ホワイトペーパー

“The” 量子インターネット

-この宇宙の物理法則に許されるサイバー空間の極致-

産官学連携研究開発コンソーシアム
量子インターネットタスクフォース

QUANTUM INTERNET
TASK FORCE

https://qitf.org/

version 1.1
2021 年 2 月 22 日

概 要

現在世界中で、量子コンピュータや量子センサーといった様々な量子技術の研究開発が加速的に進められている。これらの量子技術は、21 世紀に期待される技術革新の中でも、その規模や影響、革新性において、もっとも重要な技術革新のひとつと考えられている。量子技術革新は、半導体産業や光産業を生んだ第 1 次量子革命と対比させ、第 2 次量子革命とも言われ、その先には多数の量子コンピュータが繋がり、互いに「量子データ」をやりとりする世界が想定されている。そこでは、「量子インターネット」が量子データを伝送するための基盤を担う。量子インターネットは本格的な量子技術時代のコンピュータネットワーク基盤である。

デジタルデータ[1][2]の汎用通信基盤である現行インターネットは、その基盤上で多種多様なサービスやアプリケーションが展開されるようになり、人類になくてはならないインフラに成長した。現代では、インターネット上のサイバー空間を活動の基本とし、フィジカル空間での関係や制限を前提としない社会活動を展開する準備すら整ってきている。未来に目を向けると、SDGs や Society 5.0・知識集約型産業などの実現に向けて、データの自由な流通や高速処理といった、インターネットへの社会的要求と期待はさらに大きくなることが予想されている。一方で、インターネットの急速な発展は、様々な課題も同時に生んできた。セキュリティやプライバシー、デジタル・デバイド、寡占企業によるデータ独占、データセンターのエネルギー消費量など、現在のインターネットが抱える問題は、これからもさらに深刻さを増していくであろう。これらの問題は、技術的側面のみならず、社会的側面や法的側面、制度上の問題など様々な側面が複雑に絡み合っており、短期的な解決策を見出すことが必ずしも得策でなく、直近で問題が重篤化しないように対応しつつ、中長期的な視点での完全解決へ向けた指針を模索していくことが重要である。様々な視点から示される解決指針の中でも、「科学技術による解決」は特に重要な方向性であろう。新しい科学技術は、技術的課題の解決のみならず、社会が抱える様々な課題の解決を実装する手段を提供し、人類が目指す近未来社会の実現へ向けた大きな柱のひとつであることは間違いない。

現在においては、このような発展と課題解決の担い手となるべく次世代通信技術基盤の研究が進められている。この次世代通信技術研究開発には、Beyond 5G や IOWN、量子鍵配送ネットワークなどと並び、量子インターネットが挙げられている。量子インターネットを除くすべての次世代通信技術は、デジタルデータを伝送するためのものであるが、量子インターネットは量子データをやり取りするための技術であり、その点で、量子インターネットはこれらの技術と抜本的に異なっているということができる。通信基盤が担うデータの種類が技術を本質的に分けるのには、通信基盤で実行可能な分散処理が、通信基盤が伝送するデータの種類に依存していることがあるためである。量子データを伝送する量子

[1] いわゆる古典データ。量子情報処理と対比する場合には、従来型の情報処理は古典情報処理と呼称するのが学術的に正しいが、本ドキュメント内では 2021 年 1 月現在の日本の風潮を鑑み、わかりやすさのために「古典情報技術」・「古典データ」を「デジタル情報技術」・「デジタルデータ」と呼称する。

[2] 古典情報技術とは、量子情報技術と対比して現行情報技術を指すときの用語である。物理学の用語である古典力学・量子力学に由来する。古典と呼ばれているが、情報技術として新しい/古いがあるわけではなく、異種の情報技術としてそれぞれに長所がある。

インターネットが正しく動作すれば、デジタルデータを伝送する通信基盤では実現不可能な広域分散処理が可能になる。例えば、このような量子技術を使うことで、プライバシーを守ったままでデータをクラウド処理するを可能にし、通信のセキュリティ問題に対して科学技術によるひとつの解決方法を提案でき、より自由で安全なデータの流通や活用に繋がることも見込まれる。また、コンピュータの計算能力という観点から考えてみても、多くの量子ビットを連結するほど処理能力が指数的に大きくなる[3]という量子コンピュータの性質に照らして、量子インターネットによって世界中の量子コンピュータがグローバルに繋がることの恩恵は計り知れない。量子インターネットが実現された世界では、サイバー空間は広域分散量子情報処理能力を得て、量子サイバー空間へとアップグレードされる。つまり、現行インターネットの汎用性や規模の上に、量子情報処理や量子通信による優位性が融合した量子インターネットは、双方の長所を併せ持つ新しいサイバー空間をもたらすことになる。

これまでの量子インターネットの研究開発では、ハードウェアの要素技術の実現に重点がおかれてきた。激化するこれからの研究競争を先駆けていくためには、なお一層のハードウェアに関する基礎研究の継続とともに、そのような技術を組み合わせてひとつのシステムとして量子インターネットをフルスタックで設計・構成していく長期的視野をもった研究開発もまた重要となる。そのためには、量子インターネットを構成する多種多様な技術の専門家が協力して研究開発を推進し、基礎研究の段階から融合的に積み重ねていく必要がある。このホワイトペーパーでは、関連する世界動向、および量子インターネットタスクフォースが提案する量子インターネット実現までの道筋についてまとめる。

[3]正確には、重ね合わせで扱える状態空間が指数的に広くなる

目 次

第1章　はじめに - 量子情報の広域通信網 -

1.1 量子インターネットとは

デジタルデータの汎用通信基盤である現行インターネットにおいては、その基盤上で多種多様なサービスやアプリケーションが展開されることで、私たちの社会活動を全般を広く隅々まで支える不可欠なインフラとなっている。最近は特に、デジタルトランスフォーメーション推進のもと、数多くの分野がインターネット上へ移行し、社会構造はインターネットを前提とした形へと急速に変革している。インターネット上のサイバー空間を生活空間・仕事空間の基本とし、フィジカル空間での関係や制限を前提としない社会活動を展開する準備がある程度整っていたことは、コロナ禍において社会秩序や生産活動を維持し、生活の質を維持することに大きく貢献したことからも、改めて認識されることとなった。これからの社会では、SDGs や Society 5.0・知識集約型産業などの実現に向けて、データの自由な流通や高速処理など、インターネットへの要求と期待はさらに大きくなると予想されている。

一方で、インターネットの急速な発展が生んできた様々な課題にも目を向ける必要がある。セキュリティやプライバシー、デジタル・デバイド、寡占企業によるデータ独占、データセンターのエネルギー消費量など、現在のインターネットが抱える問題は、これからもさらに深刻さを増していくであろう。これらの問題は、技術的側面のみならず、社会的側面や法的側面、制度上の問題など様々な側面が複雑に絡み合っており、短期的な解決策を見出すことが必ずしも得策でない場合も多く、短期的に問題が顕著化しないように対応しつつも、中長期的な視点での完全解決へ向けた指針を模索していくことが重要である。様々な視点から示される解決指針の中でも、「科学技術による解決」は特に重要な方向性である。新しい科学技術は、技術的課題の解決のみならず、社会が抱える様々な課題の解決を実装する手段を提供し、人類が目指す近未来社会の実現へ向けた大きな柱のひとつであることは間違いない。インターネット技術の適切な発展により、インターネットと人類の将来を明るいものとしていくことができるはずである。

次世代通信基盤の研究開発としては、様々なものが挙げられているが、その中でも「量子インターネット」は、本質的に異なる技術体系に基づくことで、異色であると言える。次世代通信技術には Beyond 5G や IOWN、量子鍵配送ネットワークなど様々だが、どれもが基本的にデジタルデータを伝送するための技術である。これに対し、量子インターネットは、量子データをやりとりするための技術であり、この点において量子インターネットはデジタルデータの通信基盤（以下、デジタル通信基盤）と抜本的に異なっているため、デジタル通信基盤技術で代用することができない。通信基盤で実行可能な分散処理は通信基盤が伝送するデータの種類に依存しており、デジタルデータ通信基盤では実現不可能な広域分散処理は、量子データを伝送する量子インターネットが正しく動作して初めて可能

