米国における量子コンピュータの現状

鷲見 拓哉　　中沢 潔
IPA　　JETRO/IPA New York

1　サマリー

量子コンピュータでは、「量子ビット（qubit：quantum bit）」と呼ばれる情報単位が持つ「重ね合わせ（superposition）」の特徴を用いることにより、N 個の量子ビットで一度に 2 の N 乗回の並列計算が可能になり、1 量子ビット付加する毎に量子コンピュータの演算能力が飛躍的に高まる。例えば、以下の産業での実用化が期待されている。

- **交通／物流（製造）**：移動経路の最適化問題を迅速に処理できることで、交通サービスにおける移動時間の短縮や渋滞の減少やサプライチェーンプロセスの効率化等につながる
- **機械学習（AI）**：学習のフィードバックを提供する上でのデータ分析を短時間で処理できることで、ディープニューラルネットワークにおける機械学習能力を効率的に向上させられる
- **ヘルスケア（製薬）**：分子、たんぱく質、化学薬品の相互作用及び化学反応の分析や、人間の遺伝子配列・解析を効率的に処理できることで、副作用のない治療薬の開発（創薬）プロセスの短縮及び各患者にパーソナライズされた処方薬の提供につながる
- **金融サービス**：市場リスクの計測や投資評価等を行う際に用いられているモンテカルロシミュレーションを効率化することで、ポートフォリオの最適化と投資リスクの削減につながる
- **メディアテクノロジー**：オンライン上のユーザーの行動履歴に関するデータ分析を基に、ターゲット広告の配信効果が高まる
- **サイバーセキュリティ**：量子コンピュータにより機密データや電子通信の安全性を担保するために用いられている既存の暗号方式が破られる可能性が高まることでセキュリティ上の脅威が懸念される一方、第三者による盗聴を確実に防止できる「量子鍵配送（QKD）」と呼ばれる手法など、量子暗号を用いた秘匿通信の実用化が期待されている
- **AI**：人間と同様に複雑なタスクに効率的に対応できる AI により、ヒト型ロボットがリアルタイムかつ予期せぬ環境下で最適な意思決定を行えるようになる（コンピュータビジョン、パターン認識、音声認識、機械翻訳等における技術進歩が期待される）

近年、米国、中国、欧州で関連研究開発プログラムに多額の政府資金が投入され、IBM 社、Google 社、Microsoft 社、Alibaba 社等の大手テクノロジー企業や、D-Wave 社、Rigetti 社等のスタートアップが量子ゲート方式又は（及び）量子アニーリング方式でのハードウェア開発に積極的に取り組んでいる。これらの企業は、それぞれクラウド上でマシンにアクセスできるサービスを提供しているが、近年は、QC Ware 社など、主要量子コンピュータシステムで動作する企業向けアプリケーションの開発を専門とする企業も出現し、商用アルゴリズムの開発及び量子コンピュータのビジネス利用を後押ししている。McKinsey 社の調査（2015 年時点）によれば、（機密扱いとなっていない）量子技術に対する研究予算は世界で年間総額およそ 15 億ユーロ、国別では、米国が最も高く（年間 3 億 6,000 万ユーロ）、次に中国（同 2 億 2,000 万ユーロ）、ドイツ（同 1 億 2000 万ユーロ）、英国（同 1 億 500 万ユーロ）、カナダ（同 1 億ユーロ）が続く（EU 全体では同 5 億 5000 万ユーロ、日本は同 0.6 億ユーロ）。一方、量子コンピュータが既存の暗号システムに及ぼす脅威についても十分に理解する必要があり、米科学アカデミーは、今からポスト量子暗号（耐量子コンピュータ暗号）の開発・導入等の準備を進める必要があると警告している。

日本においては、政府による研究開発支援等も含め、NTT 社や富士通社等の大手企業が D-Wave 社の量子コンピュータに対抗するイジングモデル型（統計力学の理論モデルで、粒子の取り得る向きを計算するためのモデル）のコンピュータの開発を推進している。しかし、量子コンピュータへの世界的な投資が拡大する中、欧米と比較して日本の投資規模ははるかに小さく、研究者の間では、「日本は、基礎研究は健闘しているが、マシンの開発競争は北米優位であり、予算規模の差が効いているのかもしれない」との声もある。

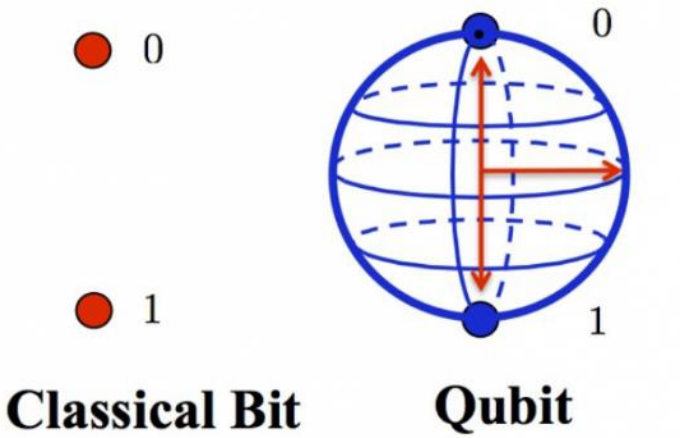
2　量子コンピュータの仕組みと現状

（1）　量子コンピュータとは

a.　量子コンピュータの特徴

「量子コンピュータ（quantum computer）」とは、量子の物理的な動きや振る舞い（原子以下の微視的な粒子が同時に複数の状態で存在できるという特性）を利用したコンピューティングシステムのことである。従来のコンピュータ（古典コンピュータ）では、情報の基本単位を「ビット（bit：binary digit）」とし、それぞれを「0」か「1」のいずれかの状態を取ることによって 2 進数で数を保持し演算することで、情報の保存・処理を行っている[1]。これに対し、量子コンピュータでは、「量子ビット（qubit：quantum bit）」と呼ばれる情報単位が用いられる。これは、一度に 2 つの状態を同時に取れる（一度に 2 つの状態で存在できる）という「重ね合わせ（superposition）」と呼ばれる量子の特徴を用いた一時点で 0 と 1 を同時に示すことができる単位であり、量子ビットは電子や光子をぶつけるなどして外部から観測されない限り 0 と 1 の両方を同時に示すと考えられている[2]。

図表 1：「ビット（bit）」と「量子ビット（qubit）」の違い



出典：ITMO.NEWS[3]

古典コンピュータで 4 ビットの情報を示す場合、16 通りの組合せ（0000、0001、0010 等）のうちの一つしか表せない（一つ一つを逐次計算しなければならない）が、量子コンピュータでの 4 量子ビットは 0 と 1 の 16 通りの組合せを同時に示すことが可能となり、古典コンピュータで 16 回繰り返さなければならなかった演算を 1 回で実現する（N 個の量子ビットで一度に 2 の N 乗回の並列計算が可能になる）。これが、1 量子ビット付加する毎に量子コンピュータの演算能力が飛躍的に高まる理由である。量子コンピュータは、空間的に離れた 2 つの量子的な粒子が影響し合う「量子のもつれ（quantum entanglement）」と呼ばれる物理現象[4]を利用して複数の量子を集積化し一括処理することで複雑かつ大規模な並列計算の実現を目指すものである[5]。

[1] 実際のコンピュータでは、「0」か「1」の状態を表すのに、IC（半導体集積回路）チップに組み込まれた数百万又は数億のトランジスタが電圧をオン・オフで切り替えて行っている。

[2] 0 か 1 かの特定の状態は観測した瞬間に決定されるが、量子力学の考えでは、量子の性質は観測されるまでは確率でしか状態を知りえないことが前提となっている。

[3] http://news.ifmo.ru/en/news/7105/

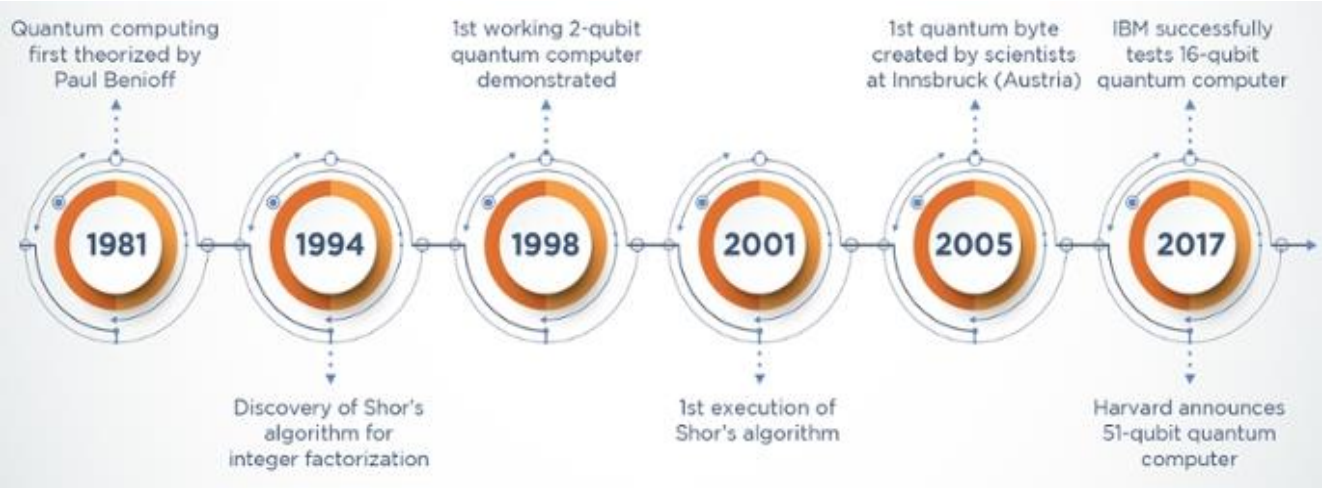
[4] 量子もつれ状態にある 2 つの粒子は、どんなに遠く離れていてもその振る舞いが同期するため、一方の状態を見るだけで、もう一方の状態を知ることができるという現象。

[5] https://www.explainingcomputers.com/quantum.html、https://www.youtube.com/watch?v=JhHMJCUmq28

b. 量子コンピュータの始まり

量子コンピュータの概念が誕生したのは比較的最近のことで、米アルゴンヌ国立研究所（Argonne National Laboratory）の物理学者である Paul Benioff 氏が 1981 年、量子力学のアプローチを情報処理に応用することを最初に理論化した。その後 1982 年に、米理論物理学者の Richard Feynman 氏は自然（量子力学）をシミュレートするための量子システムを提案し、1985 年に英オックスフォード大学の物理学者 David Deutsch 氏が最初の実用的な量子コンピュータ（「量子チューリング機械（Quantum Turing Machine）」と呼ばれる新たな計算モデル）を提唱した。こうした理論的な発展を受けて 1994 年、米ベル研究所の数学者 Peter Shor 氏が、e コマースで広く用いられている公開鍵暗号システムの多くを破ることが可能な量子アルゴリズム（素因数分解アルゴリズム）を開発したことをきっかけに、量子コンピュータに対する注目が一気に高まることになる。1998 年にオックスフォード大学の科学者らが 2 量子ビットの量子コンピュータの動作を初めて成功させてから 2017 年はじめまで、最大量子ビット数が 16 程度と小規模なものにとどまっていたが、同年夏にハーバード大学及びマサチューセッツ工科大学の研究者が 51 量子ビットを搭載したコンピュータの操作を成功させるなど、量子コンピュータ技術は最近急速な発展を遂げている[6]。

