ROLES REPORT

No.5

量子技術と安全保障

池田 有紀美
（a 未来工学研究所 政策調査分析センター）
（b 東京大学　先端科学技術研究センター）

2021.3

ROLES
Special Reports

東京大学 先端科学技術研究センター
Research Center for Advanced Science and Technology
The University of Tokyo

ROLES REPORT_No.5

量子技術と安全保障

池田 有紀美
（a 未来工学研究所 政策調査分析センター）
（b 東京大学 先端科学技術研究センター）

2021.3

発行所　東京大学先端科学技術研究センター
創発戦略研究オープンラボ（ROLES）
〒153-8904
東京都目黒区駒場4-6-1
Tel　03-5452-5462
Webサイト　https://roles.rcast.u-tokyo.ac.jp/

ROLES Special Reports

東京大学 先端科学技術研究センター
Research Center for Advanced Science and Technology
The University of Tokyo

1 はじめに

有史以来、科学技術は国家の生存に大きな役割を果たしてきた。歴史を振り返れば、先端技術が国際政治や安全保障に影響を及ぼした事例は至る所で見つけることができる[1]。20世紀前半の2度の世界大戦では、優れた暗号技術を持つ側が敵側の通信情報を捕捉、敵国の意図を戦闘前に事前に把握し、自らの陣営にとって有利な戦局をつくり出すことに成功した[2]。第二次世界大戦末期には核兵器が登場し、冷戦期の核抑止に基づく米ソ超大国間の対峙とそれに基づく戦後の国際秩序を生みだした[3]。コンピュータ化により高度に自動化された金融市場の発展は、通貨取引量を飛躍的に伸ばし、国家の経済発展を後押しして国家間の国力競争を促した。新たな技術は国際政治や安全保障、経済の様々な側面における国家の競争力に大きく影響し、その競争の結果が国家間関係や戦争の帰趨に影響を与えてきたのである。21世紀に入り、科学・技術の発展がますます加速するなか、新技術が国際政治や安全保障、経済に及ぼす影響に改めて向き合う必要がある。

近年の新技術の発展に目を移せば、サイバー技術、人口知能（Artificial Intelligence: AI）、5G、ロボティクス、生命工学、宇宙工学、量子技術、極超音速技術、PNT技術[4]など、安全保障に影響を与え得る技術は数多く存在する。なかでも、新技術と安全保障という文脈において日本でまだ殆ど注目されていないのが、量子技術（quantum

1　Eugene B. Skolnikoff, The Elusive Transformation – Science, Technology, and the Evolution of International Politics – (New Jersey, Princeton University Press, 1993), Chapter 1.
2　例えば、第二次世界大戦中にイギリスのブレッチリー・パークに置かれた政府通信本部の暗号学校（Government Code and Cypher School）では、ドイツのエニグマ暗号やローレンツ暗号が解読され、その解読情報を元にしたインテリジェンス「ウルトラ」が連合国の勝利において非常に価値があったとの分析が多くなされている。Gustave Bertrand's book Enigma ou la plus grande énigme de la guerre 1939–1945, p.256.; The Secret Life of Sir Stewart Graham Menzies, Anthony Cave Brown; Winterbotham, F. W. (1974), The Ultra Secret, New York: Harper & Row; Hinsley, F. H. (1993), "Introduction: The Influence of Ultra in the Second World War", in Hinsley, F. H.; Stripp, Alan (eds.), Codebreakers: The Inside Story of Bletchley Park, Oxford University Press, pp. 11–13.
3　Bernard Brodie, "Implications for Military Policy, in Bernard Brodie, ed., The Absolute Weapon: Atomic Power and World Order (New York: Harcourt, Brace & Company for Yale Institute of International Studies, 1946), 76.; Bernard Brodie, Strategy in the Missile Age (Princeton, NJ: Princeton University Press, 1959), pp.271, 273-275, 277.; Thomas C. Shelling, The Strategy of Conflict (Oxford: Oxford University Press, 1960), Chapters 2-5.
4　Position, Navigation, Timingの略で、位置を特定したりある地点へ誘導したりするための測位技術のこと。衛星航法や慣性航法などがある。

technology）である。量子技術とは、次章で詳述するが、量子力学特有の現象を応用した技術のことで、人類の技術水準を一変させ得る可能性を秘めている。米国海軍研究所の研究員ランザゴルタは、「量子技術が『情報時代の原爆』になり得ると信じる理由がある」と言う[5]。

量子技術の代表例は、量子コンピューティングである。2019年10月にGoogleの量子コンピュータがスーパーコンピュータの能力を超える計算を実行し「量子超越」を達成したニュースは記憶に新しい[6]。かつて殆ど全ての人が「量子コンピュータの実現は何十年も先の夢のまた夢であって、今から考える必要はない」とか「結局は消えていく実現しない技術だ」と考えていたことを思えば、隔世の感を禁じ得ない。量子コンピューティングをめぐる状況は、過去10年の急速な進展により様変わりした。

そう遠くない将来、10年から20年のうちに、数百量子ビット程度の小規模の量子コンピューティングが、量子化学計算の加速を通じて新しい化学物質や材料、薬の開発プロセスを激変させる可能性がある[7]。言うまでもないが、これらは航空機材料を始めとする各種装備の開発競争に影響する。さらに10年から30年先に大規模な量子計算が可能になれば、それを応用した成果が様々な分野で出始め、人類の技術進歩を益々加速させるだろう。Googleは、この大規模量子コンピュータを2029年に実現すると発表している[8]。量子技術は、量子コンピューティングだけではない。量子レーダー等の量子センシング技術においても既に原理が実証されている技術があり、近い将来、電磁波領域の戦い方に変更を迫る可能性がある[9]。

現在、世界の主要国は、この量子技術の研究開発に凌ぎを削っている。例えば、中国は、量子技術が安全保障に大きな影響を与えることを見据えて巨額の投資を行ってきている。対する米国は、歴史的に量子技術の開発において主導的役割を果たしてきた[10]が、中国による国家主導の量子技術開発を踏まえ、米国がリーダーの地位を維持し続けるには国家としての継続的な支援が不可欠であるとの認識を新たにし、米国政府は新たな体制づくりに着手した[11]。さらに米中だけでなく、欧州、カナダ、シンガポール、豪州、韓国、ロシアなども挙って量子技術の研究開発を進めている。

世界各国が量子技術の研究開発に乗り出す理由は、量子技術が、イノベーションと経済的な利益の源泉であるとともに、安全保障における様々な局面で、戦略的にも戦術的にも、大きなインパクトをもたらすと考えられているからである。一方で、日本においては、量子技術と安全保障の関係について説明し、問題提起を行った文献は見当たらない。安全保障のための量子技術の開発を日本が主導していく必要はなく、我が国としては純粋な科学技術の発展の見地から量子技術の研究開発に取り組めばよいとの議論もある。確かに、これにも一理ある。しかし、量子技術は革新的な技術であるが故に、それらが世界の安全保障にもたらす影響やインプリケーションを事前に分析し、必要な対策を講じておくことは、政策の立案・研究に不可欠である[12]。

---

5 Marco Lanzagorta, Naval Research Laboratory, “The Future of Quantum Sensing and Communications,” https://www.youtube.com/watch?v=5uqiQ_mP3PM (accessed August 16, 2020).
6 Frank Arute et al., “Quantum supremacy using a programmable superconducting processor,” Nature 574 (October 24, 2019), pp.505-510.
7 White House, “How America Achieved “Quantum Supremacy,” https://www.whitehouse.gov/articles/america-achieved-quantum-supremacy/ (accessed June 15, 2020).
8 Opening Keynote by Hartmut Neven, Quantum Summer Symposium 2020 (July 22, 2020), https://youtu.be/TJ6vBNEQReU (accessed December 3, 2020).
9 S. Barzanjeh, S. Pirandola, D. Vitali, J. M. Fink, “Microwave quantum illumination using a digital receiver,” Science Advances 6, no.19 (May 8, 2020); Electronic Warfare Europe, “A Study of Quantum Radar Countermeasures” available from https://www.eweurope.com/ew-europe-2020/a-study-on-quantum-radar-countermeasures#/ (accessed August 23, 2020).
10 U.S. National Academies of Sciences, Engineering, and Medicine, Quantum Computing: Progress and Prospects (National Academy Press, 2019), Appendix:E
11 H.R. 6227 – National Quantum Initiative Act (115th Congress, 2017-2018) became public law on 21 December 2018. (Public Law No: 115-368)
12 Klon Kitchen, “Quantum Science and National Security: A Primer for Policymakers,” https://www.heritage.org/technology/report/quantum-science-and-national-security-primer-policymakers; (accessed June 7, 2020).

政策決定において科学技術をどのように評価するかという課題[13]については、技術の実現に関する専門家の予測や解説をそのまま受け入れるのではなく、あるいは過去の他の技術の失敗事例を参照するのでもなく、量子技術に関する個別の学術的な発展や実用化のプロセスの事実をしっかりと押さえることで、短期的あるいは長期的な予測を支えるより客観的な議論を行うことが可能である。ここでは、そのようにして、個別の技術の発展についての事実を根拠に議論を進める。

次節以降、技術変革と安全保障に関する議論および量子技術とはどのようなものかを把握した上で、量子技術が国家間の安全保障にどのようなインパクトをもたらし得るのかについて、明らかにしていきたい。

2 技術変革と安全保障[14]に関する議論

軍事力や戦争における技術の役割については、様々な議論がある。一般的には、科学技術における変革は、技術を駆使した装備・ネットワークに支えられる軍事組織を強力にし、安全保障面でアドバンテージを与えると考えられている。対照的に、軍事史家や軍人は、技術のみに焦点を当てて重要性を論じる姿勢に否定的であることが多い[15]。例えば軍事戦略について多くの著作を残しているコリン・グレイ（Colin Gray）は、「『軍事における革命』が起こるためには新しいテクノロジーが必要だという議論は致命的な誤りだ」と言う[16]。しかしながら、技術が戦闘に影響を与えること自体を否定するのは難しいだろう。

2-1. 技術の戦闘への影響

技術は戦場において重要であった。戦闘において、兵器や支援能力における技術面での優位がしばしば決定的な要素であった。14世紀に出現した強力な長弓とそれを用いた戦術、15世紀の冶金技術と火薬の進歩による火砲の射程増大と命中精度の向上、16世紀に登場した帆船による軍艦への重量物搭載の実現と、これによる艦砲の標準装備化、16−17世紀のマスケット銃と線形戦術の採用による連続的な射撃能力の出現、産業革命による17−18世紀の兵器の標準化・高性能化・軽量化、19−20世紀にかけての内燃機関動力による艦艇、潜水艦、魚雷の発展など、技術の革新が運用上の革新等と相まって戦闘に影響を与えた例は推挙に暇がない[17]。20世紀に入ってからも、1930年代から40年代にかけてのレーダーの発達、第一次世界大戦で電撃戦を可能にしたエニグマ暗号機の開発、エニグマ暗号を解読したチューリング（Alan Turing）の暗号解読機ボンブ[18]の登場、第二次世界大戦末期の米国に

