2.13 量子 ICT 基盤技術

2001年（平成13年）4月、当時の通信総合研究所（CRL）に量子情報技術研究室が発足し、NICTで量子情報通信技術（量子ICT）の研究開発が本格的に始まった。折しも、量子力学と情報科学が融合し量子情報科学という新分野が急激に成長し始めていた。実際、Physical Review誌など物理学の主要誌に量子コンピュータや量子暗号、量子情報理論に関するおびただしい論文が発表されるようになり、世界各国でこれらに関する国家プロジェクトが立ち上がっていった。この13年間、NICTでは、量子ICTの新原理開拓やその実証実験に取り組むとともに、その実用化に向けて産学官の様々な研究機関に委託研究を受託頂き、All Japanの体制で戦略的に取り組んできた。その成果は、国際的著名誌への論文掲載や、世界最高速での量子暗号化が可能な都市圏の試験ネットワーク“Tokyo QKD Network”の構築等に繋がっている。本稿では、これまでの取組を当該分野の発展の歴史と合わせて整理する。

2.13.1　黎明期（～2000年度）

量子通信の源流はシャノンによる通信理論誕生（1948年）と同時期まで遡る。1950年に、すでにガボールは、シャノン理論を物理学の一分野としてとらえるべきであるとして量子論との統合を試み、光子検出器があれば通信路容量は古典論より上がるだろうと示唆した。同時に通信にはプランク定数によって決まる「量子雑音」という不可避な雑音が伴うことも指摘した。1960年にはメイマンがレーザーの発振に成功し、レーザーによる新時代が幕を開ける。レーザーの光子のエネルギーは、周波数が電波の10万倍あるため、温度に換算すると光子1つで1万度くらいに相当し、光子という粒の性質が電波の通信より顕在化する。レーザーの誕生は、量子通信理論の構築を迫っていたわけである。

まもなくベル研究所のゴードンが、シャノン理論を量子力学の言語である行列力学を用いて書き換え、シャノンエントロピーに代わってフォンノイマンエントロピーという量を通信の分野に初めて導入した。彼は、のちにホレボー情報量と呼ばれることになる表現を1964年に通信路容量の上界予想として発表した。しかし、当時、量子測定を定式化する理論は未完成で、システム全体の完全な記述までには至らなかった。1970年代にはホレボーら旧ソ連の学者が量子一括測定という概念をゴードン予想に持ち込み、上界が実は真の通信路容量だろうと証明を試みる。しかし当時はまだ成功しない。再び進展し始めるのは1990年代になってからである。

一方、1980年代には量子暗号と量子計算の概念が発明される。量子暗号の発明は偶然で、1982年に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、何気ない会話からのちにBB84と命名される量子暗号が生まれたと言われる。1985年には、ドイチェが多世界宇宙論の理論を発展させ量子計算の概念を提唱した。

1994年には、ベル研究所のショアによって、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、量子コンピュータが実現されれば、現代暗号も数分で解読できることがわかってきた。これを契機に、量子通信、量子暗号、量子計算の研究が合流して、量子情報科学の誕生につながる。

ちょうどその頃、CRLでも、光の量子制御技術や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年頃から郵政省の下で量子情報通信に関する調査研究が始まり、CRLが中心になって産学官の識者と協力し研究開発戦略に関する報告書をまとめた。2001年（平成13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、量子情報通信の本格的な研究開発が始まった。

2.13.2　第1期中期計画

研究室で最初に取り組んだのは、量子通信の基本原理の実証実験である。それは、究極の通信効率を実現するための符号化技術に関するものである。1964年のゴードン予想に対して、1970年代にホレボーが量子測定理論を適用し厳密な上界定理として証明したが、実際に達

成可能な通信路容量かどうかについては、その後20年、未解明のままであった。突破口が開かれたのは、1995年である。古典雑音が無い場合について、シューマッハーら米英の理論チームが、ホレボー上界は実際に達成可能な伝送容量であることを証明した。そして、翌年、ホレボーも古典雑音を含む一般的な場合へ証明を拡張し、シューマッハーらも同時に一般化に成功する。彼らの理論は、これまでのシャノン限界を超える通信が可能であることを示していた。しかし、具体的にどういう技術を用いればシャノン限界を超えた新しい通信領域へ踏み出せるか、という点については未解明で、ただそういう領域が存在するということを示しているに過ぎなかった。