図表 2：量子コンピュータ発展の経緯



出典：Science Node

技術進歩に伴う半導体集積回路の高密度化は、古典コンピュータの高性能化と高速化、低価格化を推進してきたが、集積回路を構成するトランジスタが原子サイズに近づく中、「ムーアの法則（Moore's Law[7]）」が限界を迎えつつある[8]。また、IoT 機器や AI の普及を背景とするビッグデータ時代において、複雑かつ大容量のデータを高速処理するための手法が求められており、量子コンピュータはこうした状況に対する一つの解決策として期待を集めている[9]。

c. 量子コンピュータの種類

量子コンピュータの実現においては、並列計算を行う上で量子の重ね合わせの状態を維持することが重要であるが、量子コンピュータは外部環境に非常に敏感であり、計算処理中に重ね合わせの状態が解消され量子ビットが失われる「デコヒーレンス（decoherence）」現象をいかに回避し重ね合わせ状態を長時間維持するかが一つの大きな課題となっている。現在開発が進められている量子コンピュータの多くは、量子ビット

[6] https://sciencenode.org/feature/3-reasons-why-quantum-computing-is-closer-than-ever.php
[7] 1965 年に Intel 社の共同創設者 Gordon Moore 氏が提唱した「半導体体集積回路を構成するトランジスタ等の部品数は約 2 年ごとに倍増する」という経験則。
[8] https://www.science.org.au/curious/technology-future/quantum-computing
[9] https://www.forbes.com/sites/bernardmarr/2017/07/04/what-is-quantum-computing-a-super-easy-explanation-for-anyone/#75cb0bd31d3b

を絶対零度（－273.15℃）に冷却し内部に電気的抵抗のない状態（超伝導状態）で実験が行われているほか、外来ノイズ対策にも注意を払う必要があり、誤り率の減少又は誤り訂正にも対応[10]することが求められている[11]。現在、米国の大手テクノロジー企業等を中心に開発が進められている量子コンピュータは、主に、①量子ゲート（quantum gates）方式と②量子アニーリング（quantum annealing）方式の 2 種類に分けられる。

図表 3：量子コンピュータにおける量子ゲート方式と量子アニーリング方式の特徴比較

	量子ゲート（quantum gates）方式	量子アニーリング（quantum annealing）方式
開発に取り組む主な北米企業	IBM 社、Google 社、Microsoft 社、Intel 社、Rigetti Computing 社	D-Wave Systems 社、Google 社
仕組み	従来から研究されている量子の重ね合わせの原理を用いた方式で、古典コンピュータの論理ゲートのように、量子ビットに量子論理ゲートを作用させて計算を行う	重ね合わせの原理などの量子効果を徐々に変化させることでエネルギーの最も低い状態を最適解として得るもので、最適化問題を「イジングモデル（Ising Model[12]）」で置き換え、アルゴリズムとして利用している[13]
動作温度	絶対零度	絶対零度
動作アルゴリズム	Shor の素因数分解アルゴリズムや Grover の大規模データ探索アルゴリズムのほか、およそ 50 の量子アルゴリズム[14]が存在	断熱量子計算アルゴリズム
用途	対応するプログラムが開発できれば様々な用途に応用できる汎用型	膨大な選択肢の中から最適な選択肢を探し当てる組み合わせ最適化問題（サンプリング、機械学習）に特化
実用化／開発状況	・IBM 社は 2017 年 11 月、50 量子ビットのチップを開発、Google 社は 2018 年 3 月、72 量子ビットの量子プロセッサ「Bristlecone」を発表 ・IBM 社は 2019 年 1 月、世界初の統合型量子コンピュータ商用マシン「IBM Q System One」を発表（20 量子ビット搭載）	2011 年 5 月、カナダの D-Wave Systems 社が「D-Wave One」の販売を開始（128 量子ビットを搭載）。以降、2 年毎にアップグレード版が出されており、2017 年 1 月に発表された「D-Wave 2000Q」は 2,000 量子ビットを搭載（マシン 1 台当たり 1,500 万ドル）

出典：各種資料を基に作成

量子ゲート方式の量子コンピュータ開発は、従来から研究されている量子の重ね合わせの原理を用いた方式で、古典コンピュータと同様、プログラムが開発できればどんな問題にも適用できる汎用性を持つとされ、IBM 社、Google 社、Microsoft 社、Intel 社を含む米大手テクノロジー企業が中心となり、ある程度ノイズに強い量子ビットを形成できる超伝導回路を活用した量子ビット型（superconducting qubits）コンピュータの開発を積極的に進めている。IBM 社や Google 社は最近、それぞれ 50 量子ビット、72 量子ビットのチップの開発を相次いで発表し、米スタートアップ Rigetti Computing 社も 2019 年 8 月までに 128 量子ビットのチップを開発する計画を明らかにしているほか、IBM 社においては、2019 年 1 月、米ラスベガスで開催された家電見本市 CES（Consumer Electronics Show）2019 で、世界初の統合型量子コンピュータ商用マシン「IBM Q System One」を発表している[15]。しかし、様々なビジネスに応用できる（あらゆる量子アルゴリズムを誤りなく実行できる）汎用型量子コンピュータ（ユニバーサル量子コンピュータ）の実現には数十万～数百

[10] 量子コンピュータでは、多数の可能性の重ね合わせの中からもっともらしい答えを高確率で得ることが可能であるが、古典コンピュータのように誤り訂正機能がなく、現在は誤り率を可能な限り減らし、同じ計算を何度も繰り返し行うことで誤った解を除外する方法がとられている。なお、誤り訂正の処理には多量の量子ビットが必要となる。

[11] https://www.zdnet.com/article/what-a-quantum-computer-is-and-why-it-needs-to-be-more/
https://www.explainingcomputers.com/quantum.html

[12] 統計力学の理論モデルで、粒子の取り得る向きを計算するためのモデル。

[13] 「量子アニーリング」の名称は、金属を高温から低温に徐々に冷却し、低温において全体のエネルギーが小さい状態になるよう促す「焼きなまし（アニーリング）」と呼ばれる物理過程をシミュレーションしていることからきている。同方式は 1998 年に東京工業大学の理論物理学者である門脇正史博士と西森秀稔教授によって発表された計算技術を基本としている。

[14] http://quantumalgorithmzoo.org/

[15] https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System-for-Commercial-Use

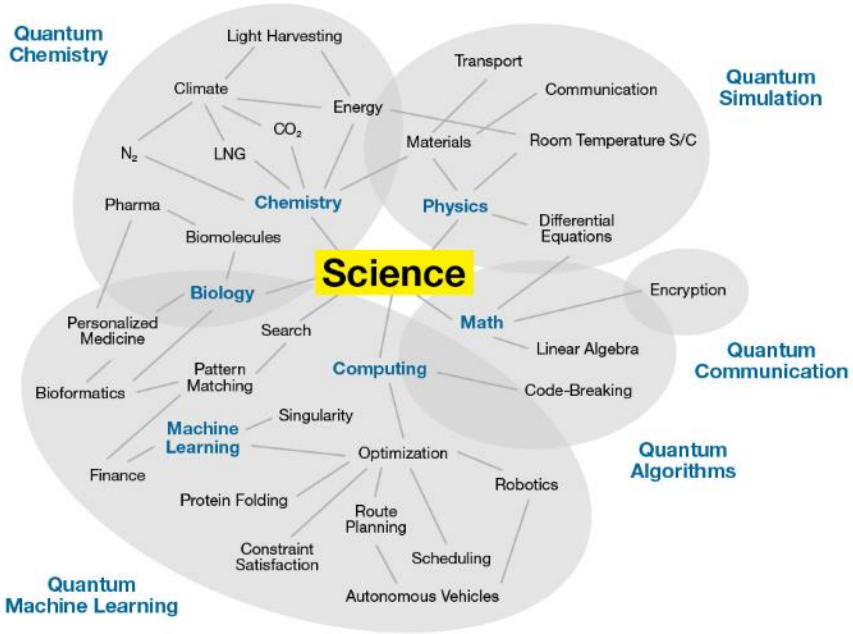
万量子ビットが必要とみられており、現時点で商用化の目途は立っていない。他方で、2016 年まで数量子ビットの量子プロセッサの動作の実現にとどまっていたことを踏まえると、近年の技術革新の速度は著しく、早期実用化への期待も高まっている[16]。

これに対し、量子アニーリング方式は、カナダのスタートアップ D-Wave Systems 社が業界初の商用マシン「D-Wave」の販売を開始し実用化で先行している。2011 年以降、2 年毎に発表されるアップグレード版で量子ビット数を大幅に増やしてきた D-Wave は、2017 年の最新版で 2,000 量子ビットを搭載するまでに進化している。量子アニーリング方式はこれまで研究されてきた方式とは異なり、量子論理ゲートを用いず、組み合わせ最適化問題に特化したものであることから、専門家の間では同方式が本当に量子コンピュータであるかについて議論されてきたが、現在、D-Wave 社のシステムではアルゴリズムの動作に量子力学的性質が用いられていることが広く受容されており、唯一の商用量子コンピュータとして Lockheed Martin 社や Google 社を含む世界の複数の業界大手企業の関心を集め、同マシンを活用した研究開発が推進されているが、規模を問わず様々な最適化問題で一貫して高速処理を行えるようにすることが同手法における最大の課題となっている[17]。

d. 量子コンピュータの産業応用可能性

量子コンピュータは、古典コンピュータでは逐次的に行われる計算を並列的に一括して実行し、計算処理にかかる時間を大幅に短縮できることで、幅広い業界分野で今後飛躍的な技術革新が見込まれている（図表 4 参照）。米 IT 市場調査／コンサルティング企業の Gartner 社は、同社が 2017 年の先進テクノロジー・ハイプサイクル（Gartner Hype Cycle for Emerging Technologies 2017）において、量子コンピュータは「イノベーションの黎明期（Innovation Trigger）」にあると位置づけており、ビジネスへの応用例や量子アルゴリズムがまだ非常に限定的であるほか、関連機器の耐性が低く標準に欠け、マシンの設計手法も幅広いとしている[18]。

