Trusted Web

Trusted Web ホワイトペーパーver2.0概要

2022年８月

内閣官房デジタル市場競争本部事務局

1. 検討の背景とこれまでの検討経緯

○COVID-19を契機に社会全体のデジタルトランスフォーメーション（DX）が加速。**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、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、2020年6月の「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」を発足**、**2021年3月にホワイトペーパー Ver1.0**をとりまとめた。

○その後、ホワイトペーパーVer.1.0で示された考え方や構想の具体化、深堀りを図るためユースケース分析やプロトタイプ開発を実施し、課題を抽出。
　それらを踏まえ、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**、あるべき**ガバナンスの検討**などを行い、Trusted Webの実現に向けた今後のさらなる道筋を示すものとして、**2022年７月にホワイトペーパーVer2.0**をとりまとめた。

2. 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、**その歪みが様々なペインポイント**をもたらしている。

ペインポイントの例

○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**

ペインポイントの原因

○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”

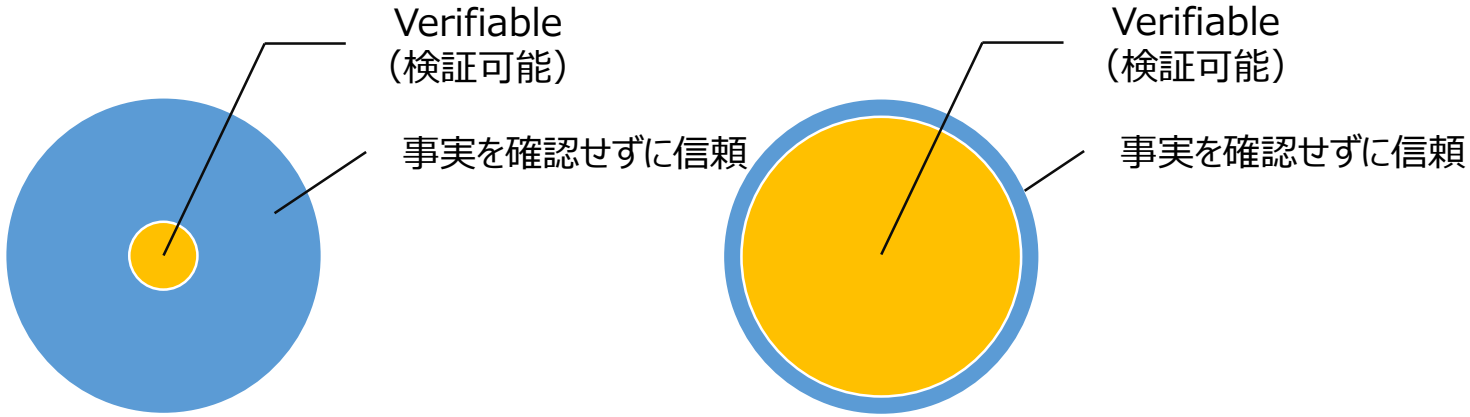
3. Trusted Webが目指すべき方向性

○**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**

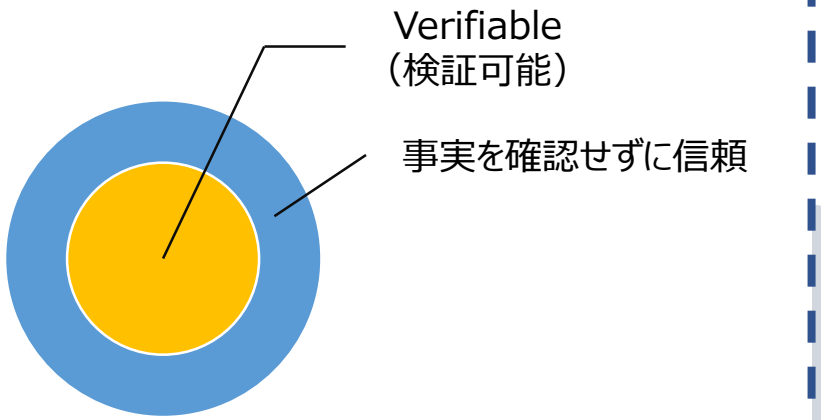
仕組みによりVerifiable（検証可能）な部分が変わる



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。

ブロックチェーンなど

＊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

3. Trusted Webと「Web3」

- 昨今、議論されている「Web3」は、現状のインターネットやウェブに対する**問題意識**や、**分散型で検証可能な部分を広げることを志向**しているという意味での方向性で、**Trusted Webと共通するものがある**と考えられるが、**「Web3」**の厳密な定義については様々な見解があり、**定義は定まっていない**と考えられる。

- Trusted Webは、**アイデンティティ管理のあり方に重点**を置き、**技術中立的な取組**として進めており、ブロックチェーン技術の活用のみでなく、検証可能性を高める様々な枠組を活用し、組み合わせることにより、Trustのレベルを高めることを目指す。

- Trusted Webの実現に当たっては、インターネットやウェブといったインフラは漸進的に作っていくことが重要である。現在のインターネットアーキテクチャ等との**継続性**や既存の仕組みとの**相互運用性**、**特定の技術に依存しすぎることのない更改容易性**を充足しながら、「Trust」のレベルを高めたデジタル社会のインフラを目指す。
  また、Trusted Webの実装を進めていくに当たっては、こうしたデジタル・インフラにおける**ガバナンスのあり方**に着目することも重要。

4. Trusted Webのもたらすベネフィット

事業者にとってのベネフィット

・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
→ 様々な主体が業種や部門を超えた**協創することが求められるデジタル・トランスフォーメーション（DX）**を進めるに当たり、その前提となる**事業者間連携を円滑にする上で不可欠**

エンドユーザーにとってのベネフィット

・データのコントロールにより、**必要に応じたデータのみをやりとり**することができる
・データをユーザーのもとに集約させることにより、**プラットフォーム事業者などの関与なしで情報を利用・共有**することも可能に
・やりとりされる**データの確からしさが高まる安心感**

デジタル・インフラたるTrusted Web実現に企業が参画していくことの意義

・新しく作られつつあるアーキテクチャを活用して**サービスの価値をいち早く検証** → デジタル・インフラ上で**スケール**させる
・**新たな技術やパラダイムを導入する側に**立つことで、今後のビジネスを優位に進めることが可能

新たな連携の在り方

・産：試行段階からのサービス検証や、検証結果のフィードバックによる共有財としてのデジタル・インフラ作りへの関与
・学：長期的な視点に立ったデジタル・インフラのトラスト設計や、ウェブ技術に関わる国際コミュニティとの連携推進
・官：ファシリテーションやインセンティブの総合デザイン

4. 事業者における価値創造につながることが期待されるケースのイメージ

①相互に信頼関係ができていない者同士のデータのやりとり

- サプライチェーン管理
  （例：脱炭素のトレサビリティ、車載蓄電池の履歴、農業分野の生産予測・調整、受発注プロセス　等）
- 相互評価のトラストスキーム
  （例：DX・コロナ後で流動化した人材・資産のリバンドリングやシェアリングサービス　等）
- モビリティ、インバウンド、防災・減災など他業種にまたがるデータ連携
  （例：ドローンのセキュリティ・運行管理、海外旅行者の個人情報管理　等）

②確認コストの高い分野・紙等での検証が大量に発生している分野

- 金融、保険分野（例：企業の財務・非財務データの共有、マイクロペイメント　等）
- 行政手続　　（例：中小企業等にとっての補助金申請、死亡届　等）

③個人（法人）によるコントロールのニーズが高い分野

- ヘルスケア分野　　（例：薬の処方や治験におけるバイタルデータ活用、ウェアラブルデバイスからの健康状態の共有　等）
- デジタルコンテンツ分野（例：コンテンツの著作権管理、メタバースでのアセット管理　等）
- デジタル広告分野　　（例：ポストクッキー後の同意スキーム　等）