になる。

既に見つかっている代表的なアルゴリズムとして、End-to-End の量子鍵配送 [1] や量子フィンガープリント [2]、秘匿量子計算 [3, 4] といった、情報理論安全性[1]を持つ暗号アルゴリズムがある。情報理論安全性に基づくセキュリティ技術は、計算量安全性による現代暗号のように将来の計算能力の向上などの影響を受けないため、長期的な安全性も保証することができる。[2]。また量子コンピュータにおいては、分散量子計算がもつ意義は、現行型コンピュータにおける分散計算よりもはるかに大きい [5, 6, 7]。量子計算では、より多くの量子ビットにわたり量子相関をもたせる（エンタングルする）ことで、量子力学の重ね合わせ原理によって量子ビット数に対して指数的に大きな計算空間で計算できる。特に期待される量子アルゴリズムは量子ビット数に対して多項式で計算時間が増えるもので、量子インターネットを介して複数の量子コンピュータを接続し、多くの量子ビットを 1 つの計算に利用することには、大きなメリットがある。これを古典計算における分散計算と比較すると、古典計算の計算処理は個々のコンピュータで完結するので、2 台、3 台と接続台数を増やしても、計算力も 2 倍、3 倍にしか増えていかない。むしろ、分散処理のためのオーバーヘッドが発生するので、実際には 2 倍、3 倍の高速化を実現するのは難しく、量子計算における分散処理の利点が際立つ。現行コンピュータの分散計算では、例えばスーパーコンピュータのようなシステムエリアネットワークで小さなコンピュータ同士を組み合わせて大きなコンピュータを作ることがまず挙げられる。インターネットを介して分散計算するアイデアはグリッドコンピューティングと呼ばれる。量子コンピュータでも同様の仕組みを考えることができ、グリッド・コンピューティングにおける通信のオーバーヘッドも考慮する必要はあるが、量子もつれによる性能上昇の大きな効果が見込めるので、古典計算よりもグリッド・コンピューティングによって大きなメリットを得られると考えることができる。

また、分散量子計算の応用可能性は、量子コンピューティング全般に広がる。量子インターネットを計測に利用するアプリケーションとしては、量子インターネットで協力するノード間のみで超高精度時刻同期 [8] できることや、超高感度長基線望遠鏡 [9] を実現できることが知られている。このように、既知の量子インターネットアプリケーションは、その概念を現行インターネットと共有しているものが多い。量子インターネット特有の概念を持ったアプリケーションも今後見出されていくことが期待されている。

次に、ここで量子インターネットの能力を抽象的に考えておくことにする。デジタル通信基盤では、チューリングマシンと呼ばれる抽象的なコンピュータで実行可能な分散処理しか実現できない [10]。他方、量子インターネットでは、量子チューリングマシン [11] で実行可能な分散処理を実現できる（図 1.1）。量子チューリングマシンが持つ計算能力は、かなり以前から、量子インターネットに先行して深く研究されており、その能力が一般にも広く知られている量子コンピュータの計算能力である。このことは、量子インターネットでは、デジタル通信基盤では実行不可能な処理も実行可能であることを強く示唆してい

[1]暗号が持ちうる、解読のために必要な情報を盗聴者が得られないので、必ず解読できないという安全性。対義語は計算量的安全性で、解読のために必要な情報を盗聴者は得られ、時間さえかければ解読できるが、解読に必要な計算処理にかかる時間が非現実的（1 万年など）であるために実質的に解読できないという安全性である。

[2]理論上は安全でも、サプライチェーン攻撃など実装・製造上の問題はまだ残る。セキュリティは、理論以外にも多方面から考える必要がある。しかし、理論上安全であることは、セキュリティの究極の目標の実現を議論の俎上に乗せられるという意味で、大きな一歩である。

る。裏返せば、理論上は、量子情報処理システムはデジタル情報処理システムで可能な計算処理は全て実行できる。ただし、利便性やコストの観点から、デジタル通信基盤で可能な処理はデジタル通信基盤で処理することが現実的である。以上のように、量子インター

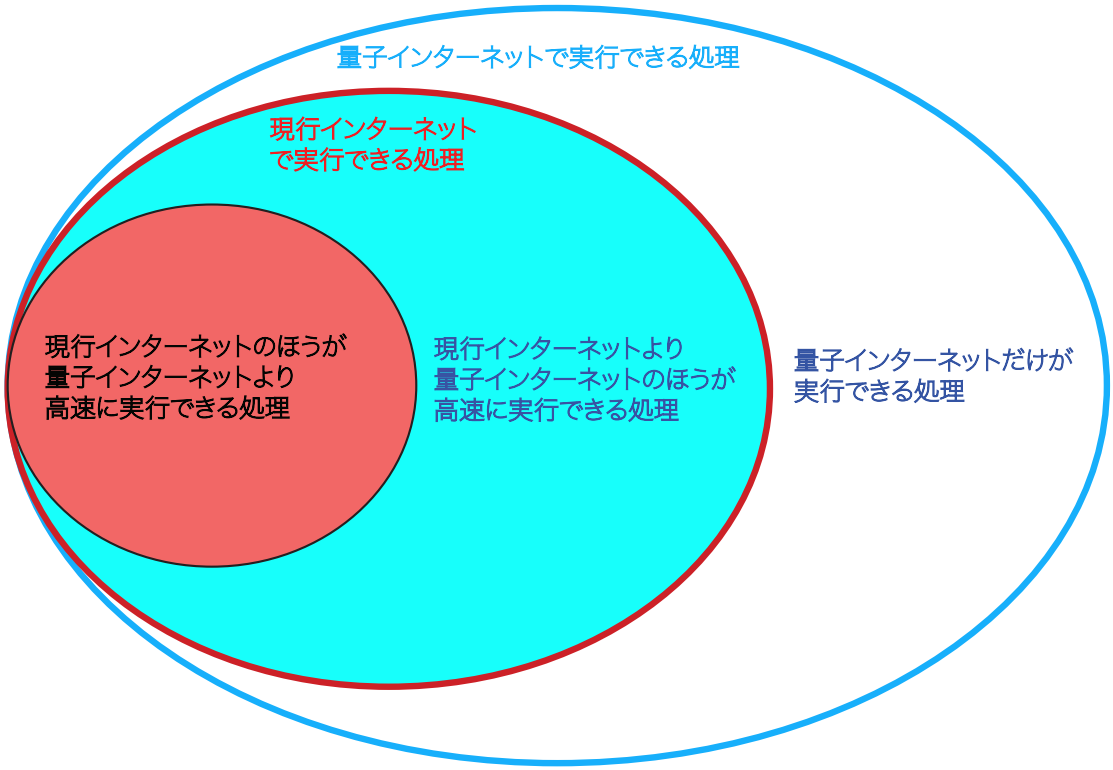


図 1.1: 量子インターネットと現行インターネットで可能な処理の比較

ネットは、量子技術が必要とする通信基盤として唯一無二であるため、長期的なビジョンを持って必ず取り組んでいく必要がある。

1.2 量子通信技術の分類

デジタル通信基盤にインターネット以外の形があるように、量子通信基盤にも、量子インターネット以外の形がある。そのような形の技術的な一つの例として、量子鍵配送ネットワークがあげられる。ここで量子インターネットとの比較を表 1.1 に示す。量子鍵配送ネットワークは、汎用的に量子データを伝送するものではなく、各リンクで量子鍵配送を実行する特定アプリケーションネットワークである。ハードウェアの実現が量子インターネットに比べて容易であり、技術的には社会実装段階にある。情報理論的安全性を持つ共有秘密鍵を比較的高速に生成できるが、隣接した中継ノード間でのみ量子鍵配送が実装されるため、ネットワーク上で運用するには全中継ノードを信頼しなければならないというセキュリティ上の強い制約がある。End-to-End 原則とは、アルゴリズムの実行に中継ノー

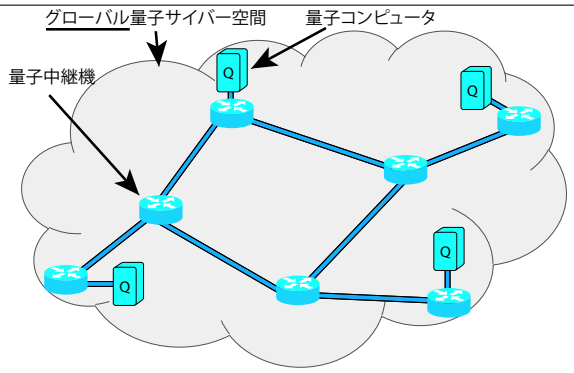
表 1.1: 量子通信基盤の比較

	量子インターネット	量子鍵配送ネットワーク
キャリア	量子もつれ	非量子もつれ
用途	多目的・汎用	共通秘密鍵生成
マルチホップ通信	量子中継により中継局の信頼不要	中継局を信頼する必要
距離	量子中継により理論上無制限	End-to-End 暗号化としては距離に限界がある

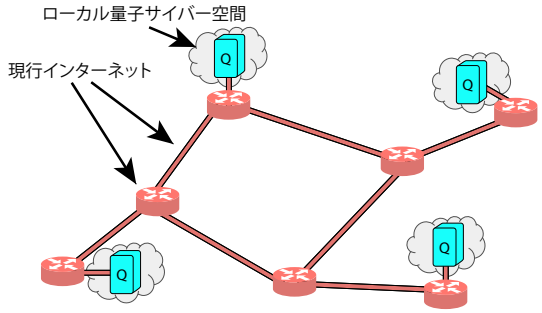
ドが関わらない原則を指す。中継ノードの負荷が軽くなり、ネットワークのスケーラビリティが担保されると同時に、中継ノードに対して処理内容を秘匿できるなどの利点がある。

