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

Version 0.1 (2020/8/3)

慶應義塾大学SFC研究所 ブロックチェーン・ラボ

村井 純
慶應義塾大学 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

松尾 真一郎
慶應義塾大学大学院政策・メディア研究科 特任教授(非常勤)
ジョージタウン大学研究教授

クロサカタツヤ
慶應義塾大学大学院政策・メディア研究科 特任准教授(非常勤)

ニューノーマルと新たなインターネット文明の調和

新型コロナウイルス感染症（COVID-19）の感染拡大は、人間社会に新しい生活様式を要求しはじめている。我が国をはじめ、世界中の多くで、人間との接触（フィジカル・コンタクト）への制限が求められる中、デジタル・テクノロジーの活用は、従来のような付加価値向上という水準を超えて、すでに生命や健康の安全にとって重要な手段として位置づけられはじめている。こうした現状を、マイクロソフトのサティア・ナデラCEOは、同社の決算発表において「この 2 ヶ月で 2 年分に匹敵するほどのデジタルトランスフォーメーションが起こった」[1]と表現している。

過去30年にわたるインターネットの社会への定着や、それがもたらした様々な技術革新は、高度な技術のコモディティ化をもたらした。その結果、経済活動は大きく発展し、社会変革も含めたパラダイムシフトが絶えず生じる、イノベーションの時代を迎えるに至った。そしてこれからのテクノロジーは、気候変動や持続的成長の達成など、国境を超えた地球規模の人間の幸福に、より能動的に寄与することが強く期待されている。

特にCOVID-19は、人間とその活動にとってのデジタルテクノロジーの重要性を高め、また社会全体でそうした認識を共有することを促した。一方そうしたデジタルファーストの意識の高まりよって、現在のテクノロジーが各々のユーザのリテラシーへ依存しているこ

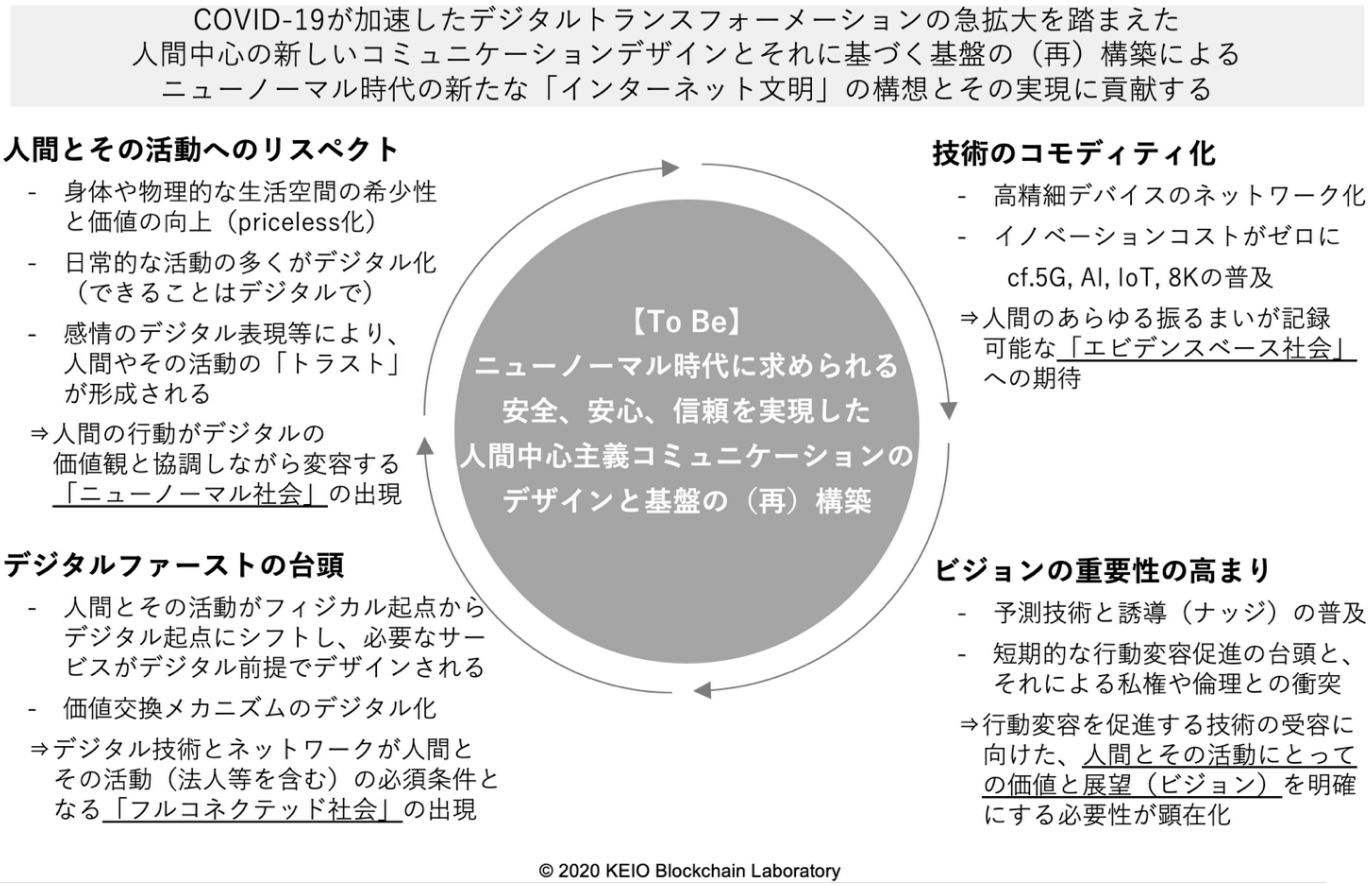
とも明らかになった。たとえば、データプライバシーに対する理解や価値観がユーザ間で異なる中で、各国で取組が進んでいるコンタクトトレーシング（我が国においては接触確認）アプリに関する議論としてある局面ではプライバシー侵害とされ、またある局面では公衆衛生に対する効果の不足が指摘されるといったギャップが生じている。

