特集2

量子コンピュータの研究開発動向

情報通信ユニット
山崎　哲也

はじめに

MIT（米マサチューセッツ工科大学）とIBMの研究グループは、量子コンピュータを使って簡単な因数分解を行なう基礎実験に成功したと2001年12月20日付けの英科学誌「ネイチャー」に発表した。実際に行われたのは15＝3×5というごく簡単なものである。ではなぜこれがネイチャーに載るほど重要かというと、現在のコンピュータとは全く違う原理で稼働する量子コンピュータによってこの計算が行われたためである。

Siを基盤とした半導体デバイスとそれを用いたコンピュータはムーアの法則に乗って急速な発展を遂げてきた。しかし、微細化と発熱の問題から限界が近いといわれる。現在の状況では2010年ごろには微細化の限界が、これを突破できても2020年ごろには発熱の問題から限界に達すると言われている。この限界を突破する方法としてナノデバイスや分子デバイスが注目されている。

現在のコンピュータには他にもいくつかの限界がある。大きな数の因数分解もその一つで、現在のコンピュータでは膨大な時間がかかって事実上不可能である。たとえば、200桁の整数の因数分解は現在最速のコンピュータを使っても数億年かかると言う。最近10年間で、コンピュータの計算速度は約200倍程度速くなっているが、同じ速度でコンピュータが進化して、10年後に現在の200倍の速度を持つコンピュータができたとしても、まだ数百万年かかることになり、事実上不可能なことは同じである。ところが、100MHz程度のクロックで稼働する量子コンピュータが実現すれば、200桁の因数分解を数分で行うことが可能だという。

因数分解の困難さは現在インターネット上で広く使われている公開鍵暗号（RSA暗号）の安全性の根拠であり、量子コンピュータが実用化されれば、公開鍵暗号の安全性は失われることになる。94年にP. Shorが、量子コンピュータを使った因数分解アルゴリズムを発表し、因数分解が高速にできることを理論的に示したことに刺激されて、量子コンピュータの研究が盛んになった。

このように量子コンピュータは、ある種の問題に対しては現在のコンピュータ（量子コンピュータに対して古典的コンピュータと呼ばれる）より飛躍的に速く計算を行うことができる。また、量子1個を操作するエネルギーは非常に小さく、時間も短いため、原理的にはナノデバイスと同様、低発熱・超高速のコンピュータとなる可能性がある。しかし、実用化されるまでにはまだ多くの時間と、多くの問題を解決することが必要である。

ここでは、量子コンピュータの原理と研究動向を解説するとともに、実用化に向けた今後の展開を考える。

量子コンピュータとは

量子コンピュータと従来のコンピュータの違い

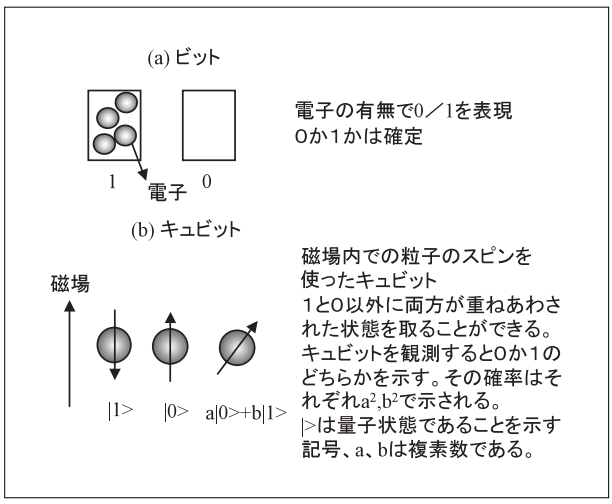
現在のコンピュータはデータを蓄えるビット（メモリ）とビットを操作するための論理ゲート（トランジスタの組み合わせ）によって構成されている。ビットは基本的にコンデンサで、そこに電荷つまり電子があるかないかで1か0かが決まる。一つのビットは1か0のどちらかを示し、n個のビットはn桁の2進数1つを表現する。

