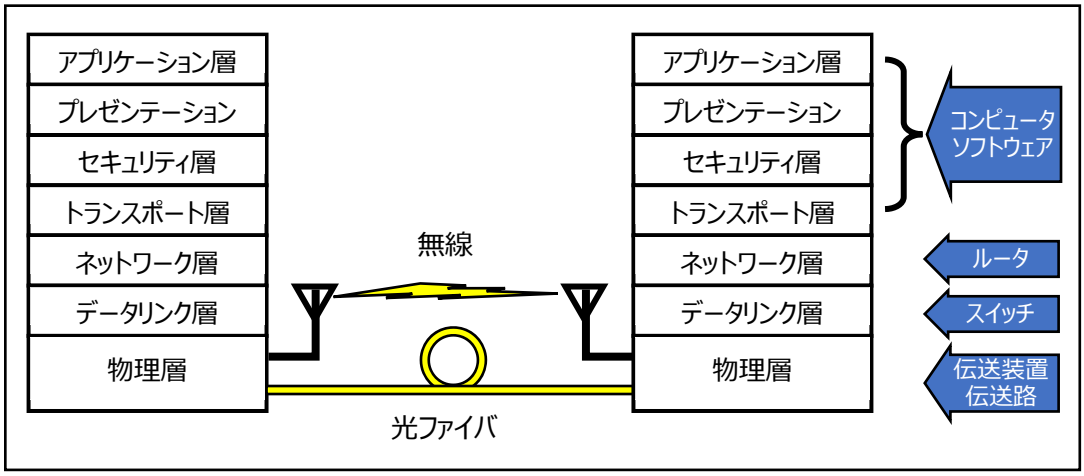


図 5-13　ネットワーク階層の構成イメージ

なお、後述の量子暗号 QNSC は、この物理層を守るセキュリティ技術であり、量子雑音を利用した物理効果で伝送路の盗聴行為からデータを守ることができる。

① 米国の AES に対する量子コンピューティングリスクの認識（Congressional Research Service「IN11921」の要約
https://crsreports.congress.gov

前述のセクションでは、公開鍵暗号系の対策として PQC の標準化について述べてきたが、本セクションでは、データの「暗号化」について考察する。暗号化は、機密文書、データ ストア、およびシステム（重要なインフラストラクチャなど）の機密性と完全性を保護するために使用される。更に暗号化は、ID を保護し、データを認証するための一意の識別子を作成し、ブロックチェーン ベースのテクノロジーを有効にするためにも使用されている。なお、「暗号化」とは、暗号化技術を使用し平文を暗号文に変えることであり、一般的には共通鍵暗号（対象鍵暗号）のことを対象としている。

暗号のサイズとセキュリティについての考え方は以下の通りである。多くの連邦政府および商用の情報技術（IT）システムでは、一般的に Advanced Encryption Standard（AES）が使用されている。主に使用されている AES の鍵の長さ(サイズ)は 128、192、および 258 ビットである。128 ビットの鍵は、$2^{128}$ ビットと表現することもできる。 攻撃者が AES-128 で暗号化されたデータにアクセスしたい場合、解析する鍵の組み合わせを平均した 1/2 の検索数($2^{127}$ 回)で鍵を発見することができる。最新の単体コンピュータを使用した場合、この鍵の探索攻撃は宇宙の年齢よりも長くかかる。そのため攻撃者はアルゴリズムを工夫してパスワード（鍵）の可能性を減らし、成功率を大幅に高めようとする。

量子コンピュータは、暗号化キーの発見に必要な時間を短縮できる。現在公開されている量子コンピュータは、開発の初期段階であるため、AES の鍵に脅威を与えるのに十分な持続的な操作を実行できる報告

はない。しかし、進行中（もしくは水面下）の量子コンピュータの研究は、そのような操作を実現する可能性がある。量子コンピュータにアクセスできる盗聴者は、既に開発されている指数関数的に速く鍵を発見できるアルゴリズムを使うと、 AES-128 においては、$2^{64}$ 回の探索回数で鍵が発見できる。このため、前述の様にサイバーセキュリティの専門家は、国家的な盗聴行為者が国政府や重要インフラ事業者から暗号化されたデータを現在もダウンロードし、将来のある時点で量子コンピュータを使ってそのデータを解読するという「steal-now and decrypt-later（今盗まれて後で解読する）」攻撃について懸念している。この様な動きを予測して、米国国立標準技術研究所（NIST）は、量子耐性暗号（QRC）標準に関する新たなプロジェクトを開始している。

