信頼の強化:
サイバーセキュリティとデジタルアイデンティティにおけるタレスの耐量子暗号(Post-Quantum Cryptography)へのアプローチ

THALES
Building a future we can all trust

信頼の強化: サイバーセキュリティとデジタルアイデンティティにおけるタレスの耐量子暗号(Post-Quantum Cryptography)へのアプローチ

モバイル接続ソリューション | アイデンティティ&バイオメトリックソリューション | サイバーセキュリティ製品

タレスのサイバーセキュリティとデジタルアイデンティティ

タレスはデータセキュリティ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、データやアイデンティティ、知的財産を保護し管理するために必要なツールを提供しています。クラウド、デジタル決済、ブロックチェーン、IoT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、自信を持って組織のデジタルトランスフォーメーションを推進しています。

タレスは、デジタルセキュリティソリューションの主要プロバイダーとして、ますます相互接続が進む世界において、重要な資産、アイデンティティ、データの保護を専門としています。Thales Cybersecurity & Digital Identityは、イノベーションと信頼性に重点を置き、サイバーセキュリティ、暗号化、認証、生体認証、セキュア通信技術を網羅する包括的な製品とサービスを、特定の市場をターゲットとするビジネスラインを通じて提供しています。

すべての人が信頼できる未来のために、タレスは脅威を予測し、それに応じて製品やサービスを進化させる必要があります。量子コンピューティングは技術に大変革をもたらす可能性を秘めていますが、同時に現在の暗号方式にとって重大な脅威でもあります。そのため、PQC (Post-Quantum Cryptography:耐量子暗号、以下PQC)の開発は不可欠であり、将来の量子ベースの攻撃からデータを積極的に保護することが求められます。戦略的に考え、変化による混乱やコストを最小限に抑えるために、今すぐ準備を始めましょう。タレスは、組織とその顧客が頼りにしている重要な信頼を維持するために、耐量子安全な未来に向けて、PQCへの移行準備を今すぐ始めることを推奨します。

タレスの量子技術への取り組み

タレスの量子技術への取り組みは、2021年に発表されたフランスの野心的な国家量子コンピューティング計画を受けて勢いを増しました。タレスは将来を見据え、量子センサー、量子通信、PQCの3つの分野に焦点を当て、量子力学という未知の領域を切り拓きました。タレスは先進的な研究を通じて物質の潜在能力を利用し、超伝導量子干渉素子(SQUID)[1]、固体センサー[2]、冷却原子技術[3]などの高度な技術を探求してきました。これらの取り組みは、医療診断や軍事情報分野への応用につながる可能性を示しました。同時にタレスは、欧州全域の機密データ通信を保護するために、EuroQCIコンソーシアムと連携し、堅牢な量子通信ネットワークの確立に乗り出しました。量子コンピュータの台頭を見越し、タレスは既存のシステムをPQCで強化し、デジタル相互接続の時代におけるレジリエンスを確保しています。フランスの戦略的ビジョンに導かれ、タレスは主権的な量子技術の分野で卓越性を追求し続けています。

タレスは10年以上にわたりPQCの研究開発に積極的に取り組んでおり、業界の規制機関によるさまざまな標準化の取り組みに貢献してきました。現在、米国、フランス(RISQ)、欧州全域で複数の研究プロジェクトに参画し、この分野に関する数多くの博士論文に資金を提供しています。また、タレスはFalconデジタル署名アルゴリズムの共同開発者でもあり、これは2022年にNISTによってPQC標準化候補として選定されました。

タレスは、フランス国内の6つの企業や組織で構成されるRESQUE(RÉSilience QuantiquE:量子レジリエンス)コンソーシアムを統括しています。RESQUEは先頃、企業や地方自治体の通信、インフラ、ネットワークを将来の量子攻撃から保護するためのPQCソリューションを開発する3年間のプロジェクトを発表しました。

さらにタレスは、Post-Quantum Cryptography Alliance(耐量子暗号アライアンス)、PKI Consortium(PKIコンソーシアム)、CFDIR Quantum-Readiness Working Group(CFDIR量子対応ワーキンググループ)など、北米および欧州の複数の耐量子暗号(PQC)コンソーシアムに参加しています。また、Thales Cybersecurity & Digital Identityと米国連邦政府専用にサービスを提供する米国拠点のThales Trusted Cyber Technologies(TCT)は、いずれも、NISTのNational Cybersecurity Center of Excellence(NCCoE)の「耐量子暗号(PQC)への移行プロジェクト」に参加しています。タレス製品は、量子に脆弱な従来の公開鍵アルゴリズムと新しいPQCアルゴリズムの間を柔軟に切り替えられるクリプトアジリティを備えており、このNCCoEプロジェクトに貢献しています。これらの製品は、あらゆる脆弱性の発見を支援すると同時に、PQCの相互運用性テストのためのプラットフォームを提供するという独自の能力を備えています。