図表 4：量子コンピュータの活用が見込まれる主な分野



出典：Gartner

[16] https://www.wired.com/story/wired-guide-to-quantum-computing/
[17] https://www.bcg.com/publications/2018/next-decade-quantum-computing-how-play.aspx
[18] https://www.gartner.com/smarterwithgartner/the-cios-guide-to-quantum-computing/

量子コンピュータの実用化においては、組み合わせ最適化問題を応用した量子アニーリング方式が現時点で概念実証段階にあり、交通／物流、機械学習（AI）、ヘルスケア（製薬）、金融サービスなど、ビッグデータを活用し最適化を行うことが求められる分野で応用研究が活発に進められている。一方、量子ゲート方式では、多様な用途に対応できる量子コンピュータチップの開発や、ノイズに強く訂正を行いながら計算を行える量子システムの実現に更なる時間を要するとみられ、米総合コンサルティング大手 Accenture 社は、量子アニーリング方式のコンピュータがビジネスで実際に活用されるようになる時期は 2～5 年後、量子ゲート方式のコンピュータがビジネス及び社会に大きな転換をもたらす時期は最低でも 5～10 年先になるとの見通しを示している[19]。なお、量子ゲート方式のコンピュータでは、ユニバーサル量子コンピュータが将来的に実現された場合、金融システムやインターネット上で現在用いられている暗号方式が破られる可能性が懸念されている。これは、古典コンピュータでは膨大な時間を要する大規模な計算処理を量子コンピュータでは短期間で実行できるためで、既存の暗号技術に多大な影響を及ぼすことが予想されている（ポスト量子暗号（耐量子コンピュータ暗号）に関する取組については後述）。他方で、量子力学の原理を利用して信頼された 2 者間で盗聴が検知できる通信チャネルを形成、暗号鍵の情報を送受信することで絶対的な安全性を担保した暗号通信を実現する「量子鍵配送（Quantum Key Distribution：QKD）」と呼ばれる手法など、量子暗号（quantum encryption）の開発も積極的に推進されている[20]。

図表 5：量子アニーリング方式と量子ゲート方式のコンピュータで短・長期的に応用が期待されている主な産業分野

量子ゲート方式 （量子アニーリング方式における応用分野以外で、ユニバーサル量子コンピュータの実現により応用が期待される分野）	**量子アニーリング方式** （組み合わせ最適化問題やサンプリング手法を応用し、短期的に応用が期待される分野）
・**サイバーセキュリティ**：計算能力が非常に高いユニバーサル量子コンピュータの実現に伴い、機密データや電子通信の安全性を担保するために用いられている既存の暗号方式が破られる可能性が高まることでセキュリティ上の脅威が懸念される一方、第三者による盗聴を確実に防止できる「量子鍵配送（QKD）」と呼ばれる手法など、量子暗号を用いた秘匿通信の実用化が期待されている ・**AI**：人間と同様に複雑なタスクに効率的に対応できる AI により、ヒト型ロボットがリアルタイムかつ予期せぬ環境下で最適な意思決定を行えるようになる（コンピュータビジョン、パターン認識、音声認識、機械翻訳等における技術進歩が期待される）	・**交通／物流（製造）**：移動経路の最適化問題を迅速に処理できることで、交通サービスにおける移動時間の短縮や渋滞の減少等を実現できるほか、航空交通管制や船舶運航、調達・製造・配送のサプライチェーンプロセスの効率化につながる ・**機械学習[21]（AI）**：学習のフィードバックを提供する上でのデータ分析を短時間で処理できることで、ディープニューラルネットワークにおける機械学習能力を効率的に向上させられる ・**ヘルスケア（製薬）**：分子、たんぱく質、化学薬品の相互作用及び化学反応の分析や、人間の遺伝子配列・解析を効率的に処理できることで、副作用のない治療薬の開発（創薬）プロセスの短縮及び各患者にパーソナライズされた処方薬の提供につながる ・**金融サービス**：市場リスクの計測や投資評価等を行う際に用いられているモンテカルロシミュレーションを効率化することで、ポートフォリオの最適化と投資リスクの削減につながる ・**メディアテクノロジー**：オンライン上のユーザーの行動履歴に関するデータ分析を基に、ターゲット広告の配信効果が高まる

出典：各種資料を基に作成

[19] https://www.accenture.com/t20170628T011725Z__w__/us-en/_acnmedia/PDF-54/Accenture-807510-Quantum-Computing-RGB-V02.pdf
[20] https://www.forbes.com/sites/bernardmarr/2017/07/10/6-practical-examples-of-how-quantum-computing-will-change-our-world/amp/
[21] 機械学習は組み合わせ最適化問題及びサンプリング手法を基本としている。

（2） 主要国における量子コンピュータへの投資状況

米大手コンサルティング会社 McKinsey 社は、（機密扱いとなっていない）量子技術に対する研究予算は世界中で年間総額およそ 15 億ユーロ、同技術研究に従事する研究者数は約 7,000 人と推定している（2015 年時点）。国別予算では、米国が最も高く（年間 3 億 6,000 万ユーロ）、次に中国（同 2 億 2,000 万ユーロ）、ドイツ（同 1 億 2000 万ユーロ）、英国（同 1 億 500 万ユーロ）、カナダ（同 1 億ユーロ）が続く（EU では同 5 億 5000 万ユーロ、日本は同 0.6 億ユーロ）[22]。

図表 6：世界における量子技術分野の年間研究予算と研究者数（国別）（2015 年時点）

出典：Medium

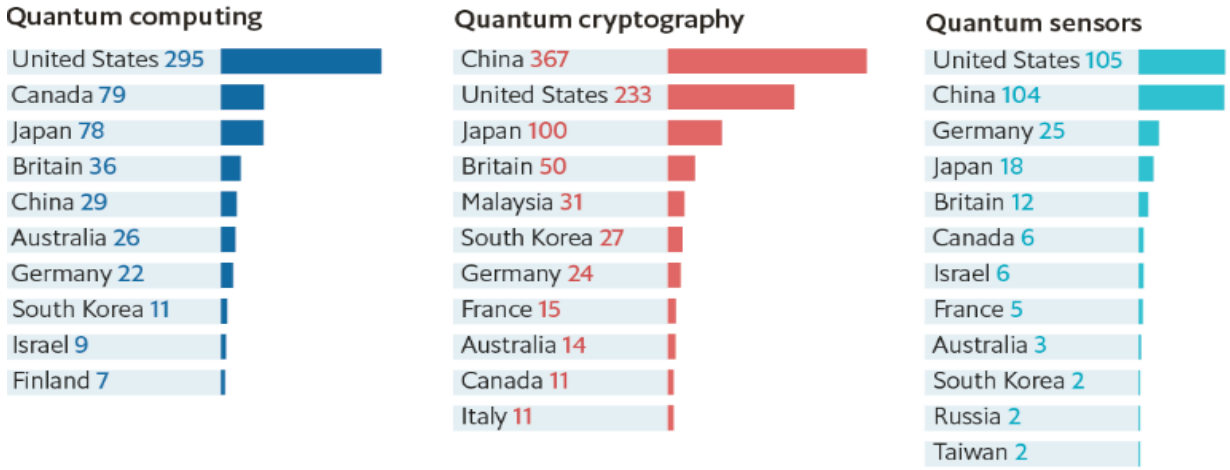
近年、主要国（地域）における量子技術分野の研究競争が加速傾向にあり、量子通信、量子センシング、量子コンピュータをはじめ、量子技術の広範な活用を目指した研究プログラムに多額の国家資金が拠出されており、中国、欧州、米国で特にその動きが活発である。2017 年 9 月から北京、上海、済南、合肥の主要 4 都市を結ぶ量子衛星ネットワークの構築にもいち早く取り組んでいる中国[23]では、政府が 100 億ドルを投じ、合肥に大規模な国家量子情報科学研究所（National Laboratory for Quantum Information Sciences）を新設中（2020 年開設予定）である[24]。欧州においても、欧州連合（EU）欧州委員会（European Commission：EC）が 10 年間で総額 10 億ユーロを出資し、技術実用化にフォーカスした量子物理学研究を支援する「量子技術フラッグシップ（Quantum Technologies Flagship）計画」を進めている[25]ほか、国レベルの取組では、英国において政府が 2014 年から 10 年間で総額 5 億 8,500 ポンドの出資を予定している量子技術の商用化加速を目指した「国家量子テクノロジープログラム（UK National Quantum Technologies Programme：UKNQT[26]）」が有名である。また、米国では 2018 年 12 月、量子情報科学の

[22] https://medium.com/@ASMLcompany/start-your-engines-the-race-to-quantum-computing-is-on-14c3076a5c47
[23] 中国は 2018 年 8 月、世界初めの量子通信衛星の打ち上げに成功し、2017 年には同衛星を通じてオーストリアと北京間の量子通信にも成功している。
[24] https://technode.com/2018/09/05/china-quantum-information-laboratory/
[25] https://qt.eu/newsroom/quantum-flagship-launch-press-release/
[26] UKNQT において英国政府は当初、2014～19 年までの 5 年間に総額 2 億 7,000 万ポンドの投資を予定していたが、同プログラムはその後 2024 年まで延長・拡大されており（3 億 1,500 万ポンドの追加投資）、同プログラムの一環で、世界初のユニバーサル量子コンピュータの構築を目指す新たな国家量子コンピューティングセンターの設立も予定されている。

推進及び関連人材の育成を支援する取組に対し、向こう 5 年間で政府が 12 億ドルを拠出する「国家量子イニシアチブ法（National Quantum Initiative Act[27]）」が制定されている（次章で後述）。