13　技術発展を推進する当事者はその実現を信じるのが当然であるため、政策の検討においてはより客観的に技術の発展を捉える態度が必要となる。
14　安全保障とは、伝統的に国家の軍事力次第であると見なされてきたが、実際には、軍事力以外のもの−経済力、外交力、世界への発信力、競争力のある産業、教育の質、相対的な社会環境、市民の福祉、国民の健康、高い指導力など−によって左右されることが多いことが明らかになるにつれて、軍事だけに偏った考え方は現在では極めて少なくなっている。しかし、あらゆる点を同時に検討して分析の焦点を失うのを避けるため、まずは軍事力の側面について考えることにしたい。なぜなら、軍事力は、今なお国際関係の主要な要素であり、かつ科学技術の進歩と極めて密接に関わっているからである。国の政策立案者や専門家は、軍事力を国際秩序の基本原則とみなしてきた。Hans J. Morgenthau, Politics among Nations: The Struggle for Power and Peace, 5th ed. (New York: Alfred A. Knopf, 1973); Kenneth N. Waltz, Theory of International Politics (Reaading, Mass.: Addison-Wesley, 1979).
15　John Baylis, James J. Wirtz, and Colin S. Gray, Strategy in Contemporary World: An Introduction to Strategic Studies, Third Edition (Oxford: Oxford University Press, 2010), Chapter 7.
16　エリノア・スローン著、奥山真司・関根大助訳『現代の軍事戦略入門 陸海空からサイバー、核、宇宙まで』芙蓉書房出版、2015年、261頁（原題：Elinor C. Sloan, Modern Military Strategy: An Introduction Second Edition, Routledge, 2017.）
17　小泉悠「I. 技術革新が外交・安全保障にもたらす影響」『技術革新がもたらす安全保障環境の変容と我が国の対応』公益財団法人未来工学研究所、令和2年3月、12−13頁。
18　ドイツのエニグマ暗号だけでなく、英国ブレッチレー・パークの情報部はドイツ、イタリア、日本暗号文から得られる情報も解読し、そこから得られた情報を「ウルトラ」と称して活用した。ウルトラは、1944年、連合軍が、ドイツ軍によるノルマンディー上陸の様子を事前に把握することを可能にし、連合国のヨーロッパ侵攻を成功させた1つの要因となったと言われている。

よる核兵器の投下など、新技術の使用が戦闘や戦争を劇的な勝利へ導き、国家生存の転換点となった例が歴史には存在する。現代においても、技術優位を獲得するという軍事的な要求は拡大し続けており、現在では、技術は国家の軍事力の相対的な有効性を支える主要な要素の一つであると言っても過言ではない。技術がもたらす変化は軍事競争の力学を修正したり、軍隊の使用や目的の概念を変えたりして、深く影響を及ぼしている。

2-2. 軍事における革命（Revolution in Military Affairs: RMA）

新たな技術や戦術を導入した結果、軍事組織が大きな変化を遂げ、軍事的効果が劇的に高まる現象が歴史上に存在し、それらの一部は「軍事における革命（revolutions in military affairs: RMA）」と呼ばれる。

技術を駆使した兵器システムの重要性を最初に認識したのは、西側諸国ではなく、むしろ技術的に遅れていた1970年代のソ連軍であった。当時のソ連軍参謀総長であったニコライ・オガルコフ（Nikolai Ogarkov）元帥は、「偵察攻撃複合体」（reconnaissance-strike complex）によって「軍事技術革命」（Military Technical Revolution）が起こりつつあると指摘した。このソ連内部での議論を注視して研究していたのが、米国防総省の総合評価局（Office of Net Assessment）局長であるアンドリュー・マーシャル（Andrew Marshall）であった。マーシャルは、1990年には同室スタッフのアンドリュー・クレピネヴィッチ（Andrew Krepinevich）に軍事技術革命について分析を行うよう指示し、技術により強化された戦闘力が真に革命的かどうかについて1990年代を通じて幅広く議論を行った。

1992年、クレピネヴィッチは、RMAが起こるためには新しいテクノロジーが必要であると論じた。さらに、RMAは、（1）技術革新に加え、（2）新たなシステム開発（革新技術の兵器化）、（3）運用上の革新（新兵器を利用した作戦のための新たな戦闘ドクトリン開発）、（4）組織的受容（軍事組織による新兵器と新戦闘ドクトリンの採用）という4つの要素が結び付き、戦争の様相と行為を「根本的に変化させた」ときに生起してきたと主張した。彼によれば、このようなRMAは14世紀以降10回起こったとされている[19]。アンドリュー・マーシャルも自身の論文で、過去のRMAにおいて決定的な要素となったのは「既存の入手可能なシステムを凌駕するような、革新的な作戦概念と組織体制の採用である」と書いている[20]。90年代に軍事技術の重要性を認識していた米国の戦略家達も、技術と組織が融合した結果の有効性が戦闘の結果を決めると主張していたのである。

クレピネヴィッチら米国の軍事理論家達は、オガルコフ参謀総長らが抱いていた、兵器の長射程化、誘導精度向上による選別攻撃、情報の伝達・共有の高度化、ドメイン横断型の戦闘といった考えを取り込み、現代におけるRMAを実現させようとした。その流れは、ロバート・ワーク元国防副長官を媒介にしてオバマ政権時代の「第3次オフセット戦略（The Third Offset Strategy）」に引き継がれ、トランプ政権下の国防イノベーションにも継承されている[21]。この現代RMAの1つの要素が「情報の伝達や共有の高度化」であり、量子技術はこの情報通信技術に大きく影響を与える。

米国を代表する戦略家の1人エリオット・コーエン（Eliot Cohen）は、「現在のRMAは、それ以前の革命と同じく、

19 Andrew F. Krepinevich, “Calvary to Computer,” National Interest, No.37, Fall 1994
20 Andrew W. Marshall, “The 1995 RMA Essay Contest: A Postscript,” Joint Forces Quarterly (Winter 1995-96), 81.
21 森聡「米国の国防イノベーション（平成30年度航空研究センターシンポジウム：発表3）」『エア・パワー研究（第6号）』、35頁。

民間のテクノロジーの世界から生まれたものであり、今回は情報通信技術の台頭に求めることができる」と述べている[22]。未来学者であるアルビン・トフラーとハイジ・トフラーも、1993年の著作で「1970年代に始まった情報テクノロジーの発展という『第三の波』が戦争の闘い方にも反映され始めた」と説いている[23]。トフラー夫妻は、「システムの統合」の重要性を指摘しており、各軍種と別の軍種とのコミュニケーションを可能にする高度に発展したC4I（Command, Control, Communications, Computer, and Intelligence 指揮、統制、通信、コンピュータ、インテリジェンス）が特に重要であるとした。90年代の戦略思想家の1人であるウィリアム・オーウェンス（William Owens）元米海軍大将が明らかにした「システムのためのシステム」（system of systems）という概念は、先進的な軍事システムの3つの異なる分野、「見る」（ISR）、「教える」（C4I）、「行動する」（精密誘導兵力）が融合するシステムを想定している[24]。90年代後半、アーサー・セブロウスキー（Arthur J. Cebrowski）は、自身が米海軍作戦部長であった際、軍事アナリストのジョン・ガルストカ（John J. Garstka）と一緒に、戦争は最新の艦船、航空機、戦車などの「プラットフォーム中心の戦い」から「ネットワーク中心の戦い」（network-centric warfare: NCW）へと根本的にシフトしているとする概念を提唱し[25]、後に国防総省の戦力変革局（Office of Force Transformation: OTT）で軍種間での技術面における相互運用性の確保に取り組んだ[26]。コーエンは「プラットフォーム自身は以前ほど重要ではなくなり、むしろそれらが運んでいるセンサー、弾薬、電子機器など、質の方が決定的に重要になったと論じている[27]。

このように、コミュニケーションやネットワーク、センシングが大きな役割を果たすようになっている現代の戦争において、量子技術はこれらの要素に大きなインパクトを与える可能性を秘めている。例えば、量子センシングは、航空優勢を確保するための今日の決定的な技術であるステルス機能を破る可能性があると言われている。量子通信は、これまで達成され得なかった絶対に破られない超秘匿通信を可能にする。量子コンピューティングは、現在の古典コンピュータでは絶対に解読できないとされているRSA暗号[28]の解読を可能にするとともに、その計算能力（問題によっては既存のコンピュータとは比較にならない程の高速化が可能）が科学と技術の様々な分野の研究を加速すると言われている。量子技術は、安全保障にインパクトを与える可能性があり、それを知っている諸外国は量子技術の研究開発に膨大な投資を行ってきているのである[29]。

3 量子力学の世界

19世紀末、粒子の運動を説明するニュートン力学と電気的・磁気的現象を説明するマクスウェル電磁気学、これら2つの物理法則をまとめた「古典物理学」で全ての自然現象が理解でき、物理学は完成されてしまったのではないかと思われていた。しかし、私たちが日常生活で接することのないミクロな世界は、古典物理学では説明できな

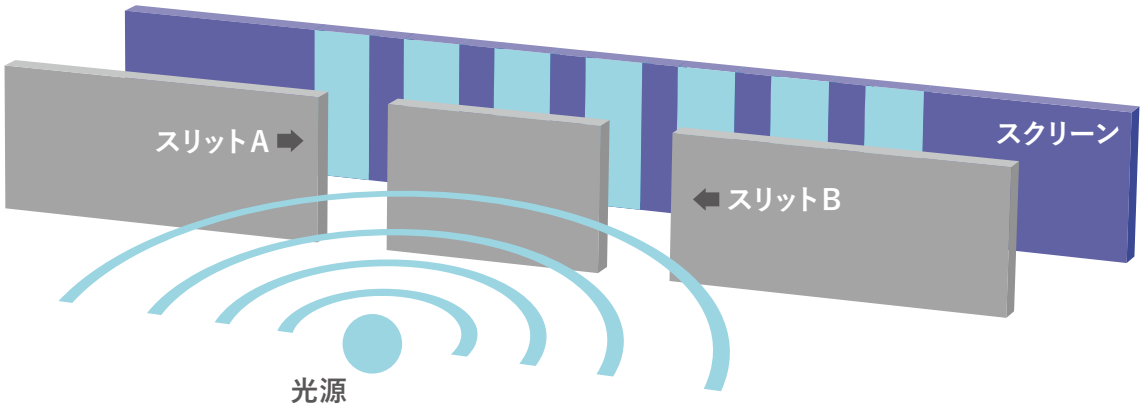
22　Eliot A. Cohen, “A Revolution in Warfare,” Foreign Affairs 75:2 (March/April 1996), p.42.
23　Alvin Toffler and Heidi Toffler, War and Anti-war (New York: Warner Books, 1993) [アルビン・トフラー&ハイジ・トフラー著『アルビン・トフラーの戦争と平和：21世紀日本への警鐘』フジテレビ出版、1993年]
24　William Owens, “The Emerging System of Systems,” Military Review (May-June 1995)
25　Arthur K. Cebrowski and John J. Garstka, “Network-centric Warfare: Its Origins and Future,” U.S. Naval Institute Proceedings 124: 1 (January 1998).
26　US Office of Force Transformation, Military Transformation: A Strategic Approach (Washington, DC: Office of Force Transformation, Fall 2003), pp.21-23.
27　Cohen, 45
28　公開鍵暗号の一つ。桁数が大きい数の素因数分解が困難であることを安全性の根拠としている。1977年に共通鍵の鍵配送問題をクリアするために発明され、発明者であるロナルド・リベスト、アディ・シャミア、レオナルド・エーデルマンの頭文字をとってRSAと呼ばれる。
29　イノベーション政策強化推進のための有識者会議「量子技術イノベーション」第1回 資料3「量子技術分野の研究動向について」（2019年3月29日、JST 研究開発戦略センター曽根純一）、3−31頁。

