

## BT、東芝欧州研究所、ADVA社は、国立物理研究所NPLと暗号化技術の「飛躍」を探る

東芝欧州研究所、BT、ADVAオプティカルネットワーキング社と、英国の国家計量標準機関である国立物理研究所（NPL）は、本日（4月24日）、ライブで「光った」ファイバネットワーク上の量子鍵配送（QKD）技術の実験の最初の成功を発表した。本実験は、より高いレベルのネットワークセキュリティを提供するデータ暗号化技術の次なる未開拓地であるQKDに、更に高度な研究の道を開くものである。

銀行やクレジットカード会社がネットワーク間でのデータ暗号化の「鍵」を使用する標準的な方法よりも上の追加的なセキュリティのレイヤを提供することで、量子力学を使って完全に安全に作られた2人の利用者間の鍵をQKDが共有する。

量子状態で情報を送信することにより、鍵を傍受しようとしても、その傍受が異常となって検出できるため、識別することができる。このようなことが起こると、「取引」を中止することができ、新しい鍵が自動的に送信される。マルチな量子鍵を每秒每秒送信することにより、ファイバ回線のセキュリティを常に監視することができ、信号を「傍受」する試みは、瞬時に識別することができる。

英国のイノベーション機関である技術戦略委員会の支援を受けているこの実験は、1本の「光った」ファイバ、すなわち、データと量子鍵自体を送信するファイバを用いる初めての例である。量子「鍵」と暗号化されたデータの両方が、今回、初めて同じ経路を使用できるので、1本のファイバの使用は重要である。以前は、安全な接続を提供するため2本又は3本のファイバが必要であった。

この実験は、実用的なセキュリティアプリケーション技術への更なる研究の道を開く。この実験は、東芝が開発した量子装置を用い、NPLの量子検出グループが測定・評価し、アダストラルパークというサフォーク（注：ケンブリッジの東側）にあるBTの技術研究拠点とイプスウィッチにある別のBTの拠点との間というライブのBTのファイバリンク上で、ADVAオプティカルネットワーキング社の暗号化装置と連携して実施された。

ケンブリッジにある東芝欧州研究所のアンドリュー・シールズは、このようにコメントした。「光ったファイバ上のQKDの最初のフィールド実験が技術の重要な進歩を示す。非常に弱い量子信号からノイズを除去する技術を用いて、地中に設置された光ファイバ上でQKDが動作し、従来のデータ信号を伝送できることを我々は示してきた。これは、多くの場合に利用できないか又は手が出ないほど高価である追加の「ダークファイバ」を必要とすることなくQKDが実現できることを意味する。」

NPLのアラステア・シンクレアはこう述べた。「QKDシステムは、光ファイバ全体のパルスで、光子として知られている単一の光の粒子を送信することにより動作する。送受信された光子の数を知らなければならないことは、このシステムのセキュリティに不可欠である。NPLでは、顧客の信頼を向上させ、市場化の主要な障壁の一つを克服するために、システムのセキュリティを独自に検証するために我々が使用している、光の個々の粒子を検出するのに十分敏感な一連の測定器を開発した。」

BTの研究・イノベーション部長のティム・ウィットレイ博士はこう述べた。「量子鍵配送は、セキュリティ技術のわくわくする新規領域である。東芝、ADVA光ネットワーク社及びNPLとの協力を通じて、現在可能なものの限界を突き破り、将来より広く使用されるこの技術の新たな可能性を開くことを、我々は支援している。」

「重要な（ミッションクリティカルな）データの統合性とセキュリティは非常に重要なので、これまで公開されたことはない」と、ADVAオプティカルネットワーク社のイェルク・ピーター・エルバース先端技術担当副社長はコメントした。「企業は、その評判に対するリスクを強く認識しており、ビジネスにおいて自社のデータ保護におけるあらゆる弱点を発見する必要がある。スループットやレイテンシーに一切の妥協をすることなく、暗号化されたサイト間の接続性が鍵である。このQKDの実験は、ネットワークセキュリティをより一層レベルアップさせる実用的なソリューションを構築するための重要な足がかりである。」

（各機関の概要は省略）

（BTプレスリリース 2014年4月24日）