2.6.3 量子通信

（1）研究開発領域の定義

量子通信ネットワークは、主に、量子の物理的な特徴を活用して送受信間で絶対安全に暗号鍵を共有する量子鍵配送ネットワークと、量子情報を遠隔地間で重ね合わせや量子もつれ等の量子状態を保ったままやり取りする量子インターネットに分類される。本研究開発領域は、1対1の量子鍵配送の高速化・長距離化技術から、既存セキュリティー技術との融合、多対多のネットワーク化と衛星系も含めた大規模グローバルネットワークの構築、量子中継技術およびそれを活用した量子インターネットの実現に関する研究開発を扱う領域である。

（2）キーワード

量子鍵配送、量子セキュアクラウド、トラステッドノード、量子暗号通信網、衛星量子通信、量子インターネット、量子テレポーテーション、量子中継、量子デバイス

（3）研究開発領域の概要

［本領域の意義］

現在の情報社会を支えている公開鍵暗号などの現代暗号は解読に膨大な計算量が要求される「計算量的安全性」によって安全性が担保されている。しかし、近年、量子コンピューターの研究が加速しており、将来的に実用的な量子コンピューターや全く新規の数理アルゴリズムの出現によって、現代暗号が容易に解読されてしまうことが懸念される。そこで、量子コンピューターが実現されても重要機関の間で機密情報を安全にやりとりするべく、解読が不可能であることが理論的に証明されている量子暗号が必須とされている。量子暗号は、量子鍵配送（QKD：Quantum Key Distribution）とワンタイムパッド（One Time Pad, OTP）暗号化という二つのステップから構成される。 OTPは、暗号化対象のデータと同じ長さの乱数を暗号鍵として用い、一度使用した乱数を二度と使わないようにする暗号方式である。量子暗号は、このOTPにおいてQKDから供給された暗号鍵を使うことで、情報理論的安全性を達成する。 QKDの送受信装置をネットワーク接続し、鍵を管理・配送する技術が量子鍵配送ネットワーク（QKDネットワーク）である。現在、世界各国でQKDネットワークのグローバルな普及に向けて実用化に向けた動きが活発化しており、地上系および衛星系の双方において、量子暗号を活用したグローバルな量子鍵配送ネットワークの構築が急務となっている。そのためには、QKDの高速化・長距離化やネットワーク化、先進的デバイス・システム技術の開発、古典セキュリティー技術（既存のセキュリティー技術）との融合など、さまざまな課題に取り組む必要がある。

さらに将来、大規模な分散量子コンピューティングや秘匿量子計算、光時計量子ネットワークによる時空間同期、量子センサーネットワーク等の量子アプリケーションが登場することによって、人々の安心・安全・便利な生活や高度な社会経済活動の実現が期待される。遠隔の量子コンピューター同士を相互接続する際、最大限の性能を引き出すには、ネットワークの送信エッジと受信エッジの間で、量子情報を、量子状態（重ね合わせや量子もつれ等）を保ったまま直接やりとりできる量子インターネット技術が必要となる。量子インターネットの実現には、量子情報を送受信する量子コンピューターや量子センサーだけでなく、量子メモリ等の量子中継に必要なデバイス技術の進展が必要不可欠であるが、当該技術はいまだ基礎研究段階であり、かつ技術の確立に長期間を要するとされており、関連技術の研究開発をこれまで以上に促進していく必要がある[1)]。

［研究開発の動向］

これまでの研究開発の大きな流れ・現在のトレンド

初期の量子暗号通信技術の研究においては、量子の物理的な性質を活用して送受信間で暗号鍵を安全に

共有可能とするQKDを、いかに安定的に高速化・長距離化するかが課題とされてきた。1984年に提案されたBB84[2]は、QKDの代表的なプロトコルであり、2018年には日本において、300 kbps × 45 kmという当時は世界最高性能の量子暗号装置が開発され、2021年に製品化・事業化がなされた。テストベッドに関しては、2010年に総務省所管の国立研究所である情報通信研究機構（NICT）等が都内100 km圏内で構築した試験用のTokyo QKD Network[3]が、世界最長の運用実績を有しており、量子暗号通信の実用化および高度化に多大に貢献している。

