デジタル庁御中

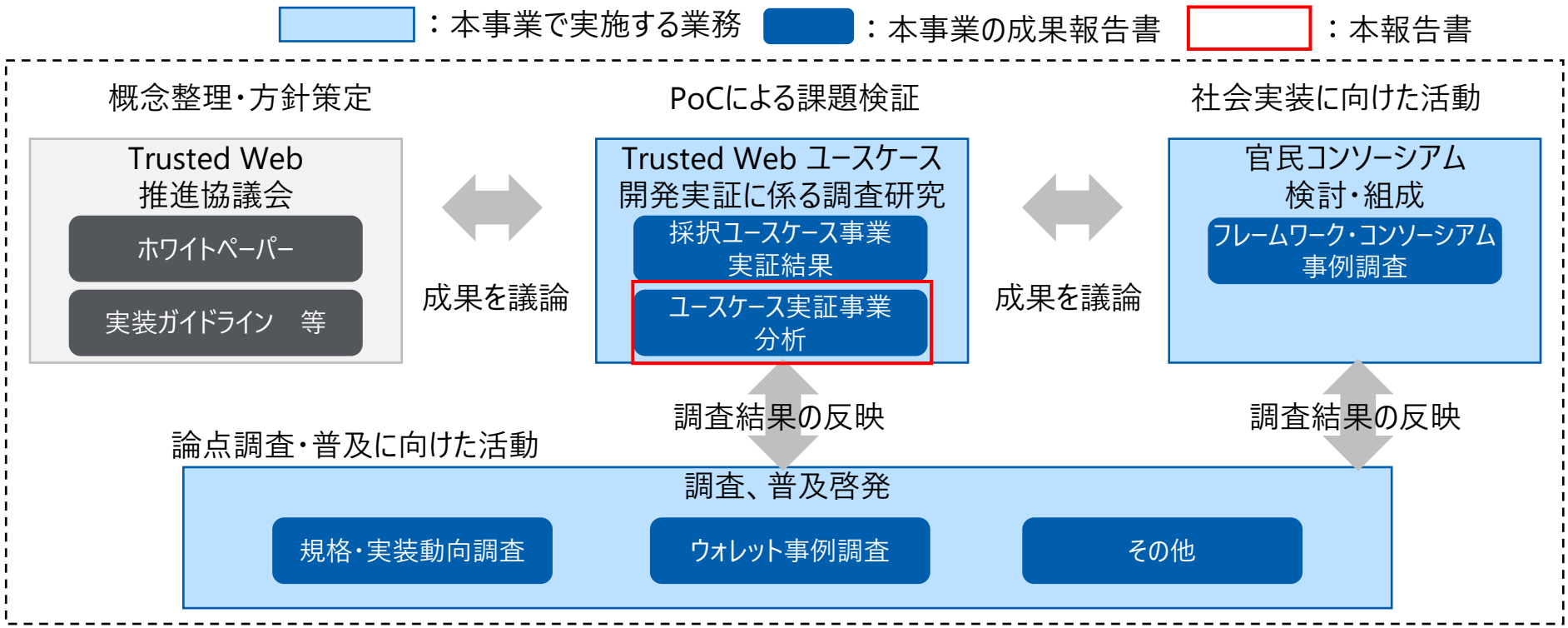
令和4年度補正
Trusted Web 開発等推進事業に係る調査研究
（Trusted Web の実現に向けたユースケース実証 分析レポート）

令和6年3月

TOPPAN株式会社

本書の位置づけ

- 本事業は、昨年度事業である13 件のユースケースの開発実証等や、内閣官房デジタル市場競争本部事務局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、デジタル庁の委託のもと以下の業務を実施
  - 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検討・組成
  - ③ 調査・普及啓発
- 本報告書は、①Trusted Web ユースケース開発実証に係る調査研究の中で、今年度採択された12件のユースケース実証事業分析をとりまとめたものである



1. 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」の提言を受け、DFFTの具現化も視野に、2020年10月に「Trusted Web推進協議会」が発足した。「Trusted Web」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）
- 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
- 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

目的

- 以下観点でTrusted Web の実現に向けたユースケース実証事業の整理・分析を行うこと
  1. UCの成果や課題をわかりやすく整理し、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整理・普及に向けて必要な取り組み・環境整備等の提言を行うこと

