



中央銀行デジタル通貨に関する実証実験  
「パイロット実験」の進捗報告書（2026年6月）  
CBDC フォーラムにおけるこれまでの議論の総括【別冊】

日本銀行決済機構局

2026年6月

## 目次

はじめに .....	3
本稿の読み方 .....	4
1. CBDC システムのアーキテクチャー .....	5
1.1 基本的な機能・性能とこれを満たすシステム構成等について .....	6
1.1.1 CBDC 台帳と顧客管理システムの構成 .....	6
1.1.2 システムへの負荷 .....	9
1.1.3 仲介機関間のネットワークシステムの整備 .....	10
1.1.4 強靭性 .....	12
1.1.5 即時決済性 .....	13
1.1.6 事務フロー .....	14
1.1.7 データモデル/データベース技術 .....	20
1.2 エンドポイントデバイスとユニバーサルアクセス（主にフロントエンド） .....	23
1.2.1 デバイスの種類 .....	23
1.2.2 UI/UX .....	26
1.2.3 顧客管理・台帳管理システム間の同期 .....	28
2. CBDC のユーザーを支えるシステム .....	31
2.1 KYC と AML/CFT .....	33
2.2 認証・認可 .....	43
3. CBDC エコシステムのあり方 .....	49
3.1 仕様の標準化 .....	50
3.2 システムの共同化 .....	54
3.3 追加サービスと API .....	56
3.4 プログラマビリティ .....	58
4. 相互運用性と水平的共存 .....	60
4.1 現金との関係 .....	61

4.2 銀行預金との関係.....	64
4.3 民間デジタルマネーとの関係.....	68
4.4 CBDC の発行・流通にかかるコスト負担と既存ネットワークの活用.....	75
5. 新たなテクノロジーと CBDC.....	79
5.1 デジタルアイデンティティ.....	80
5.2 オフライン決済.....	81
5.3 ブロックチェーン関連技術.....	84
5.3.1 アセットトークナイゼーション.....	84
5.3.2 インターオペラビリティ.....	88
5.4 次世代技術の活用.....	91

## はじめに

本稿は、「中央銀行デジタル通貨に関する実証実験『パイロット実験』の進捗報告書（2026年6月）」（以下、「本冊」という）の別冊として、パイロット実験開始以降のCBDCフォーラム（以下、「フォーラム」という）における議論を総括したものである。

フォーラムは、「実験用システムの構築と検証」と並んでパイロット実験の2本柱を成しており、リテール決済に関する技術や実務の知見を有する金融機関、スタートアップ企業を含む一般事業者等、多彩な企業の方々にご参加頂いている（2024年3月時点の参加者は計64社）。その運営に当たっては、日本銀行決済機構局が事務局となり、テーマ毎に7つのワーキンググループ（WG）を設置。2023年7月のフォーラム設置以降、84回の会合を開催し、延べ163社にご登壇頂くなど、CBDCにかかる幅広いテーマに関し、リテール決済に関わる民間事業者の協力を得て、精力的に議論・検討を重ねてきた。

フォーラムについては、より横断的かつ多面的に決済の将来像を検討する観点から、2026年度より7つのWGを3つのディスカッショングループ（DG）に再編するなど、その運営を見直すこととした。本稿は、こうした機会を捉え、これまでのフォーラムで得られた知見を総括し、民間事業者と議論してきたCBDCに関する機能別論点を下記のとおり再構成して詳細に提示することで、読者のCBDCに対する理解を深めることを目的として作成したものである。

（本稿の構成と主なトピック）

1	CBDCシステムのアーキテクチャー	CBDCの基本的な機能・性能・システム構成、 エンドポイントデバイスとユニバーサルアクセス
2	CBDCのユーザーを支えるシステム	KYC、AML/CFT、認証・認可
3	CBDCエコシステムのあり方	仕様の標準化、システムの共同化、追加サービスとAPI、 プログラマビリティ
4	相互運用性と水平的共存	現金・預金・民間デジタルマネーとの水平的共存、 発行・流通にかかるコスト負担と既存ネットワークの活用
5	新たなテクノロジーとCBDC	デジタルアイデンティティ、オフライン決済、 ブロックチェーン関連技術、次世代技術の活用

## 本稿の読み方

各章の本文中では、各論点に関する会合での議論を取りまとめた本文のほかに、関連するフォーラム参加企業等のコメント内容を列挙した表を掲載し、複数の会合で個別に議論された内容を、論点毎に把握できるように構成されている（下図参照）<sup>1</sup>。

（本稿における本文と表の関係）

### 3.2 システムの共同化<sup>33</sup>

多くの民間事業者が仲介機関として参入しやすい仕組みを整えることは、CBDC エコシステムを活性化させる上で重要な要素の一つと考えられる。このため、各仲介機関が個別に顧客管理システムや台帳管理システムといった仲介機関システムや、AML/CFT や不正検知の仕組み等の周辺システムをスクラッチで構築・維持するのではなく、共通性が高く競争優位性を生まないインフラ部分や業務プロセスについては、システムの共同化を検討することも一案。会合においては、共同化によるメリットとデメリット、システムを共同化するに当たっての留意事項について意見が交わされた。

各会合でフォーラム参加企業から聞かれたコメントを、トピック毎に整理して一覧化

（表3-5）システムの共同化のメリット・デメリット

個別運営対比で効率化に期待
CBDC システム（仲介機関システム（顧客管理、ユーザー口座））の共同化によって、①仲介機関毎にシステム構築が不要となるほか、②共同のシステム内での指図となるため、システムを跨いだ指図は不要となりフローが効率化される。結果として、仲介機関毎にシステム開発を行うのに比べ、参画することが容易になるといったメリットが考えられる。
仲介機関業務の共同化によるメリットは、大きく4点考えられる。1点目は、「効率性の向上」。共通プラットフォームの使用により取引・事務・システム運用コストが削減できる可能性。2点目は、「互換性の確保（標準化）」。各仲介機関間での情報共有やシステム連携がスムーズになる可能性。3点目は、「負荷分散のコントロール」。各仲介機関に過度な負荷がかかることを防ぎ、システム全体の安定性が向上する可能性。4点目は、「高度化」。共同化によって集められたデータの利活用が可能となることで、処理が高度化できる可能性がある。
セキュリティリスクや運用の複雑性、競争の阻害等のデメリットも想定
仲介機関業務の共同化によるデメリットは、大きく3点考えられるが、見方によってはメリットにもなりうる。1点目は「セキュリティリスクの増大」。共同システムが攻撃を受けた場合、影響が大きくなる可能性。ただし、共同化されていることで対策が打ちやすい側面もあるだろう。2点目は「運用の複雑性の増大」。複数の仲介機関が共同で運用するため、調整や管理が複雑になる懸念がある。ただし、適切に運用ができれば、むしろメリットにできる可能性もある。3点目は「競争の抑制」。共同化により、各仲介機関が提供するサービスが画一化し、競争が阻害される懸念がある。

各節の表題に付した脚注では、各論点について主に議論した会合を明記

<sup>33</sup> 本項については、主に WG3 の各会合において議論を実施。

<sup>1</sup> さらに詳しくフォーラムにおける議論内容を知りたい場合には、日本銀行 HP で公表している各会合の議事概要（[https://www.boj.or.jp/paym/digital/d\\_forum/index.htm](https://www.boj.or.jp/paym/digital/d_forum/index.htm)）も参照。

# 1. CBDC システムのアーキテクチャー

## 【第1章の概要】

本章では、CBDC システムの基本的な機能・性能およびこれを満たすシステム構成と、ユーザーとの接点となるエンドポイントデバイス等といった CBDC システムのアーキテクチャーに関する論点を整理する。

これまで日本銀行では、CBDC システムにおけるバックエンド領域、すなわち台帳管理の機能の設計パターンについて、集中管理型<sup>2</sup>ではなく、相対的により複雑で多くの項目を検証できると考えられる分担管理型<sup>3</sup>を前提に検討を進めてきた。一方フォーラムでは、必ずしも分担管理型に限定せずに台帳設計のバリエーション毎の特徴を検討した。また、周辺システムを含む CBDC システム等への負荷の観点、仲介機関間のネットワークシステムの整備、CBDC が具備すべき基本的特性（強靭性、即時決済性等）、事務フロー上の検討事項、将来的な技術革新を見据えた UTXO モデルや NoSQL/NewSQL の活用可能性等、様々な視点から考察を行った。

まず、台帳管理のパターンについては、集中管理型は台帳を管理するシステムが単一であるがゆえに効率的な仕組みであるなどの利点はある一方、耐障害性やレジリエンス確保が特に重要となるとの指摘があった。分担管理型はプライバシーの配慮や単一障害点の回避等の面での利点を享受しやすい可能性がある一方、台帳管理システムが複数存在する場合、台帳間の整合性確保は最優先であり、この実現方法が論点となるとの意見が聞かれた。さらにシステムへの負荷について、送金の都度オートチャージ・オートスウィングが発生しない設計や、各システムによる流量制限といった負荷軽減策の必要性に言及があった。また、CBDC の即時決済性は重要ではあるものの、既存のキャッシュレス決済の実情を踏まえると、購買にかかる小売店等への入金については、即時性を備えることが必ずしも小売店等のニーズと合致しない可能性があるとの意見があった。このほか、CBDC の基本機能を実行するための事務フローの検討に当たっては、台帳システム間のデータ整合性確保やエラー対応の重要性等が指摘された。最後に、台帳のデータモデルに関する UTXO モデルの活用可能性について、並列処理性やプライバシー確保の実装容易性が特徴とし

---

<sup>2</sup> 中央銀行が、すべての仲介機関とエンドユーザーの口座残高を記録する台帳を管理する方法。

<sup>3</sup> 中央銀行が、仲介機関（自己口・集約口）の口座残高を記録する台帳を管理し、仲介機関が、それぞれ自らの顧客ユーザーの口座残高を記録する台帳を管理する方法。

て挙げられる一方、想定されるシステム構成や処理フローによって特徴の現れ方が変わりうる点が指摘された。このほか、データベース技術である NoSQL や NewSQL について、高速処理や高スケーラビリティへの期待が指摘される一方、最新の技術ほど学習コストや運用管理面に課題がある点が指摘された。

エンドポイントデバイスについては、デバイスの種類や UI/UX、デバイス間での同期について議論を行った。ユーザーデバイスの種類としてはスマートフォンを主としつつ、子供などスマートフォンを保有しない幅広いユーザー層を考慮してカード型デバイスの必要性を指摘する声があった。UI/UX については、CBDC のイメージの統一化や、決済サービス事業者や端末ベンダーの開発環境のために、UI/UX ガイドラインがあった方が良さだろうといった意見が聞かれた。デバイス間の同期については、通信の不具合や障害の発生等により、ユーザーが台帳の更新状況を正確に把握できない事象が生じることに對し、ユニークな取引 ID の活用によるデバイス起点の迅速なタイムアウト処理や二重支払防止等、既存の仕組みが参考になるとの意見があった。

## 1.1 基本的な機能・性能とこれを満たすシステム構成等について

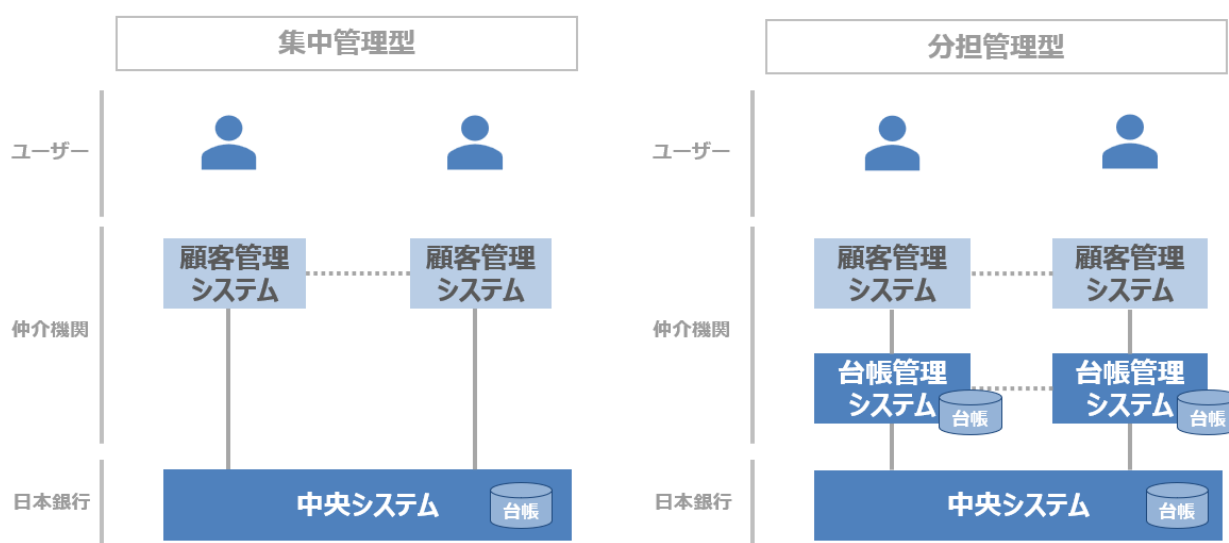
### 1.1.1 CBDC 台帳と顧客管理システムの構成<sup>4</sup>

日本銀行では、CBDC システムにおけるバックエンド領域、すなわち台帳管理の機能の設計パターンについて、相対的により複雑で多くの項目を検証できると考えられる分担管理型を前提に検討を進めてきたが、システムの効率性という観点からは、集中管理型も排除されるわけではない。また、分担管理型においては、台帳管理システムが複数存在するパターンや、付随して顧客管理システムが複数存在するパターン等、いくつかのバリエーションが考えられる。本項では、これらのバリエーションを念頭にフォーラムで提示された論点を整理する。

---

<sup>4</sup> CBDC 台帳と顧客管理システムの構成については、主に WG1 および WG7 の各会合において議論を実施。

(図 1 - 1) 集中管理型と分担管理型におけるシステム管理主体の違い



台帳管理のパターンについては、集中管理型は台帳を管理するシステムが単一であるがゆえに効率的な仕組みであるなどの利点はある一方、耐障害性やレジリエンス確保が特に重要となるとの指摘があった。分担管理型はプライバシーの配慮や単一障害点の回避等の面での利点を享受しやすい可能性がある一方、台帳管理システムが複数存在する場合、台帳間の整合性をいかに確保するかが重要な論点となるとの意見が聞かれた。

(表 1 - 1) CBDC 台帳と顧客管理システムの構成

中央システムが台帳を管理する集中管理型は、システムが単一であるがゆえに効率的な仕組みである一方、耐障害性やレジリエンス確保が特に重要
機能面や非機能面から検討すると、システム構成パターンはシンプルな構成が望ましい。一方で、シンプルであることで生じる課題を検討する必要があるだろう。
システムが単一の場合は、コストメリットは出せるかもしれないが、障害時の影響が一点に集中するので、CBDC の決済がすべて止まるようなことがありうるかもしれずレジリエンス面の課題がある。
中央システムのみが台帳を管理する集中管理型は、資金移動や残高照会の度に仲介機関システムと中央システム間で電文のやり取りが発生するので、中央システムは取引量に対するシステム耐性が求められる。

<p>分担管理型は、集中管理型と比較して資金移動の際の中央システム側の負荷を軽減可能</p>
<p>分担管理型は、資金移動や残高照会の度に仲介機関システムと中央システム間で電文のやり取りが発生するわけではないので、中央システムへの取引量による負荷を軽減できると思われる。</p>
<p>分担管理型は、プライバシーの配慮や単一障害点の回避等の面で利益を享受</p>
<p>顧客管理システムと台帳管理システムが一体かつ単一となるシステム構成で公的機関が情報をすべて管理するとなれば、プライバシー上の懸念があるかもしれない。他方、顧客管理システムと台帳管理システムが一体ではあるが複数存在するシステム構成で、仲介機関である民間事業者がそれぞれの責任範囲でシステムを管理するとなれば、市中の決済サービス同様であり、プライバシー上の懸念は少なくなるかもしれない。</p>
<p>システムが単一のパターンでは単一障害点が生じること、複数のパターンではシステム間の連携時のセキュリティ対策が必要であることについては、より詳細な検討が必要。</p>
<p>昨今は個々のシステムを極力コンパクトに分散して構築することでリスクを低減させる考え方もある。</p>
<p>台帳管理システムが複数存在する場合、台帳間の整合性確保が重要</p>
<p>台帳管理を行う主体の数が多くなると、台帳管理システム同士で直接接続することは負荷が大きく、現実的ではないかもしれない。こうした中で、台帳間の整合性をどのように確保するかが大きな論点である。</p>
<p>CBDC の送金処理は、信頼性の担保が最も重要であると考えため、台帳の整合性確保を最優先で行うことが望ましい。仮に、台帳管理システム間で決済完了した後に顧客管理システム側で何らかのエラーが発生したとしても、顧客管理システムから台帳管理システムに照会することなどによって結果的に整合性を確保できれば良いのではないだろうか。</p>
<p>顧客管理システムと台帳管理システムが複数の管理主体によって管理されている前提では、台帳管理システムの信頼性を担保する観点等から、台帳管理システム間は直接接続することが望ましいのではないか。</p>

### 1.1.2 システムへの負荷<sup>5</sup>

CBDC システムは大量のトランザクションを即時に処理する必要があるため、その検討に当たっては、各システムへの負荷を綿密に分析することが求められる。例えば、送金を行う場合に、保有額上限のあり方次第でオートチャージ・オートスウィングの処理量が変わるため、CBDC システムだけではなく、勘定系システム等への影響が変わりうる。会合では、送金の都度オートチャージ・オートスウィングが発生しない設計や、各システムによる流量制限といった負荷軽減策の必要性に言及があった。このほか、仮に性能面において CBDC システムの処理時間が目標値より長くなる場合、UX の観点からは何らかの工夫が必要と指摘された。

なお、ここでは、CBDC の送金（含むオートチャージ・オートスウィング）にかかる CBDC システムへの負荷、および勘定系システムへの負荷について整理し、払出・受入にかかる勘定系システムへの負荷については第 4 章にて記載する。

（表 1-2）システムへの負荷

CBDC の送金は大量のトランザクションを即時に処理する必要があり、システムへの負荷が大きくなる可能性
CBDC による支払いにおいて、払出と支払いが組み合わされて実行される場合、つまり、支払いに付随してオートチャージが実行される場合を想定すると、これらの処理に関連するシステムには相当な処理スピードが求められる。
トランザクションが集中すると、認証や残高操作の間のシステム制御により、単位時間当たりの処理件数（スループット）が低下していくが、CBDC システムもこの問題から逃れられない。この問題には認証とトランザクションの同期性が関係しているため、認証に用いるトークン（API 等においてユーザーがアクセス権を得るための情報）の有効期間をどの程度とするかも論点になる。
オートスウィングをリアルタイムで行う場合、顧客管理システムが常に保有額上限への抵触状況を監視しなければならないとすると、大きな負荷がかかる。必要な機能とコストのトレードオフを考えていく必要がある。
CBDC 口座には各種制限があると想定されるもとの、店舗等の事業者にはトランザクションが大量に発生する可能性があることを踏まえると、当該事業者に対する取引金額や取引回数の上限への抵触については考慮が必要。

<sup>5</sup> システムへの負荷については、主に WG1 の各会合において議論を実施。

<p>CBDC の保有額上限のあり方次第ではあるが、システムへの負荷を軽減する観点からは、送金の都度、オートチャージ・オートスウィングを行わないことや、CBDC システムや勘定系システムに流量制限の機能が必要</p>
<p>CBDC の保有額上限をどの程度厳格に管理する必要があるかにもよるが、送金の都度、オートチャージ・オートスウィングを行う必要までではないのではないかと。</p>
<p>性能不足が顕在化した際、即時に性能拡張を実施することは難しいと考えられるため、性能不足への事前対応策として流量制限は必須。また、仲介機関の勘定系システム等へのアクセス数を削減する対策も必要であろう。</p>
<p>勘定系システム側でも、CBDC システムへの流量制限に依拠するだけでなく、自衛のために勘定系システムへの流量制御等を行うことが重要。</p>
<p>性能面の目標を実現することが難しい場合には、UI/UX 等での工夫が必要</p>
<p>取引量のピークタイムは事業者の特性やユースケースによって大きく異なる。また、これまでバッチ処理としてまとめて行われていた取引が CBDC では都度行われることで、取引量の増加につながるかもしれない。</p>
<p>CBDC の取引量の予測においては、既成の概念や既存の決済慣行に基づく判断だけでは予期せぬ結果につながるおそれがある。CBDC について、将来の環境変化の可能性を踏まえることは重要な観点だろう。</p>
<p>一般的に「レスポンスが3秒を超えると遅いと感じる」とされるユーザー目線を意識した上で、レスポンスが遅延する場合には、処理の途中でポップアップウィンドウを表示させて処理を中断できるようにするといった工夫を行うことも一案。</p>
<p>送金にかかる応答時間だけを考えれば、送金処理が1つの仲介機関システム内で完結する方が早く処理できるだろう。</p>
<p>CBDC の送金等のために関係するシステムの数が増えれば増えるほど、応答時間等の面でユーザーの利便性低下につながる。</p>

### 1.1.3 仲介機関間のネットワークシステムの整備<sup>6</sup>

仲介機関が複数存在する場合、仲介機関を跨いで CBDC の送金等処理するためには、仲介機関が運営する CBDC システム同士で通信を行う必要がある。この時、各仲

<sup>6</sup> 仲介機関間のネットワークシステムの整備については、主に WG1 と WG7 の各会合において議論を実施。

介機関の CBDC システムを相対で接続する場合、仲介機関の数が増えれば増えるほど、必要な接続数が増加する。こうした点を踏まえると、相対接続ではなく、ネットワークシステムを整備して CBDC システム同士を接続することも考えられる。

会合では、新規にネットワークシステムを構築する場合に<sup>7</sup>、当該ネットワークに各種機能を実装させることで仲介機関の開発負担の低減につながりうるとの指摘があった一方、ネットワークシステムを構築する場合、ネットワークの全面停止時等の対応は考慮事項であり、仲介機関の負担軽減とトレードオフの関係となる点も指摘された。

(表 1-3) 複数の仲介機関を接続するためのネットワークシステムの整備

CBDC システム同士が相互に接続して処理する方式よりも、ネットワークシステムを経由して処理する方式の方がシステム構築の難易度は下がる可能性	
	CBDC システムを構成する各システムが分散されている構成において、複数の仲介機関が複数のパターンで組み合わせることを想定すると、各システムが相互に接続して処理する方式よりも、ネットワークシステムを経由して処理する方式の方がシステム構築の難易度は下がるかもしれない。
1つのネットワークシステムが各種機能を実装することで、仲介機関システムへの負荷は軽減されるなどの利点が考えられる一方、ネットワークシステムの全面停止等による仲介機関を跨った処理が出来なくなる可能性	
	顧客管理システム同士を結ぶネットワークや台帳管理システム同士を結ぶネットワークを1つのネットワークシステムとしてまとめ、それに電文ルーティングのような機能やリトライ処理、タイムアウト処理等を実装すれば、仲介機関が顧客管理システムや台帳管理システムを構築する上での負荷を軽減できるのではないかと。
	ネットワークシステムを設けたとしても取引の総量自体は減らないが、個々の顧客管理システムや台帳管理システムへの負荷は相対的に減少しうるのではないかと考える。なお、高度な仕組みを要する処理をネットワークシステムに負担させることができれば、各仲介機関の構築・運用負担を軽減できるのではないだろうか。
	各仲介機関が独自にシステムを管理・運用する負担を考慮すれば、ネットワークシステムを経由することで通信方法や障害時対応等を統一的なルールで運用しやすくなり、統制等も図りやすくなるのではないだろうか。

<sup>7</sup> 仲介機関間のネットワークシステムの整備方法は、新規にネットワークを構築するほかに、既存のネットワークを活用することも考えられる。既存ネットワークの活用に関する論点は、第4章に記載。

<p>ネットワークシステムを經由して CBDC システム同士を接続する場合、例えば、当該ネットワークシステムが全面停止すると、各システムを跨った処理が出来なくなる点には留意が必要。</p>
<p>1つの顧客管理システムから複数の台帳管理システムに接続することを想定した場合、顧客管理システムにおける接続情報の管理が複雑になる懸念が生じうるが、顧客管理システムと台帳管理システムの間ネットワークシステムを設けることができれば、その懸念は解消されるかもしれない。</p>
<p>ネットワークシステムの設計に当たっては、開発負担の小さい設計が望まれる</p>
<p>CBDC の実現に際して、複数の仲介機関を接続するためのネットワークシステム以外にも、勘定系システムと顧客管理システムを接続するためのネットワークシステムが必要となる可能性があり、その場合には、それぞれのネットワークシステムを集約することで開発負担を小さくできるだろう。</p>
<p>ネットワークシステムやネットワークの設計に際しては、関係者が現実的に負担可能なコストとなるようなものとする必要がある。</p>

#### 1.1.4 強靱性<sup>8</sup>

CBDC は現金と並ぶ決済手段となるため、CBDC システムの強靱性は重要な検討要素となる。例えば、停電や回線障害が発生した時、CBDC システムを構成するシステムのうち一部のシステムが停止したり、CBDC の払出・受入に利用する勘定系システムが停止した場合の対応について考慮が必要となることが指摘され、そのような状況に備えた対応のあり方について議論がされた。

