TTC標準
Standard

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
Security requirements and measures for quantum key distribution networks – key management

第 1.1 版

2024 年 5 月 29 日制定

一般社団法人
情報通信技術委員会

THE 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、2021 年 10 月に ITU-T SG17 において発行された ITU-T 勧告 X.1712 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	2022 年 2 月 24 日	制定
第 1.1 版	2024 年 5 月 29 日	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	X.1714
JT 標準	JT-X1710、JT-Y3800、 JT-Y3801 、JT-Y3802 、JT-Y3803

6. 標準作成部門

セキュリティ専門委員会

1. 適用範囲

本標準は次の項目を規定する。

- 量子鍵配送ネットワーク(QKDN)における鍵管理に対するセキュリティ脅威
- QKDN における鍵管理のための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

2. 参照文献

以下の ITU-T 勧告およびその他の参照文献は、本文中の参照を通じて本勧告の規定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るが、すべての勧告およびその他の参照文献は改訂の対象となる。したがって、本勧告の利用者は、以下に列挙された勧告およびその他の参照文献の最新版を適用する可能性を調査することが奨励される。現在有効な ITU-T 勧告のリストは定期的に公表されている。本勧告内で文書を参照することは、その文書に、独立した文書としての勧告としての地位を与えるものではない。

[ITU-T X.1710] Recommendation ITU-T X.1710 (2020), Security framework for quantum key distribution networks

[ITU-T X.1714] Recommendation ITU-T X.1714 (2020), Key combination and confidential key supply for quantum key distribution networks

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

[ITU-T Y.3801] Recommendation ITU-T Y.3801 (2020), Functional requirements for quantum key distribution networks

[ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), Quantum key distribution networks - Functional architecture

[ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), Quantum key Distribution network - Key management

3. 定義

3.1. 他の標準等で定義されている用語

本勧告は、以下の、他の標準等で定義される用語を使用する。

3.1.1　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。

3.1.2　鍵ライフサイクル[ITU-T Y.3800]：鍵が、鍵マネージャ(KM)によって受信され、ついで暗号アプリケーションで使用され、最終的に鍵管理ポリシーに従って削除または保存されるまでの一連のステップ。

3.1.3　鍵管理[ITU-T Y.3800]：暗号アプリケーションに提供し、鍵管理ポリシーに応じて削除または保存するために、量子レイヤからの受信、格納、フォーマット、リレー、同期、認証から始まる、そのライフサイクル中に鍵に対して実行されるすべてのアクティビティ。

3.1.4　鍵管理エージェント(KMA)[ITU-T Y.3802]：QKD ノード(トラステッドノード)内の量子鍵配送(QKD)モジュール/QKD モジュールによって生成された鍵を管理するための機能要素。

注 - KMA は、QKD モジュール/QKD モジュールから鍵を取得し、同期、サイズ変更、フォーマットおよび保存を行う。また、鍵管理エージェント(KMA)リンクを介して鍵をリレーする。

3.1.5　鍵管理エージェント鍵(KMA-鍵)[ITU-T Y.3803]：鍵管理エージェント(KMA)に格納および処理され、KMA と一致する KMA との間で安全に共有される鍵データ。

3.1.6　鍵管理エージェントリンク(KMA リンク)[ITU-T Y.3802]: 鍵リレーと鍵管理のための通信を行うために KMA を接続する通信リンク。

3.1.7　鍵マネージャ(KM)[ITU-T Y.3800]：量子鍵配送(QKD)ノードに配置され、鍵管理レイヤで鍵管理を実行する機能モジュール。

3.1.8　鍵管理リンク(KM リンク)[ITU-T Y.3800]:鍵管理を行う鍵マネージャ(KM)を接続する通信リンク。

3.1.9　鍵リレー[ITU-T Y.3800]：中間 QKD ノードを介して任意の量子鍵配送(QKD)ノード間で鍵を共有する方法。

3.1.10　鍵供給エージェント(KSA)[ITU-T Y.3802]：鍵管理エージェント(KMA)とクライアントの間に配置される、暗号アプリケーションに鍵を供給する機能要素。

注 - 暗号アプリケーションのアプリケーション・インタフェースは、鍵供給エージェント(KSA)に実装される。KSA は鍵を同期し、クライアントに提供する前に KSA リンクを介して鍵の完全性を検証する。

