Trusted Web ホワイトペーパー

Ver1.0

2021年3月12日

Trusted Web推進協議会

Trusted Web White Paper Ver1.0 Executive Summary

1.背景(本文1.～2.)

○フェイクニュースなど流れるデータの信頼性への懸念、プライバシー侵害リスク、勝者総取りに伴う単一障害点のリスク、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が生じている。

○「デジタル社会」への移行にあたり、通信プロトコルを主に規定する現行のインターネット/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現できておらず、Trustの再構築が不可欠。

2.Trusted Webの方向性等(本文3.～5.)

○これまでのTrustの仕組みでは、データのやりとりにおいて確認・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。データを紐づける識別子の仕組みもプラットフォーム事業者に依存。

○特定のサービスに依存せずに、データのコントロールや合意形成の仕組みを取り入れ、検証できる領域を拡大し、Trust(相手が期待した通りに振る舞う度合い)を高めていくことが必要。

○こうしたTrustの枠組みを現行のインターネットの上に重ね合わせ（オーバーレイアプローチ)、多様な主体による新しい価値の創出を目指す。これをTrusted Webと呼ぶ。

○ユーザーがデータへのアクセスをコントロールでき(Identifier管理機能)、相手やデータに関する信頼を第三者によるレビューも含めて検証でき(Trustable Communication機能)、双方の意思を反映した動的な合意形成(Dynamic Consent機能)とそのプロセスやその後の履行状況を検証できる(Trace機能)。マルチステークホルダーによるガバナンスでこれを支える。

○信頼できる情報が価値を持ち、不知の者同士でもデータの共有が容易となる等により新たな経済的価値の創出が期待される。

3.実現に向けた道筋(本文6.)

○　本ペーパーは、今後内外の様々なコミュニティと協働して検討を深めていくための「ディスカッションペーパー」。関係ステークホルダーと協働し、2030年までにインターネット全体で実装を目指す。

目次

1. 検討の背景

○　昨今、データやデジタル技術の活用が急拡大し、特に、COVID-19 を契機にその動きは加速している。これにより、社会全体のデジタル・トランスフォーメーションが進む「ニューノーマル」の時代を迎えようとしている。

こうした中で、日本政府は、「デジタルの活用により、一人一人のニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会　～誰一人取り残されない、人にやさしいデジタル化～」とのビジョンを掲げ、デジタル社会の実現に向けて取り組んでいくこととしている。

また、日本政府は、「サイバー空間(仮想空間)とフィジカル空間（現実空間)を高度に融合させ、経済発展と社会的発展を両立する人間中心の社会」(第五期科学技術基本計画。2016.1)として、「Society 5.0」を提唱している。これは、少子高齢化等の様々な社会課題を抱える日本としての目指すべき未来社会であるとともに、国際社会が推進している SDGs の目標の達成に貢献するものである。

○　他方で、様々な課題も顕在化してきている。こうした中で、デジタル市場競争の観点から検討を行っている内閣官房デジタル市場競争会議では、サイバーとフィジカルが高度に融合する Society5.0 におけるデジタル市場の在り方について、中長期的な観点から検討を行い、2020 年 6 月、「デジタル市場競争に係る中期展望レポート」（以下「中期展望レポート」という。）をとりまとめた。

○　この「中期展望レポート」においては、デジタル市場の目指すべき姿として、“一握りの巨大企業への依存”でも、“監視社会”でもない第三の道として、

- 多様な主体による競争
- 信頼（トラスト）の基盤となる「データ・ガバナンス」
- 「トラスト」をベースとしたデジタル市場

の実現を目指すとの提言がなされた。

そして、その実現の一つの方策として、「データ・ガバナンスの在り方をテクノロジーで変える分散型の“Trusted Web”の実現」が提言された。

○　この提言の背景として、「中期展望レポート」においては、以下のような指摘がなされている。

現行のインターネット上での通信の多くは、集中型のアーキテクチャーをベースとしており、データの受渡しのプロトコルは決められているが、そのデータは本来誰がどこまでコントロールすべきもので、どのようなデータに対して誰がどのような条件の下でアクセスすることができ、誰がそのデータの内容に介入することができるのか、データのアクセスや移転の履歴がどうなっているかといった点を把握したり、これを検証したりするメカニズムが存在していない。

こうした中で、データ・マネジメントの多くは、データを集中的に管理するプラットフォーム事業者に委ねられている現状にあり、そうしたプラットフォーム事業者を信頼できるかという問題に帰着している状況にある。

このように、巨大なプラットフォーム事業者等により中央集権的にデータが管理・利用されている中で、データがどのように使われるかは利用者からみてブラックボックスとなっており、これらの事業者への信頼が成り立たない場合には、そのことが、「信頼」（トラスト）の欠如をもたらすことになる。そして、信頼（トラスト）が欠如したままでは、パーソナルデータの利活用への懸念が高まり、事業者間のデータ連携の足かせとなっていくおそれがあると指摘されている。

また、こうした状態に対し、法律や契約だけでは信頼の担保には限界があり、データの公正な

取扱いのガバナンスを技術も含めた組合せによって担保することが求められている。

○　以上のような問題意識から提起されたのが“Trusted Web”であり、「中期展望レポート」では、“Trusted Web”が目指す方向性として、「データへのアクセスのコントロールを、それが本来帰属すべき個人・法人等が行い、データの活用から生じる価値をマネージできる仕組み」が示され、将来的に、現在のインターネット構造の上に「データ・ガバナンス」のレイヤーを付加し、データ社会における「信頼」を再構築するものとして、提起された。
　これは、G20 大阪サミット 2019 の首脳宣言に盛り込まれた Data Free Flow with Trust(DFFT：信頼性のある自由なデータ流通)の具現化にもつながるものである。

○　この「中期展望レポート」で掲げられた“Trusted Web”の構想を具現化するため、2020 年 10 月に、産業界、学術界の専門家からなる「Trusted Web 推進協議会」が立ち上げられ、その下に設置されたタスクフォースとともに精力的に検討を進めてきた。
　本推進協議会においては、デジタル市場という視点に限らず、広くデジタル社会における Trust を構築するという視点から、デジタル社会の一つの基盤となるインターネットやウェブの在り方について議論を行ってきた。

○　本検討は、まだ緒に就いたばかりであり、今後、更なる検討を進めていくことが必要であるが、本検討を進め、実現を目指すに当たっては、内外の様々な関係者とともに、議論し、共に構想を練り、実行に移していくことが不可欠である。
　かかる観点から、本ホワイトペーパーは、これまでの検討の結果を踏まえ、内外の様々な関係者との問題意識の共有を図り、今後、協力・連携を進めていくためのたたき台として取りまとめたものである。

2. 直面している課題とその原因

(1) 直面している課題（ペインポイント）

前述のとおり、社会全体のデジタル化が急速に進み、サイバーとフィジカルの融合が進む中で、様々な課題（ペインポイント）が顕在化してきている。
その主なものとして、例えば、以下のようなものが挙げられる。

①流れるデータに対する懸念

○　個人をはじめ、様々な主体が広く世界に情報発信し、コミュニケーションをとることが可能になった一方で、fake news やエコーチェンバー効果などにより言論空間に歪みが生じる問題が顕在化している。データを受け取る側にとっては、目に触れるデータがバイアスのかかった形で恣意的に選別されて提示されるなど、判断がコントロールされかねない状況にある。そのことが社会に混乱や分断を生み、さらには民主主義基盤を揺るがすインパクトにまでなってきている。

○　また、そうした問題への対応の在り方について、プラットフォーム事業者が担うのか、国家の関与がどうあるべきかなど、答えが見いだされていない状況にある。

○　今後、サイバーとフィジカルとの融合が様々な分野で進展していく中で、都市交通などの社会システムやヘルスケアなどを含む機器制御等において、身体・財産、社会全体が虚偽のデータによってフィジカルにも不当に誘導され、社会が混乱するなどの思いがけない悪影響を受けることも懸念される。

②プライバシーに対する懸念

○　ユーザーから収集されたデータは、事業者において集約・統合され、かつ、その処理がブラックボックス化することによって、そのデータの利用を通じて、深刻なプライバシー上の懸念を生んでいる。特に、プラットフォーム事業者等により、個人にほぼ固定的に付与される識別子（Identifier）で名寄せされ、様々なデータが統合されるが、ユーザー側としては、気づかぬうちに、また、同意があっても実質的に理解しているかには懸念がある中で、行われてしまっている状況にある。
今後、バイタル・データの活用拡大などが進むことが想定される中で、ユーザーが意識する前の段階ですらリコメンドが行われるなど、人々の判断自体が左右される状況となり、プライバシー問題が更に先鋭化する懸念もある。

③プライバシー保護と公益とのバランス

○　COVID-19 の患者の発生状況や行動履歴の活用などにおいて、プライバシー保護と全体の公益確保（感染拡大防止）のバランスが国際的に議論されてきている。
全体の公益確保を重視しすぎると国家監視の懸念に転嫁しかねないが、こうした議論がより円滑に行われていくためには、データのやり取りにおける合意形成プロセスの中で公益目的が具体的に織り込まれ明確な合意が十分になされているかや、その後、利用目的どおりに利用されたかについての検証が担保されているかといった観点などが重要となってくると考えられる。

④サイロ化した産業データが活用しきれない

○　サプライチェーン等でサイロ化された産業データを関係者間で共有し、新たな価値を生む取組はこれまで十分に成功していない。その背景には、コストの問題やビジネスモデルの問題など様々なものが考えられるが、そのベースとして、自らのデータへのアクセスをどこまでコントロールできるか、共有するプレイヤーのデータの取扱いをどこまで信頼できるのかといった問題も懸念の一つとして考えられる。

⑤勝者総取りなどによるエコシステムのサステナビリティへの懸念

○　デジタル・ビジネスにおいては、強い顧客接点を持つことにより、ネットワーク効果でユーザーをロックインし、顧客接点を活かしてデータを収集して AI 等で分析し、顧客に新たな価値を提供するモデルが力を持つことになる。この際、強力なネットワーク効果から、勝者総取りになる傾向が強く、その結果、多様なイノベーションが妨げられる懸念がある。