1.3 量子サイバー空間の形

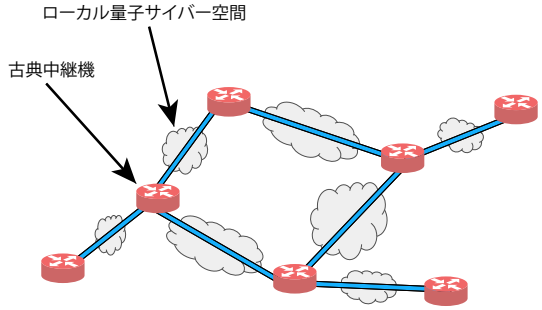
もう少し視野を広げて、量子インターネットによる量子サイバー空間が持ちうる能力と、量子インターネット以外の量子情報技術（と現行型インターネット）による量子サイバー空間の能力が異なることを整理しておく。例えば、量子インターネットがなくとも、量子コンピュータには現行インターネットでアクセスできる。また、量子鍵配送ネットワークは、量子コンピュータに入出力するデータをインターネットを介してセキュアに通信することができる。これらの技術によるサイバー空間は、量子情報技術によるサイバー空間ではあるものの、実は量子インターネットによるサイバー空間とは異なることを図 1.2 に示す。図 1.2 が示すように、量子インターネットのみが、複数の量子コンピュータを量子的につなげることを許すことがわかる。量子インターネットは、量子コンピュータにアクセスできるだけでなく、量子コンピュータに外から量子データを入力することも許す。この性質が量子サイバー空間を規定しており、End-to-End で量子通信アルゴリズムや分散量子アルゴリズムを実行するために必須である。ここからも、量子時代のインフラには量子インターネットが不可欠であることが読み取れる。



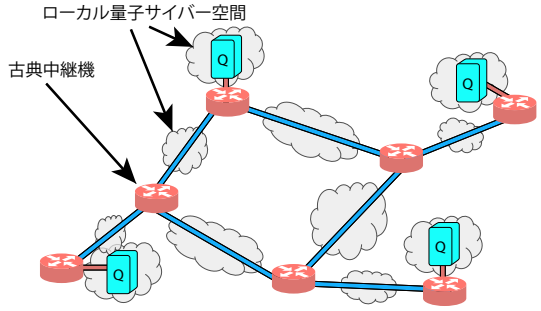
(a)“The” 量子インターネットによるグローバル量子サイバー空間



(b) 量子コンピュータと現行インターネットによる量子サイバー空間



(c) 量子鍵配送ネットワークによる量子サイバー空間



(d) 量子鍵配送ネットワークと量子コンピュータによる量子サイバー空間

図 1.2: 各量子情報技術と、対応する量子サイバー空間の形。同じ「雲」の中でのみ量子通信アルゴリズム・分散量子アルゴリズムを実行できる。(c),(d) では、リンク上の量子サイバー空間では量子鍵配送のみを実行できる。

第2章　世界の大型プロジェクト・投資

従来、量子インターネットの研究開発は、個々の要素技術のプロジェクトとして進められてきた。ここ数年、量子情報技術に関して先見的な視点を持ち、先進的な成果を挙げ続けている国々が、「量子インターネットのテストベッドの構築」や、「量子インターネットの中継機を作る」ことを目標とした大型プロジェクトを立ち上げている。このようなプロジェクトは、量子コンピュータや量子鍵配送ネットワークのプロジェクトとは独立のビジョンを持った上で、連携して進められている。

2.1 ヨーロッパ圏

2.1.1　EU

EU Quantum Flagship 開始時からの 25 プロジェクトとしてサポートされている Quantum Internet Alliance (QIA) [1]では、2018 年から、量子インターネットのテストベッドの構築が始まっている。2021 年までの 3 年間の予算額は 1000 万ユーロである[2]。量子インターネットを達成するまでの技術的な道のりを、特に物理レイヤーやハードウェアを中心にまとめた論文が公表されている [12]。2021 年 2 月には、量子メモリを使って決定的に成功する（確率的ではない）量子中継の Proof of Concept を実証した報告が、プレプリントサイト arXiv にアップロードされた [13]。

QIA の中心となっている TU Delft では、QIA の前から、長距離量子通信をビジョンとした研究が進められてきた。2013 年にダイヤモンド中の量子ビット間で量子もつれを生成することに始まり [14]、2014 年にはダイヤモンド間で量子テレポーテーションに成功 [15] し、2015 年には 1.3km の遠距離間で量子もつれの生成に成功している [16]。異なるダイヤモンド間での量子もつれ精製 [17] と呼ばれる量子インターネット独特のエラー管理手法の実験にも成功している [18]。QIA が始まってからは、上述のテストベッド構築を進めるとともに、隣接ノード間でのリンクレイヤープロトコルを開発した論文をコンピュータネットワークのトップカンファレンスである SIGCOMM 2019 で発表するなど、コンピュータネットワーク側でも大きな成果が出ている [19]。まさしく、量子インターネットの実現に必要な諸分野の専門家が多組織から集い、量子力学の理論家、実験家、計算機科学者/工学者などが連携して先端的な取り組みをおこなっていることによる成果である。

[1] https://quantum-internet.team/

[2] https://www.tudelft.nl/en/2018/tu-delft/eu-awards-ten-million-euro-to-european-quantum-internet-alliance-to-speed-up-development-of-quantum-internet/

	量子インターネット	量子鍵配送ネットワーク
日本	なし	総務省グローバル量子暗号ネットワーク
全 EU	Quantum Internet Alliance（蘭） (Quantum Technologies Flagship)	OpenQKD（西）
ドイツ	Q.Link.X	なし
米国	DOE: Q-NEXT など	Battelle Quantum Network (凍結中)
	NSF: Center for Quantum Networks	
中国	Jian-Wei Pan グループ	National quantum secure communication backbone network

表 2.1: 世界各地の量子インターネットもしくは量子鍵配送ネットワークを目的とした大型プロジェクト

2.1.2 ドイツ

ドイツには、ドイツ独自の量子インターネットコンソーシアムである Quantum Link Extension [3]が 2019 年に発足した。The German Federal Ministry of Education and Research による 3 年間の予算額は 1480 万ユーロである[4]。

2.2 米国

米国では、2020 年に入ってから国家規模の量子インターネット研究開発が活発化し、2020 年 9 月には Quantum Initiative Act を更新して量子インターネットへの支援を手厚くする法案[5]が提出されるなど、積極的な動きが始まった。この更新に合わせて、2020 年 7 月に米国エネルギー省 (DOE)、8 月に米国立科学財団 (NSF) がそれぞれプロジェクトを発表した。どちらのプロジェクトも、基礎研究から、フィールド実験など工学的な取り組みまでサポートしている。DOE の声明では、DOE 傘下のアルゴンヌ国立研究所及びブルックヘブン国立研究所を中心としたプロジェクトを発足した[6] [7]。代表的プロジェクトは Q-NEXT[8]である。DOE はこれに合わせ、2020 年 2 月に開催した量子インターネット青写真ワークショップのレポートを公開した[9]。このレポートでは 5 段階のマイルストーンを置いている:

1. ファイバーネットワーク越しのセキュア量子プロトコルの検証（1.2(c)）

[3] https://qlinkx.de/

[4] https://www.uni-wuerzburg.de/en/news-and-events/news/detail/news/a-leap-into-quantum-technology/

[5] H.R.8279 - Quantum Network Infrastructure Act of 2020: https://www.congress.gov/bill/116th-congress/house-bill/8279

[6] The Quantum Internet of the Future is Here. https://www.energy.gov/articles/quantum-internet-future-here JULY 23, 2020

[7] U.S. Department of Energy Unveils Blueprint for the Quantum Internet at ‘Launch to the Future: Quantum Internet’. https://www.energy.gov/articles/us-department-energy-unveils-blueprint-quantum-internet-launch-future-quantum-internet JULY 23, 2020

[8] https://www.q-next.org/

[9] Report of the DOE Quantum Internet Blueprint Workshop. From Long-distance Entanglement to Building a Nationwide Quantum Internet. https://www.energy.gov/sites/prod/files/2020/07/f76/QuantumWkshpRpt20FINAL_Nav_0.pdf February 5-6, 2020

2. キャンパス間・都市内量子もつれ配送（以下、1.2(a) を大きくスケールさせていくための研究開発）

3. “量子もつれスワッピング” を用いる都市間量子通信（量子メモリネットワーク・量子信号を中継させる技術の研究開発と導入・1 つ以上のテストベッドが必要）

4. 量子信号中継機を用いた州間量子もつれ配送（現行型インターネットの技術を導入・量子エラー訂正）

5. 研究所・学術界・産業界間の複数組織エコシステムの構築による、デモンストレーションから運用インフラへの移行

2021 年度の予算として 2500 万ドルが要求されている[10]。

NSF は、アリゾナ大学を中心とするコンソーシアムである、Center for Quantum Networks に出資する[11]。Tucson（アリゾナ州）と Boston の二箇所にテストベッドを設置する。2025 年までの 5 年間で 2600 万ドルの予算が配分されている[12]。

