TTC標準草案
(Draft TTC Standards)

セキュリティ専門委員会

2021年12月

新規標準の制定について（JT）

- 我が国では、2010年に構築した実証テストベッドTokyo QKD Networkで量子鍵配送(QKD)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いる。2019年10月にはY.3800が、ITU-T初のQKDに関する国際標準として承認された。その後Y.3801、Y.3802、Y.3803、Y.3804、X.1710が承認され、QKDNの基本勧告シリーズが完成している。
- ITU-T 勧告X.1712は、Y.3800が規定するQKDNの基本構成とX.1710が規定するセキュリティフレームワークをベースとして、QKDN鍵管理のセキュリティ要求条件、セキュリティ対策について規定する。ITU-Tでのこれらの国際標準の成立により、QKDを用いた秘匿性の高い暗号通信サービスの実用化と普及が加速すると期待される。
- 国内ではQKDNの商用化に向けたプロジェクトが進んでいる。QKDNの一連の勧告の完成により、関連する量子暗号通信の標準化の検討が加速し、QKD関連の製品開発やサービス創出に向けて企業が投資しやすくなり、ユーザは導入を検討しやすくなると期待される。

QKDN関連 JT標準

- セキュリティ専門委員会は、国内のQKDN製品開発、市場拡大、普及促進のため、以下のQKDN関連のITU-T勧告をベースとするTTC標準の制定を提案する。

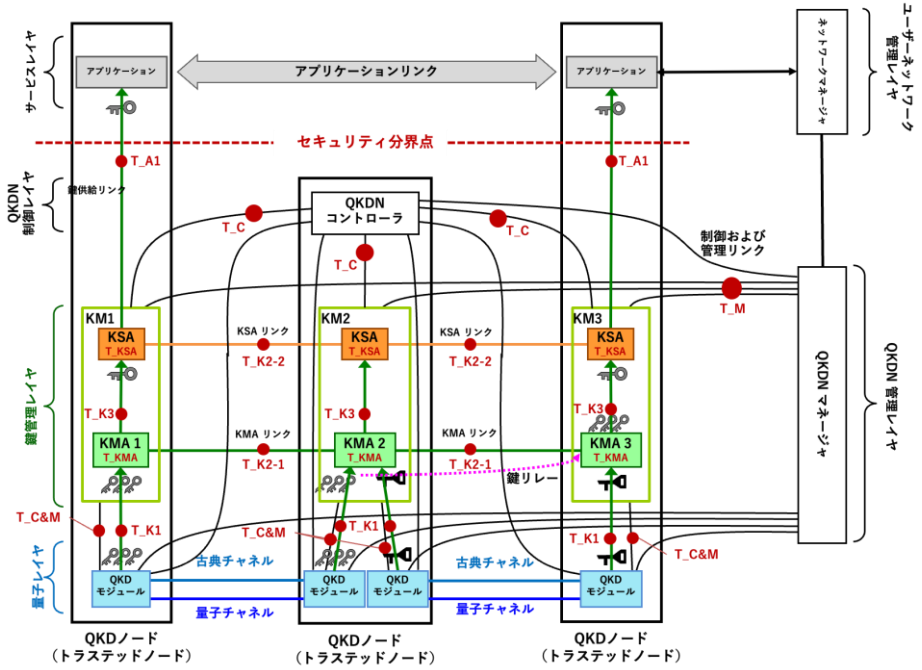
		標準類	版数	タイトル
1	新規	JT-X1712	1	量子鍵配送ネットワークのセキュリティ要求条件と対策 - 鍵管理

- ITU-T SG17では、X.1710、X.1712に続くQKDN関連勧告の開発が進められている。セキュリティ専門委員会は、引き続きこれらITU-T勧告をベースとしたTTC標準の開発に取り組み、国内標準として提案する予定である。

付録
JT標準のベースとなるITU-T勧告の概要

JT-X1712: 量子鍵配送ネットワークのセキュリティ要求条件と対策 - 鍵管理

QKDN鍵管理に対するセキュリティ脅威、セキュリティ要求条件、セキュリティ要求条件を満たすための鍵管理のセキュリティ対策を規定する。



JT-X1712 図1　QKDNの鍵管理のセキュリティ脅威

表1 - 鍵データに関するセキュリティ要求条件および対策 (抜粋)

	内容	セキュリティ要求条件	セキュリティ対策
(i) 機密性	鍵データに関するすべての情報は、許可されていない要素および関係者への漏洩から保護される。	SReq.1　KMAは、KMAリンク内の鍵データの機密性を確保することを要求される。 SReq.2　KMAは、KMAリンク内の鍵リレーに対してITセキュアな機密性保持手段を使用することが推奨される。 SReq.3　KMAは、QKDモジュールと連携して、KMAとQKDモジュールの間の鍵供給リンクにおける鍵データの機密性を確保することを要求される。 SReq.4　KMA及びKSAは、KMAとKSAとの間の鍵供給リンクにおける鍵データの機密性を保証することを要求される。 SReq.5　KSAは、暗号アプリケーションと連携して、KSAと暗号アプリケーションとの間の鍵供給リンクにおける鍵データの機密性を確保することを要求される。 SReq.6　KMAおよびKSAは、KMAおよびKSAによって処理または格納されるときに、鍵データの機密性を確保することを要求される。	- SReq.1に対して、KMAは、要求される機密性を保護するために、暗号化/復号化を伴う鍵リレーを実行する能力を有する。 - SReq.2に対して、KMAは、他のKMAにリレーされるときに、OTPのようなITセキュアな暗号化/復号化によって鍵データを暗号化する。 - SReq.3、SReq.4およびSReq.5に対して、鍵データの機密性は、KMAおよびKSAによる鍵供給リンクおよび/または暗号化方法の物理的保護を含む適切な手段によって保護される。 - SReq.6に対して、KMAおよびKSAは、改ざん防止対策および/または暗号化対策の使用を含む適切な手段によって保護される。 注1 - 改ざん防止対策は、トラステッドノードによって提供されるセキュリティ対策と共に実施することができる。

- 図1は、Y.3800が規定するQKDNの基本的な構成を示し、鍵管理に関連する機能（KMA、KSA、鍵供給リンク、KMAリンク、KSAリンク、KMに接続された制御と管理リンク）に対する潜在的なセキュリティ脅威を図示している。
- 表1は、鍵データ、メタデータ、制御と管理データ各々のセキュリティ脅威およびセキュリティ対策をi)機密性、ii)完全性、iii)認証およびアクセス制御、iv)可用性、v)責任追跡性の５分野で規定している。