

# 「量子インターネット」で 何ができるか、何が変わるか

「量子コンピュータ」に続き、「量子インターネット」についての議論も活発になってきました。そもそも「量子インターネット」とは何か、また、実現すると何ができるのか、何が変わるのかについて解説します。

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

永山 翔太

## 量子インターネットに 期待される技術革新

### (1) 政府や企業が開発研究に乗り出した量子インターネット

量子インターネットは、量子コンピュータと同じく「量子情報」を取り扱う未来の情報通信インフラです。

量子コンピュータは、従来のコンピュータに比べ圧倒的な処理能力をもつと言われ、企業も巨額の予算を投入し、積極的に研究開発をリードしてきています。

量子インターネットにおいても、政府予算における研究開発投資額が増えてきました。いち早く重要性に気付いた企業も研究開発に乗り出していきます。このように、量子インターネットは、国や企業の趨勢にも大きく関わる技術であると考えられています。

### (2) 現在のインターネットと量子インターネット

未来の情報通信技術というと、beyond 5G や IOWN などの研究開発も実施されています。

実は、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」を送送するためのものです。一方、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通信技術です。

扱うデータの種類が異なると、その通信基盤で実行できる処理や解決できる問題が異なります。

量子コンピュータが技術革新を起こしていくことが期待されているのと同様に、量子インターネットをいまのインターネットと併用することで、より便利なIT社会を実現していくことが期待されています。

### (3) 現代のインターネットが抱える問題

現代のインターネットは、デジタル情報を高速・大容量に通信すること、時間と場所を超えた情報や意思の伝達を可能にし、社会を変革してきました。

コミュニケーションの内容も、メールやチャットのような人同士のコミュニケーションから、ウェブサイト閲覧のような人と機械(コンピュータ)のコミュニケーション、株の自動売買やキャッシュレス決済のような機械と機械のコミュニケーションなど多様化しています。

IT分野の調査・助言などを行なうアメリカの企業、ガートナーの調査によると、2020年の世界のIT支出額は約3兆7000億ドルと試算されています。

インターネットはITが活用される様々な場面で直接的にも間接的にも影響するもので、「インターネットの市場規模」だけを明確に切り出して算出するのは難しいですが、この数字に大きく貢献していることは疑う余地がありません。

しかしながら、現行のデジタル情報のインターネットには、未解決の課題が多くあります。

情報漏えいやハッキングといったセキュリティ・プライバシーの問題は年々深刻化しています。

データの重要性が増す一方で、ビッグデータは一部の企業によって独占されています。

また、ITを利用して恩恵を受けられる者と利用できずに恩恵を受けられない者の間に生じる、デジタルデバイドという新たな格差問題もあります。

#### (4) セキュリティ・プライバシー

##### 問題は技術が解決する

インターネットが抱える問題の

うち、ビッグデータの独占やデジタルデバイドを解決するためには、政治的な努力が必要になると言えるでしょう。

一方で、セキュリティ・プライバシーについては、個々人の努力や技術の発達により解決されることのできる問題と言えます。

まず、個々人の努力の面で言えば、データを預けているサーバの管理者が情報を漏らさないように契約を結び、サーバ管理者側はUSBメモリをサーバに接続しないようにするといったルールを守ることなどが求められます。

しかし、ヒューマンエラーを完全に防ぐことはできませんし、管理者の知識不足や悪意による情報漏えいのおそれもあります。

そのため、技術の発達による解決が望ましいと言えるでしょう。

これまでの現代インターネットにおける技術では、情報を守る側の技術の発達と攻撃する側の技術の発達によるいたちごっこにより、決定的な解決に至ることはありませんでした。

しかし、デジタル情報とは根本的に異なる仕組みをもつ量子情報を扱う量子インターネットであれば、このような問題を根本的に解

決することができると考えられています。

## 量子インターネットの仕組み

### (1) ミクロ世界の量子力学を利用したインターネット

量子情報を利用する量子インターネットは、「量子もつれ」と呼ばれる現象を用いています。

量子情報は、ミクロ世界でのみ現われる力学である量子力学によってつくられる情報理論です。

量子コンピュータや量子インターネットといった量子情報技術がなぜ注目されるのか、この仕組みから解説していきます。

### (2) 量子情報の不思議な仕組み①「重ね合わせ」

いま、私たちが使っているコンピュータ、つまりデジタルの計算基本要素である「ビット」は、電気が溜まっているか否かで「0」と「1」を表現して計算を行います。ちなみに、ビットとは、2進数を意味する「binary digit」からきた言葉です。

