2025 年 12 月 17 日
日本銀行決済機構局

ＣＢＤＣフォーラム
ＷＧ２「追加サービスとＣＢＤＣエコシステム」
ＷＧ４「新たなテクノロジーとＣＢＤＣ」
共同開催会合の議事概要

１．開催要領

（日時）2025 年 10 月 14 日（火）14 時 00 分～16 時 30 分
（形式）Ｗｅｂ会議形式

２．プレゼンテーションとディスカッション

- 株式会社 Startale Japan より、「Web2 と Web3 の垣根がない信頼されるインターネットインフラ構築に向けて」について、プレゼンテーション[1]が行われた。概要は以下のとおり。

  - パーミッションレスブロックチェーン上で、仮に CBDC・ステーブルコイン・トークン化預金といったマネーを展開する場合、Web3 特有のインフラとして必要な対応は、主に以下の３つ。

    - ✓ 高リスクアドレスに流通させないKnow-Your-Transaction(KYT)/AML 対応：当局の要請に応じて、発行体の権限でブラックリストに該当するアドレスのトークン保有を凍結できる機能。マルチチェーン対応の徹底が必要[2]で、Wrapped-to-native[3]といった技術も登場。

    - ✓ 従来金融に匹敵する利便性・安全性を備えたウォレット：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[4]やチェーン間ブ

---

[1] プレゼンテーション資料は以下を参照。
https://www.boj.or.jp/paym/digital/d_forum/wg4/dfo251217d.pdf

[2] マルチチェーン対応を行わない場合、資産凍結機能の及ばないオフショアトークンが他のチェーンで登場してくる可能性。

[3] 他チェーンに展開された Wrapped token を、発行元チェーンにある native token に戻す技術。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、予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。

[4] 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。

リッジ等）をユーザーに感じさせない機能[5]や、目的別のサブアカウント[6]等。

✓ DeFi 展開に必要なインフラ：トークン発行のベースとなるチェーンは、処理速度の速さ、参加者の数と質、KYT/AML 等を考慮し、適切なトークン規格が設定できるかといった観点で選定する必要。また、価格情報を複数のチェーンに反映するオラクルや、DEX 取引で肝となる流動性プールの仕様に関しても要検討。

・ 発行体は上記インフラ対応だけでなく、ベンダー依存によるオペレーショナルリスクやセキュリティリスクにも注意の要。障害発生時に原因特定とトラブル対応を素早く行えるよう、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。

● 株式会社 Startale Japan の説明を踏まえ、参加者によるディスカッションが行われた。議論の概要は、以下のとおり。

（参加者）マルチチェーン展開を徹底しようとすると、ノードの構築・運用の観点で対応に要するリソースが膨大になる点が課題。投資するチェーンを意味のあるものに絞り込む必要がある。

そのうえで、こうした課題に対応する技術として、Wrapped-to-native の話があり、これは、当初、native なトークンの仕様を持つ参照実装としてのトークンコントラクトを公開し、この段階では、他チェーンに同一の仕様を持つトークンが第三者により勝手にデプロイされることを許容する、というもの。当該段階では発行体のリソースはかからないが、その後、例えば当該トークンの流通量が増え、エコシステムが盛り上がった段階で発行体がノード構築の判断を下せば、第三者と発行体の合意のもとで発行体にオーナーシップが戻され、凍結機能の発動が可能になる仕組みと理解してよいか。

---

[5] 例えば、ステーブルコイン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、ステーブルコインと 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。

[6] 親アカウントに紐づく形で、利用アプリごと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。

（プレゼンタ）ご理解のとおり。そもそもパブリックブロックチェーンの原則として、トークンをデプロイすることは比較的容易に出来てしまう。具体的には、元のチェーンにスマートコントラクトを用意し、ここにオリジナルのトークンが入ってきたら、それをロックしたうえで、もう片方のチェーンで、そのコピーをミントするという方法を用いればよい。このため、誰だか分からない人がデプロイしたオフショアトークンを完全に撤去することは難しい。仮に完全に撤去しようとすると、膨大な数のチェーンに最初からノードを構築する必要があり、この一連の対応には膨大なコストを要する。こうした状況を踏まえ、Wrapped-to-native は、発行体の裁量（経済規模等）でオーナーシップをテイクオーバーできる機能を備えたスマートコントラクトのテンプレートであり、これを配ることで、発行体に凍結機能の発動権限等が及ぶ体制を取りやすくなるほか、対象チェーンを公式にサポートするタイミング、ひいてはそれにかかるコストを概算しやすくなる。

（参加者）マルチチェーン対応に伴うオペレーションコストの低減策として、Wrapped-to-native のご紹介があったが、発行体に権限が委譲される前のトークンのコントローラビリティは、やはりトレードオフの関係にあると理解。

