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	量子情報技術の概要
他言語論題 Title in other language	Brief Overview of Quantum Information Technologies
著者 / 所属 Author(s)	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	古典物理学ではなく量子力学に則った情報を処理する「量子情報技術」の概略と歴史について記述した後、調査報告書の概要を述べる。

国立国会図書館
National Diet Library, Japan

第 1 章　量子情報技術の概要

はじめに

1920 年代中頃に確立された量子力学は、第一次量子革命（the first quantum revolution）[1]を引き起こし、半導体やレーザーといった現代の我々の生活に欠かせない科学技術（量子 1.0）に寄与している。その確立から約 100 年を迎えつつある現在、第二次量子革命（the second quantum revolution）と呼ばれる最中にあり、量子 1.0 では未利用であった量子力学の真髄である「重ね合わせ」や「量子もつれ（エンタングルメント）[2]」を利用する量子情報技術（量子 2.0）の開発競争が激化している。この量子 2.0 の中心は、量子コンピュータ、量子シミュレーション、量子センシング、量子通信・ネットワークである。いずれも、これまで量子 1.0 であるレーザーや半導体技術を超えた応用を見出すことに主眼が置かれている。ここでは、この量子情報技術の基本的な性質をまとめ、それによって進化する現代技術の概観を述べる。

Ⅰ　量子情報技術の概略

量子情報技術と従来の情報技術である古典情報技術の特徴的な違いは、処理している情報が量子力学に則った情報、つまり「量子情報」であるか、あるいは我々が通常目にする古典物理学に則った情報であるかに現れていると言ってよい。我々が通常目にする情報は、理論的には 0 と 1 で表されるビット（bit）の列で表現できる。現代のコンピュータ、センシングや通信・ネットワークといったあらゆる情報技術は、このビットを大量に用意して処理することで成り立っている。一方、「量子情報」は、0 と 1 のどちらも取り得る「重ね合わせ」が可能な量子ビット（qubit）の列で表現される。量子情報処理は、この量子ビットを大量に用意して実行する。ただし、ビットでは問題にならないが、量子ビットでは注意を払わないといけないものとして、測定（観測）がある。例えば、メモリに保存されたビットの値が 0 の場合、当然であるが、我々がそのビットを読み出すと 0 という値を得る。しかし、量子ビットの場合は、「重ね合わせ」が可能なため、0 が出たり、1 が出たりする。一旦、0 が出るとその量子ビットは 0 に確定し、元の「重ね合わせ」ではなくなる。「量子情報」は、測定（観測）をすると壊れると言われる所以である。不思議なことに、この曖昧で壊れやすい「量子情報」が、現代のコンピュータでは宇宙の年齢に相当する時間がかかっても解けないような難問を解く量子コンピュータを実現し、その量子コンピュータでも破れないセキュア通信のネットワークを実現し、超高感度なセンシングを実現するのである。これらには、もう一つの量子力学の性質である「量子もつれ」が重要な役割を果たす。

＊　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 28 日である。

(1)　例えば、以下を参照。Jonathan P. Dowling and Gerard J. Milburn, “Quantum technology: the second quantum revolution,” *Philosophical Transactions of the Royal Society of London A*, Vol.361 No.1809, August 2003, pp.1655-1674. <https://doi.org/10.1098/rsta.2003.1227>

(2)　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。

このような量子情報技術を実現するために、大学、国立研究所、企業、スタートアップに所属する多くのサイエンティストやエンジニアが切磋琢磨している。まず、基本となる量子ビットを物理的に実現する必要があり、様々な物理系において研究されている。自然に存在する物理系としては、原子、イオン、光子であり、最近では電子も候補に挙げられる。一方、自然な物理系を模倣した人工的な物理系として、超伝導回路（電気抵抗のない回路）、半導体量子ドット、結晶中の欠陥（ダイヤモンド中のNV中心、SiV中心等）が候補に挙げられる。一般に、自然な物理系は安定に存在し、同一の量子ビットを大量に準備できる。一方、人工的な物理系はサイズが大きく、設計･加工･調整が比較的容易であり、制御がしやすい。これらの量子ビットは多数用意され、その一つ一つが操作される。

