リスク管理

リスクマネジメントABC

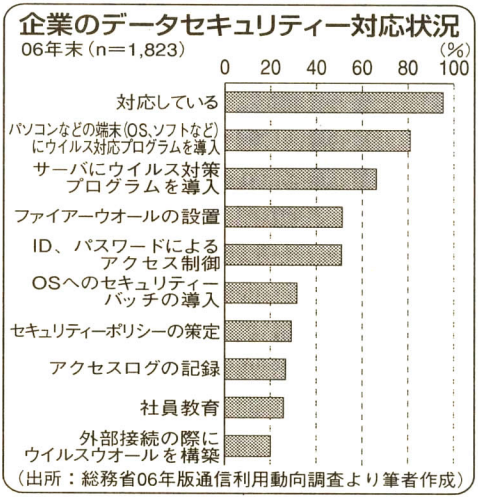
内部要因によるIT利用リスク

現場の意識高め対策を

企業のIT利用にかかわるリスクとしては、各種情報の機密にかかわるリスク、ウイルスや不正侵入等のリスクなどが想定される。これらのリスクに対する企業側の対策としては、主にファイアーウオールやアンチウイルスソフト等の導入が行われている。総務省の調査ではウイルス対策プログラムの導入はPCで9割、サーバでも6割の企業で導入しており、ファイアーウオールは5割の企業が導入している(06年度通信利用動向調査)。これらの対策は主に企業外部から侵入あるいは攻撃してくるリスクを想定した対策と考えられる。

◇

ただ企業のIT利用に関するリスクの要因は前述したような企業外部からの侵入や攻撃といった外部要因だけでなく、社員等企業内部の不正や誤操作等内部要因に基づくものも多く存在していると考えられる。この内部要因に起因しているリスクは主に各種情報の機密にかかわるリスクと関連が深く、PCの紛失、データの誤送信等ITの利用にかかわる情報漏洩(ろうえい)、情報の不正利用等の事故事例が多発している。



内部要因によるIT利用リスクについての対策は、前述した総務省の調査の項目の中では、パスワード等によるアクセス制御、アクセスログの記録等が主に該当する。導入状況はパスワード等によるアクセス制御が5割を超えている他は、全体としてこれらの対策ツール自体の導入は不十分と考えられる。これらの対策が不十分なことはもちろん情報漏洩等の要因の一つであるが、内部要因に起因するリスクを企業が十分防げていない要因としては、ITを取り扱うのが人間であり、企業内部の社員であることが大きく影響している。例えばパスワードによるアクセス制御をしても、パスワード自体が容易に知れる状態にあったり、複数の人間で共有されたりすれば、対策としての有効性はなくなる。

現状ではこれらのITを利用する社員等への対策は、マニュアルや手続きの複雑化・厳正化等が主な対応策である。しかしながら制度や手続きを定めても、前述のパスワードの例に見られるように、実際の業務と整合していないと結局制度や手続きが順守されずリスクを顕在化させてしまうと考えられる。業務に適合するリスク対策を進めていくためには、これまで各企業で行われてきた業務改善運動や品質管理活動に倣って、もっとITを利用している現場レベルにリスクを再認識させ、その対策に取り組ませることが必要と考えられる。内部要因に基づくIT利用のリスクに対しては、ツールや手続き等に安易に依存せず、現場のリスク意識を高め、リスク対策のノウハウを蓄積していくことが重要と考えられる。

(日本総合研究所)
総合研究部門 中原 隆一(主任研究員)