3.1.11　鍵供給エージェント-鍵 (KSA-key)[ITU-T Y.3803]：Key Supply Agent(KSA)に格納および処理され、KSA と一致する KSA との間で安全に共有される鍵データ。

3.1.12　鍵供給エージェントリンク(KSA リンク)[ITU-T Y.3802]：鍵同期と完全性検証を行うために KSA を接続する通信リンク。

3.1.13　メッセージ認証符号[ETSI GS QKD008]：データの偶発的な変更と意図的な変更の両方を検出するために対称鍵を使用するデータの暗号チェックサム。

3.1.14　量子鍵配送(QKD)[ETSI GR QKD007]：QKD は、量子情報理論に基づく情報理論的セキュリティを備えた対称暗号鍵を生成および配布するための手順または方法である。

3.1.15　量子鍵配送モジュール(QKD モジュール)[ITU-T Y.3800]：暗号機能および量子光学プロセスを実装するハードウェアおよびソフトウェアコンポーネントのセット。量子鍵配送(QKD)プロトコル、同期、鍵生成のための蒸留などが含まれ、定義された暗号境界内に含まれる。

注 - QKD モジュールは、鍵が生成されるエンドポイントモジュールとして機能する QKD リンクに接続されている。これらは 2 つのタイプの QKD モジュール、すなわち送信機(QKD-Tx)と受信機(QKD-Rx)である。

3.1.16　量子鍵配送 - 鍵(QKD-key)[ITU-T Y.3802]：一対の量子鍵配送 (QKD)モジュールによって生成される一対の対称ランダムビット列。特に、KM でサイズ変更およびフォーマットされる前のランダムビット列を指す。

3.1.17　量子鍵配送リンク(QKD リンク)[ITU-T Y.3800]：QKD を動作させるための 2 つの量子鍵配送(QKD)モジュール間の通信リンク。

注 - QKD リンクは、量子信号を伝送するための量子チャネルと、同期と鍵蒸留のために情報を交換するために使用される古典チャネルで構成されている。

3.1.18　量子鍵配送ネットワーク(QKDN)[ITU-T Y.3800]：2 つ以上の量子鍵配送(QKD)ノードが QKD リンクを介して接続されたネットワーク。

注 - QKDN は、QKD リンクを介して直接接続されていない場合、鍵リレーによって QKD ノード間で鍵を共有することを可能にする。

3.1.19　量子鍵配送ネットワークコントローラ(QKDN コントローラ)[ITU-T Y.3800]：量子鍵配送(QKD)制御レイヤに配置され、QKD ネットワークを制御するための機能モジュール。

3.1.20　量子鍵配送ネットワークマネージャ(QKDN マネージャ)[ITU-T Y.3800]：量子鍵配送(QKD)ネットワーク管理レイヤに配置され、QKD ネットワークを監視および管理するための機能モジュール。

3.1.21　量子鍵配送ノード(QKDN ノード)[ITU-T Y.3800]：1 つまたは複数の量子鍵配送(QKD)モジュールを含むノードで、不正なパーティによる侵入および攻撃から保護されている。

注 - QKD ノードには、鍵マネージャ(KM)を含めることができる。

3.1.22　量子鍵配送プロトコル(QKD プロトコル)[ITU-T X.1710]：量子情報理論に基づく情報理論的セキュリティを使用して対称暗号鍵を確立する手順のリスト。

3.1.23　セキュリティ分界点[ITU-T Y.3800]：鍵の使用に関する別のレイヤの責任から提供される鍵に関する 1 つのレイヤの責任を区別するための境界。

3.1.24　ユーザーネットワーク[ITU-T Y.3800]：量子鍵配送 (QKD)ネットワークによって供給される鍵を暗号アプリケーションが消費するネットワーク。

3.2.　本勧告内で定義した用語

なし

4.　略語及び頭字語

本勧告では、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)
DoS	Denial of Service (サービス妨害)
ID	Identifier (識別子)
IT-secure	Information Theoretically secure (情報理論的安全性)
KM	Key Manager (鍵マネージャ)
KMA	Key Management Agent (鍵管理エージェント)
KSA	Key Supply Agent (鍵供給エージェント)
MAC	Message Authentication Code (メッセージ認証符号)
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)

