TTC標準
Standard

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
Security framework for quantum key distribution networks

第 1.1 版

2021 年 4 月 1 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

目　次

＜参考＞

1. 国際勧告などとの関連

本標準は量子鍵配送ネットワークの機能要求条件について規定しており、2020 年 10 月に ITU-T SG17 において発行された ITU-T 勧告 X.1710 に準拠している。

2. 上記勧告などに対する追加項目など

2.1 オプション選択項目

なし

2.2 ナショナルマター決定項目

なし

2.3 その他

なし

2.4 原勧告との章立て構成比較表

章立てに変更なし

3. 改版の履歴

版数	発行日	改版内容
第 1 版	2021 年 2 月 18 日	制定
第 1.1 版	2021 年 4 月 1 日	8.2 章の誤記訂正

4. 工業所有権

本標準に関わる「工業所有権の実施の権利に係る確認書」の提出状況は、TTC ホームページでご覧になれます。

5. その他

(1) 参照している勧告、標準など

ITU-T 勧告　　ITU-T X.805

JT 標準　　JT-Y3800

6. 標準作成部門

セキュリティ専門委員会

1. 規定範囲

本標準は、量子鍵配送(QKD)セキュリティに関する一連の標準の最初のものであり、他の関連する標準のためにセキュリティフレームワークを提供する。特に、本標準は次の事項を取り扱う。

- 量子鍵配送ネットワーク(QKDN)のセキュリティ
- 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

2. 参考文献

以下に列挙する ITU-T 勧告及びその他の参考文献は、この本文中の参照を通して、本標準を構成する規定を含む。発行時点では、示された版は有効であった。すべての勧告及び他の参考文献は改訂の対象である。したがって、本標準の利用者は、以下に列挙する勧告及び他の参考文献の最新版を適用する可能性を調査することが推奨される。現在有効な ITU-T 勧告のリストは定期的に発行されている。本標準が文献を参照することは、その文献がそれ単体で勧告となる地位をその文献に与えるものではない。

[ITU-T X.805] Recommendation ITU-T X.805 (2003), Security architecture for systems providing end to end communications.

[ITU-T Y.3800] Recommendation ITU-T Y.3800(2019), Overview on networks to support quantum key distribution.

3. 定義

3.1. 他の標準等で定義されている用語

本標準は、以下の他で定義される用語を使用する。

3.1.1. 責任追跡性[b-ITU-T-X.800]：エンティティのアクションをエンティティに対して一意にトレースできるようにする特性。

3.1.2. 真正性[b-T.411]：要求されたデータソースが受領者の満足のいくように検証できる特性。

3.1.3. 可用性[b-ITU-T-X.800]：認可されたエンティティによる要求に応じてアクセス可能であり、かつ使用可能であるという特性。

3.1.4. 古典チャネル [ETSI GR QKD007]：破壊することなく読み取り可能で、完全に再生されるであろう形式で符号化されたデータを交換するために 2 つの通信当事者が使用する通信チャネル。

3.1.5. 機密性[b-ITU-T X.800]：情報が許可されていない個人、エンティティ、またはプロセスに対して利用可能にされない、または開示されないという特性。

3.1.6. 情報理論的安全性(IT セキュア)[ITU-T Y.3800]：無制限の計算資源による解読攻撃に対する安全性。

3.1.7. 完全性[b-ITU-T X.1193]：許可されていない方法でデータが変更または破壊されていない特性。

3.1.8. 鍵管理[ITU-T Y.3800]：量子レイヤからの受信、格納、フォーマッティング、リレー、同期、認証、暗号アプリケーションへの供給、鍵管理ポリシーによる削除または保存まで、鍵ライフサイクルで実行されるすべての動作。

3.1.9. 鍵マネージャ(KM)[ITU-T Y.3800]：鍵管理レイヤ内で鍵管理を実行する機能モジュールで、QKD ノード内に配置される。

3.1.10. KM リンク[ITU-T Y.3800]：鍵マネージャ(KM)を接続し、鍵管理を行う通信リンク。

3.1.11. 鍵リレー[ITU-T Y.3800]：中間 QKD ノードを経由し任意の QKD ノード間で鍵を共有する方法。

3.1.12. 量子チャネル [ETSI GR QKD007]：量子信号を送信する通信チャネル。

3.1.13. 量子鍵配送 (QKD)[ETSI GR QKD007]：量子情報理論に基づく情報理論的セキュリティを用いて対称暗号鍵を生成及び配送する手順または方法。

3.1.14. QKD リンク[ITU-T Y.3800]：QKD を動作させるための 2 つの QKD モジュール間の通信リンク。

注 - QKD リンクは、量子信号を送受信する量子チャネルと、同期と鍵蒸留のために情報を交換する古典チャネルから構成される。

3.1.15. QKD モジュール[ITU-T Y.3800]：暗号機能と、QKD プロトコル、同期、鍵生成のための蒸留などの量子光プロセスを実装するハードウェア及びソフトウェアコンポーネントのセット。定められた暗号境界内に含まれる。

注 - QKD モジュールは、QKD リンクに接続され、鍵を生成するエンドポイントモジュールとして動作する。QKD モジュールには 2 つのタイプ、すなわち送信器(QKD-Tx)及び受信器(QKD-Rx)がある。

