2021 年 7 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（6 月 11 日）議事概要

日本銀行決済機構局では、6 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」をオンライン形式にて開催しました。

分科会では、中央銀行デジタル通貨（CBDC）が、デジタル社会における決済プラットフォームとして機能することを念頭に、①CBDC に求められるセキュリティ、②CBDC に求められるユニバーサルアクセス、③デジタル通貨に関する情報技術の標準化、というテーマで三つのセッションを設け、それぞれ、企業等で実務に関わる方から、CBDC に活用し得る最新の技術や取り組みをご紹介頂くとともに、技術面からみた将来の CBDC のあり方などについて意見交換を行いました。

以下では、各セッションにおける議論の概要を紹介します。

１．CBDC に求められるセキュリティ

一つ目のセッションでは、「CBDC に求められるセキュリティ」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）。CBDC を「安心して使える」ものとするための高度なセキュリティは、昨年 10 月に日本銀行が公表した「中央銀行デジタル通貨に関する日本銀行の取り組み方針」（以下、「取り組み方針」）の中で、CBDC が具備すべき基本的な特性の一つに挙げられています。本セッションでは、まず、セコム株式会社の佐藤雅史氏より、将来の CBDC の発行形態を意識しつつ、求められるセキュリティの概要や検討すべき論点について説明がありました。続いて、日本電気株式会社の宮川晃一氏より、セキュリティに関する最近の取り組みのうち、デジタルアイデンティティや認証といった技術を中心に、基礎的な事項の説明がありました。

（セコム 佐藤氏）そもそも「セキュリティ」とは、「守りたいもの」を管理・防衛するだけでなく、安全・安心に利用を促進するものである。厳格に管理し過ぎて本来の利用ができないようでは、目的を達成したことにはならない。安全性と利便性はトレードオフの関係にある。

以下では、「取り組み方針」に示された情報をもとに、一定の想定を置いた上で、CBDC に関係する主体ごとに求められるセキュリティを整理する。まず、CBDC の発行を担う「日本銀行」は、CBDC 台帳を保持し、サイバー・物理の両面から、セキュリティ全般のマネジメントを行うことが求められる。これには、セキュリティ体制の構築、システム管理・台帳情報・暗号鍵に関する各種ポリシーの策定など、幅広い対策が含まれる。CBDC を利用者に行き渡らせる「仲介機関」は、日本銀行と利用者の間と安全な通信を確立し、利用者の本人確認を正しく行い、各種情報を管理する。CBDC の「利用者」（個人・企業）は、スマホアプリの安全性などに留意する必要がある。このほか、仲介機関と利用者の間に立って追加的なサービス（家計簿、資産管理、プログラマブルマネーなど）を提供する企業として、「サービスプロバイダー」の存在が想定される。これは、利用者に安全なアプリやウェブサイトを提供するとともに、利用者の本人確認を正しく行い、各種情報を管理する。さらに、すべての主体が、AML/CFT の観点、プライバシー保護の観点に留意して、日々のオペレーションを行うことが重要である。

CBDC のように、多くの主体にまたがってシステムが構成されている場合、それらの間でセキュリティに関する基準が共有されていることが重要である。「誰が何のために何を守るのか」、「前提となるシステムは何か」などによって、行うべき対策やその重要度も変わる。こうした点を意識しながら、既存の基準を活用して適切な基準を策定していくことになると思う。

（日本電気 宮川氏）デジタルアイデンティティの領域で重要な「本人確認」は、「身元確認」と「当人認証」という二つの要素で構成されている。「身元確認」は、登録する利用者が実在することを、身分証などを使って確認する作業である。「当人認証」は、現に取引等を行っている人物が間違いなく「身元確認された本人である」ことを、パスワードなどで確認することを指す。この二つを組み合わせて本人を認証することになるが、ネットワーク経由で電子的に認証する場合、技術的に多くの困難が伴う。これは、インターネットの世界では、相手の端末の前に座っているのが本人でなく「犬」であっても、正しいレスポンスがある限り分からないからである。

