テクノトレンド TECHNO TREND

将来の量子暗号ネットワーク（SD-QKDN）の実現に向けて

日本電気株式会社 研究＆事業開発戦略統括部シニアプロフェッショナル 中田 圭

はじめに

世界各国でDV-QKD（BB84）方式を中心として活用する量子暗号ネットワーク技術の研究開発が進み、欧州、中国、韓国、日本などでテストベッドが構築されてきた。日本では2000年頃から研究が行われてきた。これらはGeneration.1として、量子鍵配送（QKD）と鍵管理の実装可能性を示し、金融・医療・行政などへの適用検討を前進させた点で意義が大きい。

しかし近年、安全保障領域のみならず官民横断でAI・データ活用が加速し、顔認証・ゲノム等の個人データやガバメントデータに対する「長期かつ日常的な機密性」への要求が増している。更に防衛領域では、AI搭載の無人機・無人システム群、サイバー・フィジカル空間（CPS）の融合、クラウド／エッジ統合、データ中心の意思決定高速化が前提となり、通信や情報をより高度な暗号で保護するために「暗号鍵を継続的に補給し、状況に応じて供給経路・供給条件・暗号方式を切り替える能力」が必要と考える。

従って将来の量子暗号ネットワークは、①クラウドやエッジ環境で動作するAIファーストな無人環境・自律的な環境変化への追従 ②官民デュアルユース（平時の利用拡大と有事の優先度制御の両立）③クリプトアジリティ（PQC／QKD／既存暗号等の各方式を状況に応じて切り替え）を、運用や安全性を自律的に維持できるプラットフォームとして実現する必要がある。本稿では将来動向に適合できる将来（Generation.2）の量子暗号ネットワークとして、Software Defined QKDN（SD-QKDN）として定義する。加えて安全保障領域における高コスト効率での大規模展開・利活用をふまえ、CV-QKDを主力手段として位置付けて有効活用する（**図１**）とともに、DV-QKDと比較して不足する安全性を補えるセキュリティ機能を含めることとする。

本稿では、安全保障の観点を中心に、デュアルユース利用可能な量子暗号ネットワーク実現におけるGeneration.1の課題を示し、Generation.2に向けた技術課題候補を提示する。なお検討にあたり「防衛技術指針2023」の二つの技術獲得アプローチへの整合を考慮した（**図２**）。Generation.1は既存技術の成熟・活用（図２左矢印）として民間への活用と位置付ける。一方Generation.2は、５～10年以内の革新的な能力創出（図２右矢印）の早期実用化に位置付け、必要な基礎研究から各種研究を高速に進め実用化を目指す。

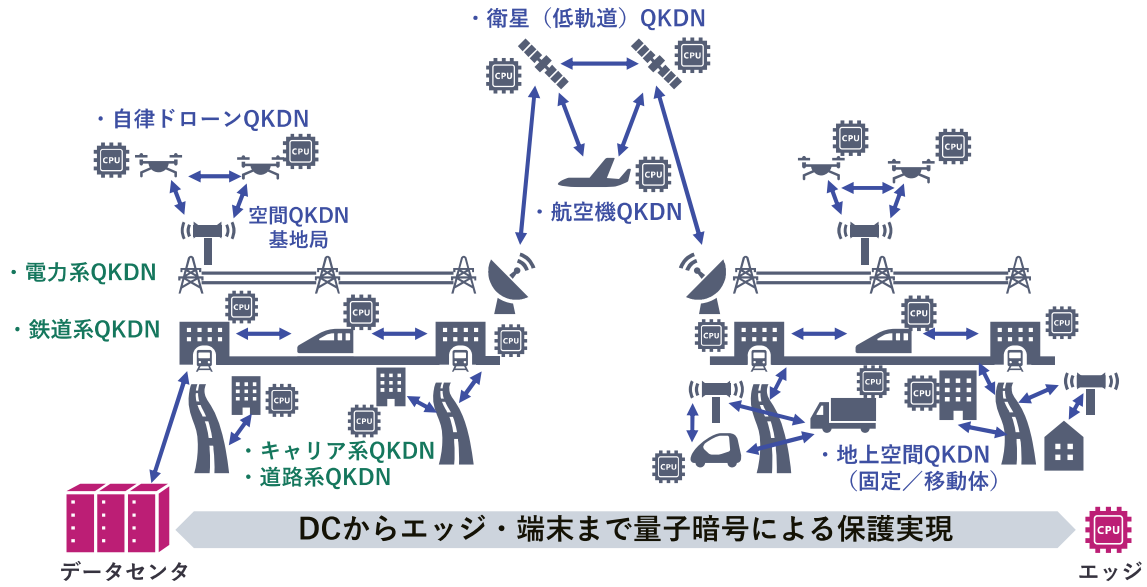

図１　小型・低コスト CV-QKD の有効活用により実現しうる QKD ネットワーク群の一例

表１　Generation.1の課題と Generation.2での方針案

Generation.1課題	課題の概要	Generation.2対応案	
課題１ 人間中心・固定構成アーキテクチャの限界	人間が介在しない AI、CPS（サイバー・フィジカル）、無人防衛、クラウド環境等の移動前提の環境で仕様が困難。	将来を見据えた、AI、CPS、クラウド、無人防衛等を優先としたアーキテクチャに刷新し、必要な機能を実現。	Software Defined QKDNとして実現
課題２ 回線利用コスト構造	DV-QKD はダークファイバ利用効率に課題あり。事業者の事業機会喪失等の高リスク事項あり、コスト低減が困難。	ファイバ所有者の負担を低減可能な、DWDM 上で展開できる CV-QKD を中心とした技術実現により、広域・多数展開を実現。	
課題３ 固定モデル前提の安全性	特定モデルでの完全な安全性を長期にわたり検証・保証を実現。一方、例外的な状況は対象外。例外的な状況下でも活動が必要な防衛領域において、今後は特に人知が追い付かない AI を悪用した高度なサイバー攻撃からの安全性への影響は見通せない。	防衛環境の特性を前提に、例外的状況や無人・移動環境への柔軟な対応を実現。完全安全性を前提とせず、QKD を含むシステムに脆弱性がある前提として、防御 AI 等も活用し攻撃者に先んじて迅速に弱点を発見し対処する能力を実現。	

１．Generation.1の到達点と、将来要求とのギャップ

Generation.1は、固定設置の疎結合アーキテクチャをベースとし、QKD のネットワーク化と鍵管理の統合、QKD コントローラ等によるシステム管理による広域化への対応や、安全性検証技術やトラステッドノード技術を用いて実装上や運用中に発生する脆弱性への対応等の各技術の研究開発が進められた。日本では、総務省／NICT 主導による研究開発およびテストベッド実証を通じて日本国内での技術理解・運用知見の蓄積に貢献している。一方で、将来動向に照らしあわせると、主に３点が課題と認識される（表１）。

(1)　課題１：人間中心・固定構成アーキテクチャの限界

Generation.1は、人間が構築・運用・監視する前提で、機能や利用者を固定的な装置に割り当て、システムを構成する前提である。将来の無人・分散環境では、様々な使用条件に基づく上位システムの自律的なノード参加／離脱、媒体（ファイバ／FSO／衛星）の切り替え、クラウド上での機能移動が常に発生することから、量子暗号ネットワーク側の機能も自律的に適合する制御が必要となる。またモザイク戦のよう