Trusted Web ホワイトペーパー

ver.3.0（案）

実装編

2023 年 11 月 15 日

Trusted Web 推進協議会

1. 用語定義

項番	用語	解説
1	アイデンティティ (Identity)	エンティティに関連する属性のセット 出典：ISO/IEC 24760-1
2	アイデンティティ管理 (Identity Management)	組織の権限とアイデンティティに関連するその目的を実現するために使用される一連の原則、実践、プロセス、および手順。 出典：Pan-Canadian Trust Framework
3	エンティティ (Entity)	個人や組織のように、明確で独立した存在を持ち、文脈の中で立法、政策、規制を受けることができ、一定の権利、社会的及び法的責務を持つことができるもの。エンティティは、デジタルエコシステムで 4 つの役割(すなわち、Subject、Issuer、Holder、Verifier である。)の１つ以上を実行できる。 出典：Pan-Canadian Trust Framework
4	合意 (Agreement)	ユーザーが自分のデジタル・アイデンティティや属性がどのように共有されるかを理解していることを確認するもの。 出典：UK digital identity and attributes trust framework beta version (0.3)
5	真正性 (Authenticity)	データが意図された情報源から得られたものであるというプロパティ。 出典：NIST Special Publication 800-63
6	相互運用性 (Interoperability)	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。
7	属性情報 (Attribute)	名前、生年月日、パスポート番号、資格、予防接種など、誰かまたは何かに固有または起因する品質または特徴 出典：The Open Identity Exchange "A Guide to Trust Frameworks for Smart Digital ID"
8	DID (Decentralized Identifiers)	DID とは、Decentralized Identifiers （分散型識別子）の略で、新しいタイプのグローバルに一意な識別子である。個人や組織が、自らが信頼できるシステムを使って自分の識別子を生成できるように設計されている。この新しい識別子は、デジタル署名などの暗号証明を用いて認証することにより、エンティティがその識別子を管理していることを証明することが可能。 これらの識別子の使用は、さまざまな状況に応じて適切に設定が可能であり、識別子の継続的な存在を保証する中央機関に依存することなく、個人情報やプライベートデータをどの程度公開するかを制御しながら、エンティティが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。

		出典：W3C Decentralized Identifiers (DIDs) v1.0 https://www.w3.org/TR/did-core/
9	デジタル署名 (Digital Signature)	公開鍵暗号技術を用いて、デジタル文書が公開鍵で特定されるエンティティが認めたものであることを確認できるデータ列
10	トラストアンカー （Trust Anchor）	公開鍵暗号の公開鍵[1]
11	トラストフレームワーク (Trust Framework)	運用規則、スキーム規則、運用方針などの仕様、規則、協定の集合。エコシステム内においてトラストフレームワークに準拠していることを示すことができる認証プロセスや、準拠状態を維持・監査するための、ガバナンスや監査機関を含むこともある。 出典：Open Identity Exchange “A Guide to Trust Frameworks for Smart Digital ID”。
12	信頼 (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
13	VC (Verifiable Credentials)	クレデンシャルとは、発行者による一つまたは複数の「発行者によって主張された属性の集合」の集合である。検証可能クレデンシャルとは、改ざん検出が容易なクレデンシャルであり、誰が発行したかを暗号学的に検証できるものである。 出典：W3C Verifiable Credentials Data Model 1.0 https://www.w3.org/TR/vc-data-model/

[1] トラストアンカーの定義は文書によって揺れがある。NIST の Glossary（ https://csrc.nist.gov/glossary/term/trust_anchor ）にもあるように NIST の文書間でも定まっていない。例えば、NIST SP800-63-3 による定義では “A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate). A trust anchor may have name or policy constraints limiting its scope.”となっており、公開鍵あるいは共通鍵を直接さしている。一方、NIST SP800-57 Part 1 Rev.5 の定義では “An authoritative entity for which trust is assumed. In a PKI, a trust anchor is a certification authority, which is represented by a certificate that is used to verify the signature on a certificate issued by that trust-anchor.” となっている。これらの事情から、本文書では、より狭い定義である「公開鍵暗号の公開鍵」とした。

2. Trusted Web が目指すべき方向性

(1).目指すべき方向性

1. Trusted Web は、「デジタル社会」における様々な社会活動に対応できる Trust の仕組みを作り、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していくこととする。

2. Trusted Web が実現を目指す Trust の仕組みは、特定のサービスに過度に依存せず、
   - ○ 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。

3. この際、既存のインターネットやウェブに、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 Trust に関する機能を、上から重ね合わせるオーバーレイのアプローチで追加していくこととする。

4. Trusted Web の実現に向けては、例えば、以下のような道筋が仮説として考えられる。
   - ○ 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していく。
   - ○ この過程において、既存の Trust を向上させる仕組みも活用しながら、例えば、用途に応じた多種多様な特性に対応できる（API を含む）ミドルウェアが提供されることが考えられる。
   - ○ そして、個々のサービスに特化した API 群からなるミドルウェアにおいては、その発展の過程において、トランザクションを行う上で共通化すべき API やデータモデル等が特定されていき、そして、それらが共通化されることにより相互運用性が確保され、標準化につながり、インフラとしての信頼の枠組みが形成されていくこととなる。
   - ○ この際、実際にユーザーが利用するのは、インフラの上で展開される様々なサービスである。このインフラとしての信頼の枠組みは、その上で動くサービスから共通化すべき部分等へ、得られた知見を逐次取り入れることにより、社会的受容性を高めつつ、社会実装が進められる形でアップデートがなされていくこととなる。

(2).必要となる原則

5. Trusted Web の設計・運用などに当たって考慮されるべき原則は、ホワイトペーパーver.1.0 において、以下のとおり整理している。

【支える仕組み】

① 持続可能なエコシステム

6. 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。

② マルチステークホルダーによるガバナンス

7. 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。

③ オープンネスと透明性

8. 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。

【機能をシステムとして実装する際に必要なこと】

〈ユーザーの観点〉

④　データ主体によるコントロール

9. 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。

⑤　ユニバーサル性

10. 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。

⑥　ユーザー視点

11. 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。

〈システムの観点〉

⑦　継続性

12. 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。

⑧　柔軟性

13. 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。

⑨　相互運用性

14. 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。

⑩　更改容易性・拡張性

15. 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ーラブルであること。

3. Trusted Web のアーキテクチャデザイン

(1).概要

16. Trusted Web では、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する。アーキテクチャにおいては、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。アーキテクチャでは、Verifiable Identity や、Verifiable Data（検証可能なデータ）、Verifiable Messaging（検証可能なメッセージ交換）、および 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）を活用することにより、Verifiable（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。

(2).Trusted Web アーキテクチャ概観

17. Trusted Web での根源的な価値は「検証できる領域の拡大による Trust の向上」である。デジタルにおける Trust を別の言葉で表現するなら「何者かによって検証済みと認められたデータを、検証した者を信じることによって、検証の詳細にまで立ち戻った確認を省略できること」と表現できる。
18. Trusted Web における検証の対象は、「何者かによって生み出されたデータ」と、「生み出されたデータのやり取りの過程」と整理できる。このため、それぞれの検証可能性を何らかの形で担保する必要がある。前者の検証については、デジタル署名技術により実現する。後者の検証については、やりとりをモデル化しデジタル署名技術と組み合わせることで実現する。
19. この際、エンティティが提示する「検証可能なデータ（Verifiable Data）」と、検証可能なデータを含む様々なエンティティ（主体）間のメッセージのやり取りを検証可能な形で実現する「検証可能なメッセージ交換（Verifiable Messaging）」を実現するために、「検証可能なデジタル・アイデンティティ（Verifiable Identity）」を活用する。これらは、様々な既存のテクノロジーを組み合わせることで実現できるものである。下記の図 3-1 で関係を図示する。また、構成要素の詳細については後述する。

【ver.2.0 からの変更点】

20. ver.2.0 では、アイデンティティグラフは、アイデンティティ間の関係であり、アイデンティティの視点での可視性を反映するグラフ構造を持つと定義していた。一方で、実証事業から、システム設計上の目的が不明瞭であると指摘があり、新たにコミュニティという考え方を議論した。議論の中で、ピア・ツー・ピア、もしくはコミュニティを丸ごと信用する、もしくはコミュニティの中のメンバをお互いに信用するというモデルを援用することによって段階的に、通信先や署名元の相手を確認できる形で整理を行った。
21. ver.2.0 では、「Trusted Web は基本的にセッション層である OSI 参照モデルにおける 5 層以上に関するアーキテクチャであり、トランスポート層（4 層）も通信効率を上げるために検討する可能性がある」と記載されており、実証事業の設計や実装を担当するエンジニアからトランスポート層を検討するかの懸念が示された。そこで、ver.3.0 では、トランスポートについては規定せず、活用可能な通信手段を貪欲に活用する点を明記した。

【Trusted Web アーキテクチャ概観と構成要素】

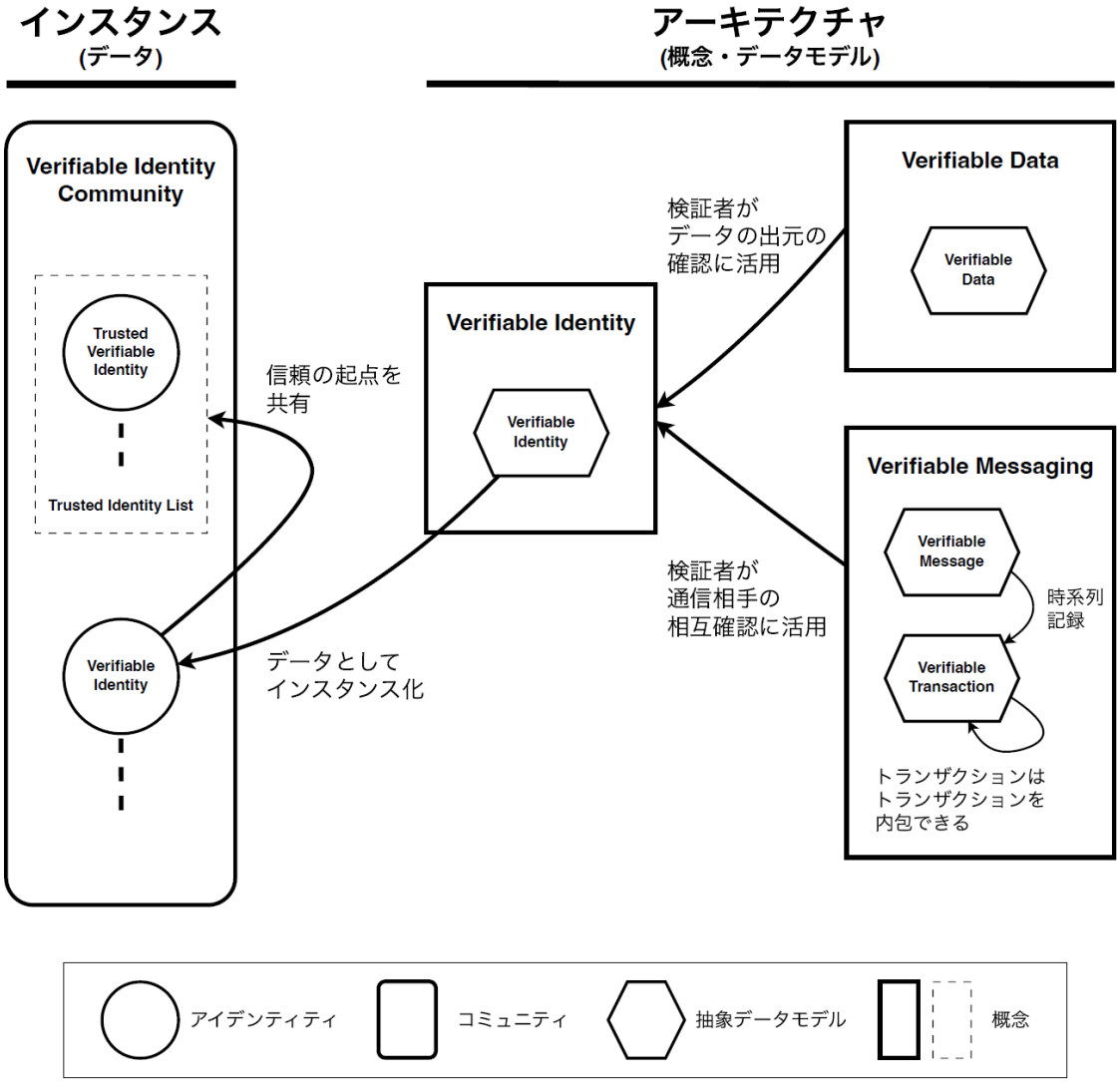

図 3-1 Trusted Web アーキテクチャ概観

① Verifiable Data（検証可能なデータ）

22. デジタル署名技術を活用することにより、「対象となるデータが署名者によって確認されていること」を検証者が確認できるデータ。

② Verifiable Messaging（検証可能なメッセージ交換）

23. 複数のエンティティ間での確実な配送をメッセージの送受信の順序性を含め確認することができるもの。単一のメッセージを表現する Verifiable Message（検証可能なメッセージ）と、複数の Verifiable Message を送受信順も含め検証できる Verifiable Transaction （検証可能なトランザクション）で表現される。なお、Verifiable Transaction には、Verifiable Message あるいは Verifiable Transaction を、複数かつ混在的かつ再帰的に内包できる。