○　さらには、そうした勝者となった少数の巨大なプラットフォーム事業者が、人々の生活や企業の経済活動のインフラとなるに従い、民主主義等のプロセスを経ていない巨大プラットフォーム事業者の判断が、社会や経済のありように大きな影響を及ぼすまでに至ってきている。

社会システム的には、いわゆる単一障害点となり、脆弱かつ深刻なダメージを与えるポイントになり得、サステナビリティの観点から懸念がある。最近のあるプラットフォーム事業者のシステム障害は、世界中で大規模な混乱が起こるリスクを想起させた。

⑥ガバナンスの機能不全

○　社会全体のデジタル化が進む一方で、デジタルでの意思決定のプロセスがプログラムのコード上で自動処理され、かつ、それが AI 等の活用とあいまってブラックボックスとなってしまっている結果、それが当事者の意思決定を正しく反映したものなのかも含め、どのようなプロセスやルールにより処理が行われたのか外部から検証することが困難となっている。このため、政府による法制度の執行やステークホルダーによる監査など、社会システム全体を機能させるためのガバナンスを効かせることが困難になってきている。

○　また、デジタル上のコミュニケーションは人々の生活に大きなメリットをもたらす一方で、集団行動による誹謗中傷など、フィジカルの領域では想定しなかったような動きにつながる事象も生じており、これまでの規律のあり方が機能しないケースも出てきている。

(2) ペインポイントをもたらしている原因・背景

社会全体のデジタル化が進む中で顕在化してきている以上のようなペインポイントをもたらしている原因、背景は何だったのか。特に、我々が議論の対象とするインターネットやウェブにフォーカスしながら以下で考察する。

①インターネットとウェブの成り立ち

○　インターネットとウェブの成り立ちに立ち返れば、インターネットという基盤が生まれ、その上で、当初からグローバルに共通なものとして設計され、情報を自由に広げるという発

想でウェブが誕生した。
そこでは、技術が標準化され、その技術はオープンに皆が自由に使うことのできるものとして発展していった。これにより、技術の標準化に乗れば、ブラウザで閲覧でき、ハイパーリンクを利用して飛ぶだけで情報にアクセスできる世界がもたらされた。

そうした技術的な自由の上で、様々なサービスが生み出されるようになった。特に、人々が欲しい情報がどこにあるかをハイパーリンクによって示す検索サービスが登場し、その上で広告モデルが誕生してハイパーリンクのつながりを市場的価値に変えることに成功した。このモデルは、サイバー空間の「無償」サービスモデルを支える一方、人々をなるべく長時間惹きつけることに注力するアテンション・エコノミーとして発展していくこととなった。

○　そうした中で、ネットワーク効果を活かしたプラットフォーム・ビジネスが発展し、ユーザーをロックインすることで、その力を増していくこととなった。強い顧客接点を通じて人々の趣味嗜好を捉えるための大量のデータ収集・統合が進み、プラットフォーム事業者にデータが集中していくこととなった。

すなわち、サイバー空間では、データを収集・統合・分析することでアテンションを高めて成長期待を上げ、それが更なる投資を呼び込む循環を作り出し、成長したプラットフォーム事業者がそれぞれの領域の中で“Trust”を作り出す役割を担うこととなった。
このビジネスモデルは、AI 等の技術ともあいまって、データを活用して新しい価値を生み出し、社会に多大なベネフィットを提供してきた。

②生じている様々な歪み

しかしながら、その過程において、様々な歪みが生じてきている。

○　まず、アテンション・エコノミーで優位に立つべく、ユーザーの趣味嗜好を探り、ユーザーに心地よい情報を届けるため、ユーザーのデータを収集・統合・分析する動きが、技術の発展とともに先鋭化していった。こうしたデータの収集は、ユーザーが気づかぬうちに、また、同意があってもユーザーが実質的に理解しているかには懸念がある中で進められていった。

また、ネットワーク効果等によって、プラットフォーム事業者が顧客接点を抑え、プラットフォームを利用する事業者（ビジネス・ユーザー）はそれに依存せざるを得ない状況となっている。こうした中で、プラットフォーム事業者がデータを活用して価値を生み出す過程において、ビジネス・ユーザーのデータがプラットフォーム事業者によって不当に利用されていないかといった懸念も生まれている。

加えて、外部からの検証が困難な AI の活用が、ブラックボックスの度合いを更に強めている。AI によりプロファイルされ、アカウントなどが削除されることなどによって、場合によっては、差別やデジタル難民が生まれることにつながりかねないリスクをはらんでいる。
しかしながら、そうした問題が発生しても、検証困難であることから外部から原因を追究することも難しく、また、AI を利用する事業者側も営業秘密として開示することに懸念を有する中で、ともすると、アルゴリズムで自動処理しているので仕方ないとされてしまいかねない状況にある。

これらの問題の背景として、プラットフォーム事業者側においても近年努力がなされてい

るものの、引き続き、ユーザー側が自らのデータへのアクセスを実効性ある形でコントロールできる仕組みが十分に整えられていないことが挙げられる。加えて、双方の意思を反映した合意形成が行われ、その後の履行状況を検証する仕組みがないことが、この問題の解決をより困難にしていると考えられる。

○　また、人々をつなぎ、自由に情報をやり取りすることができ、人々の英知を結集するとの目的で設計されたウェブの空間において、悪意の入り込む隙があった。これが悪質な情報やフェイクニュースの氾濫を生むことになり、ユーザー間でのやり取りが短期間で急速に拡大するような事態も起きているが、それに対して、ネットの自由、表現の自由もあり、多くのプラットフォーム事業者は、しばらくの間、そうした事態に介入することについて抑制的な対応をとった。
　この点については、投資家に対するリターンというビジネスとしてのインセンティブから、アテンション・エコノミーとその下での広告モデルにおける争いの中で、ともすれば、より刺激的でアクセスを生みやすいコンテンツの方がリターンを生みやすいというインセンティブ構造からくる歪みのおそれも懸念されている。

　現在においては、SNS 等で共有されるコンテンツに対してプラットフォーム事業者が一定の介入を行うケースがみられるが、不適切な情報の削除を行っていない、あるいは情報の削除が一方的に行われている、との両面からの批判がなされ、一民間企業であるプラットフォーム事業者が人々が触れる情報の是非の判断を左右する力を持ってよいのかとの議論に至っている。

　ここでの問題の一つは、SNS 等で流れる情報について、元々の情報がどの程度信頼できるソースから発信されたものか、それがどのような経路をたどって、どの程度信頼できる介在者がどのように加工したのかなどが不透明であり、現状では一部のプラットフォーム事業者が付すラベリングに頼らざるを得ない点にあると考えられる。すなわち、本来は情報の信頼性について多角的に検証でき、判断ができることが必要である。こうした情報の信頼性の検証は、機器制御等に用いられるデータの真正性を確保する際にも同様に重要となる。

○　サイバー空間においては、現実社会と比較すると、匿名性が強い状況にある。こうした中で、社会的規範を破ることについてのペナルティが十分に機能せず、「やった者勝ち」になりがちであることも歪みの要因の一つである。例えば、SNS 上においては、多数の誹謗中傷の投稿が行われ、それが人格を深く傷つけ、社会問題となる事案も生まれている。

　これについては、本質的には、匿名性の問題というよりも、デジタル上の行き過ぎた行為に対し、フィジカル空間では機能しているはずの社会規範によるガバナンスが実効的となっていないことに起因する問題であると考えられる。

　さらに、こうしたインターネットとウェブの空間において、政府による介入は、監視社会にならないよう抑制的であるべきだが、他方で、あくまでも民主的なプロセスを踏まえることを前提とした上で、現状において、ステークホルダーの一つとして、法制度の整備や執行を担う役割としての政府の位置づけがこれまで曖昧に過ぎるのではないかという見方もある。
　これらの問題については、インターネットとウェブにおいて、政府も含めたマルチステークホルダーによるガバナンスが十分に機能していない点が背景の一つにあると考えられる。

○　もちろん、これまでインターネットやウェブにおいては、電子署名、タイムスタンプ、発行元の組織を示す e シール、サーバ証明書、「電子書留」としての e デリバリーなど、

CA(Certification Authority：認証局)が公開鍵証明書を発行し、信頼性を高める仕組みが既に存在しており、大きな役割を果たしてきている。
　また、前述のとおり、プラットフォーム事業者がそれぞれのサービス領域内での ID 認証、データ保護、ポジティブリスト/ネガティブリストの策定と執行などの機能を果たしている。

　他方、信頼の源泉が、電子証明書を発行する CA やドメイン名と IP アドレスの対応関係を管理する DNS(Domain Name System)などの特定の組織に集中していることから、単一障害点の問題が生じる懸念がある。さらに、データの出し手と受け手が事前に一定の関係性を構築していることが前提となることから、デジタル化が進展すればするほど生じてくる、関係性が何ら構築されていない不知の者同士のやり取りの場合の信頼を高めることには制約がある。

○　以上でみてきたように、これらの歪みについては、これらに対応する仕組みがインターネットとウェブに存在しなかったことが問題の本質と考えられる。
　その意味で、これらの問題は、必ずしもプラットフォーム事業者に帰責すべきものではなく、プラットフォーム事業者は、こうした課題を抱えたインターネットとウェブの上で、様々な便益をもたらす一方で、これらの問題への対応に苦慮してきた立場であったとも言える。

③今後における懸念と方向性

○　以上、みてきたように、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拡大し、広く情報へのアクセスを可能としたが、他方で、その上で動くアプリケーションでは、様々な歪みが生まれている。
　そして、こうした歪みを抱えたままのこれまでのデジタル空間のパラダイムでは、おそらく、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できないのではないか。こうした状態のまま、サイバーとフィジカルの融合が更に進み、多くの社会活動のデジタル化が進行すれば、これまでの歪みが更に増幅することとなるのではないか。

○　こうした中では、これまでの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、そこに上から重ね合わせるオーバーレイのアプローチで、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必要があるのではないか。

