

Trusted Web ホワイトペーパー-ver.3.0(案) 概要

2023年11月

内閣官房デジタル市場競争本部事務局

エグゼクティブサマリ

1 背景

- フェイクニュースや生成AIによる偽情報等流れるデータの信頼性への懸念やそれに伴う社会の分断、プライバシー侵害リスク、勝者総取りに伴う特定サービスへの過度な依存、サイロ化した産業データの未活用など、デジタル化の中で様々な**ペインポイント**
- 現行のインターネットやウェブでは、社会活動において求められる責任関係や安心を十分に体现できておらず、**Trustの再構築**が不可欠
- これまでのTrustの仕組みでは、データのやり取りにおいて検証できる領域が狭く、事実を確認せずに、**プラットフォーム事業者等を信頼せざるを得ない状況**
- 内閣官房デジタル市場競争会議において“Trusted Web”の構想が提唱され、2020年10月に産学の専門家からなる「Trusted Web推進協議会」が発足。コンセプトの提示・具体化とユースケースからのフィードバックを繰り返しつつ、国際的な動向も踏まえながら議論が進められてきた

2 Trusted Webとは何か

- Trusted Webは、**特定のサービスに過度に依存せずに、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等の新たな信頼の枠組みを構築するイニシアティブ**
- 「デジタル社会」における様々な社会活動に対応できる**Trustの仕組みを、一定のガバナンスや運用面での仕組みとそれを可能とする機能を付加していく**ことにより形成し、**多様な主体による新しい価値の創出を実現**することを目指す
- Trusted Webによる**データのやり取りにおける信頼の仕組みの構築**は、様々な主体が業種や部門を超えて協創することが求められる**DXを進めるに当たって、その前提となる「事業者間連携」を円滑にする上でも極めて重要な取組**であり、ひいては、**DFFTの具体化にも資するもの**

3 実現に向けた道筋

- 実証事業等を通じて、**様々なユースケースを創出し**、内外の関係者と共有し議論を重ねることによって、Trusted Webの目指すべき方向性に沿った取組を通じた**新たなビジネスの創出**につなげるとともに、国際連携を推進する
- Trusted Webが目指す仕組みを具現化する様々なサービスが提供され、その利用領域が拡大。その過程において、既存のTrustを向上させる仕組みも活用しながら、**共通化すべきAPIやデータモデル、プロトコルが特定**されていく。それらが共通化されることで**相互運用性の確保、標準化**につながり、**Trusted Webが具現化**されていくことが期待される

4 ホワイトペーパーver.2.0（2022年8月公表）からの進展

- 2022年度「Trusted Web共同開発支援事業」等を通じて、**民間事業者等による様々なユースケースの具体化**が進みつつある中、そこで示されたベネフィットや課題を共有し、**企業における自社のビジネスとの接点を見出すための材料**を提供、ビジネス創出につなげる
- **実装上のプラクティス等の整理**を行い、**エンジニア等が具体例を把握し、相互に議論しながらサービス開発に活用していく場をGitHub上に構築し公開**
- 実証事業からのフィードバックを踏まえ、**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

ホワイトペーパーの分冊化(1/2)

ホワイトペーパーver.3.0は、Trusted Webの考え方のビジネスへの適用、実装をわかりやすく理解するためのガイドンスとして作成。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**」を公開。

概要／コンセプト編

DXに取り組む産業界の経営者を含む関係者、政策立案関係者ほか全般

- 直面している課題やTrusted Webの目指すべき方向性、ベネフィット、具現化の考え方など、Trusted Webの**大枠を理解するためのもの**
- ユースケース編や実装編の概要を記載しており、Trusted Webの考え方に則った取組を進めるきっかけとなることを期待

ユースケース編

産業界の関係者（マネジメント層や事業部門）など

- 机上検討(2021年度)及びユースケース実証(2022年度)における**プロトタイプ開発・企画を通して得られた成果概要のまとめ**
※個人、メディア、ヘルスケア、法人と行政とのやりとり、サプライチェーン、IoT等の各分野の具体的なユースケースを提示
- 得られるベネフィットや実装に至る課題を整理。自社のビジネスとの**接点を見出すための材料を提供し、ビジネス創出につなげる**

実装編

エンジニアや大学等研究機関など

- ユースケース分析を踏まえた、**アーキテクチャの再整理と、ガバナンスのあり方、セキュリティ目標**を提示
- 実装時に必要な**機能やガバナンス、守るべきセキュリティ要件**を示すことで、様々なモジュール、サービス等の開発へのインプットや国際標準化の推進につなげる

実装ガイドライン

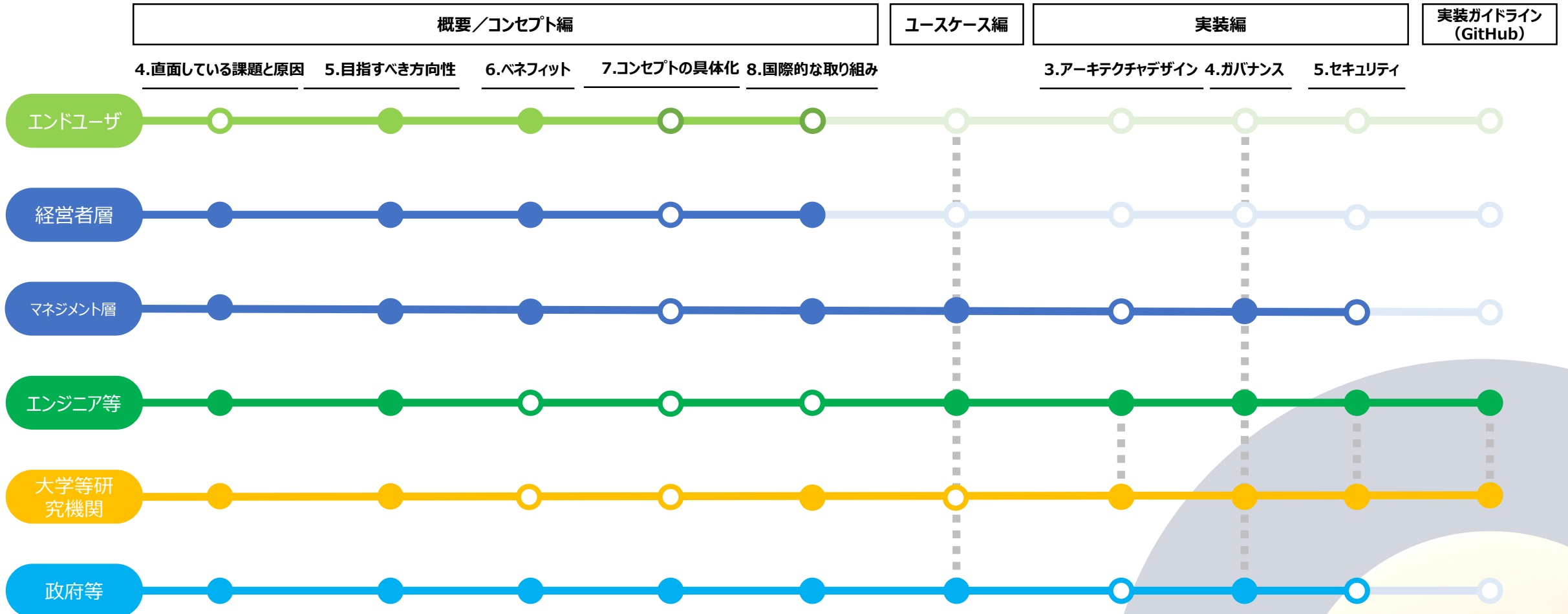
エンジニアや大学等研究機関など

- Trusted Webに則った設計思想に基づいて**事業者が実装する際に参考となるプラクティスとして位置づけ**。具体的には、以下を提示。
 - ユースケース毎に抽出した機能要件に対する**実現方式のバリエーション**
 - ユースケースに組み込む際の**留意点や、サンプル、コンポーネント配置等**
- **GitHub**上に公開することで、**進歩の早い技術動向を速やかに取り入れ**、関係するエンジニアなどステークホルダーが**具体的な実装例を把握し、相互に議論・更新しながらサービス開発に活用**されることを期待

ホワイトペーパーの分冊化(2/2)

- バックグラウンドや視点の異なる読者層の関心に応じて読みやすい形となるよう、ホワイトペーパーを「概要／コンセプト編」、「ユースケース編」、「実装編」の3つで構成し、併せてGitHub上に「実装ガイドライン」を公開。
- お読みいただく際のガイドを参照いただきつつ、経営層や事業部門、エンジニア、ユーザ等が相互に連携し実装を進めていくことを期待。