QKD技術の研究開発において、鍵配送の効率化や高速化・長距離化は、引き続き重要課題として取り組まれており、例えば、古典光通信と同じファイバーを共有して量子暗号通信を可能とする連続量（CV）–QKD[4]や、通信速度を落とすことなく通信距離を最大2倍まで延ばせるツインフィールド（TF）–QKD[5]など、BB84以外のQKD方式も研究開発が進んでいる。さらに現在、他課題として、既存セキュリティー技術との融合や、多対多のネットワーク化、量子中継を含む量子インターネットの実現など、研究開発テーマが広範囲に広がっている。

既存セキュリティー技術との融合では、いかに融合してネットワーク全体の安全性を高めるかが課題となっている。その応用技術の一つとして、量子セキュアクラウド技術があり、量子暗号、秘密分散、耐量子計算機暗号による認証基盤、秘匿計算等を融合することで、実用的な量子コンピューターが実現しても、解読や改ざん等ができないデータバックアップ保管と計算処理を行うことが可能となる。例えば、2020年には、NICT、NEC、ZenmuTechの三者が、電子カルテのサンプルデータの伝送そのものを量子暗号で秘匿化し、広域なネットワークを介して秘密分散技術によってバックアップ保管するシステムの実証実験に成功している。

ネットワーク化技術では、1対1のQKD技術を拡張し、多対多の大規模なQKDネットワークをいかに構築するかが課題となっている。そのため、BB84等による暗号鍵生成はリンクごとに行いつつも、ネットワークの中継点にトラステッドノード[6]を多数配備して、鍵リレーを行うことで、送信エッジと受信エッジの間で暗号鍵を共有する技術があり、早期の社会展開および普及が期待されている。トラステッドノードを前提としたQKDネットワークでは、応用技術としてネットワーク管理や経路制御等の研究開発が盛んに行われている[7)-10)]。また、地上系ネットワークに加えて、宇宙空間の損失が非常に小さい衛星－地上間通信も行うことによって、QKDの通信距離を大幅に伸ばすことも可能であり、QKDネットワークのグローバル化には、地上系および衛星系のネットワークの統合が必要である[11), 12)]。

量子インターネット技術[13]では、末端の量子コンピューターや量子センシングデバイス等から送信された量子情報を、いかにして、重ね合わせや量子もつれといった量子状態を純粋状態に近いまま遠隔地に届けるかが課題となっている。量子インターネットを実現するには量子中継技術[14]が必須であり、そのための1技術として量子メモリがある。量子メモリの実現方法としては、例えば、ダイヤモンド等の材料を活用してコヒーレンス時間（量子の重ね合わせ状態等が持続する時間）を増やすための研究開発が行われている[15]。当該技術は、技術的なハードルが高いことから、現状、基礎研究段階であり、技術の確立には長期間を要するとされている。量子インターネットは、量子中継技術を中継ノードに導入し、末端の量子コンピューターや量子センシングデバイス等を光ファイバー回線で接続して大規模メッシュネットワーク化することで、多対多で量子情報をやりとり可能なネットワークであり、現在、量子メモリを含むデバイス技術に加えてネットワーク制御技術も含め、さまざまな研究開発が行われている[16)-18)]。また、量子メモリをQKDに応用し、送信エッジと受信エッジの間で、上記のトラステッドノードを介さずに暗号鍵を共有する研究も行われている[19]。

国内では、政府の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」を発表し[1]、量子技術を重要戦略技術と位置づけて、量子イノベーション拠点の形成や当該技術の研究開発への積極的な投資、人材育成等が加速している。

国際標準化

QKDネットワーク技術のグローバルな普及には、国際標準化も重要である。例えば国内機関では、NICT

が、政府や企業・大学と連携し、ITU-TやISO/ IEC SC1、ETSI等において国際標準化を積極的に進めている。例えば、ITU-Tでは、2019年10月に、QKDネットワークに関連する世界初の国際標準勧告 ITU-T Y.3800「Overview on networks supporting quantum key distribution」が発刊された[20]。2022年2月には、ITU-T Y.3809「A role-based model in quantum key distribution networks deployment」が勧告承認されている[21]。

