

情報セキュリティ技術を有効利用するには

東京大学教授 工学博士
生産技術研究所

今井秀樹



不正アクセス、ウイルス、サイバーテロと情報システムに対する脅威は連日のように新聞紙上を賑わし、これに対処するための情報セキュリティ技術の重要性は、言い尽くされているかに見える。しかし、現状で情報セキュリティ技術が有効に利用されているかといえば、多くの場合、答えは否定的にならざるを得ない。

その一つの理由は、現在の情報セキュリティ技術が必ずしも利用者に安心感を与えるものではないことである。例えば、パソコン画面に表示された重要な文書をクリック一つで電子署名をすることに不安を感じる人は少なくない。一方、幾ら安全であっても、使いにくいシステムは敬遠されるか、さもなければ誤用される。情報セキュリティ技術は、一般に理解が難しいものであるし、またそれをを用いることにより、システムの使いやすさを損なうという面も持つ。これらの点を改善していくためには、結局、人という要素をより重視して研究開発を進めていくべきであろう。筆者が提唱しているヒューマンクリプトも、その方向を目指すものである。

情報セキュリティ技術が適切に利用されないもう一つの理由は、情報システム開発における競争の厳しさである。多くの情報システムは、少しでも早く開発しなければ、競争に負けてしまう。このため、危険性の多いシステムを市場に投入することも少なくない。確かに、システムによっては、当初から強いセキュリティを持たなくても、問題が生じた場合に対処すれば済むこともある。しかし、適切な情報セキュリティ技術を用いないことで致命的な損害を受けた例は、これまでも決して少なくない。個々の損害がそれほど大きくない場合でも、セキュリティの弱いシステ

ムが普及して、利用者がそれに慣れてしまった場合、強いセキュリティを持つシステムを利用者に受け入れてもらうのは難しい。これは、結局社会全体に不利益をもたらす。したがって、どのようなシステムであっても、当初から情報セキュリティを十分に考えておくことが重要である。その上で、システムの特性に依じて適切な情報セキュリティ対策を施すべきなのである。

とはいえ、放置しておけば、危険なシステムが安全なシステムを駆逐する傾向のあることは否定できない。安心できるネットワーク社会を構築するためには、公的な支援によって情報セキュリティ技術の開発環境を整える必要がある。特に、情報セキュリティ評価は、適切な情報セキュリティ対策のために必ず(須)であるが、高度な専門性を要し、大きなコストも掛かる。幸い、この面で公的な機構が、現在幾つか構築されている。電子政府のための暗号技術評価プロジェクト“CRYPTREC”もその一つであり、情報セキュリティ対策のかなめである暗号技術に関し、信頼できる情報を提供している。しかし、セキュリティ評価は継続的に行う必要があり、CRYPTRECを恒久的な公的機関に発展させていくことが今後の課題である。

もとより、情報セキュリティは技術だけで達成できるわけではない。法・制度、教育・啓発、管理・運用など、多くの面から総合的に対処していく必要がある。しかし、法や制度で人を厳しく縛るより、技術でできるところは技術で対処するのが、人に優しい情報化社会を作る道である。この意味でも、情報セキュリティ技術は今後更に重要性を増していくことは疑いない。