いる（特に米国政府は、この脅威に対しては重要視している）

耐量子コンピュータ対策として既存の暗号を利用しているインフラを新たな暗号（PQC など）へ移行するには、ソフトウェアベースでもインターネットに接続する殆どの電子機器の変換が必要になるため、少なくとも 10 年以上かかると推定されている。

2021 年度の光ファイバケーブルの普及率は、58.2%であり、日本政府は、「デジタル田園都市国家構想」の基本方針案では、2027 年度末までに光ファイバ回線を 99.9%の世帯へ普及させるとしている。更に、ファイバケーブルの国内カバー率は、2023 年度までに 99.9%以上を目標にしている。

https://www.cas.go.jp/jp/seisaku/digital_denen/dai8/shiryou2.pdf

https://www.soumu.go.jp/main_content/000803507.pdf

また、島国である日本の国間は、主に光海底ケーブルを利用して世界中に接続されている。光海底ケーブルの盗聴事例は、いくつか報告されている。

光ファイバケーブルは、現代の情報化社会活動において欠かすことができない通信インフラの中心的な役割を担っている。このように一般社会活動においても通信インフラに対する安全保障は重要であり早急に対策する必要がある。

第５節 各国の耐量子コンピュータへの取り組み

【米国の PQC の取り組み】

米国の NIST では、2016 年から量子コンピュータの暗号解読を想定した、量子コンピュータの計算能力に耐性のある耐量子計算機暗号（PQC：Post Quantum Cryptography）の公募を開始している。ここで提案されている暗号は公開鍵暗号に置き換わるものであり、認証や鍵共有（鍵配送）に適用するものである。

現在、第３ステージを終了し４つの暗号が標準化に採択された。また、更に、鍵配共有を主とする公開鍵暗号（KEMs）においては４つの暗号が最終候補として残っている。

表 5-3　第３ラウンドで標準化が決定した暗号アルゴリズム（2022 年 7 月 5 日）

目的	暗号
公開鍵暗号/KEMs （Public-Key Encryption/KEMs）	CRYSTALS-KYBER：クリスタル：ケイバー
デジタル署名 （Digital Signatures）	CRYSTALS-Dilithium：クリスタル-ダイリチウム FALCON：ファルコン SPHINCS$^+$：スフィンクス$^+$

採択された候補は、SPHINCS＋以外は格子暗号系であり、CRYSTALS-KYBER、CRYSTALS-Dilithium が本命である。ただし CRYSTALS-Dilithium は処理が重たいので軽量な FALCON も標準化に残された。また、SPHINCS＋ は、格子方式暗号だけの依存を回避する目的で残された。ただし、格子方式暗号の暗号化、復

号化は、鍵長が長く、処理が複雑で時間が掛かるため、更により軽い暗号化の検討が求められている。このため検討を更に継続し、４つの検討候補として第４ステージで下記の暗号が最終候補として残っている。

表 5-4　（ファイナル）ラウンドで候補として残った暗号アルゴリズム（2022 年 7 月 5 日）

目的	暗号
Key-Establishment Mechanisms （KEMs）	BIKE Classic McEliece HQC SIKE

BIKE と **HQC** はどちらも構造化された暗号に基づいており、どちらも格子方式に基づかない汎用 KEM として適している。NIST は、第 4 ラウンドの終了時に、標準化のために、この 2 つの候補のうち多くても 1 つを選択する予定している。

SIKE は、鍵と暗号文のサイズが小さいため、標準化に対して魅力的な候補であり、更に第 4 ラウンドで安全性の研究し続ける方針であったが、最近（2022 年 8 月）、安全性に重大な欠陥があり、解読可能であるとの論文が報告されたため、今後 NIST で検討継続をするためには、その欠陥を回避する対策が必須である。

https://eprint.iacr.org/2022/975.pdf

”AN EFFICIENT KEY RECOVERY ATTACK ON SIDH （PRELIMINARY VERSION）” WOUTER CASTRYCK AND THOMAS DECRU imec-COSIC, KU Leuven）

Classic McEliece はファイナリストであったが、現時点では、まだ標準化されていない。Classic McEliece は、既に安全であると広く見なされているが、公開鍵のサイズが大きいため、使用するソリューションは、限定的と考える。しかし第 4 ラウンドでは、標準化に採択される可能性がある。

NIST は、PQC を現在の暗号のように、様々なソリューションやシステムで利用したいと考えており、そのためには、更なる軽量化が必要であり、2022 年８月に新しいアルゴリズムの公募を開始している。同時に NIST は、格子アルゴリズムに基づかない新たな追加の汎用署名スキームを公募している。これは、証明書の透明性などの特定のアプリケーションでは、短い署名と迅速な検証を備えた署名スキームが必要なためである。

NIST は、格子アルゴリズムベース以外の暗号の追加公募も実施しており、ポスト量子署名標準（post-quantum signature standards）を多様化することを目指している。これらの公募条件を考えると、現在採択されている格子アルゴリズムの暗号だけでは不十分であり、また、実用的に軽量（処理速度の速い）暗号が必要と考えているようである。更に、SIK のように、採択後に安全性に対する弱点や新たな解読手法が確認されるなど、標準された PQC の安全性が保障されていると考えるのは、まだまだ危険である。

https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

https://csrc.nist.gov/projects/pqc-dig-sig

更に、米国 CRS (Congressional Research Service)の INSIGHT Reports によると、米国政府として、2022

年 5 月 4 日にバイデン大統領は、国家安全保障覚書 10 (NSM 10)に署名した。付随する大統領令（Executive Orde：EO）とともに、覚書では、量子情報科学（quantum information science：QIS）における米国のリーダーシップを促進することを目指している。 NSM 10 は、量子コンピュータが「暗号化」されたデータやシステムに与える可能性のある潜在的な脅威にも対処している。

https://crsreports.congress.gov/product/pdf/IN/IN11921

【中国、ロシアの PQC の取り組み】

中国とロシアは、米国を中心に標準化を進めている PQC とは異なる独自のスキームの PQC を検討している。しかし基盤となる考えは、NIST と同様に格子ベースやハッシュベースの暗号スキームである。中国暗号研究協会 (CACR：Center for Advanced China Research) は PQC の公募を開始し、2020 年初頭にその採択結果を発表した。上位の採択結果は、格子ベースの“Aigi-sig”、”LAC.PKE”、および、誤りのある非対称学習 (LWE：Learning with Errors) 問題に基づいている“Aigis-enc”である。

米国 NIST は 2016 年に PQC の公募を開始し、2022 年の 7 月に最初の採択グループを発表し、2024 年までに PQC 標準を公開することを目指している。一方、中国 CACR は、 2018 年に公募を開始し、2020 年に採択を公開した。その報告では、中国は 2022 年中に 独自の PQC 標準化プロセスを開始する予定であり、2025 年頃に商用移行を開始する予定としている。

【標準化について】

一方で、どの様な国でも、国際標準化機構 (ISO) またはインターネット エンジニアリング タスク フォース(IETF)によって設定された国際基準に従うだろうという意見もある。ISO や IETF 以外で独自の規格を開発した場合、世界の他の地域とシームレスにやり取りすることはできなくなるからである。NIST は、既に、これらの国際機関と協力している。これらの標準化団体は、NIST で行っている標準化に対して非常に期待しており、NIST の結果を待ちたいと考えている。まずは、NIST の暗号を国際標準化機関で採用し、その後で NIST 以外の他のアルゴリズムを追加する考えである。しかし、これらの考えは、注意が必要である。標準化暗号は、どこの国でも一般的な商用利用等はあるが、政府や軍、および国内の重要情報は独自暗号を利用すると考えるのが一般的である。そのため、公開する暗号スキームとクローズドする暗号スキームを個別に開発し使い分けて利用すると考えられる。

https://www.sdxcentral.com/articles/analysis/china-russia-to-adopt-slightly-different-pqc-standards-from-us/2022/10/

【中国の PQC】

中国での PQC の取り組みについて、中国科学院の Jiwu Jing から「Research of Post-Quantum Cryptography in China」というタイトルで講演があった。講演内容の抜粋した考え方は以下の通りである。

