Trusted Web　推進協議会
（第１回）

討議用資料

令和2年10月15日

内閣官房デジタル市場競争本部事務局

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）、④**IoT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）

本日の議論

Trusted Web推進協議会（以下、協議会）について

○全体的な成果イメージの共有、進め方

○検討のフォーカスなど

○課題認識、目指すべき将来像、 Trust、デジタルアイデンティティ

今年度のスケジュール・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

2021.4.6～7
Global Technology
Governance Summit

検討のフォーカスなど

＜検討のフォーカス①：　協議会とタスクフォース共通＞

“Think Big, Start Small, Scale Fast”

〇個別最適ではなく、**社会システム全体、社会インフラを意識した議論**を行う。

〇他方で、社会で実現可能な**ユースケースのシナリオをあわせて検討**していく。

＜検討のフォーカス②：　協議会とタスクフォースの役割分担＞

〇**協議会**では、**多様な視点**からの議論。

〇**タスクフォース**は、協議会での議論を踏まえつつ、**テクノロジーに裏付けされた議論**を行い、協議会に提示。

＜対外的な発信＞

〇当面のゴールは、来年４月のGTGSだが、それまでの過程においても、**国内外で発信すべき機会があれば**、**発信**していく。（その際は、協議会やタスクフォースの座長、事務局とも連携し、**統一的な発信**を行う）

〇上記の中で**グローバルで協働する仕掛け**についても検討していく。

(参考)タスクフォースメンバーでの議論

<進め方>

○ 言葉の定義は(場合によっては英語で)明確にしながら(例えばTrust, Decentralization)、共通認識を持つ

○ WEFのGTGSを当面のゴールとする場合に、インド等とのグローバルなネットワークなどもあり、第三者の目線を入れることも重要ではないか。

○ GTGSで我々が検討したことを理解してもらうためには、グローバルで共同でやっているという雰囲気を作ることが重要。３月までのプロセスで、海外で味方につけたい人とのインタラクションの場を作ることを事務局で検討してはどうか。

○ 今後の議論のためのドキュメントの管理についてテンプレートも使い、githubでオープンにすべき。

「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。分断のおそれ。

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

人間とその活動へのリスペクト

- 身体や物理的な生活空間の希少性と価値の向上（priceless化）
- 日常的な活動の多くがデジタル化（できることはデジタルで）
- 感情のデジタル表現等により、人間やその活動の「トラスト」が形成される

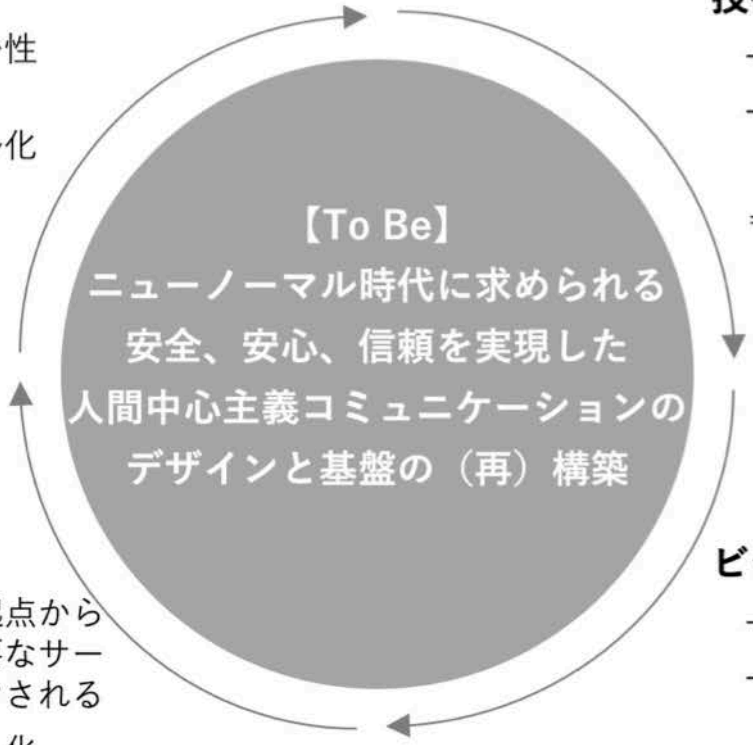
⇒人間の行動がデジタルの価値観と協調しながら変容する「ニューノーマル社会」の出現

技術のコモディティ化

- 高精細デバイスのネットワーク化
- イノベーションコストがゼロに

cf.5G, AI, IoT, 8Kの普及

⇒人間のあらゆる振るまいが記録可能な「エビデンスベース社会」への期待



デジタルファーストの台頭

- 人間とその活動がフィジカル起点からデジタル起点にシフトし、必要なサービスがデジタル前提でデザインされる
- 価値交換メカニズムのデジタル化

⇒デジタル技術とネットワークが人間とその活動（法人等を含む）の必須条件となる「フルコネクテッド社会」の出現

ビジョンの重要性の高まり

- 予測技術と誘導（ナッジ）の普及
- 短期的な行動変容促進の台頭と、それによる私権や倫理との衝突

⇒行動変容を促進する技術の受容に向けた、人間とその活動にとっての価値と展望（ビジョン）を明確にする必要性が顕在化

（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

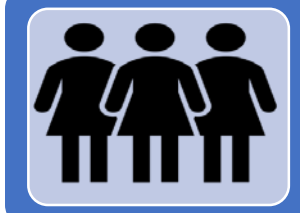
人間とその活動にとっての価値とビジョン

「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

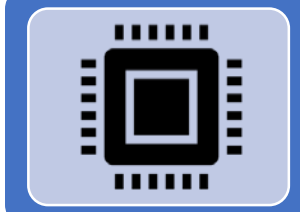
エンティティ毎に見た将来像

国家
- 価値観の共有
- それをデジタルで担保できる仕組み

組織
- デジタル上で取引完結し、契約もデジタルコード化
- サプライチェーンのリアルタイムデータ共有



個人
- ニューノーマル時代の新たなデジタルコミュニケーション
- 全ての人が様々な制約から解放され、自立する個人へ



モノ・情報
- 膨大なデバイス間で自律的なデータ交換
- フェイクニュースの淘汰

Trusted Web

Data Free Flow with Trust

(参考)タスクフォースメンバーでの議論

<実現目的・将来像>

○ テクノロジーを実装していくときのプリンシプルがいる。グローバルに共感できるストーリーや、今実装しないとどうネガティブなことになるのか、どのようなインパクトがあるのかの説明が必要。これまでの大量生産・大量消費社会の中で、ターゲティング広告ビジネスのように生産者から見た客体としての消費者としてのみ個人が捉えられてきたところに北米では歪みが生じている。その文脈から個人のコントロール拡大が必要だとすると、わかりやすいインターフェースであるUX設計が重要となってくる。この際、UXには、広義の市民の人に理解されるストーリーという意味と、狭義の意味での分かりやすさ、最終的にはテクノロジーが直感的にわかるようにしていくことの２つが必要。

○ 人間の生活を向上させるヒューマン・ライフ・セントリックでなければいけない。老若男女へのユニバーサルアクセス、ダイバーシティ、ロックインフリー、グローバルにしわ寄せがいかない仕組みとなるなどの要素が重要となってくる。

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システム**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。

