令和4年度補正Trusted Web 開発等推進事業に係る調査研究
Trusted Web ユースケース実証事業
最終報告書 概要版

「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）

SBIホールディングス株式会社

2024年3月15日

目次

1. 背景･目的

1. 背景・目的（1/2）

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。更に製造業分野においては、EU電池指令や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来ている。
- 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する必要であることが明らかになった。

※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）

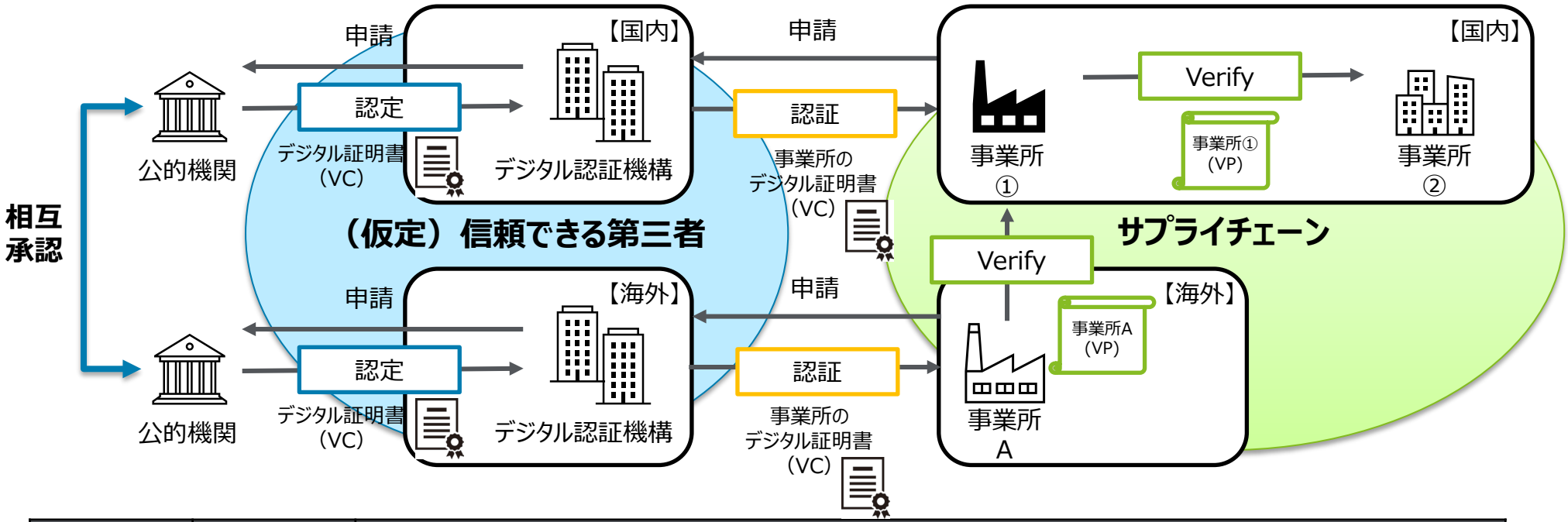
1. 背景・目的（2/2）

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、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。

2. 事業の概要

2.1. 登場する主体と概要



主体	区分	ユースケースにおける役割
公的機関		• 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	発行サービス	• 事業所のデジタル証明書（VC）（以降は、事業所（VC）とする）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。
	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ーとする。 • 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	サプライヤー	• 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）をバイヤーに提示する。
	バイヤー	• 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。

2.2. 現状の課題を解決する事業スキーム案

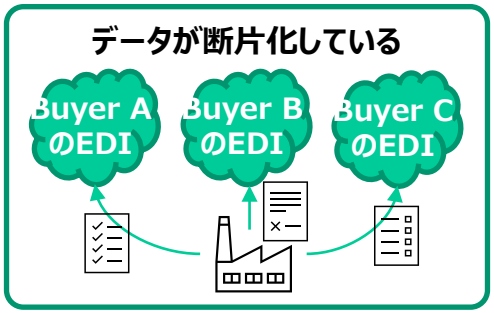
現在の課題（ペインポイント）

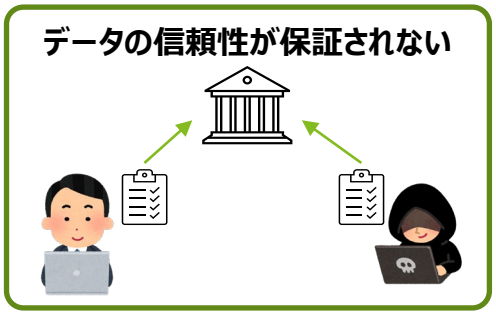
- サプライチェーンのデータが断片化している
  （標準化されておらず冗長で非効率な状況）
- サプライチェーンのデータ信頼性が保証されない
  （情報の誤りや偽造のリスクがある）
- 中小企業を含むサプライチェーン全体のネットワーク化が進んでいない
  （中小企業が情報ネットワークから取り残されている）

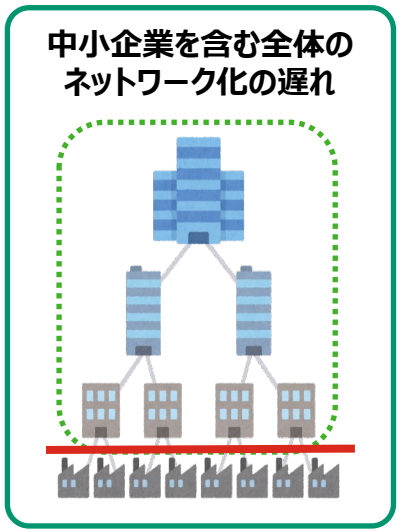
事業所IDとそのデジタル認証により解決する内容

- サプライチェーンに参加する事業者・事業所を識別・認証する事により、相互接続性のある信頼できるサプライチェーンネットワークを実現
- 複数の業種別・企業グループ別のネットワークを相互に接続し、更には国家間相互承認の規格を設ける事により国を跨って信頼できるサプライチェーンネットワークを実現

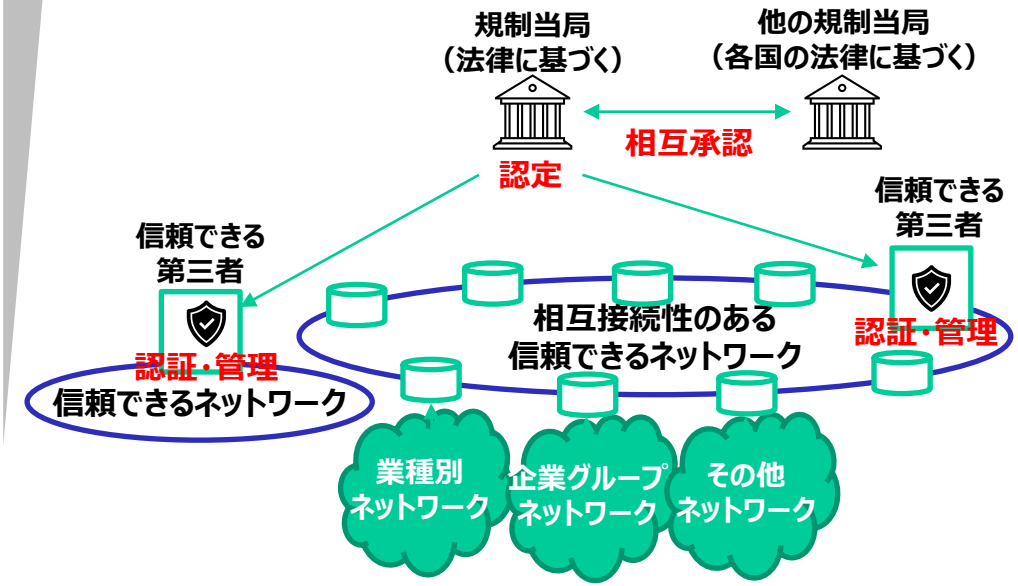
課題解決前の状況（As-Is）







創出するユースケースの事業スキーム図（To-Be）



2.3. 社会・経済に与える影響・価値(1/2)

- 2008年の米国政府調査 ※1 （Defence Industrial Base Assesment: Counterfeit Electronics, U.S. Department of Commerce, January 2010）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9000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（Trends in Trade in Counterfeit and Pirated Goods, OECD and European Union Intellectual Property Office , March 2019）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5000億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ほか、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。

※1 米国政府調査（Defence Industrial Base Assesment: Counterfeit Electronics, U.S. Department of Commerce, January 2010）
https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file

2.3. 社会・経済に与える影響・価値(2/2)

■ 本取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来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商取引情報の真正性を保証
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

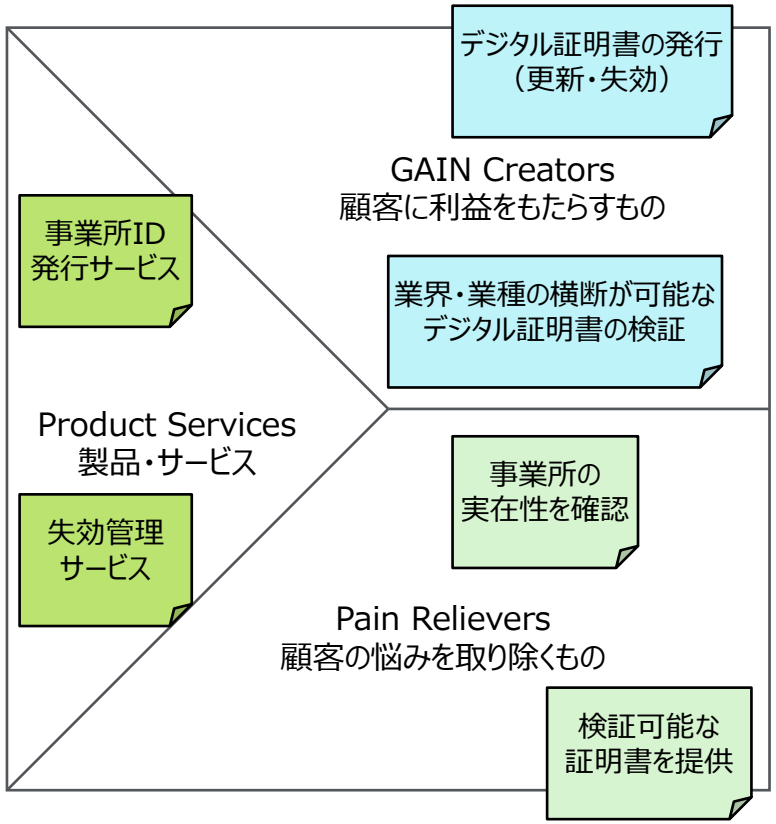
2.4. ペイン･ゲインの整理 （Value Proposition Canvas)

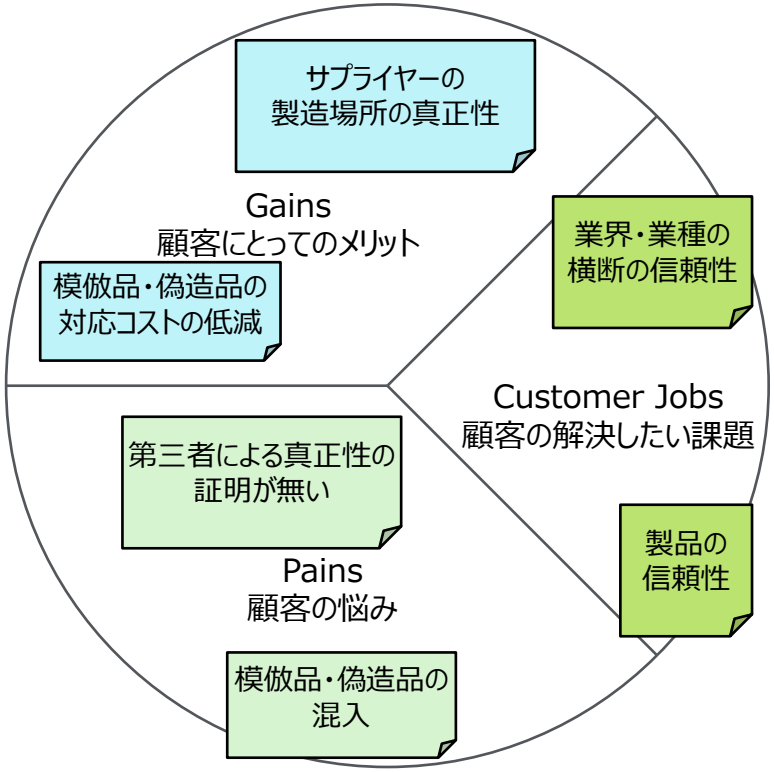
Value Proposition
企業が顧客に提供できる価値

- 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





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（1/4）

実証事業計画や有識者との討議を踏まえて、本実証で明らかにする論点の導出を行った。

観点	明らかにする論点		論点設定の背景	論点解決に向けた検証概要
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	• 事業所（VC）を容易に利用する仕組みが必要であると考える • 事業所（VC）の利用者が継続的に利用する仕組みが必要であると考える	【6.1章で報告】 • 事業所（VC）の発行依頼 利用可能なプロトコルを比較検討する • スケーラビリティ パーミッションドブロックチェーンを用いて、デジタル証明書（VC）検証の仕組みがスケーラブルに実装できることを検証する • 耐障害性 分散化したデジタル認証機構のうち発行・管理サービスがダウンしてもデジタル証明書の有効性が検証できる • アーキテクチャ 本実証ではパーミッションドチェーンを利用しているが、その他の実証結果を元に、パーミッションドチェーンとパブリックチェーンの比較軸を設定し整理する
	2	信頼性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	• 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話があがり、両者を組み合わせて検討する	【6.1章で報告】 • 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

3.1. 実証事業で明らかにする論点への導出・経緯（2/4）

実証事業計画や有識者との討議を踏まえて、本実証で明らかにする論点の導出を行った。

観点	明らかにする論点		論点設定の背景	論点解決に向けた検証概要
アーキテクチャ	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討する	【6.1章で報告】 以下について実現可否の検討結果を報告する 1. 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 2. 商品の寿命は場合によっては２０－３０年ある場合に、紐づく事業所ID（VC）を正しく管理されるのか 3. 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点 4. 企業の真正性を証明するVCについて、更新により失効した場合、あるいは有効期限切れの場合、どのような取り扱いになるのか 5. 企業のコーポーレートアクションに対してどのように対応するのか
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の分類を見直す	• 「NIST SP 800-63」第4版ドラフトを確認し、eIDASの分類との違いを確認する	【5.1.2章で報告】 • 事業所ID（VC）は法人向けだが、「NIST SP 800-63」第4版ドラフトの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

3.1. 実証事業で明らかにする論点への導出・経緯（3/4）

実証事業計画や有識者との討議を踏まえて、本実証で明らかにする論点の導出を行った。

観点	明らかにする論点		論点設定の背景	論点解決に向けた検証概要
ビジネスモデル	1	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	• 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などどのような単位があるか検討する	【4.4.5章で報告】 • 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する
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	• 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討する	【4.4.2章で報告】 • 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する
	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	• 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討する	【4.4.2章で報告】 • 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する
	3	デジタル認証機構の社会実装に向けた枠組みをどうすべきか	• 例えば、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など、今後の枠組みを検討する	【7.2章で報告】 • ユースケース実現案で報告する

3.1. 実証事業で明らかにする論点への導出･経緯（4/4）

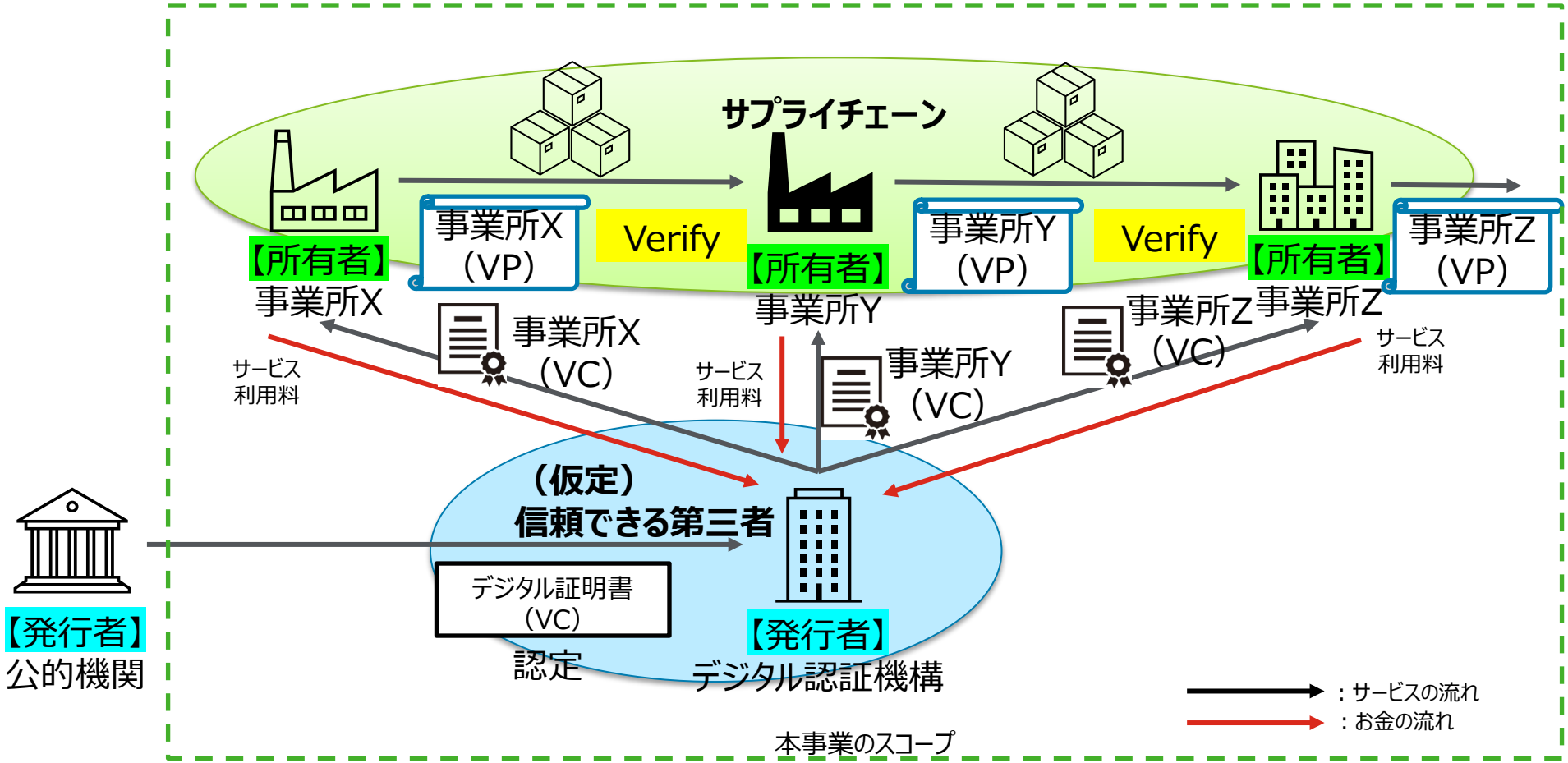
実証事業計画や有識者との討議を踏まえて、本実証で明らかにする論点の導出を行った。

観点	明らかにする論点		論点設定の背景	論点解決に向けた検証概要
非機能	1	セキュリティについて、脅威モデルを検討、その上で、システムのセキュリティリスクを評価し、必要な場合はアーキテクチャを分けること	• 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、サービスが停止に対する、現時点の考えの共有	【7.1章で報告】 • 残課題対応方針一覧で報告する
	2	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し、VC登録依頼APIと提供APIが同時に落ちた場合の対応も検討すること	• 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、サービスが停止に対する、現時点の考えの共有	【7.1章で報告】 • 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（1/9）

事業所の実在性を保証する事業所ID ※1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。

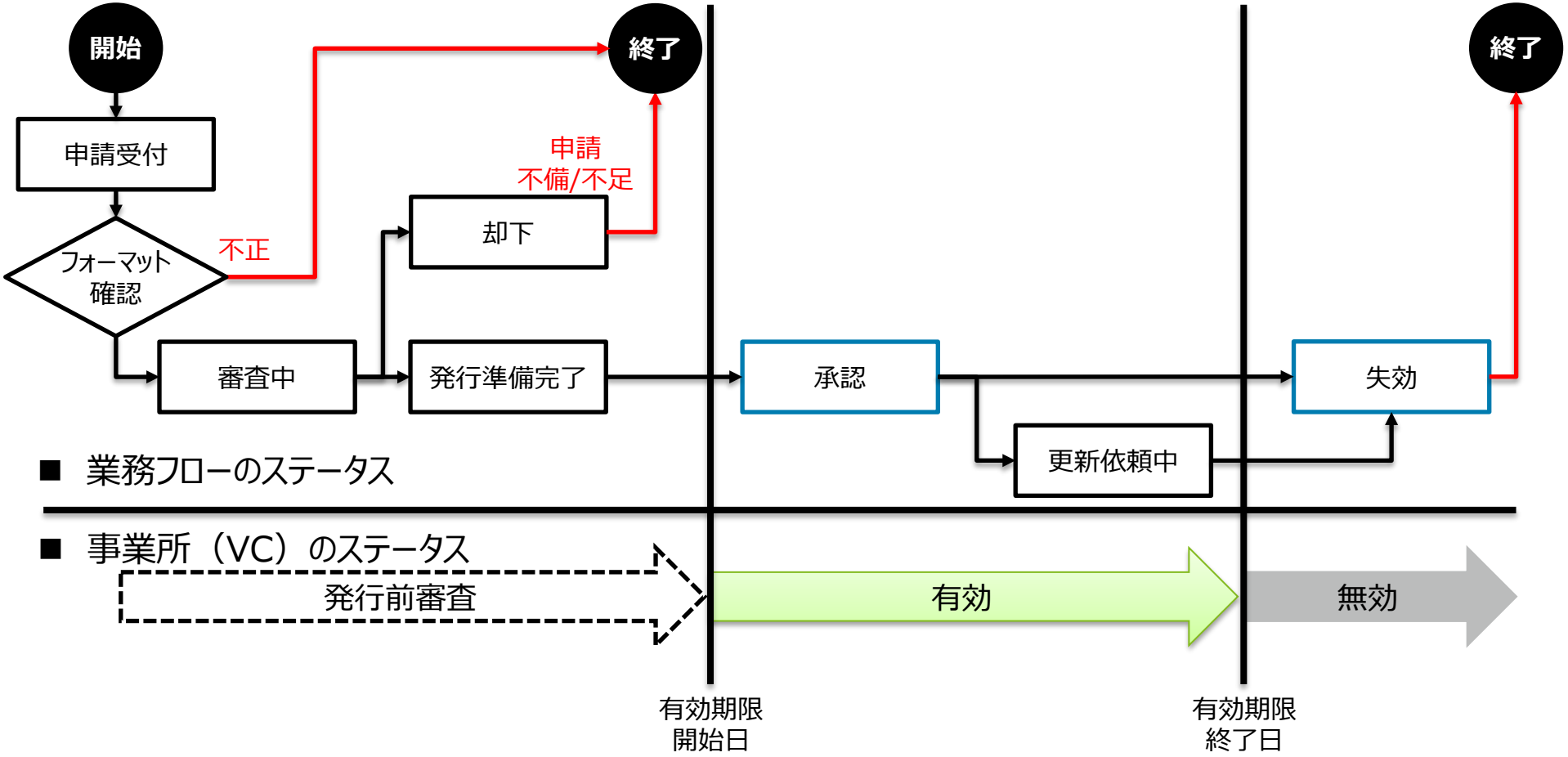
1. **信頼できる第三者が認証した事業所（VC）**を発行する
2. 提示する際、事業所（VC）の所有者の意思で相手に事業所（VC）を提示していること証明するため、**事業所（VC）を包んで自己署名した事業所（VP）**を作成し、相手は事業所（VP）を使って信頼性をVerifyする



※1　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. 本事業におけるスコープ（2/9）
「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。



3.2. 本事業におけるスコープ（3/9）
「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※1に基づき、申請者情報を審査する。
   ④ 審査の結果
      a. 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。
      b. 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。