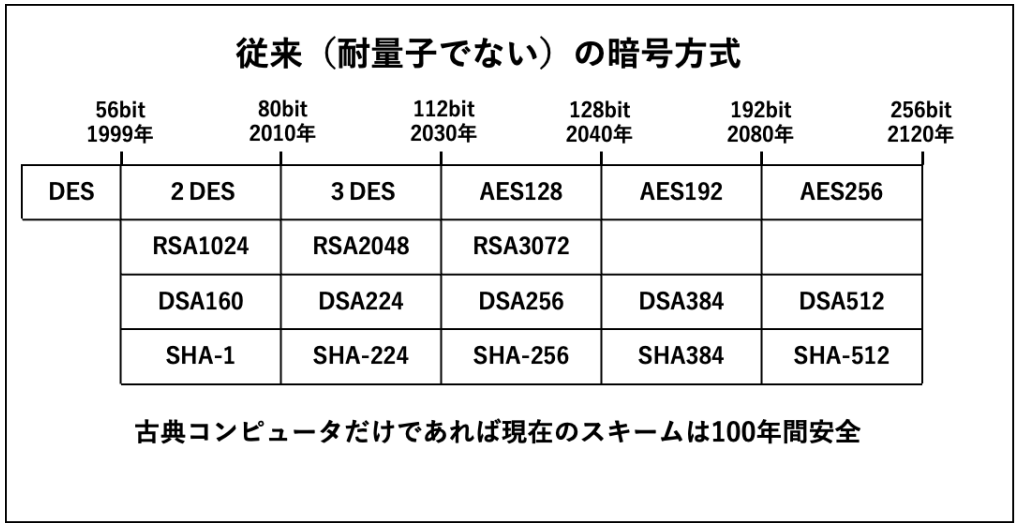

図 5-6　中国の講演資料 1

量子コンピュータが存在しなければ、既存の現代暗号は 100 年間安全である。

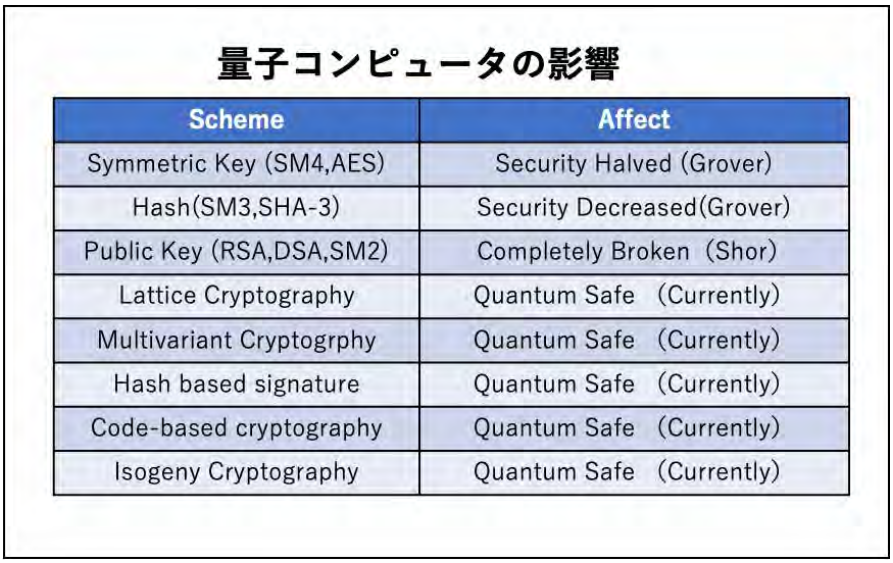

図 5-7　中国の講演資料２

しかし、量子コンピュータが実用になると共通鍵（対象鍵）暗号（SM4、AES 等）の安全性は半減し、ハッシュ暗号（SM3、SHA-3）の安全性は低下する。また、公開鍵（非対称鍵）暗号（RSA、DSA、SM2 等）は、完全に破られる。一方、Lattice、Multivariant、Hash based signature、Code-based、Isogeny は、現時点では耐量子コンピュータの安全性を保てると考えている。

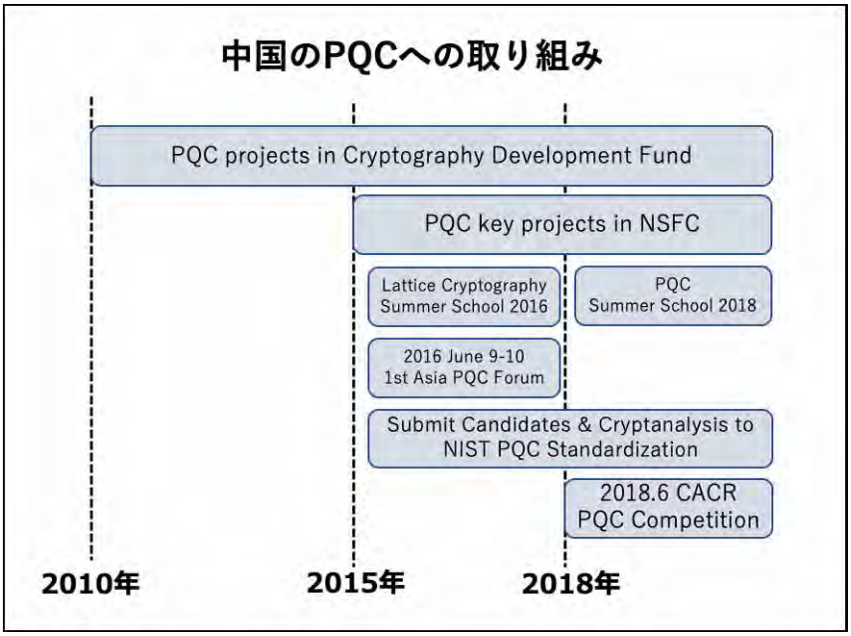

図 5-8　中国の講演資料３

CACR（中国暗号研究協会）では、2018 年 6 月に PQC 公募を開始している。

図 5-9　中国の講演資料４

また、中国は、NIST の標準化の公募に対しても上図のような候補で提案している。

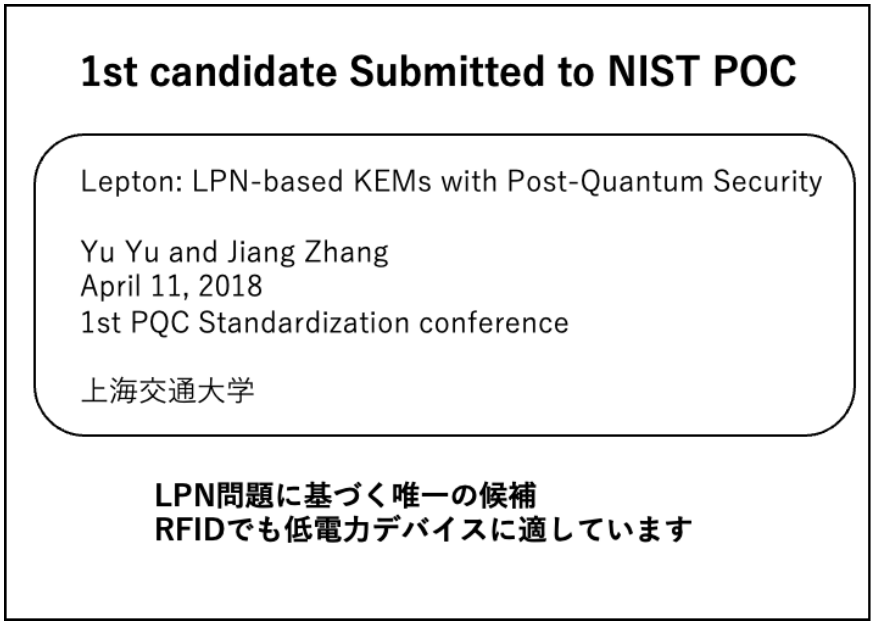

図 5-10　中国の講演資料５

NIST PQC に提案された最初の候補は、LPN 問題に基づく唯一の候補であり、RFID でも低電力デバイスに適することができる。

図 5-11　中国の講演資料６

また、国際標準化委員会である ISO/IEC SC27 WG2 SD8 の PQC プロジェクトに参加している。

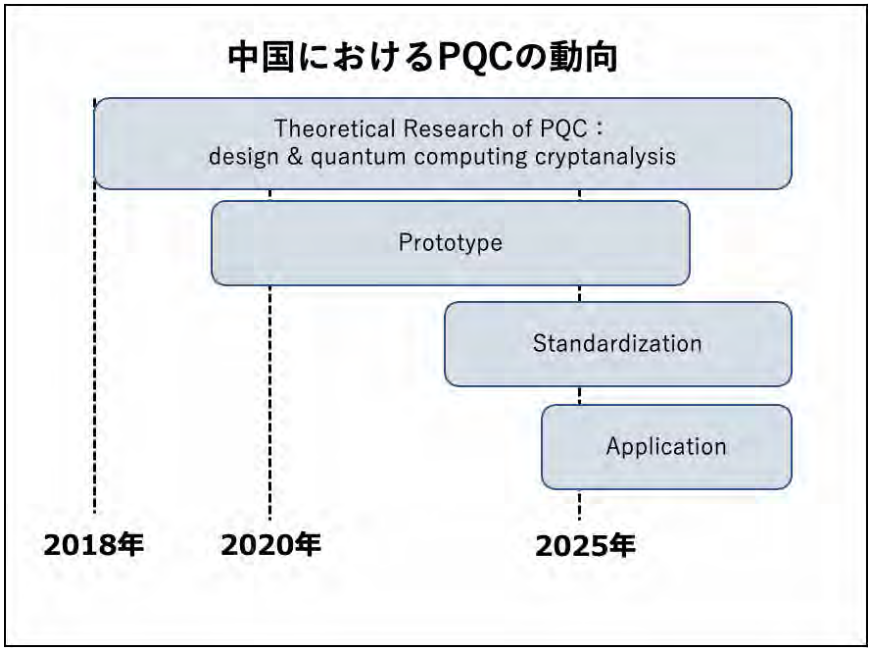

図 5-12　中国の講演資料７

一方、中国国内に向けた PQC 開発の取り組みは、2018 年より PQC の理論研究として設計と量子コンピューティングの暗号解読の研究を始めており、2023 年ごろまでに標準化、2025 年前に商用移行としている。上記のように、量子コンピュータを利用した暗号解読の研究も同時に進められており、中国では、量子技術に対して莫大な投資を行っていることを考えると、量子コンピュータを利用した暗号の解読における脅威は大きいと考えられる。

https://docbox.etsi.org/Workshop/2018/201811_ETSI_IQC_QUANTUMSAFE/EXECUTIVETRACK/JING_CHINESEACCADEMYOFSCIENCE.pdf

Research of Post-Quantum Cryptography in China　Jiwu Jing （Data Assurance and Communications Security Research Center　Chinese Academy of Science）

【ロシアの PQC 開発状況】

ロシアも PQC の国家標準を策定している。モスクワ通信情報技術大学(MTUCI) 量子センタ　Konstantin Panko　ポスト量子暗号部門責任者によると、「現在、既に量子コンピュータ耐性のある次世代の情報セキュリティシステムを構築する完全に独創的な暗号ソリューションを持っている」と発言している。彼らのチームは、現在の国際的な慣行と独自の科学的成果の研究に基づいて、情報セキュリティの 2 つの基本的な問題を解決するため、新しい国家標準の草案を準備していると強調した。「共有鍵を生成するための時代遅れの Diffie-Hellman アルゴリズムと GOST 34.10-2018 電子署名標準の代わりに、初めて代数幾何学暗号に基づく Classic McEliece タイプのシステムを提案した。そのパラメータは計算能力に応じて変更でき、また、保護されたシステムと必要な情報セキュリティの程度によって変更することができる。これは、世界の慣行と比較して優位性がり、先行していると考えている。新しい標準は、国内の情報インフラのデジタルデータプラットフォームで使用される。」と発言している。

https://digitnews.in/russia-develops-national-standards-for-post-quantum-cryptography/

