BOJ Reports & Research Papers

決済システムレポート別冊シリーズ

PSSR-Annex

Payment and Settlement Systems Report

中銀デジタル通貨が現金同等の機能を持つための技術的課題

日本銀行
決済機構局
2020年7月

（決済システムレポート別冊の目的）

日本銀行は、決済システムの動向を鳥瞰し評価するとともに、決済システムの安全性・効率性の向上に向けた日本銀行および関係機関の取組みを紹介することを目的として、「決済システムレポート」を定期的に公表している。

「決済システムレポート別冊シリーズ」は、決済システムを巡る特定のテーマについて、掘り下げた調査分析を行うことを目的としており、本号は、中央銀行デジタル通貨（CBDC: Central Bank Digital Currency）について取りあげる。CBDC については、決済システムという視点だけではなく、その発行が金融システムや金融政策に与える影響も含め検討すべきテーマが多岐にわたるが、今回のレポートでは技術にフォーカスする。具体的には、「誰もがいつでも何処でも、安全確実に決済に利用できる」という現金の特性を CBDC が備えるための技術的な課題について整理する。

デジタル通貨を取り巻く技術環境の変化のスピードは速く、このレポートは、CBDC の技術的側面に関する予備調査という位置づけである。今後、外部の専門家との意見交換における叩き台資料として活用していきたい。

日本銀行としては、外部の専門家との議論を通して、技術に関する理解を深めていくとともに、CBDC に関する様々な課題について、関係諸機関と連携しながら検討を進めていきたい。

決済システムレポートの内容について、商用目的で転載・複製を行う場合は、予め日本銀行決済機構局までご相談ください。転載・複製を行う場合は、出所を明記してください。

【本レポートに関する照会先】
日本銀行決済機構局決済システム課　（post.pr@boj.or.jp）

2020 年 7 月
日 本 銀 行
決 済 機 構 局

中銀デジタル通貨が現金同等の機能を持つための技術的課題

■要　旨■

中銀デジタル通貨（CBDC）が現金同等の機能を持つためには、「誰もがいつでも何処でも、安全確実に利用できる決済手段」であることが求められる。したがって、CBDC を検討する際には、CBDC が「ユニバーサル・アクセス（Universal access）」と「強靭性（Resilience）」という 2 つの特性を備えることが技術的に可能かどうか検討することが重要なテーマとなる。

ユニバーサル・アクセスの観点からは、多様なユーザーが利用可能な端末の開発が重要となる。強靭性に関しては、通信・電源途絶への耐性を備えたオフライン決済機能を備えることが望ましい。スマートフォンを用いたケースでは、オフライン決済に必要な機能の多くに既存技術を転用可能とみられる一方、実用化に際しては、機能の安定性や処理性能の確保、コストの面などにおいて課題も残る。ユニバーサル・アクセスの確保に関しては、スマートフォンを保有していないユーザー向けの端末の開発も検討課題となろう。

CBDC について検討する際には、こうした技術的な課題に加え、セキュリティ確保のためのセーフガードや、プライバシーと AML/CFT の両立といったコンプライアンス上の課題への対応も重要である。これらは、オンライン、オフライン決済にかかわらず重要な課題であるが、オフライン環境下ではより対応が難しくなるため、しっかり検討を行う必要がある。セキュリティに関しては、端末の定期交換などを通じて、オフライン環境における CBDC の偽造リスクに対応する必要があろう。また、オフライン環境では、管理者が脅威を常時把握できないため、CBDC の利用金額に一定の上限を設けて被害規模を予め限定することも一つの選択肢であろう。コンプライアンス面では、プライバシーの確保に向けた検討が重要である一方、AML/CFT の観点から不正リスクを抑制するために、決済情報の事後収集やオフライン利用金額の上限設定などを検討する必要がある。

[目　次]

１．はじめに

現金は、経済活動を支える重要な決済手段である。現金は、その利用に当たり特殊な機器や操作が不要で、誰もが利用できるという特性がある。また、通信や電力等のインフラに依存せず、災害等の非常時も含めいつでも利用可能であるという特性も備えている。これら２つの特性が、現金決済の利便性と安定性を支えている。

しかし、近年、社会においてデジタル化が進展するもとで、スウェーデンなど一部の国では現金流通高が減少しており、国民の中銀マネーへのアクセスをどう確保していくかについて関心が高まっている。他方、わが国をはじめ、多くの主要先進国では、現金流通高は今でも増加を続けており、中銀マネーへのアクセスについて問題が生じているわけではない。ただ、長い目で見れば、いずれの国においても、経済のデジタル化を背景に、キャッシュレス化は着実に進展していくであろう。

個々の経済主体の経済活動を支えるうえで、誰もが使える便利で安定性の高い決済手段の存在は不可欠であり、デジタル社会においても、その供給を中央銀行が担うべきということに異論を挟む人は少ないと考えられる。中央銀行デジタル通貨（CBDC: Central Bank Digital Currency）の発行意義も、基本的にはこの点に求められよう[1]。つまり、CBDC が現金同等の機能を持つためには、「誰もがいつでも何処でも、安全確実に利用できる決済手段」であることが求められる。すなわち、CBDC は、「ユニバーサル・アクセス（Universal access）」と「強靭性（Resilience）」を備えることが望ましい。

ユニバーサル･アクセスに関しては、CBDC の利用対象者を制限することがないよう、設計面で工夫が必要と考えられる。例えば、特定の端末に利用を限定するケースでは、当該機器を購入できない人々の利用が阻害されるほか、操作性や携帯性に課題があれば、多くのユーザーから受け入れられない可能性もある。子供から高齢層まで幅広い世代が利用できることが望ましいし、さらには訪日外国人観光客も利用できればなお望ましい。また、決済機能を個人から法人への送金（例：店舗での決済）に限定するのではなく、現金と同様に、個人間も含めた双方向の送金（Peer-to-peer、P2P）でも利用できるよう設計されなければならない。

強靭性の面では、インターネット等のコンピュータ・ネットワークを利用したオンライン型サービスの脆弱性の克服が課題となる[2]。伝統的なクレジットカードやデビット

[1] 雨宮正佳、「日本銀行はデジタル通貨を発行すべきか」、2019 年

[2] Pichler, P., Summer, M., and Weber, B., “Does digitalization require Central Bank Digital Currencies for the general public?,” 2020.

カードに加え、近年利用が進んでいるスマートフォンを用いた新たな決済手段の多くは、通常、送金や支払を行う際に何らかのネットワークにオンライン接続している必要があり、システム・通信障害時に利用が制約される。また、オンライン決済は継続的な電力供給が必要である。例えば、店舗等に設置される読取用の決済端末の多くは、常時オンラインを前提としており、停電時の利用には自家発電機等の設備が必要となる。自然災害の多い日本では、強靭性を備えた決済手段へのニーズは高いと考えられる。

以上を踏まえると、ユニバーサル・アクセスと強靭性という特性を CBDC が備えるには、通信・電源の途絶への耐性も備えたオフライン P2P 決済機能を多くの人々が利用可能な端末に対して実現することが望ましい[3]。

民間の決済事業者は、預金口座やクレジットカードからのチャージや残高・決済履歴の確認が常時可能なオンラインサービスを重視しており、決済機能もオンラインを前提とする先がほとんどである。このため、オフライン P2P 決済に必要なハードウェアやソフトウェアの本格的な実装は進んでいない。また、オフライン P2P 決済を許容すると、決済事業者がリアルタイムで把握できない取引が発生し、常時監視下にはない端末に様々な攻撃が行われやすくなるため、セキュリティリスクが高まることも指摘されている。さらに、決済事業者にとっては、オフライン P2P で実施された決済情報の機動的な収集・活用が難しい面もある。民間の決済事業者はこうした点を考慮し、オフライン P2P 決済の実用化に慎重姿勢をとっていると考えられる。

