TTC標準
Standard

JT-Y3800

量子鍵配送ネットワークの概要

Overview on networks supporting quantum key distribution

第 1.0 版

2020 年 11 月 12 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概要について規定しており、2019年10月にITU-T SG13において発行されたITU-T勧告Y.3800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	2020年11月12日	制定

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	Q.1743
ISO/IEC標準	ETSI GR QKD007, ETSI White pager 8, ISO/IEC 18033-3

6. 標準作成部門

ネットワークビジョン専門委員会

序文

量子鍵配送(Quantum Key Distribution (QKD))技術は、対称ランダムビット列を安全な鍵として配送する手段を提供し、無制限な計算資源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。AI、量子計算などのコンピューティング技術が急速に進歩するにつれ、QKD技術は重要なデータの伝送の安全性を確保するために重要であると期待されている。

QKDは、通信ネットワークへアドオンする技術とサービスである。QKDネットワーク(QKDN)は、QKDの到達可能性と可用性を拡張するための技術である。QKD技術には独自の特徴と制限があり、QKDNを現在の通信網と暗号インフラに導入することは、ネットワークアーキテクチャと考慮すべきセキュリティの設計に新しい挑戦をもたらす。例えば、QKDは特定の物理チャネル、すなわち基本的にポイントツーポイントリンク技術である量子チャネルを必要とする。QKDによって生成された鍵は、さまざまなネットワークセキュリティの脅威を考慮しながら、ネットワーク内で適切に管理され、リレーされなければならない。

そのため、ネットワークにおけるQKD技術の利用に関する標準を確立する強い必要性がある。本標準は、明確なセキュリティ境界を持つ基本的なQKDNの概念的構造の概要を提供する。これは、ネットワークアーキテクチャ、ネットワークセキュリティなど、さまざまな側面をカバーする一連のQKDN標準シリーズの最初の標準である。要求条件は、更なる検討を必要とする。QKDと関連技術は急速に進歩しているため、将来的には新しい技術や概念構造が出現する可能性がある。本標準は、技術と標準化の将来の進展を考慮するために改訂されかもしれない。

1　規定範囲

標準 Y.3800 は、QKD(Quantum Key Distribution) をサポートするネットワークの概要を規定し、QKD 技術を実装するためのネットワークの側面を扱う。本標準は、特に以下の内容について記述している。

- QKD 技術の概要
- QKD をサポートするネットワーク能力
- QKD ネットワークの概念的構造と基本機能

2　参考文献

無し。

3　定義

3.1　本標準以外で定義されている用語

本標準は、本標準以外で定義された次の用語を使用する。

3.1.1　古典チャネル [b-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。

3.1.2　Quality of Service(QoS)[b-ITU-T Q.1743]：サービスのユーザーの満足度を決定するサービスパフォーマンスの総合的な効果。この機能は、次のようなすべてのサービスに適用されるパフォーマンス要素の組み合わせによって特徴付けられる。

- サービスの操作性パフォーマンス；
- サービスのアクセス性パフォーマンス；
- サービスの保持性パフォーマンス；
- サービスの完全性パフォーマンス；
- および各サービスに固有のその他の要因。

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

3.1.4　量子鍵配送 (QKD)[b-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および配送する手順または方法。

3.2　本標準で定義する用語

本標準では、次の用語を定義する。

3.2.1　アプリケーションリンク：ユーザネットワークで暗号アプリケーションを提供するために使用される通信リンク。

3.2.2　情報理論的安全性 (ITセキュア)：無制限の計算資源による解読攻撃に対する安全性。

3.2.3　鍵ライフサイクル：鍵マネージャ (KM) の鍵受信から、暗号アプリケーションでの鍵利用と鍵管理ポリシーによる削除または保存までの一連の処理。

3.2.4　鍵管理：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。

3.2.5　鍵マネージャ (KM)：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。

3.2.6　鍵マネージャ(KM) リンク：鍵マネージャ(KM) を接続し、鍵管理を行う通信リンク。

3.2.7　鍵リレー：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。

3.2.8　鍵供給：鍵を暗号アプリケーションに提供する機能。

3.2.9　QKD モジュール：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およ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) および受信器 (QKD- Rx) がある。

3.2.10　QKD リンク：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。

3.2.11　QKD ネットワーク (QKDN)： 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。

3.2.12　QKDN コントローラ：QKDN を制御するために QKDN制御レイヤに位置する機能モジュール。

3.2.13　QKDN マネージャ：QKDN を監視および管理するために QKDN管理レイヤに位置する機能モジュール。

3.2.14　QKD ノード：許可されていない当事者による侵入およ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。

3.2.15　セキュリティ分界点： 供給される鍵に対する1つのレイヤの責任と、鍵の使用に対する別のレイヤの責任を区別する境界。

3.2.16　ユーザネットワーク： QKDN によって供給される鍵を暗号アプリケーションが利用するネットワーク。

注：本標準では、”鍵”は”QKDNによって供給される対称ランダムビット列を意味する。

4　略語と頭文字

AES	Advanced Encryption Standard
API	Application Programming Interface
HMAC	Hash based message authentication code
ICT	Information and Communication Technology
ID	Identifier
IT-secure	Information-Theoretically secure
KM	Key Manager

MDI-QKD	Measurement Device Independent QKD
OTP	One-Time Pad
P-to-P	Point-to-Point
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKDN	QKD Network
QoS	Quality of Service
QKD-Rx	QKD Receiver
TF-QKD	Twin Field QKD
QKD-Tx	QKD Transmitter