第６節 PQC と量子暗号（QKD）

現在、各国における暗号通信の耐量子コンピュータの対策における考え方は、以下の通りである。

① 米国（NSA：National Security Agency） 2020/10/26

NSA は、QKD に対して以下の問題点を指摘し懸念を抱いており、QKD の下記の課題が解決されない限り、セキュリティシステムでの使用の推奨や認定はしない方針である。

A) 送信者と受信者の間の初期認証がない
QKD は、送受信者間の初期認証手段を持たないので双方の安全を保証するために非対称暗号（RSA 等は既に危険なので、PQC 等と考える）か、または事前配置された鍵で認証が必要になる。
→以下の各国ともに PQC だけで十分であり、QKD は、現時点で必要ないと考えている。

B) 量子鍵配送は専用の機器が必要であり、現在の通信に適さない通信速度と距離の限界である。
QKD は物理特性に基づいており、ユーザーは専用のファイバ接続や自由空間での送信機を物理的に管

理する必要があるため、既存のネットワーク機器に簡単に統合することができない。また、通信速度や距離の限界が現在の通信環境に適さない（通信速度は遅く、伝送距離は短い）。

C)　堅牢な中継施設（trusted node） が必要のため新たな多額の投資が必要
QKD ネットワークでは､信頼できる中継設備が必要であり､新たに大規模な設備コストが必要であり、また内部脅威への安全対策も必要になるためユースケースに制限がある。

D)　現在実現可能なシステムは、現代技術で限定的なため、無条件安全の理論には達していない
実用的な QKD システムの実際の安全性は、物理法則の理論的な無条件安全性ではなく、実装と工学設計で達成する限定的な安全性である。暗号化の安全性誤差の許容度は非常に小さく検証が困難であり、QKD の実装は脆弱性をもつ可能性が考えられる（市販の QKD 装置を使った実験的な盗聴事例も報告されている）。

E)　セキュリティ確保のため通信を停止しているため、「通信の可用性」を維持できない
QKD の安全性の根拠は、盗聴者検知でのサービス停止（通信停止）であり、これ自体が QKD の重大な脅威となる。（通信の可用性が侵される脅威）

これらの QKD の課題は、以下の他国も同様に考えており、実用化においては、その対策が急務である。
https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

② 英国（NCSC：National Cyber Security Centre 英国国家安全保障局）2020/3/24
NCSC は、従来の暗号の鍵配送に対し、QKD の特殊なハードウェア要件と全てのユースケースで認証の要件を考えると、政府または軍事アプリケーションでの QKD の使用は推奨しない方針である。NSA の指摘と同様に、QKD プロトコルは、初期認証を考慮していないため、物理的な中間者攻撃に対して脆弱である。この攻撃方法は、盗聴者が送信者と受信者間の間に入り、送信者―盗聴者、盗聴者―受信者のそれぞれで偽の鍵を共有させる。送信者と受信者は互いの通信を疑う術はないので、通信する相手を信じて通信を開始する。盗聴者は、成りすましによる盗聴行為が可能になる。この成りすましを回避するためには、QKD の実行前に送受信者間での確実な認証が必須である。
→米国と同様に NCSC が推奨する量子コンピュータの脅威に対する最善の緩和策は、PQC であるとしている。
https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

③ フランス（ANSSI：Agence nationale de la sécurité des systèmes d ‘information） 2020/5/4
QKD は、現在および将来の脅威に対する必須のソリューションではないとしている。理論的には数学的攻撃に対しては安全だが、実際のハードウェアを理論通りに実装することは不可能であり、安全を達成することはできないと指摘しおり、攻撃者により QKD デバイスが異常な動作をする可能性がある(なりすましなど)と言及している。
QKD は、現在の実装によるサービスを展開する上で、技術的に大きな制約がある。また、QKD を共通鍵暗号（既存の数理暗号：AES 等）の鍵配送に使用方式は、情報理論的安全ではない（数理暗号の計算量的安全性）。情報理論的安全なのは OTP（One Time Pad）を実現したときだけであり、暗号伝送速度は QKD の鍵配

送速度で律速されるため非常に遅く、伝送距離も短く適用できるアプリケーションは非常に限定的になる。長距離化のための縦列接続（中継）型の QKD による通信では、中継施設の条件によりシステムの安全性保証が損なわれ、膨大な投資が必要になる（各国と同様の指摘）。

④ ドイツ（BSI：Bundesamt für Sicherheit in der Informationstechnik）

ドイツにおいては、BSI（連邦 IT セキュリティ局）が QKD 利用におけるガイドラインを出しており、他国のように切り捨てるのではなく、QKD の不完全さ、脆弱性を理解した上での利用について正しく詳細に説明し、その可能性とリスクについて言及している。

https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-MeldungenNews/Meldungen/Leitfaden_quantensichere_Kryptografie_211216.html

⑤ オーストラリア（Australian Army）

オーストラリア陸軍においては、2021 年 9 月に「Army Quantum Technology Roadmap」の中で、「量子通信と暗号」のセクションの中で「オーストラリア陸軍にとって量子鍵配送（QKD）の価値を認めていない。これは、QKD 自体が十分に安全である可能性が低いからであり、更に、より簡単に統合できる PQC が出現したためである。」としている。また「利用の可能性ある QKD 対応ネットワークとしては、技術的な制約とその脆弱性により、少数のリンクに限定されるだろうと結論付けている。

https://researchcentre.army.gov.au/sites/default/files/RD5734_Quantum%20Roadmap%20WEB.pdf

第７節　QRC と量子暗号（QNSC）

表 5-5 は、ISO（International Organization for Standardization：国際標準化機構）の OSI（Open Systems Interconnection）参照モデル（現在のネットワークをその機能ごとに階層化しまとめたもの）の各ネットワーク階層に対応した脅威やセキュリティ技術を纏めたものである。ここからわかるように、各層ごとに様々なセキュリティ技術が構築されているが、物理層においては、本質的に伝送路等のインフラアクセスに対する盗聴を想定したセキュリティ技術はない。現在の情報通信においては、物理層を直接守ることはできず、上位のレイヤかもしくは、伝送直前で、データに暗号化（数学的複雑性で計算量的安全を根拠とする現代暗号）をした暗号データを流すだけである。

表 5-5 国際標準化機構（ISO）の OSI 参照モデルにおける各階層のセキュリティ技術の考え方

階層	層名	定義	プロトコル例	セキュリティの脅威	ソリューション
L1	アプリケーション層	アプリケーション、サービス	HTTP、FTP、電子メール	Static Password, SNMP Private Community Strings	Anti Virus software, OS Hardening, Patching
L2	プレゼンテーション層	データの表現形式	文字コード、圧縮	Viruses, Worm	Intrusion Detection, Auditing
L3	セッション層	接続制御と管理	TLS	Personal Information Retrieval, Root Privilege Access, Net Bios, DOS	Patches, Encryption, Authentication
L4	トランスポート層	データ通信の制御	TCP/IP、UDP	Endpoint Identity	Firewall access control list
L5	ネットワーク層	アドレス管理とルーティング	IPv4、IPv6	Preventing unauthorised access to internal system	VPN network based intrusion detection and content filtering
L6	データリンク層	通信区間のデータ送受信	Ethernet、Wi-Fi	ARP spoof, MAC Flooding	Private VLANs, Static ARP (address resolution protocol) entries, STP (Spanning Tree Protocol) root priority
L7	物理層	電気尊号、無線信号	有線ケーブル、無線	Inadequate Power, Unfettered access, Open wall ports	Managed Power through UPS, Restricted Access, Close down open wall ports

出展：International Journal of Electrical Electronics & Computer Science Engineering Special Issue - TeLMISR 2015, ISSN : 2348-2273

