資料１

# Trusted Web　推進協議会（第2回）

# 討議用資料

令和2年12月25日

内閣官房デジタル市場競争本部事務局

# これまでのタスクフォースでの議論

**○これまでタスクフォースを3回開催。**

**・今後アーキテクチャーを設計するにあたって必要となる「原則」について、議論。**

課題認識・ビジョン
そのための要件
（実現したい価値とターゲットとすべき環境条件（時期等を含む））

→ **アーキテクチャー設計にあたっての「原則」**
（システムの全体像を表現するためのコンセプト）

→ （機能と性能の設定）

**・ヘルスケア、コンテンツメディアの2つのユースケースについて議論し、上記「原則」の議論にも反映**

## ヘルスケアのユースケース設定

本人が自らの検査結果を集約・管理し、必要な情報を提示することで移動時の証明や検査重複の回避や新たなサービスを受けることができる。

## コンテンツメディアのユースケース設定

フェイクニュースなどが拡散する中、流通するコンテンツについてオリジネーターからの流通経路が明確であり、コンテンツについての真偽が判断でき、閲覧者等から、必要に応じて報酬を受け取ることもできる。

# 本日、議論いただくこと

○タスクフォースにおいて、年明けから、Trusted Webの基本アーキテクチャー（コード化にあたって機能や要件の要素を整理したもの)に関する議論に入っていくところ、

①これまでタスクフォースにて議論してきたアーキテクチャー設計にあたっての「原則」

②それを踏まえて、必要となる機能

③デジタルアイデンティティなどの実装の方向性

④今後の進め方

などについて、ご意見をいただきたい。

## 今後のスケジュール　イメージ


10-12月

1-2月

3月

～2021.3
様々な国際会合において必要に応じ発信

2021.4
Global Technology Governance Summit

第一回～第二回　Trusted Web推進協議会

第三回　Trusted Web推進協議会(予定)

第一回～第三回　タスクフォース　←　タスクフォース　→

# Trusted Webに必要となる機能、実装時の必要事項、ガバナンス

引き続き精査・議論

**背景**

○全ての領域でDXが進む中でデジタルでのTrustが死活的に重要に
←フェイクニュース等、膨大な真偽不明のデータが流通
←データに基づく正しい判断や今後のIoTでのデバイス制御にはTrustが不可欠

○インターネットの構造上、特定のサービスに依存しない形で、Trustを担保する手段は用意されていない
←メガプラットフォームによるTrustは寡占やプライバシーへの懸念を生み限界
←個人・法人が安心してデータを流通させるためには上記に拠らないTrustが重要に

*Trust: 事実の確認をしない状態で、相手先が期待した通りに振る舞うと信じる度合い

**目指すべき方向性: 特定サービスに依存せず、Trustが担保される仕組み**

○データの出し手:
個人・法人がデータをコントロールし、価値に変換できること
○データの受け手:
データの出し手や改変者を確認でき、データの真正性が担保されていること
○データのやりとりのスキーム:
データのやりとりが「正しく」行われていることが担保されていること
*やりとり:単一のシステム内のプロセス、NW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

**必要となる機能 →今後の議論**

○個人・法人によるコントロール
データ及びその場所をコントロール、委任可能で監査可能

○データの受け手から見たデータの出し手やデータの真正性
・データの出し手や改変者が把握でき、データのやりとりが記録され、検証可能
・ステークホルダーに依存しない識別子があり、公開可能。その上でステークホルダ固有の属性を必要に応じて紐付けることが可能
・データへのアクセスが記録され、検証可能であること
・内容に応じて第三者機関による保証（トラストアンカー)を属性に付加できること

○データのやりとりの「正しさ」の担保
・ステークホルダーが特定され、それぞれの利害が特定され、ステークホルダー間で、Web上で行う事項について、ゴールが合意されていること、合意されたゴールを元に、ゴールが実現されているかどうかの評価とフィードバックがなされること、ゴールは、動的に修正できること
・必要に応じ、悪意の者に対し、分散的なガバナンスによるブラックリスト等で、「不正」を監視・通知ができること

……等

**原則**

**支える仕組み(ガバナンス)**

①持続可能なエコシステム
ステークホルダーで責任分担・インセンティブ、機能的救済、強靭性
②マネジメントプロセス
分散・分権型、悪意もビルトイン、トラストアンカーの組込
③透明性、相互検証可能性
アーキテクチャー、コード等の中身・プロセスがオープン、相互に検証

**機能をシステムとして実装する際に必要なこと**

ユーザー目線
④個人・法人によるコントロール: 持ち運び可能、アクセス容易、データ等から個人が特定されない、抹消などプライバシー担保の仕組み、例外として公益目的でのデータ活用のバランス
⑤誰も排除しない・ユニバーサル性: 誰でも許可・追加コストなく参加可能、誰でもTrustの程度が容易に判断できるようUI/UX設計がされている
⑥ユーザー視点:ユーザー側に選択肢、ロックインフリー、分かりやすいこと、意思決定が支援されている、技術を意識しない

システム目線
⑦継続性:Transitionalに現行webに付加、既存資産の活用、トラストは自律分散型と中央集権型のバランス
⑧柔軟性:疎結合でモジュラリティを確保、障害点なし、間接参照の活用、トラストの多様性に対応
⑨相互運用性: 社会システム全体やグローバルの様々な運用・法制度と連携可能、アジャイルに変更、グローバルな協働
⑩更改容易性:機能拡張可能、スケーラブル、アーキテクチャー自体の変化、分権的なアップデート、サイバーフィジカル

留意点
⑪相対主義:全てのデジタル化を欲張らない

**実装におけるイメージ例（技術の組み合わせ）→今後の議論**

○グローバルなDigital Identity ← Decentralized Identity/Identifier
○Personal Data Store ……等.

# 原則要素①:ガバナンス

## 原則①持続可能なエコシステム（ビジネスモデルとインセンティブ）

- ✓ ステークホルダーでの責任分担・インセンティブかあること
- ✓ インセンティブづけできること
- ✓ 機能的な救済を実現できること
- ✓ ライフサイクルを意識すること
- ✓ Resilient and antifragile business model
- ✓ Non-competitive field and competitive field
- ✓ Consider current accusation to Google
- ✓ Low (or no) additional cost to use the platform for users, but the cost to maintain the platform should be compensated.

## 原則②マネジメントプロセス

- ✓ 分散型・分権型であること
- ✓ 誰にどんな責任があるか明確にし、問題があったときに原因究明ができること
- ✓ Poly-centric stewardship
- ✓ マルチステークホルダーが取り組むことができること
- ✓ 特定組織が情報、権限、運用権限を独占しないこと
- ✓ 特定のサービス事業者によるデータ独占がされていないこと
- ✓ 少数を利する仕組みにはしないこと（fair）
- ✓ 特定の個人・法人の利益誘導とならないこと
- ✓ Not for marketing by single stakeholder
- ✓ 情報の非対称性をなくすこと
- ✓ 個人や組織の良心・良識に頼らないこと（セキュリティ面での弱点となる）
- ✓ 起こりうる悪用の仕方をある程度想定すること
- ✓ 情報の歪み・skewをなくすこと
- ✓ Common understanding for all stakeholders
- ✓ ESG等社会性に対するコミットメントの要素も取り込んでいること
- ✓ トラストアンカー（Identifierを発行するときの属性を与える人たち）が組み込まれていること

## 原則③透明性・相互検証可能性

- ✓ アーキテクチャ、実装とそのプロセスにOpennessがあること
- ✓ ソフトウェアコードの中身と作成過程が検証可能であること
- ✓ Think continuous review and refinement (loop)
  - ➢Security/privacy management process
  - ➢Process for amendment and supporting governance
- ✓ 透明性が高く、相互に検証可能であること

## <TF等での意見>

- インセンティブは、広告モデルに偏っていたものを、マイクロインカム等何らかの方法で広告モデルに依存しないビジネスが成立する環境などが必要ではないか。
- ステークホルダごとにペインポイントがあり、それらのペインポイントはトレードオフの関係にある。それを分析してマネージするかがアーキテクチャーにとって重要。ステークホルダごとのペインとゲインを見つけた上で、ペインをゲインに変えうるシステムを考えること。これ自体がフレームワークとして重要。
- 適格やフェアであるとは一体何なのか。フェアの価値判断について、当事者間の合意によるものに照らし合わせる仕組みを組み込む必要があるのではないか。
- 公益活用とのバランスをどうガバナンス構造の中に組み込むか。その際、自分のデータを公開する範囲をコントロール出来るようになっていると良い。
- 一時的に切断されても社会基盤の機能を失わない、何時間くらい切断されたときにどういう影響があるかということを考えていくべき。
- Trusted Webの上にのるアプリケーションも、インフラもどちらもエコシステムが必要。特に基盤は、どこからどこまでが社会基盤か、どこまで税金を入れるのか、グローバルでは難しいので民主導でやらないといけないのか、エコシステムを考えていく必要があると感じた。
- データは一次利用によって最大の利益が生まれる。データ主体の都合がよい様にフル活用するためには、データ主体の手元に集約されているのがよい。
- 「不正」を判断・通知するための共通化された API と UI の提供。ステークホルダー・プラットフォーマーがそれぞれ独自あるいは連携して「不正」「信頼レベル」「評価、評判」のような情報をプラグイン的に提供、確認可能にすること。「不正」に対するユーザ(コミュニティ)フィードバック、報告と評価の仕組みがあること。
- 監査：情報へのアクセス等のアクティビティを記録し、情報の所有者や運用・監査をする者が確認できること

- エコシステムを実現する上で、適したマネジメントプロセス、ガバナンス構造は何か。
- 分散と中央の組み合わせについて、個人がデータを持ち続けるのは難しいので、移譲や委任ができること。正しく運用されてることの監査ができる観点が必要。ある程度の中央集権を作るが、他のステークホルダーが監査できる仕組みづくりが必要。
- 既存のトラスト手段との組み合わせをどう考えるか
- 悪意を持ったステークホルダーを想定した異常系をどう確認するかを考える必要。
- コンテンツについて、プライバシーと法執行のバランスについて、情報の発信の自由を確保しつつ、何かあったらペナルティを課すということをどう担保するのか。
- 運用側面まで考えた形での全体設計、システムを動かす視点での制度設計をすることが非常に重要。
- ガバナンスの在り方については、必ずしも政府によるということではなくコミュニティによることがある。フィードバックを踏まえて回していく方が有効。ゴールも変化させながら、comply or explainを求めていくアプローチ。
- マルチステークホルダーガバナンスでは、レビューをしながら繰り返しリファインしていくことを全体のシステムの中に取り入れることが重要。

- 識別子、公開と記録範囲（アクセス、トレーサビリティ）など、基準・用語の明確化をした上で、それを確認するためのシステム・API・コンテンツに対するメタデータの付与。確認するためにある程度共通化された UI での確認手段をブラウザや OS などのプラットフォームレベルで提供する・できること。

# 原則要素②:システム実装(ユーザー)

## 原則④個人・法人によるコントロール

- ✓ データのコントロールはデータ主体に帰属し、不在の場合には場所・設備を有する人に帰属すること
- ✓ コントロールを委任可能であり、監査できること
- ✓ 個人の自由の基礎となること
- ✓ Portableであること
- ✓ Accessibleであること
- ✓ プライバシーに配慮すること
- ✓ 忘れられる権利に配慮すること
- ✓ 個人情報のexposureが最小化されること
- ✓ データの生成・保管・消費におけるデータやその場所のコントロールが確保されていること
- ✓ 例外として公益目的でのデータ活用とのバランスの道も残されていること

**<TF等での意見>**

- データは一次利用によって最大の利益が生まれる。データ主体の都合がよい様にフル活用するためには、データ主体の手元に集約されているのがよい。
- 集権と分散については、個人や法人のデータコントロールはあるが、個人がデータを持ち続けるのは難しいので、委譲、委任ができること、そこで正しく運用されているのかを監査できるようにするといった観点が必要と思う。この場合、ある程度の中央集権をつくるが、他のステークホルダーや個人が監査できるような仕組み作りが必要と思う。
- 識別子が公開されていることも前提としてあるのではないか。その場合、プライバシーをどう担保していくかというのは今後議論になっていくかと思っている。

## 原則⑤誰も排除しない、ユニバーサル性

- ✓ 誰でも自由に参加（・脱退）できること
- ✓ デジタルデバイドに最大限配慮すること
- ✓ ほぼ全ての年代をカバーする優しいUXであること
- ✓ Universal access
- ✓ 弱い立場にある個人の自由な選択や判断をリスペクトすること。正当な理由なく、強い組織の論理を個人に押し付けないこと。
- ✓ 誰でもTrustの程度が容易に判断できるようUI/UX設計がされている
- ✓ 公共財(Common Good)であること
  - ➢ あらゆる人が享受できる権利があること Permissionless
  - ➢ 追加的なコストを払うことなく（ある程度）同じ恩恵を享受できること

- アクセシビリティの確保が重要。自然人、法人を問わず、この人がアクセスできない、この人は権限がない、お金がかかるのでできないといったことが起きないということが必要。
- 悪意のある人の視点を含めたアーキテクチャ設計は必要不可欠であるが、何をもって安全かすべての人が理解できるような仕組みが必要。ディジタルネイティブでない人にも安心・安全に使える仕組みが必要

## 原則⑥ユーザ視点

- ✓ ユーザに選択肢があること
- ✓ Lock-in free
- ✓ ユーザにとって分かりやすいこと
- ✓ 様々な形での意思決定が支援されていること
- ✓ Write once, use everywhere
- ✓ 個人(特にラガード的な利用者の視点)に特に重きをおくこと
- ✓ 既存のWebよりもユーザー視点で実利があること（わかりやすいUX、プロトコルレベルでのインセンティブ設計など）
- ✓ どんな技術が使われているか意識させないこと
- ✓ ただ使うだけで何も心配がないこと
- ✓ コントロールの細分化によるUXの悪化を避ける工夫