3.1.16. QKD ネットワーク(QKDN)[ITU-T Y.3800]：QKD リンクを介して接続された 2 以上の QKD ノードから構成するネットワーク。

注 - QKD ネットワーク(QKDN)では、QKD リンクで直接接続されていない QKD ノード間でも、鍵リレーによって鍵を共有できる。

3.1.17. QKD ノード[ITU-T Y.3800]：許可されていない当事者による侵入及び攻撃から保護されている 1 つ以上の QKD モジュールを含むノード。

注 - QKD ノードは、鍵マネージャ(KM)を含むことができる。

3.1.18. 脅威[b-ISO/IEC27000]：望ましくないインシデントの潜在的な原因で、システムまたは組織に損害を与える可能性がある。

3.2. 本標準で定義する用語

3.2.1. 量子鍵配送プロトコル(QKD プロトコル)：量子情報理論に基づく情報理論的安全性を持つ対称暗号鍵を確立するための一連の手順。

3.2.2. 回復性：悪条件や攻撃に適応し、そこから回復する能力。

4. 略語及び頭字語

本標準では、次の略語及び頭字語を使用する。

AES	Advanced Encryption Standard (高度暗号化標準)
APP	Application (アプリケーション)
DDoS	Distributed Denial of Service (分散サービス妨害)
DoS	Denial of Service (サービス妨害)
SReq	Security Requirement (セキュリティ要求条件)
IT-secure	Information Theoretically secure (情報理論的安全性)
KM	Key Manager (鍵マネージャ)
NM	Network Manager (ネットワークマネージャ)
OTP	One-Time Pad (ワンタイムパッド)
QKD	Quantum Key Distribution (量子鍵配送)
QKDN	Quantum Key Distribution Network (量子鍵配送ネットワーク)
QKDNM	Quantum Key Distribution Manager (QKD マネージャ)
QKD-Rx	Quantum Key Distribution Receiver (QKD 受信器)
QKD-Tx	Quantum Key Distribution Transmitter (QKD 送信器)

5. 表記法

本標準ではキーワード「が要求される」は、厳密に従わなければならず、この文書への適合性が主張される場合にはそこから逸脱することは許されない要求条件を示す。

キーワード「推奨される」は、推奨されるが絶対に必要ではない要求条件を示す。従って、この要求条件は、適合性を主張するために存在する必要はない。

6. はじめに

通信ネットワーク内の 2 つの離れた当事者間で対称な鍵を確立することは、基本暗号の 1 つであり、今日使用されている多くのサイバーセキュリティシステムの基礎となっている。これは通常、公開鍵暗号方式を使用して行われる。公開鍵暗号と同様に、量子鍵配送(QKD)による鍵の確立が可能である。公開鍵暗号とは異なり、QKD プロトコルは量子力学の法則に基づいており、理論的には無限の計算能力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。この種のセキュリティは、情報理論的安全性(IT セキュア)と呼ばれる。

QKD プロトコルは、古典チャネルと量子チャネルからなる QKD リンクによって接続された一対の QKD モジュールによって実行される。次に、QKD プロトコル手順に従って、これらの QKD モジュール間に鍵(すなわち、対称ランダムビット列の対)が確立される。
QKD リンクによって接続された QKD モジュールの対と、KM リンクを介して連結された対応する鍵マネージャ(KM)の集合は、QKDN の基礎である。暗号アプリケーションは、QKDN の適切な鍵リレーによって、任意の 2 つの指定されたノード間で安全な鍵を共有できる。QKD モジュールで生成された鍵自体は、ユーザネットワークの暗号アプリケーションに提供されるまで、適切な方法により QKDN で安全に管理する必要がある。QKDN の基本機能とレイヤ構造は[ITU-T Y.3800]で規定されている。

QKDN は、様々なセキュリティ脅威にさらされており、それは、その正しい運用を侵害し、鍵のセキュリティを危うくする。QKDN の情報セキュリティを確保するためには、事業者と利用者や第 3 者などの他の主体との間の利害、取引関係、法的・規制上の制約、契約上の制約などを考慮して、セキュリティ脅威を特定すべきである。次に、QKDN、ユーザネットワーク、及び 2 つのネットワーク間のリンクに対して、適切なセキュリティ対策を定義する必要がある。

図 1 は、QKDN のセキュリティ評価プロセスを示している。セキュリティ脅威は、QKDN の機能要素、リンク、及び情報資産の基本的な特性とそれらの間の関係の両方から推測される。セキュリティ脅威から、QKDN のセキュリティ要求条件を特定することができ、その要求条件は、QKDN の効率的なセキュリティ対策を導出するために使用される。

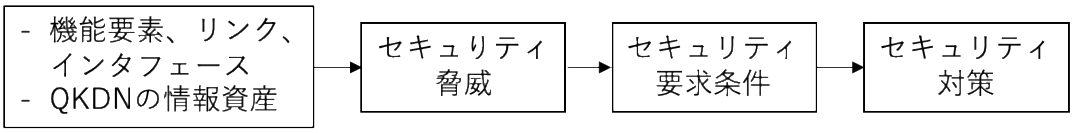

図 1　QKDN のセキュリティ評価プロセス

従って、本標準は QKDN のためのセキュリティフレームワークを提供する。QKD プロトコルのセキュリティ分析は、本標準の範囲外である。

7. QKDN 特有のセキュリティ

QKD プロトコルは、ある仮定の下で情報理論と量子力学によって証明された機密性を持つ鍵の確立を可能にする。これは、鍵に関する情報がいかなる盗聴者にも知られないことを意味する。

QKD ノードの情報セキュリティを確保するために、特に鍵のセキュリティを保護するために、QKD ノードは無許可の関係者による侵入及び攻撃から保護されなければならない。このような保護を持つ QKD ノードは、トラステッドノードと呼ばれる。トラステッドノードは、ノード外の攻撃者からすべての搭載された要素を保護する境界として機能する。

鍵がトラステッドノードで管理され、IT セキュアなプロトコル(例えば、ワンタイムパッド(OTP))に基づいてリレーされる場合、高度に安全な鍵を QKDN の任意の指定されたノード間で確立することができる。これらの機能は、データの

