている。従来は親の都合に合わせて送迎者を変更することが難しかったが、デジタルウォレットを通して信頼できる第三者を保育所側が検証可能になり、柔軟な対応ができるようになる。また、保護者と保育施設間の契約内容の変更も、契約当事者によって署名できる。

保育所のシナリオの原則は、高齢者施設、老人ホーム、病院など、第三者によって人々がケアされるすべての施設に適用することができる。

## ➤ B : ID-ideal の実証における課題についてのヒアリング

### ■ ID-ideal の課題ヒアリング

Exxeta Tech & Consulting 社へのインタビュー（2023 年 1 月 27 日に実施）

<https://exxeta.com/>

#### （1）相互運用性について

デジタルウォレットのセットアップは重要な問題である。現在、デジタルウォレットの開発を提供する企

業は数多く存在するが、これらの企業間の相互運用性は極めて低い。例えば、ID-ideal コンソーシアムには、現在少なくとも 3 社のデジタルウォレットプロバイダー（Yolo、Authada、Evans）が存在する。ある人が A 社のデジタルウォレットをダウンロードした後、B 社のデジタルウォレットで実装されているユースケースから ID を取得したい場合、その人は別のデジタルウォレットをダウンロードする必要がある。ドイツだけでなく、ヨーロッパ全体でも同じ状況になっている。非常にたくさんあるウォレットの発行者の中から、適切なベンダーを選ぶ基準となるスタンダードを作ることが重要。

### （2）Wallet のリカバリーについて

デジタルウォレットの入った携帯電話を紛失したり、デジタルウォレットにアクセスできなくなったりした場合に大きな問題が発生する。現在、ID-Ideal はウォレットや ID の回収について、ID をクラウドまたは外部に保存するオプションを提供することを検討している。しかしいずれも、セキュリティの観点からは最適とは言えない。ウォレットにアクセスできなくなったり、ウォレットの入った携帯電話を紛失したりした場合、ウォレットを再度ダウンロードし、ID を再発行する方法が最も安全だと考えている。

### （3）ユーザーへのインセンティブについて

例えば、以前のプロセスに対するコスト、時間、労力の削減を伝えることで、初めてウォレットを使うことのメリットを納得してもらうことができる。ID-ideal でのキーワードは「より快適に」ということだ。公共性の高い分野では、誰かに強制的に使わせることはできない。例えば図書館カードの例がある。ここで重要なのは、現在のプロセスを改善していることだ。現状、図書館カードをデジタルで発行したい場合、最低 1 回は図書館に行く必要がある。デジタル ID ソリューションを使えば、その登録作業をとっても簡単にすることができる。そのような明確なユーザーメリットを訴求することが重要だと考えている。



## 3.2 検証できる領域を拡大する仕組み

### 3.2.1 検証できる領域を拡大し、Trust を向上するために検証が必要な課題

#### 【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が開発されている。

共助アプリでは、見知らぬ生活者同士がマッチングするサービスが多く、ユーザーの安全性担保が各プラットフォームの責務になっている。そのため共助アプリベンダーにとって「ユーザーの信頼検証」はサービスの根幹に関わる重要なテーマとなっており、各社が独自に様々な工夫を行っている。

#### 【ペインポイント】

各共助アプリベンダーへのヒアリングを通して、下記のような現状のペインポイントが明らかになった。

- ユーザープロフィールの表示や SNS 連携を通して、ユーザー同士で確認できる信頼を拡大する工夫を行っているが、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。
- アプリ内でのユーザー評価システムによって信頼検証を促す場合もあるが、現状、利用者数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提供できるほどの規模がないサービスも多い。
- 共助実績が蓄積されない→共助アプリ内で信頼検証できない→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。

上記問題を解決するため、本実証では「共助アプリを横断した信頼共有エコシステム」の企画設計を行った。アプリを横断して共助実績データを蓄積し、ユーザー信頼の検証範囲を拡大することで、より安心な共助体験の実現を目指す。また将来的には、学校や企業に対して共助実績をデジタル証明書として提出し、新たな価値を創出することも見据える。

#### 【課題を解決するテクノロジーについて】

現在、共助アプリを含むシェアリングサービスは日本に 300 社（シェアリングエコノミー協会への登録数<sup>9</sup>）ほど存在し、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した。

---

<sup>9</sup> <https://sharing-economy.jp/ja/about/join/>

### 3.2.2 データフロー

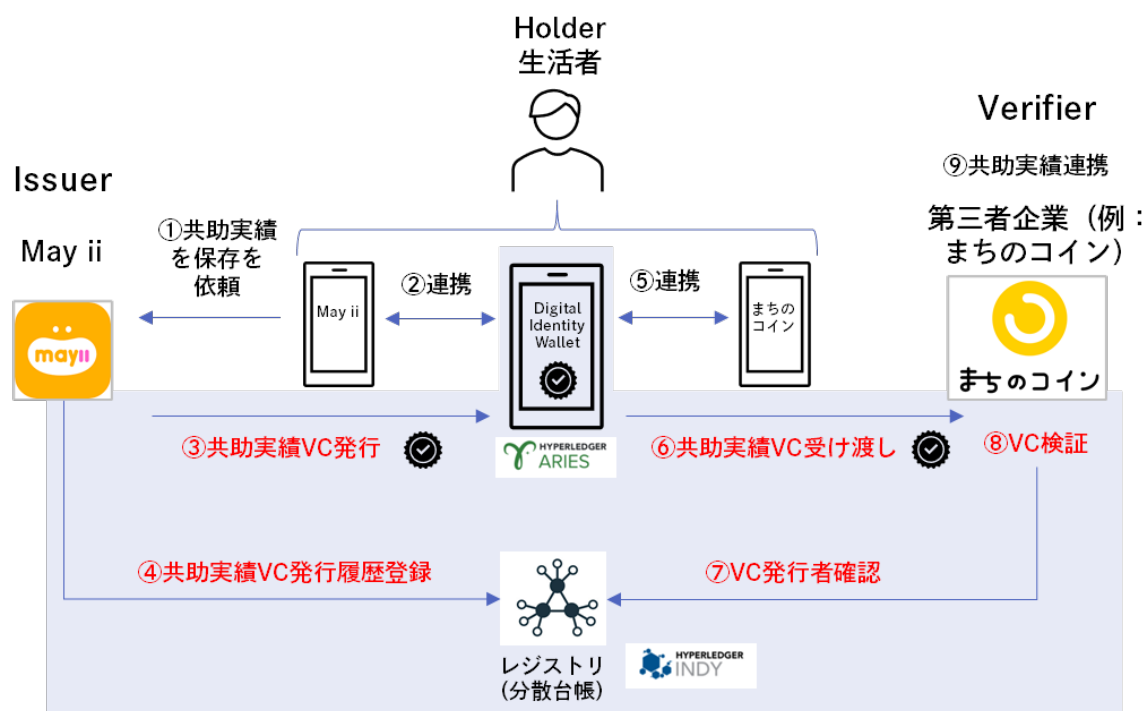


図 3.2.1 データフロー図

データの保有者である Holder は、Issuer に共助実績 VC の発行を依頼して共助実績 VC を取得する。Holder は Wallet にて共助実績 VC を管理し、情報要求者（Verifier）の資格要件を確認した上で開示を行う。開示を行う情報の範囲については Holder が主体的に選択することが可能である。

### 3.2.3 データフローに登場する主体とその概要

- 共助アプリのサポーター（=Holder）
  - 発行された共助実績 VC を保有して、Wallet 上に自分に関する属性情報を保存。他の共助アプリを利用する際に、合意形成された必要な情報のみ選択的に Verifier に提示する。一方の共助アプリを利用して蓄積された共助実績を他の共助アプリでも表示できるようになり、トラストの高い状態で共助アプリを利用することができる。
  
- 第三者の共助アプリ企業（= Verifier）
  - Holder から共助アプリ実績を受け取り、検証する。共助実績の情報を検証できた場合は、ユーザーのプロフィールに他の共助アプリ実績を表示できるように登録することで、マッチングの安全性を向上させることができる。

- 共助実績発行企業（= Issuer）
  - 共助アプリサポーターの共助実績を VC として発行し、Holder の Wallet に送る。サポーターの共助実績をデジタル証明書にすることで、サポーターへのインセンティブとなり、共助アプリの活用が促進される。