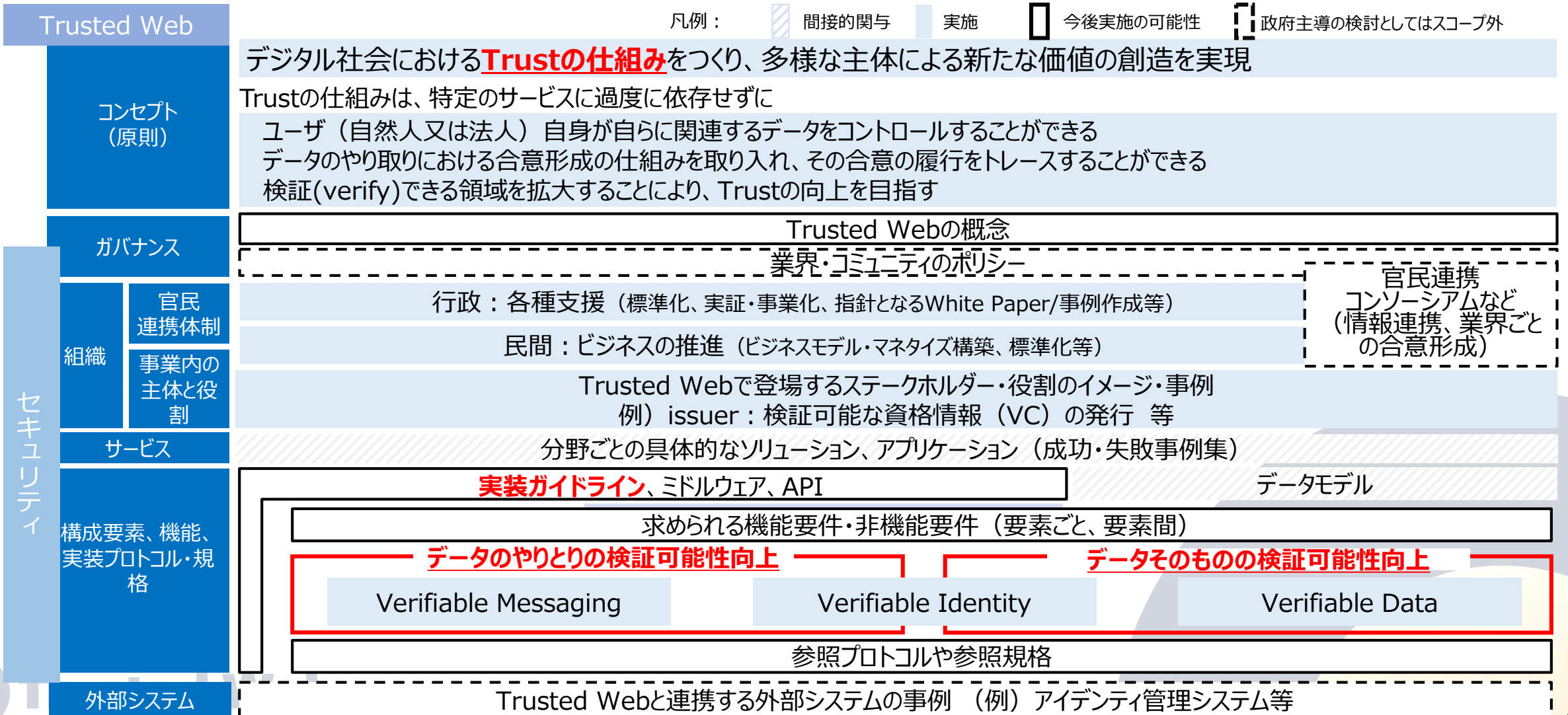
● 把握することを強く推奨するもの ○ 追加的に把握することを推奨するもの ■■■ 事業や開発の検討過程で連携が必要なもの



1. 概要／コンセプト編

1-1. Trusted Webとは

特定のサービスに過度に依存せずに、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等の新たな信頼の枠組みを構築するイニシアティブ



1-2. 検討の背景とこれまでの検討経緯

- サイバーとフィジカルの融合が進み、様々な社会活動が行われる「デジタル社会」に移行。
- しかしながら、デジタル空間では様々な課題が顕在化。“一握りの巨大企業への過度な依存”でも、“監視社会”でもない**第三の道を模索**することが必要。
- 「デジタル社会」の基盤として発展してきたインターネットとウェブでは、データの受け渡しのプロトコルは決められているものの、**アイデンティティ管理も含め、データ・マネジメントの多くはプラットフォーム事業者などの各サービスに依存**。サイロ化され、外部からの検証可能性が低く「信じるほかない」状況。
- こうした状況を踏まえ、**DFFTの具現化を視野に、Trusted Web構想**について、以下のように検討を積み重ねてきている。

2020年度

6月：「デジタル市場競争に係る中期展望レポート」公表

ホワイトペーパー

机上検討・実証事業

3月：ホワイトペーパー-ver.1.0公開

2021年度

机上検討（個人、法人、サプライチェーン）

2022年度

8月：ホワイトペーパー-ver.2.0改訂

9月～翌3月

ユースケース実証事業（13件）

2023年度

11月：ホワイトペーパー-ver.3.0改訂

6月～翌3月

ユースケース実証事業（12件）

1-3. 直面している課題とその原因

- インターネットとウェブは、グローバルに共通な通信基盤として発展して、広く情報へのアクセスを可能とし、その上で様々なサービスを創出。
- しかしながら、デジタル社会における様々な社会活動において求められる責任関係やそれによってもたらされる安心を体現する仕組みが不十分な状況であり、ユーザーが信頼の多くをプラットフォーム事業者などに依拠する中で、その歪みが様々なポイントをもたらしている。

ポイントの例

- フェイクニュースや虚偽の機器制御データなど、流れるデータへの懸念
- 生体情報も含めたデータの集約・統合によるプライバシーリスク
- プライバシーと公益のバランス
- サイロ化された産業データの未活用
- 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
- 社会活動を行う上での社会規範によるガバナンスの機能不全

ポイントの原因

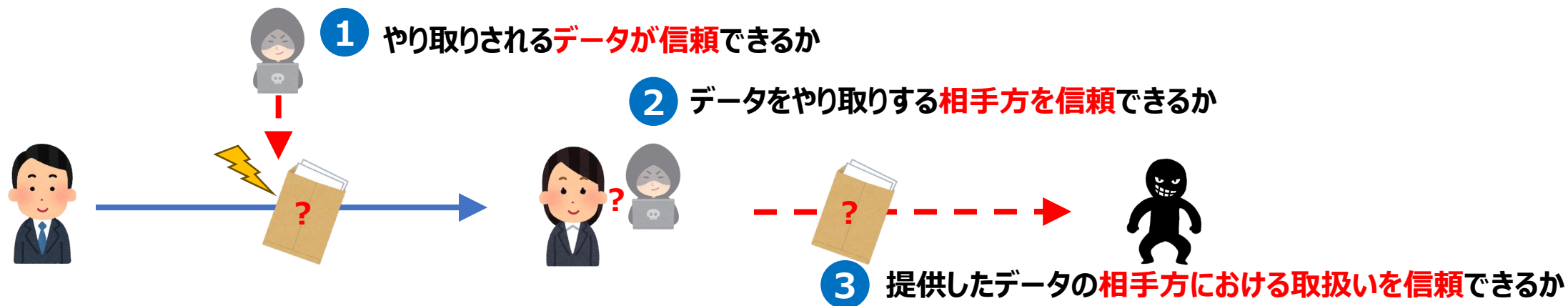
- やり取りされるデータが信頼できるか
 - データをやり取りする相手方を信頼できるか
 - 提供したデータの相手方における取扱いを信頼できるか
- について、懸念がある状況

インターネットとウェブがもたらしてきたベネフィットを活かしつつ、一定のガバナンスや運用面での仕組みとそれを可能にする機能をその上に付加していくことが必要。

カギとなるのが“Trust”

(参考) ペインポイントの原因と具体的なニーズ

- ペインポイントの原因としては、「①やり取りされるデータが信頼できるか」、「②データをやり取りする相手方を信頼できるか」、「③提供したデータの相手方における取扱いを信頼できるか」についてそれぞれ懸念がある状況
- また、これらの原因に対応する標準的かつグローバルで合意された技術や仕組みはない状況



具体的なニーズの例

データを提示するユーザーは、受領者との間で、

- **データの開示範囲をコントロール**したい
例) 受領者が開示依頼するデータの範囲が、正当かコントロールできない。
- **双方の意思を反映した合意形成**や、**データ提示後の合意履行状況**を検証したい
例) データのやり取りの合意、データの受領の記録がされたかわからない。

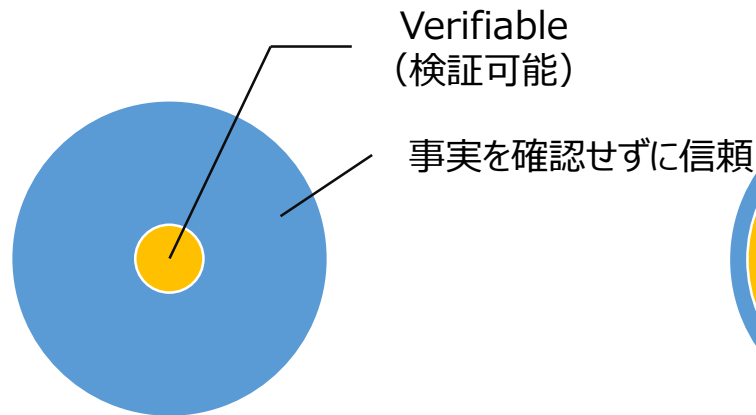
データを受領するユーザーは、

- **意図した発行者からデータが改ざんされていない**状態でデータを受領したい
- **必要に応じて**、データが改ざんされていないこと・意図した発行者であることを**検証**したい
例) 発行者が証明したい属性情報を証明する能力が発行者にあるか、信頼できる第三者が証明した属性情報なのか受領者はわからない。