一方、量子コンピュータもビット（量子ビット、キュビットと呼ばれる）とキュビットを操作・観測するための機構から構成される。キュビットとして、量子力学的な2個の状態が1/0の表現に用いられる（3個以上の状態を用いる量子コンピュータも可能である）。キュビットには､電子や核のスピンの向き、量子ドットの電子

のエネルギー準位、光子の偏光状態、量子化した磁束の向き、原子の電子軌道の基底・励起状態など様々な系が利用できる。また、キュビットに応じてそれを操作する方法も様々である。キュビットの便宜的な表現として図表1.(b)の様な表現がよく用いられるが、その正確な理解には量子力学に基づいた波動関数での表現が必要である(図表1)。

量子コンピュータで重要になる量子力学の基本的な性質は次の4つである。

図表1　ビットとキュビットの違い



(出典：C.P.ウィリアムズ他「量子コンピューティング」等から科学技術動向研究センターにて作成)

(a)重ね合わせ

2個のスリットを同じ確率で通過するように光子や電子を一個ずつ送り、スリットを通過した粒子がどこに到達するかを観測する。古典的には各スリットに対応した位置で観測されるはずだが、多数の粒子を観測するとスリットによる波の干渉縞と同様なパターンが観測される。この場合、個々の粒子はスリットのどちらか一方を通過したのではなく、それぞれのスリットを通過した状態が重ね合わせの状態になっていて、波の干渉と同じことがおきていることになる。

(b)波束の収束

上記の実験において量子力学が予言するのは、ある位置において干渉縞の強さに対応したある確率で粒子が観測されるということだけである。個々の粒子がどこで観測されるかはわからない。しかし、実際に観測すれば、個々の粒子が検出された位置を知ることができる。これは、観測されるまでは干渉縞状に広がっていた波動関数が、観測によって、ある一点に収束したと考えることができる。

(c)不確定性

古典力学では粒子の位置と運動量はそれぞれ任意の精度で観測することができた。しかし、量子力学では位置を決めようとすると運動量が、運動量を決めようとすると位置が不確かになるというようにそれぞれの量を同時には決めることができない。

(d)量子のもつれ合い（エンタングル）

複数のキュビット間で特殊な相関関係が生じること。2個の電子のスピン（磁化）の方向で考えると、それぞれどちらの方向を向く確率も等しいが、それら二つの向きを観測すると必ず反対方向を向いているという状態。波動関数で表現すると、二つのキュビットの波動関数は独立ではなく、重なった一つの波動関数として表される。一度エンタングル状態になった粒子は離れていてもその性質を失わない。ただし、外乱によって、この相関が失われる場合がある。これをデコヒーレンスという。

量子コンピュータでは特に(a)が重要である。重ね合わせによって1個のキュビットは0と1の両方の状態を取ることができる。ただしアナログコンピュータとの違いは、このキュビットを観測したときに得られる答は0か1かのいずれかであるということである。

この重ね合わせをN個のキュビットに拡張すると、N桁の二進数2^N個の状態を同時に表現する事ができる。このキュビット群で計算を行うと、一回の計算で2^N個の答を得ることができる。これは量子並列計算と呼ばれ、量子コンピュータが古典的コンピュータに対して優れている点の一つである(図表2)。

ただし、答も2^N個の重ね合わせである。答を観測することによって、(b)の波束の収束によって重ね合わせからある値へ収束する。この時、重ね合わせの中のどの答が得られるかは確率的に決まるため、必要とする答に高い確率で波束が収束するようにアルゴリズムを考える必要がある。また、重ね合わせだった答が一つの値に収束すると同時に、重ね合わせだった入力値も答に対応する値に収束する。このような入力と出力の相関がd）の量子もつれ合い（波動関数の重なり）によって常に保たれているのも量子コンピュータの特徴である。非常に単純化すれば、複数のキュビットで構成される波動関数を多数重ね、これを操作して答となる波動関数を取り出すのが量子コンピュータであるといえる。