(表 1-4) 強靱性に関する議論

<p>回線障害や電力の瞬断等の場合の対策も考慮する必要</p>
<p>障害対応の観点では、サーバーは冗長化構成とすることや、ネットワークは異なる通信キャリアが提供する回線で複線化することのほか、送電網についても停電による影響を考慮することが必要だろう。</p>

<sup>8</sup> CBDC システムの強靱性については、主に WG1 の各会合において議論を実施。

	<p>通信回線の速度の遅さ等が原因で、システム運営者に取引指図が届かないような事態は問題である。回線障害や電力の瞬断等は全国どこでも発生する可能性があり、こうした場合の対策も考慮する必要があるだろう。</p>
<p>死活監視を継続的に行うことは重要</p>	
	<p>ネットワークやソフトウェア等が正常に稼働しているかどうかの死活監視を継続的に行うことは重要だろう。障害発生時には、社内システムの調査を行いつつ、社外で回線障害等が発生していないかを調査することも重要である。</p>
<p>どの程度のシステム停止を許容しうるか</p>	
	<p>CBDC システムに求められる耐障害性、可用性は、どの程度のシステム停止を許容しうるかと裏腹の関係にあり、これについて議論しても良いのではないか。</p>

### 1.1.5 即時決済性<sup>9</sup>

即時決済性とは、二当事者間における資金の移転がその場で瞬時に行われ完了することをいう。CBDC が現金に近い性質を有するべきと考えれば即時決済性は必要と考えられる。もっとも、市中の既存のキャッシュレス決済の実情を踏まえると、小売店等は、キャッシュレスで支払われた代金の自らの銀行口座への入金について、必ずしも即時入金を求めている訳ではなく、CBDC の即時決済性は小売店等のニーズと合致しない可能性がある点が指摘された。一方で、CBDC の特性である即時決済性を活かせば、小売店等のキャッシュフロー改善に資する可能性も示唆された。

(表 1 - 5) 店舗決済の即時性

<p>CBDC が現金に近い性質を有するべきと考えれば、即時決済性は必要</p>	
	<p>CBDC が現金に近い性質を有するべきと考えれば、資金決済の即時性は必要。資金決済が即時で完了するということは、エラー発生時は即時でエラーが発生したことがわかるということでもある。エラーの発生により資金決済が完了しないトランザクションが発生した場合、処理がエラーで終了していることをユーザー含めて検知・認知できることが肝要である。</p>

<sup>9</sup> 即時決済性については、主に WG1 と WG7 の各会合において議論を実施。

	<p>即時決済性は、既存のキャッシュレス決済手段にはない CBDC の特長であるので、基本的には、支払いの都度、店舗に即座に入金すべきではないか。CBDC に保有上限額を設ける場合、CBDC を受領する機会の多い店舗の CBDC 口座と銀行口座の間では頻繁にオートスウィングが発生し、仲介機関のシステム面の負荷が高まる可能性もある。例えば CBDC の着金は即時に行う一方で、オートスウィングは、1日に1回とすれば、負荷分散も可能と思われる。</p>
<p>既存のキャッシュレス決済の実情を踏まえると、CBDC の即時決済性は小売店等のニーズと合致しない可能性</p>	<p>小売店のようなケースで、少額多頻度の CBDC の受取りシーンを想定した場合、取引の都度、そのすべてを即時に店舗へ入金することは、かえって当該小売店のニーズに沿わないかもしれない。本当にそのようなニーズがあるのかを確認しつつ、性能やコストとのバランスをとる必要がある。</p> <p>小売店等への入金については、業種によっては、即時で処理することが望まれる場合もあるかもしれない。一方、入金可否を決済事業者が判断できるようにするために、入金までに一定の時間を確保すべきケースもある。</p> <p>CBDC では、即時決済であることから、デバイスも含めて顧客と店舗との間で常時同期が取れている状態が望ましいと考えるが、これを現金と同じレベルで実現するのは、現実的ではないと思う。</p>
<p>CBDC の即時決済性を活かせば、小売店等のキャッシュフロー改善に資する可能性</p>	<p>小売店等の視点で CBDC を導入するメリットを考えると、電子マネー等とは違い、CBDC が即時で着金し、すぐに他の支払いのため使用可能となれば、当該小売店等のキャッシュフローの改善につながる可能性がある。</p>

### 1.1.6 事務フロー<sup>10</sup>

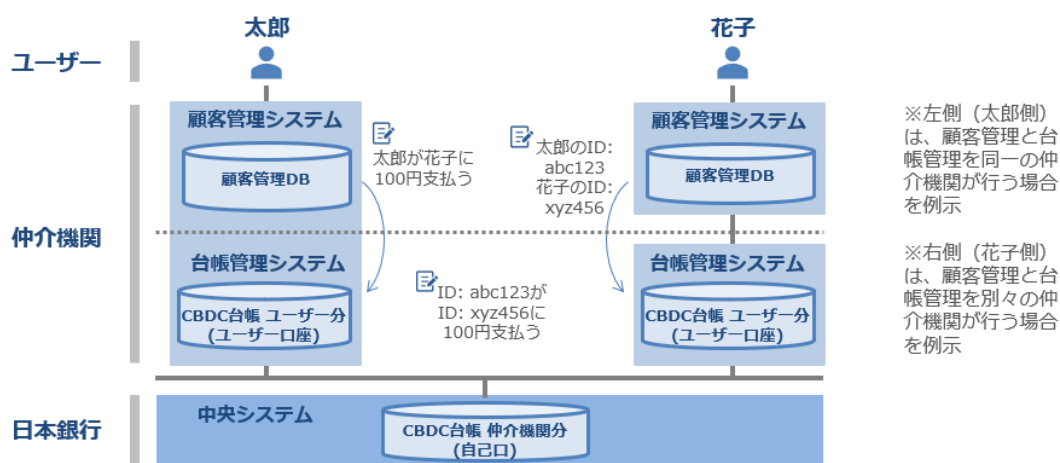
CBDC における払出・受入や送金等の機能を実行するための事務フローの検討に当たっては、CBDC システムを構成するシステム間において各種データの整合性を確保する方法や、エラー・障害発生時の対応等、様々な検討要素が存在する。

<sup>10</sup> 払出・受入や送金等の CBDC の機能を実行する際の一連の処理のうち、エンドユーザーが行う操作を除いたすべての処理の流れ。

## (各種データの整合性を確保する方法)<sup>11</sup>

実験用システムでは、台帳管理の機能の設計パターンについて、相対的により複雑で多くの項目を検証できると考えられる分担管理型を前提としてきた。また、各ユーザーに紐づく顧客管理システムと台帳管理システムは、それぞれ別の主体により管理されうるものとして検討を進めてきた。こうした前提のもとでは、システム間で各種データの整合性を確保する方法が重要な論点と考えられる。この点、新しい技術で整合性を確保する可能性についても議論がなされたが、同時に性能面の懸念も示されている。また、中央集権的な主体であるオーケストレーター<sup>12</sup>を設置する考え方（オーケストレーション）について、実験用システムの構成とは異なり、単一障害点となるリスクも存在するものの、各種データの整合性確保を図る上では有用との指摘もあった。

(図 1-2) 実験用システムの概略



(表 1-6) システム間のデータ整合性についての論点

各システム間でデータの整合性が確保できなかった場合、不整合となった原因の究明が課題

中央銀行は CBDC の発行総量を何らかの形で把握すると想定するが、これは各台帳管理システムの CBDC 残高の合算値と一致するはずである。仮に、不一致となった場合、不一致となった原因の究明が課題となりうる。

<sup>11</sup> システム間の整合性については、主に WG7 の各会合において議論を実施。

<sup>12</sup> 複数のシステムに対して中央で一括して指示を出し、全体の動作を制御・管理する主体。

CBDC システムをそれぞれ異なる主体が管理する場合、新しい技術でそれぞれのシステム間の整合性を確保できるかもしれないが、性能面の懸念もある	
	分散的なシステム構成においては、新しい技術で整合性が確保できるかもしれないが、大量のトランザクションを処理することを考えると性能面の懸念があるだろう。
	当行はフロントシステムおよび勘定系システムの両方を行内で管理しており、各システム間でリアルタイムに履歴の同期を行っている。この実務に照らせば、顧客管理システムと台帳管理システムでもリアルタイムに履歴の同期を行う必要があるかもしれない。顧客管理システムと台帳管理システムを別の仲介機関で管理する場合、顧客管理システムが認識する状態を台帳管理システムでは認識しない可能性があり、複数取引の同時発生時等に、どこまでリアルタイムに整合性を確保できるかが論点となりうる。
オーケストレーションの考え方は単一障害点の論点があるものの、データの整合性を図る上では有用	
	オーケストレーションの考え方によるシステム設計は事例があり理解しやすいが、オーケストレーターとなるシステムへの依存度が高く、単一障害点となりうることは論点となるだろう。
	障害発生時、特に処理が途中の取引の有無の調査や解析を想定すると、オーケストレーションの考え方が優位かもしれない。

### (エラーや障害発生時の対応)<sup>13</sup>

平時においては正常に機能する事務フローであっても、例えば、店舗決済の処理中に CBDC システムに障害が発生した場合、二重取引<sup>14</sup>や処理電文の滞留等のエラーが発生するようなケースが想定される。そのため、エラー発生時のユーザーへの影響を軽減する方法や、エラー対応の工夫等についての検討が必要となる。

会合では、銀行間送金等の既存の決済サービスにおけるエラーや障害発生時の対応例が紹介された。その上で、これを CBDC システムに置き換えた場合の論点として、分担管理型を前提に、各ユーザーに紐付く顧客管理システムと台帳管理システムは、

<sup>13</sup> エラー対応については、主に WG 1 および WG 7 の各会合において議論を実施。

<sup>14</sup> 例えば、店舗決済時に CBDC システムに障害が発生し、各台帳での処理は完了しているがその応答がユーザーに届かなかつた場合に、ユーザーは決済が失敗したと判断し再度支払いを行ってしまうようなケースを想定。

それぞれ別の主体により管理されうるとすると、対応難易度が高くなると想定されることや、エラーが発生しないような仕組み作りの重要性、障害時の UX（リクエスト制御やエラー応答）の設計の重要性等が指摘された。

（表 1 - 7）銀行間送金<sup>15</sup>等におけるエラー対応の例

口座引き落とし処理完了前であれば取引中断、完了後であれば前進処理を行う	
	電文途絶等のエラー発生のタイミングが、仕向銀行の勘定系システムによる口座引き落とし処理完了前であれば取引中断となり、完了後であれば障害対応を行い前進処理する流れとなる。
	仕向銀行勘定系システムと全銀システム間で障害対応が必要になった場合は、仕向銀行と全銀ネットで、データの授受をどのようにして行うか議論し対応する。
	仕向銀行でエラーを検知しても被仕向銀行にデータが到達している場合もあるため、エラー発生時は基本的にまず仕向銀行が被仕向銀行に電文が到達したか否か確認し、到達していない場合は全銀ネットと協議するといった流れで対応を検討する。
	全銀システムと被仕向銀行勘定系システム間で障害が起きた場合の異例時対応として、組み戻しの電文自体は被仕向銀行から自動で発出されるが、電文に組み込まれた組み戻し理由等のコードの内容を目視で確認の上で、事務処理を行う。
接続する外部接続サービス毎にエラー発生時の処理は異なっている	
	銀行勘定系システムと既存の外部サービスとの接続事例において、外部サービス毎にエラー発生時の処理は異なっている認識である。そのため、CBDC についてはどのような方式でエラー処理を行うのが良いのかという点も検討要素ではないか。
取引履歴を用いて各種制限の判定を行うと処理が重くなる可能性がある	
	銀行間送金では、フロントシステムで取引履歴は持たず、各種制限値を管理している。この実態を踏まえると、取引履歴を用いて各種制限の判定を行うと処理が重くなる可能性があるため、顧客管理システムは取引履歴そのものを用いて判定を行うので

<sup>15</sup> 平時における銀行間送金の流れを概略すると、仕向銀行フロントシステム→仕向銀行勘定系システム→全銀システム→被仕向銀行勘定系システム→被仕向銀行フロントシステムというフローで処理が行われている。

	はなく、各種制限値等とそれを管理するための元帳を設けて、各種制限値等に抵触するか否かのみ管理することが望ましいかもしれない。
CPM においては、POS 側で不成功の場合は自動で取消しとなる機能が実装可能	
	CPM においては、ネットワーク障害発生時に、ユーザーのアプリで処理が完了していても POS 側で不成功の場合は自動で取消しとなる機能が実装可能である。店舗オペレーション負荷軽減の観点で、このような機能も参考になるかもしれない。

(表 1-8) エラー対応についての論点

異なる主体に管理されたシステムの場合、障害時の対応難易度が高い	
	実験用システムでは顧客管理システムと台帳管理システムが4つのシステムで構成されているため、障害時の対応やユーザーから見た際の処理時間に課題が生じうる。
	取引電文がシステム間で途絶した場合等の対応は悩ましい。各システムが取引をどのように追跡して不整合を認識し、どのように正しい状態にするのかを考えた場合、取引成立照会のような機能を設けての対応等が考えられる。
二重取引等発生時の対応を可及的に減少させるために、エラーが発生しないような仕組み作りが重要である	
	二重取引が発生すると事後的な調査・対応が必要となるので、二重取引が発生しないような仕組み作りが重要となる。
	既存の銀行システムにおいては、何重にも事前にチェックがかかる仕組みを取り入れることで、勘定系システム内の元帳を修正するケースを防止している。このような背景も鑑みれば、減額留保・増額留保といった制御を取り入れて、台帳更新をする前段階で可能な限りリスクを低減させることは重要だろう。
障害時の UX (リクエスト制御やエラー応答) を適切に設計すべき	
	キューイングの仕組みを利用した場合、障害発生時にリクエストが蓄積し、障害解消後もリクエストの解消までは相当の時間がかかる可能性があるため、アプリからの残高照会は一定時間経過しなければ不可とするような設計も検討の余地があるだろう。
	エラー応答の実装は接続先任せにすべきではない。更新系 API のエラー実装を接続先事業者に委ねた結果、ユーザーに対してエラーの事実のみ応答し理由は表示されない仕様とされ、ユーザーは繰り返し実行処理を行い処理量が増加した事例があった。
	各システム間でデータの通信が発生する度に履歴が残るようにすることで、障害発生時等にどのタイミングまでデータが正しかったかがわかるかもしれない。

## （反対取引）<sup>16</sup>

クレジットカード決済の場合、誤った取引については、カードセンターでオーソリゼーションの許可処理後であっても、「取消し」処理を行うことが出来る。他方、CBDC 送金の場合、実験用システムにおける送金処理フローでは、送金元ユーザーの送金指示をもとに送金先ユーザーの台帳が増額記帳されると、決済完了となるため「取消し」処理は適さず、「反対取引」としての処理が望ましいとの意見が挙げられた。

（表 1-9）反対取引についての論点

CBDC 送金の場合には「取消し」処理は適さず、「反対取引」処理が必要
クレジットカードの場合と異なり、CBDC 送金の場合には、送金先の台帳管理システムの増額により決済完了となり、残高がすぐに利用されるリスクが存在するため「取消し」処理は適さず、「反対取引」処理が必要になるだろう。
増額された残高が使用されていなければ、反対取引を自動で行うことは可能かと推察するが、銀行間送金の組み戻しのような、戻す場合もあれば戻さない場合もある現在の業務運用から想像すると、反対取引の自動実行は難易度が高いのではないか。
反対取引を行った場合、それが取引履歴に残ることは大きな問題ではないだろう。

## （既存の金融実務との関係<sup>17</sup>）

CBDC を社会実装する場合、CBDC と既存の金融実務との関係も検討要素となり、主に既存の銀行預金を例に、両者の関係を整理すべきとの指摘がなされた。

（表 1-10）既存の金融実務との関係

既存の金融実務との関係を整理する必要
預金口座においては、取引禁止の処置がなされている場合は決済させないという制御を行うことがある。このような制御を CBDC でも行うのであれば、そのための仕組みが必要となる。

<sup>16</sup> 反対取引については、主に WG 7 の各会合において議論を実施。

<sup>17</sup> 既存の金融実務との関係については、主に WG 1 の各会合において議論を実施。

預金口座における死亡届や口座凍結等に関する運用を、CBDC ではどのようにするかも検討要素となる。
多額の現金を銀行預金から引き出す際は ATM を利用できず別途確認が必要となるのと同様に、CBDC の払出の際も、条件によっては何らかの確認が必要となることも想定される。もっとも、その際も、デジタルの特性を活かした迅速な確認が可能となれば利便性向上につながるかもしれない。

### 1.1.7 データモデル/データベース技術<sup>18</sup>

#### (データモデル)

CBDC の台帳システムのデータモデルに関し、ビットコイン等で採用される UTXO<sup>19</sup> モデルといった、伝統的な口座残高型とは異なるタイプの活用可能性を議論した。

UTXO モデルの特徴として、並列処理性やプライバシー確保の実装容易性が挙げられるものの、想定されるシステム構成や処理フローによって特徴が変わりうると指摘された。特に、同一口座へのトランザクション集中に対する性能面への影響については、送金実行前の各種上限判定処理が前提となると、トークンの集計処理の必要から、UTXO が持つ並列処理性は制限され、データモデル間の差異がなくなる可能性がある。また、口座残高型であっても、レコードを分割するなど、処理の粒度を最適化することで性能改善が見込まれる点も指摘された。

#### (表 1 -11) データモデルに関する議論

UTXO モデルの特徴は、システム構成や処理フローによって変わりうる
UTXO モデルの特徴は、並列処理の容易さとプライバシー確保の容易さ。

<sup>18</sup> データモデル/データベース技術については、主に WG4 の第 1～6 回および第 1 2 回会合において議論を実施。より将来的なコンセプトにたった関連議論は論点 5 にも記述。

<sup>19</sup> Unspent Transaction Output (未使用トランザクションアウトプット) の略。同モデルの確定的な定義はないものの、一般的には、残高を増減させることで記録を行う口座残高型とは異なり、取引の結果を、取引単位でそのまま記録するトークン型データモデルの一つとされる。同モデルでは、取引が行われると、消費されるインプットと紐づけられる形で新しいアウトプットが生成され、未使用のトランザクションアウトプットとして、将来の取引でインプットとして消費できる状態で記録される。

<p>基本的には、口座残高型はアカウントに直接紐付く形で残高が管理されるため匿名性が持ちづらい。一方、UTXO 型の場合にはまずアセットがあり、それが誰に帰属するかという処理の仕方であることから、アカウントから管理を切り離しやすく匿名性を持ちやすい傾向がある。</p>
<p>口座残高型、トークン型、UTXO 型の3つのデータモデルについて、それぞれの長所・短所は、台帳管理のあり方が集中か分散かなどによって変わりうる。</p>
<p>UTXO には並列処理しやすい傾向があるものの、粒度が細かすぎると残高計算のオーバーヘッド（間接的に必要となる計算量）が高くなる可能性。</p>
<p>同一口座へのトランザクション集中に対する性能劣化は、処理の粒度を最適化する方向で対応でき、口座残高型であっても工夫次第で対応可能</p>
<p>トランザクション集中とそれに伴う性能劣化をどの程度回避できるかは、データモデルというより、UTXO 型ならトークンの粒度の細かさ、口座残高型ならレコード分割の程度に依存するため、トランザクションの処理の粒度を適切に設計することで最適化できる可能性。</p>
<p>送金実行前の各種制限判定を想定すると、ユーザー単位でのトークンの集計処理が必要となるため UTXO が持つ並列処理性は制限され、データモデル間で性能面に大きな差異は生じないかもしれない。</p>
<p>口座残高型であっても、レコードを分割したり、データを追記していくなどの工夫を施すことで、並列処理性を高めることはできる。</p>

## （データベース技術）

CBDC の台帳システムのデータベース技術に関し、NoSQL/NewSQL といった新たな分散データベース技術や、ブロックチェーン技術の活用可能性を議論した。

会合では、高速処理や高スケーラビリティが期待される NoSQL や NewSQL の活用可能性が指摘される一方で、最新の技術ほど学習コストや運用管理面に課題がある点が指摘された。パブリックブロックチェーンの活用に関しては、スケーラビリティやガバナンス・プライバシーといった点が、現時点では大きな課題であるものの、今後の技術革新次第で評価は変わりうる可能性が指摘された。このほか、CBDC システムの性能を大きく落とさず、二重払いや改ざん防止といったセキュリティ耐性を強化できる可能性があるアーキテクチャーとして、取引履歴のみパーミッションドブロックチェーンを活用し、残高情報管理は通常のデータベースで行う、ハイブリッドなアプロ

一ちも提案された（なお、このほかのブロックチェーン関連技術の議論詳細は、後述の論点 5 も参照。）

（表 1 -12）データベース技術に関する議論

<p>大規模データ処理に対応する形で、水平拡張性が高い分散データベース技術が進展</p>
<p>SQL で複雑なクエリ（命令）を実行する伝統的なリレーショナルデータベースは、データベースの整合性と信頼性を高いレベルで担保するが、水平拡張には適していなかった。こうしたリレーショナルデータベースの持つ課題に対応する形で、大規模なデータ群の高速処理を可能とするために、NoSQL や NewSQL が誕生している。</p>
<p>NoSQL のキーバリューストア型やカラムストア型の場合、シンプルなデータ構造のため、高い処理性能が期待されるが、複雑なクエリやデータの関係性の表現は不向き。</p>
<p>NewSQL は、水平拡張をコンセンサスアルゴリズムで実現することで、リレーショナルデータベースの利点（水平拡張した状態でも整合性&lt;ACID 特性&gt;が確保しやすいことなど）を保持しながら高いスケーラビリティを備えているが、現時点では新しい技術ゆえに学習コストや運用管理面に課題がある。</p>
<p>ブロックチェーンの活用は今後の技術革新次第ながら、適した処理への部分利用等ハイブリッドなアーキテクチャーも一案</p>
<p>思考実験としてパブリックブロックチェーン上に CBDC が発行される世界を考えると、現時点では、スケーラビリティやガバナンス・プライバシーといった点が大きな課題であるが、今後の技術革新次第（例えば Layer2 技術やゼロ知識証明<sup>20</sup>等）で、評価は変化する可能性。</p>
<p>ブロックチェーンの性能改善策としては、合意形成に参加するノードを絞ったり、一部処理をバッチ化する別のチェーン（レイヤー 2）の作成がある。また、それ以外では、高性能と言われるインメモリデータベースや NoSQL/NewSQL といった新たなデータベース技術の活用がある。</p>
<p>取引履歴のみパーミッションドブロックチェーンを活用し、残高情報管理は通常のデータベースで行うハイブリッドなアーキテクチャーとすることで、性能を大きく落とさず、二重払いや改ざん防止といったセキュリティ耐性を強化できる可能性。</p>

<sup>20</sup> ゼロ知識証明とは、ある人が自分の主張が真であることを、それ以外の知識を明かさずに証明する（検証者に確信させる）手法。

既存のサービスの中では、中央集権的に進めた方が効率的なものの方が多い。分散化すべきところとそうでないところの使い分けが重要。

## 1.2 エンドポイントデバイスとユニバーサルアクセス（主にフロントエンド）<sup>21</sup>

### 1.2.1 デバイスの種類

#### （個人のユーザーデバイス）

スマートフォンの所持、IT リテラシー、年齢、ハンディキャップの有無等によらず、誰でも CBDC を使うことができるようにするための設計について、主に個人のユーザーデバイスの観点から議論した。

会合では、個人のユーザーデバイスについては、機能面で優位なスマートフォンを主としつつ、子供などスマートフォンを保有しない幅広いユーザー層を考慮してカード型デバイスを併用することが望ましいとの意見が挙げられた。

他方、デバイスの利用自体が困難なユーザーに配慮して、生体認証等を用いたデバイスレス決済の活用可能性についても検討を行った。

スマートフォンについては、ハードウェアや OS 事業者によって、セキュリティ確保方式が一律でないことやスクリーンリーダー等のアクセシビリティ機能の仕様が区々である点が留意点として指摘された。

（表 1-13）個人のユーザーデバイス

個人のユーザーデバイスは、スマートフォンを主としながらも、子供などスマートフォンを保有しない幅広いユーザー層を考慮してカード型デバイスを併用するのが良いのではないかと

機能面で優位なスマートフォンを主としながら、子供など幅広いユーザー層を考慮してカード型デバイスを併用することが良いのではないかと。

<sup>21</sup> エンドポイントデバイスとユニバーサルアクセスについては、主に WG5 において議論を実施。

	<p>あらゆる世代の人々や現金しか利用できていない人々でも利用できることが CBDC の意義の一つだとすれば、マイナンバーカードを含めて幅広い媒体を用意する必要があるだろう。</p>
<p>現在、利用シーンが徐々に拡大しつつある、生体認証等を用いたデバイスレス決済の検討も、ユニバーサルアクセスの観点では重要</p>	
	<p>最近ではユニバーサルアクセスの観点からカード等のデバイスをかざす操作が難しい車椅子利用者のためにデバイスレスの顔認証決済を導入するケースも出てきている。</p>
	<p>デバイスを必ずしも必要としない決済手段は、ユニバーサルアクセスはもちろん、特に災害時におけるレジリエンスの観点で重要であって、また、省力化が社会課題として求められていく中でも有用なアプローチとも思われる。</p>
	<p>地域 Pay 顔認証決済の実証実験では、集会所を借りて事前登録のワークショップを行い、事前登録を支援した。一度、登録してもらえれば、利便性の向上を実感してもらえるようだが、登録に対するハードルはまだ高いと認識している。</p>
	<p>認証精度と CBDC のユーザー数を考えると、現状の技術では、一種類の生体認証だけ、あるいは生体認証だけでは安定的な認証の運用が実現できないと考える。そのため、複数の生体認証方式（虹彩認証、指紋認証、手のひら静脈認証等）を組み合わせたり、生体認証とそれ以外の認証方式（デバイスレスとする場合、知識認証が想定される）を組み合わせたりすることで、認証精度を担保していく方法が適当だろう。</p>
<p>スマートフォンのセキュアエレメントの活用は特に日本で進展しているが、一部のスマートフォンにはセキュアエレメントが実装されていないことには留意する必要</p>	
	<p>様々な課題はあるものの、官民の努力によりセキュアエレメントの活用もある程度進展している点には注目している。</p>
	<p>ユニバーサルアクセスの定義次第だが、セキュアエレメントが搭載されたスマートフォンを所有していないユーザーがいることを考慮すると、スマートカードのようなカード型デバイスの必要性が高まるのではないかと考える。</p>
<p>スクリーンリーダー等のアクセシビリティ機能に関する仕様が OS によって異なる</p>	
	<p>UI/UX を重視してアプリを開発すると、OS 事業者の仕様に沿うことが難しい場合があり、そのために、OS のスクリーンリーダー機能を利用した際に、正しい順番で読み上げがされない事象が発生することがある。</p>

