【第 8 回 Web3.0 研究会】議事要旨

概要

- 日時：令和 4 年 11 月 24 日（木）13 時 30 分から 15 時 00 分まで
- 場所：オンライン開催
- 議事次第
  - 開会
  - 議事

    (1) 有識者ヒアリング（イーサリアム・ファウンデーション 宮口あや様）

    (2) 分散型アイデンティティに関する委託調査中間報告
  - 閉会

資料

- **「議事次第」**
- 【資料 1】宮口様提出資料
- 【資料 2】**デロイトトーマツコンサルティング提出資料**

主席者

構成員

- 國領　二郎（慶應義塾大学総合政策学部　教授）
- 石井　夏生利（中央大学国際情報学部　教授）
- 河合　祐子（Japan Digital Design 株式会社　CEO
  株式会社三菱 UFJ フィナンシャル・グループ　経営企画部　部長
  株式会社三菱 UFJ 銀行　経営企画部　部長）
- 殿村　桂司（長島・大野・常松法律事務所　弁護士）
- 藤井　太洋（小説家）
- 松尾　真一郎（ジョージタウン大学　研究教授）

デジタル庁（事務局）

- **河野大臣、大串副大臣、尾﨑大臣政務官、楠統括官、野崎参事官**

議事要旨

- 有識者ヒアリングにつき、イーサリアム・ファウンデーションの宮口様より説明。
  - 日本で高校教師をしていたが、教師が外へ出て学ばないという環境に疑問を感じていたこともあり、アメリカへ行き、サンフランシスコで Kraken という暗号資産取引所の初期メンバーとしてチームに参加したころから、業界に関与している。
  - ブロックチェーンに興味を持った理由は、マイクロファイナンスなどのファイナンスインクルージョン、世の中の仕組みを変えられる技術であるためである。イーサ

リアム・ファウンデーションのメンバーからチームをリードしてほしいと声が掛った際は、今後社会課題のソリューションであるアプリケーションがつくられる、唯一信頼できる、パブリックなブロックチェーンであるイーサリアムの存続が、業界のためのみならず、世界を良くするためにいかに重要かを考え、使命を感じて引き受けた。

- イーサリアムのスマートコントラクト機能の技術の基本の部分は既に議論されているため、今回はそのビジョンと社会的意義について、特に日本の将来を考えてお伝えする。
- イーサリアムプロトコルを「Protocol for human coordination」と表現している。human、「人間」が入っていることが重要。革新的な技術ができると、技術だけが注目されがちで、技術だけで世界が良くなるような話になりがちだが、あくまでも人間が中心で、意図やコーディネーションが複雑になっている現社会で技術が補足をする、そのコーディネーションをするプロトコルということである。
- プロトコルを作り、維持し、ソリューションを作っていくエコシステムがどうあるべきなのか、その答えを「Infinite Garden」というビジョンで共有している。イーサリアム・ファウンデーションのチームに年末に送るメッセージの中で、自分にとってのイーサリアムのビジョン は Infinite Garden と言ったことから始まった。Infinite は、Finite and Infinite Games という本から影響を受けた。永遠のプレーヤー、Infinite player は、ゲームに勝つためではなく、ゲームを続けるためにゲームをする、プレーをするという意味。これは私が見るイーサリアムのコミュニティーの良さと合致している。更に、なるべく自然な成長を促すということで、Garden と表現している。今コミュニティーで浸透してきている。
- Infinite Garden のエコシステムの中でのイーサリアム・ファウンデーションの役割は、エコシステムのサポートをするために、コントールせずに、なるべく外に機会を与えること。一緒にエコシステムを育てるチームを外に増やしていくこと。まさに Infinite player を増やしていく活動をしている。
- 年間約 50 億から 100 億円をパブリックグッズであるインフラに貢献できるチームや、エコシステムの健全さに貢献できるチームへ、投資ではなく助成金を出している。その他、裏方でコミュニティー活動のコーディネーションをしたり、新しい研究開発のサポートをしている。
- イーサリアム・ファウンデーションの基本理念は、3 つある。

  1 つ目は、長期的思考である。イーサリアム・ファウンデーションがいなくなった後でも、エコシステムがどうやって健全に存続していけるかを考える。

  2 つ目は引き算の美学である。イーサリアム・ファウンデーションがコントロールするのではなく、いかに引き算をして、みんなに力を分散していけるかという点。

  3 つ目は、コミュニティーの価値観。オープンソースといった大事な価値観を伝え

拡げていくというところ。

- なぜイーサリアムなのか、なぜイーサリアムがこれほど成長したのか。他に勝つことが大事なのではなく、将来どのような社会にしたいのか、どのように社会を良くしたいと思って作られているのか、が大事である。「クリプト」、「Web3.0」、「ブロックチェーン」など様々な言い方があるが、それらのどの部分が社会を良くできるのか、つまり妥協できない部分が明確かどうかが肝心である。イーサリアムにおいて、妥協できない部分は「分散型」であるということ。
- そもそも分散による問題解決を目的としているため、できるだけ分散にこだわることである。分散と言っても技術の部分だけではなく、エコシステムの在り方としても大事なこだわりである。

