2.3.6 量子情報・通信

（1）研究開発領域の定義

量子力学が記述する電子や光子などが持つ性質（量子性）を積極的に活用して、古典系では実現できない情報処理機能・性能を実現するための研究開発領域である。超伝導量子ビットを筆頭にイオンなどさまざまな物理系で研究開発が進められている量子コンピュータ、冷却原子系やイオン系での開発が進む量子シミュレータ、実装に向けた開発が急速に進んでいる量子暗号、将来に向けた基礎研究の段階にある量子中継・量子ネットワークなどが含まれる。

（2）キーワード

量子情報科学・技術、量子コンピュータ、Noisy Intermediate-Scale Quantum（NISQ）computing、量子誤り訂正、量子シミュレータ、量子アルゴリズム、量子アニーリング、量子通信、量子暗号鍵配送、量子中継、量子ネットワーク、超伝導量子ビット、冷却原子、イオントラップ、半導体量子ビット、光量子ビット、スピン量子ビット、トポロジカル量子計算、量子乱数生成、量子メモリ

（3）研究開発領域の概要

［本領域の意義］

量子力学は、20世紀において半導体、NMR、レーザなどの基礎となり、私たちの生活を陰ながら支えてきた。21世紀に入り個々の量子系を精密に制御する技術が発展・成熟してきたため、その量子性を積極的に利用することによって初めて可能となる応用をめざした研究が進められている。その代表例は、従来の古典的な論理演算に基づいた情報処理の原理を量子力学へと拡張する、量子情報処理である。ムーア則に基づく情報処理能力向上への減速感から新たな概念の情報処理技術への社会的なニーズも高く、量子情報処理は学術的な価値だけでなく社会課題の解決に直接貢献できる技術としての役割が期待される。2019年に、従来型コンピュータのパフォーマンスを量子コンピュータが超える「量子優位性」を証明した、と主張する実証実験の報告がなされ、量子情報処理の実用性にエビデンスを与える流れがみえてきた。計算原理として量子力学を利用する量子コンピュータや、実際の物質系と同じ模型を人工的に作り出す量子シミュレータは、従来の古典コンピュータで解くには効率が悪い問題を高速で解くことができると期待されている。

また、量子性は計算速度だけではなく、通信におけるプライバシーについても従来の古典情報処理では実現できない安全性を担保することができる。近年、軍事・外交機密を筆頭に、ゲノムデータや製薬情報など、長期間秘匿性を担保する必要のある情報が電子的に伝送、保管、処理されるようになっているが、実用的な量子コンピュータが実現されると、現代の暗号方式で守られていたデータが全て解読される事態が懸念される。この懸念を解決するには、将来的な通信の秘匿性・安全性確保に有用な量子暗号技術や、グローバルなセキュアサイバー空間を実現するための、衛星光通信技術やネットワーク構築技術を含む量子中継・量子ネットワーク技術が必要となる。また量子暗号技術は、フィジカル空間とサイバー空間が融合したSociety 5.0の可用性と安全性を高めるために重要である。一方で、量子中継技術は異なる情報担体（例えば光子と超伝導量子ビット）の間のインターフェースともなりうるので、分散型量子コンピューティングの実現にも重要である。

真に有用な量子コンピュータの実現には、新たな材料系や集積デバイス、実装、システム技術などの基盤技術の総合的な高度化が必須であり、量子コンピュータは広く科学技術領域の研究開発にかかわるフラッグシップハードウェアとしての役割を果たしうる。また、量子情報科学は、これまで考えられてきた問題に新た

な基礎的視点を与える。量子情報を経由することによって、例えば、従来の情報科学の定理が簡単に証明される、新たな古典アルゴリズムの発見に貢献するなど、従来の情報科学へのフィードバックが期待される。また、新奇な物性をもつ物質の発見や、ブラックホールなどの基礎物理への多大な貢献につながりつつある。量子情報科学は、未来のテクノロジーや基礎学理に大きく影響を与える研究開発領域であり、私たちの日常生活を根底から変えうる可能性を秘めている。

［研究開発の動向］

• 量子コンピュータ・量子シミュレータ

2020年代を迎えても量子コンピュータの研究開発は加速的な拡大傾向が続いている。その流れは世界中に及び、各国がそれぞれの国家戦略を構築しそれに基づいた新たな国家プロジェクトが進んでいる。特に米国、EU、中国は巨額の投資の下で活動しており、今後にわたりその動きが注目される。日本でも内閣府により量子技術イノベーション戦略が2020年に策定され、理化学研究所を中心とした国内産学連携体制が整いつつある。産業界としては米国GoogleやIBM、インテル、マイクロソフトなどの大企業に加えて、米国、カナダ、欧州ではベンチャー企業も参入し存在感を高めている。日本の産業界でもNEC、富士通などハイパフォーマンスコンピューティングに強い企業の参入が始まった。

