TTC標準
Standard

JT-X1715

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

Security requirements and measures for integration of quantum key distribution network and secure storage network

第 1.1 版

2024 年 11 月 19 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について規定しており、2022 年 7 月に ITU-T SG17 において発行された ITU-T 勧告 X.1715 および 2024 年 4 月に発刊された ITU-T 勧告 X.1715 Amd.1 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	2024 年 8 月 29 日	制定
第 1.1 版	2024 年 11 月 19 日	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.509

JT 標準　JT-X1710、JY-X1712、JT-Y3800、JT-Y3801、JT-Y3802、JT-Y3803、JT-Y3804、JT-Y3808

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、量子鍵配送ネットワーク(QKDN)とセキュアストレージネットワーク(SSN)および公開鍵インフラストラクチャ(PKI)を統合するためのフレームワークを規定する。

この標準は SSN に対して次の項目を規定する。

- セキュリティ上の脅威の分析
- セキュリティ要求条件の特定
- 特定されたセキュリティ要求条件を満たすための対策の仕様。

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.509] ITU-T X.509(2016)、情報技術－開放型システム間相互接続－ディレクトリ：公開鍵及び属性認証フレームワーク

[ITU-T X.1710] ITU-T X.1710 (2020)、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 X.1712] ITU-T X.1712 (2021)、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

[ITU-T Y.3800] ITU-T Y.3800 (2019)、量子鍵配送ネットワークの概要

[ITU-T Y.3801] ITU-T Y.3801 (2020)、量子鍵配送ネットワークの機能要求条件

[ITU-T Y.3802] ITU-T Y.3802 (2020)、量子鍵配送ネットワーク - 機能アーキテクチャ

[ITU-T Y.3803] ITU-T Y.3803 (2020)、量子鍵配送ネットワーク - 鍵管理

[ITU-T Y.3804] ITU-T Y.3804 (2020)、量子鍵配送ネットワーク - 制御と管理

[ITU-T Y.3808] ITU-T Y.3808 (2022)、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統合フレームワーク

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. 証明局(CA)[ITU-T X.509]：公開鍵証明書を作成し、デジタル署名するために、1 つ以上のエンティティによって信頼された局。任意で、証明局は主体者の鍵を作成することができる。

3.1.2. 鍵データ[ITU-T Y.3803]：暗号鍵として使用されるランダムなビット文字列。

3.1.3. 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。

3.1.4. 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。

3.1.5. 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。

3.1.6. **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。

3.1.7. **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。

3.1.8. **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。**

3.1.9. **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。**

3.1.10. **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。

3.2. 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。

CA Certification Authority (認証局)

DoS Denial of Service (サービス妨害)

FCAPS Fault, Configuration, Accounting, Performance and Security (障害、構成、課金、パフォーマンス、およびセキュリティ)

IT-secure Information Theoretically secure (情報理論的安全性)

KM Key Manager (鍵マネージャ)

OTP One-Time Pad (ワンタイムパッド)

PKI Public Key Infrastructure (公開鍵基盤)

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)

SSA Secure Storage Agent (セキュアストレージエージェント)

SSN Secure Storage Network (セキュアストレージネットワーク)

TLS Transport Layer Security (トランスポートレイヤセキュリティ)

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

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高度に安全な鍵を提供する。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。鍵管理と QKDN の制御と管理は、それぞれ[ITU-T Y.3803]と[ITU-T Y.3804]で規定されている。QKDN のセキュリティフレームワークは、QKDN に対するセキュリティ脅威を特定し、一般的なセキュリティ要求条件とセキュリティ対策を導出することによって、[ITU-T X.1710]で規定されている。QKDN の鍵管理のためのセキュリティ要求条件と対策は、[ITU-T X.1712]で規定されている。

[ITU-T X.1710]や[ITU-T X.1712]で規定されている QKDN のセキュリティ対策をサポートするためには、各種のセキュリティ技術や暗号方式を適切に組み合わせて使用する必要がある。これらの技術や方式には、鍵リレーのためのワンタイムパッド(OTP)暗号化だけでなく、完全性と真正性の保護、および制御と管理情報の暗号化のための公開鍵暗号と対称暗号が含まれる。公開鍵暗号と対称暗号は、公開鍵基盤(PKI)[ITU-T X.509]に基づく IPsec[b-IETF RFC 4301]およびトランスポートレイヤセキュリティ(TLS)[b-IETF RFC 8446]の暗号スイートでサポートされている。QKD 技術と PKI などの既存の安全なネットワークインフラストラクチャとの統合のための仕様をさらに検討する必要がある。