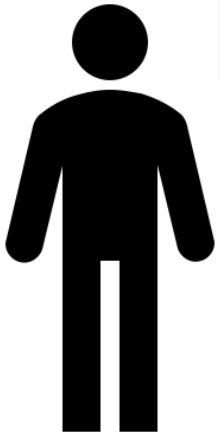
相対取引のTrust

Bを信頼できるか

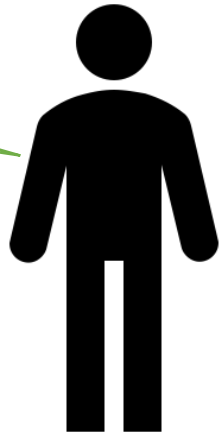
Aを信頼できるか

Bの提供データの取扱いが信頼できるか。

Aの提供データを信頼できるか



取引データ



A個人/社/デバイス

①取引相手のTrust
②取引データのTrust
③取引スキームのTrust

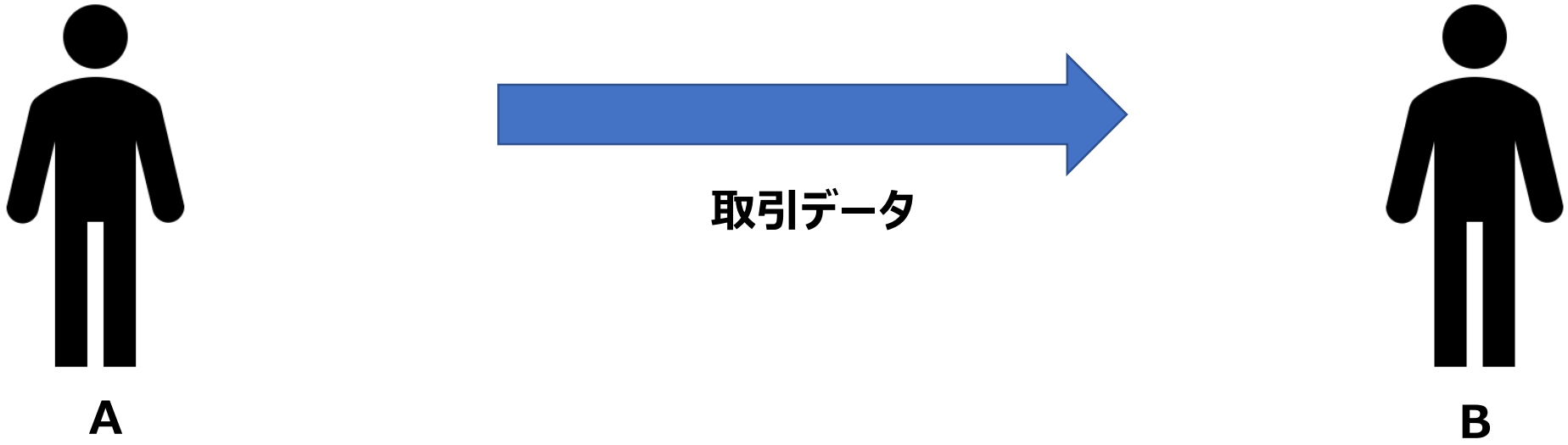
B個人/社/デバイス

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。

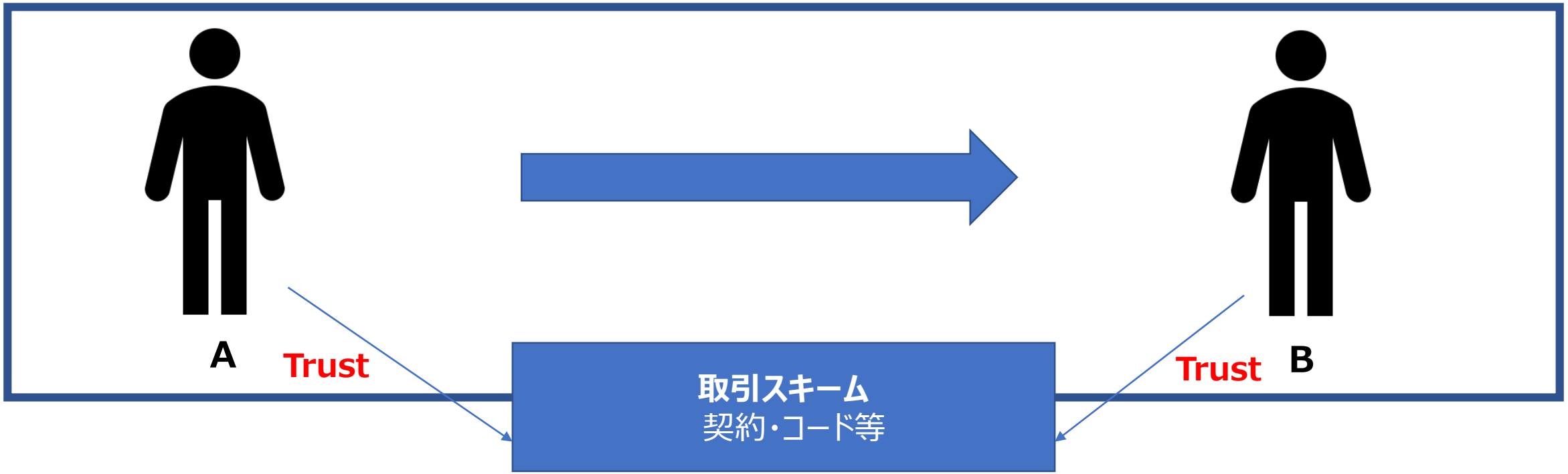
・データが同意を超えて、不正に利用されないか。(正当な理由でデータが利用できるか)
・データを集約するプレイヤーによって、データの価値を不当に搾取されないか、監視されないか。
・悪意の参加者がいたとしても、データが第三者も含めて安全に流通できるか。
・データの利用状況が透明化されるか。
→データ自体のコントロール権限の問題
・データが正しく必要な速度で処理され、伝送されるか。

