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

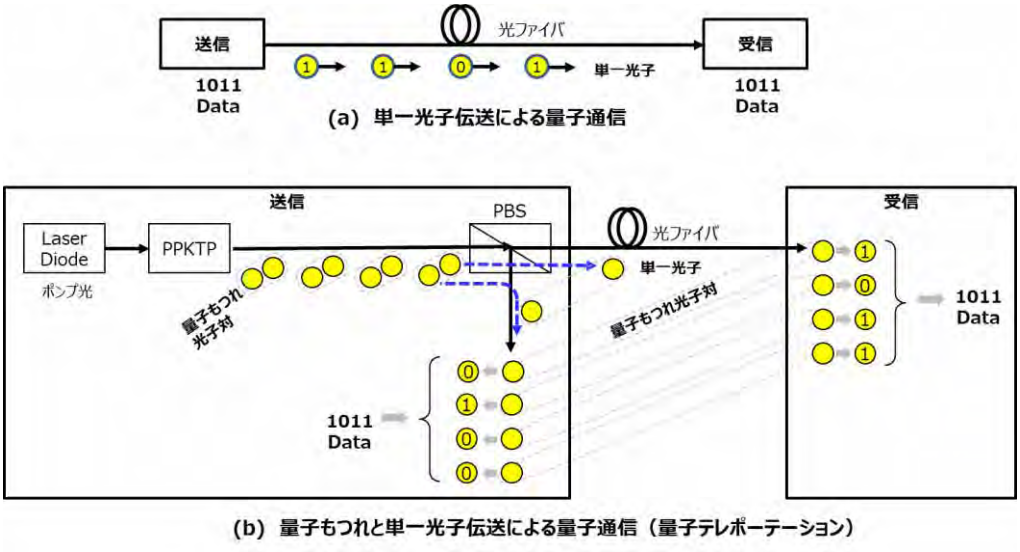

図 5-17　量子通信の概要

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。

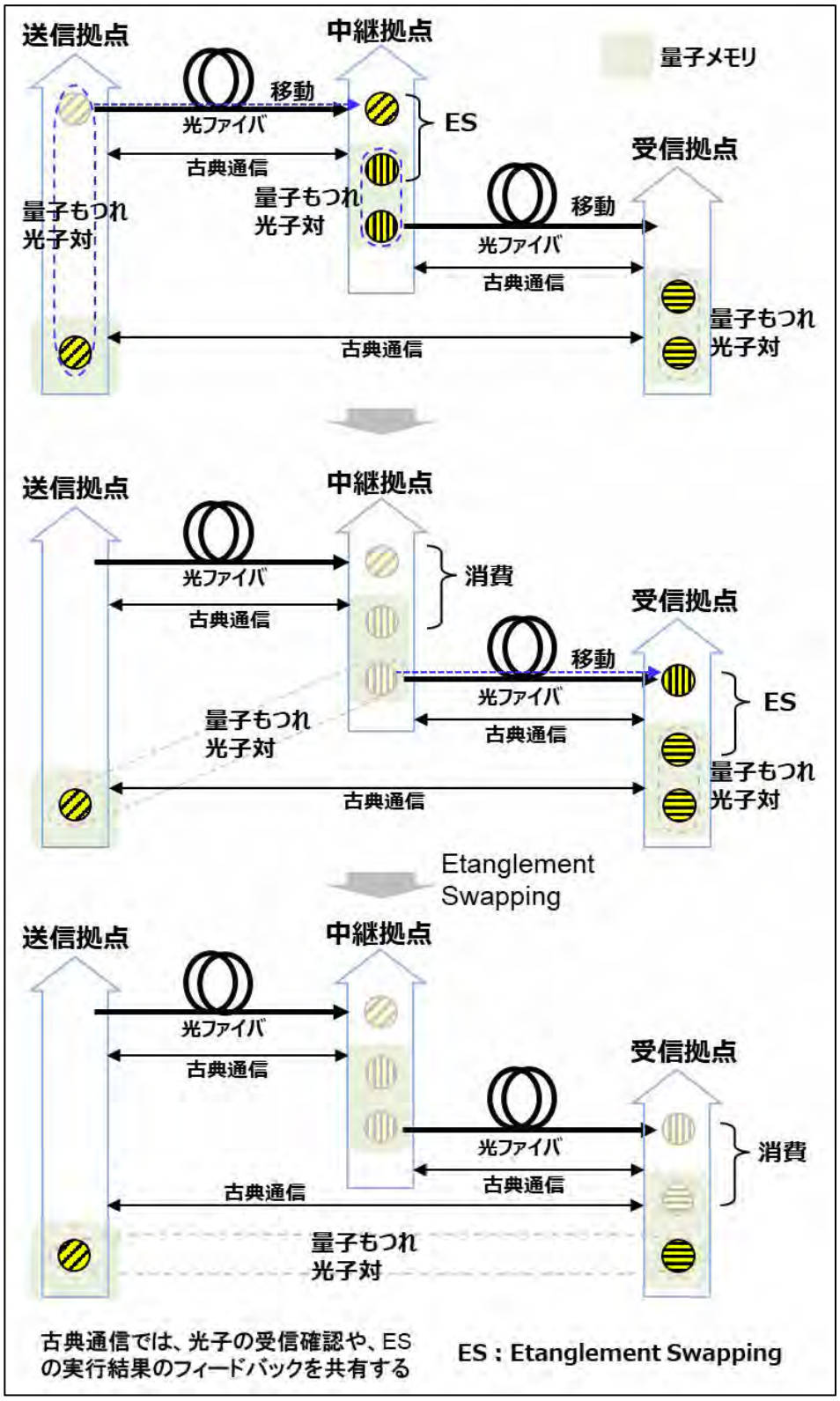
送信拠点
中継拠点
量子メモリ
移動
光ファイバ
ES
古典通信
受信拠点
量子もつれ
光子対
移動
光ファイバ
古典通信
量子もつれ
光子対
古典通信
送信拠点
中継拠点
光ファイバ
消費
古典通信
受信拠点
移動
光ファイバ
古典通信
ES
量子もつれ
光子対
量子もつれ
光子対
古典通信
Etanglement
Swapping
送信拠点
中継拠点
光ファイバ
古典通信
受信拠点
光ファイバ
古典通信
消費
古典通信
量子もつれ
光子対
古典通信では、光子の受信確認や、ES
の実行結果のフィードバックを共有する
ES：Etanglement Swapping

