認 証 報 告 書

東京都文京区本駒込2丁目28番8号
独立行政法人情報処理推進機構
理事長　齊藤　裕

原紙押印済

プロテクションプロファイル（PP）

申請受付日（受付番号）	令和6年12月12日（IT認証4907）
認証識別	JISEC-C0877
プロテクションプロファイル名称／識別	Protection Profile for Prepare and Measure Quantum Key Distribution Modules
プロテクションプロファイルバージョン番号	Version 1.0
プロテクションプロファイル開発者	一般社団法人量子フォーラム
保証要件適合	EAL2
ITセキュリティ評価機関の名称	株式会社ECSEC Laboratory 評価センター

上記のPPについての評価は、以下のとおりであることを認証したので報告します。
令和8年10月8日

セキュリティセンター 技術評価部
技術管理者　橋本 徹

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation; CC:2022 Release 1
② Common Methodology for Information Technology Security Evaluation; CEM:2022 Release 1
③ Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1

評価結果：合格

「Protection Profile for Prepare and Measure Quantum Key Distribution Modules, Version 1.0」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1　全体要約 1
1.1　評価PP 1
1.1.1　保証パッケージ 1
1.1.2　PP概要 1
1.1.2.1　セキュリティ機能概要 4
1.1.2.2　脅威とセキュリティ目標 5
1.1.3　免責事項 5
1.2　評価の実施 5
1.3　評価の認証 5
2　PP識別 6
3　セキュリティ方針 6
3.1　セキュリティ機能方針 7
3.1.1　脅威とセキュリティ機能方針 7
3.1.1.1　脅威 7
3.1.1.2　脅威に対するセキュリティ機能方針 8
3.1.2　組織のセキュリティ方針とセキュリティ機能方針 9
3.1.2.1　組織のセキュリティ方針 9
3.1.2.2　組織のセキュリティ方針に対するセキュリティ機能方針 9
4　前提条件と評価範囲の明確化 10
4.1　使用及び環境に関する前提条件 10
5　評価機関による評価実施及び結果 11
5.1　評価機関 11
5.2　評価方法 11
5.3　評価実施概要 11
5.4　評価結果 12
5.5　評価者コメント/勧告 12
6　認証実施 13
6.1　認証結果 13
6.2　注意事項 13
7　附属書 13
8　用語 14
9　参照 16

1 全体要約

この認証報告書は、一般社団法人量子フォーラムが開発した「Protection Profile for Prepare and Measure Quantum Key Distribution Modules, Version 1.0」（以下「PP[11]」という。）について株式会社 ECSEC Laboratory 評価センター（以下「評価機関」という。）が令和 8 年 9 月 14 日に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者である一般社団法人量子フォーラムに報告するとともに、PP[11]に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書と共に、対応する PP [11]を併読されたい。特に PP[11]に適合する TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、PP[11]において詳述されている。

本認証報告書は、PP[11]に適合した製品開発を行う開発者及び製品調達者を読者と想定している。本認証報告書は、PP[11]に対する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価PP

PP[11]が要求するセキュリティ機能の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

PP[11] において要求される保証パッケージは、EAL2 である。

また、PP[11]への適合を主張する PP、及び ST は正確適合を主張しなければならない。

1.1.2 PP概要

PP[11]の目的は、P&M(Prepare and Measure)プロトコルを用いた量子鍵配送(QKD)モジュールのセキュリティ要件を定義することである。

PP[11]は、ETSI の”Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules, V2.1.1” ([13]) に基づいて開発された。PP[11]と[13]の主な違いは以下の通りである。

- [13]はEAL4 augmented with AVA_VAN.5 and ALC_DVS.2を要求するが、このPP[11]はEAL2を要求する。
  - [13]に適合したTOEは高い攻撃能力を持つ攻撃者に対抗するが、このPP[11]に適合するTOEは基本的な攻撃能力を持つ攻撃者に対抗する。
  - このPP[11]に適合するTOEは、モジュールレベルの評価と、ライフサイクル評価の大部分、特にサイト監査を免除できる。開発サイト・製造サイトのセキュリティは、開発者主張に基づく。

