国立国会図書館 調査及び立法考査局

Research and Legislative Reference Bureau
National Diet Library

論題 Title	研究開発の動向
他言語論題 Title in other language	Trends of Research and Development in Quantum Information Technologies
著者 / 所属 Author(s)	藤井 啓祐（FUJII Keisuke）／大阪大学大学院基礎工学研究科システム創成専攻電子光科学領域教授、市川 翼（ICHIKAWA Tsubasa）／大阪大学量子情報・量子生命研究センター（QIQB）特任准教授、山下 眞（YAMASHITA Makoto）／大阪大学量子情報・量子生命研究センター（QIQB）特任准教授、根来 誠（NEGORO Makoto）／大阪大学量子情報・量子生命研究センター（QIQB）准教授、山本 俊（YAMAMOTO Takashi）／大阪大学大学院基礎工学研究科／量子情報・量子生命研究センター（QIQB）教授
書名 Title of Book	量子情報技術　科学技術に関する調査プロジェクト報告書（Quantum Information Technologies）
シリーズ Series	調査資料 2021-6（Research Materials 2021-6）
編集 Editor	国立国会図書館 調査及び立法考査局
発行 Publisher	国立国会図書館
刊行日 Issue Date	2022-03-30
ページ Pages	—
ISBN	978-4-87582-888-4
本文の言語 Language	日本語（Japanese）
摘要 Abstract	量子 2.0 と呼ばれる量子情報技術の中核をなす量子コンピュータ、量子シミュレータ、量子センシング、量子通信・ネットワークについて、その原理、現在の開発動向及び将来展望を解説する。

観性及び正確性、論旨の明晰（めいせき）性等の観点からの審査を経たものです。

＊ 本文中の意見にわたる部分は、筆者の個人的見解です。

第2章　研究開発の動向

【要　旨】
量子2.0と呼ばれる量子情報技術の中核をなす量子コンピュータ、量子シミュレータ、量子センシング、量子通信・ネットワークについて、その原理、現在の開発動向および将来展望も含めてそれぞれの研究分野の専門家により解説する。各分野で開発の進められている技術は用途に応じてそれぞれ異なるが、量子演算を行うデバイスの開発という点では共通項も多い。量子コンピュータと量子シミュレータはその目的や方式は大きく異なるが、多数の量子ビットもしくは量子系を用意した忠実な演算が課題である。量子センシングは実用に最も近いと言われているが、様々なフィールドに対応する必要がある。量子通信・ネットワークではセキュア通信が短距離では実装され、商用化されているが、更に長距離化し、大規模化するには課題がある。これらの課題を克服するため世界的に壮大な取組が行われており、中核技術の発展の先には、今後の量子情報技術の幅広い可能性がある。

Ⅰ　量子コンピュータ

はじめに

コンピュータは我々の生活にとって欠かせない存在となっている。半導体集積回路に搭載されているトランジスタ数が2年ごとに2倍になるというムーアの法則(1)に従って、これまでコンピュータの性能は飛躍的に向上してきた。それでもなお、Society5.0(2)やデジタルトランスフォーメーション(3)に向けた取組の中、計算資源に対する我々の要求は尽きない。一方で、半導体集積回路の微細化には限界があり、ムーアの法則は限界を迎えつつある(4)。

そのような中、0や1（ビット）で情報を表現しそれらの和や積で計算を行う古典コンピュータの原理を、ミクロな世界を支配する最も基本的な物理法則である量子力学に置き換えようというのが、量子コンピュータのアイデアである。量子コンピュータの登場は、まさに、コンピュータの有り様を根本的に考え直すまたとない機会であり、各国が研究開発への投資を加速させている（第4章を参照）。本節では、このような量子コンピュータがこれまで発展してきた歴史的経緯、量子コンピュータの仕組み、量子アルゴリズム、量子コンピュータの応用が検討されている問題や分野、そしてハードウェアの開発状況やソフトウェア開発環境について解説を行う。

1　歴史的経緯

一般に新聞やニュースにおいて量子コンピュータの名前を聞くようになったのはここ数年のことであるが、量子コンピュータそのものの研究は1980年代にその起源を見る。当時、既にコンピュータの発熱（エネルギーの消費）が問題になり始めており、そもそも計算というプロ

＊　本稿におけるインターネット情報の最終アクセス日は、令和4（2022）年2月21日である。
(1)　Gordon E Moore, “Progress in digital integrated electronics,” *Electron devices meeting*, Vol.21, 1975, pp.11-13.
(2)　「Society 5.0」内閣府ウェブサイト <https://www8.cao.go.jp/cstp/society5_0/>
(3)　「デジタルトランスフォーメーション」総務省『情報通信白書　平成30年版』2018, pp.3-4. <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/pdf/n1000000.pdf>
(4)　『ナノテクノロジー・材料分野領域別分科会「ナノエレクトロニクス」―ポストムーアに向けた技術展望―俯瞰ワークショップ報告書―』科学技術振興機構研究開発戦略センター, 2016. <https://www.jst.go.jp/crds/pdf/2016/WR/CRDS-FY2016-WR-05.pdf>

セスに発熱は必要か否か、発熱しないコンピュータは実現可能か、という問題が研究者の間で話題になった。こうした問題は、その計算を担うデバイスが従う物理法則に立ち返って計算というものを考え直すことを促し、それまで分断されていた情報と物理の分野が融合することになる[5]。そのような中、ノーベル物理学賞を受賞したことでも有名なリチャード・ファインマン（Richard P. Feynman）は、1981 年に開催された国際会議[6]において「自然は古典物理では動いていない。自然を効率よくシミュレーションしたければ、量子力学の原理でコンピュータを作らなければならない」と指摘した。当時既に量子力学の基礎は確立されており、複雑な計算を体系的に取り扱うために素粒子の反応を直感的に図示したファインマンダイアグラムを発明したファインマンは、自然界を模倣するには従来の 0 や 1 で計算を行う古典的なコンピュータ（以下、「古典コンピュータ」）では不十分であることを痛感していたのであろう。これが、量子力学の原理で計算をするコンピュータ、量子コンピュータの源流であると言える。また、量子コンピュータとはいかなるものであるべきか、その構成を具体的に提示したのは、その後のデイヴィッド・ドイッチュ（David Deutsch）による研究である[7]。なお、我が国では、当時 NTT の研究者であった井桁和浩・山本喜久が、単一の原子と光を用いた量子コンピュータの提案を 1988 年に発表している[8]。ただし、この段階では、量子コンピュータの研究は、情報と物理の境界領域に魅せられたごく少数の研究者のテーマであった。

量子コンピュータが多くの研究者の注目を集めるようになったきっかけは、1990 年代中頃に訪れる。1994 年、当時 AT&T ベル研究所に在籍していたピーター・ショア（Peter W. Shor）が素因数分解問題を効率よく解くことができる量子アルゴリズムを発見した[9]。素因数分解は、15=3 × 5 のように桁数が少ない場合は簡単に解くことができるが、桁数が増えるにつれて因数を見つけることが指数関数的に難しくなる[10]。2021 年現在、素因数分解された最も大きな整数は 250 桁である[11]。このような素因数分解の難しさはクレジットカード決済や銀行間取引で利用される RSA 暗号化方式[12]の安全性の論拠となっている。このように難しい問題の代表格である素因数分解問題が、計算の原理を 0 や 1 の和・積から量子力学の原理へと置き換えることによって、桁数に対して多項式的な、より短い時間で解けることが示された。このことは、量子コンピュータがごく一部の物理学者のトイモデル[13]にとどまるものではなく、それが実現することによって計算の難しさの尺度が根本的に変わる可能性があることを知らしめ、量子コンピュータを含めた量子情報科学分野が一つの研究分野へと広がる一つの重要なきっかけを与えた。実験側も、我が国において 1999 年に固体で世界初の量子ビット（後述）が、当時

⑸　このような流れは量子系への計算の拡張も含め、後の 1991 年に Rolf Landauer, “Information is physical,” *Physics Today*, vol.44 no.5, 1991, pp. 23-29 においてまとめられている。

⑹　*1st conference on Physics and Computation*, MIT, 1981; Richard P. Feynman, “Simulating physics with computers,” *International journal of theoretical physics*, vol.21 nos.6-7, 1982, pp. 467-488.

⑺　David Deutsch,“Quantum theory, the Church–Turing principle and the universal quantum computer,” *Proceedings of the Royal Society of London A*, vol.400 no.1818, 1985.7.8, pp.97-117.

⑻　K. Igeta and Y. Yamamoto, “Quantum mechanical computers with single atom and photon fields,” H. Inaba et al. eds., *International Conference on Quantum Electronics, OSA Technical Digest*, paper TuI4, 1988.

⑼　Peter W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994.

⑽　桁数に対して計算量が指数関数的（厳密には超多項式的）に増加する。

⑾　Paul Zimmermann, “Factorization of RSA-250,” *cado-nfs-discuss* (Mailing list), February 28, 2020.

⑿　Ronald L. Rivest et al., “A Method for Obtaining Digital Signature and Public-key Cryptosystems,” *Communications of the ACM*, Vol 21 Issue 2, Feb. 1978, pp.120-126.

⒀　物理学のモデリングにおいて、メカニズムを簡潔に説明できるように単純化したもの。

NEC に在籍していた中村泰信・蔡兆申（それぞれ現在は、理化学研究所、東京理科大学）らによって実現されるなど[14]、理論・実験両面から量子コンピュータ研究は大いに活気づいていた。これが今からみると、量子コンピュータの第一次ブームである。また、当時海外における量子コンピュータ研究の担い手は主に大学に所属する研究者であったのに対して、日本においては上述の NTT や NEC のように、企業においてこの量子コンピュータの萌芽的基礎研究が進められていたことにも注目しておきたい。しかしながら、大規模な量子コンピュータの実現にはまだ機が熟しておらず、2000 年代に入り量子コンピュータ研究は徐々に停滞期を迎える。理論面では比較的簡単に分かることは調べ尽くされ、難題ばかりが残されていた。実験面では、ミクロな量子の世界を精密に制御することの難しさが浮き彫りになり、地道な研究を必要とした。もちろん、この間にも着実に基礎研究が進められていたことは言うまでもない。

そのような中、量子コンピュータが再び注目を集めるようになったのは、2010 年頃のことである。カナダのベンチャー企業である D-Wave 社が量子コンピュータを商用化し[15]、Google がそれを用いて研究を開始したと発表した[16]。ただし、D-Wave 社が開発した量子コンピュータは、ドイッチュが提案し、それ以降量子情報科学分野で長らく研究されてきた「万能な」量子コンピュータではなく、量子効果を用いた超伝導デバイスを用いて特定の問題（組合せ最適化問題）を解く専用マシンという位置付けであった。この専用マシンは、「量子アニーリングマシン」と呼ばれており、その原理については東京工業大学の西森秀稔と当時学生であった門脇正史が提案した[17]。日本におけるメディア報道などでは、万能な量子コンピュータをゲート型、量子アニーリングマシンをアニーリング型（さらにその原理を古典コンピュータで模倣したものを擬似型）と呼ぶことが多いが[18]、次項以降では世界的に標準的な呼び方に倣い、主に前者を量子コンピュータと呼ぶことにする。万能な量子コンピュータと量子アニーリングマシンは、ともに後に説明する量子ビットを利用しているという共通点はあるものの、それに対する制御の方法やそれに要求される精度、複雑さ、そして量子性の強さについては全く異なり、前者のほうが高度な制御と高い精度、そしてより強い量子性を必要とする。このため、全く別の原理のコンピュータと考える方が正確である。

ゲート型の量子コンピュータに注目が集まるようになったのは、2014 年のことである。カリフォルニア大学サンタバーバラ校（UCSB）のジョン・マルティニス（John M. Martinis）のグループが、五つの量子ビットを集積化し、高い精度で動作させることに成功した[19]。達成された忠実度[20] は 99% を上回り、大規模な量子コンピュータを実現するために必須である量子誤り訂正を実行するために要求される忠実度と同等のレベルに到達したことが注目を集めた。この精度を維持しつつ、量子ビット数を増加させることができれば、大規模な量子コンピュータを実

⑭　Yasunobu Nakamura et al., “Coherent control of macroscopic quantum states in a single-Cooper-pair box,” *Nature*, vol.398 no.6730, 1999.4.29, pp.786-788.

⑮　Lisa Zyga, “D-Wave sells first commercial quantum computer,” June 1, 2011. Phys.org website <https://phys.org/news/2011-06-d-wave-commercial-quantum.html>

⑯　H. Neven et al., “NIPS 2009 Demonstration: Binary Classification using Hardware Implementation of Quantum Annealing,” 2009.12.7.

⑰　Tadashi Kadowaki and Hidetoshi Nishimori, “Quantum annealing in the transverse Ising model,” *Physical Review E*, vol.58 no.5, 1998, pp.5355-5363.

⑱　「日本勢、「疑似」型に力」『日本経済新聞』（電子版）2021.6.25.

⑲　Rami Barends et al., “Superconducting quantum circuits at the surface code threshold for fault tolerance,” *Nature*, vol.508 no.7497, 2014.4.23, pp.500-503.

⑳　忠実度（fidelity）とは、理想的な動作にどれくらい近いかを測るための尺度であり1（100%）に近ければ近いほど良い。

現することが可能になる。この結果を受けて、Google はマルティニスのグループごと Google に引き込んで（ゲート型の）量子コンピュータのデバイス開発に乗り出した。これがきっかけとなり、2014 年までは純粋な物理学的探究として進められてきた傾向があった量子コンピュータ研究が、実際に大規模なシステムを構築するという工学的なフェイズに転換した[21]。

その後、IBM は 2016 年にクラウドからアクセスできる量子コンピュータを公開した[22]。現状、クラウド公開されている量子コンピュータの量子ビットの規模は小さく、古典コンピュータに対して優位性があるような利用方法は現時点で存在しないが、実際に量子コンピュータに計算を実行させることができる環境を提供することは、教育的観点及び実験家だけではなく誰でも使えるようにするためのエンジニアリング（キャリブレーションの自動化など）の観点の 2 点において非常に重要な意味を持つ。

さらに、2017 年には、量子情報科学分野の指導的立場にある研究者、ジョン・プレスキル（John Preskill）が Q2B という量子コンピュータのビジネス応用を目指す国際会議における基調講演で、現在発展途上にある量子コンピュータを近未来的にどのように応用すべきかを語った[23]。その中で、近未来的に実現される、古典コンピュータに対して潜在的な優位性を持つが、量子誤り訂正を実装するには規模が足りない小・中規模の量子デバイスを、NISQ（Noisy Intermediate-Scale Quantum）技術と定義し、今後どのように活用していくべきかという問題提起を行った。2014 年以降、Google や IBM、そして同じく超伝導量子ビット方式でのハードウェア開発をめざすベンチャー Rigetti Computing などが量子コンピュータの実機をアップデートしていく中で、量子誤り訂正を実装する大規模な量子コンピュータを待たずして実機を応用するという機運が高まっていたこととも相まって、NISQ（=近未来的に実現する量子コンピュータ）の応用という新たな研究フィールドが形成されていった。

2019 年には Google が 53 量子ビットの量子コンピュータを高い精度で動作させることに成功し、ランダム量子回路を用いたベンチマークタスク[24]を実行した[25]。量子コンピュータの実機はこのタスクを 200 秒で実行できるのに対して、同じタスクを古典コンピュータで行なった場合は 1 万年かかるという見積りが発表され、この結果は「量子超越性」として日本においても各種メディアで報道され[26]注目を集めた。スパコンを用いた場合の計算速度については最適化の余地があり、IBM からの反論[27]やその後の古典コンピュータ上でのシミュレーション方法の改善によって、スーパーコンピュータを用いて同様の時間でシミュレーションができるようになっている[28]。現在、量子コンピュータが得意とするタスクにおいてスーパーコンピュー

---

(21)　Elizabeth Gibney, “Physics: Quantum computer quest,” *Nature*, vol.516 no.7529, 2014.12.3, pp.24-26.

(22)　IBM Newsroom, “IBM Makes Quantum Computing Available on IBM Cloud to Accelerate Innovation,” May 3, 2016.

(23)　*Quantum Computing for Business*, 5 December 2017; John Preskill, “Quantum computing in the NISQ era and beyond,” *Quantum*, vol.2, 2018.8.6, p.79.

(24)　ハードウェア上で実行可能な量子ゲートをランダムに選択してランダム量子回路構成し、ランダム量子回路の出力を測定する。このようにして得られるビット列には選んだ量子回路に依存した出力の偏りがあることを利用し、正しくサンプリングできているかどうかを検証するベンチマーク問題。

(25)　Frank Arute et al., “Quantum supremacy using a programmable superconducting processor,” *Nature*, vol.574 no.7779, 2019.10.23, pp.505-510.

(26)　「スパコンで 1 万年分の計算、3 分で　Google「量子超越」」『日本経済新聞』2019.10.23.

(27)　Edwin Pednault et al., “On “Quantum Supremacy”,” October 21, 2019. IBM website <https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/>

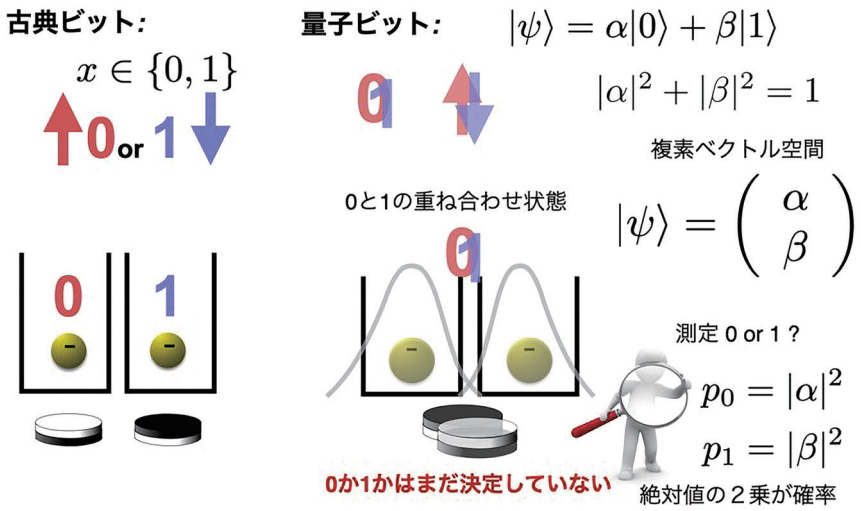
(28)　Yong Liu et al., “Closing the “quantum supremacy” gap: achieving real-time simulation of a random quantum circuit using a new Sunway supercomputer,” *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, 2021.

タと量子コンピュータが拮抗している状況であるが、いずれ量子コンピュータの量子ビット数が増え、演算精度が向上することによって、このような問題設定上での優位性は確たるものになると予想される。また、Google、IBM、Rigetti computing などが進める超伝導量子ビット方式だけではなく、IonQ や Honeywell が取り組むイオントラップ方式、さらには、PsiQuantum、Xanadu などが取り組む光量子ビットに加え、最近では冷却原子を用いた新たな方式も登場してきている。それぞれのハードウェアについては、「5　量子コンピュータハードウェア」において詳しく述べる。

2　量子コンピュータの仕組み

本項では、量子コンピュータの仕組みや古典コンピュータとの違いについて解説する。我々が日常的に利用しているコンピュータ内部では、ビットと呼ばれる 0 と 1 の二つの数字を用いて情報が表現されている。小数点以下が限りなく続く実数であっても、コンピュータの中では有限の精度で打ち切られビット列（2 進数）によって表現されている。そして、実数の足し算や掛け算などは 0 と 1 の二つの数字を受け取り、一定のルールに従って何らかの数字を返す論理演算を用いて実行される。物理的には、これらビットは異なった二つの物理状態が担っている。例えば、電圧が低い状態を 0、高い状態を 1 とする（トランジスタ）、又は、コンデンサに電荷が溜まった状態を 0、溜まっていない状態を 1 とする（DRAM メモリ）などである。そして、これらの物理状態を電気回路において制御することによって、0 と 1 の論理演算を実行する。これを高速かつ正確に行っているのが現在のデジタルコンピュータである。0 と 1 の二つの離散的な状態によって（デジタルに）情報を表現する利点は、物理的な状態（電圧やコンデンサの電荷など）が多少揺らいだとしても、適当な値で閾（しきい）を引いておけば 0 や 1 の情報は影響を受けないというノイズに対する堅牢さである。以降の量子情報の議論と区別するために、これら 0 と 1 で表現される情報やその処理を古典ビット、古典情報、古典計算などと以降で呼ぶことにする。

図 1　古典情報（ビット）と量子情報（量子ビット）の比較



（注）　量子力学の世界では異なる二つの事象の重ね合わせが許されており、0 と 1 の重ね合わせ状態である量子ビットが情報の最小単位として利用される。
（出典）筆者作成。

量子の世界における情報（量子情報）は、根本的に古典情報とは異なる。量子力学の世界には異なる状態のどちらとも確定していない重ね合わせ状態という状態が許されている。この重ね合わせ状態を許すと古典ビットの 0 又は 1 の二つの状態以外にも、0 と 1 が重ね合わさった状態を定義することができる。量子力学ではこのような重ね合わせ状態を二つの複素数（複素確率振幅）α、βと、0 や 1 の状態を表すベクトルの記法 $|0\rangle$と$|1\rangle$ を用いて $\alpha|0\rangle+\beta|1\rangle$ のように表現する。さらに、どのくらいの重みで 0 と 1 が重ね合わさっているか、という重ね合わせの重みは連続的に変化させることができる。例えば、0 と 1 がほぼ均等に重ね合わさった状態（$|\alpha|\fallingdotseq|\beta|$）や 0 がやや多く重ね合わさった状態（$|\alpha|>|\beta|$）などである。このような 0 又は 1 を取る重ね合わせの重みは、数学的には 2 次元の複素ベクトル（状態ベクトル）として $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ のように表現される。以上のように、量子力学の世界に情報の概念を拡張したものが量子ビット（量子の世界の情報の最小単位）である。

このような重ね合わせ状態にある量子ビットから我々が情報を得るためには、測定をする必要がある。量子力学の世界では、測定が不可避に状態を破壊する。例えば、重ね合わせ状態にある量子ビットに対して測定を実行することで、重ね合わせが壊れ、0 又は 1 のどちらかの状態が確定する。この時、0 を得る確率 p_0 は対応する複素確率振幅 α の絶対値の 2 乗 $|\alpha|^2$ によって、また、1 を得る確率 p_1 は同様に $|\beta|^2$ によって与えられる。ただし、確率は合計して 1 になっていないとおかしいので、複素確率振幅を要素にもつ状態ベクトルの大きさ（$|\alpha|^2+|\beta|^2$）は 1 と等しくなるように規格化されている。ある重ね合わせ状態が与えられた時に、1 回の測定では 0 と 1 が上記の確率に従ってランダムに得られるだけであるが、同じ重ね合わせ状態に準備された量子ビットに対して繰り返し測定すれば、複素確率振幅の絶対値の 2 乗の値、$|\alpha|^2$及び $|\beta|^2$ を推定することもできる。

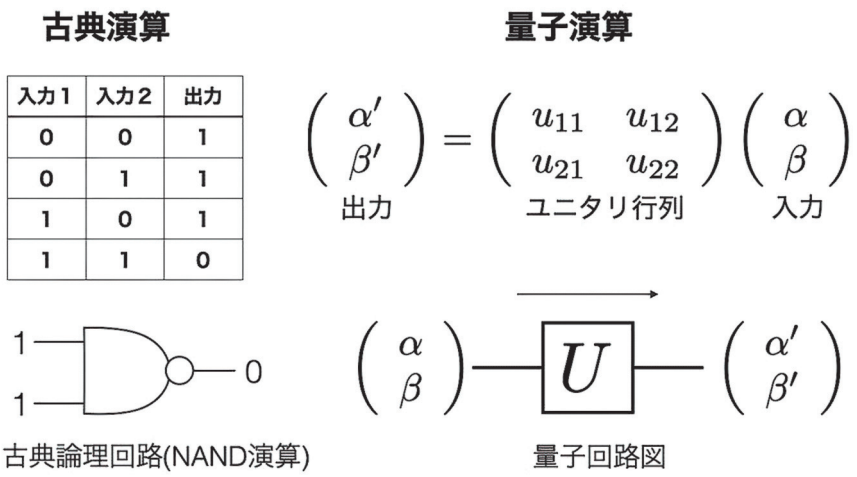
量子コンピュータでは、これら量子ビットに対して、古典計算と同様、なんらかの論理演算を実行して計算を行うことになる。古典ビットの世界では 0 や 1 を入力として受け取り、0 や 1 を返す論理演算が計算に使われる[29]。一方で、量子ビットの場合は、状態ベクトルを受け取り、状態ベクトルを返すような操作が量子演算となる。先述のように状態ベクトルは大きさが 1 に規格化されている必要があるので、このベクトルの大きさを変えないような操作が物理的に許された操作である。このような操作は数学的には、ユニタリ行列[30]として記述されることが知られている。つまり、量子情報の世界では、状態は複素確率振幅を要素にもつ状態ベクトルとして $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ のように表現され、そのベクトルに対してユニタリ行列 U を作用させることによって量子演算が実行されることになる。そして、量子演算が終わった後の状態 $\begin{pmatrix}\alpha'\\ \beta'\end{pmatrix}$ に対して先述の測定を行い、古典情報として計算結果を読み出すことになる。

---

[29]　古典計算における論理演算としては、NOT、AND、OR、NAND などが知られている。例えば、NAND 演算があれば任意の 0 と 1 を入出力にもつ関数を構成することができることが知られており、（古典）万能演算と呼ばれている。

[30]　ユニタリ行列とは、その行列の転置及び複素共役をとったものが元の行列の逆行列になるような行列であり、この性質からユニタリ行列を作用させてもベクトルの大きさは変化しない。

図２　量子ビットに対す量子演算の作用



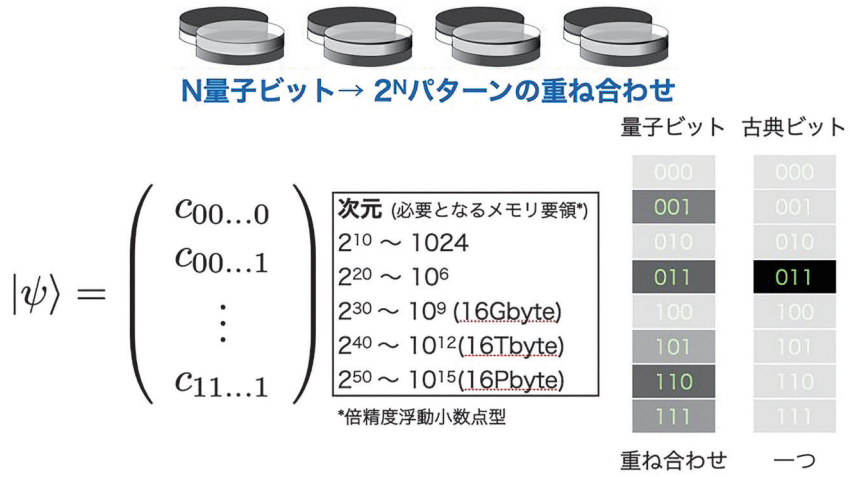
（出典）筆者作成。

量子ビットが複数ある場合について考えよう。古典情報の場合は、ビットが複数ある場合には、0 や 1 を並べて構成されるビット列で記述される。N ビット列であれば N 個の 0 や 1 の数字を並べることになる。一方で、量子の世界では重ね合わせ状態が許されている。重ね合わせ状態とは異なる事象が確定せず重ね合わさっている状態のことであった。N ビットの古典情報がとりうるパターンは、全て 0（00…0）から全て 1（11…1）までの 2^N 通りある。量子の世界では、このような N に対して指数関数的にたくさん存在するパターンを一つの量子状態として重ね合わせ状態で表現することができる。このような状態は一つの量子ビットの場合と同様に、それぞれのパターン（ビット列）を取る重ね合わせの重みである複素確率振幅を要素としてもつ複素ベクトル $\begin{pmatrix} C_{00\ldots0} \\ C_{00\ldots1} \\ \vdots \\ C_{11\ldots1} \end{pmatrix}$ によって表現される。つまり、N 量子ビットの状態は 2 の N 乗次元の複素ベクトルとして記述される[31]。一つの量子ビットの例と同じく、これに対する量子演算はユニタリ行列の積によって行い、結果の読み出しは測定によって実行される。N 量子ビットあるので測定を実行すると N ビット列の情報が得られることになる。ある N ビット列 x を測定結果として得る確率は、複素ベクトルの要素 C_x の絶対値の 2 乗、$|C_x|^2$ で与えられる。N 量子ビットに作用するユニタリ行列は状態ベクトルの次元 2^N に対応して $2^N \times 2^N$ のサイズの行列である。このため、量子コンピュータが量子力学という物理法則に従って行う量子演算を古典コンピュータ上でシミュレーションするためには、量子ビット数 N に対して指数関数的に大きな複素ベクトルの確保とそれに対するユニタリ行列の作用を実行する必要がある[32]。このため量子ビット数が増えると古典コンピュータで量子コンピュータをシミュレーションすることは一般に難しくなる。例えば、50 量子ビットの場合、約 10^{15} 個の複素数を確保する必

