巻/頭/言

安全だけど安心できない，安全でないけど安心できる

Secure but not safe, or safe but not secure?

菊池浩明
Hiroaki Kikuchi

子供を釣りに連れて行ったらオニオコゼに刺されてしまった。ポツリと血がにじんだぐらいのけがだというのに，さっきまでは平気で針を外していた魚に触れなくなってしまった。一度痛い目に会うと体が痛みを覚えていて，いくら親が安全だと勧めても，もう信用してくれない。

信用できないのは，魚か親父かはさておき，失った信頼はなかなか取り返せないものである。彼にとって，魚は安全でも“痛くない”という言葉が信じられなくて安心できない。安心とは，仕組みが安全であり，その安全性を確信して心が穏やかな様を言う。安全学の権威である明治大学の向殿教授によると，

安心＝安全×信頼

の法則がある(1)。安全と信頼のどちらが欠けても安心できない。安心を築くには長い時間がかかるのに対して，失うのは一瞬である。

近年のサイバー攻撃は，従来有効と信じられてきた情報セキュリティ対策をすり抜けるほど，高度に進化してきている。高度な暗号技術の適用，厳重なネットワーク不正アクセス対策，厳格な法令遵守を実施しても，サイバー攻撃によって情報セキュリティを守りきれなかった事例が増えている。あらゆる情報が電子化されて効率的に交換されている情報化社会にとって，サイバー攻撃は安心を脅かす脅威として，影響力を増してきた。

そもそも私たちは，“絶対に安全なセキュリティは信頼できない”ことを知っている。例えば，RSA公開鍵暗号は，何ビットに拡張しても偶然に素因数分解できてしまう小さな確率がある。どんなに厳密に安全性が評価された共通鍵暗号を使っても，鍵の元となるパスワードの選び方が安直ならば，容易に解読されてしまう。いかに法令遵守を徹底しても，悪意をもった内部者の犯罪を防ぐことは難しい。セキュアなOSの脆弱(ぜいじゃく)性に対するパッチの頻度は，そのソフトウェアの複雑性に依存して増加する。パッチを当てて安心しても，直ぐに次のパッチがリリースされ，いつになってもなかなか安心できない。結局のところ，情報セキュリティには“完全”はない。

では，リスクを消費者に明示することが製造者の責任を果たすことになるのだろうか。

“この金融商品は元本割れのリスクがある”といったリスクの説明が販売者に義務付けられている。リスクを知った上で，リターンの方が上回ると判断した消費者は購入する。リスクを説明していれば，元本割れが発生した場合の責任を販売者が問われることはない。

セキュリティの製品・サービスもリスクとリターンを消費者が判断できるように，分かりやすく説明する必要があるだろう。難しい暗号理論や証明を利用者に分かりやすく説明して納得してもらうための努力を惜しんではならない。

安全や信頼に疑問があって，安心できない場合，以下の２つのケースで安心してもらうことが考えられる。

(1) 安全だが信頼できない

安全を信頼させることが重要である。飛行機が怖い人がいる。事故が起きる確率は非常に小さいが，起きた時に逃げられないという恐怖が彼らの信頼をなくしているのではないだろうか。そこで，事故が起きることを想定して対策を立て，見えない脅威を正しく見せる必要がある。公平に調査した結果を示すことが，安心を呼び起こす手段である。

(2) 信頼しているが安全でない

リスクがリターンよりも小さいことを示すことが重要である。発がん性が分かっていても喫煙者はいる。しかし，他人への配慮は必要だが，その許容リスクが正しく理解できていれば，煙草を吸うことによってリラックス効果が得られるなどのメリットを享受できる。リスクの大きさとその対策となる情報セキュリティの原理と限界が明確に分かっていれば，たとえ完全な安全でなくても信頼できるのではないだろうか。

冒頭の話に戻る。オニオコゼはおいしい。非常に美味であるとともに可食部が少ないので高級魚と言われている。完全に安全ではないけれど，“使いこなせば有益な情報セキュリティ技術”を刺されないように食したい。

(1) 向殿政男：安全とファジィ～どこまでやったら安全か～，知能と情報(日本知能情報ファジィ学会誌)，**24**，No.2，55～62 (2012)

◆東海大学 情報通信学部 教授
Professor, School of Information and Telecommunication Engineering, Tokai University