2. 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
- 加えて、ビジネスモデル・実装手法の比較、ガバナンスを中心に2022年度ユースケース実証結果もインプットとして活用

数字：取り扱う章

インプット

2022年度ユースケース実証

13件の実証事業を採択し以下取組を実施
- ビジネスモデル検討
- プロトタイプシステム企画・開発

取組内容のブラッシュアップ

2023年度ユースケース実証

12件の実証事業を採択し以下取組を実施
- ビジネスモデル検討
- プロトタイプシステム企画・開発
- ガバナンス・コミュニティ形成

分析方針

		分析観点
3 基本情報		–
実証結果整理	4 ビジネスモデル	• 解決したい課題・ベネフィット • 収益モデル • 参画プレイヤー・ユースケースの広がり
	5 実装要件・実装アーキテクチャ	• 2022年度と比較して実装の考え方の変化 • 実装において活用する規格・技術
	6 ガバナンス	• ルール策定においてベンチマークとした事例 • 業界特有の課題も踏まえた対応
7 Trusted Webに関する考察		• 事業者がTrusted Web取組に対応するための課題 • Trusted Web普及に向けて参考となる取組

3.1. ユースケース概要（1/2）

No.	ユースケース	代表団体	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	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	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	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	富士通Japan株式会社	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	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	B	サプライチェーン	法人・製品	化学物質含有量	取引法人

*以降ユースケース参画事業者は以下表記とする
株式会社DataSign　→　DataSign
大日本印刷株式会社　→　DNP
Institution for a Global Society株式会社　→　IGS
富士通Japan株式会社　→　富士通Japan
株式会社PitPa　→　PitPa
みずほリサーチ＆テクノロジーズ株式会社　→　みずほR＆T

3.1. ユースケース概要（2/2）

No.	ユースケース	代表団体	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
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	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	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	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	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・開設情報	金融機関
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	一般社団法人情報サービス産業協会	B	行政	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	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

*以降ユースケース参画事業者は以下表記とする
SBIホールディングス株式会社　→　SBI HD
シミック株式会社　→　シミック
株式会社ORPHE　→　ORPHE
株式会社電通総研　→　電通総研
一般社団法人情報サービス産業協会　→　JISA
Originator Profile 技術研究組合　→　OP CIP

3.2. 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

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	• 二社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、DNP、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 HD 等

3.3. 今後のマイルストン

A類型 B類型

凡例 ：課題への対応・継続実証 ：初期実装・商用化 ：横展開・市場拡大

代表機関	業界	2024年度	2025年度	2026年度以降
DataSign	個人	メッセージングベータサービスリリース/汎用ウォレットをベースとした複数アプリケーションでの相互運用性の確認		メッセージング運用ノード増加
DNP	個人	PoC（UI・UX design/技術検証等）	商用化	エコシステムの拡大（共助実績以外のデジタル証明書との連携等）
IGS	個人（人材）	ガイドライン整備/アプリ・システム構築		商用化
富士通Japan	個人（人材）	フィージビリティスタディの深堀り/PoC		商用化
PitPa	個人（人材）	データモデル標準化/データポリシーの確立/ガイドライン整備	商用化	普及推進
みずほR&T	サプライチェーン	コンソーシアム設立/システム開発/運用テスト		商用化（CMP稼働/CMP運用会社の立ち上げ）
SBI HD	サプライチェーン	国際標準化に向けた準備/認証機構の受皿機関選定	初期実装・検証	商用化範囲の拡大/国際標準規格の発行
シミック	ヘルスケア	データ要素検討/総合的な計画立案コンサル・マネジメントサービスの設計		商用化（アカデミア、製薬企業向け）
ORPHE	ヘルスケア	認証取得/法律・ガイドラインへの準拠対応/ガバナンス・利用規約の整理・作成	商用化（患者-医療機関のサービス）	第三者（研究機関-製薬企業）のデータ共有リクエスト機能サービス開始
電通総研	法人・金融	KYC・KYBレベルの設定/ガバナンス整備/システムアーキテクチャ・秘密鍵プロセス確立	商用化	周辺事業者のサービス巻き込み/海外との商用レベル接続
JISA	行政	実証実験/コミュニティ検討/パイロットシステム・ユースケースの取り組み		商用化
OP CIP	メディア	秘密鍵管理プロセス・システムアーキテクチャ・運用プロセスの確立	社会実装 国際標準化	

