SE Report

広がるキャッシュレス決済に潜むリスク

f j コンサルティング株式会社　代表取締役 CEO

瀬田　陽介 Yosuke Seta

1. はじめに

政府は2018年4月に公表した『キャッシュレス・ビジョン[1)]』にて、「支払い方改革宣言」として2025年までにキャッシュレス決済比率※1 40％の目標を掲げ、さまざまなキャッシュレス推進の施策を実施している。

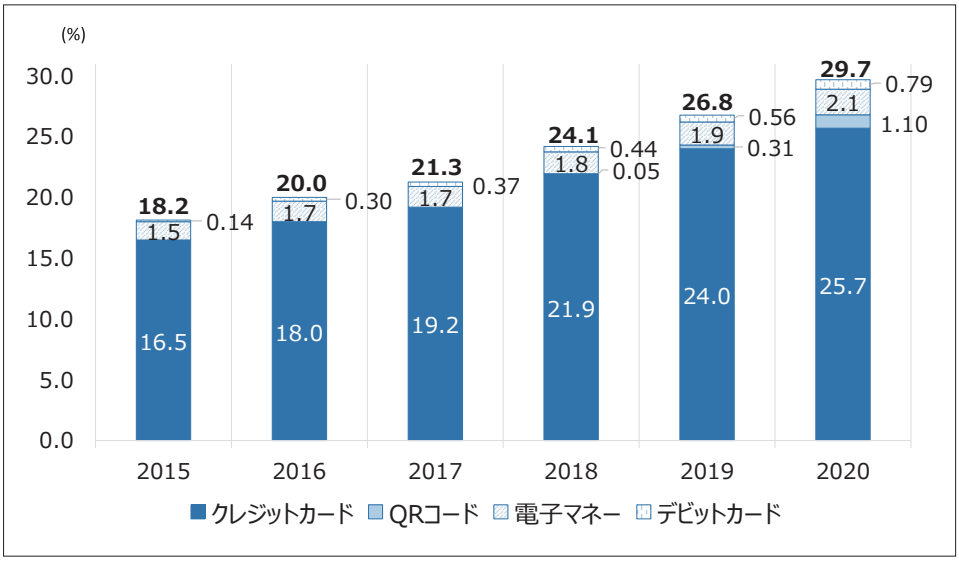
本稿では、急速に普及が進むキャッシュレス決済に潜むリスクについて解説する。

2. 普及が進むキャッシュレス決済と2つのリスク

2019年10月から2020年6月にかけて実施された「キャッシュレス・消費者還元事業」を始めとするキャッシュレス推進政策により、国内のキャッシュレス決済比率は順調に増加している[2)]（**図1**）。キャッシュレスといえば大量のテレビ広告や店頭でのポイント還元キャンペーンを行っている QR コード決済の印象が強いが、実際にはクレジットカードによる決済がもっとも多く、金額シェアで9割近くを占める。

2020年以降の新型コロナウイルス感染拡大もキャッシュレス決済の普及を後押ししている。不特定多数の人の手を介して流通する現金に対する衛生面での懸念から、業種別の感染拡大防止ガイドラインの多くでキャッシュレス決済の利用が推奨されている。消費者も QR コード決済のような少額支払いをしやすい非接触キャッシュレス決済手段の普及や、外出自粛による e コマース※2（Electronic Commerce、電子商取引：以下、EC）利用の増加により、これまでは現金で支払っていた

図 1　民間消費支出に占めるキャッシュレス決済比率の推移



野村総合研究所レポート[2)] 及び2020年統計を基に作成　※ QR コードは2018年以降

※1
キャッシュレス決済比率
民間最終消費支出に占める、クレジットカード支払額・電子マネー支払額・デビットカード支払額・QR コード決済支払額合計の割合。

※2
e コマース（EC）
本稿では主に消費者向けにインターネットを介して行われる商品やサービスの販売を指している。

ような買い物でもキャッシュレスで支払う機会が増えている。

キャッシュレス決済は便利なものだが、その反面リスクも存在する。大きくは「盗まれるリスク」と「なりすまして使われるリスク」の2つに分けることができる。

3. カード情報流出はどこで発生しているか

「盗まれるリスク」とは、クレジットカードの場合、カード番号やセキュリティコード※3など、決済に必要な情報が流出することを指す。現在、カード情報流出のほとんどはオンラインで発生している。代表的な手段が「フィッシング」と「オンラインスキミング」である（**図2**）。

