量子コンピュータの最新動向

（第 13 回 FMMC 研究会　2022 年 4 月 21 日実施）

日本アイ・ビー・エム株式会社　技術理事 東京基礎研究所 副所長
量子コンピューティング担当部長　小野寺　民也

私は、30 年以上 IBM の研究所におり、コンピュータサイエンスといいますか、IT の研究をしております。プログラム言語ですとか、その上の分散システム、最近ですと、量子計算ソフトウェアスタック等々の研究開発に従事しております。

量子コンピュータの起源から現在

量子コンピュータの起源は、1981 年の 5 月、およそ 41 年前に IBM とマサチューセッツ工科大学が共催した Physics of Computation というコンファレンスであると言われています。これは物理学者と計算機科学者を集めて開催されたコンファレンスで、当時既にプロセッサーの微細化がどんどん進行しており、このまま進行すると早晩、量子効果が無視できなくなるのではないかということで、開催されました。

1965 年にノーベル賞を受賞したリチャード・ファインマンや、IBM のリサーチャで「RISC（Reduced Instruction Set Computer：縮小命令セットコンピュータ）アーキテクチャの父」と呼ばれているジョン・コックが参加しています。この会議でファインマンが、「量子化学のシミュレーションは、普通のコンピュータでは手に負えない。同じ量子力学に基づいた動作原理を持つコンピュータでやるのがよい」といったのが、量子コンピュータの起源であると言われています。

この頃はハードウェアやソフトウェアについては、何も分かっていなかったのですが、ソフトウェアについて研究が進展して、1997 年に、当時 AT&T にいたピーター W. ショアが素因数分解の量子アルゴリズムを発表しました。

これは非常にセンセーショナルな研究成果でした。素因数分解は、今のコンピュータにとっては難しく、2048 ビットの数を素因数分解すると、たとえば 10 億年かかっても終わらないということになります。しかし、量子コンピュータでショアのアルゴリズムを実行すれば多項式時間で済みます。最も良い見積もりだと、10 秒程度でブレイクされるということで、量子コンピュータあるいは量子アルゴリズムのパワーを示す例としてよく引用されます。

この時点ではハードウェアについてはまだよくわかっていませんでしたが、この後に、日本の当時 NEC にいた中村 泰信先生（東京大学先端科学技術研究センター教授）のチームが、世界で初めて超伝導回路型の量子ビットの製作に成功という、大きな成果がありました。ここからハードウェアの研究もソフトウェアの研究も進展していって、2016 年になって、弊社が、IBM Quantum Experience を立ち上げ、量子コンピュータ（5 量子ビット）を、IBM クラウドを通じて世界中で使えるようにしました。

現在は、ニューヨークの北のポキプシーという所に、量子コンピューテーション・センターがあり、そこで IBM クラウドを通じて誰でも使えるパブリックデバイスと IBM Quantum Network の加入者が使用できるプレミアムデバイスを合わせて、20 台以上の量子コンピュータが常時稼動しています。

量子コンピュータが可能にすること

量子コンピュータが、なぜこれだけ騒がれているかというと、理論的にはスパコンを凌駕する並列計算力があるということになります。ｎ量子ビットあれば基本的な並列計算パワーとして、２のｎ乗のパワーがあるということになります。２の 10 程度だと 1,024 ですが、30 量子ビットだと２の 30 ですので 10 億になりますし、40 になると１兆となります。

もっと驚異的なのはこのｎが２の肩の方に乗っているところでして、例えば今のスパコンを２倍の性能にしようと思ったら、テニスコート１面ぐらいの敷地を用意して、そこにラックを並べてネットワークの配線をして大量の電力を供給することになります。しかし、量子コンピュータの場合、この肩に乗っているｎをｎ＋1 にすれば、つまり量子ビットを１つ増やせば、性能が２倍になるわけです。

そういう驚異的なパワーを持っていますので、今のコンピュータから見て Easy problems と Hard problems というのがあったとすれば、ある種の問題は、量子コンピュータを持ってくれば解けます。その例はまだ多くはありませんが、先ほど述べた素因数分解はその例になります。