PP[11]に適合する TOE は、QKD システムを構築するために QKD リンクを介して接続可能な QKD モジュールのペアである。TOE セキュリティ機能（TSF）は、このような QKD システムで必要と予想される機能の一貫したサブセットを提供する。

TOE のセキュリティ機能は、1 つ以上の security proof に従う Prepare & Measure (P&M) プロトコルを使用した量子鍵配送（QKD）機能である。P&M プロトコルでは、1 台の QKD transmitter が符号化された量子信号を準備し、測定のために 1 台の QKD receiver に送信する。QKD transmitter と QKD receiver のエンコード・デコード情報により、量子通信段階と鍵蒸留段階を通じて QKD transmitter と QKD receiver の間で共有ビット列が確立される。

QKD システムは、QKD transmitter と QKD receiver の 2 つの QKD モジュールを接続し、送信側の識別とデータの完全性を保証する authenticated classical channel を使用することで、QKD 鍵を確立する。QKD 鍵は、両方の QKD モジュールで共有される機密のランダムビット列であり、許可された利用者が消費できる。

要求があれば、TOE は明確に定義された品質で共有 QKD 鍵を配送するか、両方の QKD モジュールの利用者に失敗を通知する。元の鍵要求者は、各 QKD モジュールから QKD 鍵の受領を許可される利用者を定義する。確立された QKD 鍵を出力後に適切に取り扱い、特にそのさらなる使用に適用されるセキュリティ要件を確保することは、利用者の責任である。本 PP は QKD 鍵の確立に限定される。QKD 鍵の更なる使用及びその特定目的への適合性は、本 PP の範囲外である。

TOE はバックグラウンドで QKD 鍵を生成し、要求された長さの一部を利用者に配送することも、要求に応じて専用の QKD 鍵を生成することもできる。連続的な QKD 鍵ビットストリームは、1 ビットずつの配送によるバックグラウンド確立とみなすことができる。この PP は、この点において利用者インタフェースを制限しないが、QKD 鍵の事前生成ビットが TOE に保存されている間保護されること、及び消費後にビットが削除されることを要求する。

TOE は 2 つの QKD モジュールで構成されるが、その間の QKD リンクは TOE ではない（図 1-1 参照）。さらに、関連するガイダンス文書も含まれる。QKD リ

ンクは、物理的な保護なしに非管理環境を通過することができ、セキュリティサービスを提供しない。QKD リンクには少なくとも 2 つの通信チャネル、Authenticated classical channel と量子チャネルが含まれる（図 1-2 参照）。Unauthenticated classical channel も、QKD モジュールの時刻同期などに使用することができる。Unauthenticated classical channel では、アナログ通信とデジタル通信が可能である。QKD リンクを使用した通信は、TSF 間通信とみなされる。