※3
セキュリティコード
クレジットカード裏面に記載されている3桁のコード（クレジットカード会社によっては表面に記載された4桁のコード）。CVC、CVVとも言う。

図２　カード情報窃取の手段

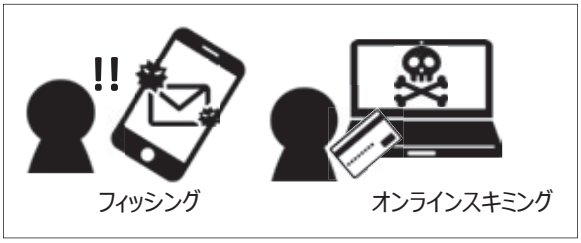
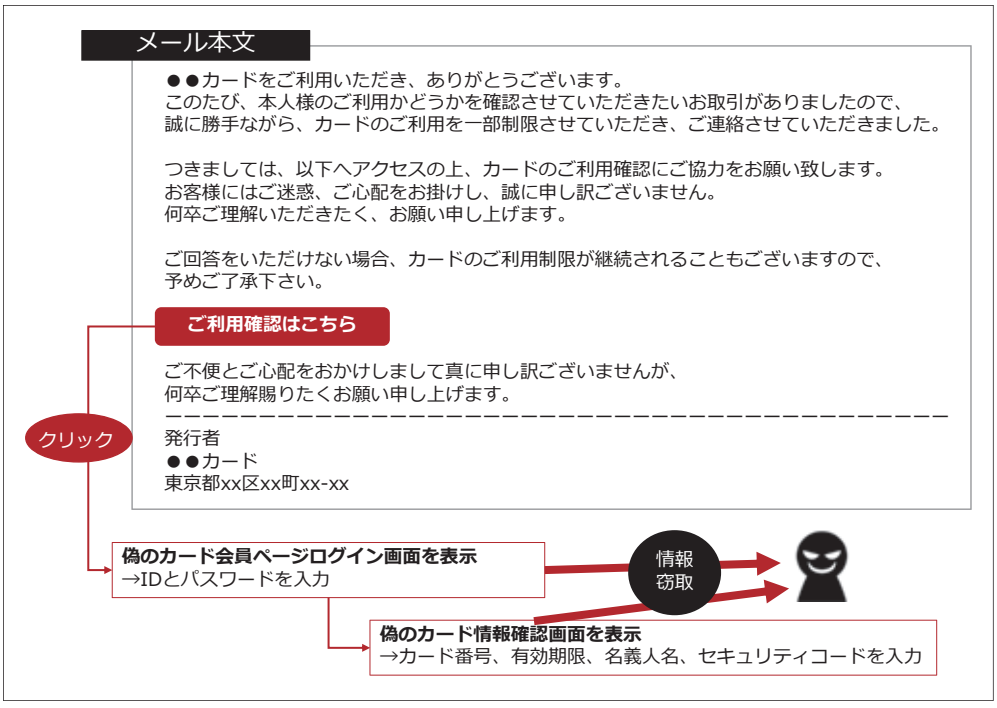


図３　フィッシングメールの例



(1) フィッシング

銀行やカード会社、EC サイトなどをかたり、偽のメール（フィッシングメール）を送信して偽のサイト（フィッシングサイト）に消費者を誘導する。誘導先のサイトで ID、パスワード、カード情報などを入力させてその情報を窃取する。

フィッシングメールの送信元は、正規のカード会社などと紛らわしいドメインのメールアドレスが使用される。文面は「第三者によるクレジットカードの不正利用の可能性があります」「ログインがロックされました」など、今すぐ確認を促す文言と共に、紛らわしい URL のリンク先が提示される。

図3は実際にカード会社をかたって送信されたフィッシングメールの例である[3)]。クレジットカードの不正利用があった旨を通知し、利用状況を確認するサイトとしてフィッシングサイトにリンクするボタンを掲載し誘導している。誘導先のフィッシングサイトは実際のカード会員向けサイトのログイン画面と見分けがつかないもので、ログインのために ID とパスワードを入力させ、次に「セキュリティ強化のため」としてカード番号、有効期限、カード名義人名、セキュリティコードを入力させる手口である。

