2025 年９月 30 日
日本銀行決済機構局

ＣＢＤＣフォーラム ＷＧ５
「ユーザーデバイスとＵＩ／ＵＸ」
第９回会合の議事概要

１．開催要領

（日時）2025 年 7 月 14 日（月）14 時 00 分～16 時 30 分
（形式）対面形式及びＷｅｂ会議形式
（参加者）別紙の通り

２．プレゼンテーション

- ＮＲＩセキュアテクノロジーズ株式会社より、既存のキャッシュレス決済から考えるＣＢＤＣのセキュリティ評価と制度設計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、ＣＢＤＣにおけるセキュリティ考慮事項（特にＵＩ／ＵＸ関連）について検討を深めるため、クレジットカード業界におけるセキュリティ基準（ＰＣＩ ＤＳＳ[1]をはじめとしたＰＣＩ基準）の概要が紹介された。具体的には、①対面決済を例とした、店舗・決済端末メーカー・決済処理センター・プロバイダー等に適用される各ＰＣＩ基準の概要とそれらの補完関係、②技術動向への対応、③審査ルールや審査品質を維持するための審査員認定プロセス等が説明された。そのうえで、ＣＢＤＣのセキュリティ評価の制度設計の際には、既存の評価制度や基準等を参考にしながらも、ＣＢＤＣ特有のセキュリティ上の論点やそのＵＩ／ＵＸ上の課題について、可能な限り、構想段階から議論し明確化することが望ましいとした。

- 株式会社日立ソリューションズ・株式会社日立コンサルティングより、ＣＢＤＣにおける生体認証の活用検討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、ユニバーサルアクセス、セキュリティ、強

[1] PCI DSS は、Payment Card Industry Data Security Standards の略。PCI SSC によって策定されたクレジットカード業界におけるグローバルなセキュリティ基準。

靭性の観点での社会課題解決案の一例として、ＰＢＩ技術[2]を用いたクラウド型の生体認証サービスプラットフォームの事例が紹介された。同サービスプラットフォームでは、予め生体情報（顔や指静脈）とクレジットカードを紐づけておくことで、「手ぶら」で決済することが可能。利用者からは、「圧倒的に便利」、「荷物がある時に楽」など、ポジティブな意見が多い一方、認証した情報の漏洩への不安の声もあること等が紹介された。

３．質疑応答とグループディスカッション

- ＮＲＩセキュアテクノロジーズ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。

（日本銀行）今回は、「誰でも、どこでも、幅広い状況下で」使えるために、といったこれまでのテーマの枠にとらわれず、セキュリティの文脈でＣＢＤＣのＵＩ／ＵＸを議論したい。

プレゼンテーションでご説明があったように、情報保護対策（漏洩対策）と不正利用防止対策の２つの観点で、店舗決済に関わる様々な事業体ごとに求められる要件を踏まえながら、決済サービス全体で不備がないようセキュリティ対策を整備していくことの難しさを改めて認識した。

店舗における情報保護対策として、ＰＣＩ ＤＳＳ準拠と非保持化対策があるとのことだが、その適用の考え方について教えていただきたい。

（参加者）情報保護対策と不正利用防止対策について、グローバル基準であるＰＣＩ ＤＳＳはクレジットカード情報の保護対策に主眼が置かれており、国内においては、クレジット取引セキュリティ対策協議会のクレジットカード・セキュリティガイドラインにおいて、ＰＣＩ ＤＳＳ準拠も含めた情報保護対策と合わせて、不正利用防止の観点からも必要な対策が整備されている状況。

ＰＣＩ ＤＳＳで保護対象とする情報は、ＰＡＮ（プライマリーアカウント番号）と呼ばれる会員番号、それに紐づく有効期限、会員名、セキュリティコードや暗証番号、フルトラックデータ（磁気ストライプデータまたはＩ

[2] PBI は、公開型生体認証基盤 Public Biometric Infrastructure の略。生体情報を復元不可能な形に変換し、「公開鍵」として安全に利用することで、プライバシーの保護と高度なセキュリティを両立する生体認証基盤。

