TOPPAN

令和 4 年度補正
Trusted Web 開発等推進事業に係る調査研究

【報告書】

（Trusted Web の実現に向けたユースケース実証
分析レポート）

2024 年 3 月

TOPPAN 株式会社

本書の位置づけ

様々な社会活動のデジタル化が進む一方で、やりとりされるデータそのものの信頼への懸念、先鋭化していくプライバシーリスク、データの取扱いへの懸念からくる産業界におけるデータ活用の停滞、勝者総取り等によるエコシステムのサステナビリティへの懸念など、信頼できる自由なデータ流通（DFFT）を妨げる、様々な歪みが生じている。

これらの懸念は、データそのものが信頼できない、データのやり取りをする相手を信頼できない、相手方におけるデータの取扱いを信頼できないといった現状が主な原因と考えられる。

上記背景から、インターネット上で、DFFT を確保する枠組みを構築すべく、特定のサービスに依存せずに、個人・法人によるデータのコントロールを強化する仕組み、やり取りするデータや相手方を検証できる仕組みなどの新たな信頼の枠組みを付加することを目指す Trusted Web 構想を実現していくことが重要であり、実証や調査、コミュニティ形成を進めていくことが求められている。

本事業は、2022 年度事業である 13 件のユースケースの開発実証等や、内閣官房において活動を進めている「Trusted Web 推進協議会」における Trusted Web ホワイトペーパー策定等の活動、他検討結果を踏まえて、TOPPAN 株式会社（以下、TOPPAN）がデジタル庁の委託を受けて以下の業務 [1]を実施した。

1. Trusted Web ユースケース開発実証に係る調査研究
2. 官民コンソーシアム組成・運営
3. 調査・普及啓発

本報告書は、上記の中でも TOPPAN によるユースケース実証事業分析結果を取りまとめたものである。

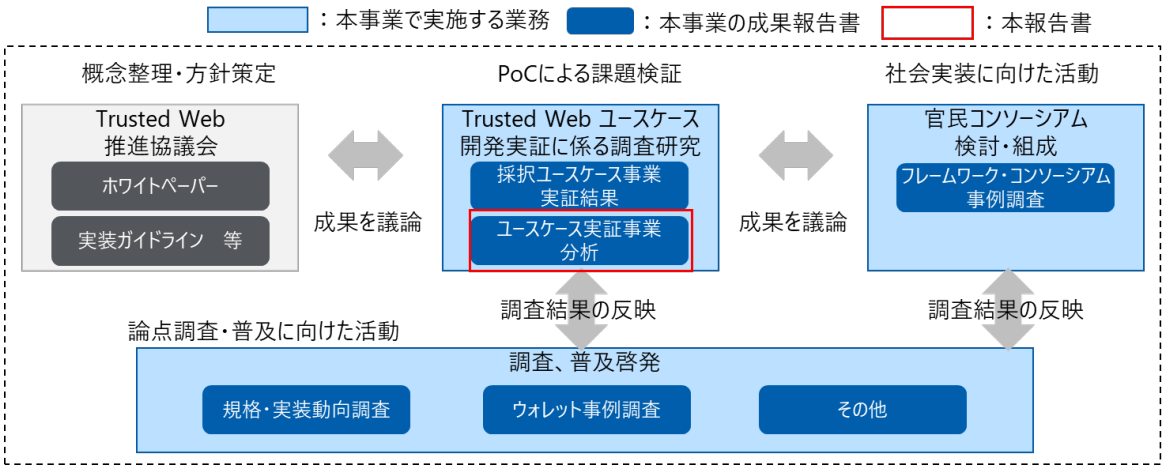

図 本事業のスコープ

[1] 本事業の業務は一部デロイトトーマツグループの委託を受けて実施している

目次

背景・目的

【背景】

デジタル市場競争会議における「デジタル市場競争に係る中期展望レポート」[2]の提言を受け、Data Free Flow with Trust（以下、DFFT）の具現化も視野に、2020 年 10 月に「Trusted Web 推進協議会」[3]が発足した。「Trusted Web」[4]はデータをやり取りする際に、データや取引相手（データ提供者、データ利用者）の検証の簡易化、相手に開示するデータのコントロールを可能にするなどの信頼の仕組みの構築を目指すものであり、DFFT の実現への寄与が期待されている。

Trusted Web 推進協議会では、これまで以下議論・検討をもとに Trusted Web ホワイトペーパーを取りまとめてきた。

2021 年 3 月： ver1.0（内外の様々な関係者と協力・連携していくためのディスカッションペーパーとして整理）

2022 年 8 月： ver2.0（ver.1.0 で示された考え方や構想の具体化、ユースケース分析やプロトタイプ開発を踏まえて、 Trusted Web が目指す信頼の姿のさらなる具体化、それを実現するためのアーキテクチャの提示、ガバナンス検討結果の反映）

2023 年 11 月：ver3.0（2022 年度「Trusted Web 共同開発支援事業」の結果・フィードバックを踏まえてアーキテクチャを再構築するとともに、それを車の両輪として支えるガバナンスのあり方を提示）るためのアーキテクチャの提示、ガバナンス検討結果の反映）

また、ホワイトペーパーver3.0 は、Trusted Web の考え方のビジネスへの適用、実装を分かりやすく理解するためのガイダンスとして作成され、多様な事業者やエンジニアが取り組む際に素材として活用できるように、「概要／コンセプト編」、「ユースケース編」、「実装編」の 3 つのパートに分冊化するとともに、GitHub 上で「実装ガイドライン」の公開を行っている。

2022 年度は Trusted Web のアーキテクチャにかかる整理を主目的に 13 のユースケースを選定して実証事業を推進した。

2023 年度もユースケース実証を踏まえて、Trusted Web 実装における課題抽出を行い、Trusted Web の具現化に向けた取組を推進させていくことが求められている。

---

[2] デジタル市場競争会議.「デジタル市場競争に係る中期展望レポート」.
https://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/dai4/siryou3s.pdf

[3] Trusted Web 推進協議会.
https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/index.html

[4] デジタル庁、日本政府、内閣官房、経済産業省.「Trusted Web とは」.
https://trustedweb.go.jp/about/

【目的】

本書は、Trusted Web 開発等推進事業に係る調査研究に係る調査研究報告書の別紙であり、Trusted Web の具現化に向けた示唆を取りまとめるものである。

本調査は、①ユースケースの成果や課題を分かりやすく整理し、Trusted Web を発信すること、②事業者が Trusted Web を実装する際の課題をまとめ、推進ステップ・実装ガイドライン・その他支援（ルール整備等補助金を必要としないもの）へ提言することを目的に Trusted Web の実現に向けたユースケース実証事業（以下、本実証事業）の整理・分析を行った。

実施アプローチ

Trusted Web の取組の発信や、他事業者が今後 Trusted Web に関する取り組む際のガイドとなることを目的に 2023 年度のユースケースにおける成果や課題を整理した。2023 年度は、2022 年度に実施したビジネスモデル・プロトタイプシステム企画・開発に加えて、新たにガバナンス・コミュニティの形成についても実施したため、ガバナンスに関する章も記載している。

加えて、ビジネスモデル・実装手法の比較を中心に 2022 年度ユースケース実証結果もインプットとして活用した。

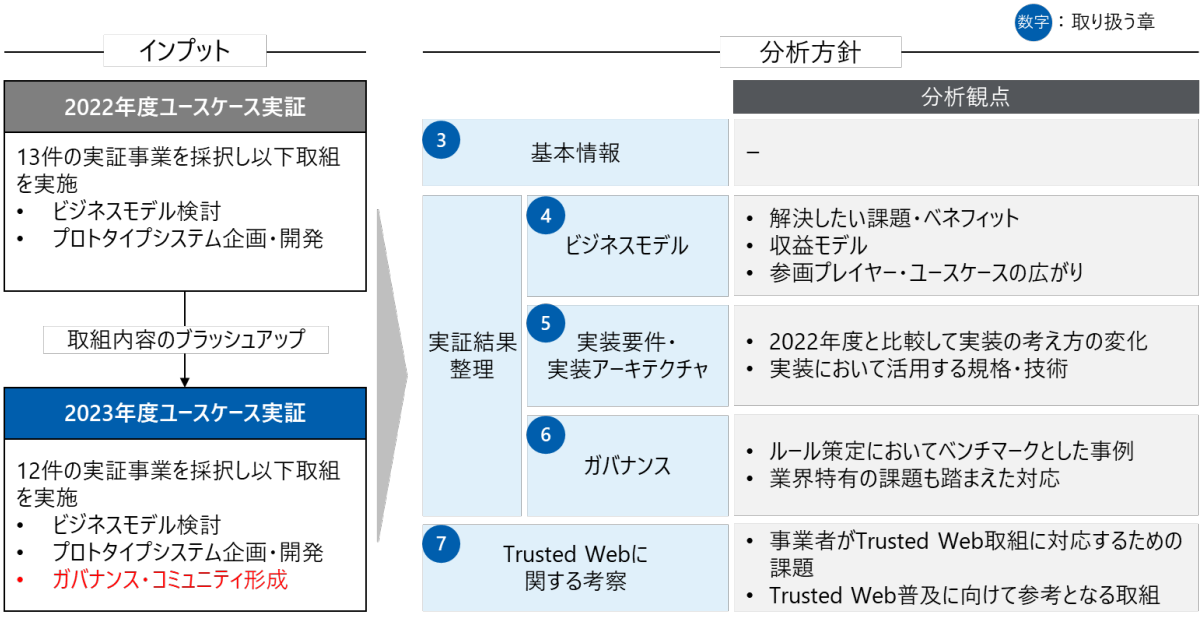

図 2-1 分析アプローチ

実証事業整理（基本情報）

１.１. ユースケース概要

本実証事業の公募で選定した 12 事業者（12 ユースケース）の基本情報として、各ユースケースが対象とする市場・業界、検証対象とするデータのエンティティ・属性情報、本実証で解決・実現したいことをそれぞれ整理した。

本実証事業は、Trusted Web のユースケースを実現するためのプロトタイプシステムの企画・開発を目的にした事業であり、企画・開発を行う A 類型と、企画のみを行う B 類型の 2 方式で公募を行っている。12 事業者中、富士通 Japan 株式会社、株式会社 PitPa、みずほリサーチ＆テクノロジーズ株式会社、一般社団法人情報サービス産業協会が取りまとめる 4 事業については B 類型で採択し、残りの 8 事業者は A 類型で採択した。なお、株式会社 PitPa については、本事業で企画するシステムの開発を別事業で実施しており、その成果についても可能な範囲で一部報告いただいた。

また、大日本印刷株式会社、シミック株式会社、株式会社 ORPHE については、2022 年度実証事業において取り組んだテーマを発展させた形で実証事業に参画している。

各ユースケースの詳細は別途公開される各事業者の成果報告書を参照いただきたい。

1. ウォレットによるアイデンティティ管理とオンラインコミュニケーション
   - ① 代表事業者名 ：株式会社 DataSign（以下、DataSign）
   - ② 類型（A/B） ：A 類型
   - ③ 分野 ：個人
   - ④ 検証対象となるエンティティと属性情報：
     個人の属性情報（企業・コミュニティ等）を、メッセージをやり取りする相手が検証する。

2. 共助アプリにおけるプラットフォームを超えたユーザートラストの共有
   - ① 代表事業者名 ：大日本印刷株式会社（以下、DNP）
   - ② 類型（A/B） ： A 類型
   - ③ 分野 ： 個人
   - ④ 検証対象となるエンティティと属性情報：
     個人の共助実績を共助実績アプリが検証する。

3. 国際間の教育拡充と労働市場の流動性を高める信頼ネットワーク構築
   - ① 代表事業者名 ：Institution for a Global Society 株式会社（以下、IGS）
   - ② 類型（A/B） ：A 類型
   - ③ 分野 ：個人（人材）
   - ④ 検証対象となるエンティティと属性情報：
     個人の教育成績・スキルを採用企業が検証する。

4. 大学技術職員の活躍に向けたスキルの見える化
   - ① 代表事業者名 ：富士通 Japan 株式会社（以下、富士通 Japan）

② 類型（A/B） ：B 類型
③ 分野 ：個人（人材）
④ 検証対象となるエンティティと属性情報：
大学職員の実績・意見・スキルを、共同研究を行う事業者・採用企業等が検証する。

5. 海外人材還流におけるクロスボーダー型個人情報流通システム
① 代表事業者名 ：株式会社 PitPa （以下、PitPa）
② 類型（A/B） ：B 類型
③ 分野 ：個人（人材）
④ 検証対象となるエンティティと属性情報：
海外人材の職務経歴を受入企業・サービス事業者が

6. ものづくりのサプライチェーンにおける製品含有化学物質情報等の確実な伝達を可能とする Chemical Management Platform
① 代表事業者名 ：みずほリサーチ＆テクノロジーズ株式会社（以下、みずほ R&T）
② 類型（A/B） ：B 類型
③ 分野 ：サプライチェーン
④ 検証対象となるエンティティと属性情報：
製品の化学物質含有量を取引法人が検証する。

7. 事業所ＩＤとそのデジタル認証基盤
① 代表事業者名 ：ＳＢＩホールディングス株式会社（以下、SBI HD）
② 類型（A/B） ：B 類型
③ 分野 ：サプライチェーン
④ 検証対象となるエンティティと属性情報：
法人事業所の実在記録を取引事業者が検証する。

8. 臨床試験および医療現場における信頼性および応用可能性の高い情報流通システム
① 代表事業者名 ：シミック株式会社（以下、シミック）
② 類型（A/B） ：A 類型
③ 分野 ：ヘルスケア
④ 検証対象となるエンティティと属性情報：
個人の医療情報やその共有同意の記録を医療機関が検証する。

9. 下肢運動器疾患患者と医師、研究者間の信用できる歩行データ認証・流通システム
① 代表事業者名 ：株式会社 ORPHE（以下、ORPHE）
② 類型（A/B） ：A 類型
③ 分野 ：ヘルスケア

④　検証対象となるエンティティと属性情報：
個人の医療情報やその共有同意の記録を医療機関が検証する。

10. 「KYC/KYB に基づいたトラストのある取引」を促進する新しい仕組み
①　代表事業者名　：株式会社電通総研[5]（以下、電通総研）
②　類型（A/B）　：A 類型
③　分野　　：法人、金融
④　検証対象となるエンティティと属性情報：
法人の実在性情報、法人口座開設申請者の在籍確認情報、法人口座情報とその開設情報を金融機関が検証する。

11. 補助金事業を題材とした法人向け行政手続 DX 社会基盤化のプレ検討
①　代表事業者名　：一般社団法人情報サービス産業協会（以下、JISA）
②　類型（A/B）　：B 類型
③　分野　　：行政
④　検証対象となるエンティティと属性情報：
法人の基本情報と実在情報、事業内容情報を補助金事業等の事務局が検証する。

12. Trusted Web Advertising System with OP
①　代表事業者名　：Originator Profile 技術研究組合（以下、OP CIP）
②　類型（A/B）　：A 類型
③　分野　　：メディア
④　検証対象となるエンティティと属性情報：
広告主・広告仲介事業者・メディア企業の資格情報を Originator Profile 技術研究組合が検証する。