なお量子コンピュータ以外では(c)は量子暗号の基礎原理であり、(d)は量子テレポートという量子通

信に使用される。

実際の量子コンピュータにおいてキュビットを操作するためには量子ゲートを構成しなくてはならない。量子ゲートは位相シフタ（位相ゲートとも呼ばれる）と制御NOTゲートの2種類で、これは現在のコンピュータの基本論理ゲートであるANDとNOT（またはORとNOT）に相当する（図表3）。この二つが実現できれば、計算可能なアルゴリズムであればすべて量子コンピュータで計算が可能になる（図表3）。

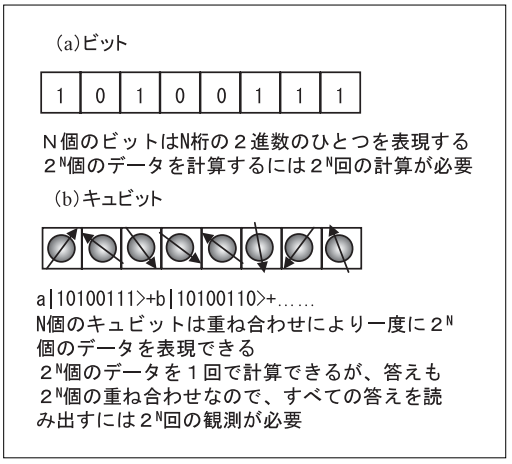
図表4に量子コンピュータのアルゴリズムの一例を示す。

量子コンピュータの歴史

量子コンピュータは、その可能性は比較的古くから指摘されていたが、具体的な研究が始まったのは70年代に入ってからである。現在のLSIが、量子効果が支配的になる大きさまで縮小したらどうなるかというところから研究が始められた。理論的には現在のコンピュータと同じくすべての論理ゲートを実現できることが1970～80年代に示された。しかし、ハードウエアを実現することが困難なこと、現在のコンピュータに比べて優位となる点が見つからないことなどから80年代後半には研究が下火となっていた。

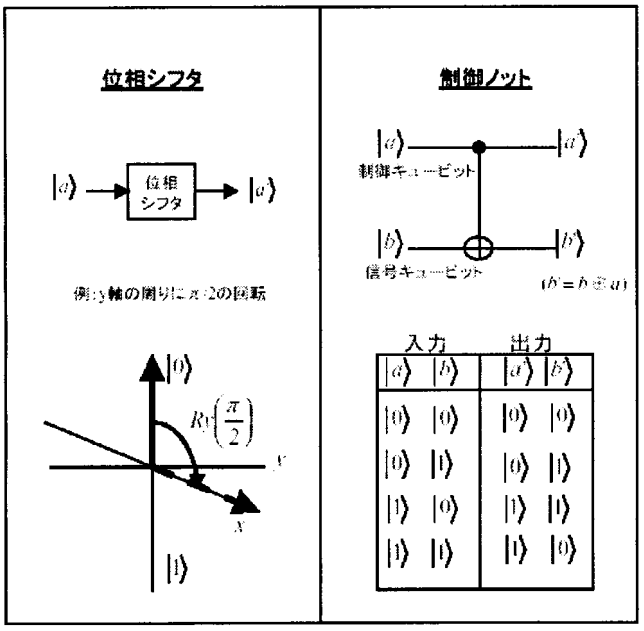
量子コンピュータが再度脚光を浴びるのは、94年にAT&T（現ルーセント）ベル研究所のP. Shorが、現在のコンピュータでは計算が困難な、大きな数の因数分解を、量子コンピュータを用いれば実用的な時間内で計算できることを理論的に示してからである。因数分解の困難さは、現在インターネットで広く使用されている公開鍵暗号の基礎となっており、量子コンピュータが実現すれば、公開健暗号が簡単に解けることになる。この研究により、量子コンピ