## (店舗決済端末)

CBDC を用いた店舗決済において、例えば、これまでキャッシュレス決済を利用したことのない店舗も含めて、個人のユーザー側と店舗側のデバイスをどのように組み合わせ設計にするかについて議論した。

会合では、QR コード（静的 MPM 方式）やスマートフォン等の決済端末化の活用は、これからキャッシュレス決済を導入する小規模店舗にとってはコストを抑えられるといった利点があるとの声があった。一方で、既にキャッシュレス決済を導入している店舗においては、特に日本の決済サービスは多様化が進んでおり、CBDC 決済が加わることによって店舗端末操作や UI が複雑化しやすいため、CBDC 決済で用いるインターフェースは、追加対応する範囲を前広に明示していくことが望ましいとの議論があった。また、ユニバーサルアクセスの観点では、将来のデバイスやインターフェースの多様化を見据えて、バックエンドは普遍的かつフロントエンドの拡張に柔軟に対応可能な仕組みの検討が重要といった議論がされた。

(表 1-14) 店舗決済端末

店舗側のキャッシュレス決済導入ハードルを下げる手段としては、静的 MPM やスマートフォン等の決済端末化が有効
静的 MPM 方式の利点は、QR コードを表示したポップアップを置くだけで設置が完了するために、圧倒的な低コストで提供できる点にある。
スマートフォン等を決済端末として利用する場合、決済端末導入コストが抑えられる可能性があり、例えば、これまで電子マネー等を導入したいが諦めていたような店舗に対しては有用と思われる。
多様な個人のユーザーデバイスに対応することを見据えると、既存の店舗決済への影響や、バックエンドも含めた全体設計への考慮が重要
CBDC においても 1つのオペレーションで、店舗決済端末側が様々なデバイスを一度に自動判別して処理できるようにしてほしいという店舗側のニーズが出てくるのが想定される。その際、カメラや NFC アンテナの配置といったハードウェア面が制約となって、既存の店舗決済端末やインフラでは実現が難しくなることもありうるだろう。
CBDC 決済が可能なカード型デバイスの種類が増えていく場合は、非接触技術の規格の違いに店舗決済端末の読み取り機能がどのように対応していくかを考えていくこと

<p>になる。まずは、対応範囲をあらかじめ見定めた上で、既存のデバイスの活用を検討していくべき。</p>
<p>デバイスの検討に関して、UI と裏方の決済の仕組みは切り分けて議論を進めていくべきだと考える。今後、新しいインターフェースや決済サービス仕様がでてきても、裏方の仕組みが同じものであれば、端末対応も含めて店舗側も対応しやすくなるのではないだろうか。逆に、新しい決済サービスが出てくる度に、仕組みも新しくなるというのであれば、上手いかわからないと思う。</p>
<p>あらゆる媒体に対応するのであれば、バリューの管理はセンターサーバで行う形になるのではないか。</p>

## 1.2.2 UI/UX

### (UI/UX ガイドライン)

会合では、利便性に関する機能は民間事業者のイノベーション領域であることを前提として、CBDC 決済の UI/UX を検討する上での、日本銀行と民間事業者との役割分担や協業体制に関する議論がされた。例えば、詳細な設定は民間事業者側に委ねつつも、CBDC のイメージの統一化や、決済サービス事業者や端末ベンダーの開発環境のためには、UI/UX ガイドラインがあった方が良好だろうとの意見があった。また、技術面においては、オープンスキーム<sup>22</sup>とすることが、各種の対応負荷の観点でも重要であるとの意見も聞かれた。

(表 1-15) UI/UX ガイドライン

<p>民間事業者の開発環境としても、UI/UX ガイドラインの提示は有用</p>
<p>CBDC 決済の UI/UX を検討する上で、民間事業者と日本銀行との役割分担や協業体制の継続的な議論が不可欠。UI 部分を民間事業者が担う場合に、CBDC のイメージをどのように設定し維持していくかも併せて考えていく必要がある。</p>
<p>他の決済サービスの事例では、事務局から UI/UX ガイドラインが提示され、画面等の大まかな見え方やロゴの使い方等を示された上で、詳細はスマートフォンアプリを提</p>

<sup>22</sup> 共通のルールや技術仕様を公開・共有することで、特定の企業や技術に依存せず、誰でも自由に参加・連携できる仕組み。

<p>供する各社に委ねられるという方式であった。この経験を踏まえると、大枠を定めたガイドラインがあった方が各社は対応しやすいかもしれない。</p>
<p>CBDC においては、決済サービス事業者や端末開発ベンダーが自身でより良いサービスや機能を開発しやすい環境にするためにも、その前提となる CBDC に求められる UI/UX に関するガイドラインや共通仕様を定めることが有効だろう。</p>
<p>デバイスに限らない話だが、極力オープンスキームとすることで、競争が発生し、結果的に、割安な仕組みが出来上がっていくと考える。</p>

### (デバイスの UI/UX とセキュリティ)

利便性のある程度犠牲にしてでも安全性を優先すべきとの意見がある一方で、デバイスの当人認証機能を厳格にしすぎると、カード型デバイス等、一部のデバイスの検討・活用が難しくなると考えられる。こうした下で、ユニバーサルアクセスの観点からは基本的に幅広いデバイスが対象となるよう検討する必要があると考えられる。例えば、デバイス毎のセキュリティ水準や当人認証の有無に応じた取引上限額を設定してリスクを低減するといった、利便性との両立を図るアプローチが議論された。

スマートフォンについては、高度な当人認証機能によって利便性とセキュリティの両立が可能だが、スマートフォンの機種変更時や、PC 等の他端末でのアクセスにおいては IT リテラシーに応じたユーザーサポートが必要であり、特に高齢者や身体が不自由な方々が利用する際に大きなハードルとなりうるとの意見があった。

(表 1-16) デバイスの UI/UX とセキュリティ

<p>セキュリティと UI/UX のバランスが重要</p>
<p>CBDC の場合は利便性のある程度犠牲にしてでも安全性を優先することが求められるのではないかと。他方、セキュリティを厳格にしすぎると、カード型デバイス等の検討・活用が難しくなり、利便性を損なうおそれもある。こうした点を踏まえつつ、セキュリティと利便性のバランスをどのようにとることが重要なポイントであり、例えば、取引金額に制限を設けることで一定のリスクに抑えつつ、利便性との両立を図るアプローチも対応策の一つではないかと。</p>
<p>幅広い媒体が対象となるよう対応する必要があるだろうとの想定のもと、決済利用時の上限額については、媒体毎のセキュリティ水準や当人認証の有無に応じて個別に検討する必要がある。</p>

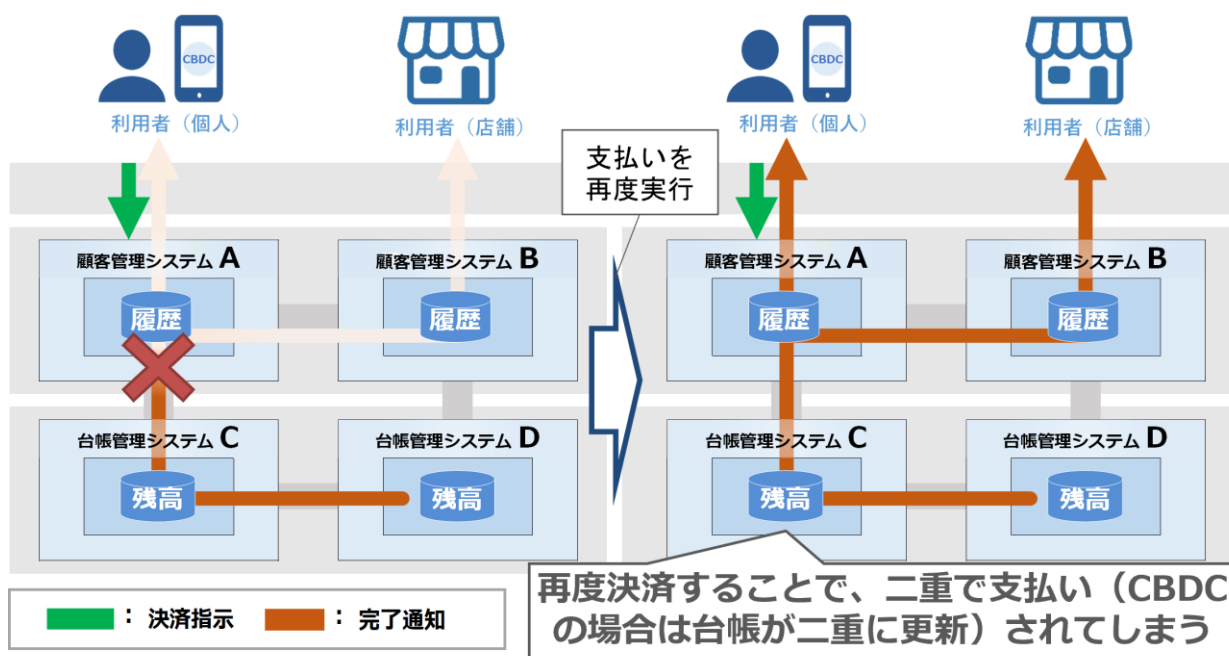
パスキー認証のようなセキュリティと UX が整っている技術を見極め、採用していくことが重要。

高度な本人認証への切り替えにより、セキュリティ機能の高度化が図れる一方で、スマートフォンの機種変更時や、PC 等の他端末でログインを試みる場面において、ユーザーの負担が増えている点は課題である。こうした点も含め、特に高齢者や身体が不自由な方々が利用する際に大きなハードルとなりうるため、簡易な UI をどう提供するかは検討事項である。

### 1.2.3 顧客管理・台帳管理システム間の同期

決済取引においては、デバイス上で送金実行を指示した後、決済が完了した際に、支払人と受取人の残高認識が一致する必要があるが、通信の不具合や障害の発生等の際には、CBDC の顧客管理システムと台帳管理システムの間で同期が適切に行われず、決済結果の不整合が生じたり、ユーザーが台帳の更新状況（決済が正常に完了したか否か）を正確に把握できない可能性がある。

(図 1-3) WG 5 第 10 回会合 事務局説明資料より抜粋



会合では、処理結果が不整合となった時のリカバリー策としてタイムアウト設定の有効性が挙げられるとともに、ユニークな取引 ID の活用によるデバイス起点の迅速なタイムアウト処理や二重支払防止等、民間事業者の決済サービスの仕組みが紹介された。あわせて、そのような状況下において、適切にユーザーに状況を伝えていくといった観点では、決済に用いるデバイスやインターフェース等の違いを考慮した設計や、不整合が発生した場合においても、民間事業者が柔軟に運用可能な仕組み作りの重要性が指摘された。

(表 1-17) 同期

処理結果の不整合や二重支払等への対策は、民間事業者の決済サービスで講じられている対応が参考になる可能性	
	事務局説明資料で紹介されたタイムアウト設定は、既存の民間事業者キャッシュレス決済手段と同じように、支払人と受取人の処理結果が整合しない場合のリカバリーに有効だろう。
	CBDC 送金においてタイムアウト設定は必要と考えられるところ、民間事業者のキャッシュレス決済手段で導入しているユニークな取引 ID 等を用いた二重支払対策も併せて検討すべき。
	既存の CPM におけるエラー処理のシーケンスでは、ネットワーク障害が発生した際に、ユーザーのアプリで処理が完了しても POS 側では成功してないと自動で取消しとなるアクションが実装可能となっている。CBDC におけるファイナリティがどのように実現されるか次第だが、店舗オペレーション負荷軽減の観点からは、こういった CPM の機能も参考にすべきではないか。
	クレジットカードにおいては、不正利用防止だけでなく、通信障害等の異常系対応も含めたオーソリゼーションの仕組みが確立されている。海外のインスタントペイメントでは、Request to pay をオーソリゼーションの代わりに用いる検討がされているように、安全面を考慮すると、決済を実行する前にオーソリゼーションのような仕組みを実施すべきという動きが出てくる可能性もある。
ユーザーへの伝達方法は、デバイスやインターフェース等の違いも考慮した設計が重要	
	UX の観点では、コード決済とタッチ決済では、ユーザー側の認識に違いがあることに留意が必要だろう。ネットワーク障害等があった場合の処理状況について、コード決済では、ユーザーが自身のスマートフォンを用いて操作を行うことから、自身のスマートフォンで確認できるが、タッチ決済では、自身のスマートフォンでは確認でき

ず、店舗の POS 側でしか確認できないことになる。店舗決済における障害時の UX は、システムとオペレーションを複合した検討が必要となってくる。

ユーザーへの伝達の観点では、決済未了・完了に関わらず、ユーザーと店舗との認識が一致することが重要。例えば、ユーザーのスマートフォンは決済完了、POS 側は未了といった不一致は、返品判断も含めて店舗としては大変困る状況であり、カード型デバイスのクレジットカードや電子マネーでは、POS 側の処理結果や残高照会表示を確認する仕組みとなっている。

決済時に顧客と店舗間で不整合が起これば、両者の間でトラブルに発展する可能性。CBDC は、即時に決済されるため、デバイスも含めて顧客と店舗との間で常時同期が取れている状態が望ましいと考えるが、これを現金での対面支払いと同じレベルで実現するのは、現実的ではないと思う。不整合が発生した場合であっても、民間事業者が適切なリスク管理の下でビジネス的な判断が行えるような弾力性を持った運用が可能な仕組みを考えることが望ましい。

## 2. CBDC のユーザーを支えるシステム

### 【第2章の概要】

CBDC を安心・安全な決済サービスにするためには、ユーザーの口座開設時の身元確認や継続的顧客管理としての顧客情報の更新、取引モニタリング等による不正取引の検知・防止等によって、ユーザー基盤を健全に維持していくことが重要である。本章では、既存の決済サービスを参考に、CBDC におけるユーザーアクション（図2-1）を想定しつつ、KYC、AML/CFT、認証・認可に関する留意点や課題等を中心にCBDC のユーザーを支えるシステムに関する論点を整理する。

身元確認のあり方については、個人の場合は、なりすまし等の不正利用への対策や、セキュリティと利便性のバランスが議論された。また、非対面手続きに不慣れな人のためには、対面等での対応が求められるが、こうしたもとでも仲介機関としてビジネスが成り立つようなインセンティブ設計の必要性等が指摘された。法人の場合は、個人より厳格な手続きが求められていることを踏まえ、デジタル技術の活用による手続きの効率化等が議論された。

継続的顧客管理の現状と課題については、金融機関や資金移動業における対応コストや人的リソース面等の負担が課題とされた一方で、ATM やアプリにおける顧客接点を活用した効率的な管理方法の検討・導入が進んでいることが紹介された。

不正検知の現状と課題については、多様化する不正取引の手口により、セキュリティ強化だけでは対応が難しい中で、デジタル技術の活用による不正取引の防止や、不審な取引の情報を関係者間で交換可能な仕組みの必要性について意見が挙がった。

KYC や AML/CFT の水準については、CBDC が提供する機能に応じて変わりうるということが指摘された。また、身元確認の実施状況に応じて CBDC の機能の提供範囲を変更可能とすることで一定のユニバーサルアクセスを確保する方法や、犯罪被害防止の観点からリスクの高い機能に制限を設ける必要性等も議論された。

KYC と AML/CFT 対応の共同化については、共同センターやコンソーシアムによる業界横断的な取組みの可能性について議論された一方で、共同化に伴う責任の所在や運営主体等の整理すべき課題が指摘された。また、口座開設の可否等の判断基準については、政府等の公的機関や業界団体がベースとなる基準を定めた上で、各仲介機関が実態に応じてプラス  $\alpha$  で審査基準等を設けることが望ましいとの意見が示された。

認証・認可における標準のあり方と最新動向については、多くの仲介機関や追加サービス事業者の参加が見込まれる CBDC において、各企業が個別で認証・認可方式を構築すると、全体として多大な労力やコストの発生と、脆弱性に個別対応することの負荷が高まる可能性があるため、標準化された認証・認可方式の採用を検討すべきとの議論がなされた。標準化の検討に当たっては、ユースケースやそのリスクを整理した上で、国内外の標準規格やガイドラインを活用することが望ましく、それらを適切に実装・運用することが求められるとされた。また、最新動向として高いセキュリティ要件を満たす FAPI (Financial-grade API) への準拠を進めている海外事例等が紹介された。

リスクを踏まえた対応のあり方については、ユーザーが安心して CBDC を利用するには、関係者間でリスクの所在や責任分界点、コスト負担等を取り決めることが必要との意見が挙がった。CBDC のユースケース毎にリスク評価を実施した上で、利便性とのバランスやコストを考慮にいて、適切な本人認証の強度を確保することが重要と言及された。その上で、低リスクのユースケースにおける、本人認証の簡略化可能性についても議論された。

(図 2 - 1) 既存の決済サービスおよび CBDC のユーザーアクションの一例<sup>23</sup>



<sup>23</sup> WG3 第 1 回会合資料 ([https://www.boj.or.jp/paym/digital/d\\_forum/dfo231025a.pdf](https://www.boj.or.jp/paym/digital/d_forum/dfo231025a.pdf)) より引用。

## 2.1 KYC と AML/CFT<sup>24</sup>

### (身元確認のあり方)

CBDC を利用するユーザーの身元確認は、安心・安全な決済サービスを実現するための重要な役割を担い、セキュリティと利便性の両立が求められる。

個人における身元確認については、犯罪による収益の移転防止に関する法律（以下、「犯収法」という）等における非対面本人確認方法（eKYC）の原則公的個人認証<sup>25</sup>への一本化および対面本人確認方法の IC チップ読取りの義務化を目指す政府方針<sup>26</sup>を踏まえつつ、CBDC の個人口座開設においては公的個人認証を活用するほか、なりすまし等の不正利用防止の観点から、公的個人認証に容貌撮影を組み合わせるなど、不正利用の実態を踏まえた追加的な対策が必要ではないかとの言及があった。他方、こうした追加的な不正利用対策を講じる場合、リスクの高いサービスに限定するなど、セキュリティと利便性のバランスに配慮が必要との指摘もなされた。さらに、非対面での手続きに不慣れな人や高齢者等のために対面等での対応が求められるが、こうしたもとでは CBDC の取扱いが仲介機関のビジネスとして成り立つようなインセンティブ設計の必要性に関する議論が行われた。

法人における身元確認について、法人口座は、事業性決済を装うことで多額の資金を移転しやすいといった特徴から悪用された際の影響が大きく、個人口座と比べ、より厳格な手続きが求められている。こうした法人口座の開設にかかる身元確認の特徴を踏まえ、CBDC の口座開設においては、銀行が保有する情報やデジタル技術の活用による手続きの効率化等が議論された。

---

<sup>24</sup> 本項については、主に WG3 の各会合において議論を実施。

<sup>25</sup> マイナンバーカードの IC チップに搭載された電子証明書を利用して、非対面でユーザー本人の認証や契約書等の文書が改ざんされていないことの確認を公的に行い、安全・確実な本人確認を行うためのサービス。（<https://www.digital.go.jp/policies/mynumber/private-business/jpki-introduction>）

<sup>26</sup> 「デジタル社会の実現に向けた重点計画」2023年6月9日 閣議決定  
（[https://www.digital.go.jp/assets/contents/node/basic\\_page/field\\_ref\\_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609\\_policies\\_priority\\_outline\\_05.pdf](https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf)）

(表 2 - 1) 個人における身元確認のあり方

<p>公的個人認証に容貌撮影を組み合わせるなど、不正利用の実態を踏まえた追加的な対策が必要</p>
<p>公的個人認証に容貌撮影を組み合わせることで、所持、知識、生体の 3 要素を組み合わせた身元確認となり、マイナンバーカードとパスワードが悪意者に渡っても、なりすましへの対策が可能。</p>
<p>新たなセキュリティ対策もすぐに陳腐化するため、「公的個人認証を導入すれば大丈夫」などの考え方は、不正利用防止の観点では危険。公的個人認証に加え、容貌や動作の撮影も行うなど、犯収法上は求められなくとも、民間事業者は不正利用の実態を踏まえた追加的な対策が必要になる可能性。</p>
<p>追加的な不正利用対策を講じる場合、セキュリティと利便性のバランスに配慮が必要</p>
<p>公的個人認証に容貌撮影を組み合わせることで、一定のなりすましへの対策に資すると考えられる一方で、手続きが増え利便性の低下を招く可能性もある。追加的な不正利用対策を講じる場合には、リスクの高いサービスに限定するなど、セキュリティと利便性のバランスへの配慮が必要。</p>
<p>非対面での手続きに不慣れな人や高齢者等には対面等での対応が求められうるが、こうしたもとは CBDC の取扱いが仲介機関の収益につながるようなインセンティブ設計が必要</p>
<p>Web 経由での口座開設申込が拡大しているが、高齢者の多くは、Web のみで手続きを完結させることが難しいため、非対面だけではすべての顧客対応ができないことが多い。ユニバーサルアクセスの観点から、店舗対応やコールセンター等の「人」によるサポートが引き続き残る可能性。</p>
<p>CBDC の特性を考慮すると、各種手続きにおいてコストのかかる対面サービスを残さざるを得ない。このため、仲介機関のビジネスとして成り立たせるためには、CBDC の取扱いによる、自社の顧客基盤の拡大や、付帯収益の創出等の、別途のインセンティブが必要かもしれない。</p>
<p>非居住者の口座開設は犯収法や外為法に基づいた対応が求められ、確認事項が多岐にわたる</p>
<p>銀行での口座開設では、日本人の非居住者に対し、犯収法に則り正当と判断できる本人確認書類で確認を行っている。また、非居住者の場合は、外為法に基づいた対応が必要であり、国内での振込であっても、外国送金扱いとなる。そのため、確認事項が多く、対応が煩瑣になる可能性。</p>

(表 2 - 2) 法人における身元確認のあり方

<p>法人口座は悪用された際の影響が大きいと、個人口座対比、より厳格な手続きが必要</p>
<p>法人口座は、事業性決済を装うことで多額の資金を移転しやすいことや、詐欺による被害金の振込先の口座に指定された場合に、被害者が不信感を抱きづらいことなどを理由に、悪用された場合の影響が大きい。このため、個人口座に比べて、厳格な口座開設の手続きが設けられている実情がある。</p>
<p>Web 経由での法人口座開設に関し、ある銀行では、提出書類（謄本等）の確認や調査に加えて、Web 面談を必要としている。申し込み受付から口座開設までは、Web 面談日の調整や各種手続きの進捗次第だが、1 カ月程度要することがある。</p>
<p>法人の場合は、登記情報等の客観的な情報だけでなく、その実体の確認を行うことで、架空の法人による口座開設を防止することが重要である。ただし、実務においては対象法人の代表者との面談や現地調査を実施しても真偽を見抜くことは難しい場合も多い。</p>
<p>銀行が保有する情報や G ビズ ID<sup>27</sup>、e シール<sup>28</sup>等のデジタル技術の活用で、身元確認業務を効率化できる可能性</p>
<p>法人の KYC は、提出が必要な本人確認書類の数や多様さから、書類不備によって複数回のやり取りが生じることも珍しくない。海外事例では、本人確認書類の電子化により事務効率化を進めた事例もあり、日本でも電子化の議論が必要。</p>
<p>信頼できる第三者によって確認済のトラスト情報の活用が考えられる。日本における情報の取得先候補としては、①法人の口座開設時に犯収法に則った各種確認により一定の保証レベルの情報を保有している銀行や、②デジタル庁が提供する G ビズ ID が挙げられる。</p>
<p>非対面での口座開設を想定した場合、必要な書類を法人から取得する際に電子書類の利用も想定されるが、その真正性の検証について、日本においては e シールといった仕組みの活用や、非対面での手続きに対応できない法人を念頭に対面での CBDC 口座開設手続きを設けるか、が検討事項になる。</p>

<sup>27</sup> デジタル庁が提供する、すべての事業者を対象とした共通認証システム。  
(<https://gbiz-id.go.jp/top/>)

<sup>28</sup> 企業等が発行する電子データの発行元を証明し、また、電子データに改ざんがないことを証明する技術。e シールが付与された情報を検証することで、電子データの発行元のなりすましや改ざんがされていないことを確かかつ簡単に確認することが可能。  
([https://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/top/ninshou-law/electronic\\_seal.html](https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/electronic_seal.html))