(31)　ここでは詳細に説明しないが、数学的にはテンソル積空間によって記述される。
(32)　実際のシミュレーションにおいては、ベクトルと行列の積を工夫することによって計算を高速化することになる。行列を疎にもつことによってベクトルを更新したり、ベクトル・行列をテンソル縮約問題に置き換えることによってシミュレーションが高速化される。しかしながら、量子コンピュータのシミュレーションは本質的に難しく、古典コンピュータにとって量子ビット数又は計算ステップ数に対して指数関数的に計算量を必要とする。

要があり、約 16 ペタバイトものメモリを要する[33]。これは、スーパーコンピュータの一次メモリをもってしても状態を確保するのが難しいレベルである。もちろん、計算を工夫することによってもう少し効率よくシミュレーションが実行できるが、50 ～ 100 量子ビットの複雑な量子計算をシミュレーションすることは難しい。このような文脈で、2019 年の Google による量子超越性に関する実験やその後の量子コンピュータと古典コンピュータの比較・競争が行われている。

図３　複数の量子ビットの記述



（出典）　筆者作成。

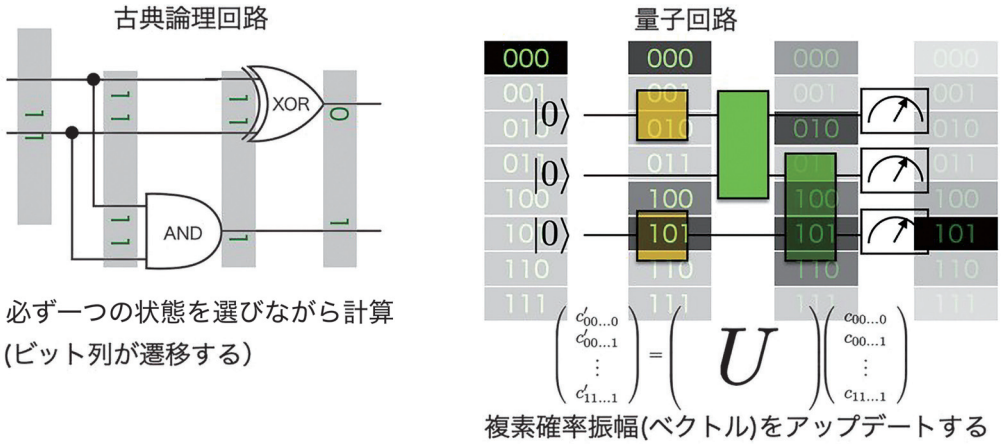
さて、量子情報の話に戻そう。量子コンピュータでは、重ね合わせ状態としてビット列を確定せず、指数関数的に大きな複素ベクトルとして状態を表現し、ユニタリ行列を量子演算として作用させることで計算が実行される。このユニタリ行列はいわば量子コンピュータのためのプログラムである。このプログラムを構成するためには個々の基本となる量子演算を並べていくことになる。基本となる量子演算のセットの取り方にはいろいろあるが、任意のユニタリ行列を構成できる基本演算のセットは、万能量子演算セット[34]と呼ばれている。万能量子演算セットが実行可能な量子コンピュータは万能量子コンピュータと呼ばれている。古典コンピュータとの最大の違いは、古典コンピュータにおいては、重ね合わせ状態が許されず、必ず計算の過程で 0 や 1 の情報が確定されて計算が実行されているのに対し、量子コンピュータでは 0 や 1 の情報を確定せず、いろいろなパターン（事象）を重ね合わせたまま計算を実行できるところにある（図 4）。

---

(33)　倍精度浮動小数点数では、一つの実数を 64 ビット = 8 バイトで表現する。一つの複素数を表現するには、実部と虚部があるので各 8 バイト計 16 バイトのメモリが必要になる。倍精度 50 量子ビットの場合に、2^{50} ～ 10^{15} 個の複素数を表現するため必要なメモリは 16×10^{15}=16Pbyte（ペタバイト）。

(34)　万能量子演算セットの例としては、重ね合わせ状態を生成するアダマール演算、位相を回転する位相回転演算、の 1 量子ビット演算に加え、エンタングル状態を生成できる制御 NOT（CNOT）演算による構成がある。エンタングル状態とは、量子系に特有な相関を持った状態であり、量子情報処理の資源として利用される。量子コンピュータにおいても、一般に量子アルゴリズムを実行している途中の量子状態は複雑にエンタングルした量子状態となっている。

図４　古典計算と量子計算の対比



（注）　古典計算は常に 0 又は 1 のどちらかを決めて計算を進めるのに対して、量子計算では 0 と 1 の重ね合わせ状態のまま計算を実行する。
（出典）筆者作成。

先ほど、量子コンピュータを古典コンピュータでシミュレーションすることが難しいと述べた。しかし、それが量子コンピュータを用いれば意味のある（役に立つ）計算を古典コンピュータにおける従来手法よりも速く計算できる、ということを直ちに意味するわけではない。例えば、複雑な風の流れをコンピュータ上でシミュレーションすることが難しい一方で、複雑な風の流れを利用してコンピュータが簡単に実行できる足し算や掛け算を高速に実行できるとは限らないことに似ている。量子コンピュータのポイントは、計算に複素確率振幅から成るベクトルを利用しているということを最大限に利用し、うまく量子演算（量子アルゴリズム）を構築することによって、特定の問題に対して古典コンピュータにおけるベストな手法よりもより高速に計算ができる、ということが示されているところにある。その最たる例は、先述の素因数分解アルゴリズムである。古典コンピュータ上のアルゴリズムでは桁数に対して多項式的な時間で解くことができないが、量子コンピュータの場合は、多項式的な時間で解を見つけることができる。つまり、重ね合わせをうまく利用することである種の意味のある（役に立つ）計算が加速されるのである。

３　量子アルゴリズム

現在、様々な量子アルゴリズムが発見され様々な分野へと応用されている。量子アルゴリズムの分類については、Quantum Algorithm Zoo[35]（及びその和訳[36]）に網羅的に記述されているのでそちらを参照されたい。代表的な量子アルゴリズムは、データベース探索アルゴリズム[37]と位相推定アルゴリズム[38]であり、これらを元に様々な量子アルゴリズムが開発されている。データベース探索アルゴリズムはソートされていないデータベースから特定の条件を満たしたアイテムを検索し取り出すアルゴリズムである。データ数が N である時、古典のデータベース

⑶5　Quantum Algorithm Zoo website <https://quantumalgorithmzoo.org/>
⑶6　「Quantum Algorithm Zoo 全訳」2018.5.20. Qmedia ウェブサイト <https://www.qmedia.jp/algorithm-zoo/>
⑶7　Lov K. Grover, “A fast quantum mechanical algorithm for database search,” *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996.7, pp.212-219. <https://arxiv.org/abs/quant-ph/9605043>
⑶8　A. Yu Kitaev, “Quantum measurements and the Abelian stabilizer problem,” 1995.11. <https://arxiv.org/abs/quant-ph/9511026>

において総当たりで探索をする場合、データ数Nに比例する時間がかかる。一方で、量子データベース探索アルゴリズムであれば、データ数Nに対してその平方根である√Nに比例した時間で目的のデータを得ることができる。その計算量はNから√Nに削減されるので、2乗加速（quadratic speedup）と呼ばれている。一方、位相推定アルゴリズムは、あるユニタリ行列Uが与えられた時に、そのユニタリ行列の固有値[39]を求めるアルゴリズムである。行列の固有値は様々な問題において重要な役割を担っている。例えば、素因数分解問題も、特定のユニタリ行列の固有値にその答えを見つけるための鍵を見出すことができる。また、量子多体系（量子力学に従って振る舞う複数の粒子からなる系）[40]のエネルギーの計算や線形連立方程式を解くための逆行列[41]の計算など、様々な応用がある。最近では、これらデータベース探索アルゴリズムによるアプローチと位相推定アルゴリズムのような固有値を取得するアルゴリズムが組み合わさった、特異値変換量子アルゴリズム[42]が構築され、量子アルゴリズムの新たな潮流となっている。

ここまで説明してきたアルゴリズムはその高速性がなんらかの形で保証されているアルゴリズムである。その反面、これらのアルゴリズムは非常に複雑な構造を持っており、現在実現しているレベルの量子コンピュータでは実現できない。これは、環境との望ましくない相互作用（ノイズ）や制御の不完全性によって、量子ビットの重ね合わせ状態が壊れてしまう、デコヒーレンスという現象があるからである。デコヒーレンスによって量子情報は失われてしまい、その結果、量子コンピュータにはエラーが生じてしまう。このようなエラーは、一つの量子ビットを複数の量子ビットを用いて符号化[43]する、量子誤り訂正[44]を用いることで訂正することができる。このとき、符号化によって埋め込まれた量子ビットを論理量子ビット、量子誤り訂正符号を構成する多数の量子ビットを物理量子ビットと呼ぶことにする。論理量子ビット数はアルゴリズムの実装において必要になる量子ビット数であり、物理量子ビット数はそれを量子誤り訂正を用いて守りながら実行するために必要となる総量子ビット数である。エラーの発生確率にもよるが、一つの守られた論理量子ビットを 100 ～ 1,000 物理量子ビットを用いて符号化することになる。量子アルゴリズムに必要な論理量子ビット数が 100 量子ビットであるとすると、全体として 1 万を優に超える物理量子ビットが必要になる。このように、量子誤り訂正によって符号化されたデータに対して、エラー検出と訂正を繰り返しつつ量子計算を実行するのが誤り耐性量子コンピュータ[45]である。様々な仮定に基づくが、2 千万物理量子ビットを用いた誤り耐性量子コンピュータによって 8 時間で 2048 ビットの整数の素因数分解を実行することができると試算されている[46]。膨大な数の量子ビットを必要とするが、それでも現在、古

---

(39)　行列 A に対して$A\vec{x} = a\vec{x}$となる複素数 a とベクトル$\vec{x}$が存在するとき、a を A の固有値といい、$\vec{x}$を固有ベクトルと呼ぶ。

(40)　分子や固体などの物質は、原子核と電子によって構成される。これら原子核や電子の振る舞いは量子力学（シュレーディンガー方程式）で記述される多体問題として取り扱う必要があるが、水素原子などの特定の可解模型を除いて厳密に方程式を解くことは難しい。このような複雑な系は多体量子系と呼ばれる。

(41)　行列 A の逆行列 A^{-1} とは、E を単位行列として $AA^{-1}=E$ を満たす行列のことである。

(42)　John M. Martyn et al., “A grand unification of quantum algorithms,” *PRX Quantum*, vol.2 iss.4, 2021.12, pp.40200-1-40203-40. <https://doi.org/10.1103/PRXQuantum.2.040203>

(43)　情報を一定の規則に従って別の形態に変換すること。

(44)　Peter W. Shor, “Scheme for reducing decoherence in quantum computer memory,” *Physical Review A*, vol.52 no.4, 1995.10, pp.R2493-R2496.

(45)　徳永裕己「量子コンピュータの誤り訂正技術―物理に即したトポロジカル表面符号―」『情報処理』55(7), 2014.7, pp.695-701.

(46)　Craig Gidney and Martin Ekerå. “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,” *Quantum*, vol.5, 2021.4.15, p.433.

典コンピュータで素因数分解できている最も大きい整数が 829 ビットであることと、素因数分解問題は指数関数的に計算時間が爆発することを考慮すると、8 時間で 2048 ビットの素因数分解ができることは驚くべきことである。この規模の量子コンピュータには 10 年から 20 年の研究開発が必要であるとされているが、暗号システムは長期にわたってセキュリティを担保できる必要があり、量子コンピュータに対しても安全性が担保される耐量子暗号の整備も重要である。

現在実現している、あるいは近未来的に実現する数十から 100 量子ビット規模の NISQ デバイスを利用したヒューリスティックアルゴリズム[47]も注目されている。主に、量子コンピュータを用いた変分量子アルゴリズム[48]が注目されている。一般的に、変分アルゴリズムとはパラメータをコスト関数に導入し、コスト関数を最小化するようにパラメータを更新することで問題を解く方法である。変分量子アルゴリズムでは、量子演算に連続的なパラメータを導入し、測定結果から計算されるコスト関数を最小化するようにパラメータを更新することで問題を解く。具体的には、コスト関数を組合せ最適化問題において最小化したいコストとすれば近似的に組合せ最適化問題を解くことができる[49]。また、コスト関数を磁性体や分子のエネルギーとすれば、材料・化学計算に必要な基底状態（最もエネルギーの低い状態）やそのエネルギーを知ることができる[50]。さらに、コスト関数を教師データ[51]と量子コンピュータからの出力の誤差、すなわち損失関数とすることで、量子コンピュータをモデルとした教師あり機械学習を実行することができる[52]。このアプローチの利点は、上記のようにコスト関数を解きたい問題によって取り替えることで、様々な用途に応用できるという点である。これらの変分量子アルゴリズムでは、変分パラメータが導入された量子状態の生成のみを量子コンピュータが担当しているため、ステップ数の少ない単純な量子回路でも実行できる。この単純さから NISQ デバイスでも実行が可能であるという特徴がある。しかしながら、従来手法に対する優位性があるかどうかはまだ定かではない。また、NISQ デバイスには誤り訂正機能を持たせることはできないため、ノイズの問題を根本的に解決することはできない。

したがって、近未来的な目標として NISQ デバイスで動作する量子アルゴリズムを用いて、従来手法に対する優位性やユースケースの探索が行われており、長期的には、量子誤り訂正の実現、そして誤り耐性量子コンピュータの実現が目標となっている。NISQ デバイスを用いたキラーアプリケーションを見つけることができるか、現在実現している NISQ デバイスから大規模な誤り耐性量子コンピュータへと継続的に技術を発展させることができるか、という 2 点が今後の展開において重要となっている。

4　量子コンピュータの応用分野

古典コンピュータが様々な用途で利用されているのと同様、量子コンピュータの応用が期待

⑷7⑸　必ずしも厳密に問題を解くことができるわけではなく、またその性能も理論的に保証されていないが、経験的な手法に基づいて近似的に問題を解く方法。

⑷8⑸　Marco Cerezo et al., “Variational quantum algorithms,” *Nature Reviews Physics*, vol.3 no.9, 2021.8.12, pp.625-644.

⑷9⑸　Edward Farhi et al., “A quantum approximate optimization algorithm,” 2014. <https://arxiv.org/abs/1411.4028>

⑸0⑸　Alberto Peruzzo et al., “A variational eigenvalue solver on a photonic quantum processor,” *Nature communications*, vol.5 no.4213, 2014.7.23, pp.1-7.

⑸1⑸　機械学習においてニューラルネットワークなどの学習可能なモデルを訓練するために利用されるデータ。例題に対応する正解という形式に整理されている。

⑸2⑸　Kosuke Mitarai et al., “Quantum circuit learning,” *Physical Review A*, vol.98 no.3, 2018.9.10, pp.032309-1-032309-6.

されている分野も多岐にわたる。最も注目されている分野は、材料・化学分野である。材料の物性や分子の性質・化学反応について知るためには、それら材料や分子を構成する電子の状態を計算する必要がある。電子は、量子力学に従って振る舞っており、粒子数が増えると厳密な計算は指数関数的に大きな計算コストを必要とする。このような計算を古典コンピュータ上で扱うために、様々な近似法などがこれまで導入されてきた。しかしながら、依然として電子間の量子的な相関が強く、複数の電子軌道に重ね合わせ状態として電子が配置されることで安定化する分子や、基底状態だけではなく励起状態が関与してくる現象など、スパコンをもってしてもシミュレーションが難しい対象が存在する。例えば、遷移金属[53]を含んだ触媒や光機能材料などがその例である。量子コンピュータであれば量子的な重ね合わせ状態を自然に表現できるため、このような量子性が強く古典コンピュータでは計算が難しい対象であってもシミュレーションができると期待されている。触媒は、窒素固定や CO_2 の回収、再利用において重要な役割を果たしている。また、究極のエネルギー問題の解決法は光機能材料を用いた人工光合成の実現である。しかし、光反応が関与する光合成には量子コヒーレンス（重ね合わせ状態の性質）が寄与しており、その機構は未だ完全には理解されていない。このような対象に対して、量子コンピュータを用いた計算科学的アプローチからの知見を得ることによって、地球規模のエネルギー問題やカーボンニュートラルの実現に大きく貢献すると期待されている。

機械学習分野も計算リソースを多く必要とする分野であり、量子コンピュータを用いた量子機械学習が期待されている。誤り耐性量子コンピュータが実現すれば、特定の条件が満たされた場合に逆行列計算を指数関数的に高速化することができる。逆行列計算は機械学習分野における様々な用途で利用されており、量子コンピュータを用いた加速が期待される。

一方で、このような量子アルゴリズムが適用できるための前提条件（入力データが量子状態として与えられる、行列が疎（ほとんどの成分が 0）である、出力は量子状態又はそれからサンプリングされたもの）が厳しく、それらの条件の下でも優位性が残るかどうかはまだよくわかっていない[54]。入力データについては、古典的なデータを量子状態にロードする（変換して読み込む）段階で計算量を要してしまうと量子アルゴリズムによる加速効果を相殺してしまうため、データ構造の工夫や、任意のアドレスに格納されている量子状態にアクセスできる QRAM（量子ランダムアクセスメモリ）[55]などの存在を仮定する必要がある。入力状態が量子コンピュータ上で処理された量子的なデータであればこのような問題は存在しない。量子センサーや量子通信など量子 ICT インフラが整うことによって量子データも身近なものになると期待される。

これら前提条件を考慮することが重要である例を一つ紹介しておく。計算の加速が期待される量子機械学習アルゴリズムとして、量子推薦アルゴリズムが 2016 年に提案された[56]。推薦とは、過去に購入や試聴したアイテムの評価から次に購入すべきアイテムを推薦するアルゴリズムであり、ネットショッピングや動画配信システムなどで利用されている。この提案された

---

(53)　遷移金属とは、電子の d 軌道や f 軌道が閉殻（全ての準位に電子が占有）しておらず、互いに強く相関するため複雑な電子状態をとる。

(54)　Scott Aaronson, “Read the fine print,” *Nature Physics*, vol.11, 2015.4.2, pp.291-293.

(55)　アドレス i を入力するとそのアドレスに格納された情報、xiを出力する RAM に対して、QRAM は、|i>|0> を入力すると対応する量子状態を |i>|x_i> として返すようなユニタリ演算のことである。入力がアドレスの重ね合わせ状態であってもよいのが QRAM の特徴である。

(56)　Iordanis Kerenidis and Anupam Prakash, “Quantum recommendation systems,” 2016. <https://arxiv.org/abs/1603.08675>

アルゴリズムでは、行列の階数[57]が低いという性質をうまく利用して量子アルゴリズムを構成し、従来手法に対して指数関数的な計算の加速を実現している。その後、階数の低い行列であれば同様の指数関数的加速を古典コンピュータでも得られることが示された[58]。このことから分かることは、二つある。一つは、量子アルゴリズムとして動作させるための前提条件は厳しいものが多く、それを仮定すれば古典アルゴリズムも改善させることができ、その結果、古典コンピュータにおいても同様の加速が得られてしまうということである。前提条件も含めて、真に量子加速があるか慎重な検討が必要である。もう一つは、量子アルゴリズムを研究する上で、既存の古典アルゴリズムに対して新たな視点を与え、古典アルゴリズムの性能を向上させることができるという点である。近年この方向性は注目を集めており、脱量子化（de-quantization）と呼ばれている。さらに、このような脱量子化によって得られた古典アルゴリズムは量子インスパイアアルゴリズムと呼ばれている。

NISQデバイスを用いた量子機械学習の応用も期待されている。このアプローチでは、ニューラルネットワーク[59]の代わりに回路に学習可能なパラメータを導入した量子コンピュータを学習モデルとして用いることになる。また、入力データを量子回路のパラメータとすることで高次元の量子状態へと埋め込み、カーネル法[60]を適用する量子カーネル法[61]も提案されている。これらのアプローチにおいても、特定の条件において量子優位性[62]が得られる可能性が示唆されている[63]。しかし、量子ビット数が少ないため扱える入力の次元が小さいことや、パラメータを最適化するために必要となる勾配の値が小さくなってしまい、パラメータが更新できなくなる勾配消失問題など、課題も多い。

その他に、量子コンピュータの応用が期待される分野としては、金融分野が挙げられる[64]。金融分野も高速取引など計算リソースを必要とする分野である。特にオプション価格[65]を決定するためには株価などの原資産価格の振る舞いを確率モデル用いて計算する必要がある。解析的に解くことができるモデルは限られており、乱数を用いて原資産価格の振る舞いをシミュ

⑸7　行列の階数とは、その行列の列ベクトルが張る空間の次元。

⑸8　Ewin Tang, “A quantum-inspired classical algorithm for recommendation systems,” *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, 2019.6, pp.217-228. <https://doi.org/10.1145/3313276.3316310>

⑸9　ニューラルネットワークは分類タスクや汎化タスクを行う機械学習の一種であり、人間の脳を模した学習可能なパラメータを含む数理モデルである。様々なタイプのモデルが提案されているが、多層パーセプトロンモデルでは、学習可能な重みを含む線形変換と活性化関数とよばれる非線形変換を多層に繰り返した構造で出力を定義する。この出力と学習用の教師データとの誤差が小さくなるようにモデルのパラメータを学習する。

⑹0　カーネル法は分類タスクを行う機械学習の一種であり、入力データを高次元空間に移し、その高次元空間上でのデータ間の内積をカーネル関数によって与えることで分類タスクを実行する。通常のニューラルネットワークと比較するとパラメータを最適化する必要がないというメリットがある一方、データ数の次元をもつ行列の逆行列計算を実行する必要がある。

⑹1　Vojtěch Havlíček et al., “Supervised learning with quantum-enhanced feature spaces,” *Nature*, vol.567 no.7747, 2019.3.13, pp.209-212.

⑹2　量子超越性（quantum computational supremacy）が特に意味を持つタスクでなくて良い一方、機械学習や化学計算など意味を持つ計算において量子コンピュータの優位性がある場合、量子優位性（quantum advantage）と呼ぶことにする。

⑹3　Hsin-Yuan Huang et al., “Power of data in quantum machine learning,” *Nature communications*, vol.12 no.2631, 2021.5.11, pp.1-9; Yunchao Liu et al., “A rigorous and robust quantum speed-up in supervised machine learning,” *Nature Physics*, vol.17 no.9, 2021.7.12, pp.1013-1017.

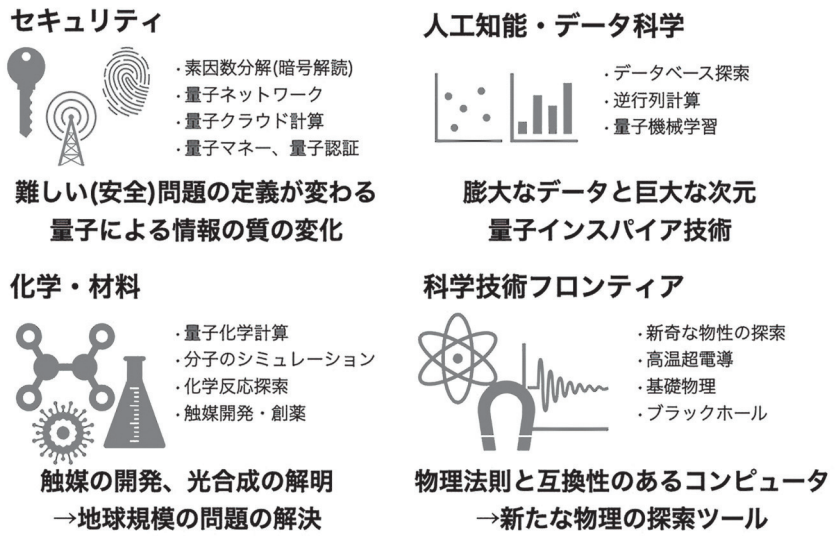
⑹4　Roman Orus et al., “Quantum computing for finance: Overview and prospects,” *Reviews in Physics*, vol.4, 2019.11, 100028.

⑹5　特定の原資産について、一定の期日（期間内）に、あらかじめ決められた数量を、あらかじめ決められた価格で、受け渡しする「権利」を「売買」する取引をオプション取引と言い、原資産のある時点における価格の期待値や金利などの要素で、現在の価値、オプション価格が計算される。

レーションするモンテカルロ計算が必要となる。量子コンピュータを用いると一般的にモンテカルロ計算を 2 乗加速することができることが知られているため、誤り耐性量子コンピュータの実現によるモンテカルロ計算の高速化が期待されている。

最後に、ここまで計算の高速化という観点から量子コンピュータの応用分野を紹介してきた。しかし、量子コンピュータは計算の高速化だけではなく計算の質を根本的に向上させることも指摘しておきたい。現在、デジタルトランスフォーメーションが加速されるなか、情報をクラウド上で蓄積し処理する利用方法が増えている。そのような中、クラウドに置かれた情報のセキュリティを、利便性を損なうことなくどのように保護するのかということが重要な課題となっている。これに対しては、量子ネットワークで接続された量子コンピュータがサーバー上にあれば、サーバーを含め第三者に一切の情報を漏らすことなく、所望の計算を実行する（委託計算）ことができる。これは、ブラインド量子計算プロトコル[66]と呼ばれ、量子コンピュータや量子ネットワークが提供する計算の質の向上の一つの例である。その他にも、改竄が原理的にできない量子マネーや量子認証システムなど、様々な量子計算暗号プロトコルが知られている。現在、ビットコインなどの暗号資産システムを支える分散型台帳技術では、ハッシュ関数（疑似乱数を生成する関数）の計算という特に意味を持たないプロセスに計算リソースを消費することが決済システムの正当性を担保するために利用されている。このように、我々が直接気づかない情報社会インフラにおいて、量子コンピュータの計算の量的優位性や質的優位性が利用される、量子情報社会インフラの実現が期待される。

図５　量子コンピュータの応用が期待される分野



（出典）筆者作成。

５　量子コンピュータハードウェア

量子コンピュータの実現のための候補として現在検討されているハードウェアの特徴及び開発状況について整理しておく。

量子コンピュータの実現に向けて最も進んでいるのは超伝導量子ビットである。低温にする

(66)　Anne Broadbent et al., “Universal blind quantum computation,” *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, 2009.