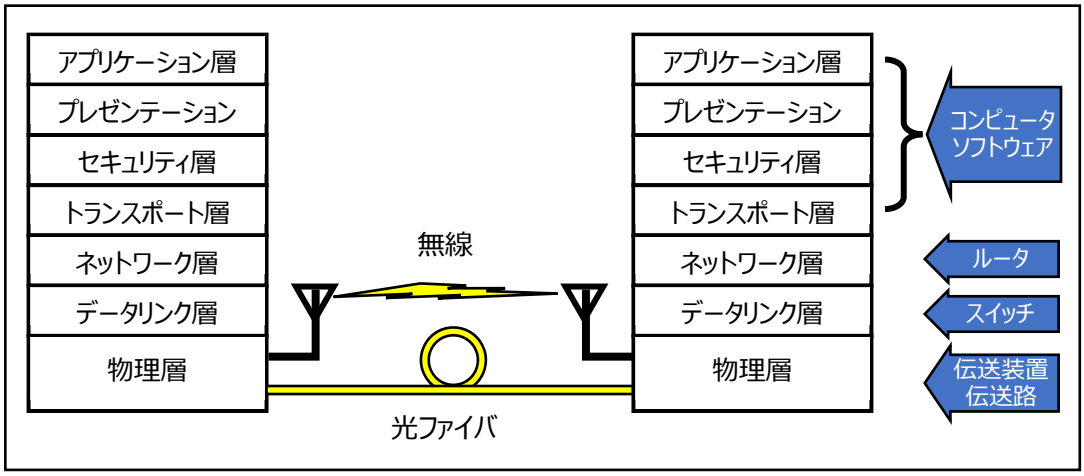

図 5-13　ネットワーク階層の構成イメージ

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。

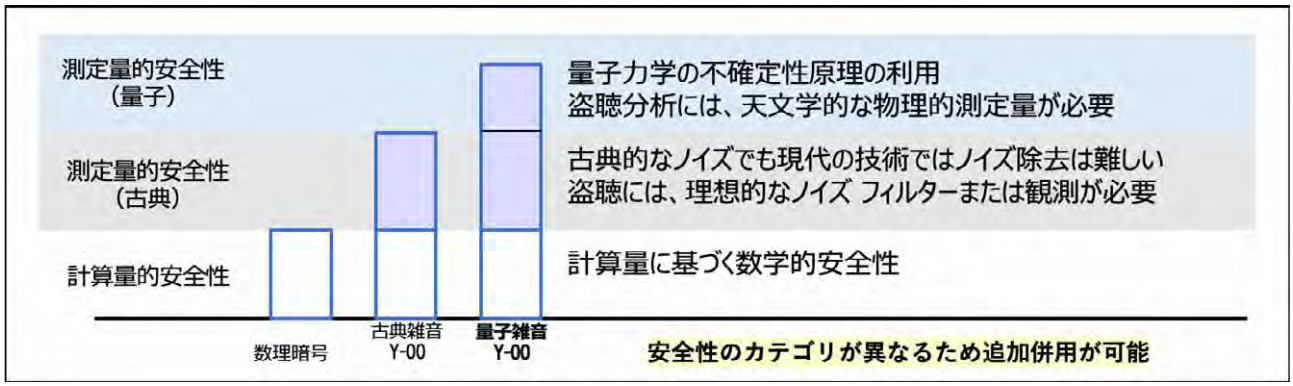

図 5-14　測定量的安全性の位置付け

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）。

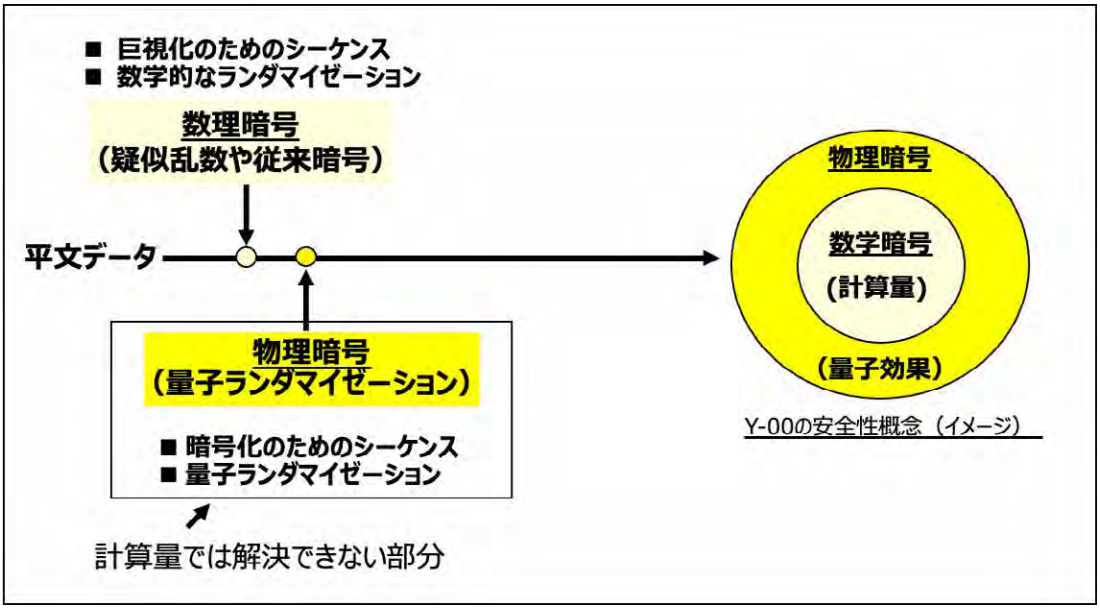

図 5-15　Y-00 プロトコルの仕組

「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。

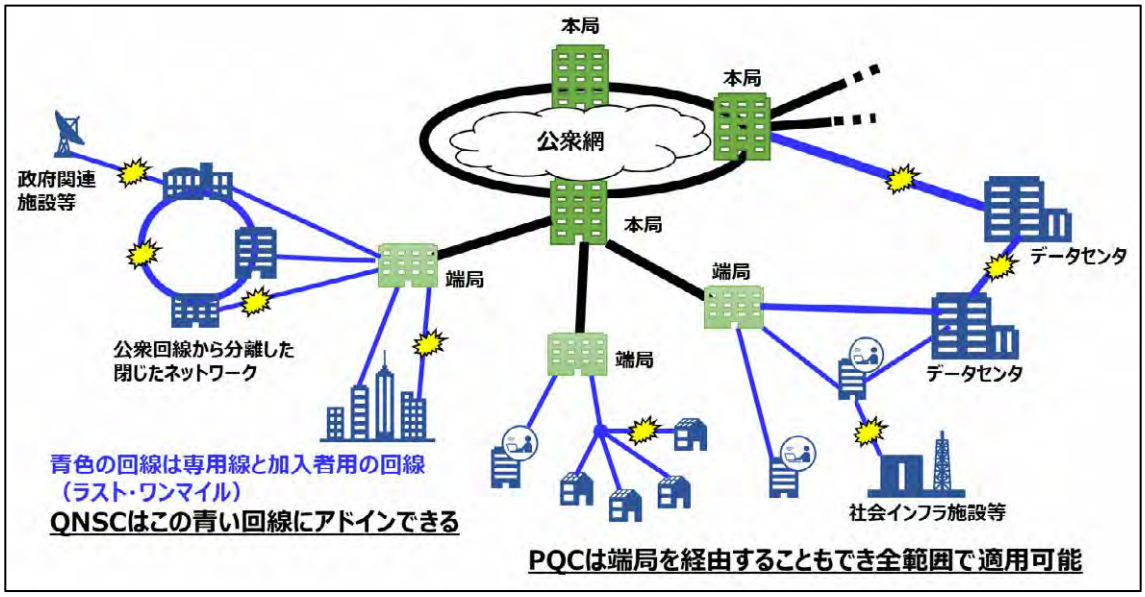

図 5-16　ネットワーク構成の例

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

学に基づく通信技術を総称していうことが多く、現在、定義はあいまいである。いずれにしても量子力学の持つ「不確定性原理」「粒子性と波動性」、「量子もつれ（エンタングルメント）」、「量子不確定性原理」などを利用する新たな通信方式として取り上げられることが多い。その中でも特に最近では、「量子もつれ」を利用する量子テレポーテーションが実用化に向け盛んに研究されている。この量子通信では、2 つの距離の離れた光子が、瞬時に情報（状態）を伝達するような相関関係を持っている。この量子もつれを形成する光源には特殊な結晶やレーザーが必要になる。またこの様な量子もつれを持つ光子対の生成や検出を高速に行うことは現在の技術では非常に難しい。

【量子通信の基本】

基本的な量子通信には、単純に光子単位に、光の偏光状態を符号化に利用する直接的な伝送（図 5-17(a)）と、送受信者間で「量子もつれ」状態の「光子対」を利用して通信を行う方式（図 5-17(b)）が報告されている。前者の直接的な伝送は、単純に光子単位に、光子の 2 つ（縦、横）の偏光状態に「0」、「1」の情報を符号化し、光子伝送を行う方式である。この方式を利用し、日本の NICT では、超小型低軌道衛星に搭載可能な小型光トランスポンダ （Small Optical TrAnsponder：SOTA）から 10Mbps で光地上局（東京都小金井市）との間でダウンリンク通信を実証している。この通信は、QKD で行っている単一光子伝送と同様であるため、前述の様に「量子通信＝量子暗号」と混同されている場合もある。この単一光子伝送を利用した量子通信は、OKD の課題と同様に、平均送信エネルギーが光子 1 個のエネルギー以下の微弱な通信となるため、伝送路の損失で、伝送途中で光子が消滅するため、大容量伝送や長距離伝送への対応は、非常に厳しい。

https://www.nict.go.jp/press/2017/07/11-1.html

次に、後者の量子もつれを利用した量子通信について説明する。量子もつれとは、２つの粒子（光子）が強い相互関係にある状態であり、光子のスピン、運動量などの状態を様に不確定な状態（量子重ね合わせ状態）のまま相関を持たせることができる。この相関をもつ量子もつれ状態の 2 つの光子は、光子間の距離に依存することなく、一方の状態を観測し状態を決定すると、もう一方の光子の状態も瞬時に決定される。例えば、一方の光子を観測したときのスピンが上向きであれば、もう一方は瞬時に下向きになる。このスピンの上向きを「０」とし下向きを「１」と定義しておけば、どんなに距離が離れていようが（例えば宇宙の端から端までも）、一方の光子を「０」と観測できれば、もう一方の光子は瞬時に「１」と決定するので、送信者から受信者へビットの反転状態で情報の伝達（通信）が成立する。量子通信としては、この量子もつれを利用する方式が一般的である。ただし、この方式も前述の単一光子伝送を利用する場合があるので混同しやすい。