　すなわち、これまでのインターネットやウェブの空間においてはコードや市場によるガバナンスが中心となり、フィジカルで人々が社会活動を行う上で前提となってきた社会規範によるガバナンスが十分に機能していなかったと考えられる。今後、サイバーとフィジカルが融合していく中では、こうした社会規範によるガバナンスが有効となるよう基礎的な機能やそれを継続的に改善し運用する仕組みを再構築していくことが求められるのではないか。

○　その際には、これまでみてきたペインポイント、その原因となっている歪みを解消すべく、
- 自らがデータへのアクセスをコントロールできること
- アクセス数ではなく、信頼できる情報が価値を持ち、ユーザーの選択によりそうした情報に触れることができること
- より透明な形で合意形成を行い、その過程・履行状況を検証できること
- 多様な主体がガバナンスに関与すること

によって、データをやり取りしつつ、それを通じて価値を創出しながら社会活動を行ってい

くことができるよう、これらを具現化する仕組みを、社会の基盤となるインターネットとウェブに付加していくことが求められているのではないか。

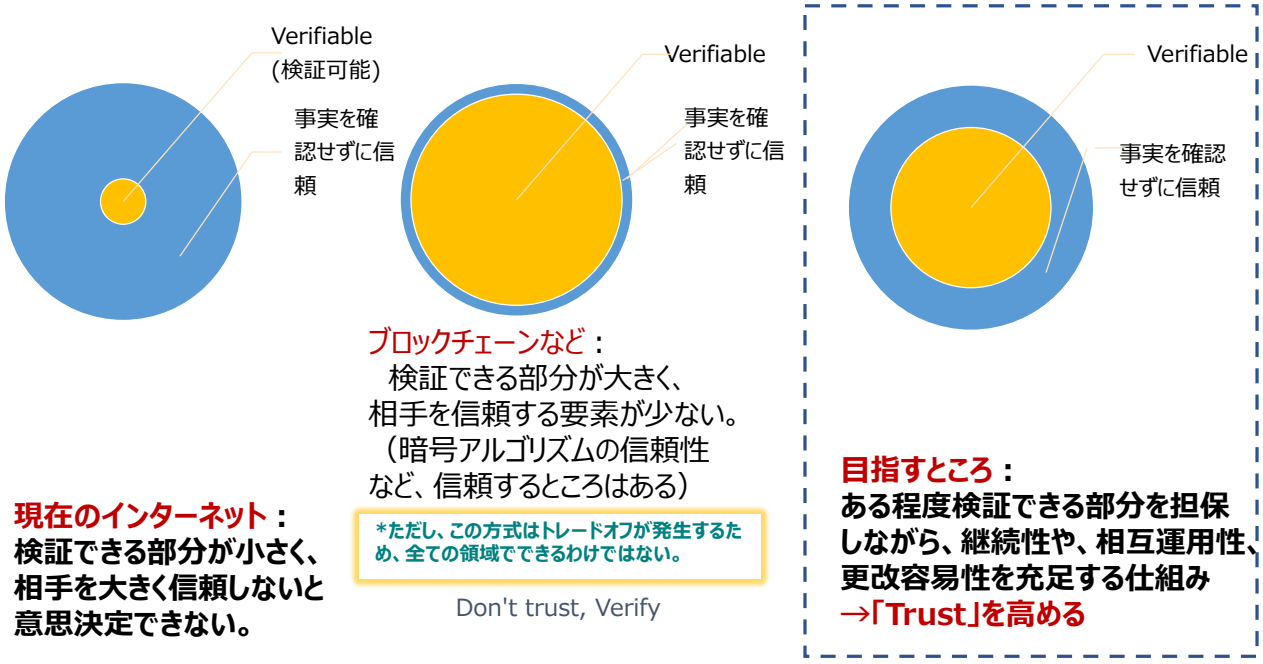
○　その鍵となるものが Trust である。ここでは、Trust を、「事実の確認をしない状態で、相手先が期待したとおりに振る舞うと信じる度合い」と定義する。その場合、Trust は、全てを確認するコストを引き下げ、システム全体のリスクを関係者で分担することに意義がある。利用者は Trust 維持コストと問題発生時のリスク（被害の程度×蓋然性）のバランスで Trust するか否かを判断することになる。

○　現在のインターネットやウェブにおけるこれまでの Trust の仕組みでは、不知の者同士の信頼を確保するには制約があるなど、確認・検証（verify）できる領域が狭くなっており、事実を確認せずに、仲介するプラットフォーム事業者等を信頼せざるを得なくなっている。

しかしながら、プラットフォーム事業者等がその領域内において実現している Trust は、サイロ化され、ブラックボックスとなっているために外部から検証が困難であり、単一障害点となるリスクも抱えており、デジタル社会の Trust としては必ずしも十分なものとはいえなくなってきている。こうした中で、プラットフォーム事業者の Trust への過度な依存が上述の様々な歪みを生み出している。

これに対し、デジタル技術の進展によって、相手が不知の者であっても過程や結果の確認・検証が可能となってきており、リスクを少なくして取引することができるようになっている。これにより、従来事実を確認せずに信頼せざるを得なかった領域を縮小し、確認・検証できる領域との最適な組合せを再構築することが可能となっている。

仕組みによりVerifiable(検証可能)な部分が変わる



○　以上を踏まえれば、データの「出し手」が相手に開示するデータをコントロールすることを可能にし、データのやり取りにおける条件設定に関する合意の仕組みも取り入れつつ、相

手から提供されるデータや合意の履行について検証(verify)できる領域を拡大し、これまで事実を確認せずに信頼していた領域を縮小できる新しいTrustの枠組みを構築することにより、相手先が期待したとおりに振る舞うと信じる度合い、すなわち、Trustを高めることを目指すこととしてはどうか。

3. Trusted Web が目指すべき方向性

(1) 目指すべき方向性

○　以上を踏まえ、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。

○　Trusted Web が実現を目指す Trust の仕組みは、特定サービスに依存せず、
・相手に開示するデータへのアクセスのコントロールを可能とし、
・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つつ、
・検証(verify)できる領域を拡大し、これまで事実を確認せずに信頼していた領域を縮小することにより、Trust(相手先が期待したとおりに振る舞うと信じる度合い)を高めていくことを目指すものである。

○　この際、既存のインターネットの上に、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。これにより、インターネットを通信基盤から、自律分散協調型の通信・情報基盤へと進化させていく。

○　具体的には、データの送受における出し手(Sender)と受け手(Receiver)の役割等において、Trusted Web が実現を目指す Trust の仕組みは以下のとおりとなる。

①データの出し手(Sender)
個人・法人が、データの受け手を確認した上で、合意に基づき、開示するデータをコントロールし、データの活用から生じる価値をマネージできること

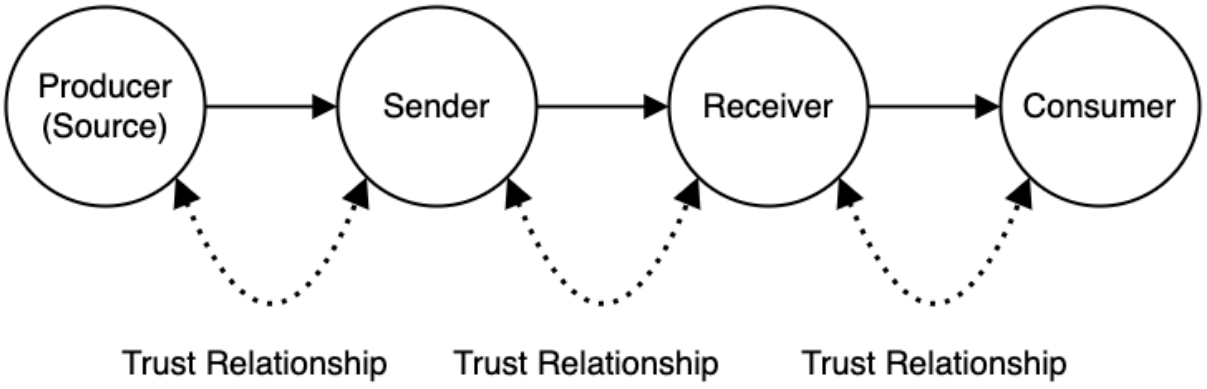
②データの受け手(Receiver)
データの出し手ややりとりするデータを確認することができ、合意に基づき、価値交換が履行されること

③データのやり取りのスキーム
検証可能なデータに基づき、送り手と受け手の間で相互の意思を反映した合意形成やその後の状況に応じた変更が可能であり、その過程や結果を検証することができること

*やり取り:　単一のシステム内のプロセス、ネットワーク化されたシステム同士のトランザクション、システムと人間のインターフェイスを含む。

④関係するステークホルダー
関係するステークホルダーの役割を明確にし、それぞれがその役割に沿って、全体の系としてトラストに関わる機能を維持・管理すること

(注 1) データは、狭義の属性・履歴、ブログ等のメディアコンテンツ、計測されたデータ等、データ主体に関連づけられるものを広く含む。
(注 2)　上記は二者間のコミュニケーションに着目したものであるが、一つのコミュニケーションにおいて出し手が受け手となり、受け手が出し手となるなど双方向性のある性質のものである。また、1 vs 1 に限るものではなく、N vs N にも適用し得るものである。
(注 3)　基本的に出し手(Sender)と受け手(Receiver)の間の信頼関係モデルで考えるが、出し手が持つ属性(データ) を生成した Producer(Source)がいる場合、この関係においては出し手が受け手となる。また、受け手が更に属性(データ)を移転させる場合には、受け手は出し手の地位に立つ。



(2) 必要な原則

Trusted Web の設計・運用などに当たって考慮されるべき原則を、以下のとおり整理する。

【支える仕組み】

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。

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。

③オープンネスと透明性
アーキテクチャー設計、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
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
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
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

既存のインターネットアーキテクチャーを基礎として、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。既存のトラスト手段とのフェデレーションも考慮すること。