  エコシステムの在り方としてこだわっている基本理念が 3 つある。1 つ目は「オープンソース」。単にソースコードがオープンであればいいということではなく、検証やコピーが可能で、誰もが参加して改善ができるものでなければ意味がない 2 つ目は「パーミッションレス」。許可なく誰もが参加でき、使え、開発プロセスにも参加ができる。3 つ目はフォークができること。実際に今までも起きている。

  例えば良いプロジェクトがあれば、改善して他の新しいプロジェクトに変換できるかどうか。これらの基本理念が常に日々の活動にあることが重要である。
- 具体的な例としてウェブサイト「ethereum.org」を挙げる。オープンソースで、サーバーやチームをサポートし、コンテンツは全てオープンソース。950 人程のコミュニティメンバーがアクティブに参加し、技術やコンセプトの説明方法を考案している。コミュニティーが一番良いと決めたコンテンツを使っているため、イーサリアム・ファウンデーションの決断権はない。
- Ethereum.org の翻訳についても、世界各地に 48 の言語に対応するボランティア 5,000 人以上が行っている。学ぶきっかけにもなるため、希望する人が翻訳をし、それを採用する。組織としてはそのシステムをサポートする役割をしている。
- 「分散」やこういったエコシステムの在り方は、本気で探求する。英語では single point of failure と言うが、システムの中で誰か 1 人に力が集中し、全体の欠陥となりうる場合、それは中央集権の問題、セントラライゼーションの問題であるため、それを技術の部分だけではなく、ありとあらゆる形で防ぐ。
- そのために全てを重複させることが大事。ノードの数が多ければ、セキュリティーが強くなる。更に例えばイーサリアムを使う時に必要なクライアントソフトウェアが 1 種類しかない場合、それに問題があってはいけない。したがって、クライアントソフトウェアの数も多くなければいけないし、誰もが様々なものを使っている環境が望ましい。皆一番良いものを使いたいため難しいが、偏り過ぎないように、可能な限りプロアクティブに活動している。
- ウォレットの分野でも、メタマスクが一番使われている状況を受け、メタマスクだ

けでいいのか、何かあった際にはどうするのか、なるべくウォレットもたくさんあった方がいいのではないか、そして、そのために私たちはどのようなことをしたらいいのかなど、常に考えている。

- ファンディングの機能も 1 箇所に集中してはいけない。パブリックグッズをサポートできる機関がイーサリアム・ファウンデーションだけではない方が良いので、他の組織が同じような機能が果たせるように即す。本気で探究するという点に関連して、イーサリアムで私が一番大好きな部分を英語で「Intellectual honesty」と言う。知的誠実さ、正直さのことであり、出来ないことを出来ないと公言すること。アイディアを持った参加者が入り、イーサリアムは、最初にあったプランから変化し、改善している。敢えてオープンに、正直にすることにより、多くの人が参加する。結果として最初のアイディアはヴィタリック氏が作ったが、現在ではヴィタリック氏以外の人がほとんどのアイディアを出している。
- 分散の探究という点で最後に 1 点、イーサリアム・ファウンデーション保有のイーサが全体のわずか 0.28%であることを強調したい。更に、助成金を外に出しているため、この数は毎年減っている。エコシステムが成長すればするほど、イーサリアム・ファウンデーションのイーサ保有量が減り、エコシステムの依存が少なくなるモデルを目指している。既に実証されてきているが、こだわって取り組んでいる部分である。
- 次にグローバルな視点から話をする。昨今、ウクライナなどの特別な状況もあるが、一般的には途上国にニーズがあり、機会もあるため途上国の例を中心に紹介する。
- まずは中南米の現状。インフレが酷い状況で、市民がインフレの波の中で生きていかなければいけないアルゼンチンでは、女性の参加率が高い。新しい楽しめる技術ではなく、生活に必要な技術として興味があり学んでいる。
- 今年、イーサリアム・ファウンデーションが開催するイーサリアムで最大規模の年次イベント「Devcon」を南米のコロンビアのボゴタで開催した。オリンピックの効果のように、ブラジル、パナマ、メキシコ、ペルー、チリなど周りの中南米の国々でコミュニティーが増え、自らイベントを次々に開催した時期が 2 か月程あった。イーサリアム・ファウンデーションが Devcon を行ったことも一因であるが、それ以上にコミュニティーが自分のイニシアチブとして開催したことが大事である。
- 国の政府よりは自治体のレベルで盛り上がりを見せているのも特徴。例えばブエノスアイレスは先見の明があり、代表が Devcon に参加したが、様々なプロジェクトが行われており、ブエノスアイレスをスタートにアルゼンチンの国全体を改善したいという姿勢になっている。
- コミュニティーの草の根活動も拡大している。例えば、スペイン語の教育コンテンツは、次々に増えており、YouTube にも動画が掲載されている。オンラインでもフィジカルでも活動が増えているため、イーサリアム・ファウンデーションはそうい