研究開発において現在先行している超伝導量子コンピュータでは、Google、IBMなどのトッププレーヤーは50～70量子ビットのレベルでの高精度な量子ビット制御に取り組んでいる。Googleは2019年に53量子ビットの量子コンピュータで量子優位性を実証したと発表し、世界中で大きな話題となった。量子優位性を実証するために設計されたタスクに対してではあるが、用いられた量子コンピュータがハードウェア技術として古典コンピュータを凌駕するレベルにいたったことが実証された。超伝導量子コンピュータではマイクロ波を用いた量子ビット制御が行われるが、これに必要な高密度（多ビット）の高周波生成・制御システムの開発、パッケージ技術、それを格納できる冷凍機の大型化に成功したことを意味しており、ハードウェア技術として100量子ビット以上のスケーラブルな量子ビットの精密制御が可能なレベルに到達しつつあるといえる。また、今後数年間で1000量子ビットが達成されると期待されている。一方で、量子ビットの数が増えるだけでは性能を発揮することができないので、量子ビット操作に伴う演算精度にも注目していく必要がある。量子ビットの方式からハードウェア構成にいたるまで、精度とスケーラビリティをどのように両立し、実現するかが今後の競争軸となるだろう。

超伝導量子ビット以外の方式ではイオントラップ方式で集積化が進んでいる。研究開発で先行し、クラウド経由でプロセッサの提供を行っているIonQに加えて、Honeywellも2020年に開発を始めたことが発表された。光を量子ビットに用いる方式でも、スケーラビリティを確保しうる手法や、シリコンフォトニクス等を活用する小型集積化への試みがなされている。シリコン量子ビット方式では、2ビットレベルの高精度（99 %超）の量子状態制御に成功した。

現状の量子コンピュータは、1つひとつの量子ビットに生じる誤りはわずかであっても、計算を長く続けるとそれが積み重なって間違った計算結果を生んでしまう。したがって、大規模な量子コンピュータの実現には、量子誤り訂正を実装した、ノイズ耐性のある量子コンピュータの実現が必須である。誤り訂正に必要となる量子ビットの数は100万とも1億ともいわれており、そのような大規模集積化の実現には20年以上が必要とされている。量子誤り訂正付きの量子コンピュータ実現はさらに先とみられてきたが、「量子優位性」というマイルストーン的な成果が出た流れのなかで、量子誤り訂正の実現へ向けた基礎研究が本格化するものと推測される。その一方で、演算精度がさほど高くなく、量子ビット数も数十から数百程度といった近未来に実現

可能な量子コンピュータでもスーパーコンピュータを上回る潜在能力を持っているため、それを有効活用しようという動きが出てきている。この新たな方向性はNoisy Intermediate-Scale Quantum（NISQ）技術と呼ばれ、世界的に活発な探索が行われている。特に、量子コンピュータを用いた変分量子アルゴリズムの量子化学計算や機械学習への応用がさかんに研究されている。それに加え、エラーによる影響を統計処理によって補償するノイズ補償技術の開発も進められている。

ここまで説明したのはゲート型量子コンピュータ（万能量子コンピュータ）と呼ばれる。その高速性の保証されたゲート型量子コンピュータ以外にも、超伝導量子ビットを用いてイジング問題の最適化に特化した専用量子マシン、いわゆる量子アニーラの研究開発がカナダのベンチャー企業 D-WaveやNECを中心に着実に進められている。超伝導量子アニール方式をとるカナダのD-Wave社は5000量子ビット超の商用ハードウェアシステムを発表するなど集積化を進めており、関係のユーザー企業やミドルウェア企業とのエコシステム構築が進んでいる。冷却原子による量子シミュレーション技術においても、シミュレーションの自由度を向上させるリュードベリ軌道電子の高速生成と制御に成功するなど実用性拡大へ向けた活動が進んでいる。

