

第2回 ブロックチェーンに関する官民推進会合

討議用資料

令和2年10月29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）

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

Trusted Web推進協議会 名簿

1

(令和2年10月15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
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
富本 祐輔	トヨタファイナンスサービス株式会社 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）

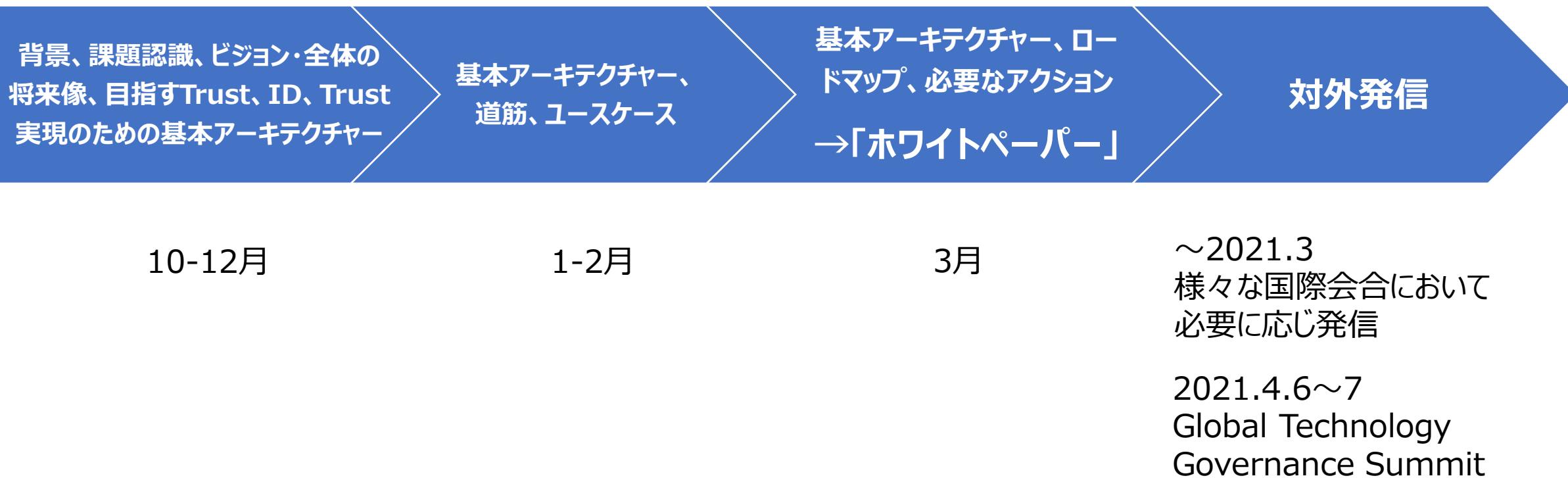
Trusted Web推進協議会タスクフォース 名簿

(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 大地	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)

今年度のスケジュール・イメージ



「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な要素
- 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

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）

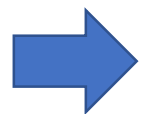
- **データがどのように活用されるか分からない**。

（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

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



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

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)

