CRDS-FY2018-SP-04

戦略プロポーザル

みんなの量子コンピューター

～情報・数理・電子工学と拓く新しい量子アプリ～

STRATEGIC PROPOSAL

Quantum Computer Science for All

- Towards novel quantum applications -

国立研究開発法人科学技術振興機構 研究開発戦略センター
Center for Research and Development Strategy, Japan Science and Technology Agency

研究開発戦略センター（CRDS）は、国の科学技術イノベーション政策に関する調査、分析、提案を中立的な立場に立って行う公的シンクタンクの一つで、文部科学省を主務省とする国立研究開発法人科学技術振興機構（JST）に属しています。

CRDS は、科学技術分野全体像の把握（俯瞰）、社会的期待の分析、国内外の動向調査や国際比較を踏まえて、さまざまな分野の専門家や政策立案者との対話を通じて、「戦略プロポーザル」を作成します。

「戦略プロポーザル」は、今後国として重点的に取り組むべき研究開発の戦略や、科学技術イノベーション政策上の重要課題についての提案をまとめたものとして、政策立案者や関連研究者へ配布し、広く公表します。

公的な科学技術研究は、個々の研究領域の振興だけでなく、それらの統合によって社会的な期待に応えることが重要です。「戦略プロポーザル」が国の政策立案に活用され、科学技術イノベーションの実現や社会的な課題の解決に寄与することを期待しています。

さらに詳細は、下記ウェブサイトをご覧下さい。

http://www.jst.go.jp/crds/

エグゼクティブサマリー

半導体微細加工技術によるコンピューターの飛躍的な性能向上が技術的・経済的な限界に近づき、これまでのようにトランジスタ数の増加による性能向上はもはや望めなくなってきている。一方で、ビッグデータ処理、メディア処理、深層学習、組合せ最適化などの計算要求はいっそう高まると予想され、コンピューターの性能向上には大きな社会的期待が寄せられている。新計算原理、新アルゴリズム、新アーキテクチャ、新デバイスなどにより微細加工技術だけに頼らずに継続的に性能向上を図ることは急務である。

このような背景の中、近年特に注目を集めているのが「量子コンピューター」である。理論通りに動作すれば､現在のコンピューターよりも本質的に高速な計算が可能となるが､現在のところ、量子性に基づく量子コンピューターの高速性を実験実証するには至っておらず、Shor の因数分解や Grover の検索などの典型的な量子アルゴリズムが要求する量子ビット数やエラー率と、今後 10 数年で登場すると考えられる小規模・高エラー率の「NISQ[1] 量子コンピューター」の間には大きな隔たりがある。

このギャップを埋めるには、ソフトウェアとアーキテクチャの研究開発を充実させ、量子アルゴリズムから量子ハードウェアに至る量子コンピューター研究開発全体を強化する必要がある。具体的に取り組むべきものとして、（1）古典・量子ハイブリッドアルゴリズムの開発・実装・実証、（2）量子ソフトウェア開発環境の整備、（3）量子誤り訂正符号に基づく量子コンピューターアーキテクチャ設計、が挙げられる。とくに、NISQ 量子コンピューターについては、どのような問題であれば量子性の恩恵を受けられるのか、新アルゴリズムとキラーアプリケーションの探索・発見が必須課題である。そのためには、新アルゴリズムの開発・実装の試行錯誤と、それを実行可能とするシミュレータやライブラリ、コンパイラ、デバッガなどの各種ツール群がパッケージとなったソフトウェア開発プラットフォームの構築が必要となる。さらに、将来的には誤り耐性量子コンピューターの実現を視野に、誤り訂正符号処理や制御・測定の古典回路まで含めたアーキテクチャ開発、ファームウェアの開発、誤り訂正符号の実装を支援するソフトウェアツールの開発などハードウェア・ソフトウェアに跨る研究課題に取り組むことも重要である。

これまで、量子情報処理分野は物理学の一分野として成長を続けてきたが、世界的な研究開発の中心は「いかに量子コンピューターを作るか」という工学的なチャレンジに移行しつつある。これからは、分野融合・企業参画・国際連携それぞれの局面で様々なプレーヤーがそれぞれ必要とされる役割を担う“みんなの”量子コンピューター研究開発が重要となる。つまり、知見、技術、人材など量子コンピューター実現のために必要となるあらゆることを、学問分野や所属の壁を越えて交流することがカギとなる。どのプレーヤーも必要な技術や人材をフルスタックで用意するのは困難であるからこそ、海外の研究チームまで含めた共同研究やオープンソースの積極活用などの形で、不足する部分を補うことも必要と考えられる。

量子コンピューター実現の社会的インパクトは大きいものの、多くの民間企業にとっては未だリスクの高い内容も多い。そのため、必然性のある融合研究を促進する目的志向のグラント、ハードウェアからソフトウェアまでをフルスタックで用意する国際的な研究開

[1] Noisy Intermediate-Scale Quantum：小規模で誤り訂正がない近似的量子コンピューター。

発ネットワークの構築、そのハブとなる研究開発・共同利用拠点の構築、量子コンピューターシミュレーターを含めたソフトウェア開発環境の提供、などを政府が先導的に行うことが必要となる。

またその上で、コンペティション形式での研究開発の促進、量子力学の理解を前提としない教育・訓練プログラムの開発・提供、正確で積極的なアウトリーチ・科学広報活動、スピンアウトする量子スタートアップ企業の積極的支援などの多様な施策により、コミュニティ形成・エコシステム形成を強力に促進することが求められる。

今後 50 年の間には、量子コンピューターだけでなく、量子センサーや量子インターネットなどの量子科学技術と組み合わせた「量子 ICT」を自由自在に使いこなす時代が確実に訪れるだろう。その中では、本プロポーザルで取り上げた機械学習や量子化学計算の進展だけでなく、新たなサービスや未だ見ぬ産業の創出が行われると同時に、量子 ICT を使った科学研究や科学的発見も行われるはずである。量子コンピューター研究開発を強力に加速・推進することで NISQ 時代を超えた量子 ICT 時代へ向けて、スケーラブルなエラー耐性量子コンピューター実現への確固たる一歩を、我が国が世界に先駆けて進めるべきである。

Executive Summary

The exponential performance improvement of modern computers approaches technological and economic limits of the semiconductor microfabrication. We are no longer able to enjoy the "free lunch" of performance improvement by the increase in the number of transistors. Meanwhile, computational demands, such as big data analytics, media processing, deep learning, combinatorial optimization, secure cloud computing, are expected to increase, thus great social expectation is given to the improvement of the capability of modern computer systems. It is urgent to continually improve the performance without increasing the number of transistors by using a new computing paradigm, novel programming models, new algorithms and software, non-conventional architectures, devices and materials, and so on.

Reflecting such a research trend headed to the post-Moore's-law era, "quantum com-puter" is attracting academia and industry in recent years. If quantum computer operates according to the theory, it is possible to perform essentially faster computation than the modern computer (or so-called "classical" computer). However, this quantum speedup has never been proven by experiment at the present time. There is still a big gap between the situation of real machines and the number of the qubit (quantum bit) and fidelity of the control gate required by typical quantum algorithms, such as Shor's factoring and Grover's search algorithms.

In order to fill this gap, it is necessary to enhance the research and development of quantum software and architecture and strengthen the whole quantum computing re-search from quantum information theory to quantum hardwares. The research targets are (1) development, implementation, and demonstration of quantum-classical hybrid algorithms, (2) preparation of quantum software development environment including lan-guage, compiler, debugger, and simulator, and (3) quantum computer architecture design based on quantum error correction code.

In particular, for NISQ[2] computers, it is essential to explore and discover new algo-rithms and killer applications as to what kind of problems can take benefit from quantum computing. To that end, it is necessary to construct a software development platform packaged with various tools and simulators that make the quantum programs executable in a trial-and-error manner. It is also important to tackle research topics that span hardware and software. More specifically, this includes the quantum computer architec-tures that implement quantum error-correcting code, the development of middleware and firmware to support the implementation of error correction codes, electrical engineering on control electronics for precise control and measurement of qubits.

The field of quantum information processing has been growing as a part of physics, but the trend of worldwide R&D on the quantum computing is gradually shifting to

[2] Noisy Intermediate-Scale Quantum

the engineering challenge of “How to build quantum computers”. This may be fully answered only by neither physics nor computer science.

From now on, “quantum computer science” will play an important role as a guiding principle for building the quantum computer. The various players are needed in each aspect of interdisciplinary integration and collaboration, the participation from industry and developers community, and partnership with international collaborators. Because it is difficult for any player to prepare the necessary technology and personnel in full stack, it is key to exchanging everything necessary for the realization of the quantum computer such as knowledge, technology, human resources, over barriers of disciplines and affiliations.

Although the great economic and social impact of realization of the quantum computer is expected, its R&D requires a long-term perspective and thus it is still too uncertainty and risky for many private companies. Therefore, the investment on the quantum com-puter from the market will be insufficient. Thus, the government should take action on the promotion of inevitable multidisciplinary research on quantum hardware and software, establish new R&D centers as a hub for the network, the provision of a quantum software development environment, and fostering quantum computing community and business ecosystem.

In addition to the promotion of R&D by “quantum-native” researchers and engineers, it is necessary to provide education and training programs to people who are not so familiar with quantum mechanics. The quantum computing community has a responsibility to provide accurate and aggressive outreach and engagement to the society. Supporting the quantum start-up companies to spin out is also important to the formation of quantum computing ecosystem.

In the next 50 years, we will enter the era of “quantum ICT”, where we can freely use and combine various quantum technologies such as quantum sensors, quantum net-work, quantum clock, quantum cryptography, and quantum computers. In this era, we should not only see the great advancement of quantum chemical calculation and quantum machine learning as discussed in this proposal but also the creation of new quantum ap-plications, services, and industries. At that time, scientific research and discovery using quantum computers will not be science fiction anymore.

We should strongly accelerate and promote quantum computer science towards the quantum ICT era beyond the NISQ era and advance a solid step to the realization of the scalable fault-tolerant quantum computer.

目　　次

1．研究開発の内容

1.1 量子コンピューターとは

半導体微細加工技術によるコンピューターの飛躍的な性能向上が技術的・経済的な限界に近づき、これまでのようにトランジスタ数の増加だけによる性能向上はもはや望めなくなってきている。一方で、ビッグデータ処理、メディア処理、深層学習、組合せ最適化などの計算ニーズはいっそう高まることが予想され、コンピューターの性能向上には大きな社会的期待が寄せられている。新計算原理、新アルゴリズム、新アーキテクチャ、新デバイスなど新しい計算パラダイムとその計算機システム実現技術への関心が、近年急速に高まっている [1, 2, 3]。

このような背景の中、近年特に注目を集めているのが「量子コンピューター」である [4, 5, 6, 7]。理論通りに動作すれば、現在のコンピューターよりも本質的に高速な計算が可能となるが、例えば Shor の因数分解や Grover の検索などの典型的な量子アルゴリズムで有用な計算を実行するには、大規模で長時間の計算が実行できる「エラー耐性量子コンピューター」が必要となる。一方で、現在のハードウェア開発の最先端から見て、今後10 数年で利用可能になるのは、小規模で誤り耐性が限定的な「NISQ[1] 量子コンピューター」であり、その間には大きな隔たりがある。

「量子コンピューター」と呼ばれる計算機は、表 1.1 のように大きく分けて 3 種類ある。（1）エラー耐性量子コンピューター、（2）NISQ 量子コンピューター、（3）量子アニーラー、である。

エラー耐性量子コンピューターは量子誤り訂正符号により多数の物理的な量子ビットから論理ビットに符号化し、大規模な計算を精度よく実行するデジタルコンピューターである。エラー耐性量子コンピューターの計算原理は量子回路モデルと呼ばれ、量子力学の性質を積極的に活用して計算を行う。具体的には、量子力学の重ね合わせ原理により指数関数的に膨大な数の超並列計算を行い、そこで得られた無数の計算結果から確率振幅の波の干渉を利用して正答を高速に取り出す。このような方法で古典コンピューターよりも速く問題を解くことができるアルゴリズムとして、Shor の因数分解アルゴリズムや Grover の検索アルゴリズムなどが知られている [8]。

NISQ 量子コンピューターは実現性の観点で注目されている。計算原理は量子的（量子回路型）であるが、誤り訂正機能を持たず量子ビット数も少ないため、近似的量子コンピューターとも呼ばれる。リソース制約が強い中で、どのような有効な計算を行うかということが焦点となっている。量子コンピューターが古典コンピューターを上回る量子超越（Quantum Supremacy）の実証プラットフォームとしても注目を集めている [9, 10]。量子・古典ハイブリッドの計算アルゴリズムが複数提案されており、古典コンピューターシステムとして見ると、CPU が実行する計算の一部分を担うアクセラレーターの位置づけとなる。また、量子誤り訂正が無いことで、計算機システムの構造は、先述のエラー耐性量子コンピューターとは異なる部分も多い。

量子アニーラーは、量子アニーリングという計算原理により組み合わせ最適化問題を解

[1] Noisy Intermediate-Scale Quantum：小規模で誤り訂正がない近似的量子コンピューター。

表 1.1: 量子コンピューターの種類

	(1)エラー耐性量子コンピュータ	(2)NISQ量子コンピュータ	(3)量子アニーラー
	因数分解や検索など様々な量子プログラムの実行により精度よく計算が実行できる汎用デジタルコンピュータ。	小中規模の量子ハードウェアによる近似的量子コンピューター。量子誤り訂正符号は実装されず、アナログの計算機に近い。	組合せ最適化問題など特定の問題にハードウェア特化したアナログコンピュータ。
(A)量子加速 計算複雑性の意味で「早い」かどうか。	いくつかの問題について、現状のベストなアルゴリズムよりも優れた量子アルゴリズムが存在。	問題によって現状のベストなアルゴリズムよりも優れた量子アルゴリズムが知られているが、どの程度の問題サイズで量子が優位となるか非自明。	古典アルゴリズムより高速であると証明された量子アルゴリズムが知られていない。量子性と計算加速の関係性も不明な点が多い。
(B)ハードウェア加速 実計算時間の意味で「早い」かどうか。	問題の種類や実装などによる。エラー訂正のクロック周波数が律速する場合が多い。現時点では理論的な比較のみ可能。	問題の種類やハードウェア実装の委細、初期値の選び方など様々な条件に依存。ベンチマークはこれからの研究課題だろう。	問題の種類やハードウェア実装の委細、初期値の選び方など様々な条件による。比較する研究が進んでいる。

く専用計算機である。カナダの D-wave Systems 社が、「世界初の商用量子コンピューター」と宣伝され注目が集まったが、エラー耐性量子コンピューターや NISQ 量子コンピューターとは異なった計算原理に基づく計算機と理解した方が良い。量子アニーラーは、組合せ最適化問題をエネルギー最低化問題としてハードウェアにマッピングし、超伝導量子ビット上の物理現象[2]により最適解を求めるアナログコンピューターである。また、ここから派生した、組み合わせ最適化問題をイジングモデル（のエネルギー最低化問題）に帰着させて解く**イジングマシン**が、日立製作所、富士通、NTT などから相次いで提案されている [11, 12]。

このように、量子力学の性質を積極的に利用した、あるいは、そこから着想を得た、高機能な計算の実現を目指して、ハードウェア・ソフトウェアの幅広いスペクトルでの研究開発が意欲的に進められている。

1.2 提案する研究開発の概要

理想であるエラー耐性量子コンピューターと現状の量子デバイスとの間にある、大きなギャップを埋めるには、量子ソフトウェアとアーキテクチャの研究開発を充実させ、量子アルゴリズムから量子ハードウェアに至る量子コンピューター研究開発全体を強化する必要がある。現在のデジタルコンピューターの構成から推測すると、エラー耐性量子コンピューターの実現に必要となるハードウェア・ソフトウェアの技術スタックは図 1.1 の右端の構造になると考えられる。一方で、後述するように、量子コンピューターの現状は、アルゴリズムをハードウェアにアセンブラで書くような、さながら現代のコンピューターの 1950 年代の様相である。

このような状況の中、（1）古典・量子ハイブリッドアルゴリズムの開発・実装・実証、

[2] 実際の量子アニーラーでは、量子アニーリングとは異なる物理現象で計算が行われているようである。また、理論的には、横磁場イジングモデルを用いた量子アニーリングには量子性による計算加速は無いとされている。

（2）量子ソフトウェア開発環境の整備、（3）量子誤り訂正符号に基づく量子コンピューターアーキテクチャ設計、を進めることが重要となる。エラー耐性量子コンピューターと NISQ 量子コンピューターでは、その計算機システムの構造が大きく異なる（図 2.4）ことから、重要な研究開発課題の位置づけはそれぞれで異なる部分もある。（1）は主に NISQ 量子コンピューターでの実行を主眼とする量子アルゴリズムについての短中期的な研究開発テーマ、（2）は主に NISQ 量子コンピューターの利用促進やハードウェア開発を念頭にした研究開発要素であるが、論理レベルでの成果の多くは大規模なエラー耐性量子コンピューターでの利用もスコープに入ってくる。（3）は主に量子誤り訂正符号とそのハードウェア・ソフトウェア的な課題をアーキテクチャ設計として解法を探るもので、エラー耐性量子コンピューターの実現に向けた中長期的な課題を多く含む。それぞれについて、具体的な研究開発項目を以下に述べる。

（1）古典・量子ハイブリッドアルゴリズムの開発・実装・実証

量子ハードウェア技術の開発は明らかに重要だが、現時点ではその潜在的な応用可能性はあまり明らかになっていない。特に、50 ～ 100 量子ビット程度の小中規模の量子コンピューターを、どのような計算の、どのような部分に用いるのが最も効果的であるかは、それほど自明ではない。したがって、中規模の量子コンピューターの恩恵を受けられる問題・用途の探索・発見、そのためのアルゴリズム開発、そして概念実証が急務である。このような試行錯誤の中から、NISQ 量子コンピューターで計算するにふさわしい、キラーアプリケーションが判明してくると考えられる。現在のところ、その候補として量子化学計算や機械学習に世界的な注目が集まっているが、それ以外にも、アナログ性（連続量）を活かした計算や量子センサーや量子通信との融合を図る応用が見つかる期待もある。ここには、量子超越の実証のための量子アルゴリズム開発も含まれる。誤り耐性量子計算に

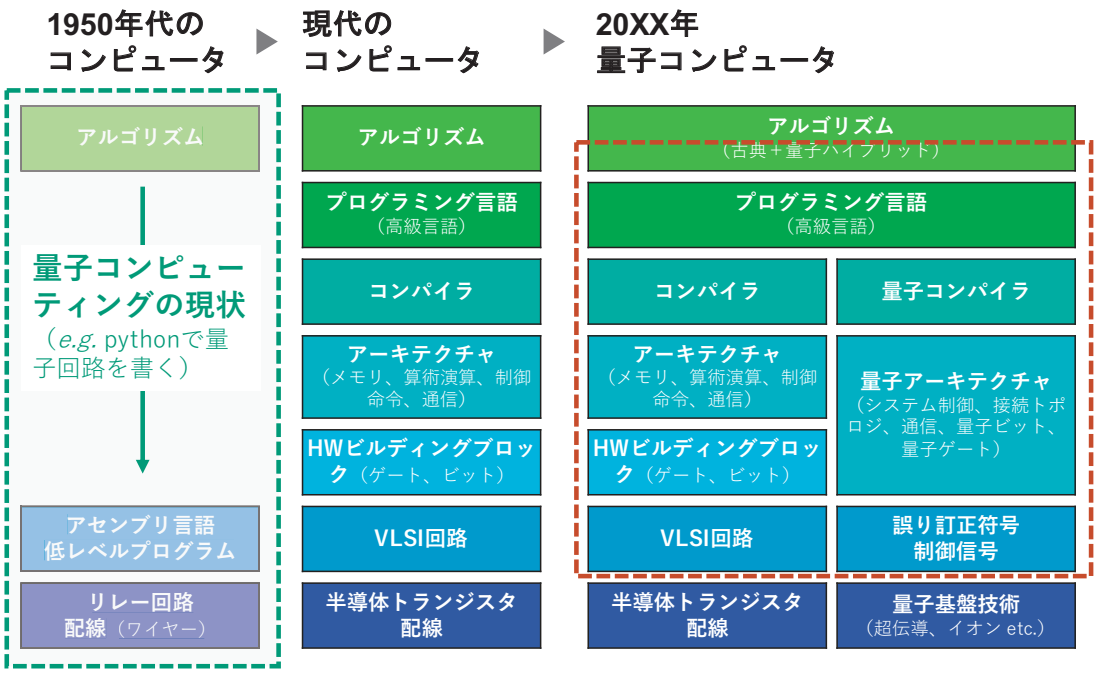

図 1.1: 量子コンピューターの技術スタック（文献 [13] より抜粋・和訳して CRDS 作成）

上位互換可能な近似量子計算アルゴリズムの研究開発も、中長期的な視点から重要である。

（2）量子ソフトウェア開発環境の整備

このようなキラーアプリを探索するためには、ソフトウェア開発プラットフォームによってこの流れを強力に支援することが必要である。量子プログラマが自由に量子プログラムを作成し、古典のプログラムと組み合わせることでさまざまなソフトウェアを開発できるような環境整備が必要である。ここには、量子化学計算や機械学習のプログラミングを助けるフレームワークやライブラリ、量子プログラムの動作を検証するデバッグツール、量子コンピューターの様々な抽象度レベルでのシミュレーションとそれを用いたリソース推定・最適化、実際のハードウェア構成を適切に論理レベルに持ち上げるハードウェア記述言語、など多岐に及ぶ。これらの全てのソフトウェア要素を、１つの研究室や１つの研究プロジェクトでフルスタックで開発するのは困難であるため、オープンソースも最大限に活用した開発が重要となると考えられる。

（3）量子誤り訂正符号に基づく量子コンピューターアーキテクチャ設計

ハードウェアとソフトウェアをつなぐアーキテクチャレベルの研究強化も不可欠である。量子化学計算や機械学習計算などについて、いくつかの既存の有望な量子アルゴリズムを念頭にした計算機アーキテクチャの最適化に向けた取り組みは最低限必要である。また、従来のコンピューターの CPU やメモリなどと量子プロセッサー部分とのインターフェースの最適化などマイクロアーキテクチャの研究開発、誤り訂正符号処理を含む量子ビットの制御・測定にかかるアナログ・デジタル変換の高度化・高速化、そのためのソフトウェア（ミドルウェア、ファームウェア）開発、1000 量子ビット以上へのスケールアップに向けた本質的な設計の探索、などハードウェアとソフトウェアに跨った挑戦的な研究課題を丁寧に解決してゆく必要がある。

1.3 推進方法

これまで、量子コンピューターを擁する量子情報処理分野は科学技術分野としては物理学・応用物理学の一分野として成長を続けてきた。これからは、分野融合・企業参画・国際連携それぞれの局面で様々なプレーヤーがそれぞれ必要とされる役割を担う“みんなの”量子コンピューター研究開発が重要となる。つまり、知見、技術、人材など量子コンピューター実現のために必要となるあらゆることを、学問分野や所属の壁を越えて交流することがカギとなる。どのプレーヤーも必要な技術や人材をフルスタックで用意するのは困難であるからこそ、海外の研究チームまで含めた共同研究やオープンソースの積極活用などの形で、不足する部分を補うことも必要である。