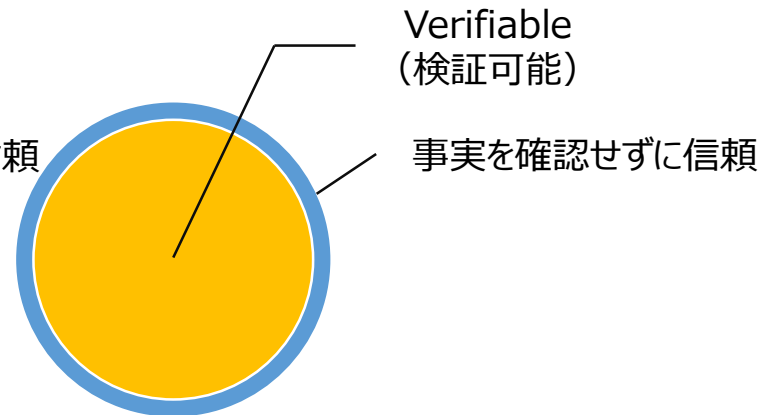
1-4. Trusted Webが目指すべき方向性

- **目的**：デジタル社会における様々な社会活動に対応するTrustの仕組みをつくり、多様な主体による新しい価値の創出を実現
 - **Trustの仕組み**：特定サービスに過度に依存せず、
 - ・ 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ことを可能とし
 - ・ データのやり取りにおける合意形成の仕組みを取り入れ、その合意の履行のトレースを可能としつつ
 - ・ 検証(verify)できる領域を拡大することにより、Trustの向上を目指すものである
 - **アプローチ**：インターネットとウェブのよさを活かしその上に重ね合わせるオーバーレイのアプローチ
- *Trust: 事実の確認をしない状態で、相手先が期待したとおりに振る舞うと信じる度合い

仕組みによりVerifiable（検証可能）な部分が変わる

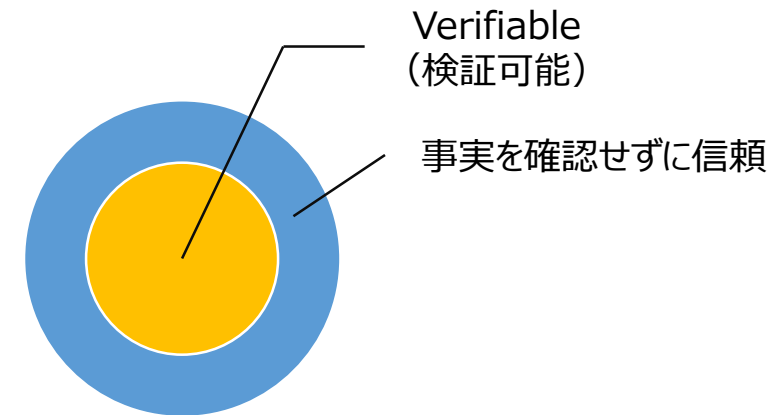


現在のインターネット：
検証できる部分が小さく、
相手を大きく信頼しないと
意思決定できない。



全てのやりとりをブロックチェーンをベースにした場合

*スケーラビリティやエネルギー消費といった課題、特定の技術に依存しすぎることのない更改容易性の観点等も踏まえたトレードオフを勘案し、Trusted Webでは、一番右の円を目指すべき姿として想定。



目指すところ：
ある程度検証できる部分を担保しながら、継続性や、
相互運用性、更改容易性を充足する仕組み

→「Trust」を高める

1-5. Trusted Webのもたらすベネフィット

- Trusted Webの考え方に則った実装を通じ、データの流通やDX、DFFTの実現を阻害する要因となっている様々なペインポイントを解消することで、デジタル技術を活用して**企業や産業の競争力強化**につなげていく。
- **エンドユーザー**は、データの**コントロール**の行使や、データの確からしさが高まる**安心感**、新たに**創出されるサービス**によってもたらされる**価値の享受**といったベネフィットを受けることができる。

企業にとってのベネフィット

- ✓ やりとりするデータや相手先でのデータの取扱い等のTrustが向上することで、**データ流通やDX、DFFTを進める上で大前提**となる「**事業者間連携**」の実現につながる**ことが期待**
- ✓ やりとりするデータや相手先そのもののTrustが向上することで、**データの検証に係るコストを低減**
- ✓ 流通するデータのTrustが向上することで、**利用するユーザの安心感が高まり、さらなるサービス活用の推進が期待**
- ✓ **デジタル・インフラ創りに早期から関わり、先行的に実装を進めることで、ビジネスプロセスやサービスの価値をいち早く検証、相互運用性を確保し検証したビジネスをスケール**できる

エンドユーザーにとってのベネフィット

- ✓ **自由意思に基づきコントロールを行使してデータをやり取りできる**
- ✓ 現在は、ユーザーがデータを利用・共有しようとするたびに、プラットフォーム事業者等によるサービスの利用が必要となるが、**データをユーザーに集約させること等**によって、プラットフォーム事業者等の**第三者の関与なしで情報を利用・共有**できる
- ✓ やり取りされるデータの確からしさが高まることで、**ユーザの安心感が向上**
- ✓ Trusted Webを実装する過程で事業者によって創出される**様々なサービスや、それによってもたらされる価値をユーザとして享受**

1-6. ユースケース検証とプロトタイプ実装

2021年度に実施した3件の机上検討と、2022年度に実施した13件のユースケース実証におけるプロトタイプ検証・企画を通して、メリットの具体化を実施

個人の属性情報（学習・就業履歴、共助実績）

就業等証明

学習歴

共助

メタバース

- リスキング等が求められる中で、個人の機微に係る情報（学修履歴やキャリア）への取扱の懸念やリスクに対し、提示する情報をコントロールするとともに、活用先や活用目的について同意し、どのような雇い手が情報にアクセスしたか等について、応募者自身がトレースできるようになることで、より安心感が増し、就職や転職において、より自分にフィットしたキャリア形成を実現
- 企業による採用時のミスマッチを回避するべく、履歴書や職務実績、勤務状況といった応募内容について偽りがないか確認するコストに対し、第三者によるお墨付き（学習機関や過去の勤務先からの証明等）によって、検証可能性を高め、検証コストを下げる
- 地域での助け合いをマッチングする共助アプリにおいて、共助実績をアプリ横断で検証可能とするために必要な指標や事前に合意されるべき事項等の整備が求められる。複数の共助アプリによるガバナンスを担保するためのトラストフレームワークを策定することで、ユーザーによる検証範囲を広げ、アプリを横断したトラストを形成。自治体によるデジタルサービス展開の促進など、他業界サービスとの連携等を可能に

法人と行政庁との情報のやり取り

法人と補助金

工業会証明書

- メーカーや工業会、所轄官庁など複数の異なる主体が発行するデジタル証明書を活用することで、行政への提出書類の信頼性を向上。これにより、改ざんや有効性、意図した発行者からの証明書か等の行政における証明書類確認工数を大幅に削減、手続きを迅速化

サプライチェーンにおける情報のやり取り

炭素排出量

化学物質の含有量

ITシステム品質保証

機械製品修理

- データが加工され伝達する中で、営業秘密等を配慮し、通信履歴の開示範囲を制限しながら、データの信頼性自体を担保する仕組み
- ITシステムの製品信頼情報（IT機器の使用部品やソフトウェア脆弱性対応等）を安全に提供し、ソフトウェア／ハードウェア改ざんの一律的な自律検知やセキュリティ運用連携を含め、ユーザが確認する仕組みの構築

1-7. ユースケース検証とプロトタイプ実装

IoTの属性情報のやり取り

複合機

- テレワークの環境整備が求められる中、真正性を求められる文書を扱う経理部門や特定の業種業務では、未だ紙を基本としたアナログ業務が多いところ、特定の複合機でスキャンされて以降、改ざんがされておらず、当該複合機でスキャンされた文書であることが検証可能な仕組み

ヘルスケアの属性情報のやり取り

臨床データ

ヘルスケアデータ

- 診療情報等の機微性の高い情報を扱うため、重要な情報やプロセスが紙媒体に記録され、運用コストがあがっているところ、病院が送信したファイル（臨床試験データを含む）が改ざんされていないことを担保し、信頼できる相手方であることを確認した受信者のみが検証することで、送信側のなりすましが行われていないことを確認でき、データの授受に関して、履歴（監査証跡）を確認することでトレース可能とする
- 健康診断での情報や職場での健康情報、日常生活におけるあらゆるタイミングでの多様な情報の医療や研究での活用を可能とする

メディアの属性情報のやり取り

広告

- ニュース配信におけるメディアの発信元を検証するための検証作業の確からしさを向上する技術として、Originator Profile (OP) の議論を進めている。これにより、偽情報の主な手法である、「コンテンツの改ざん」や「なりすまし」への有効な対応策となることが期待される。
- 審査機関が「アドテク事業者」にOPを発行し、「サイト閲覧者」がOPを検証することで、アドテク事業者の正当性を確認し、収集したサイト訪問者（生活者）の情報が不正なアドテク事業者に渡ってしまうことを防ぐことができる
- サイト閲覧者を装って広告効果があるように見せかけるボットではないことを証明する非ボット証明を発行し、「サイト運営者」および「アドテク事業者」が人間による正当なアクセスであることを検証することで、広告詐欺ではないことを確認できる

