ITU-T Recommendation Y.3800 量子鍵配送をサポートするネットワーク概要

国立研究開発法人情報通信研究機構　イノベーション推進部門 参事　釼吉（けんよし）　薫（かおる）

1. はじめに

2019年10月14日～25日ジュネーブにて開催されたSG13会合にて、勧告ITU-TY.3800 Overview on Networks supporting Quantum Key Distribution（量子鍵配送をサポートするネットワーク概要）が承認された。本稿では、Y.3800の内容と承認に至る経緯について紹介する。

Y.3800は、量子鍵配送ネットワークの概要、基本構成、基本機能などを規定する勧告で、量子鍵配送ネットワークの基本勧告として初のITU-T勧告となる。我が国では、NICT、NEC、東芝等が中心となり、世界最高性能のQKD装置を開発するとともに、2010年に構築した実証テストベッド「Tokyo QKD Network」上でネットワーク技術の開発、長期運用試験、様々なセキュリティアプリケーションの開発に取り組んできた。NICT、NEC、東芝の三者は、これらの成果をQKDネットワークの基本構成と機能、サービス手順などに関する勧告草案としてまとめ、2018年9月以後勧告の完成まで、寄書活動、中間会合のホスト、エディタを担当し、Y.3800の完成に大きく貢献した。完成したY.3800は、日本のQKDネットワーク技術が勧告の骨格を形成する形となっている。

2. Y.3800概要

2.1　イントロダクション

Quantum Key Distribution（QKD）技術は、対称ランダムビットストリングを安全な鍵として配送する手段を提供し、証明されたセキュリティモデルをサポートするいくつかの前提条件の下で、無制限な計算資源を持つ盗聴者に対しても安全であることが証明されている。AI、量子計算などのコンピューティング技術が急速に進歩するにつれ、QKD技術は重要なデータの伝送の安全性を確保するために重要であると期待されている。

QKDは、通信ネットワークへアドオンする技術とサービスである。QKDネットワーク（QKDN）は、QKDの到達可能性と可用性を拡張するための技術である。QKDNを現在の通信網と暗号インフラに導入することで、QKD技術が持つ独自の特徴と制限により、ネットワークアーキテクチャと考慮すべきセキュリティの設計に新たな課題が生じる。例えば、QKDは特定の物理チャネル、すなわち基本的にポイントツーポイントリンク技術である量子チャネルを必要とする。QKDによって生成された鍵は、様々なネットワークセキュリティの脅威を考慮し、ネットワーク内で適切に管理され、中継されなければならない。

そのため、ネットワークにおけるQKD技術の利用に関する標準を確立する必要がある。この勧告は、基本的なQKDNの概念的構造と明確なセキュリティ境界の概要を提供する。これは、ネットワークアーキテクチャ、ネットワークセキュリティなど、様々なQKDN勧告シリーズの最初の勧告である。要求条件は、更なる検討を必要とする。QKDと関連技術は急速に進歩しているため、将来的には新しい技術や概念構造が出現する可能性がある。この勧告は、技術と標準化の将来の進展を考慮し改訂される。

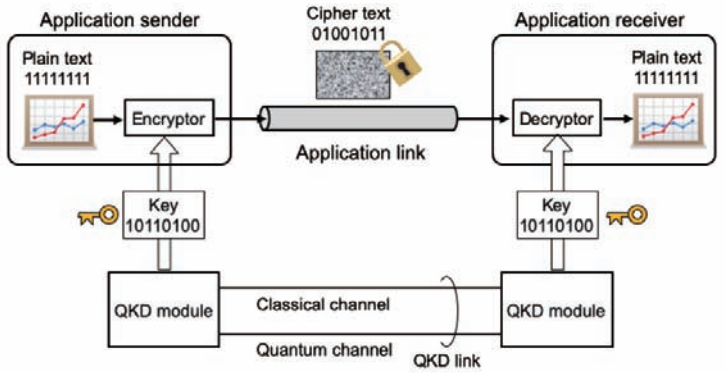
2.2　スコープ

勧告Y.3800は、QKD（Quantum Key Distribution）をサポートするネットワークの概要を規定し、QKD技術を実装するためのネットワークアスペクトに対応する。この勧告は、以下の内容について記述している。