### 3.2.4 検証できる領域を拡大し、Trust を向上するために本システムで検証を行うデータ及びデータのやり取りの内容

- 共助実績の共有
  - 他の共助アプリでの実績を証明してサポーターのトラストを向上させるために、共助実績の内容を VC の署名検証によって検証する。具体的には、共助アプリ A が発行し、スマートフォンのストレージに格納されているサポーターの VC を別の共助アプリ B が検証する。アクセスコントロールは 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する。
  - 検証にあたっての留意点としては、共助アプリの種類ごとにジャンル分けして実績を表示（お手伝い名人、モノの貸し借りの達人等）することで、マッチングするユーザーが安心してアプリを使う判断材料を増やすことを目指す。
  
- 本人確認 + a の情報付与
  - 共助アプリにおけるユーザー登録の際に、本人確認の情報だけではなく、他の共助アプリでの実績や研修受講履歴を証明してサポーターのトラストを向上させるために、実績や受講履歴の真正性を VC の署名検証によって検証する。具体的には、共助アプリ A や研修受講時に主催者が発行し、スマートフォンのストレージに格納されているサポーターの VC を別の共助アプリ B が検証する。アクセスコントロールは 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する。

### 3.2.5 本システムで形成を目指す合意とその履行のトレースの内容

- 共助実績 VC の内容について
  - 共助アプリユーザーと共助アプリ間において、情報提供の可否、提供可能な情報の選択、情報提供可能な第三者の選択、提供した情報の有効期限、共助アプリ間の実績の評価等について合意する。
  
  - ① 共助実績の共有
    - ユーザーが保持している他の共助アプリの実績について、情報提供の可否、提供可能な情報の範囲を合意したうえで、連携して表示をする。

- ②本人確認 + aの情報提供  
本人確認情報以外に、資格情報や共助実績について、提供可能な情報の選択（資格名、取得日時等）を行い、共助アプリの登録時に連携する。
- トレース方法について  
共助アプリエコシステムを導入した自治体が共助に関する VC の量や流通をトレースすることによって、地域の課題や状況をモニタリングすることに活用することを想定（本実証の検討範囲外）。
- 合意の取り消し可否について  
本実証で現在検討中のユースケースでは合意の撤回・取り消しは想定していないため、検討のスコープ外。

### 3.3 6 構成要素との対応

#### 3.3.1 検証可能なデータ

##### (1) 検証対象

- issuer (May ii)
- verifier (第三者企業 = まちのコイン)
- end-user (生活者)
- wallet
- eKYC 時の本人確認レベル等の情報
- 本人確認以外の情報（資格、共助研修履歴、共助実績等）
- 事業者間で共有される共助実績の情報
- 情報連携経路
- トランザクション情報（エラー情報や不審なトランザクション等を含む）

##### (2) 検証者

- verifier (第三者企業 = まちのコイン)

#### 3.3.2 アイデンティティ

##### (1) アイデンティティとして想定されるもの

user（共助提供者）、user（共助需要者） service provider (issuer = May ii) 、 verifier（第三者企業 = まちのコイン）

##### (2) アイデンティティ管理システム

DID/VC を用いる

### 3.3.3 ノード

(1) Wallet の使用有無

Holder であるユーザーの VC 管理においては Hyperledger Arise の Wallet ベースで実装を想定しており、共助アプリ A (Verifier)、共助アプリ B (Issuer) においては既存の web アプリケーションをベースに実装を想定。

(2) 合意形成がされているか、されている場合その手段

- ・end-user (生活者) が自らデータ (本人確認レベル等の情報、本人確認以外の情報) を管理して、利用したい共助アプリに Wallet を通じてデータを渡し、合意形成する。
- ・end-user と service provider 間のデータの取扱いに係るユーザーの同意に基づく規定を保管

(3) データのやり取りの記録場所

レジストリ (分散台帳 : Hyperledger Indy)

### 3.3.4 メッセージ

(1) コネクションオリエンテッドかメッセージオリエンテッドか

- ・Trust 情報の発行 (リクエスト+レスポンス)
- ・Trust 情報の提示 (リクエスト+レスポンス)