■ 申請者情報

事業所のDID	事業所情報	事業者情報
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）

※1 詳細は「7.2.3 ガバナンス・ルール案」を参照

3.2. 本事業におけるスコープ（4/9）
「事業所（VC）内容」

①W3C規格

Verifiable Credential
検証可能な資格情報

Credential Metadata
- 利用規格、証明書名
- 発行者、発行日付

Claim(s)
- DID Document
- 資格情報

Proof(s)
- 発行者の検証に使用する情報

②事業所（VC）の構成

利用規格、証明書名等

DID Document＋資格情報
①事業所のDID
②事業所情報
③事業者情報
④発行者及び認定者名称
⑤発行者のVCが入ったVP
⑥認証レベル等

発行者、発行日付
①発行者のDID
②発行者名
③発行日付/有効期限

発行者の検証に使用する情報
①発行者の公開鍵
②発行者のデジタル署名

③事業所（VC）の内容

```
{   "vc": {
      "@context": ["https://www.w3.org/2018/credentials/examples/v1"],
 (省略)
    "credentialSubject": {
        “didDocument”: {
            "@context": "https://w3id.org/did/v1",
            "id": "did:example:GUi5XHMycjqd1pe",
            “verificationMethod”: [
              {
               "id": "did:example:GUi5XHMycjqd1pe#vcauth-bu1-key",
               "type": "Ed25519VerificationKey2018",
               "controller": "did:example:GUi5XHMycjqd1pe",
               “publicKeyMultibase”: “z6sMHtayMaCQXw1NEEhe99F
YwwHaofTAb6zKAvF”} ]
        },
         “authenticatorInfo”: {（省略）},
         “businessUnitInfo”: {（省略）},
         “legalEntityInfo”: {（省略）},
         "authenticationLevel": "1",
         “revocationEndPoints”: ["http://uat.detc.link:3001/revoke-1/vc-
status/{uuid}",],
         “linkedVP”: {（省略）},
         “uuid”: “550e8400-e29b-41d4-a716-446655440000“
        },
   “issuer”: {
              "id":"did:detc:JPDigitalCertificateOrganization1: T1U9…(省略)# "
              "name": "JP Digital Certificate Organization 1"},
   "validFrom": "2023-09-20T06:52:09.093Z",
   "validUntil": "2024-09-20T06:52:09.093Z",
   "proof": {
        "type": "Ed25519Signature2018",
        "created": "2023-09-20T06:52:14Z",
        "proofPurpose": "assertionMethod",
        "verificationMethod":"did:detc:JPDigitalCertificateOrganization1:
T1U9…(省略)#vcauth-bu1-key”,
              “signatureValue”:“z58DAdFfa9SkqZMVPxAQa…(省略)"}
}
```

3.2. 本事業におけるスコープ（5/9）
「事業所（VC）失効（1/2）」

■ 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UUIDを使って失効確認をする際、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IDを失効した状態
    - 事業所が存在しないUUID ※1を使って失効確認

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、事業所（VC）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側）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。
   （本実証で検証無し）

※１　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. 本事業におけるスコープ（6/9）「事業所（VC）失効（2/2）」

■　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。

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	Valid	Valid
発行した事業所（VC）の有効期限切れ	Invalid※	Invalid※
デジタル認証機構が事業所（VC）を失効	Revoked	Invalid
事業所が存在しないUUIDを使って失効確認	Unknown	Invalid

※有効期限の管理は本実証スコープ外

3.2. 本事業におけるスコープ（7/9）
「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んだ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. 本事業におけるスコープ（8/9）
「Trusted List（1/2）」

■ 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」を国ごと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

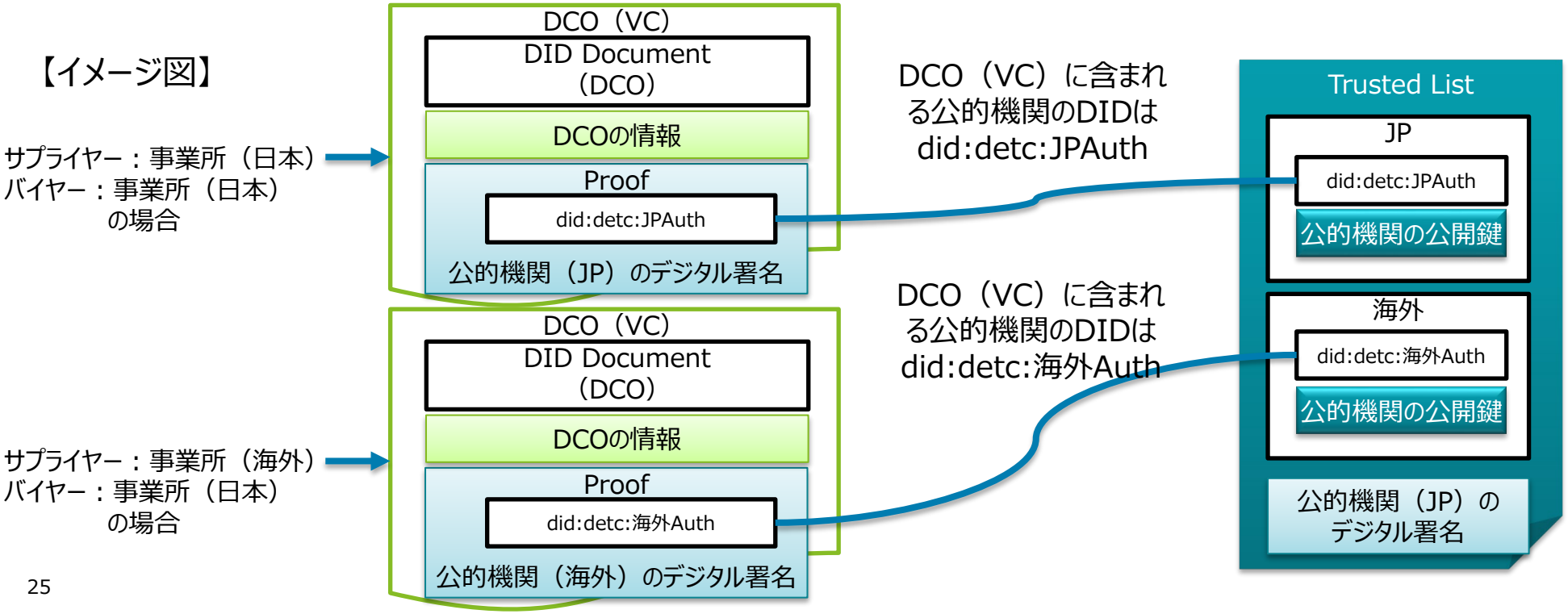
3.2. 本事業におけるスコープ（9/9）「Trusted List（2/2）」

■ 注釈
デジタル認証機構＝DCO

■ 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

【イメージ図】



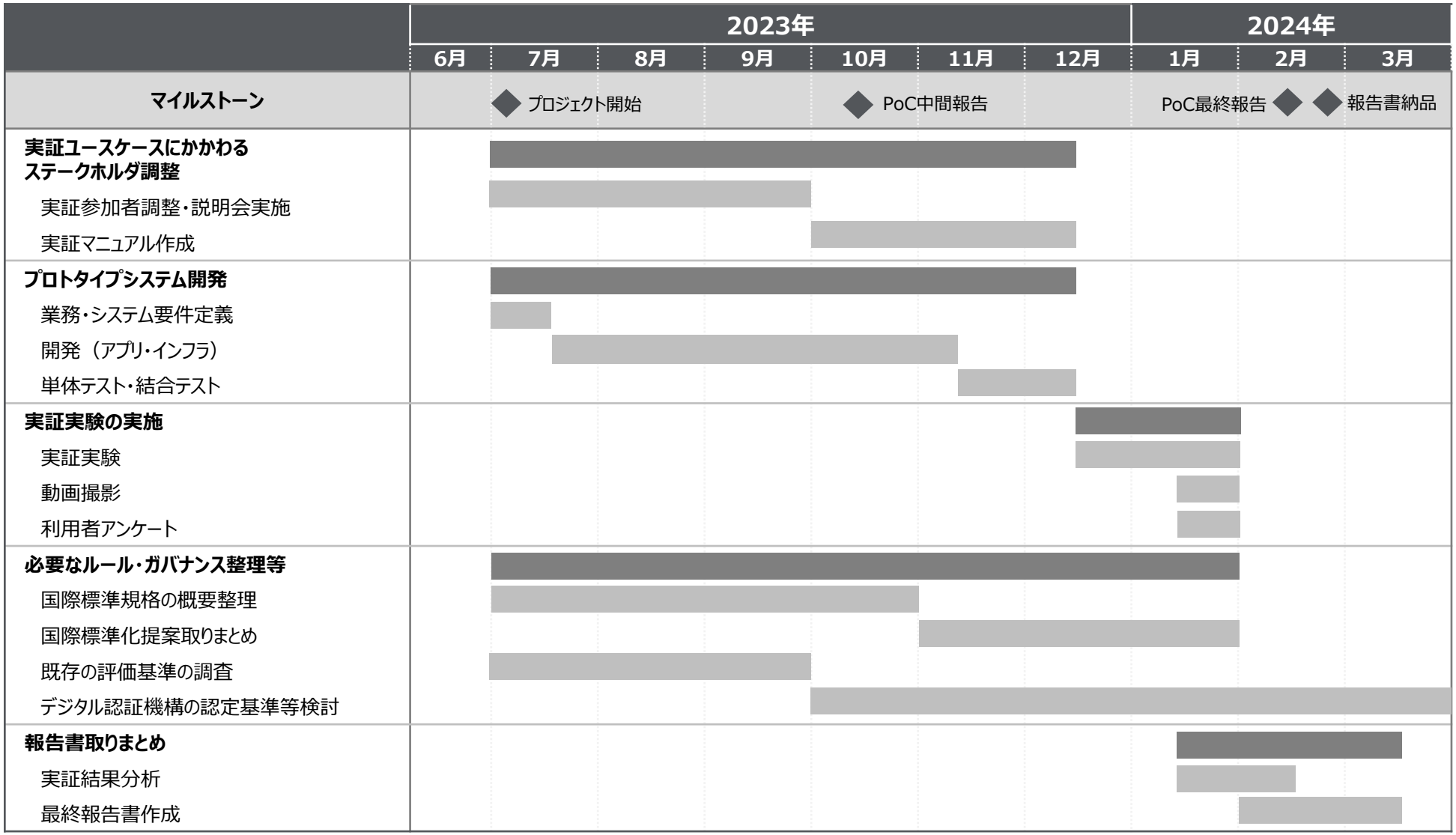
3.3. 実施事項・成果物一覧（1/2）

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及びIndustry Trust Chain HUB」参加企業、及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

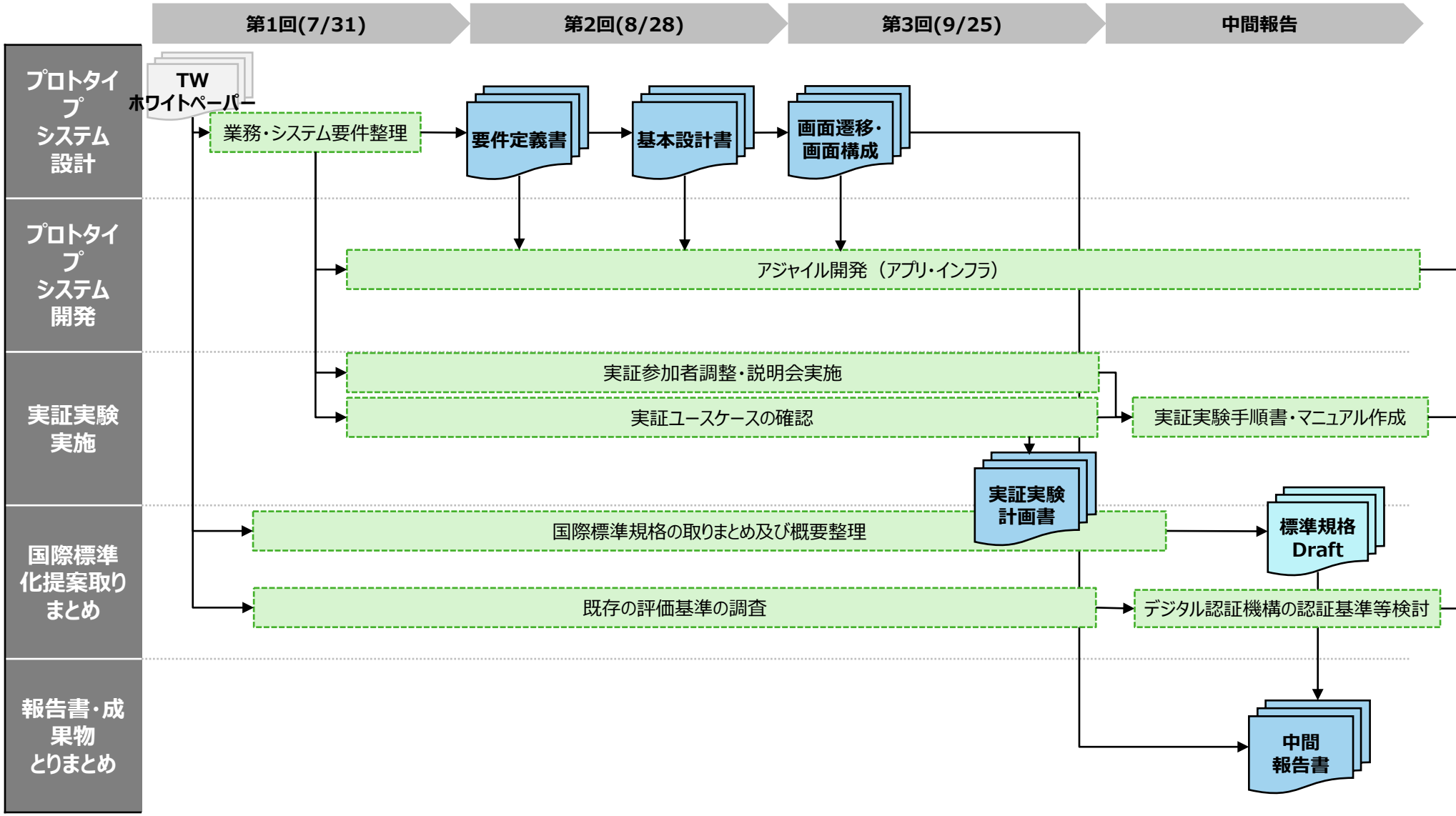
3.3. 実施事項・成果物一覧（2/2）

実施項目		具体的な作業内容	担当(会社名)	想定成果物
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

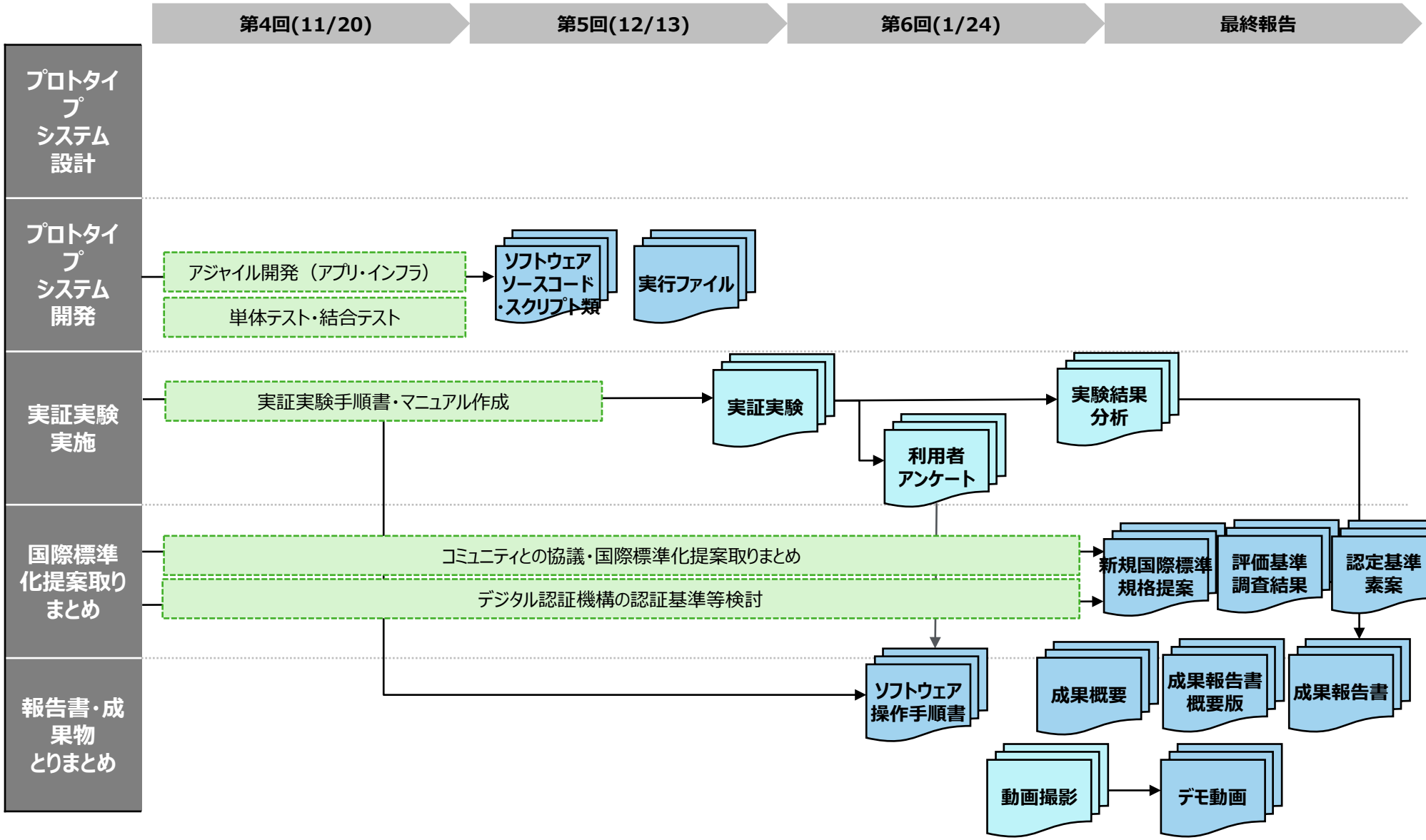
3.4. スケジュール
3.4.1. 全体スケジュール



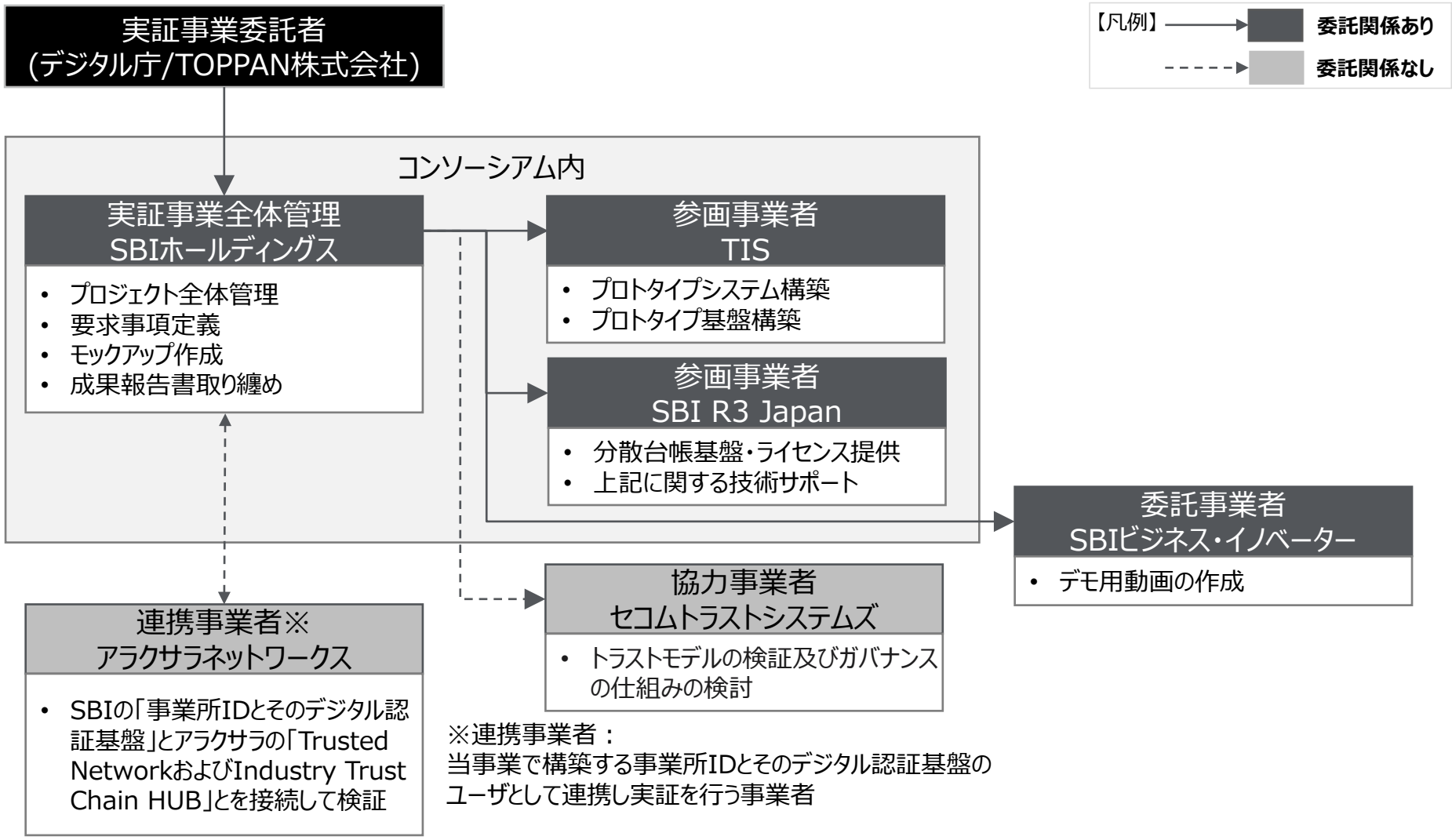
3.4. スケジュール
3.4.2. 成果物の作成フロー(1/2)



3.4. スケジュール
3.4.2. 成果物の作成フロー(2/2)



3.5. 実施体制


【凡例】
委託関係あり
委託関係なし
実証事業委託者
(デジタル庁/TOPPAN株式会社)
コンソーシアム内
実証事業全体管理
SBIホールディングス
• プロジェクト全体管理
• 要求事項定義
• モックアップ作成
• 成果報告書取り纏め
参画事業者
TIS
• プロトタイプシステム構築
• プロトタイプ基盤構築
参画事業者
SBI R3 Japan
• 分散台帳基盤・ライセンス提供
• 上記に関する技術サポート
委託事業者
SBIビジネス・イノベーター
• デモ用動画の作成
協力事業者
セコムトラストシステムズ
• トラストモデルの検証及びガバナンスの仕組みの検討
連携事業者※
アラクサラネットワークス
• SBIの「事業所IDとそのデジタル認証基盤」とアラクサラの「Trusted NetworkおよびIndustry Trust Chain HUB」とを接続して検証
※連携事業者：
当事業で構築する事業所IDとそのデジタル認証基盤のユーザとして連携し実証を行う事業者

4. 実証（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

No.	論点	検討結果とその経緯

1	取引先事業所の正当性を担保する仕組みがない	• 検討経緯
		  • 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
		  • 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
		  • 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
		• 検討結果
		  • 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
		  • 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

2	デジタル認証機構の正当性を担保する仕組みがない	• 検討経緯
		  • 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
		  • 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
		  • 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
		• 検討結果
		  • 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
		  • 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. 実施概要
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及び背景

No.	活用技術・規格	実現したい要件	選定理由とその経緯
1	• Verifiable Credentials Data Model v2.0 draft 6月（W3C）	• 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、W3CのVerifiable Credentials を活用する。	• 証明したい情報が、credentialSubject内で、自由に設定が可能で、Verifiable Credentials だけで検証可能なデジタル証明書が作成できるため。
2	• Decentralized Identifiers (DIDs) v1.0（W3C）	• 事業所（VC）の申請に必要な、識別子を事業所自身で作成するため、W3CのDIDsを活用する。	• Verifiable Credentialsを使用する際、VCのHolderに対する識別子が必要である。鍵の識別子を表現するフォーマットとして、DIDs、X.500 name、JWKS等が考えられた。本ケースでは、公開された事業者の下部組織である事業所に属する識別を必要としている。また事業所には一定程度の匿名性要件もあるという仮説をもっていた。そのため、事業所を表現するアクセスエンドポイントの存在及びその共有を仮定するJWKSやデータ項目にセマンティクスとして国情報などを含むX.500を避け、識別子及び公開鍵のみをデータ項目として持ち、エンドポイントの公開に関しても自由度を持つDIDsを採用している。