長期的な機密保護を必要とする暗号アプリケーションに高度に安全な鍵を提供するという、QKDN に独自の機能をもたらす。

鍵は、例えば、鍵リレー中の悪意のあるアクセス、鍵保存中の偶然の故障、または鍵の完全性の侵害などの状況に応じて、生成後に変更されることがある。そのため、暗号アプリケーションで使用されるまで鍵が変更されないようにするには、完全性を保護する必要がある。このような機能は、計算量的安全な暗号プロトコル(公開鍵暗号法、ハッシュ関数など)、または IT セキュアな暗号プロトコル(例えば、[b-Wegman-Carter]メッセージ認証)上に構築することができる。

QKDN を正しく制御及び管理するには、制御及び管理情報も適切なセキュリティ対策を使用して保護する必要があり、このセキュリティ対策には最大限の計算量的安全性が用いられる。従って、QKDN では異なる種類の暗号プロトコルを適切に組み合わせて使用する必要がある。

8. QKDN に対するセキュリティ脅威

8.1. QKDN の要素及び情報資産

[ITU-T Y.3800]で規定し図 2 に示されているように、QKDN は QKD モジュール、KM、QKDN コントローラ、QKDN マネージャ、及びこれらの機能要素を接続するリンクから構成される。

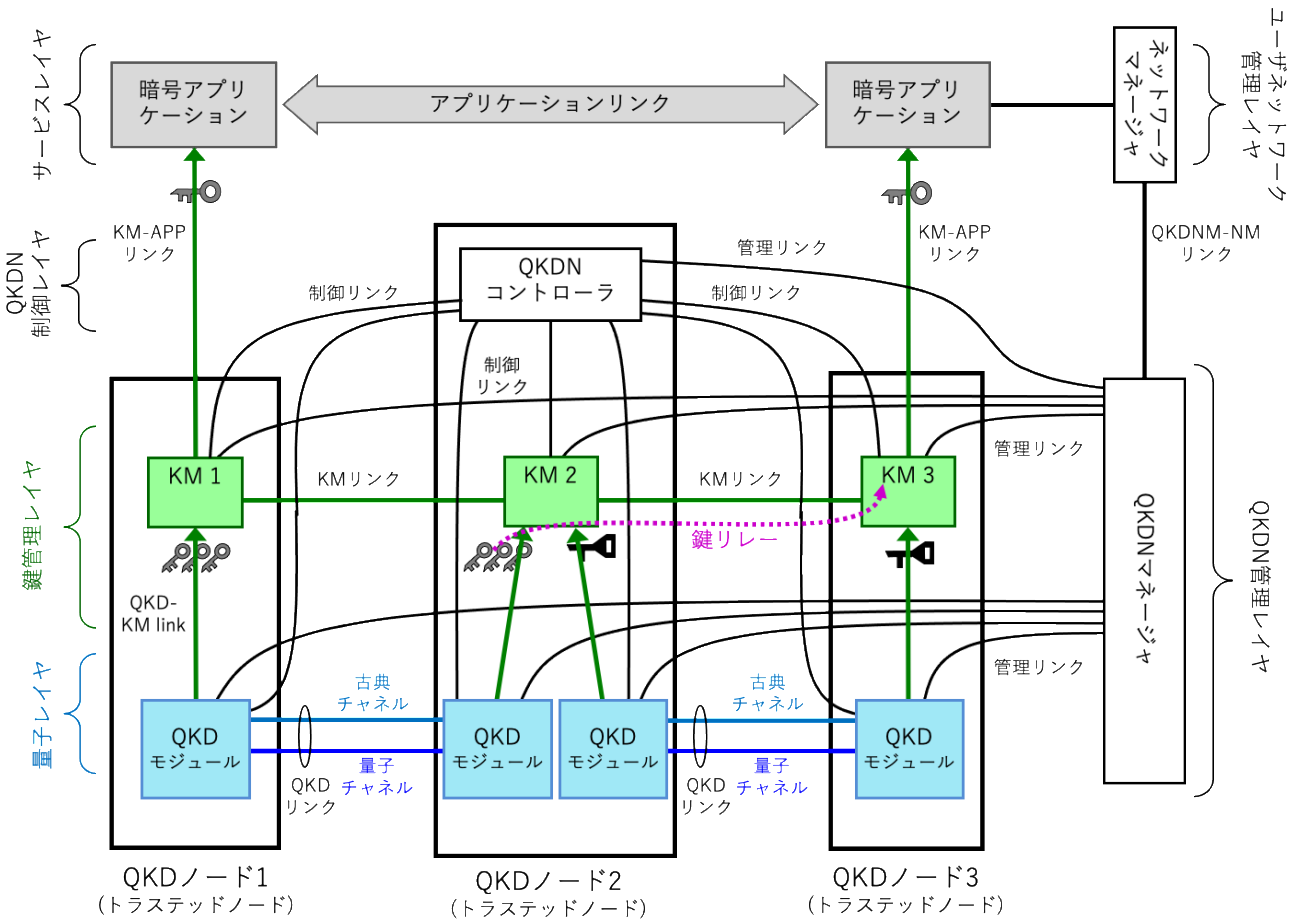

図 2　QKDN とユーザネットワークの典型的な構成

QKDN 内の機能要素とリンク、及び QKDN とユーザネットワーク間の機能要素とリンクを以下に示す。

- QKD モジュール：QKD プロトコルに基づいて鍵を生成する機能要素。

- KM：鍵管理を行う機能要素。
- QKDN コントローラ：QKDN を制御する機能要素。
- QKDN マネージャ：QKDN を管理する機能要素。
- QKD リンク：QKD モジュール間の通信リンクで、古典チャネルと量子チャネルで構成される。