「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



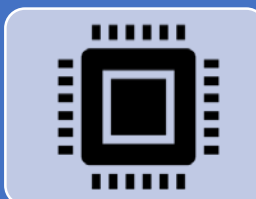
組織

- 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

人間とその活動にとっての価値とビジョン

エビデンスベース社会

ニューノーマル社会

フルコネクテッド社会

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、ログイン**。



○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。

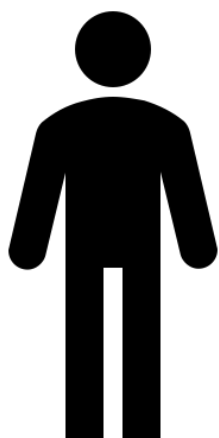
相対取引のTrust

Bを信頼できるか

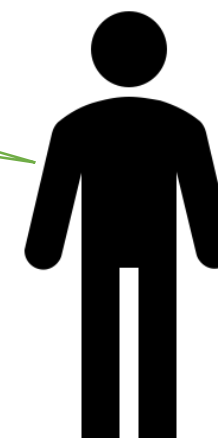
Aを信頼できるか

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



A個人/社/デバイス

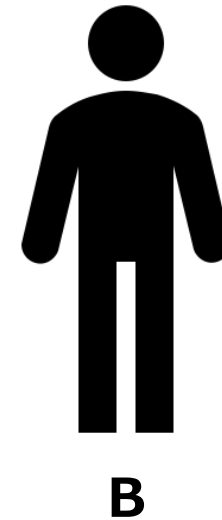
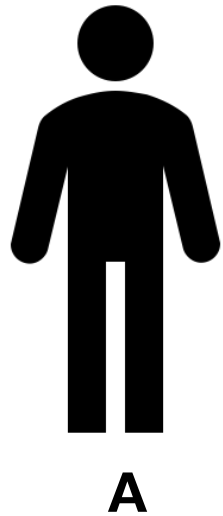


B個人/社/デバイス

取引データ

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



○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

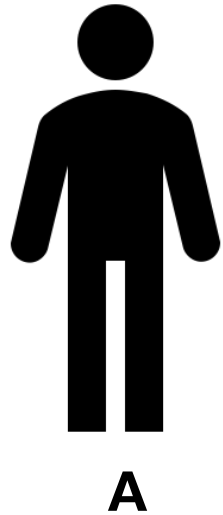
→様々な分散的に存在する属性データが統合管理され、必要に応じて相手に提示。

・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

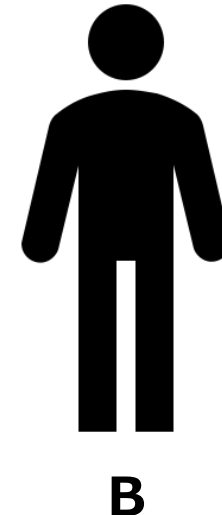
→いわゆる「オラクル」問題。

・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)



取引データ



○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。

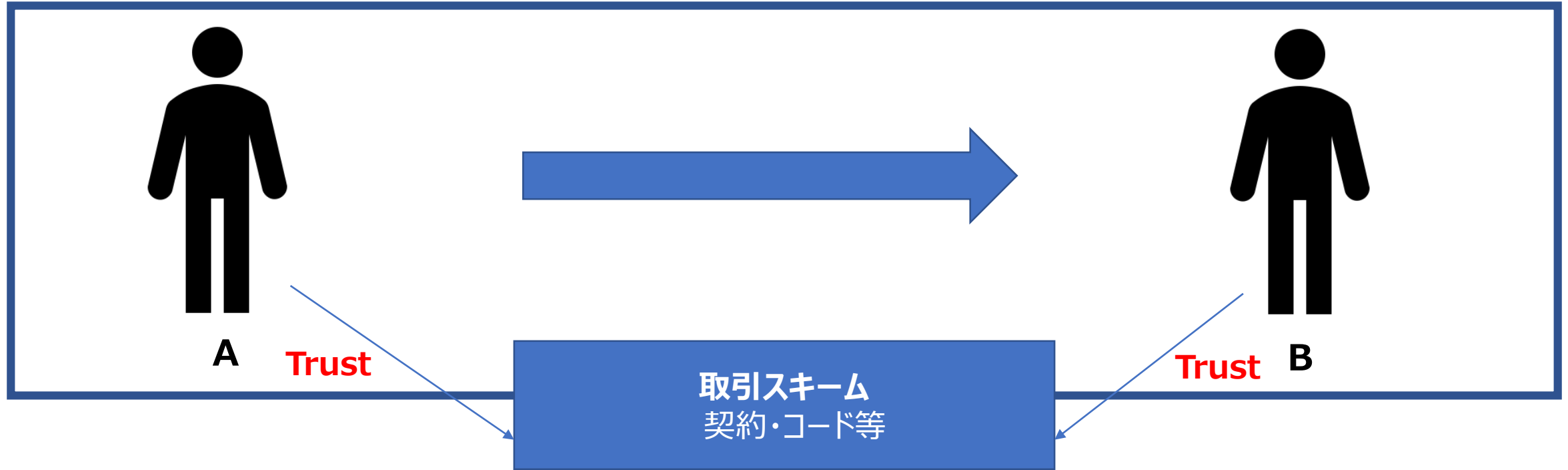
○信頼できるデータか。

- ・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の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。



- 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

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)