デジタルテクノロジーの興隆を前提とした社会の発展自体は、これまで多くの恩恵を地球上のすべての人間に提供してきた。この事実を踏まえた上で、冒頭に述べた通りデジタルテクノロジーが生命と健康にとって不可欠なものとなる「ニューノーマル社会」を、人間にとってより豊かなものとするためには、これまでの技術普及における課題を明確にした上で、新しい普及のサイクルを確立する必要がある。そのために必要とされる検討項目として、以下が想定される。

- 高度な技術のコモディティ化によって実現する特徴を、技術と社会の両面から理解すること
- 技術が目指す共通の目的をビジョンとして確立し、ステークホルダーを特定しながら、価値の表現と合意形成の促進を図ること
- 人間の活動をフィジカル起点からサイバー起点に再設定した上で、改めて人間中心設計を実践すること
- 人間とその社会的活動がネットワーク上ですべて表現されることを前提に、表層的な社会活動はもちろん、それを構成する人間の感情や機微などもリスペクト（尊重）したトラストを形成し、社会システムに昇華させること

下図はそうした検討項目とサイクルの構造を示したものである。

■ 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



これらは包括的な検討項目とそれによって構成されたサイクルであり、具体的な検証対象は個別に設定されるが、すべてに共通するテーマとして「デジタルアイデンティティ」が挙げられる。デジタルアイデンティティの概念的な確立、それを実現する技術基盤、そしてそれらに関する制度設計も含めた合意形成は、従来から重要な検討課題であったが、COVID-19の感染拡大によって喫緊に解決する必要に迫られている。

その際に重要なのは、人間の文化を尊重することである。インターネットは、過去30年の人間社会におけるデジタルトランスフォーメーションを推進してきた原動力であり、それを疑う余地はない。一方でインターネットがこれまで世界中の多くの人々に受け入れられてきたのは、多言語対応や文章表記（縦書き、横書き、分かち書き等の許容）、あるいは障害者へのアクセシビリティ等、人間が本来有している多様性を文化として尊重してきたからである。

