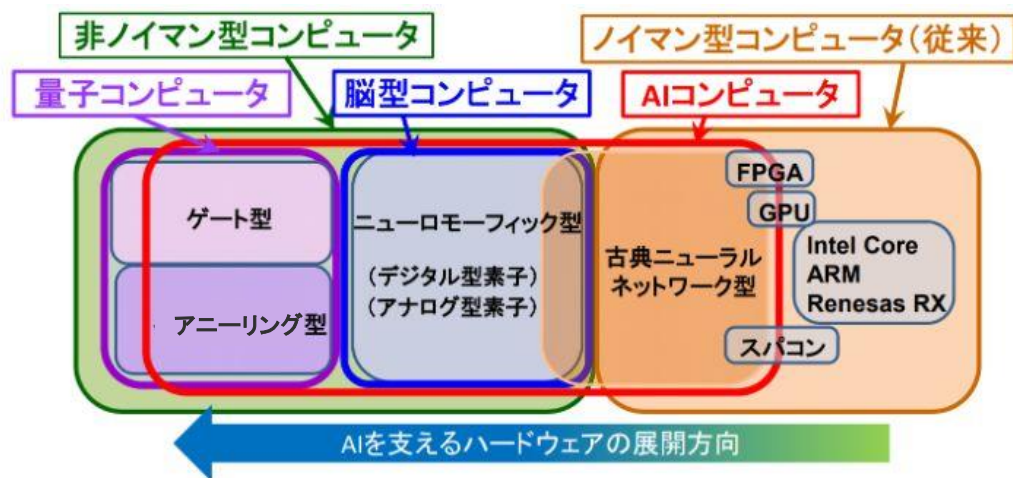


# 基礎レベル:テキスト

## 1 量子コンピュータとは？

量子力学〔[□](#)シラバス 2, 3〕特有の物理状態(量子特性)を積極的に用いて高速計算を実現するコンピュータのこと。

量子物理学以前の物理学を「古典物理学」と呼ぶことになぞらえ、従来のコンピュータを「古典コンピュータ」と呼ぶ。コンピュータのハードウェアから量子コンピュータを見ると、以下のように位置付けられる。



出典：平成30年度 NEDO『TSC Foresight』セミナー資料「人工知能を支えるハードウェア分野」を一部修正

量子コンピュータは大きく **量子ゲート** と **量子アニーリング** の2方式に分かれる〔[□](#)シラバス 4〕。量子ゲート方式は現在ノイズのある中規模の量子コンピュータ(NISQ)が開発されており、万能量子コンピュータを目指している〔[□](#)シラバス 6-1-1〕。

量子アニーリング方式と同じ組み合わせ最適化計算をするイジングマシンとの関連については[NTTデータ 量子コンピューティングガイドライン 量子アニーリング／イジングマシン編\(p.9\)](#)を参照のこと。

## 2 何がすごいのか？

近年は回路の集積が原子サイズにまで進んでおり、ムーアの法則の限界が指摘されている。また、AIやIoTの登場などにより社会の情報処理能力向上への要請はさらに高まっているが、並列方式でのデータ処理では消費電力も増大する。

量子コンピュータはこのブレークスルーとして期待されている。

## 3 何に使われているのか？

量子アニーリングでは組み合わせの最適化問題を解くことができ、現実の問題にも適用されている。中でも、D-Waveという商用アニーリングマシンが有名である。

量子ゲート方式では最適化問題に加え、量子化学・材料工学・サンプリング・量子力学、ひいてはセキュア・コンピューティング、暗号、機械学習、探索問題への適用が模索されている。〔[□](#)シラバス 5〕

## 4 参考文献

[量子コンピュータって何？ 動作の仕組みや開発ロードマップ、未来像を解説](#)  
[量子コンピューターの何が「すごい」のかー従来のコンピューターとの違いとは](#)  
[量子コンピュータとは | 古典コンピュータとの違い、実用化の最前線、AIとの関係まで](#)

## 1 ノイマン型コンピュータ(従来)

〔[目次](#)シラバス 7-1 古典との違い - 詳説〕を参照。

## 2 非ノイマン型コンピュータ

特定のタスクの処理に最適化された、ノイマン型に縛られないまったく新しい構造を持つコンピュータを指す。AIコンピュータやニューロモーフィック型、量子コンピュータも非ノイマン型コンピュータのうちの1つ。ただし、量子コンピュータはGPUやFPGA、TPU等が古典計算であるのに対して、量子性を使った量子計算であることが本質的に異なる。

## 3 GPU

Graphics Processing Unitの略。3Dグラフィックなどの画像処理に用いられているが、その高い演算性能から、GPGPU(General-purpose computing on graphics processing units)も数多く登場。定型的かつ膨大な計算を並列処理するのに適する。

## 4 FPGA

Field Programmable Gate Array の略。論理回路の構成を柔軟にハードウェア言語にて修正が出来るデバイス。FPGAを利用した製品として、高精細の液晶テレビや IBM Netezza といった高速集計のデータウェアハウスがある。近年はCloudでもFPGAを提供するサービスが出始めている。

## 5 ニューロモーフィック型

神経回路(脳)を模した構成の回路。ニューラル・ネットワークの仕組みを使うことで、従来のコンピュータ・システムのような記憶回路と演算回路を個別に搭載し、その間をデータ転送することで大量の電力を消費することと比べ、大幅な効率化を実現している。

## 6 量子コンピュータ(注意事項)

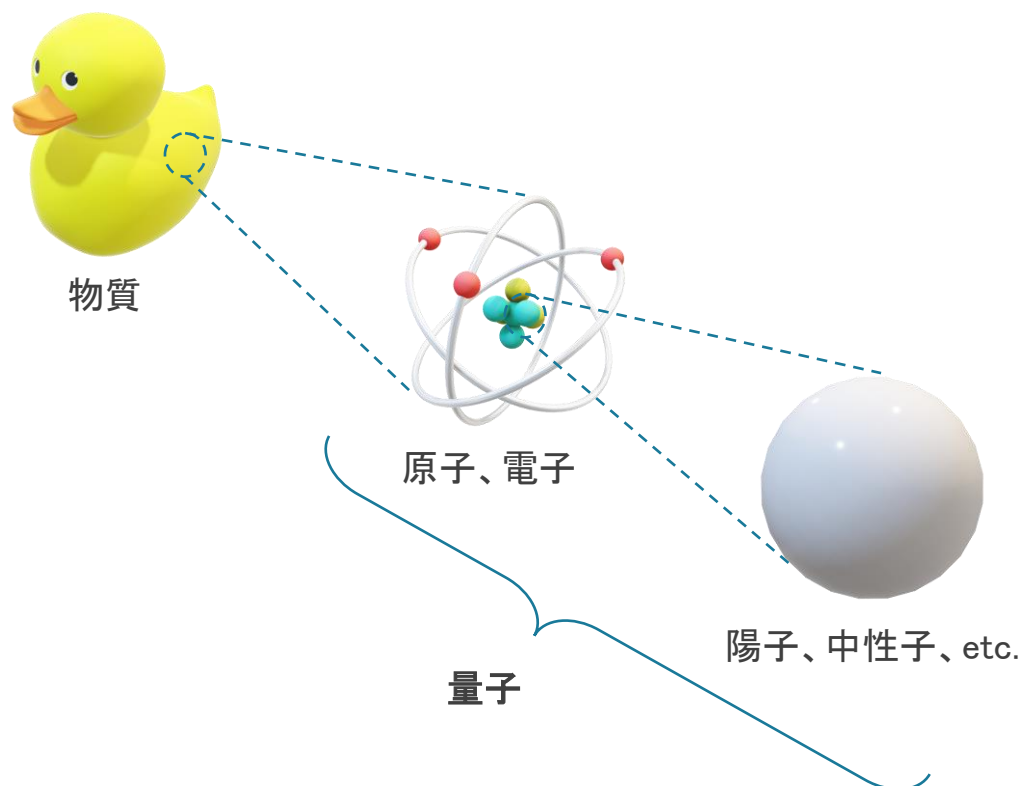
量子コンピュータは必ずしも1つ1つの計算処理が高速な訳ではなく、その計算原理を巧妙に利用して「計算ステップを劇的に減らす」ことで、計算時間を大幅に短縮できる点に本質がある。また、量子コンピュータが従来のコンピュータの完全上位互換であるとか全ての問題に向くというわけではなく、正確な計算やヒューリスティックな解、問題の種類・サイズによっても性能が異なり、アルゴリズム等を含めて見極めることが肝要となる。

## 7 参考文献

[量子コンピュータって何？ 動作の仕組みや開発ロードマップ、未来像を解説](#)  
[量子コンピュータとは | 古典コンピュータとの違い、実用化の最前線、AIとの関係まで](#)

## 1 量子とは？

物質やエネルギーを構成する、非常に小さな単位のこと。  
具体的には、電子や陽子、中性子、光子などを指す。



## 2 量子の世界では何が起きている？

量子スケールの世界では、我々が過ごす日常世界の物理学(量子に対し「古典物理」といわれる)が通用しない。

量子の”位置”や”速度”といった物理量は、量子が観測がされるまでは確率的にゆらいでおり、量子が観測されることにより初めて特定の値に決定される。

## 3 量子コンピュータへの応用

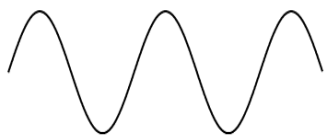
量子コンピュータ〔[□□シラバス 1](#)〕は、このような量子の性質を利用して従来のコンピュータ(量子コンピュータに対し「古典コンピュータ」といわれる)とは全く異なる仕組みで計算を実行することにより、古典コンピュータでは実現できなかった計算が実行できるようになると考えられている。

現在はハードウェアの開発だけでなく、ソフトウェアの開発や具体的な応用分野の模索などが進められている。

## 1 量子はどのような性質を持つ？

量子〔シラバス 2〕は、波と粒子の性質をあわせ持っている。

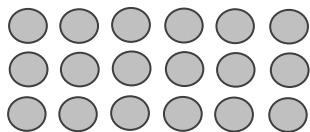
## ○波の性質



波（波動）は同じようなパターンが空間を伝播する現象のこと。波の性質には、反射、屈折、回折、干渉等がある。

この両方の性質を併せ持つことにより、量子はニュートン力学や電磁気学といった古典的な物理法則が通用せず、「量子力学」の法則に従う。

## ○粒子の性質

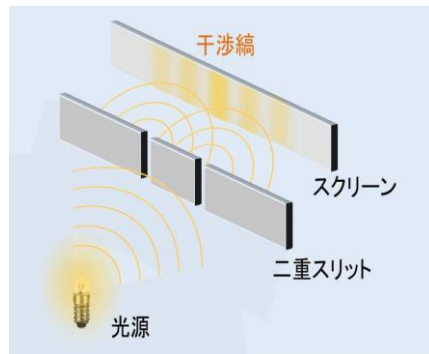


粒子は小さな粒状の物体の総称。粒子の性質は、一つの場所に存在すること（局所性）である。

## 2 波の性質を示す波の干渉とは？

複数の波の重ね合わせによって新しい波形ができることを干渉という。

右図は、光の干渉を確認する二重スリット実験である。二重スリットを通り抜けた波が干渉することでスクリーンに干渉縞が現れる。これは粒子でなく波の性質である。

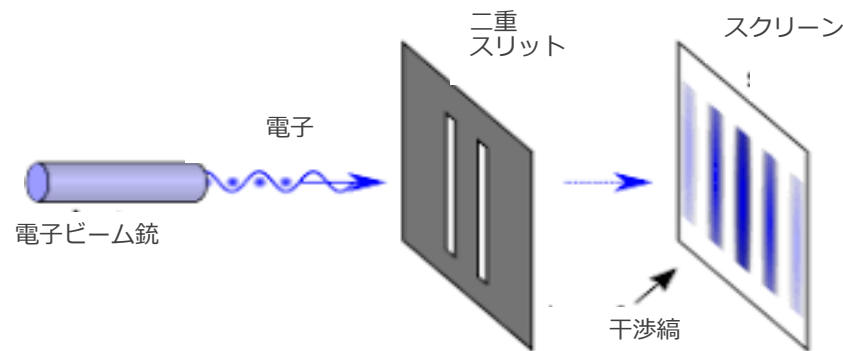


## 3 量子は波なのか？

電子はかつては粒子とされていた。しかし、二重スリット実験（光源の代わりに電子ビーム銃を使い、電子を1個ずつ打ち込む）を行ってみると、光の場合と同様に干渉縞が観測される。

