2019.08.29 (nl2019.14)

Newsletter

Institute for International Monetary Affairs
公益財団法人 国際通貨研究所

我が国のキャッシュレス（QR コード決済）に関する一考察

～「7pay（セブン・ペイ）」の不正アクセス問題を受け～

公益財団法人 国際通貨研究所
経済調査部　主任研究員
志波 和幸
kazuyuki_shiba@iima.or.jp

はじめに

2018 年 4 月に経済産業省が発表した「キャッシュレス・ビジョン」[1]では、前年の「未来投資戦略 2017」で設定したキャッシュレス決済比率目標（40%）の達成時期を 2027 年から大阪・関西万博が開催される 2025 年に 2 年前倒しした[2]。また、今年 10 月の消費税増税の需要平準化対策として、キャッシュレス対応による生産性向上や消費者の利便性向上という観点も含め、中小・小規模事業者によるキャッシュレス手段を使ったポイント還元等を支援する事業が推進されている。

こうしたなか、キャッシュレス決済の手段の一つとして、最近ではスマートフォンを介した「QR コード決済」に関するキャンペーンや宣伝が目につく。これは、前述の消費税増税により少額決済方法が現金からキャッシュレスに移行するとの推測に加え、今年 9 月のラグビー・ワールドカップや来年夏の東京オリンピック・パラリンピックに向けた外国人観光客の取り込みの一環として小売店側が興味を示していることが背景にあろう。2018 年 11 月の株式会社日本能率協会総合研究所の報告書[3]によると、日本国内

[1] 詳細は https://www.meti.go.jp/press/2018/04/20180411001/20180411001-1.pdf をご参照。

[2] 2019 年 6 月に「成長戦略フォローアップ」が実施され、2018 年時点のその比率は 24.1%であると発表された。

[3] 詳細は http://search01.jmar.co.jp/static/mdbds/user/pdf/release_20181107.pdf をご参照。

の QR コード決済市場規模は2019年度の6,000億円から2023年度には8兆円規模に急成長すると予測している。

しかし、今年7月にセブン&アイ・ホールディングスが導入したスマホ決済サービス「7pay（セブン・ペイ）」で発生した不正アクセス問題は、QRコード決済のみならずキャッシュレス決済全体に対する安全性・信頼性に水を差し、一部から「キャッシュレス決済の停滞」を懸念する声が出た。

本稿では、7payで発生した問題点を洗い上げるとともに、今後のQRコード決済市場の動向について考える。

１．「７Pay」不正アクセス問題の経緯

7payは、2019年7月1日に大手コンビニチェーンの「セブンイレブン」約21,000店舗の店頭で使用開始となったスマホ決済（コード決済）サービスである。同日に運用を開始した「ファミペイ」[4]とともに、スマホ決済市場にコンビニチェーンも本格参入したものとして話題となった。

利用者からみた7payでの支払いのメリットは（現金での支払いと比べ）、①財布の持ち運びが不要となること、②その決済を使用することにより割引クーポンが発行されること、③利用金額に応じて nanaco（電子カード）ポイントが付与されること[5]、等が挙げられる。一方、店舗側のメリットとしては、①現金管理の減少による決済事務の短縮化・効率化、②7pay 利用者の購買履歴データの取得（長期的にはそれらのデータを分析し将来の消費行動予測への活用を目指す）、が挙げられよう。こうしたなか、利用開始日前日から配信された7payアプリをインストールした利用者は150万人に達した。

しかし、その利用開始日翌日の7月2日には7pay利用者から「身に覚えのない取引がある」旨の問い合わせがあり、社内調査の結果翌3日に「不正アクセス」があったことを発表し、同日中にクレジットカード／デビットカードからのチャージを停止した。そして7月4日に緊急記者会見が開催され、7payの運営会社（株式会社セブン・ペイ）の社長が謝罪するとともに、全てのチャージ機能を停止した。その後、同社はセキュリティ体制強化によるサービス再稼働を試みた模様であるが、結局9月末に全面停止する

[4] ファミリマート店頭で使用可能のスマホ決済（コード決済）サービス。全国のファミリーマートおよそ17,000店で利用できるほか、「Kaema（カエマ）」というネットショップでも利用可能である。

