中央銀行デジタル通貨（CBDC）に関するレポート

（令和４年度）

2023 年５月

国立印刷局 CBDC 研究会

目　次

本レポートは、国立印刷局内の「中央銀行デジタル通貨に係る研究会」に関係する職員の調査・研究成果であり、今後、CBDC の検討を進める一助としての考えをまとめたものです。なお、レポート内で示された内容や意見は、執筆者個人の見解であり、国立印刷局の公式見解を示すものではありません。

1 はじめに

我が国で最初に新型コロナウイルス感染症が発生してから3年以上が経過し、ウィズコロナの考え方[1]の下で、感染症抑制と経済活動の両立を図りながら、徐々に社会経済活動が戻りつつある。感染拡大下では、新たな生活様式など国民の行動様式の変化が進む中において、キャッシュレス決済も一つの変化要素として浸透したためか、2022年時点でのキャッシュレス決済比率は、36.0%まで上昇している[2]。また、政府がデジタル給与払いや国の行政手続における手数料等のキャッシュレス納付などの施策を進めていることや、㈱NTTデータが、決済ネットワークであるCAFIS[3]の少額決済向け手数料引き下げを実施[4]していることなど、キャッシュレス決済環境の整備等が進むことにより、更にその比率が上昇していくことが想定される。

このような社会における決済のデジタル化と並行して、中央銀行デジタル通貨（以下「CBDC」という。）について、政府は、経済財政運営と改革の基本方針2021（骨太の方針2021）において、「政府・日銀は、2022年度中までに行う概念実証の結果を踏まえ、制度設計の大枠を整理し、パイロット実験や発行の実現可能性・法制面の検討を進める」としている。

日本銀行は、現時点でCBDCを発行する予定はないとしつつも、2022年11月24日の中央銀行デジタル通貨に関する連絡協議会における開会挨拶では、「今、決済の未来を考える意味について」と題してCBDCを含む将来の決済システムのことを議論すべきタイミングであることや、連絡協議会の関係者などの知見と協力を得ながらCBDCの技術面の実験と制度面の検討を進めていく必要性などを述べている。そして、CBDCの導入については、整理された検討内容や、国外の状況や社会の情勢などを踏まえて国民が判断するものとして考えられている[5]。

国外に目を移すと、バハマ、ナイジェリアなど途上国で既にCBDCが発行されているほか、中国における市民参加型の実証実験の進展や欧州中央銀行（ECB）における計画的な調査フェーズの推進に加え、米国においても2022年3月の大統領令に基づく包括的なフレームワークとしての調査研究が進められるなど、主要国のCBDCに係る検討も進んでいる。

国立印刷局CBDC研究会としては、CBDCに係る国内外の動向を整理しつつ、暗号資産、ステーブルコインなどのデジタル資産に係る事件や攻撃事例などを分析しながら、CBDCに必要となる機能や求められる安全性などを考察し、2022年9月には、プライバシー保護とデータの利活用を可能とする技術を中心に調査したレポートを公表した。プライバシー保護については、CBDC導入の最終

的な判断を行う国民の情報管理に対する不安を払拭するための重要な課題であり、誰もが安心して利用できる安全性が確保されていることが必要となると考えられる。また、2021 年 10 月に G7 が公共政策上の原則[6]の中で公表しているように法的・ガバナンスの枠組みを整理し、データプライバシーを保護しつつ、AML/CFT 等を目的とした公的当局によるデータへのアクセスを明示するなど適切な透明性による信認確保も必要となる。

そこで、本レポートにおいては、デジタル社会の中で既に実装されている暗号鍵、認証鍵といった鍵管理、その鍵を用いた演算・検証等を可能とするセキュリティ機能について理解を深めるべく、機密情報保護の仕組みの一端を調査・報告するものである。

[1] 内閣官房、「With コロナに向けた政策の考え方」、2022 年 9 月 8 日、(https://corona.go.jp/withcorona/)

[2] 経済産業省、「2022 年のキャッシュレス決済比率を算出しました」、2023 年 4 月 6 日、(https://www.meti.go.jp/press/2023/04/20230406002/20230406002.html)

[3] 「CAFIS」は、㈱NTT データが提供する日本最大級のキャッシュレス決済総合プラットフォーム。さまざまな業態・業種の加盟店と、国内ほぼすべてのクレジットカード会社・金融機関を結び、24 時間 365 日休むことなく日本の決済シーンを支えている。

[4] NTT データ、キャッシュレス社会のさらなる進展のため CAFIS 料金引き下げを実施(ニュースリリース)、2022 年 11 月 16 日、(https://www.nttdata.com/jp/ja/news/release/2022/111600/)

[5] 日本銀行、「【挨拶】「今、決済の未来を考える意味について」(第 4 回中央銀行デジタル通貨に関する連絡協議会)」、2022 年 11 月 24 日、(https://www.boj.or.jp/about/press/koen_2022/ko221124a.htm)

[6] 日本銀行、「G7 による「リテール中央銀行デジタル通貨(CBDC)に関する公共政策上の原則」について」、2021 年 10 月 14 日、(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025235/G7_Public_Policy_Principles_for_Retail_CBDC_FINAL.pdf)

2　環境分析

2.1　国内の動向

2.1.1　政府

政府は、2021 年 6 月 18 日に骨太の方針 2021 を閣議決定し、日本の未来を拓く四つの原動力として、グリーン、デジタル、活力ある地方創り、少子化対策を掲げた上で、デジタル時代の官民インフラを今後 5 年で一気呵成に作り上げる方針を示した。CBDC についても、「政府・日銀は 2022 年度中までに行う概念実証の結果を踏まえ、制度設計の大枠を整理し、パイロット実験や発行の実現可能性・法制面の検討を進める」ことが示された。それに従い、現在、日本銀行では、概念実証を進めつつ、最新の技術やノウハウの共有、制度設計面の検討などが進められている。

財務省では、制度設計の大枠の整理に向け、高い識見を有する方々から意見を聴取するため、2023 年 4 月に「CBDC（中央銀行デジタル通貨）に関する有識者会議」を設置した。

また、CBDC に対する考え方については、国会答弁等の中でも示されており、政府は、「通貨が経済社会の根幹を成す重要なインフラであるということを踏まえると、CBDC 発行に際しての政策的判断には、金融システムの安定、プライバシーの保護、セキュリティの確保、マネーロンダリング対応など、安全で信頼の置ける CBDC の在り方について、多岐にわたる制度面や法律面の論点の検討もやはり不可欠」であり、国際的な動向にも十分留意しつつ、日本銀行、財務省、金融庁、民間企業等が緊密に連携して対応していくべきとしている[1]。

2.1.2　日本銀行

日本銀行は、2020 年 10 月に示した「中央銀行デジタル通貨に関する日本銀行の取り組み方針」に基づいて、2021 年 4 月から概念実証実験を開始し、実証実験の状況や、取組の進め方などについて、民間事業者や政府との情報共有を行うために設置された「中央銀行デジタル通貨に関する連絡協議会」の中で適宜報告を行っている。また、CBDC を支える技術に関しては「決済の未来フォーラム」などを通じて、広くオープンな場で共有されている。以下、日本銀行が連絡協議会を通じて公表している中間整理[2]、実証実験の結果報告書[3]等の情報を基に概況を記す。

(1) 実証実験

日本銀行で実施されている実証実験は、2021 年 4 月から開始した概念実証実験フェーズ 1 が 2022 年 3 月に終了し、2022 年 4 月から 2023 年 3 月にかけてフェーズ 2 が実施された。フェーズ 2 では、技術的な課題のうち早期確認が望ましい各周辺機能が的確に処理されるかについて検証を行うだけでなく、各周辺機能がシステム処理性能に与える影響やセキュリティリスクへの耐性、障害耐性、可用性などの問題点の抽出及び対応策の検討が行われた。その結果、図 2.1 に示したフェーズ 2 における検証項目としての周辺機能付加により、レイテンシ（1 件当たりの処理時間）は、関係システム数の増加を背景に上昇、分布の裾野も幾分拡大するものの、大きな性能劣化を招くことはなく、社会実装する場合に必要な拡張性や信頼性を確保できる可能性が示唆される中、そのための工夫や対策が必要なことが示された[3]。

図 2.1　フェーズ２の主な検証項目

（出典：日本銀行、「中央銀行デジタル通貨に関する連絡協議会　中間整理」21 頁、2022 年 5 月 13 日）

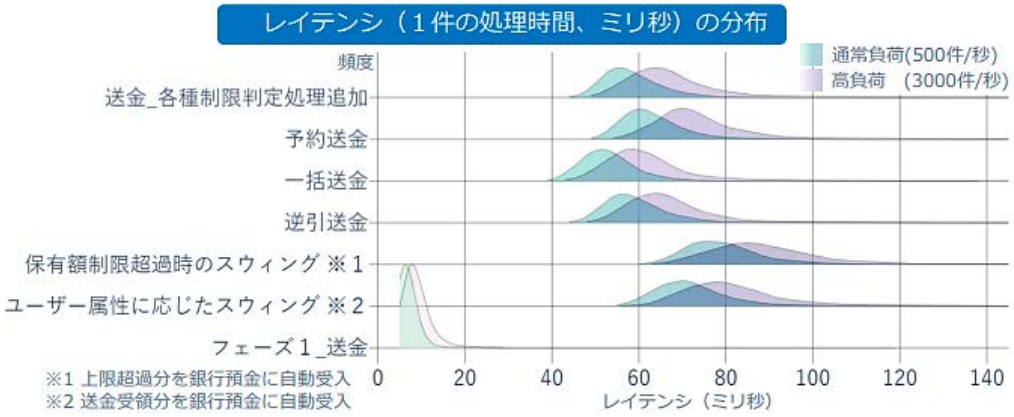


図 2.2　フェーズ２検証時のレイテンシ分布

（出典：日本銀行、「中央銀行デジタル通貨に関する日本銀行の取り組み」6 頁、2023 年 2 月 17 日）

さらに、フェーズ 2 では、各種の周辺機能を実現するために、CBDC 台帳に加えて、取引履歴を管理するシステムや、送金指図の予約・実行システムなどを追加して構築している。また、トークン型台帳システムについては、「固定額面方式」に加えて、「変動額面方式」も念頭に検討するとともに、「データベース方式」については、「リレーショナルデータベース方式」に「非リレーショナルデータベース方式（NoSQL）」を加えるなど、実現可能性の幅を広げながら、新たな技術の活用可能性も検討された。

その結果、トークン型台帳における変動額面方式については、固定額面方式と比較して、並列処理可能というトークンの性能面の特性がよりいかされやすくなる可能性があるが、口座型台帳の処理と比較すると、必要なリソース使用量の増加や、周辺機能の実装難度の上昇の可能性が確認されたとされている。また、NoSQL データベースは、性能向上の観点から台帳や台帳以外の CBDC システムのデータベースとしての活用可能性はあるが、想定される業務等の要件に応じて、活用可能性の程度差があることや、性能面以外の観点からも検討が必要とされている[3]。

(2) パイロット実験

日本銀行は、上述した CBDC に関する基本的なアイディアが技術的に実現可能かどうかを確認するための概念実証実験について、所期の目的を達成したとして、2022 年度末で終了し、2023 年度からパイロット実験を開始することとした。パイロット実験においては、仲介機関システムや利用者デバイスまで実験用システムの構築・検証の範囲を拡大し、エンドツーエンドの処理フロー確認、外部システムとの接続に向けた課題・対応策の検討などに加え、概念実証実験で必要性が示された工夫や対策などについても検討するものとしている[3]。

また、日本銀行は、CBDC の設計を適切に進める観点から、「CBDC フォーラム」を設置し、議論・検討テーマ別にワーキンググループを置き、リテール決済に関わる民間事業者のアイディアや知見を活用することとした。同フォーラムは、2023 年 4 月に日本銀行が公募し、審査期間を経て参加者を決定し、7 月の参加者公表以降、それぞれのワーキンググループにて順次議論を本格化することとされている[4]。

なお、パイロット実験用システムの構築・検証と CBDC フォーラムの検討結果は、必要に応じて相互にフィードバックすることが想定されており、それぞれの検討に有益な効果をもたらすことが期待されているようである。

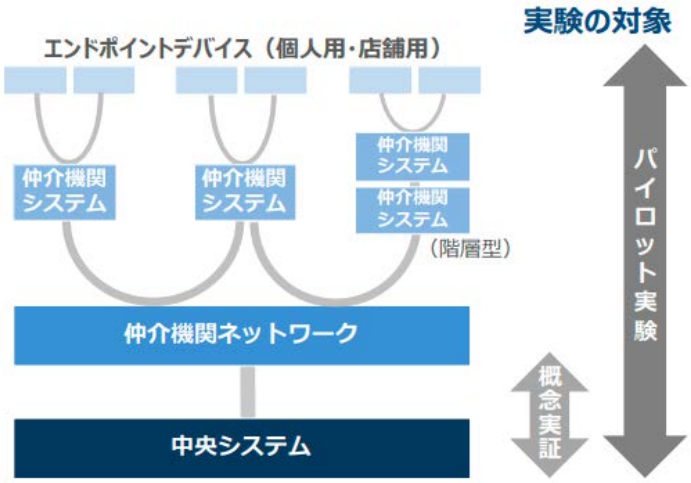


図 2.3　パイロット実験の対象範囲

（出典：日本銀行、「中央銀行デジタル通貨に関する実証実験について」、2023 年 2 月 17 日）

図 2.4　パイロット実験用システムの構築・検証とＣＢＤＣフォーラムの関係図

（出典：日本銀行、「中央銀行デジタル通貨に関する実証実験について」、2023 年 2 月 17 日）

(3) 制度設計に関する論点

イ　ＣＢＤＣシステムを構成する主体とその役割

CBDC の制度設計に関する論点の一つとして、日本銀行と仲介機関等との協調・役割分担の在り方が挙げられている。中間整理では、仲介機関である民間部門の決済インフラやサービスとの関係性を踏まえると、CBDC をユーザーに提供する構造として、日本銀行と民間部門の一部とで構成される「インフラ部分」と、民間部門が提供する「追加サービス部分」との階層構造を築き、「垂直的共存」を実現することが有益であり、CBDC に求められる機能と役割を達成することが可能となるとの考え方が示されている。

また、日本銀行及び仲介機関の役割や業務についても検討が進められており、その中では、仲介機関が、日本銀行から発行された CBDC を全

ユーザーに提供するための仲介業務を担うことについて想定されている。このため、仲介機関の業務範囲は幅広く、事業者の業態や規模により実現可能性が異なることから、図 2.5 左、中央に示す「単層型」と右側に示す「階層型」が想定されている。

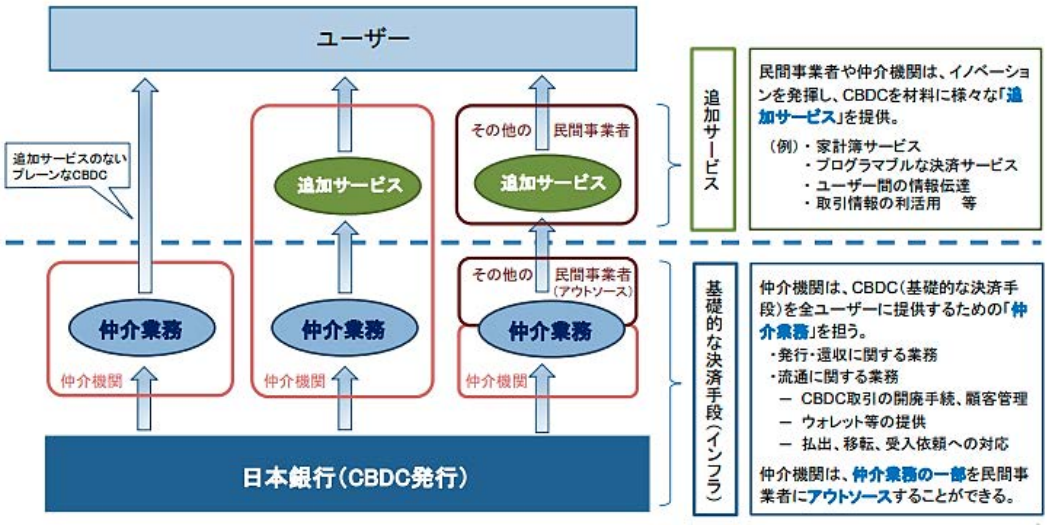


図 2.5　CBDC 発行時の階層構造（基礎的な決済手段と追加サービス）

（出典:日本銀行、「中央銀行デジタル通貨に関する連絡協議会　中間整理」24 頁、2022 年 5 月 13 日）

ロ　他の決済手段との関係（水平的共存）

「垂直的共存」と併せて、CBDC とその他の決済手段（現金、銀行預金、民間デジタルマネー等）が、その機能や役割を適切に発揮し、互いに共存するといった「水平的共存」を目指すこととしている。そのためには、CBDC とその他決済手段との相互運用性を確保し、それぞれの決済手段の利便性を高め、利用者の選択幅の拡大、決済分野における競争促進、決済システム全体の強靭性向上などに繋げることが重要となる。