### 3.3.5 トランザクション

(1) データのやり取りの記録・検証はできるか

- ・ 全ての[リクエスト+レスポンス]はトランザクションたり得ます

### 3.3.6 トランスポート

(1) トランスポートのプロトコル

- ・ Azure 基盤の機能を利用

### 3.4 本実証で企画したシステムの概要

#### 3.4.1 業務フロー

##### VC 発行者情報の登録（共助サービス事業者）

- ・事業者の発行者認定フロー

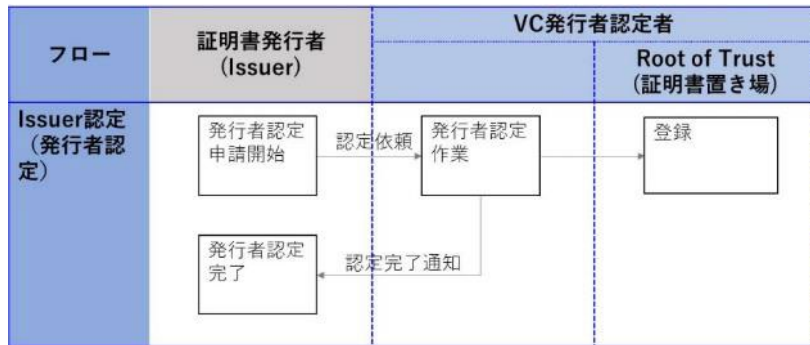


図 3.4.1.1 事業者の発行者認定フロー

- ・事業者の DID 登録フロー

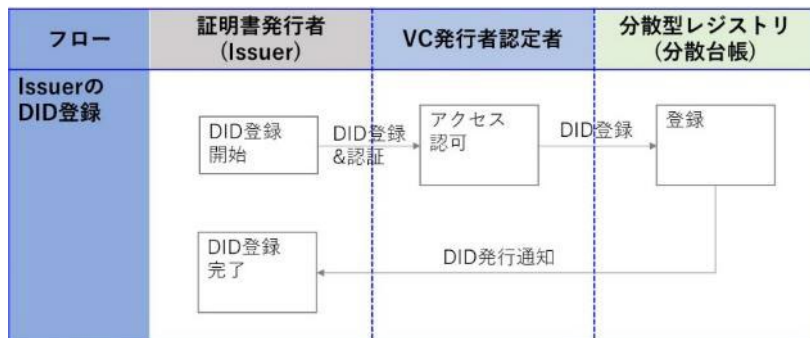


図 3.4.1.2 事業者の DID 登録フロー

・VC 発行業務（共助サービス事業者）

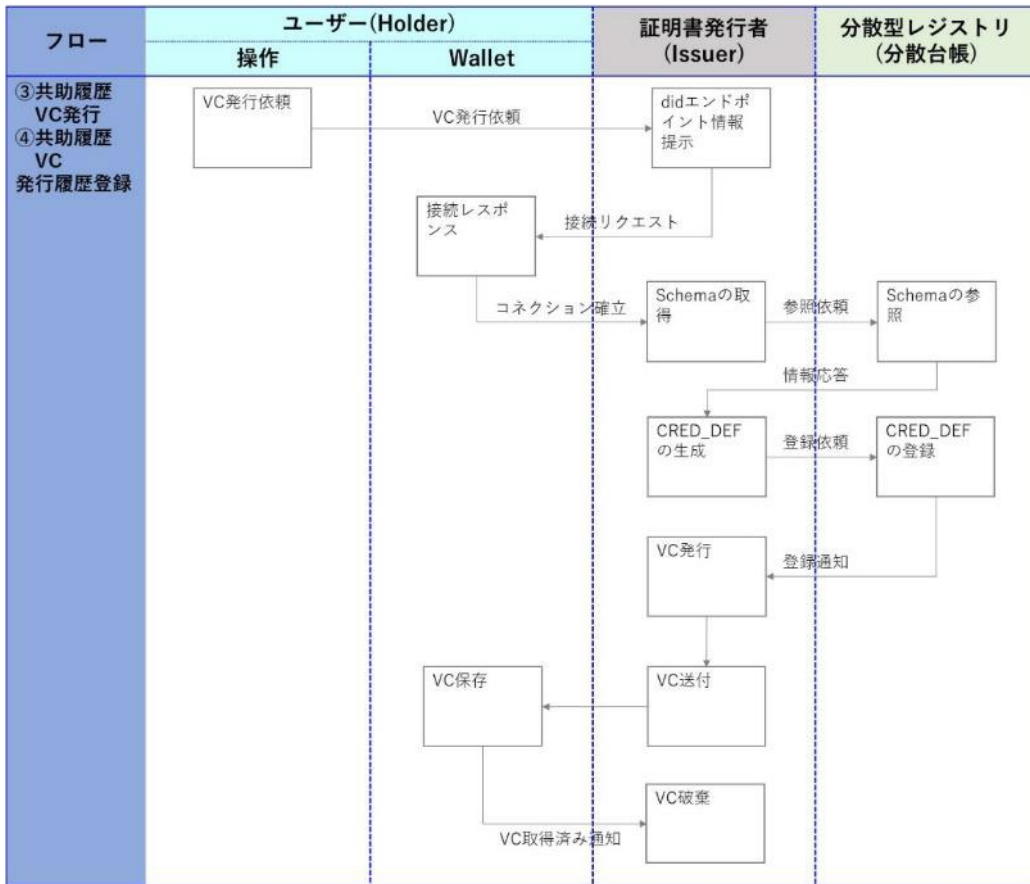


図 3.4.1.3 VC 発行業務（共助サービス事業者）

VC 検証業務（サービス提供者）

- ・ 共助履歴 VC 受渡フロー
- ・ VC 発行者確認フロー
- ・ VC 検証フロー

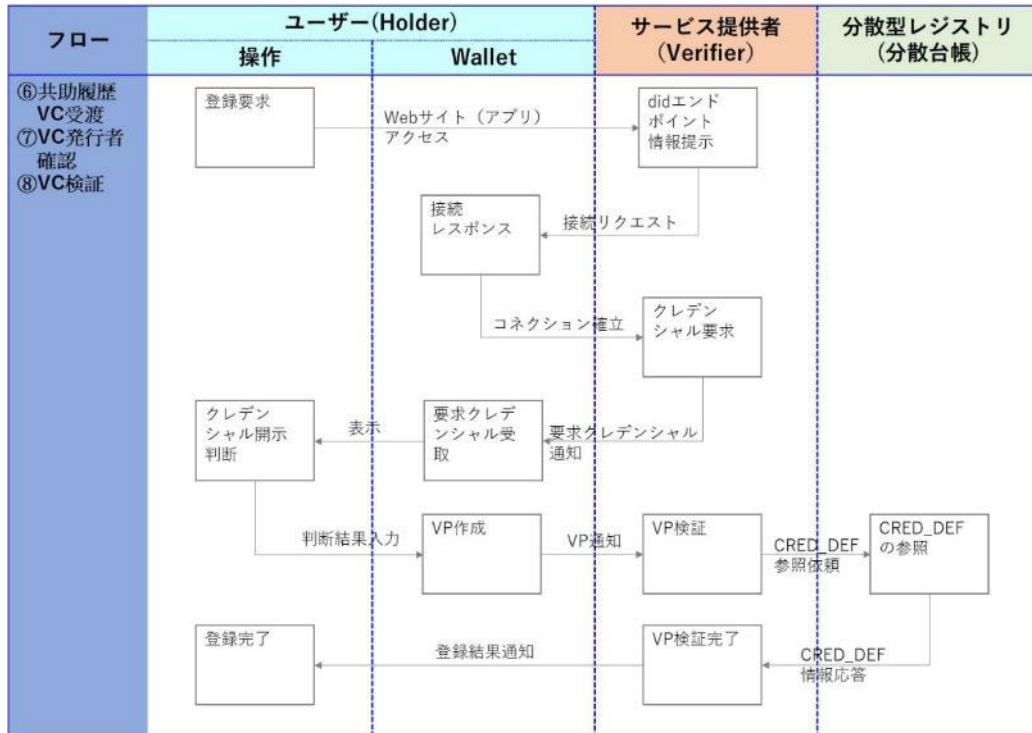


図 3.4.1.4 共助履歴 VC 受渡フロー、VC 発行者確認フロー、VC 検証フロー

スキーマの登録（スキーマパブリッシャ）

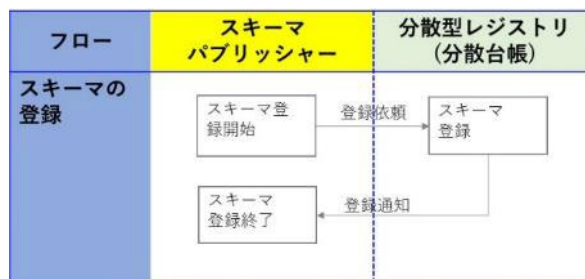


図 3.4.1.5 スキーマの登録（スキーマパブリッシャ）



### 3.4.2 ユースケース図

・共助アプリ間の実績共有

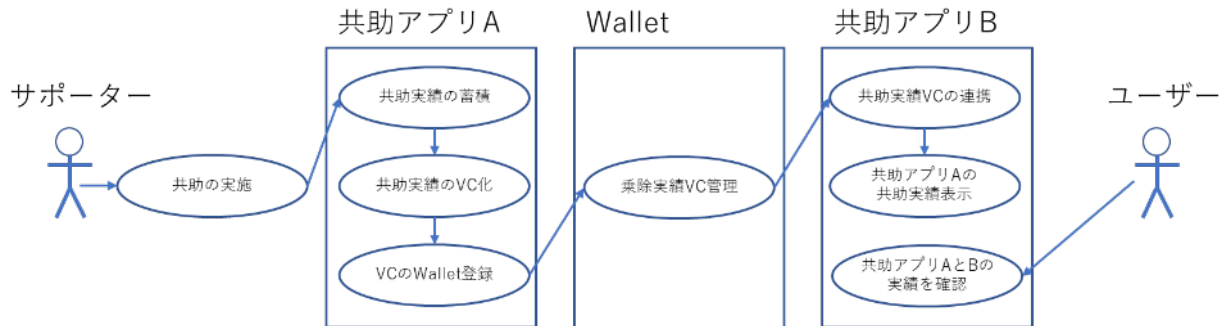


図 3.4.1 共助アプリの実績共有のユースケース図

### 3.4.3 操作画面 (UI)



### 3.4.4 機能一覧/非機能一覧

表 2.2.4 機能/非機能一覧

機能/非機能	機能名	機能概要
機能	[Holder]VC の変換	Holder は VC を VP に変換することができる。
機能	[Holder]Credential 公開設定	Holder は公開する credential の属性や期間を制限できる。
機能	[Holder]VC の Wallet 保存	Holder は Issuer から発行された VC を credential repositories (例:Wallet) に保存できる。

機能/非機能	機能名	機能概要
機能	[Holder]Credential 選択開示	Holder は Verifier に送る credential を選択できる。
機能	[Holder]Credential の検索	Holder が管理する credential から主張したい属性情報を検索することができる。
機能	[Issuer]VC 発行	Issuer はゼロ知識証明への利用、有効期限設定、更新処理、失効処理が可能な VC を発行することができる。
機能	[Issuer]Credential の取消	Issuer はその Credential を取り消すことができる
機能	[Issuer]Holder 正当 性の検証	Issuer は Holder の情報が正当であるか検証できる。
機能	[Issuer]失効理由の 開示	Issuer は失効理由を開示することができる。
機能	[Verifier]VP 検証	Verifier は Holder が提示した VP に対して真正性や Credential の検証ができる。
機能	[Verifier]Issuer 検 証	Verifier は Issuer の身元を発見し、信頼することができる。
機能	[Verifier]VC 検証必 要事項の要求	Verifier は Holder に検証に必要な Credential を最小限の範囲で要求することができる。
機能	[Verifier]真偽確認	Verifier は Predicate ができる。
機能	[Verifier]サービス利用 許可	Verifier は VC の検証が終了すると Holder にサービスを利用できる権限を付与できる。
機能	credential repositories の管理	credential repositories の中の VC は Holder の管理 下でセキュアに保存することができる。
機能	credential repositories の選択	credential repositories が選択できる。
機能	VC の credential repositories の移動	VC は Holder の credential repositories から任意のエ ンティティに credential repositories に移動することができ る。
機能	Schema 登録・削除	(第三者機関、Issuer など) 特定の Schema を登録・ 削除できる。
機能	DID Document 登録	DID Document を登録することができる。
機能	Revocation Registry 生成	Revocation Registry が生成される。
機能	Public DID の登録	Issuer の Public DID を登録できる。

機能/非機能	機能名	機能概要
機能	credential definision の登録	credential definision を登録できる。
機能	UA 連携	任意の UA と対話することができる。
機能	通信セキュリティ	Mediator 間でセキュアな通信路を生成することができる。
機能	Resolver の利用	対応する resolver を利用することができる。
機能	様々な手段による情報 入手	QR コードの読み取りや URL の受け取り、情報を入手することができる。
機能	DID の生成	対応する DID method の DID を生成することができる。
機能	DID の DID Document 解決	対応する DID method を利用して DID から DID Document を解決できる。
非機能	VC、VP 生成・検証	VC、VP の生成・検証に要する時間
非機能	VDR 登録	VDR の登録に要する時間
非機能	VC 検索	ユーザーWallet 内で VC の検索に要する時間
非機能	Wallet データ保存容 量	Wallet に保存できる VC の容量
非機能	VDR データ保存容量	VDR に保存できるデータ容量
非機能	IPFS データ保存容量	IPFS に保存できるデータ容量
非機能	データ通信容量	VC, VP を送付する際のデータ容量

