あらかじめ「電子証明書」を付与した特定の端末でしか送金手続きはできないはずだった。だが、端末に入りこんだウイルスは顧客のID、パスワードと共に証明書の情報まで盗み取っていた。

西日本の信用金庫で4月、法人顧客のインターネットバンキングの口座から資金が不正に引き出される被害が5件立て続けに発覚した。被害額は計数千万円。「対策の費用や手間を惜しまなければ……」と信金の担当者は悔やむ。

個人顧客向けには1回の取引ごとに異なるパスワードを発行する「ワンタイムパスワード」を導入済みだったが、法人顧客については数百万円の追加コストなどを理由に見送っていた。

対応後手 狙われる企業

ネット社会 リスクを知る 3

高コストに及び腰

ネットバンキングで防犯対策に使われるワンタイムパスワード用の機器

警察庁によると、国内で1～5月上旬に判明したネットバンキングの不正送金被害は計約14億1700万円。うち約3割の4億1500万円を地方銀行や信金など中小金融機関が占めた。昨年1年間では1割弱だったのが急拡大し、同庁の担当者は「対策が遅れている金融機関が狙われるようになった」とみる。

セキュリティー会社のトレンドマイクロ（東京・渋谷）は3月、国内175社を対象にサイバー攻撃対策の現状を調査。「基本ソフト（OS）の脆弱性への対策」「攻撃を受けたときの対応人員、組織」など26項目を点数化したところ、100点満点で平均は58・5点にとどまった。

ネット利用に積極的な企業もコストのかかるセキュリティー対策には腰が重い。トレンドマイクロの染谷征良氏は「被害に遭ったときの損失は企業が考えているよりずっと大きい」と警鐘を鳴らす。

都内の広告企画会社では6月、広告ノウハウを紹介する会員制ウェブサイトから氏名やメールアドレスが流出。情報管理の甘さに顧客から苦情が相次ぎ、1カ月間の営業活動の自粛を余儀なくされた。

セキュリティー意識まだ薄く

4月に発生したクレジットカード大手、三菱UFJニコスの個人情報流出は、世界中で使われている暗号化ソフトに潜んでいた欠陥が原因だった。同月7日に修正プログラムと合わせて欠陥の存在が公表されたが、修正作業までのタイムラグをつかれた。

ネット犯罪対策はこれまでシステム担当らが兼務していたが、専従8人を置く体制に強化。担当者は「世界のセキュリティー情報を集め、即座に対応するには兼務では難しいと分かった」と教訓をかみしめる。「ネットをビジネスに使う以上、セキュリティー対策のコストは避けられない」

（関連記事を電子版に▼Web刊→紙面連動）