リテール向けキャッシュレス決済における不正利用の現状と課題

成城大学経済学部教授　**中田　真佐男**

～要旨～

キャッシュレス化をさらに進めていくためには、セキュリティ面に対して利用者が抱く不安の払拭が欠かせない。本稿では、クレジットカードを主な対象としてキャッシュレス支払手段の不正利用対策の現況を概観し、取り組むべき課題の明確化を試みた。

電子商取引の市場規模拡大に伴い、近年はオンライン上でのクレジットカードの不正利用が増加している。また、物理カードの IC 化によっていったんは減少した対面取引での不正利用も、コード決済のアプリにクレジットカードを連携させて使用する方法が悪用されれば、再び増加に転じる恐れもある。

近年は不正の手口も高度化しており、官民は今後も連携してセキュリティ対策の強化を図っていくことが求められる。ただ、セキュリティ確保に必要な手順が増え、消費者や店舗の負担が増加するとかえってキャッシュレス化が停滞しかねない。この点をふまえると、ICT の活用等を通じて安全性と利便性との両立を実現していくことが今後の課題となる。

1　はじめに

日本では、民間最終消費支出額に占めるキャッシュレス支払額の比率（以下、キャッシュレス決済比率）を 2025 年までに 4 割程度、将来的には世界最高水準の 80％まで上昇させることを目標に定め、官民一体となってキャッシュレス化が推進されている。2008 年に 11.9％だったキャッシュレス決済比率は 2021 年には 32.5％にまで達しているが、この先、キャッシュレス化をさらに加速していくためには、消費者がキャッシュレス決済に抱く不安や不満を解消していくことが不可欠となる。具体的には、消費者向けの意識調査で上位回答を占めるセキュリティ面での不安を払拭していくことが求められよう。こうした問題意識のもと、本論文では、リテール向けキャッシュレス決済における不正利用の現状を示し、官民による不正利用対策の取り組み状況を概観したうえで、安全で便利なキャッシュレス社会の実現に向けた課題を明らかにした。

わが国ではクレジットカードが主要なキャッシュレス支払い手段となっている。物理カードの IC 化によって対面取引でのクレジットカードの不正利用はいったん減少したが、近年の電子商取引の伸長に伴ってオンライン上でのクレジットカードの不正利用が増加し、手口も巧妙化している。加えて、コード決済のアプリにク

レジットカードを登録できることを悪用し、物理カードを用いずにコード決済を介して対面取引でクレジットカードを不正に利用する事例も発生している。イノベーションの進展は不正対策を進化させる一方で、不正の手口の高度化にもつながる。政府は割賦販売法を改正し、決済事業者等に対して最新のセキュリティ対策の導入を義務付けてきたが、今後もICTを有効活用するなどして、①カード情報の漏洩阻止、②厳重な本人確認、③迅速な不正検知を徹底していくことが求められる。ただし、例えば、スマートフォンのショートメッセージ機能などを用いたワンタイムパスワードで2段階認証を導入したり、オンライン通販で3-Dセキュアを導入すれば不正を抑止する効果は高まるものの、一方で消費者や店舗の負担は増え、キャッシュレス決済の利便性に影響が及ぶ。利便性が大きく損なわれればむしろキャッシュレス化にブレーキがかかりかねない。この点をふまえると、セキュリティの確保を最優先しながら、同時に利便性との間に最適なバランスを見い出していくことが今後の課題となる。

本稿は以下のように構成される。まず第2節では、我が国キャッシュレス化の進展状況を確認する。続く第3節では、我が国の中心的なキャッシュレス支払い手段であるクレジットカード、および、近年急速に普及しているコード決済の不正利用の現状を示す。第4節では、巧妙化する不正利用への対策について説明し、克服すべき課題を明確化する。最後の第5節は結びとして位置づけ、明らかになった課題への対応の方向性を展望する。

2　日本のキャッシュレス化の現状

経済産業省は、民間最終消費支出に占めるキャッシュレス支払額の比率を算出し、「キャッシュレス決済比率」として毎年公表している。このキャッシュレス決済比率は2021年に32.5%に達し[1)]、2008年の11.9%から10年余りで2.7倍の伸びを見せている。一般社団法人キャッシュレス推進協議会（2021）によれば、主要各国のキャッシュレス決済比率は既に2018年時点で40～90%台に達しており、これと比較すれば日本はまだ後れをとっているものの、日本でもキャッシュレス決済は着実に浸透しつつある。表1には、支払い手段別にキャッシュレス決済比率の推移が示されている。

日本のキャッシュレス化はクレジットカードの普及によって牽引されていることがわかる。なお、諸外国ではクレジットカードの利用はリボルビング払いが一般的であるのに対し、日本では手数料が発生しないマンスリークリア（翌月1回払い）が主流である。『クレジットカード動態調査』（一般社団法人 日本クレジット協会）によれば、2021年度のクレジットカードショッピングの契約件数のうち93.6%をマンスリークリアが占める。このように日本ではある意味でクレジットカードがデビットカードに近い方法で使われていることもあり、デビットカードでの決済比率はかなり小さい。この点はキャッシュレス化が進んでいる諸外国でデビットカードが広く浸透していることとは対照的である[2)]。