った草の根活動をサポートしている。

- 具体的なプロジェクト例として、メキシコの 2 つのプロジェクトを挙げる。1 つ目は、日本語で無尽、頼母子講と呼ばれるような、地域のコミュニティーが集まり貯蓄や積立て、前借りを同時にする仕組みである。メキシコではタンダと呼ばれ、人口の 20%以上が参加している。これにスマートコントラクトを絡ませて、詐欺の阻止や、個人の信用履歴を構築できるプロジェクトが始まっている。
- もう 1 つは、ブエノスアイレスも活用しようとしている分散型 ID の例である。公共財の欠陥を直さないと、国が良くならないと強く感じている Goctech 分野の市民のチームが制作している。
- 次にアジアに移る。ベトナムでは人口の 2 割以上が暗号資産を保有しているという報告もある。明日からイベントがありホーチミンにいるが、盛り上がってきているところである。
- アジアにおける政府側の話について、例えばシンガポールでは、金融規制面では慎重に見つつも、研究開発促進のメリットを理解し、政府がイーサリアムのプロダクトを開発している。
- 日本への期待と課題については、まず、中南米のインフレや東南アジアのゲームというアダプションに繋がるニーズやアングルは何かというところから考えてもらいたい。Web3.0 を「やらなければいけないこと」と捉えるより、どこの部分に強みがあり、興味・関心があるのかというところ発見してもらいたく、若い人たちに頑張っていただきたい。
- 2 点目として、謙虚さは日本人の良いところでもあるが、日本が「Web3.0 で遅れている」、更に「Web3.0 鎖国」という言葉まで聞く。ネガティブに言う前に、日本特有の力を引き出すことができると期待している。
- 例えば長期的思考について、日本人には説明しなくてもある程度分かるコンセプトだが、アメリカ人などには説明しても理解してもらえない。また、日本人のチームワークは世界で圧倒的に良い。ボスがいなくても、チームとして成立する。日本で育ったため、それが当たり前だと思うが、海外では当たり前ではない。
- 元々日本には DAO 的文化があるため、その部分を生かしながらこの技術を追加すれば面白いことができるはず、ということをポジティブに伝えていきたい。
  Web3.0 は、シリコンバレー的ではないところの方が適している。特に若い人たちにはそういうところを強めてほしいと考えている。
- 他にも、完璧を求めることは日本の良いところでもあるが、イーサリアムが発展してきたように、最初から完璧を求めずに発展していく可能性を伸ばすことや、技術やコミュニティーの作り方のオープン性は、日本がイーサリアムから学び、日本のものづくりなどに活かせるのではないか。
- 一方、決定的な課題としては、コミュニティーの形成がこれからであること。趣味

