DELL Technologies

ホワイトペーパー

ポスト量子暗号：量子時代に備える

デル・テクノロジーズ ホワイト ペーパー

目次

概要

量子コンピューティングは、理論的研究から実用的な現実へと急速に移行しています。かつては遠い未来のことと考えられていたハードウェア、アルゴリズム、投資の進歩により、従来のコンピューターでは解決できない問題を解決できるマシンの登場が加速しています。これによる業界への影響は甚大です。量子コンピューティングは、創薬から気候モデリング、グローバル物流に至るまで、これまで手が届かなかったイノベーションを実現する可能性を秘めています。

しかし、この飛躍的進歩には破壊的な課題が伴います。量子コンピューターは恐らく、デジタル経済を保護する暗号基盤を損なうでしょう。公開キー暗号化 (RSAや楕円曲線暗号(ECC)などのアルゴリズム) は、デジタル通信、金融システム、医療記録、国家安全保障を数十年にわたって保護してきました。これらの方法は、古典的なコンピューターでは扱いにくい数学的問題に依存しています。しかし、暗号化に関連する量子コンピューター(CRQC)の登場により、これらの問題は効率的に解決され、現在のセキュリティは時代遅れになっています。

この脅威は理論上のものではありません。一部の組織では、すでに「今すぐ収集、後で復号化」(HNDL)と呼ばれる戦術を採用しています。これは量子コンピューターが成熟した段階で解読できることを期待して、現在暗号化されたデータを収集する手法です。現在安全であると思われる機密情報は、数年後には脆弱になる可能性があります。行動を起こすべきタイミングは、CRQCが届いた時ではなく、今日です。

このホワイトペーパーでは、量子脅威の緊急性について説明し、ポスト量子暗号(PQC)の新たな分野を詳しく検証し、組織がこれにどのように備えることができるかについて説明します。本書では、NISTのポスト量子暗号(PQC)標準であるFIPS 203、FIPS 204、FIPS 205に準拠し、Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)ガイドラインに沿って、サプライチェーン、ハードウェア、ファームウェア、ソフトウェア、パートナーエコシステム全体にセキュリティを組み込むという、量子安全な未来の構築に対するデル・テクノロジーズの取り組みを明らかにしています。Dellの目標は明確です。セキュリティや信頼を犠牲にすることなく、イノベーションを確実に前進させます。

用語集

このホワイト ペーパーでは、多くの専門用語が使用されています。本書の内容を理解いただきやすくなるよう、これらの用語のいくつかを概説しています。

Post-Quantum Cryptography – 新しいアルゴリズムを使用した暗号化に対する新しい数学的アプローチであり、量子コンピューター攻撃に対する安全性を確保することを目的としています。これらのアルゴリズムは古典的なコンピューター上で実行され、量子攻撃と既知の古典的な暗号化攻撃の両方に耐性があります。

量子耐性 – 量子耐性とは、暗号化に関連する量子コンピューター(CRQC)が存在しても安全性を維持するように設計されたシステム、アルゴリズム、またはインフラストラクチャを指します。量子耐性を備えたシステムでは、従来の攻撃と量子攻撃の両方に耐えるPQC (ポスト量子暗号化) またはその他の保護を使用して、将来にわたってデータの機密性、整合性、信頼性を確保します。量子耐性や量子安全など、他の用語も同じ意味で使用されます。

暗号化の俊敏性 – (暗号俊敏性とも呼ばれる) とは、組織のシステムやアプリケーションが、大幅な再設計や運用の中断を必要とせずに、暗号化アルゴリズム、プロトコル、またはキー長を迅速かつシームレスに切り替える能力です。

「今すぐ収集、後で復号化」(HNDL)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(CRQC)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。

量子コンピューティングと暗号化の脅威

量子コンピューティングの台頭

約1年前にDellのCTOであるJohn Roeseが投稿したブログ記事「Post-Quantum Cryptography: A Strategic Imperative for Enterprise Resilience」で説明したように、ノートパソコン、スマートフォン、サーバーのいずれであっても、従来型コンピューターは0または1の状態で存在するビットを使用して情報を処理しています。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。

量子コンピューティングの潜在的な応用性は並外れています。研究者たちは、従来のコンピューターでは実現できない分子相互作用の正確なシミュレーションによる、医薬品の飛躍的進歩を期待しています。気候科学者は、より正確なグローバル システムのモデルを想定しています。一方、エネルギー セクターでは、送電網とストレージの最適化の可能性を見込んでいます。物流や製造でさえ、量子最適化技術のメリットを享受できます。そのメリットは現実のもので、手の届くところにありますが、リスクもまた同様です。

暗号化がリスクにさらされる理由

暗号化は、デジタル時代における信頼の基盤となります。クレジット カード番号を入力したり、安全なWebサイトにログインしたり、署名されたソフトウェア アップデートを受け取ったりする際は、暗号化によって機密性、信頼性、整合性が確保されます。この保護のほとんどは、RSAやECCなどのアルゴリズムである公開キー暗号に依存しています。これらのアルゴリズムは、古典的なマシンでは計算が不可能と考えられている数学的問題に基づいています。

量子コンピューティングはこの方程式を変えます。**ショアのアルゴリズム**を使用すると、十分に強力な量子コンピューターは、因数分解と離散対数問題を解決することができ、これはRSAとECCの利点となります。CRQCが存在すると、ソフトウェア アップデートを保護するデジタル署名、TLSセッションを確立するキー、デバイスを認証する証明書がすべて侵害される可能性があります。その影響は体系的であり、デジタル トランザクションを安全にするメカニズムそのものを脅かしています。