- TWが何をもって安全安心という点において、すべての人が理解できることが重要。また、個人のリテラシーによらずに安全安心に使えることが重要。
- どこまで信用できるところが担保されているのかユーザーに伝わらなければ意味がない。いくつかの視点に対しては基準に沿ってどうなのかが比較的わかりやすい用語定義を普及させる、そしてその用語定義に沿ったUIを作るということが必要。
- 実際にシステムを使ったときに、ユーザーが利用するプラットフォーム、アプリケーションあるいはブラウザなのかのシステム側で、どのような形に表現するかというところを早めに具体化した方がいいと思う。そのために何をUIに表示するのか、ポイントとなっているのはどこなのかというのをいくつか絞っておきたい。
- 11の原則に違和感はない一方で、ユーザ視点ではなく、ステークホルダー視点かもしれない。これには、もちろん個人を含むし（一般的に言えば、Civil Society）、ステークホルダー間の協調が重要になるかと思います。

# 原則要素③-1: システム実装(システム)

<TF等での意見>

## 原則⑦継続性

- ✓ Transitionalな形で現行Webに付加する仕様とImplementation（拡張、遷移を目指す）
- ✓ Transition engineering（その際には現状の構造を分析（個人、組織、システムを分析すること））
- ✓ 既存インターネットアーキテクチャからの上位互換となっていること、既存の資産の上に乗る
- ✓ 確認済みデータを活用すること
- ✓ 既存のWebとシームレスに接続すること
- ✓ トラストは自律分散型としつつ、中央集権的な仕組みの組み合わせを排除しないこと
- ✓ 既存のトラスト手段との組み合わせ（フェデレーション）を排除しないこと

- 例えばヘルスケアのユースケースについては、トラストアンカーの設計自体は、既存のシステムを使う。
- 既存の考え方の歴史を学ぶ（温故知新、課題の再発見をしない）例：ISMSなどの運用ライフサイクルマネジメント（これの効率化を考える）

## 原則⑧柔軟性

- ✓ 疎結合の状態になっていること
- ✓ 連続的・連鎖的にシステムが倒れることを避けること
- ✓ 実装依存性を極力排除すること
- ✓ 個別要素技術との疎結合（特定のものにしばられない）
- ✓ 障害点がないこと
- ✓ 間接参照の活用
- ✓ 疎結合のデメリットもある：結合先が「暗にこう動いてくれるだろう」と期待してしまう（が期待通りにいかないこともある）、セキュリティ・プライバシ・マネジメントシステム(系全体として安全にするためのマネージメントがセキュリティに必要)
- ✓ Use online technology toward permissionless innovation
- ✓ 多様性に対応し、主体やデータの種別等に応じてトラストに求められる要件や水準を確保すること

- 識別子の発行の仕方は多様であり、対象は自然人、法人、データ、場所、建物などとなり得る。
- 識別子を管理できるのが誰か（認証局やweb of trustの考え方など）、コントロールの意味も多様にバリエーションがある。
- 例えばコンテンツ・ロンダリングへの対応であれば、著作権制度の違いを超えて対応できるような設計が重要となる。
- トラストアンカーが系全体の信頼性を担保するために同じ基準で執行されるケースにおいて、基準の統一ができない可能性がある。　（DNS的なものでも限界）
- 削除をできるコントロールは、限られた領域・分野にのみ求められる可能性もあるので、いれた方がよい場合と、そうでない場合がある。
- いいサービスが出てきたら前のものと挿げ替えるということができるためには、サービス間が疎結合、モジュラリティがあることである。
- リファレンス実装を示す(機能・仕様は実装を伴って始めて実用性・運用可能性が確認される)と共に、それをより良い・別の形の実装に置き換え可能な設計をすること。
- 規模対応性：すべての人が様々なことに利用するような規模に対応すること
- must haveなものはコアに入れるべきであるが、better to haveなものをコアに入れると実装や運用が大変になるので、拡張で入れられる仕組みがあるとよいと思う（「拡張性」）。

# 原則要素③-2: システム実装(システム等)

<TF等での意見>

## 原則⑨相互運用性（interoperability）

- ✓ 拡張性や社会システム全体としてのインターオペラビリティを確保すること
- ✓ Agile governanceであること
- ✓ Minimum Interoperabilityであること
- ✓ グローバルで使えるものであること
- ✓ グローバルな取組が行われているものと親和性が高いものであること
- ✓ 複数のガバナンスを認めつつ、ガバナンス間のコミュニケーションがあって、最低限同意すべきところがクリアになっていること
- ✓ Aware of the difference between Global and International
- ✓ Collaboration with global experts

- 既存のシステムを使う際の社会システム全体としてのインターオペラビリティとして、例えばヘルスケアのケースでは、医師の診断へのトラストなどは、既存の仕組みを使う
- 日本だけではなく、グローバルなアーキテクチャを前提として、各国の既存の法令も見ながら、法整備をしなくても可能なところから運用設計をしていく必要がある。前提が違っても運用ができる制度設計が必要。

## 原則⑩更改容易性

- ✓ 機能拡張を妨げることがないこと
- ✓ スケーラブルであること
- ✓ アーキテクチャ自体が変化や深化することを妨げないこと
- ✓ 中長期を意識したアーキテクチャとすること
- ✓ 分権的にアップデートができること、ルールを変えるためのルールがあること、100年後の人類が使えるもの
- ✓ サイバー・フィジカルの視点も踏まえること

- must haveなものはコアに入れるべきであるが、better to haveなものをコアに入れると実装や運用が大変になるので、拡張で入れられる仕組みがあるとよいと思う（「拡張性」）。
- 例えばヘルスケアでは状況が変わると目指すゴールが変わってくるので、求められるものも変わる。
- 何がフェアかは、プラットフォームのあり方や、時代によって変動する。その時代に合わせてどうゲーム設定するか検討する必要。
- 例えばヘルスケアのケースで要件や求められる条件が国ごとに違う中で、これは様々な業界においても言えることだと思うので、TrustedWebにおいては、公約数をとったような実装、最低限のコンポーネントを提供してその上に拡張性をもたせていくことが大事なのではないか。
- 要求事項が動的に変化する今のオンライン社会においては、物差しを相対的に、動的に定義する（そのためには、IT基盤の助けが必要）ことが重要であると考える。ゴールは動的に修正できること。
- 人間だけのみならず、IoTデバイスなどにも応用でき、オンラインの経済活動を促進できるようにすること。
- ヘルスケアの検査機関の信頼性について、診断を下した医師の診断がTrustできるか、そのデータがTrustできるか、データを出した人が本人かどうか3段階でTrustを作る必要。そのうちデータのTrustを作るのがTrusted Webで取り扱う内容と思う。 その他をどこまでアーキテクチャーのコアに含め、それ以外を拡張システムとして実装するか。

## 原則⑪デジタル相対主義

- ✓ デジタル化で頑張りすぎない、非デジタルで許容されていたことを認識していること
- ✓ 完璧を求めない、リスクを許容し、リスクへの対策・準備を図ること
- ✓ データガバナンスに関して、全てのデータを対象としないこと

- 一時的に切断されても社会基盤の機能を失わない、何時間くらい切断されたときにどういう影響があるかということを考えていくべき。

# 必要となる機能と実装

**必要となる機能　→今後の議論**

**○個人・法人によるコントロール**
**データ及びその場所をコントロール、委任可能で監査可能**

**○データの受け手から見たデータの出し手やデータの真正性**
- **データの出し手や改変者が把握でき、データのやりとりが記録され、検証可能**
- **ステークホルダーに依存しない識別子があり、公開可能。**その上で**ステークホルダ固有の属性を必要に応じて紐付け**ることが可能。
- **データアクセスが記録され、検証可能**であること
- 内容に応じて**第三者機関による保証（トラストアンカー)を属性に付加**できること

**○データのやりとりの「正しさ」の担保**
- **ステークホルダーが特定**され、**それぞれの利害が特定**され、ステークホルダー間で、Web上で行う事項について、**ゴールが合意**されていること、合意されたゴールを元に、**ゴールが実現されているかどうかの評価とフィードバック**がなされること、ゴールは、**動的に修正可能**
- 必要に応じ、悪意の者に対し、**分散的なガバナンスによるブラックリスト等で、「不正」を監視・通知が可能**

**……等**

**実装におけるイメージ例（技術の組み合わせ）→今後の議論**
**○グローバルなDigital Identity　← Decentralized Identity/Identifier**

**<TF等での意見>**

- コントロールの範囲の明確化(参照のみか、ダウンロードまで認めた際のコントロールなのか等、前提の明確化と前提に応じたコントロールの明確化)が必要。
- 出し手にとってデータをどこに置くのか。DB設計の際にリレーション正規化すると、分散と相性が悪い
- 個人がデータを持ち続けるのは難しいので、委譲、委任ができること、そこで正しく運用されているのかを監査できるようにするといった観点が必要。この場合、ある程度の中央集権をつくるが、他のステークホルダーや個人が監査できるような仕組み作りが必要と思う。
- 削除をできるコントロールは、限られた領域・分野にのみ求められる可能性もあるので、いれた方がよい場合と、そうでない場合がある。

- ステークホルダーに依存しない識別子を用いる事(DID等)。識別子にとってステークホルダーとの関係性を表現する手段が必要なのであって、識別子自体にステークホルダーとの連携を持たせる必要はない。DIDは極力リンクされないようにするのが重要。その上で、ステークホルダ固有の属性を必要に応じて紐付けること。
- 識別子の公開については、必ずしも公開が原則ではなく、必要なときに公開すればよいのではないか。
- プライバシーの特定につながらないようにすることが必要。データについては識別子は必要だと思うが、データから人に結びつけたくない。識別子が必要な場合、参照の方向性を考える必要。
- 人だけでなく、関連する物理的な場所やモノについて、公開空間においては識別子が割り当てられて共有されていること。
- 識別子を大量生産することでhackができないこと。ある対象に対して大量の識別子から悪評をつけるとか。
- 識別子の発行の仕方も多様。対象が自然人、法人、データ、場所、建物など。
- 識別子を管理できるのが誰か（認証局やweb of trustの考え方など）、コントロールの意味も多様にバリエーションがある。
- データにアクセスする側、アクセスの記録を残すこと、アクセスするのが法人、個人、匿名など、データを受け取る側の議論が少なかったと考える。
- スコアリングは価値判断を伴うため対象とすべきではない。
- スコアリングも属性の一つとして付加できるようにすべき。
- デジタルの世界と現実の世界を結びつける、オラクル問題を解決するものであること。識別子に法的保護を与え、識別子がリンクされているエンティティの法管轄をはっきりさせて法律の執行を可能にすること。

- 価値判断を伴うものをアプリオリにシステムから除くべきではない。共通基準でのチェックや、ステークホルダーの合意に照らし合わせて評価する仕組みは可能。
- 悪意を持ったステークホルダーを想定した異常系をどう確認するかを考える必要。
- 穴をついてくる悪意の者に対して、ブラックリスト・警告システムなどの仕組みができないか。その際、現在はPFが危険なサイトリスト管理や危険アプリ排除を行なっているが、レビュアーなどによる分散的なガバナンスで確保できないか。
- 誰でもトラストの程度が理解できるようなUI等の仕組みが必要。

- 現在のインターネットに明らかに欠落しているグローバルなアイデンティティは、議論しないといけなく、そこが1丁目1番目にあることは変わらない。

# 今後の進め方

○今後の検討にあたって、議論/留意すべき点は何か。

**<タスクフォース>**
- ○ 10月30日　アーキテクチャー設計にあたっての原則等
- ○ 11月20日　ユースケースベースでの議論(ヘルスケア、コンテンツ)
- ○ 12月14日　ユースケースベースでの議論/原則
- ○ **1月中旬**　**必要なる機能/基本アーキテクチャーのイメージ**
- ○ **1月下旬**　**機能を実現する技術/海外標準化等団体の動向整理/ユースケース（産業系?）**
- ○ **2月上旬**　**基本アーキテクチャー**
- ○ **2月下旬**　**海外へのアプローチも含めたロードマップ、アクションの整理**
- ○ **3月上旬**　**ホワイトペーパー原案**

**※タスクフォースは必要に応じ、追加開催も検討**

**Trusted Web推進協議会**

- ○ 10/15　第１回　協議会
- ○ **12/25　第２回　協議会**
  **アーキテクチャー設計にあたっての原則、必要となる機能、実装の方向性　等**
- ○ **3月　第３回　協議会**
  **ホワイトペーパー案**

**年明け以降の議論の焦点:「ホワイトペーパー」の項目イメージ例(第一回資料)から**

**1.背景と課題認識**
○ニューノーマルと新たなインターネット文明の調和
○今のインターネットとWebが達成していること/解決できていないこと

**2.ビジョン・全体の将来像**
○ビジョンの提示
　デジタルテクノロジーによる豊かな「ニューノーマル社会」の実現（仮説）

**3.重要な構成要素としてのTrust**
○Trustの定義
○Society5.0時代に目指すべきTrustの方向性

**4.Trustを実現するためのアーキテクチャー**
○アーキテクチャーの設計に必要となる要素
○アーキテクチャ設計の前提となる要件
○必要なガバナンス・インセンティブ設計

**5.実現に向けた道筋**
(1) 技術面での道筋
○関連する技術とその動向(Web,Data,BC)
○コアとなると考えられる技術の段階的なロードマップ
(2) 実装・需要面での道筋
○当面、期待されるユースケース、関連した動き
○実装に向けた課題
○今後の実現シナリオ

