2022年2月

日本銀行決済機構局

決済の未来フォーラム　デジタル通貨分科会（1月11日）議事概要

日本銀行決済機構局では、1月11日、「決済の未来フォーラム　デジタル通貨分科会：中央銀行デジタル通貨を支える技術（第3回会合）」をオンライン形式にて開催しました。

分科会では、①デジタル通貨とプログラマブル性、②セキュアな決済を支えるユーザーデバイス、というテーマで二つのセッションを設け、企業で実務に関わる方から、中央銀行デジタル通貨（CBDC）に活用しうる具体的な技術や取り組みをご紹介頂くとともに、その内容に関する意見交換を行いました。

以下では、各セッションの概要を紹介します。

１．デジタル通貨とプログラマブル性

一つ目のセッションでは、「デジタル通貨とプログラマブル性」をテーマにプレゼンテーションとディスカッションが行われました（モデレータ：日本銀行決済機構局　鳩貝）。まず、三菱商事株式会社の金田史歩氏より、スマートコントラクトSaaS開発とデジタル決済の取り組みについて説明がありました。続いて、株式会社LayerXの福島良典氏より、プログラマブルマネーの未来について説明がありました。その後、株式会社LayerXの福島氏、株式会社NTTデータの赤羽喜治氏、日本銀行の北條によるディスカッションが行われました。

（日本銀行決済機構局　鳩貝）現在進められているデジタル通貨のプロジェクトについては、CBDCであれ、民間のデジタルマネーであれ、「マネーにプログラマブル性を付与できること」がメリットとして挙げられることが多い。このプログラマブル性という概念はイノベーティブな響きがある一方でどこか掴みどころがなく、識者の間でも明確に定義されていない部分があると思う。また、プログラマブル性という概念と、スマートコントラクトやブロックチェーン技術との親和性についても様々な議論が見受けられる。こうした点を含め、改めて概念を整理し、プログラマブル性の可能性や実現方法について地に足を付けた議論ができればと考えている。

（三菱商事　金田氏）本日は、現在開発を進めているスマートコントラクトSaaS（Software as a Service）とデジタル決済についてご紹介する。背景にある問題意識は、日本社会の大きな課題である労働生産性の低さである。日本の一人当たり労働生産性（就業者一人当たり付加価値）は、OECD加盟38か国中28位、米国を100とすると55.6と約半分にとどまっており、さらに、年々低下傾向

にある。こうした傾向が続くと、日本は主要先進国という括りから脱落しかねない。また、仕事への熱意も生活満足度も他の先進国に比べて低いとの調査結果もある。日本人は、非効率で付加価値の低い仕事に従事し、熱意も持てず賃金も上がらないので、生活満足度も低いというループに陥っていると解釈できるかもしれない。多くの人が定型作業から解放されよりクリエイティブな仕事に従事できるよう、一企業として事業開発に取り組んでいる。

2021年7月、当社は、DX（デジタル・トランスフォーメーション）サービスを提供する会社を共同で設立し、スマートコントラクトの開発に取り組んでいる。これは決済領域に関する取引コストを削減しつつ、業界全体での最適を目指す試みである。現在、バリューチェーンの最適化のためのスマートコントラクトの導入事例はほとんどなくチャレンジングなテーマであるが、将来的に業界横断的なSaaSとして展開していきたいと考えている。経済社会を俯瞰すると、まず需要者である生活者が存在し、生活者にプロダクトやサービスを提供する産業がある。その産業の裏には様々なアプリケーション（スマートコントラクトやサプライチェーンマネジメント、決済、与信等）があり、これらを実現する手段、すなわちイネーブラー（enabler）としてAIやブロックチェーンがあるという構造が見て取れる。このアプリケーションとイネーブラーの層を「産業DXプラットフォーム」と位置付けて、事業を展開しようと試みている。

2021年には、再生可能エネルギー関連のトレーディング業務に関して、スマートコントラクトの実証実験（PoC）を開始した。この実験では、海外の生産者から商社が品物を仕入れ、商社が船会社と契約して輸送し、需要者である事業者に届けるフローを想定している。各プレイヤーの「ペイン」となるポイントを具体的にみていくと、契約や配船の調整・実行とった「フロント」業務では、配船オペレーションに伴うコミュニケーションコストが高い。取引の過程で発生するコストや関係プレイヤー間の調整を商社が行う必要があり、業務負荷がかかっている。タイムリーな在庫把握と在庫の安定化が難しいとの課題もある。また、支払金額計算、請求、入金確認など決済にかかる「ミドル・バック」の業務では、計算に必要な情報収集コストが高いことや、伝票作成、消し込み作業などが負荷となっている。これに対し、実証実験では、フロント業務とミドル・バック業務に対応する二つのプラットフォームを構築し、連携する形態を構想した。すなわち、商流ごとに個別性の高いフロント業務については商流別にプラットフォームを構築し、情報を一元的に管理する。業界横断的な課題の多いミドル・バックの業務に対しては共通のプラットフォームを構築し、決済関係の情報管理、料金の自動計算、決済の自動化などをブロックチェーン上のスマートコントラクトで行う。これらが、APIで円滑に連携し、全体として業務フローを改善していく姿である。実証実験ではデジタル通貨（企業が銀行口座に保有する預金を担保として価値を安定させたステーブルコイン）の活用も視野に入れているが、まずは銀行API等を用いた決済を実装する予定である。

スマートコントラクトの導入による想定効果は、現在、請求や支払に要している業務量を100とすると、

「請求書廃止」、「自動計算」、「デジタル通貨」のすべてを実現できた場合、商社のバックオフィス担当者の最大8割程度の業務量削減を目指すことが可能と試算している。これを商社だけでなく、生産者、船会社、事業者のバックオフィスでも採用して頂ければ、業界全体で相当のコスト削減につながる。

スマートコントラクトやデジタル通貨の導入効果は、高い信頼性・安全性が求められる商品を扱う業務や、多数の関係者で記録を共有する業務などで期待できる。これは、スマートコントラクトで自動実行した処理は改ざん不可能な形で共有されるためである。また、金額計算、監査対応など信頼性の担保に多くの労力をかけている業務や、取引件数（決済回数）の多い業務にも適していると考えている。

これまでの実験で、スマートコントラクトSaaSの実装に向けて、業務効率化の効果は確認できた。具体的には、情報収集や金額計算、契約の照合明細作成といった業務において、スマートコントラクトの情報可視化、自動決済、支払状況の可視化に対するニーズは強い。一方で課題も存在する。自動決済のキーポイントの一つは請求書を廃止できるかであるが、法的要件をクリアしたうえで社内ガバナンス的に許容できるかという整理が必要である。また、デジタル通貨については既存の会計処理と大きく異なるため、メリットを考慮しても導入効果が出るまでには時間がかかると考えている。短期的にはデジタル通貨以外の決済手段も検討する方針である。

続いて、株式会社LayerXの福島氏によるプレゼンテーションが行われました。

（LayerX　福島氏）テーマを「プログラマブルマネーの未来」としているが、具体的なイメージを持って頂くと理解が容易となるため、まずは、プログラマブルマネーと関連性が深い当社の請求書デジタル化サービスについて紹介したい。

