

# 量子コンピュータとは何か？ —そのしくみと実用性について—

1. 量子力学とは？
2. 量子コンピュータの歴史
3. 量子ビット・量子ゲート
4. 量子コンピュータのしくみ
5. 実際の量子ビットおよび量子コンピュータ
6. 量子コンピュータで何ができるのか
7. 量子コンピュータの現状と課題

話題提供者 出口 博之

# 1. 量子力学とは？

古典力学（ニュートン力学）

マクロな世界の力学

質量×加速度＝力（ $ma = F$ ）

物体の運動はニュートンの運動方程式に従う  
初期条件が与えられれば、運動は決定される

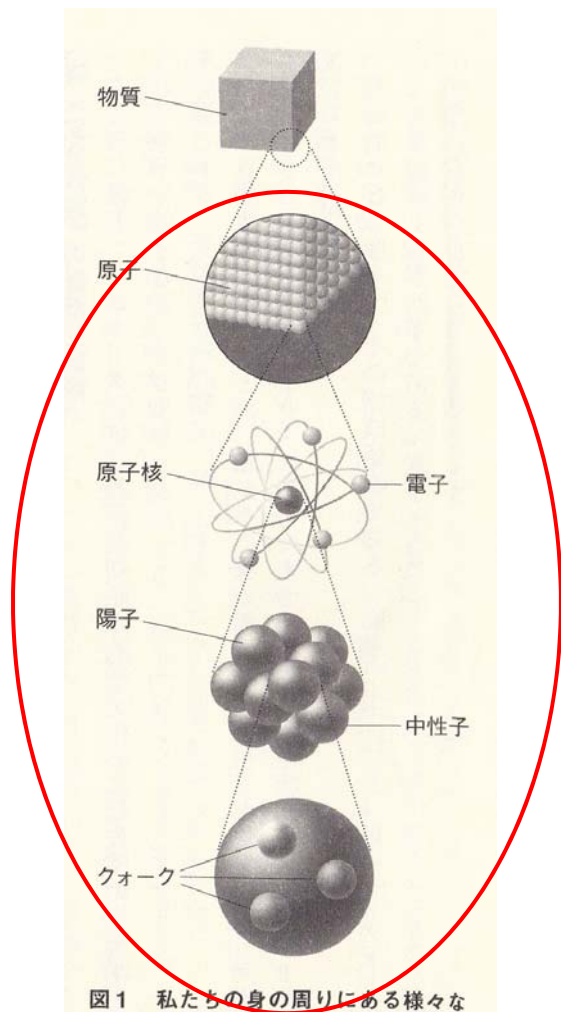


図1 私たちの身の周りにある様々な物質は、非常に小さな量子が集まることによって形作られている

出典：[https://www.mext.go.jp/a\\_menu/shinkou/ryoushi/detail/1316005.htm](https://www.mext.go.jp/a_menu/shinkou/ryoushi/detail/1316005.htm)をもとに編集部作成

## 量子力学 ミクロな世界の力学

$$i\hbar \frac{\partial}{\partial t} \psi(r, t) = -\frac{\hbar^2}{2m} \nabla^2 \psi(r, t) + V(r, t) \psi(r, t)$$

### 図5 シュレディンガー方程式

オーストリアの物理学者エルヴィン・シュレディンガーが1926年に提唱した波動方程式。古典力学における「ニュートンの運動方程式」に匹敵する量子力学の基本方程式。これを中心とする一連の業績により、シュレディンガーは1933年にノーベル物理学賞を受賞

出典：「ゼロからわかる量子コンピュータ」小林雅一著，講談社現代新書(2022)

シュレディンガー方程式の解の波動関数  $\psi(r, t)$  を用いて電子などの状態を表す

# 量子力学の特徴

## 1.1 量子力学の特徴

ここでは、量子力学の代表的な特徴を3つ紹介します。

### (1) 状態の重ね合わせ

物理状態は一般に、物理量の値が決まった状態（固有状態と呼ぶ）の重ね合わせ状態として表されます。つまり、ある物理量について異なる値を持った状態が同時に存在します。

### (2) 測定による状態の変化

重ね合わせ状態において物理量を測定すると、どれか1つの固有状態が選ばれ、それに対応する値が測定されます。ある固有状態が選ばれる確率は、重ね合わせ状態に含まれるその固有状態の“割合”に依存します。したがって、測定される物理量の値は確率的にしか予測できません。

### (3) 量子もつれ状態の存在と非局所性

複数の粒子についての量子状態には、量子もつれ状態と呼ばれる状態が存在します。この状態においては、ある粒子についての測定が離れたところに存在する別の粒子についての測定に影響を与えます。このような特性は量子論の非局所性と呼ばれます。

# 量子力学の現象論的な原理

## 粒子と波の二重性 ド・ブロイの関係式

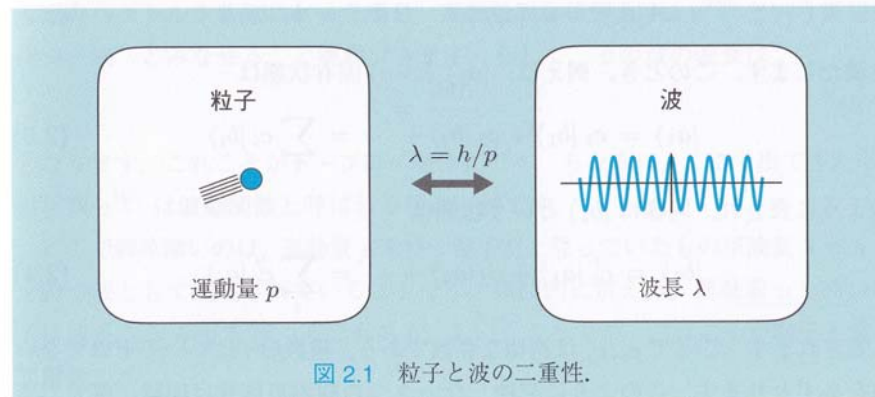
一方では粒子のように振る舞いながら他方では波のような性質を示す

### 2.1 粒子と波の二重性

この節では、量子力学における“現象論的な原理”である粒子と波の二重性とド・ブロイ関係式について紹介します。粒子と波の二重性とは

運動量  $p$  を持つ粒子は、波長  $\lambda = \frac{h}{p}$  を持つ波でもある

という事実を指します (図 2.1)。このとき粒子性と波動性を結びつける関係式  $\lambda = h/p$  はド・ブロイ関係式と呼ばれます。ここで現れた  $h$  はプランク定数と呼ばれ、 $h \approx 6.63 \times 10^{-34} \text{ J}\cdot\text{s}$  という非常に小さい値を持つ物理定数です。プランク定数を  $2\pi$  で割った定数  $\hbar \equiv h/(2\pi)$  を  $\hbar$  (エイチバー) と呼び、今後は頻繁に用います。



出典：「コア・テキスト 量子力学」三角樹弘著，サイエンス社(2023)

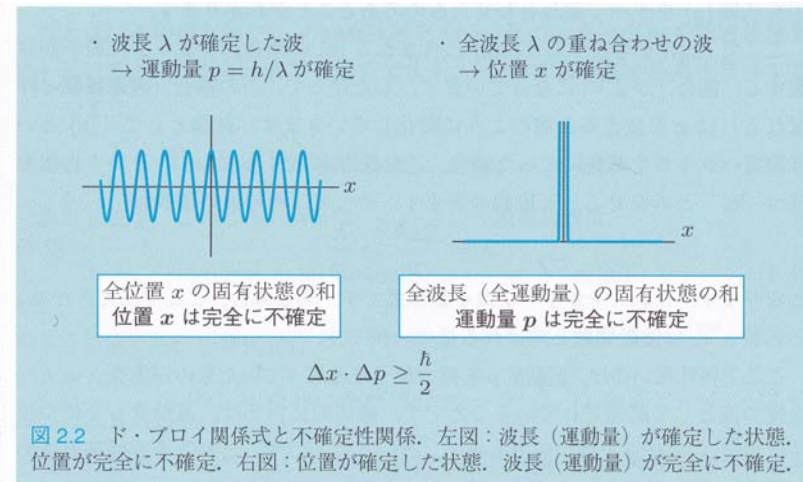
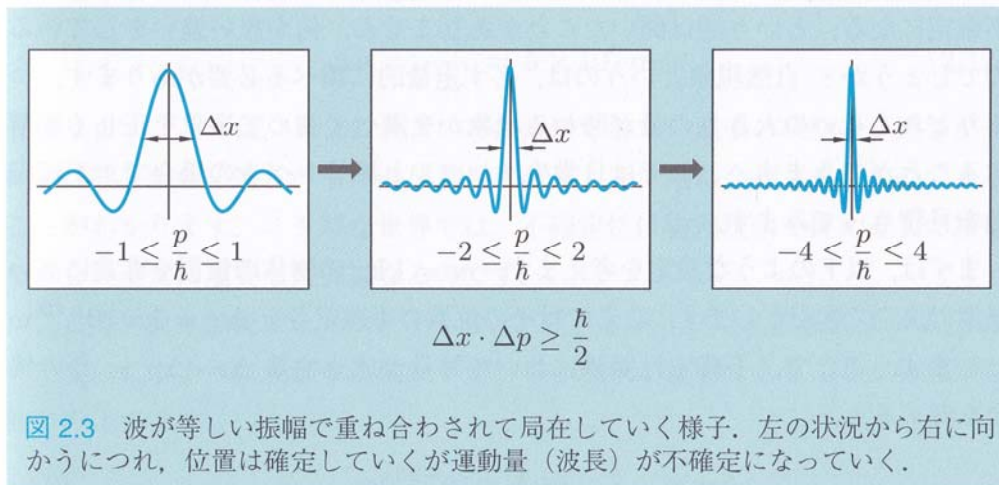
古典物理学では粒子と波は別々のもの

# 量子力学の原理

## 位置と運動量の不確定性関係

粒子の運動量が確定すると、その位置は完全に不確定になる。  
 粒子の位置が確定すると、その運動量は完全に不確定になる。

$$(\text{位置のあいまいさ } \Delta x) \times (\text{運動量のあいまいさ } \Delta p) \geq \text{プランクの定数 } h/2$$



出典：「コア・テキスト 量子力学」三角樹弘著，サイエンス社(2023)

古典力学では、位置と運動量はあいまいさなしで同時に確定する

# 量子力学の性質 運動量とエネルギーの離散性

制限された空間に閉じ込められた粒子の運動量やエネルギーは離散化（量子化）される

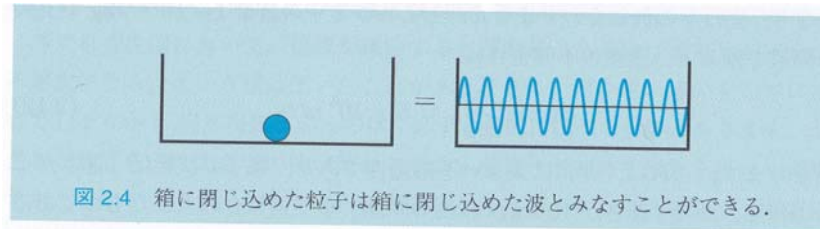


図 2.4 箱に閉じ込めた粒子は箱に閉じ込めた波とみなすことができる。

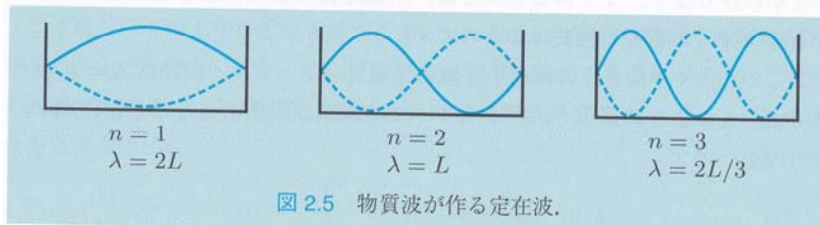


図 2.5 物質波が作る定在波。

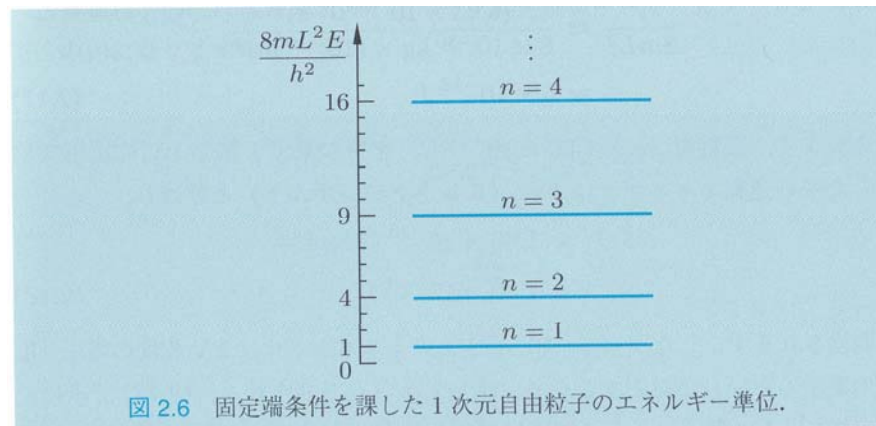


図 2.6 固定端条件を課した 1 次元自由粒子のエネルギー準位。

出典：「コア・テキスト 量子力学」三角樹弘著，サイエンス社(2023)