CRL では、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。結局、シャノン限界を超えるためには、復号過程で量子コンピュータの原理、すなわち重ね合わせの原理に基づく量子計算を用いるのが本質的であり、その過程で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ことで超シャノン限界の通信が可能になることがわかってきた。この仕組みの効果は、次のようにシンプルに表現できる：伝送に費やす通信資源の量を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）。これに対して従来の理論では、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（図2.13.1）。

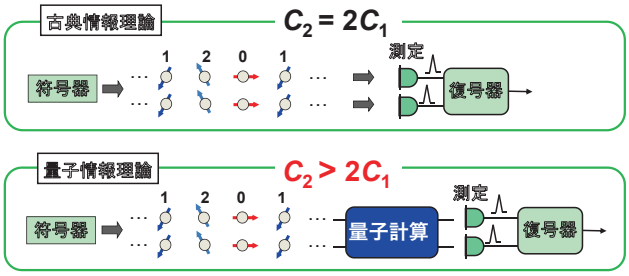

図2.13.1 古典情報理論と量子情報理論での復号方式の比較と超加法的符号化利得

超加法的符号化利得の原理実証実験は2003年（平成15年）に成功した。図2.13.2がその実験データで、縦軸が取り出された情報量、横軸のオフセット角は、送信状態と最適な復号基底間の相対位相で、最適値の前後に振って情報量の劣化を測定している。水平の赤の破線が従来の符号化を用いた場合の限界（シャノン限界）、黒の点

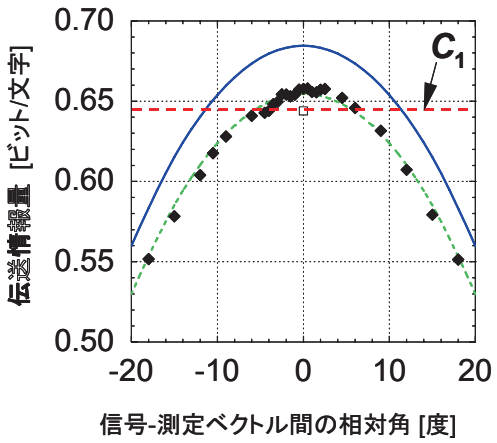

図2.13.2 超加法的量子符号化利得の実験データ

が実験データで、わずかに上に出ている部分が超加法的量子符号化利得の実験データであり、光子の信号帯域を2倍にした時、2倍以上の情報量が伝送されていることを示している。青の線は理論値を示す。大容量化へ向けた新しい原理が、ようやく見えてきたわけである。その本質は従来にはない量子計算を組み込んだ新しい受信過程にあり、この新しい復号器のことを量子デコーダと呼ぶ。

一方、量子暗号の分野は、2000年以降、本格的な実験が世界各国で始まり、ID Quantique（スイス）やMagiQ（アメリカ）などのベンチャー企業も誕生した。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。その後、アメリカでは、国家機密の研究に移行していく。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か国、41機関の研究チームによる研究開発が始まった。

同じ頃、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株式会社、日本電気株式会社（NEC）及び国立大学法人東京大学に委託する形で推進し、着々と基盤技術を開発していった。そして、2005年度末（平成17年度末）に、NICT 光テストベッド JGN2 の秋葉原アクセスポイントにて、三菱電機システムと NEC システムを相互接続し暗号鍵の最初のリレー実験に成功し、将来のネットワーク化への布石を打っていた。この時点ではまだ20kmのボビンファイバーを用いた室内伝送実験であった。

2.13.3 第２期中期計画

2003年（平成15年）に行った超加法的符号化利得の原理実証実験では、実はまだ伝送に適した信号は用いていなかった。伝送に適した信号はレーザー光、つまりコヒーレント状態で、この状態こそが唯一、損失があっても干渉性を維持できる理想的搬送波の状態である。しかし、このような巨視的信号で量子計算を行う技術は、まだ実用レベルにはなく、2003年（平成15年）の実験では、単一光子の偏光・経路変調符号という特殊な信号で原理実証を行っていた。

