ユーザーのための量子暗号入門

初版

2020 年 5 月 26 日

目次

1　はじめに 3

2　量子暗号とは 5

2.1　データの暗号化方法 5

2.2　暗号鍵の交換方法 6

2.3　量子暗号と耐量子安全性暗号の定義 9

3　量子暗号に必要な構成要素 10

3.1　QKD システム 10

3.1.1　QKD システムの構成要素 10

3.1.2　鍵情報のエンコード方法 11

3.2　QKD ネットワーク 13

3.2.1　QKD ネットワークの構成要素 14

3.2.2　QKD ネットワークの機能要件の評価 17

4　量子暗号サービスの具体例 20

4.1　安全保障（防衛・外交）分野でのユースケース 21

4.1.1　想定する運用場面 21

4.1.2　必要性 22

4.1.3　有効性 23

4.1.4　システム構成案と適用の効果 23

4.2　医療分野におけるユースケース 25

4.2.1　想定する運用場面 25

4.2.2　必要性 27

4.2.3　有効性 27

4.2.4　個人情報漏洩の影響 28

4.3　生体認証分野におけるユースケース 29

4.3.1　想定する運用場面 29

4.3.2　必要性 29

4.3.3　有効性 30

4.3.4　システム構成案と適用による効果 30

5　量子暗号サービスの運用 32
5.1　量子暗号ビジネスのエコシステム 32
5.2　量子暗号サービスにおけるセキュリティ対策指針 34
5.2.1　情報セキュリティマネジメントシステムの構築・運用の流れ 35
5.2.2　情報セキュリティ要件 35
5.2.3　情報セキュリティ対策の指針 36
5.2.4　リスク分析 36
5.3　標準化活動 45

6　量子暗号技術の現状と今後の課題 47
6.1　国内外の開発動向 47
6.2　研究の今後の課題 50

7　おわりに 51

付録 52
A.　量子暗号のプロトコル 52
A.1　BB84 52
A.2　CV-QKD 53
B.　量子コンピュータ 57
B.1　量子コンピュータの利用例 57
B.2　量子コンピュータによる暗号解読 57
B.3　量子コンピュータの開発動向 58

執筆者一覧 59

1　はじめに

近年、大手ネット企業が巨額の資金を投じて量子コンピュータの開発を加速しており、2030 年～2040 年頃実用化すると予測されている。量子コンピュータが実現すれば、現在インターネットのセキュリティを支えている公開鍵暗号が解読されてしまう恐れがある。その一方で、何百億個を超える機器・センサがインターネットに接続され、ペタバイト級のビッグデータが流れる IoT(Internet of Things)スマート社会は、もう目前に来ている。IoT セキュリティ通信を支える暗号は、大きな柱の一つであり、その暗号技術の一つに量子暗号がある。量子暗号は、3THz 以上の光の領域から量子力学に基づき現れる不確定性原理を利用し、将来的に圧倒的計算速度を有する量子コンピュータの出現にも負けない、未来永劫解読が不可能な最強の暗号として注目されている最先端技術である。量子暗号技術を用いることにより、情報を電気的信号に変換せず、光のまま通信し、大容量・低電力を可能とする信頼性の高い光通信ネットワークの構築が実現できる。量子暗号の利点は、悪意のある者が盗聴した場合、通信中に盗聴された痕跡が分かること、さらに光の領域であるため電波申請の必要がない自由で広い帯域を活用できることである。現在、世界の中でも中国の台頭は目覚ましく、量子暗号の長距離衛星通信の実験に成功し、トップデータを出している。さらに、2030 年までに、世界中で最も懸念されている対処できないセキィリティ脅威の一つに、今はまだ解読できなくても、絶えずデータを盗聴し保存・蓄積しておき、将来量子コンピュータのように高度な計算機が登場したときに過去に遡って全データを解読する攻撃(“Store now, decrypt later”-attack)がある。

そこで本書は、その危殆化に備え、「どんな計算機でも解読できないこと」（情報理論的安全性）を証明できる現在唯一の暗号通信技術である量子暗号を活用し、長期にわたって秘匿すべき情報をどのように守るか、どのような社会貢献ができるか、どのようなビジネスができるかについて、わかりやすく説明することを目的とする。

これから量子暗号の事業に携わる対象者としては、①情報通信ネットワークのエンドユーザー、②情報通信ネットワークの通信事業者、③セキュリティ技術の研究者や技術者等が挙げられるが、本書では、①情報通信ネットワークのエンドユーザーを対象とする。量子暗号分野は、横断的な学問分野から成り立っており、基礎学問として情報理論、量子論、光制御技術、ハードウェア設計技術等があり、アプリケーションとして実現するには、加えてネットワーク技術、セキュリティ技術等も深く関係する。そのため、中身を知るために何から手を付けたら良いか分からず、「得体の知れないもの」として入り口で止まってしまう潜在的ユーザーが多くいることをよく聞く。また、これまでの量子暗号の書物は、研究者や技術者を対象とした、比較的難解な数式や技術的に内容の濃いものが多い。そこで、本書では、ユーザーの観点から、距離感やユースケースをイメージしやすいように、できる限り運用的な場面を捉えて執筆している。本書が、読者にとって量子暗号の世界に関わるきっかけになれば幸いである。

本書の構成は以下の通りである。

第 2 章：量子暗号とは

まず量子暗号とは何か、データ通信のどこに使われるのか、既存の暗号技術や耐量子-公開鍵暗号との違いについて紹介する。ここでは特に用語を明確にすることを目的とする。

第 3 章：量子暗号に必要な構成要素

次に、量子暗号を使うために必要な構成要素について、最小限の構成であるシステム単体について説明し、次にネットワークを実現するための構成について説明する。ネットワークを構成する各レイヤの役割について、また、ネットワークが正しく動作しているかどうかを評価するための指針についても紹介する。

第 4 章： 量子暗号サービスの具体例

第 3 章の構成にて交換した鍵を、どのような分野で利用するかについて紹介する。本書では、安全保障分野・医療分野・生体認証分野におけるユースケースについて詳しく紹介する。

第 5 章：量子暗号サービスの運用

次に、量子暗号サービスを運用するにあたって、どのようなプレーヤーが関わるのか、安心して量子暗号サービスを利用するためにどのように情報セキュリティを維持すべきかについての指針を紹介する。また、標準化活動についても紹介する。

第 6 章：量子暗号技術の現状と今後の課題

最後に、量子暗号技術の世界の研究動向、そして今後の研究課題を紹介する。

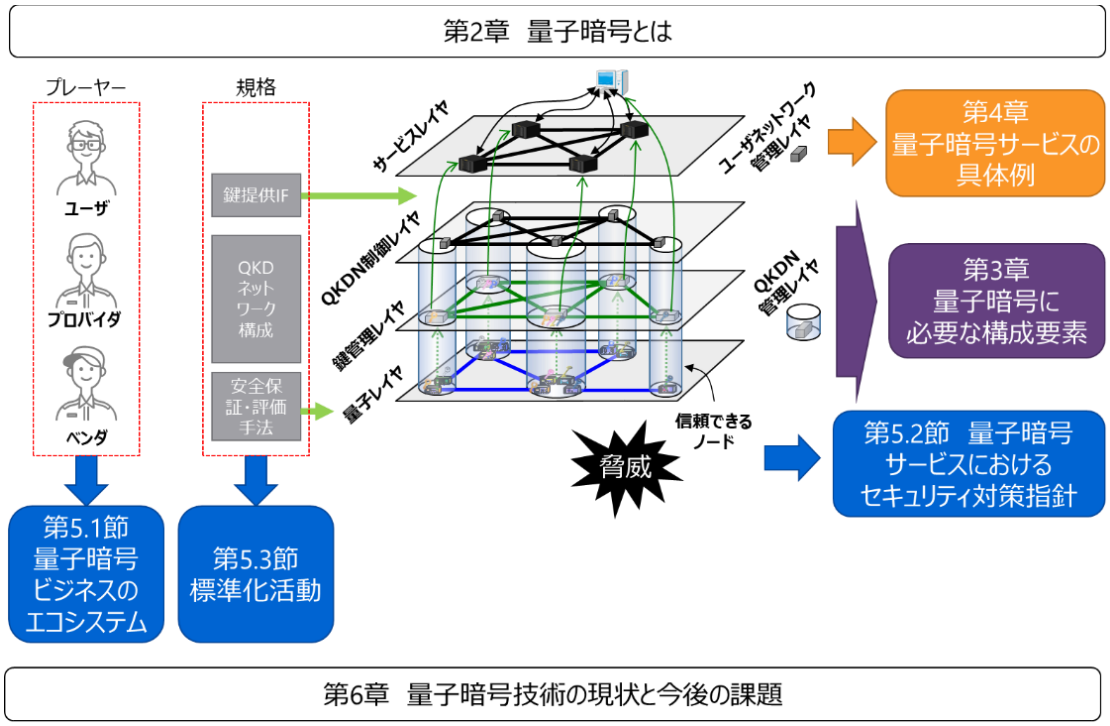


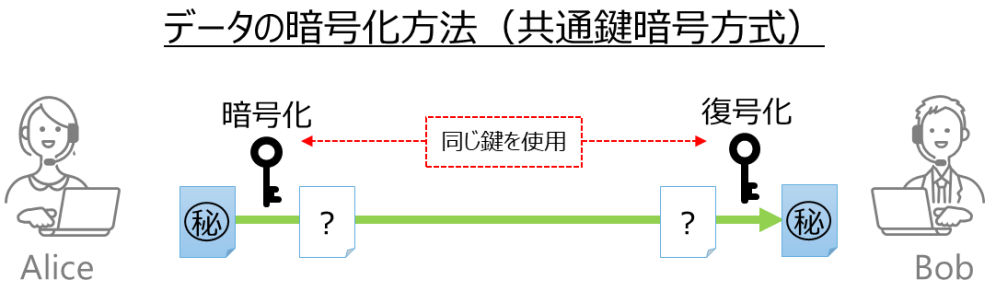
図 1：本書で扱う内容

2　量子暗号とは

量子暗号とは、量子力学の性質を利用して共有した秘密鍵を用いて、データを暗号化する暗号方式である。本章ではまず、機密情報を安全に送る方法について説明し、データの暗号化に必要となる暗号鍵交換の手法について説明する。最後に、耐量子安全性暗号の定義について紹介する。

2.1　データの暗号化方法

まず機密情報を安全に送る方法について図 2 を用いて説明する。盗聴の危険性のある通信路を使って機密情報を安全に送るには、元のデータ（平文）を適切な暗号鍵を用いて暗号化して送信し、受信した側で復号を行って復元する必要がある。一般に、暗号化・復号に係る負荷が少なく処理が高速である共通鍵暗号方式（暗号鍵＝復号鍵）が用いられる。この方式のデメリットとしては、両者が事前に鍵を交換しておく必要があり、機密情報やり取りする相手の数だけ個別に鍵を用意する必要があることである。



	特徴	
概要	データを暗号化するのと同じ鍵で復号化する	
メリット	暗号化・復号化にかかる負荷が少なく、処理が高速	
デメリット	鍵を事前に交換する必要があり、相手の数の分だけ鍵が必要となる	
アルゴリズム	**ワンタイムパッド**	平文と同じかそれ以上の長さの鍵（乱数列）を用いて暗号化する メリット：唯一情報理論的に安全な暗号方式 デメリット：十分な長さの乱数を事前に共有する必要がある
	ワンタイムパッド以外	平文よりも短い長さの鍵を用いて暗号化する（代表例：AES） メリット：事前共有する鍵の量が少ない デメリット：情報理論的に安全とは言えないため、考えうる攻撃に対して十分強固な鍵長を選ぶ必要がある

図 2：データの暗号化方法（共通鍵暗号方式）

共通鍵暗号方式は、ワンタイムパッド方式（平文と同じかそれ以上の長さの鍵を用いて暗号化）とそれ以外（平文よりも短い鍵を用いて暗号化）の方式に分類される。ワンタイムパッド方式は、唯一情報理論的に安全な暗号方式だが、一方で、十分な長さの乱数を事前に共有する必要があり、大量のデー

タをやり取りする場合には実用的ではない。ワンタイムパッド以外の方式として代表的なものは AES（Advanced Encryption Standard）が挙げられ、AES の場合平文を一定の長さごとに暗号文に変換する。事前共有する鍵の量が少なくて済む一方で、情報理論的に安全とは言えないため、考えうる攻撃に対して十分強固な鍵長を選ぶ必要がある。

2.2 暗号鍵の交換方法

上述の通り、共通鍵暗号方式でデータの暗号化を行うためには、事前に鍵を共有しておく必要がある。鍵交換の手法として、ここでは図 3 に示す 3 つを紹介する[1-2]。

(a) 鍵を直接渡す

もっとも単純な方法で、鍵を直接渡す方法である。同じ鍵を容易に共有出来るが、安全に別拠点へ持ち運ぶ必要があり、鍵が尽きたら暗号通信が出来なくなるというデメリットがある。また、鍵の運搬者には極めて重い責任を課すことになる。通信相手が n 組存在した場合、n(n-1)/2 対の鍵を配送する必要があり、大規模化に伴う複雑な鍵管理が必要となるというデメリットもある。

(b) 公開鍵暗号方式

インターネットなどで一般的に使われている方法で、鍵をやり取りするための暗号鍵と復号鍵が異なることを特徴とする。Alice は暗号鍵（公開鍵）を広く公開し、Bob はデータ暗号化用の鍵を受け取った公開鍵で暗号化して返送する。Alice は復号鍵により復号することで、データ暗号化用の鍵を得ることが出来る。この手法では、暗号鍵を公開するので、複数相手との鍵共有が容易である。一方で、暗号化・復号が複雑で処理が低速あるため、データ暗号化にはあまり用いられない。この方式は問題を解く計算の困難性を暗号の安全性の根拠としており、代表的なものとして、素因数分解問題を利用した RSA、離散対数問題を利用した楕円曲線暗号などがある。ただし、RSA と楕円曲線暗号は量子コンピュータとショアのアルゴリズムにより容易に解読できることが証明されており、近い将来安全ではなくなる。

そこで、現在 NIST が中心となって標準化を進めているのが耐量子-公開鍵暗号（Post-Quantum Cryptography）である[3]。これは、量子コンピュータでも容易に解けない問題を安全性の根拠とする方式である。格子ベース暗号、多変数多項式ベース暗号、符号ベース暗号、同種写像ベース暗号等が候補となっている。メリットとしては、現在使われている公開鍵暗号からの移行が容易であることが挙げられる。一方で、計算量的安全性を安全性の根拠としている以上、将来的に容

---

[1] "暗号技術のすべて"IPUSIRON 著，翔泳社（2017）

[2] "量子情報通信"佐々木雅英・松岡正浩　監修，オプトロニクス社（2006）

[3] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

易に解読できるアルゴリズムが発見される可能性も否定できない（危殆化のリスクがある）ため、考えうる攻撃に対して十分に安全であるか常に検証し続ける必要がある。

(c) 量子鍵配送方式（QKD: Quantum Key Distribution）

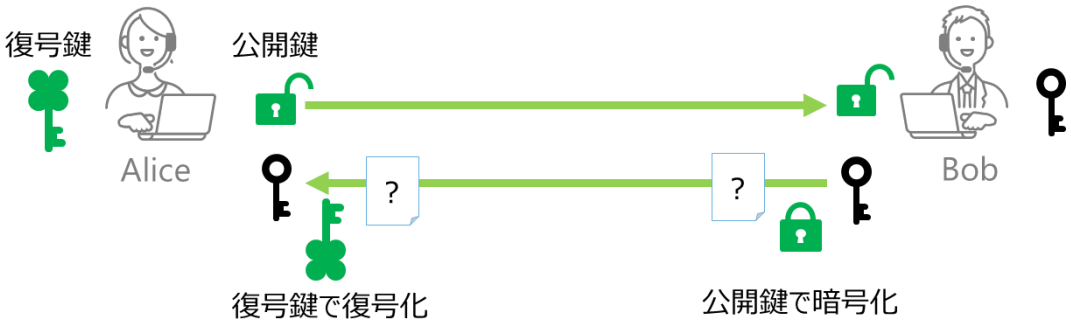
１ビットの暗号鍵の情報を１光子にエンコードすることを特徴とする。光子は分割も複製することが出来ないため、確実に盗聴を検知することが出来ることが最大のメリットである。ただし、基本的には１対１通信であり、従来の通信とは全く異なる専用装置が必要となり、現状ではコストが高い。代表的なプロトコルには BB84、CV-QKD 等がある。

データ暗号化用の鍵の共有方法

(a) 鍵を直接渡す

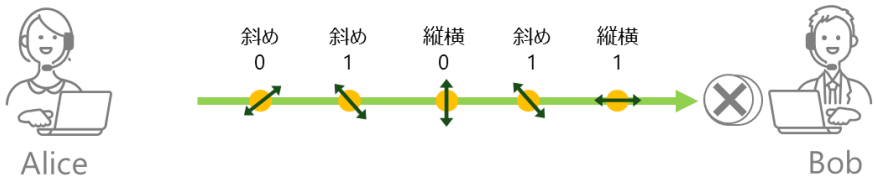
	特徴
メリット	同じ鍵を容易に共有出来る
デメリット	安全に別拠点へ持ち運ぶ必要があり、鍵が尽きたら通信が出来ない

(b) 公開鍵暗号方式



		特徴
概要		Aliceは暗号鍵 を公開し、Bobはその鍵でデータ暗号化用の鍵 を暗号化し送り返す Aliceは復号鍵 を用いて復号化してデータ暗号化用の鍵 を得る
メリット		暗号鍵を公開するので、複数の相手との鍵共有が容易
デメリット		暗号化・復号化が複雑で、処理が低速
代表的なアルゴリズム	**RSA 楕円曲線暗号**	素因数分解・離散対数問題を利用 **メリット：汎用的** デメリット：量子コンピューターとショアのアルゴリズムにより容易に解読される
	耐量子-公開鍵暗号 (Post-Quantum Cryptography)	量子コンピューターでも容易に解けない問題をベースとした暗号 **メリット：現在の暗号技術からの移行が容易** デメリット：無条件に安全とは言えないため、考えうる攻撃に対して十分安全か常に検証する必要がある

(c) 量子鍵配送方式（QKD: Quantum Key Distribution）



縦横/斜めと0/1を
ランダムに選んで送信

縦横/斜めを
ランダムに選んで受信

	特徴	
概要	Aliceは縦横/斜めと0/1をランダムに選んで送信し、Bobは縦横か斜めを選んで受信する 縦横/斜めを答え合わせして一致している場合の0/1を鍵として共有する（BB84の場合）	
メリット	光子の量子力学的性質を利用し、盗聴を確実に検知出来る	
デメリット	１対１通信、高額な専用装置が必要	
代表的なプロトコル	**BB84**	鍵情報は光子の偏光や位相にエンコードする **メリット：実証や安全性の研究が最も多い。無条件安全性が証明済** デメリット：長距離通信には高感度の検出器が必要
	CV-QKD	鍵情報は光の振幅などにエンコードする **メリット：入手容易な検出器で良い** デメリット：長距離通信が容易ではない

図 3：暗号鍵の共有方法：(a)鍵を直接渡す、(b)公開鍵暗号方式、(c)量子鍵配送方式

2.3　量子暗号と耐量子安全性暗号の定義

量子コンピュータが登場した時代に推奨される暗号技術のことを耐量子安全性暗号（Quantum-Safe Cryptography）と呼ぶ。現状では、量子コンピュータで共通鍵暗号方式を効率よく解読するためのアルゴリズムは見つかっていない。よってデータ暗号化には共通鍵暗号方式を引き続き想定する。鍵交換方法は、用途によって耐量子-公開鍵暗号方式と量子鍵配送方式を使い分けることが出来る。ただし、量子鍵配送方式で交換した鍵によるワンタイムパッド方式でのデータ暗号化が、原理的に盗聴を確実に検知でき、情報理論的に安全な唯一の方法となる。本書ではこの『量子鍵配送方式で交換した鍵によるワンタイムパッド方式でのデータ暗号化』を「量子暗号」と呼ぶ。以上を整理したものが図 4 である。

