どうする？機密情報漏洩！

近年急増する内部機密情報漏洩、特に個人情報漏洩は大きくマスコミに取り上げられ日常社会の大きな関心事になっている。日本政府としては二〇〇五年四月に個人情報保護法が施行され、その法令に違反する者は刑事罰を受けることになる。最近のIT技術の進歩・発展は目覚ましく、コンピュータ・ネットワーク内に設置されるハードウェア（H／W）やソフトウェア（S／W）のツールも格段に大容量化・超高速化・小型化に対応できるようになってきた。

それゆえIT技術は性善の人間には極めて利便性の高いものとして評価されている一方、逆に性悪の人間にも極めて便利な犯罪ツールを提供することになってしまった。現在、特にコンプライアンスを重視しているかが注目される企業として身内の人間を疑うということを前提にしたシステムなりコンセプトを構築することは、人間不信の環境を作り極めて困難な問題を提起する。それゆえ不正犯罪が発生した場合は警察の手に任せるかあるいは企業の信用確保のため内部処理してしまうケースのいずれかになるのである。しかし、次々と個人情報や企業の内部情報が漏洩し、しかもマスコミを通じて世間に大きく報道されるにつれ、内部処理だけで済ますことが、だんだん困難な状況になってきている。

それではどうすれば良いのだろうか？

この分野のH／WやS／Wの監督官庁である経済産業省は、「予防重視」から「事故前提」の対応に切り替えよと警告している。地方自治体を管轄する総務省においても同様な考え方を示している。すなわち不正犯罪は必ず起こるものであるとの前提に立ち、発生時にはシステムに組み込まれているH／WやS／Wのツールおよび高度化対応のシステムの構築により、その被害を時間的・金額的・第三者への被害面の最小化を図ることを優先し、平行して正確で判明しやすい犯罪記録が残るようにすることである。

さらに、もう一つの大切な要素はサイバーの不正犯罪に対応できる人材の確保である。残念ながらこの分野では米国に比べ日本の対応はかなり遅れている。米国はこの重要性を強く認識し、四～五年前から高度なセキュリティ技術者の養成を政府ベースで開始、現在では二〇以上の大学院で特殊教科を基に実習訓練を施しており、すでに二〇〇〇人以上がサイバー軍団として国防総省、CIA、FBI他基幹企業でセキュリティ業務に従事している。日本では本年四月、情報セキュリティ大学院一校が開校したのみである。現時点で高いセキュリティ技術を習得した技術者はわずか七～一〇名しかいないと言われており、まことに心細い限りである。

「事故前提」ポリシーに切り替え、それに対応できる最善の「防御システム」のツールを探し防御するのが一つの解決策ではないかと考えられる。

谷口芳男
情報・コンピュータシステムズセキュリティ協会　会長