2.3 中国

中国は、量子インターネットをお題目とした大型プロジェクトはないものの、量子情報技術に係る多種多様な研究をおこなっており、光子を使った量子計算で量子超越性を実証 [20] した Jian-Wei Pan のグループが、衛星を使った量子もつれ配送の実験 [21] や全光量子中継の実験 [22] を実施しており、量子インターネットを志向した研究成果を挙げている。

[10] https://www.whitehouse.gov/briefings-statements/president-trumps-fy-2021-budget-commits-double-investments-key-industries-future/

[11] Award Abstract #1941583 NSF Engineering Research Center for Quantum Networks (CQN). https://nsf.gov/awardsearch/showAward?AWD_ID=1941583

[12] https://news.azpm.org/p/news-articles/2020/8/26/179214-ua-to-lead-center-for-quantum-networks/

第3章　量子インターネットの全体像

3.1 ハードウェア

量子インターネットを構成するハードウェアに求められる機能として、量子メモリやメモリ-光子インタフェース、光子の波長変換や位相補正、もつれ光源、光スイッチやオプティカルクロスバースイッチなどのフォワーディング装置、光子検出器、多重化、光ファイバーの安定化などがある。量子メモリではゲート操作や測定なども求められ、量子コンピュータと同等の機能を統合的に実装しなければならない点において、ハードウェア実現のハードルは高い。

現行インターネットによると、汎用大規模通信網において、ハードウェアのダイバーシティ（多様性）は大切である。現在使われている有線接続だけを考えてみても、大別すると光ファイバーと UTP ケーブルがあり、それぞれ長所と用途が異なる。光ファイバーは曲げに弱いが大容量であり、固定された機器同士の接続に向く。一方、UTP ケーブルは光ファイバーに比べて低容量であるが、曲げに強く、取り回しが利くので、ユーザに近い場面での利用に向いている。光ファイバーと UTP ケーブルはそれぞれ光信号と電気信号をメディアとするので、これらのケーブルが接続されるハードウェアの実装は素子から異なっている。異なるケーブルがインターネットに同居できるのは、インターネットがハードウェアの多様性を大切にしているためである。量子インターネットの場合を考えてみると、例えば、高周波数で動作するが量子信号中継に失敗する可能性がある素子と、量子信号中継は安定的に動作するが低周波数の素子を組み合わせてネットワークを構築することで、より高パフォーマンスなネットワークを構築できる可能性がある。また、エラー管理を実装しやすい素子や、ネットワークの異常検知を実装しやすい素子があると、安定的でセキュアな量子インターネットの実現に役立つと考えられる。

3.2 レイヤードアーキテクチャ

レイヤードアーキテクチャはコンピュータネットワークにおける画期的発明である [23]。大規模通信網に必要な機能と責任が明瞭にレイヤー分割できたおかげで、大量の中継ノードを介した通信を混乱なく実行できるようになった。さらに、任意の通信を扱うことができ、汎用通信網が成立した。レイヤードアーキテクチャにおいては、各レイヤーは、下位レイヤーの機能と責任を上位レイヤーに対して隠蔽する。例えば、一定個数の量子もつれを End-to-End で作成することを責任とするレイヤーにおいて、各ノード間の物理レイヤーの実現方法を考慮して設計する必要があると、設計が複雑化する。複雑な設計は実装やデバッグを困難にすると同時に、低性能化や設計ミスを誘発する可能性もあり、システム構築の失敗に繋がる。したがって、数を保証するためのレイヤーは、数は保証しないがある

程度の個数の量子もつれを End-to-End で作ることを責任とするレイヤーの上に置くなど、下位レイヤーの責任は上位に対して隠蔽されていくアーキテクチャが望ましい。

量子インターネットを実現するには、「量子の TCP/IP」とでも呼ぶべき通信管理プロトコルや通信リソース予約アルゴリズム・プロトコル、量子もつれ精製などを備えた、量子インターネットのためのレイヤードアーキテクチャが必要である。すなわち、量子インターネットを実現するために必要な機能や責任をレイヤー毎に分割して整理し、レイヤー間のインタフェースを定義する必要がある。レイヤードアーキテクチャでは、責任を抽象化して考えるため、登場する概念は基本的にコンピュータネットワークのものが多い。しかし、各レイヤーが責任とする機能の実現には何らかのハードウェアが必要であるため、これらの概念はハードウェアモジュールとも密接に関係する。それどころか、各レイヤーの設計は、ハードウェアの設計や、関係する基礎研究の指針となるため、大変重要である。良いレイヤードアーキテクチャを生み出すためには、試行錯誤を繰り返し何度もアーキテクチャを作り直していく展開も想定しておかなければならない。特に初期の量子情報技術では、レイヤー間の依存性が強くなる見込みが強く、レイヤー設計には多面的で十分な検討が必要である。

また、量子インターネットを構成するには、技術的のみならず、社会的にもスケーラブルなアーキテクチャであることも重要なファクターである。米国の情報スーパーハイウェイの理想は、政府主導ではなく、マルチステークホルダーによって成立するインターネットによって実現された。多数の主体が各々のネットワークを構築・運用し、相互接続して超大型のネットワークを構成する。お互いの通信データはお互いに融通して伝送し合う。各々のネットワークは、各自の責任においてメンテナンスする。この「自律分散協調」の仕組みが、技術的かつ社会的にスケーラブルに働いているおかげで、全地球規模・全人類規模の通信網となることができたのがインターネットである。量子インターネットも、スケーラビリティのためには、自律分散協調の仕組みとなるのが望ましい。しかし、自律分散協調ゆえの難しさもまた存在する。例えば、他所のネットワークでインシデントが発生したときに、その発生の仕方によっては、自ネットワークでも通信障害が発生しうる（パケットブラックホールなど）。量子インターネットアーキテクチャの設計では、現行インターネットの反省について十分検討し、このような問題が発生しないようにしなければならない。また、仮に、量子力学由来の性質のために量子インターネットでは Best Effort 原則や End-to-End 原則を採用できないとしても、量子インターネットアーキテクチャもまた極力シンプルな仕組みで作られるべきであることは、現行インターネットと同様であると推察される。ハードウェア技術を組み合わせ、このような仕組みを作り上げていくのが、量子インターネットシステムの全体像を組み上げていく上で重要な研究課題となっていくと考えられる。

視点を変えて、ハードウェア実装上の都合について考えてみる。アーキテクチャ観点の研究では、以上のように、「量子インターネットを動作させるには求められる機能をいかにレイヤーに分割するか」が重要な研究課題である。大規模システムを動作させ、技術的にも社会的にもスケールさせていくためには、レイヤードアーキテクチャの研究開発は必須である。他方、ハードウェアの観点では、レイヤー化によるオーバーヘッドの発生を避けたい場面の発生も想定される。レイヤー化を無視する（レイヤーバイオレーション）によってレイヤー化に起因するオーバーヘッドの発生が回避され、高速化することは現行イ

ンターネットの研究開発からも明らかである。特に初期の量子インターネットでは、技術的に未成熟な中で十分な性能を持つハードウェアを実現するために、レイヤーバイオレーションが必要となる可能性もある。そのような場合にも量子インターネットを着実に実装・実現し、スケールさせていくためには、まず適切なレイヤードアーキテクチャを完成させてからレイヤーバイオレーションすべきであると考えられる。

以下では、古典インターネットのレイヤー構造を参考にして、量子インターネットでどのようなレイヤー構造が考えられるかの一例を提示する。

3.2.1 物理レイヤー

隣り合うノード間（1 ホップ）での量子もつれ生成を試行するレイヤーである。

メディアは一般の光ファイバーを利用できるが、現行インターネットで使われる古典中継機が途中に存在すると量子もつれが破壊されるため利用できない。量子情報専用の「量子中継機」[1] の実現は、量子インターネットの重要なマイルストーンの 1 つである。

現行インターネットの常識に照らすと奇妙であるが、データの伝送ではなく一種の相関関係である量子もつれを生成したい量子インターネットでは、隣り合う 2 ノードの間に補助ノードを挟み、相関関係の構築を助けるタイプの実装も有望視されている（TU Delft は 1 光子干渉を用いる補助ノードによる物理レイヤーを採用している。）。量子もつれは相関関係であり、向きがないので、隣り合うノードのうちどちらかが光子を送出する側でもう一方が受信する側という実装も可能である。補助ノードがある場合、採用する補助ノードタイプによっては両側が光子の送出側もしくは受信側になることもあり得る。

