

耐量子安全性を 実現する タレスLuna HSM

クリプトアジリティを備え、
PQC対応の未来に向けた
デジタルトラストの再定義

ハイライト

Luna HSMの特長

- 次世代HSM「Luna 8」は、設計段階から量子安全性を考慮して構築されており、PQCアジリティ、強力なエントロピー、更新可能なプロトコル、ポスト量子性能に最適化されたタレス独自設計の暗号プロセッサを組み合わせています。
- ハイブリッドPQC鍵交換メカニズムにより、鍵の安全な同期、バックアップ、復元を可能にします。
- TLS/SSL、鍵交換、IoT、データベース暗号化などのユースケースにポスト量子保護を提供し、「HNDL (Harvest Now, Decrypt Later: 今収集し後で解読)」リスクへの対処を支援します。
- サイドチャネル攻撃や物理攻撃への耐性を標準搭載し、高保証の暗号保護を提供します。
- Luna 7 製品ファミリーでは、NISTが標準化したアルゴリズムを Luna HSM のファームウェアに直接実装しています。これには、ML-KEM (FIPS 203) および ML-DSA (FIPS 204) が含まれます。



問題

現在広く利用されているRSA、ECC、Diffie-Hellmanなどの公開鍵暗号システムやプロトコルは、従来のコンピュータに対しては安全であり、公開鍵基盤 (PKI) の中心的な役割を担っています。これらは、デジタルエコシステム全体にわたる証明書発行、認証、信頼チェーンを支えています。しかし、将来の量子コンピュータは、これらのシステムが依存する数学的基盤を破ると予想されており、現在のアルゴリズムやそれに依存するシステムが危険にさらされます。攻撃者はすでに、後で復号することを意図して暗号化データを収集しているため、長期保存されるデータやデジタルトラスト資産は、すでに差し迫ったリスクに直面しています。

課題

組織は今すぐ、ポスト量子暗号 (PQC) への移行を開始すべきです。量子攻撃に脆弱な暗号を特定し、高リスクかつ長期保存される資産を優先順位付けし、従来のアルゴリズムとNISTが標準化したポスト量子暗号 (PQC) アルゴリズムの両方をサポートするハイブリッド環境へと移行の準備を進めましょう。

この移行は、チーム、テクノロジー、サプライヤー、運用上の制約にまたがる、複数年にわたる取り組みです。現状把握、優先順位付け、相互運用性テスト、ベンダーとの調整、段階的な導入にはいずれも時間がかかり、これらの要因は多くの場合、アルゴリズムの利用可能性と同程度に、移行の進捗ペースを左右します。また、移行のタイムラインは、インフラの成熟度、サプライヤーの準備状況、ハードウェアの制約、進化し続ける標準や規制要件の影響も受けます。

HSM (ハードウェアセキュリティモジュール) は、デジタルトラストの中核となる鍵の生成・保管・暗号処理を保護するため、この移行プロセスでは特に重要です。PQCへの移行準備を進めるにあたり、HSMには、従来型および量子安全な鍵と証明書、クリプトアジリティ、NISTが標準化したポスト量子アルゴリズムへの対応がますます求められています。HSMが移行に必要なアルゴリズム、インターフェース、証明書、運用モデルに対応できなければ、それに依存するシステムやワークフローは前進できません。そのため、HSMの選定はPQC計画上の戦略的要素となります。



ソリューション

Luna HSM は、ポスト量子暗号への移行を進める組織に、信頼性の高い、耐タンパー性を備えた基盤を提供します。セキュリティチームは、機密性の高い鍵を保護し、重要な暗号処理を支え、新たなポスト量子(PQC)機能を統制された適切な運用環境で導入できます。FIPS 140-3およびコモンクライテリアEAL 4+に対応するよう設計されており、PKI、認証局の保護、コード署名、ファームウェア署名など、トラスト(信頼)が重要となるワークフローにおいて、高保証の暗号処理をサポートします。

Luna HSMは、ML-KEM(FIPS 203)、ML-DSA(FIPS 204)に加え、NIST SP 800-208で規定されているHSSをサポートしています。これにより、リスクプロファイル、運用要件、移行タイムラインに応じて、ハイブリッド方式または完全なPQC方式を柔軟にテスト、検証、導入できます。また、Luna HSMには、QRNGベースの機能を含む、高品質なハードウェアベースのエントロピーソースが組み込まれており、高保証の鍵生成をサポートします。主要なクリプトアジリティ対応プラットフォームと統合することで、新しい暗号アルゴリズムが登場した際にも、より統制された、相互運用性の高い形で導入できます。これにより、暗号標準が進化しても大規模な再設計を必要とせず、アプリケーションやユースケースが将来の変化に適応できるようにします。