④大量のIDやデータを持っていながら、さらなる活用が考えられる分野

- 鉄道、航空会社等のインフラ事業者、小売事業者
- 地方自治体

5. ユースケース検証とプロトタイプ実装

ver1.0の公表後、ver1.0で提起された４つの機能について、その課題を抽出するために、以下の３つのユースケースについて具体的な検討を進めるとともに、１つのユースケースについてプロトタイプを実装した。

①「個人」の属性情報のやりとり ⇒ プロトタイプを実装

・「転職活動」における個人の属性情報の取扱いについて検討

【ペインポイント】　機微な個人の属性情報の開示先・開示範囲のコントロール
提供される個人の属性情報の信頼性確保

【検討すべき課題】　ver1.0で提起された**４機能について、実装を意識した再整理が必要**
Trace機能をどのように実装するかについても整理が必要

②「法人」の行政庁との情報のやりとり（法人と補助金）

・「事業再構築補助金」をケースに申請情報の取扱いについて検討

【ペインポイント】　申請者側の申請に伴う負担
申請情報の確認の負担

【検討すべき課題】　**書類の中身の検証**と**提出があったという事実の検証**といった**異なる種類の検証**の存在を踏まえた整理の必要性
既存のエンティティ間の信頼に依存しない形での検証可能性の拡大の必要性

③「サプライチェーン」における情報のやりとり

・化学物質の規制に対応するためのサプライチェーンにおけるデータの取扱いについて検討

【ペインポイント】　規制やノウハウに関係するデータの開示先・開示範囲のコントロール
提供されるデータの信頼性確保

【検討すべき課題】　複数者間で**データが加工されながら伝達**される中で、営業秘密等に配慮して、
その**通信履歴の開示範囲を制限**しながら、**データの信頼性**自体は担保される仕組みの必要性

5. プロトタイプの実装

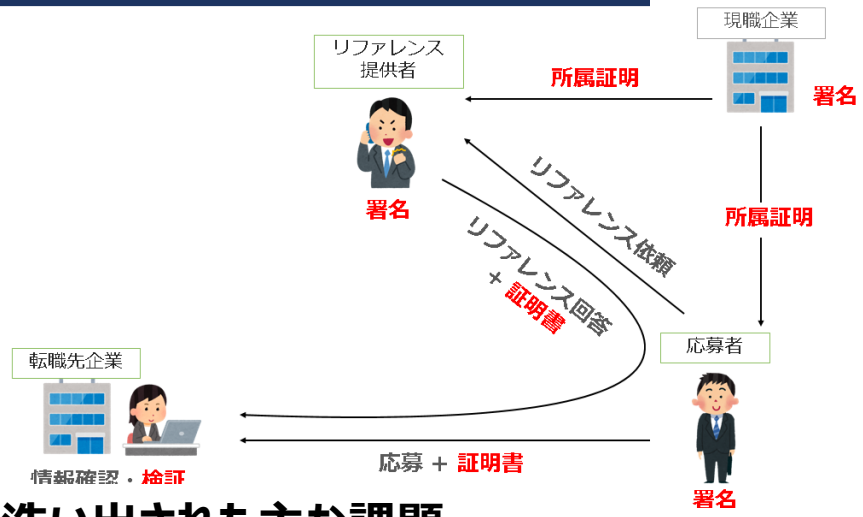
「個人」のスキル・実績等の転職時におけるやりとりについてTrusted Webの４つの機能をブラウザベースで実装
「データが確認された状態で選択的に渡す・受け取れること」をDIDやVCを利用することで実現

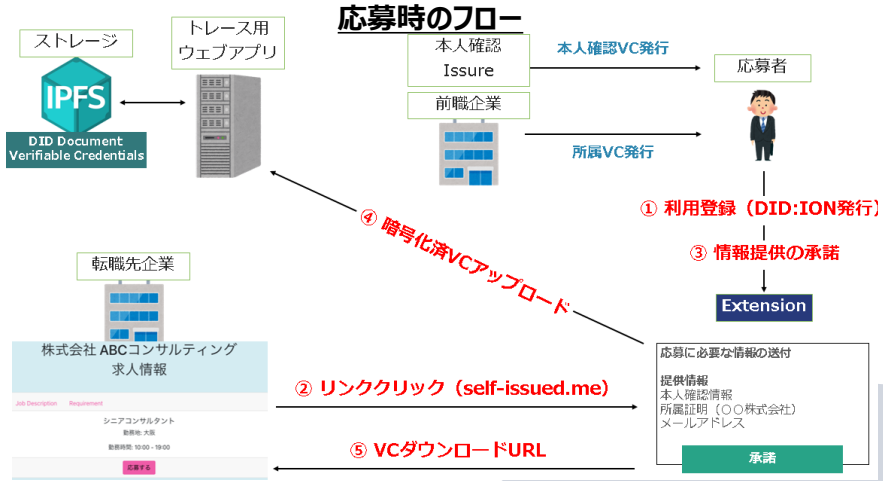
DID Decentralized Identifiers
VC Verifiable Credentials ※

■プロトタイプに実装されたTrusted Webの４つの機能

開発したプロトタイプのリポジトリ https://github.com/TrustedWebPromotionCouncil/

Identifier管理機能	利用者が自由にDIDを発行でき、必要な情報をひもづけられるような設計
Trustable Communication機能	データ受領時のみデータを復号できる形式でVCを作成し、正当な発行者による署名かを検証できる機能
Dynamic Consent機能	必要なデータをデータ提供者自身で確認し、意思決定にもとづいて提供できる機能
Trace機能	提供したデータに対して、いつ誰がアクセスしたのかを確認することができる機能





出典：【5.ピアレビュー】「プロトタイプ開発の検討状況」太田祐一氏、鈴木茂哉氏 https://www.youtube.com/watch?v=BABYKkcSjg0

■洗い出された主な課題

- ✓DIDやVCの仕組みを理解していない人でも、DIDやVCがもたらす価値が伝わるようなユーザーインターフェースをどのように作るか
- ✓データはIPFS※に保存される仕様としたため、ダウンロード履歴が残らずTraceできない（集中サーバで認証、アクセス記録を行ったが、迂回できてしまう問題あり）
- ✓本人確認VCの発行主体や所属証明VCの発行主体の公開鍵が正当性を担保した状態で公開されている必要がある
- ✓ブラウザ・エクステンションを削除すると秘密鍵が失われてしまう（HDWalletを採用したが、12種類の単語を覚えることは困難である）

※InterPlanetary File System

※DID:分散型識別子。個人や組織が自分の識別子を生成。中央機関に依存せず、個人情報等の開示範囲を制御しながら、自分自身や自分が管理するものを識別することをサポートする
VC:検証可能な属性情報。属性情報を第三者(発行者)に証明してもらうことができるしくみ。

5. ユースケースとプロトタイプ開発から抽出された課題のまとめ

○実装したい機能が「Trustable CommunicationなのかTraceなのか」等、機能の整理が必要

→ ver1.0で提起した４つの機能の実装を意識して機能間の関係を再整理する必要がある

○３つのユースケースの分析からアーキテクチャを検討するうえで、以下の論点が洗い出された

✓ **Trustと検証可能性**

「検証可能な領域を広げる」とされていたことについては、デジタル署名に着目してTrustと検証可能性について整理

✓ **データ**

データについては検証可能性の観点で整理

✓ **エンティティ**

既存の信頼のモデルはエンティティ間の信頼に頼っているものが多く、エンティティ間の信頼関係に依存せずに、検証可能性を担保することが必要
（例：法人のユースケースにおいて、金融機関からのデータが中小企業等を介して提供される場合）