QKDN によって提供される鍵は、ユーザネットワーク[ITU-T Y.3800]のサービスレイヤでの伝送において、機密性の高い高価値のデータを暗号化するために使用される。[ITU-T Y.3800]および[ITU-T Y.3802]で説明されているように、ユーザネットワークは、さまざまな暗号アプリケーションが存在する既存の安全なネットワークインフラストラクチャである。QKDN によって提供される高度に安全な対称鍵による利点を活用するためには、QKDN と安全なネットワークインフラストラクチャの統合のセキュリティ面をさらに研究する必要がある。QKD に基づく暗号技術と最新の暗号技術をどのように組み合わせるかを知ることは重要である。最新の暗号技術は数学的問題の計算の複雑さに基づいているが、QKD は量子力学と情報理論の法則に基づいている。これらのメカニズムとセキュリティレベルは異なる。

今日、様々な種類のデジタルデータがデータセンターに蓄積され、長期にわたって保存されるようになっている。これらのデータは現在、悪意のある攻撃の標的にされており、後で高度なコンピューティング技術が利用可能になったときに、データを復号化して元の形式に戻すことが可能となる。また、保存されたデータは、自然災害などの事象によっても脅かされている。これらの脅威は、長期的なセキュリティとデータの可用性を確保することを目的とした暗号技術の導入に強い弾みを与える。QKDN と統合された秘密分散方式[b-Shamir][b-Fujiwara]によってサポートされる複数のデータサーバで構成される SSN は、秘密分散と QKD の両方が情報理論的に安全な (IT-secure)プロトコルに基づいており、したがって、長期的に安全なデータ伝送と保存をサポートする有望な解決策を提供する。

注 - [b-Shamir]の(k, n)しきい値スキームは、n 個のシェアホルダーを使用し、少なくとも k(≦n)のシェアを収集することによってオリジナルデータを復元する(7.2 項も参照)。k-1 以下のシェアでは、無制限の計算能力を使用しても、オリジナルデータを再構成することはできない。

より正確に言えば、QKDN と秘密分散の組み合わせは、データの機密性と可用性を実現するが、この組み合わせ自体では保存されたデータの完全性を保証することはできない。PKI が発行するデジタル署名など、完全性を保護するためのセキュリティ技術を導入する必要がある。機密性と完全性を保護するためのセキュリティ要求条件は一般的に異なり、ある程度は互いに依存する可能性があることに留意すべきである。したがって、秘密分散、QKD、PKI の統合は、重要な課題である。

本標準は、QKDN とセキュアなネットワークインフラを統合するためのセキュリティ要求条件を規定するものであり、図 1 に示すように、QKDN と PKI および SSN との統合の概念は、[ITU-T Y.3808]に記述されている。