（参加者）２点質問がある。１点目は、トークンコントラクトの凍結機能を確実かつ迅速に発動することが重要になるが、それを実現する有効な仕組みはあるのか。２点目は、リスト管理に関して、パーミッションレスブロックチェーンでの展開を前提とした議論なため、ホワイトリスト管理よりも、ブラックリスト管理の方が、親和性が高いという理解でよいか。

（プレゼンタ）１点目に関して、発行体は、監督官庁からの命令を受けた段階で即座に凍結機能を発動することが想定されている。例えば、ブリッジのハッキングの場合、規制当局や監督官庁からの命令が来ると、当該ブリッジのサービスプロバイダーが契約しているセキュリティーベンダーが、即座にハッカーのアドレスのリストを発行体に送付し、それを受けた発行体が速やかに凍結機能を発動する想定で、当局の要請と発行体のスピーディーな連携・対応が前提となる。２点目に関しては、ご理解のとおり、ホワイトリストとなると、パーミッションレスブロックチェーンよりはコンソーシアム型のパーミッションドブロックチェーンとの親和性が高くなることから、パーミッションレスブロックチェーンにおいては基本的にはブラックリストで登録者を弾くのが適切と考える。

（参加者）ブラックリストの対象を減らし、ホワイトリストの対象を増やすと、大抵似たようなリストに仕上がるが、例えば DeFi の AMM[7]を使うと、基本的にはペア

[7] 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

リングし易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管理となると DeFi へのアクセスは制限される印象。そういった観点では、Web2 と Web3 の垣根をなくそうとすると、利便性やユースケース面でトレードオフに直面する具体例の一つとして、リスト管理の匙加減があると理解。

（プレゼンタ）ご理解のとおり。ホワイトリストだと、誰もがアクセスできる市場ではなくなるため、DeFi に求められる運用という観点では制限される。

（参加者）パーミッションレスとパーミッションドのブロックチェーンは、合意形成の部分に違いはあれ、どちらを利用しても開発の仕方次第で規制対応は可能。既に USDC のように強いプレイヤーがいる市場では、勝算のあるユースケースを特定していくことが重要。例えば、国際送金や大企業間の送金等既存のやり方を効率化するアプローチには意味があるかもしれない。

（プレゼンタ）ご理解のとおり。市場は既に飽和しており、ステーブルコインをただ発行するだけでは使われず、流動性プールやオラクル、ブリッジといったセットアップについても、発行体は率先して検討していく必要。

- TIS 株式会社より、「先進外銀の預金トークンの研究」についてのプレゼンテーション[8]および「ブロックチェーン取引におけるプライバシー保護機能（Encrypted ERC）」についてのプレゼンテーション[9]が行われた。概要は以下のとおり。
  - 本年６月に J. P. Morgan より発表された JPMD（JPM Deposit Token）関連レポートは、CBDC やステーブルコインといった他のデジタル通貨と共存し、異なる銀行間や DLT 基盤と高い相互運用性を確保する預金トークンの考え方や特徴を整理している。主なポイントは以下のとおり。

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。

[8] プレゼンテーション資料は以下を参照。
https://www.boj.or.jp/paym/digital/d_forum/wg4/dfo251217c.pdf

[9] プレゼンテーション資料は以下を参照。
https://www.boj.or.jp/paym/digital/d_forum/wg4/dfo251217b.pdf

- ✓ J. P. Morgan は 2016 年以降、預金のトークン化の先駆けとして、プライベート型やパーミッションド型のブロックチェーンを用いて、顧客企業間の支払をスマートコントラクトで効率化する取り組みを進めてきた。
- ✓ 今回新たに発表した JPMD は、パブリックブロックチェーンで預金トークンをパイロット運用する点が新しく、DeFi と伝統金融の架け橋として期待されている。
- ✓ 技術的には、Coinbase の L2 チェーンの Base を用いることで、パブリックブロックチェーンながら、スマートコントラクトで保有者制限をかけるパーミッションドな環境を構築し、KYC や AML/CFT 対応といった伝統金融で求められる統制を備えている点が特徴。
- ✓ スマートコントラクトの中身としては、ERC-20[10]をベースにし、他のトークン規格も組み合わせることで機能拡張性を持たせており、技術的にはステーブルコインと同じ（故に両者の相互運用性が確保されている）。

・ Encrypted ERC は、Ava Labs が開発したプライバシーを強化したオープンソースのスマートコントラクトで、ERC-20 トークンと互換性がある。通常の ERC-20 トークンでは、誰でも残高や取引情報を閲覧できてしまうが、Encrypted ERC では、残高・取引情報を暗号化し、ゼロ知識証明を活用して正当性を担保する。ERC-20 と比較すると、ガス代やデータサイズ、処理速度の面等、課題はあるものの、低頻度といった特定ユースケースでは、現状の水準でも実用化の可能性がある。今後、WG2 内の API サンドボックスプロジェクトにおいて、Encrypted ERC の実装と同トークンを用いたユースケースの検討を、トヨタファイナンシャルサービスと行っていく予定。