### 3.4.5 データモデル定義(VC データモデルを採用する場合)

表 3.5.5.X データモデル定義

属性値	属性取得元	属性値 (vc 内)
ユーザー/サポーターDID	holder	UserId
KYC 情報	holder	KYCInfo
保有資格/検定情報	holder	license
発行元 DID	issuer	issuerId
発行者	issuer	issuer
サービス(アプリ)名称	issuer	serviceName
サービス属性	issuer	serviceProperty
サービス ID	issuer	objectId
共助実績(回数)	issuer	achievement
評価ポイント(ave.)	issuer	ratingAve
共助実施日時	issuer	assistanceDate
ユーザ属性	issuer	userProperty
共助内容	issuer	description
評価ポイント	issuer	rating
発行日	issuer	issuanceDate
有効期限	issuer	expirationDate

### 3.4.6 実験環境

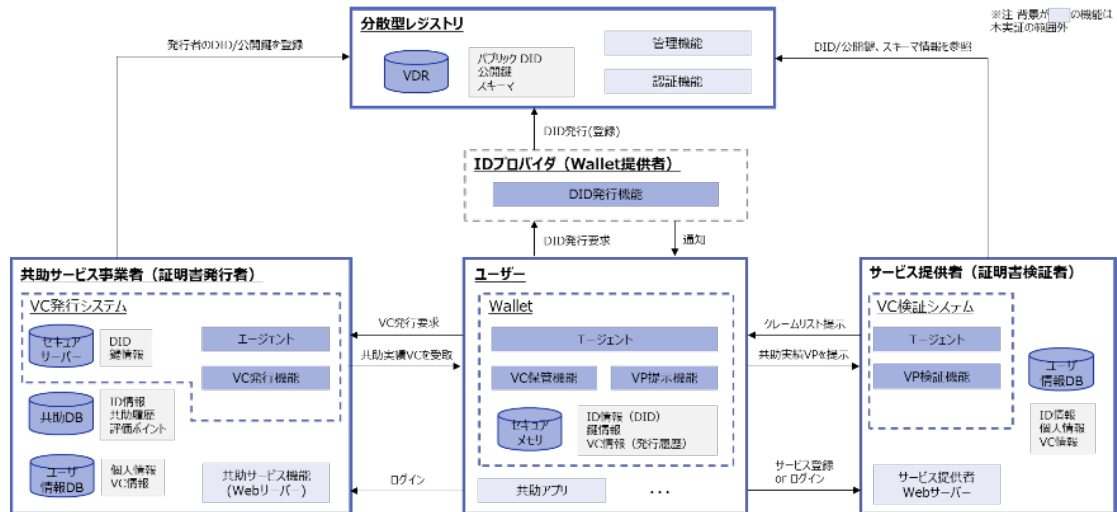


図 2.2.6. 実験環境

### 3.4.7 システムの構成要素

表 2.2.7 主要な製品・ライブラリー一覧

コンポーネント名称	型式 (製品の場合)	OSS か否か	ライセンス
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.

DID/VC の仕様については国際標準 : W3C/DIF に準拠して構築。

## 3.5 実証を通じて得られた主な成果

### 3.5.1 システムの企画・開発に関する実証内容・得られた主な成果

A:セキュリティ面での懸念事項の洗い出し

B:ユーザーの秘密鍵リカバリー方法についての検討

- A については、セキュリティ面での懸念事項を洗い出し、それぞれガバナンスと技術の面から対策を検討して表にまとめた。オレンジ網掛けの部分が特に重要と思われる項目。

## ①セキュリティ面での懸念事項（VC 関連）

懸念事項		対策		
項目	内容	ガバナンス	技術	備考
Cryptography スイートとライブラリ	安全が低下したCryptography スイートやライブラリを簡単にアップグレードし、既存のクレデンシャルを無効にすることが可能にする必要がある。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス 最新のバージョンを利用しているか監査。</li> <li>■技術 機能を無効にする。</li> </ul>
VCの外部にリンクされたコンテンツ	改ざんされる恐れが高いため、慎重に取り扱う必要がある。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス VCの設計ルールで守る。</li> <li>■技術 外部コンテンツが必要な場合はハッシュ化するなど対策を行う。</li> </ul>
Verifierの信頼性	Verifierと対話するときは安全な通信路でかつ相手の正当な相手であることを確認する必要がある。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス Verifierの認定。</li> <li>■技術 DIDComなどを利用する。</li> </ul>
Issuerの信頼性	Issuerと対話するときは安全な通信路でかつ相手の正当な相手であることを確認する必要がある。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス Issuerの認定。</li> <li>■技術 DIDComなどを利用する。</li> </ul>
VCの組み合わせの影響	悪意のあるHolderによって、複数のVCを組み合わせ虚偽のVPを作成する恐れがある。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス スキーマの登録の認定。</li> </ul>
VCの有効期限	有効期限の長いVCは、悪用可能なセキュリティの脆弱性を生む可能性がある。また短すぎる期限もHolderやVerifierに負担をかけてしまうため、有効期限を適切に設定する必要がある。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス 適切な有効期限の設定。</li> </ul>
デバイスの紛失や盗難	VCが保存されたデバイスを紛失または盗難された場合、悪用される恐れがある。そのため生体認証や多要素認証などデバイスのセキュリティも考慮する必要がある。	○	○	<ul style="list-style-type: none"> <li>■技術 生体認証や多要素認証の導入。</li> </ul>
要求するClaimの最小化	Verifierは目的に必要とする最小限のデータを要求する必要がある。一方、Issuerは最小限のデータを提示できるようなクレデンシャルを生成する必要がある。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス Claimのルールの認定。</li> </ul>
HolderのVCの保管場所	HolderのVCが保管されているリポジトリのサービス条件やアップロードされる情報の内容を認識する必要がある。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス 保管するリポジトリのルールを通知する。</li> <li>■技術</li> </ul>
想定していないVerifierにVPを提示	Holderが誤って、間違ったVerifierにクレデンシャルを送信した場合でも、最悪の状況にならないような仕組みが必要。（トークン化など）	○	○	<ul style="list-style-type: none"> <li>■ガバナンス Verifierの認定。</li> <li>■技術</li> </ul>

## ②セキュリティ面での懸念事項（DID 関連）

懸念事項		対策		
項目	内容	ガバナンス	技術	備考
DID Resolverの選択	利用するDID ResolverやDID methodが正しいものなのか理解する必要がある。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス DID ResolverやDID methodの認定。</li> <li>■技術</li> </ul>
DIDおよびDID Documentの更新	不正な更新がないか監視または、元に戻すの能力を持っている必要がある。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス DIDおよびDID Documentの更新の制限。</li> <li>■技術 不正な更新を監視、通知する仕組み。</li> </ul>
DIDおよびDID Documentの不正な更新があった通知	不正な更新があった場合、DID Subjectに積極的に通知をする必要がある。	○	○	<ul style="list-style-type: none"> <li>■技術 不正の監視、通知をする仕組み。</li> </ul>
鍵や署名の有効期限	要求側は有効期限が切れていないことを検証する必要がある。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス 適切な有効期限の設定。</li> <li>■技術 有効期限切れの検証・破棄。</li> </ul>
DIDの管理者	DIDが意図した当事者の制御下にあることを定期的に確認することが必要。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス</li> <li>■技術</li> </ul>
プライバシーリスク	分散台帳に登録されるなどDIDが公開されると、それと紐づいたVCに関連するデータと関連付けられる可能性があり、プライバシーリスクが高まる懸念がある。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス 罰則等の法整備、コミュニティでのルール作りが必要</li> <li>■技術 ユーザのdid(公開鍵)を台帳に登録しない方式の採用</li> </ul>
プライバシーリスク	複数のVerifier、IssuerとVerifier共謀し、VCに関連するデータを共有することでプライバシーリスクが高まる懸念がある。	○	○	<ul style="list-style-type: none"> <li>■ガバナンス 同上</li> </ul>

- B の秘密鍵のリカバリー対応は、セキュリティ、プライバシー、アクセシビリティの間のトレードオフを伴う。ID-ideal の調査により下記の方向性が示唆された。方向性 2、3 については一定程度の制度整備が必要であると考えられる。