## (継続的顧客管理の現状と課題)

決済サービスの安全性と信頼性を確保するためには、口座開設時の身元確認に加えて、継続的顧客管理が不可欠である。会合では、金融機関や資金移動業者の参加者から、継続的顧客管理は、対応コストや人的リソース面での負担が大きいといった課題があることが示されたほか、一部の事業者では、ATM やアプリにおける顧客接点を活用した効率的な顧客管理方法の検討・導入が進んでいることが紹介された。

(表 2 - 3) 継続的顧客管理の現状と課題

<p>継続的顧客管理は、顧客から情報更新の協力を得るための対応コストや人的リソース面での負担が大きい。協力が得られなかった場合、金融機関としては適切な管理が出来ていないにも関わらず、そのみをもったの利用制限には慎重にならざるを得ず、対応に苦慮</p>
<p>銀行での継続的顧客管理において、郵便やインターネットバンキングを通じて顧客に情報更新を依頼する際の課題を3点挙げる。1点目は、情報更新すべき対象顧客数が多く、対応するためのコストや人的リソース面での負担が大きいこと。2点目は、依頼に対する回答率が半数程度に留まり、中には苦情に発展するケースもあること。3点目は、郵便不着先への対応に苦慮すること。金融機関として適切な顧客管理ができないにも関わらず、住所変更の届出がないことだけを理由に取引停止等の顧客に不利益が生じるような対応は簡単には行えず、非常に頭を悩ませている。</p>
<p>資金移動業においても、継続的顧客管理において回答が得られない場合の利用制限は、課題と認識している。顧客の反応を踏まえると、利用制限をする場合は、慎重にならざるを得ない。</p>
<p>一部の事業者では、ATM やアプリにおける顧客接点を活用した効率的な顧客管理方法の検討・導入が進捗</p>
<p>一部の金融機関では、ATM 利用顧客に対して住所変更の有無を手続き中の画面上で確認する方法や、マイナンバーカードや免許証、在留カード等の本人確認書類を読み取れるカードリーダーを ATM に設置することにより顧客管理を行う方法について、検討・導入が進んでいる。</p>
<p>ある資金移動業者においては、アプリにおける顧客接点を活用して、ユーザーが情報更新依頼等に応じない場合は、対応期限を指定して、それを超過すると利用制限を行うといった事前警告をアプリ上に表示することなどにより、情報更新を促している。</p>

## (不正検知の現状と課題)

既存の決済サービスにおいて、不正取引の手口が多様化し、セキュリティ強化だけでは防ぎきれない事例が増加している。このため、ユーザー自身の金融リテラシー向上とともに、事業者による注意喚起等の対策が重要となる。また、AIをはじめとするデジタル技術の活用による不正取引の防止が期待されるが、その判断根拠がブラックボックス化しないよう留意する必要がある。

CBDC 口座はすべての仲介機関にとって新規開設となるため、不正検知の実効性を高めるためには、不審な取引が発生した際等に関係者間で情報交換ができる仕組みを設けることも一案との意見も聞かれた。もっとも、こうした仕組みを設ける場合、ユーザーからの同意が不可欠となるほか、誤検知の場合の責任の所在や仲裁機関について検討する必要があるなど、検討すべき点は多岐にわたるとの意見が寄せられた。

(表 2 - 4) 不正検知の現状と課題

セキュリティの強化だけではユーザー自身が騙される被害は防げないため、ユーザーのリテラシー向上や事業者による注意喚起等の対策も重要
フィッシングの攻撃方法は変遷しており、足許ではセキュリティの突破よりも直接的に本人を騙す手口にシフトしている可能性もある。そうすると、根本的な問題は、ユーザー自身の資産運用やセキュリティに対するリテラシーの低さとなる。
各金融機関が不正利用対策に注力しているものの、投資詐欺やロマンス詐欺等、お客さま自身が騙されてしまう詐欺に関しては、セキュリティ機能の強化だけでは完全に防ぐことは難しい。
AIをはじめとするデジタル技術活用により不正検知の効率化・高度化が期待できる。ただし、AI等による判断の根拠をブラックボックス化しないように留意
金融機関の不正検知における誤検知の削減には、ルールベースのモニタリングから脱却する必要がある。そのためには、金融機関が保有する内部の情報のみならず、外部の公表情報を含めて、関連するデータを収集し、顧客情報の名寄せを行い、関係者間の隠れたつながりを可視化したネットワークを生成し、送金人と受取人の関係を明らかにすることによって、検知の精度を高め、偽陽性と偽陰性を減らすことが可能。
リスクの識別と評価については、ユーザーの取引を包括的に把握することで、資金が複数ユーザーの間で循環しているかどうか、送金先のユーザーが経済制裁対象者と関

係性があるかどうかなどを可視化し、リスク評価の理由をブラックボックス化させないことが重要。
AI 技術の活用によって取引モニタリングの効率化が可能かもしれないが、AI の判断根拠がブラックボックスである場合は、その結果だけで不正とは判断できない。AI 技術を調査効率化のための補助的な位置付けとして利用し、コスト削減を実現することは可能であっても、人による判断は引き続き必要であるため、一定のモニタリング負担は残るだろう。

(表 2-5) 不正検知の実効性

CBDC 口座はすべての仲介機関にとって新規開設となるため、不正検知の実効性を高めるために、不審な取引が発生した際等に関係者間で情報交換ができる仕組みを設けることも一案
すべての仲介機関にとって CBDC 口座は新規開設となるため、個人情報の取扱いについては、不正検知目的での利用・第三者提供についてあらかじめ顧客より同意を取得した上で、不審な取引が発生した際に柔軟に関係者間での情報交換ができるようにすれば、不正検知の実効性も高まるのではないか。
不正検知を目的とした個人情報の第三者提供を行う場合、ユーザーからの同意取得等の対応が必要となるほか、誤検知の場合の責任の所在や仲裁機関について検討が必要
不審な取引が発生した際等に関係者間で情報交換ができる仕組みを整備する場合、正当なユーザーを何らかの要因で誤って不正と判断してしまうと、当該情報が各仲介機関に共有され影響が広範に及ぶため、責任の所在の整理とともに異議申立て対応等を行う仲裁機関の必要性について検討の余地があるだろう。
CBDC に関しては、不正検知を目的とした個人情報の第三者提供について、あらかじめ法令で認めておくことが望ましいのではないか。
個人情報の匿名化を行えば、個人情報の第三者提供に関する同意を得ずとも、共同化した取引モニタリングを行える可能性がある。

### (KYC や AML/CFT の水準)

CBDC が提供する機能に応じて、CBDC における KYC や AML/CFT の水準も変わってくる。会合では、既存の決済サービスと比較して CBDC のリスクが同水準以下の場合、CBDC の身元確認強度も既存の決済サービスと同水準で足りるのではないかと指摘がなされた。

このほか、身元確認の実施状況に応じて CBDC の機能の提供範囲を変更可能とすることで、ユニバーサルアクセスを一定程度確保できる可能性が挙げられた。一方で、犯罪被害を防止しユーザーを守る観点からは、高額振込等のリスクの高い機能に、適切な制限や取引モニタリングの仕組みを整備することも重要との声も聞かれている。

また、高度な本人認証は、セキュリティ機能の強化が図れる一方でユーザーへの負担にもなりうることを踏まえ、高齢者や身体が不自由な人等にも利用しやすい UI の必要性についても言及された。

(表 2 - 6) CBDC が提供する機能と KYC や AML/CFT 対応の水準

<p>既存の決済サービスと比較して CBDC のリスクが大きくないのであれば、CBDC の身元確認強度も既存の決済サービスと同水準で足りるのではないかと</p>	<p>CBDC における KYC や AML/CFT 等への対応は、金融機関や資金移動業者が提供する既存のサービスと比べてリスクが過大でない限りは、これらの既存の対応と同水準で足りると思われる。</p>
	<p>法人が行う CBDC の取引に関するリスクが、銀行預金取引と比較して同等以下の場合には、CBDC 口座開設時における KYC 水準も同様以下にできると考えられる。加えて AML/CFT 等の観点で CBDC の方が不正を防止しやすい設計にできる場合には、KYC の水準を下げることも可能かもしれない。</p>
<p>身元確認の実施状況に応じて CBDC の機能の提供範囲を変更可能とすることで、ユニバーサルアクセスを一定程度確保できるかもしれない</p>	<p>例えば 10 万円以下であれば身元確認を行わずに誰でも使えるようにし、それ以上の金額を利用するのであれば一定水準の身元確認として eKYC が求められるといった設計とすれば、ユニバーサルアクセスを一定程度確保しながら、CBDC を提供できるかもしれない。</p>
<p>犯罪被害を防止しユーザーを守る観点からは、高額振込等のリスクの高い機能に対して、適切な制限や取引モニタリングの仕組みを整備することも重要</p>	<p>ユニバーサルアクセスは重要だと考えるが、かといってすべての人が全く同じサービスにアクセスする必要はないのではないかと。SNS 型投資詐欺等からお客さまの資産を守る観点からは、高額振込ができる機能に簡単にはアクセスさせないことも重要な視点だろう。</p>
	<p>CBDC を全国民が利用するものと位置づけるのであれば、年齢等の特定の顧客属性だけで一律に取引金額等を制限することには異論が出る可能性もある。過去の取引履歴等、複数の要素を組み合わせた上で、取引モニタリングに強弱をつけて仲介機関側で安全性を担保するような仕組みの方が望ましいのではないだろうか。</p>

高度な本人認証はセキュリティ機能の強化が図れる一方でユーザーへの負担にもなる。高齢者や身体が不自由な方々の利用を想定する場合、簡易な UI の提供方法の検討が必要

金融犯罪の被害が高齢者に多い理由の一つには決済サービスそのものへの理解不足があると考えられる。これを防ぐには、対面取引時に十分な説明が必要である。しかし、その説明負担は店頭の職員への業務負担になるため、CBDC ではお客さまの理解促進と店頭の説明負担軽減を両立するシンプルな商品設計が必要。

高度な本人認証への切り替えにより、セキュリティ機能の高度化が図れる一方で、スマートフォンの機種変更時や、PC 等の他端末でログインを試みる場面において、ユーザーの負担が増えている点は課題である。こうした点も含め、特に高齢者や身体が不自由な方々が利用する際に大きなハードルとなりうるため、簡易な UI をどう提供するかは検討事項である。

## (KYC と AML/CFT 対応の共同化)

身元確認や継続的顧客管理、不正検知等、これらの取組みを効率的に推進する観点から、共同センターやコンソーシアムによる業界横断的な取組みの可能性についても議論が行われた。一方で、KYC と AML/CFT 対応を共同化するに当たっては、責任の所在や運営主体、採用する方法の選択、情報共有に伴うプライバシーリスク等、整理すべき課題も多いとの指摘もなされている。

また、口座開設の可否等の判断基準については、政府等の公的機関や業界団体がベースとなる基準を定めた上で、各仲介機関が実態に応じて上乘せの審査基準等を設けることが望ましいとの意見が示された。

### (表 2-7) KYC と AML/CFT 対応の共同化における利点

共同センターやコンソーシアムによる業界横断的な不正検知等の取組みは、高度化・効率化に資すると考えられる

CBDC を扱う事業者でコンソーシアムを形成し、取引情報を一元管理するプラットフォームを作ることも一案。CBDC の移転をコンソーシアム内で管理される CBDC 口座間に限定すれば、仕向先（送金元）および被仕向先（送金先）の情報がコンソーシアム内で共有されることになり、不正取引のリスクを低減する効果が期待できる。

規模の大きくない仲介機関が自前ですべてのシステムを用意することは難しいと想定され、何かしらの共同化は必要だろう。

<p>各事業者が個別に対応するより、共同センター等が集約して対応する方が効率的。社会全体のコストを抑えられるため、身元確認のプロセスの共同化は有益。</p>
<p>AML や金融犯罪対策の共同化の利点は、ナレッジの集約による有効性の高い不正検知を行うためのシナリオ設計が可能となることである。規模が小さく、リソース不足からナレッジの蓄積が難しいような金融機関にとって、共同化は有力な解決手段と言える。また、疑わしい取引の調査手法や届出要否の判断基準等を先進行と統一できることや、業務集約による効率化・コスト削減もわかりやすいメリットとして挙げられる。</p>

(表 2 - 8) KYC と AML/CFT 対応の共同化における課題

<p>KYC と AML/CFT 対応の共同化に当たって検討すべき課題は、責任の所在や運営主体、採用する方法の選択、情報共有に伴うプライバシーリスク等多岐にわたる</p>
<p>KYC と AML/CFT 対応を共同化する場合は、仲介機関や預金口座を紐付けている銀行との間での責任の所在や、不正な取引を検出した際の対応について、あらかじめ基準や仕組みを検討する必要があるだろう。</p>
<p>共同センター化は、責任分界をどう整理するか、運営主体をどのようにするかが重要な論点。責任分界の整理は、事業者間でのリスクの範囲が明確になることによって、各社がどのようにリスクを取りながら事業を運営していくかを検討する上で重要になる。運営主体については、共同出資等様々な方法が考えられるが、どのような主体が主導するのか、民間だけでやるのか、多数の関係者がいる中で合意形成はどのようにしていくのかなどが課題になる。</p>
<p>身元確認の共同化には、各社で様々な考え方がある。例えば、自社が既に対応している方法が採用されれば良いが、そうでない場合は新たな開発負担等が生じてしまい、望ましくないとも考えることもありうるだろう。また、他の事業者の身元確認済情報をもとに身元確認完了とすることは、その情報が実際は不正に手続きされたものであると判明した場合の対応に苦慮する可能性があり、望ましくないとも考える。</p>
<p>個人情報の取扱いには課題も考えられる。仮に、共同センター等が一括して身元確認を実施する場合、取得した個人情報を仲介機関へ共有する際には、ユーザーからあらかじめ第三者への情報提供として同意を得るか、もしくは個人情報保護法 27 条 5 項 1 号委託提供の場合として整理するかなどの検討が必要と考える。そのほか、取得した情報を目的外で利用していると見られるレピュテーションリスクも考えられ、慎重に検討を行う必要がある。</p>

CBDC にかかる取引モニタリングを受託することが、為替取引分析業務に該当するのかが不明確であり、今後整理が必要だろう。

AML や金融犯罪対策の共同化の取組みにおける最大の難点は顧客情報の取扱いが業務委託となること。委託元銀行毎に執務室およびサーバー内の環境を完全に分別していることから、環境整備コストが嵩むほか、委託元銀行を跨いだネットワーク分析等は実施できない。また、委託元銀行の拘りが強いシナリオは統合が難しく業務共通化の障害となりやすい。さらに、委託元銀行によってシステムの機能に差があり、データ化されている先がある一方で、アナログ管理されている先もあり、調査・検証の品質にばらつきが出てしまうことも難点である。

不正検知システムを共同化し、共同機関が共同システムを運営した場合において、運営上の課題は複数考えられる。1点目は、大手の金融機関へ運営上の負担が集中することにより不公平が生じうる点。具体的には、取引量が多い大手の金融機関が、不正利用に関する情報やその対策、システム開発に関するノウハウの一方的な提供側になる可能性に加え、仮にユーザー数に応じてシステム開発コストを負担することになれば、コスト負担においても大きな割合を大手の金融機関が負う可能性がある。

2点目は、大手の金融機関と同じ水準の不正検知の機能は、小規模な金融機関にとっては、過剰な機能となりうる点。不正検知のために共同システムが要求する情報（例えば、IP アドレス等の情報）を各金融機関においてあらかじめ取得する必要があるが、仮にそうした機能が金融機関のシステム内になれば、当該機能を開発する必要が生じる。こうした場合、主に小規模な金融機関では、事業規模に対してシステム開発コストが見合わないことも考えられる。結果として、適切な情報を共同機関に提供できず、適切な不正検知ができないことにつながる。また、仮にシステム開発が可能としても、小規模な金融機関の事業においては、必ずしも大手の金融機関が求める不正検知の水準に追従する必要性があるとは限らないため、共同システムを利用する金融機関間での意見調整は簡単ではないだろう。

3点目は、AI においても似たような課題があるが、不正な取引と判断した根拠について各金融機関が説明責任を果たせるのかという点。共同システムが不正の可能性が高いと判断したことを根拠に不正利用口座として凍結等を行った場合、訴訟等において各金融機関が不正と判断したことに対する説明責任を果たしたと評価されるかは判然としない。各金融機関は、自らの事業におけるリスクや個別の取引状況等を考慮した上で、不正と判断した根拠の説明責任を果たせるような何らかの仕組みを考慮する必要があると思われる。

(表 2 - 9) 口座開設の可否等の判断基準

口座開設の可否や取引制限等の判断軸は政府等の公的機関や業界団体がベースとなる基準を定め、各仲介機関が実態に応じて上乗せの基準を設けることが望ましい
「口座開設」に関して、何らかの制限を課すべき主体を想定する必要があるのであれば、各仲介機関の判断や責任に任せるのではなく、政府等の公的機関によってあらかじめ検討し、判断基準を整備する必要があるだろう。
取引制限の根拠は取引約款となると想定されるが、銀行預金では、全国銀行協会より普通預金規定の参考例が出されており、CBDC でも類似の対応が望ましい。
「口座開設」の可否や条件等について共通の条件を定めた上で、各仲介機関が上乗せの審査基準や保留基準を設けると良いだろう。また、取引制限の根拠を含む取引約款等を定めた上で、不正利用の懸念がある口座には取引制限を行えるようにすべき。

## 2.2 認証・認可<sup>29</sup>

### (認証・認可における標準のあり方と最新動向)

CBDC では、多くの仲介機関や追加サービス事業者の参加が見込まれるもとの、これらの企業が個別に認証・認可の仕様を検討および構築する場合、全体として多大な労力とコストの発生が予想される。また、認証・認可が標準化されていない場合、何らかの脆弱性に起因したインシデントが発生した際の対応についても個別での検討や実施が求められ、負荷が増加しうる。このような観点から、システム対応コストや脆弱性があった際の対応を考慮すると、CBDC では標準化された認証・認可の方式を採用すべきであり、標準を意識した技術選択が重要であるとの議論がなされた。

標準化の検討に当たっては、CBDC のユースケースとそのリスクを整理した上で、国内外の標準規格やガイドラインを活用することが望ましく、それらが解決しようとしている課題を理解した上で、適切に実装・運用することが重要である。

追加サービス提供事業者にとっては、付加価値を提供しやすい仕組みとして標準化された API と認可の実装が必要であり、標準化の粒度（どの範囲でどの程度を共通化すべきか）を検討する必要がある。ただし、仲介機関側に生じる負担にも考慮が必要である。また、高いセキュリティ要件を満たす FAPI への準拠は検討すべき事項である

<sup>29</sup> 本項については、主に WG3 の各会合において議論を実施。

が、こうした仕様の共通化を進めるに当たっては、海外事例等も踏まえると、国として強制力をもって主導することも成功のモデルの一つであると意見が示された。

(表 2 -10) 認証・認可における標準のあり方と最新動向

システム対応コストや脆弱性があった際の対応を考慮すると、CBDC では標準化された認証・認可の方式を採用すべきであり、標準を意識した技術選択が重要である	
銀行がシステム対応を行う際には、大きなコストがかかる。特に、規模の大きくない銀行では、単独で対応することが困難なケースがある。このようなケースでは銀行同士が連携をして、同じシステム基盤を使い、共同利用をすることでコストを抑えることが多い。このような際に、統一した仕様の定めがないと、どのような仕様とすべきかなどについて開発を担うベンダー側の意向が働きやすくなる可能性もある。コスト削減、検討負担削減の観点から仕様を統一頂きたい。	
CBDC では標準化された認証・認可の方式を採用すべきである。標準化された方式でないと、脆弱性があったときに個別に対応しなければならず、コストも時間もかかる。標準を意識した技術選択の重要性を強調したい。	
標準化の検討に当たっては、CBDC のユースケースとそのリスクを整理した上で、国内外の標準規格やガイドラインを活用することが望ましく、それらが解決しようとしている課題を理解した上で、適切に実装・運用することが重要である	
CBDC のユースケースやシステムモデルを整理しつつ、各ユースケースでどのような標準化やガイドラインが必要かを議論する必要がある。	
CBDC は安心安全に誰でも使えることが求められ、仲介機関、追加サービス事業者等からの連携も含めた多様なサービスの提供が想定される。そのため、CBDC には様々な認証パターンが考えられることから、各サービスの内容・リスクに応じて、セキュリティと利便性のバランスを考慮した上で、認証方式を適切に選択し、正しく実装することが必要である。	
脅威への対策には、脅威とそのリスクを分析した上で、適切な対策の設計/選定・実装が必要であり、その際には、FIDO2.0 や、Open ID Connect 等の標準規格や、NIST の SP800-63 等のガイドラインを可能な限り活用することが望ましい。ただし、標準規格やガイドラインが解決しようとしている課題を理解した上で、適切に実装・運用することが重要である。	

追加サービス提供事業者にとっては、付加価値を提供しやすい仕組みとして標準化された API と認可の実装が必要であり、標準化の粒度（どの範囲でどの程度を共通化すべきか）を検討する必要がある。ただし、仲介機関側に生じる負担にも考慮が必要である。

様々な追加サービス提供事業者に参加してもらうに当たり、付加価値を提供しやすい仕組みが重要であり、そのためには標準化された API と認可の実装が必要。

API の仕様をどの範囲でどの程度共通化すべきかについては、様々な観点がありうる。例えば、詳細なシステム仕様含めて同じに動くという観点や、セキュリティやプライバシーに関する考え方や要求が同じという観点等が挙げられ、その程度は様々にありうる。これまで各金融機関が API の提供を進めた中では、連携するサービスを作る側は、各金融機関の API の仕様の差異に対応するのが大変だったという話がある一方で、そうした個別の対応をした結果、独自性のあるサービスが打ち出せたといった良い面もある。

すべての仲介機関に対して、高い水準での標準化を推し進めると、特に規模の小さい金融機関にとっては対応負担が大きく、そもそも仲介機関になることのインセンティブが不明瞭であることも相まって、仲介機関としては参加をしないと判断する可能性がでてくるだろう。CBDC の普及においては、ユーザーに利便性や高い UX を提供することは重要であるものの、仲介機関側に生じる負担も考慮していく必要がある。

高いセキュリティ要件を満たす FAPI への準拠は検討すべき事項であるが、海外事例等も踏まえると、こうした仕様の共通化を進めるに当たっては、国として強制力をもって主導することも成功のモデルの一つである

FAPI へ準拠することで、なりすましやデータ改ざん、認可コード・アクセストークンの漏えい等への技術的観点からの対策が可能となる。また、BIS イノベーションハブとイングランド銀行による「Project Rosalind」ではすべての API が FAPI に準拠するようと言及があり、イングランド銀行の CBDC への考察文書<sup>30</sup>では FAPI によって最高標準のセキュリティ管理が可能になると言及されている。CBDC という重要度が高い金融資産に対しては高いセキュリティが要求されるため、FAPI への準拠は検討すべき事項と考える。

ブラジル等の海外の一部の国において FAPI の準拠が進んだ理由は、国として FAPI の準拠を義務化したからと考えている。日本においては、銀行法の改正に伴い、銀行のオープン API の実装が努力義務となり、多くの銀行が対応したものの、FAPI に準拠し

<sup>30</sup> イングランド銀行（Bank of England）による、デジタル・ポンドの技術的要件および設計原則をまとめた報告書。「The digital pound: Technology Working Paper」2023年2月7日公表  
(<https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-technology-working-paper.pdf>)

ている銀行は数行にとどまるため、異なる仕様の API が増えただけに映る。電代業者が提供するサービスと連携する容易さの観点からは、同じ仕様の API が幅広く実装されることが重要である。なお、仕様の共通化は、海外事例等も踏まえると、国として強制力をもって主導することが成功のモデルと考えるものの、その裏付けに大義名分がなければ、あまり上手くいかないだろう。

### (リスクを踏まえた対応のあり方)

ユーザーが安心・安全に CBDC を利用できる環境を整備するためには、CBDC における関係者間での取決めとして、リスクの所在、責任分界点、コスト負担のあり方といった重要事項についてあらかじめ合意する必要がある。また、CBDC のユースケース毎にリスク評価を実施した上で、利便性とのバランスやコストも考慮に置いて、適切な本人認証の強度を確保するなどのセキュリティ対策を講じることが重要である。

取引内容やリスクに応じて本人認証の強度を変えることも必要であり、そのためには本人認証の保証レベルの整理が重要である。例えば、CBDC の保有額制限等によって仲介機関の既存決済サービスよりもリスクが低いと判断できれば、既存決済サービスの本人認証の強度で十分である。また、低リスクのユースケース（同一名義人間の資金移動や税公金収納、公益企業への支払い等）の場合には、本人認証の簡略化も検討しうるだろう。

(表 2-11) リスクを踏まえた対応のあり方

CBDC における事業者間の取決めとして、リスクの所在、責任分界点、コスト負担のあり方といった重要事項についてあらかじめ合意しておく必要

認証をどこまで簡易にし、リスクをどこまで許容するのかのバランスは、ビジネスを考えていく中で事業者が決めていくものである。低リスクの場合は簡易な認証とし、高リスクの場合は認証強度を上げるという判断を当然していくが、その際、リスクが顕在化した場合のコストを誰が負担するのかという点が明確であることが前提。したがって、CBDC の認証のあり方を考える際も、リスクの所在や責任の分担、コストが生じた場合の負担についてあらかじめ決めておくべきだろう。