**6.必要なアクション**
○DFFTの具現化としての官民での国際発信
○国際標準化
○産、学、官それぞれの役割分担とアクション
○ユースケース実証・実装　など

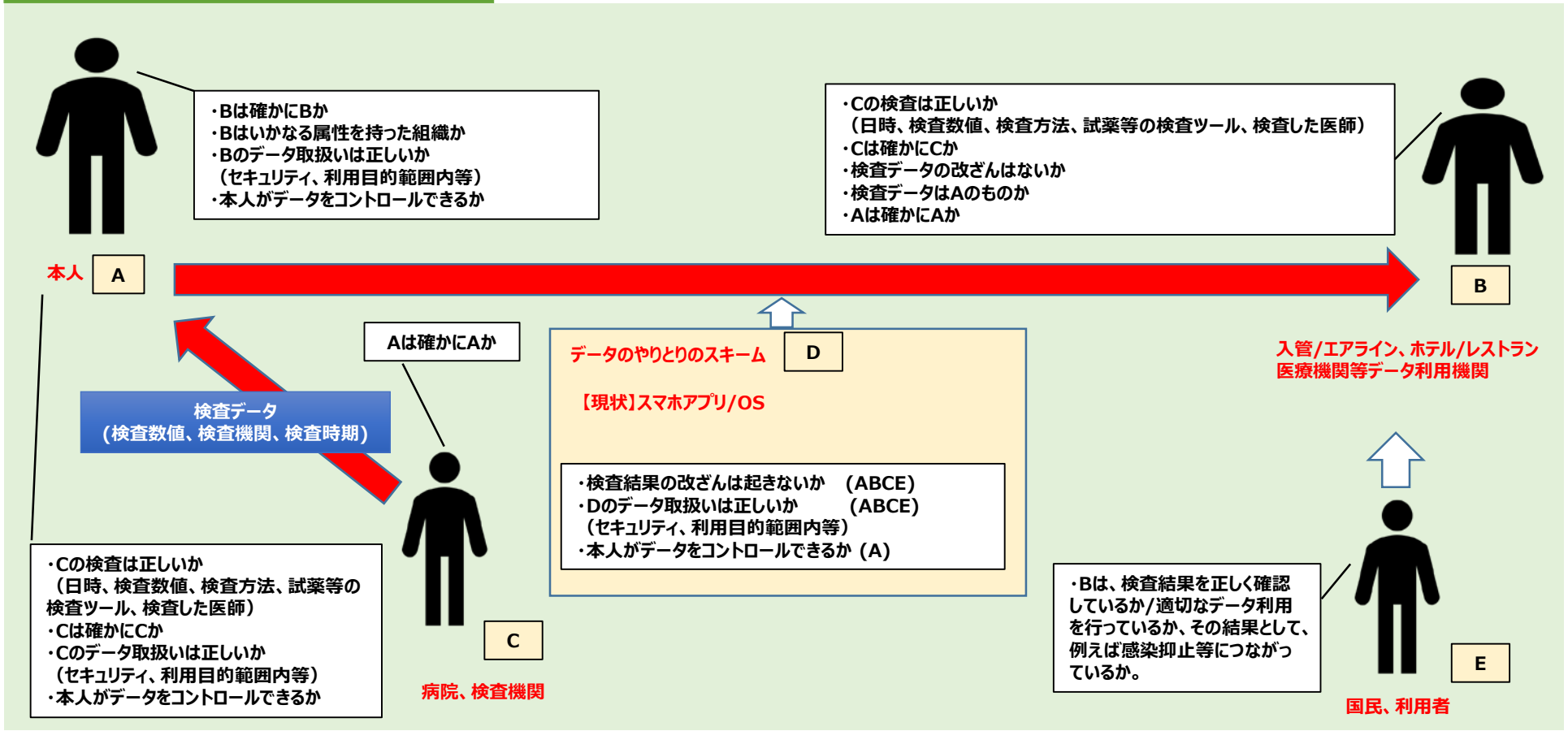
参考

# ユースケース分析関連資料

# ユースケース分析の概要 (ヘルスケア)

○特に検査結果に基づき入国等を判断する (B)から見て、本人 (A)から提示された検査結果が、「正しい」検査機関(C)により行われたものか、それが確かにAに対して行われたものかというTrustがポイントとなる。

## 基本的なステークホルダー間のTrust



**【機能をシステムとして実装する際に必要なこと】**

- ✓ 例えば国境をまたぐコンテクストにおいては、パスポートと本人が結び付いてることを示すことが追加されれば、多分足りると思う。この本人性いうことについて、これをだんだんEHRに広げていくとか、広げていけば広げるだけ難易度が上がっていくと思うが、ことアイデンティティーということで、**国のボーダーをまたぐ行動に限って言うならば、パスポート等のひも付けでいいはずである。必要な程度を少し考えたほうがハードルが下がる**のではないか。
- ✓ 一つは社会的な問題意識を踏まえて、より柔軟にさまざまな事業者や、ステークホルダーが存在している、あるいは既存のサービスインしているサービスの柔軟性や開放性をより高めていくことも含めて、新しい基盤を作っていく。そのときに重要となるのが、**恐らくアイデンティファイヤーをどのように取り扱い、そのアイデンティファイヤーは、どのような確からしさに基づいて判断されるのか。**情報システムだけではなく、社会システム側の要請ややらなければいけないリクワイアメントもあるが、システム側でやるべきこととして想定されるアーキテクチャが要件になるようなものは何なのか、あるいはそのアーキテクチャを考えるためのフレームワークは一体何なのかということが、この後議論として積み重なっていくといいと思っている。
- ✓ 昨今話題で、マイナンバーカードを保険証に使う、もしくは診療カードに使う話が出てて、その中で顔認証を使う話が出ている。最初はドキッとしたが、考えてみるとパスポートで顔認証は使われている。このため、手段と本人性の確認の程度のバランスが考えて、一番いい方法を上手に組み合わせて、それによってハードルをなるべく下げて、早めに実装実行できるようにするのがいいのではないか。
- ✓ 共通項の抽出をすることが大事だと思う。国によってコロナの感染者数、検査の基準等が違うので、その中でどのような共通項を取って、どのようなシステムを作っていくかは、アプリケーションが大事と思う。具体例で言うと、シンガポールは既にアプリケーション、フォーマーというものがあって、検温1日3回とか、場所をどうこうと全部取られている。新しいアプリが出てきたところで、その内容がフォーマーの中に入っているのであれば、それ使う必要がないとなってしまうので、**共通項をうまく抽出し、設計することが大事。かつコロナの感染者の人数も、日に日に変わってきて、流動性が激しい分野なので、既存のシステムの情報を引き継ぎながら、アップデートできるシステムであることが大事**だと思う。
- ✓ **オフラインでの正しさと、オンラインに一回載っている情報の正しさが違う**と思うので、どこまでを議論の対象にするか考えるのは大事。
- ✓ このシステムの対象となるであろう越境する人に対して、もう少し注意深く、どのようなステークホルダーか、どのような種類の人がいるのかを分析しなくてはならないと思う。国境をまたぐということについて、この状況において条件を曖昧に考えた状態で広げることは、疑いがある。なぜならば、特にCOVID-19以降、ステイアットホームでも収入が絶たれない人と、そうではなくUber Eatsのドライバーをやらなければ食べていけない人というようないろんな視点の分断があり、ある意味、構造化された搾取構造ができつつあるかもしれず、エッセンシャルワーカーと後ろにいる人たちの格差が広がってくる構造にある。そういう中で、越境を増やしたいからといって、危険がコントロールできないまま拡大するのであれば、それはあまりよろしくない。**この仕組みを入れるために、プラスアルファとして、グローバルに、実際のCOVID-19の再生産数がどのようになっているかコントロールをセットにしなくてはならないのではないか。そこまで考慮に入れなければ、エッセンシャルに越境しなくてはならない人が危険にさらされる状態のまま、ある意味、安全な所にいる人と置いてけぼりを食う人ができるような構造になる**とすると、それは人間にとって不幸。どういう人が当事者になり得て、その人に立ち返ったときに、**どういうメリット、デメリットがあるのかというところまで含めて、トラストを考えるときには織り込んだほうがいい**のではないか。
- ✓ **ペインとゲインを見つけた上で、ペインがゲインになるような機能やそれを実現するためのシステムということを考える。これ自体が、実はフレームワークとして非常に重要**だと思っているので、一つ一つのユースケースを増やして議論していくときにも、この視点をよりシェイプさせていきながら議論していく。なおかつ少し抽象度の高いレベルで標準的なものとして考えられるようになるときにも、必ずここはステークホルダーの特定と詳細な分析、ペインポイントを探るということをやっていかなければならないと思った。重要な視点を持つ、共有するということを前提とした上で、引き続き必要に応じてユースケースを議論していければと思っている。

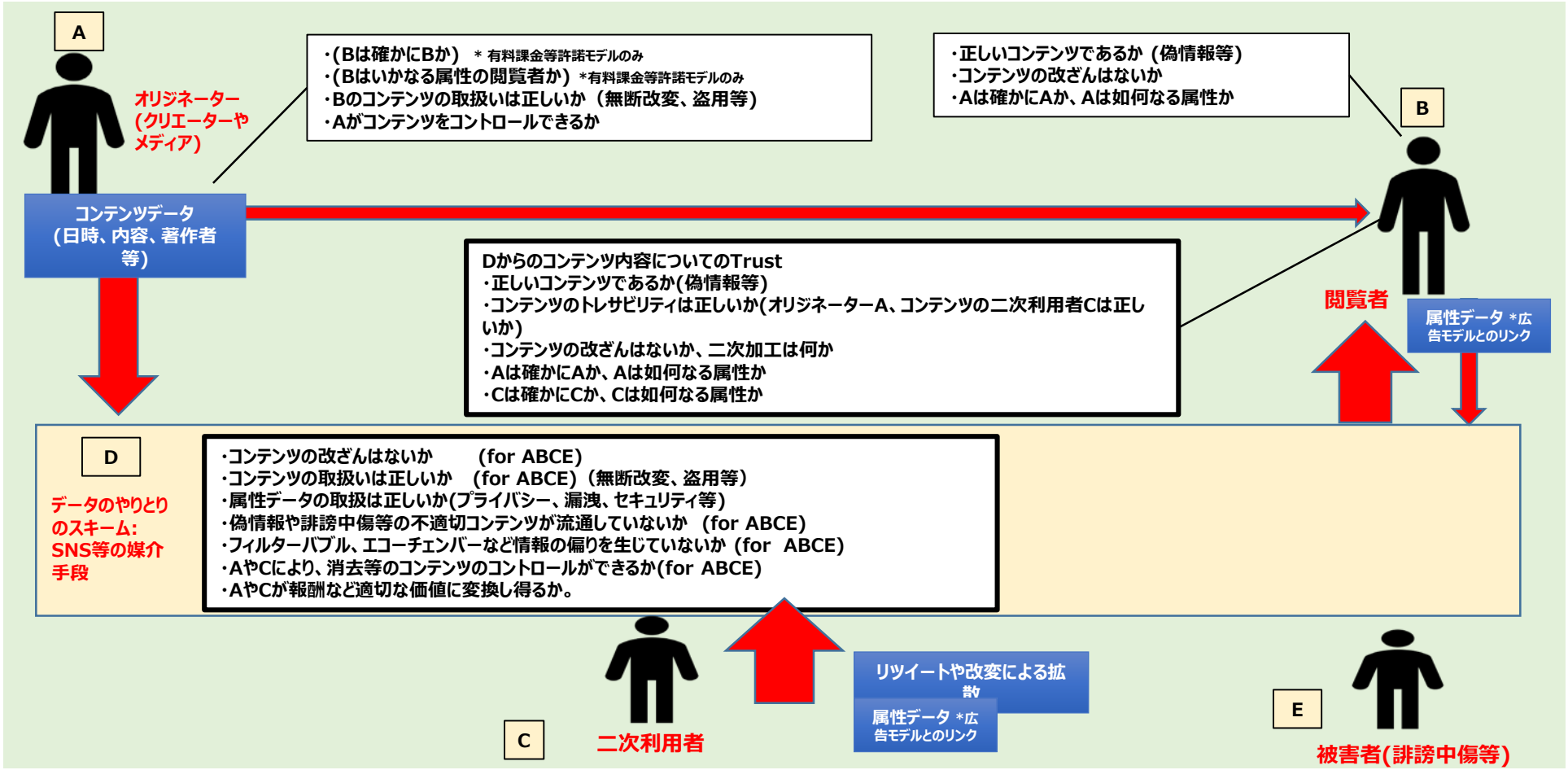
**【必要な機能】**

- 例えばワクチン接種機関や検査機関、オリジネーターの信頼性評価を、いわゆる信頼できる、できない、この機関は駄目だった、失敗したから信頼をリボークするなどだけではなく、Trusted Webの枠組みとしては、**相対的な適格性とコンテンツで言ってたのと同じように、この検査機関がどういうところが信頼できて、どういうポリシーで信頼性を判断し、組織から見ても大丈夫かどうか、その視点も忘れるべきではない**。
- ✓ COVID-19の事例では、**⑤まず診断を下した医師の診断がトラストできるか、そのデータがトラストできるか、最後にそのデータを出した人が本人かどうか、3段階でトラストを作らなくてはならない。その三つのうち、データのトラストを作る部分に関しては、このタスクフォースで取り扱う内容**だとは思う。他の部分に関しては、どこまでアーキテクチャの中に含めて、どこからが外に行く拡張システムとして実装するのか。その辺をまず決めて皆で共通認識を持っていなければ議論が紛糾してしまう。特に最初の医師の診断が正しいか、正しくないかに関しては、技術的なものではないターンが沢山あるので、そこをどうやって担保するのか議論をいきなり始めてしまうと話が進まなくなると思う。Trusted Webというアーキテクチャで進むところの範囲の線の引き方は指摘通りだと思う。例えば日本においては、医療療法学会とどうやっていくかという話とガバニングの話とテクノロジーのウェブとして吸収していく部分とに分かれると思う。
- ✓ 先ほどデータの流通があまりこのユースケースだとないと言ったが、単に自分の検査結果を誰かに証明するのみならず、**その試薬を提供した会社に実際に私のデータを公開していい、悪いとか、政府がいろんな統計データを公共の利益のために取りたいとか、後々病院に行ってやはり病気だって分かったり、やはりコロナが後から陽性だって分かったりした情報も、後々試薬会社に提供できるとかやっていくと、自分の名前までいいのか、年齢までいいのか、性別までいいのかとか、そういう公開する情報の範囲とかもコントロールできるようになるので、そうなると、Trusted Webで検討しなければならない様々な要素が入ってきていい**のかと思って、幅が広がると思った。
- ✓ 個人のCOVID-19の確認を、国をまたいだ移動のときに使うのは非常に大切だと思う。そこからさらに進んだときに、診断をした医者の人ももちろん、診療を行うために医者の知見も、医者が使った試薬も、その人がCOVID-19に感染しているかいないかの判断には影響を与えており、一定のデータの権利のようなものを主張できる可能性があるのではないか。**例えばある試薬に関して、フォルスポジティブだとか、疑陽性だとかが出てくるような場合は、試薬の問題だとか、どういう人に対して試薬は誤判定としてしまったのかを改善するためのデータとして重要な材料になるのではないか。**そこからさらに発展させたときに診断をした医者がデータをどう利活用するか、さらに使った試薬の製薬会社がどういうふうな**データの使い方**の議論ができるのかへ広がるとさらに面白い話になるのではないかと感じた。

