量子暗号と量子鍵配送ネットワーク

いかなる計算機でも解読不可能な暗号技術の社会展開を目指して

武岡 正裕
（たけおか まさひろ）
未来ICT研究所 研究統括
大学院博士課程修了後、2001年に独立行政法人通信総合研究所（現、NICT）に入所。以来、量子光学、量子情報理論、量子暗号に関わる研究に従事。2021年4月より慶應義塾大学理工学部電気情報工学科教授 兼 NICT未来ICT研究所研究統括。博士（工学）。

現在の情報社会を支える現代暗号は、近年急速に開発が進められている量子コンピュータの高性能化などにより解読されてしまう恐れがあります。これに対して、量子暗号は、将来の大規模量子コンピュータを含むあらゆる計算機を使っても解読不可能なことが数学的に証明されている現状唯一の暗号方式です。ここでは、量子暗号の核となる技術である量子鍵配送ネットワークの研究開発や実用化に向けた取組と将来展望について紹介します。

■現代のネット社会を支える暗号技術とその課題

現在社会に普及している暗号は、解読に膨大な計算量を必要とする「計算量的安全性」により秘匿性が担保されており、そのおかげで我々は日々安全にデータをやり取りすることができています。しかし現代暗号は、将来の大規模な量子コンピュータや全く新規の計算技術・数理アルゴリズムの出現により、解読が容易になってしまうという潜在的脅威も指摘されています。特に数十年以上の長期秘匿性が要求される重要情報は、今は解読できなくてもひとまず暗号化データを盗聴・入手し、将来新しい計算技術を確立してから解読する、いわゆる「harvest now, decrypt later」攻撃を仕掛けることが可能性であり、今すぐにも対策が必要な状況です。

これに対し２種類の新技術の開発が進んでいます。一つは耐量子計算機暗号と呼ばれるもので、計算量的安全性には変わりありませんが、現在知られている量子計算アルゴリズムでは解読が困難と考えられている数理構造を利用した暗号で、その実用化や標準化が進みつつあります。もう一つが、ここで紹介する量子暗号です。量子暗号は、将来どのような計算技術が出現しようとも、いかなる計算機でも原理的に解読が不可能な安全性（情報理論的安全性）を証明できる現状唯一の暗号方式です。

■量子暗号と量子鍵配送（QKD）ネットワーク

量子暗号は、図１に示すように、量子鍵配送（Quantum Key Distribution: QKD）とワンタイムパッド（One Time Pad: OTP）暗号化という２つのステップから構成されます。QKDは、光の量子である光子を使って、第三者には秘密の暗号鍵を送受信者間で共有する技術です。OTP暗号化はデータと同じサイズの暗号鍵を使って暗号化し、一度使った鍵は二度と使いまわさないという暗号化で、ここにQKDから供給された暗号鍵を使うことで、情報理論的安全性を達成します。なお、OTP暗号化と暗号化データの送受信は全て普通のコンピュータや通信回線で行われ、QKDの部分のみ、量子的な技術が必要になります。

このQKD送受信機をネットワーク接続し、安全かつ効率的に鍵を管理・配送する技術が量子鍵配送ネットワーク（QKDネットワーク）です（図2）。QKDネットワークでネットワーク上の任意の地点での暗号鍵の共有を行い、これを従来のネットワークに提供することで、情報理論的に安全な暗号鍵を使った新たなセキュリティサービスが可能になります。光ファイバーで接続されたQKDネットワークのほか、衛星通信によるQKDも開発が進んでおり、将来的にはこれらが統合されたグローバルなQKDネットワークに発展するものと期待されます。