5　表記法

無し。

6　QKD技術の概要

6.1　QKD 技術

QKD プロトコルは、対称なランダムビット列を安全な鍵として共有する手段を提供する。この鍵は、いくつかの仮定を含むセキュリティ証明モデルにおいて、無制限な計算資源を持つ盗聴者に対しても安全であることが証明できる。この種のセキュリティは、情報理論的安全性と呼ばれる。QKDプロトコルは量子力学の法則に基づいており、セキュリティの実装は考慮すべきである。[b-ETSI ETSI White Paper No.8]、[b-IEEE Trans.Inf.Theory39,733(1993)]。 QKDプロトコルを実装したQKDモジュールによって生成される鍵は、例えば、ワンタイムパッド(OTP) 暗号化[b-Shannon]、高度暗号化標準 (AES) [b-ISO/IEC 18033-3], [b-FIPS PUB 197]およびハッシュ・ベース・メッセージ認証コード(HMAC) 認証[b-FIPS PUB 198]など、対称鍵を用いる任意の暗号アプリケーションによって利用される。

QKD の基本要素は、送信機 (QKD-Tx) と受信機 (QKD-Rx) で、それぞれ QKDモジュールと呼ばれる。QKD リンクはQKDモジュールを接続し、量子リレーポイントを使用する場合がある(6.2項参照)。鍵は QKD リンクを介して共有される。QKDリンクは、通常量子チャネルと古典チャネルで構成される。量子チャネルは、ランダムビット列を送信するために、光の単一光子レベルコヒーレント状態などの量子信号の送信に用いられる。古典チャネル は、QKD モジュール間の同期とデータ交換のために用いられる。図1は、QKD を適用してポイントツーポイント (P-to-P) アプリケーションリンクを保護する例を示している。QKD モジュールは鍵を生成し、アプリケーションに供給する。暗号化データが送信されるアプリケーションリンクは、従来のネットワークまたは将来のネットワークにおける任意の通信リンクである。従って QKD は、既存または将来のネットワークへのアドオン技術 (サービス) である。この状況は、下記のようにQKD がネットワーク化されている場合でも同様である。QKDプロトコルは、QKDモジュールに一定の実装前提条件の下で情報理論的安全性 (IT セキュア) であることが証明可能である。QKD の情報理論的安全性は、量子の法則と量子理論によって保証されている。ただし、このセキュリティ様相の詳細は、本標準の範囲外である。

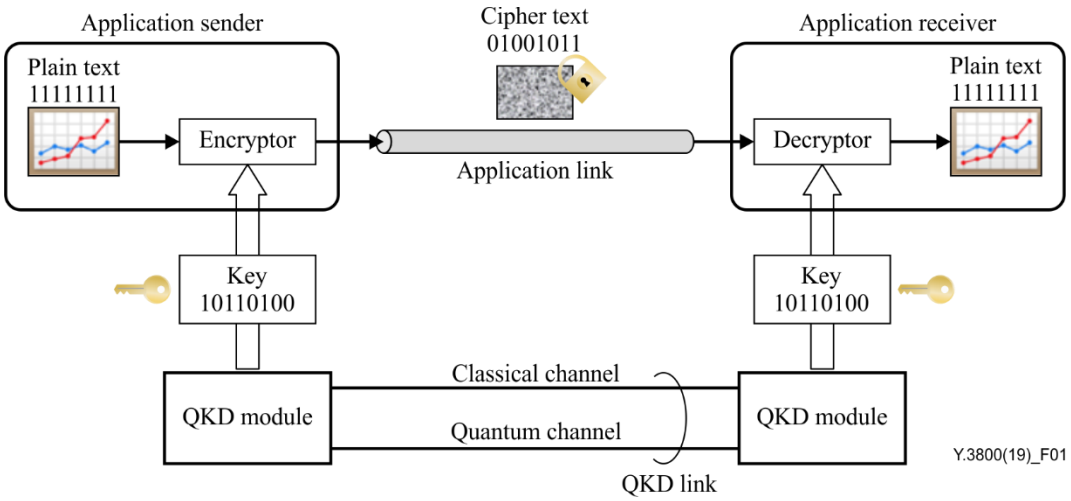

図1 P-to-P アプリケーションリンクを保護する QKD の構成例

6.2　QKDNとユーザネットワークの関係

一対のQKD モジュールは、P-to-P QKD リンクによって接続された 2 つの当事者間で鍵を共有することができるが、ユーザネットワーク内の 2 以上の指定された当事者が、様々な暗号アプリケーションの鍵を共有することができることが望ましい。さらに、P-to-P QKD リンクをマルチポイント QKDN に拡張することが好ましい。以下のいくつかの方法が可能である。

- 光スイッチまたはスプリッタ：光スイッチまたはスプリッタは、マルチポイントネットワークのQKDモジュールのペア間で QKDリンクトラフィックを切り替えたり分配したりすることができる。これにより、オンデマンドで異なるユーザ間で鍵を生成することができる。

- トラステッドリレー：この方式では、鍵は QKD ノード (トラステッドノード) に格納され、OTP が推奨される高度に安全な暗号化によって他の 遠隔QKDノードにリレーされる。現在、これ方式は長距離 QKDファイバネットワークで広く採用されている唯一知られたソリューションである。QKD ノード (トラステッドノード) は、不正なすべての当事者による侵入と攻撃に対して安全であると想定される。