この量子通信で利用する量子もつれ状態の光子対は、レーザー光を非線形光学素子に入射し生成する自発パラメトリックダウンコンバージョンという技術を利用している。この技術は、KTP 非線形結晶（PPKTP：周期分極反転構造を持った、KTP 結晶（Periodically poled KTiOPO4）等）に強いレーザー光（ポンプ光）を入射することで１対の量子もつれ光を生成する。中国の実験室では 15mW のポンプ光で、毎秒約 240 万（2.4M 個/sec）のもつれ光子ペアを生成できると報告している。

https://academic.oup.com/nsr/article/7/5/921/5695761?login=false

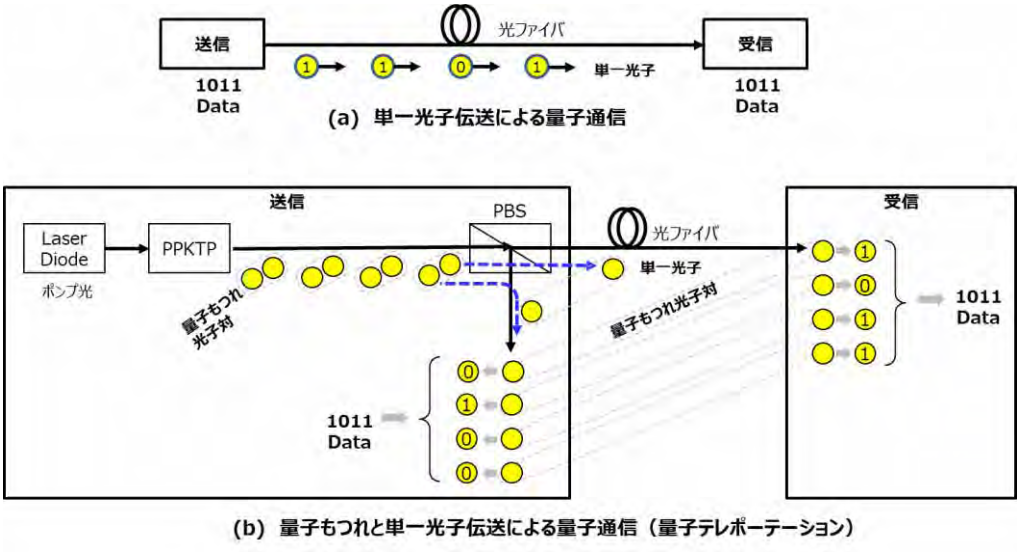

図 5-17　量子通信の概要

このような通信を行う場合は、前述の様に予め量子もつれ状態の光子対を大量に送受信間に配置しておく必要がある。なおかつこれらの光子は、量子重ね合わせ状態を保ったまま量子メモリに保存しておき、通信を行うときは、それぞれの拠点で保存してある光子対の光子同士を利用する。送信側で光子対の一方の光子を符号化すると、受信側の対になる光子は瞬時に反転した符号に決定される。この量子相関を利用し、伝送媒体を介すことなく情報が瞬時に伝達できる（この原理については、現在まだ解明されていない）。また、この現象は送受信間の距離に依存することはないため、この現象は「量子テレポーテーション」と呼ばれている。

【量子通信の課題】

ここで上記のような量子通信を行うために大きな課題となるのが、量子通信に使う大量の光子対のそれぞれの光子を送信者と受信者に予め分配することと、それぞれに配置された光子を、通信を行うタイミングまで量子もつれ状態を保ったまま保存しておく量子メモリが必要となる。現在いくつかの方式で量子メモリの研究が行われているが、現在のコンピュータや情報通信で利用されているような手軽に扱える大容量メモリは実現できていない。

また、図 5-17（b）の様に、光子対の一方の光子を受信者に伝送しながら、リアルタイムに通信を行う方法もあるが、この場合は、単一光子伝送と同様の課題として、伝送速度や伝送距離に制限ができてしまう。このため、量子状態を維持したまま中継伝送を可能にする量子中継技術が必要になる。遠く離れた拠点間の環境で量子もつれを作ることはできないので、量子通信自体が距離に依存しなくとも、どこかの拠点で作った量子もつれ状態の光子対を量子通信が行なわれるそれぞれの拠点に配送（配置）しなければならない。QKD で行われているような光子伝送では、距離に限界があり、また、QKD で使われるトラステッドノード（信頼できる中継拠点での縦続接続中継）を利用する中継では、量子状態を中継することはできない。しかし、量子インターネットによって、量子コンピュータを接続することにより、量子ビットの並列化によって、量子

コンピュータの計算能力は指数的に強化できる。現在のコンピュータ以上に、量子コンピュータの分散化は大きなメリットをもたらすことがかのうである。現時点での量子通信は、長距離伝送への課題が大きいが、データセンター内に隣接する量子コンピュータ同士を量子通信で接続し、計算能力を向上させることは現実的なアプリケーションと考えられる。米国の量子通信への積極的な取り組みは、この様な背景があるからだと考えられる。

量子中継：Etanglement Swapping (ES)

現在、実用的な量子状態を維持したまま中継できる中継器は実用化されていない。QKD 伝送においては、トラステッドノード技術では、量子状態を保つことはできず、最初の中継拠点で古典化された鍵データを後段からは、One Time Pad で伝送していくので、この技術をそのまま適用することはできない。

（応用原理）

２組の量子もつれ光子対源から別々に発生した二つの光子対から、それぞれ光子を １個ずつ選び出し、その間に量子相関測定（ベルステートアナライザ：ベル測定）を行う。すると，もともとは相関を持たなかった残りの二つの光子は、測定結果に依存した量子もつれ状態になる。この原理を応用すると、量子もつれ光子対源を通信路中に多数配置し、それらのもつれ光子対間で量子相関測定をおこなうことで、量子中継を利用した長距離間の２拠点間で、量子もつれ合いを共有することが可能になる。図 5-18 に量子中継の仕組みの概略を示す。

・送信拠点で量子もつれ状態の光子対を生成し、一方を量子メモリに格納し、もう一方を光ファイバで
　中継拠点にロスせずに送る。
・受け取られた光子は、量子メモリ内の量子ビット同士のエンタングルにする。
　ここまでを、異なるノード（中継拠点にとっての送信拠点と受信拠点）を相手におこなう。
・ES を実行する。
・古典通信網を利用して光子の受信確認や、ES の実行結果のフィードバックを共有する。

今は、要素技術が出来上がってきた、という段階である。

量子メモリ

最近の量子メモリで有望視されているのが、「ダイヤモンド NV センター」という物質を活用する方法である。ダイヤモンド NV センターは、ダイヤモンド中の複数の炭素（C）を窒素（N）に置換した物質である。N は C よりも他の原子と結合する腕の数（原子価）が 1 本少ないため、ダイヤモンド内に空孔（V）が生じ、電子が集まる。集まった電子や炭素の同位体の核子は、量子状態を長時間（とはいえ最大 20msec 程度）保持できるため、量子メモリとして扱える。半導体の量子メモリは、数ナノ秒程度しか量子状態を保持できないが、ダイヤモンド NV センターの特徴は、数秒から数分という長時間にわたって量子状態を保持できるメリットがあるという。また他の一般的な量子メモリだと動作時に冷却が必要だがダイヤモンド NV センターは、室温でも動作できるという利点もある。現在の量子メモリは、電子の量子状態を蓄積することができるが、光子を蓄積することはできないので電子から光子、光子から電子への変換も必要となる。

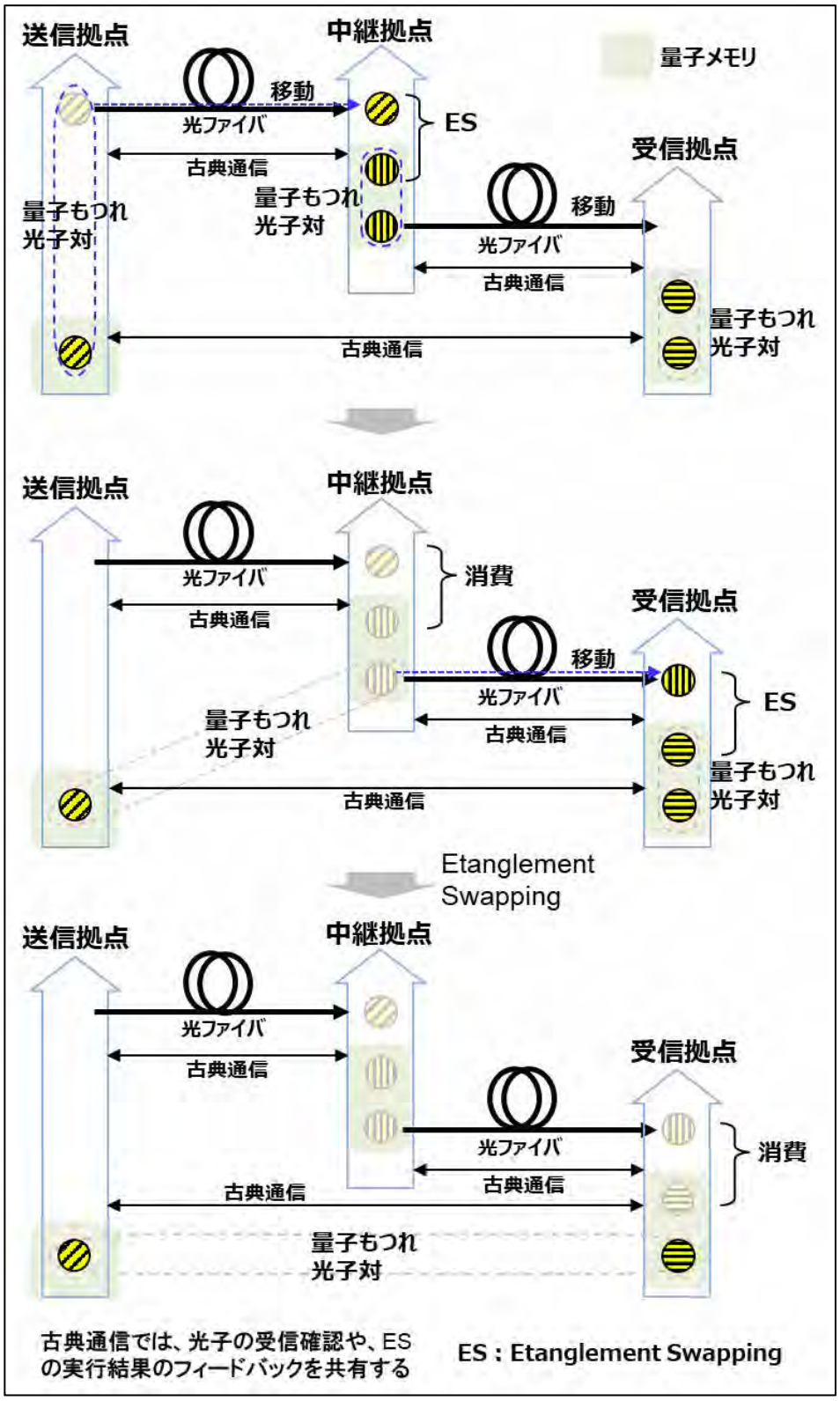
送信拠点
中継拠点
量子メモリ
移動
光ファイバ
ES
古典通信
受信拠点
量子もつれ
光子対
移動
光ファイバ
古典通信
量子もつれ
光子対
古典通信
送信拠点
中継拠点
光ファイバ
消費
古典通信
受信拠点
移動
光ファイバ
古典通信
ES
量子もつれ
光子対
量子もつれ
光子対
古典通信
Etanglement
Swapping
送信拠点
中継拠点
光ファイバ
古典通信
受信拠点
光ファイバ
古典通信
消費
古典通信
量子もつれ
光子対
古典通信では、光子の受信確認や、ES
の実行結果のフィードバックを共有する
ES：Etanglement Swapping

