Trusted Web の実現に向けたユースケース実証事業
最終報告書　詳細版

「事業所 ID とそのデジタル認証基盤」
（サプライチェーンの信頼性を確保する異業種連携基盤として）

2024 年 3 月 15 日
SBI ホールディングス株式会社

目次

1．背景と目的

1.1 背景・目的

【背景】

欧州 GDPR に端を発するデータ規制の波が世界に広がり、わが国においてもデータのプライバシーへの対応やデータの信頼性確保は待ったなしの状況になっている。さらに製造業分野においては、EU 電子指令や ESPR 等、サプライチェーンに大きな影響を及ぼす規制の流れが押し寄せてきている。

このような事業環境の変化に対応するため、わが国が提唱した Data Free Flow with Trust（DFFT）の考え方に沿った形で、異業種間連携を容易にする新たなデータプラットフォームを構築する時期が来ている。Industry4.0 や Society5.0 の実現に向けた検討が進行する中、事業所 ID およびそのデジタル認証の基盤を構築・提供することによりその基盤に接続されている誰もがデジタルで実在性が保証され安心して取引を行うことができるようになることから、DX 化が大幅に遅れている中小企業等をも含めた業種・業界横断での包括的なデータ連携の取り組みが容易になると考える。

上記のような課題認識のもと、令和 4 年度には（一財）インターネット協会が「半導体産業に於けるサプライチェーンの信頼性確保に関する国際標準化調査」を経済産業省より受託、その活動を通じて、サプライチェーントレーサビリティを実現するための事業所 ID およびデジタル認証の利用方法について仮説をたてその有効性について調査・検証を行った [1]。その結果、事業所 ID やデジタル認証の技術だけではなく、国家間の相互承認の制度、国際標準化といった、実用化のための枠組みや手続きをトータルで整備が必要であることが明らかになった。

【目的】

ブロックチェーン技術を利用してサプライチェーン情報をトレースする取り組みは既にいくつか行われているが、トレースする対象物の真正性を証明するための技術開発が中心であり、サプライチェーンの参加者（トレース情報を記録する主体）である事業者・事業所の真正性についてはプラットフォーム運営者の確認に依存している状況。業界・業種を横断したサプライチェーンの信頼性確保には、事業者・事業所の真正性を担保する国際的にも通用する仕組みの構築が必要になる。

以上を背景として、インターネット協会 OIC に設置した BRP コンソーシアムでは、半導体製造や ICT 機器導入といった実際のサプライチェーンを担うユーザーや団体と連携し、国際的なルール作り、システム基盤構築、運営管理機関整備等の検討を進めている。

[1] 国際標準化委員会 WG 主査：SBI ホールディングス藤本（ISO/TC292/SG3 国内委員）

2. 事業の概要

2.1 登場する主体と概要

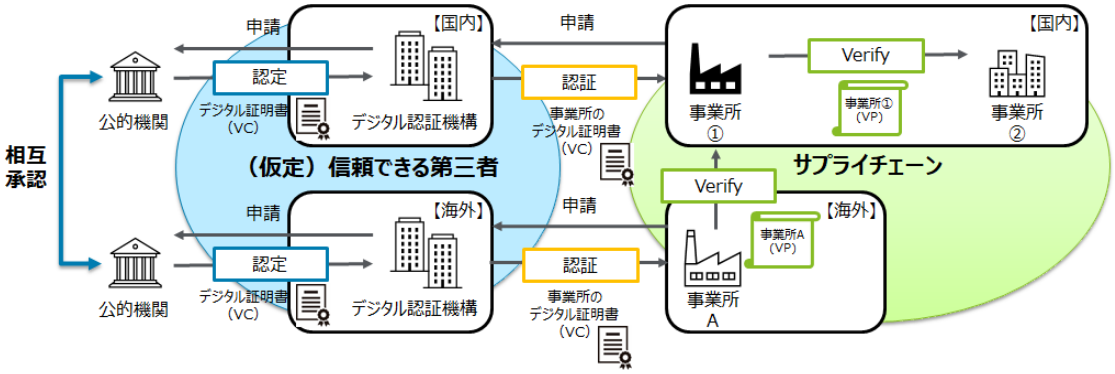


図 2-1-1：登場する主体と概要

■ 公的機関

1. 法律に基づき自身もしくは指定した機関を通じ、信頼できる第三者であるとしてデジタル認証機構を認定し、公的なデジタル証明書（VC）を発行する。

■ デジタル認証機構

1. 発行サービス
   - 事業所の事業所（VC）の発行申請を受領後、申請情報に基づき事業所の実在性を確認し、問題がなければ、事業所（VC）を発行する。
   - 定期的に当該事業所が存在しているかを確認し事業所（VC）を更新する。
   - 確認できなかった場合、事業所（VC）を取り消す。
1. 失効管理サービス
   - 事業所（VC）の有効性確認は、利用頻度が高いと想定し、発行サービスと別サーバとする。
   - 事業所（VC）の有効性確認に対し、有効/無効を回答する。

■ 事業所

【役割】

1. 事業所間で製品の受発注がある場合、サプライヤーがバイヤーに対して自身の実在性を証明するため、サプライヤーの事業所（VC）を含んだサプライヤーの事業所（VP）をバイヤーに提示し、バイヤーはその事業所（VP）を Verify することでサプライヤーの実在性を確認する。

【課題】

2. 事業所の実在性を証明するものが自己署名の場合、本当に正しいか証明することが難しい。

2.2 現状の課題を解決する事業スキーム案

従来のサプライチェーンネットワークは最終製品の製造者の下に 1 次サプライヤー、1 次サプライヤーの下に 2 次サプライヤーというピラミッド型の構造をしているケースが多く、参加者がある程度固定化されていたこともあり、それぞれのピラミッドで最適化されたクローズドな（その結果としてサイロ化された）情報ネットワークとなっていた。

クローズドなネットワークで取引先が固定化されている前提であれば、取引先のアイデンティティ確認は取引開始時のみで十分であったが、今後、サプライヤーが複数のサプライチェーンネットワークに参加するケースや、サプライヤーが案件毎にダイナミックに代わるようなケースが増えてくる場合、各参加者のアイデンティティを都度容易に確認できることが必要になると考える。

今回の実証では、信頼できる第三者が事業者・事業所の実在性を認証してデジタル証明書を発行することにより、取引先のアイデンティティ確認が容易にできるようになり、それをベースとして信頼できるサプライチェーンネットワークが実現されることを目指している。

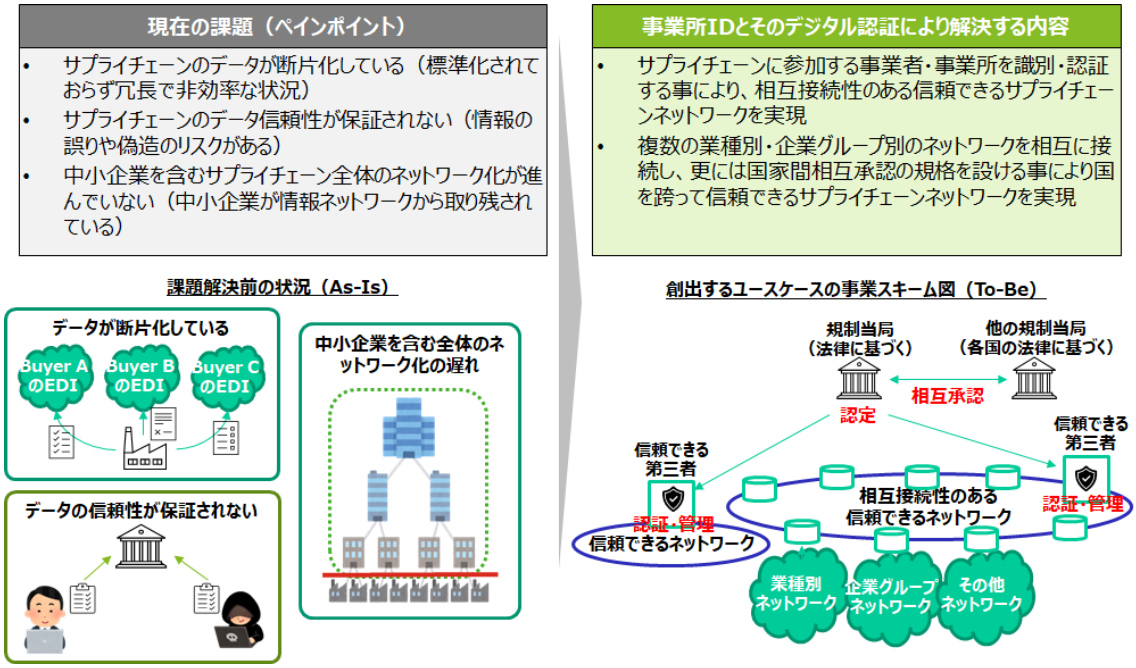


図 2-2-1：現状の課題を解決する事業スキーム案

2.3 社会・経済に与える影響・価値

2008 年の米国政府調査[2]で防衛装備品に含まれる電子製品に偽造半導体が使用されている事例が多数（年間約 9,000 件）判明、これを受けて国防授権法などにより米国に輸入される電子製品・部品等に対する検査が厳しくなっている。

また、2019 年の OECD 調査によれば、偽造品・模倣品は世界全体の貿易の 3.3%を占めており、2016 年には 5,000 億米ドルと算出され年々増加傾向にあり対策は待ったなしの状況となっている。

事業所 ID とそのデジタル認証基盤を用いてサプライチェーンの信頼性を確保することにより、偽造品・模倣品排除だけでも大きな経済効果が期待できる他、サプライチェーンのトレーサビリティ（川上まで遡ったサプライチェーンの見える化）実現によって、製品・サービスにおいて利用されている原材料情報の見える化や、付帯する温室効果ガス排出情報の見える化が容易となる。

また、EU 主導により導入された化学物質に関する規制（RoHS 指令、REACH 規則）に続き、欧州で 2024 年から順次適用される電池規則や、エコデザイン規則案（ESPR）その延長線上にある DPP（Digital Product Passport）など次々と提案される規則においてサプライチェーンおよび製品・サービスの信頼性に対する要求が益々高まっており、今回の実証事業で提案する仕組みおよびそれと表裏一体で進める国際標準化によって、これら規制への準拠や検証に要する時間とコストを低減する事も期待される。

グローバルなサプライチェーンの信頼性確保と見える化は経済安全保障の観点からも重要なテーマであり、さらに日本が提唱しリードする DFFT の実現に向けた新たなルールメーク（技術基盤構築および国際標準化）にも貢献できる取り組みになるものと考える。

---

[2] U.S. Department of Commerce. "Defence Industrial Base Assesment: Counterfeit Electronics." https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file

■　本取り組みの背景と期待値

EU 主導による EU バッテリー規則や、エコデザイン規則案（ESPR）その延長線上にある DPP（Digital Product Passport）など次々と提案される規則においてサプライチェーンおよび製品・サービスの信頼性に対する要求が益々高まっている。その中には、プロダクトに含まれる部品や原材料の製造者および製造場所（製造国）の項目があり、国際的な取引においてデジタルで信頼できる製造者・製造場所（製造国）情報が必要となってくるものと考えられる。

今回の実証事業で提案する仕組み、およびそれと表裏一体で進める国際標準化によって、これら規制への準拠や検証に要する時間とコストを低減し、製品の構成要素（BOM 情報等）および品質保証情報等の真正性を保証する一助となる事が期待される。

■　社会的価値

1. 事業所のデジタル証明により、事業所間でやり取りする情報（Information）の真正性を保証
2. 信頼できる第三者の認証による業界・業種および国をまたがるサプライチェーンの信頼性向上
3. サプライチェーンの参加者がデジタルでトレース可能になることによる偽造品・模倣品の排除

■　経済的価値

1. 信頼性を担保するために必要とされる様々な対策コストの低減
2. 情報の改ざんや偽造品・模倣品の混入が発覚した場合の被害および対応コストの低減

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

Value Proposition
企業が顧客に提供できる価値

- 第三者による真正性が保証されたデジタル証明書を付与することで
  - 取引相手の信頼度が向上
  - 出荷検査時、製品ロットに製造者の保証を追加

Customer's Segment
顧客セグメント

- 製品のサプライヤー

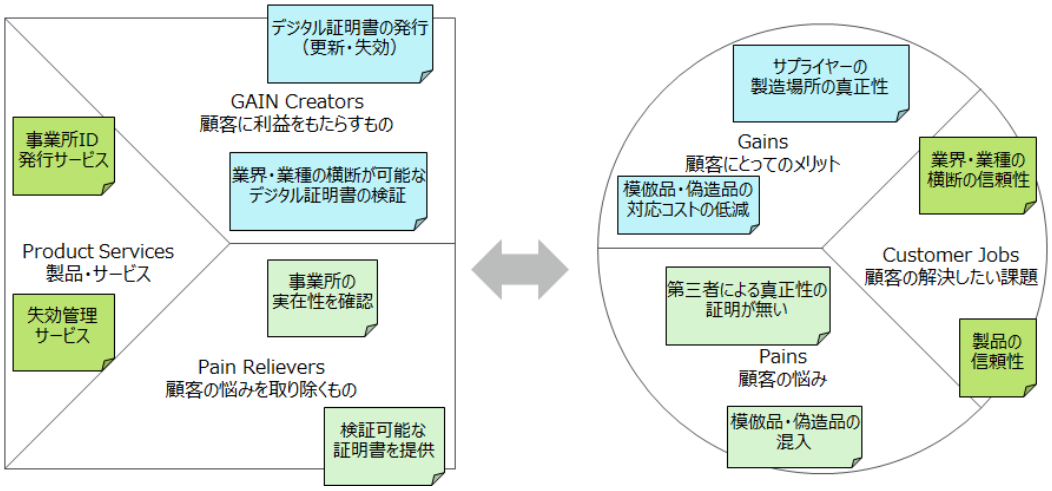


図 2-4-1 : Value Proposition Canvas

3. 本実証事業における検証計画

3.1 実証事業で明らかにする論点への導出・経緯

実証事業計画や有識者の指摘の中から、本実証で明らかにする論点を説明する。

■ アーキテクチャ

1. 広く利用するための汎用的なアーキテクチャはどうすべきか検討する。そこで、事業所（VC）を容易に利用する仕組みや利用者が継続的に利用する仕組みを検証論点として設定し、事業所（VC）の発行・スケーラビリティ・耐障害性・アーキテクチャ観点で検証・検討を行った。
2. 事業所（VC）のアーキテクチャを検討する際、X.509 の利便性と VC のスケール性について、両者を組み合わせた場合、信頼できる第三者が発行した事業所（VC）と X.509 の組み合わせで事業所の実在性が証明できるかについて検証論点として設定し、本実証では、デジタル認証基盤に参加するパーミッションドネットワーク（X.509）と事業所のオープンネットワーク（DID/VC）の組み合わせについてユースケースを通して、適合性可能性を検討する。
3. VC のライフサイクルの期間をどのように設定すべきか、VC のライフサイクルの実現可能性を検証論点として設定し、本実証では、有識者ヒアリングを行い、実現可否の検討結果を報告する。

■ 標準化

1. NIST SP 800-63」第 4 版ドラフトや、IAL に関しては「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」改訂に向けた中間とりまとめ（改定に向けた中間とりまとめ （digital.go.jp））を確認し、eIDAS の分類を再検討する。事業所 ID は法人向けだが、 SP800-63 の IAL や eIDAS は主として対象が個人向けになるため、海外参考事例として報告する。
2.