また、必要に応じて量子ビットと量子ビットの間に「量子もつれ」と呼ばれる量子力学に特徴的な相関を生成する。そして、操作後の一つ一つの量子ビットを測定することで、「重ね合わせ」を壊して、ビット値を読み出す。これらの一連の操作は、レーザー、マイクロ波、電場、磁場等を使って行われる。これらは非常に精密に制御されるが、制御によって量子ビットは外界と相互作用し、「量子情報」は徐々に壊れてしまう。これをデコヒーレンスと呼ぶ。このデコヒーレンスが起きるまでの典型的な時間をコヒーレンス時間と呼び、量子ビットの寿命を表す。量子ビットを処理できるのはコヒーレンス時間内に限られ、それを過ぎると量子ビットにエラーが生じ、正しい情報処理ができなくなる（コヒーレンス時間は、量子ビットをどの物理系で作成するかにも依存する。）。量子通信の場合は、コヒーレンス時間が光子の伝搬時間に対応するため、通信可能な距離に影響を与える。

古典情報技術においても、このようなエラー(3)が存在するが、0か1のビットは、いくらでもコピーすることができるため、エラーを訂正する方法は簡単に見つかる(4)。一方、量子情報はコピーできないため、エラー訂正の手法は自明ではなかったが、それを可能にする「量子誤り訂正符号」が提案され、実験的にも実証されている。実際の量子情報技術に、この量子誤り訂正符号を実装して動作させるためには、１個の量子物理系で量子ビットを実現するのではなく、量子ビットのエラー（誤り）を訂正する仕組みを実装した「論理量子ビット」を複数個の量子ビットで構成し、論理量子ビットによってコヒーレンス時間を任意に延ばせる「誤り耐性」を実現する必要がある。このように曖昧で壊れやすい「量子情報」を壊さずに、望みの規模と時間で処理できる技術は、いまだどの物理系でも実現しておらず、どの物理系が有望なのかも明確ではない。また、誤り耐性まで含めた量子情報技術については、実現できる物理系の探索から、それを動作させるエレクトロニクスを含めた制御技術、それを実際の問題解決に役立てるソフトウェアまで研究開発課題が山積している。

このような量子情報技術であるが、量子誤り訂正を必要とするかどうかで技術レベルは大きく異なる。量子シミュレーションや量子センシングは、一定の量子誤りがある場合でも動作させることを前提に考えられている。量子暗号を含む量子通信・ネットワークにおいては、アプリケーションによって異なるが、量子誤り訂正を古典誤り訂正で代用可能なものから量子誤り

(3)　ビットの場合には0であったものが1になったり、1であったものが0になったりする誤りはエラーである。ただし、同じビット値をコピーすれば、たまに生じるエラーは簡単に訂正できる。より効率的な誤り訂正符号も存在する。

(4)　例えば、QRコードには誤り訂正符号が使われており、QRコードに多少の読み取りエラーがあっても正しく情報を入手することができていることからも実感できるであろう。

訂正を必要とするものまである。量子コンピュータにおいては、一定程度の量子誤りのあるデバイス[5]でも動作するアプリケーションから誤り耐性のある汎用量子コンピュータの研究まで幅広い。いずれにしても、古典情報技術とは根本的に異なる原理で動作しているため、あらゆる階層の技術を見直す必要がある。また、その過程において、これまで見過ごされてきた技術課題が浮き彫りになり、そこからも新しい原理や技術が日々発見されているエキサイティングな領域であることは間違いない。

Ⅱ　量子情報技術の歴史

量子力学が物理学における最も新しく完全な理論体系となる上で、最初に見いだされた重要な「もの」の性質は、波と粒子の二重性であると言ってよい。我々が目にする「もの」は、それより遥かに小さい原子や電子などの粒子から構成されている。量子力学では、この原子や電子が波でもある。一方、光は波であると教わるが、量子力学では、光は粒子の性質も持っており、光子と呼ばれたりする。これを波と粒子の二重性と呼んでいる。このような波と粒子の二重性は現実に観測され、理論上はすべての「もの」で成立する。そして、この量子力学の性質は、現代の科学技術の根幹となっており、元素の周期律、半導体中の電子の振舞い、レーザーの原理等を説明し、コンピュータ、センサー、ネットワーク等で構成される現在の情報化社会を支えている。

この量子力学の確立から半世紀ほど経過した頃には、次の量子革命が芽生え始めた[6]。新しい量子革命は、波と粒子の二重性と密接に関係する量子力学の基本的な性質の一つである「不確定性原理[7]」と「重ね合わせ」や「量子もつれ」の積極的な利用である。量子コンピュータの最初の提唱者として名前の挙がるリチャード・ファインマン（Richard P. Feynman）[8]は、既に 1959 年にカリフォルニア工科大学で開催された米国物理学会の年会において「There's Plenty of Room at the Bottom - An Invitation to Enter a New Field of Physics」[9]と題した講演を行い、その中において、原子を一つ一つ並べて制御すると、量子力学の効果により、これまでと全く異なることが可能になると予見している。その一つが、1981 年、マサチューセッツ工科大学（Massachusetts Institute of Technology: MIT）と IBM が開催した国際会議「Physics of Computation」[10]において、彼自身が指摘した量子コンピュータによる量子物理系のシミュレーションであ