図表2　キュビットにおける重ね合わせ



（出典：C.P.ウィリアムズ他「量子コンピューティング」等から科学技術動向研究センターにて作成）

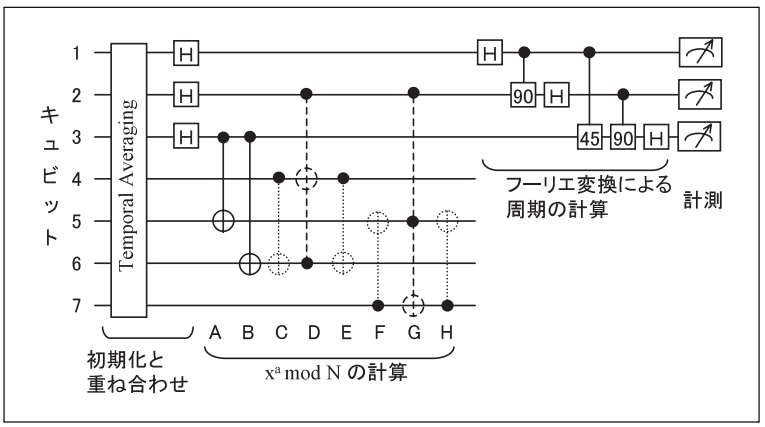
図表3　量子ゲート



位相シフタは量子状態の重ね合わせを実現するのに使用される。
制御ノットは一見0，1の論理回路であるが、重ね合わせ状態を許容する点が異なっている

（出典：情報処理振興事業協会調査報告書「量子計算機の研究動向に関する調査」）

図表4　量子コンピュータのアルゴリズムの一例（Chuangらによる Shorの因数分解アルゴリズム）



Hは重ね合わせの生成、45、90はそれぞれの角度の位相シフトを表す。点線は最適化によって省略された計算、破線はより単純な操作に変換された。

（出典：L. M. K. Vandersypen他　Nature Vol.414 p 833（2001. 12. 20））

ュータが実際に役に立つものであるという認識が広まり、各国で活発な研究が行われるようになった。同時期に量子暗号や量子通信といった量子力学を基礎とする情報通信技術の研究も進み、量子情報理論、量子情報技術（QIT）という新しい分野が出現している。

量子コンピュータの具体例

ハードウエア

量子コンピュータを構成するための条件として以下の5つが挙げられている。

⑴キュビットが実際の物理系として実現でき、かつ集積できること（1000ビットの数字の因数分解には5000個のキュビットが必要）
⑵個々のキュビットを測定できること
⑶個々のキュビットを操作できること（基本量子ゲートの演算が可能であること）
⑷キュビット間の相互作用がある時間（デコヒーレンス時間）が計算時間（1回のキュビット操作の時間×操作回数）に比べ充分に長いこと（最低でも1000倍～10000倍の比が必要といわれる。1000ビットの因数分解では5×10^{11}回の操作が必要）
⑸キュビットの初期化が可能なこと

これらの条件を満たす量子コンピュータの候補として図表5のようなものが現在研究されている。いずれも基礎的研究の段階であるが、もっとも進んでいるのはIBMを中心としたグループの有機分子とNMRを組み合わせる方式である。しかし、この方式は多ビット化が非常に困難で、10キュビット程度にひとつの壁があるといわれる。他の方式も現状では一長一短であり、次のブレークスルーに向けてさまざまな提案がなされている状況である。また、分子デバイス自体を量子コンピュータに使用しようという提案もある。

アルゴリズム

前述したように2つの基本量子ゲートが実現できればそれを組み合わせてどのようなアルゴリズムも量子コンピュータで計算可能である。しかし、現在のコンピュータと同じアルゴリズムを用いるのであれば、量子コンピュータである必然性はない。現時点で古典的コンピュータより量子コンピュータが飛躍的に効率のよい計算が行えるアルゴリズムは大きく分けて以下の3種類（および、いくつかの類似問題）である。

⑴因数分解（Shorのアルゴリズム）
⑵データベース検索（Gloverのアルゴリズム）
⑶巡回セールスマン問題（多数の都市とそれを結ぶ交通路の組み合わせにおいて、すべての都市を1回ずつ訪れる最短経路を求める問題）