■ ビジネスモデル

1. サプライチェーンに伴う情報を流通させるにあたり、業界・業種を跨いだ事業所間で情報を記録する主体の真正性を担保する仕組みをどうすべきか検討する。そこで、事業所（VC）を発行する際、申請者は、事業所あるいは事業所が所属する法人等にどのような単位があるかを検証論点として設定し、事業所単位で事業所プロファイルを添えてデジタル認証機構に申請できるか検証を行った。

■ ユースケース

1. サプライチェーンに伴う情報を流通させるにあたり、業界・業種を跨いだ事業所間で情報を記録する主体の真正性を担保する仕組みをどうすべきか検討する。そこで、業界・業種を跨いだ取引先の情報を入手する場合、自己証明した情報を信頼できるか検証論点として設定し、信頼できる第三者が証明した事業所（VC）を使って取引先の実在性が確認できるか検証を行った。

2. サプライチェーンに伴う情報を流通させるにあたり、国を跨いだ事業所間で情報を記録する主体の真正性を担保する仕組みをどうすべきか検討する。そこで、国境を跨いだ取引先の情報を入手する場合、自己証明した情報を信頼できるか検証論点として設定し、他国における信頼できる第三者が証明した事業所（VC）を使って取引先の実在性が確認できるか検証を行った。
3. 例えば、デジタル認証機構について、既存の認証局に組み込むのが良いのか、欧州の考え方を取り入れていくのが良いのか、デジタル認証機構の社会実装に向けた枠組みを検討することを検証論点として設定し、ユースケース実現案で報告する。

■ 非機能

1. デジタル認証基盤への攻撃により、事業所（VC）の発行や無失効確認等、サービスが停止した場合、セキュリティについて、脅威モデルを検討し、その上で、システムのセキュリティリスクを評価して、必要な場合はアーキテクチャを分けることを検証論点として設定し、7.1 残課題対応方針一覧で報告する。
2. デジタル認証基盤への攻撃により、事業所（VC）の発行や無失効確認等、サービスが停止した場合、スケーラビリティについて、バックエンドのプライベートブロックチェーンに関する内容を補記すること、また、VC 登録依頼 API と提供 API が同時に落ちた場合の対応について検証論点として設定し、7.1 残課題対応方針一覧で報告する。

3.2 本事業におけるスコープ

事業所の実在性を保証する事業所 ID[3]を使って、事業所の真正性だけでなく、サプライチェーン上を流通する情報の真正性を保証することで、サプライチェーンの信頼性が向上し、信頼性を担保する様々な対策コストが低減される。

1. 信頼できる第三者が認定した事業所（VC）を発行する。
2. 提示する際、事業所（VC）の所有者の意思で相手に事業所（VC）を提示していることを証明するため、事業所（VC）を包んで自己署名した事業所（VP）を作成し、相手は事業所（VP）を使って信頼性を Verify する。

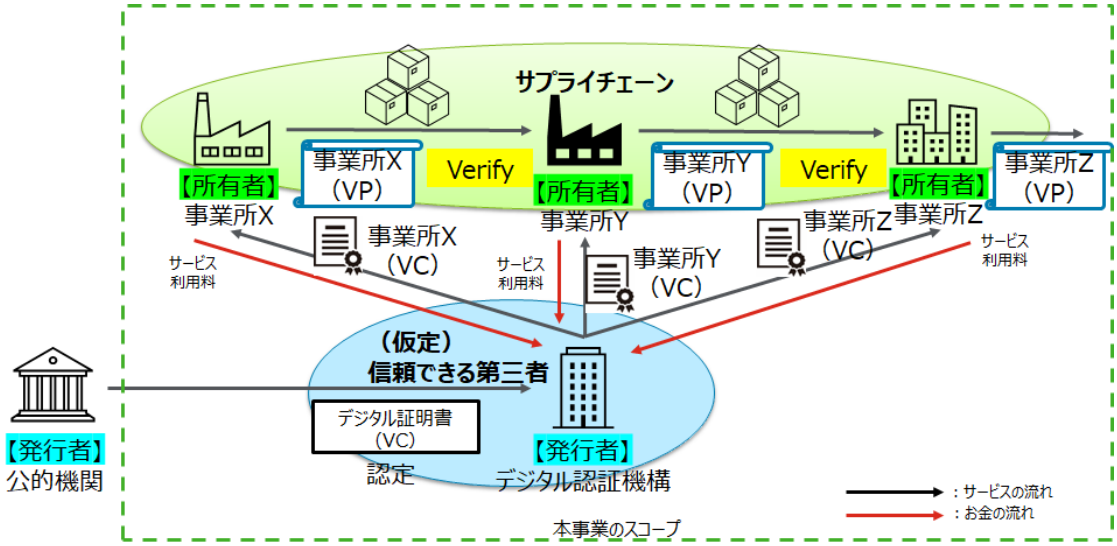


図 3-2-1：本事業のスコープ

[3] 事業所 ID とは、事業所の Identity を証明するデジタル証明書（Verifiable Credentials）。以下「事業所（VC）」とする。

3.2.1　事業所（VC）のライフサイクル

1. デジタル認証機構における、事業所（VC）のステータスは有効/無効の 2 種類あり、デジタル認証機構が失効すると事業所（VC）のステータスが無効になる。
2. 事業所（VC）のステータスの有効/無効は、「デジタル認証基盤」の仕組みが存続する限り、確認可能。

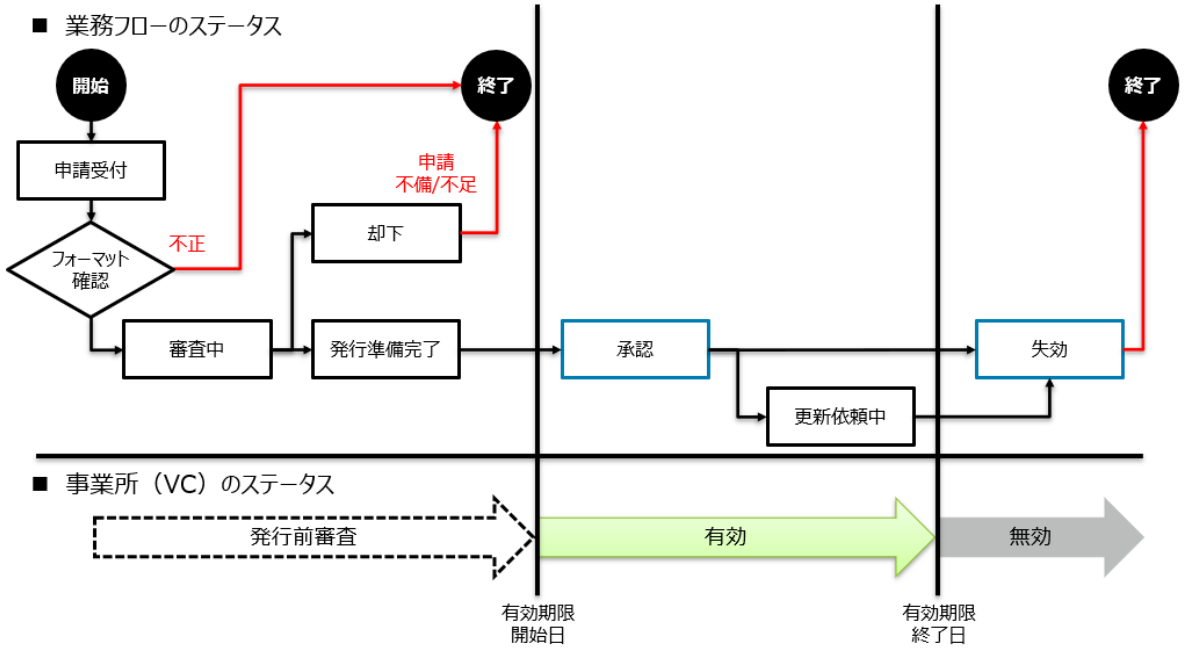


図 3-2-2：事業所（VC）のライフサイクル

3.2.2　事業所（VC）発行

1. 事業所（VC）の申請条件
   ① 申請を行うことができる者は、事業所（VC）を利用する法人（以下、申請者）とする。
   ② デジタル認証機構は、フィッシングまたはその他の詐欺的使用の疑いあるいは懸念を理由に、以前に失効した証明書および以前に拒否した証明書要求をすべて含む内部データベースを保持し、この情報を使用して、以降の疑わしい証明書要求を識別するものとする。
2. 事業所（VC）の申請手続
   ① 申請者は、申請する DID を作成する。
   ② 申請者は、申請に必要な申請者情報をデジタル認証機構に提出する。
   ③ デジタル認証機構は、証明書ポリシーや認証機構運用規定[4]に基づき、申請者情報を審査する。
   ④ 審査の結果
      (ア) 承認した申請に対し証明書を発行し、申請者に審査終了および証明書発行について通知する。
      (イ) すべての項目の審査が正常に完了しない証明書の申請は却下する。
3. 事業所（VC）の発行
   ① デジタル認証機構は、審査終了後、事業所（VC）を発行する。
   ② デジタル認証機構は、申請者に対し、発行通知する。
4. 事業所（VC）の受領確認
   ① API を使った申請に対し、発行のレスポンスを返すことで、申請者が事業所（VC）を受領したこととする。

表 1-2-1：申請者情報

事業所の DID	事業所の情報	事業者の情報
DID Document ● 事業所の DID ● 事業所の公開鍵	● 事業所名 ● 事業所の所在地国 ● 事業所の所在地	● 事業者名 ● 事業者の所在地 ● 事業者の識別子（法人番号等）

[4] 詳細は「7.2.3 ガバナンス・ルール案」を参照

3.2.3　事業所（VC）失効

■　説明

事業所が、デジタル認証機構の失効管理サービスに事業所（VC）の失効確認をする際、事業所（VC）の状態（ステータス）は、

1. 有効（Valid）
   - 発行した事業所（VC）は有効期限以内
2. 無効（Invalid）
   - 発行した事業所（VC）の有効期限切れ
   - デジタル認証機構が事業所（VC）を失効した状態
   - 事業所が存在しない UUID[5] で失効確認

という状態が想定される。

■　対応

1. 悪意のある第三者が、適当な UUID を使って失効確認することで、UUID の存在有無が分からないように、事業所の失効確認結果（API）は、Valid/Invalid の 2 パターンとする。ただし、失効管理サービス（Corda）は、無効の原因が判別できるサーバログを出力する。
2. 事業所の失効確認は、不特定多数の事業所と想定するため、失効管理サービスは外部公開と考える。その際、DDoS 攻撃等のセキュリティ対策は、WAF 等の一般的なセキュリティ対策で考える（本実証で検証なし）

■　事業所（VC）の無失効確認

デジタル認証機構の失効管理サービス（Corda）と事業所（API）を対象に事業所（VC）のステータス結果をまとめる。

表 3-2-2：事業所（VC）の状態（ステータス）

事業所（VC）の状態（ステータス）	Corda	API
発行した事業所（VC）は有効期限以内	Vaild	Valid
発行した事業所（VC）の有効期限が過ぎた	InVaild※	InVaild※
デジタル認証機構が事業所（VC）を失効した	Revoked	InVaild
事業所が存在しない UUID で失効確認をした	Unknown	InVaild

※有効期限の管理はスコープ外

[5] デジタル認証機構が事業所に発行した事業に対するユニークな管理番号。

3.2.4　アクセスコントロール

■　課題

1.　Holder が認知していない第三者が、 Holder の VC/VP の中身を見ることできる。

■　対応方針

1.　前提（鍵交換）

- 各事業所は暗号化用の公開鍵を含めて自己署名した暗号化（VC）を作成する。
- Holder と Verifier が取引前に両社で契約締結する際、契約相手の実在性を確認すると同時に、暗号化（VC）を契約締結のやり取りの中で提示しあう。
- 結果、取引前に、Holder は Verifier の暗号化（VC）を保持していることになる。

2.　対応

- Holder は、Verify 用の事業所 VP を生成する際、Verifier の暗号化（VC）に含まれる暗号化用の公開鍵を使って、 Holder の事業所（VC）を包んだ事業所 VP を暗号化する。
- 事業所 VP（暗号化）を受け取った Verifier は、暗号化用の公開鍵とペアーになる秘密鍵を使って事業所 VP を復号化する。
- Verifier は、復号化した事業所 VP を Verify する。
- 暗号化用の公開鍵とペアーになる秘密鍵を保持しない事業所は、事業所 VP （暗号化）を Verify することは不可である。

3.2.5 「Trusted List」

■ Trusted List の背景

公的機関は、デジタル認証機構（DCO）を認定機関と証明するために、公的機関のデジタル署名が付いたデジタル証明書を DCO に発行する。本実証では、公的機関のデジタル署名を検証するために必要な公的機関の情報を含んだ「Trusted List」を国毎に準備することを前提とする。

■ Trusted List の説明

1. データ形式
   公的機関が作成したことを証明するため、公的機関の自己署名が付いた Verifiable Credentials（VC）とする。
2. リスト内容
   - 公的機関の公開鍵・・・公的機関のデジタル署名の検証用
   - 公的機関の DID・・・公的機関の識別子
   - 公的機関のデジタル署名・・・公的機関が Trusted List を作成したことを証明
   - 複数国ある場合・・・自国の他、他国の公開鍵を含む

■ 使用

1. 配布方法
   - 公的機関は、DCO に Trusted List を配布
   - DCO は、事業所 ID を発行する際、登録している事業所担当者のメールアドレスに Trusted List を送付
     （補記）本実証では、配布にメールを使用したが、誤送信やメール文から手作業による転記ミス等、課題があると考えるため、今後、API 連携等システム改善が必要
2. 対象となる公開鍵
   - 事業所は、トラストアンカーになる公的機関のデジタル署名を検証する際、Trusted List に対し、「DCO（VC）に含まれる公的機関の DID」と一致する公的機関の公開鍵を使用

3.3 実施事項・成果物一覧

表 3-3-1：実施事項・成果物一覧

実施項目		具体的な作業内容	担当（会社名）	想定成果物
実証ユースケースにかかわるステークホルダ調整	実証マニュアル作成	当事業と連携してアラクサラネットワークス社が実証を行う予定の「Trusted Network および Industry Trust Chain HUB」参加企業、およびデジタル認証機構向けの業務手順作成	SBI ホールディングス アラクサラネットワークス	実証マニュアル
プロトタイプシステム開発	業務・システム要件定義	● ユースケースをもとにビジネス要件を定義 ● 上記ビジネス要件をもとにシステム要件定義 ● トラストモデルの検討	SBI ホールディングス	要件定義書
	開発（アプリ・インフラ）	システム要件定義をもとに開発	SBI R3 Japan TIS	基本設計書 画面遷移図 操作手順書 アプリ・システム
	単体テスト・結合テスト	テストケース策定のもとテスト実施	TIS	テスト結果
実証実験の実施	実証実験	サプライチェーンのユースケースにおいてアラクサラネットワークスの協力の元実証実験実施	SBI ホールディングス	実証実験結果
	動画撮影	実証実験の様子・アプリ利用の様子を動画撮影	SBI ホールディングス SBI ビジネス・イノベーター	動画
	利用者アンケート	アプリを利用したステークホルダに対して、データ作成主体の信頼担保やユーザビリティの観点からアンケートを実施	SBI ホールディングス	アンケート アンケート集計結果
必要なルール・ガバナンス整理	国際標準規格の概要整理	国際会議での説明に向けた概要説明資料作成	SBI ホールディングス	標準規格 Draft
	国際標準化提案取りまとめ	国際会議での了承を前提として新規国際標準規格提案を作成	SBI ホールディングス	新規国際標準規格提案

	既存の評価基準の調査	現行の認証局等の評価基準のヒアリング調査	SBI ホールディングス	評価基準調査結果
	デジタル認証機構の認定基準等検討	調査に基き認定基準の素案を作成	SBI ホールディングス	認定基準素案
報告書取りまとめ	実証結果分析	事前に定義した論点の検証結果分析	SBI ホールディングス	論点検証結果
	最終報告書作成	開発アプリ・アンケート・調査・検証結果分析等の取りまとめ	SBI ホールディングス	最終報告書