諸外国の政策

量子技術は、米国、欧州、中国を中心に国家戦略上の重要技術と位置づけられ、量子技術に関する研究開発戦略の策定、研究開発投資の拡充、拠点の形成、人材育成等が急速に展開されている。米国では、2018年12月に、2019年からの5年間で量子関連技術に対して最大13億ドル規模の投資に関する法律が成立したことに加え、2021年8月には、エネルギー省（DOE）が、国家量子イニシアチブ法に基づいて、さまざまな国立研究所を主導組織として量子技術関連の五つのセンターを設立し、量子インターネットや量子デバイスに関する研究開発プロジェクトに対して6,100万ドルを提供することが発表された。欧州では、オランダ、英国、ドイツ、スイス、他、さまざまな国で量子技術に関する研究開発プロジェクトが立ち上がっており、欧州委員会によって2018年10月に10年間で10億ユーロを投資する「量子技術フラグシップ」プロジェクトが開始されたことに加え、例えばオランダでは、2020年2月に、今後5年間で量子技術に対して2,350万ユーロを投じることが発表されるなど、積極的な投資がなされている。中国は、2016年から量子技術で世界をリードするための13年計画が開始され、量子関連で数十億ドルを投資しており、量子暗号通信ネットワーク分野では、世界をリードしている状況である。

QKD 装置は、日欧米中などの企業において既に製品化や一部事業化がされており、世界各国の通信事業者やスタートアップ企業などが事業化に向けた活動を積極的に行っている。量子暗号の世界市場は、2030年には約34億ドルに達すると見込まれており、2035年には日本円で約2兆円まで成長する見込みである。

（4）注目動向：

［新展開・技術トピックス］

1対1のQKDの高速化・長距離化技術

ここ数年、前述のTF-QKD方式が注目されている[5]。TF-QKD方式では、送信エッジおよび受信エッジが中間点へ向けて光パルスを送り、中間点にて単一光子を検出する構成を用いることによって、従来のBB84を用いたQKD方式と比較して、伝送距離を2倍以上に伸ばすことが可能である。2018年には、東芝欧州研究所ケンブリッジ研究所が標準的な光ファイバーを用いて通信距離を500km以上とするTF-QKD方式を開発している。ただし、安定化など、解決すべき技術的な課題はまだ多く、引き続き、研究開発を促進する必要がある。

既存セキュリティー技術との融合

特に日本国内では、ここ数年で、例えば秘密分散や秘匿計算との融合など、研究開発や実証実験が積極的に実施されてきた[22]。さらに、QKDでは一般に、古典ネットワークにおいてセキュリティー上の問題が発生し得ると考えられることから、耐量子計算機暗号（PQC）システムをQKDネットワークと接続することによってネットワーク全体でセキュリティーを向上する取り組みが必要である。例えば、北米のQuantum Xchange社が、2021年11月に、QKDとPQC双方に対応した暗号鍵配送システム「Phio Trusted Xchange」[23] を提供することを発表しており、統合技術のさらなる高度化が求められる。

QKDの多対多ネットワーク化技術

QKDでは、手動による鍵リレー経路設定方式が主に想定されてきたが、論文等の机上検討において、自

動的に経路計算する技術の発表が増えてきた。ただし、自動方式でも、現状、必ずしも最適な鍵リレー経路計算が行われていないケースが多いことから、引き続き、送受信エッジ間のホップ数や各リンクの暗号鍵残量等を考慮した最適な鍵リレー経路計算技術を確立するための研究が必要である。また、送受信エッジ間であらかじめ鍵リレー経路を決めておくエンド・ツー・エンド方式とは別に、中継ノードごとに経路（次ホップ）を決定するホップ・バイ・ホップ方式のQKDも提案されている。 NICTでは、古典ネットワーク上の情報指向ネットワーク（Information Centric Network, ICN）技術（2.6.6参照）を適用してQKDネットワーク全体の鍵消費量を低減する技術の研究開発が進められている[24)]。