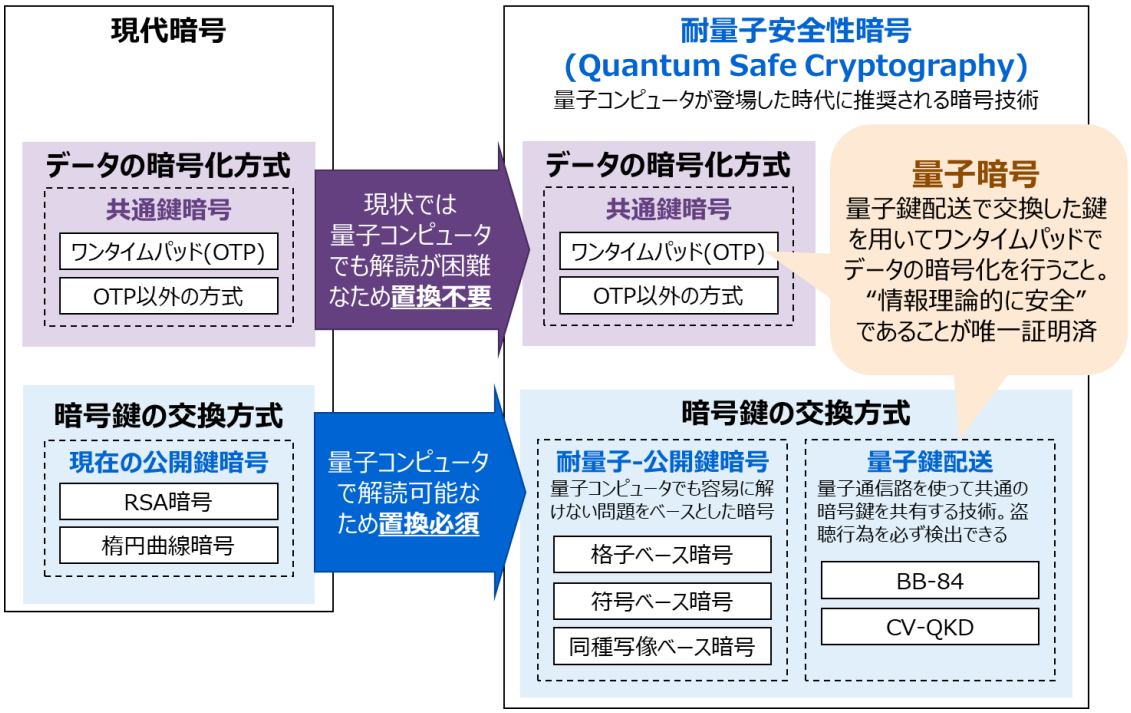


図 4：量子暗号関係の用語一覧

3　量子暗号に必要な構成要素

本章では、量子暗号を使うために必要な構成要素について説明する。QKD は本来 1 対 1 の鍵配送プロトコルだが、複数の QKD モジュールを『信頼できるノード（トラステッドノード）』内に設置し、ノード内で暗号鍵のリレー配送を行うことで、QKD をネットワーク化し広域で安全な鍵交換を行うことが出来る。複数のトラステッドノードを QKD で接続してネットワーク化し、鍵リレーなどに必要な鍵管理機能を搭載したシステムを一般に『QKD ネットワーク』と呼ぶ。まず 3.1 節で最も基本的な構成要素である 1 対 1 の QKD システム（単体）について説明し、3.2 節では QKD ネットワークの構成要素について説明する。

3.1　QKD システム

3.1.1　QKD システムの構成要素

QKD は、暗号に使用する鍵を共有する手法であり、一般的には送信者 Alice から量子力学的な状態にエンコードした鍵情報を送信し、受信者 Bob が受け取った状態の変化を調べることで、途中の通信路でどのような盗聴が行われたのか知ることができることが特徴である。量子力学的な状態を送るための量子通信路と、事後処理に必要な情報を送るための公開通信路の 2 種類の通信路を用いる。この 2 種類の通信路をまとめて QKD リンクと呼ぶ。

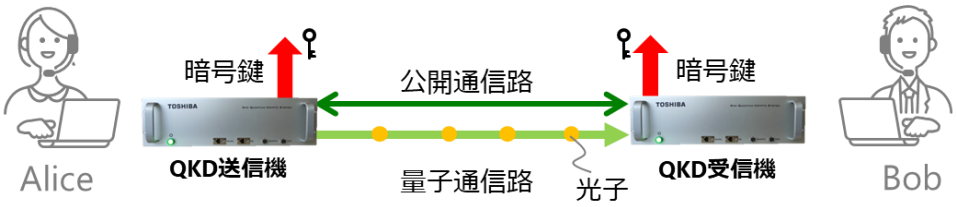


図 5：QKD システムの基本構成

次に、この構成での暗号鍵の生成プロセスについて図 6 を用いて説明する。①のプロセスを量子通信と呼び、②から⑤までのプロセスをまとめて鍵蒸留と呼ぶ。QKD は量子通信と鍵蒸留からなる。量子暗号とは、①～⑤に加えて⑥QKD で共有した鍵を用いたワンタイムパッド方式でのデータの暗号化を含む。

① 量子通信路（光ファイバーまたは自由空間）を用いて量子力学的な状態を送信する。
② 鍵として送信した信号の情報について、公開通信路を介し共有し受信ビットのふるいわけ（sifting）を行う。ここで生成されるのがふるい鍵（選別後データ）である。
③ ふるい鍵には光ファイバーのロス等に起因するビット誤りがわずかに含まれている。また、盗聴が発生した場合にも、ビット誤り率が上昇する。そこで、サンプルビットを選び比較することで漏洩情報量を評価する。
④ シンドローム（パリティ情報）を公開し、誤り訂正符号を用いてお互いのふるい鍵の食い違いの訂正（誤り訂正処理）を行う。

⑤　誤り訂正後の鍵（訂正鍵）をランダムに選んだハッシュ関数に入力して秘匿性増強処理を行う。この処理により盗聴や誤り訂正で漏れた情報と、最終的に得られる暗号鍵の相関をほぼゼロにすることができる。

⑥　QKD で共有した鍵を用いてワンタイムパッド（OTP）方式でデータの暗号化・送信・復号を行う。

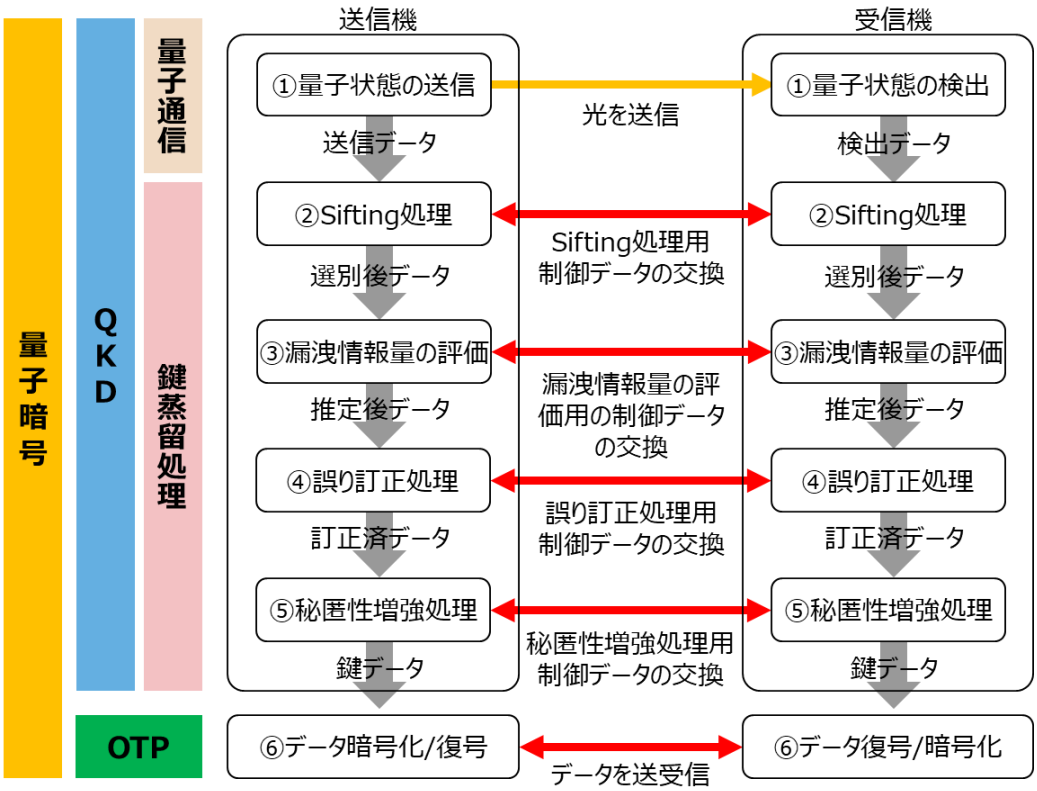


図 6：QKD による暗号鍵共有フロー及びデータ暗号化フロー。QKD は量子通信と鍵蒸留からなる。

3.1.2　鍵情報のエンコード方法

鍵情報を量子力学的な状態にエンコードするためには、大きく分けて、鍵情報を単一光子の偏光や位相に乗せる手法（BB-84 方式等）、鍵情報を光の振幅に乗せる手法（CV-QKD 方式）がある。その他、2 つのパルスの位相差等にエンコードする手法がある。本節では、最も研究が多く行われている BB-84 方式と、既存の光通信技術との親和性が高い CV-QKD 方式について簡単に紹介し、その比較を行う。詳細については付録 A に付記した。2 つのパルスの位相差等にエンコードする方式については参考文献[4,5]を参照のこと。

---

[4] K. Inoue *et al.*, Phys. Rev. Lett. 89, 037902 (2002).

[5] D. Stucki *et al.*, Opt. Exp. 17, 13326 (2009).

BB-84 と CV-QKD の最も大きな違いは、光の検出方法が異なる点である。これは鍵情報を離散量または連続量にエンコードしているかの違いに起因する。BB84 は高価な単一光子検出器が必要となる一方で、CV-QKD は安価なホモダイン検出器を利用することができる。ただし、鍵の生成レートは現状 BB84 が大幅に高く、長距離での伝送実績もある。ファイバー内のデータ通信との共存は、CV-QKD ではデータ通信の増幅が可能である点が優位である。無条件安全性は、BB84 のみ証明済みである。

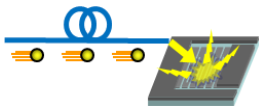
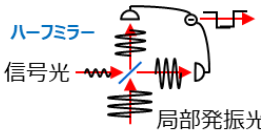
項目	BB84	CV-QKD
概要	鍵情報は光子の偏光や位相（離散量）にエンコードする	鍵情報は光の振幅や位相（連続量）にエンコードする
光検出	単一光子検出器を利用  単一光子検出器で光子数をカウント	◎**標準的なホモダイン検出器を利用**  ハーフミラー 信号光 局部発振光 ホモダイン検出器で位相・振幅を測定
鍵生成レート	◎**13.72 Mbps @ 10 km** [6] ◎**100 kbps @ 100 km** [7] ◎**10 kbps @ 150 km** [7] ◎**10 bps @ 240 km** [7]	1 Mbps @ 25 km [8] 0.5 kbps @ 100 km [9]
ファイバー内のデータ通信との共存可否	追加のフィルターが必要 データ通信の増幅不可 実験例:2 波多重した計 200Gbps のデータと共存伝送[10]	◎**追加部品不要** ◎**データ通信の増幅可能** 実験例:100 波多重・光増幅した計 18.3Tbps のデータと共存伝送[11]
技術成熟度	◎**実装・評価実績多数**	新技術のため実装評価が必要
安全性証明	◎**無条件安全性が証明済み**	変調法に応じ，攻撃モデルに制限
用途	安全保障分野などのハイエンド向け	民生用途向け
装置サイズ	19 インチラックマウント	
価格	検出器・干渉計のため高額	◎**汎用品で製造可能なため比較的低価格**
メーカー	東芝, IDQ, NEC, QuantumCTek	NEC, Huawei Research

表 1：BB-84 と CV-QKD の比較

[6] Z. Yuan *et al.*, J. Lightwave Technology 36, 3427 (2018)
[7] B. Fröhlich *et al.*, Optica. 4, 1, 163, (2017)
[8] D. Huang *et al.*, Opt. Express 23, No. 13, 17511 (2015)
[9] D. Huang *et al.*, Sci. Rep. 6, 19201 (2016)
[10] J. F. Dynes *et al.*, Sci. Rep. 6, 35149 (2016)
[11] T. A. Eriksson *et al.*, Commun. Phys. 2、9 (2019)

3.2　QKD ネットワーク

量子状態を中継するための技術は現状まだ研究段階であり、QKD システムの 1 リンクあたりの伝送距離には光損失による制限がある。また基本的に QKD システムは 1 対 1 通信である。そこで、複数のトラステッドノードを QKD で接続し、鍵リレーなどに必要な鍵管理機能（KM: key manager）を搭載して QKD をネットワーク化することで、広域で安全な鍵交換を行うことが可能となる。

ここでトラステッドノードとは、物理的・ネットワーク的なアクセスが制限されており、権限のある人間以外入退室、ネットワークアクセス、メディア接続、データ持ち出し等が出来ないエリアのことを言う（図 7）。

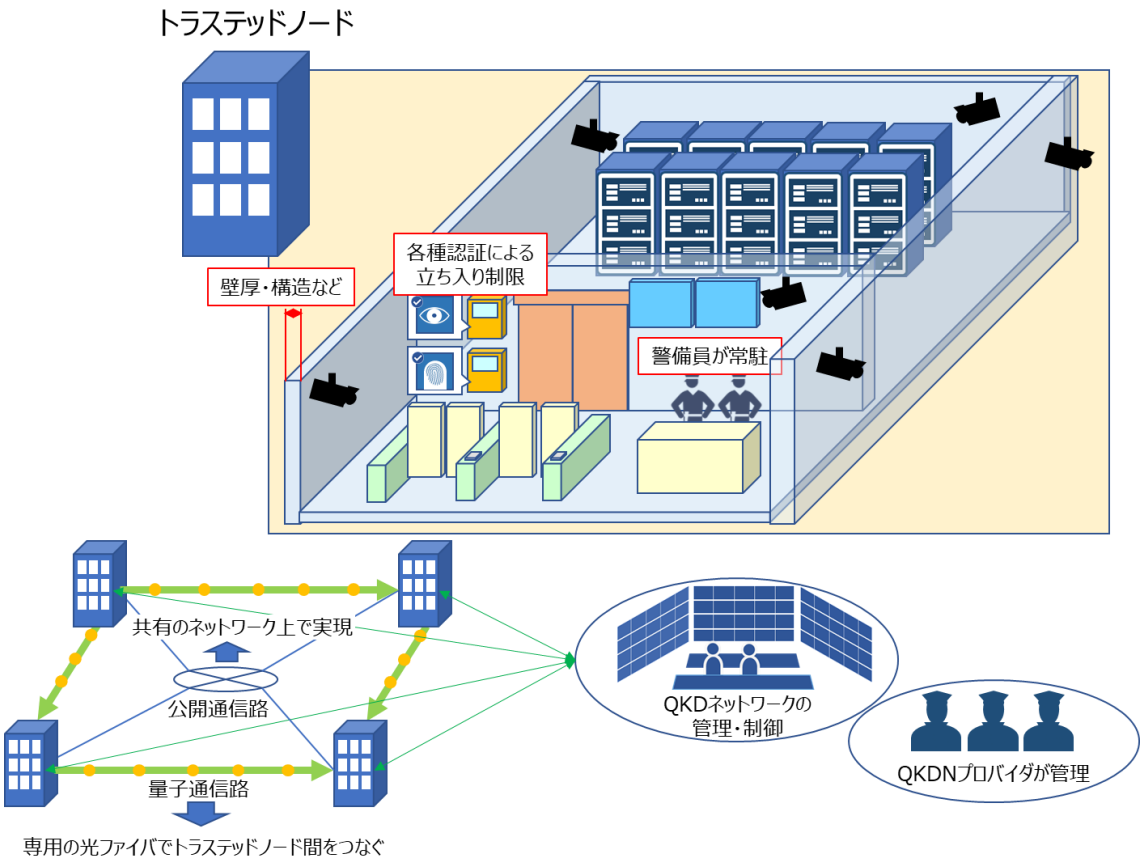


図 7：トラステッドノードのイメージ図

トラステッドノード 3 つの場合の QKD ネットワークの概念図を図 8 に示す。トラステッドノード 1 と 2 の間で共有された鍵を、トラステッドノード 2 と 3 の間で共有された鍵により暗号化して伝送する（カプセル化）する方式と、トラステッドノード 1 の KM が別途生成した鍵を、それぞれの経路で共有された鍵により暗号化して伝送する方式がある。暗号鍵を生成・供給するためのネットワークを QKD ネットワークまたは QKDN と呼び、暗号アプリケーションを利用するネットワークをユーザーネットワークと呼ぶ。

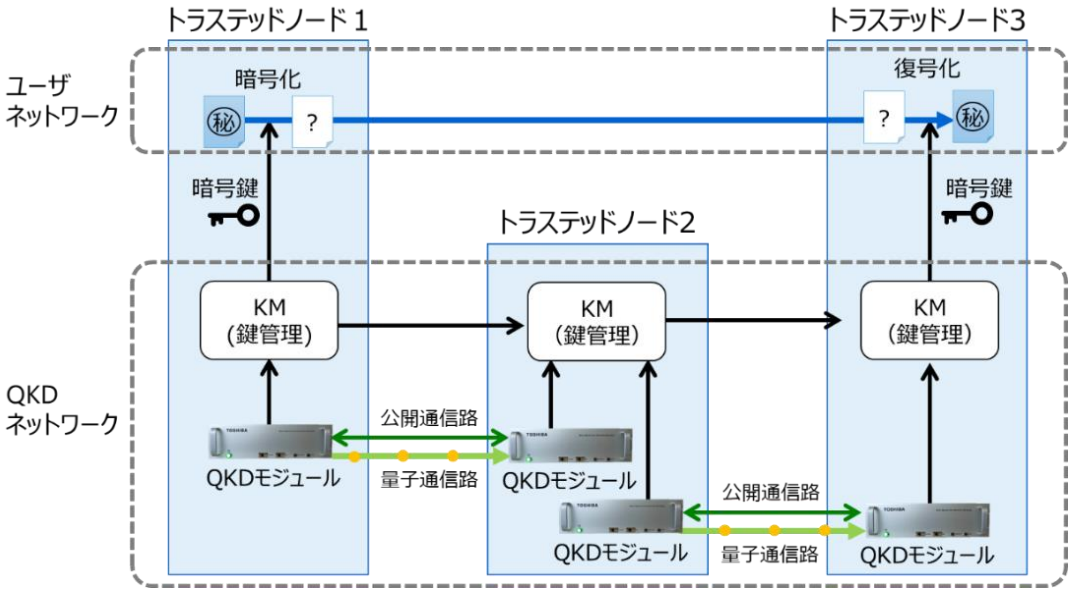


図 8：トラステッドノードを介した鍵リレーの概念図

3.2.1 QKD ネットワークの構成要素

より詳細な QKD ネットワークの構成は QKDN アーキテクチャとして定義される。本節ではまず QKDN アーキテクチャ全体について説明し、次に各レイヤについて説明する。

図 9 に示すように、QKDN アーキテクチャは下から量子レイヤ、鍵管理レイヤ、QKDN 制御レイヤ、さらにこれら 3 レイヤを管理するための QKDN 管理レイヤで構成されている。これらの 4 レイヤによって鍵が生成されて、最上位のサービスレイヤへ供給される。量子レイヤは QKD モジュールと、QKD リンクから構成される。鍵管理レイヤは KM 及び KM リンクから構成され、QKDN 制御レイヤは QKDN コントローラとリンクから構成される。QKDN 管理レイヤには QKDN マネージャが含まれる。サービスレイヤは利用者によって構成が異なるが、暗号化通信を実現するためのアプリケーションやコンピュータモジュールなどで構成される。サービスレイヤの具体例については 4 章で詳しく説明する。