3.4 スケジュール

3.4.1 全体スケジュール

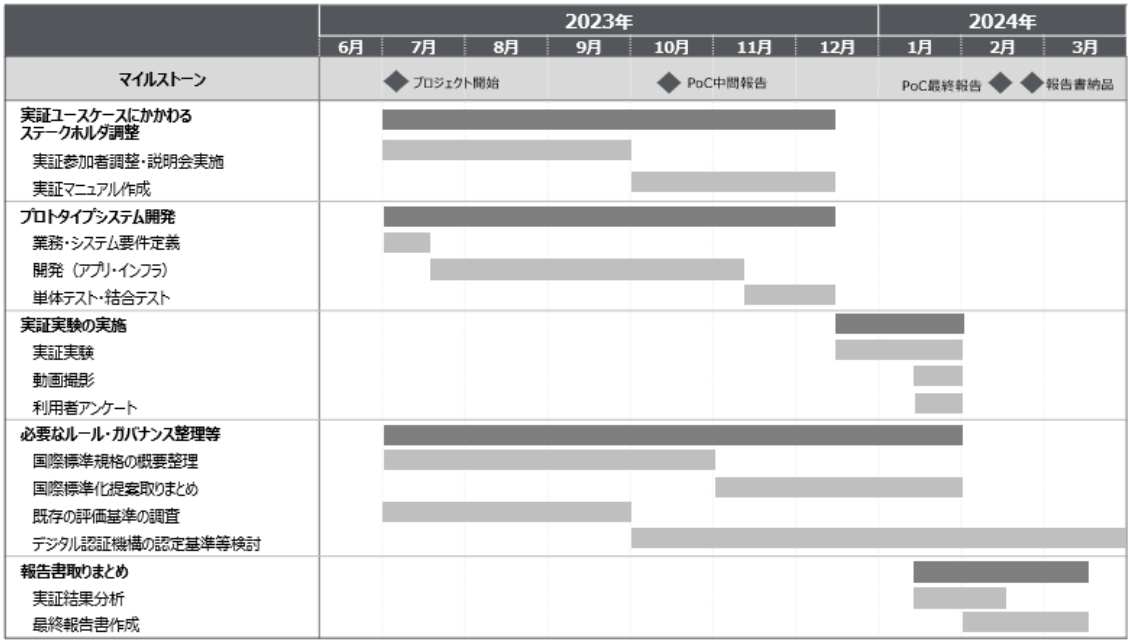


図 3-4-1：全体スケジュール

3.4.2　成果物の作成フロー

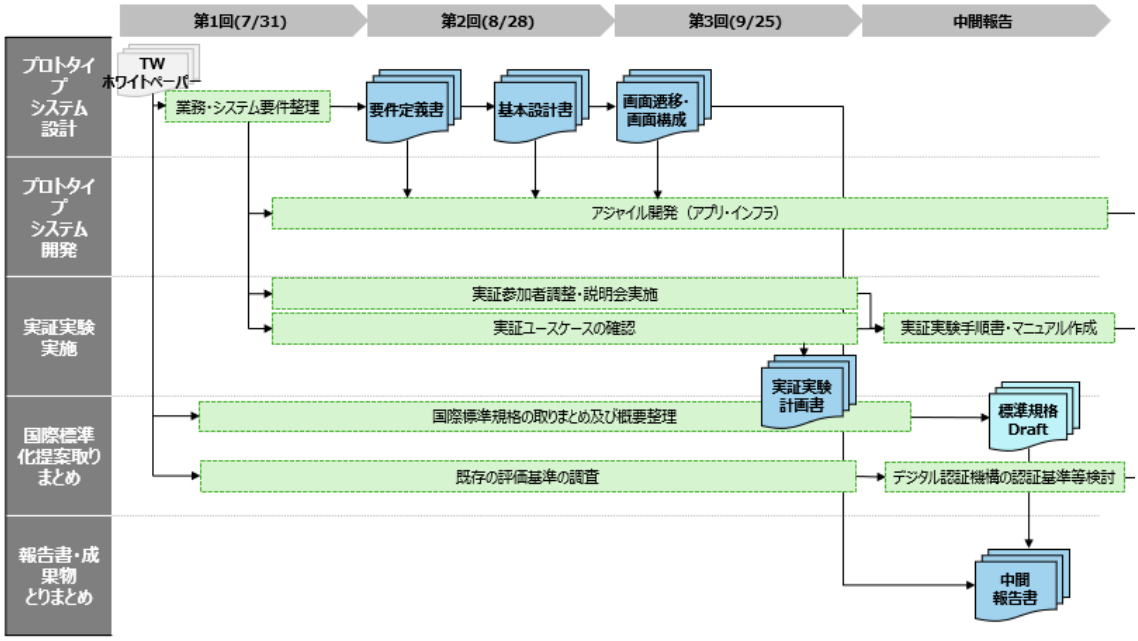


図 3-4-2（a）：成果物の作成フロー（前半）

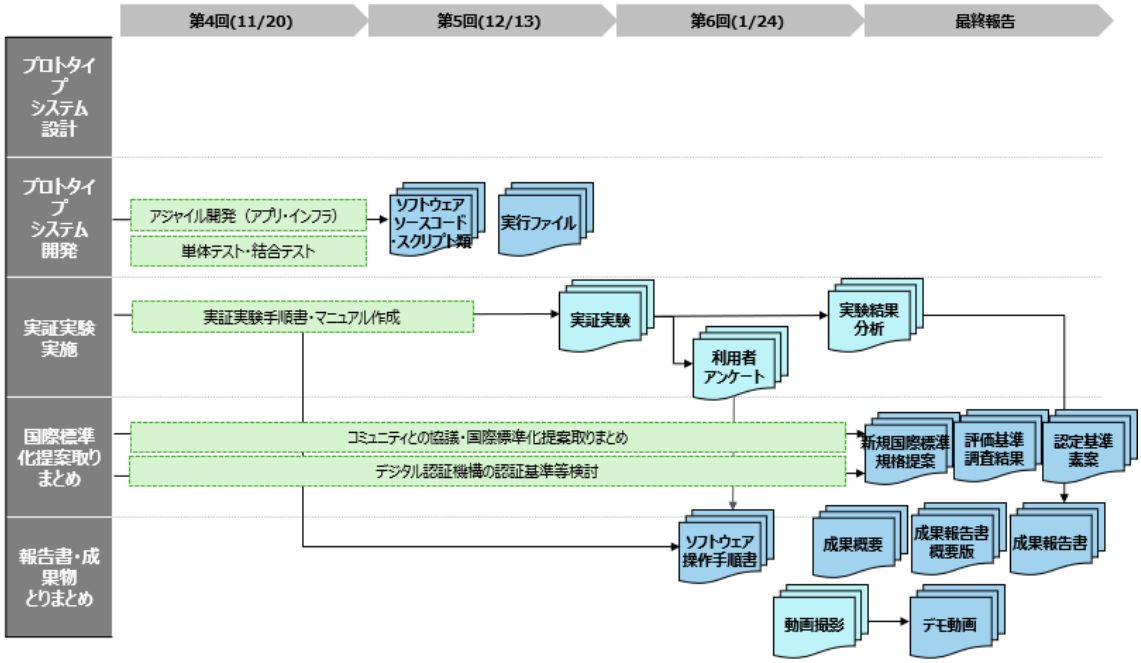


図 3-4-2（b）：成果物の作成フロー（後半）

3.5 実施体制

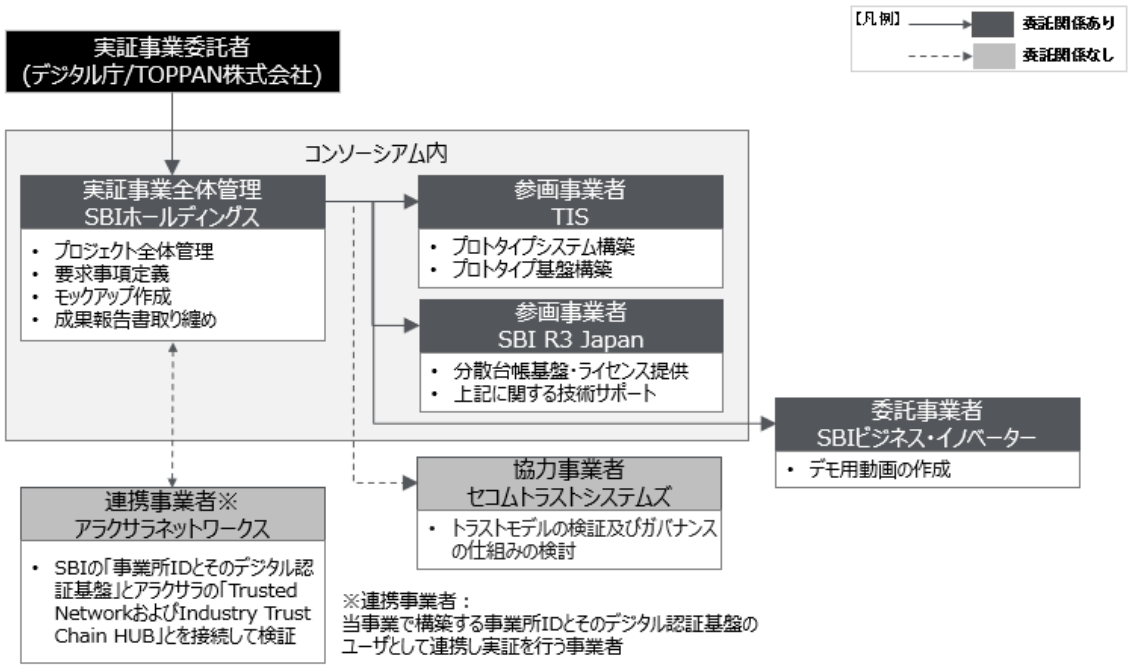


図 3-5-1：実施体制

4. 実証検証（企画・プロトタイプ開発）

4.1 実施概要

4.1.1 企画・プロトタイプ開発で明らかにする論点とその結果

論点①：取引先事業所の正当性を担保する仕組みがない

1. 検討経緯を以下に説明する。
   (ア) 信頼できる第三者となるデジタル認証機構が、事業所の実在性を認証したことを示すため、デジタル認証機構の秘密鍵を使ってデジタル署名した Verifiable Credential（VC）＝事業所（VC）を事業所に発行する。
   (イ) デジタル認証機構の公開鍵は、事業所（VC）に含むデジタル認証機構（VC）の DID Document の中に入れる。
   (ウ) 取引先事業所の事業所（VC）のなりすましを防ぐため、事業所（VC）に自己署名した Verifiable Presentation（VP）＝事業所（VP）を作成する。
2. 検討結果を以下に説明する。
   (ア) 取引先が保持する事業所（VC/VP）を使って、取引先事業所の正当性を確認する。
   (イ) デジタル認証機構の失効管理サービスを使って、取引先事業所の事業所（VC）が失効していないことを確認する。

論点②：デジタル認証機構の正当性を担保する仕組みがない

1. 検討経緯を以下に説明する。
   (ア) トラストアンカーとなる公的機関が、デジタル認証機構を認定したことを示すため、公的機関の秘密鍵を使ってデジタル署名した Verifiable Credential（VC）＝デジタル認証機構（VC）をデジタル認証機構に発行する。
   (イ) 公的機関の公開鍵は、別途 Trusted List を準備してその中に入れる。
   (ウ) デジタル認証機構のデジタル認証機構（VC）のなりすましを防ぐため、デジタル認証機構（VC）に自己署名した Verifiable Presentation（VP）＝デジタル認証機構（VP）を作成する。
2. 検討結果を以下に説明する。
   (ア) デジタル認証機構（VC/VP）と Trusted List を使って、デジタル認証機構の正当性を確認する。
   (イ) デジタル認証機構の失効管理サービスを使って、デジタル認証機構（VC）が失効していないことを確認する。

4.1.2 企画・プロトタイプ開発に用いる技術・標準等を選定した理由および背景

本実証では、事業所の実在性を検証可能なデジタル証明書を使って確認するため、識別子は W3C の Decentralized Identifiers （DIDs） v1.0 の技術を活用し、検証可能なデジタル証明書は Verifiable Credentials Data Model v2.0 draft 6 月の技術を活用することとした。

4.2 Verify できる領域を拡大する仕組み

4.2.1 登場主体・要求事項整理

■ 公的機関

【役割】

認定したデジタル認証機構に対し、デジタル証明書を発行する

【実証事業において設定した要求事項】

各国で認められたトラストアンカーとして、デジタル認証機構を認定する

■ デジタル認証機構

【役割】

- 発行サービス
  1. 事業所（VC）を発行する
  2. 事業所（VC）を更新する
  3. 事業所（VC）を失効する
- 失効管理サービス
  1. 事業所（VC）のステータスに対し有効/無効を返答する

【実証事業において設定した要求事項】

1. 業界毎にデジタル認証機構が存在し、業界に所属する事業所に対する事業所（VC）を発行する
2. 事業所が参加しやすいオンボーディングプロセスとして、認証レベルを複数設定する

■ 事業所

【役割】

1. デジタル認証機構に対し、事業所（VC）を申請する
2. 事業所（VC）を更新依頼する
3. 事業所（VC）を含んだ事業所（VP）を生成する
4. 他社の事業所（VP）を検証する

【実証事業において設定した要求事項】

3. デジタル認証機構のデジタル署名検証をもとに事業所の真正性を確認できる
4. 申請する際、住所と連絡先情報の項目については、事業所（VC）に含まない選択ができる

4.2.2　企画・プロトタイプシステムの開発におけるペインの解決方法

【As-Is】

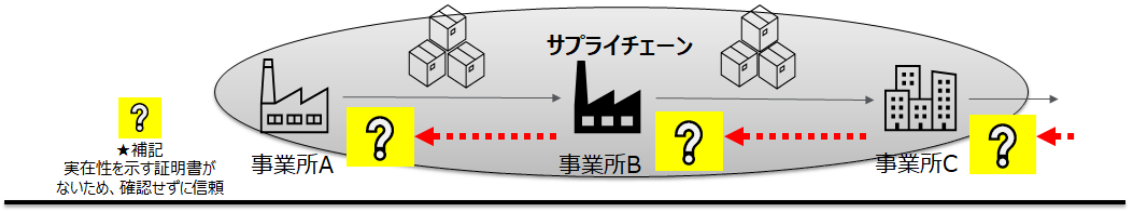


図 4-2-1：事業の As-Is

【To-Be】

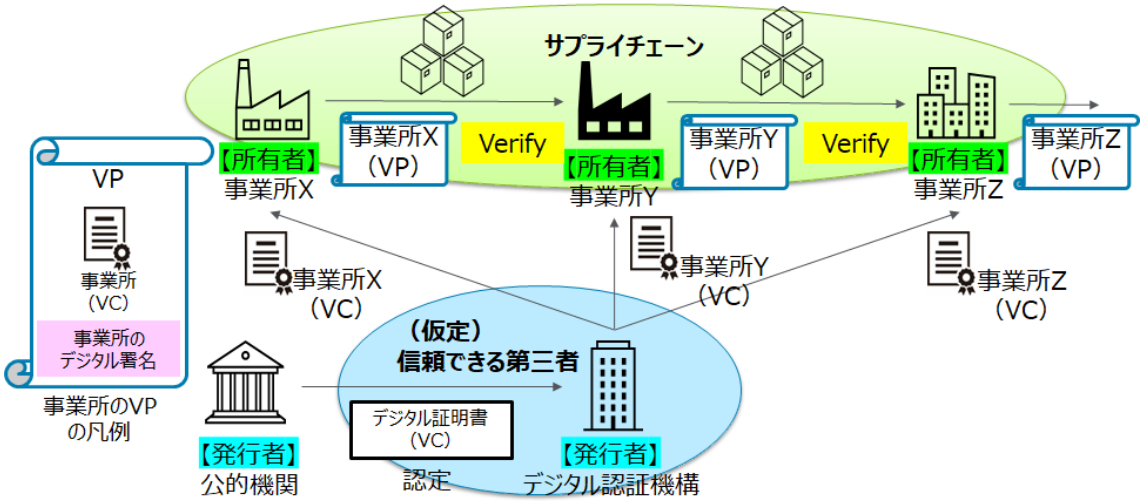


図 4-2-2：事業の To-Be

ペイン：第三者による真正性の証明がない

　事業所 B は、事業所 A から製品を入荷した際、事業所 A の実在性（所在地）を確認する場合、事業所 A の実在性を証明する第三者の証明書がないため、事業所 A を信じるしかない。

ペイン：模倣品・偽造品の混入

　事業所 C は、事業所 B から入荷した製品に模倣品・模造品が混入していた場合、川上のどの事業所が出荷したか事業所を検証する仕組みがない。

ペイン：第三者による真正性の証明がない

表 4-2-1：第三者による真正性の証明がないことに対する解決方法

ペインの解決方法（仮説）	事業所の実在性を確認
活用する規格・技術	• Decentralized Identifiers （DIDs） v1.0（W3C） • Verifiable Credentials Data Model v2.0 draft 6 月（W3C） • RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List （CRL） Profile
技術選定理由（仮説）	• 分散したネットワーク上でいくつかのトラストアンカー（公的機関）がある複雑なトラスト構造を前提にしている。 • トラスト関連技術としては DID/VC/VP 技術および X.509 技術の二つが存在するが、DID/VC/VP 技術は、完全な分散ネットワークを前提とし、特定のトラストアンカーを想定していない。X.509 技術は、単一のトラストアンカーを前提にしている。 • 特定のトラストアンカーによるトラスト構造を持つ、公的機関（国）およびその傘下のデジタル認証機関に関しては、既存技術である X.509 を補完的に活用し、今回前提にするトラスト構造に近いのは DID/VC/VP 技術であること。同技術は今後も発展が見込まれるため、将来性が高いこと。この二つを理由に、同技術が良いと判断している。

ペイン：模倣品・偽造品の混入

表 4-2-2：模倣品・偽造品の混入に対する解決方法

ペインの解決方法（仮説）	検証可能な証明書を提供
活用する規格・技術	• Verifiable Credentials Data Model v2.0 draft 6 月（W3C）
技術選定理由（仮説）	• サプライチェーンの関連団体（半導体および ICT 機器・サービス）に協力頂き、事業所や製品の製造者を証明する VC を含んだ証明書（VP）が検証可能であるか確認する。

4.2.3　Verify するデータ一覧

■　取引先の実在性

1. 検証者は事業所（Verifier）で、データの保有者は事業所（Holder）とする。
2. デジタル認証機構が事業所の実在性を確認した上で事業所に対して事業所（VC）を発行する。
3. 事業所（Holder）が事業所（Verifier）に取引先の実在性を提示するため、事業所（Holder）の事業所（VC）を包んだ事業所（Holder）のデジタル署名が付いた事業所（VP）を生成し、事業所（Verifier）に提示する。
4. 事業所（Verifier）が取引先の実在性を確認するための検証方法
   - 事業所（Holder）が事業所（VC）を事業所（Verifier）に提示したことを確認
     事業所（Verifier）は、事業所（VP）にある事業所（Holder）のデジタル署名を Verify するため、事業所（VP）に包まれた事業所（VC）に内包された事業所（Holder）の公開鍵を使って事業所（Holder）のデジタル署名を Verify する。
   - デジタル認証機構が事業所（Holder）に事業所（VC）を発行したことを確認
     事業所（Holder）の事業所（VC）にあるデジタル認証機構のデジタル署名を Verify するため、事業所（Verifier）は、事業所（VC）に包まれたデジタル認証機構のデジタル証明書に内包されたデジタル認証機構の公開鍵を使ってデジタル認証機構のデジタル署名を Verify する。
   - デジタル認証機構がデジタル認証機構のデジタル証明書を事業所（Holder）に提示したことを確認
     事業所（Holder）の事業所（VC）に内包されているデジタル認証機構（VP）にあるデジタル認証機構のデジタル署名を Verify するため、事業所（Verifier）は、デジタル認証機構のデジタル証明書に内包されたデジタル認証機構の公開鍵を使ってデジタル認証機構のデジタル署名を Verify する。
   - 公的機関がデジタル認証機構にデジタル証明書を発行したことを確認
     事業所（Holder）の事業所（VC）に内包されているデジタル認証機構のデジタル証明書にある公的機関のデジタル署名を Verify するため、事業所（Verifier）は、別途、Trusted List にある公的機関の公開鍵を使って公的機関のデジタル署名を Verify する。
5. 検証する際、データの置き場所は、検証者の PC で検証可能なアクセスコントロールがあると仮定する。

