Compliance Brief

THALES
CYBERSECURITY

量子関連に起因するサイバーセキュリティリスクへの対応に関するシンガポール金融管理局(MAS)勧告への準拠

cpl.thalesgroup.com

THALES

CYBERSECURITY

MAS勧告とは？

2024年2月20日、シンガポール金融管理局（MAS）は、金融機関のCEOに対し、「量子関連のサイバーセキュリティリスクへの対応に関する勧告（Advisory On Addressing The Cybersecurity Risks Associated With Quantum）」（以下、「勧告」）に関する通達（MAS/TCRS/2024/01号）を発出し、量子コンピューティングの発展から生じるサイバーセキュリティリスクへの対応を金融機関に強く促すとともに、検討すべき緩和策を明らかにしました。

MAS勧告は、量子コンピュータの登場によって顕在化するリスク、特に現在の公開鍵基盤で広く使用されている従来型の非対称暗号に対する脅威に焦点を当て、クリプトアジリティ（暗号の俊敏性）の確保と量子セキュリティの実装という2つの中核的な推奨事項を提示しています。

この勧告では、金融機関が量子対応への移行を進めるにあたり、クリプトアジリティを実現するために検討すべき3つの取り組みを強調しています。

- 量子コンピューティングの最新動向を常に把握し、関連するサイバーセキュリティリスクに対する認識を高める。
- すべての暗号資産のインベントリを維持し、優先して耐量子に移行すべき資産を特定する。
- 量子関連のサイバーセキュリティリスクに対応するための戦略を策定し、必要な能力を構築する。

量子関連サイバーセキュリティリスクへの対応に関する勧告と、タレスの取り組み

金融機関を量子の脅威から保護するには、耐量子アルゴリズム（QRA）をサポートし、量子鍵配送（QKD）と量子乱数生成（QRNG）のオプションも提供するサイバーセキュリティソリューションが必要です。タレスは、ポスト量子クリプトアジャイル戦略をサポートするソリューションの提供に取り組んでいます。

将来を見据えたポスト量子戦略の構築

- **耐量子アルゴリズム:** QRAは、格子ベース、多変数、ハッシュベース、符号ベースの暗号化のいずれであっても、量子攻撃から保護するための基本です。
- **量子乱数生成:** QRNGは、 量子力学固有のランダム性を利用して暗号鍵を生成する高ビットレートの乱数源です。
- **量子鍵配送:** QKDは、量子物理学の原理と量子力学の特性に基づいて、共有された当事者間で暗号鍵を配送します。

タレスは、金融機関のクリプトアジリティ実現に向けた3つの領域に取り組んでいます。

量子関連のサイバーセキュリティリスクへの対応に関する勧告	タレスのソリューション
1.量子コンピューティングの最新動向を常に把握する 「…PQCやQKDなどの量子セキュリティソリューションを用いた緩和の可能性…」 「…商用化された段階で耐量子ソリューションを提供するようベンダーに要請すること…」	タレスのLuna HSMと高速ネットワーク暗号化システムは、金融機関が確実にPQCに対応するためのクリプトアジリティを実現します。 • NISTの最終候補の耐量子アルゴリズムを追加して商用化された、量子対応のLuna HSM（ハードウェアセキュリティモジュール）で暗号鍵を強化します。 ◦ 耐量子アルゴリズム（QRA）：PQC FMにより、ハッシュベースの署名（SP800-208）をサポートします。 ◦ 統合型/カスタムメイドのPQC：Lunaの機能モジュール（FM）や、さまざまなパートナーFM/インテグレーションを使用して、独自のポスト量子暗号を実装します。 ◦ QRNG: QRNGとLuna HSMの安全な鍵ストレージで量子エントロピーを注入します。 • HSE（High Speed Network Encryptors：高速ネットワーク暗号）ソリューションは、クリプトアジャイルなFPGAベースのアーキテクチャにより、ポスト量子暗号（PQC）をサポートし、移動中データを安全に保護します。HSEは、商用化された初の耐量子ネットワーク暗号化ソリューションであり、将来の量子攻撃に備えた長期的なデータ保護を金融機関に対して提供できます。データセンターと本社間のネットワークトラフィックから、オンプレミスやクラウドでのバックアップ、ディザスタリカバリサイトまで、あらゆる場所で暗号化を実行する単一のプラットフォームを提供します。