請求書は日本のBtoB取引の99%で使われており、金田氏のプレゼンテーションでも説明があった通り、定型・標準化しやすい業務の割には、アナログな紙ベースであることから非効率な作業が多く残っている。支払い側としては、請求書受取→データ入力→承認→仕訳→支払いデータ作成→支払い→消し込み→会計ソフトへの反映→請求書の保管、といった一連の作業が存在する。デジタル通貨はこのうち支払いに近いプロセスに直接的に関係するが、支払い以前のプロセスもあわせてデジタル化することが全体の効率化のために重要であり、ここが遅れているのが日本の課題である。当社のサービスは、これら全体の効率化を目指したもので、たとえば、請求書のデータ入力については、請求書の記載内容をAIが判読して定型化された項目に自動で記入していき、仕訳も自動でサジェストされ、さらに金融機関に向けて送る支払いデータも自動で作成される。これらのプロセスには、日本全体でみれば相当な人件費がかかっている。それだけに効率化の余地があり、可能性を感じている。そして、請求書を起点に支払いの自動化が進むことで、今後さらに、銀行APIの活用や企業間の決済ネットワークへのサービス提供など、デジタル通

貨のプログラマブル性が発揮されうる領域がより明確に見えてくると認識している。今後は、民間マネーであれCBDCであれ、デジタル通貨との連携がポイントになってくる可能性が高いと考えており、当社としても大いに関心を持っている。

こうした事例も踏まえて、プログラマブルマネーについて考えを述べたい。一般的には「お金をプログラムで動かせること」と表現されがちだが、お金をプログラムで動かすこと自体は、全銀システム・日銀ネットなどを通じて既に実現できているように感じるため、それだけだとあまりインパクトはない。日本のように決済システムがしっかりしている国では、とりたてて議論をする必要はないように思う。むしろ、プログラマブルマネーは「デジタルサービスに簡単に組み込め、動かすための手続きを必要としない」ものであり、その点に新規性があると捉えることが重要ではないか。先ほど請求書SaaSを例として挙げたが、サービス開発者としては、簡単に支払いを他のサービスに組み込めるか、お金を動かす手続きを減らせるかという点で、なお課題が多いと感じる。ここを解決することが、金田氏のプレゼンテーションでもあった日本の労働生産性の低さを解決するひとつの方法となると思っている。

「お金の体験がサービスに溶けること」は、さきほどの請求書SaaSの例でいえば、ソフトのインターフェースにある「支払いデータ作成」のボタンを押してデータを作成し、それを金融機関のインターネットバンキングのサイトにファイル送信するのではなく、「支払い」というボタンがあってそれを押せば一気に支払いまで行ってくれる、というイメージである。それだけ？と思われるかもしれないが、これこそが重要なのである。メルカリのようなマーケットプレイスやライドシェアといった、一個人で完結するBtoCサービスでは「お金の体験のサービスへの溶け込み」は急速に実現されつつある。難しいのは、多くの業務プロセスが関係するBtoBの領域であり、支払いに関連して、複数人や複数企業の承認や事後的な確認が必要となる。そこにお金の体験を溶け込ませることは難易度が高い。私見だが、プログラマブルマネーの考え方は、今後、このようなBtoB領域でこそ活きてくるのではないだろうか。

プログラマブルマネーが満たすべき重要な点をいくつか挙げたい。一つは、あまり議論されていないが、開発者の体験という点である。つまり、「スクリプト一つで、お金をソフトウェアにのせられるか」ということ。サービスにお金の体験を溶け込ませるには、サービス提供者が低コストで決済まわりの機能をサービスに組み込めることが決定的に重要である。二つ目が「データの連携性」で、請求書の例であれば、社内稟議が完了すればそれをトリガーに支払われるといった業務フローにおいて、データの連携が良好でないと全体の効率化は実現できない。三つ目が、「システムとしての安定性やコンプライアンスの技術的な担保」である。既存の決済システムには、決済の完全性や、システムの安定性・安全性を確保するために莫大な投資がなされている。この点は、新興の民間企業がいわば「ノリ」で作って満たされるものではなく、CBDCのような安全な決済手段の重要性が意識される所以かと思っている。

プログラマブルマネーのあり方として、以前は、お金が流通しているプラットフォームの上に、アプリケーションを構築してサービスを提供するというイメージがあった（イーサリアムが代表例）。今は、デジタルで提供されているサービスに対し、お金を組み込んでいくイメージを持っており（Stripeが代表例）、プログラマブルマネーのあるべき姿ではないかと思っている。

最後に、デジタル通貨とプログラマブル性に関わる「素朴な問い・論点」をいくつか挙げたい。私自身、確定的な答えを持ち合わせているわけではないが、どれも重要であり、今後、議論が深まれば良いと思っているポイントである。一つ目が「銀行APIでいいのでは？」という問いで、そのとおりだと思う。もっとも銀行APIは、現時点ではスクリプト一つでお金をサービスにのせられる状況とはなっておらず、プログラマブル性という観点で改善が必要と考える。二つ目が、「プログラマブル性とブロックチェーンは関係あるのか？」という問いで、これは基本的に関係がないと思う。たとえば、先ほど挙げたイーサリアムはパブリックブロックチェーン上にお金が存在し、様々な決済サービスを提供し得るプラットフォームだが、「お金をサービスに溶け込ませる」という点や、「データの連携性」については満たしているものの、「システムとしての安定性などを技術的に担保する」といった点については十分に満たしていないと感じている。三つ目が、「民間が提供すればよくないか？」という問いで、これも民間でよいと思うのだが、やはり「システムとしての安定性などを技術的に担保する」という点をどう満たしていくかがポイントになってくる。

上記のプレゼンテーション終了後、株式会社LayerXの福島氏、株式会社NTTデータの赤羽氏、日本銀行の北條をディスカッサントとして、日本銀行の鳩貝がモデレータを務める形で、以下のディスカッションが行われました。

（日本銀行決済機構局　鳩貝）金田氏からのプレゼンテーションでは、DXを単なる事務改善を超えたビジネスモデルの変革として、さらには産業構造の変革と位置付け、そのツールのひとつとしてスマートコントラクトを位置付けていると理解した。変革に向けた現場からの切実な思いと経営層の正しい理解が重なった上で、実現可能性の高いソリューションや技術に出会うことが、変革のために重要と思っている。

また、福島氏のプレゼンテーションでは、「お金の体験がサービスに溶ける」という表現で、テクノロジーによって決済がユーザーにとって意識されなくなるという未来像を示して頂いた。また、プログラマブルマネーの実現方法のイメージが、「お金がもともと存在しているネットワークの上にアプリケーションを作る」といったものからから、「サービスに決済を埋め込む」といったものに変化してきていることもご紹介頂いた。最後にご提示頂いた「素朴な問い・論点」も、大変本質を突いたポイントであった。