これらの問題は基本的に多数の候補の中から1つを選ぶ問題であり、量子並列計算を用いて大量の計算を少ないステップ数で行えるという、量子コンピュータの特徴

図表5　研究されている量子コンピュータの候補と特徴

方式	キュビット	利点	問題点	現状
イオントラップ	真空中で電磁場により固定されたイオンの重心振動モード	デコヒーレンス時間が長い	多キュビット化が困難 真空中で動作	4キュビットでのエンタングル確認
NMR（核磁気共鳴）	溶液中の有機分子の原子核スピン（1個の分子が1個の量子コンピュータ）	常温で動作可能 多数の分子（量子コンピュータ）を同時測定可能 NMR装置で実現可能	多キュビット化が困難（分子設計が必要） キュビットが増えると測定結果の解析が難しい	7キュビットでShorのアルゴリズム実現
	結晶や原子細線の原子核スピン	多キュビット化が比較的容易 デコヒーレンス時間が長い？	測定結果の解析が難しい 極低温で動作 素子の作成が困難	素子開発中
量子ドット	量子ドットに閉じ込められた電子のスピン	多キュビット化が比較的容易 デコヒーレンス時間が長い？	極低温で動作 素子の作成が困難	素子開発中
超伝導素子	超伝導体に発生する磁束、クーパー対	多キュビット化が比較的容易 デコヒーレンス時間が長い	極低温で動作	2キュビットでのエンタングル確認
光子	光子の偏光状態他	デコヒーレンス時間が長い 常温で動作	量子間の相互作用が弱い 多キュビット化が困難	3キュビットでの実験

（出典：情報処理振興事業協会調査報告書「量子計算機の研究動向に関する調査」等から科学技術動向研究センターにて作成）

をうまく利用している。しかし、計算した結果も重ねあわせの状態で観測されるため、答となる波動関数がひとつ、少なくとも解析できる程度の少数に収束することが必要になる。この点が量子コンピュータのアルゴリズムで難しい点のひとつである（補足参照）。

また、量子コンピュータは間違った答を観測してしまう確率を0にすることは原理的にできない。さらに、キュビット間の重ね合わせも確率的に破壊される（デコヒーレンス）ため、計算エラーが起こる可能性もある。そのため、複数回の計算による誤り率の減少やエラー訂正の手法が必要となる。そしてこれらの余分な手間を含めても効率のよいアルゴリズムの範囲に収まることが要求される。

逆にいえば、現時点ではこの三つ（とその類似問題）しか、量子コンピュータの応用先がなく、より広い問題に対するアルゴリズムの開発が期待される。また、効率のよいエラー訂正アルゴリズムの開発も重要である。

《補足》量子コンピュータにおける因数分解の手法

因数分解の場合、最も単純なアルゴリズムは因数分解する数Nを2以上$N^{1/2}+1$以下までのすべての整数aで割ってみるというものである。これを量子コンピュータで行う場合、

1）第1の量子メモリにN、第2の量子メモリに2以上$N^{1/2}+1$以下の整数の重ね合わせを格納する
2）第1メモリを第2メモリで割ってその剰りを第3の量子メモリに格納する
3）第3メモリを観測して0となるときの第2メモリが示す数字（第3メモリの観測によって、第2メモリが収束する）が求める因数の一つである

この方法では、割り算は重ね合わせによって1ステップで可能だが、第3メモリが0以外の場合を読み出す確率が圧倒的に高く、結局0を観測するまで観測を繰り返すのと、古典的に割り算を繰り返すのとほとんど同じステップが必要になる（Nが10000のオーダーで、2個の素数の積であるとすると、$N^{1/2}$～100の重ね合わせの中で剰り0となるのは1つの場合だけである。この場合、100回までの繰り返しで0を観測する確率は高々63％にすぎない。一方、古典的に割り算を繰り返せば、100回の計算で必ず答を得ることができる）。