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

QKD ネットワーク(QKDN)は、データの長期的な機密性を保護するために、暗号アプリケーションに安全な鍵を提供することを可能にする。QKDN の基本的な機能とレイヤ構造は[ITU-T Y.3800]で定義されている。機能要求条件とアーキテクチャはそれぞれ[ITU-T Y.3801]と[ITU-T Y.3802]で規定されている。QKDN のセキュリティフレームワークは、[ITU-T X.1710]で規定されている。この勧告は、QKDN に対するセキュリティ脅威および対処、QKDN に対する一般的なセキュリティ要求条件とセキュリティ対策の導出について規定している。

本標準は、QKDN の鍵管理のセキュリティ問題を扱い、[ITU-T Y.3803]で記述された鍵管理フレームワークに基づいて、鍵管理のためのセキュリティ要求条件を 3.1.3 節で規定する。[ITU-T Y.3800]で規定されたレイヤモデルにおける鍵管理レイヤが、この勧告で考慮される唯一のレイヤである。さらに、鍵管理レイヤと以下に列挙された他のレイヤとの間のインタフェースはこの勧告の適用範囲内である。

- 量子レイヤ
- QKDN 制御レイヤ
- QKDN 管理レイヤ
- サービスレイヤ

7. QKDN における鍵管理において保護すべき情報資産

QKDN における鍵管理において保護すべき情報資産は、以下のとおりである。

7.1. 鍵データ

鍵データはランダムビット列で構成される。個々の鍵データは対称暗号鍵として使用できる。

鍵管理のプロセスには、次のような鍵データがある。

- QKD-鍵: QKD モジュールによって生成され、KMA によって取得された鍵データ。
- KMA-鍵: QKD-鍵を所定のサイズに結合または分割することによって、KMA によってサイズ変更された鍵データ。
- KSA-鍵: 要求された鍵長に従って KMA から KSA に転送される鍵データで、暗号アプリケーションに供給される。

7.2. メタデータ

メタデータは、鍵データおよび鍵管理に関する属性情報である。このような情報には、次の情報が含まれるが、これらに限定されない。

- 鍵 ID (QKD-鍵 ID、KMA-鍵 ID、送信元 KMA-鍵 ID、KSA-鍵 ID)
- 生成タイムスタンプ

- QKD モジュール ID
- 組合わせ QKD モジュール ID

注 1 - QKD モジュール X の場合、QKD モジュール X が QKD リンクを介して直接接続されている他の QKD モジュール Y は、組合わせ QKD モジュールと呼ばれる。

- 鍵の長さ
- ハッシュ値
- 鍵の種類(暗号化鍵/復号化鍵)
- KMA ID
- 送信元 KMA ID
- 組合せ KMA ID

注 2 - KMA X の場合、KMA X が KMA リンクを介して直接接続されている他の KMA Y は、組合せ KMA と呼ばれる。

- 宛先 KMA ID
- 鍵リレーのタイムスタンプ
- 関連するパラメータを含む鍵リレー暗号化方式
- KMA-鍵メタデータ
- 供給タイムスタンプ
- アプリケーション名
- アプリケーション送信元 ID
- アプリケーション送信先 ID など。

上記の項目は必ずしも必須ではなく、オプションである。

7.3. 制御と管理情報

鍵管理に関連する制御と管理情報は、次のとおりである。

- 鍵管理レイヤの KMA および KSA リンクを介して通信される鍵管理情報
- 鍵管理レイヤと QKDN 制御レイヤの間の制御リンクを介して通信される QKDN 制御情報
- 鍵管理レイヤ、QKDN 制御レイヤおよび QKDN 管理レイヤの間で交換される QKDN 管理情報
- 鍵管理レイヤと量子レイヤの間のリンクを介して通信される QKD モジュールのステータス情報。

8. QKDN における鍵管理のセキュリティ脅威

本標準で使用される鍵管理のフレームワークと機能要素は、勧告[ITU-T Y.3803]に記述されている。この節は、QKDN の鍵管理に対する本質的なセキュリティ脅威に焦点を当てている。

[ITU-T Y.3800]および[ITU-T Y.3802]で定義されている QKD リンク、KMA リンク、および KSA リンクに加えて、この標準は、この節の中の以下のリンクを参照する。