古典力学では，運動量やエネルギーは連続的に値を変えられる

## 2. 量子コンピュータの歴史

### 量子コンピュータ（量子ゲート方式）

量子力学を計算の原理に応用した次世代コンピュータ

「量子重ね合わせ」と呼ばれる現象を超高速計算の理論に応用  
論理回路に**量子ビット**を用いる

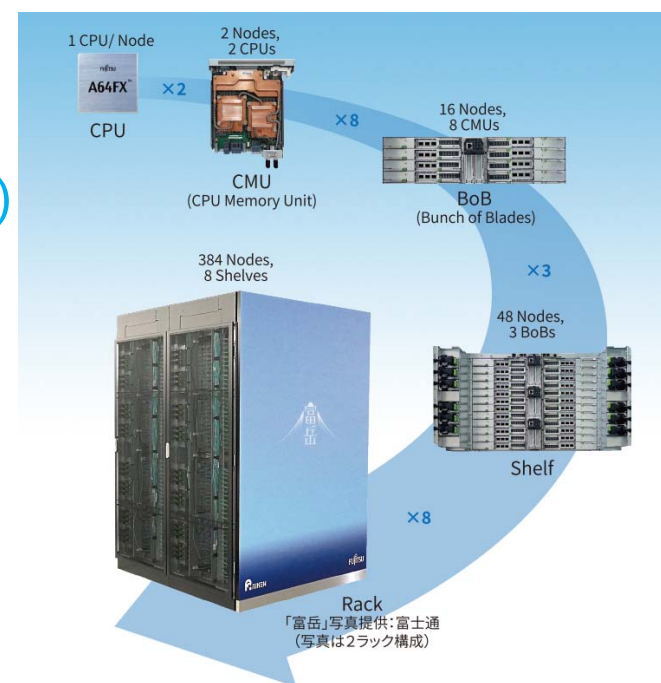
### 従来型コンピュータ（古典コンピュータ）

スーパーコンピュータを頂点とする

デジタル汎用コンピュータ

トランジスタなどの半導体素子を用いる

**ビット**によりデータ処理



スーパーコンピュータ「富岳」

<https://www.r-ccs.riken.jp/fugaku/system/>

# 量子コンピュータのアイデア・理論

1961: IBM **ランダウアー** 「情報消去の原理」を提唱  
なんらかの計算過程で情報が消去される場合に熱が発生する  
可逆計算では熱が発生しないのでエネルギー効率の良い計算  
量子力学に従う計算方法も可逆計算モデルの一つ

**量子コンピュータ開発の端緒**

1980: **ベニオフ** 量子力学の原理に基づいて従来コンピュータと同じ計算  
が可能であることを示した

1981: **ファインマン** 「物理と計算」の会議で「物理のコンピュータ・  
シミュレーション」と題して講演「物理現象をシミュレートするには、  
どんなコンピュータを使うべきだろうか？」「自然をシミュレーション  
したいなら量子力学的に実現すべきだ。」**初めて量子計算の可能性と意義  
を示唆したもの**

1985: **ドイチュ** 量子力学の重ね合わせの原理によってある種の並列計算  
が実現できる 量子チューリングマシンの定式化



# 量子コンピュータの歴史

## 図9 量子コンピュータの歴史

### 1980年代 量子コンピュータの誕生

- アイデアの提唱 (ファインマン、1982)
- 計算の基礎理論 (ドイッチュ、1985)

### 1990年代 量子コンピュータの活用方法の発見

- 素因数分解の解法の発見 (ショア、1994)
- 量子コンピュータ特有の様々な解法の発見

### 2000年代 ハードウェア開発が進展

- 様々な方式で量子コンピュータの基礎実験

### 2010年代 大手企業が開発に参戦し、ブーム到来

- Googleが量子コンピュータの独自開発を開始 (2014)
- IBMが量子コンピュータの販売を開始 (2019)

出典：「量子コンピュータが本当にわかる！」武田俊太郎著，技術評論社(2020)

# 量子コンピュータのトピック

Nature Vol 574, 505, 24 OCTOBER 2019

Googleの研究チーム 量子コンピュータの計算速度がスーパーコンピュータを越えた！（量子超越性）と発表

Article

## Quantum supremacy using a programmable superconducting processor

<https://doi.org/10.1038/s41586-019-1666-5>

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute<sup>1</sup>, Kunal Arya<sup>1</sup>, Ryan Babbush<sup>1</sup>, Dave Bacon<sup>1</sup>, Joseph C. Bardin<sup>1,2</sup>, Rami Barends<sup>1</sup>, Rupak Biswas<sup>2</sup>, Sergio Boixo<sup>1</sup>, Fernando G. S. L. Brandao<sup>1,4</sup>, David A. Buell<sup>1</sup>, Brian Burkett<sup>1</sup>, Yu Chen<sup>1</sup>, Zijun Chen<sup>1</sup>, Ben Chiaro<sup>1</sup>, Roberto Collins<sup>1</sup>, William Courtney<sup>1</sup>, Andrew Dunsworth<sup>1</sup>, Edward Farhi<sup>1</sup>, Brooks Foxen<sup>1,5</sup>, Austin Fowler<sup>1</sup>, Craig Gidney<sup>1</sup>, Marissa Giustina<sup>1</sup>, Rob Graff<sup>1</sup>, Keith Guerin<sup>1</sup>, Steve Habegger<sup>1</sup>, Matthew P. Harrigan<sup>1</sup>, Michael J. Hartmann<sup>1,6</sup>, Alan Ho<sup>1</sup>, Markus Hoffmann<sup>1</sup>, Trent Huang<sup>1</sup>, Travis S. Humble<sup>1</sup>, Sergei V. Isakov<sup>1</sup>, Evan Jeffrey<sup>1</sup>, Zhang Jiang<sup>1</sup>, Dvir Kafri<sup>1</sup>, Kostyantyn Kechedzhi<sup>1</sup>, Julian Kelly<sup>1</sup>, Paul V. Klimov<sup>1</sup>, Sergey Knysch<sup>1</sup>, Alexander Korotkov<sup>2,5</sup>, Fedor Kostritsa<sup>1</sup>, David Landhuis<sup>1</sup>, Mike Lindmark<sup>1</sup>, Erik Lucero<sup>1</sup>, Dmitry Lyakh<sup>1</sup>, Salvatore Mandrà<sup>3,7</sup>, Jarrod R. McClean<sup>1</sup>, Matthew McEwen<sup>1</sup>, Anthony Megrant<sup>1</sup>, Xiao Mi<sup>1</sup>, Kristel Michielsen<sup>1,10</sup>, Masoud Mohseni<sup>1</sup>, Josh Mutus<sup>1</sup>, Ofer Naaman<sup>1</sup>, Matthew Neeley<sup>1</sup>, Charles Neill<sup>1</sup>, Murphy Yuezhen Niu<sup>1</sup>, Eric Ostby<sup>1</sup>, Andre Petukhov<sup>1</sup>, John C. Platt<sup>1</sup>, Chris Quintana<sup>1</sup>, Eleanor G. Rieffel<sup>1</sup>, Pedram Roushan<sup>1</sup>, Nicholas C. Rubin<sup>1</sup>, Daniel Sank<sup>1</sup>, Kevin J. Satzinger<sup>1</sup>, Vadim Smelyanskiy<sup>1</sup>, Kevin J. Sung<sup>1,2</sup>, Matthew D. Trevithick<sup>1</sup>, Amit Vainsencher<sup>1</sup>, Benjamin Villalonga<sup>1,4</sup>, Theodore White<sup>1</sup>, Z. Jamie Yao<sup>1</sup>, Ping Yeh<sup>1</sup>, Adam Zalcman<sup>1</sup>, Hartmut Neven<sup>1</sup> & John M. Martinis<sup>1,2\*</sup>

53量子ビットの量子プロセッサ「シカモア」がスパコン「IBMサミット」でも1万年以上かかる特殊な計算問題（ランダム量子回路サンプリング）をわずか200秒で計算  
量子コンピュータに有利な計算問題での比較

IBMは2日半で計算できると後日反論 過大評価

出典：「量子技術の基本と仕組み」若狭直道著，秀和システム(2020)

COLUMN

## 量子超越性

2019年、グーグルのSycamore（シカモア）が量子超越性を達成したと報道され、世界中に衝撃を与えました。

量子超越性とは、“これまでの技術では達成できなかった計算を、量子技術を使えば達成可能なこと”を指します。グーグルの広報によると、スーパーコンピュータが1万年かかる計算を200秒で済ませた、ということです。

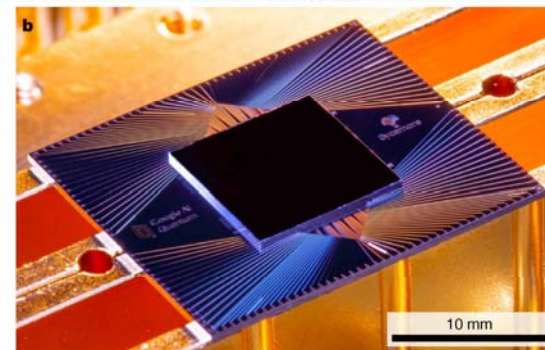
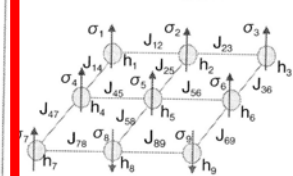
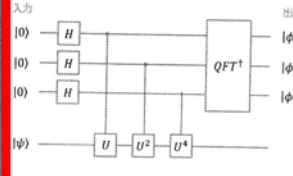
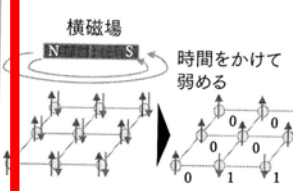


Fig. 1 | The Sycamore processor. a, Layout of processor, showing a rectangular array of 54 qubits (grey), each connected to its four nearest neighbours with couplers (blue). The inoperable qubit is outlined. b, Photograph of the Sycamore chip.

# 量子コンピュータの2つの方式

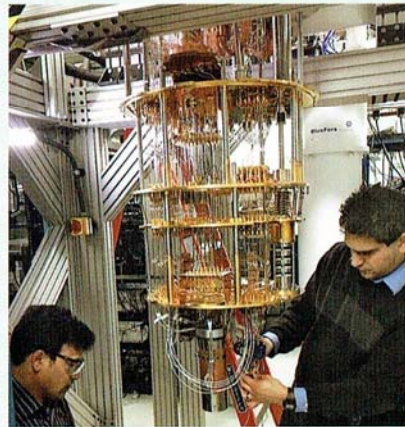
図表 1-3 量子コンピュータのプロセス (解法手順)

量子ゲート方式	量子アニーリング方式								
課題・プログラムの抽出	課題・プログラムの抽出								
量子アルゴリズムを検討	問題をハミルトニアン(エネルギー)で与えられるイジングモデル $H(\sigma)$ (またはQUBO)に定式化								
量子アルゴリズム	$H(\sigma) = -\sum_{i<j} J_{ij}\sigma_i\sigma_j - \sum_{i=1}^N h_i\sigma_i$ <p> <math>\sigma</math>: 変数の組 <math>\{\sigma_1, \sigma_2, \dots, \sigma_N\}</math>  <math>N</math>: スピンの数 (整数)  <math>\sigma_i</math>: イジングスピン (<math>\{1, -1\}</math> を取る変数)  <math>J_{ij}</math>: スピン間の相互作用  <math>h_i</math>: 局所磁場                 </p>								
<table border="1"> <thead> <tr> <th>名称</th> <th>主な用途</th> </tr> </thead> <tbody> <tr> <td>Shor</td> <td>素因数分解</td> </tr> <tr> <td>Grover</td> <td>データ探索</td> </tr> <tr> <td>...</td> <td>...</td> </tr> </tbody> </table>	名称	主な用途	Shor	素因数分解	Grover	データ探索	...	...	定式化したモデルの係数データ (各変数間の結合強度 ( $J_{ij}$ ) と各変数の重み付け ( $h_i$ )) を量子コンピュータに設定
名称	主な用途								
Shor	素因数分解								
Grover	データ探索								
...	...								
量子コンピュータに対して量子ゲートを適切に配置し、量子回路を作成									
量子ビットに対して、さまざまな操作を行う	磁場を印加し、時間をかけて弱めると、ハミルトニアンを最小化する解が返る								
									
測定	計算結果の読み出し								

**量子ゲート方式 汎用性あり こちらの方式について今後説明する**

## 汎用量子コンピューター

一般的に量子コンピューターといえば汎用的な計算ができるものを指し、その典型的なものが「量子ゲート」とよばれる計算 (演算) をくりかえし行うことで量子ビットを処理していく「ゲート型」です。将来、さまざまな量子アルゴリズムが考案されれば、現在私たちが使用しているコンピューターと同じようにさまざまな機能を実現できる、汎用的なコンピューターになると考えられています。左下の写真は、IBMが開発している超伝導回路型の量子コンピューター (冷凍機から外に出した状態) です。



## 量子アニーリングマシン

組み合わせ最適化問題を実用的に解くことを得意とした量子コンピューターです。D-Wave社の量子コンピューター (右の写真) の量子ビットは5000をこえており、デンソーやフォルクスワーゲン、アクセンチュアなど世界の企業で実用的な導入が進んでいます。



## 量子アニーリング方式

出典：「量子論のすべて 改訂第2版」Newton別冊，ニュートンプレス(2021)

出典：「量子コンピュータまるわかり」間瀬英之・身野良寛著，日経文庫，日本経済新聞出版社(2023)

# 3. 量子ビット・量子ゲート

## 量子ビットと従来のビット

従来のビットは、ある時点で「0」か「1」のどちらかの値をとる  
量子ビットは、同時に「0」と「1」という2つの状態を取りえる。

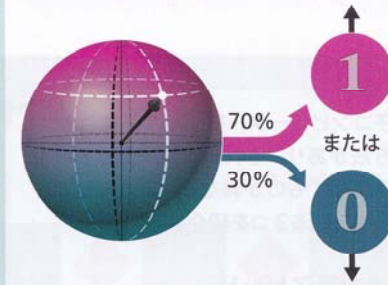
### ビット vs. 量子ビット

量子コンピューターは量子力学の法則を利用して、古典コンピューターを上回る能力を実現している。量子ビットは複数の状態の「重ね合わせ」になることができる。量子もつれと呼ばれる量子現象は、量子ビットを特殊な方法で相関させる。量子もつれになった2個の量子ビットは、個々に測定するとそれぞれ結果がランダムに表れるが、両方をまとめて見ると、それぞれの状態が相手の状態と相関している。2個の量子ビットが量子もつれになると、独立の量子ビット2個よりも多くの情報を記憶できる。

