

Trusted Web の実現に向けたユースケース実証事業 成果報告書

[中小法人・個人事業者を対象とする補助金・給付金の
電子申請における「本人確認・実在証明」の新しい仕組み]

2023年03月24日（提出日）

代表機関：株式会社電通

[電通・ISID パブリック DX コンソーシアム]

目次

1	背景と目的	1
2	事業の概要	1
2.1	事業概要及び実証の範囲	1
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	6
2.4	実証全体のスケジュール	8
3	実証内容	9
3.1	実証の実施事項、論点及び判断	9
3.1.1	プラットフォームに関する実施計画書からの変更点	9
3.1.2	プロトタイプ of 企画・開発	11
3.1.3	ヒアリングの実施	13
3.1.4	国際標準規格の調査	23
3.2	検証できる領域を拡大する仕組み	24
3.2.1	データフロー	24
3.2.2	データフローに登場する主体とその概要	25
3.2.3	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
3.2.4	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	28
3.3	6 構成要素との対応	29
3.3.1	検証可能なデータ	29
3.3.2	アイデンティティ	29
3.3.3	ノード	30
3.3.4	メッセージ	31
3.3.5	トランザクション	32
3.3.6	トランスポート	32
3.4	本実証で企画・開発したシステムの概要	32
3.4.1	業務フロー	32
3.4.2	ユースケース図	33
3.4.3	操作画面 (UI)	33
3.4.4	機能一覧/非機能一覧	34
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	37
3.4.7	システムの構成要素	38
3.5	実証を通じて得られた主な成果	39

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	39
3.5.2	ビジネスモデルに関する実証内容・得られた成果	39
3.6	本実証で開発したシステムの第三者による再現可能性（A 類型のみ）	41
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	43
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	45
5	Trusted Web に関する考察	47
5.1	Trusted Web のアーキテクチャに関する課題と提言	47
5.2	その他 Trusted Web の課題と提言	47

1 背景と目的

<背景>

長年に渡り、当社グループにおいて、中小法人・個人事業者向けの補助金・給付金事務局（以下、「事務局」という）を多数担ってきた中で、「永遠の課題」とも言えるのが、申請者の「本人確認と実在証明」であり、前述のとおり、中小法人・個人事業者の把握・捕捉のしづらさが、補助事業者等による不正や、その確認行為に伴う事務局の審査コストの増加、そして、煩雑な申請手続きにつながっている。

これまで、補助金等を申請するすべての中小法人・個人事業者は、あらゆる申請ごとにその都度同じような必要書類（登記簿や納税証明書等）を事務局に提出し、事務局での審査において、その「本人確認と実在証明」を見てきたが、そういった審査を行ったとしても、事業者ごとに全数現地検査を実施できるわけではないため、本人確認と実在証明の精度は十分とは言えない。

他方で、100%電子申請・電子業務を行っている I T 導入補助金においては、gBizID や法人番号公表サイトとの連携等により、「本人確認と実在証明」をシステムによって自動化し活用しているが、gBizID 取得時に、印鑑証明の提出や SMS 受信による認証等が必要となり、郵送による手続きに二週間程度の時間を要することに加えて、多くの補助金では申請時に事業継続性の確認等で納税証明書、確定申告書の控を提出する必要があり、申請者側の当初コストはむしろ増大していると言える。

持続化給付金に代表されるような、緊急性を要する大規模給付金や補助金の場合、gBizID 発行の審査・発行にかかる期間、短期間での大量発行などの運営体制の整備、申請に必要な印鑑証明書等のエビデンスの準備、事業者自体のリテラシーなどを考慮すると、gBizID 取得前提の運用は極めてハードルが高く、事実上対応は不可能であると考えられる。そのような課題感に対して、Trusted Web を根本的な課題解決に導く手法として活用できるのではないかと考えるに至った。

<目的>

これまで Trusted Web 推進協議会で行われてきた検討内容を活かしつつ、多数の補助金・給付金事業等の事務局運営で培った実践ノウハウや課題認識を組み合わせ、プロトタイプシステムの開発を通じて、補助金・給付金事業における Trusted Web 関連技術の社会実装の方向性を明らかにすることを目的とする。上記を行うことで、補助金・給付金等の公的支援が、必要とする中小法人・個人事業者に適切かつ迅速に到達する手法の確立と、本ユースケースを足掛かりに、その他の公的手続き等にも寄与する仕組みづくりを目指している。

2 事業の概要

2.1 事業概要及び実証の範囲

<追加・修正に関しては、記載内容検討中>

事業スキーム

補助金・給付金事業においては、申請者は各種情報を証明者から入手して申請先に提出し、申請先

はそれらの情報を確認・審査した上で、適切に補助金・給付金の支払いを行う、という流れになっている。本ユースケースにおいては、申請者から申請先に提出される情報について、検証可能な領域を広げるために、VC を活用し、情報の信頼性を担保することで、申請者の「本人確認と実在証明」を行う。創出するユースケースの事業スキームは下記の通りである。

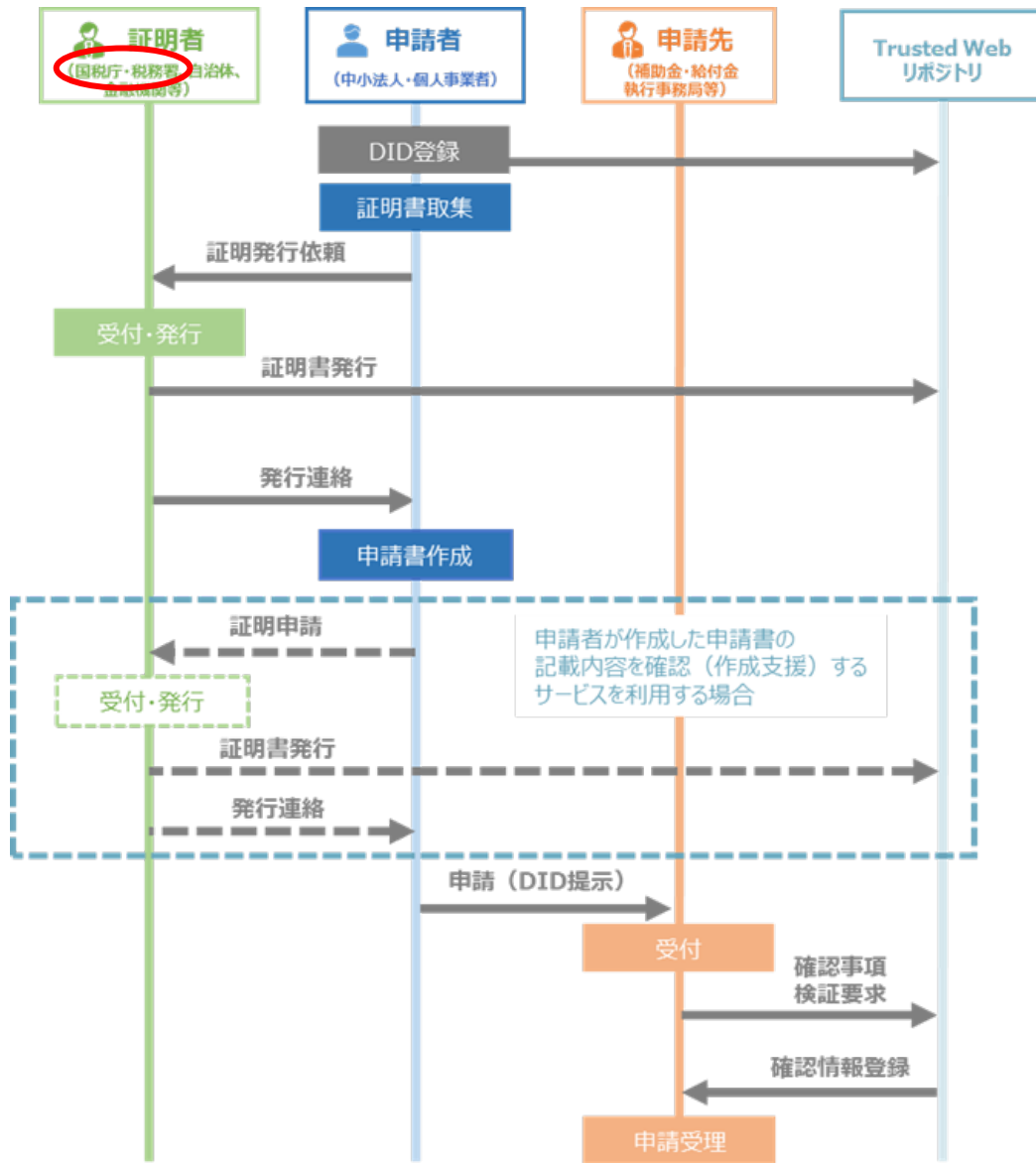


図 2.1 本ユースケースにおける事業スキーム

表 2.1 事業スキームに登場する主体とその概要

主体	設定・役割
<p>申請者 (中小法人・個人事業者)</p>	<p>設定： 補助金・給付金の申請者。申請に際し、申請に必要な証明書の収集と申請書の作成を行う。</p> <p>役割： 申請に必要な各種証明を取得するため、申請者から証明者に VC (Verifiable Credential：検証可能属性証明) 発行依頼をする。申請者は必要に応じて、申請書類の作成支援や申請書類の記載内容の証明を証明者から受けて、申請先に提出する。</p>
<p>証明者 (国、自治体、金融機関、国の認定を受けた機関等)</p>	<p>設定： 申請者からの依頼で、申請者の情報を確認・審査し VC を発行する。申請情報の信頼性を証明するために、証明者が公的機関以外の民間企業の場合は、証明者自体が国もしくは第三者機関等の団体による認証を受ける必要がある。</p> <p>証明者は、単に申請情報を確認・検証するだけでなく、計画書等の作成におけるコンサルティングなどの付随サービスを提供する可能性がある。付随サービスについては本実証外とするが、付随サービス提供者の役割を明確化することで補助金・給付金に関わるサービスと対価を整理できる可能性がある。</p> <p>役割： 申請者から受け取った情報について確認・審査を行い、証明者の VC と共に Trusted Web リポジトリ (repository：データの保管場所) に登録する。</p>
<p>申請先 (補助金・給付金事務局)</p>	<p>設定： 補助金・給付金の事務局。申請情報を受け取り、審査する。補助金・給付金が、適切かつ迅速に申請者に届くようにする。</p> <p>役割： Trusted Web リポジトリから情報を取得し、証明者の VC を検証して申請者の申請情報を審査する。そして補助金・給付金の給付の実施結果をリポジトリに登録する。</p>
<p>国 (補助金・給付金)</p>	<p>設定： 政策目標を達成するため補助金・給付金給付事業の趣旨に合致する事業</p>

主体	設定・役割
事業主体)	者を公募して選定し、事業の実行に係る費用を支払う。 補助金・給付金が、適切な事業者により速やかに給付されることを目的として、事業の運営を補助金・給付金事務局に委託する。

表 2.1-2 Trusted Web で解決し得る課題

課題の対象	解決すべき課題	Trusted Web システムによって解決できること
申請者	・ 申請のために、自身の証明や自身の情報の証明を行う必要がある	実在証明等の自身の情報を証明するプロセスを簡素化し、申請にかかる手間を削減することが可能。
	・ 申請した情報が不正利用されるリスクがある	自らの情報の開示範囲やアクセスをコントロールすることで、自身の情報管理を主体的に行うことが可能。 また、自身の情報の不正利用など、合意した範囲以外への情報提供を防ぐことが可能。
	・ 一度申請に用いた情報を再利用することができない	証明者が署名した情報を申請者が再利用することで、申請にかかる手間を削減することが可能。 また、自身が合意した範囲でのみ適切に情報の管理が可能となるため、申請者自身の意思で、自身の情報の利活用（他の申請時の情報活用、国側からの補助金の斡旋など）が可能。
	・ 自身の証明を行う作業が電子化されていないものについては、窓口訪問や、窓口営業時間内に、証明に伴う申請作業等を行う必要がある	自身の証明を行うためのプロセスを完全に電子化することで、時間にとらわれず手続きを行うことが可能。また、紙など紛失の可能性があるものを持つ必要がないため、情報流出の危険性を低下させることも可能。
	・ 申請者自身が作成する申請書など、公的機関からの証明が受けられない文書の信頼性の担保ができない	中小企業診断士等の有資格者や、国からの「お墨付き」を得た企業・個人を証明者として補助金における VC の発行元とすることで、当該申請書に記載された情報に関して信頼性を担保する。 申請を受け付けた事務局側も証明者から信頼を受けた情報として VC を活用し、一部情報の審査プロセスを簡素化することが可能。

課題の対象	解決すべき課題	Trusted Web システムによって解決できること
申請先 (補助金執行 団体/事務局)	・ 申請書に記載された情報の信頼性を確認する必要がある	証明者が署名した情報を利用することで、実在証明や申請書に記載された情報を信頼し、審査にかかるプロセスを短縮し、コスト削減が可能。
	・ 補助金・給付金業務が複雑であり、審査に時間を要する	給付（支払）における作業を Trusted Web 利用前提のシステムに標準化することで、統一化されていない国/都道府県/市区町村の事務作業の共通化も推進され、コスト削減を行うことが可能。
	・ 申請情報の確認作業、事務処理等により補助金・給付金の支払いに時間を要する	不正申請の発見・確認が容易になることや、各種本人情報の確認が Trusted Web により簡素化されることで、申請から補助金・給付金支払までのリードタイムを短縮。
	・ 申請された情報の活用ができない (申請情報の再利用)	申請者自身が自らの情報を管理できるため、申請者と情報の利用範囲を合意することで、申請情報の再利用による、申請者に恩恵のあるサービスを提供することが可能となる。(申請情報を再利用し、申請事務手続きの負荷軽減や、申請された情報から他の補助金を紹介するなど)
	・ 申請情報についての申請者への問合せや、記載内容についての申請者からの問合せなど、問合せ対応に要する負担が大きい	申請者側は、申請に必要な情報を VC として証明者から信頼を受けた形で申請するため、申請情報の不備が発生する可能性を極小化することが可能。また、事務局側は、VC により検証可能な情報のみを取り扱うこととなるため、申請者側への問い合わせ業務も極小化することが可能。これにより、問い合わせ対応における事務作業時間は大きく削減される。
証明者	・ 申請者を証明する書類は紙が多く、また窓口対応が必要な業務が多いため、事務作業や印刷コスト等が多く発生する。	申請書類を完全に電子化することで、窓口での対応業務をなくし、事務作業のコストを減らすことが可能。また、証明書自体も電子化されることで、ペーパーレス化の推進を行い、証明書交付における費用を削減することが可能。
	・ 申請者が申請を行うたび、申請者を	申請者自身で、申請者の情報管理が可能であるため、申請者が合意することを前提に、過去申請に用いた情

