リスク管理

リスクマネジメントABC

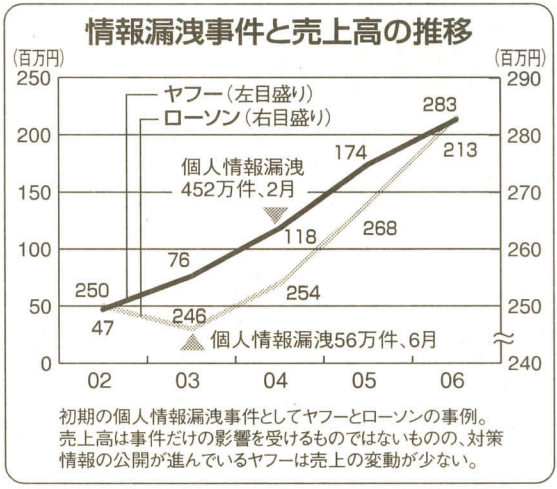
セキュリティー管理

対応策、顧客に情報公開を

情報セキュリティー管理とは誤解を恐れずにいえばリスクの評価とその対応策の選択といえる。ITに対して予測される脅威について、発生可能性や推測される被害を主観的に評価し、それに対し対策を施すことだ。セキュリティー対策に対してはIT予算の約5～10%に達し、毎年10数%ずつ増加しているとする調査結果もある。それほどの費用をかけた情報セキュリティー対策であるが、そのリスク評価結果やリスク対応策の選択結果は各企業に委ねられており顧客等外部からは見えないことが多い。

◇

顧客はサービスを受けるため企業に対し財産や個人情報を預けているのだから、その評価結果や対策内容を知っている方がよいのではないだろうか。リアルの世界では実現できていることが多い。例えばコインロッカーと銀行の貸金庫では、リスク強度が違うことを私たちは想定できていて、承知してサービスを受けている。



初期の個人情報漏洩事件としてヤフーとローソンの事例。売上高は事件だけの影響を受けるものではないものの、対策情報の公開が進んでいるヤフーは売上の変動が少ない。

一方で、情報セキュリティーについては、リスク評価結果や施策内容は明らかでないことが多い。これらを明らかにするのはセキュリティー上問題があるという人がいるかもしれない。確かに、リスク評価結果や対策内容の公開によってセキュリティーは幾分落ちるかもしれないが、それを知ったうえでサービスを購入するのであれば知らずに買わされるよりマシだろう。それに何もかも洗いざらい公開しようといっているのではない。顧客が判断できる程度でよいのだ。私たちは貸金庫のシステムの詳細は知らないがコインロッカーよりは安全そうだとは知っている。公開の仕方も工夫できる。銀行の金庫が厳重なのは知っているが鍵の番号や形式が秘密なのだ。RSA暗号などは評価のため計算方式は公開されていて鍵だけが秘密になっている。それでセキュリティーは保たれているのだ。

また、リスクを公開したからといって、そのリスクに対して何もかも対策がされている必要もない。皆が貸金庫を求めているわけではなく、預けるものと費用によってはコインロッカーでもよいからだ。それに、そもそも100%のセキュリティー対策はない。秘密はときに有効だが独善的になることもある。かつての日本海軍は暗号が米国に解読されていることを知らず高出力の通信を用いた大胆な戦術を使い失敗している。公開するということは、絶えず外部の評価にさらされることを意味する。環境は変化するので定期的な見直しが必要になるはずであり、それが行われているかを検証する材料にもなる。

(日本総合研究所)
総合研究部門 板垣 克彦(上席主任研究員)