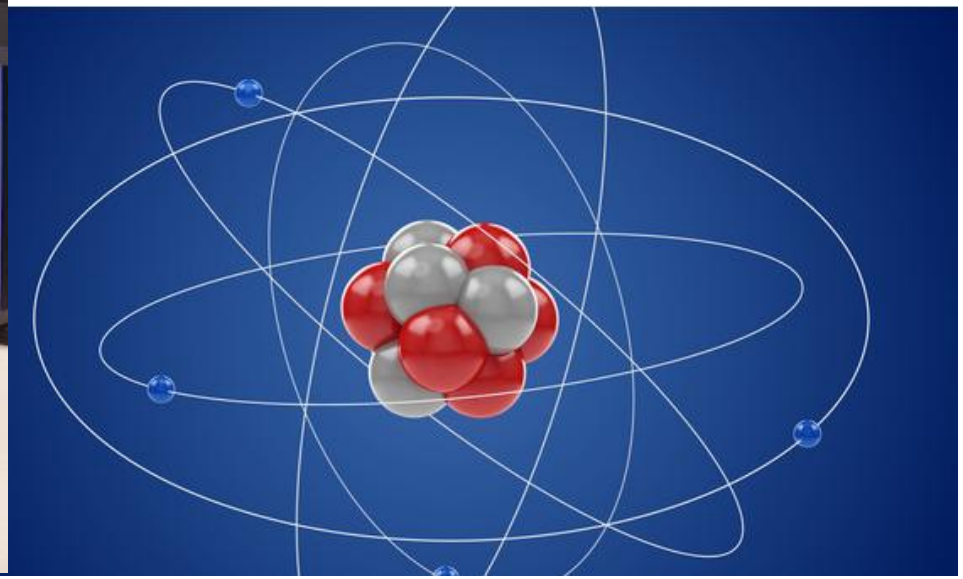
わいわいサロン勉強会
（量子コンピューター）

2018年3月11日



量子力学とは？（1）

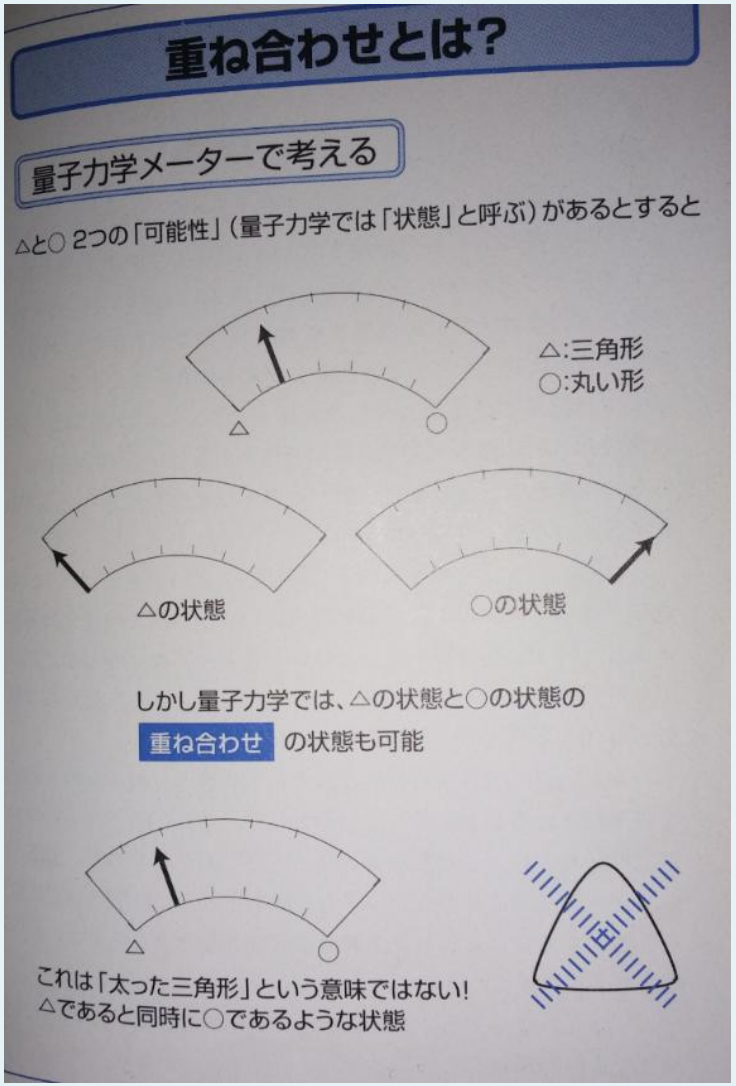
量子状態では物質を波として考えられ、その波というものは**確率的に決まる波**であって、ある特定の状況で、エネルギーの障壁を乗り越えるのではなく、"すり抜ける"状況が起こります。

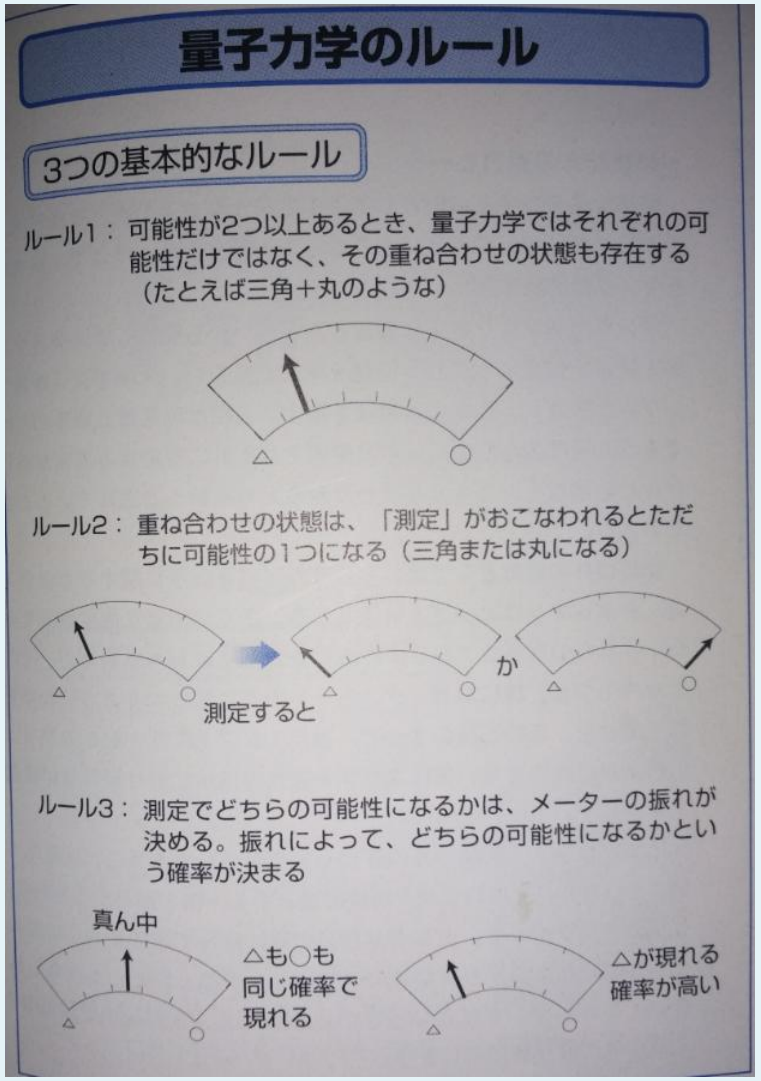
微視世界で、光や電子などが**「粒子」としての顔と「波」としての顔を併せもつ**ことを理論づけた物理学。1920年代半ばに築かれ、1つの物理状態を明快に予測できる古典力学とは異なる世界像をもたらした。粒子の状態は重ね合わさり、その様子が波として表される。**ところが、粒子を観測すると重なりが消え、1つの状態が見える。**核心に、粒子の位置と運動量、時刻とエネルギーなど対になる数値の両方をいっぺんに正確に知りえないとするW.ハイゼンベルクの**不確定性原理**がある。A.アインシュタインの相対論と並んで20世紀物理学を代表する理論。N.ボーア、ハイゼンベルク、E.シュレーディンガー、P.ディラックら物理学者群像の総力で確立した。