Ｃチップ上の同等データ）等。国内では、これらの保護対象情報を自社の機器・ネットワークで保存・処理・通過しないような非保持化の仕組みを採用している店舗は、ＰＣＩ　ＤＳＳの準拠は任意となる。もっとも足許では、非保持化を採用しているＥＣ店舗のサイトにおいて、Ｗｅｂスキミング等のサイバー攻撃による情報漏洩インシデントが問題視されていることから、クレジットカード・セキュリティガイドラインにおいては、保持・非保持にかかわらず、Ｗｅｂサイト等の脆弱性対策を求めている。

（参加者）ＰＣＩ　ＳＳＣで定めているセキュリティ基準には、クレジットカードの非接触ＩＣ・接触ＩＣ・磁気といった読み取り種類の選択とＰＩＮ入力等の決済時の認証方法の切り替え要件に関する仕様も含まれるか。例えば、ＰＣＩ基準がバージョンアップするごとに、店舗端末や決済処理システム等のハードウェアに対する変更要求となってしまうと、店舗にとっては負荷が大きい。

（参加者）決済時の端末処理の技術要件に関しては、ＥＭＶ[3]の仕様によるものだが、ＰＣＩ基準によるハードウェア変更への影響といった観点では、例えば、決済端末メーカーに対するＰＣＩ　ＰＴＳという認定がある。ＰＣＩ　ＰＴＳはバージョンごとに有効期限が設けられており、最新バージョンほど、最新のセキュリティ対策が備わっていることになる。ＰＣＩ基準については、セキュリティ脅威の変化を反映し、引き続きバージョンアップや新しい基準の策定が続いているものの、今後、ＰＣＩ　ＳＳＣでは要件の統合や整理等、スリム化を目指す動きもある。

（参加者）様々な新しい脅威に対応してセキュリティ基準をアップデートしているとのことだが、基準を厳しくしていくと、ＵＩ／ＵＸの低下につながるというコンフリクトへは、どのように対処しているか。

（参加者）セキュリティとＵＩ／ＵＸとのコンフリクトの分かりやすい例として、例えば、クレジットカード・セキュリティガイドラインにおけるＰＩＮバイパスの運用廃止が挙げられるだろう。対面決済時の当人認証のための４桁ＰＩＮについて、利便性の観点からは、ＰＩＮをバイパス（省略）してサインでも決済できる方が望ましいが、不正の温床になり得ることから、セ

[3] Euro pay International, MasterCard International, 及び VISA International の間で合意した、金融・決済分野における IC カードと端末に関する仕様を定めた標準。

キュリティの観点からは、ＰＩＮ入力必須が望ましいという考え方となる。国内では、まず 2020 年に、磁気カードからＰＩＮ機能があるＩＣカードへの移行が完了し、利用者の動向をみながら、約５年を経た今年から、ＰＩＮバイパスについても運用廃止となった経緯。

（参加者）ＰＣＩ ＭＰｏＣ（スマートフォン決済端末向けサービスプロバイダーを対象としたＰＣＩ基準）は、利便性を考慮して、決済端末に対するセキュリティステータス検証の要件をオフライン環境向けに緩和したとのことだが、その手当としてのリスク低減の要件があればお伺いしたい。

（参加者）スマートフォン決済端末のオフラインモード継続時間の上限や、オンライン復帰後の初回は特定の監視サーバーに接続して検証する等の要件を設けている。

（参加者）ＰＣＩ ＤＳＳでは対象となる事業体や店舗に対して、年次審査や３ヶ月ごとの脆弱性スキャン等を実施しているとのことだが、リテール決済は特に関連する事業体の業態の種類や全体数も多く、セキュリティ基準が十分に機能するよう中長期的に実効性を確保する仕組み作りには、難しさがあるのではないか。

（参加者）まず、前提として、ＰＣＩ基準では、組織的なセキュリティ方針の策定等、対象企業が、継続的にセキュリティ基準を遵守して運用できる態勢を整備しているかを審査している。審査会社の立場としては、例えば、ＰＣＩ基準には大きな変更が発生した際の変更管理に関する要件があるが、実際の変更の規模や変更箇所による影響分析も含めて、形式的な評価とならないよう実効性のある審査を大事にしている。

（参加者）別の観点では、審査会社と審査を受ける事業体との関係性も実効性確保のために重要。ＰＣＩ ＳＳＣでは、「審査会社の独立性の確保」や、国際ブランドの中でも特定のＰＣＩ基準について「２年ごとに審査会社を変更する」等、様々な決まりを定めている。ＣＢＤＣにおいても、そういった牽制機能を検討する必要があるかもしれない。