(2) オンラインスキミング

オンラインスキミングは、EC サイトで偽のカード決済画面を表示したり、正規のカード決済画面の中に不正なプログラムのコー

ドを埋め込むなどの手法で、入力されたカード情報を悪意のある第三者に不正に送信させ、窃取する手法である。店頭で使用するカード決済端末に細工をして不正に磁気ストライプ情報を入手する「スキミング」という手法は古くから存在していた。この手法は、そのオンライン版ということでオンラインスキミングと呼ばれている。

オンラインスキミングでは、カード情報の窃取は、消費者が決済画面にカード情報を入力する都度行われる。決済の時に入力する、カード番号、有効期限、カード名義人、セキュリティコードが、決済代行事業者に送られると同時に犯人にも送られる。決済自体は正常に完了するため商品やサービスは問題なく提供されることが多く、消費者からのクレームは発生しない。また、カード情報は消費者のブラウザから犯人に直接送られるため、EC サイトのサーバーに保存されたカード情報をまとめて窃取する手法と異なり、サーバーのログ（通信履歴）に残らず気付かれにくい。そのため、被害は少しずつ長期に渡って発生し、1事件あたりのカード情報の流出件数は比較的少ないことが多い。国内ではカード情報流出事件の1事件あたりの流出件数は2018年以降減少傾向にあり、直近では大半の手口がオンラインスキミングであると考えられる（**図4**）。

多くの場合、カード情報を窃取した犯人が、それらの情報を直接不正利用することはない。窃取されたカード情報は犯罪者が拳銃や違法薬物などを売買する「ダークウェブ※4」と呼ばれるウェブサイトで売買されているといわれている。カード情報を不正に入手して売却し利益を得る犯人と、実際にカード情報を不正利用して金銭的な利益を得る犯人の間で分業されており、一種のエコシステムが成立している。

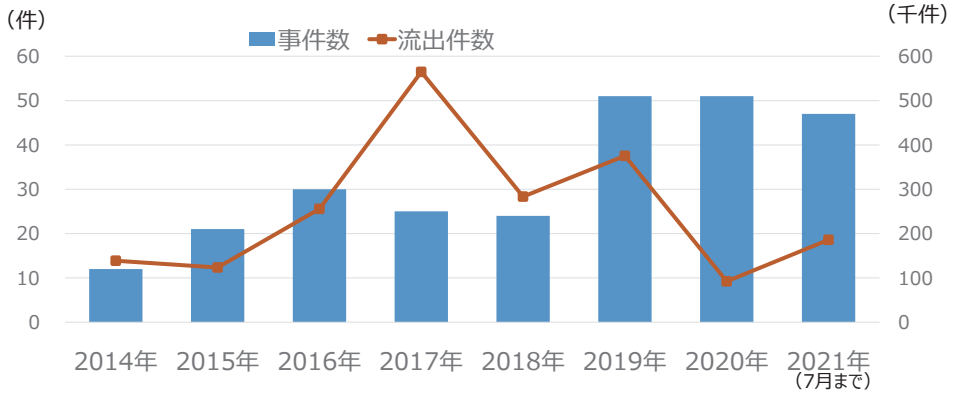
4. 銀行口座から不正に預金が引き出される事例も発生

カード情報の不正利用もまたオンラインで行われる。他人のクレジットカード情報を利用して不正に決済を行う「番号盗用」（なりすまし）による不正利用被害は増加の一途をたどっており、2020年の番号盗用被害は223億円に達している[4)]。これはクレジットカード不正利用全体の約9割に達している。

不正に入手したカード情報は、そのまま EC サイトでの決済に使用することもできるが、最近増えているのは、QR コード決済など、スマートフォン決済アプリの支払手段として登録し、高額商品や換金性の高い商品を購入して現金化したり、還元ポイントを窃取したりする手口である。いったんクレジットカー

※4
ダークウェブ
アクセスするために特定のソフトウェアや設定が必要で、通常のインターネットからはアクセスできないウェブサイト。クレジットカード情報などの他、銃器、違法薬物などの売買が行われている。

図 4　国内のカード情報流出事件発生状況



【年別の推移】

発覚年	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年（7月まで）
事件数	12	21	30	25	24	51	51	47
カード情報流出件数	138,717	123,527	255,689	564,844	283,374	375,479	90,147	185,857
1件あたり平均件数	12,611	7,266	9,132	23,535	12,321	7,362	1,768	3,957