⑸　Noisy Intermediate-Scale Quantum（NISQ）と呼ばれる。

⑹　井元信之・北川勝浩「エレクトロニクス技術を変革する量子情報技術」『電子情報通信学会誌』100 巻 9 号, 2017.9, pp.968-973; 井元信之「量子情報の黎明期から第二次ブームまで」『日本物理学会誌』74 巻 6 号, 2019.6, pp.366-367. <https://doi.org/10.11316/butsuri.74.6_366>

⑺　量子力学では物質は粒子の性質と波の性質を両方持つ（粒子と波の二重性）が、粒子の性質を観測すると、波の性質がわからなくなり、その逆もある。このように、一方を測定すると、他方がわからなくなる原理を不確定性原理と呼んでいる。

⑻　当時、カリフォルニア工科大学の教授であり、1965 年にジュリアン・シュウィンガー（Julian Schwinger）、朝永振一郎とともにノーベル物理学賞を受賞している。

⑼　Richard P. Feynman, “There's Plenty of Room at the Bottom,” *Engineering and Science*, Vol.23 No.5, 1960, pp.22-36. <https://resolver.caltech.edu/CaltechES:23.5.1960Bottom>

⑽　2021 年は、この会議の 40 周年にあたり、これを記念したイベントがいくつか行われている。例えば、MIT と IBM は QC40 と題した国際会議を行い、ベネット（Charles H. Bennett）、ショア（Peter W. Shor）、スティーブン・ガービン（Steven Girvin）が登場するトークが YouTube でも公開されている。“QC40: Physics of Computation Conference 40th Anniversary.” Qiskit Website <https://qiskit.org/events/physics-of-computation/> また、関連ある論文が次にまとめられている。“40 years of quantum computing,” 29 November 2021. Nature Website <https://www.nature.com/collections/djhfiebiig/>

る[11]。ファインマンは、量子物理系をシミュレーションするために量子コンピュータを用いると、古典コンピュータでは指数関数的に爆発する計算量を抑制して、計算できることを指摘している。

また、1985 年にはデイヴィッド・ドイチュ（David Deutsch）が万能チューリングマシン[12]の量子版として、万能量子コンピュータを示した[13]。1984 年には、IBM のチャールズ・ベネット（Charles H. Bennett）とジル・ブラッサール（Gilles Brassard）が、量子暗号通信の最初の提案である量子鍵配送のプロトコル（BB84）[14]を提案している。量子暗号通信は、古典通信（現代のデジタル通信）では秘匿性（セキュリティ）が危ぶまれる暗号通信において、量子力学に従う光子の「重ね合わせ」状態と「不確定性原理」を利用することで、原理的な秘匿性を可能にするものである。一方、物理系の測定限界を極める量子センシングの基本的なアイデアである量子非破壊測定[15]やスクイーズド状態[16]は、「不確定性原理」を巧みに利用して制御する思考から、量子コンピュータや量子通信に先駆けて 1975 年から 1980 年代にかけて提案されている。こうした研究成果から、量子 1.0 から量子 2.0 への思考の変化を垣間見ることができる。この時代には、アラン・アスペ（Alain Aspect）らの「量子もつれ」を利用したベル不等式の破れの実験[17]によって、長年のアルベルト・アインシュタイン（Albert Einstein）とニールス・ボーア（Niels Henrik David Bohr）の量子力学をめぐる長年の論争に一定の終止符が打たれたことも印象的である。

1980 年代後半から 1990 年代は、より具体的な量子情報技術が提案され、実験的に実証され始めた時代である。1989 年にドイチュは量子コンピュータの基本的な要素である量子ゲートや量子回路を提案し[18]、1992 年には、量子コンピュータが古典コンピュータより速く解ける問題が存在することとその量子アルゴリズムを示した[19]。1994 年には、ピーター・ショア（Peter W.