注 - QKD リンクには、光スイッチ、中間測定ステーション、及び量子リピータを含むことがある。

- KM リンク：KM 間の通信リンク。
- 制御リンク：QKDN コントローラと 3 つの機能要素(KM、QKD モジュール、または QKD リンク)の 1 つとの間の通信リンク。
- 管理リンク：QKDN マネージャと QKDN 内の他のすべての要素(例えば、QKDN コントローラ、KM、QKD モジュール、または QKD リンク)との間の通信リンク。
- QKD-KM リンク：QKD モジュールと KM 間のリンク。
- KM-APP リンク：KM とユーザネットワーク内の暗号アプリケーションとの間のリンク。
- QKDNM-NM リンク： QKDN マネージャ(QKDNM)とユーザネットワーク内のネットワークマネージャ(NM)間のリンク。

次の種類のデータ及び情報は、上述のリンクを通じて伝送され、当該 QKDN の情報資産として識別される。

- 鍵データ：セキュア鍵(対称ランダムビット列)を含むデータ。
- メタデータ：鍵データに付加され、鍵管理に使用される追加データ。
- 制御及び管理情報：QKDN の制御及び管理に関連する情報。例えば、鍵管理情報、鍵ライフサイクル情報、セッション制御情報、ルーティング制御情報ならびにモジュール及びリンクの性能及びステータス情報。

表 1 は、QKDN の要素またはリンクと情報資産との対応をまとめたものである。

表 1　QKDN における要素と情報資産の関係

機能要素 ＼ 情報資産		鍵データ	メタデータ	制御及び管理情報
	QKD リンク			x
	KM リンク	x	x	x
	制御リンク		x	x
	管理リンク		x	x
	KM-App リンク	x	x	
	QKDNM-NM リンク			x

QKD ノード（トラステッドノード）	QKD モジュール	x	x	x
	KM	x	x	x
	QKDN コントローラ		x	x
	QKDN マネージャ		x	x
	QKD-KM リンク	x	x	

本標準は、QKDN に対するセキュリティ脅威について記述する。トラステッドノードの要求条件と機能の詳細な脅威分析と仕様は、本標準の範囲外である。

注 - 場合によっては、暗号アプリケーションは、トラステッドノードで鍵を受信した後、トラステッドノードの外部で鍵を使用する。代表的な例としては、スマートフォンやドローンなどのモバイル端末の暗号アプリケーションがある。

8.2. セキュリティ脅威

この章では、QKDN に対するセキュリティ脅威を識別する。図 3 は、図 2 で記述した構成にこれらの脅威を重ねて図示している。

トラステッドノード間に配置され外部環境に暴露される QKD リンク、KM リンク、制御リンク、及び管理リンクに攻撃対象領域があることが識別される。また、トラステッドノードの外部からのアクセスパスがある KM-APP 及び QKDN-MN リンクに別のタイプの攻撃対象領域があることが識別される。

他の攻撃対象領域がトラステッドノード内にあることも識別される。すなわち、トラステッドノード内で保護されているものの、QKD-KM リンクがそれである。

機能要素(QKD モジュール、KM、QKDN コントローラ、QKDN マネージャ)は、たとえそれらがトラステッドノード内にあるとしても、この章で扱われるセキュリティ脅威にさらされる可能性がある。

本標準は、3 種類の脅威を区別する。

- 意図的な脅威：通信自体またはネットワークリソースのいずれかを攻撃する可能性のある悪意のある要素を含む脅威。
- 管理上の脅威：セキュリティ管理の失敗から生じる脅威。
- 偶発的な脅威：発生元に悪意がなく、技術的な障害の結果による脅威。

より正確な分析を行うために、本標準は意図的な脅威のみに焦点を当てている。

注 - 管理上の及び偶発的な脅威は、本標準の範囲外である。

意図的な脅威に関する分析は、様々な種類のシステムやネットワークに対して行われてきた。例えば、オープンシステムの相互接続については[b-ITU-T-X.800]、SDN については[b-ITU-T-X.1038]である。

同様に、QKDN の脅威分析では、以下の項目に取り組むべきである。

- なりすまし：不正な利益を得るために別の主体になりすます。例えば、攻撃者は KM になりすまして鍵にアクセスし、鍵を変更する。

- 盗聴：情報資産を解読することによって機密性を侵害する。攻撃者は、将来の攻撃のために機密システム情報(設定データ、ユーザ認証情報など)を取得する可能性がある。
- 削除または破損：許可されていない削除、挿入、変更、順序の変更、再生、または遅延によって、転送または保存された情報資産の完全性を損なう。
- 否認：何らかのタスクを実行した事実を否認する。例えば、悪意のあるネットワークポリシー(特定のトラフィックフローを悪意のあるノードにコピー及び転送するなど)を強制し、そのようなネットワークポリシーを強制しなかったと主張する可能性がある。
- Denial of Service(DoS)：QKDN の適切な運用を妨害する活動を行う。これには、QKDN へのアクセス拒否や、QKDN を輻輳させることによる鍵生成やその他の通信の拒否が含まれる可能性がある。最近の脅威は、Distributed Denial of Service (DDoS)攻撃である。この攻撃は、複数のソースからの大量のトラフィックでオンラインサービスを圧倒して利用不能にしようとする。

以後では、QKDN の各リンク及び機能要素のセキュリティ脅威について記述する。QKD リンクに対する量子及び古典的攻撃、及び QKD モジュールに対する QKD 固有のサイドチャネル攻撃を含む、QKD プロトコルに関するセキュリティ脅威は、本標準の範囲外である。

注 1 - QKD プロトコルと QKD 固有のサイドチャネル攻撃対策を適切に実施することで、QKDN は QKD モジュールと QKD リンクをこれらの脅威から保護できる。

