組織事故とセキュリティマネジメント

新潟国際情報大学　杉野　隆

高野氏が述べておられるように，近年に発生した重大事故に組織事故と呼ばれるものが多い。ここには，高度経済成長期に染み付いた効率主義，1990 年代に押し寄せてきたグローバリズムの波に呑み込まれまいとする企業経営者のうごめきが垣間見られる。

IT やネットワークの活用には，必ずセキュリティという negative な要素を伴う。IT 活用の positive な側面を伸ばすことは前向き姿勢として評価され，先に享受してしまう。negative な側面は後から対処するといった経営姿勢が，現在の e-commerce への取り組みにも見られる。両面を同時に捉えた事業展開を行わないと，ネットワーク運用関係者は板ばさみとなる，ひいては企業全体の損失にもつながることになろう。

ISO9001 は品質管理をマネジメントプロセスとして規定し，その品質方針は経営者が決定するものであり，経営者の責務 Commitment であるとしている。品質をセキュリティに置き換えると，情報セキュリティにも当てはまることが分かる[1]。

組織事故の防止のためには，安全意識の向上や組織文化の変革が必要であるが，これらはすぐに変えられるものではない。そのため，高野氏は（安全）管理の側面から組織として介入することによって，安全文化の醸成することが必要であるとされる。

表に，重大事故と言われるプラント事故と情報セキュリティ事故の違いを示した。高野氏が列挙されたようなプラント事故と異なり，情報セキュリティ事故はその被害が見えにくいという特徴を持つため，管理と教育の二つの側面が必要ではないかと思う。情報セキュリティ管理については，すでに ISO/IEC 13335 や ISO/IEC 17799（BS 7799 をベースに現在検討中。）があるが，これらの国際標準でも，セキュリティ意識の醸成，向上のための教育の重要性が強く主張されている。

表　情報セキュリティ事故とプラント事故の比較

	情報セキュリティ事故	プラント事故
被害の分かりやすさ	被害が見えにくい	被害が目で見て分かりやすい
事故直接原因の所在	分散している	事故発生場所に局在している
事故関係者（犯人）	遠隔地にいる場合が多い （自分は事故に巻き込まれる可能性が少ない）	被害現場付近にいることが多い （自分も事故に巻き込まれる可能性がある）
事故の意図性	意図的犯罪の可能性が大きい しかし，過失も多い	意図的犯罪の可能性は低い ヒヤリハット

セキュリティ事故は，その 6 割近くが内部者の関係しているものともいわれるだけに，教育を充実させ，メンバにその組織のセキュリティ対策の実態を周知すれば，内部者のセキュリティ事故に繋がるような行動を慎むようになるのではないか。このような効果も期待できる。

さらに，科学技術庁が，技術開発に伴う事故や製品の欠陥などの失敗をデータベース化し，失敗を体系的に分析する「失敗学」研究を始めるという。失敗の原因だけでなく，その背景を分析し，再発を防止するのが狙いという。ここでは，企業は失敗を隠蔽したりもみ消す風潮があるので，これを阻止し，失敗の知識を社会全体で共有しようという試みである。その意味で参考になるのは，福岡銀行で 3 月に発生したシステム障害に関してその事故内容や管理体制を含めた具体的な改善策をホームページで開示したことである。福岡銀行は，信頼を回復するためには必要な措置と判断したようである。

参考文献

[1]杉野　隆　規範的セキュリティポリシへの ISO 規格などの適用について，情報処理学会全国大会大会予稿集，1999 年 9 月。