警鐘レポート

銀行キャッシュカード スキミング防止セオリー13

評論家・小沢遼子さん67は暗証番号盗み見で410万円被害。〝知らない間に残高0円〟事件が急増中

カード偽造団から押収された大量の偽造カードとパソコン。

「まさか実際に私が被害に遭うなんて、驚いて血の気が引きました。もう悔しくて、悔しくて」

と悪夢のような出来事を振り返るのは、評論家・小沢遼子さん（67才）。思ってもみなかったキャッシュカード犯罪に巻き込まれ、怒りが収まらない。小沢さんは昨年11月初旬の土曜日に自宅近くのATMで現金を引き落とし、徒歩で帰宅しているところを狙われた。

「突然男に〝鍵束が引っ掛かりました〟と私の着ていたカーディガンの左裾を引っ張られました。

仕方なく足を止めていると、右肩にさげていたショルダーバッグにさっと触られた感触がしました。すぐ振り向くと、ダークスーツ姿の男2人組が私の右側をすっと通り過ぎていったんです」

オレオレ詐欺の被害が伝えられる一方で、銀行のキャッシュカード情報を盗んで口座預金を盗むスキミング被害が続出。クレジットカードなら補填してくれるものの、銀行カードはそれで残高が0になっても補償は一切なし。しかも犯人たちの手口はますます巧妙になるばかり。「自分のお金は自分で守る！」必読の自衛策をお教えします。

帰宅後、ショルダーバッグ内のカードケースがなくなったことに気づいた小沢さん。すぐに、カード使用の中止を電話連絡したが、時すでに遅し、何とカードを盗んだスリは、小沢さんがATMを利用したわずか十数分後に、合計410万円もの大金を引き出していたのだ。

「銀行の防犯カメラを見せてもらうと、私がATMで引き落としている最中に左斜め後方までじりじりと近づいてくる男がいました。**私は老眼なのでATMの操作パネルから体を離して入力するのですが、そのときに手の動きで暗証番号を盗み見されていたのです**」

銀行のキャッシュカードを使用した不正預金引き出しによる被害額は、'03年度は2億7200万円だったが、**'04年度は4～9月間ですでに4億6100万円とわずか半年で倍増に達する勢いだ**（日本銀行協会調べ）。

「クレジットカードに比べてキャッシュカードは被害に遭いにくいとされていましたが、**他人が知らないはずの暗証番号を入力されて、ある日突然大金を引き出されるケースが続出しています**」（カード被害に詳しい喜多英博弁護士）

さらに不気味なのは、カードは盗まれず、ちゃんと手元にあるのに、被害に遭ってしまうケースだ。

スリにカードを盗まれ、現金410万円を引き出された小沢さん。銀行の対応に対する不満は収まらない。被害に遭った通り（写真上）は、当日、人通りも多かったという。

スキミングは次々新種の手口が

なぜこんなことが起こるのだろうか。謎を解く鍵は、カードの磁気情報を不正に読みとるスキミング技術の飛躍的な進歩にある。超小型のスキミング機材を忍ばせ、被害者の隙をみて、その場で情報を盗み取り、素早く別のカードに情報を移し替えて偽造カードを作製する。被害者の手元にカードがありながらも預金は引き出されてしまうのだ。

仕掛け式スキミング

'95年から始まった〝仕掛け式スキミング〟では、店舗などのカードリーダーの中にスキミング基板をしかけ、蓄積されたカード情報を後に回収する。従来クレジットカードに使われていた手口だったが、最近になってキャッシュカードにも応用されている。

昨年8月、愛知県半田市の主婦が自宅近くの都銀ATMを訪れると、入り口に『防犯のため、この機械にカードを通してください』という貼り紙があった。主婦がカードを挿入すると、その後知らない間に口座から合計約1000万円もの大金が引き出された。識別装置に仕掛けられたスキミング基板から、偽造カードが作製されたものとみられている。

無線式スキミング

この手口は、さらにやっかいだ。ATMの通信回線に信号傍受装置と送信機を仕掛け、盗み取ったカード情報を電波で飛ばしてパソコンで受信する。

「電話工事を装った犯行グループが電柱に登り、ATMにつながる電話線から信号を傍受してアンテナを搭載した車に無線電波を飛ばすと、20～30メートル先の車の中でカード情報を受け取ることができます」（情報漏洩防止コンサルタントの藤田悟さん）

犯人たちはATMの設置工事にも目を向けているという。

「工事中、お昼休みなどで施工業者が出払うことがあります。現場にはむき出しになった通信回線が放置されており、ここをねらってスキマーを仕掛けるのです」（NPO法人日本情報安全管理協会・伏見正浩理事）