• 量子通信（量子暗号、量子中継・量子ネットワーク）

量子暗号鍵配送（QKD）は1984年のBB84プロトコルの提案に始まり、一般的な攻撃に対する安全性証明やQKDをサブプロトコルとして用いることを保証する組み立て可能性（Composability）の証明が進み、2010年ごろまでには理論的基礎が確立した。その後、装置の不完全性があっても成立する安全性理論の開拓が始まり、2010年ごろからは実験家と共同で、実装されたデバイスの特性にまで踏み込んだ解析と対策が進められている。この実装安全性の研究は、欧州電気通信標準化機構（ETSI）や国際標準化機構（ISO）におけるQKD装置の安全性保証の標準化の動きに強い影響を与えている。同時に実装の不備を突く古典的デバイスによる攻撃法（サイドチャネル攻撃）の研究も一時脚光を浴びた。現在は攻撃方法とその対策を整理することで安全性保証の標準に組み込まれようとしている。

QKDの弱点とされていた伝送距離と速度の問題を解決すべく研究開発が進められ、2015年ごろまでにはデコイBB84プロトコルを実装したクロック周波数1GHz台の実用的な装置が、東芝とNECによって完成された。近年、さらなるクロック周波数向上に向けた研究開発がスイス、中国、日本などで始まっている。

連続量（CV）QKDは従来型のコヒーレント光通信の部品のみで構成できるため、既存技術との親和性が高く、低価格のQKD装置となりうる。2019年にホモダイン検出の周波数弁別特性を活かして光通信とのファイバコア共有が実証され、近距離での実用化が期待される。その一方で、実装安全性を含めた無条件安全性の証明が未だになされておらず、デコイBB84の水準には達していない。

一方、QKDは一度に鍵を伝送できる距離、速度に限界がある。このため現状では、安全性の保証された局舎（trusted node）を介したネットワーク化が行われている。最初期の例としては、米国の高等研究計画局（DARPA）がWashigton DCで行った実験がある。ネットワークの制御まで行った例としては、ウィーン市内で欧州の研究機関が構築したSECOQCがある。日本でも2005年ごろから量子暗号ネットワークの検討が始まり、2010年世界最高速のネットワークとしてTokyoQKDが稼働した。2017年に中国が北京-上海間2000 kmの幹線と合肥などでの都市ネットワークを完成させ大型化で先行している。米国でも民間企業がQKDネットワークを提供している。欧州でもEUと各国（英国、ドイツ、イタリア、スペインなど）が量子ネットワークの建設を進めている。最近ではQKD装置を局舎でつなぐだけでなく、鍵生成の制御、生成した鍵の管理、供給といった安全な鍵をアプリケーションに提供するプラットフォームとしての研究開発が進められ、一部は国際電気通信連合・電子通信標準化部門（ITU-T）で標準化作業が行われている。

量子中継は量子もつれスワッピングを用いて隣接しているノード間の量子もつれを離れたノード間の量子もつれに変換していくものである。そのためノードにおける2つの量子ビットの量子もつれ状態（Bell状態）測定の実現が注目された。また、伝送路の光子損失のため光子対の片方が届かないことによるスケーラビリティの消失の問題が指摘され、研究の1つの焦点は量子メモリに移った。量子メモリの主な構成要素としては、原子集団（atomic ensembles）、共振器量子電磁力学（cavity QED）、結晶中の色中心（color defect centers）などが提案されている。メモリ（コヒーレント）時間、フィデリティ（忠実度）など全ての性能指標を満たすものはまだ実現されておらず、しばらくは複数の候補が並行して研究されるものと考えられる。量子メモリの研究開発とともに、量子メモリのコヒーレンス保持時間の要求を低減させるためのアーキテクチャの研究も進められている。今後は誤り訂正技術の研究開発も必要となる。量子メモリを用いない方法として、光だけによる量子中継も提案されているが、光子のクラスター状態を用いた量子誤り訂正を基本としているため、実現には解決すべき問題が多く残されている。

（4）注目動向

［新展開・技術トピックス］

• 量子優位性を実証できるレベルの量子コンピュータシステム技術

Googleが超伝導量子ビット方式で開発した53量子ビットマシンで量子優位性を実証した、と2019年に発表した。ランダムに選ばれた量子ビットに対しての1量子ビット演算と隣接する量子ビットに対する2量子ビット演算を繰り返すというランダム量子回路からの出力をサンプリングするというタスクにおいて、量子コンピュータが200秒で実行できたのに対して既存のスーパーコンピュータでは1万年以上かかると見積もられた。スーパーコンピュータの計算手法の改善による時間短縮も報告されているが、依然として量子コンピュータでの200秒に対するギャップは埋まっていない。また、スーパーコンピュータが数千ノードの計算機システムであるのに対して、量子コンピュータが1台の希釈冷凍機中の1チップを用いた計算であることを留意しておくべきである。この成果は、50ビットレベルのエラーレートの極めて小さい量子状態制御がハードウェアとして実現したことを意味する。すなわち、量子ビット、読み出し回路、結合回路の設計と超伝導チップの均一性の良い集積技術、チップ同士を3次元的にフリップチップボンディングする多層配線技術、室温からのマイクロ波による精密制御技術が総合的に動作できる環境が整ったといえる。

