２０１９．５．７

畑　啓之

量子コンピュータおよび量子暗号に政府がいよいよ力を入れると

現在用いられている公開鍵暗号は、二つの大きな素数の賭け合わせである合成数を、素因数分解して、元の素数に戻すことをその基本原理としています。強力なコンピュータを用いても、公開鍵がないとその素因数分解に長時間かかってしまい、第三者からは情報が守られるという仕組みです。

最近話題になっている量子コンピュータでは、近い将来にこの素因数分解を短時間で行うことができ、公開鍵を用いる現在の方式が使えなくなるのではとの心配です。情報化時代の現代、この量子コンピュータの脅威を無視することはできません。逆に、量子コンピュータ技術を深耕していけば、暗号技術のみならず、従来スーパーコンピュータに頼っていた種々の解析が短時間で、しかも高精度でできる可能性も出てきます。

日本経済新聞　２０１９年５月６日

9　科学技術

量子技術研究に中核拠点

政府検討　産官学の連携促す

スーパーコンピューターをしのぐ性能を持つとされる量子コンピューターなどの実現に向け、政府は「量子技術」の研究開発を担う中核拠点を新設する検討に入った。基礎から応用までの研究や産学連携、知財管理などの機能を集めて開発の速度を上げる。米中などが巨額の予算を投じて開発にしのぎを削るなか、日本がどう立ち向かうかが問われる。

量子技術は人工知能（AI）などに続く次世代のテクノロジーだ。「量子力学」と呼ぶ特殊な法則に基づき、新しい原理のコンピューターなどの実現につながる可能性を秘める。広範な用途での活用が見込まれ、政府は開発の加速に向け「量子技術イノベーション戦略」を年内にも策定する。具体策の柱として検討するのが中核的な研究拠点の新設だ。AIの開発では2015年に産業技術総合研究所が「人工知能研究センター」を設立。16年には理化学研究所が「革新知能統合研究センター」を立ち上げた。量子技術についても産官学の関係者らを集めオープンイノベーションを進める体制を築く。関連費用を20年度の予算要求に盛り込む見通しだ。

開発の目玉になるのが、既存のコンピューターで1千万年かかる計算を数十秒でこなすとされる量子コンピューターだ。AIと組み合わせて画像認識や医療診断、自動運転を高度化したり、たんぱく質の構造解析や化合物の探索を通じて創薬や触媒の開発を高速化したりできると期待される。

このほか「絶対に破られない」とされる量子暗号や、医療応用などが期待される超高感度の量子センサーを含め、幅広い技術の開発に取り組む。量子コンピューターの性能を生かすソフトウエアの研究にも力を入れる。このほど立ち上げた有識者会議を中心に拠点の詳細を詰める。

背景には量子技術を巡る世界の動きがある。彗星（すいせい）のごとく登場したカナダのベンチャー企業、ディーウエーブシステムズが10年に「量子アニーリング」と呼ぶ方式の量子コンピューターを開発。米航空宇宙局（NASA）や米グーグルに利用され脚光を浴びた。

グーグルや米IBM、中国のアリババ集団も量子コンピューター開発に参入し、しのぎを削る。国・地域間の覇権争いも激しさを増しており、米国や欧州では1千億円規模を投じる大型の開発計画が動き出した。中国では20年に安徽省に巨大な研究拠点が完成する見込みだ。投資額は1兆円に達するといわれる。

日本の量子技術関連の予算は年間60億円程度にとどまる。基礎研究に強く優れた研究者も抱えるが、米中などに比べ近年の取り組みは見劣りする。単純な資金力では太刀打ちできず、政府が策定する新たな戦略で日本独自の強みを打ち出せるかが焦点になる。

従来のコンピューターをどれだけ改良しても対応できない問題を量子コンピューターが解けるようになる「量子超越」について、東京大学の中村泰信教授は「感覚的には、あと5年もあれば実現すると考えている」と話す。開発体制を含めてスピード感を持って進めなければ、世界に取り残される恐れが強まる。（牛川暁、三隅勇気）

政府もいよいよこの量子コンピュータ、およびその利用技術に力を入れていこうとしているようです。

私の個人的見解ですが、もし、量子コンピュータで大きな素数が発見され続けて行くならば、素因数分解に基づく公開鍵方式は、用いる素数の桁数は非常に大きなものになるとは考えられますが、将来にわたって利用可能ではないでしょうか。

量子コンピュータ（Wikipedia）
量子コンピュータは、量子力学的な重ね合わせを用いて並列性を実現するとされるコンピュータ。従来のコンピュータの論理ゲートに代えて、「量子ゲート」を用いて量子計算を行う。

量子暗号（Wikipedia）
量子暗号とは、通常は量子鍵配送のことを指す。完全な秘密通信は、伝送する情報の量と同じ長さの秘密鍵を送信者と受信者が共有することで初めて可能になる。この秘密鍵の共有を量子状態の特性によって実現する。計算量的安全性でなく情報理論的安全性であることと、その実装の基礎が量子力学という物理学の基本法則に基づいていることが特徴である。なお、商用に広く用いられる公開鍵暗号は解読に計算時間が膨大にかかるだけ（計算量的安全性）であり、情報理論的に安全な秘密通信ではない。

量子ゲートマシン上で素因数分解を行うショアのアルゴリズムは、2001 年に IBM が世界で初めて 15(=3×5)で実行し、2012 年にブリストル大学が 21(=3×7)の分解に成功して記録を更新した。2019 年 1 月時点で、21 より大きな合成数の分解に成功したと言う報告は出ていない。※ 3 は素数、7 も素数、21 は複数の素数の賭け合わせであるので合成数という。