# ユースケース分析の概要(メディアコンテンツ)

○閲覧者(B)から見て、データのやりとりのスキーム(D)を介在して拡散（改変)されて閲覧するコンテンツが、オリジネーター(A)による「真正」なものであるか或いは二次利用者(c)が改変していることがわかる等のTrust、介在するスキームDへのTrustがポイントとなる。
○各ステークホルダーが特定できるのみならず、コンテンツ自体についても識別される仕組みも必要となる。また、ステークホルダーの中でもインセンティブは異なり、特に悪意のあるプレイヤーを前提とした異常系に対応する仕組みをどう構築するかなども論点。

## 基本的なステークホルダー間のTrust



**【支える仕組み】**

- ✓ **適格性判断をアビューズされると困るケースがあり、どう対応していくのか重要。例えばPKIは明らかにアビューズされていると考えられる。**恐らくは信頼関係のモデルという意味では似たような形になると思うが、結局PKIでできているはずのことができなくなってしまっている理由の一つは、ラ**ンダムに証明書を発行する、安い価格でオペレーションして、ロークオリティーのセキュリティで運用するという人たちが出てきてしまったのが良くなかった点の一つ**。もしくはガバナンスの問題で言うと、ガバメントのPKIの証明書の問題というのもある。
- ✓ 適格性判断のお話と、情報をどこにおいて、どうコントロールするか、DNSを本当に信頼していいのかといったご指摘は近いところにあるかもしれない。すなわち、分散アーキテクチャそのものをいかに安定させていくのかに関係するかと思っているが、**トラストレスの状態をアーキテクチャとして執行するときに、本当にそれが系として安定し続けられるのか、トラストレスという、つまりトラストの分かち合いが本当に機能し続けられるのかということは、原理的にはもう少し考えていかなければならない。**実装の成熟を含めて、現実問題としてどこまで普及しているのか、コンセンサスが得られているのかも含めて、評価していくということになるだろう。
- ✓ テクニカルな話で、**情報をどこに置くかという点と、アクセスコントロールをどうやるのか常に気になっている、IPFSは一つのソリューションだが、誰が情報を保管して持っていて、どのように安全に保つのか、担保がどうできるかということについては、非常に注意をしなくてはならない。**今回のユースケースだけの話ではなく、気になるところ。DNSについては、そんなに信用しているかといった話があり、後でSlackにスタティスティックスのページを掲載しますが、DNSセックが使われていない現状においては、一定以上リスクがある。そのリスクに対応した上でDNSを使う形にできると良いと思った。
- ✓ ユーザというステークホルダーとトレードオフの関係を考えるためには、全体として、有形無形問わず、どういうアセットが実際取引されてるのかということを分析する必要がある。アセットというのはお金だけではなく、ユーザのネット上の行動の情報や、あるいは投票にリンクするなど、リアルな行動もそうだし、時間をどれぐらい食うかっていうことも、有形無形のアセットがある。**一般利用者が、実は何かをただで提供してたり、あるいは何かを売らされていたりといったことの分析ができて、きめ細かく扱えるアーキテクチャになっていないと、この問題は解決とは言えず、**よくはならない。その辺の要素を分解していく必要があるだろう。**どういう売り買いがフェアなのか、フェアトレードの定義は時々で変わる。**プラットフォームの在り方によっても変わるので、何がフェアかっていうのは、時代によって変動する。それはそのときのゲーム設定であり、**動的にゲームが設定できるようになっていて、その時代に合わせてどういうゲームを設定するかっていうのは、快適にしていくようにする必要**があるだろう。
- ✓ 管理者主体に依存することなく自身のコンテンツであれ、アイデンティティーであれコントロールできる必要は非常に強く感じた。その上で、トラストレスという言葉を使われてたが、トラストフリーというほうがいいと個人的に思う。トラスト自体は悪くなく、その**管理者主体をトラストしなければ**取引自体が成り立たないことが問題だと思うので、**トラストがなくても、トラストに依存しない取引ができることが、今後アーキテクチャを設計する上で重要。**
- ✓ ユーザ視点は非常に大事。**DNSについて、検証可能性や透明性が現状ないので、自分のデータならびにアクセスがどう管理されているのかがユーザ視点では分かりにくい。**
- ✓ DNS的といったときに、運用、システム、系全体を健全にするために、**運用する人と運用方針を決める運営をする人が恐らく出てくるが、運用と運営という意味で、その辺のステークホルダーが微妙に違ってくる**と思う。その点に関しては、もう少し深く議論したいと思う。
- ✓ DNSのようなものであれば、技術的にセキュリティ担保が可能で、証明書機関の安全性など、mozilla等の確認できる団体組織があり形になるが、**対象がWebコンテンツと幅広くなると、トラストアンカーが系全体の信頼性を担保するので同じ基準で執行されることが必要という部分については、この基準の統一化ができないかもしれないことは意識しなければならない**。また、DNS的なシステムと言いつつも複雑化するかもしれない。DNSはゼロイチで大丈夫か駄目かだが、そうではない形のものを含める工夫が必要そうだ。
- ✓ アーキテクチャでDNSのようなアイデアは、分散指向を考えるときにいいと思っている。**一つの例としてIPFSを考えてみると、これはプロジェクトとして所有されてるものではなく、パブリックに所有されてるようなプロトコル**ということになる。簡単に言うと、データのハッシュ値をアドレッシングに使っている。そのため、データの中身が変わってしまうと、そのアドレスには辿り着けなくなり、その結果本物だと証明するのに非常に役立つ仕組みがあり、それをファイルシステムとして全世界にノードが立っているので、活用するのも有りだと思う。
- ✓ **IPFSについて、どれくらいのものをどのようにスケールさせていくのかに関係してくる。**今の時点では、もちろんフリーハンドで議論をしていくということと同時に、どのステップを踏んで、どのようなデザインをしていくのかということに、そのタイミングで何が一番適正に使えるものなのかということの評価を併せてしていくということなのではないかと思う。

**【機能をシステムとして実装する際に必要なこと】**

- ✓ 最初にユースケースの現状、メディア全体の価値毀損について、情報がスキューで歪んでいる状態が何故起きているのかの根本を考えたときに、一つは恐らく政治的な力というのが相当あって、例えばニューヨーク・タイムズではロシア政府によるディスインフォメーションをかなり特集していた。もう一つは、経済的なインセンティブが非常に大きい。要するにビジネスモデルそのものが広告モデルに依存し過ぎてしまって、そのアテンションをKPIとして最大化して利益を生む構造になったので、プラットフォーマーもそっちの方向を推し進めるし、コンテンツの作成者も利益を得ようとして、何とかして注意を引こうとして、過激なコンテンツばかりになってしまった**。経済的な力がこの価値毀損に非常に関係してくる**のかと思っている。
- ✓ 今のメディアやSNSにある一番大きな問題と考えているのは、単に広告ビジネスだけではなく、社会的インパクトとの関係。例えば大統領選挙とか、エコーチェンバー効果の話との関係は、広告に関するビジネスモデルや、どのようにお金が流れるかと極めて密接な関係にある。ウェブという技術だったり、その上に乗るメディアに直接関係する話なので、**ここの問題にアクセスできる透明性や、何らか第三者検証の仕組み**が得られるのかというのは、結構重要な話だと思う。
- ✓ 今のウェブの形は誰もこうしようとビジョンがあったわけではなく、**お金のインセンティブ設計に従ってたらこうなってしまったところ**もあるかと思う。既存のウェブを乗り換える、もしくは上に作っていく、作ったものをユーザに使ってもらうインセンティブ設計をどうしていくのか含めて今後議論したい。
- ✓ 解決に向けたアプローチで変えたいと思ったのは、**別の方法による経済的インセンティブ付けとして、マイクロインカム等の何らかの方法で、広告に偏ってたものをそうではないビジネス**が成立するような環境ができるといいと思った。
- ✓ **広告モデルに過度に依拠している根本的な問題は、恐らくこのアーキテクチャだけでは解決できない**。産業の在り方として、そもそも考えなければいけないと同時に、サブスクリプションであるとか、伝統的なビジネス、リカリングも含めたビジネスモデルと共存できるような状態を作っていかなくてはならないと思っている。それぞれのビジネスモデルがパラレルに存在してる状態で、お互いが共存できるものを執行する、その配慮や丁寧さを持つということが、必要になってくるのではないか、とのご意見と理解した。
- ✓ コンテンツ自体の問題、課題の話と、ウェブ広告の世界、エコシステムの中での課題とが混ざっていて、その中で、アプローチであったり、課題解決というところもミックスされたような状態で入っているので、どちらに主眼を当てるのかを明確にされたほうがいいのではないか。ウェブ・コンテンツについて、例えば**オリジナルを特定できればそれでいいのかというと、意外にそうでもなく、例えばコンテンツ・ロンダリングのような形で、一見正しく権利者から権利を受けて使っていても、権利者自体が悪意を持って、不正な形で、勝手に私がオーナーだと宣言したような状態で他の人に販売している**。これは特に海外、日本の中での使い方ではなく、日本のコンテンツが海外で使われてるときに、コンテンツ・ロンダリングされている、その逆の事例も多々あるのではないか。グローバルの観点だと、その著作権法的な意味で、日本と同じような考え方で著作権の考え方を持っているような国ではない所にサーバーを置いてといった話もよく聞く。グローバルな観点まで含めてどう扱うべきなのか。抑止力がないことが今の問題。**DRMやソーシャルDRMがあったとしても、アナログコピー等のそれを破る方法で持っていかれたらどうするのか。**解決が容易ではない課題感を感じている中で、どう扱っていくべきなのか議論が広げられるといい。
- ✓ メディア関係においては特に、**誰がこのコンテンツにアクセスしたかとか、どうやってアクセスしたかとか、アクセス側の記録は非常に重要になってくる**と思う。そのようなツールは一歩間違えるとプライバシーとの問題が非常に難しいが、**ユースケースを考えるときは、プライバシーとの兼ね合いも議論の対象**になると感じた。
- ✓ 全体を簡単にまとめると、幾つか共通した論点があった。一つは、**適格やフェアであるとは一体何なのか。**それが非常に相対的かつ時代によって遷移する概念であり価値観であるところ、スタティックに決めきってしまたり、あるいはエンフォースメントのような形で振りかざしてしまったりということが、そもそも求めているものなのか、あるいはそれが解決策として有効なのかとの指摘があった。言葉の使い方の問題もあるが、**マッチングであると指摘**があったのは、まさしく我が意を得たりのようなところがあり、いかにメディアであれ、パブリッシャーであれ、コンテンツメーカー、ライターのような人たちであれ、ユーザであれ、自分のビヘイビアや状態、欲しいものを表現できるとしたら、それを組み合わせることによって最適な状態を表現できるのではないかと思う。
- ✓ ただし一方で、**それが何であるのか、表明されているものが本当に妥当なものなのか、少なくとも誰かがうそをついていないかというようなことをどのように確認していくのかということが、トラストを考える上で重要なポイントとして指摘されている**。それは単にアーキテクチャで解決できる問題だけではなく、主体がどのように存在しているのか、既存のビジネスモデルとどのように接合しているのか、どういうふうに立脚しているのかが、視野に入っていなければどこかで理論が抜け落ちてしまっている状態になるのではないかという指摘もある。