○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

データ加工

③認証

データ作成

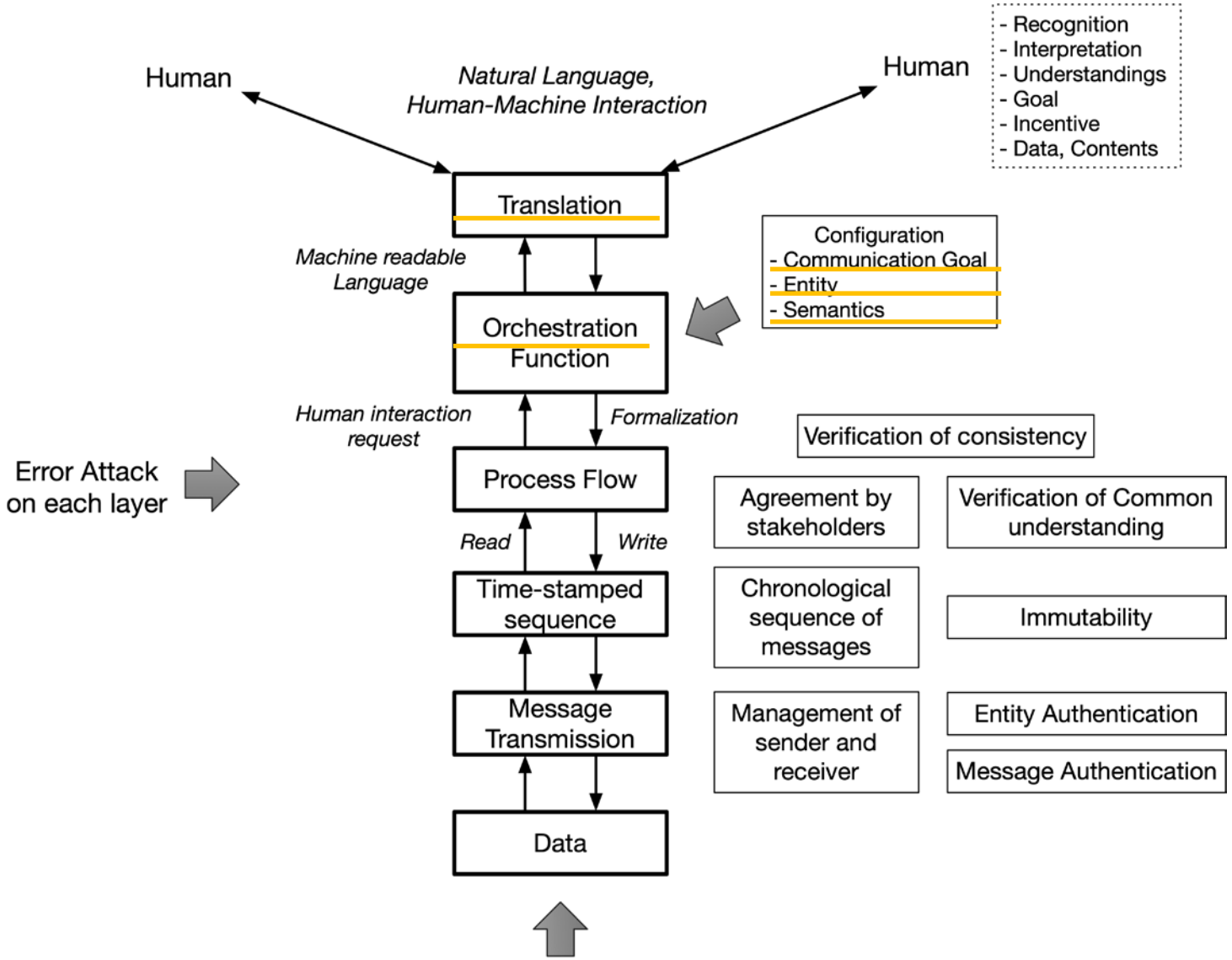
③認証

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

コミュニケーションの様々なユースケースを想定した基礎的なモデリング例



KEIO Blockchain Laboratory
<kbcl-info@sfc.wide.ad.jp>
Rev.3 2020/8/2

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

(参考)タスクフォースメンバーでの議論

<重要な構成要素としてのトラスト>

○ 「信頼の確保」を技術で実現するためには、工学的な知見のみならず、人文社会学的な知見も必要となる。リアルな社会ではポジティブな評判を得れば新たな関係性が構築されていき、ネガティブな評判が生まれれば村から追い出されていた。他方、ネットでは、IDの切替が容易なために、ネガティブ評価は機能しないとされており、ポジティブな評価に意義があるとされてはいるものの、「やらせレビュー」などで機能不全化し、リアルの社会のような前向きな機能が働きにくくなっており、デジタルでの再設計が必要。

○ 通常我々はトラストというものを意識していないが、困ったときの救済手段があることが重要。

○ ブロックチェーン的にはオラクル問題にもつながるが、アンカートラストが重要。我々が印鑑の場合、行政に登録している。ここのバインディングが重要。DIDとは、文字列に対して様々なものを結びつけることでトラストが生まれるが、その際、国の制度として、印鑑で言う公証役場のようなサービスを提供していくという方向になるのではないか。印鑑登録をするように、DIDとマイナンバーが紐づくことになるのではないか。DIDを見せることでどこでも本人確認ができるようになる、ワンスオンリーで他でも使えるようになることが信頼につながると考える。

○ トラストはグローバルに一つの形に集約されるのか、ダイバーシティの観点からそれぞれの考え方が違ってくるのか、トラストの概念が許容されるのか。人として最低限共有すべき土台のトラストがあって、その上でトラストの多様性が出てくるのではないか。何を重視するかはそれぞれによって異なるのではないか

○ 検証済みのデータとして使うことができるverifiable credential を上手に使うと、確認済みデータをダウンロードしてChain of trust のチェーンを全て持っている場合だけでなく、それがバラバラなものであっても組み合わせれば確認できるということが重要であり、UXも良いものにできる。

<Digital ID>

○IDについては、Identifier,Identification,Identityの概念が混在して世界的にも議論。既に定義も標準化されていることから、そのルールの上で議論される必要。DIDも概念が分かれており、当初はidentifierとして議論が始まり、identityとしても使えるとなったが、DIFの場合にはIdentityとして議論されている。

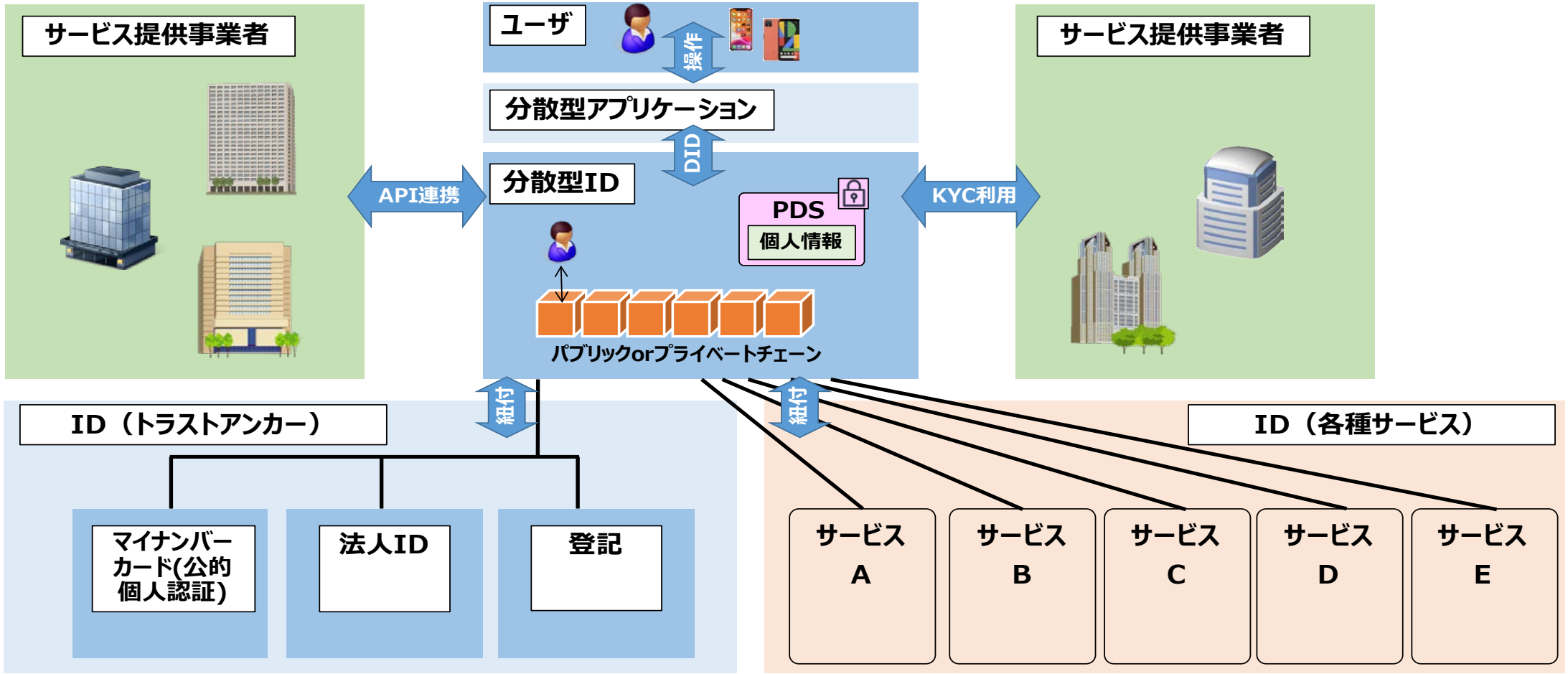
○IDを付与する粒度について、ブラウザの観点から、ドキュメント、コンテンツ単位も含めた設計なのか判断していく必要。

