米国金融機関における量子コンピューターの利用

グローバルリサーチ研究所代表
青木　武
あおき・たけし　慶大卒。99年米ニューヨーク大学経営学修士（ＭＢＡ）取得。信金中金総合研究所ニューヨーク駐在主任研究員等を経て、09年7月米国内にグローバルリサーチ研究所（ＩＧＲ）を設立。http://www.igrlc.com/

ＩＢＭは昨年、１０００キュービットの量子コンピューターを発表した。量子コンピューターの開発は順調に行われているようだ。量子コンピューターにより、例えば分子工学が飛躍的に進歩し、患者ごとにカスタマイズした薬の開発や、飛躍的に長持ちするバッテリーの開発などが期待される。米国金融界も量子コンピューターに注目している。例えば、ポートフォリオの最適化、モンテカルロシミュレーション、そして機械学習等に量子コンピューターを利用できるのではないかと期待されている。一方、量子コンピューターが開発されると、現在の素数ベースの暗号は破られることが予想される。そこで、量子コンピューターでも解けない暗号（ＰＱＣ）の開発も進められている。

（1）量子コンピューターとは

量子コンピューターは、かつてのスーパーコンピューターのように部屋いっぱいになるほどの大きなコンピューターであるが、実際のコンピューターの部分は小さく、部屋のほとんどは冷蔵庫の機能である。これは、量子コンピューターを絶対零度に近い温度に保つ必要があるためである。量子コンピューターは古典型コンピューターとは異なり、同時並列的に計算処理ができるため、手当たり次第に何かを探すことに優れている。例えば、膨大な量の電話帳の中から、特定の番号を探すような作業は量子コンピューターに向いており、古典型コンピューターには向いていない。量子コンピューターが得意と思われる分野は、組み合わせ問題、モンテカルロシミュレーション、および機械学習である。組み合わせ問題は、最適な組み合わせを計算することであり、ポートフォリオの最適化が金融機関にとっては優先度が高い。

次に、モンテカルロシミュレーションについては、複雑なモデルによるリスク計算が得意であり、通常のコンピューターでは価値の計算が難しく、計算に24時間以上かかるようなエキゾチックオプションやバミューダオプションのような複雑な金融商品の価値の計算などが考えられる。先述の分子工学でも当該能力が発揮されるだろう。

シミュレーションは金融リスク管理の分野でも利用されていることから、当該分野でも改善が期待できる。最後に、機械学習については、学習のために膨大な計算量が必要となるが、量子コンピューターを利用すれば、パワーアップさせることが考えられる。なお、量子コンピューターと古典型コンピューターでは得意分野が異なっており、古典型コンピューターは掛け算や足し算のような演

算に向いている。量子コンピューターが出てきたところで、古典コンピューターが不要になるわけではなく、いずれ双方の互換性も改善するとみられる。

量子コンピューターの仕組みは難解であるが、フィナンシャル・タイムズの特集記事は比較的分かりやすく解説している。古典コンピューターは0と1との組み合わせになり、8桁の0と1の組み合わせが1バイトという表現の単位となる。つまり、1バイトは28で256通りの表現ができることになる。英語のローマ字は26種類なので、大文字小文字ともこれで十分カバーできる。

ただし、

「01010101」と

「01010100」のように、0と1が一つ違っただけで全く異なることを表現することに注意する必要がある。一方、量子コンピューターの量子ビットは瞬間的に同時に0にも1にもなり得る。ただし、量子ビットが0か1かのどちらにもなり得る「重ね合わせ状態」になるのはわずかマイクロ秒の超短期間であり、その短期間に計算を行う必要がある。これは、コインを空中に投げているときはコインは表にも裏にもなり得るが、地面に落ちればどちらかで確定することに似ている。この重ね合わせにより、例えば迷路を進むときに古典コンピューターなら一度に右か左かどちらかにしか行けないが、量子コンピューターなら右にも左にも同時に行けることになる。これにより、古典コンピューターなら何度も試行錯誤をして迷路を進むことになるが、量子コンピューターならより少ないプロセスで、つまりより早く迷路を抜けることができる。この際、迷路を効率的に抜けるように案内する役割を果たすのがアルゴリズムであり、古典コンピューターのプログラミングとは全く異なる。ただし、コンピューターでは先述の通り、0と1が1カ所違っただけで全く違うことを意味することになるが、量子は安定しないため、エラーが多いことも課題となっている。

(2)金融界における対応

金融界ではJPMチェースやゴールドマンサックスは、すでに量子コンピュータのチームを編成してその対策を始めている。このほか、米国銀行協会（ABA）の機関誌による

と、見込み客へのマーケティング、融資審査モデル、ローンのリスクモデリングによる期限前返済とデフォルトの推定、ローンの証券化におけるポートフォリオの最適化とリスクモデリング、顧客ニーズの推察による新商品や新サービスの提供などを量子コンピューターの利用ケースとして挙げている。

