数学の時代 1

暗号の闘い 社会を支える

今年7月、米自動車大手「FCA US」（旧クライスラー）は、米国で「チェロキー」など一部車種の計約140万台をリコールすると発表した。インターネット通信機能を通じたハッカーの攻撃により、外部からエンジンなどを操作されるおそれがあることが判明したためだ。

ハッカーから防御

「こうした事態は以前から懸念されていた。ただ、こんなに早いとは…」。九州大学マス・フォア・インダストリ研究所（福岡市西区）で教授を務める数学者の高木剛（46）は表情を曇らせる。なぜ、数学者が自動車の心配をしなければならないのか。

クレジットカード決済やウェブ上の個人認証など、現代社会のセキュリティーは暗号技術なしに成り立たない。それを支えているのが、数学だからだ。

現在、広く普及している暗号技術のひとつ「RSA暗号」は、大きな整数の素因数分解が難しいことに立脚している。ふたつの素数から積を求めるのはたやすいが、その整数からふたつの素数を割り出すことは困難という、数学の原理に基づいているのだ。

最新の技術では約600桁の整数を使っており、スーパーコンピューターでも計算に数万年もの時間がかかることから、実質的に暗号を破ることはできないとされている。

国家機密も丸裸

近年、ほかにも「楕円曲線暗号」や「ペアリング暗号」などが知られている。いずれも高度な数学が応用されているが、完璧に安全だと証明されているわけではなく、解読技術といたちごっこの状態だ。

高木は「もし広く普及している暗号技術が破られてしまうと、国家機密から個人情報までが一夜にして丸裸になることもありうる」と危機感を隠さない。

開発が進んでいる「量子計算機」と呼ばれる次世代のコンピューターが実用化されれば、RSA暗号は瞬時にして破られると予想されている。そのような事態を避けるため、高木らは常に新たな理論の構築に取り組んでいる。目下の研究テーマは、量子計算機でも破ることができないという「ポスト量子暗号」だ。

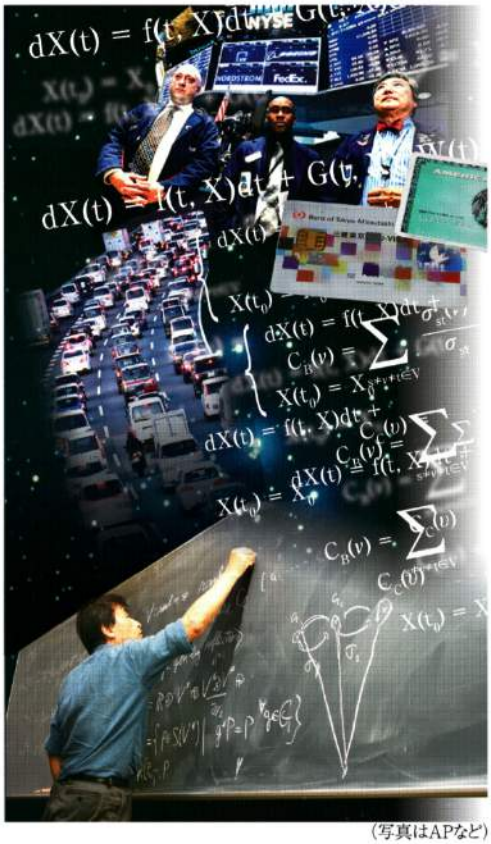
技術は日々進化

そもそも現代の暗号の歴史は第二次世界大戦までさかのぼる。ナチス・ドイツの暗号機「エニグマ」を破ったことで知られる英国の数学者、アラン・チューリングに代表されるように、それは当初から数学者たちの闘いだった。

ただ、数学を社会の基盤と位置づけて積極的に活用してきた欧米諸国などと異なり、純粋数学の研究を尊重する日本では数学者が現実的な課題に取り組むという発想は薄かった。

暗号技術の第一人者として政府の委員会メンバーなどを務める高木も、「私が学生だった20年前は暗号技術を専門とする数学者はほとんどいなかった」と振り返る。現代では高度な情報通信の発達とともに暗号は社会全体にとって必要不可欠なものとなっている。

高木は語る。「暗号と解読の技術は日々、進化している。私は、まだ数学からのアプローチが足りないと思っている」（敬称略）



（写真はAPなど）

暗号技術に利用される素因数分解の原理

2つの素数　33343×67891

素因数分解は難しい ↑ ↓ 積を求めるのは容易

大きな整数　2263689613

最新の暗号技術では約600桁の整数を使用

今年は、ノーベル医学・生理学賞と物理学賞を日本人が相次いで受賞し、日本の宇宙探査機「あかつき」が金星周回軌道投入に成功するなど、多くの科学ニュースが注目を集めた。これらを根底で支えているのは数学に他ならない。

ビッグデータを扱うには高度な数学が必要であり、ウォール街やIT産業を動かしているのも数学者だ。現代社会を動かす基本原理でありながら、一般には近づきがたい印象もある数学の世界に、さまざまな角度から迫りたい。