が合う人が集まるだけではなく、自分たちで作る力があるコミュニティーをどのようにして増やしていけるかも重要。我々としても慎重にサポート、見守りをしていく。

- 12 月 3 日に東大の Web3.0 のチームが行うハッカソンに呼ばれている。夏に会話した後、自分たちで開催することにしたという話を聞き、サポートしたく参加する。そのような活動が起きてくると楽しいと思っており、若い人たちから可能性を感じている。
- 今まではトレーディング、投機への関心が強いが、技術開発のところに目を向けてほしい。例えば規制に関しても、規制しなければいけない部分は規制する一方で、どうすれば技術を成長させられるかという点、技術開発への考え方のシフトは、国全体で必要だと考える。
- イーサリアム・ファウンデーションとしては、草の根コミュニティーの核となるような人やチームをサポートしたいと考えているが、例えばイーサリアムのカントリーマネジャーといったポジションは持たないことにしている。イーサリアムはどこかの企業のプロダクトではなく公共財であるし、カントリーマネジャーのような人がいることによりコミュニティーの力が伸びないからである。コミュニティーであるため自ら作ってほしい。しかし、核となるリーダーの人たちをサポートすることはできる。バランスを見ながら、厳選してサポート先を探している。
- 来年、コミュニティーの中で基準の高いハッカソンをグローバルに運営しているチームが、ETH Tokyo という大規模なハッカソンを開催したいと考えている。開催される際は、是非お力添えいただきたい。
- 日本への期待を実現し、どのように課題解決を促進していくかという点で、私たちの大事な哲学である引き算の美学がどのようにイーサリアムのコミュニティー発展に活かされてきたか、最後にもう一度お話ししたい。
- イーサリアム・ファウンデーションに入った当時は、研究開発者の集まりで、しっかりとした団体ではなかった。しかし、資金もある程度あり、イーサリアムの CTO や、CSO など世界中のトップタレントはイーサリアム・ファウンデーションが雇い、ベストなプロトコルを作るべきという意見、プレッシャーが強くあった。こうした足し算の考え方は成長中のスタートアップや、他のブロックチェーンを所有している会社にとっては当然であるが、イーサリアムのコミュニティーが持っている真の力を活かすためには、逆の道を行かなければいけないと考えた。私が日本人であることもあり、引き算の文化を伝えていき、元々あったものを引き出していくというやり方を採用した。これは美学だけではなく、イーサリアムの分散を保つのに決定的なストラテジーであると思っている。故に引き算の美学なくして、今のイーサリアムの成長はなかったのではないか。
- 先ほど挙げた Ethereum,org もその一例。他にも、イーサリアムのアドレスを

ayamiya.eth」などの簡単な名前にし、自分の ID としても使えることができる「ENS」と呼ばれるアプリケーションがある。ENS は元々イーサリアム・ファウンデーションに属するチームだったが、あくまで一アプリケーションであるため、プロジェクトが開始するタイミングで卒業することになり、独立し、今では DAO を作り、イーサリアム・ファウンデーションのサポートの必要も無く、自分たちで存続していけるようになった。引き算の一例である。

- もう 1 つの例として、今年一番大きい出来事だった「マージ」を挙げる。ネットワークの合意形成の方法を Proof of Work から Proof of Stake へ移行するという大きなイベントであった。消費電量が無くなるということでも大きな意味はあるが、飛行機のエンジンを飛行機が飛んでいる状態で改善するようなもので、最大の数のアプリケーションが動いているプロトコルの改善をすることは、偉業である。更にその偉業を分散型に、イーサリアム・ファウンデーションのメンバーのみではなくコミュニティーのメンバーも含め全員で取り組んだ。
- そもそも関わったメンバーは各地に分散しているため、オフィスで一緒に作業するのではなく、1 か所で盛り上がることはないが、全員が Infinite player で、自分たちが勝つためではなく、これが必要だと考え、分散型に全員で成し遂げたという部分が一番の偉業であると考えている。
- 究極的にはイーサリアムの可能性、技術の可能性、Web3.0 の可能性は、1 つの団体が所有するには大き過ぎる。可能性がどのぐらいあるのか想像できないのが正しい。想像できないほどの大きさであるため、より引き算が必要ではないか。
- 世の中では残念な事件も起きているが、自分の力だけを足し算しようとしたところで問題が起きている。世の中の表に出ている問題は、この技術とは全く関係なく、誰かがコントロールしようとした結果ということでもある。力を引き算した後に、どのような人に渡すかというところは、引き算の大事さを分かっている人には伝えていかなければならないといつも意識している。そうではないところが力を持つことは、なるべく防ぐようにしているが、今業界は混沌としているため、この点は特に大事であると考えている。

- 引き算の話は重要なキーワードだと思うが、引き算の定義が分からない。その上で、技術を見ていて感じるのは、例えば Solidity という言語の存在やスマートコントラクトを書くことはイーサリアムの特徴であると思うが、一方で、Solidity の言語そのものや、オラクルを使って拡張するスマートコントラクトに引き算が見えない。
- ブロックチェーンが目指す single point of failure の除去という理想が、オラクル問題があると解けなくなるのと同様、目指している理想の引き算という点と、実際のエンジニアリングで実現できていることに差があると思う。実際どの辺を目指されているのかとお聞きしたい。
- 具体的な質問として、日本で技術開発に関して規制とあるが、私自身はコンピューター