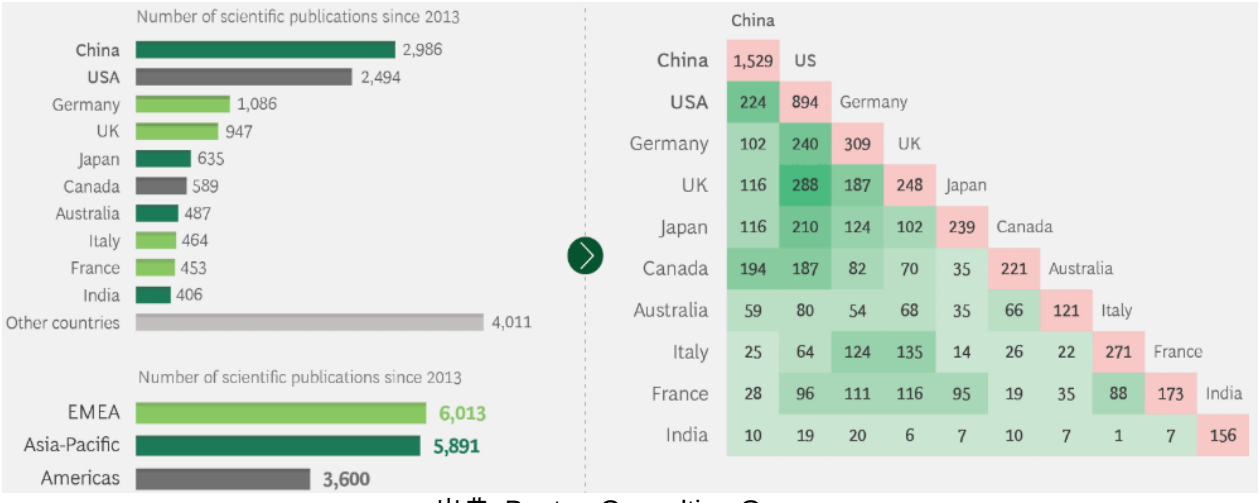
なお、世界主要国における量子技術関連の特許申請数をみると、量子コンピュータ分野では米国が圧倒的な申請数で世界をリードしており、量子暗号分野では中国でその研究開発が特に活発に進められている（図表 7 参照）[28]。また、量子コンピュータに関する研究活動では、2013 年以降、中国の科学論文の発表数が米国を上回り世界第一位となっている。一方で、海外の研究大学機関の研究者との共著論文数では米国が世界最大となっており、こうした国際連携の傾向は、量子コンピュータの開発における技術・工学的課題に関する情報交換のニーズが研究コミュニティの間で依然として高く、暗号への応用など、国家安全保障に係る量子コンピュータの利用に関する研究はまだ一部であることを示している[29]。

図表 7：世界主要国における量子技術関連の特許申請数（2015 年時点）



出典：The Economist

図表 8：主要国／地域における 2013 年以降の量子コンピュータに関する科学論文発表数（左）と海外の研究大学機関の研究者との共著論文発表数（右）



出典：Boston Consulting Group

https://www.gov.uk/government/news/new-funding-puts-uk-at-the-forefront-of-cutting-edge-quantum-technologies

[27] https://www.congress.gov/bill/115th-congress/house-bill/6227

[28] https://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own

[29] https://www.bcg.com/publications/2018/next-decade-quantum-computing-how-play.aspx

3　米国連邦政府及び主要企業による量子コンピュータの開発に向けた取組動向

（1）　米国連邦政府

米国で量子技術に関する政策指針が最初に示されたのは、ジョージ・W・ブッシュ大統領退任直前の 2009 年 1 月にホワイトハウス科学技術政策局（Office of Science and Technology Policy：OSTP）の国家科学技術会議（National Science and Technology Council：NSTC）が発表した「量子情報科学に対する連邦ビジョン（Federal Vision for Quantum Information Science[30]）」である。同レポートは、米国で量子物質の制御・操作・利用と、量子情報処理システムの物理学・数学・数理的な可能性及び限界を特定する科学的知識基盤の形成を目指すことを提案するものであり、その後オバマ政権下で、NSTC は量子情報科学の連邦研究プログラムに関する評価や関連研究活動（投資）の戦略計画を策定するための省庁間ワーキング・グループ[31]を組成し、同グループは 2016 年 7 月に発表したレポート（Advancing Quantum Information Science: National Challenges and Opportunities[32]）において、各省庁間で連携して出資等に取り組むべき優先事項の一つに量子情報科学を含めるよう勧告した。そして、機械学習／AI と並び、量子コンピュータを連邦研究開発予算の最優先事項の一つに据えるトランプ大統領[33]は、これまでの政策方針を踏襲する形で 2017 年 12 月、米国立標準技術研究所（National Institute of Standards and Technology：NIST）の共同量子研究所（Joint Quantum Institute）のフェローである Jacob Taylor 氏を OSTP の量子情報科学担当ディレクタ補佐に任命し、同氏を筆頭に、オバマ政権下で結成された省庁間ワーキング・グループを量子情報科学に関する NSTC 小委員会（NSTC Subcommittee on Quantum Information Science：SCQIS）として公式に組織化、量子技術研究に関する省庁間の連携強化に動いている[34]。

また、2018 年 12 月にトランプ大統領が署名して成立した「国家量子イニシアチブ法（National Quantum Initiative Act）」は、量子技術を発展させるための国家基本計画となるもので、政府は向こう 10 年間の量子情報科学の研究推進活動における最初の 5 年間におよそ 12 億ドルを拠出する予定である。具体的に同法は、量子技術の最前線に米国をとどめるための 5 ヵ年戦略計画の策定を SCQIS に義務付けており、同計画では、コンピューターサイエンスや物理学、工学等の異なる分野の研究者を集めて実験を行ったり、未来の量子研究者を育成したりするための専門研究センターを新設[35]することや、大手企業及びスタートアップが政府機関との共同研究プログラムにおける知識やリソースを集結させることなどを重要な目標としている[36]。その他、同法のイニシアチブの管轄・施行にあたっては、SCQIS のほか、OSTP 内に新設される国家量子調整局（National Quantum Coordination Office）と、企業、大学、連邦研究機関の専門家から成る国家量子イニシアチブ諮問委員会（National Quantum Initiative Advisory Committee）の 3 組織が連携して取り組むことになっている[37]。

量子技術に対する連邦研究資金に関しては、IBM 社などから、今後米国が同技術で国際競争力を維持するには不十分との意見がこれまで出されており[38]、量子コンピュータの開発加速化を国家レベルで後押しす

[30] http://calyptus.caltech.edu/qis2009/documents/FederalVisionQIS.pdf
[31] 主に、OSTP、米行政管理予算局（OMB）、エネルギー省、商務省及び同省下の米国立標準技術研究所（NIST）、全米科学財団（NSF）、米国防総省（DoD）の代表メンバーから構成される。
[32] https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/images/Quantum_Info_Sci_Report_2016_07_22%20final.pdf
[33] https://www.aip.org/fyi/2018/trump-administration-identifies-rd-priorities-its-next-budget-request
[34] https://www.aip.org/fyi/2018/science-committee-seeks-launch-national-quantum-initiative
[35] 同法に基づき、NSF とエネルギー省は量子情報科学研究センターをそれぞれ 2～5 つ新設する予定である。
[36] https://www.technologyreview.com/the-download/612679/president-trump-has-signed-a-12-billon-law-to-boost-us-quantum-tech/
[37] https://www.aip.org/fyi/2019/national-quantum-initiative-signed-law
[38] https://www.bloomberg.com/news/articles/2018-04-08/forget-the-trade-war-china-wants-to-win-the-computing-arms-race

る同法の成立は大方好意的に受け止められているが、セキュリティ専門家の中には、同法は量子コンピュータの開発に主に焦点が当てられており、(ユニバーサル)量子コンピュータの実現に伴う既存の暗号技術の危殆化及び国家安全保障上のリスクに対する言及がないことを懸念する声もある。米国では、国家安全保障局(National Security Agency:NSA)が 2015 年 8 月、量子コンピュータの実用化に伴うセキュリティ上の脅威を背景に、既存の公開鍵暗号システムからポスト量子暗号システムへの移行が必要であると表明し[39]、NIST が中心となり、古典コンピュータ及び量子コンピュータの両方でデータの安全性が担保される暗号システムの開発を目標とする耐量子公開鍵暗号アルゴリズムの標準化を進めている[40]。

既存の暗号システムは、①対になる 2 つの鍵を使ってデータの暗号化・復号を行う公開鍵暗号方式(インターネットの TLS 通信などに用いられている暗号方式)と、②暗号化と復号に同一の秘密鍵を用いる共通鍵暗号方式(AES など多くの政府データの暗号化に用いられている暗号方式)の 2 種類に大別される。NIST は、2016 年 4 月に発表した「ポスト量子暗号に関するレポート(Report on Post-Quantum Cryptography <NISTIR 8105[41]>)」において、大規模な量子コンピュータの実現に伴い、巨大な数の素因数分解の計算が古典コンピュータでは現実的には不可能なことを利用した RSA 暗号など、①の暗号方式の多くの安全性が脅かされる可能性が高い一方、②の方式は量子コンピュータで効率的に解く方法がまだ解明されていないことから、鍵長を大きくすることでその影響は限定的になるとの見解を示している。NIST は、耐量子公開鍵暗号アルゴリズムの規格案を 2022～24 年までに選定する計画を明らかにしている[42]。また、NSA は 2016 年 1 月、同アルゴリズムが採用されるまでの移行期間において、機密情報を扱う政府機関及びベンダのシステムが実装するよう定めた暗号規格(最高機密レベルまでの機密情報の保護を推奨された暗号アルゴリズム)を「CNSA(Commercial National Security Algorithm)スイート」に改める[43]ことを公表している[44]。

図表 9:CNSA スイートに含まれる主なアルゴリズム及び用法

Algorithm	Usage
RSA 3072-bit or larger	Key Establishment, Digital Signature
Diffie-Hellman (DH) 3072-bit or larger	Key Establishment
ECDH with NIST P-384	Key Establishment
ECDSA with NIST P-384	Digital Signature
SHA-384	Integrity
AES-256	Confidentiality