- TIS 株式会社のプレゼンテーションを踏まえ、参加者によるディスカッションが行われた。概要は以下のとおり。

（参加者）預金トークンの課題として、国内やクロスボーダーのユースケースのどちらにおいても、預金トークン同士の決済をどうするのかについて考えていく必要。

（プレゼンタ）ご指摘のとおり。例えば、昨年から進行中の Project Agorá では、既

[10]イーサリアムの実行環境である Ethereum Virtual Machine (EVM)上で、代替可能トークンを発行・管理するための最も基本的な標準規格。この規格に準拠し発行されたトークンは、ウォレットや分散型取引所（DEX）等の多様なアプリケーション間で、スムーズな送受信や交換といった高い互換性を実現。

存の仕組みを維持しながら、クロスボーダーの文脈で商業銀行マネーと中銀マネーの双方をトークン化する試みが検討されている。このような取り組みを通じ、制度的な課題や会計上の問題が整理しながら、解像度が上がっていくのではないか。

（参加者）預金トークンとステーブルコイン、CBDC の共存のあり方という観点から考えると、今後、トークン化された預金を発行する銀行や、様々なステーブルコインの発行者が増える中で、決済手段がサイロ化し、かえって分断が進むことを懸念。こうした状況を打開する上では、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、さらにはステーブルコイン等、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。相互運用性の実現にあたっては、技術面の標準化や API 連携だけでなく、そうした動きを推進する中立性を担保するイニシアティブや組織の存在が鍵になる。こうした役割を果たせるものの一つとして、CBDC があるのではないか。CBDC を裏付けとしながら、例えば店舗での決済インターフェースまでもシームレスに統一していくことで、様々な決済手段が円滑に連携しやすくなると考えている。もちろん、実現は容易ではないが、例えば、カンボジアのバコンではこれを実現できており、一つの方向性として検討していくべきだろう。

（プレゼンタ）CBDC が接着剤のような役割を果たすという方向性のあり方には同意。多様な決済手段を上手く共存させるためには、協調領域と競争領域をしっかりと見極めながら検討していく必要。

（参加者）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」、今回の JPMD のような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」と使い分けている人もみられるが、まだ定義や実装方法に対する共通理解は定まっていない。CBDC やステーブルコインとの連携・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。

（参加者）セキュリティトークンの資金決済に使えるかという観点で、預金トークン・ステーブルコイン・CBDC について考えると、ユースケースに応じてメリット・デメリットは異なる。例えば、決済金額規模が大きい取引では、中立性のある CBDC が適しているかもしれないが、小規模取引ではより簡易で利便性のある他の資金決済手段が適する場合もあるだろう。また、金融機関における会計処理を考えると、暗号資産やステーブルコイン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

同様に計上し易いというメリットが存在するため、金融機関にとっては導入のハードルが比較的低いのではないか。

- 三井住友信託銀行株式会社より、「トークン規格とコンプライアンス：海外事例を踏まえた議論」について、プレゼンテーション[11]が行われた。概要は以下のとおり。

  - 伝統金融における KYC/AML においては、国籍・住所・氏名の照合といった、機械的な手順で確認できる「ルールベース」のものと、誰をブラックリストに入れるか・入れないかのような、金融機関による個別判断を要する「リスクベース」のものが存在。トークンのビジネスロジックとしてコンプライアンス対応を埋め込むにあたっては、前者の実装は比較的容易ながら、後者の実装も検討していく必要がある。例えば LLM 等、AI の活用も選択肢に入れる必要があるのではないか。

  - コンプライアンス対応のトークン規格の主な活用事例は以下のとおり。

    ✓ ERC-3643：T-REX（Token for Regulated Exchange）とも言われ、ERC-20 をベースに AML/CFT 等のコンプライアンス機能を付加したもの。開発を進める団体に DTCC が加入したり、同団体が SEC からヒアリングを受けたりといった報道、vLEI（verifiable LEI）との連携[12]といった新しい動向を踏まえ、最近注目を集めている。

    ✓ CAST（Compliance Architecture for Security Token）：Société Générale が提唱する規制遵守のためのセキュリティトークン用のフレームワークで、ERC-1155 をベースに ISO を始めとする様々な国際規格と連携。Société Générale はこのフレームワークに基づき、MiCA 規制対応の CoinVertible というステーブルコインを発行。同ステーブルコインは、当初はホワイトリスト型の保有者管理が実装されていたが、足元ではブラックリスト型に変更されており、状況に応じて実装内容は変更できる柔軟性があることが示されている。