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ーであること。

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。

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ーラブルであること。

4. Trusted Web のアーキテクチャーを構成する主な機能・ガバナンス

(1) 基本的な考え方

○ 既存のインターネットの上に、3.で述べた基本的方向性を実現するための機能を付加する。

○ 不知の者同士の P2P(peer to peer。コンピューター同士が対等に通信を行うこと)も前提にした場合に、双方で属性を検証して合意形成を行い、データのやりとりを行う枠組みとして、「認証(Authentication)」を拡張した概念で整理する。

(注 1)Authentication には、entity authentication(主体の認証)、message authentication(内容の認証)、attribute authentication(属性の認証)を含む。
(注 2)情報の出し手(Sender)、受け手(Receiver)のモデルを考えた場合に、「Sender の持つ属性の確認」、「Receiver の持つ属性の確認」、「Sender が Receiver に送る情報の属性の確認」、「Sender が Receiver に送る情報の取扱いに関する合意」が「認証」の目的になる。

○ 基本的な機能として、(2)の①～④が考えられ、これらはそれぞれ分離して運用することが可能なものと考えられる。ただし、これらの機能については、様々なユースケースベースでテストしながら、引き続き精査していく必要がある。これら機能の運用に当たってのガバナンスは(3)のとおり整理している。

(2) 必要となる機能要件

○ Trust を実現するためには、データのやり取りをする相手を確認する必要があり、デジタル上で個人・法人等の属性が検証されることが必要となるが、属性を紐づけるための識別子を発行し、管理する機能として①の Identifier 管理機能が必要となる。

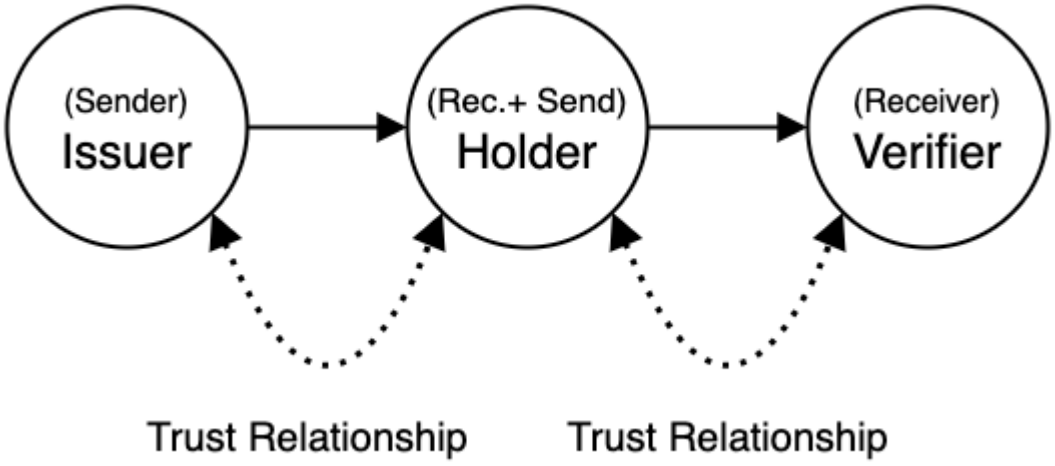
ここでいう識別子とは、固定的な識別子ではなく、自らが必要に応じて複数発行することができ、各識別子に対して、必要な属性情報を紐づけることができる。多数発行する識別子を使い分けることにより、プライバシー上、個人が特定されるリスクを回避することができ

る。

○　次に、上記のとおり、個人・法人等の「出し手」が識別子を発行し、それに対して「発行者」を含む第三者によって「お墨付き」等を与えられた属性(データ)が結び付けられて管理されることによって、必要に応じてそうした属性(データ)をコントロールしながら開示することが可能となる。発行者を含む第三者からの信頼の構築に資する属性(データ)の管理・開示の仕組みとして、②の Trustable Communication 機能が必要となる。

この機能は、これまで W3C(World Wide Web Consortium)で議論されてきている Verifiable Credentials(VC)やその他の手段の応用が可能と考えられるが、これらが想定している発行者による個人の資格の証明確認等のレベルのみならず、データの「出し手」に対する第三者のレビュー結果等も含み得ることとしている。

その場合にはレビューを行った当該第三者に関する属性を更に検証することにより、その Trust 自体を「受け手」が評価することを可能とするものである。これにより、送られるメッセージの内容の正しさを証明することは難しいとしても、メッセージの「出し手」に対するレビュー結果等で判断することにより、メッセージの内容の正しさを推定し得るものである。



(注1)　受け手が相手の属性を検証する立場にある場合には、受け手は Verifiable Credentials の場合に照らすと、確認する者(verifier)でもあり、Sender と Receiver の関係に分解できる。

(注 2)　Trustable Communication 機能においては、それ以上確認する必要がないとされるトラストアンカーに加え、信頼できる発行者やレビューを行う第三者（以下「発行者等」という。）のリスト又は発行者等自体の信頼性を評価する更なる評価の仕組み等も必要となると考えられる。

○　「出し手」と「受け手」との間でデータのやり取りをする際に、双方で様々な条件設定をして合意を行うプロセスと結果を管理する機能が③Dynamic Consent 機能である。

デジタルにおいては、本来、相手に応じて柔軟にカスタマイズした合意形成が可能であるにもかかわらず、現状のサービスでは、一律の内容の規約を承認するか否かの選択肢しかないことがほとんどであるが、その合意形成を動的に行う機能を目指すものである。

すなわち、デジタル社会における社会的活動の中で、当事者間の合意形成の際の意思を可能な限り同期させ、仮に齟齬があった場合には動的に修正できることを可能にするものであ

る。

○　合意形成のプロセスや合意の履行をモニタリングし、適正であるか検証するための機能が、④Trace 機能である。

これは、合意形成後も検証して相互の意思を同期させる意味合いに加え、特にデータ移転後も「受け手」や第三者に移転した場合にあっても合意条件に則した利用が行われているか監視し、必要に応じて措置を採ることができることにより、データを「受け手」に渡して以降は完全なブラックボックスになるという懸念を払拭する機能である。

【各機能】

①Identifier 管理機能

○　識別子を特定のサービスに依拠せず、各主体が発行でき、それを様々な属性(データ)と紐づけることができる。

○　多数の Identifier をその都度発行することでプライバシー等の特定リスクを下げることが可能である。

②Trustable Communication 機能

○　識別子とそれに紐づく属性(データ)の組合せを各主体が管理していて、属性(データ)の発行者に都度直接照会することなく、相互に相手の属性(データ)を検証することが可能な仕組み。

○　識別子と紐づいた属性(データ)を管理し、開示の範囲や利用期間等を選択して開示できる。

○　出し手や属性（データ)の発行者等に対し、トラストアンカーによる属性、第三者によるレビュー結果、ポジティブリスト/ネガティブリスト等の属性が書き込まれ、それを受け手が参照することによって、出し手から送信される属性(データ)の Trust の度合いを確認することができる。

③Dynamic Consent 機能

○　合意形成の際に、やりとりする属性（データ）の取扱いについてのきめ細かな条件設定が可能。双方の条件設定が一致すると合意が成立する。

(注)条件設定の項目:属性確認の範囲、選択的開示、保存方法、利用期間、利用目的・方法など

○　各主体の監督の下、意思決定を代理して執行するエージェントを利用することができる。(ヒト等の主体あるいはプログラムを含む。)

○　その際、相手の属性等の条件を設定して絞り込むこと(フィルタリング)ができ、悪質な相手(及びその属性(データ))をブロックできる。

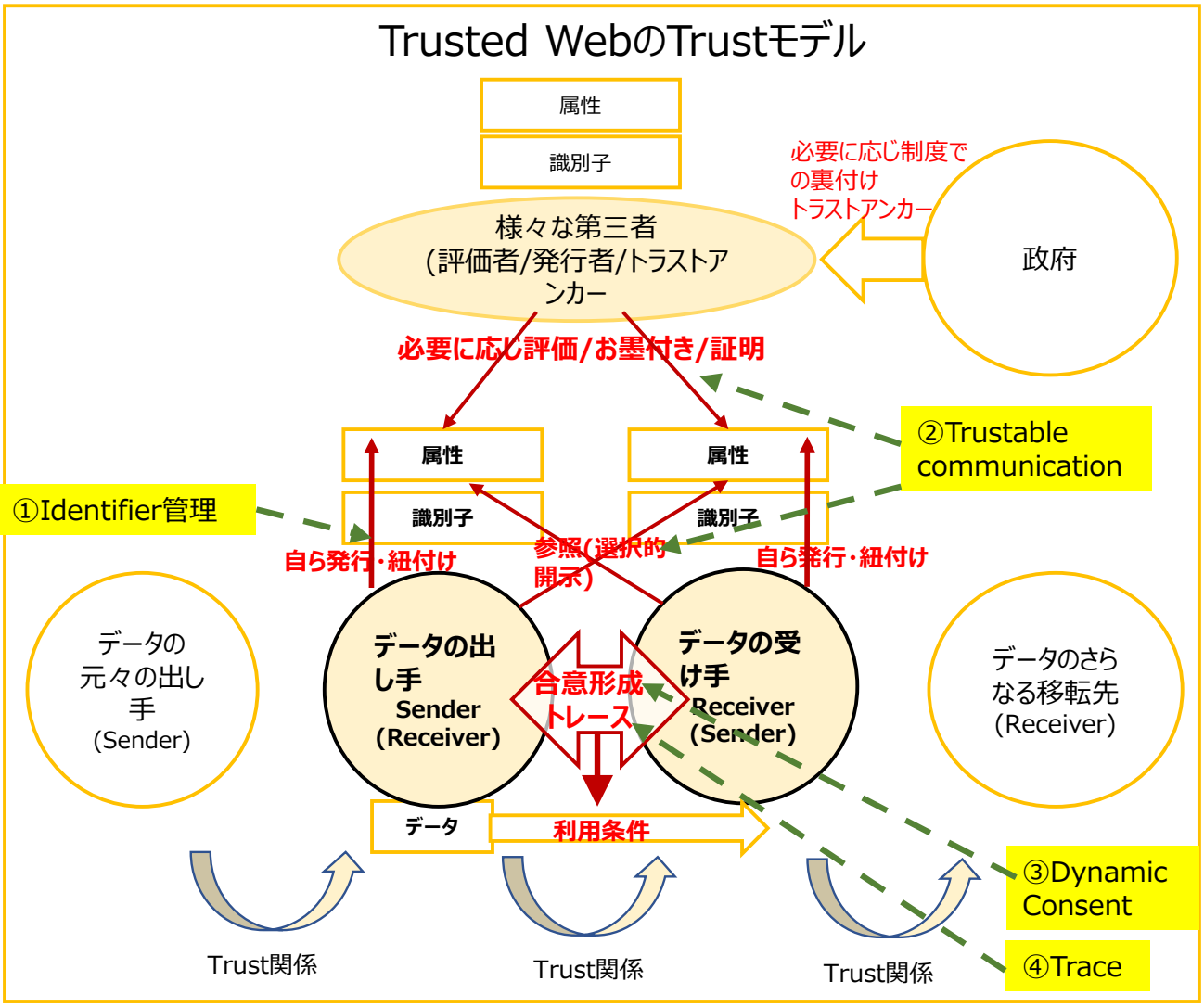
④Trace 機能

○ 合意の確認（プロセスごとの意思確認）ができる。

○ 合意の際の選択により、合意形成後にその条件設定が履行されているか否かについて、検証に必要十分な情報を取捨選択して記録することが可能な状態となっており（トレース）、検証ができる。