✓ **アイデンティティと可視性**

あるアイデンティティは複数のグループに属する可能性があるが、これらのグループ同士はグループの所属メンバーや、グループ自身の存在を知り得ない場合等、可視性にはバリエーションがある。また、グループ間で検証可能なデータについて、共有に制限がある場合がある。これらへの対応が必要
（例：ユースケースのサプライチェーンにおける川下企業と川上企業の関係等）

✓ **トランスポート**

通信における検証可能性を高める上で、送信者及び受信者を検証できる単位での通信とする観点、通信者間の合意形成を実現する観点から、メッセージオリエンテッドなサービスを基礎として用い、複数のメッセージそれぞれの内容とアイデンティティを記録する方法が有効

✓ **データの保管場所**

トランスポートをメッセージオリエンテッドなサービスで構成するならば、やり取りの参加者の各々がメッセージ単位で記録と管理ができ第三者に委ねる必要はない。
実装手段としては、データの保管場所としての視点で、ウォレットはその一つとなり得る。

6. Trusted Webで目指す信頼の姿

以上の検討を踏まえ、**Trusted Webで目指す信頼の姿**を以下のように整理した。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

・データのやりとりのモデルは、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

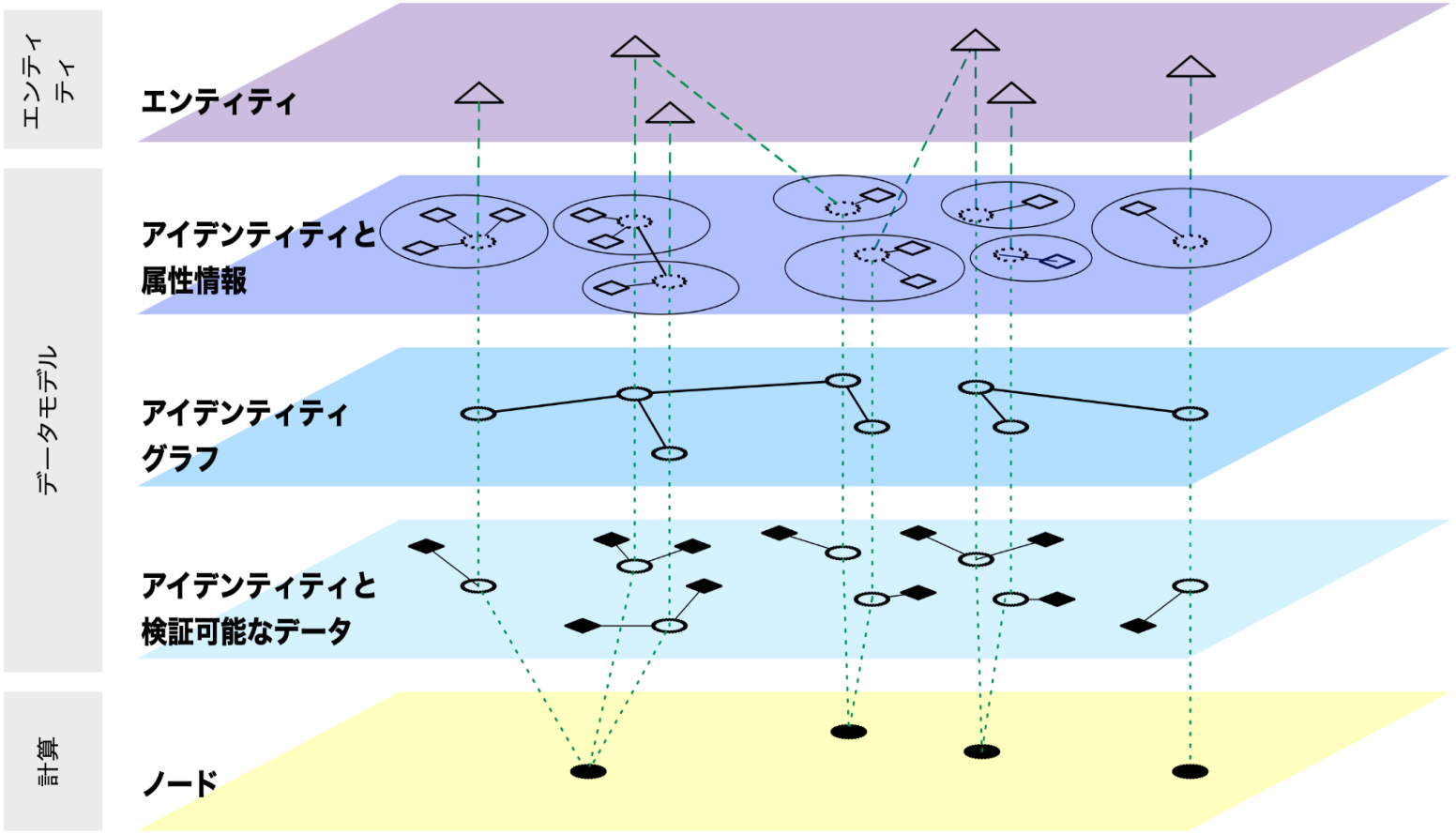
※ OpenID等の標準を用いたシステムや、DID/VCといった技術を用いた実装などが考えられる。

6. Ver1.0での４機能を６構成要素にて再整理

Trusted Web(ver1.0) の4機能を、
データを主体とした視点で、**検証可能なデータ**、**アイデンティティ**、**メッセージ**、**トランザクション**の4つの構成要素とし、
計算資源と通信を主体とした視点で、**ノード**、**トランスポート**の２つの構成要素として、あわせて**６構成要素にて整理**。

Function	Component	Description
Identifier管理	**検証可能なデータ** *Verifiable Data*	Trusted Webでの**操作の対象**となるデータ。 **《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
Trustable Communication	**アイデンティティ** *Identity*	**検証可能なデータ**の一種。**属性情報**（所属組織名など）によって構成。 データを検証可能とするため、アイデンティティに結びつけられている署名にまつわる情報との連携が必須 **アイデンティティ間の関係を表すアイデンティティグラフ**を参照可能とし、データの検証可能性を拡大
Dynamic Consent	**ノード** *Node*	**メッセージの送受信**を司る。**受信時に計算処理（合意形成など）を実行**できる。 ノードは**トランザクションを記録**し、記録はアイデンティティに紐づけて**保持**。
Trace	**メッセージ** *Message*	送信元から送信先への配送の確実性のある**一方向メッセージ送信**。 **ノード間でやりとりされるデータ**であり、ノードで実装される。
	トランザクション *Transaction*	**メッセージ送受の順番**をノード間で確認できるデータとメカニズム。 **分散保持**しつつ、記録を全てのノードで保持することを保証。 **外部記録に依存せず**、秘匿した形で関係者間のみで共有できる。
	トランスポート *Transport*	他のノードに対して**メッセージを送信するための適切な手段**を提供。 様々な技術（インターネット・近接型無線通信など）を適用可能とするため、**包括的な通信モデルの設計**が必要。

6. Trusted Webを実現するためのアーキテクチャ



エンティティは自然人や法人といった主体を示す
（例：転職者、リファレンス提供者、転職先企業　等）

エンティティは複数のアイデンティティを有する
（例：転職者の社員としてのアイデンティティ　等）
アイデンティティは属性情報によって構成される
（例：転職者の入社年、生年月日　等）