電子や陽子，中性子などの素粒子，さらにそれらより小さい基本粒子のレベルで諸現象を統制する理論体系。このレベルの世界では**粒子と波動の二重性**が顕著であり，たとえば水素原子において原子核である陽子のまわりを回る電子は，エネルギーの確定した運動をするとき，一定の軌道を刻々に速度を変えながらたどっていくのではない。こうした粒子としての描像に代えてこの場合の電子は原子核のまわりに広がって振動する波動として表現される。

素粒子・原子・分子などの微視的な系を記述する力学体系。シュレーディンガー方程式にしたがう状態を導入、観測によって得られる測定値との間に確率的な解釈を行うことで、粒子がもつ波動と粒子の二重性、測定における不確定関係などを矛盾なく説明する。量子力学は粒子および粒子集団を扱う現代物理学の基礎理論として、一方では原子核論・物性論へ、また一方で素粒子論・場の理論へと進展した。

量子力学とは？（2）


重ね合わせとは？
量子力学メーターで考える
△と○ 2つの「可能性」（量子力学では「状態」と呼ぶ）があるとすると
△:三角形
○:丸い形
△の状態
○の状態
しかし量子力学では、△の状態と○の状態の
重ね合わせ の状態も可能
これは「太った三角形」という意味ではない!
△であると同時に○であるような状態


量子力学のルール
3つの基本的なルール
ルール1： 可能性が2つ以上あるとき、量子力学ではそれぞれの可能性だけではなく、その重ね合わせの状態も存在する（たとえば三角＋丸のような）
ルール2： 重ね合わせの状態は、「測定」がおこなわれるとただちに可能性の1つになる（三角または丸になる）
か
測定すると
ルール3： 測定でどちらの可能性になるかは、メーターの振れが決める。振れによって、どちらの可能性になるかという確率が決まる
真ん中
△も○も同じ確率で現れる
△が現れる確率が高い

量子コンピューターとは？（1）

量子コンピュータ（りょうしコンピュータ、英語：quantum computer）は、量子力学的な重ね合わせを用いて並列性を実現するとされるコンピュータ。従来のコンピュータの論理ゲートに代えて、「量子ゲート」を用いて量子計算を行う原理のものについて研究がさかんであるが、他の方式についても研究・開発は行われている。
いわゆる電子式など従来の一般的なコンピュータ（以下「古典コンピュータ」）の**素子**は、情報について、「0か1」などなんらかの2値をあらわすいずれかの状態しか持ち得ない**「ビット」**で扱う。量子コンピュータは**「量子ビット」**(qubit; quantum bit、キュービット) により、重ね合わせ状態によって情報を扱う。
n量子ビットがあれば、2 n {¥displaystyle 2^{n}} の状態を同時に計算できる。もし、数千qubitのハードウェアが実現した場合、この量子ビットを複数利用して、量子コンピュータは古典コンピュータでは実現し得ない規模の並列コンピューティングが実現する。

量子コンピューターとは、
現在存在しているスーパーコンピューターをはるかに上回る性能を誇り、現在の社会生活を一新させることが予想されています。
現在のコンピューターは1ビットを基本単位として0と1の信号を切り替えることで計算して表示します。何気なく使っている我々のコンピューターは何らかの画面を表示する際にもこのような処理を高速で行うことで処理して一瞬で表示するようになっています。
スマートフォンなどの挙動も現在発売されている商品の多くは多くの情報量を一瞬で処理して表示していますが、この切り替えを高速で行っているに過ぎません。ところが量子コンピューターは、例えばこれまでのコンピューターの00、01、10、11の4つを切り替えずに計算することが出来るのです。
現在存在しているスーパーコンピューターをはるかに上回る性能を誇り、現在の社会生活を一新させることが予想されています。

量子コンピューターとは？（2）

量子コンピュータを一言で定義してしまうとすれば、それは「通常のコンピュータが演算に利用している「ビット」を、量子力学的な「重ね合わせ」の状態を持つ「量子ビット」で置き換えたもの」ということになる。

例えば、8ビット（CPU）のパソコンの場合、一度に表現できる状態は、やっぱり1つだけ（例えば「00110010」とか）なのに、8量子ビットの量子コンピュータは、「00000000」から「11111111」までのすべての状態を、同じ確率で同時に表現可能なのだ。

では、それが何の役に立つのか？

例えば、8ビットの組み合わせの中から、特定の条件に合うものを計算することを考えてみよう。

通常のコンピュータの場合、「00000000」から「11111111」まで、一度に1つずつ、総当たりで条件と照らし合わせて、解を見つけていく。

ところが、量子コンピュータの場合、「00000000」から「11111111」までのすべての状態の中から、条件に合う解を一度に見つけ出すことができるというのである。すべての状態を一度に表現しているのだから、一度計算すれば、総当たりしたことになるということだ。

つまり、量子コンピュータが実現すれば、大量の数を扱うような計算問題を、今までのコンピュータとは比べものにならない高速度で解くことができるというのである。

例えば、入力で4ビットが扱えるシステムで考えてみよう。

既存方式のコンピュータでは、4ビットを使って1つの値を表す。4ビットでは16通りのデータを表現できるが、入力できるのは1回に1つだけだ。ところが量子ビット4ビットでは1つのビットが「1」も「0」も表現できるので、1回の入力で2の4乗＝16通りのデータを入力できることになる。

その上、複数の量子ビットが「量子絡み合い」状態になると、絡み合った複数の量子ビットは1つのまとまりとして扱えるようになる。

量子力学における絡み合いの関係とは、空間的に離れていてもお互いに影響を与えることができ、かつ、それぞれが独立することがない状態のことだ。量子絡み合いができないと、それぞれの量子ビットは単独でしかデータを扱えないから、例え量子ビットが4つ存在しても、それは「4個のマス」にしか過ぎなかった。これに対し、量子絡み合い関係にあるそれぞれの量子ビットは、既存のコンピュータのように、複数のビットをひとまとめにして扱うことが可能だ。

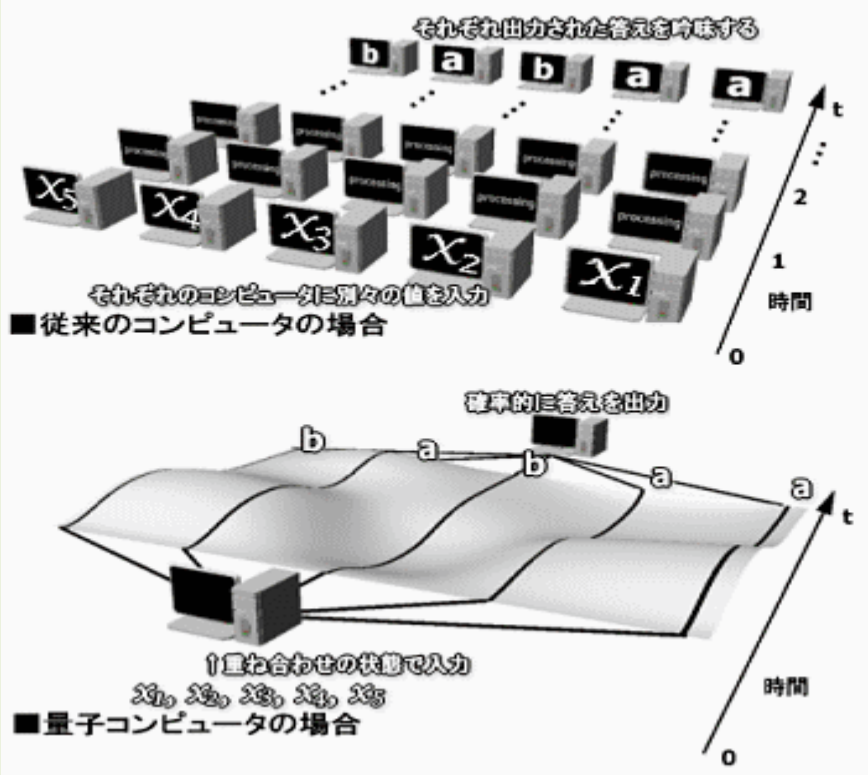
つまり、「量子重ねあい」と「量子絡み合い」によって実現される量子コンピュータでは、1つの入力用ビットの組み合わせで1つの値しか扱えなかった既存のコンピュータと異なり、1つの入力用ビットの組み合わせでなんと「2のN乗」（Nは入力用の量子ビットの数）通りの値を扱えるのである。

