令和3年度補正予算Trusted Web共同開発支援事業費
「Trusted Webの実現に向けたユースケース実証事業」
最終報告書概要版

[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]

[電通・ISIDパブリックDXコンソーシアム]

2023年3月24日

目次

01

背景・目的

1.1 背景・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ＩＴ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、申請に必要となる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。

02

実証の概要

2.1 実証概要及び実証の範囲

事業スキーム

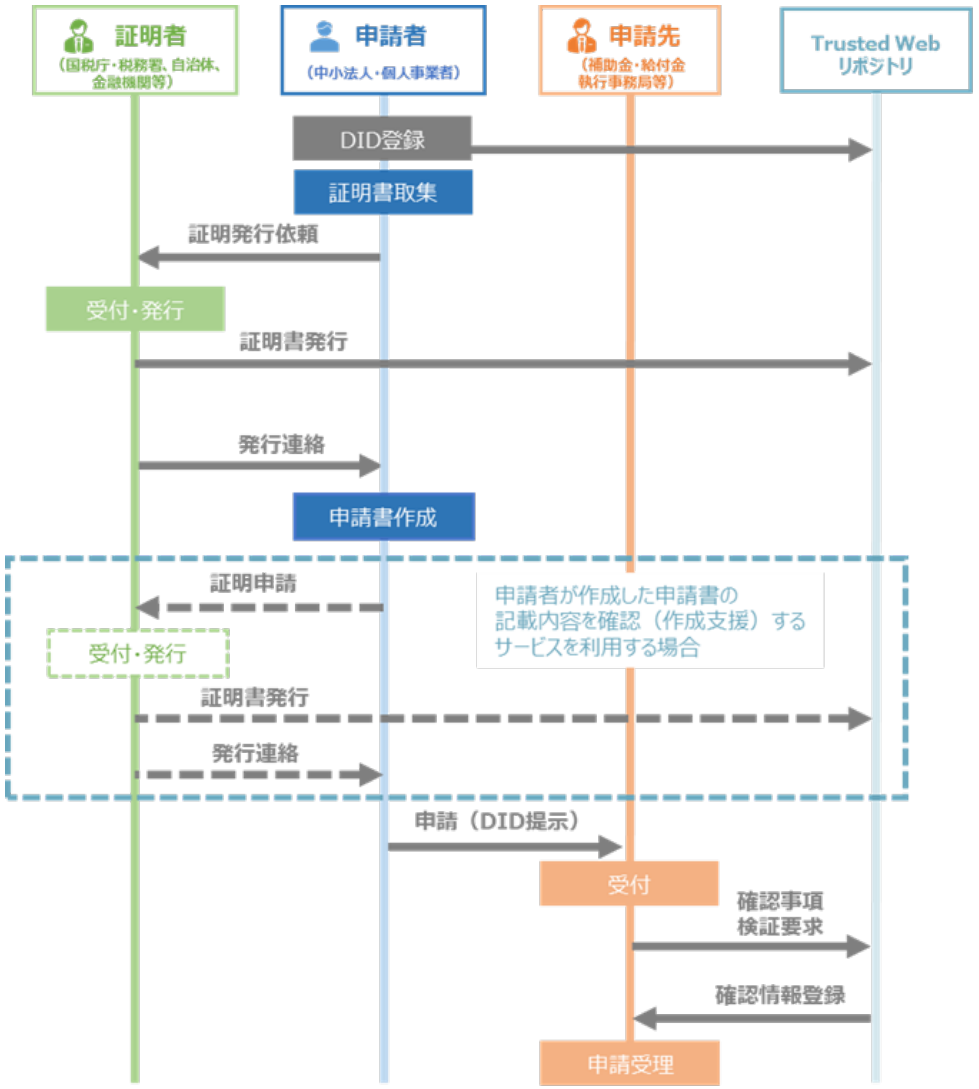
■本ユースケースにおける主体となる３者

申請者	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
証明者	国、自治体、金融機関
申請先	補助金・給付金執行事務局等

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右図の通りである。



2.2 社会・経済に与える価値・影響

社会・経済に与える価値・影響

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。

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、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。

