情報セキュリティ技術の情報化社会における役割

東京大学　生産技術研究所
教授
工学博士
今　井　秀　樹

9.11 以降の世界的な治安の悪化を一つの契機として，安全・安心が多くの国々における政策の一つの柱となってきた。今後のグローバル化の進展を考えると，これは決して一過性のものでなく，21 世紀を特徴づけるキーワードとなるだろう。21世紀のもう一つのキーワードはいうまでもなく情報化であり，この二つのキーワードの接点となるのが情報セキュリティである。情報セキュリティとは，情報および情報システムを，それに対する様々な脅威から守ることを言う。これを達成するためには，法・制度，運用・管理，監視・監査，保険，倫理，教育・啓発など，さまざまな面からの総合的対策が必須であるが，その基盤となるのは技術である。

ここで，安全・安心への流れが顕著に現れているもう一つの分野，道路交通をみてみよう。世界における交通事故死は，急速に増加する傾向にあり，将来は人の主要な死因になると予測されている。先進国では必ずしも交通事故死が増えているわけではないが，高齢運転者の増加などにより楽観できない状況にあり，交通事故死 0 を目指した取り組みも始まった。このためには，法・制度の整備，教育・啓発によるマナー向上なども重要であるが，技術的な対処なしに，交通事故死 0 を達成することは不可能であり，これが今日 ITS（高度交通システム）などによる運転支援や自動運転が注目されている理由である。

この事情は，情報セキュリティでも同じである。しかも，国境のない情報ネットワークの世界では，情報セキュリティ対策は世界が相手となる。たとえ世界中に善良な人しか住んでいないとしても，過誤に基づくプライバシー侵害等はいつでも起こり得るし，現実は残念ながら，悪意のある人が世界に満ち溢れている。このような状況下では，技術的な情報セキュリティ対策なしに安心できる情報化社会を実現するのは不可能である。また，たとえ悪いことをしたいと思っても技

術的にできないようにしておくのが,人に優しい社会と言えるだろう。もちろん,技術的対策にはコストが掛かるし,システムの使い勝手も悪くなるかも知れない。これらのバランスを決めるのは社会であるが,技術開発によってコストの増大や使い勝手の悪化を抑えながら高いセキュリティを保つシステムを構築していくことは可能であり,それが情報セキュリティ技術の主要な役割の一つである。

社会が決めるべきもう一つ重要なバランスは,社会のセキュリティとプライバシーのバランスである。情報化社会は個人情報が一元的に管理される完全管理社会になる恐れもある。社会に属するすべての個人のあらゆる行動が監視される社会である。このような社会では,一般的な意味での高いセキュリティが達成できるかも知れない。しかし,多くの人はそのような社会を望まないであろう。一方,何でも匿名でできるという社会も決して住みやすい社会でないことは,今日の中傷・迷惑メールの横行から予測できる。その社会に応じたセキュリティとプライバシーの適切なバランスを保つことが重要であり,それを可能にする情報システムを提供することも情報セキュリティ技術の重要な使命である。

以上のような役割を担う今後の情報セキュリティ技術において,重要な点をいくつか挙げておこう。第1点はヒューマンクリプトである。高齢者も含め社会の誰もが情報セキュリティ技術を用いねばならない状況にある今日,人という要素を無視して情報システムを構築することはできない。人にできるだけやさしくしかも安心感を与えるようにシステム(特に情報セキュリティの基盤である暗号システム)を設計するというのが,ヒューマンクリプトの考え方である。例えば,長いパスワードをいくつも使うというようなことは避け,高齢者にも負担は少なく,しかも高い安全性を保つ個人認証技術などはその一例と言える。

第2点として継続的評価が挙げられる。情報システムのセキュリティレベルは時間の経過とともに劣化していくのが一般である。これは,コンピュータの性能向上などによる攻撃力の進展やそのシステムの利用範囲の拡大などにより避けがたい。このため,情報システムのセキュリティレベルは,構築時に評価するのはもちろんであるが,その後も継続的に評価し,必要があればセキュリティレベルを保つ対策を施さねばならないし,そのような状況が予想される場合には,予めセキュリティレベルを調整できる設計にしておくことが望ましい。

第3点として挙げておきたいのは,正しい専門的知識の利用である。情報セキュリティ技術は決して簡単な技術ではない。攻撃側はどこでも攻撃できるが防御側はあらゆるところを守らねばならないという情報セキュリティ技術特有の難しさがあるからである。このため,そのシステムに適切な攻撃モデルを設定することも,安全性を定義することも難しい。一方,情報セキュリティに関する情報は多く流布しているが,信頼できるのはごく少数である。今後情報システムの設計には,信頼できる情報セキュリティの専門家を最初から参加させるべきであろう。

第4点として,現在用いられている情報セキュリティシステムの問題点を挙げておこう。現在ネットワーク上で行われている電子入札,電子マネー,電子投票,電子政府などの様々なサービスは信頼できるとされる機関が管理している場合が多い。このため,比較的簡単な情報セキュリティ技術を用いることができる。ところが,このような「信頼機関」からの情報漏洩が大きな問題となっている。今後は,このような問題を生じない,より高度な情報セキュリティ技術の適用を検討すべきである。

以上述べてきた情報セキュリティ技術は,第一義的には情報や情報システムに対する脅威に対処し,安全・安心をもたらす技術であるが,これはまた,社会に繁栄をもたらす技術でもある。前述のような新たなネットワークサービスは情報セキュリティ技術があってはじめて実現できたものであるし,また,安全で安心できる便利な情報システムが整備されているところに世界中からビジネス,マネー,コンテンツが流れ込んでくる。今後,情報セキュリティ技術はビジネスの一つの大きな柱となっていくことは疑いない。