いことが徐々に明らかになってきた。そこで、20世紀初頭、原子のサイズ程度以下の世界を記述する理論として量子力学が登場した[30]。量子力学は、一般相対性理論とともに現代物理学を支える最も重要な柱の一つである。そして、量子技術とは、その量子力学特有の現象を応用した技術である[31]。では、量子力学特有の現象とは何か?まずはその説明から始めるべきであろう。量子力学の父の一人であるニールス・ボーア(Niels Bohr)は「めまいを覚えずに量子力学について考えることが出来る人は、量子力学がわかっていない」という有名な言葉を残したが、量子の世界は直観に反するもので、これを理解しようとすればかなり奇妙な概念に出会うことになる。

3-1.「重ね合わせ」

まず、18世紀にトマス・ヤング(Thomas Young)が行った「ダブルスリット(光の干渉)」実験(図1)を見ておくことが役に立つ。その実験は、1つの衝立に2本のスリットを入れておき、そこに光を当てるというものだ。光の波は2つのスリットを通過し、スクリーンに到達する。この時、スリットAを通過した波とスリットBを通過した波が干渉を起こし、スクリーンには独特の明暗の縞模様(干渉縞)ができる。ある点では波の山どうしがぶつかり、波が強められる(スクリーンが明るく光る)。またある点では、波の山と波の谷がぶつかり、波が打ち消される(スクリーンは暗くなる)のである。ヤングの実験は「光の波動性」が顕になる代表的な実験であり、高校物理の教科書でも紹介されている[32]。

(図1)ヤングの光子による「ダブルスリット(光の干渉)」実験

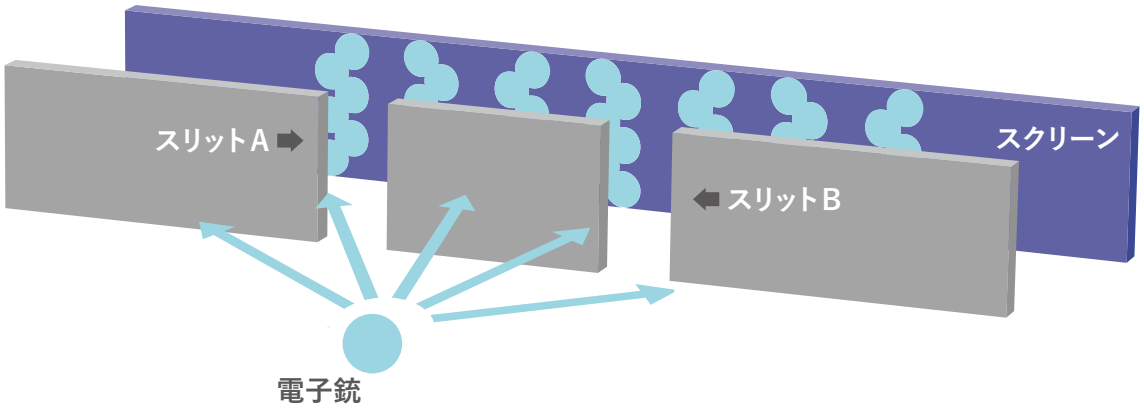


次に、原子サイズより小さな物質の代表例として、電子を考えよう。電子は一つ、二つと数えられるため、粒子のイメージで語られることが多いが、単なる粒子ではない。光のかわりに電子を使ってヤングの実験を行うことを考える(図2)。電子がスクリーンに当たると、点状の跡を残すものとする。ダブルスリットの入った衝立に向かって電子を一つずつ打ち込んでいくとき、もし電子が単なる粒子なら、スクリーン上でスリットの先付近に電子の跡が集中すると予想できる。しかし実際には、光の場合と同様、スクリーン上には複数の明るい線と暗い線からなる縞模様ができる。1個1個の電

30　現在では巨視的なスケールにおいても量子力学が重要となる現象が知られている。その代表例が超伝導現象であり、今日の超伝導量子ビットに繋がっている。
31　量子(quantum)とは、「1つ2つと数えられる小さなかたまり」という意味で、量(quantity)の基本単位(最小単位)ともいえる。
32　ノーベル賞物理学者の朝永振一郎は、1949年、一般読者に向けて『光子の裁判』を書き、量子力学の「ダブルスリット」実験の不思議を法廷劇の形で語っている。

子を飛ばしたにもかかわらず、スリットAを通過した電子の波とスリットBを通過した電子の波が干渉を起こし、スクリーンには干渉縞ができるのである。これは、電子は粒子であり、波でもあることの現れである[33]。現在では、電子だけでなく、あらゆる素粒子が波と粒子の二面性を持つことが知られており、例えば、上で見た光もまた、波動性と粒子性を併せ持つことが知られている。

(図2)電子による「ダブルスリット」実験



量子力学に基づくと、ダブルスリット実験における電子の状態は、スリットAを通ってスクリーン上のある位置に至る波(確率振幅)とスリットBを通って同じ位置に至る確率振幅の重ね合わせで与えられる。観察するまでは異なる状態が共存しており、これを状態の「重ね合わせ」(superposition)と呼ぶ。ここではスリットを使って説明したが、「重ね合わせ」はもっと一般的に成立する概念である。例えば、箱に閉じ込められた電子を考える。箱に仕切りを入れると、電子は箱の左半分にいる状態(これを|左〉と書く)と箱の右半分にいる状態(これを|右〉と書く)を取り得るが、それだけでなく、重ね合わせ状態、|左〉+ |右〉も取り得る。すなわち、左にいる状態と右にいる状態という二つの相反する状態が共存しているのである。直観的に理解することは難しいが、量子コンピューティングでは、物理系が持つこのような二つの状態を0と1に対応させ、従来の古典コンピュータには無い、状態の重ね合わせを駆使して計算を実行する。

3-2.「量子もつれ」

量子力学におけるもう一つの重要な性質は、「量子もつれ」(quantum entanglement)である。例えば、2つの電子からなる物理系を考える。2つの電子が両方とも状態|0〉または両方とも状態|1〉のとき、2つの電子の状態をまとめて|00〉や|11〉と書くとする。電子が2つあっても、状態の重ね合わせが起こり得るので、例えば、状態 |00〉+ |11〉も有り得る。このとき、片方の電子の状態を観測し、もし状態が|0〉だと分かれば、自動的にもう一方の電子の状態も|0〉に決まる。量子もつれとは、2つの粒子が強く相関する状態であり、粒子のスピン、運動量などの状態をま

33　日立製作所の外村彰博士は、ヤングの「ダブルスリット」実験を電子を使ってやってのけ、この実験はPhysics World誌が実施したアンケートで「最も美しい科学実験」に選ばれた。

るで「コインの裏表」のように共有する運命共同体のような状態を指す。この現象は粒子同士が大きく離れていても生じる。相対性理論をつくりあげたアルバート・アインシュタイン(Albert Einstein)は量子もつれを「奇妙な遠隔作用」(spooky action at a distance)と呼んだ。量子もつれは、例えば、数百km以上の遠方との量子通信に必須となる量子中継の技術で使われる。

量子力学の世界は、私達が日常接する巨視的な世界の常識が通じないため、奇想天外な話にすら聞こえるかもしれない。しかし、量子力学は20世紀初頭から現在に至るまで、ありとあらゆる実験検証に耐えてきた現代物理学の柱である。人類が100年に亘り蓄積してきた膨大な理論研究・実験研究の成果を、先端技術に応用することは必然的な流れであろう。実際、「状態の重ね合わせ」と「量子もつれ」という量子力学特有の現象を駆使することで、従来は成しえなかったような技術が実現可能となる。それが量子コンピューティングをはじめとする量子技術である。次節では、量子技術の具体例を紹介するとともに、各国の研究開発の動向や安全保障への影響を議論する。

4 量子技術と安全保障

量子技術の研究開発はここ数十年の間に目覚ましく進歩し、量子コンピューティング、量子通信、量子センシングの研究は急速な発展を見せている。これら3つの分野は、汎用(デュアル・ユース)技術である一方で、国家安全保障にインパクトをもたらし得る。そこで以下、量子コンピューティング、量子通信、量子センシングの3つの分野が安全保障にどのような影響を与え得るのかを見た上で、これらの技術をめぐる研究開発に大きな影響を与える米中競争の現状を俯瞰することとする。

4-1. 量子コンピューティング、量子通信、量子センシング

(a) 量子コンピューティング

量子コンピュータ[34]とは、スリット実験の節で見た「状態の重ね合わせ」を活用した、従来のコンピュータとは全く異なる新しい方式のコンピュータである。1981年に、米国のノーベル賞物理学者リチャード・ファインマン(Richard P. Feynman)が「自然をシミュレーションするには、古典力学ではなく量子力学で動くコンピュータをつくるべき」と述べた[35]のが始まりと言われている。その後1985年に、イギリスの科学者デイヴィッド・ドイチュ(David Deutsch)が量子物理学の法則にしたがって動作するコンピュータを定式化した。これが、現代につながる量子コンピュータの幕開けである[36]。我々が日常用いるスマートフォンやノートパソコンからスーパーコンピュータまで、現在のコンピュータ(以下、古典コンピュータ)は、0か1のビットを用いて情報を記録、処理する。例えば、3ビットの情報は011などの3つの数字で表される。一方、量子コンピュータでは $|0\rangle$状態と $|1\rangle$状態、そして、それらの重ね合わせが情報を担う(量子ビット)。3つ量子ビットがある場合は、全ての可能な組合せの重ね合わせ、すなわち、$|000\rangle$、$|001\rangle$、$|010\rangle$、$|011\rangle$、$|100\rangle$、$|101\rangle$、$|110\rangle$、$|111\rangle$の8(=2の3乗)個のビットパターンの重ね合わせが演算に用いられる。N個の

34 G Wendin, “Quantum information processing with superconducting circuits: a review,” Reports on Progress in Physics 80, 106001 (2017)
35 Physics of Computation Conference Endicott House MIT, May 6-8, 1981
36 藤井啓裕『最強の量子コンピュータ 宇宙最強マシンへの挑戦(岩波科学ライブラリー289)』岩波書店、2019年、40頁