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。

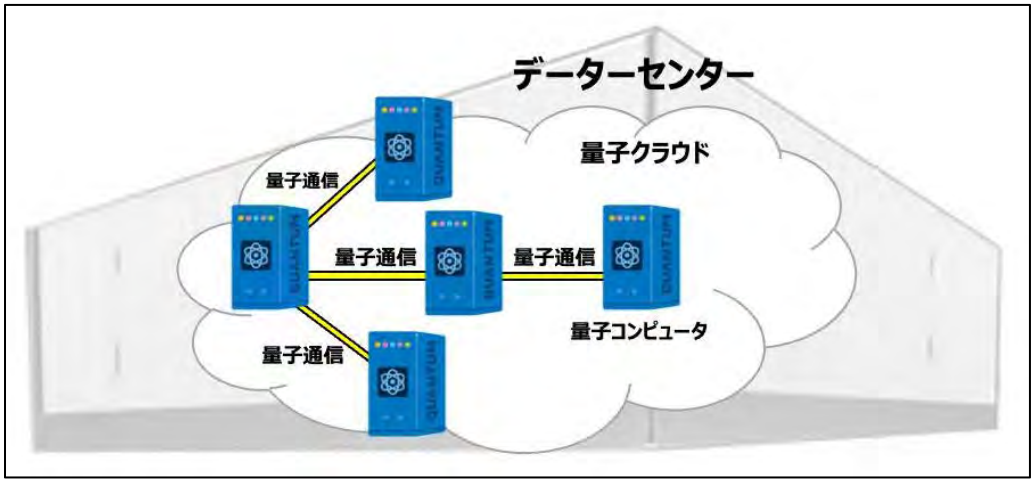

図 5-19　量子通信による量子コンピュータの分散連携

・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。

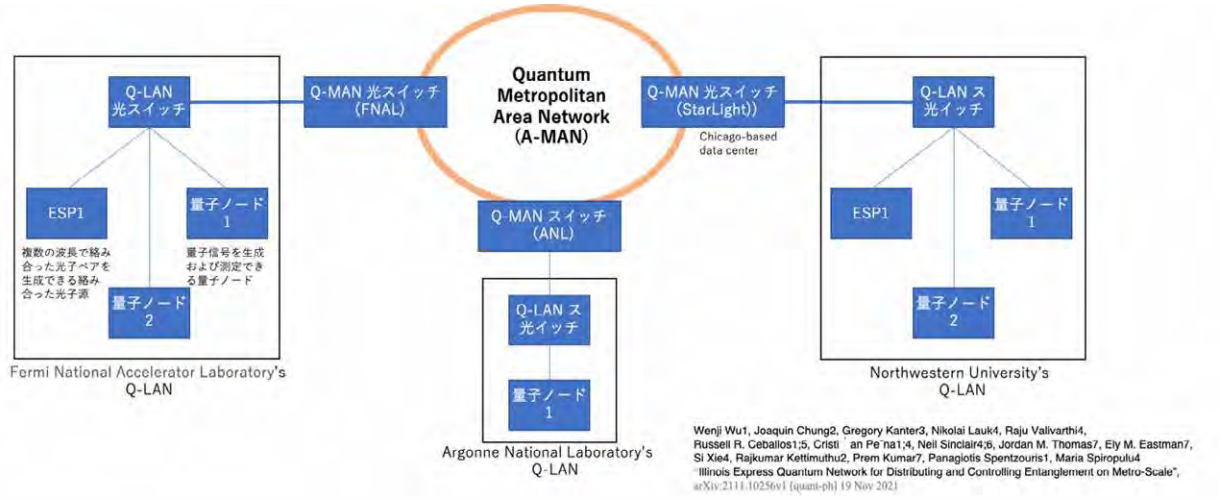