2011 年に、カナダの企業 D-Wave Systems が量子コンピュータ「D-Wave」の建造に成功したと発表した。

2017 年 5 月、中国の科学研究チームが光量子コンピュータの開発に成功し、初期の古典的コンピュータを超える量子計算能力を初めて示したと発表した。

2019 年 1 月 8 日、IBM は CES において世界初の商用量子コンピュータ（名称：IBM Q System One）を開発したと発表した。

素因数分解（Wikipedia）
インターネットでの認証等で利用されている公開鍵暗号の代表である RSA 暗号の安全性は、巨大な合成数の素因数分解を実用的な時間内に実行することが困難であることと深い関わりがある。

NTT など、「素因数分解問題」で世界記録更新--公開鍵暗号解読に一歩近づくか
ZDNetJapan　2010 年 1 月 8 日

NTT は 1 月 8 日、グループの NTT 情報流通プラットフォーム研究所（NTT 研究所）が海外の研究機関と共同で、公開鍵暗号の安全性の根拠となる「素因数分解問題」で世界記録を更新したことを発表した。

これまでの世界記録は 663 ビット、10 進 200 ケタだが、新しい世界記録は 768 ビット、10 進 232 ケタで 100 ビット以上上回っている。

素因数分解問題は、その難解さから現在公開鍵暗号として普及している「RSA 暗号」の安全性の根拠になる。素因数分解可能なビット数の検証は、RSA 暗号の安全性や強度の有効性をより精密に予測する上で極めて重要とされている。

これまでの世界記録を大きく上回る 700 ビットを超える素因数分解が可能になったが、これは将来的に RSA 暗号で使われている 1024 ビットの素因数分解も達成できる可能性があることを示唆するものと注目される。

暗号技術は量子コンピュータに対抗できるのか？
マイナビニュース　2018 年 9 月 28 日

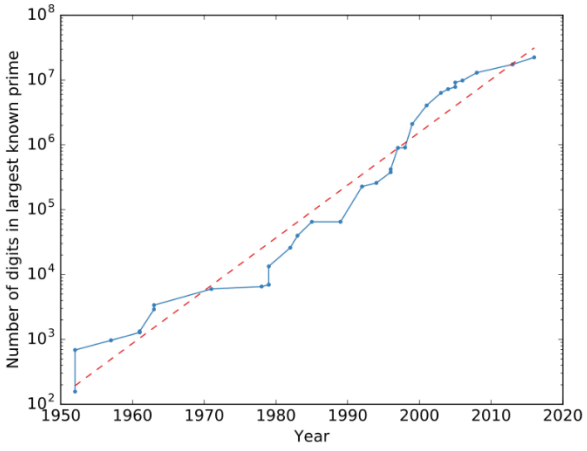
量子コンピュータによって、これまで解読不能とみなされてきた現在の暗号が使い物にならなくなる日が来ることは間違いありません。通信の秘密を守るのに欠かせない公開鍵暗号方式も、そこから逃れることはできないでしょう。
深刻な問題ですが、暗号技術の専門家は早くからこの問題を認識し対策に着手しています。このレポートでは、既存の暗号技術のどの部分が危機にあるのか、いつごろ破られる可能性があるか、そして量子コンピュータ時代に備えて暗号技術の専門家が進めている対応をご紹介します。
現在の暗号アルゴリズムが"いつ"破られるかという点では、見解が別れています。一部の専門家は、量子コンピュータが 10 年以内に先端的な研究機関や大企業の研究部門で実用化されると予測しています。
アルゴリズムの観点からは、量子コンピュータに対抗する 3 つのアプローチがあります。
共通鍵の鍵長を大きくする(現在の平均キーサイズの約 2 倍にする)
ハッシュベースのアルゴリズムを採用する
従来の暗号アルゴリズムと「ポスト量子暗号アルゴリズム」を組み合わせる

過去最大の素数発見、2233 万 8618 桁　米大学教授
これまでより約 500 万桁大きい。
朝日新聞デジタル　2016 年 1 月 24 日

クーパー教授は、世界中のコンピュータをつなげて素数を探すプロジェクト「GIMPS」のメンバー。「２●（●はｎ乗）－１（２をｎ乗して１を引いた数）」で表される「メルセンヌ数」から素数を見つける方法で素数探しを続けている。
これまでの最大は、2013 年にクーパー教授が見つけたｎ＝57885161（1742 万 5170 桁）。今回はｎ＝74207281 が素数であることを約 800 台のコンピューターを駆使した計算で突き止めたという。

巨大な素数の一覧（Wikipedia）

最大記録
2018 年 12 月時点で素数であることが確認されている最大の数は 282,589,933 − 1 であり、十進法表示で 24,862,048 桁である。この素数は 2018 年に GIMPS により発見された。この素数を印字すると



上位10 位の大きな素数

順位	素数の式	発見日	桁数
1	$2^{82589933}-1$	2018 年 12 月 7 日	24,862,048
2	$2^{77232917}-1$	2017 年 12 月 26 日	23,249,425
3	$2^{74207281}-1$	2016 年 1 月 7 日	22,338,618
4	$2^{57885161}-1$	2013 年 1 月 25 日	17,425,170
5	$2^{43112609}-1$	2008 年 8 月 23 日	12,978,189
6	$2^{42643801}-1$	2009 年 4 月 12 日	12,837,064
7	$2^{37156667}-1$	2008 年 9 月 6 日	11,185,272
8	$2^{32582657}-1$	2006 年 9 月 4 日	9,808,358
9	$10223\times 2^{31172165}+1$	2016 年 11 月 6 日	9,383,761
10	$2^{30402457}-1$	2005 年 12 月 15 日	9,152,052