- 測定支援リレー：測定装置非依存 QKD(MDI-QKD) およびツインフィールド QKD(TF-QKD) は、QKD リンクの範囲を拡張する技術であり、それによって鍵をより長い距離またはより高い損失のチャネル上で生成することが可能になる。MDI-QKD および TF- QKD は、リンク内の中間測定ステーションを使用する。これは、(トラステッドリレーの状況とは対照的に) 保護された場所に置かれたり、その動作が信頼できる必要はない。

- 完全な量子ネットワーク：完全な量子ネットワークでは、情報は中間ノードの量子形式で保持され、ノードでの保護だけでなく、ノード間の量子チャネルでの移動も保護される。量子リピータは、リンクに沿って配置された一連の中間ステーション間の量子もつれによる配送によって動作する。理論的には、このようなアプローチは、中間ステーションが信頼される必要がないため、鍵を長距離にわたって配送する理想的なソリューションとなる。

注1：量子リピータ技術は、量子メモリまたは量子エラー補正技術を必要とし、これは現在の技術では実用的な実装ではない。

図2は、これらの手段を組み込んだ QKDNと、鍵が供給されるユーザネットワークとの論理的な関係を示している。

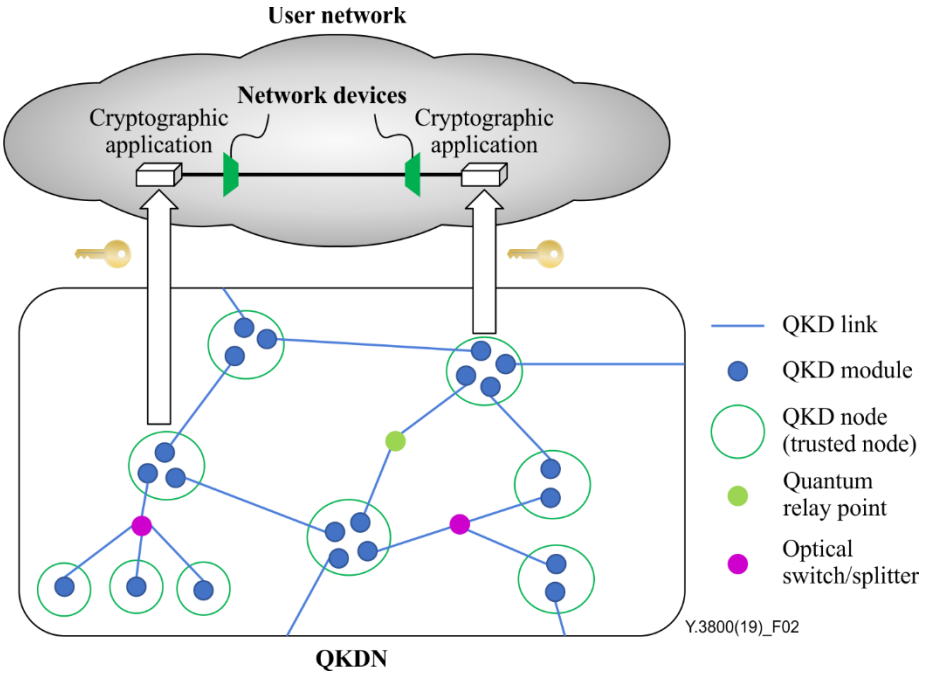

図 2 QKDNとユーザネットワークとの関係に関する一般的な概念と技術

鍵はQKD ノード間で共有され、 QKD ノードは鍵を共有するノード、または鍵リレーポイントとして機能し、QKD の範囲を拡張する。これとは対照的に、光スイッチのリレーポイントと MDI-QKD、TF QKD、量子リピータは量子リレーポイントと呼ばれ、量子信号のリレーポイントであり、必ずしも信頼されたものではない。

これらの信頼されたリレーポイントや信頼されないリレーポイントのおかげで、同じ QKDN内の任意の QKD ノード間で鍵を共有することができる。量子リレーポイントでは、鍵を生成したり共有したりすることはない。従って、QKDNの枠組みにおいて、量子リレーポイントは QKD リンクに含まれ、QKDNのより長い距離または柔軟なトポロジを提供する。これらの手段の技術的詳細の説明は、この標準の範囲外である。

前段落での所見から、本標準ではトラステッドノードに基づいた QKDNに焦点を当てている。

注2：QKDNタイプとユーザネットワークとの連携方法は、多様である。このような多様性により、いくつかの自由度を記述することができる。(多様性の例は付録 I 参照)。

注3：QKDNおよびユーザネットワークの物理およびソフトウェア実装は、さまざまな方法で実行される。つまり、分離された方法と統合された方法のいずれかである。ただし、この詳細は、本標準の範囲外である。

注4： 6.2節で述べたように、ユーザネットワーク、すなわち鍵が供給され暗号アプリケーションが実行されるネットワークは、任意の従来または将来の通信ネットワークであることが可能である。

6.3 QKDN 設計に関する考慮事項

QKDNには次のような設計上の考慮が必要である。

6.3.1 セキュリティ

- 厳格な QKD プロトコルのセキュリティ証明の提供。
- QKD 実装のセキュリティ認証の提供。
- 既知の量子レイヤの脅威に対する効果的な対策の提供。
- トラステッドノードの有効なセキュリティ強化のサポート。
- QKDNに接続された 2 つのリモート当事者の IT セキュア鍵確立のサポート。

6.3.2 拡張性

- サービスの成長に応じて、柔軟性と経済性の高いネットワーク拡張のサポート。
- 広域をカバーする柔軟なネットワークトポロジのサポート。
- アクセスネットワークにおける 1 対多 QKD の効率的なサポート。