課題の対象	解決すべき課題	Trusted Web システムによって解決できること
	証明書類の発行・証明書の発行を行う必要がある	報の再利用、や、申請書提出の省略をすることが可能。

2.2 社会・経済に与える価値・影響

1. 中小法人・個人事業者情報の横断的な情報管理の実現

申請者情報確認を Trusted Web の考え方にある検証可能性を高め、情報の自己コントロールを高める方式に統一することで、規定の証明方式によってその都度最新情報の確認が可能となる。また、どの機関でも統一して用いることができるため、今まで各機関の情報管理方法等が異なっていたことにより発生していた事業者情報の相違による差分確認等も、煩雑な手続きを介さず解消することが可能となる。

2. 証明書等のペーパーレス化

従来、データでの事業者情報の確認では、その事業者の確からしさの検証が課題となっており、あらゆる公的手続きにおいて、紙の証明書の添付、あるいはスキャンデータの添付が必要となっている。

本ユースケースのプロトタイプシステムを活用した社会が実現した場合、データ上で事業者の確からしさを確認することが可能となるため、公的証明書やその他認証団体等の認定証などについてもデータ上での本人確認が可能となり、様々な手続きのペーパーレス化に寄与できる。また、それは同時に各機関の事務処理費用の低減や事業者自身が証明書発行窓口に訪問し、発行手続きを行う手間や時間の大幅な削減にもつながる。

3. 民間企業（金融機関など含め）における活用

本プロトタイプシステムで検討する構造が民間企業にも普及することで、業界における事業者の属性を検証可能なデータとしてやり取りすることができるため、民間企業における連携がより円滑化し、より実態に即した精度の高いエビデンスを施策立案等に活用することができる。

また、金融機関における口座開設等の信頼性の評価が必要になるような場合においても、各機関から発行された VC を申請者が金融機関に提出することで、金融機関はより正確な調査を大きな負担なく行うことが可能となる。

2.3 コンソーシアムの体制

本コンソーシアムは、株式会社電通を代表者として、当該代表者と株式会社電通国際情報サービスにより構成される。株式会社電通は、実証全体の統括及び企画設計の役割を担う。株式会社電通国際情報サービスはプロトタイプシステムの企画・開発の役割を担う。

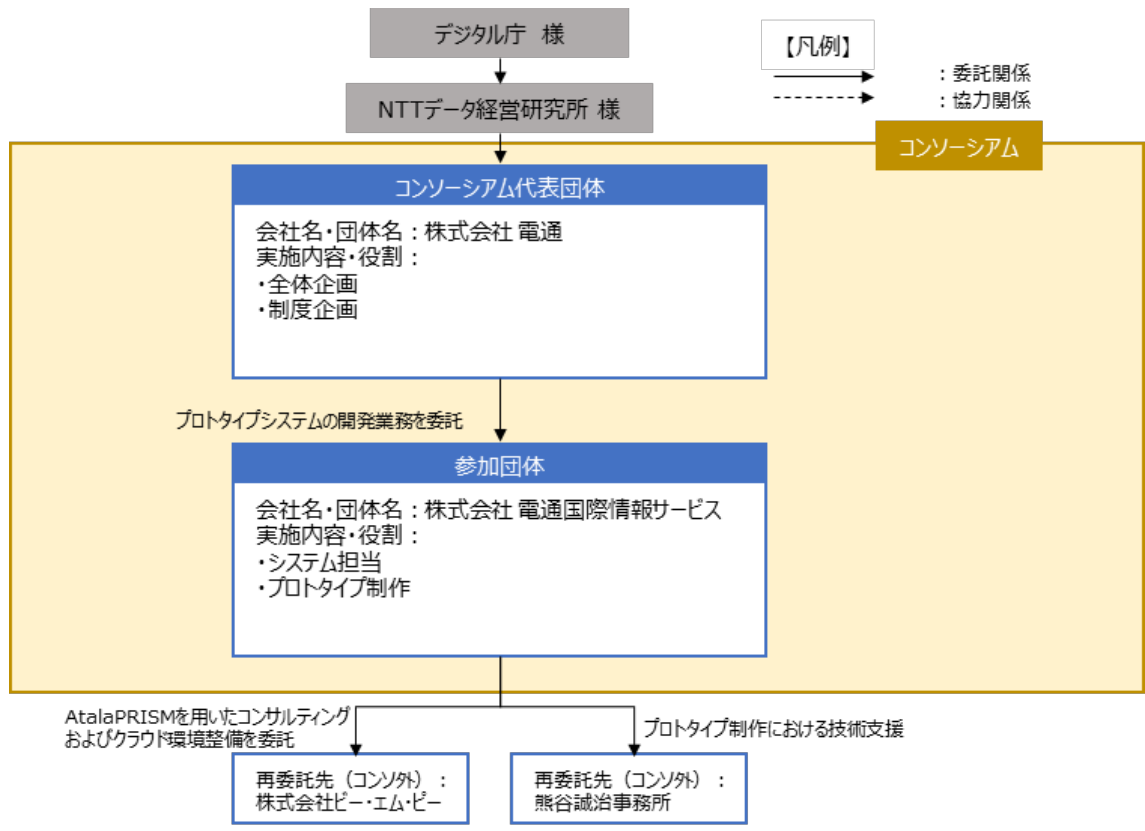


図 2.3 実施体制図

3 実証内容

3.1 実証の実施事項、論点及び判断

3.1.1 プラットフォームに関する実施計画書からの変更点

実施計画書においては、本事業で構築するプロトタイプシステムで採用するプラットフォームとしてパブリックブロックチェーン CARDANO ベースの AtalaPRISM を想定していた。

・実施計画書の記載内容（3-1-3 事業内容）

（採用するプラットフォームおよびサービスについて）

本実証事業にて構築するパブリックブロックチェーンのプラットフォームおよびサービスには

下記の理由から AtalaPRISM（アタラ プリズム）を採用する。

- ・ 政府機関における 500 万人規模の DID 発行、運用実績を有する（エチオピア）
- ・ AtalaPRISM を開発する IOG は、暗号資産総額において世界 8 位（ステーブルコインを除くと 4 位）のブロックチェーンである CARDANO の開発元であり、高い信頼性を有する
- ・ IOG は当社グループとも日常的に取引があり、開発の柔軟性が見込める

・実施計画書の記載内容（4-2 事業内容）

本実証においては、Input Output Global（IOG 社）が提供する DID/VC プラットフォームである AtalaPRISM を採用し、API を活用してプロトタイプシステムの開発を行う。AtalaPRISM の機能で実現できない箇所については、主にオープンソースを活用した開発を行い、開発箇所のソースコードを開示する。（表 3）オープンソースを適切に活用することで、第三者の再現可能性を担保するとともに、システム間連携や追加開発含めた柔軟な対応を行うことを可能にする。

また、本プロトタイプシステムは Docker コンテナを用いて環境構築を行い、Linux、Windows、OSX、AWS、GCP 等のあらゆる環境で動作可能とすることで、特定インフラへの環境依存を回避する。

2023 年 11 月度の定例報告会で、AtalaPRISM に加えて、「Algorand ベースのスクラッチ開発」の 2 パターンの検討を進めることとした。Algorand ベースのスクラッチ開発を追加した理由は、AtalaPRISM は製品であり、AtalaPRISM の仕様、及び、構成するコンポーネントやライブラリの情報開示が難しいと判明したためである。

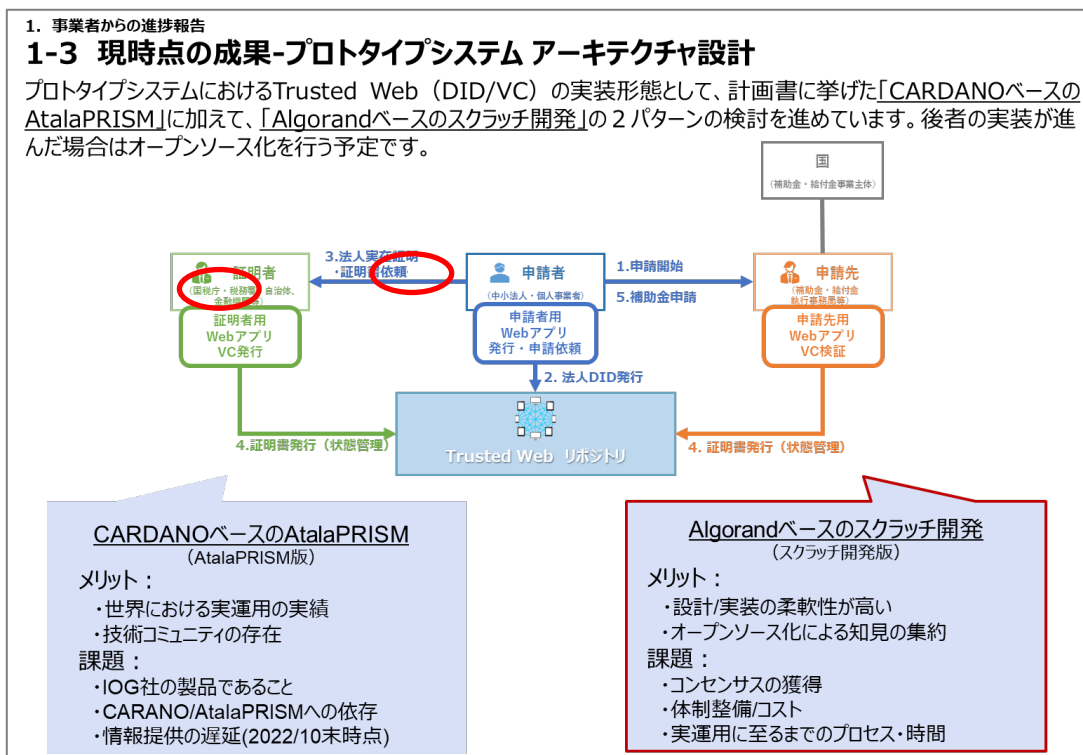


図 3.1.1 Trusted Web 定例報告資料より抜粋(2022年11月4日)

Algorand ベースのスクラッチ開発においては、Next.js¹の Static Site Generation² を利用してフロントエンドのみの開発にした。秘密鍵を暗号化してブラウザのローカルストレージに格納する仕組みにした。その際、XSS 対策³等のセキュリティを考慮し、react⁴のコンポーネントを利用することとした。メッセージの形式は、当初 JSON データに ed25519⁵署名を行っていた。

その後、2023年1月に委員からいただいた「新たなものを独自実装することにより内包するセキュリティリスク」のご指摘により、独自実装ではなく、JWT⁶(JSON Web Token)に対応する判断を行い、did-jwt⁷及び did-jwt-vc⁸を採用してプロトタイプシステムを開発することとした。

本件で実装するプロトタイプシステムは、メッセージの書込・参照にローカルストレージを用いており、メッセ

1 React ベースのフレームワークで、Server Side Rendering(SSR)や Static Site Generation(SSG)などの機能を提供している。

2 静的な HTML ファイルをビルドする手法。高速で安全な Web サイトを作ることができる

3 クロスサイトスクリプティング (XSS) 攻撃から Web ページを保護するためのセキュリティ対策

4 Facebook によって開発された JavaScript ライブラリ。UI コンポーネントの開発を支援し、コードの再利用性を高める

5 楕円曲線暗号化方式を用いた高速でセキュアなデジタル署名アルゴリズム

6 認証情報を安全かつ簡単に伝送するためのコンパクトな JSON オブジェクト

7 分散型 ID を使用して、認証、検証、署名などのデジタルアイデンティティ機能を提供する JWT ライブラリ

8 分散型 ID (DID) を使用して、検証可能なクレデンシャルを生成するための JWT ライブラリ

ージを暗号化してやり取りする仕様は実装していない。JWT ベースでノード同士がメッセージのやり取りを行うための仕組みとして、DIF⁹により仕様策定が進められている DIDComm¹⁰の採用を検討している。なお、本最終報告書において、通常の記述は本実証のプロトタイプシステムに関するものとし、本実証には含まない構想については、〈今後の検討〉 〈次の展開として〉 〈将来的には〉 等の文言を記載する。

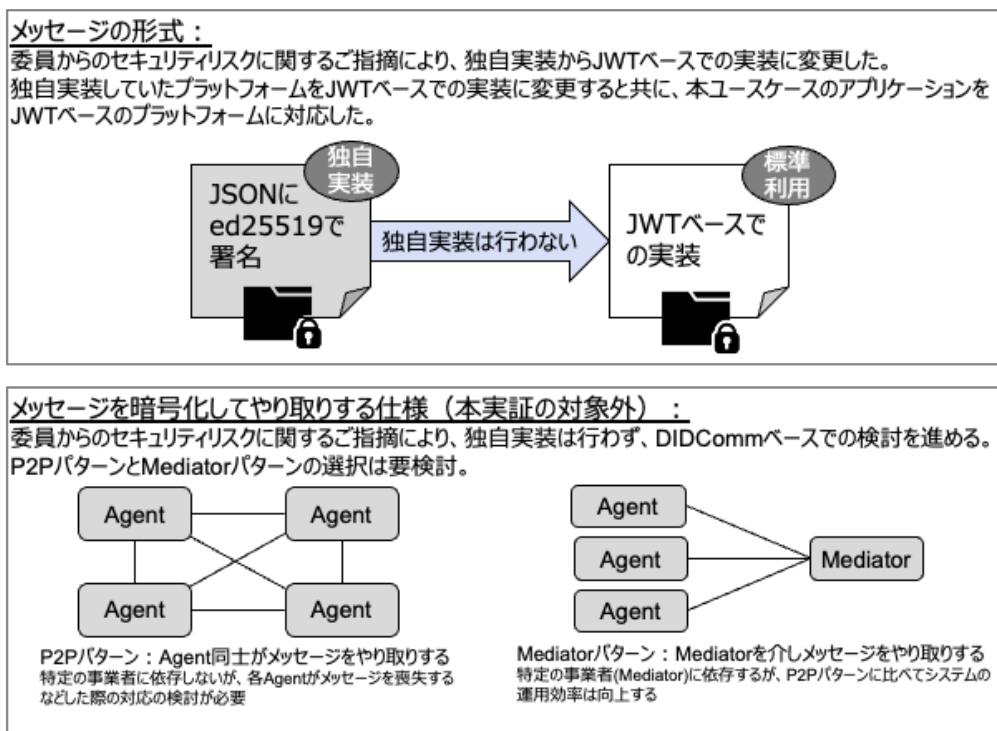


図 3.1.1 JWM¹¹の形式と JWM をやり取りする仕様における標準実装の活用

3.1.2 プロトタイプの企画・開発

(1) 要件定義

補助金・助成金事業の経験者およびそのシステム開発者との打ち合わせを実施し、「本人確認・実在確認」や「その他の認証方法」等において、Trusted Web の考え方の適用可能性と想定される方法について洗い出しを行った。論点となったのは申請手続き上で重要になる以下の4点。