従って、残高照会を一つとっても、物理社会（ATM）ではカードと暗証番号があれば足りるが、デジタル社会（スマホアプリ）では、ログイン ID・パスワードを利用者が入力した上で、IP アドレス・スマホ固有番号なども取得する必要があるなど、手続きが重くなる。さらに送金ともなれば、これに多要素認証などが加わる。ここで重要なことは、リスクベースコントロールの考え方、すなわち、直面するリスクのプロファイルや程度に応じて、対策の技術強度を調整することである。技術の強度は、評価保証レベルによって示される。米国 NIST（国立標準技術研究所）のガイドラインでは、身元確認については、「自己申告」（レベル１）から、「対面で公的身分証を確認」（レベル 3）まで設定されており、当人認証については、知識情報・生体情報・所持情報の３要素のうち「単要素認証」（レベル１）から「２要素認証＋一つは

ハードウェアを用いる」（レベル３）まで設定されている。適切な評価レベルの対策を組み合わせて、リスクに見合ったセキュリティを実現することになる。

匿名性を確保することは、CBDC にとって重要な論点と考えるが、その方法については、匿名化（Anonymization）と仮名化（Pseudonymization）があり、両者を分けて考える必要がある。一旦匿名化されたデータは元に戻せないが、仮名化されたデータは暗号技術により元に戻すことができる。いずれにせよ、将来、CBDC 決済において匿名性を確保するには、国際的な枠組みの中で、法的な手続きに基づいて実行されることが重要である。

上記のプレゼンテーション終了後、プレゼンター２名により、以下のような意見交換が行われました。

（セコム　佐藤氏）CBDC システムのセキュリティについて、重要と考える論点を挙げる。一つは、「相互運用性とセキュリティの両立」である。CBDC は、仲介機関やサービスプロバイダーなど複数の主体が運用に関わることで成り立つ仕組みであり、システム間の相互運用性は重要である。この点、セキュリティの差異に起因して相互運用性が低下する可能性があることに留意する必要がある。もっとも、相互運用性のみを重視してセキュリティが低下することは望ましくない。何らかの基準を作成するなどして、両者のバランスを取ることが重要である。「暗号鍵」の適切な管理も重要な論点だ。暗号鍵については、生成、利用、失効、廃棄、復旧などのライフサイクルを考える必要がある。また、特にオフライン決済を想定した場合には、仲介機関との連携ができないため、利用者デバイス側（ウォレット）でしっかりと暗号鍵を管理する仕組みが必要となってくる。

（日本電気　宮川氏）暗号鍵のライフサイクル管理は大変重要である。鍵の漏洩といった異例時における手続や、鍵を紛失した場合の再発行の方法など、運用上の論点が多い。CBDC の場合、紛失等により失効した鍵を管理するリストは膨大なものになると予想されるが、そうしたリストに期限を設けるかどうかも重要なポイントの一つだと思う。

（セコム　佐藤氏）CBDC に関連したアプリケーション、デバイス、プロトコルは、いずれ入れ替える必要がある。また、暗号鍵の強度が時間の経過とともに低下することを見落してはならない。CBDC に関する暗号アルゴリズムの移行は社会全体に与える影響が大きいだけに、「移行可能性」を意識した仕組み作りが重要である。

（日本電気　宮川氏）プレゼンテーションでも強調したが、「リスクベースの保証レベル」の考え方も重要である。リソースが有限である中では、保証レベルをどこまでも上げることは不可能である。守るべき情報資源の重要性、システムの特性、脅威の可能性に応じて、どこかでリソースの投入を打ち止めるなど、一

定の割り切りも必要ではないか。また、CBDC のセキュリティは、技術のみによって守るのではなく、他の方策も組み合わせてトータルで確保していくという発想が重要である。例えば、CBDC の不正利用などに対応するため、金融 ADR のような何らかの紛争解決制度を導入することも必要と考えられる。オフライン決済については、セキュリティに関する技術的なハードルの高さを考えると、当面、CBDC と現金が共存し被災時などには現金が決済を支える仕組みとすることで、全体としてセキュリティが確保されていると評価することも可能ではないか。

（セコム　佐藤氏）本日の議論を振り返ってみると、「セキュリティ」は、今回の分科会の別のセッションである「ユニバーサルアクセス」や「技術の標準化」といったテーマとも重なっており、非常に広がりがある論点といえる。本日は概説にとどまるが、今後もこの分科会の枠組みなどを通じて、セキュリティ関係の検討が進められることを期待する。