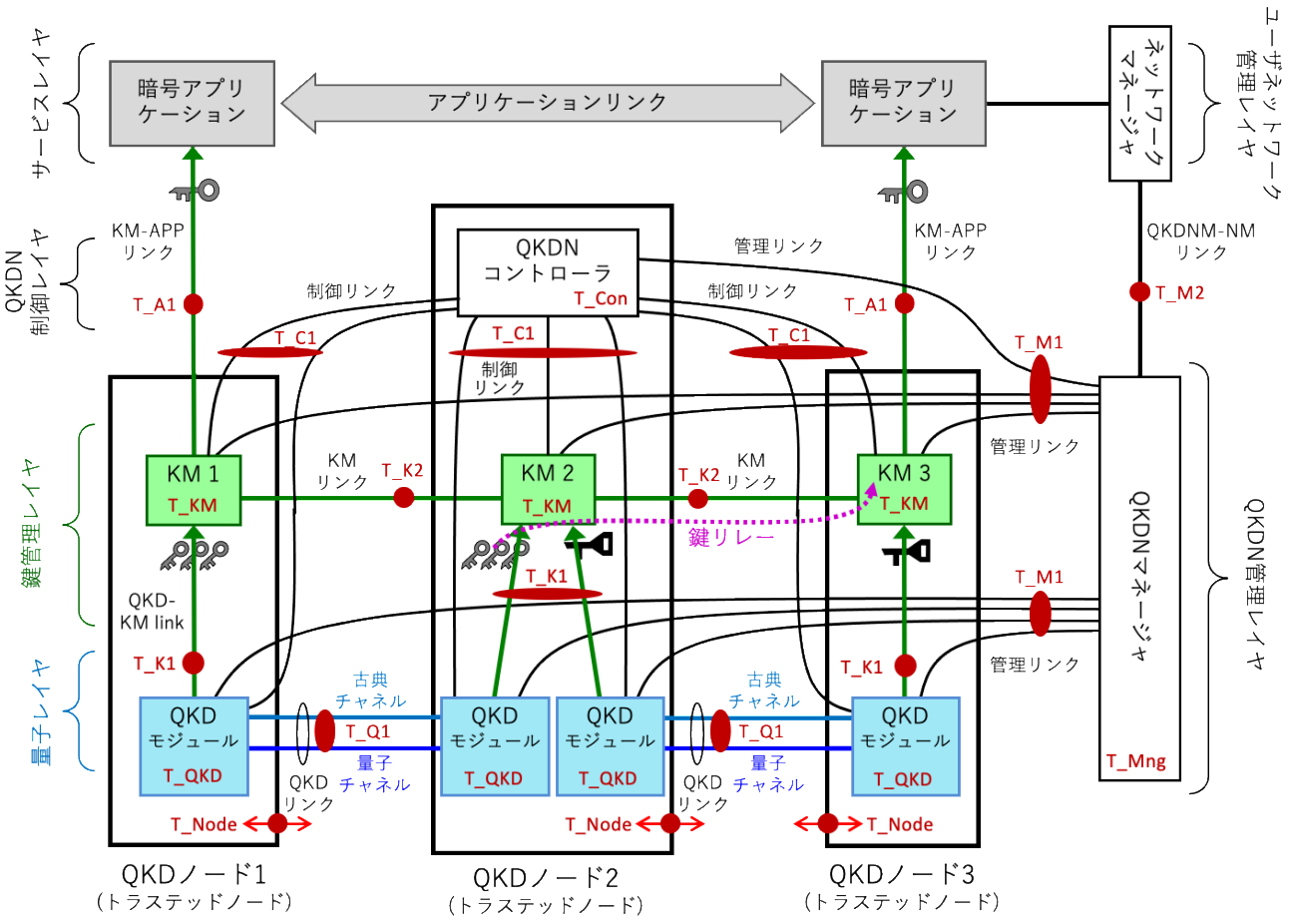

図 3　QKDN のセキュリティ脅威

1) T_Q1：QKD リンクのセキュリティ脅威：

- 削除または破損：古典チャンネル内の情報を削除または変更する。
- DoS：通信の中断またはデータトラフィックの輻輳。

2) T_QKD：QKD リンク、制御リンク、または管理リンクを介した QKD モジュールのセキュリティ脅威：

- 盗聴：量子サイドチャネル攻撃。
- 削除または破損：QKD モジュール内の情報を削除または変更する。
- DoS：アクセス拒否またはデータトラフィックの輻輳。

3) T_K1：QKD-KM リンクのセキュリティ脅威：

- 盗聴：鍵データとメタデータを傍受し解読する。
- 削除または破損：鍵データ及びメタデータを削除または変更する。
- DoS：通信の中断またはデータトラフィックの輻輳。

4) T_K2：KM リンクのセキュリティ脅威：

- 盗聴：鍵データとメタデータを傍受し解読する。
- 削除または破損：鍵データ及びメタデータを削除または変更する。
- DoS：通信の中断またはデータトラフィックの輻輳。

5) T_KM：KM リンク、QKD-KM リンク、KM-APP リンク、及び制御または管理リンクを介した KM のセキュリティ脅威：

- 盗聴：鍵データとメタデータを盗み解読する。
- なりすまし：攻撃者が KM になりすまして情報セキュリティを侵害する。攻撃者は、情報資産を不正に作成し、その資産が別の機能要素または暗号アプリケーションから受信された、または別の機能要素または暗号アプリケーションに送信されたと主張する。
- 否認：攻撃者が悪意を持って鍵管理機能を実行し、その後その事実を否認する。
- DoS：アクセス拒否またはデータトラフィックの輻輳。

