2025 年 12 月５日
日本銀行決済機構局

# ＣＢＤＣフォーラム
# ＷＧ３「ＫＹＣとユーザー認証・認可」
# ＷＧ５「ユーザーデバイスとＵＩ／ＵＸ」
# 共同開催会合の議事概要

１．開催要領

（日時）2025 年 10 月 31 日（金）14 時 00 分～16 時 30 分
（形式）対面形式及びＷｅｂ会議形式

２．プレゼンテーション

- 株式会社三井住友銀行より、インターネットバンキング（以下、ＩＢ）不正出金対策に関するプレゼンテーションが行われた。

  ―― プレゼンテーションでは、政府が 2025 年４月に策定した「国民を詐欺から守るための総合対策 2.0[1]」や、実際の被害事例に基づき、近年の不正利用被害の発生状況や傾向、不正被害の類型が紹介された。その後、特に手口の巧妙化と被害の増加が深刻なリアルタイムフィッシング等の詐欺への対策として、同行のスマートフォンアプリを用いた個人向けＩＢ用の当人認証機能「ＳＭＢＣセーフティパス（以下、Ｓパス）」や、お客さまへの注意喚起に関する取り組みが説明された。そのうえで、ＣＢＤＣにおける不正出金対策として、セキュリティと利便性のバランスや、効果的な注意喚起の難しさといった課題が提起された。

- 三井住友カード株式会社より、決済端末を活用したアプリプラットフォーム「stera market」（以下、アプリＰＦ）に関するプレゼンテーションが行われた。

  ―― プレゼンテーションでは、多様な決済サービスや読み取り方式にオールインワンで対応可能な「stera terminal（以下、stera 端末）」及び、stera 端末上で店舗の利便性に資する様々なオペレーション機能を配信

[1] https://www.kantei.go.jp/jp/singi/hanzai/kettei/250422/honbun-1.pdf 参照。

するアプリＰＦについての説明があった。ＣＢＤＣ対応を想定した場合、サーバ接続については、stera 端末として提供するゲートウェイ利用、もしくは独自アプリ開発といった方法別に、機能上の制限事項等の課題が示された。あわせて、ＣＢＤＣ決済の媒体については、あらゆる媒体や読み取り方式に対応することは容易ではない中で、利用者・店舗・事業者等のそれぞれの立場を踏まえて議論・検討していくことが重要であるとした。

３．質疑応答とグループディスカッション

- 株式会社三井住友銀行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）「国民を詐欺から守るための総合対策 2.0」では、詐欺の被害額が 2022 年以降急増しているように見受けられるが、どのような要因及び対策が考えられるだろうか。

（参加者）ＩＢ利用による被害の高額化等が一因として挙げられており、ＩＢの利用限度額の適切な初期設定や、利用限度額の引き上げ時に利用者への確認や注意喚起を行う等の取り組みを推進する方針が示されている。
　こうした状況を踏まえ、当行では詐欺対策の一環として、リスクベースで追加認証を求める仕組みを導入し、被害防止に努めている。

（参加者）生成ＡＩの発展により詐欺メールの巧妙化が著しく、対策レベルの引き上げが必要だと感じている。どのような取り組みを行っているか。

（参加者）当行では、詐欺メールを見分けるポイントの周知をホームページ上で行っているほか、お客さまから問い合わせを受けた際には、身に覚えのないメールは削除を推奨する等の案内を行っている。詐欺メールの巧妙化が進む中、個々の金融機関が対応するには限界があるため、業界全体で協力し、専門知識の共有や情報連携の強化、お客さまへの周知等について、より抜本的な対策の必要性があるだろう。

（参加者）以下、２点伺いたい。①お客さまが生体認証に対応しているスマートフォン端末を持っていない場合は、ＩＤ・パスワード方式による認証に

なるか。②スマートフォン端末が故障し、機種変更を余儀なくされた際は、どのように対応すればよいか。

（参加者）①新規のお客さまには、原則としてセキュリティ強度の高い生体認証方式等の利用を促しているが、生体認証に対応していないスマートフォン端末を利用しているお客さまや既存のお客さまで認証方式の変更を行っていない場合は、ＩＤ・パスワード方式による当人認証が可能である。ただし、その場合でも、高リスク取引の際にはワンタイムパスワード等の追加認証を求める仕組みを導入しており、セキュリティ強度を確保している。

②止むを得ない場合のフローもあるが、原則として、スマートフォン端末の機種変更が必要な場合は、旧端末の紐付け解除を行った後、新しい端末での再紐付けを行う手続きとしている。

（参加者）詐欺等の不正利用被害において、ＩＢ利用のようなネット完結の決済と、ＡＴＭから振り込ませるといったネット以外の決済での被害の比率は分かるか。また、金融機関ごとにセキュリティ対策の状況に差はあるか。