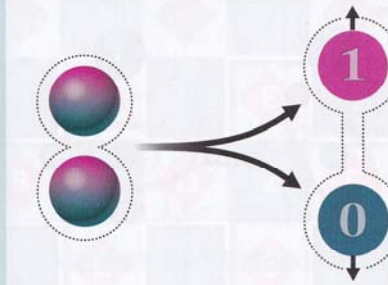
**従来のビット** 従来のコンピューターの古典ビットはコインの裏表のように、0と1のいずれかの状態を取る。



**量子ビットになると……** 量子ビットは、古典ビットよりもっと多くの状態を取りうる。量子ビットの状態は、球面上の様々な座標の点だと考えることができる。右にその一例（1が70%、0が30%の重ね合わせ）を示した。量子ビット1個が重ね合わせ状態にある場合、取りうる座標は無限個ある。しかしその量子ビットを直接測定すると、重ね合わせだった可能性は「崩壊」して、1か0のどちらかに確定する。



**さらに量子もつれになると……** 2個の量子ビットが量子もつれになると、それらの状態は独立ではなくなり、お互い相手の状態に依存する。もつれた量子ビットの一方の状態を測定すると、他方の状態は測定しなくてもわかる。この相関は、2個の量子ビットが物理的にどれだけ離れていても消えない。



Graphics by Jen Christiansen

# 量子ビットとは?

量子ビットの表現 0の状態 $|0\rangle$ と1の状態 $|1\rangle$ の重ね合わせ

$$|\Phi\rangle = \alpha |0\rangle + \beta |1\rangle \dots\dots ①$$

$$\alpha = \cos\theta, \quad \beta = \sin\theta \dots\dots ③$$

$$|\Phi\rangle = \cos\theta |0\rangle + \sin\theta |1\rangle \dots\dots ④$$

$$\alpha^2 + \beta^2 = 1 \dots\dots ②$$

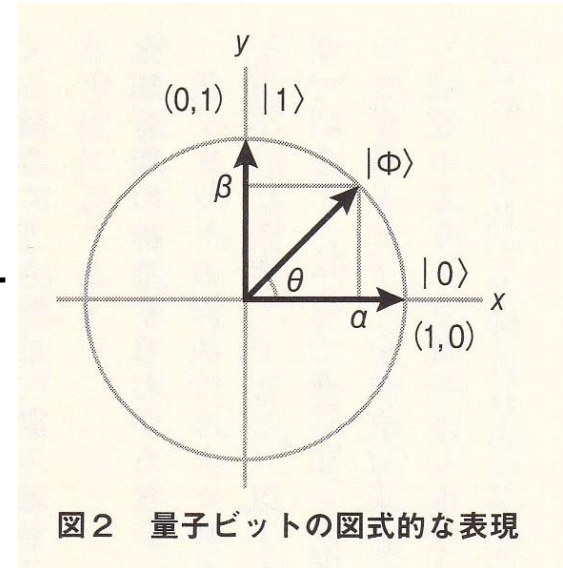


図2 量子ビットの図式的な表現

$\alpha^2$ :0の状態をとる確率,  $\beta^2$ :1の状態をとる確率

量子ビット $|\Phi\rangle$ は, 原点から半径1の円周上の1点に向かうベクトルで表現

$\theta$ は $0^\circ \sim 360^\circ$  まで連続的に変化 無限の値をとる

出典: 「ゼロからわかる量子コンピュータ」 小林雅一著, 講談社現代新書(2022)

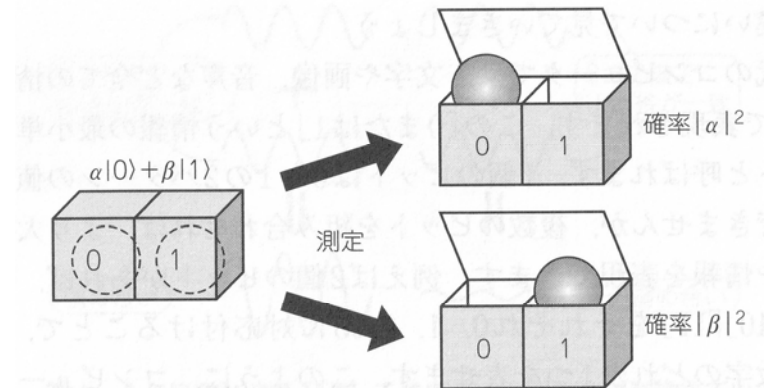


図5 量子ビットは測定すると0か1に確率的に決まる

出典: 「ラズパイ電子工作&光の実験で理解する量子コンピュータ」 藤井啓祐, 武田俊太郎著CQ文庫, CQ出版(2022)

# 量子重ね合わせの原理

マクロ（古典）の世界の状態

ミクロ（量子）の世界の状態

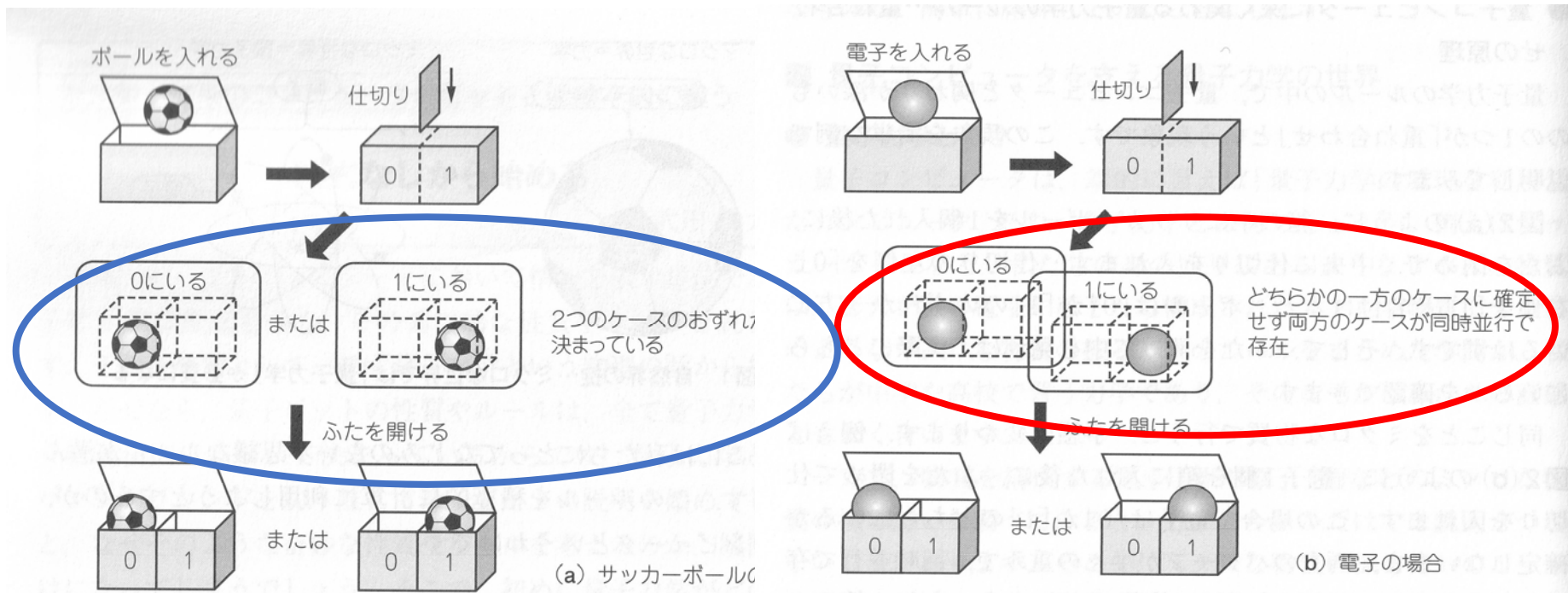


図2 ミクロの世界の量子力学では「0」にも「1」にも確定していない「重ね合わせ状態」がある

0か1のどちらか一方の状態

0と1の重ね合わせの状態

出典：「ラズパイ電子工作&光の実験で理解する量子コンピュータ」藤井啓祐，武田俊太郎著CQ文庫，CQ出版(2022)

# 従来のビットと量子ビットのちがい

3ビットの場合の比較 従来のビットは同時に「000」「001」「010」「011」「100」「101」「110」「111」のどれか1つの状態しか取りえないが、量子ビットでは、同時にこれらのすべての2の3乗の8つの状態を取りえる  
**同時並列的に次の状態に推移 量子並列性が高速計算を可能**

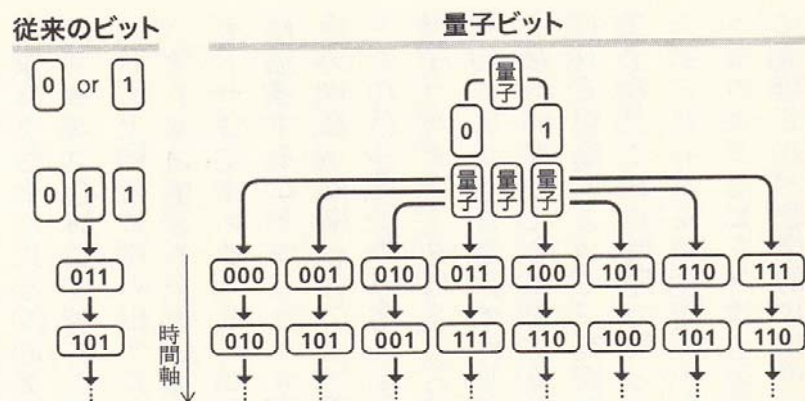


図1 従来のビットと量子ビットの違い  
 3ビットを例にとると、従来のビット(左)では同時に1個の状態(3ケタの2進数)しか取り得ないが、量子ビット(右)では同時に(2の3乗)=8個の状態を取り得る。これらの状態が時々刻々と次の状態へと推移していく。コンピュータによる情報処理(計算)とは本来そういうものだが、特に量子コンピュータ(量子ビット)の場合、複数の状態が同時並列的に次の状態へと推移していくので、従来のコンピュータ(ビット)に比べて何倍も速く計算を行うことができる。これが量子並列性と呼ばれる特徴だ 出典：<https://serokell.io/blog/modeling-large-quantum-computers>をもとに編集部作成

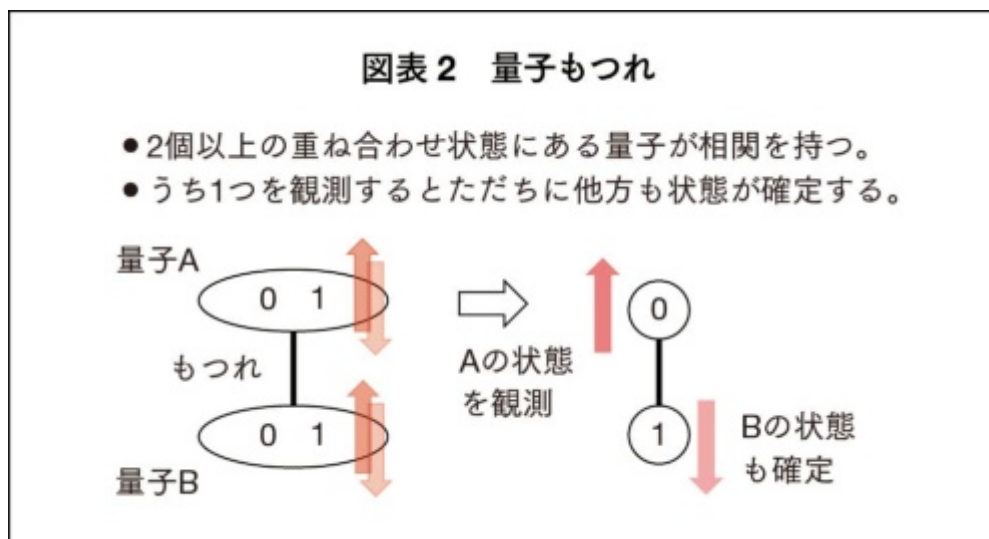
表1 量子ビット数と必要になる古典メモリの数

量子ビットの数	古典コンピュータで表現したら
10	2 <sup>10</sup> =1024 個の複素数 16 キロバイト テキスト
20	2 <sup>20</sup> =100 万個の複素数 16 メガバイト 音楽
30	2 <sup>30</sup> =10 億個の複素数 16 ギガバイト 映画
⋮	スパコン(京コンピュータ)のメモリ =1.26 ペタバイト
50	2 <sup>50</sup> =1000 兆個の複素数 16 ペタバイト
⋮	
170	10 <sup>51</sup> バイト 地球にある原子の数 10 <sup>50</sup>
⋮	
270	10 <sup>81</sup> バイト 宇宙にある原子の数 10 <sup>80</sup>

270 量子ビットの重ね合わせ状態をすべて古典メモリに書き出そうとすると、宇宙全体の原子を用いてメモリを作っても足りない。

出典：「ゼロからわかる量子コンピュータ」小林雅一著，講談社現代新書(2022)

# 量子もつれとは？



量子コンピューターで計算するためには、意図的に量子の状態を変化させられなければなりません。それに利用されるのが**量子もつれ**です。2つの量子を量子もつれの状態にすると、この2つの量子の間にはある関係性が生まれます。量子もつれの関係にある量子は、それぞれの量子の基本的な性質によって、観察されるまでは「0」と「1」が重ね合わされている、どっちつかずの状態です。しかし、どちらかの量子が観察されるとその瞬間に、もう一方の量子の状態が収束してしまうのです。