出典:NSA

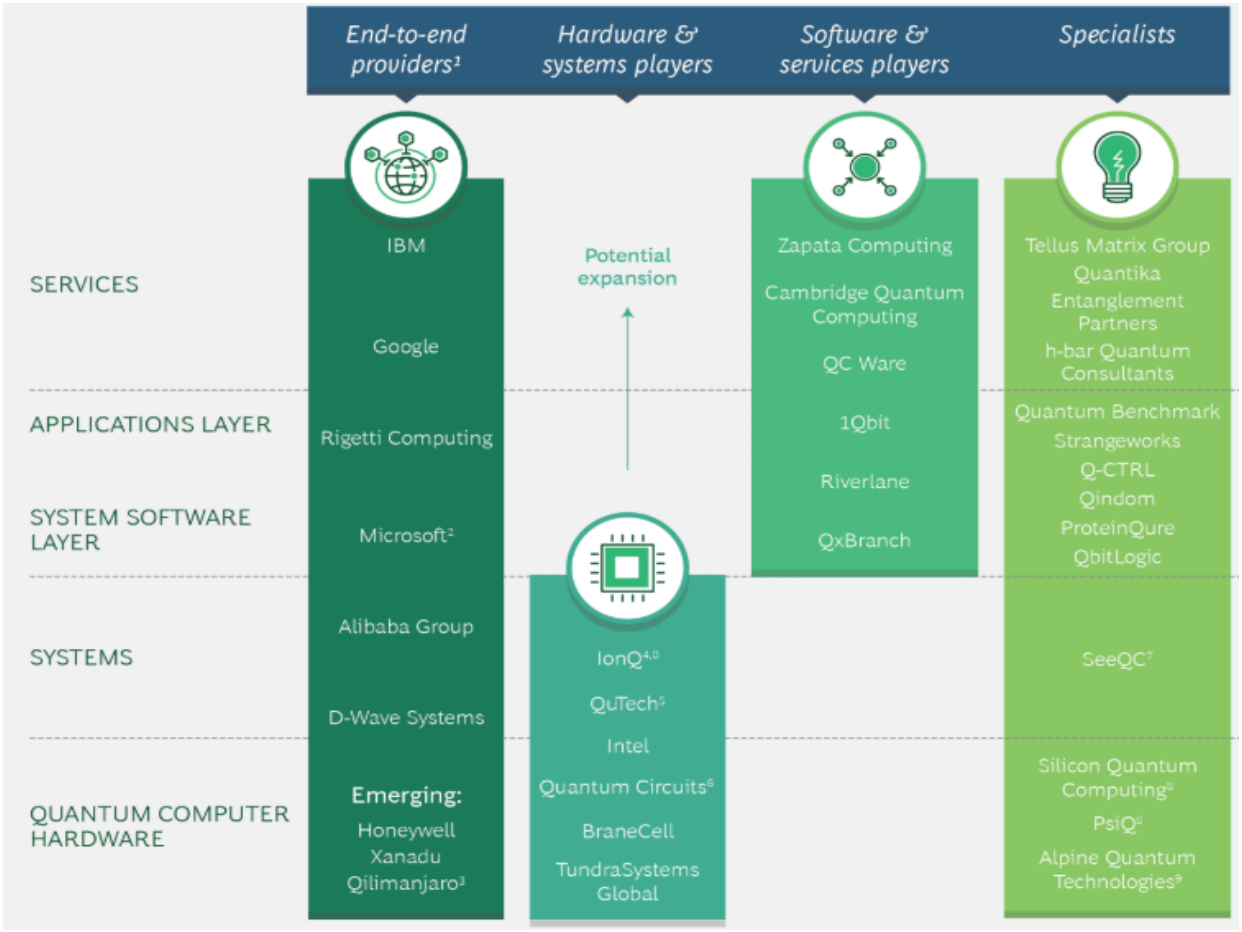
米サイバーセキュリティソリューション企業大手 McAfee 社の公共政策及び政府業務担当責任者である Thomas Gann 氏は、中国やロシアなどが国家安全保障を強化するために量子科学研究に注力する中、米国は国家機密情報の流出を防ぎ米国民の安全を守るためには、量子コンピュータ分野にとどまらず、耐量子アルゴリズムの開発及び国家通信インフラ全体における当該アルゴリズムの実装も他国に先んじて実現することが重要との考えを示している[45]。

[39] https://www.digitaltrends.com/computing/quantum-computing-is-a-major-threat-to-crypto-says-the-nsa/
[40] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
[41] https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf
[42] https://www.isara.com/standards/#NIST
[43] それまでは「Suite B cryptography」が用いられていた。
[44] https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf
[45] https://www.politico.com/agenda/story/2018/09/18/arms-race-quantum-computers-000700

（2） 企業

量子コンピュータ開発のエコシステムは、エンド・ツー・エンドでの製品／サービス開発を手がける大手テクノロジー企業を中心に形成されているが、特にハードウェア・システムの開発を手がける企業において製品／サービスを上位レベルのアプリケーション層に拡大する傾向にあるなど、変化しつつある。これまで、企業の投資は主に下層のハードウェア／システムの開発に集中している一方、大手テクノロジー企業はそれぞれ独自にクラウドベースのオープンソースソフトウェアプラットフォーム上でハードウェアやシミュレーターなどへのアクセス提供を行っている[46]。

図表 10：量子コンピュータ開発のエコシステムにおいて注目を集める主な企業

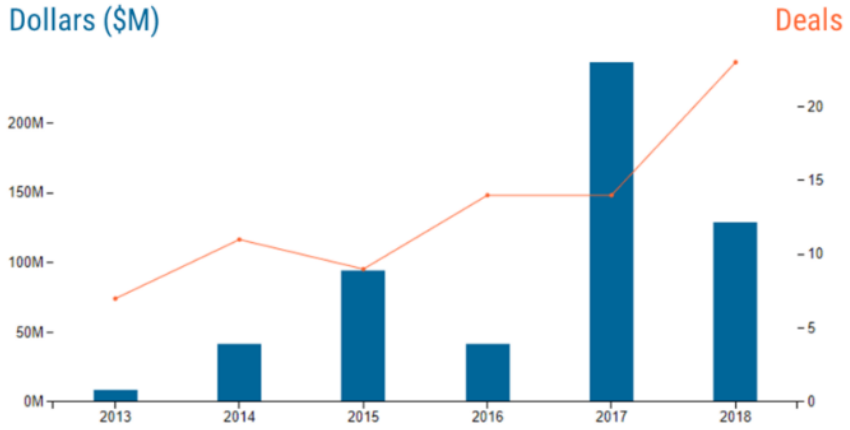


出典：Boston Consulting Group

また、量子コンピュータの開発を手がけるスタートアップへの投資件数は 2018 年に 24 件となり、過去最大となった。投資資金額では、D-Wave 社、Rigetti Computing 社、IonQ 社などが一連の資金ラウンドで総額 2,000 万ドル以上を獲得することに成功した 2017 年に過去最高額を記録したほか、Rigetti 社は 2018 年にもシリーズ C において 5,000 万ドルの資金調達に成功するなど、大手業界企業を中心に、近年、主要スタートアップへの投資が活発化している（図表 11 参照）[47]。以下では、AI 等への応用を目指し、量子コンピュータの開発において業界で注目を集める主な大手テクノロジー企業とスタートアップの取組を紹介する。

[46] https://www.bcg.com/publications/2018/next-decade-quantum-computing-how-play.aspx
[47] https://www.cbinsights.com/research/report/quantum-computing/

図表 11：量子コンピュータの開発を手がけるスタートアップへの投資額及び投資件数推移（2013～18 年）



出典：CB Insights

① 大手テクノロジー企業

a. IBM 社

過去 35 年以上にわたり量子コンピュータの開発に従事してきた IBM 社は、「IBM Q」イニシアチブの下、量子ゲート方式のユニバーサル量子コンピュータの実現を目指し先行的な取組を行っている[48]。同社は 2016 年に 5 量子ビット及び 16 量子ビットのプロセッサを持つ同社の試作量子コンピュータにクラウド上で誰もが無料でアクセスできる「IBM Q Experience[49]」と呼ばれるサービスを業界で初めて開始した企業であり、同サービスはこれまで 10 万人以上のユーザーにより活用されているほか、同社が 2017 年 3 月に提供を開始した量子コンピュータ向けのアプリケーションを開発するためのオープンソース・ソフトウェアプラットフォーム「Qiskit[50]」のダウンロード回数は 15 万回以上に上り、700 万回以上の実装試験の実施及び 140 本以上の研究論文の出版につながっている[51]。

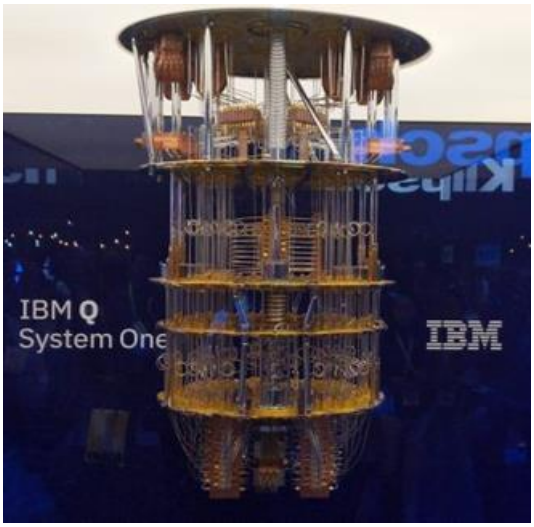
また、IBM 社は 2017 年 11 月、早期アクセス版商用システムとして 20 量子ビットのプロセッサを持つ量子コンピュータの提供と、次世代 IBM Q システムで利用可能となる 50 量子ビットのプロセッサを持つ試作機の構築に成功したことを発表した[52]。20 量子ビットのプロセッサを持つ量子コンピュータへのアクセスは、同年 12 月以降、世界の大手企業やスタートアップ、学術研究機関、国立研究所など産学共同でビジネス及び科学における量子コンピュータの実用化に取り組むために新設された「IBM Q Network[53]」のメンバーに対しクラウド上で提供されており[54]、JPMorgan Chase 社や Daimler 社、Samsung 社、Barclays 社、日立金属社、オークリッジ国立研究所（Oak Ridge National Lab）、オックスフォード大学、慶應義塾大学を含む 12 社（機関）の初期メンバーをはじめ、これまで 40 以上の企業／組織が同ネットワークに参加している。

4 ページで述べた IBM Q System One は、研究所の外で単体で動作する初の汎用量子コンピュータシステムであり、周囲の音や振動、気温の変化、電磁波等の影響を最小限に抑えるため、高さと幅がおよそ 2.7m、厚さおよそ 1.3cm のガラスで密閉し、本体をアルミとスチールのフレームで囲んだ気密環境内に収納されている。IBM Q System One の搭載する量子ビット数は 20 量子ビットであるが、同社が 2017 年末からクラウ

[48] https://www.research.ibm.com/ibm-q/
[49] https://quantumexperience.ng.bluemix.net/qx/experience
[50] https://qiskit.org/
[51] https://www.ibm.com/blogs/research/2019/02/q-network-quantum-goals/
[52] https://www-03.ibm.com/press/us/en/pressrelease/53374.wss
[53] https://www.research.ibm.com/ibm-q/network/
[54] https://www-03.ibm.com/press/us/en/pressrelease/53483.wss

ド上で提供している量子コンピュータの 2 倍のパフォーマンスを実現したとしている[55]。IBM 社はこれまで同様、IBM Q System One もクラウド上でのみ提携企業及び研究機関がアクセスできるようにするとしており、ニューヨーク州ポキプシー（Poughkeepsie）に、IBM Q Network のメンバーを対象とする世界最先端のクラウドベースの量子コンピュータシステムを備えた「IBM Q Quantum Computation Center」を 2019 年中に開設する方針も明らかにしている。同社で IBM Q の戦略・エコシステム部門バイスプレジデントを務める Bob Sutor 氏は、量子コンピュータ関連の技術変化は著しく、システムのアップグレードを頻繁に行う必要があることから、「マシンをオンプレミスに導入することは当面は合理的とはいえない」との見方を示している[56]。

図表 12：コンパクトで洗練されたデザインの統合型量子コンピュータ商用マシン「IBM Q System One」の外観（左）と CES 2019 会場で展示されたシステム本体のレプリカ（右）



