

2025 年 10 月 30 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 10 回会合の議事概要

1. 開催要領

(日時) 2025 年 9 月 22 日 (月) 14 時 00 分～16 時 30 分

(形式) 対面形式及び W e b 会議形式

2. プレゼンテーション

- 事務局から、「パイロット実験における机上検討（店舗決済における U X 上の課題）」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 N T T データより、価値移転プロトコル（電子現金）についてプレゼンテーションが行われた^[2]。

—— プレゼンテーションでは、「価値移転プロトコル」について、主に障害に対する強靱性や端末間のオフライン決済の観点から紹介され、その実行を支える認証局等の Root of Trust の役割や、価値移転プロトコルにおける価値移転の署名・検証ロジック、秘密鍵等を守るための隔離実行環境、及びセキュアデバイスといった 3 つの要素に関する技術的な取り組みが説明された。その上で、「幅広い状況下で使える」ためのディスカッションとして、店舗決済における決済結果不定時のタイムアウト処理中の価値移動リスクを取り上げ、WG 7 で議論された減額留保・増額留保^[3]の対策等が検証された。

3. 質疑応答とグループディスカッション

^[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/wg5/dfo251030b.pdf) を参照。

^[2] 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/wg5/dfo251030a.pdf) を参照。

^[3] WG7 第 6 回会合議事概要は、本行ウェブサイト

(https://www.boj.or.jp/paym/digital/d_forum/wg7/dfo251017a.pdf) を参照。

- 事務局からのプレゼンテーションを受けて、参加者による質疑応答を行った。議論の概要は、以下の通り。

(参加者) 店舗オペレーションの観点でも、災害時等にキャッシュレス決済を可能とするための検討がされており、その事例を紹介したい。全国に店舗展開し夜間帯も含めて決済を受け付けるコンビニエンスストアは、最初に障害を検知し易いが、実際の対応については、店舗決済端末等のフロント側・ゲートウェイ以降のバックエンド側・利用者媒体といった各キャッシュレス決済手段のネットワーク上で、どこが稼働/非稼働であるか次第で異なってくる。停電等でPOS等の店舗決済端末が稼働できない場合においては、QRコードのCPM決済に対してはJPQRステッカーを用いた静的MPM、クレジットカード決済に対してはエンボス転記のインプリンタ等の方式（オフライン決済）が一般的に考えられる。2020年の経産省の実証実験では、実店舗への配布等には至っていないものの、この2つの方式について店舗オペレーションの検証がされた。このほか、利用者のスマートフォンをレジ替わりとするスマレジや移動販売車といった方式に関する検討もある。

(日本銀行)「幅広い状況下で使える」CBD Cを考える上で、事務局から提示しているエラーハンドリングやタイムアウトといった処理に関する検討だけでなく、オフラインの代替手段も含めた、店舗決済を前進めさせるための議論も重要と認識している。

前段の事務局説明について補足すると、本事務局説明はオンライン決済を前提としたCBD C実験用システムの処理フローにおいて、システム・ネットワーク等の障害が発生した際の店舗決済のUX上の課題として、決済結果不定時のケースを取り上げ、二重支払防止等のUX改善策を示したもの。ここでは、台帳間の整合を保つために実験用システムの構築と検証で検討されているタイムアウト設定を用いた。また、待機画面をできるだけ避けながら適切に利用者に状況を伝えていくことも大事と考えており、民間のキャッシュレス決済手段で講じられている対応に照らして、ぜひご意見を賜りたい。

(参加者) タイムアウトは民間のキャッシュレス決済手段でも使われているが、タイムアウト時間は決済サービスの各事業者によって異なる。一般的に、フロントのPOS側は利用者を待たせないためにタイムアウト時間が短く設定されているため、ゲートウェイ以降のバックエンド側が処理応答待ちの状況でタイムアウトを返してしまうことがある。その場合、店舗オペレーションとしては、決済操作のやり直し、さらに、タイムアウトエラーが続いて

システム障害状態となれば、他の決済手段への誘導を店頭告知する対応となる。

利用者への伝達の観点では、決済未了・完了に関わらず、利用者と店舗との認識が合うことが重要であって、例えば、利用者のスマートフォンは決済完了の表示、POS側は未了の表示といったアンマッチは、返品判断も含めて店舗としては大変困る状況。クレジットカードや電子マネーのように、POS側の処理結果や残高照会表示を確認する構造の場合は、認識相違がない。

(参加者) 事務局資料で示されている店舗決済のUX上の課題への対応策については、NFCやQRコードといった店舗決済のインターフェースごとに定義して検討していく必要があるだろう。

