strategy&
Part of the PwC network

量子コンピュータがもたらす産業構造変革

著者紹介

樋崎 充（といざき・みつる） mitsuru.toizaki@pwc.com

PwCコンサルティング、Strategy&のパートナー。約20年にわたり、IT関連企業、総合電機メーカー、電子部品メーカー、製薬会社に対し、事業戦略、組織戦略、M&A戦略、SCM戦略の立案および実行支援などのプロジェクトに数多く従事している。

大塚 悠也（おおつか・ゆうや） yuya.otsuka@pwc.com

PwCコンサルティング、Strategy&のマネージャー。IT関連企業、総合電機メーカー、金融・サービス業に対し、中期経営計画、成長戦略、テクノロジーを活用した新規事業の立案および実行支援などのプロジェクトに従事。近年では、量子、AI、セキュリティ、生体認証、デジタルIDなどのエマージングテクノロジー領域におけるコンサルティングを中心に取り組んでいる。

上谷 学（かみたに・まなぶ） manabu.kamitani@pwc.com

PwCコンサルティング、Strategy&のアソシエイト。理化学研究所の研究員（主に超電導体を研究）を経てStrategy&に参画し、製造業・製薬業などのクライアントに対する事業開発支援・新市場参入戦略策定や、PEファンドに対するビジネスデューデリジェンスなど幅広いプロジェクトに取り組んでいる。

問い合わせ先

PwCコンサルティング合同会社 ストラテジーコンサルティング（Strategy&）

〒100-6921
東京都千代田区丸の内 2-6-1 丸の内パークビルディング 21 階
電話：03-6250-1209 Fax：03-6250-1201
jp_cons_srategy-info-mbx@pwc.com
http://www.strategyand.pwc.com/jp

量子「もつれ」と「重ね合わせ」技術

2019年10月、Googleの研究グループが開発した量子コンピュータを使って、スーパーコンピュータでは1万年かかる問題をわずか3分程度で解いたと発表し、世界的に大きな話題になったことは記憶に新しい[*1]。この量子コンピュータに関して、技術面の議論は世界中で多くなされているが、本稿ではまず、量子コンピュータとは何か、その概要を解説したうえで、量子コンピュータの適用が検討される主な産業について、そして、現在世界中の企業・組織で積極的に進められている研究開発の動向について考察する。さらに、量子コンピュータの今後の発展および実装時期に関する予測を提示し、また、実装された後の世界において想定される既存プレイヤーへの影響について、いくつかの産業を取り上げながら解説する。

古典コンピュータと量子コンピュータ

現在、私たちが普段使っているコンピュータは量子コンピュータと対比して「古典コンピュータ」と呼ばれ、0か1の状態をとる「ビット」を情報の基本単位として演算を行う。一方、量子コンピュータは、古典コンピュータのように0か1のどちらかの状態で演算を行うのではなく、「量子ビット」と呼ばれる情報単位を使い、量子力学的な重ね合わせの状態（0と1の状態を同時にとる状態）を活用して演算を行うことで、古典コンピュータよりも高速で問題を解くことができる。さらに、この量子コンピュータには、汎用的な演算に活用できる「ゲート型量子コンピュータ」と、最適化問題に特化した「アニーリング型量子コンピュータ」の2種類が存在する。

ゲート型量子コンピュータ

汎用的な活用が期待されるゲート型量子コンピュータでは、量子ビットの量子力学的な性質を利用してあらゆる状態を作り（量子もつれ）、正解の確率（確率振幅）を増大させ効率的に正解にたどりつくという原理が活用されている。このゲート型量子コンピュータは古くから研究されており、量子ビットを実装するハードウエアの方式は、超電導方式、半導体量子ドット方式、イオントラップ方式、光方式などがある[*2]。その中でも、絶対零度に近い極低温（10mK程度）まで量子ビットを冷却して動作させる超電導方式の量子コンピュータが最も有望視されており、研究開発が進められている。その理由としては、超電導体を用いた場合、イオントラップ方式と比べて量子ビットの制御が容易になること、また、半導体量子ドット方式や光方式と比べて量子ビットの数をより増加させることなどが挙げられる。