一方、中央銀行にとっては、ユニバーサル・アクセスと強靭性の確保は重要な課題であり、CBDC を発行する際には、民間の決済事業者とは異なる視点から、その設計を考える必要がある。具体的には、①ユニバーサル・アクセス端末によるオフライン P2P 決済を実現するうえでの技術的な課題の特定に加え、②セキュリティ確保のためのセーフガードなど CBDC の設計・運用上の課題、さらにはプライバシーの確保や AML/CFT への対応といったコンプライアンス上の課題について検討することが重要である。後者②の課題については、オンライン、オフライン決済にかかわらず重要であるが、オフライン環境下ではより対応が難しくなるため、しっかり検討を行う必要がある。

本稿の構成は以下の通りである。次の 2 節では、CBDC の記録に利用する台帳の管理について整理し、オフライン決済との関係を考察する。3 節では、オフライン P2P 決済に必要な機能と技術を整理し、4 節では、ユニバーサル・アクセス端末によるオフライ

[3] CBDC を発行する場合でも、引き続き現金が流通していれば、これが非常時等におけるバックストップとして機能し得る面がある。しかし、CBDC の普及に伴い現金流通が縮小し、現金のバックストップ機能に限界が生じるリスクもある。このため、CBDC にオフライン P2P 決済機能を確保することは重要であると考えられる。

ン決済の実装イメージと課題を整理する。5 節では、CBDC によるオフライン決済の安全面とコンプライアンス上の課題について整理する。最後に、6 節でレポートの内容をまとめる。

2．CBDC の台帳管理

CBDC の発行に当たっては、発行残高や取引履歴を記録するための台帳が用いられる。CBDC の発行体である中央銀行は、自らの財務会計や CBDC の流通管理の観点から、発行残高を適切に把握することが厳しく求められる。

オフライン決済の機能も含め、CBDC が提供し得る様々な機能やサービスについて理解するには、まずは台帳管理のあり方について理解する必要がある。台帳管理については、管理主体、情報の記録方法、情報の管理場所、の 3 つによって違いがあり、それに伴い CBDC の提供し得るサービスや技術特性にも違いが生じてくる。オフライン決済について言えば、後述するように、台帳の管理主体や記録方法の違いではなく、台帳情報の管理場所が重要になってくる。

（台帳の管理主体：中央管理型、分散管理型）

台帳の管理主体に関しては、主に中央管理型と分散管理型の 2 つがある。中央管理型とは、単一の主体が台帳を保有し、取引の検証や履歴の記録を担うケースである。単一の主体が速やかに取引を確定させるシンプルな構造であるため、大量取引への対応や高い処理速度がメリットと考えられている。もっとも、システム障害等により、システムが全面停止し得る構造（単一障害点の存在）は課題と考えられている。このため、障害等への強靭性は、バックアップ設備の設置等を通じて確保することが一般的である。既存の多くの決済サービスは中央管理型で運営されており、信頼性や安定性の面でも豊富な実績があることが利点と考えられている。

一方、分散管理型は、複数の主体が同一の台帳を保有し、それぞれが取引の検証と履歴の記録を担うケースである。分散型台帳技術（DLT）をベースとするのが一般的である。検証者の多様化を通じて台帳所在地等の分散化が図られれば、強靭性の向上が期待できる。また、分散管理型では、スマートコントラクトのように、予め定められたプログラムに基づく自動取引等の実装事例も多く、こうした機能を利用した拡張性も意識されている[4]。しかし、取引の確定に当たり、複数の検証者による合意形成が必要になる

[4] スマートコントラクトの実装は分散管理型で多くみられるが、技術的には中央管理型でも実装可能であ

ため、取引処理に時間がかかる傾向があるほか、脆弱性を抱えた検証者がサイバー攻撃等で狙われやすい点がリスクと認識されている[5]。分散管理型は比較的新しいアプローチであるため、今後の技術革新が期待される一方、現時点では技術の成熟度に欠けるとの見方もある。

このように、中央管理型と分散管理型には、それぞれ長短がある。両者の選択に当たっては、利用環境や目的に加え、今後の技術革新の可能性を踏まえた検討が重要である。例えば、先進国のリテール決済のように、膨大な取引が想定されるケースでは、大量・高速処理に優れ、利用実績も豊富な中央集権型の利用が馴染むとの見方が現時点では多い。一方、取引が一定の水準に止まるケースで、強靭性や機能拡張、将来性を重視する場合は、分散管理型を検討する余地がある。

なお、後述するように、オフライン決済に関しては、中央管理型、分散管理型いずれであっても、台帳が一定の安全性と処理性能を備えていれば、技術的には実現可能である。

（台帳の記録方法：口座型、トークン型）

台帳の記録方法については、①ユーザーごとに金銭的価値の総額（残高）を紐付けるタイプと、②金銭的価値の塊（トークン）ごとにユーザーを紐付けるタイプの 2 つに分類できる。CBDC の発行形態としては、口座型とトークン型の 2 つに分類されることが多いが、口座型は前者①、トークン型は後者②のかたちで台帳に記録するのが一般的と考えられる（BOX 参照）[6]。口座型、トークン型いずれについても、台帳の管理主体の違いによらず――中央管理型でも分散管理型でも――、CBDC の発行が可能である。

口座型 CBDC においては、民間の銀行預金と同様に考えれば、ユーザーの口座番号と本人情報（実名や住所等）をリンクさせたうえで、ユーザー別に金銭的価値（CBDC の保有総額）を紐付けることが想定される。ユーザーが送金を行うには、自らが口座の

る。この点については、Bank of England（BOE）も同様に整理している。
Bank of England, “Central Bank Digital Currency: opportunities, challenges and design,” 2020.

[5] 分散型における処理性能や安全性のリスクについては、前掲の Bank of England (2020)のほか、下記資料を参照。
Auer, R. and Boehme, R., “The technology of retail central bank digital currency,” BIS Quarterly Review, 2020.

[6] 口座型とトークン型という呼称については、様々なかたちで定義されることがあることには留意が必要である。詳しくは、前掲の Auer and Boehme (2020), Bank of England (2020)に加え、以下のレポートを参照。
Bank for International Settlements, “Central Bank Digital Currencies,” 2018.
中央銀行デジタル通貨に関する法律問題研究会,「『中央銀行デジタル通貨に関する法律問題研究会』報告書」、『金融研究』第 39 巻第 2 号、2020 年

保有者であることを証明するために、台帳管理者に対してユーザーが設定したパスワードを提示する――これらの情報は本人と台帳管理者とで共有し、漏洩しないよう管理する――。こうした仕組みは、台帳管理者による AML/CFT における本人確認（Know your customer、KYC）を容易にする一方、プライバシーを確保しにくいという側面がある。また、本人情報の提示が困難な人（例えば、外国人観光客など）は、CBDC を保有できないため、ユニバーサル・アクセスの面でも課題があると指摘されている。

一方、トークン型 CBDC は、トークンごとにユーザーを紐付ける際に、暗号技術に基づきユーザーを匿名化する方法が考えられる。すなわち、各トークンとユーザーの紐付けは、公開鍵により行われ、公開鍵は本人情報と紐付けることなく作成される（BOX 参照）。取引履歴の追跡も困難であることから、プライバシーの確保もしやすい[7]。こうした台帳管理の方法は、ビットコインなどの暗号資産取引で既に利用されている。また、公開鍵暗号を用いた認証は、法域によらず世界中で利用可能であることから、ユニバーサル・アクセスの点で、口座型に比べメリットがある。一方、匿名性の確保や追跡可能性の困難さというトークン型の特徴は、AML/CFT を行ううえで障害となり得る。

