量子インターネットの可能性

永山 翔太 ●株式会社メルカリ 研究開発部R4D シニアリサーチャー／量子インターネットタスクフォース 代表

暗号通信ほか情報処理社会を変革する次世代ネットワーク技術として期待される量子インターネット。早期にアーキテクチャの研究に取り組み、技術の現状と進展を折り込みながらの試作開始が求められる。

量子インターネットは広域の量子コンピューターネットワークであり、実現に向けて研究開発が世界的に推進されている。ご存じの通り、量子コンピューターは次世代計算機として大いに話題を呼んでいる。特にここ10年の発展が目覚ましく、既にスパコンでも解けない（人工的な）問題を解けるようになっており、もう10年もすれば実用的な問題も解けるとみられている。これは、量子コンピューターは量子力学に立脚して動作する量子ビットで作られた計算機であり、現行のいわゆるデジタルコンピューターとは異なる計算特性を持っているためである。得意な情報処理内容が異なり相補的に利用できることで、今日の情報処理社会をさらに発展させると期待されている。

量子インターネットは量子ビットでつながる（量子）コンピューターネットワークであり、同様に、ビットから成る今日のインターネットと相補的に利用されていくであろう[1]。ハードウエア的に考えれば、量子インターネットは量子的な光通信インターフェースを持つ量子コンピューター同士のネットワークである。このネットワークが構築するサイバー空間はいわば「量子サイバー空間」とでも呼ぶべきものであり、そのため今日のインターネットとは異なる処理を得意とするサイバー空間となる。

■量子インターネットへの期待

インターネットの課題を量子インターネットで解決する研究がある。これらを順番に見ていこう。

●暗号通信

量子コンピューターの計算力による恩恵が期待される一方で、その計算力による公開鍵暗号解読により、暗号によって成り立っている現代のオンライン経済・オンライン社会全般の崩壊リスクが現実的な脅威になりつつある。国際通貨基金（IMF）もリスクを指摘し、対策の必要性を訴えている[2]。

現行暗号のセキュリティは、暗号解読の実行に必要な情報がインターネットに流れており盗聴者もその情報を入手できてしまうが、解読の計算に非現実的な時間（1万年など）がかかるため、現実的には安全となっている。一方、量子インターネットによる暗号は、暗号解読に必要な情報が（量子）インターネット上を流れない仕組みとなっており、理論的に、どれだけの時間をかけても解読が不可能となっている[3][4][5]。

●クラウドのセキュリティ

昨今注目を集める秘匿計算においても、量子イ

ンターネットへの期待がある。クラウドからの漏えいは大きなセキュリティリスク・プライバシーリスクであり、これを解決するのがデータを暗号化したまま情報処理を行う秘匿計算だ。しかし、デジタル情報における秘匿計算には爆発的に大きな計算オーバーヘッドがかかることが分かっており、ある程度の大きさのデータしか処理できない。

一方、量子インターネットと量子コンピューターを用いる量子秘匿計算のオーバーヘッドは、軽いものであることが分かっている[6]。また、データのみならず、クラウド上で実行するプログラムすら暗号化できるため、社外秘のアルゴリズムをクラウドで安全に実行できるなど、さらに便利になる。

●高精度な時刻同期

高精度な時刻同期の需要もある。株取引のような大量のリクエストが到来する分散サーバー間のデータ同期は言わずもがな、自動運転の高精度化などに資するGPSの高精度化などフィジカル空間にも大きく影響する。量子ネットワークを利用すると、高精度な時刻同期が可能であることが分かっている[7]。

●分散量子コンピューティング

ある問題を解くための計算操作に必要なステップ数が小さくなるため、量子コンピューターは古典コンピューターよりも速い。実は、量子インターネットも、同様の利得を生み出せる。ただし、量子インターネットの場合、分散タスクを処理する際に必要となる通信回数が小さくなる。例えば、分散環境におけるコンピューター間の合意形成はシステムの信頼性に強く関わる問題であり、需要のあるタスクである。

量子インターネットを用いると、このタスクを古典インターネットよりも高速に実行可能であることが分かっている。合意形成をより高速に実施できるようになれば、開けてくる世界もあるだろう[8]。

●超長基線望遠鏡による宇宙からの微弱信号観測

宇宙からの微弱な信号を検出する超長基線望遠鏡は、量子インターネットによってさらに弱い信号を検出できるようになる。これは量子センサーネットワークの一種だ。量子インターネットを用いる超長基線電波望遠鏡により、遠くの天体の大きさが分かったり、宇宙を飛び交っている信号をさらに正確に検出できるようになったりすることで、天文学や宇宙物理学の発展に寄与するかもしれない[9]。

