DELL Technologies

ポスト量子暗号

開始する

はじめに

量子コンピューティングは、テクノロジーの根本的な再設計を推進しており、驚くべき可能性と新たな課題の両方を生み出しています。この未来は刺激的ですが、私たちのデジタル世界を保護する暗号形式システムに深刻な脅威をもたらします。

量子コンピューティングが注目されている理由

ノートパソコン、スマートフォン、サーバーなどに搭載されている従来のコンピューターは、0か1の状態にあるビットを使って情報を処理します。このバイナリー モデルは数十年にわたる進歩を支えてきましたが、情報の表現と操作の方法が制限されています。量子コンピューターは量子ビットを使用しており、重ね合わせや量子もつれなどの原理によって複数の状態で同時に存在することができます。これにより、量子マシンは膨大な数の可能な解を同時に探索できるため、特定の種類の問題に対して計算上の優位性を発揮します。

ポスト量子暗号とは？

Post-Quantum Cryptography (PQC)は、従来の攻撃と量子攻撃の両方からデジタル システムを保護するために設計された新世代のアルゴリズムを指します。特殊なハードウェアを必要とする量子鍵配布とは異なり、PQCは、今日の従来のインフラストラクチャ（サーバー、エンドポイント、ネットワーク）上で実行されるように設計されており、量子時代に備えるための最も実用的で拡張性のある方法となっています。

組織は量子コンピューティングからどのような差し迫ったリスクに直面しているのか？

リスクの重大性は、理論上のリスクをはるかに超えています。準備が整っていない組織は、機密性の高い知的財産の漏洩、金融システムの混乱、医療データの侵害、国家安全保障に対する脅威に直面しています。

「今すぐ収集、後で復号化」という脅威によって、緊急性はさらに高まります。攻撃者は、暗号化されたデータを今日取得したら、それを復号化する手段を待つだけです。暗号化に関連する量子コンピューターが到着する頃には、すでに損害は取り返しのつかないものとなっているでしょう。

「今すぐ収集、後で復号化」は、「今すぐ記録、後で復号化」としても認知され、攻撃者が暗号化された現在のデータを収集して保存し、将来的に暗号化に関連する量子コンピューターが利用できるようになった時点で復号することを意図した行為を指します。