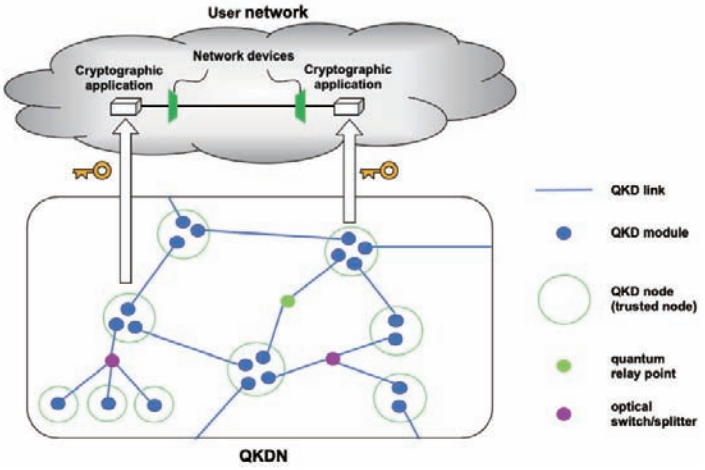
- QKD技術の概要
- QKD技術をサポートするネットワーク能力
- QKDネットワークの概念的構造と基本機能

2.3　QKDの基本構成

図1は、QKDの基本要素を示している。モジュールと呼ばれる送信機（QKD-Tx）と受信機（QKD-Rx）間を量子チャネルで接続し、量子信号の送受信を行う。量子信号の送受信と、その後の鍵生成手順によりQKDモジュールは鍵（ランダムビットストリング）を生成し、暗号アプリケーションに供給する。QKDモジュールより供給された鍵を用いて、暗号化アプリケーションはデータの暗号化を行う。暗号化データが送信されるアプリケーションリンクは、従来のネットワークまたは将来のネットワークにおける任意の通信リンクである。QKDモジュールから生成される鍵を用いてOTP（One time pad）等の適切な暗号化を行った通信は、量子の法則と量子理論によって情報理論的安全性（ITセキュリティ）であることが証明されている。



■図1. P-to-Pアプリケーションリンクを保護するQKDの構成例



■図2. QKDNとユーザネットワークとの関係に関する一般的な概念と技術

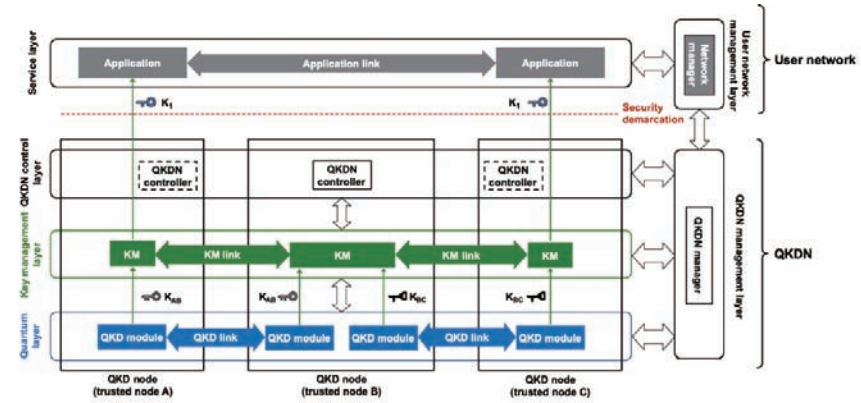
2.4 QKDNとユーザネットワーク

QKDモジュールは、P-to-P QKDリンクによって接続された2つのノード間で鍵を共有する。QKDリンクでは、微弱な量子信号を送受信するため、送信できる距離に制限がある。QKDリンクを拡張する技術として、いくつかの技術的可能性がある。中継ノードとして量子リピータが研究されているが、現時点では実用的ではない。Y.3800では最も実用的な方法として、トラステッドノードをネットワークで接続し、鍵の中継を行う方式（トラステッドリレー）について記述している。Y.3800では、2つ以上のトラステッドノードとノード間を接続するQKDリンクから構成されるネットワークをQKDN、QKDNによって供給される鍵を消費するネットワークをユーザネットワークと定義している。暗号化アプリケーションは、通常ユーザネットワークに含まれる。（図2）

2.5 QKDNの概念的構造

図3は、QKDNのハイレベルな構造を示している。QKDNは4つのレイヤ、ユーザネットワークは2つのレイヤから構成される。各QKDノードには、QKDモジュールと鍵マネージャ（KM）が存在する。QKDモジュールはQKDリンクによって接続され、KMは、KMリンクにより接続される。QKDモジュールから生成された鍵は、KMによってQKDノード間のリレーを行う。QKDNコントローラは、QKDモジュール、QKDリンク、KM及びKMリンクの制御と鍵リレールートの制御を行う。QKDNとユーザネットワーク間にはセキュリティ分界点を定義している。これにより、供給される鍵に関するQKDNの責任と、鍵を使用するユーザネットワークの責任の境界が定義される。