IC型電子マネーについて見ると、日本では

表1　キャッシュレス決済比率の推移

	2015	2018	2021
クレジットカード	16.5%	21.9%	27.7%
デビットカード	0.15%	0.44%	0.92%
IC型電子マネー	1.5%	1.8%	2.0%
コード決済	---	0.05%	1.8%
合計	18.2%	24.1%	32.5%

（注）経済産業省（2022）に示されたデータを筆者が整理して表を作成している。
（出所）経済産業省（2022）。

2001 年 11 月に Edy（現：楽天 Edy）が本格的にサービスを開始してから既に 20 年余りが経過しているものの、消費者に広く浸透しているとは言い難い。この要因としては、中田（2021）でも指摘されるように、非接触型 IC チップに対応する店舗側の決済処理設備の低価格化が遅れ、一般の中・小規模の店舗への導入がなかなか進まなかったことなどが挙げられる[3)]。一方、日本でコード決済サービスが開始されたのは IC 型電子マネーよりはるかに遅く、2014 年 12 月に LINE Pay のサービス提供が始まってからである。しかし、その普及スピードは速く、表 1 に示されるように 2021 年時点で既に IC 型電子マネーに迫る決済比率となっている。

算出方法からわかるように、キャッシュレス決済比率は決済金額ベースでキャッシュレス化の進展度を把握する指標である。このため、1 件あたりの決済金額が大きい支払い手段の比率が大きく出やすい。表 2 には、表 1 で掲載された各支払い手段の 2021 年時点での 1 件あたりの平均決済金額が示されている[4)]。

この表からもわかるように、クレジットカードやデビットカードと比べ、少額の対面決済での利用が中心となる IC 型電子マネーやコード決済の 1 件あたりの平均決済金額はかなり小さい。この点をふまえ、表 3 では、各支払い手段の利用件数が 2020 年度と 2021 年度で比較されている。

比較の尺度を件数ベースに変えると他のキャッシュレス支払手段との差は縮小するものの、それでもクレジットカードの決済件数は他のキャッシュレス支払手段を大きく上回っている。また、クレジットカードの決済件数は直近でも趨勢的に増加している。この背景として、拡大を続ける個人消費者向け電子商取引（以下、B to C-EC）において、クレジットカードが主要な決済手段として利用されていることが挙げられる。経済産業省 商務情報政策局 情報経済課（2020, 2021）によれば、2010 年には約 7.8 兆円だっ

表 2　各支払い手段の 1 件あたり平均決済金額（2021 年度）

クレジットカード	デビットカード	IC 型電子マネー	コード決済
4,994 円	4,337 円	1,040 円	1,447 円

（注 1）クレジットカードは 2 か月以下での支払い（引き落とし）に対象を限定している。
（注 2）『コード決済利用動向調査』は四半期・暦年データしか公表されていないため、筆者が四半期データをもとに年度データに変換している。
（出所）『クレジットカード動態調査』（一般社団法人 日本クレジット協会）。
『決済動向』（日本銀行 決済機構局）。
『コード決済利用動向調査』（一般社団法人 キャッシュレス協議会）。

表 3　各支払い手段の決済件数（2021 年度）

	クレジットカード	デビットカード	IC 型電子マネー	コード決済
2020 年度	118.6（億件）	5.3（億件）	59.2（億件）	31.4（億件）
2021 年度	134.1（億件）	6.5（億件）	57.4（億件）	55.8（億件）

（注 1）クレジットカードは 2 か月以下での支払い（引き落とし）に対象を限定している。
（注 2）『コード決済利用動向調査』は四半期・暦年データしか公表されていないため、筆者が四半期データをもとに年度データに変換している。
（出所）『クレジットカード動態調査』（一般社団法人 日本クレジット協会）。
『決済動向』（日本銀行 決済機構局）。
『コード決済利用動向調査』（一般社団法人 キャッシュレス協議会）。

たB to C-EC の市場規模は 2020 年には約 19.3 兆円となり、この 10 年間で約 2.5 倍にまで規模が拡大している。公正取引委員会（2022）では、クレジットカードを保有している消費者 4,200 名を対象に 2021 年 7 月から 2022 年 2 月にかけて Web でアンケート調査を実施し、クレジットカードを利用する機会について尋ねているが（複数選択可）、84.1％が「インターネットで買い物をするとき」を選択している。なお、同調査では他の決済手段の利用者にも同じ質問をしているが、「インターネットで買い物をするとき」を選択した回答者の割合は、電子マネーで 8.1％、スマートフォン決済（QR コード等）で 18.5％、スマートフォン決済（タッチ方式）で 9.2％に過ぎない。

日本においてクレジットカードが主要なキャッシュレス支払い手段である点に疑いの余地はない。ただ、その一方で、表 3 では直近 1 年間でコード決済の取引件数が著しい伸びを見せており、少額の対面取引を中心にコード決済が急速に浸透していることが窺われる。コード決済が IC 型電子マネーよりもはるかに速いペースで普及している背景として、店舗側の導入コストの低さが挙げられる。IC 型電子マネーでは、消費者のデバイス内のチップに電子的な金銭価値が記録される。そのうえで消費者のデバイスと店舗の端末の間で金銭価値を無線で送受信する仕組みになっており、ハイスペックな決済処理端末が必要となることから店舗側の導入コストも高くなってしまう。これに対し、コード決済では、インターネットで店舗側・消費者側の端末を決済事業者のサーバと結んだうえで、金銭価値を全て決済事業者のサーバで管理する。個別の取引情報の記録には 2 次元コード（バーコードや QR コード）が用いられ、利用者提示型（CPM）か店舗提示型（MPM）のいずれかの方法で決済事業者に伝達される。既に POS 端末を備えている店舗であれば CPM でコード決済を導入するハードルは低いし、POS 端末を備えない小規模な店舗でも、MPM 方式を採用すれば 2 次元コードを印刷（あるいはモバイル端末に表示）して店頭に掲出するだけでコード決済を導入できる。こうしたコスト面での優位性に加え、2019 年 10 月から 2020 年 6 月にかけて政府が実施した「キャッシュレス・消費者還元事業」や、同時期に展開されたコード決済事業者によるプロモーション活動もコード決済の普及を後押しした。