お二方からはこれら以外にも多くの論点をご提示して頂いており、これからのディスカッションで取り上げられればと思う。

（日本銀行決済機構局　北條）ディスカッションの前提として論点を整理させて頂く。CBDCの導入を検討する際は、現金や預金など様々な決済手段とともにCBDCが共存するという意味での「水平的共存」とともに、CBDCの領域の中では、中央銀行・民間事業者・仲介機関といった様々な主体が役割を分担する「垂直的共存」が、重要なコンセプトと考えている。後者の垂直的共存では、基礎的な決済手段としてのCBDCを中央銀行が発行し、仲介機関が仲介業務を担ってCBDCが流通する。そのCBDCを土台にして、民間事業者・仲介機関が、ユーザーのニーズに応じCBDCの利便性を向上させる「追加サービス」を提供する、といった役割分担が期待される。追加サービスとしては、家計簿サービスや、プログラマブルな決済サービス、ユーザー間の情報連携、取引情報の利活用などが例として挙げられる。こうした追加サービスの提供により、CBDCの機能が拡張されユーザーの利便性が向上する。また、他の情報システムとの連携が円滑化し、様々なサービスとの組み合わせによる新たなサービス提供が可能となる。他の情報システムとの連携や他のサービスとの融合が重要という点は、金田氏、福島氏のプレゼンテーションでも指摘して頂いた。まずCBDCを取り上げて話を進めてきたが、こうしたレイヤー構造や、基本機能と追加サービスを分けて考えることは、CBDCのみならず民間を含めたデジタル通貨全般でも共通しているように見受けられる。以下では、デジタル通貨一般について、論を進める。

デジタル通貨の追加サービスを実現するためのポイントをいくつか挙げたい。まず、デジタル通貨の送金などの基本機能を、追加サービスの側からスムーズに呼び出すことができるように設計することが重要であるという点である。これにより金融/非金融、toB/toCなど様々な領域で様々な追加サービスを実現できる。一方で、デジタル通貨の基本機能の仕様が追加サービス提供の制約とならず、追加サービスが基本機能に影響を及ぼすことがないようにすること、すなわち基本機能と追加サービスの緩い連携が実現できることも重要である。加えて、現時点では想定されない将来的な追加サービスの提供ニーズにも対応できる、高い自由度・拡張性を備えることも重要。デジタル通貨の「プログラマブル性」というコンセプトに寄せられる期待は、以上挙げたようなポイントとも大いに関係しているのではないかと考えている。

デジタル通貨のプログラマブル性を実現する形態として、具体的なイメージを2つ紹介する。まず「プログラム実装可能領域の提供」が考えられ、これは、デジタル通貨のシステム上に追加機能をプログラムできる領域を設け、追加サービス事業者に提供する形態である。決済インフラ自体にプログラムを埋め込む方式であり、分散型台帳においてスマートコントラクトやプログラマブルマネーとも呼ばれる手法である。ただし、この形態では、デジタル通貨の基本機能と追加サービスが垂直統合的となり、デジタル通貨の運営主体と追加サービス事業者の役割分担が不明確になる可能性があるため、この点はデメリットともなりうる。もう一つが「APIの公開」で、デジタル通貨のシステムでも、追加サービスに必要なAPIを公開することで、追加サービスの実現を支える形態である。この方式の場合は、デジタル通貨のシステムと追加サービスの境

界が整理され、運営主体と追加サービス事業者の役割分担が明確化されるメリットがある。ただし、多様な追加サービスの要請に応えるためには柔軟性のあるAPI公開が検討される必要があるが、これはなかなか難易度の高いものである。

（日本銀行決済機構局　鳩貝）それでは、ディスカッションに入りたいと思う。頂いたプレゼンテーションも踏まえて、「DXとスマートコントラクト」、「プログラマブル性とその実現方法」など、いくつかのテーマを用意した。

まず、「DXとスマートコントラクト」のテーマでご議論頂きたい。金田氏からは、労働生産性の話からビジネスモデルや産業構造全体の変革をスコープに入れてお話し頂いた。一般に、ブロックチェーン上のスマートコントラクトを用いた仕組みは、関係する主体が多い中で、情報をリアルタイムで共有し、事前に取り決めたプロセスに則って処理を行うことに大きな力を発揮するように思われる。DXの文脈でスマートコントラクトを活用することのメリットや課題についてご意見を伺いたい。

（NTTデータ　赤羽氏）自身がブロックチェーン技術を用いた貿易分野の情報連携プラットフォームを構築した際に意識していたのは、必ずしも「スマートコントラクト＝DX」という訳ではないという点である。プログラマブル性も、ブロックチェーンでなければできないとか、スマートコントラクトでなければできない、といったことではなく、従来型の中央集権型システムでも実現できる。DXに分散型台帳技術を使用するメリットの一つは特定の人に依存しなくなる点であるが、昨今の分散型金融（DeFi）と呼ばれるような分野については、高いプログラマブル性を備えてはいるものの、ガバナンスの観点で様々な課題があると思っている。こうした課題を解決してなおメリットが残るようにしないと、DXに分散型台帳技術に基づくスマートコントラクトを用いるという話にはなりにくいと感じている。

（LayerX　福島氏）DXとスマートコントラクトの関係を考える上で注意すべき点が２つある。一つが、１社のみで閉じるか複数社に跨って関係するかという点、もう一つが価値の移転を伴うか否かという点である。複数社が関係し価値の移転が伴う業務を扱う場合は、スマートコントラクトと相性が良いと感じる。一方で、請求書関連の業務のうち、請求書のデータを取り込んだり、仕訳を行ったり、支払いデータを作成するようなプロセスは、１社で完結して価値の移転を伴わないため、シンプルにデジタル化を進めればよく、スマートコントラクトとの関連性は比較的低いと思う。このような、主体の単数・複数と価値移転の有無の２軸で見てみると、整理がしやすい。

（日本銀行決済機構局　北條）複数の人達が関わって一つのものを完成させていく性質のものにはスマートコントラクトは役に立つと考える。1対1での作業が繰り返される性質のものとは対照的に、一つの取引において複数のプレイヤーが関わり、かつそのプレイヤーが毎回異なってくるような取引の場合、スマー

トコントラクトのように、業務フローを標準化して同じルールとした方が効率が良くなる。このような標準化は、誰かが全体像を描いてそれに皆が乗るケースもあれば、多くのステークホルダーが擦り合わせていくケースもあると思われ、それらの議論の出発点としてもスマートコントラクトの活用は有益となろう。

（日本銀行決済機構局　鳩貝）福島氏や北條から指摘があった通り、適用する領域やサービスの特性、すなわち主体の複数性や価値移転の有無、業務の複雑性・反復性といった点を考慮しながらスマートコントラクトの有用性を考えるべきと理解した。一方、スマートコントラクトの課題として、赤羽氏からガバナンスの問題が指摘された。透明性の確保を含め、プラットフォームの運営に関する論点が数多く存在すると思うが、この点についてご意見をお聞かせ頂けないか。

（NTTデータ　赤羽氏）貿易関係のプラットフォームを構築した際に意識したことは、それが重要な社会インフラの一つであるという点。社会インフラであるがゆえに、通常のアプリケーションと異なる「長寿命性」、すなわち20年、30年といった長い目線で起こり得るイベントを、サービスに影響を及ぼさないようにマネージしつつ、プラットフォームとしての役割を果たすことが期待される。スマートコントラクトでプログラムを書きつつも、それをどう維持していくのか、誰が責任を持つのかといった点が、スマートコントラクトを社会インフラに適用する際に重要と感じた。「DXとスマートコントラクト」というテーマを扱っているわけだが、ここでいうDXのレベルが、ひとつのビジネスにとどまるのか、産業全体なのか、さらには社会全体なのかによって、プラットフォームのガバナンスに対する要求も変わってくるのだろうと思っており、これを意識することが極めて重要と感じている。
（LayerX　福島氏）レギュレーションを考える際に重要になってくるのは、価値の移転が伴う中で AML を誰が担保するのか、という点。現在の決済システムでは、送金などの機能だけが備わっていればよいというわけではなく、その前段階において、AML を含む様々なチェックを行うゲートウェイを設け、その責務を担うことができる主体にのみ決済システム参加のライセンスを付与している。 このレギュレーションのレイヤーで実施されていることを一つ一つ紐解いてプログラムとして実装することが、プログラマブルマネーが社会のルールとコンプライアントな形で機能するために必須と考えている。また、ルールに対しコンプライアントなマネーを作る方法としては、目的や流通領域を限定したお金、例えば貿易決済に限定したお金を発行し、従来の決済システムと連動させることも考えられる。いずれにせよ、レギュレーションのレイヤーについて、現状は金融機関などへのライセンス付与によって取引ルールの遵守が担保されているところ、プログラマブルマネーにおいて誰がレギュレーションをプログラムとして実装するのか、どこまで実装できるのか、といった点に関心がある。