1-8. Trusted Webと「生成AI」

- 急速に発展している生成AIを巡っては、広範な認識と急速な普及によって、様々な分野でイノベーションを加速させ、世界に劇的な変化をもたらすことが期待される一方で、**精緻な偽画像や、偽情報による社会の混乱など、経済社会を脅かすようなリスクや課題**も指摘されている。
- 2023年4月のG7デジタル・技術大臣会合では、「**AIガバナンスや著作権を含む知的財産権の保護、透明性の促進、外国からの情報操作を含む偽情報への対処方法や、責任ある形での生成AIを活用する可能性といったテーマを含む生成AIに関するG7における議論を引き続き行うための場を設ける**」ことに関して合意し、5月のG7広島サミットの結果、「**広島AIプロセス**」が立ち上げられた。
- その後、10月には、「**高度なAIシステムを開発する組織向けの広島プロセス国際指針**」や「**高度なAIシステムを開発する組織向けの広島プロセス国際行動規範**」が示される等、国際的な議論が進められている。
- なお、広島AIプロセスにおける議論のためにOECDが9月に公表したレポートでは、G7メンバー間で懸念される主要な分野として、特に、**生成AIの開発と使用に関する透明性、偽情報、知的財産権、プライバシーと個人情報保護、公正性、セキュリティと安全性**等を挙げている。
- こうした中で、やり取りするデータや相手方を検証できる仕組みなどにより新たな信頼の枠組みを構築するTrusted Webの取組は、**生成AIに関するトラスト確保**という観点において、**重要な一翼を担い得る**と考えられる。

1-9. 企業の具体的な参画に向けた方策について

- 企業がTrusted Webの考え方に則って、具体的な取組を進めていく上では、経営層や事業部門、エンジニア等の**関係者が、必要な取組のステップを理解・共有し、取組状況を自己診断**によって随時把握しつつ、**アクションを進めることが必要**。このため、取り組むべき内容を**参照できる道標となる「推進ステップ（仮称）」**を、ホワイトペーパー-ver.3.0公表後、**検討を深め、迅速に公表**する。
- 「推進ステップ（仮称）」の活用により、各企業の取組が促進されるだけでなく、例えば、自己診断の**結果を外部に開示**することで、**企業やサービスに対する評価や、相互運用性を担保する上で相互に参照**できるといった**メリットも期待**される。
- また、広く活用を促すため、類似の事例等を参考に、事業者にとっての**インセンティブの在り方も併せて検討**していく。

参照可能な道標（推進ステップ）のイメージ

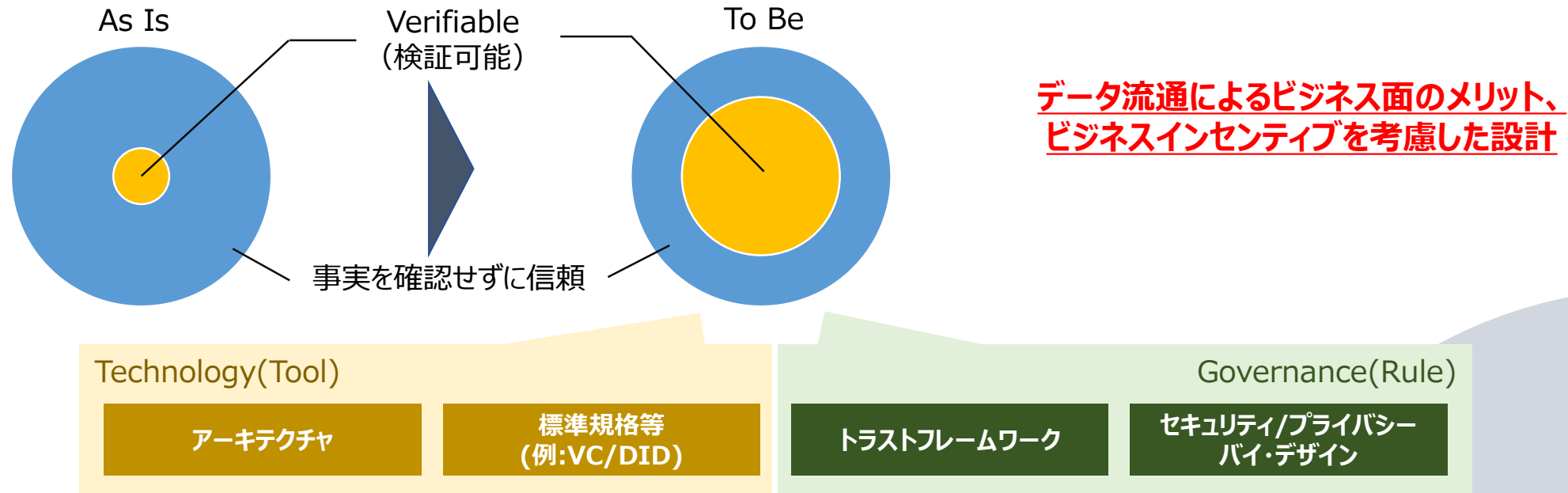


自己診断における項目のイメージ

- Trusted Webの考え方に則った仕組みを適用する領域の**特定状況**
- **ペインポイントの特定状況**
(例) 非改ざん性、なりすまし防止、選択的情報開示等
- **目指すべき方向性を踏まえた価値創出の方向性**
(例) 検証できる領域の拡大、合意形成の仕組み等
- **必要となる原則への対応状況**
(例) データ主体によるコントロール、相互運用性等
- その他、アーキテクチャやガバナンス等に関する項目も想定

1-10. Trusted Webを支える2つの軸

- 検証可能な領域を増やすためには、アーキテクチャをはじめとした**テクノロジー**のみならず、**ガバナンス**によるアプローチが必要であり、両者は**車の両輪**の関係にある。
- Trusted Webを実現するために利用される**技術の中立性を維持**するためには、一定のガバナンスを効かせることが必要。また、中長期にわたるTrusted Webの考え方の維持には、**特定のステークホルダーへの過度な依存が発生しない**ためのガバナンスの仕組みが必要となる。



データのやりとりにおいて、
検証可能性とコントロールを高める仕組みを構築

1-11. オーバーレイの考え方と実現に向けた道筋

アーキテクチャとしてオーバーレイのアプローチでの実装を目指す

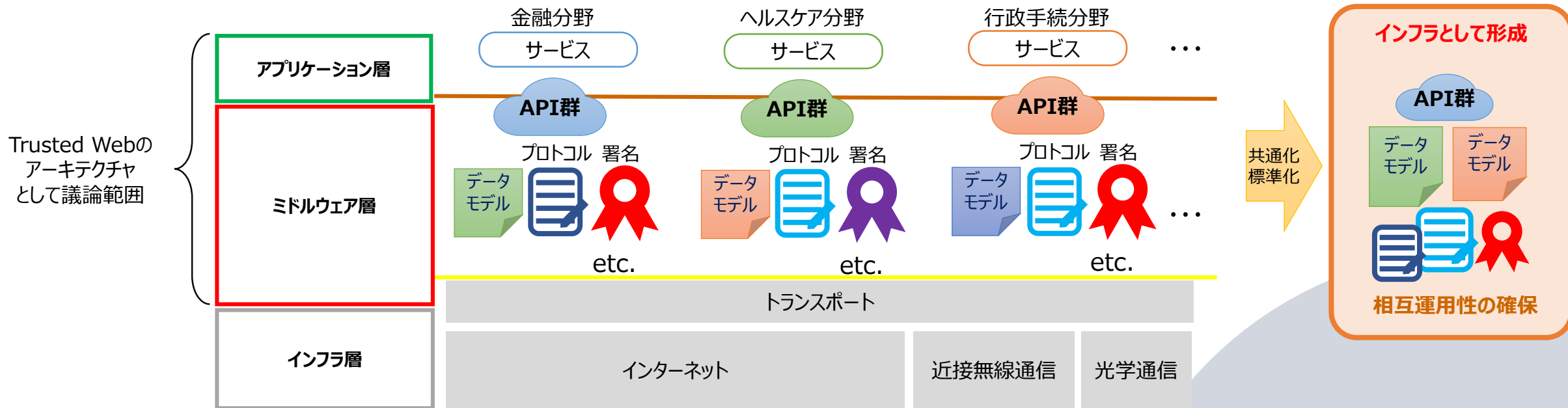
Trusted Webの実現の道筋の仮説

Trusted Webが目指す機能を具現化する様々なサービスが提供され、その利用領域（分野）が拡大していく

→ 用途に応じた多種多様な特性に対応できるミドルウェアのようなものが形成されていく

→ ミドルウェアにおいて、**共通化すべきAPIやデータモデル、プロトコルが特定され、共通化されることにより相互運用性が確保され標準化**につながる

→ 実際にユーザーが利用する様々なサービスからフィードバックを得ながら、社会実装が進められていく



ユースケース検討や実装を通じてTrusted Webがもたらすベネフィットを様々な領域（分野）のステークホルダに提示するとともに、**アーキテクチャやガバナンスなどに対する課題や改善点等のフィードバックを得る**