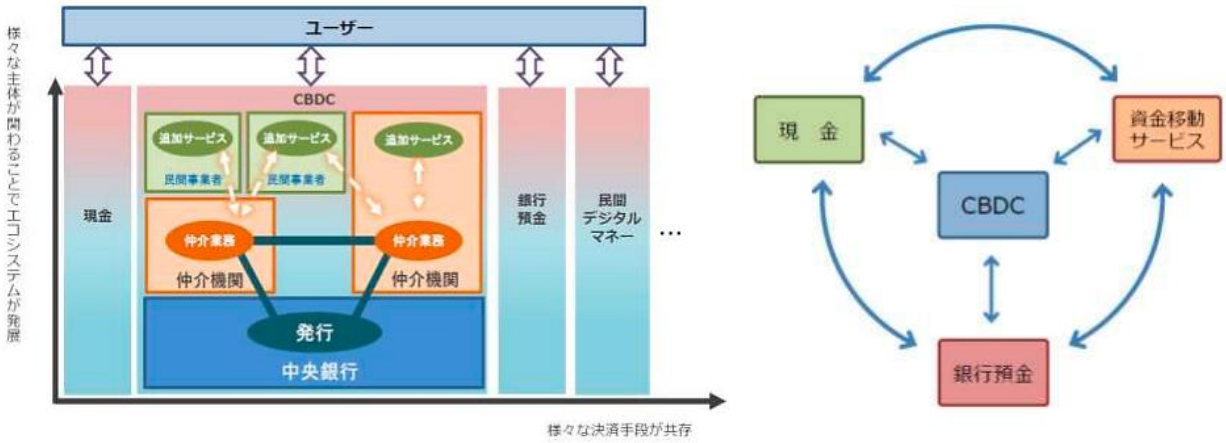


図 2.6　CBDC と他の決済手段との関係（水平的共存）

（出典:日本銀行、「中央銀行デジタル通貨に関する連絡協議会　中間整理」31,32 頁、2022 年 5 月 13 日）

ハ　プライバシーの確保と利用者情報の取扱い

中間整理では、CBDC 発行に当たって、利用者情報の取扱いに関する様々な要請を考慮した上で、中央銀行と民間事業者の役割分担などを検討していく必要があるとの考え方が示されている。具体的には、「誰が、どの範囲のデータを、どのような条件の下で取得、管理するか」について検討するものであり、データの利活用による利便性とプライバシー保護といった、トレードオフの関係を仕組みとして整理するというものである。

この仕組みについては、上述した基礎的なインフラ部分と追加サービス部分との各領域において検討する必要があるとしている。インフラ部分においては、2021 年 10 月の G7 報告書で示された[5]ように、高い透明性のある適切なプライバシー保護の実現が求められることから、日本銀行や仲介機関の役割、法制面の対応の必要性等について検討されている。一方、追加サービス部分においては、データの有効活用によるユーザーの利便性向上の観点から、ユーザー情報の適切な取得・利用や外部提供の同意取得など、ユーザー情報の適切な取扱いが必要となる。

なお、プライバシー保護に関連する技術的な要素について、日本銀行は、匿名化手法、差分プライバシー、秘密計算などを整理した決済システムレポート別冊[6]を 2022 年 9 月に公表している。

ニ　クロスボーダー決済との関係

グローバル化の進展や世界規模のステーブルコイン構想の影響もあって、クロスボーダー決済に関して、より便利で安価なサービスが望まれ、海外送金の仕組みを改善するための国際的な議論が進められており、G7 が公表したリテール CBDC に関する公共政策上の原則の一つにも、クロスボーダー機能に対する CBDC の役割が整理されている。

このように、クロスボーダー決済に CBDC を活用することも一つの選択肢として用いることを想定し、日本銀行は、各国で検討されている自国と他国の CBDC が円滑かつ安全に交換できるよう、「標準化」による「相互運用性」、「信頼性」の確保が必要として、国際標準化を巡る議論にも積極的に参画するとしている。

2.2　各国の動向

2.2.1　欧州

ECB では、2021 年 10 月から、2 年間の調査フェーズに移行するなど、調査研究が計画的に進められている。その進捗に関しては、2022 年 9 月

末、12 月末及び 2023 年 4 月にプログレスレポートを公表し、調査研究の進捗と今後の予定について共有が図られている。まず、9 月末のレポート[7]では、デジタルユーロの発行目的を再度整理し、基礎となる設計オプションが示された。

表 2.1　デジタルユーロの設計オプション

決済メカニズム	・ユーロシステムはオンライン取引時の第三者認証について調査 ・オフライン決済のP2P検証について開発（市場投入までの時間は不確実）
プライバシー	完全な匿名化は公共政策の観点から望ましくない。 ・利用者は、利用開始時に仲介者による本人確認を受ける。 ・仲介者が取得したデータは当該機関に留める。（共有しない） ・個人データ、取引データへのアクセスはAML、CFT他規制に基づく場合に限り、仲介者がアクセス ・少額利用、低リスクの取引には高いプライバシー（匿名利用）を与える
流通量管理	金融政策、金融安定、実体経済への影響を考慮 ・CBDCの設計には、限度額、報酬に基づくツールを付与（投資形態の利用を抑制） ・オンライン、オフラインともに保有額に制限。自動的に預金に移転するウォーターフォール機能も検討

（ECB、Progress on the investigation phase of a digital euro – second report を基に作成）

また、12 月末のレポート[8]では、デジタルユーロ・プロジェクトの進捗状況と併せて、デジタルユーロのエコシステムにおけるユーロシステムと仲介者の担う役割の概説、デジタルユーロの流通に関するスキームなどが提案されている。

当該スキームは、デジタルユーロがユーロ圏全ての人々の通貨アンカーとしての目的を達成し、戦略的自律性と経済効率を確保するための最良の選択肢とするため、デジタルユーロを発行・流通させる際に遵守すべきルール及びその基準、手続などをユーロシステムと監督下にある仲介者間で役割と責任のバランスを確保するものとされている。

表 2.2　取引の管理と決済（仲介者とユーロシステムの役割案）

	仲介者	ユーロシステム
利用者管理	デジタルユーロのアカウント/ウォレットの管理 決済手段の提供・管理	監督下にある仲介者の管理
取引管理	取引開始 認証、検証 決済後処理	決済 決済後処理
流動性管理	デジタルユーロ化、現金化	発行、還収

出典：ECB,“Progress on the investigation phase of a digital euro –second report“, 21 December 2022,（https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov221221_Progress.en.pdf?f91e0b8ff8cbd6654d7e6b071a8f7071）,pp.6（筆者翻訳）

なお、そのスキームは、フロントエンドソリューションの開発市場に大きな柔軟性を与えるとともに、ユーロシステムの全体的な責任を確保するものとなるため、仲介者、消費者、小売業者を含む全ての市場参加者と協力しながら、デジタルユーロ・スキームのルールブックの起草・開発に 2023 年 1 月から取り組むこととされている。

一方、調査フェーズ内においては、ユーロシステムが開発しているバックエンドソリューションとフロントエンドソリューションの統合テストを行うため、2022 年 4 月に 5 分野のプロトタイプ開発企業を公募し、9 月に選定した上で統合テストを含むプロトタイプ演習も行われている。

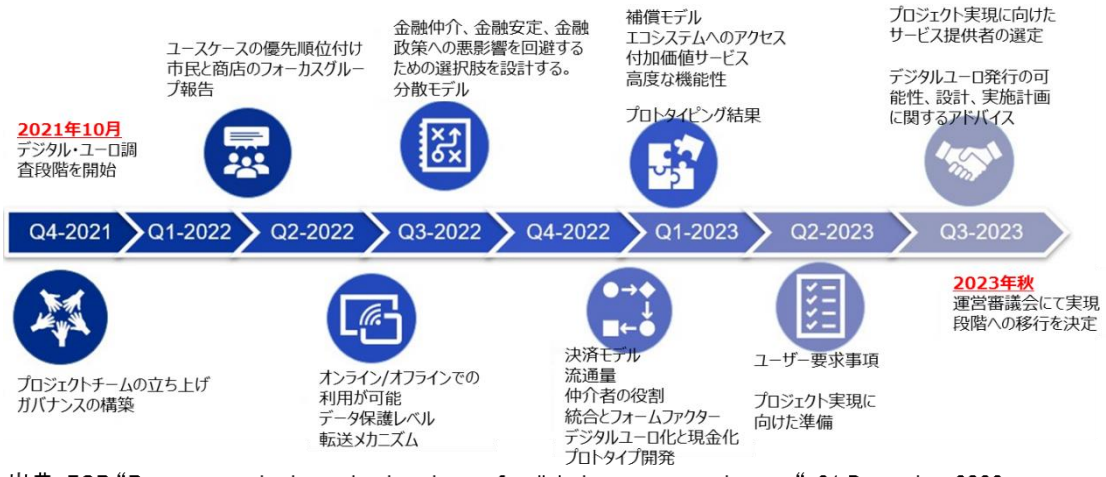
なお、プロトタイピングは、2023 年第 1 四半期に完了予定であり、その結果も公表されることとされている。

加えて、ECB は、調査フェーズ終了までにデジタルユーロ・プロジェクトの実現フェーズ移行に向けたコスト試算、導入要件を含むプロジェクト計画を作成する必要があることから、ユーロシステムの各種機能要件を整理して示すことで、ユーロシステム開発における潜在的な技術的解決策、想定コスト、開発期間などに関するマーケットリサーチを 2023 年 1 月から約 1 か月間実施した。

そして、調査フェーズが計画どおり進捗した場合、ECB 政策理事会は、2023 年秋にデジタルユーロの実現段階への移行を決定し、発行に関しては、実現段階を進める中で、立法の進展も踏まえて判断することになるとされている[9]。

表 2.3　プロトタイプ共同開発企業

ユースケース	選定企業
ピアツーピアのオンライン決済	Caixa Bank
ピアツーピアのオフライン決済	Worldline fdr1
支払者が行う店頭での支払い	EPI
受取人による販売店での支払い	Nexi
E コマース決済	Amazon



出典：ECB,“Progress on the investigation phase of a digital euro –second report“, 21 December 2022, (https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov221221_Progress.en.pdf?f91e0b8ff8cbd6654d7e6b071a8f7071),pp.3（筆者翻訳）

図 2.7　デジタルユーロ・プロジェクトのタイムライン

2.2.2　米国

(1) 米国連邦準備制度理事会の報告

米国連邦準備制度理事会（FRB）は、2022 年 1 月に CBDC をテーマとした初の報告書[10]を作成・公表し、広く一般からの意見を募集した。報告書では、公表目的を CBDC の利点とリスクに関する広く透明性のある議論を促進するためとしており、発行の決定に関しては、行政機関や議会の明確な支援なしに進めないことが示されている。その上で、CBDC のメリットとして、コスト低下や、より安全なデジタル決済手段の提供、国家間決済などの迅速化などを挙げる一方、デメリットとして、銀行など既存の金融仲介機能への影響や、プライバシー保護の確保などについて整理している。

(2) 大統領令

2022 年 3 月には、バイデン大統領がデジタルドルを含むデジタル資産の研究開発促進を指示する大統領令に署名し、米国財務省を始めとする関係機関に対して調査等を命じている。これを受けて、同年 9 月に米国財務省、科学技術政策局などが報告書を作成・公表しており、それに合わせる形で、ホワイトハウスは、デジタル資産の責任ある発展に向けた初めての包括的なフレームワークであるとして、CBDC の可能性を認識した上で米国版 CBDC のための政府の優先事項を反映した政策目標を策定した。

表 2.4　米国財務省、科学技術政策局の報告

財務省 「通貨と決済の未来」	米国における現金や決済システムの現状を概観した上で、ホールセール及びリテール CBDC の設計上の選択肢、また政策上の考慮事項を言及
科学技術政策局 「米国 CBDC システムの技術的評価」	政策目標を踏まえて、CBDC システムの技術的選択肢を分析の上、最小限の機能でプロトタイプを構築する場合の実現可能性を検討

表 2.5　米国ホワイトハウスが示す政策目標

① 消費者・投資家・ビジネスの利益提供とリスク軽減
② 経済成長と金融の安定促進、システミックリスクの低減
③ 決済システムの改善
④ 相互運用性と透明性
⑤ 金融包摂と公平性の促進
⑥ 国家安全保障
⑦ 人権
⑧ プライバシー保護、民主的及び環境的価値観

(3) 共同研究「プロジェクト・ハミルトン」

ボストン連邦準備銀行は、マサチューセッツ工科大学デジタル通貨イニシアチブとの共同研究「プロジェクト・ハミルトン」を進め、2022 年 2 月にフェーズ 1 の終了と報告書を作成・公表した。同報告書では、CBDC のコア・トランザクション・プロセッサの設計と研究、データ収集等が可能な柔軟なプラットフォーム構築を目標として、複数の設計アーキテクチャに対する評価が報告されている。なお、決済モデルには、UTXO[11]モデルを採用しており、2 種類のアーキテクチャが設計されている。

2022 年に実施しているフェーズ 2 においては、プライバシー、プログラマビリティ、相互運用性等様々な選択肢に関する検討が進められている。

なお、2022 年 12 月には、フェーズ 2 とプロジェクト・ハミルトンが終了した旨が報告された。

2.2.3 中国

中国では、2019 年末から開始したパイロット実験を、検証内容や実施地域を拡大しながら進めている。特に 2022 年 2 月に開催された北京五輪では、五輪会場の決済手段を、五輪パートナー企業の VISA カード、現金の人民元、及びデジタル人民元に限定する[12]など、認知度や技術的な優位性を各国関係者にアピールする場となった。その後もパイロット実験は、2022 年 8 月末時点で、15 省に跨る 23 都市で実施され、累計取引金額は 1,000 億元、取引回数は 3.6 億回に上っていると言われている[13]。また、2022 年 9 月の中国人民銀行の副総裁の発言において、広東省、四川省、河北省、江蘇省の各都市のパイロット区域を省全域へ段階的に拡大する方針が示されたところである[14]。

さらに、同時期に北京で開催された中国国際サービス貿易交易会（CIFTIS）において、IC カード、スマートウォッチ、デジタル ID カード、スマート学生証、電子高齢者証明書、スーパーSIM カードといった、10 数種類のハードウォレットが展示され、高齢者や学生など特殊な層の利用者もサポート可能なツールの開発が進んでいる[15]。

なお、中国人民銀行は、「デジタル人民元（e-CNY）」を、通貨流通量の公式統計に含める方針を発表し、2022 年 12 月の金融統計の公表から、e-CNY の流通量[16]を通貨流通量（M0）に含めて報告している。

2.2.4　その他

2022 年 5 月にジャマイカ中央銀行は、CBDC「JAM-DEX」を段階的に展開していく旨を発表した。JAM-DEX の特徴としては、中央銀行の RTGS である Jam-Clear と統合可能なインターフェースを提供するために、非ブロックチェーン型の形態を選択していること、金融包摂推進のため、合理化・簡素化された KYC 要件により、銀行口座を持たない国民にもアクセス可能な設計としていることなどがある。また、ジャマイカ中央銀行が、JAM-DEX での賃金支払と取引実施を促進するなど、利用環境の整備にも取り組んでおり[17]、JAM-DEX の利用は今後徐々に拡大していくものと考えられる。