インターネットはこれからの技術普及においても引き続き中心的な役割を果たす。そしてインターネットが、人間自身（理解や感情等に係る機微や他者との識別性）、その社会的な活動（日常生活、サービス、企業活動等）、そしてその文化（本来有している習慣や価値観）を尊重する姿勢は、これからのデジタルトランスフォーメーションにとって、さらに不可欠なものとなる。こうした観点を踏まえ、テクノロジーの社会的な存在理由や位置づけを明確にし、ニューノーマル時代に必要とされるデジタルアイデンティティの理想像を構想することが求められる。

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

インターネットは、それぞれのネットワークが相互に接続（インターネットワーキング）されることで構成されている。従ってインターネットにはすべてのネットワークに対して優位に立つ中心的機構が存在しない。こうした特徴をもつコンピュータネットワークが世界的に普及した結果、インターネットは今日において世界最大の分権型分散ネットワーク（de-centralized network）として存在するに至った。

こうした出自と背景はインターネットの特徴を決定づけている。具体的には、インターネットはインターナショナルではなくグローバルなネットワークである。ここではインターナショナルとは、ネーション（国家）内でネットワークが存在し、それが世界的に統合（例：国連等による合意形成）されたルールに基づいて相互に結合されることで構成される状態を指しており、インターナショナルネットワークとはそうした形態を有している（例：国連の下に設置されたITUがルールを形成して構成される電話網）。

一方、インターネットは原理的にはこうした構造を前提とせず、あくまでプライベートなネットワークが、政府から独立した主体的な技術者やステークホルダーによる意志決定に基づいたネットワークの構築と運用がなされている。すなわち、インターネットは、その理念の下ですべてのステークホルダーがフラットな状態を予め想定しており、グローバルな性格を色濃く有している。

こうした特徴は、イノベーション（技術革新と普及促進）に大きく貢献した。その結果が過去30年における「インターネットを中心としたデジタルトランスフォーメーション」であり、世界中のほぼすべての人間が、何らかの形でその恩恵を受けていることには、疑いの余地はない。またすでにインターネットのこうしたパラダイムに基づき社会システムが変化しはじめていることから、このようなパラダイム自体は今後も発展を継続する蓋然性が極めて高い。

しかしながら、イノベーションが進んだことによる様々な課題も顕在化してきた。たとえば、今日において「フェイクニュース」が世界的に大きな課題となっているが、これはニュースの信頼性（広義のトラスト）を確保するための構造が未確立であるがゆえに起きている問題である。またそれ以外にも、たとえば行政サービスにおいてデジタルによる本人確認が複雑であるがゆえに、かえって手続きが煩雑化して行政サービスの品質が低下する（迅速かつ柔軟性のある役務提供の阻害等）といった事象も散見される。

COVID-19によるデジタルトランスフォーメーションの急加速は、インターネットの普及が進んだがゆえの様々な課題を次々に顕在化させている。このような課題は、前項で述べた「デジタルアイデンティティ」が未だ確立されていないことに起因すると考えられる。そのため、課題解決に向けて、ユーザを含めたステークホルダの識別や正当性の確認、コンテンツの識別や正当性の確認を、デジタルファースト時代の社会基盤として確立することが必要である。

また、このような顕在化した課題を俯瞰すると、従来の社会システムが担ってきた「トラスト」の構造をインターネット上で実装する際に生じていることがうかがえる。従って、前述したような課題解決は、トラストを確立した暁に提供される様々なサービスに関するビジネスモデルの再構築や関連するスキームの合意形成を目指し、そうした目的と整合する理念に基づいた技術的手段によって実現されることが強く期待される。

コミュニケーションにおける信頼（トラスト）の要素分解

デジタルアイデンティティの未確立とそれに伴うトラストの不成立によって引き起こされている諸課題は、前項の通り多岐にわたる。そしてそれらが影響を及ぼす対象は、もはや単純な処理や取引といった定形業務にとどまらない。