4.2.4　証明書要件・識別子要件

【証明書】

■　デジタル証明書

1.　公的機関が認定したデジタル認証機構に対し発行する証明書

■　事業所 ID

2.　デジタル認証機構が認定ルールに基づき審査し、認証した事業所に対し発行する、デジタル認証機構の署名が入った証明書とする

3.　事業所の所在地は、発行時、含めるか否か選択を可能とする

4.　失効管理は、デジタル認証機構で行う

【識別子】

■　事業所（Holder）

1.　デジタル認証機構は識別子を発行せず、事業所（Holder）自身が識別子（DID）を作成し管理する

4.3 合意形成・トレースの仕組み

4.3.1 本システムで目指す合意形成とその履行のトレースの内容

前提として、合意形成は関係者間のみ、無関係な第三者による合意・合意拒否はビジネス上不要であるとしている。

本システムでは、合意の主体は事業所（Holder）と事業所（Verifier）になる。合意の対象としては事業所の実在性である。合意の条件は、デジタル認証機構のデジタル署名とデジタル認証機構のデジタル証明書に含まれる公的機関のデジタル署名が有効な事業所（VC）であることを条件とする。そのために、事業所（Verifier）が事業所（Holder）の所有する事業所（VC）に含まれるデジタル認証機構の公開鍵と Trusted List から取得した公的機関の公開鍵を使って、デジタル認証機構のデジタル署名とデジタル認証機構のデジタル証明書に含まれる公的機関のデジタル署名を Verify し事業所（Holder）の所有する事業所（VC）の有効性を確認する。

また、トレースの対象は、事業所（Holder）と事業所（Verifier）の間における事業所（Holder）の実在性の合意となる。

トレースの主体は事業所（Verifier）となり、トレースの手法は事業所（Verifier）が Verify の実行結果を保存し確認する。合意の取り消しは、契約書等のアナログ運用のもと、事業所 VC の Verify の取り消しを合意することとする。

4.3.2 第三者が確認する情報一覧

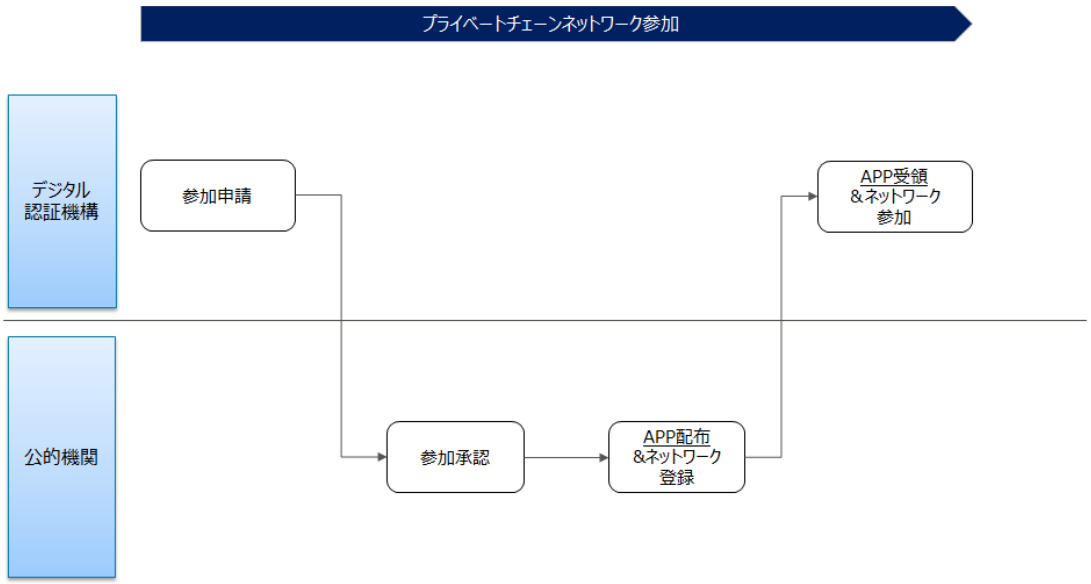
本実証で作成する事業所（VC）は、VC の中に証明に関する情報が入っており、第三者が内容を確認することができる。そのため、Holder が認知していない第三者が、 Holder の VC/VP の中身を見るリスクが想定される。

前提として、Holder と Verifier が事前に自身の暗号化用の公開鍵を交換することになるが、Holder は、Verifier の暗号化用の公開鍵を使って、事業所（VC）を暗号化してから Verifier に渡すことで、Verifier の秘密鍵でのみ事業所（VC）を復号化し内容を確認できるようにする。

4.4 企画・開発物

4.4.1 業務フロー

デジタル認証機構が公的機関に認定申請するためプライベートチェーンネットワークに参加する。



※下線部は今回の開発スコープ外

図 4-4-1：業務フロー（1/4）

デジタル認証機構が公的機関に認定申請し、認定完了後、公的機関がデジタル認証機構にデジタル証明書（VC）を発行する。

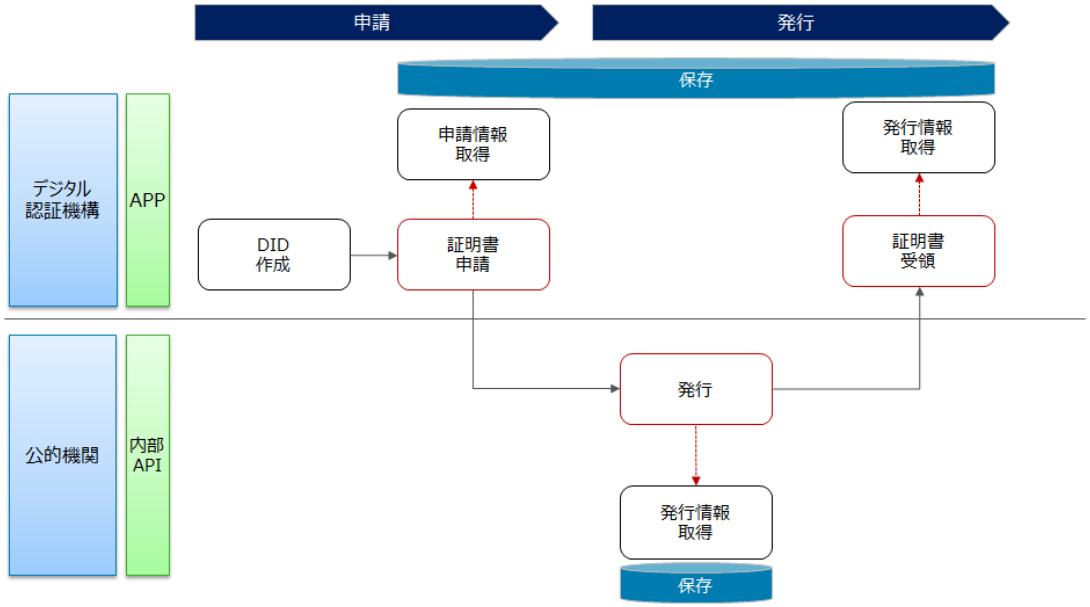


図 4-4-2：業務フロー（2/4）

事業所がデジタル認証機構に事業所（VC）を申請し、審査完了後、事業所に事業所（VC）を発行する。

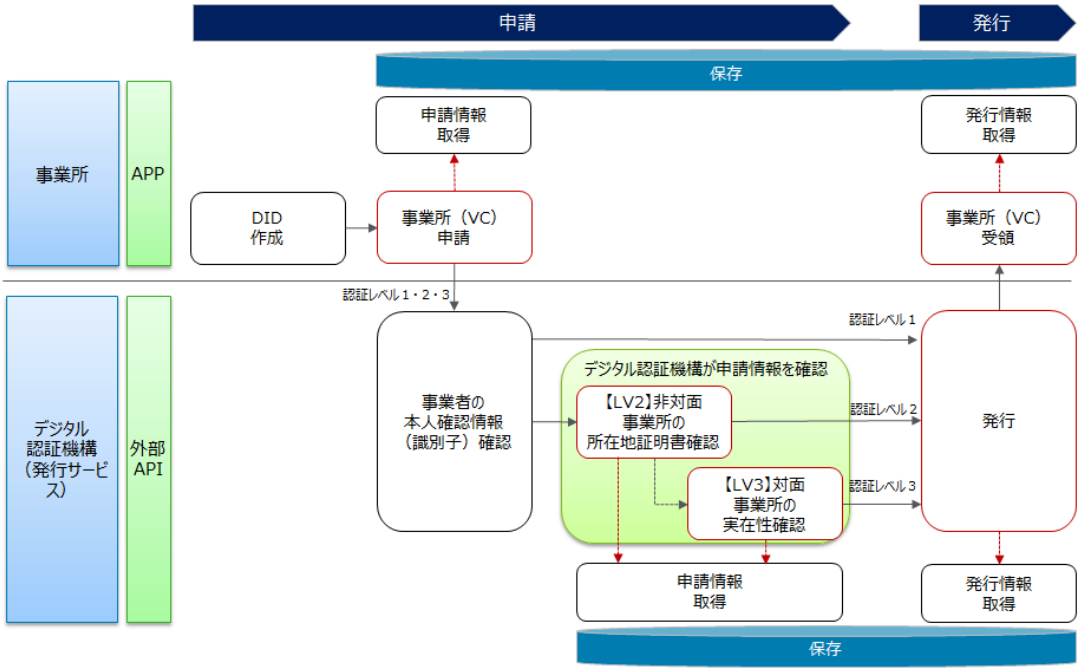


図 4-4-3：業務フロー（3/4）

事業所間で取引をする際、バイヤーがサプライヤーの実在性を確認するため、事業所（VC）を検証する。

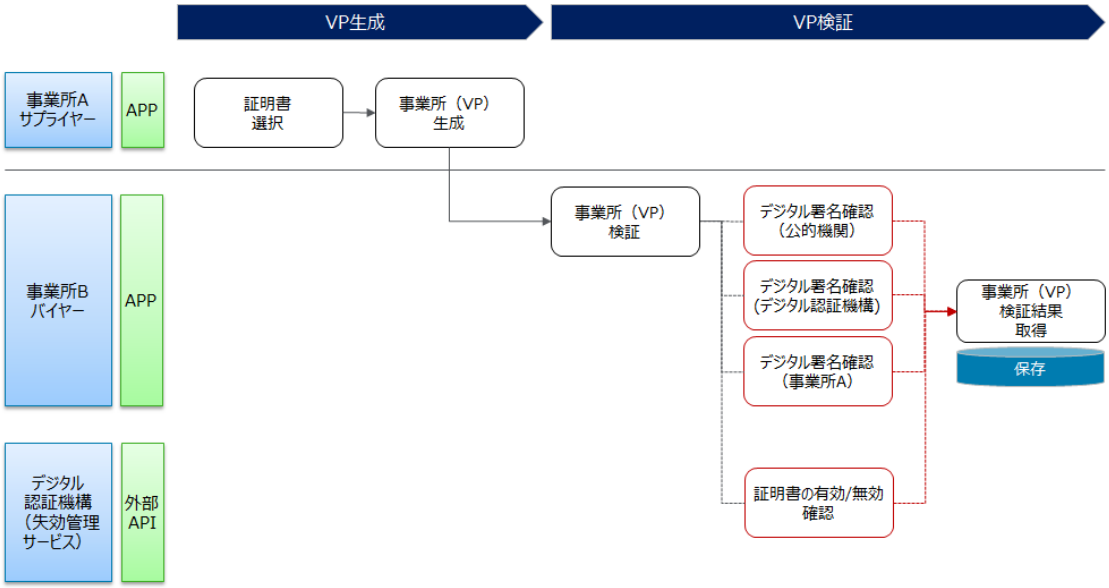


図 4-4-4：業務フロー（4/4）

4.4.2　ユースケース図

デジタル認証機構が公的機関に認定申請し、認定完了後、公的機関がデジタル認証機構にデジタル証明書（VC）を発行する。

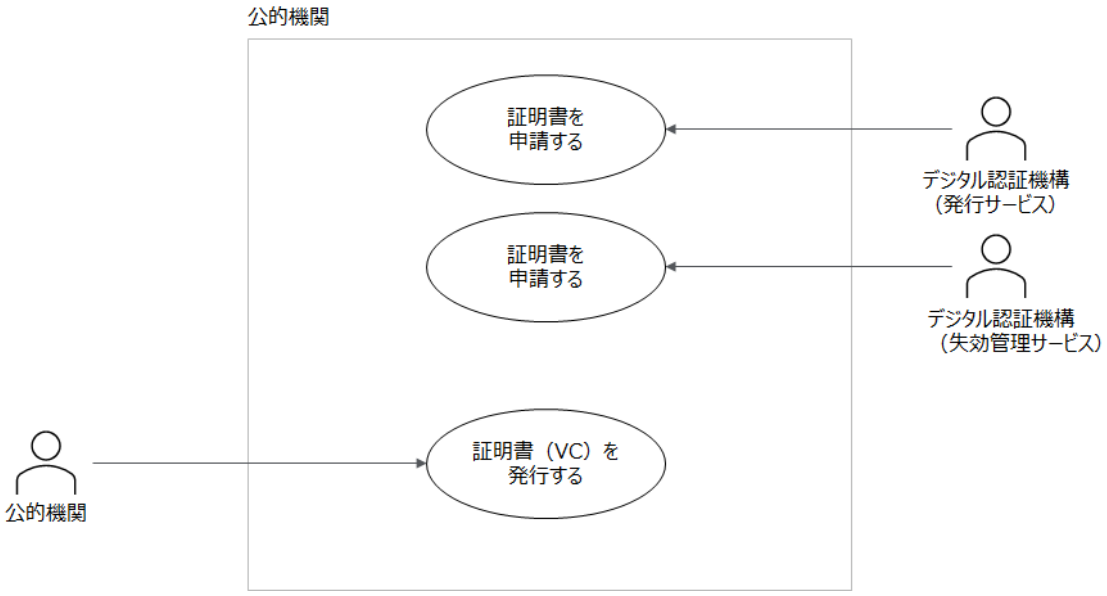


図 4-4-5：ユースケース図（1/3）

事業所がデジタル認証機構に事業所（VC）を申請し、審査完了後、事業所に事業所（VC）を発行する。また、事業所がデジタル認証機構に事業所（VC）の更新依頼を申請し、審査完了後、事業所に更新した事業所（VC）を発行する。