これまで量子コンピューターに関わりが無かった人たちが、ある程度気軽に量子コンピューターに触れるようになると、今まで誰も考えつかなかった使い方が発見される可能性も十分にある。従来の物理的な価値の方向だけではなく、ファッション、ゲーム、デジタルメディア、音楽、映画などの情緒的な価値をも追求することで、新しい量子アプリケーションが生まれることが期待される。

今後 50 年の間には、量子コンピューターだけでなく、量子センサーや量子インターネッ

トなどの量子情報処理技術と組み合わせた「量子 ICT」を自由自在に使いこなす時代が確実に訪れる。その中では、本プロポーザルで取り上げた機械学習や量子化学計算の進展だけでなく、新たな量子サービスや未だ見ぬ量子産業の創出が行われると同時に、量子 ICT を使った科学研究や科学的発見も行われるはずである。量子コンピューター研究開発を強力に加速・推進することで NISQ 時代を早期に通過し、量子 ICT 時代へ向けて、スケーラブルなエラー耐性量子コンピューター実現への確固たる一歩を、我が国が世界に先駆けて進めるべきである。

量子コンピューター研究開発ネットワークとハブ拠点

量子コンピューターの研究開発にはハードウェアからソフトウェアに至るまでの必要な全ての技術をフルスタックで用意することが重要となるが、それらに関わる機器や人材を物理的に１ヶ所に集合させることは現実的ではない。したがって、多様な研究開発拠点やチームから成る量子コンピューター研究開発ネットワークを構築するとともに、その効果的・効率的な連携・協調動作のためのハブとなる拠点も複数必要となる。

量子ソフトウェア研究開発ハブ、プラットフォーム運営・提供ハブ、教育・訓練ハブ、海外の有力研究者の日本国内の研究者を取り次ぐ国際連携ハブなど様々な種類のハブ拠点を、それぞれの機能に合わせて、大学や公的研究機関に設置することが望ましい。

その上で、量子情報処理の教育・訓練プログラムの開発・提供、正確で積極的なアウトリーチ・科学広報活動、スピンアウトする量子スタートアップ企業の積極的支援など、多様な施策により、持続性あるネットワーク構築が求められる。

コミュニティ・エコシステムの醸成

研究開発プロジェクトや研究開発ネットワークの成功は、量子コンピューターコミュニティに登場するプレーヤーの充実と、それらがエコシステムを形成して様々な役割で機能することにかかっている。計算機科学・物理学・数学・電子工学に跨がった研究者・技術者のコミュニティは萌芽期であり、多分野連携・産学連携・技術レイヤ連携を可能とする研究開発・人材育成の拠点形成を念頭にした政府投資により、コミュニティ形成・エコシステム形成を強力に促進することが不可欠である。

とりわけ量子ソフトウェアにおいては、学術的な量子ソフトウェア研究者と産業界との多くの共同作業が急務と思われる。学術研究者は量子コンピューター利用にメリットがある現実の問題の種類について理解を深める必要がある。量子コンピューティング分野に進出してくる産業界の研究者・技術者は、エコシステムの中での学術研究者との交流から、量子コンピューターの可能性と限界の両方をよりよく理解し、その経験を活かして、量子コンピューターを含む量子 ICT 分野での短期的または長期的な投資判断を下すことが求められる。

量子誤り訂正符号の方式や量子デバイスにはまだ決め手はなく、このエコシステムは当面は多様化が進むと思われる。NISQ 量子コンピューターの未だ見ぬキラーアプリケーションの発見があればエコシステムに大きな波を立てることは必至である。我が国の存在感の向上とともに、産業競争力の強化に向けて、知財化、IP コア化、パテントプール化、オープン化、国際標準化などの戦略的取り組みを駆使して臨むべきである。

量子コンピューター教育・訓練

研究推進上の課題の 1 つは、量子ソフトウェアの作成・開発の訓練を受けた人材の不足である。量子ソフトウェアのプログラミングには、波の干渉や重ね合わせなど古典的プログラミングとは根本的に異なる部分があり、ルールに慣れた人材の養成が、量子コンピューターが社会にもたらすインパクトの大小を握っている。

現在の人材プールは小さいため、大学と企業の両方で教育・訓練プログラムを開発してゆく必要がある。教科書、大学での講義、オンラインコースのほか草の根的な勉強会など初動は開始されているが、量子コンピューティングや量子ソフトウェアのための学術・産業でのカリキュラムはまだ未熟な段階と言える。また教科書やオンラインコースだけでなく、ハンズオンのトレーニングプログラムも必要である。ただし、カリキュラムに固定して広く高等教育を進めるまでには成熟しておらず、研究開発と同時並行での人材育成が重要である。

今後 50 年の間には、量子コンピューターだけでなく、量子センサーや量子インターネットなどの量子科学技術と組み合わせた「量子 ICT」を自由自在に使いこなす時代となる。従って、高度な基礎科学的成果を理解し、それを起点にしながらも量子システムとしてインテグレーションして価値形成できる量子アーキテクト人材の育成をすぐにでもスタートしなければならない。そのような人材育成は、「我が国の大学で実行する」ものと、「一人でも多くの日本人を世界に飛立たせる」ものの 2 本立てで実行すべきである。

今後も成長を続ける量子技術産業の中での仕事に適した教育・訓練プログラムを開発するためには、学界と産業界が互いに協力しなければならない。これにより、量子技術の品

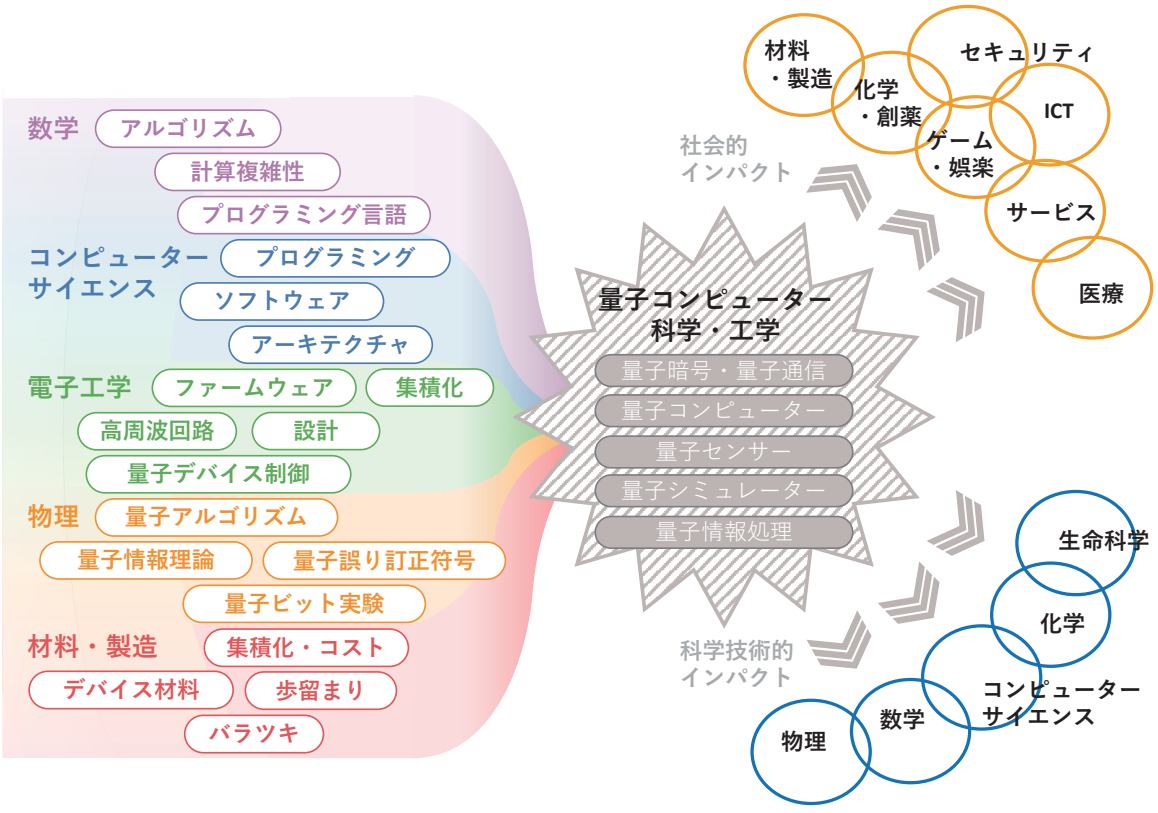

図 1.2: 量子コンピューター科学・工学のインパクト

質管理、ソフトウェアエンジニアリング、コンサルティングなどに必要となるスキルが明らかになるとともに、その品質基準を確実に満たすようになると期待される。量子 ICT 技術者を必要とする組織とそれらを教育できる組織との間での緊密な連携が、長期的な視点からも必須である。

2．研究開発を実施する意義

2.1 現状認識および問題点

2.1.1 ムーア法則の終焉、人工知能計算要求の高まり

半導体技術は微細化により性能向上とコストダウンを同時に達成し、コンピューターは私たちの豊かな暮らしを支える基盤となってきた。しかし、２年で２倍の性能を達成するような指数関数的な性能向上「ムーアの法則」が技術的・経済的な限界を迎えつつあると言われ、トランジスタ数のみに頼る性能向上は近年急速に飽和している。その一方で、IT 分野では人工知能・ビッグデータが大きな潮流となり、高効率の計算要求は高まるばかりである。

この中で、ドメイン志向アーキテクチャの考え方が注目されている [1, 14]。その代表例は、GPU（Graphic Processing Unit）である。GPU はもともと画像処理専用プロセッサーであったが、その並列性を活かして大量の積和演算を含む多層のニューラルネットワークの学習（深層学習）を可能にすることがわかり、近年ではニューラルネットワーク計算に特化した専用のチップも登場した。このほかにも、並列計算、ビッグデータ処理、画像処理、データベース処理、メディア処理、最適化問題など、様々な計算ドメインに特化したアーキテクチャ提案が行われている。

コンピューターの歴史を紐解けば、CPU の性能が未発達であった時期に、浮動小数点演算を別に高速処理するようなコプロセッサも存在し、汎用機では必要な性能が得られにくい場面での専用機利用は常套手段である。しかし、このようなドメイン指向アーキテクチャが現在ことさら脚光を浴びているのは、ムーアの法則による性能向上に陰りが見える中で、トランジスタ数のみに頼らない性能向上手法が必要となったためである。

このように、コンピューター科学の文脈において量子コンピューターは、半導体微細加工のみに頼る性能向上の行き詰まりと、急速に増加・多様化する計算ニーズとの間で、飛躍的な計算性能向上の糸口になるものの１つと認識されている [3]。同時に、量子コンピューターの要素技術が確立されつつあり、IBM、Google、Microsoft、Intel などの企業が相次いで開発に乗り出してきたことが、システム・情報科学技術分野における量子コンピューターへの期待感を高めていると言えよう。

2.1.2 量子コンピューターのブーム

量子コンピューターの研究開発は重要局面を迎えている。超伝導回路の最近の研究進展は、エラー耐性量子コンピューターの実現を期待させ、世界的に研究開発投資が過熱している [4, 5, 6]。しかし、素因数分解や検索などの高度な量子アルゴリズムが必要とする数 10 億量子ビット [1] などという大規模なハードウェアは、今後 10 数年では到達できないと認識されている [13]。

量子コンピューターの歴史は、1980 年に Benioff がエネルギーを消費しない量子計算の可能性を示唆したことに端を発し、1982 年に Feynman が量子計算の有効性を提示、1985 年に Deutsch が量子チューリング・マシンを考案したことにより、多くの物理学者

[1] Shor のアルゴリズムによって 2048 ビットの数の因数分解を行うのに必要な量子ビット数は 60 億ほどと見積もられている [15]。量子誤り訂正まで含めて 1MHz のクロック周波数で駆動できた場合、2048 ビットの数の因数分解は数日で完了できる。

や計算機科学者が量子コンピューターに注目し始めた。1994 年に Shor から因数分解アルゴリズムが提案される頃には第 1 次ブームのピークを迎えたが、誤り訂正の克服が難しいことから量子コンピュータ実現への見通しは明るいものではなかった。Calderbank、Shor、Steane らによって Calderbank-Shor-Steane（CSS）符号と呼ばれる具体的な量子誤り訂正符号も提案され、2000 年代にかけて世界中で量子コンピュータ研究が活発化する駆動力の一端を担った。当時 NEC の中村・蔡らによる固体素子での量子ビット実現もこの時期である。誤り訂正符号がハードウェアに要求する量子ビット数・エラー率は非現実的な値であり、スケールアップの技術的な見通しの悪さからブームは次第に下火となった。

現在の量子コンピューター研究の主眼は、量子誤り訂正符号の実装と、中規模の量子コンピューターの実現である。また、その中でハードウェア的な実現可能性が見えてきた（誤り訂正符号の実装がない）NISQ 量子コンピューターを、試行的に利用する動きも見られる。全体としては、量子誤り訂正符号の実装は究極のゴールであるエラー耐性量子コンピューターに至る重要なメルクマールとされている。現在のところ、最も研究が進んでいる超伝導量子ビットとイオントラップの系は、図 2.1 にある量子コンピューター開発の 7 段階中の第 4 段階目にあたる量子誤り訂正符号の実装の段階にあるといえよう[16]。スティーン符号、表面符号、猫符号などの様々な方式の量子誤り訂正符号の実装に向けた研究開発が進められている。コンピューターアーキテクチャの観点では、量子誤り訂正符号化が論理量子ビット制御と物理量子ビット制御を分ける境目となっており、量子コンピューターのアーキテクチャ設計を左右する重要な要素である。エラー耐性量子コンピューターと NISQ 量子コンピューターの技術スタックの違いは、図 2.4 で改めて触れる。

量子誤り訂正の方法は様々な提案があるが、量子ゲート操作のエラー率があまりにも大きいと、誤りを検出・訂正するまさにそのゲート操作でエラーが発生してしまい、効率的にシステム全体からエラーを取り除くことができなくなってしまう。2000 年代に入って、新しい誤り訂正符号がいくつか発見され、当初 0.001% しか許されなかった誤り閾値は 1% 程度まで緩和された。エラー耐性量子コンピューター開発の技術的ハードルの高さが認識される中、2011 年「世界初の商用量子コンピューター」を謳ったマシンを D-wave

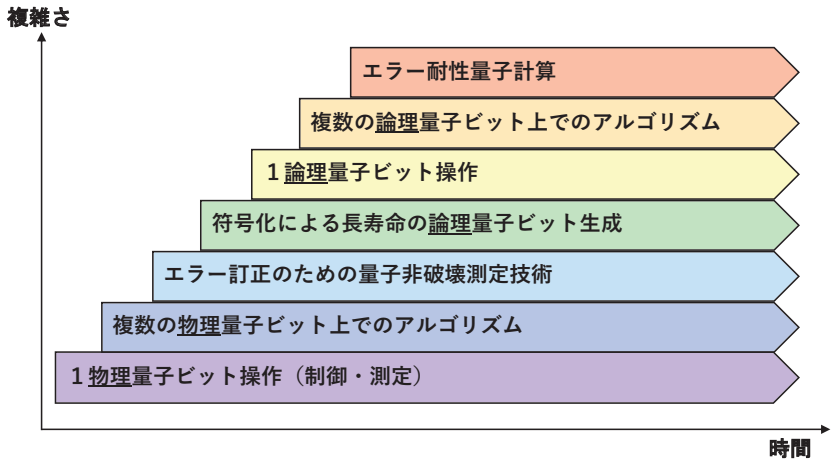

図 2.1: エラー耐性量子コンピューター開発の７ステップ（文献 [16] より抜粋、和訳して CRDS 作成）

Systems 社 [17] が発表、Google や NASA などが購入して試験をすると、にわかにブームが再燃した。これまでの量子回路型（ゲート式）とは異なる計算原理であったが「量子コンピューター」として売り込まれたので、一部で誤解が広がった。

ゲート式の「量子コンピューター」での第 2 期のブームの火付け役は米国カリフォルニア大学サンタバーバラ校（UCSB）の Martinis のグループである。彼らは 2014 年に直列結合の 5 量子ビットデバイスで、1 量子ビットゲート忠実度 99.92%、2 量子ビットゲート忠実度 99.4%、測定忠実度 99% という高い忠実度（＝低いゲートエラー率）の基本量子ゲートを実現した [18]。

このブレークスルーはこれまでの超伝導量子ビット開発の長年の蓄積によるところが大きい。超伝導量子ビットの寿命（コヒーレント時間）は、電荷雑音対策、共振器による電磁場モード閉じ込め、動的デカップリング、表面・界面効果の希釈などの様々な技術により、この 20 年弱で 5 桁も良くなった。

Martinis らが示した忠実度の値は、表面符号による量子誤り訂正に必要なエラー率の閾値を満たしており、このまま系を大規模化できれば、理論上はエラー耐性量子コンピューターが実現できることを意味していた。このことが、研究者や投資家が抱いていた量子コンピューターの実現性に対する心理的バリヤを取り除いたようだ [4]。この論文が発表された同年に、Google 社が Martinis のグループを丸抱えする形で研究支援することが第 2 期のブームに火をつけた。量子ビットの実装方法は複数の方法があるが、ゲート忠実度とゲート速度の観点で有望視されているのはゲート忠実度に優れるイオントラップ、ゲート速度に優れる超伝導回路である（図 2.2）。

第 2 期のブームは、理論・実験ともに「量子コンピューターをいかに作るか」という工学的なフェーズに入ったことが特徴である。Google、IBM、Microsoft、Intel などの米国の IT 企業が研究開発投資を拡大し、Rigetti、IonQ、1QBit などのスタートアップも次々と立ち上がった。ハードウェア技術としては、超伝導回路やイオントラップが先行してい

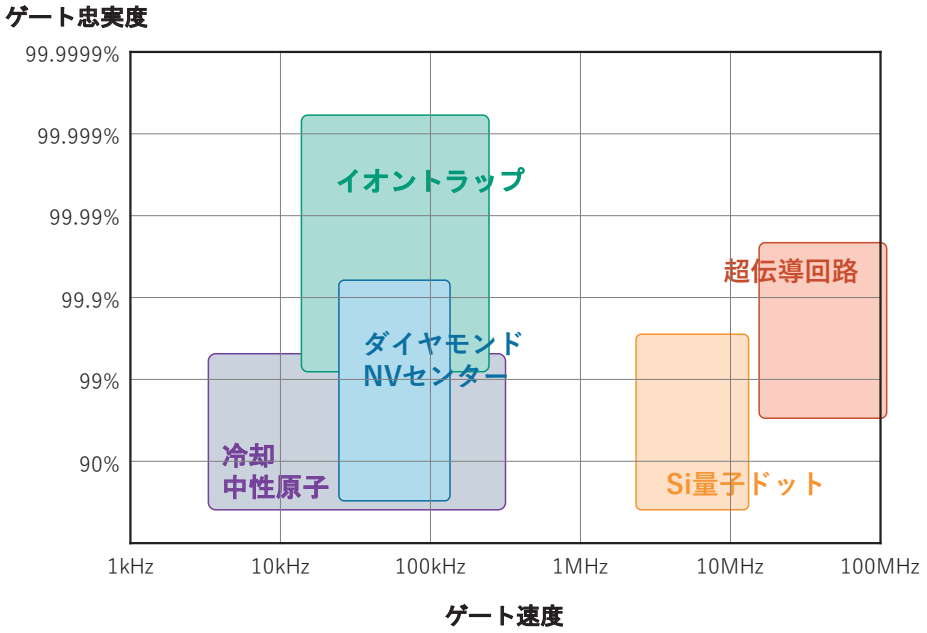

図 2.2: 量子ビット実現手法の比較

るが、大規模化への技術的なハードルは依然として高いと認識されている。

ソフトウェアやアーキテクチャの重要性が再認識され、ISCA（International Symposium on Computer Architecture） や MICRO（International Symposium on Microarchitecture）などのコンピューター科学分野のトップカンファレンスでの、量子コンピューターに関する招待講演やチュートリアルも増えている。シミュレーターによって量子コンピューティングを気軽に試せるソフトウェア開発環境もオープンソースなどで提供され、裾野が拡大していることも近年の特徴である。マサチューセッツ工科大学(米)、デルフト工科大学（蘭)、慶應義塾大学などでは、量子コンピューターに関するオンラインのコース提供も始まった。

究極の目標であるエラー耐性量子コンピューターに至る研究開発には、まだ無数の紆余曲折が待ち受け、ソフトウェア・ハードウェアとも多くのブレークスルーが必要である。このような中、ハードウェアとしての実現可能性が見えてきた NISQ 量子コンピューターが、理論・実験の両側面で量子コンピューター研究を活性化させている [9, 10]。エラー耐性量子コンピューターと NISQ 量子コンピューターはスケールも計算機システムとしての構造もかなり異なっており、エラー耐性量子コンピューターに至る中長期的な道のりの中に、NISQ 量子コンピューター研究開発をどう位置づけるかは、まだ研究コミュニティーの中でも定まっていないように見受けられる。

2.1.3 量子技術への政府投資の拡大

量子コンピューター、量子シミュレーター、量子暗号、量子通信、量子センシングなど、一連の量子技術に各国が競うように政府研究開発投資を行い、研究開発を進めている状況である。米国、欧州、中国ともに、科学技術政策として量子技術を重点分野とする位置づけが明確であり、かつ、具体的な施策として推進に積極的な姿勢を見せている。これらの国は多くは、量子技術に関係する複数の研究拠点を設立・支援する計画をもち、大型で５年以上の支援期間をもつ研究グラントや研究プロジェクトを推進する方策をとる（表 2.1)。

米国

米国では 2009 年に国家科学技術会議 (NSTC) が「A Federal Vision for Quantum Infor-mation Science」を公表し、それを受ける形で全米科学財団 (NSF) が「量子情報科学における学際的研究プログラム」（年間 400 万ドル（2015 年)、1 件あたり数千万円規模のグラント）を開始した。NSF が 2016 年 8 月に発表した「NSF が未来に向けて投資すべき 10 のビッグアイデア」の 6 つの「研究アイデア」のうちの 1 つが「Quantum Leap（量子飛躍)」であった。4 つの「プロセス・アイデア」のうち 1 つは「NSF としてのコンバージェンス研究の拡大」であったことを受け、2017 年 8 月にコンバージェンス研究関連の支援領域として「量子飛躍」が設定され、3 課題がまず採択された。

以降も「量子飛躍」領域の公募は続いて発表され、「量子システムにおける革新的な進歩」や「量子通信のための統合プラットフォーム」などがテーマとなっている。量子コンピューターの量子化学への適用については、2016 年秋に行われた「化学のための量子情報・量子計算」ワークショップを踏まえて EAGER (EArly-Concept Grants for Exploratory Research) プログラムを通じて量子飛躍の公募をかけ、10 の topic areas が示されている。