量子コンピュータには、コンピュータという名前が付いていますけれども、ファインマンの提唱から出発していることもあり、物理系の人たちが育ててきています。発表される学会も、日本で言えば物理学会とか、応用物理学会とかですし、米国の方でも APS（American Physical Society）等になります。

量子コンピュータに対して、今のコンピュータを、古典コンピュータと言います。量子力学ができたら、それまでの力学が古典力学と呼ばれているのと同様です。IT 業界からすれば、非常に違和感があると思いますが、用語として、今のコンピュータを古典コンピュータ、古典コンピュータで動くアルゴリズムを古典アルゴリズムという具合に、量子コンピュータ、量子アルゴリズムと区別するために、そういう用語が使われています。

古典アルゴリズムでは、素因数分解は、準指数関数的な時間がかかる大変難しい問題ですが、量子アルゴリズムでは多項式時間のものが発見されています。古典アルゴリズムでは準指数関数時間かかるというのは、今発見されているベストなもので、多項式時間で解けないということが証明されているわけではありません。明日突然そういうアルゴリズムが出現するかもしれないですが、もう何十年も天才たちが挑んで発見されてないので、おそらくそれは難しいと考えてよいでしょう。

応用領域については、これもまだまだこれからの詰められていくところですが、弊社に限らず、３つの領域があるといっています。１つは量子化学の計算、これはファインマンの言

った分野です。他には、機械学習、最適化/モンテカルロ・シミュレーションです。金融分野で多用されているモンテカルロの計算は、二乗加速するということが分かっています。

とはいえ、まだまだ黎明期です。今どういう状態かというと、2016 年に 5 量子ビットを公開し、現在では、量子ビットの数は 100 を超えていますけれども、まだまだです。しかも、大きな特徴というか問題として、ノイズありという状態です。

まず、量子状態を保てる時間が長くありません。量子ビットの状態を高精細に操作しながら量子計算を進めていくのが量子コンピュータですが、量子状態を保てる時間は、わずか 3 桁の μs です。このオーダーの時間しか、計算ができないことになります。

かつ、量子ビット操作には、1 量子ビットのゲートと、2 量子ビットのゲート（演算器のこと）があります。ゲートを掛けて量子状態を変えながら計算していく際にエラーが伴います。現状では、2 量子ビットのゲートが厳しく、10 の－2 乗程度のエラーがつきまといます。しかも量子ビットによって、エラー率にばらつきがあります。1 量子ビットのゲートではエラー率は格段に小さいですが、いずれにせよ、エラーが発生する状態なので、こうした状態を称してノイズのある量子コンピュータと言っています。

エラー訂正のアルゴリズムが理論的には知られていますので、いずれそれを適用してノイズがなくなり、かつ大規模、すなわち、数百万とか数千万の量子ビットを持つようなものが、登場するだろうと言われていますが、実現は 20 年－40 年先だろうと考えられています。それまでの間は、ノイズは取れませんが、中規模、数百とか千とかのオーダーの量子コンピュータの時代に入るだろうと言われています。

何か役に立つアプリケーションで、古典コンピュータではできない、あるいは、古典コンピュータよりも速くできるといったアプリケーションが登場することが期待されていますし、産学を挙げてこの方面に研究を注力しているという現状です。

予め頂いている「量子暗号との関係という質問」に関連しての説明にもなりますが、ショアのアルゴリズムがあって、いずれそれを動かせる量子コンピュータが開発され、今の RSA 暗号（桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号）が通用しなくなる時代が来ると予想されています。

量子暗号という言葉で表される分野も多様です。その 1 つの部分について説明を試みると、量子コンピュータをもってしても解けない問題というのがたくさんあります。今、暗号の世界で試みられているのは、古典アルゴリズムの暗号で量子コンピュータが出てきても解けない暗号方式（耐量子暗号ですとか、Post-Quantum cryptography 等々と呼ばれています。）で、数年前から NIST（National Institute of Standards and Technology）がアルゴリズムを募集して策定しようとしています。