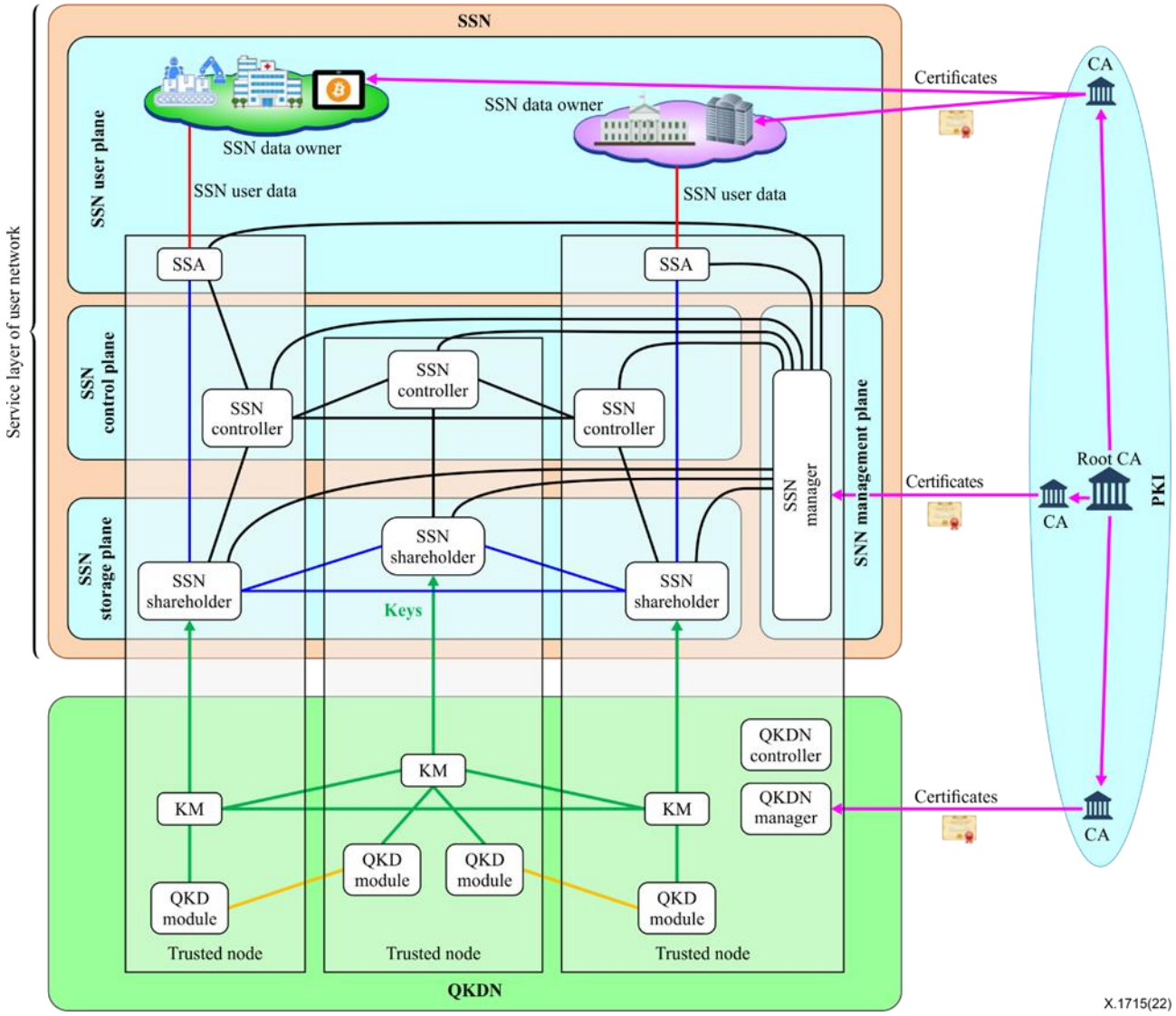

図 1 - QKDN と PKI および SSN 統合の概要 [ITU-T Y.3808]

7. 機能要素と情報資産

7.1. 機能要素

7.1.1. QKDN の機能要素

[ITU-T Y.3800]と[ITU-T X.1710]で規定されているように、QKDN は以下の機能要素とリンクを含む：QKD モジュール、鍵マネージャ(KM)、QKDN コントローラ、QKDN マネージャ、QKD リンク、KM リンク、制御リンク、管理リンク、QKD-KM リンク、KM-アプリケーションリンク、QKD ネットワークマネージャ-ネットワークマネージャリンク。

7.1.2. PKI の機能要素

以下の機能要素は、[ITU-T Y.3808]の第 7 章に記述されているとおり、PKI に含まれる。

- 認証局(CA)：デジタル証明書を発行する機能要素。PKI では、CA はツリー構造を形成してトラストチェーンを構築する。ツリーの最上位にある CA はルート CA と呼ばれる。

7.1.3. SSN の機能要素

SSN アプリケーションの以下の機能要素は、 [ITU-T Y.3808]の第 6 章のユーザネットワークに規定されている。

- セキュアストレージエージェント(SSA)：オリジナルデータからシェアを作成し、シェアからオリジナルデータを再構築する機能要素。
- SSN コントローラ：秘密分散プロセスを制御する機能要素。すなわち、オリジナルデータを受信し、データを適切に暗号化し(例えば、秘密分散プロトコルによってデータをシェアに変換する)、SSN シェアホルダーのための通信を制御する。
- SSN マネージャ：SSN の障害、構成、アカウンティング、パフォーマンス、およびセキュリティ(FCAPS)機能を管理する機能要素。
- SSN シェアホルダー：シェアの処理、交換、更新、保管を行う機能要素。
- SSN シェアホルダーリンク：SSA と SSN シェアホルダー間および SSN シェアホルダー間の通信リンク。SSN シェアホルダーリンクは、図 1 に青色で示されている。これらのリンクは、OTP 暗号などの安全性の高い暗号化を使用してシェアを送信する。
- SSN 制御リンク：SSN コントローラ間および SSN コントローラと SSN シェアホルダー間の通信リンク。SSN 制御リンクは、図 1 に黒で示されている。これらのリンクは、SSN コントローラと SSN シェアホルダー間の制御および管理情報を送信する。