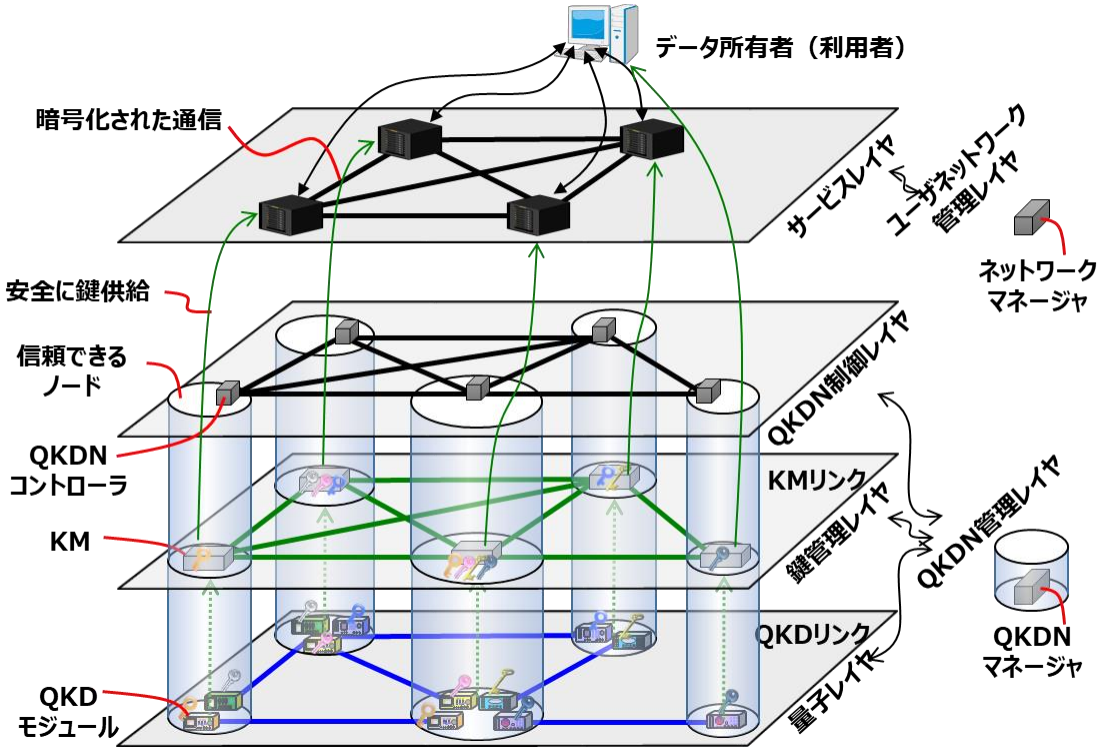


図 9：QKDN アーキテクチャ

次に各レイヤの機能について表 2 を用いて説明する。

量子レイヤは、別拠点にある QKD モジュールとの間で光子と古典情報をやり取りして、実際に鍵となる乱数列を共有するのが主な機能となる。さらに、KM へ乱数列を供給する機能を有する。

鍵管理レイヤの主な機能としては、実際にデータの暗号化を行うアプリケーションへの鍵の供給、及び KM リンクを通した他の拠点への鍵リレーなどがある。これに付随して、アプリケーションとの鍵要求の受信やインターフェースの格納など鍵管理全般を担う。

QKDN 制御レイヤは QKD ネットワーク全般のサービスの制御を行う。

QKDN 管理レイヤは、各レイヤからパフォーマンス情報を収集し、サービスが適切に稼働しているかを監視して、必要に応じて制御を QKDN 制御レイヤへ命じる機能を持つ。

レイヤ名	機能	関係要素
量子レイヤ	対称なランダムビットストリングを生成する	QKD モジュール、 QKD リンク
	KM へランダムビットストリングを供給する	QKD モジュール→KM
	QKDN マネージャへ QKD リンクパラメータを送信する	QKD モジュール →QKDN マネージャ
鍵管理レイヤ	ランダムビットストリングを受信する	QKD モジュール→KM
	同期・再フォーマット・鍵として格納する	KM
	暗号アプリケーションのインターフェースを格納する	KM
	暗号アプリケーションから鍵要求を受信する	アプリケーション→KM
	KM リンクを介して暗号アプリケーションと同期・認証し鍵を供給する	KM→KM リンク→KM
	KM リンクを介して鍵リレーを行う	KM→KM リンク→KM
	QKDN コントローラに適切なリレールートを尋ねる	KM→QKDN コントローラ
	鍵管理ポリシーを適用する	KM
QKDN 制御レイヤ	鍵リレーのルーティング制御	QKDN コントローラ→KM
	QKD モジュール、QKD リンク、KM、KM リンクの制御	QKDN コントローラ→all
	QKD サービスのセッション制御	QKDN コントローラ
	認証と認可制御	QKDN コントローラ
	QoS および課金ポリシー制御	QKDN コントローラ
QKDN 管理レイヤ	QKDN 全体のパフォーマンス情報を収集する	All→QKDN マネージャ
	KM での鍵ライフサイクル管理をサポートする	QKDN マネージャ→KM
	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管理を行う	QKDN マネージャ
サービスレイヤ	KM から鍵を受け取る	アプリケーション
	暗号化通信を実行する	アプリケーション
ユーザーネットワーク管理レイヤ	ユーザーネットワーク内の仮想化/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	ネットワークマネージャ

表 2：QKD アーキテクチャの各レイヤの機能一覧

3.2.2　QKD ネットワークの機能要件の評価

QKD ネットワークが正常に動くかどうかを判定するための、機能要件評価を行う指針について説明する。具体的には、表 2 で示した各レイヤの機能一覧を参考として、各要素の単体試験項目、システム試験項目、連接試験項目、総合試験項目を洗い出す必要がある。単体、システム、連接、総合の定義を表 3 に、模式的に表したものを図 10 に示す。

種類	説明	構成要素
単体	レイヤ内の最小単位	1 対 1 の QKD モジュールとその間の QKD リンク、1 対 1 の KM と KM リンクなど
システム	1 対 1 の QKD の最小構成	QKD モジュールと QKD リンクと KM と KM リンク
連接	QKD ネットワーク	2 つ以上の QKD システムと QKDN 管理・制御レイヤ
総合	大規模ネットワーク	2 つ以上の QKD ネットワークと衛星等の空間伝送リンク

表 3：単体、システム、連接、総合の定義

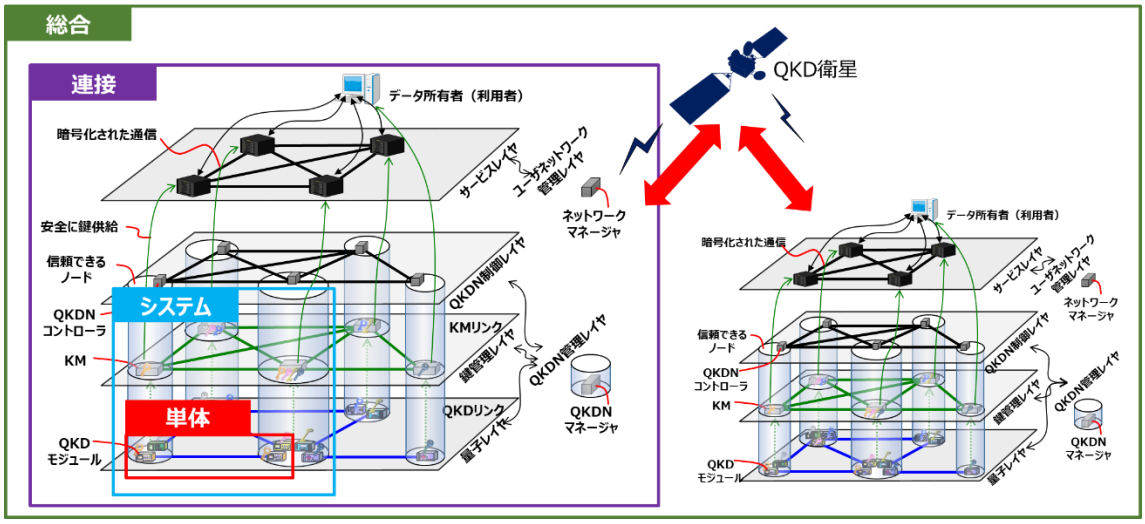


図 10：評価試験の範囲

総合の範囲としては、2 つ以上の QKD ネットワークを衛星等の空間伝送リンクでつないだ大規模ネットワークを定義した。これは、QKD ネットワークの主要拠点同士をつなぐことで、長距離離れた地方同士をつなぐ、離島と本島をつなぐなどの活用方法が考えられる。現状では原理実証の段階であり、試験項目については今後の検討事項であるため、本書では割愛する。

表 4 に単体、システム、表 5 に連接の試験項目と評価方法の例を示す。ただし、ここに示す評価項目はあくまで大項目であり、実際にはより詳細な小項目へと分岐する。評価の小項目・具体的な評価方法は実装方式によって異なる。また、サービスレイヤに関しては、サービスごとに異なるためこちらも割愛する。

種類	要素	評価項目	評価方法
単体試験	QKD モジュールと QKD リンク	量子状態の送信/受信	検出器の出力を計測
		ふるい鍵の生成	ふるい鍵の出力を確認
		盗聴情報の評価	評価結果の確認
		誤り訂正処理	訂正済データ出力確認
		秘匿性増強処理	処理済データの出力確認
	KM と KM リンク	同期・再フォーマット・鍵として格納	格納ファイルを確認
		暗号アプリケーションのインターフェースを格納	格納ファイルを確認
		鍵管理ポリシーの適用	ポリシー適用確認
		アプリケーションと同期・認証	テストアプリでのメッセージ確認
		アプリケーションへの鍵提供	テストアプリでの鍵受取確認
システム試験	QKD モジュールと KM	QKD モジュールが KM へ鍵を供給	送受信した鍵の整合性確認
		KM が鍵を受信	

表 4：試験項目・評価方法の例（単体・システム）

種類	要素	評価項目	評価方法
連接試験	QKDN コントローラ	QKD サービスのセッション制御、認証と認可制御、QoS 及び課金ポリシー制御	それぞれ設計通りに動作していることを確認
	QKDN コントローラと QKD モジュール	QKDN コントローラが QKD モジュールへ制御パラメータ送信	送受信データの整合性確認及び制御パラメータ通りの動作確認
		QKD モジュールが制御パラメータを受信	
	QKDN コントローラと KM	QKDN コントローラが KM へ制御パラメータ送信	
		KM が制御パラメータを受信	
		KM が QKDN コントローラに最適な鍵リレールートを尋ねる	送受信データの整合性確認及びルートが最適であるかを検証
		QKDN コントローラが KM へ鍵リレーの最適ルート送信	
		QKDN コントローラが KM へ鍵リレーの最適ルート受信	
		KM が鍵リレーを行う	指定ルートのリレーが実施されているかを確認
	QKDN マネージャ	障害、構成、アカウンティング、パフォーマンス、セキュリティ管理、及び KM での鍵ライフサイクル管理サポート	それぞれ設計通りに動作していることを確認
	QKDN マネージャとQKDモジュール	QKD モジュールが QKDN マネージャへ QKD リンクパラメータ送信	送受信データの整合性確認
		QKDN マネージャが QKD リンクパラメータを受信	
	QKDN マネージャと KM	KM が QKDN マネージャへ KM リンクパラメータを送信	
		QKDN マネージャが KM リンクパラメータを受信	
	QKDN マネージャと QKDN コントローラ	QKDN コントローラが QKDN マネージャへ制御パラメータ送信	
		QKDN マネージャが制御パラメータを受信	

表 5：試験項目・評価方法の例（連接）

4　量子暗号サービスの具体例

本節では、実際に QKD システムや QKD ネットワークで共有した鍵をどのような分野で利用できるのか、どのような分野から適用されるべきか、そして適用の際の具体的な構成、効果について紹介する。

応用先としては、情報漏洩の影響が大きく高いセキュリティレベルが要求される分野を想定した。国家安全保障に関わる分野の中でも、特に防衛分野への適用について（4.1 節）、人命に大きく影響を与える医療分野の中でも特に子孫などの広範囲への影響の大きい遺伝子情報分野への適用について（4.2 節）、技術が成熟しておりすでに空港等へ導入間近の顔認証の分野について（4.3 節）、紹介する。

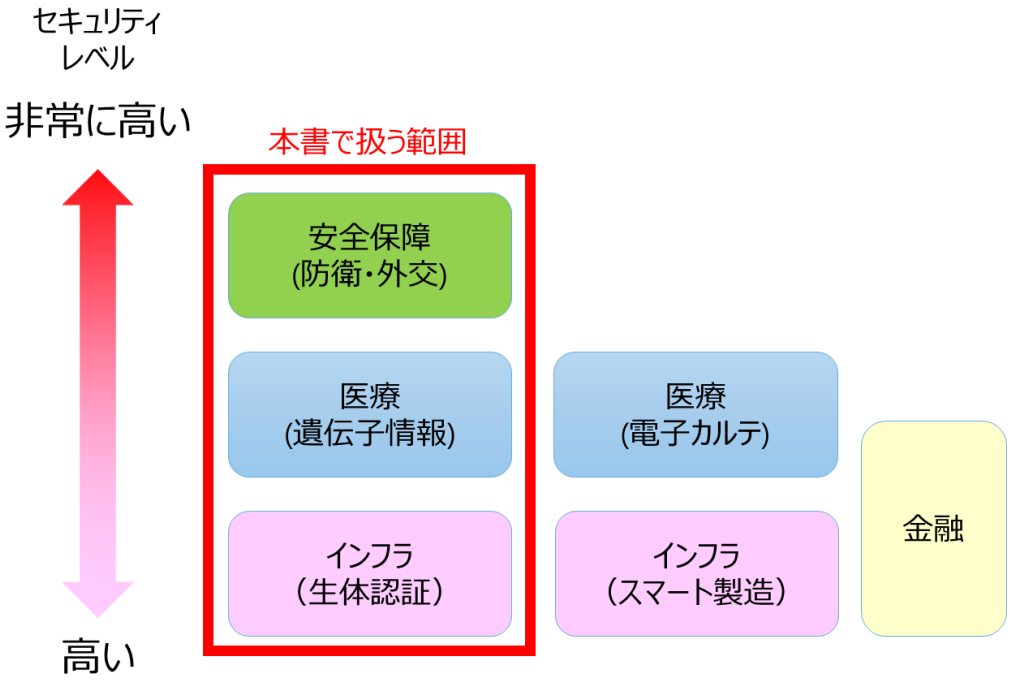


図　11：セキュリティレベルとユーザー適用分野

4.1　安全保障（防衛・外交）分野でのユースケース

4.1.1　　想定する運用場面

自衛隊の任務として BMD 対処・不審船対処・災害派遣の他、島嶼防衛、国際貢献活動を想定し、これらの活動時の通信に対して量子暗号を適用することを検討する。陸・海・空の各自衛隊が共同で活動する統合任務部隊においては各自衛隊の連携が重要であると想定され、防衛省及び各自衛隊の主要司令部間の作戦情報等の通信を主な対象として設定した。また、関係する各府省庁との連携も必要になると考え、防衛省を含めた各省庁と内閣府の間の通信も対象として設定した。想定する運用場面の全体構想を図 12 に示す。

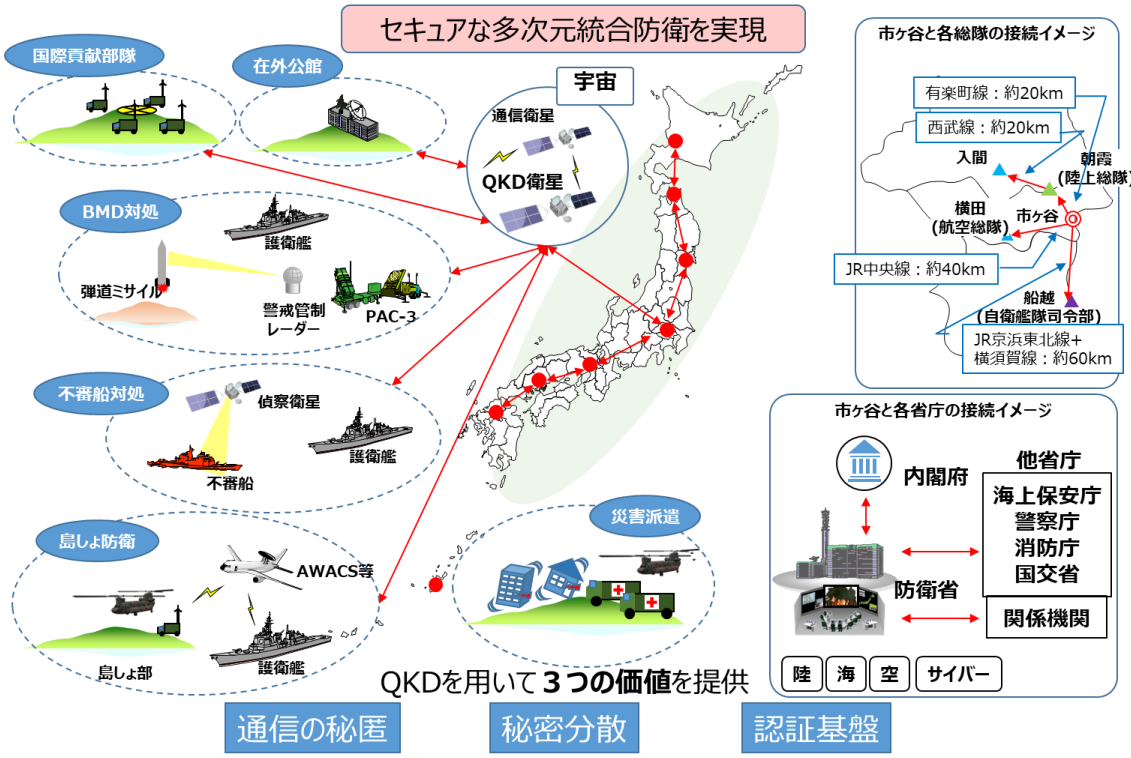


図　12　自衛隊における量子セキュアネットワーク運用構想

次に、市ヶ谷防衛省と陸・海・空の各司令部との通信に適用した場合の適用イメージを図 13 に示す。指揮システムにおける指揮命令通信など、全国の駐屯地・基地等の間での重要な通信に対して適用するイメージである。

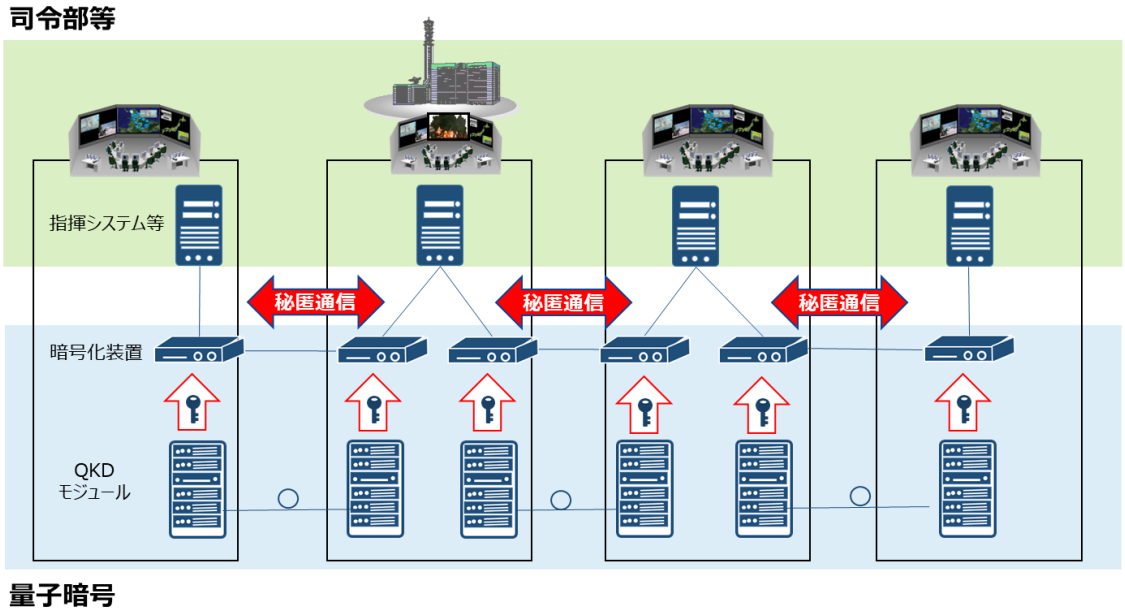


図 13 防衛省と各自衛隊の司令部間通信への量子暗号の適用イメージ

4.1.2 必要性

既存の暗号技術の課題として以下のものがあげられ、量子暗号による対策が必要となる。

① 危殆化の脅威

特定秘密保護法[12]では最大 30 年の保護期間が指定されているように、防衛に関する事項は長期の秘匿化が必要だが、既存暗号は計算技術や数学理論の進歩とともに危殆化の恐れがあるため、秘匿性を担保できなくなる可能性がある。

② 盗難が検知できない危険性

盗難などによる暗号化した秘密の情報が漏洩した場合、検知することができないため、作戦行動において不利な状況となる可能性がある。

③ 相互接続の困難性

陸・海・空の統合運用をするためには組織間の相互連携が必要となるが、それぞれの組織で非公開の組織間通信を使用しており秘匿方式の開示など秘密の情報を提供できない場合、異なるシステム間での相互での秘匿通信ができない。