図 5-20　IEQNET metropolitan testbed

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。

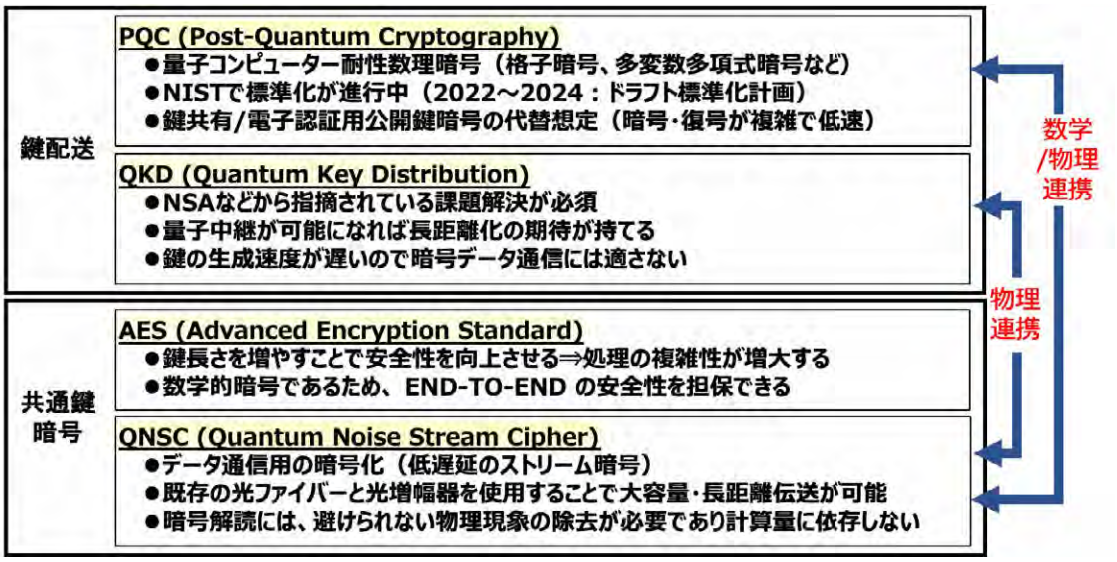

図 5-21　ニーズに合わせた新たなセキュリティ連携

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。

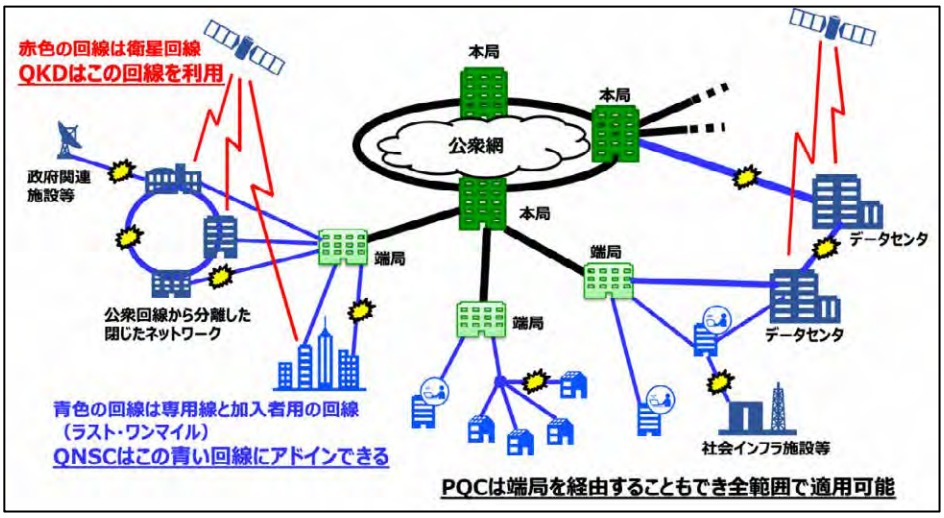

