

# 量子コンピュータの開発・導入の現状と影響

## 抄 録

本研究は、量子コンピュータの研究開発の現状を知るとともに、日本企業の量子コンピュータ導入予定を明らかにすることを目的として行った。文献調査とアンケート調査の結果から分かったことをもとに考察を行い結論を導いた。その結果、量子コンピュータは着実に開発が進んでいるものの、まだ一般企業が利用するには流通量やソフトウェアの実装、技術的進歩が不足していることがわかった。

## 1. はじめに

### 1.1 研究動機

この研究を始めたきっかけは、とある科学館で量子コンピュータの展示を見たことである。当時はほとんど理解できなかったが、自由研究のテーマを考えるにあたって少し調べてみたところ、多くの可能性を秘めていることを知り、興味を持った。先行研究では、米国企業の量子コンピュータ導入計画についてのものや、研究の現状を調べたものがあった(国立研究法人科学振興機構, 2018; 中沢・鷲見, 2019)。しかし、日本企業については調査は十分にされていないため、本研究を行うことにした。

### 1.2 研究目的

本研究の目的は、量子コンピュータの研究開発の現状と日本企業の導入予定、並びに量子コンピュータが将来社会にもたらすであろう影響を明らかにすることである。

## 2. 研究方法

### 2.1 調査対象者

今回の研究では、量子コンピュータが大きな影響を与えると予測されている新薬開発を行う日本の大手製薬会社4社と、量子コンピュータの研究を行う日本企業2社を対象にアンケート調査を行った。そのうち回答の得られた製薬会社1社、量子コンピュータの研究を行う企業1社を分析対象とした。

### 2.2 研究手順

まず文献で量子コンピュータの仕組みや有効な点、現在の世界的な研究開発の進捗や技術的課題点等を調べた。次に、アンケート調査で日本企業の研究の進捗、導入予定等を明らかにして外国との比較を行った。最後に、これらからわかったことをまとめ、本研究の成果とした。

### 3. 文献調査

#### 3.1 量子コンピュータの種類

量子コンピュータはその計算方法から大きく「ゲート型」と「アニーリング型」に分けられる。その方法は大きく異なるが、共に莫大な速度で計算を行うことが可能で、量子特有の重ね合わせ状態になれるという性質を利用して計算する点は共通している（竹内・丸山，2005）。

#### 3.2 重ね合わせ状態とは

一つの量子が同時に二つの状態を取っているという特殊な状態。量子は従来一つの状態しか取れないが、位相を変化させることによって重ね合わせ状態となることができる。ただし、重ね合わせ状態である量子は、測定すると、従来の状態に戻ってしまう。このことをデコヒーレンスと言い、これは時間経過によって自然に起こることもある。量子の位相は球と矢印で表すことがあり、矢印が上を向いた時は0，下なら1，横を向いていたら重ね合わせ状態となっている（竹内，2005）。

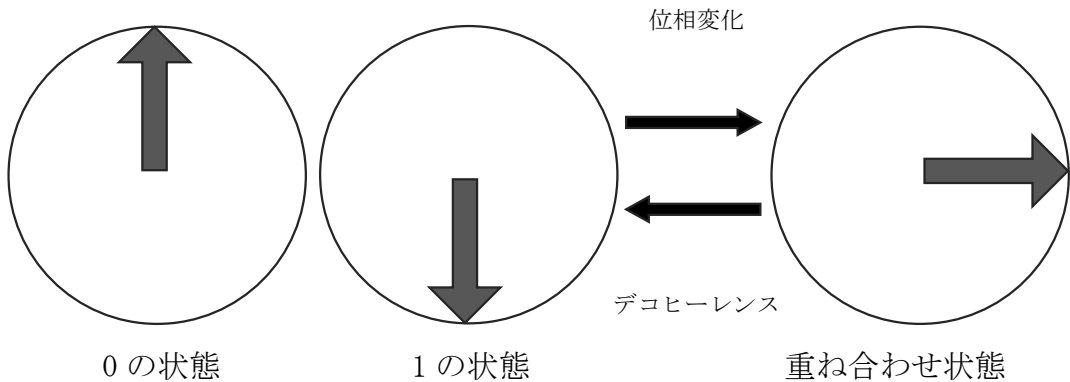


図1 重ね合わせ状態

#### 3.3 ゲート型

構造は古典コンピュータ（現在のコンピュータ）と比較的似ている。大きく違うのは、古典コンピュータはビットと呼ばれる0と1の羅列を用いて数字や文字を表し、計算しているのに対し、量子コンピュータは量子ビットを用いているという点だ。ビットは一度に一つの状態しか表せないで、いくつ集まっても一つの状態しか表せない。一方、量子ビットは重ね合わせ状態を用いることで、一つの量子ビットにつき、二つの状態を表すことができる。したがって10量子ビットでは2の10乗個もの状態を表すことが可能である。そのため、同時に大量の計算を行うことができるから、スーパーコンピュータを用いても解くのに時間のかかりすぎる問題も解くことができるのである。しかし、大量に計算を行っても、最終的に得られる答えはデコヒーレンスによって一個になってしまう。そのため、量子回路というものをを用いて欲しい答えが得られる確率を上げる必要がある。量子回路は解く問題の種類によって変えなければならず、その回路の組み方の研究も盛んである。現在高速に行えることがわかっているのは因数分解やデータ検索である（竹内，2005）。現時

