

PQCへの早期移行を迫る、 米国発2つの暗号解読論文の衝撃

2026年3月、グーグルとカリフォルニア工科大学らの研究チームが公開した二本の論文により、楕円曲線暗号（ECC）やRSA暗号の解読に必要な量子ビット数の見積りが大幅に下がった。米国は耐量子暗号（PQC）移行の期限を2030年へ前倒ししており、今後日本も対応を求められるだろう。

2026年3月、 二本の論文が前提を変えた

2026年3月31日、暗号の安全性をめぐる前提を揺さぶる二本の論文が同じ日に公開された。一本はグーグルの量子AIチーム、もう一本はカリフォルニア工科大学発のスタートアップOratomicによるものである。いずれも「暗号を量子コンピュータで解読するにはどれだけの規模の装置が必要か」を見積もり、解読が理論上実現しうることを示した。

グーグルの論文¹⁾は、暗号資産取引で使われる楕円曲線暗号（ECC）について、解読に必要な量子ビット数を50万個未満、解読時間を9分から23分の間と試算した。従来の見積りでは約900万個であり、およそ20分の1に縮小した。削減は計算手順（アルゴリズム）と回路設計の工夫によるものである。なお、グーグルは悪用回避のための回路の中身は公開せず、第三者が正しさだけ確認できる形で結果を示した。

もう一本のOratomicの論文²⁾はさらに踏み込む。量子コンピュータは計算誤りが避けられず、多数の量子

ビットを束ねて誤りを打ち消す仕組みを使うが、これをより効率のよい方式に置き換えると、約1万～2万6千個の量子ビットで10日～264日でECCを解読できるという（ITシステムで広く利用されるRSA暗号の場合は数か月から数年であると試算している）。

想定するハードウェアは異なる。グーグルは制御速度が速い「超伝導方式」、Oratomicは超伝導方式に比べて速度は遅いが少数の量子ビットで済む「中性原子方式」を前提とする。どちらのハードウェアが先に実現するかは不明であるが、結論は同じである。「暗号解読には数百万個の量子ビットが必要だから、まだ先の話だ」という常識が、二本の論文が示した試算により崩れたということである。

ただし、実行するハードウェアは 存在しない

ただし、両論文ともあくまで理論上の可能性について試算したものであって、ハードウェアの実現可能性について言及したものではない。グーグルが想定する50万個は、現在の超伝導方式の量子コンピュータの実機（千個規模）の約500倍にあたる。中性原子方式も現状は数千個程度にと

どまり、かつ動作速度は超伝導方式よりも約千倍遅い。暗号解読のためのアルゴリズムを実行させるには、誤り耐性技術の活用が不可欠だが、高い精度で長時間実行できるかも不明である。

実際、米国防高等研究計画局（DARPA）は「量子ベンチマーキング・イニシアチブ」で、2033年までに実用規模の

図表 Google論文とOratomic論文の特徴

Google Quantum AI (スタンフォード大学、イーサリアム財団)		Oratomic、カリフォルニア工科大学、 UCバークレイ
発表年	2026年3月	2026年3月
論文概要	ECC256を解く回路を検討。回路は公開せず、SP1 zkVMとGroth16 SNARKを用いて構築した暗号学的ゼロ知識証明を公開	ショアのアルゴリズムを使って暗号解析に必要な量子ビット数を推定。約1万量子ビットで解読できる
ターゲット暗号	ECC-256	ECC-256+RSA2048
物理量子ビット数	<50万	<1万～2.6万
エラー訂正方式	表面符号	qLDPC (30%レート)
量子コンピュータハード	モダリティ	超電導
	クロック	1μ秒
実行時間推計	ECC256	9～23分
	RSA2048	10～264日

(出所) 野村総合研究所

数か月～数年

NOTE

- 1) Ryan Babbush et al., Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations, 30 Mar 2026
<https://arxiv.org/abs/2603.28846>
- 2) Madelyn Cain et al., Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits, 30 Mar 2026
<https://arxiv.org/html/2603.28627v1>
- 3) Quantum frontiers may be closer than they appear
<https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/>
- 4) 「重要インフラ」とは、一般的に「無能力化や破壊によって、治安や国民経済、健康、安全、またはこれらの組み合わせを弱体化させる影響がある、システムや資産」と定義される。
- 5) SECURING THE NATION AGAINST ADVANCED CRYPTOGRAPHIC ATTACKS
<https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/>
- 6) 政府機関等における耐量子計算機暗号 (PQC) 利用に関する関係府省庁連絡会議
https://www.cas.go.jp/jp/seisaku/pqc/pdf/report_202511.pdf

誤り耐性量子コンピュータが実現可能かを検証・評価している。誤り耐性量子コンピュータはベンダー各社が名乗りを上げたのみで、いまだ登場していない。

つまり、「現実的な時間で解読できる」との論文の結論は、「理想的」な量子コンピュータが実現した場合の話にすぎない。複数の大手企業、スタートアップが、2030年ごろを目途に大規模な量子ビットを有する量子コンピュータの提供を宣言しているが、素材の開発や量子ビットの長時間制御の実現には多くのブレークスルーが不可欠である。時々、「Q-Day（量子コンピュータが暗号を解読する日）が2029年に到来する」との風説を聞くが、如何なものか。

それでも移行時期は前倒し

しかしながら、二本の論文の発表を受け、海外では動きが加速している。グーグルは、論文発表に合わせて自社が所有するITシステム、サービスの耐量子暗号 (PQC) への移行を2029年までに完了させると発表した³⁾。

米国のトランプ大統領は、政府調達システムおよび重要インフラ⁴⁾についてのPQCへの移行を2030年12月31日までに完了させる大統領令⁵⁾に署名した。続いて発表された行政管理予算局 (OMB) の指針では、各連邦政府機関に対し、PQC移行計画を策定し、120日以内に提出するよう要請としている。

ECCはビットコインの基盤技術であるブロックチェーンなどの分散台帳技術やIoT機器が通信する際の認証技術として採用され、暗号通貨のみならず、防衛をはじめとしたさまざまな分野での利用がある。RSA暗

号が2030年までに解読される可能性は極めて低いが、「Harvest Now, Decrypt Later (HNDL攻撃。今収集し後で解読する)」問題の存在も無視できない。

どのITシステムにどの暗号が利用されているかを整理する「棚卸し」だけで半年から一年、さらに暗号の移行完了は大企業で十年を超えるとの推計もあり、理想的な量子コンピュータの登場を待ってからの対応では遅い。

日本企業への示唆

日本では、金融庁が「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」(2024年11月)において、優先度の高いシステムの移行に関しては2030年代の半ばを完了目標とすると発表した。また、内閣官房国家サイバー統括室は「政府機関等における耐量子計算機暗号 (PQC) への移行について」⁶⁾(2025年11月)において、「原則として、2035年までに行うことを目指す」と宣言した。しかし、今回の論文を契機にさらにPQC移行が早まる可能性は無視できない。

日本企業が着手すべきは、暗号を棚卸し、長期の機密性を要するデータを特定することである。そのためには自社だけで完結せず、委託先やシステム供給者を含めた計画が要る。まず棚卸しに着手し、その結果をもとに優先順位と期限を定める、地味だが当たり前の姿勢が必要だと考える。

Writer's Profile



藤吉 栄二 Eiji Fujiyoshi
IT基盤技術戦略室
チーフリサーチャー
専門は先端IT
focus@nri.co.jp