衛星量子通信技術

衛星通信に適した新たなQKDプロトコルの開発や、通信リンクの安定化のための補足追尾・補償光学・単一光子検出等の技術の開発が盛んに行われている一方で、QKDを補完する技術として、近年、物理レイヤ暗号技術[12)] が注目されている。物理レイヤ暗号技術は、特に衛星通信向けに最適化されており、盗聴者の攻撃モデルに制限を課すことが可能な状況下で、情報理論的安全に送受信エッジ間で暗号鍵を共有可能とする技術である。

量子インターネットのネットワーク制御技術

量子インターネットのネットワーク制御技術（ルーティング等）は、デバイス技術の制約や困難性もあり、これまでは研究が少なかったが、量子メモリや量子インターフェースなど、デバイス基礎技術の進展により、徐々に研究発表が増えている。例えば、通信ネットワーク分野のトップカンファレンスであるIEEE INFOCOMでは、2022年において、量子インターネットの制御技術関連の研究成果が複数件発表された[16)-18)]。米国では大統領府の米国量子調整局が国家戦略の報告書[25)] を公開しており、欧州ではオランダのデルフト工科大学が量子インターネットを含む将来の量子ネットワークに関する報告書[26)] を公開するなど、量子インターネットの制御およびデバイス技術は、今後、研究開発が加速する見込みである。

［注目すべき国内外のプロジェクト］

日本

- 2018年度に総務省委託研究「衛星通信における量子暗号技術の研究開発（令和4年度まで）」が開始。衛星・地上間における量子暗号用送受信装置の研究開発を推進。
- 2020年度に総務省委託研究「グローバル量子暗号通信網構築のための研究開発（令和6年度まで）」、2021度に総務省委託研究「グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発（令和7年度まで）」が開始。地上から低/中/静止軌道まで含めたグローバル規模の量子暗号通信網構築に向けた研究開発を推進。
- 2020年に、内閣府が推進するムーンショット型研究開発の目標6に、「量子計算網構築のための量子インターフェース開発」プロジェクトが採択。2030年までに量子コンピューターの誤り訂正可能な規模でのネットワーク接続の実現、2050年までに大規模な超伝導量子コンピューターの実現を目指した研究開発を推進。

米国

- エネルギー省（DOE）が、量子情報科学関連技術で、傘下の国立研究所（ローレンス・バークレー国立研究所、オークリッジ国立研究所、アルゴンヌ国立研究所、ブルックヘブン国立研究所、フェルミ国立加速器研究所）が主導する五つの研究センターに大規模な資金投入。例えば、ローレンス・バークレー国立研究所のQUANT-NET（Quantum Application Network Testbed）プロジェクトでは、分散型量子ネットワーク構築・実証に関わる研究開発を推進。オークリッジ国立研究所とロスアラモス国立

研究所のQuAInT（Quantum–Accelerated Internet Testbed）プロジェクトでは、都市規模での量子情報送受信が可能な量子インターネット・テストベッドの設計および構築を目指した研究開発を推進。アルゴンヌ国立研究所主導の次世代量子科学光学センター（Q–NEXT）では、量子中継器を含む長距離通信リンクやシミュレーションテストベッド等を実証するためのエコシステムの構築を目指した研究開発を推進。

・NASAが資金援助を行っているSEAQUE（Space Entanglement and Annealing Quantum Experiment）プロジェクト。イリノイ大学アーバナ・シャンペーン校やウォータールー大学などが参画しており、軌道上での量子通信技術の検証を推進。

欧州

・OpenQKDプロジェクト。 QKDテストベッド構築や相互接続、産業化などを推進。13カ国から38機関が参画する大規模プロジェクト。
・QRANGEプロジェクト。量子乱数生成技術の開発を推進。
・UNIQORNプロジェクト。ベルギーのゲント大学などが参画しており、量子通信や量子コンピューター向けのデバイス技術開発等を推進。
・CiViQプロジェクト。SDN（Software–Defined Networking）–QKD、CV–QKD等の開発を推進。
・QIAプロジェクト。量子インターネット技術の開発を推進。
・スペイン科学イノベーション省が、Q–CAYLEやMadQ、BasQhuBなどを含む量子通信分野に関わる6プロジェクトを採択。（2021年11月）
・ドイツ連邦教育・研究省が資金提供し、量子メモリ等の量子デバイスによる安全な認証を可能にするための7プロジェクトを開始。（2022年3月）
・英国UKリサーチ&イノベーションが、量子技術の商業化のための16プロジェクトを採択し、計600万ポンドの資金を提供すると発表。（2022年6月）