NSM 10 は、連邦政府が QRC 標準の開発と採用に関して民間部門と提携し、それらへの移行計画を策定することを要求している。連保政府以外の組織を支援するために、Cybersecurity and Infrastructure Security Agency（CISA）は、sector risk management agencies（SRMA）と協力し、州政府、地方政府、および民間セクターと協力して、量子コンピューティングによる暗号化のリスクについて検討する。表 5-6 に、連邦政府機関の QRC 採用に関する NSM10 の要件を示す。NSA は、民間システムの場合と同様の期限で、国家安全保障システムとの同様の QRC 移行作業を管理することになっている。

表 5-6 連邦政府機関の QRC 採用に関する NSM 10 要件

| Action | Agencies | Deadline |
|---|---|---|
| QRC を推進し、採用するための官民ワーキング グループを作成 | NIST | 8/2/22 |
| 民間部門と協力して QRC に移行するための専用プロジェクトを作成 | NIST | 8/2/22 |
| 機関が使用する暗号システムのインベントリを作成するための要件を設定 | OMB | 10/31/22 |
| 量子コンピュータからの暗号化されたデータに対する攻撃に対して依然として脆弱なシステムについて報告 | すべての機関から CISA および NCD | 2023 年 5 月 4 日以降は毎年 |
| QRC および国家安全保障システムに関するガイダンスを発行 | NSA | 5/4/23 |
| 政府機関の QRC 移行の状況と、移行を促進するために必要な資金調達に関する推奨事項について、OMB に報告 | NCD | 10/18/23 以降は毎年 |
| 量子脆弱性の非推奨のタイムラインを提案する暗号規格。 | NIST | QRC 規格のリリースから 90 日以内(2024 年予定) |
| 量子脆弱性への移行計画を策定するための要件を設定するシステムを QRC に接続 | OMB | NIST が規格を発行してから 1 年 |

出典: NSM 10 の CRS 分析。

注: Office of Management and Budget：管理予算局（OMB）

National Cyber Dire：ナショナル サイバー ディレクター（NCD）

National Security Agency：国家安全保障局（NSA）

NSA は、民間システムの場合と同様の期限で、国家安全保障システムの同様の QRC 移行作業を管理する

ことになっている。これらの内容から、AES のインフラストラクチャからの脅威に対するセキュリティ施策技術は、現在確立できておらず、公募に頼るところから始まっている。ただし、この要件に対する米国政府の取り組みは非常に真剣であり、QRC 採用の要件におけるマイルストーンも詳細に計画されており、それだけ脅威の大きさと急ぐ必要性を客観的に理解している準備を開始している。

現在、考えられている AES のセキュリティ対策（技術）は、AES の鍵長を長く（128 を 256、更に 512）複雑にし、現在開発されているアルゴリズムによる探索回数の指数的な削減を補填することである。この解読アルゴリズム（Grover のアルゴリズム）は、まだ量子コンピュータが実現される以前（1996 年）に開発されたものであり、机上（シミュレーション上）で研究・開発されたものである。現在では、実際の様な量子コンピュータをクラウド上で利用することができる環境であり、この環境で新たな開発を行うことが可能である。前述の中国の取り組みの様に実際の量子コンピュータを利用した新たなアルゴリズムの開発も始まっている。暗号解読の対策は、アルゴリズムが発見されてからでは遅いので、先行的に対策を打つ必要がある。特に前述の steal-now and decrypt-later 攻撃を考えると、今すぐにでもできるところからの対策が必要となる。

② QNSC（Quantum Noise Stream Cypher：量子雑音ストリーム暗号）Yuen2000 Protocol（Y-00）

物理現象である量子雑音を信号秘匿に利用したストリーム系物理暗号を学会等では、QNSC（または量子雑音ストリーム暗号）と呼ばれている。一般的に量子暗号と呼ばれているものは、BB84 プロトコルを利用する量子鍵配送（QKD：Quantum Key Distribution）として認識される場合が多い。これは、量子暗号として最初に発表されたからであり、特に量子暗号の定義があるわけではない。純粋に「量子暗号」という言葉から想像すると、量子効果、量子現象、量子力学を利用した物理的な暗号方式（物理暗号）と捉えることができる。この報告では、以上の様な解釈で量子暗号を定義する。