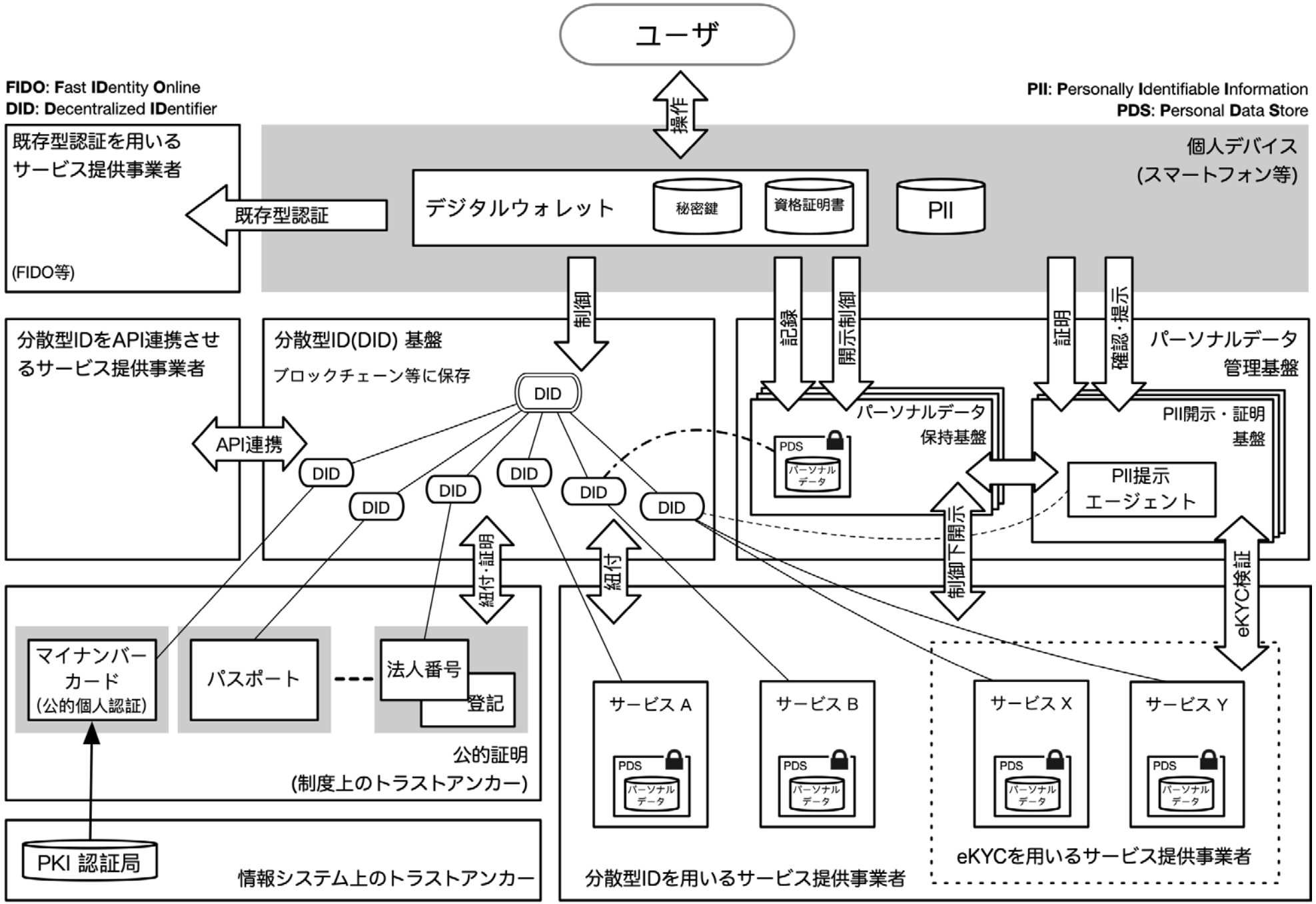
分散型ID

（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。





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

ユーザ

PDS
個人情報

ID管理(DID or SSI)

・分散型ID管理(Decentralized Identifier)
・自己主権型ID管理(Self-Sovereign ID)
個人のIDに紐付けたDID情報により
データ提供の権限を管理。

DID

例）：個人情報のリスト、公開鍵、保存先

パブリックチェーン

課題:アクセス権管理・管理主体・セキュリティ・運用・公的トラストアンカー

分散型アプリケーション

DID Agent:ID管理等を行うエージェント機能
PAI Agent:本人に代わり意思決定等の補助を行うパーソナルAIエージェント機能

・分散型Webに対応したアプリケーション(DApps)
ブラウザを含むアプリ

操作

DID Agent | PAI Agent

データ

コンテンツ指向
のアクセス
(Hash値ベース)

ロケーション指向
のアクセス
(URLベース)

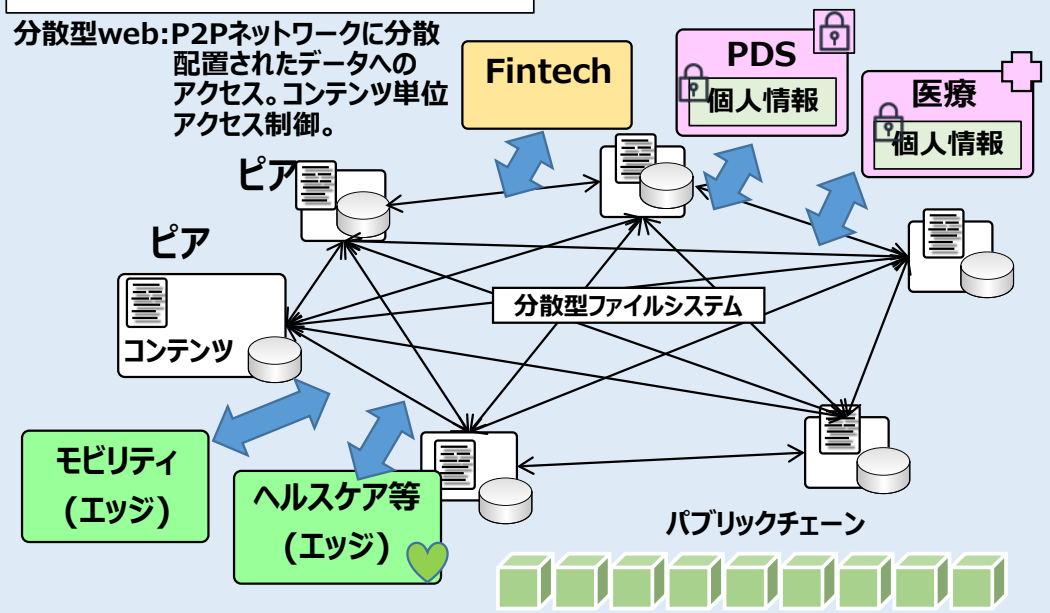
データ

PDS:Personal Data Store の略称

課題:ブラウザ・同意取得UI・互換性・検索手法

Trusted Webインターネット

分散型web:P2Pネットワークに分散配置されたデータへのアクセス。コンテンツ単位アクセス制御。

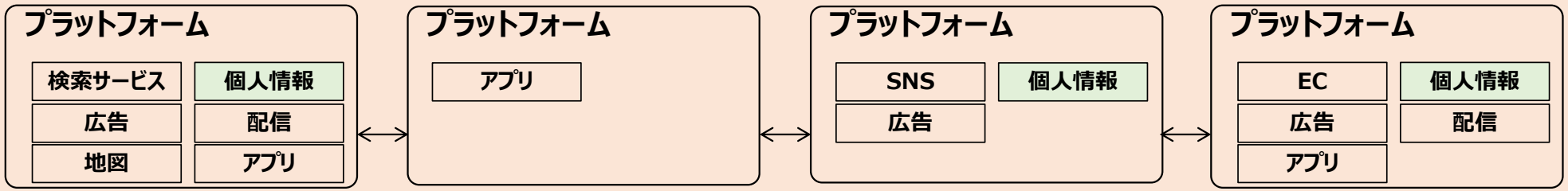


課題:データの信頼性・セキュリティ・処理性能

課題:処理性能・秘匿化技術

既存インターネット

中央集権型Web:特定プラットフォームに集約されたデータへのアクセス



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。) ● 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。 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。 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 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)。 ● P2Pネットワークの中での分散ストレージも可能に。 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）。 ● 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。 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。 ● トークンによるインセンティブとガバナンス決定。 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。

(参考)タスクフォースメンバーでの議論

<Trustを実現するためのアーキテクチャ>

○ データ、通信、計算について、分散システムのアーキテクチャを考え直す必要がある。計算をどこでやるかについては、深層学習の場合データは一社に集める方が効率的な側面もある中でどうするか。分散になると技術が複雑になるが、アーキテクチャの視点からこれら３点について耐障害性をどのように担保するか。機械学習の観点からは、データのクレンジング上は異なるデータの流通をさせたくないという求心力が働くので、経済効率性やトレサビリティの視点を含め、分散型とのトレードオフをどう考えるのかも見ながらアーキテクチャーを考えていく必要。