非接触式スキミング

究極の手口が、一昨年から囁かれているこの〝非接触式スキミング〟だ。

「これはカード自体から磁気情報が発せられる非接触型ICチップ入りのカードに有効な手段。磁気情報をたばこの箱くらいの大きさのスキミング機材で読み取るのです」（前出・伏見理事）

非接触型ICチップとは、JR東日本のSuicaや企業の入退室管理のIDカードなどに利用されており、読み取り機にカードをかざして反応させる仕組み。非接触式のスキミング機材は、この読み取り機を改良したものだという。

この方法だと、**エレベーターや満員電車など混雑した所で財布のはいっている胸ポケットやハンドバッグの上からスキマーをかざすだけで、容易にカード情報を盗むことができる。**

暗証番号はこうして盗まれる

しかし、これらの方法で偽造カードを作製しても、暗証番号はわからないはずだが、犯人はどうやって暗証番号を盗んでいるのだろうか。前出の伏見理事が解説する。

「小沢さんのケースのようにATM入力の際に盗み見るといった古典的な方法から、ATMに小型カメラを取り付けて盗撮する手口もあります。また、カードの利用明細書に記されたデータからカード情報を得ることも可能です」

また、犯人が警察や銀行員を装って、電話で、暗証番号を聞き出そうとする大胆なケースもあるという。

また、現在普及しているキャッシュカードには、暗証番号のデータは登録されていないが、10年以上前の古いカードの中には、暗証番号の情報が含まれているものも存在するというから注意したい。

「昭和62年に全国銀行協会がカードの磁気情報から暗証番号を外す『ゼロ暗証化』の通達を出しました。**しかし、いまだに昭和60年代前半のカードを使っているとスキミングされただけで、暗証番号も盗まれてしまいます。**新しいカードに作りかえましょう」（NPO法人日本情報保全協会・木村理事）

テレホンバンキングを悪用した新手口も登場。利用する際の「ピ、ポ、パ」というアナログ回線のダイヤル音から暗証番号が入手できると前出の木村理事はいう。

「屋外にある電話回線をつなぐボックスに機械を仕掛けておけ

家出歴43年。河原オジさん 荒野の43年 加村一馬 定価1,260円(税込) 絶賛発売中! 小学館

ば、電話先の銀行や暗証番号を入手できます」

最近利用者が増えているネットバンキングでも、被害が出ている。

「インターネット喫茶やホテルのフロントなど公の場にあるパソコンには、キーロガーという叩かれたキーボードすべての記録を残すプログラムが仕掛けられている場合があります。犯人はプログラムを仕掛けて立ち去るだけで、後は自動的に集めた情報を自分のパソコンに転送できます」（グローバルセキュリティエキスパートの山崎文明代表取締役）

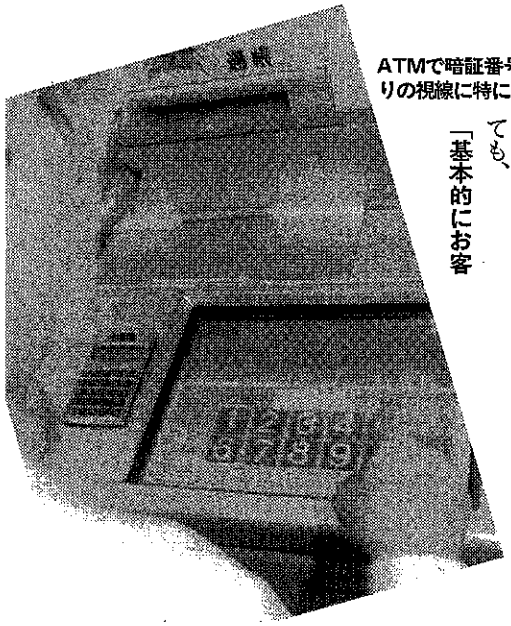
こうした場所でオンラインバンキングを利用すると、口座番号や暗証番号がすべて記録されて、他人に知られてしまうので要注意だ。

預金者がこれだけ危険にさらされているのに、銀行業界の対応はきわめて鈍い。4大メガバンクに預金者がこのような被害にあったときの対応を聞いてみても、

「基本的にお客さまの責めによるものであれば、我々が積極的に補塡していることはありません」（UFJ銀行）、**「現時点では被害額を補塡する枠組みはできていません」**（東京三菱銀行）、**「約款の規定に従った手続きを取っています」**（みずほ銀行）、**「警察の捜査の進展を踏まえ、キャッシュカード利用規定に基づき検討することになります」**（三井住友銀行）との回答。実際に銀行は、約款やカード取扱規定に記された『カードが偽造であっても預金は返還しません』という文言を盾に、決して被害額の補塡はしないと前出の喜多弁護士はいう。