これらは以下によって補足される。

- SSA リンク：SSA と SSN データオーナ間の通信リンク。SSA リンクは図 1 に赤で示されている。これらのリンクは、OTP などの高度に安全な暗号化を使用してオリジナルデータを送信する。
- SSN 管理リンク：SSN マネージャと SSN 内の他の機能要素との間の通信リンク。SSN 管理リンクは、図 1 に黒で示されている。これらのリンクは、SSN マネージャと SSN 内の他の機能要素との間で管理情報を送信する。

7.1.4. SSN の情報資産

SSN には、次の資源が含まれる。

- 鍵データ、メタデータ：鍵データおよびメタデータは、QKDN から配信され、オリジナルデータおよびシェアなどの SSN 内のデータの暗号化に使用される。

注 - 鍵データとメタデータの詳細は、[ITU-T Y.3803]と[ITU-T X.1712]に規定されている。

- オリジナルデータ：機密性および必要に応じてその他のセキュリティ(完全性、可用性および機能性など)で保護する必要がある情報を含むデータ。
- シェア：秘密分散によってオリジナルデータから生成されたデータ。
- SSN 制御と管理情報：SSN の制御と管理に関する情報。

8. セキュリティ脅威

第 7 章で述べた SSN の主な目的は、QKDN と秘密分散の統合により、オリジナルデータの機密性を長期間保護することである。QKDN に対する一般的な脅威は、[ITU-T X.1710]に規定されている。本標準は、QKDN と PKI がサポートする SSN に特有のセキュリティ要求条件に焦点を当てている。以下の脅威について詳細に考察する。

1) 盗聴
2) なりすまし(マスカレード)
3) 削除または破損
4) 否認
5) サービス拒否(DoS)

8.1. 盗聴

ネットワークからのパケットの捕捉は、ネットワークレイヤ攻撃の一種である。SSN では、オリジナルデータやシェアは暗号化されているが、現代は Harvest Now, Decrypt Later 攻撃が想定されている。

Harvest Now, Decrypt Later 攻撃とは、暗号化されたオリジナルデータを、その時点では復号化する計算能力を持っていなくても盗聴し、将来、攻撃者が大規模な量子コンピュータなどの高度な計算能力を身につければ、オリジナルデータを復号化することができるという、復号化攻撃である。この種の攻撃は、ゲノム情報のように長期にわたって有効性を維持するデータの機密性に悪影響を及ぼす。

SSN では、オリジナルデータ、シェア、鍵データがこの攻撃の対象となる情報資産である。

また、SSN 制御と管理情報などの他の情報資産を盗聴することは、攻撃者が機密性の高いネットワーク情報を理解したり、ネットワークの運用に支障をきたしたりする恐れがある。この場合、攻撃者は、ネットワークの運用中または運用直後の比較的短期間に機密情報を復号化する必要があるため、通常 Harvest Now, Decrypt Later 攻撃は効果的ではない。

8.2. なりすまし

なりすましとは、他エンティティになりすまして不正な利益を得ようとする攻撃であり、この攻撃を有効にするためには、攻撃者は通信の有効期間内という比較的短時間でなりすましに対するセキュリティ手段を解読する必要があり、この脅威は、QKDN、PKI、ユーザネットワーク内のすべてのエンティティに該当する。

8.3. 削除または破損

削除または破壊とは、不正な削除、挿入、変更、並べ替え、再生、遅延などにより、転送または保存された情報資産の完全性を損なう攻撃であり、災害などの不測の事態による削除や破壊もある。これらの脅威は、オリジナルデータ、シェア、鍵データなど、すべての情報資産に該当する。

8.4. 否認

否認とは、いくつかのタスクを実行するという事実を否定することである。悪意のあるネットワークポリシーを実施する管理者(例えば、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して転送する)は、そのようなネットワークポリシーの実施を作成しなかったと主張することがある。

