NTT DATA
Trusted Global Innovator

Trusted Web 共同開発支援事業に係る調査研究

報告書別紙　–Trusted Webの実現に向けたユースケース実証 分析レポート（概要版）

2023年3月31日

株式会社エヌ・ティ・ティ・データ経営研究所

ユースケース開発実証事業の成果物の取り纏めの方針

実証事業者から提出された成果報告書の骨子を踏まえ、①基本情報、②実証結果、③社会実装に向けた見通し、④Trusted Webに対する示唆・提言の4観点から実証成果の整理・分析を行った

実証事業の成果報告書骨子	成果の取り纏めにおける整理観点
1 背景と目的 2 事業の概要 2.1 事業概要及び実証の範囲 2.2 社会・経済に与える価値・影響 2.3 コンソーシアムの体制 2.4 実証全体のスケジュール	**①基本情報** ・対象市場、業界 ・検証対象とする主なデータ ・データのエンティティ（個人・法人・モノ） ・データの検証者
3 実証内容 3.1 実証の実施事項、論点及び判断 3.2 検証できる領域を拡大する仕組み 3.3 6構成要素との対応 3.4 本実証で企画・開発したシステムの概要 3.5 実証を通じて得られた主な成果 3.6 本実証で開発したシステムの第三者による再現可能性	**②実証結果** ・Trusted Webで解決できること・効果 ・実装する機能・非機能 ・データコントロール・ガバナンスの詳細 ・合意形成・トレースの詳細
4 実証終了後の社会実装に向けた見通し 4.1 社会実装時に想定しているビジネスモデル・ユーザーのメリット 4.2 実証を通じて判明したユースケースの課題とその解決方針 4.3 本ユースケースの社会実装に向けたマイルストーン	**③社会実装に向けた見通し** ・ユーザーの声（期待・ニーズ・課題・懸念） ・ビジネスモデル、プレーヤー ・実装マイルストーン
5 Trusted Webに関する考察 5.1 Trusted Webのアーキテクチャに関する課題と提言 5.2 その他Trusted Webの課題と提言	**④Trusted Webに対する示唆・提言** ・定義、戦略 ・実現手法、アプローチ ・サービス

01

基本情報

基本情報の整理①

本実証事業の公募を通じて13の事業者（ユースケース）の選定を行い、うち11の事業者でプロトタイプシステムの開発を実施した[1]。実証を通じて、従来検証が困難であった情報の検証性を確保を試みている。

No.	ユースケース	代表機関	対象とする市場・業界	検証対象とする主なデータ	データのエンティティ[1]	エンティティの詳細	検証者
1	**オンラインマーケティングにおけるパーソナルデータの流通**	**DataSign**	メディア	サイト閲覧者の非bot証明情報	人	サイト閲覧者	Webサイト運営者 広告事業者
				法人のOP証明情報	法人	サイト運営者 アドテク事業者	サイト閲覧者
2	**仮想現実空間におけるサービス利用資格と提供データのTrust検証**	**NRIデジタル**	エンタメ・サービス（メタバース空間で提供サービスによる）	メタバースを利用する人の属性情報	人	メタバースを利用する人	メタバース空間内のサービスを提供事業者
3	**学修歴等の本人管理による人材流動の促進**	**東大**	教育	受講証明データ	人	学生	大学、 （使用先）企業等
4	**人材育成のためのTrustedな学修情報流通システム**	**富士通Japan**	教育	研究実績・スキルデータ	人	学生	教員、 使用先企業等
5	**臨床試験及び医療現場における信頼性及び応用可能性の高い情報流通システム**	**シミック**	ヘルスケア・福祉	臨床試験データ	人	病院スタッフ	製薬会社/CROスタッフ 監査当局
6	**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流通システム**	**ORPHE**	ヘルスケア・福祉	歩行データ	人	患者	医療機関

注1）データのエンティティの区分は以下の考え方に基づくものとする
人　：対象データに対して自由なコントロール・意思決定が可能な個人が紐づく場合
法人　：対象データに対して自由なコントロール・意思決定が可能な法人・団体が紐づく場合
モノ　：対象データに対して自由なコントロール・意思決定ができない主体が紐づく場合

1) 大日本印刷とアラクサラネットワークスを除く11事業でプロトタイプシステムの開発を実施。なお、アラクサラネットワークスについては、企画のみを行う方式で選定したが、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ている。

基本情報の整理②

本実証事業の公募を通じて13の事業者（ユースケース）の選定を行い、うち11の事業者でプロトタイプシステムの開発を実施した[1]。実証を通じて、従来検証が困難であった情報の検証性を確保を試みている。

No.	ユースケース	代表機関	対象とする市場・業界	検証対象とする主なデータ	データのエンティティ[1]	エンティティの詳細	検証者
7	分散型IDを活用した炭素排出量トレースシステム	DataGateway	製造業・環境	炭素排出量	法人	炭素排出量開示企業	パートナー企業
				リレーションシップ証明書	法人	開示企業-パートナー企業の組み合わせ	お互いの企業
8	機械製品サプライチェーンにおけるトレーサビリティ管理	ヤンマーホールディングス	製造業	機械署名	人・法人	リペアショップ・ユーザー	製造メーカー
				機械の稼働データ	法人	製造メーカー	リペアショップ
				依頼内容	人・法人	機械ユーザー	リペアショップ
				修理レポート	法人	リペアショップ	機械ユーザー
9	Trusted Networkによる社会ITインフラの信頼性・強靭性向上の実現	アラクサラネットワークス	製造業	製品信頼情報（部品情報、ソフトウェア情報、設定情報等）	法人・モノ	機器ベンダインテグレータインフラ事業者	機器ベンダインテグレータインフラ事業者
10	ワークプレイスの信頼できる電子化文書の流通システム	東芝テック	製造業	文書データ	モノ	プリンタ（MFP）	文書管理システム
11	法人税制と工業会証明書	JISA	行政	補助金申請書類	法人	申請者	申請先、証明者
				従業員の所属情報	人	従業員	従業員の所属企業
12	中小法人・個人事業者を対象とする補助金・給付金の電子申請における「本人確認・実在証明」の新しい仕組み	電通	行政	補助金申請書類	法人	申請者	申請先、証明者
13	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	ヘルスケア・福祉	共助実績データ	人	サポーター（共助する人）	共助される人

注1）データのエンティティの区分は以下の考え方に基づくものとする
人　：対象データに対して自由なコントロール・意思決定が可能な個人が紐づく場合
法人　：対象データに対して自由なコントロール・意思決定が可能な法人・団体が紐づく場合
モノ　：対象データに対して自由なコントロール・意思決定ができない主体が紐づく場合

1) 大日本印刷とアラクサラネットワークスを除く11事業でプロトタイプシステムの開発を実施。なお、アラクサラネットワークスについては、企画のみを行う方式で選定したが、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ている。

02

実証結果

Trusted Webで解決・実現を目指す内容

- ユーザーによる**データコントローラビリティの確保**や、**データの検証性の確保**に関してはほとんどの事業者で共通して実現が目指されており、Trusted Webのシステムにおいて基本的な機能要件の一つであると考えられる
- 解決できること・実現できることの多くで、**安心感の向上**や**信頼性の確保**などが示されており、Trusted Webで目指す内容としては、**直接的に経済的な効果が評価しづいらい内容が多い**傾向にあると想定される
- 一方で、**検証済みの証明書（VC）の再利用**することによる**申請・承認プロセスの簡素化**など、定量的に経済効果を把握可能な効果も一部では見られた

データのエンティティ	Trusted Webで解決・実現を目指すこと	解決することによる効果	主な対象事業者
個人、法人	**データコントローラビリティの確保**	データホルダーの安心感の向上	電通、富士通Japan、ORPHE、NRIデジタル、DNPなど
個人、法人	**データ証明者（証明データの発行者）の検証性の確保**	データ証明者の信頼性の担保 データホルダーの安心感向上	富士通Japan、DataGateway、シミックなど
個人、法人	**検証者（データ提示先）の検証性の確保**	データ検証者の信頼性の担保 データホルダーの安心感向上	DataSign、DataGatewayなど
個人、法人	**データホルダーの検証性の確保**	データの信頼性の確保 データ利活用の促進	ORPHE、JISA、ヤンマーなど
個人、法人、モノ	**データの検証性の確保**	データの信頼性の確保 データ利活用の促進	電通、ORPHE、富士通japan、DataGateway、東大など
個人、法人	**データ共有・提示に係る合意形成**	正確なデータ取引の実現	DataSign、ORPHE、東大、DNP、電通、DataGateway
個人、法人	**検証情報、検証結果の再利用**	申請、検証作業に係る工数・コストの低減	電通、JISAなど
個人、法人、モノ	**データの耐改竄性の確保**	データの信頼性の担保 データ利活用の促進	アラクサラ、電通、シミック DataGatewayなど
モノ	**IoTデバイスのIDプロビジョニングの効率化**	デバイス管理者のコスト削減 脆弱性の排除	東芝テック
モノ	**・デバイスのルートオブトラストの確立 ・デバイスの暗号鍵管理**	暗号鍵管理の設計開発コストの削減	東芝テック

実装する機能・仕組み

- 分散型ストレージやウォレットを用いて、**データの分散管理を採用**している事業者多い
- **分散型識別子（DID）**を発行する機能についてもほとんどの事業者が実装しており、データの分散管理と合わせて、**データの自己コントロールの実現**を目指したユースケースが多い