#### 1.セルフサービスによるリカバリー

バックアップのフレーズやシードを使用して新しい秘密鍵を生成する機能など、ユーザーにセルフサービスの復旧オプションを提供することができる。この方法は、ユーザーが自分のデジタルアイデンティティをよりコントロールできるようになるが、セキュリティやアクセシビリティの面で問題が生じる可能性もある。

#### 2.集中的なりカバリー

デジタル ID プロバイダーなど、秘密鍵を管理する企業は、集中的な回復オプションを提供することが可能。これには、政府発行の ID やその他の検証可能な情報を使用して秘密鍵を復元する機能が含まれる。このアプローチは、信頼とセキュリティのレベルを提供するが、プライバシーの面では問題が生じる可能性もある。

#### 3.信頼できる第三者によるリカバリー

政府は、秘密鍵の管理を、安全なデジタル資産の管理経験と専門知識を持つ銀行などの第三者保管機関に委託することを義務付けることができる。この方法は、信頼と安全性のレベルを提供するが、アクセシビリティの点で問題が生じる可能性がある。

#### 4.リカバリー不可

場合によっては、秘密鍵の復元を一切行わないという選択肢もあり得る。この方法は最高レベルのセキュリティを提供するが、アクセシビリティの点で問題が生じる可能性があり、最後の手段として検討されることがある。

### 3.5.2 ビジネスモデルに関する実証内容・得られた成果

共助アプリ事業者のニーズ調査の結果、共助アプリのサービスの発展において、下記 4 点の課題があることがわかった。共助アプリのトラストエコシステム形成によって、特に「**安全性：コスト最低限で安全性を提供できる**」「**利用継続：共助実績データの活用でインセンティブを提供できる**」の解決に寄与でき、価値が高いと評価を受けた。

- サービス発展における課題と現状策

1. 安全性：ユーザー間の不安解消（安全性のスタンスと運用コスト）

現状：万が一の保険適用や推奨研修を通じた認定サポーター化、公的 ID での本人確認に

取り組んでいる

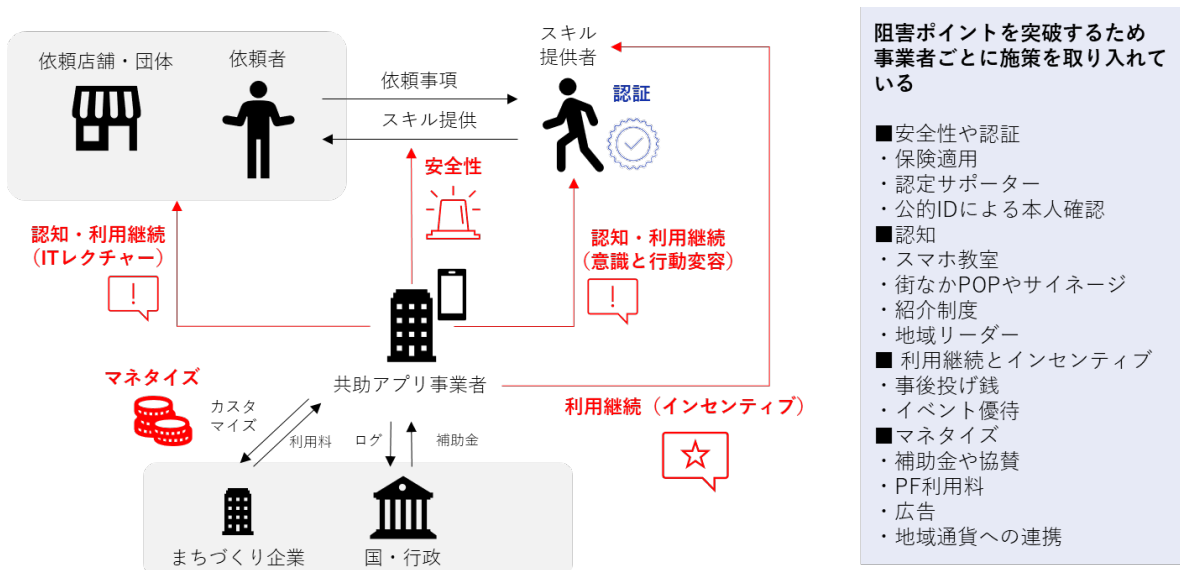
2. 認知：認知度が低く、サービス立上に時間を要す（ユーザー獲得へのコスト）
3. 利用継続（インセンティブ）：サポートユーザーへのインセンティブが不明瞭  
現状：ゲーム性の付与、イベント優待などの特別体験でインセンティブを提供している
4. マネタイズ：マネタイズポイントが小さい  
現状：保険サービスを付属することでユーザーから料金を徴収しているモデルはあるが、多くの共助アプリではユーザーから利用料を徴収していない。自治体からの利用料や広告費によるマネタイズが主。

● 「安全性：コスト最低限で安全性を提供できる」

- 本取り組みによって、安全性すべてを解決できるわけではないが、共助アプリ間でのトラスト共有によって、本人確認の負荷軽減の観点で、認証の課題解決が見込まれる。プライバシーを保護しながら、基本4情報では認証できない信頼性を証明できる。  
一方、安全性の対応の観点で、事業者—市民間での共助促進からサービス展開している事業者にとって、安全性の対応が容易にできることで、市民間での共助にもサービス展開できることが期待された。

● 「利用継続：共助実績データの活用でインセンティブを提供できる」

- 外的動機づけには原資が必要で新たなコストと負荷がかかったり、達成感やランキング・他者承認など内的動機づけでは一定のユーザー層を超えないという課題から、共助実績がKYCのプラスアルファ情報として付与できることによって、サービス内でのユーザー自身のトラストが証明できたり、他の共助アプリやシェアリングサービスを利用するときにはじめからトラストを証明できたり、共助アプリを利用するモチベーションにつながるインセンティブとなる。





4つの視点で具体的な課題があり、デジタルトラスト形成により「市民同士のマッチング促進」「サービス事業者の信用を備えたサービス立上げ」「ユーザーへの内的動機づけの提供」「マネタイズへの突破口」への期待とニーズがありそうである。

<p><b>【安全性】</b> 不測事態への対応や相手への不信任</p> <ul style="list-style-type: none"> <li>●個人的な情報開示による身バレ・ストーカー被害への対応が難しい             <ul style="list-style-type: none"> <li>・データが組み合わされた時に個人が特定されないか</li> <li>・SNSの書き込みを確認できることで作れるトラストもあるが、一方でユーザーの身バレのリスクが高まる</li> </ul> </li> <li>●センシティブな行動（例：子供預かり、視覚障がい者の移動支援）マッチングに対しデジタルでの信頼保証ができない・信頼保証の運用負荷がかかっている             <ul style="list-style-type: none"> <li>・子供相手に趣味や相性などリアルな部分のトラストに重きを置いているため、データ化・可視化は難しい</li> </ul> </li> <li>●本人確認の運用コストと効果が合わない             <ul style="list-style-type: none"> <li>・プラットフォームとして個人情報なるべく持ちたくない</li> <li>・本人確認をしても安全・信頼を担保できるわけではない</li> <li>・KYC発行のコストが負担である</li> </ul> </li> <li>●マッチング時の不測事態の対応コスト/最適な方法がわからない             <ul style="list-style-type: none"> <li>・保険提供で回避している…</li> <li>・市民同士のマッチングにも取り組んでいきたいが今は事業者と市民間である</li> </ul> </li> </ul>	<p><b>【認知拡大】</b> 利用者のITリテラシー(高齢者など)や必要性の意識醸成、ユーザー獲得のための広告販促</p> <ul style="list-style-type: none"> <li>●ユーザー登録時に「登録する情報量」のUXとインセンティブと信頼担保のバランスが難しい             <ul style="list-style-type: none"> <li>・登録の時に本人確認情報以外に、どのような情報があるとユーザーの安心になるか</li> <li>・JPKIの利用は自治体から求められるケースもある</li> <li>・JPKIを利用した際に住所情報と利用する地域情報をかけ合わせて、新たなサービスの提供が可能になるかも</li> </ul> </li> <li>●ユーザー登録情報の真正性確認ができない・確認しようとするユーザーの登録負荷が発生する             <ul style="list-style-type: none"> <li>・登録した情報の確かさを確認できない</li> <li>・ユニバーサルマナー検定の登録は自己申告登録</li> </ul> </li> <li>●ユーザー登録の動機づけ・意識付けの普及が困難（普及コストがかかっている）             <ul style="list-style-type: none"> <li>他アプリの実績を連携させることにより、称号のようなものが付けられたり、飛び級でレベルアップできたりすると「これを付けたい」と思う人が増え、利用の動機となる可能性がある</li> </ul> </li> </ul>
<p><b>【マネタイズ】</b> 利用者と受益者が一致していない、消費が発生しないマッチングでの収益</p> <ul style="list-style-type: none"> <li>●マネタイズが「広告・利用料・補助金（マッチング手数料）」のパターンにとどまり継続性が心配</li> <li>●サービス提供者自身の信用を示すことが必要             <ul style="list-style-type: none"> <li>・共助アプリという視点で見た場合に、自助・共助・公助とあるが、どういう軸・理念に基づいて運営して共助と名乗っているのが判断のポイント</li> <li>・個人情報の取扱とか大丈夫？ってユーザーから思われる</li> </ul> </li> </ul>	<p><b>【利用継続とインセンティブ】</b> 内定もしくは外的動機づけによる、利用者継続やユーザー層の拡大</p> <ul style="list-style-type: none"> <li>●外的動機づけは原資がないと作りにくい・新たな運用負荷がかかる             <ul style="list-style-type: none"> <li>・原資確保が難しく、協力・協賛が基本になる</li> <li>・ユーザー規模が小さいサービスへの協賛や協力が困難</li> </ul> </li> <li>●「達成感やランキング、他者承認」頼りでは一定ユーザー層を超えない             <ul style="list-style-type: none"> <li>・興味関心が高い人のみ利用し、コミュニティ内での広がりに留まってしまう</li> </ul> </li> </ul>