- 鍵供給リンク：QKD モジュールと KMA、KMA と KSA、KSA と暗号アプリケーションを接続し、それぞれ QKD 鍵、KMA 鍵、KSA 鍵を供給するための通信リンクである。また、メタデータや関連パラメータも送信する。

- 制御と管理リンク：制御と管理情報を伝送するための通信リンク。これらのリンクは、QKDN のコントローラとエンティティ、QKDN マネージャとエンティティ、または QKD モジュールと KM を接続する。

QKDN における鍵管理に対する攻撃対象領域は、図 1 に赤丸で要約されている。鍵データを伝達するリンクは次のとおりである。

1) KMA リンクおよび鍵供給リンク。QKD モジュールと KMA の間のリンク、KMA と KSA の間のリンク、および KSA と暗号アプリケーションの間のリンクを含む。

一方、鍵データを伝達しないリンクには、次のものがある。

2) KSA リンク

3) KM に接続された制御と管理リンク

注 1 - いったん鍵データが KSA から暗号アプリケーションに供給されると、アプリケーションは鍵データとその使用に責任を負う。

注 2 - 以下の項目は、本勧告の適用範囲外である。

(i) 鍵管理レイヤ外の機能エンティティ(例えば、QKD モジュール、QKDN 制御装置、QKDN マネージャ)に対する攻撃

(ii) KM に直接接続されていないリンク(例えば、量子チャネルおよび古典チャネルを含む QKD リンク)に対する攻撃

(iii) KM に対するインサイダー攻撃

注 3 – インサイダー攻撃とは、当該 QKDN に合法的に関与する組織内の行為に起因する攻撃を意味する。例えば、QKDN の信頼できる事業者、その取引関係者、または QKDN 内の管理された場所へのアクセス権を有する部外者による、詐欺などによる悪意のある攻撃等。

(iv) KM に対するサイドチャネル攻撃、トラップドア、ヒューマンエラーおよび自然災害

注 4 - KM の機能がデジタルであると仮定すると、(iv)のサイドチャネル攻撃は、これらのデジタル(量子ではない)機能に対するものである。潜在的な攻撃には、例えば、電力分析、タイミング分析、障害誘導及び TEMPEST が含まれる。

各攻撃対象領域では、次のようなセキュリティ脅威が発生する可能性がある。

- なりすまし
- 盗聴
- 削除または破損
- システム・リソースの破壊
- サービス妨害(DoS)

注 5 - セキュリティ脅威の用語の意味は[ITU-T X.1710]で規定されている。(iii)および(iv)の制限の下でも、リンクに対して中間者攻撃などの悪意のある攻撃が行われ、KM のそれらの機能要素に影響が及ぶ可能性があるため、KMA および KSA は、図 1 に記載されたセキュリティ脅威に悩まされることになる。

図 1 に示すように、KMA と KSA (どちらも鍵を処理する)は、適切な鍵管理のためにトラステッドノード内に配置する必要がある。ほとんどの場合、鍵供給リンクもトラステッドノード内に配置される。

注 6 - ほとんどの場合、暗号アプリケーション、QKDN コントローラおよび QKDN マネージャは、トラステッドノード内に配置される。一方、暗号アプリケーションがトラステッドノード内で鍵を受信しても、トラステッドノード外で鍵を消費する場合もある。典型的な例としては、スマートフォンやドローンなどのモバイル端末での暗号アプリケーションがあ