機能・非機能	概要	主な実現手法・手段	主な対象事業者
機能	データの分散管理（データの登録・取得）	DWN、IPFSなどの分散ストレージでの管理、ウォレットアプリケーションによる管理	Datasign、Datagateway、アラクサラ、NRIデジタル、ORPHEなど
機能	分散型識別子（DID）の発行	ウォレットや各社ミドルウェア機能（CG EDGE、IDYX、Woollet、Keychainなど）で実装	東芝テック、富士通Japan、ヤンマー、シミック、ORPHE、Datagatewayなど
機能	検証可能な属性情報・証明書の発行・管理・検証	VC、OPの実装	電通、JISA、Datasignなど
機能	データの選択的開示	BBS＋署名など	東大、富士通Japan、ORPHE、DataGatewayなど
機能	本人確認・実在性証明	Microsoft Azure AD、生体認証など	富士通japan、ORPHEなど
機能	暗号鍵・検証鍵の生成・管理	ウォレットや各社ミドルウェア機能（CG EDGE、IDYX、Woollet、Keychainなど）で実装	東芝テック、Datagateway、ORPHE、ヤンマー、シミック、電通など
機能	メッセージ・トランザクションの記録	ブロックチェーンへのDID(Document）の登録 ウォレットのストレージへのメッセージ・トランザクションデータの格納	電通、アラクサラ、Datagateway、ORPHE、DNPなど
機能	メッセージ・トランザクションのトレース	メッセージ・トランザクション記録の検証・確認	電通、富士通Japanなど
機能	データのやり取りに関する合意の形成	システム・アプリケーションのUI（承認依頼・承認）で実装	富士通japan、東大、ORPHE、DataGateway、ヤンマーなど
機能	データのやり取りに関する合意の取消	スマートコントラクト	DataSign、電通、東大、シミック、ORPHEなど
非機能	可用性	オフラインでも自身の属性情報や開示履歴にアクセス可能な構成、システム稼働率の確保など	JISA、東大
非機能	拡張性	エンティティ数に応じたスケータビリティ確保など	東大、ヤンマー、DataGateway
非機能	セキュリティ	データの秘匿性確保など	ヤンマー、DataGateway

データコントロール・ガバナンスの考え方

- ほとんどの事業者（11/13）で**データを分散管理または一部分散管理する形態を採用**している
- 半数以上の事業者で**データホルダーによる選択的開示を実装**しており、また構想外・検討中とした事業者についても直近のニーズがないためとしており、実装に向けた技術的なハードルは大きくないと考えられる

No.	代表機関	データの管理形態（分散・集中）	選択的開示の実装	データガバナンス
1	DataSign	**分散的に個人が管理** （発行された非Bot証明VCや自身のパーソナルデータをDWN及びブラウザのエクステンションに保存し管理）	サイト閲覧者は、識別子と紐づいた属性を管理し、開示するパーソナルデータと開示先、利用目的の範囲を選択して開示	組織審査機関（JICDAQ等）がサイト運営者、アドテク事業者の正当性について審査 OPが検証された正当なウェブサイト運営者のみにアクセス権限を付与
2	NRIデジタル	**一部分散的に個人で管理** （暗号鍵等の一部のデータについてはユーザ同意の下、バックアップサービス事業者で管理する）	構想外	情報無し （仮想空間サービス事業者のガバナンスが存在するものと想定される）
3	東大	**分散的に個人が管理** （学習者が自身の学修データをPLRアプリで管理）	PLRアプリを拡張して複数のDIDを管理可能とすることで、学習者がDIDやVCを含むデータの範囲等を選択して開示	情報無し
4	富士通Japan	**分散的に個人が管理** （IDYX内のWalletにて管理）	データの選択的開示は部分的に可能／特定のスキル・活動内の情報非開示のコントロールは不可となるようにプロト実装	情報無し
5	シミック	**一部分散管理** （データの送受信が可能な病院スタッフと製薬会社/CROスタッフの組み合わせ情報はTrusted Directoryで集中的に管理される）	送信するファイルにどのデータを入れるかは病院スタッフが自ら選択可能であり、かつどのファイルを送信するかも選択可能	GAMP（Good Automated Manufacturing Practice）などの臨床試験におけるデータマネジメント及びシステム設計に関する国際規格及びレギュレーションによる全体的なガバナンスの影響が示唆
6	ORPHE	**一部分散的に個人で管理** （患者が自身の歩行データをウォレットで管理するとともに、ORPHEが管理者システムの中でデータのログを記録）	患者は（ORPHE経由で）医師等からデータの要求を受け、データの公開、拒否、部分公開をウォレットで選択可能	システム全体のデータ授受をORPHEが担っており、一定のガバナンスが存在すると想定
7	DataGateway	**分散的に法人で管理** （クライアントのエージェントサーバー（ウォレット：Woollet）の中でクライアントにより、IPFSに保管されているデータのハッシュを管理）	選択的開示はウォレット（Woollet）の機能として具備	データ所有者とデータ要求者との炭素排出量開示に関する契約によるガバナンスに基づくと想定
8	ヤンマー	**分散管理** （各エンティティのデータは各エンティティが保管し、必要な場合に直接開示依頼を受ける）	アプリ（ウォレット）のUIから開示先や開示期間を選択可能	機械ユーザの本人確認は機械製品の購入時に販売会社によって実施すると想定 その際に機械製品とのペアリングも実施する想定
9	アラクサラ	**分散管理** （サプライチェーンの中で各エンティティがセキュアストレージ（IPFS）で分散的に管理）	機器を調達した事業者のみに選択的に開示。 （権限管理の仕組みは独自実装）	データの取扱い等はTNP運用者と利用者との間の契約により規定されると想定
10	東芝テック	**集中管理** （文書管理システムの中で管理。MFP デバイスが識別子（DIDs）を発行し、電子化文書などの属性（データ）として管理）	構想外	データの取り扱いは、MFP機器の導入企業（管理者）とサービス提供者（東芝テック）との間の契約書などで合意
11	JISA	**分散管理** （法人・従業員のウォレットでVCを管理）	構想外	政府プロジェクトとの連携の必要性を提起しており、将来的には政府によるガバナンスも想定
12	電通	**集中管理** （申請者が収集した証明書等（VC）は共通のローカルストレージで管理）	申請者自身の選択的開示は今後検討予定	言及なし。共通のローカルストレージの管理者によるガバナンスが想定される
13	大日本印刷	**分散的に法人で管理** （クライアントのエージェントサーバー（ウォレット：Woollet）の中でクライアントにより管理）	ゼロ知識証明で必要な情報のみを選択開示することを想定	共助版のトラストフレームワークによるガバナンスの必要性を提起

合意形成・トレースの考え方①

- 合意の対象としては、**データの内容**に関して合意するケースと**データのやり取り**（提示・開示など）についての合意とするケースが見られた
- トレースについては、**合意の事実を履歴として見える化**するケースとデータ流れをトレースするケース（**データトレーサビリティ**）が見られた

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	Webサイト閲覧者とサイト運営者・アドテク事業者の間	Webサイト閲覧者のパーソナルデータ（広告識別子、メールアドレス）の利用範囲	可能 ※情報提供の撤回を行うことでDWN上のVCを削除	DWNに格納されたWebサイト閲覧者のパーソナルデータ取得履歴 ※履歴閲覧のみで実際の利用有無はトレース不可	DWNへのアクセス履歴の確認
2	NRIデジタル	①ウォレット（メタバースユーザ）とIssuer ②ウォレットと仮想空間サービス（事業者）	①VCとして発行する本人資格情報の内容 ②要求する本人資格情報の内容および利用用途	構想外 ※①UCには不要と判断 ※②廃棄依頼しても本当に廃棄したが確認不可なため）	合意の事実	①②履行された合意をウォレットで確認し、VC発行/提示履歴としてウォレット内に表示
3	東大	学習者と企業間	属性情報の開示	可能	データのやり取り（データ開示要請、それに対する同意/非同意など）の履歴	開示要請と開示の履歴の共有
4	富士通Japan	学生と指導教員や教授	スキル・活動に関する評価、およびコメント	構想外 ※技術的には可能	合意した事実 ※送付先（企業側）で正しく受領され検証されたかを学生自身がトレース	IDYXにて証跡を保持
5	シミック	データの送信側（病院スタッフ）と受信側（製薬会社/CROスタッフ）	互いに信頼しているということ及び信頼している間でのデータの授受	可能 ※クラウドストレージ（BOX）上の暗号化ファイルを管理者が削除することで合意を取消し	合意した事実	監査証跡の確認
6	ORPHE	患者と医療機関（医師）・研究機関	患者の歩行データの共有	可能 ※ウォレットで実現	合意した事実	ウォレットの機能として実現
7	DataGateway	サプライチェーン上のパートナー企業間	企業間のリレーションシップ、炭素排出量の共有	可能 ※パートナー企業間で合意しているリレーションシップクレデンシャルを取り消すことで実現	共有されたデータの流れ	Woolletの機能として実現

合意形成・トレースの考え方②

- 合意の対象としては、**データの内容**に関して合意するケースと**データのやり取り**（提示・開示など）についての合意とするケースが見られた
- トレースについては、**合意の事実を履歴として見える化**するケースとデータ流れをトレースするケース（**データトレーサビリティ**）が見られた