アニーリング型量子コンピュータ

ゲート型量子コンピュータ同様に超電導の量子ビットを極低温まで冷却して動作させるアニーリング型量子コンピュータも注目されているが、その計算の原理はゲート型とは異なる。ゲート型が量子ビットを使ってあらゆるパターンを同時に演算するのに対し、アニーリング型量子コンピュータは、量子ビットに与えた外部刺激（磁場）をコントロールし、トンネル効果という量子現象によって安定した状態を探索することで最安定な解にたどり着く方式である。最安定解探索を行えることから、組み合わせ最適化問題を解くことに特化したコンピュータという位置づけである。量子コンピューティングシステムおよびそのソフトウェアを開発・提供するカナダのD-waveが、2011年にアニーリング型量子コンピュータの実機を発売して以降、新しい量子コンピュータとして注目を集めている。

*1：2019年10月24日の日本経済新聞朝刊を参照
*2：QunaSys, 2019.「量子コンピュータの基礎から応用まで」

適用産業

汎用的な計算が可能なゲート型量子コンピュータは、第1段階として量子ビット数が100以上を実現すると幅広い領域で活用が可能となる。次に第2段階として数千万を超えると、現在のさまざまなデータの暗号解読にも活用できるようになると言われている。

量子ビット数が100を超えた際の代表的な適応産業領域は、ヘルスケア、化学・素材などの製造業、金融、公共領域などである。それぞれの領域において、創薬につながるたんぱく質の動きやゲノム解析、新材料創製につながる化合物シミュレーション、オプションプライシングなどの金融取引シミュレーション、地殻・都市の地震や地球大気のシミュレーションを含む災害・気候予測、人・移動体の流れの社会シミュレーション、素粒子のふるまいの計算などが想定されている（図表1参照）。

さらに、数千万量子ビット数が実現されると、現在の暗号方式として活用されているRSA暗号や楕円曲線暗号を解読することが可能になると考えられている。現在の基本的な暗号であるRSA暗号は、素因数分解を行うことにより解けるが、従来の古典コンピュータの能力では桁数の大きい素因数分解問題をすぐに解くことができないため実質的には解読が不可能である。しかし、数億の量子ビットの量子コンピュータであれば、数時間もあれば解くことできると考えられており、近年では、数千万の量子ビットでも可能ではないかという研究成果も存在する。

ただし、この成果は、ある特定の問題について解く時間を比較したときにスパコンよりも高速であるということであり、RSA暗号を今すぐ解読できるわけではないことを付け加えておきたい。

また、汎用性に優れたゲート型量子コンピュータに対して、アニーリング型量子コンピュータも解きたい問題を組み合わせ最適化問題として設定することにより、適応産業・ユースケースをゲート型とほぼ同じにすることができると考えられている。高分子・無機材料の組み合わせや社会システムにおける交通経路の最適化など、最適化問題を求解するための活用が期待されている。ゲート型よりも先に実装され始めているため、当面組み合わせ最適化問題についてはアニーリング型の活用が進むと想定される。

図表1
量子ビット数と適用可能な産業

量子ビット数	主な産業	ユースケース（例）
100～	ヘルスケア	創薬探索
	化学・素材等の製造業	新材料創製
	金融	金融取引シミュレーション
	公共	災害・気候予測 人・移動体の流れの分析
	宇宙・素粒子物理学等の基礎研究	初期宇宙のモデル検討、 素粒子の振る舞い
数千万～	サイバーセキュリティ	RSA、楕円曲線暗号解読