○ 条件が履行されていない場合には、必要に応じて合意の取消し等が可能である。

○ 属性（データ）について、当事者間のみならず、第三者に「移転」した場合にも、当初の条件設定（履行済みのものを除く。）を付随してトレースできることで検証ができ、条件設定に基づき合意の取消し等のコントロールが可能な仕組みである。



(3) ガバナンス

○　「デジタル社会」の Trust を中期的に構築していくためには、機能(コード)としての Trust と、運用も含めた社会システム全体としての Trust を峻別した上で、その組合せを考える必要がある。

○　これまでのインターネットとウェブは、当初からグローバルに共通のものとして設計され、技術を標準化し、情報を自由に拡大していくことが中心のアプローチであった。しかしながら、2.でみたとおり、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できる仕組みになっていない。
　このため、Trusted Web においては、機能(技術の標準化)のみならず、ガバナンスと運用を追加していく必要がある。

○ あるべきガバナンスの方向性としては以下のとおり。

①マルチステークホルダーによるガバナンス

○ 属性に対して Trust を裏付けする様々な経路及びその連鎖について、様々なステークホルダーが分散協業してそれを支え、系全体としての Trust を形成していく。

○ また、様々なステークホルダーが、ルールや共有されたゴールに基づき、定期的な対話等を通じて合意形成を行うことにより、ルールを変える際のルールの整備も含め、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。

○ ステークホルダーには、従来のエンジニア、プラットフォーム事業者のみならず、サービス提供事業者、インフラ提供事業者、大学研究機関、利用者、消費者保護団体、シビルソサイエティ、法曹界、政府など様々なものを含む。

②政府の役割の再定義

○ 言論の自由や営業の自由をはじめとした個人や企業の権利・利益に大きく干渉したり、監視したりするのではなく、最終的にそれ以上の確認は必要ないこととされるトラストアンカー(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)やデジタル上の社会活動を裏付ける法制度の整備とそれを執行する役割に限定した上で、ステークホルダーの一人として位置づける。

○ 前述の４つの機能が安心感をもってユーザーに利用されるようになるためには、トラストアンカーとしての政府の役割も重要である。Trust を担保するための制度を整備、執行し、ユーザーが自由に結び付けられるよう、個人や法人等の証明基盤を整えて、つなげられるようにすることが必要である。

○ 法制度を整備・執行する役割としては、例えば、法制度上のグレーゾーンがあって踏み出せないような場合に明確性を高めるなど、法的安定性を高めることが重要であり、フィードバックループを回し、市民社会や開発者と協働で、ガバナンスに関与する。

③透明性、トレース、監査できること

○ ①、②に関して鍵となるのが透明性の確保であり、AI によるアルゴリズムの結果も含め、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、悪意のプレイヤーによる系全体の Trust の棄損を防ぐ。

④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

○ 上記のマルチステークホルダープロセスを採用することによって、ステークホルダーにルールメイキングに参加できるというインセンティブを与えられると考えられる。

○ 一方、長期にわたり公共財のような性格を持つ基盤について、そのコストを誰がどのように負担するのかという問題がある。そうした基盤に貢献するエンジニアや Trust を付与する機関、事業者等に対しては、公共財に携わる公共的役割を担う者（「デジタル公務員」）として、何らかのインセンティブ付けをすることなどについて、今後検討していく必要がある。

(4) 引き続き検討を深めていくべき諸課題

○ 本ペーパーにおいては以上のような機能やガバナンスのたたき台を示しているが、今後、その具体的な在り方の検討を深めていく上で様々な課題があると考えている。

○ 例えば、Trustable Communication 機能におけるレビューを行う第三者を取り込む仕組みの在り方、Dynamic Consent 機能の具体的な設計、Trace 機能の在り方とプライバシー保護の在り方の整理、マルチステークホルダーによるガバナンスの在り方などが考えられる。
また、Trustable Communication 機能においては、機能があってもそれがどう運用されるかによって、ユーザーがそれを信用して利用するかが大きく変わってくるため、そのような観点からの運用面の在り方の検討も重要である。
Dynamic Consent 機能については、個人が悪意ある者の犠牲となることのないよう、消費者保護の観点を如何に担保するかも重要な課題である。
さらに、分散的な Trust の仕組みとした場合に重要となる相互運用可能なフレームワークの在り方についても検討が必要である。

○ これらの課題について、広くグローバルなコミュニティとの意見交換をしながら、検討の深掘りを行っていく必要がある。
なお、今後の実装を進めていく中で、全体としての実現可能性を考慮し、非デジタルの領域とどのように共存・協調していくかについても留意する必要がある。

5. Trusted Webにより創出が期待される経済的価値及びユースケース分析例

(1) 創出が期待される経済的価値

Trusted Webが実装され、Trustが高まることで、デジタル社会の様々な社会活動の基盤となる場合に、どのような経済的価値が生まれ得るかについて考察する。

○　第一に、「アプリケーション・レイヤー」での価値創出である。
流れるデータについて、その出し手に対する第三者のレビュー（あるいは当該第三者に対するレビュー等の信頼の連鎖も含む。）を検証できることから、当該データがどこまで信頼できるか推定することができ、その信頼の「重み付け」を可視化することによって、信頼できるデータが他との比較で優位性を持ち、価値を持つことが考えられる。例えば、ニュースも含めたコンテンツについては、アクセス数ではなく、コンテンツの担い手に対する第三者によるレビューが付されるなど信頼性の高いものが価値を持って評価されるなどの価値創出が期待できる。

また、デジタル上で、事前の関係性がない当事者間であっても、相手の属性を検証でき、データへのアクセスのコントロールも担保され、また合意形成プロセスが保証されて、そのトレースもできるようになれば、これまで協力関係がなかった人々や企業の間での協働が可能となる。これにより、社会全体としてこれまで難しかった属性やデータの開示・共有や様々な取引がグローバルに容易になることが期待される。

この際、安心してデータ等が取引できることと、データの信頼への評価が価値化されやすくなることとあいまって、例えば、商流やエネルギー消費等に伴うデータの流れと、データの流れによって生み出される価値の流れが同期し、デジタル上で新しい価値交換を実現することが可能となる。

具体的には、これまで困難であったサプライチェーン間の取引データが必要に応じて開示・共有され、そうした取引データと連動してサプライヤーが新しいファイナンスサービスを受けることができるといったことや、サプライチェーンの各段階での環境負荷をより精緻にトレースすることにより、環境配慮に根ざした差別化とそれによる新たな価値提供を可能とすること等により、SDGsによる社会課題解決に貢献し、そうした活動に対する社会からの信頼も経済的価値に変えることができる可能性も考えられる。

○　第二に、「お墨付き」を与えるなどにより、マルチステークホルダーでの信頼のチェーンに参画し、その担い手となることによる「ミドル・レイヤー」での価値創出である。例えば、金融機関等が本人に関する何らかの属性を証明する、検査機関等が検査をすることによって対象の価値を高める、人材教育機関が教育講習をすることで受講者のスキルを高めること等について、デジタル上で評価され、確認できる仕組みができることによって、新しい経済的価値をデジタル上で生む可能性がある。
また、ユーザーにとっては、信頼を支える必要な要素が組み合わされて整合しており、それらが安定的に稼働しているかについての状態をチェックし、Trustのレベルが評価されることも重要であり、そうした役割を担うことも価値を生み出す可能性がある。

さらに、個人等からみると、これまでは様々な機関によりサイロ化して保有されていた自らの属性について、それを自らがコントロールしてアンバンドリングし、必要な範囲で切り出して利活用し、プライバシーを担保しながら価値を創出することができることを意味する。その際、例えば情報銀行のような組織が、個人等から関連する属性へのアクセスについ

て委任を受けることも考えられる。

○　第三に、識別子やそれによる属性管理、合意形成など、共通基盤である「インフラ・レイヤー」での価値創出である。
Trusted Web で掲げた 4 つの機能が意味することは、これまでそれぞれのプラットフォーム事業者などが個別に実装していた機能をアンバンドリングし、ベンチャー企業を含む様々な企業が開発・提供する可能性を開くことである。

現在の時点でも、世界的に、プライバシー保護のための識別子とそれによる属性管理、個人情報の同意を取得するためのプロセスを共通基盤サービスとして提供する事業者が出てきているが、こうした流れが加速化していく可能性がある。
利用企業側からみると、これらの機能の開発を外部化しつつロックインを避け、様々な機能を選択して組み合わせることで、それらを利用したサービスの提供が容易になることになる。

(2) ユースケース分析例

以下、具体的なユースケースを例にとって、Trusted Web の機能やガバナンスを実現したときに、解決が期待される効果を記載する。今後、様々なユースケースでの分析を行っていく予定である。
なお、あくまでも現時点で仮想的に検討したものであり、実装する場合の現時点での制約を十分に考慮しているわけではない。