中国

・2016年頃から、2030年に向けて、量子通信を含む複数の研究開発やその応用展開のためのプロジェクトを推進しており、2020年3月には、量子通信を含む重要科学技術プロジェクトの実施とサポート力を強化し、科学技術成果の応用と産業化を促進し、イノベーション型企業とハイテク企業を育成し、経済発展の新動力を増強するための施策を発表している。

（5）科学技術的課題

QKDネットワークのグローバル化

QKDネットワークの大規模化・グローバル化を目指し、現在敷設環境で動作中の量子暗号装置と比較して数倍以上、鍵配送を高速化・長距離化可能な技術が求められる。そのため、前述の通り、TF–QKDなどの新技術が注目されているが、安定動作状態で高速化・長距離化を図る技術の確立など、QKD方式の高度化は、今後も取り組むべき課題である。また、衛星系ネットワークにおいても、鍵配送の高速化・長距離化が課題であり、かつ、地上系ネットワークとの統合によって、QKDネットワークのグローバル化を目指す取り組みも必要である。

既存セキュリティー技術との融合

ネットワーク全体の安全性をQKD技術のみで実現することは現状困難であり、既存のセキュリティー技術等との融合が必須となっている。例えば、配信された暗号鍵データを安全に保持管理することを保証するストレージシステムや、耐量子計算機暗号技術との統合などの研究開発が必要である。

量子デバイス技術

量子ネットワークの大規模化・グローバル化には、それを支える量子デバイスの進展が不可欠である。量子デバイス技術の開発は課題が多く、技術の確立に長期スパンを要するとされているが、例えば、量子状態を保ったまま量子を保存・処理する量子メモリ技術や、原子と光子間などの異種量子間の変換を実現する量子インターフェース技術、光子の波長を光通信波長帯に変換する量子波長変換技術など、将来のグローバル規模のQKDネットワークや量子インターネットを構築していくためには、量子デバイス技術を早期に確立する必要がある。

量子インターネットの制御管理

量子中継技術や量子コンピューター技術の進展を踏まえた上で、さまざまな性能面（遅延や通信容量、通信要求棄却率等）で量子テレポーテーションの最適な経路動的選択/切り替え（ルーティング）やリソースの動的割り当てなどを高速かつ効率的に行うための制御管理機構を開発および構築することが、将来の量子アプリケーションの安定性向上の点で重要である。

（6）その他の課題

産学官が連携し、量子暗号装置等の安全性評価手法の確立、国際規格準拠のセキュリティー要件の文書化や運用など、各種制度を整備していくことが重要である。また、デバイスからネットワーク、さらにはアプリケーションまで多岐にわたって、大学の基礎技術を実用化・事業化に結び付けるための連携体制の構築と強化が必要である。

人材育成の観点では、これまで、量子通信技術は、1対1の量子通信や、それを活用した暗号鍵共有プロトコルの研究がメインであり、物理学や数学等の関連分野とされてきたため、現在、国内では、通信・ネットワーク技術と量子通信技術の双方に精通している人材は、産学官において極めて少数である。例えば、NICTが2020年から開始している量子人材育成プロジェクト（NQC）など、量子通信技術に関わる人材育成を今後も促進していく必要がある。