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
8	ヤンマー	①機械ユーザとリペアショップ ②リペアショップとメーカ	①修理内容（修理箇所、金額、納期） ②稼働データの開示	可能 ※合意の取消は取消の合意を持って実現している	合意した事実	①機械ユーザがアプリ上で確認（トレース） ②メーカがメーカアプリ上で確認（トレース）
9	アラクサラ	ベンダ・インテグレータ・インフラ事業者・Trusted Network（TN）運用主体の間	登録製品・サービス一覧、アセスメントレポート、製品信頼情報（TBOM）、製品信頼情報のレーティングの内容	可能 契約に連動してシステムにおける取消処理を実施	合意した事実、TBOMの内容及び所有権の遷移ステータス	ブロックチェーンに合意するデータを記録し、権限をもつユーザ(DIDで識別)が履歴を確認
10	東芝テック	合意形成、合意履行のトレースはユースケースの特性上、適用しない（適用が困難） ※データ取引履歴（特定のMFPデバイスから、いつ、どのユーザーが電子化文書を保管したのか）については文書管理システムのログを確認することでトレース可能				
11	JISA	中小事業者と設備メーカー、工業会、中小企業庁、所管税務署の間	VCの提示、及び提示先 ※申請者によるVC提示先の確認を以て合意とする	構想外	合意したVCが提示先に受け渡しされている事	法人および従業員が利用するWallet内にVC発行や提示に関する記録を実施
12	電通	申請者と証明者の間	VCの申請内容	可能 ※スマートコントラクトを利用して後からVCの取消が可能	やりとりされているメッセージ全て ※VCの有効状態の確認に活用	ローカルストレージ上のデータの読み取り
13	大日本印刷	共助アプリユーザ間、共助アプリ間	• 情報の提供可否 • 提供可能な情報 • 情報提供可能な第三者 • 提供した情報の有効期限 • 共助アプリ間の実績評価	構想外	共助に関する情報（VC）の流通量 ※地域の課題や状況のモニタリングに活用を想定	言及なし

実装の詳細　-属性情報、本人確認・実在性証明の手法について

- 属性情報の証明手法としてはほとんどの事業者（11/13）で**VCの署名検証**を採用している
- 本人確認・実在性証明については、**Azure ADの認証機能**や**スマートフォンの生体認証機能**を採用している事業者がいる一方で、机上検討としている事業者も多かった

No.	代表機関	属性情報の手法	本人確認・実在性証明の手法
1	DataSign	• 属性情報の証明手法としては**DID／VC（非bot証明）**及び**OP（サイト運営者、アドテク事業者）**を使用	• サイト閲覧者の本人確認については言及なし • サイト運営者、アドテク事業者の**実在性はJIQDAQなどの審査会社による審査**結果によって実在性を証明することを想定している
2	NRIデジタル	• 属性情報の証明手法としては**DID／VC**を使用（事前取り決めおよびID連携が必要なOIDCよりも、VCの提示による資格情報の授受を行う方が効果的であるため）	• VRゴーグルを利用している**「利用者の本人認証」を「没入感を維持したまま」実現することを課題**として解決方法を検討 • 予めPINコードを決定し、認証タイミングでVR空間に認証機能表示、ジェスチャーで矢印方向を入力する方法で解決可能と想定
3	東大	• 属性情報の証明手法としては**DID／VC**を使用	• 学生の本人確認としては、大学等でのリアルな認証を利用 • **大学等でのリアルな認証**に基づき、FIDO認証によって特定の端末と紐づけられたDIDを企業・大学等に提示することで本人認証を強化している
4	富士通Japan	• 属性情報の証明手法としては**DID／VC**を使用（富士通の分散型IDソリューションであるIDYXのサービス内で提供）	• 学生、指導教員、採用担当の本人確認方法として、**MicrosoftのAzure ADの認証機能を利用**
5	シミック	• **DIDと署名検証**によりセキュアなデータ共有を実現（属性証明は実施しないため**VCは未実装**）	• システム利用の前提として、臨床試験等を実施する上での**各種レギュレーション**の要求により、本人確認及び実在性確認が求められる。利用時は**ワンタイムパスワードによる本人認証**の実施を検討。
6	ORPHE	• 属性情報の証明手法としては**DID／VC**を使用	• アクセスするユーザーの本人確認としては**スマートフォンの生体認証**機能を利用
7	DataGateway	• 属性情報の証明手法としては**DID／VC**を使用	• プラットフォームに新規登録する法人の実在性確認を**GビズIDを利用した方法を将来的に実装する方向で検討** • アクセスするユーザの確認を**スマートフォンやPCでの生体認証**により実施する方法を検討
8	ヤンマー	• 属性情報の証明手法としては**DIDと用いた署名検証**を使用（VCの使用は明言されていない）	• 機械ユーザーの当人認証は**機械購入時に販売代理店にて実施**し、その際に機械製品とペアリングを行う想定
9	アラクサラ	• 属性情報の証明手法としては**DID／VC**を使用	TN利用契約締結・利用者登録時に本人確認・実在証明を実施
10	東芝テック	• 属性情報の証明手法としては**DID／VC**を使用	情報無し
11	JISA	• 属性情報の証明手法としては**DID／VC**を使用（VCの発行基盤としてはMicrosoft Azureを使用）	• 何らかの法人に所属する従業員の在籍確認手法により本人確認がなされていることが読み取れるものの、詳細な方法については言及なし • 法人の実在性については**GビズIDの活用を将来的に検討**する
12	電通	• 属性情報の証明手法としては**DID／VC**を使用	• 申請者の本人確認を市区町村による**対面での住民票発行**により実施 • これまで紙の証明書やスキャンデータの添付をして行っていた本人確認や実在証明を、住民票VC、口座実在証明VC、納税証明書VCのEdDSA署名を検証する方法を検討。その結果、VCの発行元と内容が改竄されていないかが確認でき、技術的に実装が可能であることを確認できた
13	大日本印刷	• 属性情報の証明手法としては**DID／VC**を使用	情報無し

実装の詳細　-ウォレットの実装、ブロックチェーンの活用について

- 10事業者でウォレットを実装しており、**属性情報や暗号鍵の保管**、**通信エージェント**としての機能を割り当てている
- DIDの登録先としてブロックチェーンを採用している事業者が多く、今回の実証においては比較的パブリックチェーンを採用している事業者が多かった

No.	代表機関	ウォレットの実装詳細	ブロックチェーン、分散台帳の活用
1	DataSign	**実装有り** metamask/eth-hd-keyringを鍵管理に用いたクロームエクステンションによりDIDの管理	**ION／Bitcoin**
2	NRIデジタル	**実装有り** スマホベース、NRIデジタルが保有するものを活用。VCを管理し、暗号鍵管理はバックアップサービスとして事業者によるアカウント管理	**ION／Bitcoin**
3	東大	**実装有り** PLRアプリをウォレットと呼称し、学習者のVC、暗号鍵管理、VPを生成・開示	**情報無し** （DIDはVerifiable Data Registry（MySQL）に登録）
4	富士通Japan	**実装有り** IDYX内のストレージ（ウォレット）で属性証明書（VC）を管理	**情報無し** （DIDはIDYXの共通台帳に登録）
5	シミック	**実装有り** 病院スタッフapp、制約会社/CROスタッフappとしてウォレットを実装 （やり取り可能なエンティティの組み合わせはTrusted Directory：Azure Serverで保管、データの授受はクラウドストレージ：BOXを使用）	**Keychain Core／Bitcoin**
6	ORPHE	**実装有り** DataGatewayのWoolletベースでウォレットアプリを実装しており、VCの管理（Hyperledger Ariesベース）に加え、暗号鍵管理を実装と想定	**Woollet Blockchain Network（Hyperledger Indy）** ※トークンの登録にはAstar Networkを使用
7	DataGateway	**実装有り** ローカルウォレット（Woollet）でVCを管理	**Woollet Blockchain Network** （Hyperledger Indy）
8	ヤンマー	**実装有り** 各エンティティのデバイス（ウォレットアプリケーション）のストレージでDID及び暗号鍵を管理	**Keychain Core／Bitcoin**
9	アラクサラ	**実装有り** Quorumにアクセスするノード(エンティティ)に対して、ウォレットを生成	**Quorum** （非公開要件への適合、ノード間のネゴシエーション機能を備えているため）
10	東芝テック	**情報無し** （通信ノードはCG EDGE、DG HUBが担当）	**ION／Bitcoin**
11	JISA	**実装有り** VCや暗号鍵をウォレットアプリケーション（Node.js）で管理	**ION**
12	電通	**実装無し** X25519などによる鍵合意（鍵共有）に対応していないためウォレットは実装しない設計とした（秘密鍵の管理はローカルストレージで実施）	**Algorand**
13	大日本印刷	**実装有り** ウォレット（Hyperledger Ariseベース）でVC、暗号鍵を保管	**Hyperledger Indy** （DIDとと紐づいたVCに関連するデータが名寄せされる可能性があり、プライバシーリスクが高まる懸念点があったため、分散台帳等で公開されないHyperledger Indyを参照している）

実装の詳細　–まとめ・考察

■ データコントロール・ガバナンスの考え方

- 本実証では、半数以上の事業者（8事業者/13事業者）が個人または法人によってデータを分散管理する形態を採用
- 一部分散管理とした3事業者については、暗号鍵のリカバリーのためにバックアップストレージを設け、その管理を第三者（ストレージ管理者）に依拠しているパターンやデータ利活用のためにサービス事業者がデータホルダーの同意に基づいてやり取りするデータをログとして管理しているパターンなどが挙げられる