このように、口座型とトークン型にはそれぞれ長短あるが、オフライン決済を実現するうえでは、次のサブセクション（台帳情報の管理場所）で説明するように、口座型・トークン型いずれでも対応可能である。

ＢＯＸ　口座型とトークン型の台帳のイメージ

口座型 CBDC の場合、ユーザーは、本人情報と紐付いた公開 ID（口座番号）を 1 つ保有する。この ID にはユーザーが保有する CBDC の合計金額が紐付いている。送金の際には、ユーザーは、ID 保有者であることを証明するための情報（本人が設定したパスワード）を台帳管理者に提示する。

一方、トークン型は、公開鍵暗号方式と呼ばれる暗号技術を利用し、金銭的価値の塊（トークン）とその保有者を紐付けており、ユーザーは複数の ID（公開鍵）を持つことが一般的である。1 つのトークンには 1 つの公開 ID が紐付けられるが、公開 ID は本人情報と対応させる必要がなく、匿名性が確保される。送金の際には、ユーザーは、暗号技術を用いて自身がトークン保有者であることを受け手に証明したうえで――すなわち、公開鍵の対となる（本人しか持っていない）秘密鍵を保有していることを取引相手に示し――、送金する新た

[7] ただし、口座型であっても、口座に紐付ける情報に、例えば実名とは異なる仮名や暗号技術を利用すれば、ユーザーのプライバシー保護を図ることが可能である。逆に、トークン型であっても、保有者名に実名等を利用する場合は、プライバシーは保護されない。したがって、プライバシーの確保は、口座型かトークン型かの違いというより、設計次第という側面がある。

なトークンと、自身が引き続き保有する新たなトークンに分解する。例えば、トークン 10 万円に対してあるユーザーの公開鍵 A が紐付けられた状態で、このうちの 3 万円を公開鍵 B に紐付くユーザーに送付するケースを想定しよう。公開鍵 A の保有者は、残り 7 万円を自らが引き続き保有するために、新たに公開鍵 C を作成し、公開鍵 C の保有者宛に――すなわち、自分宛に――7 万円を送る。このプロセスでは、台帳管理者を含む他者は、公開鍵 A と公開鍵 C の保有者が同じであることを識別できない。公開鍵 A から B、C へのトークンの流れは追跡できても、公開鍵の保有者を特定し、その個人の取引履歴を把握することは困難な仕組みになっている。

トークン型と口座型の CBDC の台帳のイメージは以下の通り。

【口座型】ユーザーごとに保有残高を紐付け

保有者	公開ID（口座番号）	保有残高（円）
日銀 太郎	88-228-504	100,000
米銀 花子	41-923-016	5,000
英銀 一郎	19-911-668	23,000
独銀 次郎	21-291-996	380,000
仏銀 桃子	07-79-7952	15,000
		合計　523,000

【トークン型】トークンごとにユーザを紐付け

トークン（円）	公開ID（公開鍵）	保有者（台帳に記録されない）
40,000	25B48BA…	日銀 太郎
60,000	F13EFE2…	〃
5,000	3EF3520…	米銀 花子
20,000	E921934…	英銀 一郎
3,000	2530CCA…	〃
100,000	1BC41E5…	独銀 次郎
200,000	1C30EC1…	〃
80,000	E72974F…	〃
15,000	1F5AC60…	仏銀 桃子
合計　523,000		

（台帳情報の管理場所：リモート型、ローカル型）

以上で整理したように、台帳は、CBDC の総額管理に加え、取引の記録を通じて（口座型にせよトークン型にせよ）ユーザーと CBDC の金銭的価値を紐付ける機能を担う。台帳への記録は、サーバー上に設置されたデータベースを利用することが一般的である。中央管理型であれば、その管理者のサーバーで、分散管理型であれば、各検証者のサーバーで台帳を管理する。いずれの場合でも、台帳は CBDC のユーザーの手元から離れたところで管理される。ユーザーにとっては、「リモート型」の価値保蔵といえる。

スマートフォンやパソコンなど、ユーザーの保有する端末に台帳の情報が格納されていなくとも――すなわち、金銭的価値が端末に保蔵されていなくとも――、台帳（元帳）とオンライン接続されていれば[8]、取引相手との決済は速やかに実行され、取引結果も

[8] 台帳とユーザーとの接続方法には複数のパターンが存在し得る。例えば、中央銀行等の運営者が台帳を

リアルタイムで台帳に反映される。また、オンライン環境のもとでは、ユーザーは常時台帳にアクセスでき、最新の CBDC 保有残高を確認できる。

このように、台帳はオンライン環境における利用が基本であるが、オフライン決済に際しては、ユーザーは予めオンライン環境のもとで台帳上に自身が保有する CBDC（金銭的価値の情報）を端末に記録する必要がある。こうした操作により、ユーザーは、自分の端末に「ローカル型」の価値保蔵を行う。オフライン決済の実現可能性は、台帳の管理主体（中央管理型、分散管理型）や情報の記録方法（口座型、トークン型）とは独立に――いずれのケースであっても――、ユーザーの端末へのローカル型価値保蔵の実施が前提となる[9]。

オフライン決済のために、ユーザーが端末に価値保蔵した CBDC の情報は、台帳（元帳）から消去せずに、記録・維持しておく必要がある。これは、仮に端末に価値保蔵された CBDC を台帳（元帳）から消去すると、中央銀行は CBDC の発行総額を過小評価することになるためである。オフライン環境下での CBDC の取引履歴は、オフラインが続く限り、台帳（元帳）には反映されないが、その間も CBDC の発行総額は変化しないため、中央銀行は残高を正確に把握できる。

一方、オフライン決済で CBDC を取得したユーザーが、これをオンラインで利用する場合には、オフライン決済の取引情報を台帳に反映させる必要がある。その際、オフラインで取得した CBDC を台帳（元帳）に記録するだけでは、台帳上は、当該 CBDC が取引相手の端末に価値保蔵された際の情報との二重計上が発生するため、取引相手が以前保有していた CBDC 情報については削除する必要がある。

（オフライン決済における二重使用リスクへの対応）

取引当事者双方がオフライン環境のもとで P2P 決済が行われると、事後的なオンライン接続により取引結果が台帳に反映されるまでの間は、二重使用（double spending）のリスクがある。例えば、ユーザーA が台帳（元帳）にある 1 万円分の CBDC を全額、自己のスマートフォンに価値保蔵したとしよう。先に整理した通り、台帳には 1 万円の CBDC が記録維持されたまま、ユーザーA のスマートフォンに 1 万円の CBDC の価値情報が記録される。ユーザーA がオフライン環境でスマートフォン内に保蔵した CBDC を用いて、ユーザーB と取引をしても、双方がオフライン環境を継続する限り、その取

保有し、ユーザーの端末と直接接続するケースのほか、決済事業者等が API（Application programming interface）等を利用して、運営者が保有する台帳とユーザーとの間に入り、台帳には存在しない多様な追加サービスを提供するケースも考えられる。

[9] Norges Bank, “Central bank digital currencies, Second Report of Working Group,” 2019.