- ・申請者による VC 発行依頼・管理方法
- ・本人確認、実在確認方法
- ・証明者による VC の発行方法と必要な要素
- ・発行済 VC の revoke ルート

⁹ 分散型 ID の標準化と促進に取り組むグローバルコミュニティ

¹⁰ 分散型 ID を使用して、暗号化、署名、認証などの機能を提供する分散型メッセージングプロトコル

¹¹ JSON Web Message の略称。安全にメッセージングを行うための JSON ベースのデータ交換フォーマット

(2) 基本設計

Trusted Web を実現するプロトタイプシステムを作るために、属性情報を含む VC やメッセージに対して署名をする必要があり、最初のプロトタイプシステムは署名を使ったアーキテクチャを考えて着手した。当初署名にはセキュリティ性が高く、広く普及している ed25519 方式の実装を含む NaCl ライブラリを使用したが、前記の委員からの指摘を受け、ライブラリを did-jwt、did-jwt-vc に置き換えた。

(3) システム開発

Figma¹²を用いて画面遷移・項目を作成し、各画面で必要な項目、処理を整理した。画面開発と Trusted Web システムの実装を分けて開発を進め、Trusted Web システムができた段階で、画面から Trusted Web システムを呼び出すように記載した。

(4) ユーザーテスト

補助金申請手続きにおける業務プロセスのテストケース（50 ケース）に基づいて、ウォークスルーテストを実施し、正常に動作することを確認した。

想定担当者	分類	確認項目	想定結果
申請者	住民票紐付申請	表示項目	・ヘッダーに申請者と表示されている ・タイトルに住民票紐付申請と表示されている
申請者	住民票紐付申請	データ入力	データが入力できる
申請者	住民票紐付申請	データ入力	氏名フリガナに、「山田太郎」と入力して確認ボタンを押すと「・全角カナで入力してください」のメッセージが表示される
申請者	住民票紐付申請	データ確認	入力したデータが確認画面に表示される
申請者	住民票紐付申請	データ保存	・申請ボタン押下で完了画面に遷移する ・申請者の申請一覧に、申請が「承認待ち」ステータスで表示される
自治体	住民票紐付申請一覧	表示項目	・ヘッダーに自治体と表示されている ・タイトルに住民票紐付申請一覧と表示されている
自治体	住民票紐付申請一覧	データ確認	申請者の申請した内容が、申請一覧に表示されている
自治体	住民票紐付申請内容照会	データ確認	・申請内容が照会できる ・ステータスが検証OK、未承認と表示されている
自治体	住民票紐付申請内容照会	承認	・承認ボタン押下で承認が完了する ・ステータスが未承認から承認済になっている
事務局	補助金申請照会	承認	・承認ボタン押下で承認が完了する ・ステータスが未承認から承認済になっている
事務局	VC一覧	VC発行確認	VC一覧に発行したVCが表示されている

図 3.1.2 実施したテストケースの例（一部抜粋）

¹² Web アプリケーションの UI/UX デザイン、プロトタイプ作成、コラボレーションに使用されるデザインツール

3.1.3 ヒアリングの実施

(1) ヒアリング概要. ヒアリングの実施

金融機関における Trusted Web での本人認証・口座照合等の実現可能性と想定される手法についてヒアリングを実施した

- ・1月下旬：地方銀行 A インターネット支店責任者
- ・2月上旬：地方銀行 B 決済ビジネス責任者・担当者
- ・2月上旬：地方銀行 C 経営企画 IT 戦略責任者・担当者

自治体における Trusted Web での本人認証・証明書発行等の実現可能性と想定される手法についてヒアリングを実施した

- ・2月上旬：自治体 A（市区町村） DX 推進責任者・担当者
- ・2月上旬：自治体 B（都道府県） デジタル戦略責任者・DX 推進担当者

国税庁・税務署における Trusted Web での納税証明・確定申告情報の発行等の実現可能性と想定される手法についてヒアリングを実施した

- ・3月下旬：国税庁 DX 担当部署、管理運営担当部署、総務担当部署

補助金事務局における Trusted Web での本人確認・実在証明・申請者管理の実現可能性と想定される手法についてヒアリングを実施した

- ・11月上旬：補助金・給付金事務局 A、B、C（十万～数百万申請の大規模補助金事業）
制度設計担当者・制度運営担当者

(2) ヒアリング結果

上記の各証明機関や申請先へのヒアリング結果を、経済面（ステークホルダーのベネフィット、システム・人的コスト）、制度面（法令等の制度や組織面での課題など）、技術面（既存システムとの連携、技術的課題など）の観点で整理し、Trusted Web 及び本ユースケースの社会実装に向けた課題、展望について、各ステークホルダーの見解をまとめた。

■ 地方銀行 A インターネット支店責任者

【経済面】（ステークホルダーのベネフィット、システム・人的コスト）

- ・Trusted Web により、今バラバラに存在している各種情報が統一化されることで、事務手続きなどが非常に効率的になる。
- ・窓口対応業務、証明書発行業務が削減できるのは、将来的に大きなメリットとなる。
- ・特に地方は、金融機関のみならず人手不足のため、本格的にこういったデジタル化が進めば、社会的に見ても恩恵は大きい。

・本人確認が共通化され、証明書類が受け取れるという仕組みに加えて、それらのデータを金融機関で取り込み、資産バランスなども見られるような仕組みとして発展すると、参加意義、利用価値が高まる。

【制度面】（法令等の制度や組織面での課題など）

・金銭的なメリットだけでなく、例えば顔認証の導入による利用者の利便性の向上など、この仕組みの理解者を増やしていく施策が必要。

・（中国等で導入されているような）信用スコアリングのような仕組みで、複数の機関、団体による信用情報を積み重ねて、利用者の信用度を評価していくという方法も、この仕組みと親和性が高いと思われる。

・振込口座の実在と残高証明程度の情報であれば、口座振替システム等で連携可能

・上記のシステム連携で、金融機関による証明発行に伴う手数料徴収も容易に行えると思う。

・実在証明、個人証明の仕組みは様々なものがパラレルで存在しており、それらの仕組みごとに運用面やシステム面の設計・調整が必要となるため、（この仕組みも、結果的に）非効率なものになってしまう懸念がある。

・金融機関が持つ信用情報は、金融機関独自の持ち物であるという意識が強いため、どこまでパブリックなものとするのが、この仕組みの発展性の鍵になると思う。

・金融機関の対応速度はかなりスローペースであるために新しい仕組みの実装には相当な労力と時間がかかる。

・補助金申請プロセスは、申請後にも例えば事業実施に伴う証明書類（請求書・領収書等）や補助対象物の性能証明書・認定機関が発行する認定証等、事業ごとに様々な書類の提出が必要になるので、より複雑な仕組み、フローが必要になるのではないか。

【技術面】（既存システムとの連携、技術的課題など）

・証明書ごとに記載内容が異なると認識している。それらを電子的に受け取る場合、それぞれ連携先（証明書発行元）の仕組みが異なること、システム連携のインターフェースや仕様が公開されていない場合、このような仕組みの構築には、個別の対応が必要となり、相当の手間がかかる可能性があると思われる。

・アナログ（紙）から電子申請に置き換えるため、レガシーシステムの環境変更に対する費用対効果に関しては、ネガティブな印象を持った。

・自身の情報がどこまで開示されてしまうのか、事前の合意を明確に取る必要がある。

・本人確認方法に関しては、例えば初回は対面での確認が必要になることや、本人と所属法人の紐づけが困難なため、申請担当者が当該法人に属する者か判断するWEB上の手法が確立されていない等、デジタル（WEB）の限界が見えてきているので、アナログとデジタルのハイブリッドをうまく活用しないと、いずれ行き詰まるのではないか。

・金融機関では、オンラインの本人確認に関しては、本人確認書類の真贋、住所（厳密には居住地域）

と IP アドレスの整合性、警察情報の確認など高い精度で行っている。

・Trusted Web 上で様々な事業者・機関が証明者となった場合、証明する情報の精度のギャップが課題となる。

・金融機関にとって、新規のシステム導入は相当ハードルが高い。

■ 地方銀行 B 決済ビジネス責任者・担当者

【経済面】（ステークホルダーのベネフィット、システム・人的コスト）

・個人向け eKYC（オンライン本人確認）市場では、そもそも個人向け eKYC を必要とするサービスが行政手続き以外では少ないことや、マイナンバーカードでの認証に流れが大きく傾いていることもあり、金融機関が保有する情報照会システムは人気や需要がない、少なくとも当行が関わっているシステムでは、管理費を賄えるか否か程度の需要でしかない。

・上記の仕組みを社会全体で活用できるようなものにまで昇華させることができれば、金融機関にとっても社会実装を目指す意義がある。

・本ユースケースの補助金・助成金における口座照合という規模感では、システムや API(Application Programming Interface)の新規開発・運用構築等を行う労力を割くことは現実的ではないが、既存のプラットフォーム、既存 API の活用という範囲内で、手数料収入などのインセンティブがあれば、実現可能性はある。

・信頼できる情報と公的証明、公的認証が紐ついたプラットフォームがあれば、電子債権発行、取引、将来的な融資などに活用できる利用価値の高いプラットフォームになると思う。

・既存 API を利用した口座認証程度であれば、本ユースケースでいう Trusted Web プラットフォームへ証明者として参加するハードルは低い。

・確度の高い当人認証（法人認証）がされている状態の仕組みが提供されるのであれば、他の用途への展開も考えられるため、将来性を見据えた先行投資を前提とした参加の可能性が生まれる。

【制度面】（法令等の制度や組織面での課題など）

・申請者が総体的に得するスキームであれば、顧客サービスとして、口座の実在証明発行を実施する価値はある。

・Web 上における法人の当人認証（登記情報に登録されない代表者以外の従業員など、その者が当該法人に所属する者であるという確認）は、未だこのサービス提供者も実現できていないので、実現すれば相当な需要が見込めると思う。

・補助金申請の事業計画に印を押すことを電子化したとしても、一金融機関では、数件程度の申請しかない補助金も多く、金融機関の業務効率化は見込みにくい。

・口座存在の形式要件のみの確認は比較的容易に可能である。

・口座が存在することの証明は可能だが、その口座が申請者自身の口座であることを証明するには、本人確認や法人確認が必要となるため、金融機関でそこまでの証明を、責任を持って実施するというので

あれば、対応が難しいと思われる。

- ・（トップダウンでなく、ユースケースの積み上げという）このプロセスでは、中央銀行デジタル通貨（CDBC）と同様に実現は難しいのではないかと思う。

【技術面】（既存システムとの連携、技術的課題など）

- ・物理的な口座番号確認だけなら、得られる情報はカナ氏名などに限られるが、技術的には個人向け API の法人拡張や、統合 ATM スwitchングサービスなどの既存システムで実現可能である。
- ・法人の紐づけであれば、当行にはネットバンクなどで法人認証を行うためのプラットフォームが存在しており、これと連携すれば技術的には実現が可能。
- ・統合 ATM 照合システムで、カナ氏名しか得られないが、技術的に連携は可能。
- ・ネットバンクの ID をそのままログイン ID として利用すれば、本人認証の手間は省ける。
- ・マイナンバーカードをトラストアンカーとした民間デジタル ID のサービス実装が始まっているが、その法人版という印象。gBizID や法人番号と連携する可能性はないのか。

■ 地方銀行 C 経営企画 IT 戦略責任者・担当者

【経済面】（ステークホルダーのベネフィット、システム・人的コスト）

- ・（外部に提供しているものではないが、）本人確認 API があるので、これを将来外部に提供するビジネスとして、こういったプラットフォームに参加する意義はあると考える。
- ・証明書発行の電子化による事務の効率化はメリットであると考ええる。
- ・法人インターネットバンキング契約を締結してもらい、法人口座連携を行い手数料収入を得るというビジネスは金融機関のメリットになる。

【制度面】（法令等の制度や組織面での課題など）

- ・銀行 API の仕様は数パターンに分かれているだけなので、連携の可能は十分にあると思う。
- ・口座の実在証明であれば比較的容易に実現可能だが、申請者がその法人の社員であるということを第三者へ証明することは制度、ルール等の整備が必要。
- ・補助金の場合、申請者が信用金庫の口座を補助金の受取口座として指定する場合も多いと思うが、銀行のみならず信金信組などへ、システム連携範囲を広げるのはハードルが高いと思う。
- ・補助金はいくまで補助金を受給するための情報として完結するため、デジタル証明書を、補助金以外の民間サービスでの利用が可能であるという世界観を全面に打ち出した方が、ビジネスとして拡張性が感じられるため、地銀は乗りやすいのではないかと思う。

【技術面】（既存システムとの連携、技術的課題など）

- ・法人の口座証明を発行する場合、法人向けインターネットバンキングを利用している法人であれば、イ

インターネットバンキングの認証を使用して、非対面での法人確認が可能。

- ・個人の場合は、既存の本人確認、口座番号照会の仕組みが金融機関内のシステムとして既にある。
- ・残高、取引明細も、電子決済代行業向けの API で技術的には連携可能である。
- ・CNS（地銀ネットワークサービス株式会社）が、個人の口座認証サービスとして全国の地銀、第二地銀、信金と繋がっているため、本ユースケースの TrustedWeb システムで、個人口座の口座番号や名義人などのデータを連携する場合には、個々の金融機関システムとそれぞれ連携するのではなく、CNS の仕組みと連携することで、システム連携が可能ではないかと思う。
- ・電子決済代行業、業務会計システムなどと同様の API 連携で実現可能だと思われる。
- ・残高照会サービスを導入している金融機関であれば、もっと容易にデータ連携が取れる可能性がある。
- ・なりすましによる証明書の不正な受け取りなどのセキュリティ対策が重要である。
- ・個人口座の持ち主が、個人事業者かどうかの情報も記録されているが、自己申告、担当者のヒアリングベースでの判定となっている。

■自治体（市区町村）A DX 推進責任者・担当者

【経済面】（ステークホルダーのベネフィット、システム・人的コスト）

- ・市区町村が実施している事業者向け補助金で利用できる証明書プラットフォームであれば、事務の効率化に繋がり利用価値は高い。
- ・Trusted Web のプラットフォームは、補助金ありきでなく、さまざまな信頼情報・証明情報授受の仕組みとして将来性を感じる。
- ・事業者向けの補助金業務として、前年売上や申告時点での四半期売上をもとにした年間売上予測を申請情報に含めることが多いが、その後の年間売上実績を後追いで、更新したり、後日確認できるような仕組みとなっていると、利用価値は高い。
- ・賃料の証明、経費の証明なども補助金申請に必要な場合があり、全プレイヤーが参加していないと補助金申請事務の全体効率は上がらないと思う。