③ Verifiable Identity（検証可能なアイデンティティ）

24. メッセージそのものや発信者、メッセージのやりとりを検証可能とする（Verifiable Data と Verifiable Messaging を実現する）には、少なくともデータの出元、メッセージの発信者や宛先

の情報が必要であるとともに、対象となるコンテクスト（状況）に応じて適切な検証がなされている必要がある。
　このように、Verifiable Identity は、検証可能かつコンテクストに応じて最低限必要な属性からなるデジタル・アイデンティティである。Verifiable Identity によって、対象となるデータが署名者によって確認されていることを検証者が確認でき（Verifiable Data の実現）、データのやり取りが検証できる（Verifiable Messaging の実現） 。

25.　なお、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、コンテクスト（状況）に応じた属性の使い分けのために、複数のアイデンティティを使い分ける場合もある。

④ 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）

26.　Trusted Web では、必要に応じて、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を構築する。
27.　データのやり取りに関係するエコシステム参加者の下で Trusted Identity を共有することにより、信頼関係の構築を容易にする。
28.　このような信頼の起点を含む情報を一定のガバナンス下で共有し、Verifiable Identity の確立を支援するアイデンティティの集合を Verifiable Identity コミュニティと呼ぶ。

【アーキテクチャの構成要素と Trusted Web の目指すべき方向性との関係】
29.　以上の４つの構成要素と Trusted Web の目指すべき方向性との関係を以下に示す。

Trusted Web が実現を目指す Trust の仕組みは、特定のサービスに過度に依存せず、

○ 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、
Verifiable Identity によってユーザ自身が自らに関連するデータの受け渡し先を検証でき、Verifiable Data と組み合わせることで選択的情報開示等をサポートする。一方で、 事前合意や開示範囲の妥当性はテクノロジーのサポートを受けつつ、ガバナンスと分担する

○ その合意の履行のトレースを可能としつつ、
Verifiable Messaging によってトレースを可能とする

○ 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。
Verifiable Data、Verifiable Identity、Verifiable Identity コミュニティの組み合わせによって検証可能性を拡大する

30.　なお、Trusted Web アーキテクチャでは、実際の情報のやり取りを行うトランスポートについては規定せず、活用可能な通信手段を貪欲に活用していく。その上で、情報をやり取りするコンテクストや、Trusted Web の原則に適合する範囲において、Verifiable Data、Verifiable Messaging、Verifiable Identity についての検証は、通信プロトコルの支援によって達成され得る。
31.　例えば、Trusted Web は、エンティティからデータをアンバンドルすることを指向するものである。一方で、主体間の関係性において、検証可能性が十分担保されており、エンティティがデータを保持することに対して、「2.(2)必要となる原則」に見合った妥当性がある場合は、エンティティとデータがアンバンドルされていないことを許容する。

(3).Verifiable Data（検証可能なデータ）

① Verifiable Data 概要

32. Verifiable Data は、デジタル署名技術を活用することにより、対象となるデータが署名者によって確認されていることを示す。これを実現するためには、署名者が Verifiable Identity として検証可能であること、また、デジタル署名を検証する際に、必要な鍵関連情報 [2]を取得可能であることの双方が必要である。

② Verifiable Data の抽象データモデル

33. Verifiable Data の抽象データモデルは、「対象となるデータ」や「署名及び発信元を示す Verifiable Identity そのもの」、あるいは、「Verifiable Identity を参照するための情報」の 3 つで構成される。
34. なお、Verifiable Data が暗号化されていることは必要要件ではないが、必要に応じて暗号化してもよいものとする。

③ Verifiable Data の操作

35. Verifiable Data を生成するためには、
    - ○ 署名に用いる Verifiable Identity を必要に応じて検証した後に、
    - ○ 鍵関連情報を取り出し、
    - ○ 対象となるデータと署名に用いる Verifiable Identity そのもの、あるいは Verifiable Identity への参照とともに、鍵関連情報を用いて署名し、
    - ○ 署名対象と署名結果を合わせること

    が必要である。
36. Verifiable Data を検証するためには、発信元の Verifiable Identity を参照し検証した上で、鍵関連情報を取り出す。その後、署名対象となるデータと署名に対して鍵関連情報を適用することで、署名を検証できる。

④ Verifiable Data として解釈できる実装の例

37. デジタル署名は様々な状況で活用されている。署名が検証でき、かつ、検証者が十分に署名者の検証ができているのであれば、Verifiable Data である。一方、何が検証できているのかについては、Verifiable Identity の検証と、Verifiable Data の署名における署名の意図（intention）が明確化されているか否かに依存する。
38. 署名の意図（intention）の明確化とは、予め合意されたデータのやりとりの枠組み（例：ある目的を達成するためにステークホルダー間で合意された業務プロセス）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を指す [3]。
39. X.509 PKI における各種証明書は Verifiable Data である。署名のコンテクストはそれぞれの署名書発行におけるポリシーに従っているとみなすことができる。
40. デジタル庁の発行したワクチン証明書の SMART Health Cards 形式の Verifiable Credentials によるデジタル化されたワクチン証明書などは、Verifiable Data である。
41. 署名された PDF ファイルは、署名者の検証可能性に依存するが、Verifiable Data である。

(4).Verifiable Messaging

[2] 検証に適用可能な暗号を用いた手法全般を指す
[3] 署名者による署名の意図は、社会一般ですべて共通化・一般化されるものでは必ずしもなく、データのやりとりの枠組み（及びそれによって達成が期待される目的）によって個別に異なる場合がある。また実際には、対象となるデータのやりとりの枠組みを採用している時点で、ステークホルダーは署名の意図に事前に合意しているので、データのやりとりが発生する際に意図そのものが都度問われることはなくなる。

① Verifiable Messaging 概要

42. Verifiable Messaging は、複数のエンティティ間でのメッセージのやりとりにおいて、発信者と受信者のアイデンティティとメッセージ本文によって「Verifiable Message（検証可能なメッセージ）」を構成し、この検証可能なメッセージの“やりとりの並び”をトランザクションとしてメッセージ送受の順序関係とともに「Verifiable Transaction（検証可能なトランザクション）」として記録する。これにより個々のメッセージを含めたメッセージのやりとり全体を検証可能とする。

② Verifiable Message 抽象データモデル

43. Verifiable Message は抽象データモデルとして表現される。Verifiable Message は、「発信者（単一）と受信者（単一または複数）それぞれにおける Verifiable Identity、または Verifiable Identity を参照するための情報」や「メッセージ自身」、「発信者による署名」で構成される。すなわち、受信者（単一または複数）が追加された Verifiable Data の一形態（サブクラス）であり、Verifiable Data と同様に検証できる。
44. なお、Verifiable Message に関しては、メッセージが暗号化されていることは必要要件ではないが、必要に応じて暗号化してもよいものとする。

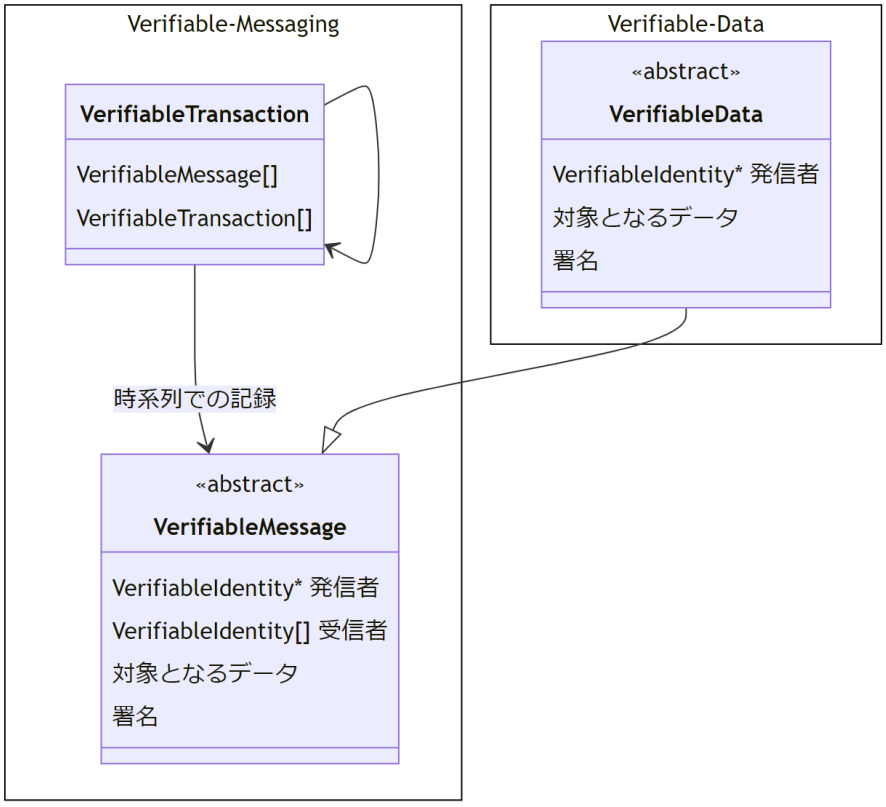

図 3-2 Verifiable Message 抽象データモデル

③ Verifiable Transaction 抽象データモデル

45. Verifiable Transaction（検証可能なトランザクション）は、Verifiable Message あるいは Verifiable Transaction について、発信の順序が検証出来る形で記録されたものである。
46. なお、Verifiable Message、または Verifiable Transaction を含む仮想的な Transaction Record を想定した場合、発信の順序が検証可能な形で Transaction Record を並べることができ、発信の順序の検証が可能であることが最低条件である。

47. 発信の順序の検証可能性を担保する方式については特に規定しない。想定される実現手段としては、Transaction Record のブロックチェーンへの記録や、Transaction Record をハッシュリンク（あるいはハッシュチェーン）でつなぐ方法、Transaction Record それぞれにタイムスタンプを打って記録していくなど、手法は複数想定される。
48. また、発信者と受信者の秘匿については必要要件ではなく、必要に応じて導入していくものと考える。その場合、高度な手法としては、個々のメンバによるそれぞれのトランザクションレコードについてアクセスコントロール等の可視性の制御可能な方式の適用も考えられる。また、Verifiable Transaction をチャットメッセージの記録と捉える方法もある。この場合、グループへの新規参加者がある場合について、過去の記録に対する可視性制御といった技術的あるいはプロトコルデザイン上の高度な話題もある。Verifiable Transaction は、入れ子構造も取れるようにデザインしているため、一定の設計は可能と考えられるが、本ホワイトペーパーでは、アウトオブスコープとする。

④ Verifiable Messaging の操作

49. Verifiable Message は、
○ 送信者や受信者の Verifiable Identity を準備し、
○ ペイロードにあたるメッセージとともにVerifiable Messageに含まれる情報を用意した後、送信者の Verifiable Identity を用いて生成する。
50. なお、Verifiable Message の検証は、Verifiable Data と同等の検証を行った後、受信者それぞれの Verifiable Identity を検証することである。
51. Verifiable Transaction は、Verifiable Message を順に記録していくことで生成される。このとき、Verifiable Message におけるメッセージへの関与者（メッセージ送信者または受信者のどちらかに含まれる者の一覧）に変化があった場合等においては、必要に応じて、Verifiable Transaction を入れ子構造に作成し記録を続けることとなる。
52. なお、Verifiable Transaction の検証は、Verifiable Transaction に含まれる Verifiable Message または Verifiable Transaction の発生順を検証できること、そして、含まれるすべての Verifiable Message に対する検証が必要となる。