※1961年以降、複数の科学者によって何度も検証されている実験。

👉 この実験から、「電子は波であり、かつ粒子である」と解釈出来る。



波と粒子の二重性があるという量子の性質を応用したのが量子コンピュータである。

## 4 参考文献

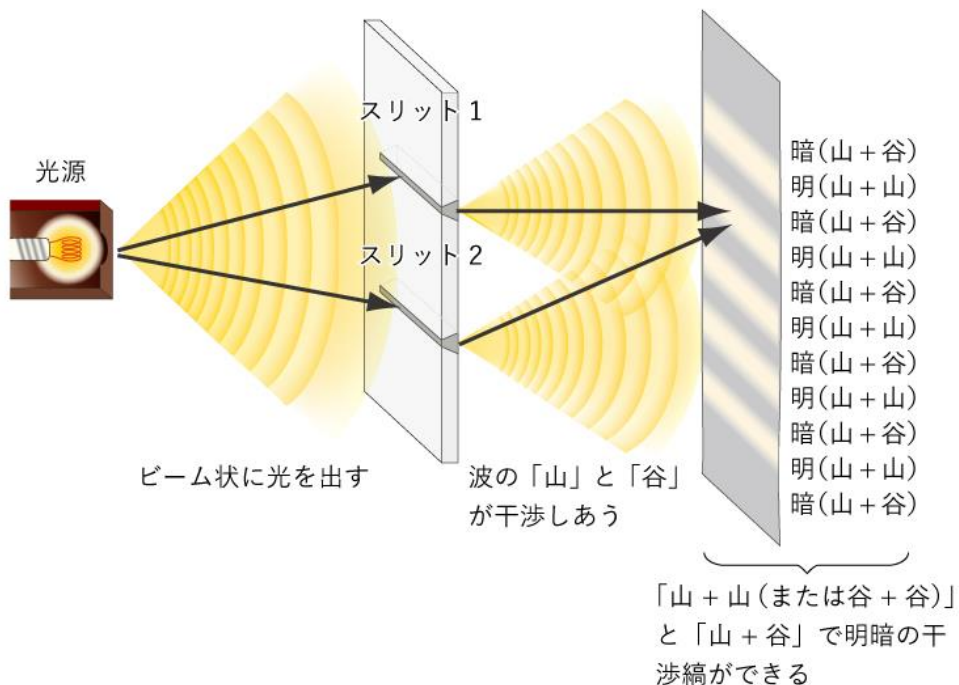
[「いちばんやさしい量子コンピューターの教本」\(株式会社インプレス\)](#)  
[academistjournal](#)  
[sciencealert](#)



## 1 古典的な二重スリット実験

トーマス・ヤングは、1805年に光を2つのスリット(縦長の切れ目)に当たるようにしたところ、2つのスリットを通り過ぎた光が「干渉」を起こして、縞模様になることを発見した。

干渉模様ができるのは、それぞれのスリットを通り抜けた波が、互いに干渉し合うからである。つまり、山と山(または谷と谷)が出会うと波が強くなり、山と谷が出会うと打ち消し合って波がなくなるのである。



## 2 量子による二重スリット実験

古典的な二重スリット実験と同様の実験を光源の代わりに電子ビーム銃を使用し、電子を1個ずつ発射してみる。

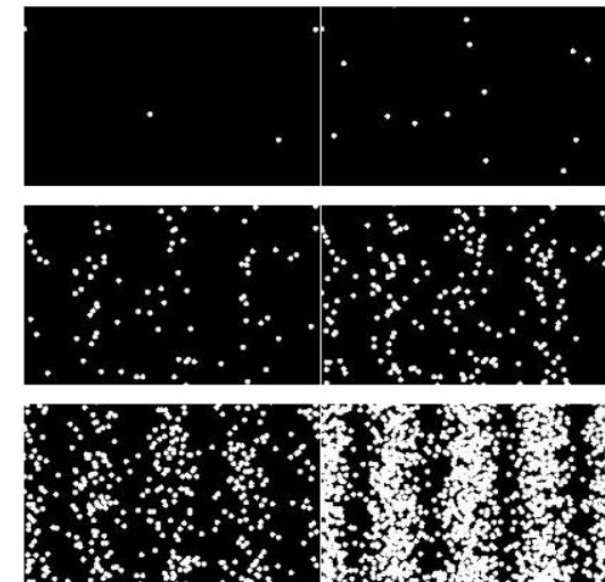
何百、何千と発射して、光子たちがどこに着弾するかを記録していくと、徐々に縞々模様があらわれる。(下図)

発射した時は1個の粒子だったのに、2つのスリットを通り抜けて干渉が起こり、最後はまた1個の粒子として点を記録している。

※量子は「同時に」粒子であり波でもある。

だから、位置が特定できない「途中」の領域においては、拡がりをもって波(但し、確率の波)として振る舞う。

最終着弾地点では、スクリーンと相互作用し、波の性質が失われ、最後には一点に収束して記録される。



## 3 参考文献

[「世界一ふしぎな実験」を腹落ちさせる2つの方法](#)

[コペンハーゲン解釈と多世界解釈②](#)

## 1 量子重ね合わせとは？

量子が同時に異なる状態を取れる性質のこと。  
量子の世界で見られる基本的な性質の一つ。

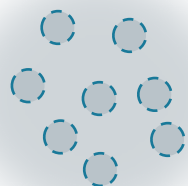
## 2 もう少し詳しく

量子力学では、“位置”や“速度”といった物理量の値は観測するまで決定されない。  
観測前に物理量が決定されていない状態を「状態が重ね合わさっている」と言う。

量子は観測するまで  
“位置”が確定しない



観測して初めて“位置”  
が確定する



↑ここ！


※位置が「分からない」  
のではなく「確定しない」

現在の量子力学においては、状態は「状態ベクトル」、状態の変化は「ベクトルに行列を掛ける演算」としてモデル化される。  
量子力学のモデルでは、重ね合わせを状態ベクトルの線形結合で表現する。

$$\begin{array}{c} \textcircled{\varphi} \\ \uparrow \\ \text{状態ベクトル} \end{array} = c_1 \begin{array}{c} \textcircled{\varphi_1} \\ \swarrow \\ \text{状態}\varphi_1\text{と状態}\varphi_2\text{が} \\ \text{重ね合わさっている} \end{array} + c_2 \begin{array}{c} \textcircled{\varphi_2} \\ \nearrow \end{array}$$

重ね合わさった状態を観測すると、それまで重ね合わさっていた状態が、物理量の観測値に対応する状態ベクトルのみとなり、重ね合わせは解消される。

## 3 量子コンピュータへの応用

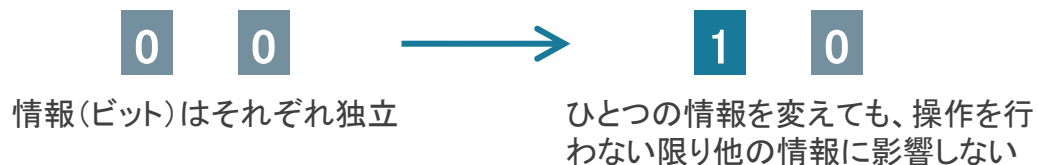
量子コンピュータでは、量子重ね合わせの性質を利用する。  
量子ビット〔 シラバス 7-1〕に0と1の重ね合わせ状態を維持させたまま状態を変化させることで、同時に大量パターンの計算を実行することができる。

## 1 量子もつれとは？

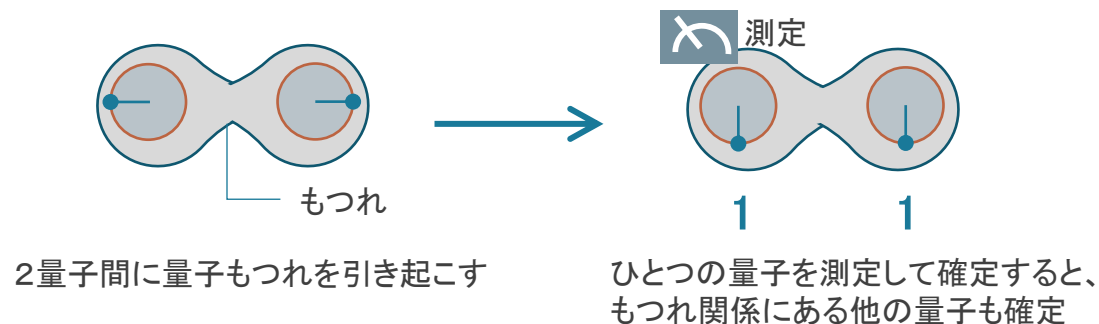
量子の世界において、2個以上の量子が古典力学では説明できない相関をもつこと、また、それにかかわる現象をいう。量子エンタングルメントとも呼ぶ。(cf. 1量子での量子重ね合わせ)

量子コンピュータでは量子もつれ(相互関係)を持たせた一方の量子ビットの状態を変えると、もう一方の量子ビットの状態が影響を受ける性質がよく利用される。

## ● 古典コンピュータの場合



## ● 量子コンピュータの量子もつれの場合



## 2 何がすごい？

量子もつれは、量子コンピュータの世界において計算のステップ数を減らし高速化することに役立っている。

## 量子の重ね合わせ



大量のパターンの  
情報を同時に表現

## 量子もつれ



- ・ 相互作用関係を持たせた複数の情報を同時に操作
- ・ 計算結果の絞り込み

また、離れていても量子の状態(情報)を移せる量子テレポーテーションを用いた量子通信〔[シラバス 5-4](#)〕や、測定すると状態が変化する性質を用いた量子暗号〔[シラバス 5-5](#)〕などに量子もつれの性質が利用されている。

## 3 関連キーワード

H(アダマール)ゲート、CNOTゲート〔[シラバス 7-2-1,2,3](#)〕

## 4 参考文献

[いちばんやさしい量子コンピュータの教本\(インプレス\) 湊雄一郎](#)  
[量子コンピュータはなぜ速いのか？](#)