表 3 に示されるように、キャッシュレス・消費者還元事業が終了し、決済事業者によるプロモーション活動の規模が一服した後もコード決済の著しい伸びは続いている。利用者へのポイント付与や店舗へのコスト面での優遇に過度に依存せずとも、コード決済が我が国でキャッシュレス決済手段として定着しつつあると言える。利用者側から見たコード決済の利点として、アプリ上での預金口座やクレジットカードとの連携を通じて利便性の向上を図れることが挙げられる。例えば、登録した銀行口座やクレジットカードからチャージができる。また、チャージしてプリペイド方式で利用する方法だけでなく、予め紐づけておいたクレジットカードやデビットカードで支払う方法も選択可能である。また、主要なコード決済事業者は送金サービスも併せて提供しており、アカウントに預金口座を登録すればこうした送金サービスも利用できる。公正取引委員会（2020）では、2019 年 12 月にコード決済を利用している消費者 4,000 名を対象に Web でアンケート調査を実施し、チャージの方法や銀行口座・クレジットカードの連携の有無について尋ねている（複数回答可）。表 4 には、この設問に対する上位回答の結果が示されている。

表４　コード決済で最も頻繁に利用されるチャージ等の方法（上位回答）

回答内容	回答割合
銀行口座からのチャージ	34.5%
クレジットカードからのチャージ	33.8%
クレジットカードとの連携	20.5%
コンビニや ATM 等での現金チャージ	14.9%

（出所）公正取引委員会（2020）。

一定割合のコード決済の利用者がアプリ上で銀行口座やクレジットカードからチャージをしていることがわかる。また、20.5%の消費者が、コード決済をクレジットカードと連携させて利用していることが注目される。こうすることで、消費者はクレジットカードを（店舗側の端末での暗証番号の入力を伴う）物理カードとしてではなく、いわゆる「スマホ決済」として利用できる。『コード決済利用動向調査』（一般社団法人 キャッシュレス協議会）によれば、2021 年のコード決済の店舗利用額約 7.3 兆円のうち、およそ 28%にあたる約 2.1 兆円はクレジットカードからの利用となっている。

３　キャッシュレス支払手段の不正利用の現状

（1）キャッシュレス化推進を阻むセキュリティへの不安

日本でキャッシュレス化をさらに促進していくためには、消費者がキャッシュレス決済に抱く不安や不満を解消していくことが求められる。消費者庁（2022）は、2022 年 2 月に 1,881 名の消費者を対象にキャッシュレス決済に関する意識調査を実施した。表 5 には、この調査においてキャッシュレス決済に抱くネガティブな側面について尋ねた設問（複数回答可）への上位回答の結果が示されている。

1 位・2 位の回答がセキュリティ面での不安で占められていることがわかる。この点をふまえ、以下ではキャッシュレス支払手段の不正利用の現状について概観する。図 1 には、日本における主要なキャッシュレス支払手段であるクレジットカード不正利用被害額の推移が示されている。なお、番号盗用による被害が独立した項目となるのは 2014 年以降であり、2013 年以前は偽造カードによるもの以外の被害額は全て「その他」に含まれていることに注意を要する。

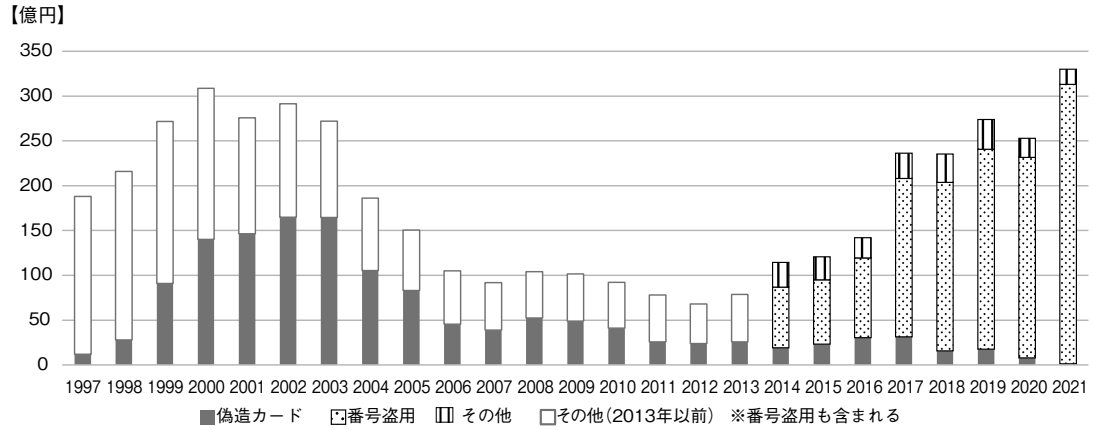
我が国のクレジットカード不正利用被害の総額は、1990 年代後半に増加した後、2000 年代に