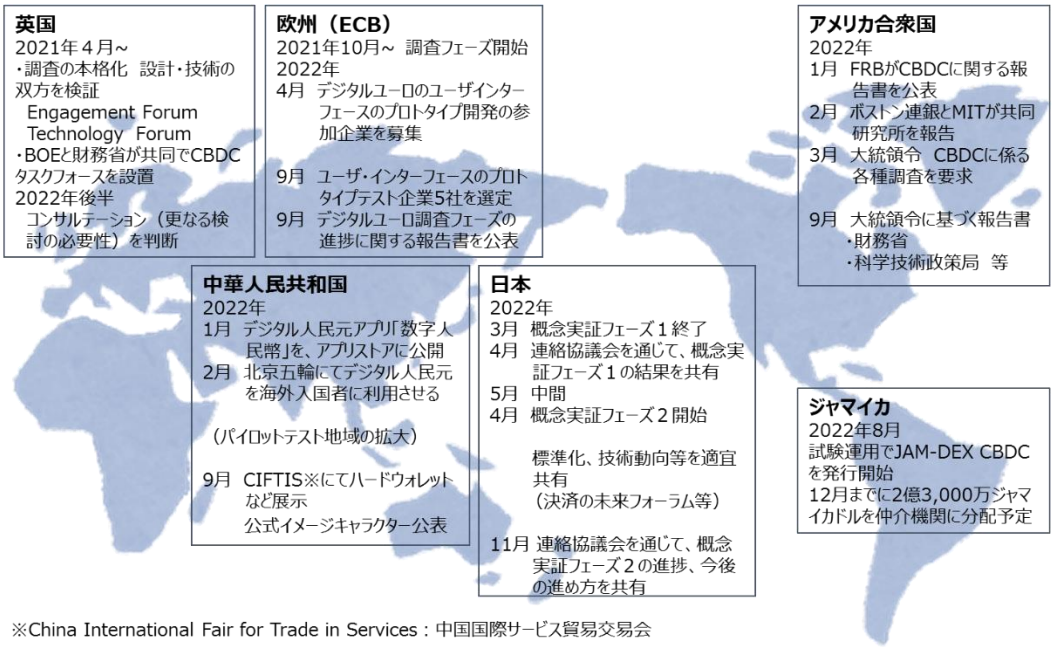


図 2.8　CBDC に関する国内外の主な状況

（各種資料[18]を基に筆者作成）

[1] 衆議院、第 208 回国会　財務金融委員会　第 18 号（令和 4 年 5 月 13 日（金曜日））会議録、（https://www.shugiin.go.jp/internet/itdb_kaigiroku.nsf/html/kaigiroku/009520820220513018.htm#p_honbun）

[2] 日本銀行、「中央銀行デジタル通貨に関する連絡協議会　中間整理」、2022 年 5 月 13 日、（https://www.boj.or.jp/paym/digital/rel220513b.pdf）

[3] 日本銀行、「中央銀行デジタル通貨に関する実証実験「概念実証フェーズ2」結果報告書」、2023 年 4 月 17 日、（https://www.boj.or.jp/paym/digital/dig230417a.pdf）

[4] 日本銀行、「「CBDC フォーラム」への参加説明会資料」、2023 年 3 月 16 日、（https://www.boj.or.jp/paym/digital/dig230316a.pdf）

[5] 日本銀行、「「リテール中央銀行デジタル通貨（CBDC）に関する公共政策上の原則」（仮訳）」、2021 年 10 月 14 日、（https://www.boj.or.jp/paym/digital/data/rel211014d.pdf）

[6] 日本銀行、「プライバシー保護技術とデジタル社会の決済・金融サービス」、2022 年 9 月 29 日、（https://www.boj.or.jp/research/brp/psr/data/psrb220929.pdf）

[7] ECB、“Progress on the investigation phase of a digital Euro”、2022.9.29、（https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf）

[8] ECB、“ECB publishes second progress report on the digital euro investigation phase”、2022.12.21、（https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews221221.en.html）

[9] ECB、Letter to ECON Chair Irene Tinagli –European Central Bank、2023.4.23、（https://www.ecb.europa.eu/pub/pdf/other/ecb.mepletter230424_tinagli~db4b48b842.en.pdf）

[10] Money and Payments:The U.S. Dollar in the Age of Digital Transformation 2022.1.20 FRB、（https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf）

[11] UTXO は Unspent Transaction Output の略称であり、「未使用のトランザクションの出力」である。UTXO モデルでは、取引ごとにインプットとアウトプット（手数料を含む）のそれぞれの合計額が等しくなるよう UTXO を消費、生成する。UTXO モデルでは、残高は保有する UTXO を全て計算することにより算出される。一方、アカウントベースのモデルでは、直接残高をブロックチェーンに記録している。

[12] 東京新聞、「「デジタル人民元」五輪会場で実証実験も存在感薄く…外国人向け PR なく、スマホアプリも使えず」、2022 年 2 月 12 日、（https://www.tokyo-np.co.jp/article/159729）

[13] ロイター、中国デジタル人民元、取引額が 1000 億元突破、2022 年 10 月 13 日、（https://jp.reuters.com/article/china-yuan-digital-idJPKBN2R80B1）

[14] 上海証券新聞、四地数字人民币试点将适时扩围至全省、2022 年 9 月 19 日、（https://news.cnstock.com/news,bwkx-202209-4958850.htm）

[15] 人民網日本語版、「デジタル人民元とトレンド玩具が出会うとどんな火花が散る！？」、2022 年 9 月 6 日、（http://j.people.com.cn/n3/2022/0906/c94476-10144029.html）

[16] 中国人民銀行の金融統計報告書によると、2022 年 12 月末時点での e-CNY の流通量は、136 億 1,000 万元（約 2,646 億円）で、M0 全体（10 兆 4,700 億元/約 204 兆円）の 0.13%とされている。

[17] Bank of Jamaica、“JAM-DEX facilitates Government Wage Payment Employment Generation (Christmas Work) Programme” ,6 January 2023,（https://boj.org.jm/jam-dex-facilitates-government-wage-paymentemployment-generation-christmas-work-programme/）

[18]【欧州】

・ECB、“Call for expression of interest for digital euro front-end prototyping”、2022.4.28、（https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs220428.en.pdf?3adf0ad3390238c2e4f0a6aa1e2a5fe3）

・ECB、“ECB selects external companies for joint prototyping of user interfaces for a digital euro”、2022.9.16、（https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews220916.en.html）

・ECB、“ECB publishes second progress report on the digital euro investigation phase”、2022.12.21、（https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews221221.en.html）

【中華人民共和国】

・JETRO、「デジタル人民元アプリ、アプリストアで提供開始（中国）」、2022 年 1 月 14 日、（https://www.jetro.go.jp/biznews/2022/01/0fe66561b1059063.html）

・日本経済新聞、「北京五輪でデジタル人民元を開放 「海外客はカードで」」、2022 年 2 月 2 日、（https://www.nikkei.com/article/DGXZQOUE255YQ0V20C22A1000000/）

・人民網日本語版、「デジタル人民元とトレンド玩具が出会うとどんな火花が散る！？」、2022 年 9 月 6 日、（http://j.people.com.cn/n3/2022/0906/c94476-10144029.html）

【日本】

・日本銀行、「中央銀行デジタル通貨に関する実証実験「概念実証フェーズ1」結果報告書」、2022 年 4 月 13 日、(https://www.boj.or.jp/paym/digital/rel220413b.pdf)
・日本銀行、「「決済の未来フォーラム　デジタル通貨分科会：中央銀行デジタル通貨を支える技術（第 3 回会合）」（1 月 11 日）の議事の概要」、2022 年 1 月 14 日、
(https://www.boj.or.jp/paym/outline/mirai_forum/rel220114c.htm)
・日本銀行、「「決済の未来フォーラム　デジタル通貨分科会：中央銀行デジタル通貨を支える技術（第 4 回会合）」（6 月 2 日）の議事の概要」、2022 年 6 月 8 日、
(https://www.boj.or.jp/paym/outline/mirai_forum/rel220608a.htm)
・日本銀行、「「決済の未来フォーラム　デジタル通貨分科会：中央銀行デジタル通貨を支える技術（第 5 回会合）」（12 月 20 日）の議事の概要」、2023 年 1 月 20 日、
(https://www.boj.or.jp/paym/outline/mirai_forum/mfo230120a.htm)
・日本銀行、「中央銀行デジタル通貨に関する日本銀行の取り組み」、2022 年 11 月 24 日、
(https://www.boj.or.jp/paym/digital/rel221124a.pdf)

【アメリカ合衆国】
・JETRO、「米 FRB、「デジタルドル」について報告書公表、5 月 20 日まで意見公募」、2022 年 1 月 26 日、
(https://www.jetro.go.jp/biznews/2022/01/f2d59929a54d2b45.html)
・ITMedia、「MIT らが CBDC の技術を検証　「Project Hamilton」の成果は」、2022 年 4 月 13 日、
(https://www.itmedia.co.jp/enterprise/articles/2204/13/news020.html)
・モーニングスター、「米国とEUによる暗号資産規制の最新動向」、2022 年 3 月 9 日、
(https://vc.morningstar.co.jp/010421.html)
・NCB Library、「米国財務省が政府に提出した CBDC 報告書」、2022 年 9 月 29 日、
(https://www.ncblibrary.com/posts/102406)
【ジャマイカ】
・Crypto Times、「中央銀行デジタル通貨(CBDC)の最新調査データが公開 ｜114 ヵ国が開発/調査に取り組み」、2023 年 1 月 5 日、(https://crypto-times.jp/cbdc-data-2023/)

参考付録１　中国人民銀行の特許出願状況について

1　概要

中国においては、デジタル人民元の発行に向けた市民参加型の実証実験が2019 年末から継続的に行われている。デジタル人民元の設計に関しては、2021 年 7 月にデジタル人民元の調査研究の進展に関する白書において、その大枠が記載されているが、その後は、設計に関する情報が少ないのが現状である。実証実験の進捗の裏でも、着実に研究開発が進められており、その動向は、特許出願に現れると考えられることから、特許出願状況を分析することで、デジタル人民元の設計と発行に向けた取組の状況を推察することとした。

2　調査内容

中国人民銀行を出願人又は権利保有者に含む出願特許を検索対象として、Google Patents における検索を行った。検索期間は、2012 年 1 月から 2022 年 8 月末日までとして、特許公開公報に記載の「技術領域」、「従来の技術」、「請求項１」等から対象となる「技術分野」や「用途・課題」について分類しながら、その傾向を分析した。

分類について

【技術分野】

出願時期と出願傾向の変化を把握するために、大きくブロックチェーン、デジタル通貨、関連技術及びユースケースに分類した。さらに、デジタル通貨及び関連技術に関しては、付表 1 のとおり細分化した。

【用途・課題】

中国人民銀行が出願する特許の目的を推察するために、当該特許が使われる用途や解決したい課題について付表 1 のとおり分類した。用途・課題に関して、複数の内容を記載する特許出願も数多くみられるが、記載が詳細である及び／又は最初に記載されている内容に基づき分類している。

なお、項目に関しては、例えば、小分類のオフライン決済は、大分類では利便性（容易）、社会性（金融包摂）ともみなせるが、多様性に区分したように、一つの大分類に代表させている。

付表１　技術分野、用途・課題の分類

【技術分野】

大分類	中分類	小分類
CBDC関連のブロックチェーン		
デジタル通貨	通貨の発行・管理	
	媒体・ウォレット	
	取引端末	
	チャージ	
	決済処理・手続	
	決済アプリ	
関連技術	データ処理	通信手段・方法
		情報の記録・管理
		情報の分散管理
		ビッグデータ解析
	情報セキュリティ	暗号技術
		認証
		鍵の管理
		不正検出・異常検知
	関連システム	インターネットバンキング
		その他の銀行システム
デジタル通貨のユースケース		
その他（関連外）		

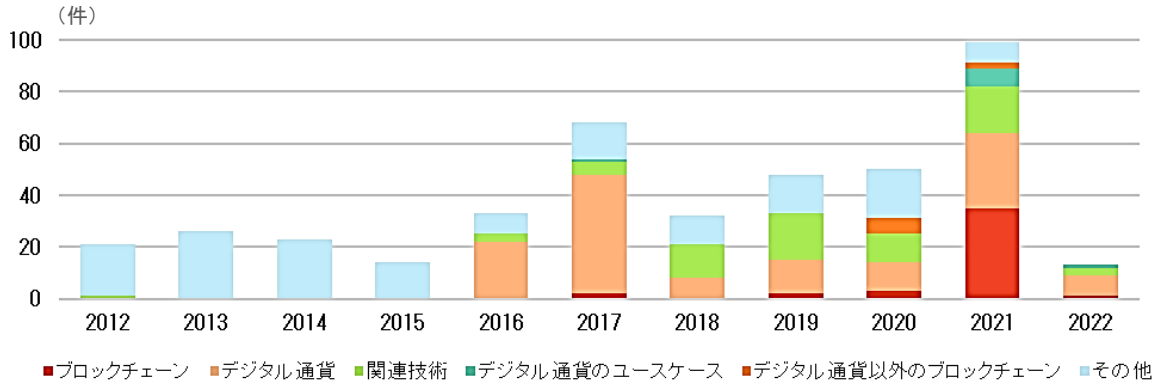
【用途・課題】

大分類	小分類
デジタル通貨の基本要件	
金融（通貨発行等）	
安全性の確保	不正・改ざんの防止
	情報漏洩の防止
	データ等の保守（維持）
利便性の向上	容易
	高速・効率
多様な決済手段の提供	取引相手・ソフト
	ハード
	オフライン決済
社会的な課題の解決	金融包摂
	相互運用
	省電力・電力確保
	事業継続
デジタル通貨のユースケース	

3　調査結果

調査の結果、427 件の特許が抽出され、その内訳としては、2015 年以前は、銀行券の偽造防止技術等を中心に出願されていたが、2014 年のデジタル通貨の研究開始を起点に、2016 年からデジタル通貨や関連技術に関する特許を中心に出願数が増加している。

次に、分野別、年代別の出願傾向から、中国人民銀行における CBDC に関する取組と現状を推察する。



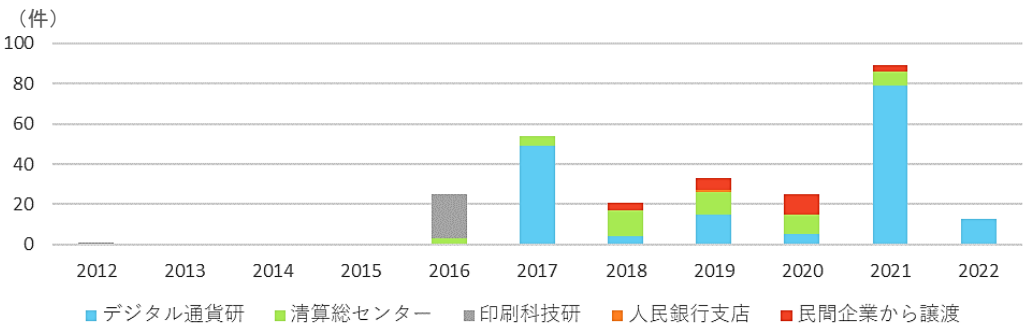
付図１　中国人民銀行の特許出願（全技術分野）

3.1　出願機関

中国人民銀行は、内部組織、支店、出資している傘下組織などを含め、多機能かつ極めて巨大な組織であり、他国の中央銀行とは比較が難しい組織である。そのような、中国人民銀行において、デジタル通貨に係る特許出願を行っている機関は、主として 3 機関である。2014 年に中央銀行が発行するデジタル通貨を研究する組織を立ち上げ、2017 年にデジタル通貨研究所を設置し、2017 年以降、同機関を中心に CBDC に関連する特許出願件数を伸ばしている。また、清算総センターにおいても、関連業務を想定して CBDC に係る研究組織を立ち上げ、研究及び特許出願を行っているものとみられ、複数の組織から特許が出願されている状況にある。その他、清華大学、建設銀行等との共同出願を行っているほか、アリペイ、工商銀行等から権利移転している特許出願も見られた。

