クレジットカード取引における**セキュリティ対策**

第3回

カード情報の悪用

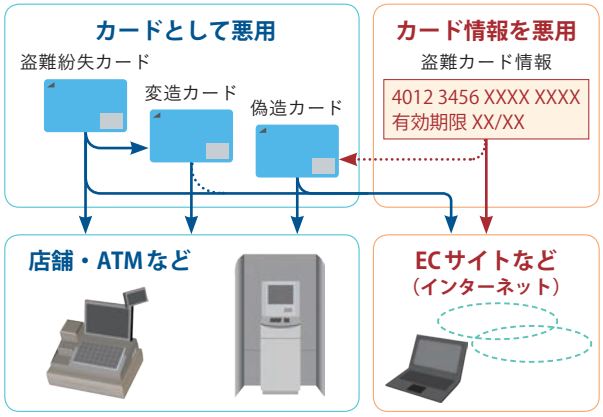
山本 正行 Yamamoto Masayuki **山本国際コンサルタンツ代表**
関東学院大学経済学部経営学科講師、決済サービス事業の企画、戦略立案を専門とするコンサルタント。消費生活相談員を対象とした研修も実施。講演、執筆多数。

先月号ではカード情報がどのように漏えいするのかを解説しました。今号では盗まれたカード情報がどのように利用(悪用)されるのか、その実態をみていきます。カードやカード情報の悪用手口はさまざまですが、その代表的な例を紹介します(図1)。当然のことながら、ここで紹介する手口はすべて問題行為で、そのほとんどは犯罪です。決してまねしてはならないことは言うまでもありません。

悪用手段① カード番号盗用

現在、被害が最も多いのが、カード情報をそのままインターネットなどで悪用する「カード番号盗用」などと呼ばれる手口です。残念ながら、カード番号、セキュリティコード、有効期限、利用者名の「基本4情報」があれば、多くのインターネット販売サイト(ECサイト)で誰もが利用できてしまいます。

図1 カード情報の悪用手口のパターン



カード情報を盗んだ者が、入手したカード情報を自ら悪用している可能性もあります。しかし、実際にはカード情報はダークウェブなど望ましくない市場で販売され、さまざまな人の手に渡っています。カード情報を盗む行為とその悪用は別々に、しかもまったく無関係の人間が行っています。現実にカード情報の闇市場が存在するという恐ろしい状態が指摘されています。

ダークウェブは検索サイトには現れず、仮にURLが分かったとしても通常のブラウザではアクセスできません。多くは犯罪や違法取引などを目的とするものですから、もしアクセス方法が分かったとしても興味本位で閲覧したり、利用してはいけません。しかし最近では一般の人がアクセス方法を知ることもあり、実際に利用しているケースもあるようです。海外では一般の人がダークウェブなどからカード情報を入手して、日常生活に利用するという犯罪も少なくありません。このような手口では、本来の利用者の手元にカードがあり、利用金額が比較的少額で目立たないため、利用明細を細かくチェックしないと見逃すこともあります。これを防ぐためにも、カード会社のウェブサイトで利用履歴を頻繁に確認することが重要です。

先述のとおり、カードの基本4情報がそろっていれば、多くのECサイトで支払いが可能です。さらにカード番号と有効期限のみでセキュリティコードや利用者名を打ち込まなくても決済可能なサイトもあり、危険な状態といえます。

被害を防ぐために、クレジットカード会社やECサイトは、カード利用時の認証方法を強化する対策を進めています。来年度施行される改正割賦販売法では、クレジットカード会社やECサイトなどに効果的な認証方法の導入を義務づけることが決まっています(別号で解説予定)。

悪用手段② 盗難紛失カードの悪用

財布やバッグをひったくられ、中に入っていたカードを悪用されることもあります。すぐに利用者が気づいてカード会社に連絡すればカードの利用を停止できます。しかし敵もさるもので、利用停止までの短い時間内に効率よく買い回り、用が済んだらバッグもカードも処分してしまいます。カードを紛失し、悪用される場合も基本的には同じ手口です。