そして今現在、金融機関が行うべきこととしては、

量子コンピューターを使用する可能性のある利用ケースをリストアップする

新しい暗号化アルゴリズムを利用するための計画を策定する

米国国立標準技術研究所（NIST）およびサイバーセキュリティ・インフラ・セキュリティ庁（Cybersecurity and Infrastructure Security Agency）が行っている次世代の暗号およびリスク管理計画を注視する

情報セキュリティ、ベンダー管理、事業継続の専門家を関与させ、リスクの評価と社内調整を行う

勘定系システムプロバイダーやその他の重要な技術サービスプロバイダーに連絡を取り量子関連計画についてヒアリングする

となっている。多くの金融機関にとっては量子コンピューターの専門家を雇うほどの余裕はないとみられるが、長期計画策定において、量子コンピューター対策を行うことは必要であると思われる。

運用会社バンガード社のBimal Mehta氏によると、同社は量子コンピューターの実証実験を始めている。使途として、ポートフォリオの最適化、機械学習、相関関係の発見、シミュレーションなどへの利用を検討している。もちろん、量子コンピューターでも解けない暗号（PQC）の研究も行っている。2030年までには現在主流となっている素数べースのRSA暗号は解かれる可能性があるので、素数を使わない暗号として、どの方式がよいかを評価している。

現在、NISTが幾つかPQCの案を出している。企業等は26年ごろから本格的にPQC対策を行う必要があると考えられる。一方、量子コンピューターにはエラーが多い。このエラーを発見する場合に古典コンピューターのAIが使える可能性がある。本格的な量子コンピューター

は10年後には完成していると思われるが、量子アドバンテージと呼ばれる状態、つまり今のコンピューターではできないことができるようになるまでにはさらに10年かかるかもしれない。

格付け・情報企業のムーディーズ社のCaroline Casey氏によると、同社では洪水リスク、リアルタイムデータなど、古典コンピューターではできなかった計算ができると期待している。ウェルズファーゴのPeter Tsahalis氏によると、量子コンピューターは予想、プロファイリング、最適化が得意であり、デリバティブのモデリングなどができると考えられる。ただし現状、同行において本格的に検討しているのはＰＱＣの分野である。このほか、量子アルゴリズムは、より効率的であり、現在のコンピューターでもＡＩを利用する場合に量子アルゴリズムの発想が使えるという。量子にインスパイアされたアイデアを古典コンピューターに使えるかもしれない。なお、量子コンピューターの利用はわずか1分だが、その結果を分析するのに1年かかるという。

①ＪＰＭチェース

米国最大の金融機関であるＪＰＭチェースの研究者は、量子コンピュータのハードウエアが実用化されたらすぐに対応できるように今から準備をしておく方針である。同行は、グローバルテクノロジー・アプライドリサーチという２０２０年に設置した研究所において量子コンピュータの研究を行っている。具体的には、ポートフォリオ最適化、オプション価格計算、リスク分析、不正検知および自然言語解析に量子コンピューターを利用している。同研究所は、行内のＡＩチームとも連携を密にしている。ＪＰＭは19年、ＩＢＭとの共同研究で、一晩かかって計算していたオプションの価格計算を量子コンピューターならほぼリアルタイムで計算できることが分かったという。ＪＰＭの量子アルゴリズムの多くにはＡＩが組み込まれている。さらに、量子コンピューター、ＡＩともクラウドがベースとなっており、異なるチームで同じ環境を共有できる。また、プラットフォームにより、量子コンピューターのプロバイダーがどこであっても、対応できるようになっているという。

②トゥルーイスト

米南部の大手行、トゥルーイストはＩＢＭと量子コンピューター対応を行っていると発表した。トゥルーイストがＩＢＭ量子アクセラレーターに参加するとともに、ＩＢＭの社員がトゥルーイストに常駐し、協力態勢を強化する。このトゥルーイストのイノベーター・イン・レジデンス・プログラムは、同行が外部の専門家を招き、銀行のイノベーションを促進する制度である。既にアマゾンと通信大手のベライゾンが同行に常駐している。この契約により、トゥルーイストはＩＢＭの量子コンピューティングシステム、専門知識、リソースを利用できるようになる。ＩＢＭは、同行のチームと協力して、量子技術を構築し、この技術が金融分野のユースケースにどのように役立つかを模索する。アメリカンバンカー紙によると、中でもＰＱＣを含めたサイバーセキュリティに力を入れるようだ。銀行が量子コンピューターを利用するからには、ポリシー（規定）、スタンダード、内部統制を整え、的確に対応する必要がある。また、現在の古典コンピューターにおいても、今後は量子コンピューターでも解けない暗号に切り替える必要がある。同行では、アプリケーション開発者、インフラ担当エンジニア、ビジネス側の責任者、サイバーセキュリティ対策担当、ネットワークエンジニア、リスク管理、監査の専門家を含む従業員からなるチームを編成し、量子機能に取り組んでいるという。ＩＢＭアクセラレーター・プログラムでは、トゥルーイストの技術者は、ユースケースをテストしている他のＩＢＭ顧客企業から学ぶことができる。