【制度面】（法令等の制度や組織面での課題など）

- ・紙の証明書しかない確定申告書情報（※発言ママ。実際は xml 形式等で本人に提供されている）、開業届、法人の届出書などの電子証明化は需要が高い。
- ・証明書を PDF ファイルの形式で発行することは行われているが、本ユースケースのように完全な電子情報としての発行となると法律面・制度面含めた電子情報授受のルール決めが必要となるのではないかと思う。
- ・振込先口座の確認も電子証明で受け取れると、振込ミス予防につながり、事務効率はアップする。
- ・マイナンバーカードでは提供できない情報（家族や世帯情報）などの証明において、こういったプラットフォームは有効的。
- ・自治体での補助金事務の場合は、マイナンバーカードの番号連携で多くの情報が取得できるので需要

は低いと考える。

【技術面】（既存システムとの連携、技術的課題など）

- ・自治体としては、マイナンバーカードの番号連携で多くの情報が取得できるが、民間事業者にとって実在・所在確認の仕組みとしての需要はあり得ると思う。
- ・証明書の PDF 送信・発行は可能だが、電子情報での発行は現時点で行っていない。
- ・個人事業主の場合、J-LIS（地方公共団体情報システム機構）のコンビニ交付システムへの問い合わせなどで、技術的には住民票の発行をもとにした実在・所在確認ができる可能性がある。

■自治体（都道府県）B デジタル戦略責任者・DX 推進担当者

【経済面】（ステークホルダーのベネフィット、システム・人的コスト）

- ・KYC（本人確認）の問題はあるが、対面発行でなく、非対面での証明発行は効率が良い。

【制度面】（法令等の制度や組織面での課題など）

- ・インターネットが社会インフラ、生活基盤になってくると、電子化は必須の流れだが、行政分野の業務に関しては法令との調整という問題もあり、一自治体だけの対応では、一筋縄ではいかなくなってきている。
- ・電子化の仕組みを導入しても、紙の証明者発行をゼロにはできないため、（法令等含め）国がトップダウンで推進しないと効果が出ず、無駄な投資になってしまう。
- ・基礎自治体は個人対応事務が圧倒的に多く、個人情報取り扱いが多いため、現場担当職員がDXに前向きでも、情報システム部門がセンシティブになり動かないことが多い。
- ・特に導入期に関しては、電子申請の利用者をサポートするような体制が重要と考える。
- ・アナログ（紙）であれば、法人名＋登記印、個人名＋実印でも、登記簿や印鑑証明が付いていれば申請は受け付けられるが、電子化される場合はルール・制度作りから対応が必要。
- ・電子申請などの新しい仕組みは、いくつか選べるような中途半端な導入では使われないと思う。
- ・強引にでも電子のみで導入して、徐々にアダプトしていくようなアジャイル対応が必要だと思う。
- ・都道府県レベルでは、広域行政として（許認可等の）法人対応業務が多いが、マイナンバーカードのような公的な認証の仕組みが、法人認証ではないので、法人登記、gBizID などの状況を様子見の状態、市区町村より対応が遅れている。
- ・基礎自治体のオンライン化が優先的に進んでいるが、都道府県は対応が遅れている。
- ・個人事業者からの申請に関しては、個人名で申告してもらう形だが、今後マイナンバーを紐つけるのか否かなどは、まだ整理がついていない状況。
- ・発行依頼から手数料の徴収までワンストップサービスにしないと、利用されない仕組みになる。（e-Japan 戦略で数多くのサーバー、システムを立ち上げたが、決済システム導入に数億円かかることが分かり導入せず、その結果、手続きはオンラインでも窓口で手数料徴収となり、利用されない仕組みとなってしまった。）

【技術面】（既存システムとの連携、技術的課題など）

- ・誰ひとり取り残されないためには、電子申請の仕組みだけでなく、UI/UX（ユーザーインターフェース/ユーザーエクスペリエンス）が非常に重要と考える。
- ・個人の実在証明はマイナンバーなどが考えられるが、法人は gBizID などとの連携はあり得るのか。
- ・ブロックチェーンの導入に関して、サーバー方式との違いが分かりにくい。ユーザーメリットが見えにくい。
- ・各行政機関のセキュリティポリシーに合致しないと、導入ハードルが高く実現は難しい。
- ・個人情報流出など、セキュリティ面に関する懸念がないか、データ自体はどこに、いつまで保存されるのかなど含め慎重な仕様検討が必要。
- ・秘密鍵、公開鍵の管理の仕方によっては、セキュリティリスクが発生してしまう。
- ・誤った使い方をしたら、情報が流出してしまうという懸念がある。
- ・技術面・人的/運用面・物理的な面でセキュリティを守っているが、新しい軸での情報セキュリティ対策を検討する必要があると思う。

■ 国税庁 DX 担当部署、管理運営担当部署、総務担当部署

【経済面】

- ・国税庁・税務署としても、窓口対応の事務コストを削減する取り組みには注力しており、現行では納税証明や e-tax による確定申告等、電子化に積極的に取り組んでいる。

【制度面】

- ・国税庁としては、個人情報保護等の観点から、情報の提供先は常に本人であり、本人を経由しない第三者への直接的なデータ提供は法的整備等が必要となる。
- ・中小企業庁が推進するミラサポコネクトでも申請者情報をプラットフォーム上で一元管理する同様の取り組みをしているため、本ユースケースは構想的にミラサポコネクトと多少重複しているように思える。
- ・確定申告書でいう収受印は、単に税務署に提出されたことに対して押されるものであり、本人の確定申告の内容の確実性を担保するものではなく、国税庁として証明する性質ではない。

【技術面】

- ・確定申告書、納税証明書ともに、すでに e-Tax 上にて PDF データと XML データで納税者本人又は税務代理人に対するデータ提供を実施済である。納税証明書の XML データについては、電子署名付で提供している。
- ・本ユースケースで用いられている VC は申請者情報の選択的開示を実現できるということだが、補助金プラットフォームにその XML データをアップロードし、同プラットフォーム上で申請者情報の選択的開示ができるよう工夫すれば、XML データを用いた、情報の選択的開示も可能なのではないかと

■ 補助金給付金事務局（A、B、C）（10万～数100万申請の大規模補助金事業）
制度設計担当者・制度運営担当者

【経済面】（ステークホルダーのベネフィット、システム・人的コスト）

- ・電子申請の場合、証明書はPDFデータ、画像などで提出を受けているため、電子発行されたものが提出されれば、申請受付・審査業務はかなり効率化されると思う
- ・各機関から取得し提出する必要のある書類が、VCとして管理されることになれば、証明書の確からしさ（捏造等の疑義含め）の確認工数が大幅に削減される。
- ・証明書の添付忘れ、年度間違い等の不備による誤申請が非常に多いので、事務局側で証明書を指定ができればかなり不備は減ると思う。
- ・アナログ審査で必要な人員が、電子申請によって不正検知システム（AI、OCR）等に置き換わるので、初期・短期的にはコストダウンにはつながらないが、長期的には審査コストのダウンにつながると思う。
- ・国・国税などのシステムとスムーズに連携できれば、証明書の電子化が進み、申請における不備などが大幅に削減され、総合的なコストダウンの達成も早いと思う。
- ・新たに導入する電子証明・申請受付の仕組みと、各事業独自の審査に使用している既存の個別システムを重複して稼働させると、システムのトータルコストが上がってしまうのではないか。

【制度面】（法令等の制度や組織面での課題など）

- ・事業者の存在確認は、登記事項証明書（3ヶ月以内）と印鑑証明で行っているが、同等のものが電子証明で提出されるのであれば、利用価値は高い。
- ・課税証明書は、市区町村によってフォーマットが異なり、掲載されている項目も異なるので、確定申告情報と同様に、審査に必要な項目・情報のみが電子化されて提出される仕組みは魅力的。
- ・国庫補助金の重複受給等の照合ができるようになれば、省庁横断的に厳格な管理が可能になり、利用価値が上がる。
- ・証明書情報がVCのような形で電子化されていれば、審査員による目視確認が不要になり、システム上で突合することが可能で、人件費コスト削減や審査精度の向上に繋がる。
- ・事務局側で証明書の記載事項が指定・限定できると利用価値は高い。（事務局が住民票のマイナンバーを黒塗り処理したり、申請者が確定申告書類の審査不要部分を黒塗りしたりする手間が省ける。）
- ・申請者が複数IDを使う必要がなくなり、利便性が向上する。
- ・信用情報の流通や信用の世界をどのように作っていくか。全体構想を描き、証明者・申請先の賛同を得て、参加者を増やしていく必要がある。
- ・VCを各機関（自治体・国税等）の証明書と同等であるというレギュレーション作りが困難に思える。
- ・アナログをデジタルに置き換えただけでは、構造的な変化がなくメリットがあまり感じられない。
- ・法人・個人事業者・個人に対する補助金で対応が異なるので整理が必要。
- ・「納税証明書」「確定申告書類」を補助金申請に用いる場合は、国税庁・税務署の運用基準を踏まえてシステム化を図ることが必要となる。

- ・個人事業者の開業、休眠、廃業をリアルタイムで追うことが非常に困難で、この仕組みでどう解決するのが重要になる。（税金は年一回の事務処理なのでリアルタイムには動かない。）
- ・それぞれの補助金事業独自フォーマットの証明書書式や特殊な業界特有の証明書の写しの提出が必要な事業もあるので、全証明書類を電子化することは難しいと思う。
- ・申請受付以降の補助金事務（交付決定・通知・実績報告）、給付金事務の審査業務などとも連携できないと、事務作業全体としての負荷の低減・事務効率化は難しいと思われる。
- ・コールセンターで申請受付状況の照会を行うなどのサポート体制が必要。
- ・電子申請できない人、使い方がわからない人のサポート体制が重要になるとと思われる。

【技術面】（既存システムとの連携、技術的課題など）

- ・発行された証明書・情報が改ざんされていない。ということがわかる技術は利用価値が高い。
 - ・必要な情報（前年度の売上など）だけ流通することが出来れば、利用価値は高い。
 - ・紙の証明書を PDF 化（スマホで紙の証明書を撮影）する作業は不要になるので申請者・事務局の負担は減る。
 - ・事業者口座からの当該補助金に関連する支払いや取引情報が電子証明として提出されれば、審査、実施報告や確定検査などに活用できる。
 - ・申請を電子化することで審査効率がアップするが、不正チェックが非常に重要な要素になってきている。
 - ・担当者が会社を辞めた後に、不正を行おうとした例もあり、会社と担当者の紐付けは重要な課題
 - ・スタートアップ企業の存在証明、納税の証明など、リアルタイムに動いているもの、動いていないものを細かく検証し、何が補足できるのか明確にしていく必要がある。
 - ・不備のある申請の差し戻しと（証明書の再提出、差替えなどの修正指示）、再提出（修正申請）受付などの仕組みも実運用には必要。（個人からの申請の場合、不備申請が 3-4 割の比率で発生する事業もある。）
- 大規模事業の場合は特に事務局の申請受付画面は工夫が必要。審査システムと自動連携して受付しないと対応できないと思う。
- ・申請内容、申請条件によって必要な証明書のパターンが変わる場合もあるため、想定されているより仕組みが複雑になる可能性が考えられる。
 - ・重複申請が排除されなかったり、申請途中で放置されてしまったゴミデータの削除を行う必要があると、事務局業務が増えてしまう危険性も考えられる。
 - ・補助金振込口座は、振込実行前に一括で振込テストを実施した上で振り込んでいるので、エラーは少ない。
 - ・申請先のシステムに合わせて、連携データを作成する必要があると想定されるが、無数にあるシステムにすべて対応するのは厳しいと思われる。
 - ・事業独自のシステムと、こういった新規 ID との連携は導入時にかなりの労力が必要で、実装に向けて事業ごとに調整が必要。
 - ・登記簿、確定申告情報などを VC として電子化した場合、記載項目が多岐に渡るため、紙の書類と

同じ粒度で可視化、閲覧を可能にできるのか。

・扱う人の全てがリテラシーの高い人ではないため、直感的なものでないと逆に手間がかかってしまう。

■ヒアリング結果まとめ

【経済面】（ステークホルダーのベネフィット、システム・人的コスト）について

Trusted Web の仕組みを活用した証明書の電子発行により、証明書発行業務、受取業務などの事務処理の効率化が期待できる。地方の人手不足対策に有効であるといった意見や、ある銀行においては既存の API 公開による証明書発行手数料の収益なども魅力的と感じるという意見が挙げられた。コスト削減に関しては、デジタル・アナログ併用環境では、その効果が限定的である点や、アナログ審査の人的コスト削減と、不正検知等の新機能を含めたシステム運用コストや申請サポート体制強化等による運営コストの増加のバランスにより、導入初期～中期まではトータルコストが増加するのではないかという懸念点も挙げられた。

また、補助金・給付金申請における証明書発行・流通の仕組みのみでの単体利用だけでは、証明者としてメリットは限定的で、積極的に導入を進めるメリットも薄いという意見もあった。

さらに、証明書発行プラットフォームだけでなく、既存の法人確認手法では確認できない納税証明書や確定申告情報などに基づく VC をもとに、金融機関側でも事業者の事業継続性を確認できるような、信用情報プラットフォームとしての利用や、補助申請時点での情報だけでなく、継続的な情報収集が可能になるなどの拡張性があれば証明者にとってもより有益な仕組みとなるという意見も聞かれ、Trusted Web の世界観・可能性に共感する証明者からの肯定的な意見が寄せられた。

【制度面】（法令等の制度や組織面での課題など）について

アナログ（紙）をデジタルに置き換えただけでは、構造的な変化がなくメリットがあまり感じられないという意見が多い中で、電子証明化により、必要な項目のみ指定、限定した上で改ざんが困難な証明が発行される仕組みについては、証明書の添付ミス対応コストや機密情報の管理コスト低減という観点で、魅力的であるという意見が多かった。

アナログ（紙）による申請書や証明書が併用可能な環境下では、電子化による効率化の効果が薄く、コスト削減も限定的となるため、完全電子化などの制度化やルールを推進するために、国による法整備などを期待するという意見が多く挙げられた。また、電子証明の法整備（VC を始めとして電子情報がどこまでの信用力を持てるのか等）、ルール化（VC 発行時の本人確認や資格情報確認などの発行ルール等）も併せて必要であり、トップダウンによる環境整備、導入決定が不可欠であるとする証明者も多いる状況であった。

