訳者まえがき

量子コンピューティングへの関心が日本国内でも高まっている。大学などの研究者の枠を超えて，企業，行政，さらには一般社会からも関心や期待が寄せられ，メディアでも「量子コンピュータ」という言葉を目にすることが多くなった。しかし，最前線の研究者であっても，物理学や計算機科学に加えて数多くの工学分野との境界領域にあるこの膨大な分野の全貌を見渡すことは困難である。

本書は，米国の科学アカデミー・工学アカデミー・医学アカデミーの下に設置された「量子コンピューティングの可能性と影響に関する技術検討委員会」が編集・執筆した報告書の日本語訳であり，量子コンピューティングに関わるほぼすべてのテーマについて詳細な記述がなされている。米国はこの分野の研究開発で世界をリードしており，一流の研究者たちが執筆に関わった本書はきわめて貴重な文書である。式や詳細なデータを用いた論文スタイルの記述ではなく，ほぼ全編にわたって文章のみを用いて，現状の分析から将来の見通しまで，正確かつわかりやすい解説が展開されている。研究者だけでなく，量子コンピュータに関心を持つ広範な読者も比較的容易に読み進められると思われる。

一流の現役研究者たちがアカデミーの下に結集して，教科書とも言えるような包括的な報告書を書き上げる努力は並大抵ではなかったに違いない。しかも，量子コンピューティングそのものの研究者だけではなく，委員長自身をはじめとする他分野の研究者や，スタートアップを中心とする企業人，行政関係者，さらには独立コンサルタントまで含むきわめて広範な人たちを執筆者や協力者に加えて，広い立場から俯瞰的な文書を仕上げる体制に米国の活力を感じる。ま

た，執筆者・協力者の所属リストからは，米国における最先端技術分野の産業構造が垣間見えて興味深い。例えば，長い歴史を持つ大企業は IBM だけである。

2018 年の暮れにウェブ上に本書が公開されたのを目にしたときにはその類を見ない重要性に驚くと同時に，日本語に翻訳して日本国内でも広く読まれるようにする必要性を強く感じた。さしあたり要約部分だけを翻訳して筆者のウェブページで公開したが，全文翻訳はハードルが高く，日常業務の波に飲み込まれる中でなかなか手が付けられなかった。しかし，この分野の進展は急速で，数年経つと情報の古さが目立つようになってしまうという危機感から，ようやく 2019 年の夏に翻訳を開始して秋には仕上げることができた。本格的な英日翻訳は初めての経験で，言葉の使い方や文章表現の難しさを痛感すると同時に，全文を何度も詳細に読み込む貴重な経験を経て，この分野に対する自分自身の理解が大きく深まったことを感じた。少しでもこの経験を読者と共有することができれば幸いである。力量不足からくる文章表現の拙さや誤訳などもまだまだあるに違いない。お気づきの点はぜひお知らせいただきたい。また，正誤表などは `https://www.kyoritsu-pub.co.jp/bookdetail/9784320124554` に載せる予定である。

言葉の使い方などについて次の方々から貴重なコメントをいただいたことに心より感謝したい（敬称略）。青木和麻呂，青野良範，五十部孝典，大森賢治，門脇正史，草川恵太，國廣昇，小寺哲夫，篠原直行，高島克幸，藤井啓祐，盛合志帆，安田貴徳。もちろん，誤訳などの責任はひとえに筆者にのみある。さらに，ファイルの整形等で研究室秘書の上杉典子さんの手を頻繁に煩わせた。また，共立出版の菅沼正裕さんにも随所で大変お世話になった。お二人の力がなければ比較的短い時間でこのような形に仕上げることはとてもできなかったことを記して，感謝したい。本書がこの分野の理解を促進し，量子コンピュータの実現に向けた研究開発活動の活性化，ひいてはその実現を通したよりよい社会の実現に少しでも寄与することができれば望外の幸せである。

2019 年 10 月
西森秀稔

まえがき

量子コンピューティングというテーマは 10 年前には一般にほとんど知られていなかったが，ここ数年の間に爆発的な関心の広がりが見られるようになってきた。ひとつの理由は，半世紀にわたってコンピュータの性能向上をもたらしてきた技術革新のペース（ムーアの法則）が停滞して新たなコンピューティング技術の必要性が高まってきたことである。しかし，より重要な要因は量子コンピュータ (quantum computer) の類を見ない計算能力や，近年のハードウェア，ソフトウェア，アルゴリズムの開発の進展だろう。