たとえば、これまでのフィジカルスペースにおける活動で、人間自身が身体的な認知機能によって補完してきた感情や表情といった、人間の振るまいに関する機微が、サイバースペースで完結する環境下において十分に代替されず、情報として欠損するようなことが、すでにWeb会議等によって先駆的に生じている。こうした情報の欠損はこれまで単なるアプリケーション品質（画像の解像度等）として位置づけられてきたが、フィジカルとサイバーの主従逆転が起きる「デジタルファースト」の時代においては、結果的に業務遂行を困難にする可能性も考えられる。実際、すでに民間企業同士の契約行為や行政サービスなどでも、同一の構造に起因する生産性低下や機能停止などの障害が散見される。

こうした事象を踏まえれば、特定のアプリケーションや特定分野に関連するシステムアーキテクチャやデータ流通構造の要件だけでは、問題の特定には至らない。むしろ人間自身の振るまいも含めた社会的活動の総体として規定する必要に迫られている。そのため本稿では、こうした人間の振るまいを含めたトランザクション（やりとり）を総合し、「コミュニケーション」と称することとする。

ここでの「コミュニケーション」を円滑に、かつ社会の観点で問題がないように実現するために重要な観点が、トラストの確立である。トラストとは、事実の確認をしない状態で、ユーザまたはその他のステークホルダーが、ある系が期待した通りに振舞うと信じる度合い[2]とすることができる。ユーザにとって必要な全ての事項をいちいち確認する行為というコストを大きく引き下げつつ、システム全体のリスクをステークホルダーで分担をすることを狙っている。トラストされる対象が負担するトラスト維持のためのコストと、期待を裏切ったときにその対象が負うリスクを見比べ、利用者の視点でトラストできるかが算定される。その上で、系としてのトラストを構築するための仕組みとして「トラストフレームワーク」が定義されている。これには、期待されるトラストのための技術の実装、運用ルールの設定と遵守、失敗時の救済手段が含まれる。その上で、トラストの度合いをサービス提供者が宣言する自己宣言モデルと、第三者が確認を行う第三者確認モデルがある。

たとえば、暗号技術を実装した製品のトラストは、第三者確認モデルの組み合わせとし

て、以下のように構成されている。

- 暗号アルゴリズム自体が、専門家の評価を経て政府が公開した電子政府推奨暗号リストに掲載されているもので
- その実装がJCMVP[3]などの認証プログラムで認めらており
- その製品を組み込んでいるシステムは、ISMS（ISO/IEC 27000シリーズ）によるリスク分析と情報セキュリティマネジメントプロセスにしたがって運用されている

もちろん製品が期待通りのセキュリティを提供しているかどうかを、ユーザが確認することは無理であるが、複数の主体による第三者認証を組み合わせることで実現している。

個別の要素、ひいては系全体をトラストするかどうかは、トラストは関係する主体が掛けているコストの総和と、問題が発生した時のリスクのバランスの問題である。これはブランドの価値に似ており、ある問題が発生した時に発生するブランド価値の毀損と結果として生じるビジネス上の損失があり、その損失が発生しないように企業なり人間は手間や時間（＝コスト）を掛ける。このコストが十分に掛かっていると認められれば、事情をよく知らない人でも、対象となる企業や人間をトラストする。故障率が低く、メンテナンスが行き届いた製品を提供する会社の製品を人が信頼して購入するのは、このような理屈である。つまり、トラストを構築するには、リスクの認識があり、そのリスクをカバーするコストを掛けることが重要になる。

多くのビジネスでは、このコストとリスクの関係についての経験則や相場感が存在し、それによって保険のようなビジネスが成立している。一方で、このコストとリスクの関係が一定ではなく、不確実性が存在するケースが多い。対面でのコミュニケーションには、この不確実性を補う要素が存在するとみなせる。しかし、ニューノーマルにおいてこの要素がなくなり、全てのコミュニケーションがオンライン上で行うようになると、前述のフェイクニュースの例にあるように、ユーザがその系をトラストできるかどうかを判断する材料が少なくなることを想定する必要がある。そのため、オンラインのみでのコミュニケーションの時代に相応しいトラストの構成方法が必要になる。