出典：「量子コンピューターまるわかり」間瀬英之・身野良寛著，日経文庫，日本経済新聞出版社(2023)



# 論理演算 (ゲート)

## 従来コンピュータの論理ゲートと量子ゲート



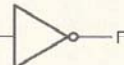


論理演算	論理ゲート	該当する算術演算	真理値表															
AND		$F = A \cdot B$ or $F = AB$	<table border="1"> <thead> <tr><th>A</th><th>B</th><th>F</th></tr> </thead> <tbody> <tr><td>0</td><td>0</td><td>0</td></tr> <tr><td>0</td><td>1</td><td>0</td></tr> <tr><td>1</td><td>0</td><td>0</td></tr> <tr><td>1</td><td>1</td><td>1</td></tr> </tbody> </table>	A	B	F	0	0	0	0	1	0	1	0	0	1	1	1
A	B	F																
0	0	0																
0	1	0																
1	0	0																
1	1	1																
OR		$F = A + B$	<table border="1"> <thead> <tr><th>A</th><th>B</th><th>F</th></tr> </thead> <tbody> <tr><td>0</td><td>0</td><td>0</td></tr> <tr><td>0</td><td>1</td><td>1</td></tr> <tr><td>1</td><td>0</td><td>1</td></tr> <tr><td>1</td><td>1</td><td>1</td></tr> </tbody> </table>	A	B	F	0	0	0	0	1	1	1	0	1	1	1	1
A	B	F																
0	0	0																
0	1	1																
1	0	1																
1	1	1																
NOT		$F = \bar{A}$ or $F = A'$	<table border="1"> <thead> <tr><th>A</th><th>F</th></tr> </thead> <tbody> <tr><td>0</td><td>1</td></tr> <tr><td>1</td><td>0</td></tr> </tbody> </table>	A	F	0	1	1	0									
A	F																	
0	1																	
1	0																	
NAND		$F = (\overline{AB})$	<table border="1"> <thead> <tr><th>A</th><th>B</th><th>F</th></tr> </thead> <tbody> <tr><td>0</td><td>0</td><td>1</td></tr> <tr><td>0</td><td>1</td><td>1</td></tr> <tr><td>1</td><td>0</td><td>1</td></tr> <tr><td>1</td><td>1</td><td>0</td></tr> </tbody> </table>	A	B	F	0	0	1	0	1	1	1	0	1	1	1	0
A	B	F																
0	0	1																
0	1	1																
1	0	1																
1	1	0																
NOR		$F = \overline{(A+B)}$	<table border="1"> <thead> <tr><th>A</th><th>B</th><th>F</th></tr> </thead> <tbody> <tr><td>0</td><td>0</td><td>1</td></tr> <tr><td>0</td><td>1</td><td>0</td></tr> <tr><td>1</td><td>0</td><td>0</td></tr> <tr><td>1</td><td>1</td><td>0</td></tr> </tbody> </table>	A	B	F	0	0	1	0	1	0	1	0	0	1	1	0
A	B	F																
0	0	1																
0	1	0																
1	0	0																
1	1	0																

図6 ブール代数に基づくコンピュータの「ゲート (論理回路)」




呼び名	量子ゲート	該当する行列
NOT		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
アダマール		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
CNOT (Controlled NOT)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

図7 量子コンピュータの基本的な論理演算を行う「量子ゲート」  
ここに示した3種類以外にもいくつかあるし、これら基本的な量子ゲートを多数組み合わせ、より複雑で大規模な量子ゲートを作ることできる

### 従来のコンピュータのゲート (論理回路)

### 量子コンピュータの量子ゲート

出典：「ゼロからわかる量子コンピュータ」小林雅一著,  
講談社現代新書(2022)

# 量子ゲートの演算 行列とベクトルの積

行列とベクトルの積 (掛け算)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a \times x + b \times y \\ c \times x + d \times y \end{pmatrix} \dots\dots ⑦$$

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \times 1 + 1 \times 0 \\ 1 \times 1 + 0 \times 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \dots\dots ⑧$$

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \times 0 + 1 \times 1 \\ 1 \times 0 + 0 \times 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \dots\dots ⑨$$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \dots\dots ⑩$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \dots\dots ⑪$$

## NOT Xの演算

|0>の状態を|1>に反転

|1>の状態を|0>に反転

## アダマール Hの演算

|0>または|1>の状態に作用させると  
|0>と|1>の「重ね合わせ状態」を作り出す

## CNOTの演算

同時に2個の量子ビットに作用する  
行列. 2個の量子ビットが互いに相  
関しながら変化する「量子もつれ」  
と呼ばれる状態を実現できる.

出典: 「ゼロからわかる量子コンピュータ」 小林雅一著,  
講談社現代新書(2022)

# 従来のゲート回路と量子ゲート回路

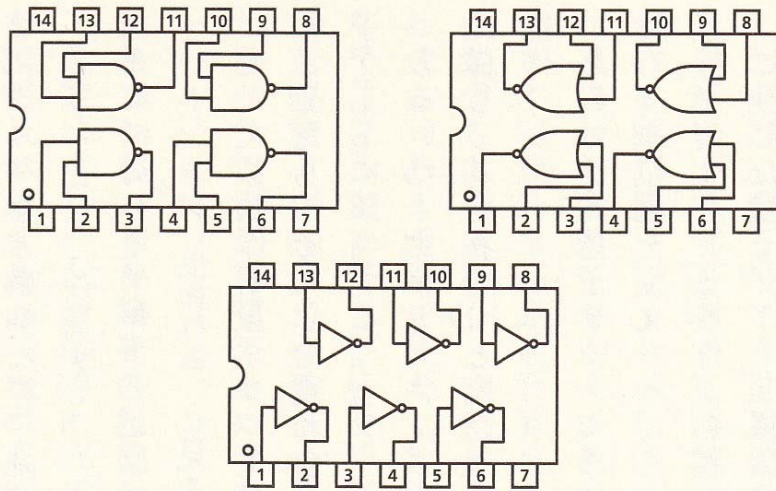


図8 従来のゲート回路

半導体基板上にトランジスタ等からなる各種ゲートが配置された静的な回路図で表現される

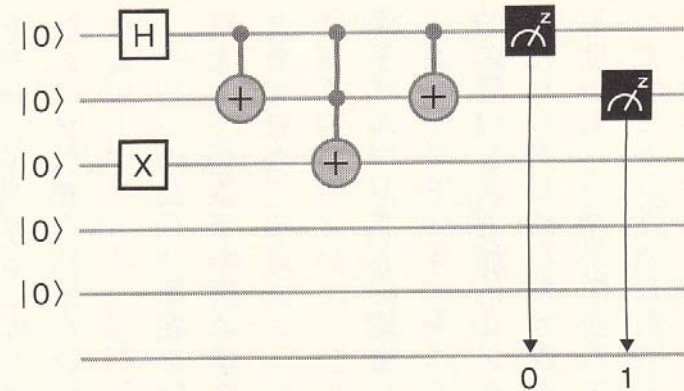


図9 量子ゲート回路

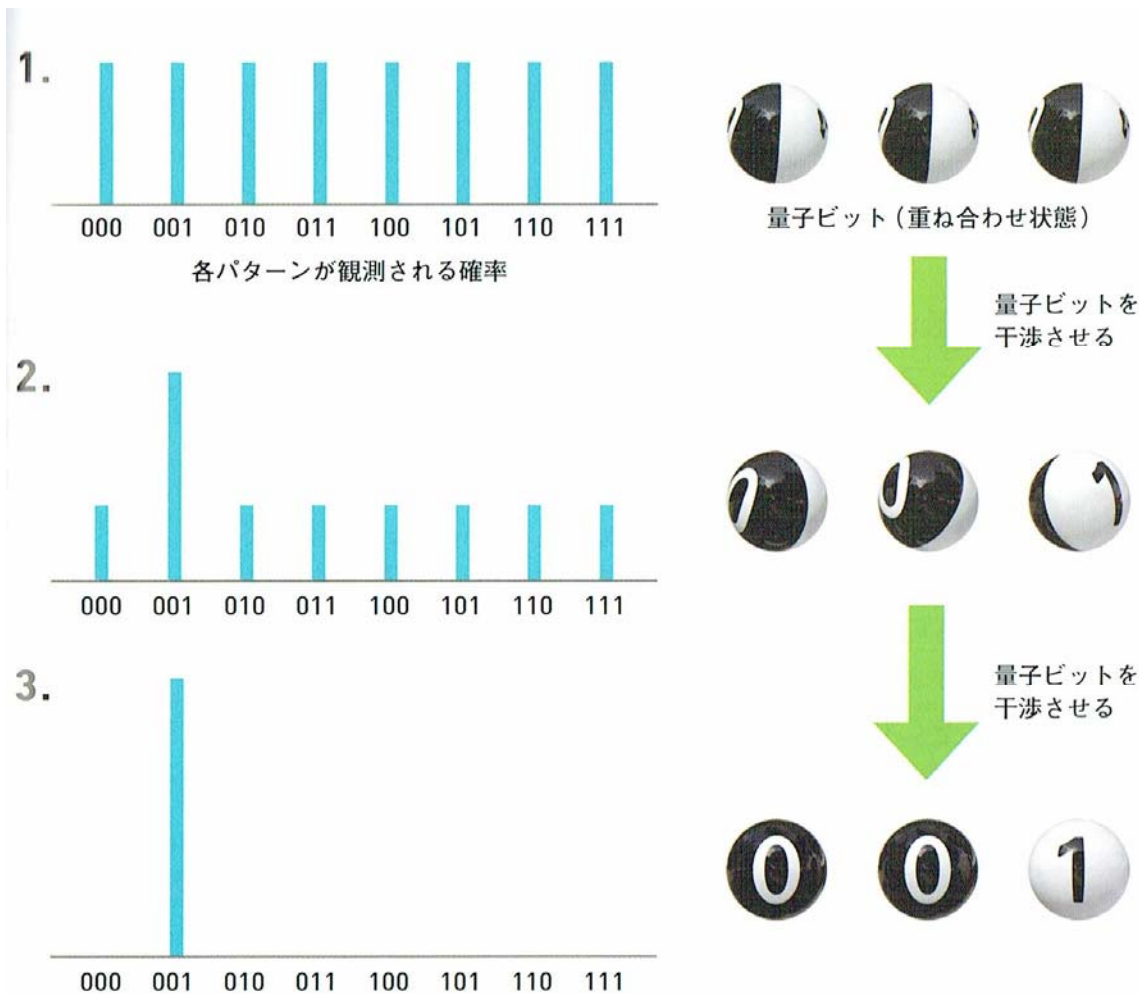
固定的な回路（ハードウェア）というより、動的な操作指示書（ソフトウェア）と見るべき。それによる量子計算は左から右方向へと進む。左端に並んだ  $|0\rangle$  の初期状態から始まり、これらにHやXなどで示された各種ゲート（演算子、行列）を作用させることによって計算が進んでいく。最終的には、メーターのシンボルで示された測定行為によって計算結果が判明する

従来のコンピュータのゲート（論理回路）はトランジスタなど電子部品の回路として実現されている。量子ゲートは、量子ビットに対する一種のオペレーション（操作行為）である。

出典：「ゼロからわかる量子コンピュータ」小林雅一著，  
講談社現代新書(2022)

## 4. 量子コンピュータのしくみ 量子アルゴリズム (計算の手順)

出典：「量子論のすべて 改訂第2版」  
Newton別冊，ニュートンプレス(2021)



### 量子アルゴリズムの考え方

量子アルゴリズムを使って、希望する答え (たとえば、最も距離が短くなる道順) を得るまでの流れを模式的にえがきました。

量子コンピュータの中で三つの量子ビットが重ね合わせ状態にあり、「000」～「111」の全8パターンを同時にあらわしているとします。初期状態 (1) では、どのパターンも均等に観測される可能性があります。棒の長さは、各パターンが観測される確率をあらわしています。

「001」が最も条件に合う (最も距離が短い) パターンだとします。量子ビットの重ね合わせ状態を維持したまま、特定の条件で量子ビットどうしを干渉 (相互作用) させると、特定のパターンが観測される確率のみを高め、そのほかのパターンが観測されないようにすることができます (2～3)。その結果、条件に合うパターンのみを観測することができるのです。

従来のコンピュ「波の干渉」や「量子もつれ」を組み合わせ、並列的に広がった計算プロセスを絞りこむ。「波束の収縮」によって複数個の状態を1つの状態に収束させて解を求める。