る。この場合、KSA と暗号アプリケーション間の鍵供給リンクは、トラステッドノード内に配置されている場合とされていない場合がある。

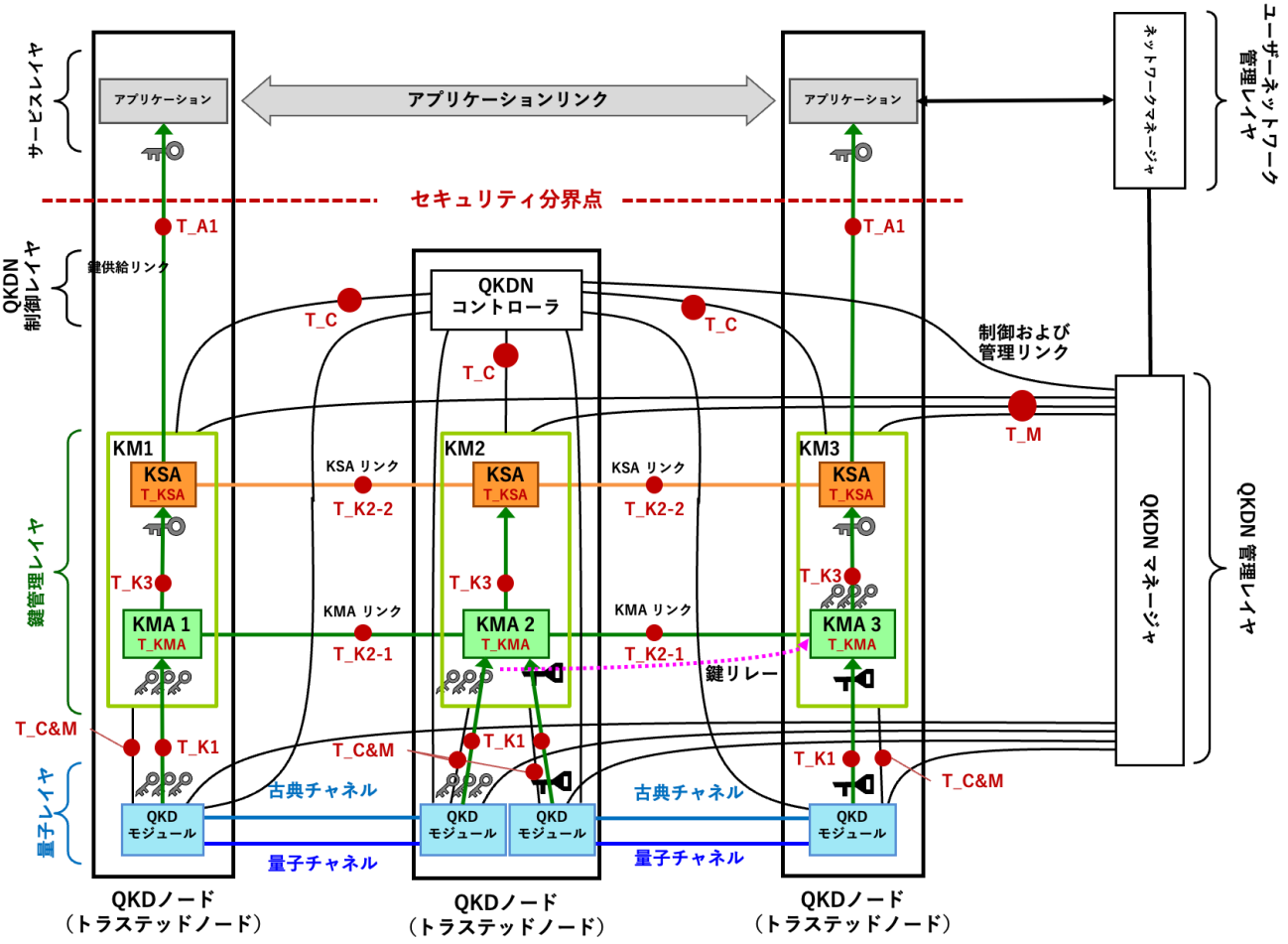

図 1 - QKDN の鍵管理の攻撃対象領域(赤丸)

注 7 - 図 1 では、鍵供給リンクと KMA リンクは緑色、KSA リンクはオレンジ色、制御リンクと管理リンクは黒色で示されている。

8.1. KMA リンク (T_K2-1)および鍵供給リンク (T-K1、T_K3、T_A1) に対する脅威

図 1 に緑色で示されているリンクは、鍵データ、メタデータ、および制御情報と管理情報を伝達する。リンクに関連する潜在的な脅威は次のとおりである。

- 盗聴：鍵データ、メタデータ、および制御と管理情報を傍受および解読すること。
- 削除または破損：鍵データ、メタデータ、制御・管理情報の削除や変更。
- DoS（サービス妨害）：通信の中断やデータトラフィックの輻輳。