2. 実装編・実装ガイドライン

2-1. Trusted Webで目指す信頼の姿

Trusted Webで目指す信頼の姿を以下のように整理。この整理をベースに、Trusted Webにおける相互運用性の高い検証可能なデータモデル、検証可能な通信モデルの設計の方向性を、Trusted Webの「アーキテクチャ」として示す。

a. アイデンティティの管理

- ・主体（エンティティ）は、外部連携等されたアイデンティティ管理システム※を利用することによって、自らのアイデンティティ管理を行う

b. Trustとデータ検証

- ・Trusted Webでの根源的な価値は「データの検証可能な領域拡大によるTrustの向上」

c. Trusted Webで対象とするデータ

- ・作成されたデータと、そのデータのやり取りの過程を対象とする
 - 作成されたデータ：デジタル署名技術により検証可能性を担保
 - データのやり取りの過程：やり取りをモデル化しデジタル署名と組み合わせることで検証可能性を担保

d. 検証領域の拡大

- ・《署名自身》の検証、《署名者》の検証、《署名の意図》の明確化によって、署名を含むデータ全体を検証できることに
 - 《署名の意図》の明確化とは、予め合意されたデータのやり取りの枠組みにおいて、目的を達成するために署名が果たす機能が特定されている状態

署名の意図が明確化される枠組みの例：

プロトコルでデザインされている意図に従って署名されている例（X.509証明書、DNSSECなど）

デジタル化された証明のためのデータ（例：Verifiable Credentials）に対する署名

e. やり取りのモデル化

- ・データのやり取りのモデルは、メッセージとトランザクションという形で整理
- ・データのやり取りの過程（順序、内容、実際に受け取ったかどうか等）を相互に記録
 - データを確実に受け渡し、受け渡しのやり取りが実際にあったことを事後に検証可能

f. プロトコルの組み合わせの必要性

- ・標準やプロトコル群の組合せの自由度が高いアーキテクチャが重要

※ OpenID等の標準を用いたシステムや、DID/VCといった技術を用いた実装などが考えられる。

2-2. ver.2.0のアーキテクチャを再整理

検証可能な領域を拡大し、データのやり取りにおけるTrustの向上を目指すため、ver.2.0のアーキテクチャの6構成要素を **Verifiable Identity**、**Verifiable Data**、**Verifiable Messaging**、**Verifiable Identity コミュニティ**に再整理



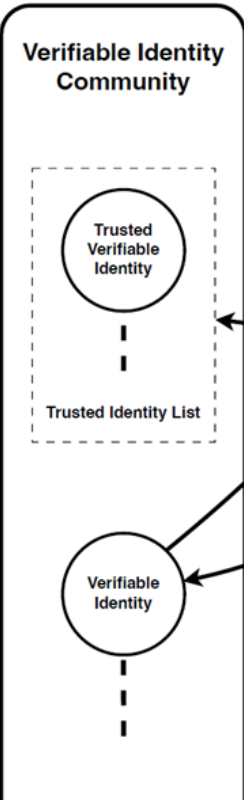
2-3. Trusted Webを実現するためのアーキテクチャ

検証可能なアイデンティティ(Verifiable Identity)を中心として、**検証可能な領域を拡大する抽象度の高いアーキテクチャ**を提示。既存のTrustのメカニズムとの**組み合わせの可能性**を提示し、より高い**インターオペラビリティの確保**を目指す。Verifiable Identity、Verifiable Data、Verifiable Messaging及びVerifiable Identity コミュニティを活用することにより、**検証可能な領域を拡大し、データのやり取りにおける Trustの向上**を目指す。

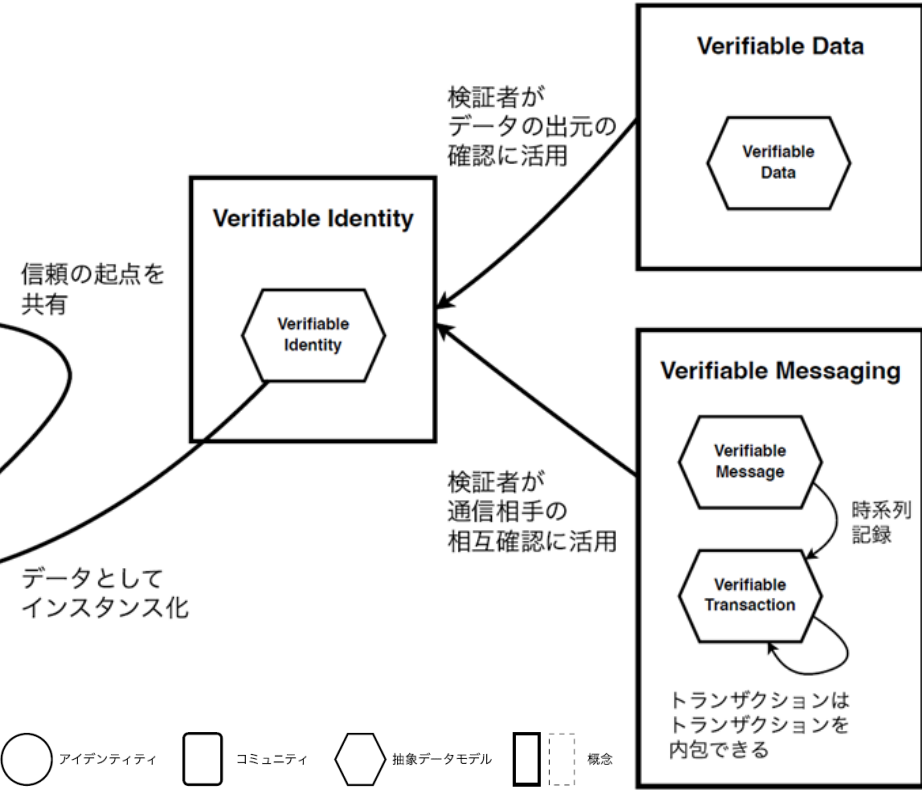
Verifiable Identity コミュニティ
(検証可能なアイデンティティのコミュニティ)

信頼の起点を含む情報を一定のガバナンス下で共有するアイデンティティの集合
←高い確度で信頼できるエンティティ
(Trusted Entity)によって運用されたアイデンティティ(Trusted Identity)を起点とした**信頼の連鎖**によって、署名者の情報をエコシステム参加者で共有することで、**信頼関係の構築を容易**とする。
例：JPKIにおける利用者証明用CA

インスタンス
(データ)



アーキテクチャ
(概念・データモデル)



Verifiable Data (検証可能なデータ)

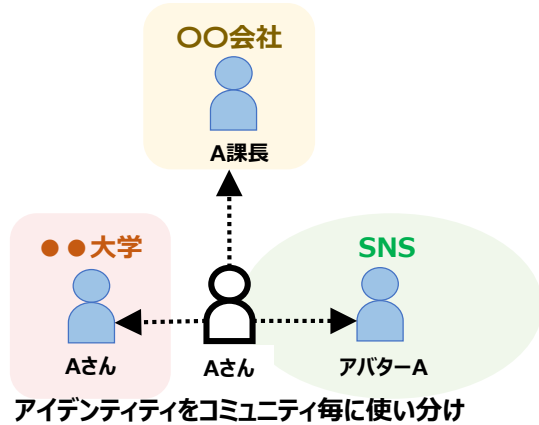
対象となるデータ、署名、発信元のアイデンティティへの参照で構成。
鍵関連情報によって署名し、生成。Verifiable Identityを参照・検証して取り出した鍵関連情報（例：公開鍵暗号）を用いて検証する。
例：X.509PKIの証明書、ワクチン証明書、署名PDF

Verifiable Messaging(検証可能なメッセージ交換)

複数エンティティ間の**確実な配送**をメッセージの送受信の**順序性**を含め記録。

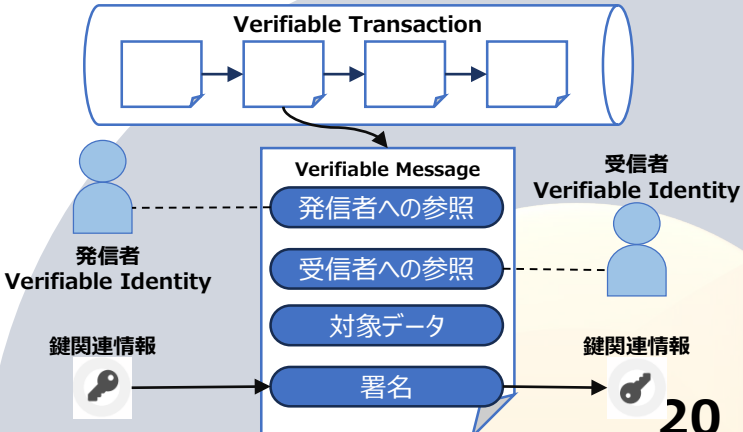
- Verifiable Message：発信者・受信者を参照するための**情報、メッセージ自身、発信者による署名**
- Verifiable Transaction：Verifiable Message あるいは Verifiable Transactionについて、**発信の順序が検証できる形で記録**（例：Transaction Recordのブロックチェーンへの記録）