# 量子アルゴリズムの具体例「ショアのアルゴリズム」(1994)

## 素因数分解の量子アルゴリズム

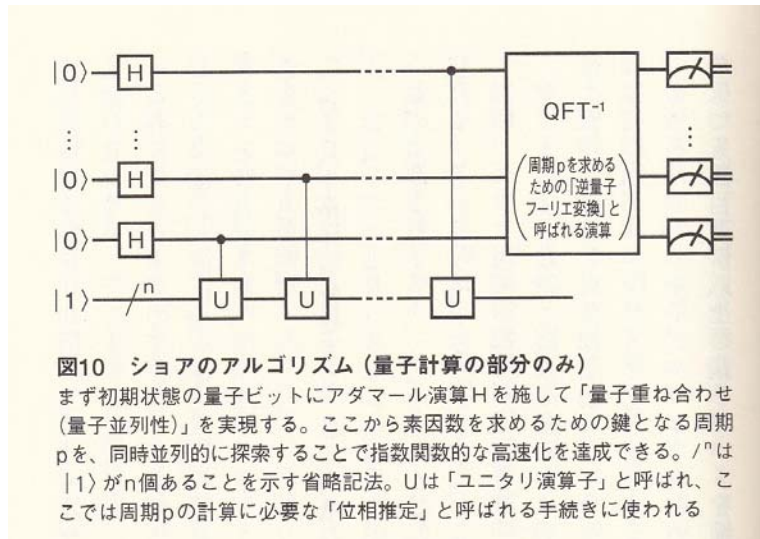
素因数分解  $91 = 7 \times 13$

素因数分解の対象の数がある桁数以上になると、分解することがスパコンを用いても困難

そのため現在RSA暗号の公開鍵におおむね600桁以上の合成数（2つの素数の積）が用いられている

素因数を求める鍵となる周期 $p$ をショアのアルゴリズムで超並列計算することで指数関数的な高速化を達成できる。

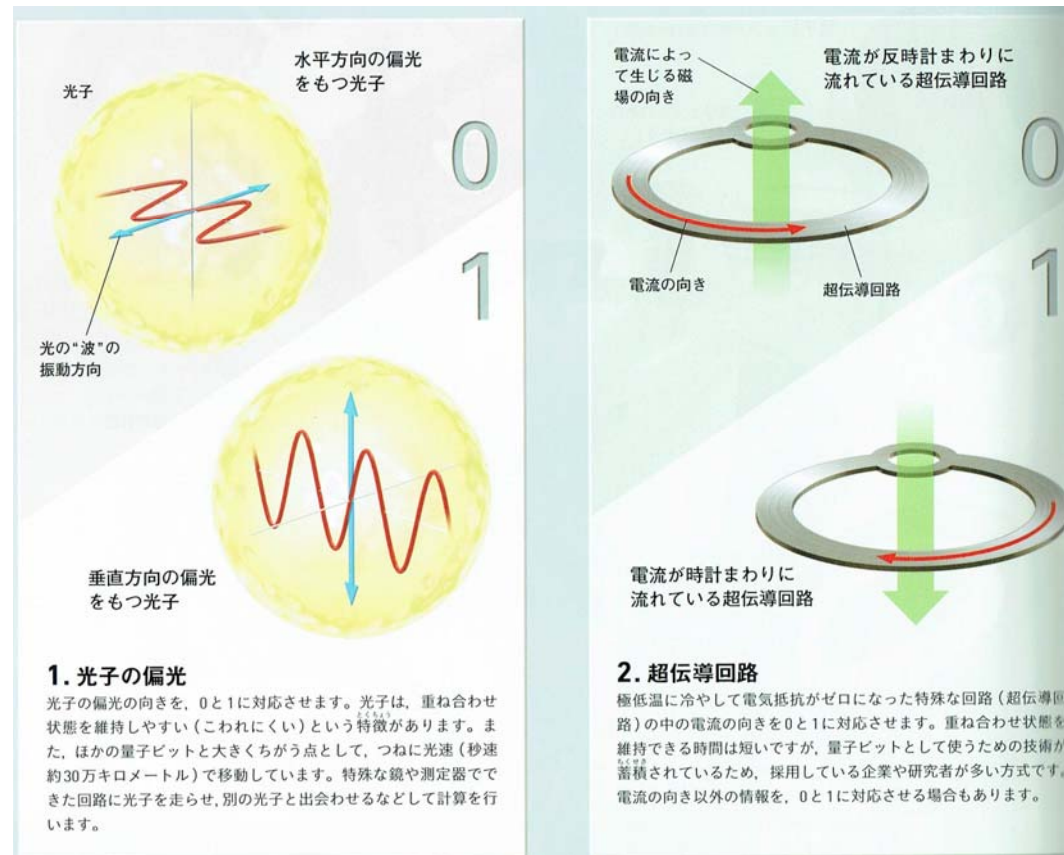
本格的な量子コンピュータでショアのアルゴリズムを用いればRSA暗号を破ることができる



出典：「ゼロからわかる量子コンピュータ」  
小林雅一著、講談社現代新書(2022)

# 5. 実際の量子ビットおよび量子コンピュータ

## 実際の量子ビットの例1



出典：「量子論のすべて 改訂第2版」Newton別冊，  
ニュートンプレス(2021)

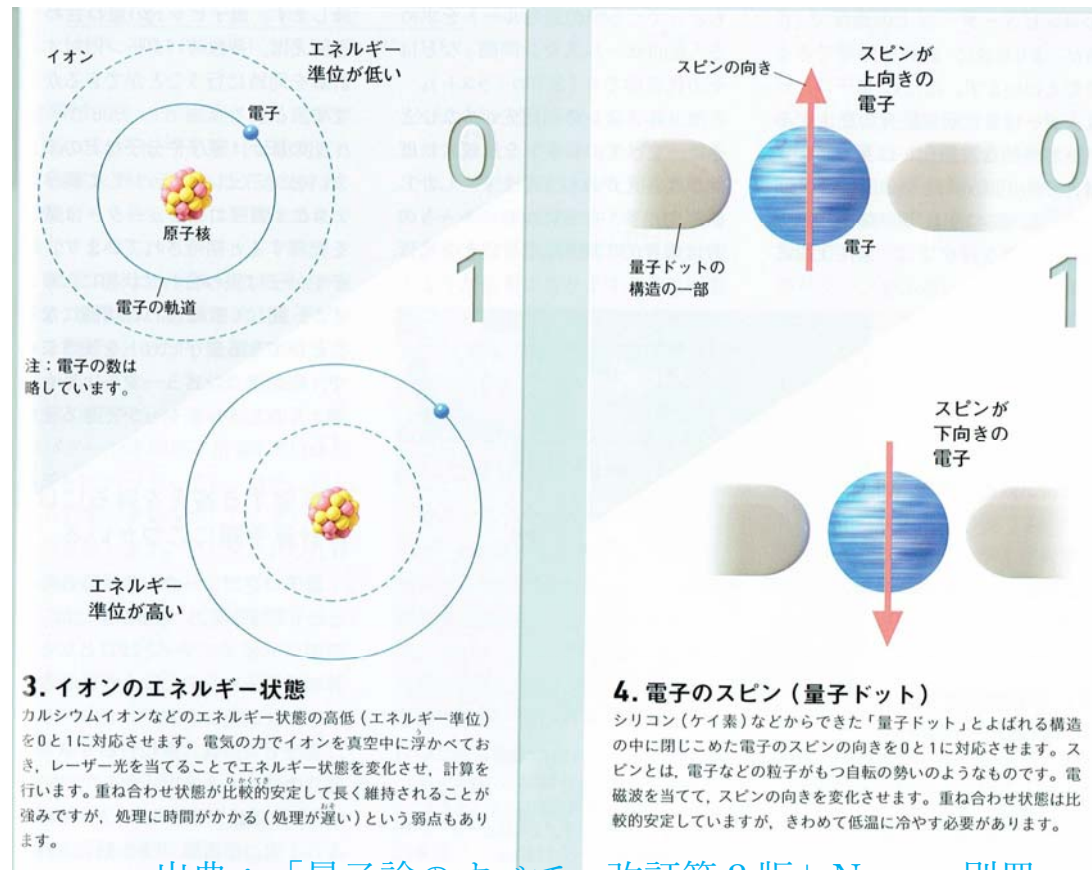
光量子ビット：光子の偏光において横方向の振動を0，縦方向の振動を1として

この重ね合わせ状態で量子ビットを表現

超伝導量子ビット（磁束量子ビット）：超伝導微小リングに流れる円電流の右回りを0，

左回りを1としてその重ね合わせ状態で量子ビットを表現

# 実際の量子ビットの例2



出典：「量子論のすべて 改訂第2版」Newton別冊，  
ニュートンプレス(2021)

イオン・トラップ量子ビット：真空中に浮かせたイオンの基底状態を0，  
励起状態を1として，この重ね合わせ状態で量子ビットを表現

量子ドット：シリコンからできた微小空間の量子ドットに閉じ込められた  
電子のスピンの上向きを0，下向きを1として，この重ね合わせ状態で量子  
ビットを表現

## 実際の量子ビット回路および量子プロセッサ(CPU)の例

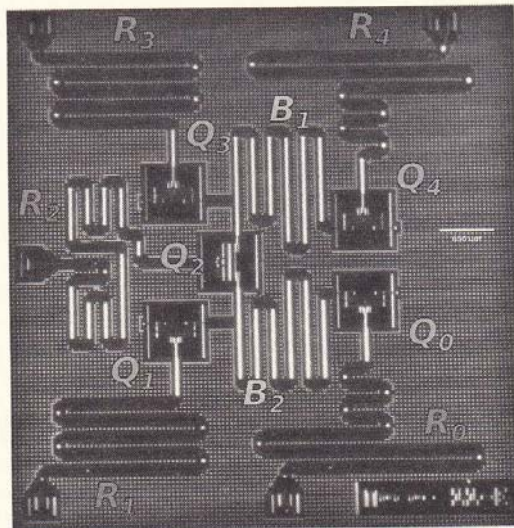


図3 IBMが開発したトランズモン型の超伝導量子ビット回路

出典：<https://github.com/Qiskit/ibmq-device-information/blob/master/>

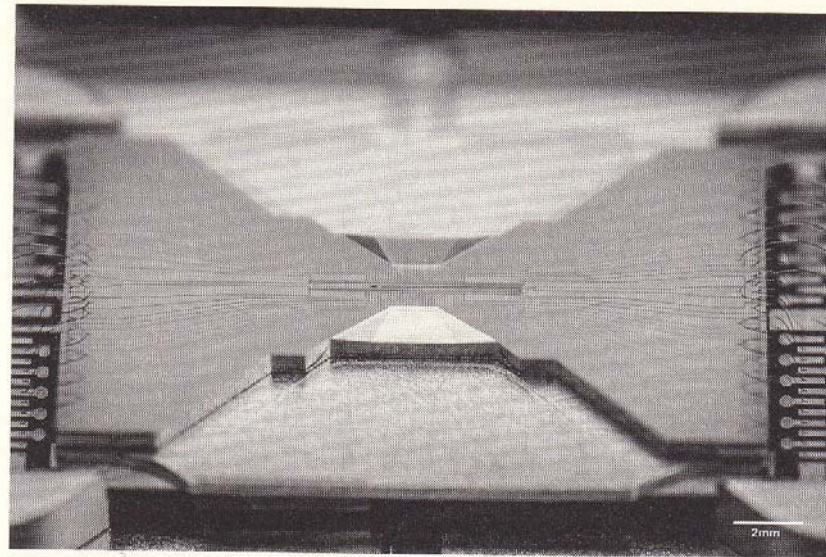


写真1 米IonQ社が開発したイオン・トラップ方式の量子プロセッサ  
写真提供：IonQ

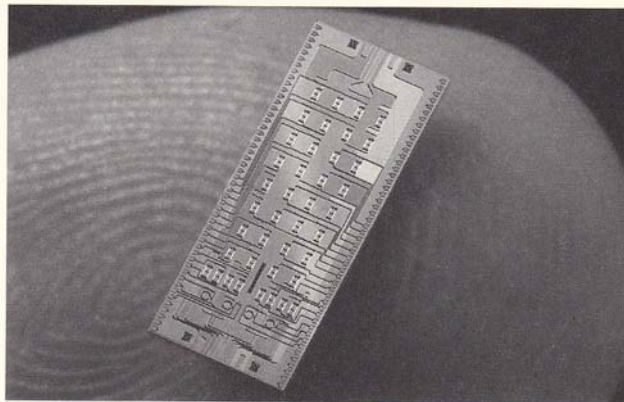


写真4 ザナドゥが開発した光量子プロセッサ

プログラム可能なので量子化学や機械学習など複数の用途に使えるという

出典：<https://spectrum.ieee.org/race-to-hundreds-of-photonic-qubits-xanadu-scalable-photon>

出典：「ゼロからわかる量子コンピュータ」小林雅一著，  
講談社現代新書(2022)



# 量子ビットの代表的な方式の比較

図7 量子コンピュータの代表的な方式の比較

	超伝導回路方式	イオン方式
量子ビットの「0」と「1」の表し方	超伝導状態の電気回路の2通りの状態	イオン1個中での電子の軌道への2通りの入り方
利点	<ul style="list-style-type: none"> <li>◎エラー率1%以下</li> <li>◎集積化可能</li> </ul>	<ul style="list-style-type: none"> <li>◎エラー率1%以下</li> <li>◎量子ビットが安定</li> </ul>
欠点	<ul style="list-style-type: none"> <li>×量子ビットが不安定</li> <li>×冷凍機が必要</li> </ul>	<ul style="list-style-type: none"> <li>×一部の演算が低速</li> <li>×真空容器が必要</li> </ul>

Google や IBM が取り組み  
現在最も主流

超伝導方式と規模は互角  
演算精度はナンバーワン

	半導体方式	光方式
量子ビットの「0」と「1」の表し方	半導体基板中に閉じ込めた電子1個が持つ磁石の2通りの向き	光子1個の2通りの波の振動方向
利点	<ul style="list-style-type: none"> <li>◎高密度に集積化可能</li> </ul>	<ul style="list-style-type: none"> <li>◎室温・大気中で動作</li> <li>◎演算が高速</li> </ul>
欠点	<ul style="list-style-type: none"> <li>×エラー率がまだ高い</li> <li>×冷凍機が必要</li> </ul>	<ul style="list-style-type: none"> <li>×エラー率がまだ高い</li> <li>×一部の演算が確率的</li> </ul>