---

(11)　Richard P. Feynman, “Simulating physics with computers,” *International Journal of Theoretical Physics*, Vol.21 No.6-7, June 1982, pp.467-488. <https://doi.org/10.1007/BF02650179>

(12)　抽象化された計算機であるチューリングマシンのいかなるものも模倣可能なチューリングマシンのことである。

(13)　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, July 1985, pp.97-117. <https://doi.org/10.1098/rspa.1985.0070>

(14)　Charles H. Bennett and Gilles Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” *International Conference on Computers, Systems and Signal Processing*, December 1984, pp.175-179. <https://arxiv.org/ftp/arxiv/papers/2003/2003.06557.pdf>

(15)　V. B. Braginskiĭ and Yu. I. Vorontsov, “Quantum-mechanical limitations in macroscopic experiments and modern experimental technique,” *Soviet Physics Uspekhi*, Vol.17 No.5, May 1975, pp.644-650. <http://dx.doi.org/10.1070/PU1975v017n05ABEH004362>; Vladimir B. Braginsky et al., “Quantum Nondemolition Measurements,” *Science*, Vol.209 No.4456, 1 August 1980, pp.547-557. <https://doi.org/10.1126/science.209.4456.547>; Carlton. M. Caves et al., “On the measurement of a weak classical force coupled to a quantum-mechanical oscillator. I. Issues of principle,” *Reviews of Modern Physics*, Vol.52 No.2, April 1980, pp.341-392. <https://doi.org/10.1103/RevModPhys.52.341>

(16)　Horace P. Yuen, “Two-photon coherent states of the radiation field,” *Physical Review A*, Vol.13 No.6, June 1976, pp.2226-2243. <https://doi.org/10.1103/PhysRevA.13.2226>

(17)　Alain Aspect et al., “Experimental Tests of Realistic Local Theories via Bell's Theorem,” *Physical Review Letters*, Vol.47 No.7, 17 August 1981, pp.460-463. <https://doi.org/10.1103/PhysRevLett.47.460>; Alain Aspect et al., “Experimental Test of Bell's Inequalities Using Time-Varying Analyzers,” *Physical Review Letters*, Vol.49 No.25, 20 December 1982, pp.1804-1807. <https://doi.org/10.1103/PhysRevLett.49.1804>

(18)　D. Deutsch, “Quantum computational networks,” *Proceedings of the Royal Society of London A*, Vol.425 No.1868, September 1989, pp.73-90. <https://doi.org/10.1098/rspa.1989.0099> なお、我が国では、原子と光を用いた量子コンピュータの提案が前年になされている。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*, Washington, D.C.: Optical Society of America, 1988, paper TuI4.

(19)　David Deutsch and Richard Jozsa, “Rapid solution of problems by quantum computation,” *Proceedings of the Royal Society of London A*, Vol.439 No.1907, December 1992, pp.553-558. <https://doi.org/10.1098/rspa.1992.0167>

Shor）が素因数分解を効率良く解く量子アルゴリズムを提案した[20]。素因数分解の計算の困難さは、RSA 公開鍵暗号による通信の秘匿性が破られない根拠となっているため、大きなインパクトを与えた。これにより、量子コンピュータの存在が広く知られるとともに、量子暗号を含む量子通信・ネットワークの重要性も認知された。1992 年には、IBM のベネットらにより最初の量子暗号（量子鍵配送）の実証が行われた。1992 年と 1993 年には、同じくベネットらにより量子稠密通信と量子テレポーテーションの提案がそれぞれ行われ、「量子もつれ」と通信量の関係が明らかにされて、「量子もつれ」がビットや量子ビットの通信のためのリソースとなることが示された。

1995 年には、ショアにより最初の量子誤り訂正符号が提案された[21]。1996 年には、ベネットらにより「量子もつれ」の誤り訂正とも呼べる量子もつれ蒸留[22]が複数提案された。また、ロブ・グローバー（Lov K. Grover）が N 個のデータから望みの 1 個のデータを効率良く探索する「グローバーのアルゴリズム」を提案したのもこの年である。さらにこの年、 現実のエラーのある環境下においてエラーを訂正しながら、あらゆる量子アルゴリズムを動作させることができる能力と規模を実現する究極の量子コンピュータの理論モデルとして誤り耐性型汎用量子コンピュータもこの年に提案された[23]。