デジタルファーストにおける人間の活動にまつわる信頼の形成の必要性

インターネットとWebによって、強靭で、グローバルで、多角的な（multi-lateral）なデータ交換は実現された。しかし、転送されるデータが、人間の社会的活動において信頼に足るものであるかどうかについては、現在のインターネットアーキテクチャは十分な機能を有していない。複数の人間による、果たすべき特定の目的を持ったコミュニケーション（たとえば保険契約とその実行）について、インターネット上のデータだけでは、社会が要請する法的責任を果たすのに十分ではない。

複数の人間によるコミュニケーション（以下、コミュニケーション）をインターネット上

で実現する際に、法的責任を果たすためには、少なくとも以下の要素が必要である。

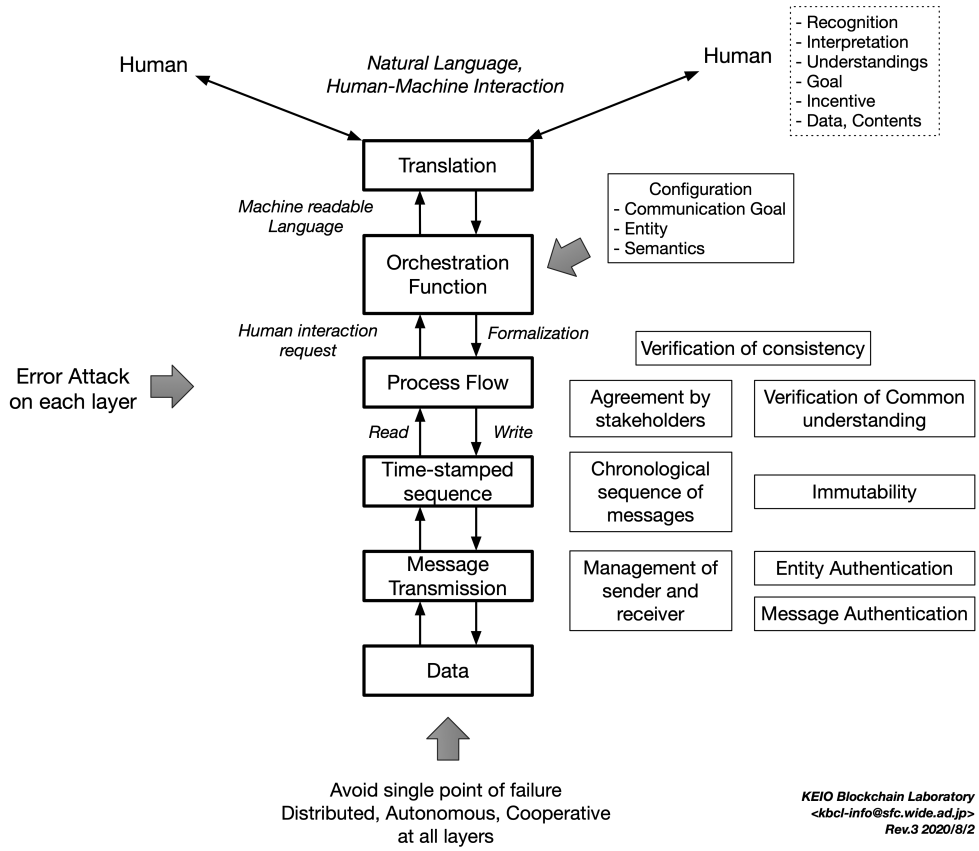
1. コミュニケーションのゴールが、参加者において共通の理解として確認されていること。
2. コミュニケーションに関わるエンティティ（人間、及び機械）が認証されていること
3. エンティティ間で送受信されるデータが改竄されておらず、作成者が認証されていること
4. コミュニケーションに関わる、データ送信、エンティティによるデータ入出力、及びデータ加工などのプロセスの前後関係が、特定可能であり、また検証可能な形で記録されること。
5. コミュニケーションにおいて、人間が介在する全ての段階で、その時点の状態に対して、全ての人が同じ理解をしていることを逐次確認できること。その結果として、コミュニケーションの最終結果は、同じ理解のもとになされた結果であることを事後で確認できること。