付表 2　デジタル通貨関連特許を出願する主な機関

デジタル通貨研究所 （数字货币研究所）	2016 年に設立。設立の目的は、法定デジタル通貨の第一世代プロトタイプシステムの構築を完了させること。デジタル人民元の研究開発を主導。
清算総センター （清算总中心）	1990 年に設立。決済システムの運営、保守管理を担う。2018 年には、センター内にポスドク[1]研究ワークステーションを設立。また、2022 年には、ブロックチェーン、ビッグデータ解析等 9 つの研究の方向性を設定し、ポスドクを募集[2]。
印刷科学技術研究所 （印制科学技术研究所）	1959 年に設立。インキ、製版、紙幣用紙、偽造防止技術及び紙幣印刷機械の設計に係る研究施設並びに製版及び紙幣印刷の実験用作業場を保有。

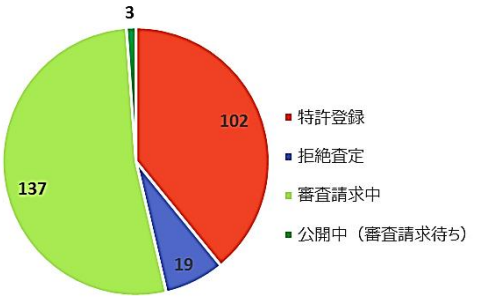


付図 2　機関別出願動向（CBDC 関連に限る）

3.2　審査の状況

中国人民銀行は、出願した CBDC 関連特許の大部分を審査請求しており、特許として登録された件数割合は、2022 年 8 月末時点で約 4 割である。ま

た、審査が終了した特許 121 件に占める特許登録件数 102 件は、84.3%の特許査定率となり、2020 年の中国における特許査定率(48.9%[3])から鑑みるに、極めて高い数値となっている。



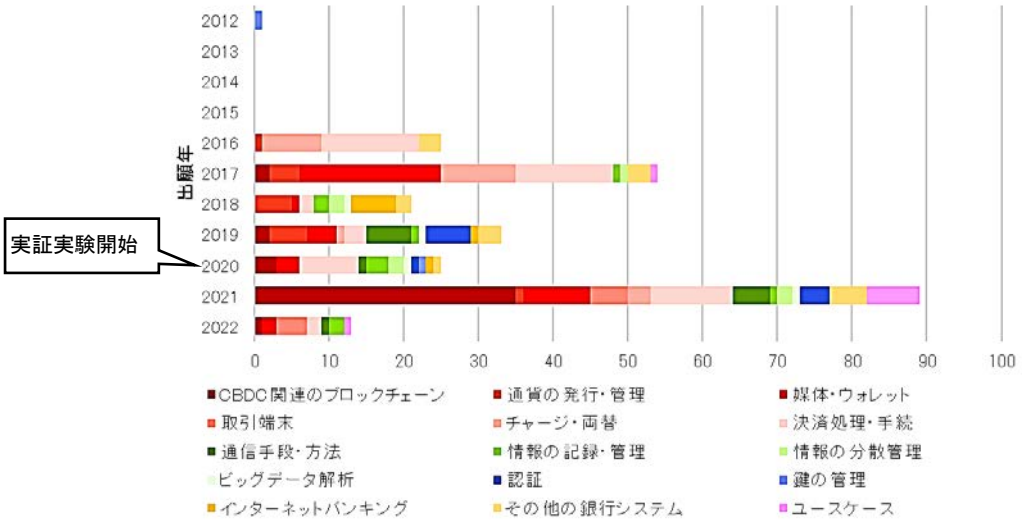
付図 3　特許査定の状況（CBDC 関連に限る）

3.3　出願傾向

本調査に当たっては、技術分野と用途・課題を分類し、それぞれの特許出願件数を整理した。その傾向の変化は、付図 4 及び付図 5 のとおりである。

技術分野については、2016 年の出願では、デジタル通貨の処理に関する基本的な事項が多く、その後、2017 年の出願では媒体・ウォレットに係る特許の比率が高まっている。

その後、2021 年の出願では、ブロックチェーンに関する特許が大幅に増加するとともに、その他取引に係る特許や情報処理に係る特許など全般的に増加している。なお、ブロックチェーンについては、スマートコントラクト、デジタル証明書の管理、ウォレットアドレスの管理など実装に近い内容の出願が複数なされているほか、国境を越えた取引やクロスチェーンのような多様

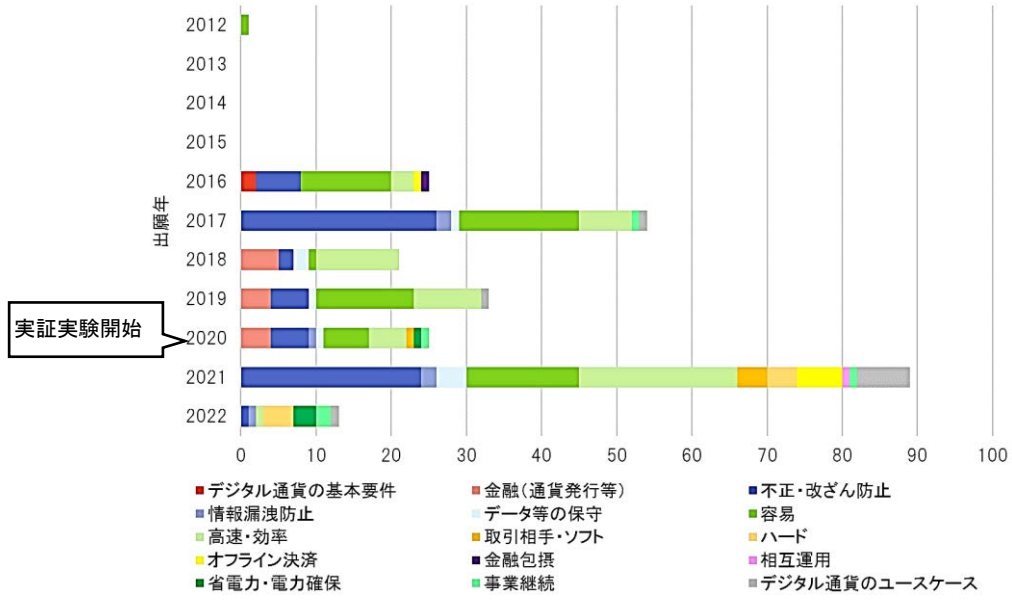


付図 4　技術分野別出願件数の推移

な取引についても出願が見られる。ユースケースについては、いずれも乗り物に関する出願であり、「公共交通機関」、「車載」、「IoV[4]」、「位置検出」等への言及が見られる。

次に、用途・課題の分類ごとに出願件数の推移を見ると、「安全性の確保（不正・改ざん防止等）」、「利便性の向上（容易、高速・効率）」については、2016年以降、主たる課題として認識して、これに関連する特許が出願されていることが分かる。特に、2021年の出願件数の大幅な増加の中では、実証実験にて課題（「不正・改ざん防止」、「高速・効率」「オフライン決済」）の解決を望むような特許出願の伸び率が大きくなっている。

「不正・改ざん防止」については、取引における各種の検証や証明に関する特許が出願されている。また、用途は未記載であるものの、ブロックチェーンノードの秘密鍵で発行したデジタル証明書のPKI[5]（公開鍵認証基盤）に関する特許が7件出願されており、発明者の中にはデジタル通貨の取引やID認証に係る特許を出願している者が含まれていることから、CBDCに関する公開鍵基盤を検討している可能性も見られる。「高速・効率」については、特にまとまった特許出願は見られないが、コントラクトの効率化、複数IDの集約と認証、データ転送の高速化等、多様な観点から特許が出願されている。オフラインに関する特許については、オフライン決済そのものに係る技術に関しては、特にまとまった出願が見られないが、デジタル通貨ICカードの紛失をオフラインで報告・検証するための方法、緊急時における衛星通信システムを用いたウォレットの遠隔制御方法のような、非常時の対応に係る特許出願が見受けられる。



付図5　用途・課題別出願件数の推移

3.4 UTXO[6]モデルに関する特許出願

ブロックチェーンに関する特許出願のうち、コアな設計に係る特許として、米国のプロジェクトハミルトンや ECB が設計を検討している UTXO モデルに関する特許 CN113592644A「ブロックチェーン UTXO モデルベースの取引方法及び装置」（2021 年 7 月出願）がある。2022 年 12 月末時点では、審査請求中ではあるが、明細書によると本特許は、旧フェイスブック社（現メタ社）の Libra 構想において提案された FastPay スケーリングソリューションがアカウントモデルに基づく処理であることに対し、UTXO モデルとして、ユーザーの取引効率、システムのセキュリティ確保、ネットワークの信頼構築に加え、システムの正常な運用を提供する特許として出願されたものである。

3.5 国際出願

中国人民銀行から出願された特許のうち、国際出願が行われているのは 4 件である。中国人民銀行の特許出願に係る方針、戦略は定かではないが、一般論として、これらの特許は、中国国外では公知の技術として自由に使えるため、我が国における CBDC の制度設計における知的財産面への影響は少ないと考えられる。国際出願された 4 件は、付表 3 のとおりである。WO2022028486A1 についてはブロックチェーン（詳細な用途は未記載）、WO2022184137A1 についてはスマートコントラクトに関する特許出願であるが、日本国内で審査を受けて権利化するために必要な「国内移行手続」は現時点でなされていない。CBDC の制度設計時等において改めて影響を確認することが考えられる。

付表 3　国際出願特許

国際公開番号（最初の出願日）	発明の名称（仮訳）（概要）	出願国等
WO2013166672A1（2012/5/9）	コンバインド印刷装置（磁気配向可能なスクリーン印刷ユニット、凸版印刷ユニットを備えた印刷機）	日、英、独、オーストリアで特許化
WO2020119608A1（2018/12/10）	Spark shuffle* ベースのリモート ダイレクト メモリ アクセス システムおよび方法	欧州特許庁にて公開
WO2022028486A1（2020/8/4）	ファイル共有方法、デバイス、およびシステム（ブロックチェーン・ファイルの共有方法で、複数のファイル圧縮パッケージを用いる）	国際公開中（各国出願期限：通常2023/2/4）
WO2022184137A1（2021/3/3）	ブロックチェーンで乱数を生成する方法および装置（ブロックチェーンで鍵生成等に用いる乱数を生成する方法）	国際公開中（各国出願期限：通常2023/9/3）

＊Apache Spark：データ解析や機械学習を実行する多言語エンジンで、Spark Shuffleとはデータ処理能力向上のためデータ再分散を行うこと。

4 まとめ

中国人民銀行のデジタル人民元発行に向けた取組は、2014 年の研究組織立ち上げから現在の実証実験に至るまで、計画的に進められており、その成果は特許出願という形でも着実に進められていることがわかった。そして、近

年では、中国国内で進められている実証実験を進める中で判明した課題解決に向けた特許出願、更に、社会実装に向けた特許出願へとその傾向も変移していることも明らかとなった。

冒頭紹介した中国人民銀行公表の白書によると、デジタル人民元のシステムの開発は、デジタル経済の時代に国民の需要を満たす新しい人民元の形を作ることを目的としている。また、信頼性、効率性、適応性、開放性に優れたリテール決済インフラに支えられたデジタル人民元のシステムは、デジタル経済、金融包摂を強化し、決済システムを効率化するものとされており、中国人民銀行内のそれぞれの組織が決済の将来像を想定しながら、研究開発を進めていることが伺える。

これまで、紙幣の製造や流通に係る特許を保有し、時代と共に新たな技術を提供してきたのと同様に、今後もデジタル人民元に関して、不正、改ざんに対する抵抗力を有し、情報を安全に流通させるための研究開発が継続されることが想定される。そして、その研究開発の動向は、公開情報が少ない中国においても、特許出願という形で現れてくるものと考えられる。

今後、発行が計画されているデジタル人民元であるが、発行後も公開情報と合わせて中国人民銀行の出願特許を分析することで、中国人民銀行の方向性を確かめることに役立つと考えられる。

---

[1] 博士号を取得したのち、大学や研究機関において任期付きで研究活動をする非正規雇用スタッフ。正式な名称はポストドクター「博士研究員」。

[2] 中国人民銀行ホームページ、http://www.pbc.gov.cn/rmyh/105208/4418520/index.html

[3] 特許庁、特許行政年次報告書 2022 年版 12 頁

[4] IoT を自動車分野に特化した「Internet of Vehecles」の略であり、自動車業界の次世代市場を攻略するためのキーワードとして拡がり、自動車メーカがインターネット企業と提携する動きが中国国内で活発化している。

[5] 「Public Key Infrastructure」の略であり、公開鍵暗号技術と電子署名を使って、インターネット上で安全な通信ができるようにするための環境のことを言う。

[6] UTXO は Unspent Transaction Output の略称であり、「未使用のトランザクションの出力」である。UTXO モデルでは、取引ごとにインプットとアウトプット（手数料を含む）のそれぞれの合計額が等しくなるよう UTXO を消費、生成する。UTXO モデルでは、残高は保有する UTXO を全て計算することにより算出される。一方、アカウントベースのモデルでは、直接残高をブロックチェーンに記録している。

3　暗号資産、電子マネー等の事件・攻撃等

3.1　概要

暗号資産、電子マネー等についての事件・攻撃を理解することは、CBDC 等デジタル通貨が普及する際のリスクを想定することにつながる。そこで、近年の事件・攻撃の傾向を時点整理し、想定されるリスクを幅広に把握することで、CBDC 設計の検討における一助とする。

3.2　国内の金融機関等への攻撃

国内の金融機関に対する攻撃に関しては、不正アクセスによるランサムウェア感染、ホームページ閲覧不可、個人情報漏えい、顧客資産の流出といった報告が金融庁からなされており、多くのセキュリティインシデントの発生が確認できる[1]。また、金融庁のホームページでは、近年の情勢を踏まえてサイバー攻撃事案の潜在的なリスクは高まっているとして、2022 年 2 月には、各金融機関等に対してサイバー攻撃の脅威に対する認識を深め、国内外の拠点においてリスク低減のための措置、インシデントの早期検知、インシデント発生時の適切な対処・回復など必要となる対策の強化を行うよう注意喚起を行っている[2]。

その他、利用者にショートメッセージサービス（SMS）を送付するなどして、アクセスさせることで利用者情報を詐取するフィッシング[3]事案は、2021 年度よりも増していることが報告されている。フィッシング対策協議会に新たに寄せられた事案の中には、国税庁や金融庁を名乗るものも発生しており、2022 年 10 月に報告されたフィッシングの内訳は、Amazon を名乗るものが報告数全体の約 20.9%、えきねっと（JR 東日本）を名乗るものが約 20.4%となり、次いで報告が多かったイオンカード、三井住友カード、国税庁、JCB を名乗るフィッシングの報告を合わせると、全体の約 74.3%を占めるとされている。

なお、フィッシング対策協議会では、報告事例を適宜更新するとともに、事業者には、業態別に対応策を例示しながら対応の検討を促すとともに、利用者に対して、メールアドレスの切替えや情報の確認など注意を促している[4]。