一般的な数理暗号（本報告では、現在主に利用されている数学的複雑性で計算量的安全性を根拠とした現代暗号を数理暗号と呼ぶ）には、主に公開鍵暗号と共通鍵暗号の 2 つのカテゴリーに分類されている。量子暗号も同様に公開鍵暗号の役割でのカテゴリーに QKD、共通鍵暗号のカテゴリーに QNSC と役割や適用分野から分類することができる。公開鍵暗号は、通信の行う双方の認証や、共通鍵の共有（配送）を行う役割である。一方の共通鍵暗号は、既に配置されている共通鍵、または公開鍵暗号にて送受信者間で共有化された共通の鍵を利用して平文データ（元になる暗号化前のデータ）の「暗号化」の処理を行い、暗号文を生成し通信を行う。この様に、公開鍵暗号の QKD と共通鍵暗号の QNSC は、役割も利用シーンも全く異なるものであり、両者を比較し優劣を議論するものではない。

安全性においてよく言われている「情報理論的安全性」について考えてみる。BB84 プロトコルは、発表当初、One Time Pad（OTP）暗号方式と組み合わされて報告されている。OTP は、クロード・シャノンにより 1948 年に情報理論的安全性の証明を報告されている。しかし、この OTP の情報理論的安全性を確実に実行するためには、平文の文字数以上の完全にランダムな秘密鍵を安全に配送する手段が必要であり、当時は、実現することが非常に困難であった。これを実現できたのが単一光子を利用した鍵配送による BB84 である。言い換えると「BB84 によって OTP の情報理論的安全性を実現できた」ということであり、BB84 自体が情報理論的安全な暗号ということではない。

表 5-7　暗号の種別例

| 項目 | 数理暗号例 | 量子暗号の例 | 用途 |
|---|---|---|---|
| 公開鍵暗号 | RSA | QKD（BB84） | 鍵の共有化、認証 |
| 共通鍵暗号 | AES | QNSC（Y-00） | データの暗号化 |

【現代の暗号に期待されている要件】

現在の情報化社会では、伝送路（有線では光ファイバ、無線では自遊空間等）に流れるデータの量は膨大であり光ファイバでは、T（テラ）bps 以上のデータ伝送も要求され、無線においても Gbps クラスの伝送速度（伝送容量）が要求され実用化されてきている。これらのデータには、国家機密から個人情報まで含まれており、社会活動を安全に維持するためにも情報漏洩やサイバー攻撃に対抗できる安全性の確保が必須である。またこれらの通信は、重要な社会インフラにも直結しており、常に通信のリアルタイム性を維持することが必要であり、低遅延の通信が要求される。

一方、有事の場合、ウクライナ、ロシア戦争における情報戦や通信傍受等の情報通信における役割が攻防において非常に重要なポイントであることが明確になってきた。この戦争で使用されている通信においての安全対策（暗号化等）は、当然行われているはずであるが、一部の報道における戦果や戦略から考えると、通信内容の傍受・解読が予想以上に進んでいるように思える。

Y-00 プロトコルの基本アイディアは、ノースウェスタン大学の H.P.Yuen 教授によって発案され、玉川大学の廣田修名誉教授との共同研究で理論の体系化を開始し、2000 年に Yuen 教授によって公開されたことで、Y-00（Yuen-2000 プロトコル）と呼ばれるようになった。

H. P. Yuen, “A new quantum cryptography,” Report in Northwestern University, 2000.

Y-00 を用いた共通鍵暗号である QNSC を用いることで共通鍵暗号の耐量子コンピュータ性能は更に向上する。図 5-14 は、既存の現代の計算量的安全性を根拠とする数理暗号と Y-00 の安全性根拠の適用範囲を図式化したものである。縦軸は、安全性の根拠の範囲を表しており、横軸は暗号の種類を表している。Y-00 は、従来の計算量的安全性に加え物理的な測定量的安全性が担保される。