6) T_A1：KM-APP リンクのセキュリティ脅威：

- 盗聴：暗号アプリケーションから鍵データ、メタデータ、情報を傍受し解読する。
- 削除または破損：鍵データ、メタデータ、及び鍵要求などの暗号アプリケーションからの情報を削除または変更する。
- DoS：通信の中断またはデータトラフィックの輻輳。

7) T_C1：制御リンクのセキュリティ脅威：

- 盗聴：QKDN 制御情報を傍受し解読する。
- 削除または破損：QKDN 制御情報を削除または変更する。
- DoS：通信の中断またはデータトラフィックの輻輳。

8) T_Con：制御及び管理リンクを介した QKDN コントローラのセキュリティ脅威：

- 盗聴：制御情報を盗み解読する。

- なりすまし：攻撃者が QKDN コントローラになりすまして情報セキュリティを侵害する。攻撃者は、QKDN 制御及び管理情報を悪意を持って作成し、その情報が別の機能要素から受信された、または別の機能要素に送信されたと主張する。
- 否認：攻撃者が悪意をもって QKDN 制御機能を実行し、その後その事実を否認する。
- DoS：アクセス拒否またはデータトラフィックの輻輳。

9) T_M1：管理リンクのセキュリティ脅威：

- 盗聴：QKDN 管理情報を傍受し解読する。
- 削除または破損：QKDN 管理情報を削除または変更する。
- DoS：通信の中断またはデータトラフィックの輻輳。

10) T_Mng：制御・管理リンク、及び QKDNM-NM リンクを介した QKDN マネージャのセキュリティ脅威:

- なりすまし：攻撃者が QKDN マネージャになりすまして情報セキュリティを侵害する。攻撃者は、QKDN 管理情報を不正に作成し、その情報が別の機能要素から受信された、または別の機能要素に送信されたと主張する。
- 否認：攻撃者が悪意を持って QKDN 管理機能を実行し、その後その事実を否認する。
- DoS：アクセス拒否またはデータトラフィックの輻輳。

11) T_M2：QKDNM-NM リンクのセキュリティ脅威：

- 盗聴：QKDN 及びユーザネットワーク管理情報を盗み、解読する。
- 削除または破損：QKDN 及びユーザネットワーク管理情報を削除または変更する。
- DoS：通信の中断またはデータトラフィックの輻輳。

12) T_Node：QKD ノードのセキュリティ脅威:

- 無許可の物理的アクセス：敵対者は、QKD ノードに物理的に侵入し、情報資産を盗むまたは他の目的(例えば、情報の損失または破損、なりすまし、否認、及び DoS)のため、QKD ノード内の QKD モジュール、KM、QKD-KM インタフェース及び他のエンティティに直接アクセスする。

注 2 - T_Node への不正アクセスには、リンクを介したサイバー攻撃や物理的な攻撃が含まれる場合がある。

さらに、これらのセキュリティ脅威は、例えば、建物の不法侵入、許可されていない関係者によるネットワーク接続を介した悪意のあるアクセス、またはシステムへのバックドアの設置などの物理的なアクセスにより、QKDN の導入、保守、更新、及び移行の間及び後に起こり得る。例えば、QKD モジュールにはメンテナンスポートがあり、これは脅威に対する抜け穴となる可能性がある

QKDN の導入及びメンテナンス中の主な脅威は、導入またはメンテナンス中のエンティティへのなりすまし、及び無許可アクセスである。例えば、エンティティのなりすましが中間者攻撃につながり、不正アクセスがバックドア感染につながる可能性がある。

セキュリティ脅威と QKDN の各要素との関係を、3 つの異なる優先度レベルを用いて表 2 に要約する。

表 2 - セキュリティ脅威と QKDN の機能要素とそれらのリンクの関係、及び 3 つの異なる優先度レベル

機能要素	脅威	なりすまし	盗聴	削除または破損	否認	DoS
	QKD リンク			3		1
	KM リンク		3	2		1
	制御リンク		1	2		1
	管理リンク		1	2		1
	KM-App リンク		3	2		1
	QKDNM-NM リンク		1	2		1
QKD ノード（トラステッドノード）	QKD モジュール		3	3		1
	KM	3			2	1
	QKDN コントローラ	2			2	1
	QKDN マネージャ	2			2	1
	QKD-KM リンク		3	2		1

表 2 の数字は、次の脅威レベルを示している。

- 3：高レベル

  このレベルは発生した場合、致命的である。これは、鍵データの機密性を損なう可能性がある脅威などである。

- 2：中レベル

  このレベルの脅威を回避することは不可欠である。これは、例えば、鍵管理レイヤ、QKDN 管理レイヤ、QKDN 管理レイヤにおける管理情報や運用情報に対する脅威である。このような脅威が発生した場合、QKDN の安全で信頼性のある運用ができなくなる。

- 1：低レベル

  このレベルには 2 種類の脅威が含まれる。第一は DoS 攻撃で、認識可能であり考慮する必要がある。このような脅威が発生すると、QKDN は正常に運用できなくなる。第二は、QKDN の制御及び管理情報の盗聴であり、認識され

ることなく実行可能である。これは、鍵データの漏洩や QKDN 運用の中断を引き起こすことはないが、敵対者にとっては有益かもしれない。

9. セキュリティ要求条件及びセキュリティ対策

この章では、QKDN におけるセキュリティ要求条件(SReq)と、それを満たすためのセキュリティ対策について記述する。セキュリティ要求条件は、第 8 章に列挙された脅威に対処するために規定される。

これらの要求条件は、[ITU-T-X.805]の第 6 章に規定された、ネットワークセキュリティに特有の側面に対処するために設計されたセキュリティ対策に対応し構成されている。QKDN のセキュリティ管理のため、セキュリティ対策には責任追跡性が追加されている。セキュリティ対策とセキュリティ脅威との間の関係は、表 3 に示す通りマッピングされる。これは、機能要素、リンク、及び QKDN の運用に実質的な影響を与えるセキュリティ対策に限定して示している。