8.5. サービス拒否

DoS は、SSN の適切な動作を妨害する特定の種類の動作を実行する。これには、SSN の輻輳による SSN へのアクセスの拒否、シェア生成およびその他の通信の拒否が含まれる。

QKDN と PKI および SSN との統合において特定されたセキュリティ上の脅威は、図 2 に示されている。

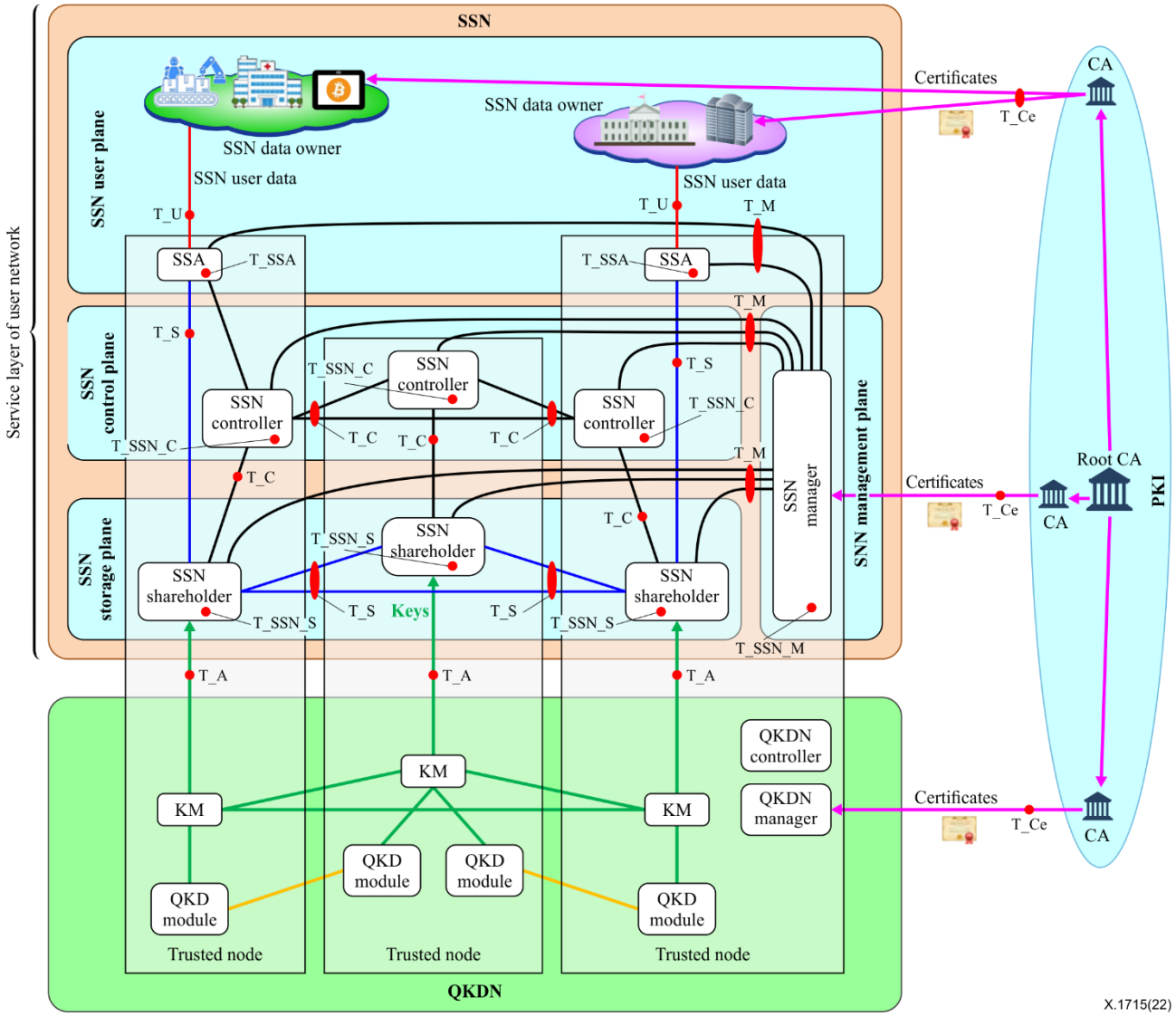

図 2 - QKDN と PKI および SSN 統合で特定されたセキュリティ上の脅威

1) T_U：SSA と SSN データオーナの間のリンクに対するセキュリティ脅威

- 盗聴：SSN データオーナからの SSN オリジナルデータおよび関連情報を傍受および解読。
- 削除または破損：SSN データオーナからの SSN オリジナルデータおよび関連情報の削除または修正。