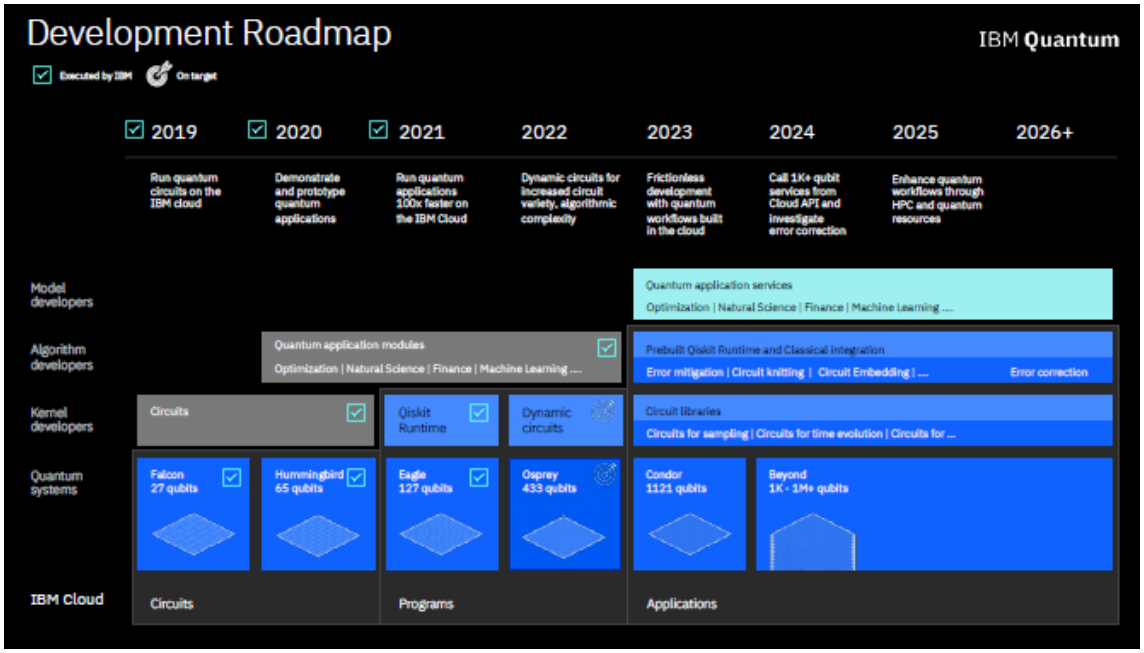
これとは別に、現在の秘密鍵の暗号方式を使い、秘密鍵を今の普通のネットワークでなく、量子状態を送れるネットワークを使って送る、というものもあります。量子通信には、ブレイクされたらブレイクされたことが分かるという特徴があります。これにより、安全な世界をつくろうというアプローチもあります。現況は、少なくとも 2 つ違う話が、「量子暗号」

にあります。

ソフトウェアとハードウェア

次に、ソフトウェアとハードウェアの話を、もう少し詳しくご紹介します。IBM では、図表 1 のようなロードマップを持って量子コンピュータに取り組んでいます（注：開発ロードマップは講演後の 5 月 10 日にアップグレードされている）。

図表 1



一番下がハードウェアのシステムで、去年 127 量子ビットのものをリリースし、今年、433 量子ビットのものをリリース予定で、来年には 1,000 を超えるものをリリースする予定です。

上の層のソフトウェアについて非常に簡単に説明すると、一番下のマシンに近いところを制御するソフトウェアと、その上の量子アルゴリズムの層があります。そして、2023 年ぐらいから、量子化学を含む自然科学や、機械学習ですとか、オプティマイゼーション等々といったアプリケーションに近いものが出てくると考えています。

IBM では超伝導型の量子コンピュータを採用しています。量子プロセッサは冷却塔に格納されています（図表 2）。冷却塔を外すとたくさんの配線が上から下、あるいは下から上に流れています。冷却塔の後ろには制御エレクトロニクスがあって、高精細なマイクロ波を発生して量子プロセッサに送り量子ビットの量子状態を操作します。