3.2.2 リンクレイヤー

単一ネットワーク内での量子もつれ生成に責任を持つレイヤーである。このレイヤーで、1 ホップでの量子もつれの品質管理や、エラー管理もすることが考えられる。古典情報の場合と異なり、量子情報のブロードキャストはできない [24] ので単純なハブは作れず、インテリジェントなハブが基本となると見込まれる。

3.2.3 インターネットワーキングレイヤー

このレイヤーは異なるネットワークの間での量子もつれ生成に責任を持つ。経路決定については、現行インターネットのサポートによりルーティングを実装する。現行インターネットでは、決定された経路に基づいてパケットをフォーワードするが、量子インターネットでは、” 量子もつれスワッピング”[25] を実行する。現行インターネットに実装されている store & forward や routing / forwarding という仕組みではなく、量子インターネットではいわば store & swap や routing & swap となる [26]。各リンクでの量子もつれ生成を同時におこなえるのは、量子インターネットアーキテクチャの特異性である。インターネットワーキングレイヤーを上下二層に分け、下位層でルーティング/スワッピングを実行し、上位層でマルチホップでのエラー管理を実行するアイデアもある。

3.2.4　プラットフォームレイヤー

End-to-End で生成した量子もつれの個数や品質に責任を持つレイヤーである。量子インターネットにおいては、あらゆる箇所で光子損失（光子が光ファイバーに吸収されてしまったり、外に出ていってしまい、管理化から失われてしまう現象）やエラーが発生するため、作成される量子もつれの数や品質を保証しにくい。数や品質を保証するレイヤーを End-to-End で持つことで、アプリケーションの要求を満たす量子もつれを提供できるようになる。

3.2.5　アプリケーションレイヤー

アプリケーションを実装するレイヤーであり、量子インターネットの汎用性を活かせるよう、任意の分散量子アプリケーションを実装できる自由度を持たせる必要がある。現行インターネットとの統合も考えるべきであるため、現行インターネット側のライブラリも含め、ライブラリ機能の再整理に取り組まなければならない可能性もある。量子コンピュータに採用されている素子や、センサーに向いている素子など、素子レベルでハードウェアとも関係すると見込まれる。

3.3 アプリケーション

1.1 でまとめた通り、量子インターネットのアプリケーションの利点は大きく分けて 2 種類存在する。

- デジタル通信基盤上では実現不可能な分散処理が可能になる。
- 特定の課題を達成するために必要な通信回数を減少させる [27]。

現行インターネットがそうであるように、生活とサイバー空間との関わり方が発展して量子計算に期待されることが増えるにつれ、また、量子センサーが発展してフィジカル空間の量子の世界と量子サイバー空間がより密接になっていくにつれ、量子インターネットに要求される性能やアプリケーションが増えていくことは間違いない。End-to-End の量子もつれ生成や量子情報の伝送により実現できる量子通信アルゴリズム・分散量子アルゴリズムの代表的なものを以下にまとめる。

3.3.1　セキュリティ

第節で述べたとおり、量子インターネットのセキュリティでは、まず、情報理論的安全性を持つ共有秘密鍵生成 [1] や認証 [2] を実現できる。情報理論的安全性を持つ鍵は、長期的に安全でもある。現行インターネットのセキュリティシステムは、あるパターンで生成された問題を効率的に解くアルゴリズムが存在しないことを仮定して構築されている（計算量的安全性）。しかし、暗号の歴史上この仮定は繰り返し破られてきており、一旦仮定が破られると過去の暗号化データも遡って破られてしまう。したがって、長期的な秘匿性が求められるような秘密情報にこのようなセキュリティシステムを適用することは、解読

アルゴリズムが発明されていない段階でも望ましくない。一方、量子インターネットのセキュリティアルゴリズムは情報理論的に安全であるため、この不安定な仮定に依存しない長期的な安全性を保証できる。情報理論的に安全な共有秘密鍵と共通鍵（対称鍵）暗号技術を組み合わせることで、より柔軟にセキュリティ要件を満たし、多様なアプリケーションを実現できる。

次に、クラウド秘匿計算について考える。現行インターネットにおいては、データの秘匿のみが実用的である。他方、量子インターネットでは、入出力データを秘匿しつつ、実行処理（プログラム）自体も制約なく秘匿できるアルゴリズムが既に提案されている [3, 4]。この秘匿量子計算の実現は、センシティブなプライバシー情報を含むデータを安全に計算処理できることに繋がり、データの自由な流通にも大きく貢献すると見込まれる。

以上のように、新しい科学技術である量子インターネットの提供するセキュリティ機能は、デジタル通信基盤では解決し得ないセキュリティやプライバシー上の問題を根本的に解決できると期待されている。

3.3.2 分散量子計算

第 3.3.1 節で述べたとおり、分散量子計算による量子コンピュータの拡張は大きな可能性を秘めている。量子インターネットを介して複数の量子コンピュータの量子メモリをエンタングルさせることで、仮想的に 1 台の量子コンピュータとして量子計算を実行することができる。素因数分解を実行する Shor のアルゴリズム [28] や、逆行列計算の HHL アルゴリズム [29] など、任意の量子アルゴリズムを実行できる。

また、ネットワークであることに意味がある分散アルゴリズムにおいても、現行インターネットより高速なアルゴリズムが発見されている。リーダー選出 [30] や、高速ビザンチン合意 [31]、ネットワークの直径 [32] を測るアルゴリズムなどがある。

3.3.3 量子センサー

量子センサーは、フィジカル空間と量子サイバー空間を結びつけることができる。さらに、量子 Internet of Things にも発展していくと期待できる。量子センサーが量子インターネットと繋がることで、グローバルな量子センシングが可能になる。例として、長基線望遠鏡の感度を原理的に改善できる [9] など、これまでにない幅広い応用先が存在することが既に分かっている。

3.3.4 計測

協力者同士での高精度時刻同期 [8] が可能になるなど、分散量子アルゴリズムが存在する。

3.4 日本の強み

表 3.1 は、量子インターネットの研究開発における日本や世界各国の強みのまとめである。日本は、現行インターネットの歴史から明らかになった、技術のダイバーシティや大規模ネットワークまで発展した後を考えたアーキテクチャの重要性に沿う、量子インターネットの研究開発があるべき姿と合致した研究スタイルになっている。

表 3.1: 世界との競争状況、日本の強み

	日本	欧州	米国	中国
ハードウェア	• ハードウェアのダイバーシティがある – 原子集団 [33]、NV 中心 [34]、希土類 [35]、超伝導 [36]、イオン [37] など様々な量子メモリ候補での基礎実験 – 全光アーキテクチャの提案 [38]・実証 [39] (2015-2018)	• 世界でいち早くフィールドでの 1 ホップ実験を展開 • NV 中心 [40]、希土類 [41] で先端的な結果 • NV 中心を用いて、確率的ではない量子中継を実証 [13] • オランダに整備済みのファイバー網を利用と予想される（TODO 要出典）	• メモリを使った光子間の量子相関測定（量子中継のコア技術）を実証 [42] • フィールドテストのためのダークファイバー網をいち早く整備	• 多額の予算を活かした衛星を利用した研究実績 (2017) • 原子集団量子メモリでの先端的な結果
アーキテクチャ	• 世界に先駆けて量子通信アーキテクチャの研究に取り組む • 現行インターネットの研究・運用の知見や量子情報理論に基づいた、トップダウン型の研究を展開 • 世界初オープンソース量子インターネットシミュレータを公開 [43]	• ハードウェアのパラメータに注目した、ボトムアップ型の研究を展開	• アーキテクチャの観点での研究は手薄	• 量子暗号ネットワークのアーキテクチャ研究に積極的
アプリケーション	• 暗号、センシングの専門家は一定数存在。 • 分散計算・秘密計算の専門家も存在。	• 古くから研究が継続されており、多くの提案がなされている。	• 量子鍵配送の発案者など、有名な理論家を多数擁する。	• 現状は存在感が薄い。
その他	• 人材は、必要な全領域にわたってまんべんなく存在している。(ただし少数なので教育が鍵)	• 世界でもいち早く量子インターネットに力を入れ始めた (2018-)	• 2020 年から急激に力をいれはじめた (DoE/NSF)	• 投入可能人材量、関連技術に優位性があるため参入すれば強力