表５　キャッシュレス決済の利用にあたって感じる不便・懸念（上位回答）

回答内容	回答割合
個人情報の流出や不正使用等の被害が発生するおそれがあること	51.6%
カード等の紛失・盗難のおそれがあること	41.0%
お金を使っている感覚がせず、使いすぎてしまうおそれがあること	37.7%
決済手段・サービスによって利用できる店舗が異なっており、利用可能な範囲が分かりにくいこと	35.4%
災害等の非常時に決済ができない場合があること	31.7%
自身の購入・決済履歴等の個人情報が事業者等に取得・利用されること	29.3%

（出所）消費者庁（2022）をもとに筆者作成。

図１　クレジットカード不正利用被害額の推移



（出所）「クレジットカード不正利用被害額の発生状況」（一般社団法人日本クレジット協会）。

入って一度は減少傾向に転じたものの、2010 年代半ばから再び趨勢的に増加していることがわかる。

(2) 減少した対面取引での不正利用

インターネットが一般家庭にまで普及する以前は、リテール決済の場は実店舗での対面取引に限定されていた。対面でのクレジットカード決済には物理カードが用いられることから、クレジットカードの不正利用の主な方法も、盗んだり拾ったりして入手した他人のクレジットカードを会員本人になりすまして使うか、カード情報を盗み取ったうえでクレジットカードを偽造するかであった。

かつてはクレジットカードの情報記憶媒体として磁気ストライプが採用されていた。磁気ストライプは情報記憶容量が小さいため、現在採用されている IC チップとは違ってデータを複雑に暗号化して格納できない。このため複製が容易で、特殊なリーダー（スキマー）で不法にカード情報を盗み出し、カードを偽造して不正利用するスキミング犯罪の標的となった。1987 年には、刑法が改正されて「電磁的記録不正作出罪」が追加され、クレジトカードの偽造に対して一定の立法措置が講じられた。しかし、この法改正ではスキミング行為が処罰の対象とされなかったこともあり、スキマーの性能が向上した 1990 年代後半にはスキミング犯罪が多発するようになった。スキミング犯罪が社会問題化すると、2001 年の刑法改正では「支払用カード電磁的記録に関する罪」が規定され、新たにスキミング行為が「支払用カード電磁的記録不正作出準備罪」として処罰の対象に追加された[5)]。あわせて警察の取り締まりも強化されたことで、2000 年代に入ってカードの不正利用被害額はいったん減少に転じることになった。

この時期にはヨーロッパでも不正利用被害が拡大し、対策が講じられた。山本（2015）では、イギリスにおけるカード偽造による被害額が 2001 年の 1 億 6,040 万ポンドから 2010 年には 4,760 万ポンドにまで減少したことが紹介されているが、この要因は物理カードの情報記憶媒体を磁気ストライプから IC チップに切り替えたことにあるという。日本よりも早くスキミング犯罪の増加に直面したヨーロッパでは、Visa・Master・Europay の国際ブランド 3 社が中心となって IC カードのセキュリティ仕様を標準化し（EMV 仕様）、カードへの IC チップの搭載と決

済端末のIC対応を強力に推進した。ICチップは磁気ストライプと比べて格段に記憶容量が大きい。このICチップにカード会員の情報を暗号化して格納すれば外部からの復元は困難であり、カード偽造による不正利用を抑制できる。なお、ICチップ搭載のクレジットカードで決済を行う場合、本人確認は署名では行わない。代わりに店舗側の決済端末にカードを挿入し、テンキーでパスコード（PIN：Personal Identification Number）を入力して本人確認を行う。この認証プロセスは一般にChip and PINと呼ばれる。

瀬田（2018）によれば、EU加盟国、カナダ、東南アジアは既に2010年前後にはカードと端末のIC対応を完了した。アメリカは当初はIC対応に消極的だったが、大規模なカード情報の流出事件を契機に当時のオバマ政権が2014年からセキュリティ強化に乗り出し、カードと端末のIC対応が急速に進んだ。これに対し、日本ではカードへのICチップの搭載は進んだものの、決済端末のIC対応が遅れた。山本（2015）はその理由として､前述のように2000年代に入って(IC対応をしなくても）不正利用が減少するなか、多額の費用を負担してPOSを改修することに大手流通業が消極的だったことを挙げている。

図1では、減少基調にあった偽造カードによる不正利用被害額が2015年～2017年にかけて増加しているが、これについて瀬田（2018）は、IC対応が他国より遅れた日本が世界から標的とされ、偽造カードによる不正利用が増加した可能性を指摘している。世界中のクレジットカード犯罪グループから集中的に攻撃されることへの懸念に加え、コロナ禍以前の観光立国戦略において外国人観光客が安心できるカード決済環境の整備が重要課題とされたことから、日本でもようやく政府と関係業界が連携して本格的な対策がとられた。具体的には、2018年6月に改正割賦販売法が施行され、2020年3月を期限として、クレジットカードの加盟店にICカード対応決済端末の導入が義務付けられた。現在、日本でも対面でのクレジットカード決済時にChip and PINによる本人確認が原則となっているのはこの法改正があったためだ[6)]。IC対応の完了の効果は目に見えるかたちであらわれており、図1に示されるように2021年の偽造カードによる不正利用の被害は1.5億円にまで減少した。