図表２

量子プロセッサーは、冷却塔内の一番下の所に装着されています。ここは極低温の 15mK で、ほぼ絶対零度に近い温度にあります。一番上で 40mK、マイナス 238 度ぐらいになっていて、そこから順次、いろんな冷却テクノロジーを駆使して、段階的に下げていって一番下が 15mK、その状態で量子ビットは動作します。外の宇宙（アウタースペース）がこれより 100 倍「熱い」環境です。

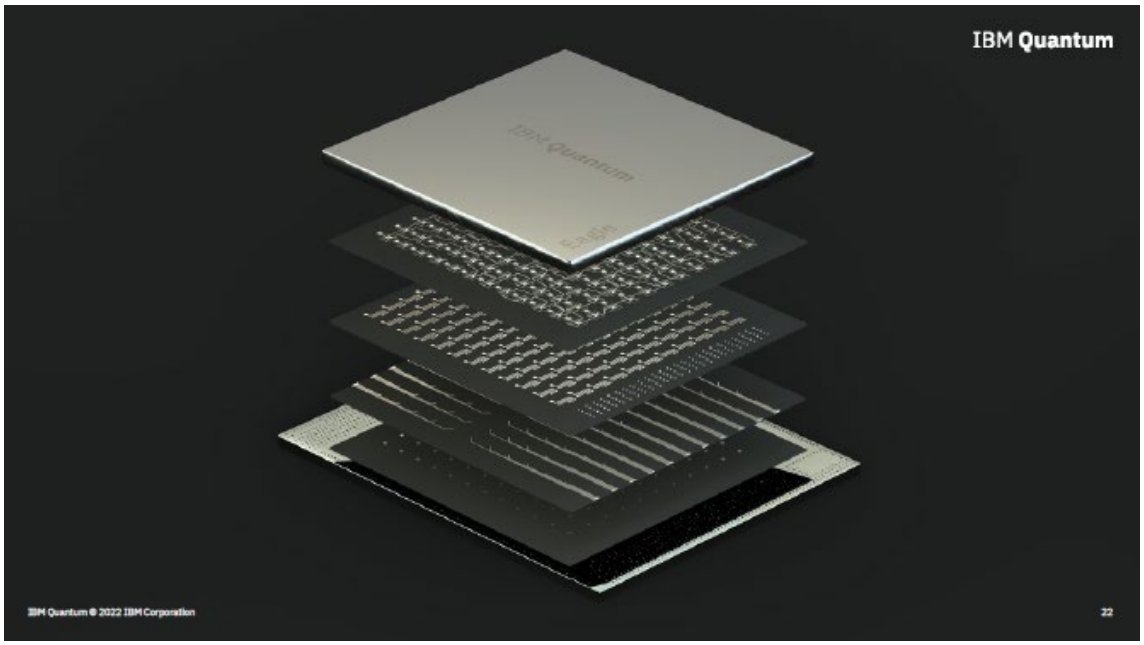
IBM の他に Google ですとか Rigetti Computing ですとかが、超伝導方式で取り組んでおります。これとは別にイオントラップ方式も有望視されていて、Quantinuum ですとか IonQ とかが、この方式を追究しています。

この量子コンピュータについて、ハードウェア寄りのところを推進するのに、IBM は、Scale、Quality、Speed という３つの測定基準を持っております。最初の Scale は単純にビット数、量子ビット数です。ロードマップでもお話したように、2021 年の 11 月 16 日のプレスリリースで、127 量子ビットのプロセッサーを発表しました。

プロセッサーの中身は、層状になっていて、大きさは 25 セント硬貨程度です。127 量子ビット間の配線ですが、これまで密な配線、疎な配線をいろいろ試行錯誤して、この Heavy Hex という構成にたどりつきました。線がつながったところに CNOT という２量子ビットのゲートが直接かけられるため、つながっているところが多い方がよいのですが、つながっているところが多いとクロストークという現象を発生して量子状態が壊れやすくなります。試行錯誤の上、この構成で落ち着いて、来年の 1,000 を超えるものも、この Heavy Hex で行く予定です。

