

2024 年 8 月 16 日
日本銀行決済機構局

C B D C フォーラム W G 5
「ユーザーデバイスと U I / U X」
第 2 回会合の議事概要

1. 開催要領

(日時) 2024 年 5 月 9 日 (木) 14 時 00 分～16 時 30 分

(形式) 対面形式及び W e b 会議形式

(参加者) 別紙の通り

2. プレゼンテーション

- 事務局から、「オフライン決済に関する海外の取り組みのご紹介」の資料¹に基づき、プレゼンテーションを行った。
- 株式会社ジェーシービーより、オフライン環境下の P 2 P 送金を主要テーマにした実証実験プロジェクトについてプレゼンテーションが行われた。また、オフライン P 2 P 送金に関するデモンストレーションが行われた。

—— プレゼンテーションでは、実証実験プロジェクトの目的として、「既存の決済インフラの活用による円滑・低コストでの C B D C インフラ構築」、「用途に応じた最適な決済インフラの選択」、「現実的な C B D C 活用方法」が挙げられた。また、実証実験プロジェクトは複数のフェーズからなっており、フェーズ 1 では店舗を対象とした既存オンライン決済インフラ活用の検証を、フェーズ 2 では P 2 P 送金におけるオフライン決済の検証を、今後行われるフェーズ 3 ではオンライン決済とオフライン決済のブリッジ機能の検証を行うとの説明があった。今回はこのフェーズ 2 を中心に説明があった。

3. ディスカッション

- 事務局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

¹ 事務局プレゼンテーション資料は、本行ウェブサイト
(https://www.boj.or.jp/paym/digital/d_forum/dfo240816e.pdf) を参照。

を行った。議論の概要は、以下の通り。

（参加者）資料の 9 ページに、デバイスの紛失時に価値を他人に不正利用されてしまうことを防ぐため、Purse のブロックリストを用いる対策例が示されていたが、Purse のブロックリストの配信はオンラインでなければならないと思われる。

（日本銀行）ご指摘のとおり、Purse のブロックリスト対応はオンライン接続が必要となるが、デバイスは、オフライン決済時はともかく、チャージや払出等の場面では何等かのオンライン接続が前提となっているため、一定の有効性のある対策かと思う。

（参加者）資料の 11 ページに、e-krona のパイロット実験ではスマートフォンのセキュアストレージと TEE を利用できなかったとの説明があったが、これは、デバイス側の技術的な課題というよりは、OS 事業者との調整に課題があったということではないだろうか。こうした課題があるにせよ、スマートフォンを使わないユーザーが一定層いることを踏まえると、このようなカードも併用したモデルは検討すべきと思われる。

（参加者）事務局から説明のあったオフライン決済の定義を踏まえると、現行の民間の決済サービスにおいてもオフライン決済をすでに実現していると考えられる。例えば、交通系 IC カードは、カード内に残高を保持しており、必ずしも決済時に中央のセンターにアクセスする必要はないためオフライン決済といえる。すなわち、交通系 IC カードを用いて店舗で決済した場合、店舗は必ずしも決済の都度 이슈アと通信しているわけではなく、一旦溜めた決済情報を後でまとめて 이슈アに連携する仕組みとなっている。

（日本銀行）CBDC と民間が提供する決済サービスとでは考え方が異なる部分もあるため、本WGにてCBDCの文脈でオフライン決済を取り扱う意義は大きい。例えば、民間の決済サービスには、オフライン状態で支払いをした結果、カードなどのローカル側とセンター側のサーバの金額に不整合が生じた場合、ローカル側の金額を基本的に正しいものとするケースもあると聞いている。これと同じ対応をCBDCのオフライン決済でとり得るかは明らかではない。

また、そもそもCBDCにオフライン決済を具備すべきかどうかという論点もある。さらに、スマートフォンのセキュアストレージ及びTEEの利

用が課題としてあげられているが、この課題に対処するためにどのようなアプローチがあるかご意見を頂きたいと考えている。

(参加者) オフライン決済は、C B D Cのオンラインシステムのトランザクションコストを下げる効果があると考えられる。これは、オンライン決済の場合には決済の都度、各デバイスとセンターサーバ間でトランザクションが発生するところ、オフライン決済では、処理がバッチ化されることでデバイス—サーバ間のトランザクション回数が減ることもあるためである。