アイデンティティ間の関係を示すグラフ
※実際はアイデンティティ毎にグラフの見える範囲は異なる
（例：転職者とリファレンス提供者は同じ企業の社員であるという直接的な関係がある）

検証可能なデータはアイデンティティによって署名されて検証可能なデータとなるため、アイデンティティに紐づくと整理
（検証可能なデータの例：転職者の業務経験　等）

アイデンティティの代理としてメッセージの送受信を司る
メッセージの送受信に伴い様々な計算処理ができる

トランスポートは、メッセージオリエンテッドなサービスを基礎とするのが有効
様々な技術を適用可能とする包括的な通信モデルの設計に

(注)　上記の例はケースによって様々な整理があり得ることに留意する必要がある

6. Trusted Webの構成要素

6つの構成要素について、それぞれ、データモデルと操作について、整理を行った。

検証可能なデータ (Verifiable Data)
- ・データモデル
  - 検証可能なデータの構成要素
  - 高度なデータ操作に関わるデータの構成要素
- ・検証可能データに対する操作
  - 検証可能な情報の作成
  - 署名自身の検証
  - 署名者の検証
- ・高度なデータ操作

アイデンティティ（Identity）
- ・データモデル
  - 単一のアイデンティティ
  - アイデンティティグラフ
- ・アイデンティティに対する操作
  - 署名（アイデンティティが制御下にある場合）
  - 発見
  - 署名自身の検証のためのデータ取得
  - 署名者の検証のためのデータ取得
  - 高度なデータ操作
- ・アイデンティティグラフへの操作
  - アイデンティティ間の関係の追加
  - アイデンティティ間の関係の削除
  - アイデンティティ間の関係の更新
  - パスの発見
  - パスに対する検証可能性の評価

ノード （Node）
- ・データモデル
- ・ノードの操作
  - メッセージ送受信操作
  - トランザクション操作
  - アクション（合意形成等）

メッセージ（Message）
- ・データモデル
- ・メッセージの操作
  - メッセージの作成
  - メッセージの検証

トランザクション（Transaction）
- ・データモデル
- ・トランザクションの操作
  - トランザクションの開始
  - トランザクションの終了
  - トランザクションの検証

トランスポート（Transport）
- ・(詳細は今後の議論)

6. 構成要素　検証可能なデータ

検証可能なデータのモデル

・データ
・データに対するデジタル署名
・検証鍵※
　あるいは
検証鍵を導出可能なアイデンティティのデータ
・署名の意図（データとして意図を示せる場合）

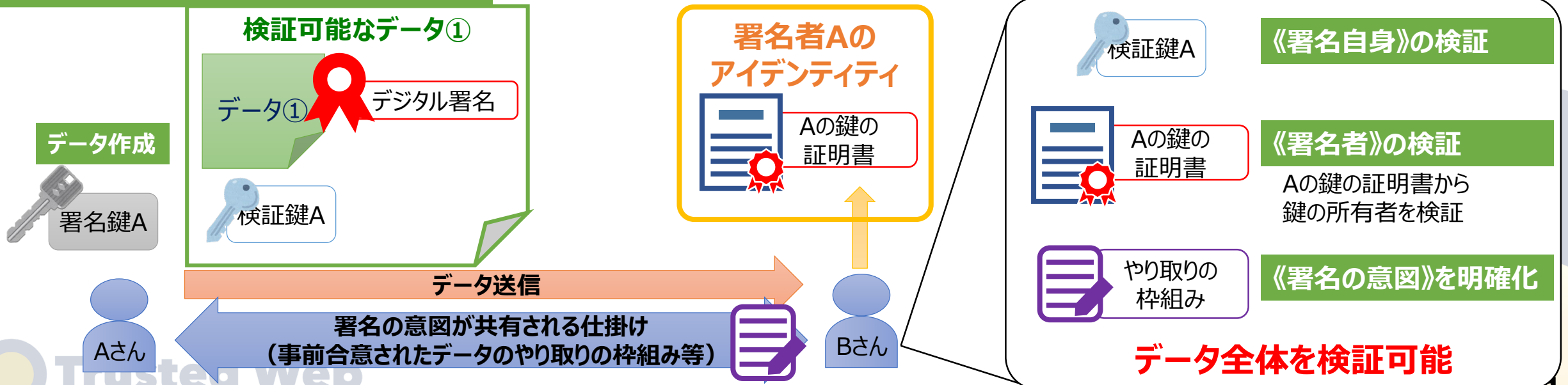
※ホワイトペーパーVer2.0では公開鍵暗号の鍵ペアについて、公開鍵を「検証鍵」、秘密鍵を「署名鍵」として記述している

高度なデータ操作

・ゼロ知識証明（※１）や秘密計算（※２）等、データに対する高度な暗号技術による操作が提案されている
・それらの操作を導入できるが、アーキテクチャの視点ではアイデンティティと連携した操作として整理した

（※１）例：パスワード自体は明かさずに、自分がパスワードを知っているという事実を証明
（※２）データを暗号化したまま様々な分析が可能な技術

検証可能なデータに対する操作の１例



6. 構成要素　アイデンティティ

アイデンティティのデータモデル

・デジタル署名に関する属性情報
・その他の属性情報

アイデンティティグラフのデータモデル

（アイデンティティを《節点》とし1対1の関係を《辺》とするグラフ。アイデンティティはアイデンティティグラフを個別に管理する。）

・アイデンティティ
・二つのアイデンティティそれぞれを識別する情報（アイデンティティ識別子等）
・アイデンティティ間の関係を示すデータ

アイデンティティに関する操作

i. 署名：
アイデンティティに紐付く署名鍵を用いた署名が可能である場合は、当該アイデンティティによる署名が可能。アイデンティティには、この署名のための操作が必要

ii. 発見：
アイデンティティは何らかの手段で発見できる必要がある

iii. 署名自身の検証のためのデータの取得：
アイデンティティによるデジタル署名を検証するためには、当該アイデンティティに結びついた鍵（検証鍵）が必要

iv. 署名者の検証のためのデータの取得：
署名者の検証を行うために、検証鍵から署名鍵の所有者を特定し、検証できる必要がある

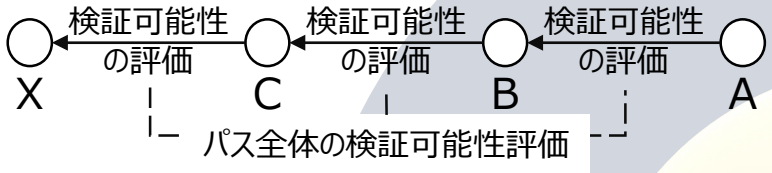
v.高度なデータ操作：
高度な暗号化技術を実装している場合は、これに関連した操作が実装されることが想定される

アイデンティティグラフに関する操作

i. アイデンティティ間の関係の追加
ii. アイデンティティ間の関係の削除
iii. アイデンティティ間の関係の更新
iv. パスの発見
v. パスに対する検証可能性の評価

※ 検証対象となるデータを署名したアイデンティティまで到達できるようにグラフをたどる。たどることができる節と辺の組み合わせをパスと呼ぶ。

※ パスを構成する辺についての検証可能性を評価することで、パス全体の検証可能性が評価でき、最終的に、終点となるアイデンティティが示したデータの検証可能性が評価できることになる。