ｆｊコンサルティング調べ

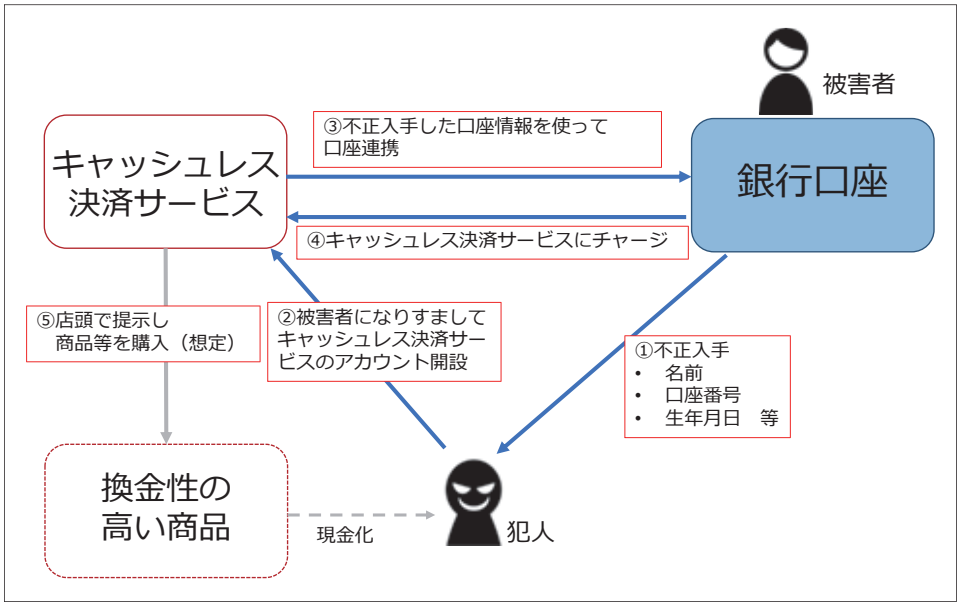
ドの登録に成功すると、EC サイトだけでなく、対面店舗での決済でも利用が可能になる。店舗では不正なクレジットカードで支払が行われていることに気づく術はなく、また商品をその場で持ち帰れてしまうため犯人の特定も困難となる。この手口は2018年の終わりに新規にサービスを開始した QR コード決済サービスで多発したことで広く知られるようになった。これがきっかけで、2019年4月にはキャッシュレス推進協議会※5により、アカウント作成時や決済手段登録時の本人認証について QR コード決済事業者が講じるべき対策を定めたガイドラインが公開された。

QR コード決済アプリのログイン ID とパスワードを乗っ取り、すでに登録されている決済手段を不正に利用する事件も発生している。ログイン ID とパスワードのリストはカード情報と同様にダークウェブで売買されており、複数のオンラインサービスでログイン ID とパスワードを使いまわしているような場合は被害に合う可能性が高くなる。2019年夏に大手流通業がサービスを開始した QR コード決済サービスは、開始から半月余りで3,800万円以上の不正利用被害が発生し、開始から1ヶ月でサービス廃止を決定した[5)]。

2020年には複数の QR コード決済サービスを含むキャッシュレス決済サービスで決済手段としてクレジットカードではなく銀行口座を登録することで、銀行預金が不正に引き出される事件が発生した。最も被害が大きかった QR コード決済サービスでは、11の銀行から128件、2,885万円の預金不正引き出し被害を認定している[6)]。また、複数のキャッシュレス決済サービスで預金不正引き出しをされた銀行もあり、最も被害の大きかった銀行では7つのサービスにおいて210件、4,940万円が不正に引き出されている[7)]。

キャッシュレス決済サービスを利用した銀行預金不正引き出しの手口を図示したのが**図5**である。まず、犯人は、預金者になりすましてキャッシュレスサービスのアカウントを開設する。その際に必要な名前、銀行口座番号、生年月日などの情報は、前述のフィッシングやダークウェブでリストを購入するなどしてあらかじめ入手しておく。アカウントが開設できたら、支払い手段として銀行の Web 口座振替サービスを利用して銀行口座を登録する。登録できたら、キャッシュレス決済サービスにその口座からチャージ※6し、タバコのカートンなどの換金性の高い商品を