4.1. 顧客の課題と提供価値（1/2）

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わからない • 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・大学間の研究推進および地域貢献（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

4.1. 顧客の課題と提供価値（2/2）

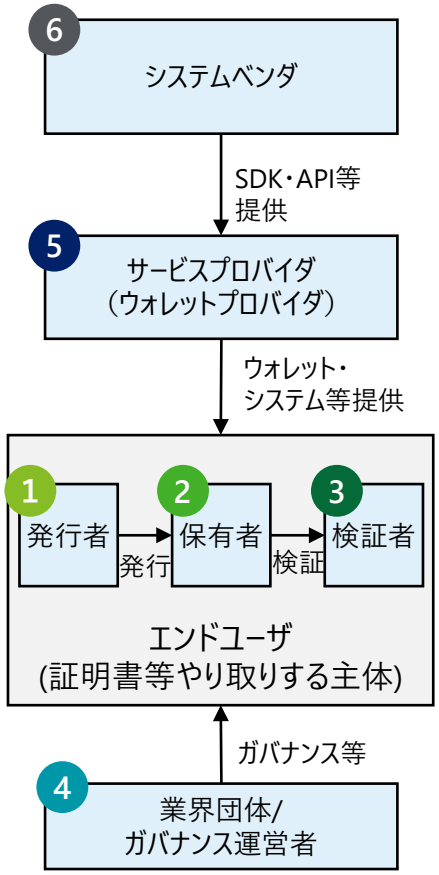
代表機関	対象顧客	課題意識（ペイン）	本ユースケースで実現する顧客への提供価値
SBI HD	製品のサプライヤー	• 業界・業種横断で事業者・製品の信頼性の担保をしたいが、実態は模造品が流通している、第三者からの真正性が担保できていない状態	• 事業所の実在性を確認でき、第三者が検証可能なデジタル証明書を付与することで取引相手の信頼度を向上すること・出荷検査時に製品ロットに対して製造者の保証を追加すること
シミック	製薬会社、CRO・SMO・ARO等の知見に関する機関の臨床事業部門	• 臨床試験、臨床研究のコスト削減と速度向上を図りたいが、関連システム・デバイスに多用なものがあり、ベンダー、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	

4.2. 実証ユースケース実現時の経済効果

■ ユースケースの経済・社会的効果をリスク抑制・コスト削減・売上拡大（市場拡大）に分類して整理した

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 HD		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 CIP	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**）	✓	–	–

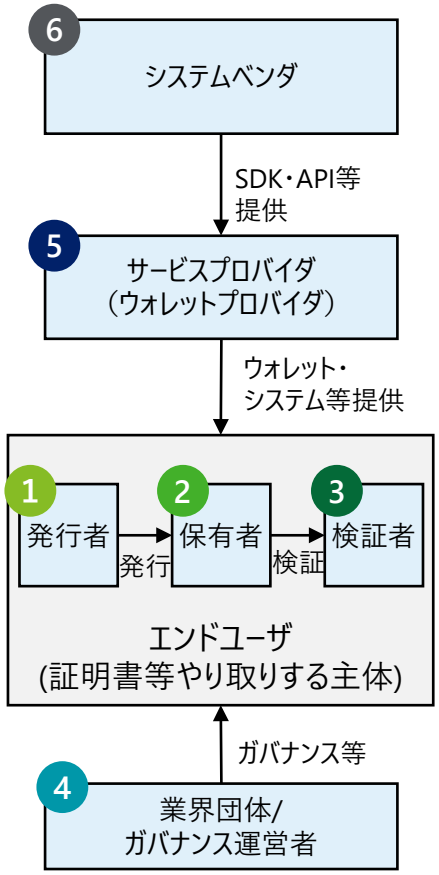
4.3. 収益モデル(1/3)



	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)*1** – 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)*1** – 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)*2、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 • **OP CIP*3** – 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 • **みずほR&T (Chemical Management Platform)*1、SBI HD (デジタル認証機構)*2、JISA、OP CIP*3** – 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)*1** – コンソーシアム参加料

*1 みずほR&T(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ため、併記としている
*2 SBI HD (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ため、併記としている
*3 OP CIPは、発行者であり、サービスプロバイダであるため、併記としている