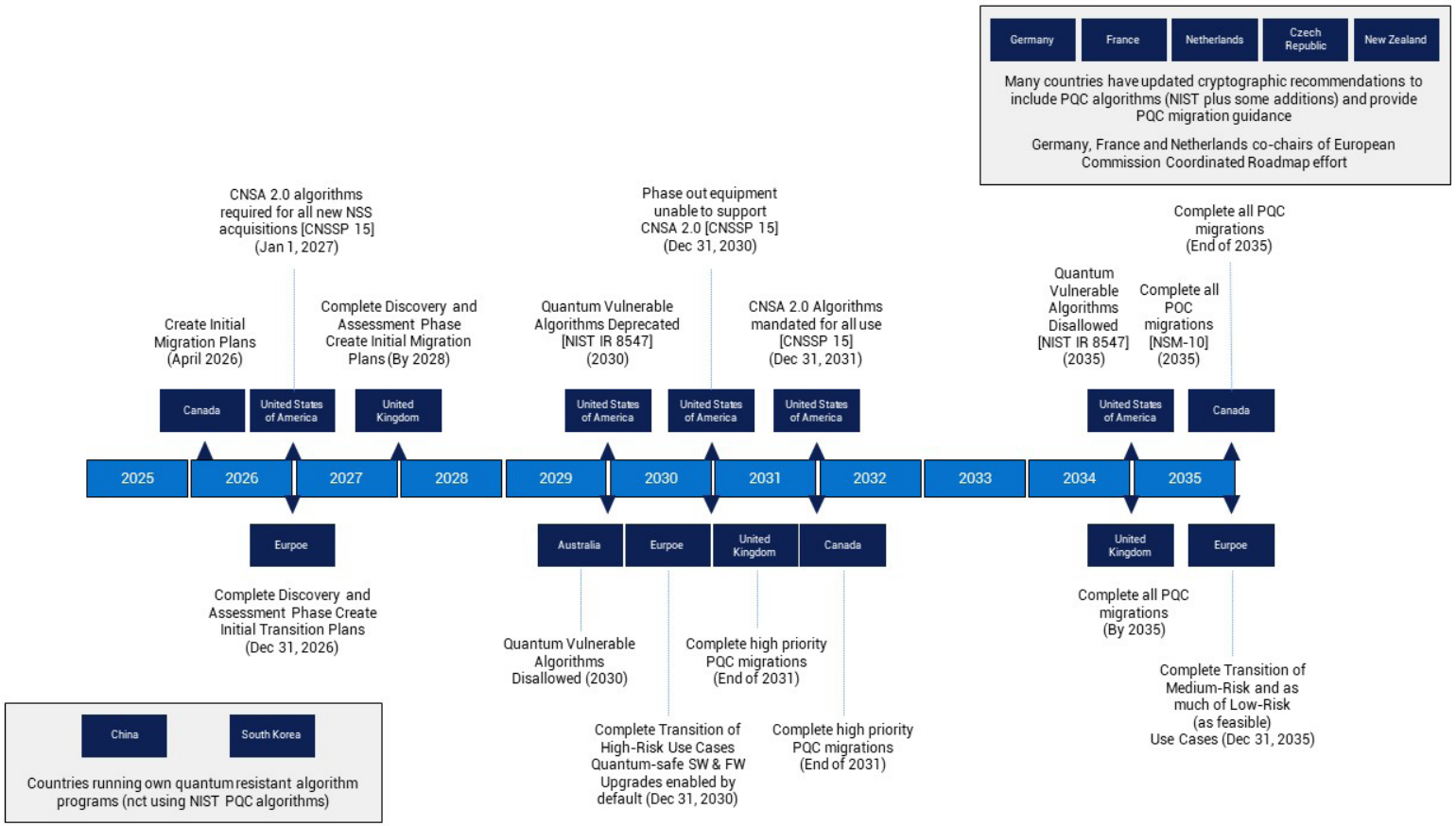
組織はPQCへの移行に向けてどのように準備すべきか？

量子安全な未来への取り組みは、短距離走ではなくマラソンのようなもので、進化し続ける道のりです。プロアクティブかつ多層的で段階的なアプローチを取ることで、組織はリスクを管理し、リソースを調整して、長期的に耐障害性に優れたセキュリティ体制を構築できます。Dellは、このプロセスのあらゆる段階でお客様をサポートするテクノロジーとガイダンスを提供します。ここでは、組織がPQC移行計画を策定する際に参考にすべき主要ステップを紹介します。

PQC移行タイムライン

脅威の緊急性を認識し、政府と基準機関はPQCをグローバルな優先事項としました。米国連邦政府は、量子耐性暗号アルゴリズムの採用の重要性を認識し、連邦政府機関にPQC要件を発行し始めています。これには、国家安全保障覚書10 (NSM-10)、商用国家安全保障アルゴリズム スイート(CNSA 2.0)、行政管理予算局覚書23-02 (OMB M-2302)、米国国立標準技術研究所の内部機関報告書8547 (NIST IR 8547)などが含まれます。

世界中の他の組織も、PQC移行のガイドラインを設定しています。これらの日付は任意ではなく、複雑なITエコシステム全体で暗号化を再設計、検証、導入するために必要なリードタイムを反映したものです。企業は、これらを政府による義務付け以上のものと見なすべきで、これらは、量子レジリエンスへの世界的な移行の実用的な指標です。以下に、さまざまな国の要件の一部を示します。



暗号学的脅威のインベントリーと監査

最優先事項は、現在の暗号ランドスケープを理解することです。この基盤となるステップが、移行戦略全体を方向づける指針となります。

適切なセキュリティ ハイジーン

量子の未来に向けた準備の第一歩は、すでに整備されている防御を強化することです。組織は、最小限の権限アクセスの強制、多要素認証の実装、厳格なパッチ管理の維持など、強力なセキュリティ ハイジーンのベストプラクティスを活用する必要があります。他にも2つの考慮事項があります。弱い暗号化の無効化は、新しいシステムがより高い暗号化でレガシー システムと相互運用できるようにするうえで、重要になるかもしれません。また、新しいシステムでは、最低限のセキュリティ強度を引き上げて（対称暗号方式にはAES-256、ダイジェストにはSHA-384以上）、Groverのアルゴリズムによるセキュリティ マージンの削減に対抗することも重要です。これらの対策は、現在のリスクを軽減するだけでなく、将来の移行を複雑化させる暗号負債の蓄積を最小限に抑えます。