そこでShorのアルゴリズムでは以下のような整数の性質を用いる。

1）互いに素である（1以外に公約数を持たない）整数x，yに対して$x^a \bmod y$（$X^a \bmod y$はX^aをyで割った剰りを求める関数、aは任意の整数)はaの周期関数になる
2）1）において$x^{nr} \bmod y = 1$（rは整数、nは0、1，2，3…）となるような周期rがあって、rが偶数の場合、

$$(x^r - 1) \bmod y = \{(x^{r/2} - 1)(x^{r/2} + 1)\} \bmod y = 0$$

であるので、$x^{r/2}-1$、$x^{r/2}+1$の少なくとも片方とyは1でない公約数を持っている

実際には、以下のような計算を行う。

1）因数分解する整数Nと互いに素な整数x（$N > x$）をランダムに選ぶ。
2）$N^2 < q < 2N^2$なる適当な整数qを選ぶ
3）$y = x^a \bmod N$（a=0，1，2，…q－1）をすべてのaに対して量子並列計算で計算する。この段階でyを観測して値kを得たとすると、aは$x^{l+nr} \bmod N = k$を満たす整数l＋nr（lは整数、rは周期、n＝0，1，2，…）の重ね合わせになるが、l，r，nがいずれも未知なのでrを求めることができない
4）aに対してフーリエ変換を行う。詳細は省くが、その値はmq/r (m＝0，1，2，…r－1)の重ね合わせとなる
5）4）を観測して$c = m_0\, q/r$ (m_0＝0，1，2，…r－1のいずれか)なる一つの値cを得る。
6）m_0とrが互いに素であれば、c/q（ともに既知）を約分する事でrを計算できる。m_0とrが互いに素である確率は繰り返しによって高めることができる
7）rが偶数であれば$x^{r/2}-1$、$x^{r/2}+1$とNの最大公約数を求める

（出典：参考文献[1, 2, 5]より科学技術動向研究センターにて作成）

各国における量子コンピュータの研究開発状況

量子コンピュータは、将来のコンピュータ技術としてだけでなく、量子暗号、量子通信を含めた量子情報通信技術やナノテクノロジーの一部として位置付けられることが多い。ここでは比較的量子コンピュータに絞ったプロジェクトを取り上げている。

米国

米国には、前述したNMRのIBM、アルゴリズムのベル研（AT&T→ルーセント）、イオントラップのNIST、量子ドットのロスアラモス研とビッグネームが多い。政府プロジェクトとしては、毎年発表されている米国情報通信政策の予算要求書（Blue Book）FY1997（1996年11月）及び実行計画書（Implementaion Plan）（1997年1月）の中でHigh End Computing and Computation （HECC）プログラムの一つとして初めて量子コンピュータが取り上げられている。ここでは、バイオ、光コンピュータとともに研究をサポートすべき将来技術として扱われており、この点はFY2002予算要求書でも変わっていない。また1999年に発表されたIT[2]計画において、量子情報通信技術は、基盤的な情報通信技術としてその研究開発を進めるべきであると提言されている。

HECC分野での中心機関はNSF、DARPA、NIST、NSA、DOE、NOAA、NASAなどであるが、量子コンピュータ関連では、量子コンピュータによる暗号解読や量子暗号に注目したNSAが中心になってプロジェクトを行っている。1994～1999年に、9以上の大学、企業と、DARPA、NISTなどの政府機関との共同で第一次プロジェクトが行われた。引き続き現在は第2次プロジェクトが行われている。個別プロジェクトの予算額は不明であるが、NSAのHECC全体の予算額は20～25M$/年程度である。

またDARPAはFY2001より「Microelectronic Device Technology」プロジェクトの下で、「Beyond Silicon」と題して、量子コンピュータを含む一連の次世代技術の研究開発を開始し、FY2002には「Beyond Silicon」をプロジェクトに格上げしている。「Beyond Silicon」プロジェクトのテーマ中で量子コンピュータ、量子通信技術に直接関連するのは「The Quantum Information Science and Technology」で、FY2001は予算実績約14.3M$、FY2002の要求予算23.8M$であり、FY2003には27.1M$の予算要求を予定している。これ以外にもナノテク関連の研究プロジェクト「Materials Science」やコンピュータサイエンス関連の「High Performance and Global Scale System」などのテーマ中に量子ドットや量子アルゴリズムなどの量子コンピュータ関連技術が上げられている。

このほか、NISTは麾下の研究所で量子コンピュータ、量子通信の研究を行っており、特にイオントラップ方式で有名である。図表6にNSFの量子コンピュータに関する助成件数を示す。