**【機能をシステムとして実装する際に必要なこと（続き）】**

- ✓ **適正性や、トラストをどのように考えていくのか、アーキテクチャで表現できるところ、できないところはどこなのかということがこのTrusted Webの観点**で、一つアジェンダとして出てくるところではないかと思った。
- ✓ 適正性の話をすると、適正性と言葉にすると、いかにもスクリーニングして、駄目なものを排除していくようなニュアンスが日本語としては非常に強くなってしまう。とりわけ適格と言ってしまうと、その資格がない者は出ていけというような聞こえ方をしてしまうが、やはり私は**マッチングの問題**だと思っている。メディアはメディアで、それが例えばイデオロギーやジェンダーの観点から好ましくないとしても、世の中に存在が許されている。それこそ条件を課して存在が許されているのであれば、それはそれで尊重しよう。**そこに対して、存在は許すが、そこに出稿するつもりは全くなかったとか、それを見にいくつもりは全くなかったとかのミスマッチが発生するということをできるだけ避けていきたいということが、まず入り口**としてある。広告業界が言っている、アドフラウドであるとか、ブランドセーフティだとかの観点の話。これ自体は既に問題として提起され、解決しなければという状態にあり、何と何がよりベストマッチというか、ベストミックスな状態になっているのかということを考えることが、今、申し上げたかったことの言葉の真意。
- ✓ 「そこにユーザは関与できなさそうな雰囲気を受けてしまう。」の問に対し、ユーザも一部関与するが、**ユーザだけで全てを決めるということが必ずしも成立しないのが、メディア分野の難しいところ**。ポルノなどがまさしくそうで、そもそものレギュレーションや、この分野に関しては、ユーザはむしろメディアの姿勢に付いてきてくれるかどうかあらかじめ選んでほしい。情報メディアの場合は、メディアの姿勢であるとかによって選択してもらうことを認めなければ、表現の自由に抵触するところが実は結構難しい。そういう意味でも、難しい状態のままユーザを識別して、巻き込んでいくことからは私は少し距離を置いたほうがいいと思う。

**【必要な機能】**

- ✓ 適正な広告マッチングのような発言があったが、解決する課題という点で、できればユーザによる再生産による被害拡大の低減、ユーザがどんどんフェイクニュースを拡散してしまうことに対して、**後々これはフェイクニュースだと分かったときに、拡散したものは消せるような課題解決手法を、できればこのTrusted Webの中でできないか**と思った。
- ✓ 適格性を有した広告主を特定するためのトークンの発行について、これはメディア側の視点で広告主が適正であるかどうかだけが重要であるだけでなく、逆に広告主側の視点でパブリッシャーやコンテンツが適格性を有しているかも重要であり、**実は適格性というのは相互**ではないか。さらに適格なのかどうかは、絶対的なものより相対的なものではないか。例えばポルノ広告を出す人からすると、ポルノ系のコンテンツの所にその広告が出ても構わないわけなので、**これは適格性という言葉ではなく、恐らくこのコンテンツや広告主がどのような性質のものなのか特定しておいて、お互いの性質同士のマッチングテーブルがあるというのが解決策**ではないか。
- ✓ まさしく相対的であってマッチングの問題であると私も考えていて、そういう方向で作るべきだと思う。ポルノメディアにはポルノの広告が載ることは、そのポルノの内容はさておいたとしても、マッチングの関係においてはフェアである。こういうものをどのように整理させていくのかということだと思う。取引条件を公開と申し上げたが、条件公開というよりは、取引が本当にフェアに行われているっていうことが確認できる状態をつくるということが重要だと思う。
- ➢ ユーザの再生産の被害拡大をどのように防いでいくのかはプライバシーと抵触する話でもあり、大きな課題まで落とし込めていない。一つの考え方として、ユーザそのものの特定ではなく、**ユーザが間違った使い方をされている状態をシステム全体としてできるだけ把握できるような状態を作る**。そのために**パブリッシャーやコンテンツそのものにアイデンティファイヤーを付けて、これは適正な使われ方をされていないことが分かる状態を明らかにすることがファーストステップ**と考えている。

参考

# 関連する標準化等国際団体リスト

※協議会委員・タスクフォース委員から協力をいただき、整理中の途中版。今後改訂予定

# （参考）関連する標準化等団体　①インターネット等全般

| 国際フォーラ | 国際フォーラの概要 | Trusted web関連の所掌 | 規格化など類似の動き | 議論状況とスケジュール |
|---|---|---|---|---|
| ISO/IEC | デジュール標準を作成する国際標準化団体 | • ISO/IEC JTC1 SC27/WG5（Information Technology, cyber security and privacy protection - Identity Management and Privacy Technology）<br>• ISO TC307 (Blockchain and Distributed Ledger Technology)<br>• ISO/TC 307/WG 05 (Governance)<br>• ISO/IECJTC 1/SC 17 (Cards and security devices for personal identification)<br>• ISO PC317 (Consumer protection — Privacy by design for consumer goods and services)<br>• ISO/TC 68 (Financial services) | JTC1 SC27/WG5における Identityのフレームワーク、プライバシに関するフレームワークなどは参考になる | JTC1 SC27, TC307ともに年2回の会合を実施。<br>TC307においては、Identityに関するIS（国際標準）までは作成しておらず、現在はTechnical Reportに止まっている。<br>複数のTR（Technical Reports）が来年頭に発行予定であり、Blockchain Governance, Trust Anchorsにまつわる2つが特に重要。 |
| World Wide Web Consortium（W3C） | Web技術に関する仕様策定と促進、新技術のプロトタイプ実装を進める国際標準化団体。全世界で四つの組織（MIT, ERCIM, 慶応義塾大学, 北京航空航天大学(Beihang)）によってホストされており、慶応はホスト組織の一つ。 | Decentralized Identifier WG、Verifiable Credentials WGV、その応用についての議論が行われているCredentials Community Group (CCG) が中心 | 分散型のID識別子、データモデル、検証可能な資格情報のモデルなどを議論 | Verifiable Credentials のデータモデルについては、2019年にW3C勧告となった。Decentralized Identifierに関しては2021年中ごろのW3C勧告をめざし、勧告候補文書の明確化に向け議論中。<br>教育関係のVerifiable Credentialについての標準が進められる見込みで、慶応はその部分に関わる予定。仕様としては来年には使われるようになるが、リコメンデーションなどになるまでは、時間がかかると考えられる。 |

# （参考）関連する標準化等団体　②ガバナンス、通信、Trust

| 国際フォーラ | 国際フォーラの概要 | Trusted web関連の所掌 | 規格化など類似の動き | 議論状況とスケジュール |
|---|---|---|---|---|
| Internet Governance Forum(IGF) | インターネットガバナンスの問題に関し、マルチステークホルダー（政府、企業、技術、学術、市民など）間で政策対話を行う、国連管轄下に設置されているフォーラム。 | IGF2020（2020年11月開催）では「データ」「環境」「インクルージョン」「信頼」の4分野を重点テーマとし、200を超えるセッションを開催（村井純教授も参加）。コロナ禍における信頼の概念について政府間で議論するための専用のラウンドテーブルが設置され、日本政府もPromoting Trust on the Internet through Osaka Trackなどを設置。 | | IGFは2006年の第1回以来毎年秋に開催（IGF2020は15回目） |
| Internet Engineering Task Force (IETF) | 通信路を通るプロトコルを中心とするインターネット技術の標準化団体。標準化文章をRFC (Request for Comments)として発行。現在は年3回のペースで会議を開いており，2020年11月までに109回の会議が開催された（うち3回が日本開催）。標準化会議への参加は，企業単位ではなく，個人単位で行われる。 | インターネット技術はTrusted Webに必要不可欠であり，通信プロトコル以外に通信の暗号化などのセキュリティ機能を提供するTLS (Transport Layer Security) なども標準化している。また，国際的な基盤運用の要となる標準化会議であり，その運用形式はTrusted Webの運用においても大きく関係すると考える。また，インターネットは自律分散協調システムとして発展してきており，マルチステークホルダーでの技術開発・運用はICANNやIANAなどの運営が参考になると考えられる。 | 昨今のセキュリティ・プライバシーへの要求に伴い，DNS (Domain Name System)などのコア技術に対し，DNS over HTTPSやDNS Privacy Extensionなどプライバシー保護技術の標準化が盛んに行われている。 | コミュニティベースでの標準化活動のため，3GPPなど他の標準化団体ほど厳密なスケジュール管理はされていないが，上述の通りセキュリティ・プイライバシー保護技術の標準化は随時行われており，新しい標準化ドキュメントを寄稿する際はセキュリティへの懸念事項等を必ず記載することになっている。ドキュメントを書く際に必ず検討をする項目を原則として入れておくことは重要。 |
| Rebooting Web Of Trust (RWOT) | 2015年から行われている、Web of Trust 視点でのワークショップ（リーダシップを取っているメンバとW3C DID WGやCredentials Community Group(CCG)の参加者とオーバラップが大きい） | | | |
| World Economic Forum（WEF） | 官民両セクターの協力を通じて世界情勢の改善に取り組む国際機関。毎年１月にスイス・ダボスで年次総会を開催。 | Global Technology Governance Summit (GTGS) において、第四次産業革命に関する新たなテクノロジーの責任あるデザイン及び実装を、官民連携を通じて実現する方策を議論。 | | |

# （参考）関連する標準化等団体　③ID

| 国際フォーラ | 国際フォーラの概要 | Trusted web関連の所掌 | 規格化など類似の動き | 議論状況とスケジュール |
|---|---|---|---|---|
| OpenID Foundation | データ主体の同意などに基づく選択的属性連携（デジタルアイデンティティ、認証連携、KYCなど）およびデータのAPIを通じたアクセス制御に関わる国際規格の作成、認証、普及啓発活動を実施。<br>崎村委員が理事長を務める。 | 属性情報および付随するTrust関連情報の伝達のためのプロトコルの作成と実装の準拠性の確認手段の提供。 | • AB/Connect WG（elf-issued OpenID Provider ver.2、Claims Binding for OpenID Connectについて新規追加）<br>• FAPI WG（より安全性の高いAPIアクセス制御のための規格として、FAPI ver.1 作成）<br>• eKYC & Identity Assurance WG（金融機関の口座開設時のKYCなどに使うことができるための、追加属性およびそれらがどう確認されたかなどを表すメタデータを表現するためのデータフォーマット規格の策定）<br>• Shared Signal & Events WG（ドメイン間でセキュリティ・イベント情報を共有するなどによって、リアルタイムにセッションの質を評価する（継続的認証, continuous authentication）ことを助けるためのプロトコルの策定）<br>• その他、電子政府、ヘルスケア、教育などの分野別規格の策定が進んでいる | • AB/Connect WG: OpenID Connect関連仕様群のメンテナンスおよび新規の追加仕様を検討中。<br>• FAPI WG: FAPI 1.0 は来年１月初旬に最終版発行見込み。<br>• eKYC & Identity Assurance WG: 現在、自然人に関する3rd Implementer's Draftの策定中。 |
| Decentralized Identity Foundation (DIF) | DIDに関連する標準をW3C外の場で議論する場（W3Cでの標準策定にはW3Cメンバでないと参加できないが、DIFの場合はそのような制約が無い） | 複数のデータモデル間の互換性(JSON - JSON-LD)、プライバシーの保護あたり | | 個別企業が標準を持ち込んでいるものがあり、その部分については、現在のDID技術に関連した仕様と合わせて見ながら注視する必要 |
| Trust over IP foundation (ToIP) | DID を中心に据え、インターネット上に信頼を構築を試みているコミュニティ | | | |
| Internet Identity Workshop (IIW) | 2005年から、毎年2回、サンフランシスコベイエリアで行われているインターネット上のアイデンティティ技術についてのワークショップ | | | |

# （参考）関連する標準化等団体　④Blockchain

| 国際フォーラ | 国際フォーラの概要 | Trusted web関連の所掌 | 規格化など類似の動き | 議論状況とスケジュール |
|---|---|---|---|---|
| Polkadot | パブリックブロックチェーン業界における異なるNetworkおよびブロックチェーンとの相互運用性確保の規格化を検討 | ミッションをWeb3.0の実現としており、Trusted WebとはVisionの方向性は一致。また技術スタックも参考になるものが多い。 | 異なるブロックチェーンを接続する際の、ブロックチェーンの要件を規格化する動き（ブロックチェーン間のトークンおよびデータの移転をどのように行う） | 異なるブロックチェーンをシームレスに接続する実験が現在テスト環境で行われている。2021年上半期を目処に本番環境で実験予定。 |
| International Association for Trusted Blockchain Applications (INATBA) | 欧州委員会が設立した、ブロックチェーンを推進する国際標準化団体 | ブロックチェーンを利用したトレーサビリティ | | |
| Blockchain Governance Initiative Network (BGIN) | ブロックチェーンの技術、運用に関する標準等の文書を作成するマルチステークホルダー会議体 | Identity, Privacy and Key Management WGにおける議論 | Identity, Privacy and Key Management WG: KYCとプライバシの関係の議論など | 年3回のGeneral Meeting、隔週のWG Meeting |
| OECD Blockchain Expert Policy Advisory Board (BEPAB) | ブロックチェーンに関する原則を検討 | プライバシーに関する原則 | | |

# （参考）関連する標準化等団体　⑤分野別等

| 国際フォーラ | 国際フォーラの概要 | Trusted web関連の所掌 | 規格化など類似の動き | 議論状況とスケジュール |
|---|---|---|---|---|
| Institute of International Finance (IIF) | 主に金融機関におけるTrust確立を、Governance面および技術面から検討 | Open Digital Trust Initiative | | |
| Automotive Edge Computing Consortium (AECC) | インテリジェントドライビングやコネクテッドカーなど，インターネット技術を活用した自動車産業に関する仕様策定を行うコンソーシアムである。企業単位で参画する形式を取っている。 | 自動車は製造過程から利用シーン，修理や中古車の流通までにおいて多量のデータを扱う一方，そのデータの一部は営業秘密やプライバシーへの配慮などが必要であり，Trusted Webのひとつのユースケースとなり得る。 | | |
| Gaia-X | 独仏産業界が主導する、欧州データ主権の実現にむけたデータ共有インフラ構想 | トラステッドなデータ共有のためのデータインフラアーキテクチャ | | |

