量子鍵配送を用いたネットワークスイッチの安全性強化

ーネットワークセキュリティへの貢献を目指してー

藤原 幹生（ふじわら みきお）
未来ICT研究所 量子ICT研究室 主任研究員

大学院修士課程修了後、1992年、郵政省通信総合研究所（現NICT）に入所。衛星搭載用遠赤外検出器、光子数識別器、極低温エレクトロニクスの研究に従事。博士（理学）。

はじめに

現代の暗号技術は文章の秘匿化のみならず、認証や署名等にも利用され、インターネットサービスには欠かせないものとなっています。NICTが開発を進めている量子鍵配送は暗号の機能のなかで文章の秘匿化を未来永劫破られない方法で行うための手段として日々改良が進められています。

量子鍵配送では送信者が光子を変調（情報を付加）して伝送します。変調を施された光子レベルの信号は測定操作をすると必ずその痕跡が残り、また単一の光子の状態を変化させずにコピーすることも不可能です。これらの原理を利用して盗聴を見破り、情報理論的に安全な乱数を送信者と受信者で共有することが可能となります。この鍵と送信情報のデジタルデータを、それと同じ長さの共通鍵（0と1のランダムなビット列）と排他的論理和をとることで暗号化し、復号はその逆過程を行うというVernam's one time padという暗号方式を用いることにより完全秘匿通信を実現します。量子鍵配送システムにおける情報の担い手は単一の光子であるため、伝送速度はファイバ内での光子の減衰や、単一光子検出の性能で律速され、NICT内にある世界最高レベルの量子鍵配送装置ですら伝送距離・速度は敷設ファイバでは50kmで数百kbpsであり、現在の光通信の速度と比較すると非常に遅いものでした。

この乱数共有速度が通信速度と同じなのですから、完全秘匿通信がいかに難しいかが判ります。この遅い装置に文章の完全秘匿化以外の機能は無いのか？量子鍵配送装置が有する先端的ハードウェアを他のセキュリティ技術に応用できないか？ということが動機となり、量子ICT研究室、セキュリティ基盤研究室、情報システム室と連携し、検討が進められてきました。今回ご紹介するのは量子鍵配送装置で生成される良質な乱数をネットワークスイッチに供給し、AES（Advanced Encryption Standard）などの共通鍵暗号の鍵として利用したり、認証に用いたりするものです。

量子鍵配送システムで生成された鍵を利用するネットワークスイッチ

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参照モデルを用いれば、量子鍵配送は通信装置そのものなので、第1層の物理層に分類されます。今回は第2層のデータリンク層と第3層であるネットワーク層でのスイッチに鍵供給する例をご紹介します。第2層、第3層のデータリンク層とネットワーク層での中継器はそれぞれLayer 2 スイッチ、Layer 3スイッチと呼ばれています。Layer 2スイッチではスイッチに繋がっている通信装置の持つMAC（Media Access Control）アドレスを宛先情報として中継を行います。Layer 3スイッチではIPアドレスを利用して経路制御やルーティングを行います。

新たに開発したLayer 2スイッチでは、量子鍵配送システムから乱数が供給され、Layer 2スイッチと各端末で認証後にその乱数を共有します。共有した乱数を用いて各端末ではMACアドレスをパケット毎に暗号化します。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て、端末が偽証していない、すなわち、なりすまし行為がされていないことを確認し、認証後要求されたパケットを繋ぎます。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らない情報ですので、なりすますことが不可能です。Layer 2内でのなりすましによるデータの不正取得が今年3月に報道されましたが、我々が開発したスイッチを用いればその不正アクセスを防ぐことが可能であったと考えられます（図1）。

Layer 3スイッチでは、IPパケット単位でデータの改ざん防止や秘匿機能を提供するプロトコルIPsec内の暗号化技術に量子鍵配送で共有した鍵を使用します。暗号プロトコルで使用する共通鍵に量子鍵配送で生成した鍵を使用し、短時間で、もしくはパケット毎に鍵を変える（一度使用した鍵は二度と使わない）ことで安全性を大幅に向上させることが可能になり、また、鍵の消費量に対し、多量のデータを伝送することも可能になります。通常のIPsec内で使用されている公開鍵暗号での共通鍵の生成に比べ遥かに高速化ができるため、従来よりも高速・安全な