そして、1997 年と 1998 年にインスブルック大学とカリフォルニア工科大学[24]から、光を使った世界初の量子テレポーテーション[25]の実証実験が報告された。続く 1999 年には、固体として世界初の量子ビットが NEC の中村泰信・蔡兆申らによって実現された[26]。この成果は、同年発足した我が国初の量子情報技術分野専門の研究会である量子情報技術研究会において、招待講演[27]として発表されている[28]。また、1999 年は量子情報技術関連の創業があった年でもある。米国では商用の量子暗号通信機器を生産する MagiQ Technologies 社[29]が誕生し、カナダでは超伝導量子回路を利用した商用量子コンピュータの製造を目指して D-Wave Systems 社[30]が誕生している。現在、量子コンピュータでも有名な Google や量子コンピュータの利用サービスを提供している Amazon の創業もそれぞれ 1998 年と 1993 年である。

---

⑳　Peter W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp.124-134. <https://doi.org/10.1109/SFCS.1994.365700>

㉑　Peter W. Shor, “Scheme for reducing decoherence in quantum computer memory,” *Physical Review A*, Vol.52 No.4, October 1995, pp.R2493-R2496. <https://doi.org/10.1103/PhysRevA.52.R2493>

㉒　量子もつれは量子ビット間の強い相関であるが、量子もつれ蒸留はその回復プロトコルである。強い量子もつれは任意の量子プロトコルの実装に欠かせない。

㉓　Peter W. Shor, “Fault-tolerant quantum computation,” *arXiv preprint arXiv:quant-ph/9605011*. <https://arxiv.org/pdf/quant-ph/9605011.pdf>; John Preskill, “Fault-tolerant quantum computation,” *arXiv preprint arXiv:quant-ph/9712048*. <https://arxiv.org/pdf/quant-ph/9712048.pdf>

㉔　カリフォルニア工科大学の成果は、当時ニコンに所属していた古澤明氏（現東京大学教授）が行ったものである。A. Furusawa et al., “Unconditional Quantum Teleportation,” *Science*, Vol.282 No.5389, 23 October 1998, pp.706-709. <https://doi.org/10.1126/science.282.5389.706>

㉕　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*, Vol.70 No.13, 29 March 1993, pp.1895.

㉖　Y. Nakamura et al., “Coherent control of macroscopic quantum states in a single-Cooper-pair box,” *Nature*, Vol.398 No.6730, 29 April 1999, pp.786-788. <https://doi.org/10.1038/19718>

㉗　中村泰信・蔡兆申「微小ジョセフソン接合を用いた量子ビット」（第 1 回 量子情報技術研究会（QIT1））1999.5.12.

㉘　当時の日本では量子情報技術関連の企業研究者や大学の研究室が増え始め、欧米と肩を並べて研究できる環境があった。中国の存在感はまだない。中国の台頭は、2008 年に潘建偉氏が帰国したことにより一気に加速する。

㉙　MagiQ Technologies website <https://www.magiqtech.com/>

㉚　D-Wave Systems website <https://www.dwavesys.com/>

2000 年代からは、1990 年代までの理論の進展に加えて、実験的な試みも量子情報技術を牽引していくようになる。2001 年にはアイザック・チャン（Isaac L. Chuang）のグループがショアのアルゴリズムによる 15 の素因数分解を実証した[31]。3 × 5という誰にでも計算できる結果が重要なのではなく、量子アルゴリズムが答えを導き出せるシステムを生み出したことに大きな意義がある。量子センシングにおける時間標準・周波数標準では、同じく 2001 年に、香取秀俊が光格子時計を提案し、その後、2005 年にその実証を報告した[32]。量子通信では、2003 年に筆者らが量子もつれ蒸留の実証を報告した[33]。2007 年にはスイスの ID Quantique 社製の装置を使って、ジュネーブにおいて、選挙の投票に量子暗号通信が利用された[34]。

2010 年には、日本でも情報通信研究機構（National Institute of Information and Communications Technology: NICT）、NEC、東芝、NTT 等が参画する東京 QKD ネットワーク[35]と呼ばれる量子暗号通信網が構築され、2022 年現在まで運用されている。我が国では、2000 年代の初めから量子情報技術に対して、科学技術振興機構（JST）等を介して公的研究費支援が始まり、研究環境が整備され、欧米と抜きつ抜かれつの研究成果を挙げるようになっていた。この時期は第一次量子情報ブームと言われている。「第一次」となっているのは、残念なことに我が国のブームは 2010 年代に一旦収束に向かうためである[36]。