出所：Strategy&分析

研究動向

この新たな原理を用いた量子コンピュータに多くの企業・組織が期待を寄せ、積極的な研究開発が進められている。次に、①ゲート型量子コンピュータ、②アニーリング型量子コンピュータ、そして量子コンピュータへの対抗手段としての③量子暗号通信の3つのテーマに関する研究動向を見ていく。

①ゲート型量子コンピュータ

ゲート型量子コンピュータは主に「量子ビット数」、「コヒーレンス時間」、「誤り訂正符号」、「ソフトウェア開発」の4つテーマについて研究が行われている。

・量子ビット数

ゲート型量子コンピュータの性能向上のためには根幹である量子ビット数を増やすことが重要である。現在主流となっている超電導方式のゲート型量子コンピュータについては、1999年に日本のNECが初めて1量子ビットの量子コンピュータを開発した。その後、量子ビット数を増やす研究は行われてきたものの、2010年代半ばまでに開発された量子ビットは最大で5程度で、増加ペースは緩やかであった。しかし、2017年にIBMが50量子ビット、2018年にGoogleが72量子ビットの量子コンピュータを開発するなど、近年量子ビット数は急増している。適用産業の議論にあったように100量子ビット、数千万量子ビットへと今後も開発は継続される。超電導量子コンピュータの開発を進めている企業にはGoogleやIBM、Alibaba、Rigetti Computingなどが挙げられ、公表情報に基づくと、特にGoogleとIBMが開発におけるトップランナーと言えるだろう*3。

・コヒーレンス時間

量子コンピュータを安定動作させるために量子力学的な状態を長く保つ、いわゆるコヒーレンス時間を長くするための研究も行われている。コヒーレンス時間が短くなる一つの要因としては、干渉の問題がある。例として、多数の量子ビットを配置した際に、ある量子ビットの操作をするために送った信号が他の量子ビットに影響を及ぼすことが挙げられる。他の量子ビットに影響を及ぼすと、計算におけるエラーが増え、結果的にコヒーレンス時間も短くなる。さまざまな技術的工夫によりこの改善に向けた取り組みが行われており、2012年にはIBMが量子ビットを三次元的に配線することでコヒーレンス時間を数十μ秒から100μ秒程度まで伸ばした*4。また、このような配線に関する課題は今後量産化を考えるときにも重要となる。必要となる数百・数千の量子ビットを並べるうえで、すべての量子ビットにアクセスするための配線を考慮し、干渉を避け、極低温を維持する最適な設計を行わなければならない。

・誤り訂正符号

現在の量子コンピュータでは、古典コンピュータがもつ誤り訂正機能を実装できていないという課題がある。計算が途中で誤っていた場合に、それを検知し訂正する誤り訂正機能を実現させることは将来的に必須である。現在この誤り訂正機能の実装に関して世界中で研究が行われているが、データ用量子ビットとエラー検出用量子ビットを2次元的に配置する表面符号（surface-code）と呼ばれる誤り訂正方式が大本命の方式として研究されている*5。

・ソフトウェア開発

量子コンピュータを効率的に動かす量子アルゴリズムおよびソフトウェアの開発も積極的に進められており、IBMの「Qiskit」、Googleの「Cirq」、QC wareの「Forge」など、既に一部の企業はソフトウェア開発プラットフォームの提供を開始してい

*3：各社プレスリリースを参照
*4：IBM, "IBM Research Advances Device Performance for Quantum Computing" (28 Feb. 2012)
*5：国立研究開発法人 科学技術振興機構 研究開発戦略センター, 2018,「みんなの量子コンピュータ」