2018 年 6 月には、量子コンピューティング研究を促進するコンソーシアムを設立する法案と、「国家量子技術イニシアティブ (National Quantum Initiative)」を立ち上げて量子技術に関する研究所の新設や研究プロジェクトの推進を図る法案の 2 つの法案が提出された。量子科学技術分野において、米国が他国（とりわけ中国を意識して）の後塵を拝してはならないという強い危機意識がある様子が見て取れ、連邦議会を通過する見通しである。イニシアティブは、各種のプロジェクト間の協調強化や、大企業やスタートアップの投資促進、米国の労働者の量子コンピューティング技能向上の支援など、多岐にわたる方策を含んでいる。

欧州

欧州では、オランダのデルフト工科大学に 2013 年に QuTech センターが開設されたのを契機とし、呼応するようにオランダ政府は翌年「量子技術」を科学技術外交における４つの「National Icon」の一つに位置づけ、研究イニシアティブとして大規模な政府投資を行うことを発表した。QuTech センターは、Microsoft や Intel などと共同研究を行うなど産業連携も熱心であり、欧州の量子科学技術研究の中心的なプレーヤーとして注目されている。オランダは半導体露光機のトップメーカー ASML 社を、隣国のベルギーは研究開発機関 IMEC を擁し、Samsung や Intel 等のユーザーと共に最先端の技術開発を行っており、その地位を欧州外に奪われてはならないとの意識もある。2016 年、QuTech センターの研究者を中心とした多数の研究者により「Quantum Manifesto」が発表され、それに応じる形で欧州委員会は Horizon2020 の枠組みの中で「Quantum Technology Flagship」事業による大規模な研究支援を 2018 年からスタートすることを決めた。

中国

中国では、科学技術に関する基本政策である「国家中長期科学技術発展計画綱要 2006 ～ 2020 年」において、重大科学研究の 1 項目として量子制御が位置づけられているほか、「第 12 次五カ年計画 (2011 ～ 2015)」においても、量子情報処理、量子シミュレーション、量子通信および情報セキュリティが重要な領域に指定された。2015 年には、中国科学院 (CAS) が IT 企業の Alibaba と共同で「量子計算実験室」を設立し、開発した量子コンピューターをクラウド提供するなど活発な研究開発を進めている。2017 年に、国の重点投資として合肥市に国営量子情報科学研究所を建設中で、2020 年には開設予定と発表、翌年 1 月には、人民解放軍の軍事科学院が、120 名の人工知能分野と量子技術分野の科学者を集めたと発表した。

日本

我が国では、量子情報処理を含む量子技術は、「ナノテクノロジー」や「ライフサイエンス」などの分野に組み込まれた個別のプロジェクトとして散発的に研究開発が進められてきた。「第４期科学技術基本計画」では「III. 2.（５）科学技術の共通基盤の充実、強化」の項に「光・量子科学技術」が、「第５期科学技術基本計画」では「第２章（３）「超スマート社会」における競争力向上と基盤技術の戦略的強化」の項の「新たな価値創出のコアとなる強みを有する技術」の一つとして光・量子の記載が散見されるものの、中長期的な展望にもとづく政策的な後押しによって量子技術を一体的に進めては来なかった。

2017 年 8 月に文部科学省量子科学技術委員会が「量子科学技術（光・量子技術）の新たな推進方策」を発表。「超スマート社会」における新たな価値創出のコアとなる強みを有する基盤技術として、量子情報処理、量子計測・センシング、極短パルスレーザー、次世代レーザー加工を重視する推進方策を打ち出した。

ファンディングプログラムとしては、文部科学省「光・量子飛躍フラッグシッププログラム（Q-LEAP）」が 2018 年に発足したほか、JST の CREST「量子状態の高度な制御に基づく革新的量子技術基盤の創出」、さきがけ「量子の状態制御と機能化」領域が発足し、公募による競争的研究資金の提供が進められた。これまでのところ、採択されたプロジェクトはハードウェア志向のものが多い。ソフトウェアに注目したプログラムとしては、IPA 未踏ターゲット事業が「アニーリングマシン」「ゲート式量子コンピュータ」の 2 部門でのソフトウェア開発人材の育成を進めている。

2.1.4 量子コンピューティングエコシステム

量子コンピューターの産業利用の試みや、ソフトウェア・ハードウェアのスタートアップ企業の動きも活性化している。米国では QC Ware 社と NASA の共催で「Q2B:

表 2.1: 量子技術関連政策

	政策文書での位置づけ	取り組み状況（予定も含む）
米国	国家科学技術会議の下のWGがレポート発表。米国の科学的リーダーシップ、国家安全保障、経済的競争性を構成する重要技術として**量子センサ、量子通信、量子シミュレータ、量子コンピュータ**を特定（2016.7）。	量子コンピューティング研究法（国防省コンソーシアム設立）、10カ年国家量子イニシアティブプログラム（DoE, NSF, NISTでグラント、研究センター新設など）の 2 法案が提案されている。 （National Quantum Initiativeの内訳） Quantum Innovation Labs ＞500億円 Quantum Research Network ＞200億円 Quantum Computing Access Program ＞100億円
欧州	欧州委員会の求めに応じ、ロードマップ「Quantum Manifesto」を産官学でとりまとめた（2016.5）。長期にわたる富の創出、安全保障、産業創出の観点で**量子通信、量子コンピュータ、量子シミュレータ、量子センサ・計測**が 4 つの柱。	•Quantum Technology Flagship （>1250億円、10年）プロジェクトを2019年より開始予定。 •イギリスは大型プロジェクト「UK National Quantum Technologies Programme」で総額270Mポンド（～456億円）を 5 年計画で実施（2014.2～）。
中国	科学技術イノベーション第13次五カ年計画（2016）の重点分野として、**量子通信、量子コンピュータ、量子制御、量子情報**を指定。重大科学技術プロジェクト、基礎研究強化などにそれぞれ位置づけた。	•「量子情報科学国家実験室」を安徽省合肥市に現在建設中。2020年完成予定。約70億元（～1190億円）。 •「国家重点研究計画」で量子制御・量子情報の基礎研究の大規模グラントを実施中（＞3 億円・5 年/チーム）。 •CAS-Alibaba Quantum Computing Laboratoryを設立最初の5年間で3,000万元/年（～5 億円/年）の投資。
日本	文部科学省 量子科学技術委員会が「量子科学技術（光・量子技術）の新たな推進方策」を発表（2017.8）。超スマート社会（Society 5.0）における新たな価値創出のコアとなる強みを有する基盤技術として**量子情報処理、量子計測・センシング、極短パルスレーザー、次世代レーザー加工**を重視。	•「光・量子飛躍フラッグシッププログラム（Q-LEAP）」の公募開始（3～4 億円/年 x 最大10年・6 PJ）。

Quantum Computing for Business」というワークショップが開かれ、産官学の真剣な議論も行われた [19]。Google、IBM、D-wave のほか、NIST（国立標準技術研究所）、LBL（ローレンス・バークレー国立研究所）などの国立研究所も参加し、EU や中国でのファンディングの取り組みも紹介された。

NISQ 量子コンピューターでは、IBM が実機での量子プログラムの実行も可能なプログラミング環境をクラウド公開し、注目されている。計画当初からクラウドでの公開を念頭に開発を進め、エラー率や結合性などハードウェア的な制限があるものの、現在では 16 量子ビットまでの実機（IBM の研究所に設置されている）に誰でもアクセス可能である。このように、機能は限定的であっても量子コンピューターが一般公開されることで、アルゴリズム研究やプログラム開発が促進されると期待される。実際、IBM Q System の利用者は合計 7 万人以上と報告されている [20]。有料のコミュニティ Q Hub もスタートし、大学やユーザー企業とのネットワークを構築し、産業応用の可能性を探索している。日本から慶應義塾大学が名乗りを上げ、2018 年に同大学に量子コンピューティングセンターが開所した [21]。

NISQ 量子コンピューターも量子アニーラーも、超伝導量子ビットの利用は希釈冷凍機環境が必須であり、実機をユーザーの手元に置くような提供の仕方は現時点では想定されていない。ユーザーに関する情報も手に入るため、各社とも API（Application Programming Interface）利用によるインターネット越しの量子コンピューターを利用できるプラットフォームを展開する戦略である。ビジュアルなプログラミング環境、トレーニング教材、ユーザーコミュニティの提供など、ユーザーの参画の敷居を下げる努力がなされている。

量子コンピューター関連のスタートアップも多数生まれており（表 2.2）、Y Combinator や Google Ventures などのベンチャーキャピタルからかなりの額の投資が集まっている。大学発の知財を持ち大学教授が CEO や CTO を兼ねるなど技術基盤を有するものもあり、人材獲得にも余念がない。ゲート方式の代表的なハードウェアスタートアップとしては超伝導量子ビットを利用する Rigetti Computing やイオントラップ方式の IonQ などがある。ソフトウェア関係では、QC Ware、1QBit、Zapata Computing のような量子ソフトウェア開発企業の他、Quantum Benchmark や Anyon Systems などツールを提供する企業も現れ、シリコンバレー的な空気感とスピード感が流れ始めている。エコシステムの中心にいるのは Google や IBM である（図 2.3）。我が国では、MDR や QunaSys といったスタートアップが量子コンピューター利用プラットフォームの開発や勉強会の開催など、コミュニティ拡大に精力的である。

2.1.5 コンピューターサイエンスから見た量子コンピューター開発の現状

量子コンピューターの研究開発成果の発表の中心となる学会は、米国物理学会（American Physics Society, APS）である。2002 年に発足した量子情報に関する Topical Group はメンバーの増加を続け、2017 年には Division に格上げとなった [22]。多くの研究成果は Nature や Science のほか物理系のジャーナルでの発表が主となる。Martinis らによる 5 量子ビット系の発表は、量子コンピューターは物理の問題ではなく、工学的なチャレンジへと移行したことを象徴としていたが、IEEE や ACM 関連の国際学会での量子コンピューターに関する発表はまだ少数である。

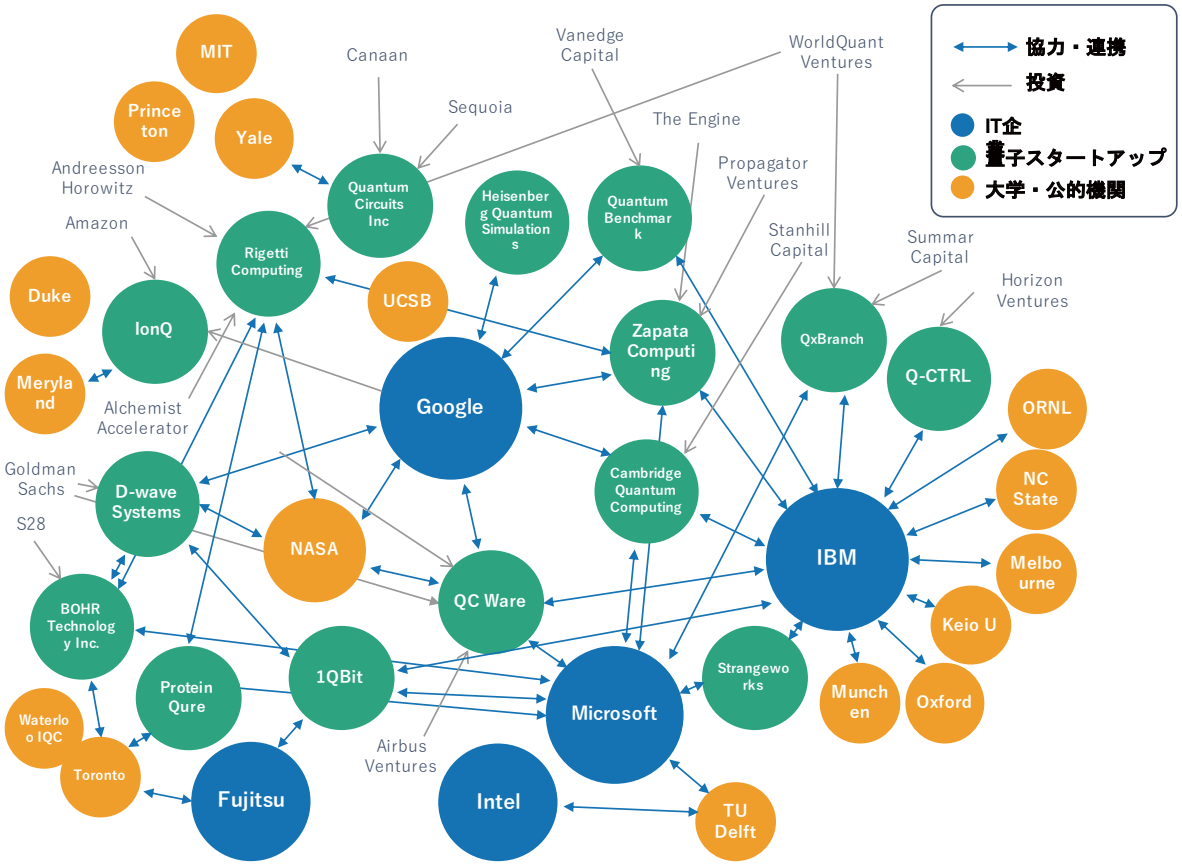

図 2.3: 量子コンピューティングエコシステム

表 2.2: 量子コンピューター関連スタートアップ

	ハードウェア	ソフトウェア	サービス、要素技術
米国	Rigetti Computing, IonQ, qci, brane, Optalysys, Qubitekk, FATHOM	QC Ware, Qbrick, QxBranch, QBI Logic, Zapata Computing	Nano mate, Photon Spot, Eagle Power Technologies, Quants, MagiQ
カナダ	D-wave Systems	1QBit, evolution Q, ISARA, ANYON, Artiste-qb, Quantum Benchmark	NQCG, SPARROW QUANTUM, Quantum Inventions
欧州		CQC, nextnano, SEQURENET, IDQ, Post Quantum, Heisenberg Quantum Simulations, Cambridge Quantum Computing	
中国	Alibaba Cloud	QuantumC Tek	
オーストラリア	Silicon Quantum Computing	Quintessence	
日本		QunaSys	MDR

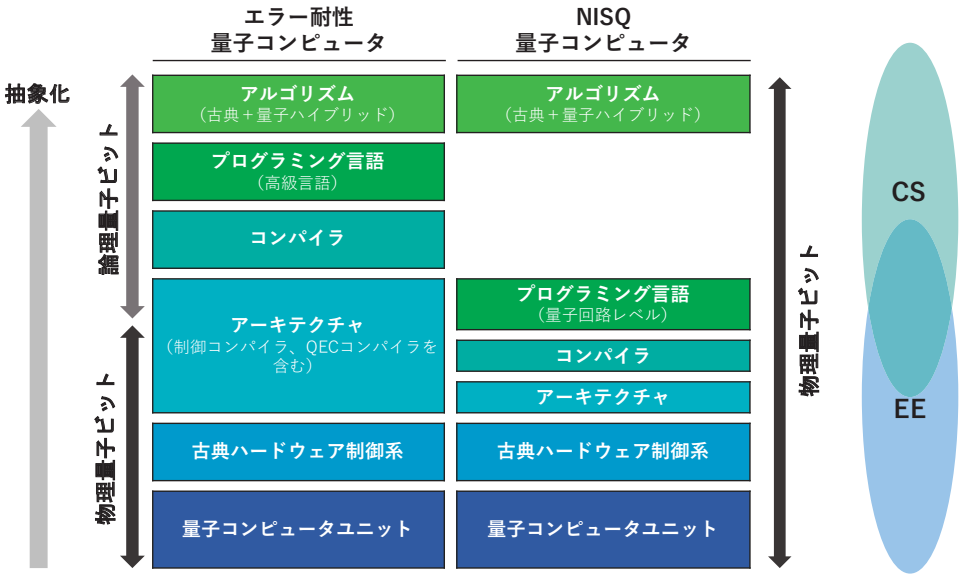

図 2.4: エラー耐性量子コンピューターと NISQ 量子コンピューターの構成の違い

ここでは量子コンピューターの研究開発動向を、アルゴリズム・理論から量子ビットハードウェアに至るまで、現代のコンピューター技術スタックに沿って上から下にレイヤごとに見てゆく。

量子アルゴリズム・量子情報理論は研究の蓄積も多く、極めて豊穣な世界となっている。現在までに提案されている量子アルゴリズムの代表的な例を表 2.3 にまとめた。エラー耐性量子コンピューター向けには多数の量子アルゴリズムが提案され、米国 NIST は古典アルゴリズムより高速になるような量子アルゴリズムを集めたウェブサイト「Quantum Algorithm Zoo」を公開している [8]。2018 年 7 月現在でおよそ 60 種類の量子アルゴリズムが紹介されている。

近年、NISQ 量子コンピューターでの実行を考慮した新しいタイプのアルゴリズムの提案が相次いでいる。代表例は、Variational Quantum Eigensolver や（VQE）、Quantum Approximate Optimization Algorithm（QAOA）、Quantum Circuit Learning（QCL）などの量子・古典ハイブリッドアルゴリズムである。また、量子コンピューターの優位性[2]を確かめるアルゴリズムも盛んに議論・提案されている。ここで試されるアルゴリズムと古典コンピューターによる計算が困難だと考えられている根拠を表 2.4 にまとめた。サンプリングアルゴリズムは、量子ビットを用いれば効率的に生成できる分布が、古典コンピューターでは効率的にシミュレートできないことを実証しようとするもので、実用的な意味合いは薄いものが多い [10]。前提とする仮定は様々であり、Google グループが実験検証をねらうランダム量子回路は、最も仮定が少なくてすむ（＝強い）方法である [23]。

量子プログラミング言語・量子ソフトウェア開発環境は萌芽的な状況であるが、実機やシミュレーターの開発の進展に伴い、量子アルゴリズムを実装する、ソフトウェア開発キット（SDK）が様々なクラウド・プラットフォームで提供され始めている [20]。ここでは、

[2] Quantum Supremacy。Quantum Advantage とも呼ばれる。

表 2.3: さまざまな種類の量子アルゴリズム

(1)エラー耐性量子コンピューター

アルゴリズム	用途・問題
Shorの因数分解アルゴリズム	因数分解による暗号解読
Groversの検索アルゴリズム	オラクル検索問題、組合せ最適化問題
デジタル量子シミュレーション	量子化学エネルギー準位計算
HHL線形ソルバー（Harrow, Hassidim and Lloyd）	レーダー散乱断面積計算
量子主成分分析（QPCA: Quantum Principal Components Analysis ）	量子データのPCA、量子化学シミュレーション
量子サポートベクターマシン（QSVM: Quantum Support Vector Machine）	量子データを用いたSVM
量子推薦システム（QRS: Quantum Recommendation System）	推薦
トポロジカルデータ分析	データ分析
量子深層学習	制限ボルツマンマシンのネットワークの学習

(2)NISQ量子コンピューター

アルゴリズム	用途・問題
量子近似最適化（QAOA: Quantum Approximate Optimization Algorithm ）	組合せ最適化問題（量子アニーリングとほぼ同じ） 教師なし機械学習
変分量子固有値ソルバー（VQE: Variational Quantum Eigensolver）	量子化学エネルギー準位計算 化学反応率計算
量子回路学習（QCL: Quantum Circuit Learning）	教師あり機械学習
量子ニューラルネットワーク（QNN: Quantum Neural Networks）	教師あり機械学習
変分量子因数分解（VQF: Variational Quantum Factoring）	因数分解

(3)量子アニーラー

アルゴリズム	用途・問題
量子アニーリング	組合せ最適化問題 スケジューリング問題 ２値ポートフォリオ最適化（BPO） Fault Tree Analysis 経路計画問題
ボルツマンサンプリング	量子・制限ボルツマンマシンの学習

表 2.4: 量子スプレマシー（文献 [10] より抜粋、和訳して CRDS 作成）

アルゴリズム	量子コンピューターでの計算	古典計算が効率的に行えないと考えられる理由（仮定）	実験検証	有用性
因数分解	難しい	RSA暗号が破られる	易しい	あり
ボソンサンプリング	易しい	多項式ヒエラルキーの崩壊	難しい	なし
低デプス回路	ほどほど	多項式ヒエラルキーの崩壊	難しい	なし
IQP	ほどほど	多項式ヒエラルキーの崩壊	場合による	なし
QAOA	ほどほど	多項式ヒエラルキーの崩壊	難しい	おそらく
ランダム量子回路	ほどほど	多項式ヒエラルキーの崩壊	難しい	なし
断熱最適化	易しい	不明	難しい	おそらく
アナログシミュレーション	易しい	特異的	難しい	しばしば

開発者がアルゴリズムをプログラムとして書き下し、SDK を用いてそのプログラムを量子回路にコンパイルし、実機やシミュレーターなどのバックエンドで実行して計算結果を得る、という流れとなる。バックエンドが実機の場合には、量子回路は実機の命令セットにアセンブリされるが、この部分は通常はユーザーから見えない。また、シミュレーターはローカルの PC での実行か、クラウド上の計算資源で実行する形態をとる。

代表的なものは、IBM の QISKit[24]、Microsoft Quantum Development Kit[25]、Rigetti Computing の Forest [26]、Google の Cirq、大学ではスイス連邦工科大学の Project Q [27] などがある（表 2.5）。プログラミング言語はとしては Python の拡張や DSL（Domain Specific Language）、独自の言語など多様な状況である。いずれも、シミュレーターを持ち（一部、実機の利用が可能）、コンパイルや最適化のためのモジュール拡張の容易性が考慮されている。既存のハードウェア構成に量子プログラムをマップするためのコンパイラの開発コンテストなども開催された [28]。このほかにも、量子化学計算のライブラリである OpenFermion や量子ダイナミクスのシミュレーション用の QuTiP など、ライブラリも増えてきている。また、Quipper という関数型プログラミング言語の提案もある。

NISQ 量子コンピューターを何らかの計算に単独で使うとは考えにくく、アクセラレーターとしての利用となるため、量子コンピューターの OS は当分想定する必要は無い。量子・古典ハイブリッドのプログラムからサブルーチンとして量子プログラムが実行されることになると考えれば、Python など既存の（古典コンピューターで使用される）プログラミング言語で用意しておくのが再利用性の観点からも合理的な選択であろう。python は比較的人気の言語で、機械学習やデータサイエンス分野のプログラマが量子コンピューター（たとえシミュレーターであっても）を利用するバリアは低いと期待される。一方で、C# に親しんだエンジニアの目には、Microsoft の提案するプログラミング言語 Q# と Visual Studio に統合された SDK が魅力的に映るかもしれない。いずれにせよ、基本的には量子回路をそのまま記述するアセンブリ言語のレベルでのプログラミングが主であり、古典コンピューターでの抽象度の高いプログラミングの状況とはやや距離がある感は否めない。量子ハードウェアから提供される量子性を、プログラマにどの程度の抽象度や粒度で何を見せるかなどは、現在は手探りの状況であり、徐々に整理・洗練されてゆくと

予想される。

量子コンピューターアーキテクチャの概念は、2008 年頃に登場して以来、量子デバイスハードウェアの進展とともにその重要性が高まっている [29]。現在の研究開発の主眼は、量子誤り訂正符号の実装に向けた、スケーラビリティのあるハードウェア構成と、その設計方法論の構築である。誤り訂正符号は論理量子ビットと物理量子ビットの境目になっており、エラー耐性量子コンピューターのアーキテクチャ設計を大きく左右する影響度の高い要素である。アーキテクチャ設計においては、ハードウェア設計に必要となる要素の抽象度や相互作用の決定、リソース推定に基づくトレードオフの最適化、ゲート分解や量子回路の最適化、命令セットアーキテクチャなどの要素も萌芽的であるが研究開発が進められている。

