リスク管理

リスクマネジメントABC

システム監査の活用

利用者の教育・啓蒙に有効

リスク管理の問題点としてコストと効果があげられる。財団法人日本情報処理開発協会による情報セキュリティーに関する調査(06年3月)では、ITリスク管理にはカネがかかりすぎる(20%)、どこまでやればよいのか基準が示されていない(14%)などコストと効果に関する問題点が上位にあがってきている。実際、IT投資のうちリスク対策に関する投資の割合は7・7%にのぼり(同調査)、決して少ない額ではないため、おのずと成果が求められてしまうのだろう。いかなる対策によってもリスクは100%除去できるわけではないことから、リスクに見合った対策とコストが必要となってくる。

◇

リスクとは脅威、脆弱性、発生頻度、発生時の損害の大きさなどの要素からなり、その評価は企業がおかれている環境や、守るべき情報資産、それに評価者によって変わる。内部からの情報漏えいのリスクに対しては顧客情報の管理を厳重にすればよいだろうが、犯人の目的が金銭であれば、新製品開発情報や特許情報なども管理対象としなければならない。

そもそもITによる情報管理ではなく、社員の待遇を改善するなど内部犯行が起こらないようにするほうが簡単な対策かもしれない。あるいは日常的に発生している伝票の誤入力の方が相対的なリスク値は高いかもしれない。最新のセキュリティー製品を購入したからとか、同業者と同じ対策をしているから、といった取り組みでは十分とは限らないのである。システム監査は、リスクに応じた適切な管理策になっているかどうか、割高な対策をしていないかどうかを見つける方法のひとつとして有効である。

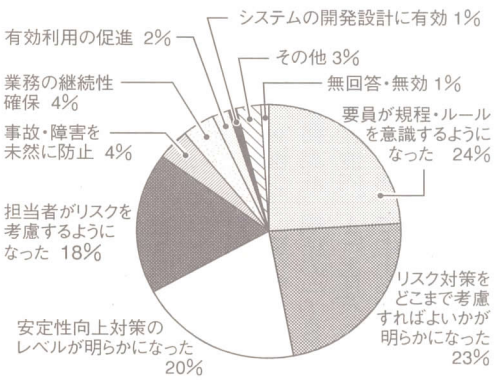
ほとんどのリスク対策は技術と運用の組み合わせといえる。技術だけの導入では万全でなく、それを運用する人間の要素も極めて重要である。すなわちITリスクは情報システム部門にまかせておけばよいということではなく、システムを利用する社員やアルバイトにかかわる部分も大きい。このような人間による運用にかかわる点に対しては利用者への教育、啓蒙が重要になる。知ってもらう、理解してもらうだけでは不十分で、実践してもらわねばならないからだ。システム監査は、そのような教育・啓蒙にも有効であるという調査結果がある(図)。

また、社内外の環境の変化に対してリスク対策を適宜見直しすることも必要である。監査結果に応じてリスク対策を見直し改善するといったマネジメントシステムの確立という点に対しても、システム監査は有効だ。経済産業省のシステム監査企業台帳などの活用も参考になる。

(日本総合研究所)

研究事業本部　板垣　克彦(上席主任研究員)

システム監査の効果



財団法人日本情報処理開発協会「システム監査普及状況調査」(07年3月)より日本総研編集