## 1 量子もつれとは

量子もつれとは、2つの粒子が強い相互関係にある状態であり、粒子のスピン、運動量などの状態をまるで「コインの裏表」のように共有する運命共同体のような状態を指す。このような量子もつれにある2粒子間の状態は、どれほどの距離があろうが維持される。この同期の速度が光の速度を超えるという、まるで空間など存在していないかのような非局所性から、偉大な物理学者アルバート・アインシュタインは、かつて「不気味な遠隔作用」と呼んだ。

## 2 EPRパラドックス

アインシュタイン＝ポドルスキー＝ローゼンのパラドックス。量子力学の量子もつれ状態が局所性を（ある意味で）破るので、相対性理論と両立しないのではないかというパラドックス。アルベルト・アインシュタイン、ボリス・ポドルスキー、ネイサン・ローゼンらの思考実験にちなむ。EPRパラドックスが発表された当時は、アインシュタインらは局所实在論の立場を取っていたため、量子論が实在論的に完全でない結果を与えることを「パラドックス」とした。 [Wikipedia](#)

## 3 ベルの不等式

隠れた変数理論などの局所实在論が満たすべき相関の上限を与える式。古典的に説明できる粒子の相関関係の上限を示した数式であり、これによって実験が「量子的」なものなのか「古典的」に説明できるものなのかを区別できる。「ベルの不等式」の上限が破られると、実際に2つの粒子が量子もつれの状態にあることが示される。

## 4 ベルの不等式を破り、量子もつれ(非局所性)を証明した実験

実験名称	年代	説明	その他
CHSH-ベル定理予測の最初の実験的試験	1972	ジョン・クラウザーとスチュアート・フリードマンによる最初の実験的試験。量子もつれ(数千個)を大量に作る装置を作成。	量子力学の間違いを証明しようとしたが、逆の結果となった。
アラン・アスぺの実験	1982	アラン・アスぺが実験でCHSH不等式(ベルの不等式の一種)が破られていることを示す。	「局所性の抜け穴」「検出効率の抜け穴」問題が残るとの批判あり。
古澤明氏らの研究チームの実験	2015	「量子(光子)の非局所性」を世界で初めて厳密に検証。	「本実験にて上記の穴を完全に塞いだ」との記述あり。
地上-衛星間量子テレポーテーション実験	2017	中国の研究者が地上から500km以上離れた上空の起動を周回する衛星に光子をテレポートすることに成功。	従来の記録(100km程度)を破る、長距離テレポーテーション。

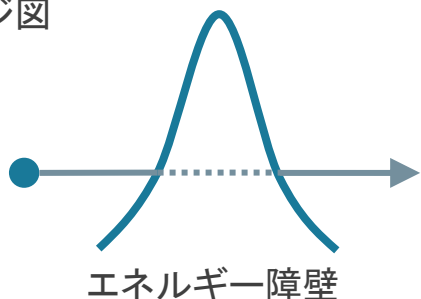
## 5 参考文献

[「量子もつれ」の瞬間を世界で初めて画像に記録、英研究チームが成功](#)  
[量子もつれ ～アインシュタインも「不気味」と言い放った怪現象](#)

## 1 トンネル効果とは？

量子力学の分野で、粒子が自分のもつ運動エネルギーよりも高いエネルギー障壁（ポテンシャル障壁）を、ある確率をもって通り抜ける現象のこと。

イメージ図



- ・ 量子の世界で、障壁が薄い時に透過する。
- ・ 障壁を高く or 広くすると透過する確率は下がる。

## 2 何がすごい？

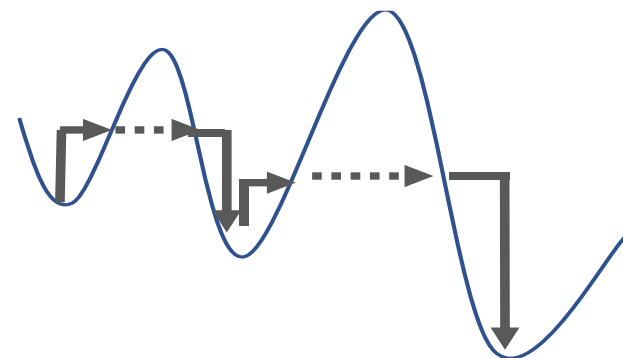
量子トンネルによって説明できる現象がいくつか存在している。恒星内での核融合や、星雲間における宇宙化学、放射性崩壊、量子生物学などの宇宙や生命に関する現象もそのひとつである。

物理学的な面や産業への影響も大きい。トンネル効果が集積回路の電力損失や発熱の原因となり、コンピュータチップのサイズダウン限界に影響を及ぼしている。

また、トンネルダイオードや量子コンピュータ、走査型トンネル顕微鏡、フラッシュメモリなどの装置に応用されている。

## 3 量子コンピュータとはどう関連するの？

量子アニーリング方式〔[□□シラバス 4-3](#)〕において、組み合わせの最適化探索を効率化することにトンネル効果が利用される。



グラフの山をすり抜け、最適解を探索する。

## 4 関連するキーワード

- ✓ 粒子と波動の二重性〔[□□シラバス 3-3](#)〕
- ✓ ハイゼンベルクの不確定性原理
- ✓ 波動関数、シュレディンガー方程式

## 5 参考文献

[トンネル効果-Wikipedia](#)

[いちばんやさしい量子コンピュータの教本 \(インプレス\) 湊雄一郎](#)

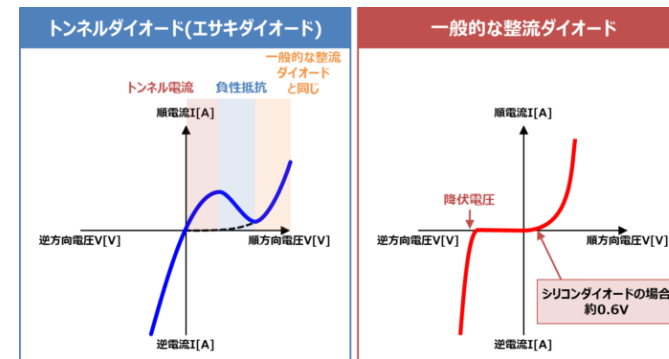
## 1 トンネルダイオード

ダイオードとは、電流を一方向にしか流さない半導体素子である。

トンネルダイオードとは、量子トンネル効果を使った半導体によるダイオードの一種であり、江崎玲於奈博士の発明によるため、その名をとってエサキダイオードとも呼ばれる。

トンネルダイオードは負性抵抗特性(電圧が増加すると、電流が減少する特性)を持つ。高周波特性が良く、マイクロ波の発振回路、増幅回路、高周波スイッチング等で用いられる。

参考文献および画像引用:【トンネルダイオード】『原理』や『特徴』などをわかりやすく解説！

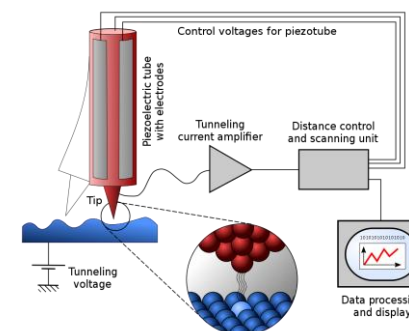


## 2 走査型トンネル顕微鏡

ゲルト・ビーニツヒ と ハイน์リッヒ・ローラー により1982年に発明された。

非常に鋭く尖った探針を導電性の物質の表面または表面上の吸着分子に近づけると、電子がポテンシャル障壁を飛び越え(トンネル効果)、探針試料間を移動する。このとき流れる電流をトンネル電流といい、トンネル電流から表面の原子レベルの電子状態、構造など観測するものが走査型トンネル顕微鏡である。

参考文献および画像引用: Wikipedia-走査型トンネル顕微鏡

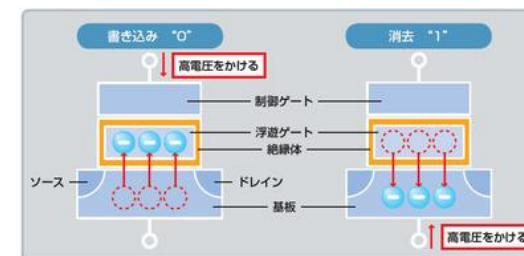


## 3 フラッシュメモリ

トンネル効果により電圧をかけて電子が絶縁体を通り抜けることができる。電圧をかけるほど電子の通り抜ける確率が増加するため、閉じ込められる電子の量が増加する。

絶縁体の中の浮遊ゲートと呼ばれるところに電圧をかけて電子を出し入れし、ビット情報を保存するのがフラッシュメモリの基本原理となる。

参考文献および画像引用:なぜ消えるのか、劣化するのか フラッシュメモリーの技術をひも解く



## 1 ハミルトニアンとは？

粒子や場のシステムのエネルギーを座標と運動量で表現したもの。  
量子力学ではエネルギー演算子をいう。ハミルトン演算子ともいわれる。  
名称はイギリスの物理学者ウィリアム・ローワン・ハミルトンに因む。

量子力学では座標  $q$  と運動量  $p$  を演算子と考え、この間に  
 $qp - p q = -i\hbar$  という関係が成り立つと考えている。

$p = -i\hbar \partial / \partial q$  は、この関係の具体的な一つの表現である。

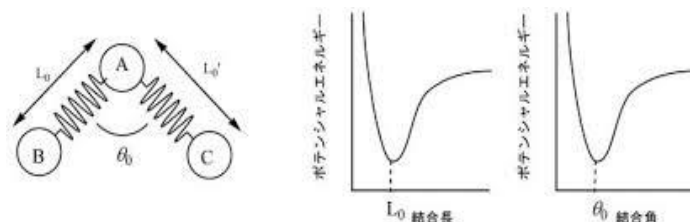
この結果、量子力学のハミルトニアンは古典力学のハミルトニアンの  
 $p$  を  $-i\hbar \partial / \partial q$  で置き換えた演算子  $H$  となり、量子力学の運動状態、  
すなわち量子的状态  $\phi$  の時間的変化は、以下で与えられる。

$$i\hbar \partial \phi / \partial t = H \phi$$

## 2 ハミルトニアンはどの様に使われる？

## ○量子化学計算

新素材の開発では、素材の分子構造が安定する状態を求めるために  
量子化学計算を使う。分子エネルギーの計算を行い、安定した状態  
(最小エネルギー)を求める。  
分子エネルギーはハミルトニ  
アンで表し、その最小値を  
求める。

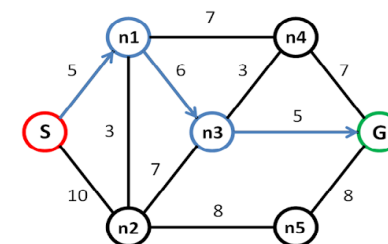


☞ 量子化学計算は分子が大きくなるほど計算が複雑となり、スーパー  
コンピュータを使用しても長時間掛かってしまう。量子コンピュータの  
活用により、新素材開発の迅速化が期待される。

## ○組合せ最適化

最短経路の選択や渋滞解決等のためには、多数ある選択枝の中から  
最適なものを選択する(組合せ最適化)が必要となる。

組合せ最適化問題は重み付きグラフで表すことが出来る場合がある。  
重み付きグラフをコスト関数(=ハミルトニ  
アン)で表し、その最小値を求めることが  
出来れば、最適な組合せを選択出来る。



☞ コスト関数は、要素数が増えると選択枝となる組合せが膨大となり  
組合せ爆発を起こしてしまう。量子コンピュータの活用により、現実  
の組合せ最適化問題の解決が期待される。

