2　量子情報通信技術研究開発の概要

武岡正裕　仙場浩一　佐々木雅英

現在の情報通信技術は 19 世紀に確立された物理法則に基づいて設計されているが、通信容量の限界や暗号解読の危機など、将来的にその性能限界を迎えることが危惧されている。このような限界を打破する手段として、究極の物理法則である量子力学に基づく新しい情報通信技術「量子情報通信技術」や、そこから派生する応用技術が注目されている。本稿では、NICT における量子情報通信技術の研究開発についての取組の概要を紹介する。

1　まえがき

現代の情報通信技術の発展は目覚ましいものがあり、今も日々進歩し続けている。一方で、現在の技術体系の延長上では、将来性能限界を迎える可能性も指摘されている。地上のファイバー網から人工衛星を介した通信まで、急速に広がる現代の通信ネットワークにおいてセキュリティの確保は極めて重要な課題であるが、現在の一般的な暗号方式は、将来のコンピュータ技術等の発展により解読されてしまう危険性が指摘されている。また、とどまることなく増大する通信量に対し、光ファイバーに入力できるレーザーの電力には物理的限界があり、惑星探査機などの超長距離通信の場面においては、信号が弱すぎて受信した信号の正確な識別が不可能になる識別限界がある。

これに対して、量子力学という原子や電子、光子などミクロな世界を扱う最新の物理学を駆使した新しい情報技術、いわゆる量子情報技術が実現できれば、従来技術では不可能な安全性を実現する量子暗号や、現在のコンピュータでは何万年もかかる計算を短時間で実行する量子コンピュータ、物理学が許す究極の通信容量限界を実現する量子受信技術など、抜本的な技術革新が可能になることが、近年、次々に予言されてきた。21 世紀に入り、その実現に向けた本格的な研究開発が世界各地で進められている。NICT では、こうした量子情報技術の中でも、特に通信に関わる技術、すなわち量子情報通信技術の実現に向けた研究開発を進めている。本稿では、NICT における研究開発の概要を紹介する。

2　量子光ネットワーク技術

現在、社会の様々な場面で暗号が用いられている。しかし、現在の一般的な暗号方式は、将来の計算技術の革新によって解読されてしまう危険性が常に指摘されている。これは、ソフトウェアで構成される現代暗号の安全性が、暗号解読に膨大な計算量を必要とするという、いわゆる計算量的安全性に依存しているためである。例えば、代表的な現代暗号の 1 つである RSA 暗号は、現在の計算機では巨大な数の素因数分解を行うのに膨大な時間がかかることを安全性の根拠としている。しかし、これは日々急速に進歩する計算機能力の向上や新しい素因数分解アルゴリズムの発明などにより、近い将来、現実的な計算時間で解読されてしまうことが危惧される。また、量子力学の性質を利用した量子コンピュータが実現すれば、RSA 暗号は極めて高速に解読できることもわかっている。これらは、国家情報や金融情報、医療情報など、長期にわたり極めて高い安全性が要求される機密情報を通信する際には、重大な問題となる。この問題を解決する手段として期待されている量子情報通信技術が、量子暗号である。

量子暗号は、どれほど強力な計算能力を使っても解読不可能な安全性を保証する情報理論的安全性と、どのような物理的な盗聴攻撃（例えば光ファイバーから一部の信号を抜き取ってしまうなど）でも検知できる物理的な盗聴に対する安全性という、現在の暗号方式にはない 2 つの大きな特長がある。量子暗号は、量子鍵配送（Quantum Key Distribution: QKD）と呼ばれる、送受信者だけが知る秘密鍵（秘密のランダムビット列）の共有と、それを用いた暗号化通信からなる。後者は、QKD で共有された秘密鍵を使って送りたい情報を暗号化し、通常のインターネット回線等を使って通信を行う。

QKD には、量子の性質を用いた通信装置が必要となる。送信者は光の粒子である光子に特殊な変調により乱数を載せて伝送する。受信者は届いた光子 1 個 1 個の状態を検出して、さらに、盗聴の可能性のある