現在ネットバンクで実装している法人認証プラットフォームを活用すれば、技術的には法人確認が行えるが、第三者への証明とするには、責任問題などのルールや制度上の調整が必要であるという意見が聞かれた。

その他にも、各種法令との調整、既存のコード体系、KYC との連携、証明者の組織面での課題により、新しい仕組みの導入ハードルが高いことを懸念する声も多く聞かれた。

また、社会実装に向けた課題として、現行システムやアナログ（紙）対応を含めた現行のフローから、Trusted Web の新しい仕組みへ移行するためには、移行期間におけるシステム対応、運用計画、サポート体制構築などの過渡期対応が重要であるという意見も聞かれた。

【技術面】（既存システムとの連携、技術的課題など）について

新規のシステム開発、新規のシステム導入はコスト面だけでなく、運用面でも導入が困難であることが多いため、既存システムの活用や API 連携を前提とした対応を進めていく必要があるとの意見が証明者、申請先の両者から挙げられた。

また、なりすましによる不正申請への対策の重要性、情報漏洩に対する懸念などセキュリティ対策に関する意見も多く聞かれ、通常のサーバークライアント型のサービスでないという仕組みの利用者メリットが見えにくいといった意見や、こういった電子申請システムでは、誰一人取り残されないために UI/UX は非常に重要であるという声も聞かれた。

なお、ビジネスモデルに関しては、本ヒアリング結果をもとに、ビジネスモデルに関する実証内容・得られた成果（3.5.3）において、考察を進めることとする。

3.1.4 国際標準規格の調査

本プロトタイプシステムのアーキテクチャは、セキュリティリスクへの対応と他の事業者による再現性を高めるため国際標準規格に沿って開発する方針とした。本実証で準拠・参考、及び今後検討する国際標準規格は、次の通りである。調査対象については、網羅的に記載されていた日経 Network 2023 年 2 月号特集記事を参考とした。

調査の結果、本プロトタイプシステムに必要な DID/VC の機能を実現するために Decentralized Identifiers (DID s) と Verifiable Credential Data Model の規格が必要であることが判明したため、アーキテクチャに取り入れることとした。

表 3.1.4 国際標準規格の一覧及び引用先

本実証との関連	名称	関連団体	標準化状況	概要
準拠	Decentralized Identifiers(DIDs) v1.0	W3C	勧告	識別子とメタ情報 (DIDドキュメント) のデータモデルとローケータに関する仕様
準拠	Verifiable Credentials Data Model v1.1	W3C	勧告	検証可能な資格情報のデータモデルに関する仕様
参考	The did:key Method v0.7	W3C	非公式草案	did:keyの仕様
今後検討	Well Known DID Configuration	DIF	Working Group Approved Draft	DIDとドメイン名をDNSを通じて紐付け、識別子が指す主体の検証に信頼性を向上するための仕様
今後検討	Status List 2021	W3C	W3C Editor's Draft	発行済みのVCの状態(取り消しなど)を管理するための仕様
今後検討	OpenID for Verifiable Credential Issuance	OIDF	Standards Track	VC・VPを発行者、所有者、検証者の間でやり取りするための仕様や、所有者が自身の管理するOpenIDプロバイダーから属性を発行するための仕様。これら3つを総称して「OpenID for Verifiable Credentials」と呼ぶ
今後検討	OpenID for Verifiable Presentation	OIDF	Standards Track	
今後検討	Self-Issued OpenID Provider v2	OIDF	Standards Track	
今後検討	DIDComm Messaging v2.0	DIF	DIF批准	DIDを持つ主体の間でのメッセージを送受信するための仕様
今後検討	Decentralized Web Node	DIF	Draft	DIDを持つ主体間でメッセージを送受信際のトランザクション管理やデータ保管、メッセージリレーなどの仕様

名称	引用
Decentralized Identifiers(DIDs) v1.0	https://www.w3.org/TR/did-core/
Verifiable Credentials Data Model v1.1	https://www.w3.org/TR/vc-data-model/
The did:key Method v0.7	https://w3c-ccg.github.io/did-method-key/
Well Known DID Configuration	https://identity.foundation/.well-known/resources/did-configuration/
Status List 2021	https://w3c.github.io/vc-status-list-2021/
OpenID for Verifiable Credential Issuance	https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
OpenID for Verifiable Presentation	https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
Self-Issued OpenID Provider v2	https://openid.net/specs/openid-connect-self-issued-v2-1_0.html
DIDComm Messaging v2.0	https://identity.foundation/didcomm-messaging/spec/
Decentralized Web Node	https://identity.foundation/decentralized-web-node/spec/
網羅的に整理されていた日経Network 2023年2月号特集記事「分散型ID」の実像を基に情報を整理	

3.2 検証できる領域を拡大する仕組み

3.2.1 データフロー

データの保有者である申請者は、証明者にVCの発行を依頼してVCを取得する。申請者はローカルストレージ上でVCを管理し、申請先の応募資格を確認した上で開示を行う。本システムはVCをブラウザのローカルストレージに保持し、アクセスコントロールは行っていないが、今後、ネットワーク越しにVCを管理する際には、送信者と受信者のみが見ることのできるアクセスコントロールを実装する。

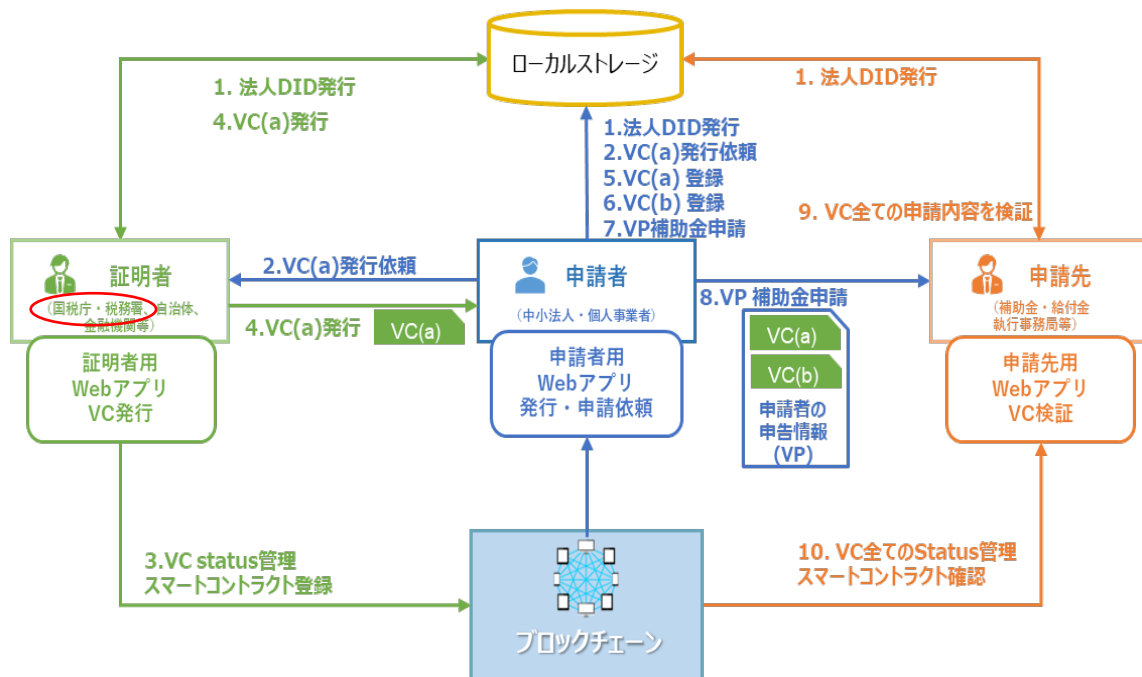


図 3.2.1 データフロー図

3.2.2 データフローに登場する主体とその概要

- 公的支援（補助金・給付金等）を申請する中小法人・個人事業者（＝申請者）
 - 発行された VC に対する所有権を持ち、ローカルストレージ上に自分に関する属性情報を保存し、申請先の依頼に基づき、申請先に提示する。申請に必要な各種証明を取得するため、申請者から証明者に VC 発行依頼をする。
- 国、自治体、金融機関（＝証明者）
 - 申請者から申請依頼を受け取り、審査する。申請された内容が各証明者が保有している内容と相違がないことを確認する。ブロックチェーン上に VC status 管理スマートコントラクトを作成して、VC を発行する。スマートコントラクトは VC の状態を保持しており、VC の取り消しは VC の状態を取り消し済みに変更することで行っている。取り消しはメッセージではなく、状態の更新であり、状態を変更したログが残るため、スマートコントラクトを利用している。また、VC の発行者しか状態の更新をできないようにしている。
- 補助金・給付金執行事務局等（＝申請先）
 - 申請者から申請情報を受け取り、審査する。補助金・給付金が、適切かつ迅速に申請者に届くようにする。VP¹³から VC を取得し、申請情報を審査する。そして審査結果についてシステムに登録する。

¹³ Verifiable Presentation の略称。VC によって証明された情報を、特定の相手に検証可能な形式で提示する際に使用される。

3.2.3 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

- 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：送信先は、送付されたデータが、確かにその相手から送付されたデータかどうか、また改ざんされていないかどうかを検証できない。
- ② 検証対象（データ/データのやり取り）：VC だけでなくエンティティ間のやり取りは JWS¹⁴で検証している。
- ③ 検証方法：EdDSA 署名¹⁵ で検証している。
- ④ 検証者：申請先、広義でいうと VC に限らず JWS の全ての受信者それぞれが検証を行っている。
- ⑤ データの所有者：VC は証明者と申請者、VP は申請者と申請先が持っている。
- ⑥ 発行者：自治体、金融機関及び税務署。
- ⑦ データ（VC）の置き場所：現状はブラウザのローカルストレージ。
- ⑧ アクセスコントロールの手法：＜将来において＞、送信者と受信者のみがメッセージにアクセスできるようにする。
- ⑨ 成果・留意点：署名を使うことによって検証できる領域が拡大した。

留意点はブラウザで完結するシステム構成になっているので、サーバーを介してエージェント同士がやり取りできるシステムアーキテクチャにすることである。

- 給付金申請者のなりすまし・申請内容の改ざん
 - 申請者のなりすましの有無を確認するために、申請書類の発行元を VC の署名検証によって検証する。具体的には、給付金執行事務局は、自治体・金融機関・税務署がそれぞれ発行した申請者の VC を、それらを束ねた VP として受け取ったのち、全ての VC を EdDSA 署名によって検証する。本システムでは、VC 以外の各エンティティ間でのやり取りについても JWS の署名で検証されている。署名検証を行うことで VC の発行元がどこか、内容が改竄されていないかを確認できるため、信頼性の検証が可能な領域を拡大させることができる。
 - 本システムの留意点としては、ブラウザで完結するシステム構成となっており、各エンティティが持つデータをローカルストレージ上で保存しているためアクセスコントロールを行っていない。社会実装していく上では、各エンティティのエージェント同士がやり取りできるシステムアーキテクチャにする必要がある。

表 3.2.3 Trusted Web システムによって解決できた課題

¹⁴ JSON Web Signature の略称。JSON データに署名するための標準規格

¹⁵ EdDSA 署名は、高速でセキュアなデジタル署名アルゴリズムで、Ed25519 などが代表的な実装として知られる

課題の対象	解決すべき課題	Trusted Web システムによって解決できたこと
申請者	<ul style="list-style-type: none"> 申請のために、自身の証明や自身の情報の証明を行う必要がある 	各証明者への申請行為及び発行される証明書をデジタル上の手続きと VC にてプロセスを簡素化、プロトタイプシステム上での手続きにおいて、従来の紙による申請・本人確認に比べ、工数削減に繋がることを確認した。
	<ul style="list-style-type: none"> 申請した情報が不正利用されるリスクがある 	合意した範囲内での情報提供を確認した。今後は申請者自身の選択的開示により、申請先で不正利用されるリスクを低減できる可能性は見込める。ただし、申請先システムの安全性が定かではない場合においては、申請者側で不正利用を感知することは難しい。
	<ul style="list-style-type: none"> 一度申請に用いた情報を再利用することができない 	VC、VP は再利用可能であることを確認した。
	<ul style="list-style-type: none"> 自身の証明を行う作業が電子化されおらず、窓口訪問や、窓口営業時間内に、証明に伴う申請作業等を行う必要がある 	申請者が、事前に受領した本人確認に関する VC を各証明者に送付し、証明者がそれを確認することで、VC 発行にあたっての資格確認がデジタル上で完了するため、申請者の窓口訪問や営業時間内の申請作業等にとらわれず、手続き可能であることを確認した。ただし、各証明者が確認に必要な項目の選定とシステムへの実装については、都度証明者との調整が必要。
	<ul style="list-style-type: none"> 申請者自身が作成する申請書など、公的機関からの証明が受けられない文書の信頼性の担保ができない 	中小企業診断士等の有資格者による補助金の申請サポートや国や独立行政法人等が発行する独自認証については、当ユースケース上の証明者として位置づけることで、その信頼性を VC という形で担保することが可能。ただし、前述のようなサポートや独自認証を証明（VC）として発行する場合には、国や独立行政法人等の機関や申請先との調整が必要。
申請先 (補助金執行団体 / 事務局)	<ul style="list-style-type: none"> 申請書に記載された情報の信頼性を確認する必要がある 	住民票や納税証明書などの紙の証明書提出と同様に、証明者が発行した住民票 VC、納税証明 VC を確認することで、申請先はその内容と信頼性を確認することができ、紙の証明書と比較して、目視確認ではなくシステムによる自動検査等が可能となり検証が容易となる。
	<ul style="list-style-type: none"> 補助金・給付金業務が複雑であり、審査に時間を要する 	(前項同様)

課題の対象	解決すべき課題	Trusted Web システムによって解決できたこと
	・ 申請情報の確認作業、事務処理等により補助金・給付金の支払いに時間を要する	補助金・給付金事務局へのヒアリングから、各証明者が発行した VC ベースでの審査となることで審査プロセスを短縮でき、審査にかかる総体的なコスト・工数の低減が見込まれることは確認できた。また、審査プロセスの短縮により、補助金・給付金支払いまでのリードタイムの短縮が実現可能。
	・ 申請された情報の活用ができない (申請情報の再利用)	Trusted Web の考え方に基づいたシステムを補助金・給付金交付状況を活用することで、同一補助金の複数年度重複申請や他補助金との重複受給などの状態管理が行いやすくなる。
	・ 申請情報についての申請者への問合せや、記載内容についての申請者からの問合せなど、問合せ対応に要する負担が大きい	事務局は、申請者から送付された VC について、VC の発行元への信頼と VC の真正性の検証により、申請者への問い合わせ回数が削減できる。もしくは不要となる。
証明者	・ 申請者を証明する書類は紙が多く、また窓口対応が必要な業務が多いため、事務作業や印刷コスト等が多く発生する。	申請書を電子化することで、窓口での対応業務を削減し、事務コストを減らすことが可能。 また、将来的には、情報の選択的開示を実装することで、申請・審査に不要な個人情報の授受を削減できる可能性がある。
	・ 申請のために、自身の証明や自身の情報の証明を行う必要がある	申請者は、過去に発行された VC について、有効期限の範囲内であれば再利用が可能となり、証明者の再発行が不要となる。