[5] 事業開始時は「株式会社電通国際情報サービス」であったが、本事業期間中に「株式会社電通総研」へ称号を変更した

表 3-1-1　本実証事業で選定したユースケースの基本情報

No.	ユースケース	代表事業者	類型	分野	実証概要		
					検証対象のエンティティ	検証する属性情報	検証者
1	ウォレットによるアイデンティティ管理とオンラインコミュニケーション	株式会社 DataSign (DataSign)	A	個人	個人	所属情報 （企業・コミュニティ等）	メッセージをやり取りする相手
2	共助アプリにおけるプラットフォームを超えたユーザートラストの共有	大日本印刷株式会社 (DNP)	A	個人	個人	共助実績	共助実績アプリ
3	国際間の教育拡充と労働市場の流動性を高める信頼ネットワーク構築	Institution for a Global Society 株式会社(IGS)	A	個人 (人材)	個人	教育成績・スキル	採用企業
4	大学技術職員の活躍に向けたスキルの見える化：スキルの質保証と主体的情報開示の試行	富士通 Japan 株式会社 (富士通 Japan)	B	個人 (人材)	大学職員	実績・意見・スキル	共同研究を行う事業者・採用企業等
5	海外人材還流におけるクロスボーダー型個人情報流通システム	株式会社 PitPa (PitPa)	B	個人 (人材)	海外人材	職務経歴	受入企業・ サービス事業者
6	ものづくりのサプライチェーンにおける製品含有化学物質情報等の確実な伝達を可能とする Chemical Management Platform	みずほリサーチ＆テクノロジーズ株式会社 (みずほ R&T)	B	サプライチェーン	法人・製品	化学物質含有量	取引法人
7	事業所 ID とそのデジタル認証基盤	ＳＢＩホールディングス株式会社(SBI HD)	A	サプライチェーン	法人の事業所	事業所の実在記録	取引事業者
8	臨床試験および医療現場における信頼性および応用可能性の高い情報流通システム	シミック株式会社 (シミック)	A	ヘルスケア	個人	個人の医療情報 同意の記録	医療機関
9	下肢運動器疾患患者と医師、研究者間の信用できる歩行データ認証・流通システム	株式会社 ORPHE (ORPHE)	A	ヘルスケア	個人	個人の医療情報 同意の記録	医療機関
10	「KYC/KYB に基づいたトラストのある取引」を促進する新しい仕組み	株式会社電通総研 (電通総研)	A	法人金融	法人	法人の実在性情報 申請者の在籍確認情報 口座情報・口座開設情報	金融機関
11	助金事業を題材とした法人向け行政手続 DX 社会基盤化のプレ検討	一般社団法人 情報サービス産業協会(JISA)	B	法人行政手続き	法人	法人基本情報 法人実在情報 事業内容情報	補助金事業等の事務局
12	Trusted Web Advertising System with OP	Originator Profile 技術研究組合 (OP CIP)	A	メディア	広告主 広告仲介事業者 メディア企業	メディア・広告主の資格情報	OP CIP

１.２. プロトタイプシステムにおいて企画・実装した機能・仕組み

公募要領で提示した Trusted Web に求められる以下 3 つの機能・仕組みを実現する手法と検討事業者を下表にまとめた。

機能 1 ：ユーザ（自然人又は法人）自身が自らに関連するデータをコントロールする

機能 2 ：データのやり取りにおける合意形成の仕組みがあり、合意の履行のトレースができる

機能 3 ：検証（Verify）できる領域を拡大することにより、Trust の向上を図ることができる

機能 1 の実現方法として、Verifiable Credentials (VC)を利用者自身で保持し、自身が情報を提示したいタイミングで提示する、証明書情報に記載されている情報を選択的に開示する手法を実装検討した事業者を確認した。また、プライベートブロックチェーン等を活用して、共有権限の管理を通じてデータコントロールの実現検討した事業者を確認した。その他、秘密計算技術の活用や端末のペアリングを活用することを検討した事業者を確認した。

機能 2 の実現方法として、合意形成の仕組みの実現方法では 2 者間のメッセージング機能を活用することや端末のペアリングを活用する事業者を確認、合意履行のトレースはその記録を耐改ざん性担保等が可能なストレージに格納する事業者を確認した。

機能 3 の実現方法として、ユーザーや事業者の信頼性を高める取り組み、デジタル署名を活用する取り組み、相互運用性を高めるために、データ連携方法・データモデルの標準化の取り組み等が確認された。

表 3-2-1　企画・実装した機能・仕組みとその実現手法

機能・仕組み	実現手法	検討事業者
ユーザ（自然人又は法人）**自身が自らに関連するデータをコントロール**できる	VC を自身で保持、あるいは選択的属性開示（SD-JWT VC 等）を活用してデータの開示範囲を自身でコントロールする	DataSign、DNP、PitPa、SBI HD、ORPHE、電通総研、JISA、OP CIP 等
	共有権限管理が可能なブロックチェーン（プライベートチェーン）等を活用することでデータ共有範囲を制御する	みずほ R&T、SBI HD 等
	秘密計算を活用することでデータを秘匿化したままスキルの計算を行い、元データを見ない状態で確認をすることで自身のデータを保護する	IGS
	ペアリングを行う端末を自身で制御	シミック
データのやり取りにおける**合意形成の仕組み**があり、**合意の履行のトレース**ができる	二者間のメッセージングの中で提示する属性情報に対する合意等を行う（SIOPv2、DIDComm 等）	DataSign、DNP、電通総研、JISA、OP CIP 等
	同意プロセスを経た後にその結果を端末ペアリングを行いそのペアリング結果の履歴を継続的にトレース	シミック
	合意した記録を耐改ざん性担保等が可能なストレージ（ブロックチェーン・IPFS 等）に格納する	富士通 Japan、みずほ R&T、SBI HD、シミック、ORPHE 等
検証（verify）できる領域を拡大することにより、Trust の向上を図ることができる	ユーザーの信頼性を向上することでの検証可能性を向上する（e-KYC 等の身元確認活用等）	DataSign、PitPa 等
	事業者の信頼性を向上することで検証可能性を向上する（PKI・トラストリスト等）	SBI HD、JISA 等
	デジタル署名の活用で検証拡大を図る	IGS、PitPa、シミック、電通総研、OP CIP 等
	ウォレット等を念頭に置いて標準仕様に準拠した証明書フォーマットや通信プロトコルを活用（W3C-VC・OID4VC 等）	DataSign、大日本印刷、みずほ R&T、ORPHE、JISA 等
	やり取りするデータモデルの標準化	IGS、富士通 Japan、SBI ホールディングス 等

1.3. 今後のマイルストン

各事業者の今後のマイルストン（課題への対応・継続実証、初期実装・商用化、横展開・市場拡大）を下図にまとめた。

12 事業者のうち 7 事業者(A 類型の 8 事業者のうち IGS 以外の 7 事業者)が、2025 年度中に初期実装・商用化を計画している。

今後の取り組みについて、A 類型の事業者は既にプロトタイプシステム開発を実施しているため、商用化に向けて相互運用性確保に向けた技術検証・ガイドライン整備、ガバナンス・認定団体の整備・業務運用プロセスの整備等を実施して商用化を目指している。B 類型の事業者は、本事業で実施した要件定義等をもとにパイロットシステムの開発等を進め、2026 年度以降の商用化に向けて取り組みを進めていく予定である。

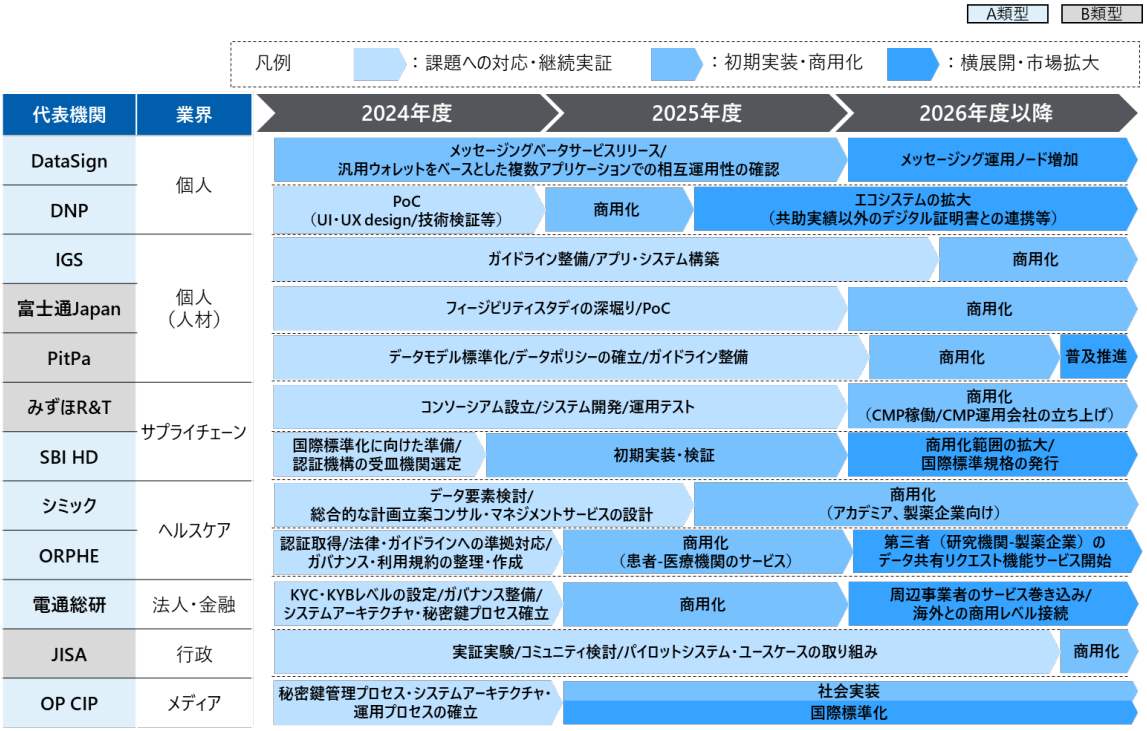

図 3-3-1　今後のマイルストン

実証事業 - ビジネスモデル

1.4. 顧客の課題と提供価値

各ユースケースでの顧客となる対象と、その顧客が抱える課題、および Trusted Web で実現できる顧客への提供価値を下表に整理した。

個人のユーザを対象に課題・提供価値を整理した事業者が 3 事業者(DataSign・PitPa・OP CIP)、法人・法人担当者を対象に課題・提供価値を整理した事業者が 11 事業者(DataSign 以外の 11 事業者)であった。

個人のユーザの受ける提供価値としては、自身でコントロールを行使してデータをやり取りできる(DataSign)、特定の事業者の関与なしで情報を利用・共有できる(DataSign)、利用するサービスの安心感の向上(DataSign、OP CIP)、サービスによって個人の信頼性担保における価値の享受ができる(PitPa)が挙げられた。

法人・法人担当者の受ける提供価値としては、データ検証に係るコスト低減(DNP、IGS、富士通 Japan、みずほ R&T、電通総研・JISA)、信頼性向上による新規サービス実現・他サービスとの連携(DNP・シミック・ORPHE)、提供・調達するサービスの安全性の向上(SBI HD、OP CIP)、エンドユーザが所属する事業者自身のトラスト向上 (PitPa)等が挙げられた。

表 4-1-1　顧客の課題と提供価値

代表機関	対象顧客	課題意識（ペイン）	本ユースケースで実現する顧客への提供価値
DataSign	情報のやりとりを行いたいビジネスパーソン	• 通信相手が本当に意図した人物か分からない • 特定の事業者に多くの情報を渡しすぎて不安	• 自らアイデンティティを管理でき、サービス事業者や他の生活者を検証しつつ、必要最小限の情報を選択的に開示し、特定の事業者へ依存せずに安全なコミュニケーションを実現
DNP	共助アプリベンダ	• アプリユーザーの信頼性を担保するためにコストがかかる、アプリユーザーの継続的利用・活性化に課題 • マネタイズの方法が広告・利用料などパターンが限られる、自社エコシステムでは規模的に収益が不十分	• 他共助アプリの共助実績をユーザートラストの検証として利用化可能 • 共助実績を、共助以外のサービスとも連携可能
IGS	国内に拠点を置く日本企業	• デジタル領域の人材不足であり、海外から人材を採用する必要があるが、海外人材は能力の把握が難しく、採用にかかるデータ管理が煩雑	• 標準化された能力データを活用し、海外人材が自身でデータを管理可能な採用マッチングサービス活用による効率的な管理のもと海外人材の採用
富士通 Japan	地域のニーズに応える人材育成・研究の推進を重点施策とする 55 の国立大学等	• 研究促進や地域貢献に繋がる機会を増やしたいが、技術職員がどのようなスキルや経験を持っているか分からない • プロジェクトへのアサインがコネクションや主観的な判断になっており、非効率・機会損失となっている	• スキルの標準化/可視化を行い、マッチング基盤を整備することで、大学とマッチングしたい一般企業・大学間の研究促進および地域貢献（産業活性化や課題解決など）の支援
PitPa	海外人材を採用したい/雇用している日本国内企業	• 海外出身従業員の採用数・満足度を向上したいが、企業認知度の不足	• 証明書発行による企業努力によってコストをかけずに海外採用 PR の実現 • 海外出身従業員のモチベーション向上、生活支援にも繋がる福利厚生ツールの獲得
	日本での労働を希望する海外人材	• 職歴に紐づくスキルや信頼の証明がないことで転職や日本での生活に支障が生じている	• 職歴が検証可能な証明書の活用によってスキル証明や日本での生活サービス享受における信頼性の向上
みずほ R&T	自動車・電機電子機器等の組立製品サプライチェーンに関わる企業における製品含有化学物質管理の担当部署・担当者	• 製品含有物質にかかる情報の授受の対応や、正確性・信頼性を確認するのに時間・負荷がある • 企業機密情報が保護されないリスクがある	• 機密情報を保護しつつ、法規制や顧客要求への対応に必要となる製品含有化学物質情報の効率的な授受手段の提供

代表機関	対象顧客	課題意識（ペイン）	本ユースケースで実現する顧客への提供価値
SBI HD	製品のサプライヤー	• 業界・業種横断で事業者・製品の信頼性の担保をしたいが、実態は模造品が流通している、第三者からの真正性が担保できていない状態	• 事業所の実在性を確認でき、第三者が検証可能なデジタル証明書を付与することで取引相手の信頼度を向上すること・出荷検査時に製品ロットに対して製造者の保証を追加すること
シミック	製薬会社、CRO・SMO・ARO 等の知見に関する機関の臨床事業部門	• 臨床試験、臨床研究のコスト削減と速度向上を図りたいが、関連システム・デバイスに多用なものがあり、ベンダー、プロダクトごとに技術基盤や操作方法がそれぞれ異なることから自社で包括的に整備することが困難	• 多用なウェアラブルデバイスに適用可能かつ、eConsent からウェアラブルデバイスデータの抽出までをシームレスに行うためのアプリ提供やコンサルティング提供により円滑な治験推進を支援
ORPHE	変形性膝関節症の患者/病院/研究機関	• 下肢運動器疾患の改善を図りたいが、患者日常データ利用の手間や、データ共有に不安があり進んでいない状態	• インセンティブのあるエコシステムの中で、歩行データを主とした患者データを安心/安全/簡易に共有できる仕組み
電通総研	法人確認業務を行う金融機関	• 取引開始や途上与信の際、相手先情報の取得と確認に時間と手間がかかる • デジタルでの信頼性確認に限界があり、窓口での対面対応が必要 • デジタル化が遅れており、ユーザリテラシーや環境整備が進んでいない	• KYC/KYB に基づいたトラストのある取引に必要となる真正性が担保された KYC・KYB VC 発行サービス
JISA	補助金事業の所管省庁の設計担当 補助金事業の事務局や事業管理機関等の運営責任者	• 事務局等の確認業務運用において、取得可能な情報の不足により、確認レベルの向上と対応負担の軽減の両立が困難 • 機械可読性のあるデータとして取得および提出可能な対象書類が限定的であり、自動照合等含む業務効率化に支障	• 「民間事業者同士のビジネス活動や行政手続き等の様々なコンテキスト」から生成されたデータの利活用の拡大により 、「行政手続き、特に補助金事業等の不適切利用の抑止、関連書類等のデジタル化促進」および「民間ビジネス環境へ寄与する可能性も念頭にした事業 KYC/KYB の DX」が継続的に進展し続ける姿の実現
OP CIP	インターネット利用者	• インターネット広告の信用度が低くアクセスしたくない、アクセスすると被害に遭う	• インターネット広告の健全性を向上させることで、生活者、広告主の双方に安心をもたらす
	インターネット広告利用企業	• アドフラウドやフェイクニュースによるブランドリスクの棄損	