注 1 - SSN オリジナルデータに関する情報とは、例えば、オリジナルデータを SSA に送信するための制御情報である。

- DoS：SSN オリジナルデータおよび関連情報などの通信の中断またはデータトラフィックの輻輳。

2) T_S：SSN シェアリンクに対するセキュリティ脅威

- 盗聴：シェアを傍受および解読すること。
- 削除または破損：シェアの削除または変更。
- DoS：シェアなどの通信の中断またはデータトラフィックの輻輳。

3) T_C：SSN 制御リンクに対するセキュリティ脅威

- 盗聴：SSN 制御情報を傍受および解読すること。
- 削除または破損：SSN 制御情報の削除または修正。

- DoS： SSN 制御情報などの通信の中断またはデータトラフィックの輻輳。

4) T_M：SSN 管理リンクに対するセキュリティ脅威

- 盗聴：SSN 管理情報の傍受および解読すること。
- 削除または破損：SSN 管理情報の削除または修正。
- DoS： SSN 管理情報などの通信の中断またはデータトラフィックの輻輳。

5) T_Ce：CA リンクに対するセキュリティ脅威

- 盗聴：認証データを傍受および解読すること。
- 削除または破損：認証データの削除または修正。

注 2 - 認証データは、SSN における認証のために PKI によって提供されるデータである。それに対するセキュリティ要求条件及び対策は、本の範囲外である。

- DoS：認証データなどの通信の中断またはデータトラフィックの輻輳。

6) T_A：KM と SSN シェアホルダーの間のリンクに対するセキュリティ脅威

- T_A は[ITU-T Y.3802]で参照点 Ak として定義されており、これらの脅威は[ITU-T Y.1710]で規定されている。

7) T_SSA：SSN ユーザプレーン内の SSA におけるセキュリティ脅威

- 盗聴：シェアおよびオリジナルデータを盗み、解読すること。
- なりすまし：攻撃者が SSA になりすまして情報セキュリティを侵害する - 攻撃者が悪意を持って情報資産を捏造し、そのような資産が別の機能要素または SSN データオーナから受信された、または別の機能要素または SSN データオーナに送信されたと主張する。
- 否認：攻撃者は、悪意をもって SSA 機能を実行し、その後その事実を否定する。
- DoS：アクセス拒否またはデータトラフィックの輻輳。

8) T_SSN_C：SSN コントロールプレーン内の SSN コントローラに対するセキュリティ脅威

- 盗聴：SSN 制御情報を盗み、解読すること。
- なりすまし：攻撃者が SSN 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 - 攻撃者が悪意を持って SSN の制御情報を捏造し、そのような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 SSN コントローラ機能を実行し、その後その事実を否定する。
- DoS：アクセスの拒否、または SSN 制御情報などのデータトラフィックの輻輳。

9) T_SSN_S：SSN ストレージプレーンのデータサーバに保存されているシェアに対するセキュリティ脅威

- 盗聴：シェアを盗み、解読すること;
- なりすまし：攻撃者が SSN シェアホルダーになりすまして情報セキュリティを侵害する - 攻撃者が悪意を持って情報資産を捏造し、そのような資産が別の機能要素または SSA から受信された、または別の機能要素または SSA に送信されたと主張する。
- 否認：攻撃者は、悪意をもって SSN シェアホルダー機能を実行し、その後、その事実を否定する。
- DoS：アクセスの拒否、またはシェアなどのデータトラフィックの輻輳。

10) T_SSN_M：SSN 管理プレーン内の SSN マネージャのセキュリティ脅威

- なりすまし：攻撃者が SSN 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 - 攻撃者が悪意を持って SSN 管理情報を捏造し、そのような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 SSN 管理機能を実行し、その後その事実を否定すること。
- DoS：アクセスの拒否、または SSN 管理情報などのデータトラフィックの輻輳。