プログラムを書いていて、規制を意識したことがない。どのような規制を具体的に言われたことがあるかお聞きしたい。

- もう 1 点、中南米で教育されている Web3.0 人材の種類について興味がある。Web3.0 という今回の掛け声が低くなっていった時、残るのは人材ではないかと思うが、その後、どのような人材が世界を動かしていくのか、あるいは残るのか。その点について意見があればお聞きしたい。
  - 現段階で例えば Solidity の言語がパーフェクトかと言えば、全く違うと思う。コミュニティーの中で研究開発され、どの程度外に見えているか分からないが、Solidity が最初に出てから相当時間が経過しているため、Solidity やコンパイラーの在り方などに問題があるかもしれない。
  - 開発者にとって使いにくくないか、single point of failure にならないか、というところも含め、常に発展段階。唯一改善されてきた点は、当初イーサリアム・ファウンデーションの Solidity のチームだったが、イーサリアム・ファウンデーションが抱えるだけでは理念に合わないため、コミュニティーで他にもチームが組成されてきており、ディベロッパーエクスペリエンスなどの改善や、コンパイラーの改善などが行われている。
  - オラクルの問題についても、オラクルは技術としては無ければならないため、我々として議論しているが、イーサリアム・ファウンデーションとしてコントロールしているわけではなく、実際色々なチームが出てきてチャレンジしている状況である。
  - イーサリアム・ファウンデーションとしては可能な限り引き算を周知することしかできない。表に強く出てきているチームなどには特に、引き算が浸透しているかというと、そういう状況ではないのではないか。
  - 技術的な部分の話については、Core Dev などと会話をしていただきたい。様々な問題点の議論はされているが、改善には時間を要する。
  - 研究開発者への規制について、明確にこれと決まっている部分はない。例えば日本に関連するものでは税制問題は言われているが、取引をするためにトークンを持つのではなく、アプリを作るためにもトークンが必要なため、作成担当の人たちに負担がかかるかというレベルの話が 1 点。

    また、分散型アプリケーションに何らかの問題があった場合、そのアプリケーションをコントロールしていない開発者に責任が発生するのかという懸念は世界的に出てきている。今後残っていく人材については、イーサリアムの中でも様々なレイヤーがあるが、例えばプロトコルの部分、パブリックグッズの部分、つまりインフラの部分は、イーサリアム・ファウンデーションだけ が作っているわけではない。そのため、インフラの部分を改善するプレーヤーはコミュニティーの中で活躍している。

    また、アプリケーションの部分、例えば GovTech のソリューションを作っているメ

ンバーも活躍している。政府がコンサルの会社に委託して行うものをスタートアップや違う形で受けて活躍する仕方もある。アプリケーションとしてユーザーが直ぐに使うことができるのが Web3.0 であるが、そのようなものも既に出てきている。

- 今までの形でも活躍することはできるが、そうではない活躍の仕方、例えば大企業に勤めないと仕事ができないということではないため、そこを理解することが大事である。中南米はそのような文化が既にあるため、個人レベルで活躍するところも増えてきている。
- パブリックグッズのレイヤーでは、イーサリアム・ファウンデーションが主導で助成金を出してサポートしているため対象者は明確である。イーサリアムが貧しかった頃は、お金も貰えず地味にやっていたが、今はできるだけ公平になるようにしている。EIP、Ethereum Improvement Proposal という形で改善点を提案されたものをどのチームが実装するかということも、イーサリアム・ファウンデーションがやるのではなく、どのチームができるのかをコミュニティーで話し合い進めている。長いプロセスではあるが、そこに中南米の人も入ってきており、多少だが日本人もいる。

- 言葉の問題について、例えば分散というのは、社会に良い影響があるということがブロックチェーンを話す時にナラティブとして出てくるが、日本語の分散は曖昧であり、様々な人が同じ単語を違う意味で使っている。コンピューターサイエンスの分散型ネットワーク、分散型コンピューティングのディストリビューテッドな分散、非中央集権のようなディセントラライズドの分散、あるいは分散という日本語から、地域創生のような話が出てくるように、分散という言葉は様々な人が違う言葉で捉えている。イーサリアムが目指す、イーサリアムが物事を良くすると言ったときの分散とはどういうことを指しているのかお聞きしたい。
  - 技術として、コンピューターサイエンスが指す「分散型」というところが主導にはなっている。イーサリアムで大事な部分は、例えばビットコインとの大きな違いで、技術だけではない部分を引き算などをもって、なるべく力を分散させ、全員で作っていくところであり、その部分は大事にしている。
  - その例として、ヴィタリックは、現在イーサリアム・ファウンデーションのリサーチャーの一人であり、リサーチチームのリードは別にいる。そのような力の分散を大事にしている。事実、分散が浸透している証拠として、イーサリアム・ファウンデーションが提案をしても、コミュニティーが承諾するとは限らない。
    ただ、エコシステムの中で力が強くなりすぎているところは、我々の出来る範囲で引き算を使いバランスを整えるよう努めている。具体的な例として、もしメタマスクが行き過ぎという判断になれば、他のウォレットが出てきた時によりサポートする方法が考えられる。
  - 分散の定義は英語でも様々なものが使われているし、理解がされていない部分もあ

る。

- 端的に言うと、究極は完全直接民主主義なのかもしれないし、元々インターネットにはキングがいないのと同様、なるべくそのようなガバナンスモデルを持つべきと理解した。