## 3 参考文献

[コトバンク](#)

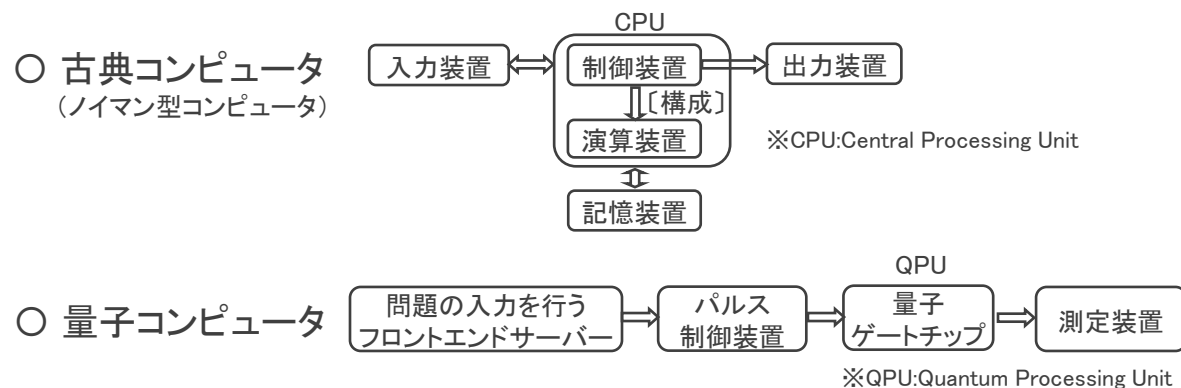
[分子力学法](#)

[2点間を結ぶ配管経路探索アルゴリズム](#)



## 1 量子コンピュータは何が違う？

従来型の古典コンピュータと量子コンピュータには、構成要素に大きな違いがある。

量子コンピュータには、コンピュータの構成要素のひとつである演算装置 (QPU) しかない。演算装置の中核となる量子ゲートチップだけが「量子力学」の仕組みで動いており、それ以外の装置は量子コンピュータに指示を与える働きをしている。



## ☞ 量子コンピュータの種類

量子コンピュータは問題を解く方法の違いにより、量子ゲート方式〔シラバス 4-2〕と量子アニーリング方式〔シラバス 4-3〕の大きく2つに分類される。

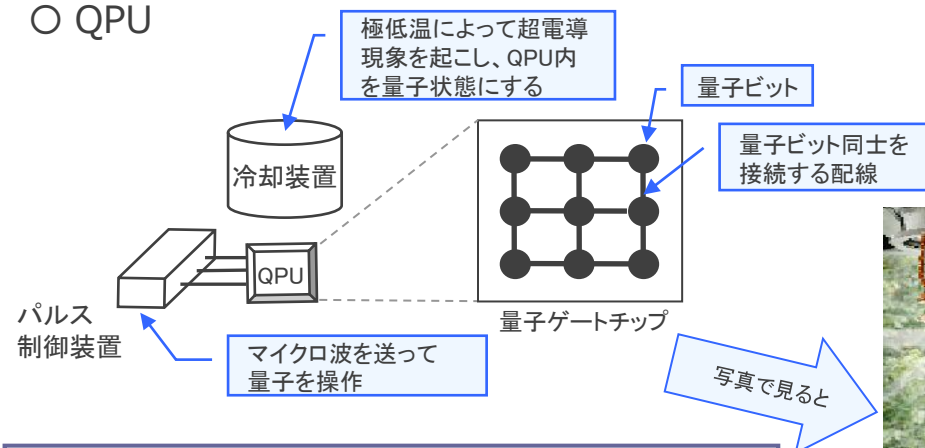
## 2 QPUとは？

QPUは複数の量子ビットを持ったプロセッサである。パルス制御装置からマイクロ波を送り、量子ビットを状態変化させて演算を行う。

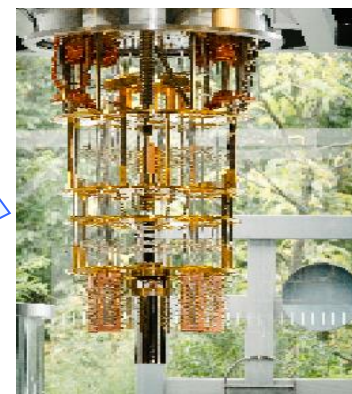
超電導状態を保つため、特殊な冷却装置 (希釈冷凍機) により極低温状態にする必要がある。

(\*)量子ビットは、ちょっとした電気抵抗やノイズによっても影響を受ける。それを防ぐために超電導状態が必要であり、そのために極低温が必要なのである。

## ○ QPU



IBM 50 qubit system の希釈冷凍機の中身。  
最下端に量子ビットが並んだチップ (QPU) がある。  
銀色の線はそのチップ上の量子ビットを操作するマイクロ波パルスの線。最下端は数十 mK (-273°C 以下) まで冷やされる。



## 3 参考文献

「いちばんやさしい量子コンピュータの教本」(株式会社インプレス)

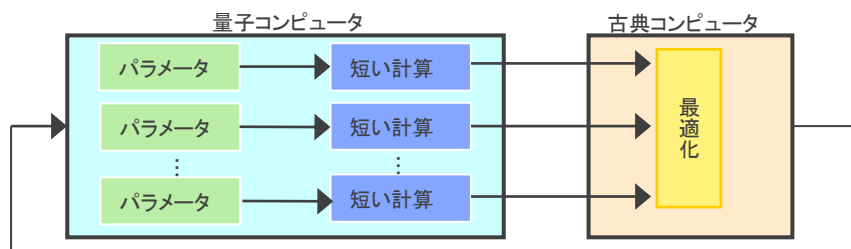


## 1 QPUって速いの？

QPUはマイクロ波のパルスにより量子ビットの操作を行う。その処理速度は、現状、 $1\mu$ （マイクロ）秒当たり数回程度である。一方、一般のPCに内蔵されているIntelのCPUは3GHz程度のクロック周波数であり、単純計算で $0.3n$ （ナノ）秒に1つの操作を行える。そのため、同じ演算を同じロジックで行うとしたら、圧倒的に一般のPCの方が速いことになる。 ※ $1000n$ 秒 =  $1\mu$  秒  
量子コンピュータが従来のコンピュータより速いというのは、量子ゲートを上手く組み合わせて従来のコンピュータよりも圧倒的に少ない計算量で計算出来る量子アルゴリズムが見つかった場合である。

## 2 量子古典ハイブリッド計算って何？

現状の量子コンピュータはコヒーレンス時間が短くエラー訂正機能が実装出来ていないことから、量子コンピュータのエラーを既存（古典）コンピュータで最適化しながら短い回路を実行するハイブリッド型が提案されている。量子コンピュータと古典コンピュータ、互いの得意分野を活かし、効率的なアルゴリズムが作成出来ると期待されている。



## 3 古典コンピュータ（ノイマン型コンピュータ）とは？

ノイマン型コンピュータとは、ハンガリー出身の数学者であるジョン・フォン・ノイマン（John von Neumann）によって提唱された、コンピュータの基本構成（アーキテクチャ）のことである。

ノイマン型コンピュータでは、記憶部に計算手続きのプログラムが内蔵され、逐次処理方式で処理が行われる。

中央演算部、制御部、記憶機構、入力部、出力部の5つの部分からなり、プログラム実行時には、主記憶装置から演算制御装置へ命令やデータが記憶レジスタを経由して転送され、命令は、命令アドレスレジスタにセットされたアドレスに沿って逐次的に実行される。

今日の一般的なコンピュータシステムのほとんどが、このノイマン型である。

## 4 希釈冷凍機って何？

超電導型の量子コンピュータでは素子を絶対零度近くにまで冷却する必要があり、ヘリウム3・ヘリウム4混合溶液の性質を用いた連続型の冷凍器（希釈冷凍機）を用いて数～数十mK（ミリケルビン）に冷却する。

## 5 参考文献

[「いちばんやさしい量子コンピューターの教本」\(株式会社インプレス\)](#)

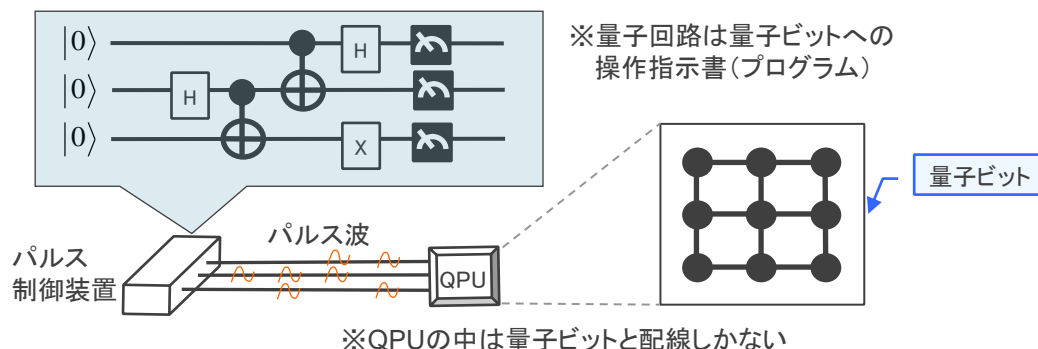
## 1 量子ゲートとは？

量子ゲートとは、量子コンピュータにおける論理回路のことである。量子ゲートを組み合わせてプログラミングを行い、アルゴリズムやアプリケーションを構築する。

## 2 古典コンピュータとの違い

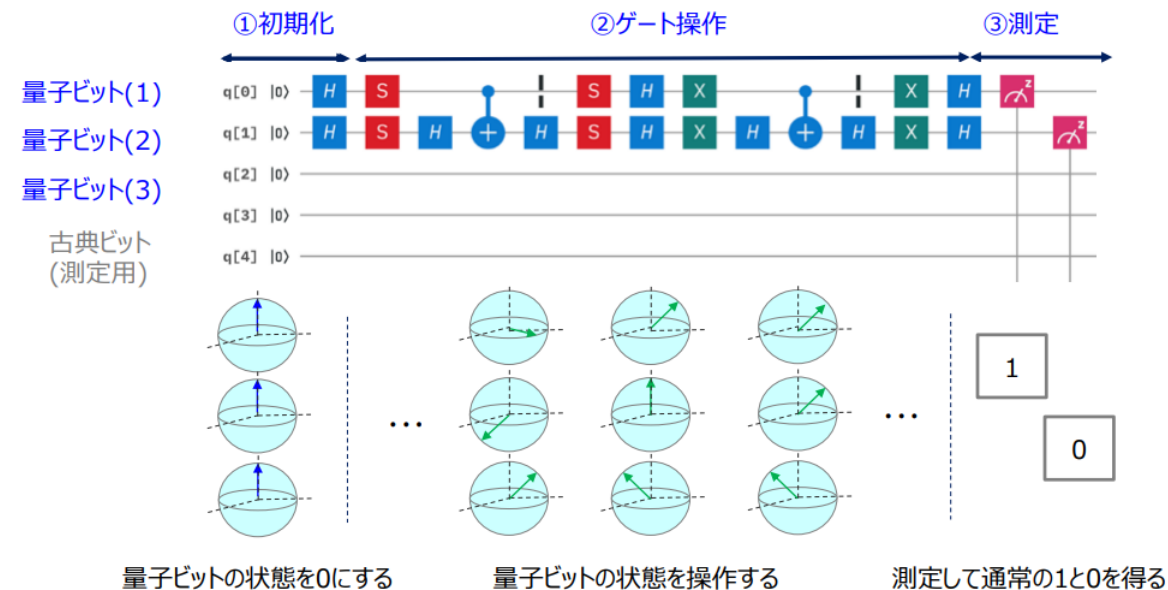
古典（従来型）コンピュータの演算装置やその中の論理回路は、CPUの中に実在する。それに対し、量子コンピュータのQPUの中に実在するのは量子ビットだけで、量子ゲートは存在しない。量子回路上の量子ゲートは、量子ビットに対する操作を表す仮想的なものである。