○ Globalは世界に１つという概念だが、Globalなネットの中で、国をどう意識するかはアーキテクチャを考える上で重要。

○ 分散型アーキテクチャーは一社が作るわけではなく、グローバルでやっていく上でステークホルダーが複数あり。運用主体が複数出てくるので、OSの場合、ユニーク原則の下でメカニズムとポリシーを分離し、メカニズムはグローバルで共通のものを使い、その上に実装・運用上ポリシーを追加できる仕組みであり、相互運用性のための共通のプロトコルが必要

○ 分散型で処理する場合、系全体のトラストを保つに当たり、末端の人間一人一人がある種の責任を負わされることになる。持続性を確保するためには、誰がどんな責任を負うのかの分析が足りないとうまくいかなくなる。普通の人が果たし得るのか、それに報いるだけの「報酬」をシステム的に組み込めるかは、アーキテクチャの設計に重要となる。

　ビットコインはマイニングという単純な報酬を組み込んでおり、小さいときはうまくいくが、社会システムレベル全体に持ち込むとすると、これを持続的なものとするためには、全てがデジタルのコード上で完結できるものではなく、併せて、要所要所で「責任を持った複数の主体が協力して運営する」ことも重要となる。キーワードとしては「Poly-centric stewardship」。誰がどう責任を持つのか、このガバナンス設計が検討のスタートポイントとなる。

(参考)タスクフォースメンバーでの議論

<Trustを実現するためのアーキテクチャ（続き）>

○ 汎用的なアーキテクチャーを目指すゴール認識について汎用すぎると使われないので、実際のユースケースを見据えた要求事項をまとめる必要。

○ ユースケース、アーキテクチャーについてコンセンサスを得るためには、ユースケースとして現実的なものをいくつか持ってきて目標を考えると、何となくアーキテクチャが見えてくるのではないか。アーキテクチャーとユースケースはパラでやるべきだと思う。

○ アーキテクチャに行かずユースケースを考えることは、踏みとどまった方が良い。ユースケースから入っていくと既存の延長線上のものにしかならない可能性あり。

○ 特定のユースケースを考えすぎることの弊害がある。社会的な背景が見えなくなる可能性があり、エンドユーザに対する本当の価値や便益が見失われる可能性がある。

〇 現状においては、人間中心ではなく、それが表面化したのがコロナであり、ニューノーマル。ネットの世界は、これまで金儲けのためにやってきたことへの反省がある。経済合理性が高いので、人がシステムに合わせてきた。しかし、このままでよいのか、人間・生活に寄り添うべきではないかという状況にある。

　こうした視点で考えると、特定アプリケーションやユースケースを考えることは重要であるが、既にトラストができ上がっていて安定状況にあるサービスの中で、使えるものは使っていって、組み合わせて連携していくフェデレーションのイメージ、分散状態であるが、そこにあるトラストを活用し、様々なアプリやサービスが結びつきフェデレーションできるインフラストラクチャーを我々が作ることが一つのビジョン。

　一つの大きな基盤があり、最初になるアプリは何かといった議論とともに、全体を支えるシステムも重要であり、常に両方を持って議論するということではないか。その際、トラストにはいろいろある、産業ごとに違う中で、何をのせて、何を協調させるかを考えるのではないか。

今後のスケジュール

Trusted Web推進協議会

○ **10/15　第１回　協議会**

○ 12月　　第２回　協議会
　背景、課題認識、検討の視点、ビジョン・全体の将来像、目指すべきTrust、デジタルアイデンティティなど

○　3月　第３回　協議会
　実現のための基本アーキテクチャー(仮)、ロードマップ、ユースケース、必要なアクション、ホワイトペーパー案

＜タスクフォース＞
○ 10月下旬　背景、課題認識、ビジョン、将来像
○ 11月上中旬　Trust、アイデンティティ　（→　ここまでを第２回協議会にて報告）
○ 12月上旬　基本アーキテクチャ　（アウトプットのレベル感、必要な要素など）
○ 1月中下旬 基本アーキテクチャ
○ 2月上旬　　基本アーキテクチャ
○ 2月下旬　　ロードマップ、ユースケース
○ 3月上旬　　ホワイトペーパー原案　（→　第３回協議会にて報告）
※タスクフォースは必要に応じ、追加開催も検討

参考資料

Trustに関する議論

ドイツの社会学者ニクラス・ルーマン

　世界は人の認識能力を超えた複雑なものであり，信頼によってその複雑性を「縮減」することで，社会が成立。

FUJITSU, Vol. 70, No. 4(09, 2019) 特集|研究開発最前線 ~ デジタル時代の信頼「Trust」~
デジタル時代の信頼「Trust」 “Trust” in the Digital Age

レイチェル・ボッツマン著「TRUST」

①小さな地域社会における「ローカルな信頼」
②様々な契約や法律に基づく「制度への信頼」
③テクノロジーを通じて人が人を信頼する「分散された信頼」

Trustとは(ボッツマンの整理から)

Trust
＝取引の確認プロセスを可能な限り縮減すること

→膨大なデータ(取引)が行き交うSociety5.0時代では、制度設計や認証などヒトの介在する従来型の仕組みでは、量・スピードの面で限界

今後のTrust

理解の共通化・一貫性、下記技術の組み合わせ・アーキテクチャー(DID、分散型台帳等) など

＋

これまでのTrust

個別の電子証明、タイムスタンプ、電子マネー、マイナンバー、プラットフォーム、Trustフレームワーク、集合知など

＋

近現代のTrust

連帯保証、信用保証、内容証明郵便、公正証書、登記、資格、監査、国の通貨発行 など

＋

原始的なTrust

評判、地縁血縁 など

テクノロジーによる分散された信用担保

基盤となる制度や第三者による信用担保

属人的・コミュニティ内の信用担保

デジタルIDの取組事例

中央集権型ID

サービス提供型ID

ID管理サービス

国家管理型サービス

分散型ID(Federated含む)／ブロックチェーン利用

分散型ID

標準化団体

政府機関・NGO

Project Mercury

世界経済フォーラム(WEF)