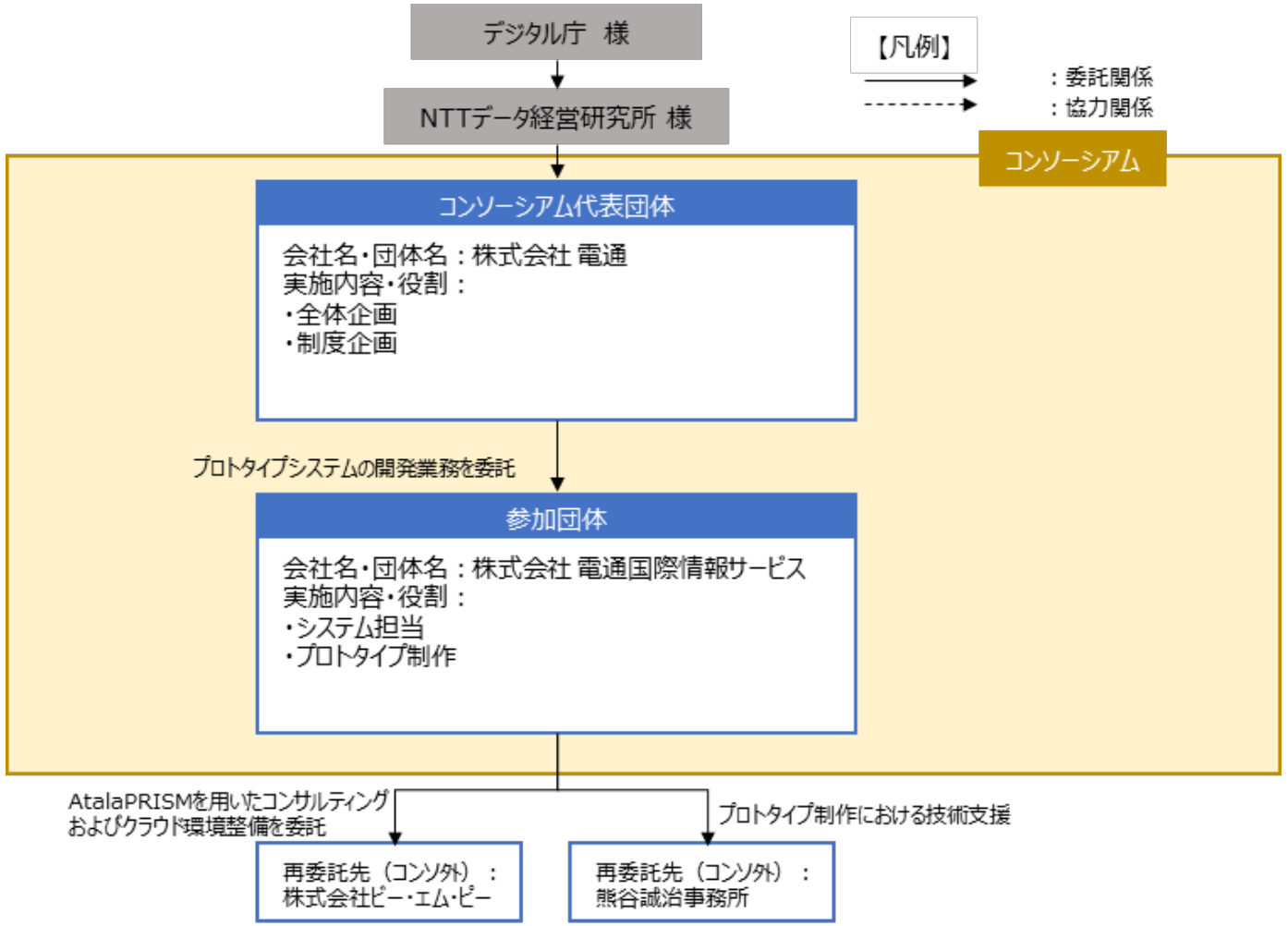
民間企業（金融機関など含め）における活用

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。



2.4 実証全体のスケジュール

実施事項					R4			R5		
大項目	中項目	小項目	担当	時期	10月	11月	12月	1月	2月	3月
プロトタイプシステム アーキテクチャ										
	DID/VC アーキテクチャ検討									
		設計	ISID	10/3-11/30						
		環境構築	ISID	10/17-11/30						
		環境設定	ISID	10/17-11/30						
		動作検証	ISID	11/1-11/30						
	システムアーキテクチャ検討（データの受け渡し・画面遷移）									
		設計	ISID	10/17-12/28						
		環境構築	ISID	10/17-12/28						
		環境設定	ISID	10/17-12/28						
		動作検証	ISID	11/1-12/28						
プロトタイプシステム開発										
	開発									
		画面設計	ISID	10/17-11/11						
		開発・チューニング（独自実装）	ISID	11/14-1/20						
		JWT対応（※R5 1月に追加）	ISID	1/23-3/3						
	テスト									
		テストケース作成	ISID	12/14-1/15						
		内部テスト	ISID	1/10-1/20 3/1-3/10						
		テスト	電通・ISID	3/1-3/10						
ユースケース検討										
	業務ヒアリング		電通・ISID	11/1-3/20						
	業務適用検討		電通・ISID	11/1-3/20						
納品対応										
	成果報告書の作成		電通・ISID	1/1-3/20						
	デモ動画の作成		電通・ISID	2/13-3/20						

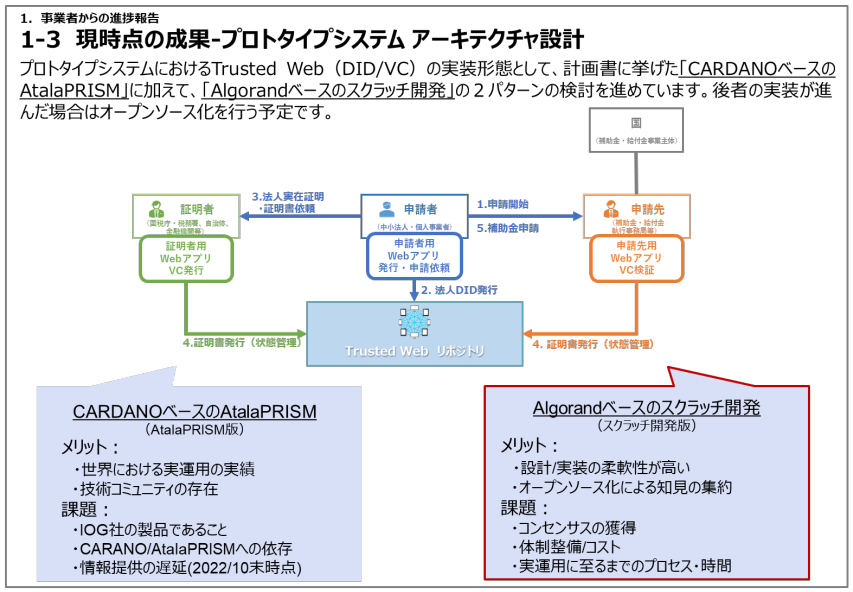
03

実証内容

3.1 実証の実施事項、論点及び判断

変更点 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。



Trusted Web定例報告資料より抜粋(2022年11月4日)

■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。

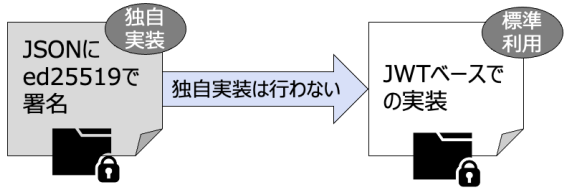
■Algorandベースのスクラッチ開発においては、Next.js[1]のStatic Site Generation[2]を利用してフロントエンドのみの開発にした。秘密鍵を暗号化してブラウザのローカルストレージに格納する仕組みにした。その際、XSS対策[3]等のセキュリティを考慮し、react[4]のコンポーネントを利用することとした。メッセージの形式は、当初JSONデータにed25519[5]署名を行っていた。

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

3.1 実証の実施事項、論点及び判断

変更点 プラットフォームに関する実施計画書からの変更点

メッセージの形式：
委員からのセキュリティリスクに関するご指摘により、独自実装からJWTベースでの実装に変更した。
独自実装していたプラットフォームをJWTベースでの実装に変更すると共に、本ユースケースのアプリケーションをJWTベースのプラットフォームに対応した。



■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、JWT[6](JSON Web Token)に対応する判断を行い、did-jwt[7]及びdid-jwt-vc[8]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。

メッセージを暗号化してやり取りする仕様（本実証の対象外）：
委員からのセキュリティリスクに関するご指摘により、独自実装は行わず、DIDCommベースでの検討を進める。
P2PパターンとMediatorパターンの選択は要検討。

P2Pパターン：Agent同士がメッセージをやり取りする
特定の事業者に依存しないが、各Agentがメッセージを喪失するなどした際の対応の検討が必要

Mediatorパターン：Mediatorを介しメッセージをやり取りする
特定の事業者(Mediator)に依存するが、P2Pパターンに比べてシステムの運用効率は向上する

■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、DIF[9]により仕様策定が進められているDIDComm[10]の採用を検討している。

図3.1.1 JWM[11]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

本最終報告書において、通常の記述は納品物のプロトタイプシステムに関するものとし、納品物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。

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
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

3.1 実証の実施事項、論点及び判断（1/3）

プロトタイプシステムの企画・開発

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

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。

システム開発

Figma[12]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。

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 実証の実施事項、論点及び判断（1/3）

プロトタイプシステムの企画・開発

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

実施したテストケースの例 (一部抜粋)

3.1 実証の実施事項、論点及び判断（2/3）

ヒアリングの実施

金融機関

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

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（国税庁・税務署）

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月上旬：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・給付金事務局

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

3.1 実証の実施事項、論点及び判断（2/3）

ヒアリング結果

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。

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

3.1 実証の実施事項、論点及び判断（2/3）

ヒアリング結果

■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、ある金融機関においては、新規システム開発・導入はハードルが高いが、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の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。