1.5. 実証ユースケース実現時の経済効果

各種ユースケースで試算された経済効果・市場規模をその効果ごと(「A.リスク抑制」、「B.コスト削減」、「C.売上拡大」)に整理した。

「A.リスク抑制」では、サプライチェーンによる模造品リスクの抑制(みずほ R&T、SBI HD)行政手続きによる不正受給のリスク抑制(JISA)、アドフラウドによる被害リスクの抑制(OP CIP)が挙げられる。

「B.コスト削減」では、大学技術職員の効率的な配置(富士通 Japan)、サプライチェーンにかかる規制対応等にかかるコスト削減(みずほ R&T、SBI HD)、医療における治験等のデータ収集の効率化(シミック・ORPHE)、法人の口座開設・確認業務の手続き効率化(電通総研)、行政手続きの効率化(JISA)が挙げられる。

「C.売上拡大」では、オンラインコミュニケーション市場の活性化(DataSign)、高齢者向け共助サービス市場の活性化(DNP)、海外人材マッチング市場の活性化(IGS、PitPa)、医薬品開発の加速化による売上拡大(シミック・ORPHE)、が挙げられる。

代表機関	業界	経済効果・市場規模（事業者試算）	効果の分類		
			A. リスク抑制	B. コスト削減	C. 売上拡大
DataSign	個人	オンラインコミュニケーション市場の活性化による効果 （2028年に海外：5-6兆円、国内：約3,500億円）	–	–	✓
DNP		共助サービスの高齢者向け支援への浸透 （国内高齢者向け市場が101.3兆円に拡大すると予測され、その一部を獲得）	–	–	✓
IGS	個人（人材）	海外人材と国内企業との人材マッチングによる成功報酬の獲得 （2030年に、79万人のIT人材をマッチングする想定で約9,500億円）	–	–	✓
富士通Japan		技術職員の増員/効率的な人材配置、研究機関/企業間での優秀人材の流動の活性化	–	✓	–
PitPa		採用にかかるキャリア情報の流通促進で、海外人材の国内の労働市場呼び込み （2030年に国内労働市場は644万人の不足が予測され、その一部にアプローチ）	–	–	✓
みずほR&T	サプライチェーン	国内企業のサプライチェーン全体での製品含有化学物質管理に要するコスト削減 （年間約3,000億円のコストの約1/3が削減できると試算）、機密情報保護	✓	✓	–
SBI ホールディングス		サプライチェーンで流通する製品の規制への準拠・検証に要する時間とコストの低減、模造品の抑制（世界で年間約5,500億ドル相当の模造品が流通）	✓	✓	–
シミック	ヘルスケア	医薬品開発市場において臨床試験等における症例集積の速度向上とコスト削減 医薬品承認加速による売上拡大	–	✓	✓
ORPHE		分散型治験による低コスト化（物理的な試験施設・人件費の削減，データ収集と管理の効率化，治験参加者の対応簡素化）、医薬品承認加速による売上拡大	–	✓	✓
電通総研	法人・金融	法人の口座開設にかかる時間短縮・効率化、他法人確認業務の効率化 （令和3年度の国内法人数は約287万社であり、アプローチ対象となる）	–	✓	–
JISA	行政	行政手続き（補助金事業等）の不適切受給の抑制・効率化 準公共分野における手続きの効率化	✓	✓	–
OP 技術研究組合	メディア	広告主が意図しないウェブサイトに流れている広告費や、アドフラウド被害に遭った広告費の抑制（国内の広告詐欺に流れた広告費：約1300億円）	✓	–	–

図 4-2-1　Trusted Web 提供価値と事業者マッピング

1.6. 収益モデル

ユースケースに関連する主体を類型化した(図 4-3-1)。プレイヤは 6 つに類型化でき、証明書等をやり取りする「①発行者」、「②保有者」、「③検証者」、証明書のやり取り等ビジネスに関連するルール・ガバナンスを規定する「④業界団体/ガバナンス運営者」、証明書等をやり取りするサービス(ウォレット等)を提供する「⑤サービスプロバイダ（ウォレットプロバイダ）」、サービスプロバイダに SDK・API 等を提供する「⑥システムベンダ」に類型化を行った。なお、ユースケースによっては複数の役割を同一の主体で実施[6]することも確認された。

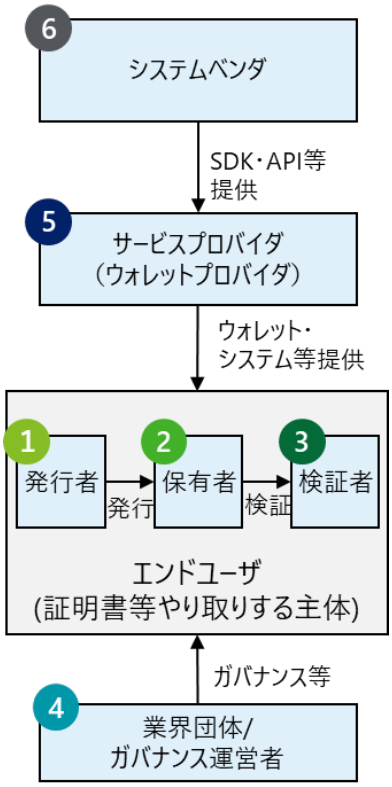

図 4-3-1　主なプレイヤの類型・役割

[6] 以下 3 つのユースケースでは、一つの主体が複数の役割を持つ
みずほ R&T における Chemical Management Platform は、サービスプロバイダであり業界団体/ガバナンス運営者である
SBI HD におけるデジタル認証機構は、発行者であり、サービスプロバイダである
OP CIP は、発行者であり、サービスプロバイダである

また、①~⑤のプレイヤから費用支払いが発生したため、収益源となる費用をどの主体からどの主体へ支払うか、支払いの対価を整理した(図 4-3-2)。

① 発行者からの支払い

- 証明書発行ができること・発行システムを利用できることを対価にサービスプロバイダへの支払いを想定している事例(DataSign、電通総研、みずほ R＆T)
- 直接サービスを提供はしないものの、そのシステムを提供したり、データ標準化を実施したりしたということを対価にシステムベンダへ支払いを想定している事例 (富士通 Japan)
- エコシステムガバナンス担保・参画を対価に業界団体/ガバナンス運営者へ支払いを想定している事例(DNP・みずほ R&T)

② 保有者からの支払い

- 信頼できる証明書を受け取ることができることを対価に発行者への支払いを想定している事例(SBI HD、電通総研、OP CIP)
- サービスを利用できること、秘密鍵/情報の管理を安全にできることを対価にサービスプロバイダへの支払いを想定している事例(DataSign、みずほ R&T、SBI HD、JISA、OP CIP)
- ガバナンスが担保されたエコシステムに参画できることを対価に業界団体/ガバナンス運営者への支払いを想定している事例(みずほ R&T)

③ 検証者からの支払い

- 信頼できる証明書を受け取ることができることを対価に発行者への支払いを想定している事例(SBI HD、OPCIP)
- 信頼できる証明書を受け取ることができること、検証を行った結果価値提供がされること等を対価にサービスプロバイダへの支払いを想定している事例(みずほ R&T、SBI HD、シミック、ORPHE、JISA、OP CIP、富士通 Japan、IGS)
- 検証を行った結果採用や共同業務等の価値提供がされることを対価に保有者への支払いを想定している事例(PitPa、富士通 Japan)
- 発行情報のガバナンス担保・エコシステム参画ができることを対価に業界団体/ガバナンス運営者への支払いを想定している事例(DNP、みずほ R&T)

④ 業界団体/ガバナンス運営者からの支払い

- エコシステムを円滑に循環すること（インセンティブ）を対価に業界団体/ガバナンス運営者への支払いを想定している事例(JISA)

⑤ サービスプロバイダからの支払い

- エコシステムを円滑に循環すること（インセンティブ）を対価に発行者や保有者への支払いを想定している事例(IGS、富士通 Japan、JISA、ORPHE)
- ガバナンスが担保されたエコシステムに参画できることを対価に業界団体/ガバナンス運営者への支払いを想定している事例(DNP、OP CIP)
- システム利用ができることを対価にシステムベンダへの支払いを想定している事例(富士通 Japan)

支払先	獲得する対価	該当UC
1 From 発行者		
サービスプロバイダ	• 証明書発行ができること・発行システムを利用できること	• **DataSign、電通総研** – 証明書発行サービス利用料 • **みずほR&T (Chemical Management Platform)** – システム・サービス利用料
システムベンダ	• 証明書発行ができること・発行システムを利用できること • データ標準化を実施したこと	• **富士通Japan** – スキル発行にかかるスキルカタログ／マップ整備サービス利用料
業界団体/ガバナンス運営者	• 発行情報のガバナンス担保・エコシステム参画できること	• **DNP (共助トラストエコシステム運営者)** – 事業者登録(トラストリスト)手数料 • **みずほR&T(Chemical Management Platform)** – コンソーシアム参加料
2 From 保有者		
発行者	• 信頼できる証明書を受け取ることができること	• **SBI HD (デジタル認証機構)、電通総研** – デジタル証明書の発行・審査・更新にかかる手数料 • **みずほR&T (Chemical Management Platform)、OP CIP** – システム・サービス利用料
サービスプロバイダ	• サービスを利用できること、秘密鍵/情報の管理を安全にできること	• **DataSign** – 秘密鍵管理にかかる手数料 • **SBI HD (デジタル認証機構) 、JISA、OP CIP** – システム・サービス利用料
業界団体/ガバナンス運営者	• ガバナンスが担保されたエコシステムに参画できること	• **みずほR&T(Chemical Management Platform)** – コンソーシアム参加料
3 From 検証者		
発行者	• 信頼できる証明書を受け取ることができること	• **SBI HD (デジタル認証機構)**[*2] – デジタル証明書の検証手数料 • **OP CIP**[*3] – システム・サービス利用料
サービスプロバイダ	• 信頼できる証明書を受け取ることができること • データ標準化を実施したこと • 検証を行った結果価値提供がされること	• **みずほR&T (Chemical Management Platform)**[*1]**、SBI HD (デジタル認証機構)**[*2]**、シミック、ORPHE、JISA(行政機関)、OP CIP**[*3] – システム・サービス利用料 • **富士通Japan (研究基盤協議会)** – スキルカタログ利用料・マッチングサービスの利用料 • **IGS** – 採用成功報酬にかかる支払い
保有者	• 検証を行った結果採用や共同業務等の価値提供がされること	• **PitPa (海外人材)** – (受入企業の検証を経て採用に至った場合)採用における対価支払い※採用仲介者含む • **富士通Japan (技術職員)** – (地域・大学等の検証を経て共同研究に至った場合)活動における対価支払い
業界団体/ガバナンス運営者	• 発行情報のガバナンス担保・エコシステム参画ができること	• **DNP (共助トラストエコシステム運営者)** – 事業者登録(トラストリスト)手数料 • **みずほR&T(Chemical Management Platform)**[*1] – コンソーシアム参加料
4 From 業界団体/ガバナンス運営者		
サービスプロバイダ	• エコシステムを円滑に循環すること（インセンティブ）	• **JISA (行政機関)** – 監督省庁から行政機関へ機能提供に関わる運用費用
5 From サービスプロバイダ		
発行者	• エコシステムを円滑に循環すること（インセンティブ）	• **IGS (教育機関)** – 証明書を発行した学生の採用成功時のインセンティブ支払 • **富士通Japan (大学)** – スキルカタログ／マップ作成にかかるインセンティブ支払 • **JISA (民間事業者等)** – 証明書発行にかかるインセンティブ支払
保有者		• **ORPHE** – 医療データ提供にかかるインセンティブ支払
業界団体/ガバナンス運営者	• ガバナンスが担保されたエコシステムに参画できること • システム利用ができること	• **DNP (共助トラストエコシステム運営者)、OP CIP (JIQDAQ)** – 事業者登録(トラストリスト)手数料
システムベンダ	• システム利用ができること	• **富士通Japan** – トラスト付与サービス利用料

図 4-3-2　収益モデル整理

1.7. プレイヤーマッピング

2022 年度の実証と 2023 年度の実証に参画した事業者等を整理した。

2023 年度実施された 12 ユースケースのうち、2022 年度から継続して参画した事業者は 7 社(DataSign、DNP、富士通 Japan、シミック、ORPHE、電通総研、JISA)、新規で参画した事業者は 5 社(IGS、PitPa、みずほ R&T、SBI HD、OP CIP)であった。

また、2022 年度と比較してサービスプロバイダの参画、業界団体/ガバナンス運営者の巻き込みが顕著に増えた。

サービスプロバイダでは、海外人材系(IGS、PitPa、フォースバレーコンシェルジュ [7])、金融系(アクシオン [8])、メディア系(OP CIP 等)の領域が新たに追加された。

業界団体/ガバナンス運営者の巻き込みでは、共助アプリ団体(DNP)、OWND Project(DataSign)、研究基盤協議会(富士通 Japan)、国内・海外政府を巻き込んだコミュニティ(PitPa)、PHR 推進協議会(シミック)、物質管理団体(みずほ R＆T)、認定機関(SBI HD)、認証機関(OP CIP)等の参画を検討した実証が実施された。業界団体/ガバナンス運営者の参画が増えたことで、社会実装に向けた取り組みがより加速したと言える。(ガバナンス・ルールの取組については 6 章で詳細で記載する。)

[7] フォースバレーコンシェルジュは PitPa のユースケース実証事業の参画企業である

[8] アクシオンは電通総研のユースケース実証事業の参画企業である

凡例　灰字：昨年度実証分野・事業者　緑字：昨年度実証から継続している分野・事業者　青字：今年度実証から新規の分野・事業者

図 4-4-1　プレイヤーマッピング

１.８. ビジネスモデル考察

【課題・提供価値訴求をステークホルダにわかりやすくする訴求することの必要性】

本事業では、各ユースケース実証事業者に対して、顧客の課題・提供価値の整理を行い、ステークホルダに実証事業への参画協力をいただいた。(各ユースケースの取組詳細は６.３. ステークホルダ協議・ヒアリング等実施概要参照)ただし、ヒアリング結果から事業者が想定した課題や価値がうまく参画者に訴求できなかったユースケースを確認できた(例えば、現在の業務・運用においてリスク抑制ができており、コスト削減も必要ない等が挙げられた)。その原因として、これらの取組に参画を検討しているステークホルダは現在運用されているエコシステムのリスクや、Trusted Web の世界観によるメリットが大きい等の便益をうまく認識できていないことが示唆された。今後多くの事業者に Trusted Web の具現化にかかる取組に参加いただくためには、各ユースケースで、ステークホルダが認知できる課題・提供価値の訴求を行っていくことや、場合によっては認知できるほどのインセンティブ(法規制等)を課していくことも考えられる。

【参加主体・責任が分散化されることを想定したビジネスモデルの設定】

2022 年度のユースケースと比較して、ガバナンス運営も想定したビジネスモデルが検討され、多くのユースケースで、エコシステムをガバナンスする業界団体/エコシステム運営者が関与する前提での検証が実施された。

