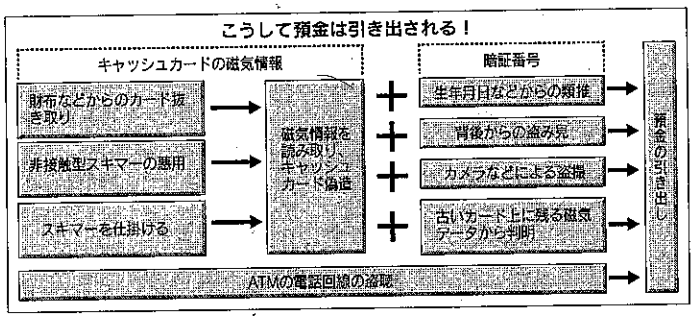
（日刊）
日本経済新聞
2月13日
日曜日
発行所　日本経済新聞社
東京本社〒100-8066☎(03)3270-0251
東京都千代田区大手町1-9-5
大阪本社〒540-8588☎(06)6943-7111
大阪市中央区大手前1-1-1
名古屋支社〒460-8366☎(052)243-3311
名古屋市中区栄4-16-33
西部支社〒812-8666☎(092)473-3300
福岡市博多区博多駅東2-16-1
札幌支社〒060-8621☎(011)281-3211
札幌市中央区北1条西6-1-2

手口ますます巧妙に

▼ATMの通信を盗聴
▼電車内でスキミング



「防犯のため、この機械にキャッシュカードを通して下さい」。昨年八月、愛知県半田市にある現金自動預け払い機（ATM）コーナーの入り口に、こんな紙が張られていた。三十代の主婦は疑いもせずにカードを通した。数日後、口座から二十万円が消えていた。

実は、この機械は預金口座の磁気情報を盗みとる装置。ATMの周りはガラス張りだったため、タッチパネルの操作時に押した数字を盗み見された可能性が高い。口座情報と暗証番号を入手した犯人にまんまと預金を引き出されてしまった。

口座情報を不正に読み取る「スキミング」。英語のskim（すくい取る）が語源で、磁気部分に記録された口座番号などの情報をスキマーという装置で読み取る。盗んだ情報をパソコンで解析、カードライターという機械で情報を転写すれば偽造カードができあがる。スキマーやライターは秋葉原などで数万円で手に入る。

磁気情報は、カードを抜き取って盗まれることが多い。飲食店などでハンガーにかけた上着のポケットから抜き取って情報を読み取った上で、元に戻す手口だ。冒頭のように預金者にスキマーを通させる手口もある。

カードを身に付けたまま、情報を盗まれるケースもある。犯罪実態を調べている特定非営利活動法人（NPO法人）、日本情報安全管理協会（東京・港）理事の伏見正浩さんは「表面から出る微弱な電磁波を読みとる非接触型スキマーが出回っている」と指摘する。満員電車などでスキマーをポケットやカバンにかざすだけで、口座番号などがわかってしまうのだ。

ただ偽造されたとしても、それだけでは預金を下ろせない。暗証番号が必要だ。自分しか知らないはずの数字が、どうして漏れるのか。

よくあるのが生年月日や電話番号などから類推されるケース。昨春、都内で被害にあった五十代の女性は「口座をつくるとき、銀行員から『面倒でしたら誕生日にしてください』といわれた」と悔る。

類推できないはずなのに被害に遭った例もある。二〇〇三年八月。大阪府豊中市のAさん宅に泥棒が入り、十枚のカードを盗まれた。暗証番号はすべて同じだったが、個人情報とはなんの関係もない数字にしてあった。にもかかわらず翌日までに約七百万円の預金が全額引き出された。

防犯カメラの映像をみると、犯人は一度も間違えずに数字を押している。引き出す前に番号を知っていた公算が大きい。実は、十枚のうち、二枚が二十年以上前に発行されたものだった。

このケースでは、古いカードから番号を知られてしまった疑いが濃厚。一九八七年以前に発行された場合、磁気部分に暗証番号がそのまま書き込まれていた。八八年以降、各銀行は「ゼロ暗証化」と呼ばれる対策を進め、番号情報を書かないようにした。専門家は「古いカードを持つのは危険」と口をそろえる。

番号を盗む古典的手口がATM操作の盗み見。昨春には盗み見されたとみられる女性が、後をつけられてカードを強奪された事件が起きた。のぞくだけでなく、ATM周辺に小型カメラを仕掛ける手口も横行しているという。