量子関連のサイバーセキュリティリスクへの対応に関する勧告	タレスのソリューション
2. 暗号資産のインベントリを維持する 「…金融機関において使用されている**暗号ソリューションのインベントリを特定し維持する**とともに、商用化された段階で**耐量子ソリューションへの置き換え**が必要となる可能性のある脆弱なソリューションを特定すること…」 「…**潜在的に脆弱な暗号**ソリューションに依存している**IT資産とデータ資産を分類すること**…」 「…既存のシステムインフラがクリプトアジリティに対応可能かどうかを評価し、段階的なアップグレードを検討すること…」	タレスの鍵管理および量子対応ソリューションを利用して、金融機関はクリプトアジリティを実現し、暗号資産のインベントリを維持することができます。 • 金融機関は、タレスの鍵管理を利用して暗号資産のインベントリを維持できます。FIPS140-2に準拠した仮想アプライアンスやハードウェアアプライアンスを活用することで、タレスの鍵管理ツールやソリューションは機密性の高い環境に高度なセキュリティを提供し、自社開発の暗号化やサードパーティのアプリケーションに対する鍵管理を一元化します。 • PQC対応のLuna HSMは、一元的な鍵管理で暗号鍵を保護し、金融機関が暗号資産のインベントリを効果的に管理できるようにします。Luna HSMは、使用中の暗号アルゴリズムと鍵長、暗号資産の所有者と管理責任者、そして暗号アルゴリズムが組み込まれている、または使用されている特定のシステムやアプリケーションに対する可視性を金融機関に提供します。 • PINやパスワードの送信に用いられる非対称暗号は、量子コンピューティングに対して脆弱です。LunaHSMで保護された鍵マテリアルを使用するハイブリッド鍵確立ソリューションは、そのリスクを軽減します。このソリューションは、耐量子アルゴリズムをサポートし、さまざまな数学的手法に基づく鍵共有と鍵配送のオプションを備えた、強固な量子対応ソリューションを構成します。 HSEソリューションは移動中データを保護し、クリプトアジャイルなFPGAベースのアーキテクチャにより、すべての製品でNIST耐量子公開鍵アルゴリズム（最終候補）の4つすべて（とさらに最終候補以外のアルゴリズム）をサポートします。HSEは、10年以上にわたり量子に対応してQKD互換性を備えており、量子乱数生成（QRNG）が統合されています。
3.量子関連のサイバーセキュリティリスクに対応するための戦略を策定し能力を構築する 「…**技術的な能力**の向上…」 「…リソースが許す限り、**量子セキュリティソリューションを用いた概念実証試験を検討**し、その潜在的な影響を金融機関に認識させること…」	タレスのPQCスターターキットにより、金融機関は量子対応ソリューションを安全にテストし、必要な能力を構築することができます。 PQCスターターキットは、Quantinuumとの提携により、安全な環境で量子耐性対策をテストするプロセスを加速します。このキットは、信頼できるLuna HSM内に信頼性の高い環境を構築し、PQC対応の鍵をテストすることで、本番環境の鍵管理プロセスに影響を与えることなく、インフラに対するこれらの変更の影響を理解することができます。

タレスについて

タレスはデータセキュリティのグローバルリーダーとして、世界中で高い信頼を得ているさまざまな組織が、あらゆる場所で重要なアプリケーション、機密データ、およびIDを包括的に保護できるよう支援しています。タレスは、革新的なサービスと統合プラットフォームを通じて、リスクの可視化、サイバー攻撃の防御、そしてコンプライアンスギャップの解消を可能にし、毎日数十億人の消費者に安心で信頼性の高いデジタルエクスペリエンスを提供します。