2016.5.23 電経新聞「Point of View」

セキュリティリスク・マネジメントは簡単だ！

藤谷 護人

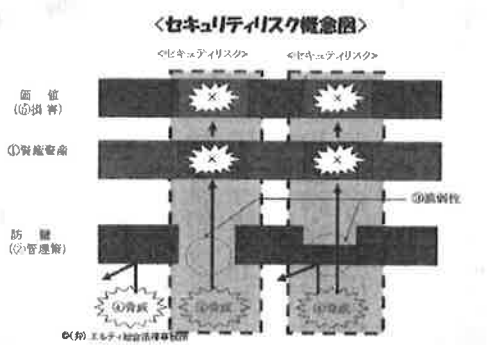
セキュリティリスクとは何かを理解するのは簡単だ。たった5つの関係を覚えればよい。リスク分析を最も適切に行い得るのは、その組織に所属する者であって、外部専門家ではない。自分たちで自分たちの仕事のやり方に潜むリスクを発見して改善しようというセキュリティマインドの育成が大切である。

セキュリティリスク・マネジメントが今日的会社経営における重要課題であるとの認識は多くの経営者が持っている。しかし、「何を」「どのように（程度・金額）行えば」「十分なのか」がわかりにくいという声がなくならない。

その原因として、コンピュータのことさえわからないのに、セキュリティとなると技術的専門性がより強くて、もっと近づき難い。さらに「リスク」とは何かにまで頭が付いていかない、という声を耳にする。

セキュリティリスクとは何かを理解するのは、実は簡単である。

たった5つの関係を覚えればよいだけだ。セキュリティリスクとは、ある組織が守らなければならない「①情報資産」を守るために取っている「②管理策（コントロール）」に存在する穴や弱いところ、すなわち「③脆弱性」を「④脅威（サイバー攻撃など）」が突破して組織内に侵入し、情報資産が攻撃され「⑤損害」が発生する危険がある状態のことである。



セキュリティリスク概念図を①→②→③→④→⑤を目で追いながらイメージいただきたい。一方、セキュリティリスクとは何かがわかったとして、どのようにマネジメントすればよいのかが専門家でないとわからないのではないか、という声も耳にする。

リスクマネジメントとは、リスクを（1）発見し、（2）評価し、その重要度や緊急性に応じて優先度や対策費用を考慮して、（3）管理策を決定し、（4）実施し、（5）実施結果をチェックし、（6）次の対策につなげていくことである。（1）－（3）がPLAN、（4）がDO、（5）がCHECK、（6）がACTのプロセスをスパイラル的に実施していくことだ。これは「問題解決プロセス」にほかならない。そして、問題解決において最も大切なのは、（1）と（2）のプロセスである。これが十分にできれば、問題解決の8割は達したといえる。

セキュリティリスクを発見し評価するために必要な能力は何か。「自分の会社の仕事でどのような情報が、どの部署からどの部署へ、どのような手段で、移動しているか」という業務フローを作成し、そのフローの各場面でどのような「リスク」があるかを分析すればよいだけである。このリスク分析を最も適切に行い得るのは、その組織に所属する者であって、外部専門家ではない。自分たちで自分たちの仕事のやり方に潜むリスクを発見して改善しようというセキュリティマインドの育成が大切である。

ふじたに・もりひと 弁護士法人エルティ総合法律事務所所長弁護士。ITーADRセンター所長。日本の弁護士の中で唯一の公認システム監査人、JISA正会員。