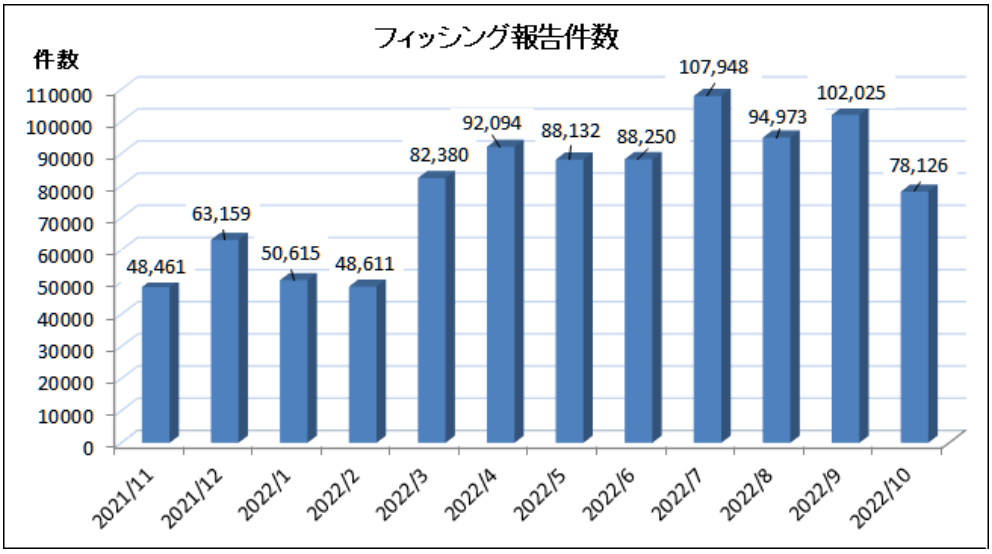


図 3.1　フィッシング報告件数の推移

（出典：フィッシング対策協議会、「2022/10 フィッシング報告状況（月次報告書）」、2022 年 10 月）

3.3　暗号資産取引に関連するサイバー攻撃等

3.3.1　2022 年の概況

2022 年の暗号資産に係る攻撃の動向を見ると、2021 年と比較して、被害件数が減少する一方、1 件当たりの被害額が上昇し、被害額合計は約 38 億ドルに達し、過去最大となったと報告されている[5]。

攻撃ターゲットについては、2019 年までは秘密鍵の窃取など暗号資産取引所を標的にすることが多かったが、近年ではブロックチェーン間の価値移転を行うためのサービスなどを標的とする攻撃が増加している。年間攻撃被害額における比率は、2021 年には全体の 73.3%、2022 年には 82.1%まで上昇し[6]、市場の広がりがブロックチェーン間の相互運用性のニーズを生じさせ、ニーズを満たすために提供されたサービスの脆弱性が狙われた結果となった。

攻撃の種別については、2021 年に増加したフラッシュローン攻撃[7]やラグプル詐欺[8]のような事例（被害額）が 2022 年に入り減少する一方、2022 年は、クロスチェーンブリッジを狙った攻撃が増加している（詳細は事例と併せて後述）。

また、攻撃者は、窃取した暗号資産の匿名性を高める「ミキシングサービス」を利用しており、米国の財務省外国資産管理室は、マネーロンダリングのために使われた一部のウォレットアドレスを特定し、これらのアドレスもブロックするとともに、2022 年 5 月に「Blender.io」、8 月には「Tornado Cash（暗号通貨タンブラー：プロトコル）」といった暗号資産のミキシング

を行う企業等に対して制裁措置を発令した。

加えて、オランダ捜査機関が同じく 8 月に Tornado Cash の開発エンジニアをマネーロンダリングほう助罪で逮捕するなど、資金洗浄を可能とするサービスへの制裁を強化している。

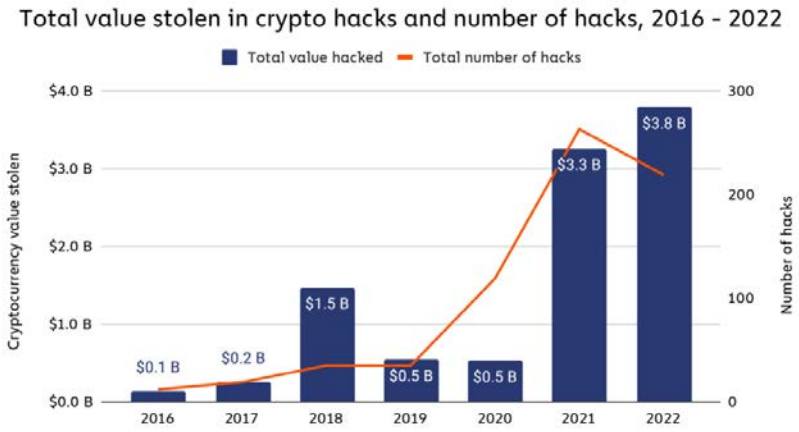


図 3.2　ハッキング件数及び被害額

出典:Chainalysis、“2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers”、2023.2.1、https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/

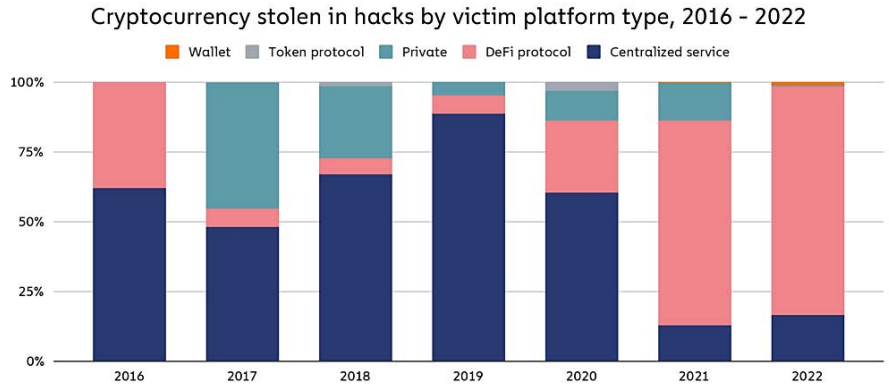


図 3.3　ハッキング被害対象の変移

出典:Chainalysis、“2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers”、2023.2.1、https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/

3.3.2　クロスチェーンブリッジを狙った攻撃

2022 年に被害額が大きく増加した攻撃事例として、ブロックチェーン間の価値移転を可能とするクロスチェーンブリッジを狙う事例がある。ここでは、ブリッジの基本的な仕組みと攻撃事例を整理する。

(1)　クロスチェーンブリッジとは

クロスチェーンブリッジは、規格・仕様の異なるブロックチェーン同士を相互に作用させ、暗号資産、トークン又はデータの転送を可能とするプロトコルである。クロスチェーンブリッジの数は近年増加しているが、一

般的な例として、図 3.4 に示すようなモデル（ロック、ミント、バーン）が適用されている。一般的なモデルとしては、一方のブロックチェーンの資産のアドレスをロックする仕組み、もう一方のブロックチェーンへ伝達する仕組み、そして、ロックされていることを確認した上で、同等の価値を有する資産を発行するような仕組みから構成される。原理としては単純であるが、取引速度、セキュリティ、プライバシーといった課題を解決するために様々な種類のブリッジが開発されている。

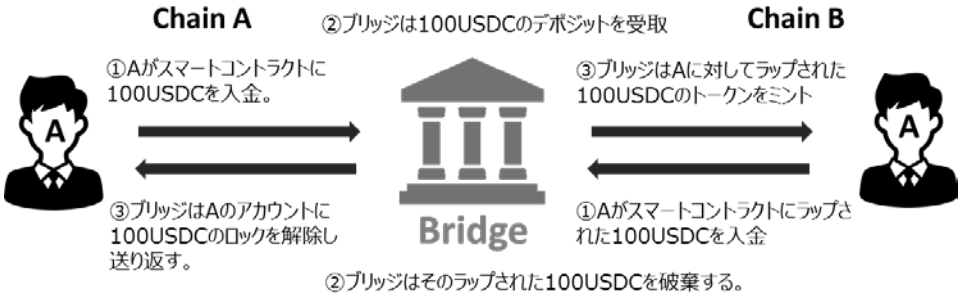


図 3.4　ブリッジの一般的なモデル（ロック、ミント、バーン）

(2)　攻撃事例

イ　Wormhole、ハッキングで約 373 億円相当流出

2022 年 2 月 3 日、異なる暗号資産の相互接続を可能とする技術を開発する Wormhole で、ソラナとイーサリアムのブリッジから 12 万 ETH（約 373 億円）が流出したと報告された。

Wormhole は、イーサリアムやソラナ、Polygon、Avalanche、Terra などの複数のブロックチェーンを繋ぐブリッジである。Wormhole では、上述したようなブリッジの基本的な仕組みを構築していたが、元のチェーンのトークンの署名検証に脆弱性を有するバグが存在し、攻撃者は、その脆弱性が狙って、有効な署名を偽造し、暗号資産を移転、ロックさせることなく新たな暗号資産を生成させたと言われている。

なお、オープンソースのコードコミットでは、この脆弱性を修正するコードについて、攻撃当日に Wormhole の GitHub リポジトリへアップロードされたことが確認されており [9]、審査等本稼働までの隙を突かれた攻撃と考えられている [10]。

図 3.5　Wormhole ブリッジへの攻撃（イメージ）

ロ　「Axie Infinity」のサイドチェーン「Ronin」への攻撃

2022 年 3 月 29 日、アクシーインフィニティのサイドチェーン「Ronin」が攻撃され、約 6 億 2,400 万ドルの暗号資産が盗まれたことを公表した。攻撃者は、九つのバリデータノードのうち過半数を上回る五つのノードを支配して、引き出しクレデンシャルを偽造し、資金の盗み出しに成功している。

なお、不正流出は 23 日であり、発覚までに約 1 週間を要しており、監視の必要性を再認識させた事案でもある [11]。

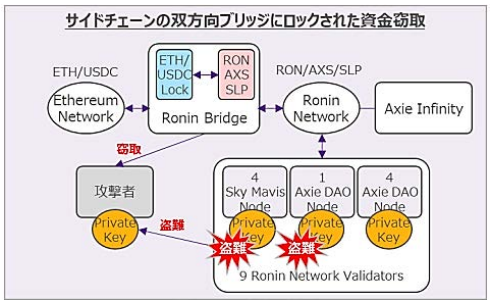


図 3.6　Ronin ネットワークからの資金窃取

出典：金融庁、「分散型金融システムのトラストチェーンにおける技術リスクに関する研究研究結果報告書（株式会社クニエ）」、122 頁、2022 年 6 月、（https://www.fsa.go.jp/policy/bgin/ResearchPaper_qunie_ja.pdf）

ハ　暗号資産交換バイナンスから約 5.7 億ドルのトークン流出

バイナンスは、2022 年 10 月 7 日、約 5 億 7000 万ドル（約 830 億円）相当のトークンが流出するハッキング被害を受けたと発表した。また、影響を受けたブロックチェーン（分散型台帳）の運用を一時的に停止し、その後に再開している [12]。

バイナンスでは、バイナンスチェーンとバイナンススマートチェーンについて、トークン・ハブを介して接続し、それぞれの資産を同期させる仕組みを構築していた。ブロックチェーンセキュリティサービスを提供する Beosin 社のセキュリティチームは、トークン・ハブがクロスチェーン取引の検証を行う際に、IAVL ツリー[13]を検証するための特別なプリコンパイルされたコントラクトを使用していたことが原因であることを発見している。そして、この実装には脆弱性があり、攻撃者が任意のメッセージを偽造することが可能となったとされている [14]。

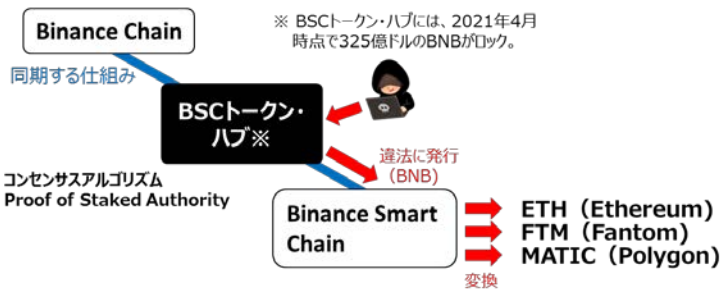


図 3.7　バイナンスへの攻撃（イメージ）

(3) 資金洗浄

2022 年は、上述したようにクロスチェーンブリッジなどを標的にした攻撃により、多くの資産が流出した。攻撃者は、不正に入手した暗号資産を洗浄するためにミキシングサービスを利用した。元来、暗号資産取引における匿名性を確保し、利用者のプライバシーや個人情報を守るために安全な使用環境を構築するために開発・提供されているミキシングサービスであるが、2022 年の攻撃時にも利用されたように、悪意ある攻撃者の資金洗浄に使われているのが実状である。

米国財務省の外国資産管理局（OFAC）や他国の同等機関は、国家安全保障や外交政策に対する脅威と見られる国、政権、個人、団体について制裁を実施している。2022 年には、暗号資産に関連する団体などに制裁を加える中、マネーロンダリングの温床となるような、ミキシングサービスを提供する組織にも制裁を加えている。

表 3.1　2022 年に米国で制裁を受けた組織等

組織名称	制裁の理由
Lazarus Group	北朝鮮政府のためのハッキングや暗号の窃盗
Ahmad Khatibi Aghada	ランサムウェア
Amir Hossein Nikaeen Ravari	ランサムウェア
Alex Adrianus Martinus Peijnenburg	麻薬密売
Matthew Simon Grimm	麻薬密売
Hydra Marketplace	ダークネットマーケットとマネーロンダリング
Garantex	マネーロンダリング
Blender.io	マネーロンダリング
Tornado Cash	マネーロンダリング
Task Force Rusich	ウクライナのロシア準軍事組織

出典：Chainalysis、How 2022's Biggest Cryptocurrency Sanctions Designations Affected Crypto Crime
https://blog.chainalysis.com/reports/how-2022-crypto-sanction-designations-affected-crypto-crime/

3.3.3　その他事例

(1) Android™、iOS[15]デバイスを標的とした暗号化マルウェアアプリ

ウイルス対策ソフト開発企業である ESET 社は、2022 年 3 月、同社運営セキュリティ情報サイトである「welivesecurity™」上で、Android™ 及び iOS 向けの暗号資産ウォレットアプリを装い、認証情報を盗み出す複数の悪意のあるアプリを確認したとして注意喚起を行っている [16]。

同サイトによると、Android™、iOS それぞれで、インストール時の挙動

が異なるとのことである。Android™ では、正規ウォレットアプリがインストールされていると、証明書署名の異なる同名アプリのインストールができないことから、攻撃ターゲットを新規ユーザーとしている。一方、iOS の場合、正規アプリと偽のアプリの両方をインストールできる仕様となっているため、攻撃ターゲットが広く設定されているようである。

ESET 社は、どちらのアプリも、広告サイトから偽のダウンロードサイトに誘導される経路を辿るため、公式 Web サイトにリンクされている公式アプリストアからのインストールをするよう注意喚起を行っている。

図 3.8　偽アプリダウンロード時の画面

（出典：ESET 社、“Crypto malware in patched wallets targeting Android and iOS devices”、
（https://www.welivesecurity.com/2022/03/24/crypto-malware-patched-wallets-targeting-android-ios-devices/））

(2) 他の暗号資産詐欺グループが運営する Web サイトへの寄生

2022 年に新たに確認された詐欺事例として、トレンドマイクロ社から攻撃グループ「Water Labbu」の事例が挙げられている [17]。Water Labbu の手口は、他の詐欺グループが作成した偽の Web サイトに不正プログラムを埋め込み寄生することで、他の詐欺グループが騙した利用者の資産を盗み取るものである。

詐欺グループが詐欺グループを利用するという構図であり、被害者からすると一つの被害として変わりないが、2022 年に新たな事例として注意喚起が行われているものである。

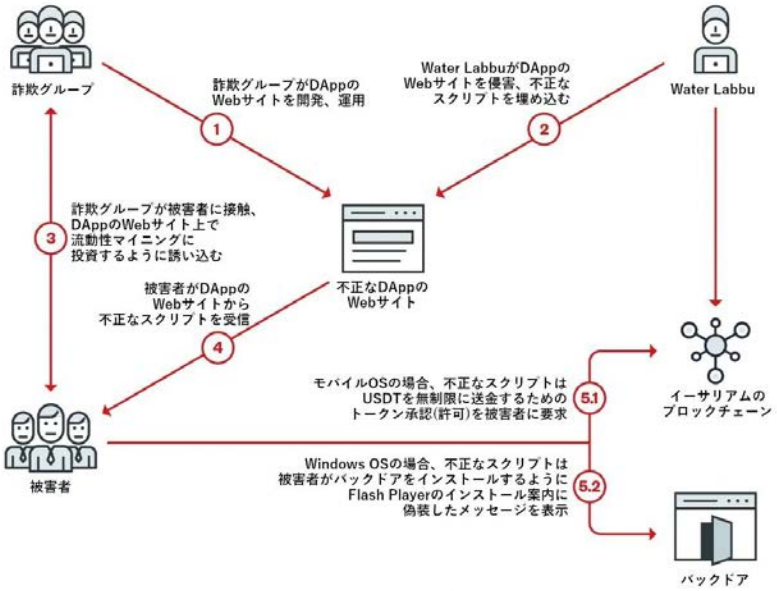


図 3.9　Water Labbu による暗号資産窃取手口

出典:TrendMicro、新たな攻撃グループ「Water Labbu」による暗号資産窃取の手口、
https://www.trendmicro.com/ja_jp/research/22/k/water-labbu-abuses-malicious-dapps-to-steal-cryptocurrency.html