（参加者）不正利用被害における具体的な比率は把握していないが、昨今はオンラインでの詐欺被害にフォーカスが当たっていると認識している。また、セキュリティ対策の状況については金融機関ごとに濃淡がある理解。

（参加者）金融機関にとってセキュリティ強化や詐欺対策への投資については、直接的な投資対効果が説明しにくい側面もあると思うが、どのような考え方で取り組んでいるか伺いたい。

（参加者）デジタル取引が一層普及し、個々の金融サービスでの差別化が難しくなる局面を想定すると、セキュリティ対策の水準が差別化要素としてお客さまに評価される時代が到来する可能性も考えられる。収益に直接貢献する要素としては認識されにくい面もあるが、将来的には重要な要素になり得ると考えている。

（参加者）振込やＡＴＭでの出金等の銀行預金取引において犯罪被害が発生した際には、振込の受け皿口座が自行口座の場合は振り込め詐欺救済法に基づく分配金の支払手続を行い、自行口座からフィッシング等による不正送

金が行われた場合は、全銀協の申し合わせの「預金等の不正な払戻しへの対応[2]」に基づき補償を検討する必要がある。特に後者の場合は、銀行は補償額について自行の損失と評価する他ない。こうした損失を軽減するため、銀行にはセキュリティを強化するインセンティブが働いている。また、銀行は安全安心な社会インフラを担う存在として、利便性をある程度犠牲にしてでも、不正利用の対策を講じるべきと期待されている部分もあると考えている。

- 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）議論の中で、決済サービス利用におけるユーザーサイドの新たなセキュリティ強化策の導入に関する自社内アンケートの結果について共有があった。強化策の導入に後ろ向きな理由として最も多かった意見は、「忙しい」や「面倒」であった。一方、強化策の導入に前向きな理由として最も多かった意見は、「自身や身近で不正利用の被害が発生した、発生しそうになった」であり、当事者としての危機意識を強く持つ出来事が起こったことが背景にあった。また、前向きな理由として「説明がわかりやすい」や「手間がかからない」という意見は全体のわずか５％程度にとどまった。このことから、お客さまへのセキュリティ強化策の利用促進を図る際には、わかりやすさや手間がかからないことをアピールするよりも、例えばアプリログイン時の画面に直近の不正利用発生件数を表示する等によって、お客さま自身に当事者としての危機意識を認識してもらう方法が有効ではないか、との意見があった。さらに、不正利用の被害発生時には「時間がない」「焦っている」といった追い詰められた心理状態による判断能力の低下が原因となるケースも考えられるため、原因分析のうえで効果的な予防策や対応策を講じることが重要だろう、との意見もあった。

（参加者）新たな手法による当人認証システムは、お客さまの慣れやサービスの浸透といった時間の経過とともにネガティブな反応は徐々に減少していくと考えられるが、技術の進歩に伴うセキュリティの陳腐化が懸念されるため、一定の周期で見直しが必要、との意見があった。ＣＢＤＣのセキュリティに関しては、予め３年や５年といった期限を設定し、その期間ごとに適切なアップデートを実施する仕組みを構築してはどうか、との意見もあった。

---

[2] https://www.zenginkyo.or.jp/news/2016/n6389/　参照。

（参加者）ＣＢＤＣにおけるセキュリティ機能について議論を行った。民間企業が提供する決済サービスでは、各社のリスク許容度に応じてセキュリティと利便性のバランスを調整することは可能であるが、ＣＢＤＣの場合は利便性をある程度犠牲にしてでも安全性を優先することが求められるのではないか、との意見があった。ただし、過剰なセキュリティ要件を課した場合、仲介機関としては参入ハードルが高くなってしまう可能性があるうえに、利用者にはかえって仕組みに対する不安感や疑念を生じさせてしまう懸念もある。加えて、セキュリティを厳格にしすぎると、カード型デバイス等の検討・活用が難しくなり、利便性を損なう恐れもある。こうした点を踏まえつつ、セキュリティと利便性のバランスをどのようにとるかが重要なポイントであり、例えば、取引金額に制限を設けることで一定のリスクに抑えつつ、利便性との両立を図るアプローチも対応策の一つではないか、との意見があった。

（参加者）まず、セキュリティ機能の高度化とその利用促進の課題について議論した。Ｓパスのような高度な当人認証への切り替えにより、セキュリティ機能の高度化が図れる一方で、スマートフォンの機種変更時や、ＰＣ等の他端末でログインを試みる場面において、利用者の負担が増えている点は課題である。こうした点も含め、特に高齢者や身体が不自由な方々が利用する際に大きなハードルとなり得るため、簡易なＵＩをどう提供するかは検討事項である、との意見があった。また、位置情報の活用によるセキュリティ強化も考えられるが、プライバシーの懸念について考慮が必要、との意見があった。

