ハッカー集団の解明が急務だ

ネット銀行被害

ハッカーの暗躍を封じ込めねばならない。

インターネットバンキングを巡り、何者かが利用者の口座に不正にアクセスして預金を盗み取る事件が後を絶たない。

警察庁によると、今年1～7月には大手銀行を含む12行で約400件、計3億6000万円が犯人側の口座に不正送金された。過去最悪のペースだという。

ショッピングや納税などに便利なネットバンキングの利用者は、急増中とされる。資金決済に使う中小企業も多い。利用の広がりとともに、ハッカー集団の標的になっていると言えよう。

ハッカー集団が使うのはコンピューター・ウイルスだ。発信元が不明のメールやネット上の無料ソフトに仕込まれている。これにパソコンが感染すると、利用者が取引時に入力したIDやパスワードが犯人側に流出してしまう。

キャッシュカードの偽造などによる被害は、預金保護法で補償される。ネットバンキングの被害についても、銀行側は同様に対応している。ただ、利用者側に重い過失がある場合には、補償に応じないケースもあるという。

不審なサイトからのダウンロードを徹底して避ける。駆除ソフトをこまめに更新する。利用者自身が日ごろの自衛策を怠らないことが、何より大切である。

銀行業界と警察が連携し、有効な対策を講じることも重要だ。

全国銀行協会は昨年、取引ごとに毎回、数字の組み合わせが変わる可変式パスワードの導入に努めることを申し合わせた。

だが、それさえ骨抜きにする新型ウイルスによる被害が一部の銀行の口座で確認されている。高度化、複雑化する手口への対策は、今後の大きな課題だ。

警察庁がこれまでの被害を分析したところ、不正送金の受け皿となった口座のうち、7割が中国人とみられる名義だった。

神奈川県警は7月、電子計算機使用詐欺容疑で複数の中国人を逮捕した。いずれも現金の引き出し役だった。供述や携帯電話の通信記録から、中国に拠点を置くハッカー集団と連絡を取り合っていたことも判明した。

組織の元締に捜査の手が及ばなければ、末端の引き出し役を代えて、犯行は繰り返されるだろう。まずは、ウイルス作成者など実行犯を特定することだ。

その上で、国際刑事警察機構（ICPO）を通して中国の捜査当局に捜査共助を求め、犯罪組織の全容解明につなげたい。