第2期中期計画では、量子デコーダの実現を目指して、コヒーレント状態を自在に量子制御するための研究開発を本格化した。主要な課題は2つあり、1つは巨視的に異なるコヒーレント状態の重ね合わせ状態を自在に生成制御する技術、もう1つはそのような状態を最高精度で計測する技術である。巨視的に異なるコヒーレント状態の重ね合わせ状態は、シュレーディンガーの猫のパラドックスとして知られる典型的な量子効果を内在しており、シュレーディンガーの猫状態とも呼ばれ、情報通信に新しい局面を切り開く重要なリソースとなるものである。このシュレーディンガーの猫状態を光の伝播モード内に生成するのは量子光学積年の夢であった。そのためには、光子レベルでの強い非線形過程が必要で、これが困難な壁として立ちはだかっていた。すでに1990年代にスクィーズド光と光子検出器を組み合わせて測定誘起型非線形過程を使う方式が提案されており、第1期中期計画後半には、NICT の研究室でも必要な技術が整備され始めていた。2003年（平成15年）から試行錯誤を続けていたが、2004年にフランス国立科学研究センターのシャルル・ファブリ研究所のグループがシュレーディンガー猫状態への第一歩となる状態の生成に成功し、初めて同じゴールをねらうライバルの存在を知った。2005年秋にはデンマークのニールス・ボーア研究所でも類似の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猫状態の生成についてサイエンス誌に投稿したと知ることとなった。

落胆からはい上がり、NICT の研究室も独自の実験装置の改良を進め、2006年（平成18年）春には何とかシュレーディンガーの猫状態を生成できるようになった。夏になり、国際会議に向けて実験の改良を続けていた研究員が、偶然試した新しい結晶で、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。図2.13.3は単一光子状態とシュレーディンガー猫状態の電場振動の様子を示したものである。光子1個の電場振幅は不確定性原理のために完全にランダムになり、位相変化に依存しない2本の平行な分布から成る。分布がぼやけているのが不確定性原理による量子雑音である。下の図はウィグナー関数と呼ばれる表現で、原点付近に負のくぼみがあるのが量子特有の効果を表している。

この状態から光子を増やしていくと、徐々に波として振動する様子が現れ始める。右の図は位相が180度ずれて振動する2つの波が同時に存在している状態を表している。そのウィグナー関数は原点で負の値をとっており、2つの波が量子力学的に重ね合わさった状態であることを示している。

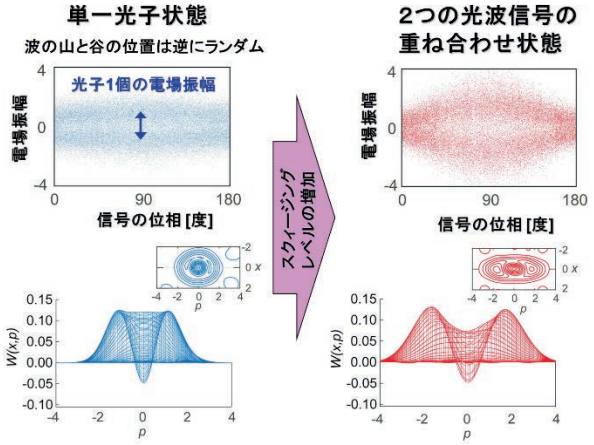

図2.13.3　単一光子状態とシュレーディンガー猫状態の電場振動の様子とウィグナー関数分布

その後、NICT で開発したシュレーディンガー猫状態生成技術を用いて、シュレーディンガー猫状態の大きさ（波の振幅）を増幅する技術や、重ね合わせ状態における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ながら新しい ICT への基盤を構築してきた。成果は Physical Review Letters 誌、Nature Photonics 誌等、物理・光学分野で最も著名な国際論文誌に掲載され、新聞、Web サイト等でも紹介された。一連の研究で用いられた実験系の写真を図2.13.4に示す。3メートル四方ほどの光学定盤上に精密光学部品がびっしりと並び、それらを制御するための電子機器と電気ケーブルがひしめき合っている。まだ、2ビット程度の量子計算処理し