3.4　総括

犯罪の動向を整理した結果、攻撃の対象にブロックチェーン間の価値移転（クロスチェーンブリッジ）を行うためのサービスが増えるなど、暗号資産取引の全体を俯瞰しながら、脆弱性を有する要素が攻撃されていることがわかる。クロスチェーンブリッジに関しては、CBDC においても何らかの形で資産をロックして、別の資産（例：オフライン）に交換するような考え方が見受けられる [18]ことから、暗号資産取引に見られるような攻撃事例から学ぶところもあると考えられる。

また、攻撃対象は、利用者からの情報窃取にも広がっており、正規のアプリになりすました偽アプリの脅威まで報告されている。同様の攻撃は、CBDC 発行時にも起こり得ることであり、こうした犯罪、攻撃事例の研究は有益であると考えられる。

[1] 金融庁、「金融機関のシステム障害に関する分析レポート」、2022 年 6 月、（https://www.fsa.go.jp/news/r3/20220630/system01.pdf）

[2] 金融庁、「昨今の情勢を踏まえた金融機関におけるサイバーセキュリティ対策の強化について」、令和 4 年 2 月 24 日、（https://www.fsa.go.jp/news/r3/cyber/0224oshirase.html）

[3] 実在する組織を騙って、ユーザネーム、パスワード、アカウント ID、ATM の暗証番号、クレジットカード番号といった個人情報を詐取する行為

[4] フィッシング対策協議会ホームページ、「2022/10 フィッシング報告状況(月次報告書)」、2022 年 10 月（https://www.antiphishing.jp/report/monthly/202210.html）

[5] Chainalysis、“2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers”、2023.2.1、（https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/）

[6] Chainalysis、“2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers”、2023.2.1、（https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/）

[7] 1つのトランザクション内で無利子・無担保の借入返済を行う仕組みを悪用し暗号資産を搾取する攻撃

[8] DeFi プロジェクトの開発者などの運営側が、投資家を騙し、資産を持ち逃げしたり、大量に売却したりする「出口詐欺」の総称。

[9] The Verge、Wormhole cryptocurrency platform hacked for $325 million after error on GitHub、（https://www.theverge.com/2022/2/3/22916111/wormhole-hack-github-error-325-million-theft-ethereum-solana）

[10] HEDGE GUIDE、「ブリッジプロトコル「ワームホール」で約 373 億円が盗難。DeFi で発生した過去最大規模のハッキングを解説」、2022 年 3 月 2 日、（https://hedge.guide/feature/wormhole-hacking-bc202203.html）

[11] Blockchain Security Alliance、Global Web3 Security Report 2022 P.4、（https://www.beosin.com/resources/Global_Web3_Security_Report_2022_.pdf）

[12] 日本経済新聞、「仮想通貨交換バイナンス、830 億円のトークン流出」、2022 年 10 月 8 日、（https://www.nikkei.com/article/DGXZQOGN07DDO0X01C22A0000000/）

[13] IAVL 木は、Immutable（不変） Adelson-Velsky and Landis (AVL) データ構造の略で、自己調整可能な二分探索木を実装しているものを指す。なお、AVL 木（えーぶいえるき、AVL tree、Adelson-Velskii and Landis' tree）とは、コンピュータサイエンスにおいて、「どのノードの左右部分木の高さの差も 1 以下」という条件を満たす二分探索木のことである。平衡二分探索木の 1 つで、木に対する操作によって条件を満たさないノードが発生しても、回転と呼ばれる操作を行うだけで木を AVL 木に再構成でき、平衡を維持できる。

[14] Blockchain Security Alliance、Global Web3 Security Report 2022 P.5、（https://www.beosin.com/resources/Global_Web3_Security_Report_2022_.pdf）

[15] iOS は Apple が開発及び提供する、iPhone、iPod touch、iPad など Apple 社製の製品向けのモバイルオペレーティングシステム。なお、IOS は、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における登録商標または商標であり、ライセンスに基づき使用されています。

[16] ESET、Crypto malware in patched wallets targeting Android and iOS devices 、（https://www.welivesecurity.com/2022/03/24/crypto-malware-patched-wallets-targeting-android-ios-devices/）

[17] TrendMicro、「新たな攻撃グループ「Water Labbu」による暗号資産窃取の手口」、（https://www.trendmicro.com/ja_jp/research/22/k/water-labbu-abuses-malicious-dapps-to-steal-cryptocurrency.html）

[18] ECB,“The Eurosystem’s technical onboarding package for digital euro prototyping-Annex 1 – Front-end prototype providers technical onboarding package”,pp.12-13,2022.12.7,(https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs221207_annex1_front_end_prototype_providers_technical_onboarding_package.en.pdf?96894d1ebc6c998d75233c57bf1c66eb)

参考付録２　暗号資産価値の急落、破綻事例

1　概要

2022 年には暗号資産取引所において無担保型ステーブルコイン価格の急落、取引所の破綻といった資産保有者にも影響を及ぼす大きな出来事が発生している。CBDC に直接関係するものではないが、デジタル資産に関するものとして、事例の概略を記すものである。

2　事例

(1) 無担保型ステーブルコイン「Terra USD」の急落

資産価値のボラティリティが激しく、支払手段としては使いにくいと言われている暗号資産の弱点を補うために作り出されたのが、法定通貨との間で安定した価値を維持するなどの仕組みを持つステーブルコインである。

価値の安定を基本とするステーブルコインであるが、2022 年 5 月、ステーブルコインの一つである「TerraUSD（UST)」が数日の間に、1 UST の対米ドル価値が 1 ドルから 10 セント台にまで一気に急落する事象が発生した。

TerraUSD は、1 UST が 1 ドルとほぼ同等の価値となるよう設計されたステーブルコインであったが、その設計は、法定通貨を担保にするのではなく、供給量をアルゴリズムに基づき調整する無担保型設計のアルゴリズム型ステーブルコインであった。そして、アルゴリズム型ステーブルコインの TerraUSD は、保有者に有利な運用利回り（年利約 20%）を保証する仕組みの「アンカープロトコル」を作り上げて投資家に投資させるものでもあり、2022 年 4 月中旬時点では時価総額がバイナンス（Binance USD）を抜いて、テザー（Tether)、USD コイン（USD Coin）に次ぐステーブルコインの第 3 位に浮上していた。

しかし、同年 5 月に入り、一部、信用不安を抱いた投資家がアンカープロトコル（Anchor Protocol）から大量引出しを行ったとの情報がソーシャルネットワーク上で流れ、それを起点に相次ぐ引出しに繋がり、取り付け騒ぎのような状態になったと言われている[1]。それにより、信用不安が更に高まり、「TerraUSD」及び供給量調整に使われていた別の暗号資産である「ルナ」が暴落し、ドルとの連動性を保てなくなったものである。

(2) 暗号資産取引所「FTX」の経営破綻

バハマに本拠を置き、各国で暗号資産交換業者として業務を行ってきた FTX は、2022 年 11 月初旬に財務の健全性を疑問視する報道がなされたことを契機に、FTX が発行する暗号資産「FTT」の価値の下落や、機関投資家の

資金引出し等を発生させた。結果として FTX は債務超過となり、同年 11 月 11 日に連邦破産法第 11 条（チャプター11）の適用を米裁判所に申請し、経営破綻した。

なお、破綻時における負債総額は推定で 100 億ドルから 500 億ドル（日本円で約 1 兆 4000 億円から最大 7 兆円近く）、また債権者は 100 万人を超える可能性があると報じられている[2]。

FTX の破綻に際し、米国証券取引委員会（SEC）は、破綻当時の FTX の経営者及び関連する他の事業者に対し、以下の行為等を行ったとして同年 12 月に提訴した[3,4]。

なお、本案件は、レポート作成時点において未だ係属中である。

- 暗号資産投資ファンド（以降、「ファンド」と表記）に対する顧客資金の私的流用
- 顧客資産と FTX 資産のファンド内での混合、非公開のベンチャー企業等への投資
- FTX プラットフォーム上における融資条件の免除等、ファンドに対する特別待遇の私的な付与

また、FTX の経営破綻は各国の子会社にも波及し、日本法人である FTX Japan においては、顧客資産の引出しが一時凍結される事態となった。これを受け、FTX Japan の有する顧客資産が国外の関連会社等に流出する事態を防ぐため、金融庁が業務改善命令等の行政処分を実施し、事態の改善を求めている[5]。

なお、FTX Japan は資金決済法上の暗号資産交換業者及び金融商品取引法上の金融商品取引業者として登録しており、顧客資産の分別管理、顧客暗号資産のうち 95%をコールドウォレットで保管する等の義務が法的に定められており、顧客の保護が図られている[6]。

3 まとめ

本来は価値が安定するはずのステーブルコインの価値の急落、暗号資産取引所の財務健全性への疑いからの経営破綻を取り上げたが、共通するのは、いずれも信用不安から起きた事案である点、短時間での大量引出しが発生している点である。また、「FTX」は報道が契機となった一方、「Terra USD」はソーシャルネットワーク上で情報が拡散され、情報伝播速度が格段に上がっているという点も近年のトレンドの一つであり、同様のことは、2023 年 2 月のシリコンバレー銀行の取り付け騒ぎの発端ともなっている。利用者の資産保護に関しては、国内の事業者に対しては資金決済法にて義務付けられているが、国際的な取引が広がる中、利用者にも潜在するリスクを適切に理解することが求められている。

[1] NHK NEWS WEB、ステーブルコイン「テラ」暴落 なぜ？【経済コラム】、2022 年 5 月 29 日（https://www3.nhk.or.jp/news/html/20220527/k10013645941000.html）

[2] NHK、「交換業大手「FTX」経営破綻 刑事事件に発展 現状は？今後は？（12 月 14 日更新）」、2022 年 11 月 24 日、（https://www3.nhk.or.jp/news/special/sakusakukeizai/20221124/543/）

[3] SEC、” SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX”、2022.12.13、（https://www.sec.gov/news/press-release/2022-219）

[4] Bloomberg、「アラメダ元CEO、FTXワン創業者が有罪認める－SECも提訴」、2022 年 12 月 22 日、（https://www.bloomberg.co.jp/news/articles/2022-12-22/RN9STDDWRGG001）

[5] 金融庁、「FTX Japan 株式会社に対する行政処分について」、令和 4 年 11 月 10 日、（https://www.fsa.go.jp/news/r4/sonota/20221110/20221110.html）

[6] 金融庁、「情報通信技術の進展に伴う金融取引の多様化に対応するための資金決済に関する法律等の一部を改正する法律 説明資料」、平成 31 年 3 月 15 日提出、令和元年 5 月 31 日成立、（https://www.fsa.go.jp/common/diet/198/02/setsumei.pdf）

4　安全な資産管理に必要となる要素（HSM、TEE 等）

4.1　概要

現在、世界的に CBDC に関する議論が活発化しており、世界各国では様々な研究開発や実証実験が進んでいる。そのような中、通信相手やデータの正当性をどのように確認（本人確認等）するか、取引情報やプライバシー等に関する機微データを誰がどのように取り扱うか、どのような仕組みで不正な攻撃から防御するかといった、デジタル社会において安心して利用可能な仕組みの構築が重要な課題とされている。また、これらの課題は CBDC のみならず、多くの先端技術を用いた情報システムや情報サービスにおける課題とされており、社会のデジタル化が進められる中で「トラスト（信頼）」に関する議論が活発化している。

「トラスト」については、これまで社会学、哲学、心理学等の分野において研究がなされており、特に社会学の分野では、人間関係における信頼のメカニズムについて論じられることが多い。代表的な捉え方として、社会的な複雑性の縮減メカニズムに基づく捉え方が提唱されている。これは、相手の身分や資格等の社会的な側面を踏まえて、相手が自分の意図に沿って必要な行動をするだろうということを、暗黙的に認知することができる場合、その相手を信頼できる相手として判断するという捉え方である[1]。また、相手が信頼できるか否かを判断する材料として、取引相手に関する情報や取引に係る社会システムの構造に関する知識が必要であると考えられる。例えば、通貨を介して対面で商取引を行う場合、通常は、取引相手との信頼が成立した上で取引を行うが、この場合、相手の身元、支払能力、担保となる資産等だけでなく、社会システムとしての流通・決済システムへの信頼や、決済通貨の真正性、通用力等が判断材料になるとも考えられる。

一方、情報通信分野における「トラスト」については、機械やコンピュータシステム、ネットワーク越しの非対面の通信相手に関するものが多く、それぞれのデバイスやシステムの仕組みが安全か、期待どおりに動作するか、信頼できる AI とはどういうものか、通信相手が本人と同一人物かどうか、運用元が信頼性をどのように確認するかなどが重要なテーマとされている。例えば、デジタル庁の包括的データ戦略においては、課題の一つとして、「トラスト」の確保について検討がなされ、包括的な「トラスト」基盤の構築に向けた制度、ルール等に関する今後の方向性についての報告書がまとめられている[2]。この中では、e シールにおける認証局側の設備について、HSM（Hardware Security Module）や、それに関する国際的に認知された規格への対応の必要

性について述べられている。

このように、情報通信分野においては、信頼できる社会基盤の構築やデータの安全な利用のため、「トラスト」をどのように確保するかが重要な課題とされており、そのための必要な要素として、今日において当然のように使用されている現代暗号理論をベースに、暗号技術の鍵管理や演算処理の安全な実装及びその実装を確認するための仕組みが挙げられている。

CBDC の検討においても、取引に利用されるデータの安全な管理などの信頼されるシステム基盤を構築するためには、「トラスト」の確保に必要となる暗号技術の安全な実装が、重要な要素の一つと考えられる。

そこで、本章では、安全なデータ処理の観点から、これら暗号技術の安全な実装に関する動向について述べる。

4.2 デジタルトラスト

現在、インターネットを介した商取引や SNS（Social Network Service）により、バーチャル空間における人間関係が拡大しており、AI 技術を用いた高度なシステムの社会への導入も進展している。一方、バーチャル空間において人を「騙す」技術も高度化しており、AI を悪用した DeepFake 等は深刻な脅威とみなされている。このため、情報通信分野においても、様々なトピックに係る「トラスト」の研究開発が進められている[3]。その中でも特に活発に取り組まれている領域は「デジタルトラスト」の領域であり、ハードウェア的な改ざん防止対策や暗号技術に基づく電子署名、個人やデバイスの認証技術などが含まれ、主に対象の真正性証明について重点が置かれている。

また、社会実装の視点に立てば、「デジタルトラスト」の確保は、これまでも情報通信システムの必須の要素となっており、1994 年には米国国立標準技術研究所（NIST）が、政府調達における暗号モジュールのセキュリティ要件として、FIPS（Federal Information Processing Standardization）140 を規定している。

本節では、「デジタルトラスト」の社会実装に着目し、ハードウェアに関する国際的に認知された標準等の動向について述べる。

なお、説明に際し、用語としてトラストアンカー（Trust Anchor）及びルートオブトラスト（Root of Trust）を用いるが、トラストアンカーとは、暗号分野における暗号鍵や秘密鍵といった機密情報を指し、ルートオブトラストとは、トラストアンカーが外部からの攻撃や不正アクセスに対して安全に保護された、「信頼の基点」となる状態を指す。

4.2.1 HSM (Hardware Security Module)

HSM（Hardware Security Module）は、暗号処理のハードウェアを検討する際に広く利用される用語の一つである。HSM について明確に定義された標準はないが、IoT 推進コンソーシアム、総務省及び経済産業省の報告書では、「鍵管理や暗号化などのセキュリティ機能を提供する専用のハードウェア」[4]と説明されており、一般的には暗号技術を適切に運用するために必要となる暗号鍵の安全管理などを提供する専用ハードウェアデバイスと捉えることができる。