[5] 2019年6月まではセブンイレブンでの支払いにnanaco（電子カード）決済を用いると100円ごとに1ポイントを付与していた。しかし、7pay開始に伴い、nanaco支払いでのポイント付与は「200円ごとに1円」に変更された。これは、店舗側としてはnanaco決済よりも7pay決済のほうがより詳細な個々人の取引データを取得することが可能であり、後者への移行を進めるための施策と思われる。

こととなった。

図表 1 ： 7pay 開始（7 月 1 日）からその終了（9 月末予定）までの動き

日付	内容
7月1日	7pay（QRコード決済）のサービス開始（登録者数：150万人） （運営業者：（株）セブン・ペイ）
7月2日	夕方、7pay利用者より「見に覚えのない取引があったようだ」との問い合わせがあり。 （会社談：早朝から数千万回のアタック（試行）があり） 時同じくして、TwitterなどのSNSに「不正チャージ／不正利用」の報告が上がり始める。
7月3日	社内調査の結果、「不正アクセス」が発覚。 ・お客さまサポートセンターが「緊急ダイヤル」を設置。 ・7payホームページの「重要なお知らせ」欄にID・パスワード管理の注意喚起を掲載。 ・クレジットカード及びデビットカードによるチャージを停止 （店頭での現金チャージ／ATMからのチャージは引き続き可）。
7月4日	詐欺未遂の疑いで犯人（中国籍男性2人）を逮捕（たばこ「20万円」相当を購入未遂）。 ⇒ただし、「受け子」の模様（主犯ではなさそう）
7月4日	【セブン＆アイ・ホールディングス】 緊急記者会見を開催。（株）セブン・ペイの小林社長らが謝罪。 ・午前6時点の不正アクセスの被害者数：約900人／被害金額：約5,500万円。 ・TwitterやFacebookなど外部IDからのアクセスを遮断。 ・7payの新規登録を停止。 ・全てのチャージ（クレジットカード、デビットカード、店頭での現金、ATM）を停止。 ・海外からのアクセスを遮断。
7月5日	【経済産業省】 ・今回の不正アクセス問題において「7pay」がキャッシュレス推進協議会が策定した 「不正利用防止のための各種ガイドライン」を遵守していなかったことを指摘。 ・決済事業者各社対し不正利用防止のための各種ガイドラインの遵守を求めるとともに、 最新情報の収集と対策の見直しでセキュリティレベルの向上に努めるよう促す。
7月16日	【セブン&アイ・ホールディングス】 ・現時点の確定被害は1574人、総額3,240万688円と公表。 ・7月中に対策を公表する旨発表。
7月30日	パスワード一斉強制リセット リセットされたパスワードは「7pay」アプリのみならず、「7iD」（※）に紐付けされている全ての アプリケーション。（それらのアプリのパスワードを再設定する必要がある。） ※「7iD」に紐付けされているアプリ（対象者1,650万人） ：7payアプリ、omni7（7&アイ系のネット通販）、セブン-イレブンアプリ、イトーヨーカドー アプリ、西武・そごうアプリ、アカチャンホンポアプリ、ロフトアプリ
8月1日	【経営陣の記者会見】 ・不正アクセスの被害者数：807人／被害金額：3,860万5,335円。 ・7月中旬以降は新たな被害は確認できていない。 ・7payサービスを9月末に全面停止する。
8月12日	【新聞報道】 金融庁はキャッシュレス送金・決済を手がける資金移動業者を対象に、立ち入りを含めた 集中検査を開始。不備が見つかれば行政処分を検討も。
9月末	7payに関する全てのサービス停止（予定）

（各種資料より国際通貨研究所が作成）

２．7pay のシステム上の問題点

それでは、7pay のどこにシステム上の問題点（セキュリティーホール）があったのだろうか？一連の記者会見／会社発表の内容と「IT 専門家による各種報告」から、大きく以下 4 点があったものと推測される。

(1)「パスワードの再設定機能」の不備（その１）

利用者が 7pay のパスワードを失念した場合、その再設定には「①生年月日」、「②登録済の（スマホの）電話番号」、「③登録済の会員 ID」の 3 項目が合致する必要があるとされていた。