④ 鍵の運搬時の盗難の危険性

人手を介して鍵を配付する場合、盗難のリスクが伴う。鍵の安全な配付ができなければ、盗聴され解読される可能性があるため、暗号通信そのものが出来なくなることが考えられる。

---

[12] 特定秘密の保護に関する法律(https://www.cas.go.jp/jp/tokuteihimitsu/gaiyou.pdf)

4.1.3　有効性

前述の既存の暗号技術の課題に対して、量子暗号を用いることの有効性を以下に記す。

① 量子暗号は、危殆化の恐れが無いので、計算技術や数学理論の進歩があっても破られない。防衛に関する特定秘密の長期的な保護が可能となる。

② QKD は特徴として暗号鍵の盗聴を必ず検知できるという特性がある。盗聴されることなく交換した暗号鍵を使ってワンタイムパッドで暗号化することで、通信路上のデータは、盗聴・盗難されても解読不能である。

③ 暗号化は鍵と平文の単純な論理和であるため、処理遅延を解消することが出来る。暗号方式も公開済みであるため、異なるシステムを有する組織をまたぐ相互接続が容易となる。

④ QKD により鍵を配送することで盗難のリスクを無くすことが可能となる。また暗号鍵の盗聴は検出可能かつ鍵情報をリアルタイムに伝送可能であるため、安全な鍵の共有により安定した暗号システムの運用が可能となる。

4.1.4　システム構成案と適用の効果

防衛省内組織間の通信へ量子暗号を適用する場合と、防衛省と関係する各府省庁間の通信へ量子暗号を適用する場合について、それぞれシステム構成案を紹介する。

防衛省と陸・海・空の各司令部間の通信へ量子暗号を適用

市ヶ谷の防衛省と、陸上自衛隊朝霞駐屯地、航空自衛隊横田基地及び海上自衛隊船越地区それぞれと量子暗号によるデータ伝送を行う場合を想定する。

各駐屯地及び基地に QKD モジュール、鍵管理・供給サーバー及び暗号化装置を設置する。防衛省と朝霞駐屯地間及び防衛省と横田基地間については短距離（直線で 20-40km）であるため、QKD モジュール間は直接光回線で結び構築する。防衛省と船越地区間は 50km を超えるため、中継地点として、QKD モジュールと鍵管理・供給サーバーを設置することを想定する。設置拠点は保全されている必要があることから厚木基地又は座間駐屯地への設置を仮定する。防衛省と各駐屯地及び基地間を接続したイメージを図 14 に示す。市谷と各総隊をつないだ場合の、提供形態・機器購入・システム構築のイメージである。

適用の効果としては、4.1.3 節でも述べた通り、長期的な安全性に加えて、鍵の物理的な輸送にかかる人的リソースおよびコストを減らすことができること、OTP による暗号化は鍵と平文の単純な論理和であるため、処理遅延を解消し、鍵 ID の管理により異なるシステムを有する組織をまたぐ互換性を確保可能である点が挙げられる。

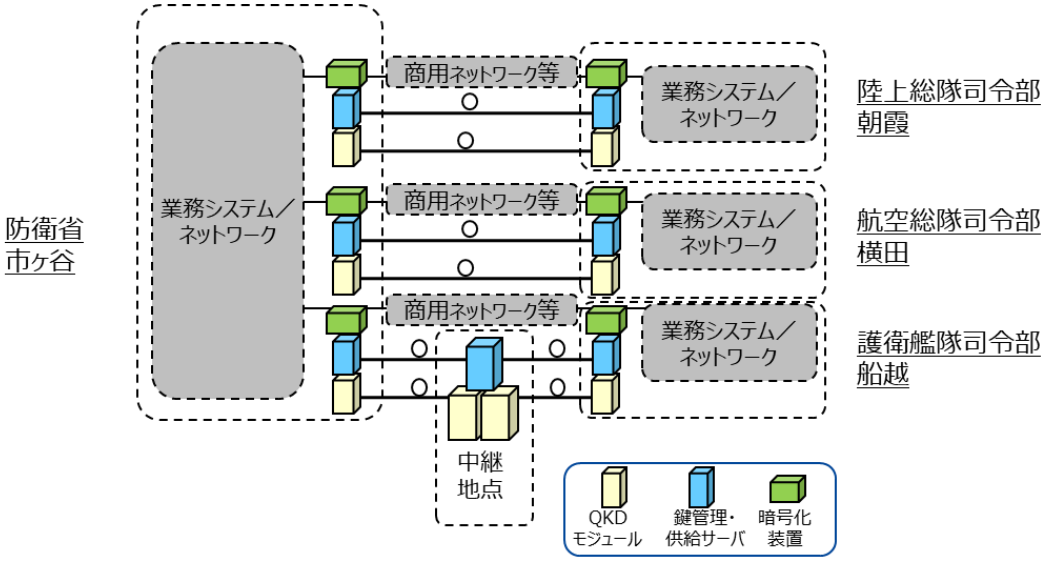


図 14 防衛省と各司令部間通信への量子暗号適用イメージ

内閣府と各省庁間の通信へ量子暗号を適用

内閣府と各省庁間の通信へ量子暗号の適用を想定する場合、霞ヶ関エリア半径 5 Km 圏内に各機関が存在することから、内閣府を中心にスター型で直接接続が可能となる。内閣府と各省庁間を接続したイメージを図 14 に示す。

適用の効果としては、4.1.3 節でも述べた通り、長期にわたって国家機密を守ることが出来る点が挙げられる。

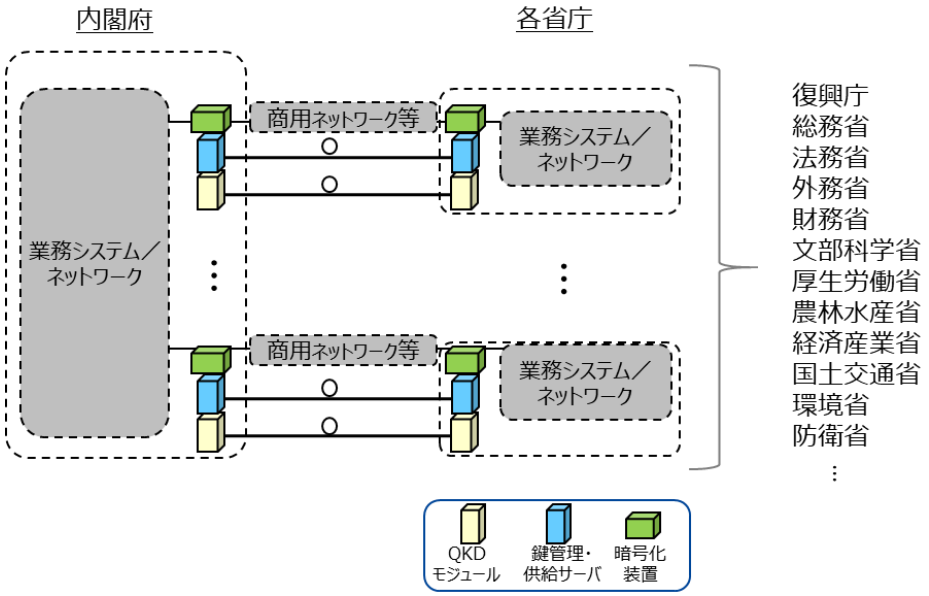


図 15 内閣府と各省庁間基幹通信への量子暗号適用イメージ

4.2　医療分野におけるユースケース

4.2.1　想定する運用場面

がんゲノム医療への量子暗号の適用を想定する。がん組織を遺伝子解析することにより、化学療法では効果のなかったがんに対して、例えばがんの発生臓器に関する情報や、効果が期待される治療薬の情報（分子標的薬や臨床検証を含む）などの情報を得られる可能性がある。このがんゲノム医療に対して、日本政府として積極的に取り組む動きが近年加速している。2018 年にがんゲノム医療推進コンソーシアム運営会議が発足し、2019 年 4 月には、ゲノム医療を牽引する機能を持つ中核拠点病院として全国 11 病院、中核拠点病院と協力してゲノム医療を行う連携病院が 156 施設認定された。また、全国から遺伝子配列データや臨床情報を集約し、がん知識データベースの構築・管理を行うための機関としてがんゲノム情報管理センターも設置された。さらに 2019 年 9 月にゲノム医療を行うことのできる中核拠点病院として全国 34 か所が認定された。

次にがんゲノム医療の流れを図 16 を用いて説明する。

① まず病院で患者説明が行われ、がん組織の採取・検体の準備が行われる。
② その後検体を持ち込んだ検査機関等でシーケンスが実施され、遺伝子配列データが生成される。
③ 遺伝子配列データを過去の症例等のデータと比較し、解析レポートを作成する。
④ 専門家による会議（エキスパートパネルという）が開催され、解析レポートの解釈、診療方針の策定を行う。専門家が遠隔地にいる場合には、Web 会議により開催されることもある。
⑤ エキスパートパネルの結果を元に、患者説明・治療が行われる。

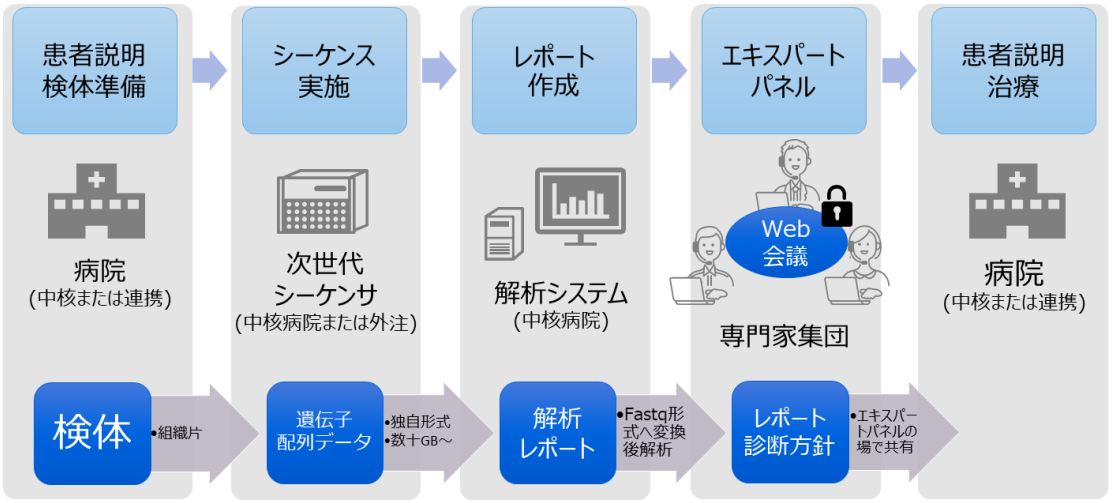
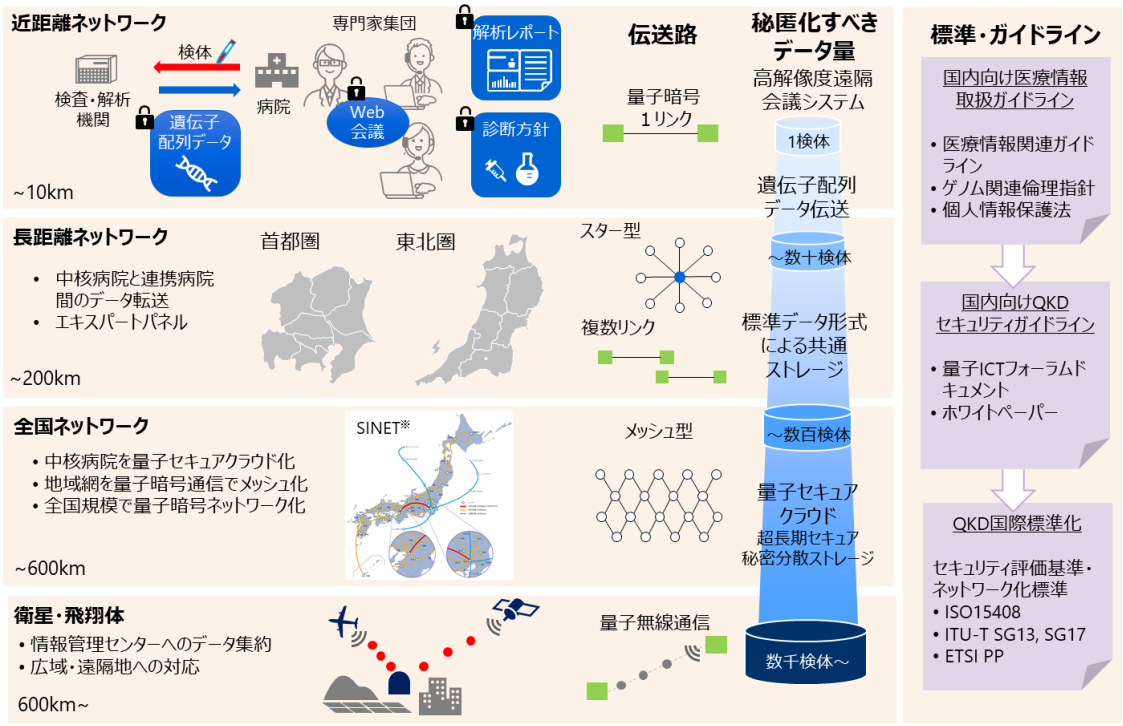


図 16：クリニカルシーケンスの流れと、各工程で生成されるデータ

この一連の検査工程はがんクリニカルシーケンスと呼ばれ、精密医療のひとつとして注目を集めている。工程②では遺伝子配列データ、③では解析レポート、④では診療方針や Web 会議のデータが生成される。次節で説明するが、これらのゲノム情報については適切に保護する必要があるため、すべてのデータの伝送に量子暗号を用いることを想定する。

運用構想図を図 17 に示す。上記で説明したがんクリニカルシーケンスを最小のユニットとして、発生するゲノム情報を量子暗号で保護して伝送することを想定したのが近距離ネットワークである。将来的には、スター型、もしくは複数リンクを数珠つなぎする長距離ネットワークや、メッシュ型の全国ネットワークでの運用も考えられる。また、有線だけでなく量子衛星を利用した量子無線通信を利用することで、広域・遠隔地とのデータ通信についても可能となると想定される。



※学術情報ネットワークSINET5ホームページより（https://www.sinet.ad.jp/）

図 17：がんゲノム医療における量子セキュアネットワーク運用構想

4.2.2　必要性

前節で説明した通り、がんクリニカルシーケンスでは、遺伝子配列データ、解析レポート、診断方針等の機密情報が生成される。一般的に、個人データ解析においては、個人の特徴に関する情報（罹患リスク等）と、個人を識別するための情報（名前等）を切り離すことで匿名化が可能だが、ゲノム情報についてはゲノム自体が個人の特徴に関する情報ともに、個人を識別する情報も有していることから、切り離して扱うことが困難である[13]。

これらのゲノムデータやゲノム情報等が流出した場合、本人だけでなく、遺伝子情報が一部共通する親族や子孫にまで不当な差別や偏見等の大きな影響が及ぶ可能性がある。また、ゲノム解析技術の進歩により、影響の程度が大きく変わりうる。現在安全とされている暗号技術により暗号化した場合においても、解読技術の進歩により、暗号化データを盗んでおいて将来的に量子コンピュータによって解読される危険性もある。よって、ゲノムに関する情報の扱いは非常に高いレベルの安全性、つまり解読技術が進歩しても破られない暗号により保護する必要がある。

現状では、ゲノム配列情報の伝送は、シーケンスがすべて終了した後に物理ディスクへ保存し、ディスクを輸送することで行っている。ただし輸送中の紛失・盗難のリスクを否定できない。

また、ゲノム配列情報は過去の報告例と照合して現在効果が期待される治療情報を得るために用いられるが、報告例の蓄積により、再度照合作業を行うことで、過去の照合では得られなかった新たな情報を得られる可能性があるため、ゲノム配列情報を適切に長期保管する必要もある。

4.2.3　有効性

そこで、がんゲノムシーケンスにおいて発生した機密情報に対して量子暗号で暗号化したデータをネットワーク上で伝送することを提案する。量子暗号は、情報論的安全性の証明された唯一の方法であり、量子コンピュータが実現した後においても安全な手法である。実用的な量子コンピュータが実現した後でも、暗号化されたデータを解読される危険が無い。また、現状の物理的なディスクの輸送に比べて、早く届けることが可能となる。例えば、遺伝子配列データを出力するシーケンシングには、場合によっては数日を要する。解析し終わるのを待つことなく、遺伝子配列データを出力した順に順次量子暗号で暗号化して伝送することで、解析終了とほぼ同時に伝送を終了することも可能となる。量子暗号を適用することにより、安全な伝送、迅速な伝送の 2 点を実現することができる。

また、ゲノムデータの適切なバックアップについては、QKD で共有した鍵を利用した秘密分散法による長期保管を提案する。例えば XOR を用いた(K,N)閾値秘密分散法という秘密分散方式を用いる。この方式は、保護対象データを K 個のシェアに分割し分割保管を行い、復元する場合は K 個のうち N 個の

---

[13] "ゲノムとプライバシー"IEICE Fundamentals Review Vol.7 No.4 p348

シェアを用いて復元する方式である。最大で（N-1）個のシェアが漏洩した場合でもそれだけでは保護対象データの中身が分からないほか、最大で（N-1）個のシェアが消失した場合でも復元できるため、漏洩時の被害を最小化し、損失時の復旧にも適した手法である。

4.2.4 個人情報漏洩の影響

個人情報流出の被害規模について試算を行った。JNSA 情報セキュリティインシデントに関する調査報告書別紙[14]によると、個人情報流出の一人当たりの損害賠償額の試算式は以下の通りである。

損害賠償額 = 漏洩個人情報価値×社会的責任度[2,1]×事後対応評価[2,1]

ここで漏洩個人情報価値とは、以下の式で表される。

基礎情報価値[500]×機微情報度[Max($10^{max(x)-1}+5^{max(y)-1}$)]×本人特定容易度[6,3,1]

機微情報度については病歴等と同じランク(経済的損失レベル x=1, 精神的苦痛レベル y=2)とした。本人特定容易度は、コストを書ければ個人が特定できる情報[3]とした。社会的責任度は判定基準より、一般より高い業種（医療）[2]と判定した。最終的な試算額は、事後対応評価が適切な場合 33,000 円、事後対応が不適切な場合 66,000 円となった。例えば情報集約拠点であるがんゲノム情報管理センター等のゲノム情報が大量に集まる拠点に対する攻撃で漏洩した場合には被害規模がより大きくなり、1 万人規模の被害となると数億円の被害賠償額となる。

また、刑事罰については、個人情報の保護に関する法律[15]によると、個人情報取扱事業者が、個人情報保護法の義務規定に違反し、不適切な個人情報の取扱いを行っている場合には、国は事業者に対して、必要に応じて報告を求めたり立入検査を行ったりすることができる。また、実態に応じて、指導・助言、勧告・命令を行うことができる。国からの命令に個人情報取扱事業者が従わなかった場合には、罰則の対象になり、6 か月以下の懲役または 30 万円以下の罰金が科せられる。虚偽の報告等をした場合 30 万円以下の罰金、従業員等が不正な利益を図る目的で個人情報データベース等を提供、又は、盗用した場合、1 年以下の懲役又は 50 万円以下の罰金が科せられる。

以上の直接的な損害以外にも、社会的信用の低下、株価変動、業務停止期間中の遺失利益、復旧コスト、対策費用、対応による業務効率の低下などの間接的な損害が生じることが予測される。

例えば適切なバックアップを怠っていた場合、災害により蓄積していたデータが損失する恐れがある。その場合の再解析費用として一人数十万円かかるとすると、1 万人規模のデータ損失で数十億円の復旧コストが予想される。