上記を実現するためには、既存のインターネットのレイヤーに加え、自然言語で書かれたコミュニケーションのゴールを計算機で理解できる言語に落とし込み、分散した計算機によるプロトコルとして構成し、そのプロトコルが完了するように構成、設定、管理の自動化を行う必要がある。

上記の要素の中で、2.と3.は、既存のインターネットにおける認証プロトコルを拡張する形で実現する。4.はPermissionless Blockchainを用いることで実現できると考える。その際に、プロセス、データ、エンティティなどを特定する（Identification）ための機構が必要である。また、複数のエンティティによるコミュニケーションのプロトコルは、Blockchain上のスマートコントラクトを用いて実現することもできる考える。ただし、Blockchainやスマートコントラクトのみで、信頼が構成されるわけではなく、1.と5.で示すように、プロトコルの実行の途中段階における人間による確認行為や、人間が認識しているコミュニケーションとプロコルとして機械的に実行される処理との対応の正しさの保証など、コミュニケーションとしての一貫性を保証するためのレイヤーも別途必要である。

この全体構成を図で示すと以下のようになる。

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



- **概要**
  - 人間、その活動（法人を含む）、接点としてのデバイス、計算機、等の構成要件の、分散処理の間での権限移譲に関する合意を定義する
  - Configurationを解釈した上で、プロセスフローの一部として書かれる
- **プロセスフロー**
  - 従来のプレゼンテーションレイヤーやアプリケーションレイヤーに加え、Translation Function (Layer)とOrchestration Function（Layer）を再定義する
- **実際の構築例**
  - コミュニケーションを行う場合には、第1ステップとしてConfiguration Set Upを行い、その後コミュニケーションの実行（完了）までを第2ステップとして行う

人間中心のグローバルデジタルアイデンティティの必要性

我々が目指すのはインターネットの再構築ではなく、既存のインターネットの上にオーバレイとして、個人の安心と安全を確保しながら、人間の社会的営みをオンラインで実現するためのコミュニケーションプラットフォームを構築することである。そのため、当初はインターネットに備わっておらず、今日までの様々な追加的要素の組み合わせによって辛うじて実現されている個人の安心と安全を確保するためのメカニズムを、グローバルネットワークの視点で再構築する必要がある。その際、信頼を形成するためのメカニズムが鍵であり、そのメカニズムの核として、インターネットの特性に合致したグローバルで用い

ることが可能なデジタルアイデンティティの確立が極めて重要であることを、ここまでで述べてきた。

ここで、インターネットにおけるアイデンティティの活用場面についての経緯を見てみよう。インターネットは、ネットワークドメイン（ネットワークの管理主体を共通に持つネットワークの集合）をつなぎ合わせることによって、グローバルなデータ交換システムを作り出した。インターネット上で様々なサービスが提供されるようになったが、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かったため、サービス毎にアイデンティティシステムを用意するデザインが広く用いられるようになった。このデザインでは、そのサービスの管理領域（以下、サービスドメイン）にて管理されたアイデンティティ（以下、サービスアイデンティティ）をユーザごとに用意する。ユーザは、サービスアイデンティティをサービスの利用開始時に作成するか、サービスドメインが許可する範囲で、他のサービスのアイデンティティを代用する。いずれの場合においても、サービスを利用する過程で生み出される情報は、用いられたサービスアイデンティティに紐付き、そのサービスドメイン内に保存され、利用されることになる。つまり、現在用いることができるデジタルアイデンティティは、特定のサービスドメインに閉じたものであり、ロックインされている。

すなわち、グローバルなデジタルアイデンティティとは、端的には、サービスドメインへの束縛から解放されたデジタルアイデンティティである。我々が必要とするデジタルアイデンティティ構築のための特性をあげるならば、人間中心で、グローバルで、かつロックインされないものでなければならない。また、ユーザにとって使いやすく、手間がかからず、制約が限り無くゼロに近いといった特性を持つべきである。そのような特性をもつ「グローバルデジタルアイデンティティ」の構築が急務である。

