Entrustソリューションで ポスト量子時代に備える

ポスト量子（PQ）暗号の問題

現在、量子コンピュータはすでに存在しており、その技術は急速に発展し続けています。正確な時期はまだわかりませんが、今後10年以内に量子コンピュータが暗号化ベースの暗号防御を破り、暗号化の全盛期が幕を閉じると予想されています。

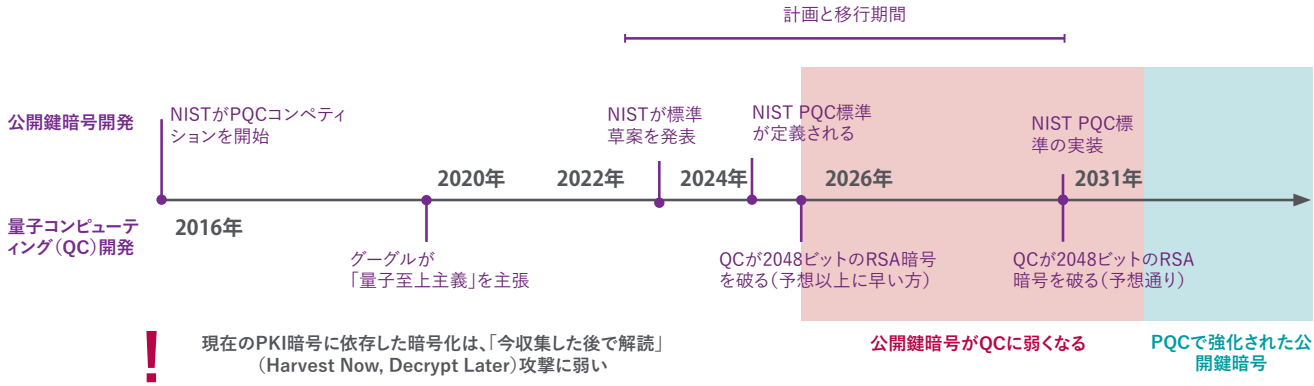
今こそ準備すべき時です

量子コンピュータは、従来のコンピュータに比べ、特定の種類の問題をはるかに短い時間で解決することができます。素因数分解は、RSA暗号の安全性の基盤となる難易度の高い問題のことですが、これは量子コンピュータで解くことが可能にります。楕円曲線暗号（ECC）についても同様です。

データや通信のセキュリティの多くがこれらの公開鍵アルゴリズムに依存しているため、企業は量子コンピュータ時代に備えた戦略の検討を開始する必要があります。

量子コンピュータに耐性のあるアルゴリズムへの移行は、ただの暗号化の更新ではありません。複雑で、数年にわたる作業が見込まれるため、企業は今から検討を開始することが重要です。

量子の脅威のタイムライン



詳しくは、entrust.com/ja/solutions/post-quantum-cryptography

Entrustのポスト量子暗号ソリューション

量子コンピュータ対応暗号アルゴリズムへの移行は、そのアルゴリズムの開発状況に大きく依存しています。前者はすでに進行中ですが、後者の計画はまだ初期段階にあります。現在すでに存在し、今後も機密性を維持すべきデータを守るために、今から準備を進めておく必要があります。

・アメリカ合衆国国土安全保障長官のアレハンドロ・マヨルカス氏

企業が今行うべきこと

1.データの棚卸し：

貴重なデータや長期保存データがどこに保存されているか、また関連するデータフローを理解することが重要です。データのカタログとインベントリを作成すれば、最も注意すべき点がどこか、つまりどこから作業を開始すべきかがわかります。

2.暗号資産の棚卸し：

企業の環境内にどのような暗号資産やアルゴリズムがあり、それらがどこに保存されているかを確認します。また、これらの資産のコンプライアンス、管理、自動化を確保することも重要です。

3.暗号化アジリティ戦略とロードマップの構築：

暗号化のアジリティは、PQCへの移行に不可欠です。また、これらのアルゴリズムは成熟したものではないため、移行後のアジリティも重要となります。その他に、プロセス、従業員、テクノロジーなど、暗号化に関連するリスク領域を特定することも重要です。

4.移行のテストと計画：

NIST PQCの標準が継続的に進化する中、企業がアプリケーション内でテストを開始することができます。ベンダーと協力し、PQをサポートする計画とロードマップが用意されていることを確認しておきましょう。

詳しくは、entrust.com/ja/solutions/post-quantum-cryptography

Entrustのポスト量子暗号ソリューション

ポスト量子時代に備えたEntrustのソリューション

Entrustは、データ保護の未来であるポスト量子暗号（PQC）標準の作成において主導的な役割を担っています。製品ポートフォリオへの投資とイノベーションを通じて、現在と将来のためのソリューションを開発し、安全なコネクテッドワールドを実現します。

PQC 対応評価

このツールは、Entrust Cryptographic Center of Excellenceコンサルティング・ポートフォリオの一部として、以下の機能を提供します：

- 暗号化のアジリティの成熟度の評価と、PQCアルゴリズムの導入に対する準備状況の特定
- 暗号化システムで特定されたリスクを軽減するための実行可能な提案の提供と、PQの対応に備えるためのサポート
- 暗号のアジリティを達成し、PQCに移行するためのロードマップの提供

PQ向けのEntrust PKIサービス

このクラウドベースのサービスは、以下の機能を提供します：

- コンポジットおよび単一の量子認証局の階層を提供する
- 従来のアルゴリズムと量子安全アルゴリズムを組み合わせたハイブリッドまたはコンポジット証明書の発行が可能
- マルチ証明書またはコンポジット証明書とそのアプリケーションをテストする機能を提供
- NIST PQドラフトアルゴリズムをサポート

Entrust nShield PQ SDK

- この製品（Entrust CodeSafeと併用）は、標準化が確認された NIST の PQ 暗号化アルゴリズムに基づく暗号化機能のソフトウェア開発スイートを提供します。このスイートは、Entrust nShield ハードウェアセキュリティモジュール（HSM）の FIPS 140-2 レベル3の物理的境界内で動作可能です
- 鍵生成、鍵署名、デジタル署名、暗号化、復号、鍵交換など、さまざまな PQ 暗号化操作をサポートします
- 開発者に以下の機能を提供します：
  - PQ アルゴリズムのテスト
  - Javaコールによる暗号化操作の実行
  - セキュリティ保護されたテスト環境内でのコードの実行

詳しくは、entrust.com/ja/solutions/post-quantum-cryptography

お問い合わせはこちら

03-4221-9718

japan.info@entrust.com

ENTRUST CORPORATIONについて

Entrustは、信頼できる認証、支払い、データ保護を実現することで、動き続ける世界をセキュアにしています。今日、支払いや国際取引、電子政府サービスへのアクセス、そして企業ネットワークへの認証において世界中でより安全で円滑なユーザー体験が求められています。Entrustは、これらの要となる部分において、他に類を見ない幅広いデジタルセキュリティとID発行ソリューションを提供しています。2500人を超える従業員、グローバルパートナーネットワーク、そして150カ国以上におよぶ顧客に支えられ、世界で最も信頼されている組織から信頼されています。

詳細は下記URLをご覧ください。
entrust.com/ja/solutions/post-quantum-cryptography

ENTRUST

エントラストジャパン株式会社
DPS事業本部
東京都港区台場二丁目3番1号
トレードピアお台場
03-4221-9718