（日本銀行決済機構局　鳩貝）ご指摘のポイントは大事な論点と思っている。新しいプラットフォームを作ることは、決済に伴うフリクションが低減されるという意味で魅力的である一方、そのプラットフォームの運営のガバナンスが重要になってくるという点をAMLの例を用いてご説明頂いた。価値移転を伴う取引を

扱う場合、その価値移転の正当性を誰が担保するのか、プラットフォームの運営者がどこまで背負っていくのかを含め重要な論点となってくる。デジタル通貨をどのような目的にも使える万能なものにした場合は、取引の正しさの確認コストが大きくなり、プラットフォームの構築コストも大きくなる。福島氏のご指摘にもあった「目的や取引参加者を限定した」デジタル通貨の場合は、たとえばガバナンスやレギュレーションが幾分軽めのアーキテクチャがありうるかもしれない。デジタル通貨の性質によって、デジタル通貨が流通するプラットフォームがカバーする領域が、伸び縮みし得るのではと思った。

（LayerX　福島氏）お金に意味を持たせられるということは、非常に意味がある。たとえば、株式の配当にしか使えないお金や、特定の企業からの請求にしか使えないお金というようなものは、今は実装できておらず、すべて銀行口座の数字の増減として表現される。こうした「意味を持った」お金がスクリプト１行で実装できるようになることが、とても重要なのではないかと思う。容易に実装できる一方で、AML含め様々なルールの遵守はプラットフォームが担保してくれているイメージである。それにより、レギュレーションがより守られやすくなるということもあると思う。

（NTTデータ　赤羽氏）今後、分散型台帳技術の応用が進んでいき、また新たなパラダイムシフトが起こっていくこともあるかと思う。信頼の拠り所となるいわゆる「トラストアンカー」を組み合わせて、そこからの信頼の連鎖により全体のガバナンスを達成することが、中央集権でないとできなかったことを分散型のアーキテクチャで実現することにつながるのではないか。

（日本銀行決済機構局　北條）トラストアンカーの重要性はその通りだと思う。トラストアンカーが存在するデジタル通貨のプラットフォームが構築できれば、福島氏が指摘された目的を限定したマネーや、プログラムによって金融サービスが自動的に行われる仕組みなど、利便性を向上させる新しい技術を組み込める。もっとも、トラストアンカーをどう組み込んでいくかは非常に難しい課題だと思う。

（LayerX　福島氏）CBDCに求められているのは、高度な機能性というよりも、まずはトラストアンカーとしての役割だと思う。民間だけで独自に決済インフラを構築した際に課題となるのは、そのインフラだけでは決済完了性が得られないこと。CBDCがいわばパブリックブロックチェーンにおけるメインチェーンとなって決済の完了性を担保し、第２レイヤーにおいてマネーが高頻度で流通する、といった形態を作れると良いのではないか。

（日本銀行決済機構局　鳩貝）徐々に「CBDCとプログラマブル性」の議論に入ってきているが、「民間マネーかCBDCか」という点よりは、民間マネーとCBDCを組み合わせた決済システム全体として新しい利便性を実現することが重要であり、プログラマブル性を付与することが、そのための一つの方法となりうると理解している。

（日本銀行決済機構局　北條）CBDCの文脈では、発行・流通のような基本機能を担う中央銀行や仲介機関がトラストアンカーとしての役割を果たすことで、民間企業が追加サービスを実現しやすくなるのではないか、と感じた。

（NTTデータ　赤羽氏）CBDCの実装が、日銀の連絡協議会資料の垂直的共存のイメージ図通り行われる場合には、仕組み自体がトラストな環境となり、トラストアンカーの機能を誰が担うかという議論の必要性は下がるかもしれない。また、福島氏が指摘されたお金に色をつける機能をどう実装するか、北條氏が述べられた将来にわたって柔軟性を担保するAPIや環境をどう準備するか、という点は重要である。運営サイドからするとなかなか負荷のかかることであるが。

（LayerX　福島氏）銀行APIでよいのではないかという議論はあるが、現在の銀行APIには柔軟性が十分に備わっていないと思っている。銀行APIは、接続するためのライセンスや契約などのコストが高く、およそ一般の開発者がそのハードルを突破することは難しい。それによってトラストな環境が守られている。レギュレーションがライセンスでなくプログラムで守られる仕組みを整えることが、柔軟性とレギュレーションの両立にとって大変重要であり、プログラマブルマネーでそれが実現できれば素晴らしいと考えている。

（日本銀行決済機構局　鳩貝）従来は組織として人力で行われていたコンプライアンスの作業が、プログラムに置き換わっていき、そのプログラムの挙動の正しさはきちんと外部から監査されるといったイメージであろう。RegTechやSupTechといったコンセプトにもつながる大事なポイントである。

続いて、「プログラマブル性とその実現方法」についてディスカッションしたい。北條が説明したプログラマブル性の２つの具体例（資料６ページ）、すなわち①「プログラム実装可能領域の提供」と②「APIの公開」について、そもそもこういうイメージでよいかどうかを含め、ご意見伺いたい。

（LayerX　福島氏）①の「プログラム実装可能領域」はAWSのようなものを考えるとわかりやすい。ヴァーチャルマシンがあって自由にプログラミングできる世界であって、柔軟性が高く、開発者の発想によって予期しないイノベーションが生まれやすい。AWSが、ヴァーチャルマシンの層を開放せず、予めAWSが用意した機能をAPIでコールして使うようなインフラであれば、今日のような幅広いウェブアプリケーションはでてこなかっただろう。一方で、このようなプラットフォームを運営することは相当にコストがかかり、維持していくことが難しい。無料で構築できるのであれば迷うことなく①「プログラム実装可能領域」を選ぶのだが、現時点での制約条件を踏まえて考えたとき、①「プログラム実装可能領域」と②「APIの公開」のどちらがよいかは難しい論点である。

（NTTデータ　赤羽氏）資料にも記載があるように、①「プログラム実装可能領域」だと、運営主体と

追加サービス事業者の役割分担が不明確となり得ることが課題となる。たとえば、自動車を例に考えた場合、安全性が担保されたエンジンとフレームが提供され、その他のパーツは自由に組み合わせることができるという仕組みの方が、自分たちのニーズにぴたりとあったプロダクトが作れる。一つの巨大なインフラを作るよりも、この自動車の例のように、安全性を担保する部分を備え、そこは勝手に開けられない（改変できない）ようにしつつ、それ以外のパーツの選択は開放し事業者に委ねる、という設計が考えらえるのではないか。こうした発想は、福島氏が提示した、カジュアルにサービスに組み込めるパーツとしてのお金という話に繋がると思う。