図表2

量子コンピュータおよび関連技術の研究例

カテゴリ	研究機関・企業	製品名プロジェクト名	概要
量子コンピュータ（ハードウエア）	Google	Sycamore	同社は超電導体を用いた53個の量子ビットを搭載する超電導体を用いた量子プロセッサを保有している。Sycamoreを用いて、特定の問題において、従来の古典コンピュータよりも計算能力が高いことを実証したとされている。
	IBM	Q System One	Q System Oneは、2019年のCES (Consumer Electronics Show) で発表された世界初の商用量子コンピュータである。Q System Oneは超電導体を用いて実装されており、20量子ビットをもつ。また、同社が指標として掲げる量子ボリュームでは16量子ボリュームを達成したと発表した。
	Rigetti Computing	16Q Aspen-4	同社は、超電導体を用いた量子ゲート方式のコンピュータ開発を担うスタートアップであり、ハードウエアからソフトウェアまで包括的に開発を進めている。「Forest」という自社のクラウドプラットフォームを運用し、開発者はシミュレーション上の量子コンピュータ向けにコードを書くことが可能である。
	量子信息与量子科技創新研究院（Alibaba）	—	中国最大の自然科学およびハイテク研究開発機関である中国科学院とAlibabaは共同で「量子信息与量子科技創新研究院（量子情報・量子技術イノベーションセンター）」を開設し、同ラボで開発された量子ゲート方式の11量子ビット超電導量子コンピュータをクラウド上で公開している。同ラボでは、2025年までに現在の世界最速のスーパーコンピュータと同等の計算処理能力を持つ量子コンピュータを構築し、2030年までに50～100量子ビットの汎用型量子コンピュータを開発することを掲げている。
量子アルゴリズム（ソフトウェア）	IBM	Qiskit	量子コンピュータを研究・教育・ビジネスに活用するためのオープンソース量子コンピューティングソフトウェア開発フレームワーク。同ソフトウェアを利用することで、16量子ビットのIBM量子コンピュータの利用が可能である。
	Google	Cirq	量子プロセッサ用のアルゴリズムを作成するためのPythonフレームワークの開発を行っている。Googleの量子コンピュータ「Bristlecone」を将来的にクラウドで利用可能にする予定である。また、分子や複雑な材料の特性をシミュレートすることに特化した量子化学計算用のライブラリ「Open Fermion」も既にオープンソース化されている。
	QunaSys	—	量子コンピュータ用のアルゴリズム開発およびアプリケーション開発を行っている。また、開発したアルゴリズムを用いて実際の材料開発をするソフトウェアの開発にも取り組んでいる。
	QCware	Forge	量子コンピュータにおけるデータサイエンスプラットフォームである。クラウドベースで機械学習や化学シミュレーションなどのためのサービスを提供している。
	量子イノベーションイニシアティブ協議会（東京大学、日立製作所、みずほフィナンシャルグループなど）	—	量子コンピューティングを実現する科学技術のイノベーションを日本国内において独自のかたちで集結させ、産官学協力のもとに日本全体のレベルアップと実現の加速化を図り、広く産業に貢献することを目的として2020年7月30日に設立。
量子暗号通信	中国化学技術大学（潘建偉教授研究グループ）	—	中国科学技術大学の潘教授が率いる量子科学実験衛星「墨子号」のチームは、世界で初めて1,000キロ級の衛星・地球双方向量子通信（量子暗号通信）を2017年に実現。
	NICT（情報通信研究機構）、NEC	Tokyo QKDネットワーク	NICT、NECなどが共同で、量子鍵配送（QKD）装置を開発するとともに、2010年に構築した実証テストベッド「Tokyo QKD ネットワーク」上でネットワーク技術の開発、長期運用試験、さまざまなセキュリティアプリケーションの開発に取り組んできた。2019年6月にはこの技術を盛り込んだ国際標準勧告が、量子鍵配送をサポートするネットワークのフレームワークに関する勧告として承認された。
	NIST（米国国立標準技術研究所）	—	2016年2月、NISTは耐量子公開鍵暗号技術の標準化活動を行うことを発表した。格子暗号などのアルゴリズムの候補を絞っている段階であり、2022年～2024年にかけてドラフト準備完了予定である。