(3) 増加が続くオンラインでの不正利用

図1からも明らかなように、クレジットカード不正利用被害の総額は2010年代の半ばから再び増加基調にある。これは番号盗用による不正利用被害額が急激に増加しているためである。その背景にあるのは、一般家庭へのインターネットの普及に伴うB to C-ECの市場規模拡大である。

物理カードが利用できないオンライン通信販売では、クレジットカード決済は加盟店の決済画面でカード番号やパスワード等を入力して行われる。これらの情報を何らかの方法で不正に入手し、やはりオンライン通販などの非対面取引で本人になりすまして使用するのが、番号盗用による不正利用の典型的な手口である。

カード番号などの個人情報の窃取もインターネット上で行われる。一度に大量の情報を窃取する手段としてEC事業者のサーバへの不正アクセスが挙げられる。ただし、サーバへのハッキングによって顧客のカード情報が大量に漏洩すると被害額も拡大してしまうことから、こうしたサイバーアタックに対しては比較的早期に対策が講じられた。具体的には、前述の改正割賦販売法（2018年6月施行）において、EC事業者等の加盟店に対し、原則としてカード情報を「非保持化」するか、保持するのであればPCI DSS（Payment Card Industry Data

Security Standards）に準拠することが義務付けられた。PCI DSSは国際カードブランド5社によって策定されたカード情報セキュリティの国際基準である。ただ、カード会社のような大手企業ならまだしも、小規模なEC事業者にとって、PCI DSS準拠の認証を得るために要求事項をすべて満たすことはリソース面・コスト面でかなりハードルが高い[7)]。よって、多くのEC事業者はカード情報を「非保持化」する対応をとった。ここで「非保持化」とは、加盟店側の機器やサーバでカード情報をデータとして保存・処理・通過しないことを意味し、カード情報の処理自体を（PCI DSSに準拠する）決済代行業者のシステムに委ねることでこれを実現できる。

EC事業者の間で「非保持化」が進んだ結果、EC事業者のサーバからのカード情報の漏洩は減少する傾向にある。これに代わって近年に不正アクセスの標的になっているのは、複数のEC事業者に「非保持化」を支援するシステムを提供し、結果的に大量のカード情報が蓄積される決済代行業者のサーバである。2022年1月にはPCI DSSに準拠している決済代行事業者のメタップスペイメントがサイバー攻撃にあい、46万件超のカード情報の流出が確認された。

個人からカード情報を窃取する手段には、フィッシングやオンライン・スキミングがある。このうちフィッシングは、標的となるECサイトに似せた偽のサイトを作成し、消費者を誘導してカード情報やパスワード、セキュリティコードを入力させてカード情報を窃取する手法である。カード会社やEC事業者を騙ったメールマガジンを送信し、URLのリンクをクリックさせてフィッシングサイトに誘導する手口が典型的である。これに対し、オンライン・スキミングは本物のサイトのセキュリティの脆弱性をついた情報窃取の方法である。瀬田（2022）では、本物のサイトの決済手段選択画面を改ざんしていったん偽の決済画面に誘導し、そこで入力されたカード情報を外部に送信するとともに、次の画面に進んだ時にエラーを表示して本物のサイトの決済画面に戻す手口が紹介されている。この方法をとると、消費者側が入力ミスをしたと勘違いして本物の決済画面にもういちどカード情報を入力すれば決済は成立し、フィッシングとは異なって商品もきちんと届く。それゆえ情報を窃取されたことに気づきにくい。この他、本物のサイトの入力画面のプログラムに不正侵入してコードを挿入し、本物の画面に入力された情報が外部に送信されるように仕向ける手法もオンライン・スキミングの一種である。

フィッシングやオンライン・スキミングでは一度に大量のカード情報が窃取されることはないが、画面に入力した情報がそのまま窃取されることから、セキュリティコード（物理カードの裏面に記載されている3～4桁のカード固有の番号で、カード認証の一手段としてしばしば入力を求められる）のようなより重要なカード情報もセットになって流出するリスクが大きい。また、オンライン・スキミングは不正行為が発覚しにくく、長期にわたって情報が窃取される恐れもある。オンラインでのクレジットカードの不正利用被害額の拡大を防ぐためには、今後はこうした小規模な情報流出への対応も重要になってくる。

番号盗用による不正利用に関しては、番号を盗用する主体とクレジットカードを不正利用する主体が必ずしも同一とは限らない点にも注意を要する。インターネット上には匿名性が高い闇サイト群、いわゆる「ダークウェブ」が存在する。一般的な検索エンジンでは見つけることができず、専用のツールでないとアクセスできないダークウェブでは、違法性の高い物品とと

もに、不正な方法で取得された個人情報が取引されている。実際、流出した日本人のクレジットカード情報が取引される「闇市場」の存在も確認されており、犯罪集団が不法に他人のカード情報を入手する経路のひとつとなっている。

(4) コード決済等のアカウントとの連携を悪用した不正利用

第 2 節で述べたように、コード決済はスマートフォンのアプリ上で預金口座やクレジットカードとの連携が可能である。プリペイド方式で使う際には、預金口座やクレジットカードから電子的金銭価値をチャージできるし、直接クレジットカードに紐づけてコード決済を実質的にポストペイのクレジットカード払いで使うこともできる。この便利な機能を悪用し、他人になりすまして預金口座やクレジットカードからチャージしたり、番号盗用したクレジットカードをアカウントに連携させるなどして、コード決済を不正利用する事案が複数発生している。