点での主要なものはこの二つだけだが、研究が進めばもっと増える可能性が十分にある。ゲート型は有効性の研究に限らず、実現するための研究もまだまだ足りていない。実現までの課題としては、デコヒーレンスにより途中で計算が狂ってしまうを防ぐために重ね合わせ時間を伸ばすことやデコヒーレンスが起きた時のエラー修正を行うこと、また使用できる量子ビット数を増やすことが挙げられる（竹内・丸山，2005）。

### 3.4 アニーリング型

アニーリング型は組合せ最適化問題という、たくさんある選択肢の中でどの選択肢が最も条件に適するかを求める問題を解くのに特化した量子コンピュータである。計算には量子アニーリング法（量子焼きなまし法）という方法を用いる。量子アニーリング法では、磁束というものを量子として用いる。磁束には、絶対零度まで冷やすと電気抵抗がほとんどゼロになるという性質があり、これを輪にする事で、電流を流すとずっと流れ続ける超電導回路というものができる。この超電導回路を大量に並べ、強力な横向き磁場を作ることで、超電導回路を重ね合わせ状態にすることができる。この状態から少しずつ磁場を弱くしていくことでデコヒーレンスが起これ、右回りで電流が流れるものや左回りで電流が流れるものができる。量子にはエネルギーが最小となるようにデコヒーレンスが起これるという性質があり、これにより右回りか左回りかが定まる。こうして最終的に全ての量子がデコヒーレンスを起こした時の状態が、解いた問題の答えとなる。解く問題によって各量子間のつながりの強さを変えることでその問題の答えが得られる。アニーリング型は最も良い運転ルートの選別や最適な新薬の構造解明など身近な問題から専門的な問題まで多くの問題を高速で解くことができるため、広範囲に影響を与えられられる。実はもうすでにカナダの企業によって2011年に商用化されており、それを機に研究が盛んになった型である。そのため、まだまだ研究の勢いは増しており今後も開発が加速していくと考えられる（竹内・丸山，2005）。

## 4. アンケート結果

以下に各企業へのアンケート結果を載せる。

### ①製薬会社

#### a) アンケート内容

- I. 量子アニーリングマシン（アニーリング型）を導入する予定はあるか
- II. ゲート型量子コンピュータ（ゲート型）を導入する予定はあるか？
- III. もしいずれかを取り入れた場合、新薬開発以外に恩恵を受ける分野はあるか？

#### b) 返答

- I. 量子アニーリングマシンを手軽に実用するための計算機やソフトウェアが十分開発されておらず、簡単に使える状況ではないため、現時点では予定はない。開発が進めば、十分導入する可能性はある。
- II. まだ実現できるかすらはっきりとわかっていないので予定はない。意識はしており、調査を行っている。
- III. 製造業から様々な分野に応用できると考えている。

② I T企業（アニーリング型の研究で日本をリードしている）

a) アンケート内容

- I. 量子コンピュータを実現するにあたってどんな課題を抱えているか？
- II. 量子コンピュータ実現に向けて、今どんなことに注力しているか？
- III. 量子コンピュータを実現するにはあとどれぐらいかかるか？
- IV. 量子コンピュータが実用されるとどのような影響を社会に与えるか？

b) 返答

- I. アニーリング型とゲート型共に、量子ビット数を増やすことと重ね合わせ時間を伸ばすこと。
- II. より多くの量子ビット数で動作させることに取り組んでいる。
- III. アニーリング型はすでにカナダの企業D-Wave社が実現・商用化しているが、当社はまだそこには至っておらず、5年後を目指して研究開発を行っている。ゲート型は日本で研究を行っている企業は少なく、国内での実現は難しいかもしれない。いろいろ意見があるが、世界全体では10～20年後には実現すると見込んでいる。
- IV. アニーリング型は、渋滞緩和やインターネットコンテンツの効率良い配信、新薬開発への貢献など日常生活をより便利なものにすると考えられる。ゲート型は、因数分解が可能となることにより、インターネット通信の安全性を守るRSA暗号が解けてしまうのでその結果新しい暗号技術やネットワーク回路の発達などあらゆる社会の仕組みを支える分野に大きな変化をもたらす可能性がある。