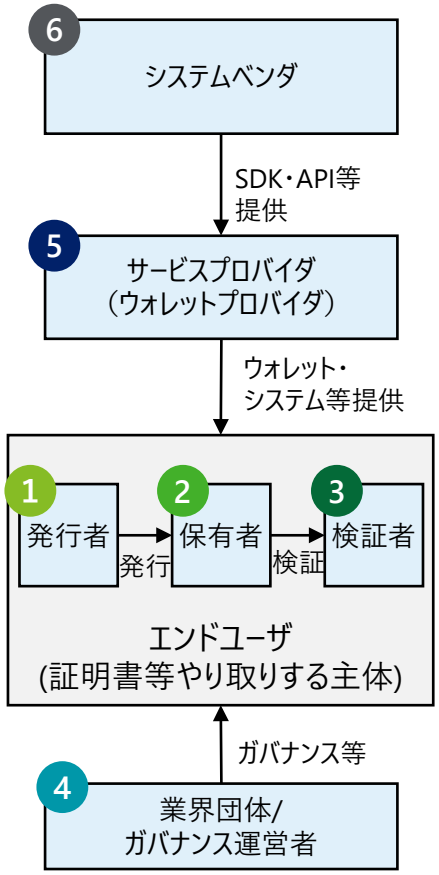
4.3. 収益モデル(2/3)



	支払先	獲得する対価	該当UC
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

*1 みずほR&T(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ため、併記としている
*2 SBI HD (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ため、併記としている
*3 OP CIPは、発行者であり、サービスプロバイダであるため、併記としている

4.3. 収益モデル(3/3)



5 From サービスプロバイダ

	支払先	獲得する対価	該当UC
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	• **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

6 From システムベンダ

事例なし

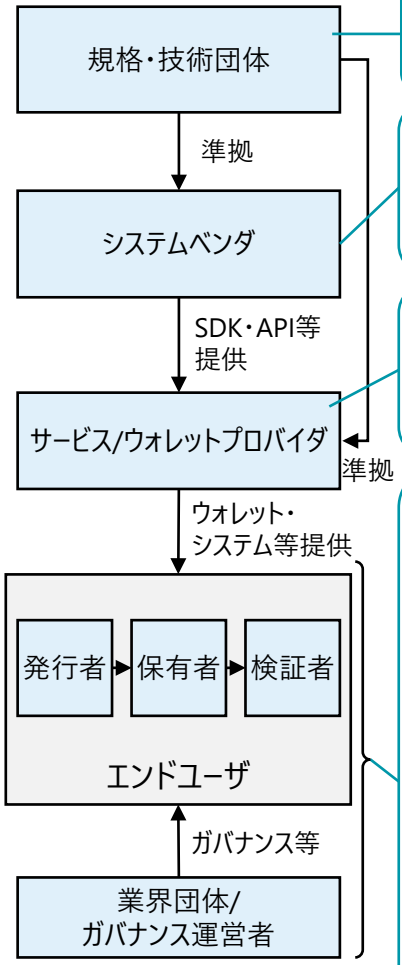
2023年度・2022年度比較

TOPPAN

4.4. プレイヤーマッピング

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

ビジネスモデル



プレイヤー

- World Wide Web Consortium (W3C)
- OpenID Foundation (OIDF)
- ISO/IEC
- Decentralized Identity Foundation(DIF)
- Hyperledger Project
- NIST　等
- Open Identity Exchange (OIX)
- Internet Engineering Task Force (IETF)

- CollaboGate Japan
- Cycaltrust
- アラクサラネットワークス
- 東京大学
- ヤフー
- Keychain
- 電通総研
- BlockBase
- 伊藤忠テクノソリューションズ
- Web DINO Japan

- DataSign
- DataGateway
- 富士通Japan
- NRIデジタル
- SBI HD

- メタバース事業者：KDDI
- 共助アプリ事業者：DNP
- 人材系事業者：IGS・PitPa(フォースバレーコンシェルジュ)
- ヘルスケア事業者：OROHE・シミック
- サプライチェーン事業者：東芝テック・ヤンマーホールディングス・CMP（みずほR&T）
- 金融：アクシオン
- 行政手続：行政機関(JISA支援)
- メディア：OP CIP、OP CIP参加メディア