次に、お客さまへの注意喚起について議論した。アプリ上で注意喚起の案内を配信する場合、プロモーション情報等の他の案内に埋もれ、肝心の注意喚起が目立たなくなるリスクが指摘された。そのため、利用者が特に意識を向けるタイミング、例えば送金取引時、において重要な情報や警告をポップアップ表示する等の効果的な方法を検討し、セキュリティと利便性の両立を図ることが重要である、との意見があった。

（参加者）各金融機関が不正利用対策に注力しているものの、お客さま自身が騙されてしまう詐欺に関しては、セキュリティ機能の強化だけでは完全に防ぐことは難しい、との意見があった。

クレジットカード業界でも同様にセキュリティ対策を行っているが、不正利用防止のためにお客さまのクレジットカード利用を制限すると、それ

がお客さまの正常な取引だった場合はお客さまや加盟店からの苦情となることも多く、セキュリティと利便性のバランスが難しい、との意見があった。また、クレジットカード会社としては、不正取引が多いと、国際ブランドとの取り決めに従ってペナルティを受ける可能性がある。これらを踏まえると、不正取引のモニタリングやお客さま対応等のバックオフィス業務は重要で残り続けるだろう、との意見があった。

（参加者）新たな手法による高強度の当人認証の導入については、まずはセキュリティに関して問題意識の高い利用者向けに選べるオプションとして提供を始め、利用が進む中で生じ得る課題への対応を行い、対応が一通り整った段階で、一般の利用者も基本的に利用いただくという段階的なアプローチがよいのでは、との議論があった。

ＣＢＤＣが仲介機関の既存決済サービスに組み込まれるとの前提を置いた場合、ＣＢＤＣのリスクが仲介機関の既存決済サービスよりも低ければ、既存の決済サービスの認証強度で十分である。一方で、ＣＢＤＣのリスクが仲介機関の既存決済サービスよりも高い場合や、一段高い認証強度を求められるような場合では、仲介機関は認証強度を個別にあげなくてはならない可能性があり、対応することは簡単ではない、との意見があった。

- 三井住友カード株式会社からのプレゼンテーションを受けて、参加者による質疑応答を行った。議論の概要は以下の通り。

（参加者）アプリＰＦにて提供されているアプリについて、具体的な内容を教えてほしい。

（参加者）例えば、小規模な店舗向けにＰＯＳ機能を提供するアプリでは、stera 端末のみでＰＯＳ操作と決済を一元的に完結させることができる。また、免税販売時の電子化手続きをサポートするアプリでは、stera 端末に搭載されているカメラを用いてＯＣＲ技術でパスポート情報を読み取ることが可能である。このように、アプリは店舗のオペレーションに必要な機能の提供や、業務の効率化を図る機能を提供している。

（参加者）stera 端末やそのアプリにおけるセキュリティ上の留意点を教えてほしい。

（参加者）カード情報の漏洩防止が重要である。stera 端末はカード情報を暗号化し、ネットワーク上で復号できない仕組みを採用した端末として第三者機関の認証を受けている。また、カード情報を復号できるのはサーバ側のみであり、ＰＯＳアプリを含む端末上のアプリ自体は基本的に暗号化されたカード情報を処理することはない。そのため、アプリは決済に関わる情報から独立したレイヤーに位置付けられている。アプリそのもののセキュリティ水準については、基本的にはアプリＰＦを運営する三井住友カード株式会社の審査を通過したアプリのみがアプリＰＦ上で配信されるため、一定のセキュリティを確保できている。

（参加者）決済端末が読み取る媒体としては、物理カードやＱＲコード、生体認証等様々ある。例えば、ＮＦＣの規格においては Type-A や Type-F は利用が多く、Type-B は比較的少ないとの認識であるが、足元ではどのような媒体・規格が利用されているかについて動向を教えてほしい。

（参加者）統計を取ったわけではないが、ＮＦＣの規格の利用動向はご認識のとおり。また、最近では自社 Pay 利用時や独自ポイントの付与時にスマートフォンアプリでＱＲコードを表示することが増えたために、ＱＲコードの読み取り機会が増えている。なお、独自ポイントについては、費用のかかる物理カード発行からのスマートフォンアプリへの移行が進んでいることが背景に考えられる。

（参加者）ＣＢＤＣを用いた決済を stera 端末で行ったと仮定した場合、「stera connect」のゲートウェイサーバにおいて、適切な宛先のＣＢＤＣの仲介機関のサーバに電文を振り分けることは論理的に可能か。

（参加者）「stera connect」のゲートウェイサーバに電文を振り分ける機能はあるが、実際にはＣＢＤＣと仲介機関の仕様によるため現時点での回答は難しい。ただし、論理的には、仲介機関側でゲートウェイサーバとの接続仕様を適切に設定すれば接続できるものと認識している。