「最も怖いのは通信回線の盗聴」。偽札鑑別機の開発などで知られる松村テクノロジー（東京・台東）社長の松村寧秀さんは最新手口に警鐘を鳴らす。銀行のシステムとATMの間の「一部はアナログの電話回線でつながっている」。そこに盗聴器と無線発信器を仕掛け、近くに止めた車の中で受信すれば、暗証番号まで漏れてしまう。これではいくら管理していても犯罪を防げない。

主な金融機関の対策

みずほ銀行	ICカード発行（3月から）
三井住友銀行	21日からICカード発行、取引などの監視システムを導入
東京三菱銀行	手のひら静脈認証を使ったICカードを発行
UFJ銀行	ICカード発行、3月からは無料に
新生銀行	カード交換は無料
スルガ銀行	他行やコンビニでのATM利用を停止できる（3月から）
大垣共立銀行	カード交換は原則無料。総合口座の貸越限度額を任意に設定できる
北国銀行	偽造被害に対し、100万円を上限に補償
イーバンク銀行	入出金時に通知メールを即時送信。カード利用時間帯を制限できる
郵便局	ゆうちょくらぶ（年会費350円）に加入すれば、偽造被害に対し100万円まで補償

銀行は補償してくれない

「銀行は全く補償してくれなかった」。被害にあったHさんは怒りを隠せない。他人にわかりにくい暗証番号を使い、カード管理にも細心の注意を払っていたが、銀行は「約款で定めているから」の一点張りだという。

銀行の約款は通常、「暗証番号が一致すれば、盗難や偽造であっても（銀行は）責任は負わない」と規定している。ただし偽造の場合は「カード及び暗証番号の管理に預金者の過失がないと確認できた場合はこの限りではない」などと書かれており、一見、補償に応じてくれるようにも読める。しかしこれは「預金者が自分に過失がないことを証明しなければならない」（弁護士の喜多英博さん）という意味。どこで数字が漏れたかなどが分からない預金者にとって不利な規定だ。

被害に遭っても預金者の負担は一定額まで、という欧米のような預金者保護ルールはない。盗難保険を導入する銀行もあるが、ほとんどの場合、偽造は対象外。偽造でも補償するのは北国銀行などごく一部に限られる。

大切な預金 どう守る

偽造キャッシュカード犯罪多発

偽造キャッシュカードを使って預金を盗む事件が多発している。ゴルフ場を舞台にした偽造団が一月に逮捕され、犯罪の一端がようやく明るみに出た。預金情報がどのように盗まれるか。預金者はいかに対策をとればいいのか。偽造の手口と対策を探った。

■暗証番号 まめに変更
■安全性高めた口座も

「暗証番号は毎月変えている」。東京都のNさん（47）は昨年夏に偽造犯罪の被害に遭って以来、対策に余念がない。四つある預金口座のうちキャッシュカードを作ったのは一つだけ。番号は両親の誕生日の組み合わせを基本に定期的に変更している。

預金を守る最後のとりでが暗証番号。生年月日、電話番号など個人情報から類推できる数字は危険だ。生活行動研究所（東京・千代田）所長の西ケ谷葉子さんは「他人が想像できない数字にして、時々変えるべきだ」と助言する。ただ頻繁に変えると忘れてしまうこともある。

どうやって設定すればいいだろう。

Nさんのやり方はこうだ。父親の誕生日が十月二日、母親が三月二十四日だとすると、これを組み合わせて「0224」とする。この数字を自分なりの法則で変更する。番号を設定した月が十一月だとすると「0224+11 24+11」で「1335」。十二月は「1436」、二月だと「0426」といった具合。「これなら無理なく覚えられる」とNさん。

暗証番号は現金自動預け払い機（ATM）でも変更可能。ただ後ろからのぞき見されたら元も子もないので、変更の際は細心の注意を払おう。銀行員や警察官を装って電話や電子メールで番号を聞き出す手口もある。大手銀行は「電話などで暗証番号を聞くことはない」と口をそろえるので、注意すべきだ。

金属ケースに収納

カード管理も重要。西ケ谷さんは「外を持ち歩くのは札束を抱えて歩いているようなもので、必要時以外は持ち歩かない」よう訴える。

持ち歩く場合は「金属製のケースに入れるのが望ましい」（日本情報安全管理協会理事の伏見正浩さん）。電磁波を遮断し、ポケットの上からカードにかざすだけで情報を読み取る非接触型スキミングを防ぐためだ。

十七年以上前に発行された古いカードだと、磁気部分に暗証番号の情報が書き込まれている場合がある。古い場合は、新しいものに交換するのが一番。交換には一枚千円程度の手数料がかかる銀行が多いので、一度口座を閉鎖し、新しく口座を開いた方が手数料をとられなくて済む。