		発行者	保有者	検証者	業界団体/ガバナンス運営者
個人の検証が主	全般	• 身元確認事業者 • 共助サービス事業者	• メタバースユーザ • 共助アプリユーザ • メッセージングサービスユーザ	• メタバース空間提供者 • 共助サービス事業者 • メッセージングサービスユーザ	• 共助アプリ団体 • コミュニティ（OWND Project）
	教育（人材）	• 大学・大学教員・教育機関・受入企業	• 学生（国内・海外） • 職員	• 採用企業	• 研究基盤協議会 • 国内・海外政府
	ヘルスケア	• 患者・医療機関・医療スタッフ			• PHR推進協議会
法人・モノの検証が主	サプライチェーン	• CFP・物質管理企業 • デジタル認証機構 • サプライヤ・エンドユーザ • デジタル複合機	• CFP・物質管理企業 • サプライヤ・ユーザ • デジタル複合機	• 左記企業と取引する企業 • 文書管理システム	• 物質管理団体（CMP） • 認定機関
	金融	• 身元確認事業者	• 企業	• 金融機関	
	行政手続	• 行政機関・民間事業者	• 企業	• 税務署・補助金事務局	• 行政機関
	メディア	• 証明書発行期間	• メディア・アドテク事業者	• サイト訪問者、メディア・アドテク事業者	• 認証機関（JIQDAQ）

4.5. ビジネスモデル考察（1/2）

課題・提供価値訴求

- 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)
- 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)
  - ➡ 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

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年度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
  - ✓ 人材系で海外の学生・求職者との成績・職歴データのやり取り（IGS、PitPa）
  - ✓ サプライチェーン関連で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）
  - ➡ 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

4.5. ビジネスモデル考察（2/2）

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
- 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
  - ➡ 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)
  - ➡ 必ずしも責任主体の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。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
  - ➡ 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）