従来は，現実的なコンピュータはすべて，拡張された Church-Turing のテーゼ [1),2)] を満たしていた。どんなコンピュータも標準的な「ユニバーサル（汎用）」コンピュータよりせいぜい多項式程度しか速くない，つまり高速化の程度はせいぜいべき乗則程度だというわけである。「古典」[3)] コンピュータは，演算の高速化（クロック周波数の向上）や 1 クロックサイクルで実行される演算数の増加を通して，パフォーマンスを何桁も向上させてきた。計算のパフォーマンスは何桁も上がったが，それはユニバーサルなコンピュータと比較しても

---

1) M.A. Nielsen and I. Chuang, 2016, *Quantum Computation and Quantum Information*, Cambridge University Press, U.K.

2) P. Kaye, R. Laflamme, and M. Mosca, 2007, *An Introduction to Quantum Computing*, Oxford University Press, Oxford, UK.

3) 量子コンピューティングの分野では，古典物理学の法則に従って情報を処理するコンピュータは，量子効果を情報処理に利用する「量子コンピュータ」と区別するために「古典コンピュータ (classical computer)」と呼ばれる。本書でもこれにならうことにする。

（大きな）定数倍の加速に過ぎない。ところが，Bernstein たちが 1993 年に量子コンピュータは「拡張された Church-Turing のテーゼ」を破る可能性があることを示した [4]。1994 年には，大きな数の素因数分解という実用的な例で量子コンピュータの持つ能力が発揮されることを Peter Shor が示した。量子コンピュータはこの問題を古典コンピュータより指数関数的に高速に解けるのである。これは画期的な成果ではあるが，その当時は，量子コンピュータのもっとも基本的な要素である量子ビットをどうやって作ったらよいか誰にもわからなかった。ましてや，完全な量子コンピュータはなおさらである。しかし近年，状況が変わってきた。

イオン化された原子を捕捉（トラップ）して使う技術（捕捉イオン）と微小な超伝導回路を使う技術の 2 つが長足の進歩を遂げ，小規模な量子コンピューティングシステムの試作機が作られただけでなく，それが研究コミュニティに公開されているケースもある。最近のこうした進展を反映して，量子コンピューティングに対する関心が世界的にも爆発的な広がりを見せている。しかしながら，関心の高まりと同時に，量子コンピューティングの可能性や現状について過剰な期待や混乱も見られる。量子コンピューティングがコンピュータのパフォーマンスを向上させ続けるだろう（実際はそんなことはない）とか，コンピュータ業界を変えてしまうだろう（実際には，短期的な影響は小さいし長期的には不明）というような記事を目にすることが珍しくない。

量子コンピューティングの可能性と影響に関する技術検討委員会は，ユニバーサルな量子コンピュータに関する最先端の研究開発状況，進展の方向性，想定される影響などを調査し明らかにすることを目的として編成された。この使命に向けて作業を進める過程で，量子コンピューティングの理論的な特性や限界についても明らかにすることや，一般社会で見られるこの分野に対する誤解を解くことにも取り組んできた。

本委員会は対面の会議を 3 回，テレビ会議を多数回実施するとともに，遠隔で

---

[4] E. Bernstein and U. Vazirani, 1993, “Quantum Complexity Theory,” in *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing* (STOC’ 93), ACM, New York, 11–20, http://dx.doi.org.stanford.idm.oclc.org/10.1145/167088.167097.

の共同作業などの方法で職務を遂行した。付託に応えるため，量子コンピューティングのハードウェア，ソフトウェア，アルゴリズムの現状を理解することと，Shor のアルゴリズムを実装することができるスケーラブル[a)] なゲートベースの量子コンピュータ実現のためにはさらにどのような進展が必要かという点に的を絞って執筆した。現状のアプローチのままでは，完全な誤り耐性 (fault tolerant) を持つスケーラブルな量子コンピュータのサイズまで大規模化することはできないということが，検討の比較的早い時期に明らかになった。そこで，最終目標に向かっての進歩の状況を追うための中間的なマイルストーンや指標を探ることにした。議論全体を通して，単一の要素ないし分野からだけではなく，多様な分野の見方を統合したシステムとしての立場から，実用的な量子コンピュータを作るという目標に向かっての進歩を考察するように努めた。