まだ規模は小さいが  
集積化へ Intel も期待

他にはない利点を持ち  
通信もできる注目株

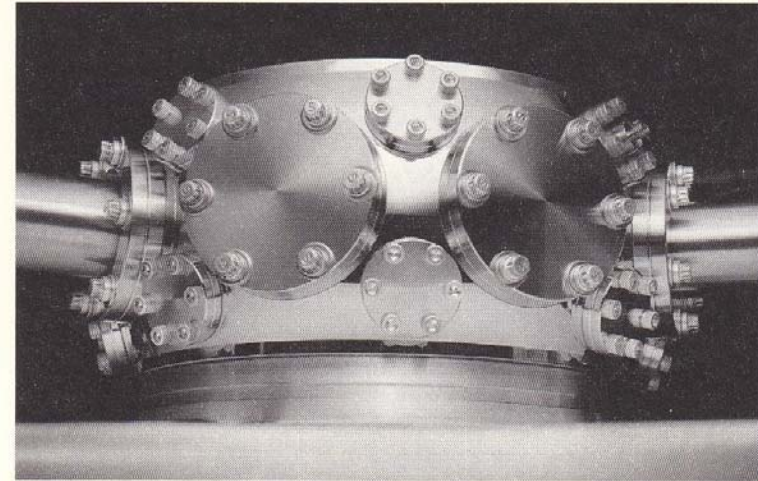


写真1 米ハネウェルのイオン・トラップ方式量子コンピュータ「H1」

出典： <https://www.honeywell.com/real/computing/quantum>

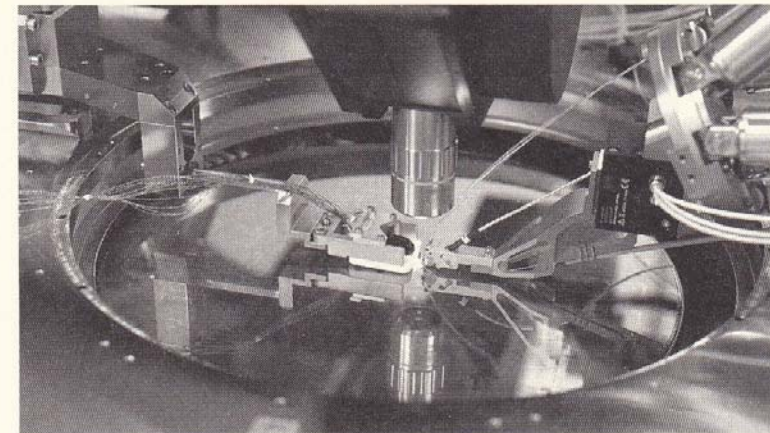


写真2 サイクオンタムが開発中の光量子プロセッサ

出典： <https://psiquantum.com/news/psiquantum-partners-with-globalfoundries-to-bring-up-q1-quantum-system>

出典：「量子コンピュータが本当にわかる！」  
武田俊太郎著，技術評論社(2020)

出典：「ゼロからわかる量子コンピュータ」小林  
雅一著，講談社現代新書(2022)

## 「誤り訂正」技術について

コンピュータの計算過程においてノイズ，誤動作が生じてビットの情報が変化（エラー）するということが起こりうる。

スーパーコンピュータのノード当たりの故障率は， $10^9$ 時間(>10万年)に数十回程度と少ない。それでもエラーが検出されれば訂正するプログラムが組み込まれている。

### 従来型コンピュータのエラー（誤り）訂正機能

誤り訂正符号 0を000，1を111と3つのコピーで表す。

3つのビットのうち1つにエラーが生じた場合，001または010のように変化している。多数決から000と推定でき誤りを訂正できる。

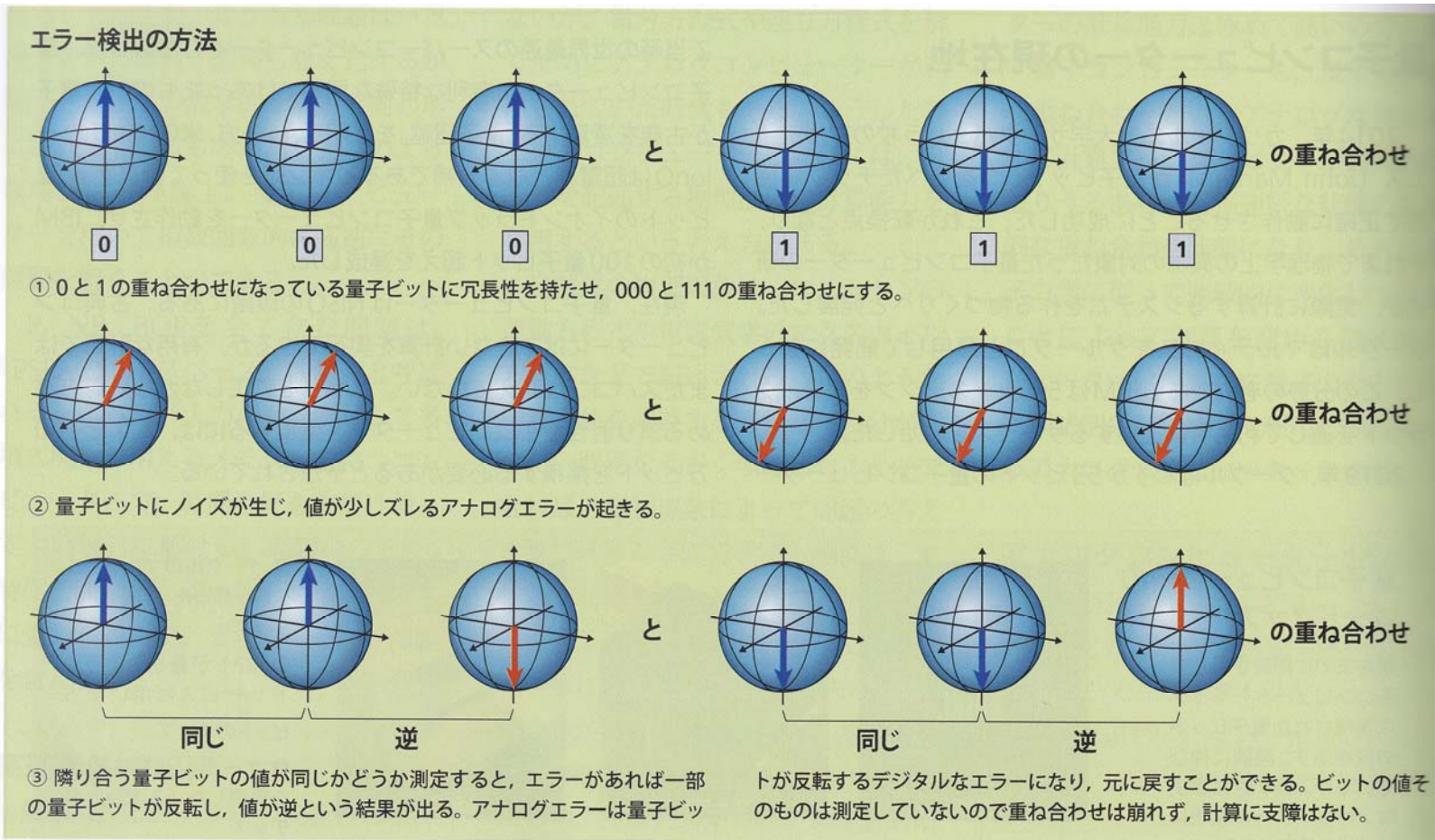
量子コンピュータの量子ビットと量子ゲートはノイズに弱く，1000回に1回程度の確率でエラーを起こす。エラー訂正機能がなければ有用な計算ができない。「量子誤り訂正技術」

エラー訂正機能を有する量子コンピュータ **誤り耐性量子コンピュータ**

# 「量子誤り訂正」技術

量子ビットの場合 値が少しずれるアナログなノイズのエラーが発生

エラー訂正のために量子ビット3つを用いて000と111という状態の重ね合わせを作り論理量子ビットをつくる。「隣り合う量子ビットが同じ値かどうか」を測定してエラー発生の有無を検出できる。（実際の論理量子ビットは9個の量子ビットを必要とする）



出典：「特集 量子コンピューター最大の壁「エラー訂正」」日経サイエンス日本版第52巻8号，日経サイエンス社(2022)

## 6. 量子コンピュータで何ができるのか 量子コンピュータの得意な問題1

計算方法はわかっているけど、それに従って実際に計算しようとするとならぬスパコンを使っても非常に長時間の計算時間がかかり事実上解けないような問題

### 1 巡回セールスマン問題

あるセールスマンが、ある地域のすべての都市を1回ずつ訪問して出発点に戻ってくる。このときの最短距離を求める問題

### 2 ナップザック問題

ナップザックの容量を越えないように品物を詰め込み、それらの品物の価値の合計が最大になるようにする問題

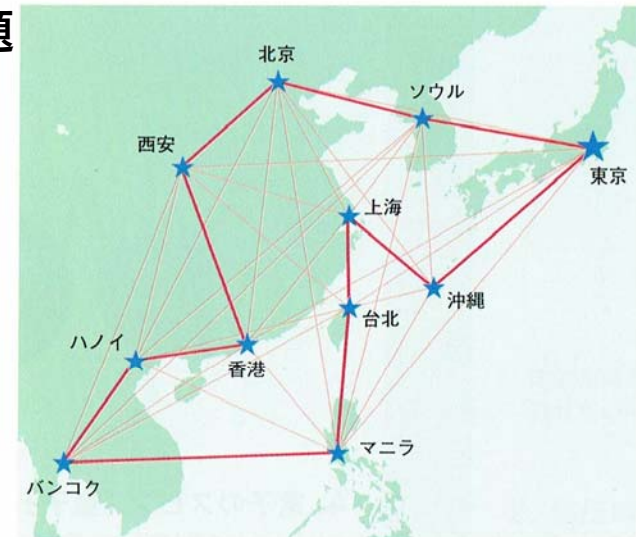
### 3 大規模信号機群を制御する最適化技術

### 4 新たな化学物質を合成するための最適の反応計算

### 5 新たに開発しようとする新薬物質の薬効をシミュレーション

### 6 投資ビジネスの競争優位性を高めるモンテカルロ・シミュレーション

出典：「基礎から学ぶ量子コンピューティング  
イジングマシンのしくみを中心に」工藤和恵著、  
オーム社(2023)



すべての訪問先をめぐる最短ルートは？

東京にいるセールスマンが上の地図で示す10都市（東京を除く）をすべて1回ずつ訪問し、同じルートは通らずに東京にもどってくることを考えます。距離が最も短くてすむルートはどこになるでしょうか。この問題は「巡回セールスマン問題」とよばれます。上の例では、訪問先が10か所ですから、とりうるルートは約363万（ $=10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$ ）通りです。上の地図では、とりうるルートの一部を示しました。

出典：「量子論のすべて 改訂第2版」Newton別冊、  
ニュートンプレス(2021)

# 6. 量子コンピュータで何ができるのか

## 量子コンピュータの得意な問題2

	例 1：グローバーの解法	例 2：ミクロな化学計算の解法		例 3：ショアの解法	例 4：連立一次方程式の解法
問題のイメージ			問題のイメージ	素因数分解 $34579 = \boxed{?} \times \boxed{?}$	$\begin{cases} 3x+2y-z=2 \\ -x+y+2z=6 \\ 2x-4y-3z=-5 \end{cases}$ $(x, y, z) = (?, ?, ?)$
計算高速化のポイント	重ね合わせて並列処理 + 干渉で絞り込み	量子コンピュータは電子が従う量子力学のルールを自然に表現できる	計算高速化のポイント	重ね合わせと干渉を使った量子フーリエ変換で周期を高速に見つける	数の足し引きを波の足し引きに置き換えて計算させる
応用分野の例	データベース検索・組合せ最適化問題	機能性材料や薬の開発	応用分野の例	暗号解読	シミュレーション・制御・機械学習・データ分析・画像処理

出典：「量子コンピュータが本当にわかる！」武田俊太郎著，技術評論社(2020)

# 7. 量子コンピュータの現状と課題

内閣府総合イノベーション戦略推進会議 「量子技術イノベーション戦略（最終報告）」

<https://www8.cao.go.jp/cstp/tougosenryaku/ryoushisenryaku.pdf>

## 量子技術を取り巻く諸外国の動向

- 米欧中を中心に海外では、「量子技術」は経済・社会に大きな変革をもたらす重要な技術と位置づけ、政府主導で研究開発戦略を策定。近年、研究開発投資を大幅に拡充するとともに、研究開発拠点形成や人材育成等を戦略的に展開。
- 各国の大手IT企業も積極的な投資を進めており、ベンチャー企業設立・資金調達も進んでいる。

### ○政府の取組



✓ 2018年9月、国家科学技術会議が「量子情報科学の国家戦略

概要」を策定

- ✓ 2018年12月、2019年より5年間で最大13億ドル(約1,400億円)規模の投資に関する法律が成立(DOD, CIA除く)
- ✓ DOEやNSFを中心に、10か所程度、研究開発や人材育成を行う拠点を形成



✓ 2017年6月、欧州委員会の有識者会議が研究開発戦略を策定

- ✓ 2018年から10年間で、10億ユーロ(約1,250億円)規模のプロジェクトを開始
- ✓ 加えて、各国が独自予算で研究開発を実施
- ✓ 特に、蘭・英等は、国際的な研究拠点を形成。民間投資を呼び込んでいる



✓ 「科学技術イノベーション第13次五カ年計画(2016年)」において、量子通信と量子コンピュータを重大科学技術プロジェクトとして位置づけ、積極的に投資

- ✓ 「量子情報科学国家実験室」を安徽省合肥市に約70億元(約1,200億円)かけて建設中(2020年完成予定)
- ✓ 衛星通信を用いた量子暗号など、暗号・通信分野での取組にも注力

### ○代表的な企業の取組

#### <大手IT企業>

Google

量子人工知能研究所を設立(2013年～)

IBM

5年間で30億ドルの研究投資(2014年～)

Microsoft

Station Qを設立(2005年～)

阿里巴巴 (アリババ)

中国科学院に量子計算実験室を設立(2015年～、3千万元/年)

