特別講演 1

コンピュータセキュリティの基礎と最新研究動向

加 藤　和 彦

（筑波大学大学院システム情報工学研究科
コンピュータサイエンス専攻）

インターネットは，我々が暮らす一般社会のようなものです．そこには家族や，職場の仲間だけではなく，見ず知らずの他人，あるいは，犯罪を企む人まで，さまざまな人々が棲んでいます．インターネットが一般社会で使われ始めた頃は，メール，ニュース，Web 等の，比較的に限られた使用でしたが，今日では，e コマース，さまざまな企業活動，個人の情報記録やコミュニティの情報共有・交換，そして家電機器の接続まで，一般社会とインターネット社会の一体化が進行しています．

一般社会で暮らす我々は，子供の頃から，自分の身を自分で守りながら暮らす術を親や知人等から学び，社会活動を営んでいます．インターネットが一般社会と一体化しつつある今日，我々は，インターネット上で，自分の身を自分で守る方法を身につけながら，それがもたらす大きな恩恵を享受していく必要があります．

今回の講演では，インターネット環境を念頭においたコンピュータセキュリティの基礎的な事項と，最新研究動向の実例を分かりやすく説明します．

基礎的な事項として解説する第一点は，バッファオーオーバーフロー攻撃と呼ばれるものです．この攻撃は，現在でも多くなされるコンピュータセキュリティの攻撃で，しかも驚くべき性質を持っています．初心者が書いたプログラムが簡単に攻撃の標的になってしまいます．たとえば，C 言語の基本標準ライブラリ scanf や strcpy を使用しているプログラムは攻撃の標的になる可能性があり，最悪の場合，ファイルを勝手に書き換えられたり，情報漏洩を引き起こす可能性があります．これはつまり，今日では，プログラミングの初心者もセキュリティに注意を払いながらプログラミングをせねばならないということを意味します．

基礎的な事項の第二点として，暗号技術の概要を説明します．インターネットで，クレジット番号やパスワード等の非常に重要な情報を送信しても安全が保たれているのは暗号技術のおかげです．暗号というと，難しいメカニズムを想像されるかもしれません．しかし，暗号系 RSA は，現在最も広く使用されている暗号の一つですが，中学生でも理解できるレベルの数学を巧みに使った，非常にエレガントなアルゴリズムです．

最新研究動向として，当発表者らの研究グループが研究開発を進めている，仮想マシンレベルでセキュリティ機能を提供する純国産仮想マシン BitVisor の概要を説明します．このシステムは，文科省科学技術振興調整費，総務省 SCOPE という大型研究予算の支援を受け，産官学の共同で研究開発に取り組んできたものです．オペレーティングシステムとハードウェアの間で，仮想的なマシンを動作させ，仮想マシンのレベルでセキュリティ保全機能を提供します．これにより，OS の選択や，ユーザの設定に依存せず，可能なセキュリティ機能を提供することが出来ます．