引は台帳（元帳）には反映されない。その間、ユーザーA が価値保蔵したスマートフォンとは別の端末を用いて――例えば、パソコンから――台帳（元帳）にアクセスして、１万円の CBDC を使うと、二重利用が発生する。

こうした事態を回避するためには、台帳（元帳）から端末へ CBDC の価値保蔵がされたタイミングで、価値保蔵がなされた分だけ当該 CBDC の台帳上の利用をロックする――利用をできないようにする――ことが一案となる。ロックの結果、端末のみに最新の CBDC の取引情報が記録されるため、端末のオフライン環境が続く限り、最新情報はオンライン上の台帳ではなく、端末内に記録されることになる。これにより、二重使用リスクは回避できる。

ロックされた台帳（元帳）上の CBDC を再びオンライン環境で使う場合は、先に整理した通り、端末上の CBDC の消去を条件にしておく必要がある。例えば、ユーザーA の端末に価値保蔵された CBDC が、オフライン決済によりユーザーB に渡り、ユーザーB が当該 CBDC をオンラインに戻して利用する際には、ユーザーB の端末に価値保蔵された CBDC の消去に加え、ユーザーA が価値保蔵した際にロックされた台帳上の CBDC 情報の削除が必要になる。

このように、台帳機能がオンラインと端末に一時的に分裂する構造のもとでは、金銭的価値のロック機能やオフライン取引の台帳反映手順を定めることによって、二重使用リスクを回避することが重要になる。

３．オフライン P2P 決済に必要な基本機能

オフライン環境下では、台帳管理者が取引を確認できないため、ユーザーの端末を用いて、決済のファイナリティをいかに安全、確実、速やかに確保するか、その仕組みが重要になる。以下では、オフライン P2P 決済の基本的な仕組みを理解するために、ケニアで実施された「DigiTally」と呼ばれるパイロットプログラムを紹介する[10]。DigiTally は、端末としてフィーチャーフォン（いわゆるガラケー）を用いるが、その仕組みは、オフライン決済に必要な機能を最も簡単なかたちで――しかし、的確に――備えたものとなっている[11]。

[10] Baqer, K., Anderson, R., Payne, J., Mutegi, L., and Sevilla, J., “DigiTally: Piloting Offline Payments for Phones,” 2017.

[11] オフライン P2P 決済の事例としては、1995 年に英国でパイロットが行われた Mondex もあげられる。Mondex では、専用 IC カードに金銭的価値を保蔵し、リーダ／ライタと呼ばれる専用の読取・書込端末に 2 枚の IC カードを差し込むことで、端末間の情報伝達を行う。IC カードに加えリーダ/ライタを用意する必要があり、機器の持ち運び負担が発生することもあって、Mondex は普及しなかった。

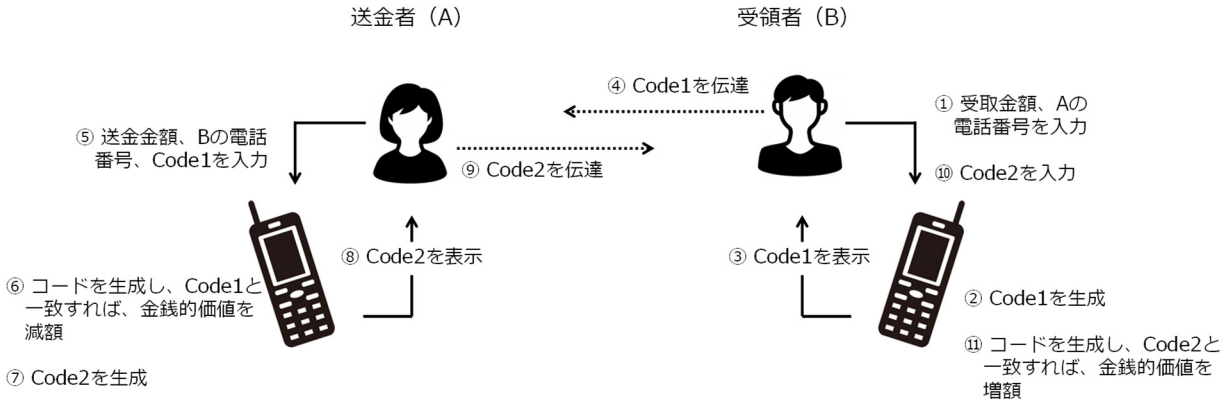
（DigiTally の概要）

送金者 A と受領者 B の間でのオフライン決済を考えよう（図 1）。まず、受領者 B は、自らのフィーチャーフォンに、受取金額と送金者の電話番号を入力する。すると、受領者のフィーチャーフォンでは、受取金額と双方の電話番号に基づき、暗号技術を用いてコード番号（Code 1）が生成される[12]。受領者 B は Code 1 を送金者 A に口頭で伝達する。

続いて送金者 A は、自らのフィーチャーフォンに、送金金額と受領者の電話番号に加え、受領者から伝達された Code 1 を入力する。すると、送金者 A のフィーチャーフォンでは、送金金額と双方の電話番号に基づき、受領者 B と同様の暗号技術を利用して、コード番号を生成し、これが入力した Code 1 と一致すれば、フィーチャーフォン内に保蔵された金銭的価値を送金額の分だけ減額する。同時に、送金者 A のフィーチャーフォンは、送金金額と双方の電話番号、Code 1 に基づき新たなコード番号（Code 2）を生成し、送金者 A は Code 2 を受領者 B に口頭で伝達する。

受領者 B が、自らのフィーチャーフォンに Code 2 を入力すると、受領者のフィーチャーフォンは、受取金額と双方の電話番号、Code 1 に基づくコード番号を生成し、これが入力した Code 2 と一致すれば、フィーチャーフォン内に保蔵した金銭的価値に受領金額を加算する。以上でオフライン送金が完了する。この間、フィーチャーフォンの通信機能は一切利用されていない。

図 1：オフライン P2P 決済のパイロットプログラム DigiTally における送金手順



[12] 受領者のフィーチャーフォンには受領者の電話番号が保管されているため、これを手入力する必要はない。Code 1 の生成には、これらの情報に加え、送金者との過去の取引履歴と乱数も利用される。

上記のオフライン決済はシンプルな仕組みに基づいているが、オフライン決済に必要な機能である、①金銭的価値の安全な保蔵、②ユーザー間の情報伝達、③保有者と端末の認証、④決済指示、⑤電力の確保、の全てを含んでいる。以下では、これら 5 つの機能について詳しくみていく。

① 金銭的価値の安全な保蔵

DigiTally では、SIM カード内の IC チップに内蔵されたセキュア・エレメントに金銭的価値を保蔵し、安全性の確保を図っている（図 2）[13]。フィーチャーフォンのセキュア・エレメントを利用するには、SIM カードに DigiTally のプログラムを追加する必要があるため、決済に必要な機能を格納したシール型の SIM を新たに開発し[14]、これを SIM カードの表面に貼り付けている。こうした操作により、SIM カード内のセキュア・エレメントへの金銭的価値の保蔵が可能になるほか、認証で用いる秘密鍵の付与なども行われる。セキュア・エレメントは、例えばハードウェアが攻撃を受けると、回路等も同時に破壊される構造を持つなど、情報の改竄や盗取を防止する耐タンパー性（Tamper resistance）を備えている[15]。

セキュア・エレメントは、安全性が求められる決済分野で既に広く活用されている[16]。例えば、Suica や PASMO などの電子マネーでは、DigiTally と同様に、金銭的価値の保蔵に利用されている。また、クレジット・デビットカードでも、後述する端末認証に必要な秘密鍵の保管にセキュア・エレメントが用いられている。現在は普及も進んだため価格も安価で、IC チップに広く搭載されている。