デジタル認証機構が事業所を定期的に審査し、条件を満たさない場合、事業所（VC）を失効する。

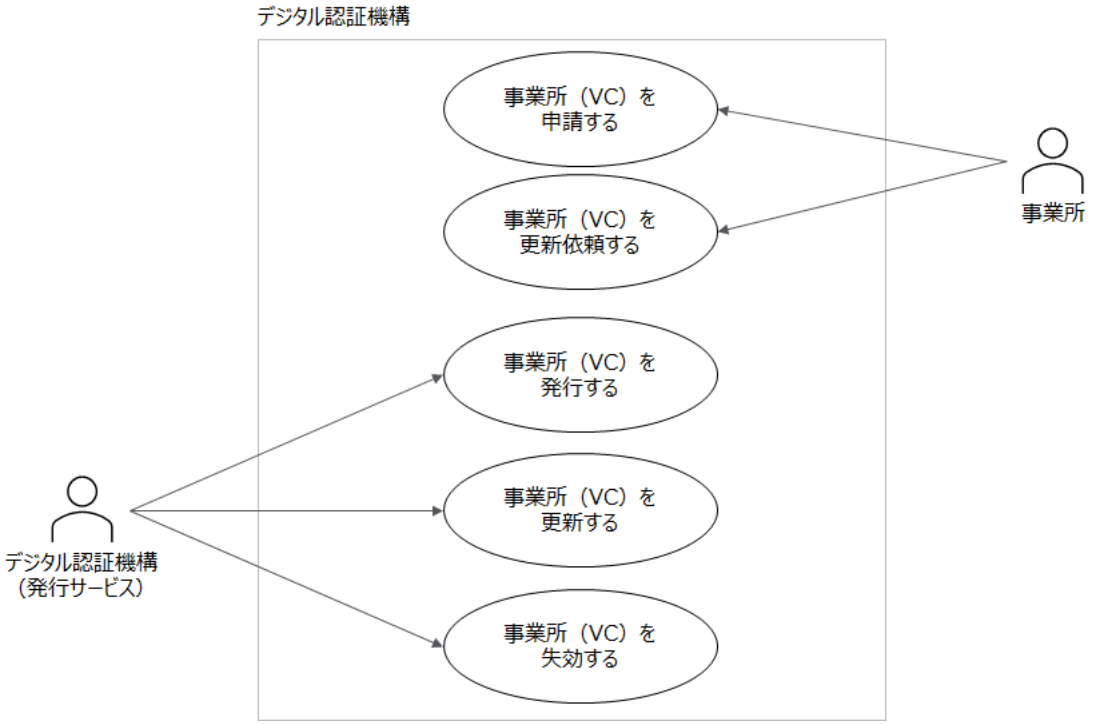


図 4-4-6：ユースケース図（2/3）

バイヤーがサプライヤーの実在性を確認するため、事業所（VC）を使った検証をする。

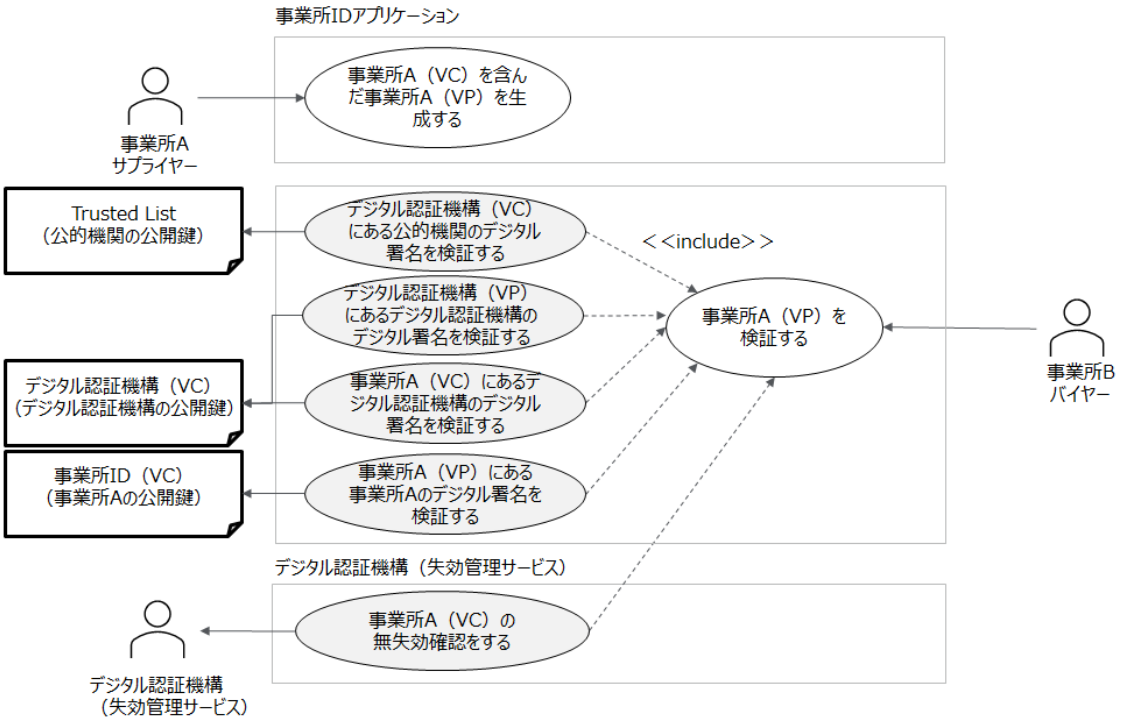


図 4-4-7：ユースケース図（3/3）

4.4.3　操作画面（UI）

公的機関が発行したデジタル証明書の一覧を表示する。

■　デジタル認証機構の証明書（DCO Digital Certifications）

1.　公的機関が発行したデジタル認証機構のデジタル証明書の一覧を表示

■　失効管理サービスの証明書（RCO Digital Certifications）

1.　公的機関が発行した失効管理サービスのデジタル証明書の一覧を表示

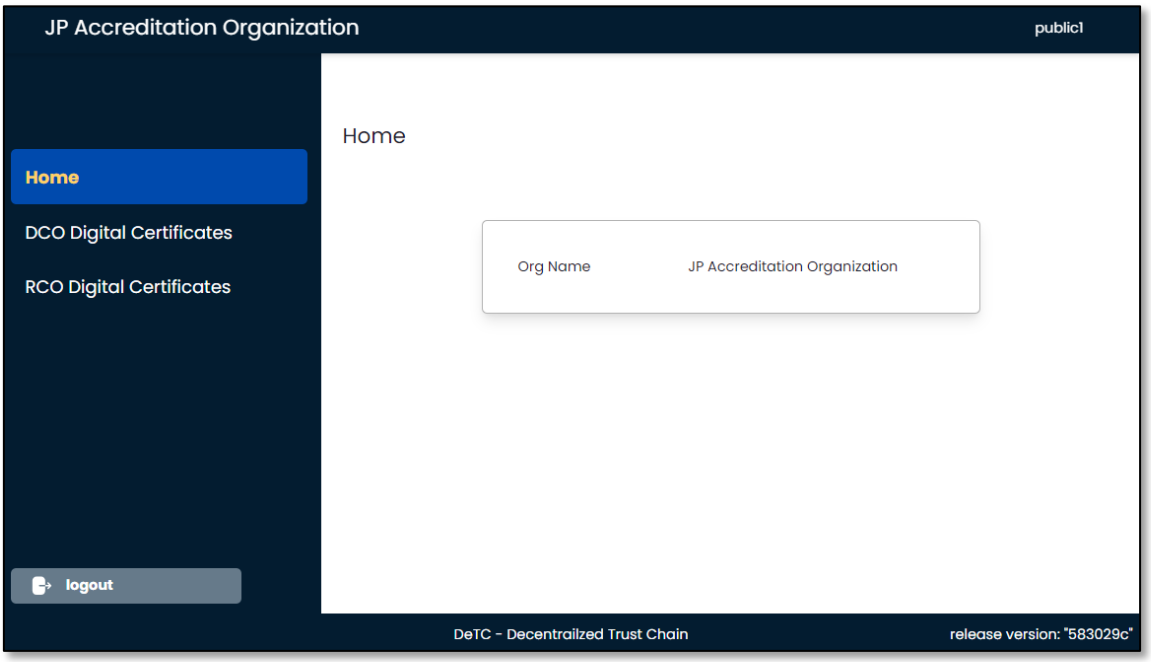


図 4-4-8：操作画面（1/3）

デジタル認証機構「発行サービス」に関するデジタル証明書/事業所（VC）の一覧を表示する。

■ オンゴーイング（Ongoing）

1. デジタル認証機構が事業所に発行した事業所（VC）の一覧を表示

■ デジタル証明書一覧（Digital Certificates）

1. 公的機関がデジタル認証機構に発行したデジタル証明書の一覧を表示

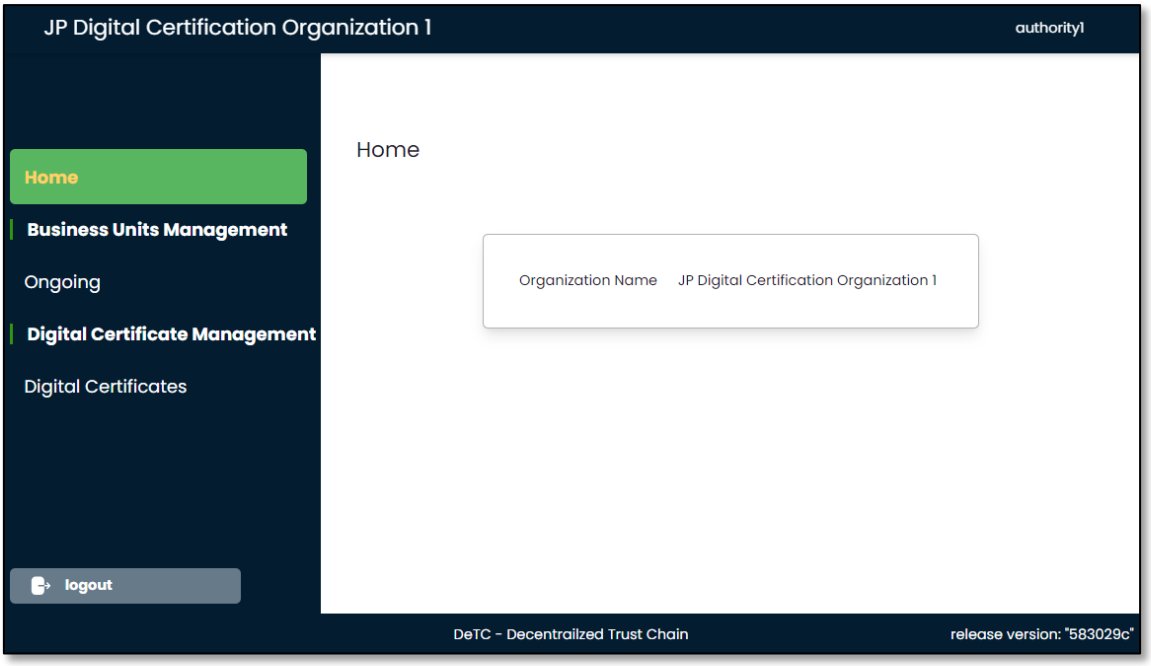


図 4-4-9：操作画面（2/3）

デジタル認証機構「失効管理サービス」に関するデジタル証明書/事業所（VC）の一覧を表示する。

■ 証明書失効一覧（Revoked Digital Certificates）

1. デジタル認証機構の証明書と事業所（VC）の有効と無効の一覧を表示

■ デジタル証明書一覧（Digital Certificates）

2. 公的機関が失効管理サービスに発行したデジタル証明書の一覧を表示

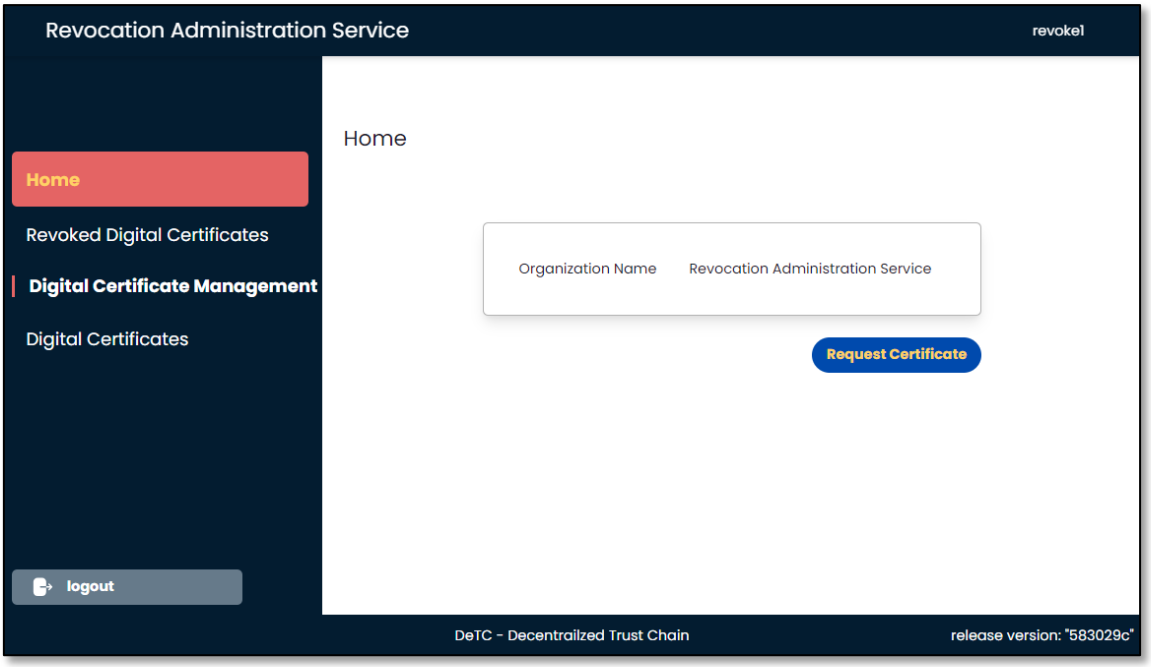


図 4-4-10：操作画面（3/3）

4.4.4　機能一覧/非機能一覧

信頼できる第三者が証明する事業所（VC）を発行/更新/失効するために必要な機能/非機能を定義する。

表 4-4-1：機能一覧/非機能一覧

機能/ 非機能	機能名	機能概要
機能	デジタル証明書の発行	公的機関が、デジタル認証機構と失効管理サービスに対し、デジタル証明書を発行する
機能	事業所（VC）の発行	デジタル認証機構が、事業所に対し、事業所（VC）を発行する
機能	事業所（VC）の更新依頼	事業所が、デジタル認証機構に対し、事業所（VC）の更新依頼をする
機能	事業所（VC）の更新	デジタル認証機構が、事業所に対し、更新した事業所（VC）を発行する
機能	事業所（VC）の失効	デジタル認証機構が、事業所（VC）を失効する
機能	VP の生成	事業所が、事業所（VC）を含んだ VP を生成する
機能	VP の検証	取引先が提示した VP を検証する
機能	事業所（VC）の無失効確認	事業所が、VP 検証を行う際、失効管理サービスに問い合わせして事業所（VC）の有効/無効を確認する
非機能	セキュリティ （不正アクセス防止）	事業所（VC）の申請前に、チャレンジを取得し、事業所（VC）にチャレンジの値を含めることで API を使った申請時のリプレイ攻撃から守る
非機能	セキュリティ （秘密鍵の管理）	クラウドベンダーが提供しているマネージド型の鍵管理サービスを利用
非機能	性能	事業所（VC）の有効性を Verify する際、失効管理サービスに問い合わせが発生する。大量の Verify が発生することを想定し、トランザクション数増加に合わせて、失効管理サービスはスケールアウトで対応できるシステム構成とする
非機能	可用性	デジタル認証機構は、発行サービスが原因によるシステムダウンが発生しても、Verify で使用する失効確認は継続利用できるように「発行」と「失効確認」のサービスを物理的に分ける

4.4.4.1 非機能検討（リスク分析とセキュリティ対応方針）

想定するリスクは、信頼できる第三者のデジタル署名の改ざんにより、不正に事業所（VC）が発行されて、事業所の実在性確認の信頼性が損なわれる。発生可能性としては、デジタル認証機構の鍵管理システムの操作権限が攻撃者に奪取された場合が考えられる。影響度は、事業所（VC）が不正に発行されると、事業所（VC）を使った事業所の実在性確認の信頼性が損なわれるリスクがあると考える。

本リスクの対応方針は、デジタル認証機構やデジタル認証機構のトラストアンカーとなる公的機関の鍵管理を第三者に知られないように安全に保持する。また、公的機関の公開鍵は Trusted List で提供するが、Trusted List のなりすまし防止対策を実施する（例：Trusted List に公的機関の自己署名をつける）。

4.4.4.2 非機能検討（大規模・商用・社会実装時の対応方針）

【社会実装時に想定する利用規模】

ICT・半導体のサプライチェーンの想定トランザクション数は、バイヤーが部品を入荷の際、サプライヤーの部品メーカー毎に、事業所（VC）を Verify する。

例えば、ネットワーク機器の型番あたり約 250 部品に対し、対象となる部品メーカーの事業所（VC）を Verify する。

将来的に社会実装された際、参加事業所（社）とアクセス数（件）を試算すると、2025 年にパイロット検証として、川上・川中・川下でそれぞれ 1 社と仮定し、ネットワーク機器の 1 つの型番を入荷タイミングで Verify する。翌年以降、商用化の範囲を拡大し、1 年あたりの参加者数を 10～30 社、ネットワーク機器の型番を 5～10 増やしていくと仮定する。

【対応方針】

事業所（VC）の有効性を Verify する際、失効管理サービスに問い合わせが発生する。大量の Verify が発生することを想定し、利用者のレスポンスタイム増加に合わせて、失効管理サービスのスケールアウトを検討する。1 件あたりのレスポンスタイムが 3 秒以上になると、スケールアウトすると仮定する。

4.4.5　データモデル定義

事業所の実在性を証明する事業所（VC）の主な属性を定義する。

表 4-4-2：データモデル定義

属性値	属性取得元	属性値（VC 内）
事業所の DID	credentialSubject	id
事業所の認証者情報	credentialSubject	authenticatorInfo
事業所情報	credentialSubject	businessUnitInfo
事業所名	credentialSubject	businessUnitName
所在地国	credentialSubject	country
所在地	credentialSubject	address
事業者情報	credentialSubject	legalEntityInfo
認証レベル情報	credentialSubject	authenticationLevel
失効サービスの URI	credentialSubject	revocationEndPoints
信頼できる第三者の証明書 •デジタル認証機構のデジタル署名 •公的機関のデジタル署名	credentialSubject	linkedVP
デジタル認証機構の DID	issuer	id
デジタル認証機構名	issuer	name