ところが実際は、新規登録時に「①生年月日」は登録必須項目ではないこと。そして、「生年月日を未設定」にした場合は「2019/01/01」にデフォルト設定されていた。

そこで、ハッカーは、

１）事前に何らかの方法で 7pay の「会員 ID」のリストを不正入手し、

２）個々の ID に対し、「携帯電話番号の数字 8 桁×2（080 と 090）の総当たり」攻撃を実施（その際、生年月日は「2019/01/01」と入力。）[6]

した結果、新規登録時に「生年月日を未設定」にした ID のなかにパスワード再設定が可能となったものがヒットした模様である。

(2)「パスワードの再設定機能」の不備（その２）

パスワードの再設定申請をした際、それが真に本人からの申請であることを確認するため、通常だと事前登録したメールアドレスに照会が入る。更に、該当メールアドレスに暗証番号・文字が自動送信され、その番号・文字を「パスワード再設定画面」の指定個所に入力しないと申請を受け付けない仕組みにしているシステムもある（これを「2 段階認証」とも呼ぶ）。

ところが 7Pay の場合、「パスワード再設定画面」の「送付先メールアドレス」に任意のメールアドレスを再登録することが可能であったうえ、既に登録済のメールアドレスに「メールアドレスが変更された」旨の通知はされていなかった。

[6] これらハッカーの一連の動きは「リスト攻撃」と呼ぶことがある。なお、この時 7pay 側には、攻撃が一定回数失敗した場合に入力が一定期間できなくなる等の「ロック」機能も有していなかった模様である。

図表 2 ： 7pay のパスワード再設定画面

新規登録時に「①生年月日」の登録は必須ではなかった。
（登録しなかった場合、システムが「2019/01/01」と自動設定）

そこで、ハッカーは「③会員 ID」を不正入手したうえで、
①生年月日を「2019/01/01」と入力
②登録電話番号をランダムに入力
し、パスワード再設定が可能なものを探り当てた。

パスワード再設定可能となったものについて、「④送付先メールアドレス」を変更。（変更の際、登録済メールアドレスには変更通知はされなかった）

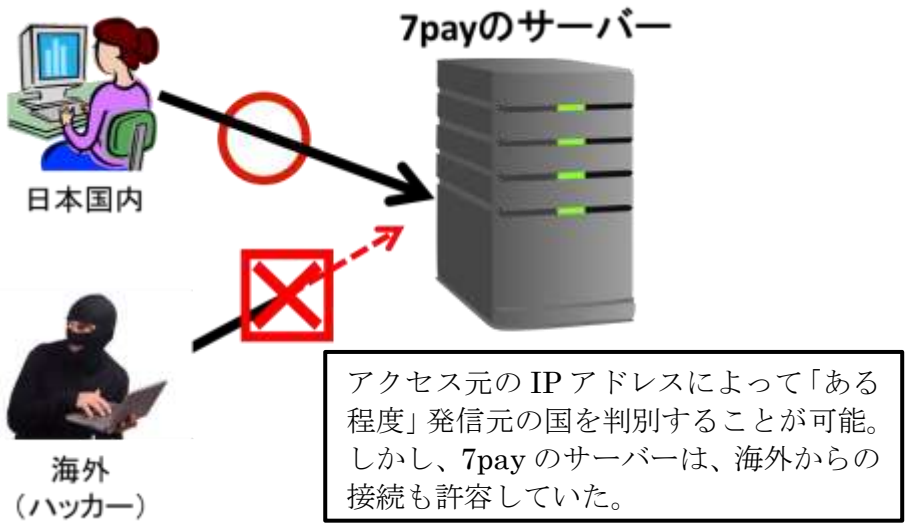
(3)「外国 IP アドレスからの通信（攻撃）」をブロックしていなかった

7pay は 7 月 1 日のサービス開始時点では「国内のセブンイレブンの店舗」のみで使用可能となっていた。その後、順次取り扱い開始店が発表される予定であったが、いずれも国内での決済を前提としたものと思われる。

その場合、セキュリティ対策の一環で「アクセス元が『明らかに』海外のものはサーバーと接続させない」との設定をすることが可能であるが、「7pay」のサーバーにはその設定がされていなかった。