量子コンピューターとは？（3）

1ステップで従来の数百ステップの処理が可能になる

既存のコンピュータで1つの式に入力する値を変化させて計算させる場合、変化させるパターンの分だけその都度入力して計算させなければならない。ところが、1つのビットで複数の状態を表現できる量子コンピュータでは、1つの入力命令で複数の計算を一気に行える。

具体的には、量子ビットをN個使うと、1回の入力は既存PCで2のN乗回の入力に匹敵する。入力や計算に要するステップが少ない回数ですむため、既存のコンピュータと比べて、処理速度が格段に向上する。以上が現在考えられている量子コンピュータの特長である。



量子コンピューターは何故登場した？（1）

キー：因数分解

古典的コンピュータ
桁の大きい整数の因数分解というのは現行の古典的コンピュータの苦手としているものです。「計算できる」ことは示されています。ですが、非常に時間がかかります。一説によると宇宙ができてから現在までの時間よりもたくさんかかるとか・・・。
ですので「計算できる」けれど、「実用的でない」ということができます。

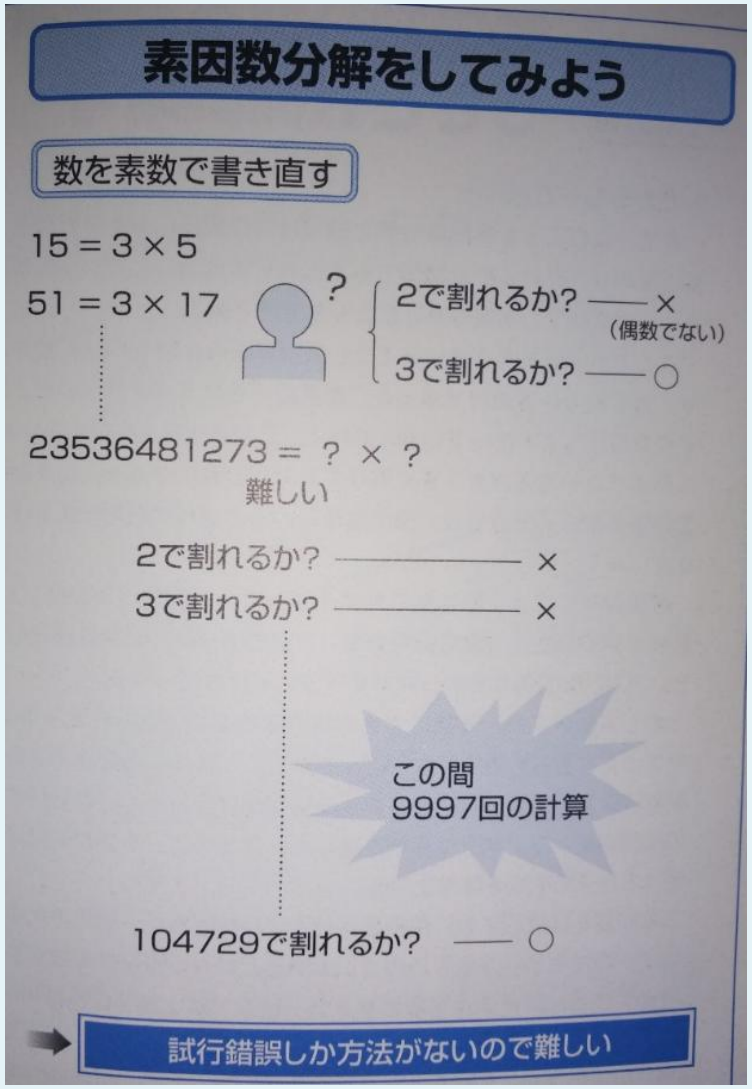
量子コンピュータ
因数分解の計算を「実用的」な時間で解くことができます。

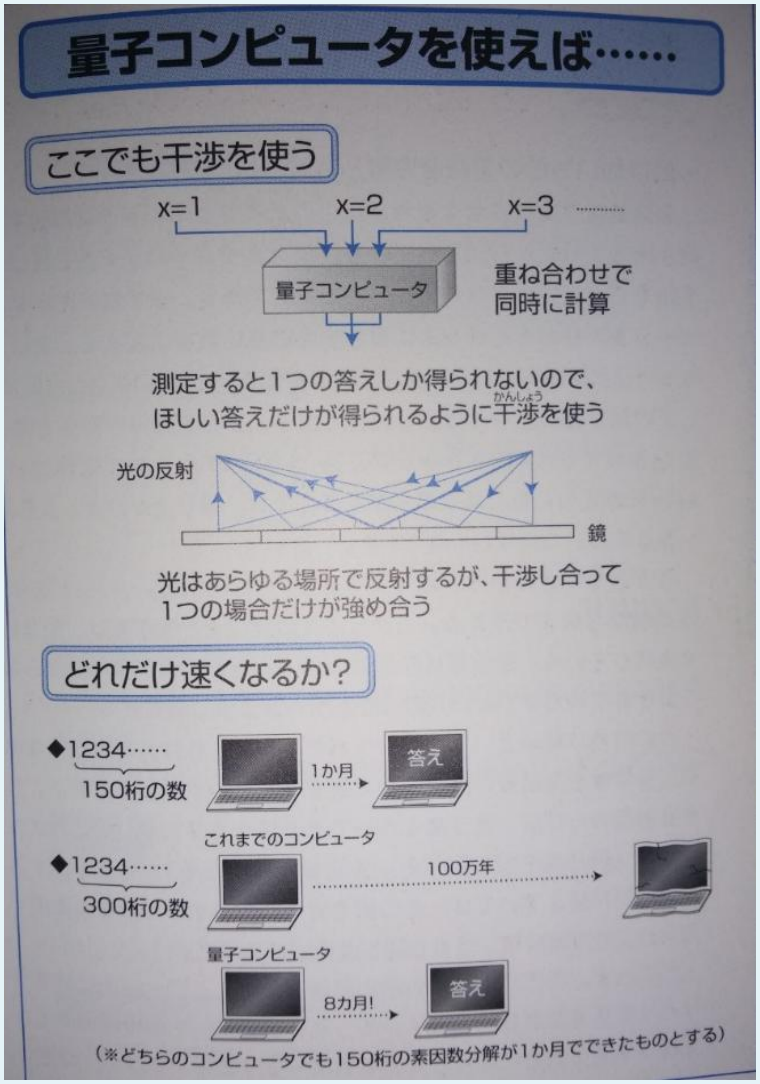
「因数分解が早く行える」ということは現在のコンピュータ**セキュリティ**を崩壊させることを意味しています。現在使われている暗号系は鍵を知らなくても決して解読ができないものではありません。計算はできます。
ですが、非常に時間がかかります。そうです、**現在の暗号系は因数分解計算に非常に時間がかかることを利用しているのです。**ですから現在の暗号系も解こうと思えば解けますが実用的な時間では解くことはできませんが。
一方、量子コンピュータができてしまうと、現行の暗号系は簡単に解読されることが予想されますので、それに替わる新しい暗号系が必要になってきます。
このあたりは**「量子暗号」**という研究分野になっています。

1994年、**AT&T**ベル研究所のPeter Shor(ピーター・ショア)氏が量子コンピュータを用いて整数の素因数分解を高速に行う**アルゴリズム**(Shorのアルゴリズム)を発表した。
2001年には**IBM社**のアルマデン研究所が、このアルゴリズムを利用して量子コンピュータで素因数分解を行うことに成功している。

