4 量子暗号

量子コンピュータが実用化されても、絶対に解読されない暗号技術の開発

これまで情報通信の安全性を担保してきた現代暗号は、量子コンピュータの登場による危殆化が危惧される。NECは量子力学・情報理論に基づいた絶対安全性が証明されている「量子暗号」に25年以上取り組んできた。実用化を目前にした「BB84」、開発中の次世代技術「CV-QKD」、2つの量子鍵配送方式について紹介する。

高度に情報化した社会の安全性を担保する暗号通信

高度に情報化した現代社会において、インターネットをはじめとした通信の安全性は不可欠だ。悪意のある第三者に機微情報が盗まれてしまうと、個人の社会生活、企業・公共団体活動、引いては国家安全保障すら危機に瀕することになる。

現在、流通・交換される情報のほとんどは、スーパーコンピュータを用いても解読に天文学的な時間がかかるRSA暗号などの「現代暗号」によって安全性を担保されている。しかし、暗号解読技術の進展によりRSA2048bitなど現代暗号の一部は2030年には利用期限を迎え、さらに現行のコンピュータの処理速度をはるかに上回る量子コンピュータの登場によって、RSAなどの標準公開鍵暗号の安全性は早晩危殆化してしまうことが危惧されているのである。

量子コンピュータの実用化は20年以上先と予想されているものの、インターネット上のデータを盗み出して保管し、量子コンピュータの実用後に解読するSNDL（Store Now、Decrypt Later）攻撃にさらされる可能性があり、より安全な暗号技術の確立は急務といえる。

現在の標準公開鍵暗号に代わる暗号技術として、量子コンピュータが苦手とする数学的な問題を基に暗号アルゴリズムを設計する「耐量子計算機暗号」（PQC）が実用化の緒に着いているものの、将来危殆化の可能性のあることが指摘されている。

耐量子計算機暗号とは異なり、量子力学の原理により「絶対に解読されない」ことが理論上保証されているのが「量子暗号」である。

量子鍵配送＋暗号化通信のメカニズム

NECは国内に主要研究拠点をもつ唯一の企業として、国立研究開発法人「情報通信研究機構（NICT）」とともに、量子暗号技術開発を牽引してきた。

研究初期の2000年頃から、量子暗号の1方式である「BB84」方式の開発に取り組み、すでに実証実験を終えたこの方式は間もなく事業化にいたる。また、より小型・低コストでシステム導入のハードルが低い、次世代技術の「CV-QKD」方式は研究の途上にあり、2025年の試作機開発を目指している。