図 5-18　量子中継の例

以上のように量子通信における課題は、まだまだ大きい。効率の良い量子もつれ光源、量子中継、量子メモリおよび光子配送などの課題を現在のネットワーク環境に当てはめて考えると、技術的なハードルは非常に高い。例えば、量子通信の場合、距離が離れた拠点間に量子もつれ状態の光子（または電子）をそれぞれ配置させておく必要はある。この配置は、量子メモリに蓄え配送するか、光子伝送配送するかである。しかもこの配送は全ての処理を 20msec 以内に終わらせなければならない。拠点間の距離に依存することなく瞬時に情報を送ることができるとしても光子配送で環境条件がきまる。また、量子通信では、QKD と同様に、伝送した光子ごとに光子の伝送状態の確認を古典伝送路で行うので、この古典通信で利用できる条件が決定する。どんなに量子テレポーテーションが遠距離で瞬時に情報を伝達できたとしても、光子を伝送の限界で通信条件は決まってしまう。

しかし、データセンター内などの限られた空間であれば、伝送距離が短いので量子コンピュータ同士の通信は現代技術の範囲で実現できる領域だと考えられる。

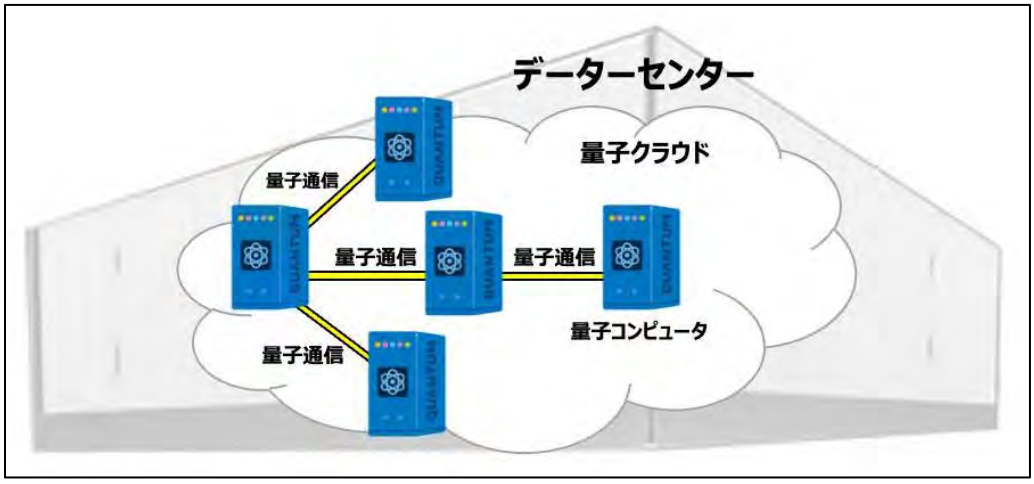

図 5-19　量子通信による量子コンピュータの分散連携

・中国の衛星を利用した量子通信の現状

中国は、「墨子号」衛星を利用した量子通信ネットワークの研究開発を実施している。墨子号は高感度光子受信機を搭載しており、地上から発信された単一光子の量子状態を検出できる。このシステムを利用し、量子もつれ、暗号、テレポーテーションなど、量子を用いたさまざまなアプリケーションの実現に向けた技術上の基礎実験行っている。

2017 年 7 月に研究チームは史上初となる衛星と地上間の量子ネットワークを作成し、その過程で、最長の距離間で量子もつれを測定し、さらに地上から軌道上に初めて光子をテレポートに成功した。長距離テレポーテーションは、大規模な量子ネットワークや分散型量子計算などのプロトコルにおける基本要素として認識されていると中国の研究チームは考えている。

量子もつれは壊れやすく、光子が大気中や光ファイバ内の物質と相互に作用することで、もつれの状態が失われる。その結果、科学者が量子もつれを利用したテレポーテーションの伝送距離は、最長でも 100km 程

度の距離に制限されていた。「墨子号」は、高度 500km の衛生軌道を利用しているため、光子は「墨子号」まで殆ど真空を通って移動するため伝送ロスが少ない。この光子伝送では、途中通過する大気の影響を最小限に抑えるため、地上局を、標高 4000m を超える場所（チベットのガリ地区）に設置した。従って、実際の地上から衛星までの距離は、衛星が地平線近くにある 1400km から、真上にある時の 500km である。

この実験では、地上で毎秒約 4000 対のペースで量子もつれ光子対を生成し、対になった光子のうち 1 つを、上空を通過する衛星に送り、もう片方の光子を地上留めた。この地上と軌道上の衛星の光子対を測定し、量子もつれを確認し、更にテレポートできることも確認した。実験は、32 日間にわたり、何百万個の光子を送り続け、911 対の光子において良好な結果が得られた。

https://arxiv.org/abs/1707.00934（arxiv.org/abs/1707.00934：” Ground-to-satellite quantum teleportation"

第９節 量子技術を利用したネットワークシステム構成と提案

量子コンピュータを複数台相互接続すると計算能力は指数的に向上する。このため量子コンピュータの相互接続を可能にする新たなネットワークインフラストラクチャが必要になる。「量子インターネット」は、現行インターネットとまったく異なるネットワークであり、新たなプロトコルと量子中継器や量子メモリが必要になる。「0」、「1」の確定された情報を光子の偏波や位相を利用して単一光子伝送を行う通信とは異なり、量子重ね合わせ状態の（「０」、「１」の確定されていない状態）を保ったまま伝送をおこなう。この伝送を量子コンピュータ間の通信に利用する情報通信基盤が「量子インターネット」である。内閣府が 2020 年 1 月に公表した「量子技術イノベーション戦略　最終報告」によると、部分的な実用化時期は早くても 2030 年ごろ。現段階ではシステムに必要とされる個々の要素技術を研究開発している段階だ。

量子コンピュータは、複数台を接続して同時に計算することで、演算処理能力を向上することができる。現在のスーパーコンピュータにもこのような並列処理機能が存在するが、「量子コンピュータの場合、重ね合わせの原理によって指数的に計算能力を上げられる。

ただし、現行インターネットが将来全面的に量子インターネットへ刷新することは考えにくい。量子コンピュータが実用化しても、従来型（古典）コンピュータは依然として必要となる。これはそれぞれが得意の計算処理の分野が異なるからであり、現行インターネットと量子インターネット専用の情報通信基盤を、併用していく必要がある。

米国では、近距離拠点間のネットワークを構築し実験を重ねている。量子通信技術に関する U.S. National Quantum Initiative（米国国家量子イニシアティブ）の目標に沿って、フェルミ国立加速器研究所 (Fermilab) が率いる Illinois-Express Quantum Network (IEQNET) は、シカゴ大都市圏での中継器を利用しない光量子ネットワーク設計の開発と動作の実証を行いる。

EQNET は、2 つの DOE（United States Department of Energy：アメリカ合衆国エネルギー省） 国立研究所 (Fermilab と Argonne) の研究者と、ノースウェスタン大学と カリフォルニア工科大学 (Caltech)、ベンチャー企業 (NuCrypt、HyperLight)、および INQNET AT&T/Caltech コンソーシアムの学術研究者を集めている。 INQNET コンソーシアムは、SRI インターナショナルが率いる国立標準技術研究所量子経済開

発コンソーシアム（QED-C）にリンクされている。

IEQNET ネットワークには、既存の Fermilab Quantum Network（FQNET）ノードと、ノースウェスタン大学 （エバンストンとダウンタウン シカゴの医科大学キャンパスの両方） に提案されている大学キャンパス ノード、およびアルゴンヌのノードが含まれる。 このプロジェクトは、既存の従来のネットワーク インフラストラクチャ（Starlight）と、ローレンス バークレー国立研究所が管理する、世界中の DOE の科学者とその協力者にサービスを提供するエネルギー科学の高速コンピュータ ネットワークである ESnet（Energy Sciences Network） の経験を活用している。

IEQNET 量子ネットワークは、同じ光ファイバ伝送システムで従来のネットワークと共存し、IEQNET の外部で開発された新しいコンポーネント （メモリ、リピータ） を技術の成熟に合わせて柔軟に組み込むように設計されている。このように米国では、すでに実用化できるところから実用し始め、研究開発を進めながら実用化研究および将来に向けたデバイス研究を進めている。