ことによって電気抵抗がなくなる超伝導と呼ばれる性質を示す特殊な材料を用いた電気回路である。このような電気回路は熱雑音が十分小さくなるくらい温度を冷やすと量子化され量子的な振る舞いをする[67]。最もエネルギーが低い基底状態と一つエネルギーの高い第一励起状態を用いて量子ビットを定義することになる。回路の構成の違いによって様々な超伝導量子ビットを構成することができ、代表的なものは、電荷量子ビット、磁束量子ビット、位相量子ビット、トランズモン量子ビットなどである。現在、超伝導量子コンピュータの構成において主流となっているのは、トランズモン量子ビットである。これらの量子ビットは、5 ～ 10GHz の周波数帯の電磁波（マイクロ波）と共鳴するため、そのような周波数帯のマイクロ波を用いて制御することになる。超伝導量子ビットの利点は、電気回路として人工的に設計ができ設計の自由度が高いという点と、超伝導が巨視的なスケールで表れる量子力学的な現象であることを利用しているために回路パターンが比較的大きくマイクロ波ケーブルの配線などがしやすいという点にある。その反面、人工物であるため、設計からの製造誤差等のため量子ビットの周波数が設計よりずれてしまうことによって、隣の量子ビットにマイクロ波が漏えい（クロストーク）するなど、量子ビット製造の歩留まりの問題もある。また、現在は希釈冷凍機[68]内にある個々の量子ビットに対してそれぞれマイクロ波ケーブルを配線している状況であり、1 万量子ビット規模への拡張はその配線の複雑さから難しい状況である。量子ビットの小型化や制御の一括化、そして量子ビットを制御するための制御デバイスを冷凍機内部に搭載するなど、拡張性・集積性を高めるブレイクスルーが必要となる。

超伝導量子ビットの次に実装が進んでいる物理系は、イオントラップ方式である。イオントラップ方式では、真空チャンバ（容器）の中にイオンを捕捉し、レーザー冷却[69]によって振動レベルが量子化されるまでイオンを冷す。このイオンの振動モード[70]と原子内部の電子状態を用いて量子計算を行う方式である。イオンの制御には、超伝導量子ビットと異なり可視光やそれより高いエネルギーの電磁波（レーザー）が利用されることが多い。イオントラップ方式の利点は、量子ビットとして利用されるイオン（原子）は自然に作られたものであり、共鳴する電磁波のエネルギーなど､どのイオンも全く同じ性質を持っている（均一性）という点にある。一方で、それらイオンを捕捉し、量子的に振る舞うまでに冷却することができるのはイオンの数が精々 100 個程度までである。このため､1 箇所に補足できるイオンの数は制限されており、拡張性において重大な問題を抱えている。この問題については、イオンを光と結合し、光を用いて異なる場所に捕捉されたイオンとの間での量子情報のやりとりを行う光結合方式や、イオンそのものを電気制御によって移動させるシャトル方式などが検討されており、その要素技術は既に実証されている。今後、これらを用いて拡張させる分散型のアーキテクチャが検討されていくと予想される。

---

(67)　有限の温度の外界と接した系は熱平衡状態となる。この熱平衡状態を特徴づける温度が十分小さい場合、外界との熱のやりとり（熱揺らぎ）が抑制される。この熱揺らぎが電気回路を構成する共振器のエネルギースケールに比べ十分小さいとき、量子的な現象を観測することができる。

(68)　液体ヘリウムの希釈熱を利用して冷却する冷凍機。超伝導量子ビットは、超伝導物質で構成された電気回路を用いているため、量子ビットが搭載されたチップを冷却する必要がある。また、量子ビットの寿命を伸ばすためには、量子ビットに共鳴するマイクロ波領域の電磁波の放射（熱輻射）を抑えるために、超伝導転移温度よりも十分に温度を下げる必要があり、10mK 程度まで冷却されている。

(69)　特定の方向に移動している原子が共鳴する光がシフトすることを利用して、レーザーを原子に照射し吸収させることで、原子の速度を低減させ冷却させる方法。

(70)　イオンの温度を十分冷やすと、イオンの振動運動が量子化されフォノンという擬似粒子として扱うことができる。

超伝導量子ビット方式、イオントラップ方式以外の候補はどれも要素技術が実現してきた段階であり、まだ計算機システムとしての量子コンピュータアーキテクチャを構成するという段階には至っていない。その中でも、いくつか将来の有望な候補として期待されている系を簡潔に紹介する。まずは、光量子ビット方式である。光は量子情報技術の黎明期から量子情報処理の媒体として研究されてきた。量子情報を離れた場所まで送る技術である量子通信を実現するためには、光を用いた量子情報処理が必須である。それに加え、光のみを用いた量子コンピュータの実装が検討されている。光を用いた量子ビットの実装は、単一光子[71]の偏光などの離散的な自由度を用いるアプローチと、光の連続的な自由度[72]に量子ビットを埋め込む方式の 2 種類が検討されている。光は他の光（光子）との相互作用が少なくノイズの要因が少ないという点が利点であるが、一方で、散乱によって光子が失われてしまう光子損失が潜在的な問題点となる。これらの問題を克服するために、光方式に特化したアーキテクチャや計算モデル（測定型量子計算）の採用が検討されている。次に、半導体量子ビットも古くから量子ビットの有力な候補として様々な方式が研究されてきた。特に、既存の半導体技術の転用が可能であり、高集積化については優位性がある。一方で、現在数量子ビットに対して高忠実度で制御することが可能となってきているが[73]、拡張性を担保しつつ高い忠実度で制御する方法を確立することは今後の課題である。このほか、最近では光格子[74]に捕獲された冷却原子を用いたアプローチも登場している[75]。

依然として、100 万量子ビット規模の量子コンピュータを可能とする実装方式がどの物理系であるかを予想することは難しく、これら様々な物理系が並行して開発されていくことが予想される。また、超伝導、イオントラップ、光といった、量子ビットを実現するための物理系に注目が集まることが多いが、これら量子ビットを制御するためにはマイクロ波技術、レーザー技術などのアナログ技術に加え、それらを制御する周辺エレクトロニクスなどのミドルウェア技術、それらを統合して量子デバイスと古典制御装置の接続をうまく制御するコンピュータアーキテクチャの設計も重要である。

6　量子コンピュータソフトウェア開発環境

小規模な量子コンピュータ実機が利用できるようになる中、量子コンピュータのソフトウェア開発環境（Software Development Kit: SDK）がオープンソースソフトウェアを中心に整備されつつある。特に幅広く様々な機能を備えるものは、IBM が提供する Qiskit[76]である。Qiskit には、用途ごとに分離されたモジュールが用意されており、アプリケーションライブラリの Aqua、古典コンピュータを用いた高速シミュレーションを行う Aer、ノイズの特徴づけやノイズ補償などのためのモジュール Ignis、そして実機実行や実機制約を満たすように回路を分解

⑺1⑻　光子とは光（電磁波）を量子力学的に記述したときに現れる粒子的描像。

⑺2⑻　電磁波を量子力学的に扱うと無限の次元の量子系（調和振動子）として定式化される。この結果、コヒーレント状態などに代表されるような連続的な値をもつ量子状態（連続的な自由度）として量子化された電磁波が記述される。

⑺3⑻　理化学研究所ほか「シリコン量子ビットで高精度なユニバーサル操作を実現―誤り耐性シリコン量子コンピュータの実現に指針―」2022.1.20. <https://www.riken.jp/press/2022/20220120_1/>

⑺4⑻　十分冷却された原子を対向するレーザーによって作り出される定在波によって格子状に捕獲した状態。

⑺5⑻　Sepehr Ebadi et al., “Quantum phases of matter on a 256-atom programmable quantum simulator,” *Nature*, vol.595 no.7866, 2021.7.7, pp.227-232.

⑺6⑻　Qiskit.org website <https://qiskit.org>

するモジュール Terra が用意されている。また、超伝導量子コンピュータの量子ゲートをパルスレベルで制御するための OpenPulse、デバイス設計をするための Qiskit Metal なども存在し、ハードウェア設計からアプリケーションに至るまで垂直統合されたライブラリ群を提供している。一方、Google は、量子回路を実機で実行するためのフレームワークCirq[77]を提供している。また、Google が提供する機械学習ライブラリ TensorFlow と統合された量子古典ハイブリッド機械学習ライブラリ TensorFlow Quantum[78]も提供している。また、Xanadu からも PennyLane[79]という量子機械学習ライブラリが提供されている。アマゾンウェブサービス（AWS）は、複数のハードウェアをクラウド環境で利用できる Amazon Braket[80]というフルマネージドサービスを展開している。Amazon Braket 独自の SDKも提供しており、AWS 上で利用可能な実機での量子回路の実行や、Amazon Braket で PennyLane を利用するためのプラグインなどが提供されている。ここでは触れないが、上記以外にも複数の量子プログラミング環境やアプリケーションライブラリが存在し、利用可能なハードウェアの種類やシミュレータも複数ある。CQ（Cambridge Quantum）は、多数のフロントエンド（プログラミング言語･環境）とバックエンド（ハードウェア、シミュレータ）に対応した汎用コンパイラとして tket[81]を提供している。

様々な量子コンピュータ実機が利用可能になりつつあるものの、利用できる量子ビット数が制限されていたりノイズレベルが依然として高いなど、課題も多い。そのような中、既存のコンピュータで構築されるシミュレータを用いたソフトウェア開発がますます重要になっている。このような背景から上記の SDK のほとんどは独自のシミュレータバックエンドを提供している。また、我が国からは、量子回路の高速シミュレーションに特化したライブラリ Qulacs[82]がオープンソースとして提供されており、Python[83]インターフェースを持つオープンソースソフトウェアの量子コンピュータシミュレータとして世界最速の性能を誇る。Cirq、PennyLane、tket などの SDK から高速バックエンドとして利用することができる[84]。

上記の SDK は、主に NISQ デバイスの利用を目的としたものである。一方で、長期的目標である誤り耐性量子コンピュータは、ハードウェアからアプリケーションに至るまで NISQ デバイスよりも複雑な階層構造を持つ。これは量子誤り訂正というプロセスがハードウェアとアプリケーションの間に挿入されているため、上位レイヤー（アプリケーション）及び下位レイヤー（ハードウェア）をうまく誤り訂正と接続する必要があるためである。上記の、NISQ 向けライブラリの一部は利用できるかもしれないが、誤り耐性量子コンピュータの設計思想は NISQ のそれとは根本的に異なり、誤り耐性量子コンピュータ用の SDK 開発も今後必要となってくると予想される。誤り耐性量子コンピュータの実現は、コンピュータを根本的に新しく作り直す試みであり、コンピュータアーキテクチャ分野やソフトウェア工学分野の研究者の参入がますます求められている。

---

(77)　Google Quantum AI website <https://quantumai.google/cirq>
(78)　TensorFlow website <https://www.tensorflow.org/quantum?hl=ja>
(79)　Pennylane.ai website <https://pennylane.ai>
(80)　Rigetti、IonQ、D-Wave が開発に当たった。「Amazon Braket 量子コンピュータ」Amazon Web Services website <https://aws.amazon.com/jp/braket/quantum-computers/>
(81)　“CQCL / pytket.” GitHub website <https://github.com/CQCL/pytket>
(82)　“qulacs / qulacs.” *ibid.* <https://github.com/qulacs/qulacs>
(83)　広く普及しているプログラミング言語。
(84)　cirq のバックエンドとして、“qulacs / cirq-qulacs.” GitHub website <https://github.com/qulacs/cirq-qulacs>、pennylane のバックエンドとして、“PennyLaneAI / pennylane-qulacs.” *ibid.* <https://github.com/PennyLaneAI/pennylane-qulacs>、tket のバックエンドとして、“CQCL / pytket,” *op.cit.*(81)が提供されている。

おわりに

ここまで、量子コンピュータを取り巻く状況を俯瞰すべく、歴史的経緯、量子コンピュータの仕組み、量子アルゴリズム、量子コンピュータの応用分野、量子コンピュータハードウェア、量子ソフトウェア開発環境について解説を行ってきた。量子コンピュータ研究は、物理学分野における基礎研究から、新原理のコンピュータシステムを作るという、もの作りへと急激にシフトしつつある。ただし、これまでのもの作りと異なる点は、高度な専門知識と分野横断型の視点が求められている点である。このため、各国がこぞって国として量子コンピュータの研究開発の加速や産学連携体制の整備を行い、新規のベンチャー企業も増えている状況である。このような中、当分野では我が国だけでなく世界的に深刻な人材不足となっている。量子コンピュータは全く新しくコンピュータを作り直す取組であり、その応用まで考えると、数学、情報、量子物理、半導体、光、化学、生物など多くの分野にまたがった分野融合的な研究を進めていく必要がある。また、研究者だけではなく、量子コンピュータ開発を支える開発者、そして量子コンピュータを利用するプログラマー、アプリケーションのユーザの育成も重要となる。そのような人材を輩出する大学においては、量子コンピュータに関連する分野を体系的に学ぶことができるカリキュラムの策定、研究室の拡充、学科・研究科などの設置が喫緊の課題である。また、そこで育った人材のキャリアパスの道の確立も優秀な人材を集めるためには必須である。既に関連する分野の専門性のある人材に門戸を開き、研究・開発の裾野を広げていくことも重要である。まさに、新たな産業として量子コンピュータを位置付け、全方位的に力強く推進していくことが不可欠である。また、このような高度な専門知識と分野横断型のエマージングな技術によるイノベーションの機会は量子以外の分野でも今後到来することが予想される。そのような時に、量子分野における取組が力強い模範となることを期待したい。

執筆：大阪大学大学院基礎工学研究科システム創成専攻電子光科学領域教授　藤井（ふじい）　啓祐（けいすけ）

コラム　論文データベースから見る量子コンピュータ研究開発の動向

1　目的

本コラムで扱う量子コンピュータは、2010 年代に入ってから急速な研究開発の進展があった。この進展の概要を定量的に把握し、本編での定性的な動向把握への補足情報を与えることが本コラムの目的である。なお、本稿は筆者の研究成果[(1)]をもとに、政策関係者の判断に直接的に資すると思われる部分を抽出し、用語や定義の説明の追加及び上記研究で説明を省いた分析の加筆を行ったものである。

2　手法

本項では、上記目的を達成するため、クラリベイト社が提供する論文データベース Web of Science Core Collection（以下「Web of Science」）を用いた論文データ分析を行った。手順は以下のとおりである。

① データベースからの対象論文の抽出
② データクリーニング
③ 要約統計量の抽出
④ クラスター分析によるトピック抽出

以下、各ステップの概要を説明する。まず、論文情報抽出のために以下の検索式を構成した。

> (“quantum computer” OR “quantum computing” OR “quantum compute” OR “quantum computers” OR “quantum algorithm” OR “quantum algorithms” OR “quantum inspired”) NOT (“post-quantum” OR “quantum resistant” OR keywords:cryptography OR “quantum key” OR conscious* OR brain OR dream OR QTAIM)

この検索式は、米国の Farinholt による検索式[(2)]を参考に、量子コンピュータ及び量子アルゴリズムに関係があるが、量子暗号やポスト量子暗号などの周辺分野には関係がない論文を抽出することを意図して作成した。Farinholt の検索式との違いは量子インスパイアドアルゴリズム[(3)]の取扱いにある。Farinholt が量子インスパイアドアルゴリズムを抽出対象外としたのに対し、本項では量子インスパイアドアルゴリズムも量子コンピュータ研究の有用な副産物であるとの立場に立ち、抽出対象としている。この検索式の Web of Science データベースへの適用の結果、14,450 報の論文を抽出した。なお、抽出日は 2021 年 3 月

＊　本稿におけるインターネット情報の最終アクセス日は、令和 4 年（2022）年 1 月 7 日である。

(1)　Tsubasa Ichikawa, “Bibliometric analysis of topic structure in quantum computation and quantum algorithm research,” *arXiv*, 2022.01911, January 2022. <https://arxiv.org/abs/2201.01911>

(2)　Jacob Farinholt, “Trends in Quantum Computing,” October 2019. ResearchGate website <https://www.researchgate.net/publication/336341290_Trends_in_Quantum_Computing>

(3)　量子計算や量子ビットの振る舞いを模倣したアルゴリズムの総称。量子ビットとは量子コンピュータにおける基本素子のこと。通常のコンピュータにおける基本的な素子であるビットは 0 と 1 の二つの状態のいずれかをとるのに対し、量子ビットでは 0 と 1 を重ね合わせた状態をとることが許される。

26 日であった。

データクリーニングでは上記抽出論文のうち、著者名が記載されている 2020 年 12 月 31 日までに出版された論文 14,085 報をさらに抽出した。

データの特徴を示す要約統計量は、各年の出版論文数及び論文一報当たり年間平均引用数などを計算した。なお、引用数は Web of Science データベース収録の引用数を用いており、他のデータベースにおける引用数とは必ずしも一致しないことに注意されたい。

クラスター分析は、要約統計量の推移をもとに 2014 年から 2020 年までの出版論文を対象に行った。各論文の参考文献リストの共通度をジャッカード係数[4]により評価して書誌結合ネットワーク[5]を構成し、Louvain 法[6]を用いてクラスタリングを行った。論文数の多い 14 のクラスターについては、アブストラクトに記載されている単語をその頻度に応じた大きさで図示したワードクラウドを作成し、トピックの判定を行った。

3　結果

(1) 1985 年から 2020 年までの論文数及び平均引用数の動向

出版論文数の年次推移は図 1 のとおりである。論文数の推移からは、量子コンピュータ研究はおおよそ三つの期間に分けられることが分かる。すなわち、1985 年から 2003 年までの論文数が増加する時期（草創期）、2004 年から 2013 年までの論文数がおおよそ一定であった時期（成熟期）、そして 2014 年から 2020 年までの論文数が再度増加した時期（急進期）である。

各時期の端境には影響力の大きい論文が観察できる。1985 年には Deutsch により量子チューリングマシンの概念が提案され[7]、量子コンピュータが理論的にも整備された形

(4)　ジャッカード係数は、二つの論文に共通して登場する参考文献の数を、二つの論文の総参考文献数（重複を除く）で除したもの。より正確には、論文 i の参考文献の集合を r_i とするとき、論文 i と論文 j とのジャッカード係数 $w(i, j)$ は

$$w(i, j)=\frac{|r_i \cap r_j|}{|r_i \cup r_j|}$$

で与えられる。ここで $|r_i|$ は集合 r_i の要素数である。二つの集合の共通する要素からなる集合を $r_i \cap r_j$ とおき、二つの集合の少なくとも一方に属する要素からなる集合を $r_i \cup r_j$ とおいた。

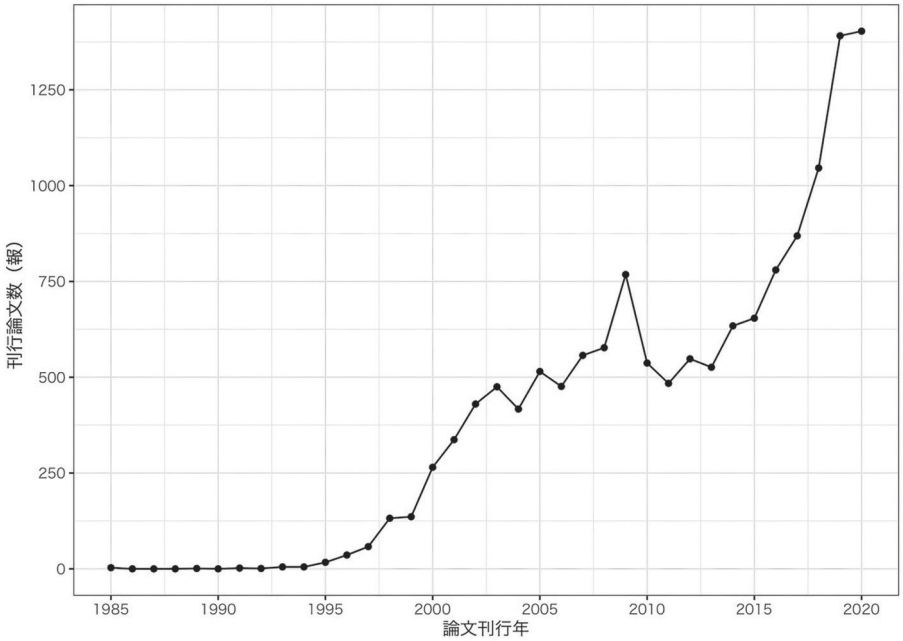
(5)　論文を頂点とし、ジャッカード係数などで辺を定義した重み付き無向グラフのこと。初出は M. M. Kessler, “Bibliographic coupling between scientific papers,” *American Documentation*, vol.14 no.1, January 1963, pp.10-25. <https://onlinelibrary.wiley.com/doi/epdf/10.1002/asi.5090140103>

(6)　Vincent D. Blondel et al., “Fast unfolding of communities in large networks,” *Journal of Statistical Mechanics*, vol.2008 no.10, October 2008, P10008. <https://iopscience.iop.org/article/10.1088/1742-5468/2008/10/P10008/pdf>

(7)　量子チューリングマシンとは、万能チューリングマシンを量子力学系に拡張したもの。量子チューリングマシンを説明するにはいくつかの概念を導入する必要がある。まず、チューリングマシンを導入する。チューリングマシンとは、無限に延長可能なテープ・テープヘッダ・有限制御部からなる仮想的な機械である。テープには一次元的にマス目が連なっており、それぞれのマス目には 0、1、B（「空欄」を意味する英単語 Blank の頭文字）のいずれかが書き込まれている。テープヘッダはマス目に書いてある記号を読み取り、有限制御部に書いてある指示に従って記号を書き換える。テープヘッダは記号の書き換えの後、隣接するマス目に移動して記号を読み取り、有限制御部に書いてある指示に従った書き換えを行う。この一連の書き換えが計算に対応している。有限制御部に書いてある指示書きが異なるチューリングマシンは、それぞれ相異なる計算に対応する。万能チューリングマシンは任意のチューリングマシンの振る舞いを模倣できるチューリングマシンのこと。（通常のコンピュータで）計算可能な関数は万能チューリングマシンで計算できる関数に限られると仮定されている（チャーチ＝チューリングのテーゼ）。すなわち、端的にいえば、万能チューリングマシンはコンピュータを用いた計算の理論基盤を与えるモデルであるといえる。量子チューリングマシンは量子力学的な特徴を考慮に入れて、万能チューリングマシンをさらに拡張したものであり、量子コンピュータの理論基盤を与えるモデルである。初出は以下の論文。チャーチ＝チューリングのテーゼについてもこの論文に言及がある。David Deutsch, “Quantum theory, the Church-Turing principle and the universal quantum computer,” *Proceedings of the Royal Society A*, vol.400 no.1818, July 1985, pp.95-117.

で提案された。2003 年には Kitaev により、量子誤り訂正[8]プロトコルの一つであるトーリック符号の論文が出版された[9]。また、2014 年には Martinis のグループにより誤り耐性量子コンピュータを実装するためのエラー閾値を下回るエラー率を持つ量子ビットが実験的に作成[10]された。また、同年には NISQ アルゴリズム[11]の一つである変分量子アルゴリズムが提案[12]されている。このように、文字どおり画期となる研究の影響を受けつつ、量子コンピュータ研究は進んできたといえる。

図 1　1985 年から 2020 年までの出版論文数の推移



（出典） 筆者作成。

図 2 に示した論文一報の年当たり平均引用数の年次推移を示すデータの振る舞いからは、2000 年以前の基盤的な研究をもとに、現在では成熟した引用関係が構築されていることを読み取ることができる。時系列に従って図を読み解いていこう。1985 年の特異的な振る舞いは、この年の出版論文が 3 報と少ないことと、そのうちの 1 報が前述の Deutsch の引用数の高い論文であることで、平均値が高留まりしていることによる。1995 年から 1999 年までの

(8)　通常のコンピュータにおける基本的な素子はビット（0 と 1 の二つの状態のいずれかをとる計算単位）であるのに対し、量子コンピュータでは 0 と 1 を重ね合わせた状態を許す量子ビットが素子となる。計算の途中で、環境系からのノイズなどの影響により、量子ビットの状態が、ノイズのない理想的な場合と異なってしまう場合がある。量子誤り訂正とは、計算単位となる量子ビットを増やすことにより量子ビットへの情報のエンコーディングに冗長性を持たせ、ノイズの影響がある場合でもその影響を訂正し、理想的な場合と同様の計算結果を量子コンピュータから出力させるための手法である。

(9)　A. Yu. Kitaev, “Fault-tolerant quantum computation by anyons,” *Annals of Physics*, vol.303 no.11, January 2003, pp.2-30. プレプリントは 1997 年に公開。

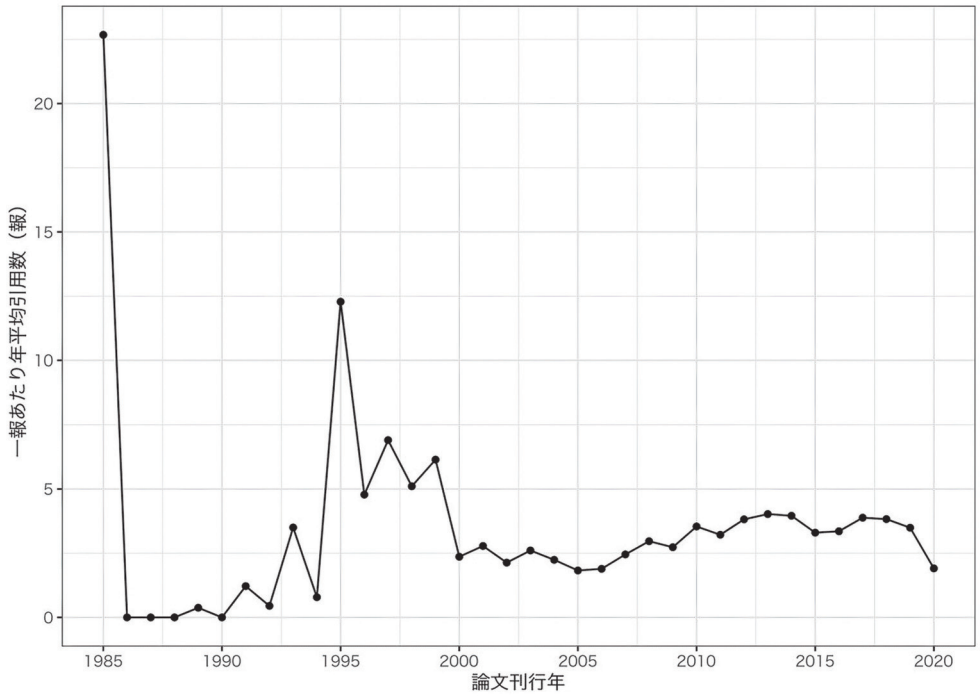
(10)　R. Barends et al., “Superconducting quantum circuits at the surface code threshold for fault tolerance,” *Nature*, vol.508, April 2014, pp.500-503. <https;//doi:10.1038/nature13171>

(11)　NISQ は Noisy, Intermediate-Scale Quantum の頭文字を取ったもの。ノイズ影響下の中規模量子コンピュータで実行可能なアルゴリズムを NISQ アルゴリズムという。日本語での定訳はなく、そのまま NISQ と書くのが通例である。

(12)　Alberto Peruzzo et al., “A variational eigenvalue solver on a photonic quantum processor,” *Nature Communications*, vol.5 no. 4213, 23 July 2014.