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。

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も多く寄せられた。

3.1 実証の実施事項、論点及び判断（2/3）

ヒアリング結果

■制度面（法令等の制度や組織面での課題など）

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（Trust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。

電子証明自体の法整備（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考える証明者も多くいる状況であった。
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。

3.1 実証の実施事項、論点及び判断（2/3）

ヒアリング結果

■技術面（既存システムとの連携、技術的課題など）

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。

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・得られた成果において、考察を進めることとする。

3.1 実証の実施事項、論点及び判断（3/3）

国際標準規格の調査

本実証で準拠・参考、及び今後検討する国際標準規格

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ケーターに関する仕様
準拠	Verifiable Credentials Data Model v 1 .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する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

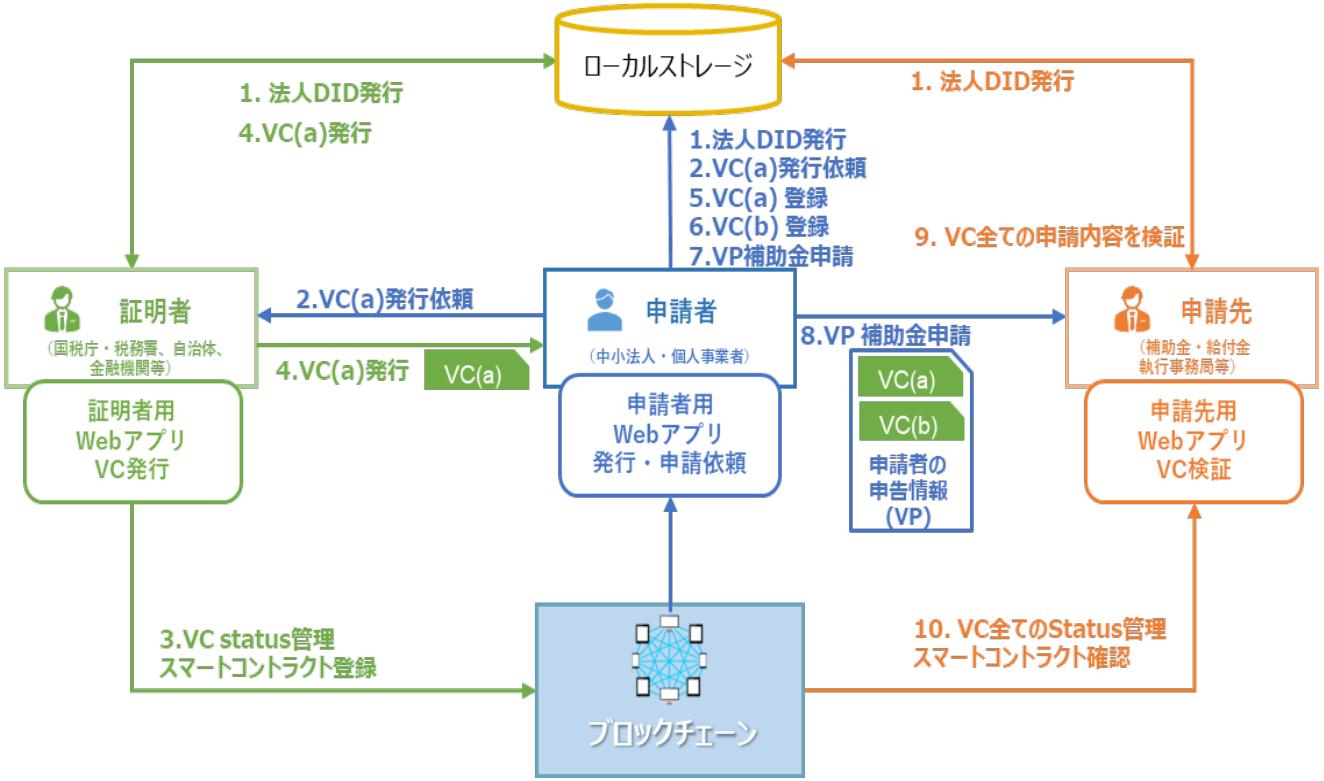
名称	引用
Decentralized Identifiers(DIDs) v1.0	https://www.w3.org/TR/did-core/
Verifiable Credentials Data Model v 1 .1	https://www.w3.org/TR/vc-data-model/
The did:key Method v0.7	https://w3c-ccg.github.io/did-method-key/
Well Known DID Configuration	https://identity.foundation/.well-known/resources/did-configuration/
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	

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。

3.2 検証できる領域を拡大する仕組み（1/3）

データフロー図



データへのアクセス

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にて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。

登場する主体とその概要

申請者　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

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。

証明者　国、自治体、金融機関

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り続けるため、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。

申請先　補助金・給付金執行事務局等

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。VP[13]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 検証できる領域を拡大する仕組み（2/3）

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JWS[14]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データの保有者：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

■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が確認できるため、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。

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

3.2 検証できる領域を拡大する仕組み（3/3）

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合意の取り消しの可否および方法：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

6構成要素		
検証可能なデータ	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書【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】
	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）
アイデンティティ	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）
	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:keyを用いて管理する。did:key[16]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。
	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。

16 公開鍵暗号化方式に基づく軽量なDIDメソッド

3.3 6構成要素との対応

6構成要素		
ノード	Walletの使用有無	既存のWalletではJWS[17](JSON Web Signature)形式の署名は可能であるが、X25519[18]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JWE[19]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。
	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。
	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
メッセージ	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。
	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