量子ビットがある場合は2のＮ乗個の状態の重ね合わせを演算に用いることができる。量子コンピュータでは、これら2のＮ乗個の状態の重ね合わせを用いて演算処理をしていき、確率の波の干渉を上手く使って答えを抽出する。

量子ビットの数Ｎが小さいと、その有難みが分からないが、Ｎが大きくなるとともに処理するビットパターンの重ね合わせが指数的に増大する。その威力を世間に知らしめたのが、2019年10月にニュースとなったGoogleによる量子超越の達成である。量子超越とは、すなわち、量子コンピュータを使って古典コンピュータではできない計算を実行することである。Googleは53個の量子ビットを持つ量子チップ「シカモア」を用い、2の53乗（=9000兆）個のビットパターンの重ね合わせによる計算の爆発的加速を実証した。スーパーコンピュータは量子コンピュータをシミュレートできなかったのである（量子超越）。

ただし現状では、量子コンピュータがスーパーコンピュータを超える計算ができるのは、実用的とは程遠い、特殊な問題のみである。科学や技術、産業や安全保障の諸課題に量子コンピュータの計算能力を応用できるようになるまでには、量子ビット数の大規模化をはじめとする様々な問題を解決していく必要がある。例えば、ノイズの問題が挙げられる。古典コンピュータであればノイズの除去（エラー訂正）は簡単である。古典ビットは0また1を取るため、ノイズの影響で入力値が0.95だったとしても、それを1と見做せば良い。デジタルの強みである。一方、量子ビットでは、各状態の重みを指定する係数がアナログ値である。例えば、3量子ビットであれば、状態は$a|000\rangle+b|001\rangle+c|010\rangle+\ldots$と書けるが、各係数a,b,c,... はアナログ値であり、デジタルな古典ビットのようなマージンは無く、ノイズは計算結果の信頼性を損ねる。そこで重要となるのが、量子誤り訂正である。量子ビットを複数用いて一つの「論理量子ビット」を構成することで誤りを訂正する手法[37]が考えられている。誤り訂正付きの大規模な量子コンピュータの実現には今後10年から30年かかると考えられている。

量子化学計算、量子機械学習、今後10-20年の小規模量子コンピュータ（NISQ）

量子コンピュータの応用先の一つとして期待されているのが、量子化学計算である。量子化学は化学における伝統的な一分野であり、量子力学に基づく計算を通じて分子のエネルギーや構造などを理解する。これまでも（約100年前から現在に至るまで）、様々な工夫を持ち込むことで手計算や古典コンピュータを用いて計算されてきた。しかし、分子が大きくなるにつれて、計算の実行には膨大な計算資源が必要となる。これは想像に難くない。分子は一つまたは複数の原子が集まることで構成されているが、その各々の原子は原子核と電子の集まりである。原子核と電子は引き合うが、電子どうしは反発しあう。分子が大きくなるにつれて、膨大な数の原子核と電子が絡み合った複雑な相互作用を扱うことになる。では、量子コンピューティングであれば簡単に計算できるのだろうか?残念ながら、話はそう簡単ではない。大きな分子の厳密な電子状態の計算は、Quantum Merlin Arthur（QMA）-hardというクラスに分類される問題であり、古典コンピュータであろうと量子コンピュータであろうと力技では手に負えないことが分かっている[38]。量子コンピュータであっても、やはり賢い計算手法とそれを実行するためのアルゴリズムの開発が必要となる。

実は現在、この分野が大きく進展しつつある。代表的なものは、2014年に提唱された量子変分固有値計算法

37　例えば、表面符号と呼ばれる手法では、一つの論理量子ビットを作るのに数十の量子ビットが必要である。この大きなオーバーヘッドが量子ビット数の大規模化を要請する。
38　G Wendin, op.cit., p.2.

(Variational Quantum Eigensolver: VQE)[39]の応用である。計算過程の多くは従来の古典コンピュータを用いて実行されるが、量子計算を使うことで計算を指数的に加速できる部分では量子コンピュータを用いる(量子古典ハイブリッド・アルゴリズム)。そのパワーの源泉は、古典コンピュータと比較して指数的に小さな規模のハードウェア上に全量子状態を保存できるという量子コンピュータの強みにある。既にVQEを使った量子化学計算は、水素分子を始めとする小さな分子に適用されて成功を収めている[40]。

こ　こで強調しておくべきは、VQEは、現在の或いは近未来の小規模な量子コンピュータでも実行可能な手法であるという点である。今後、誤り訂正付きの真の量子コンピュータが実現するまでの間に、誤り訂正ができない小規模な、せいぜい数百個の量子ビットを持つ量子コンピュータ(Noisy Intermediate-Scale Quantum Computer: NISQ)の実用的な応用が進むと考えられており、NISQ用の実用的なアルゴリズムの探索は、現在の主要テーマの一つとなっている[41]。VQEは、まさにその代表例である。

また、機械学習は現在のAIの中核技術であるが、ここにも小規模量子コンピュータNISQが応用できるとして注目が集まっている。現在の機械学習の火付け役とも言える深層学習(deep learning)では、多層のニューラルネットワークを用意し、目的とするタスクを実行できるように学習によってネットワークを繋ぎ変えていく。例えば、教師あり学習では、犬や猫などの動物の写真と写真の動物が何であるかを示す答えを与え、入力(写真)に対して正しい答え(動物の名前)を出力できるようにネットワークを繋ぎ変える。量子機械学習では、ニューラルネットワークではなく、量子ビットの演算の順序や組み合わせを繋ぎ変える[42]。この手法も2018年に5量子ビットの量子コンピュータを用いて原理実証が行われている[43]。

仮にこれら古典量子ハイブリッド・アルゴリズムによって量子化学計算や量子機械学習が大幅に高速化されれば、材料開発や薬の開発など、広範な科学・技術の研究開発(もちろん航空機材料や種々の装備品開発を含む)に少なからず影響を与えることになる。この先10年から20年は、我々が既に量子コンピュータ時代を生きていることを認識する時代となるだろう。

暗号解読

誤り訂正付きの大規模な量子コンピュータが実現されるのは、2030年頃から2050年頃と考えられている。これによって計算を大幅に高速化できる問題がいくつか知られており、特に有名な例が暗号解読である。後述するが、国家機密を秘匿する現在の主要な暗号のあるタイプの暗号を解読する際には、量子コンピュータの爆発的な計算能力を活用することで、解読することができると言われている。

ここで、暗号について簡単に振り返っておこう。暗号解読の鍵は、(1)解読する側のコンピュータの処理速度(鍵の候補数)と(2)秘匿する側の鍵配送問題の2つにある。伝統的に、秘匿通信の仕組みは、暗号化された文章は普通の通信で送信され、暗号化に使用した秘密鍵を正当な受信者だけに送る(鍵配送)、というものであった。解読する側は、暗号文を傍受した上でコンピュータ処理によって鍵候補を総当たり式にチェックするか、鍵配送をインター

39　A. Peruzzo et al., “A variational eigenvalue solver on a photonic quantum processor,” Nature Communication, 5, 4213 (2014).
40　A. Kandala et al., “Hardware-efficient Variational Quantum Eigensolver for small Molecules and Quantum Magnets,” Nature 549, 242 (2017).
41　国内でもQunaSysをはじめとする量子スタートアップ企業が、大企業や大学と連携して研究開発を進めている。
42　K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii, “Quantum Circuit Learning,” Physical Review A 98, 032309 (2018).
43　V. Havlicek et al., “Supervised learning with quantum-enhanced feature spaces,” Nature 567, 209 (2019).

セプトして鍵を盗むか、そのどちらかによって暗号を解読することができた。秘匿する側は、暗号化を複雑にし、かつ鍵配送を確実に行うことで、秘密情報を守ることができた。しかし、いくら暗号化を複雑にしても、もし鍵配送において途中で鍵を盗取されてしまえば、暗号は解読されてしまう。これが、DES暗号のような共通鍵と呼ばれるタイプの暗号時代の問題であった。これを克服すべく登場したのがRSA暗号に代表される公開鍵である。

現在使用されている暗号には、DES[44]やAES[45]のような共通鍵タイプやRSAのような公開鍵タイプなどがある。共通鍵は、暗号化や復号の高速処理にメリットがあるが、暗号文と鍵の送信者と受信者が同一鍵を持つ必要があるため、鍵配送問題を避けて通ることはできない。したがって、共通鍵の安全性は、秘密鍵を探索する計算[46]量に依拠する。対照的に、RSAのような公開鍵は、公開鍵部分と受信者だけが知り得る個人鍵部分（公開鍵部分からは解くのが困難な一方向関数によって表現）から出来ているのだが、送信者が個人鍵部分を知らずとも公開鍵によって暗号をかけて送信することができ、受信者は自分だけが知り得る個人鍵部分を使って復号することができる。そのため、公開鍵では、送信者が受信者に鍵を配送する必要がなく、鍵配送問題が起こり得ない。この一方向関数の重要な部分が二つの素数pとqの積Nである。素数pとqから積N（=p×q）を計算することは簡単であるが、Nからpとqを求める作業（素因数分解）は非常に手間がかかる。このような関数を一方向関数という。Nを非常に大きくすればするほど、この作業に莫大な時間を要することになる。現在広く使用されている公開鍵であるRSA暗号の安全性は、このNの値をとてつもなく大きくすることで生まれる素因数分解の困難さに依拠している。

しかし、この公開鍵暗号は、既知の量子計算の手順（Shorのアルゴリズム）に対して非常に脆弱だと言われるようになった。量子コンピュータ上でShorのアルゴリズムを実行できれば、公開鍵暗号の解読を困難にしてきた大きな整数の素因数分解[47]や離散対数問題が指数的に速く解けるようになる。例えば、2000論理量子ビットの量子コンピュータを用いる場合、1024ビットのRSA暗号を約4時間で、2048ビットでも30時間以内に、4096ビットでも230時間で解読可能と見積もられている[48]。

一方で、共通鍵暗号の解読は難しい。例えば、AES-GCMと呼ばれる暗号方式がある。128ビットAES-GCMの鍵を見つけるために、現行の誤り訂正アルゴリズムを備えた数1000論理量子ビットの量子コンピュータを用いて全探索（Groverのアルゴリズム）を行う場合、1兆年程度かかると見積もられている[49]。それでも心配なら、256ビット鍵に移行すれば良い。全探索に基づく解読を行う限り、Groverのアルゴリズムが最適である（それより速くなることはない）ことが知られており、全探索に対する安全性の確保は簡単だと言われている。