表1 アニーリング型とゲート型の比較

	アニーリング型	ゲート型
計算方法	量子アニーリング法	量子回路による演算
効率良く解ける問題	組合せ最適化問題	組合せ最適化問題 + 因数分解
有効な事	新薬開発への貢献 渋滞緩和 インターネットコンテンツ の効率良い配信	新薬開発への貢献 RSA暗号の高速解読 データの高速検索
開発年	2030～2040年（予測）	2011（カナダ、D-Wave社） 2024～2025（日本の予定）

5. 考察

5.1 日本と外国の量子コンピュータの研究

次のページの表2を見てもらえばわかるように日本は外国に一步遅れていることがわかる。しかし、アニーリング型を導入している企業は自社でソフトウェアの開発も手掛けているため、実用できる企業は自社でソフトウェアの開発を行えるような大手企業に限られる。そのため、量子コンピュータを導入できない企業が少なくても、日本に限らず世界に共通していることなので、現時点でそこまで問題ではないと言えるのではないだろうか。

ただ、ゲート型の開発予定がないのは問題であるように思う。なぜなら、日本のようにインターネットが普及している国はゲート型量子コンピュータが実現するとリスクを被るからだ。ゲート型はRSA暗号の高速解読が可能であるため、仮に悪用されてしまったとすると、インターネットを介して個人情報等が漏れてしまう危険がある。そうなればインターネットが普及している国ほど危険である。すぐさまインターネットの代替品を作るのは困難であり、迅速な対処はできないだろう。そのような状況の時、自国内にゲート型量子コンピュータがあれば、それをういた実験を行って対処方法を考えることが可能となる。自国の安全を確保するためにも、ゲート型の研究は国内でしっかり行っておくべきである。

表2 日本と外国の量子コンピュータ開発の比較

		日本	外国
アニーリング型	計算機本体	2024年に開発（目標）	2011年に開発済み
	ソフト	未開発	開発中
	導入	予定なし	Google, IBM, Lockheed Martin 等が導入・実用
ゲート型	計算機本体	目立った開発予定なし	Google, IBM, Intel 等が開発中 2030～2040年（予測）

## 5.2 量子コンピュータに可能な事と社会に与える影響

表1から分かる通り、アニーリング型とゲート型で可能な事はある程度同じだが、異なる部分もある。

まずアニーリング型は、交通渋滞の減少等の我々の生活に密接に関わる問題を解くことができ、その幅は広い。そのため、多くの場面で生活を便利にすると考えられる。最適なパターンを導くのを得意とするので、あらゆる場面での無駄が少なくなると予測できる。また、AIに搭載することが可能となれば、AIの苦手とするとっさの判断を行う必要がある時、アニーリング型を用いれば、その状況に適したパターンを導くことができるので、よりその場にふさわしい行動を取れるようになるだろう。さらに、AIはそのパターンが適しているということを記憶して次に生かすことが得意なので、うまく組み合わせればAIの能力は格段に向上すると考えられる。それにはまだまだ多くの研究開発と時間が必要だが、将来はこのようなことも可能になるだろう。こういったことから、アニーリング型は社会を便利で無駄のないものに近づけると予測できる。

次にゲート型は、アニーリング型に可能なことに加え、データの高速検索やRSA暗号の高速解読が可能となる。データの高速検索は我々に恩恵をもたらすと考えられるが、RSA暗号の高速解読はある程度のリスクを伴う。それは先ほど述べたように個人情報流出だが、これは逆に科学技術の進歩を促す可能性もある。個人情報流出を防ぐために新たな暗号技術が発達すると考えられるからだ。すでに量子を用いた量子暗号というものの研究も始まっている。暗号技術が進歩すればそれによってネットワーク自体が変化することも十分考えられる。ネットワークが変わればそれに伴い新たな技術も発展する、といった具合に社会のあらゆる仕組みが変わる可能性を秘めているのである。

## 6. 結論

日本は量子コンピュータ導入予定がある企業が少なく、量子コンピュータの研究開発に関して外国より遅れていると言える。

アニーリング型は社会を無駄が少なく便利なものにすると考えられ、ゲート型はリスクを伴うものの、社会のあらゆる仕組みを変え、我々の生活に大いに貢献する可能性があると言える。アニーリング型はソフトウェアの開発に伴って実用化が進みゲート型は20～30年後には実現していると考えられる。

## 7. 参考文献

国立研究開発法人 科学振興機構 『みんなの量子コンピューター』 論文 (2018)

竹内薫・丸山篤史 『量子コンピューターが本当にすごい』 PHP新書 (2015)

竹内繁樹 『量子コンピューター 超並列計算のからくり』 講談社 (2005)

中沢潔・鷲見拓哉 『米国における量子コンピューターの現状』 論文 (2019)

夏梅誠・二間瀬敏史 『(図解雑学) よく分かる量子力学』 ナツメ社 (2005)

西野哲朗 『(図解雑学) 量子コンピューター』 ナツメ社 (2005)