図5　キャッシュレス決済サービス不正利用の手口



※5
キャッシュレス推進協議会
2018年4月に発行されたキャッシュレス・ビジョン[1)]の提言を受け、キャッシュレス社会の実現に向けた業界横断の推進組織として2018年7月に設立された一般社団法人。

※6
チャージ
電子マネーや QR コード決済サービスで、現金による支払いやクレジットカード決済、預金口座からの引き出しを事前に行い、利用可能な残高を増やすこと。

購入して現金化する。

銀行口座の登録時には、当然、本人認証が必要となる。被害にあった銀行の多くが銀行口座番号と4桁のキャッシュカード暗証番号のみ、あるいは加えて生年月日などの入手・推測が容易な情報による本人認証のみで銀行口座登録を認めていた。

暗証番号が不明だった場合も、4桁の数字であれば、最大でも1万回の試行で正しい暗証番号に一致して認証に成功することになる。当然、銀行側でも対策はしており、同じ口座番号に対して一定回数連続して暗証番号を間違えた場合は不正な試行とみなして登録をさせないようになっている。

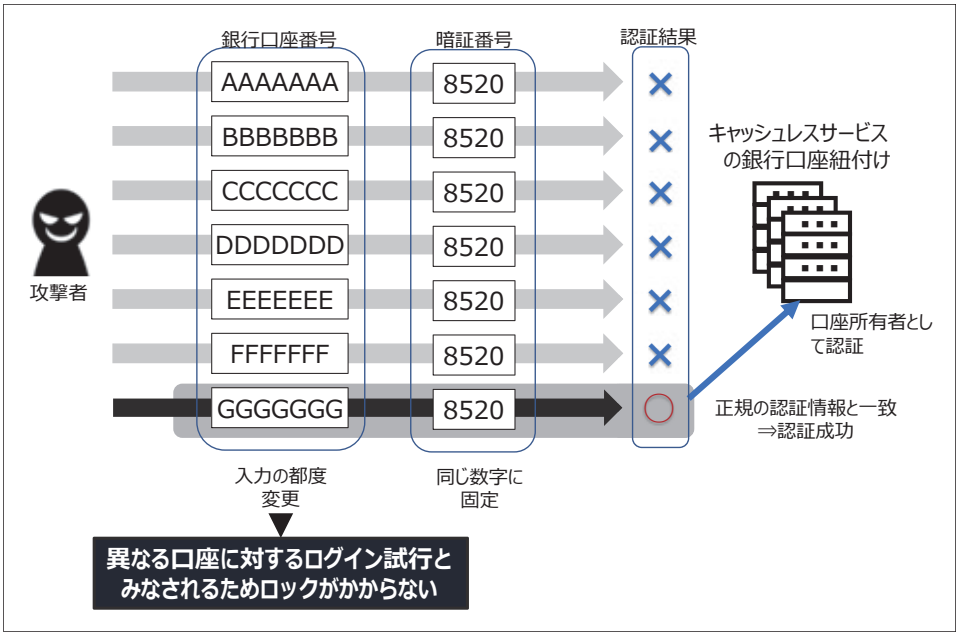
今回の事件では、逆に暗証番号を固定して銀行口座番号の方を総当りで入力する「リバースブルートフォースアタック」（**図6**）により認証が突破された可能性が指摘されている。1回の試行毎に銀行口座番号を変更することで別々の口座に対する認証試行となるため、「一定回数連続して暗証番号を間違えた場合は不正な試行とみなす」という対応では防ぐことができない。

5. キャッシュレス決済のリスクを回避するために

ここまで見てきたようなキャッシュレス決済のリスクを回避するために、消費者が留意すべきポイントを挙げる。

最も基本的な注意として、クレジットカード情報やID、パスワードなどを入力する場合は、信頼できるサイトやアプリであることを十分に確認することが挙げられる。クレジットカード情報を入力する場合は、ECサイトの正規の決済画面であることを、画面の見た目だけでなくブラウザのURLを見て確かめる。スマートフォンの場合、URLが全て確認できない、表示される文字が小さいなどの課題があるので注意が必要である。あるいは、アプリを利用する場合であれば、正規のアプリストアからダウンロードしたアプリだけを利用するといったことも必要である。また、フィッシング防止のため、メールで届いたURLについては怪しいものと考えてむやみにクリックしないことが重要である。不正利用のお知らせなど、緊急性を要する可能性が考えられるメールであれば、ECサイト