第4章　大規模に取り組む必要がある研究開発

グローバルに量子もつれ共有し量子状態伝送可能な量子インターネット実現には、まず各構成要素技術の研究が重要である。量子ビットを取り扱う物理レイヤーだけみても、量子もつれを生成する光源、量子状態保存用量子メモリ、光ファイバ伝送に適した通信波長と量子メモリ波長を結ぶ量子波長変換など多くの要素から成り立つ。それと同時に、送受信者間での通信実施を可能にするルーティング機能などのネットワーク制御により、情報通信網としての機能開発が必要不可欠である。前述のとおり、量子インターネットはハードウェア、アーキテクチャ、アプリケーションといった様々なレイヤーでの成果の集合体である。それぞれのレイヤーにおいて取扱う個々のシステム依存でなく（たとえば物理レイヤーで量子メモリとして使用される物質に依らず)、現行インターネットと同程度の抽象的なレイヤーアーキテクチャ設計を導入し、各レイヤーで抽象的な機能を背負わせることで、着実な量子インターネット実装へとすすめる可能性が高まることも前章で述べた。よって最終目標である世界中が繋がる量子インターネット実現には、各レイヤーでの進展が必要になる。各レイヤーにおける課題の早期発見と新規技術の開発・取り込みを行いながらシステム全体としての計画を随時更新・検証していく仕組み作りが重要である。そのため現実環境における量子インターネットのテストベッド構築により、まず超小型の量子インターネットを実装・検証することが必要と考える。テストベッド構築は、中長期的競争となる量子インターネットの世界における研究開発競争を戦い抜くためには極めて重要な課題である。

4.1 ラボから小規模ネットワーク、そして大規模ネットワークへ

量子インターネットテストベッドでは以下の目標が設定できる。

1. 大前提：古典ビットではなく量子ビットを送れること。
2. テストベッドのネットワーク構成は 1 次元（直線）ではなく、2 次元以上であるべき。
3. レイヤーアーキテクチャにもとづく実装に向け、物理システムに依存しない上位レイヤーのインターフェースを介したシステムとする。
4. フィールドファイバー上での実装。

これらの必要性であるが、1 はそもそもの量子インターネットの存在意義であるので、必要不可欠な機能である。2 はネットワーク上の任意の地点間を結べる重要性から、1 次元的なネットワーク構成では厳しく、2 次元以上の少なくとも網目上との表現が可能なネットワーク構成が必要。3 は、例えば物理レイヤーで様々な量子ビット伝送システムが可能

であることを考える。例えば、もつれ光子対を高いビットレートで放出できる光源もあれば、量子メモリから直接もつれ光子が放出されるメモリ－光源一体化システムもありえる。量子メモリだけを見た場合でも、受け入れる光波長がメモリ物質ごとに異なり、また帯域やメモリー時間も全く異なる。それらの違い（異種性）は、統一した物理系だけで量子インターネットを構築できる場合のシンプルさに比較しデメリットと一見感じるが、他方メリットもある。例えば、中継ノードにおける量子もつれ交換は、量子もつれをより長距離の中継ノード間もしくはエンドノードで生成するための処理であるが、中継操作という比較的短時間のメモリ時間で許容される。一方、エンドノードに設置される量子メモリはアプリケーションによっては非常に長いメモリ時間を要求し得る。つまり量子インターネット構築に必要な物理レイヤーの構築は、様々な物理系から構成される可能性があり、それら異種の要素を種に依らず使用できるシステム構築が重要である。4 は、クリーンな環境を提供できるラボ内での検証のみでは得られない実装上の知見獲得に必須である。例えば物理的に遠く隔たった拠点間での信号の時間・周波数同期といった技術獲得が必要で、また埋設された光ファイバーはラボ内の新設光ファイバーよりずっと損失が大きかったり、光ファイバー中で他の信号との混線が起きる可能性すらある。可能な限り実用に近い環境でのテストベッド構築を経て、初めて量子インターネットの社会実装が視野に入る。

以下 (図 4.1 参照) は、量子インターネットテストベッドが要素技術から大規模化していくにあたって辿るであろう展開である。

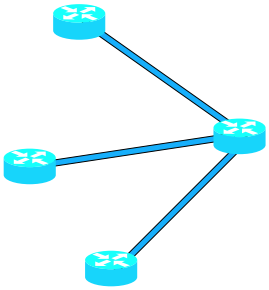
1. 実験室内において、量子信号中継から量子もつれ共有・量子ビット伝送の原理実証。
2. 図 4.1(a)　量子中継の実験室外・長距離・フィールド環境という離れたノード間での動作検証。
3. 図 4.1(b)　ルーティングやエラー管理を含め、量子インターネットに必要な機能の動作検証可能な最小規模のネットワーク構築および検証。この図のトポロジーはルーティングが発生する最小のトポロジーである。
4. 図 4.1(c)　前項実証システムが、中規模・大規模かつ複雑なネットワークに発展していっても、スケールし動作していく検証。

4.2 テストベッド

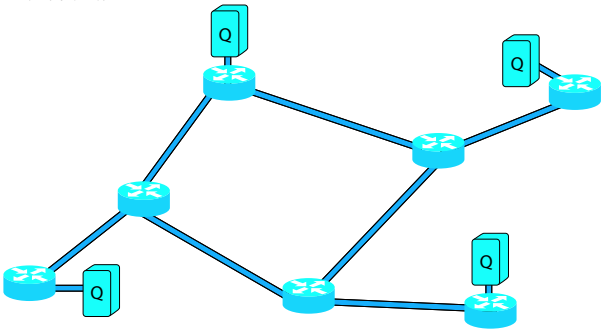
量子インターネットテストベッドの最初の目標は図 4.1(b) に対応する上記項目「3」となる。そこに向けた道筋として、具体的な研究開発フェーズ例および項目例を以下に列挙する。

- Phase 1: 仕様策定・フィールド環境準備。ラボ内での通信光源、ルーティング機能などの準備。
- Phase 2: 各機能コンポーネント化、インタフェース機能などの実装による、フィールドでのスイッチング機能獲得。単リンク間量子もつれ配送

(a) 離れたノード間の量子中継システム・プロトコルの動作実証



(b) 大規模ネットワークに繋がるシステム・プロトコルの、最小構成ネットワークでの動作実証



(c) 大規模な複雑ネットワークへのスケール実証

図 4.1: 量子インターネットテストベッドのスケーリング

- Phase 3: ルーティングによる複数拠点間切り替え量子もつれ共有機能実証。（量子メモリなし）
- Phase 4: 量子メモリつきシステムへのアップグレード。

物理レイヤーにおける研究開発の進展は、全世界的に光が先行しており、量子メモリが遅れている状況である。そのため、まず光（量子もつれ光源）によるフィールド実験を進め、ルーティング機能を実装し、それによる 2 次元ネットワークにおける量子もつれ共有機能

を獲得する。Phase 3 までの間に並行して量子メモリ開発を進め、Phase 4 において量子メモリを組み込んだフィールド実験を行う。

これに向けた必要な研究開発項目をいくつか以下に挙げるが、Phase 1 における仕様策定にて、必要な項目の洗い出し・準備を進める。

- 量子もつれ光源
  - 識別不可能性
  - レート
  - 多重化
- 量子メモリ
  - 時間
  - 効率
  - 伝令機能
  - 多重化
- 量子メモリ-光子インタフェース
  - 複数ファイバー付き量子メモリ or 光スイッチ
  - 量子波長変換
  - 量子トランスデューサ
- 量子インターコネクト
- 中継技術
  - 識別不可能性 $\rightarrow$ Bell 測定
  - 時間同期
  - 周波数同期、安定化
- 高性能光子検出器
- 量子操作（ゲート操作・測定）
  - 量子状態エラー管理
  - 光子ロス管理
  - 量子状態トモグラフィ
  - 量子もつれ交換
  - 量子もつれ純粋化
- 長距離化・フィールド環境通信の実証

- 動的な光路管理
- 多重化
- アーキテクチャ研究との合流
  - リンク管理
  - セッション管理
  - ルーティングアルゴリズム
  - ルーティング管理
  - リソース管理
  - 自律分散協調化
  - Best Effort 化
  - End-to-End 化
  - プラットフォーム化
  - レイヤー化
  - レイヤー間インタフェース
  - 上記要素の各々につき、通信プロトコル
  - ヘルスチェック機構（セキュリティ）
  - etc.
- パッケージング（可搬化含む）

第5章　推進体制

サイバー空間は今や全人類の生活空間である。文明史の観点でも、情報技術は大きな意味を持つ。既存 IT 産業のビッグネームの固定化が進む中、サイバー空間を進化させる量子インターネットの実現は、IT 産業における重要なターニングポイントとなりうるため、長期的ビジョンを持って確実に進めていかなければならない。長期的な研究開発を進めるにあたり、プロジェクトの継続性が課題となることは明らかである。このような取組みでは、国プロジェクトのような、特定のプロジェクト終了とともに推進体制まで解散するような体制ではなく、様々な資金を活用できる継続的体制に基づいて進めていくことが重要となる。産学官連携コンソーシアムである QITF は、この受け皿を担うことができる。

