1　緒言

佐々木雅英

スマートフォンやパソコン、インターネットの中を駆け巡っている情報の実体は、電気や光のパルスの膨大な羅列であり、これらは0と1という記号の流れを表している。この2つの数字（ビット）による情報の抽象化が完成したのは1948年のことである（シャノンの『情報理論』）。同時期の1950年、ガボールはシャノン理論と量子力学の統合を試み、電磁波をその最小単位である光子として制御できれば通信路容量はシャノン限界より上がるだろうと示唆した。量子通信という概念の誕生である。1960年にはメイマンがレーザー発振に成功し、レーザーによる新時代が幕を開ける。レーザーの周波数は電波の10万倍あり、温度に換算すると光子1つで1万℃に相当するため熱雑音に埋もれることなく光子という粒（量子）の性質が顕在化する。量子通信は技術的な現実味を帯びて、その後、基礎理論の研究が連綿と続くことになる。

1982年には物理学者のベネットと暗号学者ブラサールが、プエルトリコのホテルのプールで偶然出会って交わした何気ない会話から量子暗号が誕生した。1985年には、ドイチェが多世界宇宙論の理論を発展させ、これまでの0と1による抽象化に代わり、0でもありながら同時に1でもあり得るようなビット『量子ビット』の概念を導入して量子計算の定式化を行った。1994年には、ショアによって、離散対数問題を高速で解く量子計算アルゴリズムが発見され、量子計算機が実現されれば、現代暗号も数分で解読できることが示された。これを契機に、量子通信、量子暗号、量子計算に関するおびただしい論文が発表されるようになり量子情報科学の誕生につながる。

ちょうどそのころ、通信総合研究所（CRL、現NICT）でも、量子通信に関する研究が始まった。当時はまだ光情報処理研究室の中の一研究課題として、理論研究を中心に進められていた。1999年から郵政省の下で量子通信、量子暗号、量子計算を統合した量子情報通信技術（量子ICT）に関する調査研究が始まり、産学官の識者と協力し研究開発戦略をまとめた。2001年にはCRLに量子情報技術研究室が発足し、高度通信・放送研究開発助成金交付業務（TAO）による量子暗号に関する委託研究と連携する形で、量子ICTの本格的な研究開発が始まった。

1　第1期中期計画（2001～2005年度）

研究室で最初に取り組んだのは、量子通信の基本原理、すなわち究極の通信効率を実現するための符号化技術の実証実験である。量子通信分野では1995年に大きな転機を迎えていた。すなわち、シューマッハーら米英の理論チームが量子通信の容量に関するホレボー上界予想に厳密な証明を与え、シャノン限界を超える通信の存在が証明された。しかし、具体的にどうすればシャノン限界を超え究極のホレボー限界へ近づけるのかは未解明で、存在定理にとどまっていた。

我々の研究はそのエッセンスを抜きだし、実験可能なモデルへ具現化するという作業から始まった。1996年に箱根で開催された国際会議で著者は初めてホレボーと出会い会議後の1週間をともに過ごし、彼が容量定理を更に一般化してゆく様子を目の当たりにした。彼との議論の中で、著者もシャノン限界を超えるための仕組みに思い至る。その原理とは、復号過程で量子計算を行いながら符号語状態間の量子干渉を引き起こして信号の識別性を向上させるもので、これにより超シャノン限界の通信が可能になる。その効果はシンプルに表現できる（通信資源を2倍に増やすと、伝送情報量が2倍以上に増える：超加法的符号化利得）。従来の理論では、伝送情報量は最大で2倍までは増えるが、決して2倍以上に増えることはない。超加法的符号化利得の原理実証実験は2003年に成功した。しかし、その実用化は予想以上に困難であることが明らかになっていく。

一方、量子暗号分野では2000年以降、本格的な実験が世界各国で始まった。2005年には、アメリカの国防総省国防高等研究計画局の支援を受けたプロジェクトがボストン地区に3地点を結ぶ量子暗号ネットワークを構築しフィールド実験に成功した。ヨーロッパでは2004年に欧州連合のプロジェクトSECOQC