---

[14] https://www.jnsa.org/result/incident/

[15] https://www.ppc.go.jp/

4.3　生体認証分野におけるユースケース

4.3.1　想定する運用場面

空港内監視カメラ映像を警備会社と共有し、空港内の警備に利用するために、利用する個人データや重要情報のデータ通信に対して量子暗号を適用することを検討する。

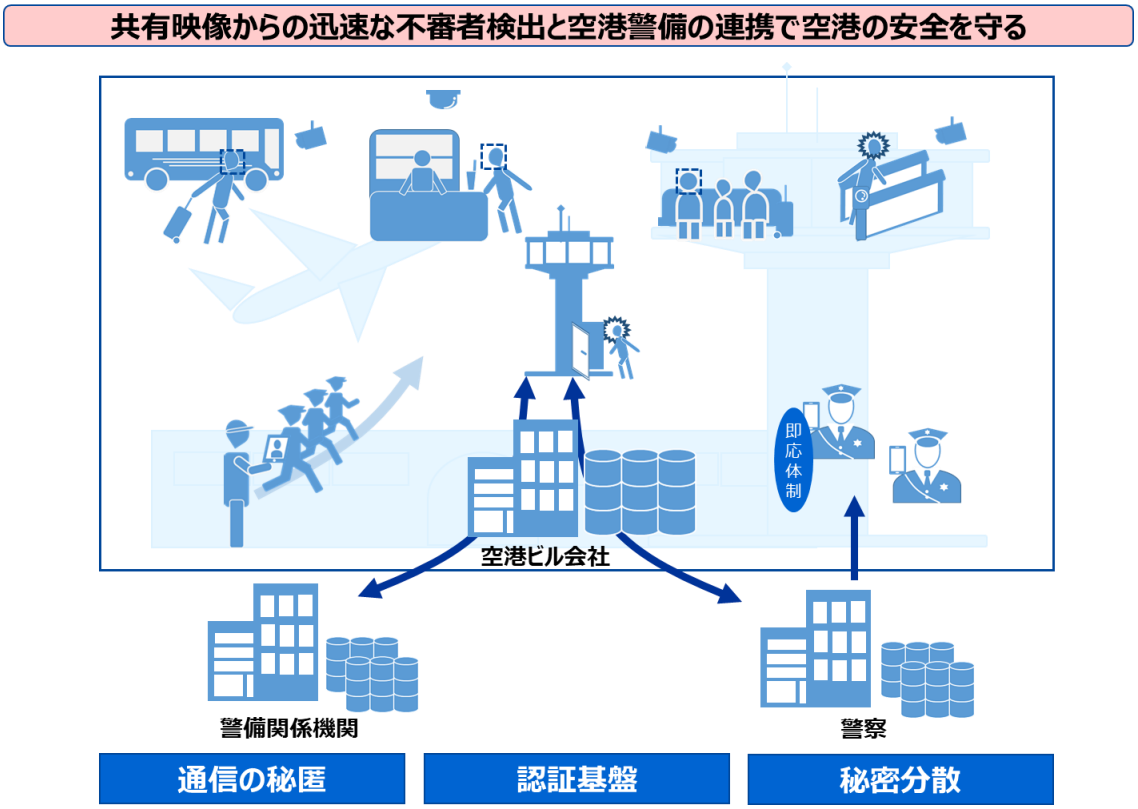


図　18：空港警備における量子暗号の運用構想

4.3.2　必要性

空港では多数の監視カメラが設置され、顔認証を利用したサービスの提供も進んでいる。これらの映像を空港内警備に活用するためには、個人情報の取り扱い規定とともに、安全な通信での個人情報の保護が必要である。

①　危殆化のリスク

個人の生体情報を含めた情報を一元管理して取り扱うため、超長期的に極めて高い強度の秘匿が必要となる。現代暗号では量子コンピュータの開発や計算能力の向上による危殆化のリスクが伴うため、秘匿の強度として不十分である。

②　システム連携におけるデータ漏洩リスク

システムを攻撃する立場からは、システムのうち最も脆弱なところを攻撃する。空港と警備会社のシステム連携により、共用データが通信時に漏洩した場合、連携した機関間での責任問題が生じる[16]。

③ サイバー攻撃のリスク

民間側を狙った攻撃で警備システムに侵入された場合、機密情報漏洩の可能性があり、リスクの回避が必要となる。

4.3.3 有効性

前述の顔認証を利用したシステム間の連携課題に対して、量子暗号適用の有効性を以下に記す。

① 量子暗号は危殆化のリスクが無い
② 鍵の盗聴は確実に検知・暗号文を盗難されても解読不能である
③ 量子暗号で外部ネットワークとの連接点である通信を保護し、システムを堅牢化することで、サイバー攻撃による機密情報漏洩のリスクを下げ高可用性を実現することができる

4.3.4 システム構成案と適用による効果

量子暗号を適用した際のシステム構成を検討し、適用による効果を整理する。

空港内監視カメラ映像を共有して不審者を検知した際、手配に要する顔認証などの生体情報や捜査上の重要情報などを一時的に共用する場合の顔認証基盤を共有した通信に量子暗号を適用する場合について、システム構成を検討する。

航空会社が運用する業務システムのネットワークと空港に設置される共有顔認証基盤へ量子暗号を適用した場合を想定する。航空会社の業務システムのネットワークとそれに対抗するデータベースが置かれたネットワークそれぞれに QKD モジュール、鍵管理・供給サーバーおよび暗号化装置を設置する。空港構内間の接続（短距離）を想定し、QKD モジュール間は直接光回線で結び構築する。業務システムとデータベース間の通信へ量子暗号を適用したイメージを図 19 に示す。

---

[16] （NPO 日本ネットワークセキュリティ協会「2017 年情報セキュリティインシデントに関する調査報告書」）によると、個人情報漏洩インシデントの一件当たり平均損害賠償額 5 億 4,850 万円

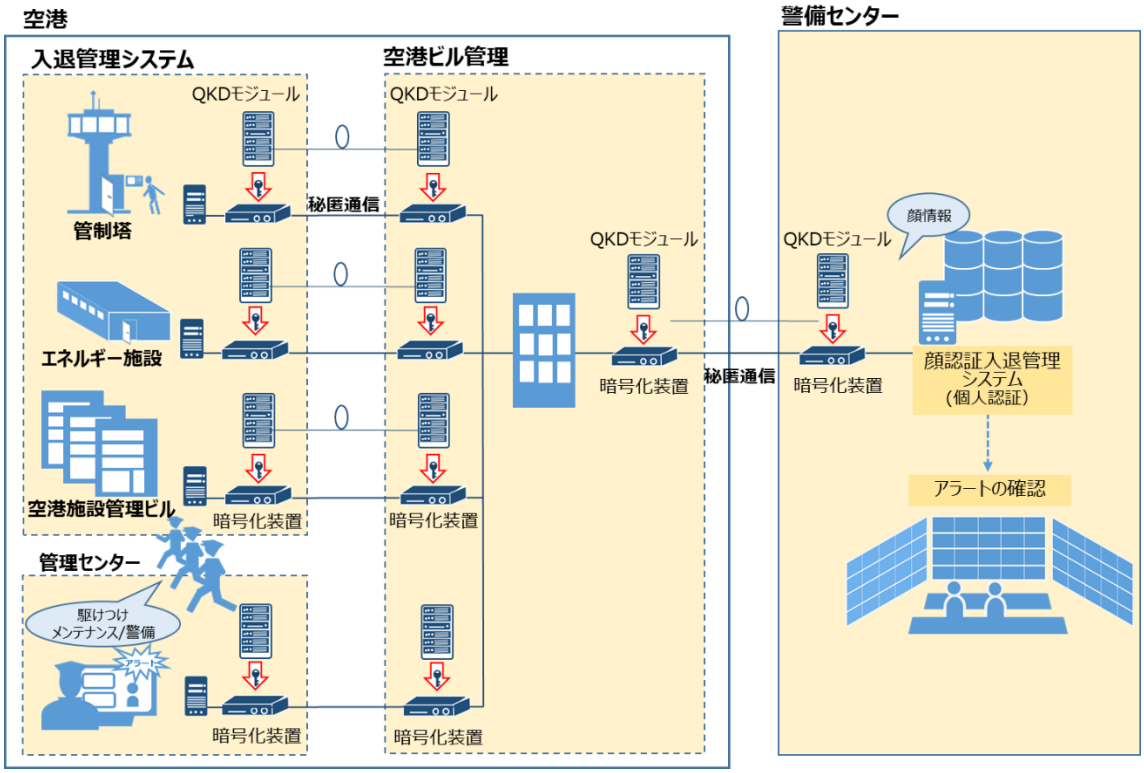


図 19：入退管理システムと顔認証システムの通信イメージ

適用の効果としては、長期的な安全性の確保が可能となること、そして、顔情報などの生体情報をシステム間で安全に共有できるようになり、サービスを提供することが可能となり、それらの統合的なサービスを堅牢化することで、事業を安定して継続することが挙げられる。

5　量子暗号サービスの運用

本章では、量子暗号サービスを運用するにあたって、どのようなプレーヤーが関わるのか、安心して量子暗号サービスを利用するためにどのように情報セキュリティを維持すべきかについて紹介する。また、標準化活動についても紹介する。

5.1　量子暗号ビジネスのエコシステム

量子暗号ビジネスにおけるプレーヤーについて、3.2 節で説明した QKDN アーキテクチャに沿って説明する。図 20 に示すように、量子レイヤに深く関わるプレーヤーとしては、QKD モジュールを作製し保守を行う QKD モジュールベンダ、QKD リンクの敷設・保守を行う光回線プロバイダ等がいる。そして暗号鍵の提供・QKDN の総合管理、ノード管理を担うのが QKDN プロバイダである。そして受け取った鍵を取り込み利用するためのアプリケーションプロバイダ及び利用者がサービスレイヤに属する。また、第三者機関として国、推奨機関、標準化団体、QKDN の監査会社、QKD モジュールの認証会社も運用上重要な役割を果たす。

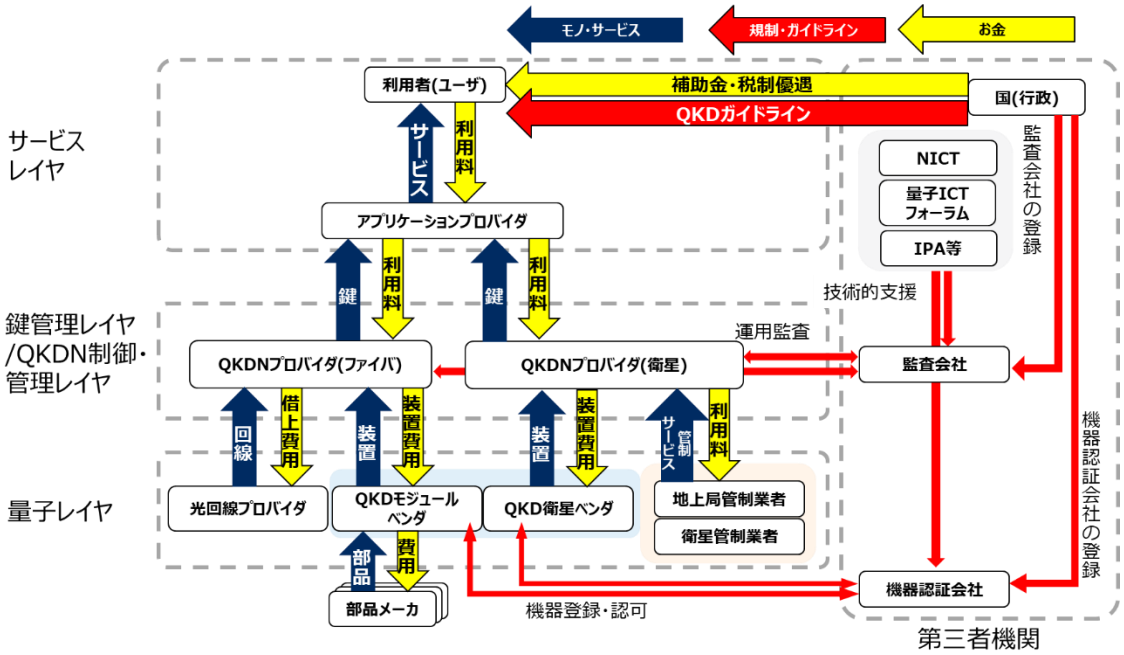


図 20：量子暗号ビジネスのエコシステム

以上をカテゴリごとにまとめたものを表 6 に示す。

カテゴリ	プレーヤー	説明
量子レイヤ	光回線プロバイダ	QKD リンクの敷設・保守
	QKD モジュールベンダ	QKD モジュールの作製と保守
	QKD 衛星ベンダ	QKD 衛星モジュールの作製・保守
	地上局管制業者	QKD 衛星に関する運用・保守
	衛星管制業者	QKD 衛星に関する運用・保守
鍵管理レイヤ/QKDN 制御管理レイヤ	QKDN プロバイダ	暗号鍵の提供・QKDN の総合管理、ノード管理
サービスレイヤ	利用者	量子暗号サービスの利用
	アプリケーションプロバイダ	サービスを提供
第三者機関	国	法整備
	推奨機関	ガイドライン策定、量子 ICT フォーラムなど
	標準化団体	標準化の制定
	監査会社	サービスやセキュリティに関する監査など
	機器認証会社	装置の安全性に関する認証など

表 6：エコシステムのプレーヤーとその役割一覧

また、上記プレーヤーが今後どのように発展していくか予想したものを表 7 に示す。

		2020	2021	2022	2023	2024	2025	2026	2027
官公庁・中央省庁 量子 ICT フォーラム		安全運用ガイドライン策定、標準化			サービス提供ガイドライン・法整備		教育体系、国家資格取得の整備、就職先の確保		
研究機関		基礎研究・実装安全性研究		性能向上手法の研究(長距離化・高速化)			5G（6G）との融合		
QKD モジュールベンダ		製品化		量産化・機能向上			次世代機の開発・製品化		
QKD サービス事業者		サービス検討		サービス用のシステム構築			サービス提供・エリア拡充		
QKD ユーザー	官公庁・中央省庁	試行運用		システム構築(専用システム)			システム運用		
	民間	市場動向調査		サービス先行利用			サービス利用		

※光回線プロバイダ・QKDN 事業者・アプリケーションプロバイダ等を想定

表 7：量子暗号ビジネスの中長期計画（案）

5.2 量子暗号サービスにおけるセキュリティ対策指針

量子暗号サービスを安心して便利に利用するためには、ネットワーク全体の可用性、性能・拡張性、運用・保守性、移行性、セキュリティ、環境・エコロジーなど（いわゆる非機能要件[17]）を考慮した設計が必要となる。また、運用していく中で、これらの要素を維持していかなければならない。

QKD は、通信路に対するいかなる攻撃も検知することが出来るため、QKD で共有した鍵を用いてデータの暗号化を行う量子暗号は、情報理論的な安全性を得ることのできる唯一の手段である。しかし、量子力学が保証するのは、あくまでも量子力学的な性質を保持している通信路の間のみであり、トラステッドノード内で量子状態からひとたび暗号鍵として 0と 1 のデジタルデータとして保存された途端、従来の機密データとまったく同じように、情報漏洩、かいざん、不正アクセス等の脅威にさらされることを忘れてはならない。また、『暗号鍵』というツールである以上、以下の要件を満たす必要がある。

1. **権限のある利用者（アプリケーション）へ渡されること**

   これは情報セキュリティの 7 要素のうちの機密性(confidentiality)に関わる。正当な利用者以外が鍵を入手すると、その鍵を用いて暗号化されたデータの内容が漏洩してしまうためである。

   脅威：鍵の漏洩、鍵リレーの経路情報の改ざん

   対策：アクセス制限やパーミッション設定

2. **暗号化と復号へ使われること**

   これは情報セキュリティの 7 要素のうちの完全性(integrity)に関わる。データの送受信者の持つ鍵が一致していなければ、正しく暗号化・復号が出来ないためである。

   脅威：鍵の改ざん、鍵の削除

   対策：ログを残す

3. **利用者（アプリケーション）からの要求があるまで保管されること**

   これは情報セキュリティの 7 要素のうちの可用性(availability)に関わる。KM は利用者からの要求に応じて鍵を供給する。言い換えると、要求があるまで共有した鍵を保管する必要がある。

   脅威：停電・災害やサイバー攻撃によるシステムダウン

   対策：冗長化、電源対策、災害復旧計画

情報セキュリティの 7 要素の他の 4 要素（真正性：正当な利用者であること、否認防止：行為をなかったことに出来ないこと、責任追跡性：誰の行為か追跡可能なこと、信頼性：致命的なバグがないこと）についても、当然トラステッドノード構築において考慮すべき要素ではあるが、上記の 3 つが特に鍵の特有のものであると言える。

[17] https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html

本節では、トラステッドノードの安全性確保のための、情報セキュリティマネジメントシステムの構築・運用の流れ、セキュリティ要件、セキュリティ対策の指針ついて紹介し、量子暗号におけるリスク分析についても詳しく紹介する。

5.2.1 情報セキュリティマネジメントシステムの構築・運用の流れ

情報セキュリティの確保に組織的・体系的に取り組むことを情報セキュリティマネジメントといい[18]、情報セキュリティマネジメントシステムを構築・運用し、継続的に改善するための規格として ISO/IEC27001[19]がある。

情報セキュリティマネジメントを実施するにあたっては、以下のような情報セキュリティマネジメントの実施サイクル(PDCA サイクル)によって、実態に沿った内容になっているかを常にチェックし、絶えず見直し、改善を図る必要がある。

1. 計画(Plan)：組織や企業の状況に合った情報セキュリティ対策の方針を定めた情報セキュリティポリシーを策定する。そして情報資産の洗い出しと漏洩リスクの分析を行い、リスクに対する対策方法とその手順を策定し、その手順書として明文化する。
2. 導入・運用(Do)： 1 で策定した方針と手順書を全社員・全職員に周知し、必要に応じて、教育を行う。 関係者が情報セキュリティポリシーに則って行動することで、目的とする情報セキュリティレベルの維持を目指す。
3. 点検・評価(Check)：導入後の現場の状況や新たな脅威、新しい法律の施行などの社会的な状況などを踏まえて、定期的に情報セキュリティポリシー自体を評価する。また、遵守されているかどうかの内部監査・第三者機関による審査を行う。
4. 見直し・改善(Act)：点検・評価の内容を参考にして、情報セキュリティポリシーと手順書の見直し・改善を行う。

5.2.2 情報セキュリティ要件

では具体的に安全性を確保するためにはどのような要件を満たすべきか、どのように対策を考えれば良いのかについて考える。セキュリティ要件としては NIST SP800-171[20]で細かく示されているので参考に出来る。

- アクセス制御 （アクセス許可の制限、リモートアクセスセッションの監視・制御、アクセス保護のための暗号利用等の要件）

---

[18] https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html

[19] 日本語化規格 JIS Q27001

[20] 日本語版：https://www.ipa.go.jp/security/publications/nist/index.html

- 意識向上と訓練　（教育、周知訓練に関する要件）
- 監査と責任追跡性　（監査自称のレビュー・アラート・報告書作成等の要件）
- 構成管理　（組織のシステムの確立と維持等に関する要件）
- 識別と認証　（利用者やデバイスを識別すること、識別コードの利用制限等についての要件）
- インシデント対応　（防御・検知・分析・対応・普及の対応の追跡、能力テストに関する要件）
- メンテナンス　（システムメンテナンスの実施、メンテナンス要員の監視、メンテナンス時の攻撃対策実施等の要件）
- メディア保護（メディアの保護・アクセス制限、廃棄時に破壊等の要件）
- 人的セキュリティ（アクセス前の個人審査、離職等の影響調査等の要件）
- 物理的保護（物理アクセスの制限、訪問者の行動監視、物理的アクセスの制御・監視・記録等の要件）
- リスクアセスメント（リスクアセスメントの実施、脆弱性のスキャン等の要件）
- セキュリティアセスメント（管理策が有効化どうか定期的確認、管理策の監視等の要件）
- システムと通信の保護（通信の監視・制御・保護、FIPS 認証暗号使用等の要件）
- システムと情報の完全性（システムの定期スキャン、外部情報のリアルタイムスキャン等の要件）

5.2.3　情報セキュリティ対策の指針

NIST のサイバーセキュリティフレームワーク [20] によると、情報セキュリティリスク対策は大きく分けて、以下の 5 つ分類される。

1. 識別（情報セキュリティリスクの管理に必要な理解を深める）
2. 防御（重要サービスの提供を確実にするための保護対策の検討・実施）、
3. 検知（インシデント発生を識別するための対策検討・実施）
4. 対応（検知したインシデントの対処法の検討・実施）
5. 復旧（レジリエンスを実現するための計画の策定・維持と、インシデントで阻害された機能やサービスを元に戻す対策の検討・実施）