（参加者）決済操作ごとに stera 端末のディスプレイでＱＲコードを表示するといったようなＭＰＭ方式も考えられるところ、現状では対応していない理由について、例えば利用ニーズが乏しい、もしくは何らかの制約のため対応していないなどがあれば教えてほしい。

（参加者）ＭＰＭ方式の利点は、ＱＲコードを表示したポップアップを置くだけで設置が完了するために、圧倒的な低コストで提供できる点にある。こうした点を踏まえると、店舗側としてはシステム開発費用を負担してまで決済端末でＭＰＭ方式を実現することのメリットは少ない。また、お客さまがスマートフォン等を決済端末に提示するケースを考えた場合、お客さまも店舗側も利便性がより高いと考えられるＣＰＭ方式で処理すべきと考えられ、stera 端末では基本的にはＣＰＭ方式を提供している。

- 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）ＣＢＤＣに関してどのような媒体を用意することが望ましいかというディスカッションポイントについては、物理カードやデジタル媒体等それぞれセキュリティ基準が異なるため対応は大変であるが、あらゆる媒体に対応するのであれば、バリューの管理はセンターサーバで行う形になるのでは、との議論があった。また、ゲートウェイサーバからＣＢＤＣ関連のサーバへ電文を飛ばす場合、ＣＢＤＣ関連のサーバに直接電文を飛ばすのではなく、振り分けを行う事業者が間に入って処理していく方が良いのでは、との意見があった。

（参加者）ＣＢＤＣの決済利用時に当人認証を行うとすれば、本人を特定した形で利用の記録が残る可能性があることから、ＣＢＤＣの利用を躊躇する利用者が生じ得る。そのため、ＣＢＤＣの媒体としては無記名式の電子マネーのように個人が特定できない匿名の形で利用できる方がよいのでは、との議論があった。この場合、例えば端末を落としたときなど、不正利用のリスクは増加することになるが、現状のクレジットカードや電子マネー、デビットカード等の対応を参考に考えていくべき、との意見があった。また、運営上セキュリティは重要であるものの、店頭決済の場合は利用者や店舗側もスピード感をもって手軽に利用できることが大事であるため、こうした点も考慮いただきたい、との意見があった。

（参加者）媒体は基本的に幅広く対応する必要があるだろうとの想定のもと、決済利用時の上限額については、媒体ごとのセキュリティ水準や当人認証の有無に応じて個別に検討する必要がある、との議論があった。

（参加者）あらゆる世代の人々や現金しか利用できていない人々でも利用でき

ることがＣＢＤＣの意義のひとつだとすれば、マイナンバーカードを含めて幅広い媒体を用意する必要があるだろう、との議論があった。また、ＣＢＤＣの運営を考えた際には、サーバの運営者のあり方やネットワークの利用に伴うトランザクションコストの発生についても考慮する必要がある、との意見があった。

（参加者）日本におけるＣＢＤＣの具体的なユースケースが定まっていない中、今回のディスカッションポイントでは日常の店頭決済での利用を前提とされたため、まずは海外ではどのようなユースケースを想定しているかについて言及がされた。海外では、同様に日常での利用を想定されているが、その理由としては、①紙幣の利用には限界がありデジタル通貨へシフトする必要性が高まっていること、②決済インフラを自国以外の事業者に依存している場合は経済安全保障上の問題が生じ得ることなどの問題意識から、自国の事業者が決済インフラを運営し、当該インフラが自国のコントロール下にあることが重要との考えがあるという２点であると認識している。こうした国としての必要性のもと、ＣＢＤＣ用の媒体の発行にかかる費用やセキュリティを担保するための費用を誰が負担すべきかについて議論が及んだ。これまで明らかにされた仲介機関の役割を踏まえると、ＣＢＤＣの利用者への対応やその運営の多くを仲介機関が担うことになると理解しているが、民間企業である仲介機関にとっては、そうした対応に費やす費用をまかなうだけの収益を、ＣＢＤＣを取り扱うことによって稼げるかは懸念事項であり、仲介機関としてＣＢＤＣを取り扱うことによる収益と費用のあり方については今後の検討課題である、との意見があった。

（日本銀行）本会合はＷＧ３とＷＧ５の共同開催ということで、安全性と利便性というトレードオフ関係に立ち得る論点について、それぞれ専門性を有する参加者間でのご議論を通じて議論が深まったように感じている。セキュリティ強化に向けた取り組みが利用者に受け入れられ、広がっていく仕組みづくりの重要性などについて、今後も議論を深めていければと思う。

４．次回予定

次回のＷＧ３会合は未定。ＷＧ５会合は 2025 年 12 月９日（火）開催予定。

以　上