8.2. KSA リンクに対する脅威(T_K2-2)

図 1 のオレンジ色で示されているリンクは KSA リンクであり、このリンクを介してメタデータ、制御、および管理情報が交換される。

- 盗聴：KSA リンク上のメタデータ、制御と管理情報を傍受および解読すること。
- 削除または破損：KSA リンク上のメタデータ、制御と管理情報の削除または変更。
- DoS（サービス妨害）：通信の中断またはデータトラフィックの輻輳。

8.3. 制御リンクと管理リンクに対する脅威 (T_C、T_M、T_C&M)

図 1 では、制御リンクと管理リンクが黒で示されている。これらのリンクは、メタデータ、制御情報、および管理情報を伝達する。

- 盗聴：メタデータ、制御と管理情報を傍受および解読すること。
- 削除または破損：メタデータ、制御情報および管理情報の削除または変更。
- DoS（サービス妨害）：通信の中断またはデータトラフィックの輻輳。

8.4. KMA および KSA (T_KMA、T_KSA)に対する脅威

KMA リンク、KSA リンク、鍵供給リンクを介した KMA および KSA のセキュリティ脅威には、次のものがある。

- なりすまし：攻撃者が KMA および KSA 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悪意をもって捏造し、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か、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。
- 盗聴：鍵データおよびメタデータを傍受および解読すること。
- 削除または破損：鍵データおよびメタデータの削除または変更。
- システムリソースの破壊：機器に対する物理的な攻撃。

9. QKDN における鍵管理の情報資産に対するセキュリティ要求条件及びセキュリティ対策

前項で取り上げたセキュリティ脅威から情報資産を保護するために、資産ごとにセキュリティ要求条件とセキュリティ対策が導出される。

セキュリティ要求条件を満たすための鍵管理のためのセキュリティ対策は、[ITU-T Y.3803]で規定された鍵管理の手順に従って検討される。この手順には、QKD モジュールからの鍵取得、鍵同期、鍵の保管、KMA における鍵リレー、および KSA から暗号アプリケーションへの鍵供給が含まれる。

注 1 - 表 1、2 および 3 に記載されたセキュリティ要求条件および対策は、KMA および KSA を対象とするが、それらの一部は、KMA および KSA のみによって実施されるものではない。これらは、対応するエンティティと連携して実施されるべきである。

注 2 - 表 1、2 及び 3 に掲げるセキュリティ対策は、必要であるが、対応するセキュリティ要求条件を満たすには十分ではない。けれどもセキュリティ対策の中には、複数のセキュリティ要求条件を満たしているものもある。

注 3 - QKDN 内のエンティティおよびメッセージの認証および認可の詳細は、本勧告の適用範囲外である。

9.1. 鍵データのセキュリティ要求条件と対策

鍵データのセキュリティ保護に関する要求条件と対策を表 1 に要約する。

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

	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。

(ii) 完全性	鍵データは変更されない。	SReq.7　KMA は、管理する鍵データの完全性を確保することを要求される。 SReq.8　KSA は、管理する鍵データの完全性を確保することを要求される。	- SReq.7 に対して、以下の (i)、(ii) および (iii) 項を実施する。 (i) KMA は、QKD モジュールから受信した QKD 鍵の完全性を検証する。 (ii) KMA が受信した QKD 鍵から KMA 鍵を作成する場合、KMA は KMA 鍵の処理の完全性をチェックする。 (iii) KMA は、他の KMAs から受信した KMA 鍵の完全性を検証する。 - SReq.8 に対して、以下の項目(i)および(ii)を実施する。 (i) KSA は、KMA から受信した KMA 鍵の完全性を検証する。 (ii) KSA が受信した KMA-鍵から KSA-鍵を作成する場合、KSA は KSA-鍵の処理の完全性をチェックする。 - SReq.7 および SReq.8 に対して、KMA および KSA は、不正改造防止対策および/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 2 - 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装することができる。
(iii) 認証及びアクセス制御	鍵データは許可されたエンティティから取得され、鍵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.9　KMA および KSA は、送信エンティティの ID が認証され、鍵データを提供する権限が付与されていない限り、他のエンティティから受信した鍵データを信頼しないことを保証することを要求される。 SReq.10　KMA および KSA は、暗号化されていない鍵データへのアクセスを他のエンティティに許可しないことを要求される。	- SReq.9 および SReq.10 に対して、KMA および KSA は、例えば、それらが通信する他のエンティティとの相互認証を実行するか、または他のアプローチを利用することができる。 - SReq.9 および SReq.10 に対して、KMA および KSA には、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がある。