5.2.4　リスク分析

次に、計画(Plan)で欠かせないリスク分析について QKDN アーキテクチャに沿って説明する。

まず初めに一般的なリスク分析の流れを説明する。最初に①情報資産とその重要度を定義し、②脅威源と想定される脅威イベントを洗い出して、③脅威イベントが実行される可能性（脅威レベル）を検証し、④各脅威に対する対策状況（脆弱性）の評価を行い、⑤脅威に対するリスク値を算定する。本節では、量子暗号の適用におけるリスク分析を行う。脅威に対する対策状況やリスク値は個々の運用形態に依存するため、ここでは、QKD システム・QKD ネットワーク一般における①－③までの脅威分析と、と、医療分野を例にしてサービスレイヤまでを含めた④－⑤までの脅威分析に分かれている。

5.2.4.1　情報資産の洗い出し

サービスネットワークにおいては暗号化すべきデータ、QKD ネットワークにおいては暗号鍵と鍵リレーの経路情報（QKD ネットワークを管理するための情報）、を守るべき情報として定義する。

5.2.4.2　脅威源の洗い出し

そして脅威源の洗い出しを行う。NIST の Special Publication 800-30 “Guide for Conducting Risk Assessments”[21]によると、脅威源は下記４つの分類に分けられる。

(i)　サイバー攻撃、物理攻撃を行う悪意を持った攻撃者・攻撃組織
- 個人（外部の人間、内通者）
- グループ、組織、国家

(ii)　構造上の欠陥や不具合の発生源
- IT 設備（ストレージ、プロセス処理、通信、ディスプレイ、センサ、コントローラ）
- 環境制御（温度・湿度制御、電源供給）
- ソフトウェア（OS、ネットワーク、一般アプリケーション、専用アプリケーション）

(iii)　人的ミス、自然災害、人災、制御不能な事象
- 人的ミスの発生源（一般ユーザー、特権ユーザー）
- 自然災害、人災（火災、洪水、津波、嵐、ハリケーン、地震、爆撃、オーバーラン）
- 特別な自然災害

以上を参考として、量子暗号システムにおいて特定した脅威源を図 21 に示す。

[21] https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

(i) 悪意を持った攻撃者・攻撃組織
(ii) 構造上の欠陥や不具合の発生源
(iii) 人的ミス、自然災害、人災、制御不能な現象

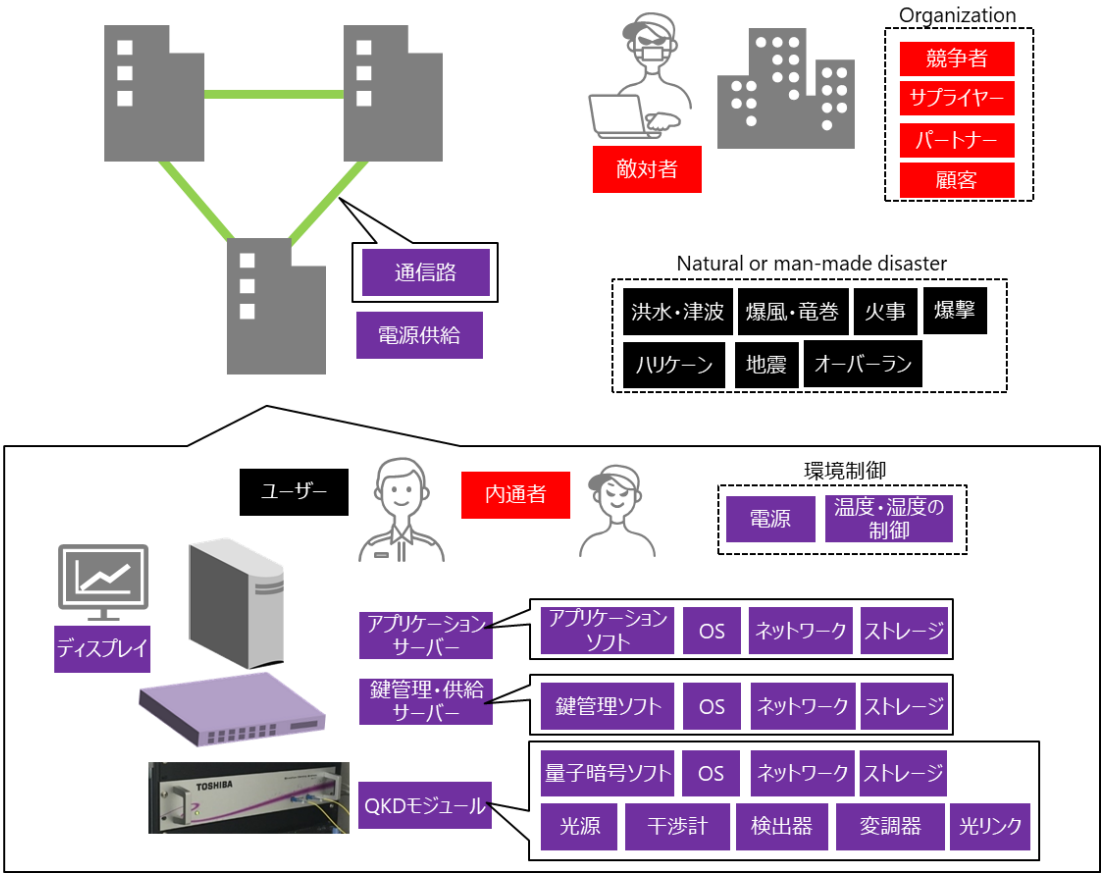


図 21：量子暗号システムにおける脅威源

5.2.4.3 脅威イベントと対策例

次に想定される脅威イベントについて検討する。ITU-T の M.3016.0[22]によると、脅威の種類としては下記 3 つの分類に分けることができる。基本的には、それぞれ前節で述べた脅威源(i)から(iii)に対応しているが、攻撃者は管理上の脅威（弱点）を利用した攻撃を仕掛けることもできる。

(i) 意図的な脅威：悪意を持った攻撃者に起因する脅威

- 情報漏洩
- なりすまし
- 不正アクセス
- 情報破壊・消去

[22] https://www.itu.int/rec/T-REC-M.3016.0

- 否認
- 偽造
- Dos 攻撃

(ii) 管理上の脅威：セキュリティ管理不足に起因する脅威

(iii) 偶発的な脅威：悪意の無い脅威源に起因する脅威

さらに、IPA の制御システムのセキュリティリスク分析ガイド第 2 版[23]記載の脅威イベントも参考として作成した量子暗号システムで想定される脅威一覧を表 8 に示す。

分類	脅威の種類	対策例
情報漏洩	通信路の盗聴	通信路暗号化、専用線
	装置からの情報漏洩	入退室管理、施錠管理
	装置の盗難・廃棄時の盗難	耐タンパ、難読化、セキュア消去
	サイドチャネル攻撃	脆弱性対策
	バックドア攻撃	組み込みデバイスの精査、耐タンパ
なりすまし	なりすまし	認証
不正アクセス	物理的侵入	入退室管理、施錠管理
	装置・サーバーへの不正アクセス	脆弱性対策、認証
	不正操作	操作者認証
	不正媒体の接続	デバイス接続制限
	マルウェア感染	アンチウイルス
	アプリからの不正アクセス	アクセス制御、認証
情報改竄・消去	鍵情報、鍵管理情報の改ざん・消去	アクセス制御、権限管理、データ暗号化
否認	否認	デジタル署名
偽造	偽造	データ署名
DoS 攻撃	サーバーへの高負荷攻撃	冗長化
	通信路遮断	冗長化
	通信輻輳・通信妨害（無線の場合）	冗長化
災害	通信路障害	冗長化
	インフラ障害	無停電電源装置
人的エラー	過失操作	フィルタリング、確認画面
管理上の脅威	不具合・故障・バグ	定期メンテナンス

表 8：量子暗号システムで想定される脅威と対策例一覧

[23] https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

脅威イベントを QKD ネットワークへとマッピングした結果を図 22 に示す。ここでは責任分界点をサービスレイヤと鍵管理レイヤの間に設定し、鍵管理レイヤと量子レイヤ及び QKD ネットワーク管理・制御レイヤのみ脅威を示した。

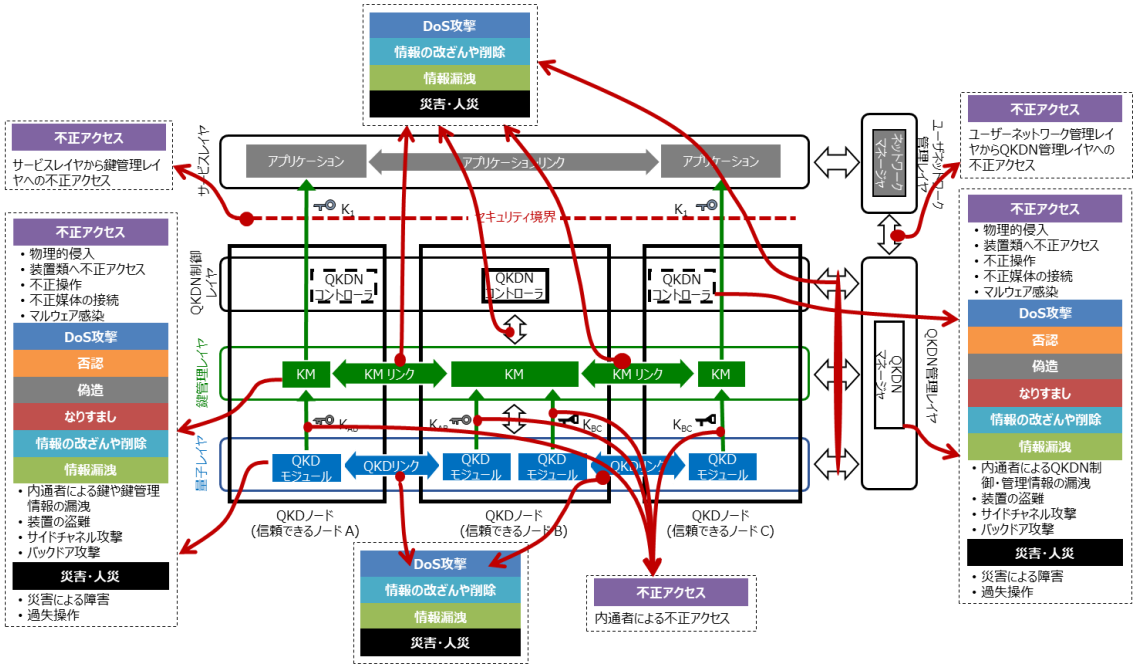


図 22：QKD ネットワークにおける脅威イベント。情報漏洩、なりすまし、不正アクセス、情報改竄・消去、否認、偽造、Dos 攻撃、その他脅威（人的エラー、災害等）の 8 分類とした。

5.2.4.4　脅威レベルの分析

図 22 の構成を元に、表 8 に示される脅威の発生可能性を 3 段階（最も可能性の高いものが 3）で評価した結果を表 9 に示す。

脅威＼資産	拠点内 NW (アプリ－鍵管理間)	拠点内 NW (鍵管理装置間)	鍵管理・供給サーバー	QKD モジュール	QKDN 制御・管理装置	QKD リンク	KM リンク	フィールド NW (QKDN 制御・管理)
機器			○	○	○			
NW 系資産	○	○				○	○	○
通信路の盗聴	2	2				2	2	2
機器からの情報漏洩			2	2	2			
装置の盗難			2	2	2			
サイドチャネル攻撃	2	2	2	2	2			
バックドア攻撃	2	2	2	2	2			
なりすまし	2	2	2	2	2			
物理的侵入	2	2	2	2	2			
不正アクセス	2	2	2	2	2			
不正操作	2	2	2	2	2			
不正媒体の接続	2	2	2	2	2			
マルウェア感染	1	1	2	1	2			
情報改竄・消去	2	2	2	2	2			
否認	2	2	2	2	2			
偽造	2	2	2	2	2			
高負荷攻撃	3	3	1	1	1			
通信路遮断	2	2				3	3	3
通信輻輳・通信妨害	2	2				2	2	2
通信路障害	2	2				2	2	2
インフラ障害	2	2	2	2	2			
過失操作	2	2	2	2	2	2	2	2
不具合・故障・バグ	2	2	2	2	2	2	2	2

表 9：脅威イベントの発生頻度の評価（NW：Network の略）

5.2.4.5　サービスレイヤを含めた脅威分析

実際に量子暗号サービスを提供・利用する際には、サービスレイヤ側でも脅威分析が必要となる。ここでは参考として、医療分野への量子暗号応用を考えた場合に考慮すべき脅威や対策について紹介する。

「医療情報システムの安全管理に関するガイドライン 第 5 版 - 厚生労働省」[24]を参照すると、医療情報システム、及び医療情報システムに格納されている電子データに対する脅威として、以下が挙げられている。

1. 医療情報システムに対する脅威
   (ア) サイバー攻撃による IT 障害
      ① 不正侵入
      ② 改ざん
      ③ 不正コマンド実行
      ④ 情報かく乱
      ⑤ ウイルス攻撃
      ⑥ サービス不能（DoS：Denial of Service）攻撃
      ⑦ 情報漏えい 等
   (イ) 非意図的要因による IT 障害
      ① システムの仕様やプログラム上の欠陥（バグ）
      ② 操作ミス
      ③ 故障
      ④ 情報漏えい 等
   (ウ) 災害による IT 障害
      ① 地震、水害、落雷、火災等の災害による電力供給の途絶
      ② 地震、水害、落雷、火災等の災害による通信の途絶
      ③ 地震、水害、落雷、火災等の災害によるコンピュータ施設の損壊等
      ④ 地震、水害、落雷、火災等の災害による重要インフラ事業者等における IT の 機能不全
2. 医療情報システムに格納されている電子データに対する脅威
   (ア) 権限のない者による不正アクセス、改ざん、き損、滅失、漏えい
   (イ) 権限のある者による不当な目的でのアクセス、改ざん、き損、滅失、漏えい
   (ウ) コンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん、き損、 滅失、漏えい

[24] https://www.mhlw.go.jp/stf/shingi2/0000166275.html

これらに対する具体的な対策についても上記ガイドラインに示されているため、基本的にはガイドラインに従った対策を行うこととなる。量子暗号に関する部分については、前節を参考として具体的な対策を行う必要がある。

以上の脅威を、4.2 節の医療分野におけるユースケースで想定したがんクリニカルシーケンス向け量子暗号システムの構成においてマッピングしたものが図 23 と図 24 である。量子暗号システムはサービスレイヤ、鍵管理レイヤと量子レイヤに分けることができ、図 23 ではサービスレイヤに対する脅威と対策候補、図 24 では量子レイヤと鍵管理レイヤに対する脅威と対策候補をマッピングした。図中では、システムで扱う機密情報を青枠で、脅威を赤枠で、脅威に対応する対策候補を緑枠で表している。

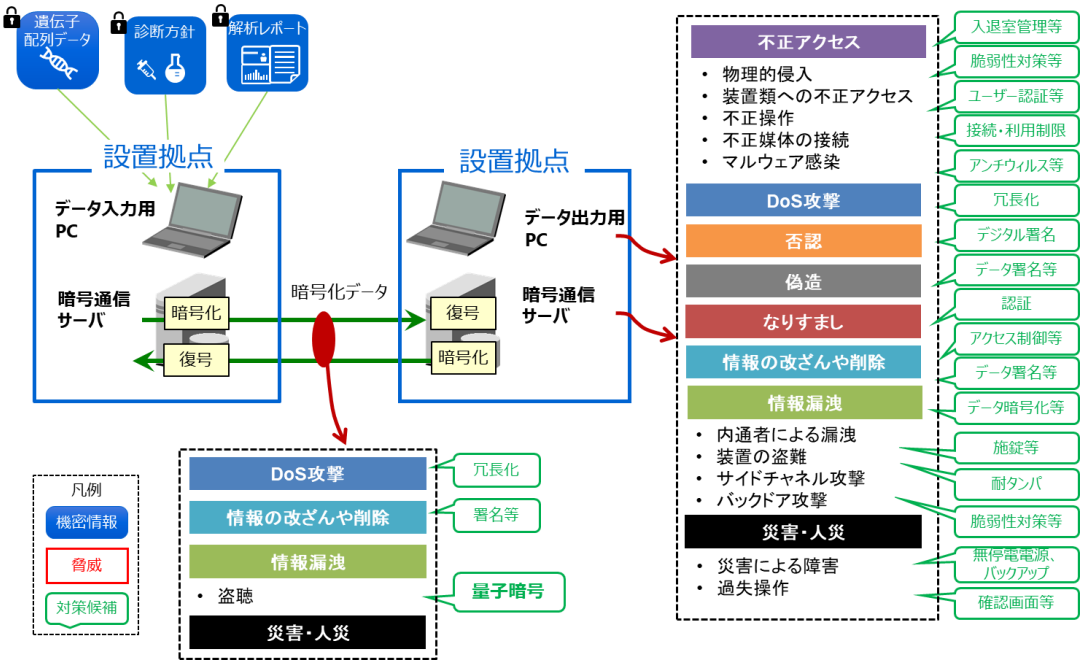


図 23：サービスレイヤにおける脅威とその対策例

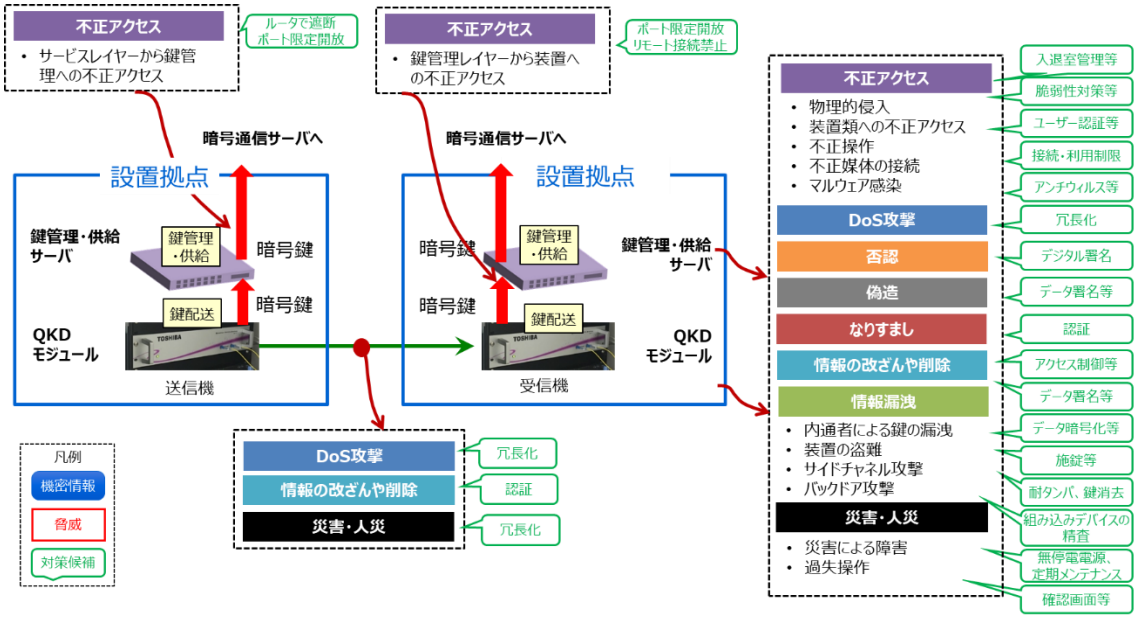


図 24：量子レイヤと鍵管理レイヤにおける脅威とその対策例

5.3 標準化活動

標準化は、製品の互換性・インターフェースの整合性・品質の確保、生産効率の向上や正確な情報の伝達・相互理解の促進などの多くのメリットをもたらす。量子暗号に関しては、ETSI（European Telecommunications Standards Institute）、ITU-T(International Telecommunication Union Telecommunication Standardization Sector)、ISO/IEC JTC1（International Organization for Standardization/ International Electrotechnical Commission, Joint Technical Committee 1）等の多数の標準化団体において、日本、中国、韓国、イギリス、スイス、ドイツ、スペイン、カナダ、米国などによる標準化推進の機運が高まっている（図 25）。特に ITU-T では日本が主導権をとっている状況である。また、日本の量子技術の①情報発信、②標準化・実用化の支援、③交流・連携の場の提供を目的として、産官学が連携し、2019 年 11 月に一般社団法人量子 ICT フォーラムが設立された。