①SNS 等におけるメディアコンテンツの流通

【ユースケース上の課題】

SNS 等におけるメディアコンテンツについて、
- 真偽不明のニュースが流通し、ユーザーによる再生産による被害拡大
- 広告モデルにも起因するフィルターバブル効果等、プライバシーの侵害リスクや個人の判断基盤となる情報のバイアス
- コンテンツの削除やアカウント停止についてのプラットフォームの関与の是非
- コンテンツの価値が評価されにくい構造の中でのパブリッシャーの経営基盤の脆弱化

【ステークホルダー例と代表的な利害関心】

○　ユーザー（視聴者・購読者）
関心のある情報を得たい/関心がなくとも多様な情報に触れたい/なるべく無料でコンテンツを見たい/本当に良いコンテンツには対価を支払ってもよい/発信情報の正確性、発信情報源の信頼性を担保したい/閲覧履歴等による過度のプロファイリングはやめてほしい/閲覧履歴等個人情報を悪用されたくない、コントロールしたい/煩わしい広告は見たくない

○　情報を拡散するユーザー
自分の好きなコンテンツを嗜好が近い仲間と共有したい/コンテンツを拡散して世の中に影響を与えたい/課金収入、広告収入を得たい/発信情報を改ざん・悪用されたくない/過度のプロファイリングはやめてほしい。個人情報を悪用されたくない

○　パブリッシャー/メディア企業/ライター/ブロガー

オリジナルな発信情報を多数の人に視聴・閲覧してほしい/課金収入、広告収入、著作権収入を得たい/発信情報を改ざん・悪用されたくない/個人情報を悪用されたくない

○ ネット広告事業者
広告の成約を増やして手数料収入を上げたい

○ プラットフォーム事業者
ユーザー、コンテンツ、広告主を増やしたい/ユーザー体験を向上させ、滞在時間を増やしたい/ユーザーのプロファイリングによりターゲティングの精度を高めたい/ユーザーのプライバシーを保護したい/ユーザーコンテンツに関する過度な責任を問われたくない/広告の成約を増やして手数料収入を上げたい/広告不正を排除したい

○ OS ベンダー/ブラウザ
識別子を発行して広告のエコシステムを維持したい/ユーザーのプライバシーを保護したい

○ データ事業者
SNS 等のデータを可能な限り多く収集してマーケティングデータとして分析して活用してほしい

○ 広告主
広告のコストパフォーマンスを上げたい/広告不正を排除したい/ブランドイメージを守りたい

○ 悪意を有する者
扇動してアクセス増による利益を得たい、あるいは相手を陥れたい/アドフラウド等の虚偽請求で不正な利益を得たい

【Trusted Web によって解決が期待されること】

○ ユーザーによる経路不明の情報の見極め
Identifier 管理機能によって、コンテンツの出し手の属性（更には必要に応じてオリジナルの発行者の属性まで)を受け手が検証することにより、経路の検証が容易となる（ただし、プライバシー上の保護は考慮される必要がある)。
これにより、ユーザーはコンテンツを閲覧する際に、より客観的な判断を行うことができる。ただし、集団効果による煽動自体を防ぐことはできない。

○ ユーザーによる多様な評価に基づく情報の見極め
Trustable Communication 機能によって、プラットフォーム以外の様々なステークホルダーがコンテンツの出し手に対してレビューを行い、それを参照することが可能になることで、より客観的な判断が可能となる。

○ 信頼性のある情報の価値を高める
データの出し手であるパブリッシャーに対し、第三者によるレビューが行われ、それを属性として参照できることから、パブリッシャーは、その信頼に応じ、コンテンツとしての価値を高められる可能性がある。

○ プライバシー保護の強化、広告取引の透明化、新しい価値評価モデル

Identifier 管理機能や合意形成機能により、ユーザーがデータへのアクセスのコントロールを高めることにより、プライバシー保護の強化が可能となる。

アドフラウド等については、Identifier 管理機能によって広告の経路を検証し、かつ、Trustable Communication 機能によって、経路上の参加者に対し第三者によるレビューの属性を付与することにより、信頼性の高い広告ネットワークの構築がより容易となると考えられる。

②感染症下のヒトの円滑な移動と感染防止

【ユースケース上の課題】

- COVID-19 等感染症下にある場合のヒトの円滑な移動と感染拡大防止
- グローバルな移動を伴う場合に提示が求められる、感染の有無等に関する検査結果等への信頼担保（他国の検査・ワクチン接種機関の信頼担保、検査結果の改ざん防止）
- プライバシーの保護

【ステークホルダー例と代表的な利害関心】

○ 海外渡航者
海外にスムーズに渡航したい(なるべくなら待機したくない)/データを目的外に利用されたくない

○ 入国管理局/航空事業者/ホテル/飲食店
海外渡航者が陰性であることを効率的に確認したい

○ 病院/医師/検査技師/検査機関
自らの検査結果が改ざんされずに正確に伝達されてほしい

○ OS 事業者
ユーザーのプライバシーを保護したい

○ 検査機関の認証・監査機関
検査結果が他国でも信頼されるようにしたい

○ 渡航先の国民
自国内の感染を抑えたい

○ 国際機関
グローバルで検査結果を効率的に確認できる仕組みをつくりたい/感染の拡大を抑止したい

○ 政府
国内外で検査結果を効率的に確認できる仕組みをつくりたい/必要な海外渡航を可能にしたい/個人情報の保護を担保したい

○ オフライン環境にある者/災害発生状況下にいる者
アナログでの利用や代理人への委任など、代替的な手段が準備されてほしい

○ 悪意を有する者

陰性の結果に改ざんして渡航したい/ずさんな検査で検査料収入を上げたい

【Trusted Web によって解決が期待されること】

○ 渡航者は円滑な移動が可能に
Identifier 管理機能と Trustable Communication 機能により、検査機関等の識別子とともに、検査(接種)証明書が発行され、それを入管等に提示することで、グローバルで円滑に証明できる。

○ 渡航者のプライバシーの保護
Identifier 管理機能や Trustable Communication 機能、Trace 機能により、検査結果等の陰性証明を提示するに当たって、必要最小限度の開示で足りるようコントロールができ、トレースすることにより利用目的以外での利用を検知することができる。

○ 検査機関の信頼性確認
Trustable Communication 機能により、国際機関等による検査機関に対する評価を検査機関の属性として検証でき、検査機関の信頼性が確認できる。

③人材の資格等の証明

【ユースケース上の課題】

- 進学・就職等の際に証明として提示する学歴・資格等について、経歴詐称等を防止するとともに、証明機関が廃止されても一定の利用を担保
- プロファイリング等の事業者によるプライバシー侵害からの保護

【ステークホルダー例と代表的な利害関心】

○ 資格等の証明を進学・就職等に利用する学生等の資格等保有者
自らの属性情報をコントロールしながら、成績・学位・就業証明・資格証明を信頼される情報として進学先・就職先に簡便に提示したい/目的以上にデータを渡したくない

○ 証明機関(大学・企業・資格発行機関)
オンラインの証明書発行で、資格保有者の利便性を向上させるとともに窓口コストを下げたい/外部に対するなりすましや改ざんを防ぎたい/属性に組み込まれることで資格等の価値を上げたい

○ 就職/転職時の採用企業
虚偽でないか改ざんしていないか確認したい

○ 採用・転職エージェント
人材の価値を的確に評価するために虚偽がない履歴・資格を把握したい/プロファイリング・ビッグデータ分析に基づき、マッチングの精度を上げたい/プライバーに対する配慮を示したい

○ 政府
進学・就職等の公正性の確保や、国家資格制度等の適切な運用・活用を確保したい

○　評価機関
　大学等を評価・監査し、大学等の信頼性を高めたい

○　国際機関・標準機関
　国際的に証明ができるようインターオペラビリティを確保したい

○　悪意のある者
　ずさんな方法あるいは虚偽の証明を行って手数料等をだまし取りたい/経歴詐称によって不正に入学・就職あるいは不正な経済的利益を上げたい

【Trusted Web によって解決が期待されること】

○　長期間にわたり、オンライン上で簡便に証明が可能に
　Identifier 管理機能や Trustable Communication 機能を利用して、大学等の証明機関が学歴・資格等について本人に証明書を発行することにより、簡便にオンライン上で証明することが可能になる。証明機関がなくなっても証明書を利用することができる。

○　プライバシー保護が容易に
　Identifier 管理機能や Trustable Communication 機能により、データの開示範囲や利用期間などデータへのアクセスに対するコントロールができる。

○　証明機関の信頼について評価が可能
　証明する機関の属性として、トラストアンカーあるいは第三者によるレビューが紐付けられ、それが参照できることにより、証明機関が発行した事実の確認だけでなく、当該機関の信頼性も含めて評価できる。

④車両等のライフサイクルにおける価値評価

【ユースケース上の課題】

- 車両のオーナーにとって、車両の正確な状態を反映した価値評価が得られていない。
- 車両に関するデータは関係事業者がそれぞれバラバラに保管している。このため、事業者が異なると、車両の正確な状態が把握できず、効果的な査定ができない。
- 車両のライフサイクルに関与する関係事業者が多く、事業者間での情報共有には限界。
- 中古車売買等で高く販売するために事故歴・修理歴などは隠すインセンティブが働きやすい。

【ステークホルダー例と代表的な利害関心】

○　自動車オーナー
　自ら車両の正確な状態を把握し、それを第三者に証明することで車両の価値を高く評価してもらいたい/自車の安全な状態をキープして適切に評価されたい/メンテナンス費用を安くしたい

○　中古販売事業者/オークション事業者/リース事業者/金融機関（銀行、保険）
　可能な限り正確かつ効率的に車の価値を査定したい/車の正確な状態に応じてリスクを判定して保険等の利率を変えたい

○ OEM メーカー(製造情報、コネクテッドカーからの通信によるセンサーによる機器の状態等)/部品製造業者/販売店(出荷情報)/整備点検事業者(点検結果)/中古販売事業者(査定結果)/修理事業者(修理情報)/保険事業者(事故情報)
提供したデータが改ざんされることなく正確に保存され、伝達されてほしい/何らか問題が起こったときの責任の所在が客観的に検証されてほしい