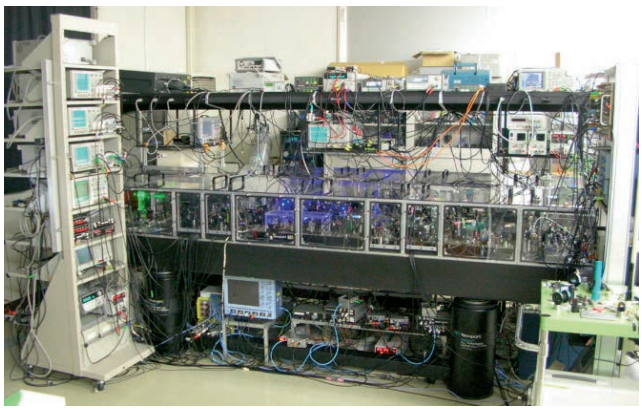

図2.13.4　シュレーディンガー猫状態を生成・制御する装置

かできないが、将来は、より小型で多ビットの処理ができるような量子回路に改良していく計画である。そして、このような回路内にシュレーディンガー猫状態をあらかじめ用意しておき、ファイバから入ってきたコヒーレント状態と相互作用させ、ある適切な状態に変換してから測定することで、従来限界を超える高効率の通信を実現するのが量子デコーダであり、量子 ICT 分野での長期的な目標である。現在の光通信では1ビット当たり10万個以上の光子を使っているが、このような量子デコーダが実現できると、1ビット当たり1個に満たない光子でも、信頼性の高い情報伝送が原理的に可能であることが理論的に示されている。

量子暗号分野では、欧米で研究開発が加速する中、フィールド実験の時代に入り、日本では三菱電機株式会社、NEC に続き、NTT にも本格参入していただき、順調に第2期中期計画に移行した。ヨーロッパでは、SECOQC プロジェクトのもと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。NICT に最新の超伝導光子検出器が整備されたのを機に2007年（平成19年）夏、当初計画には無かったが、NEC と NICT の連携による本格的なフィールド実験に踏み切った。SECOQC が2008年に大規模なフィールド実験を予告しており、日本でも早急に経験値を上げておく必要があった。けいはんなオープンラボにおいて、京都と奈良の県境にあるJGN2の敷設ファイバを用いた、波長多重による量子暗号の伝送技術の実験を行った。

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。その後、ヨーロッパでは、ジュネーブ、マドリッドに量子暗号のテストベッドが開設され、南アフリカではダーバンに、中国では蕪湖（Wuhu）にフィールドテストベッドが開設され、米国でも Telcordia やロスアラモス国立研究所が粛々と伝送実験に取り組んでいた。

日本では、2009年（平成21年）から JGN2plus の敷設ファイバを用いて、多地点の量子暗号ネットワーク“Tokyo QKD Network”の構築に着手した。QKD は、量子鍵配送の英語略である。量子暗号では、まず、送り手と受け手に量子鍵配送装置を用意し、光回線を介して安全な暗号鍵（0,1の乱数列）を共有する。次に、送り手はこの鍵と送りたい情報を足し算（ビット値の論理和）して暗号文とし伝送する。受け手は暗号文に共有しておいた暗号鍵を足し算すると情報が復元される。一度使用した鍵は二度と使わないワンタイムパッド方式で運用することで原理的に破れない暗号通信が可能となる。

NICT、NEC、三菱電機株式会社、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、2010年（平成22年）10月に、最新鋭の Tokyo QKD Network を開設し、そこで動画伝送の完全秘匿化に世界で初めて成功した（図2.13.5）。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。そこでの成果は、テレビ、新聞、Web サイトなど多くのメディアで広く紹介いた