出所：Strategy＆分析

る。例えば金融の分野では、量子コンピュータを活用したオプションプライシングの計算も試みられている*6。日本では東京大学を中心とする産学連携の協議会が発足し、IBMの量子コンピュータを活用したソフトウェア開発を加速させる見込みである*7。また、東京大学発のスタートアップであるQunaSysも量子コンピュータ用のソフトウェア開発を進めている（図表2参照）。

②アニーリング型量子コンピュータ

アニーリング型量子コンピュータの研究は、D-waveを中心に開発が進んでおり、既に活用が開始されている。解きたい組み合わせ最適化問題をアニーリング型用のモデル（イジングモデル）に変換し、適用していくこと、効率的なソフトウェアを開発することが主流のテーマである。また、学術的には、現在実装されている量子アニーリングを量子コンピュータと呼んでよいのかという議論がされている。量子アニーリングの理論としては量子的な重ね合わせ状態を活用しているが、それを実機で実現したとされるアニーリング型量子コンピュータでは本当に量子性を活用して最適化問題が解かれているのか、あるいは量子性を活用した結果、古典コンピュータのベストなアルゴリズムよりも計算が高速になっているのかという点について、現時点では完全な検証ができていない。今後、実社会で役立つ問題を解いていくことで、こうした学術的な懸念も払拭されていくかもしれない。

③量子暗号通信

量子暗号通信の分野は、量子コンピュータがもたらす脅威に対抗する手段として盛んに研究が行われている。現在、暗号化に利用されているRSA暗号や楕円曲線暗号は、量子コンピュータが実現した場合に破られる恐れがある。RSA暗号を解読するためには、数千万から数十億量子ビットで数時間必要とされていたが、Googleは解読を行うアルゴリズムである「Shor」の実装における最適化を行い、最大量子ビット数2千万の量子コンピュータによって8時間で解ける可能性があることを発表している*8。暗号解読の脅威に対抗するための研究として、主には通信媒体に量子性を持たせ、光の量子を活用する「量子鍵配送」と、量子コンピュータでもアルゴリズムを高速で解けないものにする「耐量子コンピュータ暗号」の2つの研究が行われている。

量子鍵配送については、特に中国での研究成果が目覚ましい。中国科学技術大学の潘建偉教授の研究グループは、2017年に世界で初めて1,000キロ級の衛星・地球双方向量子通信を実現した*9。さらに、潘教授を中心メンバーとして、量子コンピュータや量子通信の技術に関する実験施設「量子情報科学国家実験室」を安徽省合肥市に建設している。2030年までに、量子暗号通信ネットワークを構築することを目標にしており、量子鍵配送の社会実装が進んでいくことが期待される。日本でもNICT（情報通信研究機構）、NECなどが共同で2010年から量子鍵配送用の装置開発やネットワーク技術の開発を行っている（東京QKDネットワーク）。量子鍵配送をサポートするネットワークのフレームワークの国際標準化に向けて積極的に動いており、2019年には国際標準勧告が承認されている*10。

また、耐量子コンピュータの暗号開発については、2026～2030年頃までに米国連邦政府で使用する公開鍵暗号を耐量子コンピュータ暗号に移行することを想定し、NIST（米国国立標準技術研究所）が標準化を進めている（図表2参照）。

*6：N. Stamatopoulos, et al, 2020. “Option Pricing using Quantum Computers”
*7：東京大学, プレスリリース「[量子イノベーションイニシアティブ協議会]設立」(2020年7月30日)
*8：Craig Gidney, Martin Ekerå, 2019. “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits”
*9：Nature, 2017. “Satellite-to-ground quantum key distribution”
*10：国立研究開発法人 情報通信研究機構、プレスリリース「国際標準化機関ITU-Tで初の量子鍵配送ネットワークに係る勧告が成立」(2019年7月2日)