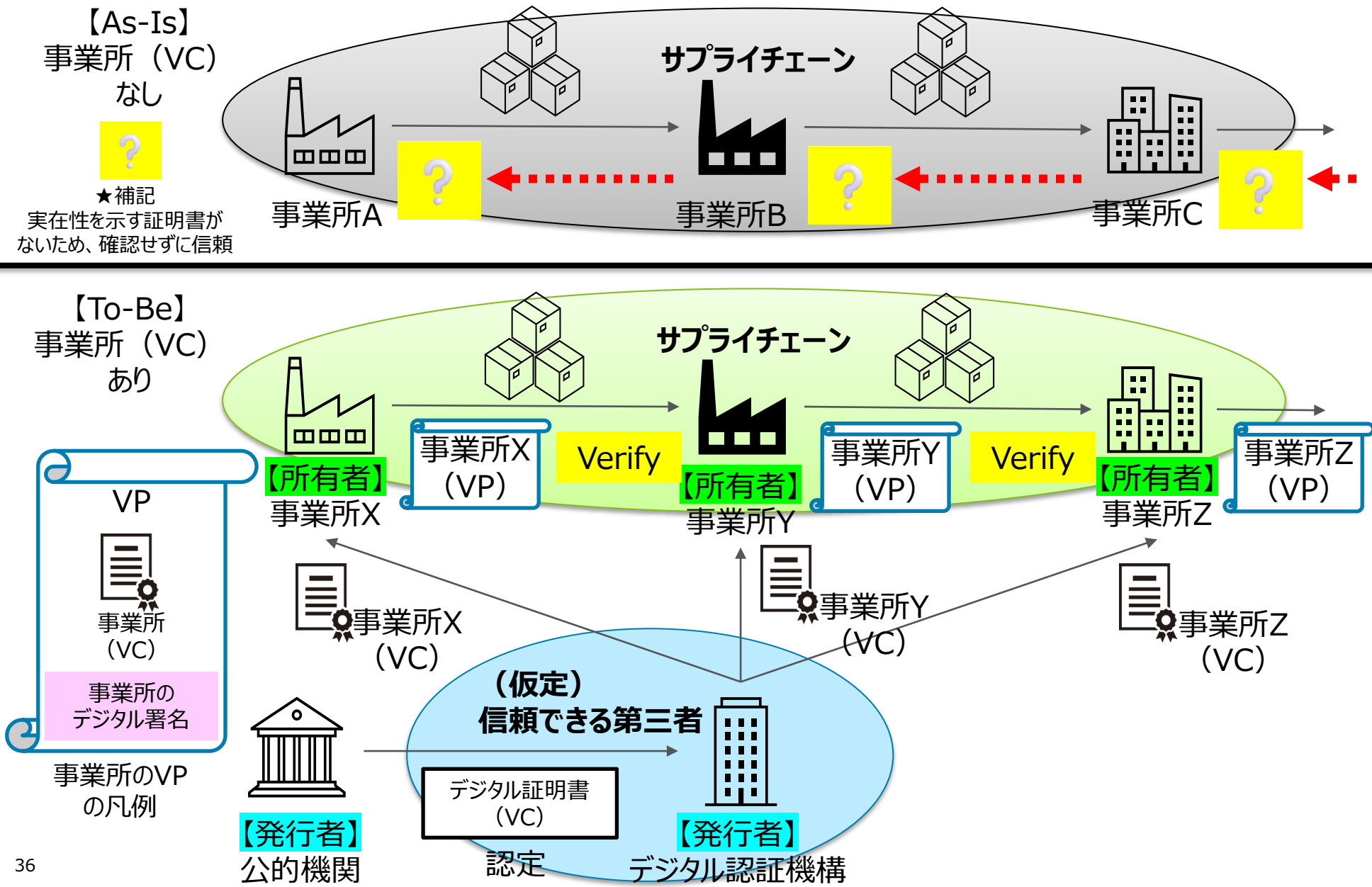
4.2. Verifyできる領域を拡大する仕組み
4.2.1. 登場主体・要求事項整理

主体	実証事業での役割	実証事業において設定した要求事項
公的機関	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	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	• 発行サービス
	  • 事業所（VC）を発行する
	  • 事業所（VC）を更新する
	  • 事業所（VC）を失効する
	• 失効管理サービス
	  • 事業所（VC）のステータスに対し有効/無効を返答する
		• 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
		• 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	• デジタル認証機構に対し、事業所（VC）を申請する • 事業所（VC）を更新依頼する • 事業所（VC）を含んだ事業所（VP）を生成する • 他社の事業所（VP）を検証する	• 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 • 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. Verifyできる領域を拡大する仕組み
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（1/2）

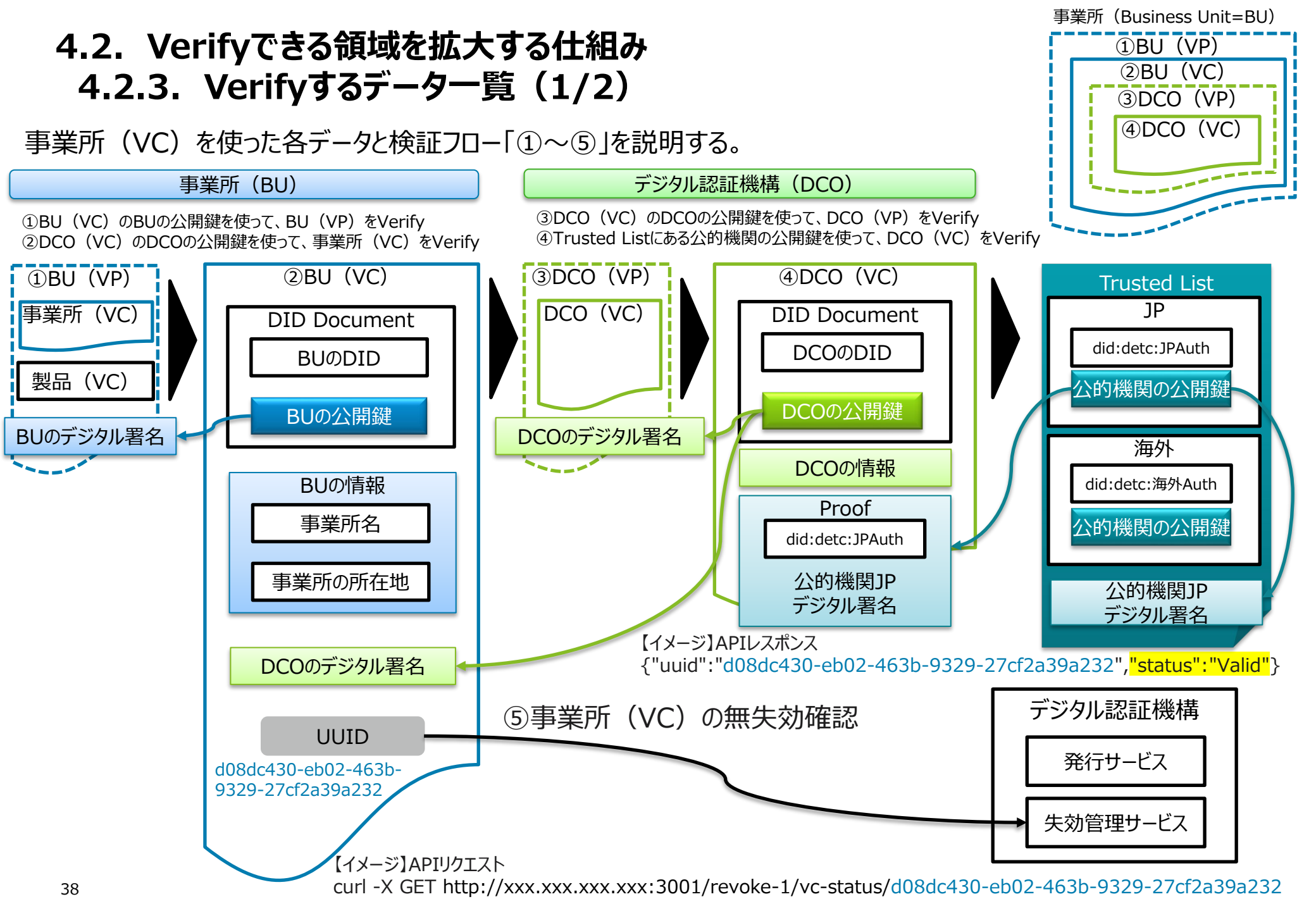


4.2. Verifyできる領域を拡大する仕組み
4.2.2. 企画・プロトタイプシステムの開発におけるペインの解決方法（2/2）

ペイン	ペインの解決方法(仮説)	活用する規格・技術	技術選定理由(仮説)
第三者による真正性の証明が無い 「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。」	事業所の実在性を確認	• 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	• 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。
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。」	検証可能な証明書を提供	• Verifiable Credentials Data Model v2.0 draft 6月（W3C）	• 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. Verifyできる領域を拡大する仕組み
4.2.3. Verifyするデータ一覧（1/2）

事業所（VC）を使った各データと検証フロー「①～⑤」を説明する。



4.2. Verifyできる領域を拡大する仕組み
4.2.3. Verifyするデーター一覧（2/2）

注釈
- 事業所（BU）
- デジタル認証機構（DCO）

課題	Verifyの対象	Verify方法	検証者(verifier)	データの保有者(ownership)	発行者(issuer)	データの置き場所(storage)	アクセスコントロール(access control)	成果・留意点
取引先の実在性	BU（VP）	BUの公開鍵で、BUのデジタル署名検証	事業所（Verifier）	事業所（Holder）	事業所（Holder）	検証者のPC	検証者がBU（VP）にアクセスしてVerify	BUが発行したことを証明
取引先の実在性	BU（VC）	DCOの公開鍵で、DCOのデジタル署名検証	事業所（Verifier）	事業所（Holder）	DCO	検証者のPC	検証者がBU（VP）に含まれるBU（VC）にアクセスしてVerify	DCOが発行したことを証明
取引先の実在性	DCO（VP）	DCOの公開鍵で、DCOのデジタル署名検証	事業所（Verifier）	事業所（Holder）	DCO	検証者のPC	検証者がBU（VP）に含まれるBU（VC）のさらに含まれるDCO（VP）にアクセスしてVerify	DCOが発行したことを証明
取引先の実在性	DCO（VC）	Trusted Listにある公的機関の公開鍵で、公的機関のデジタル署名検証	事業所（Verifier）	事業所（Holder）	公的機関	検証者のPC	検証者がBU（VP）に含まれるBU（VC）のさらに含まれるDCO（VP）に含まれるDCO（VC）にアクセスしてVerify	公的機関が発行したことを証明
取引先の実在性	BU（VC）	失効管理サービスにて無失効確認	事業所（Verifier）	事業所（Holder）	DCO	検証者のPC	検証者と失効管理サービスが直接通信を行う	BU（VC）が有効あるいは無効であることを証明

4.2. Verifyできる領域を拡大する仕組み
4.2.4. 証明書要件・識別子要件

証明書要件

証明書名	記載情報	要件	活用する規格	規格選定理由
デジタル証明書	• DID Document • デジタル認証機構名	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	Verifiable Credentials Data Model v2.0 draft 6月（W3C）	検証可能なVerifiable Credentials （VC）にするため
事業所ID	• DID Document • 事業所 • 事業者 • 認証レベル	• 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 • 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 • 失効管理はデジタル認証機構で行う	Verifiable Credentials Data Model v2.0 draft 6月（W3C）	検証可能なVerifiable Credentials （VC）にするため

識別子要件

識別子名	何を識別しているか	要件	活用する規格	規格選定理由
事業所	事業所(Holder)	• 事業所（Holder）自身がDIDを作成する • デジタル認証機構は識別子を発行しない	Decentralized Identifiers (DIDs) v1.0（W3C）	Verifiable Credentials （VC）を付与する識別子としてDIDが適しているため

4.3. 合意形成・トレースの仕組み

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：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置いている

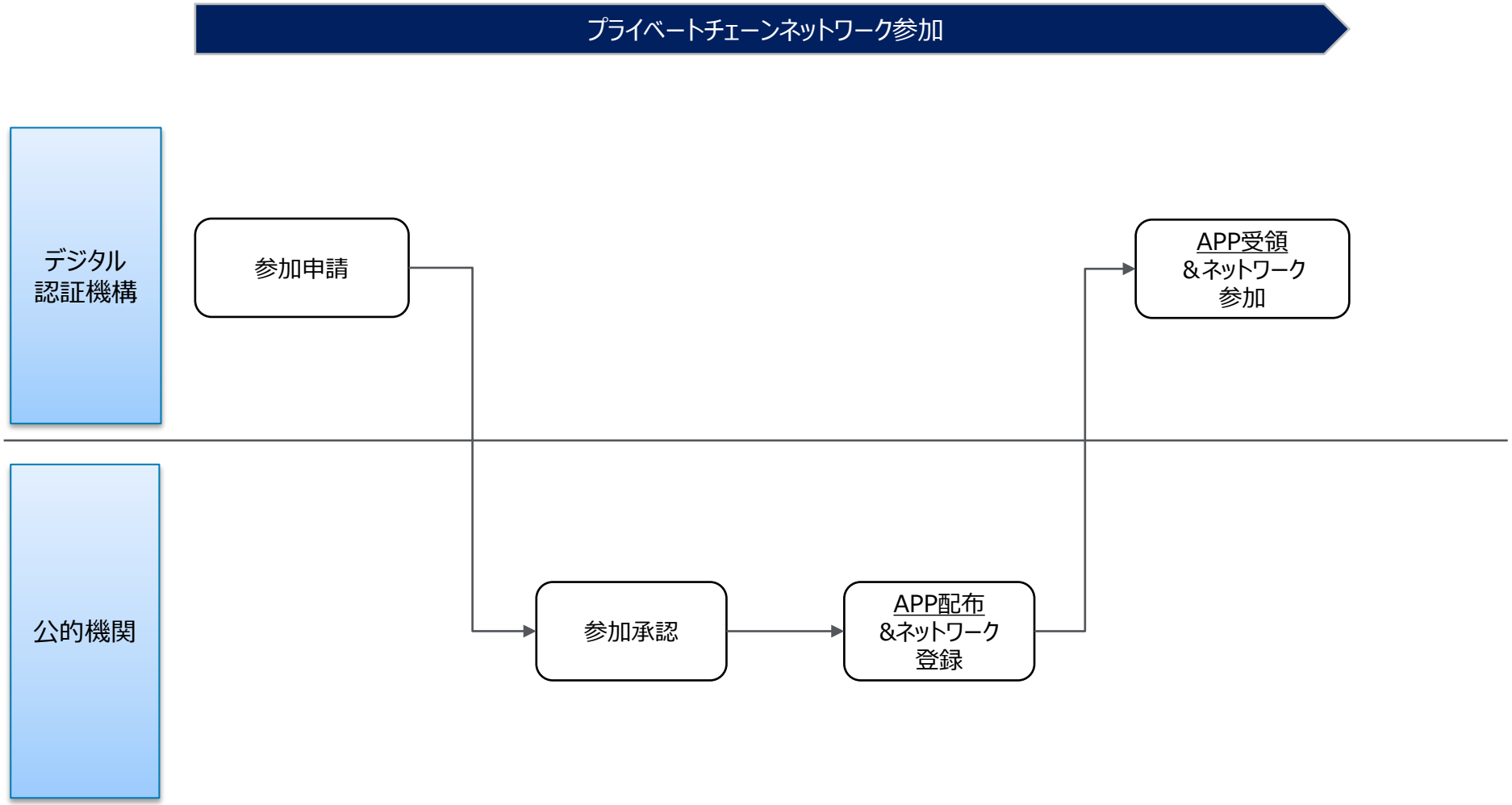
合意の主体	合意の対象	合意の条件	トレースの対象	トレースの手法	合意取消の可否・方法
公的機関(Issuer)とデジタル認証機構(Holder)	デジタル認証機構の認定	公的機関のデジタル署名	履行された左記の合意	デジタル認証機構が保有するデジタル証明書(VC)	契約書等のアナログ運用のもと、合意取消が可能
デジタル認証機構(Issuer)と事業所(Holder)	事業所(Holder)の実在性	公的機関とデジタル認証機構のデジタル署名	履行された左記の合意	事業所(VC)	契約書等のアナログ運用のもと、合意取消が可能
事業所(Holder)と事業所(Verifier)	事業所(Holder)の実在性	公的機関とデジタル認証機構のデジタル署名	履行された左記の合意	事業所(VC)	契約書等のアナログ運用のもと、合意取消が可能

第三者が確認する情報一覧

トレース情報	トレース手法	第三者が確認することのリスク・対応方針
デジタル認証機構が事業所を認証した記録	事業所が保有する事業所(VC)	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（1/4）

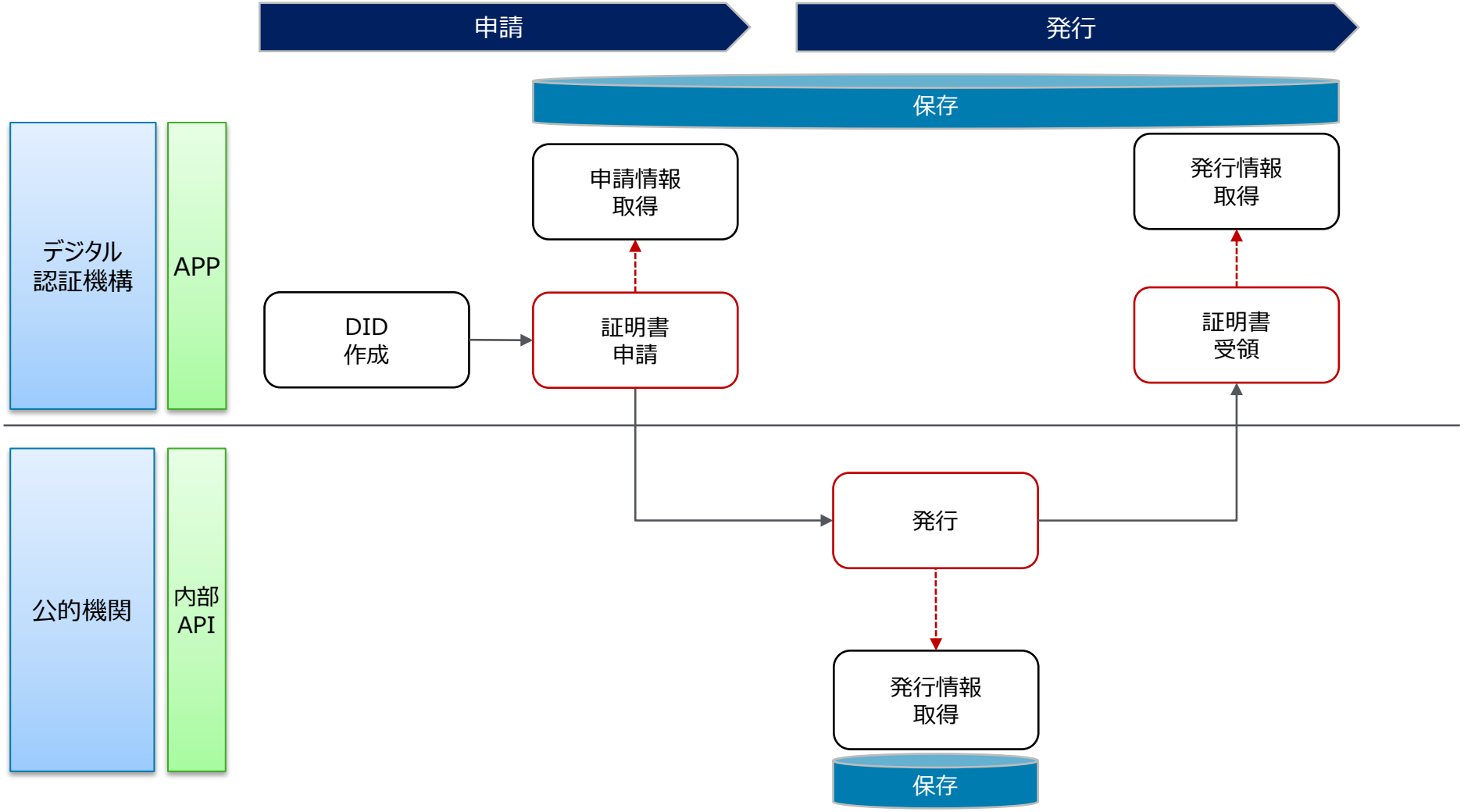
デジタル認証機構が公的機関に認定申請するためプライベートチェーンネットワークに参加する。