5.1 学際連携（異分野間連携）

第 3 章で述べたとおり、量子インターネットの実現には、多分野間の学際的連携が欠かせない。初期の研究開発においてはコンピュータネットワークの専門家とハードウェアの専門家の連携が特に強く必要であり、必須機能の責任分解やモジュールに求められる仕様・性能などについて互いの専門分野の相互理解を深めながら研究開発を進め、困難点やボトルネックを相補的にサポートしていき、最終的に量子インターネットという 1 つのシステムとして整合性が取れるようにする必要がある。この連携にあたり、関係者間での定期的な会合の開催は有効であると考えられる。一方、研究競争や知財としての側面を考えると、特にハードウェアでは、取り組んでいる課題の困難点や技術の過度な公開・共有は難しいという現実もある。このような場合には、量子インターネットを作るという共通の大目的を持つ全体としての組織体を持ちつつ、特定課題をターゲットとした分野横断ワーキンググループ（WG）を作り、WG 単位での会合を開催するなど、小回りの利く連携体制を敷くことが有効であると考えられる。多分野的で全日本的かつマルチステークホルダーな協力体制を構築している QITF は、量子インターネットの研究開発について十分に検討するために必要な、広い意見の集約をおこなうことができる。

5.2 産・学・官・民 連携

量子インターネットが健全に発展するためには、産・学・官・民の皆が積極的主体・重要なステークホルダーであることを認めながら研究開発を推進していく必要がある。

インターネットが成功した鍵は、技術的のみならず社会的にもスケールしたことであり、すなわち自律分散協調である。インターネットにおいては、特定の中央集権的な主体を持たず、産・学・官のマルチステークホルダーが各々のネットワークを管理運用し、連携して相互接続することで、世界規模のインフラが構築されている。また、民が自由に活動し

ていること、ひいては発言権を持っていることも、インターネットが自由なインフラ・開かれたインフラであるために重要な役割を果たしている。自由を保証しない/自由を阻害するネットワークなどのインフラや、SNS などのプラットフォームは、民を含むユーザから見放されやすく、競争力を失っていく。オープンソース文化の観点でも、市井の開発者は重要な役割を果たしている。おかしなソフトウェアや仕組みは発見され、淘汰される自浄作用が働いている。他方、自律分散協調であるがゆえの問題をインターネットが抱えていることも事実である。例えば、通信の綿密な品質管理には他組織の管理するネットワークの協力が必要であるが、必ず協力を得られる保証はない。これはユーザの体験品質の低下に繋がる。場合によっては、致命的アプリケーションの求める最低限の通信品質を満たすことができない可能性もある。

量子インターネットの研究開発においては、現行インターネットの良いところは引き継ぎ、悪いところは克服していくべきである。したがって、産・学・官・民の皆が積極的主体・重要なステークホルダーであることを認め合いながら、新しい形の自律分散協調について検討すべきである可能性がある。これは、インターネットの自由を守り、すべての人々が幸福に暮らしていく社会を作っていくためにも重要である。

5.3 研究開発成果の形

量子インターネットの実現を目指すプロジェクトでは、成果の形も多岐に渡る。 表 5.1

研究・学術論文	科学の理論や実証をおこなう研究成果。物理学に係る理論や原理実証から情報科学・工学に係る研究など。
開発物	必要機能の原理を単一システムとして統合（パッケージング）したり、ハードウェア・情報システムなどの構築など。
標準化活動	標準ドキュメント。レイヤーアーキテクチャや、レイヤー間インタフェース、モジュールインタフェース、内部バス、通信プロトコルなど。

表 5.1: 量子インターネットを実現するプロジェクトで達成される成果の例。

に、成果の形を例示する。量子インターネットというシステム、そしてインフラの実現を目指した研究開発では、研究要素と開発要素の距離が近く、研究者が研究だけに取り組むことも、開発者が開発だけに取り組むことも難しい。研究と開発の距離が近いと、研究者が開発に関与するモチベーションや、開発者が研究に関与するモチベーションが重要である。実働を担う若手研究者は、キャリア形成上、論文にならない仕事、すなわち、量子インターネットに関係する部分の中でも、基礎科学である物理学に係る理論や原理実証以外の研究に取り組みにくい。これは、大学などの採用や競争的研究費の申請評価の際に論文の件数で研究者を評価することになっているという仕組みに由来する問題でもある。旧態依然とした、研究は論文だけ、開発は開発物だけという評価ではなく、既に実証された必要な機能を統合していくことや既に実証された科学を元にシステム構築していくこと、性能を向上させていくこと、標準化活動など、研究から一歩進んだ活動も研究者の成果として認めることが、国際的競争力を持って量子インターネットを実現していくために重要で

あると考えられる。これは、量子インターネットに限った話ではなく、複雑化・深化・細分化が進む最先端技術を基礎研究から開発・社会実装まで連続的に推し進め、世界に先駆けるために肝要と考えられる。

5.4 エコシステム

エコシステムの構築は、一般に、研究開発を効率的に推進してシームレスに社会実装に至るために必須である。特に量子インターネットにおいては、マルチステークホルダーモデルを健全に機能させるため、早い段階からエコシステムを構築し、ステークホルダー同士で連携して研究開発を進める必要がある。しかも、既存の現行インターネットとのインテグレーションになるため、シームレスな移行の準備も必用である。移行をやりやすいように、量子インターネットの研究開発の方向性を作っていくこともまた肝要である。量子アニーリングや Noisy Intermediate-Scale Quantum 量子コンピュータの研究開発では、日本は世界に先駆ける研究成果を持っていたものの、開発競争において海外企業に遅れを取ってしまった。この原因の 1 つは、エコシステムが存在しておらず、研究から開発への移行が適切な形でおこなわれなかったことがあると考えられる。この結果、量子コンピュータアーキテクチャや応用、エラー訂正機能を持つフルスペックの量子コンピュータの研究開発など、遅れを取り戻すチャンスはあるものの、ハードウェア開発で一度出遅れてしまったことによるハンディキャップは否めず、苦戦を強いられている。日本は量子インターネットにおいても重要な研究成果を持っており、二の轍を踏んで出遅れるわけにはいかない。研究から社会実装にシームレスに至るためのエコシステムの構築を早くから進める必要がある。

また、人材教育・供給も、エコシステムの重要な機能である。早いうちから量子インターネット人材を育て、産業界や官公庁に送り込んでおくと、いざ開発に至った際に手戻りなく量子インターネット敷設を進めることができる。

5.5 国際連携

世界中の英知を結集するという観点では、現在量子インターネットは欧州や米国など諸外国でも重要な課題として積極的に推進されているため、それらの重要拠点と意見交換を行ったり日米欧のワークショップを開く等が考えられる。最終的には彼らと協力し、彼らのテストベッドなどと相互接続して、グローバルに 1 つのインフラを作っていく必要がある。このため、通信の仕様決定や標準化などにおいて積極的に協力していく強いモチベーションがある。インターネットの標準化団体 IETF [1] の長期目標を見据える姉妹団体 IRTF [2] での活動として、量子インターネットのアーキテクチャ概念を整理する世界初のドキュメントが、世界的に共同執筆され、日本からも研究者が参加しているのは、良い皮切りである [26]。

[1] https://www.ietf.org/
[2] https://www.irtf.org/

執筆体制

主筆	永山翔太	株式会社メルカリ	シニアリサーチャー
	生田力三	大阪大学	助教
	小坂英男	横浜国立大学	教授
	佐々木寿彦	東京大学	講師
	高橋優樹	沖縄科学技術大学院大学	准教授
	根本香絵	国立情報学研究所	教授
	堀切智之	横浜国立大学	准教授
	山崎歴舟	国際基督教大学	准教授
	山本俊	大阪大学	教授
	Rodney Van Meter	慶應義塾大学	教授

連絡先: contact@qitf.org

更新履歴

2021 年 2 月 10 日　version 1.0 公開。

2021 年 2 月 22 日　QIA の量子中継の実証（2021 年 2 月報告）について追記。version 1.1 公開。

関連図書

[1] H.-J. Briegel, W Dür, J I Cirac, and P Zoller. Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. *Physical Review Letters*, 81(26):5932–5935, dec 1998.

[2] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical review letters*, 87(16):167902, 2001.

[3] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS*, pages 517–526, 2009.

[4] Tomoyuki Morimae and Keisuke Fujii. Blind topological measurement-based quantum computation. *Nature Communications*, 3(1):1–6, sep 2012.

[5] Lov K. Grover. Quantum Telecomputation. apr 1997.

[6] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello. Distributed quantum computation over noisy channels. *Physical Review A - Atomic, Molecular, and Optical Physics*, 59(6):4249–4254, 1999.

[7] Rodney Van Meter, W. J. Munro, Kae Nemoto, and Kohei M. Itoh. Distributed arithmetic on a quantum multicomputer. *Proceedings - International Symposium on Computer Architecture*, 2006:354–365, 2006.

[8] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin. A quantum network of clocks. *Nature Physics*, 10(8):582–587, 2014.

[9] Daniel Gottesman, Thomas Jennewein, and Sarah Croke. Longer-baseline telescopes using quantum repeaters. *Physical Review Letters*, 109(7):1–5, 2012.

[10] A. M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, s2-42(1), 1937.

[11] D. Deutsch. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of The Royal Society of London, Series A: Mathematical and Physical Sciences*, 400(1818):97–117, jul 1985.