図 3.5.2 共助アプリ事業者の課題とニーズ

### 3.5.3 共助トラストフレームワーク策定の実証内容・得られた主な成果

- A: 共助トラストフレームワークの項目洗い出し
- B: 共助トラストフレームワークを策定する意義
- C: 各ステークホルダーの役割の整理
- D: トラストフレームワーク策定に関する課題についての整理

➤ A については、GAIN Trust Framework、OIX Guide to Trust Frameworks for Smart Digital Identity を参考に項目を下記の通り整理。本実証においては、項目 1~4 について検討して課題を抽出した。項目 5~9 については今後引き続き検討予定。

1. 共助トラストフレームワークを策定する意義
2. 各ステークホルダーの主な役割と責任について
3. 原理・原則、トラストマーク
4. ユーザー体験の内容（Wallet の利用方法/UI の表示等）
5. 会員企業へのサービス（ユーザーアクセス、SLA 等）
6. 技術的な基礎知識
7. モニタリングとコンプライアンスの基礎
8. 法的規則（データ管理、記録保持等）
9. セキュリティと技術要件（スキーマ、トラストチェーン等）

- Bについては、下記の通り整理を行なった。

【共助トラストフレームワークを策定する意義】

共助トラストフレームワークは、共助アプリ（生活者同士のマッチングで社会課題を解決するアプリ）における生活者の属性情報を、他の人々や組織とより簡単に共有する方法を提供する。

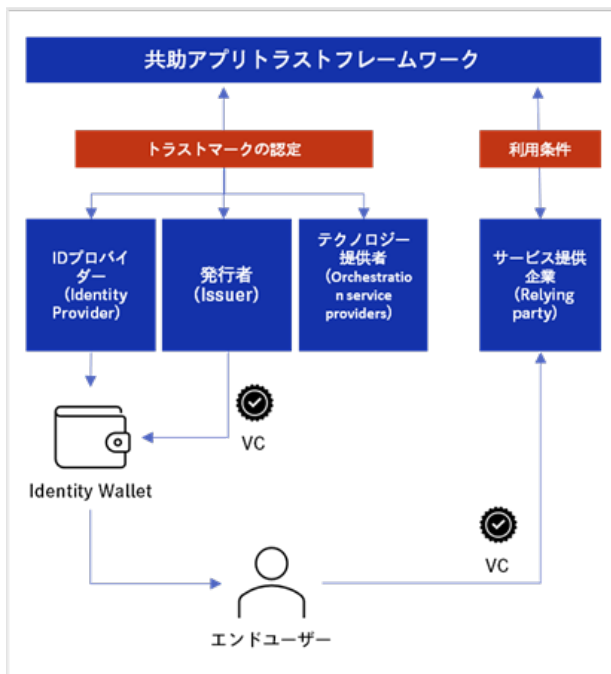
現状、共助アプリ同士で ID や属性情報を共有することは困難である。その原因の1つは、各共助アプリでデジタル ID や属性情報の作成方法がサイロ化されており、他の共助アプリで作成された属性情報が自分たちのニーズを満たしているかどうか信頼することができないことである。

共助トラストフレームワークは、様々な共助アプリが組織を横断して従うことに同意する一連のルールを指している。

このルールに従うことで、共助トラストフレームワークを使用するすべてのサービス及び組織は、生活者のデジタル ID と属性情報について統一のフォーマットで活用することができる。

その結果、共助アプリベンダーや生活者は、他の人々や組織と共助実績等の情報を検証可能なデータとして相互に共有することが容易になる。

- Cの各ステークホルダーの役割については、下記の通り整理を行なった。



役割	定義
エンドユーザー	共助アプリトラストフレームワークがマスアダプトするかどうかは、エンドユーザーの利便性に依存する。共助アプリエコシステムは、エンドユーザーが信頼できるIDプロバイダー、使いやすいインターフェース、および共助アプリに接続するシンプルなプロセスや相互運用性を保証する。
共助アプリトラストフレームワーク	トラストフレームワークには仕様、規則、協定が記載されている。共助アプリエコシステム内の他の役割がトラストフレームワークに準拠していることを示すことができる認証プロセス（トラストマーク認定）も含まれる。
IDプロバイダー	ユーザーが誰であり、何をやる資格があるかを証明するために、ユーザーがサービス提供企業に提示することができるデジタルIDを作成する。デジタルIDは、トラストフレームワークのルールに準拠していなければならない。本実証においては、VCを保持するためのウォレットのプロバイダ（共助アプリコンソーシアムを想定）がIDプロバイダとなる。
発行者	ユーザーが誰であるか、または何をやる資格があるかを証明する何らかの形のVCを発行する。これは、ID文書（マイナンバーカード、運転免許証など）の電子的発行、研修受講資格、共助アプリの活動履歴、ユーザーの年齢層（18歳以上など）の確認等が含まれる。
テクノロジー提供者	技術インフラを提供することで、トラストフレームワークの参加者間でデータを安全に共有できるようにする。
サービス提供企業	ユーザーがアクセスしたい商品やサービスを提供し、そのユーザーが誰であるか、または何をやる資格があるかについて、ある程度の信頼性を必要とする企業。

➤ Dについては大きく2つの課題が残ったため、今後の検討において議論を深めていく予定。

- トラストマークの発行基準について

どのような基準でトラストマークを発行するかを定めることが困難であった。各共助アプリでサービス内容や特徴が大きく異なるため、「共助アプリ」の定義自体にも議論の余地が生じ、本実証内での共助アプリベンダーとのディスカッションの中では統一の見解を出すことができなかった。この点については、今後シェアリングエコノミー協会とも議論しながら継続的な検討を実施する予定。

- 共助実績 VC に記載するデータと UI の表示方法について

各共助アプリで取得できているデータを整理し、共助実績 VC としてどのような情報を記載するかを議論した。取得しているデータの種別として、①資格・認定②行動③評判に分け、共助アプリごとに重視するトラストの種類が異なることも判明した。共助実績のデジタル証明書として、どのような内容の表示であればユーザーのトラスト向上に寄与するのか今後も継続的に議論していく予定。

## 4 実証終了後の社会実装に向けた見通し

### 4.1 社会実装時に想定しているビジネスモデル・ユーザーのメリット

現状の共助アプリの収益モデルは以下「3.5.2 ビジネスモデルに関する実証内容・得られた成果」の通り。

- ・行政からの補助金・企業協賛
- ・システム構築費用、システム利用料
- ・広告収益

認証に限っては、「eKYC 利用」「フェデレーション ID 利用」、事業者独自で運営する認定方法「研修・イベント」「身分証明書の確認」でコストをかけて実施している。

本取り組みにおいて、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事業者」がサービサーとなり、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。共助アプリ発行者および共助アプリ検証者が享受するベネフィットは、「共助アプリトラストフレームワーク」に準拠した信用を付与された証明書を発行または利用できることである。エンドユーザーが享受するベネフィットは、共助実績 VC の証明書を「デジタル ID ウォレット」に保管でき、必要に応じて共助アプリ検証者へ証明書を提示できることである。

