リスク管理

ITに関するリスクについては、日本版SOX法においても内部統制の基本的な要素としてリスクへの対策が求められている。ITが企業の事業活動に欠かせないものになっていること、またIT自身が複雑化・高度化しリスクを多く抱える存在になっていることと関係がある。ただ、49%以上もの企業が、ITリスク管理は重要と考えながら実践できていないと回答している(図)。これは、どういったリスクを対象に、どこまでリスク対策を行えばよいのかが、わかりにくいことが原因と考えられる。

◇

ITリスク管理は、(1)保護対象の選定、(2)リスク分析、(3)対応するリスクの選定、(4)リスク対応の実施、(5)統制活動・モニタリング、の手順を繰り返すことにより実施する。多くの企業でこれらの作業が概ね実施されているが、一部ではリスク分析が十分でなかったり、リスク分析などをとばしてリスク対応から統制活動へ一気に進めているところもある。リスク対策が場当たり的、パッチワーク的なものにならないよう、やはり、リスク分析を実施し対応すべきリスクを選定して適切なリスク対策を実施すべきである。

ただ、みな同じ対策である必要はない。リスク対応は企業のおかれた環境やリスク選考の結果に応じ異なってよいからだ。例えばヤフーでは、個人情報漏洩事件以降、指紋認証システムの導入、私物持込を禁止するため入退室管理とポケットのない制服の着用、ビデオカメラによる監視、きめ細かなアクセス管理などを行っているといわれ、個人情報管理に対してはほぼ完璧な対策といえる。しかし、一般の企業が同じ対策をとることはなかなか難しい。さらにITリスクは時間によっても変化するので追随して対応する必要がある。その時点で対策が十分であっても技術の進展で脆弱性は増減するからだ。たとえヤフーほどのリスク対策でも新しい情報持ち出し技術が登場すれば見直しが必要になるのである。

また、リスクを外部へ移転することによる対策もあり得る。最低限のリスク対策はとりながら、それ以上のITリスクについては、市場にリスクを委ねることも可能である。市場では、さまざまなリスクの取り手がいる。

そもそもITリスク対策に100%はないのだから、残存リスクを認識し市場に説明していくという観点としても重要である。

日本版SOX法の対応をしている企業は多いと思われるが、ITリスクと統制に関する報告だけで終わるのではなく市場に委ねるITリスクを明らかにすること、(1)~(5)のステップをもとに環境変化などに応じて見直し、PDCAのサイクルを絶えず進めていくことが重要だ。

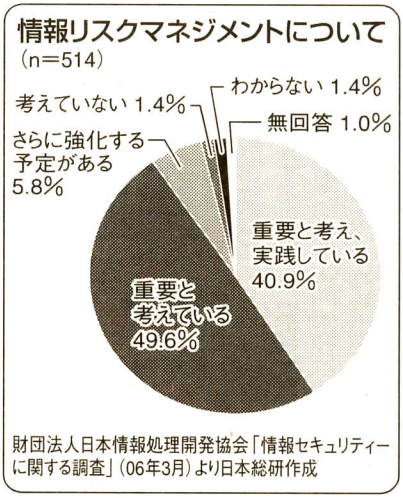
(日本総合研究所)

総合研究部門　板垣　克彦(上席主任研究員)

リスクマネジメントABC

企業のIT管理

対象の選定・分析を十分に



財団法人日本情報処理開発協会「情報セキュリティーに関する調査」(06年3月)より日本総研作成