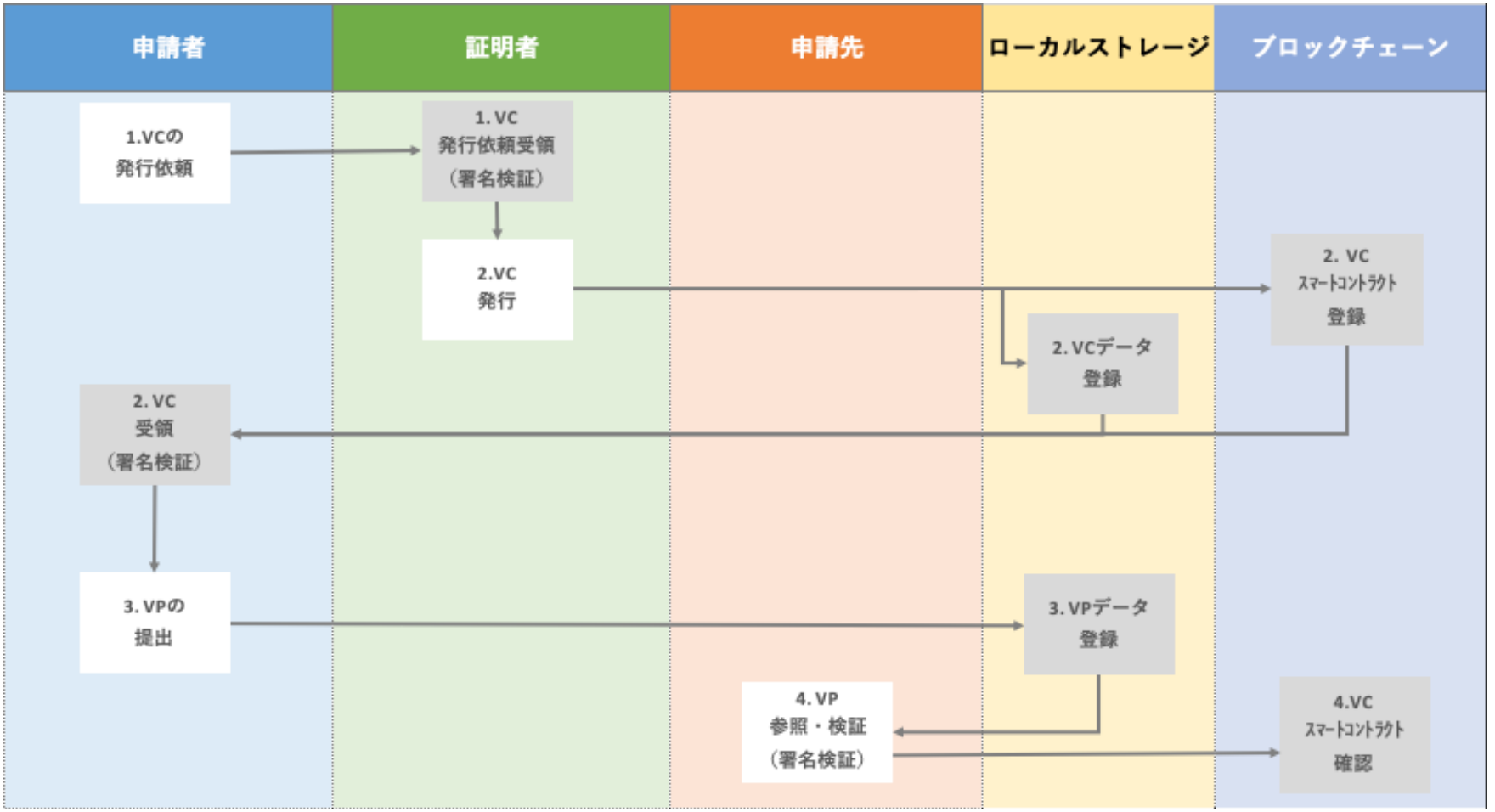
17 JSON Web Signatureの略称。JSONデータに署名するための標準規格
18. Curve25519を使った楕円曲線アルゴリズムの一つで、高速でセキュアな鍵交換に使用される
19. JSON Web Encryptionの略称。JSONデータをセキュアかつプライバシーが保護された形式でエンコードするための仕様

3.3 6構成要素との対応

6構成要素			
メッセージ	メッセージのデータモデル	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	④ 補助金申請VP ・ 住民票VC名 ・ 口座実在証明書VC名 ・ 納税証明書VC名 ・ 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
トランザクション	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。	
トランスポート	トランスポートのプロトコル	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。	