スケーラビリティのあるハードウェア構成としては、光と固体系を組み合わせた誤り訂正モデルに基づくシステム設計の提案や、超伝導量子ビット、イオントラップ、ダイヤモンド NV センターと光など様々なハードウェアプラットフォームでの検討・概念実証が進められている。

NISQ 量子コンピューターは、誤り訂正符号を持たないため、基本的には量子チップのデバイス構造や特性そのものがソフトウェア側から見えているような状態である。量子ビットのレイアウト・結合は、一般には量子ビットどうしの結合性が高い方がより複雑な問題を扱えると考えられているが [30]、問題特化のやり方や他のリソースとの組み合わせ次第で多様なアーキテクチャの可能性が考えられる。

論理量子ビットと物理量子ビットの境目にもなっている誤り訂正プログラムの実行に関するサブコンパイラ、誤り訂正の高速データ処理など論理ビット処理上の課題や、制御・測定処理に関するリソース推定・配分、制御信号のサブコンパイラなど、コンピューター科学の視点では萌芽的な状況と言える。どの方式の誤り訂正符号を利用するかの選択は、物理量子ビットどうしの結合・配線や、補助量子ビットの設置など回路レイアウトのレベルまで根深く影響を及ぼす。現在 IBM や Google が精力的に研究開発を進めている超伝導量子ビットのレイアウトも、２次元表面符号の実装を前提としたものとなっている。

量子誤り訂正は量子ビットに物理的に起きる誤りを論理的に訂正し、正しく計算できるようにするのが「誤り訂正技術」である。古典的な（量子ではない）誤り訂正技術は確立しており、CD 再生、無線 LAN、携帯電話、ハードディスクなど、身の回りの情報機器に入っている。コンピューターとしての技術スタックの中では、現在のコンピューターでのミドルウェアまたはファームウェアに該当する部分である。しかし、エラー耐性量子コンピューターでは、量子計算モデルから物理量子ビットのレイアウトまでレイヤを貫通して大きな影響を及ぼす要素である。

エラー耐性量子コンピュータの実現困難な理由として挙げられるのが、量子コンピュータの核ともいえる「量子ビット」がもつ状態の壊れやすさである。量子ビットの量子状態は思い通りに正確に制御できず、誤りが起きやすい。量子コンピュータに現れる誤りは、古典コンピュータでのそれとは違い、種類の異なる誤りが雪だるま的に重なり複雑化しやすい。また、量子ビットの状態の複製が原理的に不可能であることも、古典的な方法での冗長性の確保を困難にしてしまう。量子誤り訂正符号の進歩により実装困難さは少しずつ

緩和されている。

マイクロアーキテクチャのレイヤでは、制御系まで含めて、どのようなシステム構成でどのような命令フローになっているべきかなど、萌芽的ではあるが研究開発は着実に進められている [31]。超伝導量子ビットや Si スピン量子ビットの場合には、量子プロセッサー部分は希釈冷凍機環境下に置かれ、室温環境に設置されている制御・測定用機器と同軸ケーブルで接続されているなど、さながら物理実験室の様相である。冷凍機技術、高周波回路技術、FPGA による制御のハードウェア高速化などこれまで電気工学が扱ってきた要素技術のほか、極低温でも動作するアンプや AD 変換器などを Cryo-CMOS や超伝導回路で作り込むというような取り組みもある。

TSV やフリップチップボンディングなど量子チップと制御用チップの２～３次元配置・配線など、これまでの半導体開発で培われてきた技術を最大限活用する動きも見られる。量子ビットを２次元平面に配置する場合には、中央部分の量子ビットへのアクセスは 1000 量子ビットを超えるスケーラビリティを考える上での重要課題である。また、どのように冷凍機をまたいで量子チップ間で量子情報をやり取りするか、量子通信への接続を念頭に光子系にいかに量子情報を変換（テレポーテーション）するか、などは分散型アーキテクチャまで含めて挑戦的な課題として残る。技術的には、量子通信分野で開発が進む量子中継器の技術との関連も深い。さらに、３次元トポロジカル量子誤り訂正符号の実装まで考えると、このレイヤは測定型量子計算モデルの実装を検討する必要もでてくる [32]。

量子デバイスの実現を支える物理系としては、超伝導回路、イオントラップ、光子、量子ドット、核スピン、冷却原子など様々な取り組みがある。ビット数とゲート忠誠度（エラー率）の点で、もっとも進んでいるのは超伝導量子ビット技術である。2004 年のイェール大学の Schoelkopf らの回路 QED の提案 [33] に始まり、現在は超伝導トランズモン方式と呼ばれる超伝導回路による量子ビット表現が主流で、Google-UCSB グループ、イェール大学グループ、デルフト工科大学グループ、IBM グループの４グループが主要なプレーヤーである [4]。一方で、歴史的には世界で最初の「量子コンピューター」であるイオントラップ方式は、結合性と均一性に利点があり、DARPA、IonQ など精力的に研究開発が進められている。非固体であるため IT 企業からは風変わりと感じられている節がある [6] が、デューク大学が NSF からグラントを受けた STAQ プロジェクトなど、実用的

表 2.5: 量子ソフトウェア開発環境

		Forest	QISKit	ProjectQ	QDK	Cirq
作成元		Rigetti	IBM	ETH Zurich	Microsoft	Google
プログラミング言語		Python	Python	Python	Q# (C# / Python)	Python
量子プログラミング言語		Quil	OpenQASM	DSL	Q#	Cirq
バックエンド	量子ハードウェア	8	5-20	-	-	-
	シミュレーター	20 (local) 30+(cloud)	25 (local) 30 (cloud)	28 (local)	30 (local) 40 (cloud)	30 (local)

（注）上記シミュレーター（local）で計算可能な量子ビット数はあくまで目安である。
PC性能によってはこれよりも小さい量子ビット数までしか計算が実行できない場合もある。

NISQ 量子コンピューターのプラットフォームとして着実に研究開発が進められている。

いずれの物理系を利用するにしろ、実験研究的に量子ビット数をじりじりと増やしてゆくことと、スケーラブルなエラー耐性量子コンピューターをいかに作るかとの間には、依然としてギャップがある。工学的に現実的な実現化モデルや設計指針に基づいて物理系を取捨選択（複数の物理系や性質を組み合わせて使うハイブリッド系も含む）し基本素子を作ってゆくという、アーキテクチャに基づいたスケーラビリティの考え方は、徐々に定着しつつあるようだ [32]。光と量子ビットの系により誤り耐性トポロジカル量子計算モデルを実装するアーキテクチャの提案や、大規模量子コンピューターへのスケーラビリティを考慮した超伝導量子ビットやイオントラップでの実験成果もあり、量子コンピューターを構成する基本モジュールの構築が精力的に進められている。

2.1.6 問題点

量子コンピューターの研究開発はこれまで量子情報理論や量子物理実験としての研究対象であることがほとんどであったが、近年ソフトウェア・ハードウェアともに、量子情報技術・量子情報工学とでも呼ぶべき工学的な側面へと発展してきている。私たちが手にしているコンピューターと比べると現在の量子コンピューターは 1960 年代のコンピューターの状況と似ているとも指摘されている [34] が、その実現に向けて物理学、コンピューター科学、電子工学、情報学、数学などが融合して、社会に役に立つ量子情報技術とその構築のための学理基盤が生み出されようとしている。

コンピューターサイエンスの観点から見て、現状の量子コンピューター開発の問題点・課題は（1）NISQ 量子コンピューターのキラーアプリケーションが不明確、（2）スケーラブルな量子コンピューターの設計指針が未成熟、（3）学際的分野として萌芽期のため人材が不足・コミュニティが小規模、である。これらのことは、実験的な状況の量子デバ

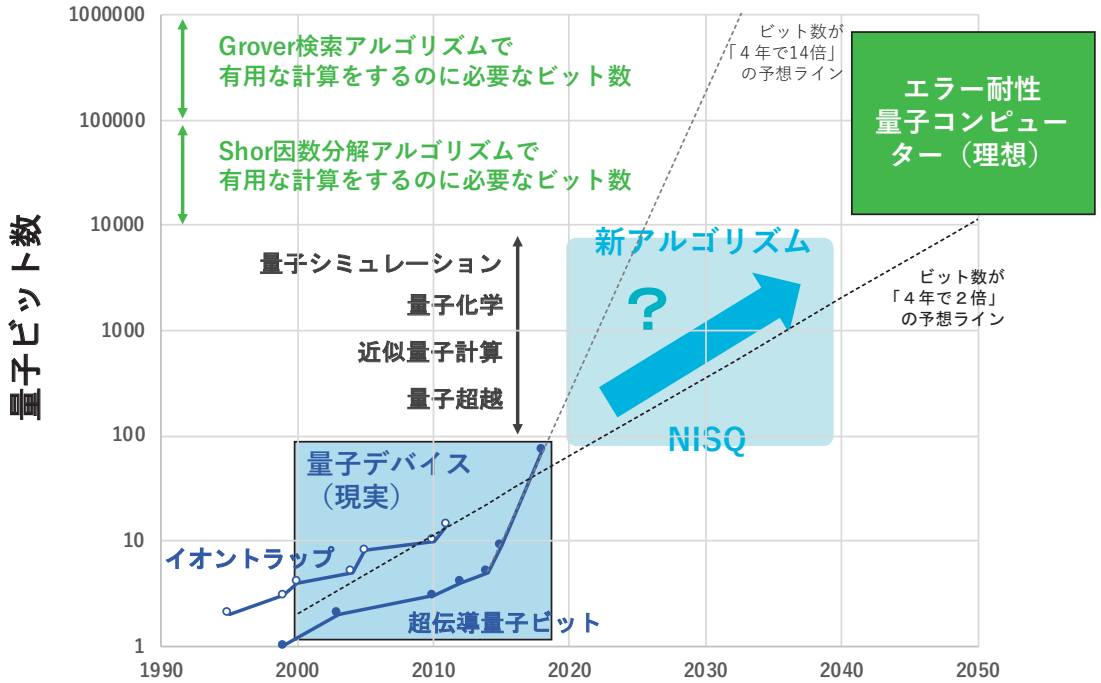

図 2.5: 量子ビット数の推移

イスと理論的に高度な議論が進む量子アルゴリズムとの間のギャップをいかに埋めてゆくかという課題にまとめられる [13]。

（1）と（2）は主に科学技術的な課題であり、多くの科学的発見や工学的発明が求められる。量子コンピューターを組立てるのに必要なソフトウェア・ハードウェア技術だけでなく、その設計指針や設計・製造に関する技術、指示通り動作させて情報処理を行うために必要な技術など、多数のブレークスルーが必要であり、これらは 5 ～ 10 年の研究期間であらかた解決できるとは考えられない。そのような中長期の量子コンピューター開発を勇気づける意味でも（1）に挑戦することは重要である。

短期的には（1）に対応する量子コンピューターを「つかう」ための研究開発が、中長期的には（2）の解決の糸口を見いだすような量子コンピューターを「つくる」ための研究開発が必要である。また、量子コンピューターの研究開発や利用を行うのは全て「人」であるので、（3）に挙げた問題である人材を徐々に充実させ、骨太のコミュニティーを醸成することで（1）と（2）にかかる研究開発を強力に支えることが不可欠である。このため、研究開発リソースの継続的な支援だけでなく、共同利用設備、国際協力推進、産学連携の促進など総合的な推進施策が求められ、政府や公的機関が果たす役割は小さくない。

2.2 社会・経済的効果

2.2.1 化学計算の加速

2022 年の医薬品の世界市場は 150 兆円を越えるとの試算が出されている [35]。現時点で、高性能コンピューターの存在の医薬品開発への影響力は限定的だが、高性能コンピューターを用いた *in silico* 研究アプローチが既存の創薬の閉塞感を打破するカギであることに疑いの余地は無く、量子コンピューターを用いた「量子コンピューター創薬」も決して絵空事では無い。

20 世紀後半は、数十～数百万種類の膨大な低分子化合物ライブラリの構築と効率的なスクリーニング系の構築という、「量」重視の創薬が隆盛を極めた。その結果、現在の医療現場で日常的に処方されている様々な医薬品が登場、内科的治療技術は飛躍的に進展し、医薬品産業は年間 40 ～ 50 兆円規模の巨大産業となった。

20 世紀末には従来の開発モデルで克服可能な疾患は枯渇し、低分子医薬品から高分子医薬品へのシフトが始まった。高分子医薬品の開発では、治療標的の精緻な解析に基づき分子を取得・設計し、実験系でアッセイし得られたデータを元に更に改良を重ねる、という「量より質」を重視した分子の作り込みがカギを握ることとなった。例えば、当該方法論に基づき 2014 年に小野薬品工業（株）が商品化した「オプジーボ」は、従来の低分子化合物ベースの抗がん剤では達成不可能であった、ある種のがんに対する特効薬として世界が注目している。

生化学・医学的な実験系は限界まで洗練されつつある中、大きなポテンシャルを秘めた技術が、高性能コンピューターを用いた *in silico* 分子設計である。近年のハードウェア、ソフトウェアの劇的な進展によって、徐々に生化学的・医学的な実験系を補いうる方向性が見え始めている。その背景には、ソフトウェアの開発に加えて、米国 D.E.Shaw Research が開発する Anton シリーズ（2009 ～）、日本の理研・泰地博士らが開発する

MD-GRAPE シリーズ（1997 ～）をはじめとした、分子動力学（Molecular Dynamics: MD）計算専用機の発展が大きい。現在も Anton2 後継機の開発、MD-GRAPE4 後継機の開発で日米が性能を競っているところである。

in silico 分子設計の課題は、（1）生理学的に重要なタンパク質の、構造的にカギを握る部位に動的に作用することで機能を阻害・活性化させる低分子化合物の設計、（2）細胞内環境の全タンパク質の挙動を MD シミュレーションで再現し、医薬品候補の細胞内送達・動態を完全に *in silico* 上で設計すること、である。

タンパク質は数万～数十万の分子量を有する巨大分子であり、その全貌を計算することは困難である。しかし、部分を限定することで、低分子化合物との動的な相互作用を計算し予測することは現実味のある研究テーマである。例えば、わが国における創薬ベンチャーの成功事例とされるペプチドリーム社も、当初目標としたペプチド（＝非常に小さなタンパク）そのものを医薬品化する方向が予想以上に高難易度であったことが分かりつつあるため、「タンパクと結合し機能を有するペプチドを低分子化合物へと置換するために *in silico* 手法をフル活用する」開発戦略へと転換する兆しを見せ始めている。欧米のメガファーマも同様の戦略をとっている。

今のところ、NISQ 量子コンピューターで扱える分子サイズは限定的である [36]。2017 年に IBM の研究者らは、BeH_2 分子などの構造が単純な分子について、最大 6 つの量子ビットを使用した NISQ 量子コンピューターによる量子化学計算の可能性を示した。これは、あくまで BeH_2 というシンプルな分子を対象とした研究である。例えば高血圧治療薬として有名な「スタチン」は BeH_2 の 50 倍の分子サイズ、2017 年に *in silico* 的アプローチ活用したと思われる創薬標的「BCL-2」は 2500 倍の分子サイズである。

課題となるのは分子サイズだけではない。創薬への応用には創薬標的と作用分子の間の複雑な相互作用を、1 ミリ秒を大きく越えるタイムスケールで観察する必要も出てくることから、計算の複雑さや要求精度は飛躍的に高まる。そのため、NISQ 量子コンピューターのハードウェア的な性能向上だけでなく、大規模 MD 計算を精度良く近似する古典・量子ハイブリッドアルゴリズムの発見が、量子コンピューターの創薬への影響の大きさを決定づける重要な要因となるだろう。

今後量子コンピューターならではの創薬用ソフトウェアが登場すると、上記（1）（2）の概念にそもそもとらわれない大胆な創薬の実現、或いは既存の高性能コンピューターとの上手な協調動作による量子・古典ハイブリッド *in silico* 創薬の加速が実現するものと期待される。

2.2.2 機械学習・最適化の加速

機械学習は産業応用上極めてインパクトのある技術であり、量子コンピューターに開かれた市場機会は巨大である。現在の人工知能ブームの技術的な背景は統計的機械学習技術であり、自動車、鉄鋼、材料、創薬などの製造業は言うに及ばず、金融、小売業、流通、通信、エネルギー、など極めて広範囲の産業領域で、機械学習の重要度は増すばかりである。このような広範囲の産業領域に応用を持ち、かつ、今後急速な発展が見込まれると予想されているため、量子コンピューターの実用化をスコープに入れる長期の市場規模予測は困難である。

コンピューターの発展と、データ分析技術の発展は、互いに関係し合う歴史として理解

するとわかりやすい。コンピューターの計算能力の急速な進歩によって、主成分分析や回帰分析などの統計的・線形代数的な手法を大規模なデータに適用できるようになった。また、1950 年代には、パーセプトロンに代表されるような人工ニューラルネットワークの導入と実装が進み、ボルツマンマシンやホップフィールドネットワークなどに発展した。また、バックプロパゲーションによる学習を行う深層学習（ディープラーニング）が導入され、巨大なデータセットを GPU によって高速処理することで深い（多層の）ニューラルネットワークを学習することが可能となった。画像認識などで人間の識別率を上回る性能が示されたことを発端に、現在の人工知能ブームが始まった。

2017 年現在の機械学習の市場規模は 14 億ドルという見積もりがあり、2022 年には 88 億ドル市場にまで増加すると予測されている。市場規模の推移は予測困難であるが、少なくとも 2030 年にはこの程度の市場規模があるとして、その頃に実現しているであろう小規模の NISQ 量子コンピューターが 5% 程度でも従来コンピューターからシェアを奪えれば、それだけで単純には 5 億ドルの市場機会となる。

量子コンピューターによる統計的機械学習へのアプローチで期待されているのは、古典コンピューターでは認識することが困難なパターンの効率的な認識である。とくに量子系は古典的なシステムでは効率的に生成できないパターンを効率よく生成できると期待されており、一部の機械学習タスクでは従来コンピューターよりも量子コンピューターのほうが優れている可能性がある。

このような量子機械学習への展開により量子コンピューターが社会的・経済的なインパクトを産むかどうかは、効率的な量子・古典アルゴリズムの発見に大きくかかっている。量子機械学習は、全体としては従来コンピューター上で実行される機械学習ソフトウェアの一部分を、量子コンピューター上で行うサブルーチン的なアルゴリズムとして動作し、特定の計算において古典コンピューターで実行するよりも必要計算ステップ数が小さく済む（量子加速がある）ことが期待されている。この高速性は、数学的な証明による計算量の議論か、有限のサイズの問題を有限の性能の現実のデバイスによって実行する場合の実時間の議論なのかに注意する必要がある。また、古典的アルゴリズムで可能な性能の限界がどこにあるのかは必ずしも知られておらず、現時点でそのような（古典的）アルゴリズムが未発見であり、量子アルゴリズムの高速性としては、現時点で知られている古典ベストアルゴリズムよりも高速である、というだけしか言えない。そのため、現在提案されている量子機械学習アルゴリズムよりも高速な古典アルゴリズムが発見される可能性は否定できない。実際、量子推薦システムと呼ばれるアルゴリズムは、それまでの古典ベストアルゴリズムを指数関数的に上回る優れた量子アルゴリズムであったが、提案されてから数年で、より高速な古典アルゴリズムが報告された。

エラー耐性量子コンピュータ上で機械学習を行う量子アルゴリズムはいくつか提案されている。代表例は、分類問題に対応する量子サポートベクターマシン (Quantum support vector machine)、リッジ回帰と呼ばれる回帰分析手法の量子版である量子リッジ回帰 (Quantum Ridge regression) 、教師なし学習手法としてボルツマンマシンを量子コンピューター上で実現する量子深層学習 (Quantum deep learning) などが提案されている。これらの手法の有効性はまさに議論の最中であり、古典のベストアルゴリズムよりも計算量の点で優れているとするとは必ずしも言えないものもある [37]。

短期的な応用で期待されているのは、古典・量子ハイブリッドアルゴリズムと呼ばれて

いる、古典コンピューターと量子コンピューターを両方とも使う、新しいタイプのアルゴリズムである。前節で触れた通り、量子化学計算では VQE アルゴリズムと呼ばれる手法が代表的である [36]。量子機械学習で注目されている古典・量子ハイブリッドアルゴリズムのひとつに、量子近似最適化アルゴリズム（Quantum approximate optimization algorithm (QAOA)）が挙げられる [38]。このアルゴリズムは組合せ最適化問題を解くアルゴリズムであるが、Rigetti Computing の研究者らによるデモンストレーションで、（教師なし）機械学習タスクに適用できることから、注目を集めた。

具体的には、データの類似度に応じて重みつけをすることで、機械学習での分類問題を（重み付き）MAXCUT 問題という組み合わせ最適化問題の一種として定式化し、その組合せ最適化問題を QAOA を実行することで解くという手立てになっている。Rigetti Computing の研究では、19 量子ビットの量子コンピューター上で QAOA を実際に実行するデモンストレーションを行った。量子計算の機械学習への適用という新しいジャンルを開拓した意味でこの QAOA というアルゴリズムは注目に値するが、その計算能力が古典アルゴリズムを超えると理論的に証明されているわけではなく、現時点では期待が先行している感がある点には注意が必要である。

2.2.3 暗号・ブロックチェーンなどへの波及効果

誤り耐性量子コンピューターの実現によってもたらされると予想されるもっとも大きな社会的インパクトは、SHA や楕円暗号などの暗号システムの切り替えの加速である。Nature 誌 2017 年 9 月 14 日号は量子ソフトウェアを特集し、表 2.6 に示すように、量子アルゴリズムの代表的な暗号システムへの影響を示した。ショアのアルゴリズムが公開鍵暗号を破壊し、共通鍵暗号（ただし十分な鍵長）のみ生き残ることがわかる。このように、量子技術が成功すれば、影響は破壊的である。

表 2.6: 量子コンピューターの登場による暗号の安全性の変化

共通鍵暗号	機能	現状の安全性	ポスト量子安全性
AES-128	共通鍵暗号	128	64 (グローバー)
AES-256	共通鍵暗号	256	128 (グローバー)
Salsa20	共通鍵暗号	256	128 (グローバー)
GMAC	メッセージ認証コード	128	128 (影響なし)
Poly1305	メッセージ認証コード	128	128 (影響なし)
SHA-256	ハッシュ関数	256	128 (グローバー)
SHA3-256	ハッシュ関数	256	128 (グローバー)
RSA-3072	暗号化	128	解読 (ショア)
RSA-3072	署名	128	解読 (ショア)
DH-3072	鍵交換	128	解読 (ショア)
DSA-3072	署名	128	解読 (ショア)
256-bit ECDH	鍵交換	128	解読 (ショア)
256-bit ECDSA	署名	128	解読 (ショア)