Thales Trusted Cyber Technologies(TCT)と米国家安全保障局(NSA)は、米国国立標準技術研究所(NIST)が選定したPQCアルゴリズムをHSM(ハードウェアセキュリティモジュール)上で動作させた場合の評価に関する共同研究開発契約(CRADA)を締結しました。

タレスは、NIST PQCアルゴリズムの最終候補を積極的に自社製品に試し実装することで、製品ライン全体にクリプトアジリティを導入しており、現在はこれらの選定されたPQCアルゴリズムに注力しています。タレスはまた、特にデジタル署名と鍵交換メカニズムにおけるハイブリッドアルゴリズムについて、顧客との実用的な概念実証(PoC)に向けて加速しています。タレスは、組織が強力な耐量子暗号戦略(クリプトアジャイル)を採用する必要があると認識しており、量子コンピューティングの本格化に備えて、今からクリプトアジリティを実践することを推奨しています。これにより、将来的なセキュリティ改修に伴う多大なコストを回避できます。この設計原則は、導入後も暗号方式の変更を容易にし、NISTの標準化プロセスが完了した後の耐量子ソリューションへの移行準備を可能にします。最後に、タレスは最近、GSMAの電気通信ユースケース向けのポスト量子暗号ガイドラインの執筆に貢献し、ガバナンス、リスク分析、クリプトアジリティの重要性を強調しています。

[1] ***超伝導量子干渉素子:*** *極めて高い精度で磁束を測定できる高感度機器。*
[2] ***固体センサー:*** *温度、圧力、力、加速度などの物理現象を検出して測定し、通常は電子信号として対応する出力を提供する電子センサー。*
[3] ***冷却原子技術:*** *原子を極低温まで冷却することで、新たな量子現象の探究や未知の物質状態の発見を可能にし、さまざまな量子現象の研究と理解を深めるための科学的アプローチ。*

サイバーセキュリティとデジタルアイデンティティのための耐量子ソリューション

耐量子安全な未来に向けた準備

サイバーセキュリティ製品

- HSE（高速ネットワーク暗号化システム）
- HSM（ハードウェアセキュリティモジュール）
- CipherTrust Data Security Platform

アイデンティティ＆バイオメトリックソリューション

- セキュアID
- セキュアパスポート
- アイデンティティサービス

モバイル接続ソリューション

- eSIM（組み込みSIM）
- eSE（組み込みセキュアエレメント）
- OTAプラットフォーム
- リムーバブルSIM

コード署名　ネットワーク　通信　認証局（CA）　TLS　PKI　アイデンティティ

サイバーセキュリティとデジタルアイデンティティにおけるタレスのPQCへの注力

アイデンティティ&バイオメトリックソリューション

政府市場において、タレスは「安全で持続可能なユーザー中心のソリューションで、人々のアイデンティティと市民の権利を守る」ことを使命としています。タレスは、物理的セキュリティと電子的セキュリティのあらゆる効果を組み合わせた包括的なセキュリティアプローチにより、アイデンティティ&バイオメトリックソリューションとサービスを設計、構築、提供しています。暗号技術もその一部です。

量子コンピュータは、電子ID、健康カード、パスポートなどの渡航文書に現在導入されている非対称暗号を破る可能性があり、事前に対策を講じなければ、セキュリティとプライバシーに深刻な影響を及ぼすおそれがあります。以下は、その影響の例です。