この作業はすべて，非機密事項の枠組みにおいて実施した。それゆえ，量子コンピューティングの進歩やその意義についての本委員会の評価は，委員の専門知識や経験，公開の会議で得られたデータ，外部の専門家との 1 対 1 の会話，そして一般に広く公開されている情報のみに基づいて作成している。機密活動に関する情報は，どの国のものであれ本委員会は所有していない。そのため，本委員会の評価は正確であると信じているが，どうしても不完全な情報のみに基づいたものであることは認識しており，（企業のものであれ国家のものであれ）オープンサイエンスの枠外の研究に関する知見によっては評価が変わる可能性を否定できない。

本書を読むにあたって

本書は本委員会の活動成果を報告するものである。まずサマリーを読んで主要な結果をざっと把握することをお勧めする。サマリーでは，それぞれの論点について本文中で詳述している個所を挙げてあるので，興味を引く話題についてのより詳細な議論をすぐ参照することができる。

各章の要約を述べておこう。

- 第 1 章はコンピューティング分野についての背景や状況を述べ，量子コン

[a)] （訳注）「スケーラブル (scalable)」という言葉は，大規模化が可能という意味で用いている。

ピュータの優位性を紹介する。古典コンピューティング技術の半世紀以上にわたるパフォーマンスの向上は，どのようにして成し遂げられてきたかについて注意深く分析する。このスケーリング（大規模化）は，新たな技術による製品が収益を増やし，それがまたさらに新たな技術開発に結び付くという好循環によるところが大きい。量子コンピューティングも同じように成功するためには 2 つの道がある。量子コンピュータの実用的な能力がどんどん向上し好循環が始まるか（このステージに達するまでは政府の経済的支援が必要），当面は収益や有用性がないにしても実用的に役に立つマシンを作るという目的に向けて必要な投資を惜しまない組織が研究開発を続けるかである。後者の場合，投資の総量はとてつもなく大きくなるだろう。

- 第 2 章では，量子コンピューティングを支える量子力学の原理を紹介する。従来のコンピュータとは違った原理で動く量子コンピュータは極めて面白いが，実際に作るのは難しい。そこで，古典物理学の法則に従って情報を処理する現在のコンピュータ（量子コンピューティングのコミュニティでは「古典コンピュータ」として知られている）と量子コンピュータを比較する。ここでは，量子コンピュータに量子ビットを 1 つ付け加えるだけで扱える問題サイズが 2 倍になる理由を説明する。この計算能力の向上には制約がある。ゲートのノイズが大きいこと（量子ゲート演算は大きな誤り率を伴う），データは一般には効率よく読み込めないこと，システムの測定能力には限度があること，これらの理由により有効な量子アルゴリズムを作るのが難しい。本書で調べた 3 つの違ったタイプの量子コンピュータを，本章では紹介する。アナログ量子コンピュータ (analog quantum computer)，デジタルなノイズあり中規模量子 (NISQ，noisy intermediate-scale quantum) コンピュータ，そして完全な誤り耐性量子コンピュータである。
- 量子コンピューティングの能力を引き出すのが難しいことを念頭に置いて，第 3 章では量子アルゴリズムをより深く見ていく。完全な誤り耐性コンピュータ用の基本的なアルゴリズムから始めるが，誤り耐性を実現するためのオーバーヘッド (overhead) がきわめて大きいことを示す。誤りなしに複雑なアルゴリズムを実行できるいわゆる論理量子ビットをエミュレートするための物理量子ビット数や物理ゲート演算の数が非常に大きいので

ある。それゆえ，このようなマシンは長年にわたって出現しないだろう。さらに，アナログ量子コンピュータや NISQ コンピュータ用の実用的で役に立つアルゴリズムの候補を調べ，この分野でのさらなる研究の必要性を指摘する。

- Shor のアルゴリズムを使えば，現行の公開鍵暗号を破る（秘密鍵を知らずに復号する）ことが可能になる。第 4 章では現在用いられている電子データや通信を保護している従来の暗号について議論し，大規模な量子コンピュータがどうやってそれを破るのか，またそうした脆弱性に対処するために暗号分野のコミュニティが今取り組むべき（あるいはすでに取り組んでいる）ことは何かを述べる。
- 第 5 章と第 6 章では，量子コンピューティングに必要なハードウェア（第 5 章）やソフトウェア（第 6 章）を構築するための一般的なアーキテクチャやこれまでの進歩の状況を議論する。
- 第 7 章においては，量子コンピューティングが顕著な進歩を遂げるのに必要な技術的進展などについての本委員会の評価を述べるとともに，想定される時間スケール，進展の意義，そしてこの分野の将来の見通しを紹介する。