    ✓ DS Protocol：BUIDL 等を取り扱う Securitize が開発した、セキュリティトークン（Digital Securities）の規格。ERC-20 をベースに、KYC/AML といったコンプライアンス対応が組み込まれている。KYC した情報を全てオ

---

[11] プレゼンテーション資料は以下を参照。
https://www.boj.or.jp/paym/digital/d_forum/wg4/dfo251217a.pdf

[12] vLEI は、従来の国際的な法人識別子である LEI（Legal Entity Identifier）を基に GLEIF の監督下で、発行体が組織・人のアイデンティティを検証可能な資格証明（Verifiable Credentials）として発行したデジタル証明書を指す。

ンチェーンに載せるのではなく、取引の制御に必要な情報のみをオンチェーンに格納し、それ以外の情報はSecuritizeの責任が及ぶところで管理される点が特徴。

- ✓ DAMA2（Digital Asset Management Access）：Deutsche Bank AGらが推進するプロジェクトで、EthereumのL2技術とゼロ知識証明を活用し、コンプライアンス対応と処理の効率化の両立を目指す、レイヤー1-2-3のアーキテクチャを提案。

- ✓ DeFi研究会：金融庁のFintech実証実験ハブの支援案件に採択された銀行・証券・信託・暗号資産交換事業者からなる研究会。金融機関によるKYC済のアドレスを保有する顧客等に、AMM機能といったDeFiサービスが提供できるかといった観点で検討中。

・ 将来的なデジタル通貨に求める機能は何かを考える上で、ユーザー目線で現金あるいは預金に近いデザインなのか、といった観点で検討をすると示唆を得られるかもしれない。例えば、現金型は、対面での利用や台帳レスの設計が想定され、基本的には当事者間で決済は完結し、匿名性が担保され、ユーザーの制限もなく、誰でも簡単に利用できる仕組み作りが課題となる特徴がある。その一方、預金型は、非対面も利用可能・利用にあたっては登録（KYC）が必要な台帳ネットワークが想定され、ネットワーク間の連携が課題となる特徴がある。

・ 近年、GoogleがAIエージェントに委ね決済を自動化するAgent Payment Protocolを発表しているほか、CoinbaseらもUSDC対応のAIマイクロペイメント用にHTTP402を活用するプロトコル[13]を公開する等、決済分野におけるAIエージェント活用の動きが積極化している。こうしたAI活用のトレンドも踏まえ、将来的な決済手段のあり方も検討していく必要。

● 三井住友信託銀行株式会社からのプレゼンテーションを受けて、参加者によるディスカッションを行った。議論の概要は以下のとおり。

（参加者）CBDCなり預金トークンなり、デジタル通貨を新しい決済サービスとして提供するにあたっては、ステークホルダーへのメリットの訴求が重要。近年Peppol[14]

---

[13] 長年未活用であったHTTP402（支払が未完了である事を示す予約コード）を基盤に、オンチェーン決済をHTTPレベルでシームレスな処理を可能とするx402プロトコルを指す。

[14] Pan-European Public Procurement On-Lineの略で、請求書等のビジネス文書のデジタルデータをネットワーク上でやり取りするための国際標準規格を指す。

も普及していることを踏まえ、例えば、EDI 情報[15]をデジタル通貨に付加し、入金の消込や翌月請求書の発行といった工程を削減する業務改善とセットで、金流と商流を一致させるようなスマートコントラクトの実装には、大きなチャンスがあるのではないか。

（参加者）WG4 の第 10 回会合で紹介された価値移転プロトコルは、将来的なデジタル通貨のデザインの方向性として説明のあった、いわゆる現金型の特徴を備えていると認識。仮に金融・決済分野に AI エージェントが本格的に参入する将来を想定すると、取引件数の爆発的な増加が予想されることから、既存の台帳ネットワークの仕組みで決済を行うことは難しく、プロトコルレイヤーや通信レイヤーで決済の仕組みを補完していく必要があるかもしれない。

（日本銀行）新しい決済手段が実現・検討されている中で、流動性の分断という課題を回避するためにも、改めて相互運用性の重要性が増している。本日の議論では、相互運用性を高めるために、どういった主体がイニシアティブをとるかといった観点で、中立的な主体である中央銀行に期待する声も聞かれたほか、店舗や消費者といったステークホルダー全体のエコシステムが連携をとっていくことの重要性も指摘された。また、CBDC の姿として現金型や預金型に分けた特徴の整理や、AI 活用のトレンドも踏まえた場合の仕組みに関するアイデアも紹介された。本日も、どのような形で中央銀行マネーを提供していくべきかを検討していくうえで重要なご示唆を頂き感謝申し上げる。

３．次回予定

次回の会合は 12 月 22 日（月）に開催予定。

以　上

[15] Electronic Data Interchange（電子データ交換）の略で、企業間の取引において、取引先との取り決めに従い、振込データ等に付加する標準化された情報を指す。