

08年3月24日

## 個人認識情報詐取

(JSS の和訳)

3月にはカナダ政府が詐偽防止をキャンペーンする月であり、多くの機関や報道が注意を促している。この種の犯罪はきわめて多様な方法で行われるが、その多くは被害者の欲心をそそる、ないしは危機感ないしは義侠心をそそる話を持ち掛け、ことの信憑性を検討する時間を与えずに行動を取らせるやり方が基本である。また電話やインターネット、手紙など発信者の身元が判明しにくい媒体を使って行われることも稀ではない。

ここでは最近急激に増加しているといわれる Identity Theft (個人認識情報詐取) について公的機関が広報している情報を元に、被害を防ぐ方法を述べる。

### Identity theft とは？

詐取などによって盗み出した個人情報を使って、被害者の銀行口座などから現金を盗み取る、ないしはクレジットカードなどを不法に使用して金品を盗み取る犯罪は、預金取り扱いの利便性が大幅に高まり、インターネットなどが大幅に普及した現代できわめて多くの被害をもたらしている犯罪である。

内閣に付属する Office of Privacy Commissioner (OPC) のウェブサイトによると、不正なテレマーケティングや電話などを使った詐欺被害通報のために州警察、RCMP、公正取引委員会が 1993 年に発足した通報センターである Phonebusters は、2006 年中に identity theft による被害 7,800 件、被害総額 16 百万ドルを超える通報を受け付けており、ま

たこの数字は全被害の約 5% に満たないのではないかと推測している。推測が正しいとすると、被害総数は 15 万件以上、被害総額は約 320 百万ドルにも及ぶことになり、莫大である事が分かる。2003 年に Ipsos Reid は、カナダでは一生の間で人口の約 9% (2.7 百万人) が被害を受けるという調査結果を発表しているし、FBI は米国での被害が年間 5 億ドル、10 百万件に及ぶとしているという。なお、被害は個人ならびに団体共に起きている。

### 手口(一般消費者の場合)

銀行カードやクレジットカードなどで個人認識のために使われる情報は氏名、住所、生年月日、SIN (Social Insurance Number)、多くのパスワードなど多種である。関係する多くの機関が、これらを不法に盗み出すきわめて多様な手口を紹介し、注意を促しているが、以下はその一部である。

- ごみ漁り  
家庭などから出されたごみの中に、情報が抹消されずにある書類などを見つけるやり方。情報は細断する等して読めない状態で捨てよう。
- Skimming (掬い取り)  
デビットカード、クレジットカードなどを使用する際に、係り員が情報盗み取りの目的で別の端末装置を操作するケース。防止するためにはカードの読み取りは自分の手で行うこと。なお、この場合、カード操作に必要なパスワードは、肩越しの盗み見、天井などに設置されたビデオカメラで読み取るものが多い。
- ATM 操作  
銀行などの現金引き出し機のカード読み取り部分に、情報読み取るために付加装

置を取り付け、他に上記同様ビデオカメラなどをセットしてパスワードを読み取るやり方(この場合、キーパッド打ち込み状況を外部から監視している場合がある)。

- ・ インターネットの悪用。  
正規の発信者を偽装したメールを送りつけ、情報詐取を目的にしたサイトに誘導したり、連絡先を指定し電話をかけさせたりして、情報を盗むやり方。なおこの方法は、いわゆる前金詐偽(大金や物品を入手できる僥倖と偽って、取扱料や前金を詐取するやり方)などが重複している場合が多い。
- ・ カードなどの盗み出し。  
財布などからカードを盗みだすケースはもとより、新規発行などで郵送されたカード、郵送された事前承認済みのクレジットカード発行依頼書などを郵便箱から盗み出し、情報を入手する方法。
- ・ 住所変更偽装  
被害者を装って住所変更手続きをし、個人認識情報を伴う郵送物を入手する方法。
- ・ 企業などのデータベース侵入。
- ・ 社交ネットワークの利用。