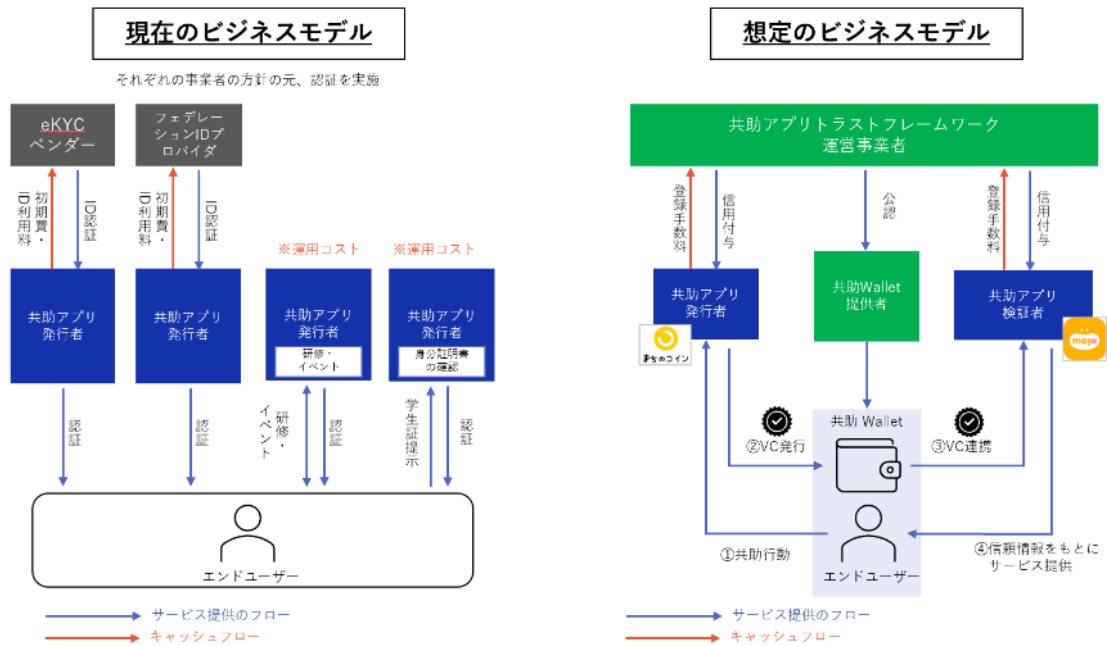


図 4.1.1 共助アプリトラストフレームワーク ビジネスモデル

また、このビジネスモデルが構築できると、既存ビジネスにない価値の創出が期待できる。

- マイクロインフルエンサーを活用した新たな広告：特定地域にて多くの共助実績を持つユーザーを地域での影響力・情報への信頼性が高いマイクロインフルエンサーとして認定。企業のマーケティング施策に起用する。
- 信憑性が高いクラウドファンドサービス：各共助アプリでの共助実績を持つユーザーがクラウドファンディングサイトで寄付を集める際に、信憑性の証明として共助実績を活用する。
- 個人の社会的信頼証明書発行：大学入試や就職・転職、バーチャル上でコミュニティ参画にて、ボランティア活動や課外活動など自身の共助実績を証明書として発行する。