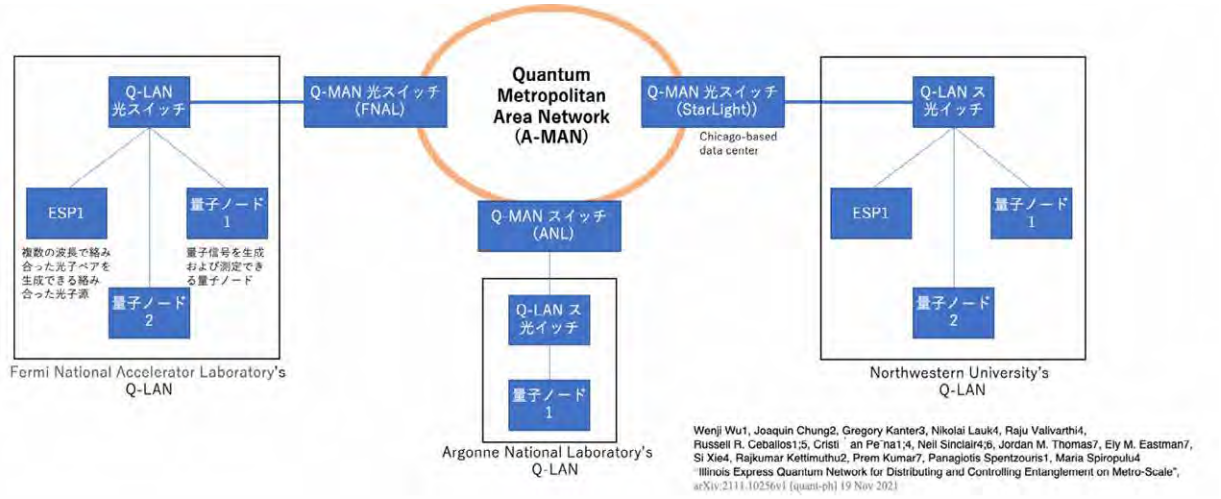

図 5-20　IEQNET metropolitan testbed

IEQNET の主な機能。

- マルチノードの柔軟で回復力のあるネットワーク構成をサポート
- マルチユーザーをサポート
- 同じ光ファイバ伝送システムで従来のネットワークと共存し、DWDM ネットワーク コンポーネントを共有可能
- 階層化されたアーキテクチャと集中管理を採用

https://ieqnet.fnal.gov

第１０節 まとめ

・セキュアネットワークの構成

現在の量子技術開発の状況を考え、耐量子コンピュータの安全性を担保できる将来の量子インターネットにつながる様なセキュアネットワーク構築が必要である。また、この対策の実施は量子コンピュータの開発状況や各国の研究投資やウクライナ戦争の情報戦の実情等も考慮すると、今すぐにでもできるところから対処していく必要があると考える。

図 5-21 に耐量子コンピュータを考慮した暗号技術の構成について纏めたものである。

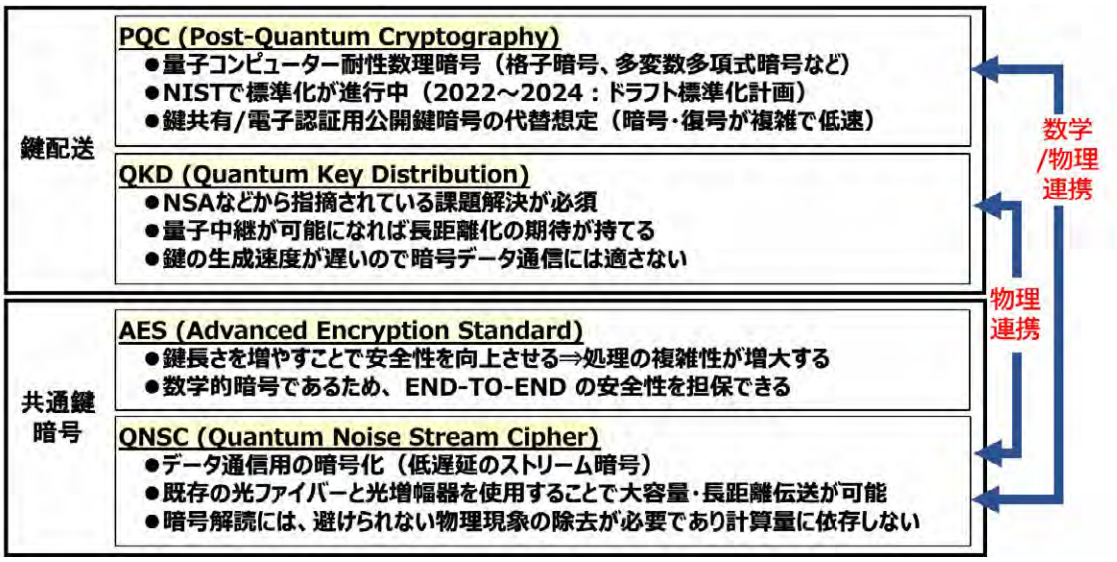

図 5-21　ニーズに合わせた新たなセキュリティ連携

暗号化を行う共通鍵暗号系としては、AES の鍵長を増やして複雑性を向上させる手法も考えられるが、前述の様に米国では、すでに AES を継続して利用することに対して懸念をいだいており、耐量子コンピュータに対して恒久的な効果が期待できる物理暗号系の QNSC の開発と実装が急務と考えられる。また、共通暗号系（鍵配送）においては、QKD は米国、英国、仏国等が懸念している様に安全性を確実に担保し実装できるまでに課題が多く、まだまだ時間がかかる。まずは、PQC を利用し、実装していくことが懸命である。しかし、PQC においては日本国内での研究成果や実績は少なく、政府からの支援プロジェクトも少ない。また、現時点では、NIST の標準化結果からもわかるように格子系暗号に頼るしかないが、安全性を確保するためには、鍵の複雑性も確保する必要があり、早急に開発を強化する必要がある。量子通信や量子コンピュータを利用した量子インターネットや量子クラウドにおいても、量子デバイスだけに頼るのではなく、現代の古典技術と融合させるハイブリッド構成で早期実用化を進めることが重要である。そのためには現在利用されているインフラやデバイスを効率よく利用することも重要である。

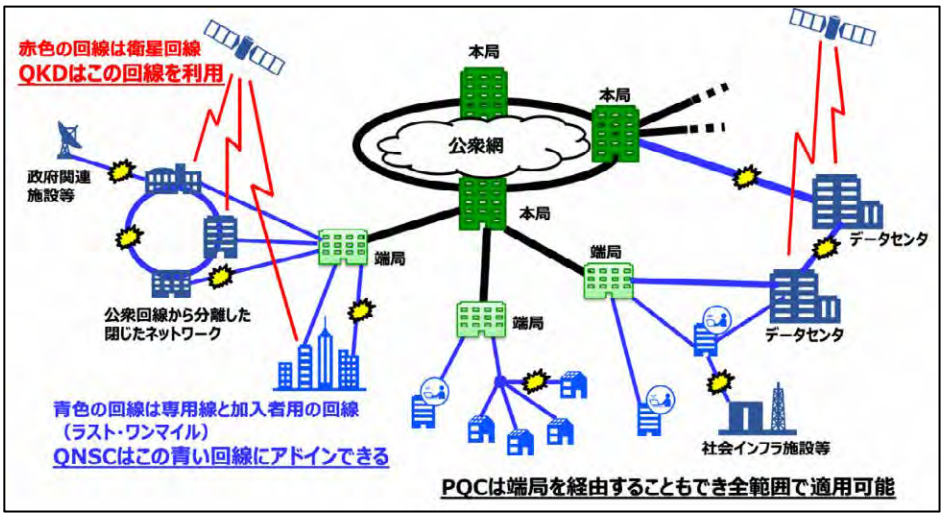

図 5-22　セキュアネットワークにおける通信の適用

図 5-22 は、現在のネットワークをベースにした耐量子コンピュータを考慮したセキュアネットワークにおける通信の適用を纏めたものである。この図の青い伝送路のところは、QNSC や PQC を利用することで、早急に実用化を進めることが可能である。まずは、できるところからセキュリティ対策を実施し、赤の折れ線で示す QKD や衛星を利用する量子通信においては時間をかけて将来的に導入をすることで、完全なセキュリティシステムに向け段階的に構築していくことが重要である。

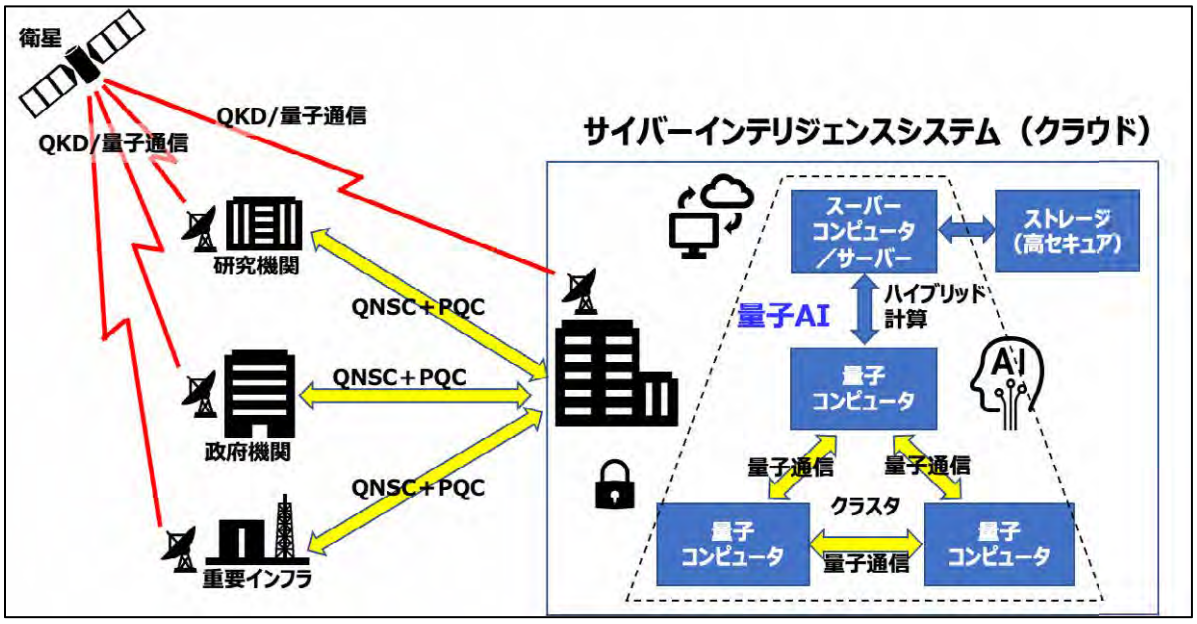

図 5-23　サイバーインテリジェンスシステム（クラウド）に向けた構想

量子通信が実現できると、量子コンピュータは高機能化のために量子ビット数を増やすだけではなく、量

子コンピュータ同士を量子通信で接続するクラスタ化が進み、更にスーパーコンピュータとも連携したハイブリッド利用による両システムの優位性を活かした効率の良い利用形態へと進化する。この場合においても現在のシンフラを効率よく利用し、すぐにでも対応できるところから実施し、検証や試用を進めていきながらシステムを進化させていくことが必要と考える（図 5-23）。