出版論文も他の年に比べて論文一報の年当たり平均引用数が高い。これは、グローバーのアルゴリズム（Grover's Algorithm）や CSS 符号（Calderbank-Shor-Steane code）といった長期にわたり量子コンピュータの理論基盤となる研究がなされた時期[13]であり、これらの研究が多く引用されていることによると思われる。2000 年以降は論文一報の年当たり平均引用数は漸増の傾向にあり、2014 年以降はほぼ一定となっている。2000 年以降の振る舞いからは 2020 年について論文一報の年当たり平均引用数の減少が読み取れるが、これは論文が引用される典型的な期間（数年程度）に比較して出版後の経過期間が短いため、平均値が収束していないことによると思われる。

図２　1985 年から 2020 年までの論文一報当たり年平均引用数の推移



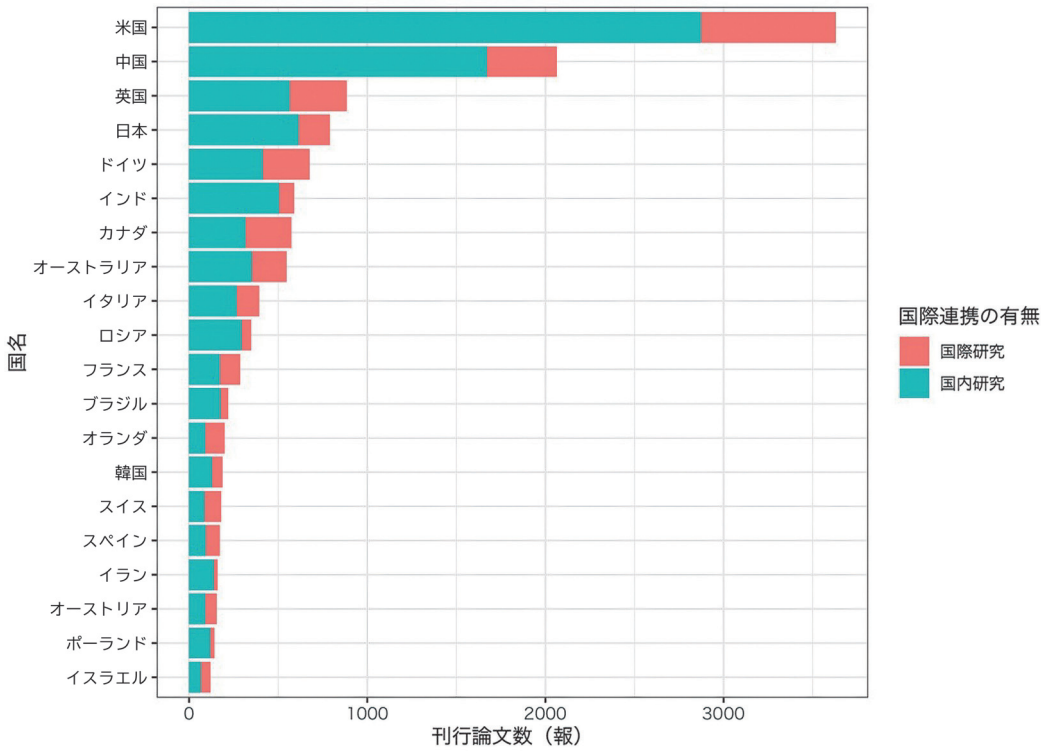
（出典）筆者作成。

(2) 1985 年から 2020 年までの各国の動向

図 3 は各国の総論文数を集計したものである。米中が他国を引き離しており、我が国は英国に続き、総論文数は第 4 位である。一方で、英米中独などに比べて我が国は多国間研究の割合が少ないことが示唆される。

(13)　この時期の代表的な研究をまとめた教科書に Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000 がある。

図３　1985 年から 2020 年までの各国の出版論文数



（注）　積み上げ横棒グラフのうち、青い横棒は国内グループ研究での出版論文数を、赤い横棒は国際グループ研究での出版論文数を表している。なお、筆頭著者の所属機関の所在国で論文の分類を行った。
（出典）筆者作成。

各国の論文の引用動向を表 1 にまとめた。総引用数では上位 3 か国は米国・英国・ドイツである。中国は論文数に比較して引用数が低いことが分かる。また、平均引用数では上位 3 か国はオーストリア・オランダ・デンマークである。総引用数及び平均引用数の定義は表 1 の注をご覧いただきたい。このように引用数から誘導される指標で集計した場合、欧米各国、特にアングロサクソン諸国と中欧諸国が量子コンピュータ研究を長期的に牽引してきたことが見てとれる[14]。

(14)　平均引用数上位 3 か国が本文記載の 3 か国であることには三つの要因が考えられる。一つ目の要因は、この 3 か国は総論文数が比較的少数であることである。平均引用数は、一般に引用数が多くなり、通常論文に対して外れ値的な傾向を持つ総説論文などの影響を受けやすいため、総論文数が少ないと、総説論文の影響を受け、平均引用数が大きめに出る可能性がある。二つ目の要因は、インスブルック大学（オーストリア）、デルフト工科大学（オランダ）、ニールス・ボーア研究所（デンマーク）など、量子科学技術研究を牽引してきた研究機関が所在することが考えられる。三つ目の要因はこの 3 か国が量子力学の構築への貢献が大きい国であることである。具体的には、シュレーディンガー（Erwin Schrödinger. オーストリア）、エーレンフェスト（Paul Ehrenfest. オランダ）、ボーア（Niels Bohr. デンマーク）などの量子力学の創設者達をこの 3 か国は輩出している。この歴史的事情が上記研究機関の量子科学技術推進に当たっての文化的背景となっていることが考えられる。

表 1　1985 年から 2020 年までの各国の総引用数及び論文一報当たり平均引用数

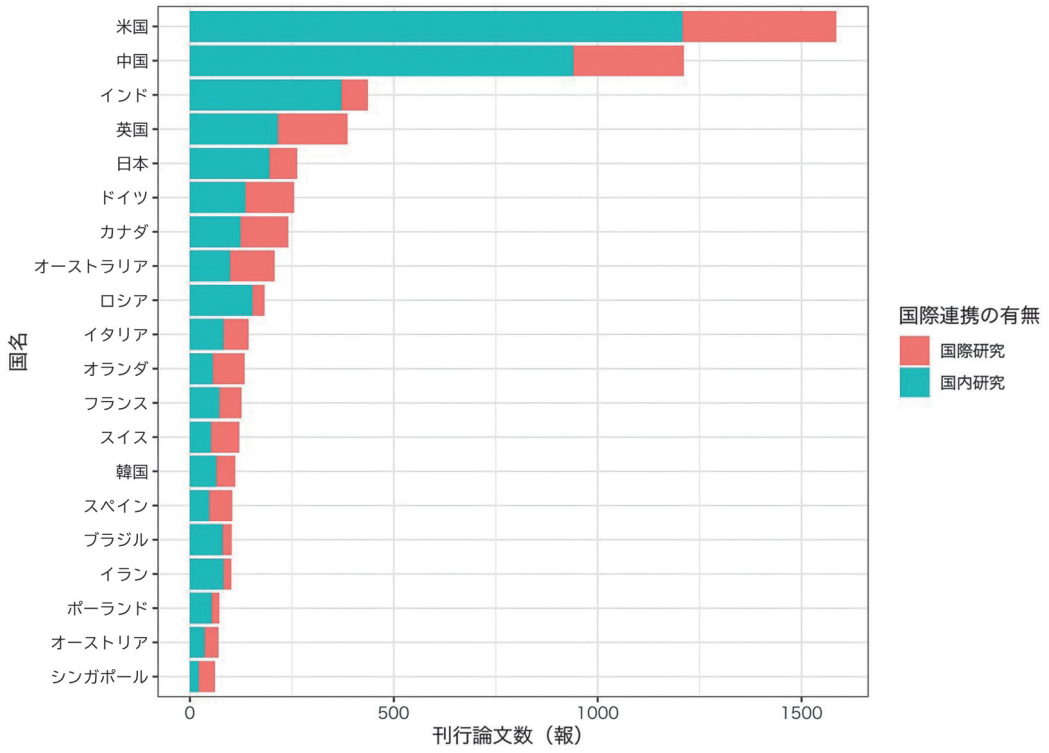
No.	国名	総引用数	平均引用数	No.	国名	総引用数	平均引用数
1	米国	158,397	43.6	11	フランス	7,137	24.9
2	英国	34,715	39.3	12	イタリア	6,480	16.4
3	ドイツ	26,982	39.9	13	イスラエル	5,928	49.4
4	中国	25,769	12.5	14	スペイン	5,223	30.2
5	オーストラリア	22,160	40.4	15	デンマーク	4,250	51.8
6	カナダ	19,237	33.4	16	ロシア	3,742	10.7
7	日本	15,455	19.5	17	インド	3,423	5.8
8	オランダ	11,747	58.4	18	韓国	3,418	18.2
9	オーストリア	10,502	67.3	19	ブラジル	2,729	12.5
10	スイス	8,515	47.0	20	ベルギー	1,515	28.1

（注 1）　対象国は 1985 年から 2020 年までの総引用数上位 20 か国。
（注 2）　総引用数は 1985 年から 2020 年までの対象国の出版論文の引用数の和。
（注 3）　平均引用数は上記総引用数を対象国の対象期間における出版論文数で除したもの。
（出典）　筆者作成。

(3) 2014 年から 2020 年までの各国の動向

前述の量子コンピュータ研究の長期的動向を踏まえ、2014 年から 2020 年までの各国の動向を観察する。各国の総論文数の動向を図 4 にまとめた。米中が他国を引き離していることは長期動向と変わらないものの、米中の差は図 3 から読み取れる差よりは縮まっている。我が国は英国に続き、総論文数は第 5 位である。これはインドが第 3 位になったことにより、日英の順位が下がったことによる。このように、2014 年から 2020 年は総論文数では中国及びインドなど、アジア諸国の台頭が注目される。

図 4　2014 年から 2020 年までの各国の出版論文数



（注）　積み上げ横棒グラフのうち、青い横棒は国内グループ研究での出版論文数、赤い横棒は国際グループ研究での出版論文数を表している。なお、筆頭著者の所属機関の所在国で論文の分類を行った。
（出典）　筆者作成。

2014 年から 2020 年までの各国の論文の引用動向を表 2 にまとめた。総引用数では上位 3 か国は米国・中国・英国である。中国が総引用数でも米国を追随する立ち位置についたことが分かる。また、平均引用数では上位 3 か国はデンマーク・南アフリカ・オーストリアである。南アフリカは、クワズールナタール大学に量子機械学習の有力研究者[15]が在籍しており、このことが NISQ パラダイムにおいて研究推進に有効に作用していると思われる。このように引用数から誘導される指標で集計した場合、中国・インド・南アフリカなどの新興国の台頭が特徴的である。

表２　2014 年から 2020 年までの各国の総引用数及び論文一報当たり平均引用数

No.	国名	総引用数	平均引用数	No.	国名	総引用数	平均引用数
1	米国	26,466	16.70	11	オーストリア	1,729	24.70
2	中国	11,481	9.48	12	スイス	1,717	14.19
3	英国	6,222	16.08	13	イタリア	1,488	10.33
4	オーストラリア	4,563	21.94	14	スペイン	1,357	13.05
5	ドイツ	4,015	15.75	15	デンマーク	1,339	38.26
6	日本	3,862	14.68	16	ロシア	905	4.95
7	オランダ	3,023	22.56	17	南アフリカ	783	27.00
8	カナダ	3,015	12.51	18	韓国	580	5.23
9	インド	1,798	4.12	19	スウェーデン	550	14.47
10	フランス	1,733	13.75	20	イラン	497	4.92

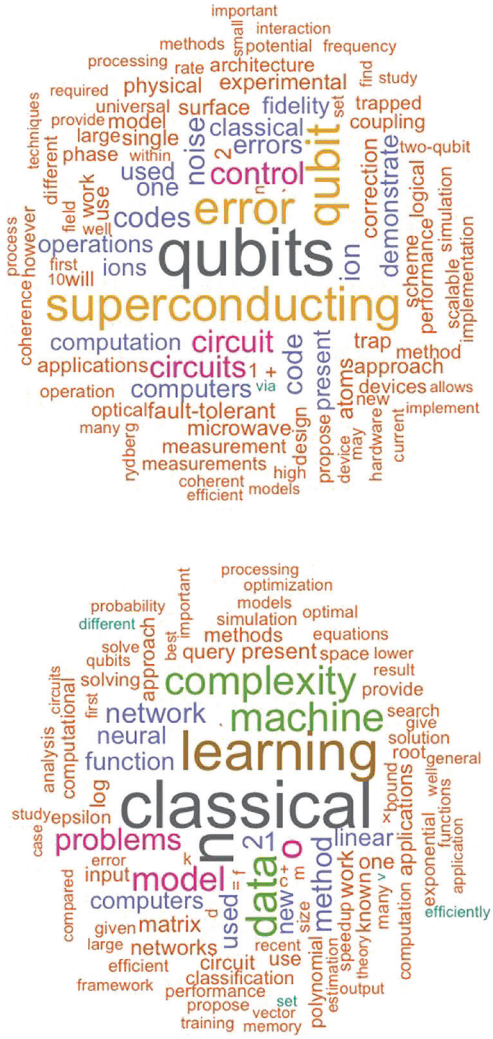
（注 1）　対象国は 2014 年から 2020 年までの総引用数上位 20 か国。
（注 2）　総引用数は 2014 年から 2020 年までの対象国の出版論文の引用数の和。
（注 3）　平均引用数は上記総引用数を対象国の対象期間における出版論文数で除したもの。
（出典）　筆者作成。

(4) 2014 年から 2020 年までの主要研究トピック

ここでは、2014 年から 2020 年までに出版された論文 6,777 報について、その主要研究トピックを紹介する。まず、クラスター分析の結果を述べる。クラスター分析では、論文 6,777 報を 911 個のクラスターに分類することができた。このうち、100 報以上の論文からなるクラスター 14 個を主要クラスターと定義し、各クラスターの主要トピックを同定した（図 5）。また、結果を表 3 に示す。

(15)　Maria Schuld 及び Francesco Petruccione など。

図５　主要クラスターにおける頻出単語の WordCloud の例。
超伝導量子ビットのクラスター（上）
及び量子機械学習のクラスター（下）



（注）　単語の表示の大きさは、該当単語のアブストラクトにおける出現頻度に応じて調整されている。
（出典）　筆者作成。

主要 14 トピックで 5,797 報の論文がカバーされており、これは全論文数の約 85.5% に相当する。また、研究対象となる量子コンピュータの方式[16]に注目すると、各トピックを以下 3 グループに分類することができる。

①　ゲート方式に関するトピック　　（13 トピック・4,670 報・68.9%）
②　イジング方式に関するトピック　　（1 トピック・270 報・3.98%）

(16)　量子コンピュータの実装方式には大きく分けてゲート方式とイジング方式の二つの方式がある。通常の計算機科学における回路モデルでは、ゲートと呼ばれる基本的な演算（AND 演算や NOT 演算など）から構成される回路によって計算過程を記述するのと同様、量子ゲート方式では、量子ビットに作用させる操作を量子ゲート（通常の計算機科学におけるゲートに対応する量子操作、厳密にはユニタリ変換）・量子ビットに対する測定・測定結果に依存した量子操作の組み合わせによって構成される回路として表現する。ゲート方式は回路を上手く構成すれば量子力学で許される任意の（ユニタリ）変換を良い精度で模倣できることが知られているため、さまざまな量子アルゴリズムを実装することが理論的には可能である。一方で、イジング方式は組み合わせ最適化問題の求解に特化した実装方式である。イジング方式では、組合せ最適化問題をイジングモデルと呼ばれる物理系に置き換え、その最低エネルギー状態を求め、当初の組合せ最適化問題の解に読み替えることで問題を解く。

③　量子コンピュータの関連トピック（4 トピック・827 報・12.2%）

このように、2014 年から 2020 年までについても主要研究トピックの多くはゲート方式量子コンピュータに関するものであり、関連分野と相互に影響を与え合いながら研究が進展しているといえる。

本調査の対象であるゲート方式に関するトピックに注目すると、各トピックを以下 3 グループに分類することができる。

①　ハードウェア、特に量子ビット実装に関するトピック（No.1, 7, 11, 13・1,630 報・24.1%）

②　ハードウェア、特に量子ゲート実装に関するトピック（No.2, 6・1,268 報・18.7%）

③　ソフトウェアに関するトピック（No.3, 4, 5・1,772 報・26.1%）

このように、量子コンピュータ研究では基本素子である量子ビットの実装、基本操作である量子ゲートの実装、及びその応用としてのソフトウェア開発がバランス良く研究されていることが分かる。特にソフトウェア研究では、近年の AI の興隆に触発された量子機械学習が独立したトピックを構成していることが特徴的である。

表３　2014 年から 2020 年までの主要研究トピック

No.	論文数	分類	主要研究トピック
1	895（13.2%）	ゲート方式	低エラー量子ビットの製造・利用。特に超伝導量子ビット
2	838（12.4%）	ゲート方式	光量子コンピューティング・ボゾンサンプリング等及びその基盤技術
3	760（11.2%）	ゲート方式	量子アルゴリズム一般。特に画像処理などへの応用
4	547（8.07%）	ゲート方式	量子シミュレーション（量子化学・ゲージ理論・製薬等）
5	465（6.86%）	ゲート方式	量子機械学習
6	430（6.34%）	ゲート方式	トポロジカル物質・トポロジカル量子計算
7	388（5.73%）	ゲート方式	シリコン量子ビット
8	346（5.11%）	関連研究	量子インスパイアドアルゴリズム
9	270（3.98%）	イジング方式	断熱量子計算・量子アニーリング
10	219（3.23%）	関連研究	可逆回路の構成・実装
11	206（3.04%）	ゲート方式	ダイヤモンド窒素 - 空孔中心（NV センター）量子ビット
12	148（2.18%）	関連研究	耐量子計算暗号（格子暗号など）
13	141（2.08%）	ゲート方式	分子スピン量子ビットの生成・操作
14	114（1.68%）	関連研究	量子ウォーク

（注 1）　比率は 2014 年から 2020 年までの総論文数 6,777 報に対するもの。
（注 2）　量子コンピュータを直接の研究対象とはしないが、量子コンピュータに関連する研究トピックを「関連研究」と定義した。
（出典）　筆者作成。

４　まとめ

本コラムでは、データに基づいて量子コンピュータ研究の現状を確認した。2014 年から 2020 年までが研究の拡大期に入っており、新興国のプレゼンスも拡大していることが分かった。また、研究トピックについてはゲート方式が主要なものであり、ハードウェア及びソフトウェアの研究がバランスよく行われている。特に、量子機械学習などの新興トピックは、独立したトピックとなるほど急速に成長している。

執筆：大阪大学量子情報・量子生命研究センター（QIQB）特任准教授　市川（いちかわ）　翼（つばさ）

Ⅱ　量子シミュレータ

はじめに

量子技術の著しい進歩により、原子、分子、イオン、電子、光子といった量子力学に従う極微の粒子を高い精度で制御し、更に測定することが可能となっている。量子シミュレータ（量子シミュレーション）は、古典計算機では解くことのできないような物理や化学の難問を、これらの粒子をプラットホームとした模擬実験を通して非常に効率よく調べようとする研究開発の総称である(1)。高温超伝導(2)や量子磁性(3)など物質が示す新奇な性質や複雑な化学反応機構を始め、高エネルギー物理や天体物理までもの諸問題が量子シミュレータを用いて解明できると考えられている。また、量子シミュレータでは、新物質の設計探索、高機能デバイスの開発、更には新薬開発などの幅広い応用も期待されており、世界各国の量子情報技術戦略においてメインターゲットの一つになっている。本節では、量子シミュレータの概要及びその研究開発動向について説明する。

1　量子シミュレータと量子コンピュータ

制御性に優れた量子系を使った模擬実験で物理や化学の未解明の問題を効率よく調べようとする量子シミュレータのアイデアは、米国の著名な理論物理学者リチャード・ファインマン（Richard P. Feynman）によって 1981 年に初めて提案された(4)。量子効果を使って問題を解くといった点では、量子シミュレータも量子コンピュータの範疇に含まれると考えられる。ただし、図 1 が示すように量子シミュレータと量子コンピュータでは演算過程に違いがある。量子シミュレータでは解明したい問題に合わせて実験パラメータ（電場、磁場、レーザー光の強度や波長など）を制御し、量子状態を連続的に時間変化させて演算（すなわちシミュレーション）を実行するのに対して（図 1(a)）、量子コンピュータでは量子ゲート操作に基づいてデジタル的に演算を実行する（図 1(b)）。量子シミュレータのデジタル化されていない連続的な演算プ

＊　本稿におけるインターネット情報の最終アクセス日は、令和 4（2022）年 2 月 15 日である。

(1)　I. Buluta et al., “Quantum Simulators,” *Science*, Vol.326 Iss.5949, 2009.10.2, pp.108-111. また、量子シミュレータに関する最近の総合解説として、Ehud Altman et al., “Quantum Simulators: Architectures and Opportunities,” *Physical Review X Quantum*, Vol.2, 2021.2.24. pp.017003-1-017003-19. <https://doi.org/10.1103/PRXQuantum.2.017003>

(2)　高温超伝導とは文字通り高い温度で実現する超伝導のことであるが、現在では応用の観点から、寒剤として広く一般的に使用されている液体窒素の沸点（1 気圧下で -196℃）よりも高い温度で実現する超伝導を指すことが多い。高温超伝導を示す物質としてよく知られているのが、1986 年に IBM チューリッヒ研究所のヨハネス・ゲオルク・ベドノルツ（Johannes Georg Bednorz）とカール・アレクサンダー・ミュラー（Karl Alexander Müller）によって発見された銅酸化物である。この発見を契機として数多くの研究機関で銅酸化物の材料探索が行われ、1993 年には水銀系銅酸化物が大気圧下ではこれまで報告された中で最も高い温度（-140℃）で超伝導状態になることが示された。液体窒素の沸点をはるかに超える高温での超伝導は 1957 年米国の物理学者 ジョン・バーディーン（John Bardeen）、レオン・クーパー（Leon N. Cooper）、ジョン・ロバート・シュリーファー（John Robert Schrieffer）によって構築された超伝導の基礎理論（BCS 理論と呼ばれる）では説明がつかず、物理学上の未解明問題の一つとして、現在も精力的に研究されている。

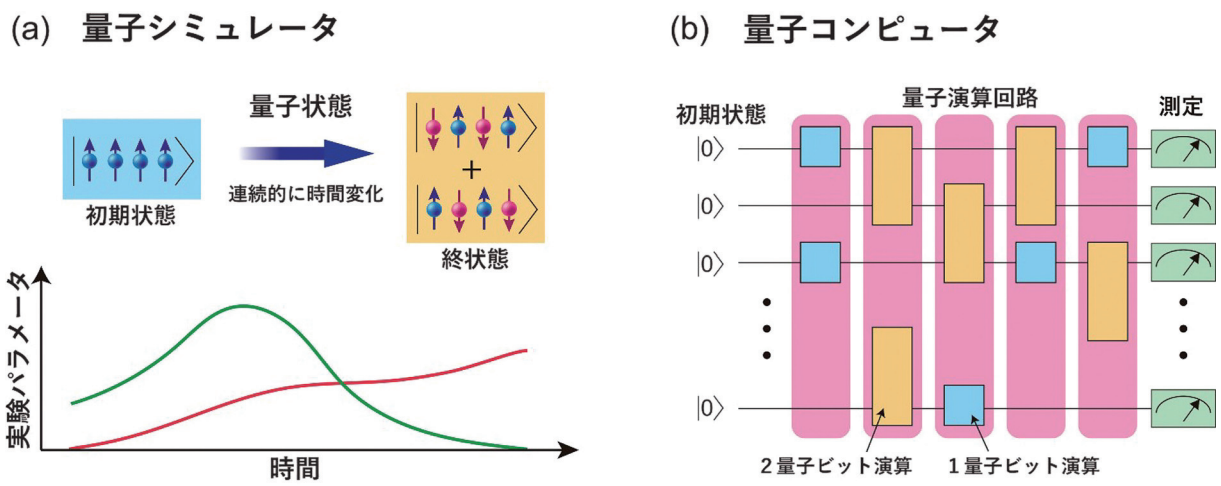
(3)　量子効果によっていくつかの磁気秩序の重ね合わせ状態が実現したときに現れる新奇な磁気的性質を量子磁性と呼ぶ。大きな量子揺らぎを伴うため、通常の磁性体では見られないような物性が観測されると期待されている。ごく最近、ハーバード大などの研究チームが原子を使った量子シミュレータで、磁気秩序が固定せず液体のように揺らいだ量子磁性状態（量子スピン液体と呼ばれる）を実現させた。G. Semeghini et al., “Probing topological spin liquids on a programmable quantum simulator,” *Science*, Vol.374 Iss.6572, 2021.12.2, pp.1242-1247.

(4)　Richard P. Feynman, “Simulating physics with computers,” *International Journal of Theoretical Physics*, Vol.21, 1982, pp. 467-488. <https://doi.org/10.1007/BF02650179> リチャード・ファインマンは量子シミュレータのアイデアを 1981 年 5 月 6 ～ 8 日に米国のマサチューセッツ工科大学で開催された第 1 回計算の物理に関する会議（1st conference on Physics of Computation）での基調講演において初めて発表し、論文としては翌 1982 年に出版された。

ロセスに着目すると、量子シミュレータはアナログ量子コンピュータの一種と分類できるであろう[5]。

量子シミュレータ、量子コンピュータともに、プラットホームとなる量子系を非常に高い精度で操作、測定する技術が求められている。ただ、解明したい現象に似た状態を多数の粒子を使って人工的に作るといった模擬実験としての性質から、量子シミュレータで必要とされる精度は量子コンピュータと比較してかなり緩和される傾向にある。そのため、現状では両者の研究開発の方向性に違いが生じている。量子シミュレータはある程度大規模な量子系に対して操作・測定精度を高めていく方向であり、量子コンピュータは高い操作・測定精度を実現している小規模な量子系に対してその規模を拡大していく方向である。量子シミュレータでは大規模化が容易な原子・分子気体がメインのプラットホームとしてよく研究されており、一方、量子コンピュータでは高精度の量子ゲート操作を実現している超伝導量子ビット方式やイオントラップを中心として研究開発が進められている。

図 1　量子シミュレータと量子コンピュータの概念図



（注）　図 1(a) の量子シミュレータを補足説明する。量子力学的な 4 個の粒子を考え、それぞれの粒子は矢印で示されるように上向きと下向きの二つの状態を取るものとする。初期状態として 4 個の粒子の矢印がすべて上を向いた状態を準備し、実験パラメータを変化させながら粒子の矢印の向き（すなわち量子状態）を連続的に時間変化させて量子シミュレーションを実行する過程が概念的に描かれている。図では 4 個の粒子の最終状態として、矢印の向きが交互になった二つの異なる量子状態の重ね合わせが実現し、これが量子シミュレーションの結果である。量子シミュレータではこのように量子状態が連続的に時間変化する過程そのものが演算に対応していることが分かる。驚くべきことに、その過程では粒子の個数を N として 2^N（2 の N 乗）の数の量子状態を使った演算が実行されている。ここで、因子の 2 の値は矢印の向きに上向き、下向きの二つの状態があることに由来する。図 1(a) のように粒子が 4 個の場合は量子状態の数は N = 4 として 2^4=16 と小さな値であるが、粒子が 100 個になると N=100 として $2^{100}\approx10^{30}$（10 の 30 乗、すなわち 100 京の 1 兆倍）とその数は指数関数的に増大する。このため大規模な量子シミュレータでは莫大な数の量子状態を使ったシミュレーションが可能となる。最近、米国のハーバード大学の研究チームとフランスのパリ・サクレー大学の研究チームが独立して、2 次元的に並べた 200 個ほどの原子を用いた高精度の量子シミュレータの開発に成功し、大規模化に大きな進展があった。ハーバード大学チームの研究成果は Sepehr Ebadi et al., “Quantum phases of matter on a 256-atom programmable quantum simulator,” *Nature*, Vol.595, 2021.7.7, pp. 227-232. パリ・サクレー大学チームの研究成果は Pascal Scholl et al., “Quantum simulation of 2D antiferromagnets with hundreds of Rydberg atoms,” *Nature*, Vol.595, 2021.7.7, pp. 233-238. にそれぞれ掲載されている。

（出典）　筆者作成。

(5)　M. Morgrado et al., “Quantum simulation and computing with Rydberg-interacting qubits,” *AVS Quantum Science*, Vol.3 Iss.2, 2021.5.3, p.023501.