同時に、同誌は、論理量子ビットのエラーを 10^{-15}（1 京分の 1）、かつ、物理量子ビットのエラーを 10^{-5} に抑えるとすると、誤り訂正に、10^4 から 10^7 個の量子ビットが必要としており、上記の表のような攻撃が可能となるには 30 ～ 50 年かかると予想される。他方で、米国標準技術研究所 NIST は、暗号システムの移行は 10 年がかりの作業であることと、アルゴリズムや量子ビットの開発加速の可能性もあるため、2016 年 2 月に、量子コンピューターによる高速な因数分解が可能となっても安全性を保証できる「ポスト量子暗号」の標準化計画を発表している [39]。エラー耐性量子コンピューターによって因数分解が高速化されても安全性を確保できる格子暗号と呼ばれる次世代の暗号も開発されている。

因数分解の高速化は、より単純な暗号システムを採用している仮想通貨にも影響を及ぼすと考えられる。実際、ビットコインでは SHA256 がハッシュ関数として使われており、エラー耐性量子コンピューターにより高速にマイニングすることも可能となると見られる。Credit Suisse は 2018 年 1 月 11 日に「Blockchain 2.0」というレポートを発行し、「量子計算技術は高度な利用にはまだ何年もかかるし、商業利用はさらに先なのに、脅威をあおり、例えば、2026 年までに 1/7 の確率、2031 年までに 50 %で公開鍵暗号が解読されると言い立てる者がいる。しかし、もし、そうなったら、デジタル署名に使われる既存の公開鍵暗号は全て量子アルゴリズムに負けてしまい、ブロックチェーンを心配しても意味がない」と述べ、量子コンピューターの暗号分野への影響は、ブロックチェーンをはるかに超えて大きいことを指摘している [40]。

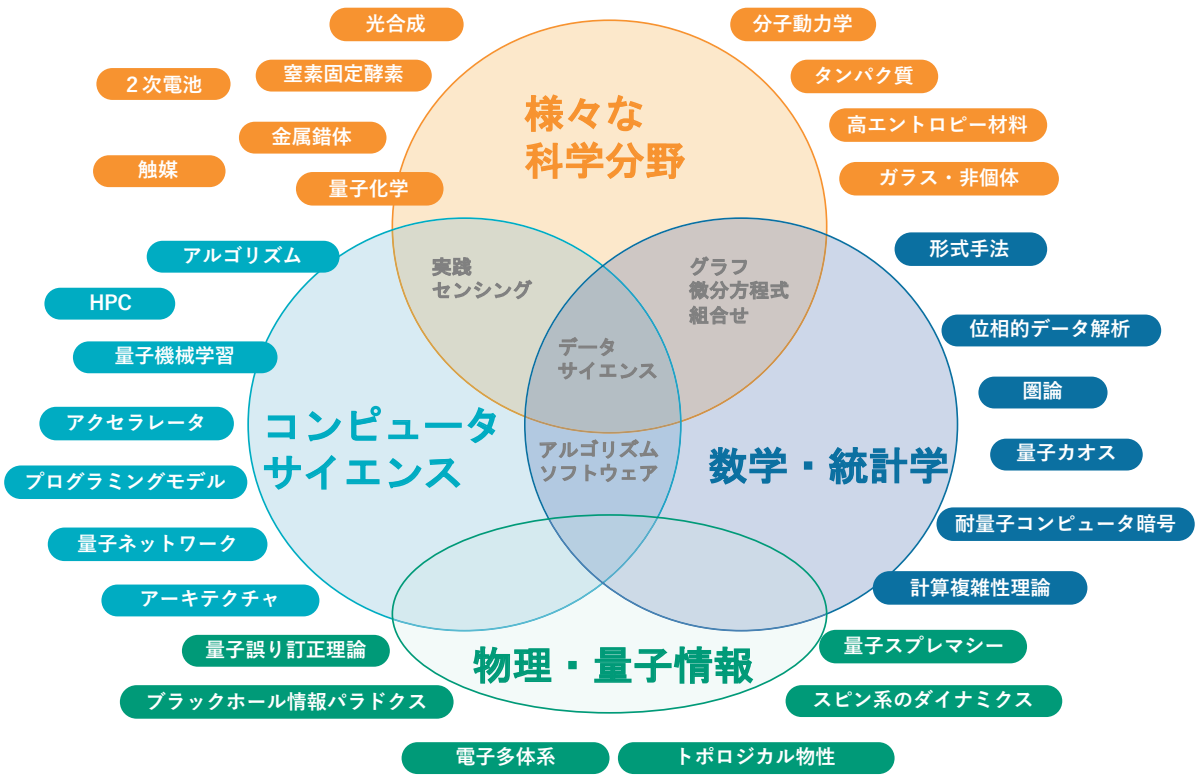

図 2.6: 量子コンピューターの科学的インパクト

2.3 科学技術上の効果

量子コンピューターが及ぼす科学技術上のインパクトは、図 2.6 に示すように様々な分野に及ぶ。量子コンピューターによる量子化学計算は、明らかに化学分野に大きな影響を与えうる。人工光合成、二次電池、触媒金属錯体などの化学分野の様々な領域では量子化学計算は明らかに重要であり NISQ 量子コンピューターの活躍が期待できる。また、タンパク質やガラスなどを対象とした大規模な分子動力学計算では、必ずしも量子コンピューターの直接利用は見込まれない。しかし、その場合であっても、量子・古典ハイブリッドアルゴリズム開発を通して、分子動力学計算の理論的解明が進み、量子インスパイアの形で効率良い（古典の）計算手法が見つかる可能性もある。

コンピューター科学や数学・統計学へのインパクトも無視できない。ポストムーア時代での計算機性能を継続的に向上する手段として、量子コンピューターをアクセラレーターに使うことはかなり現実的に思われる。また、理論としても、量子コンピューター（＝量子チューリングマシン）という従来のチューリングマシンとは異なる計算機械上でのアルゴリズムの研究は、今の（古典）アルゴリズムの研究にとって有意義と思われる。優れた量子アルゴリズムの発見は、たとえそれが現時点でのハードウェアで実行できる見込みがなくとも、計算複雑性の理解を大いに助ける。古典コンピューターで効率的にシミュレーションできない量子コンピューターの振る舞いは、計算複雑性理論における多項式階層（が崩壊しないと強く信じられていること）と深く関係しており、量子超越の実証は計算機理論にとって重大な結果となる。

量子コンピューターの影響は物理学の中にも広がりを見せる。ブラックホールの情報パラドクスなどの量子情報理論上の議論のいくつかを NISQ 量子コンピューター上で量子シミュレーションとして実証することは有意義だろう。スピン系のダイナミクス、量子カオスなどでも同様に、対応する系の量子シミュレーションを量子コンピューターが行うようになるだろう。物理学への究極のインパクトは、量子コンピューターを研究することではなく、量子コンピューターで研究する時代の到来である。

3．具体的な研究開発課題

3.1 問題点と研究開発課題

現状の量子コンピューター開発の大きな問題点・課題は第２章で述べたとおり（１）NISQ 量子コンピューターのキラーアプリケーションが不明確、（２）スケーラブルな量子コンピューターの設計指針が未成熟、（３）学際的分野として萌芽期のため人材が不足・コミュニティが小規模、である。

NISQ 量子コンピューターに向くアプリケーションの探索には、量子・古典アルゴリズムの精力的な研究開発が不可欠である。3.2 では現在期待されている量子化学計算と量子機械学習に関する研究開発課題と、応用から見た NISQ キラーアプリケーションの展望を述べる。現状のハードウェアに対する実装容易性の考慮はある程度は必要だが、ハードウェアと無関係に（論理レベルで）量子・古典ハイブリッドアルゴリズム開発を進め、それに応じて適切な NISQ 量子コンピューターのアーキテクチャを設計する「ドメイン志向アーキテクチャ」の考え方 [14] も有効と考えられる。

様々な量子・古典アルゴリズムの試行錯誤には、アルゴリズムをプログラムとして書き下し、ソフトウェアに仕立てるためのソフトウェア開発環境が必要である。3.3 で述べるように、コンパイラ、ライブラリ、デバッガなどの各種ツール、エラーのある量子デバイスの振る舞いをシミュレーションする高性能シミュレーター、量子プログラミング言語（高級言語や DSL[1]）など従来はコンピューター科学や電子工学がターゲットとしてきた研究開発項目が多数必要である。また、量子ビット間の接続関係や量子デバイスごとの性能バラツキなどを適切に抽象化する（または隠蔽する）ハードウェア記述言語の開発、その抽象度レベルでのシミュレーション・検証、それを用いた設計、配線・パッケージ・周辺制御回路など古典制御技術との融合を支えるハードウェア・ソフトウェア開発も重要である。

エラー耐性量子コンピューターの実現に向けた、スケールアップのための現実的な設計指針の構築が必要である。ここでは、3.4 に挙げるように、アーキテクチャに基づいて量子コンピューターの研究開発を進めてゆくことが肝要である。その根幹は、量子誤り訂正符号をいかに取り入れるかである。ハードウェア実装性に優れた新しい量子誤り訂正符号の開発、トポロジカル量子誤り訂正プログラムの実装に必要となるコンパイラ開発（量子回路の最適化・リソース推定・検証ツール、ゲート列分解の効率化）や、測定結果を解析して誤り訂正の制御を返すハイスループットの古典データ処理、基本演算や命令を処理する複数の機能ユニット、命令セットアーキテクチャをどのようにするか、全体的なアーキテクチャの試行錯誤と整理が求められる。

3.2 古典・量子ハイブリッドアルゴリズムの開発・実装・実証

3.2.1 量子化学計算

現時点で有望視される量子コンピューティングアプリケーションの１つは、古典コンピューターで計算するには複雑すぎる量子力学的システムのふるまいのシミュレーションである。材料設計や創薬などで頻繁に登場する量子系は、複数個の電子がクーロン相互作

[1] Domain-specific language（ドメイン固有言語）

用によって互いに影響を及ぼしあう電子多体系である。

化学や物理学における究極の目標のひとつは、物質の微視的な性質を支配するシュレーディンガー方程式を厳密に解くことである。多数の電子を含むシュレーディンガー方程式を解いて、厳密な波動関数を知ることができれば、電子状態、分子構造、化学反応経路、物性などを精度よく予測することが可能となり、材料設計や創薬に活かせる知見が得られる。

しかし、シュレーディンガー方程式を厳密に解くのに必要な計算時間は、計算すべき電子数に対して指数関数的に増加する。そのため、多電子系のシュレーディンガー方程式を厳密に解くことは一般には不可能であり、近似的に解く方法が多数開発されている。

量子コンピューターを用いた量子化学計算を行う際の手順は以下の通りである。

⑴ 解きたい電子系のハミルトニアンを Born-Oppenhimer 近似[2]する。
⑵ 第二量子化[3]を行い、0 と 1 の値のみで処理できるようにする。
⑶ Bravyi-Kitaev 変換[4]を行い、量子ゲートで計算できるようにマッピングする。
⑷ 位相推定アルゴリズム（Phase Estimation Algorithm：PEA）もしくは変分量子固有値ソルバー（Variational Quantum Eigensolver：VQE）を用いて量子コンピューターで解く。

古典コンピューターによる厳密な解法である全配置間相互作用法（Full Configuration Interaction Method：FCI 法）は電子数の増加に対し計算時間が指数的に増加するのに対し、PEA を量子コンピューターで実行した場合には同じサイズの問題を多項式時間内で行えることが示されている。しかし、精度の良い PEA の実行は、多数の量子ビットと多数の量子ゲート操作（深い量子回路）が必要であり、基本的にはエラー耐性量子コンピューターでの実行を想定する必要がある。

一方で、VQE アルゴリズムは、古典の変分最適化アルゴリズム中に比較的少ない量子ゲート操作からなる量子計算が埋め込まれた、量子・古典ハイブリッドアルゴリズム [41] である。そのため、エラーが多く深い量子計算に不向きな NISQ 量子コンピューターでもある程度意味のある計算が可能である。必要となる量子ビット数は、試行波動関数を表すのに必要なだけの電子スピン軌道数だけであり、BeH_2 などの小さな分子であれば、基底状態のエネルギーを計算するために考慮すべき電子軌道の数はたかだか 6 個となるので、6 量子ビットの NISQ 量子コンピューターに問題が載せられる [36]。

VQE アルゴリズムでは、変分パラメータつきの試行波動関数を使い、量子計算サブルーチンによってエネルギーを計算し、その値が小さくなるようにパラメータを更新しながら繰り返し計算を行う。ポイントは、試行波動関数と解の波動関数とがどれほど似ているかであり、酷似していれば少数の繰り返しで計算が終了するが、試行波動関数の表現力が不足していれば、必要な精度が得られるまでの計算の繰り返し数は膨大となる。また、多次元のパラメータの初期値も解の収束性を左右し、古典計算である程度よい波動関数（すな

[2] 原子核の質量が電子の質量よりも遙かに大きいことを利用して、原子核と電子の動きを分離し、原子核は固定されているものと見なすこと。
[3] 場の量子化を意味し、物理量を演算子で置き換えたシュレーディンガー方程式（第一の量子化）と同様の方程式において、波動関数を再び演算子と解釈することから第二量子化と呼ぶ。
[4] 量子化学計算と量子コンピュータを結びつけるための変換方法

わち答えとよく似ている波動関数）になっているように事前に計算をしておいて、そこからVQEアルゴリズムで最適化するというようなテクニックも必要となる。

NISQ量子コンピューターでの量子化学計算で用いる基底関数のセットとして、どのようなものを用いて試行波動関数を作ると良いか、設計方法論の構築は重要な研究開発課題である。現在提案されている試行波動関数は従来法でGold standardとされる試行波動関数を量子コンピューター用にアレンジして使用しているが、そのような試行波動関数がさまざまな化合物の計算で有効かどうかはわからない。

利用できる量子ビット数が限られている状況では、シミュレーションしたい分子に含まれる全ての電子軌道を計算に取り込むのは早晩不可能となる。そのため、どの電子軌道が計算結果の精度に影響を及ぼすかを先見的知識も活用して見極め、試行波動関数に効率的に取り入れてゆく近似が不可欠となる。さまざまな分子（または注目部分）のエネルギー計算のための基底関数のセットと必要となるスピン・軌道数の例を表3.1にまとめた。VQEアルゴリズムではスピン・軌道数と同じだけの量子ビットを用意する必要があるが、これらの値はNISQ量子コンピューターとして現実的な値に留まっている。試行波動関数の量子回路での表現方法（量子ビット数、量子回路）と得られる計算結果の精度のトレードオフの系統的な検討など、試行波動関数の設計指針の構築は、NISQ量子コンピューターでの量子化学計算の重要な研究開発ターゲットである[42]。

3.2.2 量子機械学習・近似最適化

量子コンピューターによる機械学習は、指数関数的に高速に特定の一次方程式を解くことができるHarrow、Hassidim、Lloydによる画期的な量子アルゴリズムを発端とし、近年新たな展開を迎えた領域である[37]。このアルゴリズムに基づき、フィッティング、SVM（Support Vector Machine）、分類などの機械学習タスクのための新しい量子アルゴリズムも開発された。

最近では、エンドユーザーアプリケーションも、量子アルゴリズムの形式で提示されており、例えば「量子推薦システム」と呼ばれるアルゴリズムは、NetflixやAmazonのようなシステムのユーザに、それまで知られていた古典アルゴリズムよりも指数関数的に高

表3.1: 量子化学計算に必要なスピン軌道数の例

分子	スピン・軌道数	基底
NH_3	16	sto6g
H_2S	22	sto6g
H_2O	14	sto6g
H_2O	38	dzvp
H_2O	50	p6311ss
FeMoco	16	tzvp
FeMoco	24	tzvp
FeMoco	108	tzvp
FeMoco	114	tzvp

速に推薦を出力することができる[5]。しかし、多数の提案にもかかわらず、これらの量子アルゴリズムが機械学習に実際の影響を与えるには、**データ入出力**や**リソース推定**などについて多くの課題が残っている。また、多くはエラー耐性量子コンピューター上での実行を想定しているアルゴリズムであり、NISQ 量子コンピューター用の機械学習アルゴリズムの開発は今後も重要となる。

データ入出力

これらの量子機械学習アルゴリズムを実行するには、データを量子メモリに格納し量子機械学習の計算処理（学習・推論）の中で随時データにアクセスできる必要があるが、現実世界の数 GB ともなるデータセットのサイズに対応できる量子メモリはハードウェア的に未成熟である。また、基本的には量子コンピューターにおける計算は量子レジスターにゲート操作を施すというプログラミングモデルである（プログラムは古典データとして書かれている）ため、そもそも量子メモリは想定されていない [44, 45]。

いずれにせよ、機械学習タスクを行う量子アルゴリズムは、データの入出力に何らかの量子－古典の変換が関係しており、これを量子力学の性質を利用して高速化できるアルゴリズム（プロトコル）の登場が望まれる。データ処理のステップ数が指数関数的に短縮された場合でも、データの入出力にかかる処理ステップ数が大きいまま残ると、アルゴリズム全体の計算コストを圧迫することになる。従って、データ入出力まで含めて量子機械学習の優位性を判断する必要がある。

古典データの入出力は（1）古典データと量子状態の振幅を変換するアナログ符号化、（2）振幅を量子ビット列に変換するデジタル符号化の２つのタイプがある。HHL アルゴリズムでは、この２つの符号化を組み合わせて計算を行う。２つの符号化の間を取り持つ量子 AD 変換 [46] も提案されており、古典計算によってデータを二分木構造に前処理しておけば、量子 AD 変換を通じて量子メモリ（QRAM）を作成するコストは $\log(N)$ のオーダーである。従って、ハードウェア実装での課題はあるが、QRAM の存在を仮定することは量子機械学習のボトルネックとまでは言えない。ただし、量子 AD 変換は決定論的にできるが、その逆の量子 DA 変換は確率的である。

量子コンピューターを用いた機械学習の優位性（従来コンピューターによる機械学習よりも優れているかどうか）の判断は、極めて難しい問題である。計算複雑性理論の観点からは、アルゴリズムをクエリ複雑さとゲート複雑さの両方の尺度で評価でき、古典アルゴリズムと量子アルゴリズムを比較することが可能である。クエリ複雑さはアルゴリズムが情報源にアクセスする回数（クエリの数）で評価し、問題を解決するために必要なクエリ数が少ないほうが優れている（早い）とする考え方である。ゲート複雑性は、所望の計算結果を得るために必要な基本演算ステップ（量子計算の場合にはゲート操作）の数を数えることに相当し、この数が少ない方が優れていている（早い）とする考え方である。どちらも、評価方法は自然に理解されるが、一般に言う「早さ」の語感とは一致しない点に注意が必要である。

計算リソース推定

様々な量子アルゴリズムについてのリソース推定と量子回路の最適化は中心的研究テー

[5] その後、量子アルゴリズムにインスパイアされる形で、より高速の古典アルゴリズムが発見された [43]。

マとして議論されているが、現在のところ量子機械学習アルゴリズムの実行に必要となるゲート数の見積もりはあまり知られていない [37]。サイズが十分に大きい問題については量子機械学習アルゴリズムが古典アルゴリズムよりも優れていると計算複雑性の観点から考えることができるが、具体的にどの程度の問題サイズから利点があるのかは不明である。アルゴリズムやプログラムのベンチマークは不可欠な研究開発課題である。量子推薦システムでの例 [43] のように、特定の量子アルゴリズムが今後現れうる全ての古典アルゴリズムよりも優れていることの証明はしばしば困難となる。そのため、ベンチマークとなる問題設定の考案と、多くのヒューリスティックスな既知手法との様々な条件下でのベンチマーク実験を通じて、量子アルゴリズムが古典アルゴリズムを凌駕する、クロスオーバーポイントを調べることは有意義である。

3.2.3 キラーアプリケーションの探索

大規模のエラー耐性量子コンピューターは、因数分解、検索、主成分分析、機械学習、位相推定アルゴリズムを利用した量子化学計算など、古典コンピューターを凌駕するキラーアプリケーションにつながるアルゴリズムがいくつも提案されている。しかし、NISQ 量子コンピューターは、一部の特殊な計算問題 [10] での優位性は実証されそうだが、これぞという応用は依然として不明確であり、その探索は NISQ 量子コンピューターの重要な研究開発課題である。

現状のハードウェアスペックから考えて、NISQ 量子コンピューターに向く問題は、複雑ではあるが問題サイズは小さなものが良い。また、前節で紹介した VQE アルゴリズム

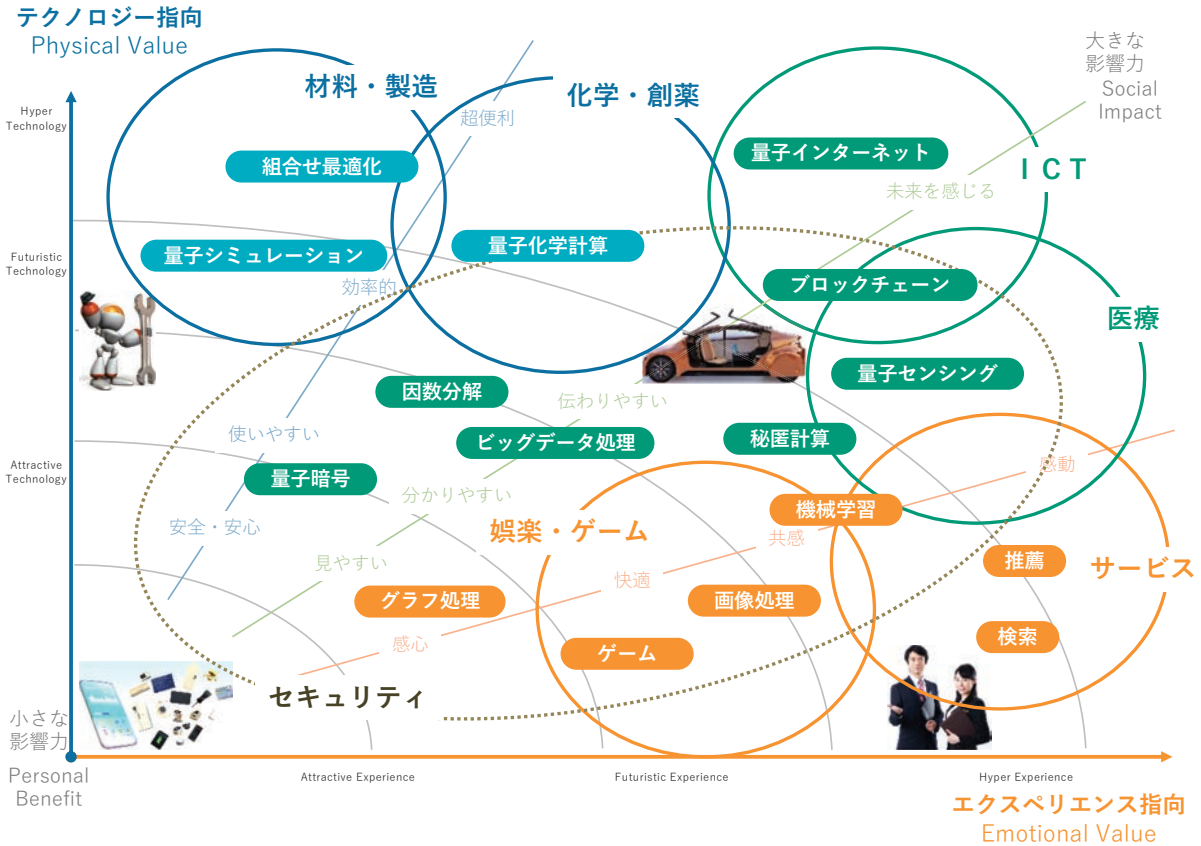

図 3.1: 量子コンピューターが変える社会

のように、NISQ 量子コンピューターをアクセラレーターとして使って性能を発揮できる問題が良い。

このようなことは、国際会議 ISCA2018 (International Symposium on Computer Archi-tecture) のチュートリアル講演で、シカゴ大学の Fred Chong 氏が「量子コンピューターにとって良い問題」の条件として明快に指摘している。その内容を以下に列挙する。