- オンラインまたはオフラインのシステムやデバイスに対する PKI ベースの認証や認可が偽造され、安全でなくなる可能性。
  - 不正な検査端末や検証端末がIDカードやパスポートを認証し、チップに格納された秘密データにアクセスする可能性がある。
  - 攻撃者が市民のアイデンティティを盗み、公共の電子政府サービス、バンキングやeヘルスなどの民間の電子サービスにログインし、ユーザーデータにアクセスする可能性がある。
- データに対するデジタル署名が、署名者の証明や改ざん防止機能を失う可能性。
  - 発行国によって署名されたID カードやパスポート内のアイデンティティデータが改ざんまたはゼロから偽造された場合でも、パッシブ認証に使用されるCSCA（Country-Signing CA）のDS（Document Signing）鍵が破られると、それを検出できない可能性がある。
  - 電子署名付きの文書（PDF、Webフォームなど）が、PKI証明書に含まれる公開鍵から秘密署名鍵が特定されることで、手書きの署名と同等の法的効力を失う可能性がある。
- 攻撃者が直前の鍵交換を傍受し、使用された秘密鍵を特定することで、2者間の暗号化通信の機密性が失われる可能性。
  - ICAO（国際民間航空機関）の渡航文書で使われるEACおよびSACプロトコルの鍵交換が、チップの複製防止や機密データへのアクセス保護、文書と検査端末間の非接触通信の暗号化解読防止といった機能の強度を失う可能性がある。
  - IDカードとオンラインサービス間の暗号化通信、またはIDカードを用いた暗号化メール、Webセッション、VPNの設定といった用途におけるセキュリティが破られる可能性がある。

アイデンティティ&バイオメトリックのための PQCソリューション

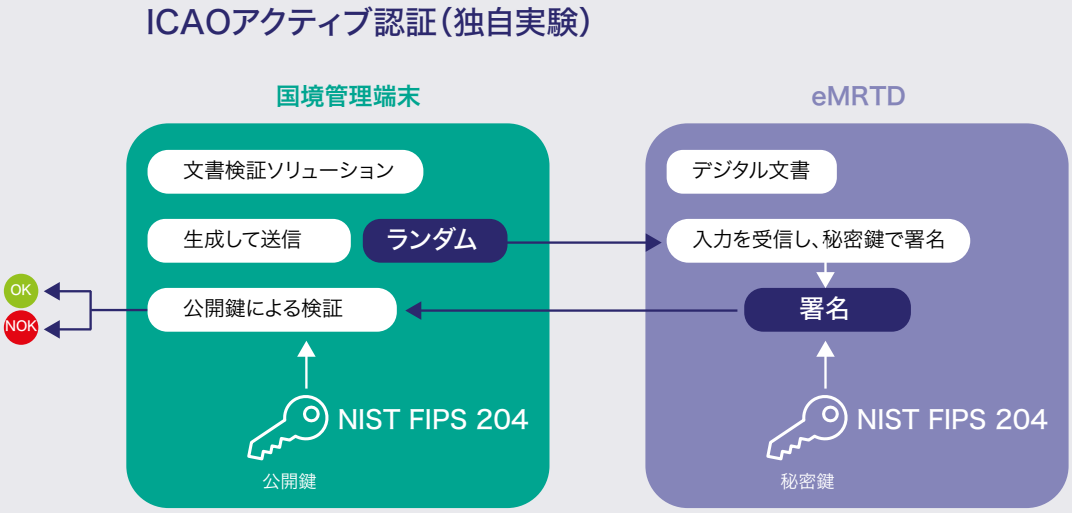
上記の懸念に対応するため、タレスは電子文書プレミアムPQC向けの初の耐量子対応オペレーティングシステムであるMultiApp v5.2を導入しています。タレスは、ユーザーデータの拡張に対応できる十分な空きメモリを備えた新しい高性能チップ上に、このオープンかつアジャイルなプラットフォームを構築しました。最新のJavaCardおよびGlobalPlatform標準に準拠しており、多様な政府用途に対応するJavaCardアプレットのフルスイートも提供します。この全く新しい製品は、ハイブリッド暗号アプローチを採用し、サポートしています。

- 従来の暗号機能(RSA、ECC、3DES、AES)
- ハイブリッド耐量子署名(RSA(最大4K))とNIST FIPS 204 (ML-DSA) – 重なり構造または連結構造
- 非対称オンボード鍵生成(RSA、ECC、NIST FIPS 204)
- 将来の鍵交換用途のためのCrystals-Kyber JavaCard APIサービス

欧州のセキュリティ機関(ANSSIおよびBSI)が発表した最新のサイバーセキュリティ勧告に沿って、タレスの新製品が提供するハイブリッドアプローチは、従来のRSAアルゴリズムですでに保証された実証済みの特性を活用しつつ、それを最新の耐量子技術によって強化するものです。

また、タレスのエンジニアリングチームは、機械可読旅行文書(eMRTD)の進化に関連する複数の取り組み(欧州研究プロジェクト、技術RFI)にも参画しており、近い将来にeMRTDを耐量子化することを目指しています。