一方、量子情報を取り扱う量子コンピュータの計算基本要素であ

る「量子ビット」は、不思議なことに、量子ビットそのままの状態では0か1かが、はっきりしていません（重ね合わせ）。量子ビットを「測定」することで、0か1かがはっきりします。

マクロ世界の住人である私たちにはわかるように、測定によって翻訳することで、ミクロ世界の情報である量子情報を、マクロ世界の情報であるデジタル情報に変換します。

量子ビットを測定してデジタル情報を取得するときに0が出るか1が出るかは確率的に決まりますが、量子力学世界の存在である量子ビット自体は、0が出る確率と1が出る確率を保持しているわけではありません。

量子ビットがもっているのは、もつと成分とでも言うべきパラメータです。

量子コンピュータのプログラムの量子ビットは、計算開始時にはすべての値が同確率で出るパラメータをもっています。この成分を操作して、答えとしてもつと適切な値が計算終了時の測定で高い確率で出るようになっていきます。この成分の操作については、次項で解説していきます。

### (3) 量子情報の不思議な仕組み②

#### 「量子もつれ（+重ね合わせ）」

量子ビットが2つあるとき、そこには、0と1だけがあつて、自身の成分を操作して0と1それぞれが出る確率を操作できるサイコロが2つあるようなものです。

この2つのサイコロの出目は、00、01、10、11の4パターンがあり得ます。

私たちの常識によると「左のサイコロを振って1が出たら右のサイコロも必ず1が出る。しかも、何回振り直しても」という事象は起こり得るでしょうか？ もちろん起こりません。左のサイコロの出目に関係なく、右のサイコロの出目はランダムに出てきます。しかし、量子情報ではこのような事象が起こります。

2つの量子ビットがあると、重ね合わせにより、前述の4パターンの値が出る成分があるわけですが、成分操作によって、01と10が出る成分を完全に消滅させることもできます。すると、00と11の成分だけが残るので、「左のサイコロで0（1）が出たら右のサイコロも必ず0（1）が出る」という状態がつかれます（図）。

このような、サイコロの出目が

なぜか揃つてしまう量子ビット同士

の関係を「量子もつれ」と呼びます。量子もつれは運命の赤い糸のようなもので、一度もつれると、どれだけ離れていようと、この関係性は持続します。

量子インターネットは、この量子もつれを地球上のあらゆる場所の間でつくれるようにし、通信アプリケーションに利用しようという通信インフラです。

#### 実現すると

#### 何ができるようになるのか

### (1) 量子インターネットに期待される応用技術

量子インターネットのアプリケーションの研究開発はまだ始まったばかりですが、セキュリティ・プライバシーについての応用が期待されています。

ほかにも、強力な計算力をもつ量子コンピュータ同士を接続してさらに強力な計算力をもたせるのも有力な使い方ですし、量子ビットコインのような活用方法も提案されています。

ここからは、量子インターネットのアプリケーションについて解説していきます。

### (2) 暗号システム

現在の暗号システムは、解読に必要な情報がすべてインターネット上を飛び交っています。

しかし、解読に1万年かかるなど、膨大な計算時間が必要になるため、実際的には安全という論理です。

このような安全性は「計算量的安全性」と呼ばれています。しかし、現用されている暗号システムは、解読のための量子アルゴリズムがすでに発見されており、量子コンピュータの前には無力であるという将来的な課題があります。

一方、量子インターネットの暗号システムは、解読に必要な情報がインターネット上を流れない仕組みになっています。

未来永劫どのようなコンピュータが開発されて、攻撃者がそれを用いようとも、そもそも暗号解読に必要な情報が不足しているので解読できません。

このような安全性は「情報理論的安全性」と呼ばれています。量子インターネットの暗号システムが実現すると、暗号開発と解読のいちごっこにも終止符を打てます。また、秘匿性のための暗号のみならず、なりすましを防ぐ認証

を担う量子暗号システムもすでに提案されています。

### (3) 安全なデータ処理

現在、データ処理をクラウドなどのサーバで実行することが日常的になっていますが、この仕組みには、サーバの管理者がデータを閲覧できてしまうという根本的課題があります。

これを解決できるのが、秘匿計算と呼ばれる技術です。秘匿計算では、データを暗号化したままデータ処理を実行します。暗号化を解除しないことにより、サーバ管理者によるデータ閲覧は原理的に不可能になるわけです。