（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	○	→	2020年、内閣府ムーンショットプログラムにて、2030年および2050年をターゲットに、量子デバイス基礎技術を含む量子インターネット実現に向けたプロジェクトが開始（※1）。 （※1） https://www8.cao.go.jp/cstp/moonshot/gaiyo/ms6_kosaka.pdfseconds
	応用研究・開発	○	↗	内閣府の戦略的イノベーション創造プログラム（SIP）第2期（※2）において、2019年および2020年に量子暗号による分散保管実験に成功。2020年および2021年に総務省委託研究が開始され、グローバル規模の量子暗号通信ネットワーク構築に向けた研究開発を促進。東芝が2021年に量子暗号装置を製品化し、同年10月にロンドンで世界初の量子暗号通信の商用メトロネットワークを構築。 （※2）https://www.qst.go.jp/site/sip/35666.html

米国	基礎研究	◎	↗	科学技術政策局（OSTP）や全米科学財団（NSF）、エネルギー省（DOE）が、量子インターネット実現のための要素技術に関する研究開発やテストベッド環境提供、人材育成等にへの大規模投資を実施。DOEは、2020年2月に開催された量子インターネットのワークショップ「Quantum Internet Blueprint Workshop」のレポートを同年7月に公開し（※1）、傘下の国立研究所が主導する5研究センターに資金投入。既に、量子インターネットに関わるさまざまな開発・実証に成功。さらに、国際会議INFOCOMでの研究発表（文献18））など、学術的な成果も出ている。 （※1）https://www.osti.gov/servlets/purl/1638794
	応用研究・開発	○	↗	Quantum Xchange社が、2021年11月に、QKDと耐量子計算機暗号双方に対応した暗号鍵配送システム「Phio Trusted Xchange」の提供を発表。Qryptが、2022年2月に、量子暗号ソリューションをクラウドサービスとして提供する「Key Generation」を発表。JPモルガンチェイスが、2022年2月、大都市圏向けQKDネットの実証実験。
欧州	基礎研究	○	↗	2020年3月には、「量子技術の研究戦略アジェンダ」が公表され、研究開発、産業化、標準化、人材育成等が促進され、ロードマップが公表。欧州25カ国が、量子インターネットの構築のためのテストベッド「EuroQCI」の構築に合意。 【オランダ】QuTechが、2022年に、高性能な量子メモリを用いた量子テレポーテーションの実験や、固体中の光アクティブ・スピンを使ったマルチノード量子ネットワーク実験環境構築に成功。 【英国】2021年9月、ブリストル大学が、量子コンピューターの開発に資する量子ビットをエラーから保護するためのフォトニックチップを利用した量子誤差補正コードを実証。2022年2月、ケンブリッジ大学が、室温での量子情報保存を可能とする単一光子源となる2次元材料を特定。 【ドイツ】2022年5月、マックス・プランク研究機構が、量子ネットワークの量子ゲートの性能を大幅に向上。 【フィンランド】2022年3月、オウル大学が、超電導量子ビットで保護された量子状態の制御に成功。
	応用研究・開発	○	↗	「OpenQKD」プロジェクト等により、量子暗号技術とその応用の開発・実証を促進。 【オランダ】2022年7月、QuTechが、オランダでデータセンター間を相互接続するQKDテストベッドを開始。 【英国】2022年4月、英国のBritish Telecom社が、東芝と合同で、世界初の商用向けQKDメトロネットワークのトライアルサービスを開始。 【ドイツ】2022年4月、ADVAが、IDQuantique社のQKD装置およびADVAの物理層暗号化技術を用い、架空ファイバー・リンクでの量子安全データ伝送実験に成功。2022年7月、フラウンホーファーが、UNIQORNプロジェクトで、2×4mmチップに搭載可能な小型QKD送信機を開発。 【スイス】IDQuantiqueが、2021年10月、量子ラボ構築のためのプラットホーム製品「Cerberis XGR」を発表。2022年5月、高性能なQKD製品「Clavis XG」を発表。
中国	基礎研究	○	→	ジャーナル誌や国際会議INFOCOMにおいて、中国科学技術大学から、量子インターネット関連の研究発表（文献15), 17））がなされるなど、学術的な成果が出ている。
	応用研究・開発	◎	↗	2016年頃から量子暗号通信分野への大規模投資がなされており、例えば、2021年1月に、人工衛星と地上の通信ネットワークを接続して、約4600kmのQKDネットワークを構築。2021年1月、衛星系および地上系を統合した大規模量子ネットワークの実証実験の実施を発表。Quantum CTek社がQKD装置を製品化し、CAS Quantum Network社がQKDネットワークサービスの事業化を促進。超電導ナノワイヤ単一光子検出器を搭載したシリコンフォトニクスチップを使った量子通信システムを開発。