今後の発展と産業への影響

本章では、ゲート型の量子コンピュータの発展および実装時期を予測し、適用産業に関与するプレイヤーへの影響を考察する。

ゲート型量子コンピュータの発展予測

ゲート型量子コンピュータの発展は、前述の通りスパコンを超える段階、そして暗号解読が可能な段階の大きく2つの段階が存在する。

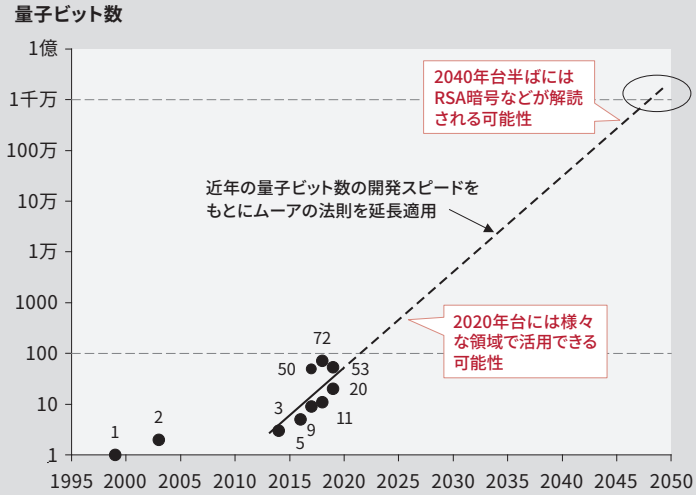
図表3は、スパコンを超える量子コンピュータとRSA暗号などが解読可能な量子コンピュータの実現時期について、量子ビット数に基づいた見立てを示している。まず、量子ビット数が100以上になる第1段階の量子コンピュータは2025年までに実現すると推定される。一方、第2段階となるRSAなどの暗号の解読が可能なレベルの量子コンピュータの実現については、2040年台中ごろと先の未来になると考えられる。なお、量子ビット数の予測にあたり、近年の量子ビット数の進展をもとに1年半で半導体の集積率が2倍になるムーアの法則を量子ビット数に適用した議論を参考にした。

(1)2030年ごろの量子コンピュータの普及状況

暗号解読は、まだ当面先ではあるものの、スパコンを代用していく未来はそう遠くない時間軸で実現する。その際に、量子コンピュータはどのように普及し、活用されているだろうか。超電導のゲート型量子コンピュータが超極低温を維持するかなり大型のデバイスであることを考えると、2030年までに商用化が実現したとしても、それは個人が1台ずつ持つようなものではなく、Google、IBM、Alibabaなど米国・中国系の先行開発する巨大IT企業や国家研究機関が所有し、クラウドを通じて貸し出すモデル、タイムシェアリングとなるであろう。

一方、量子コンピュータに対抗する演算処理として従来のスパコンもより高速な演算ができるような研究も行われている。一説には2020年に実現されているスパコンの演算能力を2030年には個人所有レベルに近しい形で持てるかもしれないとも言われて

図表3
量子ビット数の増加推移と今後の予測(超電導量子ビットの数をベースにプロット)