ちなみに、インターフェースのうちNFCタッチ決済の仕様では、利用者のスマートフォンやカードといった支払元のデバイス側にはエラーハンドリングに関する手当てはない。デバイス側は、店舗決済端末から送られてきた処理を単純に処理実行してレスポンスを返すだけであって、例えば、決済処理中にカード等が離れてしまったら、また一からやり直す操作となるだけである。NFCタッチ決済と違い、QRコード決済では、支払元のスマートフォンにおいて決済サービスごとに様々な対策を行っていると思われることから、参考になることがあるのではないか。

(参加者) 一方、店舗側のデバイスであるリーダライター機能を含む店舗決済端末は、ゲートウェイセンターと一定の情報をやり取りする役割を担っている。平常時も含めた通信障害を前提に、タイムアウトの側面から、民間キャッシュレス決済手段ごとの実装方式の関係について紹介したい。

クレジットカード決済は、最終的に店舗決済端末からセンター側へ情報を送り届ければよい仕組みだが、通信が不安定で送信容量も少なかった電話回線の時代には、オフライン処理を可能として決済完結できるよう店舗決済端末側で一時的に情報格納できる構造としていた。もっとも最近では、インターネット回線を前提に、運用コストの低減や迅速な利用者への情報提供のためにセンター側にアプリケーションを配置してデータを一元管理する構成が出てきており、オフラインでの決済処理には不向きとなっている。どちらを軸にシステム構成を考えるかという議論が今後の社会インフラを含めて必要となってくるかもしれない。

電子マネーは、代表的には利用者のデバイス側に残高を保持するため、店舗決済端末がデバイスに残高を書き込む際にセンター側の情報と一致していることを確認する必要がある。そこで処理未了が発生した場合は、利用者

デバイス側とセンター側とのアンマッチを解消しない限り、利用者は当該電子マネーを次の決済に使うことができない仕組みとなっている。

QRコード決済は、クレジットカードと同様に、基本的にはオンライン処理であって通信障害時には利用できないが、一部では、事業者側がリスクを負ってオフライン決済を許容するサービスが提供されている。

(参加者) クレジットカードのNFCタッチ決済が利用可能な自動販売機を例に、タイムアウトについてお話ししたい。

当該自動販売機においては、利用者を待たせず、決済の再試行、もしくは現金等の代替手段での決済といった次の操作を促すために、タイムアウトの時間は数秒程度としている。その際、自動販売機側はタイムアウトとなったにも関わらず、クレジットカードのイシュア側にはオーソリゼーションの電文が届いて取引が成立してしまっていた場合に備えて、取引ごとのユニークなキーを付したリバーサル電文が設けられている。これにより、タイムアウトとなった場合には、自動販売機側から同電文がイシュア側に送られ、取り消し判断が可能な仕組みとなっている。

また、自動販売機のような少額決済では、事業者等のポリシーによっては、オフライン決済を許可することがあるため、オーソリゼーションの電文は流さずに売上精算の電文のみで売上確定することもできる仕組みとなっている。

最後に、即時決済であるデビットカードによる決済が通信障害等で取り消し処理となった場合について述べる。与信枠を復活させればよいクレジットカードと異なり、預金口座からは一度引き落とされてしまうため、後日、預金口座へ返金処理が行われるオペレーションとなっている。

(参加者) クレジットカードにおいては、決済サービス事業者側と店舗側とのやり取りとして、クレジットカードの有効性確認や不正利用防止だけでなく通信障害等の異常系対応も含めたオーソリゼーションの仕組みが確立されており、オーソリゼーションがエラーであれば失敗、それが想定外に積みあがればシステム障害の判断を行い店舗等にお伝えすることとなる。例えば、海外では、インスタントペイメントの利用拡大に伴い不正利用が増加しており、Request to pay をオーソリゼーションの代わりに用いる検討がされている。このように、安全面を考慮すると、決済を実行する前にオーソリゼーションのような仕組みを実施すべきという動きが出てくる可能性もある。

また、災害時の利用について考える場合、民間のキャッシュレス決済手段は、最終的には現金の利用に誘導することを前提にしたシステムやオペレー

ションとなっているため、法定通貨として通貨や金融システムへの信認を担うC B D Cには当てはまらない部分が多いかもしれない。

- 株式会社N T Tデータからのプレゼンテーションを受けて、参加者による質疑応答を行った。議論の概要は、以下の通り。

(参加者) ネットワーク上に計算能力をもたせるインクルーシブコアの取り組みを活用し、キャリアネットワークのエッジ(モバイル・ネットワークの入り口となる基地局等)にT E E (Trusted Execution Environment)といった隔離実行環境の機能をもたせることで、オフラインの価値移転に汎用性や拡張性をもたらすアイデアについてご紹介いただいたが、これはシステム負荷が分散されるメリットがある一方で、コストも含めたフィージビリティ面での課題もあると思われるが、将来の実装イメージ如何。