(iv) 可用性	鍵データは、必要に応じていつでも使用できる。	SReq.11　KMA には、鍵データを格納する機能を要求される。 SReq.12　KMA は、2 つの QKD ノード間に直接の QKD リンクがない場合でも、KSA から要求されたときに鍵データを提供することが推奨される。	- SReq.11 に対して、KMA には鍵ストレージ用の一定量のストレージ・スペースがある。 - SReq.12 に対して、QKD ノードがそれらの間に直接 QKD リンクを持たない場合、QKD ノードの KMA は 2 つのエンドポイント KMA 間で鍵リレーを実行して、ルーティング、再ルーティングおよび他の可能なアクションのために QKDN コントローラの制御下で必要な量の KMA 鍵を共有する。
(v) 責任追跡性	鍵のライフサイクルはトレース可能である。	SReq.13　KMA および KSA には、要求に応じて鍵をトレースすることを要求される。 SReq.14　鍵リレーの暗号化方式と関連するパラメータを、QKDN コントローラおよび／または QKDN マネージャに通知することが、KMA に推奨される。	- SReq.13 に対して、KMA および KSA は、鍵ライフサイクル管理のために、鍵 ID などのメタデータを作成および格納する。 - SReq.14 に対して、KMA は、メタデータおよび関連するパラメータを作成し、それらを QKDN コントローラおよび/または QKDN マネージャに送信する能力を有する。 注 3 - 代替的に、鍵リレーのための固定暗号化方式を有する KMA の場合、QKDN コントローラおよび QKDN マネージャは、KMA 暗号化方式を用いて初期化し、それらに関連パラメータを構成に追加することができる。 注 4 - QKDN コントローラおよび／または QKDN マネージャへの情報提供のための実際のアクションは、実装に依存する。

注 5 - 機密性に関しては、鍵リレー機能は、IT セキュアで保護された暗号化を採用することができる。例えば、IT セキュアで保護された鍵リレーに必要な量の鍵が利用できない場合、少なくとも 256 ビットの対称鍵を使用する AES のような対称鍵暗号を持ついくつかのバックアップ鍵リレー方式は、[ITU-T X.1714]に記述されているように実装する必要がある。

注 6 - 認証は、IT セキュアで保護された認証または公開鍵証明書による認証などによって行うことができる。

注 7 - Wegman-Carter 認証 [b-Wegman-Carter]は、almost strongly universal$_2$ ハッシュ関数に基づく IT セキュアで保護されたメッセージ認証符号の例である。

9.2.　メタデータに関するセキュリティ要求条件および対策

メタデータのセキュリティ保護に関する要求条件と対策を表 2 に要約する。

表 2 - メタデータのセキュリティ要求条件および対策

	内容	セキュリティ要求条件	セキュリティ対策
(1) 機密性	メタ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.15　KMA は、KMA リンクおよび鍵供給リンク内のメタデータの機密性を、これらを介して送信される際に、QKD モジュールと連携して確保することが推奨される。 SReq.16　KSA は、KSA リンクおよび鍵供給リンクのメタデータの機密性を、これらを介して送信される際に、暗号アプリケーションと連携して確保することが推奨される。 SReq.17　KMA と KSA は、KMA と KSA で処理されるか格納される際に、メタデータの機密性を確保することが推奨される。	- SReq.15 および 16 に対して、メタデータの機密性は適切な手段によって保護される。これには、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が含まれる。 - SReq.17 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。