韓国	基礎研究	−	−	（顕著な動きは見られない）
	応用研究・開発	○	→	SKブロードバンドが、2020年9月にQKDに関する標準ロードマップを策定し、さらに、2022年7月に全長800kmとなる韓国全土QKDネットワーク構築のフェーズ1を完了。
豪州	基礎研究	−	−	（顕著な動きは見られない）
	応用研究・開発	△	−	2021年11月、米国と、量子技術の成果を実用的応用につなげるための協力に合意。「Quantum Commercialisation Hub」に7000万オーストラリアドルを確保。
カナダ	基礎研究	○	→	国際会議INFOCOMにおいて、ブリティッシュ・コロンビア大から、量子インターネットのルーティングに関する研究発表（文献19））がなされるなど、学術的な成果が出ている。
	応用研究・開発	△	→	2022年2月、カナダ政府が、国家量子戦略の策定に向けた公開協議の結果をまとめた報告書を発表。2022年6月、ケベック州の非営利団体Numanaが、産業界および研究者向けのオープンな量子通信インフラの立ち上げを発表。

（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

◎：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

×：活動・成果がほとんど見えていない

―：評価できない（公表する際には、表示しない）

（註3）近年（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・通信（HW）（ナノテク・材料分野 2.3.5）

参考文献

1）統合イノベーション戦略推進会議「量子技術イノベーション戦略（最終報告）（令和2年1月21日）」内閣府, https://www8.cao.go.jp/cstp/tougosenryaku/ryoushisenryaku.pdf,（2023年2月26日アクセス）.

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

3）Masahide Sasaki, et al., “Field test of quantum key distribution in the Tokyo QKD Network,” Optics Express 19, no. 11（2011）: 10387-10409., https://doi.org/10.1364/OE.19.010387.

4）Xiaoyu Ai and Robert Malaney, “Qptimized Multithreaded CV-QKD Reconciliation for Global Quantum Networks,” *IEEE Transactions on Communications*, vol. 70, issue 9（2022）: 6122-6132., https://doi.org/10.1109/TCOMM.2022.3188018.

5）Marco Lucamarini, et al., “Overcoming the rate-distance limit of quantum key distribution without quantum repeaters,” *Nature* 557, no. 7705（2018）: 400-403., https://doi.org/10.1038/s41586-018-0066-6.

6）Philip G. Evans, et al., “Trusted Node QKD at an Electrical Utility,” *IEEE Access* 9（2021）: 105220-105229., https://doi.org/10.1109/ACCESS.2021.3070222.