セキュリティ要求条件の詳細な規定と、QKDN の否認防止及び信頼性は、本標準の範囲外である。

注 - QKD リンクへの量子及び古典的攻撃、及び QKD モジュールへの QKD 固有のサイドチャネル攻撃を保護するためのセキュリティ対策は、本標準の範囲外である。

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

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

9.1. QKDN 運用のためのセキュリティ対策

9.1.1. 認証

SReq.1　　QKDN は、識別子を確立し、QKDN 内ならびにユーザネットワーク内の機能要素、及びその他のエンティティ(これらが外部から QKDN に接続されている場合)が主張する識別情報を検証することが要求される。

SReq.1 をサポートするセキュリティ対策には、次のものがある。

- ユーザ認証：QKDN に接続されているユーザネットワーク内の機能要素(例えば、暗号アプリケーションやネットワークマネージャ)の識別情報の証明を確立する。
- エンティティ認証：通信中の QKDN 内の機能要素の識別情報の証明を確立する。
- データ発信元認証：特定のデータユニットの発信元を識別する識別情報の証明を確立する。

認証機能は、許可された当事者のみが鍵データにアクセスできることを保証することによって、鍵データの機密性を保護する(9.1.3 節を参照)、また鍵データの完全性及び真正性を保証する(9.1.4 節を参照)という重要な役割を果たす。それらの詳細は本標準の範囲外である。

SReq.1.1　　QKDN は、鍵を配送する前に、関連する機能要素間のエンティティ認証を実施することが推奨される。

認証機能は、特定のタイミングで証明を確立する。継続的な証明を保証するには、認証を繰り返すか、完全性サービスにリンクする必要がある。

注 – 例えば、認証タグは、鍵データまたはメタデータ(鍵 ID、機能要素 ID、タイムスタンプなど)から生成され、新しい要素としてメタデータに付加され、QKDN 内の関連する機能エンティティで処理される。

9.1.2. アクセス制御

SReq.2　　QKDN は、QKDN 内の機能要素によるアクセスを許可されていない情報や資源へのアクセスを防止することを推奨される。

アクセス制御機能は、リソースが許可された方法でのみアクセスされることを保証する手段を提供する。関連するリソースには、物理システム、システムソフトウェア、アプリケーション、またはデータがある。アクセス制限は、次の内容を指定するアクセス制御情報に記載される。

- どのエンティティがアクセスを許可されているかを決定する手段。
- 許可されるアクセスの種類(読み取り、書き込み、変更、作成、削除)。

アクセス制御は、認証機能によってサポートされる。

注 - 物理アクセス制御は、トラステッドノードで処理される。この場合、単一のトラステッドノード内のすべての機能エンティティのアクセス制御は、単一のセキュリティ手段によって実行することができる。

9.1.3. 機密性

SReq.3　　QKDN は、保存及び転送された鍵データの機密性を保証することが要求される。

SReq.3 を満たすためには、以下の要求条件が必要である。

SReq.3.1　　鍵に関する情報は、暗号アプリケーションによって指定された十分に長い期間、認可されていない当事者が入手できないようにすることが推奨される。

注 - KM から提供される鍵データの場合、高度な将来のコンピュータテクノロジーによる攻撃に抵抗する場合でも、この長期的な機密性が要求されることがよくある。

転送された鍵データの長期的な秘密性を保持するために、鍵が QKDN 内の KM リンクを介して中継される場合、高度に安全な暗号化方式が採用されるべきである。

SReq.3.2　　QKDN は、鍵リレーに OTP 暗号化などの IT セキュアなプロトコルを使用することが推奨される。

また、OTP 鍵リレーに必要な数の鍵がない場合など、鍵管理ポリシーに応じて AES([b ISO/IEC 18033 3]、[b-FIPS PUB 197])などの他の適切な方式が選択できるべきである。

SReq.3.3　　QKDN は、個々の鍵中継に使用される暗号化方式を記録するためのメタデータを作成することが推奨される。このメタデータは、中継される鍵の鍵ライフサイクル管理にも使用される。

注- 暗号アプリケーションが、QKD モジュールによって生成された鍵と同じセキュリティレベルを持つ鍵を要求する場合、QKDN は、鍵リレー暗号化方式のメタデータを使用して、OTP 暗号化によってリレーされた鍵を選択すべきである。

SReq.3.4　　QKDN は、トラステッドノード内の QKD-KM リンクや KM-APP リンクを介して鍵が転送される場合、鍵データを暗号化することが推奨される。

SReq.3.5　　格納された鍵データの長期的な機密性を保持するために、安全な鍵格納と鍵漏洩防止技術の採用が推奨される。

SReq.4　　QKDN は、QKDN に保存され転送されるメタデータ、制御及び管理情報及びその他のデータの機密性を確保することが推奨される。

制御及び管理情報の機密性は、QKDN が運用されている間のみ保護されるべきであるため、ほとんどの場合、必ずしも IT セキュアのレベルではない。計算暗号アルゴリズム、例えば、ポスト量子暗号技術を適用することができる。

9.1.4. データの完全性

SReq.5　　QKDN は、保存及び転送されたデータの完全性を保護することが要求される。

データの完全性機能は、保存及び転送されたデータの正確性を保証する手段を提供し、交換されたデータの変更、削除、作成(挿入)、再生から保護をする手段を提供する。鍵データは、暗号アプリケーションで利用されるまで、転送と保存において完全性が保護されるべきである。制御及び管理情報は、QKDN が運用されている間、完全性が保護されるべきである。

