

量子コンピュータと耐量子コンピュータ 暗号の展望 (NCWG会合)

株式会社コンピュータ
福原英之

2026年9月15日

量子実用化ロードマップの加速背景

主要ベンダーの開発加速

IBM等の主要量子ベンダーがエラー訂正技術の統合ロードマップを大幅に前倒しして提示。

2029年にはエラー訂正付き（200論理量子ビット）「**Starling**」の市場投入が予測される事態に。

2030年には、**4,000**量子ビットが実現する恐れも

新しい物理設計の台頭

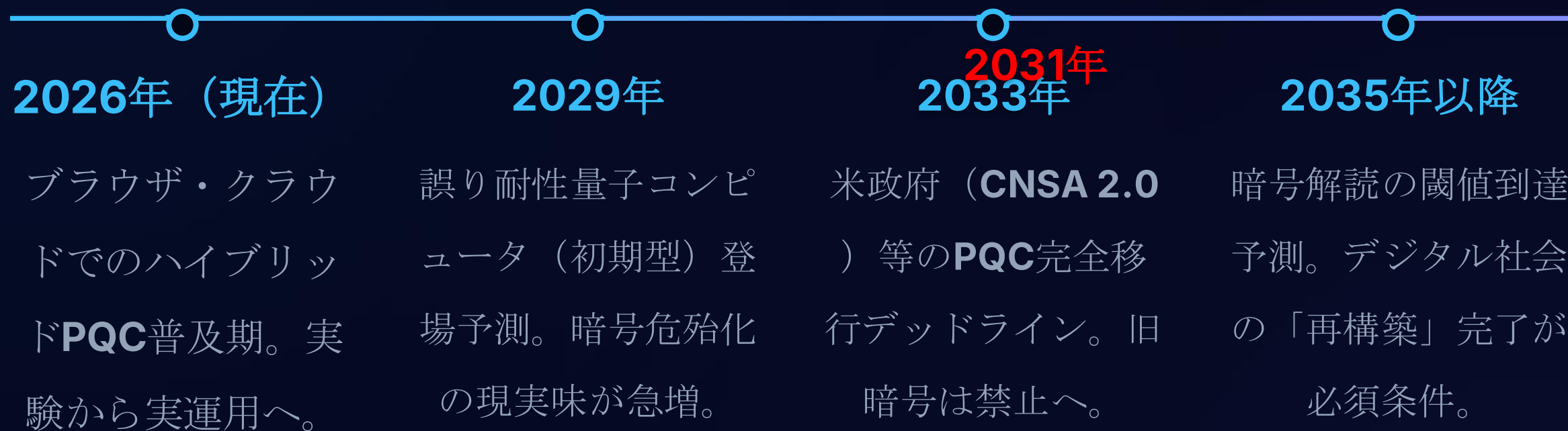
超伝導方式だけでなく、光量子や中性原子など、スケーラビリティに優れた新アーキテクチャが急速に台頭。

論理量子ビットを大量に連結する技術的ブレイクスルーが、当初予測よりも早く到来しつつある。



ROADMAP: ACCELERATING QUANTUM TIMELINE

Y2Qへのカウントダウン：2026-2035



量子時代の 暗号クライシス

量子コンピュータの実用化により、現代のデジタル社会を支える「信頼の基盤」が根本から揺るがされようとしています。

- ⚡ **Shor**のアルゴリズム：公開鍵暗号（**RSA**/楕円曲線）を多項式時間で解読可能に。
- 🗄️ **SNDL**脅威：「今盗んで、将来解読する」攻撃が既に進行中。
- 🛡️ 耐性のある暗号：**AES-256**（共通鍵）や**PQC**（格子暗号等）が盾となる。



耐量子暗号（PQC）の現状と即時対応



標準化の完了

NISTによる標準化

（**FIPS 203 [ML-KEM]**

等）が**2024**年に完了。

世界基準のアルゴリズムが確定しました。



今すぐやるべき事

暗号資産の棚卸し、

AES-256への一本化。

PPK（事前共有鍵）による暫定的な対量子シールドの構築。



実装の進展

Google Chromeや

Cloudflareが本番環境

で実装。**Web**通信の

PQC化は既に「実用フェーズ」です。

署名用PQCの課題：巨大パケットの壁

認証の危殆化：中間者攻撃のリスク

署名（証明書）が旧暗号のままであれば、**2029**年以降、秘密鍵の逆算による「偽サイトの証明書偽造」が容易になります。

最大の問題：パケットの肥大化

ML-DSA：署名サイズが数**KB**に拡大。**MTU**サイズを超過しフラグメントが発生。

RFC 7383：**IKEv2**等で「暗号レイヤーでの分割」機能を有効化し、**FW**によるドロップを回避。

🚫 クライアントVPNは無理



モダン建築：VPN撲滅とゼロトラスト



クライアントVPNからの脱却

端末1台1台にPQCの設定・管理を強いるのは運用上不可能です。また、横展開（ラテラルムーブメント）のリスクも排除できません。

ZTNAへの移行戦略

ZTNA / IAP への移行： 通信を**TLS 1.3 (HTTPS)**ベースに集約。ブラウザとクラウドが自動で**PQC**化を吸収し、企業を複雑なインフラ管理から解放します。

Image Sources

Thumbnail for
<https://media.gettyimages.com/id/2164158933/zh/%E7%85%A7%E7%89%87/microprocessor-abstract-connections.jpg?s=612x612&w=gi&k=20&c=T27PpSrmeIVL8AZWmmaU2JnKPZMLoFISBKTjvpzOv4Y=>
Source: www.gettyimages.hk



<https://images.ctfassets.net/slt3lc6tev37/5aYOr5erfyNBq20X5djTco/3c859532c91f25d961b2884bf521c1eb/tls-ssl-handshake.png>
Source: www.cloudflare.com



https://elements-resized.envatousercontent.com/elements-cover-images/438850ab-c603-4366-b8c2-523f94b87d9a?w=433&cf_fit=scale-down&q=85&format=auto&s=31d8bd4012a909a2f553dd20fc7b8a50543b468239601ad7cd84f42a87d5af16
Source: elements.envato.com



https://www.mdpi.com/data/data-10-00097/article_deploy/html/images/data-10-00097-g001-550.jpg
Source: www.mdpi.com



https://network-insight.net/wp-content/uploads/2022/07/AdobeStock_657436912-scaled-1200x675.jpeg
Source: network-insight.net