• NISQ時代の研究開発

NISQ技術の主なターゲットは、(i)量子による計算の加速を科学的に実証する量子優位性の実証、(ii)大規模な量子コンピュータに発展させる要素技術の実証基盤の確立、(iii)古典コンピュータと合わせてその性能を最大限に引き出す古典-量子ハイブリッドアルゴリズムの開発、の3つである。(i)については、2019年にGoogleによって量子優位性が示された。しかし、これは特定のタスクにおいて実時間でスーパーコンピュータに比べて速い、という結果にすぎず、計算量理論的な計算の加速の実証にはまだいたっていない。量子計算理論分野では、量子加速を実験的に検証するための方法が構築されつつある。

長期的な視点に立ち、大規模な量子コンピュータを実現するためには、量子誤り訂正が必須であることは依然として変わっていない。(ii)では、50量子ビット級の量子コンピュータを用いて1つの論理量子ビットに対して量子誤り訂正を実証することが次のマイルストーンになるであろう。また、1万量子ビットへと拡張するためには、現在の制御方法をそのまま拡張するのでは不十分である。大規模化に向けた技術的課題をあぶり出し、それを解決するための方策をNISQデバイスで検証しながら研究開発を進めることが理想的である。

(iii)では、NISQを意味のあるタスク、量子化学計算、近似最適化、機械学習などへ応用する試みが行わ

れている。古典コンピュータでもできる処理と量子コンピュータが得意なタスクを分離し、それぞれを接続して処理を行う量子-古典ハイブリッドアルゴリズムの研究が進められている。

• QKD商用化の動き

中国でQKD機器を開発しているQuantumCTekが、2020年の7月に上海NASDAQ市場に上場し、初日に914%という記録的な値上がりを記録した。このことは研究や安全保障の観点で語られてきた量子暗号技術が民間の投資の対象となったことを示している。日本でも、2020年10月に東芝が、2020年度第4四半期より、国内外での量子暗号通信システムのプラットフォームの提供およびシステムインテグレーション事業を順次開始することを発表した。国内外で、QKDネットワークを構築し、金融機関を中心とした顧客向けQKDサービスを2025年度までに本格的に開始する予定である。

• QKDの長距離化技術

QKDの長距離化技術として、2018年に英国の東芝欧州研究所が、量子メモリを使わずに量子中継1回分の長距離化を実現できるTwin-Field QKD方式を提案し、原理的な実証に成功した。最近では509㎞の伝送に成功している。しかし、この方法は異なる光源の間での位相同期が必要になり、実用にはまだ障害が残っている。位相同期は、コヒーレント光通信やCV-QKDと共通な課題であるので、これらの研究開発から解決策が見出される可能性もある。

もう1つの長距離化技術として、衛星を用いたQKDシステム開発の動きがある。現時点で、グローバルな鍵配送を可能にする唯一の方法であることが主な理由である（地上で大陸を横断するためには、他国の領土に局舎を置く必要があり、非現実的）。2017年に中国が世界初の衛星-地上間 QKD 実証を発表しており、また日米欧それぞれで衛星量子暗号の研究開発が進められている。重要な技術要素の1つは光子レベルでの光ビームの捕捉追尾である。

• 量子中継技術

量子中継、または量子インターネットについては、デルフト工科大学（オランダ）のQuTechプロジェクトが注目されていたが、米国でも研究が本格化している。特にシカゴ大学とハーバード大学の研究グループが注目される。シカゴ大学とアルゴンヌ国立研究所は共同で、量子ネットワークのプロトタイプを開発している。2020年2月にシカゴ郊外の敷設済みファイバを使い、52マイル（約84 km）の量子もつれ共有に成功したことを発表した。また、ハーバード大学、MIT、BBNテクノロジーズが共同でBoston-area Quantum Testbedを運用しており、新しいQKDプロトコルやデバイスのテストとともに、量子中継に用いる量子メモリのインストールを行おうとしている。ハーバード大学のグループは1次元フォトニック結晶共振器の中にシリコン空孔センターを入れたデバイスを試作しており、量子中継に必要な量子メモリの候補として注目される。