⑤ Verifiable Messaging として解釈できる実装例
53. Verifiable Messaging を忠実に実装している例は現時点ではないと認識している。一方で、Verifiable Message および Verifiable Transaction に近い実装をしている例は存在する。
54. PGP（Pretty Good Privacy）によるメールは、Verifiable Message の一形態である。相手先及び発信元の Verifiable Identity に相当する PGP の Web of Trust で検証できている範囲において、発信者と受信者を指示した形で単一方向のメッセージ送信が可能である。
55. S/MIME[5] によるメールの場合は、X.509 PKI のエンドエンティティ証明書をそれぞれのユーザーが用い、発信者と受信者の検証ができているという前提において、Verifiable Message である。
56. 一般的なグループチャットシステムの場合、個々のチャットの参加者がすべての参加者に向けたメッセージを受け取った上で、それぞれのアカウントに紐付いた形でメッセージを保存していると解釈できる。チャットシステムにおける送信元や送信先の検証が十分であると捉え、サービス側でのメッセージ削除があるというリスクを想定する前提で、Verifiable Messaging の一形態とすることが可能である。

(5).Verifiable Identity（検証可能なアイデンティティ）

57. ここまで示してきたように、Verifiable Data と Verifiable Messaging を実現するためには、Verifiable Identity が必要である。本節では、Verifiable Identity の概念と、抽象データモデ

5 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification
https://datatracker.ietf.org/doc/html/rfc8551

ルに加えて、Verifiable Identity の発見と検証について議論するとともに、実際のアプリケーションで構築する指針を示す。

① アイデンティティとエンティティ

58. アイデンティティは、あるエンティティが他のエンティティとやりとりする際に相手に見せる一つの面、俗に表現するならば《顔》である。
59. つまり、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る場合もあれば、コンテクストに応じて属性を使い分けるために、複数のアイデンティティを用いる場合もある。
60. Trusted Web に限らず、一般的な例を用いて説明するならば、自然人であれば、ソーシャルネットワークごとに異なるアイデンティティを使い分ける場合がある。法人においても、やりとりする相手によってアイデンティティを使い分けることがある。
61. 例えば、対外的なアイデンティティと社内、あるいは社内と協業している企業とのやりとりでは、異なるアイデンティティを使い分ける場合がある。さらに、プライバシーを確保するための技術的な手法として、アイデンティティをやりとりする相手ごとに使い分ける、といったことも行われている。

② Verifiable Identity

62. アイデンティティにおけるそれぞれの属性は、単にその属性が提示されただけでは真偽は不明である。例えば、ある人が自身の年齢を主張したとき、その年齢が実際の年齢かどうかはわからない。
63. Verifiable Identity（検証可能なアイデンティティ）とは、検証可能かつコンテクストに応じて最低限必要な属性からなるデジタル・アイデンティティである。 Verifiable Identity によって、対象となるデータが署名者によって確認されていることを検証者が確認でき（Verifiable Data の実現）、データのやり取りが検証できる（Verifiable Messaging の実現）。Verifiable Identity の発見と検証は後述する。

③ Verifiable Identity 抽象データモデル

64. Verifiable Identity の抽象データモデルは、以下で構成される。
    - ○ Verifiable Data や Verifiable Messaging の検証に用いられる Verifiable Identity に紐付いた鍵関連情報、
    - ○ Verifiable Identity コミュニティ中での識別（identification）に用いられる identifier（識別子）、
    - ○ Verifiable Identity 自身を検証するための必要となる自身への署名などといったデータ

65. また、詳細は後述するが、Verifiable Identity が検証者（Verifier）として振る舞う場合は、
    - ○ 相手先の Verifiable Identity を検証するために、期待される相手先の Verifiable Identity そのものを保持する《Verifiable Identity リスト》と、
    - ○ 期待される相手先の Verifiable Identity が属する可能性がある Verifiable Identity コミュニティからなる《Verifiable Identity コミュニティリスト》の

    二つのリストを持ち得る。リストを持つことで、検証者が Verifiable Identity からのアクセスを第三者視点で検証可能となる。

④ Verifiable Identity に対する操作

66. Verifiable Identity の生成は、抽象データモデルで示された情報を持つだけでなく、実装に応じて、固有の情報を追加で持つことが想定される。

67. Verifiable Identity は、Verifiable Data に紐付けられている。Verifiable Data が検証される際は、Verifiable Identity が発見され、鍵関連情報が取り出されて用いられる。
68. Verifiable Identity を成立させるためには、アイデンティティにおけるそれぞれの属性を検証可能にする必要がある。このためには、信頼できる第三者に依存しつつ信頼関係を拡張する信頼の連鎖を活用する必要がある。
69. 以下の節で信頼の連鎖について議論する。

(a).信頼の連鎖を構成する X.509 PKI と Web of Trust

70. あるデジタル署名の正当性を確認するためには、署名者についての情報が必要である。その署名者の情報は署名者本人から信頼できる形で直接的に入手できれば、そのまま信用できる。一方、署名者本人から信頼できる形で直接的に入手できない場合は、信頼できる第三者に頼ることによって、間接的に入手することが可能である。このとき、信頼関係が連鎖的に確保できる場合、連鎖上の信頼の程度の判断は必要となるが、対象となる署名者についての情報を信頼できると考えられる。このような信頼における連鎖的な関係を「信頼の連鎖」と呼ぶ。
71. この連鎖を確立するためには、鎖を構成する部品である鎖の輪（link of chain）を入手し、繋いでいく必要がある。この連鎖として、主に根元から枝分かれするようなツリー構造を用いるのが X.509 PKI であり、蜘蛛の巣状の関係を用いるのが Web of Trust である。

(b).X.509 PKI

72. X.509 証明書を用いた PKI（以下 X.509 PKI）は、ツリー構造をなしており、根元と節の位置に配置される認証局（Certificate Authority – CA）群と、末端についた葉にあたるエンドエンティティによって構成される。CA 群とエンドエンティティに対して証明書が結びつけられる。木の根元に位置するルート CA からエンドエンティティに至る複数の証明書によって信頼の連鎖が構成されている。ルート CA を信頼することによって、ツリー上の X.509 証明書を信頼することができる。
73. X.509 証明書によって、使われている公開鍵と、証明書中に明記されている各種属性情報との関係を信頼できる形で入手できる。さらに、X.509 PKI に加えて運用規程を導入することによって、証明書がどのような対象に対して発行されているかを、付帯する属性情報と併せて示すことができる。
74. 例えば、マイナンバーカード付帯の証明書は、公的個人認証サービス（JPKI）によるものであり、利用者証明用認証局運用規程 [6]に従って利用者証明用認証局が運用されている。利用者証明用認証局による証明書は、「住所地市区町村に備えられている住民基本台帳に記録されている者に対して、その者の申請に応じて、利用者証明用電子証明書を発行し、利用者証明用 CA の運用に必要な電子証明書を発行」するので、利用者が本人であることの証明に用いることができる
75. 一方、アイデンティティにまつわる運用規程を取り入れていない X.509 PKI が提供する基本的な仕掛けだけでは、公開鍵とその属性情報の結びつきについての情報を得られる以上のことは担保されない。例えば、Web PKI において現在広く用いられている DV 証明書は、完全解決後のドメイン名（Fully Qualified Domain Name）と公開鍵の結びつきを表現したにすぎないので、メリットは限定的であるといえる。これに加え、OV 証明書や EV の場合は、それぞれ、属性情報が検証済みであることが保証されている。

(c).Web of Trust

76. エンティティが用いているそれぞれのアイデンティティ、そして、アイデンティティ同士の間の Trust に基づいた蜘蛛の巣状 – ウェブ – に張り巡らされた関係を活用する。このようなアイデンティティ間の Trust の関係を示した情報を Web of Trust と言う。

[6] 利用者証明用認証局運用規程 https://www.jpki.go.jp/ca/pdf/auth_cps.pdf

77. Web of Trust は、PGP で導入された概念であり、直接実際に会合した人の間でお互いを示す公開鍵（実際は公開鍵のハッシュであるフィンガープリント）と e-mail アドレスの結びつきを対面で確認した上で、PGP ソフトウェアを用いてお互いの鍵に署名する。このような対面の署名の会合[8]によって集めた公開鍵に対する署名群を公開・共有することで、PGP 参加者の間で網の目のような信頼関係を構築し、公開鍵と本人についての情報の紐付けを確認できるようにしたものである。これにより、PGP では、発信者による署名を確認できるとともに、複数の受取人を対象とした暗号化されたメッセージを作成することができる。

(d).信頼の起点（エンティティ）とトラストアンカー（Trust Anchor）

78. 高い確度で信頼できるエンティティを起点とした信頼の連鎖によって署名者についての情報を得られるのであれば、得られた署名者の情報は信頼のおけるものと見なすことができる。このような信頼の起点となりえるようなエンティティが用いる公開鍵暗号の公開鍵のことをトラストアンカーという。X.509 PKI では、検証者があらかじめ複数の CA（通常は root CA）の情報をトラストアンカーとして手元に持つ形で信頼の連鎖の起点として用いる 。

(e).Verifiable Identity コミュニティ

79. Trusted Web では、必要に応じて、信頼の起点を共有する [10]ことにより、信頼関係の構築と、Verifiable Data の共有や Verifiable Messaging の実現を容易にする。
80. このような信頼の起点を含む情報をガバナンスとともにメンバ間で共有し、Verifiable Identity の確立を支援するアイデンティティの集合を Verifiable Identity コミュニティと呼ぶ。[11]
81. Verifiable Data や Verifiable Messaging を実現するためには、何らかの方法で通信相手を信頼できる形で特定あるいは発見できる必要がある、すなわち、Verifiable Identity の発見が必要である。相手を発見したり、検証したりするために一番確実な方法は Web of Trust のように、それぞれのエンティティ間の直接的なやりとりの積み重ねによる信頼関係の構築が一つの手段である。ただし、直接的なやりとりには限界がある。
82. そこで、複数のアイデンティティからなる Verifiable Identity コミュニティを構成し、この Verifiable Identity コミュニティを信頼あるいは参照するモデルを検討する。
83. こうした Verifiable Identity コミュニティにおいて、個々の Verifiable Identity コミュニティのメンバであるそれぞれのアイデンティティは、Verifiable Identity コミュニティ内での識別子（identifier）に識別（identify）されるとともに、信頼の起点を共有するモデルを想定する。このモデルにおいて、それぞれのアイデンティティは、個別のアイデンティティを直接的に信頼することに加え、これらの Verifiable Identity コミュニティを信頼あるいは参照するという関係を確立する。
84. それぞれのアイデンティティは、様々な組織等の複数の Verifiable Identity コミュニティに属していると考えられる。Verifiable Identity コミュニティの例を挙げる。
85. 例えば、会社で働いている日本人であれば、日本という国籍をもち日本人であること、住んでいる国、都道府県、市区町村、所属する会社や部署、卒業した大学の卒業生として等、様々な Verifiable Identity コミュニティに顕名のアイデンティティをもって属していることが想定される。一方、匿名の SNS に対し、匿名のアイデンティティをもって参加することができ、アイデンティティを使い分けることもできる。この関係を図 3-3 に示す。

[8] キーサイニングパーティとも呼ばれる
[10] Trusted Web は、信頼の起点を共有しないデータのやり取りの構成も取り得る。
[11] コミュニティの議論については、クリストファー・アレグザンダーによる、建築・都市計画にまつわるパタン・ランゲージ(Alexander, Christopher. A pattern language: towns, buildings, construction. Oxford university press, 1977)との関係を指摘されている。

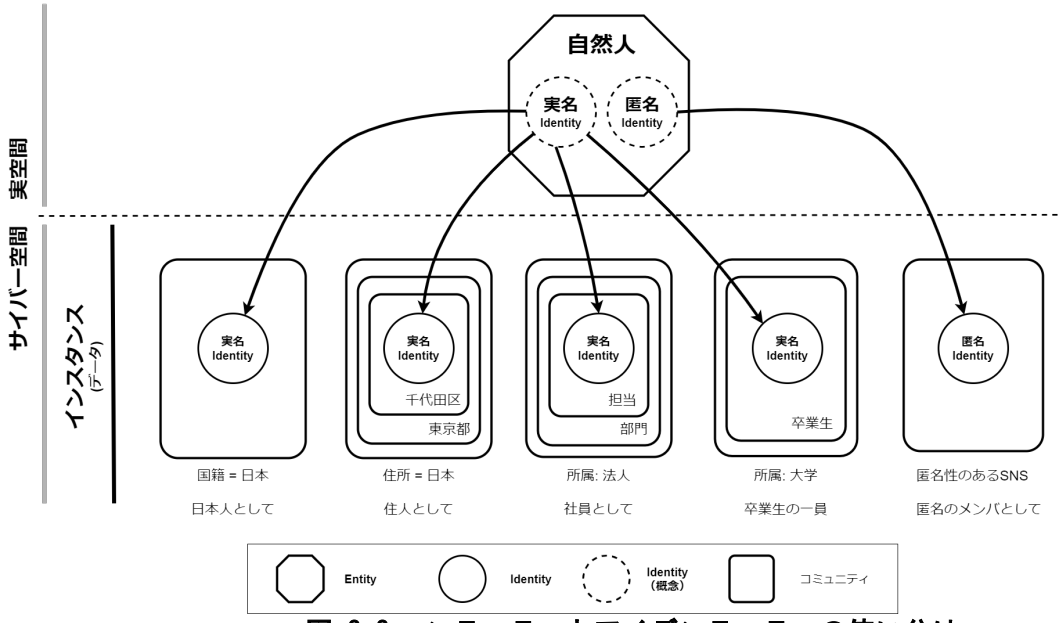

図 3-3 エンティティとアイデンティティの使い分け

86. 法人の場合は、法人の所在する市区町村や都道府県、サプライチェーンを構成する様々な企業連合（コンソーシアム）も Verifiable Identity コミュニティといえる。例えば、サプライチェーンに着目するなら（図 3-4 参照）、ある企業 X は、