---

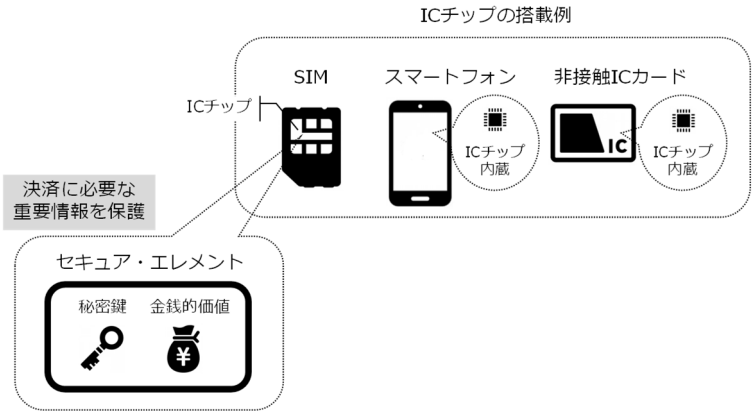
[13] SIM（Subscriber identity module）カードは、携帯電話（フィーチャーフォンやスマートフォン）に装着されている IC カードのことを指す。携帯電話の新規契約をすると、携帯電話会社は新しい SIM カードを発行し、カード内のセキュア・エレメントに契約者（利用者）の識別番号や電話番号、メールアドレスなどの情報が記録される。

[14] こうした SIM カードは、Overlay/Sticker SIM と呼ばれ、例えば、国外の携帯電話サービスを利用する際に用いられている。

[15] セキュア・エレメントの安全性については、下記資料が参考になる。
宇根正志、廣川勝久、「モバイル端末による金融サービスの安全性を高めるために：セキュア・エレメント等の活用」、日本銀行金融研究所ディスカッション・ペーパー、2017 年

[16] 決済分野では、セキュア・エレメントが用いられる以前は、磁気ストライプにカード情報を保管するケースが多かった。しかし、磁気ストライプは安全性に課題があり、例えばスキミングと呼ばれる手法により、カード情報が盗取される事例が発生している。決済分野のセキュリティについては、例えば下記を参照。
岩下直行、「金融機関の情報セキュリティ対策のあり方について」、『金融研究』第 25 巻別冊 1 号、2006 年

図 2：IC チップとセキュア・エレメント



② ユーザー間の情報伝達

DigiTally のケースでは、端末間の通信機能を利用しないため、ユーザーは決済を行う際、必要な情報（決済金額、送金者と受領者の電話番号、Code）を口頭で伝達する。これらの情報は、以下で説明する取引相手の端末認証と、決済指示において利用される。

③ 認証：保有者認証と端末認証

ユーザーは、決済の安全性を確保するために、自らのフィーチャーフォンの利用に必要な保有者認証と、取引相手の端末認証の 2 つの作業を行う。

保有者認証とは、フィーチャーフォンの利用者が正当な保有者であることを確認するための手法である。フィーチャーフォンの利用・操作に際しては、パスワード入力を設定することができる。端末の紛失・盗難時には、パスワードを知らない真の保有者以外による不正利用を防止できる。

さらに、ユーザーは決済に先立ち、取引相手の端末の正当性を確認する必要がある。こうした作業は端末認証と呼ばれ、電子マネーやクレジット・デビットカードでも広く利用されている。仮に、偽造された端末と取引すると、本来期待されるセキュリティ水準が確保されず、端末内に保蔵された金銭的価値の盗取などの不正が発生するおそれがあるため、安全性を確保するうえで端末認証は重要なプロセスである。DigiTally では、SIM カードにプログラムが追加された正当な端末には「秘密鍵」と呼ばれるデータが保管されている。ユーザーは、取引相手の端末が秘密鍵を保有していることを確認できれば、相手端末の正当性を認証できる。ただし、秘密鍵の内容が漏洩すると、秘密鍵を偽造端末に保管することで様々な不正が可能になるため、実際の取引では、秘密鍵を開示する代わりに、秘密鍵に基づき生成した Code を用いて端末認証を行っている。具体的には、ユーザーは、自身のフィーチャーフォンで生成した Code が、取引相手から伝達

された Code と一致することを確認することにより、相手の端末の正当性――取引相手の端末が秘密鍵を保有すること――を確認している[17]。

④　決済指示

決済を実行するには、送金者、受領者のフィーチャーフォンに対して、保蔵されている金銭的価値の増減を指示・記録する――金銭的価値の情報を上書きする――必要がある。DigiTally では、ユーザーが決済金額、取引相手の電話番号、Code を自らのフィーチャーフォンに入力することで、決済指示の伝達・実行を実現している。

⑤ 電力確保

フィーチャーフォンは、電池切れへの対応が課題となるが、乾電池による給電が可能な機器は安価に入手可能であり、停電時への対応力は確保可能と考えられる。

（DigiTally の課題）

DigiTally には、オフライン P2P 決済に最低限必要な機能が備わっているが、実用化に向けた課題は多い。まず、情報伝達（上記②）に関しては、口頭伝達の負担が生じる。取引相手の端末認証（③）でも、情報の口頭伝達が必要になるため、長さの短い Code を利用せざるを得ず、安全性に課題がある――悪意ある者が Code やユーザーの電話番号を入手した場合、金銭的価値が偽造されるリスクがあるため、Code は十分長く複雑である方がよい――。さらに、決済指示（④）でも口頭伝達と手作業が利用されており、利便性が高いとは言い難い。こうした安全性や利便性における課題を踏まえると、実用化に向けたハードルは高いと考えられる。

4．ユニバーサル・アクセス端末によるオフライン P2P 決済の実装

以下では、利便性や安全性を重視したオフライン P2P 決済の実装方法として、（1）スマートフォン、（2）カードやウェアラブル端末等の新たな端末を用いた手法を整理する。いずれもまだ実用化された事例ではないが、現時点で利用可能な技術や新規開発が必要な機能を組み合わせた実装案として紹介する。

4.1. スマートフォンを用いる手法

スマートフォンは、既に様々な決済サービスに利用されており、オフライン決済への

[17] DigiTally における端末認証では、全ての端末が共通の秘密鍵を利用している。こうした認証方法は、共通鍵暗号方式と呼ばれる。

転用が可能なハードウェア・ソフトウェアが多数搭載されている。さらに、オンライン接続機会も確保しやすいため、台帳との機動的な接続やソフトウェアの遠隔更新が可能な点もメリットと考えられる。

ここでは、ユーザー同士がスマートフォンを使うケースを想定する。具体的には、受領者が自らのスマートフォンに受領金額を入力し、送金者のスマートフォンに近付けるだけで、オンライン接続することなく、送金が完了する実装案を紹介する。こうした手法は、現在、店舗等における対面決済で利用されている非接触型決済に近い。以下、オフライン決済の基本機能（前節の①～⑤）に沿って説明する。

① 金銭的価値の安全な保蔵

CBDC の保蔵に当たっては、フィーチャーフォンと同様、安全性の確保を重視し、セキュア・エレメントを利用する方法が考えられる。スマートフォンの中には複数のセキュア・エレメントを持つタイプも少なくなく、SIM カードのほか、端末内の IC チップに内蔵されたタイプ（Embedded secure element、eSE）を利用することも可能である。

② ユーザー間の情報伝達

情報伝達では、近年普及しつつある無線通信の利用が考えられる[18]。スマートフォンには、オフライン環境でも端末間の情報伝達が可能な近距離無線通信技術（Near-field communication、NFC）の搭載が拡大している[19]。具体的には、電波受信のアンテナに加え、電波発信機能を備えた「リーダ/ライタモード」機能が搭載された機種では、NFC の利用が可能になっている（図 3）。