図表6　NSFの量子コンピュータ関連研究採択件数

年	採択件数	総額（$）	金額/件	期間
1995	23	4,930,629	214,375	1～4年
1996	20	5,851,012	292,551	2～4年
1997	23	5,923,848	257,559	0.8～4年
1998	25	6,504,615	260,185	2～4年
1999	22	4,808,112	218,551	2.8～4年
2000（注）	6	1,361,800	226,967	3年
総　計	119	29,380,016	246,891	0.8～4年
現在進行中のプログラム	61	15,435,106	253,035	

注）2000年は4月時点でのデータ

（出典：郵政省（現総務省）調査報告書「21世紀の革命的な量子情報通信技術の創生に向けて」）

欧州

ECにおいては、1984年以来、4年ごとに地域全体の研究計画（フレームワーク）を策定し実行しており、現在は第5次フレームワークが進行している。量子コンピュータを含む情報通信技術については、第1次から第4次フレームワークにおいてESPRITプロジェクトの一環として研究開発が行われてきた。

第5次フレームワーク（1998～2002年）においては、4つの垂直分野と3つの水平分野に分けられており、量子コンピュータを含む情報通信技術関連は、IST（Information Society Technology research）として実施されている。

ISTのプログラムは、技術分野別に既存技術4、新規技術1の5種類、研究補助を主目的とした活動形式による4種類の計9種類に分けられる。量子情報通信は新規技術分野であるFuture and Emerging Technologies（FET）内のQuantum Information Processing & Communications（QIPC）プロジェクトで行われている。

現在QIPCは1999年に募集された12研究プロジェクト（1999～2000初開始、期間は3～4年）の他、FET-OPENという、研究プロジェクトを随時募集する制度で4プロジェクト（期間は1～3年）が行われている。郵政省調査報告書「21世紀の革命的な量子情報通信技術の創生に向けて」によると、QIPC全体の研究資金は、総額約22.4M Euroが見込まれており、そのうちECの負担額は、約17.2M Euro（総額の約77％）である。

ECの研究プロジェクトの特徴として参加機関が多国間に渡る点がある。ISTには参加研究機関の連携を強め、かつ産業界へのフィードバックを活発にすることを目的としたNetwork of Excellenceプログラムがあり、QIPCでもThe Physics of Quantum Information European Research Network（QUIPROCONE）というネットワークプロジェクトを持っている。期間は2000年7月から3年間である。

なお、2002～2006年の第6次フレームワークでもISTとQIPCは継続され、2002年3月に第二次の研究プロジェクト募集が行われている。

ECのプログラム以外の動きとして、1995年ごろから英オックスフォード大学を中心にした欧州各国の大学間研究ネットワークが自発的に広がっている。

日本

日本国内では、1990年頃までは一部グループによる理論的研究が主であったが、1994年度ころから、科学技術振興事業団のCREST（戦略的基礎研究推進事業）やERATO（創造科学技術推進事業）の採択テーマの一部として量子コンピュータ関連の研究が行われる様になった。1999年には電子情報通信学会の下に時限的研究会として量子情報技術研究会が組織され、理学系、工学系のさまざまな分野の研究者間の情報交換や研究協力の体制が立ち上がっている。また2000年2月に情報処理振興事業協会が「量子計算機における研究開発に関する調査」、同6月に郵政省（現総務省）が「21世紀の革命的な量子情報通信技術の創生に向けて」と題した調査報告書を出版している。現在のプロジェクトとしては、図表7のようなものがある。総務省の公募研究は量子暗号、量子通信を含む量子情報通信技術全体を対象としている。