量子コンピュータ誕生に向けた課題

誤り訂正付きの大規模な量子コンピュータが実用化されれば、量子コンピュータ耐性のある暗号（耐量子コンピュー

44　DESの強化版であるトリプルDES暗号は2023年に使用の終了が決まっている。National Institute of Standards and Technology（NIST）Special Publication 800-131A Revision 2, “Transitioning the Use of Cryptographic Algorithms and Key Lengths,” March 2019.
45　1976年に米商務省標準局（National Bureau of Standard）がDESを標準暗号に採用して以来、DES系暗号は米国の公式な暗号だったが、DESの弱点を強化すべく、90年代以降AESを標準暗号に指定した。
46　全数探索法やショートカット法などの解読方法がある。金子敏信「共通鍵暗号の安全性評価」『電気情報通信学会基礎・境界ソサイエティ Fundamental Review』Vol.7 No.1、2013年7月、14頁。
47　公開鍵は一方向関数であり、その関数の中で変更可能な成分N（素数p × 素数q）が公開鍵で送信者を含め誰もが知ることができる部分である。逆に受信者しか知り得ないのが、素数p、qの個人鍵部分となる。
48　Emily Grumbling and Mark Horowitz, Editors, Quantum Computing: Progress and Prospects, by National Academics of Sciences, Engineering, and Medicine, pp.96-98; 西森秀稔訳『米国科学・工学・医学アカデミーによる量子コンピュータの進歩と展望』Emily Grumbling, Mark Horowitz編、共立出版、2020年1月、110−111頁。
49　Ibid., pp.97-101; 西森、112−113頁。

タ暗号）で暗号化されていない国家機密は瞬時に見破られることになる。最初にその技術を手にした国は、国家間の通信を傍受し、敵対国の意図を把握する力を持つ。悪意ある潜在敵国が安全保障上の情報の取得に活用すれば、自国の国家機密が流出してしまう。例えば、我が国は電子政府システムの標準暗号としてRSA2048を推奨しているが[50]、RSA2048は、先に見たように、量子コンピュータが実現すれば解読されてしまう。このような危機を回避するには、あらかじめ脅威の内容を想定し、必要な部分については、事前に耐量子コンピュータ暗号へ移行しておくことが重要である。

誤り訂正付きの大規模な量子コンピュータが2040年代に動き出すという予測（先に述べたように、Google は2029年と公言しており、仮にそれが実現すれば10年以上早くなる）に従えば、我々には対処するだけの十分な時間的余裕があるように思えるが、実際には、世の中で広く使われている暗号を耐量子コンピュータ暗号へと更新する期間が必要であり、余裕など無いことが分かる。米国国立標準技術研究所は、耐量子コンピュータ暗号を選定し、標準化するプロセスを2016年に開始しており、現在のスケジュールでは選定は2022年から2024年である。広く使われている暗号の更新には、過去の経験から10年程度かかると考えられており、世の中の様々な製品が耐量子コンピュータ暗号に完全に移行するのは2030年代半ばから2040年頃となるだろう。これは、誤り訂正付きの大規模な量子コンピュータが実現すると思われている時期とあまり変わらない。耐量子コンピュータ暗号への完全な移行の前に、誤り訂正付き量子コンピュータが動き始めれば攻撃の対象となる可能性がある。特に、長期間に亘って稼働することを前提としているインフラや防衛装備品などは移行が迅速に進まない可能性もあり注意を要する。

安全保障の文脈で量子コンピュータの話になると暗号解読が話題に上りがちであるが、それだけでなく、上で述べたとおり、今後10年から20年の NISQ 時代の間に徐々に量子化学計算や量子機械学習への応用が始まるだろう。これらは、材料や薬の開発を始めとする幅広い分野における研究開発過程を激変させるポテンシャルを持っている。防衛装備品の開発現場も例外ではないだろう。

(b) 量子通信

「秘密を暴きたいという強い衝動は人間の本性に深く根ざしたもの」とは、第二次世界大戦中イギリス海軍で日本海軍の暗号解読に関わり、後に線文字Ｂを解読したジョン・チャドウィック（John Chadwick）の言葉だが[51]、その衝動は、国家においては安全保障上の重要な機能の1つとして捉えられる。孫子の言葉にもあるように、敵勢力がどのような策略を立てているかを探ること（情報の取得）は、重要な国家の戦略の一つである。一方で、自国を守るためには、敵対する勢力に自国の戦略を知られないように味方とは秘密裏に交信しなければならない（情報の通信）。既に見た量子コンピューティングによる暗号解読は「秘密を暴く」側の、情報の取得に関わる話であったが、ここでは「秘密の交信」の側、情報の通信について話をする。

上の節4−1（a）では、既存の暗号に対する量子攻撃の脅威と、どのようにすれば量子攻撃への耐性を持たせられるかについて説明した。この節では、量子力学に基づく新たな秘匿通信の手段である量子通信について説明する。

50　CRYPTEC「電子政府における調達のために参照すべき暗号のリスト」（平成25年3月1日）総務省、経済産業省；情報セキュリティ対策推進会議決定「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1及び RSA1024に係る移行方針」（平成24年10月26日改定）
51　ジョン・チャドウィック『線文字Ｂの解読』大城功訳、みすず書房、1976年

量子鍵配送

量子通信の一つの手法に、量子鍵配送（Quantum Key Distribution: QKD）がある。量子鍵配送は、送信者と受信者が盗聴者に情報を漏らすことなく秘密鍵を共有する方法で、その安全性は量子力学の基本的な性質によって担保されている。もっとも有名な手順はチャールズ・ベネット（Charles Bennett）とジャイルス・ブラサード（Gilles Brassard）によって1984年に提案されたBB84プロトコルである。送信者アリスは二つの異なる方法（XとZ）で量子ビット $|0\rangle$ または $|1\rangle$ をエンコードし、受信者ボブに送る[52]。ボブはX用またはZ用の検出器を適当に選んでアリスからの信号を受信する。ボブは古典通信（例えば電話）でXとZのどちらを使って受信したかアリスに知らせる。エンコードの方法と検出器の種類が一致していない場合、ボブが得る受信結果は完全にランダムである（量子力学が持つランダム性）。一致した場合だけ、情報の送信は成功である。これを繰り返すことで秘密鍵を共有することができる。盗聴者イブが存在する場合、イブはアリスからの情報をXまたはZの検出器を使って盗み見た後、ボブに同じ情報を送ることで盗聴の証拠隠滅を図る。しかし、正しい検出器を選んでいない場合、盗聴に失敗する上、誤った情報をボブに送ることになる。これがアリスとボブのやり取りの中に矛盾を引き起こすため、盗聴が発覚する。盗聴の痕跡を見つけた場合は、この秘密鍵を使うのをやめて、例えば、別の通信路を使って再び秘密鍵の共有を試みれば良い。このようにして、盗聴の無い超秘匿通信の実現が可能であると期待されている。既に日本を含む多くの国で技術検証が行われており、100km程度の通信距離であれば既に製品化もされている[53]。

送信者と受信者の距離（量子鍵配送は、通信路の長さ）が数百km程度と長い場合、光子が途中で失われて受信者まで届かなくなり、量子鍵配送による秘密鍵の共有が難しくなる。そのため、東京―ワシントンDC間のような遠距離で完全な秘匿通信を実行するには、上手く通信距離を延ばす必要がある。従来の方法では、単純に、光子が直接届く距離ごとに基地を設けて基地間でのみ量子通信を行う。この方法は、各基地のセキュリティや基地運営者が完全に信頼できるという前提に立っており、各中継基地における安全性を保証できないという欠陥がある。そこで量子中継器（quantum repeater）が必要となる。量子中継器は量子もつれを用いた量子技術である。中継基地において、二つの量子もつれから拡張された一つの量子もつれを生成すること（量子テレポーテーション）によって、光子が一度では届かない遠方との超秘匿通信が可能となる。

安全保障における情報通信の重要性

量子通信の目的は、「確実性」と「秘匿性」の確保である。これらは軍事や外交における機密情報を伝達する際に非常に重要な要素であり、軍隊にとって通信は、指揮中枢から末端部隊までを指揮統制するための基盤である。通信の秘匿が侵されれば、戦争の帰結を左右する。歴史を遡れば、第二次世界大戦中、イギリスの暗号解読者たちは、ドイツのエニグマ暗号を解読することによりヨーロッパ戦線の流れを変え、アメリカの暗号解読者たちは、パープルと呼ばれる日本の暗号を解読することにより太平洋戦線に重大な影響を及ぼした。例えば、米国は、1942年6月のパープル暗号解読により、日本軍がアリューシャン列島を攻撃すると見せかけて実はミッドウェーを占領しようとしていることを事前に把握し、その計画に乗せられたふりをしてミッドウェー諸島で日本軍を撃破した。現代において

52　通常は光の粒子「光子」を用いる。
53　例えば、スイスのID Quantique社や米国のMagiQ Technologies社がある。また、日本の東芝は、国内外での量子鍵配送システムのプラットフォーム提供とシステムインテグレーション事業を、2020年度第4半期から順次開始。国内では初の事業化であり、海外では米国のVerizon Communications等と共同事業を開始する。

は、通信の秘密を破る手段としてサイバー攻撃がある。敵の軍事活動を低コストで妨害できる非対称的な攻撃手段であり、国の防衛に関わる情報の窃取に利用されている。情報通信技術の発展によって、軍隊が情報通信ネットワークへ依存する度合いは一層増大しており、多くの機微な情報がサイバー空間でやり取りされるようになるにつれ、情報窃取の被害は一層重大なものとなってきている[54]。情報通信を確実に秘匿することは、いつの時代も安全保障の要諦である。

(c) 量子センシング

量子技術は、世界を新しい方法で認識することを可能にする。量子センシングはその一手段であり、量子もつれなどの量子力学的なふるまいを利用して物理量を計測する超高感度の測定技術である。近年、一般には量子コンピュータや量子通信の実現に関する議論が活発だが、その陰で、量子センシングの研究開発は着実にめざましい発展を遂げている。専門家の間では、実用的な(誤り訂正機能を持つ数百万量子ビット規模の)大規模な量子コンピュータの実現には10年から30年程度かかるとの見込みがある一方で、量子センシングが応用された一つの形態である量子レーダーは5年から10年後には実現し得ると言われており、量子技術の中でも実用化に近い分野の一つと見られている。マイケル・グリフィン前米国防次官(研究・工学担当)は、2020年3月に開かれた米国下院軍事委員会において、量子技術の国防への応用に楽観的であってはならないと指摘する一方で、量子センサーは戦時における情報ナビゲーションを改善するものとして期待でき、短期的に達成可能なものだろうと証言している[55]。

量子レーダー:実験の成功と意義

量子レーダーは、量子センシングの応用先の一つであり、量子力学特有の現象である「量子もつれ」を応用したレーダーである。従来のレーダーと違い、測定対象物からの反射が少なくノイズが大きい状況でも機能し、対象物を高感度で詳細に補足することができるとして期待されている。

まず、従来のレーダーの仕組みを説明する。これは、暗闇の中で落としてしまった家の鍵を探している状況を想像すると分かりやすい。懐中電灯で辺りを照らし、キラリと光る物があれば、それは恐らく鍵であろう。これをもう少し科学的な言葉で書くと、懐中電灯から数百nmの波長をもつ電磁波(可視光)を放射し、鍵で反射された電磁波を人間の眼で探知した、ということになる。航空機用のレーダーも同様である。波長が数cmから数10cmの電磁波(マイクロ波)を送信し、航空機から反射された電磁波を受信することで航空機を発見する。