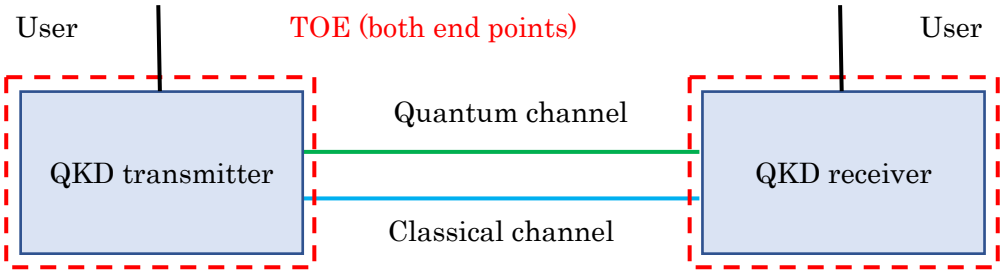


図 1-1: The TOE-boundary, i.e. the two QKD modules

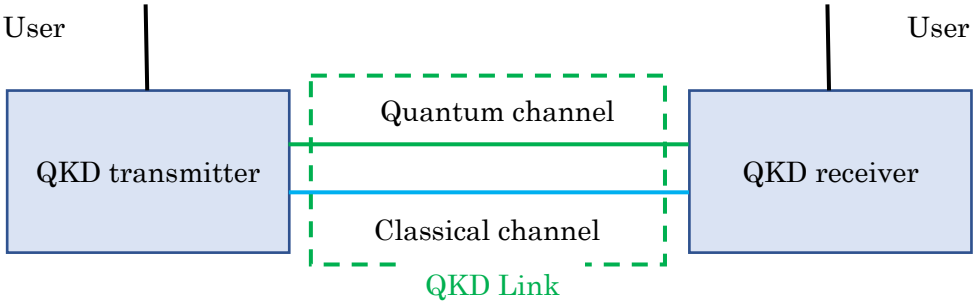


図 1-2: The QKD link

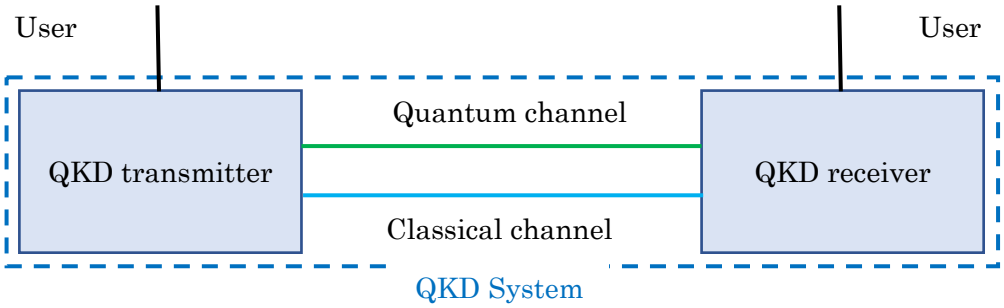


図 1-3: The QKD System

QKD システムの目的は、QKD transmitter と QKD receiver の 2 つの QKD モジュールを接続し、送信側の識別とデータの完全性を保証する authenticated

classical channel を使用することで、QKD 鍵を確立することである（図 1-3 参照）。QKD 鍵は、両方の QKD モジュールで共有される機密のランダムビット列であり、許可された利用者が明確に定義されたチャンク単位で消費できる。「ランダム」という特性は、ビット列が予測不可能で、一様に分布し、互いに独立している、すなわち、QKD システムにより前方秘匿性と後方秘匿性を実装できるという意味で使用されている。これらの特性はそれぞれ不完全である可能性がある。

TOE は、セキュリティパラメータを持つ QKD プロトコルを実装する。セキュリティパラメータは、QKD プロトコルの 1 回の実行中に、プロトコルが中断せず、ビット列のいずれかの特性が保証されないことを示すイベントが発生する最大確率を示す。TOE は、関連する構成された security proof に従って、これがある上限を超えないことを保証する。

PP[11]は、オプションの機能パッケージ「Trusted interface Version 1.0」を定義している。この機能パッケージは、QKD 鍵の鍵マネージャへのエクスポート時に trusted channel の使用を要求する SFR などを定義している。この機能パッケージは TOE と QKD 鍵マネージャとの間、または TOE と他の非 TOE IT 製品の間の通信が物理的に保護されていない場合に適用する。

1.1.2.1 セキュリティ機能概要

PP[11]では、量子鍵配送(QKD)モジュールに求められるセキュリティ機能を要求する。その主要なものを以下に示す。

(1) 量子鍵配送

TOE は、1 つ以上の security proof に従う Prepare & Measure (P&M)プロトコルを使用した量子鍵配送(QKD)機能を提供する。

(2) TSF 間通信のための Authenticated classical channel

TOE は、QKD モジュール間の QKD リンクにおいて、Authenticated classical channel を提供する。

(3) 暗号演算

TOE は、QKD リンクに関わる暗号演算機能を提供する。暗号演算機能は、Authenticated classical channel のためのメッセージ認証、乱数生成機能を含む。また不要になった時の鍵または鍵材料の破棄の機能を提供する。

(4) TOE 放出（emanation）の防止

TOE は、TSF データおよび利用者データへのアクセスを可能にするような、外部から観察可能な現象による放出をしないことを保証する。

(5) 物理的攻撃への対抗

TOE は、TSF の内部状態への QKD リンクを介した能動的プロービングに対抗する。

1.1.2.2 脅威とセキュリティ目標

PP[11]に適合する TOE は、以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

攻撃者が QKD リンクを介して交換されるデータを盗聴、生成、操作を試みるかもしれない。そこで、TOE は、1 つ以上の security proof に従う Prepare & Measure (P&M)プロトコルを使用した量子鍵配送 (QKD) 機能を提供する。