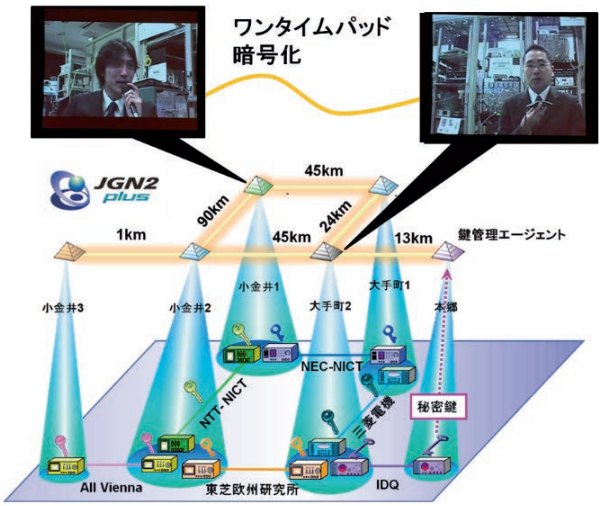

図2.13.5　量子暗号ネットワーク（Tokyo QKD Network）と盗聴不可能なテレビ会議システム

だき、Nature Photonics 誌、Science 誌などトップ科学誌のニュース欄でも紹介された。

2. 13. 4　第３期中期計画

コヒーレント状態の自在な量子制御と並んで量子 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。これは、光が光子の集まりであるという離散性を最大限に活用するために必須の技術である。量子通信のほか、量子計算及び量子計測標準の実現に欠かせない技術である。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は、現在、超伝導転移端センサーが最も有望な方式であり、第2期中期計画期間中に独立行政法人産業技術総合研究所、日本大学、独立行政法人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が開発された。

この技術を活用し、量子 ICT 研究室では、まず量子デコーダの基幹部品となる量子受信機の開発に取り組んだ。図2.13.1で説明した量子デコーダでは、2つ以上の光信号を測定する前に量子計算機に通して量子的な演算を行い、その後光子を検出するというものであったが、前述の通りこれをコヒーレント状態の光で自在に行うことは現在の技術では困難である。量子受信機は、この量子計算の部分を最も簡単化し、1つの光信号に対してのみ量子計算（量子制御）を行い、その後に光子を測定し、量子雑音による信号識別性能の劣化を限界まで抑制する受信機が、量子受信機である。

図2.13.6に、その概念図と実験結果を示す。コヒーレント光の位相変調で作られた0, 1の信号は、「量子受信機」内で、まず波の制御（量子制御）がなされ、その後光子数識別器で信号識別を行う（上部左は量子受信機の装置写真）。量子受信機が、従来の光通信理論の信号識別限界（ショット雑音限界）を超えた、超低ビット誤り率を実現し得ることは、理論上は予想されていたが、2011年（平成23年）に、本実験で NICT が世界に先駆けてその原理実証に成功した。本成果が物理学分野の国際的著名誌 Physical Review Letters 誌に掲載されると、その後世界の主要研究機関の量子受信機開発を促進することとなり、現在では、米国の NIST、Raytheon BBN