#### <ベンチャー>

D-WAVE

世界初の商用量子アニーリングマシンを販売。2億ドルを資金調達。

rigetti

超伝導型量子コンピュータを開発。約1.2億ドルを資金調達。

注)為替レートは、発表時の当該月の我が国財務大臣が公示する基準外国為替相場及び裁定外国為替相場をもとに算定

世界的な競争が激化する中、量子技術をどのように推進するか岐路に立たされている

# 企業の量子コンピュータの開発状況

図表 3-1 量子コンピューティング業界のプレイヤー俯瞰

ハードウェア				ソフトウェア			
北米		欧州		北米		欧州	
<b>超伝導</b>		<b>超伝導</b>		QCウェア(米)	リバーレーン(英)	ラーコ(英)	
IBM(米)	グーグル(米)	オックスフォード・クオンタム・サーキット(英)		ザパタAI(米)	フェーズクラフト(英)		
アマゾン(米)	リゲッティ(米)	クオントウェア(蘭)	アリス&ポブ(仏)	リンドボックスAQ(米)	エイチ・キュー・エス(独)		
シーク(米)	ブレキシモ(米)	アイキューエム(芬)		ストレンジワークス(米)	クオントファイ(仏)		
ディーウェーブ(加)		<b>イオントラップ</b>		キュービット・エンジニアリング(米)	キュービット・ファーマシューティカル(仏)		
<b>半導体</b>		ユニバーサル・クオンタム(英)		キューシミュレート(米)	パリティQC(澳)	マルチバース(西)	
インテル(米)		オックスフォード・アイオニック(英)		ワンキュービット(加)	テラ・クオンタム(瑞)		
イークワル・ワン(米)		エレクトロン(独)		プロテイン・キュア(加)			
<b>イオントラップ</b>		アルパイン・クオンタム・テクノロジーズ(澳)		--- アジア・オセアニア ---			
<b>光</b>		<b>光</b>		<b>半導体</b>		<b>半導体</b>	
アイオンキュー(米)		オーカ・コンピューティング(英)	クオンタム・モーション(英)	ブルーキャット(日)	キュナシス(日)		
クオンティニウム(米)		クイックス・クオンタム(蘭)	<b>中性原子</b>	フィックスターズ(日)	ジェイアイジェイ(日)		
<b>光</b>		NQCG(諸)		クオンマティク(日)			
プサイ・クオンタム(米)		パスカル(仏)		クラシック(以)	ケドマ(以)		
クオンタム・コンピューティング(米)		--- アジア・オセアニア ---		Qコントロール(豪)			
ザナドゥ(加)		<b>超伝導</b>		<b>量子クラウドサービス</b>		<b>量子インスパイア</b>	
<b>中性原子</b>		富士通(日)		北米		北米	
キューセラ(米)		日本電気(日)	日立製作所(日)	アマゾン(米)		エヌビディア(米)	
アトム・コンピューティング(米)		アリババ(中)	シリコンQC(豪)	マイクロソフト(米)			
<b>トポロジカル</b>		<b>光</b>		グーグル(米)			
マイクロソフト(米)		バイドゥ(中)	NTT(日)	IBM(米)			
<b>超冷却技術</b>		本源量子(中)		ファーウェイ(中)			
<b>制御機器</b>		チューリングQ(中)		--- アジア・オセアニア ---			
オックスフォード・インストゥルメンツ(英)		<b>ダイヤモンド</b>		富士通(日)		日本電気(日)	
ブルーフォース(芬)		富士通(日)		日立製作所(日)		東芝(日)	
		クオンタム・プリリアンス(豪)		--- 欧州 ---			
		キーサイト・テクノロジー(米)		アトス(仏)			
		キューブロックス(蘭)		キューエル(日)			

出典：「量子コンピュータまるわかり」間瀬英之・身野良寛著，日経文庫，日本経済新聞出版社(2023)

[注] 加：カナダ、蘭：オランダ、芬：フィンランド、  
 諾：ノルウェー、澳：オーストラリア、瑞：スイス、  
 西：スペイン、星：シンガポール、以：イスラエル

## 日本の研究開発の現状

2020年 内閣府総合イノベーション戦略推進会議 「量子技術イノベーション戦略（最終報告）」

<https://www8.cao.go.jp/cstp/tougosenryaku/ryoushisenryaku.pdf>

2021年 日本初のIBM製「ゲート型商用量子コンピュータ」が新川崎・創造のもりかわさき新産業創造センター（KBIC、神奈川県川崎市幸区）で稼働

2023年新たに127量子ビットの「IBM Quantum Eagle」プロセッサを搭載したIBM Quantum System Oneを設置

2022年 内閣府総合イノベーション戦略推進会議 「量子未来社会ビジョン～量子技術により目指すべき未来社会ビジョンとその実現に向けた戦略～」

[https://www8.cao.go.jp/cstp/ryoshigijutsu/ryoshimirai\\_220422.pdf](https://www8.cao.go.jp/cstp/ryoshigijutsu/ryoshimirai_220422.pdf)

2023年 理化学研究所を中心とする研究グループが国産量子コンピュータ初号機「叡」を公開，クラウドサービスを開始

[https://www.riken.jp/pr/news/2023/20231214\\_1/index.html](https://www.riken.jp/pr/news/2023/20231214_1/index.html)

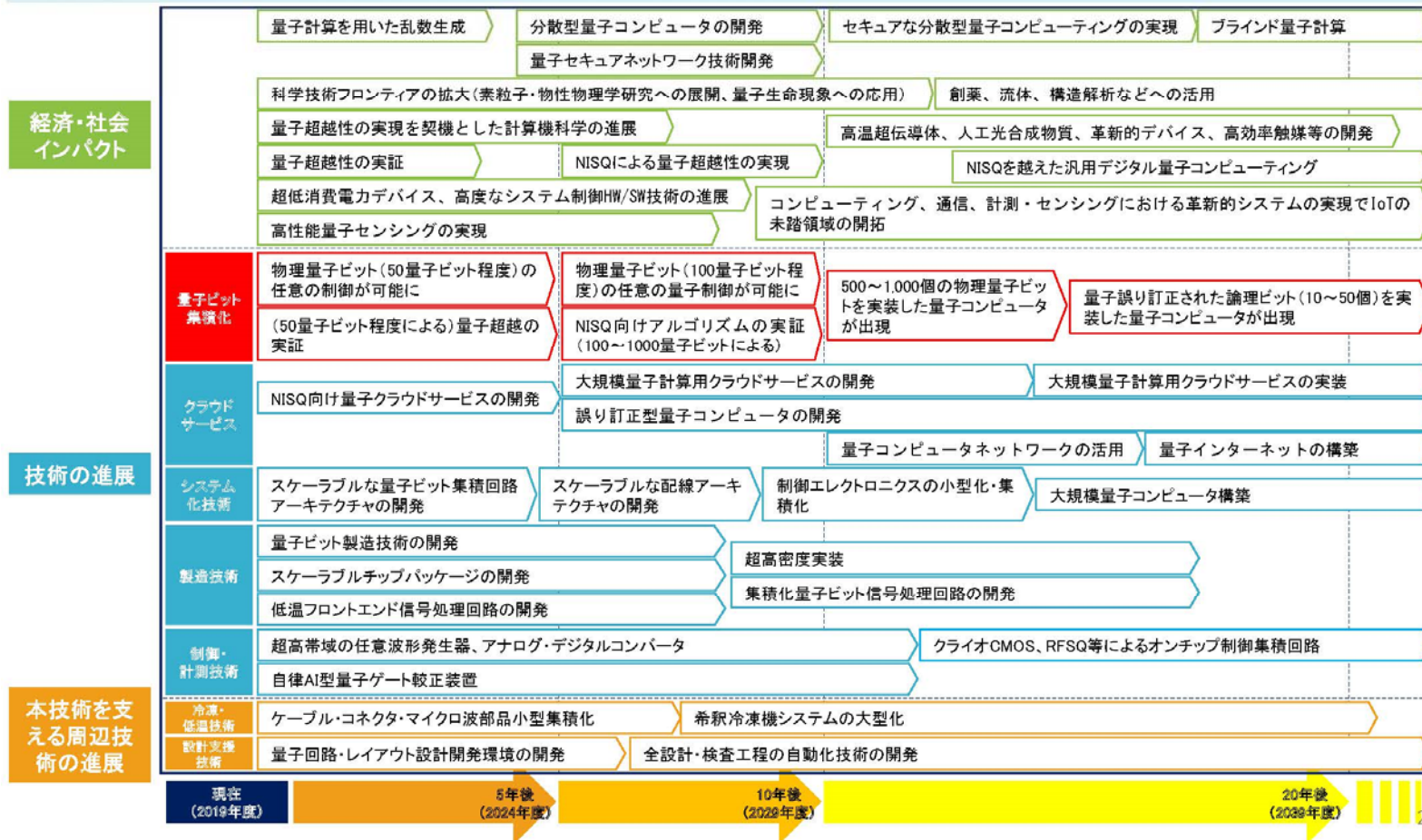


# 内閣府総合イノベーション戦略推進会議 「量子技術イノベーション戦略 (最終報告)」

<https://www8.cao.go.jp/cstp/tougosenryaku/ryoushisenryaku.pdf>

## ①ゲート型量子コンピュータ(超伝導量子ビット)

- 大規模で複雑な計算を高速・高精度・低消費電力で実行可能な汎用デジタル量子コンピュータを実現
- 10年後以降、1,000個程度の物理量子ビットを実装。さらに、量子誤り訂正された50個程度の量子ビットを実装
- 大規模化に向けた設計支援技術や冷凍・低温技術開発により、大規模化を進める



## 主要技術領域① 量子コンピュータ・量子シミュレーション

- ゲート型量子コンピュータ、量子シミュレーションの実現には技術的課題があるものの、**新奇材料や薬剤開発を効率化**することや**セキュリティ技術の向上**などに貢献し、産業・社会のあらゆる分野で飛躍的なイノベーションをもたらす
- 量子アニーリングは、**実問題の解決に向けた動きが企業を含めて活発**。得意とする組合せ最適化問題を解くことで、**交通渋滞の解消、工場生産プロセスの最適化**などを通じ、生産性向上に貢献

### ゲート型量子コンピュータ (超伝導量子ビット)

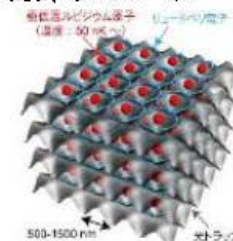
- ✓ 量子力学的な状態を情報処理の単位 (量子ビット) として利用したコンピュータ
- ✓ 日本は超伝導量子ビット製作に世界に先駆けて成功。高品質の超伝導量子ビットの製作・制御に高い技術力を保持
- ✓ 高品質の超伝導量子ビットによる大規模化が課題
- ✓ 大規模超並列計算により、因数分解、検索、量子深層学習などの問題を短時間かつ超低消費電力で計算が可能となる見通し



量子ビットの冷却・制御装置 (東大 中村教授)

### 量子シミュレーション (冷却原子)

- ✓ 量子多体系のふるまいや相互作用に特化した問題について、人工的な多数の粒子の量子状態を制御してシミュレーション実験を行う技術
- ✓ 我が国は、強相関電子系の理論的研究で世界をリード
- ✓ 複数原子間の長距離相互作用等の実装に関する課題がある
- ✓ 量子多体系物理、高温超伝導の理論的解明に期待。光や冷却装置などの周辺技術の産業への波及に期待



超高速量子シミュレータの概念 (分子研 大森教授)

### 量子ソフトウェア

- ✓ 量子コンピュータで計算を行うために必要となるOSやシステムアーキテクチャ、アルゴリズム、アプリケーションの研究開発
- ✓ 大学・研究機関に加え、ベンチャー企業を中心にゲート型・アニーリング型の双方で、開発が激化
- ✓ 機械学習や量子化学計算などの量子計算の高速化・大規模化により、産業・社会のイノベーションに期待