2　量子シミュレータのプラットホーム

この節では量子シミュレータのプラットホームとして使用されている代表的な量子系を四つ紹介する。どのプラットホームにおいても、最先端の実験技術（レーザー技術、測定技術、低温技術、真空技術、半導体微細加工技術、エレクトロニクスなど）を駆使して量子シミュレータの研究開発が行われている。

(1) 原子・分子

レーザー冷却（Laser cooling）と呼ばれる実験技術を利用すれば、ある特定の原子や分子の気体を 10 ～ 100 ミリ秒程度の間に 1 ～ 100 マイクロ・ケルビン(6)の極低温にまで冷却することが可能である(7)。図 2 は超高真空のガラス容器の中に封じ込めたリチウム原子の気体をレーザーで冷却している実験の写真である。中央の白い小さな点がリチウム原子の気体であり、赤く見えるのは冷却用のレーザー光である。気体の温度は 100 マイクロ・ケルビン程度で、１ミリメートル程のサイズの中に約 10 億個の原子が含まれている。

原子・分子を使った量子シミュレータでは、このようなレーザー光で冷却された気体をプラットホームとして使用する(8)。レーザー技術が著しく進展したことにより、レーザー光は気体を冷却するだけではなく、原子・分子の量子状態を制御するためにも利用されている。ここでは代表的な実験技術を二つ紹介する。図 3(a) は光格子（Optical lattice）と呼ばれる技術で固体物質の状態を疑似的に実現させる目的で用いられている(9)。実験ではレーザー光を向かい合った配置で 6 方向から気体に照射する。この時、光の干渉(10)でレーザー光の強度は周期的に変化し、図のように空間的な格子構造が形成される。原子はこの格子の中をあたかも固体中の電子のように動き回る。光格子はレーザーで作成した人工の結晶であり、不純物や格子欠陥も存在しないため、固体物質の性質を調べるには理想的な結晶になっている。図 3(b) はレーザー光を使って微小物体を捕捉する光ピンセット（Optical tweezer）を応用した技術である(11)。最先端の光学素子を使えば光ピンセット用レーザー光のビーム径を 1 マイクロメートル程度にまで絞り、図のように原子や分子を 1 個ずつ捕獲して格子状に配置することが可能になっている。更に、光学素子の電気的制御により、光ピンセットに捕獲された原子や分子を 1 個ずつ自由に動かすこともできる。高い制御性を備えた光ピンセット技術は量子シミュレータの研究開発において大きな注目を集めている。

---

(6)　ケルビンは熱力学で定義される絶対温度の単位である。気体中の原子や分子の熱運動が消失し、これ以上に温度を下げることができない最低温度を絶対零度と呼び、0 ケルビンと定義する。この温度は我々が日常使用している摂氏温度では -273.15℃に相当する。極低温の温度領域を研究対象とする量子シミュレータでは絶対温度を使って温度を表記することがほとんどである。1 マイクロ・ケルビン（マイクロ＝ 100 万分の 1）は絶対零度に対してわずか 100 万分の 1 度だけ温度が高い状態を表す。

(7)　レーザー冷却の原理についてわかりやすく説明している教科書として、久我隆弘『量子光学』朝倉書店, 2003, p.90.

(8)　レーザー冷却された原子を用いた量子シミュレータの解説記事として、Immanuel Bloch et al., “Quantum simulations with ultracold quantum gases,” *Nature Physics*, Vol.8, 2012.4.2, pp.267-276.

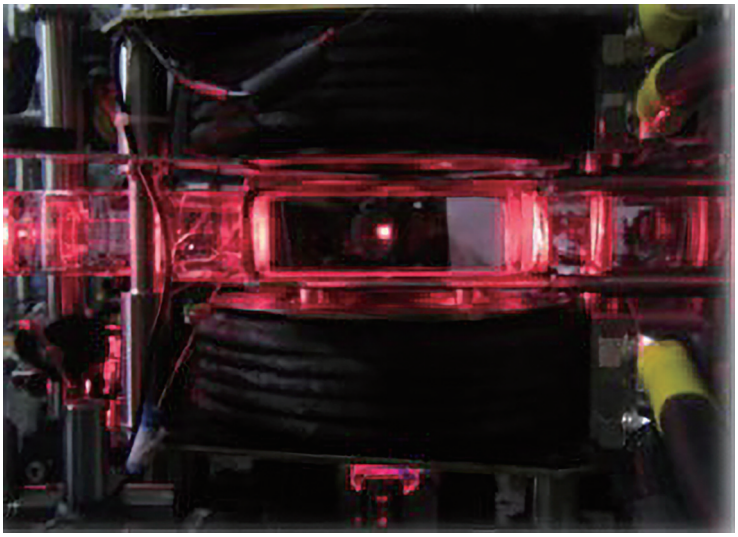
(9)　Imanuel Bloch, “Ultracold quantum gases in optical lattices,” *Nature Physics*, Vol.1, 2005.10, pp.23-30.

(10)　複数の波が出会うとき、波が重なることで、強め合ったり、弱め合ったりして新しい波形ができることを波の干渉と呼ぶ。光の干渉は光が波の性質を備えている証拠となっている。光格子の場合、通常 1 本のレーザー光から分岐した光を 2 本ずつ対向的な配置で重ね合わせているため、干渉によってレーザー光の波長の半分（数 100 ナノメートル）の周期で光の強度が周期的に変化する。

(11)　Antoine Browaeys, “Alkaline Atoms Held with Optical Tweezers,” *Physics*, Vol.11 No.135, 2018.12.28. <https://physics.aps.org/articles/v11/135>

他方、レーザー冷却された極低温の原子や分子の優れた特徴として、磁場を使って原子同士に働く相互作用の性質（引力あるいは斥力）や強さを自由に変化させることが可能である[12]。最近ではリュードベリ状態（Rydberg states）と呼ばれる励起状態（原子に含まれる電子を高いエネルギー準位に昇位させた状態）を利用して瞬時に原子同士の相互作用を制御する技術[13]なども進展しており、量子シミュレータとしての可能性が広がっている。

図２　ガラスセル中のリチウム（Li）の冷却原子気体

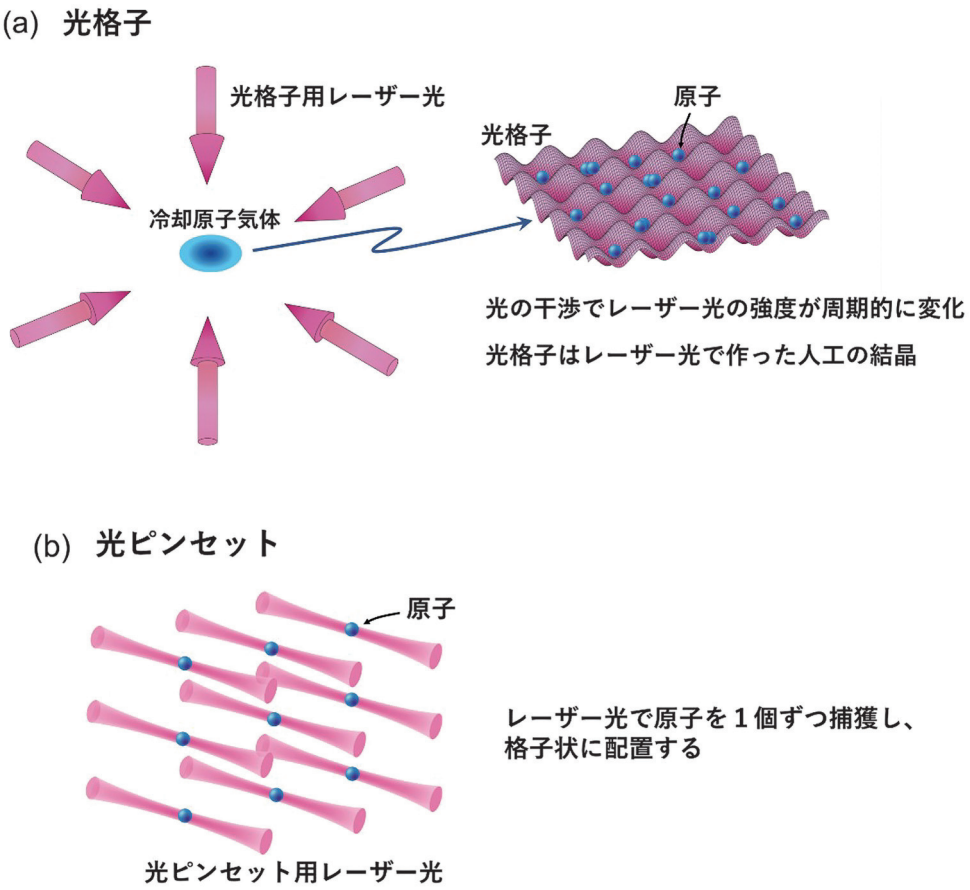


（出典）大阪大学大学院基礎工学研究科向山敬教授提供。Jun Yoshida et al., “Scaling Law for Three-Body Collisions of Identical Fermions with *p*-Wave Interactions,” Physical Review Letters, Vol.120 Iss.13, 2018.3.30, pp.133401-1-133401-5. <https://doi.org/10.1103/PhysRevLett.120.133401>

⑿　C. Chin et al., “Feshbach resonances in ultracold gases,” *Reviews of Modern Physics*, Vol.82 Iss.2, 2010.4-6, pp.1225-1286. <https://doi.org/10.1103/RevModPhys.82.1225>

⒀　Antoine Browaeys and Thierry Lahaye, “Many-body physics with individually controlled Rydberg atoms,” *Nature Physics*, Vol.16, 2020.1.20, pp.132-142. レーザー光を照射して原子をリュードベリ状態に変化させることで、10 ナノメートル程度だった原子間の相互作用距離を 1000 倍の 10 マイクロメートル程度にまで増大させることが可能である。リュードベリ状態の原子間に働くこのような強い相互作用は量子コンピュータの量子ゲート操作にも利用できると考えられている。

図３　光格子と光ピンセットの模式図



（出典）筆者作成。

(2)　イオン

電気的に中性な原子からレーザー光などを使って人為的に電子を奪い取ったイオンも量子シミュレータのプラットホームとして利用されている[14]。イオンに対してもレーザー冷却が可能であり、ミリケルビン以下の極低温にまで冷却されたイオンを使って実験が行われている。前述の中性の原子、分子の気体とは異なり、イオンは電荷を持っているため、電場を使って空間的に強く、かつ安定的に閉じ込めることができるのが特徴である。

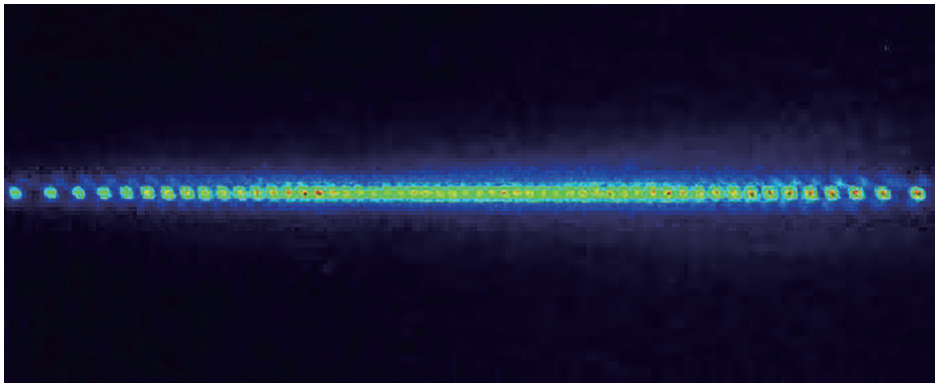
図４は高周波で振動する電場に静的電場を加えることで実効的に細長い１次元的な電場ポテンシャルを形成させ[15]、その中に 54 個のカルシウムイオン（Ca^{+}）を閉じ込めたときの画像である。測定用のレーザー光の照射により、それぞれのイオンは発光している。正電荷を持つカルシウムイオン間に働く斥力の静電気力（クーロン相互作用）により、イオン同士が避けあいながら一列に並んでいるのが分かる。レーザー光を使って個々のイオンを非常に高い精度で制

(14)　Christopher Monroe et al., “Programmable quantum simulations of spin systems with trapped ions,” *Reviews of Modern Physics*, Vol.93 Iss.2, 2021.4-6, pp.025001-1-025001-57. <https://doi.org/10.1103/RevModPhys.93.025001> イオンを用いた量子シミュレータの解説記事として、R. Blatt and C. F. Roos, “Quantum simulations with trapped ions,” *Nature Physics*, Vol.8, 2012.4.2, pp.277-284.

(15)　安定にイオンを捕獲（トラップ）するための重要な実験技術であり、発明者ヴォルフガング・パウル（Wolfgang Paul）の名にちなんでパウルトラップ（Paul trap）と呼ばれている。Rainer Blatt and David Wineland, “Entangled states of trapped atomic ions,” *Nature*, Vol.453, 2008.6.19, pp.1008-1015.

御、測定することが可能であり、量子シミュレータとして優れた特性を持っている。また、隣り合ったイオン同士はクーロン相互作用で連結しており、バネ振動のようなイオンの運動も存在する多様性のある量子系になっている。

図４　一列に並んだ 54 個のカルシウムイオン（Ca^{+}）



（出典）大阪大学量子情報・量子生命研究センター（QIQB）豊田健二教授より提供。M. Tamura et al., “Quantum Walks of a Phonon in Trapped Ions,” Physical Review Letters, Vol.124 Iss.20, 2020.5.22, pp.200501-1-200501-6. <https://doi.org/10.1103/PhysRevLett.124.200501>

（3）電子

最先端の半導体微細加工技術を使えば、半導体上の直径 10 ～ 100 ナノメートル（ナノ＝ 10 億分の 1）の微小な領域に電子 1 個を閉じ込めて、制御・測定することが可能となっている。これは量子ドット（Quantum dot）と呼ばれ、半導体で作製された人工原子として量子シミュレータのプラットホームに利用されている[16]。電子は電荷だけでなく磁気双極子モーメントを担ったスピンの自由度を持っているため、この系は物質の磁気的性質を調べるのに適している。現在のエレクトロニクスを駆使すれば、電子 1 個の運動やスピンの量子状態を測定できる。また、今後の半導体技術の進展に伴い、多数の量子ドットを集積することで大規模化も可能になると期待できる。

図 5 はオランダのデルフト工科大学のグループが作製した半導体量子ドットデバイスの電子顕微鏡写真である[17]。図中央の 1 ～ 4 の丸印で示されているのが量子ドットであり、プラケットと呼ばれる正方形の配置にすることにより、電子のスピンが全て揃った強磁性状態が観測された。これは日本人物理学者の長岡洋介が理論的に発見した量子磁性状態であり、「長岡の強磁性」と呼ばれている[18]。

量子ドット以外に電子を使った量子シミュレータとして、超伝導量子ビットの集積回路も重要である。超伝導量子ビット 1 個 1 個は人工原子と見なすことができ、超伝導量子ビットを 2

---

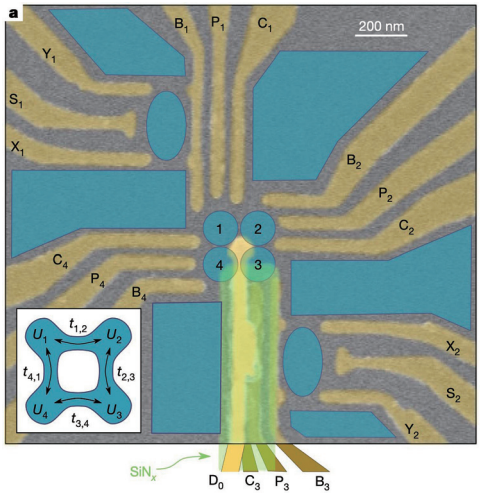
⑯　Anasua Chatterjee et al., “Semiconductor qubits in practice,” *Nature Reviews Physics*, Vol.3, 2021.2.19, pp.157-177. 半導体量子ドットを用いた量子シミュレータの解説記事として、Pierre Barthelemy and Lieven M. K. Vandersypen, “Quantum Dot Systems: a versatile platform for quantum simulations,” *Annalen Der Physik*, Vol.525 Iss.10-11, 2013.11, pp.808-826. <https://doi.org/10.1002/andp.201300124>

⑰　J. P. Dehollain et al., “Nagaoka ferromagnetism observed in a quantum dot plaquette,” *Nature*, Vol.579, 2020.3.26, pp.528-533.

⑱　Yosuke Nagaoka, “Ferromagnetism in a Narrow, Almost Half-Filled *s* Band,” *Physical Review*, Vol.147 Iss.1, 1966.7, pp.392-405. <https://doi.org/10.1103/PhysRev.147.392>

次元的に配置した回路は 2 次元結晶の量子シミュレータに相当する[19]。量子コンピュータの研究開発と並行して、超伝導量子ビット集積回路を使った量子シミュレータの研究も精力的に進められている[20]。

図５　半導体量子ドットデバイスの電子顕微鏡写真



（出典）J. P. Dehollain et al. “Nagaoka ferromagnetism observed in a quantum dot plaquette,” *Nature*, Vol.579, 2020.3.2, p.529. <https://doi.org/10.1038/s41586-020-2051-0> Springer Nature 社の許諾を得て転載。

(4) 光子

量子シミュレータのプラットホームとして光子を使った研究は近年急速に進展しつつある[21]。その背景には、単一光子発生源、制御性に優れた光集積回路、更に高効率の光子検出器などの基盤技術が揃ってきたことがある。特に光集積回路の進歩は目覚ましく、半導体微細加工技術を使ってシリコンチップ上に作製した導波路回路に光子を伝搬させることで様々な疑似実験（シミュレーション）がマイクロ秒程度の短時間に実行できる。光集積回路は量子コンピュータへも応用できるため、現在、大規模化に向けた激しい開発競争が繰り広げられている。

一例として、図 6 に米国のマサチューセッツ工科大学（MIT）のグループが作製した光集積回路を示す。回路中には 88 個の分岐点が配置されており、それぞれに端子が接続されており電気的に制御できるような構造になっている。MIT グループは光子をチップの左側から入力し、チップ上の導波路回路を伝搬させ、右側から出力された光子の状態を計測することで、量子輸送現象のシミュレーションに成功した[22]。

---

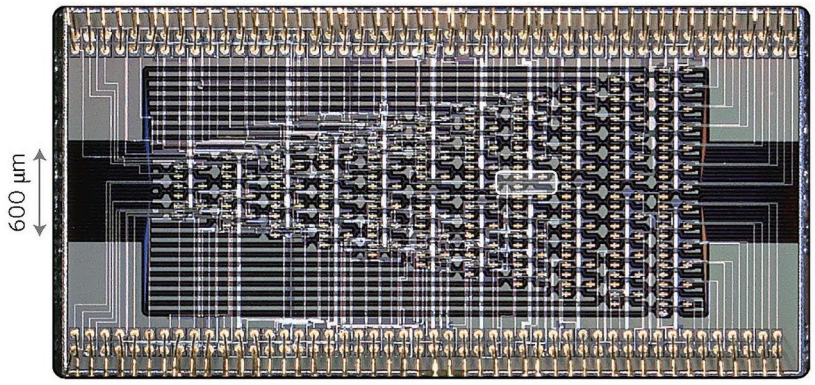
(19)　Yariv Yanay et al., “Two-dimensional hard-core Bose–Hubbard model with superconducting qubits,” *npj Quantum Information*, Vol.6 No.58, 2020.6.26. <https://doi.org/10.1038/s41534-020-0269-1>; Ming Gong et al., “Quantum walks on a programmable two-dimensional 62-qubit superconducting processor,” *Science*, Vol.372 Iss.6545, 2021.5.6, pp.948-952.

(20)　超伝導量子ビットに関する最近の解説記事として、Morten Kjaergaard et al., “Superconducting Qubits: Current State of Play,” *Annual Review of Condensed Matter Physics*, Vol.11, 2020.3, pp.369-365. <https://doi.org/10.1146/annurev-conmatphys-031119-050605>

(21)　光子を用いた量子シミュレータの解説記事として、Alán Aspuru-Guzik and Philip Walther, “Photonic quantum simulators,” *Nature Physics*, Vol.8, 2012.4.2, pp.285-291. 光集積回路の最近の技術的進展を解説した記事として、Jianwei Wang et al., “Integrated photonic quantum technologies,” *Nature Photonics*, Vol.14, 2020.5, pp.273-284.

(22)　Nicholas C. Harris et al., “Quantum transport simulations in a programmable nanophotonic processor,” *Nature Photonics*, Vol.11, 2017.6, pp.447-452. <http://dx.doi.org/10.1038/nphoton.2017.95>

図６　シリコンチップ上に作製された光集積回路



（出典）Nicholas C. Harris et al., “Quantum transport simulations in a programmable nanophotonic processor,” *NaturePhotonics*, Vol.11, 2017.6, p.449. <http://dx.doi.org/10.1038/NPHOTON.2017.95> Springer Nature 社の許諾を得て転載。

(5) 量子シミュレータの研究開発動向

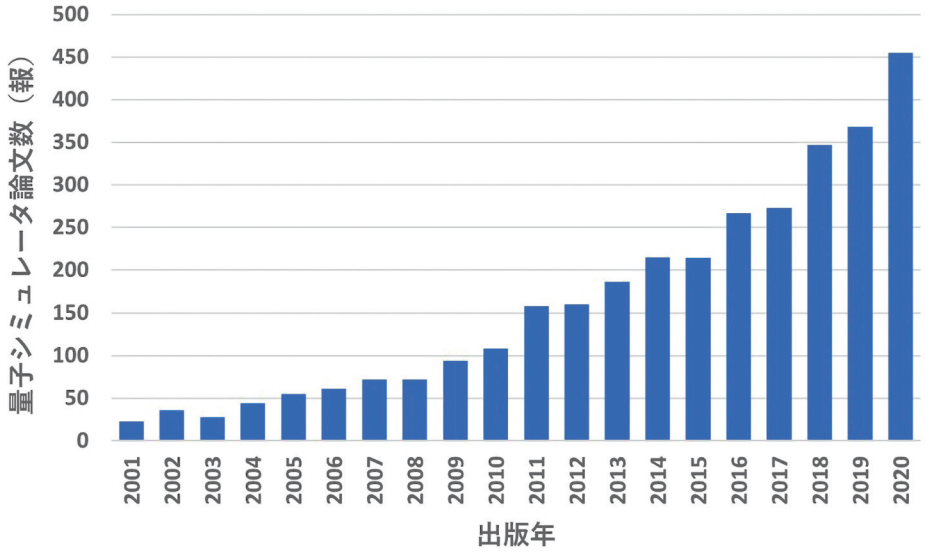
量子シミュレータの研究開発は基礎科学分野への貢献として、主要な成果のほとんどは学術論文を通して発表されている。ここではエルゼビア社の文献データベース Scopus[23] から得た学術論文に関するデータを分析し、量子シミュレータの研究開発動向について説明する。

（ｉ）全世界的な動向

図 7 は 2001 年から 2020 年までの各年に出版された量子シミュレータに関する論文の数を棒グラフで示したものである。Scopus に登録されている全世界の科学技術論文の中から「量子シミュレータ」あるいは「量子シミュレーション」をキーワードに持つ論文を検索することによって求めた。グラフからは、量子シミュレータの論文数は 2001 年からの 20 年間で 20 倍にもなり、特に近年は加速度的に増加していることがわかる。これは各国における量子情報技術戦略を反映したものであり、量子シミュレータの研究開発が熾烈な競争下にあることを意味する（参照：本報告書第 4 章　世界各国の政策）。この傾向は今後ますます顕著になってくると予想される。

(23)　Scopus website <https://www.scopus.com/>

図 7　出版年ごとの量子シミュレータ論文数の推移



（注）　検索に用いたキーワードは quantum simulator*, quantum simulation* である。
（出典）商用データベース Scopus の検索結果を基に筆者作成。

（ii）研究競争力の国別比較

次に、量子シミュレータ研究開発の国別競争力を比較してみたい。ここでは、各年に出版された量子シミュレータ関連の論文について、著者がどの国の研究機関に所属しているかの割合を国別競争力の指標として採用する[24]。

図 8 は 2011 年から 2020 年までの 10 年間、主要 5 か国（米国、ドイツ、中国、英国、日本）の著者割合がどのように推移しているかを示したグラフである。米国が圧倒的な強さを見せており、直近の 10 年間では量子シミュレータ関連の論文の 4 分の 1 から 5 分の 1 が米国の研究機関に所属する研究者を著者として含んでいることが分かる。5 か国のうちでは中国だけが顕著な右肩上がりの傾向を示しており、驚くべきことにこの 10 年間で 3 倍も増している。欧州ではドイツが頭一つ抜きんでた存在ではあるが、ドイツ、英国の推移からも分かるように、欧州ではいずれの国もほぼ横ばいの傾向にある。一方で、日本はしばらく低迷していたが、2018 年くらいから増加傾向にあり競争力が少しずつ向上している。

国別競争力について更に詳細な情報を得るために、今度は 2015 年と 2020 年に注目し、それぞれの年において、著者の割合が高い順にトップ 10 の国を示す（図 9、図 10）。2015 年は米国を筆頭にドイツ、中国、スペインと続き、英国を始めとする先進国がその後を追うといった状況であった。中国が 2015 年の段階で既に量子シミュレータの研究で世界トップレベルに位置するのは注目すべき点である。日本は 8 位に位置している。

2020 年には国別の競争力に変化が生じていることが分かる。米国のトップは揺るぎないが、中国は 2015 年と比較して大幅に割合値を増加させており、ドイツを抜き、米国に次ぐ 2 位に

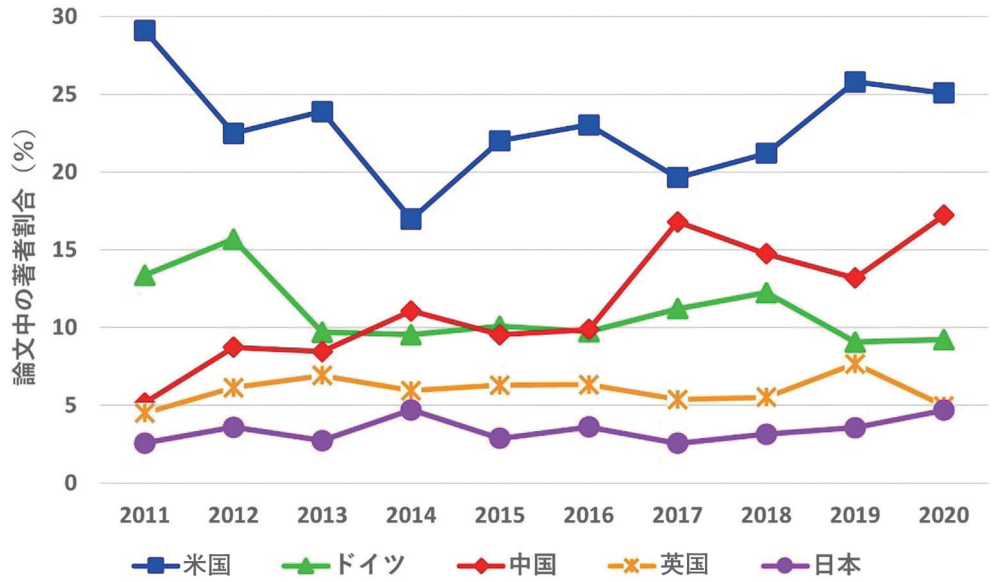
(24)　国際連携が盛んな量子シミュレータの研究開発分野では、論文は異なる国の研究機関に所属する複数の著者たちによる共著が多い。このような状況をデータに反映させるため、図 7 で求めた量子シミュレータ関連の論文に対して、著者が所属する研究機関の国別割合を調べ、出版年毎にその割合値の平均を求めて指標とする。

上がっている。中国の躍進の背景には国家戦略によって量子技術開発が推進されたことがあると考えられる。

日本は 2020 年には 5 位に位置し、量子シミュレータの研究開発に対して競争力が向上していることが分かる。これは近年開始された量子情報技術分野の大型プロジェクト[25]による手厚い支援が結実したものであると言えるであろう。2020 年には国家戦略「量子技術イノベーション戦略」が制定され、量子情報技術分野に対する継続的な支援が予定されており、今後の日本の競争力のさらなる向上が期待される。

図 10 のグラフでインドがトップ 10 内に入っていることも注目すべき点として挙げておく。最近、インド政府も量子技術分野への大規模予算支出を発表しており[26]、IT 大国であるインドの今後の動向にも注意が必要である。