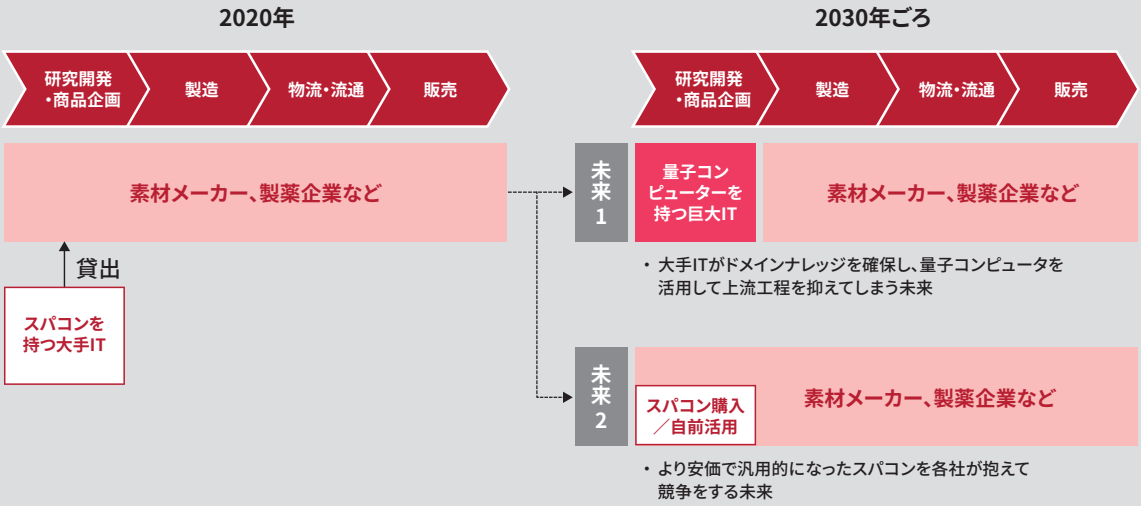
量子ビット数	発表年	開発企業
1	1999	NEC
2	2003	
3	2014	IBM
5	2016	
9	2017	Google
11	2018	Alibaba
20	2019	IBM
50*	2017	IBM
53	2019	Google
72*	2018	Google

*発表段階では、量子コンピュータとしての動作検証中

注)1年半で半導体の集積率が2倍になるという法則を、1年半で量子ビット数が2倍になるという法則に置き換えている
出所:Strategy&分析

図表4

量子コンピュータが創薬・素材産業に起こす変化のシナリオ



出所：Strategy&分析

いる。実際に、データフロー型マイクロプロセッサの活用など、スパコンでも従来の性能向上に向けた開発（マイクロプロセッサ単体の機能向上、マルチコアプロセッサなど）とは異なる新たな方向で計算能力を高める研究が進められている*11。

一つの可能性として、法人企業には現在のスパコンレベル、もしくはそれ以上のスペックのものがある程度行き渡っている未来が想像できる。更にスパコンを遥かに凌駕する演算能力を持つ量子コンピュータを所有する一部の先行開発した巨大IT企業または国家研究機関は、量子コンピュータ活用ニーズのある企業にクラウドを通じて貸し出している状態となっているだろう。

(2) 適用産業に関与するプレイヤーへの影響

量子コンピュータを持つ機関は、現在は国家機関または巨大IT企業であり、巨大IT企業は単に高速コンピューティング処理能力を持つだけではなく、さまざまなITケイパビリティを掛け合わせていくことができるため、適用産業においても複数のポジションをとることができる。

〈創薬・素材産業の場合〉

未だに治療薬が見つかっていないHIVやがん等に対する治療薬の発見、環境負荷の低い画期的な材料等が期待されるヘルスケアや化学・素材などの領域では、関与するプレイヤーにどのような影響が出ているだろうか。創薬・素材の新素材探索は、ドメインナレッジを保有して適切なデータベースを構築し、コンピューティング処理を行うことで可能となる。一つの考えとして、量子コンピュータを保有する巨大IT企業がドメインナレッジを習得、データベースの構築・またはオープン化されたデータベースを活用し、超高速に無数のシミュレーションを行うことで、研究開発の上流工程を握って特許を多数保有、半導体のIPビジネスのような役割に転じることもできるのではないか。そして、材料・薬品の案をもって安価な素材・医薬品メーカーと水平分業することで、既存の製薬・化学・素材などの企業に対し新たな競合となり得る未来も考えられる。もちろん、進化しているスパコンを活用して対抗することは可能かもしれない。しかし、製薬企業が、現在推し進めているIT企業や創薬ベンチャー、CROなどとの水平分業や協力関係によるドメインナレッジを、この後の10年で