出典：ExtremeTech[57]

b. Google 社

Google 社は、量子アニーリング方式及び量子ゲート方式の両方式での量子コンピュータ開発に注力し、先進的な取組を行っている企業の一つである。同社は 2013 年 5 月、D-Wave 社の商用アニーリングマシン「D-Wave Two」を購入し、米航空宇宙局（National Aeronautics and Space Administration：NASA）と大学宇宙研究連合（Universities Space Research Association：USRA）と協力しながら、量子コンピュータを用いた機械学習技術等の研究開発を推進することを目指す量子 AI 研究所（Quantum Artificial Intelligence Lab：QuAIL）を立ち上げた[58]。Google 社と NASA は 2015 年 9 月、D-Wave 社と同社の最新の量子コンピュータ技術を最長 7 年間利用できる契約を締結し、D-Wave 社最大の提携組織（顧客）となっている[59]。一方で、Google 社は 2014 年、超伝導量子回路を用いた量子ゲート方式の権威として世界的に知られるカリフォルニア大学サンタバーバラ校（UC Santa Barbara）の物理学教授である John Martinis 氏率いる量子コンピュータ研究チームを自社に取り込み、5 量子ビットと小規模ではあるが信頼性の高い量子コンピュータの開発に成功していた同チームの技術を基に、QuAIL 内で独自のハードウェア開発にも乗り出している[60]。

---

[55] IBM 社は、量子コンピュータのパフォーマンス指標として、「量子ボリューム（Quantum Volume）」と呼ばれる量子ビット数のほか、コヒーレンス時間、エラー率やキュービット間の接続の質などを考慮した独自指標を提案している。https://interestingengineering.com/ibm-reveals-major-performance-gain-for-ibm-q-system-one

[56] https://www.zdnet.com/article/ibm-at-ces-2019-outlines-q-system-one-quantum-computer/

[57] https://www.extremetech.com/extreme/283427-quantum-computing-goes-commercial-with-ibms-q-system-one

[58] https://ai.googleblog.com/2013/05/launching-quantum-artificial.html

[59] https://www.pcworld.com/article/2987153/google-nasa-sign-7-year-deal-to-test-d-wave-quantum-computers-as-artificial-brains.html

[60] https://www.extremetech.com/extreme/189155-google-begins-developing-its-own-quantum-computer-chips-to-

QuAIL のエンジニア 3 名は 2017 年 3 月、英国の科学雑誌「Nature」の記事において、小規模なデバイスであれば 5 年以内に量子技術を商用化できるとの見通しを示している[61]が、QuAIL が 2018 年 3 月に発表した 72 量子ビットの同社の最新量子プロセッサ「Bristlecone」は、この実現に向けた大きな進展の一つとして業界で話題を集めている。Google 社は、同プロセッサを用いてエラー率の低減や量子技術の拡張性に関する研究と、量子シミュレーション、最適化、機械学習への応用可能性を模索し、古典コンピュータの限界を超える計算量の処理が量子コンピュータで可能になる「量子超越性（quantum supremacy）」の達成[62]を目指すとしており[63]、同社が今後開発するハードウェア、アルゴリズム、ソフトウェアは同チップが基盤となる見込みである。また Google 社は 2018 年 7 月、量子ゲート方式の NISQ（Noisy Intermediate Scale Quantum）量子コンピュータ向けオープンソースフレームワーク「Cirq」も発表している[64]。NISQ 量子コンピュータとは、ノイズが多くエラー率の高い 50 ～100 量子ビットの中規模量子コンピュータを指し、Cirq は、現在から近い将来に実現するとみられる量子コンピュータにおいて短期的な課題となっている有用なアルゴリズムの開発を推進するものである。ユーザーは Cirq をインストールすることで特定の量子プロセッサ用の量子アルゴリズムを書けるようになり、NISQ 量子コンピュータが実用性の高い重要な計算上の問題を解決できるかについて研究者の理解を支援するものとなっているという。

図表 13：72 量子ビットを実現した Google 社の最新量子プロセッサ「Bristlecone」

出典：Google

c. Microsoft 社

Microsoft 社による量子コンピュータの研究開発の歴史はおよそ 20 年前に遡り、トポロジー（位相幾何学）と呼ばれる数学理論の研究で知られる Michael Freedman 氏が同社の研究機関 Microsoft Research に加わったことが始まりであり、同社は、「トポロジカル量子ビット（topological qubits）」と呼ばれる手法を用いて量子ゲート方式のコンピュータの研究開発を進めている[65]。同手法は、通常の量子ビットではなく、安定性の高い特殊な性質を持つトポロジカル量子ビットを用いるもので、Microsoft 社は超伝導量子回路等の他の手法と比べ、エラー率を低減できる（最終的にエラー訂正に必要なシステムリソースを低減できる）と考えている。2005 年にカリフォルニア大学サンタバーバラ校のキャンパス内に設置された Station Q ラボは、Freedman 氏が技術フェローとして研究活動をリードする Microsoft 社の量子コンピュータ研究開発における中核拠点となっている[66]ほか、パデュー大学（Purdue University）、メリーランド大学（University of Maryland）、オランダのデルフト工科大学（TU Delft）やデンマークのコペンハーゲン大学ニールス・ボーア

prepare-for-the-future

[61] https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/45919.pdf

[62] Google 社は、量子超越性の実証には 49 量子ビットで量子回路の深さが 40 以上、2 つの量子ビットのエラー率が 0.5%以下であれば実現できると考えているが、Bristlecone の 2 つの量子ビットによるエラー率は 0.6%で今後の更なる改善が必要となる。

[63] https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html

[64] https://ai.googleblog.com/2018/07/announcing-cirq-open-source-framework.html

[65] https://www.microsoft.com/en-gb/quantum/topological-qubit

[66] https://www.microsoft.com/en-us/research/group/microsoft-quantum-santa-barbara-station-q/

研究所（Niels Bohr Institute）、オーストラリアのシドニー大学（University of Sydney）、スイスのチューリッヒ工科大学（ETH Zurich）をはじめ、Microsoft 社は世界中に共同研究拠点を拡大し、拡張性の高いユニバーサル量子コンピュータの実現を目指している[67]。また、同社が本社を置くワシントン州 Redmond では、Quantum Architectures and Computation（QuArC）と呼ばれる専門チームにより、将来的に実現が見込まれる量子コンピュータで動作可能なソフトウェア（量子アルゴリズム及び次世代量子プログラミングプラットフォーム）の開発も進められている[68]。

Microsoft 社で量子コンピュータ開発のコーポレート・バイスプレジデントを務める Todd Holmdahl 氏は、同社のクラウドプラットフォーム Azure 上で商用量子コンピュータのサービス提供を 2023 年にも実現できるとの見通しを示している[69]。こうしたサービスの商用化も視野に入れ、Microsoft 社は 2017 年 12 月、量子コンピュータ開発キット（Microsoft Quantum Development Kit）のプレビュー版を公開した[70]。同社のサイトから無料でダウンロードできる同開発キットは、①量子コンピューティング用のプログラミング言語 Q#と、②Q#で開発した量子アルゴリズムやソリューションをテストするためのシミュレーター[71]、③量子コンピュータ向けコードのライブラリ及びサンプルの 3 項目から構成されており[72]、次世代の量子コンピュータ開発で開発者を支援することが期待されている。

d. Alibaba 社

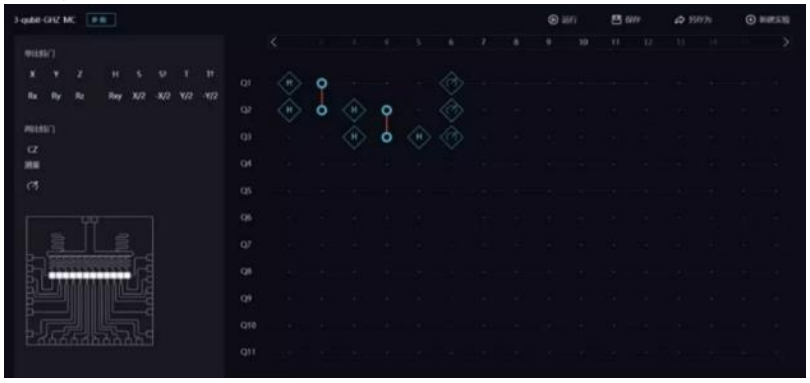
中国の E コマース企業最大手 Alibaba Group（以下 Alibaba 社）は 2015 年 7 月末、中国最大の自然科学及びハイテク研究開発機関である中国科学院（Chinese Academy of Sciences：CAS）と、「中国科学院－Alibaba 社量子コンピューティングラボ（CAS - Alibaba Quantum Computing Laboratory：QAL）」を共同で開設した[73]。Alibaba 社の発表資料では、同ラボは、Alibaba 社のクラウドコンピューティング技術や計算アルゴリズム技術と、CAS の有する量子コンピュータ及び量子 AI といった技術的な強みを合わせ、E コマースやデータセンター向けの革新的なセキュリティ技術や古典コンピュータを上回る高速計算処理技術に関する量子理論の先駆的研究に取り組むとしている。その後、Alibaba 社は 2018 年 3 月、QAL の開発した量子ゲート方式の超伝導型 11 量子ビットのコンピュータを同社のクラウド上で一般公開することを発表した[74]。同社は、技術的なボトルネックの特定やユーザーエクスペリエンスの最適化、次世代プロセッサの開発につなげるため、同プラットフォーム上でアルゴリズムの動作を試験するよう様々なユーザー（特に研究者）に促している[75]。

AQL は、2025 年までに現在世界最速のスーパーコンピュータと同水準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の試作機を開発する計画を公表している[76]。また、Alibaba 社は 2018 年 9 月、社内で独自の量子プロセッサを開発中であるほか、Alibaba DAMO Academy[77]では、クラウド上で量子コンピュータの能力を提供するための技術や、機械学習、最適化、物理学のシミュレーションにおける基本問題を解くための古典・量子コンピュータのハイブリッド型アルゴリズムの開発を進めており、E コマース、物流、材料、製薬等の幅広い業界分野における量子コンピュータの活用を模索するため、ソリューションパートナーのネットワーク拡大にも注力する方針を明らかに

[67] https://www.microsoft.com/en-us/research/lab/quantum/
[68] https://www.microsoft.com/en-us/research/group/microsoft-quantum-redmond-quarc/
[69] https://www.computerweekly.com/news/252440763/Microsoft-predicts-five-year-wait-for-quantum-computing-in-Azure
[70] https://cloudblogs.microsoft.com/quantum/2017/12/11/announcing-microsoft-quantum-development-kit/
[71] ユーザーの開発システム上で動作するローカルのシミュレーターのほか、40 量子ビットを超える量子コンピュータの動作をシミュレートできる Azure 上で動くシミュレーターも提供されている。
[72] https://www.microsoft.com/en-us/quantum/development-kit
[73] https://www.alibabagroup.com/en/news/article?news=p150730
[74] https://www.alibabacloud.com/press-room/alibaba-cloud-and-cas-launch-one-of-the-worlds-most
[75] https://medium.com/syncedreview/alibaba-launches-11-qubit-quantum-computing-cloud-service-ad7f8e02cc8
[76] https://physicsworld.com/a/joint-quantum-computing-venture-is-a-first-for-china/
[77] DAMO Academy は、技術・科学分野の調査研究を Alibaba 社がリードするための国際的なイニシアチブに取り組む機関。

