情報技術を悪用したサイバー犯罪の対策とは？

Q 最近、新聞やテレビ、雑誌において、信じられないような巧妙な手口の犯罪がたくさん報じられて驚かされます。コンピューターやインターネット利用に際し、知っておくべきこと、注意すべき点がありましたら、教えてください。

A 情報技術を利用するサイバー犯罪の急増は社会問題となっています。サイバー犯罪は大きく三つに大別されます。圧倒的に多いのが①ネットワーク利用犯罪です。次いで②不正アクセス禁止法違反、③コンピューター・電磁的記録対象犯罪です。特に、ソーシャルエンジニアリングといって、人の盲点をついて侵入し、情報を盗む手口が横行しています。巧妙な手口と対策について説明します。

1 スキミング

キャッシュカードやクレジットカードに書かれている情報をスキマーという装置で読み取り、偽造カードを作成したり読み取ったパスワードを利用したりして、銀行預金を引き出したり、借り入れ（キャッシング）をしたり、買い物をしたりする行為です。銀行やコンビニエンスストアに設置されたATM機に小型カメラ（CCDカメラ）を設置し、遠隔操作で情報を盗む手口もあります。

カード業界や経済産業省がICチップと生体認証（バイオメトリクス）を利用した防止策を進めていますが、個人が注意すべき点は、ID／PWの管理をしっかり行うことや、通帳の記帳を定期的に行い、カードの利用明細書を確認することです。

被害に気づいたら、すぐにカード会社や銀行に届け出ましょう。カード会社で差異があるものの、一般に六〇日前までの不正使用であれば損害金が補償されます。また、二〇〇六年二月に預金者保護法（〇五年八月成立）が施行され、預金者の過失を銀行側が立証できなければ預金全額を銀行が補償することになりました。ただし、いずれも万全とはいえません。利用限度額を引き下げ、引き落とし銀行口座に大金を預けておかないなど、個人で対策を講じることが重要です。

2 フィッシング／ファーミング

フィッシングとは、銀行やプロバイダーを装い、メールを送りつけ、ID／PW、クレジットカード番号などを盗み取る行為です。「釣り」を意味する「fishing」が語源ですが、偽装の手口が巧妙かつ洗練されている（sophisticated）ことから「phishing」と呼ばれています。

フィッシングの一種で、もっと巧妙な手口に、ファーミングがあります。正規の銀行などのURLを入力しているのに、偽のホームページを表示して、ID／PWを盗み取るものです。ユーザーが利用している端末機には何の問題もないうえ、操作上のミスもまったくないのに、特定のホームページのURLとIPアドレスを登録しているDNSサーバーを改竄することで、このようなことが起こってしまいます。

対策として、送信フォームにSSL（暗号化技術）が利用されているか、URLの先頭に「https://」といったセキュアーなページが作られているかを確認しましょう。また、メールに示された送信者名や連絡方法、リンク先以外に、正規のものであると確認できる所在（電話番号やURL）をしっかり確認することです。そして、ネットバンキングやISP事業者を選定する段階で、カード型乱数表等のセキュリティー保護対策に力を入れているところを選ぶことが重要です。

3 ウォードライビング

セキュリティーで保護されていない無防備な無線LANのアクセスポイントを探して、車内に専用ソフトをインストールしたパソコン端末を載せて移動するクラッキングの手口です。非公開の電話回線を探し出す「ウォーダイヤリング」と類似の手法で、映画「ウォーゲーム」からつけられたともいわれています。無線LANは障害物がなければオフィスビルに面した道路上でも弱い電磁波をキャッチできます。ユーザーがインターネットバンキングを使って振込作業をしていた場合、ID／PWを盗み取ることができます。

対策として、無線LANの接続制限を行います。例えば、SSID（Service Set Identifier）を設定し、接続先の無線LANアクセスポイントを指定するIDを用いて、同じSSIDを持った機器だけを接続させる方法や、MACアドレスフィルタリングを用いて、接続を許可する機器の固有番号をあらかじめ無線LANアクセスポイントに登録しておく方法です。また、暗号化機能も有効です。WEPという共通の暗号化キーで無線LANのアクセスポイントと端末間のデータを暗号化します。

4 スパイウェア

ユーザーがホームページにアクセスし、また、メールを受信し開封した時に、ユーザーのパソコンに侵入します。そして、①ユーザーがキーボードに入力した情報を外部へ送信したり（キーロガー）、②ユーザーがキーボードに入力した情報をクッキー（cookie）というファイルにして端末に保存し、このファイルを外部へ送信したりします。

スパイウェアとは機能的に選別されるもので、直ちに有害であるとはいえないものにアドウェアがあり、ユーザーごとに自動的に広告を表示させるために情報を収集するものです。現在、アドウェアのほとんどはスパイウェアの機能を兼ね備えています。知らずにインストールすると端末機の動作が遅くなり、見たくない広告が頻繁に表示されることがあります。

対策として、基本ソフト（OS）のバージョンアップを行い、セキュリティーレベルを上げること、また、スパイウェア対策ソフトを導入することも重要です。なお、新規アプリケーションをインストールする際は、必ず利用規約をよく読んでください。特に無償で配布されているものには、アドウェア機能を持ったものが多くあります。

5 コンピューターベスト―ウィニー

不正プログラムには、ウィルスとベストという二つの種類があります。ウィルスは自己伝染力を有し、不特定者に被害を及ぼします。感染先を必要とするウィルスと、必要としないワームに分かれます。これが脅威であるのは周知のことで、対策ソフトも普及しています。これに対してベストは感染力がないもので、被害者を特定して利用されます。本来は正規のプログラムから発生しており、対策ソフトで検出できないことが多いのです。中でも、最近問題になっているのがウィニーです。サーバーを必要とせず、利用者間で情報交換をするP2P（Peer to Peer）ソフトであり、音楽やアプリケーションの違法コピーや個人情報の流出などの事件が頻発しています。

ネットワーク上に流出したデータを削除するためには、ウィニー利用者の全データを削除することが必要で、対策が困難です。インターネットを利用する人々の自覚と責任の喚起、ネットワークの利用方法に対する情報の提供、普及活動が重要です。

サイバー犯罪（2）

情報技術を悪用した犯罪の対策