TTC標準草案
(Draft TTC Standards)

セキュリティ専門委員会

2024年5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、Y.3808、X.1710、X.1712が承認され、QKDNの基本勧告シリーズが完成している。
- 2022年2月にITU-T SG13から発刊されたY.3808は、QKDNとセキュアストレージネットワーク(SSN)の統合フレームワークを規定する。SSNは、QKDNが生成する鍵を利用しデータを暗号化して分散保存するソリューションで、高い秘匿性と可用性を同時に実現する。
- 今回制定するJT-X1715は、Y.3808が規定するSSNの機能アーキテクチャをベースとして、SSNの情報資産、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、QKDNとSSN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SSNの実用化に向けたプロジェクトが進んでいる。JT-X1715の発刊により関連する標準化の検討が加速し、製品開発やSSNを利用した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。

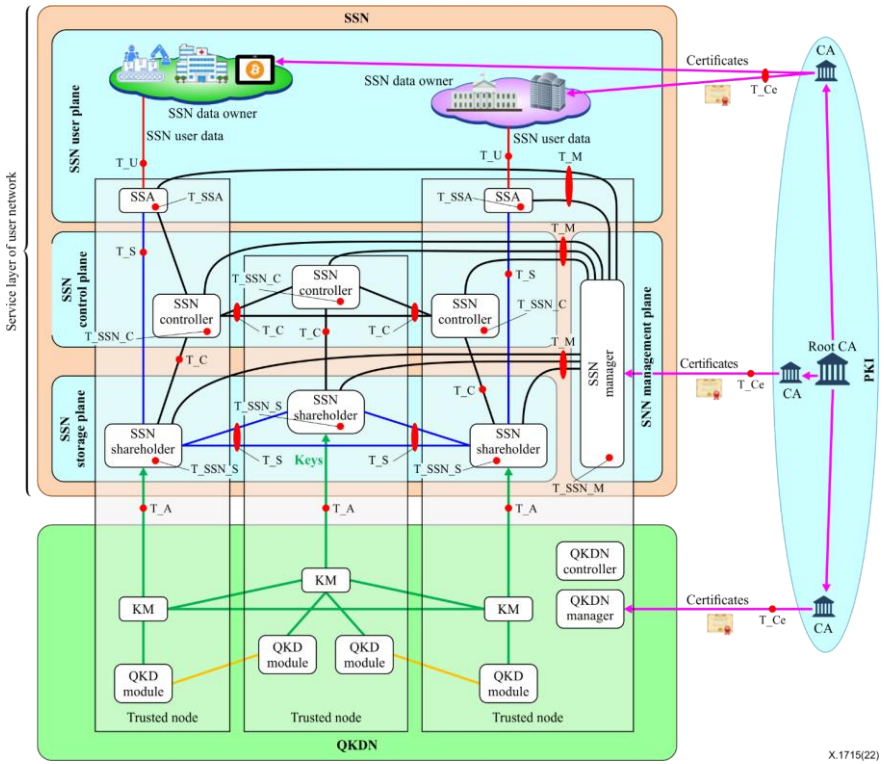
		標準類	版数	タイトル
1	新規	JT-X1715	1	量子鍵配送ネットワークとセキュアストレージネットワークの統合のためのセキュリティ要求条件と対策

- ITU-T SG17では、X.1710、X.1712、X.1715に続くQKDNのセキュリティ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-X1715:QKDNとSSNの統合のためのセキュリティ要求条件と対策

SSN(Secure Storage Network)に対するセキュリティ脅威、セキュリティ要求条件及びセキュリティ要求条件を満たすためのSSNのセキュリティ対策を規定する。



JT-X1715 図2　QKDNとPKIおよびSSN統合で特定されたセキュリティ上の脅威

JT-X1715 表3 – オリジナルデータに対するセキュリティ要求条件および対策 (抜粋)

	記述	セキュリティ要求条件	セキュリティ対策
(i) 機密性	オリジナルデータに関するいかなる情報も、許可されていない要素や関係者に漏洩することから保護する。	SReq.1 - SSAは、SSNデータホルダーと協力し、SSAリンクを介して送信されるオリジナルデータの機密性を確保することが要求される。 SReq.2 - SSAは、SSAによって処理または保存するときに、オリジナルデータの機密性を確保することが要求される。	- SReq.1の対策として、SSAは、要求された機密性を保護するために、暗号化または復号化を伴うオリジナルデータを供給または受信する能力を有する。 - SReq.2の対策として、SSAは、物理的保護措置または暗号措置の使用を含む適切な手段によって保護される。
(ii) 完全性	オリジナルデータが変更されない。	SReq.3 - SSAは、オリジナルデータの完全性を保証することが要求される。	- SReq.3の対策として、SSAは、SSNデータオーナから受信したオリジナルデータの完全性を検証する。 - SReq.3の対策として、SSAは、物理的保護措置または暗号措置の使用を含む適切な手段によって保護される。
(iii) 認証とアクセス制御	オリジナルデータへのアクセスは、許可されたエンティティに制限される。	SReq.4 - SSAは、SSNデータオーナから受信したオリジナルデータが、送信エンティティの身元が認証され、オリジナルデータを提供する権限が与えられていない限り、信頼されないことを保証することが要求される。 SReq.5 - SSAは、他のエンティティが暗号化されていないオリジナルデータを受け取る権限を与えられていることを保証しない限り、他のエンティティがそのオリジナルデータにアクセスすることを許可しないことを保証することが要求される。	- SReq.4およびSReq.5の対策として、SSAは、通信する他のエンティティとの相互認証を実行するか、または他の対策を利用する。 - SReq.4およびSReq.5の対策として、SSAはセキュリティ関連の属性を処理し、アクセス制御セキュリティポリシーを実装する機能を備える。
(iv) 可用性	オリジナルデータは必要なときにいつでも利用できる。	SReq.6 - SSAは、SSNデータオーナからの要求に従って、オリジナルデータを提供することが要求される。 SReq.7 – SSNシェアホルダーの誤動作または破壊によって一部のシェアが失われた場合、SSNシェアホルダーは、残りのシェアの数がしきい値と同じかそれ以上であれば、残りのシェアからオリジナルデータを再構築することが要求される。	- SReq.6およびSReq.7の対策として、SSAはシェアを取得し、部分的なシェアからオリジナルデータを再構築する機能を備えている。
(v) 責任追跡性	オリジナルデータは追跡可能である。	SReq.8 - SSAは、SSNコントローラまたはSSNマネージャにインシデント関連パラメータを通知することが推奨される。	- SReq.8の対策として、SSAはインシデント関連のパラメータを作成し、それらをSSNコントローラまたはSSNマネージャに送信する機能を備える。

- 図2は、Y.3800が規定するQKDNの構成とY.3808が規定するSSNの構成を示し、SSNの各インタフェース及び機能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、SSNに保管するオリジナルデータ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。