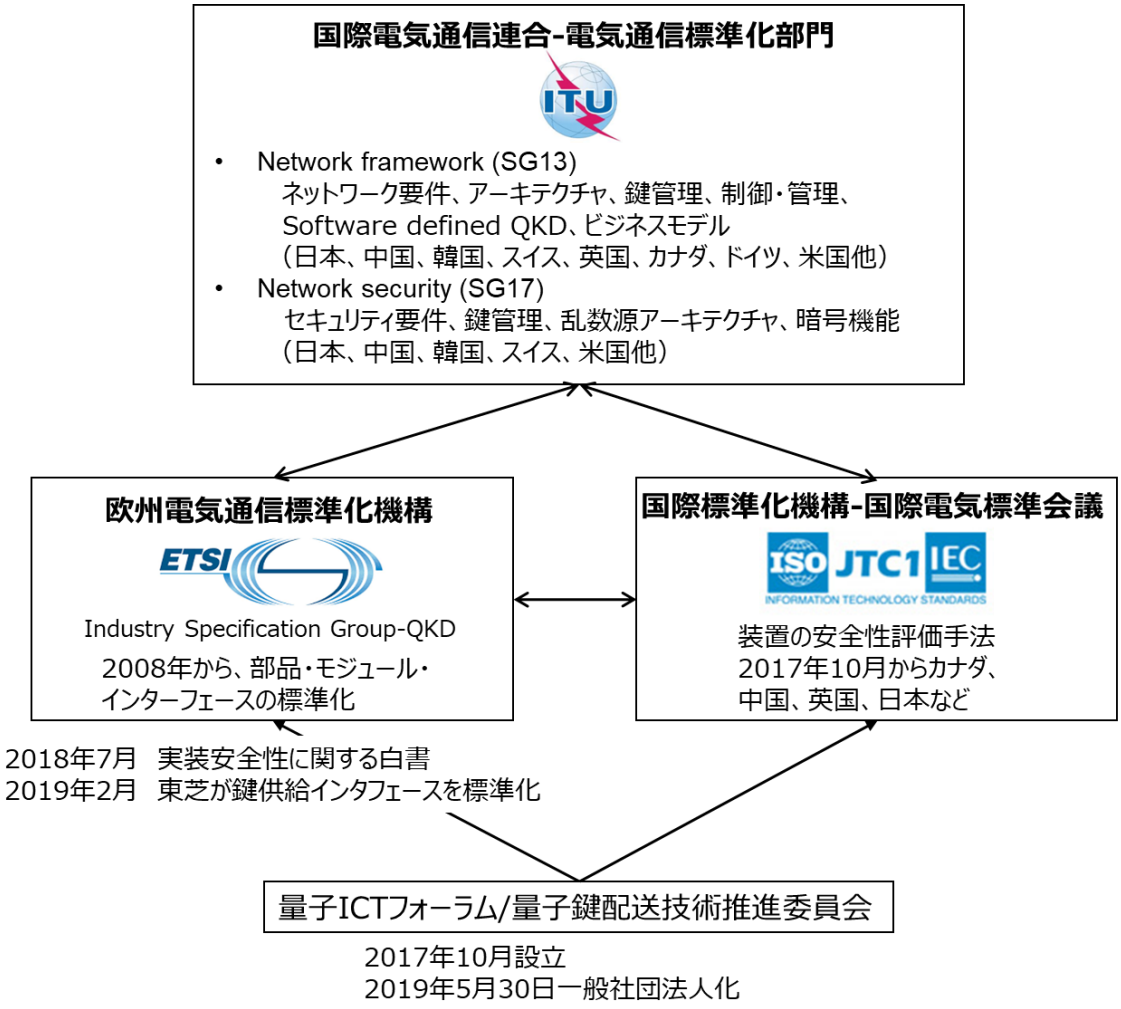


図 25：量子暗号に関係する代表的な標準化活動一覧

代表的な標準化活動を QKDN アーキテクチャにマッピングしたものを図 26 に示す。

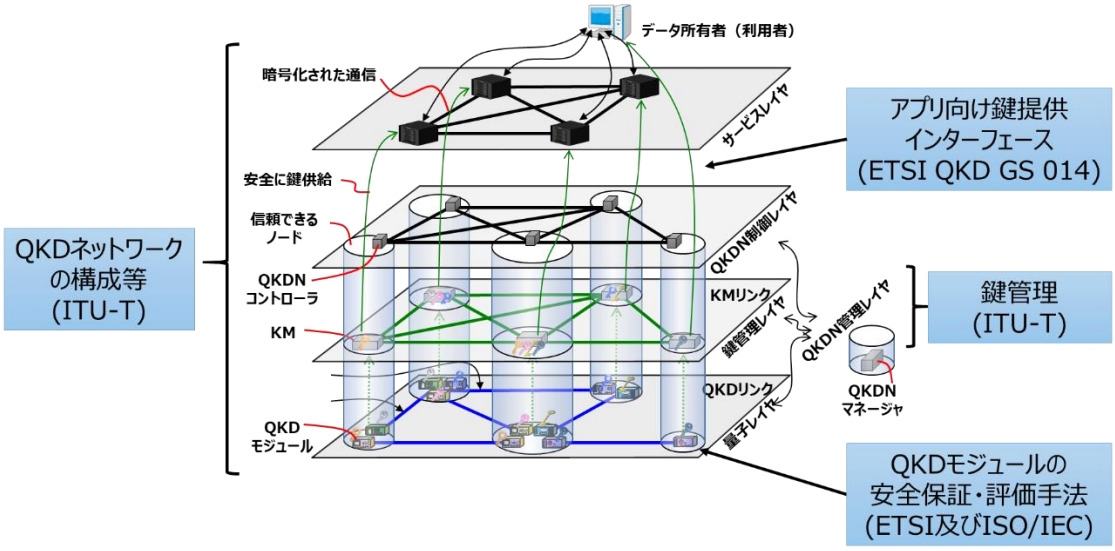


図 26：QKD ネットワークに関わる主な標準化活動の概略図

6　量子暗号技術の現状と今後の課題

6.1　国内外の開発動向

日本は、実用化に向け高性能装置を開発し、実証試験を継続している。2010 年には NICT 主導でテストベッド(東京 QKD ネットワーク)を構築した[25]。ImPACT 量子セキュアネットワークプロジェクトにて、都市圏 QKD ネットワークを実証している。2018 年度からは、内閣府の戦略的イノベーション創造プログラム(SIP)「光・量子を活用した Society5.0　実現化技術」にて、量子暗号と秘密分散を統合した社会実装に取り組んでいる。SIP の成果として、NICT と NEC は顔認証データの伝送・保管への量子暗号適用の実証[26]、東芝と東北大学東北メディカル・メガバンク機構は全ゲノムデータ伝送への量子暗号適用の実証[27]に成功している。

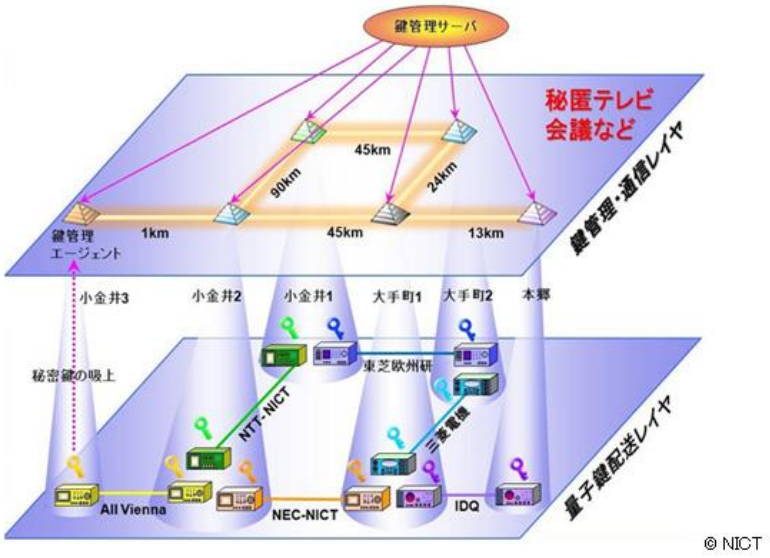


図 27：東京 QKD ネットワーク

鍵の配信速度が他国と比較して 1 桁以上高く、抜群の性能を誇る装置を開発しており（図 28）、今後、量子暗号業界の発展を日本が牽引していくことが期待される。

[25] https://www.nict.go.jp/press/2010/10/14-1.html
[26] https://jpn.nec.com/press/201910/20191029_02.html
[27] https://www.toshiba.co.jp/rdc/detail/2001_01.htm

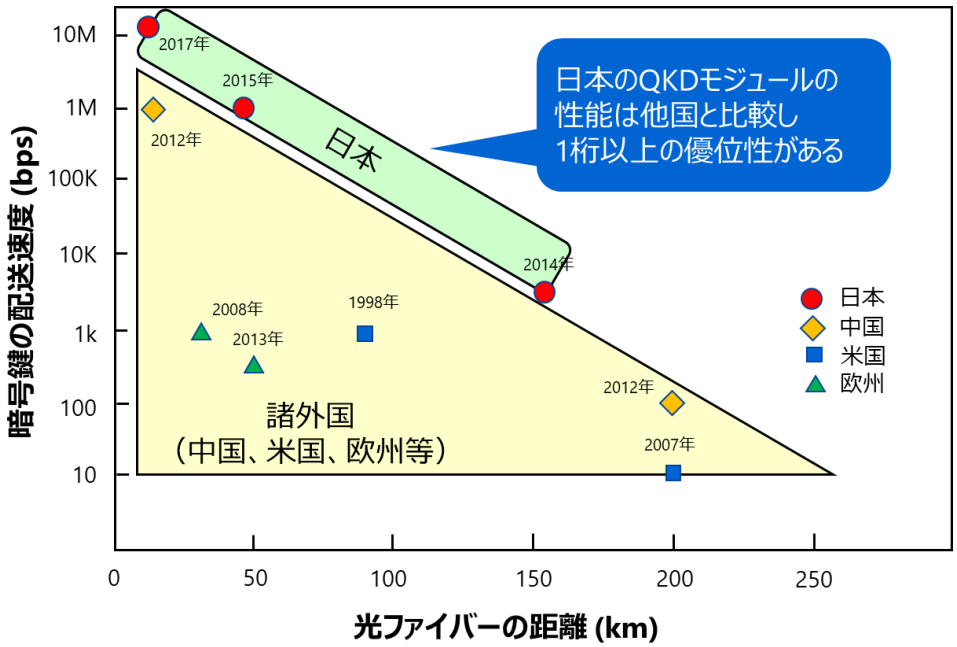


図 28：暗号鍵の配送速度の比較。横軸は送受信機の間の光損失を標準的なファイバーの距離に直したもの。

米国ではスタートアップ中心に量子暗号を活用した事業を展開している。2018 年には Quantum Xchange が同国初の量子暗号サービスを発表した。これは Boston-Washington DC 間で主に Wall Street の金融向け市場が狙いで、New York-New Jersey 間のダークファイバーを初期サービスに活用している。

欧州では大手通信キャリアによる実用化に向けた動きが近年加速している。英 BT が同国初の量子暗号網を Cambridge-Ipswich 間に構築した（東芝、IDQ、ADVA 等が参画）[28]。テレフォニカ、ファーウェイ、マドリード工科大学が既存商用光通信網での運用実証試験を開始した例や、ドイツテレコムの実証通信網に SK Telecom/IDQ がシステムを提供し、2019 年商用網への拡大を目指すとの報道もある。

28

https://docbox.etsi.org/Workshop/2017/201709_ETSI_IQC_QUANTUMSAFE/EXECUTIVE_TRACK/BT_BEESON_KEYNOTE.pdf

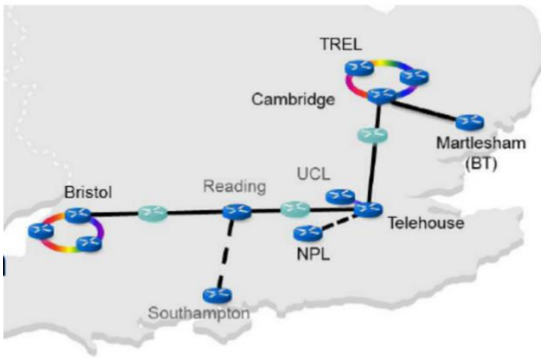


図 29：英国の量子暗号ネットワーク

中国は近年地上・宇宙両面で存在感を増している。世界最大規模の量子暗号ネットワーク[29]を構築し、国営企業が利用する例や、北京－上海間の政府向けバックボーンや上海－杭州間の商用バックボーン構築などを進めている。また、2016 年量子通信衛星を打ち上げ、2017 年世界初の衛星地上間での量子鍵配送実験に成功した(距離 1200km、鍵配信速度 1kbps)。

図 30：中国の量子暗号ネットワーク

韓国では、実用化を視野に国主導で通信キャリアが実証試験を行っている。SK Telecom が、2018 年にスイスの IDQ へ 65 百万ドルを投資し自社 R&D 部門と統合、量子暗号システムの研究開発を推進している。

29 https://docbox.etsi.org/Workshop/2015/201510_IQCWORKSHOP/UofChongqing_HongXiang.pdf

6.2 研究の今後の課題

QKD の研究の方向性としては主に以下の 3 点が挙げられる。

- コスト削減や安定性向上
- 鍵の生成速度の向上・通信距離の延伸
- ネットワーク化
- トラステッドノードの実装手段

コスト削減や安定性向上へ関しては、集積化や多重化や室温動作検出器等の取り組みがある。

鍵の生成速度向上と通信距離の延伸に関しては、単一光子検出器等の性能向上、TF-QKD、自由空間 QKD 等の取り組みがある。QKD の鍵配送は光ファイバーを経由したものが多く提案・実験されているが、ファイバー中の光損失の影響で通信距離は数百 km が限界とされる。量子中継器はまだ実用段階に到達していないので、通信距離を延ばす方法の 1 つとして、自由空間を伝播させる QKD が提案されている。地上同士の通信では地球の球面形状や空気中の外乱の影響があるため、数百 km 以上の長距離通信の実現には、衛星を介した衛星通信ネットワークの構築が必要となる。ただし、現状では下記のような課題がある。

① 光子への乱流等の影響：光子が伝送路で受ける影響がファイバーの場合とは全く異なるため、専用の安定化技術が必要。散乱、吸収以外に、ビームの方向や乱流や光の拡がり等も考慮する必要がある。
② 検出器への日光の影響：単一光子レベルの光子検出を行うためには高感度の検出器が必要となるが、その場合日光が単一光子検出器へのノイズとなる。追跡システムに用いられる参照レーザの検出器にも日光が入るため影響を受ける。ノイズカット用のフィルターを入れる必要があるが、信号強度も下がる。ほとんどの量子衛星 QKD の実験は夜行われている。
③ 耐環境性：耐環境性を上げる必要がある。低温・高温、打ち上げ時の影響を受けない部品が必要。宇宙線から守るシールドも必要。
④ 受信機と送信機間の高精度の位置合わせ技術：地上と衛星間の位置合わせが必要となる。過去の実験例では追跡用の参照レーザを搭載。
⑤ 地上局との接近時間の制限：過去の実験例では、衛星の高度によって異なるものの、衛星が移動しているため地上局との間で一定量の鍵生成ができる時間が 1 日のうち数分間しかない。

ネットワーク化に関しては、世界各国の企業や研究機関が、様々な企業やユーザーにとって使いやすい QKD アーキテクチャの構成を検討し、標準化へ向けて活動を行っている。

トラステッドノードの具体的な実装方法に関しては、耐タンパ、鍵消去などの技術開発が進められているものの、より網羅的な開発・安全性の評価方法が求められている。

7　おわりに

本書は、これから量子暗号の事業に携わる情報通信ネットワークのエンドユーザーを対象に執筆した。最後に、量子暗号の本格的な普及のために検討すべき項目と、今後の展望を併せて紹介する。

１つ目はコストである。現状では、量子暗号の初期導入費用は、装置等を含めてマイホーム約１件分の高コストであり、IoT スマート社会等のエンドユーザー市場に浸透させていくためには、さらなる低コスト化が必要である。ビジネスモデルを確立させることで、実際の経済活動に連動させ、製品の量産化、ひいては、低コスト化が実現していくと考えられる。また、低コスト検出器を用いることのできるプロトコルについても、初期導入費用の低コスト化が期待される。

２つ目はキラーアプリの開発である。ハードウェアだけでなく、スマートフォンを爆発的に普及させたようなキラーアプリを充実させることも、普及には重要である。秘匿計算，ストレージ機能を有する量子セキュアクラウド技術の実証が予定されているため、そのインフラ上で動作するキラーアプリが期待される。

３つ目は標準化である。量子暗号の推奨標準技術の明確化は、製品の互換性だけでなく、品質の確保、生産効率の向上などをもたらす。現在、標準化文章の更新，国際標準への適合、運用ガイドラインの策定、並びに認定制度に向けた準備が進められている。

４つ目は意識の浸透である。日本では他国と比較して、情報セキュリティに関する危機感が浸透しにくく、情報漏洩の場合の損害賠償や訴訟に対するリスク対応も盤石とは言えないため、情報セキュリティに対する啓蒙が必要である。そこで、まず現状特に高いセキュリティ意識のあるユーザ（安全保障、医療分野等）から開拓し、政府への働きかけを含めてセキュリティに関する啓蒙活動を実施していく。

５つ目は人材である。量子 ICT 分野に携わる人材を増やすためには、教育の機会と就職の機会を増やす必要がある。教育の機会としては、大学や企業における長期的な教育体系の整備や、国家資格取得体制の確立などが期待される。就職先の確保としては、ビジネスモデルの確立により市場が拡大することで実現されると期待される。

以上の５つの検討項目を課題として、今後普及活動のため、本書を改訂していく予定である。また、本書では、光ファイバー有線を用いた固定系通信を中心として取り上げたが、量子衛星通信を活用することで、全国規模のネットワークの実現が可能となる。さらに、移動系通信への量子暗号を適用することで、アプリケーションが大幅に広がることも期待される。これら最新の動向についても追記していく予定である。

付録

A. 量子暗号のプロトコル

A.1 BB84

単一光子を利用する QKD を総称して「離散量量子鍵配送（DV-QKD: Discrete Variable QKD）」と呼ぶ。離散量量子鍵配送方式の中でも、1984 年に Bennett と Brassard によって提唱された BB84 は、理論的に無条件安全性が証明され、最も多く採用されている方式である。

鍵情報は、偏光または位相差にエンコードする。光ファイバー伝送の場合には、光ファイバー中での偏光の回転や偏光遅延現象が起こるため、最近の実験では位相差状態を用いることが多い。オリジナルの BB84 の提案では単一光子源と単一光子検出器の組み合わせでの実装だったが、現在のところ高効率・室温動作の通信波長帯単一光子検出器は研究段階であるため、実際には、前述の通り、コヒーレント光源を強度変調器によりパルス波形にして、減衰器により 1 パルスあたりの平均光子数が 1 個以下になるよう弱めて用いるのが一般的である。

簡単のため、偏光に情報をエンコードするタイプの BB84 を例に取り、鍵共有の手順を説明する。概略図を図 31 に示す。

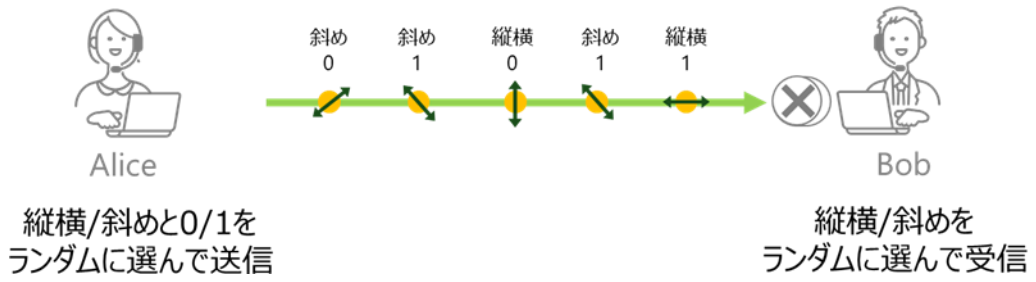


図 31：偏光エンコード BB84 の概略図

まず送信者（Alice）は、値（0/1）と基底(縦横/斜め)をエンコードした以下の 4 つの偏光方向のうち、1 つをランダムに選択して送信する。

基底＼値	0	1
縦横	↕	↔
斜め	⤢	⤡

次に受信者（Bob）は、2 つの基底(縦横/斜め)のうち、1 つをランダムに選択して受信する。すると、送信者と受信者の選んだ基底(縦横/斜め)がたまたま一致する場合のみ、受信者は正しいビット情報