量子暗号化
中国の例

量子コンピューターは何故登場した？（2）

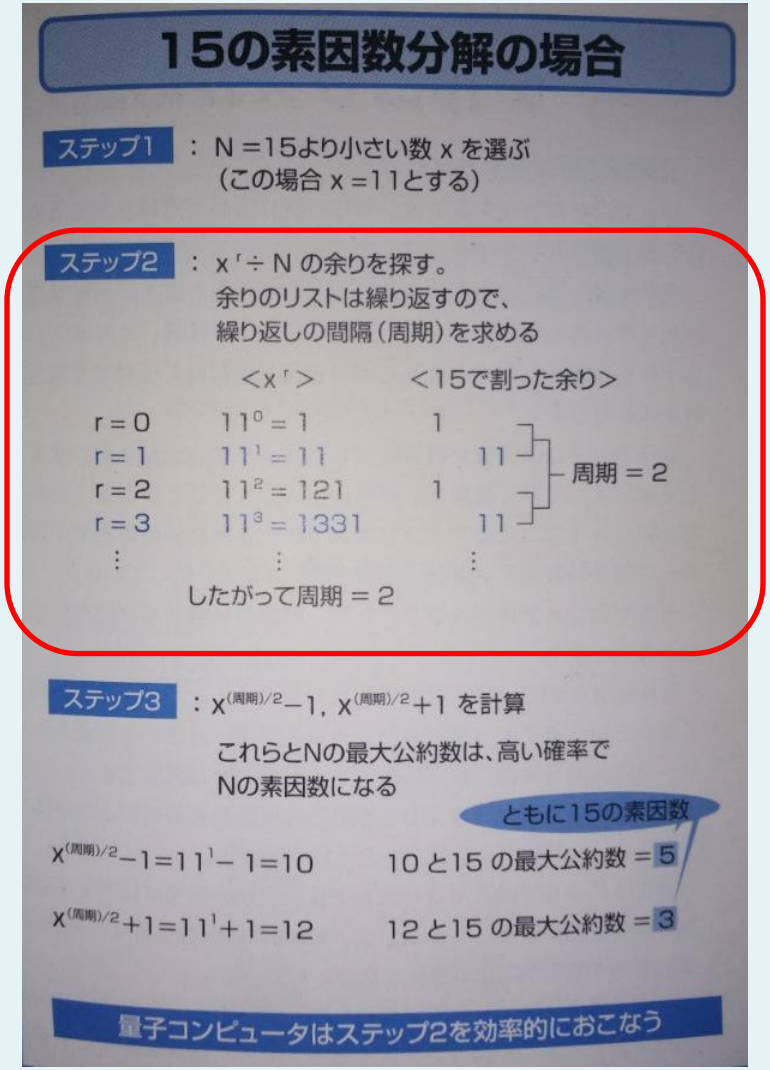




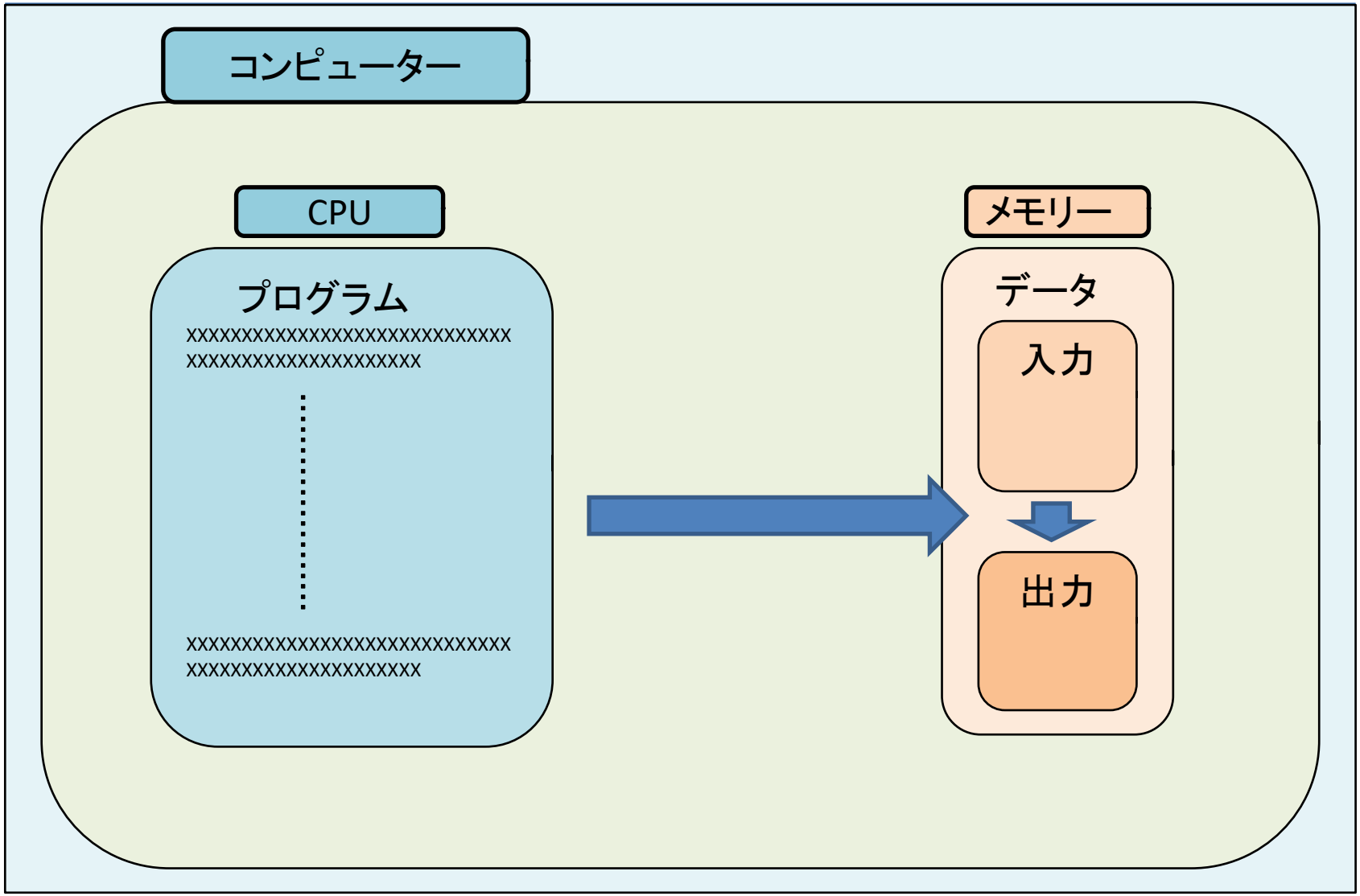
量子コンピューターは何故登場した？（3）

素因数分解
⇩
ショアのアルゴリズム

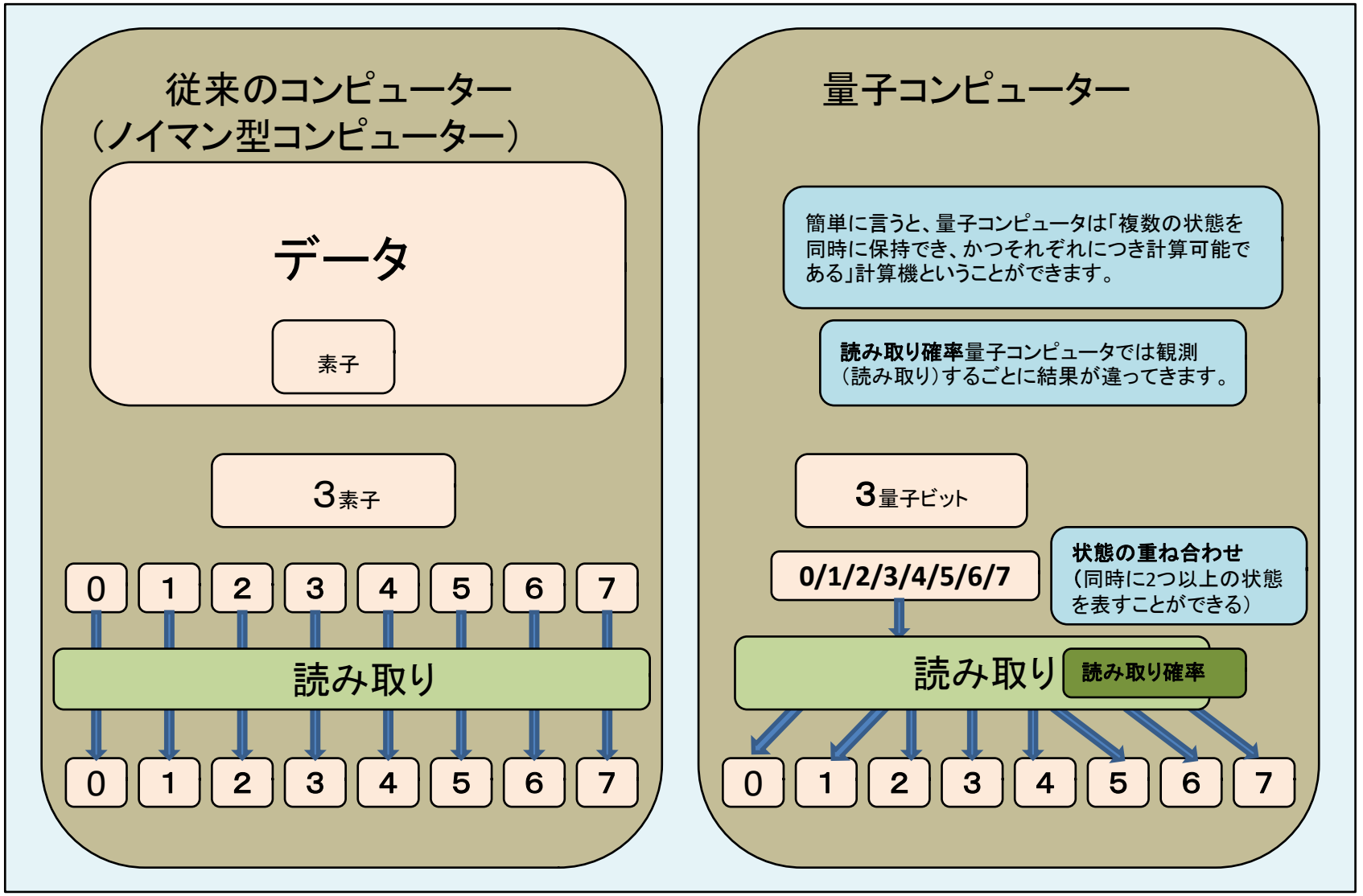
従来のコンピュータでは計算困難（時間がかかり過ぎる）
⇩
量子コンピューターが得意



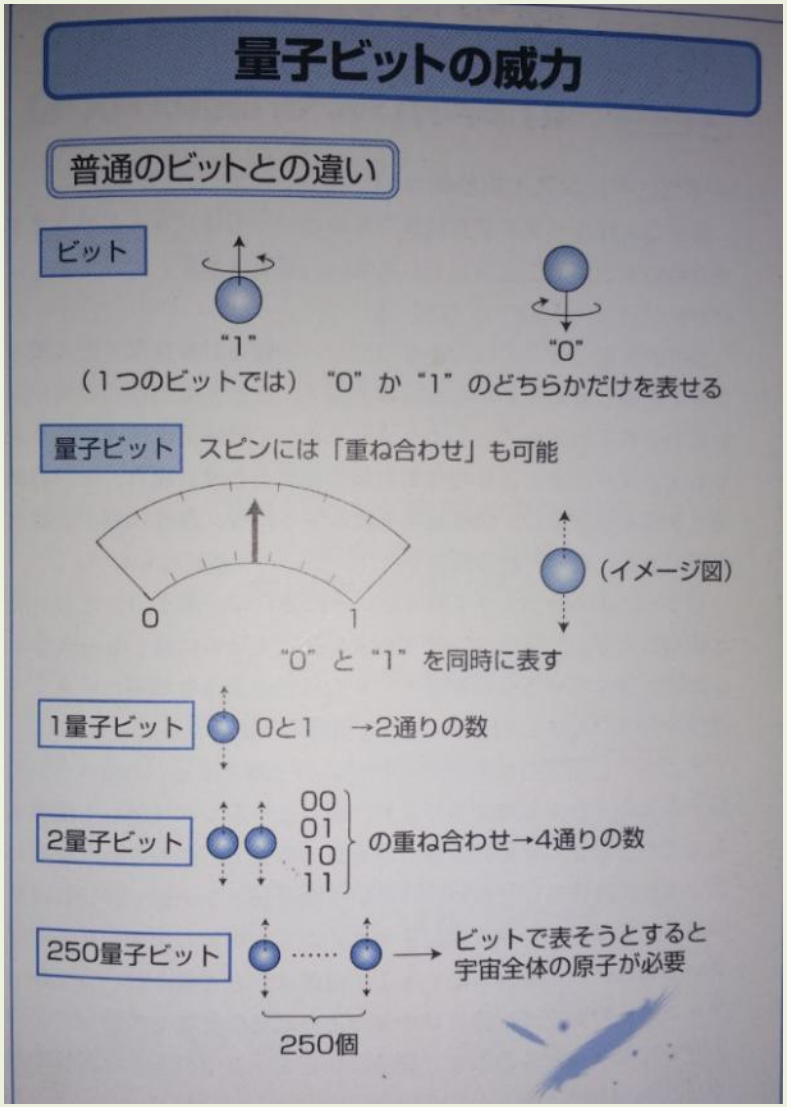
コンピューターの仕組み（1）



従来コンピューターと量子コンピューターの違い



量子ビット


量子ビットの威力
普通のビットとの違い
ビット
"1"
"0"
（1つのビットでは）"0"か"1"のどちらかだけを表せる
量子ビット
スピンには「重ね合わせ」も可能
0
1
（イメージ図）
"0"と"1"を同時に表す
1量子ビット
0と1
→2通りの数
2量子ビット
00
01
10
11
の重ね合わせ→4通りの数
250量子ビット
ビットで表そうとすると
宇宙全体の原子が必要
250個

量子コンピューターの方式（1）

量子アナログ式

（大まかなイメージ図）

デジタル式があるならアナログ式もあるだろうということで「**量子アナログ式**」も存在します。現在実用化されているもの、実用化間近なものの殆どがこちらの方式で、より正確に言えば「**量子イジングマシン方式**」と呼ばれます。
量子イジングマシンでは、「イジング模型」と呼ばれる格子状のモデルをコンピューターの中に物理的に作り、物質の量子力学的な性質を利用して問題と同じ状況を擬似的に再現し、シミュレーションを行なう形で問いに答えます。
D-WAVEの量子コンピューターもこちらの方式を使っています。D-WAVEの場合は、量子イジングマシン方式の中でも「アニーリング方式」という方式を使っており、極低温環境で生まれる量子現象を利用して演算を行えるのが特徴です。
一方、日本で開発中のものは「レーザーネットワーク方式」と呼ばれており、こちらはレーザー照射によって量子現象を発生させます。こちらは常温で使えるのが強みです。
現代のコンピューターはデジタル式ですが、アナログ型のコンピューターもかつては存在しており、究極的に言えば「計算尺」もアナログコンピューターと言えます。

