50 盗聴不可能な通信は可能？

現在，多くの人にとってインターネットは日々の生活になくてはならないものとなっている．利用者は政府機関や企業といった大きな組織から個人まで多岐にわたっており，情報通信における安全性（盗聴や改ざんを防ぐこと）は非常に重要である．さらに，今後はゲノム情報など，長期間秘匿性を保つ必要のある情報のやりとりも行われるようになると考えられる．しかし，現在広く用いられている公開鍵暗号の安全性は，解読に膨大な計算時間が必要であるという事情に頼っている．そのため将来，アルゴリズムや量子コンピュータの進歩によって，現状のコンピュータでは何年もかかる暗号解読も，一瞬で行えるようになる可能性がある．

そこで，未来永劫にわたって秘匿性が保障できる通信方法の開発が盛んに行われている．それが量子暗号である．量子暗号は，量子力学の基本法則に基づいて，第三者の知らない秘密鍵を，情報の送信者と受信者が共有する技術である（量子鍵配送）．これは，量子力学的な観測の理論を，協力し合う送受信者と，彼らに敵対する盗聴者という関係性に適用したものである．このとき，盗聴者の観測によって生ずる情報の運び役である光子などの状態変化を，盗聴者が知ることができる情報量の上限を決定するのに用いることができる．すなわち，受信者が受け取る量子状態の変化を監視することにより，盗聴を検知することができる．そして，理論的に見積もった盗聴者の知りうる情報量の上限をもとに，送受信者が共有しているビット列を短縮（秘匿性増幅）して生成した秘密鍵は，盗聴が不可能である．

量子暗号装置はすでに市販品もあり，日本でも東京都心と小金井市間を結ぶ光ファイバー網などで量子暗号通信を行う「東京 QKD ネットワーク」（QKD: Quantum Key Distribution）が試験運用されている．普及のために標準化やコスト低減などの努力が払われている一方で，基礎的な研究でも，ベルの不等式を利用して装置の不完全性を補う方法，もともと盗聴できない暗号方式，長距離化のための量子中継技術など，さまざまな研究が活発に行われている．

会誌編集委員会