3.2.4 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

- ①合意の主体：申請者・証明者（申請者が申請した内容に合意した時に VC が発行される）
- ②合意の対象：住民票、口座実在証明及び納税証明書の発行申請内容及び発行
- ③合意の条件：申請内容が正しい時。

- ④トレースの対象：やりとりされているメッセージ全てがトレースされている。
- ⑤トレースの主体：システムの参加者。
- ⑥トレースの手法：本システムでは、署名による改竄の検証にのみ対応している。データの削除にも対応するため、＜次の展開として＞データの ID とデータのハッシュ値をスマートコントラクトに記録することも検討する。
- ⑦合意の取り消し：スマートコントラクトで VC のステータスを管理しているのでスマートコントラクトを取り消しのステータスにする。

- 住民票・口座実在証明・納税証明書の内容について
 - 申請者が申請した内容と申請者が保有している VC の内容との相違がないことを申請者が確認することにより、各証明者との合意が形成される。
 - 履行された上記の合意について、申請者と各証明者は各々が承認したメッセージの状態をローカルストレージ上のデータを読み取ることでトレース可能。
 - VC の status はブロックチェーン上のスマートコントラクトで管理しているので、スマートコントラクトを取り消しのステータスにすることで合意の破棄が可能である。

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

- 1 自治体が発行する住民票【住民票 VC】
- 2 金融機関が発行する口座実在証明【口座実在証明書 VC】
- 3 税務署が発行する納税証明書【納税証明書 VC】
- 4 補助金の申請者が補助金事務局へ申請する内容【補助金申請 VC】

(2) 検証者

- 1 申請者（中小企業、個人事業者）
- 2 申請先（補助金事務局）

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するもの

証明者（金融機関、自治体、税務署）、申請者（中小企業、個人事業者）、申請先（補助金事務局）

(2) アイデンティティ管理システム

本プロトタイプシステムでは、アイデンティティ管理システムではなくローカルストレージ内で did:key¹⁶を用いて管理する。did:keyを採用した理由は、初期の実証実験として、実装が容易であるためである。今後、実証実験を進める際には適切な did メソッドを検討し実装を行う。例えば、DID（Decentralized Identifier：分散型 ID）の長期運用を考えるとキーのローテーションが必要となるが、did:key は対応していないため、実証実験が進んだ際には、キーのローテーションに対応可能な did メソッドを選ぶ必要がある。

(3) アイデンティティグラフとして想定されるものは何か

- ・申請者←→自治体
- ・申請者←→金融機関
- ・申請者←→税務署
- ・申請者←→申請先（補助金事務局）

申請者が証明者に VC を発行してもらう際は、申請者が各証明者に対してリクエストを送信し、各証明者が VC を発行する流れとなる。そのため、申請者と各証明者は双方向のやりとりを行う。

3.3.3 ノード

(1) Wallet の使用有無

既存の Wallet では JWS¹⁷(JSON Web Signature)形式の署名は可能であるが、X25519¹⁸などによる鍵合意（鍵共有）に対応していないという認識である。今回のプロトタイプシステムは、全体的に簡易な実装になっているので JWE¹⁹による JSON データの暗号化は行なっていないが、秘密鍵を暗号化した上でブラウザのローカルストレージに保存する方式を採用した。

(2) 合意形成がされているか、されている場合その手段

合意形成は エンティティが VC を発行し、受領したエンティティが VC の署名が正しいことを検証することにより確認する。

(3) データのやり取りの記録場所

① ローカルストレージ

- ・エンティティ間の全メッセージ（VC の発行依頼、VC、VP）

② ブロックチェーン（Algorand）

- ・ VC の status 取り消し用のスマートコントラクト

¹⁶ 公開鍵暗号化方式に基づく軽量の DID メソッド

¹⁷ JSON Web Signature の略称。JSON データに署名するための標準規格

¹⁸ Curve25519 を使った楕円曲線アルゴリズムの一つで、高速でセキュアな鍵交換に使用される

¹⁹ JSON Web Encryption の略称。JSON データをセキュアかつプライバシーが保護された形式でエンコードするための仕様

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

メッセージオリエンテッドなサービスで構築しており、全てのメッセージの内容をローカルストレージに保存している。

<次の展開として> DIDComm を使用したサービスでの構築を行う。

(2) メッセージのデータモデル

メッセージは、ヘッダ、ペイロード、署名で構成される。ペイロードには以下を含む。

① 住民票 VC

- ・ 氏名
- ・ 氏名フリガナ
- ・ 住所
- ・ 住民となった年月
- ・ 本籍地

② 口座実在証明書 VC

- ・ 銀行コード
- ・ 支店番号
- ・ 口座番号
- ・ 法人名称
- ・ 申請者名
- ・ 申請者住所

③ 納税証明書 VC

- ・ 申請年度
- ・ 法人名称
- ・ 所在地
- ・ 申請者名
- ・ 申請者住所

④ 補助金申請 VP

- ・ 申請者名
- ・ 申請者住所
- ・ 住民票 VC
- ・ 口座実在証明書 VC
- ・ 納税証明書 VC

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

全てのメッセージはローカルストレージに記録されており、検証することが可能である。

<次の展開として> DIDComm を使用した構築を行い、DIDComm の仕様に準拠する。

3.3.6 トランスポート

(1) トランスポートの Protokol

メッセージのやり取りにはローカルストレージ経由で行うため、トランスポートプロトコルを使用していない。プロトタイプシステムで採用したローカルストレージでは、ネットワーク越しに VC をやり取りすることができないため、<次の展開として> DIDComm を使用した構築を行い、DIDComm の仕様に準拠する。

3.4 本実証で企画・開発したシステムの概要

3.4.1 業務フロー

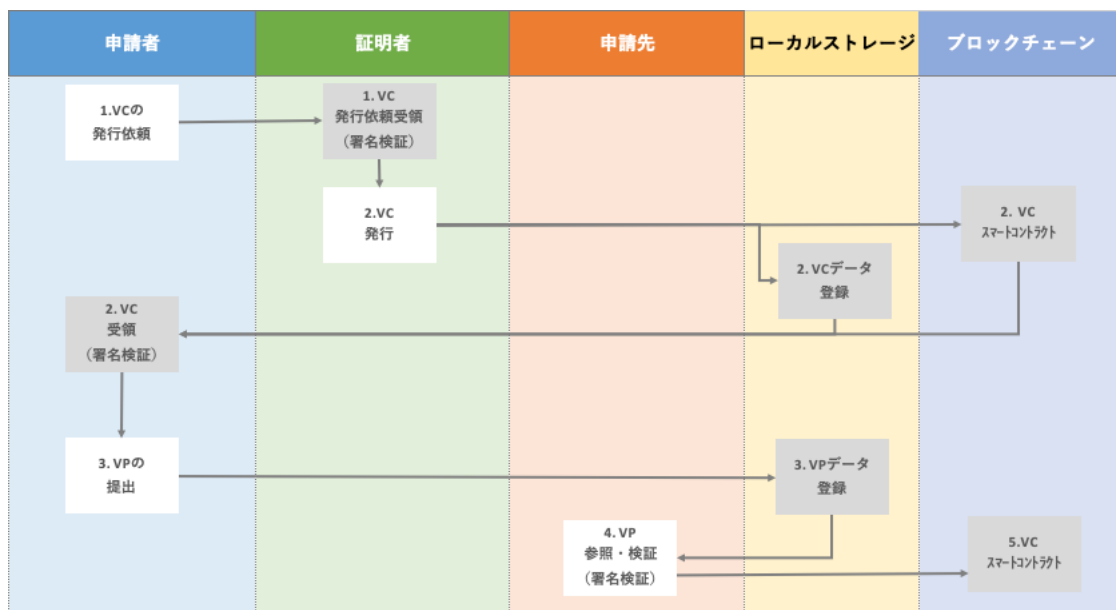


図 3.4.1 業務フロー

3.4.2 ユースケース図

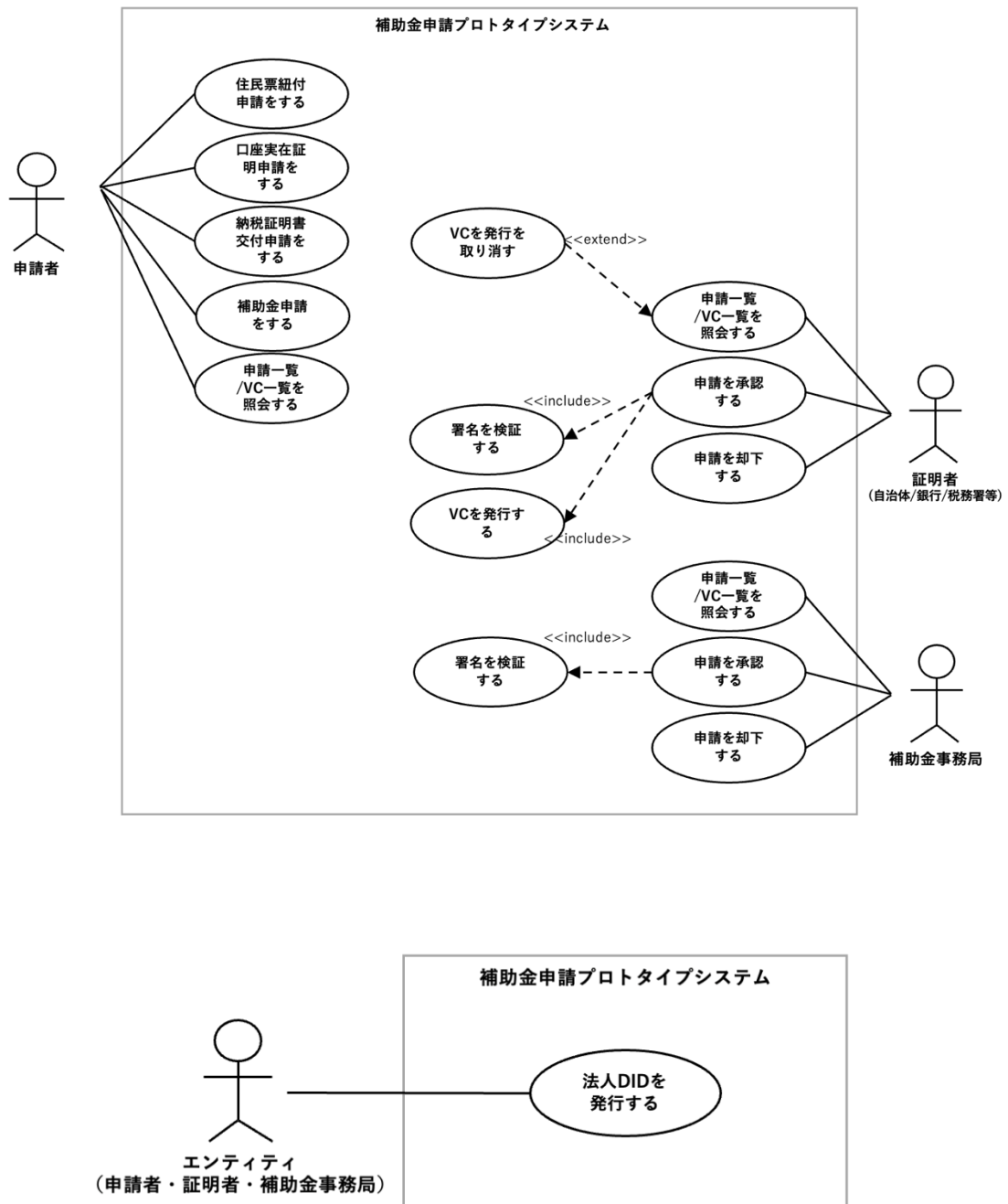


図 3.4.2 ユースケース図

3.4.3 操作画面 (UI)

操作画面については成果報告書概要版にて記載する。

3.4.4 機能一覧/非機能一覧

機能一覧/非機能一覧は下表の通りである。

表 3.4.4 機能一覧/非機能一覧

機能/非機能	機能名	機能概要
機能	住民紐付申請	申請者が補助金申請に必要な、住民票の紐付申請を行う。自治体に申請が承認されると、デジタル証明書を受け取ることができる。
機能	口座実在証明申請	申請者が補助金申請に必要な、口座実在証明の申請を行う。銀行に申請が承認されると、デジタル証明書を受け取ることができる。
機能	納税証明書交付申請	申請者が補助金申請に必要な、納税証明書の交付申請を行う。税務署に申請が承認されると、デジタル証明書を受け取ることができる。
機能	補助金申請	申請者が手に入れたデジタル証明書を元に、補助金申請を行う。
機能	申請一覧の照会	申請者が自分が申請した内容を照会することができる。
機能	デジタル証明書(VC)一覧の照会	申請者が自分が取得したデジタル証明書を照会することができる。
機能	住民票紐付申請一覧の照会	証明者(自治体)が申請された内容を一覧で確認できる。
機能	住民票紐付申請の検証	証明者(自治体)が申請された内容を検証(既存システムとの突合)できる。
機能	住民票紐付申請の承認/却下	証明者(自治体)が申請された内容を承認又は却下できる。承認されると申請者へデジタル証明書が発行される。
機能	住民票紐付申請のデジタル証明書一覧の照会	証明者(自治体)発行したデジタル証明書一覧を照会できる。
機能	口座実在証明申請一覧の照会	証明者(銀行)が申請された内容を一覧で確認できる。
機能	口座実在証明申請の検証	証明者(銀行)が申請された内容を検証(既存システムとの突合)できる。
機能	口座実在証明申請の承認/却下	証明者(銀行)が申請された内容を承認又は却下できる。承認されると申請者へデジタル証明書が発行される。
機能	口座実在証明申請のデジタル証明書一覧の照会	証明者(銀行)発行したデジタル証明書一覧を照会できる。
機能	口座実在証明申請のデジタル証明書の取消	発行した特定のデジタル証明書を証明者(銀行)が取り消すことができる。
機能	納税証明書交付申請一覧の照会	証明者(税務署)が申請された内容を一覧で確認できる。