*11： 理化学研究所、佐野 健太郎、計算科学の世界「スパコンはどこまで速くできるのか？新しいアーキテクチャの可能性を追求する」

巨大IT企業が獲得していった場合、新たな競争が起こり得る可能性は否定できない（図表4参照）。

〈金融の場合〉

量子コンピュータの活用先として、リアルタイム性やリスク予測の重要性が高い金融領域（金融取引）でも大きなインパクトを持つかもしれない。金融機関が他社よりも優れたアルゴリズム/ソフトウェアを開発できれば、その金融取引における利益に莫大な差が生まれ、そのインパクトは非常に大きいであろう。既に高速取引が市場に大きな影響を与えているが、フィンテックや貨幣の電子化が進み金融領域と非金融領域の境目が曖昧になり、量子コンピュータ開発先行企業が圧倒的なコンピューティング処理能力を持っている世界では、その企業がドメインナレッジや免許を取得し金融領域に参入すると、計り知れない影響を持つことが想像される。

全産業にまたがるセキュリティ領域への影響

さらに、量子コンピュータが最も活躍するのはサイバーセキュリティの領域である。RSA暗号や楕円曲線暗号の解読が可能になる第2段階においては、国防も含めたサイバーセキュリティ領域に多大な影響を与える。

ゲート型量子コンピュータを最初に開発した企業もしくは国家が暗号解読において圧倒的優位性を持つことになる。したがって、軍事・国家セキュリティの観点から、企業間にとどまらず国家間の競争になることも想定され、量子ビット数が数千万以上となる第2段階の量子コンピュータの実現が2040年のよりも前倒しになる可能性も十分にあるであろう。実際に、Googleの取り組みでも見られたように、量子アルゴリズム/ソフトウェア面の工夫をすることで、想定よりも少ない量子ビット数でRSA暗号の解読が可能になることもあり得る。その場合には、既存のデータはおろか、ブロックチェーンなど、現時点では秘匿性が高いとされている技術に基づいたデータも含めて暗号が解読されるリスクがある。2030年ごろを目途に、耐量子コンピュータのアルゴリズムの標準化に向けNISTがすでに動いているが、その実装は2030年が実はぎりぎりのタイミングで猶予はないかもしれない。

終わりに

量子コンピュータは、2020年現在のわたしたちがコンピュータと言われて通常想定するようなノート型のパソコンとは異なり、これまで述べてきた特性から当面、一部企業・国家機関が所有する形にならざるを得ないだろう。スパコンを遥かに凌駕する処理能力を持ち、またそこに投資できる資金余力やITなどのケイパビリティを擁する機関に対して、競争・協調領域をどのように設定するのか。10年先を見据えた戦略を今から考えておく必要があるのではないだろうか。

strategy&
Part of the PwC network

Strategy&

Strategy&は、他にはないポジションから、クライアントにとって最適な将来を実現するための支援を行う、グローバルな戦略コンサルティングチームです。そのポジションは他社にはない差別化の上に成り立っており、支援内容はクライアントのニーズに応じたテイラーメイドなものです。PwCの一員として、私たちは日々、成長の中核である、勝つための仕組みを提供しています。圧倒的な先見力と、具体性の高いノウハウ、テクノロジー、そしてグローバルな規模を融合させ、クライアントが、これまで以上に変革力に富み、即座に実行に移せる戦略を策定できるよう支援しています。

グローバルなプロフェッショナル・サービスにおいて唯一の大規模な戦略コンサルティング部門であるStrategy&は、クライアントが目指すべき方向を示し、最適な方法を選択し、実現させる方法を提示すべく、戦略策定のケイパビリティをPwCの最前線のチームに提供しています。

その結果は、可能性を最大化するために強力なだけでなく、効果的に実現できるような実践的アプローチであり、信頼性の高い戦略プロセスです。今日の変革が明日の成果を再定義するような戦略です。ビジョンを現実のものへと作り上げる戦略です。“It’s strategy, made real.”戦略が現実のものになるのです。

www.strategyand.pwc.com/jp

発行：2020年11月