※下線部は今回の開発スコープ外

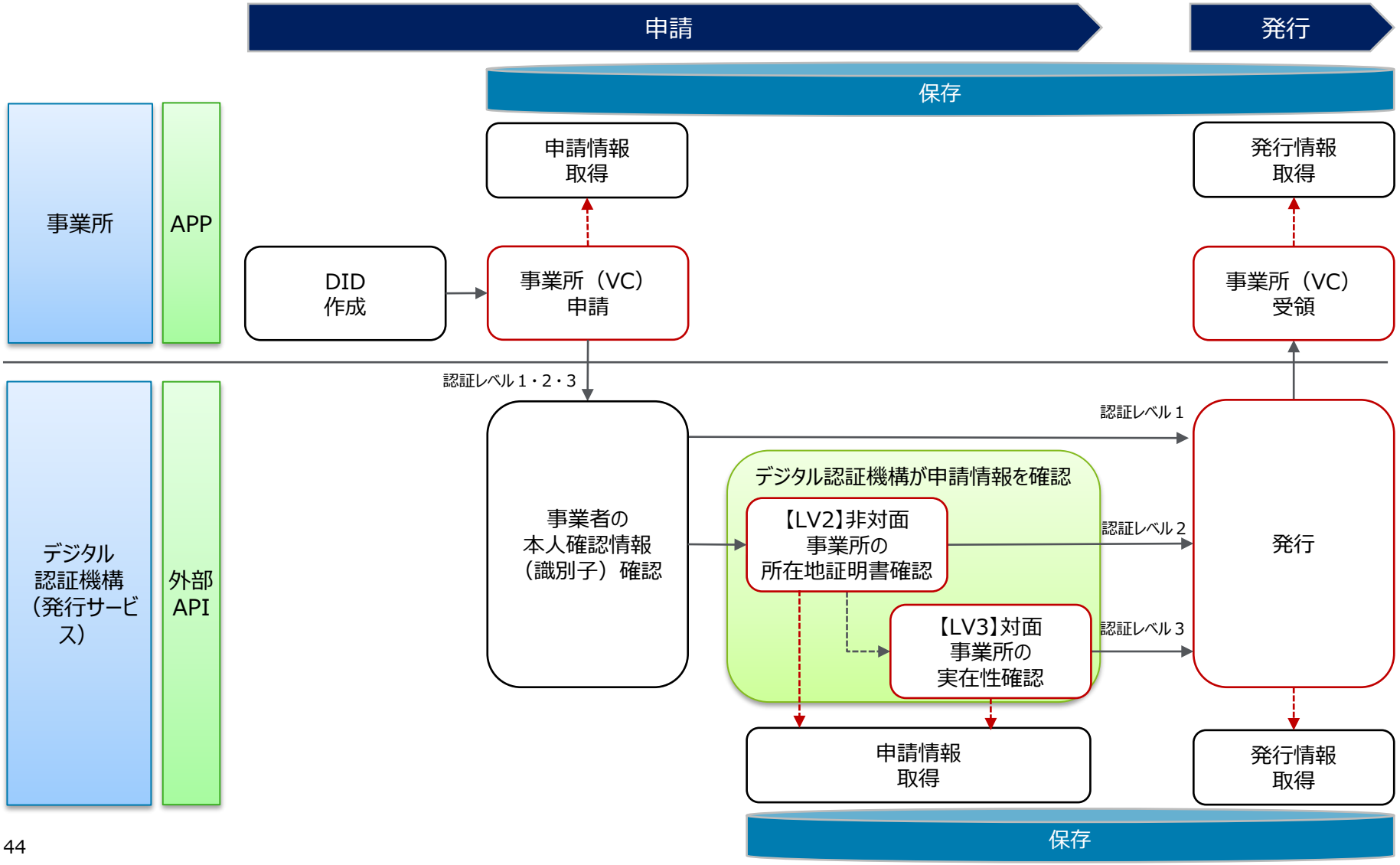
4.4. 企画・開発物
4.4.1. 業務フロー（2/4）

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。



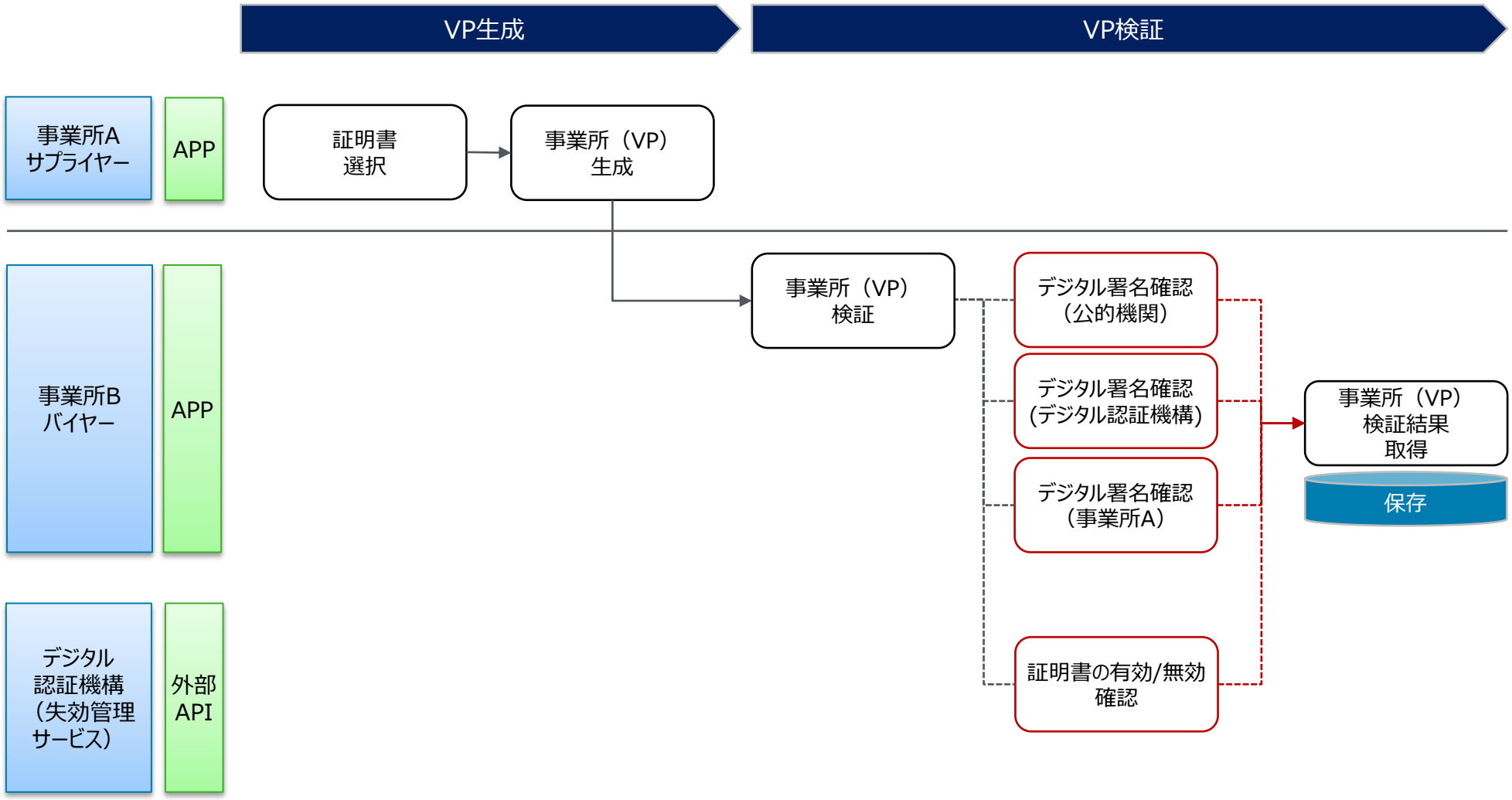
4.4. 企画・開発物
4.4.1. 業務フロー（3/4）

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。



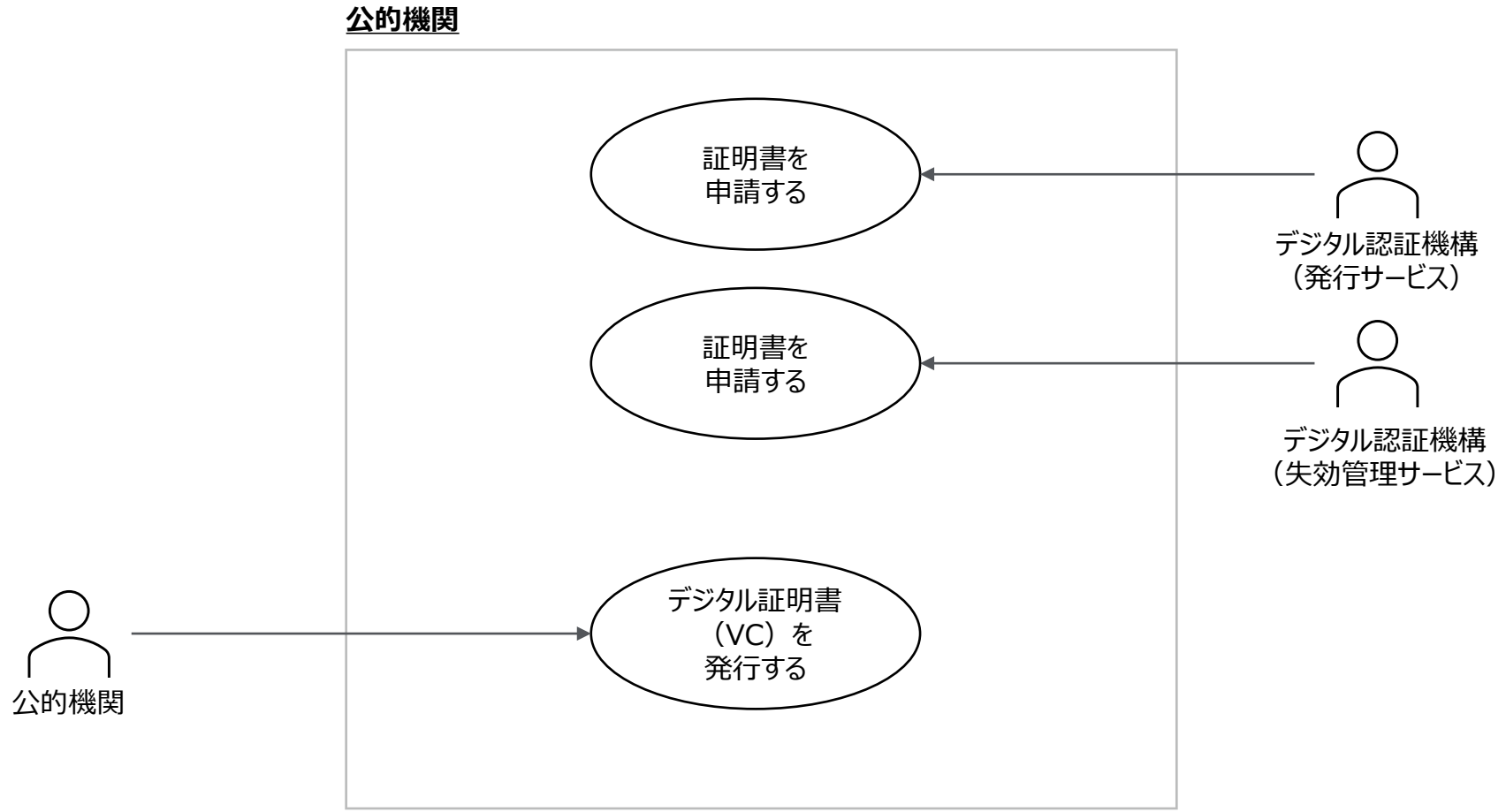
4.4. 企画・開発物
4.4.1. 業務フロー（4/4）

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。



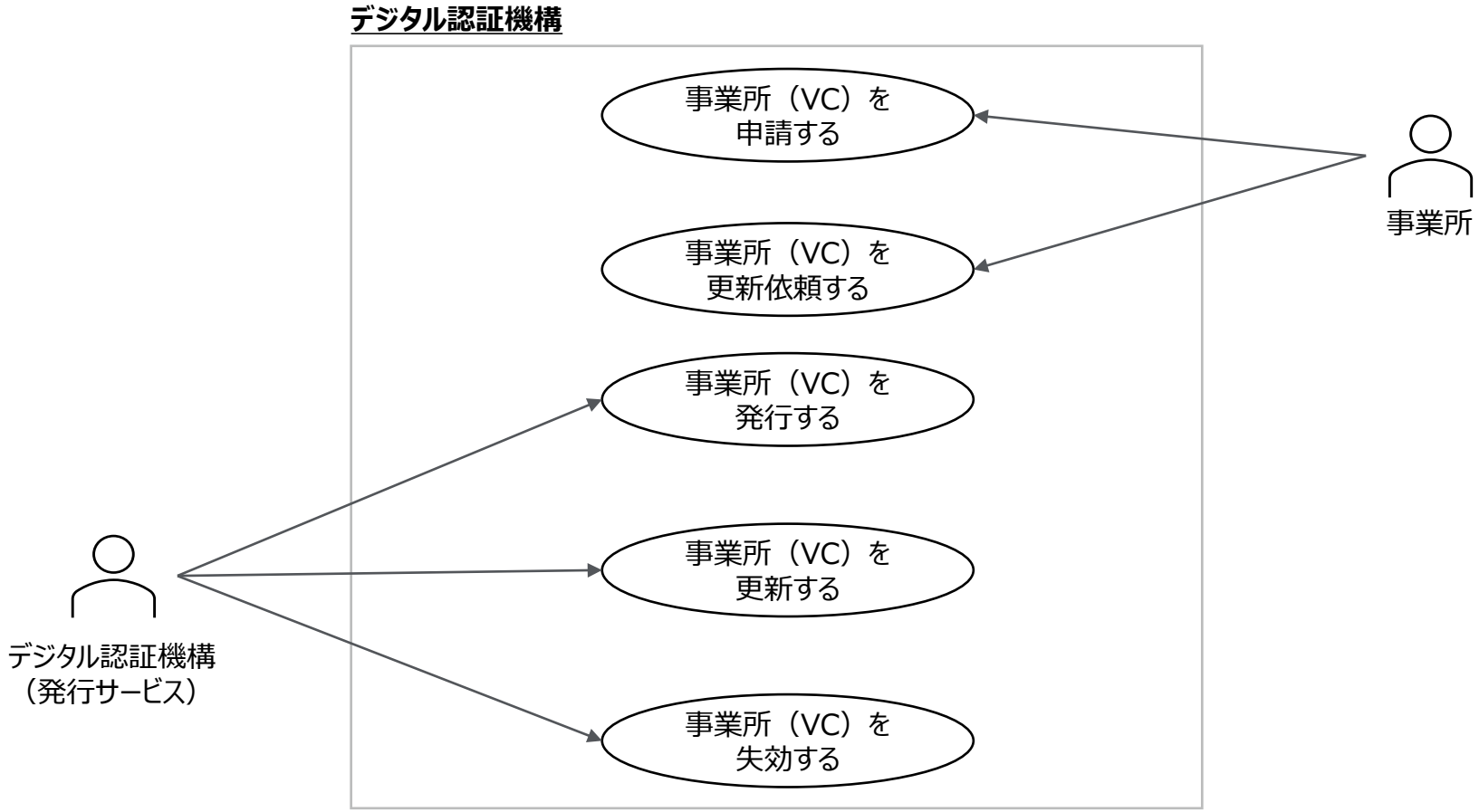
4.4. 企画・開発物
4.4.2. ユースケース図（1/3）

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。



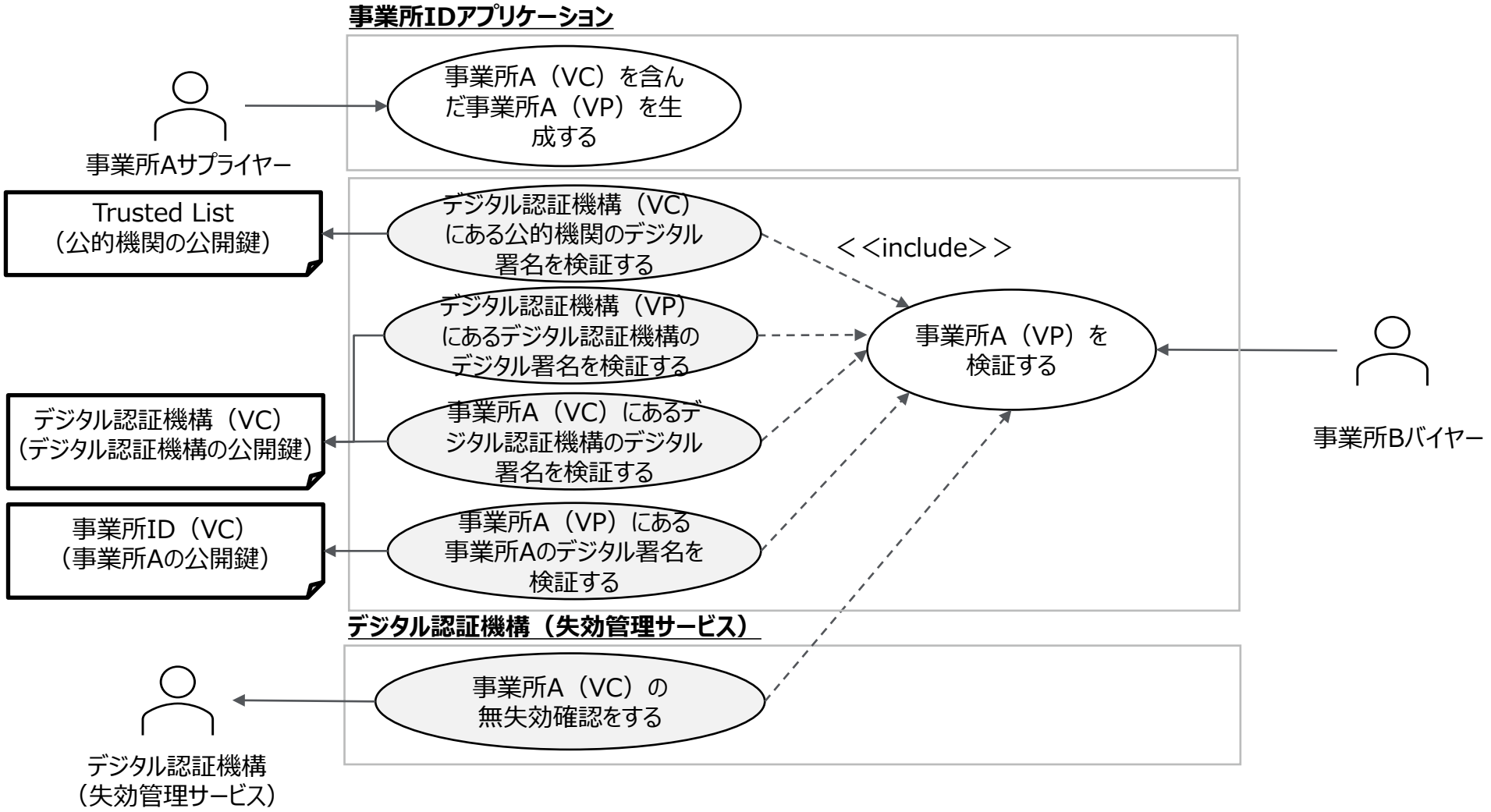
4.4. 企画・開発物
4.4.2. ユースケース図（2/3）

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。



4.4. 企画・開発物
4.4.2. ユースケース図（3/3）

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。



4.4. 企画・開発物
4.4.2. ユースケース図（ユースケースパターン）

事業所の真正性を確認する場面を想定し、事業所（VC）を使った検証のユースケースパターンを説明する。

■ ユースケースパターン

- パターン①
  - 事業所（VC）を保有している事業所と取引
    取引先と新規契約をする際、事業所（VC）の有用性を確認する。

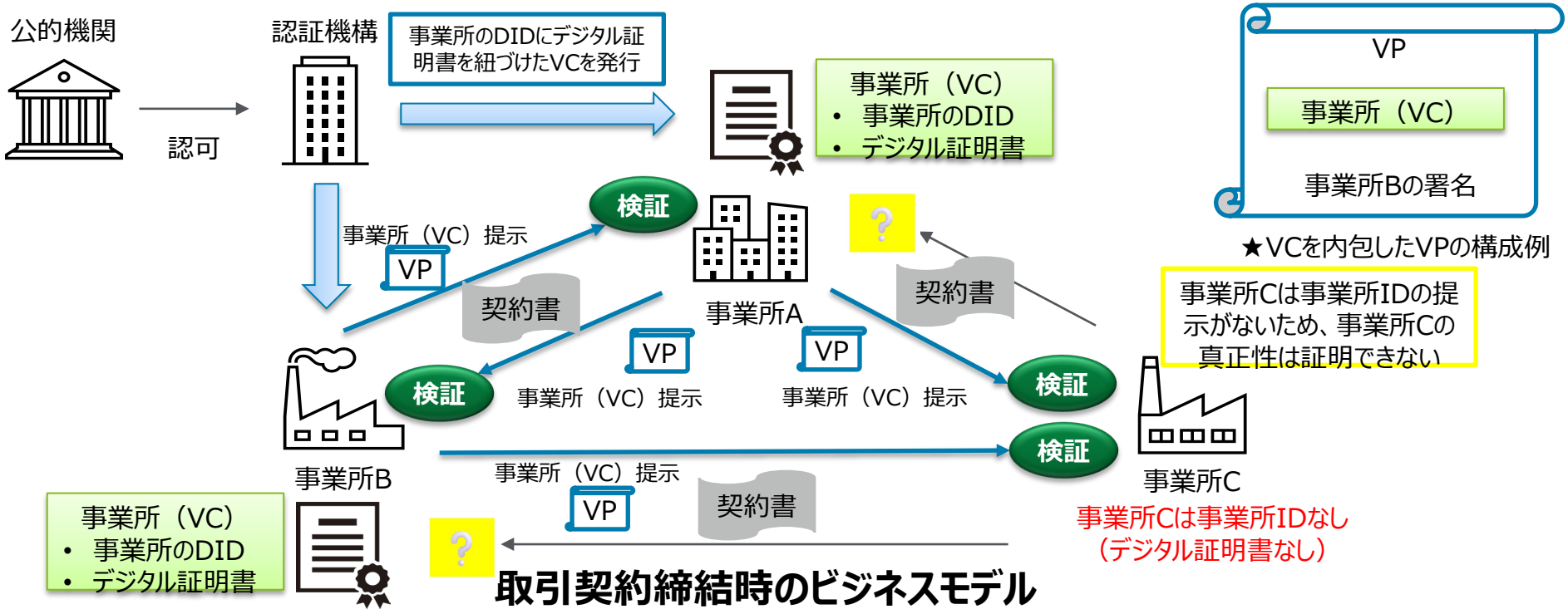
- パターン②
  - 既存の証明書と事業所（VC）の組み合わせ
    ICTメーカーが、複数の取引先からネットワーク機器に関する部品を購入する際、部品に対する証明書と事業所（VC）を組み合わせた証明書を使って真正性を確認する。

- パターン③
  - 海外にある事業所と取引
    海外の半導体事業所から半導体を購入する際、海外で発行した事業所（VC）を使って海外にある事業所の真正性を確認する。

4.4. 企画・開発物
4.4.2. ユースケース図（ユースケースパターン①）

分野	ユースケース	エンティティ	扱う属性情報
共通	取引契約	公的機関、認証機構、事業所	契約書、事業所（VC）

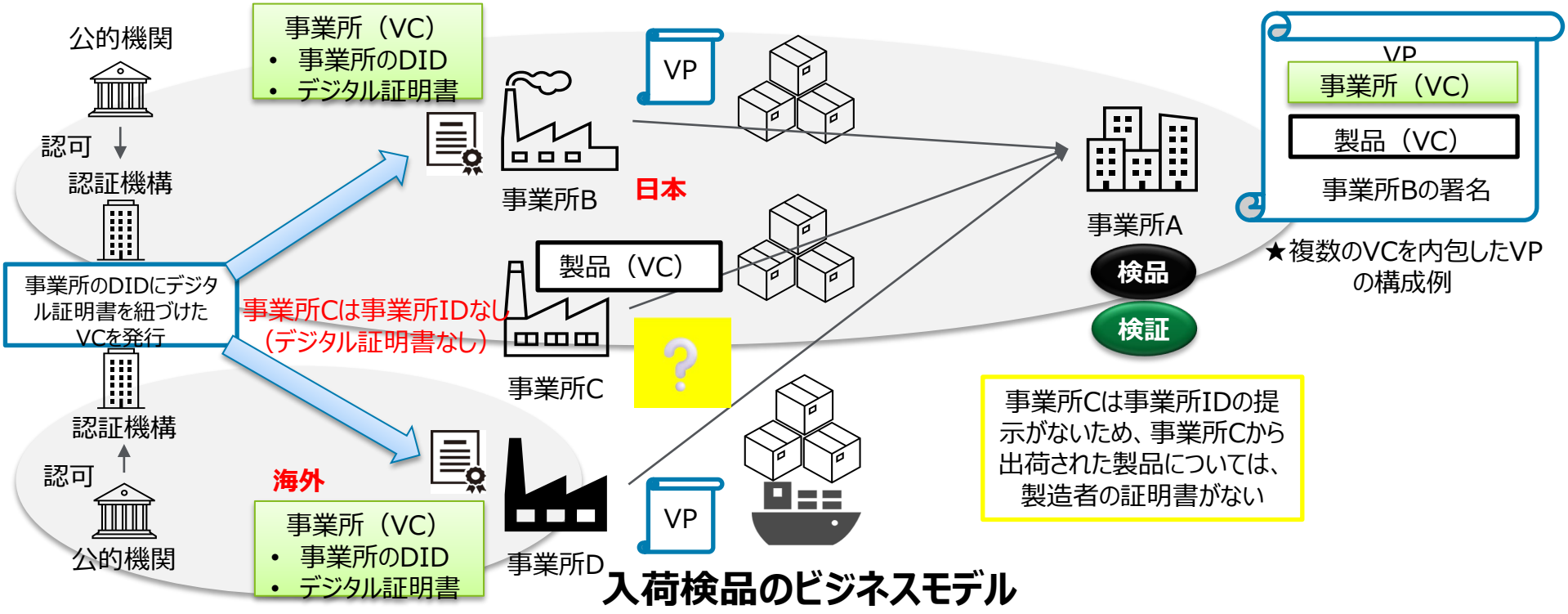
区分	説明
ペインポイント	事業所の真正性は自己署名による証明
提供する価値	公的機関に認可された認証機構である第三者が事業所の真正性を保証



4.4. 企画・開発物
4.4.2. ユースケース図（ユースケースパターン②③）

分野	ユースケース	エンティティ	扱う属性情報
ICT	製品の品質保証	公的機関、認証機構、製造者	製品、事業所（VC）

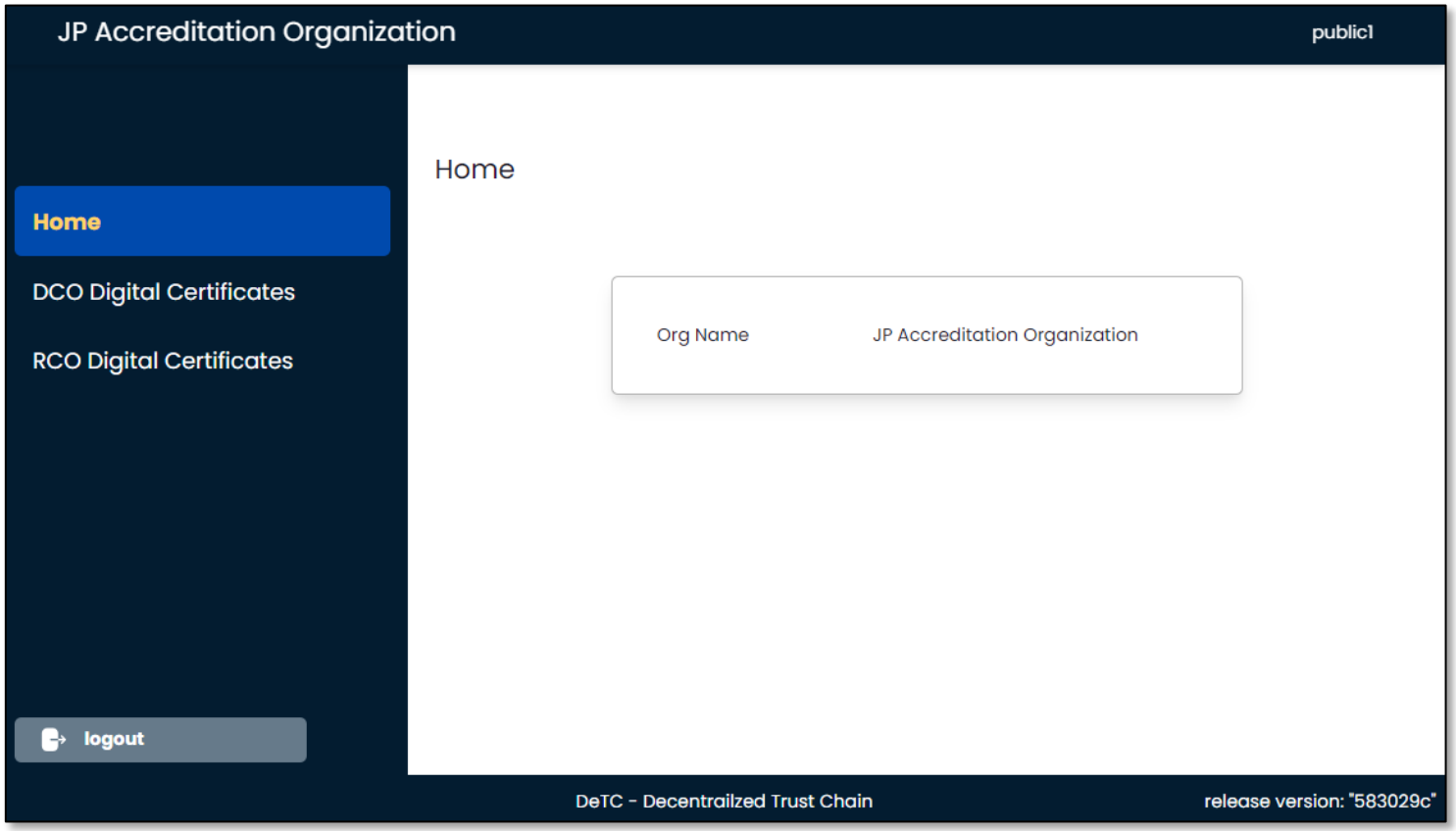
区分	説明
ペインポイント	製品の製造者を証明するものがない
提供する価値	公的機関に認可された認証機構である第三者が製造者の真正性を保証