［注目すべき国内外のプロジェクト］

［日本］

2020年1月に策定された量子技術イノベーション戦略により、わが国として研究開発や産業化・事業化を促進するための指針が示され、イノベーション創出に向けた重点推進項目として、「重点領域の設定」「量子拠点の形成」「国際協力の推進」が掲げられた。

量子コンピュータ関連では、JST ERATO中村巨視的機械プロジェクト、JST CREST「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」、JSTさきがけ「量子の状態制御と機能化」が2016年度に発足した。また2018年度からは文科省Q-LEAPプロジェクトが開始し、理化学研究所における超伝導量子ビットハードウェア開発をフラッグシップとして、イオントラップ、半導体量子ビット、量子ソフトウェアなど、量

子コンピューティングに関する研究が強化されてきている。 SIP「光・量子を活用したSociety 5.0実現化技術」（2018年度～）でイジング型コンピュータ、NISQ コンピュータ等のソフトウェア開発が進められている。2019年度からはJSTさきがけ「革新的な量子情報処理技術基盤の創出」が開始され、2020年度からは、NISQ型量子コンピュータの応用研究を中心とする文科省Q-LEAPプロジェクト「量子AIフラッグシップ」が発足し、量子ソフトウェア領域の研究強化が始まっている。同じく2020年度に、内閣府ムーンショットプロジェクトの目標6に「2050年までに、経済・産業・安全保障を飛躍的に発展させる誤り耐性型汎用量子コンピュータを実現」が設定された。さらに、NEDOは2020年に「高効率・高速処理を可能とするAIチップ・次世代コンピューティングの技術開発/【研究開発項目〔2〕】次世代コンピューティング技術の開発」に関する公募を行った。このなかに“量子コンピューティング関連技術”があげられており、アニーリングマシン開発および周辺技術開発が含まれている。2020年に、大学などを中核とした産学連携を推進するためのプログラムである、JST共創の場形成支援プログラム 本格型 政策重点分野「量子ソフトウェア研究拠点」が開始した。加えて2020年度からは、持続的な量子技術分野の人材層の強化を目標とした文科省Q-LEAPプロジェクト「人材育成プログラム」が開始した。以上のように、中期的・長期的な目標設定のもと、量子コンピュータ関連の研究が加速されている。

一方、量子通信については、SIP「光・量子を活用したSociety 5.0実現化技術」（2018年度～）でQKDネットワークの実用化研究が行われている。また、量子通信に関する基盤技術開発の底上げのため総務省の直轄プロジェクトとして「グローバル量子暗号通信網構築のための研究開発」が2020年度から開始される。これは初年度14.1億円を投じて、QKD技術の高度化（高速化、長距離化、耐環境性の向上）とネットワーク管理技術、量子中継技術に関する研究開発を民間企業、大学、国研から12機関が参画して行うものである。

［米国］

米国では、2018年に出された国家戦略方針（The National Quantum Initiative Act）に基づく国家プロジェクト投資が進んでいる。大統領府は2021年度の予算要求として量子情報研究に4億6700万ドルを計上した。エネルギー省（DOE）は2020年1月に、米国内に2つから5つの学際的な量子情報科学（QIS）研究センターを設立するため今後5年間で最大6億2500万ドルを投資すると発表した。他にも全米科学財団（NSF）などからの国家プロジェクトが複数公募されている。

現在米国では量子インターネットの基盤技術開発のためにThe Chicago Quantum Exchange（CQE）が設立され、シカゴ大学とアルゴンヌ国立研究所、フェルミ加速器研究所が中心となり、中西部の3大学と2020年7月現在15企業パートナーが参加している。また、ブルックヘブン国立研究所を中心としてオークリッジ国立研究所、ロスアラモス国立研究所とストーニーブルック大学がニューヨークでテストベッドを建設している。量子インターネットに向けた動きがDOEとその傘下の国立研究所を中心に進められている。

［中国］

2019年には中国科学技術大学（USTC）が超伝導量子ビットで12ビットの動作を報告し、また2020年12月には、光を使った量子コンピュータで量子優位性の実証に成功した、と発表した。 USTCは、建設が進められている量子情報科学国家実験室（2020年末に第1研究棟完成）と同じ安徽省合肥市にあり、大型研究開発拠点として中国の研究開発加速の中心となるものと思われる。中国科学院と中国IT大手のアリババ(阿里巴巴）グループは、共同で量子計算実験室を設立し量子情報科学の先進的研究、量子コンピュータの開発に取り組んでいる。現在、11ビットの量子コンピュータのクラウドサービスを展開している。