攻撃者は量子チャネルへの量子放出に含まれる意図しない情報を観察し、QKD 鍵の機密性を侵害することを試みるかもしれない。そこで、TOE は、TSF データおよび利用者データへのアクセスを可能にするような量の timing of signals, signal strength, signal waveform, quantum state を攻撃対象領域に放出しないことを保証するように設計する。

攻撃者は QKD リンクを介して光学的な能動的プロービングを試み、QKD 鍵の機密性と完全性を侵害することを試みるかもしれない。そこで、TOE は SFR が常に実施されるよう自動的に対応することによって対抗する。

1.1.3 免責事項

なし。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価及び認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって PP[11]に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、令和 8 年 9 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[14]、所見報告書、及び関連する評価証拠資料を検証し、PP[11]の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、PP[11]の評価が CC（[4][5][6][7][8]）及び CEM（[9]）、及び補助文書（[10]）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 PP識別

PP[11]は、以下のとおり識別される。

PP名称：	Protection Profile for Prepare and Measure Quantum Key Distribution Modules
バージョン：	Version 1.0
開発者：	一般社団法人量子フォーラム

この PP に適合する TOE の評価は、以下の Supporting Document (SD) に従って実施する。

SD名称：	Supporting Document Mandatory Technical Document Evaluation Method for Protection Profile for Prepare and Measure Quantum Key Distribution Modules
バージョン：	Version 1.0 EnJp

3 セキュリティ方針

本章では、PP に適合する TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

PP[11]では、以下のセキュリティ機能を TOE に要求する。

- 量子鍵配送

3.1 セキュリティ機能方針

PP[11]では、3.1.1.1 に示す脅威に対抗する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

PP[11]では、表 3-1 に示す脅威に対抗し、これに対抗する機能を TOE に要求する。

表3-1 脅威

識別子	脅威
T.UNTRUSTED_QKD_LINK	攻撃者は、QKD鍵の機密性および完全性を侵害するため、QKDリンクを介して交換されるデータを盗聴、生成、または操作する。 場合によっては、盗聴とAuthenticated classical channel上の情報の改変が組み合わされる。
T.SIDE_CHANNEL	攻撃者は、量子チャネルへの量子放出に含まれる意図しない情報を観察し、QKD鍵の機密性を侵害する。 例えば、QKDプロトコルは、光量子状態の偏光方向を利用して鍵ビット値を送信する。しかし、QKDプロトコルの実装に不備があると、平均光子数の鍵ビット値に対する依存性が意図せずに生じる可能性がある。この場合、偏光方向は意図された鍵ビット値のエンコードであり、平均光子数は意図されずに量子状態の異なる性質に同じ情報を再エンコードすることになる。攻撃者は、量子状態の光子数を観測することで、鍵のビット値を推定できる可能性がある。

識別子	脅威
T.ACTIVE_PROBING	攻撃者は、QKDリンクを介して光学的な能動的プロービングを試み、QKD鍵の機密性と完全性を侵害する。たとえば、攻撃者は、QKDモジュールの内部状態を推定するため、またはreceiverの内部状態を制御するために、量子チャネルから強い光を注入する。そして、攻撃者はQKD鍵の機密性と完全性を侵害する可能性がある。

3.1.1.2 脅威に対するセキュリティ機能方針

PP[11]に適合する TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.UNTRUSTED_QKD_LINK」への対抗

本脅威は、QKD リンクを攻撃して、QKD リンクを介して交換されるデータを盗聴・生成・操作を試みることを想定している。

この脅威に対して、TOE が信頼できるプロトコルとして P&M プロトコルに基づく鍵配送サービスを提供することで対抗する。この鍵配送サービスは、QKD リンク上の通信に盗聴者や操作者が存在する場合でも、QKD リンク上の、送信側の識別とデータの完全性を保証する Authenticated classical channel を利用し、両 QKD モジュール間で共有され、機密性があるランダムなビット列を QKD 鍵としてエクスポートするための鍵を確立する。