本人確認サービス

bPassport

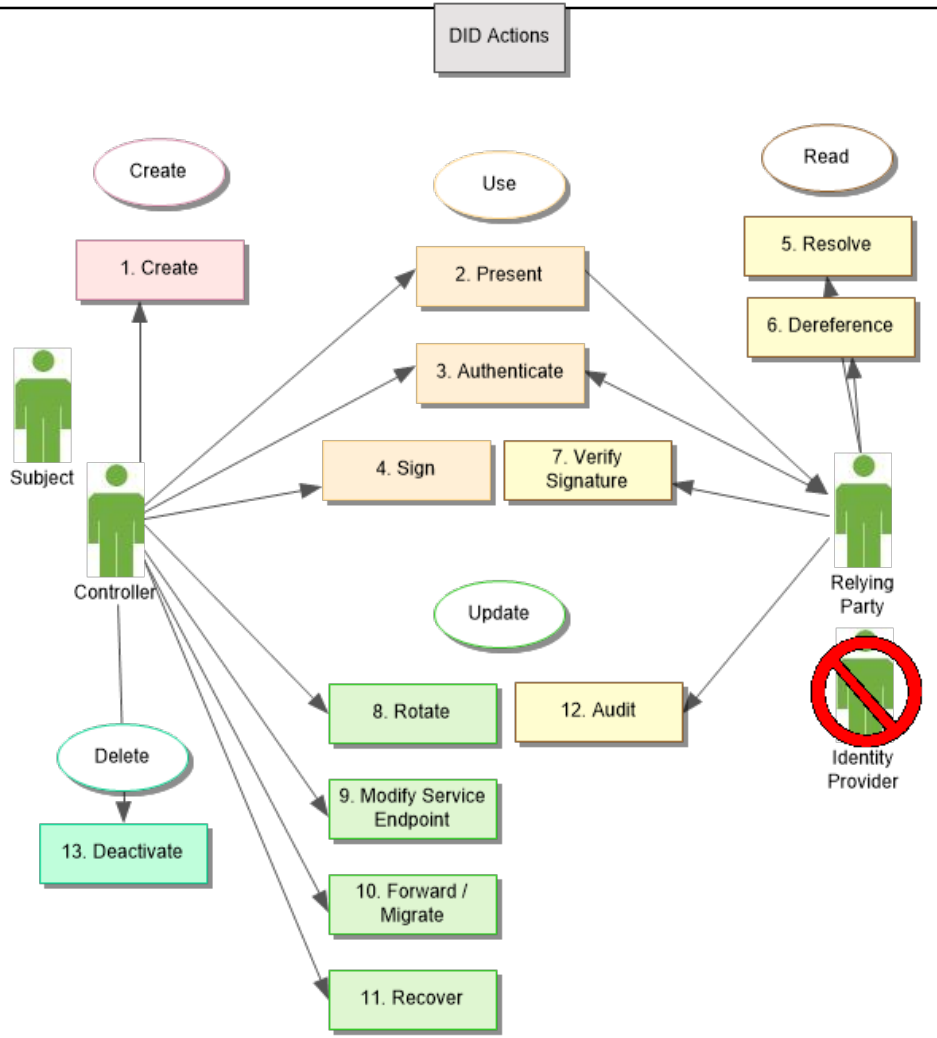
分散型ID／データ管理　事例

【取組事例：W3C】
- 分散型識別子WGのミッションは、初期ユースケースを可能にするDIDに関連する情報を含むDID URIスキーム、DIDドキュメントのデータモデル及び構文、及びDIDメソッド仕様の要件を標準化すること。

W3CはSSI（自己主権型アイデンティティ）という、「自分が自分の個人情報を管理する」というデジタル個人情報のポリシーを提唱し、DID（Decentralized Identifiers：非中央集権型識別子）と、Verifiable Credential（暗号技術で証明可能な個人・法人情報）を開発。
これらは、暗号技術を駆使し、「第三者機関の認証なしに、自分が自分であることを証明」できる画期的なID、そして個人情報の電子形式。

W3Cが提唱するユースケース

1.Online shopper
2.Vehicle assemblies
3.Encrypted Data Vault
4.Accessing Master Data of Entities
5.Identifiers in an ecosystem of verifiable credentials (VCs)
6.Sharing opted-in information across platforms
7.Collecting payments for work conducted anonymously
8.Anonymity within a supply chain
9.Digital Permanent Resident Card
10.Importing retro toys

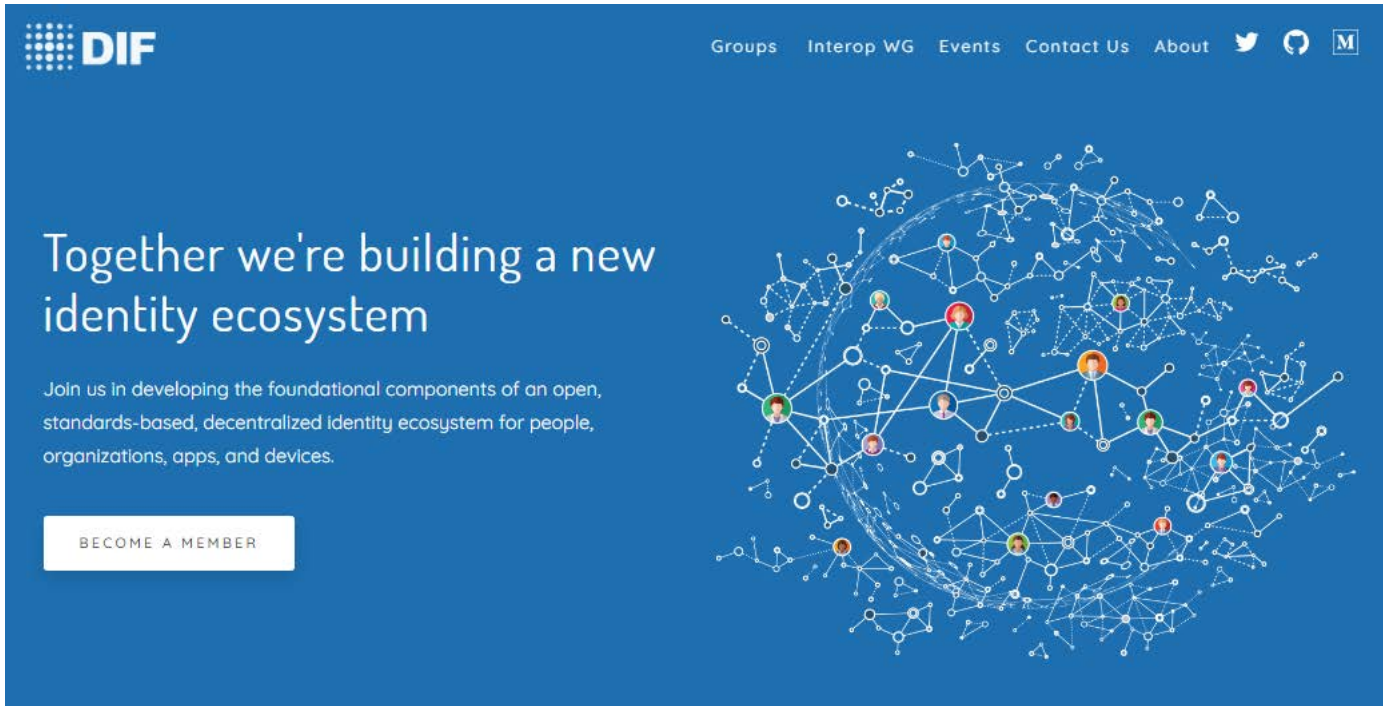


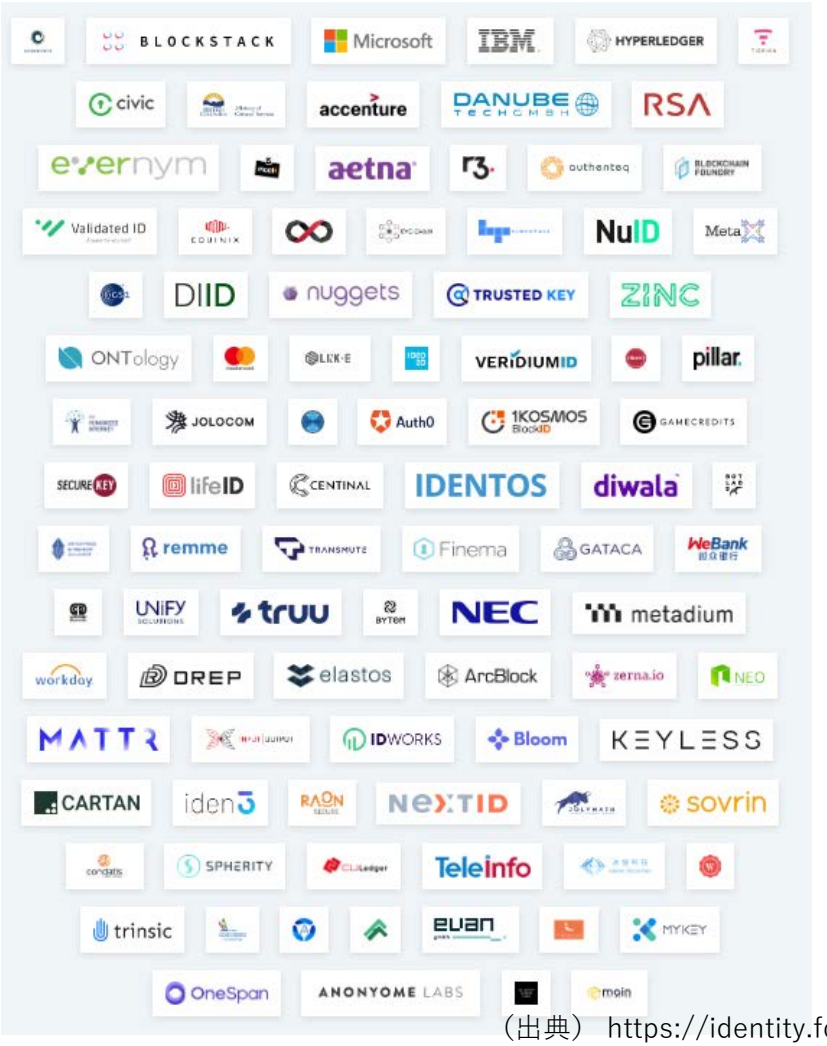
（出典）https://www.w3.org/TR/did-core/

分散型ID／データ管理　事例

【取組事例：DIF(Decentralized Id Foundation)】
- DIFは、分散型アイデンティティのためのオープンなエコシステムを確立し、すべての参加者間の相互接続を確保するために必要な基礎的な要素の開発に焦点を当てたエンジニアリング主導の組織。