量子コンピュータのハード/ソフトウェアの階層

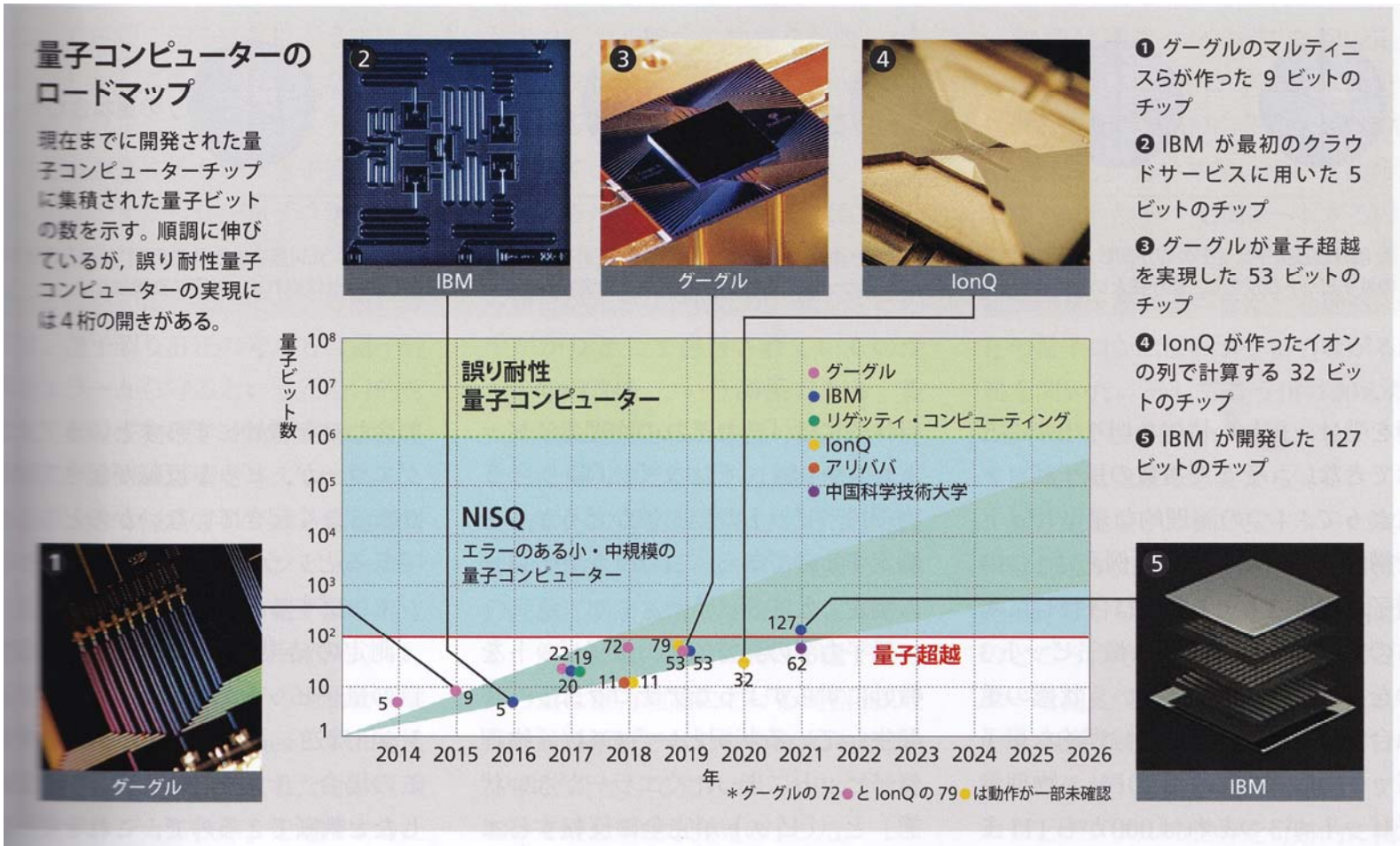
### 量子アニーリング

- ✓ 量子力学的「重ね合わせ」を利用し、最適な組合せを導くことに特化したコンピュータ
- ✓ 東工大西森らが理論提唱した量子アニーリングと超伝導量子ビットの技術を基にカナダのベンチャーが商用機を開発
- ✓ 国内企業により、量子技術にinspireされたハード開発が活発化
- ✓ 交通問題などの実社会問題の解決に向けた取組みが先行



D-Wave社(カナダ)が開発した量子アニーリングマシン (出典: D-Wave社)

# 量子コンピュータ開発のロードマップ



出典：「特集 量子コンピュータ最大の壁「エラー訂正」」日経サイエンス日本版第52巻8号，日経サイエンス社(2022)

現在，量子コンピュータはNISQの段階にある。従来コンピュータにはできない計算を実行できるが，有用な計算ではまだスパコンを越えていない。エラーを訂正しながら計算を進める誤り耐性量子コンピュータを実現するにはおよそ100万量子ビットを集積する必要あり

# 量子コンピュータ（量子情報技術）が軍事転用される可能性

主要各国は量子情報技術の軍事利用に向けた研究開発を進めている。

**中国** 2017年量子暗号通信の成功，国家量子情報科学研究所の建設 広範な量子技術の軍事研究を加速

**米国** 2021年国防総省 量子技術の研究開発費 この分野の研究予算の80%を占める

米軍の中で量子技術に関心を寄せているのが空軍。宇宙を舞台にした次世代の戦争で，転換的な役割が期待

**ロシア** 国営原子力企業「ロスアトム」が量子技術の研究開発  
2019年「量子技術ロードマップ」を策定  
ウクライナ侵攻により停滞

**EU** 2018年「量子フラグシップ計画」

表向きは平和利用を挙げているが，実際には軍事利用を念頭に置いた動き  
核兵器を保有する一部の国々が，今後は量子情報技術のような安全保障にかかわるテクノロジーによって覇権国の地位を確定させる恐れ

出典：「ゼロからわかる量子コンピュータ」小林雅一著，  
講談社現代新書(2023)

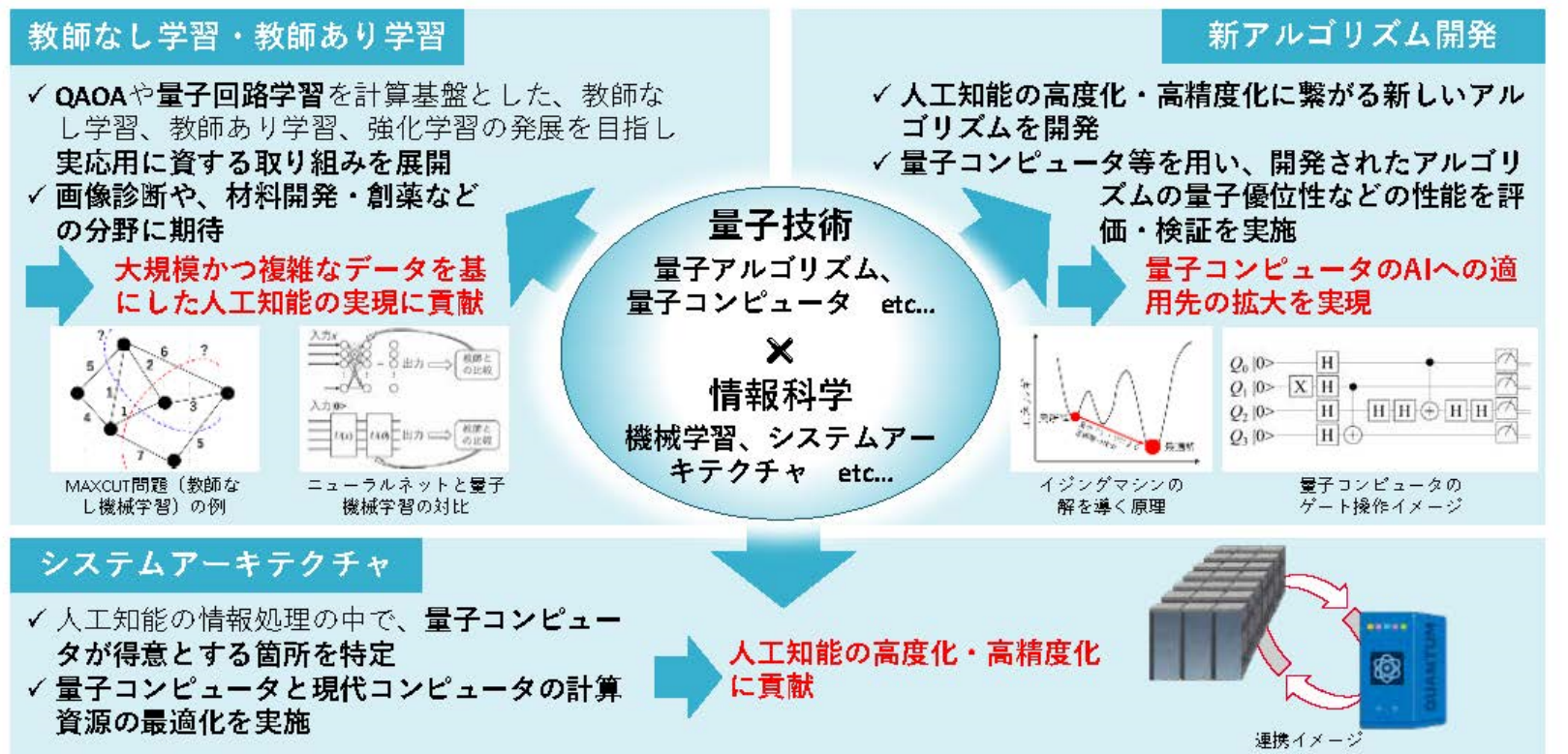
# 量子AI技術 量子コンピュータと人工知能の融合

内閣府総合イノベーション戦略推進会議 「量子技術イノベーション戦略（最終報告）」

<https://www8.cao.go.jp/cstp/tougosenryaku/ryoushisenryaku.pdf>

## 量子融合イノベーション領域① 量子AI技術のイメージ

- 人工知能の高度化は、Society 5.0実現の重要な鍵。AIの実社会への展開が次々となされているが、今後、この発展を支えていくためには、次世代コンピューティング技術の発展も重要な要因となる。
- 量子コンピュータのキラーアプリ候補として、機械学習に注目が集まっている。将来、量子コンピュータの高度化が実現した際、優位性が出る可能性が指摘されている。世界に先駆けて重点的な研究開発を実施し、世界をリードする。



量子AI技術により、経済・社会の発展の鍵であるより高速かつ精度の高い人工知能を実現し、競争力の高い産業の創出や日本の抱える諸課題の解決に貢献！

# 量子コンピュータの課題

## ハードウェアの課題

ノイズなどの影響による誤り発生確率が高い. 1量子ビット演算0.05%発生  
コヒーレンス時間（重ね合わせ状態を保てる時間）が短い  
超伝導方式では1 ミリ秒以下

## ソフトウェアの課題

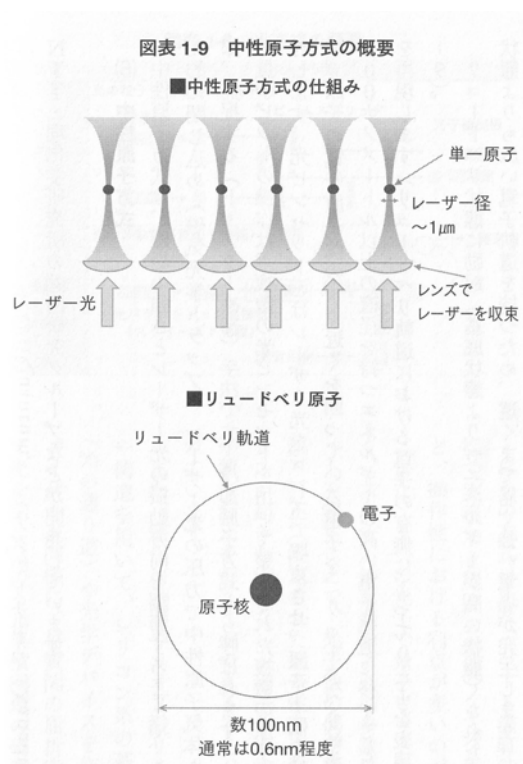
エラーのある小・中規模のNISQの量子コンピュータの有用な用途がない  
（従来コンピュータでも可能な計算の範囲を超えていない）  
ソフトウェア資産を維持するコストが高い

**量子コンピュータの現状** エラーのある小・中規模のNISQ量子コンピュータ  
（2022:IBMオスプレイ433量子ビット, 2023:IBMコンドル1121量子ビット）

真の量子超越を可能にするには「量子誤り訂正」+100万量子ビットの量子コンピュータが必要 2030年～2040年ごろ？

# 量子コンピュータの最新のニュース 2024年2月

**中性原子方式** 280量子ビット+誤り耐性機能を有する量子コンピュータ  
磁場とレーザー光で中性原子Rbを閉じ込め リュウドベリ軌道における  
電子の有無で量子ビット  
利点：大規模化が可能，ノイズが少ない，コヒーレンス時間が数秒と長い



## 量子情報：大規模量子コンピュータの実現へさらに前進

2024年2月1日 Nature 626, 7997

量子誤り訂正を通して複数の物理キュービットに量子情報を符号化することによる情報の保護が、大規模量子コンピュータの実現への道であると考えられている。しかし、誤り訂正量子コンピュータの実証は、実用上のオーバーヘッドのために今のところ小規模なものに限定されている。今回D Bluvsteinたちは、物理キュービット（個々に捕捉された中性原子）を280個用いて、完全に誤り訂正された量子レジスタの動作を報告している。このプラットフォームの区画化されたアーキテクチャーによって、原子の移動、操作、読み出しが可能になるとともに、さまざまな誤り訂正コードが実現され、このコンピュータのアルゴリズム性能の能動的な向上が示されている。

出典：「量子コンピュータまるわかり」間瀬英之・身野良寛著，日経文庫，日本経済新聞出版社(2023)

出典：「Logical quantum processor based on reconfigurable atom arrays」Dolev Bluvstein et.al. Nature Vol.626, p58, 1 February 2024

## 参考文献・資料 (インターネット資料はURLを資料ページに掲載)

「ゼロからわかる量子コンピュータ」小林雅一著，講談社現代新書(2022)

「基礎から学ぶ量子コンピューティング イジングマシンのしくみを中心に」工藤和恵著，オーム社(2023)

「量子コンピューティング 基本アルゴリズムから量子機械学習まで」嶋田義皓著，オーム社(2020)

「量子もつれとは何か」古澤明著，講談社ブルーバックス，講談社(2011)

「コア・テキスト 量子力学」三角樹弘著，サイエンス社(2023)

「驚異の量子コンピュータ 宇宙最強マシンへの挑戦」岩波科学ライブラリー 岩波書店(2019)

「量子コンピュータが本当にわかる！」武田俊太郎著，技術評論社(2020)

「量子技術の基本と仕組み」若狭直道著，秀和システム(2020)

「ラズパイ電子工作&光の実験で理解する量子コンピュータ」藤井啓祐，武田俊太郎著CQ文庫，CQ出版(2022)

「量子コンピュータの数理」大矢雅則著，パリティ物理学コース，丸善(1999)

「量子アニーリングの基礎」西森秀稔，大関真之著，基本法則から読み解く物理学最前線，共立出版(2018)

「特集 量子コンピューター最大の壁「エラー訂正」」日経サイエンス日本版第52巻8号，日経サイエンス社(2022)

「量子コンピュータまるわかり」間瀬英之・身野良寛著，日経文庫，日本経済新聞出版社(2023)

「量子論のすべて 改訂第2版」Newton別冊，ニュートンプレス(2021)

「Quantum supremacy using a programmable superconducting processor」Frank Arute et.al. Nature Vol.574, p505, 24 OCTOBER 2019

「Logical quantum processor based on reconfigurable atom arrays」Dolev Bluvstein et.al. Nature Vol.626, p58,

1 February 2024