2018 年にはコード決済サービス「PayPay」において、他人のクレジットカードを紐づけて物品を購買する不正利用が確認された。当時、PayPay は総額 100 億円を還元する大規模なキャンペーンを実施中で、支払った額の 2 割が還元されたことから、(B to C-EC で直接的にカードを不正利用するのではなく) コード決済に紐づけるかたちでの不正が行われたものと考えられる。

2019 年 7 月には、セブン & アイ・ホールディングスが開始したばかりのコード決済サービス「7pay」において不正利用が発生した。このケースでは、番号盗用したクレジットカードをアカウントに登録するかたちでの不正ではなく、会員本人が正規の手続きに則ってクレジットカードを連携させた後にコード決済のアカウント自体が乗っ取られ、不正に利用された。原因は 7pay のセキュリティ・システムの不備にあったとされる。具体的には、パスワード再設定用のリンクを、アカウント利用者本人以外の第三者のメールアドレスにも転送できる仕様になっていたため、犯罪集団がパスワードを勝手に再設定してアカウントを乗っ取ることができてしまった。登録されたスマートフォンの電話番号にしか再設定のリンクが送られないような仕様になっていればこうした不正は防げた可能性が高いことから、セブン & アイ・ホールディングスのセキュリティへの認識の甘さに批判が高まり、被害額を全額補償したうえで同年 9 月 30 日に 7pay のサービスは廃止された。

2020 年 9 月には、NTT ドコモが提供するキャッシュレス決済サービスの「ドコモ口座」で他人の預金口座からの預金の不正な引出しが発生し、引き出された資金が連携するコード決済サービスである d 払いを通じて不正利用される被害も発生した。このケースではクレジットカードではなく銀行の預金口座が不正に利用されているが、ドコモ口座を開設する際の NTT ドコモ側の本人確認のチェックの甘さ（受信可能なメールアドレスさえあれば口座を開設できた）と、ドコモ口座に銀行の預金口座を登録する際の金融機関側の本人確認の甘さ（2 段階認証の未採用）が原因となっている点は共通している。

図 1 で示されるように、偽造カードによる不正利用は現在では大幅に減少し、クレジットカードが不正利用される場は対面取引からオンライン取引にシフトしたかのように見えた。しかし、近年になってコード決済が急速に普及し、クレジットカードと連携させての使用も増えたことで、実質的にはクレジットカードが再び対面取引で不正利用されるようになってきたと言える。

4　クレジットカードの不正利用を未然に防ぐ取り組み

技術の革新に伴ってクレジットカードの不正利用の手口も高度化・巧妙化することから、政府と関係業界はこれまでも連携しながら不正利用対策に取り組んできた。不正利用を防ぐためには、(1) カード情報の漏洩を未然に防ぐこと、(2) カードの利用等にあたっての本人確認を厳格にすること、(3) 不正が疑われる取引を可能な限り早期に発見してカードを使用停止にすること、が重要になる。

既に言及したように、我が国では2018年6月に改正割賦販売法が施行され、対面取引におけるカードと決済端末のIC化と、非対面取引におけるEC事業者のカード情報の「非保持化」が推進されたことで、カード情報の保護に関しては大きな前進が見られた。また、対面取引ではIC対応に伴ってChip and PINによる認証が原則となったため、本人確認についてもそれ以前の署名による認証と比べて厳格になった。

クレジットカード決済に関係する事業者（カード会社・決済代行業者・端末機器業者など）から構成されるクレジット取引セキュリティ対策協議会は、2016年にセキュリティの向上を実現するための重点的な取り組みをまとめた「実行計画」を策定し、これを毎年改訂している。2018年6月の改正割賦販売法の施行にあわせて改訂された「実行計画 2019」においては、非対面取引についても認証強化のための具体的な方策が示された。その1つは、ECサイト利用者へのセキュリティコード入力の要求である。カード裏面に記載された3～4桁のセキュリティコードはPCI DSSにおいては秘匿性の高い情報として保存が禁止され、非保持化を求められる加盟店はもちろん、決済代行事業者も決済処理後に削除することが求められている。よって、たとえEC事業者や決済代行事業者のサーバが不正アクセスにあってもセキュリティコードが流出することはないという前提に立てば、認証手段として有効だと考えられる。しかし、既に述べたように、近年はオンライン・スキミングのようにより巧妙な手法でカード情報が窃取され、カード番号とセキュリティコードが紐づけられた形で情報が流出するケースも増えており、この意味では必ずしも安全性の高い認証手段とは言えなくなりつつある。

もう1つの認証強化の手段は、国際ブランドが提供する「3-Dセキュア」の導入である。3-Dセキュアとは、カード会員がカード会社にあらかじめパスワードを登録しておくと、EC事業者のサイトでカード決済を行う際にカード会社の認証画面にいったん移行し、そこでパスワードを入力して本人確認を行う仕組みである。セキュリティコードが券面に記載され、かつ、比較的覚えやすいのに比べ、3-Dセキュアでは新たに一定のルール（長さや文字の種類など）を満たすパスワードを設定する必要が生じるので利用者の負担は増える。また、途中でEC事業者のサイトがいきなり切り替わるので利用者からフィッシングと誤認される可能性も排除できない。しかし、カードの認証情報がEC事業者（および決済代行業者）のサーバからは完全に切り離されて管理されることから、安全性はセキュリティコードの入力と比べて高い。2018年に不正利用が発覚した「PayPay」では、クレジットカードと連携させる際に当時はセキュリティコードの入力を求めていたが、これを3-Dセキュアに変更したことで不正利用の大幅な減少に成功したという[8)]。