図3は、ノードAからノードCへの鍵リレーの動作を表している。ノードAとノードB間で生成された鍵ABは、ノードBとノードC間で生成された鍵BCによってノードBで暗号化され、ノードCへリレーされる。ノードCへリレーされた鍵ABは、ノードAとノードCより各々鍵1として、ユーザネットワークの暗号化アプリケーションに供給される。



■図3. QKDN、ユーザネットワーク及びセキュリティ境界のハイレベルな構造図

3. Y.3800開発の経緯

2018年7月SG13会合（7/16−27、ジュネーブ）にて、KTよりQKDNのフレームワークを検討する新勧告草案を提案する寄書（C509）が提出された。この提案は、KT、KAIST、RURA、Tunisie Telecom、SKT、NTTがサポートメンバとなり、承認され勧告草案の開発が始まった。

2018年10−11月SG13WP会合（10/22−11/2、ジュネーブ）に、NICT、NEC、東芝の共同提案寄書を提出し、日本におけるTokyo QKD Networkの研究成果をベースとして、①QKDネットワークのGeneral structure、②QKDネットワークのBasic function、③Reference model等の提案を行った。提案内容はおおむね合意され、ベーステキストに反映された。この会合で日本からの提案の骨格がドラフトに採用され、その後NICTがメインエディタを担当している。

その後、2019年1月Q16/13中間会合（1/10−11、ソウル）、2019年3月SG13会合（3/4−15、ジンバブエ）でドラフトを更新し、NICTがホストした2019年5月Q16/13中間会合（5/14−16、NICT）会合では、筆者：釼吉（NICT）がActing Rapporteurとして議事を進行した。会議には計14件の寄書が提出され、活発に議論を行われ、Consentに向けた最終案を作成した。

2019年6月SG13 WP会合（6/17−28、ジュネーブ）にて、NICTよりConsentを提案した。SG13 Closing plenaryでは、米国、英国、カナダより慎重にレビューする時間が必要との理由により、Consentを次会合へ延期すべきとの発言があったが、賛成多数でConsentは承認された。

AAP LC comment期間中に、米国、英国、カナダ、Orange、QuantumCTekから合計124件のAAP LC（Last Call）commentが提出された。NICTは、エディタとしてこれらのコメントに対するResolution案を作成し、これらコメント提出者と電話会議により調整を行っている。AR（Additional Review）では、Orangeより再度コメントが提出されたため、これらのコメントを考慮した改版ドラフトを作成し、10月SG13会合で承認を求めることとなった。

2019年10月SG13会合（10/14−25、Geneva）では、米国、英国、カナダより改版ドラフトに反対する意見が出たため、SG13議長、Q16/13ラポータとエディタ（筆者）の3名で、Closing plenary前夜に集まり、最終コンプロマイズ案（議長仲裁案）として、勧告名をFrameworkからOverviewに、本文中のRequirementsをCapabilitiesに変更することを主とする修正案を作成し、Closing plenaryに臨んだ。Closing plenaryでは、米国、英国、カナダが改版ドラフトに反対する立場を変えなかったため、SG13議長よりコーヒーブレークを宣言し、SG13議長、ラポータ、エディタ、米国、英国、カナダのHoDによるオフラインの議論が行われた。オフライン議論では、SG13議長より議長仲裁案が提示され、その後のSG13プレナリでは大きな反対無く承認された。

4. おわりに

QKDの技術と実装は各国で積極的に進められている。我が国においては、政府による量子技術イノベーション戦略の策定が行われ、一般社団法人量子ICTフォーラムが発足した。ベンダーによる量子装置の開発が進み、防衛省や警察庁による量子暗号の導入が計画されている。QKDネットワークの本格的普及に向けて、ITU-TにおけるY.3800の制定は大きな意義を持つ。現在ITU-T SG13とSG17では、Y.3800に続いてQKDNアーキテクチャ、要求条件、鍵管理、セキュリティ概要等の勧告制定が予定している。NICTはこれら重要勧告のエディタを担当しており、今回制定したY.3800をベースに、引き続き主導的な役割を果たして行く。本稿で概要を紹介したY.3800は、近日TTCより国内標準として制定する予定である。