4.4. 企画・開発物
4.4.3. 操作画面（UI）（1/4）

公的機関が発行したデジタル証明書の一覧を表示する。

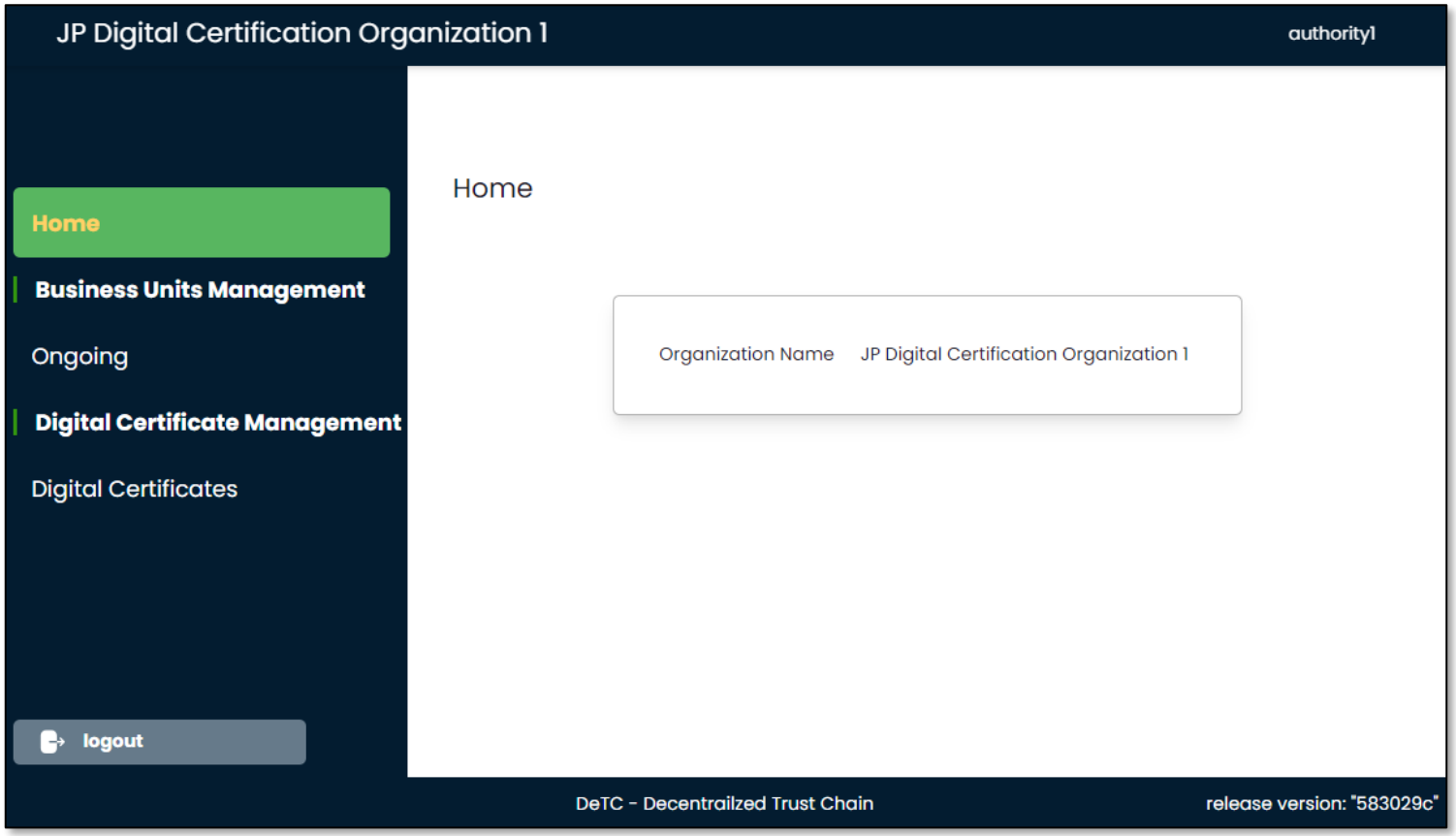
1. デジタル認証機構の証明書（DCO Digital Certifications）
   公的機関が発行したデジタル認証機構のデジタル証明書の一覧を表示
2. 失効管理サービスの証明書（RCO Digital Certifications）
   公的機関が発行した失効管理サービスのデジタル証明書の一覧を表示



4.4. 企画・開発物
4.4.3. 操作画面（UI）（2/4）

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。

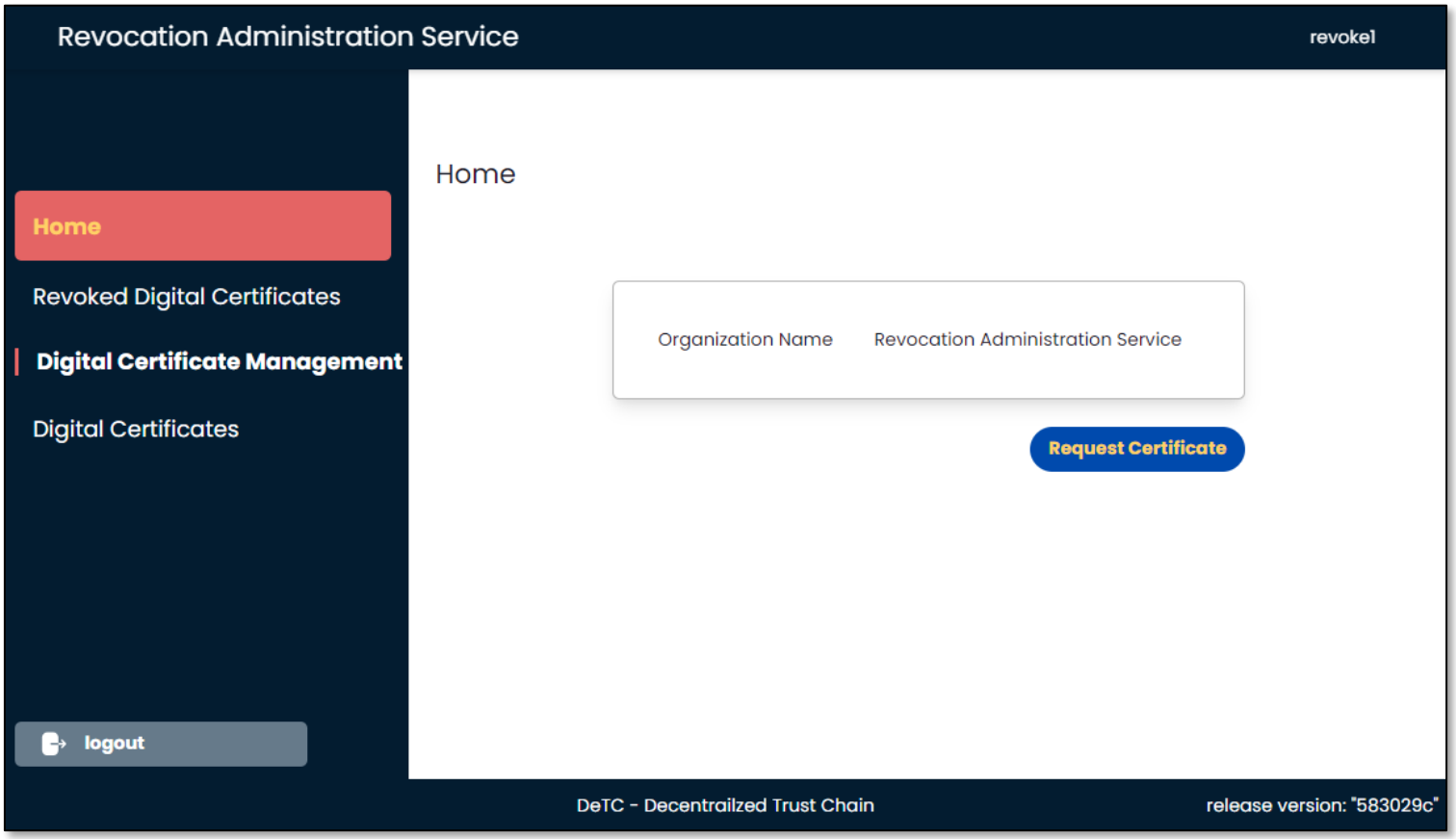
1. オンゴーイング（Ongoing）
   デジタル認証機構が事業所に発行した事業所（VC）の一覧を表示
2. デジタル証明書一覧（Digital Certificates）
   公的機関がデジタル認証機構に発行したデジタル証明書の一覧を表示



4.4. 企画・開発物
4.4.3. 操作画面（UI）（3/4）

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。

1. 証明書失効一覧（Revoked Digital Certificates）
   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
2. デジタル証明書一覧（Digital Certificates）
   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



4.4. 企画・開発物
4.4.3. 操作画面（UI）（4/4）

事業所（シミュレーター）

事業所が、デジタル認証機構に事業所（VC）の申請をする際、申請情報の一部は、申請内容に記載するが、
申請者の意思によって事業所（VC）に含めないことが可能。

例：
事業所の住所や担当者の連絡先を事業所（VC）に含めない場合、Noを選択

4.4. 企画・開発物
4.4.4. 機能一覧/非機能一覧（1/2）

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。

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

4.4. 企画・開発物
4.4.4. 機能一覧/非機能一覧（2/2）

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。

機能/非機能	機能名	機能概要
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する
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. 企画・開発物
4.4.4.1. (非機能要件)リスク分析とセキュリティ対応方針

サービス(アプリ)利用にかかるリスク	影響度 (機密性・完全性・可用性への影響)	発生可能性 (どのような悪意的な攻撃が考えられるか)	左記リスクへの対応方針・攻撃防止の根拠
信頼できる第三者のデジタル署名の改ざんによる事業所（VC）の不正発行	• 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	• 鍵管理システムを操作可能な権限が奪取された場合	• デジタル認証機構・公的機関は、秘密鍵を第三者に知られないように安全に保持する • Verify用のトラストアンカーとなる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. 企画・開発物
4.4.4.2. (非機能要件)大規模・商用・社会実装時のシステム・運用方針

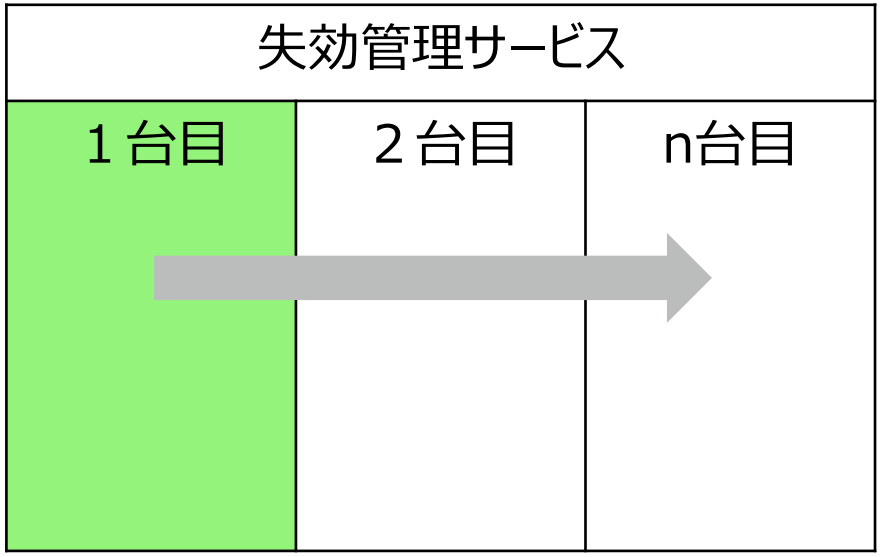
社会実装時に想定する利用規模

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ごとに、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。

システム・運用方針

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

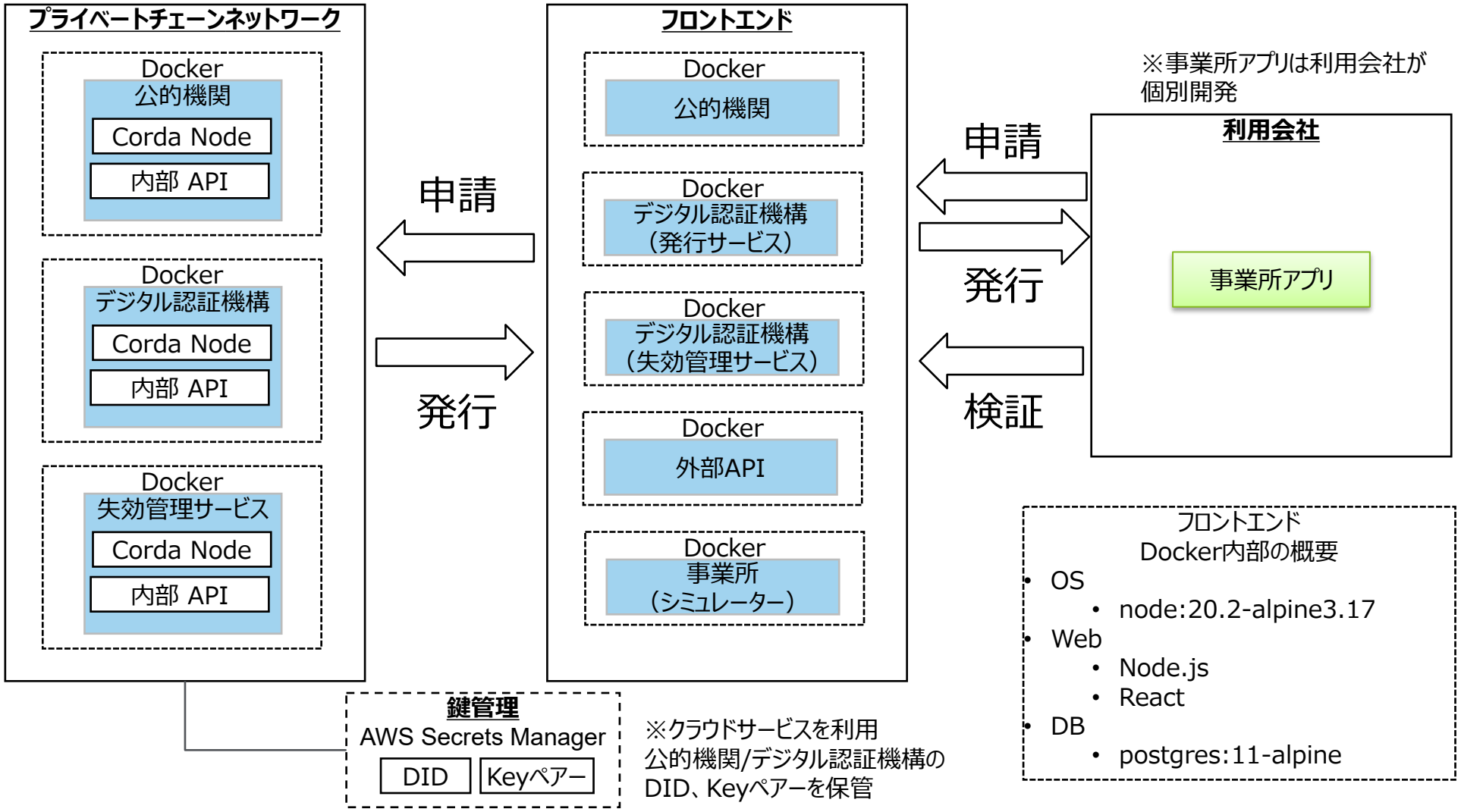
4.4. 企画・開発物
4.4.5. データモデル定義

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。

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. 企画・開発物
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。



4.4. 企画・開発物
4.4.7. 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 「失効管理サービス」	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
事業所	新規 ※シミュレータとして開発	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）

※プライベートチェーンネットワークに関する補足説明
- 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なうためCordaを使った分散台帳技術を使用
- 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
- Cordaライセンス
  - https://sbir3japan.co.jp/corda/corda-enterprise-license/

※鍵管理の補足説明
- 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。

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

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	すでにある、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. 実施概要
5.1.2. 実施内容・手法：ビジネスフィージビリティ検証

No.	実施内容	実施手法
1	事業所IDとそのデジタル認証の申請・更新フローの確認	システム利用者へのヒアリング
2	サプライチェーンネットワークとの接続・連携の容易性の確認	
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の確認	

5.1. 実施概要
5.1.2. 実施内容・手法：ガバナンス・ルール整理（1/4）

■ 事業所IDとそのデジタル認証の国際標準化

1.「インターネット協会ＯＩＣ運営委員会」
- ビジネスのフィージビリティ確認・新規規格原案策定を完了した。

2.「国際標準化委員会」
- ビジネスのフィージビリティ確認・新規規格原案策定検討、承認を得た。

3. 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。

成果物は
「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」を参照

■ 認証機構認定ルールに関連する事例調査
- 身元保証レベルに関する調査（eシール、NIST SP800-63-4、eIDAS）
- 認定方法に関する調査

5.1. 実施概要

5.1.2. 実施内容・手法：ガバナンス・ルール整理（2/4）

■ デジタル認証機構の認定ルール

➢ 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。

本実証	
LV1	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
LV2	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）
LV3	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）

➢ 【参考】国内における法人のデジタル認証のレベル分けの例（eシール）

Eシール	
レベル1	裸のeシール（eシールの定義に合致はするが、レベル2の要件を満たす保証がないもの）
レベル2	一定の技術基準を満たすeシール（技術的には発行元証明として十分機能することが確認できるもの）
レベル3	レベル2に加えて、十分な水準を満たしたトラストアンカーによって信頼性が担保されたeシール（発行元証明として機能することに関し、第三者によるお墨付き（将来的には国による認定制度等の要否を検討）があるものを想定）

参考：総務省 サイバーセキュリティ統括官室「eシールに係る検討状況」令和５年９月６日eシールに係る検討会（第1回）
https://www.soumu.go.jp/main_content/000899795.pdf

5.1. 実施概要
5.1.2. 実施内容・手法：ガバナンス・ルール整理（3/4）

■ デジタル認証機構の認定ルール

➢ 事業者・事業所が参加しやすいオンボーディング

海外における個人のデジタル認証のレベル分けの例（NIST SP800-63-4、eIDAS）

NIST SP 800-63-34		eIDAS	
Identity Assurance Level（IAL）		**Identity proofing and verification (natural person)**	
IAL0	身元確認不要、自己申告の登録でよい。メールアドレスの到達確認など	Low	•個人の身元に対して限定された程度の信頼度を提供。Identityの誤用又は改ざんリスクを減らすことを目的 •eIDAS仕様外の簡易なトラストサービス •トラストサービスプロバイダによって提供。事後監査が必要
IAL1,2	識別に用いられる属性をリモートまたは対面で確認する必要あり	Substantial	•個人の身元に対してSubstantialレベルの信頼度を提供。Identityの誤用又は改ざんのリスクを大幅に減らすことを目的 •仕様に幅がある
IAL3	識別属性を対面で確認する必要があり。検証担当者は有資格者	High	•個人の身元に対してSubstantialのアシュアランスレベルを備えた電子識別手段よりも高い信頼度を提供。Identityの誤用又は改ざん防止を目的 •厳密に守るべき要件やポリシーが定められている •適格トラストサービスプロバイダによって提供。定期的な監査が必要

参考：
デジタル庁「事務局説明資料（資料1）」令和４年１月25日 トラストを確保したDX推進SWG（第４回）
https://www.digital.go.jp/councils/trust-dx-sub-wg/GLvad6b1
NIST「SP 800-63-4」2023年12月08日
https://pages.nist.gov/800-63-4/sp800-63a.html#identity-assurance-levels

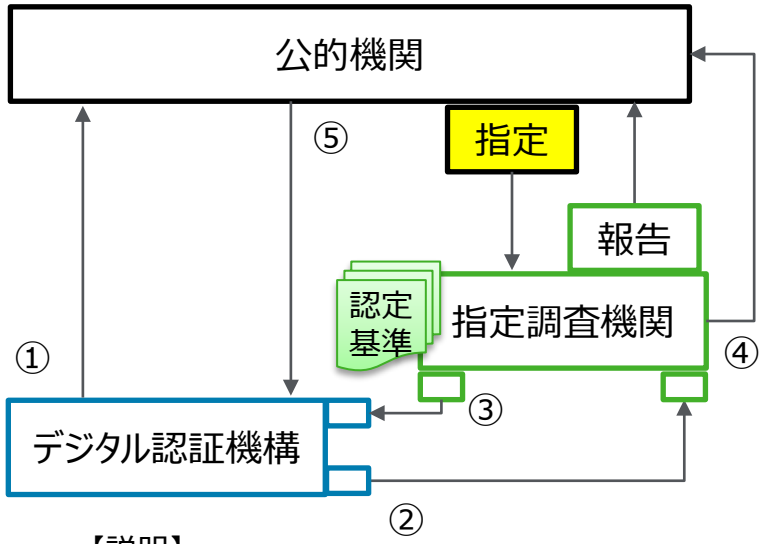
5.1. 実施概要
5.1.2. 実施内容・手法：ガバナンス・ルール整理（4/4）

■ デジタル認証機構の認定ルール

2種類の認定方法について、調査した。

- **法令等に基づく<u>指定調査機関</u>**による適合性調査（イメージ図①）
  - 電子署名法
- **国際標準に基づき認定された<u>適合性評価機関</u>**による適合性評価（イメージ図②）
  - 国際標準
    - ISO/IEC 17065（製品、プロセス及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）

イメージ図①

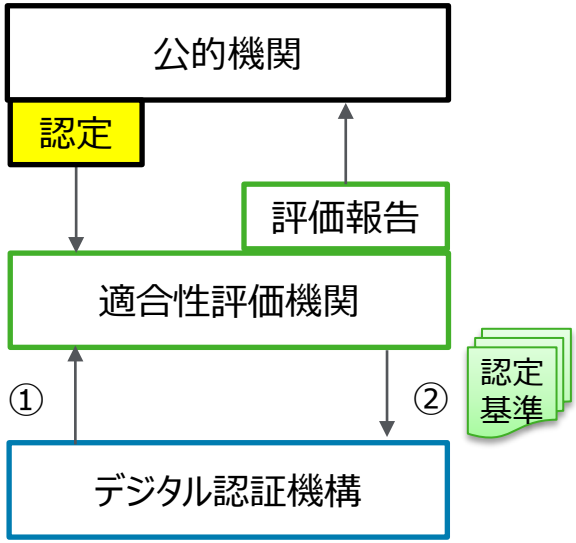


【説明】
①認定申請
②調査申請
③調査
④結果通知
⑤認定

国際間の利用者が
相互に適格性を確認できるように、
以下の項目の同等性などを検討し、
相違点を補完することが必要あり。

①法制度
②監督・適合性評価
③技術標準
④トラストアンカー間の接続の仕組み

イメージ図②



【説明】
①申請
②評価/認定

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」を整理していく。

参考：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

5.1. 実施概要
5.1.2. 実施内容・手法：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た準備

1. プロトタイプ実証への参加呼びかけ・調整
   「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」と連携して本実証を進める。

2. コミュニティ参加ルール（全体スケジュール・依頼事項・会議予定等）の整備
   週1で定例会を実施し、事業所IDを使った検証の準備を進めている。
   - 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
   - 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

■ 国際標準化に向けた情報共有

1. 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・調整
   - 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及び規格提案のDRAFT策定

5.2. 検証結果
5.2.1. 検証結果（1/3）

ビジネスフィージビリティ検証

No.	実施事項	検証結果	有用性検証
1	事業所IDとそのデジタル認証の申請・更新フローの確認	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た。	• 事業所の実在性について信頼性が向上する。
2	サプライチェーンネットワークとの接続・連携の容易性の確認	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た。	• API連携で利用できるのが望ましい。 • 既存システムにadd-on（あるいはPlug in）で利用できるのが望ましい。
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の確認	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。	• 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。

5.2. 検証結果
5.2.1. 検証結果（2/3）

- 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。
- 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。

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）

国際標準化活動の成果と今後の予定

国際標準化原案及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＞から前向きな活発なコメントが寄せられ、次のステップである、NP提案の道筋が出来た。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及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。又、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為、今後継続的に実証プロトタイプシステムに展開検討予定。