Aが、Bによって提供されたデータについて、CやXが示したデータの検証可能性を評価できる

6. 構成要素（ノード、メッセージ、トランザクション、トランスポート）

ノード

データモデル
- ノード識別子
- アイデンティティ
- アイデンティティグラフ
- トランザクションの記録
- アクション

ノードの操作
- メッセージ送受信操作
- トランザクション操作
- アクション（合意形成等）

メッセージ

データモデル
- ヘッダ
  - 送信先ノード識別子
  - 送信元ノード識別子
- ペイロード
  - 送信するデータ
- 送信元による署名

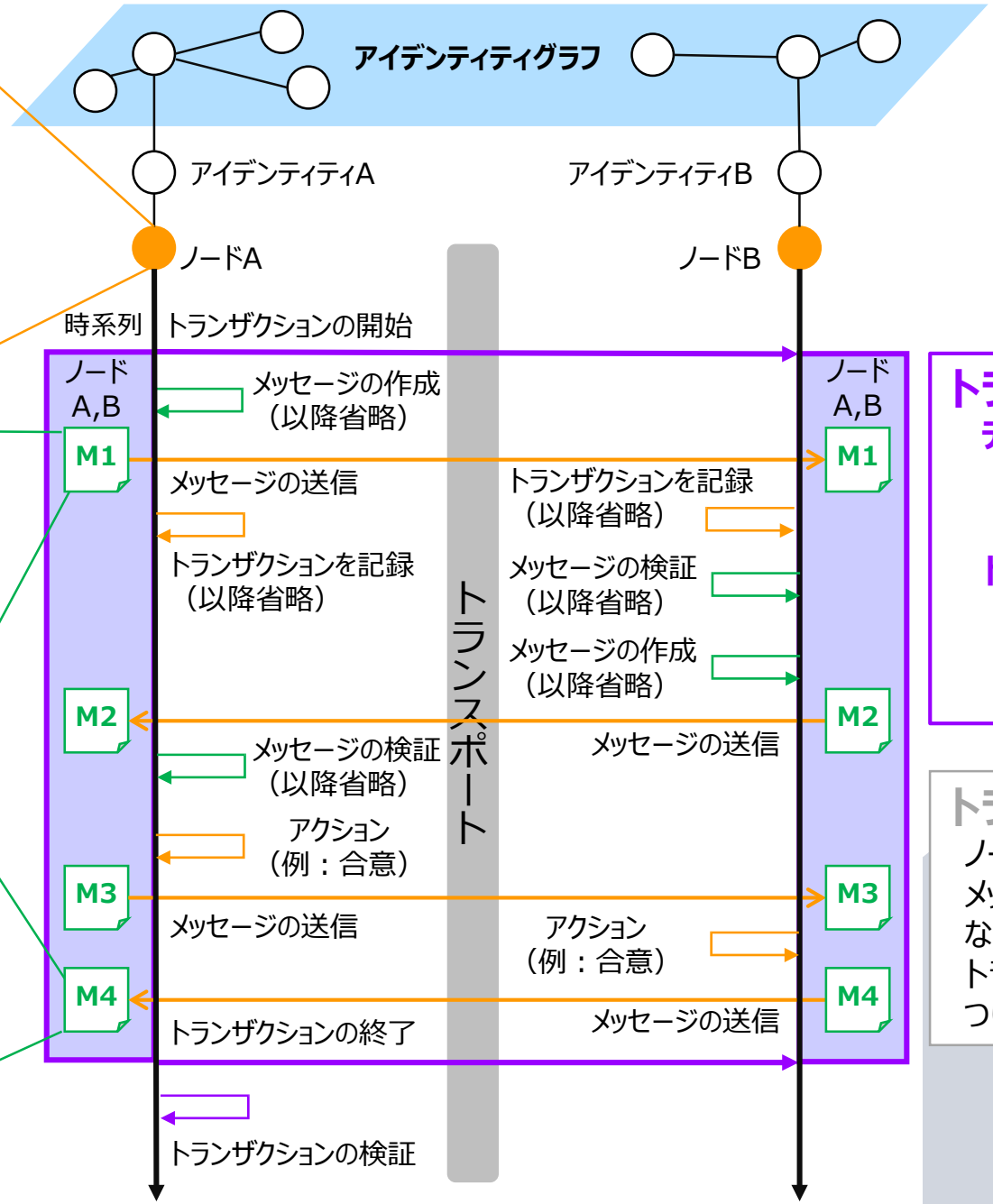
メッセージの操作
- メッセージの作成
- メッセージの検証

メッセージ１

To　　：ノードB
From：ノードA
データ①
（部分開示）
デジタル署名

メッセージ４

To　　：ノードA
From：ノードB
データ④
デジタル署名



トランザクション

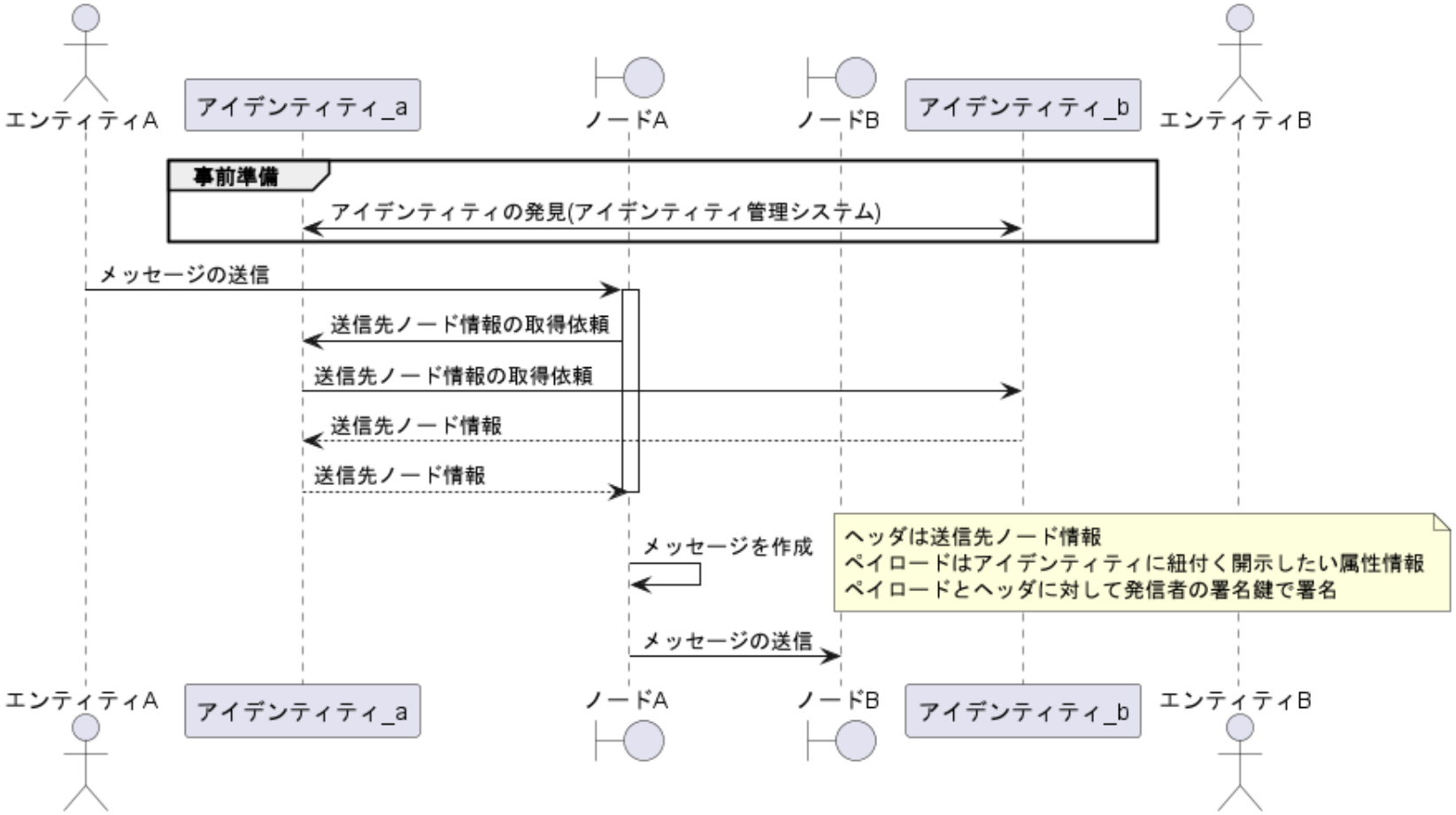
データモデル
- 参加ノード