なお、これらの金融機関のほかに、米銀ではアリーバンクが量子コンピュータの準備を進めている。金融機関の多くは、D-Wave、ＩＢＭ、アマゾン、グーグル、マイクロソフト、QC Ware、Rigetti社などのクラウドを利用した量子コンピューターアズアサービスを利用している。元米連邦預金保険公社（ＦＤＩＣ）のSultan Meghji教授によると、トップ20銀行以外であれば、アマゾン、グーグル、マイクロソフトなどの主要クラウド業者を利用することが最も現実的であるという。なぜなら、こうした大手クラウド企業は、すでに量子対策を始めているからである。

（3）量子暗号対策

先述の通り、ＲＳＡをはじめ現在の暗号の多くは量子コンピューターが実用化されれば解読されるとみられている。そこで、量子コンピューターでも解けない暗号（Post-Quantum Cryptography＝ＰＱＣ）を利用するか、暗号鍵のやりとりを量子力学の原理を利用して安全に行う量子鍵配布（Quantum Key Distribution＝ＱＫＤ）の二つが解決策として考えられている。

ＰＱＣについては、ＮＩＳＴが23年８月に最初のスタンダードのドラフトを出している。具体的には、暗号のCRYSTALS-Kyber、電子署名のCRYSTALS-Dilithiumおよびｓｐｈｉｎｃｓ＋についての標準化の案を発表した。もう一つの電子署名の案であるＦＡＬＣＯＮの標準化案については、24年までに作成する予定となっている。16年から行っていたこのプロジェクトは24年に標準化が終了する。現在の量子コンピューターではまだ暗号を解くには至っていないが、数年以内にはそうなる可能性がある。よって、今のうちに準備をしておく、ということになる。

ただし、これらの４種類で終わり、ということではなく、来年までに補足的に幾つかの暗号の標準化を行う予定となっている。上記の第１陣が破られたときの補完が目的である。

もっとも、今現在、人類は暗号を解読できる量子コンピューターを持っているわけではなく、さまざまな前提をおいて、「これなら量子コンピューターでも解けないだろう」と考えてＰＱＣを開発している。一方、インターネットが普及する前は、誰もアマゾンやフェイスブックのことを思いつかなかった。実際に量子コンピューターが手に入れば、悪者は悪用する方法を考える可能性が高い。一方、サイバーセキュリティは一つの解決策だけで対応するものではなく、玉ねぎのように何層もの異なる対策を重ねて行うものである。そのことは、量子コンピューターが導入された後も変わらない。

企業は今後10～15年かけて現在の暗号をＰＱＣに変えていく必要がある。このほか、これから開発するプロジェクトについては、ソフト・ハードの基本的な構造は変えずに、将来的に暗号の部分だけ取り替えることができる構造とするようにＩＴベンダーに依頼すべきである（KnowBe4社のRoger A. Grimes氏）。また、量子コンピューター対応プロジェクトをまだ始めていない場合、今すぐにでも始めるべきであるという。まずは、経営陣・取締役会を啓蒙（けいもう）する必要がある。これから10～15年以内にほとんどすべてのデバイスを取り替えるかアップデートすることになる。

次に、社内のＩＴ資産を整理してインベントリ（在庫リスト）を作る。これには、どのような暗号が情報資産に利用されているのかを洗い出す。また、暗号鍵のサイズも明記する。これから開発する場合、最低でも２５６ビットの暗号鍵にすべきであり、２５６ビットであれば量子コンピューターでも簡単には解けないとみられるためである。また、重要な情報資産はインターネットから切り離した環境に保管することも考えられる。ハッカーは情報資産を今盗み、後日量子コンピューターが開発されてから解読することも考えられるので、現時点でもサイバーセキュリティには注意する必要がある。

なお、バイデン政権は22年に量子コンピューターについてのロードマップを発表し、米政府としては35年までにすべての暗号をＰＱＣとする方針となっている。つまり、米国は国家としても量子コンピューターに本気で取り組もうとしている。

（3）おわりに

量子コンピューターは良くも悪くもコンピューターの世界を大きく変える可能性があり、そのための備えを今のうちから行うべきと米国では考えられている。その筆頭はＰＱＣ対策であり、膨大な数のデバイスやソフトウエアをどのようにしてアップデートしていくかを検討する必要がある。量子コンピューターには前向きのメリットも多くあるとみられており、各分野においてもどのような利用法があるか、検討が始まっている。例えば、量子コンピューターのアルゴリズムの研究を今のうちから行っておけば、実際に導入された際に迅速に対応できると考えられている。雇用の分野では、現在はＡＩブームのためデータサイエンティストが引く手あまたとなっているが、いずれは量子物理学者が金融機関等でも重宝されるようになるのかもしれない。