○ サプライチェーン全体や、
○ 川上から川中企業までで構成されるサプライチェーン、
○ 川中から川下企業までで構成されるサプライチェーン、

それぞれの Verifiable Identity コミュニティに属するものとして捉えることができる。
この場合は、それぞれの構成メンバに応じて可視性をコントロールするような Verifiable Identity コミュニティとすることも可能と考えられる。

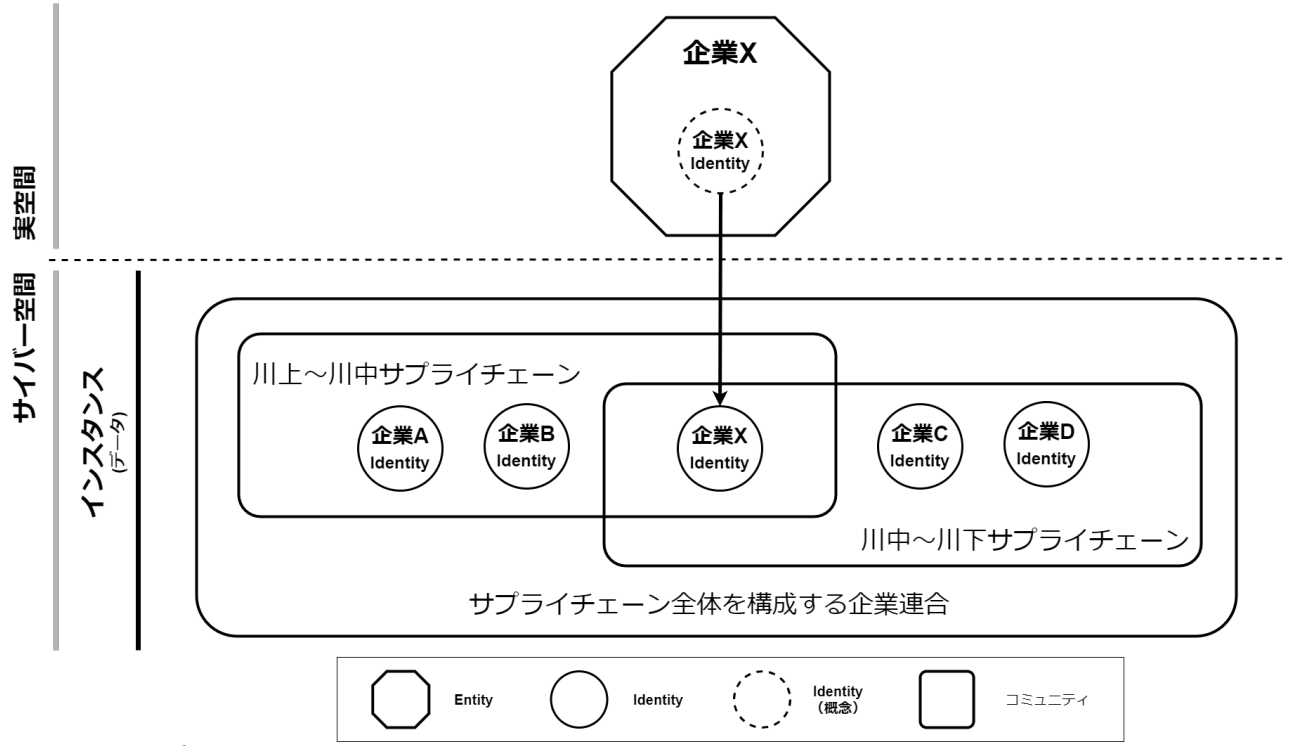

図 3-4 サプライチェーンにおける Verifiable Identity コミュニティと Verifiable Identity

87. 一方、成立するための要素が共有されている限りにおいては、Verifiable Identity コミュニティは任意に成立し得る。例えば、家庭も Verifiable Identity コミュニティの一形態と考えられる。また、任意の目的を共有するグループやタスクフォースなども Verifiable Identity コミュニティの一形態と考えられる。特定のアプリケーションプログラムを用いているユーザーも Verifiable Identity コミュニティを形成していると捉えることも可能である。

(f).Verifiable Identity コミュニティと Trust Framework

88. Verifiable Identity コミュニティは、いわゆる Trust Framework に置き換え、あるいは、Trust Framework を包含できるようにデザインしている。抽象的な意味での Trust Framework の定義や、比較対象となる実際の Trust Framework によっては、Trust Framework とそれを活用するエンティティ群を Verifiable Identity コミュニティ [12]と解釈することが可能である。

(g).Verifiable Identity コミュニティの構成

89. Verifiable Identity コミュニティは、複数のアイデンティティから構成されるグループと、そのグループで共有されるトラストマネージメント、そしてそれら全体に対してガバナンスが適用されたものと考えることができる。さらに、Verifiable Identity コミュニティの中に Verifiable Identity コミュニティを構成する再帰的な構造を取り得る。
90. 共有される情報は、Verifiable Identity コミュニティのポリシーや、アイデンティティ間を区別するために用いられる Verifiable Identity コミュニティ固有の名前空間、アイデンティティの一覧、信頼の起点、その他必要に応じてメタデータが用意される。Verifiable Identity コミュニティの全体像を図 3-5 に示す。

Verifiable Identity コミュニティは識別子の名前空間と信頼できるアイデンティティを共有する

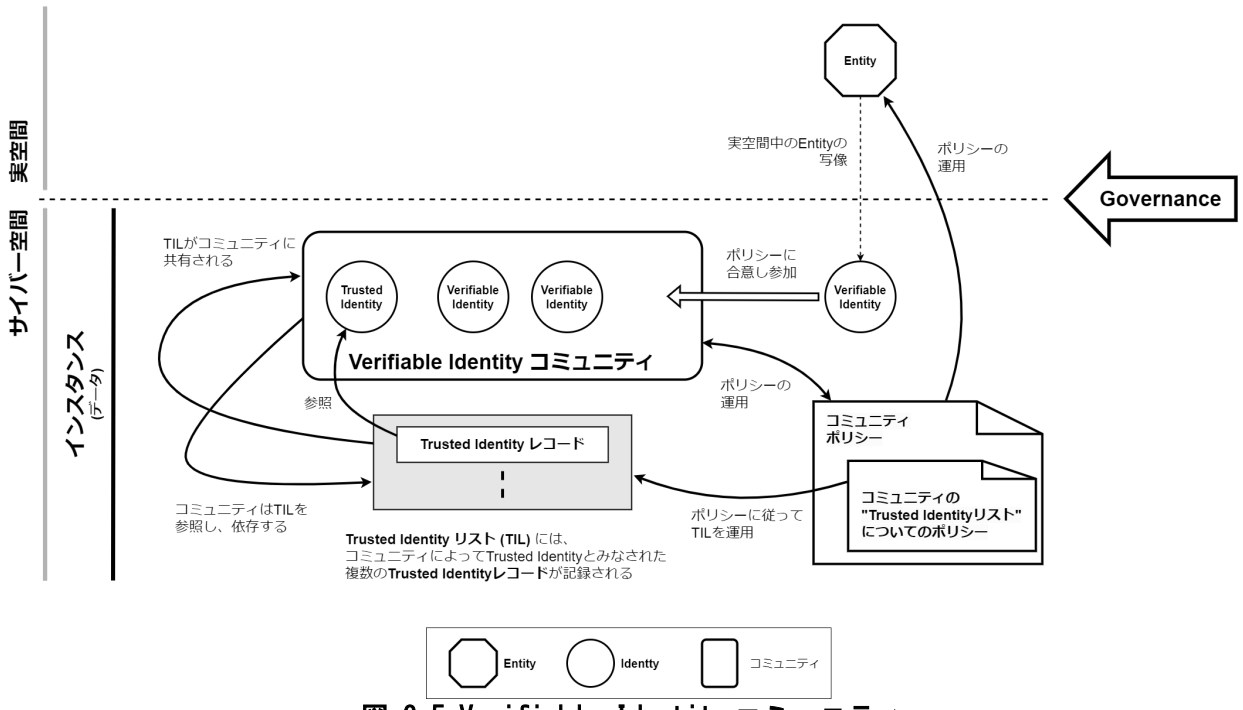

図 3-5 Verifiable Identity コミュニティ

[12] 後述する「Trusted Web のガバナンス」におけるトラストフレームワークを執行、認証（認定）、運用するガバナンス主体が対応する。

91. 以下、それぞれについて説明する。

(ア)Verifiable Identity コミュニティのポリシー

92. Verifiable Identity コミュニティが成立するためには、最低限のポリシーが必要である。以下にポリシーの例を挙げる:
- ○ Verifiable Identity コミュニティ参加のためのポリシー
- ○ 信頼の起点 -Trusted Identity --管理のためのポリシー（トラストマネージメント）
- ○ Verifiable Identity コミュニティ内で用いられるプロトコルの合意
- ○ Verifiable Identity コミュニティ内で用いられるデータモデルの合意

(イ)識別子と名前空間

93. Verifiable Identity コミュニティ内でのアイデンティティそれぞれを識別するためには、アイデンティティそれぞれに対して、Verifiable Identity コミュニティ内でユニークな識別子（identifier）が付与されている必要がある。識別子の割り当てについては、Verifiable Identity コミュニティのポリシーで規定される。

(ウ)アイデンティティー覧

94. Verifiable Identity コミュニティ内では、必要に応じて、Verifiable Identity コミュニティを構成するアイデンティティの一覧が管理される。識別子の割り当て方法によっては、技術的な理由でメンバー覧が必要になる。また、このアイデンティティー覧は、Verifiable Identity コミュニティ内あるいは Verifiable Identity コミュニティ外に対し、共有される場合も、されない場合もあるだろう。

(エ)信頼の起点

95. Verifiable Identity コミュニティ内では、共通の基盤として、信頼の起点を共有する。信頼の起点に対するマネージメント、すなわちトラストマネージメントは、Verifiable Identity コミュニティのポリシーで規定される。
96. 信頼の起点は、アイデンティティとも表現できる。または、コミュニティの信頼の起点の成り立ちによって、エンティティとアイデンティティの関係とも整理できる。このようなアイデンティティを Trusted Identity とし、その運用者を Trusted Entity と呼ぶ。
97. また、コミュニティによっては、Trust できる検証者のみを許す場合がある。そのような検証者はある種の Trusted Identity である。

(オ)その他のメタデータ

98. 必要に応じて、その他の情報が共有される。

(h).Verifiable Identity におけるやりとり

99. 各 Verifiable Identity は、相手先の Verifiable Identity を検証するために、期待される相手先の Verifiable Identity そのものを保持する《Verifiable Identity リスト》と、期待される相手先の Verifiable Identity が属する可能性がある Verifiable Identity コミュニティからなる《Verifiable Identity コミュニティリスト》の二つのリストをもつ。
100. 各 Verifiable Identity は、直接的なやりとりにより得た Verifiable Identity を《Verifiable Identity リスト》に登録する。あるいは、Verifiable Identity が直接または間接的に得た

Verifiable Identity コミュニティを示す情報を《Verifiable Identity コミュニティリスト》に登録する。

101. 直接的なやりとりの手法としては、例えば、《Verifiable Identity リスト》に既に登録されているアイデンティティからの紹介や、QR コードなどを用いた out-of-band 通信を伴う方法等が考えられる。

(i).Verifiable Identity の発見

102. ある Verifiable Identity の視点で、既知であり相手先として期待される Verifiable Identity か否かを、以下の二つの条件によって決定できる。
- ○ 《Verifiable Identity リスト》に登録されている Verifiable Identity である
- ○ 相手先の Verifiable Identity が《Verifiable Identity コミュニティリスト》で示される Verifiable Identity コミュニティに属しており、かつ、当該コミュニティのメンバ全てに対して期待される相手先として用いるように opt-in されている

