日刊工業新聞
2007年（平成19年）5月24日（木）

情報セキュリティー

内部統制の基本要素に

ＩＴ再評価

リスクマネジメントＡＢＣ

日本版ＳＯＸ法（内部統制報告制度）の成立・導入により、企業経営において内部統制の確立が求められるようになった。その日本版ＳＯＸ法の求める内部統制の基本要素としてＩＴ（情報技術）への対応が求められている。内部統制の基本要素としてＩＴが組み込まれているのは、企業活動における浸透度、利用度が高まっていることと、一方でＩＴ自体の技術高度化で、ＩＴの不備によるリスクの影響が急拡大していることが要因と考えられる。

◇

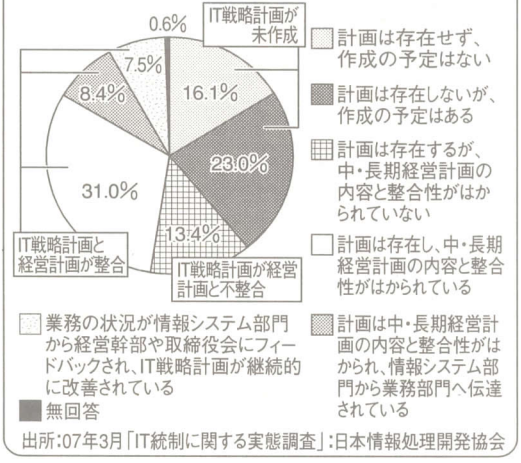
前者は企業活動におけるＩＴの浸透度、利用度が高まっていることを反映しており、ＩＴが公式に経営上重要なものであることが認められたことを意味する。単に社員の事務作業を支援し、機械・設備の作動を制御するツールではなく、従来からのいわゆるヒト・モノ・カネの経営要素の中に新たに加えるべき対象になったと考えられる。また後者はネットワーク化やＥＵＣ（エンドユーザーコンピューティング）化などが代表的な例で、ＩＴ不備のリスクが影響度の面でも発生頻度の面でも、飛躍的に増大していることを意味する。

これまで経営におけるＩＴの重要性は訝われてきたが、実際には一般の企業では他の要素のヒト、モノ、カネに比べてその存在感は弱く、それがもたらすリスクの影響範囲や発生可能性についての認識は低い状況にあった。例えばカネのリスクは資金不足や運用上の損失につながることが多くの企業で実感され、対応されている。

それに比べ、情報システムは生産現場、営業現場、間接部門等の作業支援ツールとして導入されてきた経緯から、それらの不具合に対するリスクは各担当部署でのリスクとして認識されるにとどまり、企業経営のリスクとまでは考えられてこなかったと推測される。それが今般新たに内部統制の基本要素として織り込まれ、ＩＴの不具合に関するリスクやＩＴの管理不備によるリスクに対応することを迫られている。

実際に最近の上場企業対象のアンケートでも、内部統制上要求されているＩＴ戦略計画を経営にリンクあるいは反映させている企業は半分以下であり、約40％の企業は計画さえ立てていない（図）。同じ経営の重要な要素であるカネ・ヒト・モノで、それらにかかわる計画を経営計画とリンクさせないことは通常考えにくい。

各企業は今般の日本版ＳＯＸ法への対応を機に、経営におけるＩＴへの依存度を再確認し、ＩＴによるリスク拡大を再認識し、経営におけるＩＴの位置づけを再評価することが必要と考えられる。



出所：07年3月「IT統制に関する実態調査」：日本情報処理開発協会

（日本総合研究所）
研究事業本部　中原　隆一　（主任研究員）