👉 古典コンピュータの論理回路は、予め加算や乗算等の回路が用意されており、プログラムの指示でどの回路を使うかが切り替わる。それに対し、量子回路の量子ゲートは仮想的なものであり、自由に組み替えられる。つまり、量子回路はプログラムなのである。



## 3 量子ゲート方式のプログラミングと計算

量子ゲート方式では、課題を解くアルゴリズムを用意し、量子ゲートを組合せることでアルゴリズムを量子回路に作り込む。その量子回路に従って、量子ビットに対して色々な変換操作（量子ゲート操作）を行い、結果を測定して計算結果を読み出す。



## 4 参考文献

[「いちばんやさしい量子コンピューターの教本」\(株式会社インプレス\)](#)  
[量子コンピュータの概説と動向\(株式会社日本総合研究所\)](#)

## 1 量子アニーリングとは？

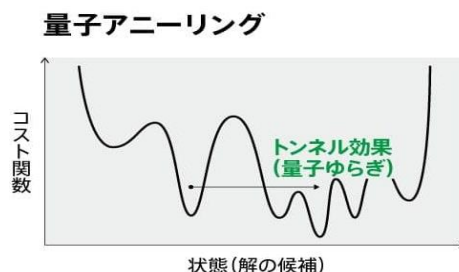
量子アニーリングは、多数の選択肢から最もよい組み合わせを選ぶ「組合せ最適化問題」を解くための量子アルゴリズムである。

1998年に東京工業大学の西森秀稔教授らによって考案された。

一般に、古典コンピュータでは膨大な数の組み合わせから逐次選択と確認を行いながら問題を解いていくのに対し、量子アニーリングでは「量子力学的もつれ」を伴う「量子ゆらぎ(トンネル効果)」を用いて比較的容易に最適解に近づける。

## ○量子アニーリングの原理

量子アニーリングでは、量子ゆらぎ(トンネル効果)を用いてエネルギーが最小となる最適解を求める。



## 2 量子アニーリングの計算の仕組み

量子アニーリングマシンを使用する場合、組み合わせ最適化問題を定式化し、それをイジングモデル〔[図](#) 詳説〕に変換してマシンに投入する。

イジングモデルは下記のエネルギー関数で表されるモデルである。

$$H = \sum_{i \neq j} J_{ij} \sigma_i \sigma_j + \sum_i h_i \sigma_i \quad (\sigma = \pm 1)$$

アニーリングマシンへの入力、 $J_{ij}$ 、 $h_i$  を与えることだけである。これらのパラメータを与えるとマシンがアニーリングを実行し、エネルギーが最小となる組合せ  $\sigma$  の最適解を出力する。

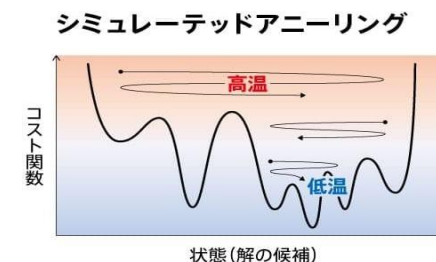
## 3 量子アニーリングマシン

量子アニーリングマシンは、D-Waveが2011年に製品化している。なお、日本のメーカーは、主にシミュレーテッドアニーリング方式の研究を行っている。

量子ゲート方式	量子アニーリング方式	シミュレーテッドアニーリング方式
Google Honeywell IBM ION Q Microsoft Rigetti Computing XANADU	D-Wave Systems NEC	富士通 日立製作所 東芝 Fixstars NEC NTTデータ NTT

量子アニーリングマシンを使った実問題への取り組みについては、幾つかの企業・大学が検証を行っている(トラフィック・フロー最適化、交通信号最適化、工場内の経路最適化等)。しかしながら、未だに現実の大規模問題への適用は難しいようである。

☞ シミュレーテッドアニーリングは、高温にした材料を冷却する際のエネルギー状態変化(熱ゆらぎ)を古典コンピュータでシミュレートして最適解を求める方法。



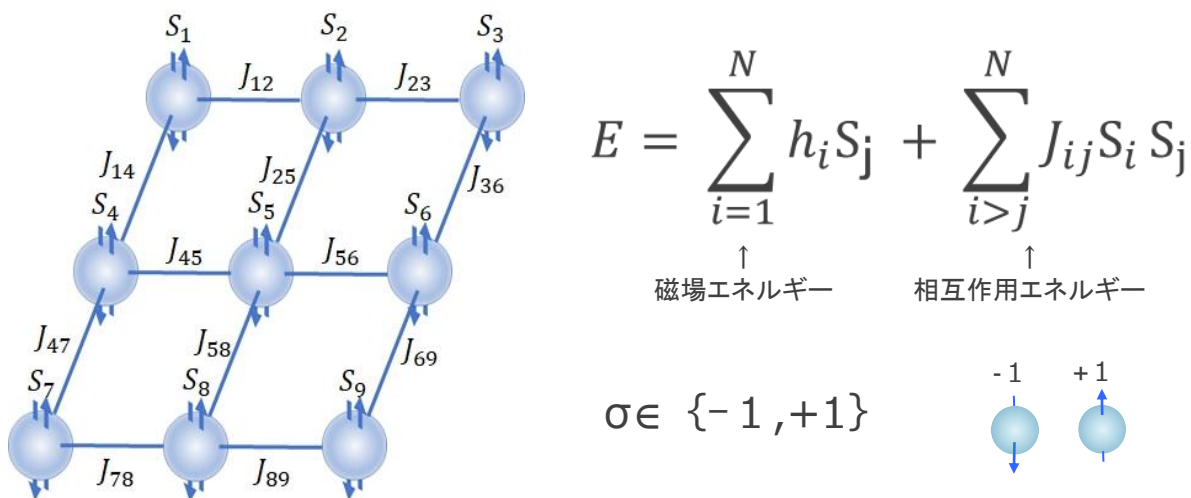
## 4 参考文献

[株式会社デンソー The COREs](#)

[NTTデータ 量子コンピューティングガイドライン](#)

## 1 イジングモデルとは？

磁石などの磁性体の性質を表す統計力学上のモデル(模型)のこと。イジングモデルは、上向きまたは下向きの二つの状態をとるスピン(格子点)から構成される。隣接するスピンは、相互作用および外部から与えられた磁場の力によってその状態が更新される。最終的に、イジングモデルのエネルギーが最小の状態ですピンは収束(安定)する。



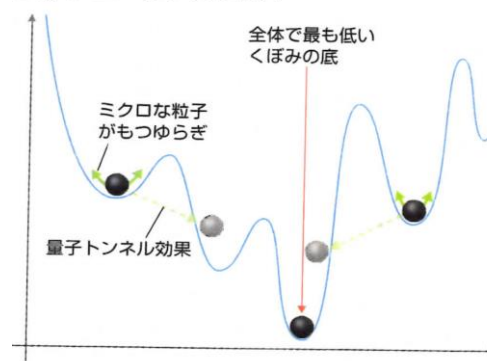
※ アニーリング(焼きなまし)前は、各量子のスピンは上向きと下向きの両方の状態(重ね合わせ)を同時に持っている。アニーリング後は、各量子は全体のエネルギーを最小化する上向きもしくは下向きのスピン状態になる。量子アニーリングを用いると、わずかな時間でこの全体のエネルギーを最小とするスピン変数の組み合わせを求めることが期待できる。

## 2 量子アニーリングとシミュレーテッドアニーリング

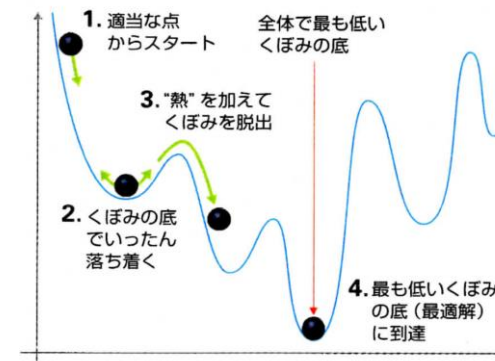
シミュレーテッドアニーリングでは、最適解の探索のために組合せを変化させていく。この過程では、必ずしもコスト関数が小さくなるとは限らず、ある確率で次の状態を選択する。この時、コスト(エネルギー)の低下をどの程度重要視するかを「温度」というパラメータで制御する。高温から低温に徐々に変化させることで局所解での凍結を回避し、最適解を探索する。

量子アニーリングでは「温度」の代わりに「量子効果」を変化させる。量子効果が非常に強い状況下では、すべての状態(組合せ)の重ね合わせになっている。つまりこの時に測定を行うと、すべての状態がそれぞれ等しい確率で出力される。量子効果が強いほど各状態の間でトンネル効果による状態遷移が起きるが、そこから量子効果を小さくすることで状態が動かなくなる。

### 量子アニーリングとは？



### シミュレーテッド・アニーリングとは？



## 3 参考文献

[日立製作所 HP](#)  
[ネットワン HP](#)

[QUANTUM COMPUTING SOLUTIONS HP](#)  
[Qiita「【初心者向け】数式もプログラミングもなしで量子コンピュータを説明してみる」](#)

## 1 組合せ最適化とは？

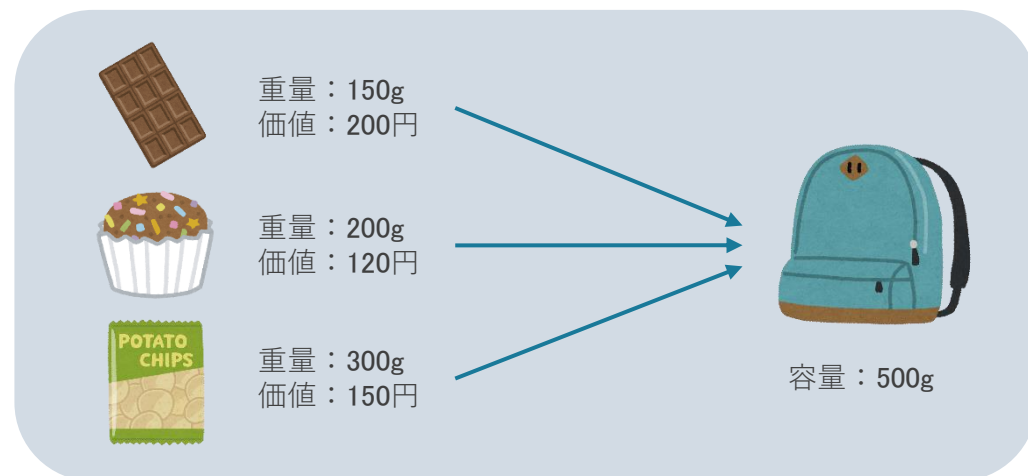
ある条件を満たす組合せの中から、最も良い解を見つける形式の問題のこと。

この問題は交通渋滞緩和や新薬開発、勤務シフト最適化といった様々な社会問題の中に現れ、高速に解くことが求められる。

## 2 具体例

**ナップサック問題**：有名な組合せ最適化問題のひとつ。

- 荷物にはそれぞれ重量と価値が設定されている。
- 袋には重量の上限値があり、詰め込む荷物の重量の合計が、袋の上限値を超えてはならないという制約がある。
- この条件のもと、最も価値が高くなる荷物の組み合わせを探す。