２．CBDC に求められるユニバーサルアクセス

二つ目のセッションでは、「CBDC に求められるユニバーサルアクセス」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）。CBDC を「誰でも使える」ものにするというユニバーサルアクセスも、「取り組み方針」の中で、CBDC が具備すべき基本的な特性の一つに挙げられています。本セッションでは、まず、株式会社 NTT ドコモの江藤俊弘氏より、わが国におけるモバイルネットワークの「世代移行」の経験を参考に、新たなインフラを円滑に浸透させていく方法やその際の留意点について説明がありました。続いて、App Annie Japan 株式会社の上村洋範氏より、将来、CBDC を提供する媒体として想定されているスマホアプリについて、内外における近年の利用状況やユーザニーズの分析等に関する報告がありました。

（NTT ドコモ　江藤氏）過去 30 年間におけるわが国のモバイル通信市場の変遷をみると、時代とともに消費者の行動が大きく変容し、それに伴いモバイル通信のデータ量が急増している。この背景には、単なる通話から、テキストや画像データの送信、さらには動画データの多頻度のやり取りなど、通信に求められる役割が大きく変化したことがある。こうしたデータ量の増加を支えるために、当社が提供するモバイル通信ネットワークは、約 10 年周期で世代交代が進んできた。そのたびに旧方式から新方式への切り替えに必要となるが、これまでの経験では、全国の顧客への周知を含めると、実際の移行には 15 年以上の期間が必要となる。また、新世代のインフラが浸透していくには地域差があり、通常、都市部から地方へと時間をかけて進んでいくことがわかっている。このように、モバイル通信ネットワークの世代移行は長期間かつ大規模なプロジェクトである。デジタル方式の決済手段である CBDC についても、いま述べたような決済

インフラの世代移行の問題が存在し、それがユニバーサルサービスのあり方にも影響してくるのではないかと考えている。

過去の経験を踏まえつつ、こうした世代移行をスムーズに行う観点から、新たなインフラを導入する際に求められる要件をまとめてみる。まず、利用者からみて、利便性や価格の面で、新方式に切り替える明確なインセンティブが存在していることが最も重要である。サービスを提供する側の視点に立てば、機能改善やコスト効率化の面で利用者ニーズへの合理的な解となり得ているか、また、システム的な考慮点として旧インフラを一定期間引き続き利用できるか、つまり下位互換性を確保できているかがポイントとなる。

（App Annie Japan 上村氏）モバイル市場はコロナ禍を経てさらに大きくなり、多くの国民の生活にますます入り込んできている。CBDC のユニバーサルサービスを考える際にも、スマホやアプリをどのように利用していくかが重要なポイントとなる。

2020 年における日本のモバイル市場を概観すると、新規アプリのダウンロード数やアプリストアでの消費支出などは引き続き拡大しており、1ユーザ当たりの1日のアプリ利用時間 は3.7時間に達している。また、ダウンロードされる海外アプリのシェアは 2018 年には 20%であったが、この 2 年で、若者向けアプリを中心に 33%に急伸した。このことは、日本のモバイルユーザの志向が変化している可能性があることや、満たされていないニーズに対応することで国内市場を開拓する余地がなお大きいことを示唆している。ユーザの年齢別にみると、若年層はゲームや SNS、社会人層は仕事の効率化に関するアプリ、高齢者層はニュースや天気予報アプリの利用率が高い。日本については、他国と比較して、年齢が高い層もモバイル利用に精通している点が特徴といえる。

金融アプリやフィンテックアプリについても、国や年齢層によって特徴がある。例えば、米国の若年層は、銀行アプリよりも先にフィンテックアプリを利用している。日本では、銀行以外の企業が、積極的なユーザ還元や CM 効果を通じて金融アプリの導入をリードしている。一部に急激にシェアを伸ばしている先もあるが、それでも普及率は 30%程度である。この点を踏まえると、仮に将来 CBDC アプリを導入したとしても、全国的な普及には相当時間がかかる可能性があるのではないか。なお、ブラジルの金融アプリCaixaは、政府のコロナ支援金がこのアプリを通じて支給されることになったため、利用者が一気に増加した。このように、多くの利用者を抱えるサービスを調査・研究する際は、国内だけでなく海外のサービスの動向もみていく必要がある。

上記のプレゼンテーション終了後、株式会社ボストン・コンサルティング・グループ（BCG）の東海林一氏をディスカッサントに招いて、以下のような意見交換が行われました。

