特集 この夏以降、情報漏洩は防げるか

財界 REPORT

ZAIKAI
a japanese business biweekly

夏季第2特大号

2004 8/3

セキュリティ責任者の能力と地位の向上が不可欠

三分の二の従業員が買収に応じる！

三百七十八件。この数字は、政府がまとめた二〇〇一年四月から今年五月までの三年間で、自治体や企業から流出した個人情報漏洩の件数だ。

しかし、なぜ、これほどまでの漏洩事件が起きるのか……。このほとんどの漏洩事件を操っているといわれるのが、情報ブローカーだ。

情報ブローカーが個人情報を盗み出す手口について、帝京大学教授（危機管理論）の宮崎貞至氏がこう話す。

「ブローカーたちは個人情報を入手するため、大手企業の従業員や契約社員、また、その顧客情報を管理する業者の従業員に声を掛け、五十万円程度で彼らを買収する。買収率は三分の二程度、なかにはブローカーが契約社員になりすます例もある」

ここでブローカーが入手した個人情報は、国内に百社程度あるといわれる名簿屋（通称）に売られる。値段は情報内容により異なるが、一件当たり一円～百円。特に多重債務者の情報は高く売れ、一件当たり一万五千円以上の値が付くという。消費者金融が顧客を獲得するために要する費用は二万五千円程度、この価格でも買い手は十分あるわけだ。

情報漏洩を防ぐ二つの施策

いまや個人情報は、価値ある商品として、売買される仕組みが出来上がっている。その中で、自治体や企業は情報漏洩をどのように防いでいけばいいのか。

情報漏洩防止に努める日本情報安全管理協会（NPO法人）は、二つのポイントを上げる。

その一つが、御茶ノ水アソシエイツ主任研究員の堀川直子氏が主張する、組織内にCSO（最高セキュリティ責任者）を置くことだ。

現在、多くの企業におけるセキュリティ担当者は、その位置づけが低く、セキュリティに掛かる費用対効果などをきちんと説明できる能力を持たない。

予算の配分を決定する取締役レベルは、ネットワークの専門用語を聞いたことはあっても、費用対効果まではわからない。そのため、取締役レベルと対等に話をし、セキュリティの費用対効果をきちっと説明でき、そのための予算を取ってくるCSOの存在が不可欠なのだ。

そして、このCSOを中心にチームを組んで、社内におけるすべての情報を安全に管理する仕組みを作る。

もう一つが、日本エス・アイ研究所代表の中橋治氏が主張する、セキュリティに最新の標準化を取り入れることだ。

いま企業が、セキュリティ対策の標準化の指標としているのが、セキュリティ実施基準のISO／IEC17799や、一九九六年に改定されたシステム監査基準。この年代は、Windows95や2000など、旧式タイプのOSが主流だった頃で、いま実施すべきセキュリティ対策には、到底及ばない。

また、企業はセキュリティ対策に取り組んではいるが、そのレベルを点数化するなどの標準化を取り入れていない。

一連の顧客情報流出事件で、企業のセキュリティに対する意識は高まってきた。しかし、十分なセキュリティと確信できるものかどうかすら、わからないのが実態だ。自分たちの顧客は、自分たちで守る。まずは、この基本的な意識を持つことから始めなければならない。