また、特に加盟店は、大企業から中小企業も含めて非常に裾野が広く、当然にセキュリティにかけられる予算も異なる。ＰＣＩ ＤＳＳでは自己問診できるプログラムも用意しているが、知見やリソースの限界もあって、多くの店舗は非保持化を選択する傾向にあり、前述のＷｅｂスキミング等の情報

漏洩リスクにつながっている。

（参加者）店舗による不正利用防止対策の実施は、万が一不正利用が起きた場合の補償の考え方にどのように影響するか。

（参加者）例えば、ＥＣ店舗がＥＭＶ３Ｄセキュア[4]を導入していれば、ブラックマーケット等で出回っているような漏洩したカード情報等を用いた決済が発生しても、通常、店舗側が負うチャージバックをカード発行企業が補償する仕組みになっている。最近では、ＥＭＶ３Ｄセキュアを突破するリアルタイムフィッシングが増えており、不正利用防止対策の観点で、大規模なＥＣ店舗をはじめとして、追加的に属性・行動分析による不正検知等を実施している。

- 株式会社日立ソリューションズ・株式会社日立コンサルティング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）デバイスを必ずしも必要としない決済手段は、ユニバーサルアクセスはもちろん、特に災害時におけるレジリエンスの観点で重要であって、また、省力化が社会課題として求められていく中でも有用なアプローチとも思われる。

質問だが、生体認証サービスプラットフォームに紐づけ可能な決済サービスに制限はあるのだろうか。また、顔認証と指静脈認証について生体認証情報の更新頻度はどのように定めているか。

（参加者）現状は、クレジットカードとポイントサービスのみの対応であるが、技術上はオンライン決済であれば基本的には対応可能であって、今後さらに拡大していく予定。

生体認証情報の更新頻度については、顔情報は経年変化があるものの、指静脈は、成人以降は変化せず、基本的には大きな怪我等がない限り、一度登録すれば更新の必要はない。将来的には、例えば顔認証であれば、毎回店舗で顔認証する際に、利用者の同意のうえで、最新の顔情報にアップデートし

[4] オンラインショッピング時にクレジットカード番号等の情報の盗用による不正利用を防ぎ、安全にクレジットカード決済を行うために国際ブランドが推奨する本人認証サービス。

ていくような方法が技術的には可能となると思われる。

（参加者）生体認証サービスを利用開始する際には、一旦対面で本人確認書類の確認を実施後に生体情報を登録するといった手続きが必要とのことだが、足許では、本人確認書類のデジタル化や携帯のカメラ等での生体情報の登録等、オンラインで完結するケースもあるように思う。それらを活用してさらに効率化することは可能なのだろうか。

（参加者）本人確認書類の活用による効率化は技術的には可能だが、民間サービスであるため、制度上の検討課題は多くある認識。また、特にご高齢の利用者は、登録の際に必要な情報の入力にも不慣れな場合が多く、対面での丁寧なサポートの提供が必要となっている。

（参加者）生体認証サービスプラットフォームは、ＣＢＤＣシステムにおける追加サービスの位置づけと整理できるだろう。

より確からしい認証とするために、生体認証以外の情報も確認するのだろうか。その場合は、情報取り扱いの観点で課題が増えるかもしれない。

指等の静脈認証に関しては、過去に、銀行ＡＴＭにおけるキャッシュカードを用いた取引時の追加の認証方法として注目されていた時期があったが、結果として、広く普及しなかったと理解しており、どのような課題があったのだろうか。

（参加者）生体認証以外の追加情報としては、電話番号がある。これは利用者が忘れてしまったり、運用が難しいといった心配が少ない。

銀行ＡＴＭでの静脈認証については、磁気併用型ＩＣキャッシュカードのスキミングリスク等に対するセキュリティ強化を目的に導入された経緯。ＡＴＭ取引時において、通常のキャッシュカードと暗証番号による認証に加えて、静脈認証を必要としたものだが、あまり利便性が高くなかった。最近では、セブン銀行がキャッシュカード不要な顔認証によるＡＴＭサービスを開始する等、セキュリティ強化というよりも、利便性向上を目的とした生体認証の活用が検討されている。