- ここで前半が終了。デロイトトーマツコンサルティングより分散型アイデンティティに関する委託調査中間報告について説明。
- 構成員から質疑応答・意見交換において、主に以下の発言。
- 用語を整理した方がいいと思うのは、元々W3C で標準化する時の DID は Identifier で DID である。「S」をつけなくても、Identifier のことしか言っていなかった。それと識別したアイデンティティは全く違うものだが、ここで言う Identity の DID は、事実上は SSI とやっていることは一緒である。
- 同じ DID という 3 文字を識別子の話とアイデンティティメカニズムの話で混同したものがある。この手の技術や、運用、制度の議論にマーケティングワードを入れるとブロックチェーンがマーケティングワードになってしまったことと同様に破綻する。DID と Identifier の話で、ここでいう分散型アイデンティティは SSI と似たようなことをやるため、その用語の整理をした方が望ましい。
- その上で、分散型アイデンティティに記載のある「データ主権の非中央集権制」とは何か、これは分かるようで分からない言葉である。データ主権とは何かということと、データ主権の非中央主権制とは何かということと、仮にそれが定義されて、データの主権を実現する仕組みを非中央集権的にできるとして、それとアイデンティティメカニズムとどのような関係があるのか。これは正確ではないか、難しいことを言っている感じがするため、どのような意味か教えてほしい点と、もし繋がっていないのだとすると、深掘りする必要があるのではないか。
  - データが従来型の ID の場合、よく言われる GAFA などのアカウント情報で様々なサービスを利用していると、帰属する情報などは、事業者に握られている実情があると思われる。そのような情報を管理できる権限が個人に宿るという意味で、非中央集権的ではないということを申し上げた。
  - もう 1 点は、今後の方向性についてのコメントと受け取ったが、分散型アイデンティティなどの用語の整理とマーケティングワードが公表資料の中でどのように受け取られ得るのかということは重要な観点であるため、事務局と取りまとめの報告書などを編さんしていくに際し配慮したい。
- Federated ID でなぜ SSI が出てきたかというと、グーグルやアップルなどの Federated ID を管理することができるようになり、歴史的に意味がある。オンプレミスで各事業者が ID パスワードを保管している場合漏洩リスクがあるため、よりセキュリティー管理がしっかりしたところで管理して 1 度の認証になったという歴史的必然性がある。
- その場合、単一障害点になるため、改めて単一障害点を減らそうということである。そ

のような思想から、SSI で今の DID で利用されているアーキテクチャーが出てきており、非中央集権というよりは、フォールトトレラントや単一障害点の除去ではないか。

- 非中央集権という言葉も分かるようで分かっていない。誰もが定義できないのではないか。技術や運用ができることとできないことを明らかにすることは重要で、このセンテンスではできないことがぼやけているため、突き詰めていただきたい。
- 私たちが持っているマイナンバーカードは、電子証明書の鍵ペアが含まれている。国民の少なくとも 2～3 割の人が公開鍵のペアを持っている国はほぼない。
- DID に関して、マイナンバーカードの鍵ペアの利用、つまりマイナンバーそのものは使えないが、マイナンバーカードに含まれている電子証明書の部分の鍵に関しては、民間企業が使える領域になっているのではないか。
- 今後は恐らく電子証明書の鍵にアクセスを希望する DID 事業者が出てくると思うが、丁寧に繰り返し電子証明書の仕組みを説明できるような場所になると望ましい。マイナンバーはできないというところで終わってしまうことが多いため、私たちが手にしている電子証明書の可能性や、難しくてできないという話についても指摘をしていただきたい。
  - 基本的にマイナンバーカードの法的個人認証自体は、民間も含め幅広く利用可能である。DID やその他の新しく出てくる仕組みとの連携は進めていくことが望ましいが、注意すべき点が 1 点ある。証明書のシリアル番号は、マイナンバーの裏番号の形で悪用されないように、総務大臣の認定を得られた事業者のみが保管できる。
  - 電子署名を打ったドキュメントを手元に置くなど、幅広く流通できれば望ましいが、署名を打つことにより、証明書のシリアル番号が署名された文書にも入ってきてしまい、取り扱いは法的規制がかかっているため、何かしらの工夫が必要である。あるいはブロックチェーンなどに書き込む場合、証明書シリアル番号がブロックチェーン上に書き込まれない工夫をするなど考えていかなければならないため、どのようなやり方であれば問題なく連携できるのか、今後お示ししていきたい。
- ブロックチェーンか、ブロックチェーンではないかということに係わらず、シリアルナンバーをどう扱うかという問題として認識すればいいか。
  - ご認識通りである。分散台帳であるか否かに係わらず、分散台帳の場合、一般的にパブリックチェーンでは誰もが自由にアクセスできてしまうため、そういった面で慎重な対応が必要となってくる。
- 総務大臣や総務省が認めた認証局でないと取り扱えないという話は、早く変わる気配はないと理解していいか。
  - 根底にあるものは、識別子が持つプライバシーインパクトが大きいという点である。現時点ではその規制の緩和は予定していないが、一方で、署名検証者を増やし、広く民間でマイナンバーカードを使ったサービスが出てくることにより、マイナンバーカードの普及や、保有されている方々の利活用という点でも重要になってくる。そのため署名検証の環境を、どのように低廉なコストで使い勝手よくできるように