4.4.6　実験環境

事業所がデジタル認証機構に事業所（VC）の申請/発行/検証をする際に必要な実験環境の構成図になる。

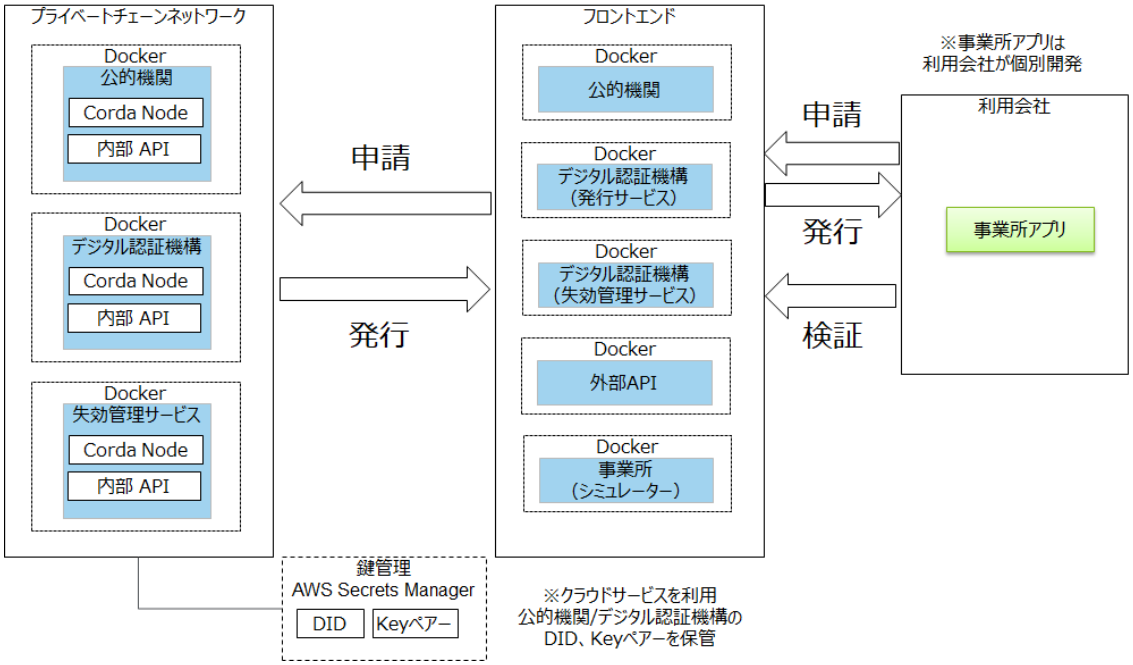


図 4-4-11：実験環境

4.4.7　システムの構成要素

表 4-4-3：システムの構成要素

コンポーネント名称（システム・ライブラリ名）	開発区分（新規/既存）	開発先/権利の帰属先（OSS）	型式名・ライセンス名（製品の場合）/OSS 名（OSS の場合）
auth-corda	新規	SBI R3 Japan TIS	React、Node.js、postgres
デジタル認証機構（発行サービス）	新規	SBI R3 Japan TIS	React、Node.js、postgres
デジタル認証機構（失効管理サービス）	新規	SBI R3 Japan TIS	React、Node.js、postgres
事業所	新規	SBI R3 Japan	React、Node.js、postgres
プライベートチェーンネットワーク	既存	SBI R3 Japan	Corda Enterprise 開発ライセンス（有償ライセンス）

コンポーネントの説明は以下になる。

■　公的機関

1. 法律に基づき自身もしくは指定した機関を通じ、信頼できる第三者であるとしてデジタル認証機構を認定し、公的なデジタル証明書（VC）を発行する。

■　デジタル認証機構

1. 発行サービス
   - 事業所の事業所（VC）の発行申請を受領後、申請情報に基づき事業所の実在性を確認し、問題が無ければ、事業所（VC）を発行する。
   - 定期的に当該事業所が存在しているかを確認し事業所（VC）を更新する。
   - 確認できなかった場合、事業所（VC）を取り消す。
2. 失効管理サービス
   - 事業所（VC）の有効性確認は、利用頻度が高いと想定し、発行サービスと別サーバとする。
   - 事業所（VC）の有効性確認に対し、有効/無効を回答する。

■　事業所

1. 事業所はシミュレーターとして開発する。

■　プライベートチェーンネットワーク

1. 公的機関やデジタル認証機関（発行サービス/失効管理サービス）といった公的な役割を担うネットワークにおいては、X.509 証明書による相互認証を行うため Corda を使った分散台帳技術を使用する。
2. Corda 製品サポートと一部機能を除いた、「Corda Open Source（トライアル版）/Apache2.0」あり
   - https://github.com/corda/corda
3. Corda ライセンス

- https://sbir3japan.co.jp/corda/corda-enterprise-license/

■ その他

1. 本実証では、AWS Secrets Manager を使用したが、他の鍵管理サービスの利用は可能である。

5. 実証（事業実現に向けたガバナンス・コミュニティ等の検討）

5.1 実施概要

5.1.1 事業実現に向けたガバナンス・コミュニティ等における論点とその結果

表 5-1-1：事業実現に向けたガバナンス・コミュニティ等における論点とその結果

No	論点	検討結果とその経緯
1	製造業を中心にサプライチェーンに対する新たな規制や経済安全保障上の対応が課題となる中、サプライチェーンの信頼性を確保する仕組みが必要	事業所の真正性を保証する仕組みについて、国際標準化を提案 ● 新規国際標準 ISO/TC292 国際会議で規格の概略発表（2023 年 10 月） ISO/TC292 国際会議で規格の提案（2024～25 年予定）
2	デジタル認証機構の、国際的な仕組みを構築するため、国際標準と同一レベルの「認定基準」を整理	既にある、認証局やタイムスタンプ局といったトラストサービスプロバイダーのサービス基準を参考に、デジタル認証機構の個別要件と事業所（VC）の適格要件を整理する。

5.1.2 実施内容・手法

【ビジネスフィージビリティ検証】

ビジネスフィージビリティについて、ICT 機器・サービス提供会社およびその川上・川下の企業や半導体関連会社に対し、ヒアリングを実施した。

1. 事業所 ID（事業所 VC）とそのデジタル認証の申請・更新フローについては、サプライチェーンの参加判定に事業所（VC）の有無を追加し、利用できることを確認し、事業所（VC）を所有している事業所の方が、事業所の実在性について信頼性が向上するのではないかとコメントがあった。
2. サプライチェーンネットワークとの接続・連携の容易性については、WebAPI による P2P ベースで事業所（VC）の申請・更新・失効確認が容易に利用できることを確認し、API 連携や既存システムに add-on（あるいは Plug in）で利用できる点に有効性があるのではないかとコメントがあった。
3. トレーサビリティ検証時における事業所のデジタル認証の検証容易性については、サプライチェーンに参加する取引先の間で、バイヤーが仕入れた製品を構成する各サプライヤーの製造場所を確認する際、事業所（VC）を使った検証の容易性を確認したが、さらに、事業所（VC）に含まれる、事業所の情報について、事業者自身が相手に合わせて、情報の開示/非開示をコントロールする仕組みがあると良いとコメントがあった。

【ガバナンス・ルール整理】

EU 主導による EU バッテリー規則や、エコデザイン規則案（ESPR）その延長線上にある DPP（Digital Product Passport）など次々と提案される規則においてサプライチェーンおよび製品・サービスの信頼性に対する要求が益々高まっている。その中には、プロダクトに含まれる部品や原材料の製造者および製造場所（製造国）の項目があり、国際的な取引においてデジタルで信頼できる製造者・製造場所（製造国）情報が必要となって来るものと考えられる。

上記の背景より、3 つに分けて整理した。

■ 事業所 ID とそのデジタル認証の国際標準化

インターネット協会 OIC 運営委員会で、国際標準化に向け規格の概略を作成、その内容を日本規格協会および ISO/TC292 国内委員会に説明し、10 月の ISO/TC292 国際会議で発表した。

■ 事業者・事業所が参加しやすいオンボーディング

デジタル認証の信頼度に応じた認証レベルを用意し、事業所の参加条件を選択できるように考える。

1. レベル 1
   - 所属する事業者（法人等）の本人認証を行うが事業所情報については自己表明
2. レベル 2
   - 公的・準公的機関が発行する書面等の提出による事業所情報の確認（非対面）
3. レベル 3
   - 有資格者による現地実査を通じた事業所の実在確認（対面）

■ デジタル認証機構の認定ルールの整理

２種類の認定方法について、調査した。

1. 法令等に基づく指定調査機関による適合性調査（イメージ図①）
   - 電子署名法
2. 国際標準に基づき認定された適合性評価機関による適合性評価（イメージ図②）
   - ISO/IEC 17065（製品、プロセスおよびサービスの認証を行う機関に対する要求事項）
   - ETSI EN 319 403（トラストサービス評価特有の追加基準）

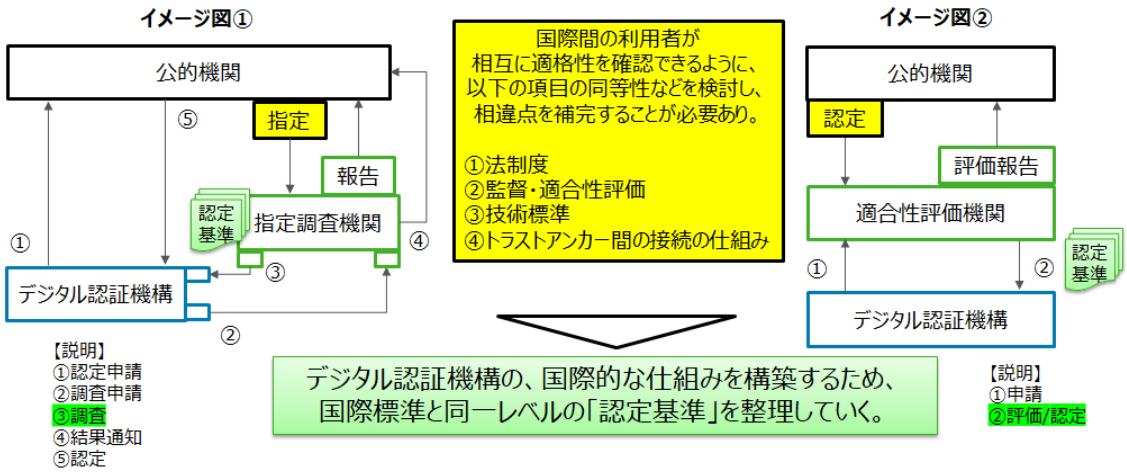


図 5-1-1：デジタル認証機構の認定ルールの整理 [6]

[6] デジタル庁.「トラストを確保した DX 推進サブワーキンググループ 報告書」. 令和４年７月 29 日
https://www.digital.go.jp/councils/trust-dx-sub-wg

【コミュニティ形成】

■ プロトタイプ実証からパイロット導入に向けて、初めにプロトタイプ実証への参加について「一般社団法人　沖縄オープンラボラトリ（OOL）」が実証を行う「Trusted Network PJ Phase 2」と連携した本実証の参加を進めた。その中で、コニュニティー参加ルールの整備として、週 1 で定例会を実施し、事業所 ID を使った検証準備をし、技術実装の検証、ビジネス実装の検証を実施した。

1. 技術実装の検証（2023 年 9 月下旬から 11 月）
    - 事業所（VC）の申請/発行、検証、更新、失効
2. ビジネス実装の検証（2023 年 12 月から 2024 年 1 月）
    - 事業所（VC）を使った、新規契約時の取引先の証明
    - 事業所（VC）を使った、製品の製造者の証明

■ 国際標準化に向けて、インターネット協会 OIC 国際標準化委員会への参加呼びかけや調整をし、2023 年 10 月の ISO/TC292/WG4 国際会議に向けて規格の概略と実証プロトタイプの説明および規格提案の DRAFT を策定した。

5.2 検証結果

インターネット協会 OIC に設置した委員会等において各種検討を実施した。

表 5-2-1：検証結果（1/2）

No.	委員会等および実施時期	実施内容
1	国際標準化委員会 （6/16、7/6、26、8/10、29、9/12、26、10/5、27、11/8、28、12/14、1/10、1/19、2/21）	● 新規規格原案を策定、国際標準化テーマ調査票申請を提出 ● ISO/TC292/WG4 国際会議に向けて規格の概略と実証プロトタイプの説明資料作成、国際会議での発表実施 ● 新規規格提案の DRAFT 作成（継続中）
2	研究開発委員会 事業所 ID プロトタイプ構築 WG （ 6/26 、 7/24 、 8/28 、 9/25 、 10/30 、 11/27 、 12/18、1/22）	● 実証プロトタイプに向けた要件検討 当初シナリオでは製品出荷と合わせて事業所デジタル証明を提示するような画面イメージを作成したが、現実的には取引開始前に相互確認するのが通常であるためシナリオを変更。 ● 実証プロトタイプの確認およびフィードバック 所在情報の開示範囲のバリエーションについて意見があり所在を開示する・しない２つのデジタル証明を作成するよう仕様を修正。
3	その他（国際標準化検討） IPADADC 日本規格協会 （適宜）	● 国際標準化テーマ調査票申請内容の確認 IPADADC が検討を進めるウラノス・エコシステムのトラスト基盤において検討されている内容との関連性を確認した。 ● ISO/TC292/WG4 国際会議における発表内容の確認 日本規格協会に事前確認した上で、国内委員会（ISO/TC292/SG3）で取り上げていただき承諾を得た。

● 国際標準化活動の成果と今後の予定

国際標準化原案およびその実証プロトの内容をまとめ、それのプロモーションを行うべく、10 月 16 日から 10 月 19 日まで、オーストリアで開催された ISO/TC292/WG4 国際会議に対面で出席してきた。その結果、各国＜ドイツ、フランス、スイス、UK、オーストリア、米国等＞から前向きかつ活発なコメントが寄せられ、次のステップである、NP 提案の道筋ができた。これに伴い、日本規格協会 SG3 国内委員会/国際標準課、インターネット協会国際標準化委員会および関係省庁との必要な調整後、NP 提案を予定。

並行して、令和 6 年度国際標準化テーマ調査票を経済産業省に申請し経済産業省にて審査が完了した。その結果を受け「テーマ名：サプライチェーンデータ連携基盤の信頼性確保に関する国際標準

化」の公募申請を策定・検討中。また、ドイツ Industrie4.0 の専門委員会より、招待を受け実証プロトタイプシステムのプロモーションを行い、実ビジネスでの具体的質疑がなされ賛同を得られたため、今後継続的に実証プロトタイプシステムを展開することを検討予定。

沖縄オープンラボラトリの Trusted Network PJ Phase2 に参加、「事業所 ID とそのデジタル認証」との連携実証を実施した。

表 5-2-2：検証結果（2/2）

No.	委員会等および実施時期	実施内容
1	その他（実証プロトタイプ） 沖縄オープンラボ Trusted Network PJ Phase 2 （週次定例、他適宜）	● 実証プロトタイプの説明およびフィードバック OOL 向けに、デジタル認証機構の API（事業所（VC）申請/発行等）とエンドポイントへのアクセス方法の説明をしながら、OOL 側で実装したが API のアクセス、事業所（VC）の授受などが想定通りに行かない事象が発生したため、説明内容の補足・修正を行った。このことから、デジタル認証機構と事業所側のシステムと API 連携する際、DID/VC の仕様理解・意思疎通が難しいことが分かった。

6. 調査検証

6.1 実施概要

6.1.1 調査で明らかにする論点とその結果

0. 本ユースケースにおけるパブリックチェーン/パーミッションドチェーン比較

1. 従来型の Web サービスを標準評価した場合における、パブリックチェーン（PoS ベース Ethereum 想定）/パーミッションドチェーン（Corda 想定）という 2 つの分散型システムのアーキテクチャを比較評価した。

① 機能開発
両チェーンは要件次第になるため、評価は同じであると想定する。

② サービス維持
パブリックチェーンは事実上リスクなしと評価するが、パーミッションドチェーンはサービサーに依存するリスクがあると想定する。

③ データロストリスク
パブリックチェーンは事実上リスクなしと評価するが、パーミッションドチェーンはアーキテクチャに依存するリスクがあると想定する。

④ 参加者負担
パブリックチェーンは鍵管理のリスクが高いと評価するが、パーミッションドチェーンはアーキテクチャに依存するリスクがあると想定する。

⑤ プライバシー管理
パブリックチェーンは情報漏洩時のリスクコントロール不可でリスクが高いと評価するが、パーミッションドチェーンは Need to Know 原則に従っており、
リスクコントロールが容易でリスクが低いと想定する。

⑥ 参照パフォーマンス
パブリックチェーンは本件と関係ない情報も検索対象になるためパフォーマンス劣後と評価するが、パーミッションドチェーンは必要な情報のみを検索するためパフォーマンス改善が容易と想定する。

⑦ 登録パフォーマンス
パブリックチェーンは要求に対応できない可能性が高く、2nd レイヤ活用により改善の検討が必要と評価するが、パーミッションドチェーンはサービサーに依存（データ同期/分散に追加コストが必要なため Web サービスに対しては劣る）と想定する。

2. パブリックチェーンの場合、エコシステムへの依存度が高く、パブリックチェーンの持つ制約がビジネス化に当たってのブロッカーとなるリスクがあるため、今回はパーミッションドチェーンを必要な部分へ活用することを前提としたアーキテクチャを採用した。

1. Central Data Registry（以下 C.D.R.）不要なアーキテクチャにおける選択的開示の技術的実現手法の検討

1. W3C C.C.G（Credential Community Group）他と、各種技術の実装や規格化の進捗について検討した。

2. その結果、主要な実装方の一つである、SD-JWT は（個人向けかエンタープライズ向けかに起因する）技術要件の差が大きく、今後、本取り組みで採用する可能性は低いと結論づけた。
3. 一方、JSON-LD と BBS+を活用した実装については、エンタープライズ用途との親和性があるものの、現時点で論文レベルでの選択的開示に関する実装が出てきたという状況。技術的成熟度が低いため、現時点での採用は時期尚早であると判断した。特に、選択的開示の開示内容を指定する Presentation Exchange 規格との整合性のある実装が待たれる。
4. 仮に選択的開示を現時点で構築するのであれば、非開示情報を含まない VC を別途構築し使用する方が確実であると整理している。
5. また、論点 3, 4, 7, 9 との整合性を持った構成の実装可能性の検討も今後の論点と考えている。

