

ふじさん

fujijoho group monthly magazine

～ 2025年指針 ～

富士情報

開 点

[今月のひとこと]

量子コンピュータ

- ・KK 線廃止
- ・育児介護休業規程の改定
- ・Good Sleep (?)



ふるさと時代祭り

写真提供：都留市 産業課



今月のひとこと

量子コンピュータ

社長 渡辺直企

100 年前の 1925 年、23 歳でゲッティンゲン大学の若手研究員だったハイゼンベルクは運動量や位置などの物理量を行列を用いて表現する行列力学を提唱しました。これは量子力学の理論形式の一つとなりました。量子力学は、分子や原子、電子などを対象とした物理現象を記述する力学です。ニュートン力学などの古典力学と異なり、量子力学は粒子の振る舞いを確率的に記述します。また「粒」のような粒子の性質と「波」のような波動的性質を持ちますが、粒子性と波動性は同時に確認できず、粒子的に観測するときには波動性は消えて、波動的に観測するときには粒子性が消えるなど直感では理解しがたい性質が多く見られます。アインシュタインは「神はサイコロを振らない」と言って、量子力学を受け入れようとしなかったそうです。量子は「重ね」や「もつれ」などの特徴があります。「重ね」は 0 と 1 の重ね合わさった状態を持つことができます。従来のコンピュータは 0 と 1 の 2 つの状態(ビット)しか持てません。量子コンピュータは「重ね」を用いることで多くの状態を表すことが出来るので並列計算が可能になります。

1981 年、アメリカの物理学者リチャード・ファインマンは「物理学と計算」会議の基調講演で古典的なコンピュータで量子力学の計算が難しいという課題に対して「自然(量子系)のシミュレーションをするなら量子力学を(そのまま)使ってシミュレーションすれば良い」といったそうです。量子力学は原子、電子の単位でしか現れず、微細な素子を製造、制御するのは非常に困難です。1962 年、ケンブリッジ大学の大学院生のブライアン・ジョセフソンが理論的に導いたジョセフソン効果があります。これは絶縁体を超伝導体で挟むとマクロで量子的な振る舞いをするという現象です。このジョセフソン効果を利用した量子ビットを超伝導量子ビットといいます。IBM や Google の量子コンピュータは超伝導量子ビット方式を用いています。2016 年、IBM はオンラインでアクセスできるインターフェイスを公開し、5 量子ビットの量子コンピュータ「IBM Q 5 Tenerife」を発表しました。2019 年、Google は 53 量子ビットの「Sycamore」でスーパーコンピュータで 1 万年かかる計算を 200 秒で計算し、いわゆる古典的なコンピュータでは現実的には解決不可能な計算を可能にする「量子超越性」を実現したと発表しました。これに対して IBM は 53 量子ビットの状態を 250 ペタバイトのハードディスクに格納し計算することでスーパーコンピュータなら 2.5 日で計算できると反論しています。

量子コンピュータは通常のコンピュータに比べて得意とする分野が異なり、暗号解読(因数分解)、素材(分子)のシミュレーション、ゲノム解析、などを得意としています。今年 5 月 Google の Craig Gidney は 100 万量子ビット未満で、一週間以内に現在一般的に利用されている暗号鍵(RSA-2048)を解読出来ると示しました。超伝導量子ビット方式は 1 量子ビットが数百 μm で周辺回路を入れると数 mm あり実装密度を向上させるのは困難です。IBM は 2023 年 12 月に 1,121 量子ビットの量子コンピュータを発表しています。intel は半導体製造密度の向上により半導体量子ドット方式を実現し、2023 年 6 月に 12 量子ビットを実装した半導体チップを発表しました。半導体量子ドット方式は電子一つを量子ビットとして使用し計算します。intel の量子ビットは、約 $50\text{nm}(=0.00005\text{mm}) \times 50\text{nm}$ の大きさなので、今後の拡張性が期待できます。Craig Gidney は耐量子暗号(PQC)への移行を急ぐ必要性を訴えています。NIST(米国立標準技術研究所)は 2030 年以降 RSA2048 のような 112 ビットのセキュリティ強度を持つ暗号アルゴリズムは非推奨、2035 年以降は使用禁止としています。今年 6 月にデジタル庁の「デジタル社会の実現に向けた重点計画」では「次期サイバーセキュリティ戦略に盛り込む」としています。情報の安全に関わる問題ですので今後の動きには注意し、他の前向きな課題解決に期待したいと思います。