■ 高倉　弘喜 アーキテクチャ科学研究系　教授

【「光」と裏腹の「影」に備えるサイバーセキュリティ研究】

高校時代はどちらかといえば文系タイプだったのですが、アマチュア無線好きが嵩じて大学の情報工学科に進みました。ところが偶然から、卒業研究でコンピュータの研究に携わり、その後様々な分野に関わって、助教授でサイバーセキュリティ（以下、セキュリティ）の研究を始めて現在に至っています。セキュリティには、幅広い知識が必要なので、これまでの経験と知識は、文系タイプだったのも含めて、今も役に立っています。

自動車の乗っ取り運転まで起こっている、現在のインターネット

大学や研究機関では、数多くの情報が取り扱われています。その中には、学生の住所や成績など教育にかかわる個人情報はもちろんのこと、研究に関する情報、組織と運営に関する情報など、守らなくてはならない情報が数多く含まれています。様々なサイバー攻撃のリスクに対し、大学や研究機関は予測して備え、問題が発生した際にはすぐに対応し、被害を最小限に食い止める必要があります。それが、2000 年代の私の研究テーマでした。

ところが 2010 年代に入り、「IoT（Internet of Things: モノのインターネット）」、あらゆるモノをインターネットに接続し、インターネット通信を用いてセンシングや制御を行おうとする動きが盛んになりました。特に動きが早かった米国では、現在、高速道路の電光掲示板も自動車もコーヒーメーカーもTV も化学プラントの制御システムも、インターネットにつながっています。もちろん、たとえば自動車のカーナビがサイバー攻撃されたとしても、自動車のエンジンコントロールには影響が与えられないように対策は取られているのですが、開発者の詰めが甘いと、サイバー攻撃によって自動車の制御を乗っ取ることができます。この攻撃は実際に起こり、数百万台のリコールへと発展しました。

日本では、インターネット事情や各メーカーの考え方の違いが幸いし、さまざまな問題が発生してはいるものの、現在のところ、そこまで危険な事態は発生していません。しかしグローバル化の流れの中では、決して油断できません。

必要とされる人材育成とその方法も視野に入れつつ

今の日本で、セキュリティについて最も深刻な問題の一つは、人材育成です。飛び抜けた技術力を持つ人は時々現れるのですが、マネジメント能力を習得するチャンスが得られないことが多いのです。現在の日本に足りないのは、有能な技術者たちの技術や仕事の内容を理解し、彼ら彼女らの技術を生かす一方で、企業の経営陣に対してはセキュリティに関する情報を経営判断に役立つように分かりやすく説明できる、技術にも法律にも経営にも一定の知識と理解がある人材です。既に欧米各国や韓国では、セキュリティマネジメント人材を育成するためのコースを作り、技術者育成とは別ルートで育成しています。「技術者として修行すれば、マネジメント能力も身に付く」という日本的人材育成では、限界があるかもしれません。

でも、セキュリティの世界に「最初から完璧、その後もずっと完璧」はありません。現実はいつも「絶対安全」と「まったく危険」の間のどこかにあります。セキュリティも、セキュリティ人材育成も、バランスを取りながら前進させていきたいですね。　（取材・構成　みわよしこ）