CBDC においては、仲介機関の役割として行った口座開設やその後の取引モニタリング等、様々な場面において、誰がどのような責任を持つのかという責任分界点について明確にしていく必要があると考えている。また、「個人ユーザーは CBDC 口座を複

	<p>数保有できる」という制度設計となった場合は、1つの口座では少額の振込しか行っておらずとも、口座を多数開設することで、全体としては多額の振込を行っている、等の問題の発生が考えられるため、名寄せの可否を含め、どのように確認を行うかを考える必要がある。いずれの場合においても、異常値の検知方法や、そのためのコストおよび責任の所在等について検討する必要がある。</p>
	<p>CBDC のユースケース毎にリスク評価を実施した上で、利便性とのバランスやコストも考慮にいて、適切な当人認証の強度を確保するなどのセキュリティ対策を講じることが重要</p> <p>CBDC 口座は、預金口座や資金決済アカウントに紐付けられると認識しているが、預金口座や資金決済アカウントの身元確認や当人認証の強度に差がある場合、差を許容するか否かは論点になりうる。不正利用防止の観点からは、より強度の高い方式に揃えることが望ましいが、利便性とのバランスも重要になる。</p> <p>セキュリティと利便性だけでなく、コストも考慮に入れる必要。自社内でもコスト削減は度々議論になる。ただし、コストを抑えるために当人認証を軽くしようといった議論ではなく、セキュリティ水準を維持しながらどうにかコストを抑える工夫ができないかといった議論が主になっている。</p> <p>現在、サービスの内容が事業者毎に異なるため、各事業者のポリシーに従い設定される認証のレベルと利便性は事業者毎に異なる。CBDC の場合、仲介機関毎に共通するポリシーを作るのか、あるいは作らないのか、作るのであれば金額・用途によって認証のレベルをどのように設定するのかは論点となる。</p>
	<p>取引内容やリスクに応じて当人認証の強度を変えることも必要であり、そのためには当人認証の保証レベルの整理が重要である</p> <p>取引内容やリスクに応じて当人認証の強度を変えることも必要と考えており、そのためには当人認証の保証レベルを整理することが重要である。国内における eKYC 方式の身元確認や当人認証の保証レベルは、独立行政法人情報処理推進機構（IPA）のデジタルアーキテクチャー・デザインセンター（DADC）で整理されており、参考になる。保証レベルの整理が不十分であったり、各仲介機関に保証レベルの判断を任せたりすると、対応に差異が生じうるため留意が必要である。その対策として、eKYC システム等の共同化は一つの方法と考えられる。</p>
	<p>CBDC の保有額制限等によって仲介機関の既存決済サービスよりもリスクが低いと判断できれば、既存決済サービスの当人認証の強度で十分である。また、低リスクのユースケースの場合、当人認証の簡略化は検討しうる</p> <p>CBDC が仲介機関の既存決済サービスに組み込まれるとの前提を置いた場合、CBDC のリスクが仲介機関の既存決済サービスよりも低ければ、既存決済サービスの認証強</p>

度で十分である。一方で、CBDC のリスクが仲介機関の既存決済サービスよりも高い場合や、一段高い認証強度を求められる場合では、仲介機関は認証強度を上げなくてはならない可能性があり、その場合に対応することは簡単ではないだろう。

同一名義人間の資金移動や税公金収納、公益企業への支払いといった低リスクのユースケースの場合や、取引をリアルタイムで監視しつつ不正率が一定の基準を下回る場合は、認証の一部省略・簡略化の検討ができるのではないか。また、不正率等のデータは、複数の民間事業者が横断的に取りまとめるよりも、公的・中立的な機関によって蓄積される方が望ましい可能性もある。

### 3. CBDC エコシステムのあり方

#### 【第3章の概要】

本章では、CBDC の利便性を向上させる追加サービスを含めた CBDC エコシステムのあり方に関して、仕様の標準化、システムの共同化、追加サービスと API、プログラマビリティ等の論点について、各会合で議論された内容を紹介します。

仕様の標準化に関しては、エコシステムを担う仲介機関や追加サービス事業者の技術レベルやセキュリティレベルを一定水準以上に保つ重要性和、それを実現するための仕様書やガイドライン等を制定する必要性および留意点について議論が交わされた。仕様の標準化を主導する中立的な機関が必要であり、当該機関が技術の進展に応じて適切な仕様の見直しを図っていくことや、海外における標準化の動向や国際標準を意識した議論の必要性等について議論を行った。

システムの共同化に関しては、多くの民間事業者が仲介機関として参入しやすい仕組みを整えることが CBDC エコシステムを活性化させるための重要な要素であるとの問題意識のもと、共通性が高く競争優位性を生まないインフラ部分や業務プロセスについて共同化することを検討課題として、対象となる業務や機能の範囲、事業者間の合意形成の難しさ、共同化に伴うメリットやデメリットについて、様々な意見が交わされた。

追加サービスと API に関しては、CBDC エコシステム全体の信頼性を確保する観点から、基礎的な決済機能だけでなく追加サービスについても品質保証が重要であり、導入するサービスにかかる十分な検討と信頼のおける機関によるシステムテストの必要性について議論が行われた。また、追加サービスの提供を持続可能とするための仕組みの構築や、API の開発容易性の重要性についての指摘があった。

プログラマビリティに関しては、API サンドボックスプロジェクトで参加企業が構築した追加サービス事例等を踏まえながら、様々なユースケースや可能性について活発な議論が行われた。具体的には、エスクロー機能（一時的な資金確保）、プログラマブルペイメント（条件付き支払い）、パーパスバウンドマネー（用途制限機能、地域限定利用機能）についてのニーズや社会実装時の課題等が検討された。その中では、CBDC システムそのものにプログラムを組み込むことはセキュリティ上のリスクを伴うため、同システムの外側でプログラムすることが望ましいとの指摘もあった。

### 3.1 仕様の標準化<sup>31</sup>

安心・安全な CBDC エコシステムの形成に当たっては、エコシステムを担う仲介機関や追加サービス事業者の技術レベルやセキュリティレベルを一定水準に保つ必要がある。そのためには、仕様書やガイドライン等の制定により、仲介機関毎の対応にばらつきが生じないような措置を講ずる必要があるほか、仕様書等の制定に当たっては事業者で合意形成を図りながら技術の発展に合わせて適切に見直していく必要があるとの議論がなされた。また、仕様の標準化を主導する中立的な機関が必要であり、公的機関、民間事業者の組織・団体、新しい組織の設立等、様々な可能性について検討すべきとの議論があった。さらには、各国・地域において CBDC の検討が進むもとの海外での標準化の動向や国際標準を意識した議論の必要性についての指摘があった。

他方、仕様の標準化の検討に際しては、民間事業者におけるイノベーションを阻害しないためにも、競争領域と協調領域の線引きの見極めが重要との指摘があったほか、脆弱性発覚時のリスク分散の観点から敢えて仕様を統一しない考え方もあるといった指摘もなされた。

(表 3 - 1) 仕様の標準化の重要性<sup>32</sup>

CBDC エコシステムを担う仲介機関や追加サービス事業者の技術レベルやセキュリティレベルを一定水準に保つためには、仕様書やガイドライン等の制定による標準化が重要
仕様の標準化は重要な論点。CBDC においても、仲介機関間の振替やチャージといったケースによって標準化が必要となるだろう。API 接続の標準化はもとより、UX 全体を意識した標準化を進めていくことが大事である。
仕様の標準化やインターオペラビリティの重要性は、予てより指摘されてきたが、結果的に実現しなかった例が多くある。その背景には、標準化やインターオペラビリティは民間の競争の中で決まっていくものだといった考え方や、既存の仕組みを変えることができなかったという側面がある。CBDC システムをスクラッチで作るのであれば、将来を見越した標準化の動きが求められる。
CBDC システムにおいて、仕様を標準化するのか、各仲介機関の対応に委ねるのかは大きな論点。対応が各仲介機関に委ねられた場合、CBDC の取引において、例えば仲

<sup>31</sup> 本項については、主に WG2 と WG3 の各会合において議論を実施。

<sup>32</sup> KYC、AML/CFT や認証・認可に関する標準化は第 2 章にも記載。

	<p>介機関毎に認証強度の差が生まれるだろう。他方、仕様を標準化する場合には、民間事業者のイノベーションを阻害しないためにも、競争領域と協調領域の線引きの見極めが重要。</p>
	<p>銀行預金から民間デジタルマネーにバリューを移転する既存の仕組みを踏まえれば、CBDC と既存の民間決済システムとの連携は、さほど難しくないようにも思われる。もっとも、接続インターフェースを統一すれば済むのか、何らかのクリアリングシステムが必要になるのかといった論点は存在する。</p>
	<p>カンボジアでのバコン導入当初は、中央銀行が統一アプリを提供する形をとったが、民間金融機関からの反発もあって加盟店開拓が進まなかった。このため、民間金融機関の既存アプリケーションを利用しながらも、QR コード規格を統一し、API も共通化することで、アプリケーション間の互換性をとる仕組みに変更した。こうした対応が奏功し、加盟店開拓が進むようになった。</p>
	<p>CBDC において、標準仕様やガイドラインを策定した場合は、各仲介機関がどう実装していくかについても合意形成が必要。そうした合意形成を怠った場合、標準仕様に沿う形で対応したとしても、微妙な実装上の差異が生じる可能性がある。特に、アプリの仕様やユーザーの認証情報の連携をする場合には留意が必要だろう。</p>
<p>仕様を統一せずに脆弱性発覚時のリスク分散を図ることも一案</p>	
	<p>仕様を統一化すると、脆弱性が発覚した際の影響が広範囲に及ぶ可能性がある。敢えて仕様を統一せずにリスク分散させた方が良いという考え方もありうる。CBDC のような新しいものを検討していく過程においては、統一すべきものとそうでないものを区別して検討することも重要である。</p>

(表 3-2) 標準化に向けた事業者間での合意形成の必要性

<p>事業者に一定水準以上のセキュリティレベルやサービスレベルを維持させるためには、事業者間で合意形成を図りつつ、仕様書やガイドライン等を制定する必要がある。また、技術の発展に合わせた適切な見直しも必要</p>	
	<p>不正対策が十分でない仲介機関が存在する場合、情報が悪意のある攻撃者の間で共有され、当該仲介機関が集中的に狙われる可能性がある。そのような事態を避けるためには、一定水準以上の統一された仕様書やガイドライン等を定め、仲介機関に守らせることが必要である。</p>
	<p>ガイドラインよりも技術仕様書として定める方が良い。過去、銀行 API のオープン化の際にガイドラインが制定されたものの、各行やベンダーがそれぞれ API を構築した</p>

<p>結果、仕様の異なる API が乱立してしまった。こうした経験も踏まえ、ガイドラインよりも技術仕様書を定めて公開し、どの事業者であっても同じ技術仕様で参入させる方法にした方が良い。</p>
<p>標準化を目的とした仕様書やガイドライン等を制定する場合、その目的は以下の3点が考えられる。1つ目は、CBDC エコシステム全体のセキュリティレベルの維持。2つ目は、サービスレベルと利便性の共通化。3つ目は、仲介機関や追加サービス提供事業者の負担軽減。</p>
<p>標準化を前提に仕様書やガイドライン等を制定する場合には、以下4点に留意すべき。1つ目は、記載内容の抽象度と個社の裁量とのバランスが重要。2つ目は、仕様書やガイドライン等を多くの民間事業者にも利用してもらうためには、法的・制度的な強制や業界団体の自主規制、準拠によるメリット等が必要。3つ目は、正しく準拠しているかを確認・検証するためのスキームとしてチェックリストといった確認手段の確立と、確認結果をステークホルダーや第三者が検証する枠組みが必要。4つ目は、仕様書やガイドライン等のリリース後に見つかった改善点や技術進歩・市場環境変化を踏まえた見直し等によって、定期的なメンテナンスが必要だが、それらを行う業界団体の設立・維持、知識・ノウハウの継承が課題。</p>
<p>ガイドラインやチェックリストで目線を合わせても解釈の違い等でセキュリティレベルを一定に維持できない可能性には注意する必要がある。</p>

(表 3-3) 標準化を主導する中立的な機関等の必要性

<p>仕様の標準化を主導する中立的な機関が必要。公的機関、民間事業者の組織・団体、新しい組織の設立等、様々なオプションが考えられる</p>
<p>仕様書やガイドライン等を策定する際に想定されうる主体の候補は大きく3つ挙げられる。1つ目は公共機関。政府や日本銀行、そのほかの公共機関が主体となり、民間事業者の組織・団体や有識者の協力のもとで、策定・改定していくことが考えられる。2つ目は、民間の組織・団体。CBDC の仲介機関となりうる民間企業が主な構成者である業界団体や、キャッシュレスやセキュリティ等に関する民間事業者団体・組織が主体となることが考えられる。3つ目は、新しい組織・団体の設立。CBDC は新たなサービスであり、ステークホルダーも多岐に亘るため、新たに新組織・団体を組成し、当該組織が主体となることも考えられる。</p>
<p>トークン化預金やステーブルコイン等の発行が増えると、決済手段のサイロ化によって分断が進む可能性。サイロ化を防ぐ手立てとして相互運用性が重要であるが、それ</p>

<p>を実現するためには技術面の標準化や API 連携だけでなく、中立的な組織や、標準化に向けたイニシアティブが鍵となる。</p>
<p>米国では、民間団体が標準仕様を策定し、後から政府が公認するパターンもある。標準化に強制力を持たせつつ、技術の進歩や状況の変化に応じて、民間事業者ならではのスピード感や柔軟性をもって対応することで、官民の良さをバランスさせている。</p>

(表 3 - 4) 海外動向や国際標準を意識した議論の必要性

<p>CBDC にかかる海外の動向や国際標準を意識した議論・検討が必要</p>	
<p>CBDC の検討が各国で進む中、海外で国際的な標準仕様が制定されると、日本も準拠せざるを得なくなる可能性もある。過去にも FeliCa 方式の採用を巡って IC カードの国際標準との関係が問題になったケースがあり、国際的な標準化の動向を睨みつつ、状況に応じて日本の立場の発信や、国際的な協調を働きかけることが重要になる。</p>	
<p>CBDC のアーキテクチャーの検討が進んだ後で大幅な見直しが生じないように、海外の CBDC システムとの接続についても事前に検討しておく必要がある。</p>	
<p>JPQR は QR コードの世界標準を採用している規格であり、既に多くの加盟店が採用していることや、既存の決済サービスとの相互運用性への影響を加味すると、採用のメリットが大きいのではないか。</p>	

### 3.2 システムの共同化<sup>33</sup>

多くの民間事業者が仲介機関として参入しやすい仕組みを整えることは、CBDC エコシステムを活性化させる上で重要な要素の一つと考えられる。このため、各仲介機関が個別に顧客管理システムや台帳管理システムといった仲介機関システムや、AML/CFT や不正検知の仕組み等の周辺システムをスクラッチで構築・維持するのではなく、共通性が高く競争優位性を生まないインフラ部分や業務プロセスについては、システムの共同化を検討することも一案。会合においては、共同化によるメリットとデメリット、システムを共同化するに当たっての留意事項について意見が交わされた。

(表 3-5) システムの共同化のメリット・デメリット

個別運営対比で効率化に期待	<p>CBDC システム（仲介機関システム（顧客管理、ユーザー口座））の共同化によって、①仲介機関毎にシステム構築が不要となるほか、②共同のシステム内での指図となるため、システムを跨いだ指図は不要となりフローが効率化される。結果として、仲介機関毎にシステム開発を行うのに比べ、参画することが容易になるといったメリットが考えられる。</p>
	<p>仲介機関業務の共同化によるメリットは、大きく4点考えられる。1点目は、「効率性の向上」。共通プラットフォームの使用により取引・事務・システム運用コストが削減できる可能性。2点目は、「互換性の確保（標準化）」。各仲介機関間での情報共有やシステム連携がスムーズになる可能性。3点目は、「負荷分散のコントロール」。各仲介機関に過度な負荷がかかることを防ぎ、システム全体の安定性が向上する可能性。4点目は、「高度化」。共同化によって集められたデータの利活用が可能となることで、処理が高度化できる可能性がある。</p>
セキュリティリスクや運用の複雑性、競争の阻害等のデメリットも想定	<p>仲介機関業務の共同化によるデメリットは、大きく3点考えられるが、見方によってはメリットにもなりうる。1点目は「セキュリティリスクの増大」。共同システムが攻撃を受けた場合、影響が大きくなる可能性。ただし、共同化されていることで対策が打ちやすい側面もあるだろう。2点目は「運用の複雑性の増大」。複数の仲介機関が共同で運用するため、調整や管理が複雑になる懸念がある。ただし、適切に運用ができれば、むしろメリットにできる可能性もある。3点目は「競争の抑制」。共同化により、各仲介機関が提供するサービスが画一化し、競争が阻害される懸念がある。</p>

<sup>33</sup> 本項については、主に WG3 の各会合において議論を実施。

(表 3-6) システムを共同化する際の留意事項

共同化の範囲等を検討するポイント
<p>共同化における考察ポイントの一つは、「何をどこまで共同化すべきか」であり、以下の6つの課題があると考えている。①機能と業務に関し、共通化部分と仲介機関個社部分の機能や業務の明確化。②データに関し、共有化範囲の十分な検討。③役割と責任分担に関し、日銀・仲介機関・ユーザーの責任範囲の明確化。④セキュリティリスクに関し、データを集中して持つことによるリスク増加への対策。⑤ガバナンスコントロールに関し、チェック機関のような第三者評価の仕組み作りの必要性の検討。⑥事務コスト・システムコストに関し、システムの複雑化によるコスト増加懸念への対応および運用コストの按分方法の明確化。なお、運用コストの按分方法は、例えばSaaSではAPIのコール数で従量課金を行っている等、既存のサービスの考え方を参考にできるだろう。</p>
<p>共同化の範囲や仕様次第では、参加企業の既存システムや業務仕様への影響が大きくなる場合もある。</p>
共同システムを利用する仲介機関間でのコスト配分や合意決定プロセスをあらかじめ定めておくことが望ましい
<p>共同システムを利用する仲介機関が多いと、各種の合意形成が課題となるケースが多いため、仲介機関間でのコスト負担の配分の根拠や、機能追加や拡張等の仕様変更における合意・決定プロセスをあらかじめ定めておくことが望ましい。</p>
<p>取引モニタリング等の管理を共同化する場合は、仲介機関や口座を紐付けしている銀行との間での責任の所在や、不正な取引を検出した際の対応について、あらかじめ基準や仕組みを検討する必要がある。</p>
<p>仮に共同化を進めるとなった場合、事業者が多岐にわたるため、どのような主体が主導し、どのようなモチベーションで推進されるかによって、実現可能性、実現に至るスピード、予算の確保のハードルの高さ等が変わってくる。</p>

### 3.3 追加サービスと API<sup>34 35</sup>

CBDC の利便性を向上させる追加サービスを提供する場合、CBDC エコシステム全体への信頼を確保する観点から、追加サービスにかかる品質保証が重要であるとの議論がなされた。加えて、提供する追加サービスとして何を想定するかによって、実装時の課題や考慮すべき事項が異なるため、プロトタイプシステム等を活用しながら、課題を洗い出していく作業が必要との指摘があった。このほか、追加サービスの提供を持続可能とする仕組みの構築や、APIの開発容易性が重要である点について指摘がなされた。

(表 3-7) 追加サービスと API

<p>CBDC エコシステムへの信頼を確保する観点から、追加サービスにかかる品質保証は重要。十分なテストを経ずに追加サービスがローンチされ、ユーザーに不安を与える結果となった場合、CBDC そのものに対する信用にも影響を及ぼすリスクがある</p>
<p>追加サービスを巡る議論は、CBDC システムの品質保証と密接に関連する。例えば、紙幣は「突然使えなくなることがない」という観点で品質が保証されており、その信頼のもとで国民は安心して使っている。クレジットカードの決済網は、端末・データセンター・通信経路といったシステムに支えられているが、事前に十分なテストを経て、当該テストをクリアできたシステムのみを利用している。CBDC の追加サービスにおいても、十分なテストを実施しなければ、CBDC そのものに対する信用に影響を及ぼすリスクがある。</p>
<p>追加サービスにかかる十分なテストを実施するには、追加サービス提供者以外のシステム管理者によって検査・許可されたプログラムのみが動く領域や仕組みが必要である。追加サービス提供者自身が管理している領域では、システム管理者は十分なテストを実施することが相当程度困難なのではないか。</p>
<p>追加サービスとして、利用場所を限定する地域通貨や、年齢制限付き機能を提供する場合には、加盟店サイドでの対応も必要となる。加盟店のシステムも含めて十分なテストを行わなければ、CBDC の品質を保てない可能性がある。</p>

<sup>34</sup> 本項については、主に WG1 と WG2 において議論を実施。

<sup>35</sup> API サンドボックスプロジェクトで実装した具体的な追加サービス事例は、本冊 3.2 の BOX を参照。

追加サービスに関する議論を深めていくためには、追加サービスとして何を想定するのか、提供の際には何を考慮すべきなのか、事実関係を整理することが重要
追加サービスに関する議論を深めていく上では、どのような追加サービスを念頭に置くのか、追加サービスの提供に関して考慮すべきポイントは何かといった観点から事実関係を整理することが重要である。例えば、追加サービスとして家計簿サービス等との連携を考えた場合、CBDC の取引情報を照会する機能が必要。
実装に向けては、プロトタイプを活用しつつ、データ整備や API 連携、アプリケーションベースでの識別方法等の課題解決が必要
追加サービスの実装に関して、最初から完璧なシステムを構築するのは難しいと考えられるため、まずはサンドボックスプロジェクトのようなプロトタイプを活用しながら課題を洗い出していく必要がある。お酒やタバコのように年齢制限がある商品を、ある一定年齢以上のユーザーだけが購入できる機能を実装する場合、何らかの形でユーザーの年齢データを取得する必要があり、システムの構築だけではなく、データ整備の必要性も検討すべきだろう。
商品毎に CBDC の用途制限を設けるのは、実装の難易度が相当高いと思われる。例えば、現状、法人向けクレジットカードの利用先を飲食店に限定することが可能なのは、クレジットカード会社が加盟店に付している加盟店カテゴリーコードをもとに、店舗ベースでの利用制限を課しているからである。仮に CBDC の追加サービスにおいて、商品毎に用途制限を課す場合、POS システムにおける商品データ群を利用する必要があり、データ形式や API 連携、決済アプリでの識別方法等が課題になると考えられる。
追加サービスの提供を持続可能とする仕組みの構築が必要
追加サービスの提供をすべて民間事業者に委ねると、CBDC エコシステムが長続きしない可能性がある。公的機関も含めて、追加サービス基盤の改善を継続していくために必要な人的・金銭的リソースを確保できる仕組みを構築しておく必要がある。
CBDC エコシステムの発展にとっては API の開発容易性が重要
API は常にメンテナンスやアップデートをしていかなければならないし、ライブラリや各種ドキュメント、それらを含めた SDK (Software Development Kit、ソフトウェア開発キット) を更新していかなければならない。プロトタイプの段階ではここまで意識しなくて良いと思うが、実装段階においては事業者の開発容易性が、CBDC エコシステムの発展にとって重要である。
エンジニアファーストを意識している API はよく利用される。

### 3.4 プログラマビリティ<sup>36</sup>

CBDCエコシステムにおけるプログラマビリティに関しては、APIサンドボックスプロジェクトで参加企業が実装した機能等を踏まえながら、様々なユースケースや可能性について活発な議論が行われた。まず、事業者の取りはぐれリスクを回避するための方策として「エスクロー機能」に対するニーズが指摘されたほか、利用可能なエリアの制限（いわゆる地域通貨）や、お酒・タバコ等の特定品目の購入を制限する「用途制限機能」（パーパスバウンドマネー）についてのニーズや社会実装時の検討課題が議論された。また、プログラマブルペイメント（条件付き支払い）とプログラマブルマネー（マネー自体がプログラム可能であること）については分けて議論することが重要であり、追加サービスの観点からは前者について議論することが必要との指摘があった。このほか、CBDCシステムそのものにプログラムを組み込むことはセキュリティ上のリスクを伴うため、アプリ等CBDCシステムの外側で実現する仕組みである「外部プログラム方式」が望ましいとの指摘がなされた。

（表3-8）プログラマビリティ

<p>「エスクロー機能」は、実装により現金やカード決済の未収リスクや入金遅延を回避できることから、一定のニーズが見込まれる</p>
<p>出前を現金で決済する場合、注文を受けた小売店は、購入者から代金を回収するまでの間、代金未収リスクを負うこととなるが、エスクロー機能を使えば、事前に資金を確保できるため、代金未収リスクを回避できる。</p>
<p>クレジットカードやデビットカードを用いた決済の場合、資金の受け手は即時に資金を受け取ることはできず、カード会社が定めた入金サイクルに応じて資金を受け取るが、CBDCの場合、資金の受け手に即時着金され、当該資金をすぐに別の支払いに利用できる点が大きく異なる。BIS イノベーションHubとイングランド銀行が共同で取り組んだ「Project Rosalind」では、役務の提供と資金の入金がずれることに伴うリスクを回避するために、資金を事前に取り置く「エスクロー機能」を実装した。</p>
<p>用途制限機能の実装には様々なパターンが考えられ、論点は多岐にわたる。POSシステムとの連動やAIの活用により実装可能性はあるが、プライバシーの問題も含めて課題は多い。</p>
<p>用途制限機能と一言でいっても様々なパターンが考えられ、購入対象物を制限するケースもあれば、地域通貨のように利用できる地域を制限するケースもあり、どこまで考えるかという論点がある。</p>