NEC
アドバンストネットワーク研究所
ディレクター　**前田 和佳子** 氏

量子暗号通信は、「量子鍵配送」と、ワンタイムパッドによる「暗号化通信」の2つの技術によって成り立っている（図2）。

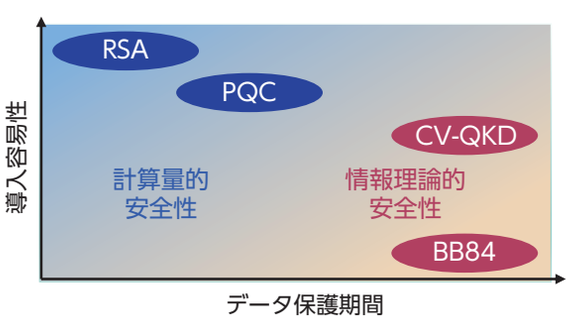

図1　暗号技術の導入容易性・データ保護期間比較

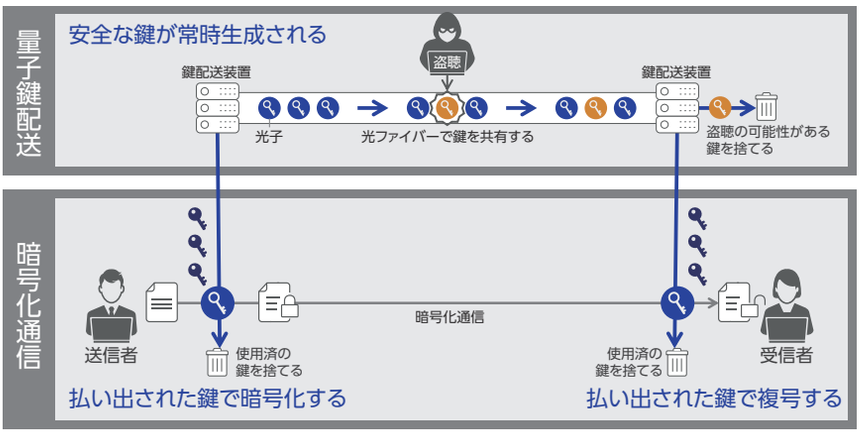

図２　量子暗号通信＝量子鍵配送＋暗号化通信

量子鍵配送によって事前に暗号鍵を伝送・共有し、暗号化通信で通信文を送る際に暗号化・復号を行う。

量子鍵配送では、1 粒の光子ごとに鍵情報 (1bit) を乗せて光ファイバ上を伝送する。盗聴者が光子を抜き取ると、光子は受信者に届かないため暗号鍵として成立せず、盗聴者は通信者と同じ鍵情報を取得できない。また、盗聴者が光子を盗み見ても、量子力学的に光子の状態が変化するため、盗聴の判別ができる。こうした盗聴の検知と防止により安全な暗号鍵だけを共有するのである。

一方、ワンタイムパッドによる暗号化通信では、量子鍵配送によって安全性を保証された暗号鍵を使用し、1 回ごとに破棄する。

NEC が開発を手がける 2 つの量子鍵配送方式

前述したとおり、NEC は BB84 方式(光子検出)と CV-QKD 方式(光波検出)、2 つの量子鍵配送方式の開発を推進してきた（図 3)。

量子力学・情報理論に基づいた絶対安全性が証明されている BB84 方式は、NEC 独自の PLC 干渉計技術の採用、長年にわたる安定化技術への取り組みによって、各種実証実験（生体情報や電子カルテ情報、大容量金融取引データ、設計情報などの秘匿）に成功しており、2024 年 3 月現在、事業化を推進中。ラック搭載（2U/4U）装置、専用の光ファイバが必要な方式で高コストとなることから、通信の早期保護が必要とされる状況への順次適用が予定されている。

既存の光通信用ファイバを共用可能で、小型・低コスト化が期待される CV-QKD 方式は、学習院大学とともに研究開発を行っており、試作機開発に向けて、リアルタイム CV-QKD の実装・安全性の確立が当面の課題となっている。

次なる課題は、光通信領域で培ったデジタルコヒーレントトランシーバの小型化技術を踏襲した超小型低コストの CV-QKD モジュールの実現。CV-QKD モジュールが劇的に小型化され、既存のサーバなどネットワーク機器への搭載が可能になれば、量子鍵配送で共有された暗号鍵はエンドツーエンドで利用可能になり、企業の重要情報、医療・金融取引、公共サービスの情報保護が広く行えるのである。

NTT が主導する IOWN security での取り組み

NEC の量子暗号技術は、NTT が主導する IOWN 構想にも寄与している。セキュリティ対策全般に取り組む IOWN Global Forum のタスクフォース IOWN security における情報通信の暗号化に特化した議論は、2023 年 3 月のリリース 1 ドキュメントで公開された。

このドキュメントには、暗号鍵を交換する手段の一つとして量子鍵配送方式も記載されたが、量子鍵配送用の光ファイバは、IOWN 構想の APN（All Photonics Network）の外部にあるため、QKD over APN に向けて他のタスクフォースと連携議論を推進している。

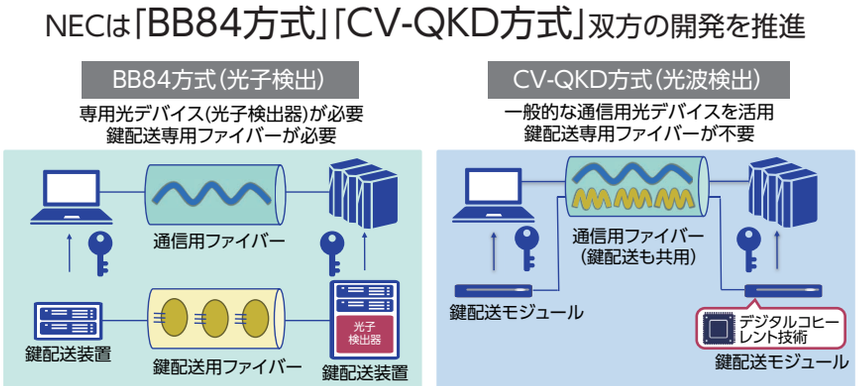

図３　量子鍵配送を実現する２つの方式