そのため、今般の海外からの不正アクセスを許容してしまった模様である。

図表 3 ： 7pay のサーバーへのアクセス方法図（概要）



（4）「omni7」のプラットフォームに 7pay を上乗せしていた。

7pay は決済手続きを取り扱うアプリケーションに付、本来ならば他のサイトやアプリケーションと分離し、よりセキュリティが強いシステムを構築する必要がある。しかし、同サービスはセブン&アイ系の総合通販サイト（omni7）のプラットフォームに乗せる形で開発された[7]。

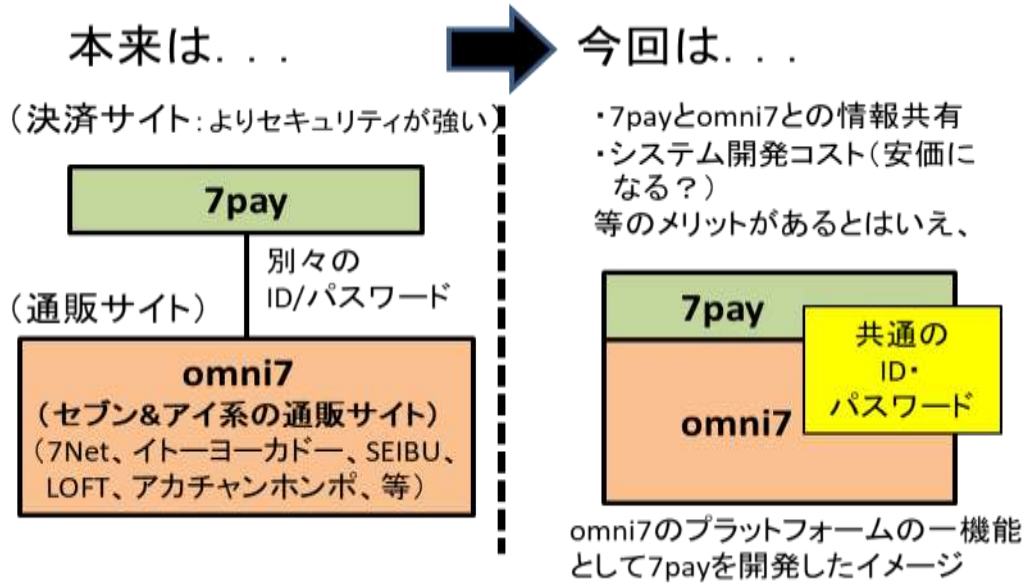
この開発方法は、7pay で取得した情報と omni7 で取得した情報を共有しやすいうえ、7pay のアプリケーションを総じて安価に開発できるなどのメリットがある一方、セキュリティ管理体制が概して脆弱である総合通販サイト（omni7）の ID／パスワードを共同使用することから情報が漏洩するリスクがあった。そして、実際にそれが漏洩したことにより 7pay の利用者に多大なる迷惑をかけることになった[8]。

---

[7] 実際、上掲図表 2 の「7pay のパスワード再設定画面」の左上に omni7 のロゴがあることからも、7pay が omni7 のプラットフォームの上で開発されたことが見て取れる。

[8] この件について、岩下直行京都大学公共政策大学院教授のコメントを以下掲載する。
「今回の 7Pay 事件の本質は、7Pay というスマホ決済を独自に作ったのではなく、既存の「omni7」の ID やパスワードやメールアドレスが 7Pay と共用されているのだから、決済システムとしてのセキュリティが弱くなるのは当然だ。
（中略）
150 万人の 7Pay 利用者の多くは、スマホから新規に会員登録したと思われるので、そもそも omni7 と認証情報が共有されていることすら知らないだろう。」

