TTC標準草案
(Draft TTC Standards)

セキュリティ専門委員会

2020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。昨年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。Y.3800には、日本のQKDネットワーク(QKDN)技術をベースとする提案が採用され、その骨格を形成している。
- ITU-T 勧告X.1710は、Y.3800が規定するQKDNの基本構成をベースとして、QKDNのセキュリティ概要、セキュリティ脅威、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。Y.3800とX.1710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	X.1710	1	量子鍵配送ネットワークのセキュリティフレームワーク

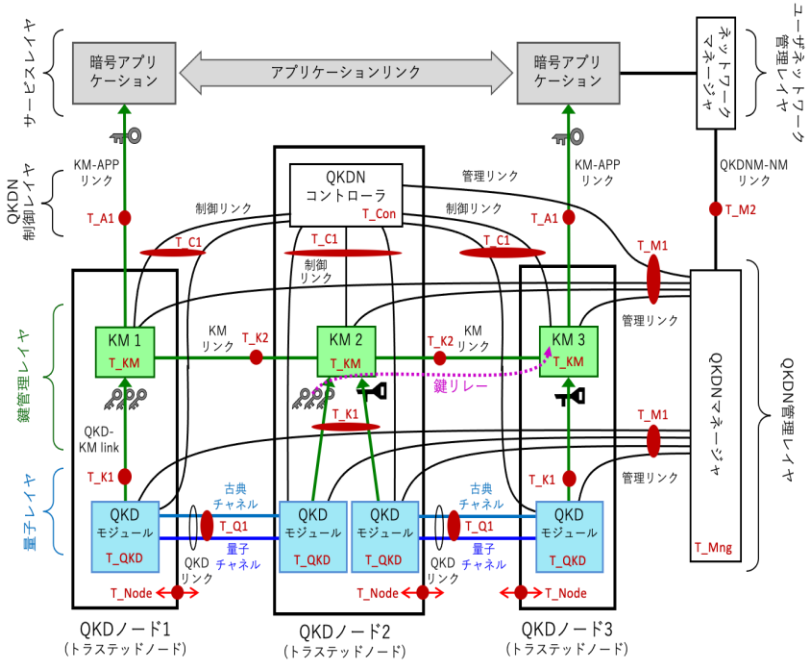
- ITU-T SG17では、X.1710に続くQKDN関連勧告の開発が進められている。セキュリティ専門委員会は、引き続きこれらITU-T勧告をベースとしたTTC標準の開発に取り組み、次回第131回標準化会議に提案する予定である。

		標準類	版数	タイトル
1	新規	X.1712	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

付録
JT標準のベースとなるITU-T勧告の概要

JT-X1710:量子鍵配送ネットワークのセキュリティフレームワーク

QKDNの情報資産を定義し、QKDNに対するセキュリティ脅威、QKDNのセキュリティ要求条件、QKDNのセキュリティ対策を規定する。



JT-X1710 図3　QKDNのセキュリティ脅威

セキュリティ対策	脅威	なりすまし	盗聴	削除または破損	否認	DoS
認証		x			x	
アクセス制御		x		x	x	
機密性		x	x			
データの完全性		x		x		
可用性	鍵の蓄積及び鍵リレー			x		
	ダメージ制御及び復旧			x		
	QKD リンクへのDoS 攻撃に対する堅牢性					x
責任追跡性	動作ログ	x		x		x
	セキュリティアラーム通知	x		x		x
	ログデータのセキュリティ監査	x			x	x

JT-X1710 表3
セキュリティ対策とセキュリティ脅威のマッピング

- 図３は、Y.3800が規定するQKDNの基本的な構成を示し、各機能要素に対する潜在的なセキュリティ脅威を図示している。
- 表３は、QKDNのセキュリティ脅威を1)なりすまし、2)盗聴、3)削除または破損、4)否認、5)DoSに分類し、各脅威に対して有効なセキュリティ対策を示している。