- 分散管理をする上でのデメリットとしては、複数のデバイスで管理されているデータの完全な同期を担保するための設計・実装コストが嵩むこと、分散管理されたデータを（特に個人が）管理するには従来よりもリスク・負荷が大きくなることが挙げられる
- 特にパーソナルデータや暗号鍵のようなセキュアな管理が求められるケースでは、個人が管理を担う行うことは大きなリスクであり、データコントローラビリティを個人に与えることの価値とのバランスを経済性・運用性の観点も踏まえて正確に評価することが必要と考える

- ある事業者で実施したユーザーヒアリングの結果からは、一部の企業によってデータを集権的に管理することに対して課題感を感じない、とする意見も見られており、ニーズの強さも考慮要素となる
- Trusted Webではデータコントローラビリティを機能要件の一つとして掲げているが、データコントローラビリティに対するTrusted Web構想としてのスタンスをどうするのか（前提とするのか、任意とするのか）を明確に事業者に示していくことが、今後の実装を事業者が担うことを踏まえると有効であると考える

- データの検証性やトラストの担保に向けて、法規制等によるガバナンスの必要性を掲げている事業者がいくつか見られ、中には共通トラストフレームワークの必要性を言及している事業者もいる
- 今回のプロトタイプシステムにおけるデータやシステムにおけるガバナンスの前提については、全ての事業者で明確に設定はしていないものの、一部の事業者では物理的な契約によってサービスの利用に対するガバナンス（例：データの取扱いに関する合意、データへのアクセス権の付与など）を図ることとしていた
- 今後サービスとして実装していく上では、「ガバナンスをどのように確保していくのか」、「どの程度ガバナンスによって統制を図っていくべきであるのか」について、いずれ詳細な検討が求められると考える
- また事業者側からのインプットとして、どのような内容をガバナンスで担保していく必要があるのか、そしてそのガバナンス・ルールの案を具体的に示していただくことが、今後の検討を有効に進めていく上で重要であると考える

実装の詳細　–まとめ・考察

■ 合意形成・トレースの考え方

- 合意形成に関与する主体（合意の範囲）としては、いずれの事業者も事業スキームに登場するステークホルダーの範囲内に留まっており、サービス・システムで想定していない第三者を含む合意形成（例えば、データホルダーのデータ共有先からさらに別の第三者にデータ共有される時に、データホルダーの合意に基づいて共有される仕組み）までをコミットしている事業者は確認できなかった
- これは技術的に課題があることも考えられるが、そもそもサービスのスコープとして第三者へのデータ共有を考慮していないためであると考えられる。他方、今後社会実装や横展開による市場拡大を考えた時に、データの利活用範囲を拡大しようとする動きは基本構想内であると想定されるため、第三者も含めた合意形成の実現に向けた方法を整理することは、今後の実装性を高める上では有効と考える

- 合意の取消についてはいずれの事業者も技術的には可能としていた（スマートコントラクトを用いる場合と合意の取消に関する合意をUIに実装するパターンがあった）
- 他方、いくつかの事業者については、合意の取消を実装するニーズがないとして構想外としている。データの内容について合意を図っている事業者に関しては、合意を取消したとしてもデータが共有された事実は変わらず、また破棄を求めたとしても実際に破棄されたことを厳密に確認する術はないことを構想外とした理由としている

- トレースの対象としては合意した事実のトレース（合意履歴をUI上で確認するケース）と合意履歴に加えてやり取りしたメッセージの内容までトレースしているケースが見られた
- 本事業内で想定しているトレースは、同サービス・システム内のステークホルダーが、自らのやり取りの履歴を後から確認できることを指していることが主であり、いわゆるデータトレーサビリティで担保されるデータの第三者利用のトレース・利用の防止までをコミットしたケースは見られなかった
- より実用的なサービスを考えると第三者まで含めたデータトレーサビリティが担保されたシステムの実装を目指すことが重要と考えるが、実装コストやそれを必要とするユースケースの数を考慮した時に、Trusted Web構想の中でどの程度時間を割いて検討するかは協議が必要であると考えられる

実装の詳細　–まとめ・考察

■ 属性情報の証明手法

- 今回の実証事業では、全ての事業者でDIDを採用し、かつ13事業者中11事業者がDIDとVCの組み合わせを属性情報の証明の仕組みとして採用している
- 今回の実証事業の中ではVCの採用に際して、他の手法と比較評価をした上で採用しているケースはなく、次年度の実証事業の中では他の手法の評価もしくは比較検討した上で何故その技術を採用することにしたのかを、明確化することが重要と考えられる

■ 本人確認・実在性証明の手法

- 本人確認・実在性証明の実装については、Azure ADの認証機能を利用しているケースやスマートフォンの生体認証を利用しているケースが見られた一方で、対面による確認を前提としてプロトタイプシステムの構築を行った事業者もあった
- 一部の事業者ではGビズIDの採用可能性について言及しており、将来的な連携が想定される
- メタバース空間における認証サービスのユースケースに取組んだ事業者からは、没入感を維持した本人確認の必要性を課題として掲げており、ユースケースの内容によって、本人確認に求める要件の差異があることが改めて確認することができた

■ ウォレットの実装、ブロックチェーンの活用

- 13事業者中11事業者でウォレットの使用について言及があり、ウォレットの機能としては属性証明（VC等）や暗号鍵を管理する通信ノードとして位置付けられていることが大半であった
- 本実証事業の中ではウォレットの定義について明確に示しておらず、ユースケースの実現に必要な機能をボトムアップで事業者に構築を求め、構築されたシステムに対してウォレットの使用有無を確認する形でウォレットの機能範囲を確認する形となった
- 各事業者ともに、ウォレットに対して明確な定義を定めていない一方で、いずれの事業者もＶＣや暗号鍵を管理するデバイス、データ通信する上でのエージェントとして、ウォレットを活用していた

- 今回は全ての事業者でDIDを採用していたため、DIDの登録基盤としてブロックチェーン／分散台帳またはVDR（Verifiable Data Registry）を活用している
- 今回の事業においてはbitcoinベースのパブリックチェーンを使用している事業者が比較的多かったが、アラクサラや大日本印刷、DataGatewayなどはパーミッション型（プライベート型）のQuorumやHyperledger Indyをそれぞれ採用しており、今後実証事業を行う場合は、そのメリット・デメリット（名寄せのリスク・実装コスト等）を整理していくことが、他の事業者も含め、システムの設計を検討する上で有効であると考える

03

社会実装に向けた見通し

ユーザーの声（期待・ニーズ、課題・懸念点）

No.	代表機関	ヒアリングの対象	主なヒアリング結果
1	DataSign	サイト運営者、アドテク事業者	➢ 取組は素晴らしいが、すぐに全てを社会実装することは難しい。データ送信の際にOPが必須となると、現状のwebサイトが正常に動作しなくなる ➢ サイト運営者、アドテク事業者に対する審査機関による審査方法が課題である ➢ DIDやDWNという言葉の説明を加えるか、もしくはそれを意識させないUXの構築が社会実装に向けては必要 ➢ パーソナルデータの提供条件設定は一般の利用者にはハードルが高いと思われる。利用者の性格・属性に合わせて自動設定できる仕組みが望ましい
2	NRIデジタル	ヒアリング未実施	
3	東大	ヒアリング未実施	
4	富士通Japan	学生、教員、大学のキャリアセンター、採用センター	➢ 一部の企業が個人情報を保有していることについては、サービスが便利になるのであれば構わない ➢ 自分の何の情報がどのように使われているのかよくわからないことに不安を感じる ➢ 個人情報の取り扱いに敏感な一部の人だけが問題視していると感じる ➢ 学習履歴を採用にどのように生かすかについて企業と議論を継続している ➢ 評価者の信頼性についても議論が必要 ➢ 研究室での学生の成果物が、確かにその学生のものであることが証明できるようになると良い ➢ あまり細かな入力を必須とすると、評価を入力する教員の負荷が上がるため、システムの採用が進まないことが懸念 ➢ 学生が学んだことやスキルを漏れなく評価すること、定性的なソフトスキルを評価可能にすることで新たな検証可能領域を創出 ➢ スキルと履修科目の紐づき及びその学習深度を定量的に評価する事、及び社会人基礎力をベースとしたソフトスキルの評価によって企業側採用担当が検証可能な領域を新たに創出＝企業にとっての価値に繋がる
5	シミック	医療機関担当者、某大学の医療情報部門責任者・担当者、社内のデータマネジメント担当者	➢ 病院やアカデミア主導で実施する臨床研究や疫学調査など、低コストでの計画及び実施が要求されるため現状ではデータインテグリティを担保できていない試験に対しては現状のものでも十分有用性がある ➢ データの改ざんやなりすまし行為が根本的に実施不可能な環境にすることができれば、医療機関だけでなく治験依頼者及びCROの立場にとっても有用であるものの、現時点で要求されているデータインテグリティの考え方と比較するとオーバースペック ➢ データの扱いに関する透明性が保たれていれば、患者のデータ提供意思が向上する可能性がある
6	ORPHE	大学病院医師、理学療法士、リハビリテーション病院の理学療法士、製薬会社の新規事業企画担当	➢ 製薬会社などでエビデンスとしてデータを活用したい場合は同意の撤回によってデータにアクセスできなくなることはビジネス上大きなデメリットになってしまう ➢ 労災認定の場面など、医師にとっても患者のデータの確からしさが重要な場面がある ➢ 歩容や痛みのデータの共有については不安は感じないが、位置情報の共有には相手を選びたい ➢ 既存の信頼できる歩行データの有用性に関するエビデンスを提示すれば、メリットを訴求できる可能性がある
7	DataGateway	炭素排出量提示先企業	➢ データ連携を行う上で、国などが相手の場合は別だが、企業・個人が相手になると怖さがある。提供先の信頼性検証を可能にすることでデータ連携を促進できる ➢ データ連携に向けては社会貢献だけでは難しく、減税などの直接的なインセンティブがあれば検討する