6.3.3 安定性

- QKDNの安定した設計、導入、および運用のサポート。

6.3.4 効率

- 効率的な鍵供給スキームと鍵リレースキームのサポート。
- セキュリティアプリケーションの要求条件を満たすための、高い信頼性の鍵スループットと低いレーテンシーの提供。

6.3.5 アプリケーション指向

- モジュール、ユーザーおよびアプリケーションの多様な要求条件をサポート。
- QKDN能力に対する開発が容易な API の提供。
- さまざまな ICT プロトコルおよびアプリケーションとの統合の促進。

6.3.6 堅牢性

- 一部のノードまたはリンクでサービス継続性の保証に失敗した場合、迅速な障害検出とリカバリが実行されること。

6.3.7 統合する機能

- さまざまな QKD 技術を統合する機能のサポート。

6.3.8 相互運用性

- QKD とネットワークモジュールの両方でのマルチベンダーの相互運用性のサポート。

6.3.9 移行性

- QKD 技術、モジュール、実装の移行性と暗号化方式の指定のサポート。

6.3.10 管理機能

- QKDN のモジュール、ネットワーク構成、運用、監視、変更およびアップグレードなどの管理機能のサポート。

7 QKD をサポートするためのネットワーク能力

7.1 QKDNの能力

QKDNは、以下の能力を備えている。

7.1.1 QKDNは、QKDNのサービス可用性と信頼性の仕様が合意された状態で、暗号アプリケーションに要求された鍵を提供する能力を持つ。

7.1.2 QKDNは、機密性、完全性、真正性、否認防止、可用性、トレーサビリティを考慮することを含め、セキュリティと保護をサポートする能力を持つ。

7.1.3 QKDNは、統合された管理方法または独立した管理方法でユーザネットワークと協同する能力を持つ。

7.1.4 QKDNは、鍵管理能力を持つ。

7.1.5 鍵リレー機能を提供する QKDNは、鍵リレーにOTPを推奨し、高度に安全な暗号化を使用する能力を持つ。

7.1.6 QKDNは、P-to-P アプリケーションに加えて、複数端末アプリケーションに共通鍵を提供する能力を持つ。

注： アプリケーションは、複数の端末間でのセキュアなスマートフォン通信の場合など、複数当事者による鍵共有を必要

とすることがよくある。

7.1.7　QKDNは、ネットワーク制御能力と管理能力を持つ。

7.1.8　QKDNは、さまざまなアプリケーションに鍵を適切な鍵形式で提供することを可能とするために、ユーザネットワークと QKDNの間にインタフェースの能力を持つ。

7.1.9　QKDNは、ユーザネットワーク内の暗号アプリケーションから鍵の要求を受信し、鍵の供給が実行された後に鍵を削除や保存するなど、鍵管理ポリシーを適用する能力を持つ。

7.1.10　QKDNは、ユーザネットワークと QKDNの間のインタフェースが提供するさまざまなフォーマットから、暗号アプリケーションによって選択されたフォーマットで鍵を提供する能力を持つ。

7.1.11　QKDNは、量子チャネルのネットワーク形成のために、光ファイバチャネルまたは光空間通信チャネルを使用する能力を持つ。

7.1.12　QKDNは、古典通信のために、認証されたチャネルを使用する能力を持つ。

7.1.13　QKDNは、再起動した QKD ノードを自動的に認証および動作させる能力を持つ。

7.1.14　QKDNは、ユーザネットワークからの要求を考慮してQoSを管理する能力を持つ。

7.2　QKD をサポートするためのユーザネットワーク能力

ユーザネットワークは、以下の能力を備えている。

7.2.1　ユーザネットワークは、暗号アプリケーションから QKDNに鍵の要求を行い、その応答として鍵を受信可能とする能力を持つ。

7.2.2　ユーザネットワークは、任意の必要な情報含む鍵を要求する能力を持つ。

注： 必要な情報とは、例えば鍵の長さを含む。

7.2.3　ユーザネットワークは、関連するインタフェースを介して QKDNの管理と制御に必要な情報を提供する能力を持つ。

7.2.4　ユーザネットワークは、QoS 要求条件を QKDNに要求する能力を持つ。

8　概念的構造と基本機能

この章では、QKDNとユーザネットワークの概念的構造と、これらの構造を説明するためのハイレベルな図を解説する。さらにその概念的構造の詳細と関連する基本機能を解説する。

8.1　QKDNとユーザネットワークの概念構造

QKDNの主な目的は、通信のセキュリティを高めることである。この目的を達成する主な方法の 1 つは、QKD ノードを介して QKD リンクを連結し、一つのQKD リンクで直接接続されていない場合でも、指定された QKD ノード間で 安全な鍵を共有し、ユーザネットワーク内の暗号アプリケーションに鍵を供給することである。ITセキュアな鍵の共有という目標を実現するためには、鍵が送信先ノードに到着するまで、ノードから別ノードへそれぞれの鍵でリレーすることが求められる。鍵は QKD ノードに格納され、必要に応じて鍵リレーに使用され、暗号アプリケーションに供給される。これらの操作全体を鍵管理と呼ぶ。QKDノードは、不正な当事者による侵入と攻撃から保護されているという意味で、トラステッドノードであることがQKDNにとって不可欠な前提条件となる。

図3は、QKDNとユーザネットワークの概念的な構造を示す。各 QKD ノードには、QKD モジュールだけでなく鍵マネージャ (KM) も配置される。一対のQKD モジュールは、QKD リンクによって接続され、QKD モジュールのペアと QKD リンクは QKD ノードを介して連結される。KM は、KM リンクにより接続される。これらは、鍵リレー機能を含む鍵管理機能を提供する。QKD モジュール、QKD リンク、KM および KM リンクは、通常 QKDN コントローラによって制御される。鍵リレー