また、社会実装を見越して多くのステークホルダーを巻き込んだ検証を行ったことで、ビジネスモデルの多様化・複雑化が見られた。この背景として、各ユースケースの主体がどの役割 (証明書等のデータ発行者/保有者/検証者、業界団体・ガバナンス運営者、サービスプロバイダ・システムベンダ) までを担うかについては、各ユースケースの課題の起点(その起点に対するインセンティブの有無)、業界慣習等によって異なることが考えられる。商用化・横展開のタイミングで今後より多くのステークホルダの巻き込みが行われることにより主体の役割やガバナンスの位置づけ等はより多様化・複雑化されることが想定される。(例えば、実証・初期商用化タイミングではサービスプロバイダとガバナンス運営を兼務していた主体がエコシステム拡大によってその役割を分散化すること等が考えられる)

Trusted Web の取組においては特定の事業者/サービスに依存しないでサービスを提供することが期待されており、その結果、エコシステムに関わる主体が多様かつその責務が分散化されること望まれる一方で、必ずしも分散化がビジネスモデル実現の成功要素にはならないことに留意する必要がある。例えば、参加主体ごとに役割を分散化し過ぎるとかえってステークホルダ調整等の負担増が想定されること、必ずしも分散化することがステークホルダのニーズにそぐわないケース(特定事業者に依拠することでエコシステムに簡単に参画できメリットを享受できる等)が考えられる。分散化が行き過ぎた結果中央集権的なプラットフォーマーがサービスを提供することが効率的で競争環境上優位となり、分散化されたエコシステムが不成立になるリスクがあることにも留意すべきである。

したがって、特定の事業者に依存しないことを価値にビジネスモデルを検討する際には、顧客ニーズ・コストも踏まえて主体の責務・役割の分散化・あるいは集権化の調整を行う必要がある。ビジネス優位性を超えて特定の事業者/サービスに依存しないことを重視していくためには、必要に応じて法整備・執行の観点から特定の事業者/サービスに依存しないでサービスを提供すること(各主体の役割の分散化)の意義を訴求していく必要がある。例えば EU で検討されている EU デジタルアイデンティティウォレットは、サービスのモデル上中央集権モデルの方が利便性が高いがデータ安全保障の観点で中央集権的なプラットフォーマー事業者の過度な関与を規制の中で抑制しており、取り組みとして参考になる。

【クロスボーダーのユースケース対応】

2023 年度ユースケース実証事業では、2022 年でにはない海外との連携があるユースケースが確認された。事れとしては人材系では、海外の学生・求職者との成績・職歴データのやり取りの事例（PitPa・IGS）、サプライチェーン関連では認証機関の相互承認の業務フィージビリティの検証（SBI HD）が該当する。ユースケースがクロスボーダーで適用される場合は、ガバナンス・ルールの整備も必要(６.５. ガバナンス・ビジネス普及に向けた取組考察も参照すること)であるが、整備に向けては政府間の協力が必要であり、本邦政府の各国の政府機関との調整が期待される。

実証事業整理（要件・アーキテクチャ実装）

1.9. 実装要件

1.9.1. Verify・データコントロールの考え方

各ユースケースのデータの検証方法・検証データの置き場所を分析し、データの管理形態の分析を行った。データの管理形態としては「分散的に管理」「一部分散的に管理」「不要」に類型化できた。

ここでの「分散的に管理」は証明書や証明書を検証する鍵(鍵の在りかを特定する識別子)等をデータ主体・データをやり取りしたい相手方・管理主体が存在しない/複数存在するブロックチェーン等で管理することを意味している。証明書・識別子ともに個人のウオレットで管理し、検証するときには相手方に直接渡す事例(DataSign、電通総研、JISA)、ブロックチェーン等をデータレジストリに活用して検証鍵を渡すケース(富士通 Japan、PitPa、ORPHE)、事前に相手方に検証鍵を渡しておいて証明書をやり取りするケース(SBI HD)が挙げられた。

「一部分散的に管理」は、証明書や、証明書を検証する鍵(鍵の在りかを特定する識別子)等を一部特定のクラウド事業者等で管理することを意味している。証明書情報や暗号化された情報を事業者が管理をして、復号・検証鍵等を個人やブロックチェーンで管理するケース(DNP、IGS、シミック)が挙げられた。

「不要」はその特性から証明書が他ステークホルダに公開されても問題ないことを意味している。OP CIP の事例ではガバナンス機関等からの認証結果を証明書として記録するが、その証明書自体は公開されても問題ないことから管理が不要という整理を行った。

No.	代表機関	検証方法 （署名検証・暗号された情報の復号化）	検証データの置き場所	データの管理形態
1	DataSign	• 検証可能な選択的開示（SD-JWT等）に対応した証明書の検証	証明書・識別子ともにユーザアイデンティティウォレットで管理	**分散的に個人で管理** （発行された証明書を自身のウォレットで管理）
2	DNP	• 検証可能な証明書の検証	証明書：ウォレット（クラウド環境） 識別子：データレジストリ（Hyperledger Indy）	**一部分散的に個人で管理** （証明書をクラウド環境下のウォレットで管理しユーザ自身がアクセス可能、識別子はデータレジストリに格納）
3	IGS	• 成績生データの暗号化 • 成績生データを暗号化した状態で秘密計算された成績スコアの暗号化	ブロックチェーン及びデータベース	**一部分散的に個人で管理** （成績生データは、暗号化、分割化しブロックチェーン及びデータベースに格納、暗号化した状態で秘密計算されたデータは事業者システムで管理）
4	富士通Japan	• 電子署名及び電子証明書検証 • eシール検証	Data e-TRUSTと接続するシステムのデータベース	**分散的に個人で管理** （IDYX内のWalletにて管理）
5	PitPa	• 検証可能な証明書の検証	証明書：Webサーバ 識別子：データレジストリ（ionネットワーク）	**分散的に個人で管理** （証明書をWebサーバ・識別子をビットコインレイヤ2のionネットワークで管理）
6	みずほR&T	• 検証可能な証明書の検証	プライベートブロックチェーン or クラウドストレージ or 各ステークホルダデータベースから選択予定（今後検討）	**今後検討**
7	SBI HD	• 相手方に公開鍵を渡しておいて秘密鍵で署名したVPを公開鍵活用して検証	証明書：自社のストレージ 公開鍵：相手方のストレージ	**分散的に法人で管理** （証明書と検証鍵は取引間で保持）
8	シミック	• 署名情報の検証	ユーザー情報：データストレージ（Box） 公開鍵：データレジストリ（Public Blockchain）	**一部分散的に個人で管理** （ユーザー情報はクラウドストレージに格納、識別子はデータレジストリに格納）
9	ORPHE	• 検証可能な選択的開示（SD-JWT等）に対応した証明書の検証	証明書：スマートフォン・IPFS 識別子：データレジストリ（Hyperledger Indy）	**分散的に個人で管理** （証明書をウォレット・IPFSで管理しユーザ自身がアクセス可能、識別子はデータレジストリに格納）
10	電通総研	• 検証可能な証明書の検証	証明書・識別子ともにユーザアイデンティティウォレットで管理	**分散的に法人で管理** （発行された証明書を自身のウォレットで管理）
11	JISA	• 検証可能な証明書の検証	データレジストリ（詳細は今後検討）	**分散的に法人で管理** （発行した証明書を自身のウォレットで管理）
12	OP CIP	• 検証可能な証明書の検証	メディアのサイトプロファイル内、広告HTML	**不要** （流通しても問題ないため）

図 5-1-1　検証方法と検証データの置き場・管理形態

１.９.２. 合意形成・トレースの考え方

各ユースケースの合意形成・トレースの考え方を整理した。2023 年度は、2022 年度と比較して第三者にトレースする情報を新たに追加した(図 5-1-4)

第三者への情報トレースは①ビジネスユースケース上上トレースが必要・望ましいものと、②ユースケース上は必要なく可能であればトレースを避けたいものに分類することができる。

① ビジネスユースケース上トレースが必要・望ましいもの

情報提供に同意した記録をトレースすることで紛争時の解決手段(ADR 等)に用いることを想定したユースケースが確認された(IGS、富士通 Japan、ORPHE、JISA)。また、証跡を残すこと自体が法規制・業界ルール上求められているユースケースを確認した(シミック)。また、個人の意思次第では証明書の内容を積極的に公開したい場合、トレースを妨げない事例を確認した(PitPa)

② ユースケース上は必要なく可能であればトレースを避けたいもの

合意形成やトレースの仕組み上、意図せずにメタな情報からプライバシーな情報・機密情報が類推されてしまうこと・セキュリティ上の問題から情報が漏洩してしまうリスクが生じる可能性がある。SD-JWT 等の証明書を活用すると、署名値が同じことから Verifier が結託すると証明書を保有する個人の情報が類推できてしまう可能性(DataSign)、データ共有へ同意した記録からその個人が有疾患と類推できていしまう可能性(ORPHE)を取り上げた事業者を確認した。また、有識者からは、製品情報等の機密情報は秘匿しながら取引を行っている事実のみをトレースできたとしても、当事者間ビジネス関係は明らかになってしまうことからこれが機密な情報当たる可能性があるのではないかという指摘を受けた。

このように第三者へトレースする情報の仕組み作りは、紛争時の解決手段を高めること（公平性・透明性）とプライバシー・機密情報の保護の両観点で留意する必要があり、ユースケースのエコシステム内でその便益とリスクを合意して進めていく必要がある。

No.	代表機関	合意の主体	合意の対象	合意の取消	トレースの対象	トレースの方法
1	DataSign	証明書発行者と証明書保有者の間	属性情報・資格情報の取得	可能 （Walletからクレデンシャルの削除）	履行された左記の合意	Wallet内の証明書として照会
		エンドユーザーとOWND Messenger	属性・資格情報の証明	可能	履行された左記の合意	メッセージアプリの画面にて照会
		エンドユーザーとエンドユーザー	メッセージング所属証明	一度相手に送信されたメッセージを削除することは不可	履行された左記の合意	メッセージアプリの画面にて照会
2	DNP	共助アプリ（発行者）と共助アプリサポーター（保有者）	サポーターが実施した共助実績情報（VC）	可能 （Hyperledger Ariesのrevocation機能によりVCを無効化）	履行された事実	VC発行システム・ウォレットのログ確認
		共助アプリサポーターと共助アプリ（検証者）	サポーターが実施した共助実績情報（VP）	不可	履行された事実	ウォレット・VP検証システムのログ確認
3	IGS	転職者と企業 （マッチングシステム）	能力データの提供	可能	能力データ	システムログ、DB格納方法で判断
		転職者と企業	企業とのチャット開始の同意	可能	チャット利用への同意	システムログ
4	富士通Japan	データ提供者（技術職員）とトラストアンカー（所属大学）	スキル・活動に関する実績及び評価の内容	可能 データ提供者（技術職員）が合意取消を申告する	履行された左記の合意	ブロックチェーンによるレジストリにて照会
5	PitPa	外国人労働者と育成機関や受入機関	日本語能力および受入機関における職歴証明書の完全性と有効性、発行者の真正性	可能 取り消しはIssuer（受入機関 / 育成機関）のみが証明書発行システムから行えるものとする。	日本語能力および受入機関における職歴証明書の完全性と有効性、発行者の真正性	育成機関や受入機関がシステムを通して証明書を発行した際に、サービスプロバイダーのサーバー（本実証ではPitPa）に証跡を保持する。
6	みずほR&T	サプライチェーン上のB2B間	物質リスト 調査依頼・回答データ	可能	履行された左記の合意	スマートコントラクト等の共通アプリケーションにより照合

図 5-1-2　合意形成・トレースの考え方(1/2)

No.	代表機関	合意の主体	合意の対象	合意の取消	トレースの対象	トレースの方法
7	SBI HD	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	契約書等のアナログ運用のもと、合意取消が可能	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）
		デジタル認証機（Issuer）と事業所（Holder）/ 事業所（Holder）と事業所（Verifier）	事業所（Holder）の実在性	契約書等のアナログ運用のもと、合意取消が可能	履行された左記の合意	事業所（VC）
8	シミック	患者と被験者/ 医療機関スタッフ製薬企業とCROスタッフ	同意取得～ウェアラブルデバイスの利活用までのシームレスな管理、データの共有、統合制御	可能	Pairingの実施 臨床試験等への参加同意	公開鍵暗号方式による暗号化・署名/復号化・署名の検証
9	ORPHE	患者・医師と」理学療法士/ 患者・研究機関と製薬企業	患者情報・データの共有	可能	履行された左記の合意	ブロックチェーンによるレジストリにて照会
10	電通総研	①所有者（口座開設法人/法人担当者）と発行者（KYC/KYB、所属確認VC発行機関） ②所有者と発行者・検証者（金融機関での口座VC発行）	① 法人口座開設におけるKYC/KYB・所属確認 ② 口座開設	VCの発行取り消し（ステータスリスト）で行う	VC発行・提示・検証にまつわるリクエストとレスポンスの全てがトレースされている	メッセージのリクエストとレスポンスの全てを保存する
11	JISA	民間事業者等の発行者と、補助金等を申請する事業者	当該事業者自身の情報を当該事業者からの依頼に基づき発行する事/ 発行データの管理責任は発行者にはない事の合意	–	履行された左記の同意	発行者の発行サービス機能における同意管理の証跡
		補助金等を申請する事業者と、補助金事業等の事務局等および所管省庁	申請情報の目的外利用の禁止（審査や交付に関係する事務連絡、通知、調査等。例外規定あり）	–	–	–
12	OP CIP	広告主とメディア（を代理するDSPとSSP）	表示する広告と価格など	不可能 （広告取引は表示まで瞬時に行われ合意取消にはそぐわない）	なし（相手のOP IDや落札価格のログは残るが第三者検証/トレース可能データとはしない）	–

図 5-1-3　合意形成・トレースの考え方(2/2)

No.	代表機関	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
1	DataSign	クレデンシャル	JWT形式のクレデンシャルより、発行者の署名でJWTを生成	JWT_VC_JSON、SD-JWTともにLinkabilityが発生し、verifierの結託するとクレデンシャルの持ち主が同一人物だと判明する
2	DNP	–		
3	IGS	転職者が企業に能力データを共有・チャットのやり取りに同意した記録	データ共有した記録・同意した記録をログとして管理	第三者が確認できるのは、提供に同意した事実のみ
4	富士通Japan	スキルマップ生成プロセス/マッチング関連プロセス	Data e-TRUSTの監査機能	機密情報へのアクセスを制限し、第三者には必要最小限の情報だけを提供する。改ざん不可能なように参照のみとする
5	PitPa	日本語能力証明書と職歴証明書	保有者のみに対して、各証明書に対して公開設定（ON/OFFのみ）の機能を提供、保有者が公開設定を変更した場合、サービスプロバイダのサーバ（本実証ではPitPa）に証跡を保持	日本語能力証明書と職歴証明書の情報を、保有者はVerifiable Presentationの形式で第三者に情報を公開（保有者の意思で開示するのでリスクなし）
6	みずほR&T	–	–	–
7	SBI HD	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）	第三者が、事業所（VC）の内容を確認できるリスクあり 取引相手は各自「暗号化用の公開鍵」を準備し、先方に事業所（VC）の提示依頼する際、自身の暗号化用の公開鍵を先方に提示する。先方は、受け取った暗号化用の公開鍵を使って、自身の事業所（VC）を暗号化して当方に渡すことで、当方の秘密鍵でのみ先方の事業所（VC）を復号化し内容を確認できるようにすることで対応
8	シミック	本ユースケース外の第三者による監査としての確認の位置づけであれば発生しない（臨床試験等の実施上のプロセスにおいて通常発生する監査）		
9	ORPHE	患者が他者へ自身のデータ共有することへの同意の記録	データ共有した記録をログとしてIPFSに管理	第三者がデータリクエスト者とリクエストへ回答したことがわかるため、今回のサービスケースにおいては、ユーザ（患者）が有疾患であることがわかる可能性がある
10	電通総研	システムで情報は保持しているが、第三者に情報開示を行うかどうかは別途業界での合意に基づくと考える		
11	JISA	当該事業者自身の情報を当該事業者からの依頼に基づき、約款同意の上で発行する事に合意した同意の記録	発行時の、発行者側サービス機能における同意管理の証跡	データ内容自体ではない為、リスクは低い
12	OP CIP	–		