量子コンピューターの方式（2）

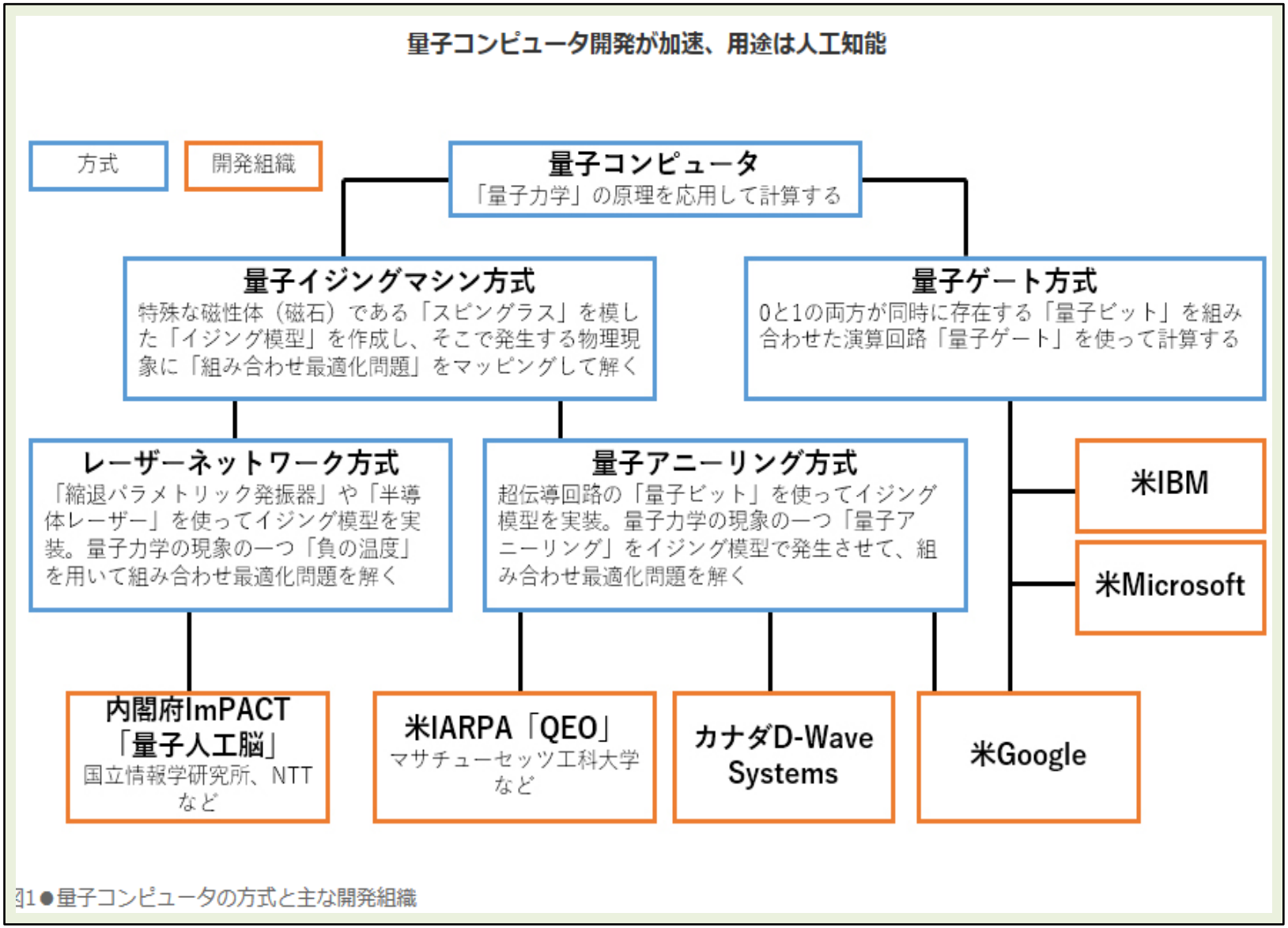


図1●量子コンピュータの方式と主な開発組織

量子コンピューターの方式（２－１）

量子デジタル式

まず、「暗号解読に使ったらヤバイ」と言われている量子コンピューターは「**量子ゲート方式**」と呼ばれる原理的には今までのコンピューターに近い方式です。後述するイジングマシン方式の原理と比較して「**量子デジタル式**」とも呼ばれることもあります。さらにそれを発展させると、現代のコンピューターとほぼ同等の汎用性を有する「**チューリングマシン型**」になります。

「あれ？　量子コンピューターって今のコンピューターに比べて汎用性がないの？」という疑問が生まれますが、結論から言えばその通りです。目標は現代のコンピューターのように「これがあればなんでもできる」コンピューターなのですが、その前段階として「限定的な目的に使えるコンピューター」が完成するということです。

今まで「量子コンピューター」と呼ばれていたものの殆どがこちらの量子デジタル式のことであり、複数の状態を併せ持つ「量子ビット」もこちらの量子コンピューターで利用されます。**電子的な信号を大量に組み合わせる**形で情報処理を行うため、今までのコンピューターと原理が似ています。

ちなみに、こちらの量子コンピューターは実用レベルには達していません。

2つの方式を考える上で、注目したいのは2つのマシン「チューリングマシン」と「イジングマシン」です。チューリングマシンはいわゆる「万能チューリングマシン」のことで、一連の命令文に従って情報処理を行なうだけであらゆる問題を解決できる機械となります。

人間が長々と書かれたマニュアルや指令書を読んで意味内容を理解し、問題を解決できるように、チューリングマシン型のコンピューターは「0と1」もしくは、それに準ずる「量子ビット」などの信号だけで、理論上何でも問題が解決できます。現代のコンピューターはこの「万能チューリングマシン」にあたる存在で、**リソースが無制限にあって天才的なプログラマが大勢いた場合、人間を超える人工知能も作れてしまいます**。一方で、「イジングマシン」は模型を演算に流用したシミュレーション機械のことです。チューリングマシンのように何でも解決できるというわけではありませんし、何ギガバイトもあるような複雑で長ったらしい信号を読み取って情報処理を行なうわけでもありません。

解決したい問題や計算したい問題は「組合せ最適化問題の解説が分かりやすいです）」と呼ばれる特定の問題に限られており、あらゆる問題を解決できるわけではありません。

その代わり、特定の問題を解決する能力は極めて高く、チューリングマシン型のコンピューターでは敵いません。特に**組合せ最適化問題はデジタル式のコンピューターが苦手としている問題の1つ**で、この問題に限って使うのではあればメリットはあります。

また、格子状の模型をニューラルネットワークに置き換えることでニューラルネットワークのシミュレーションが行える可能性を秘めており、場合によっては量子コンピューターによるディープラーニングが実現する可能性もあるのです。イジングマシンも侮れません。

量子コンピューターの方式（3）

量子コンピュータとして話題に上がっているマシンは大きく分けて2方式あり、**量子ゲートモデル**と**量子アニーリングモデル**(Annealing：”焼きなまし”）と呼ばれるものである。量子アニーリングモデルは現在では専用機として認識され始めている。

量子アニーリングモデル
東京工業大学理学部長）西森秀稔教授が考案
アニーリング (Annealing)とは”焼きなまし”のことです。昔からある金属加工の手法で、金属に熱を加え原子を振動させ配列を均質化させることで、内部構造からヒズミ・ストレスを取り除き、内部構造を均質にする処理のことです。
自然現象はエネルギー準位が低い状態を指向するのですが、統計力学的に見た場合、均一度が高いほど、エネルギーレベルが低い状態となります。

この自然現象をコンピュータ上でシミュレーションすることが組合せ最適化問題の近似解法として有効であることが、1983年にKirkpatrick氏らによって発見されました。この手法はシミュレーテッド・アニーリング法（SA法）と名づけられ、今も多くの場面で使われています。
問題は、このSA法ですと、膨大な量の反復計算が必要になります。計算時間が必要です。

そこで出てきたのが量子アニーリング法です。
量子力学ではすべての状態 (組合せ) が”確率”という形で同時に存在できます。いわゆる「量子力学的な重ね合わせ」です。この確率波を適切に処理することで、一つの状態 (組合せ) だけが残ります。この残った値が最適解となるのです。

「この計算時間が、**D-Wave Systems社の量子コンピュータ**を使うことで1億分の1になった」というのが、NASAの発表でした。

量子アニーリング方式の量子コンピュータが注目されているのは、人工知能の開発に欠かせない「機械学習」や「ディープラーニング」の計算処理の実態である「組み合わせ最適化問題」を高速に解ける可能性があるからだ。
実は、パターン認識・自然言語処理を含む機械学習は、最適化問題として定式化されています。
汎用性は低いとはいえ、現行コンピュータとは桁違いの速さで実現できる量子アニーリングを機械学習に応用すれば、パターン認識・自然言語処理等の分野において人工知能の高速化が進むでしょう。