通常、盗難紛失カードは、暗証番号は分からないためATMでは使用されず、サインで取引可能な店舗で使用されます。この対策として、最近は磁気カードからICカードへの切り替えが進んでいます。ICカードには暗証番号が設定され、ATMばかりでなく店舗の決済でも暗証番号を打ち込むよう求められます。ICカードであれば、たとえカードを盗まれても暗証番号が分からなければ利用されない可能性が高く、比較的安全です。

実際に、ヨーロッパ、オセアニアなどでは基本的にすべての店舗がICカードに対応しています。日本はICカードへの切り替えと店舗の決済端末のIC対応(IC化対応)が途上の段階にあるため、ICカードに対応していない店舗が残っています。そのため、改正割賦販売法では、加盟店などに対しIC対応を義務づけ、2020年までに100%達成することをめざしています。IC対応は盗難カードの悪用被害を抑制するには効果的でとても重要な対策です。今後の速やかな対応に期待しましょう。

しかし、先月号で解説したとおり、最近はATMや券売機などで暗証番号が盗まれ、直後にひったくられてカードが悪用される被害も出ています*1。このような事例では、暗証番号とカードの両方が盗まれるため、ICカードでも利用されてしまいます。主に海外で発生していますので、海外への渡航の際には注意を払う必要があります。例えば海外ではメインカードの頻繁な利用や携行を避け、海外利用専用の国際プリペイドカードを使う、などの対策が考えられます。万一の場合の被害を最小限に食い止める工夫です。

なお、盗難とは性質が少し異なりますが、家族や交際相手、友人などによる悪用も少なくありません。身近な人を疑うことはよくありませんが、家族や交際相手が簡単に自分のカードや財布に触れられるような管理は避けるべきでしょう。本連載第1回でも述べたことですが、家族や交際相手などによる悪用の場合、利用者本人が善良な管理義務を怠ったとされ、被害が救済されないケースがほとんどです*2。

悪用手段③ 偽造カード・変造カード

偽造カードが用いられる犯罪には、カード情報を使った偽造カード製造、輸送、買い回り、などのいくつかの過程があります。最終的に入手した商品の現金化まで含むので、ほとんどが相当な規模の組織犯罪です。

カードの偽造には、生カードと呼ばれる発行前のカード原盤の印刷、生カードにカード情報を書き込む処理、エンボス加工などを行う設備が必要です。正規のカードを製造、発行する印刷会社ほどの大規模な設備でなくとも一定以上の機能を持つ印刷装置や発行設備が必要です。それでも、これまでに海外に拠点を置く偽造カードの製造工場の存在が何度も確認されています。偽造カードの製造は犯罪行為ですので、摘発さ

*1 ウェブ版「国民生活」2017年7月号「クレジットカード取引におけるセキュリティ対策」第2回「クレジットカード情報はこうして盗まれる」
http://www.kokusen.go.jp/wko/pdf/wko-201707_10.pdf

れれば関係者は逮捕され、設備は差し押さえられます。しかし警察などが偽造カード工場に駆けつけてみたら既に撤収ずみ、ということもあります。そして、しばらくしてまったく別の地域で製造が始まった、という例もあります。