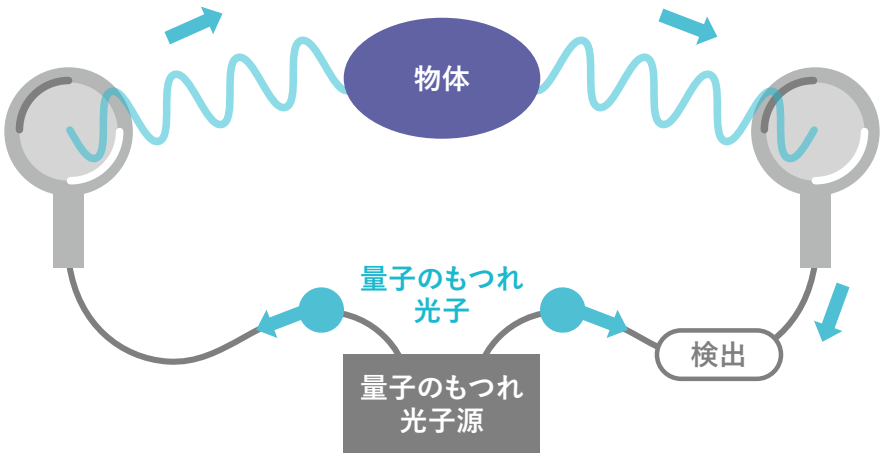
暗闇で落とした物が、鍵よりもずっと小さな米粒サイズの物であったなら、反射される光が少なくなり、発見が難しくなるだろう。レーダーの場合も同様で、対象物からの反射が小さくなれば発見が難しくなる。これを利用してレーダーによる探知から逃れているのがステルス機である。ステルス機は、機体を特殊な形状に設計することによって、レーダーからの電波を送信元以外に反射し、送信元に打ち返されるレーダー波を少なくしている。微量のレーダー波が受信されても、バックグラウンドノイズに十分に埋もれてしまうため検知されない。

シグナルがノイズに埋もれてしまい検出できなくなるという問題は、レーダーでステルス機を捉えようとする場合

54 『令和2年度防衛白書』第I部第3章第3節「サイバー空間と安全保障」
55 US Department of Defense, "DOD Should Focus on Short-Term Goals in Quantum Science," March 12, 2020, https://www.defense.gov/Explore/News/Article/Article/2110617/dod-should-focus-on-short-term-goals-in-quantum-science/ (accessed August 16, 2020).

だけではなく、微弱な光を検出しようとする際の一般的な問題である。そのような中、量子センシングの分野で、バックグラウンドノイズの影響を除去する方法「量子イルミネーション」(quantum illumination)が提案された[56]。量子もつれを起こしている2つの光子のうち一方の光子を対象物に照射し、もう一方の光子は受信機側で保持しておく。物体からの反射光子と受信機側で保持している光子の相関関係を利用することでバックグラウンドノイズの影響を除去できる。この量子イルミネーションをマイクロ波領域の電磁波の検知に応用したものが量子レーダーである[57]。2020年5月には、オーストリアのクロステルヌベルグ科学技術研究所の研究者らが、量子もつれを起こしたマイクロ波を利用して、反射が少なくノイズが大きい場合でも探知できる高精細度の量子レーダーの実験に成功したという論文を発表した[58]。短距離での実験ではあるが、反射が少なくノイズが大きい状況下でも対象物を検出できる可能性があり量子レーダー技術の実証実験に成功したという事実は大きい。長距離量子レーダーの開発につながれば、ステルス機能を破る可能性が出てくるからだ。これまで概念レベルでしかないと言われていた量子レーダー技術が実現に向けて大きく前進したと言える。

(図3)量子レーダーのしくみ



ステルス打破の可能性

量子レーダーが使われれば、量子レーダーが持つ内部信号の量子状態を知り得ないため、発信元の信号を模擬したノイズを発生させられない。さらに、たとえ妨害側がノイズを発生させても、受信元は受信した光子がレーダー内に保管された光子との相関関係を確認することで、ノイズを見分けることができ、ノイズは役に立たなくなる。この仕組みにより、量子レーダーは、強大なノイズの中でも、戻ってくる極めて微弱な信号を検出し、従来型レーダーより高解像度の情報を受信することが可能になる[59]。

ステルス機能の軍事戦術上の意義は、現代でもなお重要なドメインである空や海、特に航空戦において先制発見・先制攻撃を容易にし、優位性を獲得できることである。1970年代以降、米国の対ソ戦略に関する中心人物であったウィリアム・ペリー(William Perry)元国防長官は、ステルス技術を含むテクノロジー面での相乗効果の利用を通じて対

56 S. Lloyd, "Enhanced sensitivity of photodetection via quantum illumination," Science 321, 1463 (2008).
57 S. Barzanjeh et al., "Microwave quantum illumination," Physical Review Letter 114, 080503 (2015).
58 S. Barzanjeh et al., "Microwave quantum illumination using a digital receiver," 当該論文で発表された量子レーダーは、ジョセフソン・パラメータ変換器を使って量子もつれを起こした電磁波光子(signal photon, idler photon)をつくり出し、一方の光子(signal photon)をターゲットに向けて放出し、反射して帰ってくる情報を受信する。量子もつれを起こしているもう一方の光子(idler photon)は、放出された光子(signal photon)と量子もつれを起こしているため、放出された光子(signal photon)が戻って来た時に、それが放出された光子であると、ノイズに惑わされずに検知することができる。現在使用されているレーダーでは、戻って来た信号を他のバックグラウンドノイズの妨害によって受信できないという問題があるが、量子レーダーはノイズがあっても量子もつれという量子力学の振る舞いを利用することによってこの課題を克服することができる。
59 さらに量子レーダーは放出エネルギーが少ないため逆探知されにくいという戦術上のメリットがある。

ソ戦闘力が向上したと強調したが[60]、航空支配に重要なステルスによる優位性が、量子レーダーによって脅かされる可能性がある。例えば、日本政府は2018年、105機のステルス性に優れた第5世代戦闘機F-35を米国から追加で購入すると決定し、航空自衛隊が保有する戦闘機290機中147機体制を目指すとした。しかし将来、仮に長距離で機能する量子レーダーが実用化されステルス性が無効化されてしまえば、装備体系の再検討を余儀なくされるかもしれない。

電磁波領域での戦いと量子センシング

現代の戦闘では、レーダーによる探知や索敵、部隊間の通信、ミサイルの精密誘導など、多くの局面で電磁波が利用されており、電磁波領域は、現代の戦闘における攻防の最前線として、主要な領域の1つと認識されるようになっている[61]。仮にこうした電磁波の利用に支障が生じた場合、部隊は作戦を適切に遂行できず、深刻な影響が生じる可能性がある。量子センシングは、この電磁波領域での戦いに影響を与える。日本政府は、2018年末に改定した「防衛計画の大綱」で、電磁波を含む「新たな領域」での能力強化を打ち出し[62]、具体的な施策として、我が国への侵攻を企図する相手方のレーダーや通信などを無力化するための電子妨害などの能力の強化を挙げている。しかし、相手方が量子レーダーを使用すれば、上述した量子レーダーの性能からして、電子妨害がどれほど有効かは疑問であり、精査される必要がある。量子レーダーが現実に使用されるようになった場合に備えて、電磁波領域で使用すべき技術、戦術およびそれらを踏まえた防衛政策の立案が求められる。

4-2. 量子技術の研究開発をめぐる米中競争

(a) 量子コンピューティング、量子通信、量子センシング

量子コンピュータの研究開発をめぐる世界的な競争は、2014年頃から潮目が変わった。超伝導量子ビットの専門家である、カリフォルニア大学サンタバーバラ校のジョン・マルティニス（John M. Martinis）が、量子誤り訂正の要求を満たすほど超低雑音の超伝導量子ビット（5量子ビット）とそれに対する演算を実現した頃である。Googleがマルティネスのグループを丸ごと抱え、量子情報科学分野の黎明期から基礎研究を続けてきたIBMも人員を増やし、IT業界の巨人であるMicrosoftも研究開発を加速させた。

中国は、2016年8月、1200億円を拠出した「科学技術イノベーション第13次5か年計画（2016−2020）」[63]において、重点分野の中でも、量子通信と量子コンピュータを重大科学技術プロジェクトとして指定した。同計画および2018年の「国家重点研究計画」においては、強化すべき基礎研究として量子情報を挙げ、量子技術分野に研究開発費を投入している。さらに、国家が抱える巨大な研究施設の立ち上げも進んでおり、合肥市に1兆円をかけて建設中と言われる「量子情報科学国家実験室」は2020年内に完成予定と言われている[64]。中国科学技術大学の潘建偉（Jian-

60 William J. Perry, “Defense in an Age of Hope,” Foreign Affairs 75:6 (November / December 1996), p.77.
61 『令和2年度版防衛白書』第III部第1章第3節「宇宙・サイバー・電磁波の領域での対応」
62 「平成31年度以降に係る防衛計画の大綱について」（平成30年12月18日 国家安全保障会議決定 閣議決定）。同大綱では、領域横断作戦を実現するため、電磁波の新領域における優越性確保が不可欠とし、そのための情報通信能力の強化、電磁波に関する情報収集・分析能力の強化、情報共有体制の構築、相手方からの妨害を局限・無力化する能力の向上、電磁波管理の機能強化を図るとしている。また、すべての領域における能力を効果的に連接する指揮統制・情報通信能力の強化を図るとしている。
63 The People’s Republic of China, The 13th Five-Year Plan for Economic and Social Development of the People’s Republic of China (2016-2020), https://en.ndrc.gov.cn/policyrelease_8233/201612/P020191101482242850325.pdf (accessed June 16, 2020).
64 国立研究開発法人科学技術振興機構「研究開発の俯瞰報告書（2019）」、181頁