（LayerX　福島氏）完全に同意する。決済システムとしての整合性は保ちつつも、簡単にサービスが組み込めることができると最高だと思っている。

（日本銀行決済機構局　鳩貝）①「プログラム実装可能領域」、②「APIの公開」の組み合わせもあり得る。たとえば、柔軟性を持たせたい部分はプログラム実装可能領域を作って「皆さんどうぞ」としつつ、そこでの価値交換の情報を中央台帳にAPIで連携するイメージが考えられる。
（LayerX　福島氏）システム設計の大原則として、「柔軟性は高くつく」というのがある。どのレイヤーまで柔軟性を持たせるかを考えたとき、アプリケーションのレイヤーまで柔軟性を持たせようとするとかなり高コストになる。お金に関するレイヤーだけ柔軟性を高くして、その先は目的に応じて狭めるというのが理想ではないか。もっとも、イーサリアムのように、「プログラム実装可能領域」を低コストで提供する方向性でイノベーションが進んでいることも事実で、この分野には多額の資金と多くの知能が集結している。ここ数年の進捗は芳しくないが、関心を持って見ている。

（日本銀行決済機構局　北條）①のように「プログラム実装可能領域」を想定した際、そこに載せようとしているプログラムや機能が適切かどうかを誰がチェックするのかは重要なポイントである。プログラムのロジックまで把握したり、新機能が実装された場合に既存の機能に与える影響まで判断したりすることは、誰でも簡単にできるものではない。パブリックブロックチェーンであるイーサリアムなら、プログラムを載せるのもそれを利用するのも自己責任ということになるが、デジタル通貨の場合、安全性が担保されたものを提供する必要がある。

（LayerX　福島氏）そういう専門職が生まれるのだろう。プラットフォーム運営者に必要な官僚的センスと、サービス提供者に必要なプログラマー的センスを合わせ持ち、両者をつなぐ役割を果たすことが期待される。

（NTTデータ　赤羽氏）法学者や法律の作り手に技術を理解してもらう必要も感じる。法学者コミュニティに正しく技術を伝える取組みを行っているが、法律はITや分散型台帳技術が存在しない時代に作られたものが多く、難しさも感じる。我々プログラマーからだけではなく法律のほうからも歩みよりがあると良

いと感じる。

（日本銀行決済機構局　鳩貝）デジタル通貨とプログラマブル性に関する論点を一つの軸としながらも、DX、スマートコントラクト、API、ブロックチェーン、分散型金融、RegTechと多岐にわたる話題についてご議論頂いた。大変感謝する。今後もこうした領域について、皆さまとともに知見を深めて参りたい。

２．セキュアな決済を支えるユーザーデバイス

二つ目のセッションでは、「セキュアな決済を支えるユーザーデバイス」をテーマに、プレゼンテーションとディスカッションが行われました（モデレータ：日本銀行決済機構局　山田）。まず、ソニー株式会社の栗田太郎氏より、主に現行のリテール決済で用いられている決済手段やその背後にあるシステムの特長や課題に関する説明がありました。続いて、大日本印刷株式会社の土屋輝直氏と佐藤精基氏より、リテール決済における各種デバイスを用いた決済ソリューションの動向や同社の取組みについて説明がありました。最後に株式会社 TRUSTDOCK の千葉孝浩氏より、eKYC やデジタルアイデンティティの活用に関する現状や事例について説明がありました。

（日本銀行決済機構局　山田）仮に CBDC が発行された場合、どのようなデバイスを用いるかは固まっていないが、すでにリテールのデジタル決済で広く用いられているような、スマートフォン上で動くアプリやカードが候補になると考えている。したがって、こうした決済ツールのバリエーションやバックエンドにおけるシステムの現状、課題を理解することは CBDC の検討を進める上で重要である。また、これらのデバイスを起点とした決済サービスの変遷や潮流を理解することが、将来のリテール分野における決済像を考える際に有益となる。決済の周辺で必要となる様々な手続きがオンラインで行われるようになっている中、これらの技術が決済に限らない分野でも活用され始めている。このため、決済に必要な技術とその応用について理解を深めることも、将来を考える上で有益と考えている。以上が本セッションの問題意識である。

（ソニー　栗田氏）本日は現行システムの特長、課題についてお話ししたい。まず、システム/ソフトウェアの製品品質と利用時の品質は、それぞれが ISO で個別に規格化されている。様々な観点があり、システム/ソフトウェアの品質は、機能適合性や性能効率性、信頼性、セキュリティ、移植性などで議論される一方、利用時の品質は、リスク回避性や網羅性などをもって語られる。立場によって求めるものが違い、全ての特性を満たす必要はないが、システムを開発、運用する時に関連する項目を検討する必要がある。

続いて、具体的なユーザーデバイスについて述べる。まず、IC チップが搭載されていないものとして、ユニークなコード、例えばバーコードが印刷されたカードのようなものがある。これを持って店舗で店員に提示す

るとスキャンされてポイントが付くほか、ポイントを代金の支払いに充てられるという点でお金のような役割を果たす。バーコードは簡単に複製できてしまうため、利用者が店員も含めたシステムを信頼するモデルといえる。

セキュアな IC チップが搭載されたものとしては、クレジットカードや電子マネーといったものがある。バーコードと同様に所有認証であるが、大きな違いは複製が難しいことにある。セキュアな IC チップの中で安全に情報の記録、認証、決済処理を行うことが可能であり、情報ののぞき見や不正利用、コピーが難しくなっている。また、所有認証だけでなく、カードに PIN コード認証や指紋認証を組み込むことも可能であり、様々な企業が実際に製品やサービスを展開している。もっとも、複数の認証を行うことは、単体の認証を行うことと比べ、認証に時間がかかるなど利便性が低下するほか、一番大きな問題としてコスト高となってしまうため、なかなか普及していないのが現状である。

さらに、セキュアな IC チップが搭載されたスマートフォンを使ってサービスを提供するものがある。この場合、所有認証に加えて、ログイン時に入力する PIN コードによる知識認証やスマートフォンの生体認証を組み合わせることで、よりセキュアな運用が可能となる。一方、知識認証や生体認証のセキュリティはスマートフォンのメーカーによって異なることが課題として挙げられる。認証レベルとのトレードオフとなるが、アプリケーションを起動する必要がなく、簡便に高速で動作するとか、オフラインの決済でも使えるため、ネットワークのトラブルや災害が起きても動作するといった特徴もある。オフライン決済で使えるものは「落としてしまった時に心配」との声が多く寄せられるが、実際には様々なサポートサービスがあり、例えば記名式のものであれば落としても何らかの救済措置があることが多い。

オンライン決済の場合、一時的な QR コードの表示や、スマートフォンアプリで QR コードを読み込むものがあり、スマートフォンに備わっている知識認証や生体認証の機能によってセキュリティが守られる。決済に限らずもう少し広く、ネットサービス利用時に、またはネットにある情報にアクセスするために、ID・PW を入力するものもある。複数の端末からログインできるのは便利であるが、PW がネット上にあるため情報が流出する可能性、あるいは PW 変更手続き時にメールが送付されるが、同メールの送付先アカウントが乗っ取られていると PW が再発行されてしまう可能性といったセキュリティ上の課題がある。こうした課題への対策として、2 要素認証やワンタイムパスワードといったものとの組み合わせも行われている。