<sup>36</sup> 本項については、主にWG2やAPIサンドボックスプロジェクトにおいて議論を実施。

	<p>用途制限を厳密に設定しようとする、事前に設定しておくべき内容が多岐にわたるため、その実装は容易ではないかもしれない。他方、AI を活用することで簡易的な形で用途制限を実現できるかもしれない。例えば、レシート情報をアプリケーションで読み込み、AI で品目を判定するような仕組みが考えられる。</p>
	<p>現在でも民間決済事業者が、特定の商品の購入者に対して割り増したポイントを付与するキャンペーンを実施するケースがあるが、これは JAN コード (Japanese Article Number) 等を活用して実現しているのだろう。こうした方法で用途制限機能を実装できるかもしれない。ただ、決済データだけでなく、商品データも仲介機関が見られるとなると、プライバシーが問題となるかもしれない。</p>
<p>プログラマブルペイメントとプログラマブルマネーは分けて議論する必要</p>	
	<p>支払い手続きをプログラムすることで条件付き支払いを可能にする「プログラマブルペイメント」と、マネーそのものにプログラムが組み込まれ制御される「プログラマブルマネー」は分けて考える必要。前者に関しては、マネー自体をプログラムするのではなく、マネーの外側でシステムを用いて動きを制御するイメージ。例えば欧州では、「プログラマブルペイメント」については検討がなされている一方、「プログラマブルマネー」については否定的。一言に「プログラマビリティ」といっても様々な実装方法が考えられるため、しっかりと切り分けて議論をする必要。</p>
<p>CBDC システムのセキュリティ上のリスクを考慮し、高度な決済機能は CBDC システム外のアプリ等で実現する外部プログラム方式が適当</p>	
	<p>CBDC システムにプログラムを組み込むのはセキュリティ上のリスクを伴うため、決済機能を高度化するに当たっては、アプリ等 CBDC システムの外側の仕組みで実現することが適当ではないか。</p>

## 4. 相互運用性と水平的共存

### 【第4章の概要】

CBDC の社会実装に当たっては、既存の決済手段（現金、銀行預金、資金移動業マネーや前払式支払手段等の民間デジタルマネー）との相互運用や共存のあり方について検討する必要があり、既存のビジネスへの影響に配慮しつつ、公的インフラとしてデジタル決済・サービスの利活用促進や異なる決済手段の相互運用等をサポートするといった役割が期待されている<sup>37</sup>。本章では、CBDC と現金や銀行預金、民間デジタルマネーとの相互運用性と水平的共存について論点を整理する。

現金との関係について、CBDC 発行後当面の間は、CBDC 未対応の店舗での決済や災害対応等の場面で、CBDC を現金に交換するニーズが存在しうると指摘された。このほか、ATM を経由した現金と CBDC の交換方法が複数検討され、いずれの方法でも勘定系システムの更新等が不可避であることや、CBDC に関する仕様や既存の金融機関の ATM の仕様によっても ATM や勘定系システムの改修コストは変動しうる点が指摘された。

銀行預金との関係について、CBDC システムと金融機関の勘定系システム等の接続方式の検討のため、参考としうる既存の外部インフラ・システムが参加者より紹介された。その上で、既存の仕組みを用いて CBDC の払出・受入を行う場合、一時的に仮勘定を立てたり、事後に精算を行うといった処理が必要となる可能性や、既存の勘定系システムに対しても一定程度の追加改修は避けがたいこと等が指摘された。また既存のネットワーク系を活用した CBDC システムと既存勘定系システムの接続のほかに、新規に接続方式を構築することも考えうるといった指摘がなされた。このほか、CBDC が 24/365 に対応する場合、金融機関の既存の勘定系システムが 24/365 に対応していないことを考慮する必要があることや、他行の預金口座等を用いた CBDC の払出・受入にも対応していた方がユーザーの利便性は高いといった点にも言及がなされた。

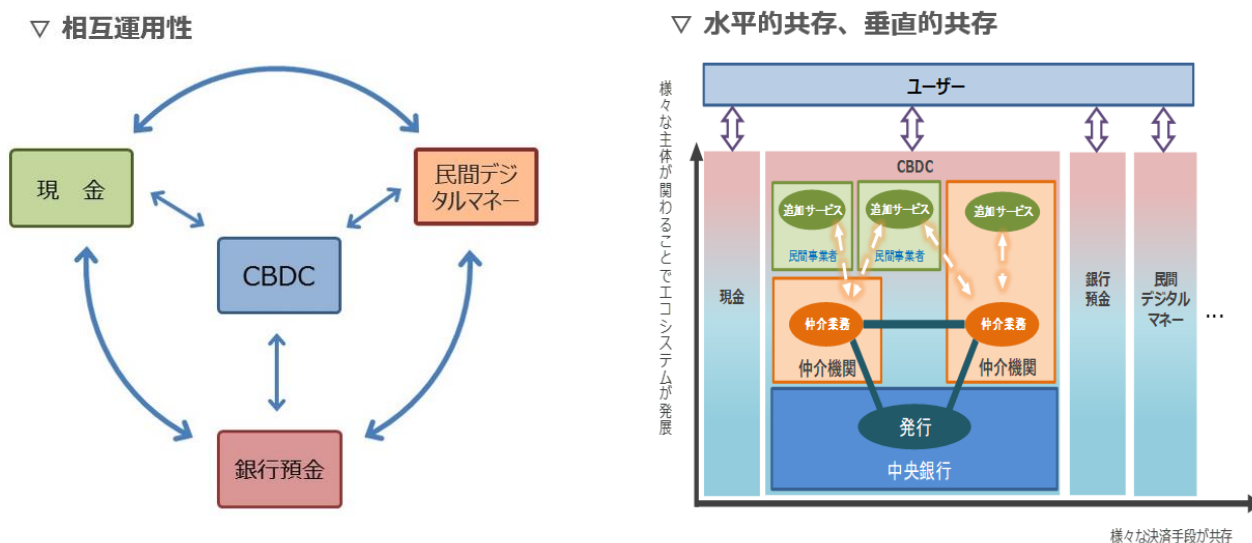
民間デジタルマネーとの関係について、民間決済ビジネスの現状を前提とした CBDC が果たしうる役割に関し、民間デジタルマネーのファンドソースやキャッシュレス決済手段同士のブリッジ等の役割や、キャッシュレス市場の拡大等への寄与を

<sup>37</sup> CBDC（中央銀行デジタル通貨）に関する関係府省庁・日本銀行連絡会議「第2次中間整理」（[https://www.mof.go.jp/about\\_mof/councils/meeting\\_of\\_cbdcre/index.html](https://www.mof.go.jp/about_mof/councils/meeting_of_cbdcre/index.html)）21頁を参照。

期待する声が聞かれた。また、CBDC の機能や役割次第では、民間デジタルマネーのイノベーションを促進しう一方、既存のビジネスモデル（収益・コスト構造）への変化も想定されることから、CBDC の交換や支払い等に一定の制限等を設ける可能性も指摘された。このほか、決済事業者（前払式支払手段取扱業者、資金移動業者等）が仲介機関を担う場合の論点についても議論された。

このほか、CBDC の発行・流通過程で生じるコストの担い手や方法について、民間決済ビジネスの取組み等を整理しながら検討していく必要性が指摘されたほか、CBDC を社会実装するに当たって、既存の決済におけるネットワーク・インフラを活用する可能性と課題についても議論を行った。

(図 4 - 1) 相互運用性と水平的共存



#### 4.1 現金との関係<sup>38</sup>

##### (現金と CBDC を交換するニーズ)

現金と CBDC を交換するニーズは、CBDC の使用が一般的になるにつれて低下する可能性がある等、CBDC の普及度合いによって変わりうるが、少なくとも CBDC 発行後当面の間は、両者を交換するニーズが一定程度存在すると考えられるとの指摘があった。また、CBDC 未対応の店舗での決済や災害対応等の場面で、CBDC を現金に交

<sup>38</sup> 現金と CBDC の交換については、主に WG7 の第 2 回および第 3 回会合において議論を実施。

換するニーズが存在しうると指摘された。一方で、預金と現金および預金と CBDC の交換チャンネルも存在するもとでは、現金と CBDC を直接交換するニーズがどの程度存在するかは不透明である、との声も聞かれた。このほか、CBDC の導入直後は現金が引き続き使用可能であるとすれば、発行当初の CBDC が現金のあらゆる特性を備えている必要はないのではないかと指摘もなされた。

(表 4 - 1) 現金と CBDC を交換するニーズ

現金と CBDC を交換する必要性は、CBDC の普及度合いによって変わりうる	
	現金と CBDC の交換チャンネルは、少なくとも CBDC 導入当初は必要。一方で、CBDC での給与受取りや店舗決済が一般的になれば、その必要性は低下する可能性。
	CBDC が普及していくにつれて現金の需要が減少する可能性はあるが、CBDC 未対応の店舗での決済等で現金が必要となる可能性は残るため、現金と CBDC を交換するニーズは一定程度残り続けるだろう。
災害時に CBDC を現金に交換するニーズが生じる可能性がある	
	停電時等に現金のみ使えるとなった場合等には、CBDC を現金に交換するニーズがあるのではないかと。
現金で支払いを行った際のおつりを CBDC で受け取るニーズもあるのではないかと	
	紙幣で支払いを行った際の硬貨でのおつりを CBDC で受け取るニーズもあるのではないかと。硬貨が不要となれば、社会全体の硬貨の管理コストが下げられるかもしれない。
預金と現金、預金と CBDC の交換が可能である場合、現金と CBDC を交換するニーズがどの程度あるかは不透明	
	預金口座と CBDC 口座をいずれも保有している前提に立つと、現金が必要な場合は預金口座から引き出せば良く、CBDC で現金を引き出すニーズがどこまであるか不透明である。
	既存の仕組みを活用する観点からは、現金をユーザーの預金口座に入金し、当該預金を CBDC と交換する方法もある。
CBDC が、発行当初から現金のあらゆる役割を担う必要はないのではないかと	
	日本銀行券を当面残すのであれば、CBDC が発行当初から現金のあらゆる役割を担う必要はないのではないかと。

## (現金と CBDC の交換方法と実装コスト)

現金と CBDC の交換は、現金の保有主体と CBDC の保有主体との間で ATM 等のデバイスを介して行う CBDC の順送金や逆引送金の一類型との整理を前提に、ATM を利用した現金と CBDC の交換のフローについて議論を行った。

現金と CBDC の交換方法として、金融機関の勘定系システムにあるユーザーの預金口座を介して CBDC に交換する方法のほか、ユーザーの預金口座は介さないが、勘定系システムは処理電文の中継のみを行う方法や、そもそも勘定系システム自体を経由しない方法が示された。他方、いずれの方法であっても勘定系システムの改修が不可避であることが指摘された。また、勘定系システムの改修コストは、エンドポイントデバイス等にかかる CBDC の仕様のほか、ATM の仕様によっても変わりうる点が指摘された。

(表 4 - 2) 現金と CBDC の交換方法と実装コスト

現金と CBDC の交換は、CBDC の順送金や逆引送金の一類型と整理可能	
	現金と CBDC の交換は、現金の保有主体と CBDC の保有主体との間で ATM 等のデバイスを介して行う CBDC の順送金や逆引送金の一類型と整理できる。
勘定系システムにあるユーザーの預金口座を介して現金と CBDC を交換することで勘定系システムの改修コストを下げることも考えられる	
	現金と CBDC の交換において、現金⇄預金口座⇄CBDC という形で預金口座を介する方法とすることで、勘定系システムへの影響を小さくすることができるのではないかと。
	預金口座を用いた現金と CBDC の交換では、預金口座残高は一時的に増額されたのち、すぐに増額分だけ減額されることが想定されるが、これは預金口座が増額された後の処理として、預金口座から CBDC の払出が行われていると考えることができる。
	預金口座を介して現金と CBDC を交換する場合であっても、ユーザーとしては預金取引をしているとの認識は持たないと考えられるため、預金の取引履歴が記録されると、ユーザー視点では不自然に映るかもしれない。
ユーザーの預金口座は介さないが、勘定系システムは処理電文の中継のみを行ったり、そもそも勘定系システム自体を経由しない方法も考えられる	
	ユーザーの預金口座を介することなく、勘定系システムが処理電文の中継のみを行う方法も考えられる。

	<p>そもそも勘定系システム自体を経由せずに、ATM と CBDC の顧客管理システムとを直接つなぐ仕組みも考えられる。ただし、この場合であっても現金の入出金に伴う残高の管理のために ATM と勘定系システムとの間の連携は必要となると考えられる中、ATM と勘定系システムの接続仕様は金融機関により異なっているため、こうした点を考慮した設計が必要となる。</p>
<p>ATM を用いて現金と CBDC を交換する場合、勘定系システムで何らかの処理が生じることは避けがたく、結果として勘定系システムの改修は不可避</p>	
	<p>ATM を介して取引される現金の処理は勘定系システムで行っているため、ATM で現金と CBDC を交換する仕組みを構築する場合は、勘定系システム側で何らかの対応が必要。</p>
	<p>ATM で現金と CBDC を交換する場合、ATM の中を流れる電文の改修等が発生するものと予想されるが、これは当該 ATM を保有している金融機関の勘定系システムの改修につながる。</p>
<p>エンドポイントデバイス等にかかる CBDC の仕様のほか、ATM の仕様によっても ATM や勘定系システムの改修コストは変わりうる</p>	
	<p>多くの金融機関の ATM ではスマートフォンを用いた取引が実現されていない中、CBDC がスマートフォンを用いる前提となれば、ATM にスマートフォン対応の機能を実装する必要がある。このためのハード面での対応コストは大きくなるだろう。</p>
	<p>ATM を用いて現金と CBDC の交換を行うには、当該 ATM が、一部の流通系 ATM でみられるような電子マネー事業者との外部接続を前提とした設計となっている必要がある。</p>

## 4.2 銀行預金との関係<sup>39</sup>

銀行預金は、ユーザーが CBDC を入手する原資として典型的に想定されるものの一つである。このため、CBDC システムと金融機関の勘定系システムや API 基盤との相互運用性を確保することは、CBDC を社会実装する上で重要な論点となる。

会合では、CBDC システムと勘定系システム等の接続方式を検討するために参考となりうる既存の外部インフラ・システムとして、全銀システム、CAFIS、CARDNET、ことらシステム、API 基盤、J-Debit、統合 ATM 等が紹介された。その上で、CBDC シ

<sup>39</sup> 銀行預金との関係については、主に WG1 の第 1～8 回会合において議論を実施。

システムと金融機関の既存の勘定系システムやAPI基盤を接続することを念頭に、CBDCの払出・受入の処理フローや、24/365対応を想定した場合の留意事項、CBDC口座を有する仲介機関以外にある預金口座等を用いたCBDCの払出・受入についての対応等の論点について議論が行われた。

CBDCの払出・受入の処理フローについて、既存の仕組みを用いてCBDCの払出・受入を検討する場合、一時的に仮勘定を立てたり、事後に精算を行うといった処理が必要となる可能性が指摘された。また、CBDCの払出・受入機能を既存の仕組みを用いて実装する場合、勘定系システムの改修は避けがたいことや、トランザクションにかかるレイテンシーが長くなるとUXが低下する可能性が指摘された。

CBDCシステムと勘定系システムの接続方式については、複数の接続方式があり、それぞれに優劣や課題があることから、統一するよりかはいずれからを選択可能とすることも考えられるとの指摘がなされた。また、既存のネットワーク系を活用してCBDCシステムと勘定系システムを接続できる可能性がある一方で、ネットワーク構成をシンプルにする観点から、新しいネットワーク系を構築することも考えうるといった議論もみられた。

また、CBDCの機能として、24/365対応を求めることを想定する場合、金融機関の勘定系システムには24/365に対応していないものもあることを踏まえた対応が必要になることが指摘されたほか、CBDC口座を有する仲介機関以外にある預金口座等を用いたCBDCの払出・受入にも対応していた方がユーザーの利便性は高まるといった意見も示された。

(表4-3) CBDCの払出・受入にかかる処理フロー

既存の仕組みを用いてCBDCの払出・受入を検討する場合、一時的に仮勘定を立てたり、事後に精算を行うといった処理が必要となる可能性
既存の決済サービスを参考にしつつ、CBDCの払出(受入)の処理を検討する場合、勘定系システム内部の処理は、CBDCの払出(受入)時点ではユーザーの預金口座を減額(増額)しつつ仮受金(仮払金)を増額(減額)し、勘定締めタイミングで精算を行う処理が考えられる。
即時グロス決済により処理されている1億円以上の他行宛振込の処理フローでは、ユーザーの預金の減少とあわせて未決済為替借が発生する。こうしたフローをCBDCの

	<p>払出・受入に応用するならば、当該未決済為替借を自己口の CBDC 残高と相殺することになるか。</p>
	<p>他行にある CBDC 口座への払出のために自行にある預金口座を減額する際、自行の勘定系システムにおいて仮勘定を建てる必要がある。</p>
<p>CBDC の払出・受入機能を既存の仕組みを用いて実装する場合、勘定系システムの改修は避けがたい</p>	
	<p>CBDC の払出・受入機能を実装する場合、勘定系システムのシステム刷新までは必要ないが、改修は必要になると考えられる。もっとも、運用面での負荷等も含めたコストがどうなるかなど、費用対効果についての詳細な検討は必要。</p>
<p>CBDC の受入については、CBDC 台帳の書換え後に勘定系の処理を行うため、エラー防止の方法を検討しておく必要</p>	
	<p>CBDC システムから勘定系システムに指示電文が飛ぶタイミングが、払出では CBDC 台帳の書換え前である一方、受入では CBDC 台帳の書換え後となる。顧客の普通預金取引を制限しているケースでは、CBDC 台帳の書換え後にエラーが発生しないようにするためには、台帳の書換え前にエラーチェックを行うか、エラーとなった後に CBDC の取引を取り消す処理を行う必要があると思われる。</p>
<p>CBDC の払出・受入について、トランザクションにかかるレイテンシーが長くなると、UX が低下する可能性</p>	
	<p>CBDC の払出・受入にかかるすべての処理が完了してから、ユーザーのデバイスに処理結果を表示すると仮定すると、トランザクションにかかるレイテンシーが長くなり、UX が低下する可能性がある。</p>

(表 4-4) CBDC システムと勘定系システムの接続方式に関する論点

<p>CBDC システムと勘定系の接続方式が複数ある中、それぞれの方式には優劣や課題があることを考慮すると、統一するよりかはいずれかを選択可能とすることも一案</p>	
	<p>仲介機関になりうる金融機関の多くが、Open API への対応を通じて API 接続の基盤を既に有しており、CBDC システムとの接続において、API を活用することは十分ありうる選択肢。もっとも、接続方式は複数あり、それぞれに優劣や課題があることを考慮すると、接続方式は API のみに絞るのではなく、いずれかを選択可能とするのが適切である。</p>

既存のネットワーク系を活用して接続できる可能性がある一方、ネットワーク構成をシンプルにする観点から、新しいネットワーク系を構築することも一案

既存のネットワーク系を活用して CBDC において必要とされる機能を実現できる可能性はある。一方で、CBDC と勘定系システムの接続方式について、既存システムとの依存関係等の観点から、ネットワーク構成をできるだけシンプルにすることが重要と考えるのであれば、CBDC システム用に新しい外部ネットワーク系を構築することが望ましいとの見方もありうる。

(表 4 - 5) CBDC の機能として、24/365 対応を求める場合の論点

CBDC の 24/365 対応を前提とする場合、金融機関の勘定系システムや API 基盤には 24/365 対応していないものもある点に注意が必要

CBDC は 24 時間 365 日稼働が必要となりうるが、勘定系システムには停止時間があり、停止中の挙動は整理が必要。

CBDC システムが 24 時間 365 日稼働であったとしても、勘定系システムにはオンライン停止時間が存在するため、払出・受入ができない時間ができてしまう。こうした時間の管理や、当該時間帯の処理を検討する必要があるかもしれない。

(表 4 - 6) CBDC 口座を有する仲介機関以外にある預金口座等を用いた CBDC の払出・受入

CBDC 口座を有する仲介機関以外にある預金口座等を用いた払出・受入にも対応していた方がユーザーの利便性は高まる

銀行 A 自身が CBDC の受入・払出に対応していないとしても、銀行 A にあるユーザーの預金口座から他の仲介機関に開設した同ユーザーの CBDC 口座に CBDC を払い出すことができれば、ユーザーの利便性は高まる。

### 4.3 民間デジタルマネーとの関係<sup>40</sup>

#### (民間決済ビジネスの現状を踏まえた CBDC に期待される役割)

民間決済ビジネスの現状を踏まえると、CBDC が民間デジタルマネー（資金移動業マネー、前払式支払手段等）と共存するには、民間デジタルマネーが抱える課題の解決や、決済事業者がカバーできない領域を担うことなどが期待される。こうした観点から、CBDC に民間デジタルマネーのファンドソースやキャッシュレス決済手段同士のブリッジ（中継）、民間デジタルマネーの（災害時・障害時等における）バックアップといった役割を求める意見や、民間デジタルマネーの性能改善やコストダウン、ひいてはキャッシュレス市場の拡大等に寄与することを期待する声が聞かれた。

(表 4 - 7) 民間決済ビジネスの現状を踏まえた CBDC に期待される役割

CBDC には民間デジタルマネーのファンドソースとしての役割を期待	
	日本では、民間デジタルマネーにあらかじめチャージして支払う方法が広く使われている。こうした事情を踏まえると CBDC を民間デジタルマネーのファンディングソースとして活用することで、民間デジタルマネーへのチャージコストの削減や利便性向上が期待できる。
	CBDC をあらゆる民間デジタルマネーと交換できる仕組みを作り、実際の支払いではよく使っている民間デジタルマネーを使うこととすれば、加盟店としては、既存の決済端末や加盟店契約をそのまま使用でき、負担の増大を回避できる
CBDC は民間デジタルマネーを「ブリッジ（中継）」する役割を担う	
	多様な決済手段が連携・共存するには、デジタルなバリューを用いて、様々なキャッシュレス決済手段の間を「ブリッジ」（中継）する機能が必要。
	相互運用性を向上させるためには、「ブリッジ」の機能は、一事業者のサービスとしてではなく、公的なインフラにおいて提供されることが望ましい。
	現行の法規制では、前払式支払手段については、原則として現金への出金ができない。CBDC への出金も同様にできないとなれば、相互交換は実現しない。
	デバイスに内蔵された IC チップでバリューを管理するケースを想定したとき、オフライン環境下で使用される当該バリューからの多重払いを防ぐため、あらかじめ CBDC

<sup>40</sup>主に WG 6 の各会合において議論を実施。

	<p>のインフラにおいて、当該バリューでの送金・支払に使用する残高に相当する額をいったん「確保」（ホールド）しておく機能を設けることはできないか。</p>
<p>CBDC が民間デジタルマネーと他のデジタル資産を仲立ちする役割を果たす可能性</p>	<p>CBDC は、民間デジタルマネーと他のデジタル資産を交換する際に、それらをつなぐ役割を果たす可能性もある。</p>
<p>CBDC には、民間デジタルマネーの（災害時・障害時等における）バックアップとしての役割を期待</p>	<p>他のキャッシュレス決済手段においてサーバーダウンが起こった時等に使う避難的インフラとして、CBDC を位置付けるというアイデアもある。</p> <p>通信障害や災害時にも問題なく使える決済インフラを決済事業者のみで構築するのは、ビジネス上難しい。いつ発生するかもわからない事象に備える観点からは、CBDC のように公的な決済インフラの存在はありがたい。</p>
<p>CBDC の活用が民間デジタルマネーの機能や性能の改善、コストダウンにつながると良い</p>	<p>CBDC を活用することで、決済事業者が加盟店に対して、決済コストの削減やスピードアップを含めた、より多くの価値を提供できるようになると良い。</p> <p>CBDC は地域通貨を下支えする基盤として、使い勝手の良いものになりうる。</p> <p>CBDC には、①必要な情報が提供され、交通インフラの維持やユーザー・店舗へのサービス向上に活用できること、②安全で安価なネットワークが用意され、ユーザー・店舗・決済事業者が負担するコストが低廉であること、③訪日外国人が外国の CBDC とわが国の CBDC を交換できること、を期待する。</p> <p>前払式支払手段取扱業者や資金移動業者はリカーリング（継続課金）するために銀行やカード会社と連携する必要がある。CBDC が同機能を備えている場合、民間デジタルマネーの弱点を補う存在になりうる。</p>
<p>CBDC を活用してユーザー、店舗、決済事業者が過度なコストを負わないサービスを考え、CBDC をきっかけとしたキャッシュレス決済市場全体の拡大につながると良い</p>	<p>CBDC をきっかけに現金主義の店舗が他のキャッシュレス決済手段を取り入れるようになるかもしれないし、CBDC の導入がキャッシュレス決済市場全体の底上げに寄与するのであれば、決済事業者としても意義のあることだと思う。CBDC を活用し、ユーザー、店舗、決済事業者の皆が過度なコストを負わない形で、自律性、持続可能性のある新たな決済スキームを考えたい。</p>