2010 年代に入ると、さらに活発な動きが出てくる。まず、D-Wave Systems 社が商用量子コンピュータ（量子アニーリングマシン）を販売し始める。2012 年には、量子情報技術分野としては初めてのノーベル物理学賞がセルジュ・アロシュ（Serge Haroche. 仏）とデービッド・ワインランド（David J. Wineland. 米）に贈られる。受賞理由は “for ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems（個々の量子系の測定及び操作を可能にする画期的な実験手法）” であり、まさに量子ビットの測定と制御に関してである。アロシュは光子、ワインランドはイオントラップを用いている。これらは、上述の自然に存在する物理系である[37]。2014 年以降は、Google や IBM の超伝導量子回路による汎用量子コンピュータ開発が一気に加速する。2016 年には IBM がクラウド上での利用を開始している。そして、2019 年に Google は、ある特定の問題を現代のスーパーコンピュータより速く解く量子コンピュータを実現して見せた。量子コンピュータの新時代の幕開けである。現在では、Google（米）、IBM（米）や Rigetti computing（米）の超伝導量子コンピュータ、IonQ（米）や Honeywell（米）が取り組むイオントラップ量子コンピュータ、PsiQuantum（米）や Xanadu（加）の光量子コンピュータ、PASQAL（仏）や QuEra Computing（米）の原子量子コンピュータなどが切磋琢磨している。

2010 年代からは中国の台頭も著しい。2016 年には、上海 - 北京間を結ぶ量子暗号通信の光

⑶1　Lieven M. K. Vandersypen et al., “Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance,” *Nature*, Vol.414 No.6866, 20 December 2001, pp.883-887. <https://doi.org/10.1038/414883a>

⑶2　Hidetoshi Katori, “Optical lattice clocks and quantum metrology,” *Nature Photonics*, Vol.5 No.4, April 2011, pp.203-210. <https://doi.org/10.1038/nphoton.2011.45>

⑶3　Takashi Yamamoto et al., “Experimental extraction of an entangled photon pair from two identically decohered pairs,” *Nature*, Vol.421 No.6921, 23 January 2003, pp.343-346. <https://doi.org/10.1038/nature01358>

⑶4　Paul Marks, “Quantum cryptography to protect Swiss election,” 2007.10.15. New Scientist website <https://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election/>

⑶5　Project UQCC website <http://www.uqcc.org/QKDnetwork/>

⑶6　これは、北川 - 井元予想として語られている。井元　前掲注⑹

⑶7　人工的な量子物理系に関してのノーベル物理学賞も大いに期待される。

ファイバーリンクを実証し、量子暗号実験衛星を打ち上げ、2017 年には地上 - 衛星間量子暗号通信、「量子もつれ」配信、その後に量子テレポーテーション実験を相次いで成功させている。2021 年には、地上の光ファイバーリンクと量子暗号実験衛星を組み合わせて、総延長 4,600km の量子暗号通信に成功している。ただし、中継点では古典ビットになっているため、完全な量子暗号通信ではない（第 2 章第 4 節）。量子コンピュータにおいても、光量子コンピュータや超伝導量子コンピュータを相次いで開発し、上述の欧米企業やスタートアップと抜きつ抜かれつの開発競争を行っている。

量子センシングも幅広いフィールドで実証され始めている。光格子時計は、その精度の世界記録を更新し続け、重力の時間への影響まで検出するその精度により土地の高低差の精密センシングを可能にした。原子波干渉計は、精度の高いジャイロスコープとして注目され、海洋資源探索や自動運転船舶等への利用が考えられている。ダイヤモンド NV 中心を用いたセンシングデバイスは、生体内のイメージングやセンシングへの応用研究が進み、医療応用へ向かっている。

Ⅲ　本調査報告書の概略

量子情報技術と題した本調査報告書は、量子力学と情報科学の融合分野である量子情報科学に立脚した量子 2.0 とも呼ばれるエマージングな技術領域の現状を様々な視点から俯瞰し、21 世紀中に起こるであろう量子革命による社会の進化が垣間見えるように構成した。第 2 章では、量子 2.0 の中核技術である量子コンピュータ、量子シミュレータ、量子計測・量子センシング、量子通信・ネットワークについて、現在の開発動向も含め、それぞれの専門家に執筆いただいた。上述の概観では説明しきれない量子情報技術の幅広い適用範囲を感じてもらえると期待している。第 3 章では、量子情報技術関連の企業の動向や取組、世界的に不足している人材の育成や大学教育のあり方、資格制度や特許等、量子情報技術を育てる人及びその集合体としての企業に関して、民間からの視点で執筆いただいた。第 4 章では、量子情報技術に急速に投資を始めた世界各国の政策に関して、精緻にまとめていただいた。

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）