また、仮想通貨のウォレットのように、利用者のみが手元で知っている秘密鍵を用いるものもある。アカウントがネット上にあり、そこに ID・PW を入れてログインする形ではなく、所有認証＋知識認証＋生体認証を端末側で行い、その中に入っている何らかの秘密鍵によりアクセスする形になる。いわゆるハードウェアウォレットと呼ばれるものであり、パスフレーズを失くしてしまうとアクセスできなくなってしまう。

アプリの設計次第でサービスの使い勝手は様々であるが、開発者の視点からは、セキュリティとのトレードオフになる。また、セキュアに行う必要がある処理はクラウド上で行われるものが多く、スマートフォン側は認証とユーザーインターフェースの提供が中心である。可用性（いつでも使えるか）の確保という観点もある。

次に、セキュアな IC チップが搭載されたユーザーデバイスに絞って、システムの構成パターンなどについて紹介する。こうしたデバイスの場合、物理的なカードの中に複数枚の論理カードがあり、決済処理や認証、情報の記録が行われる。また、例えば店舗や駅に端末があり、カードをかざすと論理カードと端末が相互認証し、その後に決済処理が行われ、端末とカードにそれぞれ新しい決済ログが記録される。一般的には、ネットワーク上に情報が送られなくても、端末側の処理により利用者の代金債務は消滅する扱いとされている。そのうえで、タイミングは不特定であるが、端末上の記録が上位システムに伝わり、その記録が最終的に正となる。情報は最終的に上位システムに伝わればよいため、利用者としては、いつでもリアルタイムなど短い時間で決済でき、また、サービスの提供者としては、有事対応ができることになる。また、カード概念をもう少し広げると、スマートフォンの中にカードを入れて、カードのようにスマートフォンをかざすことができる。また、決済端末と組み合わせることによりタブレットのようなものでレジ機能を担うことができる。この時に端末側では電源が必要となるが、カード側、スマートフォン側には必ずしも電源は必要なく、バッテリがなくとも作動する。このように、アプリを起動せずともいつでも使える可用性を実現している。

各カード・端末から上位システムに決済関連情報が上がっていく中、A 社、B 社、C 社のそれぞれがシステムを保有している場合、システム間の取決めが必要となる。例えばA 社のシステムを使うとB 社のポイントが付くケースであれば、A 社とB 社のシステムが事前の約束に従い連携してデータを処理する形となる。あるいは、端末にある物理カード内に約束があり、例えば電車、バス、それぞれにおける利用データが取決めに従って後々に上位システムに送られる形をとることもある。このように、システム間の連携に関しては上位システム内で事後的にゆっくり行うパターン、端末内でリアルタイムに行うパターンの 2 つがある。

セキュアな IC チップが搭載されたユーザーデバイスを ISO25010 の品質モデルに基づいて整理すると、その機能の「正確性」は、IC チップの中に入っている演算機の正確性や、2 つのもの（IC チップと端末）が同一の結果となることをもって担保される。「性能効率性」の面では、バッテリを使わないほか、ローカルで即座に処理するために計算コストが低くなっており、全体としてはエコなシステムになっている。また、「信頼性」の観点からは、アトミック性があるため処理が確実に行われたことが保証される。誰に対しても分かりやすいユーザーインターフェースを提供できることも特徴の一つである。カードによる簡単な使い方もできるし、スマートフォンを利用した複雑な使い方もできる。このほか、セキュリティ、機密性、インテグリティ、責任追跡性、否認防止性、正真性なども、ISO25010 の品質モデル上、考慮される要素である。ほかにも、

デバイスのセキュリティを担保する国際的な規格として、ISO15408 がある。これにより、システムが運用も含めて安全であることを開発者以外の第 3 者である専門家に客観的に評価、承認してもらうことができる。そこでは、セキュリティを機能要件、保証要件の 2 つに分けて評価、認証することが行われている。なお、セキュリティに対する攻撃の進化は日進月歩のため、暗号アルゴリズムが進化する攻撃に対して十分にセキュアであることを保証し続けることは難しい。また、昨今は、プライバシーの観点からどのような形で安全に利用できるのかという課題もある。

上記のプレゼンテーション終了後、以下の質疑応答が行われました。

（日本銀行決済機構局　山田）栗田氏からは、決済の方法にはオンラインとオフラインそれぞれで利用することができる様々なデバイスや仕様があるとの説明があった。日本銀行は、様々な観点から CBDC の機能や特性を検討しているが、オフライン決済についてはセキュリティレベルの低さを懸念する声もある。オフライン決済とオンライン決済を比較したとき、どのような留意点があるか。

（ソニー　栗田氏）オフライン決済には障害時や災害時でも使えるという点で可用性が確保しやすいメリットがある反面、各 IC チップに処理を委ねてしまうので、この IC チップに重大な欠陥が見つかった場合、そこから攻撃される可能性がある。それを防ごうとしても、各 IC チップを更新することは非常に難しい。一方、オンライン決済の場合、ID・PW が盗まれてしまうとなりすましで使われてしまうおそれがあることなどが、課題である。

（日本銀行決済機構局　山田）システム構成に関するお話や資料の中で、IC チップが搭載されたカードや端末以外に様々な上位システムがあり、それぞれが責任をもって構築・運用され、重層的に system of systems を構成しているとの指摘があった。CBDC の文脈では、よく CBDC エコシステム内の競争領域と非競争領域の切り分けの議論が聞かれている。公的部門を含む複数の企業がエコシステムを構成する場合、どのようなシステムが競争領域、どのようなシステムが非競争領域と考えられるか。どのようにシステムを分けていくべきか。また、この点について、現行のリテール決済システムの特長はどうなっているのか。

（ソニー　栗田氏）現行のリテール決済システムは、上位システムＡ、Ｂ、Ｃがそれぞれ決済システムとして稼動するとともに、Ａ社、Ｂ社、Ｃ社それぞれのサービスと分かちがたい少し広い意味での決済サービスを提供している。決済システムのみが単独で存在しているわけではないという話がセッション 1 であったが、実際に決済システムとサービスが一体化したものが上位システムとして存在していると認識している。こうした仕組みを前提に、競争領域と非競争領域をどのように分けていくのか、各社のサービスと関係するデータから決済情報をどのように分離するのかが課題となる。競争領域については、現在は上位システム A、

Ｂ、Ｃの中で個別に流通している決済情報を取り出しこの透明性を確保しつつ関係者の間で様々なことを取り決めていく、あるいは API 接続といったベーシックな部分、共通化されている部分を民間事業者に広く提供していくことが重要なポイントになると考えている。

上記の質疑応答終了後、株式会社大日本印刷の土屋氏と佐藤氏からプレゼンテーションが行われました。

（大日本印刷　土屋氏）当社は、今から約 40 年前に IC カードの研究開発に着手し、1990 年代後半以降、そのコアとなるテクノロジーを用いて様々なサービスを展開している。具体的には、ユーザー向けのフロントサービスとして、「モバイル Wallet サービス」や「スマートフォン向け銀行口座開設用アプリ」を、加盟店向けには、「決済端末とそのゲートウェイ」を提供してきた。また、アクワイアラ向けの「業務システム」や、イシュア向けの「決済のプロセッシング」や「認証関連」のサービス提供も行ってきた。これらに加えて、脆弱性診断、不正検知などのセキュリティ対策をワンストップで提供可能なところが当社の特徴である。印刷会社として培ってきた長い歴史の中で、決済のみならず、幅広い事業領域において顧客支援サービスを展開してきた。こうした経験から、本日は、当社が提供する幅広い決済および決済サービスに関するテクノロジーの紹介などを通じて、「セキュアな決済を支えるユーザーデバイス」について説明する。