 例：PGPやS/MIMEによるメール、グループチャット



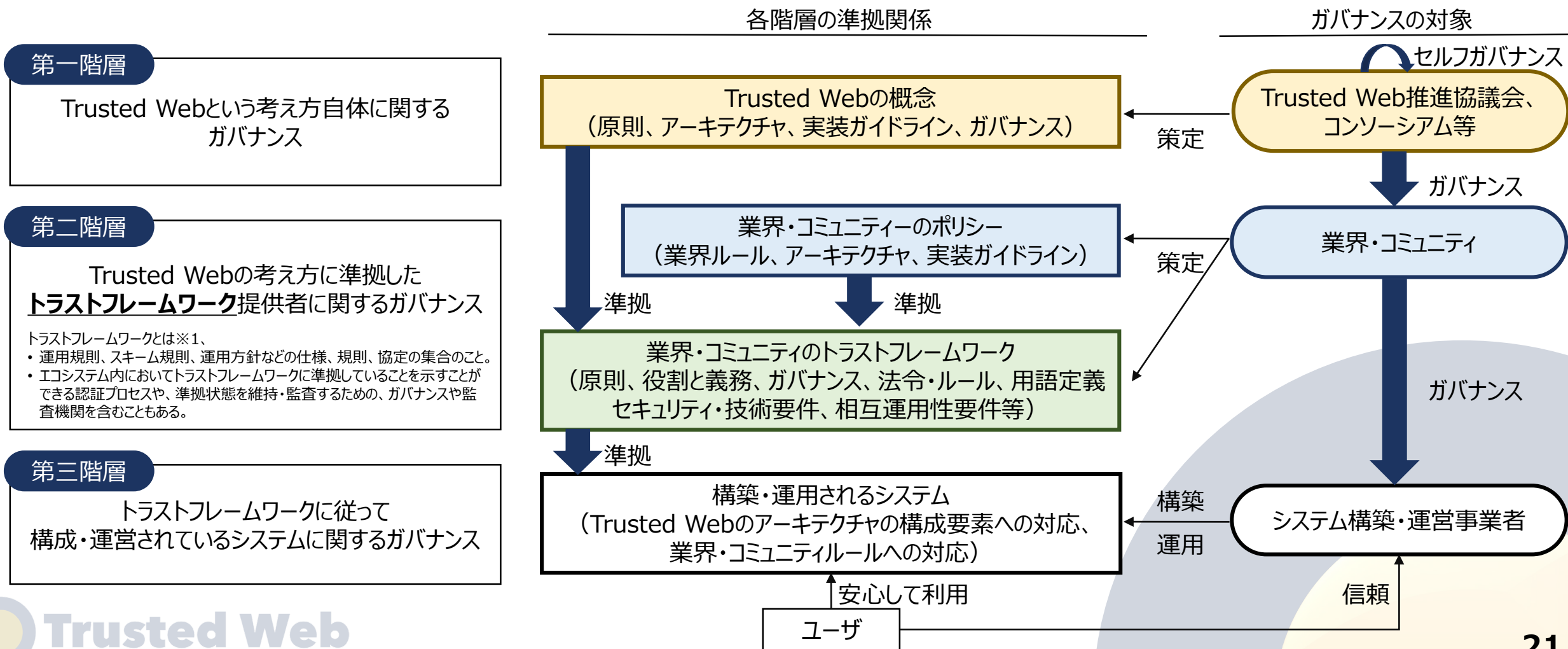
Verifiable Identity (検証可能なアイデンティティ)

検証可能かつコンテキストに応じて最低限必要な属性からなる**デジタル・アイデンティティ**
鍵関連情報、**identifier(識別子)**、**自身への署名**で構成。
※一つのエンティティ（自然人、法人等）は、一つのアイデンティティを用いている場合もあれば、コンテキスト（SNS、法人）に応じて複数のアイデンティティを使い分ける場合もある。
例：WebPKI、OpenID Connectを用いたプラットフォーム



2-4. ガバナンス（全体像）

- 技術の発展や社会システムの変化に応じて、Trusted Webの原則自体や、Trusted Webの原則に則り構成される系（業界やシステム）が、その原則を失うことなく運営・利用されるための「ガバナンス」が必要。
- Ver.3.0では、今後の検討の素地として、ガバナンスの階層性やガバナンスの運営体制のあり方、トラストフレームワークのアウトライン等を示している。



2-5. ガバナンス（今後の検討事項）

- ガバナンスの運営体制やトラストフレームワークは、OIX※1が2022年に公開したガイドライン※2も参考とし今後具体化。
- 特にガバナンスの運営体制については、**中立的かつ持続可能な組織形態として、官民のリーダシップによる非営利連合であるカナダのDIACCも念頭に具体的な検討を行っていくことが必要。**

※1 Open Identity Exchange

※2 A Guide to Trust Framework for Smart Digital ID

ガバナンスの運営体制のあり方の例

- **独立した運営組織**
例) カナダのDIACC（Digital ID and Authentication Council of Canada）のような官民による非営利連合
- **参加者によるコンソーシアム型組織**
例) CA/Browserフォーラム（ブラウザベンダーと認証局が参加）のようなトラストフレームワークに参加している主体により組成されるコンソーシアム型組織
- **単一主体による管理組織**
例) 米国政府の運営するlogin.govのような単一主体により構成される管理組織
- **非政府の標準・認定団体**
例) Kantara Initiativeなどの独立した非政府の標準化/認定団体
- **全ての参加者による相互合意（ガバナンス主体を設けない）**

2-6. ガバナンス（今後の検討事項）

ガバナンスの運営体制やトラストフレームワークは、OIX※1が2022年に公開したガイドライン※2も参考とし今後具体化。

※1 Open Identity Exchange ※2 A Guide to Trust Framework for Smart Digital ID

トラストフレームワークのアウトライン

構成要素

Trusted Webに求められること（例）

用語定義 (Glossary)	-
原則 (Principles)	Trusted Webの原則に準拠すること
信頼の表明 (Trust Mark)	仮にユーザー等に向けてTrusted Webに準拠したトラストフレームワークであることを表明する場合は原則の遵守状況のモニタリングの必要性などについて検討すること
役割と義務 (Roles and Obligations)	Trusted Webの原則の遵守を義務として定義すること
ガバナンス (Governance)	Trusted Webのガバナンスの概念を踏襲すること（マルチステークホルダー等）
信頼のルール (Trust Rules)	Trusted Webの原則に則り構成されるエンティティを信頼すること
ユーザー向けサービス (User Services)	
業務サービス (Relying Party Services)	Trusted Webの原則に則り構成されること（検証可能性、透明性など）
法令・ルール (General and Legal Rules)	-
セキュリティ・技術要件 (Security and Technical Requirements)	検証可能性を担保できる技術を採用すること。特定の事業者によってのみ策定された技術ではなく、標準として広く受け入れられている技術を採用すること。
相互運用性要件 (Interoperability Requirements)	標準として広く受け入れられている技術を採用し、必要に応じてエコシステムの拡大を容易に行うことが可能なこと

2-7. 設計・運用における原則

1 持続可能なエコシステム

ステークホルダーがそれぞれの責任を分担し、責任を果たすインセンティブがあること。

3 オープンネスと透明性

アーキテクチャ設計、実装とそのプロセスがオープンであり、透明性が高く相互に検証可能であること。

5 ユニバーサル性

誰も排除せず、弱い立場にある人を取り残さないこと。誰でも自由に参加できること。

7 継続性

既存のインターネットアーキテクチャを基礎として、上位に構築することとし、transitionalな形で現行ウェブに付加されること。既存のTrust手段とのフェデレーションも考慮すること。

9 相互運用性

技術のみだけでなく、法制度、ガバナンス、組織等の社会システム全体について異なるシステム間で連携可能であること。

2 マルチステークホルダーによるガバナンス

マルチステークホルダーがガバナンスに関与し、ステークホルダーの責任が明確で、問題が発生したときに原因究明ができること。

4 データ主体によるコントロール

データへのアクセスのコントロールは、データ主体（個人・法人）に帰属すること。

6 ユーザー視点

ロックインフリーでユーザーに選択肢があること。ユーザーにとって分かりやすく安心して使えること。

8 柔軟性

構成部品が疎結合で構成され、拡張可能なアーキテクチャであること。

10 更改容易性・拡張性

特定の技術に依存し過ぎず、中長期での利用を意識して継続的に機能拡張が容易でスケラブルであること。

2-8. 実装ガイドラインについて

- Trusted Webの設計思想に基づいて**事業者が実装する際に参考となるプラクティスとして位置づけ**。具体的には、以下を提示
 - ユースケース毎に抽出した機能要件に対する**実現方式のバリエーション**
 - ユースケースに組み込む際の**留意点や、サンプル、コンポーネント配置等**
- **GitHub**上に公開し、[Trusted Webのウェブサイト](#)にて、議論に参加していただける方を募集。**進歩の早い技術動向を速やかに取り入れ、関係するエンジニア等のステークホルダーが具体的な実装例を把握し、相互に議論・更新しながらサービス開発に活用されることを期待**

ライセンスフリーのアイコンセット (デジタル庁デザインシステムのカラーパレット利用)

Trusted Web Icons for Guideline

Color Blind Check

- Issuer (I)
- Holder (H)
- Verifier (V)