「約款の但し書きには『預金者の側にカードと安全管理について落ち度がない場合にお金を返します』とあります。これを銀行側は『銀行側に落ち度がない限り』とも読む。つまり、預金者側がカードの管理を完璧にしていたと証明しなければならないのです。**預金者から預かったお金を間違えて他の人に渡しておいて、『すみません』のひと言もない。常識的には考えられないことです」**

まさか何時何分にカードがどこにあったかまで記録している預金者はいないだろう。しかし、これが現実なのだ。



ATMで暗証番号を押すときは周りの視線に特に注意すべきだ。

スキミング防止のための13のセオリー

警察に押収された、手のひらに載るほど小型のカードデータ読み取り機。カードを通してスキミングを行う。

いまや私たちの生活の一部となっている銀行キャッシュカード。預金者が虎の子の預金を守るための対処法をまとめた。

①必要なとき以外はカードを持ち歩かない。

②ATMで数か月に一度は暗証番号を変更する。その際、番号は誕生日、電話番号、車のナンバーなど類推されやすい番号も避ける。忘れないようにと、暗証番号をカードの裏面に書いておくのはもってのほか。

③一口座あたりの預金残高を少なくする。預金は複数の口座に分け、カードを作る場合は、すべて違う暗証番号にする。

④ATM利用時は、周囲の人や小型カメラの有無に細心の注意を払う。

⑤三井住友銀行など、ATMで1日の引き下ろし限度額を0～300万円まで、自分で設定できる口座もあるので、利用する。普通の口座でも1日の引き出し限度額が200万～500万円（銀行によってさまざま）などと設定されているが、限度額を低く設定しておけば、犯人も一度に大金を引き出すことができない。

⑥大口口座にはカードは作らない。預金の引き出しは印鑑と通帳で行う。

⑦10年以上前の古いカードは銀行窓口で、必ず交換する。不要なカードは、磁器ストライプにハサミを入れ、処分する。

⑧通帳記入をこまめに行う。犯人は目立たぬよう数回に分けて引き出すケースもあるので、頻繁に残高をチェックしておく。

⑨銀行員や警察官が暗証番号を尋ねることはないので、聞かれても絶対に答えない。

⑩テレホンバンキングを行う場合は、ハッキングされにくいデジタル回線にする。

⑪カードは金属性のケースに入れて持ち歩く。非接触型のスキミング防止に有効。

⑫他人のパソコンに口座番号や暗証番号を入力しない。

⑬少しでも不審なことがあったら迷わず素早く銀行に連絡してカードの使用をとめてもらう。警察にも届ける。

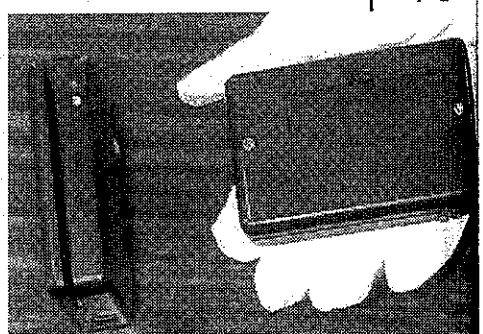
しかし、預金者の自己防衛にも限界がある。前出の小沢さんも憤りを隠せない。

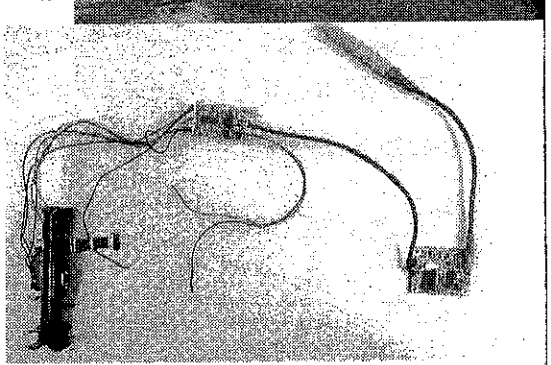
「銀行なんて使うものじゃないですよ。これだけ被害が多いのに、何の対策もしていないばかりか、補塡もない。預金者は盗られてしまったらもうおしまいだなんて。せめて何パーセントかは銀行が補償するべきです」

安心のためわざわざ銀行へお金を預けているのに、こんな対応では、現金を抱えて寝た方がよっぽどましだ。

「銀行も抜本的な対策として、クレジット会社のように保険にはいることを検討すべきだと思います」（前出・喜多弁護士）

しかし、スキミング被害に遭わないためには、ともかくあなた自身でしっかりカードを管理するしかないのだ。





都内のホテルで発見されたカードからスキミングしたデータを無線でとばす電波式スキマー。