2. C.D.R.不要なアーキテクチャを前提とした、より高度な情報の秘匿
    1. 個別の事業所（VC）は、P2P ベースでやり取りをするアーキテクチャであることをユーザーへ提示した結果、VC そのものの漏洩を防ぐことができるのか？という質問が寄せられている。
    2. VC の活用時には自己署名 VP の提示が必要ではあるが、セキュリティを高める観点で、第三者への VC 漏洩を防ぐ暗号化手段が今後必要となる。
    3. 認証された相手であることを確認した上で暗号化を行う既存のプロトコルとして TLS 等の既存の暗号化技術があるが、事前の相互認証に中央集権的なトラストルートがあることを前提としているため、分散化にそぐわないと理解している。
    4. そのために必要な暗号化プロトコルを選定することが今後の課題。（OSI の 5 層か 7 層のどちらが適切かについての検討も必要。）
    5. DIF は、アプリケーションレイヤーでの規格として、DIDComm Messaging という規格を提唱しており、その中で Message Encryption に触れている。今後、この規格の適用可能性・実装可能性を検討したい。
3. データ順序を確保した上での拡張性の確保
    1. JSON データの順序同一性は VC の署名検証において必須の要件となる。
    2. 一方で、データ構造の拡張性（分散環境におけるユースケース毎の独自拡張の可能性）を確保するためには、任意の拡張性を確保しつつ、検証のための順序性の固定が必要である。
    3. 実証期間中にアップデートされた V.C. 2.0 の仕様にのっとり、「JSON-LD の @context を独自に提示、共有」する、もしくは「JSON-Schema を独自に提示、共有する」形で、順不同性を維持できることを確認した。
    4. 今後の検討課題は二つある。
        ① データ構造の拡張は@context や Schema データの拡張性および後方互換性を持つ必要があると考えており、その具体的なロジックの検討が必要である。

② データ構造のチェックを行うツールの開発である。W3C の C.C.G.の中で V.C. 2.0 のテストスイートの整備が検討されており、そのスコープに@context や Schema による検証が含められるかどうかが重要な課題と考えている。

4. Credential Subject の子要素として VP を含めることの技術的意義
    1. 今回の実装では、信用の流れをつくる 2 種類の VC を入れ子構造にして検証可能な形で実装している。
    2. この実装は、安全性が高い一方で、実際に実装した場合にエンジニアにとっての実装負荷が非常に高いことが判明した。
    3. 本論点および論点 6（VC 発行依頼プロトコルに活用可能な技術プロトコルの調査および実装検討）に関する議論を内部／W3C C.C.G.と重ねた結果、VP に複数の VC を並列的に入れ込むことでより実装負荷の低い実装になる可能性が高いと整理している。
    4. VC の入れ子構造ではなく、VC の並列化については、一部実装は完了したが、検証プログラムを含めた全体的な変更はサプライチェーン等の実ユースケースへの組み込みとセットで行う必要があるため、今後の検討課題とした。
5. 分散型ネットワークにおけるトラストアンカー実現に向けたトラストリスト構築およびトラストリスト管理手法の検討
    1. ヨーロッパでは、X.509 ベースのトラストリスト提示によって、信頼できる認証機構を示す形でトラストリストの整備が進んでいる。
    2. ただ、上記のやり方は中央集権的な EU という権力機構があって初めて機能するものであり、ヨーロッパの取り組みをベースに、より多様な国家間で活用可能なトラストリスト管理のあり方について、内部で検討を重ねた。
    3. 現時点では、公的機関が提示する VC の形式でトラストリストを用意することが実装負荷／管理負荷／セキュリティの 3 つの観点でバランスの取れた実装になる可能性が高いと整理した。
    4. VC 形式のトラストリストについては本実証の中で実装を完了している。
6. VC 発行依頼（On Boarding）プロトコルに活用可能な技術プロトコルの調査および実装検討
    1. 実装上は Challenge&Response 認証のプロトコル（RFC1994）を応用して On Boarding の実装を行った。
    2. 実装の結果、当該プロトコルは今回の取り組みに合わない点も多いことが判明した。また、論点 8 と合わせた観点に見合う適切なプロトコルを検討した。
    3. 現時点では、DIF により公表された VP の交換プロトコルである Presentation Exchange および通信プロトコルである DIDComm Messaging を適用できる可能性が高いと考えているが、個人ユースケースを想定したプロトコルであること/C.D.R.を前提にしたプロトコルである可能性が高いことから、より詳細な検討が必要。
    4. 詳細検討および実装は今後の課題である。
7. 事業所（VC）のライフサイクルの精緻化

1. VC の有効性には VC そのものの失効と VC の Credential Subject に記載した記載した有効期限切れの二つがある。
2. VC ライフサイクルに関して、ユーザーから以下のようなフィードバックを得ている。
   ① 企業のコーポレートアクションに対して、どのように対応するのか？
   ② 特定の VC の失効確認時に、特定時点における失効確認が可能であるか？
   ③ 有効期限が切れた VC の失効情報を失効情報管理体は管理しているのか？
   ④ サプライチェーン上を流れる商品の寿命は場合によっては 20-30 年ある一方、一般的な電子署名で用いられる鍵はこうした長い期間使われることを想定していないが、どのように対応することを想定しているのか？
   ⑤ 更新により失効した場合、有効期限切れを起こした場合、当該 VC を業務上どのような取り扱いにすべきなのか？
   ⑥ 事業所 ID に対するオンゴーイング検証の頻度がどの程度であるのか（どの程度の即時性を期待できるか）？
3. フィードバックをもとに、エンタープライズ領域での VC の汎用的ライフサイクルの整理を行い、ビジネス価値とシステム運用コストを最適化するように、失効と有効期限の意味を精緻化することが今後の検討課題である。
4. EBSI では、この問題を長命 VC と短命 VC それぞれに求められる VC の特性という形で整理しており、参考になるが、個人向けユースケースを念頭に置いて検討しているため、そのまま活用できるかどうかは今後の検討課題である。

8. 信頼できる第三者に関わるセキュリティの確保
   1. 公的機関／デジタル認証機構は、「信頼できる第三者」に関わる組織として、高いセキュリティを確保する必要がある。
   2. 今回、JIPDEC 等の「信頼できる第三者」としての業務／サービスを提供する組織との議論を通じて、セキュリティを高めるためにより分散化したサービスを構築するべきという結論を得ている。
   3. 具体的には①公的機関（トラストアンカー）、②デジタル認証機構（事業所からの VC 発行依頼の受付）、③デジタル認証機構（事業所への VC 発行）、④デジタル認証機構（失効管理サービス）の４つにサービスを独立させ、サービス間の情報同期の実現には、プライベートブロックチェーンを活用する。
   4. このようにアーキテクチャを細分化することで、（発行済み VC や VC 発行に必要な秘密鍵等）重要な情報を保持するサービスと、インターネット上に API が広く公開され、アクセスを受ける可能性のあるサービスを独立／分化させることが可能であり、結果としてセキュリティのレベルを大きく上げることができると結論づけた。
9. ビジネス化に向けたサービス内容の精緻化
   1. 論点８によって細分化されたサービスをベースに内部で議論を重ねた結果、ビジネス化に向けて、「不特定多数への無償～安価な発行サービスの展開」と「失効管理サービスを軸とした、有償検証関連サービスの展開」というサービス内容の分化について検討を始めた。

2. 利用の浸透を図るため、発行サービスを安価に提供する一方で、サプライチェーン上の検証はビジネスによって様々なレベル頻度でのオンゴーイング検証サービスを提供することで、ビジネス化の可能性を高められないかについて、今後検討する。

10. オフライン検証
    1. Africa Union では、相互運用性のあるデジタル ID フレームワークのアーキテクチャについて検討を進めている。
    2. 分散、相互運用、デジタル主権といった点をビジョンに含んでおり、Trusted Web の理念にも通ずる取り組みであると考えている。
    3. Africa Union では、オフライン環境でのデジタル ID クレームの検証が可能であることをゴールの一つに掲げている。
    4. 事業所 ID（VC）の検証がオフラインで行われるニーズはない認識だが、Central Data Repository を必要としない我々の取り組みと技術的な親和性は高いため、今後の課題として、オフライン検証に関するニーズや技術開発の状況を把握していきたいと考えている。
11. VC 発行体に対するプライバシー
    1. Africa Union 等のハイレベル要求には、Issuer（本プロジェクトで言うところのデジタル認証機構）に対する Verifier／Holder のプライバシー要求が明示されている。（当該箇所参考訳：IDC-ID の分散化により、発行機関は個人がデジタル ID を使ってどのサービスにアクセスしたかを知ることはできないが、ID クレデンシャルの真正性はチェックすることができる。）
    2. C.D.R.を用いる場合、ブロックチェーン情報へのアクセス API の提供者（フルノード所有者）が、どのサービスにアクセスしたかを知ることができる可能性が高く、仮にアクセス API の提供者と Issuer が連合した場合、上記のようなプライバシー要求を実現できない可能性がある。この点は、W3C の Verifiable Credential Data Model v2.0 の中でも指摘がある。
    3. C.D.R.を用意しない我々の取り組みも、現状ではプライバシー要求を実現できないが、将来、この Issuer に対するプライバシー要求が高まった場合、以下の二つの方法のいずれかを採択することで、プライバシー要求に応えることができる。
        ① 失効管理サービスのアクセスログ取得を禁じる。
        ② 失効管理サービスを独立したガバナンスのもとにおき（例えば公的機関）、事業所 ID の情報とサービスアクセスログを結びつけられる主体がいない状態にする。
    4. 技術的蓋然性は確保できているが、ビジネス上のニーズおよびビジネス上の実現手法（ガバナンスのあり方/運用主体の検討）については、今後の検討課題と考えている。
12. 失効情報のなりすまし／改ざんリスクの低減
    1. 失効情報管理の API のレスポンスは署名等のつかない JSON ファイルで実装している。
    2. 失効情報管理へのアクセスポイントは、認証機構が事業所 ID（VC）内で指定している。

3. VC 内でアクセスポイントを指定しているため、通信に対するなりすまし／改ざんのリスクは限定的。
4. ただ、このリスクはより低減することが可能で、二つの解決策が存在する。
    ① 課題 2「C.D.R. 不要なアーキテクチャを前提とした、より高度な情報の秘匿」の解決によって、なりすまし／改ざんのリスクをなくす。
    ② 失効管理機構は、公的機関から VC を取得可能であり（認証機構と同じスキーム、実装済み）当該 VC＋失効情報の VC 化によって、レスポンスの改ざんリスクを無くす。
5. ①は API の複雑化、②は失効管理機構のパフォーマンス悪化を引き起こす可能性があり、実装による検証およびセキュリティ専門家との必要性の検討は、今後の課題である。

13. 鍵の保管

1. 本実証では、デジタル署名アルゴリズムである Ed25519 を使って生成した鍵の保管について比較検討はスコープ外としたが、使用したクラウドサービスが用意するシークレット管理サービス「AWS Secrets Manager」の利点と課題について考察を行う。
2. クラウドサービスの利点は、鍵に対して「暗号化して保存」「アクセス制御」「ローテーション」「モニタリング」など情報セキュリティに関する対策が備わっている点が挙げられる。
3. クラウドサービスの課題は、今回使用したクラウドサービスは鍵管理の機能がないため、例えば、AWS Key Management Service （AWS KMS）等を使用し、利用者側で生成した鍵の管理を準備する必要がある。

6.1.2　検証結果

弊社実装中に発生した課題のうち、分散化固有の課題について記載する。

事業所（VC）を複数の開発会社で申請/発行し、相互に流通させた上で事業所（VC）の Verify を行ったが Verify の失敗が続いた。原因は、事業所（VC）が正しく申請、あるいは受取りができていないことが判明した。

対応として、既存のライブラリ（JSON 処理や KMS アクセス等）の仕様に依存しているため、その内部の動作の理解、さらには各社で使用するライブラリの内部実装の差などに起因する課題の解決には、実装者同士のコミュニケーションが必要になった。

課題 1

JSON ベースの実装を行ったが、相互の署名検証に失敗した。原因は多くの既存ライブラリが JSON の順序を様々なタイミングで改変することだったが、複数開発者の間で、問題の切り分けが非常に難しかった。

課題 2

VC 一つの検証に必要な公開鍵が複数存在し、複数鍵間の関係の対応づけおよび DID と鍵の紐付けについて、全体像が複雑なため、エンジニアの理解に時間がかかった。

課題 3

各社が使用したライブラリの中で、Base エンコーディングの種類が異なっており、使用している公開鍵の取り出しに失敗していた。

7. 実証終了後の社会実装に向けた実現案と今後の見通し

7.1 残課題対応方針一覧

検証を通じて残った課題・検証を通じて新たに発見した課題・有識者から指摘を受けた課題と対応方針を記載する。

1. PKI と VC の組み合わせが本当に要求事項を満たすかに関するユーザーヒアリング
   - ユーザーヒアリングの結果、6.1.1 の No.6、7 に合わせた再検討が必要であることが判明した。要素技術として「分散した環境での VC の活用」および「認証機構における PKI（およびパーミッションドチェーン）の活用という方針に問題はないものの、ライフサイクル、およびアーキテクチャに合わせた PKI および VC の組み合わせ方（結合方法）は、改めて検討が必要と考える。
2. 脅威モデル
   - アクセス制御や鍵管理などを対象にセキュリティリスク評価を実施する。
   - 必要に応じてアーキテクチャの見直し改善を実施する。
3. 発行サービスにある「VC 登録依頼 API」と「提供 API」が同時に落ちた場合の対応
   - 両 API が同時にサービス落ちした場合、事業所 ID の申請/発行ができなくなるため、社会実装に向けて冗長化構成等アベイラビリティの向上を検討する。
4. プライベートブロックチェーンのスケーラビリティ
   - 本実証では、最も高い負荷がかかる可能性のある失効管理サービス（API）を対象に負荷テストを実施し今回の構成で問題なく処理できることは確認できたが、今後、社会実装に向けてシステム構成を検討する。
5. 選択的開示の実現
   - BBS＋実装による選択的開示の試行実装とその技術的実用性を確認する。
6. 更新された W3C 規格（VC2.0）への対応
   - 単一 VP への複数 VC 入れ子構造を実現する。
   - JSON−LD 対応のための定義作成およびチェッカー実装する。
7. オンボーディングプロセスの規格対応
   - 複数あるオンボーディング規格から適切なものを選定し実装することによる、拡張性を確保する。
8. VC ライフサイクルの精緻化と実装
   - VC ライフサイクルの精緻な仕様の策定と実装を検討する。
9. 認証機構アーキテクチャの変更
   - 失効管理サービスに対し、新たに検証サービスの機能を追加する。
   - デジタル認証機構に検証サービスを持たせることでビジネス化の可能性を広げる。
   - 事業所が DID 独自に発行可能とする SDK を準備する。

7.2 ユースケース実現モデル

7.2.1 ビジネスモデル案

■ デジタル認証機構のビジネスモデル

1. 提供方式
   - デジタル認証基盤は複数のサプライチェーンネットワーク（そのアプリケーション）に対する「協調サービス」（異業種横断共通基盤）として提供することを想定する。
2. サービス内容
   - 独立した「信頼できる第三者」としてサプライチェーンネットワークと連携し、各ネットワークに参加する事業所・事業者に対するデジタル認証＝事業所（VC）の発行と、デジタル認証の Verify をサービスとして提供する。

■ デジタル認証機構のサービスフィー（現状想定）

できるだけ多くの事業所・事業者が参加できるよう、オンボーディングにかかるフィーは低く設定した上で、デジタル認証の利用に応じたサービスフィーの課金モデルを想定する。

1. 事業者（法人等）のオンボーディング
   - 初期登録時に法人本人確認情報の提出を必須とする。
     - 無償
2. 事業所デジタル認証（審査およびデジタル証明書の発行）
   - レベル 1
     - 法人の本人確認（外部参照情報との突合等）を行う。
     - 所在は自己表明とする。
     - 事業者（法人等）毎に登録料を徴収する。（事業所は複数登録可能）
   - レベル 1 ＋レベル 2
     - 公的（準公的）機関による事業所の所在証明提出とその確認を行う。
     - 事業所 1 件目は無償とする。2 件目より登録料を徴収する。（※所在証明がデジタル化された場合、無償化を検討）
   - レベル 1 ＋レベル 2 ＋レベル 3
     - 事業所の所在を現地訪問により確認する。（※将来的には 4 次元時空間情報基盤の活用を想定。）
     - 1 事業所（デジタル証明書）毎に審査・登録料を徴収する。
3. 事業者（法人等）および事業所デジタル認証の更新・廃止
   - レベル 3 の更新については現地訪問有無により変わることを想定する。
     - 更新（毎年）
       - 発行レベルに準じる。
     - 廃止
       - 無償
4. 事業所デジタル認証の Verify

- 接続するネットワーク毎に条件を設定する想定する。
- デジタル証明（VC）に含むプロファイル情報についても要望に応じた追加を想定する。
  - 認証レベル・Verify する件数等により段階的に課金を想定する。（連携先のネットワーク毎に調整）

■ 各ステークホルダの巻き込み案

インターネット協会および沖縄オープンラボラトリでの活動を軸に、その他のステークホルダに展開する。

1. 国際標準規格化を進めるため日本規格協会の ISO/TC292/SG3 に参加し国際標準規格の検討に着手している他、半導体模倣品防止を目的とした SEMI Japan の規格に事業所デジタル認証を利用する方向で検討に参加する。
2. 社会実装に向けては、産業横断のシステム連携基盤をデザインする IPA DADC のウラノス・エコシステムとの情報交換や、デジタル技術を用いたサプライチェーンの信頼性確保を目指す団体に加盟し、社会実装に向けコミュニティ拡大を図っている。