- 株式会社ジェーシービーからのプレゼンテーションおよびデモンストレーションを受けて、参加者によるディスカッションを行った。議論の概要は、以下の通り。

(参加者) 1つ目のデモンストレーションは、支払人と受取人がそれぞれI Cカードを用いて行うオフラインP 2 P決済を行うものである。これは、リクスバンク等が実施した実証実験と同様のモデルであるが、N F C機能付きスマートフォンを介して、支払者のI Cカードから受取者のI Cカードへ価値を移転するもの。本モデルでは、価値は、I Cカードに常時保管されており、スマートフォンはI Cカード内の価値の参照やI Cカード間の価値の受け渡しを行う通信機器として用いられる。

本モデルは、I Cカードだけではなく、スマートフォンも必要となるため、ユーザビリティは必ずしも高くない。一方で、本モデルは、価値はI Cカードにのみ保管されるという点で、今後求められるであろうセキュリティ要件の充足性をより容易に確認できるというメリットがある。すなわち、I CカードはE M Vというスタンダードがあるが、スマートフォンの場合はセキュリティ要件の充足性を確認するためにはデバイスメーカーやO S事業者との調整等が必要となり、中央銀行にとってはチャレンジな課題になると考えられる。このため、リクスバンク等の実証実験では、I Cカードに価値を保管する上記モデルが採用されたものと思われる。

なお、既存の電子マネーの決済サービスも、I Cカードに価値を保管するものだが、閉じた環境や特定の決済端末のみで利用可能という前提が置かれており、誰でも価値を取り出せる仕組みにはなっていない。一方、C B D Cは、よりオープン環境で利用できる必要があるため使える、これが民間サービスにはない実装上の考慮点となる。

(日本銀行) スマートフォンを用いてＩＣカード間の価値を移転する際に、一瞬であれ、通信機器であるスマートフォンが価値を保持する仕組みであると理解しているが、例えば、そのままスマートフォンの中に価値が留まってしまふような状況も起こり得るということだろうか。そうした状況ではその価値をどのように扱うのか。

(参加者) そのような状況が発生した場合の価値の扱いや、決済の取消処理の方法までは考慮していない。

(日本銀行) すでに活用されている技術を活用すること、安全性やファイナリティなどの要件を満たすこと、利便性や拡張性の高い決済サービスを実現することの全てが同時に実現できれば理想的ではあるが、このうち２つを満たそうとすると、残りの１つが満たされにくいといった、トリレンマのような状況があるのかもしれない。

(参加者) 欧州を中心に各中央銀行の実証実験で様々な検証が行われてきたが、おっしゃるような問題があるがゆえに、例えば、ＣＢＤＣの実装を既存の民間決済システムに寄せる、つまりディレイドのファイナリティのような、厳密なファイナリティ定義から多少離れるような選択肢も検討し始めている中銀もあるように自分としては見ている。

(日本銀行) ファイナリティの定義については、中央銀行業界においては前提も含めて様々な議論がなされているところ、皆さまのビジネスサイドにおけるターミノロジーと異なる部分はあるかもしれない。しかし、それ自体の定義を突き詰めて議論するというよりは、まずは様々な考え方がありうるという前提で議論を進めて頂ければと思っている。

(日本銀行) 通信機器としてのスマートフォンを使わずに、カード側にＮＦＣのリーダー機能を持たせて対応することは難しいのだろうか。

(参加者) カード側にリーダー機能をもたせることは、現状ではかなり難しいと思われる。

(参加者) 価値の移転が途中で途切れてしまった場合はどうするかという話は重要な論点である。２つのＩＣカードを同時に更新することは極めて難しく、情報工学的には未解決問題の１つだと思っている。

(参加者) 2つ目のデモンストレーションは、支払者と受取者がそれぞれスマートフォンを用いてオフラインP2P決済を行うものである。まず、オンライン状態にある支払者のスマートフォンを操作して、オフライン決済時に使う分の価値をロックする。その上で、オフライン状態にある支払者と受取者のスマートフォン同士をタップすることで、支払者が先にロックした価値を受取者のスマートフォンに移転させる。

価値の受取側は、Tap on Mobile または Pay with iPhone と呼ばれるようなスマートフォンを決済端末化する技術を利用している。ユーザーインターフェース上は、スマートフォンをタップした時点で資金移動がされているよう表示されるが、ファイナリティは、取引を行ったいずれかのスマートフォンがオンライン接続して、センターサーバに売上データが反映された時点で実現する仕組みとなっている。つまり、取引時点とファイナリティが付与される時点が異なることとなるが、こうした状況が許容されるならば、このモデルはC B D Cのオフライン決済に活用できることとなる。