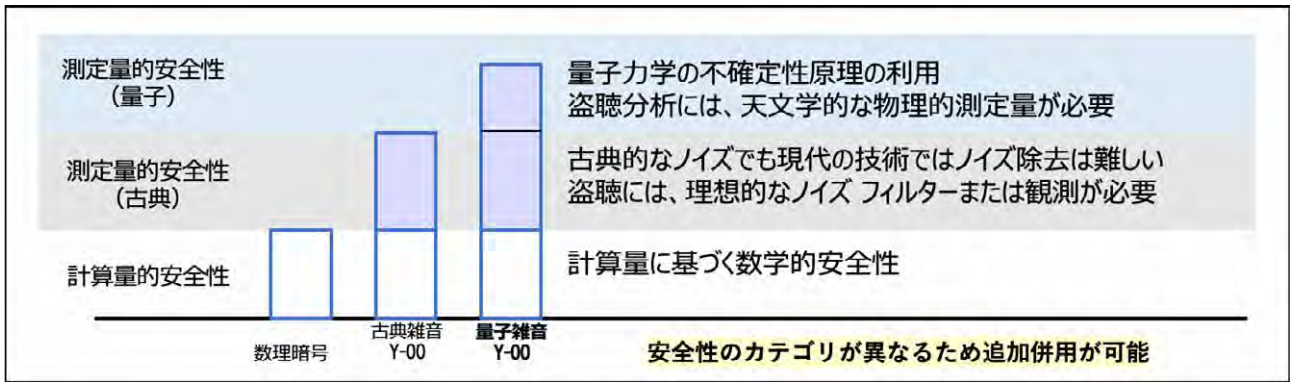


図 5-14　測定量的安全性の位置付け

この測定量的安全性を生成するために量子雑音を利用する。量子雑音は、量子力学で定義されている以下の３つの法則に基づいている。

O. Hirota, M. Sohma, M. Fuse, and K. Kato, “Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme,” Phys. Rev. A, vol. 72, p. 022335, 2005.

K. Harasawa, O. Hirota, K. Yamashita, M. Honda, S. Akutsu, T. Hosoi, Y. Doi, K.Ohhata, T. Katayama, T. Shimizu, “Consideration of the Implementation Circuit of Randomization for Physical Cipher by Yuen 2000 protocol”, The Transactions of the IEICE C, vol. J91-C, No8, p1-10, 2008.

K. Harasawa, O. Hirota, K. Yamashita, M. Honda, K. Ohhata, S. Akutsu, and Y. Doi, "Quantum encryption communication over a 192 Km, 2. 5 Gbit/sec line with optical transceivers employing Yuen-2000 protocol based intensity modulation", IEEE/OSA, Journal of Light Wave Technology, vol-29, No. 3, p316-323, 2011.

これらの法則によって、盗聴を目的とする観測者は完全ランダムな雑音の影響を避けることができず、タッピング（盗聴）で得られる暗号データは、例え同じ暗号文を繰り返し流したとしても、抜取るたびに異なったエラーを発生する。また、この抜取りデータのエラー確率は、限りなく 50%に近くすることができる。

図 5-15 に Y-00 プロトコルの仕組みの概略を示す。Y-00 の安全性は、LD 光の量子ゆらぎ（量子雑音）効果に基づいており、量子不確定性理論的に量子ノイズは完全にランダムであり、従来のノイズとは異なり、人為的に除去することはできない。Y-00 の安全性概念イメージでは、物理の殻を破らないと数学的根拠が見ることはできない。この物理の殻を破るには、天文学的な測定量（測定機材や測定時間）を重ね物理量を解析することが必要となり、そのデータを基にその後解読計算のプロセスとなる。

・ボルンの規則

量子力学において量子系について物理量の測定をしたとき、確率的にある値が得られるという最も基本的な原理（規則）である。また、そのときの量子系（光子や電子）を観測する確率は、波動関数Ψの絶対値（量子の振幅）の２乗に比例する。（$|\Psi|^2=\cos^2\theta$）