以下の図は、検討されたコンセプトの一例を示しています。



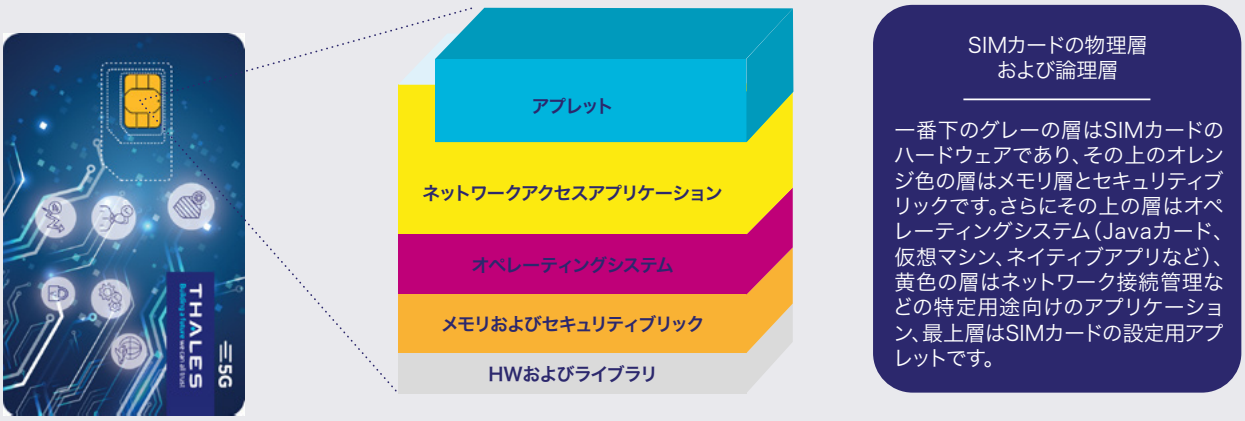
耐量子仕様のeMRTDテスト

タレスは、eMRTD文書の耐量子仕様を策定するために、eMRTD標準化(ICAO DOC 9303新技術ワーキンググループ)に貢献しています。詳細情報は、こちらのEurosmart文書で公開されています: Eurosmart | The voice of the Digital Security Industry | Quantum computers will compromise the security of identity documents

モバイル接続ソリューション

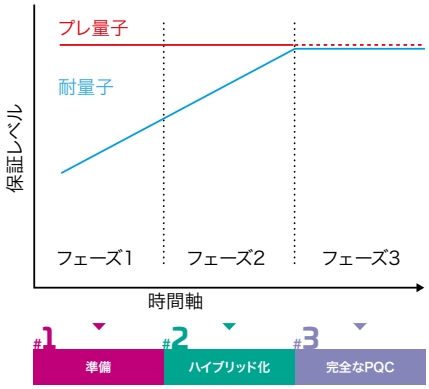
タレスは、つながる世界のためのセキュアなソリューションを提供しており、主にハードウェア（HW）、組み込みソフトウェア（SW）、セルラー接続を促進・管理・保護するためのソリューションに注力しています。MCSは、SIMカード、eSIM、eSE（組み込みセキュアエレメント）などの製品に特化しており、これらは自動車やIoTを含むさまざまなコンシューマー機器や産業機器に不可欠なものです。

SIMとeSIMは論理的な階層構造で構成されており、HW（チップ）と、オペレーティングシステムやアプレットを含むSWスタックがあり、加入者の認証情報、契約内容、設定、そして特にセキュリティ面を管理するために不可欠です。また、タレスは、SIMカードの更新や接続管理を行うための、主にクラウドベースのプラットフォームサービスも提供しています。