103. どちらのリストも、最低でも Verifiable Identity または Verifiable Identity コミュニティごとに利用する、あるいは拒否するといった形で利用の可否を表現できるようにする必要がある。例えば、特定の Verifiable Identity を指定してやりとりを拒否するようなコントロールができるようにすることを想定しており、Verifiable Identity コミュニティは対象とするが、そのコミュニティに含まれる一部の Verifiable Identity を拒否するような繊細な制御も必要となると考えられる。

104. また、コミュニティに属する者の一覧に対する閲覧あるいは検索が可能であれば、直接面識がない対象であっても、発見できる。

105. 身近な例としては、連絡先管理があげられる。連絡先管理アプリのユーザーは、連絡先を発見するのに、氏名や社名など何らかの手がかりを元に検索し、検索結果から発見する。連絡先の登録にあたっては、相手と直接やり取りをする場合、もしくは誰かに紹介してもらうというステップを踏むことが想定される。直接やり取りする場合は、例えば名刺情報から連絡先をコピーして登録したり、QR コードなどの手段で名刺相当情報のコピーを受け取ったりできる。これが Verifiable Identity を《Verifiable Identity リスト》に登録することに相当する。また、《Verifiable Identity コミュニティリスト》への登録も同様である。

106. 一方、誰かに紹介してもらう場合は、紹介してもらった相手がどのような会社やサークル等のコミュニティに属しているという情報から突合したり、コミュニティに対して問い合わせたりするなどのステップを経て、発見することができる。これが、《Verifiable Identity コミュニティリスト》から Verifiable Identity を発見することに相当する。

⑤ Verifiable Identity として解釈できる実装の例

107. 例えば、ウェブブラウザがウェブサイトに接続するとき、指定された URL に基づいて接続を行う。このとき、Web PKI で可能な範囲において、X.509 PKI を用いて、実際に通信を行っているときの証明書を取得できる。これはアイデンティティといえる。アイデンティティには用いられる公開鍵暗号の公開鍵が記載されている。ここから、アクセスしているサーバのドメイン名や、証明書上で示されているドメイン名、そして実際に通信時に用いられている秘密鍵と証明書に記載のある公開鍵の一致を検証することができる。これらのことから、ここでの証明書は、一定の検証ができたアイデンティティとなる。すなわち、Web PKI は Verifiable Identity であると解釈できる。

108. また、OpenID Connect を利用したフェデレーションが構成された Relying Party（クライアント）と OpenID Provider（ID 基盤）の間でユーザーのアイデンティティ情報のやりとりを行う際、OpenID Provider は自身の秘密鍵を利用して id_token に署名を行い、Relying Party は OpenID Provider が提供する jwks_uri エンドポイントより取得できる公開鍵を利用して真正性の検証を行う。また、OpenID Connect のベースレイヤである OAuth2.0 においても高度なセキュリティが要求されるプロファイル（例：Financial-grade API/FAPI）においては mTLS を用いたクライアント認

証やクライアント証明書に紐づいたトークンの処理を行うことにより、トークンの発行先となるクライアントを検証することができる。これらのことから、Verifiable Identity はシステムで提供できると解釈できる。

109. また、デジタル庁が発行していたワクチン証明書の発行者は、ある種の Verifiable Identity である。この場合、ワクチン証明書の発行者欄に示されているデジタル庁の管理するウェブサイトの URL を起点として、アイデンティティを取得できる。そのアイデンティティには、ある種の Verifiable Data であるワクチン証明書の署名を検証するための公開鍵が記載されている。
110. なお、ここで定義される検証とは、必要とされる範囲で行われるものである。一定レベルの本人確認がなされているといった状況が均一に用意されることを前提としていないことに留意されたい。
111. 最後に、それぞれの抽象データモデルのクラスの全体像は図 3-6 に示す。

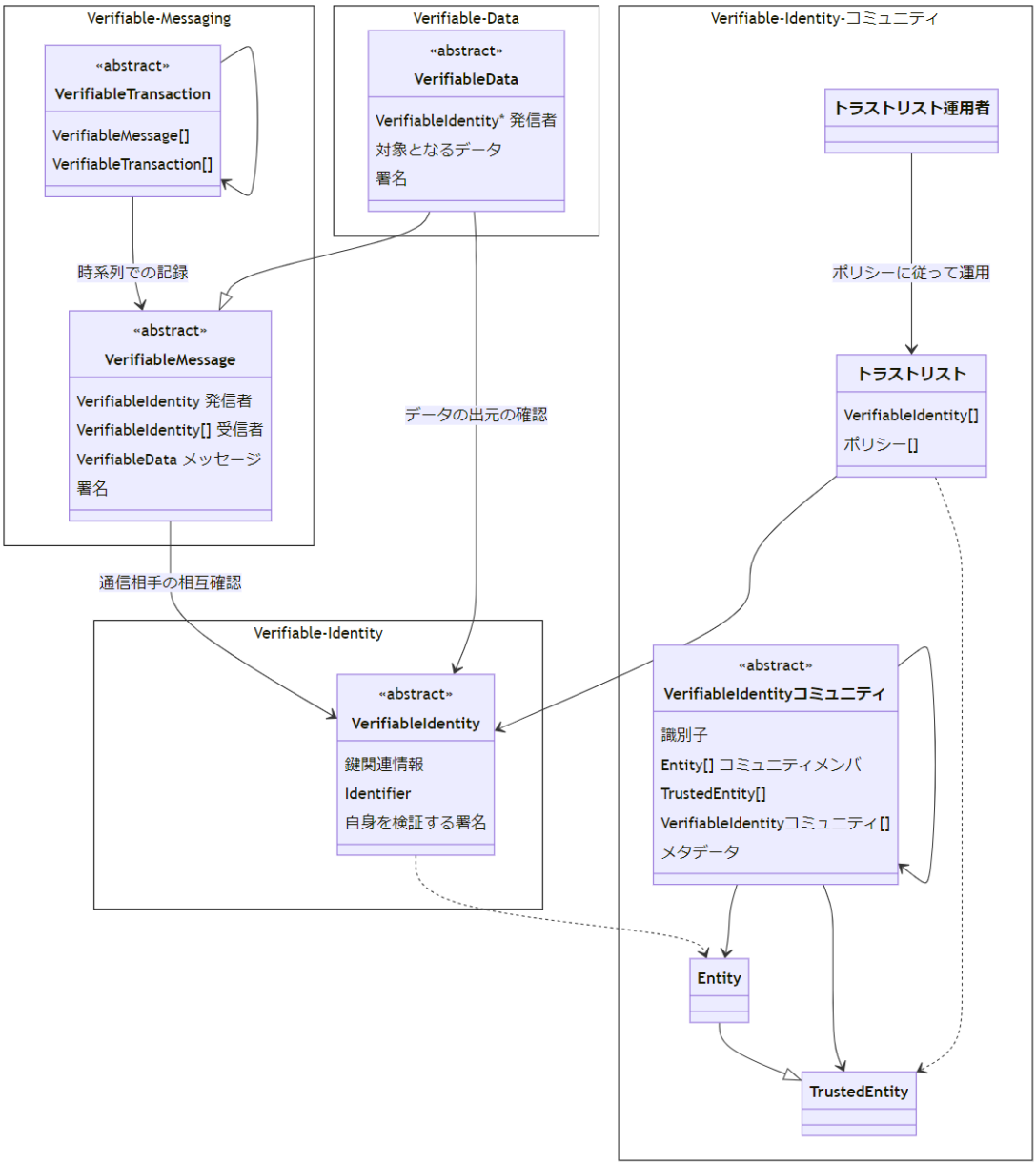

図 3-6　抽象データモデルのクラスの全体像

4. Trusted Webにおけるガバナンス

112. Trusted Webの実現において、データのやり取りに関係するエコシステム参加者がそれぞれ講ずるべき取組についてのガバナンス、およびガバナンスを有効に働かせるための仕組み（トラストフレームワーク）は、Trusted Webのパフォーマンスを左右する極めて重要な要素である。

113. 2022 年度に実施されたユースケース実証においては、様々なガバナンス上の課題が指摘された。また、G7 などの国際連携の場でも、デジタル・アイデンティティやデジタル証明書（Digital Credentials）に関する諸外国の取組において、データ及びデータのやり取りの相手方に関する信頼を供与するトラストサービスのエコシステムに関して、ガバナンス・フレームワークを策定する取組が共有され、それらの間での相互運用性が共通課題として認識されている。

114. 一方で、ホワイトペーパーver.3.0 への改訂に向けた議論では、こうしたガバナンスについての検討が十分に尽くされたとはいえない。今後はTrusted Web推進協議会を中心とした議論、また、それを踏まえた諸外国を含む有識者との討議等を通じて、ガバナンスに係る議論を深めていくことが期待される。このため、本項は、将来的な検討の基礎として、これまでの検討内容を整理したものという位置付けで取りまとめる。

(1).Trusted Webの実現におけるガバナンスの必要性

115. 前述のとおり、ガバナンスはTrusted Webの実現に大きな影響を与える要素である。例えば、下記の側面においてはガバナンスに関する考慮が重要である。

① テクノロジーだけでは解決できないことへの対応

116. Trusted Web はテクノロジーだけで実現するものではない。例えば、Trusted Web で定義するアーキテクチャを適用する際、システムを構成するエンティティ[13]がコミュニティ単位のルールや既存のトラストフレームワークに則っていることを求めるケースが存在する。そのようなケースにおいては、コミュニティ毎のガバナンスが有効であることを確認する必要がある。

② 技術的な中立性の維持

117. 検証可能性を高めることがTrusted Webの目指す姿の一つではあるが、特定の技術によって実現することを前提としてしまうとスケーラビリティや中立性の観点で問題が発生する。このため、Trusted Web を実現するために利用される技術が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必要がある。

③ ステークホルダー間での合意

118. Trusted Web はマルチステークホルダーによる合意を前提としている。中長期にわたりTrusted Web の考え方を維持するため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。

(2).ガバナンスの検討に関する課題と考え方

119. Trusted Web は、既存のインターネットとウェブというインフラの上に新たなTrustの枠組みをオーバーレイで付加することを目指すものである。この際、新たにインフラとして付加されるTrustの枠組みの部分に関して、ガバナンスの在り方がどうあるべきかについて、Trusted Webの特性を踏まえて検討する必要がある。

[13] 前述のアーキテクチャで示しているエンティティではなく、事業者、ステークホルダー、サービス、ユーザー等を指す

120. こうした、ガバナンス検討を行う上で特に考慮すべき Trusted Web の特性として下記が挙げられる。

○ Trusted Web の原則は特定の技術に依存するものではない

121. 将来的な技術や業界構造の変化に対応し、特定のエンティティ（政府や事業者等）により主導されることなく自律的に理念や原則が維持され続ける必要がある。

○ 特定の業界・コミュニティに対してのみ適用されるものではない

122. 業界・コミュニティ毎の自由度を残しつつ Trusted Web の原則（表 4-1 に再掲）から乖離しないようにする必要がある。

表 4-1 Trusted Web の原則（再掲）

カテゴリ	原則
支える仕組み	持続可能なエコシステム
	マルチステークホルダーによるガバナンス
	オープンネスと透明性
ユーザーの視点	ユーザー主体によるコントロール
	ユニバーサル性
	ユーザー視点
システムの視点	継続性
	柔軟性
	相互運用性
	更新容易性・拡張性

123. 上記の特性を踏まえ、マルチステークホルダー環境を前提とし、透明性を維持しつつ、持続可能なエコシステムを構築するためのインセンティブ設計を意識したガバナンスモデルの構築が必要となる。このモデルはインターネットのガバナンスモデルを参考にすることができる。（下記コラム参照）

［コラム］インターネットのガバナンスと Trusted Web

インターネットがその開発・運用においてガバナンスを意識しはじめたのは、ドメイン名や IP アドレスなどのネットワーク資源管理の必要性が 70 年代以降顕在化したことに端を発する。gTLD（generic Top Level Domain：国に依らない TLD のこと、代表的には.com や.net 等）の議論を得て、The Internet Corporation for Assigned Names and Numbers（以下、ICANN） が 1998 年に設立され、米国の監督下を経て、2016 年に民営化された。

インターネットは ICANN 設立時からマルチステークホルダー指向を強め、政治的中立性のあるガバナンスを目指してきた。また、インターネットとは、個別ネットワークが共通のプロトコルによって相互接続（インターネットワーキング）されたネットワークの総体であり、インターナショナル（政府の連携による国際的な構造）ではなくグローバル（インターネットをネットワークの複合によって構成される単一の系とみなす構造）での相互接続性の担保を重視してきた。ウェブも基本的にそのパラダイムの上に立脚しており、グローバルかつ技術中立指向であることが期待されている。