(ii) 完全性	メタデータは変更されない。	SReq.18　KMA は，自らが管理するメタデータの完全性を確保することを要求される。 SReq.19　KSA は，自らが管理するメタデータの完全性を確保することを要求される。	- SReq.18 に対して、以下の(i)、(ii) および (iii) 項を実施する。 (i) KMA は、QKD モジュールから受信したメタデータの完全性を検証する。 (ii) KMA が、受信した QKD 鍵から KMA 鍵を作成する場合、KMA は、KMA 鍵のメタデータの処理の完全性をチェックする。 注 2 - KMA 鍵のメタデータの処理の完全性のチェックには、KMA とそれに対応する KMA が含まれる場合がある。 (iii) KMA は、他の KMA から受信したメタデータの完全性を検証する。 - SReq.19 に対して、以下の(i)および (ii) 項を実施する。 (i) KSA は、KMA から受信したメタデータの完全性を検証する。 (ii) KSA が受信した KMA-key から KSA-key を作成する場合、KSA は KSA-key のメタデータの処理の完全性をチェックする。 注 3 - KSA 鍵のメタデータの処理の完全性のチェックには、KSA および対応する KSA が関与する場合がある。 - SReq.18 および SReq.19 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 4 - 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。

(iii) 認証及びアクセス制御	メタデータは許可されたエンティティから取得され、メタ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.20　KMA および KSA は、送信エンティティの ID が認証され、メタデータを提供する権限が付与されていない限り、他のエンティティから受信したメタデータが信頼しないことを保証することを要求される。 SReq.21　KMA および KSA は、メタデータを受信する権限が付与されていない限り、他のエンティティが暗号化されていないメタデータへのアクセスを許可しないことを要求される。	- SReq.20 および SReq.21 に対して KMA および KSA は、例えば、それらが通信する他のエンティティとの相互認証を実行するか、または他のアプローチを利用することができる。 - SReq.20 および SReq.21 に対して、KMA および KSA には、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がある。
(iv) 可用性	該当なし	該当なし	該当なし
(v) 責任追跡性	該当なし	該当なし	該当なし

9.3.　制御と管理情報に関するセキュリティ要求条件及び対策

制御と管理情報のセキュリティ保護に関する要求条件および対策を表 3 に要約する。

注 - KM がセキュリティ要求条件の対象である場合、その 1 つ以上の実装された機能がこの要求条件に対して責任がある。KM に実装可能な機能には、Y.3802 で規定されている KMA、KSA または KM の制御と管理が含まれる。

表 3 – 制御と管理情報のセキュリティ要求条件および対策

	内容	セキュリティ要求条件	セキュリティ対策
(i) 機密性	制御と管理情報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.22　KM は、制御リンクおよび管理リンクを介して送信される場合に、制御情報および管理情報の機密性を確保することが推奨される。	- SReq.22 に対して、KM は適切な暗号化方式によって制御リンクおよび管理リンク内の制御情報および管理情報を保護する。
(ii) 完全性	制御と管理情報は変更されない。	SReq.23　KM は、管理対象の制御と管理情報の完全性を確保することを要求される。	- SReq.23 に対して、KM は伝達された制御と管理情報の完全性を確保する。
(iii) 認証及びアクセス制御	制御と管理情報は許可されたエンティティから取得され、制御と管理情報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.24　KM は、他のエンティティから受信した制御と管理情報が、送信側のエンティティの身元が認証され、制御と管理情報を提供する権限が与えられていない限り、信頼しないことを保証することを要求される。 SReq.25　KM は、暗号化されていない管理情報を受け取る権限があることを確認せずに、他のエンティティにその情報へのアクセスを許可しないことを要求される。	- SReq.24 および SReq.25 に対して、KM は、例えば、それらが通信する他のエンティティとの相互認証を実行するか、または他のアプローチを利用することができる。 - SReq.24 および SReq.25 に対して、KM は属性を処理し、アクセス制御セキュリティポリシーを実装する機能を持つ。
(iii)可用性	該当なし	該当なし	該当なし
(v)責任追跡性	該当なし	該当なし	該当なし

9.4.　損失と破損、および DoS（サービス妨害）

情報の損失は、データの損失を検出して再送信することで対策できる。さらに、ファイアウォールや侵入防御システム(IPS)などによる適切なパケットフィルタリングと連動して、制御されたアクセスによって DoS（サービス妨害）から保護できる。

参考文献

[b-ETSI GS QKD 005] Group Specification ETSI GS QKD 005 (2010), *Quantum Key Distribution (QKD); Security Proofs*

[b-ETSI GR QKD 007] Group Report ETSI GR QKD 007 (2018), *Quantum Key Distribution (QKD); Vocabulary.*

[b-ETSI GS QKD 008] Group Specification ETSI GS QKD 008 (2010), *Quantum Key Distribution; QKD module security specification*.

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