SIMカードの技術スタック

完全なPQCに向けて

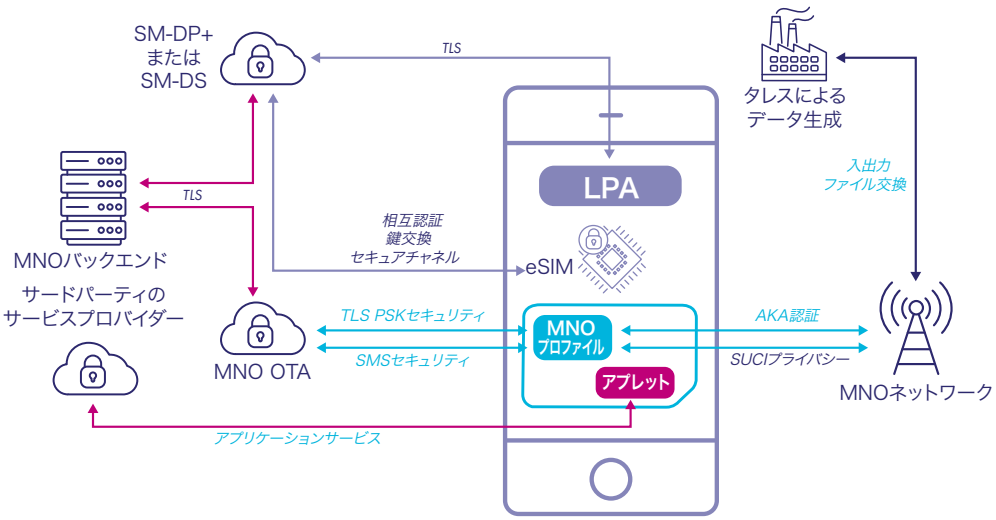


しかし、量子保護が必要なのは、タレスが提供する製品だけではありません。モバイル接続のエコシステムでは、コアネットワーク、エンドユーザー、サービスプロバイダー、SIM/eSIMメーカー、SIM/eSIM管理プラットフォームの間で、データ交換が多岐にわたって行われています。このエコシステム全体を保護する必要があります。これらのデータ交換を保護するために、暗号アルゴリズムとプロトコルをアップグレードしなければなりません。

モバイル接続ソリューションを耐量子化するために、以下の対策を採用しています。

1. OSをOTA（Over-the-Air）でアップグレード可能にし、製品がすでに現場で使用中であっても新しいアルゴリズムに対応できるようにします。これがクリプトアジリティです。
2. セキュリティ機関の最新の勧告に準拠するため、ハイブリッド暗号方式を含む既存の暗号セキュリティメカニズムにPQCアルゴリズムを統合します。
3. 長期的には、暗号処理に必要な演算能力を向上させることで、要求の高い新しいPQCアルゴリズムを搭載できるよう、新しいハードウェアおよびソフトウェア層を設計します。

