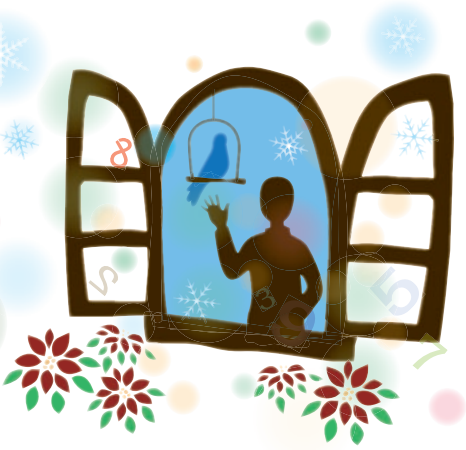
数理の窓



量子コンピュータの憂鬱

最近、量子コンピュータの実用化も近いのではないかと思わされるニュースがあった。今年8月、商用量子コンピュータを開発しているカナダD-Wave Systems社は、1000個を超える「量子ビット」を搭載する量子コンピュータの出荷を開始したと発表した。この新モデルでは「組み合わせ最適化問題」を現行の「古典的コンピュータ（いわゆる0と1のビットで計算するコンピュータ）」よりも「最大で600倍高速」に解けると主張している。夢の技術の実用化は意外と早く訪れるかもしれない。

量子コンピュータは「0」と「1」を重ねあわせた状態を持つ量子ビット（キュービットと呼ばれる。q-bit：Quantum bit）を用いることで、ある種の問題を古典的コンピュータとは比べ物にならない速度で解くことができる。例えば、量子コンピュータを用いてデータベースを検索するための「グローバーのアルゴリズム」がある。古典的コンピュータではN個のデータからある値を検索するには一般にNステップの計算が必要だが、このアルゴリズムではNの平方根ステップ（$\sqrt{N}$回）で検索できる。この「グローバーのアルゴリズム」はNが大きい場合に威力を発揮するため、大量データを扱う人工知能の機械学習の高速化への応用が近年研究されている。

この夢のコンピュータが実現すると、実は困ったことが起きる可能性がある。現在知られている古典的コンピュータを用いて最も効率的に素因数分解を行うアルゴリズムでは、128ビットの整数（約40桁の数）を素因数分解するのにおおよそ「10の40乗回」の計算が必要となる。こうした素因数分解の計算困難性は、現在広く利用されているRSA暗号などの「公開鍵暗号方式」の安全性の拠り所となっている（ちなみにBitCoinにも公開鍵暗号方式が利用されている）。

ところが1994年、AT&T Bell研究所のピーター・ショアは、量子コンピュータ（厳密には「量子デジタル型（量子ゲート型）」の量子コンピュータ）を利用することで、素因数分解を実用的な時間で計算できるアルゴリズム（「ショアのアルゴリズム」）を発表した。これを用いると、原理的には数回から数千回程度の計算で素因数分解が可能となる。つまり量子コンピュータが実現すると、上述の公開鍵暗号方式の安全性は保証されなくなってしまうのだ。この事態に対応するため、量子コンピュータでも解読されないような暗号アルゴリズム（「格子暗号」などが代表例）の研究が現在活発に行われている。

金融の世界では様々な場面で公開鍵暗号が利用されている。量子コンピュータは新たな憂鬱の種をもたらすかもしれない。

（柏木 亮二）