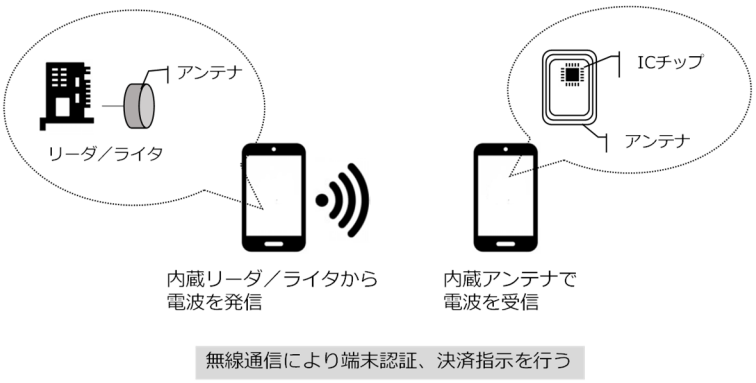
ユーザー間の情報伝達に NFC を利用すると、利便性の向上を図ることができる。フィーチャーフォンを用いる DigiTally のケースのように手作業を要することなく、短時間で正確に情報を伝達できる。さらに、（以下で説明する）認証のプロセスでも、口頭では伝達が難しい十分な長さの暗号文を利用できるため、安全性の面でもメリットがある。

---

[18] その他の情報伝達手段としては、スマートフォンにバーコードや QR コードを表示し、これをカメラで読み取る光学的な情報伝達手法も存在する。

[19] NFC Forum, “Device Requirements, High Level Conformance Requirements, Version 2.0,” 2017.

図 3：NFC の概要



③ 認証：保有者認証と端末認証

NFC のような無線通信の場合、端末の保有者認証が省略されると、近隣の端末保有者との合意がない状態で決済が行われるリスクがある。このため、保有者認証を通じたセキュリティ確保が重要となる。スマートフォンの保有者認証は、フィーチャーフォンで用いられるパスワード入力だけではなく、指紋や顔等の身体的特徴を利用する手法も存在する。こうした生体認証は、パスワードのように他者に盗取されるおそれが相対的に低いため、真のユーザー以外による不正利用の防止が期待できる。

取引相手の端末認証では、無線通信の利用に伴い、暗号技術に基づく DigiTally と同様の仕組みを速やかに実現できる。無線通信では、口頭伝達とは異なり、多くの情報量が含まれた十分な長さを持つ暗号文が利用可能であり、セキュリティの向上を図ることができる。

④ 決済指示

決済を実行するには、セキュア・エレメントに取引内容を指示し、金銭的価値の変化を記録する必要がある。現在普及が進んでいるスマートフォンを用いた電子マネーでは、店舗等に設置されたリーダ/ライタと呼ばれる据付型読取端末が、ユーザー端末内の IC チップのセキュア・エレメント情報を読み取った後（read）、リーダ/ライタの通信機能を利用して決済指示を発信し、セキュア・エレメントに金銭的価値の変化を書き込む（write）運用が一般的である。最近のスマートフォンには、店舗に設置された読取端末リーダ/ライタと同様、決済指示の発信・実行が可能とみられる「リーダ/ライタモード」機能が搭載されているため、オフライン P2P 決済では、これを活用したアプローチが想定できる。具体的には、受領者が決済金額をスマートフォンに入力した後、これを送金者のスマートフォンに十分近付けると、リーダ/ライタモードから送金指示が発信され、受領者のセキュア・エレメント内の CBDC の増額と、送金者の CBDC の減額

が実現する仕組みが想定される。

⑤　電力確保

スマートフォンは、フィーチャーフォン同様、乾電池から給電できる機器を安価に入手できるため、停電時への抵抗力はある程度確保されていると考えられる。

（課題）

スマートフォンを用いたオフライン P2P 決済は、ユーザーに利便性の高い決済方法を提供可能である一方、課題もある。まず、わが国では、スマートフォンの普及率が 2018 年時点で 65%であり、ユニバーサル・アクセスの確保という点では必ずしも十分とはいえないと考えられる[20]。また、金銭的価値の保蔵（①）に関しては、既存のセキュア・エレメントを利用する場合は、ライセンス料等が発生する可能性があるほか、これらを新規開発する場合は、追加的な費用負担や端末メーカーとの搭載交渉等が課題になる。スマートフォンの保有は、フィーチャーフォンに比べて費用がかかるため、コストの面でユニバーサル・アクセスの確保が難しいということも考えられる。さらに、決済指示（④）におけるリーダ/ライタモードの活用のように、実用化に向けて十分なフィージビリティ・チェックが必要な分野もあり、機能の安定性や処理性能の確保など、技術の成熟度の面で検証すべき点は少なくないと思われる。

4.2. カードやウェアラブル端末等の新たな端末を用いる手法

次に、現時点では存在しない新たな端末を用いたオフライン決済の実装イメージを紹介する。例えば、予め CBDC が保蔵されたカードを安価に提供できれば――Suica や PASMO のカードのイメージ――、子供や高齢者、あるいは海外からの旅行者など幅広い層の人々の利用も展望され、ユニバーサル・アクセスに資する可能性がある。このほか、腕時計型等のウェアラブル機器にも搭載できれば、多様なユーザーニーズへの対応も可能になる[21]。

まず、比較的イメージしやすいケースとして、CBDC を保蔵したカードとスマートフォンとのオフライン P2P 決済を想定すると、現在利用可能な技術を組み合わせることで、実装は可能とみられる。具体的には、スマートフォンに決済金額を入力し、CBDC を保蔵したカードに十分近付けて決済を実行する方法が考えられる。前述の通り、スマートフォンには、取引相手の端末への電波発信や送金指示機能を備えたリーダ/ライ

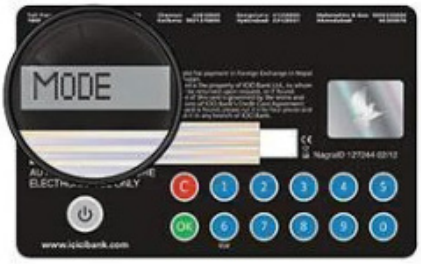
[20] 総務省、「令和元年版　情報通信白書」、2019 年

[21] Bank of Canada, “Contingency Planning for a Central Bank Digital Currency,” 2020.