5.2. 検証結果
5.2.1. 検証結果（3/3）

No.	委員会等および実施時期	実施内容
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） ーIPADADC ー日本規格協会 （適宜）	• 国際標準化テーマ調査票申請内容の確認 IPA DADC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）で取り上げて頂き承諾を得た。
4	その他（実証プロトタイプ） ー沖縄オープンラボラトリ（OOL） Trusted Network PJ Phase2 （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

6.1. 実施概要（1/22）
No.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

ヒアリング／調査先	ヒアリング／調査手法	ヒアリング対象者/調査ドキュメントURL
内部検討のみ	–	–

従来型の仕組みを△という評価をした場合における、パブリックチェーン/パーミッションドチェーンという2つの分散型システムのアーキテクチャ比較評価

比較軸	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）	従来型（Webサービスを想定）
機能開発	要件次第であり同等である想定		
サービス維持	◯事実上リスク無し	△ サービサーに依存	△サービサーに依存
データロストリスク	◯事実上リスク無し	△～◯ アーキテクチャに依存	△サービサーに依存
参加者負担	×鍵管理が必要	△～× アーキテクチャに依存	△サービサーに依存
プライバシー管理	×情報漏洩時のリスクコントロール不可	◯Need to Know原則に従っており、リスクコントロールが容易	△サービサーに依存
参照パフォーマンス	×本件と関係ない情報も検索対象になる為パフォーマンス劣後	◯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	△サービサーに依存
登録パフォーマンス	×要求に対応できない可能性。2ndレイヤ活用により改善の可能性あり。	△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従来型に対しては劣る）	△サービサーに依存

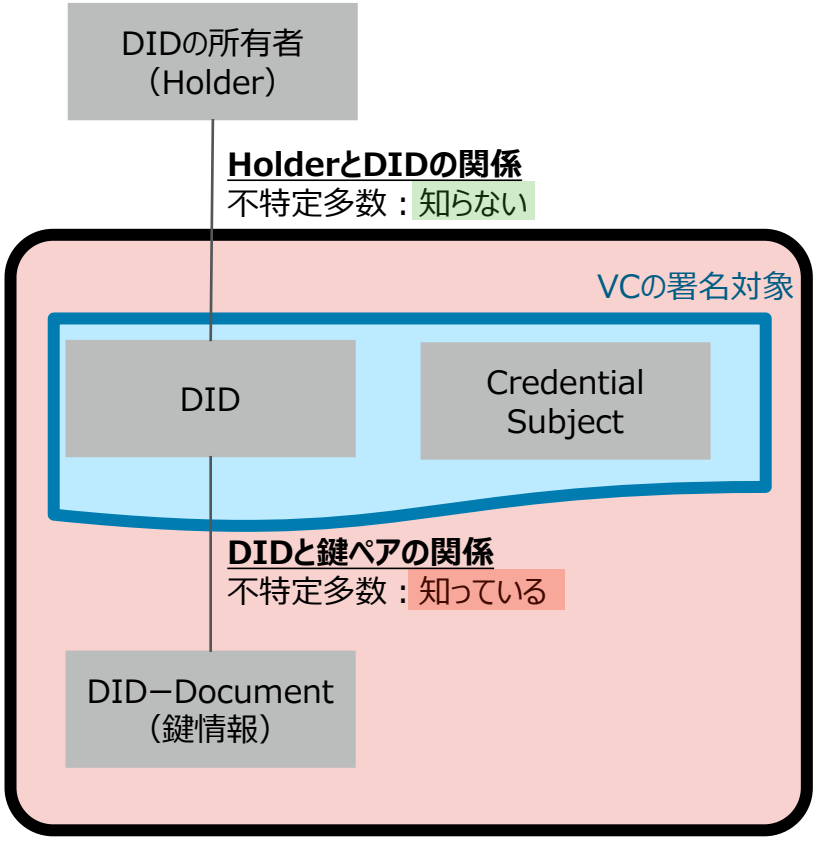
パブリックチェーンの場合、エコシステムへの依存度が高く、パブリックチェーンの持つ制約がビジネス化に当たってのブロッカーとなるリスクがある為、
今回はパーミッションドチェーンを必要な部分へ活用することを前提としたアーキテクチャを採用

6.1. 実施概要（2/22）
No.0 Central Data Registry不要なアーキテクチャの必要性

ヒアリング／調査先	ヒアリング／調査手法	ヒアリング対象者/調査ドキュメントURL
内部検討のみ	–	–

既存のDID/VCアーキテクチャ（弊社理解）

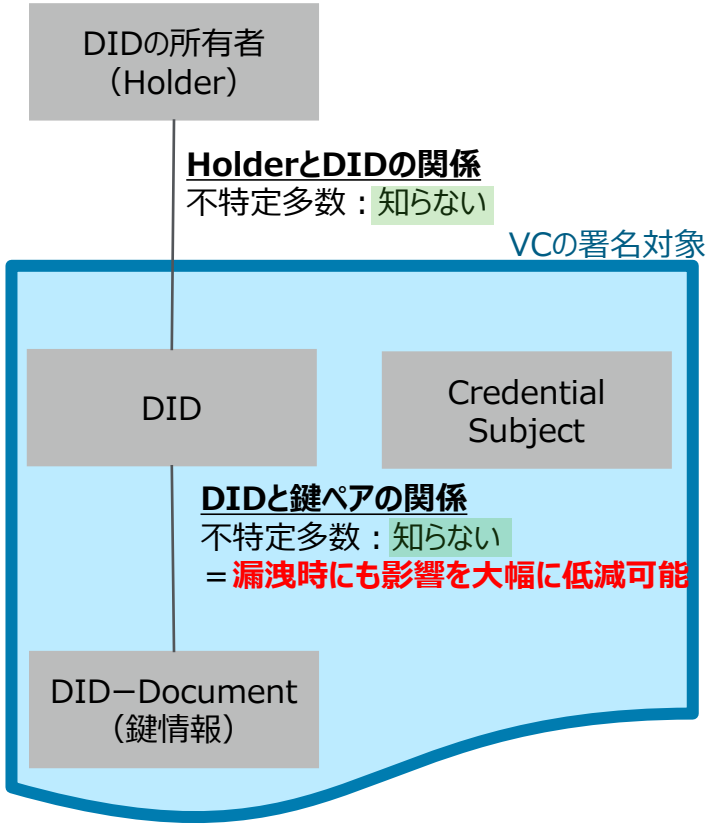
不特定多数が知ることができる情報が多いため漏洩時の影響大



Central Data Registry（公開情報）

本案件のアーキテクチャ

不特定多数が知ることができる情報が無いため漏洩時の影響小



Central Data Registryが提供していた対改竄性をVCの電子署名により実現（X.509／Federated IDの考え方に近い）

6.1. 実施概要（3/22）
6.1.1. 調査で明らかにする論点とその結果

No.	論点	検討結果とその経緯
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	• 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。 • 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、本取組で採用する可能性は低いと結論づけた。 • 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。 • 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。 • また、論点3, 4, 7, 9との整合性をも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**	• 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。 • 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。 • 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。 • 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。） • 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。

6.1. 実施概要（4/22）
No.1 Credential 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

ヒアリング／調査先	ヒアリング／調査手法	ヒアリング対象者/調査ドキュメントURL
W3C Credential Community Group	メーリングリスト上でのDiscussion	BBS: https://www.w3.org/TR/vc-di-bbs/
IETF	資料精査	https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/ https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/
Transmute Industries	W3Cへのプレゼンテーション	https://docs.google.com/presentation/d/1ZueDxEfoPLuyXSRh5Ud5C1NtNbThJigXiBmgQJE-PLQ/edit#slide=id.g2572cdf73b0_0_5
EBSI	資料精査	https://api-pilot.ebsi.eu/docs/specs/guidelines/selective-disclosure-sd-jwt
Hyperledger Aries BBS+ Signature	ライブラリ動作検証	https://github.com/hyperledger/aries-bbssignatures-rs

個人向けにおける選択的開示要求の例

```
"credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "alumniOf": {
        "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
        "name": "Example University",
        "degree": {
            "type": "ExampleBachelorDegree",
            "name": "Bachelor of Science and Arts",
            "acquisiton_date": "2024/3/31"
        }
    }
}
```

隠したい情報

隠したい情報

・属性情報の「ほとんど」を隠蔽したい。
・開示する部分も、相手によってそれぞれ異なる。

法人向けユースケース（本件）における選択的開示要求の例

```
"credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "location": "Izumi Garden Tower, 6-1 Roppongi, Minato-ku",
    "country": "Japan"
}
```

隠したい情報

・事業所の場合、属性情報の「一部」を隠蔽したい。
・非開示にしたい項目は相手先によって変わる事はほとんどない。

VC自体を複数構築することによる選択的開示要求の実現例（Maskingによる実現）

```
"credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "location": "not available",
    "country": "Japan"
}
```

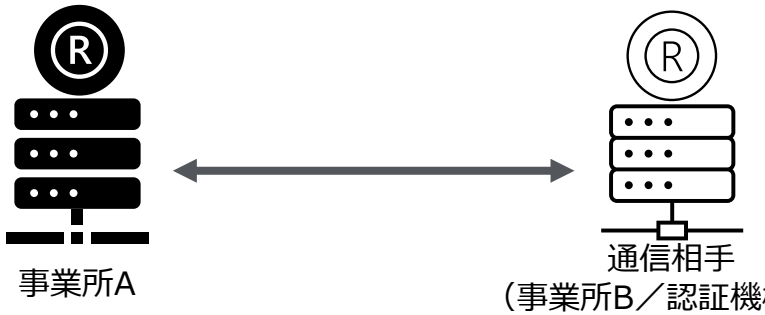
※いずれの例も、理解の為、簡素化しており、実装とは異なる。

6.1. 実施概要（5/22）
No.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

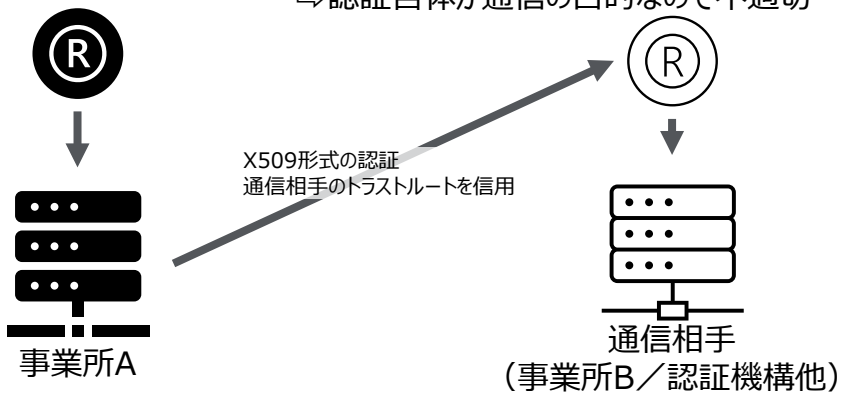
ヒアリング／調査先	ヒアリング／調査手法	ヒアリング対象者/調査ドキュメントURL
アラクサラ社	個別ヒアリング	–
DIF	資料精査	https://identity.foundation/didcomm-messaging/spec/#message-encryption

既存の通信秘匿プロトコル（mTLS/TLS：レイヤー５）のトラストモデル

mTLSの場合:自己署名なので、**相互認証なし**

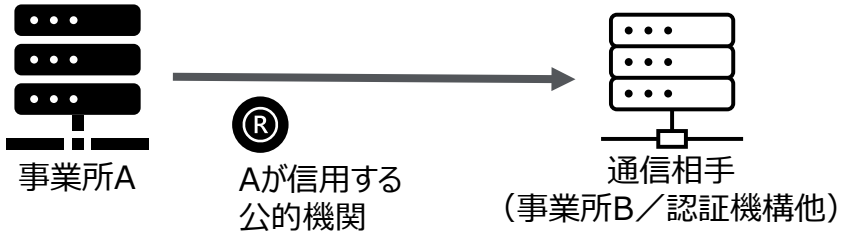


クライアントーサーバTLSの場合:Trust Rootを通じた認証が必要
⇨認証自体が通信の目的なので不適切

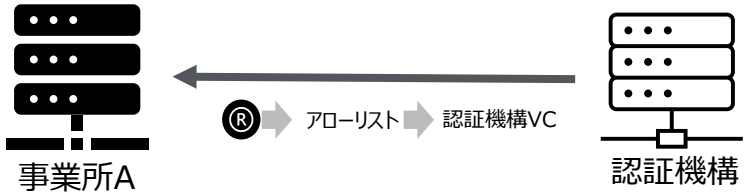


DID/VCベースでの通信暗号化プロトコルイメージ

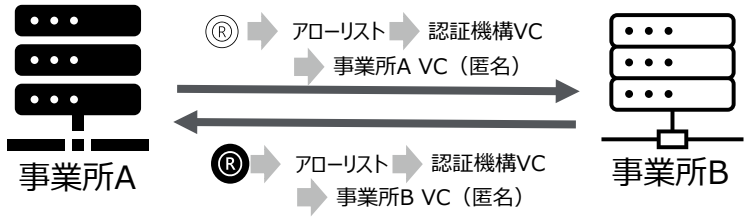
Step1:事業所Aが信用している公的機関の提示（暗号化不要）



Step2A:認証機構VCの提示および通信用の鍵提示⇨暗号通信開始



Step2B:匿名通信鍵（属する認証機構による認証済み）相互提示



6.1. 実施概要（6/22）
6.1.1. 調査で明らかにする論点とその結果

No.	論点	検討結果とその経緯
3	データ順序を確保した上での**拡張性の確保**	• 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。 • 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ごと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。 • 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。 • 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データの拡張性及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	• 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。 • 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。 • 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。 • 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。

6.1. 実施概要（7/22）
No.3 データの順序を確保した上での拡張性の確保

ヒアリング／調査先	ヒアリング／調査手法	ヒアリング対象者/調査ドキュメントURL
W3C Credential Community Group	メーリングリスト上での Discussion	エンジニア
W3C Verifiable Credential V2.0 (draft)	資料精査	https://github.com/w3c/vc-data-model/ https://www.w3.org/TR/vc-data-model-2.0/
W3C JSON-LD 1.1 Processing Algorithms and API	資料精査	https://www.w3.org/TR/JSON-ld11-api/

順序変化の影響

credentialSubject": {
"authenticationLevel": "1",
"uuid": "550e8400-e29b-41d4-a716-446655440000"
}
⇨ハッシュ値：83142843737b3e9964f794b4b4e797b0

credentialSubject": {
"uuid": "550e8400-e29b-41d4-a716-446655440000”,
"authenticationLevel": "1"
}
⇨ハッシュ値：a3f8df4b9bb73141cdb67bdde397dcbb

@container/@list指定(VC 2.0より)

EXAMPLE 82: Specifying that a collection is ordered in the context

Compacted (Input) | Expanded (Result) | Statements | Turtle | Open in playground

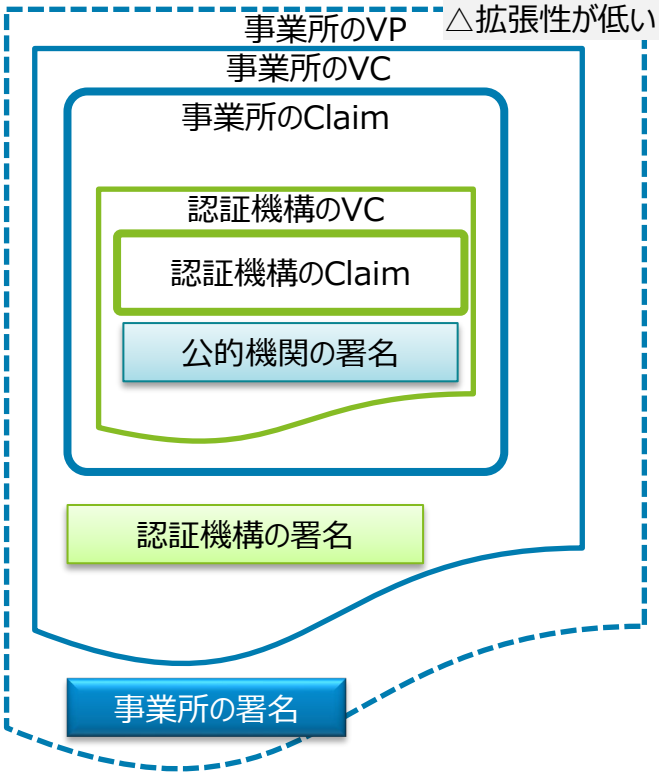
```
{
  "@context": {
    ...
    "nick": {
      "@id": "http://xmlns.com/foaf/0.1/nick",
      "@container": "@list"
    }
  },
  ...
  "@id": "http://example.org/people#joebob",
  "nick": [ "joe", "bob", "jaybee" ],
  ...
}
```

6.1. 実施概要（8/22）
No.4 Credential Subjectの子要素としてVPを含めることの技術的意義

ヒアリング／調査先	ヒアリング／調査手法	ヒアリング対象者/調査ドキュメントURL
W3C Credential Community Group	メーリングリスト上での Discussion	エンジニア
W3C Verifiable Credential V2.0 (draft)	資料精査	https://github.com/w3c/vc-data-model/ https://www.w3.org/TR/vc-data-model-2.0/

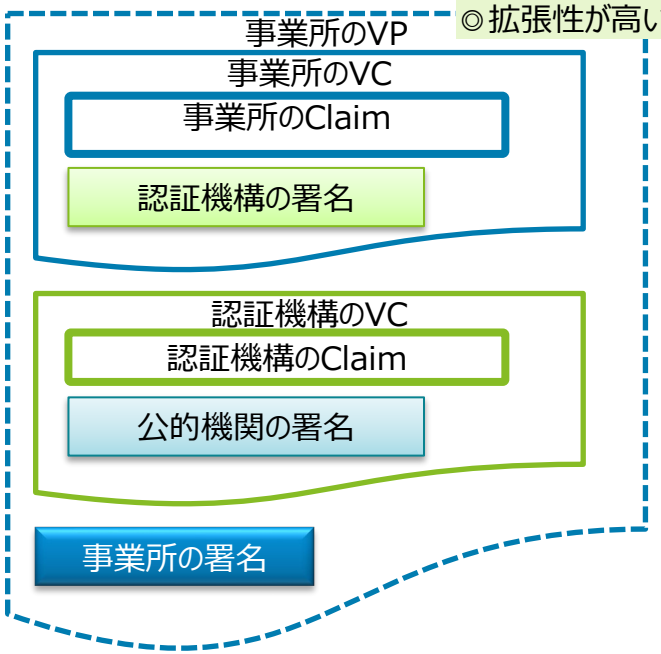
今回実装したVP/VCのイメージ

◎より高いセキュリティ
△実装が複雑
×既存ツール対応不可
△拡張性が低い



より適切と考えるマルチVC in VPのイメージ

○十分なセキュリティ
△実装が複雑
○既存ツール対応可能
◎拡張性が高い



6.1. 実施概要（9/22）
6.1.1. 調査で明らかにする論点とその結果

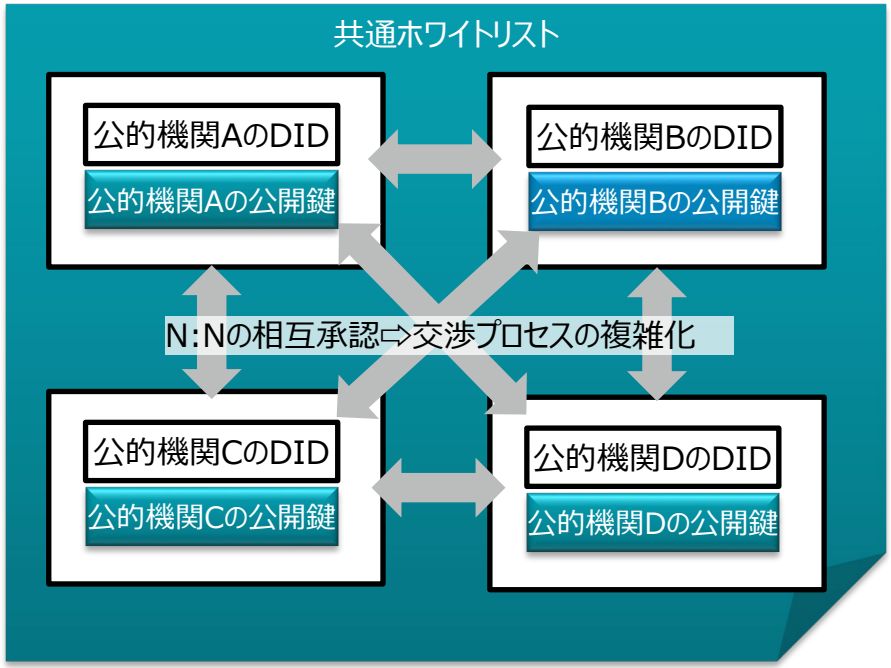
No.	論点	検討結果とその経緯
5	**分散型ネットワークにおけるトラストアンカー**実現に向けたトラストリスト構築およびトラストリスト管理手法の検討	• ヨーロッパでは、X.509ベースのトラストリスト提示によって、信頼できる認証機構を示す形でトラストリストの整備が進んでいる。 • ただ、上記のやり方は中央集権的なEUという権力機構があって初めて機能するものであり、ヨーロッパの取り組みをベースに、より多様な国家間で活用可能なトラストリスト管理のあり方について、内部で検討を重ねた。 • 現時点では、公的機関が提示するVCの形式でトラストリストを用意することが実装負荷／管理負荷／セキュリティの３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。 • 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	• 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。 • 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。又、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。 • 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DID Comm 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。 • 詳細検討及び実装は今後の課題である。

6.1. 実施概要（10/22）
No.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

ヒアリング／調査先	ヒアリング／調査手法	ヒアリング対象者/調査ドキュメントURL
内閣官房　情報通信技術(IT)総合戦略室	資料精査	P.27 Trusted Listを介した証明書有効性検証 https://www.soumu.go.jp/main_content/000750520.pdf

■ホワイトリスト（当初想定）

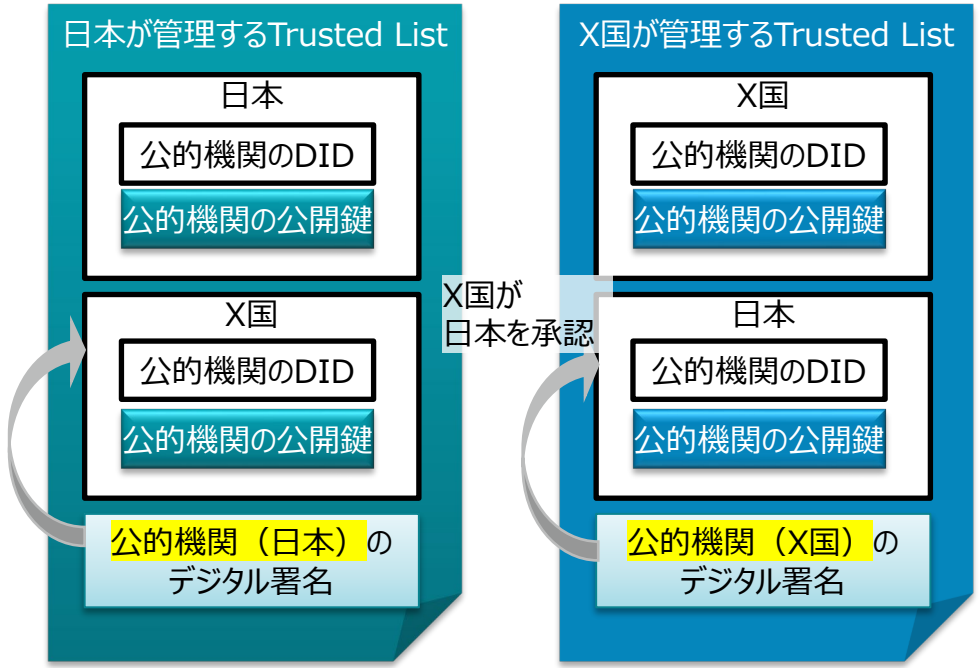
- トラストアンカーの役割をする公的（準公的）機関が集まって、共有のホワイトリストを作成する
- ホワイトリストに含まれる国は**N:Nで相互承認**する。
- 相互承認が行われた国間では、他国の事業所（そのデジタル証明書）が検証できる



■トラストリスト（本取り組みを通じて実装）

- 公的（準公的）機関がトラストアンカーとなることで、他国の事業所（そのデジタル証明書）が検証できる
- トラストリストに含まれる国は当該国と**1:1の関係で承認**する。
- 各公的機関がそれぞれVC化したTrusted Listを作成し、※デジタル認証機構を通じて、各国内の事業所に配布する