## (CBDC の利用パターン)

店舗決済においてユーザーが保有している CBDC を利用する方法について、会合では3つのパターン（（表4-8）参照）を想定して議論を行った。それぞれのパターンの違いとして、①店舗が決済事業者と結ぶ契約（決済代金の精算フローやサイクル等）、②ユーザーが使用するアプリ（CBDC 専用アプリか、民間決済アプリか）、③店舗が受け取る負債の性質（決済事業者の負債か、中央銀行の負債か）等がある。また、利得性の観点から、ユーザーが CBDC と民間デジタルマネーを使い分ける可能性が指摘された。

(表4-8) CBDC の利用パターン

<p>ユーザーが店舗で支払いを行う場面において、ユーザーが保有する CBDC の利用パターンとして、以下の3つのパターンが考えられる</p>
<p>パターン A：ユーザーは、店舗への支払いの前に CBDC を対価に民間デジタルマネーをチャージした上で、店舗での支払いは民間デジタルマネーで行う。店舗は、民間デジタルマネーを受け取る。</p>
<p>パターン B：ユーザーは、CBDC の仲介機関が用意するアプリを使用して CBDC を店舗に支払う。店舗は、CBDC を受け取る。</p>
<p>パターン C：ユーザーは、民間デジタルマネーのアプリを使用して CBDC を店舗に支払う。店舗は、CBDC を受け取る。</p>
<p>CBDC の利用パターンによって、店舗が決済事業者と締結する契約が異なり、決済代金の精算フローやサイクルが異なりうる</p>
<p>店舗での支払いを民間デジタルマネーで行うパターン A では、CBDC の即時決済性という特徴を最大限に活かすことができない。</p>
<p>店舗が CBDC を受け取るパターンは、店舗が決済事業者と結ぶ契約に着目し、CBDC の仲介機関が店舗と契約する場合はパターン B、民間デジタルマネーの加盟店契約であればパターン C と整理。このように整理すると、パターン C では、決済代金の精算フローやサイクルは加盟店契約に基づく（加盟店にはリアルタイム着金しない）可能性。</p>
<p>CBDC の利用パターンによって、UI（CBDC 専用アプリか、民間決済アプリか）が異なりうる</p>
<p>パターン A とパターン C は、事前に民間デジタルマネーをチャージして支払う現行のフローと変わらない使い方である点がメリットになりうる。パターン B は、既存の民</p>

	間デジタルマネーのアプリを用いないことから、現金決済を志向しているユーザーにも利用してもらいやすい可能性がある。
CBDC の利用パターンによって、店舗が受け取る負債の性質（決済事業者の負債か、中央銀行の負債か）が異なりうる	
	パターンCのような形で CBDC が活用可能であれば、事業者が自社の負債としてのマネーを発行することなく、事業者として必要なニーズを満たせるようになるだろう。この点を踏まえると、CBDC が、地域限定型マネー等の新たなサービスを立ち上げる際のコストを下げつつ、デジタル化や UX 向上を支える共通の決済基盤になることも期待できる。
利得性の観点で、CBDC と民間デジタルマネーを使い分ける可能性	
	利得性の観点から、ポイントが付与される民間デジタルマネーを使える店舗ではそれを使い、使えない店舗では CBDC を使う、という共存のあり方が考えられる。

### （民間決済ビジネスへの影響）

CBDC は、その役割や機能を通じて、決済事業者の競争やイノベーションを促進することが期待される。会合では、送金・支払に使用する残高に相当する額をいったん確保（ホールド）しておく「残高確保」機能等を例に、これまでの民間デジタルマネーが提供できなかった UX の実現可能性について議論が行われた。

一方、CBDC によって民間デジタルマネーの交換が容易になる場合には、既存のビジネスモデル（収益・コスト構造）が変化する可能性がある。例えば、CBDC が民間デジタルマネーのファンドソースとしての役割を担うことを想定すると、決済事業者は、残高のチャージ等の場面では差別化が難しくなり、別のサービスレイヤーで競合することが想定される。CBDC に即時決済性を設ける場合には、決済代金の加盟店への振込みを即時ではなくまとめて行っている既存の民間デジタルマネーのビジネスに影響が生じうるとの声も聞かれた。

会合では、こうした点を踏まえて、CBDC の交換や支払い等に一定の制限や絶妙な使いにくさを設ける可能性についても議論がなされた。

(表 4 - 9) CBDC が決済事業者の競争やイノベーション促進する可能性

CBDC が決済事業者の競争やイノベーションを促すことが期待される
CBDC が導入されれば、口座数拡大に向けた競争やイノベーションが進展し、新たなサービスが生まれたりすると思う。
各決済事業者の得意とする領域や、目指している方向性は様々。各社の強みを活かして競争することで、結果的にユーザーにもメリットがあるサービスが生まれる。
CBDC に「残高確保」機能が備われば、民間デジタルマネーがこれまで提供できなかった UX を実現できるかもしれない
CBDC の機能として、送金・支払に使用する残高に相当する額をいったん確保（ホールド）しておく機能が備われば、例えば鉄道運賃等のケースにおいて、①残高不足の可能性のある限り改札で入場させない、②ホテルの「デポジット」のように一定金額 + $\alpha$ の金額をあらかじめ確保しておく、③「ブリッジ」機能を活用して他のキャッシュレス決済手段の残高も含めてあらかじめ確保しておく、④残高が不足したら下車駅でチャージする、といった対応が可能となる。CBDC の「残高確保」機能を含む「ブリッジ」機能が社会インフラとして提供されれば、以上の「民間事業者が実現したくても実現できなかった何か」を実現しうる環境が整う可能性。

(表 4 - 10) CBDC 発行に伴う既存のビジネスモデルへの影響

CBDC によって民間デジタルマネー同士の交換が容易になる場合、既存のビジネスモデル（収益・コスト構造）が変化する可能性がある
CBDC を介することで民間デジタルマネー同士の交換が容易になった場合、店舗決済等の場面で選ばれにくい決済事業者の収益機会は減少していく可能性。
交換容易性が高まると、民間デジタルマネーが土管化するリスクがある。決済事業者は銀行にチャージのコストを支払っており、自社の加盟店で使用された場合は手数料を収受してコストを回収できるが、手数料無料で CBDC に転換され出金された場合には、コストを回収できない可能性がある。
CBDC が民間デジタルマネーと同等の利便性を持つと、CBDC に利用が集中し、民間キャッシュレス決済のビジネスモデルにリスクが生じる可能性。
CBDC がファンドソースとしての役割を担う場合、決済事業者は、別のサービスレイヤーで競い合うのだろう
CBDC を民間デジタルマネーの「ファンディングソース」と位置づける場合には、残高をチャージする部分では差がつかなくなるため、各社はそれ以外のところで差別化を図るのだろう。

「ファンディングソース」や「ブリッジ」の部分での差別化は期待しないが、別のサービスレイヤーで各決済事業者が工夫できる余地を与えることが望ましい。
CBDC に即時決済性を設ける場合には、決済代金の加盟店への振込みを即時ではなくまとめて行っている既存の民間デジタルマネーのビジネスに影響が生じうる
民間デジタルマネーによる決済代金の加盟店への振込は、月に何回といった形で、まとめて行われているのが通例である。CBDC が取引の都度、即時に店舗へ入金されるとなれば、既存の決済事業者にとっては脅威となりうる。

(表 4 -11) CBDC 発行に伴う既存のビジネスモデルへの影響と機能制限

CBDC の交換や支払いには制限を設けるべきかもしれない
民間デジタルマネーの健全な競争環境を維持するためには、CBDC を介した民間デジタルマネー同士の交換や CBDC を用いた支払い等に、一定の制限を設けるべきかもしれない。例えば、①民間事業者によるデジタルマネーから CBDC への出金に対して、決済事業者が手数料を自由に設定する、②CBDC に利息は付さず、保有金額に上限を設定し、超過した部分は銀行口座へオートスイングされる、③他人への送金や店舗等への支払い、民間デジタルマネーへのチャージについて利用上限を設ける、④日本銀行は CBDC の利用に対してリワードを提供しない、といったことが考えられる。
民間事業者が発行するデジタルマネーに、CBDC との相互交換が可能なバリューのほか、相互交換が不可能なバリュー等、複数種類のバリューを持たせてはどうか。
決済事業者に制約をかけたとしても、加盟店が CBDC を優先する可能性はある。
CBDC の利便性は民間デジタルマネーに劣る方が良い
現金の利便性には、民間デジタルマネーと比べて劣る部分もあるため、両者の棲み分けができている側面がある。CBDC が民間デジタルマネー並に優れているとなると、水平的な共存関係が崩れかねないため、CBDC には何らかの利用制限をかけるなど、「絶妙に使いにくく」してはどうか。
CBDC には「絶妙な使いにくさ」を残しておき、物足りない部分を決済事業者が担うことで対価として手数料を得る、というあり方が考えられる。
CBDC にポイントを付与しないことで、民間デジタルマネーとの共存が成立する可能性があるが、UI の設計には工夫が必要
CBDC による支払いにポイントが付かなければ、民間デジタルマネーに対する脅威が薄れ、共存関係が成立するかもしれない。

CBDC による支払いに関してはポイント等の特典が付与されないとしても、UI が既存の民間事業者によるデジタルマネーと同じである場合には、ユーザーに誤認が生じ、クレームに発展する可能性がある。

### (決済事業者が仲介機関の役割を担う場合の論点)

決済事業者が仲介機関を担う可能性についても議論がなされ、既存の顧客基盤を活かした顧客管理サービスの提供等には強みを持つ可能性が指摘された。一方、これまで決済事業者が担ってこなかった台帳管理業務等については、システム共同化等の工夫が考えられるが、こうした取組みと追加サービス等の面でのビジネスの拡張性・自主性の間にはトレードオフが存在するとの指摘がなされた。

(表 4 -12) 決済事業者が仲介機関の役割を担う場合の論点

<p>決済事業者が仲介機関を担う可能性もある。その場合、既存の顧客基盤を活かして顧客管理のサービスを提供することが考えられる</p>
<p>決済事業者のビジネス上、同業他社が仲介機関となる場合には、競合に劣後することを避けるため、自らも仲介機関業務を担う可能性。</p>
<p>決済事業者が仲介機関になった場合、既存の顧客基盤を持つことから、そのノウハウを活かして、顧客管理のサービスを提供することになると思われる。</p>
<p>決済事業者が仲介機関を担う場合、馴染みのない台帳管理業務等におけるシステムの共同化等の工夫とビジネスの拡張性・自主性のトレードオフが論点となる</p>
<p>決済事業者が既に有する顧客 ID の活用方法や、システムの共同化とビジネスの拡張性のトレードオフは、今後の論点。</p>
<p>決済事業者に馴染みのない台帳管理については、新たに共同利用センターのようなものを設立し、そこに委託するというアイデアが考えられる。もっとも、台帳管理を集約した場合、各決済事業者が何らかの機能やユースケースを追加的に実現したいと考えても、各決済事業者の要望が相反し、柔軟な対応が難しくなることも想定される。</p>

## 4.4 CBDC の発行・流通にかかるコスト負担と既存ネットワークの活用<sup>41</sup>

### (CBDC の発行・流通にかかるコスト負担のあり方)

CBDC の発行・流通においては、そこで提供される CBDC の機能に応じて様々なコストが発生することが想定される。会合では、こうしたコストを誰がどのように負担していくべきかについて、CBDC の機能によって、コストの内容は異なりうるとの指摘がなされたほか、コスト分担については、受益者負担が基本ではあるものの、個人ユーザーに負担を求めると普及の足枷になる可能性があるとの議論がなされた。また、インフラコストの負担に関する問題は、民間決済ビジネスの取組み等を整理しながら検討していく必要があるとの声が聞かれた。

(表 4 -13) CBDC の発行・流通にかかるインフラコスト負担のあり方

CBDC の機能によって、コストの内容は異なりうる
CBDC を既存の民間デジタルマネーにチャージして使用させるようなサービス展開を想定するのであれば、新規の加盟店開拓に付随するコストは不要だが、決済事業者の加盟店網が及んでいない地域にまで CBDC を行き渡らせるのであれば、加盟店の新規開拓コストが生じうる。
CBDC を受け入れる店舗は、誰が開拓していくのか
CBDC が、決済事業者のネットワークの届かない店舗まで含めて、「どこでも使える」のだとすると、誰がその店舗を開拓するのか。
サービス提供のコストは、受益者負担が基本
決済事業者は、CBDC の提供が自社の収益につながるのであればコストを負担すべきだし、店舗側も CBDC を受け入れることで集客につながったり、他の決済手段よりも手軽に導入できたりするといった利益を享受するならばコスト負担すべきだろう。
CBDC の受益者が誰になるかは、CBDC を導入する政策的な目標に依存するのではない。例えば、全国にくまなくキャッシュレス決済手段を整備することが目標ならば、社会全体が受益者となる。その場合、CBDC のコストは、通信事業におけるユニバーサルサービスコストのような形で全ユーザーが負担することとなるか。CBDC を全国で使用可能にするためのネットワーク維持にかかるコストと仲介機関のサービス

<sup>41</sup> CBDC の発行・流通にかかるコスト負担と既存ネットワークの活用については、主に WG5 の各会合や WG6 の第 7 回会合において議論を実施。

	<p>提供にかかるコストを峻別し、後者については仲介機関自身が負担したり、加盟店手数料等を通じて店舗ひいては個人ユーザーに転嫁したりする設計もありうる。</p>
<p>CBDC を「どこでも誰でも使える」ようにしようとした場合、インフラコストを受益者負担とすることは適当ではない可能性がある</p>	<p>受益者負担の原則に基づけば、個人ユーザーにも一定のコストを負担してもらうことが想定されるが、代替候補としての民間デジタルマネーが存在するもとの、通信事業者のユニバーサルサービス料や電気事業者の再生可能エネルギー発電促進賦課金のような形でコスト負担を求めると、かえって CBDC 普及の足枷となる可能性。</p> <p>個人ユーザーが無料で使えるという設計にすると、結果としてミニマムなサービスになってしまうのではないか。</p>
<p>CBDC の発行・流通にかかるインフラコスト負担のあり方は、現金や民間デジタルマネーの取組みを整理しながら検討する必要がある</p>	<p>現金は、日本銀行が発券を担い、民間銀行が流通を支えている。民間デジタルマネーは、加盟店手数料を前提に、決済事業者がコストを負担している。CBDC は、これらと比較してどう違うのか、ビジネス環境として望ましい構造を実現できるか、といった観点からインフラにかかるコスト負担のあり方を議論していくのが良い。</p> <p>仮に、CBDC の導入や利用に当たって店舗が負担する手数料の水準がゼロに設定されるならば、CBDC に比べてコスト負担が重い民間デジタルマネーを店舗が導入する動機は無くなりかねない。</p> <p>CBDC が決済事業者の加盟店網を流用するのであれば、決済事業者にとっての利益や、店舗に対する継続的なコストメリット等を議論して、サステナブルな仕組みを構築することが重要。特に、導入初期の加盟店の開拓や維持には相応のコストがかかっている点等を考慮すべき。</p>
<p>CBDC の発行・流通のためのインフラにかかるコストの一部を公的機関が負担することも考えられる</p>	<p>台帳部分の開発や維持コスト等、コストの一部を公的機関が負担することも考えられる。まず CBDC の発行・流通のためのインフラ全体の構築方針を決めた上で、どのコストを民間事業者が負い、どのコストを公的機関が負うかを議論する必要がある。</p>

## (既存の通信（電文）ネットワーク・インフラ等の活用)

CBDC を社会実装するに当たって必要となるネットワーク・インフラについて、既存の決済におけるネットワーク・インフラを活用することも考えられる。会合では、既存のネットワーク・インフラの活用が CBDC の利用促進に役立つとの指摘がなされた一方、既存のネットワーク・インフラそのものが複雑であることを踏まえた難しさについても議論され、既存ネットワークの活用と新規ネットワークの構築それぞれのメリット・デメリットを慎重に考慮する必要があるとの声が聞かれた。

(表 4 -14) 既存の通信（電文）ネットワーク・インフラ等の活用

CBDC の支払いチャネルに既存のネットワーク・インフラを活用することも考えられる。認知度の高い既存インフラを活用することが CBDC の利用促進につながる可能性もある
CBDC を店舗支払いに導入するに当たって、CBDC 用の公共ネットワークを整備する方法のほか、既存の民間ネットワークを活用する方法も考えられる。
水平的共存を考える際には、既存の決済事業者のインフラを活かすことができれば望ましい。具体的には、加盟店網や決済端末については、活用が可能かもしれない。
認知度が高い民間マネーのインフラを活用することで、CBDC の利用促進につなげるという考え方もある。
既存のネットワーク・インフラは複雑であり、網羅的に活用するのは容易ではない
既存の民間デジタルマネーは、様々なゲートウェイを使って取引を成り立たせているため、それらを網羅的に活用するのは容易ではないと思われる。
現在の日本の店舗決済端末は、多種多様な決済サービスに対応していったことで複雑化している。CBDC が、既存の店舗決済インフラを活用する形で非接触や QR コード等といった決済方式や、スマートフォンやカード等といった様々なデバイスに対応していくことを目指すのであれば、まずはこの複雑化した状況を整理する必要。
店舗側から、CBDC を用いた決済について、1つのオペレーションで様々なデバイスに対応して決済処理できるようにしてほしいというニーズが出てくるのが想定される。その際、カメラや NFC アンテナの配置といったハードウェア面が制約となることもありうるだろう。

新規ネットワークを構築する事とのメリット・デメリットを慎重に考慮する必要

既存のネットワークを活用する案は、既存のゲートウェイが持つ多くの事業者とのつながりや安定性を利用できる一方で、重厚長大なネットワークであるがゆえに、事業者が CBDC に実装していきたいと考える新規機能に柔軟に対応できるか不安。分散台帳技術等の新しい技術との相性にも疑問が残る。新興の決済事業者の立場からは、既存の民間ネットワークよりも新規の CBDC 用ネットワークの方が接続しやすい可能性もあり、両者のメリット・デメリットは慎重に評価すべき。

既存のインフラを活用する場合、同インフラのシステム障害が CBDC に波及しうる。この点について、既存の決済インフラをカスタマイズしてネットワークやシステムを分けるなどの方法で、システム障害の影響を抑えることは可能だが、カスタマイズ部分が多い場合は、新規に構築した方が良いのでは、といった議論にもなりうる。

## 5. 新たなテクノロジーと CBDC

### 【第5章の概要】

本章では、デジタルアイデンティティやオフライン決済、ブロックチェーン関連技術、その他の次世代技術等といった新たなテクノロジーの CBDC システムへの導入に向けた技術的課題や可能性に関して中長期的な観点から論点を整理する。

デジタルアイデンティティについては、身元確認に関して公的個人認証の活用を前提としながらも、新たな身分・属性証明の手法として、Verifiable Credential (VC) の利用可能性の検討が示された。

オフライン決済については、災害時等において有用な決済手段となりうるが、価値の発行者（中央銀行）と、その価値を管理するスマートフォンアプリ提供者等が異なりうる点等に留意しつつ、技術的に安全な価値移転を実現する仕組み作りが重要との声が聞かれた。また、技術的なハードルやシステム整備コストを考慮して、ディファードオフライン決済を導入する可能性についても検討がなされた。

ブロックチェーン関連技術については、計算リソースの飛躍的な向上・遍在化を背景に登場し、それらを用いた自動化やプログラマビリティが期待される形で、アセットトークナイゼーションが国内外で進展している様子が紹介された。技術的な課題として、多様なアセットのトークン化の取組みが国内外で進展している一方で、その決済手段であるマネーのトークン化が十分に進んでおらず、CBDC やトークン化預金、ステーブルコイン (SC) といった多様なマネーの可能性に関して、利便性や各種リスクのほか、流動性調達負担への対応等も考慮し検討していく必要性が指摘された。また、トークナイゼーション等の新たな決済サービスが登場する中で、サービスやシステム基盤間の相互運用性を確保するニーズも高まっており、ユースケースに応じたトラストの置き方や拡張性等を踏まえて技術選択をしていく必要性や、伝統的金融 (TradFi) と分散型金融 (DeFi) の結節点となるような技術群 (トークン規格やプライバシー保護技術、アカウントアブストラクション等) の動向も紹介された。

上記技術に限らず、新たなテクノロジーと CBDC を考えていく上では、長期的な視野にたち、中立的な技術評価や、関連する技術群をセットでみていく必要性、高速・大量なマイクロペイメント化が進むことが想定される中での実務課題を検討する必要性等が、改めて指摘された。

## 5.1 デジタルアイデンティティ<sup>42</sup>

ユーザーの属性情報の集合体であるアイデンティティをデジタル形式に変換した仕組みであるデジタルアイデンティティは、ユーザーを一意に特定することや、適切なAML/CFTを実施し、CBDCにおける取引の安全性を確保するための不可欠な基盤要素である。

この観点から、CBDCの利用開始時にはユーザーの身元確認を適切に実施し、必要な属性情報を登録した上で、CBDCの利用時には登録済みの本人であることを確認する本人認証を行うことが重要である。

身元確認に関しては、公的個人認証の活用を推す意見が多く見られた一方、様々な属性情報をデジタルアイデンティティウォレットに集約し、ユーザー自身がその属性情報を管理しながら必要に応じ選択的に開示もできる仕組みである Verifiable Credential (VC)<sup>43</sup>の活用についての言及も数多くあった。

(表5-1) デジタルアイデンティティ

身元確認には公的個人認証の活用が考えられる一方、ユーザーが自身の属性情報を管理しながらも利便性の高いサービスを楽しむという観点から、VCの活用も検討の余地
CBDCシステムでVCを利用する場合、マイナンバーカードのICチップ情報読取と同等の身元確認・本人認証保証レベル3相当となるだろう。仲介機関に提示する個人情報の範囲をユーザーが選択できることや、スマートフォン内に保存されたVCの提示のみで認証が完了させられることなど、VCならではの利点も期待できる。もっとも、取引の重要度に応じて変えるため、マイナンバーカードのパスワード入力やライブネスチェック等の要否について判断する必要があるだろう。また、VCとマイナンバーカード内電子証明書の有効期限を一致させる仕組みが求められる。このほか、例えば、所有者がマイナンバーカードを紛失した場合等に備えて、VCの無効化プロセスを設計する必要があると考えている。
VCについては、ビジネスでの利用に向けた議論が一部で進みつつあるが、個人的には本人確認は公的個人認証の利用が良いのではないかと考えている。健康保険証のマイ

<sup>42</sup> 本項については、主にWG3において議論を実施。

<sup>43</sup> Verifiable Credential (VC) は、デジタル署名による真正性確保・改ざん防止等の機能を実現することができる、「人、法人、モノ等」の「身元、資格、属性等」の情報に関する汎用的で機械可読なデータ形式・データ流通形態。(https://www.digital.go.jp/policies/trust)

<p>ナンバーカードへの一本化等によりマイナンバーカードの利用がさらに浸透すれば、個人が本人確認の際にマイナンバーカードによる公的個人認証を利用することへの意識は変わっていくだろう。VC は、マイナンバーカードには含まれない様々な情報の保持に活用するなど、棲み分けが可能と思われる。</p>
<p>VC を利用した本人確認の場合は、法律やセキュリティの観点で、現行方式と比べてどのような違いが生じるかは整理が必要だろう。</p>
<p>本人確認は、VC ではなくマイナンバーカードによる公的個人認証を利用する方が良い。ただし、EU のデジタルアイデンティティウォレット等で、金融機関や携帯キャリア等のサービス提供者が保有する様々な属性情報をデジタルアイデンティティウォレットに集めていくという考え方があり、そうした観点でも VC が今後必要とされる可能性はあるだろう。</p>
<p>ペーパーベースの地域通貨は、商品券等の形態で発行することで利用可能な地域を限定していたが、デジタル化によりウォレットで制御できるようになれば、地域だけでなく年齢でも制御できるようになるなど、ユースケースが広がるかもしれない。</p>

## 5.2 オフライン決済<sup>44</sup>

CBDC のオフライン決済は、「台帳管理システムを介さずに決済完了を可能とする決済方式」であり、システム障害に対する強靱性の向上や、台帳管理システムやネットワークへの取引処理の集中を避け、各デバイスに処理を分散させることで性能上限を解消するなどの利点をもつ。例えば BIS では「台帳システムへの接続を必要とせずに行われるデバイス間の価値移転」<sup>45</sup>とされている。パイロット実験の実験用システムの構築と検証における机上検討では、「災害時を念頭に置いた決済のレジリエンス強化」を主目的として、台帳との同期タイミングやオンライン決済システムの残高との連携方法等、技術的な観点から各種検討を行っている。