- やり取りされたメッセージ

トランザクションの操作
- トランザクションの開始
- トランザクションの終了
- トランザクションの検証

トランスポート

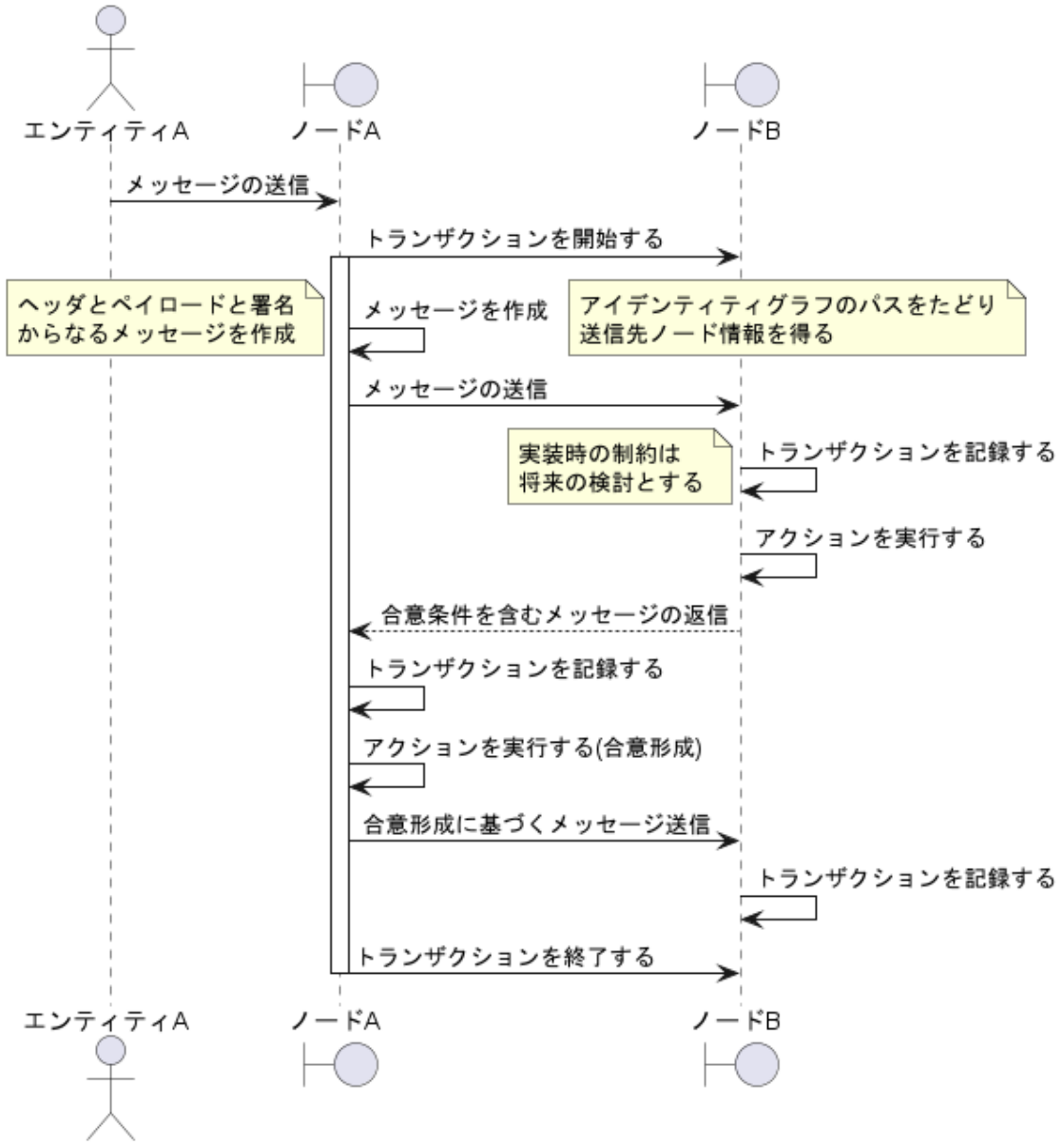
ノードに対し、他のノードに対してメッセージを送信するための適切な手段を提供
トランスポートの具体的な実装については、今後検討

6. ワークフローのイメージ：ユーザー（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する



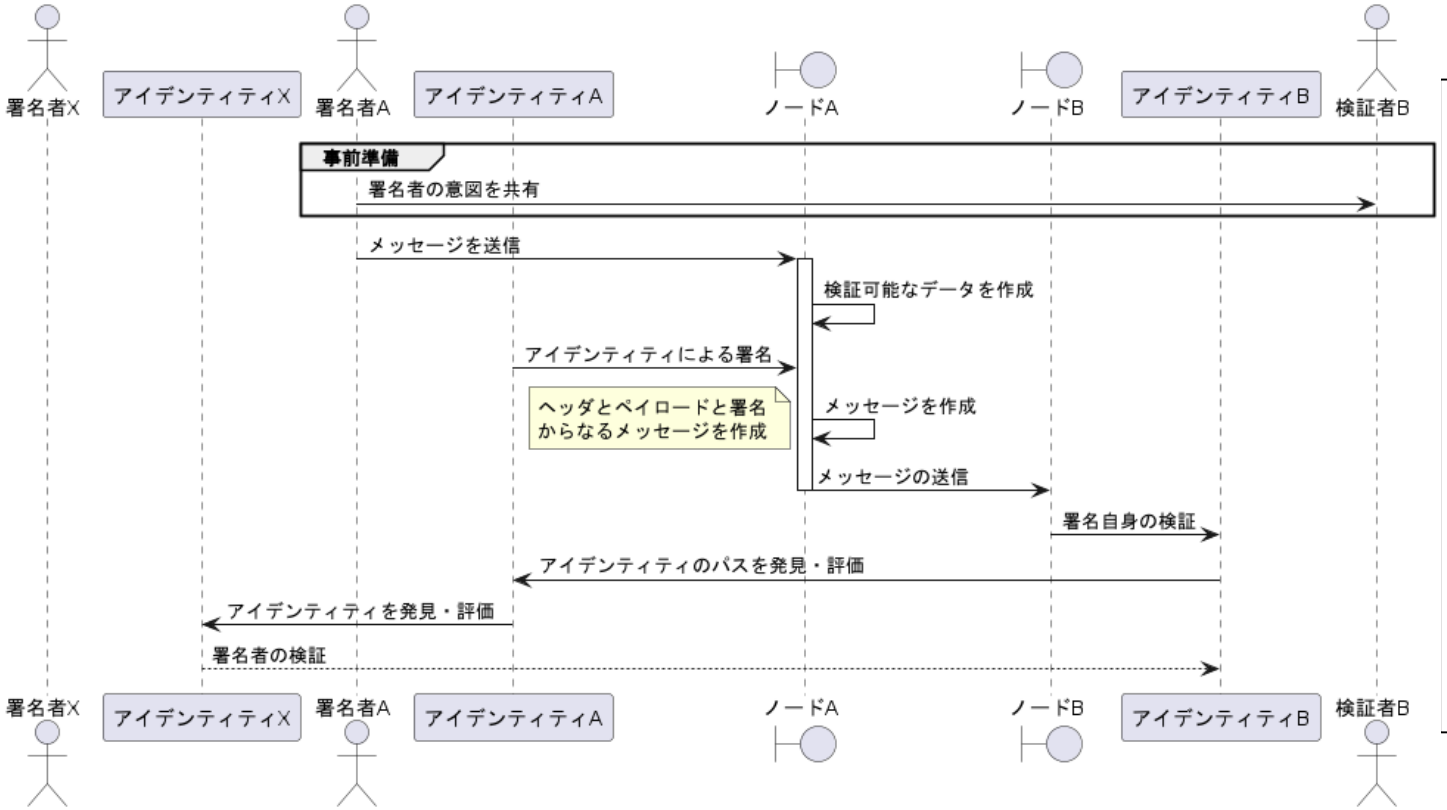
- 【アイデンティティ】双方がアイデンティティ管理システムなどを利用して事前に作成されている相手のアイデンティティを発見する
- 【メッセージ】ヘッダとペイロードと署名からなるメッセージを作成する
  - ヘッダはアイデンティティグラフのパスをたどって取得した送信先ノードの情報
  - ペイロードはアイデンティティに紐付く開示したい属性情報
  - 署名は検証可能なデータ
- 【ノード】における操作でメッセージ送受信を行う