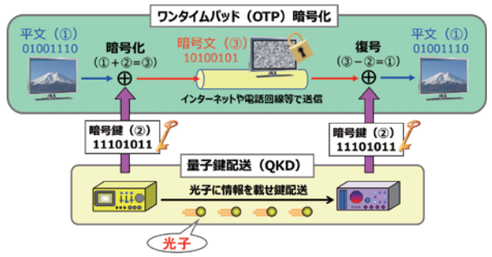

図1　量子暗号のしくみ

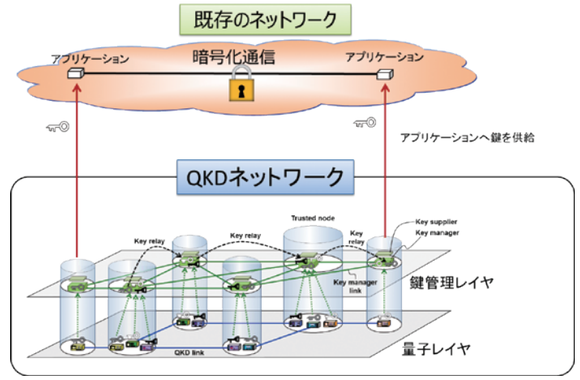

図2　量子鍵配送（QKD）ネットワークからの鍵供給

■研究開発や実用化に向けた取組

NICTでは大学・企業と連携し、2000年代からQKD装置の技術開発やQKDネットワークの制御・管理技術の開発、そしてこれらの実証実験を進めてきました。2010年に産学官連携で構築したテストベッド「東京QKDネットワーク」は、世界最長期間の運用実績を有しており、今も様々な原理実証・社会実証実験が行われています。実用化についても、QKD装置自体は日欧中などの企業において既に製品化されており、またQKDネットワークによるサービスも、世界各国の通信事業者やスタートアップ企業などが事業化に向けて次々と動き出しています。

また、QKDネットワーク技術のグローバルな普及には、国際標準化も重要です。NICTでは、政府や企業・大学と連携し、国際電気通信連合電気通信標準化部門（ITU-T）や国際標準化機構・国際電気標準会議第一合同技術委員会（ISO/IEC SC1）、欧州電気通信標準化機構（ETSI）などにおいて国際標準化を積極的に推進しています。特にITU-Tでは、QKDネットワーク概要に関する国際標準勧告を始め、多数の勧告の開発・発刊に、日本が主導的に関わっています。

■QKDネットワークの活用と今後の展望：量子セキュアクラウド技術

量子暗号の高い秘匿性を社会で最大限生かすためには、通信システムやセキュリティ技術全体を俯瞰（ふかん）し、応用技術を開発する必要があります。そのような技術の一つが、NICTが産学連携し開発を進めている量子セキュアクラウド技術です。これは、量子暗号、秘密分散、耐量子公開鍵暗号による認証基盤、秘匿計算等を融合することにより、どんな計算機でも解読や改ざんのできないデータバックアップ保管と計算処理を実現する技術です（図３）。データを複数のサーバに分割・暗号化して保管することにより、一部のサーバの情報が漏えいしても元データの復元が不可能な情報理論的な秘匿性と、一部のサーバの情報が消失しても残りの情報から元データが復元できる可用性を同時に実現できます。これは日本独自の技術であり、NICTと企業等により、医療を始め様々な分野で重要データの保管に活用するための実証実験を進めています。このように、QKDネットワークを各種の現代セキュリティ技術と適切に融合することで、ネットワーク社会の新しいセキュリティ基盤が切り拓（ひら）かれていくものと期待されます。NICT量子ネットワークホワイトペーパーでは、技術の仕組みや要求条件から社会展開の展望まで、より詳細な説明がなされています。

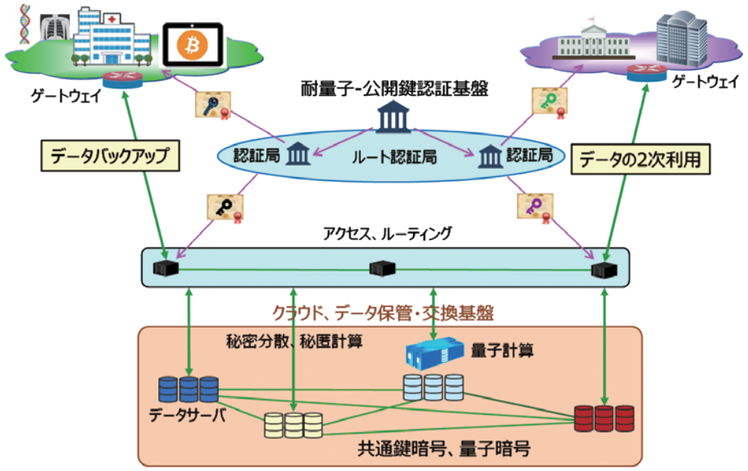

図3　量子セキュアクラウド技術