ユーザーの声（期待・ニーズ、課題・懸念点）

No.	代表機関	ヒアリングの対象	主なヒアリング結果
8	ヤンマー	ヒアリング未実施	
9	アラクサラ	インテグレータ、ベンダ	➢ 社会的価値はある、あるいは改善次第で価値を出すことは可能 ➢ すぐにでも必要である業界とそうでない業界に分かれると考えている ➢ 社会的価値を高めるには、技術だけでなく、制度面と一体となった普及活動が必要。エコシステムに向けての仲間つくりが必要。 ➢ 法的にではなく、実際に需要がある業界について深掘りし、よりニーズに合ったシステムにカスタマイズしていくことが必要
10	東芝テック	地方自治体、東芝テック MFP営業部	➢ 財務文書や行政文書などの原本管理が求められる紙文書のデジタル化が進んでいない ➢ 従業員が受け取る領収書の原本保管など、経理・財務系の紙文書の保管は継続して必要
11	JISA	証明書交付事務局（JISA）	➢ ソフトウェア機能要件の確認や、関係官庁等からの問い合わせを申請書類と照会する処理が煩雑で、VCの属性情報として必要な証明事項を検証し、証明書同士の紐づきを認定番号で管理することによって事務処理の簡易化への期待がある
12	電通	地方銀行、地方自治体、補助金・給付金事務局	➢ 証明書発行業務、受取業務などの事務処理の効率化が期待できる ➢ 地方の人手不足対策に有効である ➢ 電子証明化により必要な項目のみ指定、限定した上で改ざんが困難な証明が発行される仕組みは魅力的である
13	大日本印刷	共助アプリ事業者	➢ 徐々に利用者数が増えるにつれて性善説でのトラストの検証には限界が来る ➢ データ連携を実施するために発生する開発費や、その検討に要するコミュニケーションコストが実施の課題になる ➢ 共助アプリが生み出すトラストの仕組みを個人間のやり取りにおいても検証可能にすること、及び学生の就職・入試におけるボランティア参加実績証明のための共助実績の活用によって、新たなサービスの創出に繋がる

社会実装に向けたマイルストーン

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	対象市場・業界	2023年度	2024年度	2025年度以降
DataSign	広告・メディア	ｴﾝﾄﾞﾕｰｻﾞｰへの訴求、組織が審査を受ける利点の訴求、ﾎﾟｯﾌﾟｱｯﾌﾟ合意への対応 実証・試験運用		ｴﾝﾄﾞﾕｰｻﾞｰへの訴求の対応 広告業での商用化／市場拡大
NRIデジタル	サービス全般	継続的な実証・ステークホルダ候補へのヒアリング・ビジネスモデルの見直し		商用化開始／市場拡大
東大	教育	明確なマイルストーンまでは未提示		
富士通Japan	教育	課題対応/目標に基づく実証	学生を対象としたサービス開始	社会人対応/マッチング機能強化
シミック	ヘルスケア	課題対応・UI/UX向上（継続的に改善） 実際の臨床研究での検証	サービス運用開始	
ORPHE	ヘルスケア	小規模な臨床現場での活用 治療の最適化効果の検証	実用化	横展開
DataGateway	モノづくり	継続的な実証（炭素排出量計算の義務化産業領域）		商用化
ヤンマー	モノづくり	サプライチェーン上の他のユースケースの検討、システム実装の規模の最適化、導入検証、展開判断		
アラクサラ	モノづくり	国際価値検証・公的機関との交渉 商用化に向けた実証	特定分野での商用化	他分野への横展開
東芝テック	モノづくり	MQTTデータサイズの検討、MFPアプリUIの検討・PoCの実施		商用化検討
JISA	行政	未定		
電通	行政	クラウド上で稼働するシステム開発検証、社会実装に向けた調整（βテスト、機能改善、導入検証）		社会実装
大日本印刷	社会福祉	共助アプリコンソーシアムの設立、ガバナンスルールの合意・運用 UI・UXの設計、リカバリー方法の検討	商用化	大学・企業に対して共助実績をデジタル証明書として発行

ビジネスモデル・プレイヤーマップ

※**青字**：本事業への参画企業・団体

ビジネスモデル	プレイヤー	
エンドユーザー（関連ステークホルダ）	・MFPユーザー ・メタバースユーザー ・患者、医療機関、研究機関 ・学生、大学、使用企業 ・証明書発行団体、中小法人、補助金事務局 ・炭素排出量開示企業	・設備メーカー、中小事業者、補助金事務局 ・製品ユーザー（部品サプライヤー、製造工場、販売会社、保守サービス事業者） ・病院/病院スタッフ、製薬企業/CROスタッフ ・共助アプリユーザー ・基幹インフラ事業者 ・Webサイト閲覧者、サイト運営事業者、アドテク事業者
サービス・システム（アプリ） ↑ サービス・システム（アプリ）代金 or 利用料 ↓		
サービスプロバイダ・アプリケーションプロバイダ	・東芝テック（MFPメーカー） ・KDDI（仮想空間提供） ・ORPHE ・JISA ・ヤンマーホールディングス ・シミック	・電通 ・大日本印刷（共助アプリベンダ） ・Trusted Network Provider（公益的第三者：IPAなど）
ミドルウェア・API提供 ↑ ライセンス料 or 月額利用料 ↓		
システムベンダ（ミドルウェア・API・OS・ネットワーク）	・CollaboGate Japan ・Keychain ・BlockBase ・伊藤忠テクノソリューションズ ・Cycaltrust ・アラクサラネットワークス	・ISID ・東京大学 ・ヤフー
参照規格・トラストフレームワーク	・Verifiable Credentials Data Model v1.1 （W3C） ・VC Implementation Guidelines（W3C） ・Decentralized Identifiers (DIDs) v1.0（W3C） ・DIDComm Messaging v2.0（DIF） ・Sidetree v1.0.0（DIF） ・Well Known DID Configuration（DIF） ・ISO/IEC 18033（ISO/IEC）	・OpenID for VC Issuance（OIDF） ・OpenID for VP（OIDF） ・SIOP v2（OIDF） ・GAIN Trust Framework（GAIN） ・OIX Guide to Trust Frameworks for Smart Digital Identity（OIX）

・DataSign
・DataGateway
・NRIデジタル
・富士通Japan

社会実装の見通し　–まとめ・考察

■ ユーザーの声

- トラストを担保する上での源泉として、データ共有に関する不安・怖さというのが、実際のユーザーの声として確認できた
- 自分の情報がどのように使われているか分からないことに対する不安を感じるとした学生がいる一方、別の学生からは、サービスが便利になるのであれば一部の企業がデータを保有していても構わない、といった声が挙がっており、ユースケースや共有するデータの質、個人の考え方に応じて、Trusted Webに対する期待感には差があるものと考えられる
- 「同意の撤回によってアクセスできなくなることはビジネス上大きなデメリットになってしまう」という声について、トラストの担保と経済合理性がトレードオフとなるケースがあることが読み取れる
- Trusted Webの実装を進めていく上では、信頼性の確保と経済性の両面から検討が必要になると考えられる

■ 社会実装に向けたマイルストーン

- プロトタイプシステムを開発した事業者については、いずれも社会実装に向けた残課題があるとして、2023年度においては（未定とした2団体以外の）全ての事業者で課題への対応・継続実証の実施を行う計画としている

- ヘルスケア領域を対象として実証を行った2事業者については、2024年度から初期の実装・商用化を開始する計画としており、ニーズや扱うデータ（ライフログデータなど）の面で同領域とTrusted Webの親和性の高さが伺える
- 他方、業界特有の法制度やパーソナルデータを扱う場合の留意点に関しては整理すべき内容が残っていると考えられるため（証明情報として個人情報を発行する場合に、発行者が確認すべき本人確認レベルなど）、対象事業者が円滑に社会実装を進められるように、Trusted Webの取組の中でも、引き続き議論していく必要があると考える

- 教育の分野においては、2事業者で類似したユースケースの開発に取り組んだものの、片方が2024年度からの初期実装を計画しているのに対して、もう片方の事業者は明確な実装に向けたマイルストーンまでは示していない
- 類似するケースの展望等について意見交換を行うなどにより、社会実装に向けたノウハウを共有していくことが望ましいと考えられる

社会実装の見通し　–まとめ・考察

■ ビジネスモデル

- ユースケースによって参画するステークホルダーの数や種類、マネタイズ方法は異なるが、Trusted Webに関するサービスやアプリケーションを商材として、サービスプロバイダー・アプリケーションプロバイダーが直接、もしくは国・自治体などのステークホルダーを通じて間接的にエンドユーザーに価値提供する形で、ビジネスモデルを作成している