機能/非機能	機能名	機能概要
機能	納税証明書交付申請の検証	証明者(税務署)が申請された内容を検証(既存システムとの突合)できる。
機能	納税証明書交付申請の承認/却下	証明者(税務署)が申請された内容を承認又は却下できる。承認されると申請者へデジタル証明書が発行される。
機能	納税証明書交付申請のデジタル証明書一覧の照会	証明者(税務署)発行したデジタル証明書一覧を照会できる。
機能	補助金申請一覧の照会	証明者(事務局)が申請された内容を一覧で確認できる。
機能	補助金申請の検証	証明者(事務局)が申請された内容を検証(既存システムとの突合)できる。
機能	補助金申請の承認/却下	証明者(事務局)が申請された内容を承認又は却下できる。承認されると申請者へデジタル証明書が発行される。
機能	補助金申請のデジタル証明書一覧の照会	証明者(事務局)発行したデジタル証明書一覧を照会できる。
非機能	可用性	プロトタイプのため、障害発生時の機能停止は実装していない。
非機能	運用・保守性	プロトタイプのため、メンテナンスの実施は計画していない。
非機能	性能・拡張性	業務量及び機能が増加した場合も、did-jwt と did-jwt-vc を活用してシステムを改修することができる。
非機能	セキュリティ	本システムの秘密鍵は JWT の署名のために使用しており、他人に知られないようにパスワードで暗号化している。

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)

データモデル定義は下表の通りである。

表 3.4.5 データモデル定義

種類	属性値	属性取得元	属性値 (vc 内)
共通	申請日	申請者 (Holder)	applicationDate
共通	発行日	発行者 (Issuer)	issueDate
共通	検証ステータス	発行者 (Issuer)	verifyStatus
共通	承認ステータス	発行者 (Issuer)	approvalStatus
共通	スマートコントラクト ID	発行者 (Issuer)	appIndex
住民票 VC	氏名	申請者 (Holder)	fullName
住民票 VC	氏名フリガナ	申請者 (Holder)	fullNameFurigana

種類	属性値	属性取得元	属性値 (vc 内)
住民票 VC	住所	申請者 (Holder)	address
住民票 VC	住民となった年月	申請者 (Holder)	addressRegistDate
住民票 VC	本籍地	申請者 (Holder)	permanentAddress
口座実在証明書 VC	銀行コード	申請者 (Holder)	bankCode
口座実在証明書 VC	支店番号	申請者 (Holder)	branchNumber
口座実在証明書 VC	口座番号	申請者 (Holder)	accountNumber
口座実在証明書 VC	法人名称	申請者 (Holder)	corporateName
口座実在証明書 VC	申請者名	住民票 VC	applicantName
口座実在証明書 VC	申請者住所	住民票 VC	applicantAddress
納税証明書 VC	申請年度	申請者 (Holder)	applicationYear
納税証明書 VC	法人名称	申請者 (Holder)	corporationName
納税証明書 VC	所在地	申請者 (Holder)	corporationAddress
納税証明書 VC	申請者名	住民票 VC	fullName
納税証明書 VC	申請者住所	住民票 VC	address
補助金申請 VC	住民票 VC 名	申請者 (Holder)	residentVC
補助金申請 VC	口座実在証明書 VC 名	申請者 (Holder)	accountVC
補助金申請 VC	納税証明書 VC 名	申請者 (Holder)	taxVC
補助金申請 VC	申請者名	住民票 VC	fullName
補助金申請 VC	申請者住所	住民票 VC	address
補助金申請 VC	住民票 VP	住民票 VC	residentVP
補助金申請 VC	口座実在証明書 VP	口座実在証明書 VC	accountVP
補助金申請 VC	納税証明書 VP	納税証明書 VC	taxVP

3.4.6 実験環境

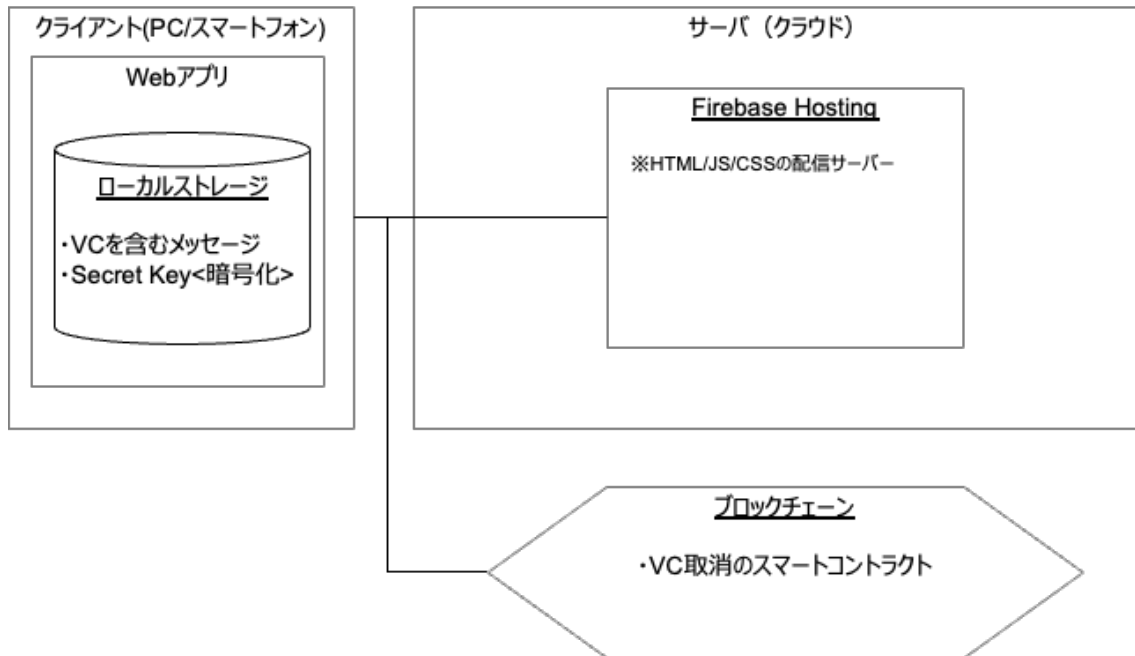


図 3.4.6 実験環境

<次の展開として> 今後の想定しているシステム構成は下記のとおり。クラウドはサーバレスの仕組み (Cloud Run) 上で、DIDComm を動作させることを検討している。

3.4.7 システムの構成要素

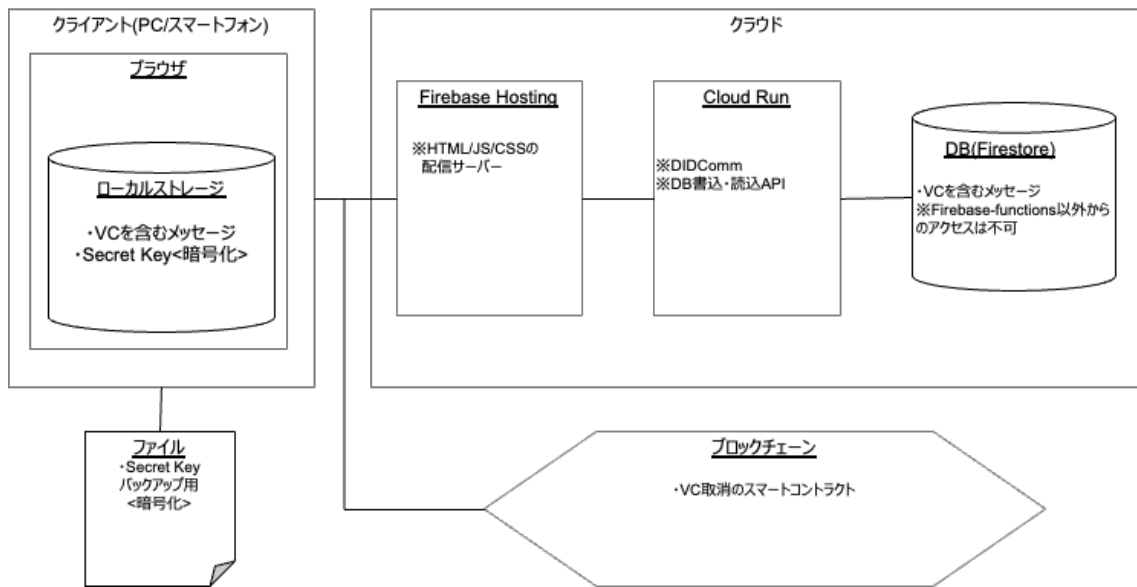


図 3.4.7 今後想定されるシステムの構成要素

表 3.4.7 主要な製品・ライブラリー一覧

本実証との関連	名称	OSS かどうか	ライセンス	概要
使用	Typescript DID Resolver	OSS	Apache-2.0	DID から DID ドキュメントを取得する汎用的な I/F
使用	did-jwt	OSS	Apache-2.0	DID の JWT ベースの実装
使用	did-jwt-vc	OSS	Apache-2.0	VC の JWT ベースの実装
今後検討	didcomm-rs	OSS	Apache-2.0	DIDComm v2 の Rust 実装
今後検討	Server-side implementation of DID communication(DIDComm)	OSS	GPL-3.0	DIDComm v2 の Python 実装
今後検討	SD_JWT	OSS	Apache-2.0/MIT	Selective Disclosure の JWT ベースの Typescript 実装

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

従来の補助金・給付金申請の流れを Trusted Web を活用した仕組みで電子化することについて技術面での検討を行った。具体的には、これまで紙の証明書やスキャンデータの添付をして行っていた本人確認や実在証明を、住民票 VC、口座実在証明 VC、納税証明書 VC の EdDSA 署名を検証する方法で実施した。その結果、VC の発行元と内容が改竄されていないかが確認でき、技術的に実装が可能であることを確認した。また、今回の要件においては、申請者の本人確認を市区町村による対面での住民票発行により実施することとしたが、非対面での発行や既存 KYC との連携など、より効率的に行う方法を検討する必要があることを確認した。

3.5.2 ビジネスモデルに関する実証内容・得られた成果

Trusted Web を活用した本人確認・実在確認および各種証明書発行におけるデジタルへの移行は、申請者・証明者・申請先にとっても総体的な手続き工数の削減につながり、事務業務の大幅な効率化が実現すると思われるが、各証明者・申請先のどの業務範囲にどの程度のニーズがあり、導入によるメリットをどう生み出せるかが不明瞭であった。そのため証明者・申請先になり得る関係各所へヒアリングを実施し、導入を想定するうえでのフィジビリティと課題感について確認・検討を行った。

(1) 電子証明の活用によるコストダウン効果とシステム運用における負担増について

改ざんが困難な電子証明の流通環境の構築により、紙の申請書を PDF 化（画像化）する作業が不要になること、申請書類の発行のため窓口に来訪する手間の削減等による申請者の負担軽減（実質的なコスト削減）や、申請先である補助金・給付金執行事務局での証明書類確認工数が大幅に削減されること、不備申請の減少による事務コスト削減効果が期待できる。また、証明者にとっても、非対面での証明書発行システムの導入は、事務手続きの効率化や窓口業務のコスト削減につながるだけでなく、地方の人手不足に対する社会的な貢献にもつながるといった肯定的な意見も寄せられた。

数多くの補助金・給付金の申請で必要とされる、納税証明書や確定申告情報については、電子化による波及効果が高く、申請先の需要が高い状況でありスムーズな連携が進むとコストダウン効果が大きいと期待される。確定申告情報に関しては、審査に必要な情報はその一部に限られており、その一部のみの証明が電子化される仕組みであると、申請者と申請先にとっては、より効率的な申請フローの構築が可能となり、効率化によるコストダウン効果が高まると期待されている。

その一方で、申請に必要なすべての情報（登記簿など）が電子化されないと、全体効率は期待しているほど上がらないという見解もあり、業界特有の証明書なども存在しており、それらを含めたすべての証明を一気に電子化することは困難であると思われるため、より多くの証明者にとって、参加するメリットのある魅力的な電子証明プラットフォームとすることが必要であると考えられる。

補助金・給付金の申請と申請に必要な証明の電子化により、申請先である事務局の審査効率が向上することにより、アナログ（紙ベース）申請で必要な審査人員削減が期待できるが、電子化、自動化の導入により、不正チェック機能が非常に重要な要素になり、不正検知 AI システムの構築、運用が必要なり、それにかかるシステムコストの増加が、導入期においては審査人件費削減効果を上回ると思われる。また、各補助金事業独自の電子申請・審査システムと重複したシステム稼働による運用コスト増、コールセンター設置・増席費用、申請者サポート体制拡充による運営費増などによるコスト増加も導入期において想定する必要がある。

（２）証明者の手数料収入などのベネフィットについて

証明発行による手数料収入については、新たな収益源として民間の証明者にとって魅力的ではあるが、新規にシステムを開発したり、全く新しい仕組みを導入したりすることは、組織的に見てもコスト面でもハードルが高く、手数料収入だけでは導入コストが賄えず、新システム導入の動機付けにはならないという現状が明らかになった。

その一方で、既存の仕組みである金融機関が所有する本人確認 API、ネットバンク API などの連携、活用により、口座存在の形式要件のみの確認について、技術的には比較的容易に実現が可能であると考えられる。また、これらの API 利用により、（簡易的な）本人認証も可能であり、非常に大きな課題の一つである証明発行手数料の徴収方法についても、ネットバンクを利用した徴収などの可能性も考えられる。

（３）アナログ（紙）ベースの世界からの転換に要するコストとエコシステム化へ向けた取り組みの重要性

本ユースケースの社会実装に向けては、申請者、証明者、申請先それぞれのベネフィットがコストを上回り、ステークホルダーにとって魅力的な収益構造が構成できるようなエコシステム化が必須であるが、アナログ（紙）ベースで成り立っている現状から、電子化への転換期においては、各種システムの改修費、統合費、その期間重複したシステム稼働の運用費などのシステム投資やユーザーへのサポート体制、オペレーター等の運用体制構築のコストなど、導入・普及のためのコスト面でのハードルは非常に高いと思われる。

そのため、ヒアリングにおいて、証明者にとっては「補助金申請ありきの世界観だけでなく、様々な信頼情報・証明情報授受の仕組みであれば参加者がより増え、利用価値が向上する。」、「信用情報と公的証明、公的認証が紐ついたプラットフォームであれば、将来的に融資などにも活用が期待され、民間事業者による信用情報の利活用につながる。」や「自治体では、番号連携により多くの情報が取得できるため、マイナンバーカードではできない家族や世帯などの情報連携に活用できるとよい」といった意見や、「国庫補助金の重複受給等の照合ができるようになれば、省庁横断的に厳格な管理が可能になり、利用価値が上がる。」、「事業者口座からの当該補助金に関連する支払いや取引情報が電子証明として提出