ここで、用語「信頼できる QKD プロトコル」は、そのプロトコルが 1 つ以上の責任のある組織によって承認された security proof に従うことを意味する。信頼された QKD プロトコルは、鍵の確立によって得られるビット列の機密性と完全性を保護するための学術的な研究を反映している。

また、TOE は Authenticated classical channel とメッセージ認証アルゴリズムを要求する。これらの要件は、有効な security proof に従う。有効な security proof に従う QKD プロトコルは、無限の計算能力を持つ攻撃者に対抗する。

authenticated classical channel のメッセージ認証には共有秘密が必要であるが、それは開発者によってインストールされる初期の事前共有鍵を使用、または事前共有鍵から導出することを想定している。

(2) 脅威「T.SIDE_CHANNEL」への対抗

本脅威は、量子チャネルへの量子放出に含まれる意図しない情報を観察し、QKD 鍵の機密性を侵害することを想定している。

この脅威に対して、TOE の TSF は、表 3-2 に特定されている TSF データおよび利用者データへのアクセスを可能にするような量の放出を攻撃対象領域に放出しないことを保証するように設計することで対抗する。

表 3-2 Definition of Side-Channel Protection

Emissions	Attack surface	TSF data	User data
Timing of signals	QKD-link	any confidential TSF data	any confidential user data
Signal strength, signal waveform or Quantum state	QKD-link	any confidential TSF data	any confidential user data

(3) 脅威「T.ACTIVE_PROBING」への対抗

本脅威は、QKD リンクを介して光学的な能動的プロービングを試み、QKD 鍵の機密性と完全性を侵害することを想定している。

この脅威に対して、TOE は SFR が常に実施されるよう自動的に対応することによって、TSF の内部状態への QKD リンクを介した光学的な能動的プロービングに抵抗することで対抗する。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

組織のセキュリティ方針はない。

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

組織のセキュリティ方針はないため、組織のセキュリティ方針に対するセキュリティ機能方針はない。

4 前提条件と評価範囲の明確化

本章では、想定する読者が PP[11]に適合する TOE の利用の判断に有用な情報として、PP[11]に適合する TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

PP[11]に適合する TOE を運用する際の前提条件を**表 4-1** に示す。これらの前提条件が満たされない場合、PP[11]に適合する TOE のセキュリティ機能が有効に動作することは保証されない。

表 4-1 前提条件

識別子	前提条件
A.PHYSICAL	TOE、TOEに接続される非TOE IT製品、およびTOEと非TOE IT製品間のネットワークは、その動作環境において物理的に保護される。 この前提条件は、QKDリンク以外のすべての運用環境が物理的に保護されていることを想定している。また、信頼できる人員以外の物理的保護エリアへの立ち入りは制御されている。例えば、それらは入場管理されたインターネットデータセンタ内に配置される。
A.OPERATOR	物理的保護エリアにてTOEや非TOE IT製品を操作するオペレータは信頼できる。 オペレータは、適切にトレーニングされ、セキュリティポリシー、利用者ガイダンスを順守し、組織のセキュリティの最善の利益のために行動する。
A.IT_PRODUCTS	物理的保護エリアに設置され、TOEに接続される非TOE IT製品は信頼できる。 非TOE IT製品は運用組織によって適切に管理され、TOEに悪影響を与えない。

5 評価機関による評価実施及び結果

5.1 評価機関

評価を実施した株式会社 ECSEC Laboratory 評価センターは、IT セキュリティ評価及び認証制度により承認されるとともに、ISO/IEC 17025 の要求に基づいて認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

5.2 評価方法

評価は、CC パート 3 の保証要件について、CEM に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、PP[11]の概要と、CEM のワークユニットごとの評価内容及び判断結果を説明する。

5.3 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、令和 6 年 12 月に始まり、令和 8 年 3 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。

評価作業中に発見された問題点は、所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

5.4 評価結果

評価者は、評価報告書をもって PP[11]が CEM のワークユニットすべてを満たしていると判断した。

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

・APE_INT.1、APE_CCL.1、APE_SPD.1、APE_OBJ.2、APE_ECD.1、APE_REQ.2

5.5 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

6 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の観点で認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