Luna HSMで実現できること

- 量子安全な署名方式に備えることで、デバイスやソフトウェアのデジタル署名戦略を将来の変化に適応できるようにし、長期にわたり信頼性の高いソフトウェアおよびファームウェアの更新を維持できます。
- ステートフルハッシュベース署名方式を、高保証の署名用途に利用できます。NIST SP 800-208で規定されている標準に基づく方式や、NSAのCNSA 2.0におけるソフトウェア/ファームウェア署名のガイダンスに準拠した方式も利用できます。
- ML-KEM(FIPS 203)やML-DSA(FIPS 204)など、鍵交換、暗号化、デジタル署名に使用するNISTが標準化したPQCアルゴリズムを実環境で検証できます。
- インフラに大きな変更を強いることなく、進化する暗号モデルに適応し、従来の暗号からPQCへの移行をより統制された形で進められます。
- 重要な鍵、証明書、署名処理を支えるハードウェアの信頼の基点(Root of Trust)を強化します。
- PKI、TLS、コード署名、IoT、データベース暗号化など、トラスト(信頼)が極めて重要となる環境全体でPQC対応を推進します。
- ビジネスニーズに最適な量子安全ハードウェアを、幅広い選択肢の中からお選びいただけます(Luna Network、PCIe、USB、Backup HSMソリューション)。

主なメリット

- コード署名、ファームウェア署名、PKI、マシンアイデンティティなど、重要度の高いユースケースを量子移行に備えることで、レジリエントなデジタルトラストの基盤を構築します。
- 認証取得済みの耐タンパー性ハードウェア内で、耐量子性を備えた鍵を安全に生成し保護します。
- 暗号ポリシーを継続的に検証・適用・更新できるように設計されたプラットフォームにより、クリプトアジリティを支援します。
- 従来型、ハイブリッド、ポスト量子環境に統制の取れた形で対応することで、移行リスクを低減します。
- 移行期間を通じて信頼性を維持する必要があるシステムやワークフローに対し、より強固なガバナンスと保証を維持します。



PQCエコシステム全体で 実証済み

PQCへの移行は、プラットフォーム、アプリケーション、サプライヤー間の相互運用性に依存します。タレスは市場でも屈指の広範なパートナーエコシステムを有し、PKIや鍵管理環境のPQC対応状況の検証を支援し、より確かな自信を持って移行を進められるようにします。

タレスは、主要なテクノロジーパートナーや一部のお客様と緊密に連携し、実際のHSMユースケースを通じてPQC機能のテストと検証を行っています。これにより、多様なプラットフォームや導入モデルにおける運用準備状況を確認し、お客様がより実践的に量子対応を進められる道筋を提供します。最近行われた大手金融機関との共同取り組みの一例では、FIPS認証済みのタレスLuna HSMの暗号境界内で、検証済みの量子エントロピーを用いた、QRNGベースの安全な鍵生成を可能にし、クリプトアジリティの強固な基盤の構築を支援しました。



タレスは、標準化、提携、パートナーシップを通じて、信頼できるPQCエコシステムの形成を主導しています。

次のステップ: 反復的なPQC移行 プログラムを構築する

こうした対応準備を踏まえ、PQCへの移行は一度きりのチェックリストではなく、反復的なプログラムとして取り組むべきです。効果的な移行は、まずシステム、アプリケーション、サプライチェーン全体で量子攻撃に脆弱な暗号を特定することから始まります。その後、リスク評価、ポリシーの見直し、重要インフラがハイブリッドモデルやポスト量子モデルに対応できるかどうかの検証を行います。4つの成熟度レベルを通じて、最もリスクにさらされている資産を優先し、段階的な移行と緩和策の計画を立て、継続的な監視・ガバナンス・改善を通じて、クリプトアジリティを段階的に強化できます。

Luna HSMが、クリプトアジリティと量子安全な移行を支える基盤の強化にどのように役立つかをご覧ください。

タレスについて

タレスはサイバーセキュリティのグローバルリーダーとして、企業、政府機関、そして世界で最も信頼される組織が、重要なアプリケーション、機密データ、ID、ソフトウェアを場所を問わず大規模に、かつ最高の投資対効果(ROI)で保護できるよう支援しています。フォーチュン・グローバル500企業の58%を含む3万社以上の顧客を抱え、そのソリューションは世界148カ国で導入されています。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して信頼性の高いデジタルエクスペリエンスを提供します。

クリプトアジリティ: 反復的なループ

NIST CSWP.39 Crypto Agility Strategic Plan (クリプトアジリティ戦略計画)



出典: [NIST CSWP.39 Crypto Agility Strategic Plan \(クリプトアジリティ戦略計画\)](#)