されれば、審査、実施報告や確定検査などに活用できる。」といった申請先である補助金事務局の意見に見られるように、アナログをデジタルに置き換えるだけでなく構造的な変化を生み出し新しい価値創造が可能なプラットフォームという世界観を共有し、信用情報の流通や信用の世界をどのように作っていくか全体構想を描くことで賛同する参加者を増やしていく必要があると考える。

また、電子化の仕組みを導入しても、紙の証明書発行を完全に廃止することには繋がらないため、十分な効果が出ず無駄な投資になってしまうことが懸念される。そのため電子申請の利用者をサポートするような万全の体制を敷いた上で、法令等含め国によるトップダウンでの完全電子化を実施していく必要があると考える。

3.6 本実証で開発したシステムの第三者による再現可能性（A 類型のみ）

本プロトタイプシステムでは Visual Studio Code Dev Containers と Docker を利用して開発を行ったため、Linux、Windows、OSX 等のあらゆる OS で動作し、特定の環境に依存しない。また、ソースコードを Github 上に公開する予定のため、第三者による再現が可能である。

本プロトタイプシステムでは Alphabet 社が提供する Firebase を利用しており、同製品のライセンスを利用することで第三者による再現が可能になる。

第三者による再現を安易なものとするため、手順書を用意した。

表 4.1 各ステークホルダーのベネフィット及び想定している利用料

ステークホルダー	ベネフィット	負担するコスト
証明者 (証明書発行団体)	証明書発行および申請先からの照会等に係る事務コストの削減、紙の証明書の印刷費用の削減	証明書の電子発行サービス利用料は負担しない。
申請者 (申請を行う企業/個人)	証明書取得に係る煩雑な手続きの簡略化	証明書発行時に発行手数料を負担(金額は証明書の種別により異なる。)
申請先 (補助金・給付金執行事務局)	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ことによる受付審査業務の効率化	事業規模(想定申請数、申請受付期間等)により、申請の電子化サービス利用料を負担。

納税証明書などの証明書については、従来より補助金申請の際に必要とされることが多く、すでに申請者が手数料を負担しているが、口座証明の発行に関しては、追加の費用負担となるため、申請者にとって手数料負担額が費用対効果の観点から、妥当な範囲内か検討・検証が必要である。

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

本ユースケースの実証を進めることで、以下の課題が判明したため、その解決方針に関する検討を行った。

課題①申請者の KYC について

本ユースケースでは、法人向け DID の発行を想定しているが、法人の存在確認に加えて、その法人の担当者であること、または個人事業者の場合はその本人であることの確認を取る必要が発生するため、自治体の住民情報をもとにした窓口での対面による本人確認を起点とするフローを検討していた。しかし、自治体を含めた各証明者に対するヒアリングを通じて、申請者証明者の双方にとって、手続きに要する時間の削減や事務コストの削減効果などが期待できる非対面による本人確認手法に関する検討が必要であると改めて認識させられた。

非対面での本人認証に関しては、自治体 J-LIS (地方公共団体情報システム機構) のコンビニ交付システムなどとの連携により、オンラインでの認証、住民情報 VC 発行なども、技術的には実現の可能性があるとされる。

また、公的個人認証サービス以外に、法人という視点で考えると、本ユースケースの証明者である、金融機関の本人認証 API やネットバンク ID の活用なども、法人認証として使用できる可能性があることがヒアリングにより判明した。法人の実在確認や非対面での本人認証は、本ユースケースのみならず

Trusted Web の社会実装において検討すべき課題であるため、上記に記した手法を含め、<今後の検討>が必要であると考え。

課題②証明者の KYC

本ユースケースにおける証明者は、自治体、税務署、金融機関であり、自治体、税務署は公的機関であるため事前登録等の手続きで証明者として認証することは可能である。金融機関に関しては、法人営業がない営業形態の場合、法人の实在確認機能が十分に果たせるかどうかの議論はあるが、一定以上の社会的信用があり、また数も限られているため、一定の審査基準などの策定が必要となる可能性もあるが、証明者として事前に認証を受けたものに限ることが可能であると思われる。

一方で、補助金・給付金においては、中小企業診断士等の有資格者が申請代行を行うことが考えられるが、<将来的には> 証明者として VC を発行することで、申請代行の機能を実現する予定であるが、上記の証明者と異なる認証体系、認定基準などの検討が必要であると考え。

また、ビジネスモデルの検討の項で、本ユースケースの社会実装には、エコシステム化が重要であると記したが、<将来的には> 民間事業者を含めた多様な証明者が参加するプラットフォームとなる必要があるため、証明する内容、信頼性精度などをもとに証明者の再定義、分類を行い、それぞれに見合った認証、認定基準、KYC 手法などの体制を整える必要があると考え。

課題③証明者のモチベーション、インセンティブ

証明者にとっては、Trusted Web の仕組みを活用した証明書の電子発行システムの導入により、証明書発行業務の事務処理の効率化が期待でき、地方の人手不足対策等に有効であるといった意見が聞かれた。

また、証明書発行手数料の収益なども魅力的と感じるという意見が多く挙げられたが、その一方で、新規システム開発、新規システムの導入は、コスト面と組織面両面で非常にハードルが高いという意見も多かった。また、補助金・給付金申請における証明書発行・流通の仕組みのみでの単体利用だけでは、証明者としてメリットは限定的で、積極的に導入を進めるメリットも薄いという印象を感じるという証明者が多く存在した。

これらの証明者からは、手数料収入等のインセンティブの提示より、様々な信用情報プラットフォームとしての拡張性などの将来性が示された方が、この仕組みへ参加するモチベーションが上がるという積極的な考えを持つ者が多く、社会実装に向けて手数料等のインセンティブを示すと同時に、Trusted Web の世界観、可能性に共感する証明者のモチベーションをアップさせ、これらを取り込んでいく必要があると考え。

課題④証明者及び申請先の業務システムとの連携

言うまでもないが、各証明者、申請先は証明書発行、授受を含めた情報管理のための膨大な既存システムを運用している。また、これらの情報の重要性から、セキュリティ対策を含め非常に厳しい運用基準を定めている。その状況下では、レガシーシステムの変更、及び新たなシステム開発や全く新しい仕組みを導入することに対して、コスト面のみならず、運用体制面、組織面のハードルが高く、導入には困難が伴

う。という実状についてヒアリングを通じて改めて認識した。

その一方で、特に金融機関はネットバンク等のオンライン化が進んでおり、本人認証のための API や相互接続のインターフェースなどが整備されており、これらを活用することで技術的にシステム連携を行うことは容易であると思われる。また、これらの API は全ての金融機関で異なるわけではなく、独自のものも含まれるが一定の種別、タイプに分けられるため、連携のためのシステム対応も比較的容易であると思われる。API 連携を想定した仕組みを作っていくことで、証明者の参加を促し普及に繋げていくことが有効な手法であるとする。

課題⑤VC発行プロセス

各証明者がVCを発行する際、特にコスト削減と効率化の観点において、VC発行プロセスは自動化されていることが望ましいと考えられる。一方、プロセスの自動化には一般的にシステムの初期投資が必要となるが、各証明者がそれぞれ初期投資を行うのでは無駄が多く実現性も低くなる。VC発行をSaaS化してサービスとして利用する形態が有効と考えられるが、VC発行を社会実装する上ではどのような形態においても、組織がVCを署名する際に秘密鍵をセキュアに扱う仕組みと運用方法の検討が必要である。

課題⑥システム面においては、エージェント同士の通信をセキュアに行う方法

3.4.7 で示した通り、＜次の展開として＞ DIDComm を使うことを検討しているが、エージェント同士の通信をセキュアに行う方法について＜今後の検討＞が必要であるとする。

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

本ユースケースの社会実装に向けて引き続き継続検討を進め、令和 7 年度以降の社会実装を目指す。

今後の対応① クラウド上で稼働するシステムの開発と検証（3.4.7 システムの構成要素を参照）

今後の対応② 社会実装に向けた調整 を以下のマイルストーンで実施する予定。

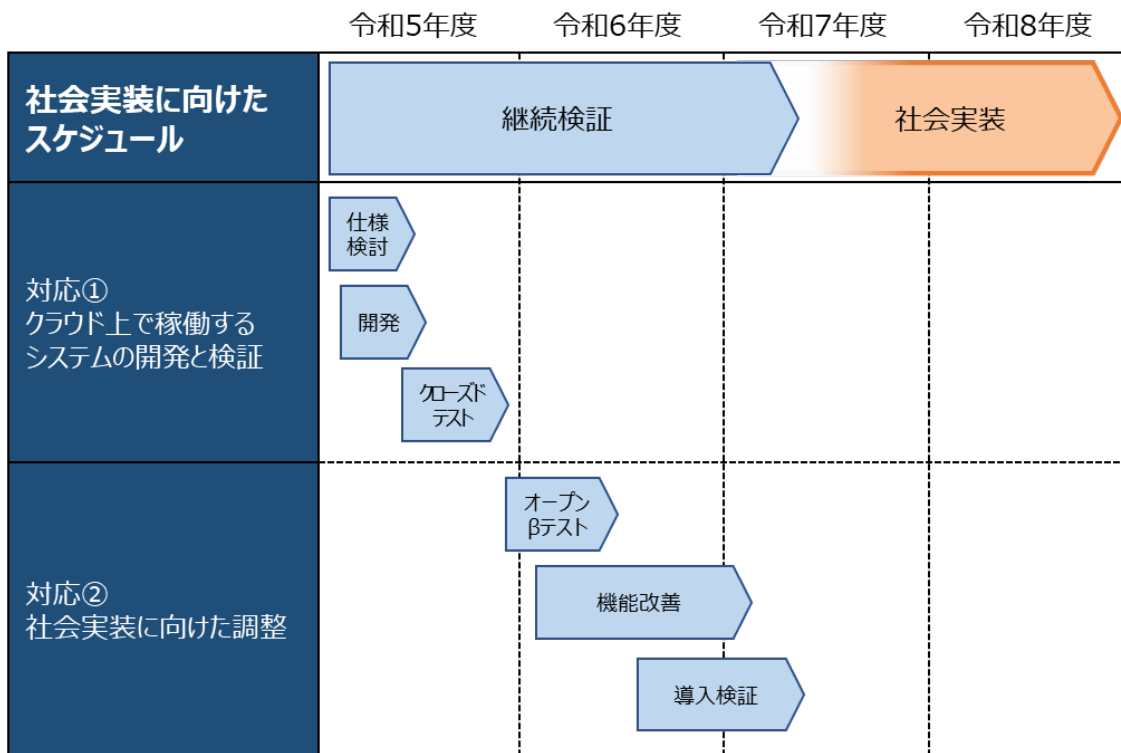


図 4.3 社会実装に向けたマイルストーン

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

Trusted Web のアーキテクチャに基づくシステムの実運用を行う際に必要なことの視点で、下記の課題を検討し、対応策を実装し検証する必要があると考えている。

課題① 秘密鍵が漏洩した時に具体的にどうするか？

課題② 秘密鍵を忘れた際にどのようにリカバリするか？

課題③ データは各エージェントにデータを保存する形をとっているが、何らかのアクシデントでデータが消失した場合にどのようにリカバリするか？

5.2 その他 Trusted Web の課題と提言

課題と提言① Trusted Web の実運用における KYC について

4.2 でも記したが、KYC については、本ユースケースのみならず Trusted Web の社会実装において不可避の課題であると考え。本ユースケースでは、申請者の KYC、将来的な証明者含めた証明者の KYC に関して考察を行ったが、非対面での法人認証、本人認証は、現時点ではその信頼性、汎用性に限界があること、対面での本人確認には時間やコストが掛かることから、決定的な手法一つに絞ることは難しい。

緊急性を要する大規模給付金や補助金の申請に使用できるような法人確認方法に関しては、発行手続き、発行までに要する期間、発行体制など、大量即時発行が可能な仕組みが存在していない。本ユースケースでは、申請者の本人確認を市区町村による対面での住民票発行により実施したうえで、各種証明を取得できることとしたが、非対面での本人確認や既存 KYC との連携など、より効率的な方法を検討する必要がある。

また、補助金申請においては、法人と代表者以外の申請担当者を紐付けることが必要となるケースが考えられるが、その手法に関しても確立されたものは存在していないため、非対面で効率的かつ安全性の高い手法を検討する必要がある。

その一方で、絶対的な KYC ではなく、証明する情報のレベルに応じた確認であったり、いくつかの証明情報や信用情報を積み上げることで、その DID の信頼性、信用度を高めていくような仕組みなども、Trusted Web の仕組みと親和性が高いのではないかと、証明者のヒアリング時に提言を受けたが、アナログをデジタルに置き換えただけではない、概念や構造的な変革をもたらすような仕組みとして、〈今後の検討〉が重要であると考え。

課題と提言② 利用者が、Trusted Web を意識することなく利便性を享受できる UX の実現

本ユースケースでは、中小法人、個人事業者のユーザー属性を考え、スマートフォンによる操作が可能な UI や、利用者、特に申請者にブロックチェーンや VC といった技術を意識させずに、その効果を実感し安心して利用してもらうため、わかりやすい VC 検証結果のアイコン表示などを提示した。また、複雑な補助金申請をできるだけわかりやすくするための UI/UX、スマートフォンで申請が可能な補助金申請手続きなども＜今後の検討＞課題であると考えている。

その一方で、本実証事業において、様々なユースケースの実証が行われ、今後、Trusted Web の社会実装が進んだ際には、Trusted Web 全体での UI/UX が、その世界観と共に理解され、受け入れられることが重要である。個々のシステムやサービスの使いやすさ、わかりやすさ以上に、Trusted Web 全体として、安心して使える、わかりやすい信頼情報流通の仕組みとなるための UI/UX ガイドラインの策定なども必要であると考えている。

課題と提言③ Trusted Web の本格導入・社会実装に向けて

本ユースケース本格導入に際しては、将来的な利便性の向上および総体的な事務処理コストの低減は見込めるものの、その前段階として、現行の窓口業務からデジタル上での受付・発行・その他手続きへの移行や、現行のレガシーシステム・ローカルデータベースとの連携・データ移行等、運用面・システム面での移行について各証明者や申請先（補助金・給付金事務局等）での移行コストは必ず発生するものと考えている。

上記のことから、人的・組織的要因、システム要因等の面から見ても、民間事業者等の働きかけのみでは証明者となる各機関等との調整は非常に困難であると考えられるため、Trusted Web の本格導入・社会実装に向けて、法令の整備、費用負担なども含めた国によるトップダウンでの政策実施など、行政と民間が一体となった推進体制の構築が重要であると考えている。