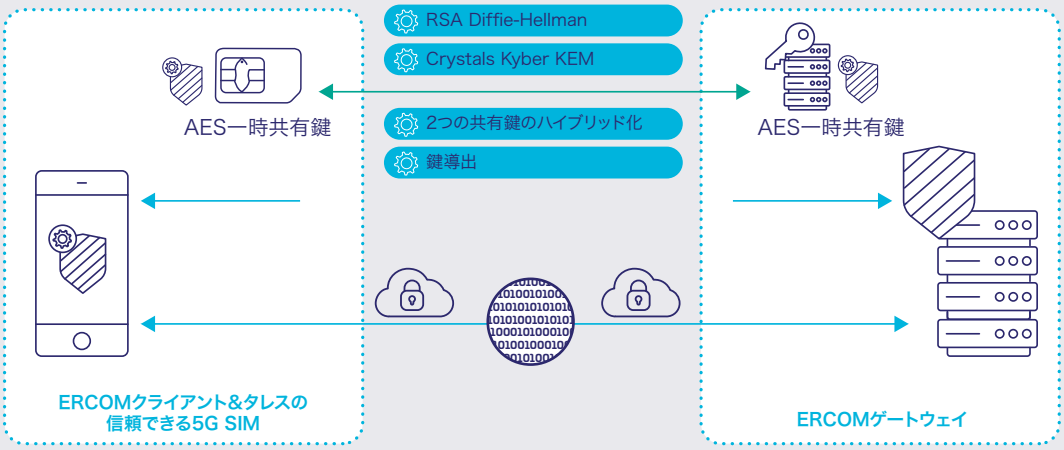
UICC /eUICC暗号技術の概要



モバイル接続のためのPQCソリューション

量子脅威への積極的な対応の一例として、すでに開発されているモバイル間PQC暗号化通信ソリューションがあります。

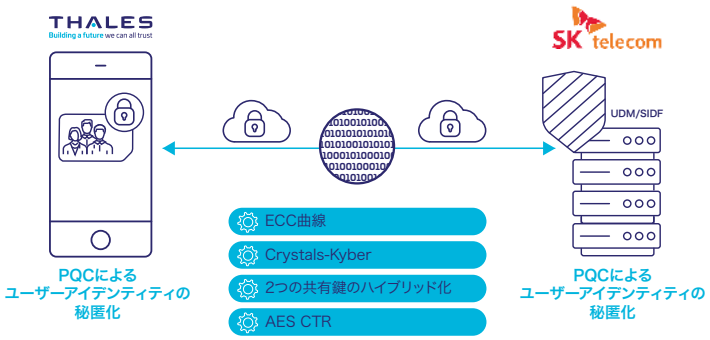
「Cryptosmart」は、タレス傘下のERCOM社が開発した通話を保護するモバイルアプリケーションです。ハイブリッド暗号化アプローチを通じて、耐量子の潜在的なHNDL（Harvest Now, Decrypt Later）攻撃に対する保護を提供するように強化されました。この進化では、NIST（米国国立標準技術研究所）により承認され、SIMオペレーティングシステムにネイティブに実装された鍵交換管理およびアルゴリズムであるCRYSTALS-Kyberを利用しています。このCRYSTALS-Kyberアルゴリズムは、タレスが独自に開発し実装したもので、第三者の関与はありません。特筆すべきは、このソリューションが機密性に重点を置いていることで、ネットワークセキュリティとは無関係に、端末のすべてのインターフェイスを保護し、エンドツーエンドのモバイル通信セキュリティとしてNATOの認定を受けています。



プレ量子およびポスト量子防御メカニズムを組み合わせたハイブリッド暗号アプローチにより、通話中に交換されるすべてのデータがポスト量子攻撃に対して耐性を持ちます。

より広範な協業による、別の事例をご紹介します。

韓国最大のモバイル通信事業者であるSK Telecomとの協業において、タレスは5Gネットワーク上でSK Telecomのユーザーのアイデンティティを保護するために、ソリューションを検討しました。その結果、PQCアルゴリズムを搭載したタレスの5G SIMを商用スマートフォンに組み込み、SK Telecomの商用5Gスタンドアロンネットワーク上で使用することで、将来の量子脅威からユーザーのプライバシーを保護し、潜在的なHNDL（Harvest Now, Decrypt Later）攻撃を遮断することができました。この試験は、現実的な認証と使用条件のもとで実施され、ポスト量子暗号アルゴリズムとハイブリッド証明書を組み合わせて加入者のアイデンティティを保護する点で、重要な進展とみなされています。これにより、位置情報の追跡リスクからユーザーを保護することで、将来的にもGDPRへの準拠を確保できます。



**タレスの5G PQC SIMにより
SK Telecomの通常の5Gスタンドアロンネットワーク上で
PQC SUCIを実現**

この試験の成功には、いくつかの重要な要素が必要でした。まず、従来の非対称鍵とPQCアルゴリズムのハイブリッド鍵交換に基づき、耐量子性のあるユーザーアイデンティティの秘匿化が可能なアップグレードされた信頼できる5G SIMです。さらに、PQC SUCI（ユーザーデジタルアイデンティティ）を処理するためのSK Telecomのコアネットワークのアップグレードも必要でした。これにより、SIM内でのユーザーアイデンティティのシールド、PQC暗号化鍵の交換、コアネットワーク側でのユーザーアイデンティティの秘匿解除が可能になりました。

タレスは、コンシューマー機器、自動車、IoTのアプリケーションをホストする「強固な保管領域」であるセキュアエレメント（eSE）においても、耐量子ソリューションの開発を加速させています。新世代のセキュアエレメントでは、PQCアルゴリズムを統合し、オペレーティングシステムがクリプトアジリティに対応可能となり、既存製品でもPQCアルゴリズムの更新が可能になります。

このビジョンは、SIMおよびeSIM管理プラットフォームへの将来的な影響を特定し、OTA（Over the Air）接続サーバー、サブスクリプション管理サーバー、Thales IoTコネクティビティスイート全体など、複数のサブスクリプション管理ソリューションに必要なアップグレードを判断し、進化するセキュリティ要件との整合性を維持することまで見据えています。

サイバーセキュリティ製品

タレスは、クラウド、データ、ソフトウェアによって支えられる世界において、サイバーセキュリティソリューションを提供しています。ハードウェア、ソフトウェア、ハイブリッド/クラウドベースのソリューションに至るまで多岐にわたる製品とサービスを通じて、組織が機密データを検出、保護、管理する方法を簡素化することを使命としています。タレスの製品とサービスは、リスクの低減、データの保護、簡素化、業務効率の向上により、企業が本来のビジネスに専念できるよう支援します。