■歴史的情勢

Quantum Internet（量子インターネット）という言葉が論文に登場したのは2008年にさかのぼる[10]。素因数分解を実行できるShorのアルゴリズム[11]の発見によって第1次量子コンピューターブームが起こった1990年代後半と、超伝導量子コンピューターにおけるブレークスルー[12]によって第2次量子コンピューターブームが起こった2010年代の、ちょうど間の時期だ。

ただ、この時に提案されたネットワークは量子コンピューターを光子で物理的にただ連結しただけのものであり、今日のインターネットをグローバルで不可欠なインフラたらしめているような賢いアーキテクチャやシステム、ソフトウエアについては検討されていなかった。

その後、基礎研究が重ねられた。量子インターネットは光通信インターフェースを持つ量子コンピューターネットワークであることから、量子コンピューター研究の進展とともに量子インターネット研究も進展した。その中には、量子

ビットから光子を打ち出したり、逆に吸収したりする研究や、そこで培った技術を応用して離れた量子ビット間に量子もつれを作るような研究があった。

インターネットの人間として興味深いのは、量子インターネットにおいても「通信波長」を利用する動きがあることである[13]。

通信波長は、今日我々が利用している光ファイバーに光を通す際に利用される、光ファイバーにおいて光の減衰率が小さくなる波長帯である。一方、量子ビットが直接送受信できる光子の波長は、その量子ビットに利用している原子種や技術に依存する。そのような、例えば可視光帯の波長の光子を、量子状態を壊さないように、通信波長に「量子波長変換」して今日の光ファイバーを利用しようとする一連の研究がある。

また、量子ネットワークのアーキテクチャやソフトウエアに関する研究も始まった。アーキテクチャには、分散量子コンピューターアーキテクチャ[14]を研究する流れと、量子ネットワークアーキテクチャ・量子インターネットアーキテクチャ[15]を研究する流れがある。これらは密接に関係しており、デジタル情報技術の研究者も参入している。筆者の研究分野もここであり、量子インターネットのプロトコルスタックについて研究している[16]。また、理論研究として、量子インターネットの通信容量に関する研究や、量子インターネット上で実行できるアルゴリズムやアプリケーションの研究も盛んになった。

そのような進展がある中、2010年代末から各国は大型プロジェクトを発起するようになった。口火を切ったEUは2018年に、その大型量子研究開発構想である「Quantum Flagship」の中で、オランダを拠点とするプロジェクトである「Quantum Internet Alliance」を開始した（2018～2021年）[17]。この第1期量子インターネットアライアンスは4年で1000万ユーロのプロジェクトであり、量子インターネットのテストベッドを志向するものであった。

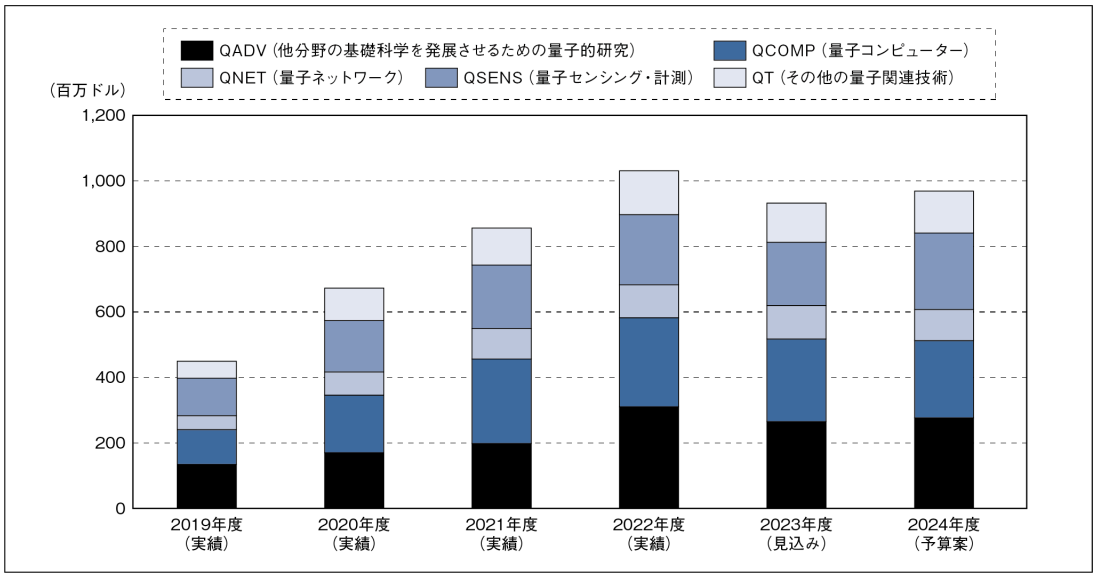
当初は2020年に、オランダのデルフト－アムステルダム－ハーグ－ライデンを接続する広域量子インターネットテストベッドを構築する予定とされていた。コロナ禍もあってその目標は達成できずに修正されたようだが、2021年に重要マイルストーンである量子信号中継の原理実証を、ダイヤモンド内に作る量子ビットを用いて達成した。EUは2022年から、さらに3年半で2400万ユーロの追加投資を行い、量子インターネット研究を強く後押ししている（2022～2025年）[18]。