図 5-1-4　合意形成・トレースの考え方(第三者にトレースされる情報)

1.10. 実装規格・アーキテクチャ – 比較整理対象

本実証では、各ユースケースで採用している規格・アーキテクチャの整理を実施した。整理の枠組みとしてはDIFの「interoperability-mapping-exercise[9]」を採用した。

技術規格動向を踏まえて一定程度技術仕様が固まりつつある技術規格(Credential Format、Credential Proofing、Envelope、Transport)を中心に比較整理対象とした（加えて参考として、Key Operations (秘密鍵管理)・Anchor Types (公開鍵の連携方法)の比較を行った）。本番商用化においておいて各ユースケースでの実装規格やアーキテクチャは変更になる可能性があることに留意する必要がある。また、下記図で取り上げられている規格の動向・概要については別資料[10]を参考されたい。

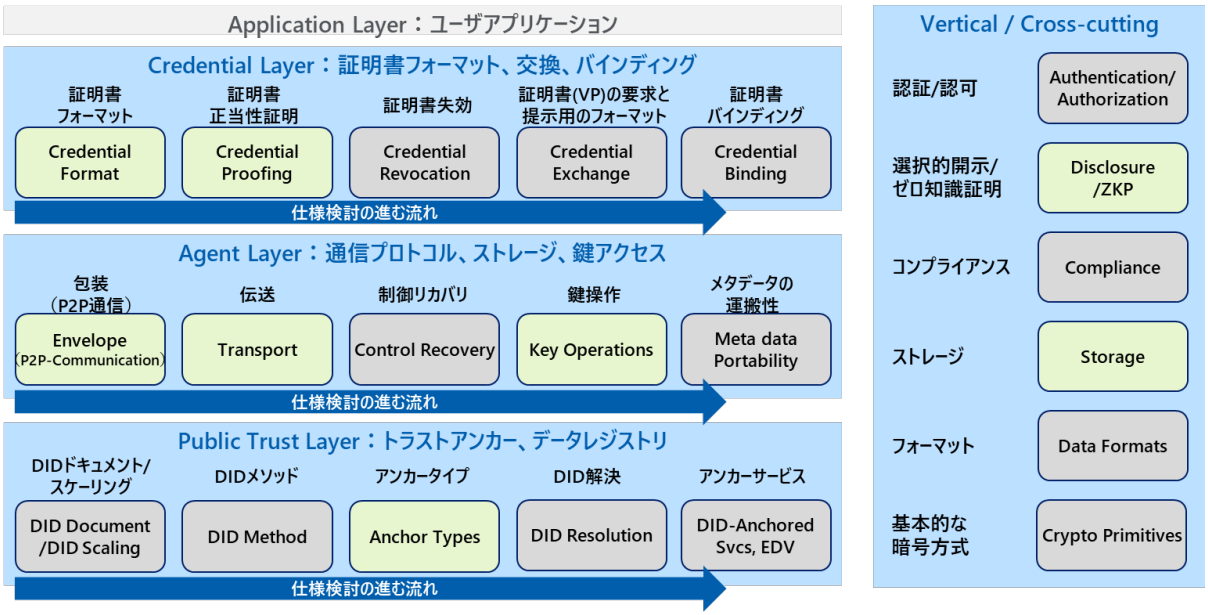

図 5-2-1　実装規格・アーキテクチャの比較整理

1.10.1. 実装規格・アーキテクチャ - Credential Layer

（1） Credential Format

Credential Format は検証可能な資格情報のデータモデルを定義している。各ユースケースで採用した資格情報のデータモデルの規格を下図にマッピングした。

※富士通 Japan、みずほ R&T、JISA は実装を行っていない。（次年度以降検討）、IGS は証明書を活用した実装を行っていないため、図には含まれていない

X.509 形式の証明書を活用した事例として DataSign、SBI HD が挙げられた。DataSign、SBI HD は証明書を発行する事業者の真正性を高めるために X.509 形式の証明書形式を採用している。

(広義の)Verifiable Credentials(VC)を活用している事例として W3C VC（PitPa、SBI HD）、OID4VCI/VP（DataSign、DNP[11]、電通総研）、Aries RFC(DNP[11]、ORPHE)、独自実装(シミック、OP CIP)が挙げられた。

---

[9] Decentralized Identity Foundation. “interoperability-mapping-exercise-10-12-20.pdf.” https://github.com/decentralized-identity/interoperability/blob/master/assets/interoperability-mapping-exercise-10-12-20.pdf

[10]令和 4 年度補正 Trusted Web 開発等推進事業に係る調査研究（規格・実装動向調査）

[11] DNP は相互運用性テスト用のウォレットを OID4VCI/VP、ユースケースの実証事業用のウォレットを Aries RFC で実装している

VC は、主に証明書の保有者のデータコントロールを柔軟にするために採用されている。

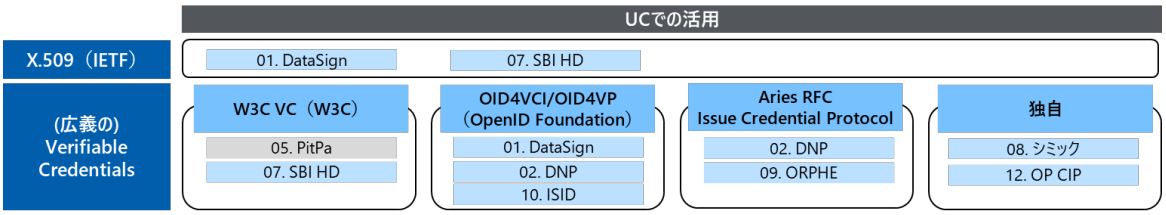

図 5-2-2　各ユースケースで採用した Credential Format 規格

（２） Credential Proofing / Selective Disclosure (ZKP)

Credential Proofing は、証明書の正当性を示すデータ形式を定義している。また、選択的属性開示とも関連が深く、セットで検討されることが多いため、各ユースケースで採用した Credential Proofing の規格と選択手的属性開示の手法を下図にまとめた。

※富士通 Japan、みずほ R&T、JISA は実装を行っていない。（次年度以降検討）、IGS は証明書を活用した実装を行っていないため、図には含まれていない

JWT-VC の活用が 2 件(DataSign[12]、OP CIP)、SD-JWT VC の活用が 3 件(DataSign[12]、DNP[13]、電通総研)、LDP-VC の活用が 2 件(PitPa、SBI HD)、AnonCreds の活用が 2 件(DNP[13]、ORPHE)確認された。

選択的属性開示については、SD-JWT を活用して提示するデータの最小化を行った事例を 3 件、ゼロ知識証明等を活用した事例を 2 件確認した。選択的属性開示の手法として LDP-VC-BBS+署名(ゼロ知識証明)を活用した事例も有名でありいくつかの事業者が実装検討を行ったが、今回工数・期間の制約で実装されることはなかった。選択的属性開示の手法は複数あるが、実装手法によってメリット・デメリットがあるためその詳細は別資料 [10] を参考とされたい。

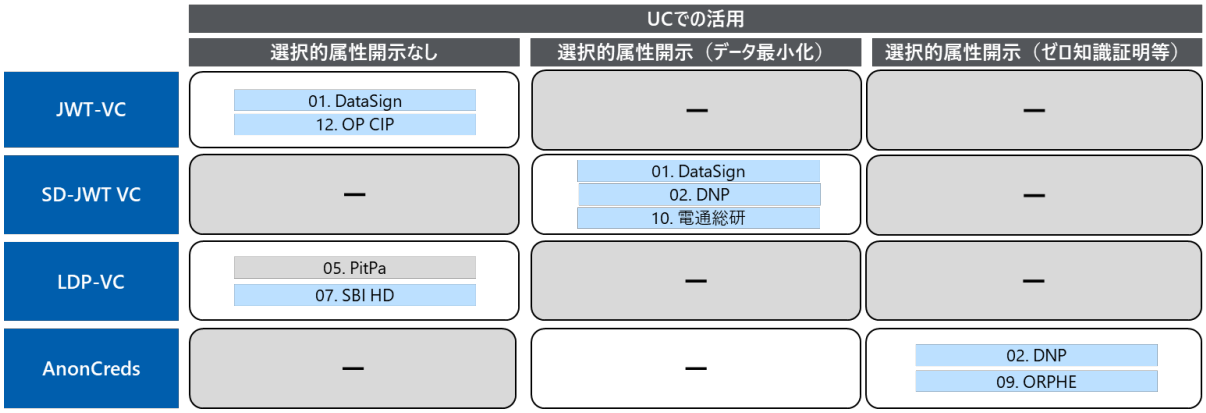

図 5-2-3　各ユースケースで採用した Credential Proofing / Selective Disclosure (ZKP)規格

[12] DataSign は実証事業内で 2 つの Credential Proofing の実装を検討した

[13] DNP は相互運用性テスト用のウォレットを SD-JWT VC、ユースケースの実証事業用のウォレットを AnonCreds で実装している

1.10.2. 実装規格・アーキテクチャ - Agent Layer

（1） Envelop（P2P-Communication）

Envelop（P2P-Communication）は、エージェント間で証明書を連携する際の通信プロトコル、エンコード方式等を定義している。各ユースケースで採用した Enveolp の規格を下図にまとめた。

※富士通 Japan、みずほ R&T、JISA は実装を行っていない。（次年度以降検討）、IGS は証明書を活用した実装を行っていないため、図には含まれていない

規格によらない独自実装を行っているユースケースを 5 件確認した。また、標準化が進んでいる規格を採用している事例として DIDComm Message v2 がを 2 件(DNP[14]、ORPHE)、SIOP v 2 を 3 件(DataSign、DNP[14]、電通総研)確認した。

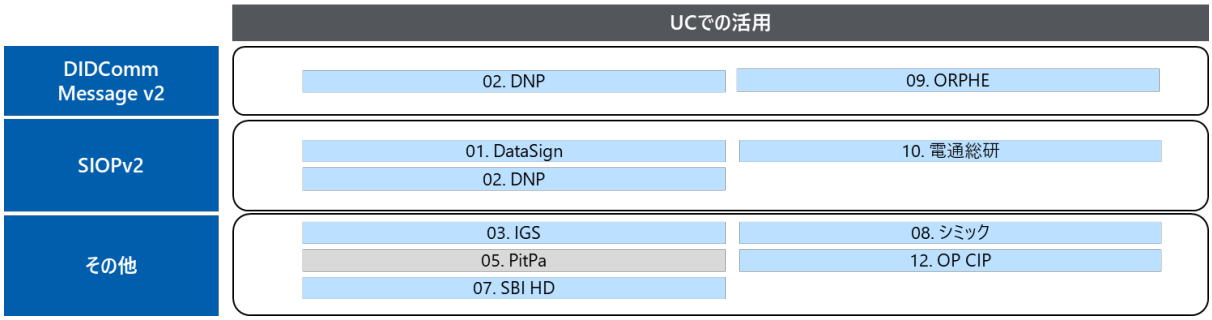

図 5-2-4　各ユースケースで採用した Envelop 規格

（2） Envelope（P2P-Communication）

異なるデバイス間で証明書やアイデンティティ情報の格納先などを連携する方法を定義している。各ユースケースにおけるデバイス間でのデータ交換方法を下図にまとめた。

※富士通 Japan、みずほ R&T、JISA は実装を行っていない。（次年度以降検討）、IGS は証明書を活用した実装を行っていないため、図には含まれていない

複数デバイスでのデータ交換で QR コードを用いるユースケースが 5 件(DataSign、DNP、PitPa、ORPHE、電通総研)あった。NFC を用いたデータ交換は見られなかった。

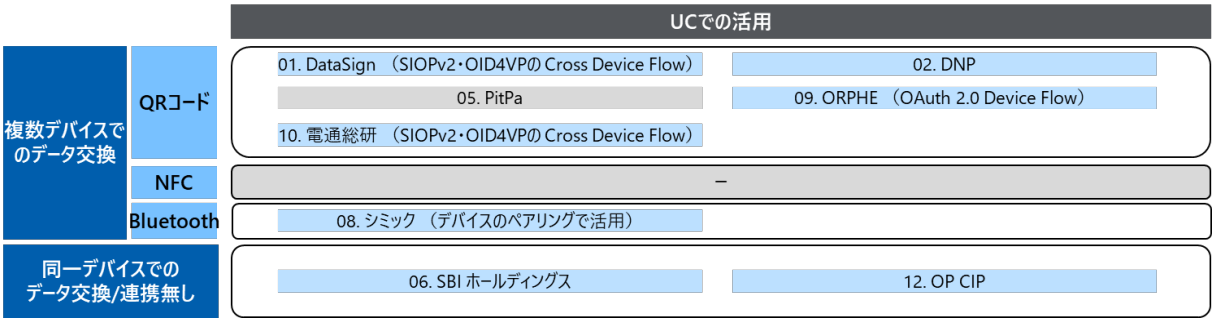

図 5-2-5　各ユースケースで採用した Transport 規格

[14] DNP は相互運用性テスト用のウォレットを SIOPv2、ユースケースの実証事業用のウォレットを DIDComm で実装している

１.１０.３. 実装規格・アーキテクチャ - 秘密鍵管理 / 公開鍵の連携

各ユースケースにおける秘密鍵（署名・暗号鍵）の管理方法と公開鍵（検証・復号鍵）の連携方法を下表にまとめた。

※富士通 Japan、みずほ R&T、JISA は実装を行っていない。（次年度以降検討）

秘密鍵の管理方法では、スマホ端末等のデバイスで管理する事例が 3 件(DataSign、シミック、ORPHE)、カストディサービスやクラウドインフラサービス等を活用してクラウドで管理する事例が 4 件(DNP、IGS、PitPa、SBI HD)確認された。電通総研はスマートコントラクトを活用した分散管理(ICP Threshold ECDSA Signature)、OP CIP は事業者によって端末/クラウド管理を選択できるケースだった。

秘密鍵の管理方法は、大きく①デバイス管理、②クラウド管理、③分散管理に分類することができるが、それぞれメリット/デメリットがある。秘密鍵管理・鍵紛失時の復旧方法等の鍵運用プロセスについて、現時点では通説的な解が確立されていないため引き続き規格・実装団体での議論が期待される。

公開鍵の連携方法については、①P2P 通信によって直接相手方と連携する方法を 4 件、②公開鍵(あるいは DID ドキュメント等公開鍵に紐づく情報)をデータレジストリに格納して相手方にアクセスしてもらって連携する方法を 5 件確認した。2022 年度は 13 件中 13 件が DID・データレジストリを活用した実証だったため、2023 年度ではその割合が減少した。データレジストリとして、Web サーバ、プライベートブロックチェーン、パブリックブロックチェーンの活用が確認された。