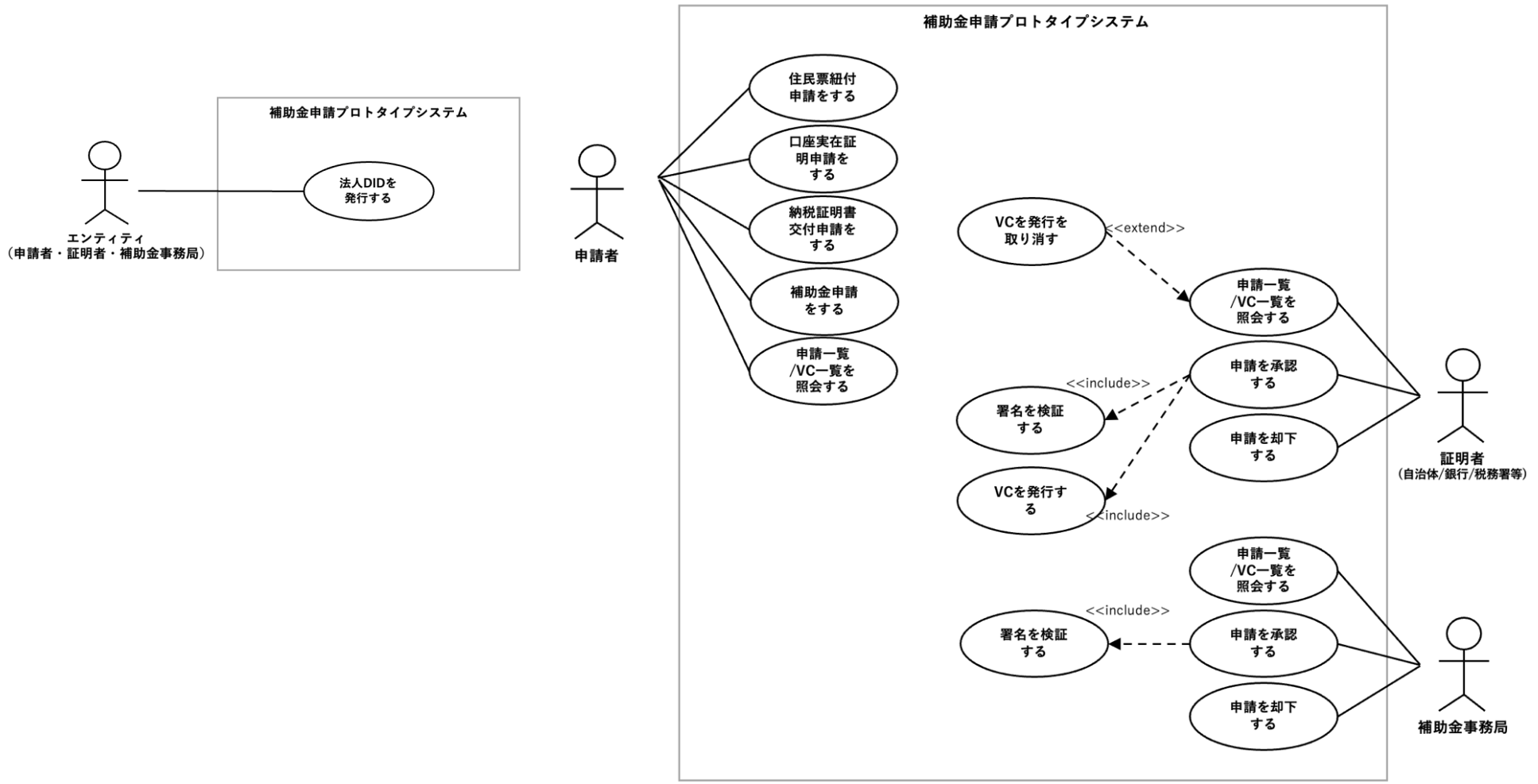
3.4 本実証で企画・開発したシステムの概要（1/6）

業務フロー



3.4 本実証で企画・開発したシステムの概要（2/6）

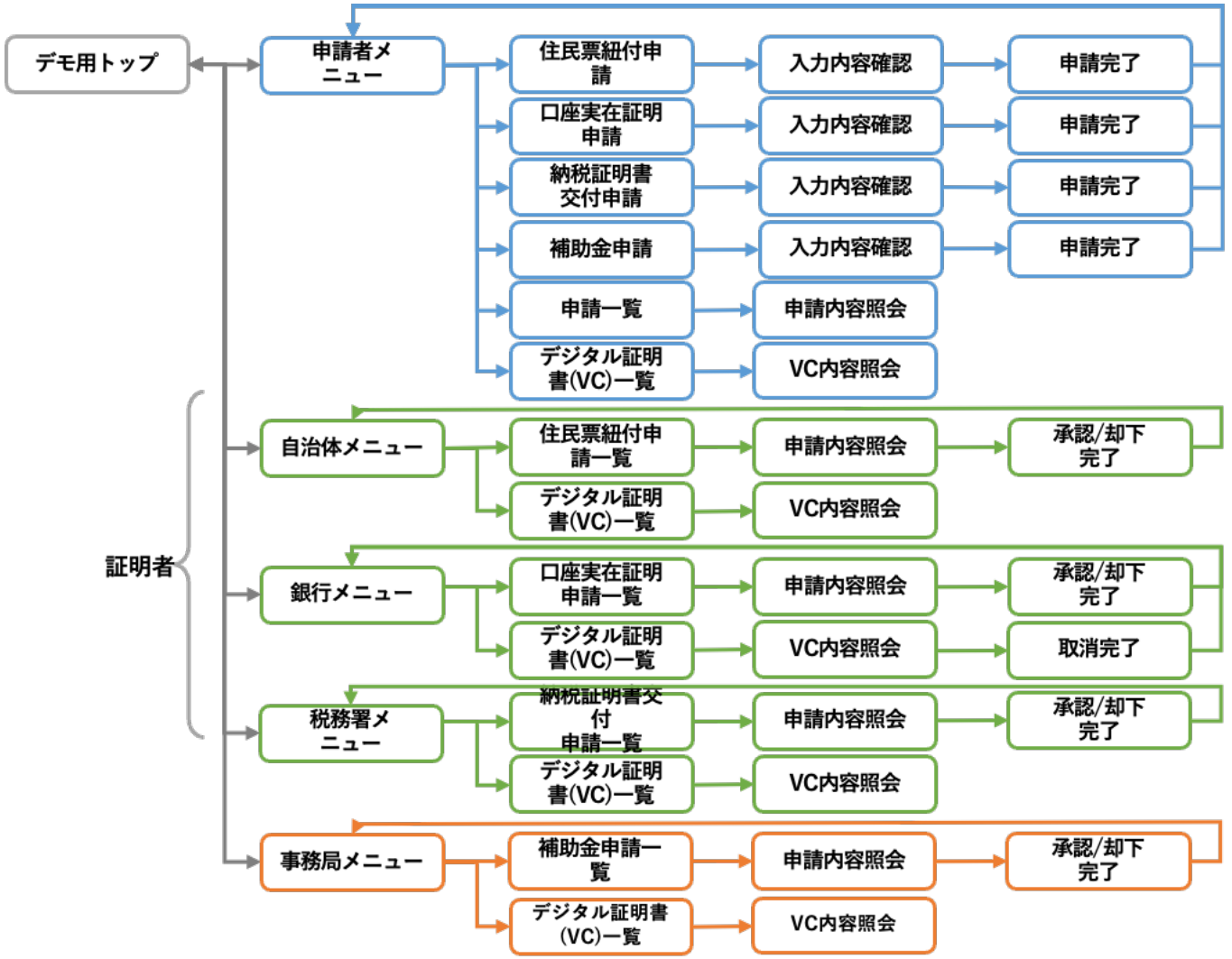
ユースケース図



3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）

画面遷移図（参考）



3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）

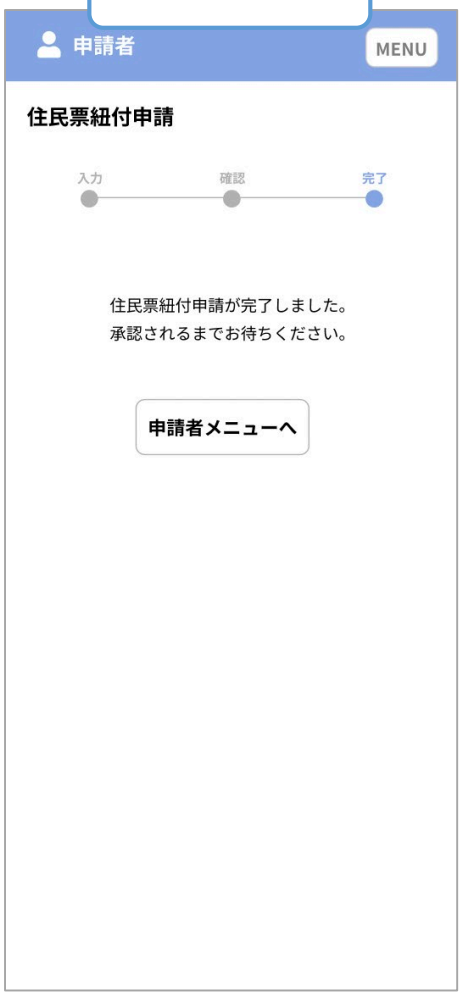
※本メニューはデモ用のため
ユーザーには表示されない想定

申請者

申請者メニュー

住民票紐付申請

申請完了



3.4 本実証で企画・開発したシステムの概要（3/6）

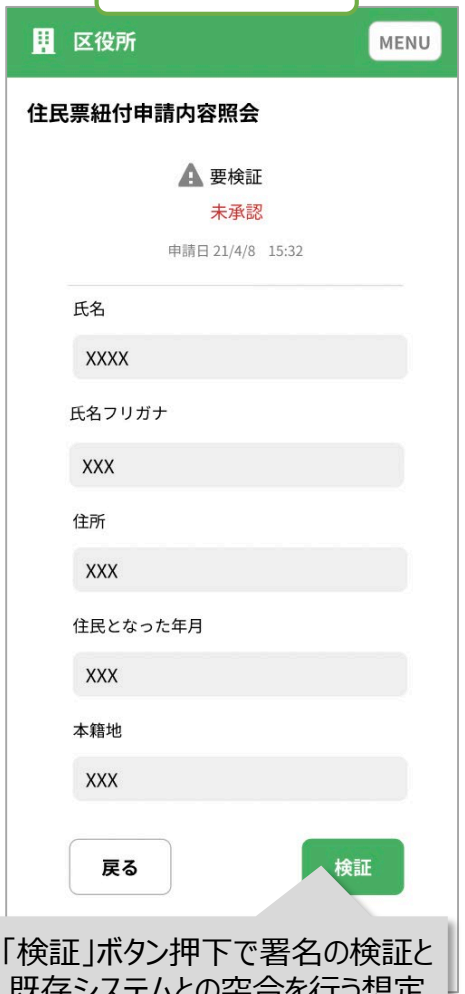
操作画面（UI）

証明者

区役所メニュー

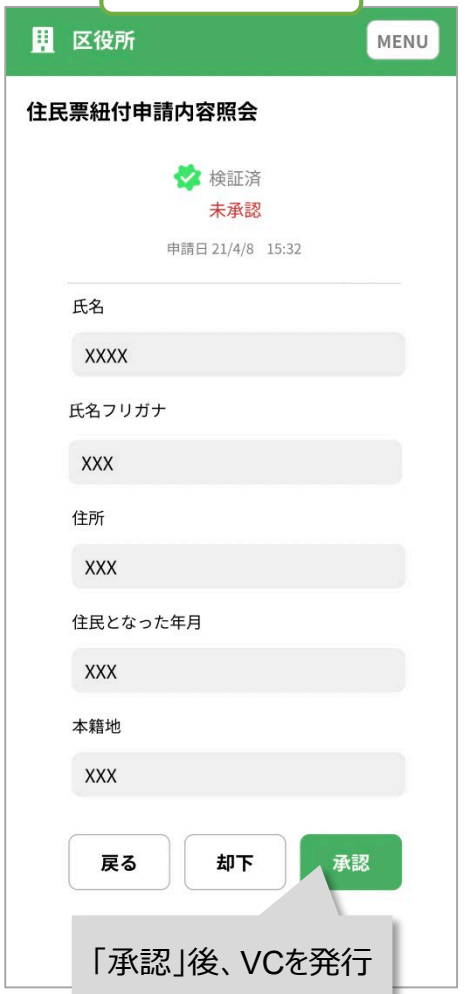
住民票紐付申請一覧

内容照会(検証前)



「検証」ボタン押下で署名の検証と既存システムとの突合を行う想定

内容照会(検証後)



「承認」後、VCを発行

3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）

申請者

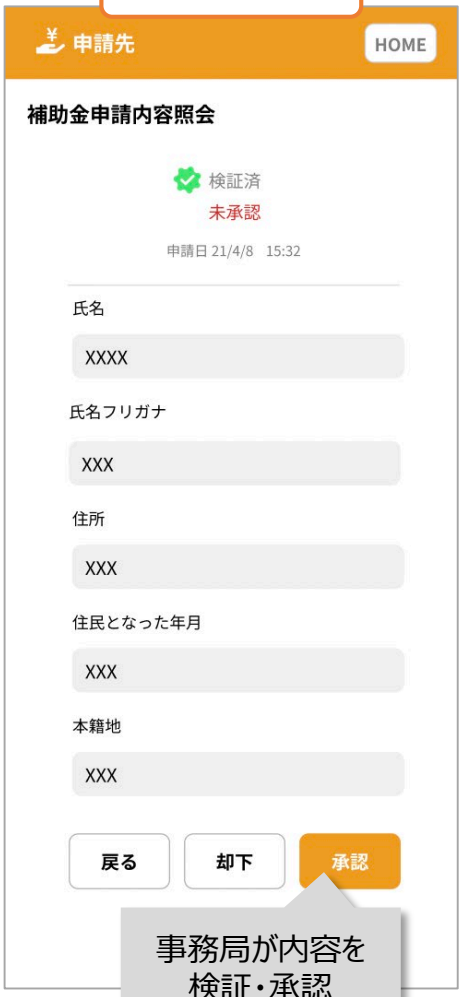
デジタル証明書(VC)一覧

補助金申請

申請先 (補助金事務局等)