している[78]。Alibaba 社の CTO 兼 Damo Academy 責任者の Jeff Zhang 氏は、量子コンピュータの開発における同社の目標は、量子ビット数を増やすことのみにとどまらず、既存のプログラムの中から量子コンピュータで処理することが（古典コンピュータより）効率的な計算処理タスクを選定し、エンジニアの抱える問題を解決することだとしている[79]。

図表 14：Alibaba 社の量子コンピュータクラウドプラットフォーム



出典：Medium

② スタートアップ

a. D-Wave Systems 社

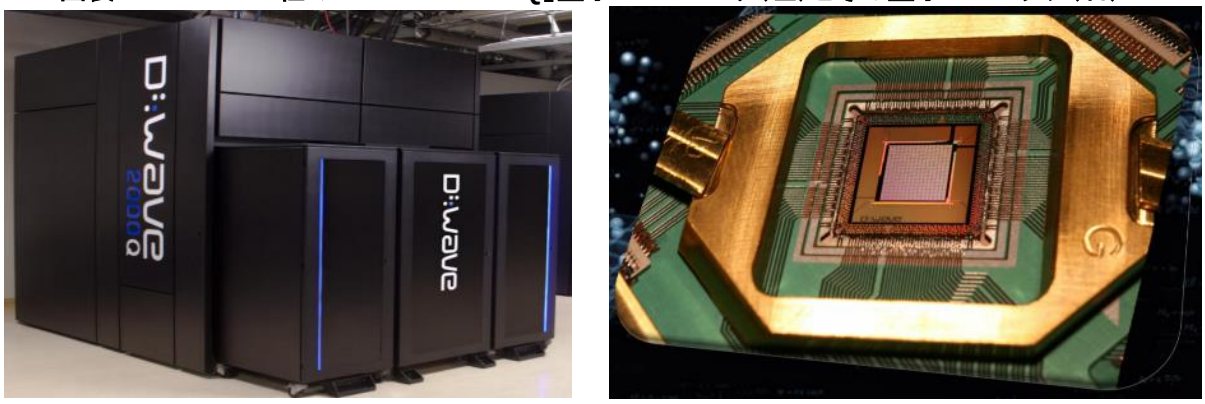
D-Wave Systems 社は、カナダのブリティッシュコロンビア大学（University of British Columbia）出身の Geordie Rose 氏らにより 1999 年、ブリティッシュコロンビア州バーナビー（Burnaby）に創設された量子アニーリング方式のコンピュータ開発で業界をリードするベンチャー企業である。ノイズの影響を受けにくく量子ゲート方式よりも壊れにくい量子コンピュータモデルを謳った D-Wave 社の量子コンピュータ開発ビジョンは、AI 開発を加速する次世代コンピュータ技術として 2003 年までにベンチャーキャピタリストの Steve Jurvetson 氏をはじめとする著名な投資家やベンチャーキャピタル（VC）の関心を集めるようになり[80]、同社は Amazon 社の共同創設者兼 CEO の Jeff Bezos 氏や In-Q-Tel 社[81]等から 1 億ドルの資金を獲得、2007 年には、実用的な問題[82]を解くことができる初のシステムとして 16 量子ビットのマシンの開発に成功した[83]。

D-Wave 社は 2011 年 5 月、世界初の商用量子コンピュータとして 128 量子ビットの「D-Wave One」を Lockheed Martin 社に 1,000 万ドルで売却する契約を締結[84]したことで業界に衝撃を与え、その後 2013 年に発表された 512 量子ビットの「D-Wave Two」を Google 社（NASA）が購入したことは上述の通りである。同社はその後も、2015 年に 1,152 量子ビットを搭載した「D-Wave 2X」を発表[85]し、2017 年 1 月に 2,000 量子ビットの「D-Wave 2000Q」の発表及び米セキュリティ企業 Temporal Defense Systems 社と同マシンの最初の導入契約を締結[86]したことを明らかにするなど、2 年毎に量子ビット数を倍増させた新モデルを市場に投入し、注目を集めている。また、同社は 2018 年 10 月、D-Wave 2000Q にクラウド上でアクセスでき

[78] https://damo.alibaba.com/events/38
[79] https://www.technologyreview.com/s/612190/why-alibaba-is-investing-in-ai-chips-and-quantum-computing/
[80] D-Wave 社は、その他 Goldman Sachs 社やカナダ政府なども含め、これまで総額 2 億 1,000 万ドルを調達している。
[81] 米中央情報局（CIA）が 1999 年に設立した VC 企業。
[82] 数独パズル、食卓への着順問題、特定の分子と分子データベースとの照合という 3 つの最適化問題。
[83] https://www.wired.com/2014/05/quantum-computing/
[84] https://www.dwavesys.com/news/d-wave-systems-sells-its-first-quantum-computing-system-lockheed-martin-corporation
[85] https://www.dwavesys.com/blog/2015/08/announcing-d-wave-2x-quantum-computer
[86] https://www.dwavesys.com/press-releases/temporal-defense-systems-purchases-first-d-wave-2000q-quantum-computer

る「Leap」サービスを開始した[87]。同サービスでは、登録すれば誰もが毎月 1 分間無料でアクセスできる[88]が、1 時間当たり 2,000 ドルの有料プランも提供されており、D-Wave 社は同社のシステムを多数の開発者に開放し、新たなソフトウェアアプリケーションの開発等を奨励することで、そのエコシステムを拡大することを狙いとしている[89]。

図表 15：D-Wave 社の「D-Wave 2000Q」量子コンピュータ（左）とその量子プロセッサ（右）



出典：D-Wave

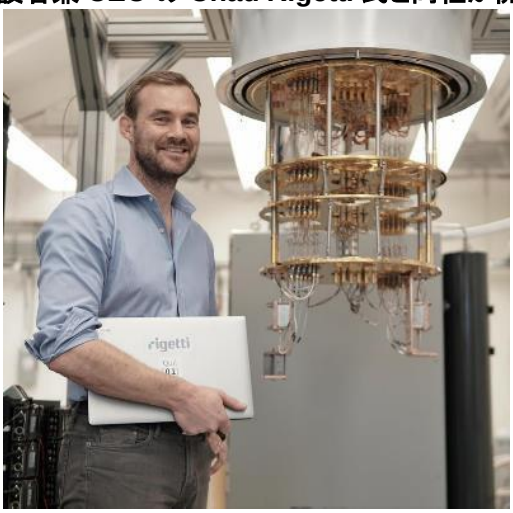
D-Wave 社が量子コンピュータ関連の技術に関してこれまで取得している米国特許数は 160 件以上に上るほか、同社は主要科学誌 100 本以上の論文を寄稿している[90]。同社のシステムは当初、一部の専門家による激しい批判に晒され、量子コンピュータと呼べるかどうかについて議論を巻き起こしたが、同社の技術に関する論文や Google 社をはじめとする大手企業のシステム導入例などを背景に、こうした議論は収束しつつあり、同社のシステムを機械学習や量子物質科学等の分野に応用するために活用する企業及び研究機関も日本、欧州、北米を中心に近年増加傾向にある[91]。D-Wave 社は 2019 年 2 月末、5,000 以上の量子ビットを搭載予定の次世代機を 2020 年半ばまでに発表し、クラウド上でも利用できるようにする計画を明らかにしており、同社によると、次世代機では、プロセッサに用いられている量子ビット間の結合数を D-Wave 2000Q の 6 から 15 に増やすことで、より大規模で複雑な最適化問題を少数の量子ビットで解けるようになるという[92]。

b. Rigetti Computing 社

カリフォルニア州バークレー（Berkeley）に拠点を置く Rigetti Computing 社は、イェール大学（Yale University）で応用物理学の博士号を取得後、IBM 社の量子コンピュータラボで量子ハードウェア研究に従事した経験を持つ Chad Rigetti 氏により 2013 年に創設された、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る。ハードウェアの設計・製造からソフトウェア開発までを包括的に手がける同社は、「世界で最も強力なコンピュータを構築する」というミッションを掲げ、IBM 社や Google 社、Microsoft 社といった大手テクノロジー企業と量子コンピュータの開発分野で競合関係にあるが、シリコンバレーの著名 VC、Andreessen Horowitz 社等からこれまで 1 億 1,900 万ドル以上の資金を獲得するなど[93]、業界でその動向が注目されている。

[87] https://www.dwavesys.com/press-releases/d-wave-launches-leap-first-real-time-quantum-application-environment
[88] D-Wave 社は、D-Wave 2000Q の計算処理能力を用いれば、1 分間で 400～4,000 の問題を解くことが可能としている。
[89] https://siliconangle.com/2018/10/04/d-wave-provides-free-access-developers-build-ecosystem-around-quantum-computing/
[90] https://www.dwavesys.com/our-company/meet-d-wave
[91] https://www.dwavesys.com/press-releases/new-customers-and-funding-fuel-d-wave-growth
[92] https://venturebeat.com/2019/02/27/d-wave-previews-quantum-computing-platform-with-over-5000-qubits/
[93] https://rigetti.com/about

図表 16：Rigetti 社の創設者兼 CEO の Chad Rigetti 氏と同社が開発中の量子コンピュータ



出典：Rigetti

Rigetti 社はこれまで、8 量子ビットと 19 量子ビットのプロセッサを開発し、クラウド上のオープンソースプラットフォーム「Forest」を通じて一般公開してきたが、2018 年 8 月、量子コンピュータの開発において、「量子アドバンテージ（quantum advantage[94]）」と同社が称する短期的なマイルストーンを達成するためには、まず、エラー率を下げながら量子ビット数を増やすことが必要とし、2019 年 8 月までに 128 量子ビットのシステムを構築する計画を明らかにしている[95]。また、同社は 2018 年 9 月、量子コンピュータを用いたアルゴリズムのテストスピードを大幅に向上させるための新クラウドサービス「Quantum Cloud Services（QCS）」を立ち上げることを発表した[96]。同社によると、QCS では、古典コンピュータと量子コンピュータの両方を備えたデータセンターを通じて（古典・量子）ハイブリッドアルゴリズムの実行が最適化されており、その実行速度を既存のクラウドサービスより 20～50 倍向上させられる[97]ほか、クラウド上での量子プログラミングに用いる Forest などのツールが予め設定された状態で提供されているため、システム環境に不慣れな研究者も容易に実験の準備やアルゴリズムの試験を行えるようになっているという。当初、QCS で研究者がアクセスできるのは Rigetti 社の 16 量子ビットのプロセッサのみであるが、将来的には 128 量子ビットのプロセッサも利用できるようになる予定である[98]。Rigetti 社は、2019 年 1 月末から、QCS のパブリックベータ版の公開を開始している[99]。

