量子計算機の開発・普及状況（内閣府（文科省））

【関連事項メモ】

- 量子コンピュータの開発は、現在「NISQ（Noisy Intermediate-Scale Quantum）」段階から、「誤り訂正型量子計算機（Fault-Tolerant Quantum Computer, FTQC）」への移行期にあり、IBM、Google、IonQ、Quantinuum、富士通などの企業が競って技術開発を進めている。IBM は 2023 年に 1,121 量子ビットのプロセッサ「Condor」を発表し、2029 年までに誤り訂正機構を備えた量子スーパーコンピュータを構築するロードマップを公開している。現在インターネットなどの通信で使われている RSA 等の公開鍵暗号を現実的な時間で解くためには、100 万量子ビット以上の量子コンピュータが必要と言われており、現時点では、数年内に公開鍵暗号の危殆化が起こる可能性は低い。
- 公開鍵暗号を危殆化するような量子コンピュータの実現時期については諸説あるが、例えば Sevilla & Riedel（2020, arXiv:2009.05045）の研究によれば、2040 年までに RSA-2048 を 24 時間以内に解読できる量子コンピュータが実現する確率は 5%、2048 年までは 50%と推定されている。近年の急速な技術発展を鑑みると、2030 年代にも公開鍵暗号の危殆化が本格化する可能性が示唆されている。