［欧州］

EUでは2018年にEU Quantum Flagshipが採択され活動している。前半は立ち上げフェーズであ

り、2021年から本格化の予定である。この間、2019年にはQuantERAコンソーシアムによる20Mユーロを投じるプロジェクト公募もなされた。この公募は2017年に次いで2度目である。ドイツでは、EU Flagshipの一翼をなすOpenSuperQプロジェクトで、ユーリッヒ研究所にD-Waveのコンピュータを2021年までに導入する計画を発表している。英国は2014年から進められているThe UK National Quantum Technologies Programmeに対する2019年からの追加投資が表明された。産業界からの投資も含めて総額3億5000万ポンドになる。フランス・イノベーション省（MESRI）が量子国家戦略を2021年1月に発表。量子コンピュータ、量子暗号・通信、量子センサなど7つの分野に5年間で18億ユーロを投資する予定であると表明した。

量子通信基盤の構築に向けたEuroQCI initiativeが進められており、これをサポートするように2019年6月にEuroQCI declarationが採択され、現在25カ国が署名している（2020年10月）。また、QKD実用化のため2019年9月から3年間のプロジェクトOPENQKDが始まっている。ここではQKDを組み込んだ通信インフラの実現をめざして15百万ユーロの予算、38機関（13カ国）からなるコンソーシアムが組まれている。

（5）科学技術的課題

今後は量子ビットの精度向上とシステムとしてのスケーラビリティを同時に実現することがより重要になる。物理研究だけではなく、広く材料科学、デバイス集積技術、3次元実装技術、高周波制御回路、実装部品、冷凍機、システムアーキテクチャなどの広い分野にわたる協業が重要になるものと思われる。これらの技術開発により、現在主流の超伝導量子ビットやほかの方式においても技術的制約・課題が顕在化する可能性があり、どこにブレイクスルーが必要なのかが明確になるだろう。

NISQの応用研究は、この1、2年でかなりの広がりを持った反面、いろいろな課題も浮き彫りになってきた。変分量子アルゴリズムにおける量子状態の表現能力を向上させるためには量子計算のステップ数を増やす必要があるが、パラメータの勾配が消失してしまう問題が生じており、初期パラメータの選択法やパラメータの更新方法において新たなブレイクスルーが必要である。また、扱える問題のサイズにも制限があり、量子化学計算や機械学習などにおいて興味のある対象を扱うにいたっていない。量子コンピュータ実機を使えるメリットを毀損しない形で問題分割し、小規模な量子コンピュータ上で実行可能にするなど、より高度なアルゴリズム設計が求められている。

大規模な量子ネットワークの実現のためには量子暗号通信の高速化や長距離化が必須であるが、長距離化には検出器の低雑音化やTwin-Field QKDなどの新たなプロトコル開発が必要である。また、グローバルネットワークに接続するローカルネットワークでは、低コスト化のために既存の光通信との共存が望まれ、雑音耐性の高いQKDシステムの開発が必要となる。一方、大規模なネットワークでは、異なる方式・異なるベンダの装置の相互接続も課題となる。また、量子セキュアネットワークとしてのキラーアプリの確立も重要な課題である。将来的な全量子ネットワーク実現のためには、十分離れた中継点に置かれた量子メモリ間を光でリンクする必要があり、量子波長変換や光と量子メモリのインターフェース、誤り訂正技術が必要である。

（6）その他の課題

量子技術への国家プロジェクトや産業界からの投資がなされ、研究開発拠点が形成されるなか、世界的に量子技術の人材が不足していくことが予想される。わが国に注目すると、時限的拠点による人材育成以前に、その基盤となる大学における教育体制や安定的地位についた指導側の人材が圧倒的に不足している。基盤予算の削減による大学教員の減少のなか、特に理論分野は海外と比して全くもって脆弱な体制である。国内の

研究者への安定的な地位の拡充や、数少ない既存の研究者が研究教育に専念できる環境や制度の構築、待遇の改善による海外研究者の取り込みによる長期的な教育体制を敷かなければ、量子技術の分野で世界と競争し存在感を示すことは難しいだろう。

量子コンピュータや、量子通信の研究開発は、挑戦的・総合的な工学研究の様相を呈し始めており、これまでの物理学のスキルを中心とした量子人材は視野をより広げることが求められる。同時に、周辺の研究開発分野に携わる人材の関与がますます必要となるため、厚い人材層や周辺技術を保有する産業界とは特に連携を図るべきであり、そのための補助金や研究開発コンソーシアムの形成などの体制づくりが望まれる。また、量子技術を啓蒙する場を作り人材の広がりと育成を図る必要があり、量子技術イノベーション拠点ではこのような活動を強化すべきである。