5.1.1. 実装要件 - Verify ・データコントロールの考え方

A類型 B類型

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）

5.1.2. 実装要件 - 合意形成・トレースの考え方（1/2）

A類型 B類型

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

5.1.2. 実装要件 - 合意形成・トレースの考え方（2/2）

A類型 B類型

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）	–

5.1.2. 実装要件 - 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）

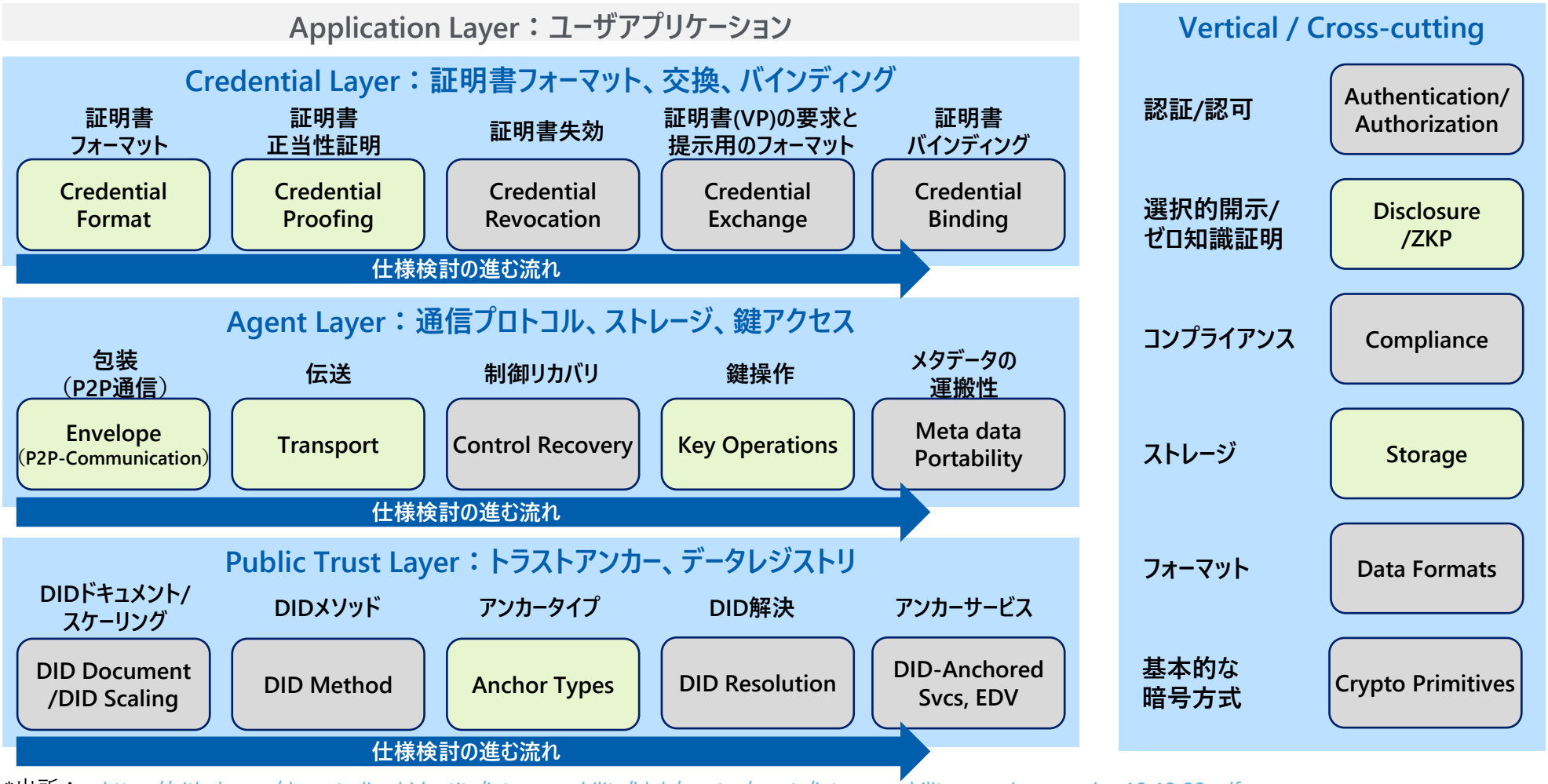
A類型 B類型

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が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	–		

5.2.1. 実装規格・アーキテクチャ - 比較整理対象

凡例: 比較対象 / 比較対象外

- DIFの「interoperability Mapping Exercise」をもとに、本ユースケースで活用された規格を整理した
- 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）



*出所： https://github.com/decentralized-identity/interoperability/blob/master/assets/interoperability-mapping-exercise-10-12-20.pdf

5.2.1. 実装規格・アーキテクチャ - Credential Layer :証明書の検証方法・選択的属性開示

A類型 B類型

■ Credential Format

	UCでの活用			
X.509（IETF）	01. DataSign 07. SBI HD			
(広義の) Verifiable Credentials	**W3C VC（W3C）** 05. PitPa 07. SBI HD	**OID4VCI/OID4VP（OpenID Foundation）** 01. DataSign 02. DNP 10. ISID	**Aries RFC Issue Credential Protocol** 02. DNP 09. ORPHE	**独自** 08. シミック 12. OP CIP

■ Credential Proofing / Selective Disclosure (ZKP)

	UCでの活用		
	選択的属性開示なし	選択的属性開示（データ最小化）	選択的属性開示（ゼロ知識証明等）
JWT-VC	01. DataSign 12. OP CIP	—	—
SD-JWT VC	—	01. DataSign 02. DNP 10. 電通総研	—
LDP-VC	05. PitPa 07. SBI HD	—	—
AnonCreds	—	—	02. DNP 09. ORPHE

※JISA、富士通Japan、みずほR&T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

5.2.2. 実装規格・アーキテクチャ - Agent Layer :通信プロトコル・I/F

A類型 B類型

■ Envelope（P2P-Communication）

	UCでの活用	
DIDComm Message v2	02. DNP	09. ORPHE
SIOPv2	01. DataSign 02. DNP	10. 電通総研
その他	03. IGS 05. PitPa 07. SBI HD	08. シミック 12. OP CIP

■ Transport

		UCでの活用	
複数デバイスでのデータ交換	QRコード	01. DataSign （SIOPv2・OID4VPの Cross Device Flow） 05. PitPa 10. 電通総研 （SIOPv2・OID4VPの Cross Device Flow）	02. DNP 09. ORPHE （OAuth 2.0 Device Flow）
	NFC	–	
	Bluetooth	08. シミック （デバイスのペアリングで活用）	
同一デバイスでのデータ交換/連携無し		06. SBI ホールディングス	12. OP CIP

5.2.3. 実装規格・アーキテクチャ - Agent Layer：秘密鍵管理/Public Trust Layer : 公開鍵の連携

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(事業者による)** • 広告主またはDSP事業者等が自身のDPレジストリサーバ等で管理	**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