図８　量子シミュレータ論文の国別著者割合の推移
（米国、ドイツ、中国、英国、日本）

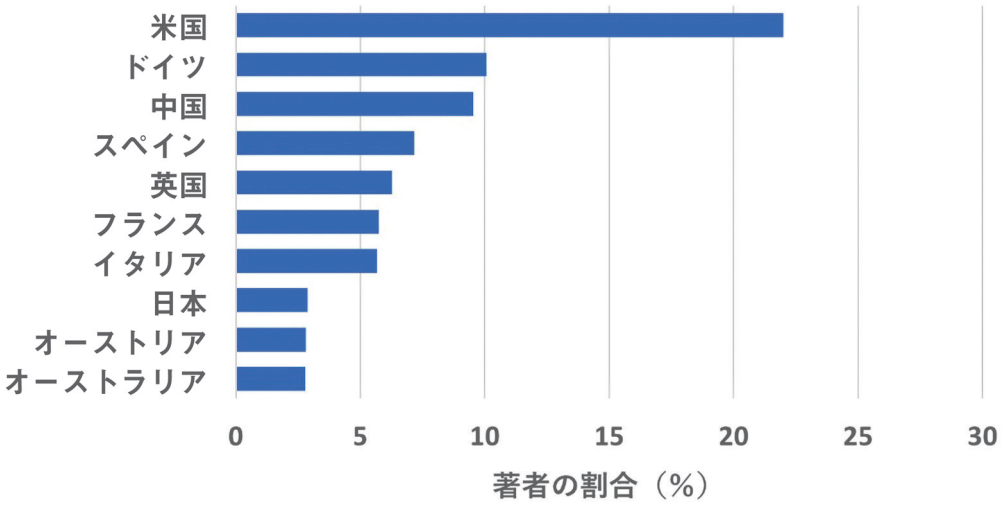


（出典）　商用データベース Scopus の検索結果を基に筆者作成。

[25]　2016 年開始：「量子状態の高度な制御に基づく革新的量子技術基盤の創出」科学技術振興機構 ウェブサイト <https://www.jst.go.jp/kisoken/crest/research_area/ongoing/bunyah28-2.html>;「量子の状態制御と機能化、革新的な量子情報処理技術基盤の創出」同 <https://www.jst.go.jp/kisoken/presto/research_area/ongoing/bunya2019-6.html> 2018 年開始：「光・量子飛躍フラッグシッププログラム（Q-LEAP）」同 <https://www.jst.go.jp/stpp/q-leap/> 等。

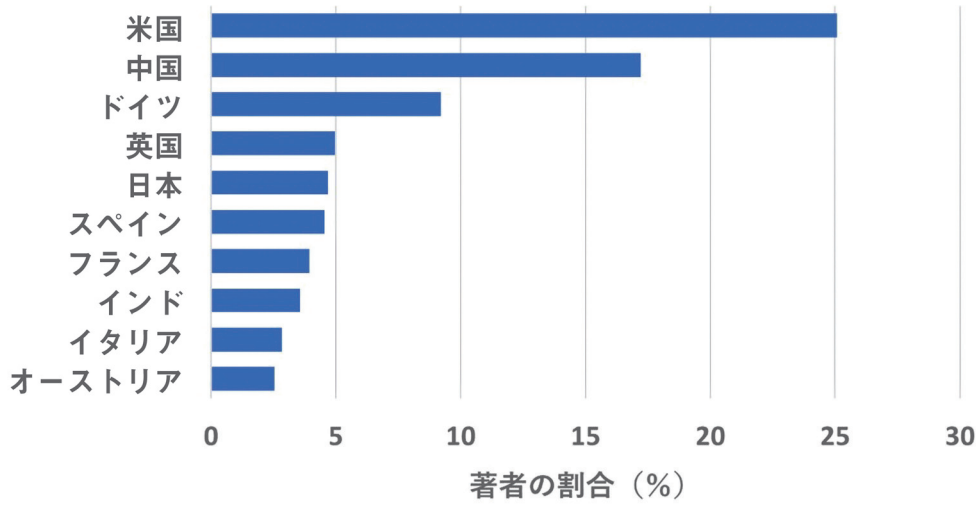
[26]　T.V. Padma, “India bets big on quantum technology,” *Nature*, 2020.2.3. <https://www.nature.com/articles/d41586-020-00288-x/>

図９　2015 年に出版された量子シミュレータ論文の国別著者割合



（出典）商用データベース Scopus の検索結果を基に筆者作成。

図１０　2020 年に出版された量子シミュレータ論文の国別著者割合



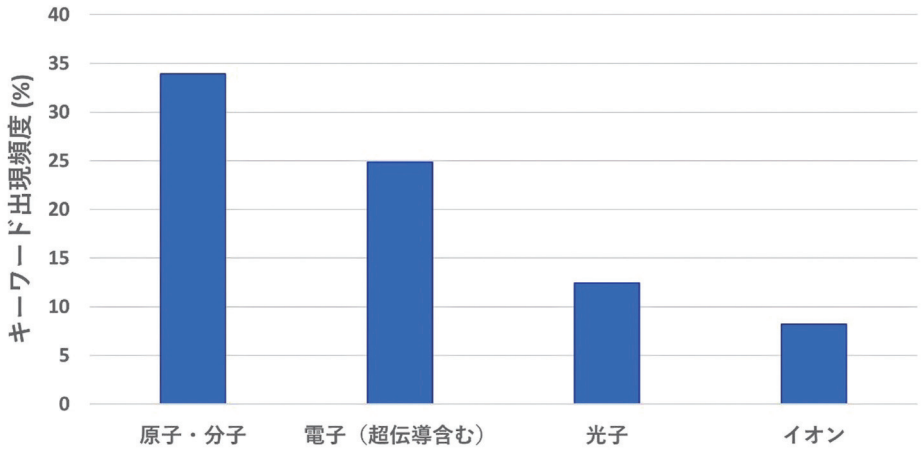
（出典）商用データベース Scopus の検索結果を基に筆者作成。

（iii）プラットホームの研究状況比較

量子シミュレータの研究開発において、原子・分子、イオン、電子、光子といった量子力学的な極微の粒子がプラットホームとして使用されているが、ここではその研究状況を最新のデータを通して比較してみたい。指標として、2020 年に出版された量子シミュレータ関連の論文に対して、原子、イオンといったプラットホームを示すキーワード検索を行い、その出現頻度を調べた。図 11 から、原子･分子のキーワードの頻度が他と比べて高く、量子シミュレータのプラットホームとして広く研究されていることが分かる。これは、原子・分子は大規模化が比較的容易であり、量子シミュレータの研究開発に向いていることを反映している。一方で、量子コンピュータの研究開発では、極めて高い精度での操作・測定が可能な超伝導デバイス、

イオン、光子がメインのプラットホームとして使用されている。どのプラットホームにおいても、大規模化、高精度化に向けた技術開発の進歩は速く、量子シミュレータの研究状況も数年後には図 11 から一変している可能性も否定できない。

図１１　2020 年出版の量子シミュレータ関連論文におけるキーワードの出現頻度



（注）　検索に用いたキーワードは原子・分子に対しては atom*, molecule*, optical lattice* であり、電子（超伝導含む）に対しては electron*, quantum dot*, superconduct* であり、光子に対しては photon* であり、イオンに対しては trapped ion*, ion trap*, ion-trap* である。
（出典）　商用データベース Scopus の検索結果を基に筆者作成。

執筆：大阪大学量子情報・量子生命研究センター（QIQB）特任准教授　山下（やました）　眞（まこと）

Ⅲ　量子センシング

はじめに

量子コンピュータや量子通信、そして量子センシングと言った量子技術による第 2 次量子革命に向けた研究開発が世界中で加速している。中でも量子センシングは第 2 次量子革命において非常に重要な役割を果たすと考えられている。量子センシングの発展において、日本は先駆的かつ重要な貢献を成しており、最新の応用研究でも世界をリードする研究がいくつも存在している(1)。まず、第 2 次量子革命における量子センシングについて、次に、従来のセンシングと量子センシングの比較について、また、日本の貢献について述べながら量子センシングの理論や応用を俯瞰する。

1　第 2 次量子革命における量子センシング

本節では、本章だけを読む人が量子技術全体における量子センシングの立ち位置が分かるように、他章で説明された内容を重複して説明することになるのをご容赦いただきたい。

20 世紀において、量子力学が誕生し社会に大きな変革がもたらされた。量子力学は半導体工学を生み、コンピュータが誕生し、これにより IT（Information Technology）革命が起きた。また、量子力学はレーザーを生み、光通信が誕生した。通信の発展も含めて ICT（Information and Communication Technology）革命と呼ばれている。さらに、MRI（Magnetic Resonance Imaging）や電子顕微鏡、核医学検査、レーザー分光法などの量子力学の原理に基づいて物体をセンシングする手法が次々に発展し、生体診断や物質分析の世界が一変した。これらを第 1 次量子革命と捉えて、量子コンピューティング・シミュレーション、量子通信・インターネット、量子センシング・標準の応用研究開発が進展する現在は、まさに第 2 次量子革命が到来したと考えられている。

量子もつれや量子重ね合わせといった量子力学が許す不思議な性質をただ理解するだけではなく、量子コンピューティング、量子通信、量子センシング等として積極的にいわゆる「量子技術」として実用化することによって達成されるのが第 2 次量子革命である。量子技術の最終目標は、量子コンピューティングであり、特に、より複雑な量子アルゴリズムでも実装可能になる誤り耐性量子コンピュータの実現である。当初この目標はばかげているぐらい難しいのではないかと考える人も多かったが、2014 年に Martinis が超伝導量子ビットにおいて誤り耐性実現のための閾値を突破し、30 年以内に完成する可能性が一気に高まった(2)。そして、2019 年に彼と Google のチームは、スーパーコンピュータでも成し得ない計算を 53 量子ビットの超伝導量子コンピュータで実現し、「量子超越性」（古典コンピュータでは成し得ない計算を量子コンピュータにより実現すること）を達成した(3)。量子超越性を定義した Preskill は 2012 年の

＊　本稿におけるインターネット情報の最終アクセス日は、令和 4（2022）年 2 月 14 日である。

(1)　量子センシングについては日本語で体系的に理解するための教科書はほとんどなかったが、今後の更なる研究の発展への一助となるべく、筆者は 2021 年に『量子センシングハンドブック』を監修した。幅広いバックグラウンドからなる多くの量子センシング研究者が執筆にあたった。本章は、このハンドブックに書かれた情報をまとめるような形をとっている。根来誠監修『量子センシングハンドブック―量子科学が切り拓く新たな領域―』エヌ・ティー・エス, 2021.

(2)　R. Barends et al., “Superconducting quantum circuits at the surface code threshold for fault tolerance,” *Nature*, vol.508, 2014.4.23, pp.500-503. <https://www.nature.com/articles/nature13171>

(3)　Frank Arute et al., “Quantum supremacy using a programmable superconducting processor,” *Nature*, Vol.574, 2019.10.23, pp.505-510.

論文において「大規模量子系を制御することは、単に本当に難しいだけなのか、それとも、ばかげているぐらい難しいのだろうか。前者の場合、大規模量子コンピュータの構築は、数十年の非常に困難な作業の後に成功するだろう。後者の場合は、成功したとしても何世紀も先になるかもしれない。」と述べていた(4)。そして、量子超越達成を受けて彼は、「今回の Google チームの成果は、量子コンピューティングは単に本当に難しいだけだという我々の確信を強めた。もしそれが正しいならば、これから数十年の間に、数多くの量子技術が花開くことになるだろう。」と表現した(5)。

応用範囲がとても広い誤り耐性量子コンピュータを 2040 年代に達成するには、量子状態の精密制御技術を 20 年以上安定して発展させる必要がある。この発展を支える技術が量子通信と量子センシングであると考えられている。半導体工学がコンピュータとして花開く前に、通信のデバイスやセンシングのデバイスとして市場を開拓したように、量子情報技術もこうした道を歩むと期待されている。世界の投資は量子コンピューティングのみに偏ることなく量子情報技術の各分野に分散されており、日本でも多くの投資が量子センシングになされている（第 4 章を参照）。米国ホワイトハウスの科学技術政策局（Office of Science and Technology Policy: OSTP）の量子情報科学部門の補佐官を務めた Jacob Taylor 博士は、量子超越性達成前のインタビューにおいて、暗号解読にも使えるような量子コンピュータが最終的に実現しない可能性はあるかもしれないとしながらも、「量子センサは実際に存在し、機能しており、これは巨大な新産業になる可能性がある」と話し、このさほど不確かではない量子技術が米国の経済的リーダーシップにとって重要であることを強調している(6)。

2　従来のセンシングと量子センシング

日本中の工学部のカリキュラムにはセンシング工学や計測工学という科目があり、数多くの優れた専門教育向け教科書が存在する(7)。教科書の中ではまず言葉の定義がなされるが、センシング技術という言葉は、「センサを用いて物質や環境などの様々な情報を計測・数値化する技術」と定義される。センシング対象としては、例えば電場・磁場があるが、これらをセンシングするデバイスとしてはホールセンサや SQUID（superconducting quantum interference device. 超伝導量子干渉計）による磁気センサが、また、電磁場のセンシングには電気光学プローブなどが用いられている。空間や変位・運動をセンシングの対象とするものもある。例えば、高度を計測する場合は気圧計を用い、三軸加速度を計測する場合はジャイロスコープを用いる。微小な変位をとらえる超音波検出素子は医用センシングにも用いられている。対象は化学・生物学にも及ぶ。pH センサやグルコースセンサは古くから用いられている。また、蛍光蛋白質をプローブとして、生体内をセンシングすることもできる（表 1）。センサの性能を評価する方法に関して、センシングにおけるノイズや計測標準について議論される。最近の計算・通信技術との融合技術の発展は目覚ましく、IoT（Internet of Things）やセンサネットワークなどにつ

(4)　John Preskill, “Quantum computing and the entanglement frontier,” arXiv: 1203.5813.
(5)　John Preskill, “Why I Called It ‘Quantum Supremacy’,” 2019.10.2. Quantam Magazine website <https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/>
(6)　“Science Committee Seeks to Launch a National Quantum Initiative,” 2018.5.29. American Institute of Physics website <https://www.aip.org/fyi/2018/science-committee-seeks-launch-national-quantum-initiative>
(7)　南茂夫ほか『はじめての計測工学　改訂第 2 版』講談社, 2012; 山崎弘郎『センサ工学の基礎　第 2 版』オーム社, 2014.

いて述べているものもある。

量子センシングの応用までをカバーした日本語の教科書は現時点では見当たらない。量子計測の理論的な教科書としては沙川ほか著『量子計測と量子制御』を挙げることができる(8)。量子センシング工学については、教科書のようにまとまっていないものの、『量子センシングハンドブック』を参考にされたい(9)。

量子センシング技術を定義すると「量子センサを用いて物質や環境などの様々な情報を計測・数値化する量子技術」である。量子情報技術に即してより意義のある定義は、Degan、Reinhard 及び Cappellaro のレビューによる(10)。そこでは、

Ⅰ．量子状態 [Qubit（量子ビット）, qutrit, …, qudit, …, qunat]（角括弧内は筆者補足）を用いて物理量を測定する。

Ⅱ．量子コヒーレンス（量子状態間のコヒーレンス）を用いて物理量を測定する。

Ⅲ．量子もつれを用いて、計測の感度や精度を古典的な（従来の）限界を超えて向上させる。

のいずれかを満たすものとして定義されている。これら全てを満たすという狭義の定義を考える立場もある。筆者の意見は後者である。Qubit は 2 準位の量子状態を持つもので、量子情報ではそれぞれを|0> と|1> とラベルを付けるのが標準的である。qutrit は 3 準位を持つもの、qudit は 10 準位、qunat は無限次元のものを考えている。|0>と|1>が重ね合わせられた $(|0\rangle+|1\rangle)/\sqrt{2}$ のコヒーレンス状態をセンシング対象にさらすことで、位相（重ね合わせ方を示す量）の変化量から測定対象をセンシングする。この原理を用いるのが量子センシングデバイスであり、センシングの対象により異なった方式がものがある（図 1）。2qubit のセンサでは、両方の量子ビットが |0> の状態である |00> と |1> の状態である |11> が重ねあわされた (|00>+|11>)/2 の量子もつれ状態をセンシングに用いることで感度を向上できる。これによって従来知られていた限界「標準量子限界」を突破できるのである。

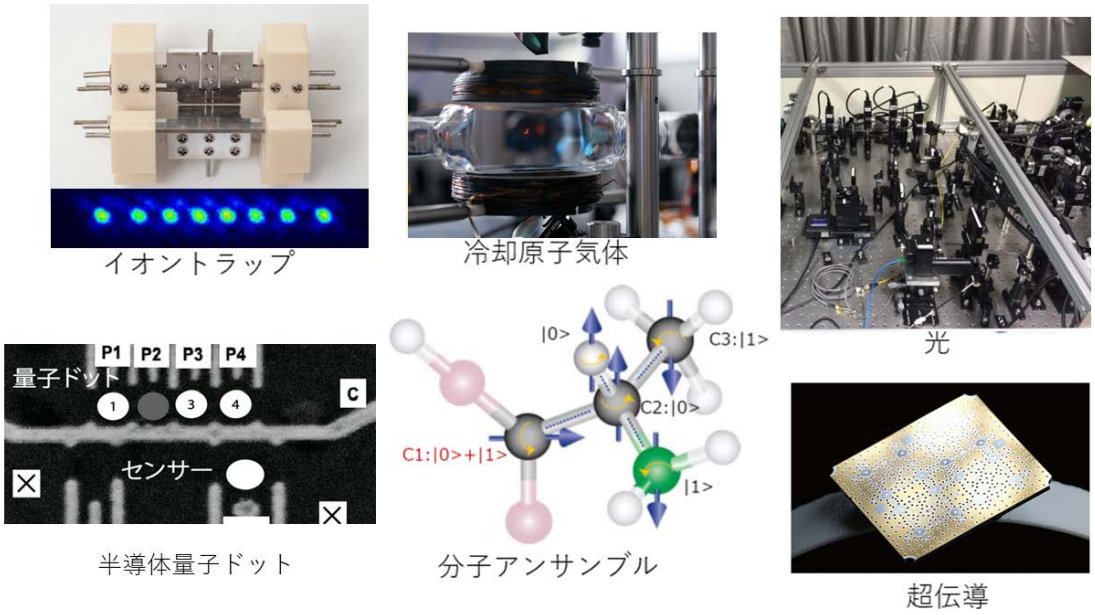
表 1　センシング対象とセンシングデバイス

センシング対象	従来センシングデバイス	量子センシングデバイス
磁場・電場	ホールセンサ SQUID センサ 電気光学プローブ	原子気体 qubit ガスセル 超伝導 qubit センサ 単一 NV 中心
高度	気圧計	光格子による重力センサ
三軸加速度	ジャイロスコープ	原子気体 qubit ガスセル イオントラップ
pH	pH センサ	単一 NV 中心 分子アンサンブル
血中グルコース濃度	グルコースセンサ	分子アンサンブル
生体内センシング	蛍光蛋白質	単一 NV 中心 分子アンサンブル
医用センシング	超音波検出素子	分子アンサンブル 光

（出典）筆者作成。

(8)　沙川貴大・上田正仁『量子測定と量子制御　電子版』サイエンス社, 2016.
(9)　根来監修　前掲注(1)
(10)　C. L. Degan et al., “Quantum sensing,” *Reviews of Modern Physics*, Vol.89 035002, 2017.7.25. <https://doi.org/10.1103/RevModPhys.89.035002>

図 1　様々な量子デバイス



（出典）　イオントラップ：大阪大学量子情報・量子生命研究センター（QIQB）豊田健二教授、冷却原子気体と光：大阪大学大学院基礎工学研究科及び QIQB 山本俊教授、半導体量子ドット：大阪大学産業科学研究所大岩顕教授、超伝導：理化学研究所量子コンピュータ研究センターよりそれぞれ提供。

3　量子コンピュータデバイスと量子センシングデバイス

Degan のレビューでは、量子センサとして用いる物理系が満たすべき要件も述べられているが、その前に量子情報分野で有名な量子コンピュータとして用いる物理系に対する「DiVincenzo の要件」について紹介する[11]。

（1）性質が理解された qubit 系でスケーラブル[12]に構成されていること
（2）各量子ビットを基準となる状態に初期化できること
（3）コヒーレンス時間（量子重ね合わせ状態の保持時間）の方が量子ゲートの作用に要する時間より十分長いこと
（4）任意の量子ゲート操作を実行するために必要な量子ゲートの組（ユニバーサルセット）の実行が可能なこと
（5）Qubit ごとに状態測定できること

である。

これに対応させた Degan-Reinhard-Cappellaro による量子センサとして用いる物理系が満たすべき要件は、

①　性質が理解された qubit（qutrit なども可）系で構成されていること
②　Qubit 系の初期化と状態測定ができること
③　Qubit 系がコヒーレントに（重ね合わせ状態を保ったまま）制御できること
④　Qubit 系が測りたい物理量と相互作用していること

⑾　David P. DiVincenzo, “The Physical Implementation of Quantum Computation,” *Fortschritte der Physik*, Vol.48 Iss. 9-11, 2000.9, pp.771-783.
⑿　量子ビットを増やす労力（リソース、計算資源）が、量子ビットを増やすことによる計算能力の向上率を上回らないときにスケーラブルであるという。

である。①～③は量子コンピュータのそれと大きく変わらないが、④は量子センサ特有の要請である。筆者はこれに以下の要件を付け加えたい。

⑤　Qubit 数に対する量子もつれによる感度の向上率よりも、量子もつれ状態にある qubit 数を増やすことによる労力が上回らないこと

このような要件の下、量子コンピュータデバイスと同様のデバイスが量子センサのデバイスとして研究開発が行われている。量子コンピュータデバイスとしては、イオントラップや光格子を用いた原子気体 qubit 系、分子アンサンブルや固体中欠陥などのスピン qubit 系、超伝導量子ビットや半導体量子ドットなどの人工 qubit 系、そして、光 qubit 系、その他の系での研究がこれまで進められてきた（図1）[13]。量子センシングデバイスもやはりこれらの系で研究が進められている。原子気体 qubit の系ではガスセル（ガラス容器の中に原子ガスを閉じ込めたデバイス）を使うものが磁気センサとして研究が進められている。光格子を用いる系では重力のセンシング、イオントラップの系では慣性センシング（三軸加速度のセンシング）の研究が進められている。スピン qubit の系では、単一 NV 中心を用いた磁気センサの研究（後述）や pH センシングが進められている。分子アンサンブルでは生体センシングや医用センシングが期待されている。超伝導 qubit の系では磁気センサが、光 qubit の系では、医用センシングや重力波の検出の研究も進んでいる。前述の表 1 にはこれらも併記した。

４　量子センシングの理論・応用研究における日本の貢献と国内外の最新状況

量子センシングには様々なデバイスが用いられているが、そのプロトコル（手順）や理論は各種のデバイスで共通している。日本では量子計測の基礎的な研究において先駆的貢献がなされてきている。井元らは、光子数の量子非破壊測定（測定後の状態において測定結果の光子数が保存されている測定）を可能にするプロトコルを考案した[14]。小澤は重力波の検出への応用を考え、標準量子限界[15]を打破する測定法を発見した[16]。さらに、量子雑音の起源である量子不確定性関係[17]に対して新しい不等式を導入した[18]。北川と上田は、スピンのスクイーズド状態[19]による量子雑音の圧搾とそれを利用した標準量子限界を超える感度の向上を提案した[20]。北川と上田の研究は、Yuen による光のスクイーズド状態による理論的成果とともに[21]、米国物理学会誌 *Physical Review A*（原子、分子、光に関する物理学、量子情報科学等を扱う）の 50 周年を記念する 26 本のマイルストーン論文に日本から唯一選ばれた[22]。

---

⑬　T. D. Ladd et al., “Quantum computers,”*Nature*, Vol.464, 2014.3.4, pp.45-53;.Elizabeth Gibney, “Physics: Quantum computer quest,” *Nature*, Vol.516, 2014.12.3, pp.24-26.

⑭　N. Imoto et al., “Quantum nondemolition measurement of the photon number via the optical Kerr effect,” *Physical Review A*, Vol.32 Iss.4, 1985.10, pp.2287-2292.

⑮　光位相の測定精度は、その光に含まれる光子数（すなわち光の強度）n に対して $1/\sqrt{n}$ が限界であるとされていた。

⑯　M. Ozawa, “Measurement breaking the standard quantum limit for free-mass position” *Physical Review Letters*, Vol.60 Iss.5, 1988, 385; J. Maddox “Beating the quantum limit (cont'd),” *Nature*, Vol. 331, 1988.2.18, p.559.

⑰　量子力学では位置と運動量が不確定になるが、その不確定性が満たすべき関係。

⑱　M. Ozawa, “Universally valid reformulation of the Heisenberg uncertainty principle on noise and disturbance in measurement,” *Physical Review A*, Vol.67 Iss.4, 2003.4, p.42105.

⑲　あるスピン成分の不確定性がコヒーレント状態よりも小さくなっている状態。

⑳　M. Kitagawa and M. Ueda, “Squeezed spin states,” *Physical Review A*, Vol.47 Iss.6, 1993.6, pp.5138-5143.

㉑　Horace P. Yuen, “Two-photon coherent states of the radiation field,” *Physical Review A*, Vol.13 No.6, 1976.6, pp.2226-2243.

㉒　“Physical Review A 50th Anniversary Milestones.” American Physical Society, Physical Review A website <https://journals.aps.org/pra/50th>

光のスクイーズド状態の生成は 1985 年頃に実験が成功し、今では米国の重力波干渉計 LIGO[23] の感度を 2 倍に増強できるまでに発展している[24]。また、竹内らは多光子の量子もつれ状態である N00N 状態[25] による量子標準限界の突破を世界に先駆けて実現した[26]。一方、スピンを用いたスクイーズド状態についても、イオントラップの系と原子気体系においても大規模なスピンスクイージングが達成されており[27]、今後更に有用な応用が開拓されるものと期待されている。

量子センシングデバイスの応用研究でも、日本は世界をけん引する立場に立っていると言えよう。香取らは原子気体 qubit を格子状に配置した光格子時計において、時計としての精密度の世界記録を保持し続けている（2021 年時点）[28]。現在は、この時計の精密度を利用して、重力の差[29]、すなわち、標高の差の精密センシングに用いるべく研究開発を進めている。東京スカイツリーに設置した光格子時計によりこの実証実験を行ったことは記憶に新しい（図 2）[30]。上妻や向山らは原子波干渉計[31] を用いて従来のレーザー干渉計よりも自己位置推定精度の高いジャイロスコープの研究開発を進めている[32]。海洋資源探索の効率化や、自動運転船舶、さらには衛星測位システムの使えないトンネル内での自動運転車の自己位置推定[33] などへの民生応用が期待されている。向山らは最近、電場により真空中にトラップ（捕捉）したイオンを三次元的に運動させる際に生じる物質波干渉の観測に世界で初めて成功し、イオンを用いたジャイロスコープの実現への重要な一歩を切り開いた[34]。もちろん海外でも、原子波干渉計の研究は進んでおり、2021 年には宇宙空間での応用を目指した無重力下での原子干渉実験が行われ、宇宙空間での応用への道が開かれた[35]。海外では軍事技術として非公開で研究開発が進む可能性があり、のちに民生用や基礎科学にこの技術を利用することが困難になるため、自前で基礎研究を行う必要があることが文部科学省量子科学技術委員会（第 6 回）で議論されている[36]。

⑵3　Laser Interferometer Gravitational-Wave Observatory. レーザー干渉計重力波観測所。2015 年に完成し、同年重力波の検出に成功した。2017 年のノーベル物理学賞は「LIGO 検出器への決定的貢献と重力波の観測」の業績により米国三氏に与えられた。“The Nobel Prize in Physics 2017.” Nobel Prize website <https://www.nobelprize.org/prizes/physics/2017/summary/>

⑵4　Yuhang Zhao et al., “Frequency-Dependent Squeezed Vacuum Source for Broadband Quantum Noise Reduction in Advanced Gravitational-Wave Detectors,” *Physical Review Letters*, Vol.124 Iss.17, 2020.5.1, p.171101.

⑵5　N 個の光子数状態と 0 個の光子数状態が重ね合わせられた量子もつれ状態。

⑵6　Tomohisa Nagata et al., “Beating the Standard Quantum Limit with Four-Entangled Photons,” *Science*, Vol.316 Iss.5825, 2007.5.4, pp.726-729.