補助金申請一覧

内容照会(検証後)



3.4 本実証で企画・開発したシステムの概要（4/6）

機能/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。

3.4 本実証で企画・開発したシステムの概要（4/6）

機能/非機能一覧

機能/非機能	機能名	機能概要
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	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。

3.4 本実証で企画・開発したシステムの概要（4/6）

機能/非機能一覧

3/3

機能/非機能	機能名	機能概要
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パスワードで暗号化している。

3.4 本実証で企画・開発したシステムの概要（5/6）

データモデル定義

1/2

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
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

3.4 本実証で企画・開発したシステムの概要（5/6）

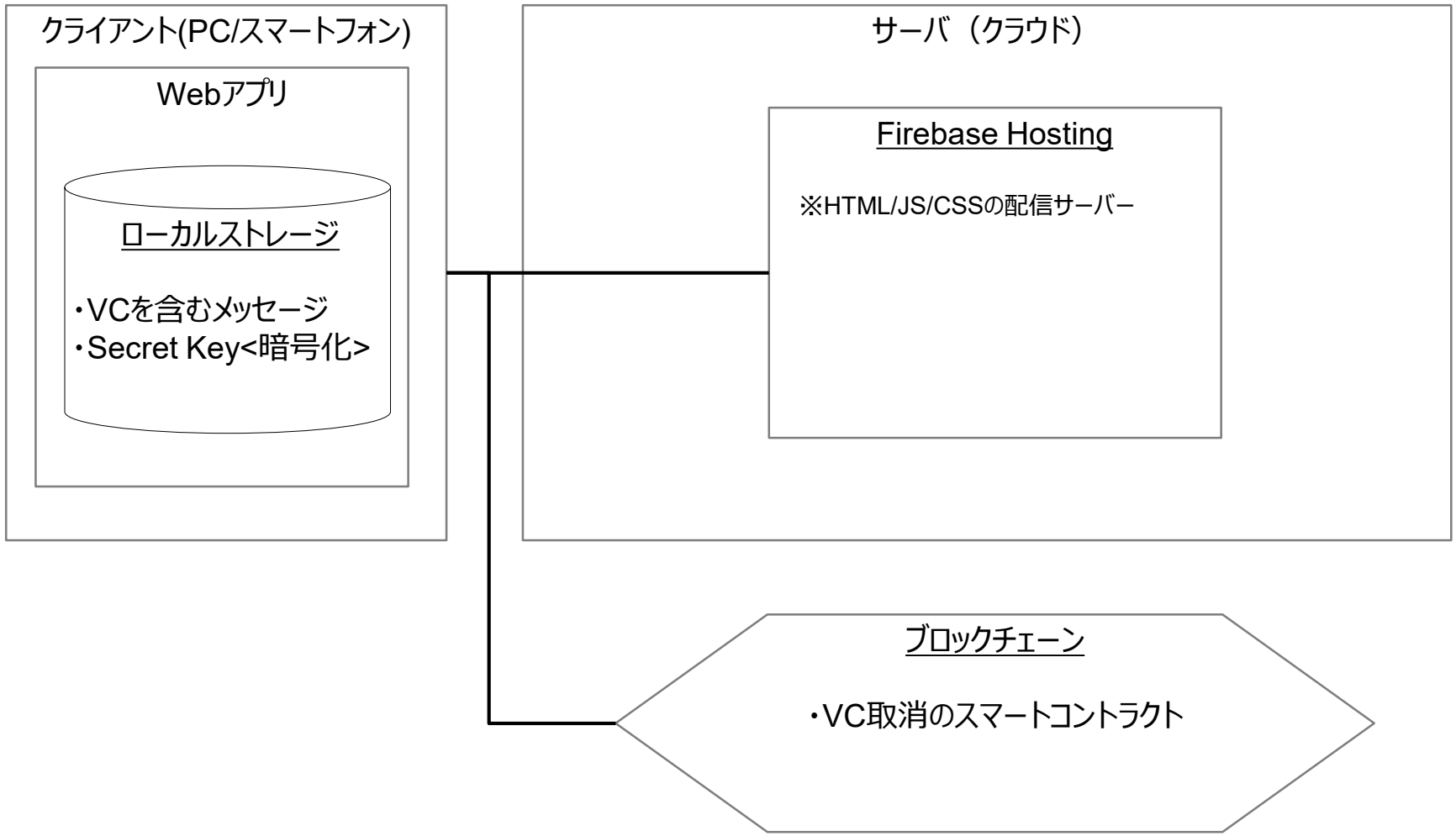
データモデル定義

種類	属性値	属性取得元	属性値（vc 内）
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 本実証で企画・開発したシステムの概要（6/6）