Wei Pan）[65]率いる研究グループは、2016年8月、世界で初めて量子通信衛星「墨子号」を打上げた。

その2か月後、2016年10月には、政権交代を迎えようとしていたオバマ（Barack Obama）政権において、ホワイトハウスの米国科学技術委員会（US National Science and Technology Council: NSTC）が「量子情報科学の推進：国家の課題と機会」と題した報告書を発表し、領域・セクター横断的な研究開発が鍵となる量子技術の研究開発には国家が一丸となって取り組む必要があること、国家による安定した投資を継続することの必要性を訴えた。同じ月には、米国の産業界、アカデミア、政府の専門家からなる協力枠組み「米国光工学イニシアティブ（National Photonics Initiative: NPI）」が、量子技術の研究開発戦略（後の「国家量子イニシアティブ法」）を策定することの意義について、米国議会の議員やスタッフへの働きかけを開始した[66]。2017年6月には、NPIは「国家量子イニシアティブの必要性」と題した提言を下院の科学・宇宙・技術委員会の議会スタッフと議論し、同年10月の「量子技術における米国のリーダーシップ」と題された下院公聴会へとつながった。2018年6月に下院、上院ともに超党派でそれぞれ法案を上程し、下院可決後の調整を経て上院でも可決、2018年12月に大統領署名によって「国家量子イニシアティブ法（National Quantum Initiative Act: NQIA」[67]が成立した。NQIAは、量子技術を安全保障にとって致命的に重要なものと位置づけ[68]、5年間で約1400億円をDoE、NSF、NIST傘下の量子科学技術研究所等へ拠出すること、官民の研究力を結集させた研究開発の促進を決定し、量子技術研究のための国家体制の整備を規定した。このNQIAは、大統領に対しては、国家量子イニシアティブ諮問委員会（National Quantum Initiative Advisory Committee）の設置、各プログラムの目標設定と優先順位付け、必要な国家支援の分析、国際協力の可能性の評価を義務付けており、単なる努力目標を定めた法律ではなく量子技術開発における具体的な実現目標を設定させる実用的なものとなっている。

このように米国は、中国における政府主導の量子技術の研究開発の加速化を注視しつつ、自国の研究開発体制づくりに努めてきた。2017年には、ホワイトハウスの科学技術政策室（Office of Science and Technology Policy: OSTP）へ、メリーランド大学の量子コンピューティングの専門家ジェイク・テイラー（Jake Taylor）をOSTPの量子科学担当部長補佐として迎えた[69]。2018年9月には量子技術の研究開発に関する戦略文書「量子情報科学の国家戦略概要（National Strategic Overview for Quantum Information Science）」を策定している。

量子通信については、中国は米国よりも進展を見せている。上述のように、2016年8月には中国科学技術大学の潘建偉のグループが、世界初の量子通信衛星「墨子号」を打上げ、2017年にはオーストリアの研究グループと共同で約7,400kmの量子鍵配送を成功させて地球周回軌道を回る衛星－地上局間の量子通信を成功させている[70]。

米国の国防インテリジェンス当局は、量子センシング以外の量子技術の短期的な実用化は現実的ではないとしつつも、中国の量子通信における研究開発を踏まえて、「敵対国の技術が米国の情報保全と機密性の確保を飛躍的に難しくする」と認識している。米軍内では、長期的には、無条件の秘匿性を与えてくれる量子通信を国防上の通信

65　中国科学院量子信息（情報）・量子科学技術創新研究院院長で、中国科学技術大学の副学長でもある。中国共産党員ではなく、中国にある八大民主党派の内の一つ、「九三学社」の党員で中央副主席を務めている。https://baike.baidu.com/item/%E6%BD%98%E5%BB%BA%E4%BC%9F/12245（accessed December 5, 2020）
66　Michael G Raymer and Christopher Monroe, “The US National Quantum Initiative,” Quantum Science and Technology, 4（2019)020504,（IOP Publishing, February 22, 2019), pp.3-5.
67　H.R. 6227 – National Quantum Initiative Act（115th Congress 2017-2018) became public law on 21 December 2018（Public Law No: 115-368).
68　Committee Statement and Views, Committee Report, H. Rept. 115-950 – National Quantum Initiative Act, 115th Congress（2017-2018).
69　NQIAは、OSTP内の組織の増設・拡充も規定している。
70　Sheng-Kai Liao et al., “Satellite-to-ground quantum key distribution,” Nature（Vol.549)（09 August 2017), p.43-47 and pp.70-73.

システムとして取り入れる構想の具体化に着手しているようである[71]。国防総省傘下の国防高等研究計画局（Defense Advanced Research Projects Agency: DARPA）は、量子鍵配送ネットワーク構築や量子中継[72]などの具体的な研究プログラムを進めている[73]。安全保障上の通信に関し、トランプ政権は安全保障のための情報インフラ保護への問題意識を高めており、2019年11月には、大統領令13873号に基づいて米国の情報通信技術・サービスのサプライチェーンを保護するための規則案を公開し、米国の通信ネットワークにとって安全保障上の脅威となる華為技術（ファーウェイ）や中興通訊（ZTE）といった企業からの調達を一部停止させる規制を採択するなどしている。

量子センシングについては、上述したオーストリアの研究所による量子レーダー実験が成功する約1年半前、2018年11月、中国最大の防衛電子機器メーカーで国有企業でもある中国電子科技集団（China Electronics Technology Group Corporation: CETC）が、飛行中のステルス機を検出できる量子レーダーシステムのプロトタイプを開発したと発表した。このCETCが開発したという量子レーダーは、実験成功距離は約96キロメートルとさほど長くはない上、レーダーの性能を裏付けるだけの詳細が発表されていないとして、米国の専門家は実際にはCETCが量子レーダーの実現に成功したかについては疑問が残るとしている[74]。一方で、中国側が量子レーダーの開発に力を入れて進めてきていること自体は事実として表面化したと見ることができる。実際にどれほどの成果が得られているかは明らかでないため、中国の今後の動向を注視していく必要がある。

この量子レーダーについて、米国では2000年代前半から、南カリフォルニア大学、Lockheed Martin社、DARPAなどが開発に取り組んできており、米軍内でも注力して研究開発が行われてきた。2018年10月には、米海軍が電磁スペクトル（electromagnetic spectrum）を、海上、地上、空、宇宙、サイバー空間に匹敵する戦闘ドメインとして指定している。同年8月、米海軍研究所の研究者が、全米科学・技術・医学アカデミー主催のセミナーにおいて、同研究所が力を入れて研究している分野としてスタンド・オフ電磁波量子センシングを指摘している。ノイズに対してシグナルが少ない低観測性の状況下で今までより早く正確にターゲットを探知できるため、量子センシングを重視しているという。そして、中国の研究開発状況を踏まえると、米国が量子センシングの研究開発において最先端を走っているようには見えないとの懸念を隠さなかった[75]。米空軍研究所も、上で見たように、量子技術が空軍の運用能力向上の鍵であるとして研究開発に力を入れており、2019年12月にカリフォルニアで開かれた量子技術の祭典ともいえる国際会議（Q2B）[76]において、空軍が必要とする量子技術について発表を行った[77]。これによると、量子センシ

71 米空軍研究所情報局で量子技術の研究開発に携わるマイケル・ヘイデュク博士は、量子技術の実用化をめぐる最新状況を議論する国際会議Q2Bにおいて、米空軍が今後必要とする技術として、量子時計、量子センシング、量子コンピューティングと並んで量子通信・ネットワーキングを挙げている（Dr, Michael Hayduk, Deputy Director at Air Force Research Laboratory Information Directorate, “Quantum Technologies and Air Force Needs, Quantum Information Science at Air Force Research Laboratory,” Q2B Conference, December 11, 2019）。また、マイケル・グリフィン前米国防次官（研究・工学担当）は、米国議会において、短期的に実現できる量子技術の国防への応用に集中すべきと発言した一方で、長期的に見た量子通信の実現可能性を否定してはいない。（US Department of Defense, “DOD Should Focus on Short-Term Goals in Quantum Science,” March 12, 2020, https://www.defense.gov/Explore/News/Article/Article/2110617/dod-should-focus-on-short-term-goals-in-quantum-science/ （accessed August 16, 2020）.

72 量子鍵配送は、途中で弱まった信号を復元して同内容の情報をより遠距離へ送信するために量子中継器の技術を必要とする。

73 例えば、DARPAには次のような研究プログラムがある。Quantum Information Science and Technology program, https://www.darpa.mil/about-us/timeline/quantum-key-distribution-network; （accessed August 16, 2020）; QUINESS https://www.darpa.mil/program/quiness （accessed August 16, 2020）.

74 2008年に量子レーダーの理論的基礎を発表したマサチューセッツ工科大学のセス・ロイド博士（Seth Lloyd, “Enhanced Sensitivity of Photodetection via Quantum Illumination,” Science 12 Sep 2008: Vol. 321, Issue 5895, pp. 1463-1465）はこのように述べ、防衛目的に耐えうるデバイスの実現にはまだ時間がかかるだろうとの見方を示している。The International Society for Optics and Photonics, “Quantum Radar, Can quantum entangled photons reveal the shape and location of cloaked military fighter jets? Maybe, but probably not yet.,” November 18, 2019, https://spie.org/news/quantum-radar （accessed December 5, 2020）.

75 Lanzagorta, Naval Research Laboratory, “The Future of Quantum Sensing and Communications”

76 「量子技術をビジネスへ（Quantum to Business）」というコンセプトの下、量子コンピュータのソフトウェア開発を行う米国企業QC Wareが主催する国際会議。量子コンピュータのハードウェアやソフトウェアの研究開発に携わる最先端の企業や研究者が集う。

77 Michael Hayduk, Air Force Research Laboratory, “Quantum Information Science at Air Force Research Institute,” Q2B 2019, https://www.youtube.com/watch?v=PO_PKbeVIBU （accessed June 4, 2020）

ング技術を用いて、GNSS[78]や外部電波に頼らず自らの位置や速度を算出する慣性航法装置の強化や、より軽量化され偵察機能も高いセンサーを開発するという。

(b) 国家間競争の側面

量子技術をめぐる米中競争は、研究者や企業間だけでなく、国家間においてもその競争が加速している。2019年10月23日、米国政府は、OSTPの最高技術責任者で大統領副補佐官でもあるマイケル・クラツィオス（Michael Krastios）氏による論稿「米国はどのように量子超越を達成したか」（How America Achieved “Quantum Supremacy”）をホワイトハウスのウェブサイトに掲載した[79]。興味深いのは、この記事が出る直前に「量子超越性」の実証に成功して世界を驚嘆させたのはGoogle社とそこで働く研究者達[80]であったにもかかわらず、「米国が」科学技術において歴史的偉業を達成したと米国政府が強調している点である。さらに、同記事は、わざわざ名指しで中国と比較し、米国が量子超越の偉業を達成できたのは、米国の自由で民主的な国家体制と、それが支える自由闊達な議論の風土、創造性を涵養する科学技術政策があったからだと主張している。

また、米国は自国が開発した技術が中国へ流出することを懸念し、それを防止するための法整備も進めている。2018年8月には、「2019年度国防授権法」[81]の一部として「2018年輸出管理改革法（ECRA）」[82]を制定し、今後、安全保障のための重要な「新興・基盤的技術（emerging and foundational technologies）」も輸出管理の対象とする方針を示している。この検討されるべき新興・基盤的技術として14の技術が指定されているが[83]、AI、極超音速技術、バイオ技術等と並んで、量子技術も指定されている。米国政府が、量子技術の獲得競争を、安全保障と経済のための米中競争という大きな流れに明確に位置付けていることがうかがえる。