対策の決め手といわれるのが偽造が困難とされるICカード。しかし単にIC化するだけでは万全とはいえない。

「磁気で引き出せるなら磁気カードと同じ」。松村テクノロジー（東京・台東）社長の松村喜秀さんはIC化の「落とし穴」をこう指摘する。大半の銀行は、IC化しても、表面に磁気情報を残している。ICに対応したATMがまだそれほど普及していないからだ。つまりIC化しても、預金情報をスキミングされる恐れがある。

UFJ銀行は昨年十一月から、ICカード上の磁気データを使って一日に引き出せる金額を、預金者が設定できるようにした。この限度額をゼロにしておけば、磁気データを盗まれる被害はなくなる。

残高照会を頻繁に

「もっと早めに気付いていたら……」。昨春、三千万円を盗まれた東京都のYさんはこう悔やむ。Yさんの預金口座の一日の引き出し限度額は五百万円。犯人に六日連続で引き出された。

対策として多くの銀行が引き出し限度額を自由に設定できるように変更し始めており、引き下げ手続きをとろう。ただ限度額を十万円にしても一カ月気付かなければ三百万円盗まれる。引き下げと同時に「残高照会もマメにしよう」と西ケ谷さんは強調する。

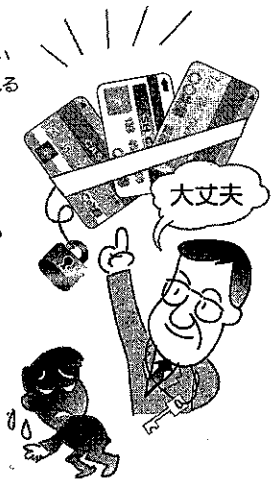
カードのある預金口座に、大金を預けておかないことも大切。株式や債券などに資金を分散したり、預金の場合なら定期預金へ移したりすべきだ。ただ普通預金残高がゼロでも、定期預金を担保にしてATMから現金を引き出せる預金があるので注意が必要。大垣共立銀行では、貸越限度額をゼロから一千万円の間で自由に設定できるサービスを提供している。

普通預金に一定額を預けておく必要があるなら、安全性を高めた口座を利用しよう。スルガ銀行の「バイオセキュリティ普通預金」は、入金はATMでできるが、出金は専用窓口だけ。しかも手のひらの静脈認証を使ったシステムだ。郵便局では手続きすれば窓口からしか引き出せないようにできる。

偽造対策してますか？

～自分でできる17項目～

1. カードは必要なとき以外は持ち歩かない
2. 飲食店などで、カードを安易に他人に手渡さない
3. カードを持ち歩くときは金属製のケースに入れる
4. 暗証番号は誕生日や電話番号などにしない
5. 暗証番号はときどき変える
6. 暗証番号は誰に聞かれても教えない
7. カードの暗証番号をロッカーなどで使わない
8. 持っているカードはすべて違う暗証番号にする
9. 17年以上古いカードは交換する
10. ATMを使うときは周りの視線に注意する
11. 万が一に備え、1日に引き出せる額を制限する
12. ICカードは磁気で下ろせる金額を下げておく
13. 通帳記入はマメに
14. 生活資金用の口座と、貯蓄用を分ける
15. 大口の預金口座にはカードを作らない
16. 総合口座は貸越限度額を下げる
17. キャッシング機能がついていても、不要なら解除する



万一、被害に遭ったら…

銀行に被害届提出求めて

被害に遭ったらどう対応すべきか。まずカードを発行する銀行に電話し、預金の引き出しを停止することが肝心。あらかじめ連絡先を確認しておこう。全国銀行協会では加盟行の連絡先を一覧表にしている。アドレスはhttp://www.morebank.gr.jp/category_d/index_kinkyu.html。

法律的には銀行が被害者となるため、被害届を出すよう銀行に要請する必要がある。届けを出すのは、預金を引き出されたATMを管理する銀行。口座はA銀行でも、B銀行のATMから引き出されたなら、被害届はB銀行が出す。銀行への連絡と同時に、警察にも速やかに連絡すべきだ。

ATMが映っている防犯カメラの映像を確保するよう、銀行や警察に要請することも忘れてはいけない。通常、防犯カメラの映像は一週間で消えてしまう。銀行の連絡の不備や、警察の対応の遅れで映像が消えてしまったケースもある。

被害者の会「ひまわり草の会」（http://www.yy-com.jp/hima.wariso/）事務局は日本情報保全協会、☎06・6946・7236）では情報交換を呼びかけている。