## 3 何がポイント？

組合せ最適化問題は、問題の規模が大きくなると探索する組合せの数が非常に大きくなることもある(**組合せ爆発**)。

解きたい問題によっては、古典コンピュータでは現実的な計算時間で解ききれないものがある。

## 4 量子コンピュータとの関係

**量子アニーリング**〔[□□シラバス 4-3](#)〕と呼ばれる方式の量子コンピュータでは、組合せ最適化問題を(近似的に)解くことに特化している。問題をモデル化したものを量子アニーリング方式の量子コンピュータに設定すると、**量子ゆらぎ**という性質を利用することで組合せ最適化問題の解が得られる。

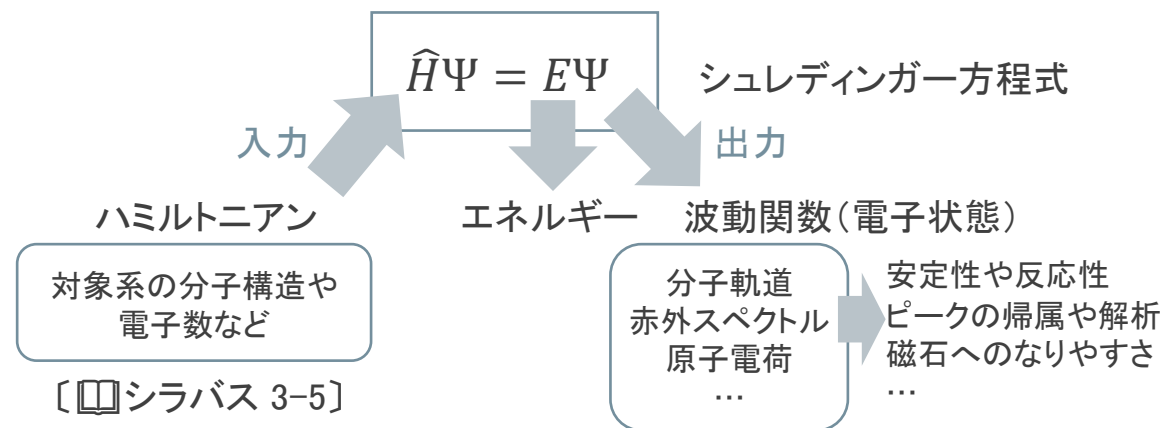
## 5 参考資料

[簡単そうで難しい組合せ最適化 -京都大学 永持研究室-](#)  
[NTTデータ 量子コンピューティングガイドライン](#)



## 1 量子化学計算とは？

量子化学とは、分子の特性を電子から解析・予測する学問分野である。



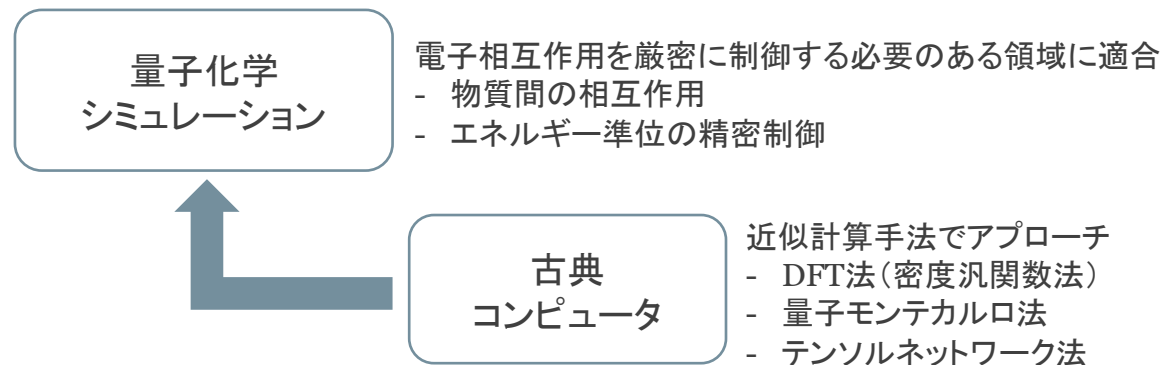
対象となる材料を構成する分子そのものの個性が材料全体の主たる性質を特徴づけているため、材料設計の方向性や機能制御・問題の特定などへ大いに役立つ。

量子化学計算は古典・量子コンピュータで物質の性質や反応をシミュレーションし、化学現象を明らかにする手法を指す。

古典コンピュータでも量子化学計算があることに注意。  
量子コンピュータでの化学計算が量子化学計算ではない。

量子化学計算の分野ではノイズのある中規模のNISQデバイスでも、解析内容によっては既に古典コンピュータより優位性が発揮できることが見込まれている。[ 詳説 ]

## 2 量子コンピュータでの量子化学計算は何ができるの？



量子化学シミュレーションにおける古典コンピュータの近似計算手法では、解きたいが解けない問題[ 詳説 ]として、分子相互作用の特定が必要な系などがある。量子コンピュータには、この解けない問題に該当する電池や触媒、太陽電池、熱電変換、製薬など、組成で勝負が決まる材料探索が期待されている。

## 3 量子化学×量子コンピュータのキーワード

量子化学計算に用いられる代表的なアルゴリズム

- ✓ 量子位相推定 (量子フーリエ変換:QFT)
- ✓ VQE

## 4 参考文献

[量子化学の基礎知識](#)

[Qmedia—素材企業が拓く「量子コンピュータ」の未来](#)

[量子化学計算のモチベーション](#)

## 1 NISQデバイスでも優位性のある量子化学計算の例：励起状態解析

物質の構造は、X線や電子線を照射して物質中の電子を励起し、励起状態に応じて測定されるスペクトルを解析することで、物質の原子配列と電子構造として調べることができる。

図1は、励起状態解析における誤り訂正量子コンピュータ及びNISQデバイスと既存計算方法の得意領域比較を示したものである。この図から、対象電子軌道数が100以下の領域であれば、NISQデバイスであっても、古典コンピュータを用いた既存計算手法(DFT等)よりも優位性を発揮できる可能性が高いことがわかる。

図2では古典コンピュータにおけるTD-DFTの計算コストが低いことが示されており、計算結果の精度が低くても良い解析には古典コンピュータも利用できることが分かる。

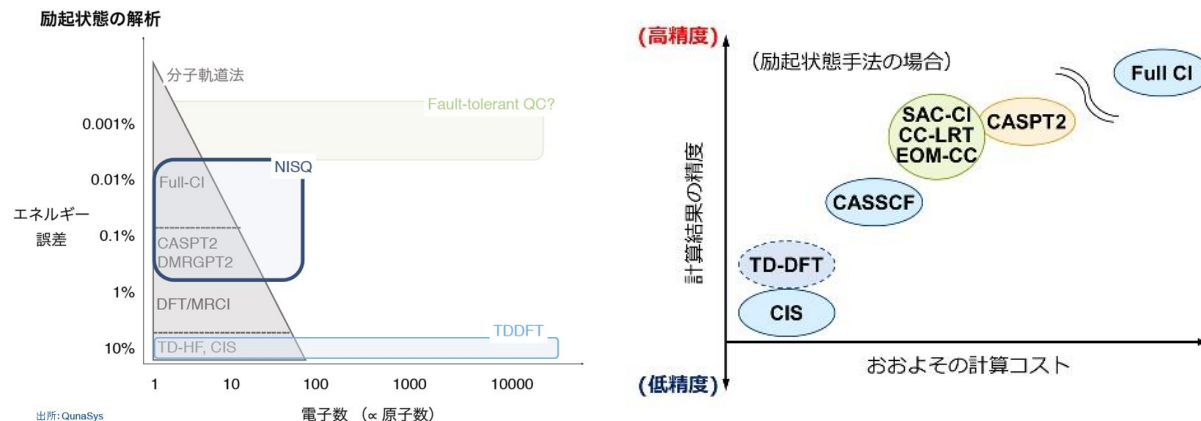


図1: 誤り訂正量子コンピュータ及びNISQデバイスと既存計算方法の得意領域比較例

図2: 励起状態計算手法の精度とコスト

## 2 量子コンピュータの量子化学計算への適用範囲

古典コンピュータでのDFT法などで解くことができない複雑系は以下のようなものである。これらは、量子コンピュータの最初のターゲットとなる可能性が高い。

- 分子相互作用の特定が必要な系
- ファンデルワールス力の精密制御が必要
- より低エネルギーの反応経路探索が必要
- 励起状態の特定が必要な系
- エネルギー準位(バンドギャップ)の精密制御が必要
- 電荷移動の精密制御が必要
- 複雑な界面を持った系
- 電子同士が強い相関を持った系(磁性材料等)

このターゲットに対し、市場ニーズがあるかが以下の図である。

素材化学業界が見据えるべき大トレンド	量子コンピュータが開発加速できる領域	2030年市場規模 <sup>※1</sup>	量子コンピュータの経済インパクト <sup>※2</sup>
モビリティ	● 軽量化・マルチマテリアル化 ● CASE対応	電気・電機材料 6兆円 (デバイス市場の10%で想定)	1,200億円
インフラ・建築	● 更なる省エネ(ZEB, ZEH等) ● インフラマネジメントの在り方変化	熱電変換・磁性材料 2.5兆円 (リニア型磁性材料)	1,000億円
環境・エネルギー	● 既存プロセスの更なる効率化 ● 新材料・新エネルギー利用	炭素(低分子) 2兆円 (加圧R&D費用の10%で想定)	4,000億円
エレクトロニクス	● 半導体(NAND, パワー半導体, 等) ● ディスプレイの進化 ● ウェアラブル・IoT	石油化学プロセス向け触媒 4兆円	1,700億円 (4000億円未満で想定)
ヘルスケア	● 非侵襲・低侵襲医療、診断の高度化 ● 再生医療 ● バイタルセンシング	フォトレジスト 3,700億円	70億円
		成膜・エッチング材料 4,200億円	85億円
		色変換材料 <sup>※</sup> (量子ドットでクOLED)	800億円
		有機エレクトロニクス 9,000億円 (デバイス市場の10%で想定)	180億円

図3: 素材業界が見据えるべきトレンド及び量子コンピュータの貢献余地

## 3 参考文献

Qmedia—素材企業が拓く「量子コンピュータ」の未来

## 1 機械学習とは？

過去のデータを用いて、解決すべき問題(タスク)に対するプログラムの性能を改善させること。(タスクの例: 明日の売上を予測する、映像から特定の物体を検出する)

性能を改善させる過程を「学習させる」と言う。

## 2 機械学習の応用

機械学習は、データの増加(ビッグデータ)やコンピュータ性能の向上に伴い、次のような分野の問題解決に利用されるようになっている。

- 金融工学: リスク分析、最適なポートフォリオの作成
- 画像処理: 顔認識、物体検出、自動運転車のカメラ
- 生命科学: 病理画像解析、創薬
- 予知保全: 機器の状態を監視し設備の劣化状態を予知する