最初に、「クラウドペイメントサービス」である。これは、スキームオーナー、決済ブランド、TSP/TSM ベンダー（当社）という主体のもとで、クレジットカード番号をトークン番号に置き換えてスマートフォンに発行するサービスである。「バーチャルカードが主で、物理カードが副」という近年の Digital First の時流に合わせ、ユーザーからのリクエストに応じてリアルタイムにカードを発行し、即時に決済サービスを提供することが可能となっている。

2 つ目のテクロノロジーが、現在財布の中にあるものをスマートフォン等に格納する「モバイル Wallet サービス」である。このサービスは、スマートフォンの UI アプリと、クレジット・プリペイド等の各種カードやクーポン・ポイントといった外部の複数の電子決済サービス等の中継サーバとしての役割を担っており、これらを一つのゲートウェイに束ねて顧客に提供している。プロダクトレイヤーでは、各種スマートカードや NFC タグをスマートフォンと連携して提供することも可能である。また、アプリケーションレイヤーでは、デジタルなカードを発行するだけでなく、個社向けの Wallet としてアプリからゲートウェイまでをクラウドサービスを用いて提供している。このほか、これらと連携したマーケティングサービスも提供している。

3 つ目が、「NFC タグ認証プラットフォーム」の取り組みである。わが国における決済インターフェースの変遷をみると、最初は磁気カードから始まり、次に接触・非接触型 IC チップが登場し、その後、スマートフォンにおける NFC 決済や QR コード決済が拡がった。こうしたもとで、今後、新たなサービスが登場し、市場

が拡大していく可能性がある分野として NFC タグ決済に注目している。これは、カード番号や ID をユーザー側の端末に持ち、店舗側のリーダーで読み取るという従来の仕組みを、店舗側のタグ（ID）をユーザー側の端末で読み取る仕組みとすることで、認証情報の送り手と受け手をチェンジしようとするものである。NFC サービスを巡る環境変化をみると、2012 年に NFC リーダーモード機能を活用したサービスが登場したが、当時は Android のみでしか使用できず、NFC の読み取り能力も低かったため、サービスとして普及しなかった。非接触型 IC の使用についても、TypeA、TypeB、TypeF などが存在し、相互換性がない状態となっていた。この点については、当社も参加する NFC Forum（国際標準化団体）において標準化が試みられている。また、最近では、スマートフォンの普及率の高まりや 2019 年に iOS で NFC リーダーモード機能が開放されたことを背景に、決済に関する情報をユーザー側の端末で読み取る環境が整いつつある。社会環境として非接触サービスの需要増加やセキュリティを高める仕組みの確保等といった流れも併せて考えると、NFC タグは、非常に有望なサービスであると考えている。

NFC タグ認証プラットフォームでは、NFC タグにタッチしたスマートフォンが読み取ったタグ情報を、事業者アプリを経由して、当社の NFC タグ認証サーバに問い合わせ、認証鍵を用いて認証を行い、その結果を返すという流れとなっている。QR コード決済の MPM（Merchant-Presented Mode）と同じような電文の流れとなっているが、一点異なるのは、暗号鍵を持ったセキュアなタグを用いることにより、その場所に確実にそのタグが貼られていることが認証され、そのうえで次のアクションに移せる流れになっている。想定されるユースケースとしては、第 1 にスマートフォンによる店頭での対面オンライン決済、第 2 に自販機やゲームセンター、コインランドリーにおける自動精算機での決済、第 3 に交通乗車券などがある。2 つ目の自販機については、すでに非接触型の IC リーダーが埋め込まれているが、NFC タグおよび制御ユニットを搭載することで、読み取り機能を埋め込まずに決済が可能になる。3 つ目の交通乗車券については、読み取り機等を設置することなく NFC タグを貼るだけで、バスなどの乗降車が可能となる。将来的には、新たなインフラを低コストで整備することが可能となったり、様々なタッチポイントを通じて取得したユーザー情報をマーケティングで活用したりするなど、地方創生といった文脈を含め、非常に大きなポテンシャルを有していると考えている。

（大日本印刷　佐藤氏）最後に、「本人確認・認証」の取り組みを紹介する。決済分野でも、セキュリティがますます重要になってきているが、当社でも、その特徴である印刷技術を活かし、マイナンバーを用いた公的個人認証や、当社独自の真贋判定補助サービスを提供している。これは、免許証等の各種証明書を用いた処理の際に、IC チップを読み取るだけでなく、スマートフォンのカメラを用いて写真撮影を行い、それが本物かどうかを判断する技術である。2022 年度からは、マイナンバーカードや在留カードについても対応予定である。その他にも、犯収法に準拠したサービスとして、マイナンバーカードの IC チップを

NFC 端末で読み込み、PIN 入力で本人確認する方法にも対応している。

なお、最近では、生体認証によって顔情報を取得・収集した後、他業界との連携を通じて本人確認を行う取り組みを始めている。現在 30 社近くの企業が参加し、決済だけでなくセキュリティや認証面も含めて、各種の課題解決に力を入れて取り組んでいる。

上記のプレゼンテーション終了後、以下の質疑応答が行われました。

（日本銀行決済機構局　山田）近年の決済サービスの特徴の一つとして、ソフトウェアを活用したオンラインでのサービス提供が増加しているように思われる。こういったソフトウェアの活用やオンラインでのサービス提供について留意すべき課題はあるか。

（大日本印刷　土屋氏）決済サービスのメインはオンラインであり、特に最近は、シンクライアントを用いて通信を行いサーバ側で管理するという流れがある。オンラインについては、ユーザーのスマートフォンに複数のサービスを載せられるということが一番のメリットであろう。スーパーアプリのように便利なサービスを次々に搭載していく、というのが大きな流れであると承知している。

上記の質疑応答終了後、株式会社 TRUSTDOCK の千葉氏からプレゼンテーションが行われた。

（TRUSTDOCK　千葉氏）当社からは、「ユーザーデバイスのセキュリティ」に関し、特に人にフォーカスしながら、eKYC・デジタルアイデンティティについて説明する。まず、CBDC と eKYC・デジタルアイデンティティの関係性についてであるが、CBDC は単純に「お金がデジタル化」するという話ではなく、日本銀行が金融機関だけを相手にしていた世界から、CBDC が配布される個々人が「誰」なのかを意識するという話である。すなわち、様々なセキュリティ技術について検討する前に、そもそも個々のアイデンティティやそれに紐づくエンティティとは何かを考える話である。その意味で、CBDC は実はロマンティックな話と捉えている。

KYC（Know Your Customer）は、金融用語で顧客確認を意味し、本人確認と同義で用いられている。本人確認の中には、①身元確認、②当人認証の 2 つの概念が存在し、これらは基本的に別のものである。②の当人認証には、自己のみが知り得る ID やパスワードといった情報を用いてログインを行う知識認証、物理的な鍵やカードに代表される所有物認証、各種の生体情報を確認する生体認証が含まれる。多要素認証とは、これらの組み合わせによって、認証の強度（当人性）を高めるというものである。他方で、いくら認証強度を高めても、当人の属性たる身元情報を確認するのは困難であり、これを確認するのが①の身元確認である。具体的には、一人に 1 点のみ発行されている公的身分証を用いる方法のほか、住民票や公共料金の支払い領収書といった複数書類を組み合わせる方法、銀行の口座開設における契約書のように一度身元確認を行った契約に依拠する方法が存在する。基本的には、①

