

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

I.<概要>

TTC 標準 JT-X1712 では、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を規定する。

II.<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

JT-X1712

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

I.<Overview>

TTC standard JT-X1712 specifies security threats to key management in quantum key distribution networks (QKDN), security requirements for key management in QKDNs, and security measures for key management to meet security requirements.

II.<References>

1. Relation to International Recommendations

This standard specifies the functional requirements for quantum key distribution networks and is based on the ITU-T X.1712 issued by ITU-T SG17 (10/2021).

2. Additional items to the above recommendations

2.1 Optional Choices

None

2.2 National matter decision item

None

2.3 Others

None

2.4 Comparison of Chapter Structure with the Original Recommendation

None

3. Change history

| 版数 | 制定日 | 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

III.<目次>

| | |
|-----|---------------------------|
| 1 | 規定範囲 |
| 2 | 参照文献 |
| 3 | 定義 |
| 3.1 | 他の標準等で定義されている用語 |
| 3.2 | 本標準で定義する用語 |
| 4 | 略語及び頭字語 |
| 5 | 表記法 |
| 6 | はじめに |
| 7 | QKDN における鍵管理において保護すべき情報資産 |

| Version | Date | Outline |
|---------|--------------------|------------------------------|
| 1.0 | 24, February, 2022 | Established |
| 1.1 | 29, May, 2024 | Error correction in clause 2 |

4. Industrial property

The status of submission of "Confirmation letter concerning the right to use industrial property rights" related to this standard can be viewed on the TTC website.

5. Others

(1) References

| | |
|----------------------|---|
| Recommendation ITU-T | X.1714 |
| ISO/IEC Standard | None |
| TTC Standard | JT-X1710、JT-Y3800、JT-Y3801、JT-Y3802 JT-Y3803 |

6. Working Group that developed this standard

Security working group

III.<Table of contents>

| | |
|-----|--------------------------------------|
| 1 | Scope |
| 2 | References |
| 3 | Definitions |
| 3.1 | Terms defined elsewhere |
| 3.2 | Terms defined in this Recommendation |
| 4 | Abbreviations and acronyms |
| 5 | Conventions |
| 6 | Introduction |

| | | | |
|------|---|-----|---|
| 7.1 | 鍵データ | 7 | Information assets to be protected in key management in the QKDN |
| 7.2 | メタデータ | 7.1 | Key data |
| 7.3 | 制御と管理情報 | 7.2 | Metadata |
| 8 | QKDNにおける鍵管理のセキュリティ脅威 | 7.3 | Control and management information |
| 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 | 8 | Security threats of key management in QKDN |
| 8.2. | KSA リンクに対する脅威(T_K2-2) | 8.1 | Threats to KMA links (T_K2-1) and key supply links (T-K1, T_K3, T_A1) |
| 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) | 8.2 | Threats to KSA links (T_K2-2) |
| 8.4. | KMA および KSA (T_KMA、T_KSA)に対する脅威 | 8.3 | Threats to control and management links (T_C, T_M, T_C&M) |
| 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 | 8.4 | Threats to KMA and KSA (T_KMA, T_KSA) |
| 9.1. | 鍵データのセキュリティ要求条件と対策 | 9 | Security requirements and measures for information assets of key management in QKDN |
| 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 | 9.1 | Security requirements and measures on the key data |
| 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 | 9.2 | Security requirements and measures on the metadata |
| 9.4. | 損失と破損、および DoS (サービス妨害) | 9.3 | Security requirements and measures on the control and management information |
| | | 9.4 | Loss and corruption, and DoS |