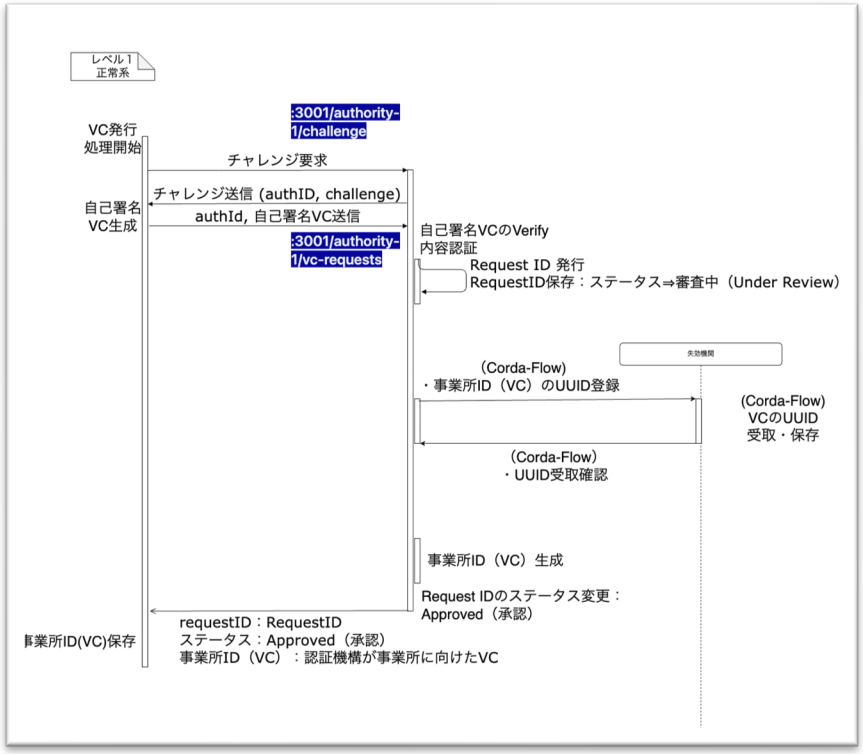
※配布部分は未実装



6.1. 実施概要（11/22）
No.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

ヒアリング／調査先	ヒアリング／調査手法	ヒアリング対象者/調査ドキュメントURL
RFC	資料精査	RFC1994他（https://www.ietf.org/rfc/rfc1994.txt）
DIF	資料精査	https://identity.foundation/presentation-exchange/ https://identity.foundation/didcomm-messaging/spec/v2.1/
W3C	資料精査	https://w3c-ccg.github.io/credential-handler-api/

今回実装したオンボーディングプロトコル



プロトコルへの要求とプロトコルごとの適合性

ビジネス要求	DIF Presentation Exchange	DIF DIDComm	W3C Credential Handler
トラストルート不要な通信暗号化（課題6.1.6）	×	○	△
検証項目の事前合意	○	×	○
使用暗号種類の特定	○	○	×
オンボーディングセッションの維持	×	×	×
規格スコープの適合性	△ VPがターゲットでVCではない。	△ DIDがターゲットでVCではない。	○ ただし、実装規格なのでユースケース適合性の検証が必要

一つの技術プロトコルが完全に適合することはないことを前提に、パーツとして取り込み可能なプロトコル／実装を今後も検討していく予定

6.1. 実施概要（12/22）
6.1.1. 調査で明らかにする論点とその結果

No.	論点	検討結果とその経緯
7	**事業所（VC）のライフサイクル**の精緻化	• 3.2で示した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。 • 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）？ • フィードバックを元に、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。 • 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。

6.1. 実施概要（13/22）
No.7 事業所ID（VC）のライフサイクル精緻化

ヒアリング／調査先	ヒアリング／調査手法	ヒアリング対象者/調査ドキュメントURL
EBSI：失効戦略	資料精査	https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/EBSI+Presents+on+New+Study+about+Verifiable+Credential+Revocation
DIF：プレゼンテーションエクスチェンジプロトコル	資料精査	https://identity.foundation/presentation-exchange/
一般社団法人　沖縄オープンラボラトリ	ヒアリング	PO、PM、PJメンバー

事業所IDの状況（実装済み）

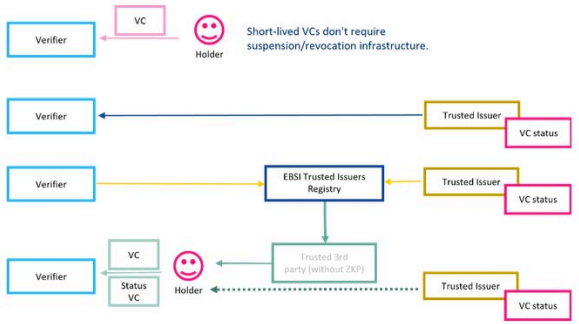
事業所IDの状態		有効期限	
		期限内	期限切れ
VCの失効ステータス	有効	有効	無効（発行時点で定義された失効）
	失効	無効（認証機構による強制失効）	（想定しているユースケースなし）

ヒアリング等で得られたVCライフサイクル課題

1. 企業のコーポレートアクション
2. 特定時点におけるVC失効確認
3. VC失効情報の管理期限
4. 電子署名の技術寿命を超えた商品に対する保証
5. 失効・有効期限切れVCの業務上の取り扱い
6. オンゴーイング検証の頻度

⇨汎用的なライフサイクル仮説の定義及び実装が今後の課題

参考：EBSIの失効戦略（長命VCと短命VC）



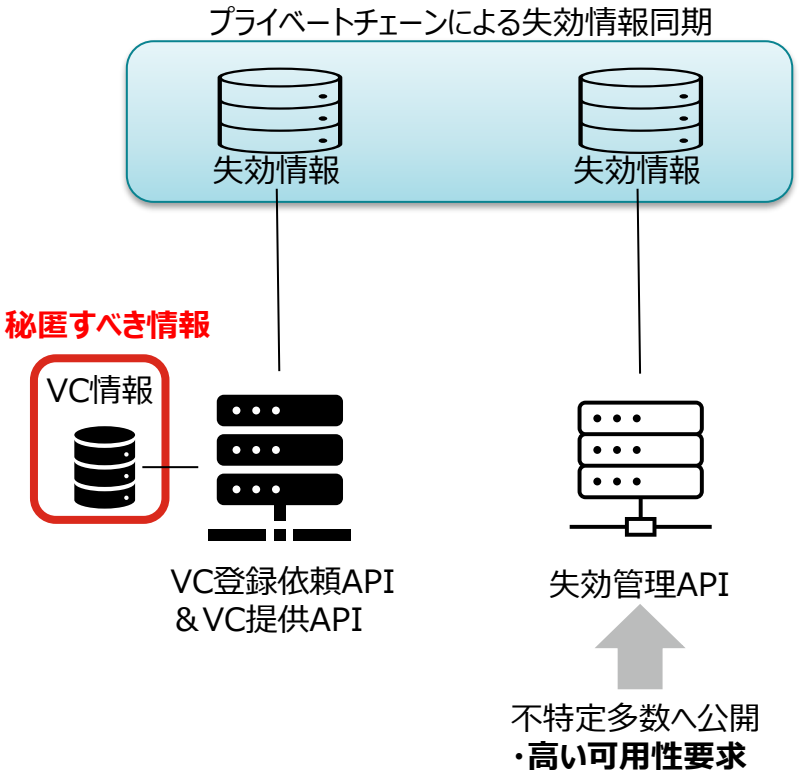
6.1. 実施概要（14/22）
6.1.1. 調査で明らかにする論点とその結果

No.	論点	検討結果とその経緯
8	**信頼できる第三者に関わるセキュリティ**の確保	• 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。 • 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。 • 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。 • 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、アクセスを受けるであろうサービスを独立／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	• 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。 • 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。

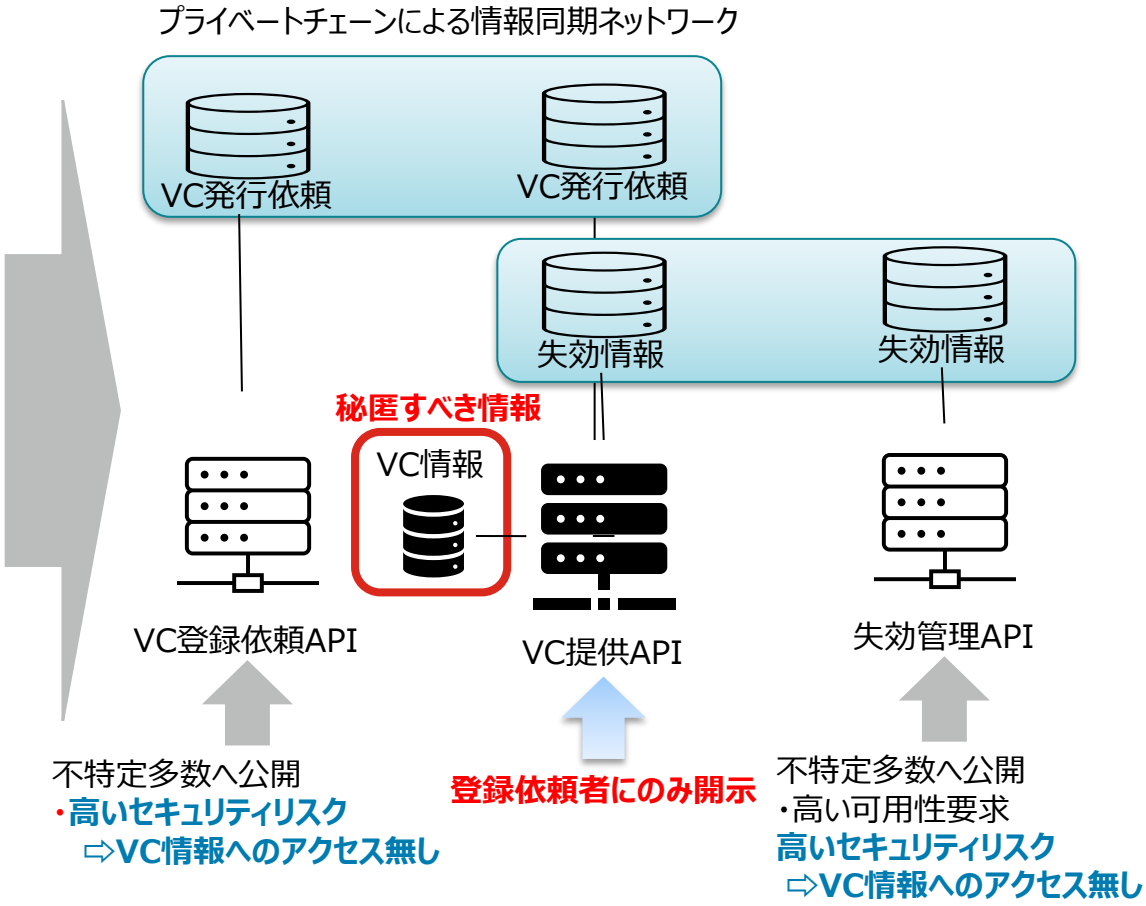
6.1. 実施概要（15/22）
No.8 信頼できる第三者のセキュリティ確保
No.9 ビジネス化に向けたサービス内容の精緻化

ヒアリング／調査先	ヒアリング／調査手法	ヒアリング対象者/調査ドキュメントURL
JIPDEC	ヒアリング	－

今回実装したアーキテクチャ



セキュリティを高めたアーキテクチャ（想定）



6.1. 実施概要（16/22）
6.1.1. 調査で明らかにする論点とその結果

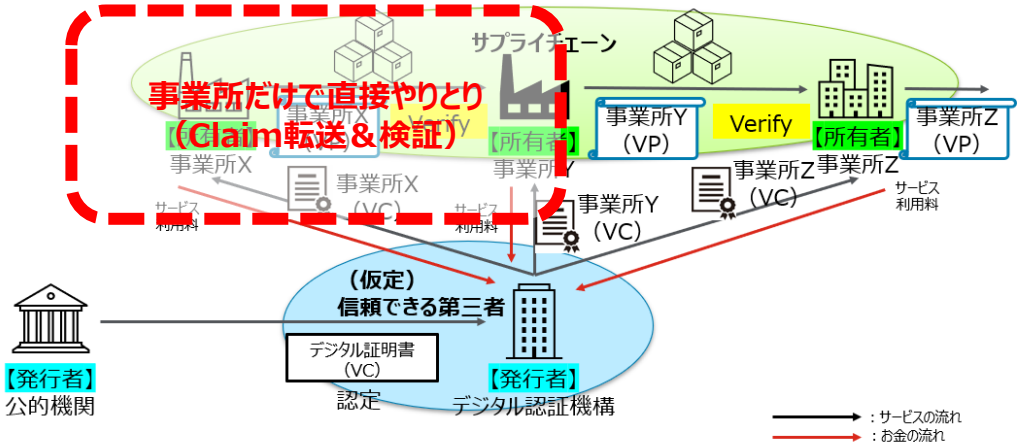
No.	論点	検討結果とその経緯
10	**<u>オフライン検証</u>**	• Africa Unionでは、相互運用性のあるデジタルIDフレームワークのアーキテクチャについて検討を進めている。 • 分散、相互運用、デジタル主権といった点をビジョンに含んでおり、Trusted Webの理念にも通ずる取り組みであると考えている。 • Africa Unionでは、オフライン環境でのデジタルIDクレームの検証が可能であることをゴールの一つに掲げている。 • 事業所ID（VC）の検証がオフラインで行われるニーズは無い認識だが、Central Data Repositoryを必要としない我々の取り組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。

6.1. 実施概要（17/22）
No.10 オフライン検証

ヒアリング／調査先	ヒアリング／調査手法	ヒアリング対象者/調査ドキュメントURL
Africa Union:ドキュメント	資料精査	https://africaunion-my.sharepoint.com/:w:/g/personal/mihretw_africa-union_org/EdsLHszS3LpAuNyYkHaBSJIBirszQhdhkGrPqwdiM7_SZg?rtime=_fUioyXU20g

オフライン検証イメージ
（Africa Unionのドキュメントから画像取得＆追記）

弊社取り組み検証イメージ



検証プロトコルはオフラインでも行えることが必要
ドキュメントより以下抜粋（強調はSBI）

This AU Digital ID Framework proposes to define at the continental level a harmonized approach for individuals to share digital identity claims issued by trusted authorities with service providers **in order to prove their identity in an online and offline environment**. Claims are a collection of attributes about a data subject: e.g., family name, date of birth

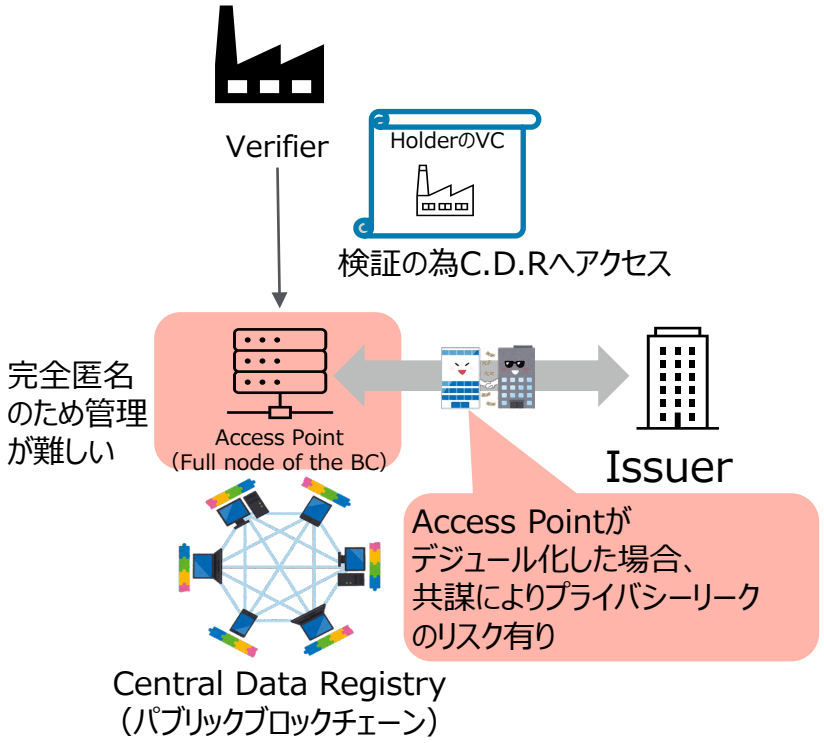
6.1. 実施概要（18/22）
6.1.1. 調査で明らかにする論点とその結果

No.	論点	検討結果とその経緯
11	VC発行体に対する**プライバシー**	• アフリカユニオン等のハイレベル要求には、Issuer（本プロジェクトでい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。） • 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。 • 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。 • 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。

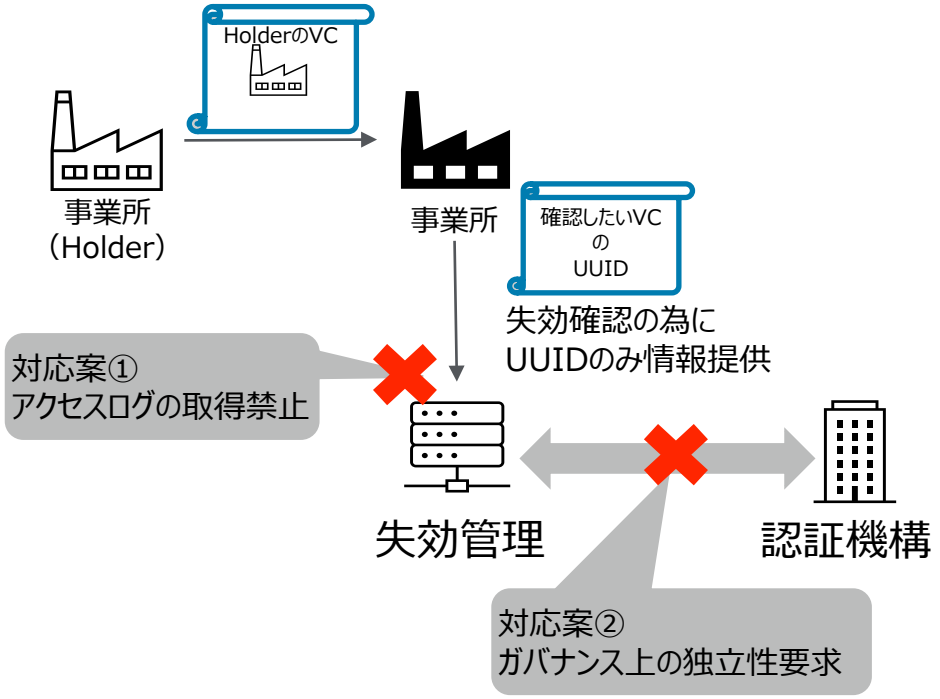
6.1. 実施概要（19/22）
No.11 VC発行体に対するプライバシー

ヒアリング／調査先	ヒアリング／調査手法	ヒアリング対象者/調査ドキュメントURL
Africa Union:ドキュメント	資料精査	https://africaunion-my.sharepoint.com/:w:/g/personal/mihretw_africa-union_org/EdsLHszS3LpAuNyYkHaBSJIBirszQhdhkGrPqwdiM7_SZg?rtime=_fUioyXU20g
W3C Verifiable Credential V2.0 (draft)	資料精査	https://www.w3.org/TR/vc-data-model-2.0/#life-cycle-details

プライバシー要求に対するリスク
（Central Data Repository有りの場合）



プライバシー要求に対する対応
（弊社取り組みにおける可能性）



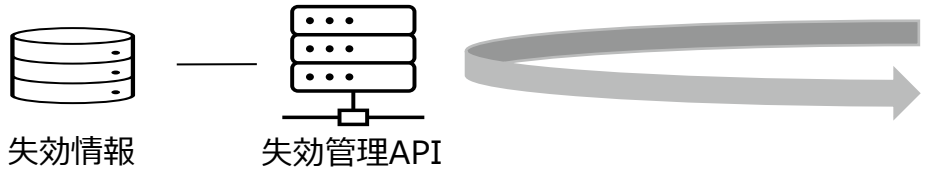
6.1. 実施概要（20/22）
6.1.1. 調査で明らかにする論点とその結果

No.	論点	検討結果とその経緯
12	失効情報の**なりすまし／改竄リスクの低減**	• 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。 • 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. • 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／改竄のリスクは限定的。 • 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／改竄のリスクをなくす。 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。 • 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、実装による検証及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。

6.1. 実施概要（21/22）
No.12 失効情報のなりすまし／改竄リスクの低減

ヒアリング／調査先	ヒアリング／調査手法	ヒアリング対象者/調査ドキュメントURL
内部検討のみ	–	–

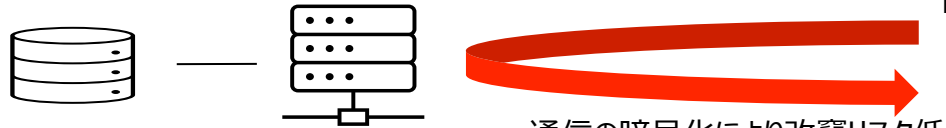
今回実装したAPI



Response Data(署名無し／改竄リスク有り)

{"uuid":"ec20079a-3886-4b1a-927c-b1e65b81e35f","status":"Valid"}

リスク低減策①クライアント／サーバTLSの活用

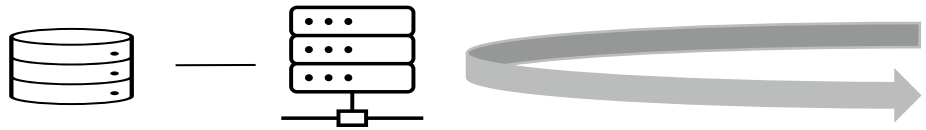


通信の暗号化により改竄リスク低減
（課題6.1.2）

Response Data(署名無し／改竄リスク有り)

{"uuid":"ec20079a-3886-4b1a-927c-b1e65b81e35f","status":"Valid"}

リスク低減策②Response Dataへの署名



Response Data(署名有り／改竄リスク無し)

{・・・
“CredentialSubject”:{
“uuid”:“ec20079a-3886-4b1a-927c-b1e65b81e35f”,“status”:“Valid”}
}
・・・
}

6.1. 実施概要（22/22）
6.1.1. 調査で明らかにする論点とその結果

No.	論点	検討結果とその経緯
13	**鍵の保管**	• 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。 • 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。 • 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. 実施概要
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為、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及び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

No.	残課題（指摘事項含む）	対応方針
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No6、7に合わせた再検討が必要であることが判明。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
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 • 必要に応じてアーキテクチャの見直し改善を実施
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た場合、事業所IDの申請/発行が出来なくなるため、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
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
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の確認
6	更新されたW3C規格（VC2.0）への対応	• 単一VPへの複数VC入れ子構造の実現 • JSONーLD対応のための定義作成およびチェッカー実装
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寄る、拡張性の確保
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
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追加 • 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の準備