参考

# 前回資料からの抜粋

# デジタル市場競争に係る中期展望レポート概要(Trusted Web関連)①
# 2020/6/16 デジタル市場競争会議

**1. 問題意識:**
サイバーとリアルが融合する**Society5.0におけるデジタル市場のあり方**について、ビジネス動向、市場環境、テクノロジーの動向等**多角的な視点から、**将来のリスクを見通しつつ、多様なイノベーションによりデジタル化がもたらすメリットを最大化できるよう、**ダイナミックな競争が行われる市場をどう構築していくか**との観点から、提言。

**2. デジタル市場を巡る現状**: 現状のサイバー空間を中心としたデジタル市場について、**メガ・デジタル・プラットフォーム（以下「メガPF」）の強みと今後の動き**を分析。
強　　み： **強い顧客接点**（ネットワーク効果で利用者をロックイン。顧客接点を活かしてデータ収集、AI等で分析して、顧客に新たな価値を提供）
今後の動き： **３つのベクトル** **①顧客接点の拡張・深化**（身体の近くへ、意思決定の近くへ）、**②リアル分野への進出**、**③上流への進出**（仲介だけでなく、自社製品・サービスを販売）

**3.今後のデジタル市場のリスク**: メガPFの動きに加え、リアルとの融合からくるものも含め、今後、以下の**４つのリスク**に直面。
メガPFの動き → **①勝者総取りの懸念**、**②個人の判断すらコントロールされる懸念**
リアルとの融合に伴うリスク → **③データの信頼性の欠如**（自動運転やヘルスケア等ではデータの出元や履歴などの信頼性がより重要に）、**④IoT進展に対応できないデータ処理とコスト**

**4. 今後目指すべき方向性: デジタル市場のダイナミックな競争によるイノベーションがSociety5.0を加速化し、より豊かなものに**
◆**デジタル市場の目指すべき姿**： “一握りの巨大企業への依存” でも、“監視社会” でもない **第三の道へ**

1) **多様な主体による競争**　2) **信頼（Trust）の基盤となる「データ・ガバナンス」**　3) **「Trust」をベースとしたデジタル市場の実現**

◆その実現に向け、短期、中長期の視点を持ちつつ、①ビジネス環境、②ルール、③テクノロジー等の多角的な視点から、状況の変化に柔軟に対応しつつ、以降の３つを進める。

(①DX、②ルール整備について省略)

# デジタル市場競争に係る中期展望レポート概要(Trusted Web関連)②

## ③データ・ガバナンスのあり方をテクノロジーで変える分散型の"Trusted Web"　（中長期）

**<現状の課題>**

・現行のインターネットの構造では、**メガPFが中央集権的にデータを管理・利用**。
　（**データがどのように使われるかは利用者から見てブラックボックス　→「信頼」（Trust）の欠如**）
・信頼（Trust）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。
・こうした状態に対し、**法律や契約による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的に担保**することが求められている。（世界では、一部のエンジニアがそれを目指す動きも）

**<対応の方向性>**

●「**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」　**（"Trusted Web"）**　を構築

- 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**
- デバイス間で自律的にデータがやりとりされ、人間がほとんど介在しない**IoT社会にも対応**

（考えられる技術要素の例）
特定のPFや国家が中央集権的に発行・管理するのではなく、個人・法人自らが発行・管理して自らのデータを管理できる分散型ID、改ざんが困難でデータの履歴を透明化するトレサビリティ、特定のPF等のサーバなどの場所に囚われずに分散的にデータが保存・管理される仕組み、中間事業者を介さない直接取引を容易にする仕組み（P2P取引）、クラウドと連携してデバイスあるいはデバイス近傍でデータを効率的に処理するエッジコンピューティング　等

**（当面１年間のアクション）**

新たな構造への移行は急激に起こるものではないが、**将来のデータ・ガバナンスの構造を描きつつ**、人々のニーズやビジネス・ニーズに応じて**ユースケースを積み上げ**、**「信頼」の構築において**、**グローバルに連携**しながら、**日本が技術とビジネスをリード**していく。

◆**内外への発信**（**DFFT**-Data Free Flow with Trust **の具現化の一つ**）、**内外のネットワーク形成**
◆**官民の推進体制**を立ち上げ、将来実現を目指す**データ・ガバナンスの構造設計**、その際に**必要となる要素**やそれを実現する**技術の抽出・課題検証**、**移行のためのロードマップ等を策定**
◆提案公募等を通じた**先行ユースケース分野の特定**、**技術・ビジネス・制度上の課題抽出、課題解決に向けたロードマップ等を策定**　（データ・ガバナンスの構造設計の議論と連動）

# 「ホワイトペーパー」の項目イメージ例

**1.背景と課題認識**
○ニューノーマルと新たなインターネット文明の調和
○今のインターネットとWebが達成していること/解決できていないこと

**2.ビジョン・全体の将来像**
○ビジョンの提示
デジタルテクノロジーによる豊かな「ニューノーマル社会」の実現（仮説）

**3.重要な構成要素としてのTrust**
○Trustの定義
○Society5.0時代に目指すべきTrustの方向性

**4.Trustを実現するためのアーキテクチャー**
○アーキテクチャーの設計に必要となる要素
○アーキテクチャ設計の前提となる要件
○必要なガバナンス・インセンティブ設計

**5.実現に向けた道筋**
(1) 技術面での道筋
○関連する技術とその動向(Web,Data,BC)
○コアとなると考えられる技術の段階的なロードマップ
(2) 実装・需要面での道筋
○当面、期待されるユースケース、関連した動き
○実装に向けた課題
○今後の実現シナリオ

**6.必要なアクション**
○DFFTの具現化としての官民での国際発信
○国際標準化
○産、学、官それぞれの役割分担とアクション
○ユースケース実証・実装　　など

**以下、仮説**

# 背景と課題認識

**デジタル技術の活用の急拡大**（COVID-19を契機に加速）

→ 社会**全体がDX**化する「ニューノーマル」へ
→ しかしながら、以下のような様々な課題が顕在化

＜各レベルにおける課題＞

（①人と人とのコミュニケーションのレベル）
→ 現状のテクノロジーでは、使い手である**人間の活動とは完全に一体化できていない**。(コミュニケーション、感情、信頼、多様な文化など)

（②経済社会活動のレベル）

→ **データがどのように活用されるか分からない**。
（個人の判断すらコントロール、囲い込みの懸念（勝者総取り）、サプライチェーン間のデータ活用も進まず）

→ **データそのものが信頼できるか**。（フェイクニュース、IoT・自動運転・ヘルスケアでの懸念）

（③国家間のレベル）

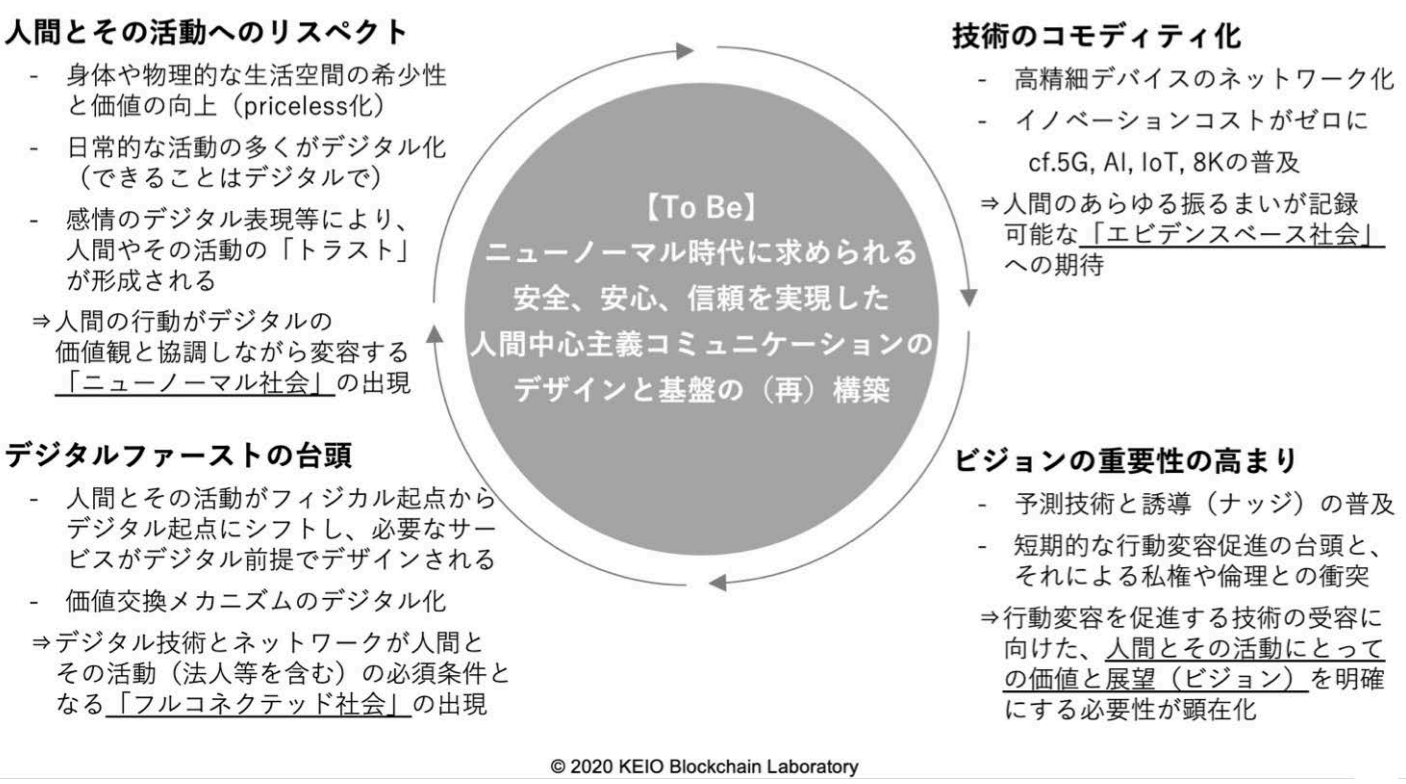
→ デジタル化への移行に当たり、**国家間で考え方、価値観に相違**が発生。分断の危機。

**システム全体を通じた“Trust”の枠組みが構築できていない。**

# ビジョン

## ■ ロードマップ：ニューノーマルと新たなインターネット文明の調和

COVID-19が加速したデジタルトランスフォーメーションの急拡大を踏まえた
人間中心の新しいコミュニケーションデザインとそれに基づく基盤の（再）構築による
ニューノーマル時代の新たな「インターネット文明」の構想とその実現に貢献する






（注）以下は、適宜、「ニューノーマル時代における人間の社会活動を支える情報基盤の在り方とデジタルアイデンティティの位置づけ」慶應義塾大学SFC研究所ブロックチェーンラボ　2020/8/3 version0.1　から引用したもの。

# ビジョンと全体の将来像(イメージ)

フルコネクテッド社会

ニューノーマル社会

エビデンスベース社会

人間とその活動にとっての価値とビジョン

「ビジョン」
ニューノーマル時代に求められる安全、安心、信頼を実現した人間中心主義コミュニケーションのデザインと基盤の（再）定義

エンティティ毎に見た将来像

**国家**

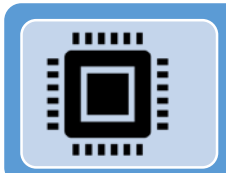
- 価値観の共有

**組織**

- デジタル上で取引完結し、契約もデ

**個人**

- ニューノーマル時代の新たなデジタ



**モノ・情報**

- 膨大なデバイス間で自律的なデー

Trusted Web

Data Free Flow with Trust

# これまでのWebには何が欠けているのか

インターネット：国家を前提としないグローバルなネットワーク、分権型分散ネットワーク
**→イノベーションの源泉**

**「Trust」の問題**

・フェイクニュースなど、やり取りされる**情報/コンテンツの識別や正当性**が不明確

・**相手先の識別や正当性**などトランザクションの確認コストが高止まり

・人間同士の**機微なコミュニケーション**の不可欠な要素が欠落

その背景として、**インターネット自体には、アイデンティティのための仕掛けが備わっていない。**
その結果、**サービス・ドメインごとにアイデンティティ**を用意する仕組みに。
→ データは、ドメイン内で紐づき、保存・利用され、**アイデンティティは、サービス・ドメインに閉じて、ロックイン。**

○インターネットの構造に、デジタルに本来期待されるTrustのみならず、従来の社会システムが担ってきた**Trustすら十分に実装できていない**ことから生じている問題