機械学習はタスクやアルゴリズムによって、大きく3種類に分けられる。

### ① 教師あり学習

- 「入力」と「出力」がセットになったデータを用いて、未知の入力に対する答えが正しくなるように学習させる方法。
- 例: メールの文章(入力)が迷惑メールかどうか(出力)を学習し、新たな受信メールが迷惑メールかどうかを推測させる。

### ② 教師なし学習

- 「出力」となるデータを与えずに、「入力」となるデータのみを用いて学習させる方法。
- 例: メールの文章データを用いて、近い内容の文章ごとにメールを分類(クラス分類)する。分類されたメールのクラスが迷惑メールかどうかは人間が判断し決定する。

### ③ 強化学習

- ある「環境」の中で、目的に対して設定された「報酬」を最大化させる行動の「方針」を学習させる方法。
- 例: ビデオゲーム(環境)でより高いスコア(報酬)を取るために、どのタイミングでこういった操作をするか(方針)を学習させる。

## 3 量子コンピュータへの応用

機械学習では、学習させる際に大量の計算を行う必要がある。機械学習計算のアルゴリズムを工夫することで、量子コンピュータの大きな計算力を機械学習に応用させることが期待されている。

## 1 量子通信とは？

安全な通信を実現する**量子暗号**、多くの情報を伝送する**量子通信**など、量子力学の原理に基づいた通信方法のこと。

量子コンピュータの実現により、従来の主な暗号は全て破られてしまうとされている。また、現在の技術の延長線上では、通信回線をこれ以上大容量化するには限界があると言われている。量子通信は、これらの課題をブレークスルーする技術となる。

## 2 量子暗号、何がすごいのか？

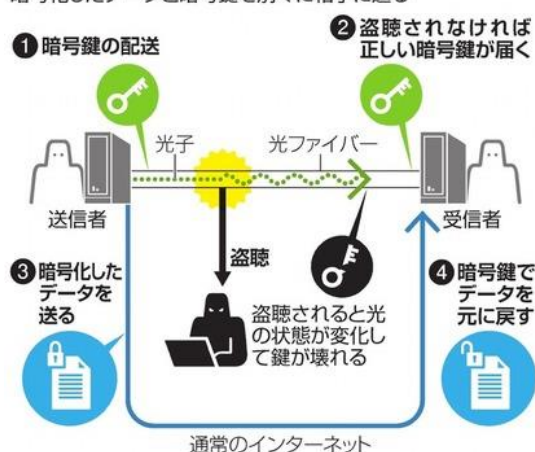
現在普及している暗号化技術は、「暗号の解読には膨大な時間が掛かる」という前提により、通信の安全性を保障している。そのため、量子コンピュータが実現すれば、この前提が崩されることになる。

量子暗号では、暗号化・復号化に使用する暗号鍵を量子の経路を通じて伝送する。この暗号鍵は量子力学の法則（ハイゼンベルグの不確定性原理）により、盗聴し解読することが出来ないとされている。

暗号が途中で盗聴された場合は量子の状態に変化が生じるため、解読することは出来ず、盗聴が瞬時に検出されることになる。

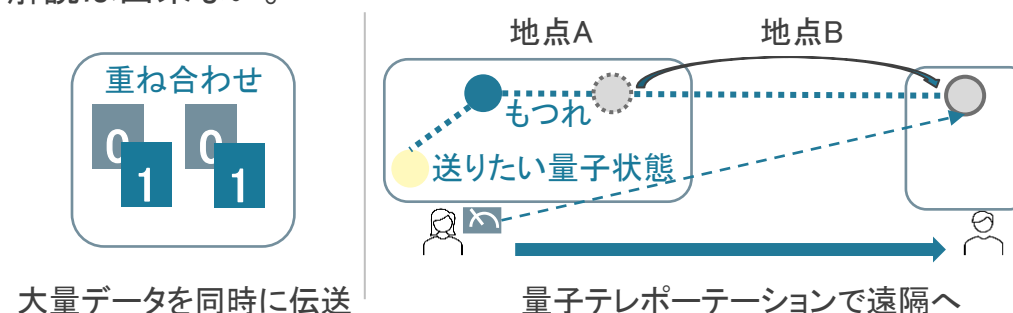
## 量子暗号通信の仕組み

暗号化したデータと暗号鍵を別々に相手に送る



## 3 量子通信、何がすごいのか？

現状の通信（古典通信）では0と1からなる情報を伝送しているが、量子通信では0と1の重ね合わせ状態にすることで、大量のデータを同時に伝送することが出来る。さらに、量子テレポーテーションを利用することで、量子状態を瞬時に遠隔地へ送ることも研究されている。なお、量子状態となっているデータは、量子暗号と同様に、盗聴による解読は出来ない。



## 4 情報の伝達はどうするのか？

量子情報の運び手としては「光子」が使われる。

光子が使用されるのは、外部環境との相互作用が小さいためデコヒーレンス（重ね合わせ状態の破壊）が起き難く、且つ光速で移動するという特徴があるためである。

## 5 参考文献

[\(いちからわかる！\)絶対解読できない「量子暗号」って？](#)

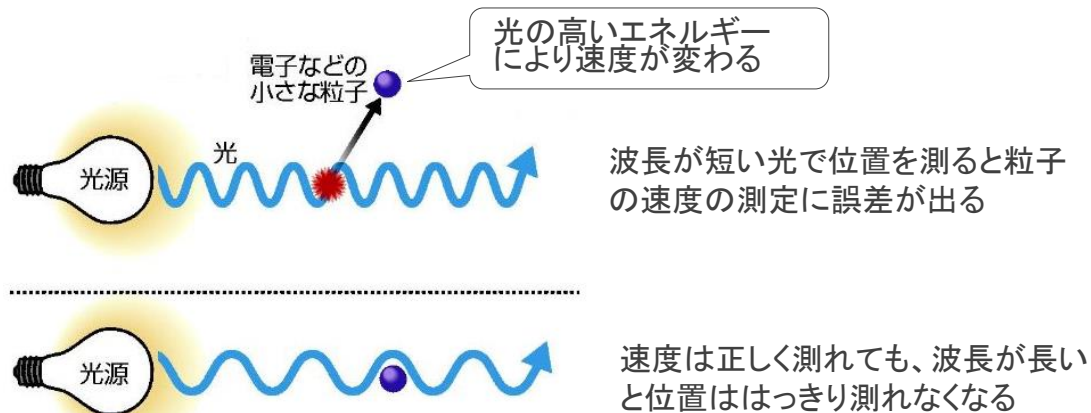
[\(朝日新聞デジタル\)](#)

[国立研究開発法人 情報通信研究機構](#)



## 1 ハイゼンベルグの不確定性原理って何？

原子や素粒子などの粒子の位置と運動量を測定すると、粒子の状態が一定であって測定値がばらついてしまい、位置と運動量を同時に正確に知ることは出来ないというもの。

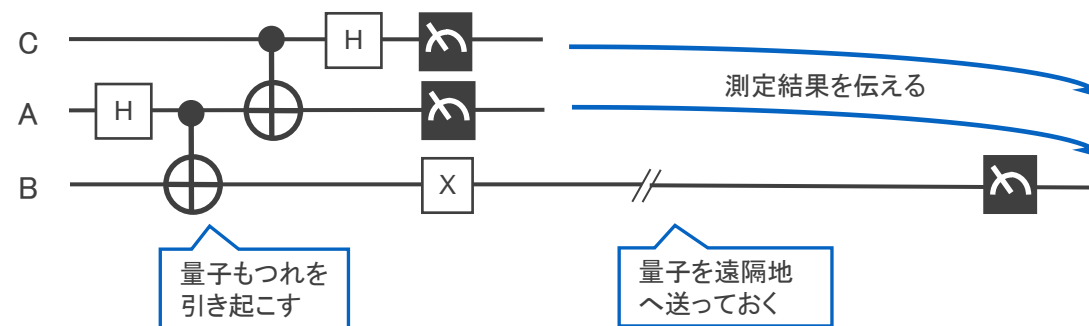


量子通信・量子暗号の場合、測定(=盗聴)を行うと、粒子の状態が変化してしまうため、正確に知ることが出来ず(=正しく解読出来ず)、状態が変化することで測定(=盗聴)したことがばれてしまう。

## 2 量子テレポーテーションって何？

もつれ状態にある量子の一方を遠隔地に送り、もう一方の量子と送りたい量子状態の測定結果を別の手段で送ると、それらを使用して量子状態を復元出来る。このような仕組みで量子状態を遠隔地に転送することを量子テレポーテーションという。

テレポーテーションという名前であるものの、粒子が空間の別の場所に瞬間移動するわけではない。



「量子の一方(B)」を遠隔地に送り、「もう一方の量子(A)」と「送りたい量子状態(C)」の測定結果を別の手段(通常のメール等の古典通信)で送ると、それら(測定結果とB)を使用して量子状態を復元(遠隔地でCを再現)出来る。

量子テレポーテーションは、既に実験で実証されている。

## 3 参考文献

[excite blog](#)

[「いちばんやさしい量子コンピューターの教本」\(株式会社インプレス\)](#)



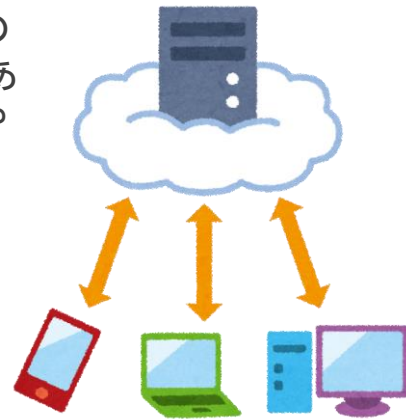
## 1 暗号化とは？

通信や記録媒体へのデータ保存などの際に、第三者がそのデータを見ても、特別な知識なしでは読めないように変換する手法のこと。「暗号化」の対義語(＝誰でも読める状態に変換すること)は「復号化」である。

## 2 現代における暗号

現代社会では、セキュリティが必要となる様々な場面で暗号技術が利用されている。

- **SSL/TLS通信**: ネットワーク上を行き交う情報を暗号化する通信方法。URLが“https”から始まるWebサイトではこの通信方法が使われており、データは暗号化されている。一方、“http”から始まるWebサイトは暗号化がされていないため、第三者に通信内容を見られてしまう恐れがある。
- **デジタル署名**: データを送信する際に、そのデータが送信者から正しく送られたものであることを証明するための技術。なりすましや改ざんを防ぐことができる。
- **ブロックチェーン**: 暗号技術を応用することによって、データの“耐改ざん性”を高めたデータベース。仮想通貨や取引システムなどで利用されている。



## 3 量子コンピュータとの関連

現代社会でよく利用されている暗号技術は、古典的な計算機では解くことが困難とされている問題を応用している。

- よく知られた暗号方式の例
  - **RSA暗号**: 「非常に大きな2つの素数を掛け合わせた数を素因数分解することは困難である」という性質を利用した暗号方式。
  - **楕円曲線暗号**: 楕円曲線上の離散対数問題という数学上の問題の困難さを利用した暗号方式。