7）Yoshimichi Tanizawa, Ririka Takahashi and Alexander R. Dixon, “A routing method designed for a Quantum Key Distributed network,” in *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*（IEEE, 2016）, 208-214., https://doi.org/10.1109/ICUFN.2016.7537018.
8）Omar Amer, Walter O. Krawec and Bing Wang, “Efficient Routing for Quantum Key Distribution Networks,” in *2020 IEEE International Conference on Quantum Computing and Engineering (QCE)*（IEEE, 2020）, 137-147., https://doi.org/10.1109/QCE49297.2020.00027.
9）Miralem Mehic, et al., “A Novel Approach to Quality-of-Service Provisioning in Trusted Relay Quantum Key Distribution Networks,” *IEEE/ACM Transactions on Networking* 28, no. 1（2020）: 168-181., https://doi.org/10.1109/TNET.2019.2956079.
10）Li-Quan Chen, et al., “ADA-QKDN: a new quantum key distribution network routing scheme based on application demand adaptation,” *Quantum Information Processing* 20（2021）: 309., https://doi.org/10.1007/s11128-021-03246-2.
11）Yu-Ao Chen, et al., “An integrated space-to-ground quantum communication network over 4,600 kilometres,” *Nature* 589, no. 7841（2021）: 214-219., https://doi.org/10.1038/s41586-020-03093-8.
12）Hiroyuki Endo, et al., “Group key agreement over free-space optical links,” *OSA Continuum* 3, no. 9（2020）: 2525-2543., https://doi.org/10.1364/OSAC.389853.
13）David Awschalom, “From Long-distance Entanglement to Building a Nationwide Quantum Internet: Report of the DOE Quantum Internet Blueprint Workshop,” U.S. Department of Energy, Office of Scientific and Technical Information, https://doi.org/10.2172/1638794,（2023年2月26日アクセス）.
14）Qiao Ruihong and Meng Ying, “Research Progress of Quantum Repeaters,” *Journal of Physics: Conference Series* 1237, no. 5（2019）: 052032., https://doi.org/10.1088/1742-6596/1237/5/052032.
15）Shuhei Tamura, et al., “Two-Step Frequency Conversion for Connecting Distant Quantum Memories,” in *Proceedings of Conference on Lasers and Electro-Optics Pacific Rim (CLEO-PR) 2018*（Optica Publishing Group, 2018）, W2G.3., https://doi.org/10.1364/CLEOPR.2018.W2G.3.
16）Yangming Zhao, Gongming Zhao and Chunming Qiao, “E2E Fidelity Aware Routing and Purification for Throughput Maximization in Quantum Networks,” in *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*（IEEE, 2022）, 480-489., https://doi.org/10.1109/INFOCOM48880.2022.9796814.
17）Yiming Zeng, et al., “Multi-Entanglement Routing Design over Quantum Networks,” in *Proceedings of IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*（IEEE, 2022）, 510-519., https://doi.org/10.1109/INFOCOM48880.2022.9796810.
18）Ali Farahbakhsh and Chen Feng, “Opportunistic Routing in Quantum Networks,” in *Proceedings of IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*（IEEE, 2022）, 490-499., https://doi.org/10.1109/INFOCOM48880.2022.9796816.
19）Yumang Jing and Mohsen Razavi, “Simple Efficient Decoders for Quantum Key Distribution Over Quantum Repeaters with Encoding,” *Physical Review Applied* 15, no. 4（2021）: 044027., https://doi.org/10.1103/PhysRevApplied.15.044027.
20）International Telecommunication Union Telecommunication Standardization Sector

（ITU-T）, “Y.3800: Overview on networks supporting quantum key distribution, 10/19,” https://www.itu.int/rec/T-REC-Y.3800-201910-I/en,（2023年2月26日アクセス）.
21）International Telecommunication Union Telecommunication Standardization Sector（ITU-T）, “Y.3809: A role-based model in quantum key distribution networks deployment, 02/22,” https://www.itu.int/rec/T-REC-Y.3809-202202-I/en,（2023年2月26日アクセス）.
22）Mikio Fujiwara, et al., “Long-Term Secure Distributed Storage Using Quantum Key Distribution Network With Third-Party Verification,” *IEEE Transaction on Quantum Engineering* 3（2022）: 4100111., https://doi.org/10.1109/TQE.2021.3135077.
23）Quantum Xchange, “A Cryptographic Management Platform for the Ages: Phio Trusted Xchange（TX）,” https://quantumxc.com/phio-tx/,（2023年2月26日アクセス）.
24）Kazuhisa Matsuzono, Takaya Miyazawa and Hitoshi Asaeda, “QKDN meets ICN: Efficient Secure In-Network Data Acquisition,” in *Proceedigs of IEEE Global Communications Conference (GLOBECOM)*（IEEE, 2021）, 1-7., https://doi.org/10.1109/GLOBECOM46510.2021.9686026.
25）The White House and National Quantum Coordination Office, “Quantum Frontiers: Report on Community Input to the Nation’s Strategy for Quantum Information Science, October 2020,” National Quantum Initiative, https://www.quantum.gov/wp-content/uploads/2020/10/QuantumFrontiers.pdf,（2023年2月26日アクセス）.
26）QuTech, “Creating the Quantum Future: QuTech Annual Report 2019,” https://qutech.h5mag.com/annual_report_2019/cover,（2023年2月26日アクセス）.