(参加者) 2つのデモンストレーションについて、それぞれ残高のマスターデータはどこで保持されているか。また、スマートフォンなどのローカル側のデータとセンター側のデータをどう同期させるかは難しい問題のように思うがどうか。

(参加者) 1つ目のデモンストレーションでは、カードのICチップ上に正の残高(マスターデータ)を保持している。一方、2つ目のデモンストレーションでは、センターのサーバが正の残高を保持している。後者の場合、オフライン状態にあったスマートフォンは、オンラインとなった時にセンターのサーバへ接続してはじめて最新の正の残高を確認できることとなる。

1つ目のデモンストレーションにおけるローカル側にあるICチップ上の残高とセンター側のサーバ上の残高、2つ目のデモンストレーションにおけるセンター側のサーバの残高とローカル側の残高を、それぞれどのように同期させるかは、今後の検討テーマだと考えている。このバリュー管理システム間の同期機能が構築できれば、オンライン決済モデルとオフライン決済モデルがインフラをまたぐ形で併存する仕組みが実現できると思っている。

(参加者) まず、事業者目線で平時においてオフライン決済が必要なケースを考えると、通信環境のない地下や山間部で利用する場合も考えられるが、多くはオフライン状態が数時間程度しか継続しない状況下で利用する場合だと

思う。こうした想定を前提とすれば、B I Sのオフライン決済の3つの分類におけるFully offlineは必要なく、Staged offlineでも問題ないと考えられる。

次に、災害時には、通信途絶は3日間ほどで概ね解消されている。また、最近の大規模地震のケースでは、地震発生から2日間は命を保つ行動に集中し、その後3、4日目から生活復旧のために店舗に行き決済をするという状況が見られ、こうした状況下では、オフライン決済で利用されたC B D Cが転々流通することはあまり想定されないと考えられる。つまり、C B D Cのオフライン決済においては、通信途絶により3、4日間ほど転々流通ができなかったとしても、許容できるのではないか。このように考えると、日本ではStaged offlineの考え方で十分耐えられるのではないか。

C B D Cにオフライン決済を実装するのであれば、ユーザビリティを確保することは重要であり、転々流通をオフラインで実装するために、ユーザビリティを犠牲にすることは望ましくない。このため、オフライン決済を実現するために何かを犠牲にしなければならないということであれば、Staged offlineを採用するとともに、ディレイドのファイナリティのようなファイナリティの定義を緩やかにするという方法は一つの選択肢であると思っている。

(参加者) 支払者側のオフライン残高が50 あったが、100 に改ざんされたとする。その後、受取者側から支払者側に対して100の支払いリクエストがあった場合は、オフライン上では一応トランザクションが成立する。ただし、その後、支払者側がオンラインとなった際に、センター側のサーバの残高との不整合が明らかとなり、最終的なトランザクションは成立しない。このような理解で合っているか。

(参加者) おっしゃる通りである。2つ目のデモンストレーションにおいては、正の残高のデータは中央のサーバで管理されているため、スマートフォンの残高が改ざんされたところで、オンライン接続時に整合性が無いことがわかれば最終的なトランザクションは成立しない。

(参加者) 欧州ではスマートフォンのセキュアエレメントを活用することが難しいため、カードを用いる苦渋の選択をしたのではないかと個人的には認識している。他方、本邦では、様々な課題はあるものの、官民の努力によりセキュアエレメントの活用もある程度進展している点には注目している。

（日本銀行）本日も非常に活発なご議論及び、様々に忌避ないご意見いただき、
学びの多い会合であった。引き続き、様々な観点からの分析、意見交換が必要
であると思っており、先進的な業界の取り組みなど、情報共有頂ける内容
があれば、ぜひ参加者の皆様よりお寄せ頂きたい。

4. 次回予定

次回の会合は7月17日（水）に開催。

以 上

C B D C フォーラム WG 5
「ユーザーデバイスとUI／UX」
第2回会合参加者

(参加者) ※五十音・アルファベット順
チャンネルペイメントサービス株式会社
株式会社ジェーシービー
株式会社常陽銀行
ソニー株式会社
大日本印刷株式会社
日本電気株式会社
パナソニック コネクト株式会社
フェリカネットワークス株式会社
株式会社ふくおかフィナンシャルグループ
三井住友カード株式会社
株式会社三井住友銀行
株式会社三菱 UFJ 銀行
三菱 UFJ ニコス株式会社
株式会社ローソン
NRI セキュアテクノロジーズ株式会社
株式会社 NTT データ
株式会社 NTT ドコモ
TOPPAN エッジ株式会社

(事務局)
日本銀行