セキュリティ脅威と SSN の各要素との関係を、3 つの異なる優先順位レベルとともに表 1 に要約する。

表 1 - セキュリティ脅威と安全なストレージ機能要素との関係

3 つの異なる優先順位レベル

要素	脅威				
	なりすまし	盗聴	削除または破損	否認	DoS
SSAリンク		3	3		1
SSNシェアホルダーリンク		1	2		1
SSN制御リンク		1	2		1
SSN管理リンク		1	2		1
CAリンク		1	2		1
KM-SSNシェアホルダーリンク		1	2		1
SSA	3			2	1
SSNシェアホルダー	2			2	1
SSNコントローラ	2			2	1
SSNマネージャ	2				1

表 1 の数字は、以下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、オリジナルデータの機密性、整合性、および可用性を損なう可能性がある脅威である。

- 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。これらは、例えば、秘密分散、SSN 制御、SSN 管理のプロセスにおける制御と管理情報に対する脅威であり、そのような脅威が発生した場合、SSN の安全で信頼性のある運用を達成することはできない。

- 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、SSN は正常に運用できなくなる。第二は、SSN 制御と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、オリジナルデータの漏洩や SSN 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と対策

QKDN の基本的なセキュリティ要求条件とセキュリティ対策は、[ITU-T X.1710]に規定されている。この章は、SSN における追加的かつ具体的なセキュリティ要求条件と対策を記述している。

表 2 – 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
機密性		✓	✓			
完全性		✓		✓		
認証とアクセス制御		✓		✓	✓	
可用性	シェアの作成、交換、および保存			✓		✓
	ダメージコントロールと回復			✓		✓
責任追跡性	動作ログ	✓		✓		✓
	アラームレポート	✓		✓		✓
	監査	✓			✓	✓

情報資産の性質に関する基本的な考え方は以下のとおりである。

- オリジナルデータの機密性：長期的セキュリティ
- その他のセキュリティ対策/資産：短期的セキュリティ

盗聴、なりすまし、削除または破損に関する SSN のセキュリティ要求条件とセキュリティ対策は 9.1 章から 9.3 章に規定されている。

9.1. オリジナルデータに関するセキュリティ要求条件と対策

オリジナル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 3 に示す。

表 3 – オリジナルデータに関するセキュリティ要求条件と対策

	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、物理的保護または暗号の使用を含む適切な手段によって保護される。 (注1)

	記述	セキュリティ要求条件	セキュリティ対策
(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、物理的保護または暗号の使用を含む適切な手段によって保護される。 (注1)
(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。 (注2)
注1 - 物理的保護の例としては、機能エンティティによって実装される改ざん防止と、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がある。 注2 - QKDNコントローラまたはQKDNマネージャへ情報への情報提供の実際の方法は、実装によって異なる。			

9.2. シェアに関するセキュリティ要求条件と対策

シェアのセキュリティ保護に関する要求条件と対策を表 4 に示す。

表 4-シェアに関するセキュリティ要求条件と対策

	記述	セキュリティ要求条件	セキュリティ対策
(i) 機密性	シェア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される。	SReq.9 - SSAとSSNシェアホルダーは、SSNシェアホルダーリンクを通じて伝達される際に、SSNシェアホルダーリンクのシェアの機密性を確保することが要求される。 SReq.10 - SSAとSSNシェアホルダーは、SSNシェアホルダーリンクを介してシェアを送信するために、高度に安全な秘密保持手段を使用することが推奨される。 SReq.11 - SSAおよびSSNシェアホルダーは、SSAまたはSSNシェアホルダーによって処理または保管される場合、シェアの秘密性を確保することが要求される。	- SReq.9の対策として、シェアの機密性は、SSNシェアホルダーリンクの物理的保護、またはSSAおよびSSNシェアホルダーによって提供される暗号方法を含む適切な手段によって保護される。 - SReq.10の対策として、SSAとSSNシェアホルダーは、シェアが他のSSNシェアホルダーに送信される際に、OTPなどの情報理論的に安全な暗号化/復号化によってシェアを暗号化する。 - SReq.11の対策として、SSAおよびSSNシェアホルダーは、物理的保護または暗号の使用を含む適切な手段によって保護される。 (注1)
(ii) 完全性	シェアが変更されない。	SReq.12 – SSNシェアホルダーは、処理および保管されるシェアの完全性を確保することが要求される。	- SReq.12の対策として、以下の項目i)、ii)、iii)が実施される。 i) SSNシェアホルダーは、SSAから受領したシェアの完全性を検証する。 ii) SSNシェアホルダーは、他のSSNシェアホルダーから受領したシェアの完全性を検証する。 iii) SSNシェアホルダーは、シェアの長期的な完全性を確保するために、シェアを定期的に更新する能力を有する。 iv) SSNシェアホルダーは、物理的保護又は暗号の使用を含む適切な手段によって保護される。 (注1)