量子コンピューターの方式（4）

量子アニーリングモデル

量子コンピューターの方式（5）

量子ゲートモデル

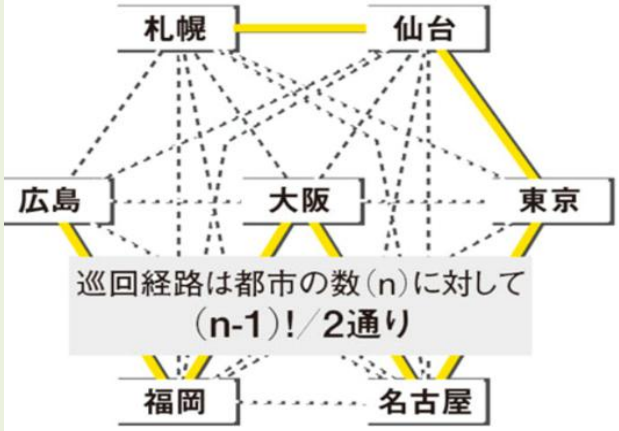
未完

アニーリングモデルセールスマン問題

量子アニーリングモデルセールスマン問題について

巡回セールスマン問題を考えるにあたって、あるセールスマンが、複数の都市を巡回するときに最も距離が最小になる経路を考えます。
例えば3つの都市（例えば東京と名古屋と大阪）は
東京→大阪→名古屋→東京と東京→名古屋→大阪→東京ですが、
逆向きに巡るのは同じものとみなすらしいので、3つの都市の場合は1です。

セールスマンが複数都市を全て巡回する場合に、最も距離が短くなる経路はどれ?



スーパーコンピュータ「京」（1秒間に1京回計算可能）を使って総当たり方式で最短経路を探すと?

都市数	巡回経路数	計算時間
8	2520	2.52×10^{-13}秒
15	435億	4.35×10^{-6}秒
20	6京800兆	6秒
25	3.10×10^{23}	359日
30	4.42×10^{30}	1401万年
⋮		

計算が終わらない

スーパーコンピュータでは厳密解を得られないので、現在は「近似解」を計算している

量子コンピューターの方式（3）

巡回サラリーマン問題
https://qiita.com/onhrs/items/aa0aa181c27743956689

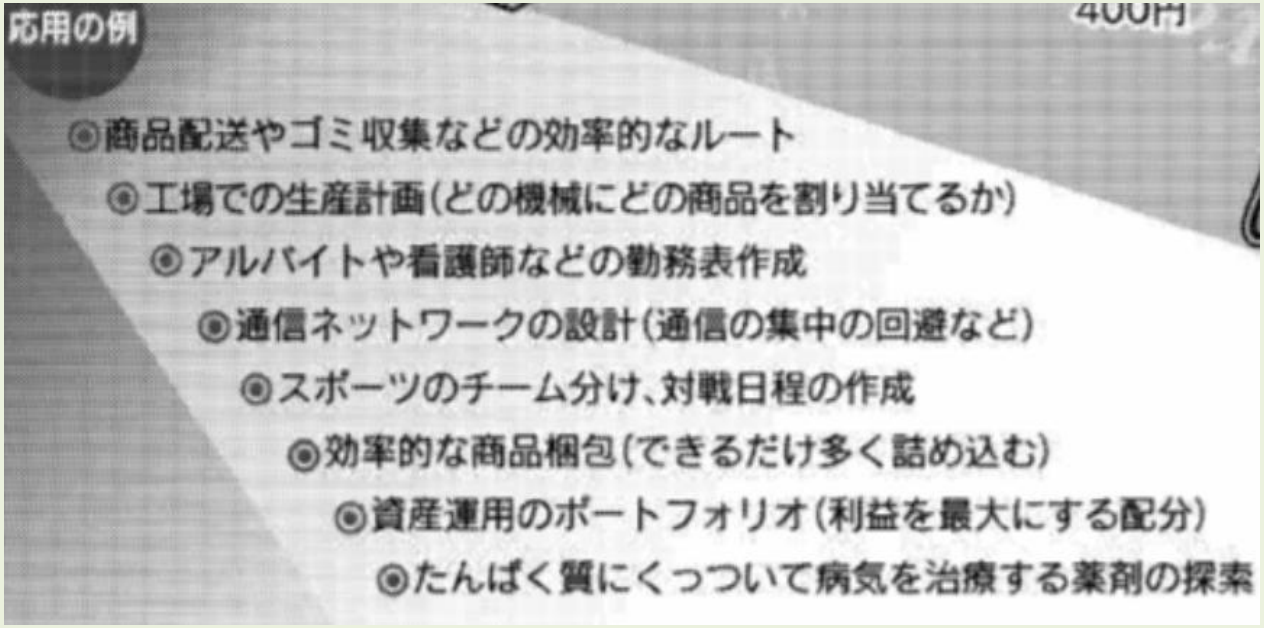
量子コンピューターの衝撃と期待

衝撃

・ネットワーク依存社会のセキュリティ基盤の崩壊（暗号システムの破壊）
・ビットコインで使用されているブロックチェーンの破壊
など

期待

・人工知能の加速（高速化）
AIである「機械学習」や「ディープラーニング」の計算処理の実態である「組み合わせ最適化問題」を高速で解く。
パターン認識・自然言語処理、投資のポートフォーリオの最適化問題、画像認証、医療、法律、考古学等の分野において人工知能の高速化が進む。



ロッキード社がD-Webの量子コンピューターを購入した経緯

ロッキード・マーチン社の大きな問題は開発コストの増大である。そのなかでもF35などの戦闘機用に開発しているソフトウエアーの正当性の検証に費用がかかる。どんなプログラムにもバグがつきものである。正当性の検証に開発コストの半分が費やされると言う。その問題に主任科学者のネッド・アレン(Ned Allen)が取り組んできた。プログラムの検証方法として、デジタル・コードをアナログ・コードに書き換えて、それをアナログ・コンピューターで走らせることをアレンは考えた。量子コンピューターは1種のアナログ・コンピューターである。
彼は量子コンピューターの専門家である南カリフォルニア大学のダニエル・ライダー(Daniel Rider)に相談したところ、D-Waveを推薦された。アレンはD-Wave社の量子コンピューターに関する論争を知っていたので、あまり乗り気はしなかったがライダーは強力に推薦した。そこでアレンは古い戦闘機F16のすでに開発されているコードをD-Wave社に送った。このコードにはバグがあり、社内の技術者がそれを発見するのに数カ月もかかったものである。そのバグはD-Wave社により6週間で発見された。そこでアレンは量子コンピューターの可能性を確信し、会社のお偉方を説得して量子コンピューターD-Wave Oneを買わせた。
そのコンピューターは南カリフォルニア大学の研究センターに設置され、ロッキード・マーチンの技術者と大学の研究者が共同で利用している。ライダーはそのセンターの所長になった。ライダーは、このコンピューターは汎用の量子コンピューターではなく特別目的用の量子コンピューターであると述べている。

量子コンピューター実用化の状況（1）

2012年にカナダのD-wave社が商用化を行なった量子アニーリング（Quantum Annealing）という方式のマシンはこれまで考えられていた量子コンピュータとは異なる方式ではあったが、そのマシンの動作原理に一部量子効果が見られるのではないかと話題になった。2015年にGoogleとNASAが共同でその技術を使用したアプリケーションに既存計算機との比較で1億倍程度の高速化の効果が見出されたと発表したため、全世界で大きな話題となり

量子コンピュータが実用化され始めた。2012年にD-wave社により商用化された量子コンピュータは、既存コンピュータの1億倍という超高速を記録。GoogleやIBMなどがしのぎを削り、MicroSoftはQ#という量子コンピュータの言語を発表した。コンピュータの世界は新たな次元に到達した。

量子コンピューター実用化の状況（1）

米Google社

特に量子コンピュータの開発に積極的な企業だ。現在はUSサンタバーバラのJohn Martinis氏のチームを迎え、積極的に量子ゲートモデルの開発を行なっており、22量子ビットの実機開発を終え、現在量子超越性（Quantum Supremacy）と呼ばれる量子コンピュータが既存スパコンを明確に計算量で超えるという議論に向かって49量子ビットの開発と測定を行なっている。