また、各国が国をあげて研究開発に取り組んでいることから、国家間の技術的な機密性が高まることが予想される。最終形態の量子コンピュータばかりでなくそれを構成する各種要素技術も高度な機密技術となり、必要な要素技術の調達が困難になる可能性もある。要素技術を含むキーとなる技術の育成戦略も重要となる。

（7）国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	→	量子技術イノベーション戦略が策定、基礎研究から実用化へつなぐ戦略と体制ができた。理化学研究所（Q-LEAPフラッグシッププロジェクト）、大阪大学量子情報・量子生命研究部門、慶應義塾大学量子コンピュータセンターなど、拠点形成が進み、関連研究のシナジーがみえてきている。JST ERATO、CREST、さきがけ、などのプロジェクトにおいて幅広く基礎研究が支援されている。 量子暗号通信に関する理論的研究は東京大学、名古屋大学、富山大学、慶應義塾大学、NICT、NII、産総研、三菱電機等で行われている。実験的研究もNICT、北海道大学と学習院大学でQKDに関して、大阪大学と横浜国立大学で量子中継に関してそれぞれ活発な研究を行っている。 停滞期に比べると上昇傾向にあるが、海外の加速度に比べると相対的に現状維持とせざるをえない。
	応用研究・開発	○	→	Q-LEAP フラッグシッププロジェクト、量子情報処理フラッグシップでは、基礎基盤研究とともに、量子コンピュータや量子シミュレーションの応用研究が進む。イジング専用マシンについては、NEDOプロジェクトにおいて量子デバイスを用いたハードウェア、統合ソフトウェア環境整備、従来型の半導体デバイスを用いた専用マシンの研究開発が進む。 NEC（Q-LEAP、NEDO）、富士通（NEDO）など企業からの国家プロジェクトへの参画が見られ、産学連携による遂行体制が確立しつつある。 NICTを中心に、SIPにおいてネットワークと量子セキュアアプリケーションの研究が進められている。衛星量子通信についても実証に向けた研究がソニー、スカパーJSATも参加して進められている。 停滞期に比べると上昇傾向にあるが、海外の加速度に比べると相対的に現状維持とせざるをえない。
米国	基礎研究	◎	↗	DOE傘下の国立研究所や大学において古くから量子技術・量子情報科学の基礎研究が続けられてきた。総額1000億円を優に超える米国の国家プロジェクトNational Quantum Initiativeにおいても、基礎研究重視や研究インフラの整備が唱えられており、2020年には新たな量子拠点づくりに巨額の投資がなされる。最近では量子中継ネットワークについての研究も進展。

	応用研究・開発	◎	→	上記の基礎研究に支えられ、米国では産業セクターが積極的に量子技術の応用研究を進めている。IT企業からは、Google、IBM、インテル（欧州と連携）、マイクロソフト（世界各国と連携）などが応用研究を進め、また、Rigetti computingやIonQなどに代表されるようなベンチャー企業も多数登場している。量子通信分野では、Quantum XchangeがId Quantiqueと協業し、QKD ネットワークサービスを開始した。各地でフィールドテストのための量子ネットワークテストベッドが作られ、衛星量子通信も量子もつれ共有をターゲットにプロジェクトが始まっている。
欧州	基礎研究	◎	↗	国立研究所や大学において古くから量子技術・量子情報科学の基礎研究が続けられてきた。予算規模1300億円（10年）を超えるEU Quantum Technology Flagshipプロジェクトがスタートし、第一次の採択が決定し本格始動した。英国ではQuantum Technology Hubsのもと約400億円規模（5年）の国家プロジェクトが2014年から進む。 オランダQuTechを中心とした量子ネットワーク研究Quantum Internet Allianceやジュネーブ大・東芝ケンブリッジ研究所ではQKD研究が行われている。
	応用研究・開発	◎	↗	オランダ、デルフト工科大学を中心とするQuTechでは、インテルやマイクロソフトと共同して、量子コンピュータの実現や応用に向けた研究が進む。 英国Quantum Communication Hubによる量子暗号ネットワークが建設されている。 EUにおけるOPENQKD、スペインでのCVQKDによるネットワーク、ドイツでのQuNet Initiativeなど各国で量子ネットワーク開発が進む。衛星量子通信の研究開発もドイツなどで行われている。ETSIによる標準化活動も進展している。
中国	基礎研究	○	↗	第13次五カ年計画のもと、中国科学院を中心として量子情報科学の拠点形成が進む。安徽省合肥市に量子技術や量子情報科学を対象とする量子情報科学国家実験室の第1研究棟が2020年に完成。また、中国科学技術大学で12量子ビット動作を成功させるなど具体的な成果が出始めた。中国科学技術大学のグループは量子暗号でも新しいプロトコルの実証実験を実施。Atomic ensemble量子メモリ研究も進む。
	応用研究・開発	○	↗	アリババ（阿里巴巴集団）、Huaweiに続き、Origin Quantum（本源量子）も、量子コンピュータのクラウドサービスを提供開始。 北京-上海間の2000 ㎞ネットワークは現在も稼働中。世界に先駆けて衛星量子通信を成功。量子専業企業の株式が上場され量子が投資の対象にもなっている。 ITU-Tでのネットワーク標準化、ISOでの実装安全性の標準化ではリード。
韓国	基礎研究	×	→	現状、量子暗号通信の研究が一部で見られるものの、活発ではない。量子情報処理技術に対する大型国家プロジェクトが発表された。
	応用研究・開発	△	→	SKテレコムがId Quantiqueへの出資、量子乱数源の開発、Korean TelecomがITU-Tを舞台にした標準化活動をそれぞれ行っている。