Rigetti 社は 2018 年 10 月末、量子コンピュータの実用化を加速するための大胆なイニシアチブとして、「量子アドバンテージ・プライズ（Quantum Advantage Prize）」と称する賞金 100 万ドルのイノベーションコンテストを開催することを発表した[100]。Rigetti 氏は、「過去 5 年間は量子コンピュータ市場の発展における第 1 フェーズであり、同社及び他のテクノロジー企業は汎用型のプログラム可能な量子コンピュータの構築という課題を達成することに成功した」と述べ、次の第 2 フェーズでは、量子アドバンテージの達成が課題となる

[94] Rigetti 社は、量子コンピュータが重要で価値のある現実問題を古典コンピュータよりもうまい方法で、迅速又は安価に解決できることを示すことと定義する。
[95] https://medium.com/rigetti/the-rigetti-128-qubit-chip-and-what-it-means-for-quantum-df757d1b71ea
[96] https://medium.com/rigetti/introducing-rigetti-quantum-cloud-services-c6005729768c
[97] 研究者がクラウド上で量子コンピュータを用いる場合、古典コンピュータで古典・量子ハイブリッドアルゴリズムのプログラミングを行ってから、アプリケーション・プログラミング・インターフェース（API）を介してクラウド上の量子コンピュータを呼び出して計算処理を実行する（その後、計算結果は古典コンピュータに送り返される）手法を取ることが多い。しかし、Rigetti 社によると、同手法ではレイテンシ（通信遅延）問題が発生し、アルゴリズムのパフォーマンスが遅くなることが同社の開発チーム及び同社の既存のクラウドサービスユーザーにより発見されたとしている。
[98] https://www.technologyreview.com/s/611962/faster-quantum-computing-in-the-cloud/
[99] https://medium.com/rigetti/quantum-cloud-services-opens-in-public-beta-31989e15e36e
[100] https://medium.com/rigetti/the-rigetti-quantum-advantage-prize-8976492c5c64

としている。同コンテストでは、各参加チームに対し、①Rigetti 社の QCS 上で動作するアルゴリズムが、古典コンピュータより高速であるか、質が高いか、安価であること、②純粋理論的な実証ではなく真のビジネス価値を創出すること、の 2 つの条件を満たすことが求められている。特に Rigetti 氏は、「米国で量子コンピューティング産業を発展させるためには、技術の構築ではなく、技術を実際のビジネスに応用し、市場や顧客にとって価値を生み出すことが重要である」としている。Rigetti 社は、今後数カ月かけてパートナー企業と問題を提議し、関連データの提供も行う予定である。参加チームにより提出されたアルゴリズムの評価プロセスは、まず量子コンピュータの研究コミュニティによる評価を受け、承認されれば、その後ビジネス／科学界のリーダーから成る第三者委員会による審査を受けられる。第三者委員会から承認されれば、そのチームは賞金を獲得できるが、Rigetti 氏によると、それは 3～5 年後になる見込みであるという[101]。

c. QC Ware 社

2014 年にカリフォルニア州パロ・アルト（Palo Alto）に創設された QC Ware 社は、量子コンピュータを用いた企業向けソフトウェアソリューションの開発を手がけるスタートアップである。量子アルゴリズムの研究に第一線で取り組む研究者を集めて組織[102]された同社は、IBM 社や Google 社、Rigetti 社、D-Wave 社等の主要企業の開発する複数の量子コンピュータシステムにアクセスできる単一のソフトウェアプラットフォームをクラウド上で提供しており、量子コンピュータに関して特定の知識を持たない企業ユーザーが、ノイズの多い量子プロセッサ等を制御し、最適化、シミュレーション、機械学習関連の問題を解くためのアルゴリズムを容易に動作させられるよう支援している[103]。同社の顧客には、航空・宇宙、金融サービス、電力、石油・ガス、自動車等の業界における多数の大手企業が含まれるほか、NSF、NASA、USRA 等の政府機関とも提携しており、2018 年 7 月には、Citigroup 社や Goldman Sachs 社、Airbus Ventures 社、Fenox Venture Capital 社などから総額 650 万ドルの資金を調達している[104]。

QC Ware 社のビジネス開発担当責任者である Yianni Gamvros 氏は、「量子コンピュータの活用に今から取り組む企業にとっての利点は、必要なスキルを早くから蓄積し、機械学習（AI）と同様、将来的に既存の業界に破壊的な変化をもたらすことが予想される同技術の導入準備が整った段階で、いち早くその恩恵を受けられることだ」と語る。同社は、2018 年夏からアルファ版としてサービスのテスト提供を行っており、2019 年後半から拡張ベータ版サービスを企業ユーザー及び政府機関向けに、単独サービス又はソフトウェア開発プロジェクトの一環で提供する予定である。同社は主に、サブスクリプション形式で提供している同社のソフトウェアプラットフォームのクラウドサービスと、大手企業と共同で取り組んでいる量子コンピュータを用いたプロトタイプアプリケーションの開発で収益を上げている[105]。同社は、量子コンピュータを有効なリソースとして活用する上で、現在企業が直面している技術的な課題に対応するためのソフトウェア開発に注力し、非常に速いペースでビジネスを構築してきたが、今後、顧客層をデータサイエンティストや最適化問題及び化学分野の専門家などに拡大したいと考えている。同社の CEO、Matt Johnson 氏は、同社の短・中期的なビジネス目標について、向こう 1～2 年間は顧客の問題や要求に沿ったアルゴリズム及びソフトウェアの開発を継続しながら、ソフトウェアプラットフォームの構築に注力し、今後 3～5 年以内に実際のビジネスで量子コンピュータを活用した問題解決のブレークスルー事例を一つでも誕生させ、様々な業界における顧客の利用につなげたいとしている[106]。

---

[101] https://www.forbes.com/sites/alexknapp/2018/10/31/can-make-a-quantum-computer-live-up-to-the-hype-then-rigetti-computing-has-1-million-for-you/#53c2972271ce

[102] https://qcware.com/team

[103] http://techgenix.com/quantum-computing-startups/

[104] https://qcware.com/about、https://www.prnewswire.com/news-releases/qc-ware-raises-6-5-million-series-a-financing-for-its-cloud-quantum-computing-software-service-300678415.html
QC Ware 社の年間収益は現在 500 万ドルである。

[106] https://www.quantumtechcongress.com/blog/qc-ware-quantum-computing-for-the-masses-1

4　今後の展望と日本への示唆

量子コンピュータの開発においては、特に近年、米国、中国、欧州で関連研究開発プログラムに多額の政府資金が投入され、その開発競争が過熱しており、IBM 社、Google 社、Microsoft 社、Alibaba 社といった大手テクノロジー企業や、D-Wave 社、Rigetti 社等のスタートアップが量子ゲート方式又は（及び）量子アニーリング方式でのハードウェア開発に積極的に取り組んでいる。D-Wave 社の量子アニーリング方式のコンピュータは、最適化問題に特化したものであるが、機械学習への応用が期待される中、マシンの商用化や導入、実用化に向けた実証実験等の取組で先行している。量子ゲート方式では、IBM 社が研究所の外で動作する世界初の統合型量子コンピュータ商用マシンを最近発表するなど、商用化に向けて大きな進展がみられる。一方、実用化においては、今後数年以内に主流となることが見込まれる、ノイズが多くエラー率の高い数百量子ビット規模のプロセッサ上で、古典コンピュータでは不可能な計算性能を実現することでビジネス等における現実的な問題解決につなげること（Google 社や Rigetti 社が取り組む「量子超越性」や「量子アドバンテージ」の実現）が主要課題となっている。量子コンピュータを開発する企業は、それぞれクラウド上でマシンにアクセスできるサービスを提供しているが、近年は、QC Ware 社など、主要量子コンピュータシステムで動作する企業向けアプリケーションの開発を専門とする企業も出現し、商用アルゴリズムの開発及び量子コンピュータのビジネス利用を後押ししている。

日本においては、NTT 社や富士通社等の大手企業が D-Wave 社の量子コンピュータに対抗するイジングモデル型のコンピュータの開発を推進している。特に、内閣府総合科学技術・イノベーション会議が主導する革新的研究開発推進プログラム（ImPACT）の一環で、東京大学と NTT 社が共同開発した、光を量子ビットとして使って組み合わせ最適化問題を解く 2,000 量子ビットのマシン「量子ニューラルネットワーク（QNN）」が、2017 年 11 月末にクラウド上で一般公開された際には、日本も世界で加熱する量子コンピュータ開発競争に加わったとして、複数の海外メディアでその取組が取り上げられている[107]。しかし、量子コンピュータへの世界的な投資が拡大する中、欧米と比較して日本の投資規模ははるかに小さく、研究者の間では、「日本は基礎研究は健闘しているが、マシンの開発競争は北米優位であり、投資規模の差が効いているのかもしれない」との声もあがっている[108]。

量子コンピュータの潜在的可能性を実現する上では、重大な技術的問題を克服する必要があり、今後、より安定性の高い量子ハードウェアのほか、ソフトウェア開発に必要な商用プラットフォーム、量子コンピュータのリソースにアクセスするためのクラウドコンピューティング機能の開発が求められる[109]。様々な業界で実用化への期待が高まる一方、量子コンピュータが既存の暗号システムに及ぼす脅威についても十分に理解する必要がある。2018 年 12 月はじめに米科学アカデミー（National Academy of Sciences）が発表した量子コンピュータに関する最新レポート[110]によると、公開鍵暗号が破られるまでには 10 年以上の期間を要するが、量子コンピュータを使用した攻撃により各業界が受ける情報／データ流出被害は、1 億 4,300 万人の個人情報が流出した 2017 年の Equifax 社ハッキング事件の 1,000 倍と推定され、今からポスト量子暗号の開発・導入等の準備を進める必要があると警告している[111]。

[107] http://quantumbusiness.org/japan-intends-forefront-quantum-leap/ 、https://www.techpowerup.com/239040/japan-opens-prototype-quantum-computing-system-for-public-worldwide-use、https://www.thedailystar.net/world/asia/japan-launches-its-first-quantum-computer-prototype-nii-ntt-university-of-tokyo-1494877
[108] https://jp.reuters.com/article/conputer-us-japan-idJPKCN1BB16M
[109] https://www.cbinsights.com/research/report/quantum-computing/
[110] http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=25196
[111] https://www.forbes.com/sites/arthurherman/2018/12/17/2019-americas-quantum-leap-year/#76514c402896

が、本レポート内の情報の利用によって損害を被った場合も、執筆者及び執筆者が所属する組織が如何なる責任を負うものでもありません。