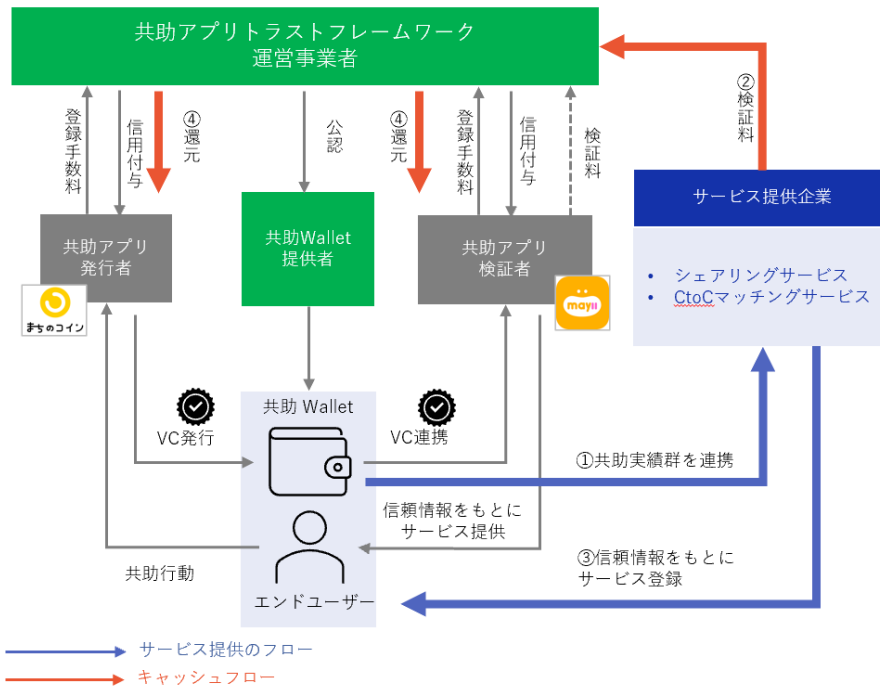


図 4.1.2 マイクロインフルエンサーを活用した新たな広告ビジネスモデル

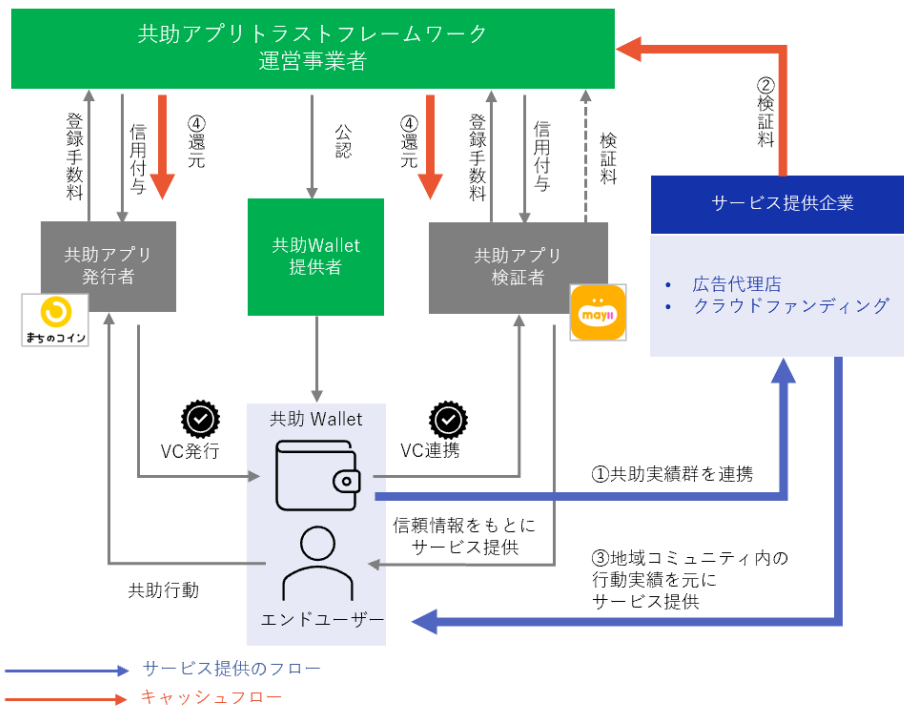


図 4.1.3 信憑性が高いクラウドファンドサービス

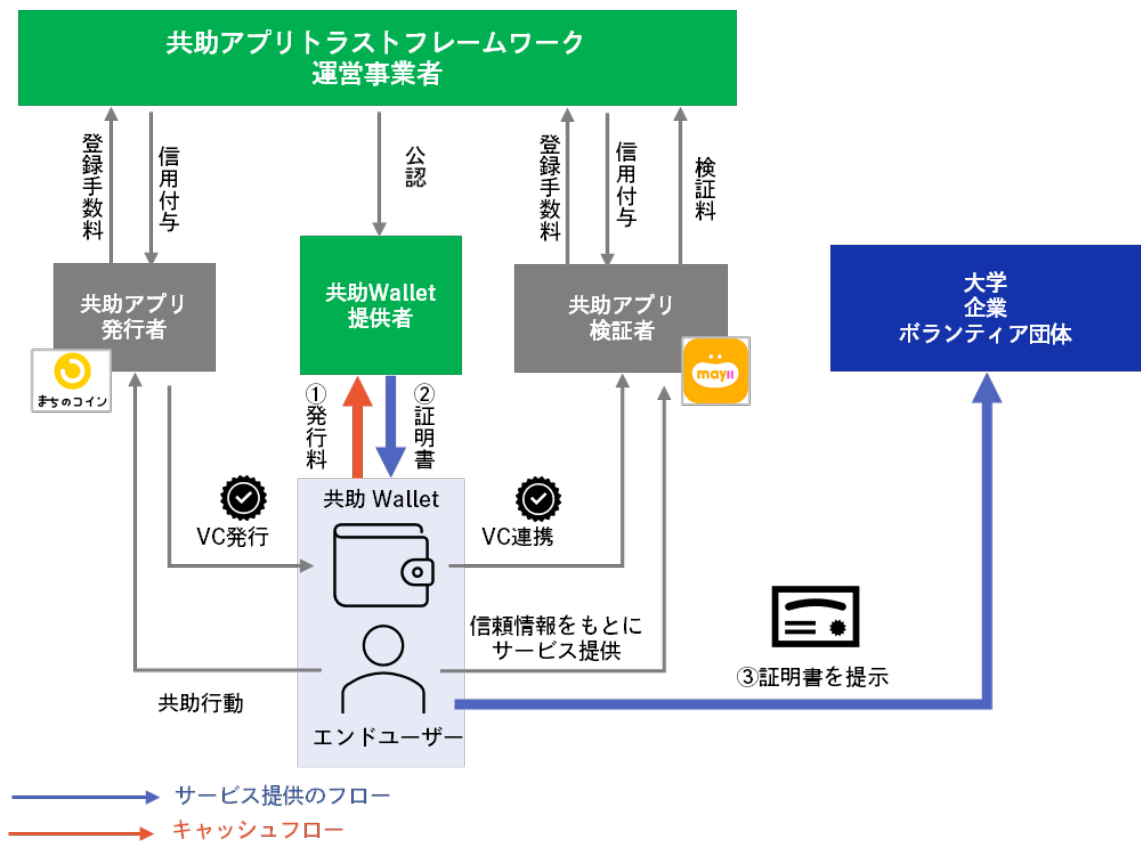


図 4.1.4 個人の社会的信頼証明書発行 ビジネスモデル

表 4.1 共助アプリトラストフレームワーク 各ステークホルダのベネフィット

ステークホルダ	ベネフィット	負担するコスト
エンドユーザー	個人の「行動」と「評判」に関する信用の証明書を保有できる	なし
共助アプリ発行者	共助アプリのユーザーのインセンティブとして証明書を発行できる	登録手数料
共助アプリ検証者	共助アプリのユーザーの安全性を向上できる 発行された証明書の真正性を検証することが容易になる	利用料

## 4.2 実証を通じて判明したユースケースの課題とその解決方針

共助アプリベンダー等へのヒアリングを通して本取り組みのニーズは確認できたものの、社会実装に向けては下記が課題になることが想定される。特に下記の課題③、④については公的機関によるサポートが必要と考える。

### 課題①トラストマークの認定（Issuerの信頼確認）

- 信頼できる共助アプリから発行された共助実績を蓄積することができるように、エコシステム運営主体による Issuer の認定が必要。現在すでに「シェアリングエコノミー認定制度」を実施するシェアリングエコノミー協会と協業しながら検討を進めていく予定。

### 課題②共助実績の表示方法（UI/UX）

- 一目で理解できるユーザーのトラストが向上する共助実績 VC の UI/UX が必要。共助アプリのジャンルごとに VC を集計・表示できる UI 等を検討する。また VC に記載するデータの種類も継続的に議論していく。

### 課題③Walletの秘密鍵、共助実績 VC のリカバリー方法

- 現状、Wallet の入った携帯電話を紛失した際のリカバリーが困難な状況。DNP が第三者機関として秘密鍵や VC を保管するか、ユーザーの自己責任で管理してもらうか等の検討が必要。

### 課題④エコシステム外への共助実績 VC の提示

- 共助実績 VC を蓄積した後、共助アプリのエコシステムの外でも活用することを目指していく想定。その際に現在検討している Wallet や VC の仕様で外部との相互運用性があるか不透明であり、実際に開発を行っていくリスクが大きい。

### 4.3 本ユースケースの社会実装に向けたマイルストーン

- ・ 本ビジネスモデルの社会実装については、令和 5 年度まで継続的な実証を行い、令和 6 年度以降の商用化を想定
- ・ 前述の課題①については、令和 5 年度上半旬まで関係者間の合意を行い、対応方針を決定することを予定
- ・ 令和 6 年度のサービス開始当初は、共助アプリ市場への展開を想定しているが、令和 7 年度以降は大学や企業の HR 業界をターゲットにマーケティングを行い、市場の拡大を目指す

	令和5年度	令和6年度	令和7年度	令和8年度
<b>社会実装に向けたスケジュール</b>	継続的な実証	商用化	エコシステムの拡大	
課題① 共助トラストフレームワークの策定	共助アプリコンソーシアムを設立し、ガバナンスルールについて合意・運用を行う			
課題② 共助実績VCの表示方法の設計	UI/UXの設計			
課題③ 秘密鍵・VCのリカバリーについて	リカバリー方法の検討			
課題④ 共助アプリ以外への共助実績の提示			大学や企業に対して共助実績をデジタル証明書として発行する	

図 4.3 社会実装に向けたマイルストーン



## 5 Trusted Webに関する考察

### 5.1 Trusted Web のアーキテクチャに関する課題と提言

- ・ 「分散型で検証可能な部分を広げる」という Trusted web の技術選択について、分かりやすく納得できるメリットの整理が必要。例えば、サービスイノベーションの観点での課題克服として、本実証においては、共助アプリを含むシェアリングサービスが現状 300 社以上存在し、それらの関連情報をつなぐ集中型のデータベース構築は実現生に乏しいため、分散型 ID 技術での実現を検討した。ステークホルダーが膨大となる、または将来的な拡張可能性が未知数の場合に、既存のシステムでは対応できないイノベーションの方法として分散型の仕組みが有効なのではないか。
- ・ 分散型 ID の活用を前提とした個人情報の法的保護についての検討も必要。現行の個人情報保護法は、サードパーティによる個人情報の取り扱いについては記載しているものの、VC のように生活者が直接管理することが想定される個人情報については想定されていない。課題が想定されるケースとして、例えばユーザーの DID が公開されると、それと紐づいた VC に関連するデータが名寄せされる可能性があり、プライバシーリスクが高まる懸念がある。このような生活者自身の判断で提示した VC に関しても、一定程度の法的保護が受けられるように、参照すべき個人情報保護法の条文等を議論すべきではないか。
- ・ 技術的な課題がクリアできたとしても、最終的に組織を横断してトラストデータを流通させるためには「トラストフレームワーク」の策定が重要になる。本実証では、GAIN や OIX のフレームワークを参照して共助アプリのためのガバナンスを策定したが、今後、日本において様々な業界別コンソーシアムが立ち上がることを想定して、共通の土台となる日本版のデジタル ID に関するトラストフレームワークが必要。海外で先行して構築されているフレームワークを参照しながら、日本の状況に合わせたトラストフレームワークの価値・構造を整理した枠組みを作るべきだと考える。

### 5.2 その他 Trusted Web の課題と提言

今後分散型 ID の仕組みを社会実装していくうえで、ルール化・ガイドライン策定等の政府の関与が必要だと思われる項目を記載した。

#### ■ Identity Wallet のインターオペラビリティについてのルール

- ドイツの ID-ideal の事例においては、Wallet が乱立することによるユーザービリティの低下（相互運用ができていない）とセキュリティの懸念が課題となっていた。今後、日本においても同様の課題が出てくるのが想定されるため、Wallet の適正普及・適正利用のための枠組みを政府も含めて検討いただきたい。

#### ■ ユーザー-Wallet の秘密鍵管理について

- ユーザー-Wallet の秘密鍵の管理については、「自己責任原則」と「適合性原則」のバランスの観点からルールづくりを検討することが重要である。
- ユーザーがデバイスを紛失した場合などのリカバリー対応策として、企業がユーザーの秘密鍵を管理するケースが想定される。アイデンティティ管理における秘密鍵は、流出すれば第三者が当人になりすましてきてしまうため、消費者保護の観点から、高いセキュリティによって守られる必要がある。暗号資産のように、ユーザーの秘密鍵の取り扱いができる業者を限定することも視野に入れながら、認証・セキュリティの観点で安心できるガバナンスのルール作りが必要だと考える。
- また一般の生活者にとっては秘密鍵管理について十分に理解が浸透していない状況であり、リカバリー対応や鍵の流出等でトラブルが起きることも想定されるため、ユーザーリテラシーの強化のためにも教育コンテンツの情報発信を積極的に行なっていくべきである。

#### ■ オープンコミュニティの形成

- 現状は Trusted web の社会実装について、それぞれの企業がバラバラに方法を検討している。今後 Trusted web を実現するために様々な企業が意見交換をすることができるオープンコミュニティがあると、相互運用性を見据えた実装の構想も進んでいくのではないかと。