2017 年5 月に、分散ID 連携に関する各種仕様の検討を行うための団体として分散型ID ファウンデーション（DIF）が設立。米国企業を中心に現在70 社以上がメンバーとして参画し、DID の標準化に向けた検討が進められており、分散型ID を標準化することで複数業界に渡って本人確認として利用できるID を構築することを目的。





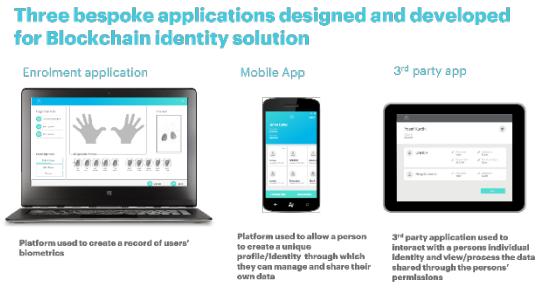
（出典） https://identity.foundation/

分散型ID／データ管理　事例

【取組事例：ID2020】

- 国連は持続可能な開発目標の中で「2030年までにすべての人に出生証明を含む法的なアイデンティティーを提供する」という目標を定めている。ID2020はこの目標を達成するべく国連機関、NGO、政府、企業が連携して現在IDを持たない人たちにデジタルIDを提供するとともに、分散型のIDネットワークのフレームワークの標準を作り、効率的に開発人道支援を提供できるようにすることを目指している。

Accentureは2016年からMicrosoftと共同で前述の生体認証システムとDIFで開発中のデジタルID技術を利用し、ID2020のためのブロックチェーンベースのデジタルIDシステムを構築。2017年7月に行われた国連のID2020に関する会議では、Enterprise Ethereumのプライベートなブロックチェーンを利用し、Microsoftのクラウドプラットフォーム Azureで動作するデジタルIDシステムのプロトタイプを公開。



（出典） https://id2020.org/

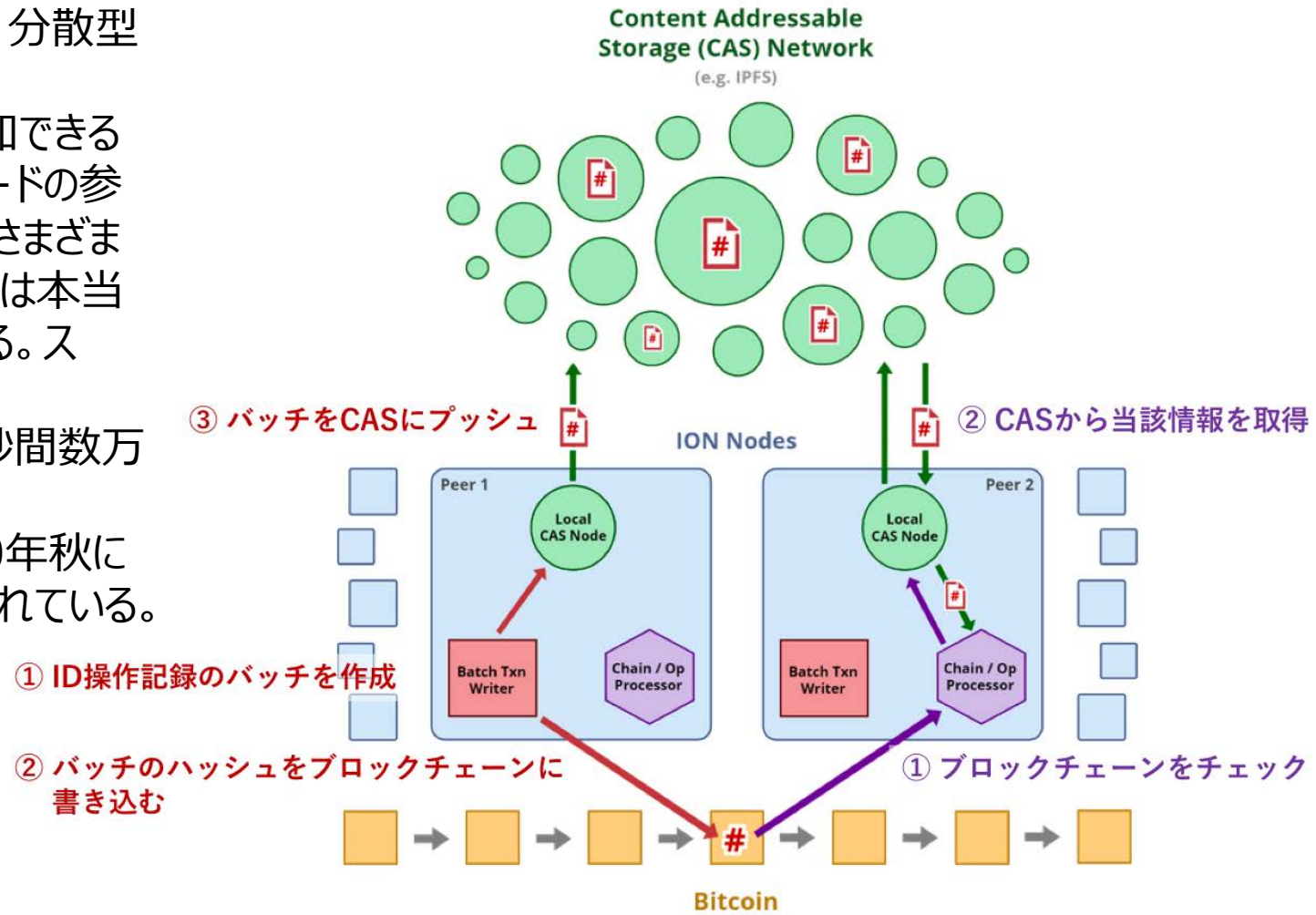
分散型ID／データ管理　事例

【取組事例：Microsoft ION】
- ブロックチェーンネットワークにレイヤーを加えることで、分散型デジタルIDシステムを実現。

ION（Identity Overlay Network）はBitcoinネットワークに新たなレイヤー、セカンドレイヤーをかぶせて、分散型デジタルIDシステムを実現するもの。

IONのネットワークは誰もがノードを立ち上げて参加できるパーミッションレスなパブリックネットワーク。このためノードの参加を許可する中央集権的な組織はなく、将来的にさまざまなノードがIONのネットワークに参加することで、IONは本当の意味で「分散型」のIDシステムとなる可能性がある。スケーラビリティについては、セカンドレイヤープロトコルSidetreeによってデジタルIDシステムに求められる秒間数万という処理能力を実現しようとしている。