図6　リバースブルートフォースアタック



やクレジットカード会社の問い合わせ窓口に電話で問い合わせて確認する。その際も、メールに書かれた電話番号ではなく、EC サイト上に記載された問い合わせ窓口や、クレジットカードの裏面に書かれた電話番号を使用する。

複数のサービスで ID とパスワードの使い回しを行わないことも重要な対策である。ID についてはメールアドレスを用いているサービスも多い。変更が難しい場合は、パスワードを十分な長さで、かつ推測されやすい英単語などを避け、他のサービスと重複しないように設定することが望ましい。

また、キャッシュレスサービスの多くが、ID とパスワードに加えて、SMS（ショートメッセージサービス）やスマートフォンのアプリで提供されるワンタイムパスワード※7も認証要素として使用する「多要素認証」の導入を進めている。可能な場合は設定することで、決済情報を盗まれるリスクや不正利用のリスクは大きく軽減される。

もしも不正利用の被害にあった場合は、クレジットカードの場合、被害の届け出からさかのぼって60日以内の被害は原則としてクレジットカード会社から補償される。被害から時間が経ちすぎた場合は補償されないので、日頃からクレジットカードの利用明細をよく確認して、身に覚えがない決済がないかどうかをきちんと確認する習慣が大切だ。なお、補償を受ける条件として、警察への被害届と、クレジットカードの裏面に署名欄がある場合は自筆サインがされていることが必須となる。

QR コード決済については、全国銀行協会、日本資金決済業協会、キャッシュレス推進協議会などが中心となって、セキュリティ対策や利用者への補償に関する業界統一ルールが整備されつつある。4章で紹介した事件については、不正利用と認定された被害は銀行やキャッシュレス事業者により補償されている。

6. まとめ

QR コード決済など新しいキャッシュレス決済の登場により、クレジットカードの不正利用だけでなく新しい決済手段を悪用した銀行預金の不正引き出しなどの新たなリスクが生まれている。しかし、必要な対策を行い迅速に気づくことができれば、被害は原則補償される。過度にキャッシュレスを恐れず、必要なセキュリティ対策をした上で利用することが肝要である。

参考文献

1） 経済産業省：キャッシュレス・ビジョン，2018. https://www.meti.go.jp/press/2018/04/20180411001/20180411001-1.pdf
2） 野村総合研究所：キャッシュレス決済比率 28.5% のさらなる拡大に向けて，中小事業者への導入に伴うハードル低減を，NRI パブリックマネジメントレビュー，208，November，2020. https://www.nri.com/jp/knowledge/publication/mcs/region/lst/2020/11/04
3） （一社）フィッシング対策協議会：フィッシングに関するニュース，202. https://www.antiphishing.jp/news/alert/
4） （一社）日本クレジット協会：クレジットカード不正利用被害の発生状況 ,2021年9月．https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf
5） （株）セブン・アンド・アイ・ホールディングス：「7pay（セブンペイ）」サービス廃止のお知らせとこれまでの経緯，今後の対応に関する説明について，2019年8月1日．https://www.7andi.com/company/news/release/201908011500.html
6） 日本経済新聞：ドコモ口座，判明被害の補償完了　128件で2885万円，2020年10月28日．https://www.nikkei.com/article/DGXMZO65570570Y0A021C2000000/
7） 日本経済新聞：ゆうちょ銀，決済被害4900万円の補償完了　顧客210人に，2020年10月5日．https://www.nikkei.com/article/DGXMZO64627370V01C20A0EE9000/

せた●ようすけ

クレジットカードの国際的セキュリティ標準である PCI DSS の認定評価機関（QSA）代表、日本初の PCI SSC（Payment Card Industry Security Standards Council）認定フォレンジック機関（PFI）ボードメンバーを経て2013年ｆｊコンサルティング株式会社を設立。キャッシュレスやセキュリティのコンサルタントとして、講演・執筆活動を行う。直近の著書は『改正割賦販売法でカード決済はこう変わる』（日経 BP 社、共著）

※7
ワンタイムパスワード
認証の都度発行される、1回限りの使い捨てのパスワード。