タモードが搭載されることが多いため、この機能を利用すれば、カードとスマートフォンとの決済は概念的には可能である。

一方、カード同士や、ウェアラブル端末同士のオフライン P2P 決済に関しては、現在の技術で実装可能な機能もある一方、新たな技術開発を要する分野が少なくない。例えば、カード同士を十分近付けて決済する方法では、金額を入力・表示するための小型テンキー・モニターをカード上に搭載し、電池もカードに内蔵する必要がある（図 4）。こうした機能は、一部クレジットカードへの搭載実績があるが、オフライン決済を行うには、カード間で情報を伝達するための無線通信機能も求められる[22]。以下では、前述の①～⑤に沿って必要な機能・技術を整理する。

図 4：テンキー・モニター搭載型カードの例



(出典) icicibank.com

① 金銭的価値の安全な保蔵

CBDC や秘密鍵の保管に当たっては、他の手法と同様、IC チップ内のセキュア・エレメントの利用が想定される。セキュア・エレメントは既に一定の小型化が実現しており、電子マネーやクレジット・デビットカードへの利用が定着している。このため、新型カードやウェアラブル機器に、CBDC や認証向けの秘密鍵を保管することは、技術的には可能と考えられる。

② ユーザー間の情報伝達

ユーザー間の情報伝達に用いられる無線通信の実装に当たっては、新規の技術開発が必要になる。スマートフォンにはリーダ/ライタモードが搭載されており、ある程度の小型化が図られているものの、同様の機能をカード等の端末に実装するには、さらなる小型化が必要と考えられる。

---

[22] クレジットカードの中には、オンライン・ショッピングの支払時に利用するワンタイムパスワードをカード上のモニターに生成可能なタイプが存在する。具体的には、ユーザーがオンライン・ショッピングの支払い時に、カード上の小型テンキーに自らの PIN を入力すると、カード上のモニターに、オンライン認証向けのワンタイムパスワードが表示される仕組みで、カード内部には電池も内蔵されている。腕時計型のウェアラブル端末でも、テンキー、モニター、電池が搭載されるケースが一般的である。

③　認証：保有者認証と端末認証

保有者認証では、パスワードに加え、指紋等の生体情報の利用が想定される。パスワードに関しては、ウェアラブル端末では一般的に用いられているほか、カード型の場合も、後述するように決済指示で利用されるテンキーやモニターを用いた実装が考えられる。一方、一部のクレジットカード等では、既に指紋センサーが搭載されており、セキュリティを強化する観点からは、こうした生体認証の利用も考えられる。

端末認証は、スマートフォン同様、無線通信を利用する場合は、十分な長さの暗号文を利用することで、一定のセキュリティが確保できると考えられる。

④　決済指示

決済指示には、決済金額の表示・入力に利用するモニターやテンキーなどと、取引相手の端末に情報を記録するためのリーダ/ライタ機能が必要である。前述の通り、一部のカード型端末やウェアラブル端末では、モニターやテンキー機能が搭載されているが、決済への利用を想定すると、十分な処理性能と安定性を確保することが求められる。リーダ/ライタは、前述の情報伝達だけではなく、金銭的価値の記録も担うため、小型化を通じた実装が必要と考えられる。

⑤　電力確保

ウェアラブル端末は、乾電池からの給電が可能である一方、カード型は電力の確保が課題となる。現時点では、カードに内蔵可能な小型電池はパスワード表示のように用途が限定されている。しかし、決済処理への利用も想定すると、電池寿命は短期化すると考えられる。このため、電池寿命の長期化や、乾電池等からの充電機能の確保が課題になると思われる。

（課題）

カード等の新たな端末の価格を、スマートフォンに比べて安価に抑えることができれば、ユニバーサル・アクセスの確保に資するとみられる一方、必要な機能の開発に当たっては一定の期間とコストが必要と考えられる。特に、ユーザー間の情報伝達（②）や決済指示（④）に必要になるリーダ/ライタ機能の小型化が必要と考えられる。さらに、決済金額の入力・表示に利用する小型テンキー・モニターに加え、十分な寿命や充電機能を備えた小型電池の開発（⑤）が重要である。

5．オフライン決済の安全面とコンプライアンス上の課題

CBDC のオフライン決済の実用化に当たっては、前節で整理した実装面における技術的な課題だけではなく、セキュリティ確保のためのセーフガードなど CBDC の設計・運用上の課題、さらにはプライバシーの確保や AML/CFT への対応といったコンプライアンス上の課題も重要になる。これらは、オンライン、オフライン決済にかかわらず重要な課題であるが、オフライン環境下ではより対応が難しくなるため、しっかり検討を行う必要がある。

（セキュリティ確保のためのセーフガード）

セキュリティの強化は、CBDC の偽造抵抗力の確保や、各種不正を排除するうえで不可欠である。CBDC の発行や利用が拡大すれば、攻撃者は不正手口をより巧妙、大規模に行う可能性がある。また、中央銀行にとっては、不正発生に伴う信頼喪失も大きなリスクである。オフライン決済のセキュリティについては、セキュア・エレメントと暗号技術を利用した認証により、一定の安全性が確保されるが、オフライン決済に固有の事情を踏まえ、不正手口の巧妙化や暗号技術の安全性が低下するリスクへの対応が重要になる。脅威は常に変化し得るため、リスクのタイプを事前に想定することは難しいが、以下ではオフライン決済に固有の構造に着目し、セキュア・エレメントが搭載される IC チップと暗号技術に関するリスクを整理する。

IC チップ内のセキュア・エレメントは、直接的な物理攻撃や、IC チップの消費電力や放射電磁波等を観測・解析して秘密鍵を盗取する間接的な攻撃（例：サイドチャネル攻撃、フォールト攻撃）への耐タンパー性を備えている。しかし、IC チップに対する攻撃は絶えず巧妙化・複雑化しており、継続的な対応が不可欠である[23]。万一セキュア・エレメントが破られ、攻撃者による秘密鍵の盗取や CBDC の不正記録が可能になると、オフライン決済の場合は CBDC が偽造されるリスクがある。正当性のない端末のセキュア・エレメントに秘密鍵を保管し、実際には発行されていない偽造 CBDC を記録すれば、取引相手はこれらを正当なものと誤認し、偽造 CBDC の受領に応じてしまう。こうした操作は、運営者による対応が講じられるまで何度も繰り返すことが可能であり、深

[23] IC チップへのサイドチャネル攻撃やフォールト攻撃への対策については、以下を参照。
鈴木雅貴、菅原健、鈴木大輔「サイドチャネル攻撃に対する安全性評価の研究動向と EMV カード固有の留意点」、『金融研究』第 34 巻第 4 号、2015 年 10 月
崎山一男、「電子情報通信学会 知識ベース 1 群（信号・システム）- 3 編（暗号理論）-14 章（サイドチャネル攻撃と耐タンパー技術）」、電子情報通信学会、2019 年 7 月

刻な被害が生じ得る[24]。

対応策の一つは、セキュリティを確保するための定期的な端末交換である。オンライン接続が可能であれば、技術的にはセキュリティ関連ソフトウェアのアップデートを通じた強化が可能である一方、オンライン機能のない端末の場合は、こうした対応を採ることができない。このため、端末交換時に、高度な安全性を備えた新機種の提供が可能となるよう、セキュリティ向上に向けた継続的な取組みが求められる。また、スマートフォン等に比べて交換頻度が低いとみられるカード型等については、クレジット・デビットカードのように有効期限を設け、定期的な交換を義務付ける対策が有効と思われる。このほか、端末がマルウェア等の不正なプログラムに感染すると、CBDC が不正送金されるおそれもあるため、セキュア・エレメント以外におけるソフトウェア面の工夫も必要と考えられる[25]。

暗号技術の安全性が低下するリスクにも注意が必要である。現在広く利用されている手法では、セキュア・エレメント内に保管されている秘密鍵の盗取は事実上不可能と一般には考えられているが、攻撃者の計算能力向上に伴い、暗号技術のセキュリティは低下する。暗号技術に利用される秘密鍵や暗号文の生成手法（暗号アルゴリズム）は、事後的な修正を許容しないかたちでセキュア・エレメントに組み込まれることが多いため、セキュリティを継続的に確保するには、一定期間ごとにハードウェアを交換する必要があると考えられる[26]。さらに、量子コンピュータのように、極めて高い処理能力を持つ技術が実用化されれば、多くの暗号技術の安全性が損なわれるおそれがある[27]。業界では、量子コンピュータによる不正を阻止するための技術開発も続けられているため、最新の知見を踏まえた暗号アルゴリズムの実装に取組むことが重要と考えらえる。