図表３のように層状になっているのを、もう少し詳しく見ますと、この一番上の層が、量子ビットが載っている層です。ここの下の層が、２量子ビットを操作する共振器という部品が載っている層で、一番下がワイヤーリングの層になります。IBM では数十年にわたってコンピュータのハードウェアを作っていますが、長年培ってきた半導体テクノロジーを、量子プロセッサーを作るのにも応用しています。

図表３



２番目の Quality については、エラー率を少なくするですとか、量子状態を保てる時間、コヒーレンスタイムと呼びますけれども、そのコヒーレンスタイムをできるだけ長くするということです。量に対して質を計る測定基準も必要で、弊社は量子体積(Quantum Volume)というものを提案して論文で発表しており、当初から、この量子体積を毎年２倍にするというというのを目指してきました。。

最初は量子体積は 8 でしたが、2022 年に Prague というデバイスで 256 を達成しております。これは、意味のある結果を出せる量子回路の大きさと考えることもできます。ですからどれだけ大きなプログラムが書けるかということになるのかと思います。

３番目は Speed で、CLOPS（Circuit Layer Operations per Second）という測定基準を定義しました。１秒間にどれだけの数の回路を流せるかということです。CLOPS についても、こういう具合に計りましょうという論文を去年発表しました。超伝導方式の場合は、１量子ビットゲートの操作時間は数ナノ秒といわれています。CLOPS はデバイスの素子のスピードも含めた指標になります。

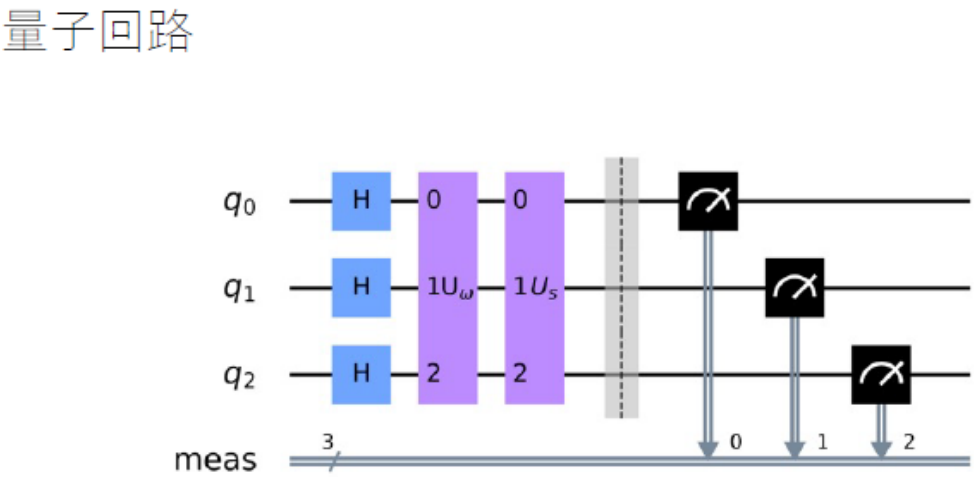
量子プログラミング

量子プログラミングとはどのようなものかについて、ほんの少しだけ話します。今のプログラミング、古典のプログラミングとは全然違う発想であり、全然違う動き方をするというのを感じていただければと思います。

量子プログラミングは、こういう量子回路を作ることです（図表４）。これは３量子ビットの量子プログラムで、五線譜のように、左から右に時間が流れていくという形で、一番左で１量子ビットのアダマールゲートをかけています。次に３量子ビットにまたがった操作