A類型 B類型

No.	代表機関	秘密鍵（署名・暗号鍵）管理	公開鍵（検証・復号鍵）の連携方法
1	DataSign	**端末管理** • Holder の秘密鍵をSecure Enclaves, Android Key Storeでスマホのセキュア領域内で鍵管理	**P2P通信による連携** • HolderからVerifierと直接公開鍵にやり取り • VerifierからIssuerに証明書の真正性を確認
2	DNP	**クラウド管理** • クラウドウォレットを活用した鍵管理	**データレジストリの活用（Private Blockchain）** • Hyperledger Indyを活用してVerifierがIssuerとHolderのDID Documentを取得して検証
3	IGS	**クラウド管理** • プロセシングシステム・マッチングシステムを管理する事業者のクラウドストレージで管理	**P2P通信による連携** • マッチングにかかるデータ（秘密計算済）について、事前に公開鍵をやり取りしておき相手方の公開鍵を活用して暗号化し、自身の秘密鍵で復号化を実施 • マッチングの元となる個人の成績データは**Polygonと、IPFS or RDB**を活用して転職者の個人情報や学習履歴などを暗号化して格納し、秘密計算を実施
4	富士通Japan	–	–
5	PitPa	**クラウド管理** • Crypto Garage のカストディサービスを活用して秘密鍵を管理	**データレジストリの活用（Public Blockchain/Webサーバ）** • HolderのDID Documentをion network、IssuerのDID DocumentをWebサーバから取得して検証
6	みずほR&T	–	–
7	SBI HD	**クラウド管理** • AWS Secrets Managerを活用して秘密鍵を管理	**P2P通信による連携** • HolderからVerifierが事前に公開鍵をやり取りし、相手方の公開鍵を活用して暗号化した情報を相手に渡して相手方の秘密鍵で復号化 • 失効確認はVerifierがIssuerに対して失効管理APIを活用して確認 （失効情報はCordaを活用して連携）
8	シミック	**端末管理** • スマホ端末・ウェアラブル端末で秘密鍵を管理	**データレジストリの活用（Public Blockchain）** • Public Blockchainに公開鍵を格納、Pairing時（同意プロセス後）にPublic Blockchainから相手方の公開鍵を取得して署名
9	ORPHE	**端末管理** • スマホ端末（Woolletアプリ）で秘密鍵を管理	**データレジストリの活用（Private Blockchain）** • Hyperledger Indyを活用してVerifierがIssuerとHolderのDID Documentを取得して検証
10	電通総研	**スマートコントラクト等を活用した管理** • ICP Threshold ECDSA Signatureを活用して秘密鍵を分散管理	**P2P通信による連携** • HolderからVerifierと直接公開鍵にやり取り
11	JISA	–	–
12	OP CIP	**端末/クラウド管理** • 広告主またはDSP事業者等が自身のDPレジストリサーバで管理	**データレジストリの活用（Originator Profileレジストリサーバ）** • VerifierからURL経由で公開鍵を取得して検証

図 5-2-6　各ユースケースにおける秘密鍵管理と公開鍵連携方法

１.１１. 実装要件、実装規格・アーキテクチャ考察

【Verify・データコントロールの考え方】

昨年度は全てのユースケースで DID を活用して、DID をデータレジストリ（ブロックチェーン等）に格納する方式だったが、今年度は DID 非活用の事例が増えた。

要因としては、EU デジタルアイデンティティウォレット（以下、EUDIW）で公開された EU Architecture Reference Framework（以下、EU ARF）や、OpenID Foundation（以下、OIDF）の VC に関連する技術仕様の普及で、DID を活用する必要性がないケースが浸透したことが挙げられる。また、デジタル庁でリリースした新型コロナウイルスワクチン接種証明書も VC は活用しているが DID は活用していないため、そのような国内事例が普及したことも要因として挙げられる。

ユースケース実証の中で、公的機関が発行・管理している情報を資格証明書として発行・検証できるスキームを採用する事業者が実証の過程で見られたが、関係省庁との調整の中で、発行・検証スキームの再検討を行ったうえで実証を進めた。

公的機関が発行する書類の情報活用は、関係省庁の法規制を十分に確認したうえで、情報の取扱いに留意すべきであると考える。また、特定サービスを受けるための個人・事業者の確認方法として、VC で記録された情報の検証をもって身元確認・法人実在性確認を行うことは技術上可能であるが法令上可能であるとは言えない可能性が高い。身元確認・法人実在性確認における VC 等の検証利用については今後関係省庁との議論が期待される。

【合意形成・トレース、第三者の監査に対する考え方】

合意形成・トレースの実装は各ユースケースで何の責任説明が必要であるかによってトレース情報や公開範囲が異なるが、多くの事業者で当事者間がやり取りした事実をログとして記録することを採用した。

事業者と当事者間でやり取りした事実を公開する場合、やり取りした記録から類推できる事項（当事者間にビジネス関係が存在すること、ユーザが他サービスを利用していること等）から機密情報や個人のプライバシー保護が棄損されるリスクがあることから、情報トレースの設計を行う際は十分に留意する必要がある。（例えば、Pairwise な ID と公開鍵の生成を行い、当事者間のやり取りした記録を他者から類推できないようにすること等が挙げられる。）

【規格動向との関連 – 実装が定まりつつある領域】

証明書フォーマットについて、OIDF が OID4VCI/OID4VP を仕様化したことで、証明書の検証モデルにおいて一定程度相互運用性を確保した実装が可能となり、複数の事業者で OID4VCI/OID4VP を実装、相互運用性のテストを実施した。

証明書のフォーマット・選択的属性開示の実装方式は今年度標準化団体の成果が一定あったこともあり、仕様が固定化しつつあることが実証からも確認できた（大きく SD-JWT / JSON-LD（BBS+署名）/AnonCreds（CL 署名 or BBS+署名）の活用が挙げられる）。今後これらの方式の収束がより進んでいくと想定される。

ゼロ知識証明の実装は、前項で述べた当事者間のやり取りした記録を他者から類推できないようにすること（Unlinkability の確保）おいて一定有用な案となるが現時点では OSS の普及が十分できていないこと等から本実証では実装できた事例は少なく、今後より社会実装を見越した普及が期待される。

証明書の検証においては、選択的属性開示が不要なのもので真正性を検証するものとしては従来の証明書方式（X.509 PKI）も活用が見られた。主に発行者側の真正性担保・失効管理を行うものとしての活用が期待される。

通信プロトコル・デバイス連携については、OIDF が策定している仕様（SIOPv2、OID4VP 等）の規格化が進んだことにより、実装方法が OIDF 系の利用と従来から規格化されている DIDComm （DIF、Hyperledger Project で主に検討）の仕様に二分されている。

【規格動向との関連 – 実装が未確定の領域】

証明書失効管理・ライフサイクルマネジメントは、現時点で技術仕様が固まっていないので引き続き規格の動向を注視する必要がある。また、社会実装を行うためには各ユースケースでポリシーを策定する必要がある。

ウォレットの鍵管理の実現方式については、クラウド管理・ハードウェアのセキュリティ領域の管理やスマートコントラクトを活用して秘密鍵を分割して管理する事例が確認された。

鍵の復旧方法や鍵の管理方式はデバイス各種の標準的な技術仕様含めて引き続き規格の動向を注視する必要がある。

データレジストリ・データベースの選定については、公開鍵の連携方法として DID Document/データレジストリを活用する方式だけでなく、DID を活用しない事例・P2P でやり取りする事例が確認された。

各ユースケースの特性にもよるが、ある程度利用用途が限定されているエコシステムであれば、P2P で公開鍵をやり取りすることで十分であり DID やデータレジストリを活用しなくても成立するため、上記の事例が昨年度と比較して増加したと想定される。ただし、エコシステムを跨いだ相互運用性の確保が本格化したタイミングで、DID を活用したスキームやデータレジストリとしてブロックチェーン活用可否の議論が増えてくる可能性がある。

加えて、個人情報保護・相互運用性確保の観点でデータレジストリとして何を選択すべきか（データベース・IPFS・ブロックチェーン）、did メソッドの選定は引き続き規格の動向を注視する必要がある。

実証事業 - ガバナンス・ビジネス普及に向けた取組

1.1 2. 取組類型整理

ガバナンス・ビジネス普及に向けた取組の全体像を下図に示す。

本実証事業では、ガバナンス・ルール策定に向けた取組を実施した。ガバナンス・ルール策定の取組に向けては①ステークホルダ内部での検証・協議、②外部団体の取組・規制等をベンチマークとした調査・分析を実施した。

また、社会実装・商用化に向けては策定されたガバナンス・ルールが、Trusted Web 推進協議会で策定を進めている Trusted Web ホワイトペーパーVer.3.0 等と整合性が取れていることや、各ユースケースで構築されたサービス・システムに対して実効性をもって適用されることが望ましい。本実証で策定されたガバナンス・ルールは有識者との協議やプロトタイプシステムを活用した検証を継続的に実施することでブラッシュアップされていくことが期待される。

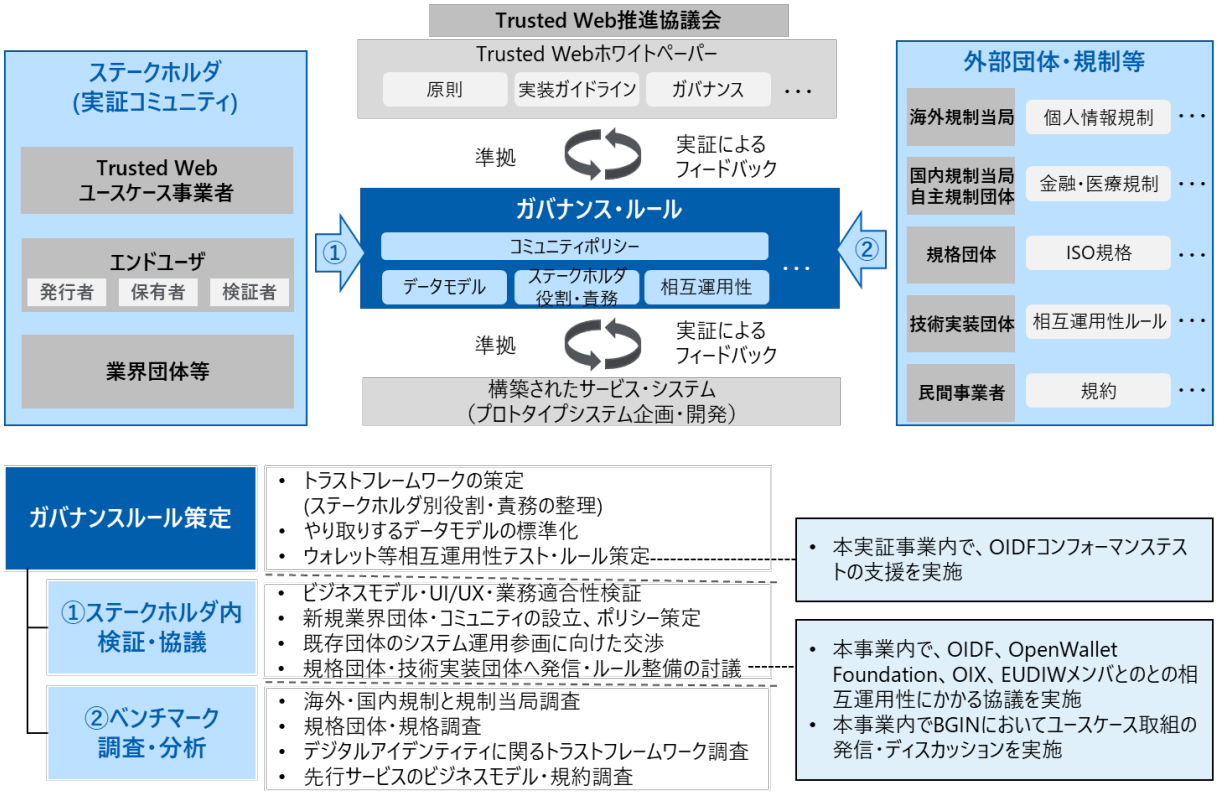

図 6-1-1　取組類型の整理

１.１３. ガバナンス・ルール策定実施概要

各ユースケースのガバナンス策定概要と検討主体を整理した。ガバナンス・ルール(案)の策定を行ったユースケースを 7 件(DataSign、DNP、IGS、PitPa、みずほ R&T、SBI HD、OP CIP)確認した。また他の事業者(富士通 Japan、シミック、ORPHE、電通総研、JISA)も、ガバナンス・ルールにかかる論点や必要性を提示した。

また、策定主体について、業界団体・開発コミュニティが主体となって策定したユースケースが 3 件（DataSign、みずほ R＆T、OP CIP）を確認した。他 9 件のユースケースにおいても、業界団体を巻き込んだガバナンス・ルール策定の取り組みはなかったものの、実施実証コミュニティの中でルール形成にかかる活動や、今後業界団体等との連携を見越した取組を進めた。ガバナンス・ルール策定においては、既存の業界団体との調整が必要な領域（サプライチェーン・大学・ヘルスケア・金融・行政手続き等）は、ステークホルダの合意合意形成に時間を要すことが示唆される。また、ルール策定主体としては特定の一事業者で策定するのではなく、業界団体を設立・既存の業界団体等を巻き込むことが必要であると示唆される。

その他に、サービスで活用するデータモデルの標準化(IGS、富士通 Japan)や、ウォレット等の相互運用性テストを実施したユースケースを確認した。本実証は、OIDF Japan と協力して OIDF 関連の規格に準拠したテスト[15]を実施した。

[15]本事業では、OpenID for Verifiable Presentations の仕様が適切に実装されているかテストを実施した
https://openid.net/certification/conformance-testing-for-openid-for-verifiable-presentations/

表 6-2-1　ガバナンス・ルール策定実施概要

No.	代表機関	策定概要	本実証でのガバナンス・ルール策定・検討主体
1	DataSign	• ガバナンスのあり方やビジネスモデル策定を目的にホワイトペーパーを策定 （ビジョン・ミッション・コアバリュー、課題・提供価値、ガバナンス構造、技術アーキテクチャ、ビジネスモデル検討等を記載） • OIDF のコンフォーマンステスト参加	• OWND Project （DataSign が主となって立ち上げたオープンソースコミュニティ）
2	DNP	• Open Identity Exchange を参考に共助トラストフレームワークを策定 （通信プロトコル・標準規格管理方針、プライバシーポリシー、証明書発行・検証方針、データスキーマ管理、証明書有効期限・失効管理の方針、エコシステム参加者に関する方針、ユーザーに関する方針、Wallet に関するポリシー等を記載） • OIDF コンフォーマンステスト参加 • 海外共助アプリとの相互運用性テスト実施	• DNP （今後共助アプリを活用する団体（共助トラストコンソーシアム）で運営する想定）
3	IGS	• 「国際間の教育拡充と労働市場の流動性を高める信頼ネットワーク」の利用にかかるガバナンス・ルール案を作成 （求職者のデータプライバシー・個人情報の取扱い、ステークホルダごとの役割、やり取りするデータ標準、国際間での採用マッチングにかかるルール等を記載） • ESCO 基準のデータモデルを採用マッチング向けに標準化	• IGS の実証コミュニティ （教育機関・転職先企業・政府機関）
4	富士通 Japan	• 各種証明にかかるプロセスと各主体の役割を明確化 （人・組織の実存証明、スキル情報の証明、資格情報の証明、実績情報の証明、マッチングにかかる証明） • 技術職員のスキルカタログの標準化	• 富士通 Japan （今後共助トラストコンソーシアム研究基盤協議会・研究基盤協議会に所属する大学・富士通を中心とするメンバで詳細検討）
5	PitPa	• Open Identity Exchange を参考に外国人材市場における外国人材採用推進コミュニティに対するガバナンス・ルール（ドラフト版）を策定	• PitPa （今後外国人材採用推進コミュニティを設立し、その中で策定予定）
6	みずほ R&T	• 既存の製品含有化学物質情報伝達スキームである IMDS や chemSHERPA のルールを参考に Chemical Management Platform タスクフォース内で、CMP 利用ルール（案）を整備 （製品含有化学物質管理体制の構築、製品含有化学物質情報、製品含有化学物質情報伝達、化学品・成型品の製品含有化学物質情報伝達にかかるルール等を記載）	• Chemical Management Platform コンソーシアム