- コンパクトな問題表現（関数、小分子、小グラフ）
- 複雑さが高い計算
- コンパクトな解
- 簡単に検証可能な解
- 古典スパコンとの共同処理
- 少数の量子カーネルの利用

量子化学計算や量子機械学習は、問題の設定の仕方によっては、上記の条件を満たすように見えるが、これ以外にも有望なアプリケーションやアルゴリズムが眠っている可能性は十分にある。そのような（量子コンピューターにとって）未開拓のドメインを探索する指針として、本項では利用する社会や人々が感じる価値という側面から、NISQ 量子コンピューターへの期待を検討する。

図 3.1 には縦軸をテクノロジー指向（フィジカルバリュー）、横軸をエクスペリエンス指向（エモーショナルバリュー）として、量子コンピューターの活躍を期待する応用ドメインを配置した。濃い円と太文字が応用ドメイン、薄い太文字は NISQ 量子コンピューターによる計算を期待する計算ドメインである。

「製造」や「化学」の領域は、組合せ最適化や機械学習、量子化学計算などの計算ドメインとして、NISQ 量子コンピューターがある程度有望視されている分野である。右上の「ICT」は現代社会を支えるインフラとして重要であり、量子通信と共に、量子コンピューターを有効に使える部分も大きい。また、「ICT」と密接な関係を持つのが「セキュリティ」だ。暗号における符号・復号処理、ハッシュ関数や乱数計算、秘匿計算などは NISQ 量子コンピューターに期待できそうである。また、仮想通貨やスマートコントラクトなどブロックチェーン応用への展開も期待される。

エクスペリエンス志向軸には、「娯楽・ゲーム」「サービス」「医療」が並ぶ。「娯楽・ゲーム」領域では、レイトレーシングなどの 3D レンダリングや、高解像度の動画編集など、高速処理できる量子・古典ハイブリッドの新アルゴリズムが提供されれば歓迎される。また、将棋や囲碁などの既存のゲームに量子力学的なルールを追加することでゲーム性を増加させたり、量子性によってのみ可能になる全く新しいゲームも生まれるかもしれない。

「サービス」での生産性向上や顧客経験価値向上に貢献するアルゴリズムも歓迎されそうである。推薦や検索、様々な最適化問題など、量子コンピューターが持つ指数関数的に広い表現空間を使ってこれまでの機械学習では不可能だった表現の学習やパターンの認識に期待が寄せられる。「医療」におけるボトルネック課題に対し、量子技術の特殊性・優位性を活用するアプローチは、NISQ 量子コンピューターでの情報処理に、量子センサーを含む多様な量子技術モジュールや既存技術との統合化・システム化の必要性を喚起すると考えられる。

3.3 量子ソフトウェア開発環境の整備

3.3.1 量子ソフトウェア開発キット（SDK）

量子コンピューターの実現には、ハードウェアにおける研究開発の進展と同様に、計算理論やプログラミングなどソフトウェアの発展も欠かせない。量子・古典アルゴリズム研究にも、量子ソフトウェア開発を支える一連のツール（場合によってはツール自身も量子ソフトウェアかもしれない）は必要だ。

量子コンピューター用のソフトウェア開発の支援には、プログラミング言語、ライブラリ、コンパイラ、デバッガに加えて、バックエンドに高性能シミュレーターも必要である。１量子ビットに対する回転ゲート操作と、２量子ビットゲートである CNOT ゲートがあれば、理論的にはどのような量子アルゴリズムも構成できるが、現時点ではユーザーはゲートのレベルでアルゴリズムをプログラミングする必要がある。変分法、探索、行列積演算のようなサブルーチンや、量子情報処理固有の操作（測定基底の変換、テレポーテーションなど）は、関数・ライブラリとして提供されるのが望ましい。また、量子化学計算や機械学習など、計算ドメイン固有の概念や操作などもライブラリや DSL 等の形で提供されると、効率的に量子ソフトウェアの開発が可能となる。

コンパイラも重要である。現在提供されている量子 SDK は、リソース推定、スケジューリング、デバッグなどの機能をもつコンパイラを含んでおり、例えば、QISKit ではユーザーが書いたプログラムのうち実際のハードウェアの量子ビット間の接続関係から実行不可能な部分は、コンパイラ（インタプリタ）により警告が出される。NISQ 量子コンピューターでは、物理ビットがそのまま論理ビットであるため、物理デバイスのエラー率や結合性などの情報をコンパイラ（実態としてはアセンブラ）とユーザーに適切に伝える必要がある。現状では、ユーザーから見ると、量子プログラムを量子回路にコンパイルすることは、ハードウェアにマッピングすることにほぼ等しい。エラー耐性量子コンピューターの場合には、ここに誤り訂正符号が入るため、論理ビット処理と物理ビット処理は切り分けられているが、NISQ 量子コンピューターの場合には、物理ビットの状況を十分に考慮してアセンブリ言語レベルでプログラムを書く必要がある点に改めて注意が必要である。

このように現在の量子ソフトウェア開発環境は、古典コンピューターでは、アセンブラでプログラムを書いていた頃の状況である [20]。高級言語としてどのような抽象度があれば良いか、優秀なコンパイラをどう開発するか、最適化された量子回路をどう検証するか、どのようなライブラリを用意するか、などコンピューターサイエンスの挑戦を待つ課題が数多く眠っている。

ソフトウェアの互換性

以上のように応用を起点としてアーキテクチャレベルまでの深い検討を行い、量子ソフトウェアを充実させてゆく上で特に注意したい点は、ソフトウェアスタックの互換性である。ソフトウェアは元来、ハードウェア技術の進展や変更による互換性の問題に曝されているが、量子コンピューティングにおいては、量子ハードウェアの進展が著しく、まだデファクト標準もない多様な状況であるので、顕著にその影響を受ける。

可能性として最もあり得そうなのは、超伝導トランズモン量子ビットやトラップイオン量子ビットが様々な理由から大規模化に適してないと判断されることだ。そのときには、

量子ドット、冷却原子、光、核スピン、欠陥、マヨラナフェルミオンなど、それまでとはかなり異なった制御方法や構造をもつ量子系を用いることになり、コンパイラやアセンブラが吸収できる許容範囲を超えるかも知れない。制御・測定のレベルで見て似ている量子系どうしであれば、高級言語で書かれたプログラムの新環境への移行はそれほど困難でないようにも思われる。

しかし、計算原理としても現在の量子回路型（ゲート式）が大規模な量子計算を行う観点からは必ずしも良いモデルではないと判断され、より実装性の高い計算モデルへの移行が生じた場合には、もはやこれまでの量子回路型むけのソフトウェアスタックの大半を諦める必要が出てくる。測定型量子計算モデルや断熱量子計算モデルなど計算能力としては等価な複数のモデルの提案があり、現在積み上げられている量子ソフトウェアの多くは、このようなモデルでの計算はまったく想定されていない。さまざまな可能性を十分に残して研究開発を進めておくのが、現時点での最良の対処法だろう。

3.3.2 高性能 NISQ シミュレーター

現在公開されている多くの量子 SDK には、バックエンドとして量子コンピューターのシミュレーターが含まれている。これらのシミュレーターはクラウド上で実行されるものと、手元の PC で実行されるものとの両方がある。量子ビットのふるまいの高精度シミュレーションは負荷のかかる計算であり、総じてクラウド上シミュレーターのほうが高性能である。IBM の QISKit には、ローカルの PC 上で動作するシミュレーターが 2 種類（python 製と C++ 製）付属しているが、クラウドで提供されているシミュレーターであれば対応できる 32 量子ビットなどという規模の計算はローカル PC では難しい（もちろん PC の性能に依る）。

シミュレーション可能となるビット数は HPC リソースの利用により 50 量子ビット程度までは拡大可能と考えられる。また、シミュレーションする量子コンピューターの振る舞いをある程度制限する（例えば、ランダム回路のみ）ことで、ビット数や計算精度を維持しながら計算負荷を下げる近似コンピューティングも可能と思われる [47]。

また、より実際の NISQ デバイスの状況（エラー率のバラツキや結合性）を反映したシミュレーターが必要である。このようなシミュレーターで必要な計算のうちのいくつかは、FPGA で試行したうえで、専用ハードウェアアクセラレーターで計算する、というような研究開発も可能であろう。優れたシミュレーターは、実用的な量子ソフトウェア開発だけに限らず、古典アナログ制御系や他の量子情報デバイス（量子センサー、量子通信機器）とのシステム化・統合化など、量子 ICT 機器の設計支援なども視野に入ってくる。

3.3.3 量子情報機器との複合システム開発

NISQ 量子コンピューター単体ではなく、量子センサーや量子中継器などの技術の進展にあわせ、量子情報機器と NISQ 量子コンピューターを組み合わせた複合システムも可能となる。量子情報を量子情報のまま処理するのは、原理的に古典コンピューターの扱えない領域であり、NISQ 量子コンピューターのアナログ性を活かしたキラーアプリケーションが見つかる可能性は高い。

量子情報の入出力を扱うことができれば、例えば、量子センサーからの量子情報を量子情報のまま量子レジスターに書き込み、NISQ 量子コンピューターで計算（古典コンピュー

ターによる量子レジスターの制御・測定）を行い、場合によってはその計算結果を量子情報のまま出力して量子センサーにフィードバックするようなシステムも可能となる。

現在の NISQ 量子コンピューターの計算モデルは、量子レジスタを古典制御して情報処理するマシンである QRAM モデル（Quantum random access machine）であり、命令やデータの入出力は古典コンピューターを介して量子レジスタに書きこまれる [44, 45]。そのため、量子センサーからの量子情報をそのまま量子レジスターに入力したり、量子コンピューターによる処理結果を量子情報として出力したりは想定されていない。

そのため、計算モデルのレベルから、量子・古典ハイブリッド計算機システムの設計・開発をサポートするようなソフトウェア・プラットフォームが必要である。古典・量子ハイブリッドシステムで量子の力を引き出し役に立つ応用に使えるようにするには、ソフトウェアとしてどのように取り扱うかが極めて重要である。量子センサーや量子通信機器などの量子情報処理モジュールとの間の相互作用最適化も必要になる。そのために必要な制御ソフトウェアや、設計に必要となるリソース推定・検証ツール、量子情報制御言語（量子 VHDL）、様々なレベルでのシミュレーターも不可欠である。また、これらを支える設計指針となるようシステムズエンジニアリングを量子版にアップグレードする必要も出てくる。ドメインスペシフィックアーキテクチャ（必要な計算・処理に対する計算機アーキテクチャの最適化）の考え方も取り入れ、ソフトウェア・ハードウェアのコデザインで臨みたい。

3.4 量子誤り訂正符号に基づく量子コンピューターアーキテクチャ設計

3.4.1 量子誤り訂正符号

エラー耐性量子コンピューターのアーキテクチャ設計では、どのような要素で構成するか、それぞれの要素をどのレベルで抽象化するか、各要素をどのように相互作用させるか、に複雑な制約条件のもとで一定の答えを出すことが求められる。

エラー耐性量子コンピューターのアーキテクチャ設計を左右する最も大きな要素は、量子誤り訂正符号である（図 2.4）。量子誤り訂正符号の方式の選択が、システム構成と各要素のトレードオフを決定するだけでなく、物理量子ビットのレイアウトや接続性など抽象度の低いレベルまでも深く影響を及ぼす。

物理量子ビットの誤りは原理的に避けられないが、たとえ物理ビットに誤りが生じても、システム全体として論理的な誤りが起こらなければ良い。このような考えのもと、たくさんの物理量子ビットの量子状態に論理量子ビットの状態を埋め込むことで冗長性を確保し、エラーの起きたビットを随時訂正することで、論理的なエラーが生じにくい論理量子ビット上で量子計算を行う方法が多数考案されている。

量子誤り訂正技術の初期には、物理ビットに許容されるエラー率はハードウェア性能の状況からは非現実的な値だったが、近年は 1% 程度という現実的な許容エラー率をもつ符号も登場した。このような量子誤り訂正符号の進展と、２章で紹介した超伝導量子ビット系の性能向上が重なり、いよいよ、エラー耐性量子コンピューターにむけたスケールアップを技術的な側面から議論できるようになってきた。

現在最も有望視されているエラー耐性量子計算モデルは、トポロジカル誤り訂正符号を持つ計算モデルである [48]。アプローチ方法は大きく分けて物性アプローチと情報アプ

表 3.2: 量子誤り訂正符号の種類としきい値

	エラー耐性閾値		Single-shot 誤り訂正	符号上でサポートされる論理演算
	（現象論）	（回路）		
Steane符号	~0.01%			
2D 表面符号	2.9%	0.6-1%	不可能	Clifford
2D ヘキサゴナルカラー符号	2.8%	0.3%	不可能	Transversal Clifford
3D ゲージカラー符号	0.31%	-	可能	Transversal Clifford
3D カラー符号	-	-	不可能	Transversal T, S, CNOT
4D 表面符号	1.59%	-	可能	-

ローチの２種類がある。物性アプローチは、マヨラナフェルミオンなどのエニオンと呼ばれる準粒子をナノ構造中に生成しブレイディングと呼ばれる特殊な操作をすることで量子計算を行う方法だが、まだエニオンの操作が実証できていない状況である。一方の情報アプローチは、トポロジカル量子誤り訂正符号によって多数の物理量子ビット上のトポロジカルな性質に論理ビットの情報を埋め込み、その上で量子計算を行う方法である。たくさんの量子ビットが必要になるというデメリットはあるものの、その原理的な基礎はほぼ確立している。現在考案されているスケーラブルな量子コンピューターアーキテクチャのほとんどは、トポロジカル量子計算モデルによるものである。

２次元表面符号

有望視されているトポロジカル量子誤り訂正符号の一つは、２次元表面符号と呼ばれる符号で、2 次元面の正方格子状に配置された複数の物理量子ビットの上で動作する。この誤り訂正符号は、許される物理エラー閾値が約１% と高く、エラーの検出・訂正に最近傍の量子ビットの間での２量子ビットゲートまでしか必要としないため、ハードウェアとして実装しやすいことが特徴である。

また、エラー耐性を決めるファクターである符号距離[6]を大きくしたいときに、二次元正方格子の各辺をそのまま伸ばせばよいという、高い拡張性もハードウェア実装を惹きつけている要因だ。

50 ～ 100 個程度の量子ビットの NISQ 量子コンピューターは、このような２次元表面符号による量子誤り訂正の実現可能性をテストするのに重要な意味をもつ。超伝導量子ビットを用いて単に２次元表面符号が設計通りに働く実証実験するだけではなく、スケールアップする方法への洞察も得られるはずである。ただし、そのためには、（少なくとも超伝導量子ビット系では）中央部にある量子ビットへのアクセス・配線、ジョセフソン接合の精度、極低温システム環境のエンジニアリングなどのハードウェアの課題を解決してゆくことが求められる。

T ファクトリー

表面符号をはじめとしたトポロジカル量子誤り訂正符号で作り出した論理量子ビット上

[6] 符号距離を大きくするほど、エラー耐性は上がる。例えば、符号距離が２の表面符号ではエラーの検出しかできないが、符号距離７であれば１論理ビットを構成するために必要な複数個の物理量子ビットのうち３つまでの物理エラーであれば論理エラーは生じない。

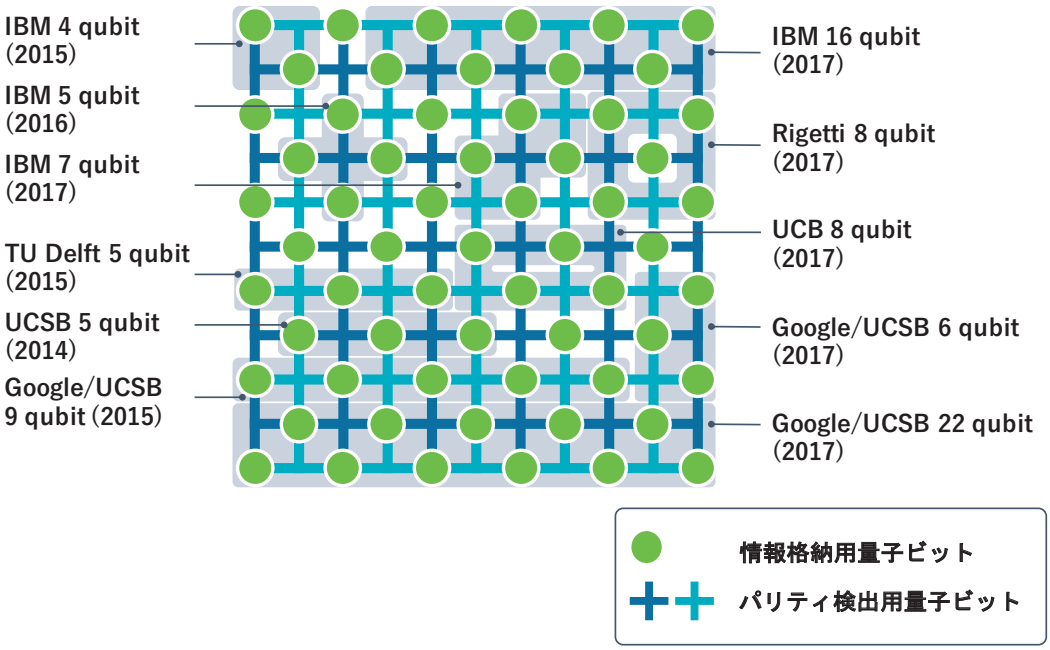

図 3.2: 2 次元表面符号を狙う超伝導量子コンピューター研究グループ

では、実は実装できる論理ゲート操作の種類が非常に限られてしまう。エラー耐性量子コンピューターがどのような量子計算も任意の精度で行うことができる[7]ようになるには、T ゲートと呼ばれるゲートが必要だが、トポロジカル量子誤り訂正符号上で T ゲートを直接実行することは不可能になっている。

この問題の解決策の一つとして、魔法状態と呼ばれる特殊な量子状態を一時的に準備し、それを消費して T ゲート操作を実行する方法がある。魔法状態もやはりエラーを含んでいるため、多くの魔法状態を作って「蒸留」と呼ばれる手順によってそれらを比較して、計算に注入するのが安全ないくつかの魔法状態を見つけることが必要になる。実際はこの手順は効率が悪く、エラーのない少数の魔法状態を得るためだけに、量子コンピューターのリソースの大半を費やすこととなる。その負担は、リソースの 90% 以上にも及ぶという推定もある [49]。

このように、T ゲートにかかる魔法状態の生成スピードは、エラー耐性量子コンピューター全体の性能の大半を決めてしまうと考えられている。表面符号は現在のところハードウェア実装容易性の観点からは魅力的な誤り訂正符号だが、論理ゲート操作のオーバーヘッドとのトレードオフを考慮の上でアーキテクチャ設計に取り入れるべきである。また、T ゲートがもともと実行可能な新しい誤り耐性符号の開発や、魔法状態蒸留のための要件を軽減するような新しいプロトコルの開発も進めるべき研究開発課題である。

また、このような事情から、単純に必要ゲート数を見積もるだけでは不十分で、むしろ必要となる T ゲート数こそが重要な計算リソース推定になっているとする考え方もある。つまり、アルゴリズムを量子回路として書き下す際に、なるべく T ゲートを少なくするように最適化する必要がある。このような T ゲートの数に基づく計算複雑性は T ゲート複雑性などと呼ばれ、誤り訂正符号上で機能するさまざまなアルゴリズムについて議論が

[7] ユニバーサリティ、万能性とも呼ぶ

されており、今後も注目すべき研究開発課題のひとつである。

3.4.2 ゲート分解・量子回路最適化

アーキテクチャ設計の観点からは、各要素をどの程度抽象化し、抽象度の異なる要素間をどのようなインターフェースで繋ぐかも重要な研究開発課題である。エラー耐性量子コンピューターでは、先に見たような誤り訂正符号による物理ビットの論理ビット化という抽象化と同時に、ゲート操作の抽象度も変化している。

最も抽象度の高いレベルである量子アルゴリズムから、抽象度の低い方向（ハードウェア側）を眺めると、アーキテクチャ設計として解決すべき研究開発要素がいくつか見えてくる。

まず量子アルゴリズムに登場する連続量でのゲート操作（回転操作など）を有限精度の離散的な操作に分解する必要がでてくる。これはいわばアナログ値のデジタル表現であり、要求される精度にもよるが、１つの連続量ゲートを再構成するのには多数のゲートが必要となる。精度に応じた最適なゲート分解を行うアルゴリズム [50] は提案されているが、このような最適化を行うソフトウェア（コンパイラ）は未発達のようである。

さらに、これらのゲート列を量子誤り訂正符号上で実装できるゲート列に分解する必要がある。前節で見たように特定のゲートは高コストであることから、この利用をなるべく避けるような最適化や、魔法状態の生成のために必要な無数のゲート列まで含めてトポロジカル構造へマッピングしたときの、トポロジカル量子回路全体の最適化は欠かせない。トポロジカル回路を最適化することで計算を高速化し、必要なリソースを低減できることも報告されている [51]。この圧縮した量子回路がはたしてもとの量子回路を正しく実装できているかどうか、将来的には検証ツールも必要となる。

3.4.3 古典・量子マイクロアーキテクチャ

現代のコンピューターにおけるアーキテクチャ設計の役割と同様に、量子コンピューター開発においても、各要素間のトレードオフの見極めと解決（妥協）は重要である。エラー耐性量子コンピューターは、古典・量子モジュールを両方とも持つようなハイブリッドシステムであり、その効率的なアーキテクチャ設計には、量子コンポーネントと古典コンポーネントとの間の相互作用を最適化する必要がある。

エラー耐性量子コンピューターの計算性能に大きな影響を及ぼす重要な要素は、誤り訂正に必要な計算（古典の情報処理）の速度である。誤り訂正符号上で実行されるゲート操作のサイクルは、もともとの物理的な量子ゲート操作のサイクルとは一致せず、誤り訂正の処理の分だけ余分に時間がかかる。具体的には、エラーを検出するために物理量子ビットの測定を行い、その測定結果を解析して、誤り訂正の制御信号を量子ビットに送り返す必要がある。このときのデータ量は、物理量子ビット数やモジュールのクロック周波数に依存するが、トポロジカル量子誤り訂正符号を用いたエラー耐性量子コンピューターで 2048 ビットの Shor のアルゴリズム（因数分解）を実行する場合には数 10 ペタバイト秒のデータを転送・解析する必要もでてくるとされている [32]。