第６章 日本のサイバー能力強化のための提言

本章では、日本としてのサイバーインテリジェンスのめざす姿を述べる。サイバーインテリジェンスは、ひとつの国だけで達成することはもはや難しく、現時点で知られているもっとも強力サイバーインテリジェンスは、いわゆるファイブ・アイズ（米国、英国、カナダ、オーストラリア、ニュージーランド）を構成する国どうしで作られている。日本は、ファイブ・アイズへの仲間入りを果たすためには、日本において未整備の国家サイバーインテリジェンスシステムを可及的速やかに構築する必要がある。そうすれば、図 6-1-a に示すような、国家サイバーインテリジェンスのめざす姿であるシックス・アイズの実現に近づく。

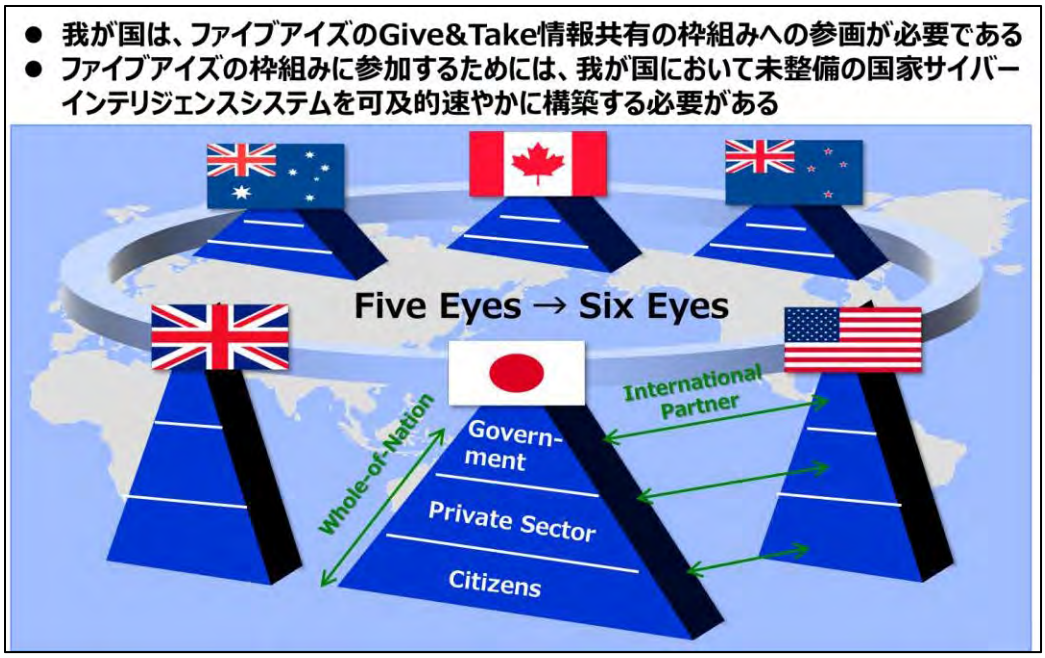

図 6-1-a ファイブ・アイズからシックス・アイズへ

サイバーインテリジェンスを確立するためには、図 6-1-b に示すような「データを守る」「人を守る」「システムを守る」という３つのアクションを、米国の整備状況の鑑み、推し進める必要がある。

「データ守る」には、クラシファイド／アンクラシファイド／アンクラシファイドではあるがコントロールすべき情報、といった機密情報の区分を進化させる。さらに Need to Know の原則の実現に向け、知るべき情報、知ってはならい情報を確実に分ける。このようなデータ区分の改訂を推し進める。

「人を守る」には、セキュリティクリアランスの制度を制定するとともに、当該制度にもとづくデジタルアイデンティティ基盤および ID 管理システムを進化させる。さらには情報を知るべき人、知ってはならない人を確実に分ける。このようなセキュリティクリアランスの制定を推し進める。

「システムを守る」には、サイバーインテリジェンスシステムを実現するための、政府クラウドを早期に確立する。そのために、政府クラウドの認定制度として、現状行われている ISMAP を改定し、FedRAMP 相当のクラウドセキュリティ認定制度を推し進める。さらに地政学を加味した冗長化やバックアップの機能を

備えたハイブリッドクラウドを推進する。

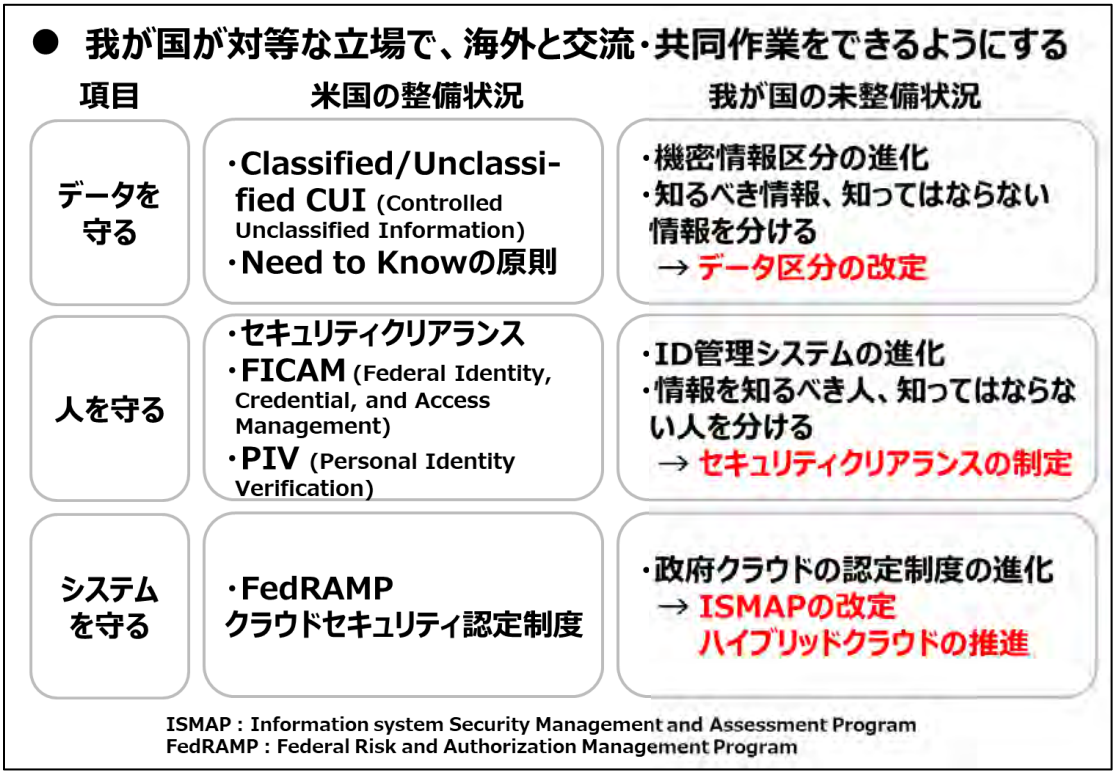

図 6-1-b 日本が取り組むべき内容

まとめとして、日本のサイバー能力強化のための重要提案 6 項目を述べる。

１．ウクライナ戦争においては、ハイブリッドの戦争が現実となった。有事のリスクも現実味を帯びてきた。日米同盟の最大の弱点はサイバーセキュリティである。日本の通信網や電力網がダウンすれば、戦闘が始まる前に在日米軍や自衛隊が敵対国の軍隊によって倒される可能性がある。

２．日本は、米国だけでなく、有事の同盟国となりうる英国やオーストラリアに追いつくために、多くの宿題をこなす必要がある。

(1) 官邸にサイバーセキュリティ司令官を設置し、自衛隊を含むスタッフを配置すること

(2) サイバー司令官のための法的権限を確立すること

　(a) サイバー状況認識、サイバースペースの監視

　(b) 物理的な国境を越えたサイバー攻撃者の特定

　(c) 物理的な境界を越えて持続的かつ反復的に行われる攻撃を阻止するアクティブ・ディフェンス

(3) 強固なファイアウォールを備えたガバメントクラウドを構築すること

(a)日本のインテリジェンスコミュニティのデジタル統合

(b)機密性の高いハイテク企業や防衛産業を政府のクラウドに取り込む

(c)AI を活用した効果的な検索エンジンにより、良質な情報報告書を作成する

(d)AI とスパコンを備えたサイバーインテリジェンスのための OSINT センタを設立する

(e)データフロー全体をスパコンに保存し、オープンソースのインテリジェンス分析を行う

(4)政府の Intelligence イントラネットを、場合によっては量子技術を用いた高度な暗号化で構築すること

(5)政府職員が外国人エージェントと癒着している可能性を精査するクリアランス制度を確立すること

(6)安全保障分野、インテリジェンス、産業、科学技術のシナジーを高めるために、量子サイバー研究センタを設立すること

(a)外国人の研究者にも門戸を開く

(b)十分な政府や民間のファンドが必要である