ルートも、QKDN コントローラによって制御することも可能である。鍵は、KM から本標準では特別に暗号アプリケーションと呼ばれるユーザに提供され、ユーザネットワークで暗号アプリケーションに使用される。KM には鍵供給機能も含まれる。ITセキュリアな鍵リレーとそのセキュリティの詳細は、本標準の範囲外である。QKDN マネージャは通常、QKDN全体をモニターして管理する。

典型的なシナリオでは、ユーザネットワークの暗号アプリケーションは、KM に必要な鍵を要求する。この要求に従い、対応する KM は、指定されたフォーマットで安全に鍵を供給する。アプリケーションリンク内のデータ送信は、暗号アプリケーションによって提供される鍵で暗号化される（鍵は認証や他の目的でも使用される）。鍵が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自身の責任で鍵を使用し、QKDNは鍵管理ポリシーに従い鍵を削除または保存することが求められる。これにより、ユーザネットワークと QKDNとの間にセキュリティ境界を設定することができる。この境界は、鍵の要求、供給および受信と、ネットワーク管理機能のための共通のインタフェースの開発およびセキュリティ要求条件と機能を規定する上で有用である。より具体的には、アプリケーション開発者は、QKDN内のプロセスの詳細を知ることなく、鍵受信のためのインタフェースを簡単に作成することができる。同様に、QKDNプロバイダは、暗号アプリケーションが鍵をどのように使用するかを知る必要はなく、必要な鍵サイズとアプリケーション名または認証用 ID に関する最小限の情報を持てばよい。

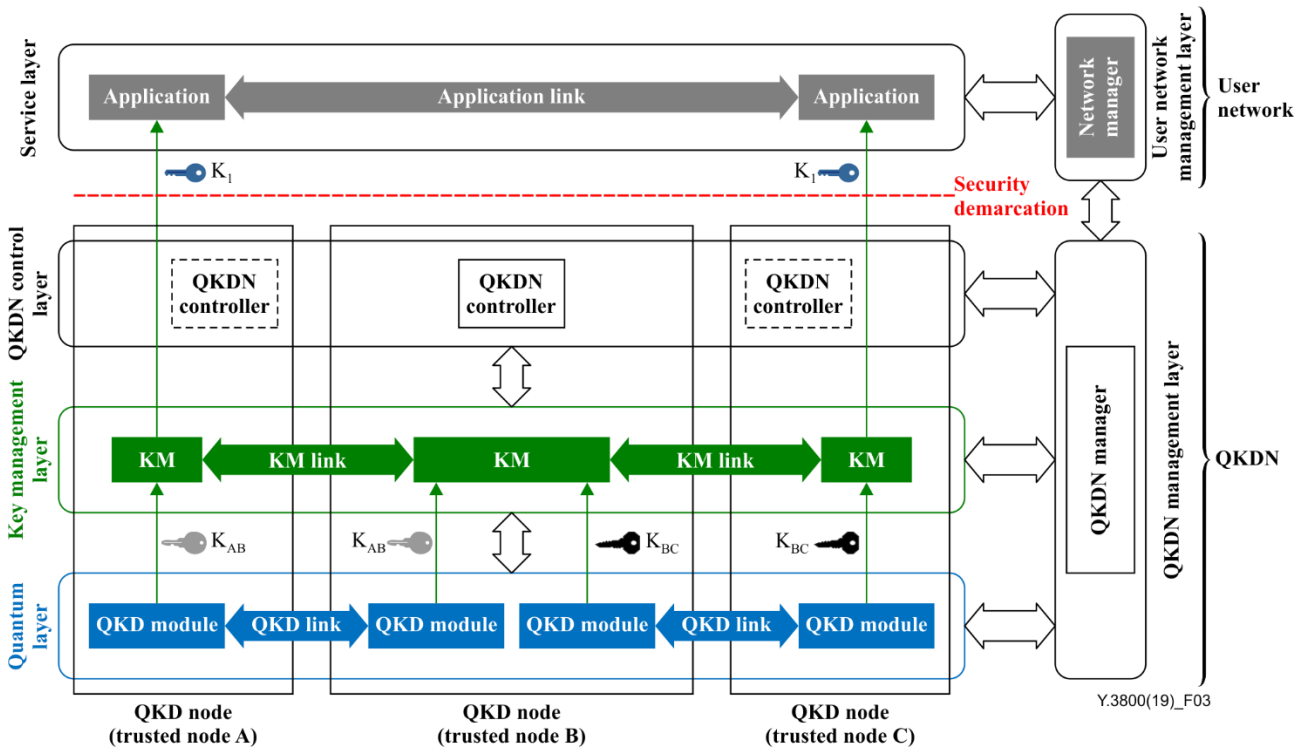

図 3 QKDN、ユーザネットワーク、およびセキュリティ境界の概念的な構造図

注1：図3では、長方形のボックスと矢印はそれぞれ論理エンティティと論理リンクを表す。

注2：量子信号を伝達するQKDモジュールとQKDリンクは、量子レイヤに存在する。KM、KMリンク、およびKMに接続された垂直矢印によって表されるインタフェースパスは、特定のセキュリティに関連する鍵を転送する。レイヤ間の矢印は、関連するレイヤ内の機能エンティティまたはQKDノードが、QKDリンクステータスおよび制御シグナルなどのQKD動作に必要な古典的情報を伝達することを示す。

