お知らせ

HITACHI

2026 年 7 月 14 日
株式会社日立ソリューションズ

量子コンピュータ時代に向け、耐量子計算機暗号に関する技術検証を実施【お知らせ】

金融庁が移行を推奨する耐量子計算機暗号について、処理時間、メモリ使用量、通信量の性能に関する影響を検証

株式会社日立ソリューションズ（本社：東京都品川区、取締役社長：森田 英嗣／以下、日立ソリューションズ）は、量子コンピュータ時代に向けて注目される耐量子計算機暗号[*1]（以下、PQC）に関する技術検証を実施しました。

量子コンピュータ技術の進展により、現在利用されている RSA[*2] や曲線暗号(ECDH/ECDSA[*3])などの公開鍵暗号が将来的に解読される可能性が指摘されています。こうしたリスクに備え、NIST[*4] は量子コンピュータでも解読が困難とされる PQC のアルゴリズム（ML-KEM(鍵交換)、ML-DSA(楕円電子署名)など）を標準化し、PQC への移行が世界的に進められています。国内においても金融庁が金融機関に対し、2030 年代半ばを目安に PQC への移行を推奨しています。

日立ソリューションズは、2025 年より企業のシステムで使用されている暗号技術の洗い出しからリスク評価、移行方針の提案までを行う「耐量子計算機暗号への移行に向けた支援サービス」を提供し、金融に加え製造やサービス業からも問い合わせをいただいています。このたび、関心が高まる PQC の処理時間、メモリ使用量、通信量の性能を検証し、既存暗号との比較を行いました。今後は、本検証結果で得られた知見も合わせて提供し、金融機関をはじめとするさまざまな事業者における PQC への移行検討を支援します。

*1 耐量子計算機暗号（PQC）：Post-Quantum Cryptography。格子ベース暗号、符号ベース暗号、多変数多項式暗号のように、量子計算でも解読困難な数学的構造を基盤にした暗号方式

*2 RSA（Rivest Shamir Adleman）

*3 ECDH/ECDSA（Elliptic Curve Diffie-Hellman/Elliptic Curve Digital Signature Algorithm）

*4 NIST：米国国立標準化技術研究所

技術検証と結果

1. 実施期間 2025 年 4 月 1 日～2026 年 3 月 31 日
2. 検証の概要

既存暗号から PQC という新たな暗号技術に安心して効率よく移行するために、プログラムの集合体である「ライブラリ」の選定が重要になります。どのライブラリを採用すれば既存システムへの影響が少なく、運用しやすいかという実践的な判断を支援するため、今回、複数のライブラリについて性能（処理時間、メモリ使用量、通信量）を評価しました。

また、PQC の移行では、暗号化通信を行うための共通の秘密鍵を通信相手と安全に共有する「鍵交換」と、データや文書の正当性を証明する「電子署名」が重要な要素となります。これらは処理内容や利用される場面が異なるため、システムへの影響を正しく把握するため、それぞれについて性能を評価しました。

評価においては、同一条件での繰り返し実験が可能な環境に仮想マシンを構築して測定しました[*5]。本検証の概要は以下の通りです。

*5 測定環境：Amazon Elastic Compute Cloud (インスタンス：c6i.large) 、OS：Ubuntu 24.04LTS、スペック値：vCPU:2 コア (3.5GHz)・メモリ:4GiB・ストレージ:EBS・ネットワーク帯域幅: 最大 12.5Gbps・EBS 帯域幅: 最大 10Gbps。1,000 回の測定の平均値を算出。

1）RSA や ECDSA などの従来暗号と PQC について、鍵交換、電子署名ごとに性能を比較
2）PQC を実装した 4 つのライブラリについて、同条件で性能を比較
3）従来暗号とハイブリッド暗号[*6]における TLS[*7]通信性能を比較

3. 検証の結果
1. 鍵交換では、PQC は従来暗号と比較して処理時間が約 20 分の 1 となり、高速に動作することを確認。
   一方、電子署名では、PQC と従来の処理時間は同程度。
2. ライブラリ間の比較では、鍵交換の処理時間は最大でも 0.08ms 以内の差にとどまった。
   一方、電子署名では、署名処理時間に差があり、最小 0.09ms から最大 1.02ms と約 11 倍の開きがあった。
3. TLS 通信においては、一部処理で差が出たものの、全体では約 0.66ms の差にとどまり、データ量もハイブリッド暗号で約 1KB の増加にとどまった。

*6 既存暗号と PQC を組み合わせた方式。PQC に未知の脆弱性が発見された場合でも既存暗号により安全性が維持される。
*7 TLS：インターネット通信を暗号化するプロトコル

技術検証結果の評価

・PQC への移行後、性能面で大きな劣化があると、システム性能を維持するための追加対応が必要になります。しかし、今回の結果では PQC 導入による性能影響は限定的であり、性能面での懸念は生じないことがわかりました。

・鍵交換では、ライブラリ間の性能差は小さい一方、電子署名では最大で約 11 倍の差がありました。このため、高頻度処理を行う必要のあるシステムでは高速なライブラリを選定するなど、用途に応じた選定が重要であると考えられます。

・実際の移行におけるライブラリ選定にあたっては、今回検証した性能評価に加え、プログラミング言語の違いや既存環境との互換性、ベンダーサポートの有無などビジネス要件を加味することが必要となります。

背景

量子コンピュータ時代を見据え、公開鍵暗号の安全性に対する懸念や、通信データを保存して将来解読する HNDL 攻撃[*8]への対策が求められています。NIST による標準化や金融庁の移行推奨を背景に、企業における検討は本格化しています。日立ソリューションズは 2025 年 10 月より「耐量子計算機暗号への移行に向けた支援サービス」を提供し、金融業を中心に、既存システムに適用した場合の性能影響や、暗号方式やライブラリの選定に関する具体的な問い合わせをいただいています。

日立ソリューションズは、30 年以上にわたり情報漏洩防止ソリューション「秘文」の開発で培った暗号化技術の知見に加え、秘匿化、暗号鍵分野の実績を有し、市場に先駆けて先進的なソリューションを幅広い業種に提供してきました。これらの知見やノウハウを、量子計算という新たな技術分野に発展させるとともに、新たなセキュリティリスクに対して中期的な視点で先行して取り組んでいます。本支援サービスでは、既存の暗号技術の分析からリスク評価、移行方針の提案まで、企業の対応を包括的に支援しています。さらに、このたび、研究企画部門による先進技術の検証活動を通じて、移行判断に資する実践的な知見を提供します。

*8 HNDL 攻撃：Harvest Now, Decrypt Later。現在の暗号データを盗聴・保存しておき、将来量子コンピュータで解読する攻撃手法

「耐量子計算機暗号への移行に向けた支援サービス」について

https://www.hitachi-solutions.co.jp/pqc/

日立ソリューションズについて

日立ソリューションズは、お客さまとの協創をベースに、最先端のデジタル技術を用いたさまざまなソリューションを提供することで、デジタルトランスフォーメーションを実現します。欧米、東南アジア、インドの各拠点が連携し、社会や企業が抱える課題に対して、グローバルに対応します。

そして、人々が安全にかつ安心して快適に暮らすことができ、持続的に成長可能な社会の実現に貢献していきます。

詳しくは、日立ソリューションズのウェブサイト(https://www.hitachi-solutions.co.jp/)をご覧ください。

評価結果に関するお問い合わせ先

担当：人見、松本

株式会社日立ソリューションズ

経営企画本部 研究企画部

――