Case Study

THALES
CYBERSECURITY

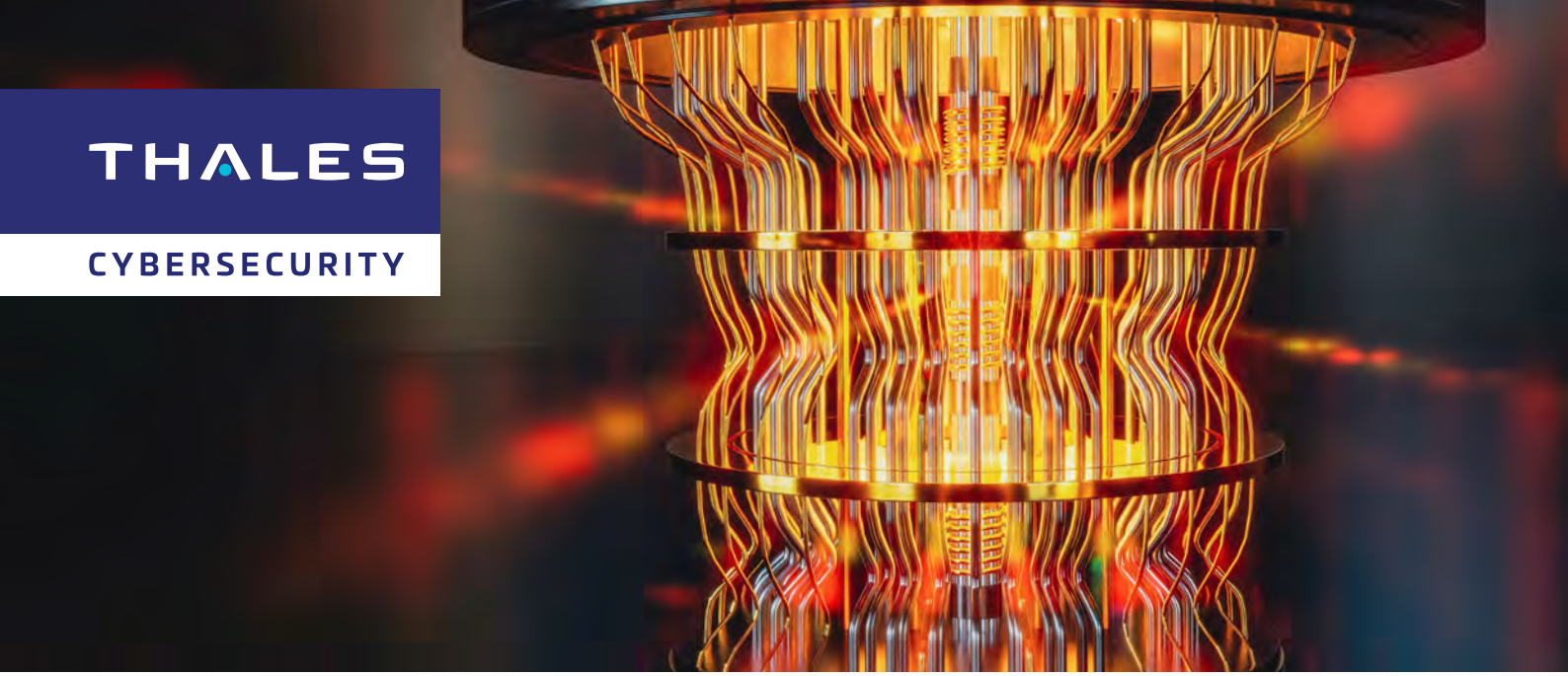
金融サービス企業におけるタレス Luna HSMとQuantinuumの活用

大手金融サービス企業が、タレスと連携して耐量子暗号ソリューションを開発

cpl.thalesgroup.com

THALES

CYBERSECURITY



量子コンピューティングの商業利用が現実味を帯びてくる中、標準的な公開鍵暗号は重大なセキュリティ上の課題に直面しています。現在のアルゴリズムのいくつかは、量子コンピューティングプラットフォーム上では数時間から数分で破られる可能性があります。このため、データセキュリティを将来にわたって維持するために、多くの企業がポスト量子暗号（PQC）ソリューションを活用し、レジリエンスとクリプトアジリティ（暗号の俊敏性）を構築しています。このような耐量子アルゴリズムやプロセスを導入することで、日々進化する将来の脅威に対しても揺るぎないデータ保護を実現できますが、多くの企業は、労力がかかるプロセスやコストのかかる改修に不安を感じています。

課題

ある多国籍金融サービス企業は、顧客が信頼を寄せるデータ、システム、アプリケーションの安全性を維持できるよう、戦略的で堅牢な技術ソリューションの策定に積極的に取り組んでいました。

同社は、データ収集（data harvesting）の脅威から保護するために、証明可能安全性を持つ鍵生成を使用して、銀行業務とイノベーションのワークフローにPQC対応のセキュリティ対策を確立することを目指していました。レガシーハードウェアやシステム全体のアプリケーション、関連証明書、複数ベンダーのソリューションが混在する中で、日常業務への影響を最小限に抑えながら、既存のIT環境に容易に統合できる新たなソリューションを選定する必要がありました。選択肢を検討する中で、このチームは、全社的に展開可能で拡張性と俊敏性に優れたPQCアプローチを開発したいと考えていました。