していくかは諸々検討が進んでいる。規制を直ちに緩めるという考え方はないが、発生するコストや使い勝手を上げていくことは重要な課題だと認識している。

- そちらのサービスはブロックチェーンの上にも載せられるか。
  - やり方次第ではあるが、署名検証事業者が何かしら分散台帳との関係を持たせること、例えば暗号資産のウォレットの KYC をする際にマイナンバーカードの使用を検討している署名検証事業者があるとのことで、今後様々出てくるのではないか。
- 事業者が出てくるのは喜ばしいことである。高校での情報の授業などで入り込んだ授業を行っており、マイナンバーカードの利活用の増加に伴い、公開鍵認証や暗号であるものの Web3.0 の基盤になっている情報の構成についても、リテラシーを持った国民や市民が増えてくることが期待できる。議論をより活発にし、実装する事業者が現れ、事故などを踏まえながら対話ができるのが望ましい。
- 2 点質問がある。

  1 点目は、そもそも ID というデータ自体、あるいはその ID に紐づいているものを中央集権的に管理することと、分散的に管理することで、ID の本来のオーナーであるべき本人にとって、どのような違いがあるのかということでさる。あるいは分散的に管理をしていくことは、データ主権を持つために望ましいこととした場合、技術的にどこまでどのように可能になっているのか。例えばパブリックブロックチェーンを使うことは、今すぐ取り組もうと思えばできることなのかどうなのかということ自体、国民目線として説明があると望ましい。
- 2 点目は、各国の中でも個別のプロジェクトについて、既に実例が幾つか出てきているが、各国の様々なプロジェクトで Identifier のシステムができていることは Web2.0 的だと思っているが、相互に話をすることができるのか。自分がデータ主権を持ち、できれば国の中でも組織を超えて、国を超えて、どういう人間であるかというアイデンティティを持っていればいいというのが理想であった場合、現在、国で様々なことが起きているものは、相互に話をすることを前提になっているものなのかお聞きしたい。
  - ID の分野にブロックチェーンを使うことの意味合い、例えばパブリックチェーンでできるのかという質問について、中央集権型の組織によって管理されるような ID となると、その事業者が単一障害点になるため、個人で管理するより安全だという経緯で発展してきた。例えばそこが技術的な弱点を突かれての漏洩や、あるいはそこの事業者に所属する方のヒューマンエラーなど何らかの人為的な行動によって情報流出するといった事例も昨今見られるため、そのようなことが無くなっていくことは 1 つのポイントなのではないか。
  - こういった ID をブロックチェーン上で実現していくことには、幾つかのアプローチがある。今回は敢えて分散型識別子を出しているが、DIDs がどのように実装されるかということについては、VC はブロックチェーンが関係ない分野になっている。分散型識別子をブロックチェーンに書き込み、ブロックチェーンに識別子を持ち、

その識別子の公開鍵がセットになった時に、ブロックチェーンに記録されている識別子を持っている個人や企業という証明は取れるようにする。

- その後、VC 自体の証明には識別子や公開鍵が必要なため、そういったものがないと確認が取れないような仕組みにすることで、VC と DIDs の組合せでブロックチェーンを絡めた形で認証ができる仕組みを分散的に作り上げることは、パブリックチェーン上で実現すること自体は既にできている。
- 一方で、すぐに実用化や広く普及していないところについては、識別子自体が重要な情報であり、場合によっては個人情報やプライバシーに関わってくるものだという議論も同時にされているため、パブリックチェーンに識別子を書くような仕組みを前提としていいのかどうか、議論ではまだ決着はついていない。
- Federated ID から分散型の仕組みが良いのではないかということで、ブロックチェーンを使うことを念頭に、こういった分散型アイデンティティの議論も発展してきた。一方で、ブロックチェーンを使うことのメリット、デメリットなど、やりづらいところも見えてきており、その 1 つは、識別子が良くも悪くも見えてしまっているため、個人情報やプライバシーといった現実上の問題との兼ね合いが難しい。このような制約にどのように折り合いをつけるかは、今議論されているポイントの 1 つである。
- 2 点目について、個々の取組みは、民間の事業者の取組みもあり、例えば NHS はイギリス政府関係の機関であるため、官の主体が音頭を取って進めていくこともある。その中で相互運用性やお互いに情報連携がし易いように平仄を合わせていく動きというのは、例えば分散型識別子、Decentralized identifier の定義自体も W3C で定義がされているなど、そういった組織の垣根、国の垣根を跨ぎ協調するための取組みも存在するため、どのような議論がされるのか、そこを合わせたような形が一番普及させやすいものになると考えている。
- 相互運用性を担保するという意味でも、ブロックチェーンの活用が良いのではないかというのが、元々W3C でブロックチェーンを使うことを念頭に DID の定義がなされた背景と認識している。

