資料4-2

公開可

量子暗号通信による安全な通信の実現

2026年3月23日

日本電気株式会社

NEC \Orchestrating a brighter world

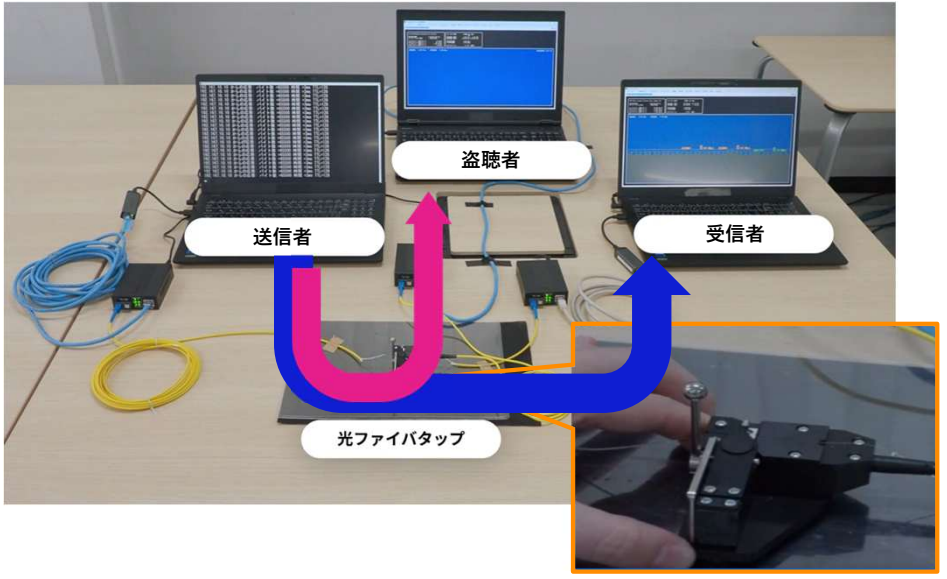
量子暗号(QKD)と耐量子計算機暗号(PQC)の関係

量子暗号(QKD)と耐量子計算機暗号(PQC)との比較は以下の表の通り

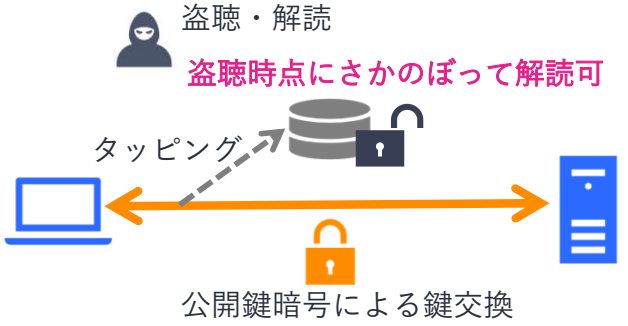
	安全性の根拠	用途	導入コスト	利用シーン
量子暗号(QKD)	情報理論的	暗号/鍵交換	高（専用ハードが必要）	特定の拠点間で行う、重要な通信の秘匿化
耐量子計算機暗号(PQC)	計算量的	暗号/鍵交換,デジタル署名	低（ソフトウェアだけで実現可）	今のインターネットで使われている公開鍵暗号の置き換え

光ファイバの盗聴リスク

光ファイバーの盗聴



Harvest Now, Decrypt Later (HNDL)攻撃



量子暗号(QKD)装置と2つの主要方式

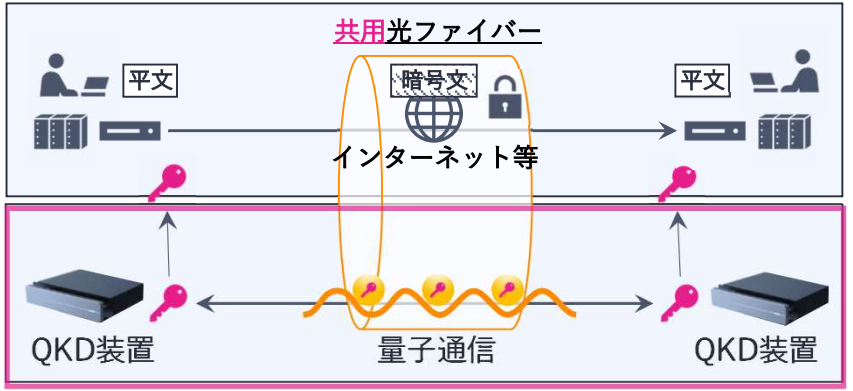
* BB84:Bennett and Brassard 1984

BB84方式（光子検出≒粒を数える）

- 量子鍵配送の**専用光ファイバー**が必要
- 長距離（～50 km）
- コスト高
- **国内企業：NEC、東芝**
- 海外企業：IDQ(スイス)、HEQA(イスラエル)、QTI（伊）、QunatumCTek（中） 他
- **適用箇所：長距離伝送が必要な基幹ネットワークのリンク**

* CV: Continuous Variable(連続変数)

CV-QKD 方式(光波検出≒揺れ方を測る)



- **既通信使用中の光ファイバーが利用可能**
- 短距離（～20 km）
- コスト低
- **国内企業：NEC**
- 海外企業：LuxQuanta(伊)、Luxquanta（スペイン）QuintessenceLabs(豪)、KEEQuant(独)
- **適用箇所：ユーザ拠点へのアクセスなど多数配備が必要なリンク**

将来の量子暗号によるネットワーク構想～PQCとQKDのハイブリッド構成～

■ 原理的に安全なQKD-NWと、危殆化していないPQCによるNW拡張のハイブリッド構成により
QKDの制約をPQCで補完し、広域に安全な鍵共有を実現します