- サービスやアプリケーションの具現化に際しては、システムベンダが主体となってミドルウェアやAPIをライセンス売り切るパターン、もしくはサブスクリプションとして提供するパターンがマネタイズ方法として考えられている
- Trusted Webの具現化に向けては、サービスプロバイダーとシステムベンダが担うケイパビリティが不可欠であり、分野・業界の観点も踏まえたプレイヤーマップの精緻化とマッチングを促進するコミュニティの形成が有効と考えられる

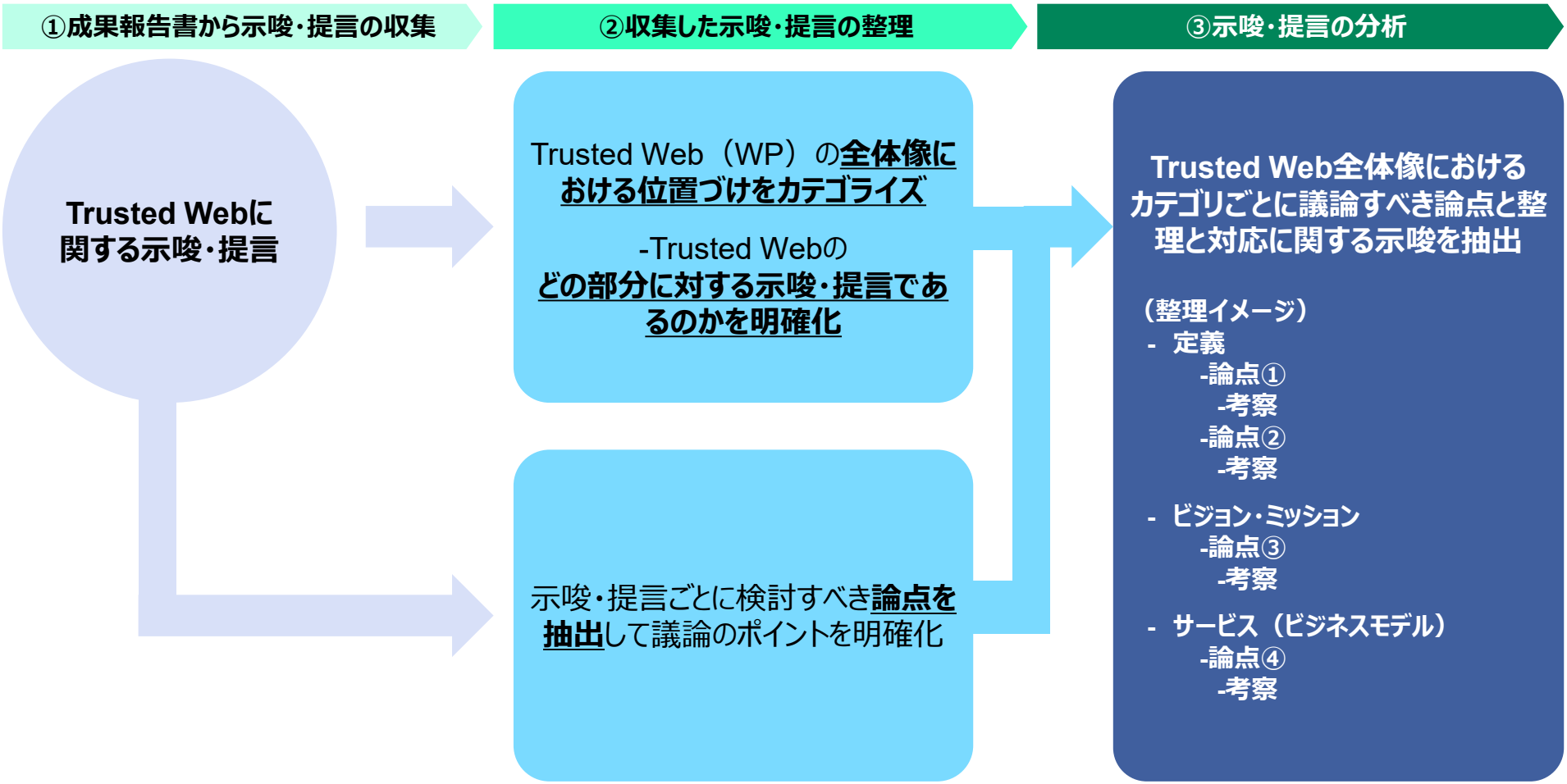
- また、本実証事業に応募した事業者の中で、エンドユーザーを含んでいるケースはわずかであった
- 社会へのTrusted Webの価値の訴求に向けては、ユーザーサイドを参画させた上で、ユーザーによる効果・価値の算定を含む実証事業の実施が有効と考えられる

04

Trusted Webに対する示唆・提言

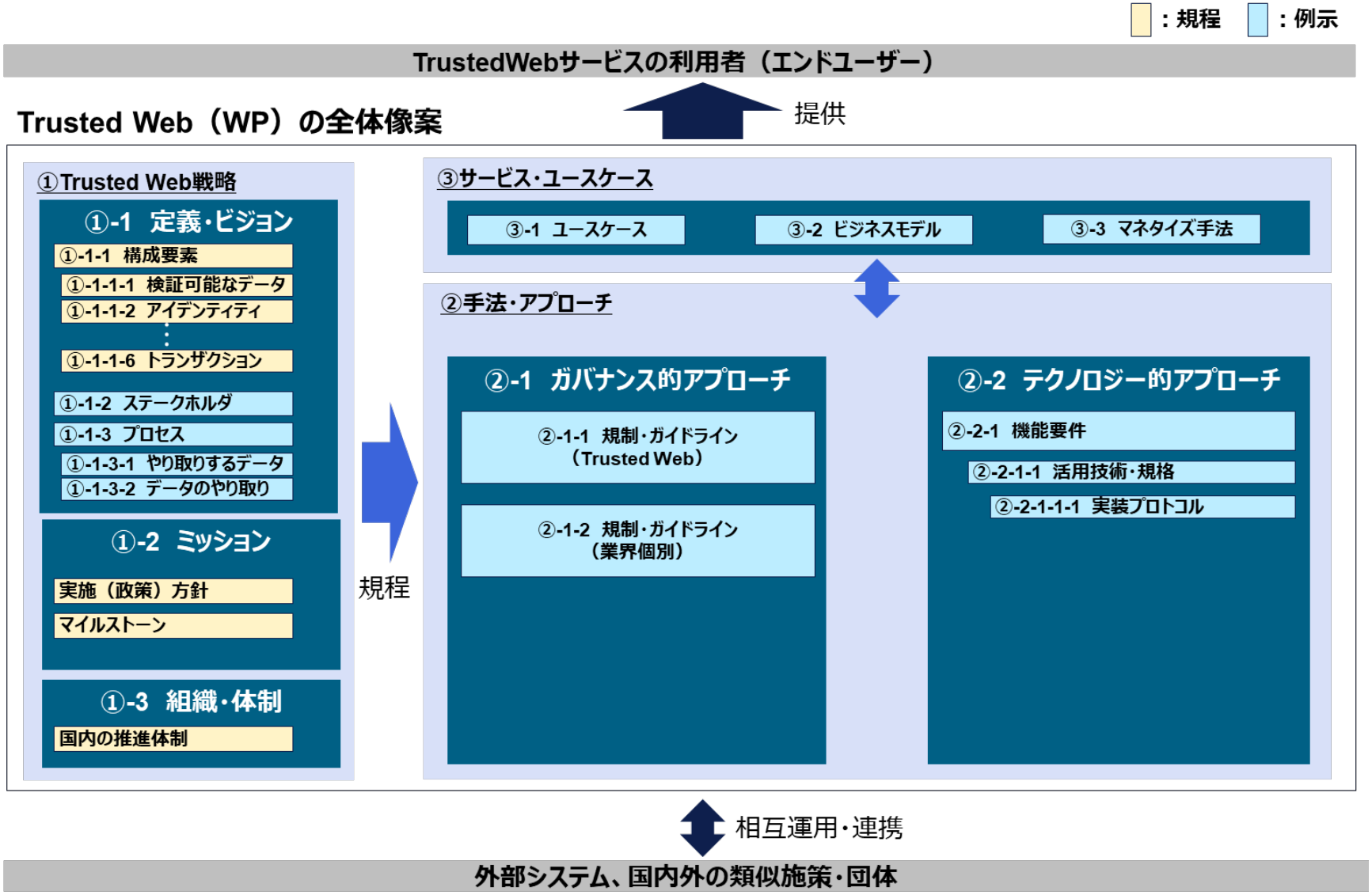
示唆・提言の整理要領

各事業者から報告されたTrusted Webに対する**示唆・提言を収集**、**Trusted Webの全体像に照らして整理**を行うとともに、**示唆・提言から論点を抽出**することで、Trusted Webで取り組むべきポイントを明確にしながら、具体的な対応方針を検討する



Trusted Webの全体像（案）

Trusted Webを具現化する上で明確にする必要のあること、取り組む必要のあることの観点から、Trusted Webホワイトペーパーで定めるべき内容を意識して項目の抽出、項目間の関係性を考慮して全体像のイメージを作成した