(c) トランプ政権及びバイデン政権における政策

この量子技術の研究開発における米中間の競争は、トランプ（Donald Trump）政権下での米国の敵対的な対中政策を受けて加速してきたように見える。というのも、米国の科学技術政策の専門家は、トランプ政権下では米国の科学技術政策は全体として後退したと評価しているにもかかわらず、量子技術政策に関しては、トランプ政権下で複数の具体的かつ新しい政策が打ち出されているからである。例えば、オバマ政権で科学技術担当大統領補佐官及びOSTP長官を務めたジョン・ホルドレン（John P. Holdren）博士は、トランプ政権は前政権が追求してきた様々な国内あるいは国際的な科学技術プログラムの多くを打ち切ったり遅滞させたりしてきたと評価している[84]。にもかかわらず、量子技術政策だけは例外で、政策文書や関連法を立て続けに策定するなど、むしろトランプ政権下で複数の政策が打ち出されてきたのは事実である。2017年末以降、米国の対中警戒は政治、経済、軍事の全般にわたって先鋭となったが、技術覇権の争奪を背景とした米中間の貿易摩擦によって、将来のゲームチェンジャー技術とも

78　全球測位システム（Global Navigation Satellite System: GNSS）。GPS、GLONASS、Galileo等の衛星測位システムの総称。
79　White House, “How America Achieved “Quantum Supremacy,” https://www.whitehouse.gov/articles/america-achieved-quantum-supremacy/ (accessed 15 June 2020). クラツィオス氏のツイッター公式アカウントのプロフィール写真には、フェルミ米国国立研究所の量子研究所（Fermilab Quantum Institute）にある希釈冷凍機を物理学者と覗き込む彼の写真が使用されている。
80　Arute et al., op.cit., pp.505-510.
81　H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019
82　H.R.5040 - Export Control Reform Act of 2018
83　U.S. Department of Commerce, The Bureau of Industry and Security, “Review of Controls for Certain Emerging Technologies” (November 19, 2018)
84　2020年11月10日、ホルドレン博士は、政策研究大学院大学（GRIPS）科学技術イノベーション政策研究センター主催のウェビナー「SciREX Webinar 変わりゆく世界での科学技術と国際関係」において、クリントン政権およびオバマ政権における科学技術政策と比較して、トランプ政権の科学技術政策をこのように評価した。

言われる量子技術をめぐる米中競争が米国の政策関係者の耳目を集めたのではないかと考えることもできる。

バイデン（Joe Biden）大統領とハリス（Kamala Harris）副大統領は、科学に理解があり科学技術に関する事実や専門家の意見を尊重すると評されている。ホルドレン博士によれば、次期米国政権は国内外の科学技術振興政策、環境問題、STEM教育推進などにおいてオバマ政権時代の科学技術政策を取り戻すよう尽力すると言う。その大きな枠組みの中で量子技術政策も扱われるのであれば、またバイデン大統領の対中姿勢がそこまで大きく融和に傾くとは考えられない現状も考慮すれば、米国の量子技術政策は引き続き推進されていくのではないかと考えられる。さらに、ハリス副大統領は2018年6月に、量子コンピューティングが米国の安全保障にとって不可欠であるとの認識の下[85]、国防総省が主導する防衛目的に特化した量子研究コンソーシウム[86]の設立を目指して、上院軍事委員会に「量子コンピューティング研究法案（Quantum Computing Research Act of 2018）」を提出している[87]。米海軍研究所（Office of Naval Research: ONR[88]）と米陸軍研究所（Army Research Laboratory[89]）、OSTPを中心とした量子研究のための共同体の創設を求めるこの法案は、当時の米国議会の政治的な理由から廃案となったが、この動きを主導したハリス副大統領が任期中にどのような量子政策をとるのかについては注視していく必要がある。

1957年にソビエト連邦が人類史上初の人工衛星スプートニク1号の打上げを成功させた後、米国は、宇宙開発競争に打ち勝つべく、1958年にNASAを設置して有人宇宙飛行の達成を目指したが、その時代さながらの量子コンピュータ開発競争、「21世紀版スプートニク・ショック競争」が始まっているといっても過言ではないだろう[90]。

5 おわりに

量子コンピューティング、量子通信、量子センシングは、計算能力や情報通信能力を飛躍的に発展させる可能性を秘めており、コミュニケーションやネットワークが死活的に重要になっている現代の戦争において、電子戦、ステルス技術、ISR、C4I、精密誘導、情報の秘匿に影響を与える可能性がある。

クレピネヴィッチによれば、前述のとおり、RMAは、（1）技術革新、（2）新たな兵器・システム開発、（3）戦闘ドクトリンの開発などの運用上の革新、（4）組織的受容という4つの要素が結び付き、戦争の様相と行為を「根本的に変化させた」ときに起こる。このテーゼに照らしたとき、（1）の技術革新は起きつつあり、量子技術を活かした防衛装備や兵器の開発も一部の国では既に着手されており、（2）のフェーズに入っている。

（3）の運用上の革新が起きているかについては、未だ断言しがたい。先見の明ある一部の軍人は、量子技術がもたらすインパクトを認識してその研究開発の動向を注視しているが、それが戦闘ドクトリンにまで取り込まれていると言えるほどの証左は公には未だ見当たらない。例えば、米軍の現在の統合作戦に関する戦闘ドクトリン、その通信システムに関する文書を見ても、2019年のサイバー軍の役割拡大に関する記述変更や電磁スペクトラム関連の

85 Press Release, “Harris Introduces Bill to Increase Resources for Quantum Computing and Research to Benefit National Security (June 07, 2018),” https://www.harris.senate.gov/news/press-releases/harris-introduces-bill-to-increase-resources-for-quantum-computing-and-research-to-benefit-national-security (accessed December 4, 2020).
86 産業界、アカデミア、政府組織間の量子研究の取組みを調整・監督し、補助金を支出するための研究共同体の創設を目指していた。
87 S.2998 - Quantum Computing Research Act of 2018, 115th Congress (2017-2018)
88 科学技術の重要性に鑑み1946年に海軍省のもとに設立された米海軍の研究所。米海軍および海兵隊の科学技術研究の計画策定、大学・政府系研究機関・非営利機関・企業等を通じた計画の実行・推進を任務とする。
89 1992年に米陸軍内に創設された研究所。コンピュータ・情報科学、センサー・電子デバイス、人間工学、生存時間・致死性、兵器・材料、車載技術などについて研究を行っている。
90 藤井啓祐、前掲書、118−119頁。

追記などは見られるが、量子通信や量子センシングに関するはっきりとした記述はない[91]。

しかしながら、現代の戦闘において電磁波領域が主要なドメインの1つとして重要視されるようになっており、情報通信技術の能力強化が枢要であることが軍関係者の常識となっている今、量子技術の重要性を加味した戦闘ドクトリンが作成され、それが軍組織に受容されるのは、時間の問題と言えるかもしれない。ただし量子技術は、コンピューティング、情報収集、通信を支える基盤技術であり戦闘ドクトリンに明示的には示されるとは限らない。さらに言えば、量子技術は、先に手に入れてしまった側が大きな優位を獲得するゲームチェンジャー技術となり得るため、秘密裏に戦闘ドクトリンが開発されている可能性はあるだろう。

米国は近年、量子技術、特に量子センシング技術を国防へ活用することに積極的な姿勢を示しているように見える。具体的な政策は既に述べたとおりだが、2020年7月13日、エスパー前国防長官は、ホワイトハウスで最高技術責任者を務め量子技術政策の推進に力を入れてきたクラツィオス氏を国防次官代理（研究・工学担当）に任命した[92]。

そのような米国と同盟関係にある日本は、どのような日米協力を検討していくべきか。日本政府においては、内閣に設置された統合イノベーション戦略推進会議が2020年1月に「量子技術イノベーション戦略」を策定した。この量子戦略では、安全保障貿易管理が盛り込まれた一方で、それ以外の安全保障上の観点からの記述は見当たらない。中長期的な視点で日本の防衛力を定める直近の防衛大綱では、量子技術の研究開発に関する具体的な記述はないものの、防衛装備庁が策定した研究開発ビジョンでは、主な研究開発の進め方の1つとして、「量子コンピュータ・センシング・通信といった量子技術等の将来のゲームチェンジャーとなりうる技術は、ボーダーレス化・デュアルユース化が進展し、特に民生分野において進展が速いことから、国内外の技術の進展に合わせて、継続的な技術向上および最先端技術の反映に努める」としている[93]。これは努力目標として記述されており、具体的な応用技術の獲得に向けてどの程度の予算・プログラムが企図されているかは定かでないが、我が国の防衛当局が安全保障分野における量子技術の活用に目を向けていることは確かである。今後、安全保障分野への量子技術の影響について、大学・研究所や量子スタートアップ企業の研究者に協力を仰いで積極的な分析・検討が進められることが期待される。

量子技術の研究開発は、それがもたらすインパクトを考えると「21世紀を規定する安全保障上の優位性をめぐる争い」という側面がある。ハリス米国副大統領の次の言葉[94]は、これを的確に表している。「量子コンピューティングは、私たちの世界を変える次の技術フロンティアであり、米国は後れを取ることはできない。量子コンピューティングは、次世代の雇用を創生し、疾病を治療し、国をより強く安全にする。量子コンピューティングに関する十分な研究や調整がなければ、サイバー空間における世界的競争で後れをとるリスクを侵し、それは敵対国からの攻撃に対して脆弱になることを意味する。この技術の発展に立ちふさがる課題に、我々は今こそ対処しなければならない。我々の未来は、そこにかかっている。」本稿ではあまり触れられなかったが、量子技術は伝統的な安全保障の側面だけでなく、経済安全保障を含むより幅広い安全保障分野に影響を与える。国家としてどこまで量子技術に投資するかは、ゲー

91　Joint Chiefs of Staffs, “JP-6.0, “Joint Publications Communications System, 10 June 2015, Incorporating Change 1, 04 October 2019,” https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_0ch1.pdf?ver=2019-10-15-172254-827 (accessed July 23, 2020).
92　U.S. Department of Defense, Release, “DOD Names Acting Under Secretary of Defense for Research and Engineering (July 13, 2020),” https://www.defense.gov/Newsroom/Releases/Release/Article/2271633/dod-names-acting-under-secretary-of-defense-for-research-and-engineering/ (accessed July 23, 2020).
93　防衛装備庁「研究開発ビジョン スタンド・オフ防衛能力の取組（多次元統合防衛力の実現とその先へ 解説資料）令和2年3月31日」、12頁。本資料では、31防衛大綱の「島しょ部を含む我が国への侵攻を試みる艦艇や上陸部隊等に対して、相手の脅威圏の外から対処を行うためのスタンド・オフ能力等の必要な能力を獲得するとともに、(…)関連する技術について総合的な研究開発を含め、迅速かつ柔軟に強化する。」との方針の下、将来のゲームチェンジャー技術となりうる量子技術の反映に努めるとしている。
94　Press Release, “Harris Introduces Bill to Increase Resources for Quantum Computing and Research to Benefit National Security (June 07, 2018)”

ムチェンジャー技術である量子技術がもたらす優位性を獲得できるかどうかを決定づける大きな要素となる。今こそ、量子技術が国家安全保障にもたらすインパクトに真剣に向き合うべきときであろう。