IONはテストネットからメインネットに移行し、2020年秋にバージョン1の最終版をリリースするべく開発が続けられている。



（出典）https://gaiax-blockchain.com/microsoft-ion

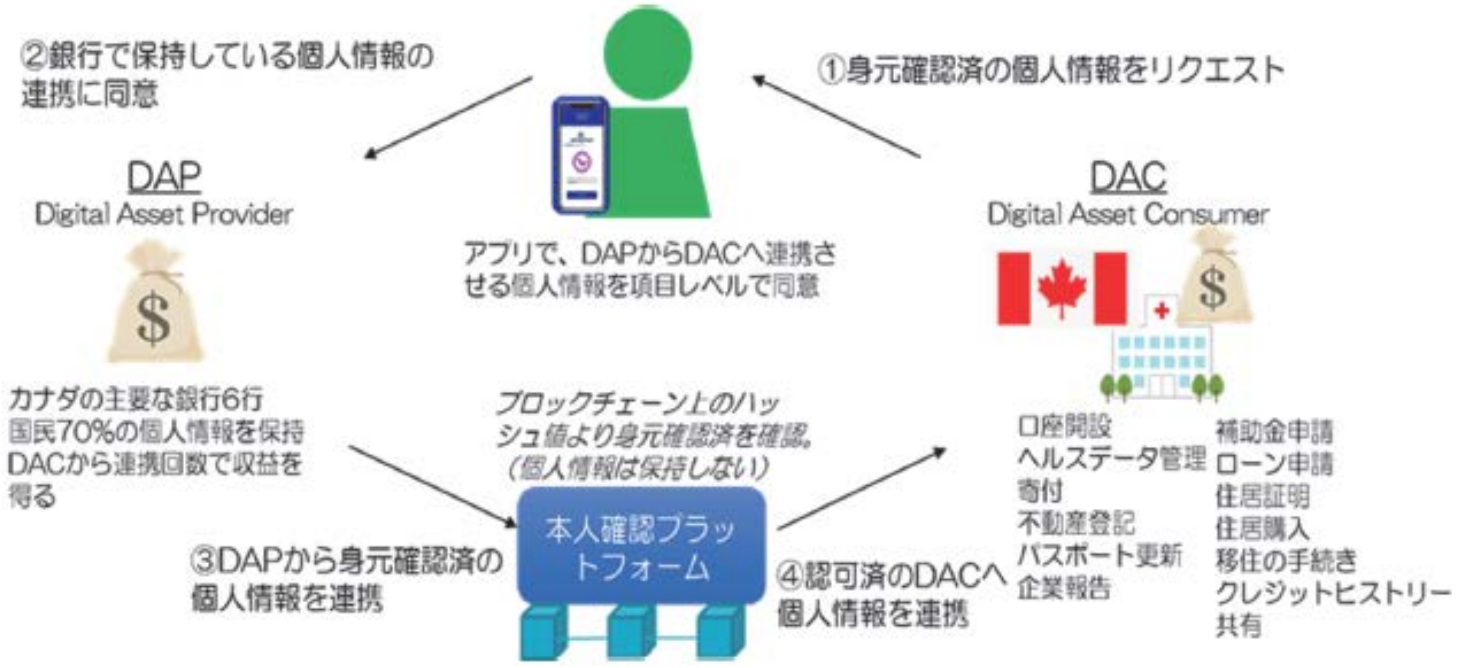
分散型ID／データ管理　事例

【取組事例：カナダ SSI事例】
カナダではデジタルアイデンティティと認証フレームワークを開発する、政府/産業界の合同のNPO であるDIACC（Digital Identification and Authentication　Council of Canada）が、カナダ国内の大手銀行と連携して実用化を進めている。

　不正が困難で、かつ本人確認、個人情報の取扱いが低コストで可能なSSI/DID の仕組みが検討され、実証実験が進められている。
　実証実験では、DAC（デジタルアセットコンシューマー）と呼ばれる、個人の本人確認等を目的として個人情報の提供を求める事業者等からの要求に応じて、DAP（デジタルアセットプロバイダー）と呼ばれる、本人確認済みの個人情報を保持するサービス群が、DAC に対して個人情報を提供。個人は、DAP がDAC へ個人情報を提供してよいかを判断し、同意をすると、DAP は本人確認済みの個人情報をDAC に対して送信。DAC は、当該個人情報を用いて本人確認等が可能となる。

（出典）デジタルアイデンティティ
～自己主権型／分散型アイデンティティ～
株式会社野村総合研究所
NRIセキュアテクノロジーズ
株式会社ジェーシービー

組織	課題
政府	・公的手続きでの各種身分証明書の確認のコスト ・本人確認のための窓口の運用・管理の維持
民間	・マネーロンダリング ・非効率なKYC ・偽装された身分証明書による手続き多発 ・個人情報収集の煩雑さ



分散型ID／データ管理　事例

【取組事例：UNiD CollaboGate社】
- 分散型ID、DIF／W3C準拠、ToIP Foundation

「未来の信頼を形にする」

データ社会における「信頼」の再起動

現在のWebには「信頼」を構築する仕組みが欠けています。結果として、個人のIDやデータはバラバラに分断され、プライバシーやセキュリティなどの多くの社会問題を引き起こしています。
私たちは、人と人、人と企業との関係を新しくする分散型ID基盤技術を開発し、個人がオンラインでオフラインと同じように弊害なく行動できる未来を形にします。

次世代型ID管理クラウドサービス
UNiD

分散型IDによる認証・認可・ID管理機能を提供するクラウドサービス。エンジニアが簡単にDID基盤を構築できるためのリソース・ソリューションの提供

（出典）https://collabogate.com/products/index.html

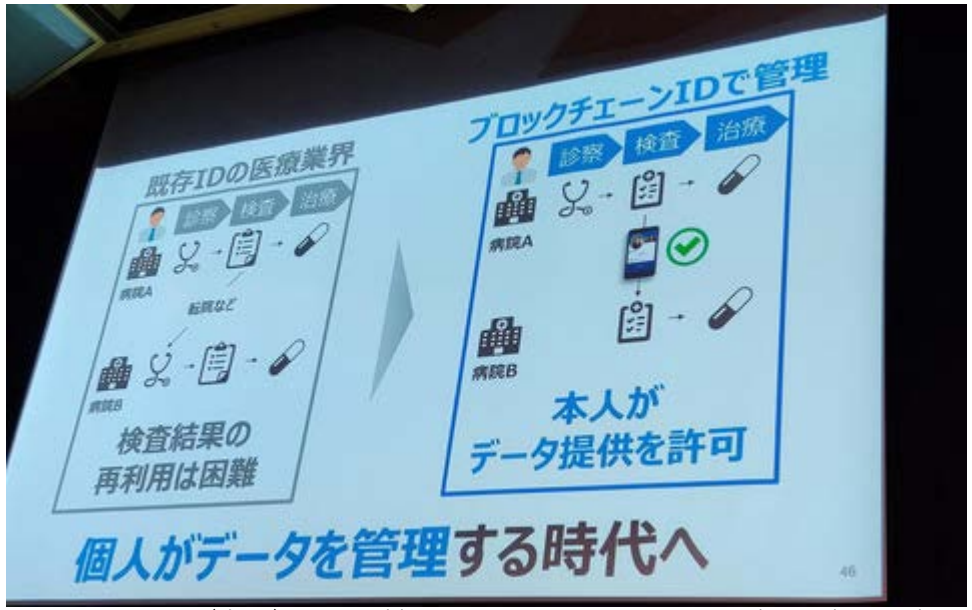
分散型ID／データ管理　事例

【取組事例：bitFlyer bPassport】
- ブロックチェーンIDで個人がデータを管理するサービス。

Webサイトなどで個人情報を入力して作成する従来のIDに対して、「ブロックチェーンID」というものが考えられる。ブロックチェーンに自身の氏名・性別・住所・生年月日の基本4情報をはじめとした各種情報を、暗号化して記録、自身の情報をコントロールすることできる。

ブロックチェーンIDは、入力の手間を大きく削減することができる。現在、会員カード1枚作るにしても、基本4情報に加えていくつかの情報を手書きしたり、入力する必要がある。

ブロックチェーンIDを用いれば、提供を要求された情報だけを、特定の企業に対して公開することが可能になる。ボタン1つで会員カードの作成に必要な個人情報の入力を終えることができ、何度も同じ住所を書くような手間が発生しない。このように作成したカードもまた電子化できるので、財布をポイントカードで膨らますことも避けられる。さらに、情報の提供によって対価を得る仕組みも実現できるという。



（出典）https://crypto.watch.impress.co.jp/docs/event/1210425.html