暗号資産のインベントリーと監査

移行計画の基盤は可視性です。組織は、包括的な暗号化インベントリーを実施し、アプリケーション、デバイス、ワークフロー全体で公開キー暗号化が使用される場所と方法を特定する必要があります。これには、TLS証明書、VPN、Eメール システム、コード署名メカニズム、顧客データ、アーカイブ データなどが含まれます。特定された資産は、ビジネスの重要性、機密性、寿命に基づいて優先順位を設定する必要があります。医療記録や機密文書などの長期保存データは、「今すぐ収集、後で復号化」という脅威に対して非常に脆弱であるため、最も緊急に対処する必要があります。

PQCを使用したパイロットと試験

明確なインベントリーにより、PQC対応テクノロジーを使用した実践的な試験を開始し、パフォーマンスや統合性を検証できます。

暗号ランドスケープを理解したら、組織は制御された環境でPQCソリューションのテストを開始する必要があります。これらのソリューションをラボで試験的に導入することで、ITチームは大規模な導入前にパフォーマンス、相互運用性、管理機能を検証できます。この暗号俊敏性（システム全体をオーバーホールすることなく暗号アルゴリズムを切り替える機能）を構築することは、長期的なレジリエンスと移行の容易さを確保するうえで不可欠です。

相互運用性アプローチの採用

PQC標準が成熟するにつれて、本番環境への導入計画を立て始めることができます。ハイブリッド アプローチは、完全な量子安全環境へ移行するための橋渡しとなります。

標準が成熟するにつれて、ハイブリッド モデルは将来に繋ぐ役割として機能します。多くのベンダーは、従来のアルゴリズムと量子耐性アルゴリズムを1つの実装に統合するハイブリッド暗号スイートをすでにサポートしています。このデュアル アプローチにより、1つのアルゴリズムが後に侵害された場合でも、保護の継続性が確保されます。企業は、インフラストラクチャ ベンダーの製品ロードマップとマイルストーンに合わせて社内タイムラインを調整しながら、ハイブリッド戦略の採用を今すぐ開始する必要があります。これにより、量子安全アルゴリズムが標準化の達成に向け進化する中でも、組織は中断することなく導入を拡張できます。

完全な移行と継続的な検証の実行

最終的な目標は、完全に統合されて継続的に検証された量子安全エンタープライズです。

完全な移行と継続的な検証の実行

最終的な目標は、企業全体でPQCに完全に移行することです。これは1回限りのイベントではなく、検証と適応の継続的なプロセスです。組織は、新しい標準と実装を継続的にテストしながら、PQCをITスタックのすべてのレイヤーに組み込み、詳細な移行計画を実行する必要があります。従来型と量子のコンピューターから成るハイブリッド構成を使用することで、お客様は攻撃シナリオをシミュレートし、暗号形式の整合性を検証して、進化する脅威に対するシステムのレジリエンスを確保できます。

コラボレーションと知識の共有

組織はこの課題に単独で立ち向かうべきではありません。

業界コンソーシアム、学術研究者、政府機関は、PQCへの移行を加速させるための知識を蓄積しています。標準化グループ、ワーキング グループ、パイロット プログラムに参加することで、企業はベスト プラクティスと新たな要件に常に対応できます。Dellは、NIST NCCoE PQCプロジェクトなどのイニシアティブに積極的に関与しているため、お客様はこの総合的な専門知識から直接メリットを得ることができます。

結論

量子の時代は、もはや遠い可能性ではなく、目前に迫った現実であり、今こそ先を見据えた行動が求められています。この技術的な変化に備えることは、最も重要な資産であるデータを守るための戦略的な必須事項です。前述のように、インベントリーと監査から完全な移行に移行する段階的なアプローチは、量子安全な未来へ向かう最も明確な道筋です。

PQCへの移行は、近年で最も重要なインフラストラクチャの変化の1つになるでしょう。この移行は、サーバーやストレージからエンドポイント、クラウド プラットフォーム、ネットワーク プロトコルまで、ITのほぼすべての側面に関連しています。成功には、先見性、計画、統制のとれた実行が必要です。デル・テクノロジーズでは、今後の道筋を段階的な取り組みと見なしており、セキュリティの即時強化とPQC導入に向けた長期的な準備態勢とのバランスを取る必要があります。

Dellでは、PQCの実装に向けた戦略を支援する準備が整っています。当社は、段階的な移行計画を推奨しており、また、PQC移行の戦略化、計画、実行、監視に役立つ一連のアクティビティーの概要を示しています。