身元確認と②当人認証をどういったレベルで行うべきか、事前設計するのがベストプラクティスといわれている。

金融取引では、項目の違いはあるものの、その全ての取引において、「身元確認を伴う本人確認」が必要となる。また、我々の生活に関連する手続き等においても、例えばアパートや携帯電話の手続きのように、当人認証だけでなく、身元確認が要求される場面が多い。DX の文脈の中で、本人確認に関する様々な技術が生まれており、これが eKYC（electronic Know Your Customer）である。基本的にはオンライン等の非対面・デジタルで行う KYC を指すが、eKYC の手法自体は各国の各種法規制により区々となっている。

日本では、2017 年以降、各種取引・手続きのオンライン化の進展する中、2017 年以降、本人確認のオンライン化・厳格化が進み、これに対応する法改正が継続的に行われている。犯収法については、2018 年末に改正が行われ、それまでの対面・郵送による本人確認手法に加えて、郵送なしの非対面手法（eKYC）が追加された。具体的には、顔写真や身分証の撮影、身分証の IC チップの読み取りと顔写真の組み合わせ、銀行 API との連携、マイナンバーカードを用いた公的個人認証等といった方法が認められている。現在、最も利用されている手法は、全ての身分証が対象である点で非常にカバレッジが広い、顔写真および身分証の撮影である。

eKYC 事例について、当社では、全ての書類に対応しており、非スマートフォンユーザー向けにパソコンのみで完結する方法や、第三者利用等に対するセキュリティ確保を行うなどプライバシーに配慮した方法、動画撮影・画像認識・音声認識を行う方法も提供している。社会全体では、コロナ禍のもとで、業界一律で eKYC を導入する動きが進んでいる。金融関連では、すぐに実行したい金融取引を有する業界、例えば、価格のボラティリティが高く、口座開設時に直ぐに取引を実行するニーズが大きい証券や暗号資産業界で実装が進んでいる。金融以外では、eKYC に関する法改正が済んでいる古物商や通信業界において導入が進んでいる。このほか、法規制がない業界においても、利用者の安心・安全等を理由に、自社のポリシーとして eKYC の活用を検討する企業が増えてきている。

行政側では、2019 年に行政手続きにおける本人確認のガイドラインが整備された。この間、マイナンバーカードが普及してきており、今では運転免許証に次ぐ水準（約 5,000 万枚）になっている。保険証やパスポート等が行政の本人確認書類から除外されていく一方で、マイナンバーカードへの集約が進んでいる状況である。最近偽造運転免許証が増えているが、今後は、IC チップを NFC で読み取る本人確認手法も普及していくと考えている。このように行政は「デジタル to デジタル」に向けた検討を本格化しており、マイナンバーカードについては、すでに保険証の格納が実装されているほか、免許証の格納も近々

予定されている。その他、マイナンバーカード情報のスマートフォン搭載や、受け側である自治体などの行政システムの仕様統一等も検討されている。法規制のない分野の身元確認についても、様々な省庁の委員会等において検討が行われており、身分証の提示以外のセキュアな手法が模索されている。

eKYC の次に来るデジタルアイデンティティについて検討するにあたっては、個人やエンティティのような「名乗る側」の話だけでなく、それを「確かめる側」であるカスタマーデューデリジェンス（CDD&KYC）との両方を意識しなければならない。両者はコインの表裏の関係にある。この点、デジタル ID が 100%普及すれば KYC は不要という議論があるが、当社としては引き続き KYC は必要と考えている。これは、KYC とは誰を顧客とするかという「確かめる側」の企業の話であり、誰が自分をどの手段でどのように名乗ろうと、企業側が安全管理として確かめたければ発生するプロセスであるためである。

デジタルアイデンティティについては、コロナ禍の下で、様々な概念実証等が行われてきた。例えば、パーソナルデータ連携に関する実証実験、位置情報や顔認証技術を活用した Digital ID、外国人 IT エンジニア向け人材採用サービス、デジタル ID の相互運用に関する共同実験、在学証明書や卒業見込証明書のスマートフォンアプリへの発行などである。デジタルアイデンティティの定義や概念について確りとしたコンセンサスがあるわけではないが、当社しては、技術的な話とは別に、法律・規制に準拠しながら進める必要があると考えている。

当社事例として、「名乗る側」のデジタル身分証アプリ「TRUST DOCK」の取り組みを紹介する。これまで、「確かめる側」である企業を DX するための様々な確認業務 API を提供してきたが、これと対になるものとして、「名乗る側」であるユーザーのデジタルアイデンティティもカバーし、情報が滑らかな流通するデジタル社会を作っていきたいと考えている。現在は、リアルな身分証を企業に渡さなくても身元確認が可能なデジタル身分証についての実証実験を開始している。最近では、身分証情報の提供先企業におけるセキュリティが重要となってきているため、当該企業に対して必要最低限の情報のみを渡すといった、個人情報の適切な流通網を構築することが必要であると考えている。また、当社では、携帯電話会社や銀行との API 連携を通じた、身分証の提出以外での本人確認の取り組みを行っている。災害大国である日本で、身元確認書類がないために避難所で必要な手続きが進められないというのは問題である。これからのデジタル社会では、スマートフォン一つあれば身元を証明可能とすることが必要ではないか。

海外に目を向けると、ワクチン接種証明を皮切りに、専用スマートフォンアプリで能動的に資格証明を行う場面がどんどん広がってきている。同様に、デジタル身分証の制度面・環境面の整備も進んでいる。制度面では、EU においてデジタル ID の規則案が公開され、いずれ様々なサービスが花開くことが予期される。環境面では、iOS15 よりウォレットアプリが進化し、デジタル身分証明証を保存できるよう機能拡張

がなされる見込みにある。

企業が顧客を確認する CDD と、個人が身元証明するデジタルアイデンティティの双方の活用が進んだ世界を実現するためには、「相互運用性」が重要となってくる。CBDC をはじめとする真のデジタル社会に求められるセキュリティを実現するには、官民を超えて、日本社会全体、さらには国際社会全体で、規格やプロトコルを合わせながら情報の流通網を構築していく必要がある。

上記のプレゼンテーション終了後、以下の質疑応答が行われました。

（日本銀行決済機構局　山田）本人確認の領域では、個人情報保護の観点も必要である。また、個々の決済データを利活用してより良いサービス提供に役立てるという観点もある。どちらも重要であるが、この点に対する考えを伺いたい。

（TRUSTDOCK　千葉氏）2022 年 4 月に施行される改正個人情報保護法は、個人情報の保護と情報の利活用の両方に配慮した形となっている。例えば個人の権利保護が強化され、半年以内に削除されるデータも個人情報に該当することになるほか、情報の第三者提供記録の開示請求等が認められるようになる。一方で、個人情報の提供者から同意を取得すれば情報の利活用が可能となるほか、海外のトレンドに併せてデジタル ID 等に関する下地も整う見込みである。当社としては、社外の有識者とアドバイザリーボードを設置して、オンラインの本人確認の在り方について定期的な情報発信を行っている。情報の保護と利活用の境界は、社会でインシデントが発生すると揺れ動くことがあると思うが、それに合わせて調整可能なシステムを社会全体で作っていくことが重要と考える。

以　上