## 被害防止策

情報流出および流出した情報によってもたらされる被害は大別すると被害者が何らかの行動をとることで起きる場合と、被害者が感知できない状況で行われる場合とに分けられる。被害を避けるためには上記したような手口で情報を詐取されない事が第一であるが、たとえば金融機関やネット販売機関などのデータベースが盗み出されるなどのケースでは、被害者はなんら対策を立て得ない。したが

って被害を受ける可能性は誰にもあるという前提で日常を過ごす必要がある。

### 情報を盗み出されない対策

情報を盗み出されないためには、上記した手口が無効となるような行動をとる必要がある。たとえば、銀行やクレジット会社、政府機関からの手紙などは処理が終わったら細断するなどして読み取りができないようにしてから廃棄する、郵便物を長期に郵便箱に置かない、ないしは郵送物を他人が手に入れやすい場所に放置するなどを避けることも重要である。また、インターネットや電話、手紙を通じて要請された情報については、相手の身元と情報の用途を確認、納得できた場合にのみ伝えること(これらが確実に確認できる事が決め手である。相手が電話機の向こうでどう名乗っても確認は出来ない)。

また何らかの事由で個人認識情報を他人に伝える場合、相手の身元を確認(相手の指示に従って行うのではなく、信頼できるリストなどを使って自ら連絡先を選ぶ事が肝要)することも習慣としたい。筆者は以前、銀行と称する相手からインターネットを通じて口座確認の要請があり、銀行の窓口に問い合わせたところ、銀行はそういった情報をインターネットを通じて要求することは一切無いので無視して欲しい旨伝えられたことがある。

日常、個人確認のための多くの情報が盛り込まれたカードやパスポートなどを多数持ち歩くなども避けなくてはならないことの1つだし、一方所持品を常時確認することも必要な手立てだ。そして、そういったものを盗まれないように対策すること、万一盗まれたり紛失した場合躊躇せずに関係機関に通報し、対策をとってもらうことも必要だ。また、支払いカウンタ

一などでパスワードを打ち込む場合、覗き見や撮影を避けるためにキーパッドを手のひらで覆って行うなどの注意が大切だ。ATM を利用する場合には、機械に不審な付加装置が装着されていないか、周囲に不審な人物や車がいなかを確認すること。

なお、パスワードなどをメモすることは出来るだけ避け、仮に何らかの理由でそうした場合、メモを放置しないことはもとより、廃棄の際にも十分注意しなくてはならない。

#### 被害を防ぐ方法

銀行やクレジット会社の計算書は、面倒がらずに全項目確認し、不審な項目については発行機関に問い合わせること。これを怠らなければ救済できた被害が、怠ったゆえに莫大になった例は多数ある。自身が日常の行動からは感知できない被害も、このやり方で避けられる場合が多い。

一方、詐欺的な方法での犯行は被害者を、必要な手順を踏まず即応しざるを得ない状況に追い込んで行われる場合が多い。一攫千金の機会のもとより、義侠心や危機状態をあおられ、時間の余裕が無い緊急事態と伝えられても、いったん時間をとり、信頼できる機関などに確認を取ってから行動する事が必要である。

参考になるウェブサイト;

[www.safecanada.ca/identitytheft\\_e.asp](http://www.safecanada.ca/identitytheft_e.asp);

Government of Canada

[www.privcom.gc.ca/fs-fi/02\\_05\\_d\\_10\\_e.asp](http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp);

Office of Privacy Commissioner of Canada

[www.rcmp-grc.gc.ca/scams/identity\\_theft\\_e.htm](http://www.rcmp-grc.gc.ca/scams/identity_theft_e.htm);

[//ww2.ps-sp.gc.ca/publications/policing/Iden](http://ww2.ps-sp.gc.ca/publications/policing/Iden)

[tity\\_Theft\\_Consumers\\_e.asp](http://www.safecanada.ca/identitytheft_e.asp); Public Safety  
Canada