タレスは現在、HSM(Luna 7およびTCT Luna Tシリーズのハードウェアセキュリティモジュール)とHSE(高速ネットワーク暗号化システム)へのPQC機能の実装に取り組んでいます。すでに、耐量子性のあるハッシュベースの署名(LMSSとXMSSを含む)、DilithiumおよびKyberをFunctionality Module内に実装しており、QRNGとQKDもさまざまなパートナー統合により導入済みです。HSE製品ラインでは、FIPS準拠の従来型とPQCのハイブリッドアプローチを使用して、標準化前のPQCアルゴリズムを組み込んでいます。また、現在提供中のハードウェアアプライアンスの全製品において、PQC候補を含むクリプトアジャイルアルゴリズムのサポートを提供しています。

NISTの標準化の取り組みとNCCoEとの連携と並行して、タレスは現在、自社のPQC製品をNISTが選定したアルゴリズムに合わせて調整し、今後のファームウェアリリースに向けてPQC性能の最適化を進めています。タレスが標準化前の実装に早期から取り組んできたことは、クリプトアジャイルアーキテクチャの価値を実証しています。この取り組みは、米国国家安全保障覚書10号(脆弱な暗号システムに対するリスクを軽減しつつ、量子コンピューティングにおける米国のリーダーシップを促進する)に合致しています。タレスは、お客様が耐量子暗号((PQC)の将来に備え、今からPQC対応状況をベータテストできるように、HSEネットワーク暗号化とHSMのスターターキットを提供しています。

タレスは、現行のアルゴリズムから代替の耐量子アルゴリズムへの移行を円滑に進めるためのプラクティスを開発する目的で、すでに以下の製品をNISTのNCCoEラボに提出済みです。

- Thales Luna 7 HSM(ハードウェアセキュリティモジュール)
- Thales TCT Luna TシリーズHSM(米国政府向け)
- Thales CipherTrust Manager s (鍵管理用)
- Thales HSE(高速ネットワーク暗号化システム)

タレスとともに、今から量子時代に備える

実践
クリプトアジリティ&暗号要素の検出

Thales HSE(高速ネットワーク暗号化システム)

適用
量子鍵生成

Thales Luna HSM(ハードウェアセキュリティモジュール)

実装
耐量子アルゴリズム

CipherTrust Data Security Platform

利用
量子鍵配送

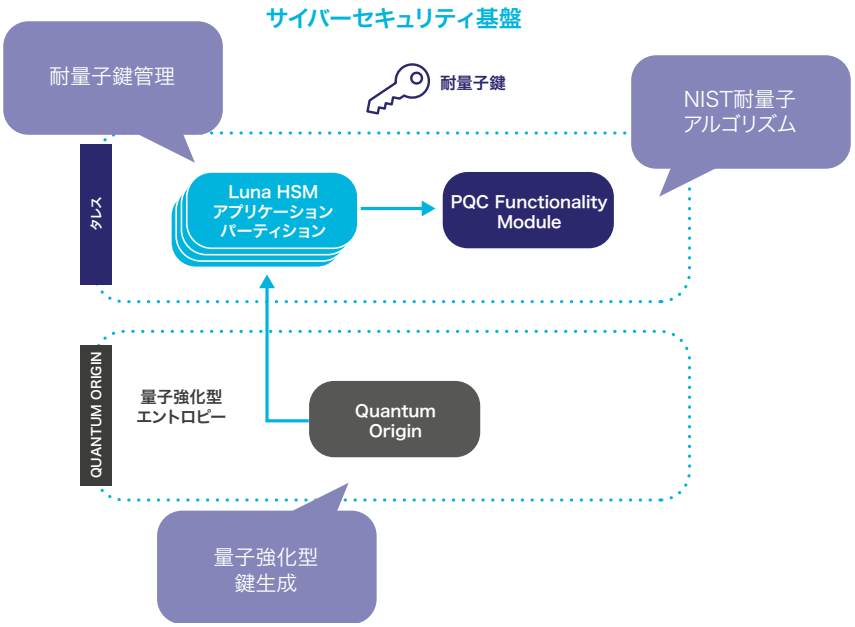
ケーススタディ

ある大手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、アプリケーションを、HNDL（Harvest Now, Decrypt Later）攻撃や既存の暗号方式を破る能力といった量子リスクによる将来の脅威から安全に保護するために、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、証明可能安全性を持つ鍵生成とNISTが提唱するポスト量子暗号アルゴリズムを使用して、銀行業務や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し、その鍵を最も安全に保護することを目指していました。