図 5-22　セキュアネットワークにおける通信の適用

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。

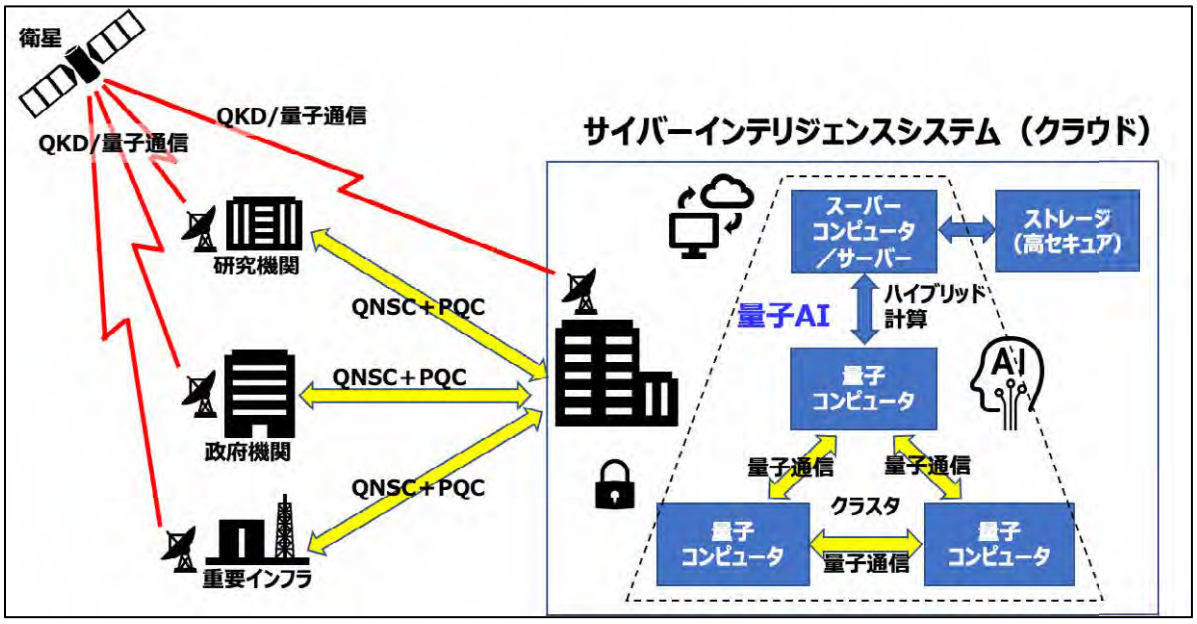

図 5-23　サイバーインテリジェンスシステム（クラウド）に向けた構想

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。

