岐阜新聞真学塾

コラム　岐阜聖徳学園大学教育学部教授
数学専修・室政和

デジタル通信では公開鍵暗号と呼ばれる暗号方式が使われています。このアイディアは簡単で，情報を暗号化する暗号化鍵とそれを元に戻す復号鍵を分離するのです。暗号化鍵は暗号化するときだけ使います。元に戻す操作には使えません。復号鍵を知らないと暗号化はできても復号ができません。これを使って通信を始める前に暗号化鍵だけを相手に伝えます（復号鍵は秘密です）。相手はその暗号化鍵を使って暗号化して情報を送ります。暗号化された情報を受け取った人は復号鍵も持っていますのでそれを使って復号できますが、そのほかの人は暗号化の鍵しか知りませんから（暗号化した人も含めて）復号できません。このようにして安全な通信ができるようになるというわけです。そのためには，暗号鍵から復号鍵を計算することが難しくなければいけないのですがそういう仕組みを見つけるのが大変でした。

量子コンピューターと暗号

この暗号は20世紀の後半になってからＲＳＡ暗号で実用化されます。このＲＳＡ暗号が成功したのは、「現在のデジタルコンピューターでは桁数の大きい整数の因数分解は難しい」という数学的な事実を利用したからです。暗号化鍵から復号鍵を計算するのにはこの因数分解が必要になるのです。このＲＳＡ暗号ができてから何十年も経ちましたが、この暗号方式を破る方法は見つかっていません。それどころか、この公開鍵暗号は暗号通信にとどまらず、電子署名（誰が文書を書いたのかを暗号を使って証明できる方法）にも使えます。それを利用して今最も話題になっているのがビットコインをはじめとする暗号資産です。ここでは電子署名が有効に使われています。公開鍵暗号は現在のネットワーク通信のセキュリティにおいて基幹的な役割を果たしており、これなくして現在のネットワーク社会は実現しなかったと言っても過言ではありません。

ところで、最近「気になる」ニュースがあります。コンピューターの原理を根本から変えた量子コンピューターの研究が近年になって盛んになってきました。量子コンピューターでは従来のデジタルコンピューターより「ある種の計算に限って言えば」ずっと高速の演算ができます。そして、もし量子コンピューターが実現したらＲＳＡ暗号において暗号鍵から復号鍵を簡単に計算できるという研究結果があるのです。そして、最近の研究の進展から、数十年内に実用的な量子コンピューターが実現するかも知れないという見通しをたてる人が出てきました。ＲＳＡ暗号は現在のデジタルコンピューターに対しては安全なのですが、あと数十年でＲＳＡ暗号は使えなくなると大胆な予想をする人もいます。その一方で、量子コンピューターが実現してもそれに耐えうる耐量子コンピューター暗号の研究も行われています。私達の生活にはＩＴ技術が浸透しており、この技術の基礎となる暗号の役割は非常に大きくなっています。今使われている暗号が誰にも簡単に破られるようになれば現代世界に深刻な影響を与えるのは確実です。技術的な進歩は突然起こることがあります。量子コンピューターの研究はこれからどうなっていくでしょうか？