・不確定性原理

量子力学において量子系について運動量と位置は同時に正確に測定することはできない。すなわち、ミクロな領域では粒子の位置と運動量は正確には決められず、$\Delta x \cdot \Delta p \geq \hbar/2$（ここで $\hbar \equiv h/2\pi$、Δx は位置（光の位相）の測定誤差、Δp は運動量（光の強度）の測定誤差、h はボルツマン定数）という「不確定性関係」が成り立つ。一方の測定誤差を極めて小さくすれば他方の誤差が極めて増すことになり、結局誤差の積を一定以下には下げることが出来ない。

・ノークローニング定理（no-cloning theorem：量子複製不可能定理またはクローン禁止定理）

未知である任意の量子状態に対し、それと全く同じ複製を作る事は不可能であるという定理。複製を作ることは、同じ因子を持った分離可能状態を作ることである。コピーが可能だとすると、基本定理である不確定性原理が成立しなくなる（コピーした一方で運動量、もう一方で位置情報と同時に２つの物理量の測定が可能になるため不確定性原理に反する）。

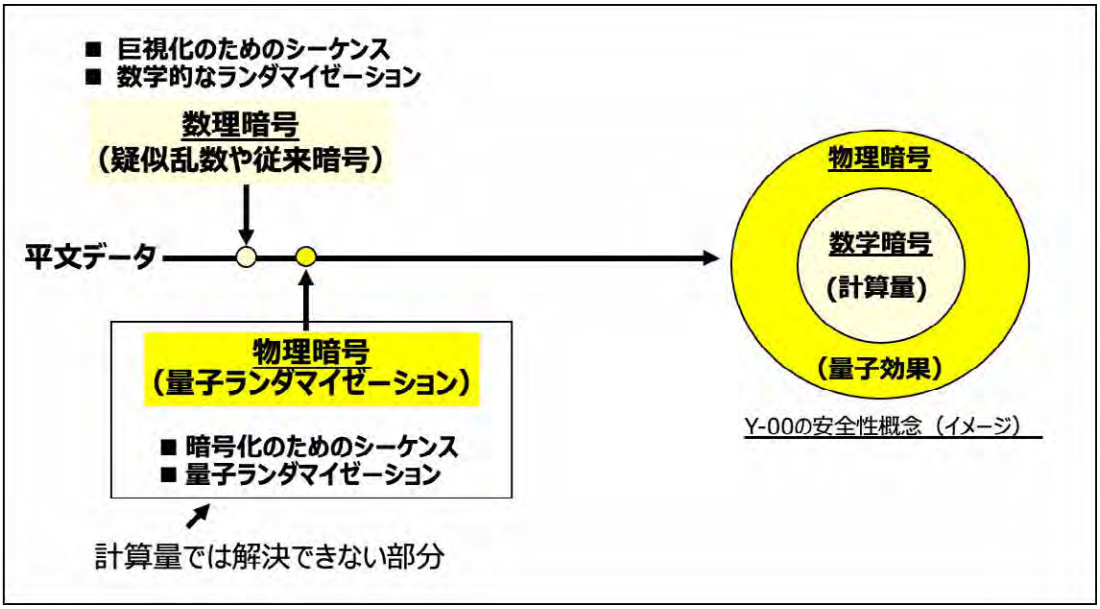


図 5-15　Y-00 プロトコルの仕組

「測定量的安全性」とは?

Y-00 暗号化信号を盗聴では、量子力学の原理によるランダムで回避不可能な量子雑音のため、正しい信号検出ができない。そのため、最善の攻撃方法は、秘密鍵のない Y-00 受信機（疑似受信機）を利用したキーブルートフォースキー（鍵の総当たり）攻撃である。この攻撃を行う場合、Y-00 の暗号解読には物理的な信号復調処理（ハードウェア処理）を伴うため、計算処理を行う前に以下の物理処理（測定）が必要になる。

盗聴者が受信機によるキーブルートフォース攻撃をおこなうには、1077 セットの疑似受信機を使用する必要がある。(物理的な並列攻撃⇒物理量による「測定量の安全性」) 盗聴者が盗聴信号をシリアルに解読するために、必要なデータ量は「1079 ビット」であり、10Gbps の伝送を想定すると、解析に必要な正しいデータを取得する時間は、1060 年間となる。(物理的直列攻撃⇒測定時間による「測定量の安全性」)