また、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していることを踏まえ、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。金融業界のリーダーとしての評判を守るためにも、顧客データやデジタル取引のセキュリティを確保し、新しいソリューションへの移行によってオンラインサービスの継続性を損なわないことが重要でした。

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。これを実現するために、同社は、タレスと、その広範なPQCパートナーエコシステムと連携して、安全な鍵生成、管理、保護のための包括的な耐量子商用ソリューションを開発しました。このソリューションには、Thales Luna HSMの堅牢な鍵保管ソリューション内で証明可能な安全性を持つ鍵生成を提供するパートナー統合が含まれています。さらに、NISTが現在提案しているアルゴリズムを搭載したPQC Functionality Moduleと組み合わせることで、同社は新しいアルゴリズムが自社のデータやアプリケーションに与える影響をテストするためのラボ環境を構築しました。

PQC HSMスターターキット: 耐量子アーキテクチャ



Thales Luna PQC HSMスターターキットのアーキテクチャ

タレスは、耐量子暗号（ポスト）量子時代の信頼できるパートナーです

セキュリティは、タレスのすべての製品とサービスの中核にあります。そのため、政府や軍、また極めて機密性の高いデータを扱う組織は、数十年にわたりタレスに信頼を寄せています。デジタル取引への依存度が高まり、データが莫大な価値を持つ現代において、タレスは重要な役割を担っています。量子サイバー攻撃は、大規模なネットワークを数分で機能停止に追い込むおそれがあります。この進化を見越して、攻撃者はすでに、今はまだアクセスできないがやがてアクセスできるようになる、長期間保持されるデータを窃取するHNDL（Harvest Now, Decrypt Later）戦略を始めています。

SIMやeSIMは、接続性における信頼の基点です。同様に、CipherTrust Managerを備えたLuna HSMは、データにおける信頼の基点を担っています。Thales HSE（高速ネットワーク暗号化システム）は、ネットワークを介した安全なデータ伝送を可能にするソリューションとして広く採用されています。さらにタレスは、電子文書用のオープンかつアジャイルな初のポスト量子対応オペレーティングシステムを構築しました。こうした基盤の上に、タレスは現在、お客様がPQCに万全の備えを整えられるよう、すべての製品とサービスを耐量子かつクリプトアジャイルにすることに注力しています。クリプトアジリティは不可欠であり、十分なセキュリティ対策を講じている組織は、変化が生じた際にプロトコルや鍵などを迅速に切り替えることが可能です。これにより、耐量子暗号時代の到来後も、組織は進化する脅威に迅速に対応でき、より高いレジリエンス（回復力）を実現できます。

Thales Cybersecurity & Digital Identityは、耐量子暗号分野において確固たる姿勢を示しており、最新の暗号アルゴリズムのサポートに注力しています。その取り組みには、Falcon暗号署名アルゴリズムの共同開発、新たな通信と鍵管理プロトコルの採用、証明書の耐量子性の強化といった施策が含まれます。また、ハードウェアやソフトウェアだけでなく、タレスグループ内外をつなぐ広範なエコシステムにも十分な配慮がなされています。
こうした積極的な取り組みにより、MultiApp v5.2、5G PQC SIMカード、PQC対応Luna HSM、HSEネットワーク暗号化ソリューションといった現行のタレス製品の差別化と活用の大きな機会が創出されています。

従来の暗号技術と同様に、タレスは自社のサイバーセキュリティ専門知識（サイドチャネル攻撃防御などの物理的セキュリティを含む）を活用して、PQC実装のセキュリティレベルを強化し、組み込みデバイスの制約に適合するよう最適化を図っています。

タレスは、設計段階からクリプトアジャイルなソリューションを開発しており、現在および将来にわたってHNDL（Harvest Now, Decrypt Later）攻撃から防御できるよう支援します。さらに、PKIプロバイダーやPQCパートナーを含む広範かつ拡大中のパートナーエコシステムを活用し、最適な量子移行を即時に開始できる環境を整えています。

タレスは、PQC技術の継続的な探求と活用を通じて、量子技術の進展に柔軟に対応できるクリプトアジリティを提供しています。データとアイデンティティのセキュリティに重点を置きながら、拡大し続けるデジタル環境で信頼を確保し、将来の量子脅威に備えるという使命をさらに強固なものにしています。

THALES

Building a future we can all trust

お問い合わせ先

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。

> cpl.thalesgroup.com/ja <