（BCG　東海林氏）様々なタイプのユーザが利用するモバイル通信に関し、インフラを更新し、旧方式から新方式へ乗り換えてもらうインセンティブをどのように設定したのか。

（NTT ドコモ　江藤氏）ユーザに具体的なメリットを訴求することが重要。多量のデータをより高速かつ安価で送ることができるというメリットに加え、新方式乗り換えに伴う手続きが簡便であるという点もアピールした。さらに、こうしたメリットをユーザに分かりやすく伝えることが重要である。

（BCG　東海林氏）様々なモバイルアプリが存在する中で、あるアプリが使われるためのインセンティブは何か。アプリが使われ続ける条件は何か。

（App Annie Japan　上村氏）消費者向けビジネス（B2C）では、ポイント付与などを通じて自社収益を消費者に還元することがアプリ普及率の向上につながっているケースが少なくない。また、利便性の高いインターフェースを利用者に提供すること、とりわけ、利用にあたってのストレスをどれだけ軽減できるかも重要。利用者のタッチポイントをどのように増やすかという視点も大事である。この点、特定の機能だけを提供するのではなく、生活全般や地元経済圏に密着した多様なサービスをまとめて提供する「スーパーアプリ」はユーザの利用インセンティブを高めるうえで有効な仕組みだと思う。

（BCG　東海林氏）特に高齢者に対し、新たな技術やアプリの利用を広める手立ては何か。CBDCの普及という観点では何が必要か。

（NTT ドコモ　江藤氏）当社では、新方式に金銭的な優位性を持たせたり、同じ価格条件での利便性を強調したりしてユーザに訴えかけてきた。もっとも、通貨として機能する CBDC に、ポイント還元のような経済的なメリットを付してよいのかどうかは、慎重に検討する必要があるのかもしれない。新方式の利用インセンティブという点では、スマホやアプリを作って配るだけでなく、現場のサポート力をどのように確保するかが重要だと考えている。スマホの販売を開始した当初は、利用方法がわからないという声が多数寄せられたため、そうした声に対応すべく、現場のショップで様々なサポートを行った。当社は全国に多数展開する店舗で、高齢者のユーザに直接対応できるのが強みである。CBDC については、全国各地の国民がストレスなく利用できることが求められるので、その普及にあたっては、こうしたサポート体制を整えることも必要だと考えている。

（App Annie Japan　上村氏）ユーザーインターフェースについては、作りがすっきりしていて、どこを操作すれば何ができるかが容易にわかることが重要。そもそも、高齢者だからといって新しい技術に適合する能力が低いと決めつけることはできない。孫とコミュニケーションをとるために高齢者がメッセージアプリをすぐに使いこなせるようになった、といった話はよく聞く。私の母も、少し前にスマホを使い始めたが、既に数十の

アプリがインストールされている。重要なことは、ユーザのニーズにどのように応えていくかである。CBDC の利用を促進するための方策としては、例えば、スーパーアプリの中に CBDC を搭載することが考えられるのではないか。決済機能だけなく、日常的に利用する他の機能とセットでユーザに提供すれば、CBDC が利用される機会もおのずから増えていくと思う。

３．デジタル通貨に関する情報技術の標準化

三つ目のセッションでは、CBDC に関連する情報技術の標準化について、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。情報技術の標準化のあり方は、「取り組み方針」において、制度設計面の今後の検討項目の一つに掲げられています。本セッションでは、まず、本年 5 月に日本銀行が公表した決済システムレポート別冊「デジタル通貨に関連する情報技術の標準化」の概要説明が行われ、続いて、デジタル通貨の分野を中心とした標準の活用のあり方について議論が行われました。

―― なお、ディスカッサントとして参加した ISO/IEC JTC 1/SC 17 国内委員長の廣川勝久氏については、国内委員長の立場には限定せずご発言頂いています。

（日本銀行決済機構局　森）「標準化」とは、自由に放置すれば、多様化、複雑化、無秩序化する事柄を少数化、単純化、秩序化することである。特にデジタル通貨における標準化については、①金融取引を処理するシステム間の「相互運用性の確保」、②金融取引を処理するシステムに対する「信頼性の確保」、③先進的な情報技術を中心とした「専門的知見の集約・活用手段」という意義がある。こうした意義に照らすと、デジタル通貨における標準化領域としては、主に、①データを伝送するフォーマットやデータ項目、②必要なデータを識別しやすくするための付番・コード体系、③データを安全に伝送する技術の三つが挙げられる。CBDC においても、標準化を通じた相互運用性と信頼性の確保は極めて重要である。また、国内の優れた情報技術が CBDC にも幅広く応用されるよう、技術の研究・開発に関わる関係者が国際標準化の議論に積極的に参画していくことが望まれる。