をしているように見えますけれども、これは内部では１量子ビットと、先ほど挙げた CNOT ゲートを使ったものに分解されています。

図表４



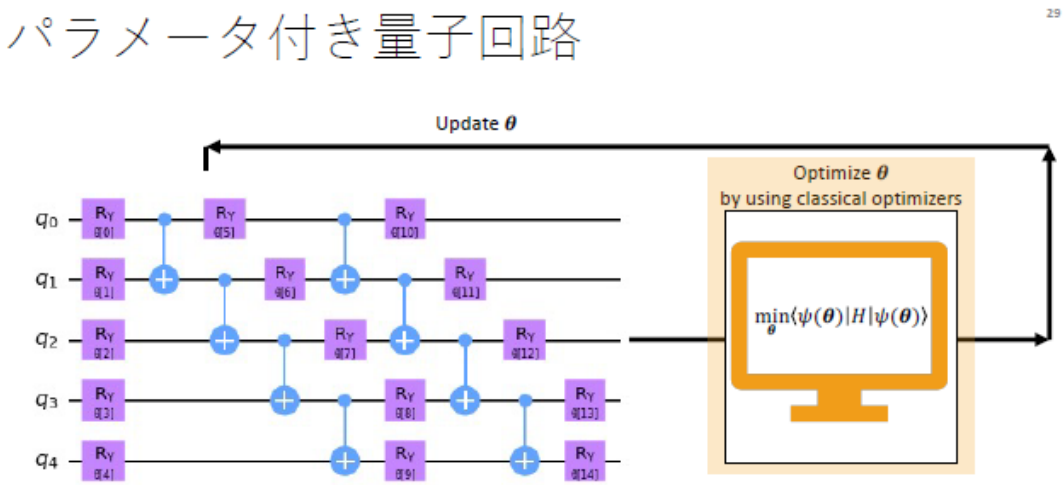
ゲートをかけて、量子状態を操作しますが、この３量子ビットのプログラム、普通のデジタル回路と似たようなものと思うかもしれません。しかし、この３量子ビットを表しているのは、実は２の３乗の大きさの空間を表していて、その２の３乗の空間を操作します。

ところが、この２の３乗の空間を丸ごと人間が取り出すことはできなくて、最終的には測定します。測定すると２の３乗の空間の、どこか１つの状態がプログラムしたとおりの確率に従って出現するため、この同じプログラムを何回も 1,000 回とか 2,000 回とか 3,000 回とか走らせて、測定した値の分布を見て出現確率の高いところが自分の求める答えになるようにプログラムを作ります。

もし 30 量子ビットあったら、操作する空間の大きさは２の 30 乗なので、10 億次元の空間を操作しているということなので、一見普通の回路図に見えますけれども、やっていることは全然違うことです。

量子コンピュータの世界では、今、図表５のようなパラメーター付の量子回路が非常に注目されており、世界中の研究者によってさまざまに追究されています。パラメーターをある初期値に設定して、回路を動かし、その測定結果に基づいて、なんらかのコスト関数が最小になるようにパラメーターを調整して、また新しいパラメーターで回路を動かして、ということを繰り返します。ディープニューラルネットワークでの重みパラメータの調整を髣髴させますが、量子化学の計算でも、機械学習のアルゴリズムでも、最適化周りのアルゴリズムでも、頻繁に使われています。

図表５



これまでは、量子回路の部分は、クラウドの向こう側の量子コンピュータで動かし、古典のコスト関数の計算は、自分の手元のコンピュータで動かすという形になっていました。古典と量子の、この行ったり来たりはもう何千回と必要なので、これまでは時間がかかっていました。