米国は、EUに追従するように、2020年から量子インターネットへの集中投資を開始した。米国では当時「National Quantum Initiative 法」が量子技術の研究開発を広く支援しており、特に量子コンピューターに関する取り組みが重点化されていた。米国は2022年にこの法律に改正して量子ネットワークをさらに重点化し、エネルギー省や科学技術政策局、国立標準技術研究所（NIST）などを通して、大学、国立研究所、企業の研究を後押ししている（5年間で最大1億ドル以上／年）[19]。

そもそも米国は一部のトップスクールに限らず各地の大学や国研がおのおのの強みを持って盛んに研究開発活動を行っており、これを下地として量子インターネットテストベッドを掲げるプロジェクトが各地に発足した。この数は年々増えている。

日本も量子インターネットの基礎研究で強みを持っている。しかし、これらを生かすためには、また実際に量子インターネットをつくるためには、これらを糾合する異分野連携コミュニティが必要であった。このための活動を筆者は2018年から始め、2019年に、研究者の集まりとして量子インターネットタスクフォースを立ち上げ

資料1-1-3　米国の量子情報科学（QIS）の研究開発におけるPCA（Program Component Area）別内訳



出所：NSTC, National Quantum Initiative Supplement to the President's FY 2024 Budget, Dec., 2023

た[20]。30年後に責任を持てる体制とするため若手をボードメンバーとし、実績ある研究者にアドバイザーとなってもらい、量子インターネットについての理解を広める活動や、社会実装までの道筋を描くホワイトペーパーを執筆・公開した[21]。

一方、日本政府は、誤り耐性型量子コンピューターの実現を目指す超大型プロジェクトである科学技術振興機構（JST）のムーンショット型研究開発事業の目標6において、分散量子コンピューターを実現するための量子ネットワークに関する研究プロジェクトを立ち上げた[22]。これには物理に関する複数のプロジェクトが存在するほか、筆者自身もテストベッド環境を整備してデータセンターサイズの量子コンピューターネットワークのプロトタイプ実装を行うプロジェクトを提案するとともに、プロジェクトマネージャーを務めている。今日のインターネットがコンピューターネットワークであることを考えれば、量子コンピューターネットワークを実現するプロジェクトが量子インターネットと深い関わりを持つことは想像にたやすい。

このようなプロジェクトを文部科学省が支援する一方で、総務省は、より長距離での量子通信を実現するプロジェクトを立ち上げた。量子インターネットタスクフォースでは多拠点接続の手始めとして、慶應義塾大学の矢上キャンパスと新川崎タウンキャンパスの間をつなぐ約4kmのダークファイバーを確保し、キャンパス間接続の準備を進めている。WIDEプロジェクトでも、全光ネットワークの実験に相乗りする形で、都心のファイバー網を用いる実験を計画中だ。

TCP/IPなどインターネットの通信標準を策定するIETF（Internet Engineering Task Force）は、その姉妹団体であり研究段階の技術を扱うIRTF（Internet Research Task Force）に、量子インターネットのリサーチグループ（Quantum Internet Research Group：QIRG）を設置した[23]。量子インターネットの設計指針を論じるinformational

RFCが、QIRG初のRFCとして発行された[24]。

量子コンピューターのプロトタイプ試作は2010年代に始まった。このプロトタイプは、不完全であることを前提としていた。例えば、量子ビットの数が極端に少なく、エラーだらけで、普通の計算機としてはとても使い物にならない。しかし、この試作によって工学的な研究が進み、アルゴリズムを含む重要な理論研究も大きく刺激した。2020年代は、量子インターネットにおいてもこのような試作が始まる時代になるだろう。