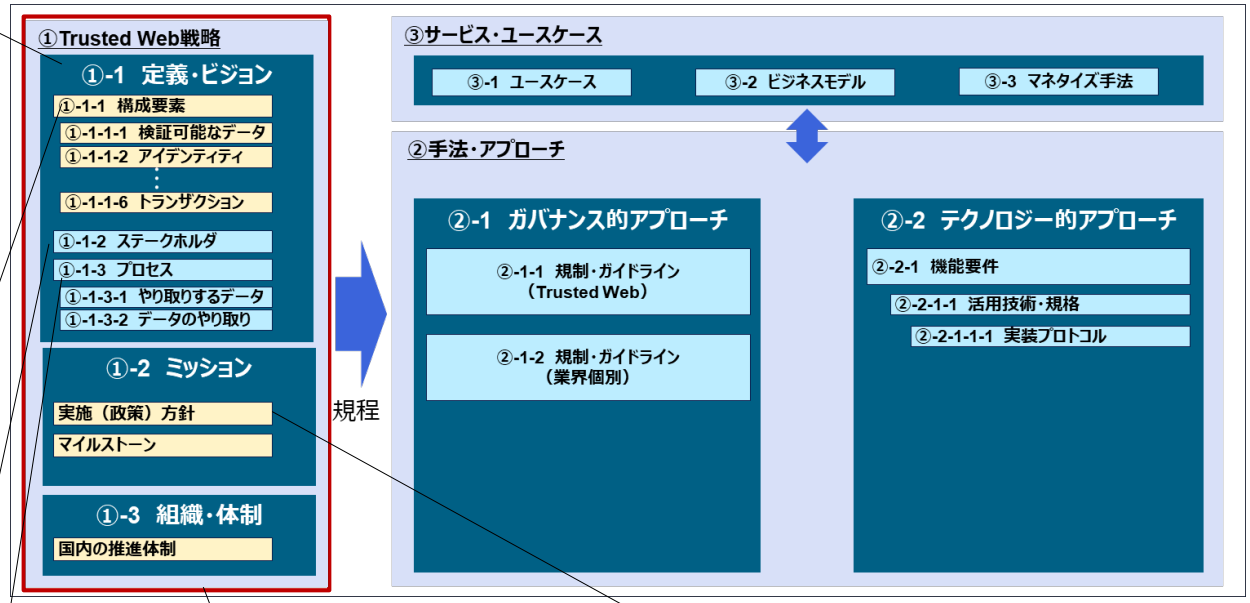
示唆・提言の整理①　-Trusted Webの戦略

（定義・ビジョン全般）
- 「検証可能性」の定義・考え方の明確化
- トラストの対象と内容の明確化
- 用語の定義の明確化、平易な表現への見直し
- 実装プロトコルに関する位置づけの記載表現について
- 議論する上での前提の排除（再設定）の必要性
- Trusted Wedで充足が必要な要件の明確化
- Trusted Webによるメリット・効果/デメリット・リスクの具体化
- セキュリティ/プライバシーを含めた目指すべき姿の明確化
- モノをエンティティとした場合の要件（目指す姿）の設定

（構成要素）
- 構成要素の定義の明確化
- パーソナルデータを扱う場合の構成要素（アーキテクチャ）の考え方
- アイデンティティを使い分ける場合の扱い・考え方
- トランスポートプロトコルの選定基準
- VCフォーマットや属性名の定義の必要性
- モノのアイデンティティの取扱いに関する考え方
- アイデンティティグラフの活用場面・方法の定義
- Walletを共同利用する際の権限について
- やり取りされるデータの定義・標準化
- VC（検証可能なデータ）の有効期限について

（ステークホルダ）
- パーソナルデータを扱う場合のIssuerの要件
- Trusted Webを評価する主体・仕組み

（プロセス）
- 自己主権型のデータ管理・コントロールの実現方法
- プロセス（合意履行のトレース）の定義・考え方の明確化
- 合意履行のトレースにおけるデータトレーサビリティの考慮
- パーソナルデータの保管ルールの考え方・規定について
- 暗号鍵管理に関するガイドラインの明示の必要性
- 暗号鍵管理に関する課題
- Trusted WebにおけるKYCの位置づけ、考え方
- KYCの実現手法について
- Wallet間のインタラクション、Wallet及びWalletユーザーの信頼性担保について
- 当人性認証の信頼性強度の考え方、方法について

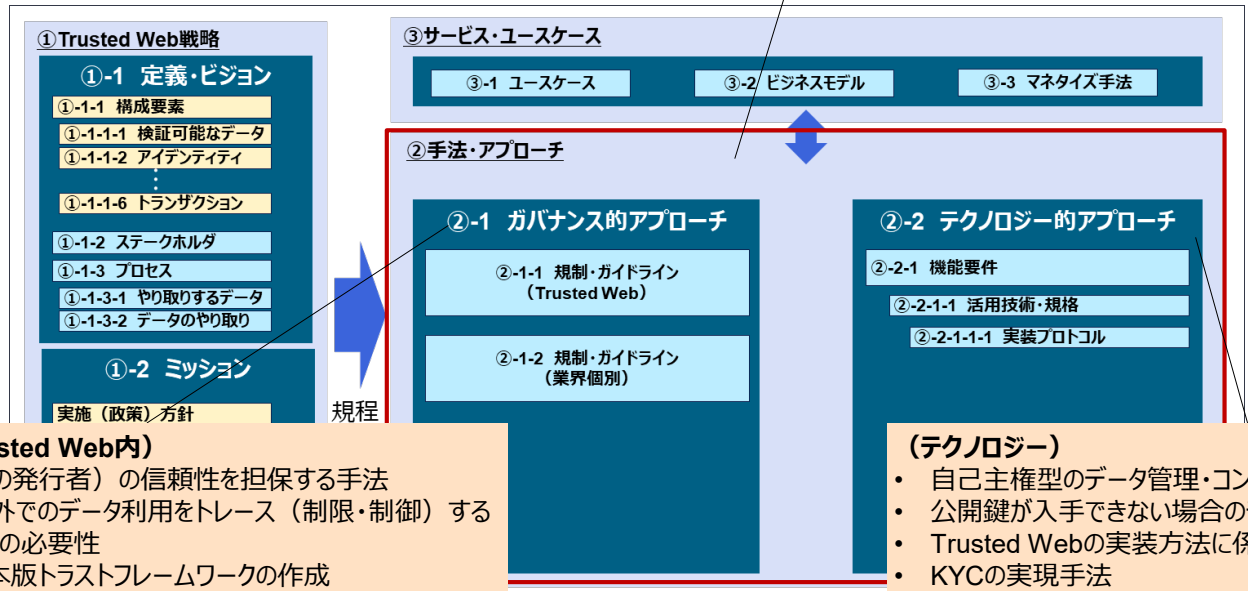


（組織・体制）
- Trusted Webの推進に係る国の関与の必要性について
- Trusted Webのオープンコミュニティの組成

（ミッション）
- Trusted Web SDKの開発・普及に向けた取組
- 一般ユーザ・企業向けてのPRコンテンツの制作
- Trusted Webの国際的な合意に向けたロードマップ
- 一般消費者に対するリスク（情報漏洩、なりすまし等）の周知

示唆・提言の整理②　-Trusted Webの手法・アプローチ

（実装手法・アプローチ全般）
- Trusted Webの要件に対する実現手法・アプローチの整理
- 実装方法・方針に対するWPの記載粒度・強制力
- データの特性に応じた信頼性担保の手段の選定
- 特定のコミュニティにおけるデータ、データのやり取りのトラストを担保する方法
- 収益性を考慮した実装手法の検討
- Walletを紛失した場合のリカバリー方法



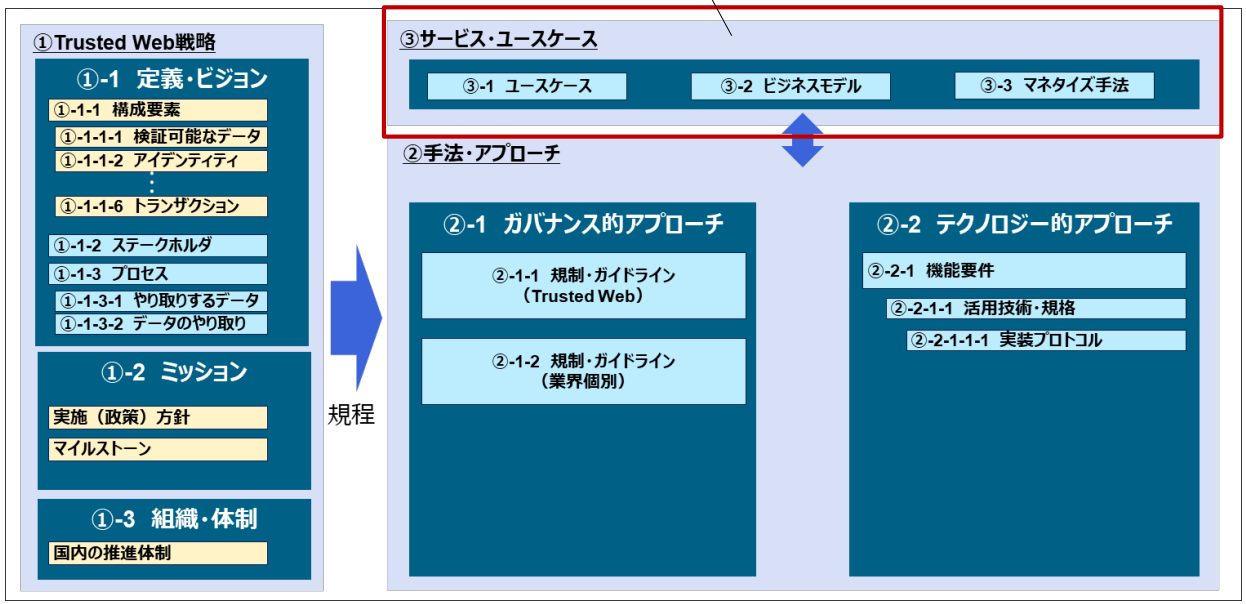
（ガバナンスーTrusted Web内）
- Issuer（データの発行者）の信頼性を担保する手法
- 合意履行範囲外でのデータ利用をトレース（制限・制御）するためのガバナンスの必要性
- 業界横断の日本版トラストフレームワークの作成
- Trusted Web（分散型ID）における個人情報保護に関する規定の必要性
- ユーザーによる秘密鍵管理を規定するルールの検討