が発足し、12 カ国、41 機関の研究チームによる研究開発が始まった。同じころ NICT では、量子鍵配送装置のプロトタイプの開発を三菱電機、NEC 及び東京大学に委託し着々と基盤技術を開発していった。

量子計測標準分野では、単一イオンを共振器内に閉じ込め自在に制御することで、周波数標準の確度を向上させる技術や、単一光子を生成制御する技術を開発した。

2　第 2 期中期計画（2006 ～ 2010 年度）

2003 年に行った超加法的符号化利得の実証実験では、単一光子の偏光・経路変調符号という特殊な信号を使っていた。しかし、実用化にはレーザー光の状態（コヒーレント状態）に対して量子計算を実装する必要がある。第 2 期中期計画では、コヒーレント状態からなる量子ビットの制御技術の開発を本格化した。コヒーレント状態の量子ビットは、『シュレーディンガーの猫のパラドックス』として知られ、その生成は量子物理学積年の夢であった。NICT でも 2003 年から試行錯誤を続けていたが、2004 年にフランスのシャルル・ファブリ研究所のグループが基礎技術を論文発表し、初めて同じゴールをねらうライバルの存在を知る。2005 年秋にはデンマークのニールス・ボーア研究所でもシュレーディンガーの猫状態を生成したとの報が入り、12 月にはシャルル・ファブリ研究所がついにシュレーディンガーの猫状態の生成をサイエンス誌に投稿したことを知る。

先陣争いに敗れた落胆からはい上がり、我々も独自の実験装置の改良を進め、2006 年夏にこれまでとは質的に違った高純度のシュレーディンガー猫状態の生成に成功した。その後、この技術を用いて、猫状態の大きさ（波の振幅）を増幅する技術や、猫状態の奇数光子と偶数光子の比重を自在に制御する技術など、新しい技術を次々と開発し、量子光学に新局面を切り開き新しい ICT への基盤を構築してきた。成果は物理・光学分野で最も著名な国際論文誌に掲載された。

シュレーディンガーの猫状態生成と並んで量子 ICT の実現に欠かせないのが、パルス内の光子数を正確に識別できる光子数識別器である。光子数識別器は低雑音であるのはもちろん、光子を電気信号に変換し読み出す効率（量子効率）もほぼ 100 % に近くなくてはならない。このような要求を満たす光子数識別器として、超伝導転移端センサーの開発を産業技術総合研究所、日本大学、物質材料研究機構に研究開発を委託し、世界トップレベルの光子数識別器を開発していただいた。

量子暗号分野は、フィールド実験の時代に入り、日本では三菱電機、NEC に続き、NTT にも本格参入していただき第 2 期中期計画に移行した。ヨーロッパでは、SECOQC プロジェクトの下で多地点間の量子暗号ネットワークの構築が始まっていた。2008 年 10 月 8 日、ウィーンで SECOQC のフィールド実験が研究者や報道陣に公開された。平均の伝送距離は 30 ㎞、鍵の生成速度は 1 kbps で音声の完全秘匿化を行える性能だった。日本では 2010 年 10 月に、NICT、NEC、三菱電機、NTT のほか、東芝欧州研究所、ID Quantique、オーストリア工学研究所やウィーン大学にも参加していただき、最新鋭の量子暗号ネットワーク“Tokyo QKD Network”を開設し、動画伝送の完全秘匿化に世界で初めて成功した。わずか 2 年で伝送距離は、SECOQC ネットワークの 2 倍近くの 50 km に伸び、暗号化速度は 100 倍以上に向上した。また、各機関の仕様の異なる QKD 装置を相互接続するための最新のアプリケーションインターフェースを開発し、ネットワーク運用を行いながら様々なノウハウを蓄積した。