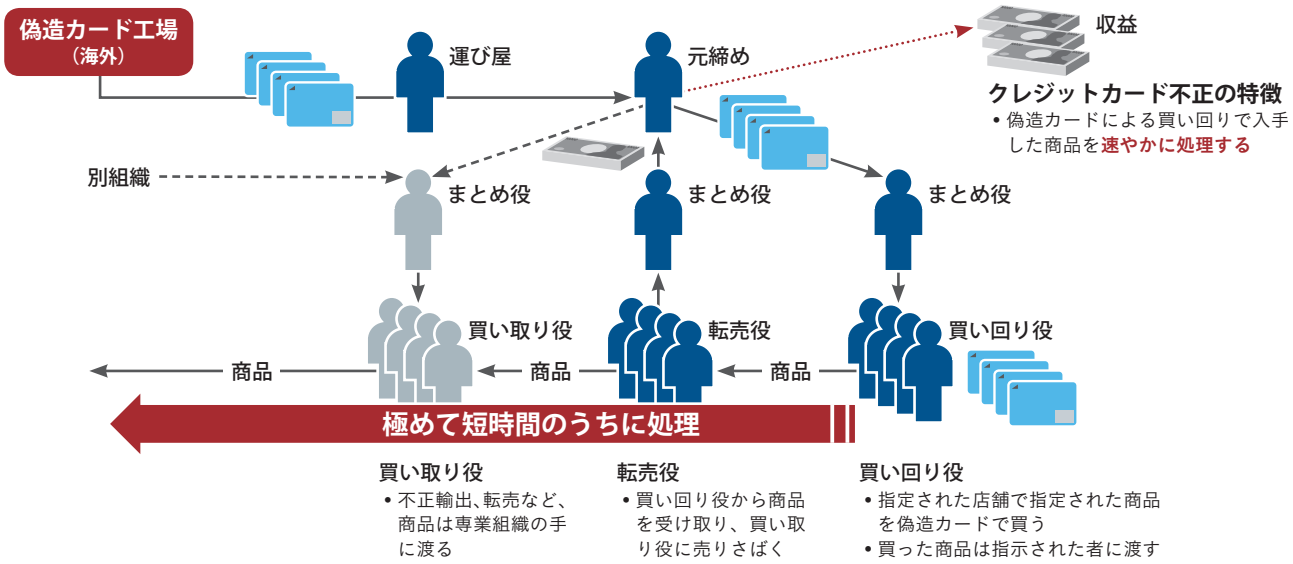
偽造カードはダークウェブなどを通して販売されることもありますが、特徴的な悪用パターンは、組織的な買い回り行為(図２)です。偽造カードは１枚ずつではなく一度に大量に製造され、買い回りを行う地域に運び屋を使って輸送します。日本でも、空港の入国審査で大量の偽造カードが押収されたことが何度もあります。入国審査をすり抜けて違法に持ち込まれた偽造カードは、買い回り役に渡され店舗での高額商品購入に使われます。そして入手した商品は転売役の手に渡り速やかに処理されます。一連の行為は短い時間で行われ、その後各役割を担う犯罪者は分散してしまうため、足がつかないことも多いのです。

昨年、日本でもコンビニエンスストアなどのATMで大量の偽造カードが使われ、現金が引き出されるという事件が発生しました。海外の金融機関がサイバー攻撃を受け、大量のカード情報が盗まれことがきっかけで、カード情報から大量の国際デビットカードが偽造されました。この事件ではATMの防犯カメラが実際に偽造カードを使い現金を引き出すようすをとらえ、それが証拠となり多数の逮捕者が出ています。逮捕者(出し子)は暗証番号を含め現金の引き出し方法などを詳細に指示された形跡があり、指示どおりにコンビニエンスストアなどのATMで現金を引き出したようです。問題の偽造カードは「白カード」と呼ばれるデザインのない白地のカードでした。白カードのままでは店員の目に触れる店舗で利用できないため、ATMでの預金引き出しに集中したというわけです。

最近は減少傾向にありますが、盗難紛失カードのカード券面を加工したり、記録されている磁気データを書き換える「変造カード」の悪用もあります。盗難紛失カードは利用停止措置が取られると使えなくなるので、カードの磁気情報をまったく別のカード情報に書き換えて利用し続けるという手口です。これを防ぐため、最近のカードの磁気情報は簡単に書き換えられないようになっています。

次号では、ICカードによるセキュリティ対策について解説します。

図２ 偽造カードの買い回りパターン(例示)



＊２ ウェブ版「国民生活」2017年６月号「クレジットカード取引におけるセキュリティ対策」第１回「クレジットカードの不正使用とセキュリティ対策」
http://www.kokusen.go.jp/wko/pdf/wko-201706_11.pdf