（ガバナンス一業界個別）
- ヘルスケアデータの信頼性担保の仕組みの標準化、ガイドラインの策定一般ユーザ・企業向けてのPRコンテンツの制作

（テクノロジー）
- 自己主権型のデータ管理・コントロールの実現方法
- 公開鍵が入手できない場合のデータ検証手法
- Trusted Webの実装方法に係る具体的な規定の必要性
- KYCの実現手法
- UI/UXを意識したアプリケーション機能、Wallet機能の考え方
- UI/UXに関する機能・非機能要件の考え方
- UI/UXの要件について
- ブロックチェーンの利用に係るセキュリティ要件の設定

示唆・提言の整理③　-Trusted Webで提供するサービス

（サービス）
- Trusted Webにおけるビジネスモデルの実現について
- ビジネスモデルの実現に向けたインセンティブ設計の必要性
- ヘルスケアデータのユースケースにおけるデータコントロールの要件の適用是非について
- Trusted Webシステムの構築、サービスの提供の実現に係る推進体制



示唆・提言の分析①　-Trusted Webの戦略

■ **Trusted Webで規定する内容の明確化**
- Trusted Webの6構成要素については、「理解が難しい」、「定義を明確にすべき」といった声が挙げられた
- 具体的には、「データのやり取りの記録がトランザクションとノードのそれぞれで定義されていることから構成要素ごとの役割の違いを明確にする必要があるのではないか」、「ユースケースの内容（モノのアイデンティティやパーソナルデータを扱うケースなど）に応じてパターンがあった方が良い」など、アーキテクチャの再構成・再検討の必要性も提起されている

■ **合意・トレース定義・考え方の明確化**
- 合意についてはデータの内容だけではなく、提示・開示などのデータのやり取りに関して合意を図っている事業者もあり、またトレースについても合意の履行に対するトレース（確認・閲覧）と定義していた事業者もいれば、データの流通に関するトレース（いわゆるデータトレーサビリティ）を念頭に検討を進めていた事業者もいた
- 合意やトレースの考え方を含め、Trusted Webで目指す内容を明確に示すことで、事業者がサービスやシステムを検討する際に、Trusted Webを参照する機会が増えると考えられる

■ **Issuer（証明書の発行者）の信頼性を確保・評価する仕組みの規定**
- Trusted Webに登場し得るステークホルダーに関する論点として、Issuerの要件やIssuerの信頼性を評価する仕組みの実装を期待する声が多かった
- Issuerは属性情報を証明する主体であり、サービス・システム全体の信頼性を担保する上で重要な位置づけ（信頼の根幹を担う主体）であることから、個別要件やそれを評価する仕組みをどうするのか、ホワイトペーパーの中で言及すべきと考える

■ **Trusted Webの組織・推進体制**
- ユースケースの中には、業界としてのデジタル化の推進に関して、民間事業者の働きかけのみでは調整が難しく、デジタル化の推進に向けた法令の整備、費用負担なども含めた国によるトップダウンでの政策実施など、行政と民間が一体となった推進体制の構築が重要であるとの意見も挙がっている
- 現状、企業ごとにTrusted Webの社会実装に向けた動きが個々に進められていることを受け、様々な企業が意見交換をすることができるオープンコミュニティを組成し、相互運用性を見据えた実装の構想を進めていく方向性に関する提言も見られた
- このような意見を踏まえ、今後の政府の関与するスコープや国内具体的な推進体制について検討し、ホワイトペーパーの中で示していくべきであると考える

示唆・提言の分析①　-Trusted Webの戦略

■ **アーキテクチャ（6構成要素）の再構成・再設計に向けた方針**

- Trusted Webのアーキテクチャ（6構成要素）については理解することが難しいという意見が挙がっている
- アーキテクチャの改善点を見つけるために、実証期間中にユースケースの内容を6構成要素に当てはめる作業を事業者主体で実施したが、その際も当てはめに苦戦した印象を受けた
- その理由としては、定義が明確に定められていないことやユースケースの種類によっては適用することがそもそも困難であるという点が考えられる
- 上記に加え、6構成要素が当初（ホワイトペーパーver1.0で）設定されていた4機能を再整理したもの、とされていたことから、各要素に対して何らかTrusted Webの機能的特徴を具備しようと事業者が検討を試みた可能性があり、それによって当てはめが、さらに難しくなった可能性がある

- 実際には、構成要素と機能は必ず連関するものではなく、「検証可能な領域を拡大することによるトラストの向上」のような、Trusted Webの目指す姿を実現しようとした時に、ユースケースごとの前提に寄らないプリミティブな構造が6構成要素であると考える
- そのため、事業者に対しては、6構成要素に固執する必要はなく、また検討したシステム構成が必ずしも6構成要素に当てはまるものではない、さらに各要素それぞれでTrusted Webに特徴的な観点が含まれないこともある、などを事前に周知することで、混乱を避けることが可能になると考える

示唆・提言の分析②　-Trusted Webの手法・アプローチ

■ ガバナンスによるTrusted Webの実現について

- 技術とガバナンスでカバーされる領域を明確に分離することを求める意見も見られた
- 具体的にガバナンスによって担保されるべき内容・仕組みとしては、Issuerの信頼度をTrustGraphなどによって図る方式や、データのコピーなどでトレースしきれない範囲を法制度によって担保するなど、データガバナンスの観点からの意見も多く見られた
- これらの課題提起について、政府やTrusted Web推進協議会等が答えをもっている訳ではなく、事業者には問題意識だけでなく具体的な解決案を提示してもらいたいという考えがあり、今後はそれを明示していくことが必要と考える
- 事業者からの意見の通り、データコピーやダウンロードの制限など、技術的に担保しえない領域におけるトラストや検証性の確保に対しては、法制度を含むガバナンスで規定してく必要があると考える
- 他方、（ガバナンスでなければ担保し得ない）その領域で、本当にトラストを確保する必要があるかどうかについては議論が必要であると考える。特にガバナンスの設定と自由なデータの利活用はトレードオフの関係となることが多く、データ利活用よりもトラストが優先されるというのは一義的な見方であるので、倫理面・技術面・事業面など多様な視点に立って、意欲のある事業者が中心となり、業界横断で関連するステークホルダーを招集して議論すべき内容であると考える

■ 暗号鍵の管理方法について

- 暗号鍵を管理する方法を議論する必要性があるという意見が寄せされている
- 今回のユースケースでは暗号鍵（秘密鍵）を用いた電子署名の検証による検証性・トラストの確保を前提としている傾向があり、電子署名において暗号化を担っている秘密鍵をセキュアに管理することは、Trusted Webで提供するトラストの価値を担保していると当社は理解している
- 仮に暗号鍵を流出させてしまった場合、本人以外でも署名してデータ送信することが可能になるため、なりすましのや改ざんが横行するリスクが懸念されるほか、紛失した場合、再発行ができないと、これまで保有していたデータを使用できなくなるリスクも想定される
- 他方、データコントローラビリティの確保に向けて、本事業で構築したシステムの大半は分散型を志向しており、鍵を管理するリスクを個人に分担させるか、部分的に集中管理的な構造として鍵の管理を第三者に移譲するかを論点として検討した事業者も見受けられた
- 暗号鍵を紛失した際のリスクと鍵を管理するリテラシーを鑑みて、特定の組織が集中的に鍵を管理する選択肢を採用することは現実的にも想定され得ると考える。それを踏まえ、データコントローラビリティや分散的な思想をTrusted Web構想の中でどのような位置づけとするのか（前提とするのか、任意とするのか）、明確に示すことが必要であると考える

示唆・提言の分析③ -Trusted Webで提供するサービス

■ ビジネスモデルの実現に向けて

- ビジネスモデルの実現（費用・収益モデルの成立）に向けては、Issuerがデジタル上の証明書を発行するインセンティブを確保する仕組みについての課題感が示されている
- Issuerは一度証明書をデータホルダーへ発行すれば、当該証明書はその後、または有効期限を設けない、更新内容がない場合）永続的にデータホルダーによって再利用することが可能な場合もある（Issuerが証明書の有効期限を設ける場合、更新内容がある場合は再発行が生じる）
- この場合、初期の発行時は発行手数料という形でデータホルダーからIssuerへ費用を支払うことが想定され得るが、その後の持続可能性を考えた場合にも、ビジネスモデルが本当に成立するのかが課題である。そしてその場合に、システムの利用料は誰が負担する形で成立し得るのか、事業者からの現実性のあるアイデアと検証を期待するところである
- 本実証事業は「開発実証」であり、エンドユーザーや特定のIssuerの参画は仮定して実施されているケースが大半であるが、次年度以降の実証事業においては参画するステークホルダーを拡大し、収支モデルの評価を含む「課題解決実証」の建付けにすることで、より具体的な実装可能性を検証できると考えられる

NTT DATA

Trusted Global Innovator