図表 4 ： 7pay と omni7 との関係（イメージ図）



図表 5 は以上の問題点を図示したものである。これらの問題点のうち 1 つでも事前に解決していれば不正アクセスは大幅に減少していたものと推測される。

図表 5 ： 7pay 不正アクセスの全体図（予想）

【主な被害内容】

・7pay と紐付けているクレジットカード／デビットカードから見知らぬ決済がある。

・自分の 7Pay に見知らぬ金額がチャージされている。知らない購入履歴がある。

（岩下直行京都大学公共政策大学院教授のブログ掲載図を引用）

３．7pay の開発は「ガイドライン」を遵守していたのか？

2019 年 3 月に一般社団法人キャッシュレス推進協議会は、スマートフォンでバーコードや QR コードを表示して決済するコード決済について 3 つのガイドラインを発表した[9]。 そのうち『コード決済に関する統一技術仕様ガイドライン【利用者提示型】』[10]の冒頭で本ガイドラインの制定目的を、(1) QR コード等の乱立状態を解消・防止し契約店及び利用者にとってわかりやすいコード決済手段の提供をするべく QR コード等の仕様を定めその統一化を図るとともに、(2) 契約店及び利用者にとって安心かつ安全な決済手段が提供されるよう、各コード決済事業者に対しコード決済のセキュリティ対策の向上を要請するもの、であるとしている。

そして、その項目「6.2（本人認証）」で、コード決済事業者に対し本人認証プロセスの重要性を説明するとともにその義務履行を求めている。

図表 6 ：「コード決済に関する統一技術仕様ガイドライン【利用者提示型】」（抜粋）

6.2 本人認証

(1)総論(抜粋)

・コード決済事業者(今回は「7pay」)においては、不正利用等を防止するためにコード決済を利用できる者を本人に限定するとともに、決済を行おうとする者が当該決済を行う権限がある者であることを担保するために、本人認証を行うことが重要と考えられる。

・本人認証のあり方においては、「基礎認証」と「利用時認証」の組み合わせにより様々なパターンがあるが、**事業者は想定される不正利用を防止するために、適切な本人認証プロセスを設けなければならない**。

7pay の開発責任者は、「想定したアクセス不正に基づき、セキュリティ対策を施した」と主張するかもしれない。しかし、上掲 2.に記載した通り「2 段階認証」等の基本的な対策機能が有していないなか、はたしてその主張が通るかは疑わしい。ちなみに、8 月 1 日の会見で、「システム開発にあたりリスク管理上、相互検証、相互牽制の仕組みが

9 ガイドライン策定にあたっては、182 の企業・団体が検討メンバーとして参加。携帯電話会社や、金融機関、決済関連サービス、鉄道事業者、食品メーカー、小売事業者など幅広く参画していた。

10 詳細は https://www.paymentsjapan.or.jp/wordpress/wp-content/uploads/2019/03/CPM_Guideline_1.1.pdf をご参照。