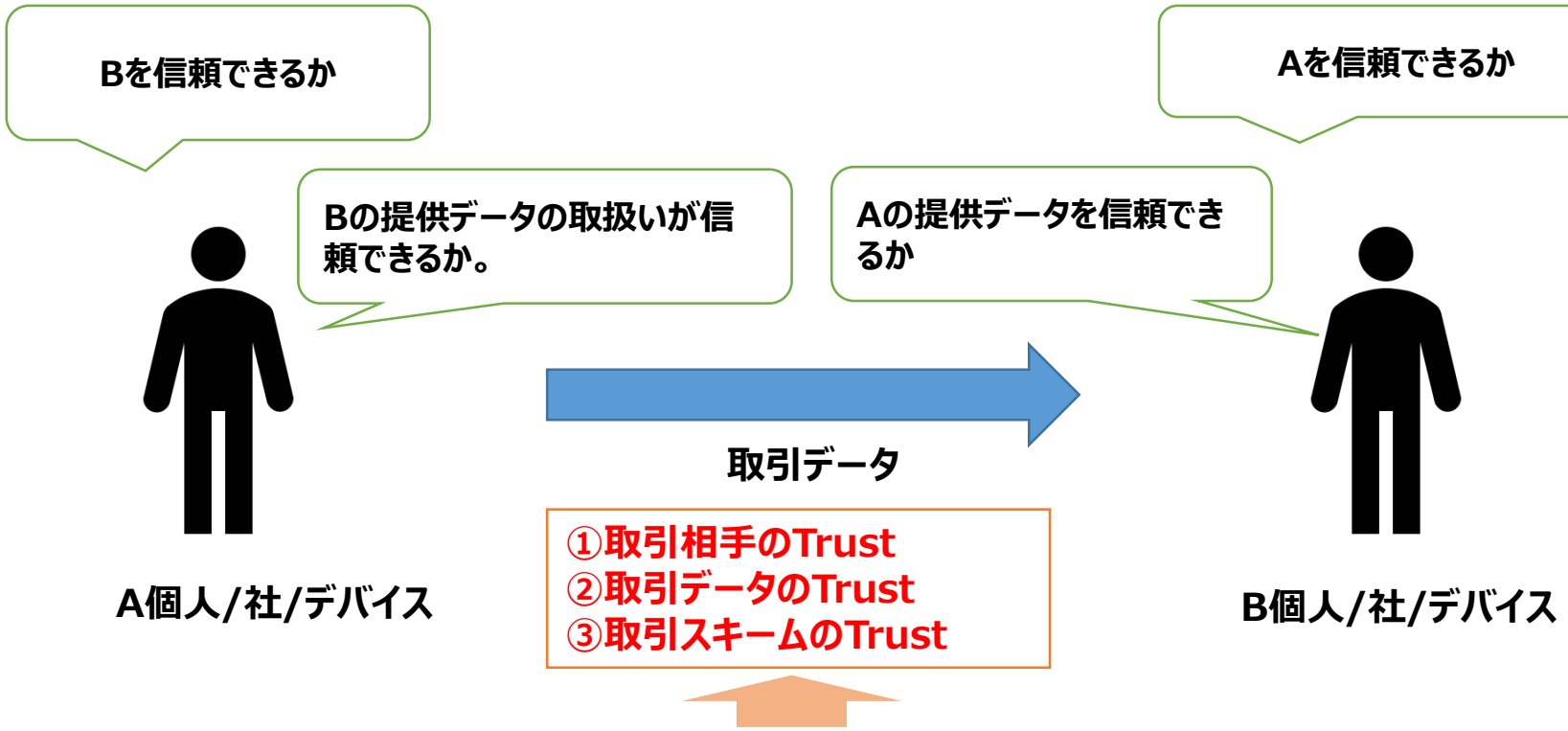
○この**中核として「デジタルアイデンティティ」の確立**が緊急課題

# Trustの定義、目指すべきTrustとは



Trustとは、
・事実の**確認をしない**状態で、相手先が**期待した通りに振舞うと信じる度合**。
・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。
・利用者は**Trust維持コストと問題発生時のリスクのバランス**でTrustできるかを判断。

# 相対取引のTrust



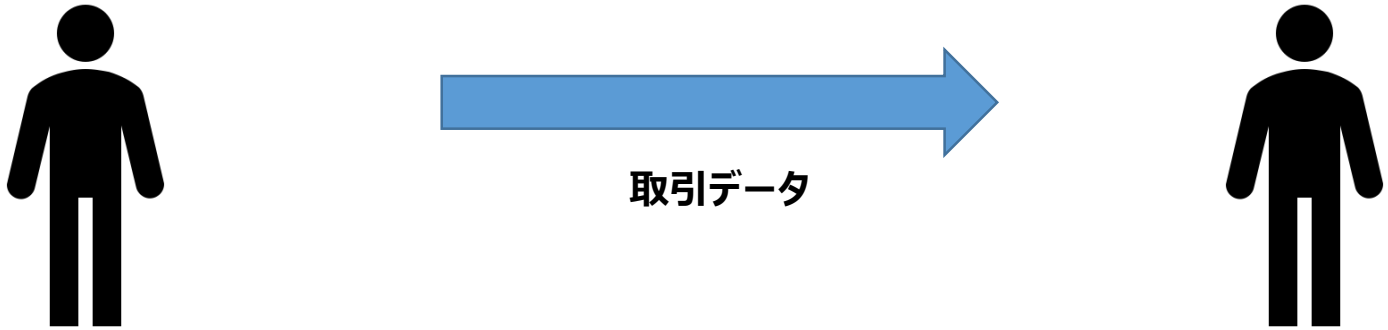

Trustを支えるコミュニティ、社会/取引システム
→法制度、透明性・監査・認証等の仕組み、セキュリティ、これまでの実績(評判)、
技術的枠組み(コード・アーキテクチャー)

# ①取引相手のTrust


○信頼できる人/法人/デバイスか。
・同一か。 Identifier
→何らかの識別子が存在し、複数の識別子が紐づけられている。
・どのような人か。 Identity 氏名、住所、年齢、性別、学歴、職歴、そのほか履歴など属性の集まり
→様々な分散的に存在する属性データが統合管理され、必要に応じて相手に提示。
・それが確かに裏付けられて証明できるか。 Credential/Identification 国、証明機関
→いわゆる「オラクル」問題。
・過去の実績だけでなく、今後の行動についても信頼できるか。
→デジタルでは、相手先の行動自体をコードで一定程度コントロールすることは可能。(→②へ)

# ②取引データのTrust






○取引データがコントロールできるか。

・データが同意を超えて、不正に利用されないか。(正当な理由でデータが利用できるか)
・データを集約するプレイヤーによって、データの価値を不当に搾取されないか、監視されないか。
・悪意の参加者がいたとしても、データが第三者も含めて安全に流通できるか。
・データの利用状況が透明化されるか。
→データ自体のコントロール権限の問題
・データが正しく必要な速度で処理され、伝送されるか。

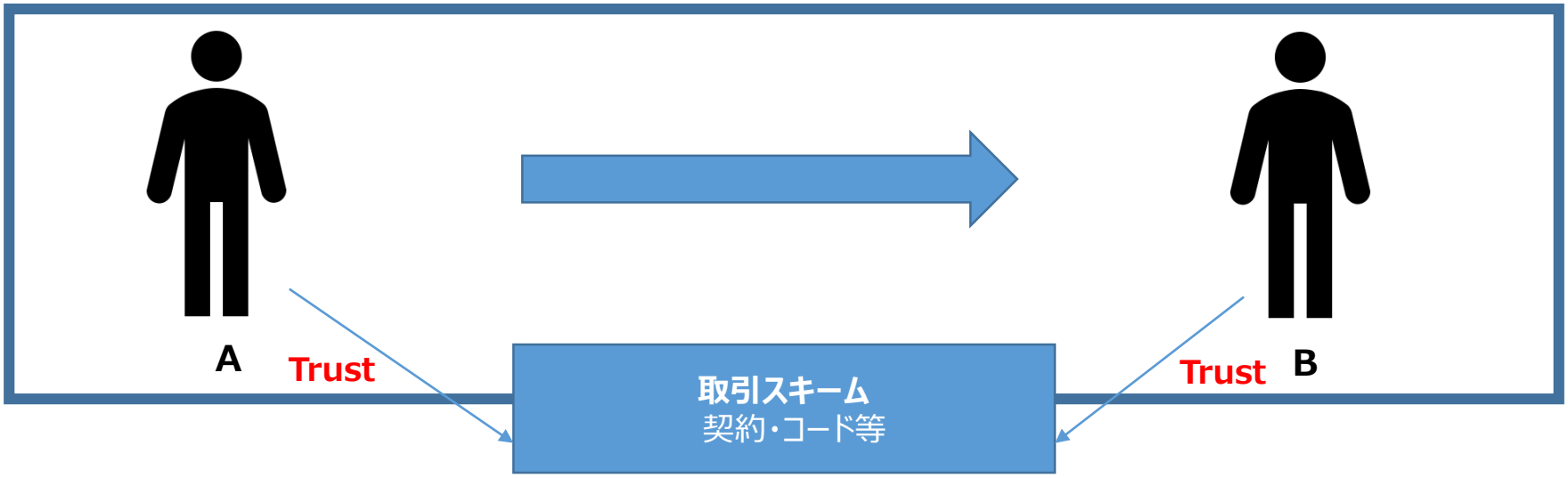
○信頼できるデータか。

・データの出所はどこか。(正しく作成されたものか)
・データの履歴(サプライチェーン)は確認可能か。
・データは不正に改竄されていないか。
・データの利用権限は正当か。
→データのサプライチェーンの透明化の問題
・データが正しく必要な速度で処理され、伝送されるか。

<データの内容>
*これ自体は価値判断となるのでシステム的に完全な担保は難しいため、①の出所たる相手先の信頼で担保されることが通常。
・データの内容が正しいものか。
・データの精度・頻度が利用する価値のあるものか。

# ③取引スキームのTrust






○取引スキームが信頼できるか。
・契約・コード等の実効性が信頼できるか。
等

# 社会システムとしてのTrustの設計

**系としてのTrustを構築するための仕組み**
**・技術の実装、運用ルールの設定と遵守、失敗時の救済手段**
**・自己宣言モデル、第三者確認モデル**

**Trustのためのステイクホルダーの責任分担とインセンティブをどのように組み込むか。**

○オンラインのみでのコミュニケーションに対応し、広義の「コミュニケーション」(トランザクション/やりとり)を**極限まで円滑化**し、**社会システム**としてどのように**最適化**していくか

# ニューノーマル時代の広義の「コミュニケーション」の再構築 (Trustの再構築)

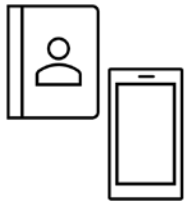
①ゴールの共有

⑤参加者が同じ理解をしていることが常に確認でき、事後的にも検証可能

①は自然言語から落とし込んでプロトコルとして構成し、それが完了するように、構成、設定、管理を自動化する必要

⑤一貫性を保証するレイヤーが必要

送受信データ



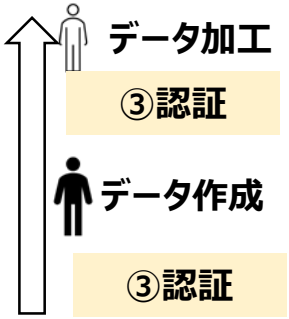
④プロセスの前後関係が特定可能で、検証可能な形で記録

④Permissonless Blockchainで実現可能

エンティティ

②認証

③改竄されていない




エンティティ

②認証

②③インターネットの認証プロトコルの拡張で実現可能

# グローバルデジタルアイデンティティの方向性

現行: 各サービスドメイン毎で閉じたもので、ロックイン構造

(仕組み)

**○人間中心、グローバル、ロックインされない仕組みへ**

サービスドメインからの独立だけでなく、個人によって完全に制御できる、第三者に頼らない方式(自己主権型アイデンティティ- Self Sovereign Identity)の動きも

(エンドユーザーの視点)

**○使いやすく、手間がかからず、制約が限りなくゼロに近い、など…**

・サービスごとに用意されたアイデンティティを作成し、管理する煩雑さからの解放

・特定のサービスに紐づけられたアイデンティティへの利用強制からの解放

・アイデンティティの不適切な管理によって生じるセキュリティリスクの緩和

・アイデンティティ利用の永続性と可用性の確保

・PII(個人を特定できる情報)等が直接的にサービスと結びついてしまうことによって発生しうるリスクの回避

# グローバルデジタルアイデンティティの実現手法



既に実装や検討が進められている構成要素を取り込むことが可能。

**・グローバルな識別子(GID:Global Identifier)は、既に標準化済みで様々なIdentifier技術との読み替えが可能なUniform Resource Identifier(URI)を活用**
→あらゆる名前で区別できるモノとデジタルアイデンティティとの直接的間接的な結びつけが可能に
→必要に応じ、GID間を間接参照とすることで、結びつき変更のためのフレキシビリティが向上

**・W3Cでの分散ID(Decentralized Identity/Identifier)の検討結果を適用**
→自己主権型のアイデンティティの活用が可能+既存のアイデンティティプラットフォーム/サービスドメイン群と連携が可能となる
→GIDとGIDの間の関係性を信頼できる第三者なしに表現できる