オフライン環境では、管理者が脅威を常時把握することが困難であり、脆弱性が発覚した場合でも、決済サービスの利用停止など実効性のある対応を採ることは難しいと考えられる。こうした事態に備えるには、上記のように、端末のセキュリティ確保に万全

---

[24] オンライン決済の場合でも、認証に必要な情報が盗まれれば、真のユーザーのなりすましにより CBDC が盗取されるリスクがある――ただし、被害額はオフライン決済に比べ小さいと想定される――。オンラインでは、最新の取引実績を真のユーザーの端末にリアルタイムで通知する機能等を用いることで、不正を逸早く察知し、利用停止等の被害抑制策を講じることが重要である。

[25] 宇根・廣川 (2017) は、マルウェアによる不正対応として、ソフトウェア・ベースの実行環境である TEE（Trusted execution environment）の研究動向を紹介し、金融分野で活用していくうえでの留意点や課題を考察している。

[26] 宇根正志・神田雅透、「暗号アルゴリズムの 2010 年問題について」、『金融研究』第 25 巻別冊 1 号、2006 年

[27] 日本銀行金融研究所、「第 19 回情報セキュリティ・シンポジウム『量子コンピュータが金融サービスのセキュリティに与える影響』の模様」、『金融研究』第 38 巻第 1 号、2019 年

を期すとともに、端末への CBDC の保蔵金額や利用金額に上限を設けることで、被害規模を予め限定することも一つの選択肢となろう。あるいは、オフライン決済が連続し、累計利用金額が一定水準に達した場合は、端末の利用を一時的に停止する仕組みも考えられる。ただし、こうした制約を導入した結果、災害時のようにオンライン接続が困難な局面における機動的な利用が妨げられれば、オフライン P2P 決済の目的である強靭性が損なわれるため、セキュリティと利便性のバランスをどう確保するかが重要となる。

（プライバシーの確保と AML/CFT への対応）

決済における匿名性やプライバシーを CBDC においてどのように、そしてどの程度確保していくかは重要な課題である。一般に、口座型 CBDC に比べ、トークン型 CBDC の方が暗号技術を活用することにより、ユーザーの特定を回避するための匿名性（anonymity）を確保しやすい。もっとも、口座型の場合でも、CBDC の設計上は、口座に実名とは異なる仮名等を用いることで、口座と本人情報との紐付けを回避することにより、匿名性を確保することは可能である[28]。

一方、デジタル決済においては、プライバシーや匿名性への配慮と同時に、AML/CFT への対応を両立させていくことが重要である[29]。オンライン決済における匿名性と（AML/CFT への対応に不可欠な）取引データの追跡可能性については、日本銀行が技術的な観点から調査研究を進めている[30]。オフライン決済に関しては、CBDC の台帳管理者（や公的当局）が決済情報を把握することが困難になるため、AML/CFT への対応のハードルも一段高くなる。すなわち、オフライン決済情報については、取引当事者のいずれかの端末がオンライン接続されない限り、台帳管理者や公的当局は把握することができない。オンライン接続が可能な端末でも、ユーザー同士が決済情報を秘匿するためにオンライン接続を回避し続ければ、当局はいつまでも決済情報を把握できない。また、カード型のように機能を限定した端末の場合、オンライン機能の搭載が難しい可能性があり、こうしたケースでは、当局による決済情報の把握は困難と考えられる。この

---

[28] 取引相手や公的当局がユーザーの実名を把握できない状況でも、仮名に紐付いた決済情報を収集することで、同一ユーザーの決済履歴を追跡することは可能である。プライバシーの確保に当たり、こうした「追跡を許容しない性質（untraceability）」も CBDC に求める場合は、仮名の利用だけでは不十分となる。この場合、暗号技術の利用や、端末が予め複数の仮名を保有しこれらを状況に応じて使い分ける等の工夫が必要になる。

[29] 公的当局による決済情報の把握を前提とする場合は、実名とは異なる仮名の利用を許容しても、仮名と本人情報を紐付ける仕組みが必要になる――端末保有時に予め本人確認が必要になる――。

[30] 日本銀行・欧州中央銀行、「プロジェクトステラ：分散型台帳環境における取引情報の秘匿とその管理の両立（日本銀行仮訳）」、2020 年

ように、ユーザーが端末のオンライン接続を回避できる設計であれば、ユーザー同士が秘匿意思を持つ限り、当局に対してプライバシーを確保できるが、当局にとっては、AML/CFT への対応が困難になる。

AML/CFT やプライバシーの問題にどう対応すべきかは、中央銀行が直接所管する分野ではなく、公的当局が決済以外の観点も含め様々な観点から多角的に検討する必要がある[31]。仮に、決済情報が把握できない状態を一切許容しない場合には、そもそもオフライン決済の利用を禁じる他ない。一方、オフライン決済を許容しつつ、不正取引のリスクを抑制するアプローチを採るのであれば、台帳へのオンライン接続の都度、過去の決済履歴の台帳記録を求めることで、異常な反復取引などを検知できるようにすることが必要になる。また、セキュリティ面への対応と同様、オフライン取引に利用制限を設けることも一つの選択肢となる。例えば、ローカル型の価値保蔵金額に上限を設けたり、少額の反復取引による大口化を防止するために、毎月の価値保蔵回数や累計利用金額を限定することが選択肢となる。カード型等のオフライン専用端末の場合は、一回の購入で入手可能な個数に上限を設ける方法が考えられる。もっとも、これらの対応は不正抑止につながる一方、オフライン決済を小口取引に限定すれば、災害時等における利用や利便性を損なう面もあるため、両者のバランス確保が重要となる。

6．おわりに

本稿では、「誰もがいつでも何処でも、安全確実に決済に利用できる」という現金の特性――すなわち、ユニバーサル・アクセスと強靭性――を CBDC が備えるうえでの課題について、技術的な側面から検討した。ユニバーサル・アクセスに関しては、多様なユーザーが利用可能な端末の開発が求められるほか、強靭性に関しては、通信・電源途絶への耐性を備えたオフライン P2P 決済機能を確保することが望ましい。ユニバーサル・アクセス端末による CBDC のオフライン P2P 決済について、安全性を確保しながら実現するにはなお課題が多く、さらなる調査研究や技術開発が必要と考えられる。また、現金決済のもう一つの特徴である匿名性やプライバシーについても、CBDC の発行に際しては十分な検討が必要となる。AML/CFT の観点も念頭に、これらコンプライアンス上の課題をクリアしていくには、中央銀行は関連する公的当局と議論を深めていくことが重要である。安全性やコンプライアンスの問題については、技術的な視点から

[31] ちなみに、前掲の Bank of England (2020)は、現金の匿名性は現金という決済手段が持つ特徴であって、追跡不能性や匿名性を備えた決済手段（untraceable or anonymous payment methods）の提供に関する具体的なマンデートは BOE には課されていないと指摘している。

の解決策だけではなく、取引制限など CBDC の運用という制度的な視点からも検討していかねばならない。

CBDC を巡っては、本稿で取り扱った決済手段という視点だけではなく、その発行が金融システムや金融政策に与える影響も含め、検討すべきテーマが多岐にわたる。社会の中銀マネーに対するニーズを的確に汲み取り、デジタル社会に相応しい中銀マネーのあるべき姿について、様々な視点から議論を深めていく必要がある。日本銀行としては、実証実験等を通して、技術面からみた実現可能性（フィージビリティ）を確認していくとともに、海外中銀や内外の関係諸機関と連携をとりながら、CBDC に関して検討を進めていく方針である。

以　上