Solution Brief

量子コンピュータ時代への備えは暗号の俊敏性から始まる

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

量子に備えよ

量子コンピュータによる脅威が、従来の暗号技術を危うくしています。今こそ、データ保護に向けた対策が求められています。サイバー攻撃者は、暗号化されたデータを収集・保存し、将来的に量子コンピュータを用いて復号を試みる「HNDL（Harvest Now, Decrypt Later：今収集し後で解読）」攻撃を既に実行に移しています。

PQC（Post-Quantum Cryptography：耐量子暗号、以下PQC）対応の暗号化をテストし、量子コンピューティングが既存インフラのセキュリティに及ぼす可能性のある影響を特定し、迅速な対応計画を策定するための信頼できる環境を整備しPQCの備えをしましょう。

2024年8月、NISTは最初の3つのPQCアルゴリズムを正式に発表し、組織に対し可能な限り早期の移行開始を推奨しました。NISTがこれらのアルゴリズムを正式に標準化したことで、世界各国の規制当局はNISTのPQC標準に基づくコンプライアンス要件を順次策定・発行することが見込まれます。各組織は、こうした新たな指令に対応するため、PQCへの移行準備を急速に進める必要があります。

暗号化アジャイルアーキテクチャを組み込んだPQC対応ネットワーク暗号化ソリューションで「移動中のデータ」を保護

なぜ今PQCが求められるのか?

PQCへの移行には時間を要する――だからこそ、今すぐ準備を始めることが最善の戦略です。先行して対応を進めることで、組織と顧客への影響を最小限に抑え、コストとリスクを削減し、さらに移行期間中の事業継続性を確保することが可能になります。また、NISTや各業界のPQC規制が正式に発表され次第、組織はそれらに確実に準拠できる体制を整えることが可能になります。すでに「HNDL（Harvest Now, Decrypt Later）」型の量子攻撃が確認されている今、より長い対称鍵の採用や帯域外での鍵配送といった暫定的な対策を今すぐ講じることが重要です。これにより、組織をHNDLからリスクを軽減できるだけでなく、PQC技術が実用化された際にも、より適切な準備を整えることができます。

HSE（High Speed Encryptors）PQCスターターキットをリクエストするにはスキャンしてください。（英語サイト）

PQCスターターキットで最初の一歩を踏み出しましょう

タレス高速暗号化装置（HSE）を搭載したPQCスターターキットは、量子耐性に向けた取り組みを加速する、低コストかつ信頼性の高いテスト環境を提供します。このPQCラボでは、PQCとエントロピーを活用し、アプリケーションの実行やデータ転送をシミュレーションすることで、アーキテクチャの検証を支援します。今から準備を始めることで、将来ファームウェアにおいてPQCアルゴリズムが正式に実装された際にも、スムーズに本番環境へ移行できるような運用計画を立てることが可能です。

以下の機能により、耐量子テスト環境を簡単に構築できます。

- ✓ **NISTポスト量子アルゴリズムを実装済み**
- ✓ **NIST承認のKDF方式による帯域外鍵管理**
- ✓ **ETSI eQKD v14.01による量子鍵配布（オプション）**
- ✓ **QRNG（量子乱数生成）または外部エントロピーソース（BYOE – お客様独自の暗号化方式）（オプション）**

HSE PQCスターターキットに含まれるもの

本スターターキットは、フル機能のHSE（高速暗号化装置）で構成されており、実稼働環境に導入することで、既存のネットワークのセキュリティを強化とパフォーマンス向上を実現します。

- **タレスHSEポートフォリオから選択された3つのHSEネットワーク暗号化アプライアンス**
  - **CN4010/CN4020:** 最大1Gbpsのネットワーク暗号化装置。認証取得済みの高性能小型フォームファクタで、CNI、SCADA、音声/ビデオなどのリモート拠点に最適。
  - **CN6010:** 1Gbpsのネットワーク暗号化装置。ラックマウント可能で、完全冗長設計の堅牢な設計。プライベートネットワークやデータセンターに最適。
  - **CN6140:** 最大4x10Gbpsのネットワーク暗号化装置。拡張性を高める4つの独立した暗号化チャネルを備え、高い拡張性とマルチリンクネットワークをサポート。
- **CM7 Network Manager – 暗号化管理プラットフォーム（カスタマーポータルサイトからダウンロード可能）**
- **推奨される追加項目**
  - 電源コード（CN6000シリーズ）
  - トランシーバー（CN6000およびCN4020ユニット専用）
  - メンテナンスとサポート
  - リモートインストールと設定

cpl.thalesgroup.com/ja
お問い合わせ先 すべてのオフィスの所在地と連絡先情報につきましては、cpl.thalesgroup.com/ja/contact-us をご覧ください。