③ 提出された証拠資料を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、PP[11]及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

6.1 認証結果

評価機関より提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、PP[11]の評価が CC パート 3 の APE_INT.1、APE_CCL.1、APE_SPD.1、APE_OBJ.2、APE_ECD.1、及び APE_REQ.2 に対する保証要件を満たすものと判断する。

6.2 注意事項

SD が PP[11]の評価時の版([12])から改版され、PP[11]に適合する TOE の評価を改版された SD に基づいて実施する場合、SD の内容が他の要件と一致しており矛盾がないことを再評価し、SD の内容の違いが PP 適合に影響しないことを追加で評価する必要がある。

PP[11]に適合する TOE の評価に先立ち、責任のある組織から QKD プロトコルの security proof の承認を得る必要がある。SD においては、security proof の内容に基づいて、各種評価が要求されている。

7 附属書

特になし。

8 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
SD	Supporting Document（サポート文書）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された用語の定義を以下に示す。

Authenticated classical channel	真正性を保証するための認証機能を備えた古典チャネル。
Classical channel (古典チャネル)	非破壊で読み取り、完全に再生することができる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。
Prepare and measure QKD protocol	片方のQKDモジュールが量子状態を準備し、もう片方のQKDモジュールが量子状態を測定するQKDシステムでQKD鍵を確立するためのプロトコル。
QKD link	一対のQKDモジュールを接続し、QKDを実行できるようにするための能動コンポーネントおよび受動コンポーネントのセット。
QKD module (QKDモジュール)	QKDプロトコルの一部と暗号機能を実装し、少なくとも1つの他のQKDモジュールと共有された機密のランダムビット列を安全に確立できるハードウェア、ソフトウェア、および／またはファームウェアコンポーネントのセット。
QKD protocol (QKDプロトコル)	QKDモジュールの共有された機密なランダムビット列を中止または同意する操作のセット。
Quantum channel	量子信号を送信するための通信チャネル。
Quantum key distribution (量子鍵配送), QKD	量子もつれに基づく安全性、あるいは未知の伝送量子状態を完全に複製または測定することの不可能性を持つプロトコルを使用して、遠隔の当事者間で共有された機密のビット列に合意するための量子状態の伝送を含む手順。
Security proof	QKDモジュールの物理モデルやその他の前提条件に基づいているQKDプロトコルに従った結果として確立される鍵の安全性を

	保証する数学的手法。 注: 安全性の記述は、セキュリティパラメータと呼ばれる理想的な鍵からのずれの度合いの上界を用いて行われる。
Unauthenticated classical channel	Authenticated classical channel でない classical channel。

9 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 令和7年8月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 令和5年12月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 令和3年10月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version CC:2022 Revision 1, November 2021, CCMB-2022-11-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version CC:2022 Revision 1, November 2021, CCMB-2022-11-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version CC:2022 Revision 1, November 2021, CCMB-2022-11-003

[7] Common Criteria for Information Technology Security Evaluation Part4: Framework for the specification of evaluation methods and activities Version CC:2022 Revision 1, November 2021, CCMB-2022-11-004

[8] Common Criteria for Information Technology Security Evaluation Part5: Pre-defined packages of security requirements Version CC:2022 Revision 1, November 2021, CCMB-2022-11-005

[9] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version CEM:2022 Revision 1, November 2021, CCMB-2022-11-006

[10] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, 2024-07-22

[11] Protection Profile for Prepare and Measure Quantum Key Distribution Modules, Version 1.0, 2026年9月14日, 一般社団法人量子フォーラム

[12] Supporting Document Mandatory Technical Document Evaluation Method for Protection Profile for Prepare and Measure Quantum Key Distribution Modules, Version 1.0, 2025年5月, 一般社団法人量子フォーラム

[13] Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules, V2.1.1

[14] PP評価報告書, 第1.7版, 2026年9月14日, 株式会社 ECSEC Laboratory 評価センター

[15] 所見報告書 NIT-EOR-0001-00, 2025年6月10日, 株式会社ECSEC Laboratory評価センター

[16] 所見報告書 NIT-EOR-0001-01, 2025年7月4日, 株式会社ECSEC Laboratory評価センター