クロック周波数は、誤り訂正符号そのものと同様に、アーキテクチャに依存する部分が大きい。Clark らの分析では、イオントラップ量子ビットが 7 ビットある系で Steane 符号と呼ばれる誤り訂正符号を用いた際に、物理的な量子ゲートのサイクルが 10 マイク

ロ秒、誤り訂正のサイクルが 1.6 ミリ秒のときに、論理ゲートのクロックサイクルは 260 ミリ秒に膨れ上がると示唆されている。周波数で表現すると約 4Hz であり、現代のコンピューターが数 GHz のクロック周波数で駆動していることを考えると、これは極めて低速である。

量子ビットの測定データを古典の処理系に送るのに必要なバンド幅をどう確保するかは、ハードウェア的な研究開発課題である。しかし、量子ビットが希釈冷凍機内に置かれている状況では、打てる手は制限される。測定データから誤りの場所を推定するアルゴリズム（最小重み完全マッチングアルゴリズム）が知られているが、エラー率が高い場合でのエラー位置推定の精度をソフトウェアとして実行するシミュレーション研究も必要である。

量子ビットの測定・制御・ゲート操作は、論理的な量子回路に基づく命令とアナログの制御信号とをエンコード・デコード処理することで行われる。現在のアナログ・デジタル変換や信号処理技術の援用も期待できる。量子コンピューターのクロック周波数が低く、サイズも大きくない現状では問題は顕在化しないが、量子誤り訂正の処理を担う古典コンピューター部分のハイスループット化は長期的に見て必要な研究開発要素である。既存の（必ずしも量子コンピューター向けではない）技術の利用によって活路が見いだせる可能性や、FPGA などの高性能化にもかかっている。

中長期的に見ると、現在提案されているゲート方式のデバイス・システムでは、そのままビット数を 10000 量子ビットまで拡大するようなことは不可能と思われる。エラー率の面で最も基礎技術的に進んでいるとみられる超伝導トランズモン方式（IBM、Google、Rigetti などが採用）は冷凍機で 10mK 温度環境下にチップをおかねばならない点がボトルネックとなる。物理的には 10mK の冷凍機環境にチップを収めることは可能だろうが、エラー訂正の制御信号の計算は冷凍機の外にある古典計算機が行うので、高バンド幅の通信を冷凍機の内外で行う必要が出てくる。Cryo-CMOS やジョセフソン接合など、低温で動作する情報処理モジュールを、極力量子ビットの近くに置くというのがハードウェア的な戦略となる。

検証、デバッグ、シミュレーションは量子デバイスが正しく動作するために不可欠だが、まだ新しい理論アイディアが必要である。サイズが大きくなるにつれ、古典計算機で量子デバイスを第一原理的に全てシミュレーションすることは困難になる。テストは一般的に設計後の課題とされてきたが、古典デバイスがそうであるように、性能だけでなく、テスト容易性も重要な設計与件になると予想される。小さな量子デバイスのブートストラップで大きなものをテストし、暗号ツールキットを使用して正直な動作を強制するなど、ソフトウェア工学的なアプローチも求められる。

ある程度実用問題を想定したベンチマークツールも必要である。セキュリティや安全性などが重要なアプリケーションでは、プログラムとプロトコルの正式な検証が最も重要視される。関数型プログラミング言語の形式検証で攻めるというのが正攻法だが、量子プログラムの場合にどのように検証するか、新しいアプローチが必要である。また、量子コンピューターはクラウド上にあり実際の手元にはハードウェアがない場合がほとんどであろうから、クラウド上の量子コンピューターが期待通りに正しく動作しているかどうか検証する方法論やブラインド量子計算の実行と検証方法の構築も必要となる。

4．研究開発の推進方法および時間軸

4.1 分野融合・企業参画・国際連携の促進

本研究開発の推進においては、様々な方策を駆使して量子ソフトウェアから量子デバイスまでの技術スタックを上から下まですべて用意し、垂直統合的に研究開発を進めることが必要となる。特に、分野融合・企業参画・国際連携それぞれの局面で様々なプレーヤーがそれぞれ必要とされる役割を担う“みんなの”量子コンピューター研究開発が重要である。

これまで、量子情報処理分野は物理学の一分野として成長を続けてきたが、これからの量子コンピューター研究開発は、コンピューター科学、電子工学、数学、材料科学などの多様な学問分野に基礎を置く研究者や技術者の協働・触発が必要となる。知見、技術、人材など量子コンピューター実現のために必要なあらゆることを、学問分野や所属の壁を越えて交流することが必要である。また、量子コンピューターだけでなく、量子センサー、量子暗号・量子通信、量子メトロロジー、量子シミュレーションなど量子情報科学分野の中での融合・連携も重要である。

計算機システムとして組み上げる技術・ノウハウ・人材の多くは民間企業にあるため、フルスタックで用意された要素技術群の統合化には大学や公的研究機関と民間企業との深いレベルでの産学官連携がカギとなる。また、ひとつの研究チームはおろか研究所レベルでもフルスタックの技術を全て用意するのは困難であり、スタートアップや海外の研究チームとの共同研究や技術の相互提供、オープンソースコミュニティの活用などの形で、不足部分を補うことも不可欠である。

全体としては量子コンピューターアーキテクトが指揮をとり研究開発を進められるよう、研究者の発想を活かした散発的な研究支援だけでなく、異分野融合を促進する目的志向のグラントもしくは研究プロジェクトも必要である。

今後投じることが可能な予算規模が小さい場合には、シミュレーターを活用したアルゴリズム研究およびアーキテクチャ研究と、量子コンピューターエンジニアの育成から優先的に取りかかるべきである。特定のハードウェアプラットフォームに集中投資するのは、アルゴリズムの有望性やスケールアップ設計指針が明らかになってからでも遅くはない。ソフトウェア研究やアーキテクチャ研究は、限られた予算で効率的にハードウェア研究を加速することができる。

量子ソフトウェア研究開発を担うハブ拠点のタイムラインは、１～４年目にシミュレーターをバックエンドとして利用したアプリケーション・アーキテクチャ探索、５～８年目には実機のバックエンド利用開始、９～１０年目には継続的な自立運営にむけた資金調達などを行うといった流れが考えられる。ただし、既存のリソースの状況や技術蓄積などにも依存するほか、拠点の特性によっては、研究開発以外へのエフォートが大きくなる場合もあり、様々な拠点やプロジェクトを横一列でゲート管理などするのは困難である。エラー耐性量子コンピューターの実現は長期的なテーマであり、それまでの間の研究開発のドライビングフォースとして、NISQ 量子コンピューターのキラーアプリを探索することは重要である。エラー耐性量子コンピューター開発に向けた計画を精緻化し、ハードウェア・ソフトウェア技術の現状と進展予測と照らして現実的なスケジュールを引くこともこの期

間での重要な研究開発項目となる。

4.2 量子コンピューター研究開発ネットワークとハブ拠点

量子コンピューターの研究開発にはハードウェアからソフトウェアに至るまでの必要な全ての技術を用意することが必要となるが、それらに関わる機器や人材を物理的に１ヶ所に集合させることは現実的ではない。この事情は他国の研究機関でも程度の差こそあれ同様である。したがって、多様な研究開発拠点やチームから成る量子コンピューター研究開発ネットワークを構築するとともに、その効果的・効率的な連携・協調動作のためのハブとなるような拠点も複数必要となる。

国内には有望な研究チーム・研究拠点・研究者が数多くあるが地理的に点在し、かつ、分野としても物理学、コンピューター科学、電子工学などに分散している状況である。近年、文部科学省「光・量子飛躍フラッグシッププログラム（Q-LEAP）」、CREST「量子状態の高度な制御に基づく革新的量子技術基盤の創出」、さきがけ「量子の状態制御と機能化」領域などで量子技術の研究開発支援が進められており、これらのグラントをうけた研究拠点・チームは本プロポーザルで想定する量子コンピューター研究開発ネットワーク中の重要なノードとなる。また、すでに量子技術に関する研究開発センターを内部に有する国立情報学研究所（NII）や情報通信研究機構（NICT）、半導体や計算機に関する研究開発拠点をもつ理化学研究所や産業技術総合研究所などのイニシアティブも求められるところである（図 4.1）。

研究開発テーマの性質からは、量子ソフトウェア研究開発に関する部分はある程度集合してハブ拠点を形成し、ハードウェア依存性の高い研究開発については分散のままハブ拠点との連携によりフルスタックの技術を用意できる体制を構築するのが効率的である。また、このようなハブ拠点には、次節で述べるように量子コミュニティ全体の研究・教育活動のために必要となるプラットフォームや教育・訓練コンテンツ、サービスの提供といった事業を担う役割も期待したい。とくに、量子ソフトウェア開発環境の提供や高機能なシミュレーターのクラウド公開、ツールやライブラリなどの管理・維持・利用支援など、大学附置研究所だとしても共同利用施設としての機能が求められる。

海外から有力研究者を招聘した際に日本国内の研究者へと取り次ぐような国際連携に長けた物理的なハブ拠点も考えられる。トップレベルの研究者の短期滞在を可能とすれば、共同研究の形で国内の量子コンピューター研究や教育をエンカレッジするといった利用方法も可能となる。招聘される研究者にとっての魅力の一つは、多様な研究者・技術者との議論・交流の機会の多さであろうから、このような拠点は、大規模な研究大学の中に何らかの拠点的機関として設置されるのが望ましい。

またその上で、量子情報処理の教育・訓練プログラムの開発・提供、正確で積極的なアウトリーチ・科学広報、量子スタートアップ企業の積極的支援など、多様な施策により、持続性あるネットワークを構築してゆくことが求められる。

4.3 コミュニティ・エコシステムの醸成

研究開発プロジェクトや研究開発ネットワークの成功は、量子コンピューター研究開発

のコミュニティに登場するプレーヤーの充実・多様化と、それらがエコシステムを形成して様々な役割で機能することにかかっている。したがって、単にグラントによる研究資金の提供や研究開発拠点の設置だけでなく、エコシステムの構築を志向した総合的な施策が重要である。

プレーヤーとして従来の科学技術政策の枠組みで扱われてきた研究大学や大企業だけでなく、量子ソフトウェアではスタートアップやオープンソースコミュニティといった非従来型プレーヤーが重要な役割を担うエコシステムが出現しようとしている。シミュレーターやコンパイラなどのツールキットの充実は、コンピューター科学や電子工学の専門性を持った多くの人の参入を促進する意味でも重要である。

とりわけ、量子ソフトウェアにおいては、学術的な量子ソフトウェア研究者と産業界との多くの共同作業が急務と思われる。学術研究者は量子コンピューター利用にメリットがある現実の問題の種類について理解を深める必要がある [52]。また、量子コンピューティング分野に進出してくる産業界の研究者・技術者は、学術研究者との交流から、量子コンピューターの可能性と限界の両方をよりよく理解し、その経験を活かして、量子コンピューターを含む量子 ICT 分野での短期的または長期的な投資判断を下すことが求められる。

２章で見たように、IBM、Google、Microsoft などの大企業は量子ソフトウェア開発プラットフォームを公開し、スタートアップを含むエコシステムを囲い込むような戦略の実行に着手しつつある（図 2.3)。量子誤り訂正符号の方式や量子デバイスにはまだ決め手はなく、このエコシステムは当面は多様化が進むだろう。NISQ 量子コンピューターについても、未だ見ぬキラーアプリケーションの発見はエコシステムに大きな波を立てると考えられる。今後は、量子コンピューターを利用する産業と製造する産業の両面で、中長期的な視点からの産業政策が重要となる。高性能の量子ハードウェアが開発可能となったとしても、その上で動く量子ソフトウェアとセットで、あるいはサービスとして商業化するアプローチが必要となる。我が国の存在感の向上とともに、産業競争力の強化に向けて、知財化、IP コア化、パテントプール化、オープン・クローズ戦略、国際標準化などの戦略的取り組みを駆使して臨みたい。

4.4 量子コンピューター教育・訓練

量子コンピューティング分野が直面している課題の 1 つは、量子ソフトウェアの作成・開発の訓練を受けた人材の不足である。量子コンピューターだけで無く、量子情報処理技術全体での量子エンジニアも不足している。量子ソフトウェアのプログラミングには、波の干渉や重ね合わせなど古典的プログラミングとは根本的に異なる部分があり（かつその性質こそが量子計算の指数関数的な加速を実現する)、ルールに慣れた人材の養成は量子コンピューターの社会インパクトのカギを握っている。

量子コンピューターをプログラミングするのに十分な知識を持っている人材のプールは小さいため、大学と企業の両方で教育・訓練プログラムを開発してゆく必要がある。教科書、大学での講義、オンラインコースのほか草の根的な勉強会など初動は開始されているが、量子コンピューティングや量子ソフトウェアのための学術・産業でのカリキュラムはまだ未熟な段階と言えよう。

短期的には、NISQ 量子コンピューターの潜在的なアプリケーションを考える必要があ

る。NISQ 量子コンピューターによる情報処理からどのような問題が実際に恩恵を受けるのか、どのようなアプリケーションが最も有用であるのかを発見することと、これらの問題を解決する新しい量子・古典アルゴリズムの開発は急務である。これには教科書やオンラインコースだけでなく、ハンズオンのトレーニングプログラムも必要だ。ただし、カリキュラムに固定して広く高等教育を進めるというまでには成熟しきっておらず、研究開発と同時並行での人材育成となる。

今後 50 年の間には、量子コンピューターだけでなく、量子センサーや量子インターネットなどの量子科学技術と組み合わせた「量子 ICT」を自由自在に使いこなす時代となる。従って、高度な基礎科学的成果を理解し、それを起点にしながらも量子システムインテグレーションして価値形成できる量子アーキテクト人材の育成を今すぐにスタートしなければならない。そのような人材育成は、「我が国の大学で実行する」ものと、「一人でも多くの日本人を世界に飛立たせる」ものの 2 本立てで実行すべきであり、そのような科学技術政策の企画・実行を期待したい。

学界と産業界が、今後も成長を続ける量子技術産業の中での仕事に適した教育・訓練プログラムを開発するために協力しなければならない。これにより、量子技術の品質管理、ソフトウェアエンジニアリング、コンサルティングなどに関するスキルが明らかになるとともに、その品質基準を確実に満たすようになると期待される。量子 ICT 技術者を必要とする組織とそれらを教育できる組織との間での緊密な連携が、長期的に見て必要なのは明らかである。

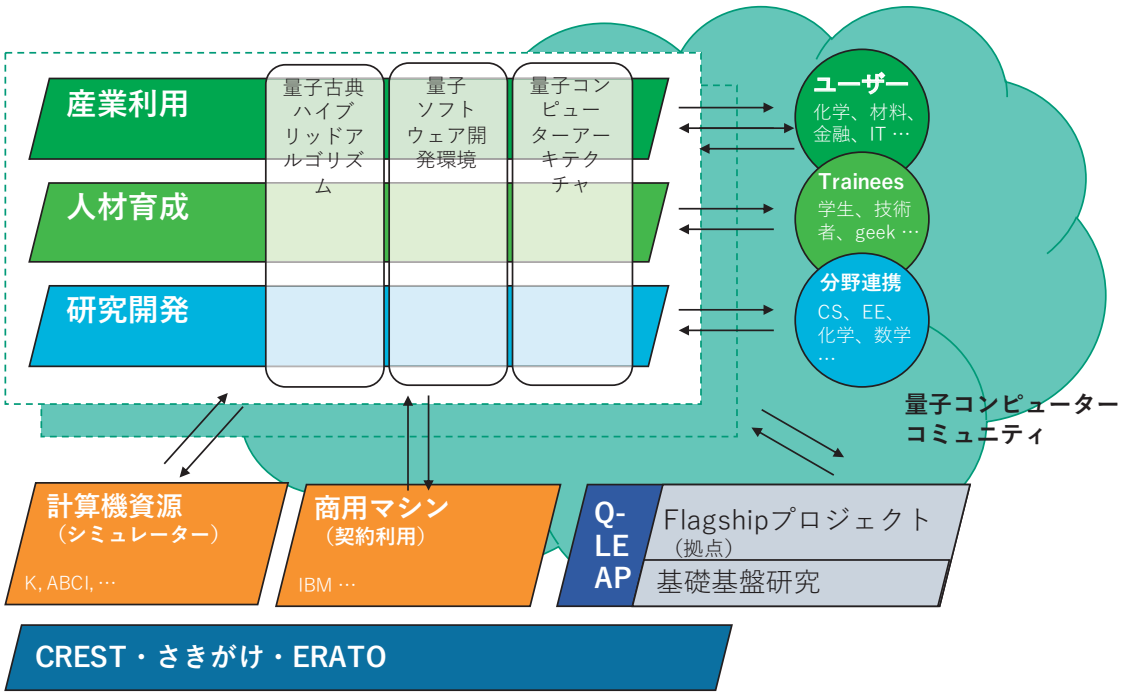

図 4.1: 量子コンピューター研究開発ネットワークのハブ拠点イメージ

付録A　検討の経緯

国立研究開発法人科学技術振興機構（JST）研究開発戦略センター（CRDS）では、2018 年度の戦略スコープ策定委員会において、本テーマを戦略プロポーザルを作成すべきテーマの候補に選定し検討チームを発足させた。検討チームは 2018 年 4 月から活動を開始、半年間に渡り検討を進めてきた。その間、以下のようなインタビューとワークショップを開催し、研究開発状況の把握や研究課題・方向性の議論を深めてきた。

A.1 インタビュー

本プロポーザル作成にあたり、研究内容や推進体制、国内外動向について関連する研究分野に高い専門性を有する有識者への個別インタビューを実施した。インタビューに協力いただいた専門家は表 A.1 のとおりである（インタビュー実施日時順、敬称略、所属・役職はインタビュー実施当時）。

A.2 科学技術未来戦略ワークショップ

本プロポーザル作成にあたり、下記の通り、科学技術未来戦略ワークショップを開催した。詳細についてはワークショップ報告書を参考されたい。

概要

日時：2018 年 8 月 17 日（金）10:00 ～ 17:30
場所：JST 東京本部別館 2 階セミナー室
主催：国立研究開発法人科学技術振興機構研究開発戦略センター（CRDS）

招聘有識者

井上 弘士（九州大学システム情報科学研究院教授）
田中 宗（早稲田大学グリーンコンピューティングシステム研究機構主任研究員）
田渕 豊（東京大学先端科学技術研究センター助教）
根本 香絵（国立情報学研究所情報学プリンシプル研究系教授）
平木 敬（東京大学大学院理学系研究科特任研究員）
藤井 啓祐（京都大学大学院理学研究科特定准教授）
望月 祐志（立教大学理学部化学科教授）
山崎 清仁（OpenQL Project）
廣川 真男（広島大学大学院工学研究科教授）
楊 天任（株式会社 QunaSys CEO）

プログラム

10:00 ～ 10:10　開催挨拶・参加者紹介
10:10 ～ 10:25　趣旨説明（問題意識、論点、プロポーザル骨子の説明）
（招聘者からの発表　30 分 / 人＝発表 15-20 分＋残りは質疑・討論）
10:25 ～ 12:45　量子コンピューティング コンピューター科学
10:25 ～ 11:00 田渕 豊（東京大学）

11:00 ～ 11:35 根本 香絵（国立情報学研究所）
11:35 ～ 12:10 平木 敬（東京大学）
12:10 ～ 13:00（昼食休憩）
13:00 ～ 13:35 井上 弘士（九州大学）
13:35 ～ 14:10 山崎 清仁（OpenQL Project）
14:10 ～ 14:20（休憩）
14:20 ～ 16:05　量子コンピューティング 機械学習・量子化学
14:20 ～ 14:55 藤井 啓祐（京都大学）
14:55 ～ 15:30 望月 祐志（立教大学）
15:30 ～ 16:05 田中 宗（早稲田大学）
16:05 ～ 16:20（休憩）
16:20 ～ 17:20　総合討論
17:20 ～ 17:30　ラップアップ

表 A.1: インタビューした有識者

氏名	所属・役職	ｲﾝﾀﾋﾞｭｰ日時
中村 泰信	東京大学先端科学技術研究センター 教授	4月17日
藤井 啓祐	京都大学大学院理学研究科 特定准教授	4月23日
井上 弘士	九州大学システム情報科学研究院 教授	4月25日
湊 雄一郎	MDR株式会社 代表取締役	4月25日
伊藤 公平	慶應義塾大学理工学部 学部長・教授	4月26日
根本 香絵	国立情報学研究所 教授	4月26日
中井 浩巳	早稲田大学理工学術院 教授	4月27日
西森 秀稔	東京工業大学理学院 教授	4月27日
古田 彩	日経サイエンス 編集長	5月1日
山崎 清仁	OpenQLプロジェクト	5月7日
谷 誠一郎	NTTコミュニケーション科学基礎研究所 上席特別研究員	5月9日
杉田 有治	理化学研究所杉田理論分子科学研究室 主任研究員	5月16日
田渕 豊	東京大学先端科学技術研究センター 助教	6月5日
松岡 聡	理化学研究所計算科学研究センター センター長	6月5日
田中 宗	早稲田大学グリーン・コンピューティング・システム研究機構 主任研究員	6月7日
根来 誠	大阪大学大学院基礎工学研究科 助教	6月14日
中前 幸治	大阪大学大学院情報科学研究科 教授	6月22日
合原 一幸	東京大学生産技術研究所 教授	6月27日
平木 敬	東京大学大学院理学系研究科 特任研究員	6月29日
望月 祐志	立教大学理学部化学科 教授	6月29日
三好 健文	わさらぼ合同会社 代表	7月2日
松田 佳希	株式会社フィックスターズ リードエンジニア	7月5日
石原 良一	デルフト工科大学電子数理情報工学部 准教授	7月30日
Rodney Van Meter	慶應義塾大学環境情報学部 准教授	8月7日

（敬称略、所属・役職はインタビュー時点）

付録B　論文で見た国内外の状況

B.1 量子コンピューター関連論文マクロ動向

量子コンピューターに関係する論文のマクロな動向を Scopus データベースで調査した。“quantum computer” をタイトル・アブストラクト・キーワードに含む論文・プロシーディングス・レビューを抽出し、図 B.1(a) と (b) に著者の所属機関の所在国別の整数カウント論文数とシェアの経年変化をそれぞれ示した。

2000 年頃から中国のシェアが拡大し、半数を占めていた米国からシェアを奪う形で 20% 程度のシェアとなった。ドイツ、イギリス、日本、カナダ、オーストラリアが続き、それぞれ約 100 報 / 年、シェアでは 6 ～ 10% で推移している。これら 5 カ国は中国が躍進した 2000 年以降も目立ったシェア低下は見られない。我が国の論文数シェアは一定程度認められる。

“quantum computer” を含む文献を母集団とし、さらにコンピューターサイエンスに関連する用語（algorithm, software, compiler, programming, architecture, instruction, circuit, device, processor）を含むものを抽出し、著者の所属機関の所在国別の整数カウント論文数とシェアの経年変化を図 B.1(c) と (d) にそれぞれ示した。以下では “量子コンピューター科学” 関連論文と呼ぶ。

量子コンピューター科学関連論文は、量子コンピューター関連論文よりも、中国からの寄与が減少しているが、米国のシェアも 30% 弱と少ないままである。ドイツ、イギリス、カナダなどについで日本も概ね 5% 程度のシェアを有している。