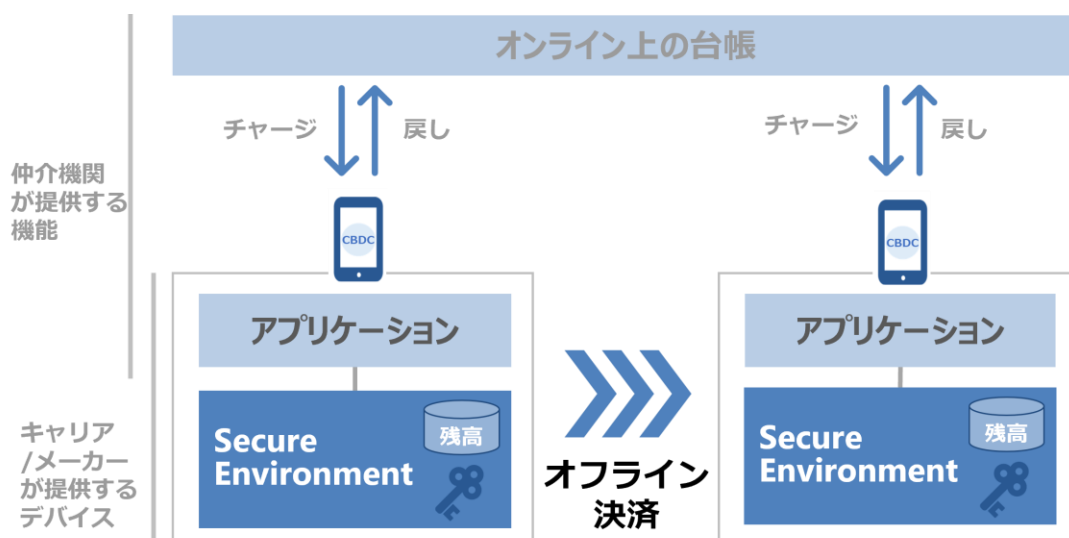
会合では、国内外の実証実験の取組みが紹介され、CBDC のオフライン決済は、災害時等において有用な決済手段となりうるが、トランザクションの有効性検証等、技術的に安全な価値移転を実現する仕組み作りが重要となることが指摘された。また、仕組み作りに当たっては、価値の発行者（中央銀行）と、その価値を管理するスマー

<sup>44</sup> オフライン決済については、主に WG4、WG5 において議論を実施。

<sup>45</sup> 2023 年の BISIH のハンドブック Project Polaris のオフライン決済の定義。

トフォンアプリ提供者等が異なりうることや、特定の決済端末でのみ利用可能とするのではなくオープンな環境で利用できるようにする必要がある点等に留意する必要があるとの声も聞かれた。また、技術的なハードルやシステム整備コストを考慮して、既に海外を中心に民間の決済サービスで利用されているディファードオフライン決済<sup>46</sup>を導入する可能性についても検討を行った。

(図5-1) CBDCを用いたオフライン決済の構造



また、新しい技術として、プラットフォームによらないプロトコルレイヤーでの標準化を志向した価値移転プロトコル<sup>47</sup>や、オフライン決済の汎用性や拡張性を向上する次世代に向けた取組みが紹介された。

(表5-2) オフライン決済に関する議論

<p>CBDC のオフライン決済は、災害時等において有用な決済手段となりうるが、トランザクションの有効性検証等、技術的に安全な価値移転を実現する仕組み作りが重要</p>
<p>価値移転プロトコルについては、オンラインの残高から価値を切り出して、オフラインでの保存や端末間送金が可能であることから、災害時等において有用な決済手段と</p>

<sup>46</sup> オフラインでの取引時に支払人と受取人のデバイス間で支払指示を送付しておき、いずれかのオンライン接続等のタイミングで台帳上の資金の移動を行う決済手法。

<sup>47</sup> 田村裕子ほか、「台帳を用いない決済方式に関する技術面からの一考察」、『金融研究』第44巻第3号、2025年 (<https://www.imes.boj.or.jp/research/abstracts/japanese/kk44-3-3.html>) を参照。

	<p>考えられる。今後の検討においては、耐タンパ性デバイスも含めた、技術的に安全な価値移転を実現する仕組み作りがポイント。</p>
	<p>例えば、価値移転プロトコルでは、価値移転プロトコルの発行者がトランザクションの有効性検証を実施するプロセスがあり、こういったトラストの役割として、金融システムが重要である。</p>
<p>制度設計に当たり、CBDC は既存の決済サービスと違い、価値の発行者とスマートフォンアプリ提供者等が異なりうるほか、オープンな環境で利用できるようにする必要</p>	<p>CBDC の場合、既存の決済サービスと違い、価値の発行者とスマートフォンアプリ提供者等が異なりうるため、安心安全にセキュアエレメントを利用できるための仕組み作りに向けて、検討すべき論点は多いと感じる。</p> <p>既存の電子マネーの決済サービスも、IC カードに価値を保管するものだが、閉じた環境や特定の決済端末のみで利用可能という前提が置かれており、誰でも価値を取り出せる仕組みにはなっていない。一方、CBDC は、よりオープン環境で利用できる必要があり、これが民間サービスにはない実装上の考慮点となる。</p>
<p>技術的なハードルやシステム整備コストを考慮すると、CBDC の即時決済性を緩和し、ディファードオフライン決済を導入することも一案。ただし、広く利用してもらいたいという側面と不正利用防止の両立といった点は課題</p>	<p>システムエラー等により、価値の移転が途中で途切れてしまった場合の対応は重要な論点。2 台のデバイスを同時に更新することは極めて難しく、情報工学的には未解決問題の一つ。こうした技術的なハードルがあるなか、万能なオフライン機能を実装するために利便性を犠牲にすることは望ましくないことから、CBDC の特徴とされる即時決済性について緩和することも一つの選択肢ではないか。</p> <p>オフライン決済を整備するためのコストの目線でも、デバイス間の価値移転による決済を前提に重厚なシステムを作りこんでしまうとコスト倒れになる可能性もある。BOE でも検討されているディファードオフライン決済の方が現実感のあるインフラではないか。</p> <p>鉄道利用者がプリペイドカード等を使って改札に入場する際の処理では、ディファードオフライン決済に似た仕組みが採用されている。もっとも、こうした取引と決済に時間差を設ける仕組みは、不正利用される可能性が高く、不正利用のリスクを誰が負担するのか、導入する店舗の業種を制限するのか、といった点が論点となりうる。</p> <p>ディファードオフライン決済によって生まれるリスクの大きさは、店舗の業種だけでなく具体的なビジネスの内容によっても変わりうる。ディファードオフライン決済の</p>

	設計に当たっては、個々の店舗が負うリスクの大きさを踏まえたリスクベースでの検討が必要となる。
	6Gで検討 <sup>48</sup> されているネットワークのエッジに隔離実行環境（TEE）の機能をもたせるインクルーシブコアといった、オフライン決済の汎用性や拡張性の向上が期待できる取組みの動向も注視していく必要
	隔離実行環境やセキュアエレメントの技術自体は以前から普及しているが、そこにインクルーシブコアという通信ネットワーク技術を組み合わせようとしている点が、これまでなかった新しさ。
	従来は、デバイス紛失の際に、その中にある価値も消失してしまう、といったことが生じがちだったが、ネットワークの中にインクルーシブコアという隔離実行環境を構築し、トークンの保持や証明書、ロジックの保護を行う仕組みを持たせることで、こうしたデバイス固有のリスクを失くすことができる。

## 5.3 ブロックチェーン関連技術

### 5.3.1 アセットトークナイゼーション<sup>49</sup>

#### （トークン化関連技術）

技術革新を背景に、アセットのトークン化（アセットトークナイゼーション）<sup>50</sup>が国内外で進展している。会合では、トークナイゼーションの背景となる技術革新の中身として、計算リソースの飛躍的な向上・遍在化によって、分散的なシステム形態が実現可能となり、ブロックチェーンやスマートコントラクトといった技術が誕生したことが挙げられる、との指摘があった。このほか、トークン化関連技術の留意点として、分散化の程度により、ブロックチェーン技術に内在するセキュリティ・ガバナンス・スケーラビリティといった課題の程度が変化すること、トークン化はブロックチェーンの利用が前提となるケースが多いものの、必ずしもブロックチェーンを利用としなくても必要なプログラマビリティが達成できる可能性もあること、などが指摘された。

<sup>48</sup> 第6世代移動通信システム（6G）におけるネットワークの高度化に向けた検討。

<sup>49</sup> アセットトークナイゼーションについては、主にWG4の第1～11回会合において議論を実施。

<sup>50</sup> トークン化の定義は様々あるが、例えばBISでは「金融資産や実物資産に関する権利を、プログラマブルなプラットフォームにおいて、デジタルに表章するプロセス」とされている。

(表 5-3) トークン化関連技術に関する議論

<p>計算リソースの飛躍的な向上・遍在化によって、分散的なシステム管理形態が実現可能となった結果、ブロックチェーンが誕生</p>
<p>ブロックチェーンの誕生には計算リソースの飛躍的な向上と遍在化が影響。リソースが貧弱な状況では、処理内容を一か所に集約して「保証」するシステムが合理的であったが、一昔前の基幹系システム以上の性能を備えたデバイスが、ネットワークに常時接続される形でリソースが遍在化した結果、複数主体の合意形成で処理内容を「検証」する分散管理システム形態が実現可能となった。</p>
<p>2009 年に Bitcoin が始動し、2015 年に Ethereum が公開されて以降のこの 10 年間、ブロックチェーンを用いたビジネスモデルと技術は、急激に増加。</p>
<p>ブロックチェーンといっても、分散化の程度によって、技術に内在するセキュリティやスケーラビリティといった課題の程度が変化</p>
<p>ブロックチェーン技術の特徴として、分散性・セキュリティ・スケーラビリティを高度なレベルで同時に成り立たせることが難しいというトリレンマが存在。</p>
<p>参加者を特定したパーミッションドブロックチェーンも、ある種の分散性を犠牲に、スケーラビリティやセキュリティを向上させている一例。</p>
<p>パーミッションドブロックチェーンの場合、既存システムに類似し責任分界は事業者間で比較的明確。一方、パブリックブロックチェーンの場合、中央集権的な運営主体の存在が排除され、より分散的なシステム構造となり、ノードやスマートコントラクトの提供・責任主体も不明確になっている点は、パーミッションドブロックチェーンとの大きな違い。</p>
<p>トークン化は、ブロックチェーンとスマートコントラクトの活用が前提となるケースが多いが、既存技術でも必要なプログラマビリティが達成できる可能性</p>
<p>Ethereum が誕生して初めて、スマートコントラクトの実行環境として、ネットワーク全体があたかも 1 つのコンピューターであるかのように振る舞う、分散アプリケーション基盤が登場。</p>
<p>Ethereum では各ノードに EVM (Ethereum Virtual Machine) と呼ばれる仮想マシンが組み込まれており、異なる環境の差異を吸収し、共通仕様のコンピューターをエミュレートして、プログラムが実行できるようになっている。</p>
<p>スマートコントラクトはアプリケーションと本質的な違いはなく、ブロックチェーン技術が採用されているプラットフォーム上のアプリケーションを指す場合が多い。</p>
<p>ブロックチェーンを用いなくても、ユースケースに応じて、スマートコントラクトで実行するようなプログラマビリティ・処理の自動化は達成しうる。</p>

## (トークン化アセット)

会合では、セキュリティトークン (ST) や MMF・担保のトークン化等、多様なアセットのトークン化の取組みが国内外で進展してきている一方で、その決済手段であるマネーのトークン化は十分には進んでいない、との指摘が聞かれた。トークン化アセットの決済手段としては、CBDC やトークン化預金・SC といった多様なマネーが用いられる可能性があるが、利便性やシステム投資負担、取りはぐれリスクやシステムリスク、オペレーショナルリスクや流動性調達負担への対応等も考慮し検討していく必要がある、との指摘があった。

(表 5-4) トークン化アセットに関する議論

国内では ST の発行実績が増えており、今後の拡大には関連業務全体の DX・効率化や、DvP 決済の実現が課題
ST は、株式・社債・受益証券発行信託等の有価証券をブロックチェーン上にトークンとして発行したもの。ブロックチェーン上で投資家情報をリアルタイムに管理できる特徴やスマートコントラクトを活用することで、従来対応が困難であった公募や私募・小口化・条件に応じた利払い自動化といった新しい商品ラインナップの拡充、ポストトレード含む業務全体の効率化等が期待される。
ST 市場の拡大に当たっては、トークン化の部分だけでなく関連する業務全体のオペレーションの DX・効率化や、決済における取りはぐれリスクの低減・DvP の実現が必要な可能性。
海外を中心に、MMF や担保のトークン化の取組みがみられる
Ethereum 上で発行された BUIDL は、米国の法律に基づき、米大手運用会社 BlackRock が運用する MMF を、米 Securitize 社が提供・管理するプラットフォーム上でトークン化し販売しているもの。主な機能として SC である USDC への即時換金や月次の分配金支払いを提供。
リーマンショック以降の国際規制強化の流れで、清算機関 (CCP) へのリスク集中が進んだ結果、CCP に預託される担保が増加し、担保資産の確保が容易でない状況となった。こうしたもと、担保をトークン化し、24/365 かつクロスボーダーでの担保管理の効率化・最適化を目指す動きが、国内外で生じている。

アセット側のトークン化は進展しているが、その決済手段のマネーのトークン化は十分には進んでいない。決済手段としての、SC や預金トークン、CBDC といったマネーの共存に当たっては、利便性やリスク・流動性効率といった点を考慮する必要

アセット側のトークン化は進展しているが、それらの決済手段のトークン化は十分に進んでいない。

システム投資負担の観点から ST の資金決済を考えると、複数の手段に対応しサイロ化するよりも、広く利用されている安全な決済手段に対応していくことが望ましい。

平時においては、決済金額が小さいほどマネーの種類はあまり意識されない傾向があるが、危機時においては、取りはぐれリスクの観点から誰の負債なのかが意識される印象。中央銀行マネーを利用するかは、こうしたリスク認識に応じて判断されるのかもしれない。

何らかのデジタル通貨を用いてリアルタイムでの DvP 決済が実現した場合、取りはぐれリスクは解消する一方、プレファンドの負担が増加する可能性には留意が必要。流動性負担が軽減されるような仕組みのセットで検討する必要。

SC 発行体は、オペレーショナルリスクやセキュリティリスクに留意する必要。包括的なリスク把握やスマートコントラクトの監査等を実施する必要。

会計処理を考えると、暗号資産や SC はバランスシートに新規計上することに伴うスイッチングコストが高いと考えられる一方で、預金トークンは既存の銀行預金と同様の取扱いで良いと考えられるため計上しやすい。

預金のトークン化に関しては、企業内のプライベートブロックチェーン上で発行し自行の顧客間で流通するものを「トークン化預金」、流通先を制限しつつもパブリックブロックチェーンで発行し自行の顧客以外にも流通する可能性のあるものを「預金トークン」と使い分けている向きがみられるが (IMF の整理等)、定義や実装方法に対する共通理解は定まっていない。CBDC や SC との連携・相互運用性は、技術面だけでなく法制度面からも、既存の仕組みとの整合性も踏まえ検討していく必要。

### 5.3.2 インターオペラビリティ<sup>51</sup>

トークナイゼーション等新たな決済サービスが登場する中で、サービスやシステム基盤間をつなぐ相互運用性を確保するニーズが高まっている。

会合では、システム間の連携手法に関し、ユースケースに応じたトラストの置き方や拡張性、プラットフォームだけでなくプロトコルレイヤーの共通化の有用性等を考慮しながら、技術選択をしていく必要性が指摘された。このほか、ガス代<sup>52</sup>やチェーン間連携、鍵管理といった Web3 特有の煩雑さを、ユーザーに意識させない工夫として、アカウントアブストラクション<sup>53</sup>といった技術の進展も紹介された。

既存システムとの連携を考える上では、TradFi と DeFi の結節点となるような機能も必要となる。例えば会合では、トークン規格で保有者制限や凍結機能等を追加することで、パブリックブロックチェーンであってもパーミションドな環境を構築する技術や、ゼロ知識証明やアクセスコントロール等で、ブロックチェーンであっても情報の透明性を調整するプライバシー保護技術が進展し始めていることが紹介された。

(表 5 - 5) インターオペラビリティに関する議論

多様な決済サービスや決済手段が登場する中で、それらを円滑につなぐ相互運用性・システム間連携ニーズが高まっている
従来の預金や預金トークン、資金移動業者が提供する決済サービス、さらには SC 等、多様な決済手段を円滑につなぐ相互運用性の実現が必須。
SC やトークン化預金といった新しい形態も登場し、決済システムのサイロ化が課題となっているため、決済システム間の相互運用性を実現していくことが、CBDC に期待される役割の一つ。

<sup>51</sup> インターオペラビリティについては、主に WG4 の第 4 回～第 11 回会合において議論を実施。なお、第 4 章の「相互運用性と水平的共存」は、既存の銀行預金や民間デジタルマネーとの制度的な相互運用性に焦点を当てている一方で、本項のインターオペラビリティは、トークナイゼーションといった新たな決済サービスを取り巻くシステムや基盤間の連携技術や、Web3 におけるマルチチェーン対応といった技術的な観点を主な対象としている。

<sup>52</sup> パブリックブロックチェーンでの取引実行時に徴収される手数料で、通常 ETH といった native token での支払が必要。

<sup>53</sup> アカウントアブストラクション（アカウント抽象化）の定義は多様なが、一般的には、ユーザーアカウントとコントラクトアカウントの差異を抽象化することで、ユーザー自身での秘密鍵管理を不要とするなど、UX を向上させる技術群を指す。

システム間の連携手法に関しては、ユースケースに応じたトラストの置き方、プラットフォームだけでなくプロトコルレイヤーの共通化の有用性等を考慮しながら、技術選択をしていく必要
DLT 基盤との主な連携技術としては、Notary 方式 <sup>54</sup> や HTLC 方式 <sup>55</sup> 、Light Client 検証方式 <sup>56</sup> があり、ユースケースに応じた技術の選定が必要。
DLT 基盤間の連携については、①信頼できる第三者の存在を前提としない安全性、②ユースケースの広がり、③ネットワーク拡張性のすべてを高いレベルでは実現すること、ができないトリレンマが存在。ユースケースに応じ、トリレンマ要素の優先度やトラストモデル等を検討し、技術選択をしていく必要。
ST の DvP 決済の技術的実現に当たっては、異なるシステム間の連携について、業務フローの工夫や信頼できる第三者を介して行うといった工夫を検討する必要。
プラットフォームレベルまでいかずとも、仕組みやルールといったプロトコルレベルでの処理の標準化・共有化が進めば、サイロ化を解消するインターオペラビリティを提供できるのかもしれない。
チェーン間連携、鍵管理といった Web3 特有の煩雑さをユーザーに意識させない工夫として、アカウントアブストラクションといった技術も進展
従来金融に匹敵する利便性・安全性を備えたウォレットの開発として、Web3 特有の複雑さ（例えば、秘密鍵の分散管理やリカバリー機能、ガス代やチェーン間ブリッジ等）をユーザーに感じさせない機能 <sup>57</sup> や、目的別のサブアカウント <sup>58</sup> 等、アカウントアブストラクションといった技術が進展している。

<sup>54</sup> 信頼ある第三者の公証人である Notary が取引の検証を行うことでブロックチェーン間の取引を実現する方式。

<sup>55</sup> Hashed Timelock Contract、暗号的ハッシュ関数とタイムアウト機能を組み合わせることで、特定の時間枠内で特定の条件が満たされた場合にのみ取引が実行されるスマートコントラクトを活用し、ブロックチェーン間の取引を実現する方式。

<sup>56</sup> チェーン上で動作する Light Client で、ブロックのヘッダーのみ検証することで、検証にかかるリソースを効率化し、中継サーバーである Relayer を介して通信を行うことで、信頼ある第三者を介さずにブロックチェーン間の取引を実現する方式。

<sup>57</sup> 例えば、SC しか保有しておらず、ガス代の支払に必要な ETH を保有していない場合、SC と ETH の両替を、チェーン間ブリッジを介して行う必要がある。こうした両替操作をユーザーに意識させないよう、ウォレット機能をコントラクト化し、両替と取引実行を自動的に行うといった工夫が施されている。

<sup>58</sup> 親アカウントに紐づく形で、利用アプリ毎に生成されるアカウント。サブアカウントの一部権限を例えば銀行や他のサービスプロバイダーに託すことで、サブアカウント内の支払・送金時の承認をユーザーが都度関与する必要がなくなる、いわゆる自動引き落としのようなことも可能になる。

<p>パブリックブロックチェーンであっても、TradFi に求められるマネーの保有者管理等をトークン規格等で実装し、パーミッションドな環境を構築する技術を検討</p>
<p>Ethereum 上でトークンを発行・管理するための標準的規格として ERC-20 があり、トークンの転送や残高確認、承認等の基本的な機能を提供する関数が定義されており、ここから様々な機能が追加されることで他の多くの規格が誕生。</p>
<p>DeFi であってもトラストを必要とするニーズがあり、トークン規格等で規制に準拠する機能を埋め込むことで、TradFi と DeFi が交わっていく世界もありうる。</p>
<p>パブリックブロックチェーンでも、トークン規格で、保有者制限やいざというときの資産凍結機能を実装すれば、一定程度のパーミッションドな環境が構築可能。</p>
<p>民間事業者が CBDC を裏付け資産としてロックし、トークン規格で保有者を限定する制御をかけ、パブリックブロックチェーン上で流通させる方法もありうる。その場合、カストディアーの信頼性をどう確保していくか、ユーザーのデジタルリテラシーの問題にどのように対応していくかなど、様々な検討を要する。</p>
<p>SC を展開するに当たっては、マルチチェーン対応の徹底が必要であり、Wrapped-to-native<sup>59</sup>といった技術も登場している。</p>
<p>DeFi の AMM<sup>60</sup>ではペアリングしやすいマッチングを行う必要があるため、狭い対象でのホワイトリスト制御となると、DeFi へのアクセスは一部制限される印象。</p>
<p>ブロックチェーンにおける取引情報の透明性は、ゼロ知識証明やアクセスコントロールといったプライバシー保護技術によって、調整するアプローチを検討</p>
<p>デフォルトのブロックチェーンではすべての取引情報が公開されるが、ゼロ知識証明等を用い、秘匿性を保ちながら取引の正当性を参加者全員で合意することが可能。</p>
<p>パーミッションドブロックチェーンのうち、データセパレーションとアクセスコントロールによって、プライバシーを柔軟に保護できる特徴を持つものも存在する。</p>
<p>プライバシー保護と透明性のバランスは、各法域の状況や業務要件に応じ、検討していく必要。</p>

<sup>59</sup> 他チェーンに展開された Wrapped token を、他チェーンにおける native token に更新する技術。トークンコントラクトのオーナーシップを発行体に戻す機能を、あらかじめスマートコントラクト等で実装することで、オーナーシップが発行体に戻った段階で、発行体は資産凍結機能を発動できるように仕組むことができる。

<sup>60</sup> Automated Market Maker の略で、暗号資産取引において仲介者を介さずに、スマートコントラクトが価格を自動的に決定する仕組み。AMM では、暗号資産であるトークンのペアがあらかじめ流動性プールに用意されており、トークンの交換を希望するユーザーは、自分が保有するトークンを流動性プールに加え、流動性プールに蓄積されたトークンを引き出すことで、交換することが可能、交換時の価格は事前に決められているアルゴリズムによって自動決定される。

## 5.4 次世代技術の活用<sup>61</sup>

これまで述べてきた分野以外でも、将来的な CBDC システムに関連しうる新たなテクノロジーは日々進展している。

会合では、CBDC における新たな技術の活用検討においては、これまでの当たり前を前提とせず長期的な視野にたち、中立的な技術評価や、関連する技術群をセットでみていく必要性が指摘された。その上で、例えば、AI の決済システムへの活用に関しては、異常検知やシステムログ・スマートコントラクトの監査といったビックデータ解析だけでなく、システム開発サポートの可能性に期待する声も聞かれた。仮に AI エージェントが本格的に普及した場合、高速・大量なマイクロペイメント化が進むことが想定され、そうした状況下では、分散的なアーキテクチャーの方が決済システムとして親和性があるかもしれないが、プライバシーや消失リスクといった実務課題も検討する必要性が指摘された。

(表 5 - 6) AI 等、その他の次世代技術に関する議論

<p>新たなテクノロジー活用に当たっては、これまでの当たり前を前提とせず、関連する多様な技術の進捗を、長期的かつ中立的な視点でみていく必要</p>
<p>加速する技術革新の中では、これまでの当たり前を前提とせず 20~30 年後も視野に入れて検討することに意味がある。</p>
<p>実際の技術進化は指数関数的な変化だが、社会の期待は過大評価と過小評価といった三次関数的な発展をたどる傾向。バイアスの少ない技術評価をしていく必要。</p>
<p>技術の進展は、他の関連する技術とセットでみていく必要。例えば生成 AI の場合、ハードウェアの進展が大きく影響していたように、関係ないと思われていたイノベーションが思わぬところで異なる技術革新につながるケースは多い。</p>
<p>AI の決済システムへの活用は、異常検知やスマートコントラクトの監査、システム開発サポート等に期待。AI エージェントが普及した場合、利便性駆動のマイクロペイメント化・決済システムの分散化が進む可能性があるが、様々なリスク対応の実務課題も要検討</p>
<p>AI の決済システムへの活用可能性としては、異常検知やシステムログ・スマートコントラクトの監査といったビックデータ解析だけでなく、システム開発サポートとしての活用も考えられる。</p>

<sup>61</sup> その他のテクノロジーについては、主に WG4 の第 3・4・10~12 回会合において議論を実施。

仮に AI エージェントの導入・普及が本格化していく将来を想像すると、業務の細分化が進み、それぞれの業務に適した専門性を備えた AI エージェント同士で処理を行い、高速・大量なマイクロペイメント化が進むことが考えられる。こうしたマイクロペイメントに対しては、Peer to Peer (P2P) の分散アーキテクチャーの方が決済システムとして親和性があるかもしれない。

米 Project Hamilton やカナダ中央銀行のディスカッションペーパーで紹介された CBDC の実験的デザインは、性能やプライバシー重視に振り切った分散アーキテクチャーの傾向がみられる。そこで登場するセルフカストディアルウォレットは、高い利便性が期待される一方で、現金同様の消失リスクや AML/CFT 対応の難しさといった課題も存在するため、実務的には検討すべき事項が多い。

以 上