実験環境

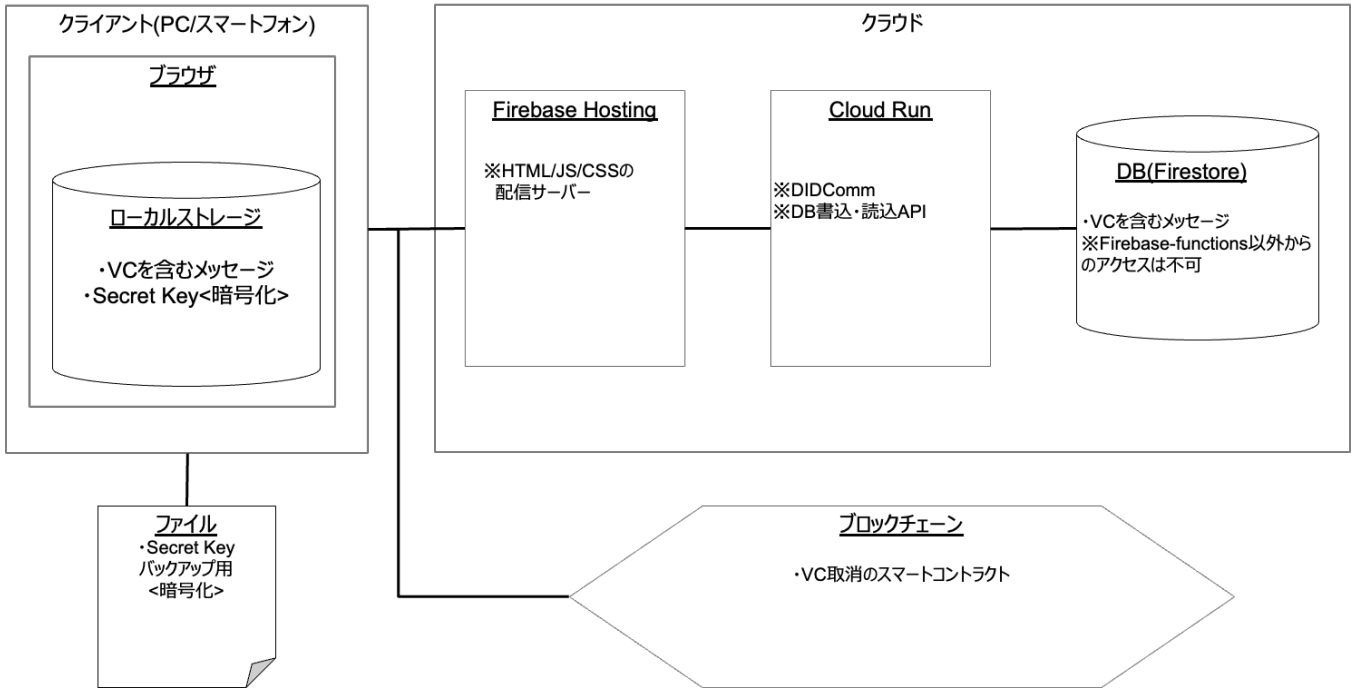
本実証スコープにて納品物とするプロトタイプシステムの構成は下図のとおり。



3.4 本実証で企画・開発したシステムの概要（6/6）

システムの構成要素

＜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。



主要な製品・ライブラリー一覧

本実証との関連	名称	OSSか否か	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

システムの企画・開発に関する成果

■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証をおこなった

・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。

ビジネスモデルに関する成果

■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、申請者、証明者、申請先にとって工数削減が期待できる。

補助金事務局にとっても人件費の削減が期待できるが、電子化の導入によりAIによる不正検知などのシステムコスト、サポート体制の拡充による運用コストが増加する。特に導入初期においてはトータルコストが増加することが想定される。

■証明者の手数料収入などのベネフィットについて

新規システム開発・導入はコスト面、運用面でハードルが高い。金融機関のネットバンク等の既存API活用により、技術的には比較的容易連携が可能であり、同時にネットバンクによる手数料徴収などの可能性も考えらる。

■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についての重要性

様々な信用情報・証明情報の利活用が可能な利用価値の高いプラットフォーム化による新しい価値の創造など、アナログからデジタルへの転換コストを上回るようなベネフィットの提示や、完全電子化などのトップダウン政策が必要。

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

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。

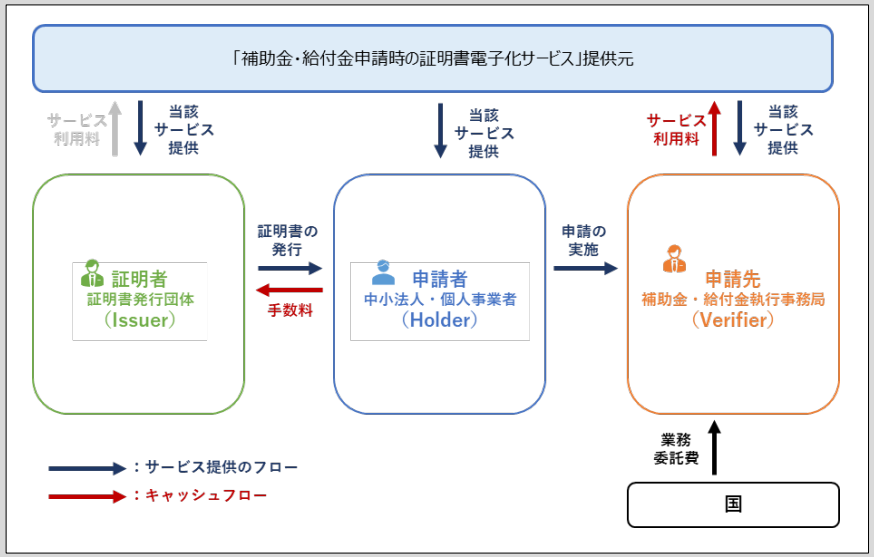
第三者による再現を安易なものとするため、手順書を用意した。

04

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

ビジネスモデル



ステークホルダ	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	証明書の電子化サービス利用料は負担しない。
申請者 （中小法人・個人事業者）	証明書取得に係る煩雑な手続きの簡略化	証明書1通につき手数料を負担（金額は証明書の種類によりことなる。）
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審査業務の効率化	事業の規模（想定申請数、期間等）により、補助金・給付金申請の電子化サービス利用料を負担。