一方、インターネットやウェブは、単に技術優位なガバナンスによる、機能（コード）がシステムのすべてを支配するような体系を標榜してきたわけではない。むしろ、技術があらゆる人間社会に調和することを理念として目指しており、暫定的な合意形成（ラフ・コンセンサス）と自由な開発・実装（ランニング・コード）を両立させてきた。これにより、インターネットを構成するネットワーク同士の相互接続性や、インターネットが普及した後のシステムとしてのスケールの担保を実現してきた。

また、インターネットやウェブは、オペレーションテクノロジーであり、安定的運用のためのデザインも極めて重要である。すなわち、インターネットやウェブは、停止してはならず、発展・変化し続けることが求められる。そして、それを実現ならしめているものが、自律分散処理である。中央処理とは異なり、自律分散処理であるからこそ、何かがあっても自律的に動作し、それを修復して運用を持続することが可能であり、そうであるからこそ、オペレーションがスケーラブルとなり、成長し続けることが可能となった。

インターネットは、技術階層ごとに存在する要素技術を組み合わせることで、サービスが提供される。ネットワークの技術が持つ階層性の理解のために参照される構造として Open System Interconnection（以下、OSI)参照モデルが存在する。OSI 参照モデルは第 1 層の物理層から第 7 層のアプリケーション層の機能及びこれら層の間でやりとりされる情報を定義している。現在のインターネットでは、このような層上の構造を持つ、Transmission Control Protocol/Internet Protocol（以下、TCP/IP)や Ethernet などが標準的に実装されている。

インターネットの主要なサービスの一つであるウェブも同様で、HTTP（以下、Hyper Text Transfer Protocol）という標準化されたプロトコルに準拠して技術が実装されている。具体的には、OSI 参照モデルの 7 層モデルにおいて、第 4 層（トランスポート層）までは TCP や UDP といったプロトコルを、ウェブ以外のサービス（例：電子メール）と同様に用いる。一方、第 5 層（セッション層）以上が HTTP によって定義され、ウェブとしての振る舞いを構成している。このように、標準技術の組合せによる構成によって、インターネットそのもの、またはインターネットで提供されるサービスの相互運用性が実現する。

しかしながら、データ及びデータのやりとりの相手方に関する真正性の点においては、たとえば HTTP や TLS（Transport Layer Security[14]）では、サーバの運用者証明以外の Trust に係る機能が提供されていないこと、また、認証は OIDC（OpenID Connect）などで取り組まれているがそれも担保している範囲が限られていることなどの観点から、Trust を実現するための技術は十分には提供されていないと考えられる。

このため、Trusted Web においては、やりとりするデータ及びデータのやりとりの相手方についての検証可能性を向上するための技術（例えば、クレデンシャルフォーマット）の利用を促進する。また、特定の事業者が過度に影響力を持ちすぎない形で、グローバルな相互運用性及び技術的中立性を目指すことに留意することが必要である。

Trusted Web は、現在のインターネットとウェブに立脚し、既存の技術要素に対するオーバーレイのアプローチによって進める。また、その際、相互運用性と技術中立性の実現と継続を目指す。さらに、オペレーションが止まらずに持続し、発展し続けることができるように自律分散処理が担保される必要がある。こうした点で、Trusted Web の基本理念は、上述のインターネットガバナンスの考え方に原則として準じている。

(3).Trusted Web におけるガバナンス

124. 前述のとおり Trusted Web は、特定の技術へ依存しない技術中立的な考え方であるとともに、特定の業界やコミュニティに特化した考え方でもない。これらのことから Trusted Web の考え方に則って構成された具体的なシステムのみならず、Trusted Web のアーキテクチャ等についても、将来的な技術の発展・変化、法令等の社会システムの変化に応じて将来変化していくことが想定される。一方で、こうした変化により Trusted Web の根源となる原則が失われることがないようにするための仕組み・枠組みが必要となる。

125. 上記を勘案すると、Trusted Web におけるガバナンスは、対象、目的、主体が異なる複数の階層で構成されるものとして定義できる。（下図参照）

[14] TCP/IP ネットワークでデータを暗号化して送受信するプロトコルの一つ。デジタル証明書（公開鍵証明書）による通信相手の認証（一般的にはサーバの認証）と、共通鍵暗号（秘密鍵暗号）による通信の暗号化、ハッシュ関数による改竄検知などの機能を提供するもの

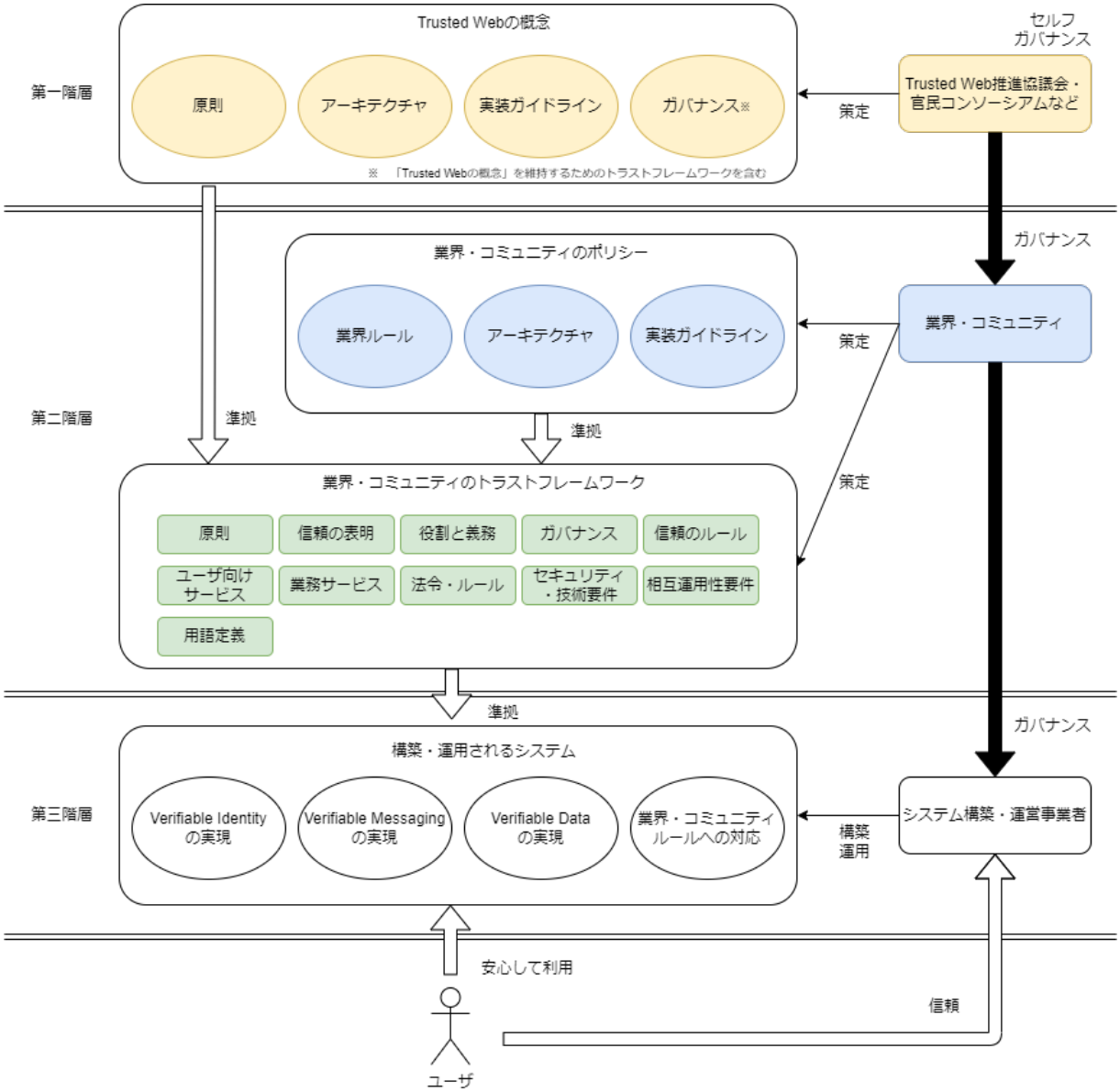

図 4-1 Trusted Web におけるガバナンスの全体像

126. 図 4-1 に示した階層構造ごとのガバナンスの目的、対象、主体は以下の通りとなる。

[第一階層] Trusted Web という考え方自体に関するガバナンス
127. 目的：Trusted Web の原則の維持
128. 対象：Trusted Web 推進協議会、将来的に検討する官民コンソーシアム※セルフガバナンス
129. 主体：Trusted Web 推進協議会、将来的に検討する官民コンソーシアム

[第二階層] Trusted Web の考え方に準拠したトラストフレームワーク提供者に関するガバナンス
130. 目的：トラストフレームワーク提供者を含むエコシステムの維持
131. 対象：業界・コミュニティ毎のトラストフレームワーク提供者
132. 主体：Trusted Web 推進協議会、将来的に検討する官民コンソーシアム

[第三階層] トラストフレームワークに従って構成・運営されるシステムに関するガバナンス
133. 目的：各システムが Trusted Web の原則に則って構成・運営される状態の維持
134. 対象：システム（構築・運営事業者）

135. 主体：業界・コミュニティ毎のトラストフレームワーク提供者

136.　各階層に関するガバナンスについて解説する。

① ［第一階層］Trusted Web という考え方自体に関するガバナンス

137.　本階層におけるガバナンスは Trusted Web の原則が一部の事業者等によって改変され、失われることを防ぐことを目的としている。現在、Trusted Web 推進協議会により定義されている Trusted Web の概念（ホワイトペーパーの Trusted Web の原則やアーキテクチャ、実装ガイドライン等）を将来的な技術の進歩や社会環境の変化等に適応させていくための運営体制に関する考え方を整理しておく必要がある。

138.　運営体制を考える上では、Open Identity Exchange（OIX）[15]が公開している「A Guide to Trust Framework for Smart Digital ID[16]（以下、OIX ガイドライン）」を参考にすることができる。OIX ガイドラインではトラストフレームワーク（本階層におけるトラストフレームワークは図 4-1 内の「Trusted Web の概念」を維持するためのルール等を指す）を維持するためのガバナンス主体となる組織の在り方として、以下のような形態を挙げている。

○　独立した運営組織
例）カナダの DIACC（Digital ID and Authentication Council of Canada）[17]のような官民のリーダーシップによる非営利連合

○　参加者によるコンソーシアム型組織
例）CA/Browser フォーラム[18]（ブラウザベンダーと認証局が参加するコンソーシアム）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[19]や Google が運営する ID プロバイダのような単一の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[20]など独立した非政府の標準化・認定団体・組織

○　全ての参加者による相互合意

○　特別なガバナンス主体を設けず参加者全員による合意に基づく運営

139.　これら列挙されている形態と Trusted Web の特徴（マルチステークホルダー）に鑑みると、カナダの DIACC に類する独立した運営組織を、官民のリーダーシップにより構成していくことが望ましいと考えられる。この際、現在内閣官房デジタル市場競争本部に設置されている Trusted Web 推進協議会をより中立的かつ持続可能な組織形態へと移行していくため、こうした官民コンソーシアムの組成なども今後の検討課題となってくる。

140.　また、以上のようなトラストフレームワークの「ガバナンス主体」は、OIX ガイドラインによれば以下の役割を持つとされており、Trusted Web においても同様の役割を持つことが想定される。

[15] https://openidentityexchange.org/
[16] https://openidentityexchange.org/a-guide-to-trust-frameworks-for-smart-digital-id
[17] https://diacc.ca/
[18] https://cabforum.org/
[19] https://login.gov/
[20] https://kantarainitiative.org/

なお、ここでトラストフレームワークに参加するエンティティはTrusted Web推進協議会や将来的に検討する官民コンソーシアムを構成する主体を指す。

(a).トラストフレームワークの執行

トラストフレームワークに参加する各エンティティは定義されたルールに従いその状態を維持する必要がある。場合によっては強制力を持って統制を行うこともガバナンス主体の役割となる。

例えば、執行には以下のような内容が含まれる。

○ 参加エンティティの管理
- 参加エンティティの管理・登録・認証・紛争解決

○ 対外的な情報提供によるネットワークの発展
- マーケティング、コミュニケーションに関する戦略立案と実行

○ 参加エンティティおよび対外的な情報提供や不正管理のための仕組みの構築と運用（トラストリストの作成・公開・維持など）によるルールが遵守されていることの保証（評価・監査を含む）、変更・リリース管理