ビットをコンピュータ上のアルゴリズムにより排除（鍵蒸留と呼ばれる）し、安全な秘密鍵を生成する。光子レベルの信号は、盗聴者が何かの盗聴行為を行うと、ハイゼンベルグの不確定性原理により必ずその痕跡が残るため、これを利用して盗聴攻撃を見破る。また、伝送する乱数には物理乱数と呼ばれる確率的な物理現象から生成された乱数を用いることにより、盗聴者の計算能力とは全く無関係な秘密鍵の共有が可能となり、情報理論的安全性が達成される。以上が、量子暗号の原理の概要である。なお、量子暗号が発明された1980年代から1990年代にかけては、光の粒子を正確に1つだけ準備した単一光子状態の信号が必要と考えられてきたが、その後の理論研究の進展により、単一光子レベルの極めて微弱なレーザー光（コヒーレント状態の光）を使っても、送受信方法の工夫により単一光子とほぼ同じ性能が得られることが明らかとなり、今世紀に入り実用化に向けた研究開発が一気に加速している。

NICTでは、2001年から産学と連携し量子暗号の基礎研究を開始し、2006年以降、地上ファイバー網での量子暗号ネットワークの実証や、その実用化に向けた研究開発に取り組んできた。また最近では、量子暗号システムそのものの実用化に加え、量子暗号システムを構成する要素技術（微弱光通信や鍵蒸留、物理乱数生成など）を切り出して使うことで、ドローンとの通信やモノのインターネット（IoT）など、量子暗号そのものの実装はまだ困難な通信ネットワークにおいても、新しいセキュリティ技術を提供できる可能性も明らかとなってきた。我々はこれらの技術を総称して「量子光ネットワーク技術」と呼び、研究開発を進めている（図1）。

3　量子ノード技術

冒頭で述べたように、光通信は現在最も大容量の情報伝送が可能な手段だが、急速に増大し続ける通信量に対して、いずれ原理的な限界を迎えることが危惧されている。また、宇宙空間のような超長距離で途中の増幅が不可能な通信路では、量子雑音に埋もれた超微弱な信号から最大の情報を取り出すことが必要となり、現在の技術では困難である。一方セキュリティの面においても、前節で紹介した量子暗号技術は究極的な安全性を実現できる反面、光子レベルの信号を送受信しなければならないため、現在実用化が進んでいる量子暗号方式では距離や鍵生成速度に制限があり、その応用範囲が限定されている。

これらの問題を抜本的に解決するためには、ネットワークの中継点（ノード）で光信号の量子的な性質を自在に計測・制御・保存できる技術が必要となる。しかし現実には、量子力学的性質は非常に壊れやすいため、実現にはまだいくつかの技術革新が必要な状況である。我々はこれらの技術を「量子ノード技術」と総称し、長期的な視点に立った基礎研究に取り組んでいる（図2）。具体的には、光の量子状態を自在に制御し、従来の電磁気学に基づく光学（量子と対比して古典光学と呼ばれる）の世界では実現不可能な情報通信プロトコルを実証する「光量子制御技術」、原子やイオンを1つずつ制御して量子通信や次世代の周波数標準技術に応用する「量子計測標準技術」、マクロサイズの人工原子である超伝導回路を使い、光と物質の相互作用を光子1個レベルで精密制御し、量子物理の新現象を解き明かす「超伝導量子回路技術」の3つのテーマを中心に研究を進めている。いずれも量子物理学その