○ 取引スキーム提供事業者
可能な限り多くの関係者に参加してもらいたい

○ 政府
車が安全な状態で流通してほしい/トラストアンカーとして、正しいデータが流れるようにしたい

○ 購入者等
不当に高く評価された価格で購入したくない/事後的に瑕疵が判明して査定額が減少するといったリスクを負いたくない

○ 悪意を有する者
データを改ざんして、評価を不当に高めたい/不都合な状態は隠したい

【Trusted Web によって解決が期待されること】

○ 保有する車両の資産価値向上、重複検査の回避
関係事業者によるセンサー情報や修理査定履歴等のデータを Identifier 管理機能や Trustable Communication 機能によって、車両に対して時系列で記録し、非改ざん性を担保する。
国はトラストアンカーとして登録車の確認や車検等の制度整備・執行を通じて最終的な信頼を担保する。これらにより、車の正確な状態を把握でき、証明が可能となる。
これに基づき、車両のオーナーは、中古車販売や融資、保険等のファイナンスといったサービスで利益を受けるとともに、重複検査を避けることができる。

○ 修理等のサービスを幅広い事業者から選択できる
Identifier 管理機能や Trustable Communication 機能により、事業者間での属性の検証が容易となることで、これまで困難だった事業者間の協働が可能となる。これにより、車両オーナーは、修理等のサービスを受けるに当たり、幅広い事業者から選択できる。

○ 中古事業者・修理事業者等の信頼性を確認できる
Trustable Communication 機能により、第三者によるレビューなどの関係事業者の属性を検証することでき、関係事業者の信頼性を確認できる。

6. 実現に向けた道筋

○　Trusted Web を実現していくためには、グローバルなコミュニティと協働して進めていくことが不可欠である。既に、当協議会の問題意識に関連する動きとして、各種機関での DID/SSI プロジェクト、WWW の創始者などの有識者によるデータ主権の提唱、データ・コントロールを重視する様々なベンチャービジネス、ブロックチェーンを活用した様々なプロジェクトなどの動きが起こっている。

○　今回のホワイトペーパーで当協議会としての基本的考えをたたき台として明らかにしたが、検討すべき課題は多い。今後、グローバルな動きと連携し、残る課題について深掘りした検討を行いつつ、実現に向けた歩みを進める必要がある。
　その際、GitHub などにおいて、過程も含めてオープンかつ透明性を持たせながら検討を進めていく。

○　また、Trusted Web の実現に向けては、エンジニアや大学等研究教育機関、産業界などが主体となって、必要となる機能の実装やそれを利用したサービスを創出していくことが必要である。さらに、国際標準機関においても、Trusted Web に賛同するエンジニアなどが積極的に議論を展開するなどの取組が不可欠となってくる。
　このため、当協議会としては、こうした各分野の関係者のコミュニティを形成し、広げながら、関係者による活動を活性化していくこと、関係者による実装やサービス展開により得られる知見のフィードバックを集め、全体の議論をさらに発展させていくことなど、実現に向けた取組をファシリテイトする役割を担っていくことが重要である。

○　以上の考え方を踏まえ、今後の実現に向けた道筋について、以下に述べる。

(1) 今後の課題

○今後、以下の点について深掘り検討していく必要がある。
- 機能に関する更なる検討の深掘り(4.(4)参照)
- ユースケースベースでの具体的なアーキテクチャーと具体的な実装の検証(特に Dynamic Consent 機能、Trace 機能、トラストアンカーとの接続、ユーザーを支援するエージェント機能など)
- インターネット上の実装のオプションの検討(http 等のプロトコルレベル、情報の配置及び配置場所の指示方法などを含めた表現方法、ブラウザ等、ブロックチェーン)
- ガバナンスの具体的な在り方(ガバナンスの対象、マルチステークホルダープロセスの在り方等)
- インセンティブの具体的な在り方

以上を含む点について検討を進め、今後「ホワイトペーパー2.0」としてまとめていく。

○　なお、Trusted Web に関する検討の範囲としては、インターネット上に付加する機能を議論しているが、例えばセキュリティについてはハードウェアも含めてバーティカルにみていく必要がある点に留意する。

(2) 道筋（イメージ）

○　今後の検討深掘りや実装に当たっては、3.(2)の原則も踏まえ、特に以下の点が重要となる。

・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にすることが重要であり、その観点から UI/UX を重視する。例えば、検証されて確認できていることをユーザーが分かりやすく実感できるようにすること、合意の際にどのような確認がなされたかが容易に理解できるようにすること等が重要である。
・アーキテクチャーを考える上でのユースケース分析の際に、誰も取り残さないという観点から、見逃しているステークホルダーがいないか、常に意識し、配慮する。そして、ユーザーにとって敷居の高いものにならないよう、”Trust By Design”の考え方で取り組んでいくことが重要である。
・作って終わりではなく、運用が重要であり、テストし、評価するサイクルが重要である。
・中長期的な視点に立って、実装と運用について持続的、継続的に発展させていくためのサイクルを回し続けることか重要である。
・ラフなコンセンサスをとりながら、ワークしない場合にすり合わせを行うなど、相互運用性を担保していく。
・各機能やビジネス面でのアイデアを幅広く集める手段として、ハッカソン、アイデアソン、ワークショップのような機会を活用していく。

●2021～2022

～STEP1～　　始動期

〈検討の深掘り〉
- ホワイトペーパーについてグローバルに発信し、機能や運用等についてグローバルなコミュニティからのフィードバックを得る。
- インターネットコミュニティなどとの協働体制を構築(例えば、W3C、IETF、IEEE、ISO、OpenID Foundation 、My Data Global、World Economic Forum など)
- (2)で述べた課題の検討
  →ホワイトペーパー2.0の策定

〈実装〉
- プロトタイプの開発
- サンプルコード開発とレビュー
  →エンジニアなどがオープンソースで開発参加するサンドボックス環境の提供
  →ブラウザや OS で検証できる形での実装を目指す

〈ビジネス〉
- フォーラム等で産業界のニーズや課題について議論するなど、ビジネスベースでの動きとの連携体制の構築

●2023～2024

～STEP2～　　機能を構成するコンポーネントを提供するサービスやそれを利用したサービスの創出

〈実装〉

- 相互運用可能性を担保しながら、Identifier 管理機能や Dynamic Consent 機能等がベンチャーも含めた様々な企業によりアンバンドリングされ、多様なサービスの提供が広がる
- ブロックチェーン等の関連技術とも融合していく可能性も

〈ビジネス〉
- Trusted Web における機能のコンポーネントを利用したサービスの展開
  例として、人材証明、PHR のデータ共有、コンテンツ・広告の透明化、サプライチェーン共有等

●2025 以降

～STEP3～　　各分野での実装、普及フェーズ

- 多様な Identifier 管理機能や Dynamic Consent 機能等の開発・応用のサービスが収斂していき、おおむね確立。
- それを各分野で利用し、信用を価値変換につなげる多様なサービスが定着、普及。
- 他方、各コンポーネントは、収斂するだけでなく、運用しやすいように進化していくことが必要であり、そのサイクルは維持。

〈ビジネス〉
- 例として、IoT/M2M など、様々なサイバーフィジカル融合型のサービス等

●2030 頃

～STEP4～　　インターネット全体での実装

(3) 今後の協働において、各ステークホルダーに期待したい役割

○ 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のできる場を形成していくことも必要である。
　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

エンジニアは、疎結合を志向する Trusted Web の中で協働して、アーキテクチャーを設計し、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。

(アーキテクチャー)
Transitional Engineering の考え方も踏まえて、従来のインターネット/ウェブとの継続性を考慮しつつ、ウェブ、データベース、ブロックチェーン等を組み合わせながら、疎結合をベースとしてオープンなアーキテクチャーを設計していくことが期待される。

（基盤に関する標準化やリファレンスモデルづくり）

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）

アーキテクチャーの中でモジュールごとに機能を開発して様々な機能を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）

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。例えば、Trustable Communication 機能を補完する、信頼できる評価機関のレビューやポジティブリスト作り、悪質なプレイヤーをチェックしたネガティブリスト作り等も重要なポイントとなる。これらの貢献についても上記リファレンスモデル作りと同様に、インセンティブ設計を検討していく必要がある。

（試験）

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）

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）

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

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。

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。

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。

また、大学に限らないが、トラスト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産業界

産業界は、自らのデータの「出し手」あるいはデータの「受け手」でもあり、Trusted Web 上の新たなサービスのビジネス化を担う重要な主体である。

5.で触れたとおり、「アプリケーション・レイヤー」において、データの利活用や信頼の価値変換などにより、様々な分野での新たなサービスを提供すること、「ミドル・レイヤー」において信頼の創出に貢献するサービスを提供すること、「インフラ・レイヤー」においてアンバンドルされた新たな Identifier 管理機能や合意形成基盤等を提供することなどが期待される。

従来型のビジネスの延長線上でなく、デジタル社会における Trust を新たなビジネスモデルの競争軸としてこうした新しいビジネスを生み出していくことが期待される。特にベンチャー企業にとっては、「インフラ・レイヤー」においてアンバンドルされた基盤の開発・提供はよいビジネス機会にもなると考えられる。

また、Trusted Web に関連する様々な技術開発を行いつつ、社会の課題解決のための実装プロジェクトを推進するとともに、国際標準化などに参加することが期待される。

今後のデジタル社会のインフラの形成に関与を深めることは、各企業にとっても意義があることと考えられ、自社のエンジニアが標準化やリファレンスモデルの構築に貢献する活動に対し、産業界としてインセンティブを与えていくことも期待される。

プラットフォーム事業者にとっても、その技術力を生かし、マルチステークホルダーの一員として、アンバンドリングされた Identifier 管理機能や合意形成基盤等の開発に協力参加することなどにより、Trust の基盤形成に参画することが期待される。こうした基盤の上での多様な主体による競争とイノベーションが実現されれば、自らもコアサービスに集中できるメリットを享受できるとともに、社会からの信頼を高める機会と考えられる。