図 B.2 に、1996 年から 2016 年に発行された文献のうち、被引用数がトップ 10% となる論文の割合を、各キーワードごとに国別でまとめた。アルゴリズムは “algorithm”、ソフトウェアは “software”、コンパイラは “compiler” または “programming”、アーキテクチャは “ar-chitecture” または “instruction”、回路は “circuit”、デバイスは “device” または “processor” をキーワードとして含む論文である。バブルの大きさは 1996 ～

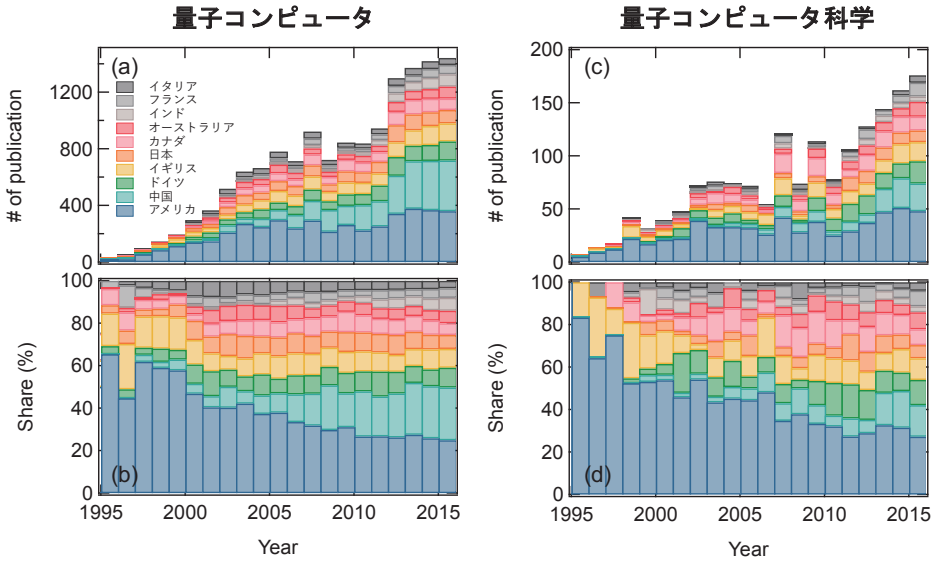

図 B.1: 量子コンピューター関連論文数の推移

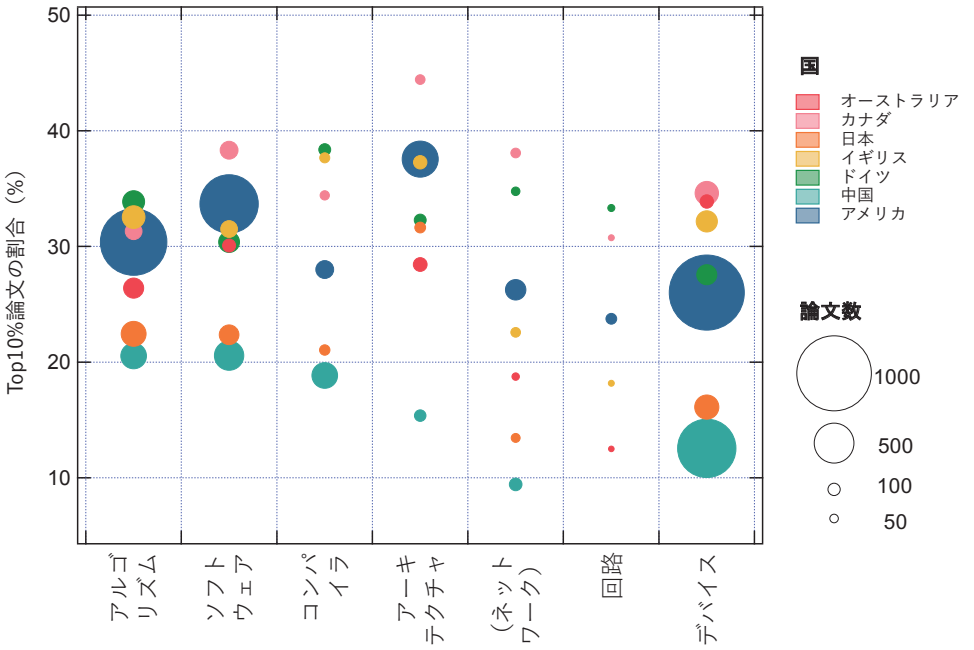

図 B.2: 量子コンピューター科学関連論文のトップ 10% 被引用論文割合の国際比較

2016 年の合計の出版数を表す。これをみると、アルゴリズム、ソフトウェア、デバイスのレイヤでは多数の論文が出版されているのに比べ、コンパイラ、アーキテクチャ、回路の論文数は少ない。参考までに“quantum communication”と“network”を含む文献を「ネットワーク」レイヤとしてプロットした。

国別では、ドイツ、イギリス、カナダのトップ 10% 被引用論文数の割合がどのレイヤでも高い。米国は必ずしも全レイヤでトップ 10% 被引用論文数の割合が高いわけではないが論文数では群を抜いている。この指標は、分母である総論文数が小さいと指標が高めに出やすい傾向があるが、図 B.1 で見たように、カナダの論文数はドイツやイギリスと同程度である。日本と比べても 2 倍の開きもないため、小さい分母によってトップ 10%論文割合が高く見積もられすぎているということはない。むしろ、米国やそのほかの国との国際共著論文が高い引用を得ていることが影響しているだろう。中国は論文数では米国に次いで 2 番手であるが、被引用数の面では見劣りする。日本は比較的得意分野と思われているデバイスでも、この指標では強みとして認識されない。むしろ、全体としてトップ 10% 被引用論文数の割合が他のレイヤよりも高いアーキテクチャレイヤで、世界水準についていっている様子がうかがえる。絶対数としては 20 年間でおよそ 100 報であり、他国と比べて極端に小さいということはない。

B.2 Quantum Algorithm Zoo から引用された論文

ウェブサイト Quantum Algorithm Zoo には量子アルゴリズムごとに複数の引用文献があり、2018 年 6 月調査時点では、引用論文は合計で 210 報であった。アルゴリズムの種類別に、引用されている論文の発行年ごとの推移を図 B.3(a) に示した。近年までに量子アルゴリズムの提案が毎年増加している様子が伺える。その内訳は図 B.3(b) に示したとおり大きくは変化しておらず、およそ半数がオラクルアルゴリズム、30% ほどが近似ア

ルゴリズム・シミュレーションアルゴリズム、残りが代数的アルゴリズム・数論アルゴリズムである。

所属機関が同定できた著者 351 名の国（所属機関の所在国）の分布を図 B.4 に示した。37% を米国が占め、国別ではカナダ、ドイツと続く。中国は Quantum Algorithm Zoo に登録されているアルゴリズム（に引用されている論文）の観点では米国には及ばない。機関別では Waterloo 大学（カナダ）や Maryland 大学（米国）、MIT（米国）などと並び、Microsoft（米国）、Google（米国）も顔を出している。

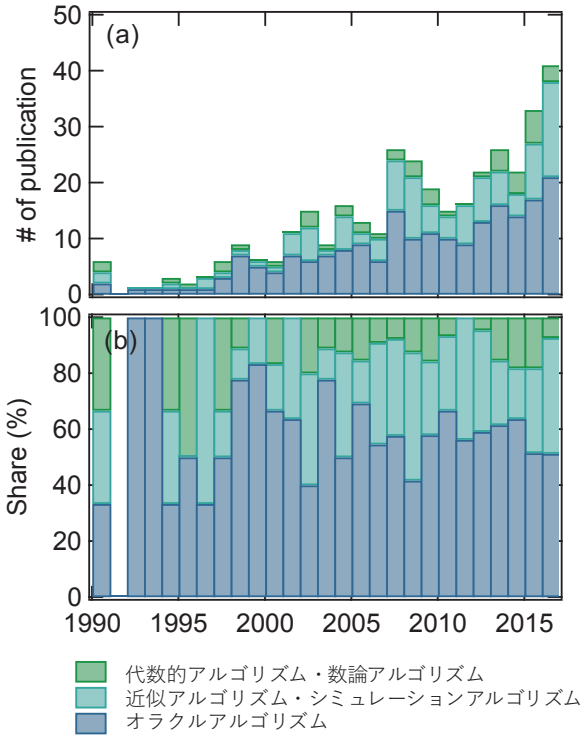

図 B.3: Quantum Algorithm Zoo から引用されている論文数の推移

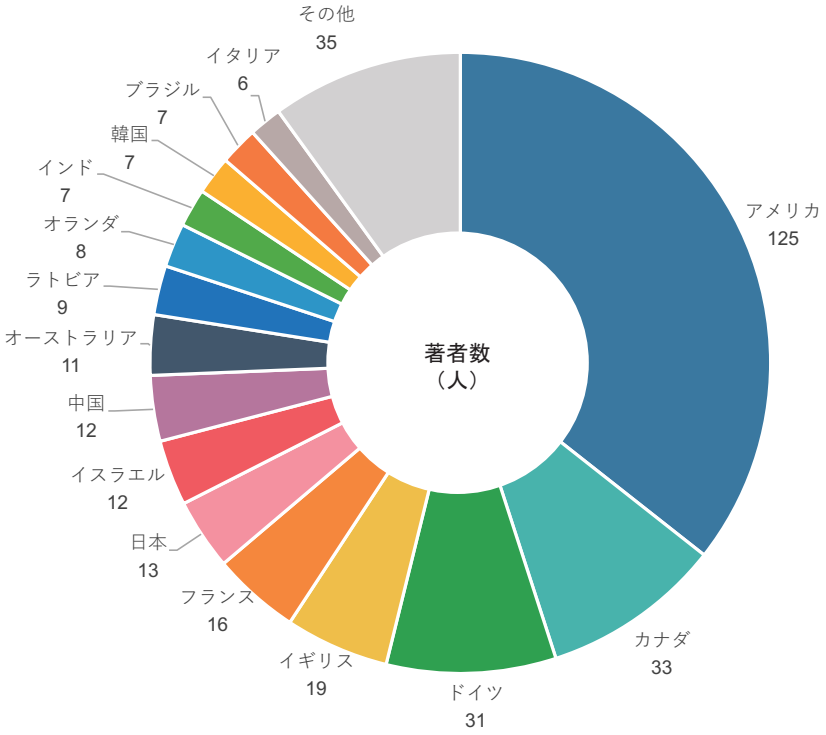

図 B.4: Quantum Algorithm Zoo から引用されている論文数の著者の国別内訳

付録C 専門用語説明

量子ビット：量子コンピューター上での情報の最小単位のこと。通常のデジタル回路では「０か１か」の２状態に情報が保持されるのに対し、量子ビットでは「０でありかつ１でもある」状態を任意の割合で組み合わせて表現することができる。

量子ゲート：量子ビットを操作するゲート演算。

量子アルゴリズム：量子コンピューター上で用いるアルゴリズム。アルゴリズムとは、コンピューターが問題を計算する方法や手順をいう。

量子もつれ：複数の量子ビットの間に生じる量子力学的な相関のこと。例えば、２つの量子ビットが各々「０または１」であるが、「一方が０のときに他方は１」であることは確定していて相関がある」ような状態を指す。量子コンピューターは、量子ビット間の量子もつれを利用して計算を進める。

デコヒーレンス：量子コンピュータは量子力学的な重ね合わせ状態を維持しながら計算を行うが、その重ね合わせ状態が維持できなくなることをデコヒーレンスという。エラー耐性量子コンピュータの実現にはデコヒーレンスが一定のレベルより抑えられている必要がある。

ユニタリー：量子ビットを操作する量子ゲート操作は行列による変換で表すことができる。変換の前後で確率の総和が１になることを保つため、行列に「ユニタリー性」という数学的な性質が要請される。

量子誤り訂正符号：雑音やデコヒーレンスによる量子ビットに生じる未知の変化を元の状態に戻す手法。古典的な誤り訂正と同様に冗長性を持たせ、複数の物理量子ビットを符号化して１つの論理量子ビットを構成する。

コンピューターアーキテクチャ：コンピューターの基本的な設計・構成・様式などを意味する。狭義には命令セットアーキテクチャを意味するが、マイクロアーキテクチャやシステムアーキテクチャなどの意味でも用いられる。

命令セットアーキテクチャ：機械語（アセンブリ言語）から見たプロセッサの抽象化されたイメージ。ソフトウェア側から見ると、命令セット、アドレッシングモード、レジスタ、アドレスとデータの形式などのインタフェース定義といえる。

プログラミング言語：コンピュータプログラムを記述するための形式言語。

コンパイラ：高水準のプログラミング言語で書かれたソースコードを、機械語（または、元のプログラムよりも低い水準のコード）に変換するプログラム。プログラミング言語を

処理する「言語処理系」のひとつ。

デバッグ：プログラムや電気機器中の欠陥（バグ）を発見・修正し、動作を仕様通りのものとする作業。サブシステムが密結合であると、1 箇所の変更が別の箇所でのバグを作り出すので、バグの修正がより困難となる。

ソフトウェア開発キット（SDK）：アプリケーションソフトウェアを作成するためにソフトウェア技術者が使用する開発ツールのセット。一般的には、統合開発環境、ライブラリ、デバッグ用ツールのほか、サンプルコードやサポートのための技術ノートなどを含む。

ハードウェア記述言語：集積回路を設計するためのコンピュータ言語ないしドメイン固有言語（DSL）で、回路の設計、構成を記述する。プログラミング言語とは異なる。

計算複雑性理論：計算に要するリソース（時間、メモリ、通信量など）について研究する学問分野。

P: 古典コンピューターで効率よく（問題サイズに対し多項式時間で）解くことができる決定問題（Yes か No で答えられる問題）の集合。P に属する問題は当然 NP に属すが、両者が一致することはないと信じられている（$P \neq NP$ 予想）。

NP: 効率的に解くのは難しいが、解の正しさの検証は効率よくできる決定問題の集合。例えば、全ての都市を一回だけ巡って戻ってこられるルートは存在するかという問題は、全てのパターンをしらみつぶしに調べると膨大な時間（指数時間）がかかるが、答えとなるルートの正しさは容易に検証できる。

BQP: 量子コンピュータによって効率的に（多項式時間で）解ける決定問題の集合。Bounded-error Quantum Polynomial time の頭文字をとったもの。BQP に属す問題については、多項式時間で実行可能な量子コンピュータのためのアルゴリズムが存在する。ただし、そのアルゴリズムは最大で 1/3 の確率で間違った答えを返す。

付録D 参考文献

[1] CRDS,『戦略プロポーザル　革新的コンピューティング　～計算ドメイン志向による基盤技術の創出～』, CRDS-FY2017-SP-02 (2018).
[2] IEEE Rebooting Computing, https://rebootingcomputing.ieee.org/
[3] T. M. Conte, E. P. DeBenedictis, P. A. Gargini, and E. Track, Rebooting computing: The road ahead, *Computer*, 50, 20 (2017).
[4] 阿部英介 , 伊藤公平 , 固体量子情報デバイスの現状と将来展望 , 応用物理 , 86, 454 (2017).
[5] 井元信之 , 北川勝浩 , エレクトロニクス技術を変革する量子情報技術 . 電子情報通信学会誌 , 100, 968 (2017).
[6] 古田彩 , クラウド時代の幕開け , 日経サイエンス , 2018 年 4 月号 , 48, 33 (2018).
[7] 野澤哲生 , “量子コンピューター” 続々役に立つのはどれか , 日経エレクトロニクス , 2018 年 2 月号 , 41, (2018).
[8] Quantum algorithm zoo, https://math.nist.gov/quantum/zoo/
[9] J. Preskill, Quantum computing in the NISQ era and beyond, arXiv:1801.00862 (2018).
[10] A. W. Harrow and A. Montanaro, Quantum computational supremacy, *Nature*, 549, 203 (2017).
[11] 株式会社フィックスターズ, Quantum computer information site, https://quantum.fixstars.com/
[12] 西森秀稔 , 大関真之 ,『量子アニーリングの基礎』, 共立出版 (2018).
[13] F. T. Chong, D. Franklin, and M. Martonosi, Programming languages and compiler design for realistic quantum hardware, *Nature*, 549, 180 (2017).
[14] J. L. Hennessy and D. A. Patterson, *Computer Architecture: A Quantitative Approach*, Elsevier, sixth edition (2018).
[15] R. Van Meter and C. Horsman, A blueprint for building a quantum computer, *Communications of the ACM*, 56, 84 (2013).
[16] M. H. Devoret and R. J. Schoelkopf, Superconducting circuits for quantum information: An outlook, *Science*, 339, 1169 (2013).
[17] D-wave systems inc., https://www.dwavesys.com/home
[18] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P.O ’ Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland, J. M. Martinis, Superconducting quantum circuits at the surface code threshold for fault tolerance, *Nature*, 508, 500 (2014).
[19] Quantum Computing for Business, https://www.q2b.us/
[20] 今道貴司 , 井床利生 , ルディー・レイモンド , 量子コンピューターを使ってみよう―qiskit を用いた量子プログラミングの紹介―,『オペレーションズ・リサーチ』, 2018 年 6 月号 , 350 (2018).
[21] 慶應義塾大学量子コンピューティングセンター , https://quantum.keio.ac.jp/

[22] American Physical Society, Division of quantum information, https://www.aps.org/units/dqi/
[23] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, Quantum supremacy and the complexity of random circuit sampling, arXiv:1803.04402 (2018).
[24] QISKit, https://qiskit.org/
[25] The Microsoft Quantum Development Kit, https://www.microsoft.com/en-us/quantum/development-kit
[26] Rigetti Computing, https://www.rigetti.com/
[27] Project Q, https://projectq.ch/
[28] IBM QISKit developer challenge, https://qe-awards.mybluemix.net/
[29] N. C. Jones, R. Van Meter, A. G. Fowler, P. L. McMahon, J. Kim, T. D. Ladd, and Y. Yamamoto, Layered architecture for quantum computing, *Physical Review X*, 2, 031007 (2012).
[30] N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, Experimental comparison of two quantum computing architectures, *PNAS*, 114, 3305 (2017).
[31] X. Fu, M. A. Rol, C. C. Bultink, J. van Someren, N. Khammassi, I. Ashraf, R. F. L. Vermeulen, J. C. de Sterke, W. J. Vlothuizen, R. N. Schouten, C. G. Almudever, L. DiCarlo, and K. Bertels, An experimental microarchitecture for a superconducting quantum processor, in proc. of MICRO-50, Cambridge, MA, USA, October 14–18 (2017).
[32] 根本香絵 , Simon Devitt, W. J. Munro, スケーラブル量子コンピュータの最先端と量子情報技術の展望 , 情報処理 , 55, 702 (2014).
[33] M. H. Devoret, A. Wallraff, and J. M. Martinis. Superconducting qubits: A short review, arXiv:cond-mat/0411174 (2004).
[34] P. Teich, Quantum computing enters 2018 like it is 1968, https://www.nextplatform.com/2018/01/10/quantum-computing-enters-2018-like-1968/
[35] IQVIA, *2018 and beyond: outlook and turning points* (2018).
[36] A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J. M. Chow, and J. M. Gambetta, Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets, *Nature*, 549, 242 (2017).
[37] J. Biamonte, P. Wittek, N. Pancotti, P. R., N. Wiebe, and S. Lloyd, Quantum machine learning, *Nature*, 549, 195 (2017).
[38] E. Farhi, J. Goldstone, and S. Gutmann, A quantum approximate optimization algorithm, arXiv:1411.4028 (2014).
[39] NIST, Post-quantum cryptography, https://csrc.nist.gov/projects/post-quantum-cryptography
[40] C. Brennan, B. Zelnick, M. Yates, and W. Lunn, Blockchain 2.0, *Global Equity Research Technology* (2018).
[41] 藤井啓祐 , 量子コンピューターの基礎 , オペレーションズ・リサーチ , 2018 年 6 月号 , 311 (2018).

[42] M. Reiher, N. Wiebe, K. M. Svore, D. Wecker, and M. Troyer, Elucidating reaction mechanisms on quantum computers, *PNAS*, 117, 7555 (2017).
[43] E. Tang, A quantum-inspired classical algorithm for recommendation systems, arXiv:1807.04271 (2018).
[44] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Tenth anniversary edition (2011).
[45] M. Ying（著）, 川辺治之（訳）,『量子プログラミングの基礎』, 共立出版 , 2017.
[46] K. Mitarai, M. Kitagawa, and K. Fujii, Quantum analog-digital conversion, arXiv:1805.11250 (2018).
[47] Q. Xu, N. S. Kim, and T. Mytkowicz, Approximate computing: A survey. *IEEE Design & Test*, 33, 8 (2015).
[48] S. J Devitt, W. J. Munro, and K. Nemoto, Quantum error correction for beginners, *Reports on Progress in Physics*, 76, 7 (2013).
[49] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland. Surface codes: Towards practical large-scale quantum computation, *Physical Review A*, 86, 032324 (2012).
[50] B. Giles and P. Selinger, Exact synthesis of multiqubit Clifford+T circuits, *Physical Review A*, 87, 032332 (2013).
[51] S. J. Devitt, A. M. Stephens, W. J. Munro, and K. Nemoto, Requirements for fault-tolerant factoring on an atom-optics quantum computer, *Nature Communications*, 4, 2524 (2013).
[52] QuSoft, Quantum Software Manifesto, http://www.qusoft.org/quantum-software-manifesto/

（ウェブサイトは 2018 年 12 月 1 日時点）

■戦略プロポーザル作成メンバー■

総括責任者	木村 康則	上席フェロー	（システム・情報科学技術ユニット）
チームリーダー	嶋田 義皓	フェロー	（システム・情報科学技術ユニット）
チームメンバー	鹿島 泰介	主任調査員	（未来創造研究開発推進部）
	辻 真博	フェロー	（ライフサイエンス・臨床医学ユニット）
	津田 憂子	フェロー	（海外動向ユニット）
	永井 諭子	副調査役	（研究プロジェクト推進部）
	日江井 純一郎	フェロー	（科学技術イノベーション政策ユニット）
	福島 俊一	フェロー	（システム・情報科学技術ユニット）
	藤田 維明	主任調査員	（監査・法務部）
	的場 正憲	フェロー	（システム・情報科学技術ユニット）
	宮下 哲	フェロー	（ナノテクノロジー・材料ユニット）

※お問い合せ等は下記ユニットまでお願いします。

CRDS-FY2018-SP-04

戦略プロポーザル

みんなの量子コンピューター

～情報・数理・電子工学と拓く新しい量子アプリ～

STRATEGIC PROPOSAL

Quantum Computer Science for All

-Towards novel quantum applications-

2018年12月　December 2018
ISBN 978-4-88890-616-6

国立研究開発法人 科学技術振興機構研究開発戦略センター
システム・情報科学技術ユニット
Systems and Information Science and Technology Unit
Center for Research and Development Strategy,
Japan Science and Technology Agency

〒102-0076　東京都千代田区五番町7番地
電　　話　03-5214-7481（代表）
ファックス　03-5214-7385
http://www.jst.go.jp/crds/

ISBN978-4-88890-616-6