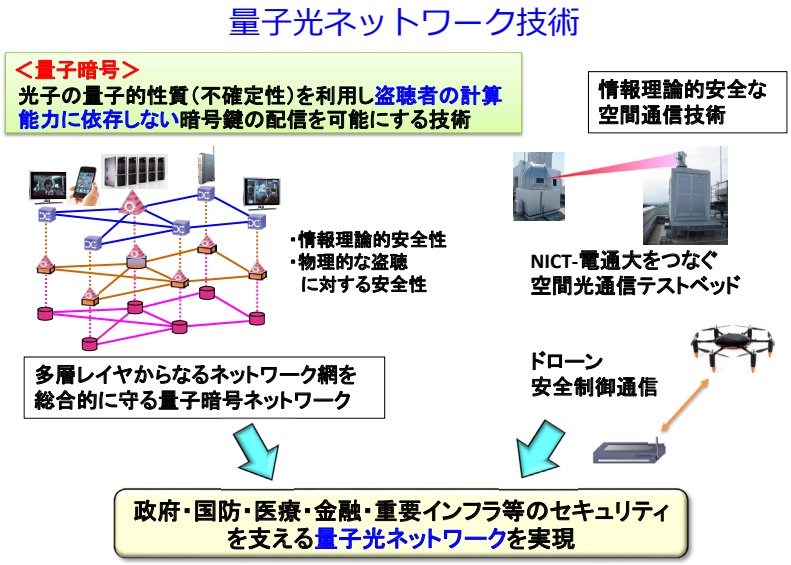

図1　量子光ネットワーク技術の概要

ものを開拓する未来技術であり、まだ人類が手にしていない技術の実現に挑む挑戦的な課題である。

これらの量子技術の開発において重要となる概念が量子もつれ（エンタングルメント）である。量子もつれは、力学や電磁気学のみからなる古典物理だけでは説明不可能な、量子力学の世界だけに現れる相関のことである。例えば、2つの光子を同じ縦偏光に準備したとすると、光子の偏光には（古典的な）相関が形成される。このとき、それぞれの光子に対して縦横偏光を識別するフィルターで測定を行えば相関が検出されるが、違う偏光基底、例えば右回り・左回りの円偏光を測定しても、それぞれの光子の回転方向はランダムとなり、相関は見えない。一方、量子もつれが形成された光子対では、それぞれの光子の縦横偏光を測定しても相関が見えるし、同じ光子対に対して円偏光の測定を行ったとしても、やはり強い相関を検出することができる。しかも、測定の方法は、状態が準備された後に選択したとしても結果は変わらない。

このように、異なる測定方法でも相関が形成されていることが量子もつれの最大の特徴であり、この特徴を活かせば、例えば、量子もつれ光子対を離れた2者間に配信した際、途中で第三者に盗聴攻撃を受けたどうか、複数の測定方法で監視することにより必ず検出することができる。量子もつれは壊れやすいため、そのまま送るだけでは長距離伝送に適さないが、ネットワークの中継点で部分的に壊れた量子もつれを適切に修復しながら伝送していく量子中継技術が実現すれば、現在フィールド実証されている量子暗号方式と同じ安全性を、超長距離で実現することも可能になる。また、量子もつれは複数の計算を並列的に実行する量子コンピュータにおいても不可欠なリソースであることが知られている。

NICTにおける各研究課題では、光子の間の量子もつれ（光量子制御）、原子間の量子もつれ（量子計測標準）、光と超伝導人工原子の間の量子もつれ（超伝導量子回路）などを自在に制御する技術の確立を目指している（量子もつれの確立だけが研究の目的ではないが、その詳細については、本特集号の各記事を参照していただきたい）。特に最後の超伝導量子回路の系では、量子もつれを形成する光–人工原子間の結合を他の系では実現できないほど強くすることが可能であり、物質と光の深強結合と呼ばれる、これまで誰も観測できなかった新しい物理現象の開拓にもつながっている。

4　量子情報通信技術の社会展開に向けて

量子技術は、究極の安全性や超高速演算など社会を変える大きなポテンシャルを持っているが、多くの場合、量子技術単体ではなく、様々な既存のICT技術と適切に組み合わせることで初めて社会に役立つものになると予想される。そこで、NICTの第4期中長期計画では、量子情報通信技術（量子ICT技術）と現代ICT技術の融合をテーマに掲げ、社会の様々なICTに量子技術（及びその派生技術）を有効に展開していくことを目指している（図3）。

また、量子暗号は現代暗号に無い安全性を提供できると述べたが、それは将来的に現代セキュリティ技術が全て量子暗号に取って代わるという意味ではなく、現代セキュリティ技術の中で量子暗号が必要とされている部分に適切に組み込まれていくことで、その能力を最大限発揮できると考えている。具体的には、例えば現代セキュリティ技術でよく知られた秘密分散技術