No.	代表機関	策定概要	本実証でのガバナンス・ルール策定・検討主体
7	SBI HD	• 国内にある既存のトラストサービス（e シール等）を参考に事業所（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・ルール案を作成 （Issuer のルール、Issuer の適格認定、デジタル証明の国際間の利用、サービスプロバイダ―の共通要件等を記載）	• SBI HD （インターネット協会 OIC BRP コンソーシアム、沖縄オープンラボラトリ Trusted Network プロジェクトと連携）
8	シミック	• 上市されているデバイスのウェアラブルデバイスへの DID 実装可否リストの作成 • PHR サービス事業協会との連携し、日常診療や臨床試験等におけるウェアラブルデバイス等の PHR 利活用のためのあるべきガバナンスやルールについて今後策定予定	• シミック （PHR サービス事業協会と連携）
9	ORPHE	• Health Level Seven Fast Healthcare Interoperability Resources （HL7I FHIR）をもとに今後ガバナンス・ルール案を策定予定 • OIDF コンフォーマンステスト参加	• ORPHE （連携機関は今後検討）
10	電通総研	• eIDAS との互換性を意識してサービスの全体運営管理や監視を行う組織・団体等の設立の必要性を提示 （事業者の認定条件設定・監査・認定取消機能の必要性、ウォレット、プロトコル、ネットワークやソースコードに関するシステム仕様の必要性等を提示）	• 電通総研 （連携機関は今後検討）
11	JISA	• 「事業者 KYC/KYB に関わる範囲」「支出・投資の事実確認に関わる範囲」において事業者アイデンティティに関わる Verifiable Identity Community（官民連携）のルール整備・コミュニティ形成の必要性を提示 • OIDF コンフォーマンステスト参加	• JISA （今後補助金事務局の管轄省庁、行政データ発行の管轄省庁、民間データのガバナンス機関・民間事業者の連携が必要）
12	OP CIP	• ステークホルダの役割を規定、原則となる OP 憲章を策定	• OP CIP 理事会

1.14. ステークホルダ内検証・協議等実施概要

各ユースケースの実証コミュニティ内でのステークホルダとの協議やヒアリング等の取組概要を整理した。

プロトタイプシステムを実装したユースケース(DataSign、DNP、IGS、SBI HD、シミック、ORPHE、電通総研、OP CIP)は、そのシステムをエンドユーザにデモ・実際に利用してもらうことでビジネスフィージビリティ・UX/UI 検証・業務適合性・ガバナンスの在り方等の検証を実施した。他ユースケースも部分的なシステム構築やアンケート・ヒアリング・協議等を実施することでビジネスフィージビリティ・UX/UI 検証・業務適合性・ガバナンスの在り方等の検証を実施した。

表 6-3-1　各ユースケースにおけるステークホルダ内検証・協議概要

No.	代表機関	実施概要
1	DataSign	• OWND Project の設立に向けた取組、ビジネスフィージビリティ検証としてステークホルダと協議 （Code for Japan / MyData Japan / OpenID Foundation コミュニティメンバ、有識者、政府機関関係者・関連団体・事業者） • ウォレットのユーザビリティテスト（エンドユーザ）
2	DNP	• 国内共助アプリ団体と UX/UI・ビジネスフィージビリティ検証 （カヤック、Asmama、アサヒ飲料、保育園に子供を預けている or 過去預けていた、共働きの夫婦等) • 海外共助アプリ（ボランティア証明書発行サービス）との連携を想定した協議 • VC 発行・検証における官民の役割にかかるディスカッション (Internet Identity Workshop のセッション主催・Open Identity Exchange と協議)
3	IGS	• 国際間採用マッチング検証と検証に向けた討議・ビジネスフィージビリティにかかるヒアリング、プロトタイプシステムを活用した検証 （国内採用企業・教育支援機関（FTU）FTU 学生・教育機関（慶応大学経済学部フィンテック研究所）等）
4	富士通 Japan	• ヒアリング、ガバナンス・ビジネスモデル検討、スキル標準化にかかる討議 （技術研究組合・国立大学とその技術職員） • ビジネスフィージビリティにかかるヒアリング（地域民間事業者）
5	PitPa	• ビジネスフィージビリティにかかるヒアリング（受入機関・送出機関・育成機関・仲介業者・日本語関係機関） • 外国人材へのアンケート • 日本企業での証明書発行プロセスの検証
6	みずほ R&T	• CMP タスクフォース内でビジネスフィージビリティ・ガバナンス案検討
7	SBI HD	• 沖縄オープンラボラトリ（OOL）の「Trusted Network PJ Phase 2」と連携し実証検証 • ISO/TC292/WG4 国際会議での発信 • ドイツ Industrie4.0 の専門委員会より、招待を受けプロトタイプシステムデモとビジネスにかかる討議を実施

No.	代表機関	実施概要
8	シミック	• デバイスメーカー、製薬企業、医療機関、社内外有識者へのヒアリング • 医療機関での実証、医療機関・患者へのヒアリング
9	ORPHE	• 企業（CRO・製薬企業）、下肢運動器系疾患患者・既往歴を有するユーザー、医療従事者へのヒアリング • データ計測や共有に対するポイント・NFT の付与と参加動機の検証
10	電通総研	• GAIN PoC プロジェクトで OID4VCI の実装にかかる討議、OpenID ファウンデーション・ジャパンで法人実在性にかかる議論参加 • 金融機関都市銀行・地方銀行とビジネスフィージビリティや KYB VC の仕様に関するヒアリング、業務等に関する意見交換
11	JISA	• 補助金事務局事業者・補助金運営政府当局との協議
12	OP CIP	• JICDAQ とガバナンスにかかる協議 • OP CIP 参加者への実装フィージビリティ・運営にかかる協議、プロトタイプシステムを通じた業務検証

１.１５. 調査分析等を実施したベンチマーク先

各ユースケースで調査・分析を実施したベンチマーク先を整理した。ベンチマークを「一般法規制・ルール」、「業界規制・ガイドライン」、「規格・技術標準」、「業界団体・自主規制」、「サービス」を分類して整理した。

- DataSign

  EUDIW との相互運用性を念頭に置いた取組を進めているため、eIDAS2.0、EU ARF をベンチマークに調査・分析を実施した。また、認証ウォレット・メッセージングサービス構築において、EU ARF の仕様にもなっている OIDF、また、メッセージングプロトコルを検討している Matrix をベンチマークとした。

- DNP

  相互運用性の観点で、Hyperledger Anoceds / Indy / Aries に準拠したウォレットと、OIDF 関連の仕様に準拠したウォレット双方の調査・分析を実施した。ガバナンス・ルールの策定では、シェアリングエコノミー国際規格（ISO/TS42501）、Open Identirty Exchange で策定している「A Guide to Trust Frameworks for Smart Digital ID」、台湾で共助実績証明書を発行しているウォレットをベンチマークとした。

- IGS

  ベトナムの大学生向けに日本企業への就職マッチングサービスを提供するため、ベトナムの個人情報規制の調査を実施した。また、採用マッチングにあたっての学生のスキルを把握する指標として、欧州が標準化を実施した ESCO 基準・EQF をベンチマークとした。

- 富士通 Japan

  大学技術職員のスキル可視化に向けて厚生労働省が取組を進めているキャリアマップを参考とした。また、技術職員のスキル共有・共同研究にかかるガバナンス・ルール策定に向けて教育基盤協議会や各大学の規定をベンチマークとした。

- PitPa

  ネパールの海外人材受入に向けてネパールの関連規制の調査を実施した。また、ガバナンス・ルールの取り組みでは Open Identirty Exchange で策定している「A Guide to Trust Frameworks for Smart Digital ID」をベンチマークとした。

- みずほ R&T

  化学物質関連・サプライチェーン関連の規制、国際標準の取組()や、サプライチェーンのユースケースを取り組んでいる業界団体(Catena-X、MOBI 等)や、実証実験等でブロックチェーン活用した先行事例をベンチマークとした。

- SBI HD

  事業所の真正性を保証する仕組みや、事業所にかかる証明書の認定・運営の仕組み実現に向けて、身元保証レベルにかかるルール(eIDAS2.0、NIST 800 63-4、e シール)、認証局等を認定する団体の評価にかかる規格・取組事例(ISO/IEC 17065、ETSI EN 319 403、JIPDEC)等をベンチマークとした。また、サプライチェーンのユースケースでの取組(沖縄オープンラボラトリ)と連携して実証を行った。

- シミック

  欧州・米国の電子署名にかかる規制(GDPR、21 CFR Part11)や米国の医療関連規制(HIPAA、DHT for Remote Data Acquisition in Clinical Investigations)についてベンチマークとした。また、シミックが所属する業界団体の取組(PHR サービス事業協会等)や ORPHE 社の取組との連携を検討した。

- ORPHE
  パーソナルデータを取り扱う国内外のサービスの中で比較的長期間サービス提供を継続できているサービス(Patients Know Best、Intuit Mint)について深掘り調査・分析を実施した。また、ガバナンスの取組では、準拠すべき規制・ガイドラインの提言を行った(次世代医療基盤法、HL7 FHIR 等)。
- 電通総研
  eIDAS2.0 に準拠したウォレットの構築を目指し、GAIN PoC プロジェクト、OpenID Foundation の取組・議論に参画した。また、犯罪収益移転防止法へ対応する業務にをベンチマークとして事業者ヒアリングを実施した。
- JISA
  行政手続きにかかる業務検討にあたって各種省庁の補助金事務にかかるガイドラインや、G ビズ ID、国税庁納税情報の添付自動化の仕組み等を参考にした。また法人情報の管理方法として eIDAS2.0 や EBSI-VECTOR プロジェクトにおける法人ウォレットの取組をベンチマークとした。
- OP CIP
  コンテンツ利用、広告利用等で普及している OP に類似もしくは近似する技術やその技術普及に取り組んでいる団体・サービス(EV SSL 規格、Open Graph Protocol、JOURNALISM TRUST INITIATIVE、ads.txt)や、広告関連の業界団体(JIQDAQ 等)について調査・整理を実施した。

代表機関	ベンチマーク先				
	一般法規制・ルール	業界法規制・ガイドライン	規格・技術標準	業界団体・自主規制	サービス・個社取組
DataSign	• GDPR • eIDAS2.0	–	• OpenID Foundation • Matrix.org Foundation • OpenWallet Foundation	–	• EUデジタルアイデンティティウォレット (EUDIW ARF Type 1)
DNP	–	–	• ISO/TS 42501 • OpenID Foundation • Open Identity Exchange • Hyperledger Project	• シェアリングエコノミー協会	• Turing Space (台湾の証明書発行・管理ウォレットベンダ) • Hyperledger Indyを活用した事例 (SITA、IDunion、Instnt、カナダBC州、DICE ID)
IGS	• ベトナム個人情報規制	• ESCO基準 (欧州のスキル標準) • EQF (欧州の資格レベルを標準)	–	–	–
富士通Japan	–	• 厚生労働省策定 キャリアマップ	–	• 研究基盤協議会 • 大学の各種規定	–
PitPa	• ネパール関連規制 • ネパール政府	–	• W3C • Open Identity Exchange	–	–
みずほR&T	–	• ELV指令 • RoHS指令 • TSCA • REACH規則 • SCIPデータベース	• ISO/IEC82474 • ISO/TC323 PCDS	• IMDSコミュニティ • MOBI • Gaia X、Catena-X • アーティクルマネジメント推進協議会(chemSHERPA) • IPA DADC (ウラノスエコシステム)	• Hyperledger Fabricを活用した事例 (三井化学、Chemchain、TradeWaltz、Circulor) • Cordaを活用した事例 (SBI Traceability、axedras等) • 他事例 (SEMI)

図 6-4-1　調査分析等を実施したベンチーマーク先(1/2)

代表機関	ベンチマーク先				
	一般法規制・ルール	業界規制・ガイドライン	規格・技術標準	業界団体・自主規制	サービス
SBI HD	• eIDAS • 電子署名法 • （eシールに係る検討）	–	• ISO/TC292 • ISO/IEC 17065 • ETSI EN 319 403 • NIST SP800-63-4 • W3C Credential Community Group 等	• 一般社団法人沖縄オープンラボラトリ • インターネット協会OIC BRPコンソーシアム • IPA DADC（ウラノスエコシステム） 等	• JIPDECトラステッド・サービス登録（認証局）
シミック	• GDPR • 21 CFR Part11	• HIPAA • Digital Health Technologies（DHT）for Remote Data Acquisition in Clinical Investigations	–	• Decentralized Trials Research Alliance (DTRA) • 一般社団法人PHR普及推進協議会 • PHRサービス事業協会	• ORPHE
ORPHE	• 個人情報保護法	• ALCOA原則 • 次世代医療基盤法 • 経済産業省_医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン	–	• 一般社団法人PHR普及推進協議会	• シミック • Patients Know Best • Intuit Mint 等
電通総研	• eIDAS2.0	• 犯罪収益移転防止法 • 金融規制	• GAIN PoCプロジェクト • OpenID Foundation • ISO/IEC 27017 • ISO/IEC 27001	–	–
JISA	• eIDAS2.0 • インドにおけるアカウントアグリゲーターフレームワーク	• 各種省庁の補助金事務にかかるガイドライン	–	–	• EBSI-VECTORプロジェクトにおける法人ウォレット • Gビズ ID • 国税庁納税情報の添付自動化の仕組み
OP CIP	–	–	• EV SSL規格 • Open Graph Protocol • JOURNALISM TRUST INITIATIVE • ads.txt	• Coalition for Content Provenance and Authenticity （C2PA） • JIQDAQ • Trustworthy Accountability Group	• NewsGuard

図 6-4-2　調査分析等を実施したベンチーマーク先（2/2）

１.１６. ガバナンス・ビジネス普及に向けた取組考察

【ガバナンス・ルールの策定にかかる成果】

ガバナンス・ルールの成果として、各フローに対してのステークホルダの責任分界点・技術論点の整理を行った(詳細は DNP の取組を参照すること)。また、異常系が発生した際の保証・補償内容等を明確にしていく必要性が提示された(詳細は電通総研の取り組みを参照すること)。これに対して、契約法の区分に則って、どのケースで誰が誰に対して責任を果たすべきかというのをフレームワークとして提示していくことが有効ではないかという意見を有識者いただいた。

【ガバナンス・ルールの策定にかかる継続課題・対応方針】

- ガバナンス・ルール策定ノウハウの共有

ガバナンス・ルールを策定することは与えられたルールに準拠することよりも高度であり、専門性・ノウハウを要するため、ガバナンス・ルールの共有化の必要性や、事業者だけでは対応が困難という指摘を受けた。トラストフレームワーク策定・コミュニティ形成等の取り組みを進めるにあたっては、作成ノウハウを共有化、ガイドライン化することで事業者が社会実装を早めることができる素地を醸成することが重要である。(図 6-5-1 参照)

- 海外とのデータやり取りするユースケースにおける合意形成

海外とのデータやり取りをする場合、ガバナンス・ルールの討議を行う前段階で、海外法規制や政府との調整を要する。また、事業者間で合意した内容がプライバシー上の観点で問題ないかを確認する必要があり、事業者だけでは解決が困難な事例を確認した。各国のプライバシー規制・トラストフレームワークとの相互運用性確保は政府がリードして行っていく必要がある。例えば、EU-米国間では、データプライバシーフレームワーク(DPF)の十分性認定 [16]や、デジタルアイデンティティの保証レベルのマッピング [17]等が進められている。行政においては、比較元となるトラストフレームワークを策定したうえで、海外各国とのプライバシー保護、アイデンティティ保証レベル等の比較整理を行っていく必要がある

- 業界規制が複雑、業界を横断するユースケースにおける合意形成

ステークホルダが果たすべき責任はユースケースの業界で適用されるルールや慣習によって異なり、業界によってはステークホルダ内外の調整を要し社会実装の課題になるケースがある。例えば、金融・サプライチェーン・ヘルスケア等は現行の業界関連国内外の規制や業界団体が存在しており、どのルールに準拠して仕組みを構築していくかの検討や、ステークホルダ内の意思決定が困難となる。また、行政手続のデジタル化等、関係省庁や業界横断の取組は、上記に比較してステークホルダや、調整すべきルールがより多様であるため、ステークホルダ間の責任分界点の整理自体が困難となる。業界間で参照すべき規制・ルールが複雑化していたり、監督省庁が複数いたりすることでルール策定が困難な場合、政府機関・事業者等の連合(官民コンソーシアムの組成)等を組成し、ルール形成を行っていくことが必要となる。また、ルール・ステークホルダが複雑な場合は一体的な法改正についても検討する必要がある。