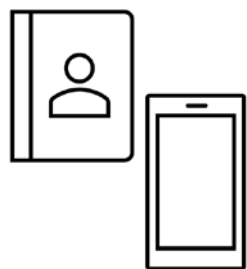
①ゴールの共有

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

⑤一貫性を保証するレイヤーが必要

送受信データ



1010
1010



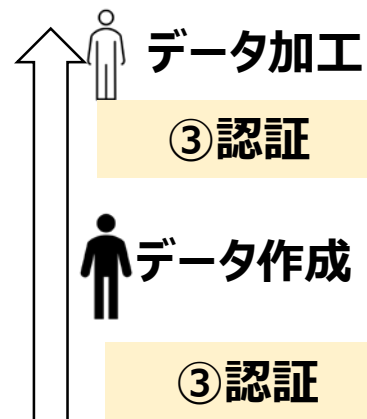
④プロセスの前後関係が特定可能で、検証可能な形で記録

④Permissionless Blockchainで実現可能

エンティティ

②認証

③改竄されていない



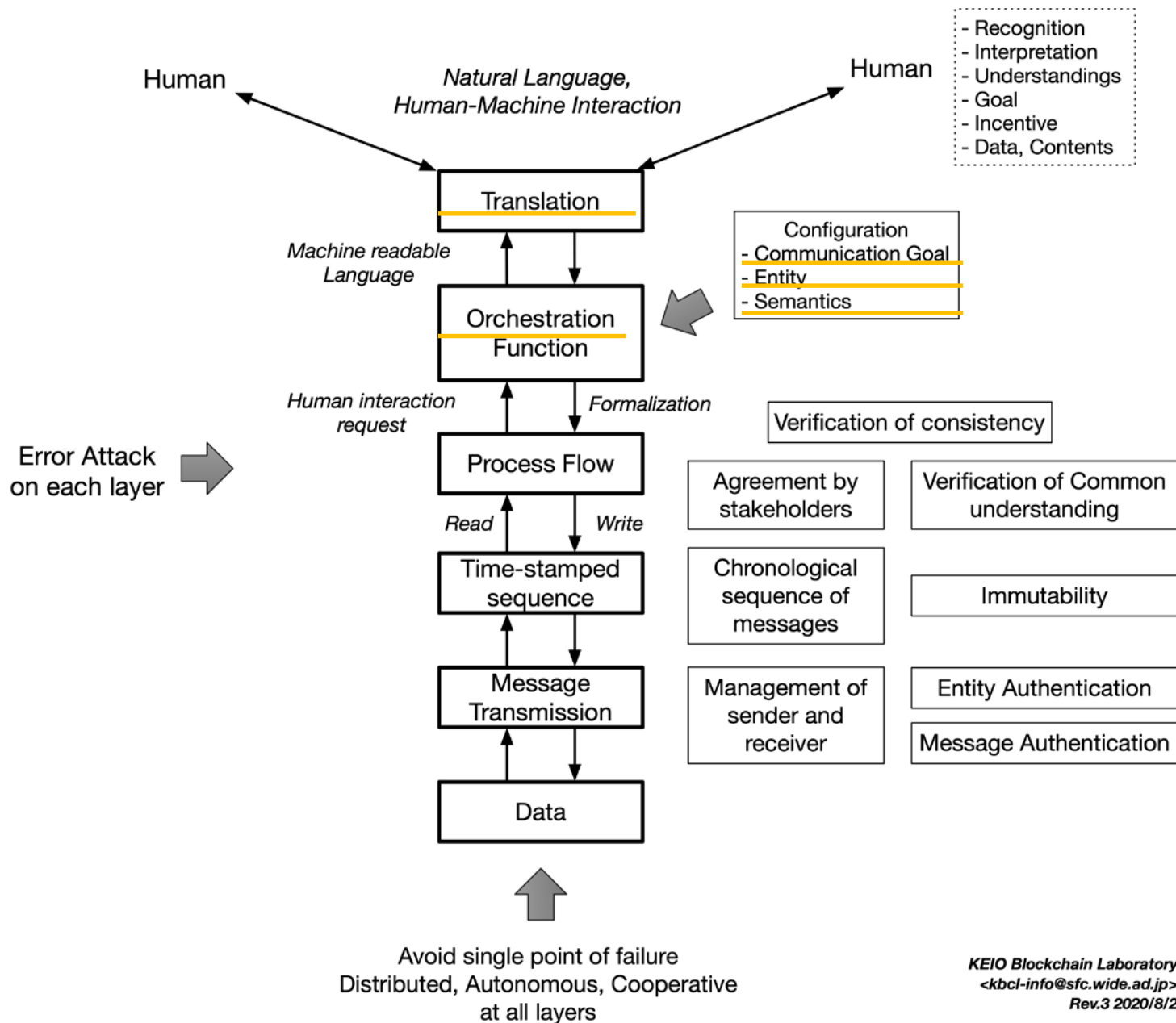
エンティティ

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