- 1 点目として、要するに未来系の Web3.0 の方向から現代に引き戻してきた時に期待される DID の話と、マイナンバーカードの上に載せていき、分散型アイデンティティに近づけていく後半の説明にギャップがあるように感じている。そのまま延長しても Web3.0 に行く気がしない。特に日本のマイナンバーというシステムの上にある法制度やプライバシーの話を抱えたままその先に行けるとは思えず、未来から引き戻してきた時と今の延長線上のギャップの部分があるという理解で正しいか。もし正しいのだとすれば、そこの辺りを明らかにした方が、マイナンバーシステムの限界など課題を浮き彫りにしてしまうようなことにもなる恐れはあるが、それは事実として、整理が必要ではないか。
- 2 点目は、各国の事例が紹介されているが、各国それぞれに日本のマイナンバーに相当

するようなものの事情が異なるのではないか。その辺りの事情やプライバシーのルールが異なるがゆえに、出来ているものや出来ないものが整理されていた方がよいのではないか。技術だけで決まる話であれば、技術はどこでも利用することができ、国でやられていることであれば、日本もこういう技術を使ってやればいいではないかという話に発展していくと思うが、各国でそれぞれ作られており、今の法制度やルールの下で囲われている部分が大きいと感じている。その辺りをお聞きすることで、各国の話をどこまで日本に持ってこれるのかということが分かると考えており、今の段階で補足があれば補足いただきたい。

- 識別子に紐づく情報が個人情報に当たるかという論点は、個人情報保護の分野では本研究会以外でも議論されている論点である。話を聞いていて、識別子や公開鍵は個人情報に該当する可能性は大いにありそうだという印象があることと、パブリックチェーンに載せることについては、個人情報保護的に許容しにくい面があるのではないかと思われる。
- 検証事業者や発行事業者、鍵管理事業者の方々が、個人情報取扱事業者に当たるとなると、個人情報保護法の規制が全部かかることとなり、到底パブリックチェーンに載せるという議論に進まないと感じている。
- 個人情報をブロックチェーンに格納せずに個別に通信するなど、鍵をウォレットの中で中央集権的に管理するような記載もあり、パブリックチェーンに載せてやるのがいいのかというのは、慎重に議論していく必要があることと、海外の動きを注視しながら、研究会のアウトプットを出していくことが望ましい。個人情報のところはハードルになりそうだと、議論を伺っていて感じた印象である。
  - ワクチンパスポートの時もブロックチェーンの利用が検討されたが、懸念や課題があるがゆえに各国では利用しなかった。日本も情報収集はしたが、利用しなかった。この辺りは既にあるプロジェクトでも相当ケアしている部分であるため、国際的な動きを見ながら考えていく必要がある。
  - 一方で、チェーンそのものを公開している中で、どのように選択的に自分の開示したい情報だけを開示するのかは、1 つの Identifier に全部を結びつけるのではなく、1 人が様々な Identifier を使い分けるような、その文脈に応じて紐づけを本人の意思で行うなど様々な方法があり、R&D は研究開発が進んでいるため、しっかりと確認していきたい。
  - 関連するところでは、今のマイナンバー制度との接合はどうなのかということである。概ね今の法的個人認証の仕組みは、各国で 1990 年代末から 2000 年代前半に開発された技術がベースとなっており、必要な基盤である。ここ 5 年、10 年で起こった様々なイノベーションをどのように EID やナショナルアイデンティティと接合させていくかというヨーロッパなどの動きを見ても、各国で活発な議論や、国際標準化でも動いており、簡単ではないと諦めてしまうより、各国でも論点を把握して

いきながら、日本としての活用の仕方や高度化させていくための流れを考えていきたい。

- 次回の研究会は、11 月 30 日水曜日開催予定であることを事務局より説明。
- 議事要旨は、構成員の皆様に内容を確認いただいた後に公表させて頂くことを事務局より説明。

以上