(b).トラストフレームワークの認証

トラストフレームワークに参加する各エンティティが定義されたルールに従っていることを認証する必要がある。各エンティティは自己評価を行い、ガバナンス主体による承認を経て認証される。

(c).トラストフレームワークの運用

先述の通り、ガバナンスの在り方を含むトラストフレームワーク自体も将来的な技術の進歩や社会環境の変化等に適応させていく必要がある。

141. なお、各種のガバナンス主体がトラストフレームワークの執行の結果として、トラストリストを作成・管理することは従前から行われている手法の一つである。このため、Trusted Webにおいても検討すべき手法である。トラストリストの作成にあたり、Trusted Webの構成要素と同様にトラストリスト自体の検証可能性を担保することが重要となる。

142. その他、トラストフレームワークの作成・維持を行う際には、業界毎（場合によっては国を跨ぐ）に成熟度は異なること、また、特定の場所（対面・非対面、国・地域）や技術（デバイス、ネットワーク環境）、分野（公共・民間）は限定されないこと、について十分に配慮する必要がある。これらの点については OECD 理事会によるデジタル・アイデンティティのガバナンスに関する勧告[21]が参考となる。

② ［第二階層］Trusted Webの考え方に準拠したトラストフレームワーク提供者に関するガバナンス

143. 本階層におけるガバナンスは、Trusted Webの原則に加え業界・コミュニティ単位のルール・慣習等に従い策定される、業界・コミュニティ単位のTrusted Web準拠のトラストフレームワークを取り巻くエコシステムの維持を目的としている。

144. 先述の通り Trusted Web は特定の業界・コミュニティに特化するものではない汎用的な概念であり、適用対象となる業界・コミュニティが解決する課題は様々である。例えば、Trusted Web のアーキテクチャに則ってシステムを構成する場合も、システムを構成するエンティティを信頼するために、業界・コミュニティ毎のルールや認定制度によって認められていることが必要とされるケースも存在[22]する。このように、ある程度の自由度を維持しつつもTrusted Webとして機能す

[21] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491

[22] 例えば学術機関における学術認証フェデレーション（https://www.gakunin.jp/）等

るためには、各業界・コミュニティにおいてトラストフレームワークの策定・提供を行う事業者等に対する「適度な」ガバナンスが重要となる。

145. なお、OIX のガイドラインでは、トラストフレームワークを構成する要素として以下を挙げている。Trusted Web 推進協議会もしくは今後の検討事項である官民コンソーシアムは、業界・コミュニティがトラストフレームワークを策定する際に、そのトラストフレームワークの各構成要素に Trusted Web の概念が正しく反映されることを求めていく必要がある。

表 4-2 トラストフレームワークの構成要素と Trusted Web に求められること

構成要素[23]	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）	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）
業務サービス（Relying Party Services）	同上
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

146. なお、業界・コミュニティの規模や、組成されてからの期間などの要素によってはトラストフレームワークの策定が不必要、もしくは十分な運営体制の整備ができないケースも存在する。こうしたケースにおいては、業界・コミュニティ内で Trusted Web に準拠していく旨を合意（例えば、Trusted Web の原則に賛同していることを自主的に表明する等）しつつ運営していくことが重要となる。

③ ［第三階層］トラストフレームワークに従って構成・運営されるシステムに関するガバナンス

147. 本階層におけるガバナンスは、業界・コミュニティ毎に策定されたトラストフレームワークに準拠した形で実際に構築・運用されるシステムが、トラストフレームワークに定義された状態を維持し続けること、つまり、Trusted Web の原則に則って構成・運用されている状態を維持することを目的としている。実際の運用は業界・コミュニティ毎に異なるが、基本的には、第二階層で策定されたトラストフレームワークに則って各システムが構成・運用されていることを確認（例えば、アセスメント等により認定する等）する運用を継続的に実施していくこととなる。

[23] OIX のトラストフレームワーク構成要素より引用（https://openidentityexchange.org/a-guide-to-trust-frameworks-for-smart-digital-id?page=digital-identity-trust-framework）

148. 以上を踏まえ、Trusted Web では、上記の通り第一階層から第三階層までのガバナンスが有効に機能することによって、ユーザーに対して信頼を与え、安心してシステムを利用することが可能となる姿を目指す。

5. Trusted Web におけるセキュリティの考え方

(1).Trusted Web におけるセキュリティ目標

149. Trusted Web で指向しているシステムのセキュリティは、ユースケースごとにセキュリティ目標が異なり、また技術的な実装方法も異なるため、一般的には、ISO/IEC 27000 シリーズのような情報セキュリティマネジメントの考え方に基づき、個別のシステムのユースケースとシステム構成に応じて、リスク分析を行い、その上でリスク管理に見合うセキュリティ対策しての技術と運用を設計し実行する。

また、そのセキュリティ設計と運用は、定期的に見直される必要がある。

つまり、セキュリティ目標は、ユースケースと実装に依存し、かつ、レイヤー化による共通化ができるものではない。また、技術的中立を重視して設計することを考えると、Trusted Web のホワイトペーパーにおいて、具体的な実装方針に関連したセキュリティ目標を挙げることは難しい。

一方で、アーキテクチャの設計検討や机上検討、ユースケース実証事業の実施によるセキュリティ上の課題の抽出が進んだ ver.3.0 においては、[1] Trusted Web の主要な目標であるデータのやり取りにおける検証可能性の向上による信頼の向上のための仕組みそのものの安全性、および [2] Trusted Web を支える仕組みの安全性の 2 つに分けてセキュリティを検討する必要性が明らかとなった。それは[1]の部分で、特定のエンティティに依存しない検証の仕組み（プロトコルなど）が構成できたとしても、[2]の部分が特定のエンティティに依存していたり、単一障害点となったりする場合、Trusted Web の目標達成の阻害要因となるからである。

具体的には、[1]に含まれるセキュリティ目標として以下のものが挙げられる。これは、主に Trusted Web でやり取りされる属性情報とそれに付随する電子署名の付与と検証に係る部分である。

- ○ 属性情報の発行者の特定と検証
- ○ 属性情報の検証（改ざん検知）
- ○ 属性情報の通信における提供元の特定と検証
- ○ 属性情報の通信における提供先の特定と検証
- ○ 選択された属性情報のみの開示の保証
- ○ トランザクションの非改ざん

150. 一方、[2]に関係するセキュリティ目標として以下のものが挙げられる。

- ○ Trusted Web で用いられる暗号技術の鍵（特に秘密鍵、公開鍵）の安全な管理
  - ● 秘密鍵や公開鍵が、Hardware Security Module (HSM)、スマートカード、CPU 上の Trusted Execution Environment (TEE) などの秘密に計算できる領域から外に出ないこと
  - ● 鍵の生成、活性化、不活性化、廃棄などのライフサイクルマネジメント、有効期限の管理ができていること。利用者による紛失に対応できるように、安全にリカバーする仕組みを有すること。

- ○ VC などの電子署名に基づいたデータには、有効期限が存在するため、これらのデータのライフサイクルマネジメントが正しくなされること。

- クレデンシャルの生成や活性化、不活性化、廃棄などのライフサイクルマネジメント、また、有効期限の管理ができていること。利用者による紛失に対応できるように、安全にリカバーする仕組みを有すること。
- 有効期限外のクレデンシャルによって誤って認証・認可されないようにすること

○ Trusted Web に基づいて構築された個別システムのリスク評価、およびセキュリティ評価結果の公開検証性

○ Trusted Web における暗号プロトコルの実行ノードが自動実行可能な IoT デバイスの場合のセキュリティ確保

○ データの保管場所として、InterPlanetary File System（IPFS）などの大規模分散ストレージが想定されるユースケースが多いが、これらのストレージのデータの信頼性や、IPFS 以外の情報からのデータの信頼性については、Trusted Web と同等の検証可能性やトラストが期待できない場合が多いため（いわゆるオラクル問題）、これらのデータの信頼性を確保する手段が用意される必要がある。

○ 各ノードにおけるセキュリティマネジメントのポリシーやプロセスが明確化され、そのプロセスに従って実行していることを検証可能であること。

○ 秘密計算など、高度な暗号プロトコルを組み込む場合には、証明可能な安全性を有すること。

(2).Trusted Web におけるセキュリティ目標の実現方法

151. 今回のユースケースに応じたプロトタイプの設計においては、現実的な実装として DID を用いた方法の経緯が示されている。この設計を念頭に、先述のセキュリティ目標を達成しようとすると、以下の技術が必要であるとともに、これらの技術は第三者によってグローバルに安全性の確認とその確認内容に対する合意がとれたものである必要がある。

○ 電子署名、および属性証明

○ DID プロトコル（暗号プロトコルに関する安全性の検証（形式検証等））

○ （必要であれば）基盤としてのブロックチェーン（署名のハッシュによる連鎖、分散合意、インセンティブメカニズム等）

○ 認証プロトコル（ISO/IEC 9798 など）

○ 認証付き鍵交換（ISO/IEC 11770 など）

○ セキュアなウォレットの実現技術、Trusted Execution Environment（TEE）など

○ 情報セキュリティマネジメントシステム（ISO/IEC 27000 シリーズ）

(3).セキュリティに関する今後の検討課題

152. インターネット上での Trusted Web で指向しているシステムの構築においては、リスク分析そのものの実行や、リスク分析結果に基づいたセキュリティ対策の立案や運用が、利益を産まない、あるいは利益の阻害要因になるなどの理由で後回しになることが非常に多い。
　このため、長年にわたり、セキュリティ・バイ・デザインやプライバシー・バイ・デザインの考え方が提唱されているが、これらの考え方は、総論としては賛同されるものが多いものの、ベンチャー企業やスタートアップでも実現可能な現実的な実行方法が存在しておらず、現実には現在の多くのシステムで実行されていない。また、いわゆる Web3 などの、新しいウェブに関するアーキテクチャの議論でも、デジタル署名のような暗号技術を使い、セキュリティの向上を目指しつつも、全体のセキュリティデザインについての議論が進んでいない。
　そのため、Trusted Web 推進協議会におけるウェブの新しいアーキテクチャとガバナンスの議論においては、Trust の重要な構成要素として、セキュリティ・バイ・デザインとプライバシー・バイ・デザインの実現に向けた取組を検討する必要がある。

153. Trusted Web における主要な性質である検証については、それが、情報数学におけるプロトコル仕様や、その実行コードとしてどう反映させるか、どうセキュアに設計するか、についての検討が必要である。これまでの議論は、自然言語として、その要求条件を議論しているが、セキュアに実装するためには、形式的にアルゴリズムや数式で記述できる必要がある。Trusted Web のセキュリティを考えるために、プロトコルの要件と仕様について、自然言語ではなく、数式で記述するための取組を行う必要がある。この記述が、プロトコルセキュリティの安全性証明、あるいは検証のために不可欠であることがその理由である。

154. 多くのユースケースにおいて、電子署名を基盤とした検証が行われており、通常の電子署名とともに、新しく Verifiable Credential などの属性情報に対するクレデンシャルが用いられている。前述したように、秘密鍵、およびクレデンシャルのライフサイクルマネジメントをセキュリティ目標の１つとしているが、これらのライフサイクルマネジメントは、NIST SP800-57 に示されている PKI のモデルとは異なるため、新しいモデルの構築が必要である。また、鍵管理についても、従来のモデルではない Wallet を中心にした新しいモデルの構築が必要である。

155. また、プロトコル設計におけるセキュリティの評価には、攻撃者の特定と攻撃者の能力の想定が必要である。前者は、ユースケースに依存する。後者については、暗号プロトコルの一般的な攻撃者モデルとして Dolev-Yao モデルなどの既存のモデルについて、その適用方法を今後検討すべきである。これらの検討により、例えば、よく知られた中間者攻撃（Man in the Middle 攻撃）に対する安全性の検証などが可能になる。

6. 今後の取組について

(1). 今後の課題

156. ここまで見てきた検討を踏まえ、今後、以下の点についてさらに深掘り検討していく。

① アーキテクチャについて

157. 「署名の意図」が共有されるための具体的なデータモデルや、操作についての検討
158. 合意形成にまつわるモデルについて、合意形成に必要なデータ、合意条件、合意の内容などのモデル化とともに、合意の破棄の記録の検討
159. 例えば「合意形成の前に、その内容が倫理的に正当かどうかの検査をし、足切りした上でユーザーは足切り後の安全な空間の中だけで選択する。相手の提示した term はウォレットに入って管理され、それを使って権利行使ができる」といったユーザー保護の観点からの検討