⑵7　Justin G. Bohnet et al., “Quantum spin dynamics and entanglement generation with hundreds of trapped ions,” *Science*, Vol.352 Iss.6291, 2016.6.10, pp.1297-1301; Han Bao et al., “Spin squeezing of 1011 atoms by prediction and retrodiction measurements,” *Nature*, Vol.581, 2020.5.14, pp.159-163.

⑵8　高本将男・香取秀俊「光格子時計を用いた高精度時空間計測」根来監修　前掲注⑴, pp.183-192.

⑵9　重力の強い場所ほど時間の流れが遅くなる。

⑶0　東京大学ほか「18 桁精度の可搬型光格子時計の開発に世界で初めて成功～東京スカイツリーで一般相対性理論を検証」2020.4.7. 科学技術振興機構ウェブサイト <https://www.jst.go.jp/pr/announce/20200407/>

⑶1　原子の波の性質を利用した干渉計。

⑶2　「技術テーマ「自己位置推定機器の革新的な高精度化及び小型化につながる量子慣性センサー技術」」科学技術振興機構ウェブサイト <https://www.jst.go.jp/mirai/jp/program/large-scale-type/theme03.html>

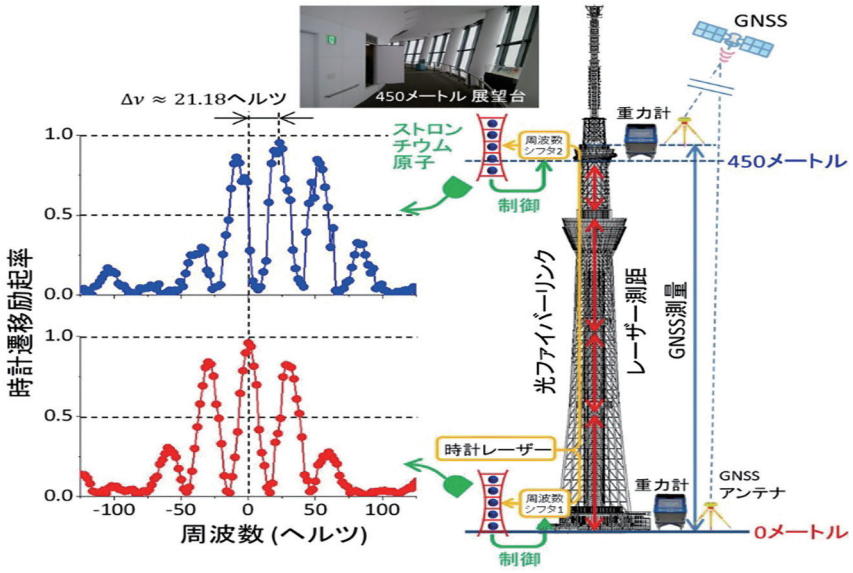
⑶3　「量子慣性センサー」東京工業大学理学院物理学系上妻研究室ウェブサイト <http://www.kozuma.phys.titech.ac.jp/research_category/entry15.html>

⑶4　Ami Shinjo et al., “Three-dimensional matter-wave interferometry of a trapped single ion,” *Physical Review Letters*, Vol.126 Iss.15, 2021.4.16, p.153604. <https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.126.153604>

⑶5　Maike D. Lachmann et al., “Ultracold atom interferometry in space,” *Nature Communications*, Vol.12, No.1317, 2021.2.26. <https://doi.org/10.1038/s41467-021-21628-z>

⑶6　中川賢一「冷却原子を用いた原子干渉計慣性センサーの最近の研究動向」（文部科学省科学技術・学術審議会先端研究基盤部会　量子科学技術委員会（第 6 回）配布資料 2-3）2016.10.7. <https://warp.ndl.go.jp/info:ndljp/pid/11293659/www.mext.go.jp/b_menu/shingi/gijyutu/gijyutu17/010/shiryo/__icsFiles/afieldfile/2017/01/13/1381050_003.pdf>

図２　光格子時計実験



（出典）「１８桁精度の可搬型光格子時計の開発に世界で初めて成功～東京スカイツリーで一般相対性理論を検証～」<https://www.t.u-tokyo.ac.jp/shared/press/data/setnws_20200407140138283045523 5_287172.pdf> より、東京大学大学院工学系研究科香取秀俊教授の許可を得て転載。

ダイヤモンドの NV 中心[37]を用いたスピンqubit センシングデバイスは世界中で幅広く研究が行われているが、量子科学技術研究開発機構（QST）、産業技術総合研究所、筑波大学が作成したデバイスが世界中で用いられている。Wrachtrup らは低温環境下でペンタセンの単一分子での光検出磁気共鳴を実現した[38]。その後、室温下でダイヤモンドの NV 中心においてもそれが可能であることを示した[39]。ダイヤモンドはその安定性から、ナノ粒子や薄膜としても頑丈で使い勝手が良く、固体センシングデバイスとして使えるため研究が進んだ。荒井らは、固体センシングデバイスに近接した単一磁気バクテリアのイメージングに成功しており[40]、DARPA の QuASAR（Quantum-Assisted Sensing And Readout）プロジェクトにおいて最も重要な成果の一つとして紹介されている[41]。2016 年には、固体センサ表面に付着した単一蛋白質の NMR（核磁気共鳴）分光が実現した[42]。日本でも東工大の波多野ら[43]、また QST の馬場や大島らによって大規模プロジェクトが進められている。QST では生命のセンシングに的を絞って、細胞内の pH や温度のセンシングといった生物実験を次々と成功させている（図 3）[44]。

(37)　人工的に作られたダイヤモンド結晶の格子にある炭素原子の一つを窒素原子に、隣接する炭素原子を空孔としたもの。

(38)　J. Wrachtrup et al., “Optical detection of magnetic resonance in a single molecule,” *Nature*, Vol.363, 1993.5.20, pp.244-245. <https://doi.org/10.1038/363244a0> 光検出磁気共鳴とは、スピン状態間のマイクロ波帯の遷移を光によって間接的に検出することを指す。光はマイクロ波に比べ非常に高い感度での検出が可能であり、これにより微小な領域の磁気をセンシングできるようになる。

(39)　A. Gruber et al., “Scanning Confocal Optical Microscopy and Magnetic Resonance on Single Defect Centers,” *Science*, Vol.276 Iss.5321, 1997.6.27, pp.2012-2014.

(40)　D. Le Sage et al., “Optical magnetic imaging of living cells,” *Nature*,Vol.496, 2013.4.24, pp.486-489. <https://doi.org/10.1038/nature12072>

(41)　“Quantum-assisted Nano-imaging of Living Organism Is a First,” 2013.5.2. DARPA website <https://www.darpa.mil/news-events/2013-05-02>

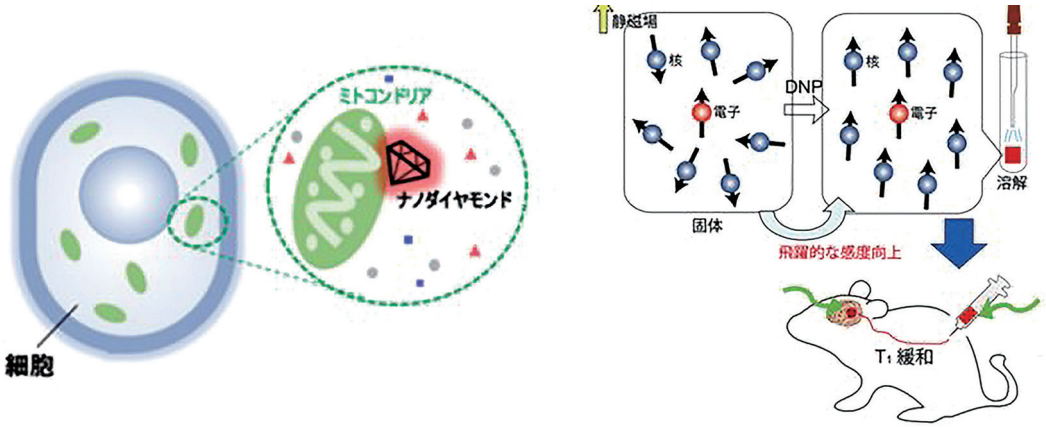
(42)　I. Lovchinsky et al., “Nuclear magnetic resonance detection and spectroscopy of single proteins using quantum logic,” *Science*, Vol.351 Iss.6275, 2016.2.19, pp.836-841.

(43)　波多野睦子「固体量子センサの可能性」根来監修　前掲注(1), pp.11-26.

(44)　「Q-LEAP 量子生命 Flagship プロジェクトについて」量子科学技術研究開発機構ウェブサイト <https://www.qst.go.jp/site/qlsrh/46837.html>; Takahiro Fujisaku et al., “pH Nanosensor Using Electronic Spins in Diamond,” *ACS Nano*, Vol.13 No.10, 2019.9.20, pp.11726-11732. <http://dx.doi.org/10.1021/acsnano.9b05342>

Wrachtrup らと同時期にペンタセンの単一分子光検出磁気共鳴を実現した Schmidt らは、ペンタセンによる室温下での核スピン高偏極化実験[45]を進めた[46]。のちに、日本に技術が輸入され、飯沼らが 77K（－ 196℃）において約 30％の偏極率を達成する[47]。そして、筆者らは室温で 34% の偏極率を達成し、本技術を「室温超偏極」と銘打った[48]。核スピンの高偏極化技術は超高感度 NMR 分光を可能にするため、現在、創薬スクリーニングへの応用研究が進んでいる。また、超高感度 MRI によって抗がん剤の治療効果判定を劇的に短縮する技術としても期待されている[49]。従来の高偏極化法は 1K（－ 272℃）程度の極低温を使うものであり装置が大型のものとなり普及が難しかったが、量子技術により室温で行うことが可能となり、医療分野への応用を目標として筆者らは動物実験を進めている（図 3）。室温超偏極に関しては、ドイツや米国、オーストラリアでも NV 中心を用いた研究が進められてきている[50]。筆者らも五十嵐や大島らと協力して NV 中心での室温超偏極に成功すると[51]、ドイツのベンチャー企業を含むチームはペンタセンの超偏極に成功しており、競争が激化している[52]。

図３　スピン qubit を用いた量子センシング



（出典） 図左：量子科学技術研究開発機構量子生命科学研究所五十嵐龍治氏より提供、図右：筆者作成。

---

(45)　核スピンの磁場に対する揃い具合を示す偏極率を向上させる実験。

(46)　A. Henstra et al., “High dynamic nuclear polarization at room temperature,” *Chemical Physics Letters*, Vol.165 Iss.1, 1990.1.5, pp.6-10.

(47)　M. Iinuma et al., “High Proton Polarization by Microwave-Induced Optical Nuclear Polarization at 77 K,” *Physical Review Letters*, Vol.84 No.1, 2000.1.3, pp.131-174; Sarah Tomlin, “More spins for protons,” *Nature*, Vol.403, 2000.1.13, p.151. <https://doi.org/10.1038/35003090>

(48)　Kenichiro Tateishi et al., “Room temperature hyperpolarization of nuclear spins in bulk,” *PNAS*, Vol.111 No.21, 2014.5.27, pp.7527-7530. <https://doi.org/10.1073/pnas.1315778111>; 根来誠「室温超偏極量子符号化センサ　量子技術による NMR/MRI 高感度化」根来監修　前掲注(1), pp.93-104.

(49)　Sam E. Day et al., “Detecting tumor response to treatment using hyperpolarized 13 C magnetic resonance imaging and spectroscopy,” *Nature Medicine*, Vol.13, 2007.10.28, pp.1382-1387. <https://doi.org/10.1038/nm1650>

(50)　Q. Chen et al., “Optical hyperpolarization of 13C nuclear spins in nanodiamond ensembles,” *Physical Review B*, Vol.92, 2015.11.18, p.184420. <http://dx.doi.org/10.1103/PhysRevB.92.184420>; Ashok Ajoy et al., “Orientation-independent room temperature optical 13C hyperpolarization in powdered diamond,” *Science Advances*, Vol.4 Iss.5, 2018.5.18, p.5492. <https://doi.org/10.1126/sciadv.aar5492>; David A. Broadway et al., “Quantum probe hyperpolarisation of molecular nuclear spins,” *Nature Communications*, Vol.9 No.1246, 2018.3.28. <https://doi.org/10.1038/s41467-018-03578-1>

(51)　Koichiro Miyanishi et al., “Room-temperature hyperpolarization of polycrystalline samples with optically polarized triplet electrons: pentacene or nitrogen-vacancy center in diamond?” *Magnetic Resonance*, Vol.2 Iss.1, 2021.2.17, pp.33-48. <https://doi.org/10.5194/mr-2-33-2021>

(52)　Tim R. Eichhorn et al., “Hyperpolarized solution-state NMR spectroscopy with optically polarized crystals,” arXiv:2108.06147. <https://arxiv.org/abs/2108.06147>

光格子時計、慣性センサ、NV 固体量子センサ、室温超偏極技術は、EU の研究開発プログラム Quantum Flagship の量子センシング分野において支援されており[53]、日本でも科学技術振興機構（JST）の未来社会創造事業と文部科学省の光・量子飛躍フラッグシッププログラム（Q-LEAP）の「Flagship プロジェクト」において支援されている。さらに、Q-LEAP の「基礎基盤研究」、JST の戦略的総合研究推進事業「CREST」、同「さきがけ」の量子機能領域及び量子生体領域において、光 qubit を用いたセンシング、超伝導 qubit を用いたセンシングなどの多岐にわたるシーズへの支援が行われている[54]。これら政府による投資は、日本における量子センシング研究の多様性や、日本の研究が世界的な貢献を果たすことに寄与していると言ってよいであろう。研究の一層の発展が今後も期待される。

執筆：大阪大学量子情報・量子生命研究センター（QIQB）准教授　根来（ねごろ）　誠（まこと）

⑸3　EU Quantum Flagship website <https://qt.eu/>

⑸4　「光・量子飛躍フラッグシッププログラム (Q-LEAP)」科学技術振興機構ウェブサイト <https://www.jst.go.jp/stpp/q-leap/>;「量子状態の高度な制御に基づく革新的量子技術基盤の創出」同 <https://www.jst.go.jp/kisoken/crest/research_area/ongoing/bunyah28-2.html>;「量子の状態制御と機能化」同 <https://www.jst.go.jp/kisoken/presto/research_area/ongoing/bunyah28-2.html>;「量子技術を適用した生命科学基盤の創出」同 <https://www.jst.go.jp/kisoken/presto/research_area/ongoing/bunyah29-1.html>

Ⅳ　量子通信・ネットワーク―量子鍵配送から量子インターネットまで―

はじめに

ここでは、これまで解説されてきた量子コンピュータ、量子シミュレータ、量子センシングをつなぐ量子通信・ネットワークに関して解説する。第 1 章でも述べたとおり、量子暗号通信は最もインパクトのある応用である。まず、量子鍵配送を含む量子通信及びネットワークに関する研究の概観を述べ、それらを量子コンピュータ、量子シミュレータ、量子センシング含め、一体的に運用する構想である量子インターネットを解説する。また、量子暗号の一つである量子鍵配送に関しては、その動作原理を述べる。

1　量子通信・ネットワークの概略

量子 2.0 と呼ばれる量子情報技術の発展において、量子通信(1)のプロトコルは常に先鞭の役割を果たしてきた。その始まりは、1984 年のベネット（Charles H. Bennett）とブラッサール（Gilles Brassard）が提案した量子鍵配送(2)（量子暗号通信）(3)のプロトコル（BB84）である(4)。その後に、量子もつれ(5)を利用した E91 や BBM92 などの量子鍵配送プロトコルが発見された(6)。量子 2.0 のコアである量子もつれの万能性は、深く研究され、古典通信の限界を超えて通信容量を増大させる超稠密通信(7)や量子状態を転送する量子テレポーテーション(8)といった通信の原理限界(9)を与える基本プロトコルが次々と発見された。同時に、1990 年代から光子の量子状態（量子情報）を送信する実験室での実験が行われるようになり、2000 年代になり敷設された光ファイバー網での量子通信実験や望遠鏡を利用した空間伝搬による光通信を利用した量子通信実験が盛んに行われた。黎明期から約 30 年を経た現在では、地球を周回する人工衛星から配信した量子もつれの光子対を利用する量子テレポーテーション(10)や、衛星と地上の光ファイバー網を利用して数千 km もの量子暗号通信（量子鍵配送）を実現するに至って

＊　本稿におけるインターネット情報の最終アクセス日は、令和 4（2022）年 2 月 25 日である。

(1)　量子ビットを送受信する通信は量子通信と呼ばれる。現代のデジタル通信を含めビット値のみの送受信を行う通信は、その対比として古典通信と呼ばれる。これは量子力学より前の物理学を古典物理学と呼ぶ慣習に沿った呼び方であり、量子 1.0 と量子 2.0 の違いを明確にするためによく用いられる。

(2)　暗号技術の一つである秘密鍵配送を量子通信によって実現する方法を指す。これにより、原理的に盗聴不可能なセキュア通信が実現する。量子コンピュータでも盗聴はできない。以下の節で詳しく解説する。

(3)　量子暗号は量子鍵配送を含む量子通信を利用する暗号技術全般を指す。ただし、量子鍵配送によるセキュア通信を指して利用される場合も多い。

(4)　Charles H. Bennett and Gilles Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984, pp.175-179.

(5)　離れた量子ビットの間の量子力学特有の相関を指す。古典通信だけでは量子もつれの相関を作ることは原理的にできないため、量子 2.0 に特徴的な性質である。

(6)　Nicolas Gisin et al., “Quantum cryptography,” *Reviews of Modern Physics*, Vol.74 Iss.1, 2002.1-3, pp.145-190.

(7)　量子もつれを利用することで、1 量子ビットの量子通信で 2 ビット送信が可能になる方法。C. H. Bennett and S. J. Wiesner, “Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states,” *Physical Review Letters*, 69(20), 1992.11.16, pp.2881-2884.

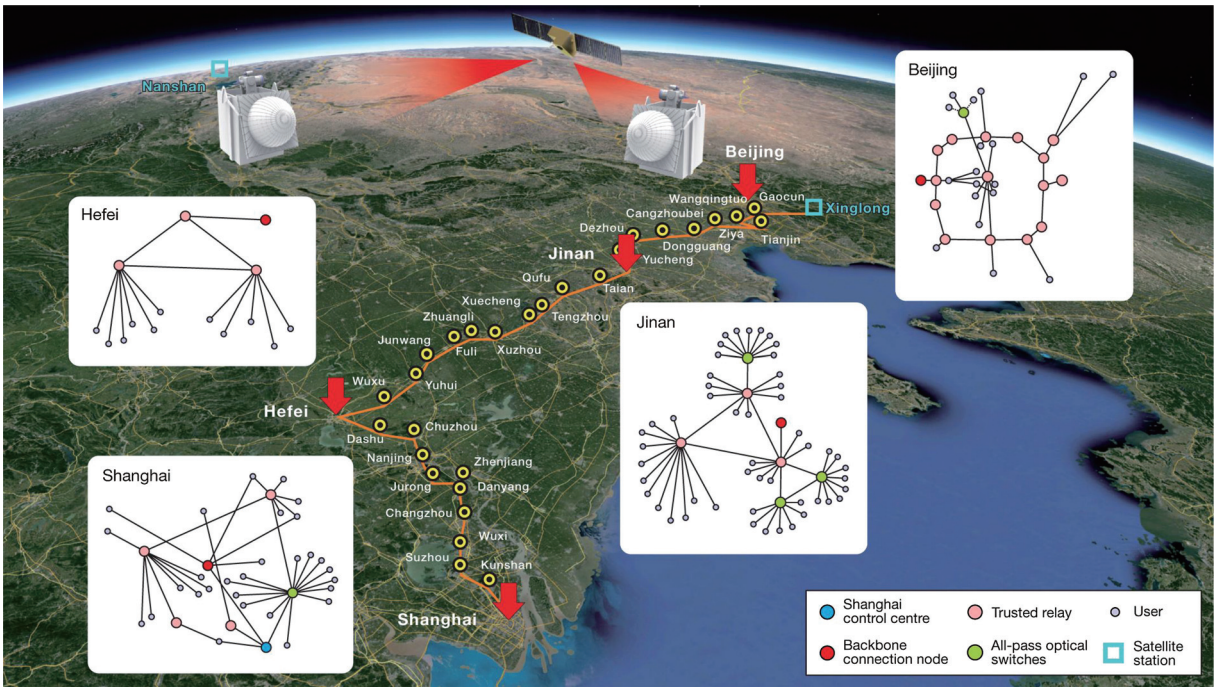
(8)　量子もつれを利用することで、古典通信によって量子ビットの状態を遠隔地へ転送する方法。Charles H. Bennett et al., “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” *Physical Review Letters*, 70 (13), 1993.3.29, p.1895.

(9)　理論的には、量子通信は古典通信を含むため、量子通信の原理限界が一般的な通信の原理限界を与える。

(10)　Gabriel Popkin, “China's quantum satellite achieves ‘spooky action' at record distance,” *Science*, 2017.6.15. <https://doi.org/10.1126/science.aan6972>

いる（図 1 参照）[11]。また、最新のプロトコル[12]を利用した 830km の光ファイバーでの実証実験も行われた[13]。今後は、実用化がさらに進み、いずれは地球規模のグローバルな量子通信・ネットワークが実現し、現在のインターネットの量子版である量子インターネットが実現すると考えられている。

図 1　最新の量子通信実験



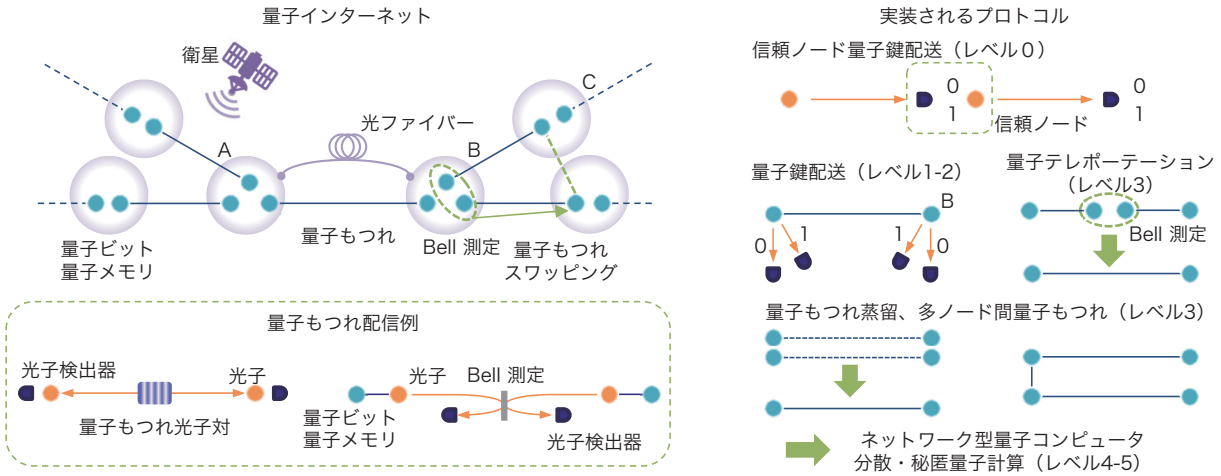
（出典）Yu-Ao Chen et al., “An integrated space-to-ground quantum communication network over 4,600 kilometres,” *Nature*, Vol.589, 2021.1.6, pp.214-219. Springer Nature 社の許諾を得て転載。

量子インターネットの最終形は、現在のようにコンピュータやセンサがインターネットに接続し連携して動作する大規模なネットワーク型コンピュータの量子版（ネットワーク型量子コンピュータ）である。図 2 に示すように、量子インターネットのネットワーク上の各ノード（結節点）に配置された量子コンピュータや量子センサなどの量子デバイスは、量子もつれによりつながる。この量子もつれは、量子通信により配られる。このように、量子もつれによりつながった量子デバイス群によって構成される量子インターネットは一つの量子コンピュータとしても動作し、量子テレポーテーションを駆使した様々な量子プロトコルを実現できる万能性を有している[14]。ネットワーク上の任意のノード（結節点）間で量子暗号通信（量子鍵配送）を行うことも当然可能である。実は、量子インターネットの空間的な距離を縮めて、一つの量子デバイスに押し込めると、それは量子コンピュータそのものである。そのため、量子コンピュータ内に形成される量子ネットワークを量子インターネットと呼ぶこともある。このような量子コンピュータ内のネットワークに関する研究は、本章第Ⅰ節の量子コンピュータに包

(11)　Yu-Ao Chen et al., “An integrated space-to-ground quantum communication network over 4,600 kilometres,” *Nature*, Vol.589, 2021.1.6, pp.214-219.
(12)　Marcos Curty et al., “A quantum leap in security,” *Physics Today*, 74(3), 2021.3, p.36.
(13)　Shuang Wang et al., “Twin-field quantum key distribution over 830-km fibre,” *Nature Photonics*, Vol.16, 2022, pp.154-161.
(14)　量子通信・ネットワークにおいては、量子状態（情報）を送受信するチャンネルだけでなく、古典ビットを送受信するデジタル通信も併用する。

含されるため、以下では、空間的な距離の長い、量子インターネットに関して説明する。特に、今後の研究開発の中心となる量子インターネットの研究開発動向を押さえつつ、現在、商用化が進んでいる量子鍵配送も含めて解説する。

図２　量子暗号通信を含めた量子インターネットの概念図



（注）　Bell 測定とは、２つの量子ビットの量子もつれを識別する測定。量子テレポーテーション、量子中継、ネットワーク型量子コンピュータを可能にする量子インターネットの要である。
（出典）筆者作成。

２　量子インターネット構想

現在のインターネットは 1969 年に実証された米国国防総省高等研究計画局（Defense Advanced Research Projects Agency: DARPA）の ARPANET が始まりとされており、そこから現在のグローバルなネットワークへ発展し、サイバー空間を支えている[15]。50 年目のタイミングで、グローバルな量子ネットワークとしての量子インターネット構想が披露されている[16]。量子インターネットという考え方はそれ以前から自然な形で受け入れられていたが[17]、ローカルかグローバルかといったネットワークの空間的な大きさに関してはあまり意識されていなかった。現在の量子インターネット構想は、インターネットと同様にノード間距離が長く、規模の大きい量子ネットワークを指すことが多い。量子インターネット構想では、自動運転などと同様に、可能なタスクに応じて、必要となる量子インターネット上の各ノードの技術レベルにより、レベル分けがされている[18]。各レベルを以下に要約する。高レベルのノード技術は、低レベルのノード技術を包含するため、基本的に高レベルインターネットは低レベルインターネットの機能を包含する。ただし、通信速度などの別の指標では必ずしもそうではない。

(15)　「インターネットの歴史」Yahoo! JAPAN ウェブサイト <https://history-of-the-internet.yahoo.co.jp/>;「インターネット歴史年表」日本ネットワークインフォメーションセンターウェブサイト <https://www.nic.ad.jp/timeline/>
(16)　Stephanie Wehner et al., “Quantum internet: A vision for the road ahead,” *Science*, 362(6412), 19 Oct 2018, p.303; Executive Office of the President of the United States “A Strategic Vision for America's Quantum Networks,” 2020.2. National Quantum Initiative website <https://www.quantum.gov/wp-content/uploads/2021/01/A-Strategic-Vision-for-Americas-Quantum-Networks-Feb-2020.pdf>
(17)　H. J. Kimble, “The quantum internet,” *Nature*, Vol.453, 2018.6.19, pp.1023-1030.
(18)　Wehner et al., *op.cit.*(16)

レベル 0：信頼ノード（Trusted node）[19] では古典ビットのみを保存するもの。以下で解説する普及段階に来ている量子暗号通信（量子鍵配送）インフラに相当する。ネットワーク上の全てのノードにおいて量子ビットを古典ビットに変換し保存し、その古典ビットが第三者に漏洩しない信頼できる条件を満たした中間ノード（信頼ノード）を経由して、終端ノード間での量子鍵配送を実現するレベル[20]。

レベル 1：量子ビットの状態が終端ノードに送信され、測定されるもの。レベル 0 における信頼ノードが中間ノードとして存在しないため、量子ビットの状態のまま終端ノードに送信できるレベル。応用例として、量子鍵配送を含めた量子暗号プロトコルなど。

レベル 2：終端ノード間に量子もつれ生成を実現するもの。ユーザのみでセキュリティを確認できる量子鍵配送プロトコルなど。

レベル 3：終端ノード間の量子もつれ生成に加えて、各ノード内での量子ビットの演算（操作）が可能なもの。ノード内での量子ビットの演算が可能になることで、秘匿量子計算[21]、秘密分散量子暗号[22]、リーダー選挙、超長基線望遠鏡[23]、時計同期等への応用が可能になる。

レベル 4：少数の論理量子ビットに対する誤り耐性量子ゲート操作[24]を実現するもの。分散量子計算などのネットワーク型量子コンピュータとしての機能を持つ。

レベル 5：多数の論理量子ビットに対する誤り耐性量子ゲート操作を実現するもの。任意の量子アルゴリズムが実装可能なネットワーク型量子コンピュータとしての機能を持つ。

技術として既に存在し、それを基にインフラとして導入できるレベルにあるものが、レベル 0 である。レベル 1 は中間ノードが存在しない又は中間ノードが一つ程度の短中距離通信であれば、技術として存在している。この二つのレベルの技術は、既に一定程度確立しており、実用段階にするための技術開発やパフォーマンス向上のための技術開発が主となる。特に、レベル 0 に関しては、既に民間セクターでのサービス提供が予定される段階であり、標準化も着実に進んでいる。

レベル 2 は未開拓な要素技術が多くあり、科学技術としての基礎研究が重点的に行われている段階である。実証できる程度の技術フェーズに到達した要素技術は、レベル 0 と 1 のインフ

---

⑲　量子鍵配送はランダムなビット列を光子の状態に符号化して送信するが、その途中のノードで光子の状態を測定してビット列に復号化して、再送する場合がある。主に中継やルーティングのために行われるが、一旦、ビット列に復号化すると、いくらでもコピーできる古典情報となるので、量子鍵配送としてのセキュリティは担保できない。セキュリティを担保できるためには、この途中のノードは送信者と受信者にとって、第三者に侵害されない信頼できるノードである必要がある。このような中間ノードを信頼ノードと呼んでいる。一方で、量子インターネットの高レベルでは、この中間ノードも量子プロセッサによって動作させるため、原理的に第三者に侵害されない状況が達成できる。

⑳　信頼ノードからの情報漏えいは量子鍵配送では想定されていないため、量子暗号としての安全性は低い。一方、実用化は容易になる。

㉑　量子コンピュータの所有者（管理者）に計算内容を知られずに、ユーザが量子計算を量子コンピュータ上で実行するプロトコル。クラウド量子コンピュータの利用法の一つ。

㉒　秘密分散プロトコルの量子版。秘匿したい量子情報を複数ユーザでシェアするが、個々のユーザだけでは元の量子情報を復元できず、十分な数のユーザが協力すれば元の量子情報を復元できる。

㉓　離れた望遠鏡間の相関を利用して観測する方法。量子もつれによる高解像度化のプロトコルが提案されている。

㉔　量子ゲートに対する誤り確率が一定のしきい値を下回れば、それを用いて任意の精度の量子計算が可能になる。そのような量子ゲートを誤り耐性量子ゲートと呼ぶ。Michael. A. Nielsen and Isaac. L. Chuang, *Quantum Computation and Quantum Information*, 2d ed., Cambridge: Cambridge University Press, 2010, pp.482-488.