量子コンピュータが進歩すれば、こうした問題を現実的な時間で解くことができる(＝暗号が突破される)と考えられている。その結果、暗号を利用している様々な技術の安全性が脅かされることになるため、その対策として量子コンピュータによる攻撃に耐性のある暗号方式(**耐量子暗号**)の標準化が進められている。

- 耐量子暗号の候補例
  - **格子暗号**: 格子問題と呼ばれる数学上の問題の困難さを利用した暗号。格子問題は古典コンピュータでも量子コンピュータでも効率的に解くのが難しいとされている。

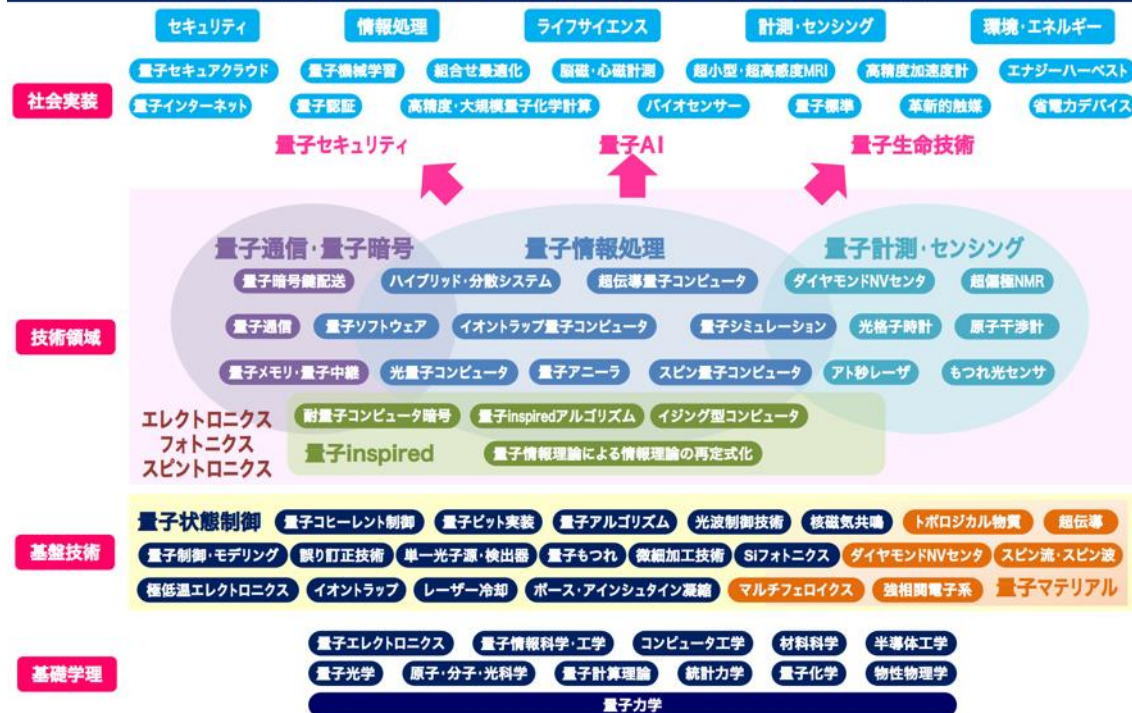
## 4 参考文献

[量子コンピュータに耐性のある暗号技術の標準化動向: 米国政府標準暗号について](#) - 日本銀行金融研究所

## 1 概要

ここまでに触れなかったいくつかの量子技術について、本項で記す。

## 「量子技術イノベーション戦略」が対象とする技術の範囲 (案)



17

## 2 基盤技術: 量子マテリアル

量子マテリアルでは量子情報処理等の革新のみならず、エネルギー変換やエレクトロニクスの革新など現在の技術レベルでは到達が不可能なレベルの機能の実現が期待される。

トポロジカル量子物質

超低消費電力デバイスや新方式の量子コンピュータの実現

エネルギー変換材料

無電源 IoTセンサの実現

スピントロニクス材料

超低消費・大容量メモリの実現

フォトニクス材料

省エネ光源や次世代量子通信の実現

## 3 技術領域: 量子計測・センシング

量子計測・センシングは、量子状態のもろさを逆にとり、従来技術を凌駕する感度・精度を実現する技術を指す。生命・医療技術の向上による健康長寿社会、防災等の安全安心な社会の構築が期待される。

固体量子センサ

脳磁・神経磁場の計測の高度化によるヘルスケア、安全走行、脳疾患の予防・治療

量子慣性センサ

完全自動運転車、自律型無線潜水機

光格子時計

地震・火山防災や物理定数の恒常性検証

もつれ光センサ

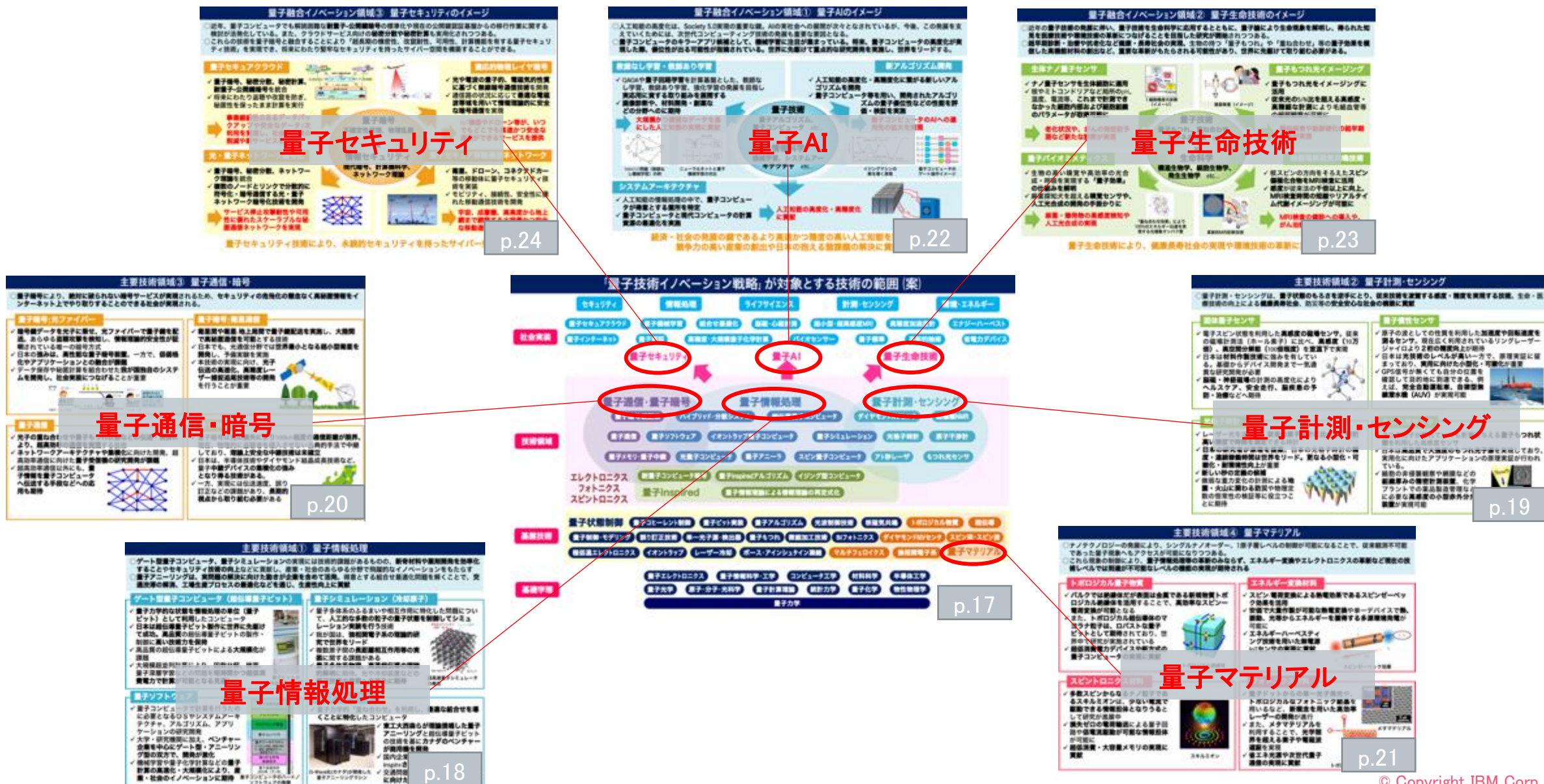
細胞の非侵襲観察や網膜などの組織厚みの精密計測装置、化学プラントでの薬品製造管理などに必要な高感度の小型赤外分光装置

## 4 参考文献

[量子技術イノベーション戦略 中間整理](#)



## 量子技術イノベーション戦略 中間整理の参考マップ



本資料の著作権は、日本アイ・ビー・エム株式会社（IBM Corporationを含み、以下、IBMといいます。）に帰属します。

ワークショップ、セッション、および資料は、IBMまたはセッション発表者によって準備され、それぞれ独自の見解を反映したものです。それらは情報提供の目的のみで提供されており、いかなる参加者に対しても法律的またはその他の指導や助言を意図したものではなく、またそのような結果を生むものでもありません。本資料に含まれている情報については、完全性と正確性を期するよう努力しましたが、「現状のまま」提供され、明示または暗示にかかわらずいかなる保証も伴わないものとします。本資料またはその他の資料の使用によって、あるいはその他の関連によって、いかなる損害が生じた場合も、IBMまたはセッション発表者は責任を負わないものとします。本資料に含まれている内容は、IBMまたはそのサプライヤーやライセンス交付者からいかなる保証または表明を引きだすことを意図したものでも、IBMソフトウェアの使用を規定する適用ライセンス契約の条項を変更することを意図したものでもなく、またそのような結果を生むものでもありません。

本資料でIBM製品、プログラム、またはサービスに言及していても、IBMが営業活動を行っているすべての国でそれらが使用可能であることを暗示するものではありません。本資料で言及している製品リリース日付や製品機能は、市場機会またはその他の要因に基づいてIBM独自の決定権をもっていつでも変更できるものとし、いかなる方法においても将来の製品または機能が使用可能になると確約することを意図したものではありません。本資料に含まれている内容は、参加者が開始する活動によって特定の販売、売上高の向上、またはその他の結果が生じると述べる、または暗示することを意図したものでも、またそのような結果を生むものでもありません。パフォーマンスは、管理された環境において標準的なIBMベンチマークを使用した測定と予測に基づいています。ユーザーが経験する実際のスループットやパフォーマンスは、ユーザーのジョブ・ストリームにおけるマルチプログラミングの量、入出力構成、ストレージ構成、および処理されるワークロードなどの考慮事項を含む、数多くの要因に応じて変化します。したがって、個々のユーザーがここで述べられているものと同様の結果を得られると確約するものではありません。

記述されているすべてのお客様事例は、それらのお客様がどのようにIBM製品を使用したか、またそれらのお客様が達成した結果の実例として示されたものです。実際の環境コストおよびパフォーマンス特性は、お客様ごとに異なる場合があります。

IBM、IBM ロゴは、米国やその他の国におけるInternational Business Machines Corporationの商標または登録商標です。他の製品名およびサービス名等は、それぞれIBMまたは各社の商標である場合があります。現時点でのIBMの商標リストについては、[ibm.com/trademark](http://ibm.com/trademark)をご覧ください。