図表7 日本における量子コンピュータ、量子通信関連の主な研究プロジェクト

研究開発スキーム	テーマ	研究機関（研究期間）	備考
科学技術振興事業団 国際共同研究	量子遷移プロジェクト	東京大学 ノートルダム大学カリフォルニア大学 （平成6年から5年間）	
科学技術振興事業団 戦略的基礎研究	相関エレクトロニクス	ＮＴＴ、東京大学、総合研究大学院大学、電総研 （平成10年から５年間）	
科学技術振興事業団 国際共同研究	量子もつれ	スタンフォード大学 CNRS（仏国立科学研究センター （平成11年から５年間）	日本側が、5年間で10億円を負担。
科学技術振興事業団 戦略的基礎研究	量子相関機能の ダイナミクス制御	理化学研究所 （平成11年開始）	
科学技術振興事業団 戦略的基礎研究	核スピンネットワーク 量子コンピュータ	大阪大学 （平成12年開始）	
科学技術振興事業団 創造科学技術推進	今井量子計算機構	東京大学 （平成13年度開始）	
総務省　公募研究	量子情報通信技術の 研究開発	平成13年度開始の公募研究	予算250M万円

（出典：郵政省（現総務省）調査報告書「21世紀の革命的な量子情報通信技術の創生に向けて」を参考に科学技術動向研究センターにて作成）

最後に　―量子コンピュータ実現に向けて―

現在のコンピュータの、直接の後継者はナノ・分子デバイスであり、ナノ・分子デバイスにより高い集積度で発熱量のきわめて少ないコンピュータが実現されると考えられる。では量子コンピュータはどのような位置付けとなるのだろうか。

最初に考えられるのが、量子コンピュータで効率よく解ける問題を専門とするコンピュータのサブセットとしての応用である。しかし、そのためにはある程度のキュビット数を集積し、古典的コンピュータと比較して充分な計算速度の優位性を実現する必要があるが、それにはまだ時間がかかるであろう。また、現在開発されているアルゴリズムでは応用先が限定されすぎるという問題もある。

そこで、比較的少ないキュビット数でも実用になる応用先のひとつとして量子通信、量子暗号システムにおける、送、受信機や中継装置等が考えられている。量子暗号システムは、現時点でもコストや通信距離の制限を除けば実用化可能であり、特に光子方式の量子コンピュータは量子暗号システムとの相性がよい。実際ハードウエア的には、単光子の発生、検出機構など両者で共通に使用される技術も多い。

一方、まったく新しいアルゴリズムが発見されれば、急速に実用化が進む可能性もある。ひとつのアイデアとして、量子状態のシミュレーションによる材料開発に量子コンピュータを使用できないかというものがある。古典的コンピュータでは原子1000個のシミュレーションにペタフロップスクラスが必要になるが（科学技術動向2001年12月号参照）、元々量子状態を計算に用いる量子コンピュータならより効率の良い計算ができるのではないかと考えられている。まだ具体的な成果は発表されていないが、いくつかの研究グループが研究を行っている模様である。

このように、新しい応用先やブレークスルーを探しつつ、実用化できる点から実用化を進めていくことが重要であると考える。

一方、研究分野としての量子コンピュータ、量子情報技術を考えると、理論計算機科学や情報理論、数学などの理論、物理、化学、光学から製造技術などの工学までの広い範囲を含む分野である。つまり、多くの分野の間から、新しいアイデアが生まれやすい境界領域の一つと言うことができる。また、研究分野として新しいため、まだ手が着けられていない、魅力的な部分が多く残っている可能性が高い。そういう意味では新しい発想を取り入れたプロジェクトを数多く進めていくような方式が必要ではないだろうか。

参考文献

1）C. P. ウィリアムズ他、「量子コンピューティング」、シュプリンガー・フェアラーク東京、2000年
2) 西野哲朗、「量子コンピュータと量子暗号」、岩波書店、2002年
3）特集「量子情報と量子コンピュータ」、数理科学 No.456，p5，（2001年6月号）
4）竹内繁樹、電子情報通信学会誌 Vlo. 84，No.1，p17（2001年1月）
5）L. M. K. Vandersypen他 Nature Vol. 414，p833（2001. 12. 20）
6）情報処理振興事業協会調査報告書「量子計算機における研究開発に関する調査」（2001年2月）
7）郵政省調査研究会報告書「21世紀の革命的な量子情報通信技術の創生に向けて」（2001年6月）
8）10Th JST International Symposium "Quantum Computing" Abstracts（2002. 3. 12-14）