注3： 量子レイヤと鍵管理レイヤにおけるQKDノード内の要素間の水平な論理リンクは、それぞれQKDリンクおよびKMリンクを使用し、QKDN設計および動作のためにさらに特徴づけられるべきである。コスト効率を高めるために、これらの論理リンクは実装時により少数の物理リンクに統合することができる。この説明は付録IIに記載されている。

注4：QKDリンク内の量子チャネルは物理リンクであり、その実装では6章で述べた量子力学の法則に基づいてQKDプロトコルを動作させる。

注5：ユーザネットワークは、QKDN制御レイヤと鍵管理レイヤの機能を持つことができる。この場合、セキュリティ境界はユーザネットワーク内に存在し、ユーザネットワークとQKDN間には存在しない。

注6： QKDN制御レイヤと量子レイヤとの間に直接の相互作用が存在することがある。詳細については8.2章を参照。

注7： QKDNとユーザネットワークの構成と関係は、時間の経過とともに変化する可能性がある。セキュリティ境界は静的である必要はない。ユーザネットワークの構成の詳細は、本標準の範囲外である。

注8： 図3は、3 ノードで最も単純な方法で QKDNを説明している。このような単純化では、鍵リレーを記述することはできても再ルーティングは表現できないが、これを除外していない。図3は論理的な概念を表しているため、物理的な実装とソフトウェアの実装はさまざまである。詳細なアーキテクチャと実用的な実装の様相は、本標準の範囲外である。

8.2 QKDNとユーザネットワークのレイヤ

この章では、図3に示すレイヤについて記述する。QKDNは、量子レイヤ、鍵管理レイヤ、QKDN 制御レイヤ、およびQKDN 管理レイヤから構成される。ユーザネットワークは、サービスレイヤとユーザネットワーク管理レイヤで記述される。

8.2.1 量子レイヤ

このレイヤでは、QKD リンクによって接続された QKD モジュールの各ペアが、独自の方法で対称的なランダムビット列を生成する。各 QKD モジュールは、ランダムビット列を同じ QKD ノード内に位置する KM へ供給する。QKD モジュールは、また QKD リンクパラメータ (例えば量子ビット誤り率(QBER) など) を QKDNマネージャに送信する。QKD リンクによって接続された QKD モジュールのペアは、QKD ノードを介して連結される。

8.2.2 鍵管理レイヤ

このレイヤは、 KM と KM リンクを含む。

各 KM は QKD ノードに格納される。KM は、鍵管理を実行する。KM はKM リンク経由で接続される。KM は、同じ QKD ノードに位置する QKD モジュールからランダムビット列を受信する。KM はこれらのビット列を同期して再フォーマットし、それらを鍵としてストレージに格納する。さまざまな暗号アプリケーションのインタフェースが KM に実装される。KM は暗号アプリケーションから鍵要求を受け取り、ストレージから必要な量の鍵を取得し、取得した鍵を KM リンク経由で同期、認証し、暗号アプリケーションに対して適切なフォーマットで供給する。

KM 間に直接 KM リンクがない場合は、鍵リレーで必要な量の鍵を共有する。KM は、QKDN コントローラに対して適切なリレールートを尋ねる。QKDN コントローラからの制御により、各 KM は、他方のKMによる高度に安全な暗号化（例えばOTP)を施された別の鍵を使い、KM リンクを介して鍵をリレーする。その結果、鍵は転送され、最終的に暗号アプリケーションに供給される。鍵が暗号アプリケーションに供給されると、KM は鍵の削除や鍵の保存などの鍵管理ポリシーを適用する必要がある。ITセキュア鍵リレーとそのセキュリティ問題の詳細は、本標準の範囲外である。

注：図 3 は、ノード B を介して信頼されるノード A と C の間で鍵 K_1 を共有する鍵リレー(ケース 1)を例示している。鍵 K_1 は、例えば、ノード A とノード B の間で生成される鍵 K_{AB}(ケース 1)、あるいはノード A でローカルに生成される K_{RN}(ケース 2) などのランダムビット列である。ケース 1 では、K_{BC} を用いた OTP 暗号化により、K_{AB} がノード B から C にリレーされる。ケース 2 では、鍵 K_{RN} は、最初に K_{AB} を用いた OTP 暗号化によりノード A から B へ送られ、ノード B で復号化され、鍵 K_{BC} を用いた OTP 暗号化によりノード B から C に送信され、ノード C で復号化される。このように、鍵 K_1 (K_{AB} または K_{RN}) はノード A と C の間で共有される。

KM は、QKD モジュールと QKD リンクにアクセスして、アクティブ化、非アクティブ化、パラメータ制御、およびキャリブレーションを行うことができる。

KM は、鍵ライフサイクル管理を実行する。

8.2.3 QKDN 制御レイヤ

QKDN 制御機能は、QKDN コントローラによって提供される。これらの機能には、鍵リレーのルーティング制御、QKDリンクとKMリンクの制御、QKD サービスのセッション制御、認証と許可制御、および QoS および課金ポリシー制御が含まれる。

注： 集中アーキテクチャでは、図3のノードB に示すように、単一の QKDN コントローラがQKDN 制御機能を実行する。分散アーキテクチャでは、各 QKD ノードには、実線と点線で囲まれたQKDN コントローラが示すように、これらの機能を実行するための QKDN コントローラが含まれている必要がある。

8.2.4 QKDN 管理レイヤ

QKDN マネージャがこのレイヤに位置し、QKDN全体を監視管理する。そのタスクには、障害、構成、料金、パフォーマンスおよびセキュリティ管理が含まれる。QKDN マネージャは、量子レイヤの QKD モジュールと QKD リンク (量子リレーポイントを含む) のパフォーマンス情報と、鍵管理レイヤの鍵管理情報を収集し、これら 2 つのレイヤを監視する。