グローバルデジタルアイデンティティ構築における検討課題

デジタルアイデンティティの構築には、関係各方面によって、様々な検討が相当なスピードをもって進められている。また、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 Soverign Identity）も提案されている。

我々は、それらのアクティビティから独立して提案するのではなく、現在実装されたり検討が進んでいる技術を構成要素としたインターネットにおけるグローバルデジタルアイデンティティの議論を進めている。以下で、その議論の一部と、現時点での検討結果を示す。

まず、エンドユーザの視点での課題を以下に挙げる:

- サービス毎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付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

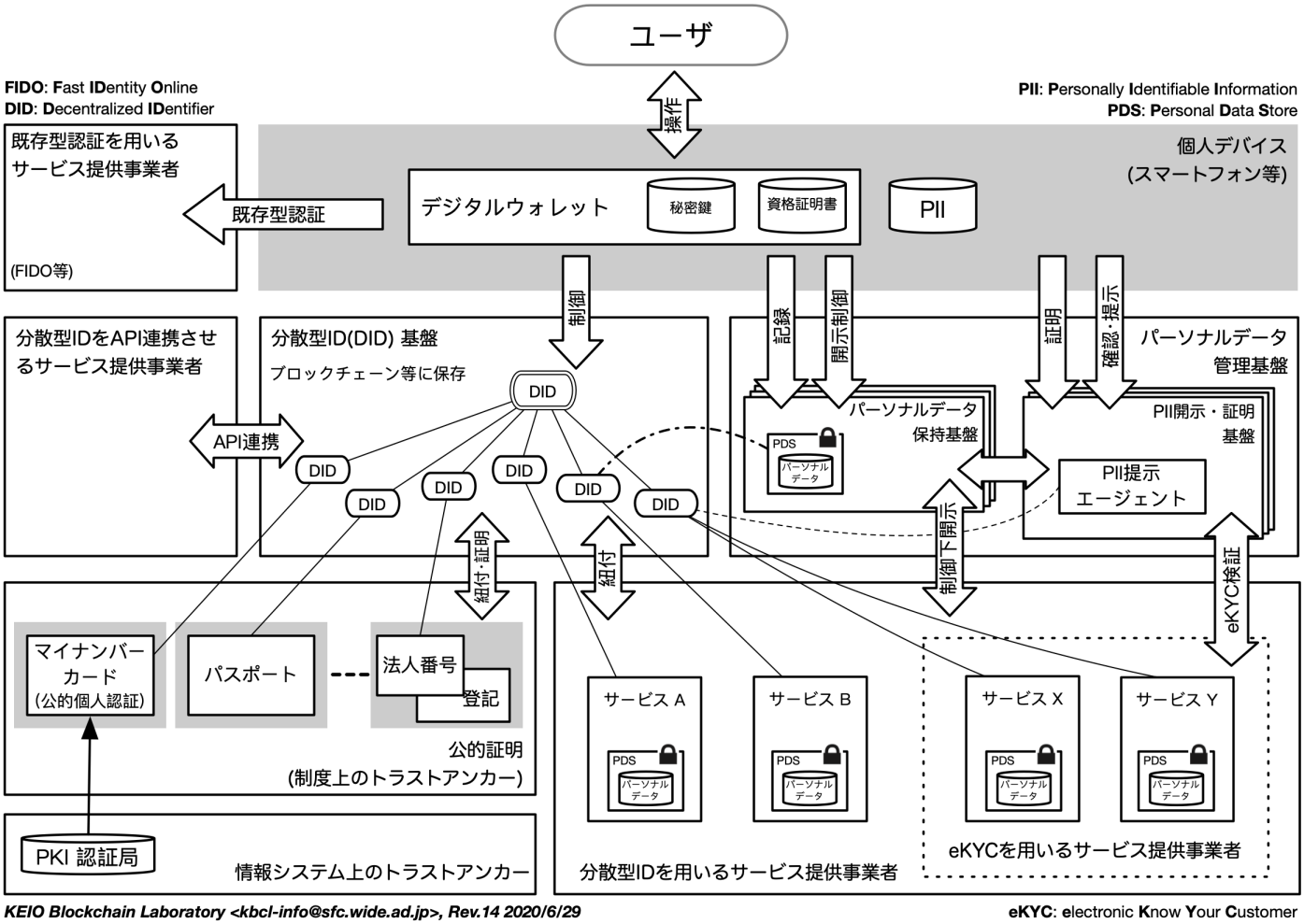
技術側面では、以下の構成要素の組み合わせと手法を検討している:

- グローバルに用いることができる名前（identifier - 識別子）は、標準として成立しており、様々なIdentifier技術との間での読み替えが可能である、Uniform Resource Identifier (URI)[4]を中心とする。ここでの名前はURIでも構わないが、仮に「GID」とする。
- 現在検討が進んでいる分散ID(Decentralized Identity/Identifier)技術[5]での検討結果を適用する。DIDにおける「名前」はURI形式であるので、表現形式としてはGIDはDIDを包含している。DIDの実装にはブロックチェーン技術に基づくものがある。
- Verifiable Credential技術[6]を転用し、複数のGID間の関係性と関連するメタデータを表現する。このためにブロックチェーン技術を活用する。
- 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する。
- 依存関係を記述する際に、高い自由度が必要な場面では、直接的な結びつきではなく、代理となるGIDを介在させることで、間接的な結びつきとなるようにする。

以下に、この手法によるメリットを述べる:

- GIDによって、あらゆる名前で区別出来る（識別可能 - identifiableな）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となる。
- 必要に応じて、GIDとGIDの間を間接参照とすることで、結びつきの変更のためのフレキシビリティが向上する。
- DID技術の適用により、自己主権型のアイデンティティを活用することが可能となるばかりでなく、既存のアイデンティティプラットフォームと連携を計れる。すなわち、先に議論したサービスドメイン群と連携できる。
- 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。
- Verifiable Credential技術の活用により、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（密結合）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。

一例として、デジタル市場競争会議[7]による「デジタル市場競争に係る中期展望レポート」で示されている図[8]に基づき、ここまでの検討結果を図示したもの以下に示す。詳細な議論は、今後レポートとして用意する予定である。



参考文献

[1] 人間の創意工夫と AI の融合で力が高まることが最先端企業の動向で明らかに、Microsoft Japan News Center https://news.microsoft.com/ja-jp/2020/05/13/200513-leading-businesses-reveal-the-power-of-combining-human-ingenuity-with-ai/

[2] 松尾、楠、崎村、佐古、佐藤、林、古川、宮澤、「ブロックチェーン技術の未解決問題」、日経BP、ISBN-13: 978-4822258429

[3] 暗号モジュール試験及び認証制度, https://www.ipa.go.jp/security/jcmvp/index.html

[4] RFC3986: Uniform Resource Identifier (URI): Generic Syntax, January 2005, Internet Standard, Online: https://tools.ietf.org/html/rfc3986

[5] Decentralized Identifiers (DIDs) v1.0 https://www.w3.org/TR/did-core/
(現在はWorking Draft。執筆時の最新版は https://www.w3.org/TR/2020/WD-did-core-20200728/)

[6] Verifiable Credentials Data Model 1.0 https://www.w3.org/TR/vc-data-model/

[7] デジタル市場競争会議

http://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/index.html

[8] デジタル市場競争に係る中期展望レポート、デジタル市場競争会議、2020年6月16日
http://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/dai4/siryou3s.pdf

お問い合わせ等

本件についてのコメント及びご質問などを含むお問い合わせについては、慶應義塾大学SFC研究所 ブロックチェーン・ラボまで、下記emailアドレス宛で、ご連絡頂きたい。

kbcl-info/at/sfc.wide.ad.jp
(/at/ は @ に置き換え)

本ラボについては、下記URLをご参照されたい。

https://kbcl.sfc.keio.ac.jp/

なお、この文書は、随時更新し、以下のURL にて公開する予定である。

最新版のURL:
https://kbcl.sfc.keio.ac.jp/TR/global-digital-identity-for-new-normal/
本バージョンのURL:
https://kbcl.sfc.keio.ac.jp/TR/global-digital-identity-for-new-normal-20200803/