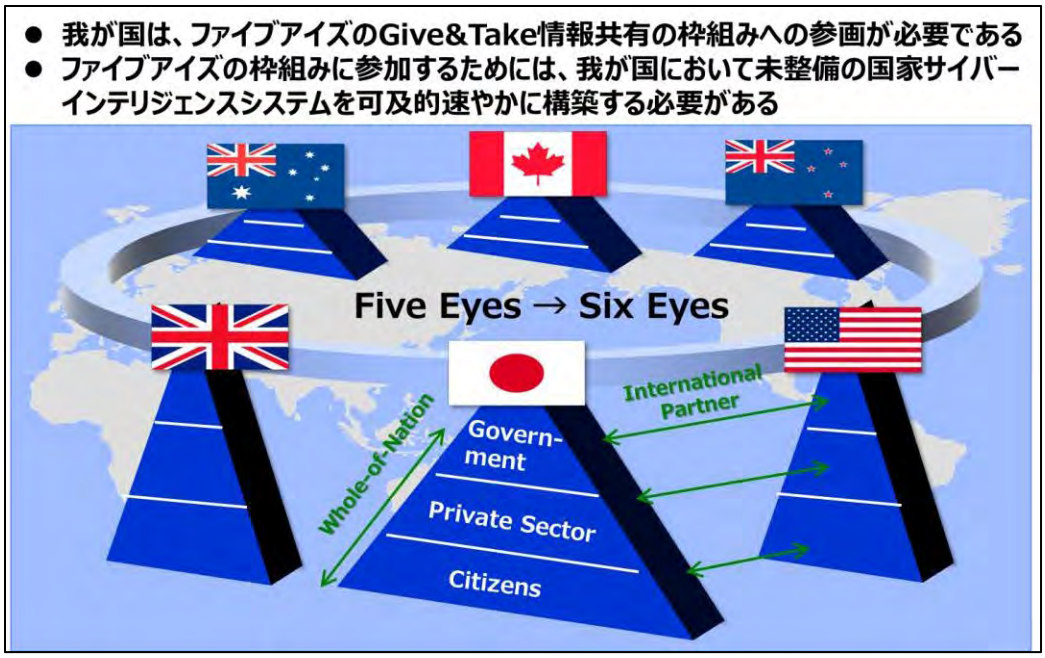

図 6-1-a ファイブ・アイズからシックス・アイズへ

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。

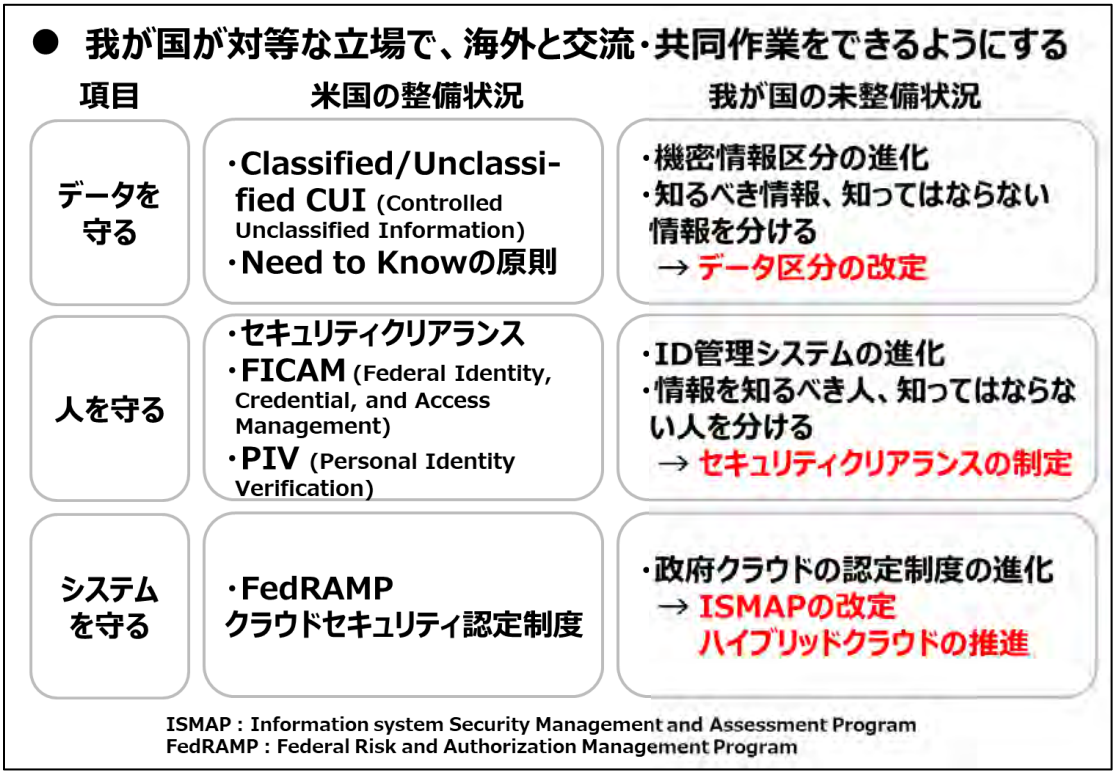

図 6-1-b 日本が取り組むべき内容

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