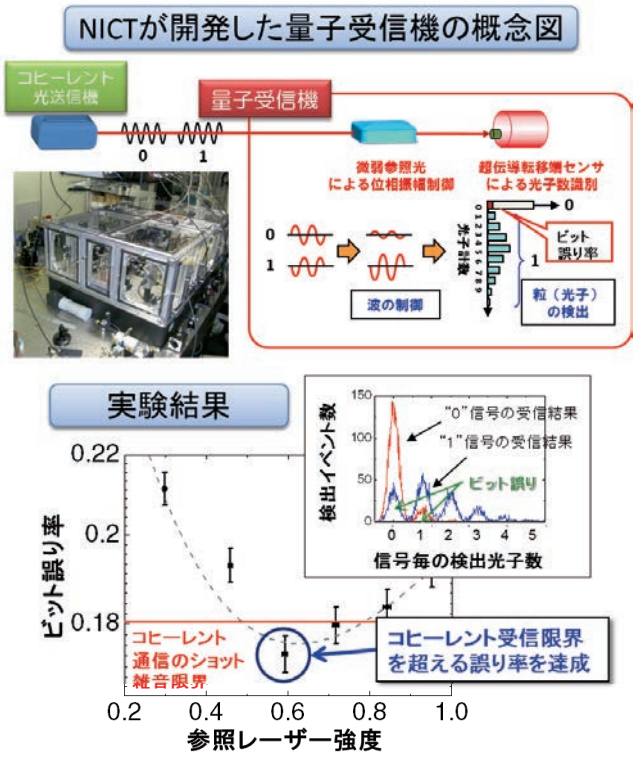

図2.13.6　開発した量子受信機の概念図と実験結果

Technologies、ドイツの Max-Planck 研究所等から次々と本成果を発展させる新しい実験成果が発表されており、熾烈な研究開発競争が始まっている。

一方、第2期中期計画で開発したシュレーディンガーの猫状態の生成技術の応用研究も進め、光の入力信号を無雑音に増幅し、出力側に転送する「量子増幅転送」技術を発案し、2013年（平成25年）に実証に成功した。図2.13.7にその概念図を示す。図中下のグラフは、この技術を将来的に量子暗号に応用した場合の伝送距離に対する量子鍵生成率の試算であり、本技術が将来的により確立されていけば、従来の量子暗号の伝送距離限界を大きく超え得る可能性を示している。こちらの成果も光学分野の国際的著名誌である Nature Photonics 誌に掲載され、新聞、Web サイト等でも紹介された。

量子暗号分野においては、量子鍵配送システムの実用化をにらみ、現在のインターネットの安全性に直接寄与することを目的として、量子鍵配送システムで生成された情報理論的に安全な鍵をネットワークスイッチに供給し、IP ベースの通信の安全性を飛躍的に向上させ得るシステムの開発を行った。

現在のインターネットで使用されている標準通信プロトコルの TCP/IP の OSI 参照モデルでは7階層モデルに

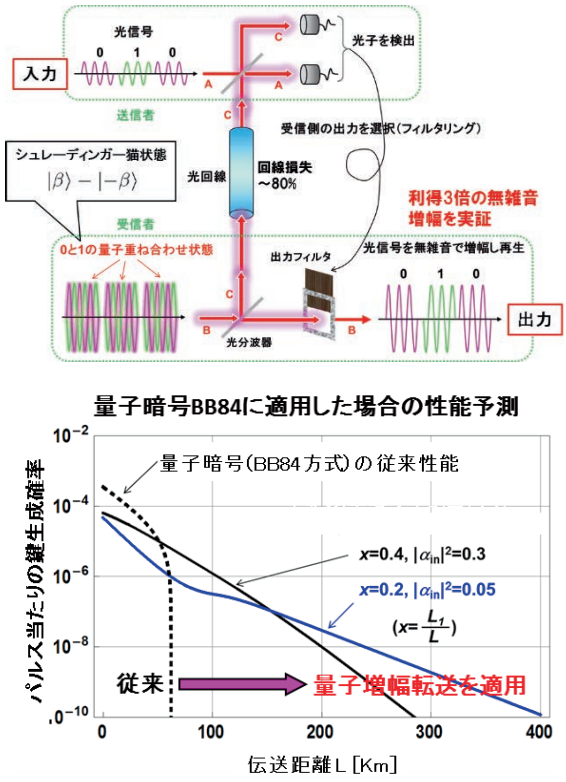

図2.13 7　量子増幅転送の概念図と実験結果

則って構成されている。この中で IP アドレスを基に通信を行っているのは第3層のネットワーク層（Layer 3）であり、この層で利用されているスイッチでは IP アドレスを利用して通信先を判断している。IP パケット単位でデータの改竄防止や秘匿化を提供するプロトコルとして IPsec が開発されている（図2.13.8）。IPsec のこの機能に対し、暗号化と認証用に量子鍵配送で生成した情報理論的に安全な鍵を用いることで情報理論的に安全に暗号化と認証を IP パケットで実現するシステムを開発した。暗号化にはワンタイムパッドを用い、認証にも情報理論的安全性が証明されている Wegman-Carter 認証方式を採用した。量子鍵配送と IPsec を融合することにより現在の IP ベースの通信でメール、TV 会議システムなどアプリケーションを選ばず情報理論的に安全な