---

[16] Adequacy decision for the EU-US Data Privacy Framework
https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

[17] DRAFT EU-US TTC Digital Identity Mapping Exercise Report
https://www.nist.gov/identity-access-management/eu-us-ttc-wg-1-digital-identity-mapping-exercise-report

【取組発信にかかる成果】

国際標準の働きかけやオープンソースコミュニティを形成して発信する事業者を確認した（SBI ホールディングス、DataSign の取組を参照すること）また、本事業において OIDF、OpenWallet Foundation、OIX、EUDIW メンバとのとの相互運用性にかかる協議や、BGIN においてユースケース取組の発信・ディスカッションを実施した

コミュニティ形成・他コミュニティでの発信・技術標準策定の取組を進めることで、技術標準団体からの支援等を受けることができ、自身のユースケースが活用する技術の普及・相互運用性の確保等が期待される。

【取組発信にかかる継続課題・対応方針】

実証事業の中で、取組発信の支援等を実施したが、ガバナンス・ルール策定の結果は英語での文書化・国際会議等の場での発信が重要となり、実証が終わっても引き続き取り組んでいく必要がある。発信のインセンティブ設計を行う必要があると有識者から意見を頂いた。また、政府機関がアイデンティティ・プライバシーにかかる国際会議の場を設定することで標準化・相互運用性の確保が期待される。

	分類		ユースケースの社会実装に向けて留意すべき事項
高 検討の優先度 低	基本法	• 民法の契約法 • 電子署名法（eシール等） • 個人情報保護法（GDPR等） • ほか海外規制 等	• トラストフレームワーク等を活用することで責任分界点・補償の範囲等を明確にすること、契約と一体となっていて当事者間において複雑な契約にならないような工夫がされていること • 発行者・利用者の署名・同意を法的根拠があるように実装すること • 海外から/へのデータ移転について十分なプライバシーの対策を行うこと、各国の法規制について十分な留意をすること（暗号資産等のトークン管理・個人情報保護等）
	業界ルール	• 身元確認・デジタルアイデンティティにかかる規制 • 行政手続きに係る規制 • 金融規制 • 医療・ヘルスケア規制 • サプライチェーン規制 等	• 個別業界のルール・慣習に沿った対応を行うこと（発行した証明書の法的効力や、データ項目/流通/保護の要件充足性等について検討すること） • 既存の業界団体・規制を管轄する関係省庁との調整を十分に検討したうえで、ステークホルダの巻き込み・コミュニティ形成を行っていくこと（特に複数のエコシステム・コミュニティにまたがる領域は注意すること）
	規格・標準（フレームワーク等）	• ISO • ETSI • W3C • NIST 等	• ウォレットの規格や、セキュリティやプライバシー等は既存の検討されている標準規格等に対応すること • 相互運用性を高める際は海外の同様の取り組みをしているサービス・事業者の対応している国際規格を確認すること • 自社・コミュニティ等で取り組んだ内容はドキュメント化（英語）・発信することで標準化の支援を行うこと
	規定（組織・業務）	• 雇用規定 • 業務ルール 等	• 雇用関係・業務規程に留意して、法人/個人のデータ持ち主、データ共有の権限を決定すること（法人担当者と法人の権限管理/職員経歴の共有権限等）

図 6-5-1　ユースケースの社会実装に向けて留意すべき事項

Trusted Web に関する考察・分析

1.17. Trusted Web に関する事業者からの課題提起

事業者からユースケース実証を通じて提起された課題を紹介する。Truted Web ホワイトペーパーVer3.0 に記載されている原則をもとに課題・提言が記載されている

（1） 持続可能なエコシステム関する課題と提言

- エコシステム実現とビジネス化は鶏が先か卵が先かの問題が存在する。
  （ビジネスのインセンティブとして多様なステークホルダーを巻き込みながらユースケース創出できることが必要であるが、初期はビジネス利用のインセンティブが無いためステークホルダが参加せずエコシステム形成ができない。）
- エコシステムが適切に形成・運営されていることの可視化・効果測定の仕組みを構築することに課題がある。
- エコシステムやそのインセンティブを構築するためには、規制・ガイダンスでの発信が必要であることもあり規制当局・業界団体との議論が求められる。

（2） マルチステークホルダによるガバナンス関する課題と提言

- マルチステークホルダーによる参加は可能となるが、コミュニティ参加者においてすべてのステークホルダーの責任を明確にするのは難しい。
- ステークホルダーが増えれば増えるほどガバナンスが有効に機能しているのか判断する難易度が高まり、タイミングも複雑になる。
- エコシステム全体において、トラスト形成のために各ステークホルダーが担う責任が時系列ごとに変化していくため、抜け漏れなく全体像を指し示すことが難しい。
- 海外との連携で、データの管理の仕方における思想的部分の擦り合わせに時間を要する。

（3） オープンネスト透明性に関する課題と提言

- ユーザー目線でトラストの検証範囲が透明性を持って実感できるかどうか検証が必要。ユースケースごとにヒアリング調査を実施し、UI/UX の観点からもオープンネスと透明性について検討を行う必要がある。
- プライバシーを高めるための暗号化方法がサービス上ブラックボックス化されてしまうので、その方法のアカウンタビリティをどう担保するかが課題となる。
- 透明性を高めるための取組では、ステークホルダの認定・ホワイトリスト等の管理する費用等が発生し、その運用コストをどのように負担するかが課題となる。

（4） データ主体によるコントロールに関する課題と提言

- 検証者によるデータの取得について、どのタイミングでユーザーからの同意を取るか議論が必要。毎回ユーザーに確認すると、ユーザービリティが損なわれる可能性がある。
- 将来的にユースケース等が広がってくると、データ主体がすべてのデータをコントロールすることが難しくなるため、データ主体によるコントロールを保証する代理人のような存在をどのように定義するかが課題となる。

- 事業者に関係する情報は、法人格の情報と、事業者に関連する自然人の情報の 2 つが存在する、各々の主体の識別と当人性の確認、およびデータ管理の観点で、法人格と自然人を機能分離しながら、業務運用上、円滑に制御と連携が可能とする仕組みの検討が必要となる。
- 利用者が保持する全てのデータに対して開示/非開示の権限を与えるべきだが、最初から個人ごとに権限を与えすぎると事業者が成立しないケースが多く想定された。また、利用者自身のデータであるが組織の機密ポリシー上利用者が開示コントロールができないケースも存在した。

（５） ユニバーサル性に関する課題と提言

- 資格証明実績の蓄積がない人が社会的に排除されることがないように、その蓄積方法や活用シーンについてはユースケースごとに事業者も含めて慎重に検討する必要がある一方で、悪意を持った第三者からの攻撃を想定した対策は、新規参入者へのハードルにもなりかねないためユースケースごとに対策のレベルを調整する必要がある。
- 技術的な制約により対応しているスマホや PC を持っていない人は排除することになってしまうことは課題となる。
- デジタルアイデンティティウォレットの利用は新しい体験となるため、使い方を理解してもらうためには現状においてはハードルがあると感じており、それが排除につながることが危惧される。
- どんな企業も参加できる仕組みは想定していない。例えば評価機関の評定や、海外とのやり取りが発生する際には安全保障上（技術/人の輸出）の観点をクリアした企業とそのプロジェクトを推進するのが一般的である。そのため、参画する企業の信頼性を評価する必要が別途発生する。

（６） ユーザ視点に関する課題と提言

- Wallet という概念を知らない生活者に対して、様々なアイデンティティ情報が蓄積されて、サービス利用時に連携可能であるというコンセプトを伝えることにハードルが存在する。
- 複数の発行者、複数の VC、複数の検証者が選択可能となった場合の UX の複雑さが課題となる。

（７） 継続性に関する課題と提言

- 既存のトラスト手段とのフェデレーションをするためにトラストチェーンが複雑になってしまうこともある。
- 従来まで存在しない領域へのトラスト付与となるためコストが高価になる可能性がある。コストを安価にしていくためには参画していくステークホルダーを増やす必要があり、その初期のステークホルダーを増やす期間にはコストに対する補助策や各ステークホルダーへのトラスト自体の啓蒙が必要である。

（８） 柔軟性に関する課題と提言

- すべての構成部品を疎結合にすることは逆に効率性が失われることもあるため、どの程度の拡張性を持たせるかに課題がある。

- 可能な限り疎結合で構成部品を検討したい一方で、データの保守やリカバリーの問題を考慮すると企業側が一定程度の管理をした方がユーザービリティが高くなる領域がでてくる。両者のバランスを鑑みながら、実装の実情に則したアーキテクチャ設計の検討が必要。

（９） 相互運用性に関する課題と提言

- Verifiable Credentials のデータフォーマットについて、標準化団体の中でも意見が割れており今後の相互運用性の確保については適宜状況をみながら方向性を定めていく必要がある。
- 法制度の相互運用性には課題がある。特に DIW の法制度で先行している EU の規制に準拠するためには、個人情報保護における十分制認定のような国家間の取り組みが必要となる。
- 法制度やガバナンスについてはまだ議論が十分にされていないのが現状であり、今後の発展が期待される。
- ステークホルダーごとにデータポリシーに差異があり、例えばクラウドにデータを格納する際の扱いやステップが異なる。グローバルの観点では安全保障の観点を考慮する必要がある。

（１０） 更改容易性・拡張性に関する課題と提言

- 現状のウォレット仕様については、仕様が決まっていないものが多いため、それに追従するための開発が機能拡張の容易性に対して悪影響を及ぼす場合もある。特定の技術に依存したほうが機能拡張が容易な場合もある。
- 特定の技術に依存しすぎることに問題があることは同意する一方で、実装レベルで相互運用性を確保するためには一定程度の道標となるガイドラインが必要。EUDIW の議論を参考に、Trusted Web 実現のためのアーキテクチャーフレームワークとしてデータ形式や通信プロトコルの明示に踏み込むことも必要ではないかと考える。

１.１８. 事業者が Trusted Web を具現化する上で有効な取組の提言

ここでは、事業者の取組や有識者との議論の過程で、Trusted Web を具現化する上で有効な取組と判断したものを紹介する。

（１） 持続可能なエコシステム

- ステークホルダに対してエコシステムへの参加（継続）インセンティブがあるビジネスモデルを検討する必要がある。
  - ステークホルダの課題解決・価値設定を行ったうえで、実際にステークホルダに対して利用意向・支払ってもよい価格等を確認すること。
  - 導入前と導入後で責任モデルが明確に変化する場合、責任個所が提供価値になる可能性が高い。責任モデルとその責任が果たせなかった補償モデル等も考慮すること。
  - 既存の業界規制・慣習の影響が強いユースケースは既存団体との調整を行うこと。（場合によっては行政機関からの支援を受けることが有効である。）

（２） マルチステークホルダによるガバナンス

- マルチステークホルダのガバナンスを検討する上では、トラストフレームワークの策定・運用が 1 つの有効策として挙げられる。（ルール策定において考慮すべき事項は「6.5.ガバナンス・ビジネス普及に向けた取組考察」参照）
- マルチステークホルダがルールに則っているかの監査では、ステークホルダーの役割・責任を踏まえて起こりうるリスクが整理されており、そのリスクを低減する形でガバナンスを利かせることができているかという観点で監査設計が重要、また、トランザクションデータから監査する場合は、「第三者への証跡が必要な情報」の整理、その整理を行った際のプライバシーリスクについて留意する必要がある。

（３） オープンネスと透明性

- ユースケースのビジネスモデルにおいてどの程度透明性が重要であるか検討したうえで以下のような取組を検討することが有効であると考えられる。（参考例：OpenID Foundation や Open Banking の取組等）
  - 開発コードがオープンソースで公開されていること、API が公開されドキュメントとして整備されていること。
  - 提供 API に事業者検証用のガイド等が整備されていること。
  - 事業者が相互運用性を確保してサービス提供できるかの確認等（Conformance Test）がツールで提供できること。

（４） データ主体によるコントロール

- ステークホルダとの関係上自身でデータコントロールができない可能性や、当事者のニーズでデータの代替管理が求められるケースもあるため、必ずしもすべてデータコントロールをデータ主体に寄せる必要はないことに注意すること。
- プライバシーに配慮されたデータ管理の考え方としては、以下が挙げられる。

- ✧ データやり取りの主体間に unlinkability があること。（データやり取りの履歴から本人が類推されないこと。）
- ✧ 忘れられる権利に対応すること。（Verifier が持つ個人情報を明確化して、Holder から削除要望があった際に削除できるようにすること、データの生成・保管・消費におけるデータやその場所のコントロールが確保されていること。）
- ✧ 検証する公開鍵等の個人情報を、他ステークホルダーが確認できないこと。（パブリックチェーン等に記帳しないこと。）
- ✧ 個人の属性情報と認証/認可に必要な情報の切り分けができていること。

（５） ユニバーサル性

- ➢ ユニバーサル性の目指すべきレベル感は OECD の Recommendation on the Governance Digital Identity が参考になるが、エコシステムによっては必ずしもすべてのユーザを包摂している必要はないため、各ユースケースの中でどのような参加者を期待するかとその要件を検討すること。（ユニバーサル性と参加者の信頼性担保は一定トレードオフが発生する。）
- ➢ ステークホルダ間でどの程度のデータの信頼性を担保する必要があるかは、証明書の保証レベル等にかかる議論を参考して Trust の程度がを明らかにすることが有用である。

（６） ユーザ視点

- ➢ プライバシー通知と同意は、ISO/IEC 29184 等を参考にすること。
- ➢ 利用者への選択肢がある UX/UI の実装例としては Open Banking カスタマージャーニー等が参考となる。

（７） 継続性

- ➢ 継続性を有効に活用している事例としては、①サービスを提供する事業者の検証に PKI（トラストリスト）を活用する、②利用者の証明書と本人であることの紐づけは既存の身元確認プロセスを活用する、③証明書の発行・検証プロセスに既存の認証認可のプロセスと組み合わせて活用する（OID4VC/VP）等が挙げられる。

（８） 柔軟性

- ➢ 柔軟性を担保する取り組みとしては、レイヤ間のインターフェースを高めていく運用を高めていく工夫が必要となる。（以下例示）
  - ✧ Credential Layer - Public Trust Layer ：DID Document の取得インターフェースが変わらないこと。
  - ✧ Credential Layer - Agent Layer ：データフォーマットが変わっても同じ通信プロトコルで動かせること。
- ➢ Vertical Cross - Cutting の領域が固定化されてそれぞれのミドルウェアがその方式に対応していることが今後期待される。

（９） 相互運用性

- 実装における相互運用性担保は柔軟性・更改容易性を参照する。現在の実装事例は別紙「規格動向調査」を参照されたい。
- プライバシー、セキュリティレベルの相互運用性は、CBPR・GDPR の十分性認定、Data Protection Framework といった、クロスボーダー連携時のプライバシー領域での取り組みを確認する。
- ユースケース内で取り組んだルール策定は、英語ドキュメント化・国際会議での発信、ディスカッション等によって相互運用性にかかる働きかけを行っていくことが重要である。

（１０） データ主体によるコントロール

- データフォーマットの拡張性について十分留意すること。（VC を活用する際に VC/VP の構造が複雑になると拡張性に対応できないのでシンプルな検証フロー・データフォーマットに留意すること。）
- ライブラリの更改に対応できるアーキテクチャにしていくこと、ライブラリが公開される際は外部レイヤとの互換性担保まで確認してから追加実装すること。