5.3. 実装要件、実装規格・アーキテクチャ考察（1/3）

【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（実装した9件のうち5件）
  - ➡ EUデジタルアイデンティティウォレット（EUDIW）で公開されたArchitecture Reference Framework（以下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要因として挙げられる（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）
- 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
  - ➡ 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、第三者の監査に関する考え方】

- 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）

5.3. 実装要件、実装規格・アーキテクチャ考察（2/3）

【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（選択的属性開示含む）

- 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った。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）の活用があげられる）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）において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

- OIDFが策定している通信プロトコル/デバイス連携にかかる仕様（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

5.3. 実装要件、実装規格・アーキテクチャ考察（3/3）

【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

- 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

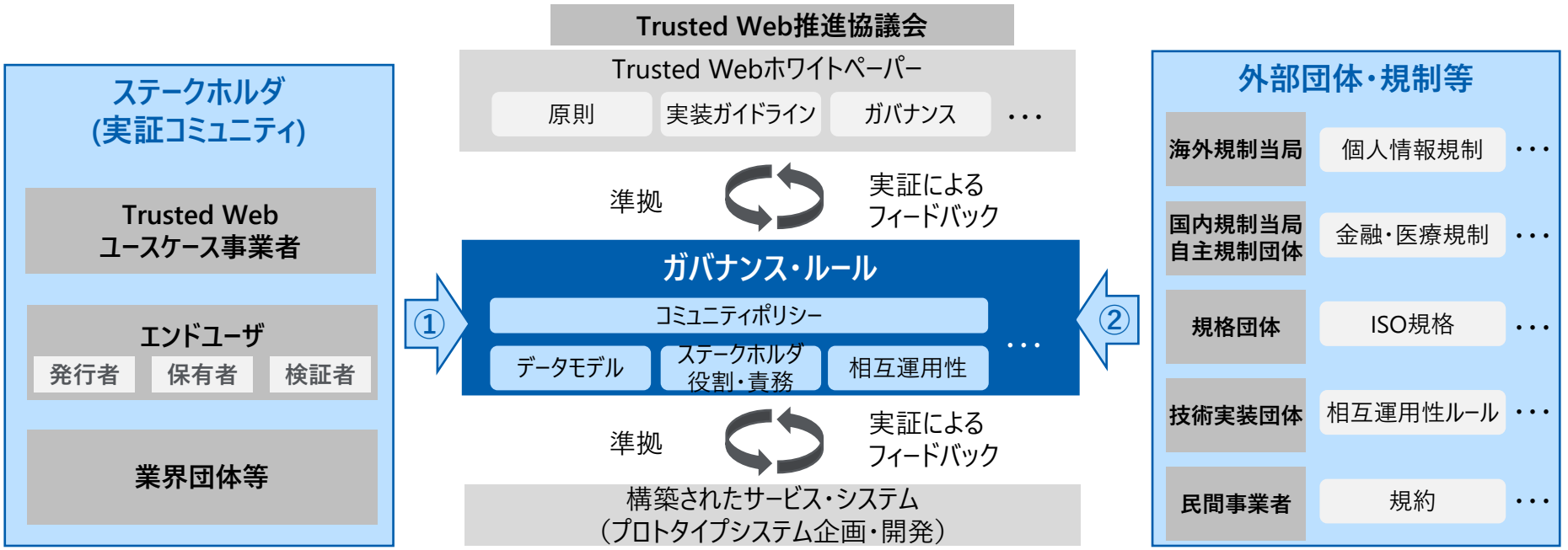
■ ウォレットの鍵管理の実現方式

- 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

- 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
- 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（RDB・IPFS・ブロックチェーン等）、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

6.1. 取組類型整理



ガバナンスルール策定

- トラストフレームワークの策定
  (ステークホルダ別役割・責務の整理)
- やり取りするデータモデルの標準化
- ウォレット等相互運用性テスト・ルール策定

- 本実証事業内で、OIDFコンフォーマンステストの支援を実施

①ステークホルダ内検証・協議

- ビジネスモデル・UI/UX・業務適合性検証
- 新規業界団体・コミュニティの設立、ポリシー策定
- 既存団体のシステム運用参画に向けた交渉
- 規格団体・技術実装団体へ発信・ルール整備の討議