（註1）フェーズ

基礎研究：大学・国研などでの基礎研究の範囲

応用研究・開発：技術開発（プロトタイプの開発含む）の範囲

（註2）現状　※日本の現状を基準にした評価ではなく、CRDS の調査・見解による評価

◎：特に顕著な活動・成果が見えている　　○：顕著な活動・成果が見えている

△：顕著な活動・成果が見えていない　　×：特筆すべき活動・成果が見えていない

（註3）トレンド　※ここ1～2年の研究開発水準の変化

↗：上昇傾向、→：現状維持、↘：下降傾向

関連する他の研究開発領域

・量子コンピューティング（システム・情報分野　2.4.2）
・物質・材料シミュレーション（ナノテク・材料分野　2.6.4）

参考・引用文献

1) F. Arute et al., “Quantum supremacy using a programmable superconducting processor”, *Nature* 574, no. 23（2019）：505-510. doi：10.1038/s41586-019-1666-5
2) K. Takeda, A. Noiri, J. Yoneda, T. Nakajima and S. Tarucha, "Resonantly Driven Singlet-Triplet Spin Qubit in Silicon", *Phys. Rev. Lett.* 124, no. 11（2020）：117701. doi：10.1103/PhysRevLett.124.117701
3) M. Mizoguchi et al., “Ultrafast creation of overlapping Rydberg electrons in an atomic BEC and Mott-insulator lattice”, *Phys. Rev. Lett.* 124, no. 25（2020）：253201. doi：10.1103/PhysRevLett.124.253201
4) V. Scarani et al., "The Security of Practical Quantum Key Distribution", *Rev. Mod. Phys.* 81, no. 3（2009）：1301. doi：10.1103/RevModPhys.81.1301
5) H.-K. Lo, M. Curty and K. Tamaki, “Secure quantum key distribution”, *Nature Photon.* 8, no. 8（2014）：595–604. doi：10.1038/nphoton.2014.149
6) A. Tomita, "Implementation Security Certification of Decoy - BB84 Quantum Key Distribution Systems", *Adv. Quantum Technol*. 2, no. 5-6（2019）：1900005. doi：10.1002/qute.201900005
7) A. Huang, S. Barz, E. Andersson and V. Makarov, “Implementation vulnerabilities in general quantum cryptography”, *New J. Phys.* 20, no.（2018）：103016. doi：10.1088/1367-2630/aade06
8) M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD Network", *Opt. Express* 19, no. 11（2011）：10387-10409. doi：10.1364/OE.19.010387
9) T.A. Eriksson et al., “Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels”, *Commun. Phys.* 2（2019）：9. doi：10.1038/s42005-018-0105-5
10) S. Muralidharan et al., “Optimal architectures for long distance quantum communication”, *Sci. Rep*. 6：（2016）：20463. doi：10.1038/srep20463
11) Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, “Large scale quantum key distribution：challenges and solutions”, *Opt. Express* 26, no. 18（2018）：24260-24273. doi：10.1364/OE.26.024260
12) H.-S. Zhong et al., “Quantum computational advantage using photons”, *Science* 370, no. 6523（2020）：1460-1463. doi：10.1126/science.abe8770