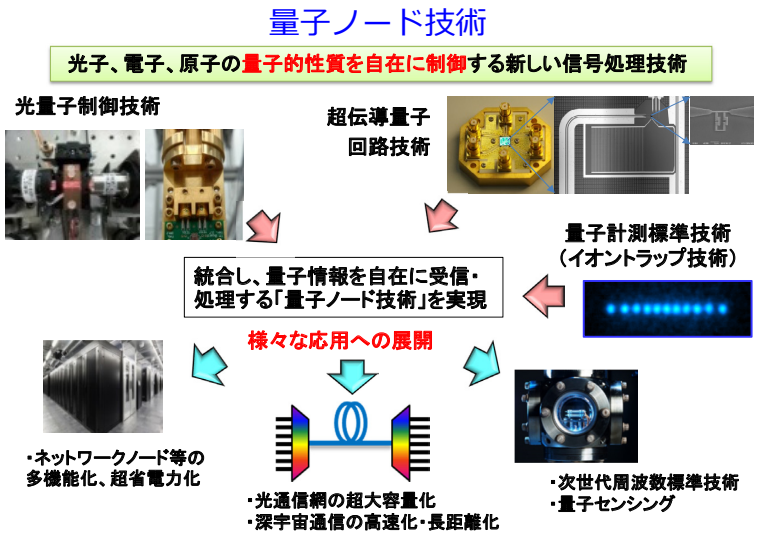

図2　量子ノード技術の概要

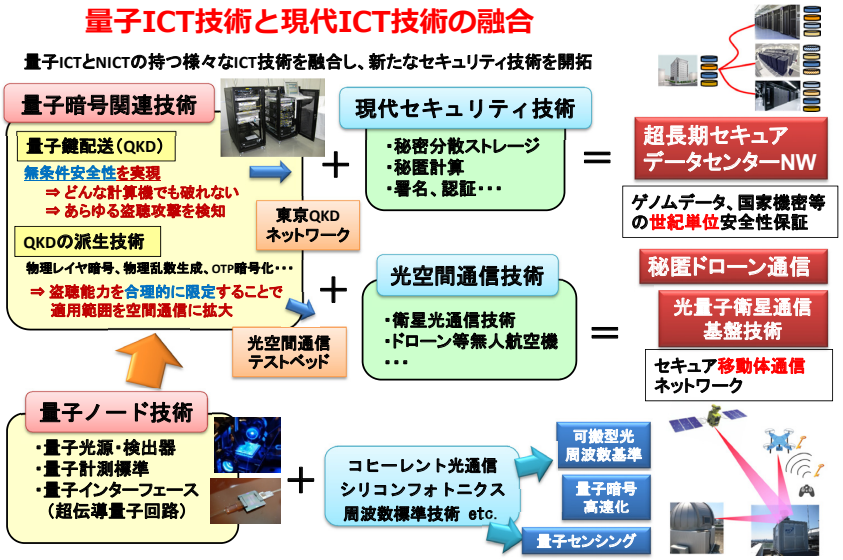

図 3　量子情報通信技術の社会展開に向けて

において、分散されたデータストレージ間の通信に量子暗号を用いることで、システム全体で情報理論的安全性の保証された、超長期セキュアデータセンターネットワークの実現が可能になる。

こうした研究開発を進めるには、現代セキュリティ技術を専門とする研究者との密な連携が欠かせない。また、量子暗号やその派生技術を衛星光通信・ドローンとの通信等の空間通信に組み込むためにも、それぞれ要求されるニーズ・仕様を適切に満たし意味のある社会実装を実現するため、各分野のエキスパートと連携し研究開発を進めている。また、量子ノード技術に関しては、まだ基礎研究の段階であるが、コヒーレント光通信、シリコンフォトニクス、周波数標準等、他の最先端 ICT 技術も取り込みながら、ICT 技術の将来を支えるべく NICT にしかない独自技術を研ぎ澄ましている。本特集号では、それぞれの技術課題について、NICT における研究開発を中心とした現状を紹介する。

武岡正裕　（たけおか　まさひろ）
未来 ICT 研究所
量子 ICT 先端開発センター
センター長
博士（工学）
量子光学、量子情報理論

仙場浩一　（せんば　こういち）
未来 ICT 研究所
フロンティア創造総合研究室
上席研究員
博士（工学）
超伝導量子物理

佐々木雅英　（ささき　まさひで）
未来 ICT 研究所
主管研究員
理学博士
量子通信、量子暗号