7.2.2　アプリ・システム案

デジタル認証機構の実現に向けて、アプリ（UX/UI）に関する将来のアーキテクチャ案を整理する。

- データ主体によるコントロール

  本実証の取り組みでは、事業所（VC）は、業界・業種が違う事業者/事業所が利用することを想定し、VDR（Verifiable Data Registry）といった共通のデータ保管場所は不要で、所有者自身のウォレットアプリケーションで保管し、データコントロールする。実現に向けての取り組みとしては、所有者自身が、相手によって事業所（VC）の開示/非開示等、データコントロールできるように、ウォレットアプリケーション SDK を提供する。

- ユニバーサル性

  本実証の取り組みでは、事業所（VC）の発行・失効・更新の登録は、誰でも利用できるようにWeb ブラウザ版としたが、実現に向けての取り組みとしては、引き続き実施する。

- ユーザー視点

  本実証の取り組みでは、申請に必要な識別子は、事業所自身がユニークになる識別子（DID）で対応可能とし、事業所（VC）の利用機能は、利用ユーザーが分かりやすいように、API 提供とする。実現に向けての取り組みとしては、利用ユーザーに、DID 作成や VC/VP を使った Verify が容易にできるように、ウォレットアプリケーション SDK を提供する。

- 継続性

  本実証の取り組みでは、事業所（VC）は、W3C の DID/VC の規格に沿って開発し、事業所（VC）の申請・発行は利用者の既存システムから API コールする仕組みとする。実現に向けての取り組みとしては、一般的には、VDR（Verifiable Data Registry）を使用しているが、本実証では、①業界・業種が違う事業者/事業所が共通のデータ保管する VDR（Verifiable Data Registry）を使用することは困難②VDR に一括登録していた場合の高い漏洩リスクを回避したい、と考えており、使用しない。

- 柔軟性

  本実証の取り組みでは、①公的機関（トラストアンカー）、②デジタル認証機構（事業所からの VC 発行依頼の受付）、③デジタル認証機構（事業所への VC 発行）、④デジタル認証機構（失効管理サービス）の４つにサービスを独立させ、サービス間の情報同期は、プライベートブロックチェーンを活用する。実現に向けての取り組みとしては、引き続き実施する。

- 相互運用性

  本実証の取り組みでは、国際標準規格化を取り組む中で、国家間の相互認証の制度、国際標準化といった、実用化のための枠組みや手続きをトータルで整備する。実現に向けての取り組みとしては、国際会議で提案するため、日本規格協会および国内委員会の承諾を得る必要がある。

■ 更改容易性・拡張性

本実証の取り組みでは、事業所（VC）は、W3C の DID/VC の規格に沿って開発する。実現に向けての取り組みとしては、事業所（VC）の利用ユーザーが容易にデータコントロールできるように、サンプルアプリや SDK を用意し、OpenID for Verifiable Credentials など他の規格の開発方法を整備する。

7.2.3　ガバナンス・ルール案

Trusted Web ホワイトペーパーver.3.0 のガバナンス（全体像）に記載されている三階層で考えた場合、この章では、国内にある既存のトラストサービスを参考に、第二階層にあたる、事業所（VC）を発行するデジタル認証機構のトラストフレームワークに関するガバナンス・ルール案を示す。

※「Trusted Web ホワイトペーパーver.3.0 概要」より抜粋 [7]

トラストフレームワークとは

- 運用規則、スキーム規則、運用方針などの仕様、規則、協定の集合のこと。
- エコシステム内において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や、準拠状態を維持・監査するための、ガバナンスや監査機関を含むこともある。

既存のトラストサービス（電子署名の認証局等）を参考に Issuer のルールを策定するため、内閣官房 IT 総合戦略室「トラストに関するワーキングチーム」[8]による取り纏めにおいて提示されている枠組みに準じて、事業所のデジタル認証に対する要件を整理する。

デジタル認証機構の適格認定およびデジタル証明の国際間の利用について（想定）

- デジタル認証機構の適格要件として検討すべき事項
  1. 運営組織の健全性・公平性
  2. デジタル証明書の発行および管理に関する基準（通常よりも厳格な基準）
  3. デジタル証明書が適格であることを示す記載に関する基準
- デジタル証明が国際的に通用するために検討すべき事項
  1. 適合性評価機関が満たすべき基準と制度上の位置づけ
  2. 適格認定およびデジタル証明の国際的な相互承認（同等性）の要件
  3. 公的機関が管理する Trusted List に関する基準

[7] 内閣官房デジタル市場競争本部事務局.「Trusted Web ホワイトペーパーver.3.0 概要」.
https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/pdf/trustedweb_3_gaiyou.pdf

[8] 内閣官房 情報通信技術室（IT）総合戦略室.「トラストに関するワーキングチーム-中間報告-」.
https://www.soumu.go.jp/main_content/000750520.pdf

トラストサービスプロバイダーの共通要件（認証局の例 [9]）

■　運用基準

1. 利用者の真偽の確認
2. 関係要員および運用体制
3. アクセス認証
4. 運用管理（含、CP/CPS）
5. 電子証明書のライフサイクル管理

■　技術基準

1. ネットワーク管理
2. 認証・権限確認
3. 認証局の秘密鍵の管理

■　設備基準

1. 建物
2. 設備への物理的アクセスコントロール

[9] 一般財団法人 日本情報経済社会推進協会.「JIPDEC トラステッド・サービス登録（認証局）」. https://www.jipdec.or.jp/project/jtsr/ca.html

デジタル認証機構としての個別要件（想定）

■ 運用基準

1. 利用者の真偽の確認においては、デジタルガバメントの進展を念頭においた追加的な手法および、（認証レベルに応じた）厳格な確認の手法を定める。
2. 運用管理においては、分散 ID の利用を念頭においた追加的な手法（利用者に対するウォレットアプリ提供等）を定める。
3. 電子証明書のライフサイクル管理においても、分散 ID の利用を念頭においた追加的な手法（CRL または OCSP 等に代わる失効証明の仕組み等）を定める。
4. デジタル認証機構の終了においては、利用者の継続利用を念頭においた手続きを定める。

■ 技術基準

1. 運用基準にあげた、分散 ID の利用を念頭においた追加的な手法を提供するために必要となる技術的な措置を定める。

■ 設備基準

2. 現時点で特段の追加要件はない。

※上記は「デジタル認証機構」に対する要件であるが、分散 ID を活用する場合にはトラストを担保するために利用者が満たすべき要件（利用者自身による鍵管理およびデジタル署名の仕組み等）についても別途定める。

7.3 実現に向けたアクション・ロードマップ

実証事業の検証を通じて今後の展望について記載する。

タイムライン	マイルストン	マイルストン達成に向けて実施すること
2024年	国際標準化に向けた新規提案の準備	• 実証事業の結果を踏まえ国際標準化の予備段階PWI（Preliminary work item）から提案段階NP（New work item proposal）へ進める。
2024年	デジタル認証機構の受皿機関選定	• パイロット実施対象のサプライチェーンにおいてデジタル証明書を発行する機関の候補団体を調整する。 • デジタル認証機構を認定する枠組みについてJIPDEC協力のもと検討する。
2024～25年	パイロット導入・検証	• デジタル認証機構のネットワークとサプライチェーンネットワークを結ぶパイロットシステムと運営体制を構築し導入する。
2026年	商用化範囲の拡大	• パイロット導入の結果を受け、認証機構ネットワークの業務プロセス、規約・ルールを確立する。
2027年	国際標準規格の発行	• 商用化リリースに向けた活動と並行して、国際標準化団体において、IS（International Standard）化を進める。

図 7-3-1：実現に向けたアクション・ロードマップ

8. Trusted Web に関する考察

8.1 求める機能や Trusted Web ホワイトペーパーver.1.0 の原則に関する課題と提言

Trusted Web で求める機能と Trusted Web ホワイトペーパーver1.0 の設計・運用における原則に対し、今回の実証事業の取り組みの中で気づいた課題や提言について記載する。

- 求める機能

  今回、事業所（VC）を使ったユースケースヒアリングの中で、製品によっては 10 年以上使用することがあるため、購入時の確認だけではなく、「過去のある時点で事業所が存在していた証明に使えるのか」という話があった。このような、データのやり取りにおける「過去の合意形成」をトレースする仕組みは、ブロックチェーンが活用できるのではないかと考える。

- Trusted Web ホワイトペーパーver1.0 の設計・運用における原則

  今回、事業所（VC）を使った Verify をする際、トラストアンカーが確認できるように、事業所（VC）の中に、入れ子構造でデジタル認証機構（VC）を入れていたが、VC の構造が複雑になり、事業所の Verify に関する開発が困難になることが分かったため、VP の中に VC を並列にした構造がより適切と考える。

  また、本実証では、デジタル認証機構は事業所に対して事業所（VC）を直接発行し、事業所自身が事業所（VC）を管理・運用することで分散性が高まると考え、デジタル認証機構として Verifiable Data Registry（VDR）は準備しなかったが、 Data-Spaces-Business-Alliance の資料を参考にすると、デジタル認証機構とは別組織で VDR を用意し、トラストアンカーに関するデータ（公開鍵等）を管理することで、入れ子構造が解消し、構成部品が疎結合に構成され、柔軟性が向上できるのではないかと考える。

  ただし、単純な鍵の検証になると、VC 以外に、X.509 でも対応ができると想定するため、専門委員で X.509 と VC の利用比較を準備頂きたいと考える。

8.2 Trusted Web のガバナンスに関する課題と提言

- マルチステークホルダーと政府の役割

  国家間サプライチェーンの管理に対して政府の果たす役割はトラストアンカーになると理解している。従来、国家間はトラストレスな関係であり、そこに明示的なトラストをかけること自体が今後の貿易に対するリスク低減に繋がり、国益に資すると考える。弊社の取り組みで言えば、公的機関の間で取り交わされるトラストリストの管理機能を政府機関が担うことで、分散型の世界でトラストを行き渡らせることが可能になると理解する。

- 透明性とインセンティブ

  透明性や検証可能性は、プライバシーへの配慮なしには実現しないと考えている。例えば「どんな条件下で、誰が検証可能なのか」や「ビジネスの維持可能性の観点では、匿名性は必要か？プライバシーは必要か？」といったより精緻な方針が必要になると理解している。
  本取り組みでは、Unlinkability といった概念の実現や ZKP によるプライバシー課題の解決ではなく、Central Data Registry が必要ではないアーキテクチャによる解決方法を模索している。これはプライバシーリークの「可能性が低い」ではなく、そもそも「プライバシー情報の存在を知り得ない」という形でプライバシー課題を解決しておくことで、エンタープライズで求められるより高い要求への回答になるのではないかと考える。（実際、エンタープライズ領域での Unlinkability 要求は個人レベルとは全く異なるレベルにある可能性があると考えている）

- 脅威モデルの提供

  Trusted Web の概念がビジネス面から見て有用であることを示すためには、Trust を脅かす具体的な脅威についての共通認識が必要だと考える。どのような脅威が想定できるのか？脅威の顕現による経済的な被害がどのように発生するのか、被害額の想定はどのように算定できるのか？脅威に対して、従来型の Web アプリケーションでは防ぐことができず、Trusted Web を利用することでどのように軽減できるのか？こうした点について、より掘り下げた議論と、それに基づく共通した（脅威による被害額を算定可能な）脅威モデルの提供が必要であると考える。

8.3 Trusted Web のアーキテクチャに関する課題と提言

Trusted Web ホワイトペーパーver3.0 のアーキテクチャの中から、課題と提言を記載する。

発信者と受信者の関係性を、直接取引のようなクローズドな関係と間接取引になるオープンな関係の２種類で考えた場合、発信者と受信者の間におけるデータの配送方法は、違いがあると考える。本実証でヒアリングをした際、オープンな関係の場合、相手先によって自身を特定する情報を開示したくない話があった。ただし、発信者を特定する情報が非開示な場合、

1. Verifiable Identity

   受信者は、発信者を特定する情報が非開示なデータをどのように Trust できるか

2. Verifiable Messaging

   受信者が、発信者を分からずにデータをどのように受信するか

課題があると考える。

上記２点に関する提言は、ゼロ知識証明のような、発信者が証明したいデータ以外、受信者に開示不要な仕組みができると対応できるのではないかと考える。

8.4 その他 Trusted Web に関する課題と提言

- 日本における「トラストサービス」の実現に向けた協調を促進
  Trusted Web 実証事業に採択されたユースケースでは、当方が提案するデジタル認証機構のような信頼できる第三者の存在を想定（もしくは自らが信頼できる第三者であることを想定）しており、デジタル庁の「トラストを確保した DX 推進サブワーキンググループ」の 報告書（令和 4 年 7 月 29 日）において提示された「トラストサービス」の存在を前提としている。
  これらの「トラストサービス」を社会基盤として実現するためには、官民連携によるルール・体制作りが必要であり、既に進められている取り組み（例えば IPADADC が進めるウラノス・エコシステム等）との協調を促す場の提供および旗振りを Trusted Web 推進協議会にお願いしたい。

Appendix

用語集

表 9-1-1：用語集

用語	内容
事業所 ID	事業所の Identity を表すデジタル証明書。 本実証では、Verifiable Credentials（VC）を使ったデジタル証明書を使用するため、事業所 VC と称する。
識別子	本実証では、事業所自身が W3C の DID を使った識別子を準備する。
公的機関	事業所 ID の真正性を保証するトラストアンカーの役割を有すると仮定する。
デジタル認証機構	公的機関から認定された信頼できる第三者機構とし事業所 ID を発行すると仮定する。
事業所	サプライチェーンに参加者し、他のサプライチェーン参加者である取引先に対し、検証可能な事業所 ID を使って自身の実在性を証明する。または、取引先の検証可能な事業所 ID を取得し、取引先の実在性を検証する。
事業者	「事業所の所在をデジタルに証明する仕組みがない」点がペインポイントと考える。 本実証では、信頼できる第三者が事業所の真正性を証明するデジタル証明書（事業所 ID）を発行することで、事業所 ID を使った事業所の真正性を検証可能とし、ペインポイントが解決できるか検証する。
Trusted List	公的機関がデジタル署名したデジタル認証機構のデジタル証明書の検証に必要な情報（本実証は DID と公開鍵）を含んだリスト。 リストは、各国で 1 つと仮定し、公的機関が発行し、デジタル認証機構を通じて事業所は入手する。 また、海外の特定国と相互承認が行われた場合、その国のデジタル認証機構のデジタル証明書の検証に必要な情報を自国の Trusted List に追加する。

本実証で開発したシステムの第三者による再現可能性

■ ライセンス取得は不要

1. 開発したプロトタイプシステムはオープンソースで構築し、そのソースコードと利用手順書を GitHub 上で公開することで、第三者による再現可能である。
2. デジタル認証基盤で使用する「DID」「デジタル署名で使用する Key ペアー」の管理については、別途「AWS Secrets Manager」の準備が必要である。
3. 対象システム
    - デジタル認証基盤
        - 公的機関
        - デジタル認証機構
        - 失効管理サービス
    - サプライチェーン参加事業所

■ ライセンス取得が必要

1. SBI R3 Japan が販売するブロックチェーン基盤 Corda の開発ライセンスを使用することで再現可能である。
2. ソースコードと利用手順書を GitHub 上で公開することで、第三者による再現可能である。
3. 対象システム
    - 分散台帳アプリ構築システム
    - 分散台帳ネットワーク構築システム

ヒアリング詳細・結果
ICT 機器・サービス提供会社のヒアリング結果を記載する。

【論点１】
サプライチェーンに伴う情報を流通させるにあたって、業界・業種を跨った事業所間で情報を記録する主体の真正性を担保する仕組みがない。

【ヒアリング事項と回答１】
■ 事業所 VC に対し、他に含みたいと思う情報はあるか。
1. 誰がどのように確認したか、審査方法や審査エビデンスがあると良い。
■ 川下になる第三者の取引先から自身の事業所の実在性確認が来た場合、事業所 VC を例にして、提示できる情報は何があるか。
1. 開示・非開示は契約に準ずるものと考えるため、ゼロ知識証明的な価値があるとユースケースが拡大すると想定する。
2. 稼働（あるいは生産）しているという情報があるとよい。

【論点２】
サプライチェーンに伴う情報を流通させるにあたって、国境を跨った事業所間で情報を記録する主体の真正性を担保する仕組みがない。
※事業所 VC が国境を跨って利用する場合の有用性

【ヒアリング事項と回答２】
■ 海外で発行した証明書を確認する際、海外のトラストアンカーが確認可能なデジタル証明書は有用であるか。
1. 証明書発行機関のスコープによるが、基本的に各組織が証明書を準備すると考えるため、自組織以外の第三者が証明しなければならない場合には有意である。

【論点３】
広く利用されるためにトラストの単位（事業所）の申請者をどのように設定すべきか判明していない。

【ヒアリング事項と回答３】
■ サプライチェーンにおけるバイヤーが n 次のサプライヤーたちに対して、サプライヤーの実在性を確認した際、各サプライヤーの実在性の証明はどの単位になるか。
1. 基本的にサプライヤー自身の実在性証明になるが、いくつか例外ケースがある。例えば、EMS（Electronics Manufacturing Service）の場合、製造を請け負った製造工場の代わりにメーカーの実在性が証明書になる。