ラに導入し、フィールドテストが実施され、レベル 2 相当であることが実証されている。レベル 3 は最先端の科学技術の領域であり、サイエンスとしての研究が主である。インフラへの導入自体もサイエンスとして研究されている。

レベル 4 と 5 は中長期的計画があり、研究が始まったばかりである。レベル 3 までの技術からの更なる飛躍が必要な技術が多くあり、中長期的なサイエンスとしての研究が必要である。

各国のプロジェクトはおおむね上記の量子インターネット構想に含まれる応用先である量子コンピュータネットワーク、量子セキュリティ通信、量子センサネットワークを包含する。米国ではエネルギー省（Department of Energy: DOE）を中心に、Quantum Internet Blueprint が 2020 年に取りまとめられた[25]。この計画では、今後 10 年程度で、世界規模の量子インターネットのプロトタイプが実現することを念頭に研究方針がまとめられており、各国のプロジェクトとも歩調を揃えている。これを基に、2021 年 6 月 8 日に連邦議会上院で米国イノベーション・競争法案（The United States Innovation and Competition Act of 2021）が可決された。この法案には量子ネットワークインフラ・労働力開発法案（Quantum Network Infrastructure and Workforce Development Act of 2021）が含まれ、本法案が制定されれば 2022 年から 2026 年までに年間 2000 万ドルの予算が確保される見込みである[26]。日本国内では各省庁が所管する従来の専門領域に連動してプロジェクトが別れており、総務省ではレベル 0 を中心とした量子セキュリティ通信のプロジェクトがあり、文部科学省では量子コンピュータ開発の一部として、ネットワーク型量子コンピュータが研究されている（「ムーンショット型研究開発事業」として実施）。これに対して産学官連携コンソーシアム「量子インターネットタスクフォース」（QITF）は、包括的な研究プロジェクトを提言している[27]。

量子インターネットのネットワーク階層は、従来のインターネットで使われている通信プロトコルである TCP/IP と対比して議論されている。図 3 のように、TCP/IP と同様に最下位層から物理層（physical）、データリンク層（data link）、ネットワーク層（network）、トランスポート層（transport）、そして、最上位層のアプリケーション層（application）から成る。量子インターネットの物理層は、全ての量子デバイス（プロセッサやメモリ等）と光ファイバーを含み、量子情報を生成、操作、測定し、タイミングの同期等を実現する。データリンク層は物理層を動かす役割を担い、離れた量子ノード間に量子もつれを作り出す操作を実施する。この際、上位層からデータリンク層に要求を受け付ける。ネットワーク層は、光ファイバー等で直接接続されていないノード間（近接ノードでない）を量子もつれスワッピングにより、長距離量子もつれを生成する役割を担う。トランスポート層は、量子テレポーテーションを使用して量子ビットを確実に送信する役割を担う。アプリケーション層では、アプリケーションが従来のネットワーク機能と量子ネットワーク機能の両方を利用可能であり、任意の量子暗号プロトコル、分散量子計算、量子センサネットワーク等のプロトコルが実装される。現状では、各層毎の研究開発とはなっておらず、オーバーラップが大きいため、最下位の物理層（本章第Ⅲ節で述べる）

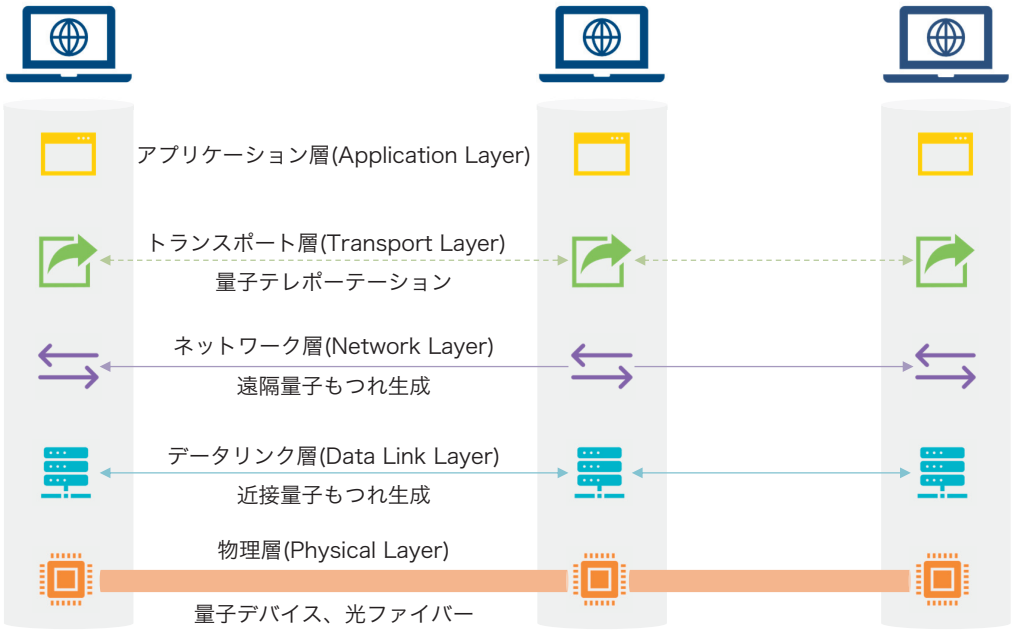
⑵5　Nicolas Peters et al., *From Long-distance Entanglement to Building a Nationwide Quantum Internet: Report of the DOE Quantum Internet Blueprint Workshop*, 2020.2.1. Office of Scientific and Technical Information, Department of Energy website <https://www.osti.gov/servlets/purl/1649002>

⑵6　“S.1260 - United States Innovation and Competition Act of 2021,” U.S. Senate, 117th Cong. <https://www.congress.gov/bill/117th-congress/senate-bill/1260/text>

⑵7　産官学連携研究開発コンソーシアム量子インターネットタスクフォース「ホワイトペーパー “The” 量子インターネット―この宇宙の物理法則に許されるサイバー空間の極致―」2021.2.22. <https://qitf.org/files/20210210_qitf_whitepaper.pdf>

と最上位のアプリケーション層の両端を中心に、以下で紹介する。中位層は量子コンピュータ研究におけるミドルウェア開発と深く関連があり、物理層とアプリケーション層の開発に合わせて進むと考えられる。

図３　量子インターネットのネットワーク階層



（出典）筆者作成。

量子インターネットのアプリケーションは大きく分けて、以下の三つが考えられ、新しいアプリケーションの創出も求められている。

①量子センサネットワーク：原子時計などの量子クロックのネットワークは注目され、研究対象となっているアプリケーションである。量子技術による望遠鏡のネットワークも高精度化に寄与する。

②ネットワーク型量子コンピュータ：量子コンピュータの量子ネットワーキングは、古典システムを仲介しないネットワーク型量子コンピュータを実現する。また、分散量子コンピューティングは、量子ネットワークを介して多数の小さな量子コンピュータを接続し、単一の量子コンピュータでは不可能な規模の計算能力を提供する。さらに秘匿計算などの任意の量子アルゴリズムを実現する。例えば、ブラインド量子コンピューティング（Blind Quantum Computing[28]）であり、秘匿量子計算が可能となる。

③量子暗号：信頼ノードのない量子インターネットは、量子コンピュータを含むあらゆる盗聴法に対してセキュリティ通信を実現する量子暗号通信（量子鍵配送）を可能にするもので、いわゆるキラーアプリケーションとなりうる。これをいち早く利用するのは、国家安全保障、銀行、エネルギー供給インフラなどの分野である。また、医療サービス、政府サービスのセキュリティ（例：選挙）、ゲームなども含まれる。

---

(28)　Joseph F. Fitzsimons, “Private quantum computation: an introduction to blind quantum computing and related protocols,” *npj Quantum Information,* Vol.3 No.23, 2017.6.15. <https://doi.org/10.1038/s41534-017-0025-3>

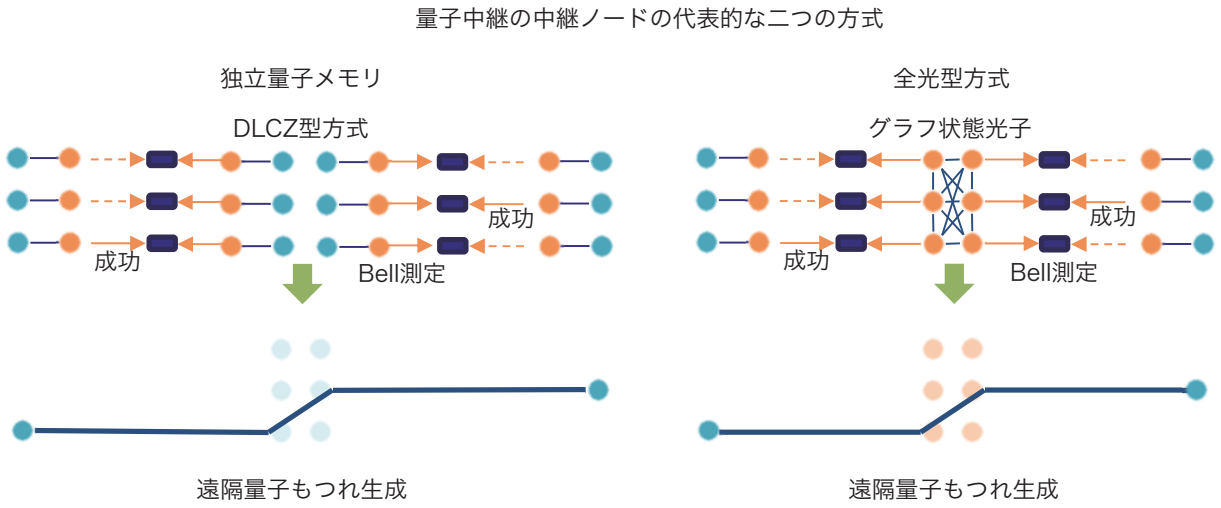
3　量子ネットワーク技術開発動向

量子インターネットのネットワーク階層において、物理層のノード技術が前述の量子インターネットのレベルに直結し、その開発スピードが高レベルネットワークへの進展に大きく関与するため、ここでは物理層を中心に技術開発動向を述べる。物理層には多数の量子ビットが用意され、その量子状態（量子情報）を保持するための量子メモリ、量子ビット間の演算、量子ビットの測定が組み込まれる。そして、最も重要な機能として、量子状態を光により送信するために量子ビットの状態を光子に転送又は量子ビットと光子の量子もつれを生成する量子インターフェースが必要である。現状で全ての機能を包含したものはないが、複数の機能を有した量子デバイスの研究開発が実施されている。

量子ビットの準備、メモリ、演算、測定を含む量子プロセッサは、量子コンピュータの構成要素でもあるため、量子コンピュータの開発と重複する部分が多い。量子インターネット研究では量子ネットワークに特化する方向での研究開発が多いが、量子コンピュータへの応用も可能である。量子プロセッサ（量子コンピュータ）の実装方法が様々であるため、量子インターフェース技術も様々に検討されている。

量子インターネットにおける最大の課題は、光子を送信する際に、光子の損失によって量子情報が失われてしまう点である。光子損失は、通信距離に対して指数関数的に増大するため、光ファイバー通信において、信頼ノードを置いて中継を行わない場合は、通信距離は数百 km が限界となる。この光子損失を劇的に低減するアーキテクチャとして量子状態を保持したまま中継を行う量子中継の技術が研究されている。図 4 に示すように、量子中継には、各ノードの物理層における適切な量子プロセッサ（量子メモリを含む）の動作と物理層より上位層であるトランスポート層まで含めた実装が必要となる。当然ながら、現在の実現している信頼ノードでは、保存できるのは古典ビットのみであるため、量子中継はできない。

図４　量子中継を含めた各ノードにおける物理層の要素技術



（出典） 筆者作成。

重要な量子デバイスや技術の例として、次のようなものが挙げられる。

・量子限界[29]の性能を持つ検出器（光子検出器等）、超低損失光チャネル（光ファイバーやインターコネクト技術）、衛星を含む空間光学系と地上ネットワークの接続技術
・量子もつれ光源とその伝送、制御、測定技術
・光の空間、時間、波長（周波数）、内部自由度[30]等を利用する多重化量子通信技術
・量子メモリに対応する波長域、通信に対応する波長域、マイクロ波を含む量子コンピュータに関連した領域の量子状態の波長域を相互に変換する量子周波数変換技術
・可視光又は通信波長における光子の量子ビットと互換性のある量子メモリ及び量子中継等を行うための小規模量子コンピュータの開発
・これらを組み合わせた量子中継器を用いた長距離量子もつれ配送（地上及び衛星）による小規模及び大規模量子プロセッサ間の量子もつれベースの通信プロトコル実装

これらの要素技術を組み合わせて、量子インターネット構築に向けたマイルストーンとなるプロトタイプ又はテストベッドが考案されており、各国で逐次実現に向けた試みがなされている[31]。

4　量子暗号通信インフラ整備動向

量子暗号通信インフラは、量子暗号の中でも量子鍵配送（Quantum Key Distribution: QKD）に特化した通信インフラであり、要素技術が揃っており、実用に最も近く、急速にその整備が進められている。量子ビットの送受信は二者間で行われ、送信者及び受信者は最終的に量子ビットを測定して得られるビット値を記録して、秘密鍵として用いるため、量子ビットの測定を行うが、量子ビットを保存しないもので構成される。量子インターネット構想においてはレベル 0 に位置付けられるものが主であり、レベル 1 に相当するものも視野に入っている。このような量子暗号通信インフラで量子ビットを送受信する距離は最長でも数百キロメートル程度であり、それより長距離になる場合は、一旦ビット値にして保存し、再度、量子ビットにエンコードして送信することになる。そのため、保存したビット値に対するセキュリティは既存の技術で担保せざるを得ない点が課題である。レベル 0 が信頼できるノード（信頼ノード）のネットワークと呼ばれるゆえんである。

量子暗号通信インフラの整備は、現在の光ファイバー網を利用して構築する方向性、光衛星通信を利用して構築する方向性、さらにそれらを組み合わせた試みなどが行われている。最も有名な量子暗号通信インフラは、2016 年に実現した中国の北京 - 上海間を結んだ約 2,000km

---

⑵⑼　ここでは量子力学で達成可能な測定（精度）限界という意味で用いた。
⑶⑽　光では偏光や角運動量のような内部自由度を量子ビットとして用いることができる。
⑶⑴　米国：Department of Energy, “U.S. Department of Energy Unveils Blueprint for the Quantum Internet at ‘Launch to the Future: Quantum Internet’ Event,” July 23, 2020. <https://www.energy.gov/articles/us-department-energy-unveils-blueprint-quantum-internet-launch-future-quantum-internet>; オランダ：Quantum Delta website <https://quantumdelta.nl/>; 英国：“The UK Quantum Network.” Quantum Communications Hub website <https://www.quantumcommshub.net/research-community/about-the-hub/phase-2/work-package-1/>; 中国：Daniel Garisto, “China is pulling ahead in global quantum race, new studies suggest,” *Scientific American*, 2021.7.15. <https://www.scientificamerican.com/article/china-is-pulling-ahead-in-global-quantum-race-new-studies-suggest/>

の地上のネットワークである[32]。さらに、中国では量子衛星による量子暗号通信も実現し、それを北京 - 上海間とも連結し、全長数千 km のネットワークを構築している[33]。日本においては、2010 年に東京 QKD ネットワークが始動し、現在まで都内 4 か所を結んだネットワークが稼働している[34]。QKD のための装置開発が進んでおり、ID Quantique（スイス）や東芝など企業の参入が相次ぎ、各地で量子暗号通信インフラの整備が進む様相を呈している。最近では、野村ホールディングス、野村證券、NICT、東芝、NEC によって、ユースケース探索の一環として、大容量金融取引データの量子暗号による高秘匿通信・低遅延伝送の検証実験が行われた[35]。また、経済安全保障の観点からの議論も始まっている[36]。量子暗号通信インフラのうち、既存の通信のための光ファイバーネットワークは高レベルの量子インターネットにも流用可能である。一方、量子暗号装置の物理層は、高レベルの利用のためにはリプレースが必要である。ネットワーク階層の中位層から上位層に上がるにつれて、リプレースの度合いは下がることが期待される。

5　量子暗号

量子通信・ネットワークにおいて、重要とされているアプリケーションの一つがセキュア通信を担う量子暗号である[37]。広い意味での暗号プロトコルは様々なものが存在し、その量子版としての量子暗号が議論されている。現状では、その中でも、秘密鍵配送を担う量子鍵配送に関する研究が圧倒的多数である。そのため、量子暗号通信と言った場合に量子鍵配送を指していることが多い。また、現状の量子通信は量子鍵配送に特化したものが多く、全ての量子暗号プロトコルが実装できるわけではない。ここでは、量子鍵配送について解説し、その他の量子暗号プロトコルに関しては別の解説に譲ることにする[38]。量子インターネットが実現すれば、量子鍵配送を含め、どのような量子暗号プロトコルも実装することができる。

現在では、ペーパーテストや手紙など手書きのものを除くと、ほぼ全てのメッセージのやり取りはデジタル化されている。画像も含め、あらゆるメッセージはコンピュータ内で 0 と 1 からなるビット列で表現され、ビット列を送受信することで、メッセージをやり取りすることができる。このメッセージとそれを表すビット列は等価であり、平文と呼ばれるが、平文をそのまま送ってしまうと第三者に読まれてしまうので、秘密にしたいメッセージは平文から暗号化して暗号文にする必要がある。

暗号文には、二つの種類がある。第三者が①原理的に解読できないもの（情報理論的安全性）と②原理的には解読できるが、解読のための計算に非常に時間がかかり、実質的に解読できな

⑶2　Rachel Courtland, “China’s 2,000-km Quantum Link Is Almost Complete: The Beijing-Shanghai project will form the backbone of the nation’s quantum communications network,” 26 Oct 2016. IEEE Spectrum Website <https://spectrum.ieee.org/chinas-2000km-quantum-link-is-almost-complete>

⑶3　Chen et al., *op.cit.*⑴1

⑶4　M. Sasaki et al., “Field test of quantum key distribution in the Tokyo QKD Network,” *Optics Express*, 19(11), 2011, pp.10387-10409. <https://doi.org/10.1364/OE.19.010387>

⑶5　野村ホールディングスほか「大容量金融取引データの量子暗号による高秘匿通信・低遅延伝送の検証実験に成功」2022.1.14. <https://www.nomuraholdings.com/jp/news/nr/holdings/20220114/20220114.html>

⑶6　「経済安全保障法制に関する有識者会議（第 1 回）議事要旨」2021.11.26, p.6. 内閣府ウェブサイト <https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai1/gijiyousi.pdf>

⑶7　小芦雅斗・小柴健史『量子暗号理論の展開』（臨時別冊・数理科学 SGC ライブラリ　67）サイエンス社, 2008.

⑶8　同上; Feihu Xu et al., “Secure quantum key distribution with realistic devices,” *Reviews of Modern Physics*, Vol.92 Iss.2, 2020.4-6, pp.025002-1-025002-60.

いものである（計算量的安全性）。①の代表例が秘密鍵暗号方式であり、②の代表例が公開鍵暗号方式である。公開鍵暗号方式は現在のインターネットでも利用されており、現在のスーパーコンピュータをもってしても解読には宇宙の年齢を要すると考えられている(39)。しかし、新しいアルゴリズム（計算方法）や量子コンピュータに代表されるような想定外の超高速な計算機技術によって、解読のための時間が大幅に短縮されるおそれがある。例えば、現在の公開鍵暗号の一つである RSA 暗号で利用されている 2048 ビットの整数の素因数分解は、13436 量子ビットの能力を持つ量子コンピュータによって 177 日で実現可能となるとの試算もある(40)。現状ではこのような量子コンピュータの実現の目処はたっていないが、日本でも、内閣府のムーンショット型研究開発事業がムーンショット目標 6 で掲げるように、2050 年までの量子コンピュータの実現に向けて精力的に研究が行われている。

①の秘密鍵暗号方式には、超高速な計算機技術によって解読されることはないが、現在のデジタル通信では実現の見込みがなく、量子通信・ネットワークを使った秘密鍵配送である量子鍵配送が実現のための唯一の方法として開発が行われている。

秘密鍵暗号方式では、送信者と受信者が暗号化と複号化のための秘密鍵と呼ばれるランダムなビット列（乱数列）を共有する。a）この乱数列は送信者と受信者で同一であるが第三者は知らないこと、b）秘密鍵の長さは平文のビット列と同じ長さであること、c）暗号化のために利用した秘密鍵は再利用しないことという三つの条件を満たすとすると、暗号化は、平文と秘密鍵の各ビットごとの XOR 演算をすることによって簡単に実現される。暗号文は、インターネットなどを使って送信者から受信者に送信される。受信者は暗号文と秘密鍵の XOR 演算により復号化し元の平文を得る。この暗号文は、第三者に配られても解読できない。なぜなら、第三者は秘密鍵を知らないため、暗号文を復号化して元の平文にすることができない（平文が有意に判別できない）からである。

この秘密鍵暗号方式の課題は、秘密鍵を第三者に知られずに送受信者で共有する方法が存在するか、という点である。上記 a）～ c）の三条件にあるように、再利用ではセキュリティを保証できないために、秘密鍵の補給はセキュリティを確保するための重要な課題である。しかし、インターネット上での秘密鍵の補給はできない。なぜなら、秘密鍵をそのまま送れば、第三者に知られるし、暗号化するには、同じ長さの秘密鍵を消費してしまう。この場合、秘密鍵は一向に増えない。そこで、量子鍵配送の登場である。秘密鍵のビット列を量子ビット列に符号化（変換）して、量子ビット列を送り、それを測定してビット値を得ることで、秘密鍵のビット列を共有する。

量子通信で送る量子ビット列を盗聴される恐れがあるが、量子力学の性質から、盗聴されると秘密鍵となるビット列の一部にエラーが生じ、それにより、送受信者が後から盗聴に必ず気づくことができる。量子ビット列の盗聴に気づけば、送受信者は秘密鍵を破棄し、暗号文を送らなければ盗聴されることはない。盗聴者が盗聴するためには、暗号文を送ってもらう必要があるため、量子ビット列を盗聴することができないというジレンマに陥る。盗聴者がたとえ量子コンピュータを駆使した盗聴を考えても、気づかれてしまう。より実用的には、秘密鍵とな

(39)　Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, London: Fourth Estate, 1999.

(40)　Élie Gouzien, Nicolas Sangouard, “Factoring 2048-bit RSA Integers in 177 Days with 13436 Qubits and a Multimode Memory,” *Physical Review Letters*, 127(14), 2021.9.28, pp.140503-1-140503-6. <https://doi.org/10.1103/PhysRevLett.127.140503>

るビット列のエラーを見積もり、プライバシー増幅[41]を行うことで、盗聴された情報を必要なセキュリティレベルにまで落とした後に、秘密鍵として用いる。いずれにしても、盗聴者にとっては、できるだけ盗聴をしないことが最善の策となってしまうところが、量子暗号通信（量子鍵配送）の強力なところである。

おわりに

本節では、量子ビットの状態を遠隔地に送信し、様々なプロトコルを実装するための一般的な枠組みとして、最近注目を浴びている量子インターネットを中心に量子通信・ネットワークの研究開発動向をまとめた。通常の解説では、量子鍵配送を重点的に説明し、その先まで議論が及ばないことが多い。本調査報告書では量子情報技術全般を俯瞰することを目的にしているため、量子通信・ネットワークに関しても、最も広い枠組みである量子インターネットから解説することを試みた。量子センサや量子コンピュータを接続し構築される量子インターネットには光の量子技術や光と量子デバイスのインターフェース、量子中継を実現する量子プロセッサなど、様々な量子情報技術が絡んでおり、研究開発のフィールドとしても興味深い。量子鍵配送に関しては、実証実験や社会実装が最も進んでおり、学会誌のような専門誌だけではなく、様々な機関の報告書[42]やより一般のメディアでも度々解説されている[43]。最も歴史の長い量子情報技術であるため、その実装方法も多岐にわたっている[44]。最近では、開発の主体が企業に移っており、詳細な情報は入手困難になるとともに、安全保障や経済安全保障にも関連し始めているため、機密性も高まっている。

執筆：大阪大学大学院基礎工学研究科／
量子情報・量子生命研究センター（QIQB）教授　山本（やまもと）　俊（たかし）

⑷1）　盗聴者に一部漏洩したビット列を、公開通信も使って、短くすることで秘匿性を増幅する処理。
⑷2）　後藤仁「量子暗号通信の仕組みと開発動向」『金融研究』28(3), 2009.10, pp.107-149.
⑷3）　村井信哉「Q&A でわかる！量子暗号通信」日経クロステックウェブサイト <https://xtech.nikkei.com/atcl/nxt/column/18/01624/>
⑷4）　Xu et al., *op.cit.*⑶8