前述の様に光ファイバネットワークにおけるラストワンマイルと専用回線は、利用者の光ケーブルを特定し易く、盗聴者は利用者拠点の近くのとう道や架線からアクセスすることも可能である。図 5-16 は、現代のネットワーク構成例である。図中の青い回線が加入者線の端局から回線利用者までのラストワンマイルや利用者の拠点間をダークファイバ等で、直接接続する専用線であり、黄色いマークのところが比較的利用者を特定し易い部分である。盗聴者は、このような物理層のポイントを狙うため、データを取り溜められないためにも物理系暗号の QNSC 等で守る必要がある。

端局より上位のネットワーク（図中の公衆網）では、様々な利用者のデータが入り乱れることになるので、ある特定の利用者の回線を見つけ出すのは困難になる。しかし内部にひそむ脅威アクターが存在すれば、ラストワンマイルや専用線だけでは安全性を確保するのは不十分である。NTT で進めようとしている IWON 構想（アイオン：Innovative Optical and Wireless Network）の様に、端末から公衆網やクラウドまで電気信号に変換することなく光信号のまま全ての通信が可能になるオールフォトニック・ネットワークが実現

されるとQNSCは、ネットワーク全ての領域で適用可能になると期待できる。この期待は、あくまでも将来性についてであり、セキュリティ対策を先延ばしにする理由にはならない。現時点で完成できなくとも、安全性の効果と実用性が確認できるのであればすぐにでも対応すべきである。

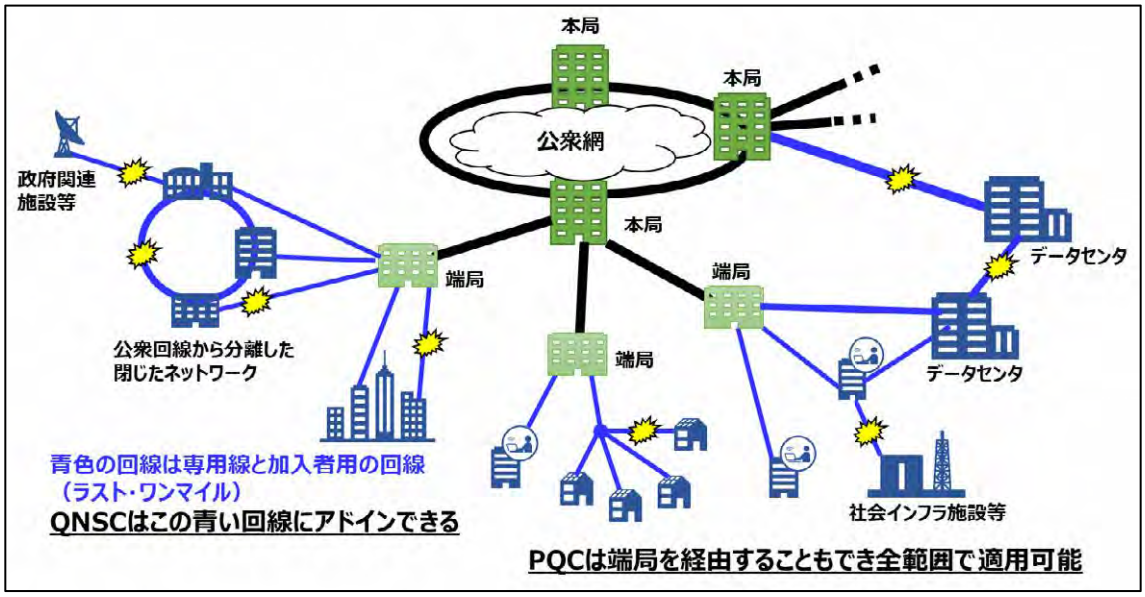


図 5-16　ネットワーク構成の例

## 第８節 量子通信

量子コンピュータを利用した計算能力向上を図る手段として、複数台の量子コンピュータを利用したクラスタ連携等を実現する方法がある。量子コンピュータ間を接続するためには、従来（古典）のコンピュータの様な「０」、「１」が決定されているようなバイナリ情報の通信方式では、量子コンピュータの性能を十分引き出すことはできない。量子コンピュータ間の伝送には、量子重ね合わせ、量子もつれ（エンタングルメンと）などの量子状態を維持したまま情報伝達することが必要になる。光子は、この状態を維持しながら伝送させる媒体として有力であり、現在主に研究開発されている量子状態を維持したままの伝送技術は、QKD で利用されている単一光子伝送である。