十分に機能していたか」を検証するべく、弁護士を中心とするチームが 1～2 ヵ月かけて検証する予定との発表があった。

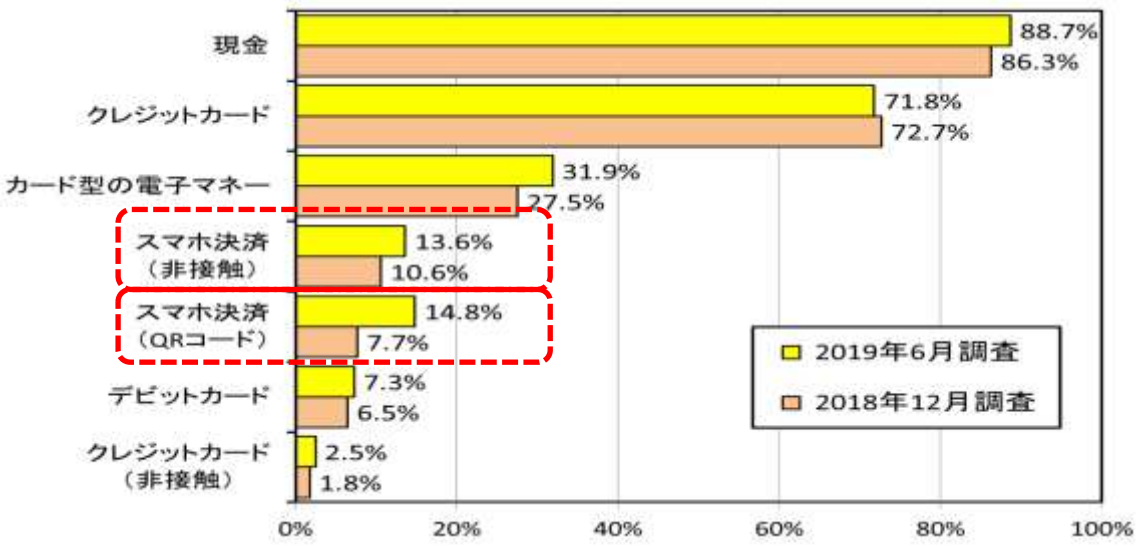
４．7pay 不正アクセス問題により QR コード決済は衰退するのか？

鳴り物入りでリリースされた 7pay であったが、不正アクセス問題を受け一部報道やネット（SNS）では、「キャッシュレス決済への信頼性がほぼゼロになった」や「一般的に『QR コード決済は危険』という認識が広まって、たいして普及せずに終わりそうだ」などの悲観的なコメントが相次いだ。

しかし、それらのコメントは正しいだろうのか？ここでは、Mobile Marketing Data Labo 社[11]がホームページで公表している調査結果[12]を用いて検証してみたい。

先ず普段の支払い方法（複数回答可）のヒアリング結果は以下の通りである。

調査結果 1：普段の支払い方法（複数回答可）



ここで注目するべき点は、半年前（2018 年 12 月）の同じ調査と比べ、QR コード決済の伸びが一番大きいうえ、その使用比率が「非接触決済（スマホの決済アプリにクレジットカードや電子マネーを登録し、店頭レジや改札口でスマホをかざし決済する方法）」を上回り、「現金」・「クレジットカード決済」・「電子マネー（カードをかざす方法）」に次ぐものとなったことである。

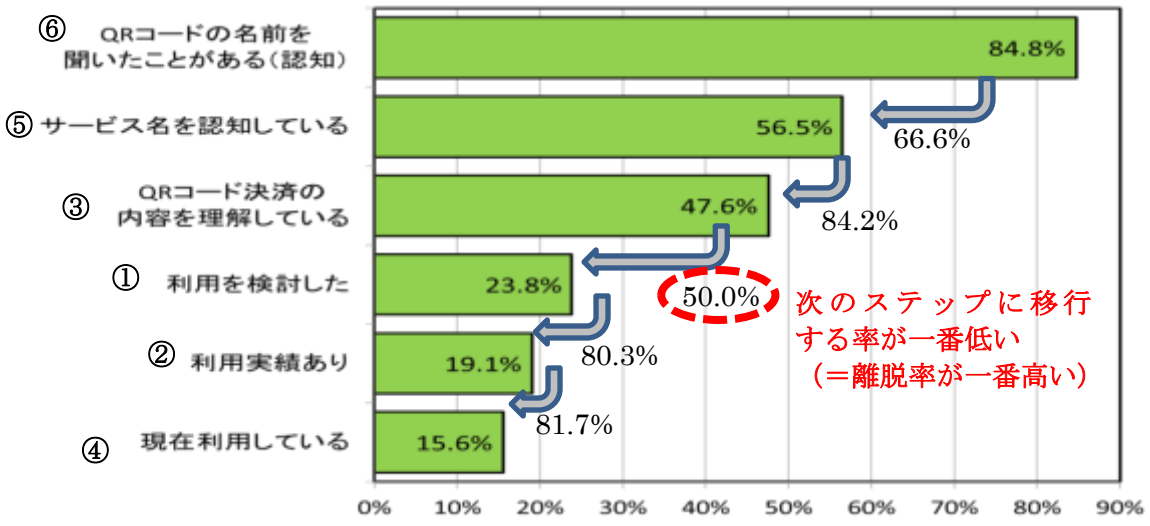
---

[11] 2006 年設立のモバイルに特化した民間調査研究機関（https://mmdlabo.jp/）。

[12] 18 歳～69 歳の男女 30,000 人を対象に 2019 年 6 月 14 日～18 日の期間で「2019 年 7 月 QR コード決済利用動向調査」を実施。詳細は https://mmdlabo.jp/investigation/detail_1807.html（サマリー）をご参照。