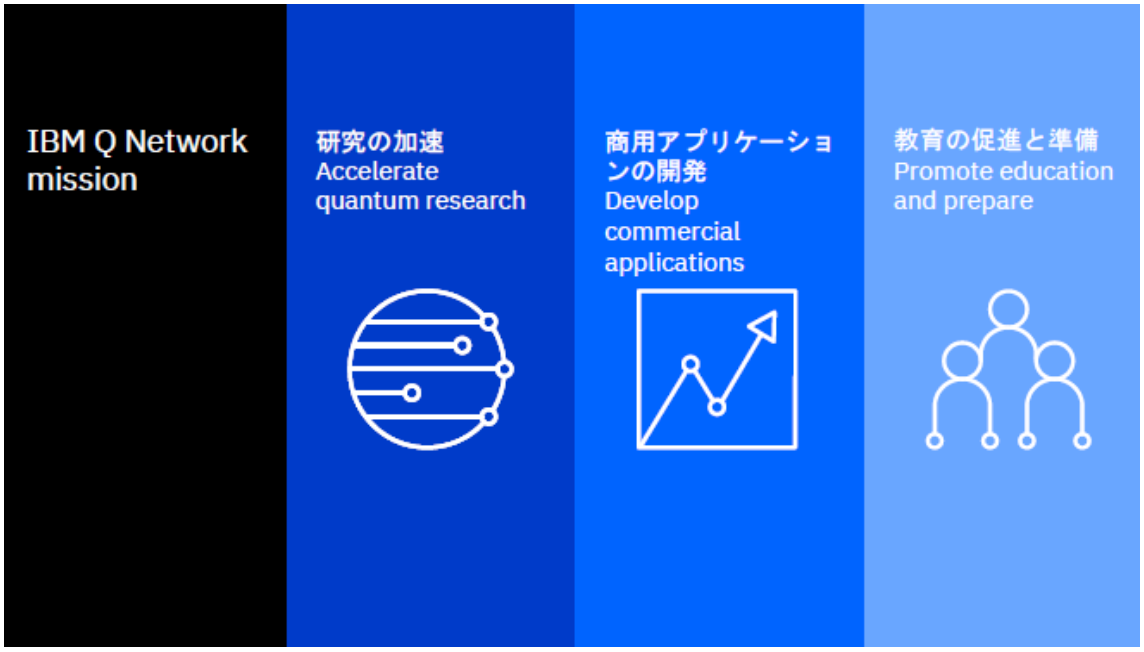
2021 年 5 月に発表した Qiskit Runtime では、量子プログラムの部分だけでなく、古典のプログラムの部分もクラウドの向こうに投げられるようになりました。ですから、古典と量子の行ったり来たりが全部クラウドの向こう側で完結することになり、パラメーター付量子回路の実行が格段に早くなるという、そういう革新的機能になります。

量子コンピュータの実用のための共創

量子コンピュータについては、世界中の有力な企業、研究所、大学と共同して推進しています。その舞台が IBM Quantum Network で（図表６）、ミッションとしては、研究の加速と、商用アプリケーションの開発、量子人材の育成、の３つの柱で取り組んでいます。2017 年の 12 月に発足して、2022 年 4 月の時点で 180 を超えるメンバーが世界中にいます。

日本の活動ということで紹介すると、2019 年 12 月に東京大学と共同で、「Japan-IBM Quantum Partnership」の設立を目指すことを発表しました。このとき、1)日本の顧客専用の実機を日本に設置すること、2)それとは別にもう１台、日本には世界でもかけがえのない材料メーカーとか周辺機器メーカーもおりますので、彼らと協力して周辺機器のテストベッドとするため実機を持ってくること、3)基礎的なサイエンスを推進するために、また、人材育成を強化するためにコラボレーションセンターを設置すること、の３つの目標を発表しました。

図表６



これを推進する母体として、量子イノベーションイニシアティブ協議会が、７カ月後に設立され、日本を代表する企業に入っていただいております。東京大学、慶応大学、IBM も含めて 14 のメンバーで発足しました。

そして、2021 年７月には、IBM の量子コンピュータが「新川崎・創造のもりかわさき新産業創造センター（KBIC）」に設置されました。

これより１カ月前には東京大学内にハードウェアテストセンターが設置され、もう一台の実機がテストベッドとして設置されています。量子コンピュータの中には、非常にさまざまな部品があり、冷却塔の中にはケーブルがたくさん走っておりますし、増幅器とか減衰器も配置されています。電気、通信、素材、装置産業といった分野の、日本の優秀な世界最先端の企業と一緒に周辺機器の進化を加速させていきたいと考えています。

IBM は教育活動にも大いに力を入れておりまして、この Qiskit という弊社のソフトウェアを使って実際に実機をたたきながら量子コンピュータ、量子コンピューティングをマスターするという、そういう教材も用意しております。ぜひご活用いただけたらと思います。今の時代は、実機でプログラムを動かしながら、量子アルゴリズムの勉強ができます。ひと昔前では考えられなかったことですが、今は、そういう、実機のある新しい時代に突入しています。　ご清聴ありがとうございました。