6. ワークフローのイメージ：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つつ、その合意の履行のトレースを可能とする



- 【メッセージ】ヘッダとペイロードと署名からなるメッセージを作成する
  - ヘッダはアイデンティティグラフのパスをたどって取得した送信先ノードの情報
  - ペイロードは合意条件（開示範囲・開示期間など）
  - ペイロードとヘッダ全体に対して発信者の署名鍵で署名し、メッセージの署名とする
- 【トランザクション】を開始する
- 【ノード】における操作でメッセージ送受信を行う
- 【ノード】に受信したメッセージに対してアクションを実行し、合意形成する
- 【ノード】送受信したメッセージを順次記録し、トランザクションを構成する
- 【ノード】各送受信ノードはメッセージの送受に伴い、逐次、トランザクションを記録する
- 【トランザクション】を終了する
- 【トランザクション】の検証をする

6. ワークフローのイメージ：検証（verify）できる領域を拡大し、Trustを向上する



- 【検証可能なデータ】検証可能なデータを作成する
- 【検証可能なデータ】署名の意図が署名者と検証者の間で共有される仕掛けを活用する
- 【アイデンティティ】アイデンティティによる署名を行う
- 【メッセージ】ヘッダとペイロードと署名からなるメッセージを作成する
- 【ノード】検証可能なデータをメッセージとして送信する
- 【ノード】検証可能なデータをメッセージとして受信する
- 【アイデンティティ】アイデンティティグラフのパスを発見する
- 【アイデンティティ】アイデンティティグラフのパスから検証可能性を評価する
- 【アイデンティティ】アイデンティティを発見する
- 【アイデンティティ】署名自身の検証のためのデータの取得
- 【アイデンティティ】署名者の検証のためのデータの取得
- 【検証可能なデータ・メッセージ】メッセージの検証をする

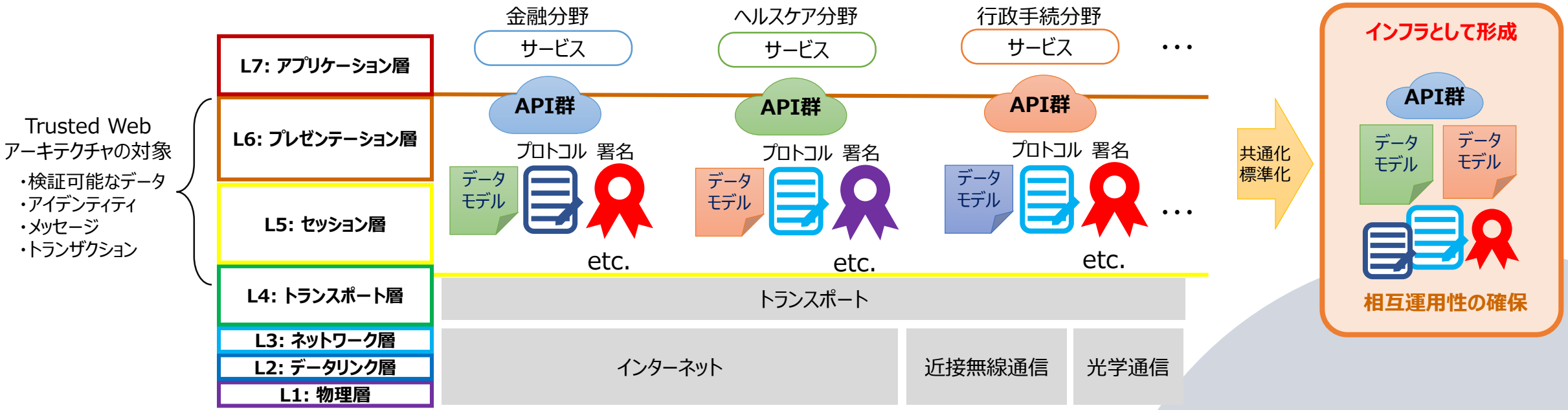
6. オーバーレイの考え方と実現に向けた道筋

セッション層以上に関する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

※トランスポート層も通信効率を上げるために検討する可能性がある

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
→ トランスポートと個々のサービスのレイヤとの間に**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
→ **インフラとしてのTrusted Webが形成**。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



ver2.0の公表とともに民間事業者から様々な分野における**ユースケースを募集開始**
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、
アーキテクチャなどに対する課題や改善点等のフィードバックを得る

7. ガバナンス

課題意識：新たにインフラとして付加されるTrustの仕組みの部分におけるガバナンスのあり方がどうあるべきか

＜基本的な考え方＞

○共有財（コモンズ）としてのガバナンスのあり方の追求

・デジタル・ビジネスにおけるネットワーク効果や収益逓増・費用逓減等の要因によって、独占・寡占に至りやすく、ロックイン効果が働きやすい。

→ 新たなTrustの仕組みをデジタル・インフラに構築していく上では、現在見られるペインポイントの再来を回避するため、一部の企業活動に過度に依存することとならないよう、共有財（コモンズ）としてのインフラとしてのガバナンスのあり方の検討が不可欠。

- ✓ このため、グローバルかつ技術中立指向のインターネットガバナンスを準用することが必要。
- ✓ 標準化、実装、運用、コミュニティ形成等において、様々なステークホルダーが関与していくことが重要。