(参加者) インクルーシブコアについては、実際には、6 G (第6世代移動通信システム) の議論の中で検討されているものだが、国内の基地局になるべく広く分散されるよう実装されとの認識。また、T E E機能は、当然コストアップの要素にはなりうるが、同様にインクルーシブコアに載せることが検討されているA Iと比べるとはるかに計算負荷が小さいことから大きな負担にはならないと考えられる。

(参加者) 例えば、既存のキャッシュレス決済手段の手数料のように、価値移転プロトコルを用いた決済システムを形成するためのコスト負担構造について想定があれば教えてほしい。

(参加者) 例えば、Root of Trust は価値移転プロトコルが機能するために重要な役割を担っていることから、その認証局から提供される証明書に対する利用手数料という考え方はあるだろう。C B D Cの役割を考えると、同様のビジネスモデルを当てはめることはできないかもしれないが、この価値移転プロトコルの仕組み自体は、C B D C以外にも、チケットや町内のポイントなど様々なユースケースに活用できる。

(参加者) 取引完了とU I / U Xの考え方についてお聞きしたい。既存のキャッシュレス決済手段それぞれに、何をもって取引完了としてそれをどのように確認するのかについて、本会合の前半に言及された技術面とビジネス面での様々な工夫に関連して、価値移転プロトコルでは、どのように実現する

想定か伺いたい。

(参加者) 基本的には、新しい考え方があるというわけではなく、受取側のウォレットの増額完了によって決済完了とするという前提をおいている。そのうえで、決済結果不定时等の支払側と受取側の間で認識が合わない状況においては、受け取った資金がさらに別の取引に利用されてしまう等のリスクを防ぐために、追加的に支払側と受取側の双方の確認プロセスを設け、それが上手くいかない場合は、決済完了せず、受取側の増額分の取消及び支払側の減額分の復元といった元の状態に戻す処理が実行されるような仕組みを想定している。

- 参加者による質疑応答の後、グループディスカッションが行われ、各グループ代表者からの発表が行われた。概要は以下のとおり。

(参加者) 事務局説明資料で紹介されたタイムアウト設定は、既存の民間キャッシュレス決済手段と同じように、決済結果不定时のリカバリに有効だろうという話があった。

一方で、UXの観点では、例えば、コード決済とタッチ決済では、利用者側の認識に違いがあることに留意が必要だろう。コード決済の場合は、利用者が自身のスマートフォンを用いて操作を行うことから、ネットワーク障害などがあった際に、自身のスマートフォンで決済処理状況を確認することができるが、タッチ決済の場合は、タッチのみの操作であることから、基本的には、店舗のPOS側の処理結果表示で気づくことになる。このように、店舗決済における障害時のUXは、システムとオペレーションを複合した検討が必要となってくるだろうという意見が聞かれた。

(参加者) CBDC送金においてタイムアウト設定は必要と考えられるところ、先ほどの議論であったような民間のキャッシュレス決済手段で導入しているユニークな取引ID等を用いた二重支払対策も合わせて検討すべきという話があった。

価値移転プロトコルについては、オンラインの残高から価値を切り出して、オフラインでの保存や端末間送金が可能であることから、災害時等において有用な決済手段であり、今後の検討においては、耐タンパ性デバイスも含めた、技術的に安全な価値移転を実現する仕組み作りがポイントになるだろうという意見があった。

(参加者) 価値移転プロトコルのようなプログラマブルなマネーが、将来的に、既存の決済システムのあり方にどのような影響を与えうるだろうかといった議論がされた。例えば、価値移転プロトコルでは、端末間決済の移転履歴を一定頻度でリセットする際に価値移転プロトコル(電子現金)の発行者がトランザクションの有効性検証を実施するプロセスがあり、こういったトラストの役割としての金融システムの重要性が言及された。

(参加者) オンライン決済の取引増に伴う処理量の限界といった課題に対して、各利用者のデバイス等に負荷が広く分散できる価値移転プロトコルは意義があるといった意見があった。

また、個人間送金と店舗決済で求められるUX上の違いについて議論がされ、個人間送金は、基本的には顔見知り同士の送金である等、ある程度の信頼関係が前提となるが、店舗決済ではそのような関係性が期待できないことから、双方が確りと決済結果を受け取ってアンマッチが発生しないような仕組み作りがより重要だろうという話があった。

(日本銀行) 前半のプレゼンでは、通信技術の進展に伴い、デバイスからセンターへデータが集約されることで、効率性の高いオンライン型の決済システムが形成されつつあるという民間キャッシュレス決済手段の変化にふれていただいた。その一方、後半のプレゼンでは、安全性を高めながら分散化を可能とする次世代の通信システムが示される等、CBDCシステムを考える上で、非常に示唆深い議論が多くあった。

本日の会合で、他WGでの検討内容も踏まえた議論があったように、今後もWGをまたがる形で多様な知見をいただきながら、実験用システムや各種机上検討に活かして参りたい。

4. 次回予定

次回の会合は10月31日(金)に開催。

以 上