HSM の主な機能としては、ハードウェアによる乱数の生成、デバイス内での暗号鍵/認証鍵の生成・保管、デバイス内での暗号鍵/認証鍵を用いた演算/署名検証、ハードウェア/ソフトウェアの改ざんの検知・保護などが挙げられる。また、HSM では、耐タンパー性のあるハードウェアで暗号鍵等のトラストアンカーを保護しているため、単体でルートオブトラストとなりうるとともに、専用ハードウェアによる高速処理が期待される。

HSM と最も関連のある規格として、NIST が規定する FIPS 140 がある。FIPS 140 は、米国政府機関の ICT 関連製品の調達において、暗号モジュールに求められるセキュリティ要件の仕様に関する規格であり、1994 年に FIPS 140-1[5]が発行され、2001 年に FIPS 140-2[6]、2019 年に FIPS 140-3[7]が発行されている。また、FIPS 140 は ISO/IEC 19790 の主要な参照資料とされ、FIPS 140-3 では ISO/IEC 19790 を参照する形で更新がなされている。この FIPS 140 は、ヨーロッパ連合（EU）の e シール用の認証局設備においても、HSM の基準の一つ（FIPS 140-2 Level3 以上又は ISO/IEC15408 EAL4 以上）とされるなど、HSM を評価する基準の一つとなっている。FIPS 140-2 で定める要件[8]の概要は、以下のとおりであり、レベルが高くなるほど多くの要件が求められる。

- レベル 1：テスト済みの暗号化アルゴリズムの使用や出荷品質の機器の使用等により、甚だしくセキュリティの欠如がないこと
- レベル 2：レベル 1 の要件に加えて、シールやピッキング防止ロック等により、外部からの改ざんの痕跡を物理的に記録できること、評価済みのオペレーティングシステム環境によって実行されること、オペレータの認証を役割ベースで行うこと等
- レベル 3：レベル 2 の要件に加えて、物理的な改ざん耐性を有し、外部の攻撃から内部の秘密情報を保護可能であること、セキュリティパラメータの入出力が物理的又は論理的に分離されていること、オペレータの認証を ID ベースで行うこと等
- レベル 4：レベル 3 の要件より強固なセキュリティ要件をみたすこと

HSM においては、一般的にレベル 3 以上の要件を満たすことが求められる。

なお、FIPS 140-2 は 2021 年 9 月に新たな認証を終了し、現在は、FIPS 140-3 へ移行している[9]。

一方、情報セキュリティに関する別の規格として ISO/IEC 15408（Common Criteria）[10]がある。ISO/IEC 15408 は、情報技術に関連する製品やシステムが適切に設計・実装されていることを評価するための国際標準であり、暗号モジュールだけではなく、ハードウェアからソフトウェアまで広く適用される標準である。また、FIPS 140 のように満たさなければならないセキュリティ要件を規定するものではなく、ISO/IEC 15408 は、セキュリティ評価の枠組み（フレームワーク）を規定するものであり、別途、記載されるセキュリティ要件（プロテクションプロファイル）に対して、評価機関で評価を実施することとなる。そのため、HSM においても、システムごとにセキュリティ要件の設定や評価機関での評価が必要となる。

以上のように、HSM は機密情報の暗号処理を専用ハードウェアで実装するものであり、現在、クラウドサーバ等で使用されるラックマウントシャーシや、サーバ、PC 等で利用される PCI-E ボードなど、様々なデバイスで広く使用されている。また、デジタル庁の報告書[11]で e シールにおける認証局側の基準として FIPS 140-2 レベル 3 相当又は ISO/IEC 15408 EAL4+相当での検討が進められるなど、HSM は高い安全性の求められる暗号装置の基本となるものである。

4.2.2 TPM (Trusted Platform Module)

TPM（Trusted Platform Module）は、コンピュータの信頼性や安全性向上に向けた業界団体 Trusted Computing Group（TCG）によって公開されている仕様を満たす半導体のことであり、IoT 推進コンソーシアムほかの報告書では、「コンピュータのマザーボードなどに装着される、セキュリティ関連の処理機能を実装した LSI チップ」[12]とされている。主なものとして、独立したチップ等のハードウェアとして実装されるディスクリート TPM があり、プロセッサ（CPU、SoC）上の TEE（Trusted Execution Environment）等の信頼された実行環境において、ファームウェア上のコンポーネントとして実装されるファームウェア TPM もある。

ディスクリート TPM の基本構造は、図 4.1 に示すとおりであり、主な機能として HSM と同様に乱数生成、チップ内部での暗号鍵の生成・保管、チップ内部での暗号鍵を用いた演算・署名、改ざん検知などがある[13]。TPM の特徴として、半導体で大量製造可能であることから、モジュール単位で増設

する HSM より安価に実装可能であるものの、HSM と同様にベンダ専用プログラムが必須であり、単体での処理能力は HSM に劣るため、小規模かつ限定的な処理で使用される。

TPM は、主として基盤上のチップに実装されるハードウェアであり、単体でルートオブトラストとなるものだが、基盤上に実装される性質上、搭載されるシステムと密接に連携することとなる。そのため、TPM を搭載することによってシステムのセキュリティを担保させるためには、搭載するシステムの要件定義からアプリケーションの実装までを考慮して、適切に設計する必要がある。

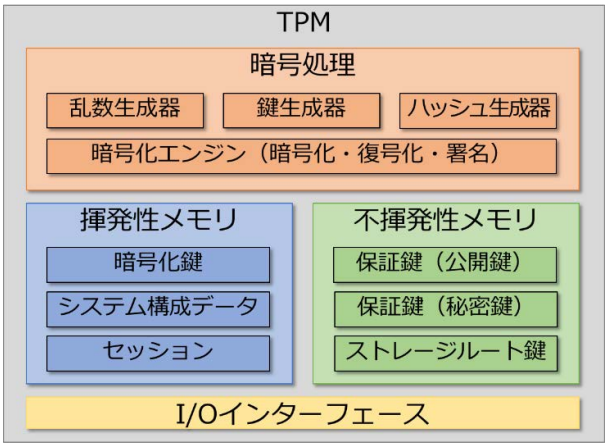


図4.1　TPMの基本構造[14]

（“Trusted Platform Module Library Part 1: Architecture, Figure 2 Architectural Overview”を参考に作成）

TPM に関する規格については、RSA 暗号と SHA-1（ハッシュ関数）を搭載した TPM1.2[15]が 2009 年に ISO/IEC 11889 として標準化され、ECC 暗号と SHA-256 に対応した TPM2.0[16]が 2015 年に ISO/IEC 11889:2015 として標準化されている。

PC 用途としては、マイクロソフトが Windows Vista[17]から TPM1.2 を[18]、Windows 8 [17]から TPM2.0 をサポートしており[19]、Windows 11 [17]からはシステム要件において TPM2.0 が必須[20]となるなど、事実上の業界標準として使用されている。その他、TPM2.0 では PC 用途に加え、スマートフォンや自動車など、組込用途向けの要件や仕様についても策定されている[21,22]。

このように、HSM がハードウェア全般のシステムから発展したのとは異なり、TPM は、集積化が進む IC チップへの実装から発展しており、システム上のデバイスである一般的な PC への搭載を中心に普及してきた技術と言える。

4.2.3 TEE (Trusted Execution Environment)

TEE（Trusted Execution Environment）は、機密データの処理やクリティカルな処理を実装するためにデバイス内に構築される、汎用 OS と隔離されたプログラム実行環境のことである。近年、コンピュータやスマートフォン等の情報端末では、OS がサポートするデバイスやアプリケーションに提供する機能が多様化（複雑化）しているのに対し、情報端末のインターネット接続も一般化しており、インターネットからの攻撃に晒されている。そのような中、鍵管理や暗号化などのクリティカルな処理も OS の一部又は OS 上のアプリケーションで実行されていることも多く、OS の脆弱性がそのまま暗号処理の脆弱性につながる脅威も高まってきている。このような OS の脆弱性に起因する脅威を低減するため、より安全な環境で処理を実行できる TEE 機能が、デバイスのプロセッサ（CPU、SoC）に実装されるようになってきている[23]。

TEE 機能については、IoT 推進コンソーシアムほかの報告書では、「IC カード管理技術の標準化組織の一つである Global Platform が定義する、認証された実行環境とそれに関わる API（Application Programing Interface）の仕様」[24]と説明されており、Global Platform では、以下の七つのアーキテクチャ要件が定義されている[25]。

① Regular OSとは独立に実行すること
② 他のTA(Trusted Application)とは独立して実行すること
③ 信頼された者のみがTEEとTAを修正できること
④ TEEプラットフォームとTAの真正性と完全性を強制できること
⑤ 信頼できるストレージを用意すること
⑥ ペリフェラル（周辺機器）には安全にアクセスすること
⑦ 最新の暗号技術を使うこと

TEE 機能のアーキテクチャのイメージを図 4.2 に示す。TEE 機能は図 4.2 に示すように、デバイスのプロセッサ（CPU、SoC 等）の内部に、Windows、Android™ などの汎用 OS 上で実行される処理とは別に、機密性の高いデータを処理するための Trusted OS を設け、クリティカルな処理は Trusted OS 上で隔離実行する仕組みとなっている[26]。つまり、TEE 機能とは、通常の OS やアプリケーションが動作する環境（REE：Regular Execution Environment）とは独立して、クリティカルな処理を安全に実行可能な隔離環境を備えたプロセッサと捉えることができる。

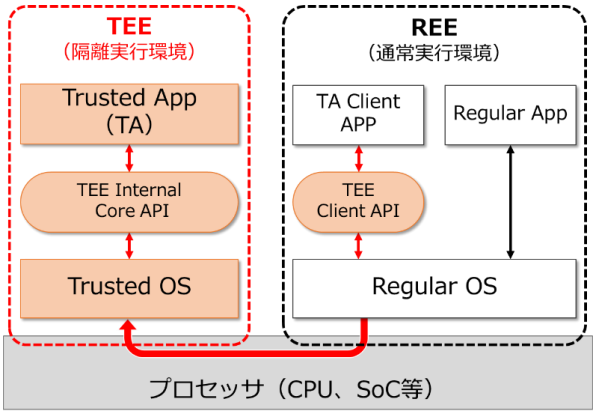


図4.2　TEEのアーキテクチャ（イメージ）[27]

（“GPD TEE System Architecture Public Release v1.3”を参考に作成）

TEE 機能の特徴として、HSM や TPM のようなベンダ固有の特殊なコードではなく、第三者が作成した任意のコードが実行可能であり、TEE 機能により提供される隔離実行環境が一般ユーザーやサービスプロバイダにも開放されていることが挙げられる[28]。ただし、これまで様々な TEE 機能が提唱されているものの、その多くは実装方法やアーキテクチャが異なるため、共通するのはハードウェアのサポートによる隔離実行環境の提供のみとなっている。

これまでに提供されている主な TEE 機能を表 4.2 に示す。主要ベンダが提供する商用の TEE 機能としては、ARM 社の TrustZone®や Intel 社の SGX などが挙げられる。他方、オープンアーキテクチャである RISC-V はマサチューセッツ工科大学の Sanctum や MI6、カリフォルニア大学バークレー校の Keystone 等の研究開発のベースとされており、研究開発用の TEE 機能として、様々な研究機関でカスタマイズされて利用されている[29]。

表4.2　TEE機能の比較[30]

（“Trusted Execution Environmentによるシステムの堅牢化，表-1 TEE比較表，p.578”を参考に作成）

	ARM TrustZone®	Intel SGX	RISC-V
実装の特徴	ソフトウェア機能が主	ハードウェア機能が主	機能をソフトウェア/ハードウェアで変更可能
隔離実行環境	起動時に一つ作成	起動時に複数作成	動的に複数作成可能
メモリ	・起動時に固定 ・領域内暗号化なし	・起動時に固定 ・領域内を暗号化	・領域の動的設定可能 ・領域内暗号化なし
ルートオブトラスト	なし	あり（製造時に Intel が付与する CPU 固有 ID）	現状なし （ソフトウェアのみ）
実装例	スマートフォンにおける鍵管理等	クラウドサーバ等におけるデータの隠蔽等	研究開発用途が主

TEE 機能については、共通の規格、仕様等が存在しないため、表 4.2 のとおり、複数のハードウェア実装方法が存在し、実装方法によって機能も異なるだけでなく、同一の TEE 機能に実装されるシステムソフトも複数存在する。また、TEE 上で実行するアプリケーションは TEE のシステムソフトに合わせて作る必要がある。このため、TEE プラットフォームの種類や OS のバージョンによってアプリケーションの実装方法が異なることから、全てに対応することが困難であり、TEE 機能の利活用における課題となっている[31]。

さらに、TEE は、あくまでも隔離実行環境のみであるため、HSM や TPM と異なり、TEE 機能単体ではルートオブトラストとはならない。このため、TEE プラットフォームにおいてルートオブトラストを確保するためには、TEE プラットフォームが信頼できるかを検証するための仕組みが別途必要である[32]。このための仕組みとしては、TEE とは別の耐タンパー性のあるハードウェアに保存された検証鍵やデバイスの構成証明を参照する方法や、TEE プラットフォームの信頼性を検証可能な第三者の情報を参照して検証する方法がある。

具体的には、TEE と連携可能なセキュアエレメント（Secure Element）やセキュアエンクレーブ（Secure Enclave）など、機密性の高いデータを保護するためのハードウェアの実装や[33]、対象となる TEE プラットフォームの真正性や完全性を、CPU ベンダ等の第三者がネットワーク上で検証する、リモートアテステーション（Remote Attestation）と呼ばれる検証方法によって実現される[34]（図 4.3 参照）。

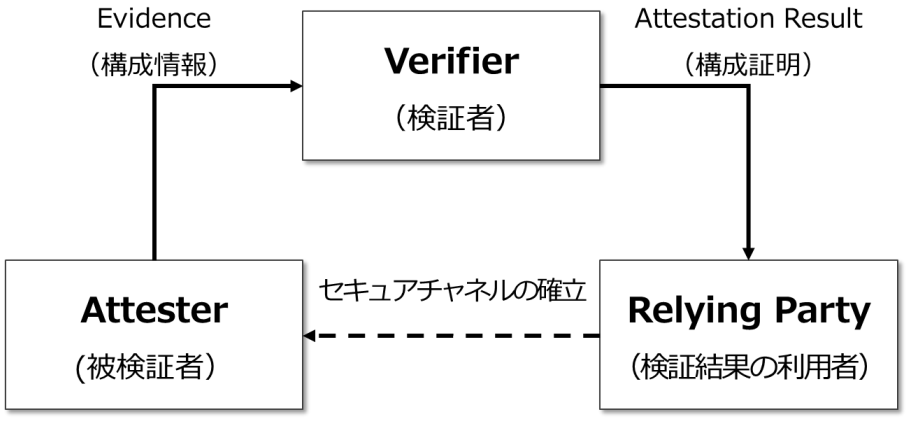


図4.3　リモートアテステーションのフロー概念[35]

（“RFC 9334_Remote ATtestation procedureS (RATS) Architecture, Figure 1: Conceptual Data Flow”を参考に作成）

リモートアテステーションについては、これまで、TCG、Global Platform 等の様々な団体による規格化や標準化が行われてきただけでなく、Intel 社、Google 社等の特定の企業による実装が行われてきたため、異なる規格や技術に個別に対応する必要がある。この課題への対応を図るため、現在、インターネット技術標準化委員会（IETF）において、データフォーマットや伝送プロトコル等の標準化に向けた検討が進められている[36]。

4.2.4 HSM/TPM/TEEの違い

機密情報を暗号化して処理するための装置については、そのセキュリティ強度はハードウェアや論理領域の実装方法によって異なり、耐タンパー性のあるハードウェアによる実装領域が多いほどセキュリティ強度は高いものとなる[37]（図 4.4 参照）。HSM や TPM がハードウェアモジュールや半導体チップの開発史とともに登場してきたのに対し、TEE 機能は、CPU 内の処理として開発が進められてきており、ソフトウェア実装も多数の領域で使用されることが想定されている。