（送信者が選んだ値）を検出する。送信者の選んだ基底と受信者の選んだ基底が一致しない場合には、50%の確率で 0 または 1 が検出される。

光子の送受信が終わった後に、両者は互いに選んだ基底(縦横/斜め)の情報のみを公開する。送信者と受信者はそれぞれ、相手が選んだ基底と自分が選んだ基底が一致する場合の値のみ残して基底が不一致する場合の値を捨てる。すると、両者の間で同一の値を共有することができる（図 32）。

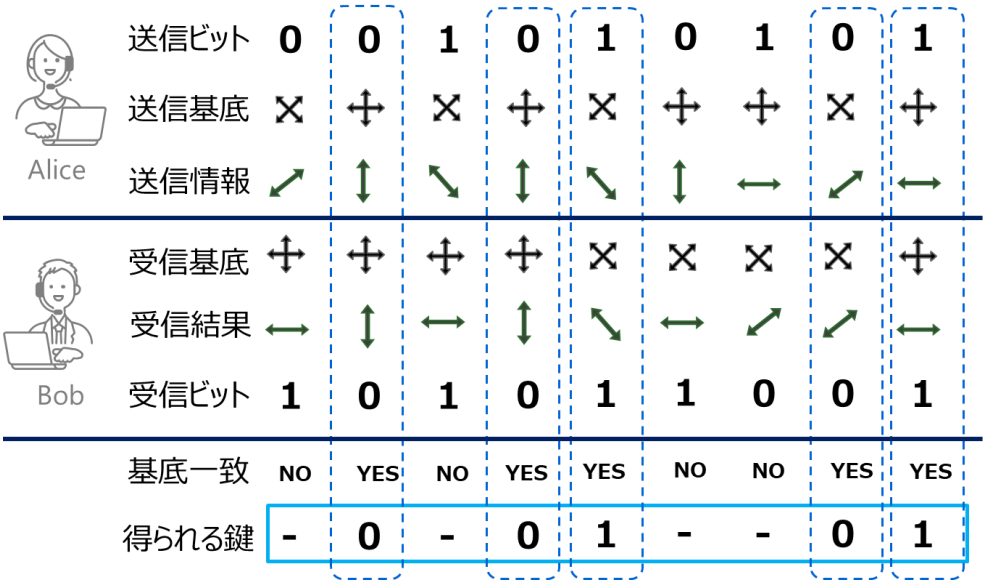


図 32：送信者と受信者の選ぶ値と基底および測定結果の例

ここで盗聴者がいて、経路の途中でランダムな基底を選んで受信し、同時にランダムな基底を選び元の経路に光子を挿入する場合を考える。盗聴者は実際に送信者が選択した送信基底を知らないので、挿入する光子の基底は、ランダムに選ぶしかない。よって、後から送信者と受信者が基底について公開し、送信基底と受信基底が一致した場合の値のいくつかを答え合わせすると、本来ほぼ 100%一致するはずの値が 50%しか一致しなくなる。このように、盗聴があるとビット誤りが発生するため、技術的にどんな進んだ攻撃に対しても誤り率の変化で検出することが可能となる。

A.2 CV-QKD

アナログ量である光電場の振幅を利用する QKD は「連続量量子鍵配送（CV-QKD: Continuous Variable QKD）」と呼ばれる。CV-QKD は主にコヒーレント光の直交振幅と光ホモダイン検出を用いており、常温で動作する汎用の光検出器を用いているため安価で小型な装置として応用できることが期待されている（図 33）。

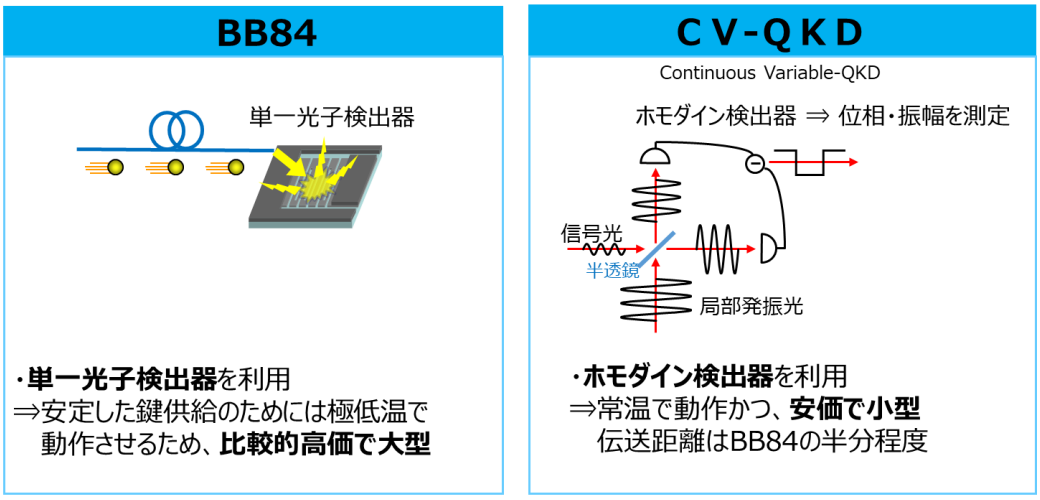


図 33：BB84 と CV-QKD における検出方法の違い

BB-84 では鍵情報を単一光子の偏光や位相に乗せるのに対し、CV-QKD では光の振幅に鍵情報を乗せる。微弱なコヒーレント光の場合には量子的な揺らぎのために、盗聴者が鍵情報、例えば 0 か 1 を完全に区別することができない。この性質により、CV-QKD の安全性を担保している。(図 34)

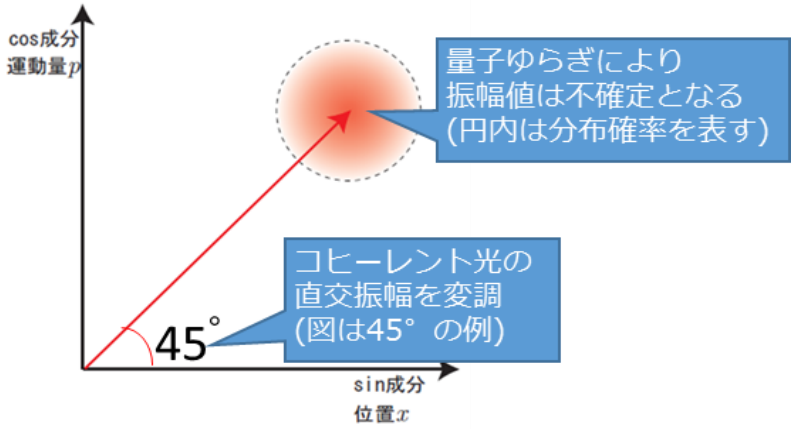


図 34：CV-QKD における不確定性の考え方

常温で動作する汎用の光検出器を用いることから、CV-QKD 技術では装置が安価に製造可能となることが期待されている。また CV-QKD の性質から既存の光通信網にも比較的容易に組み込むことができると期待されている(図 35)。

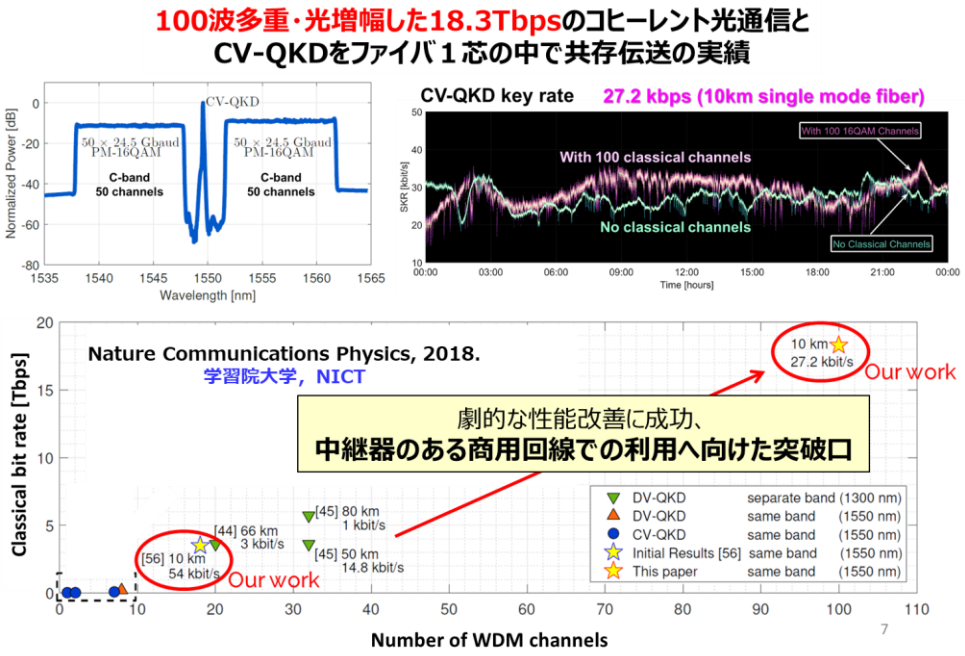


図　35：既存の光通信との共存

以上の２つの性質から、BB84 が基幹ネットワークへ適用できると考えられているのに対して、CV-QKD 方式はコンシューマ向けのラストワンマイル回線に適用できると考えられている。(図　36)

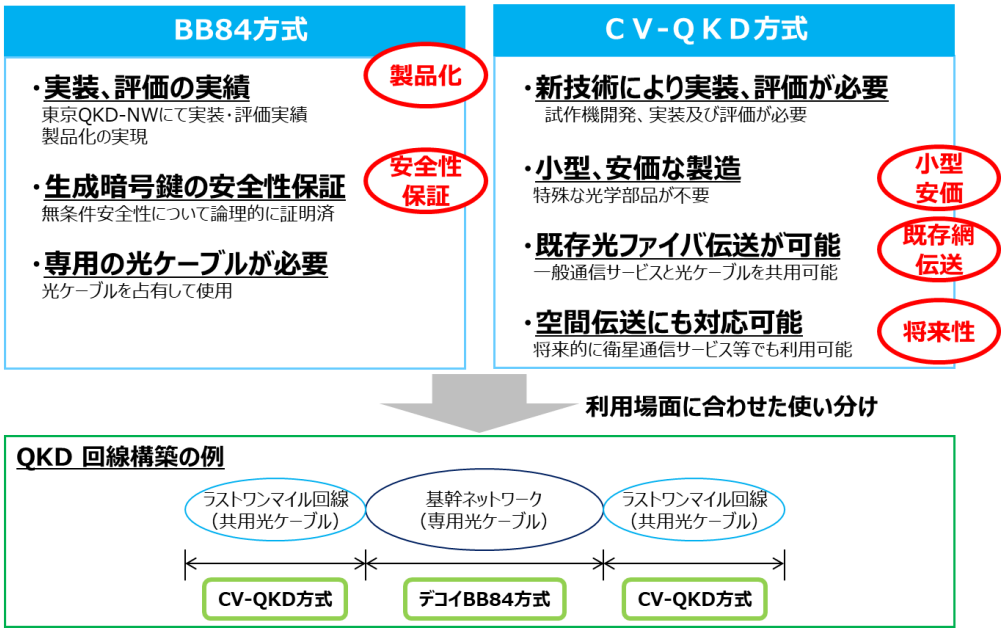


図　36：BB84 方式と CV-QKD 方式の使い分け

CV-QKD の方式は変調方式と、LO 光の生成方法により分類される。

変調方式による分類では離散変調とガウス変調がある。離散変調では一般のデジタル変調で用いられる技術・デバイスを利用することができるが、現時点では無条件安全性の証明が課題となっている。一方ガウス変調は無条件安全性が証明されているが、離散変調に比べて乱数の使用量が多い、変調方法が特殊である、鍵蒸留処理が重いなどが課題となっている。

LO 光の生成方法による分類では主にセルフホモダイン方式とリアル LO 方式 とデジタルコヒーレント方式の 3 つがある(図 37)。セルフホモダイン方式は CV-QKD 方式の概念実証に用いられた方式で、Alice 側で 1 つの光パルスを 2 つに分岐し、一方を信号光、もう一方を LO 光とする。ビームスプリッタを使用して簡単に実現することができる。ただし LO 光が伝送路を通るため、LO 光への盗聴攻撃や長距離化が難しいといった安全性・性能面での課題がある。

リアル LO 方式はデジタルコヒーレント方式で用いるホモダイン検波の安全性確認の技術実証のための方式で、Bob 内に LO 光を発生するためのレーザ光源を用意し、Alice から信号光とは別に強い光を送信し、Bob ではその光を元に LD を用いて LO 光を生成する。安定化や雑音の低減が課題となっている。

デジタルコヒーレント方式では Bob での受信結果に対してデジタル信号処理を行うことで、LO 光を Alice と同期させることなく直交振幅を測定する方式であり高性能化が期待されている。

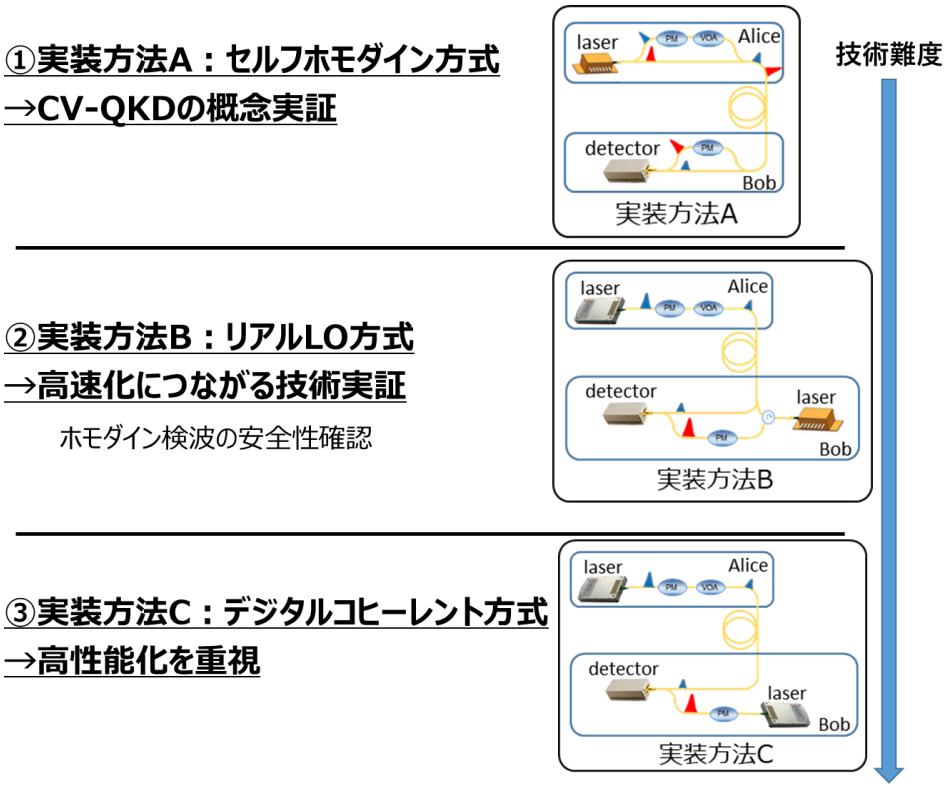


図 37：CV-QKD 方式における量子暗号技術の分類

B. 量子コンピュータ

量子コンピュータとは、従来コンピュータのような電気的情報(デジタル信号)ではなく、量子力学という新しい概念を導入した次世代のコンピュータである。デジタル信号においてビットは「0」か「1」のいずれか 1 つを表現するが、量子ビットでは量子力学的な「重ね合わせ」と呼ばれる性質により、「0」と「1」を同時に表現することができる。この性質により複数の値を同時に(並列に)計算することで、素因数分解などの従来型コンピュータで時間がかかる問題も、高速計算が可能となる（図 38）。

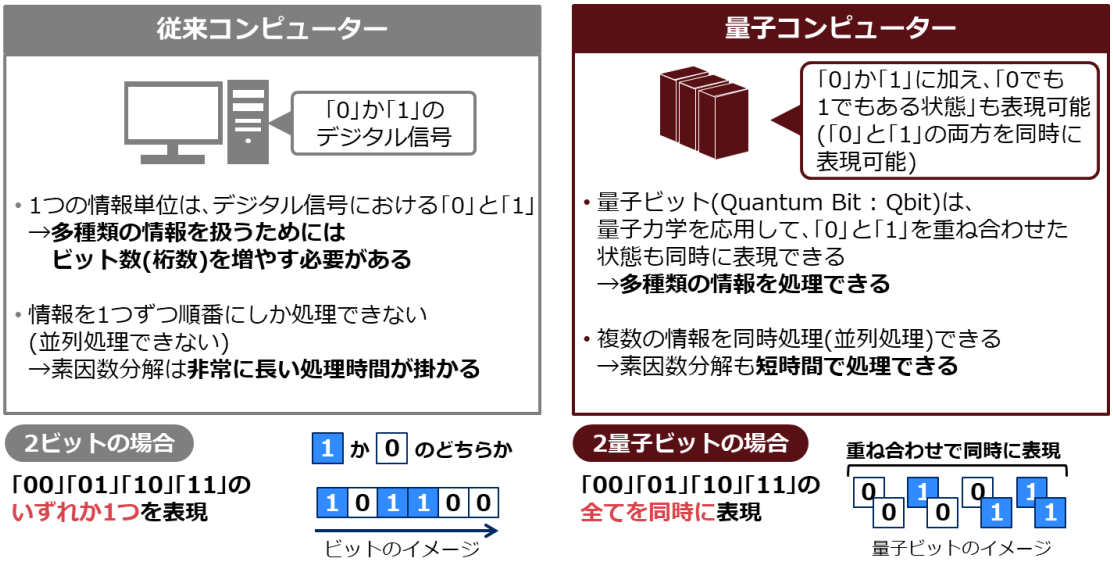


図 38：従来コンピュータと量子コンピュータの比較

B.1 量子コンピュータの利用例

量子コンピュータの方式には「量子ゲート方式」と「イジングマシン方式」の 2 方式ある。量子ゲート方式は、汎用型の方式で、現在の計算機の上位互換としての利用が可能である。イジングマシン方式は組み合わせ最適化問題という問題に適しており、巡回セールスマン問題などの現在の計算機では解くのに時間がかかる問題を高速に解くことが可能である。

B.2 量子コンピュータによる暗号解読

量子コンピュータを利用した暗号解読のための研究が行われており、代表的なアルゴリズムとして Shor のアルゴリズムと Grover のアルゴリズムが知られている。

Shor のアルゴリズムは周期性を持つ暗号方式に対して有効で、素因数分解や離散対数問題に適応可能である。RSA 暗号や楕円曲線暗号等の現代暗号は素因数分解や離散対数問題の計算が困難なことに安全性を依存しているため、Shor のアルゴリズムを用いることで現実的な時間内で容易に解読することができる。

Grover のアルゴリズムは秘密鍵の総当たりに適用することで共通鍵暗号の解読にも利用できる。鍵長を延伸することで当面は共通鍵暗号の安全性を保持できる可能性が高いが、量子コンピュータの計算速度向上により、暗号解読にかかる計算時間は従来想定よりも確実に短縮されることとなる。

量子コンピュータが開発され、これらのアルゴリズムが実装されると現代暗号は解読される危機がある。そこで、量子コンピュータによる解読を困難にする耐量子安全性暗号に期待が集まっている。

B.3 量子コンピュータの開発動向

現時点で量子ゲート型の量子コンピュータは、演算処理における重要な量子の「重ね合わせ」の状態維持が技術的に難しいため、実用化には時間が掛かると見られており、公開鍵暗号も直ちに危殆化する状況にあるというわけではない。その反面、昨今の量子コンピュータ開発は加速の一途を辿っていることから、現状の見立てを上回るスピードで量子コンピュータの課題が克服され、一気に実用化に進む状況も考えられる。

執筆者一覧

小林 宏明	（主筆）	国立研究開発法人情報通信研究機構
佐々木 雅英	（執筆）	国立研究開発法人情報通信研究機構
藤原 幹生	（執筆）	国立研究開発法人情報通信研究機構
飯塚 浩巳	（執筆）	日本電気株式会社
伊東 洋一郎	（執筆）	日本電気株式会社
遠山 裕之	（執筆）	日本電気株式会社
谷澤 佳道	（執筆）	株式会社東芝
佐藤 英昭	（執筆）	株式会社東芝
鯨岡 真美子	（執筆）	株式会社東芝
松尾 昌彦	（編集）	国立研究開発法人情報通信研究機構

本書は、内閣府総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「光・量子を活用した Society 5.0 実現化技術」（管理法人：量子科学技術研究開発機構）の光・量子通信出口戦略検討分科会 普及戦略タスクフォースによって編纂された。