上記の様な理由により、量子通信を一部の一般的な解釈では、「量子通信＝量子暗号（QKD)」と説明されることもあるが、正確には、量子技術を応用し、多くの情報を効率よく伝送するための情報通信システムであり、その技術は、量子暗号や量子コンピュータ間の通信に応用できるものである。特に量子コンピュータ間の通信においては、「量子インターネット」と呼ばれている。量子インターネットは、現在のインターネットとは全く異なるものであり、機能的にも技術てきにも現在のインターネットの延長線上に量子インターネットがあるわけではない。

量子通信を行うためには、量子ノードと呼ばれる量子力学の原理に基づく送受信機や中継機の新たな開

発が必要になる。これらは光子や原子レベルの量子状態を観測し、制御することが要求される。更に量子状態は、環境条件等に対して非常に敏感であり、長時間維持することが困難である。このため従来の通信とは全く異なる環境や技術が必要になる。

https://www.nict.go.jp/data/nict-news/NICT_NEWS_1608_J.pdf（ NIINCT NEWS No.459 AUG 2016）

米国は、量子ネットワークの観点から、2020 年 2 月に「U.S. Quantum Network Strategic Vision：米国量子ネットワーク戦略ビジョン」を発表した。米国は、世界で初めて量子ネットワーク インターネットを推進する国であり、その戦略ビジョンでは、次の 2 つの目標が設定されている。1 つ目は、今後 5 年間で、米国の企業と研究所は、量子ネットワークを可能にする基礎科学と主要な技術を実証し、これらのシステムの潜在的な影響と、ビジネス、科学、健康、および国家安全保障において量子アプリケーションの改善効果における利点を確認する。2 つ目は、今後 20 年間で、量子インターネットリンクがネットワーク量子デバイスを使用して、従来の技術では実現できない新しい機能を実現すると同時に、量子エンタングルメントに対する人々の理解を促進する。

ロシアは、2020 年 9 月に「量子通信ロードマップ」を発表した。この中で 2024 年までに光ファイバや大気・衛星量子通信技術の開発、商用量子通信ネットワークの確立や特殊通信など、120 以上の対策やプロジェクトを実施することが規定されている。これは、連邦プロジェクト「デジタルテクノロジー」の枠組みの中での 2 番目の量子技術戦略文書である。その最初の重要なプロジェクトの 1 つには、全長約 800 キロメートルのモスクワ-サンクトペテルブルク間のバックボーン量子ネットワークの構築が含まれている。

オランダは、2021 年 1 月に「国家量子技術アジェンダ」を発表した。これは、量子技術におけるオランダのリーダーシップを加速することを目的として、プログラム集中の最前線の中に国家量子ネットワークの開発が含まれている。

中国の 2015 年から 2022 年 8 月まで量子通信政策は、以下の様に発信している。中国では、量子通信技術を国家戦略目標に推進し出したのは比較的遅い。近年、量子技術の重要性が多くの国家政策文書で明確にされ、量子開発を「第 13 次 5 カ年計画」国家科学技術イノベーション計画と「第 14 次 5 カ年計画」デジタル経済開発計画に組み込んでいる。2016 年 7 月に国務院が発行した「第 13 次 5 カ年計画」国家科学技術革新計画では、2030 年に向けて、量子通信と量子コンピュータが国家戦略の意図を反映した主要な科学技術プロジェクトの 1 つとして選択されており、量子情報技術の開発に焦点を当てている。2022 年 1 月に国務院は「第 14 次 5 カ年」デジタル経済発展計画を発表した。これは、センサーや量子情報などの将来を見据えた分野を目指し、デジタル技術の基礎研究開発能力を向上させ、主要製品の自給自足を強化することを目的としている。現在、中国は、量子情報技術、特に量子通信分野の産業化の探求において課題を克服しつつあり、世界の広域量子安全通信技術のロードマップの実現をリードしている。国際標準化において重要な発言権を獲得した。

https://www.chyxx.com/industry/1124216.html

■一般的な量子通信の原理（光子の量子もつれ交換）

量子通信(quantum communication)とは、量子力学に基づいた理論や原理を応用した通信であり、量子力