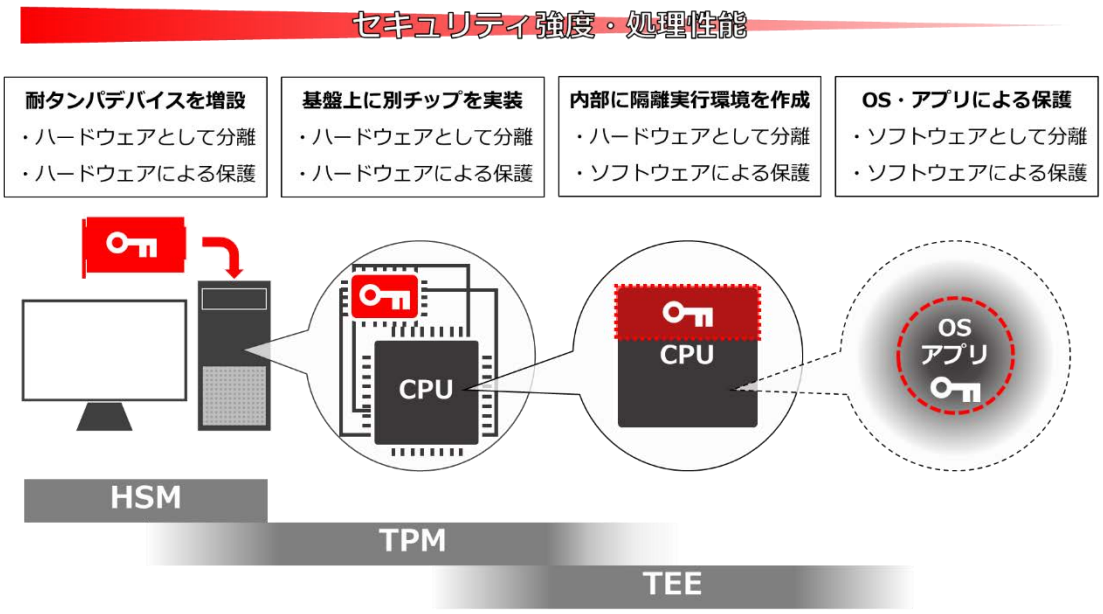


図4.4　各実装方式とセキュリティ強度等のイメージ

（「グローバル環境において求められるIoTセキュリティに関する考察　-日本製造業に向けて-」を参考に作成）

一般的には HSM や TPM といったハードウェアによる保護の方がセキュリティ強度は上がるものの、ハードウェアの実装コストが必要とされる[38]。他方、TEE 機能を利用する場合、トラスト環境の構築に必要なセキュリテ

ィを十分に確保するためには、別途ハードウェアの実装やリモートアテステーションが必要となる。また、リモートアテステーションを利用する場合、アプリケーションを提供するサーバ系と、アプリケーションを利用するクライアント系の双方に対応する必要がある[39]。

したがって、機密情報を暗号化して処理するための装置を利用する場合、要求されるセキュリティ要件、実行するアプリケーションの内容、システムの運用方法等だけでなく、実装や運用における条件、制約等を考慮し、必要な機能を十分に検討した上で選定又は設計する必要がある。

4.3 まとめ

ICT の根幹をなす半導体の高集積化や高速化、有線/無線通信技術の広帯域化の発展とともに、サーバ、PC、スマートフォンなど様々なデバイスの高機能化も進み、更には、データベース技術や各種データ処理、人工知能（AI）といった様々な情報処理技術が発展することで、社会のいたるところに情報機器が導入され、ネットワークによる相互接続が当然の社会になりつつある。そのような中、ネットワークによる相互接続の複雑化に伴い、システム運用側では通信先の個人や端末が信頼できるか、ユーザー側では運用側のシステムや通信環境が信頼できるかなど、「トラスト」にかかる要望が高まってきている。また、今後の社会のデジタル化による更なる複雑化を想定し、従来の境界型セキュリティを拡張した考え方である、ゼロトラストアーキテクチャなどの議論も進展している[40]。

本稿で述べた、近年のハードウェアデバイス等の社会実装に関する各種動向は、CBDC などの新たな社会インフラの実装を考える上で重要な要素の一つとなるとともに、公開鍵暗号基盤やデジタル社会基盤に関連する各種機関においても必須の検討事項になるものと考えられる。

[1] 国立研究開発法人科学技術振興機構研究開発戦略センター,「俯瞰セミナー＆ワークショップ報告書「トラスト研究の潮流 ～人文・社会科学から人工知能、医療まで～」」, 2022 年 2 月, pp.65-72.
[2] デジタル庁,「トラストを確保した DX 推進サブワーキンググループ報告書」, 2022 年 7 月 29 日, p.21, (https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/658916e5-76ce-4d02-9377-1273577ffc88/1d463bfc/20220729_meeting_trust_dx_report_01.pdf)
[3] 国立研究開発法人科学技術振興機構研究開発戦略センター,「戦略プロポーザル デジタル社会における新たなトラスト形成」, 2022 年 9 月.
[4] IoT 推進コンソーシアム IoT セキュリティ WG,「IoT セキュリティガイドライン ver 1.0」, 2016 年 7 月, p.59, (https://www.soumu.go.jp/main_content/000428393.pdf)
[5] National Institute of Standards and Technology, "FIPS PUB 140-1 SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES", 1994 年 1 月 11 日, (https://csrc.nist.gov/csrc/media/publications/fips/140/1/archive/1994-01-11/documents/fips1401.pdf)
[6] National Institute of Standards and Technology, "FIPS 140-2, Security Requirements for Cryptographic Modules _ CSRC", 2002 年 12 月 3 日,(https://csrc.nist.gov/publications/detail/fips/140/2/final)
[7] National Institute of Standards and Technology, "FIPS 140-3, Security Requirements for Cryptographic Modules _ CSRC", 2019 年 3 月 22 日,(https://csrc.nist.gov/publications/detail/fips/140/3/final)
[8] Corel® Discovery Center JAPAN, "WinZip - FIPS 140-2 暗号化とは。なぜ重要なのか。", (https://jp.learn.corel.com/security/winzip-fips-140-2-encryption-explained/)
[9] National Institute of Standards and Technology, "FIPS 140-3 Transition Effort _ CSRC", 2021 年 6 月 2 日, (https://csrc.nist.gov/projects/fips-140-3-transition-effort)
[10] 独立行政法人情報処理推進機構 HP,「情報処理推進機構:情報セキュリティ:IT セキュリティ評価及び認証制度(JISEC):CC 概説」, 2008 年 10 月 10 日,(https://www.ipa.go.jp/security/jisec/about_cc.html)
[11] デジタル庁,「トラストを確保した DX 推進サブワーキンググループ報告書」, 2022 年 7 月 29 日, p.21, (https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/658916e5-76ce-4d02-9377-1273577ffc88/1d463bfc/20220729_meeting_trust_dx_report_01.pdf)
[12] IoT 推進コンソーシアム IoT セキュリティ WG,「IoT セキュリティガイドライン ver 1.0」, 2016 年 7 月, p.60, (https://www.soumu.go.jp/main_content/000428393.pdf)
[13] 中村智久, 東川淳紀, ㈱NTT データ,「解説 PC 搭載セキュリティチップ(TPM)の概要と最新動向」, 情報処理, 47 巻, 第 5 号, 2006 年 5 月, pp.473-478.
[14] Trusted Computing Group, "Trusted Platform Module Library Part 1: Architecture", 2019 年 11 月 8 日, p.33, (https://trustedcomputinggroup.org/resource/tpm-library-specification)
[15] Trusted Computing Group HP, "TPM 1.2 Main Specification _ Trusted Computing Group", (https://trustedcomputinggroup.org/resource/tpm-main-specification)
[16] Trusted Computing Group HP, "TPM 2.0 Library _ Trusted Computing Group", (https://trustedcomputinggroup.org/resource/tpm-library-specification)
[17] Windows、Windows Vista は米国 Microsoft Corporation の米国およびその他の国における登録商標です。また、Windows の正式名称は、Microsoft Windows Operating System です。
[18] 日経クロステック(xTECH) HP,「ボリューム・レベルの暗号化機能「Bitlocker」の仕組みを知る」, 2007 年 6 月 12 日,(https://xtech.nikkei.com/it/article/COLUMN/20070611/274342/)
[19] 株式会社 FFRI セキュリティ, マンスリーリサーチ,「TPM 2.0 の概要と IoT デバイスでの利用例」, 2015 年 10 月, p.9, (https://www.ffri.jp/assets/files/monthly_research/MR201510_Overview_and_usage_examples_of_TPM_2.0_JPN.pdf)
[20] Microsoft, "Minimum Hardware Requirements for Windows 11", 2021 年 6 月, (https://support.microsoft.com/en-us/windows/windows-11-system-requirements-86c11283-ea52-4782-9efd-7674389a7ba3)
[21] Trusted Computing Group HP, "TPM 2.0 Mobile Reference Architecture Specification _ Trusted Computing Group",(https://trustedcomputinggroup.org/resource/tpm-2-0-mobile-reference-architecture-specification/)
[22] Trusted Computing Group HP, "TCG TPM 2.0 Automotive Thin Profile For TPM Family 2.0; Level 0 _ Trusted Computing Group", (https://trustedcomputinggroup.org/resource/tcg-tpm-2-0-library-profile-for-automotive-thin/)
[23] 須崎有康,「Trusted Execution Environment の実装とそれを支える技術」, IEICE Fundamentals Review Vol.14, No.2, 2020 年 10 月, p.108.
[24] IoT 推進コンソーシアム IoT セキュリティ WG,「IoT セキュリティガイドライン ver 1.0」, 2016 年 7 月, p.60,

(https://www.soumu.go.jp/main_content/000428393.pdf)

[25] GlobalPlatform, “Introduction to Trusted Execution Environment”, 2018 年 5 月, p.2, (https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Trusted-Execution-Environment-15May2018.pdf)

[26] GlobalPlatform, “GPD TEE System Architecture Public Release v1.3”, 2022 年 5 月, (https://higherlogicdownload.s3.amazonaws.com/GLOBALPLATFORM/transferred-from-WS5/GPD_TEE_SystemArchitecture_v1.3_PublicRelease.pdf)

[27] GlobalPlatform, “GPD TEE System Architecture Public Release v1.3”, 2022 年 5 月, pp.21-46, (https://higherlogicdownload.s3.amazonaws.com/GLOBALPLATFORM/transferred-from-WS5/GPD_TEE_SystemArchitecture_v1.3_PublicRelease.pdf)

[28] 須崎有康,「Trusted Execution Environment の実装とそれを支える技術」, IEICE Fundamentals Review Vol.14, No.2, 2020 年 2 月, pp.107-108.

[29] 須崎有康,「TEE(Trusted Execution Environment)とそれに関する研究開発動向」, デジタルサービス・プラットフォーム技術特別研究専門委員会, 2021 年 9 月 27 日.

[30] 須崎有康, 佐々木貴之,「Trusted Execution Environment によるシステムの堅牢化」, 情報処理, 61 巻, 第 6 号, 2020 年 6 月, p.578.

[31] 須崎有康,「TEE (Trusted Execution Environment)は第二の仮想化技術になるか ?」, 第 32 回コンピュータシステム・シンポジウム(ComSys2020), 2020 年 12 月 1 日.

[32] 須崎有康,「Trusted Execution Environment の実装とそれを支える技術」, IEICE Fundamentals Review Vol.14, No.2, 2020 年 2 月, p.112.

[33] 須崎有康,「Trusted Execution Environment の実装とそれを支える技術」, IEICE Fundamentals Review Vol.14, No.2, 2020 年 2 月, p.112.

[34] 須崎有康,「遠隔デバイスとの信頼を築くための技術とその標準」, 第 11 回サイバーセキュリティ国際シンポジウム, 2021 年 11 月 28 日, pp.9-16.

[35] Remote ATtestation procedureS HP, “RFC 9334_Remote ATtestation procedureS (RATS) Architecture, Figure 1: Conceptual Data Flow”, 2021 年 1 月,(https://www.rfc-editor.org/rfc/rfc9334)

[36] Remote ATtestation procedureS HP, IETF, “RFC 9334_Remote ATtestation procedureS (RATS) Architecture”, 2021 年 1 月,(https://www.rfc-editor.org/rfc/rfc9334)

[37]一般社団法人セキュア IoT プラットフォーム協議会,辻井重男,「グローバル環境において求められる IoT セキュリティに関する考察 -日本製造業に向けて-」, 2020 年 3 月, (https://www.secureiotplatform.org/static/images/report_20200325.pdf)

[38] 飯田正樹, 松田俊寛, 永見健一, 遠藤貴裕, 古瀬正浩, ㈱インテック,「IoT をセキュアにする TEE 応用技術とその実用化への取り組み」, INTEC TECHNICAL JOURNAL, 第 17 号, 2016 年 9 月, p.55.

[39] 須崎有康,「Trusted Execution Environment の実装とそれを支える技術」, IEICE Fundamentals Review Vol.14, No.2, 2020 年 2 月,pp.112～114,

[40] デジタル庁,「ゼロトラストアーキテクチャ適用方針」, 2022 年 6 月 30 日, (https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5efa5c3b/20220630_resources_standard_guidelines_guidelines_04.pdf)

5　おわりに

電子決済、暗号資産取引などにおいて脆弱性を標的とした不正な引き出しや、個人情報詐取などの攻撃が年々増えており、その手口も変化している。2022 年 3 月、6 月に発生した暗号資産の盗難に関しては、北朝鮮のハッカー集団が関与していると米国連邦捜査局が発表している[1]ことなどに鑑みると、国家安全保障といった観点からも安全な CBDC の設計が必要となると考えられる。

CBDC の実証実験や制度設計に係る議論は、日本銀行を含む各国中央銀行で確実に進んでおり、日本銀行は、本レポート執筆中の 2023 年 2 月 17 日に、先述した実証実験フェーズ 2 の結果などを踏まえ、パイロット実験を 4 月から開始することを発表した[2]。あわせて、CBDC の制度設計を適切に進めるための「CBDC フォーラム」の設置を公表[2]しており、日本国内における制度設計に係る取組についても、財務省における有識者会議の議論の結果を含め、多くの関係者との議論を踏まえながら検討するフェーズへと進むこととなる。このように、中央銀行が管理するコアな領域と仲介機関とのシステム連携、そして、リテール決済、個人間取引を含むエコシステムの実現に向けた取組が段階的、計画的に拡張され、様々な関係者と協調しながら設計に関する考え方の整理が進められていくことが想定されるが、最終的な CBDC 導入の判断は、国民によるもの[3]とされている。

国民の判断においては、CBDC に対して資産、情報、取引など、あらゆる面で「信頼」を得ることが重要なファクターとなると考えられることから、本レポートにおいては、既に電子端末機器などに実装され、標準化の取組も進められていると考えられる取引における「信頼」を確保するための要素の一端を整理した。それらは、eID、スマートコントラクト、位置情報、エコシステムにおけるデータや計算モデルの保護など、CBDC の実装においても関係しうる要素を多分に含んでいる。

もちろん、「信頼」を得るためには、これらに限らず、セキュリティ、強靭性、継続性など多くの要素を必要とするが、それぞれの要素を支える技術等への理解を深めることが、CBDC 導入、導入後の普及に大きな効果をもたらすことと考えられ、本レポートが CBDC を始め、他のデジタル社会の取引に対する「信頼」の向上の一助となることを期待したい。

---

[1] 日本経済新聞、「北朝鮮、7 回目核実験の準備は最終段階　安保理パネル」、2022 年 10 月 8 日、（https://www.nikkei.com/article/DGXZQOCB082MY0Y2A001C2000000/）

[2] 日本銀行、「中央銀行デジタル通貨に関する実証実験について」、2023 年 2 月 17 日、（https://www.boj.or.jp/paym/digital/dig230217b.pdf）

[3] 日本銀行、「【挨拶】「今、決済の未来を考える意味について」（第 4 回中央銀行デジタル通貨に関する連絡協議会）」、2022 年 11 月 24 日、（https://www.boj.or.jp/about/press/koen_2022/ko221124a.htm）