■量子インターネットの定義

実際のところ、量子インターネットの定義ははっきりしていない。そのような現状で筆者の考える量子インターネットの定義は、以下の2点である。

①ネットワークのネットワークであること
世の中に存在する運用主体で運用・管理できるネットワークのサイズにはおのずと限界がある。インターネットはあらゆるサイズのネットワーク同士を相互接続することで、世界規模のコンピューターネットワークとなることを可能にした。すなわち、技術的のみならず組織的・社会的にもスケーラブルであった。人類社会は多様なコミュニティ同士の連結で成り立っているため、量子インターネットもこの流れを踏襲するべきである。
②量子情報の汎用通信網であること
インターネットはデジタル情報におけるあらゆる分散・通信アプリケーションを載せられる汎用通信網であることで、ここまで大きくなった。

もちろん、ベストエフォート性やエンドツーエンド性などインターネットを支える重要な特徴や性質は他にもあるが、どのような特性が量子情報・量子通信の性質に適合しているかはまだ分からない。そこで、まずは上記の2点に的を絞って量子インターネットの研究を続け、その中で適切なアーキテクチャを見いだしていく方針が適切と考えられる。

■量子インターネット実現に向けて

量子インターネット実現への道程はまだ長い。量子的なハードウエアは変換技術が実現すれば局所的に交換・代替することが可能になるため、技術同士の切磋琢磨が起こるだろう。一方、インターネットのような広域コンピューターネットワークのアーキテクチャは、一度そのアーキテクチャを採用してインフラを敷設してしまうと更新するのが難しい。インフラ全体を交換する必要が出てきてしまうためだ。

この意味で、量子インターネットアーキテクチャは量子コンピューターアーキテクチャとは異なる難しさがあり、早期から注力することが重要である。世界と接続する必要もあるので、国際連携の重要性も特に高い。量子インターネットの研究開発は、インターネットで培ってきた知見を大いに生かしたい。

1. Science, Vol 362, Issue 6412, 2018
2. Deodoro, J. et. Al.,QuantumComputingandtheFinancialSystem:SpookyActionataDistance?,IMF,Mar. 12, 2021 https://www.imf.org/en/Publications/WP/Issues/2021/03/12/Quantum-Computing-and-the-Financial-System-Spooky-Action-at-a-Distance-50159/
3. Theoretical Computer Science, Volume 560, Part 1, Dec. 2014
4. Gottesman, D. et. Al., Quantum Digital Signatures, arXiv, Nov. 15, 2001 https://arxiv.org/abs/quant-ph/0105032
5. Physical Review Letters, Volume 87, 167902, 2001

6. npj Quantum Information, volume 3, Article number: 23, 2017
7. Physical Review Letters, Volume 85, 2010, 2000
8. Nagayama, S., Distributed Quantum Computing Utilizing Multiple Codes on Imperfect Hardware, arXiv, Apr. 9, 2017 http://arxiv.org/abs/1704.02620
9. Physical Review Letters, Volume 109, 070503, 2012
10. Nature, volume 453, pp.1023-1030, 2008
11. SIAM Journal on Computing, Volume 26, Issue 5, pp.1484-1509, Oct. 1997
12. Nature, volume 508, pp.500-503, 2014
13. Nature Communications, volume 9, Article number 1997, 2018
14. Computer, Volume 49, Issue 9, pp.31-42, 2016
15. Van M., R., Quantum Networking. John Wiley & Sons, Apr. 14, 2014
16. ACM, QuNet '23: Proceedings of the 1st Workshop on Quantum Networks and Distributed Quantum Computing, pp.25-30, Sep. 10, 2023
17. EC, Quantum Internet Alliance https://cordis.europa.eu/project/id/820445
18. QIA, The Quantum Internet Alliance will build an advanced European quantum internet ecosystem, Oct. 14, 2022 https://quantum-internet.team/2022/10/14/the-quantum-internet-alliance-will-build-an-advanced-european-quantum-internet-ecosystem/
19. National Quantum Initiative, Quantum in the CHIPS and Science Act of 2022, Aug. 9, 2022 https://www.quantum.gov/quantum-in-the-chips-and-science-act-of-2022/
20. 量子インターネットタスクフォース https://qitf.org/
21. 量子インターネットタスクフォース、"The" 量子インターネット、version 1.1、2021年2月22日 https://qitf.org/files/20210222_qitf_whitepaper.pdf
22. JST、ムーンショット型研究開発事業目標6 誤り耐性型汎用量子コンピュータ https://www.jst.go.jp/moonshot/program/goal6/
23. IRTF Quantum Internet Research Group (QIRG) https://www.irtf.org/qirg.html
24. RFC 9340, 2023

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dおよび株式会社インプレスが1996年～2024年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&Dおよび株式会社インプレスと著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | インプレス・サステナブルラボ | ✉ iwp-info@impress.co.jp