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。

ユーザーのベネフィット

想定しているスキームでは、補助金・給付金を申請する者が、自治体・税務署・金融機関等の証明者に対してVC発行依頼を行い、補助金・給付金に必要なVCを取得したうえで補助金事務局に申請を行う。

■申請者たる中小法人・個人事業者は申請に必要となる各種証明書を従来は窓口で発行する必要があったが、Trusted Webでは証明書がVCに置き換わるため、窓口に出向く必要がないつでも発行依頼が可能。
（条件によっては、証明書の再利用も可能）

■証明者たる自治体、税務署、金融機関は各種証明書の発行作業およびその費用、また窓口対応が不要となるため、総体的な人的コスト、物理的コストの削減が可能。

■補助金事務局は、証明書データ添付・郵送等で受付・審査を行う必要がなくなり、申請データに付属しているVC情報から申請者の確からしさを確認することが可能。

このように、VCによる本人確認・実在確認が可能となることで、申請者・証明者・申請先のどのユーザも総体的な事務コストの低減を図ることが可能となる。

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

実証を進める上で課題となった点（開発面、ビジネスモデル面）と解決の方向性

■申請者のKYC

法人向けDID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、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、非対面での本人確認手法に関する検討が必要であり、金融機関の本人認証APIやネットバンクIDなどの連携は技術的には実現可能性が高い。

■証明者のKYC

自治体、税務署等の証明者については、事前に認証を行うことが可能。金融機関についても、一定上の信頼性が担保されていると考えるが、審査基準等の策定を検討。＜将来的には＞、民間事業者を含め、多様な証明者が参加するプラットフォームを想定しており、証明する内容、信頼性精度により、認証、認定基準、KYC方法を整える必要がある。

■証明者のモチベーション、インセンティブ

本ユースケースの活用により、証明者の事務処理効率化が期待できる。証明書発行による手数料収入も魅力的であるが、新規システム導入はコスト面、運用面、組織面でハードルが高く、補助金・給付金申請の証明書発行・流通だけでなく、拡張性・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。という積極的な意見も多く聞かれ、この層へアプローチし巻き込んでいくことが必要。

■証明者及び申請先の業務システムとの連携

新規システム導入の困難さをヒアリングを通じて改めて認識した。その一方で、整備の進んでいる金融機関の本人認証APIやネットバンクIDとシステム連携していくことが有効な手法であると考えられる。

■VC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、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。

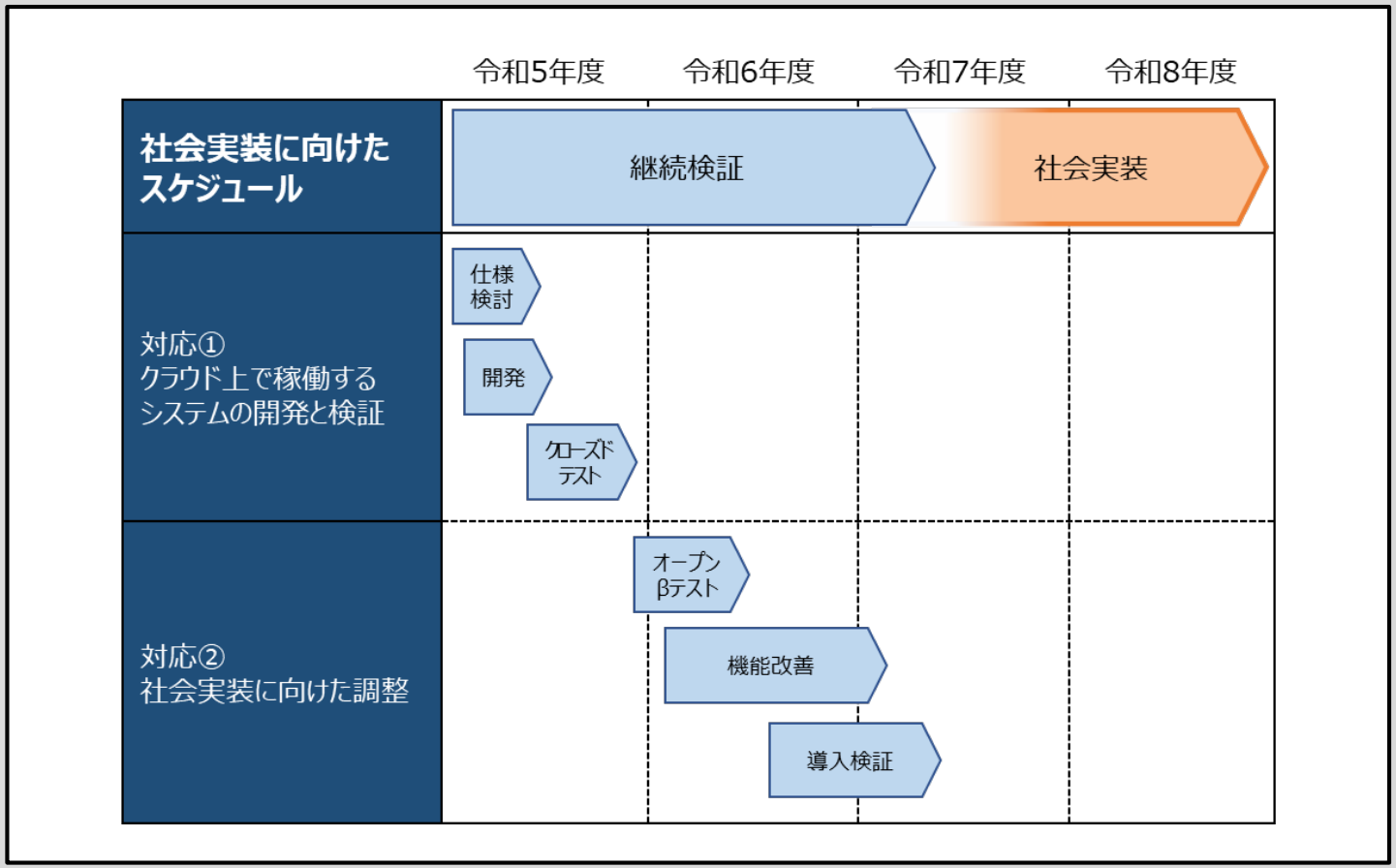
■エージェント同士の通信をセキュアに行う方法について＜今後の検討＞が必要

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。



05

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

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。

■秘密鍵が漏洩した時に具体的にどうするか？

■秘密鍵を忘れた際にどのようにリカバリするか？

■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

その他 課題と提言

■Trusted Webの実運用におけるKYCについて

・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る。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、非対面でのデジタルでの法人認証、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、住民票発行を申請者の本人確認として実施したが、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。

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と思われ、アナログをデジタルに置き換えただけでない、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る。

■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

・ 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（申請項目数の制限）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る。

5.2 その他Trusted Webの課題と提言

その他 課題と提言

■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る。