②ベンチマーク調査・分析

- 海外・国内規制と規制当局調査
- 規格団体・規格調査
- デジタルアイデンティティに関するトラストフレームワーク調査
- 先行サービスのビジネスモデル・規約調査

- 本事業内で、OIDF、OpenWallet Foundation、OIX、EUDIWメンバとのとの相互運用性にかかる協議を実施
- 本事業内で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

6.2. ガバナンス・ルール策定実施概要（1/2）

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
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）
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）
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）
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）
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）
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

6.2. ガバナンス・ルール策定実施概要（2/2）

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
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）
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）
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）
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）
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）
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

6.3. ステークホルダ協議・ヒアリング等実施概要

代表機関	ステークホルダ（エンドユーザ）との協議・ヒアリング
DataSign	• OWND Projectの推進、ビジネスフィージビリティ検証として以下の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）
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）
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）
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）
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
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
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
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
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
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
JISA	• 補助金事務局事業者・補助金運営政府当局との協議
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

6.4. 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)

6.4. 調査分析等を実施したベンチーマーク先（2/2）

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	• 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

6.5.ガバナンス・ビジネス普及に向けた取組考察 – ガバナンス・ルール策定

主な成果

- 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(DNP)。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(電通総研)。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からいただいた

継続課題・今後の対応方針

- 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・ルールの策定を支援する取組が必要である
  - ➡ 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(事業者が検討すべき事項は次々頁参照)
- 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る
  - ➡ 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等が進められている
- 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
  - ✓ 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
  - ✓ 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
  - ➡ 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

6.5.ガバナンス・ビジネス普及に向けた取組考察 – 取組発信

主な成果

- 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）
- 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

継続課題・今後の対応方針

- 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、ユースケース実証が終わっても引き続き取り組んでいく必要がある
  - ➡ 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
  - ➡ 事業者の国際会議での発信や英語文書化にかかるインセンティブ設計が期待される

6.5.ガバナンス・ビジネス普及に向けた取組考察 – 社会実装に向けて留意すべき事項

検討の優先度：高 → 低

分類		ユースケースの社会実装に向けて留意すべき事項
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）

7.1. Trusted Webに関する事業者からの課題提起（1/3）

	事業者からの課題・提言
①持続可能なエコシステム	• 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	• 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オープンネスと透明性	• 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

7.1. Trusted Webに関する事業者からの課題提起（2/3）

	事業者からの課題・提言
④データ主体によるコントロール	• 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	• 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	• 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

7.1. Trusted Webに関する事業者からの課題提起（3/3）

	事業者からの課題・提言
⑦継続性	• 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	• 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	• 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	• 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。欧州のEU DIW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

7.2. 事業者がTrusted Webを具現化する上で有効な取組の提言（1/3）

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つの有効策としてあげられる（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

7.2. 事業者がTrusted Webを具現化する上で有効な取組の提言（2/3）

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、以下があげられる
  - データやり取りの主体間にunlinkability*1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）
  - 忘れられる権利への対応（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*2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）
- 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*3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*4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*5等が参考となる

*1 ISO/IEC 27551「Information security, cybersecurity and privacy protection - Requirements for attribute-based unlinkable entity authentication」https://www.iso.org/standard/72018.html
*2 OECD「Recommendation on the Governance Digital Identity」 https://www.oecd.org/governance/digital-government/oecd-recommendation-on-the-governance-of-digital-identity.htm
*3 例えば、デジタル庁におけるIAL見直し等が参考になる https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e1265816-bf26-4d65-963a-b3a853b587b0/52da0dac/20231127_meeting_identification-guideline-revision_outline_01.pdf
*4 ISO/IEC 29184:2020 Information technology Online privacy notices and consent https://www.iso.org/standard/70331.html
*5 Open Banking「Customer Experience Guidelines」 https://standards.openbanking.org.uk/customer-experience-guidelines/introduction/latest/）

7.2. 事業者がTrusted Webを具現化する上で有効な取組の提言（3/3）

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を用いて、その認証を受けている事業者をリスト化し他ユーザが事業者の真正性を検証できる仕組み（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）等があげられる

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
  - 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、現在の実装事例は別紙「規格動向調査」を参照
- 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 更改容易性・拡張性

- 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

すべてを突破する。

TOPPA!!!

TOPPAN