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

16



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…**

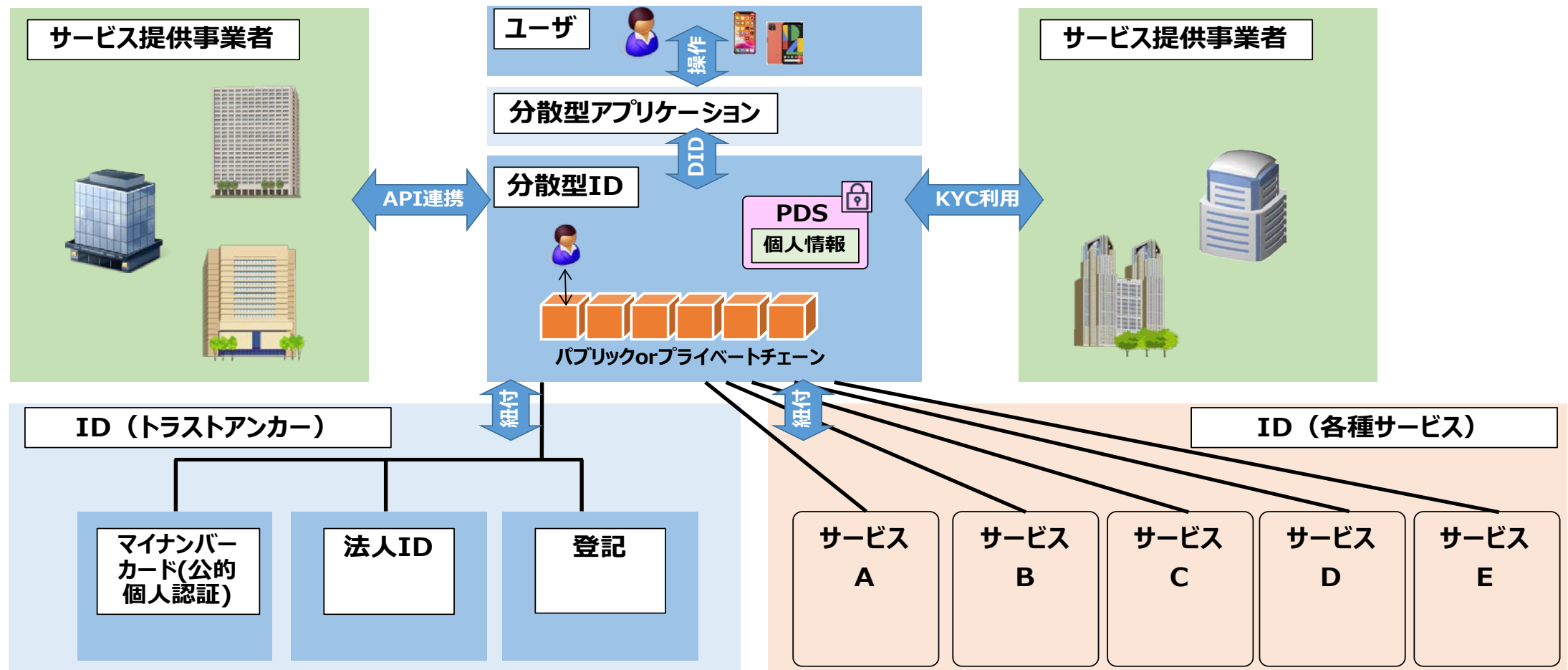
- ・サービスごとに用意されたアイデンティティを作成し、管理する煩雑さからの解放
- ・特定のサービスに紐づけられたアイデンティティへの利用強制からの解放
- ・アイデンティティの不適切な管理によって生じるセキュリティリスクの緩和
- ・アイデンティティ利用の永続性と可用性の確保
- ・PII(個人を特定できる情報)等が直接的にサービスと結びついてしまうことによって発生しうるリスクの回避