- 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）店舗決済端末へのＰＩＮ入力時の覗き見対策の要件について、テンキ

ー周辺のプライバシーシールドの設置要件が店舗決済端末によって異なるケースや、ハードではなくソフトウェア側で対策が実装されているケース等、ＰＣＩにおけるルールや考え方について議論がされた。

続いて、オフライン決済への対応については、スマートフォン決済端末における情報保護や、決済時の不正利用防止等の様々なセキュリティ観点が相互に関連しているという話があった。

最後に、ＣＢＤＣのセキュリティ評価基準の策定については、汎用的なセキュリティの考え方に基づいているＰＣＩ　ＤＳＳが参考になる一方、ＣＢＤＣの特徴を踏まえた検討は必要になるだろうという意見があり、また、策定主体は、監督官庁や業界団体等、様々に考えられるという意見があった。

（参加者）民間デジタル決済手段とは異なるＣＢＤＣの特性を踏まえながら、どのようにセキュリティと利便性を両立していくかという観点で議論がされた。例えば、オンボーディングや決済時の本人確認に関して、整理すべき論点は多いなか、特にマイナンバーカードやクレジットカードの認証等、既存の仕組みの活用について検討すべきとの意見があった。また、ＣＢＤＣ決済における不正利用発生時の補償については、自己責任となっている現金と同様の考え方を基本とすべきとの観点や、利用者の理解と日本銀行の役割といった観点、さらには、ＰＣＩのように、ＣＢＤＣに関しても国際ルールが定められるのであれば、それらを踏まえた議論・検討が可能ではないか、といった意見があった。

（参加者）まず、クラウド上の生体認証関連情報について、基本的には、リージョン指定での保管・利用になっていると考えられるところ、海外旅行時の決済のために一時的に開放するといったユースケースに応じた対応について議論がされた。

また、店舗にとっての生体認証を導入するモチベーションについては、生体認証の読み取り装置等の設備投資が必要になる可能性はあるが、セキュリティが向上することで、店舗が負担する決済手数料の減額への期待感はあるのではないかといった意見があった。一方で、対面環境（顧客が来店）であっても、あらかじめセンターに登録されたカード情報を利用して決済する対面ＥＣスキームの場合、ＥＭＶ３Ｄセキュア実施は生体認証登録時のみとなり、イシュアによる認証が行われていないため、期待されたほどのセキュリティ向上が得られない可能性がある点やそれを踏まえた補償のあり方についても議論がされた。

（参加者）クレジットカード決済の枠組みにおいては、不正利用時のリスク分担とそれに対するセキュリティ対応のインセンティブが明確に整理されている。ＣＢＤＣ決済において、それらがどのように設計されるか次第で、店舗側のモチベーションも変わってくるだろう、といった議論があった。

生体認証サービスについて、ローカル型であれば支払いを行う利用者のスマートフォンで対応できるが、クラウド型において、静脈や顔といった各種生体認証用の読み取り装置を取り揃えることは現実的ではなく、例えば、最低限、モバイルデバイスのカメラ機能で対応できるのか、といった議論があった。

（日本銀行）本日の議論では、既存のリテール決済のエコシステムの奥深さや、ユニバーサルアクセスの観点から新しい技術の可能性を感じることができた。一方で、様々な論点もご指摘いただき、将来の技術進歩や社会の変化を見据えながら、ＣＢＤＣエコシステムを考えていくべき、という課題をいただいたと考えている。

本日の会合でセキュリティの観点からＵＩ／ＵＸを議論したように、ＷＧ５で取り扱っているＵＩ／ＵＸというテーマは、他のＷＧの議論とも関係してくることから、今後、他のＷＧの参加者もまじえて議論できる体制も検討していきたい。

４．次回予定

次回の会合は９月 22 日（月）に開催。

以　上

別紙

ＣＢＤＣフォーラム ＷＧ５
「ユーザーデバイスとＵＩ／ＵＸ」
第９回会合参加者

（参加者）※五十音アルファベット順
キャナ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
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
株式会社日立コンサルティング
株式会社日立ソリューションズ
日立チャネルソリューションズ株式会社
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
株式会社みんなの銀行
株式会社りそなホールディングス
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
Ridgelinez 株式会社
ＴＯＰＰＡＮエッジ株式会社

（事務局）
日本銀行