④ユーザー

ユーザーは、Trusted Web においては、その自由意思に基づき、コントロールを行使してデータをやりとりすることができる主体である。場合によってはプラットフォームを介さず、直接相手とやり取りし、自らが情報の Trust や合意形成について自由な判断を行う反面、一定の責任を追う立場でもある。

従来の受動的立場だけではなく、系全体の Trust を支えることが自らの利益にも資することから Trust をレビューして評価属性を与える、あるいは検証する側に回るなど、能動的なプレイヤーとしてルール形成にも参画することが期待される。

さらに、UI/UX の観点からレビューを行い、その改善について開発・運用者に対して積極的にフィードバックしていくことが期待される。

また、消費者保護の視点や、誰も取り残さないという観点から、例えば消費者保護団体やシビルソサイエティなどからのインプットも期待される。

⑤国際標準機関

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。

⑥政府等

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。

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。

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。

この他、立法、行政、司法の三つの機能ごとに関わり方の検討が求められる。

(4) Trusted Web 推進協議会の今後の活動

- ○ 上記(4)に記したホワイトペーパー2.0 の検討を進めていくとともに、グローバルなコミュニティへの働きかけやフィードバックの取得、協働に向けた取組を進めていく。議論の経過についてもオープンにしていく。
- ○ また、Trusted Web に関心を持つエンジニアや大学等研究教育機関、産業界やベンチャーなどの関係者が参加できるコミュニティを組成し、プロトタイプやサンプルコードの開発や実装に参画し、また、自らのサービス創出における課題のフィードバックなどが行えるような環境を整えていく。さらに、ハッカソンやアイデアソンを通じたプロジェクトの公募なども行っていく。

以上

Trusted Web 推進協議会　名簿

（令和３年３月 12 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 取締役専務執行役員
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	株式会社富士通研究所　セキュリティ研究所　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：内閣官房 IT 総合戦略室、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３年３月 12 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 リサーチャー
岩田　太地	日本電気株式会社 デジタルインテグレーション本部 主席ディレクター
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 CEO
○黒坂　達也	株式会社 企 代表取締役
佐古　和恵	早稲田大学 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
藤村　滋	ＮＴＴサービスエボリューション研究所　主任研究員
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）

Trusted Web 推進協議会
Trusted Web 推進協議会　タスクフォース

開催実績

令和２年	10 月 15 日	第１回 Trusted Web 推進協議会
	10 月 30 日	第１回 Trusted Web 推進協議会タスクフォース
	11 月 20 日	第２回 Trusted Web 推進協議会タスクフォース
	12 月 14 日	第３回 Trusted Web 推進協議会タスクフォース
	12 月 25 日	第２回 Trusted Web 推進協議会
令和３年	1 月 15 日	第４回 Trusted Web 推進協議会タスクフォース
	2 月 3 日	第５回 Trusted Web 推進協議会タスクフォース
	2 月 12 日	Trusted Web 推進協議会タスクフォース 集中検討セッション１
	2 月 17 日	第６回 Trusted Web 推進協議会タスクフォース
	2 月 18 日	Trusted Web 推進協議会タスクフォース 集中検討セッション２
	2 月 25 日	第７回 Trusted Web 推進協議会タスクフォース
	3 月 8 日	第８回 Trusted Web 推進協議会タスクフォース
	3 月 12 日	第３回 Trusted Web 推進協議会

用語集

項番	用語	解説
1	Authentication	Authentication（認証）とは、ネットワークやシステムへ接続する際に本人であることを確認すること。主に二者間で相手の真正性を確かめることであり、暗証番号や ID とパスワードの組み合わせなどにより本人を特定する。
2	電子証明書	電子証明書は、公開鍵証明書の一般的な呼び名です。公開鍵証明書は、公開鍵とその所有者の名前が入った電子データです。 その他に所有者や公開鍵に関する付加的な情報が入っていることがあります。公開鍵とそれらの情報を結びつけるため、公開鍵証明書には電子署名が施されています。電子証明書に関する標準化活動は、現在 ITU-T と IETF の PKIX-WG、 および ANSI で行われています。 最新のドキュメントは、ITU-T の X.509 2005 と、IETF の RFC5280、 ANSI の X9.55-1997 で、これらは電子証明書を使った認証基盤である PKI(Public-Key Infrastructure)について書かれています。 出典：一般社団法人日本ネットワークインフォメーションセンター https://www.nic.ad.jp/ja/basics/terms/denshi-shoumei.html
3	DID	DID とは、Dicentralized Identy（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/
4	SSI	SSI とは、Self-Soverign Identiy（自己主権型アイデンティティ）の略で、管理主体が介在することなく、個人が自分自身のアイデンティティをコントロールできるようにすることを目指す考え方。管理者を介さずに自分自身でアイデンティティ情報を管理できることを重視している点が特徴。 出典：デジタルアイデンティティ～自己主権型／分散アイデンティティ～ 株式会社野村総合研究所、NRI セキュアテクノロジーズ株式会社、株式会社ジェーシービー
5	Verifiable Credentials	Verifiable Credentials(検証可能なクレデンシャル)。 現実世界において、クレデンシャルは以下により構成される。 ・対象者の識別に関連する情報（例：写真、名前、識別番号） ・発行機関に関連する情報（例：政府、国家機関、認証機関） ・種類に関連する情報（例：パスポート、運転免許証、健康保険証） ・発行機関が対象について主張している特定の属性情報（例： 国籍、生年月日）

		・どのようにして得られたかについての証跡 ・制約に関連する情報（例：有効期限、使用条件） 検証可能なクレデンシャルは、物理的なクレデンシャルが表すのと同じ情報をすべて表すことができ、加えてデジタル署名などの技術を用いることで、現実の物理的な確認より改ざん防止性や信頼性を高くすることができる技術である。 出典：W3C Verifiable Credentials Data Model 1.0 https://www.w3.org/TR/vc-data-model/
6	DNS	DNS は、Domain Name System の略で、 インターネット上で ドメイン名を管理・運用するために開発されたシステム。 現在のインターネットを利用するときに必要なシステムの一つ。通信に使用する IP アドレスを扱いやすい文字列（ドメイン名）に変換。 DNS は、 世界中に存在する多数のサーバが協調しあって動作するデータベース。特定のサーバがドメイン名情報をすべて持っているわけではなく、 「委任」と呼ばれる仕組みでデータを階層ごとに分散化して管理。 出典：一般社団法人日本ネットワークインフォメーションセンター https://www.nic.ad.jp/ja/basics/beginners/dns.html
7	トラストアンカー	トラストアンカーとは、インターネットなどで行われる、 電子的な認証の手続きのために置かれる基点のことです。 トラストポイントとも呼ばれます。ここで言う認証の手続きとは、 アクセスしている通信相手が正しいことを確かめたり、電子データが途中で変更されずに、 正しい状態にあることを確かめることを意味しています。 トラストアンカーという概念は、 PKI(Public Key Infrastructure)の電子証明書のような、 電子的な証明が連鎖した構造を持つ認証基盤を使うときに用いられます。 この証明の連鎖とは、「ある者が別の者の正しさを証明し、 その者が更に別の者の正しさを証明する」といった構造のことです。 このような認証基盤を使った認証の手続きは、通信相手の電子的な証明、 または電子データに付けられた署名が、あらかじめ設定しておいた基点との間で、 正しく連鎖しているかどうかを確認することで行われます。 この基点がトラストアンカーです。トラストアンカーは必ずしも連鎖の頂点ではなく、 認証の手続きを行う者が各自に信頼を置くところに設定します。 あらかじめ複数のトラストアンカーを設定しておくこともあります。 出典：一般社団法人日本ネットワークインフォメーションセンター https://www.nic.ad.jp/ja/basics/terms/trust-anchor.html
8	Certification Authority	CA（Certification Authority）とは、主にインターネット取引などで使用されるデジタル認証（公開鍵証明書）などを発行する機関（認証局）です。CA にはパブリック CA、プライベート CA の 2 種類があります。パブリック CA は、電子署名法で規定されている指定業者です。不特定多数の電子商取引や個人のホームページでデジタル認証が使用されます。 プライベート CA は、自由に発行が許されている認証局です。自由にデジタル認証を発行できることから、イントラネットや限られた利用を限定した電子商取引で使用されます。パブリック CA は維持に費用がかかることから、プライベート CA の方が数が多く、企業間の電子メールにおけるデジタル署名に使用されています。 出典：セコムトラストシステムズの BCP 用語辞典 https://www.secomtrust.net/secword/ca.html

9	サーバ証明書	サーバ証明書（SSL サーバ証明書）は、運営者の実在性を確認し、通信データの暗号化を行うための電子証明書であり、認証局によって発行される。実在性の確認として、認証レベルが簡易な順（＝信頼性の低い順）に、以下の三種類がある。 • ドメイン認証型(ドメイン使用権のみ確認) • 企業認証型（運営団体の実在性を第三者機関等を利用して確認） • EV 型（Extended Validation：組織の所在や、署名者等の実在確認を行う）
10	World Economic Forum	世界経済フォーラム https://www.weforum.org/ Common Pass Project https://commonpass.org/
11	World Wide Web Consortium	W3C(World Wide Web Consortium)は、メンバー組織と専任スタッフ、そして一般市民が協力して Web 標準を開発する国際的なコミュニティです。ウェブの発明者であるティム・バーナーズ=リー氏が創設。 https://www.w3.org/
12	IETF	インターネット技術の国際標準化団体 オープンなプロセスで、オープンな標準を開発 https://www.ietf.org/
13	OpenID Foundation	OpenID Foundation は、OpenID 技術の実現、促進、保護に取り組む個人や企業による非営利の国際標準化組織。 https://openid.net/foundation/ https://www.openid.or.jp/
14	GitHub	GitHub は、ソースコードをホスティングすることで数百万人もの他の開発者と一緒にコードのレビューを行ったり、プロジェクトの管理をしながら、ソフトウェアの開発を行うことが可能な開発プラットフォーム。 https://github.co.jp/