[12] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412), oct 2018.

[13] Matteo Pompili, Sophie L. N. Hermans, Simon Baier, Hans K. C. Beukers, Peter C. Humphreys, Raymond N. Schouten, Raymond F. L. Vermeulen, Marijn J. Tiggelman, Laura dos Santos Martins, Bas Dirkse, Stephanie Wehner, and Ronald Hanson. Realization of a multi-node quantum network of remote solid-state qubits. pages 1–28, 2021.

[14] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, and R. Hanson. Heralded entanglement between solid-state qubits separated by three metres. *Nature*, 497(7447):86–90, 2013.

[15] W. Pfaff, B. J. Hensen, H. Bernien, S. B. Van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, M. Markham, D. J. Twitchen, and R. Hanson. Unconditional quantum teleportation between distant solid-state quantum bits. *Science*, 345(6196):532–535, 2014.

[16] B. Hensen, N. Kalb, M. S. Blok, A. E. Dréau, A. Reiserer, R. F.L. L Vermeulen, R. N. Schouten, M. Markham, D. J. Twitchen, K. Goodenough, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free Bell test using electron spins in diamond: second experiment and additional analysis. *Scientific Reports*, 6(1):30289, aug 2016.

[17] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical Review Letters*, 76(5):722–725, jan 1996.

[18] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J.W. Bakermans, S. J. Kamerling, N. H. Nickerson, S. C. Benjamin, D. J. Twitchen, M. Markham, and R. Hanson. Entanglement distillation between solid-state quantum network nodes. *Science*, 356(6341):928–932, jun 2017.

[19] Axel Dahlberg, Julio de Oliveira Filho, Ronald Hanson, Stephanie Wehner, Matthew Skrzypczyk, Tim Coopmans, Leon Wubben, Filip Rozpędek, Matteo Pompili, Arian Stolk, Przemysław Pawełczak, and Robert Knegjens. A link layer protocol for quantum networks. In *Proceedings of the ACM Special Interest Group on Data Communication - SIGCOMM '19*, pages 159–173, New York, New York, USA, 2019. ACM Press.

[20] Han Sen Zhong, Hui Wang, Yu Hao Deng, Ming Cheng Chen, Li Chao Peng, Yi Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, Peng Hu, Xiao Yan Yang, Wei Jun Zhang, Hao Li, Yuxuan Li, Xiao Jiang, Lin Gan, Guangwen Yang, Lixing You, Zhen Wang, Li Li, Nai Le Liu, Chao Yang Lu, and Jian Wei Pan. Quantum computational advantage using photons. *Science*, 370(6523), 2021.

[21] Juan Yin, Yuan Cao, Yu Huai Li, Sheng Kai Liao, Liang Zhang, Ji Gang Ren, Wen Qi Cai, Wei Yue Liu, Bo Li, Hui Dai, Guang Bing Li, Qi Ming Lu, Yun Hong Gong, Yu Xu, Shuang Lin Li, Feng Zhi Li, Ya Yun Yin, Zi Qing Jiang, Ming Li, Jian Jun Jia, Ge Ren, Dong He, Yi Lin Zhou, Xiao Xiang Zhang, Na Wang, Xiang Chang, Zhen Cai Zhu, Nai Le Liu, Yu Ao Chen, Chao Yang Lu, Rong Shu, Cheng Zhi Peng, Jian Yu Wang, and

Jian Wei Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, jun 2017.

[22] Zheng Da Li, Rui Zhang, Xu Fei Yin, Li Zheng Liu, Yi Hu, Yu Qiang Fang, Yue Yang Fei, Xiao Jiang, Jun Zhang, Li Li, Nai Le Liu, Feihu Xu, Yu Ao Chen, and Jian Wei Pan. Experimental quantum repeater without quantum memory. *Nature Photonics*, 13(9):644–648, sep 2019.

[23] Vinton Cerf, Dalal Yogen, and Sunshine Carl. Specification of Internet Transmission Control Program. RFC 675, dec 1974.

[24] Howard Barnum, Carlton M. Caves, Christopher A. Jozsa, Richard Jozsa, and Benjamin Schumacher. Noncommuting mixed states cannot be broadcast. *Physical Review Letters*, 76(15):2818–2821, apr 1996.

[25] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "Event-ready-detectors" Bell experiment via entanglement swapping. *Physical Review Letters*, 71(26):4287–4290, dec 1993.

[26] Wojciech Kozlowski, Stephanie Wehner, Rodney Van Meter, Bruno Rijsman, Angela Sara Cacciapuoti, Marcello Caleffi, and Shota Nagayama. Architectural Principles for a Quantum Internet. Internet-Draft draft-irtf-qirg-principles-05, Internet Engineering Task Force, sep 2020.

[27] Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing - STOC '04*, page 128, New York, New York, USA, 2004. ACM Press.

[28] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[29] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical Review Letters*, 103(15):1–4, 2009.

[30] Seiichiro Tani, Hirotada Kobayashi, and Keiji Matsumoto. Exact quantum algorithms for the leader election problem. In *Lecture Notes in Computer Science*, volume 3404, pages 581–592. Springer Verlag, 2005.

[31] Michael Ben-Or and Avinatan Hassidim. Fast quantum byzantine agreement. In *Proceedings of the Annual ACM Symposium on Theory of Computing*, pages 481–485, New York, New York, USA, 2005. ACM Press.

[32] François Le Gall and Frédéric Magniez. Sublinear-time quantum computation of the diameter in CONGEST networks. In *Proceedings of the Annual ACM Symposium on Principles of Distributed Computing*, pages 337–346, New York, NY, USA, jul 2018. Association for Computing Machinery.

[33] Rikizo Ikuta, Toshiki Kobayashi, Tetsuo Kawakami, Shigehito Miki, Masahiro Yabuno, Taro Yamashita, Hirotaka Terai, Masato Koashi, Tetsuya Mukai, Takashi Yamamoto, and Nobuyuki Imoto. Polarization insensitive frequency conversion for an atom-photon entanglement distribution via a telecom network. *Nature Communications*, 9(1), dec 2018.

[34] Kazuya Tsurumoto, Ryota Kuroiwa, Hiroki Kano, Yuhei Sekiguchi, and Hideo Kosaka. Quantum teleportation-based state transfer of photon polarization into a carbon spin in diamond. *Communications Physics*, 2(1), dec 2019.

[35] Kazuya Niizeki, Daisuke Yoshida, Ko Ito, Ippei Nakamura, Nobuyuki Takei, Kotaro Okamura, Ming Yang Zheng, Xiu Ping Xie, and Tomoyuki Horikiri. Two-photon comb with wavelength conversion and 20-km distribution for quantum communication. *Communications Physics*, 3(1):1–7, dec 2020.

[36] Atsushi Noguchi, Rekishu Yamazaki, Yutaka Tabuchi, and Yasunobu Nakamura. Single-photon quantum regime of artificial radiation pressure on a surface acoustic wave resonator. *Nature Communications*, 11(1):1–6, dec 2020.

[37] Hiroki Takahashi, Ezra Kassa, Costas Christoforou, and Matthias Keller. Strong Coupling of a Single Ion to an Optical Cavity. *Physical Review Letters*, 124(1):13602, 2020.

[38] Koji Azuma, Kiyoshi Tamaki, and Hoi-Kwong Lo. All-photonic quantum repeaters. *Nature Communications*, 6:6787, 2015.

[39] Yasushi Hasegawa, Rikizo Ikuta, Nobuyuki Matsuda, Kiyoshi Tamaki, Hoi Kwong Lo, Takashi Yamamoto, Koji Azuma, and Nobuyuki Imoto. Experimental time-reversed adaptive Bell measurement towards all-photonic quantum repeaters. *Nature Communications*, 10(1), dec 2019.

[40] Anna Tchebotareva, Sophie L.N. Hermans, Peter C. Humphreys, Dirk Voigt, Peter J. Harmsma, Lun K. Cheng, Ad L. Verlaan, Niels Dijkhuizen, Wim De Jong, Anaïs Dréau, and Ronald Hanson. Entanglement between a Diamond Spin Qubit and a Photonic Time-Bin Qubit at Telecom Wavelength. *Physical Review Letters*, 123(6):063601, aug 2019.

[41] P. Zarkeshian, C. Deshmukh, N. Sinclair, S. K. Goyal, G. H. Aguilar, P. Lefebvre, M. Grimau Puigibert, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, K. Heshami, D. Oblak, W. Tittel, and C. Simon. Entanglement between more than two hundred macroscopic atomic ensembles in a solid. *Nature Communications*, 8(1):1–10, dec 2017.

[42] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin. Experimental demonstration of memory-enhanced quantum communication. *Nature*, 580(7801):60–64, 2020.

[43] Takaaki Matsuo, Clément Durand, and Rodney Van Meter. Quantum link bootstrapping using a RuleSet-based communication protocol. *Physical Review A*, 100(5), 2019.