量子計測標準分野では、2 種の異なるイオンを共振器内で共同冷却することで、周波数標準の確度を向上させ、高精度で周波数を測定する技術を開発した。

3　第 3 期中長期計画（2011 ～ 2015 年度）

第 3 期中長期計画では世界トップの光子数識別器を生かして、量子通信の基幹部品となる量子受信機の開発に取り組んだ。これは 1 つの光信号パルスに対して量子計算を行い、究極のビット誤り率を実現する受信機である。量子受信機の原理実証は、2011 年に NICT が世界に先駆けて成功した。また 2013 年には、猫状態生成技術を拡張し、光入力信号を無雑音に増幅し遠方に転送する「量子増幅転送」を発案・実証した。しかし、これらの技術はまだ実験室内の限られた環境下でしか使えず、超シャノン限界通信の実用化は依然として至難の業で、抜本的に新しい技術を開発する必要がある。実際、光学素子のみでの実現には限界があり、より強い非線形相互作用を実現できる超伝導素子の導入などが必要と考えられる。第 3 期中長期計画後半では、超伝導素子上で磁気的な量子ビットとマイクロ波量子を強結合させるための新たな研究も始まった。

量子暗号分野においては、Tokyo QKD Network 上で新しいセキュリティアプリケーションの開発に取り組んだ。まず、量子暗号によって生成した暗号鍵を 2 つの拠点の IP ルータに供給し、IP パケットごとに完全秘匿化を行いかつ改ざん防止の認証を行う技術を開発した。この技術によって、オープン系として動いているインターネット上で、重要通信を行う拠点間に完全秘匿なプライベートネットワークを自在に構成できるようになる。また、暗号鍵をスマートフォンやド

ローンなどの移動体に供給し無線通信を完全秘匿化する技術を開発した。

量子暗号技術は、NEC、東芝の事業部に移管され、2015 年には東京都内や仙台市のユーザー環境の敷地内で試験稼動が始まり、現在も信頼性試験が継続的に行われている。

量子計測標準分野では、時計遷移を担うイオンと共同冷却・読み出しを担うイオンとの間で自在な制御や情報転写を行う量子論理分光技術を開発した。

4　第 4 期中長期計画（2016 ～ 2020 年度）

NICT における量子 ICT の研究開発は、当該分野の勃興と発展の歴史そのものである。2001 年の研究室発足以来、量子 ICT の新原理実証と実用化に向けた研究開発という基礎と応用の 2 つを柱として取り組んできた。基礎研究は益々深まり、光、イオン、超伝導など複数の物理系を統合したシステムが持つ新しい現象の解明や ICT への応用探索の研究フェーズに移行している。将来は、このような統合システムをネットワークのノード内に導入し『量子ノード』を形成することで、従来の伝送容量や計測標準の限界を打ち破ることが可能になる。しかし、実用化にはまだ多くの課題が残っており、長期的な基礎研究が必要である。応用研究はますます広がり、量子暗号は現代暗号との融合や移動体への要素技術の適用などが進み、暗号分野、ネットワーク技術分野自体に新局面を切り拓きつつある。特に、量子暗号の距離や速度の限界を打破することを目的に取り組んだ研究からは、情報理論と暗号技術を統合する『物理レイヤ暗号』という新領域も生まれている。これは光空間通信をバックボーンとする新しいグローバルセキュアネットワークの構築を可能とするものである。このような新潮流を踏まえ、地上光ファイバネットワークから衛星を頂点とする移動体のワイヤレスネットワークまでカバーする、安全かつ伝送効率に優れた新たなネットワークを『量子光ネットワーク』と名づけ、『量子ノード』とともに第 4 期中長期計画の根幹テーマに据えた。

シャノンの情報理論によって 0、1 のビットに抽象化された情報は、今『量子』という最も深い物理のレイヤ（量子レイヤ）からその枠組みごと再構築されようとしている。量子レイヤは、ICT という体系を最も広い視点からとらえるもので、これからも科学に新知見をもたらし続け、ICT に変革を与え続ける舞台となるだろう。本特集号では、その取組の最前線を紹介する。

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