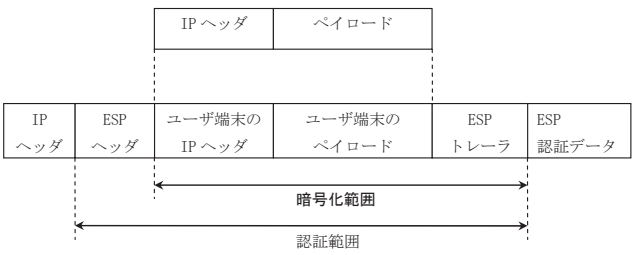

図2.13.8　IPsec のパケット構成：量子鍵配送による暗号化・認証範囲

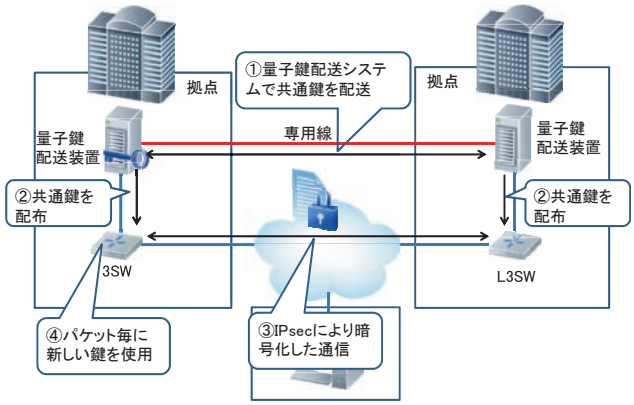

図2.13.9　量子鍵配送装置と組み合わせた Layer 3 スイッチ動作手順

通信が可能となった（図2.13.9）。

情報通信の総合的な安全性を高めるためにはあらゆる階層での安全性を担保する必要がある。ネットワーク拠点内部からの不正アクセスを防ぐ技術も量子鍵配送システムの総合的な安全性を高める上で不可欠である。特に量子鍵配送システムと物理的に接続するデータリンク層（Layer 2）での安全性の向上が望まれている。Layer 2 でのパケットの中継はメディアアクセス制御（MAC）アドレスを基に行われているが、MAC アドレスを詐称するツールはインターネットで公開されており、Layer 2 での成りすましによるデータ不正取得の実例が報告されている。NICT では量子鍵配送システムに実装されている物理乱数発生機を利用し、周期性のない乱数を Layer 2 スイッチとそれに接続されている端末とで共有させ、その乱数を用いて MAC アドレスを暗号化するシステムを開発した。MAC アドレスをパケットごとにワンタイムパッドで暗号化し、Layer 2 スイッチでは解読した MAC アドレスと予め設定されている IP アドレスを照らし合わせ、端末が偽証していないことを確認後にパケットを

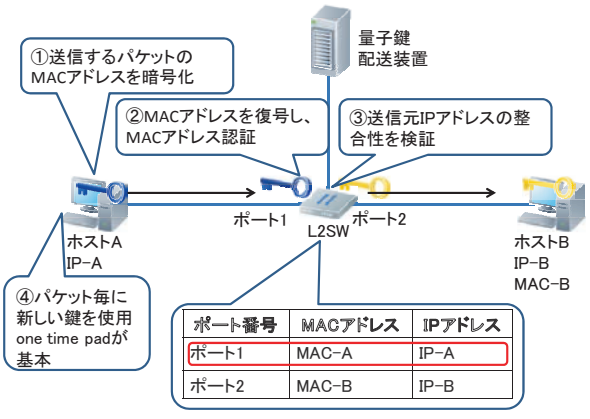

図2.13.10　量子鍵配送システムと組み合わせた Layer 2 スイッチ動作概要

繋ぐ。MAC アドレスの暗号化に使用する乱数はスイッチと端末しか知り得ない情報であるため、成りすますことが非常に困難なシステムとなった（図2.13.10）。さらに NICT では Layer 2スイッチと端末で乱数を共有するためのデバイスとしてスマートフォンに着目し、スマートフォンを介して端末に乱数を供給し得るシステムを構築した。乱数発生機から乱数を受け取り、使用する端末にスマートフォンを介して転送するシステムを開発した。これによりスマートフォンを認証用デバイスとして用いることも可能となった。

量子鍵配送システムをネットワークスイッチと組み合わせることにより安全性と利便性、拡張性を向上させることに成功した（図2.13.11）。すなわち量子鍵配送システムを安全性を劣化させることなく IP ベースのネットワークとの親和性を向上させることが可能となった。利便性の向上はヒューマンエラーの確率を低減させ、より安全なシステムとなったといえる。

2. 13. 5　今後の展望

2001 年（平成 13 年）の研究室発足以来、量子情報通信の新原理実証と基盤技術開発、そして量子暗号の基盤技術開発から実用化に向けた研究開発の2つを柱として、研究開発を進めてきた。