8.2.5 サービスレイヤ

暗号アプリケーションは、このレイヤに配置され、QKDNから鍵が提供され、アプリケーションリンク内で安全な通信を実行する。

8.2.6 ユーザネットワーク管理レイヤ

ユーザネットワーク管理レイヤ内の機能は、ユーザネットワーク内の仮想化リソースと非仮想化リソースの管理とオーケストレーションを実行する。

8.3 QKDNの基本機能

この章では、QKDNの基本機能を記述する。

8.3.1 量子鍵生成

量子鍵生成は、次のタスクを実行する。

- 古典チャネルを用いたQKDモジュールの認証。
- 各 QKD モジュールの鍵生成。

注 : 異なる QKD リンクは異なる QKD プロトコルを使用することができる。

- 図3に示すように、対応する KMペア への鍵ペアの配送（例えば、QKD モジュールからKM へ鍵供給を行う、またはKMによるQKDモジュールからの鍵の取得）。

8.3.2 鍵管理

鍵管理は、次のタスクを実行する。

- 鍵のサイズ調整、メタデータを付与する鍵の再フォーマット (鍵 ID、生成日、鍵長など必要なヘッダとフッタ)、鍵の格納。
- QBER、鍵レート、リンクステータスなど、QKDプロトコルとその実装に依存するQKD リンクパラメータの組合せの取得。
- KM リンク経由での KM 間の ITセキュア鍵リレー。例えば、隣接する QKD リンクで生成された他の鍵または以前にリレーされた鍵による OTP 暗号化など。

注 : ITセキュア鍵リレー用の鍵の必要量が利用できない場合、鍵は鍵管理ポリシーに従って別の適切な方法 (AES など) によってリレーされることがある。

- KM リンクを介した鍵同期と認証。

- ユーザネットワーク内の暗号アプリケーションへの鍵供給。
- 鍵ライフサイクル管理 (鍵 ID、QKD モジュール ID、鍵生成日、鍵が供給される暗号アプリケーションの名前、鍵供給日など)。

8.3.3 QKDN制御

QKDN制御は、次のタスクを実行する。

- 鍵を必要とする暗号アプリケーションの 2 つのエンドポイント間の再ルーティングを含む鍵リレールートの制御。
- サービスレイヤからの要求および鍵管理レイヤと量子レイヤのステータスに基づく鍵リレーの制御。
- 障害または盗聴が発生した場合の量子リンクの再構成の制御。
- KM および KM リンクの制御。
- QKD モジュールと QKD リンクの制御。
- 認証と認可制御。
- QoS および課金ポリシー制御。

8.3.4 QKDN管理

QKDN管理は、次のタスクを実行する。

- 障害管理、料金管理、構成管理、パフォーマンス管理およびセキュリティ管理のサポート。
- QKDN 全体のステータスのモニター。
- KM での鍵ライフサイクル管理のサポート。
- 認証と認可制御。

注 ： 例えば QKDNのモジュールの識別と登録の管理、およびアクセス権の管理など。

- QoS および課金管理。

9 セキュリティの考慮

セキュリティ上の脅威と潜在的攻撃を軽減するために、機密性、完全性、真正性、否認防止、可用性、トレーサビリティの問題を解決する必要があり、適切なセキュリティとプライバシー保護スキームを QKDN、ユーザネットワーク、および 2 つのネットワーク間のインタフェースで考慮する必要がある。詳細は、本標準の範囲外である。

付録 I　QKDNとユーザネットワークを形成するためのバリエーション

(この付録は本標準の一部を構成するものではない**)**

QKDNとユーザネットワークを形成するには様々な方法があり、これはいくつかの自由度、すなわち QKDNから供給される鍵の種類、ユーザネットワークで利用する鍵とこれら 2 つの統合のレベルに関連する。QKDNおよびユーザネットワークを形成するためのバリエーショ ンの例は、第 I.1. 節から第 I.3. 節までで説明されており、図 付録 I-1 に示すように、QKD トラステッドノードに関連するものである。

I.1.　タイプ I バリエーション

リレー鍵 K_1は、QKDNから 2 つのエンドポイント A および D に供給されるが、これらはQKD リンクによって直接接続されていない。鍵リレーは、ノード A からノード C を介して、ノード A からD までの QKDNで実行される。この鍵リレーは、1 つまたは複数の中間ノードを図3に追加することによる直接的な拡張として理解できる。

I.2.　タイプ II バリエーション

3 つの QKD リンクで生成された鍵 K_{AB}、K_{BC}、K_{CD} は、鍵リレーなしでユーザネットワーク内のアプリケーションモジュールに各々直接供給される。各アプリケーションリンクでは、データは指定された鍵で暗号化される。アプリケーショントラステッドノード B において、受信データはまず鍵 K_{AB} により復号化された後、鍵 K_{BC} によって暗号化されてノード C に送信される。同様に、ノード C でデータリレーが実行される。

