特集「情報セキュリティ」の発刊によせて

柏 木 直 哉

2003 年 10 月，経済産業省が示した情報セキュリティ総合戦略に基づき，各企業に於ける情報セキュリティ対応施策が本格化し始め，2005 年 4 月からの個人情報保護法全面施行で対応が一層進んだ．

日本は，他国と海で隔てられており，また，社会生活面では近所が互いに昔からの知り合いというセキュリティ面からみればこの上ない環境にあった．その中で安全・安心を当たり前のこととして，長く暮らしてきたこともあって，セキュリティを余り意識せずに来た．しかしながら，人々の生活スタイル・価値観が多様化するにつれて近所との関係は希薄になり，セキュリティ面への配慮が求められるようになってきた．また，経済のグローバル化や IT の進化の中で，ビジネスや情報システムは世界に通じるネットワークに繋がっており，否が応でも世界で起きている様々な情報セキュリティ関連の事件に無関係では居られなくなって来てもいる．政府のウェブサイトの改竄，意図的なウィルス埋め込みによる汚染，企業などにおける顧客情報の漏洩等，日々の新聞に情報セキュリティ関連の話題が絶えることはない．

情報セキュリティは，いったん情報漏洩等の事故，事件が起こるとリカバリーの大変な事が目に見えている．そのため，ともすると，報道の都度，事故を自社に置き換えての防御策の有無が経営トップから問われ，マスコミ等で話題になっている様々な施策を性急に行いがちになる．しかしながら，いくら，金をかけても，100% 完璧な対策は作りようが無い．大切なことは，個々の情報の資産価値を洗い出した上で，企業毎の業務特性や事故が発生した場合の業務への影響度，情報資産価値とのバランスをみた適切な施策を適切な時期に進めていくことである．

一方，あいつぐセキュリティ事故は，大きな意味では日本経済へのインパクトでもある．企業のイメージダウンにも繋がることから，IT に関わる部分で情報漏洩が生じた場合に無制限の損害賠償を IT ベンダーに迫る契約も出始めてきている．これが行きすぎになると IT 産業や大きく言えば日本経済全体の健全な発展を阻害する危険も孕んできている．

米国では州によって既に，個人情報窃盗罪など施行済みであると報告されており，今後，この傾向は増えていくものと予想される．振り返って日本では，情報という目に見えないものの窃盗という認識が行われず，ものに読み替えた結果，記憶媒体の窃盗としてしか認識されない時代が続いていた．しかしながら，ここへ来て，政府でも「情報漏洩罪」の検討が始まってきている．

企業においても，PC の盗難等を，ハードウェアの価値で捉える傾向が未だ残っているものの，ここへ来て，そこに含まれていた情報の持つ価値の重要性が認識されるようになってきている．

総じて言うと，日本における情報セキュリティは「産業の健全な発展」という課題を孕みつ

つも着実に対応が進みはじめたということができる．

情報セキュリティはグローバル時代への対応としての位置づけも重要であることから，事件・事故の報道に短期的対策を迫られつつも，本質的には総合長期対策を必要とする．最後は企業文化そのものを如何に変えていくかが鍵を握ることとなる．重大事故に繋がりかねないミスを事前に防御する仕掛けを作り込む事は，もちろん重要であるが，一方で，仕事の進め方を変え，社員個々人の情報に対する意識を変えていく事が必要だからである．これらは，今後，IT ガバナンスを見直すときにも大切な視点となる．

日本ユニシスグループでも現在，総合セキュリティ戦略を 3 カ年計画として立案し，私が CISO（Chief Information Security Officer），CPO（Chief Privacy Officer）となり戦略を数十のアクションプランに落として PDCA マネジメントを実施，業界最高水準の情報セキュリティレベルを目指して実行中である．また，企業の社会的責任の重要性が認識される中，日本ユニシスグループにも CSR（Corporate Social Responsibility）専任部門が設置され，情報セキュリティを社会的責任という視点でも捉えていくことになった．今後は BC（事業継続）や DR（災害復旧）を総合マネジメントする BCM が重要になってきている．

本号では情報セキュリティを CSR や IT ガバナンス，企業戦略の視点で捉えることの必要性を論じると共に，法令対応，監査，国際標準，そして評価や適用事例と多方面からの見方で取り上げている．読者の一助になれば幸いである．

（CISO/CPO　代表取締役常務取締役）