近年はスマートフォンのSMS（ショート・メッセージ・サービス）を活用した2段階認証の導入も進んでいる。2段階認証とは、EC事業者の

サイトで決済をする過程で利用者が登録した電話番号に SMS で追加的な認証情報を送信し、受信した利用者がこの認証情報を EC サイトで入力することによって確実に本人確認をとる方法である。携帯電話番号は複製できないため、スマートフォンが盗難にあわない限りは本人しか受信できない。追加的な認証情報としてワンタイム・パスコード（1 回限り有効な数桁の数字などのパスコード）を採用すればさらにセキュリティを強化できる。

不正利用が疑われる取引の早期発見に関しては、近年は AI の導入などによって不正検知システムの精度が向上している。会員のこれまでの購買行動の傾向から逸脱する取引が検出されると、確認が取れるまではカード使用を停止できるようにもなっており、不正利用被害額の減少につながっていると考えられる。

5　キャッシュレス化のさらなる推進に向けて克服すべき課題

ICT を有効活用することで技術的にセキュリティを強化することは可能になってきている。ただし、セキュリティ強化のために認証に際して消費者や事業者に求める負担が重くなると、キャッシュレス決済手段としての利便性が低下してしまうことは否定できない。例えば、3-D セキュアは高い安全性を有するものの、一方で利用者にとっては手間の増える認証手段である。この手間を嫌って購入を途中で止めれば、EC 事業者は収益を得る機会を逸してしまう（いわゆる「カゴ落ち」）。スマートフォンの SMS を活用した 2 段階認証に関しても同様のことが言える。第 3 節ではコード決済の不正利用の事案が紹介されたが、被害が発生したコード決済サービスで 2 段階認証の導入が見送られていた背景としては、登録の手間を敬遠してサービスの利用者が伸び悩むことへの懸念もあったものと考えられる。もちろん、セキュリティの確保は最優先されるべきではあるものの、同時に利便性との間に最適なバランスを見い出していくことが今後の課題となろう。特に、キャッシュレス決済に関しては、従前から高齢者などデジタルディバイドに直面する層への対応が懸案となっている。キャッシュレス化をさらに促進するためには、本人確認に関する技術革新は単に正確性の向上を図るだけでなく、手順の簡便さも追及されていくことが望ましい。

この点に関し、課題解決のひとつの方策となるのが、より先進的な認証プロセスである「EMV 3-D セキュア」の導入である。EMV 3-D セキュアは、2022 年 10 月でサービスを停止する 3-D セキュアの後継規格であり、精度が向上した不正検知システムを認証プロセスに活用した「リスクベース認証」の導入によって消費者の手間の軽減を図っている。具体的には、実行されようとしている取引のリスクを 3 段階で評価し、最もリスクが低いと評価された取引群についてはパスワード入力を不要とし、逆に最もリスクが高いと評価された取引群については即座に認証を拒否する。そして、中間の取引群にのみ 3-D セキュアのパスワード入力を要求する。その際のパスワード入力についても、従来の 3-D セキュアでは事前に登録する必要があった。だが、EMV 3-D セキュアではスマートフォンの SMS へ送信されるワンタイムパスワードで認証できるようになる。これによってセキュリティが向上することに加え、パスワード忘れによる取引の断念も無くなるために利用者の利便性向上と、EC サイトにおける「カゴ落ち」の解消にもつながる。もっとも、高齢者などのなかにはスマートフォンを使いこなせない人もおり、そうした人々にとっては 2 段階認証に対応するこ

とも難しい。この点に関し、EMV 3-D セキュアは将来的には生体認証にも対応する予定になっている。このようにICT技術を有効に活用しながら、安全性と利便性が高いレベルで両立されたクレジットカード決済が実現されていくことが期待される。

その他の課題として、B to C-EC の市場規模拡大に伴い、カード会社や加盟店以外にもカード情報を取り扱う事業者が増加している点をふまえ、こうした環境変化に即した情報の管理体制を構築していくことが求められる。近年は、加盟店のカード情報の「非保持化」実現を支援する決済代行業者やシステム提供会社の役割が重要性を増し、大量のカード情報が蓄積されるがゆえにサイバー攻撃の新たな標的となっている。また、クレジットカードとの連携サービスを提供するコード決済事業者も、不正利用が続発したことを教訓としてカード情報のより適正な管理が求められる。この点に関しては、さらに改正された割賦販売法が2021年4月に施行され、新たに決済代行業者・システム提供業者・コード決済事業者などがPCI DSS準拠を義務付けられるようになった。しかし、既に述べたように2022年にはPCI DSSに準拠していた大手決済代行業者のメタップスペイメントのサーバからカード情報が大量に流出し、同社には2022年6月30日に所管の経済産業省から改善命令が出された[9)]。法整備は体制構築の出発点に過ぎないことを認識し、キャッシュレス決済に関わる全ての事業者が高い意識と責任感を持ってセキュリティ対策に臨むことが求められよう。

【注】

1）経済産業省ウェブサイト ニュースリリース（2022年6月1日公開）「2021年のキャッシュレス決済比率を算出しました」（https://www.meti.go.jp/press/2022/06/20220601002/20220601002.html）

2）日本でこれまでデビットカードが普及してこなかった経緯については中田（2018）pp.78-79. で詳しく述べられている。

3）中田（2021）p.40.