I.3.　タイプ III バリエーション

タイプ I とタイプ II バリエーションは、ネットワークで結合することができる。

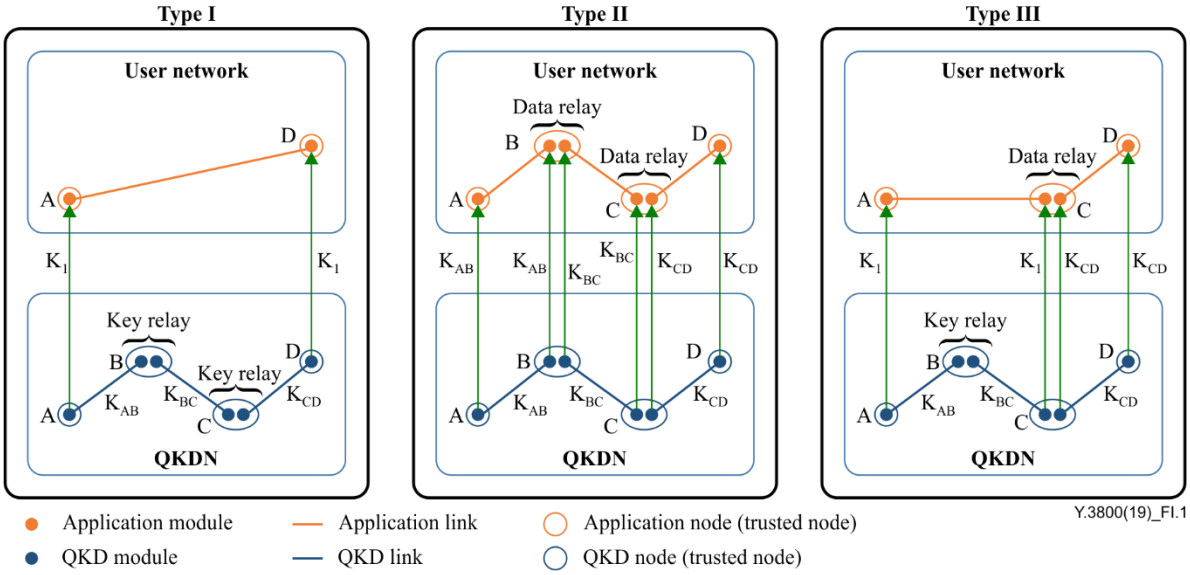

図 付録 I-1 QKDNおよびユーザネットワークを形成するための バリエーションの例

QKD ノード (トラステッドノード) とアプリケーションノードは、それぞれ QKDNとユーザネットワークの論理ノードを表すものであることを理解すべきである。実際には、これらの論理ノードは同一の物理ノードに配置されることが多い。

付録 II　QKDN での水平なリンクに関する詳細な説明

(この付録は本標準の一部を構成するものではない**)**

本標準の８章に含まれる図 3は、QKD ノード間の 2 つの水平なリンクのケースを示している。すなわち、KM リンクと QKD リンクである。実際の実装のために、QKDNの設計、導入、運用または管理の困難さと複雑さを回避するために、各リンクは明確に識別される必要がある。

本付録に示されるKM リンクと QKD リンクは、さらに論理的なリンクと物理的なリンクに分類できる。KM リンクは論理的であり、QKD ノードのペア間に存在できる。図 付録II-1 では、QKD リンクに2 つのチャネルが含まれている。すなわち、量子チャネルと古典チャネルである。量子チャネルは物理的な光チャネルであるが、古典チャネルは同期、蒸留などのために 2 つ以上の物理リンクによって実装される論理的なリンクである。

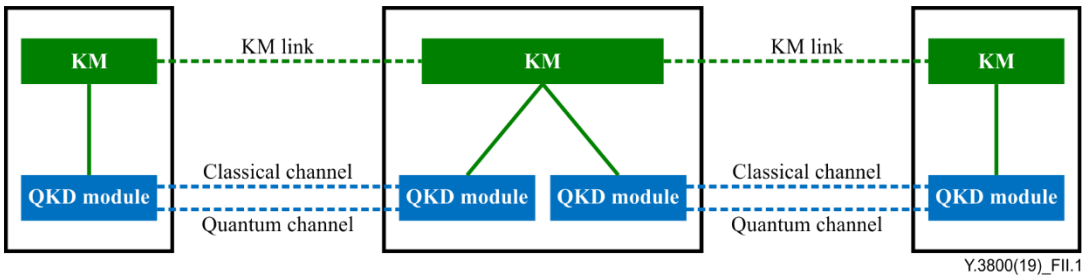

図 付録 II-1 QKDNにおける３つの水平リンク

QKDNの効率的な導入と運用を目的として、QKD ノード内の多重化による論理リンクの組み合わせは、以下のように実現できる。

1) KM リンクと古典チャネルを単一の物理リンクへの統合 (量子チャネルを除く)。
2) KMリンクと 2 つのチャネルを単一の物理リンクへの統合。

参考文献

[b-ITU-T Q.1743] Recommendation ITU-T Q.1743 (2016), *IMT-Advanced references to Release 11 of LTE-Advanced evolved packet core network*.

[b-Shannon 1949] Claude Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, vol. 28, pp. 666–682, 1949.

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

[b-FIPS PUB 197] Federal Information Processing Standards Publication 197 (2001), Announcing the ADVANCED ENCRYPTION STANDARD (AES)

[b-FIPS PUB 198] Federal Information Processing Standards Publication FIPS PUB 198-1 (2008), The Keyed-Hash Message Authentication Code (HMAC)

[b-ISO/IEC 18033-3] ISO/IEC 10833-3:2010 (2010), *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.*

[b-IEEE Trans. Inf. Theory 39] *Network Information Theory* (1993), by El Gamal and Kim, Cambridge University Press. More precisely, U. Maurer, IEEE Trans. Inf. Theory 39, 733.

[b-ETSI White Paper 8] ETSI White Paper No. 8, *Quantum Safe Cryptography and Security*.