本書は専門家でなくても読めるように努力したが，いくつかの章では問題点を詳しく説明するために少々（あるいはそれ以上に）専門的になってしまっている。そのような部分は読み飛ばしてもらっても構わない。重要な点については，章ごとのまとめの中で強調するか節や章の終わりで要約している。

謝辞

本書執筆にあたっては多くの方々からご協力をいただいた。本委員会および米国科学アカデミー・工学アカデミー・医学アカデミーより心からの感謝を申し上げたい。海軍海上戦センター Dahlgren 部門の Jake Farinholt 氏より提供された量子コンピューティングおよび関連分野の文献解析結果は，世界的な動向をわかりやすく示すのに役立った。欧州委員会 (EU) 駐米代表部参事官の Mary Kavanagh 博士と在ワシントン駐米オーストラリア大使館参事官 Anthony Murfettm 氏からは，量子科学技術における EU とオーストラリアの研

究状況についてご教示いただいた。

委員会の席上で技術面での専門知識を提供して下さった方々に加えて，Mark Saffman，Jonathan Dowling，Pete Shadbolt，Jelena Vuckovic，Helmut Katzgraber，Robert Colwell，Eddie Farhi の各氏からも本委員会の委員に個別に，本書に関連して専門的な助言をしていただいた。

本調査に対しては米国国家情報長官室から財政的な援助を受けた。CSTB のシニアディレクター Jon Eisenberg 氏からは助言をいただいた。本委員会の委員は，貴重な時間を本書執筆に費やしただけでなく，量子コンピューティングが専門でない委員長にいろいろと教示してくださった。心から感謝したい。また，シニアディレクターの Emily Grumbling 氏に特別の感謝を表明したい。彼女の長時間にわたる尽力がなければ，本書はできなかっただろう。委員長が職務を心地よく遂行することができたと述べるのは特に珍しいことでもないかもしれないが，今回は本当にその通りだった。量子コンピューティングの持つ力，進歩の状況，そして問題点などについて学ぶのは素晴らしい経験だった。本書が，読者にとってこのテーマを学ぶための一助となれば幸いである。

量子コンピューティングの可能性と影響に関する技術検討委員会
委員長　Mark Horowitz

レビューアーへの謝辞

このコンセンサス研究報告は，出版に先立つ草稿の段階で幅広い見識と専門知識を持つ研究者にレビューをお願いした。米国科学アカデミー・工学アカデミー・医学アカデミーは，率直な批判を受けることにより報告書の信頼性を向上させるとともに，高品質，客観性，エビデンス，任務への対応などにおける水準の保証を目指している。いただいたコメントと草稿は，審議が率直に行われるために非公開とすることにした。

以下の方々のレビューに対して感謝の意を表したい。

Scott Aaronson（テキサス大学オースティン校）
Kenneth R. Brown（デューク大学）
Jerry M. Chow（IBM トーマス J. ワトソン研究所）
William J. Dall[1)]（工学アカデミー，NVIDIA コーポレーション）
Sean Hallgren（ペンシルベニア州立大学）
John P. Hayes（ミシガン大学）
Daniel Lidar（南カリフォルニア大学）
John Manferdelli（ノースイースタン大学）
Anne Matsuura（インテル研究所）
William H. Press[2)]（科学アカデミー，テキサス大学オースティン校）
Steven J. Wallach（工学アカデミー，マイクロンテクノロジー）

1) 米国工学アカデミー会員。
2) 米国科学アカデミー会員。

上記の方々は建設的なコメントや提案を多数提出してくださったが，本書の結論や提言を是認することを求められたわけではなく，最終版を公開前に見る機会があったわけでもない。報告書に対するレビューは Samuel H. Fuller 氏（工学アカデミー会員，アナログ・デバイセズ社）が監修した。科学・工学・医学アカデミーの基準に従って本書が第三者によって審査され，レビューアーからのコメントが適切に処理されたことを氏が責任をもって確認した。最終版の内容に対する責任は，ひとえに本委員会と科学・工学・医学アカデミーが負っている。