	記述	セキュリティ要求条件	セキュリティ対策
(iii) 認証とアクセス制御	シェアへのアクセスは、許可されたエンティティに制限される。	SReq.13 - SSAとSSNシェアホルダーは、送信エンティティのIDが認証され、シェアを提供する権限が与えられていない限り、他のエンティティから受信したシェアが信頼されないことを保証することが要求される。 SReq.14 - SSAとSSNシェアホルダーは、他のエンティティが暗号化されていないシェア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シェア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.13およびSReq.14の対策として、SSAおよびSSNシェアホルダーは、通信する他のエンティティとの相互認証を実行するか、または他の対策を実施する。 - SReq.13およびSReq.14の対策として、SSAおよびSSNシェアホルダーは、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能力を有する。
(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
注1 - 物理的保護の例としては、機能エンティティによって実装される改ざん防止と、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がある。			

9.3. SSN 制御と管理情報に関するセキュリティ要求条件および対策

SSN 制御と管理情報のセキュリティ保護に関する要求条件と対策を表 5 に示す。

表 5 – SSN 制御と管理情報に関するセキュリティ要求条件と対策

	記述	セキュリティ要求条件	セキュリティ対策
(i) 機密性	SSN制御と管理情報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への漏洩から保護される。	SReq.15 - SSA、SSNシェアホルダー、SSNコントローラ、およびSSNマネージャマネージャは、SSN制御と管理リンクを介して送信される場合、SSN制御と管理情報の機密性を確保することが要求される。	- SReq.15の対策として、SSA、SSNシェアホルダー、SSNコントローラおよびSSNマネージャは、適切な暗号方法によって、SSN制御と管理リンク内のSSN制御と管理情報を保護する。

	記述	セキュリティ要求条件	セキュリティ対策
(ii) 完全性	SSN制御と管理情報が変更されない。	SReq.16 - SSA、SSNシェアホルダー、SSNコントローラ、およびSSNマネージャは、管理するSSN制御と管理情報の完全性を確保することが要求される。	- SReq.16の対策として、SSA、SSNシェアホルダー、SSNコントローラおよびSSNマネージャは、互いに通信する際に、SSN制御と管理情報の完全性を確保する。
(iii) 認証とアクセス制御	SSN制御と管理情報へのアクセスは、認可されたエンティティに制限される。	SReq.17 - SSA、SSNシェアホルダー、SSNコントローラ、およびSSNマネージャは、他のエンティティーから受信したSSN制御と管理情報が、送信エンティティーのIDが認証され、SSN制御と管理情報を提供する権限を与えられていない限り、信頼しないことを保証することが要求される。 SReq.18 - SSA、SSNシェアホルダー、SSNコントローラ、およびSSNマネージャは、他のエンティティが暗号化されていない制御と管理情報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制御と管理情報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.17およびSReq.18の対策として、SSA、SSNシェアホルダー、SSNコントローラおよびSSNマネージャは、通信する他のエンティティとの相互認証を実行するか、または他の対策を実施する。 - SReq.17およびSReq.18の対策として、SSA、SSNシェアホルダー、SSNコントローラおよびSSNマネージャは、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能力を有する。
(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

参考文献

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

[b-IETF RFC 4301] IETF RFC 4301 (2005), Security architecture for the Internet protocol.

[b-IETF RFC 8446] IETF RFC 8446 (2018), The transport layer security (TLS) protocol Version 1.3.

[b-Fujiwara] M. Fujiwara, M., Waseda, A., Nojima, R., Moriai, S., Ogata, W., Sasaki, M. (2016). Unbreakable distributed storage with quantum key distribution network and password authenticated secret sharing, Sci. Rep., 6, pp. 28988(1)-28988(8). Available [viewed 2022-08-11] from: https://doi.org/10.1038/srep28988

[b-Shamir] Shamir, A. (1979). How to share a secret. Commun. ACM, 22(11), pp. 612-613. Available [viewed 2022-08-11] from: https://doi.org/10.1145/359168.359176.