○利用する際のガバナンスの重要性

・Trusted Webは技術基盤（インフラ）としてグローバルかつ技術中立的に機能が提供されることを目指す。

一方で、Trusted Webの上で利用されるアプリケーションは、各国の既存の法制度や商慣習が構成するTrustに根差した仕組みとも必要に応じて協調

＜ガバナンスを構成する理念＞

a.マルチステークホルダー指向

Trustを裏付けする様々な経路やその連鎖について、様々なステークホルダーが分散協業してそれを支え、系全体としてトラストを形成。
様々なステークホルダーが、合意形成を行うことにより、系全体が機能しているかについて、持続的なガバナンスを行う。

b.政府の役割の再定義　トラストアンカーとしての役割、デジタル上の社会活動を裏付ける法制度の整備　など

c.透明性、トレース、監査できること

合意形成の過程・結果・事後が記録されて検証可能性を持ち、様々なステークホルダーが検証・牽制することによって、悪意あるプレイヤーによる系全体のトラストの棄損を防ぐことを目指す

d.エコシステムを持続的なものとするためのインセンティブ設計

共有財の構築・運用に携わる役割を担う者に対する何らかのインセンティブ付けの検討が必要

8. 今後の当面の活動（2022年度）

ユースケース創出

・「Trusted Web共同開発支援事業」を通じて、様々な分野における10件程度のユースケースを公募
・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
・開発中や開発されたユースケースをベースにエンジニア間のアイディア創発を活性化

コミュニティ形成

・ウェブサイトの立ち上げ・運営、GitHubの更なる活用によるコミュニティの形成・活性化
・GitHubを活用して、昨年度開発されたプロトタイプの独自改変・独自実装を促すとともに、フィードバックを得てアップデート
・GitHubを活用して、issues などを用いて技術的な検討を常時更新（上記の各ユースケースに関与するエンジニア等関係者の積極的な関与も想定）

海外との連携

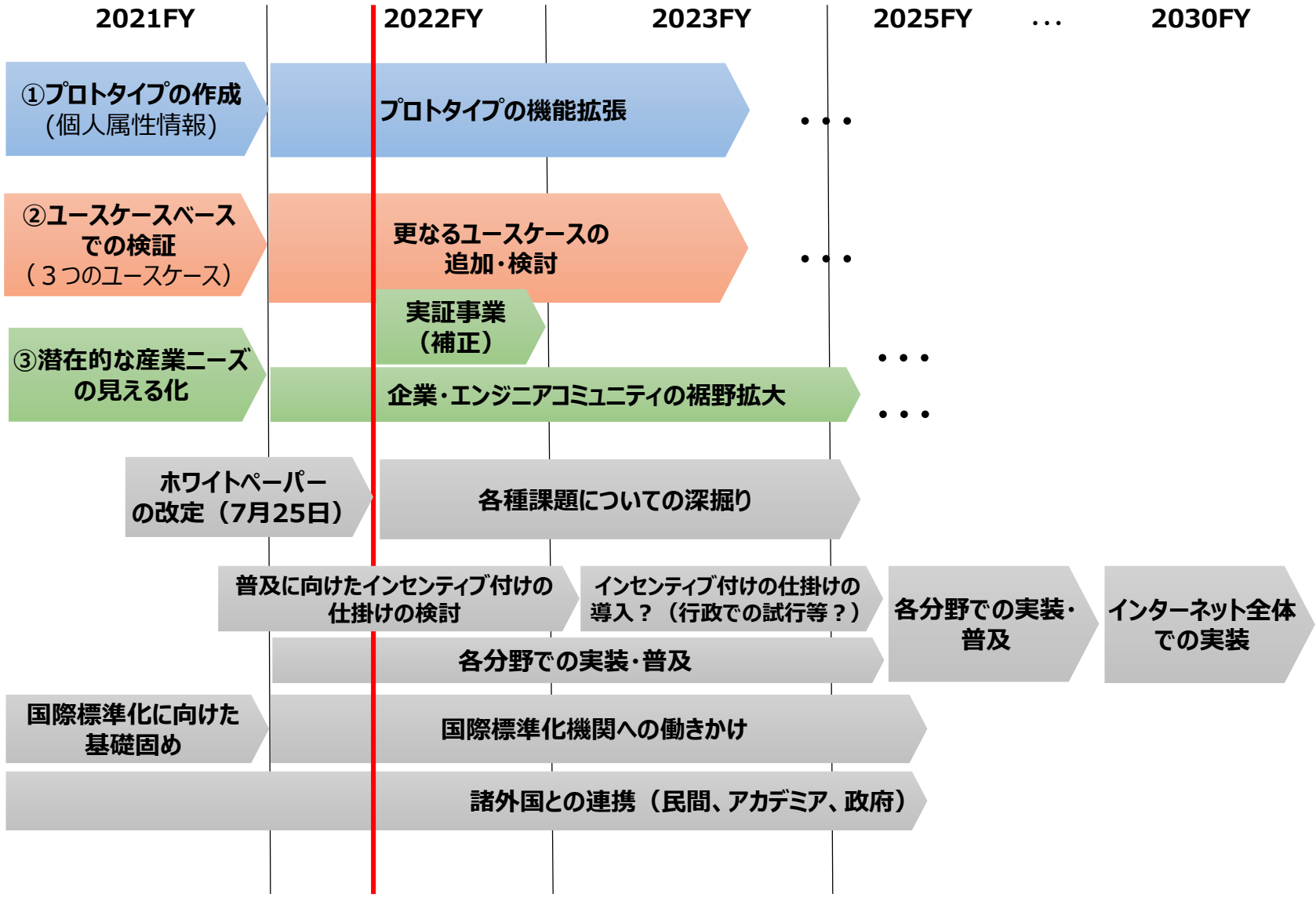
・ユースケースの検討状況も踏まえ、国際標準化の方向性（どの機関に何を働きかけるべきか等）を議論、国際標準化機関や国際標準化につながる活動を行う機関への必要な働きかけ
・EU等の海外の政府機関や類似の取組みをしている団体との情報交換、更なるネットワーク構築

全体

・今年度の取組状況（上記ユースケースの紹介を含む）について、昨年度同様、イベント等を開催して情報発信
・「ホワイトペーパー3.0」の策定

今般、提示されたTrusted Webが目指す信頼の姿やアーキテクチャは、あくまで現時点での提案であり、**今後内外の関係者から広くフィードバックを得、議論**を重ねながら、Trusted Webの具現化に向けた取組みを進めていく。

8. 2030年に向けた中期的な戦略（イメージ）



＜2021年度達成目標の結果＞

- シンプルながらも動くものを作る
→ プロトタイプを実装

- 機能・ガバナンス等の深堀り
→ ホワイトペーパーの改定

- 国際標準化に向けた基礎固め
→ Trusted Webの国際標準化に向けた調査を実施

Trusted Web推進協議会　名簿

（令和４年７月25日現在）

内山　幸樹	株式会社ホットリンク　代表取締役グループCEO
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　取締役執行役員 CIO
太田　祐一	株式会社DataSign 代表取締役
黒坂　達也	株式会社 企 代表取締役
﨑村　夏彦	東京デジタルアイディアーズ株式会社 エグゼクティブ・パートナー主席研究員
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、データ&セキュリティ研究所長
冨本　祐輔	トヨタファイナンシャルサービス株式会社 イノベーション本部　副本部長
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	世界経済フォーラム第四次産業革命日本センター ヘルスケア・データ政策プロジェクト長
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	Research Professor, Computer Science Department at Georgetown University / Head of blockchain research, NTT Research Inc.
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）

Trusted Web推進協議会　タスクフォース　名簿

（令和４年７月25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 シニアリサーチャー・インフラ戦略担当VP
岩田　太地	日本電気株式会社　エンタープライズビジネスユニット　主席ビジネスプロデューサー
内山　幸樹	株式会社ホットリンク 代表取締役グループCEO
菊池　将和	Secured Finance AG 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
富士榮　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	Research Professor, Computer Science Department at Georgetown University / Head of blockchain research, NTT Research Inc.
渡辺　創太	Stake Technologies株式会社CEO

（○：座長）