この量子超越性が明確に示されれば以降スパコンを含めた既存の計算機は特定領域での計算において量子コンピュータをうわまることができなくなり、さらに量子コンピュータの開発が加速される見込みである。また、近い将来米Google社のクラウド計算サービスへの量子コンピュータの提供が発表された。

また、米Google社の親会社であるアルファベット傘下のベンチャーキャピタルであるGVは米国内での他方式のイオントラップ方式を使用したIonQという企業にも出資を行なっている。ちなみにIonQには米Amazonも出資を行なっていることで話題となっている。

米IBM

早くから量子コンピュータの開発を進めてきた企業で、現在唯一米Googleと量子超越性を含めた議論で量子コンピュータ開発のしのぎを削っている。彼らの特徴はすでにクラウド経由で全世界から量子コンピュータを使用できる状態にあることで、登録することで個人で5量子ビットのマシンを無料で使用し、計算を行うことができる。

そのため、全世界の研究者やアプリケーション開発者はそれらのサービスを利用し、議論を行なっている。また、商用での利用には企業向けのプランもありより大きな量子ビットのマシンが使用できる。

米MicroSoft社

現在量子コンピュータ本体は開発中だが、世界中に抱える膨大なWindowsの開発者向けに量子コンピュータをプログラミングできる新しいQ#言語が人気だ。

Visual Studioと呼ばれる開発環境にインストールすることで自分で量子コンピュータ向けのプログラミングを行い、シミュレータと呼ばれる量子コンピュータの挙動を再現した仕組みによって実際の量子コンピュータと同様の計算を行うことができる。ちなみに量子コンピュータがなくても簡単な問題や小さい問題は私たちの持っているPC上で量子コンピュータを模擬した形で同様の計算を行うことができる

量子コンピューター実用化の状況（2）

半導体大手の米Intel社

最近量子コンピュータに力を入れている。ヨーロッパのデルフト工科大学と組み、超電導方式の量子コンピュータのチップの開発を加速させている。現在49量子ビットの試作を行なったとアナウンスしており、より動作の検証や周辺開発アプリケーション環境の整備とともに市販を行うなどの可能性も捨てられない。

カリフォルニアの米Rigetti社

注目のベンチャー企業の一つだ。IBMの量子コンピュータ開発出身の研究者が米国の最大手企業を相手にシリコンバレー方式で開発を行なっており、ITベンチャー企業らしく洗練され使いやすいソフトウェア環境が話題だったが、最近急速に技術力をつけており、19量子ビットの実機を発表した。また、アプリケーションも話題の分野をカバーしているのが特徴で、機械学習やAI、創薬、量子化学計算など既存の流行分野を的確に抑えている。

カナダのD-wave社

現在の量子コンピュータ開発競争に火をつけたベンチャー企業で、その他の企業とは異なる方式での開発や商用化を進めている。主に組合せ最適化問題と呼ばれる問題を得意とし、他の方式よりも消費電力が大幅に少ないのも特徴となっている。米Goldman sachs社なども出資しており、金融や機械学習、創薬への応用が期待されている。クラウド経由だけではなく本体の販売も行なっており、価格は10億から17億と言われている。

アリババ

2018年に本格的に量子コンピュータ開発に参入してくるのが中国勢だ。その中でも先陣を切って話題となっているのが中Alibaba社で上海に中国科学院と共同で量子コンピュータの研究所を開くという。中国は現在10量子ビットの開発が済んでいるといわれており、かつ超電導量子ビットの開発に欠かせない希釈冷凍機などの調達を2018年に大幅に行なっているため、急速に力をつけて開発レースに参加してくるものと思われる。

Accenture社

アプリケーション開発においても多くの企業がしのぎを削り始めている。Accenture社はカナダのベンチャーで量子コンピュータソフトウェア企業の1qbit社と共同で量子コンピュータ向けのアプリケーション活用領域を研究しており、既存の量子コンピュータ向けのアプリケーションを大幅に拡大し、顧客の要望に応えられるように準備を進めている。

量子コンピューター実用化の状況（3）

日本勢

量子イジングマシン方式の研究・実用化に日本は大きく貢献している
・量子アニーリング方式を考案したのは日本人 (1998年、東工大)西森教授稔氏と門脇正史氏(博士論文))
・レーザネットワーク方式の動作確認も日本の国立情報科学研究所 (2014年3月。2019年実現を推進中)

量子コンピューター関連の主な銘柄

銘柄	証券コード	概要
富士通	6702	カナダ・ワンキュービット社と人工知能分野で協業
NTT	9432	国立情報学研究所と共同開発。QNNで長時間の安定動作を実現
日立製作所	6501	組み合わせ最適化問題に特化した「イジングモデル」コンピューターを開発中
フィックスターズ	3687	2017年にDウェーブ社と協業の開始に合意
ブレインパッド	3655	量子アニーリング理論のビジネス活用で先行
エヌエフ回路設計ブロック	6864	超電導デバイスの信号増幅に用いる微少信号測定器を手がける
ユビキタス	3858	量子コンピューター向け公開鍵暗号技術で国内販売総代理店契約

量子暗号

暗号を制す者は世界を制す。
ナチスの暗号をコンピューターで解読しナチスを破った。

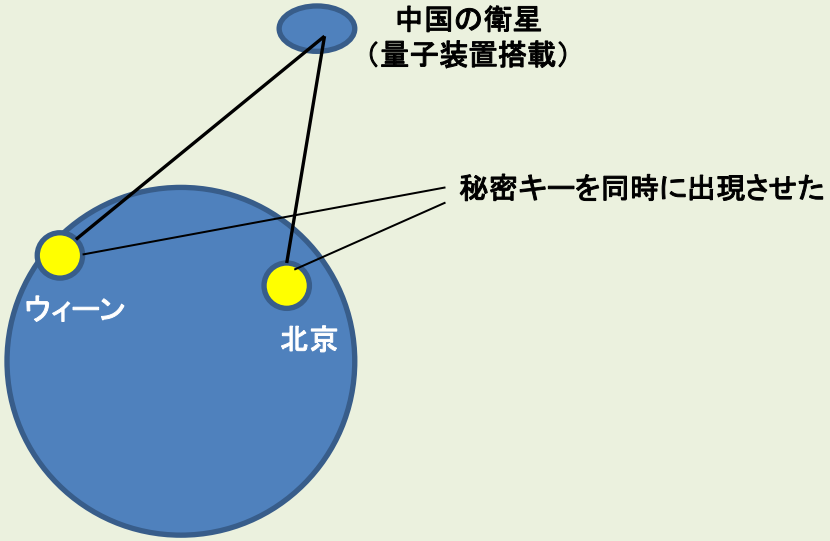
解読不能な暗号＝量子暗号
世界を変える最強の暗号　　基盤技術は欧米で生まれたが実用化では中国が先行している。

オンライン詐欺、ID盗難、ハッカー攻撃、電子的盗聴などから解放される。

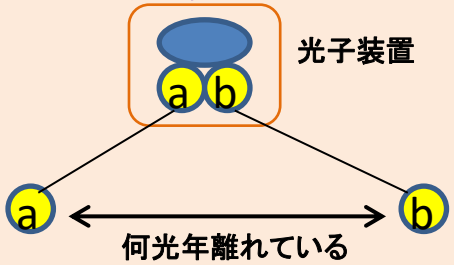
テロリストや犯罪組織が秘密に連絡を取り合ったり、政府が誰にも知られずに秘密を隠匿する可能性もある。

2017年9月に中国科学院の暗号学者と物理学者のチームが量子暗号を使用し北京とウィーンで30分に及ぶビデオ会議実験に成功。

量子のもつれ：1935年に発見、1984年に実験で確認された
　「同時に生み出された2つの光の粒子（光子）はどんなに遠く引き離されても双子のように同じ状態を維持し続ける」



量子からみあい（もつれ）



光子aの影響が瞬時にb伝わる

アインシュタインの相対性理論に反しないか？
“情報は光速以上では伝わらない。影響が光速以上で伝わることは問題ない！！”