7.2. 将来的なユースケース実現モデル
7.2.1. ビジネスモデル案（1/3）

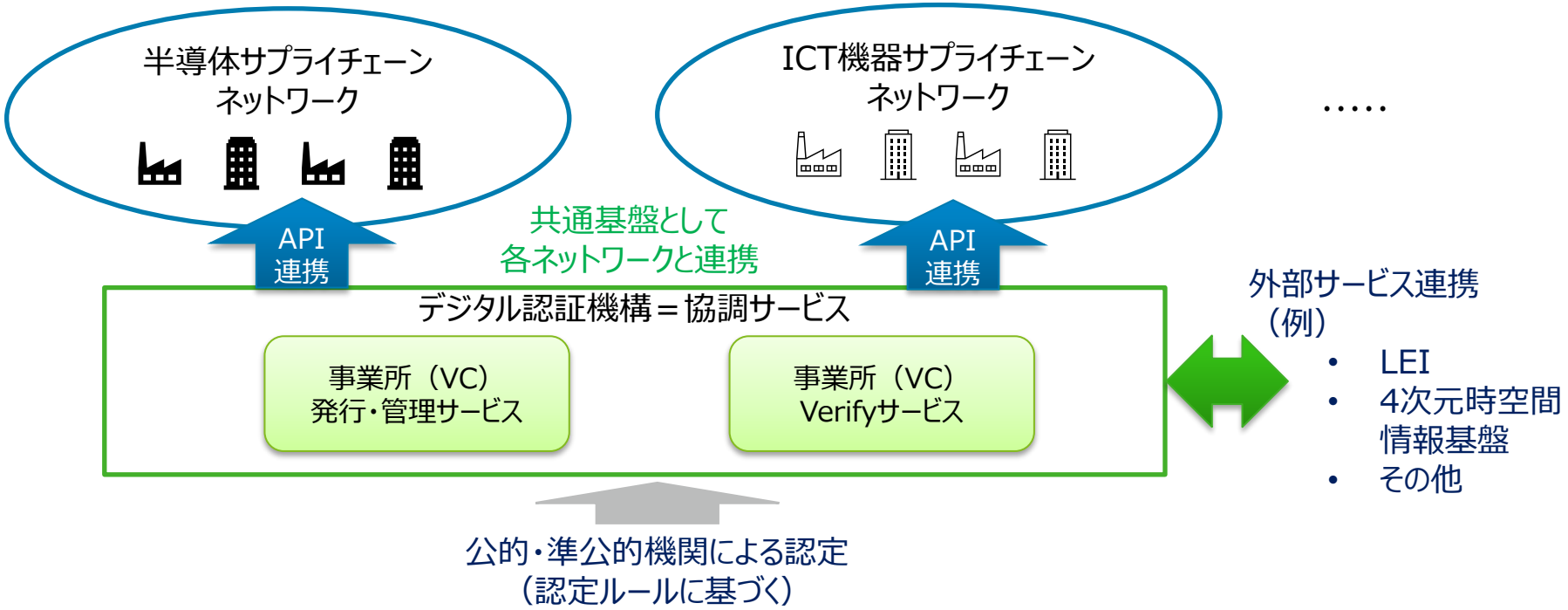
■ デジタル認証機構のビジネスモデル

➢ 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。

➢ 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。



7.2. 将来的なユースケース実現モデル
7.2.1. ビジネスモデル案（2/3）

■ 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。

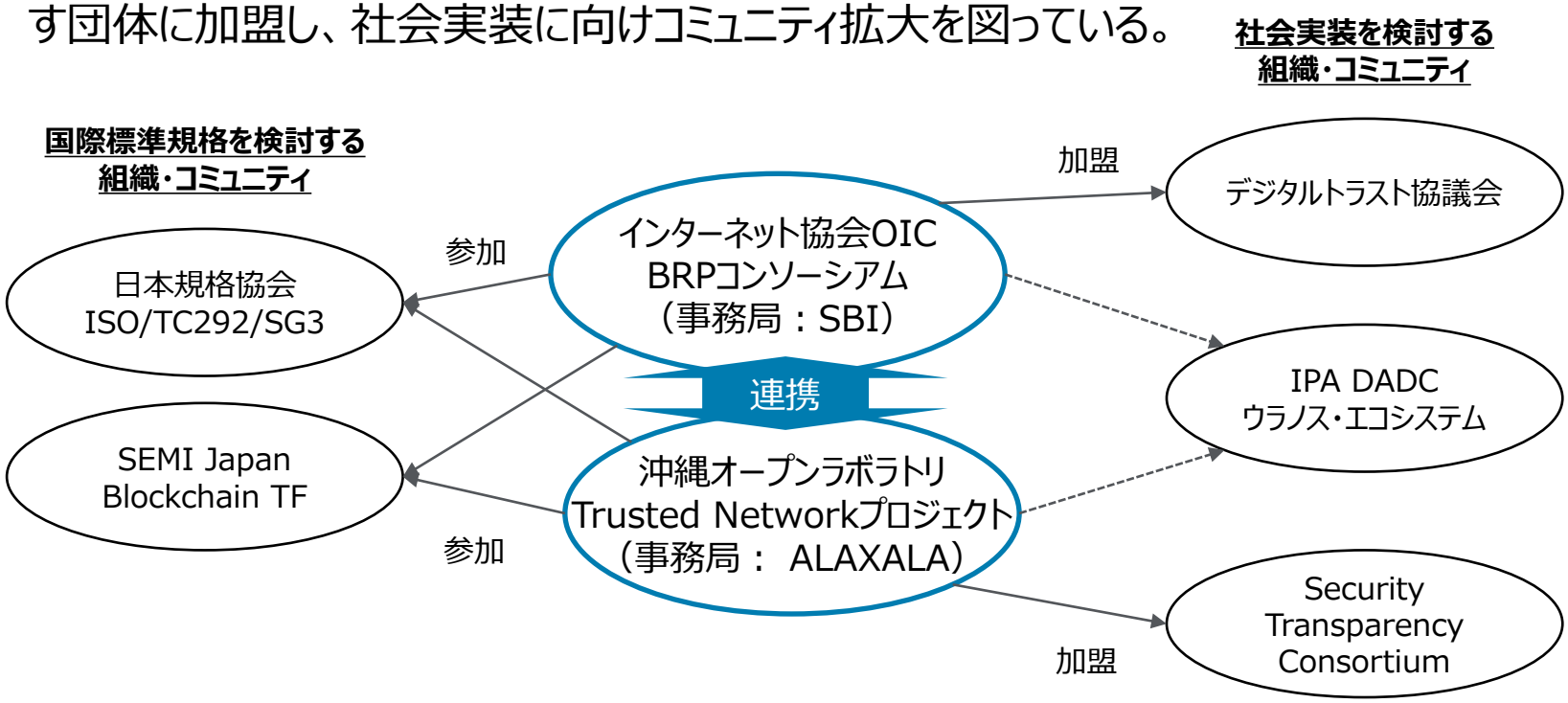
No.	提供サービス	サービスフィー（現状想定）	補足説明
1	事業者（法人等）のオンボーディング	無償	初期登録時に法人本人確認情報の提出を必須とする。
2	事業所デジタル認証 （審査およびデジタル証明書の発行）	レベル１： 事業者（法人等）毎に登録料を徴収 （事業所は複数登録可能）	法人の本人確認（外部参照情報との突合等）を行う。所在は自己表明。
		レベル１＋レベル２： 事業所１件目は無償、２件目より登録料を徴収（※所在証明がデジタル化された場合、無償化を検討）	公的（準公的）機関による事業所の所在証明提出とその確認を行う。
		レベル１＋レベル２＋レベル３： １事業所（デジタル証明書）毎に審査・登録料を徴収	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。）
3	事業者（法人等）および 事業所デジタル認証の更新・廃止	更新（毎年）：発行レベルに準じる 廃止：無償	レベル3の更新については現地訪問有無により変わる想定。
4	事業所デジタル認証のVerify	認証レベル・Verifyする件数等により段階的に課金する想定 （連携先のネットワーク毎に調整）	接続するネットワーク毎に条件を設定する想定。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て追加する想定。

7.2. 将来的なユースケース実現モデル
7.2.1. ビジネスモデル案（3/3）

■ 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。

- 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ほか、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。
- 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. 将来的なユースケース実現モデル
7.2.2. アプリ･システム案（1/4）

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。

観点	本実証の取組み	実現に向けての取組み
データ主体によるコントロール	• 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。	• 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	• 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ブラウザ版とする。	• 引き続き左記を実施する。
ユーザー視点	• 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）で対応可能とする。 • 事業所（VC）の利用機能は、利用ユーザが分かりやすいように、API提供とする。	• 利用ユーザに、DID作成やVC/VPを使ったVerifyが容易でにできるように、ウォレットアプリケーションSDKを提供する。

7.2. 将来的なユースケース実現モデル
7.2.2. アプリ･システム案（2/4）

デジタル認証機構の実現に向けて、システムに関する将来のアーキテクチャ案を整理する。

観点	本実証の取組み	実現に向けての取組み
継続性	• 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。	• 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	• 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。	• 引き続き左記を実施する。
相互運用性	• 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。	• 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あり。
更改容易性･拡張性	• 事業所（VC）は、W3CのDID/VCの規格に沿って開発する。	• 事業所（VC）の利用ユーザ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を用意する。 • OpenID for Verifiable Credentialsなど他の規格の開発方法を整備する。

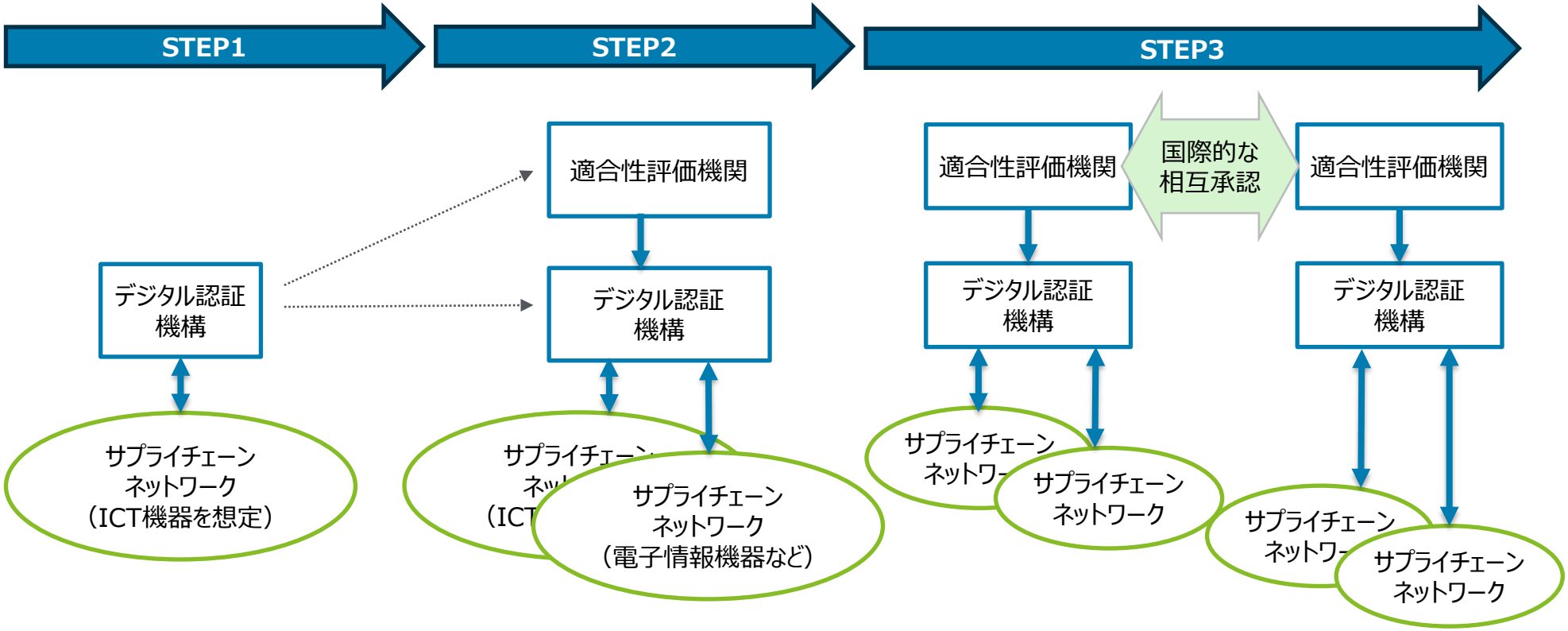
7.2. 将来的なユースケース実現モデル
7.2.2. アプリ･システム案（3/4）

■ 段階的に発展させるシステムロードマップ

STEP1：国内でミニマム構成にてスタート

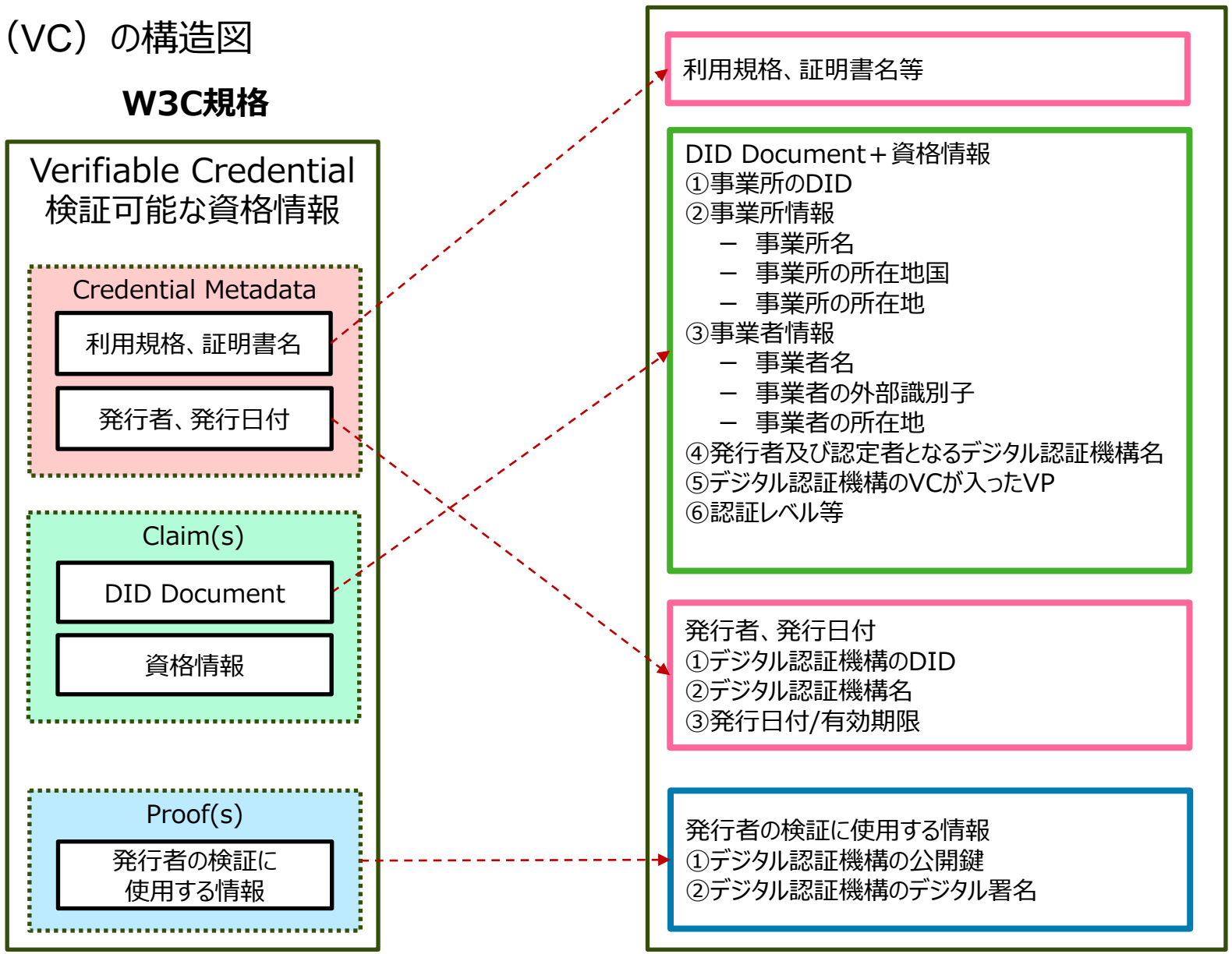
STEP2：適合性評価機関を独立、複数のネットワークへのサービス提供

STEP3：適合性評価機関の相互承認による国際的な展開



7.2. 将来的なユースケース実現モデル
7.2.2. アプリ･システム案（4/4）

■ 事業所（VC）の構造図



7.2. 将来的なユースケース実現モデル
7.2.3. ガバナンス・ルール案（1/5）

■ 全体説明

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。

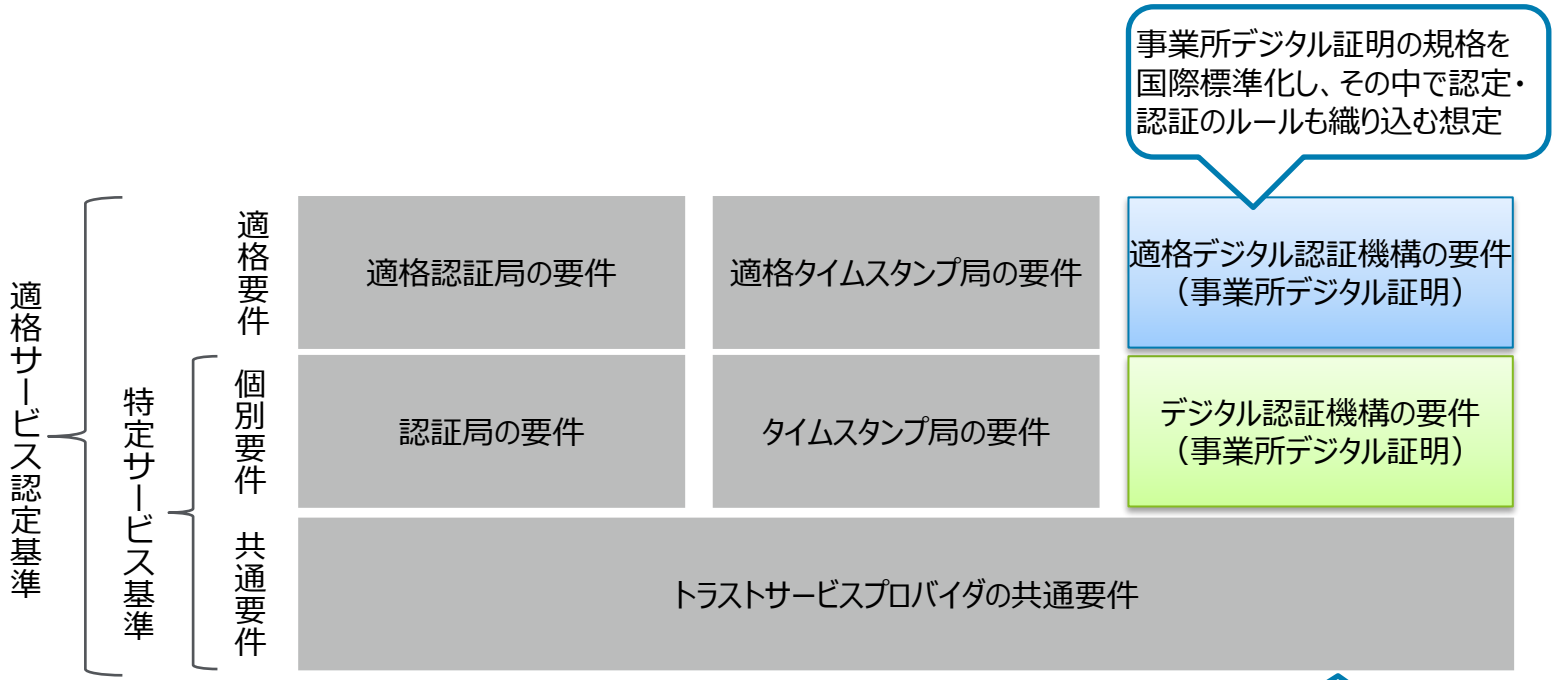
※「Trusted Web ホワイトペーパーver.3.0概要」より抜粋
トラストフレームワークとは
- 運用規則、スキーム規則、運用方針などの仕様、規則、協定の集合のこと。
- エコシステム内においてトラストフレームワークに準拠していることを示すことができる認証プロセスや、準拠状態を維持・監査するための、ガバナンスや監査機関を含むこともある。

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」2023年11月
https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/pdf/trustedweb_3_gaiyou.pdf

7.2. 将来的なユースケース実現モデル
7.2.3. ガバナンス･ルール案（2/5）

■ トラストフレームワーク提供者に関するガバナンス

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。
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」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。



参考：トラストに関するワーキングチーム-中間報告-（令和3年4月26日）

7.2. 将来的なユースケース実現モデル
7.2.3. ガバナンス・ルール案（3/5）

■ トラストフレームワーク提供者に関するガバナンス

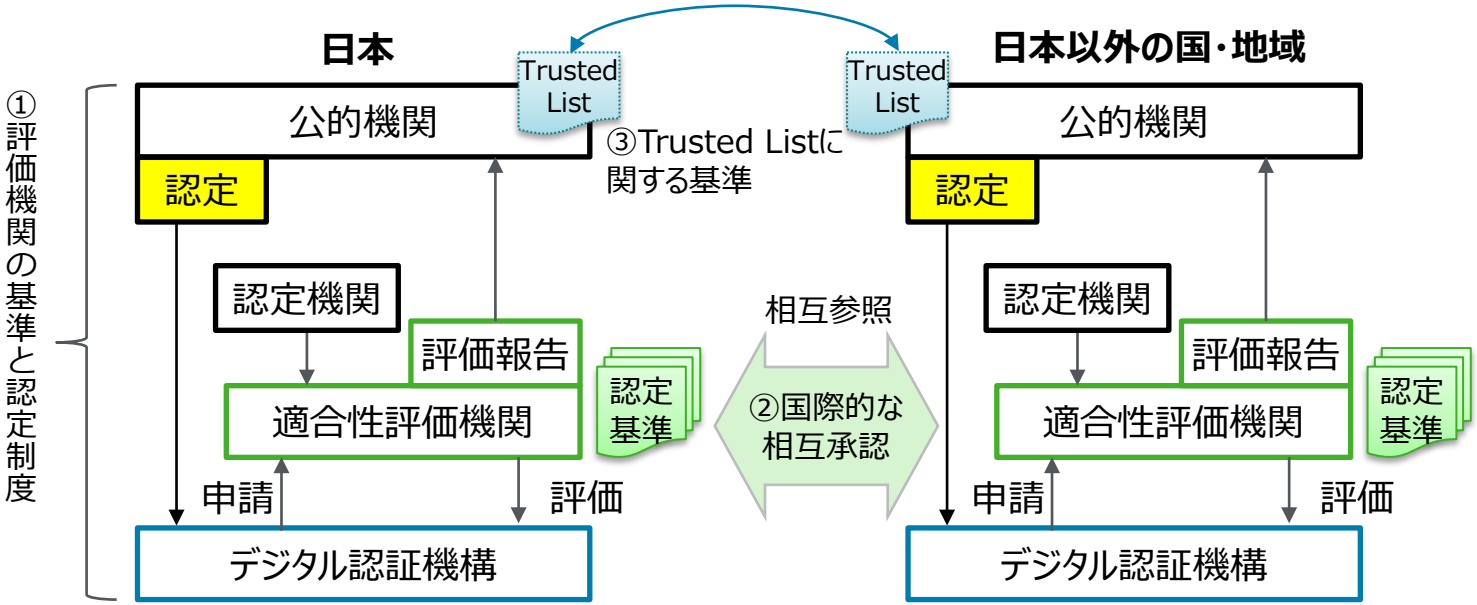
デジタル認証機構の適格認定およびデジタル証明の国際間の利用について（想定）

■ 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及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



7.2. 将来的なユースケース実現モデル
7.2.3. ガバナンス・ルール案（4/5）

■ システムに関するガバナンス

トラストサービスプロバイダーの共通要件（認証局の例*）

- ■ 運用基準
  - ① 利用者の真偽の確認
  - ② 関係要員及び運用体制
  - 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

*参考：JIPDECトラステッド・サービス登録（認証局）｜一般財団法人 日本情報経済社会推進協会

7.2. 将来的なユースケース実現モデル
7.2.3. ガバナンス・ルール案（5/5）

■ システムに関するガバナンス

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又は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
- ① 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プラン・ロードマップ

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。

8. Trusted Web に関する考察

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（柔軟性）
  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。

参考： Data-Spaces-Business-Alliance「 Technical Convergence Version 2.0」2023年4月21日
https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf

8. Trusted Web に関する考察
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（脅威の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. Trusted Web に関する考察
8.3. Trusted Web のアーキテクチャに関する課題と提言

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. Trusted Web に関する考察
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

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

システム	ライセンス取得有無	第三者による再現方法

• 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
	無し	• 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
		• 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

• 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	検証に必要な開発ライセンスが必要	• 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 • 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

ヒアリング詳細・結果

ヒアリング先	課題No./検証する課題論点	ヒアリング項目	回答
ICT機器・サービス提供会社	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 ※事業所VC利用における信頼度	取引先確認の際、調査会社に依頼する代わりに、事業所VCを使いたいと思うか	➢ 取引先確認の際に何らかの調査（調査会社又は自社による）は必ず必要になると想定するため、事業所の所在確認に対する実在性証明に活用したいと思う ➢ 信用度を示す情報に満たしていれば、調査会社の代わりに使うのはありだと思う。ただ一般的に企業調査を想定すると、財務情報等が含まれているが、その辺については関わっていないと感じた
同上	同上	上記を踏まえて、使えないと思う場合、追加で必要なものとしては何を想定するか	➢ 事業者の証明をセットで提供してもらうと有難い ➢ 業務の実績・業績、事業継続年数、設立準拠法国、国籍等
同上	同上	事業所VCに対し、他に含みたいと思う情報はあるか	➢ 誰がどのように確認したか、審査方法や審査エビデンス ➢ 信用度という意味では、その企業の過去の取引実績が想定される（今までの取引回数、他社との取引有無等）。また、米国商務省産業安全保障局（BIS）が発行している貿易上の取引制限リスト(Entity List)における記載有無も参考になる指標であると想定
同上	同上	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	➢ 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 ➢ 稼働（あるいは生産）しているという情報

ヒアリング詳細・結果

ヒアリング先	課題No./検証する課題論点	ヒアリング項目	回答
ICT機器・サービス提供会社	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、感じる有用性	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	➢ 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。 ➢ 各国でトラストの管理が必要である。 なお、海外によっては、機密管理される情報は自国のクラウド以外への格納はゆるされていないため、自国で発行、検証できるデジタル証明書が必須と思います。
同上	同上	事業所VCを例にして、海外で発行した証明書に入っていてほしい項目は他にあるか	➢ （国内VCの回答と同様）
同上	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	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	➢ 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製造メーカーの実在性が証明書になる。