ほとんどの場合、適切な計算量的安全性を備えた暗号アルゴリズムを使用できる。ポスト量子暗号技術は、それらの標準化と実際の展開に従って採用されるべきである。さらに、IT セキュアな方法([b-Wegman-Carter]メッセージ認証など)を使用して、データ転送の完全性を保護できる。

9.1.5. 可用性

9.1.5.1. 鍵の蓄積及び鍵リレー

SReq.6　　QKDN は、鍵データの可用性を保証することが推奨される。

この機能をサポートするためのセキュリティ対策は次のとおりである。

- KM での鍵データの蓄積。

- KM 及び KM リンクによる鍵リレー、及び鍵リレールートの再ルーティング。

この機能は、QKD モジュールの鍵生成性能と鍵管理ポリシーによって制限される。

9.1.5.2. ダメージ制御及び復旧

SReq.7　　QKDN は、ネットワークの回復性の能力が要求される。

ネットワークの回復性とは、セキュリティ上の脅威に直面しても許容可能なレベルのサービスを継続するために、中断を含む状況の変化に適応して回復する能力を持つことである。

注 - [b-NIST SP800 - 160-2]は、QKDN に適用できる回復性に関するセキュリティ対策(システムの冗長性、ネットワークのセグメント化など)を紹介している。

セキュリティ違反が検出された場合、この機能により管理された方法で確実に処理され、被害が最小限に抑えられる。さらに、システムの復旧を保証し、必要なセキュリティレベルでシステムを修復する。

9.1.5.3. QKD リンクへの DoS 攻撃に対する堅牢性

SReq.8　　QKDN は、DoS 攻撃への対策の実施が要求される。

DoS 攻撃は、9.1.5.2 節のシステムダメージカテゴリの一部として扱うことができる。ただし、この脅威を考慮することは、QKDN ならびに他のネットワーク(光トランスポートネットワークなど)にとって重要なセキュリティポイントである。QKD リンクに対する DoS 攻撃によって、鍵生成レートが低下する(0 になる)こともある。この問題は、バックアップ QKD リンクへの切り替えや鍵リレーの再ルーティングなど、適切な方法で軽減できる。

別のバックアップオプションとして、別の適切な鍵リレー方法を適用することも考えられる。例えば、(AES などの)ポスト量子暗号方式を使用するなどである。この場合、KM は鍵リレーの方法と関連パラメータを報告する必要がある。

QKD リンクの DoS 対策の詳細は、本標準の範囲外である。

9.1.6. 責任追跡性

SReq.9　　QKDN は、セキュリティ上の重要な行為の記録が、その行為を実行した機能要素に対して一意に追跡可能とすることが推奨される。

SReq.10　　QKDN は、鍵データのトレーサビリティをサポートすることが推奨される。

SReq.9 及び SReq.10 は、動作ログ(9.1.6.1 節を参照)及びセキュリティ監査(9.1.6.3 節を参照)の機能によってサポートされる。

責任追跡性の他の実現方法(ただし脆弱であるかもしれない)として、認証、アクセス制御、監査証跡の機能を適切に組み合わせることも考えられる。

9.1.6.1.　動作ログ

SReq.11　　QKDN は、QKDN 内のセキュリティ関連活動に関する情報を保存する能力を有することが推奨される。

QKDN の機能要素は、ログ機能と通信することができる。

9.1.6.2. セキュリティアラーム通知

SReq.12　　QKDN は、セキュリティイベントに関するアラーム通知を生成することが推奨される。

セキュリティアラーム通知は、セキュリティに関する操作情報である。

9.1.6.3. ログデータのセキュリティ監査

SReq.13　　QKDN は、セキュリティイベントに関するログデータを分析する能力を有することが推奨される。

注 - 監査は、システム管理の妥当性をテストし、確立されたセキュリティポリシー及び運用手順へのコンプライアンスを確保し、セキュリティの侵害を検出するために、システムの記録及び活動を独立してレビュー及び調査を行う。監査の結果、制御、ポリシー及び手順の変更が特定される。

9.2.　導入、サポート、保守、移行

SReq.14　　QKDN は、導入、サポート、保守及び移行の期間中、及びその後にも QKDN のセキュリティ制御を継続的に提供されるよう、これらの操作のためのセキュリティ対策を備えることが要求される。

QKDN を起動し運用を継続するには、導入、サポート、及びメンテナンスが必要である。

参考文献

[b-ITU-T T.411] ITU-T Recommendation T.411 (1993), *Information technology – Open Document Architecture (ODA) and interchange format: Introduction and general principles.*

[b-ITU-T X.800] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*

[b-ITU-T X.1038] ITU-T Recommendation X.1038 (2016), *Security requirements and reference architecture for software-defined networking*.

[b-ITU-T X.1193] ITU-T Recommendation X.1193 (2011), *Key management framework for secure Internet protocol television (IPTV) services*.

[b-ISO/IEC 18033-3] ISO/IEC 18033-3:2010, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.*

[b-ISO/IEC 27000] ISO/IEC 27000:2010, Information security management systems — *Overview and vocabulary*

[b-ETSI GR QKD 007] ETSI GR QKD 007, V1.1.1 (2018), *Quantum key distribution (QKD); Vocabulary*.

[b-FIPS PUB 197] Federal Information Processing Standards Publication 197 (2001), *Advanced encryption standard (AES).*

[b-NIST SP 800-160-2] Ross, R., Pillitteri, V., Graubart, R. Bodeau, D., McQuaid, R. (2019). Developing cyber resilient systems: A systems security engineering approach, NIST Special Publication 800-160, Volume 2. Gaithersburg, MD: National Institute of Standards and Technology. 205 pp. Available [viewed 2020-07-04] at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

[b-Wegman-Carter] Wegman, M.N., Carter, J.L. (1981). New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* 22, pp. 265-279