量子デコーダ技術については、この10年間の基礎研究開発の結果、現時点で最先端の光波制御・光子検出技術を使い、この新しい原理を世界に先駆けて実証し、基礎研究としては世界最先端の地位を確立することができた。一方、実用までの道のりにはまだ時間が必要であろう。最近実用化が始まった光通信技術であるコヒーレント光通信方式でも、その原理実証実験が1980年代には既に盛んに行われていたことを考えると、量子デコーダの研究も、適正な予算規模の中で引き続き息の長い研究開発を継続することが重要である。

量子暗号については、より実用化に近い技術であり、NICT が産学官の様々な研究機関と連携することで、All Japan の体制を作り、基礎理論、デバイスの研究からネットワークシステム、アプリケーションの開発まで、戦略的な研究開発を進めることができた。それらを結集して東京の JGN 上で構築した量子暗号試験運用ネットワーク“Tokyo QKD Network”は、世界的にも最も実用に近い量子暗号ネットワークであるとの評価を確立している。一方で、本技術は国家機密・軍事機密等の最重要機密のセキュリティに関わる技術であることから、欧米や、特に最近では中国が、膨大な国家予算を投じて急激に追い上げている。日本としては、現在の技術的な優位性を生かし、実用化への最後の仕上げとして、長期試験運用実績の蓄積など、技術開発に引き続き取り組むと同時に、量子暗号の導入に興味を持っている（将来的な）ユーザーとの議論を通じて運用方法、アプリケーションなどの改良を進め、実際の導入事例へとつなげ、最終的には民間への技術の早期受け渡しを目指す。一方、量子暗号

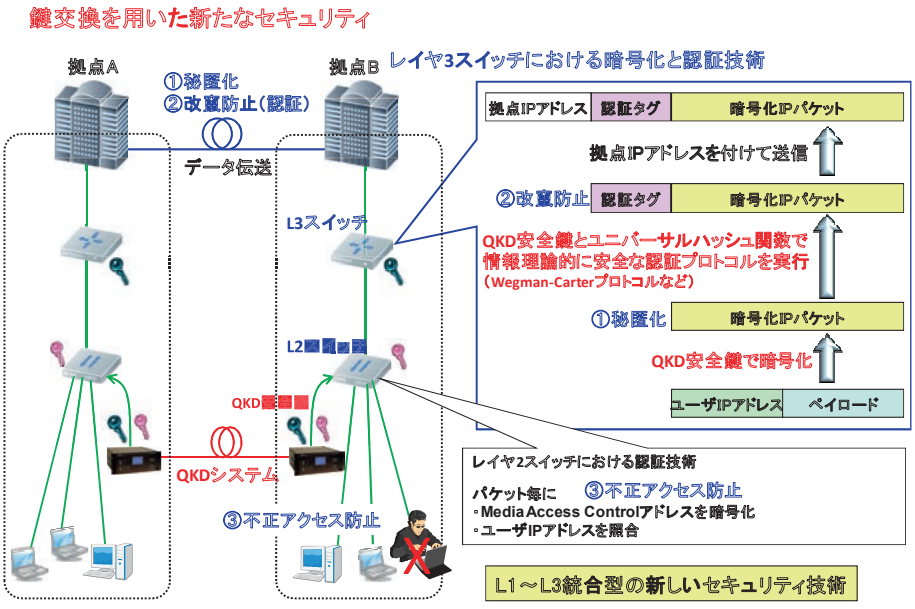

図2.13.11　量子鍵配送を用いたセキュアネットワークの概念図

の基礎研究においても、量子もつれなどを駆使したより高度な新世代の量子暗号プロトコルや、量子暗号の究極の安全性の条件を多少緩めることで大幅な伝送性能の改善を可能にする物理暗号（概念的には、従来の古典情報理論で長く研究されていたが、近年量子情報分野の研究者がその著しい進展を促している）など、次々と新しいアプローチが議論されており、引き続き産学官連携のもと、次世代の量子暗号・物理暗号の基礎研究開発に取り組むことも重要であり、NICT では引き続き産学との連携を密にして研究開発に取り組んでいく所存である。