次に、「QR コード決済」の浸透度について、「ファネル分析」[13]を用い分析している。

調査結果 2：QR コード決済の認知～利用状況「ファネル（漏斗）分析」



その調査結果によると、QR コード決済を更に広めるためには「『③QR コードの内容を理解している』人に対し『④いかに利用を検討させる』ようにするか」の仕掛けが重要であることが分かる。実際、その一環として各 QR コード決済事業者は、2018 年末以降キャッシュバックや割引クーポン発行等のキャンペーンを大々的に開催し、その利用を促している。

そして、問題の「⑥現在も QR コード決済を利用している」層であるが、前々回（2017 年 11 月）調査（1.9%）、前回（2018 年 12 月）調査（7.5%）から大幅増加の 15.6%となった。しかも、そのうちの 1/3 は 2～3 日に 1 回は必ず QR コード決済を使用する「ヘビーユーザー」であることが判明している。

当該調査は 7pay の不正アクセス問題が発覚した前に行ったものにつき、その影響を踏まえ次回の調査まで QR コード決済の方向性を結論付けるのは早計だという声もある。しかしながら、QR コード決済業者によるキャンペーン活動が恒常的に続いていることや、QR コード決済の「ヘビーユーザー」が一定数既に堆積していることを鑑みると、**今般の 7pay 不正アクセス問題はその決済アプリ及び 7&アイグループ社内の情報セキュリティ管理体制の不備に起因するものであり、QR コード決済自体の問題ではない、**

[13] 商品購入や会員登録などアプリ内でユーザーにしてほしいアクションに至るまでのプロセスの離脱率を把握し、どこで多くのユーザーが離脱しているかを確認する分析手法。各プロセスの離脱率を見ることで、ユーザーがゴールに至るまでにどこで一番多く離脱しているかが分かるとともに、その離脱を防止するために優先的に改善するべき対策の策定が明確になる、というメリットがある。

と冷静に判断する利用者が多く、その結果 QR コード決済市場は引き続き拡大するものと考えるべきではなかろうか。

終わりに

日本人は総じて「現金決済」を好むが、「外的要因（ラグビー・ワールドカップ、東京オリンピック・パラリンピック、インバウンド等）」と「内的要因（人口減少、労働生産性の向上、間接コストの削減圧力等）」とを鑑みると、他国と比べると浸透スピードは遅いかもしれないが、キャッシュレス決済の流れは今後も止めることはできないであろう。

このような動きを踏まえ決済事業者が相次ぎ参入しているが、今般の 7pay 不正アクセス問題を見るに、QR コード決済を始めとするキャッシュレス決済市場はハイプ・サイクル[14] でいう「流行期」から、その可能性や将来性に関する「過度な期待」の急落とともに運営元の淘汰が始まる「幻滅期」に入ったと思われる。

図表 7 ：国内キャッシュレス事業者一覧

（CROWD CAST より）

14 米コンサルティング会社であるガートナー社が考案した、特定の技術の成熟度、採用度、社会への適用度を示す概念図。新技術の進化段階として「黎明期（技術の引き金）」、「流行期（過剰期待の頂）」、「幻滅期（幻滅のくぼ地）」、「回復期（啓蒙の坂）」、「安定期（生産性の台地）」の 5 段階があると説く。

事業者が撤退すると、短期的には「今まで確保した各利用者のデータをいかに保護するのか」や、「他の決済方法に円滑に移行することができるのか」などの問題が発生しよう。また長期的には、利便性が高いと感じていた決済手段が突然利用停止となることで、利用者が「QR コード決済」に不信感を抱き、その結果他の決済方法にとって取って代わられるおそれがある 。

かようなリスクがあることを勘案すると、利用者の混乱を最小限に抑えるべく、官民でバックストップ（安全策）をあらかじめ検討しておくことに加え、利用者サイドも世の中の流れにいち早く変化に対応できるよう、様々なサービスを利用しながら情報感度・リテラシーを高めておくことが大事だと筆者は考える。

以　上

Address: 3-2, Nihombashi Hongokucho 1-chome, Chuo-ku, Tokyo 103-0021, Japan
Telephone: 81-3-3245-6934, Facsimile: 81-3-3231-5422
〒103-0021　東京都中央区日本橋本石町 1-3-2
電話：03-3245-6934（代）ファックス：03-3231-5422
e-mail: admin@iima.or.jp
URL: https://www.iima.or.jp