TWDP-A : 学生証を用いた学割のユースケース

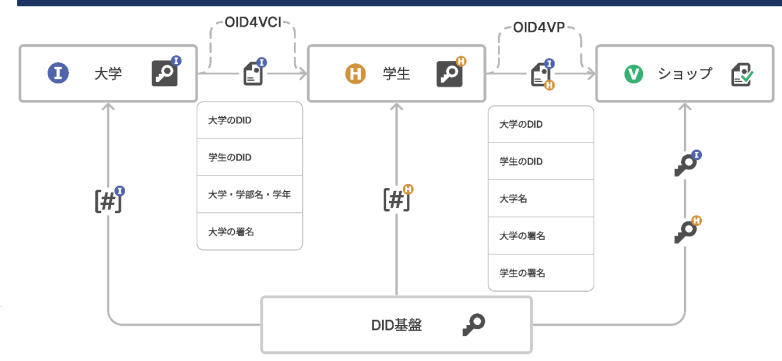
- TWDP-A : 学生証を用いた学割のユースケース
 - 解決する課題
 - どのように解決するか
 - 実装
 - 前提
 - シーケンス
 - メリット
 - 注意点
 - Trusted Webの目指すべき方向性との対応
 - アーキテクチャとの対応

オンラインにおける学生割引を例に説明する。この場合Issuerが大学、Holderが学生、Verifierが学割を実施するオンラインショップとなる。

解決する課題

- 学生 (Holder) の課題 ○X大学の学生である太郎君は、新しいパソコンを買うために、学割キャンペーンを実施しているオンラインショップで購入しようとしている。しかし、学生証の画像の送付を求められ面倒に感じ、またオンラインショップの情報の管理に対して不安感があり、躊躇している。
 - | ペインポイント・画像を撮影して送付するのは面倒・顔写真等の情報もあり、何に使われるかわからず不安
- オンラインショップ (Verifier) の課題 オンラインショップは学生であることを確認するために、学生証の画像の送付を求めており、受け取った画像はクラウドストレージに保存して、目視で有効期限を確認しているが、運用が面倒な上に、本当に本人の学生証かを確認する方法も無く、画像などの情報の漏洩の懸念から学割キャンペーンは終了しようとしている。
 - | ペインポイント・目視確認の運用コストが高い・別人の学生証の画像の可能性はあるが、そこは目をつむっている・画像には個人情報が含まれているため管理コストが高い

システム構成図やシーケンスの掲載



Issue/Pull requestsによるアップデート

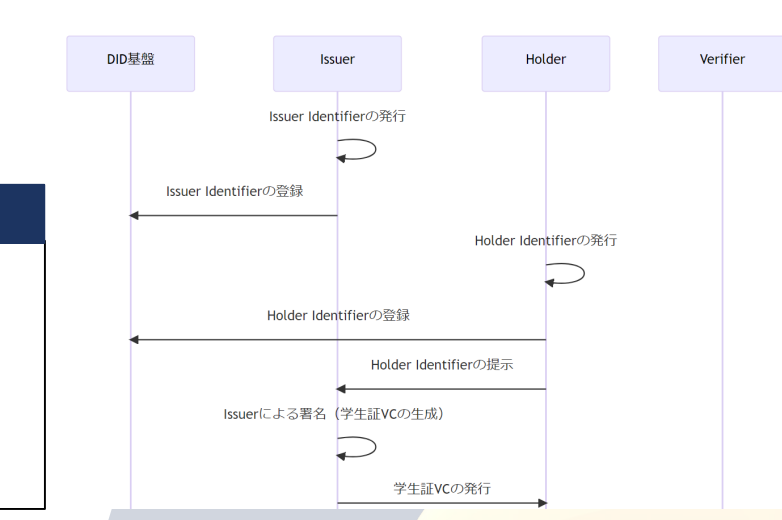
- ☐ どういうシナリオだったらどういテクノロジーを選定すべきか #34 by hqdmc was closed 3 weeks ago
- ☐ デザインパターンと言わずに、実装ガイドラインとして例示するという形がいい #33 by hqdmc was closed 3 weeks ago
- ☐ ユースケースとデザインの間要件の明確化 #30 by hqdmc was closed 3 weeks ago
- ☐ VDR の役割と DID 基盤の役割とその違い・関係性の説明があった方がよい

どのように解決するか

Issuerが大学、Holderが学生、Verifierが学割を実施するオンラインショップであるという情報を学生がオンラインショップに提供し、学割を受け取る。

主な掲載項目

- 解決する課題
- どのように解決するか (要件や技術選定)
- 実装 (前提・シーケンス)
- メリット
- 注意点
- 目指すべき方向性との対応
- アーキテクチャとの対応



実装バリエーションを拡充し、どういシナリオだったらどういテクノロジーを選定すべきかがわかるようにアップデートしていく

3. 国際連携

2-9. G7群馬高崎デジタル・技術大臣会合における関連イベント・閣僚宣言等

4月30日のG7群馬高崎デジタル・技術大臣会合において、デジタルアイデンティティやデジタル証明書について、ベストプラクティスを共有することを合意。本会合の関連イベントとして、「トラストのためのデジタル技術に関するステークホルダー会議」にて、Trusted Webの政策的取組、ユースケースについて、議論を行った。

経済社会のイノベーションと新興技術の推進

閣僚宣言抜粋（仮訳）

我々は、デジタル・アイデンティティ・システムやデータ共有における信頼やセキュリティ構築のためのその他の手段についての政策的な議論を発展させることの重要性を共有する。また、**デジタル・アイデンティティやデジタル証明書についてのベストプラクティスを共有し加速させるとともに、現在行われているデジタル・アイデンティティのガバナンスに関する OECD の勧告案の進展にかかる議論を支持する。**我々は、トレーサビリティの向上やデータの可制御性、データの共有相手の検証性の向上などの論点を含む、信頼できる形でのデータ交換のための互換性ある政策的アプローチと技術について、**2023年3月29日の「信頼確保のためのデジタル技術の活用に関する G7 ステークホルダーカンファレンス」における議論に留意する。**

DFFT具体化のための G 7 ビジョン及びそのプライオリティに関する附属書

閣僚宣言抜粋（仮訳）

コロナ危機と最近のグローバル情勢は、イノベーションと成長を促進するために、ヘルスケア、グリーン／気候変動、モビリティ（自動走行のための地理空間情報プラットフォームなど）といった優先分野におけるデータ共有アプローチについて、志を共にするパートナーが合意を見出すことの価値と必要性を示している。我々は**DFFT 具体化に向けた取り組みの一環として、データ共有を促進すべく、デジタル証明書やデジタル・アイデンティティに係る技術やユースケースの役割を支持する。**データの利用促進は、経済成長のための戦略的な機会でもある。

トラストのためのデジタル技術に関するステークホルダー会議

G7各国政府、招待国/招待機関、トラストサービスに取り組む企業並びに学術団体の関係者が参加し、信頼性のある自由なデータ流通（DFFT）の具体化に向けたトラスト確保のための取組みについて、講演およびディスカッションを実施。「Trusted Web」の基本構想や取組についてクロサカ座長、ユースケースについてORPHE・大日本印刷から紹介した。各国政府より集まったパネリストとのディスカッションが展開された。



2-10. 海外事例

EU : EU Digital Identity Wallet

- 分散型で自らの属性データを管理するDigital ID Walletを導入する法案を2021年発表。
- 認証のためのお墨付きのついた属性情報の利用を含め、Trusted Webと類似した発想（2030年までに広く普及を目標）
- 技術仕様を定めたArchitecture and Reference Framework(ARF)を公表(2023/2)

カナダ : PCTF (The Pan-Canadian Trust Framework)

- DIACC※1(カナダの官民組織)がデジタル・アイデンティティを安全に活用するハイレベルな要件を定めたフレームワークを発表。
- VCを活用し、越境を想定したデジタル学修証明書のユースケースを進めている。
- この他、ブリティッシュコロンビア州で、銀行が確認した属性情報を、本人の同意の元に他のサービスに利用する取組もあり。

※1 Digital ID & Authentication Council of Canada

Trusted Web

英国 : The UK digital identity and attributes trust framework

- 個人に関する情報を証明できるサービスを簡単かつ安全に使用可能にすることを目的として、属性情報を提供する際に遵守するべきルール等を記載。
- VC、DIDを活用し、医療従事者の資格証明に活用。職場移転に7日程度要していたものの短縮に成功。

→ これら各国等と**情報共有**やユースケースベースでの**相互運用性の検証**を進めているところ

4. 今後の取組

2-11. 今後の活動（2023年度）

ユースケースの創出

- ・実践的な導入例の創出に向けたユースケースベースでの具体的な実装の検証（2023年度12件の実証事業を実施中）
- ・ユースケースの開発の進捗に応じたレビュー及びフィードバックを通じた課題の抽出
- ・インターネット上のデータを活用する生成AIに対して、Trusted Webがどのように貢献し得るかについて議論

企業・エンジニアによる取組の更なる促進

- ・企業のさらなる取組推進に向けた「推進ステップ（仮称）」の具体化
- ・GitHubの活用（実装ガイドラインの公開）による技術的検討の活性化（エンジニア等の積極的な関与による継続的な更新も想定）
- ・開発されたユースケースをベースにしたワークショップを通じて多様な主体のアイデア創発を活性化