4）クレジットカードの1件あたり平均決済金額は「クレジットカードショッピング信用供与額／契約件数」（『クレジットカード動態調査』（一般社団法人 日本クレジット協会））、コード決済の1件あたり平均決済金額は「店舗利用金額／店舗利用件数」（『コード決済利用動向調査』（一般社団法人 キャッシュレス協議会））として筆者が算出した。デビットカード・IC型電子マネーの1件あたり平均決済金額は『決済動向』（日本銀行 決済機構局）で公表された「1件あたり決済金額」である。

5）神例（2013）では、2001年の刑法改正によって新たに設けられた「支払用カード電磁的記録に関する罪」の概要が詳しく説明されている。

6）ただし、加盟店の中には顧客の利便性に配慮し、一定金額未満の支払いについてはPINの入力が不要となるように、決済事業者と個別に契約しているところもある。

7）PCI DSS準拠の認定を受けるためには、12の要件に基づく最大約400の要求事項を満たす必要がある。加えて、定期的に審査を受けたり、「サイトスキャン」と呼ばれるシステムのチェックを受けなければならない。

8）payment navi ウェブサイト掲載記事（2019年9月6日8:00公開）「スマホ決済「PayPay」の不正利用が大幅減少、3-Dセキュア導入などが効果」（https://paymentnavi.com/paymentnews/87082.html）

9）同社からの流出データの中には、PCI DSSで保存が認められないはずのセキュリティコードも含まれていた。調査の結果、同社のシステムは診断ツールで脆弱性の高さが複数回指摘されたにもかかわら

ず、民間の監査機関への報告書を改ざんして問題がないように装っていたことも発覚し、行政処分が下された。

【参考文献】

一般社団法人キャッシュレス推進協議会（2021）「キャッシュレス・ロードマップ 2021」

神例 康博(2013)「Ⅳ. 日本刑法における「支払用カード電磁的記録に関する罪」」『立命館法学』2013 年 5 号（351 号）pp. 397（2573）- 408（2584）.

経済産業省 商務情報政策局 情報経済課（2021）「令和２年度 産業経済研究委託事業（電子商取引に関する市場調査）報告書」（2021 年 7 月）

経済産業省 商務情報政策局 情報経済課（2020）「令和元年度内外一体の経済成長戦略構築にかかる国際経済調査事業（電子商取引に関する市場調査）報告書」（2020 年 7 月）

公正取引委員会（2022）「クレジットカードの取引に関する実態調査報告書」

公正取引委員会（2020）「QR コード等を用いたキャッシュレス決済に関する実態調査報告書」

消費者庁（2022）「[参考・２月（確報）] 店頭購入及びキャッシュレス決済に関する意識調査結果」

瀬田 陽介（2022）「『クレジットカード・セキュリティガイドライン 3.0』PCI DSS 対応義務の整理と EMV 3-D セキュア促進」『カードウェーブ(Card Wave)』340 号、pp.24-29.

瀬田 陽介（2018）「カード決済セキュリティの指標『実行計画 2018』MOTO 加盟店の非保持化・不正使用対策も明確に」『カードウェーブ（Card Wave)』316 号、pp.32-39.

中田 真佐男（2021）「対面決済のキャッシュレス化の進展に伴って検討すべき諸問題とその対応の方向性」『国生活研究』第 61 巻第 2 号、pp.32-55.

中田 真佐男（2018）「我が国における非現金リテール決済手段の浸透に向けた課題」『季刊個人金融』2018 年冬号、pp.68-92.

山本 正行（2015）「カード決済セキュリティの基盤「EMV」はなぜ日本市場で普及が進まないのか」『カードウェーブ（Card Wave)』299 号、pp.16-25.

なかた　まさお
慶應義塾大学大学院経済学研究科博士課程修了（博士（経済学））。
千葉経済大学講師、財務省財務総合政策研究所主任研究官、九州大学大学院経済学研究院准教授を経て、2011 年 9 月より成城大学。
【主な著書】
『日本経済の課題と針路 経済政策の理論・実証分析』（吉野直行氏、亀田啓悟氏、中東雅樹氏との共編著）慶應義塾大学出版会、2015 年
『基礎から学ぶ 動学マクロ経済学に必要な数学』日本評論社、2011 年
【主な論文】
「農業分野における資金供給の効率性向上に向けた課題」（2022）『フィナンシャル・レビュー』第 174 号、pp.59-86.
「対面決済のキャッシュレス化の進展に伴って検討すべき諸問題とその対応の方向性」（2021）『国民生活研究』第 61 巻第 2 号、pp.32-55.
「我が国におけるキャッシュレス化の普及加速に向けた課題～交通サービスにおけるキャッシュレス化の展望を交えて～」（2021）『運輸と経済』NO.883、pp.20-25.
「キャッシュレス化推進のために何が必要か 消費者、小売・サービス事業者の視点から」（2019）『経済セミナー』（特集 経済学で見る新しい決済と金融）NO.710，pp.22-26.
「我が国における非現金リテール決済手段の浸透に向けた課題」（2018）『個人金融』Vol.12，No.4，pp.67-92.