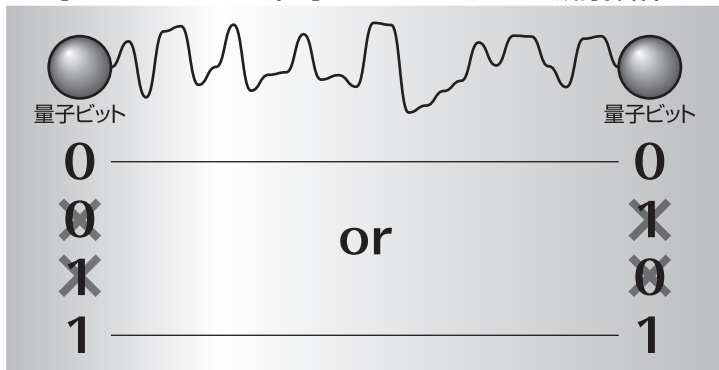
しかし、デジタルコンピュータによる秘匿計算は処理にかかる負荷が大きく、また、実行できるデータ処理も限られており、現実的ではありませんでした。一方で、量子インターネットと量子コンピュータによる秘匿量子計算は、処理にかかる負荷も小さいため、セキュリティやプライバシーへの応用が期待されています。

### (4) 量子コンピュータによる並列計算（分散量子計算）

コンピュータを接続して計算す



## ■量子もつれのイメージ(量子インターネットによる成分操作)



ることの意義が、現在のデジタルコンピュータと量子コンピュータではまったく異なります。

現在のデジタルコンピュータでは、2台のコンピュータがあっても、計算力はただか2倍になるだけです。

量子コンピュータでは、たとえば10量子ビットをもつ量子コンピュータは、2の10乗(1024)個の解の候補のなかから、1つの答えを見つけてきます。10量子ビットをもつ量子コンピュータ

タが2台あると、量子もつれを使ってお互いの量子ビット同士を接続することで、2の20乗(約100万)個の解の候補のなかから1つの答えを見つけてこられるようになります。

量子インターネットは、よりたくさんさんの量子コンピュータ同士を接続するための量子情報通信を担います。これにより、量子コンピュータのアプリケーションである量子化学計算や量子金融計算、量子機械学習、最適化や意思決定などで、より複雑で大きなデータを使った処理も実行できるようになります。

### (5) 今後広がる活用方法

前述した技術のほかに、微弱な電波が宇宙のどの方向から飛んできているのか正確に観測するための超長基線宇宙望遠鏡、量子センサーを繋げて医療応用や環境応用が見込まれる量子IoT、量子ビットコインの構築など、多様な応用が提案されています。

IoTやビットコイン、それにクラウドも、デジタルのインターネットが開発されて30年以上経って普及した技術です。

量子インターネットにおいて

も、実際に量子インターネットが開発されてから、いまはまだ考えられていない技術やアプリケーションが研究開発され、私たちの生活をさらに豊かにしてくれることが期待されます。

## 量子インターネットが社会に与える影響

### ●量子トランスフォーメーション(QX)

デジタル情報技術により社会や産業の構造をつくり変えるデジタルトランスフォーメーション(DX)が叫ばれて久しいですが、DXはデジタル情報の通信と計算の爆発的發展を両輪としたIT革命により可能となりました。

量子情報技術でも同様に、量子インターネットと量子コンピュータの発展により、量子情報技術を前提とした社会構造・産業構造への変革、量子トランスフォーメーション(QX)が引き起こされると予想されます。

そのようなQXの時代には、現在のインターネットでは解決できていない人類の課題を量子インターネットが解決していくと期待されます。

## 量子インターネット 実現までの道筋

量子インターネットは量子情報技術の総合格闘技です。社会実装が進む量子暗号ネットワークの技術や、盛んに研究されている量子コンピュータの技術を活かしつつ、様々な研究開発が必要になります。

量子コンピュータや、医療や環境問題への応用が考えられる量子センサーの研究開発が進むにつれ、それらを量子的に接続したい、量子データをもっと詳しく分析して人々のために役立てたいという社会的要請が高まることで、量子インターネットの研究はどんどん加速していくでしょう。

量子インターネットの研究開発は、必要な技術の実験室内原理実証が出揃ってきた段階です。量子インターネットの実現は長期に及ぶ困難な研究課題ですが、現在のインターネットだけでは解決できない社会問題を解決する次世代通信インフラとなるので、着実に取り組んでいく必要があります。

量子インターネットは、人類の今後を左右する重要課題です。▲

ながやま しょうた 専門は量子インターネット。とくに量子エラー訂正符号およびインターネットアーキテクチャ・通信プロトコル。2018年度末踏タゲット事業に採択され「分散量子計算プラットフォーム」プロジェクトを実施。