社会実装の加速化

- ・ガバナンスそのものやガバナンスの運営体制の在り方、トラストフレームワーク等の具体化
- ・Trusted Webを具現化するための官民の情報連携や業界ごとに議論を深める場の検討

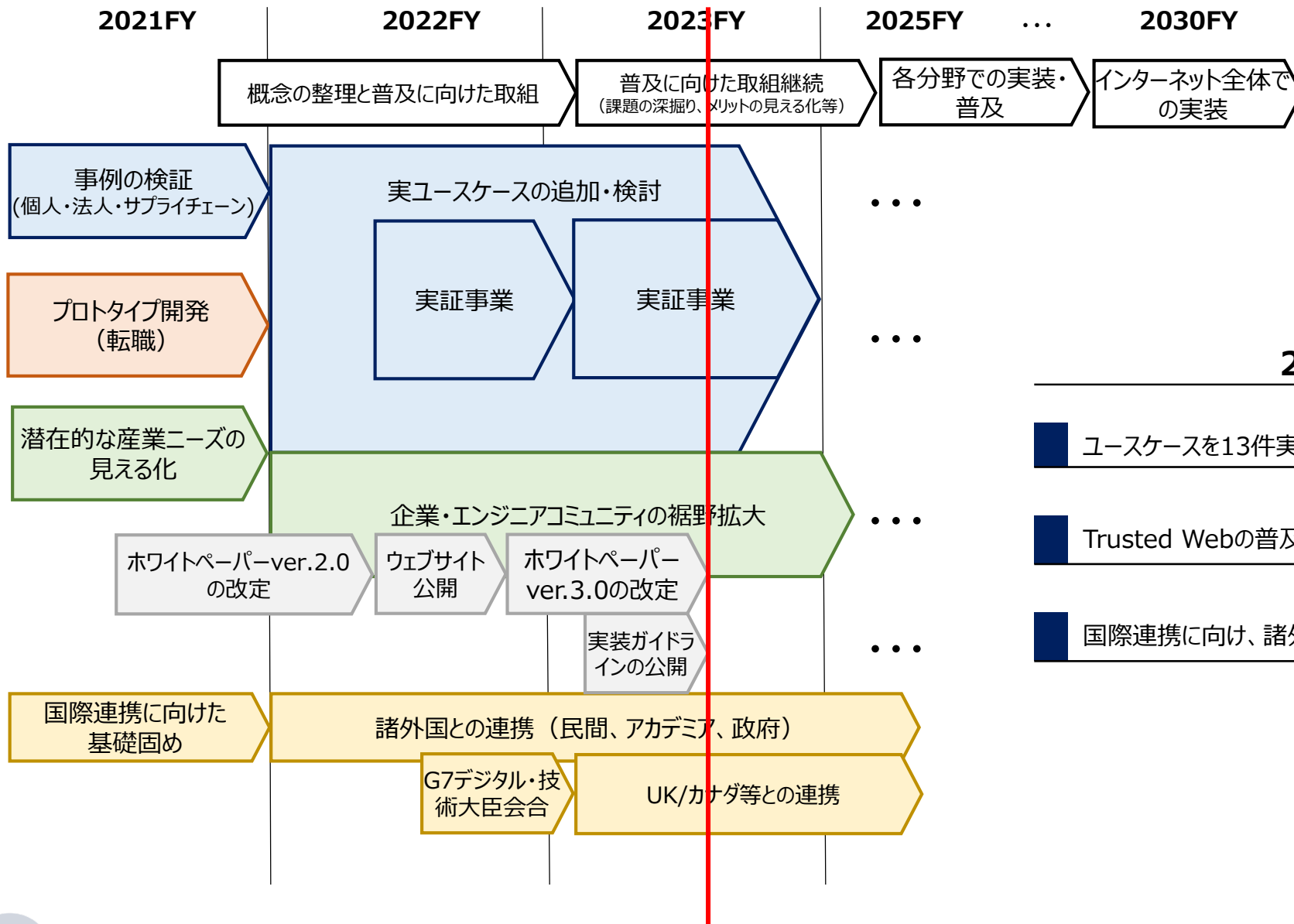
国際連携

- ・G7を契機にした各国や関連団体との具体的なプラクティスの共有や相互運用性の確保に向けた議論の推進

全体

- ・官が主導して既に設計が進んでいる取組（例：ウラノスエコシステム）とTrusted Webとの連携推進
- ・ユーザーの行動変容を含めた、Trusted Webのあるべき姿のデプロイメント
（同じ動作やプロセスを経ることで、誰もが同じ結果を得られるため、安心して信頼が醸成されていくといった「セレモニー」の確立）
- ・既存の仕組みからシフトしていくプロセスのイメージやその注意点、今後のロードマップの検討

2-12. 2030年に向けた中期的な戦略（イメージ）



2022年度達成目標の結果

- ユースケースを13件実証し、事業領域や実装のバリエーション拡大
- Trusted Webの普及に向け、ウェブサイトを開発
- 国際連携に向け、諸外国との連携、G7デジタル大臣会合での合意

2022年度 選定されたユースケース一覧

	ユースケース名	事業者名	分野
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	株式会社DataSign	個人
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デジタル株式会社	個人（メタバース）
3	学修歴等の本人管理による人材流動の促進	国立大学法人東京大学	個人（人材スキル）
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株式会社	個人（人材スキル）
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	シミック株式会社	ヘルスケア
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	株式会社ORPHE	ヘルスケア
7	分散型IDを活用した炭素排出量トレースシステム	DataGateway PTE LTD	サプライチェーン（CO2）
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株式会社	サプライチェーン（製造業）
9	Trusted Networkによる社会ITインフラの信頼性・強靱性向上の実現	アラクサネットワークス株式会社	サプライチェーン（経済安保）
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	東芝テック株式会社	文書（IoT）
11	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	株式会社電通	行政
12	法人税制と工業会証明書	一般社団法人情報サービス産業協会	行政
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 ※企画のみ、開発なし	大日本印刷株式会社	個人

2023年度 選定されたユースケース一覧

	ユースケース名	事業者名	分野
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	個人
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	個人
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 ～お金の問題なく学び自らの可能性を広げられる世界へ～	Institution for a Global Society株式会社	個人（人材）
4※	大学技術職員の活躍に向けたスキル見える化：スキルの質保証と主体的情報開示の試行 【企画のみ、開発なし】	富士通Japan株式会社	個人（人材）
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	個人（人材）
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（CMP）【企画のみ、開発なし】	みずほリサーチ&テクノロジーズ株式会社	サプライチェーン
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	サプライチェーン
8※	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（該当分野：医療・ヘルスケア）	シミック株式会社	ヘルスケア
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	ヘルスケア
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	株式会社電通国際情報サービス	法人、金融
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【企画のみ、開発なし】	一般社団法人情報サービス産業協会	行政
12	Trusted web advertising system with Originator Profileを活用したWeb広告取引における信頼性付与	Originator Profile 技術研究組合	メディア

※ 昨年度からの継続案件

(令和5年11月15日現在)

浦川 伸一	日本経済団体連合会 デジタルエコノミー推進委員会企画部会長 損害保険ジャパン株式会社 顧問
太田 祐一	DataSign 代表取締役
黒坂 達也	株式会社 企 代表取締役
崎村 夏彦	東京デジタルアイディアーズ株式会社 主席研究員
白坂 成功	慶應義塾大学大学院 システムデザイン・マネジメント研究科 教授
武田 晴夫	株式会社日立製作所 技師長
津田 宏	富士通株式会社 フェロー SVP 富士通研究所
富本 祐輔	トヨタファイナンシャルサービス株式会社 シニアバイスプレジデント
橋田 浩一	東京大学大学院情報理工学系研究科 教授
藤田 卓仙	神奈川県立保健福祉大学 特任准教授
増島 雅和	森・濱田松本法律事務所 パートナー弁護士
松尾 真一郎	ジョージタウン大学、バージニア工科大学 研究教授
三島 一祥	合同会社Keychain 共同創設者
○村井 純	慶應義塾大学 教授
安田 クリスチーナ	Microsoft Corp. Identity Standards Architect

(○：座長)

オブザーバー：デジタル庁、総務省、経済産業省、

国立研究開発法人情報通信研究機構（NICT）、独立行政法人情報処理推進機構（IPA）

(令和5年11月15日現在)

浅井 智也	一般社団法人 WebDINO Japan CTO
浅井 大史	株式会社Preferred Networks インフラ戦略担当VP・シニアリサーチャー
阿部 涼介	慶應義塾大学 大学院政策・メディア研究科 特任助教
岩田 太地	日本電気株式会社 DGDFビジネスユニット/主席ビジネスプロデューサー
菊池 将和	Secured Finance AG Founder & CEO
○黒坂 達也	株式会社 企 代表取締役
佐古 和恵	早稲田大学 理工学術院 基幹理工学部情報理工学科 教授
鈴木 茂哉	慶應義塾大学大学院 政策・メディア研究科 特任教授
富士栄 尚寛	OpenID ファウンデーションジャパン 代表理事
松尾 真一郎	ジョージタウン大学、バージニア工科大学 研究教授

(○ : 座長)