（日本銀行決済機構局　橋本）クレジットカード決済はデジタル化された既存の決済システムの一つであり、デジタル通貨の標準化について検討していくうえで参考になる部分がある。クレジットカードの情報技術に関する標準化分野は、ISO/IEC JTC 1/SC 17 などの委員会を中心に議論されているほか、日本銀行決済機構局が国内委員会事務局を務める ISO/TC 68 の委員会でも、店舗からクレジットカード会社に送られる情報の電文フォーマットなど業務面に関する技術仕様が議論されている。クレジットカード会社は、これらの様々な国際標準を組み合わせながらビジネスに活用している。

仮にこうした国際標準が存在しないとどのようなことが生じるだろうか。企業の立場を考えると、「自社のビジネスを有利に進める」、「顧客を囲い込む」といった理由から、標準を活用するよりも、自社独自の仕様でビジネスモデルを構築したいというモチベーションもあろうかと思う。企業は、標準の仕様と個別の仕様をどのように使い分けているのか。

（廣川氏）標準の仕様と個別の仕様の使い分けについては、クレジットカードやデビットカードの国際ブランドが決済用 IC カードの共通仕様として開発した EMV 仕様の考え方が参考になると思われる。

すなわち、各国際ブランドは競争関係にある一方、世界市場で IC カード化を進めていくためには、単独ではなく、世界のビジネス環境を共通化する標準化領域が必要であるとして、ISO の国際標準を活用しつつ EMV 仕様を共同で開発した経緯がある。ただし、リスク管理の詳細など個々の国際ブランドやクレジットカード会社に委ねるべき固有の領域には、独自の仕様が認められている。このように、システム全体としては共通仕様を持ちつつ、同時に、個社の独自仕様も認める自由度のある構造となっている。

どのような領域で標準を必要とし、活用していくかは、いかなるビジネスを意図しているかに深く関わっている。また、標準化には、国際標準だけでなく、国家標準、地域標準、業界標準など、適用範囲の異なる様々な標準化があり得る。ビジネスを考える場合に、特定の業界を想定するのか、異なる業界との連携も想定するのか、あるいは、特定の地域や国だけを対象にするのか、全世界を対象にするのか、などによって求められる標準化の範囲は変わり得る。さらに、社会ニーズの変化や技術の進歩・発展に応じて、標準化の範囲も変化していくものと考えられる。

（日本銀行決済機構局　橋本）クレジットカードの標準化を踏まえると、今後、デジタル通貨の検討を進めていくにあたり、システム面・技術面の要件と、ビジネス面の要件の関係性について、どのように整理すべきとお考えか。

（廣川氏）デジタル通貨は新しいビジネスであり、ビジネス環境自体も変化している。難しい作業だとは思うが、システム面・技術面の要件を考えていくうえでは、そのビジネス環境において想定する前提条件を明確化しておく必要がある。

また、そうした前提条件については、必須の条件か任意の条件か、将来的に変更していく可能性があるか否か、市場拡大を視野に共通化していく領域か、それとも競合を視野に差別化していく領域か、などの視点で整理しておく必要がある。前提条件が明確化されると、ビジネス環境の「意図された変化」と「意図せざる変化」への対応をスムーズに行えるようになる。

（日本銀行決済機構局　橋本）デジタル通貨に関連する標準化については、今後も関係者間で対話を重ねていく必要があると思われるが、議論を進めていくうえでの留意点は何か。

（廣川氏）デジタル通貨は新しいビジネスであるが、それが利用される場面では既存のビジネスと無縁ではない。既存のビジネスとデジタル通貨の間で前提条件がどのように異なるのかを整理することが重要である。例えば、決済のファイナリティ（支払完了性）の考え方、オフライン環境下における利用の有無など、様々な論点が考えられる。そうした整理に基づいて、標準化の議論を進めていくことが求められるのではないか。

以　上