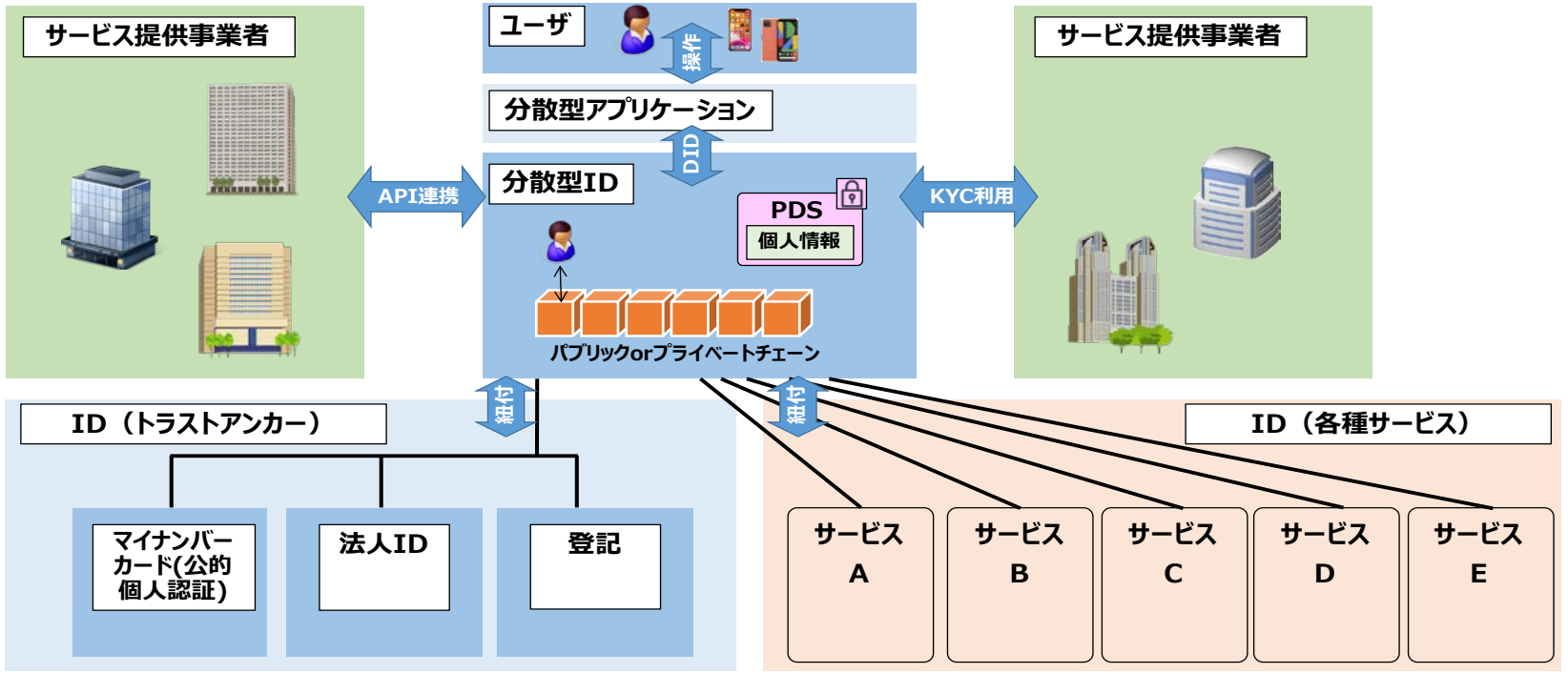
**・複数のID間の関係性と関連するメタデータを表現するため、Verifiable Credential技術を転用・ブロックチェーンを活用**
**・依存関係の記述にあたってはユーザからの直接的な了解をその時点でリアルタイムに得られるようなメカニズムを導入。高い自由度が必要な場合には、代理となるGIDを介在させて間接的な結びつきにする**
→情報の出元で確認が済んでいる情報の伝達が、直接的な結合に頼らず可能となり、システム間の依存関係を最小化できる

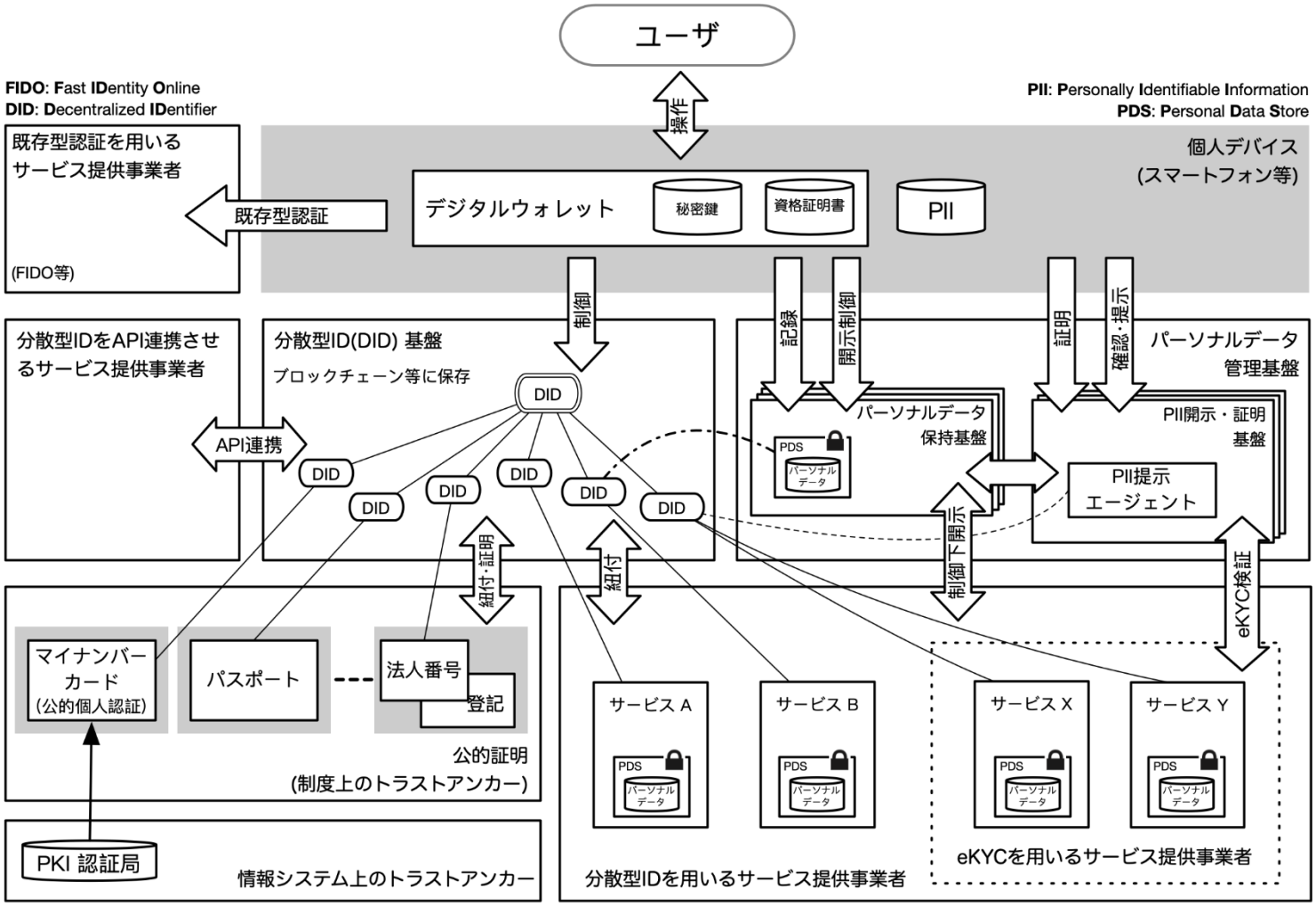
# 分散型ID

（出典）6/16 デジタル市場競争会議資料

## 分散型IDのイメージ

分散システムによりIDが発行される。非中央集権型で個人によるID管理。IDを基にパーソナルデータのアクセスをコントロール。当該IDにトラストアンカー（マイナンバーカード(公的個人認証)、法人ID、登記等）を紐付けることで、各種API接続やKYCに利用。





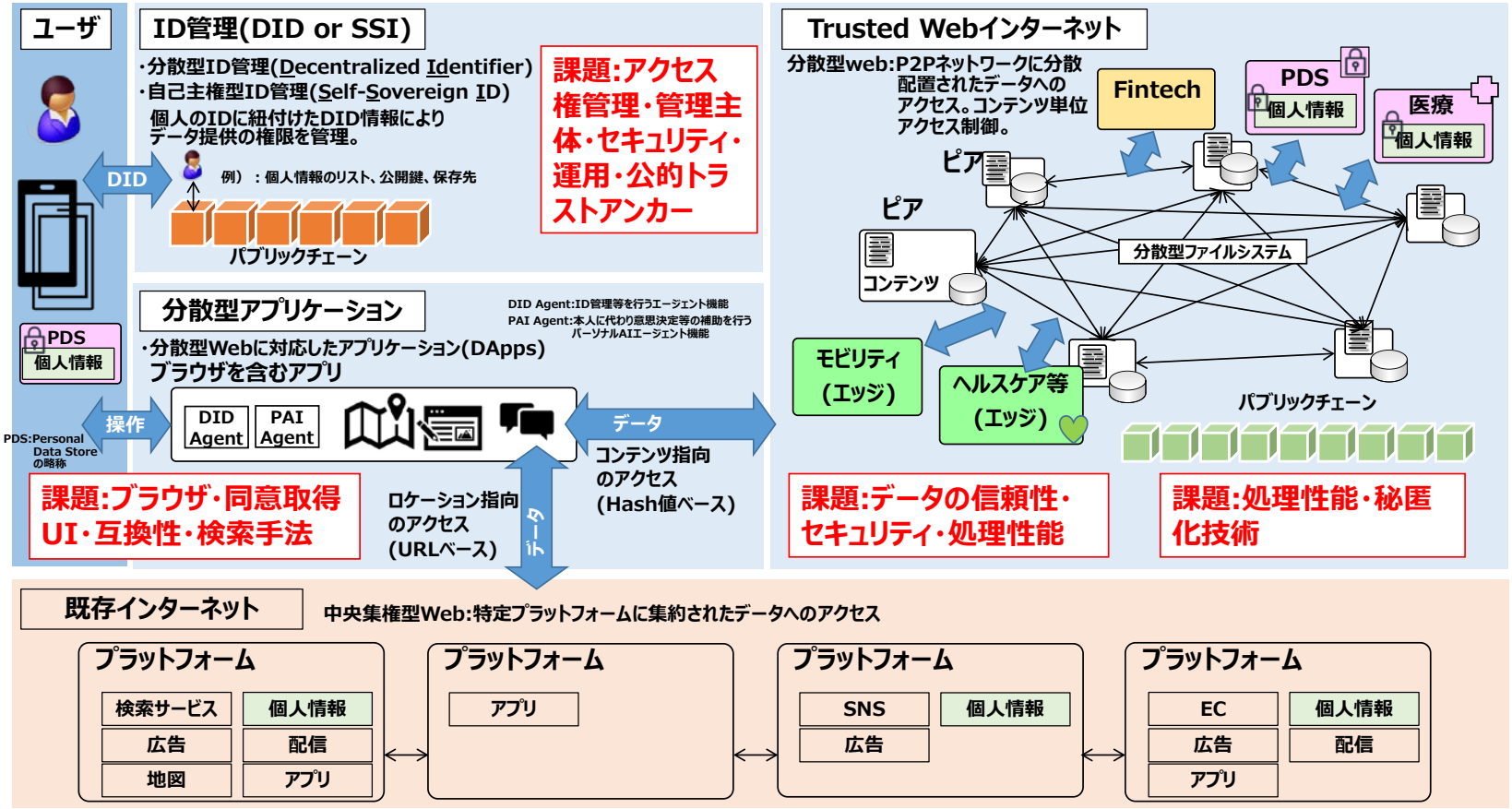

*KEIO Blockchain Laboratory <kbcl-info@sfc.wide.ad.jp>, Rev.14 2020/6/29*

**eKYC**: electronic Know Your Customer

# アーキテクチャーはどうあるべきか

（出典）6/16 デジタル市場競争会議資料

## Trusted Webの現実的な実装の姿



# どのような技術要素があるか

（出典）6/16 デジタル市場競争会議資料

## Trusted Webのコンセプトとその要素

**Trusted Web**

**個人・法人等がデータへのアクセスをコントロールし、価値をマネージできる仕組み**
**→「データ・ガバナンス」のレイヤーの構築**

**データ社会における「信頼」を再構築する**

| 構成要素 | Trusted Webによる技術要素 | 現行のインターネット |
|---|---|---|
| ● 分散ID/データ管理 | ● 分散システムにより、横断的に使えるIDが発行され、個人等が管理。(複数の分散型IDを紐づければ、一意にする必要はない。)<br>● IDを基にパーソナルデータ等をアクセスコントロール。当該IDにトラストアンカー（マイナンバーカード(公的個人認証)、法人ID、登記等）を紐付けることで、API接続やKYCに利用。<br>例:国連ID2020, マイクロソフトのホワイトペーパー、三菱総研、ビットフライヤー | ● プラットフォーム等の各サービス提供者がIDを発行し、中央集権型の管理。 |
| ● パーソナルAIエージェント | ● 個人等がデータをコントロールする場合に、個人等の利益の最大化を図る、自律的な人工知能によりサポートを行う。<br>例: IEEEによる議論 | ● プラットフォーム等の各サービス提供者がコントロール可能な項目を提供。 |
| ● トレサビリティ | ● 改ざんが困難な取引記録によるトレサビリティの確保<br>例: 各種ブロックチェーン、分散型台帳 | ● プラットフォーム等の各サービス提供者のサーバーにおけるデータの利活用（外から見えない） |
| ● コンテンツベース／分散ストレージ | ● ストレージの場所が意味を持たなくなる仕組み(コンテンツベースアクセス)。<br>● P2Pネットワークの中での分散ストレージも可能に。<br>例:分散型ファイルシステム | ● ロケーションベース(URL)のアクセスにより、サービス提供者側のサーバーに蓄積。 |
| ● P2P取引／スマートコントラクト | ● 中間事業者を介さない形での取引（取引の透明性、信頼性の向上）。<br>● 取引における新しい価値設計。 | ● 取引はプラットフォーム等のサービス提供者が提供する基盤上で行われる。 |
| ● エッジ(IoT) | ● クラウドと連携しつつ、処理はエッジまたはエッジ近傍で実行。<br>例: 各種エッジコンピューティング | ● プラットフォームで集中的にデータ管理、処理実行。 |
| ● ガバナンス | ● 参加者の合意によるコンセンサスに依存。<br>● トークンによるインセンティブとガバナンス決定。<br>例: 各種ブロックチェーン | ● プラットフォーム等の各サービス提供者が中央集権的にルールを決定。 |

# Trusted Web推進協議会 名簿

（令和２年12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<br>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　戦略企画本部　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）

＊今後、追加の可能性あり

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２年10月15日現在）

| | |
|---|---|
| 浅井　智也 | 一般社団法人 WebDINO Japan CTO |
| 浅井　大史 | 株式会社Preferred Networks 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　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 | ProtoSchool Tokyo Leader |
| ○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）