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

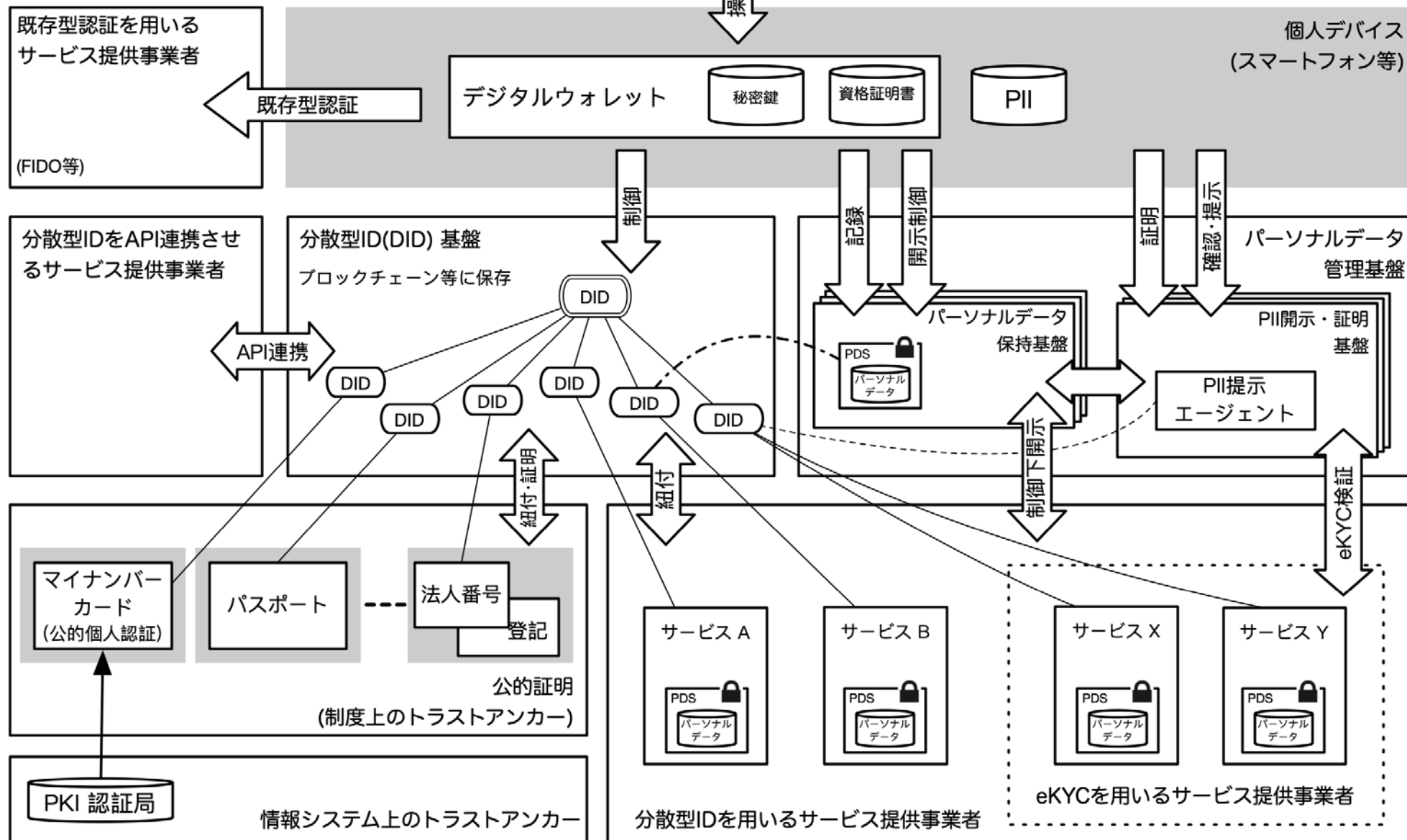
分散型IDのイメージ

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。

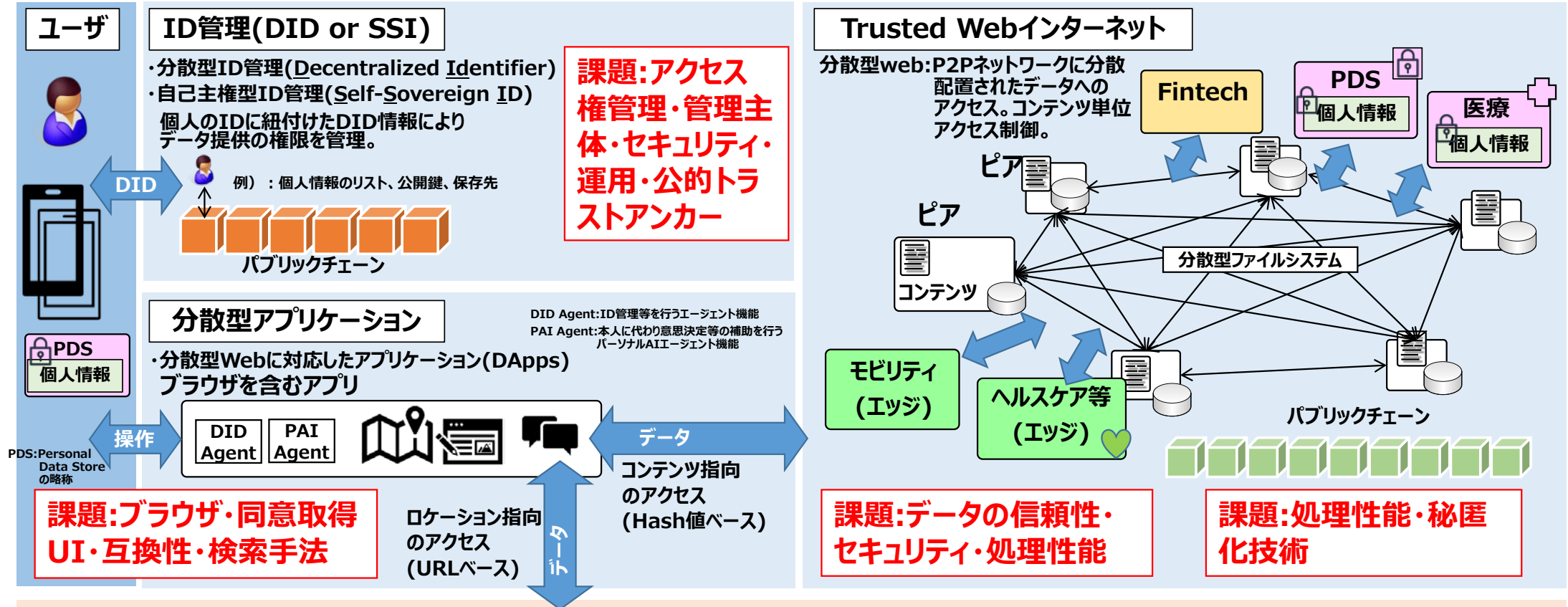


FIDO: Fast IDentity Online
DID: Decentralized IDentifier

PII: Personally Identifiable Information
PDS: Personal Data Store

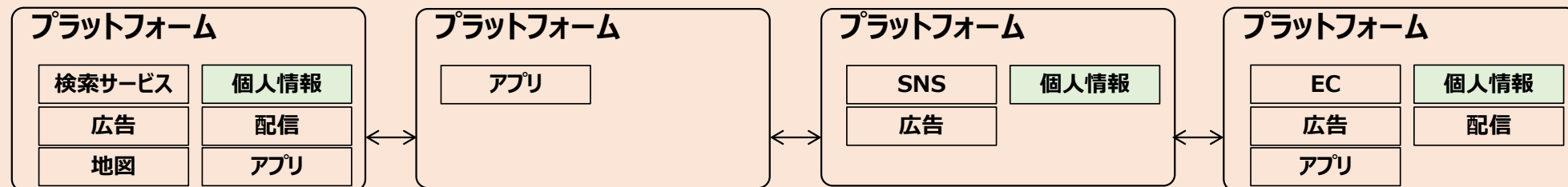


Trusted Webの現実的な実装の姿



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。

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