ソリューション

同社は、Quantinuumおよびタレスと連携し、安全な鍵の生成、管理、保護を実現するための商用の耐量子ソリューションを共同で開発しました。

Quantinuumは、量子コンピュータで強化されたエントロピーを活用するQuantum Originソリューションを通じて、極めて予測困難な鍵を生成する能力を提供しています。暗号技術では、エントロピーは乱数生成に利用され、強力な暗号鍵の基盤となります。量子コンピュータによって駆動されるこのプラットフォームは、安全な鍵生成のために高品質な固有のランダム性を提供します。このような大手金融サービス企業は、一般的な業界標準を超える数学的に検証可能なプロセスに基づいて、耐量子暗号鍵をオンデマンドで生成することが可能となり、真性乱数生成器（TRNG）や第一世代の量子乱数生成器（QRNG）で発行された鍵と比較して、セキュリティが向上します。

タレスのLuna HSM（ハードウェアセキュリティモジュール）は、鍵を物理的にも論理的にも保護するために活用されています。Luna HSMはデジタルトラストの基盤として機能し、現在からPQCの未来に向けたクリプトアジリティを実現します。Luna HSMの利用者は、その俊敏性、使いやすさ、拡張性のメリットを受けています。Luna HSMは従来のテクノロジーと新しいテクノロジーの両方に対して、セキュリティと高性能のバランスを提供するよう意図的に設計されており、オンプレミス、クラウド、ハイブリッド環境のいずれにも展開可能です。Luna HSMは、暗号鍵を常にハードウェア内に保管することで、最高レベルのセキュリティを提供します。侵入に強く、改ざん検知機能を備えたFIPS検証済みのアプライアンスに鍵が閉じ込められるため、安全な暗号基盤が提供されます。すべての暗号処理はHSM内部で行われ、強力なアクセス制御により、権限のないユーザーが機密性の高い暗号マテリアルにアクセスすることを防ぎます。

さらに量子脅威への耐性を強化するため、Quantum OriginがタレスLuna HSMにシームレスに統合されています。Quantum Originプラットフォームは、量子強化エントロピーを、Luna HSMの既存の決定論的乱数ビット生成器（DRBG）にシードとして供給します。この統合により、タレスLuna 7 HSMから直接、量子コンピューティングに耐性を持つ暗号鍵を生成できます。

成果

この耐量子ソリューションにより、同社は強固な耐量子暗号鍵を、生成し、安全に保管し、既存の業務手順にほとんど影響を与えることなく大規模なITインフラ全体に展開することができます。Quantinuumとタレスによるこのソリューションを活用することで、同社はFIPS 140-2レベル3認定アプライアンス内で耐量子非対称鍵を生成できるようになりました。

特筆すべきは、この大手金融サービス企業が、既存および進化するインフラに対してクリプトアジャイルな耐量子保護を開発することで、PQC時代への備えが可能であることを実証している点です。これと並行して、同社はタレスおよびQuantinuumと連携して、ネットワーク移動中データの暗号化の保護にも取り組んでいます。現在からクリプトアジャイルなソリューションを活用することで、将来的に耐量子保護の標準が確立された後も、セキュリティ改修にかかる多大なコストを回避できます。

結論

量子コンピューティングは、データに重大なセキュリティリスクをもたらします。こうした新たな脅威から保護し、顧客が信頼を寄せるシステムの安全性を現在から将来にわたって維持するために、この大手金融サービス企業は、レガシーおよびポスト量子暗号（PQC）アルゴリズムの両方に対応可能なクリプトアジリティを確保するPQC戦略を確立し、Quantinuumとタレスのソリューションを活用しています。タレスとQuantinuumは協力して、組織が持続可能な量子レジリエンスを構築し、日々進化する量子コンピューティングによるサイバーセキュリティの脅威からビジネスを保護するための支援を行っています。

Quantinuumについて

Quantinuumは、Honeywell Quantum Solutionsの世界最先端のハードウェアと、Cambridge Quantumの業界をリードするミドルウェアおよびアプリケーションを併せ持つ世界最大級の量子コンピューティング企業です。科学主導で事業を展開し、量子コンピューティング、化学、サイバーセキュリティ、金融、データ処理の最適化などのアプリケーション開発を加速させています。エネルギー、物流、気候変動、健康などの分野で、世界が直面する最も差し迫った問題を解決するための拡張性のある、商業向け量子ソリューションの開発に重点を置いています。

タレスについて

今日の企業は、決定的な意思決定を行うために、クラウド、データ、ソフトウェアに依存しています。そのため、世界で評判の高いブランドや最大手の組織は、クラウドやデータセンターからデバイス、ネットワーク全体に至るまで、作成、共有、保存場所を問わず機密情報やソフトウェアを保護し、それらへのアクセスを安全に確保するために、タレスに信頼を寄せています。当社のソリューションは、企業がクラウドに安全に移行し、自信を持ってコンプライアンスを達成し、何百万人もの消費者が毎日利用するデバイスやサービスにおいて、ソフトウェアからより大きな価値を生み出すことを可能にします。

当社は、データ保護における世界的リーダー企業です。暗号化、高度な鍵管理、トークン化、認証とアクセス管理を通じて、企業がデータ、ID、知的財産を保護・管理するために必要なものすべてを提供しています。クラウド、デジタル決済、ブロックチェーン、モノのインターネットのいずれのセキュリティを確保する場合でも、世界中のセキュリティ専門家がタレスに信頼を寄せ、組織のデジタルトランスフォーメーションを自信を持って推進しています。タレス クラウドプロテクション&ライセンシングはタレスグループの一部です。

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、https://cpl.thalesgroup.com/about-us をご覧いただくか、@ThalesCloudSec on Twitter.をフォローしてください。

cpl.thalesgroup.com/ja

お問い合わせ先 – Email: cpl.jpsales@thalesgroup.com

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。