暗号とネットワークセキュリティ

東京大学　生産技術研究所
教授　今井　秀樹

暗号技術がネットワークセキュリティの基盤の一つであることは、ネットワークセキュリティに関わる人なら誰でも理解していることでしょう。しかし、暗号だけで、ネットワークセキュリティが解決できるわけではないことも明らかです。では、ネットワークセキュリティ全体のなかで暗号はどのような地位を占めるのでしょうか。「今、暗号は使えるものがいくらでもある、適当に選んで使えばよい。暗号はただの道具の一つ。」という考え方が主流なのかも知れません。確かに、それも一理あります。ただし、暗号を選ぶ際には、CRYPTRECの電子政府推奨暗号リスト*などを利用して、安全なものを選ぶ必要があります。

しかし、暗号をブラックボックスとしてだけ扱うのは、余りにももったいないことです。暗号は、安全性を最も厳密に扱う科学であり技術です。情報セキュリティを考える際に、暗号の考え方がとても役に立つのです。ある著名な暗号技術者が「情報セキュリティを考える際、暗号を考えなくてよいことはない」と言っていましたが、その通りであると思います。どのような前提のもとで安全性をいかに定義し、それをどのようにして保証していくのかについて、最も論理的に扱っているのが暗号分野なのです。

暗号の考え方が有用であることを示すには、暗号研究者が暗号分野以外のセキュリティ分野でいかに活躍しているかを見れば十分でしょう。一流の暗号研究者は安全性についてあらゆる点から論理的に考える習慣が身についています。このため、システムの脆弱性に関し、鋭い洞察力を持っているのです。例えば、横浜国立大学の松本勉教授がほとんどの指紋センサーを欺ける偽造指紋をグミで作れることを示したことは、バイオメトリックス認証における重要な研究成果として世界的話題になりました。彼は筆者の弟子で暗号研究者に他なりません。このような例は他にも多くあります。

ただ、暗号理論で扱えるモデルが、非常に簡単なものに限られていることは事実です。現実の複雑なシステムにそのまま適用することはできません。しかし、最近、複雑なシステムでも簡単なモデルの合成で表せるなら、その安全性を要素モデルの安全性に基づいて議論するという研究も多くなされるようになってきました。将来は、かなり複雑なシステムでも、暗号的手法で厳密に安全性を議論できるようになるかも知れません。

もちろん、そうなったとしても、人を重要な要素として含む複雑な情報システムの安全性を、すべて理論的に厳密に扱えることはないでしょう。ただ、暗号技術や暗号的

な考え方がネットワークセキュリティ全般においても、次第に大きな部分を占めていかねばならないと考えています。それにより、簡単には崩せないセキュリティのコアの部分が拡がり、人が神経をすり減らさなくても安心して利用できるネットワークが実現していくと思えるからです。ネットワークセキュリティに携わる方々に、ここでもう一度、暗号の重要性を見直してして頂ければ、筆者として望外の幸せです。

* http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index.html
  http://www.ipa.go.jp/security/enc/CRYPTREC/index.html