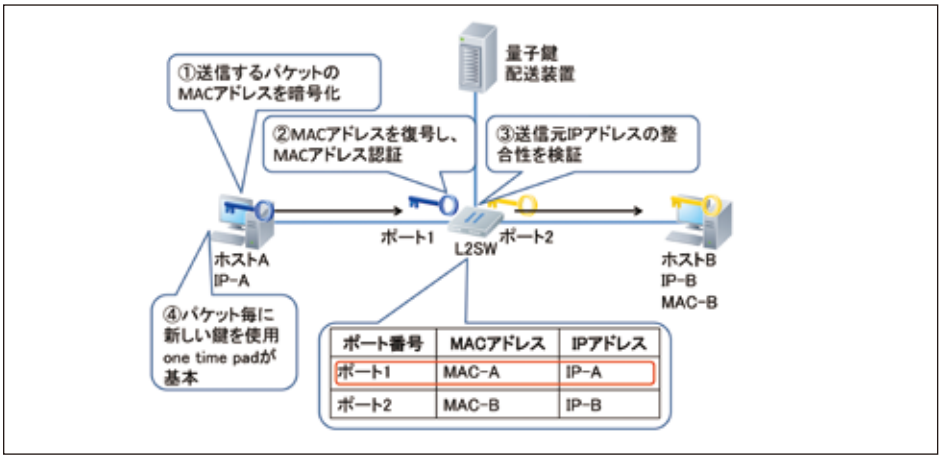

図1●Layer 2スイッチに鍵を供給することによる認証機能の概要

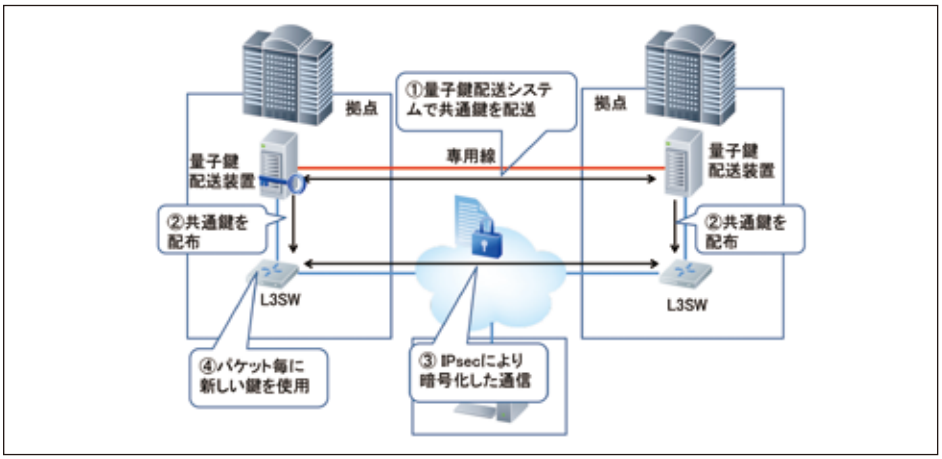

図2●Layer 3 スイッチに量子鍵配送装置より鍵を供給することによるIPsecの安全性の向上

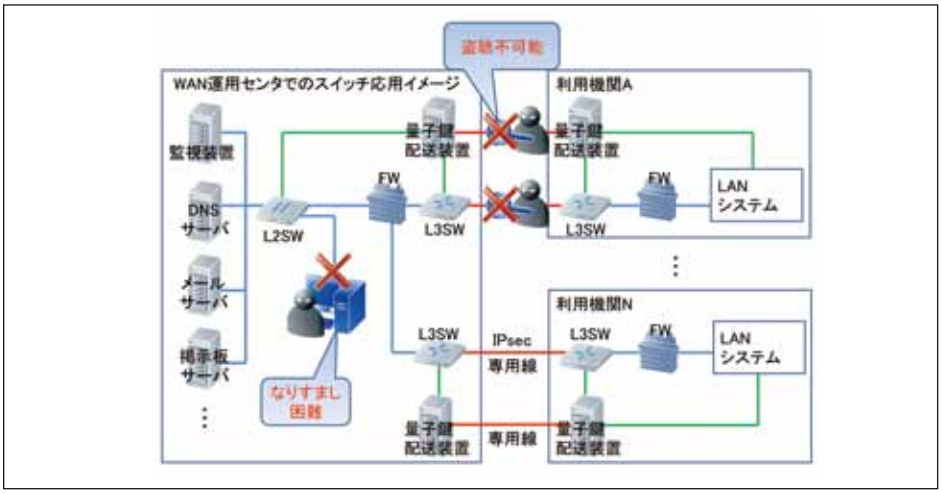

図3●セキュリティ強化されたネットワークスイッチの運用イメージ

システムとなることが期待されますが、安全性向上の定量的評価は今後の理論研究を進めていく必要があります（図2、3）。

まとめ

量子鍵配送を実現させる物理は通信や物理の根幹である公理に基づいており、多くの研究者を魅了して止まない研究テーマです。しかし、現在のところ通信の機能として一般に提供できるものは二者間で秘密裏に乱数を共有するということだけです。この今までに無かった乱数共有技術を支える基礎研究を進めつつ、この乱数共有で日常生活にどのような貢献ができるかも考え、開発を進めています。

ネットワークを通しての「情報漏洩」が国家及び国民の脅威となり、その対策が轍鮒の急となった今でも不正アクセスを防ぐ最大の防壁はシステムエンジニアによる丹念なチェックです。今回、我々が開発したスイッチは当然それだけで安全性が担保されるものではありませんが、将来のネットワークスイッチに応用され、人の手によるチェックの手間をわずかでも軽減できることを期待して止みません。