② 実装における課題

160. シリアライゼーション、アルゴリズム選択、公開鍵の指定、パッケージングといった視点での技術適用において、適切なフレキシビリティを持たせつつも共通化していくための検討

③ ガバナンスについて

161. 新たに共有財（コモンズ）としてのインフラに付加される Trust の枠組みの部分におけるガバナンスの在り方がどのようなものであるべきかのさらなる検討
162. マルチステークホルダーによるガバナンスの具体的な在り方（政府の役割の在り方を含む）の検討
163. 発行者が共通ウォレットアプリに発行するインセンティブ（独自ウォレットアプリにおける双方向通信、プッシュ通知、あるいは利用履歴の情報の取得など、金銭以外のインセンティブ）や、何をもってウォレットは検証者からのリクエストをアクセプトするかという事業者にとってのインセンティブの具体的な在り方の検討
164. Trusted Web の理念を実現するトラストフレームワークに対してお墨つきを与えて、そのトラストフレームワークに則って各コミュニティがシステムの認定・運営をしていくといった認定を想定した場合の、認定を受けるメリットやその方式の検討
165. トラストフレームワークをコミュニティに委ね、コミュニティの中でガバナンスを担保するための仕組みづくり

④ セキュリティについて

166. Trusted Web における共通的なセキュリティ目標のさらなる検討
167. Trust の重要な構成要素として、セキュリティ・バイ・デザインとプライバシー・バイ・デザインの実現に向けた取組みの検討
168. 検証について、情報数学におけるプロトコル仕様や、その実行コードとしてどう反映させるか、どうセキュアに設計するかについての検討
169. プロトコル設計におけるセキュリティの評価における攻撃者の能力の想定のための既存のモデルの適用方法の検討
170. 秘密鍵、クレデンシャルのライフサイクルマネジメントモデルの検討

(2). 国際連携の方向性

171. Trusted Web のコンセプト普及を国際的に推進する上では、まずは他国政府や企業、技術者等の間で認知度を高め、理解を得ることが必要であり、規格策定を前提としない自由度の高いディスカッションの場に参加することが有益であるという提言が得られた。

172. 国際的な認知度を向上させるのと同時に、具体的な標準規格の提案内容や、Trusted Web を国際的に推進するために必要な要素（例えば、技術的な相互運用性、各国制度との整合性）を明確にする必要がある。その議論を国内で深めた上で、スコープや粒度が近い国際標準化機関・団体を選定することにより、効果的な国際連携ひいては国際標準の提案や検討を行うことができると推測される。

173. なお、Trusted Web に関連する標準や Trusted Web 実現に向けての今後の課題の整理、必要となる標準策定についての検討の詳細については、「Trusted Web の国際標準化に向けた調査」[24]を参照されたい。

174. まず、Verifiable Credentials を中心とした取り組みは、W3C においては主には特定のアプリケーションによらない、抽象度の高いデータモデルについての議論である。従ってデータモデルに関連した部分については W3C での議論が自然である。

175. また、データ自身をどのようにやり取りするのかというトランスポートの視点では、IETF にて標準化を進める必要もあり、実際、Verifiable Credentials に関連した標準化の一部は IETF で行われている。

176. そして、IETF は、OIDF（OpenID Foundation）や DIF（Decentralized Identity Foundation）で検討したことが部分的に切り出されるので、これらの組織との連携を深めていくことが重要である。

177. OIDF は、法人、金融、健康関連データ等の個別論点・テーマへの OIDC の適用について議論が行われており、ユースケースとの連携の可能性があり、OIDC と VC や DID を連携させるための規格として OID4VCI/VP（OpenID for Verifiable Credential Issuance ／Verifiable Presentations ）が策定されており、連携を深めていく必要がある。

178. 一方、データモデルにおけるドメイン知識についての議論にあるように、適用対象となる業界毎に扱うデータは異なり、業界内でデータモデルが整っている業界もそうでない業界もある。また、仮に国内での業界標準があったとしても、国際的に共通したデータモデルが存在しない場合もある。すなわち、業界毎にデータモデルの成熟度にはばらつきがあるのが実情である。

179. しかし、高度かつグローバルなデータ流通を志向するのであれば、データモデルは適用するアプリケーション領域ごとにグローバルスタンダードとして整える必要がある。そのような整備が進まない限り、Trusted Web によってデータの正しさが検証できたとしても、十分な効果は得られないと考えられる。従って、Trusted Web を適用するためには、業界によっては、データモデルの共通化を併せて進める必要があり、Trusted Web の適用自身がデータモデル共通化を後押しする形にできる可能性はあると考えられる。

180. 例えば、DCC（Digital Credentials Consortium）を中心に、W3C で検討している vc-ed（Verifiable Credentials for Education Task Force）における取組を継続したり、連携したりするといったアプローチがあり得る。

[24] 「令和３年度産業標準化推進事業委託費（戦略的国際標準化加速事業：ルール形成戦略に係る調査研究 Trusted Web の国際標準化に向けた調査）」

181. Trusted Web との協調可能性を探る上では、ISO/IEC JTC 1/SC 27（情報セキュリティ、サイバーセキュリティとプライバシー保護に関する小委員会）における WG5（プライバシー、アイデンティティ管理とバイオメトリクス）、特にアイデンティティ管理領域に関する検討について関連性が強いと考えられる。

182. この WG5 の議論には、Trusted Web 推進協議会やタスクフォースの委員が議論に参画しており、まずは、こうした委員の協力も得ながら、議論の検討状況を注視していくことが望ましい。

183. 特にアイデンティティ管理のような領域はシステムの規模が極めて大きくなりやすい中、むしろ、ISO のような「標準化機構」よりも、以下の表で記載された機関において、仕様が決められ、実装され、利用された上で、その後に、アーカイブ的に ISO などに持ち込まれる傾向がある。

184. 実際にこうした認識は、ISO TC 307 が W3C や Kantara Initiative と連携していること、また ISO/IEC JTC 1/SC 27 WG 5 において取組が複雑化していることなどからも裏付けられる。このため、これらの機関との連携の模索も重要である。

表 6-1 標準化における協調先機関の例

機関名	活動対象としている地域	概要
NIST	米国	National Institute of Standards and Technology：米国立標準技術研究所。米国政府機関で利用される情報セキュリティ技術等の標準化を行う、商務省傘下の機関。ISO/IEC JTC 1/SC27 WG 5 等の米国の国内審議団体でもある。
MITRE	米国	米国の連邦政府が資金を提供するセキュリティ分野の非営利組織であり、R&D センターと官民のパートナーシップを通じて、国の安全性、安定性、福祉に関する事項に取り組んでいる。NIST の連邦研究開発センター（Federally funded research and development center：FFRDC）の運営主体でもある。
ENISA	欧州	European Network and Information Security Agency：欧州ネットワーク情報セキュリティ機関。ネットワークと情報に関する欧州の中心的な機関で、 EU 加盟国や民間の部門と緊密に連携することにより、サイバーセキュリティ対策を向上するためのアドバイスや提言を行う。また、国家情報セキュリティに関する EU の政策と法案の開発や実施もサポートする。
Kantara Initiative	米、欧、豪、日	アイデンティティ管理に関する技術仕様と推奨事項を提言する非営利団体。崎村氏は創業者の一人でもある。
OpenID Foundation（OIDF）	米、英、欧、豪、伯、中東、アフリカ、日等	アイデンティティ管理・API 保護に関する技術標準規格策定団体。米国非営利法人。DIF との提携により、VC の連携規格はここで策定されているほか、金融機関などの持つ情報の連携などの観点で各国当局と共同で規格開発、適合性試験開発をしている。
Decentralized Identity Foundation（DIF）	米国、欧州	2017 年に設立された。分散型アイデンティティ・ソリューションにより、エンティティが自分のアイデンティティをコントロールし、信頼できる相互作用を可能にする世界を実現するために、相互運用可能なグローバルスタンダードの確立に向けた「事前競争的」技術基盤を促進するための研究開発を行うことをミッションとしている。

Modular Open Source Identity Platform (MOSIP)	印	インド国内のデジタル ID プログラム （India Stack）をベースに、e ガバメント（電子政府） のあらゆるデジタル公共サービス提供メカニズムの基礎的なビルディング・ブロックを形作るデジタル身分証明（デジタル ID）プラットフォームを、第三国展開用にパッケージ化
iSpirt	印	2013 年にバンガロールで設立された非営利のシンクタンクで、India Stack の設計を主導した団体。ソフトウェアやデジタルプラットフォームを用いて社会のトランスフォーメーションを行うという趣旨に賛同した多数のボランティアで構成されている。

(3).今後の社会実装において、各ステークホルダーに期待したい役割

185. 今後、Trusted Web の構想を具現化していくためには、内外の各ステークホルダーが協働していくことが必要であり、また、各ステークホルダーが連携していくことができる場を形成していくことも必要である。
186. 各ステークホルダーに期待したい役割としては、例えば以下のとおり。

① エンジニア等

187. エンジニアは、疎結合を志向する Trusted Web の中で協働して、アーキテクチャの検討を深化させ、リファレンスモデルを作って普及を拡大し、様々なモジュール開発やサービス開発を行うとともに、保守運用を担うことなどが期待される。これらについては、オープンかつ高い透明性を持って取組が進むことが望まれる。

（基盤に関する標準化やリファレンスモデルづくり）
188. Trusted Web を実現する上で肝となるのが、様々なウェブ上の標準化やリファレンスモデルづくりである。特にこうした標準化やリファレンスモデルづくりに貢献したエンジニアに対しては、その貢献が評価され、Trusted Web の価値を向上させることが自らの利益にも資するようなインセンティブ設計を検討していく必要がある。

（開発）
189. アーキテクチャの中でモジュールごとに、Trusted Web を具現化するために組み合わせて利用できるようにすることが期待される。

（保守・運用）
190. 系を正しく運用していくこと、系が正しく動いているかをモニターし、改善を加えていくこと、中期的にもサステイナブルにしていくことが重要であり、こうした運用面を担うエンジニアの役割も重要である。

（試験）
191. 長期運用性、セキュリティ・バイ・デザイン視点で、システムの設計、実装、運用保守にわたり、それぞれの段階で、試験可能性、動作の検証可能性を追求する必要がある。

（サービス）
192. これまでのプラットフォームサービスとは異なる競争軸で、データ主体のコントロールを尊重する新しいビジネスモデルを創出していくことが期待される。

（UI/UX）

193. Trust が担保されていることが、ユーザーにとって分かりやすく実感できるよう、デザイナーの参画によって、UI/UX を重視した実装を行うことが期待される。

② 大学等研究教育機関

194. 大学等については、中立的な立場で Trusted Web の技術開発や技術評価、国際標準化等を進めることが期待される。

195. 技術的に進んだ事例の標準化に当たっては、参加するステークホルダーの思惑から国際標準の精度が不十分となったり、十分に活用されない標準となったり、実際に運用することが不可能なものとなるような事例が過去にある。プロトタイプの実装など、「動くコード」で実証していくことが求められるが、大学等の研究機関が他のステークホルダーと共に中立的な立場で開発に参加することで、Trusted Web を、実験的な利用にとどまらず、広く使われる技術として成熟化させることが可能になる。

196. 特に、Trusted Web はセキュリティ関連技術と密接な関係がある。エンジニアと連携しながら設計段階から検証を可能とするようにするなど、手法の確立などを含め、セキュリティ・バイ・デザイン思想で進める点では、研究機関からの協力が欠かせない。

197. また、大学に限らないが、Trust に関する技術の教育の不足は対応すべき課題である。大学が教育推進の中心的な役割を担う必要がある。

③ 国際標準機関

198. Trusted Web の実現に向けては、国際標準機関との協働が不可欠である。まずは、本ホワイトペーパーにおける今後の課題も含め、フィードバックが得られることを期待する。技術面だけでなく、運用やガバナンスも併せて考えていく必要があり、こうした点も含めて、今後議論が活発に行われていくことが期待される。この際、当協議会としては、検討や実装によって得られる知見をフィードバックする等により、貢献していく。

④ 政府等

199. 政府は、Trusted Web 上の機能としては、本人確認や登記等についてのトラストアンカーとしての役割（なお、トラストアンカー自体は、必ずしも政府に限定されない）や、Trust を担保するための制度を整備し、執行する役割を担っている。

200. このため、トラストアンカーを担う制度等の整備とそれへの接続を可能とすること、国際標準機関に政府としてのユースケースを提示するなどにより議論に貢献すること、関連する法制度を整備し、コード上も含めたエンフォースメントの担保やルールメイキングを担うこと、Trusted Web のマルチステークホルダーによるガバナンスに参加することが期待される。

201. また、各国政府間で問題意識を共有し、議論を深めていくことも必要である。