対称暗号化（保存されたデータの保護や安全な通信に使用されるAESなどのアルゴリズム）は、それほど深刻ではありませんが、異なる課題に直面しています。**Groverのアルゴリズム**を使用すると、量子コンピューターは対称キーの有効強度を低下させ、セキュリティを効果的に半減させることができます。これは、AES-256など、より大きいキー サイズに移行することで軽減できますが、この調整は、量子脅威による影響が拡大していることを浮き彫りにしています。

緊急性と重大性

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」戦略は緊急性の度合を高めます。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。CRQC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。

ポスト量子暗号と新たな基準

ポスト量子暗号の定義

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。

PQCの基盤は、現在知りうる限りでは、ShorのアルゴリズムやGroverのアルゴリズムといった量子技術に対して耐性を持つ一連の数学的問題です。ラティスベースの暗号、ハッシュベースの署名、コードベースの方式、多変数方程式は、最も有望な手法です。これらのアプローチは厳格にテストされ標準化されており、かつてRSAやECCが提供していた信頼性と相互運用性を、同様に確実に提供しています。

グローバル標準化の取り組み – 新しい業界標準

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。米国国立標準技術研究所(NIST)は、2016年にPQCプロジェクトを立ち上げ、暗号学研究コミュニティーに候補となるアルゴリズムの提案、分析、改良を求めています。数年にわたるテストの後、NISTは2024年8月に標準化されたアルゴリズムの最初のグループを発表しました。

- **CRYSTALS**-Kyber（公開キーの暗号化とキーの確立）
- **CRYSTALS** -DilithiumおよびSPHINCS（デジタル署名）

組み込みファームウェアなどの軽量システムを含む、さまざまな実装ニーズに対応する多様性と柔軟性の提供に向けて、追加アルゴリズムも引き続き検討されています。この進化する標準化プロセスにより、世界中の組織が量子耐性ソリューションを採用するための明確な道筋を確保できます。

NIST標準 – FIPS 203、204、205

2024年8月、米国国立標準技術研究所(NIST)は、以下に列挙する、最初のPQCアルゴリズムを完成させました。

- FIPS 203 (ML-KEM) – キー カプセル化メカニズムであるCRYSTALS-Kyberに基づく。IND-CCA2の安全性を確保し、これにより、適応的選択暗号文攻撃が発生した場合でも暗号文は識別されません。
- FIPS 204 (ML-DSA) – デジタル署名アルゴリズムである、CRYSTALS-Dilithiumに基づく。強力なEUF-CMA安全性（選択メッセージ攻撃における存在偽造不能性）を確保し、デジタル署名の標準要件を満たします。
- FIPS 205 (SLH-DSA) : ハッシュベースの署名スキームであるSPHINCS+に基づく。ラティス問題に依存しない保守的なフォールバックとして選択されました。

必須のロードマップ

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)、米国国立標準技術研究所(NIST)の内部機関報告書(IR) 8547、行政管理予算局覚書23-02 (OMB M-2302)などが含まれます。

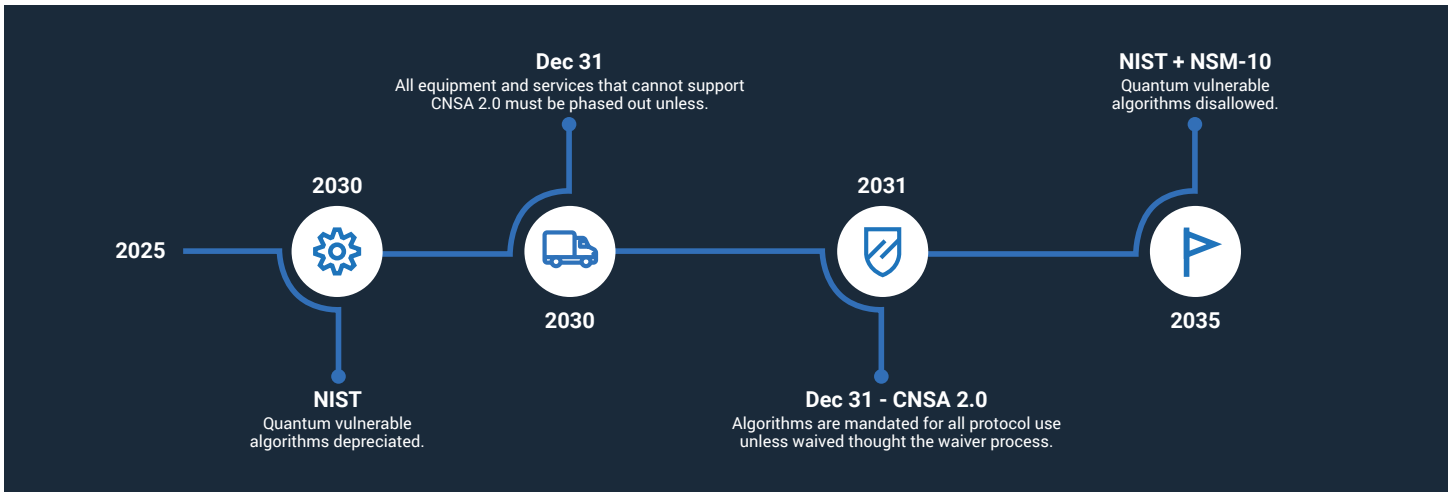
National Security Memorandum 10 (NSM)
Provides a roadmap to create crypto inventories, adopt crypto agility methodologies.

Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)
Introduces the first recommendations post-quantum cryptographic algorithms

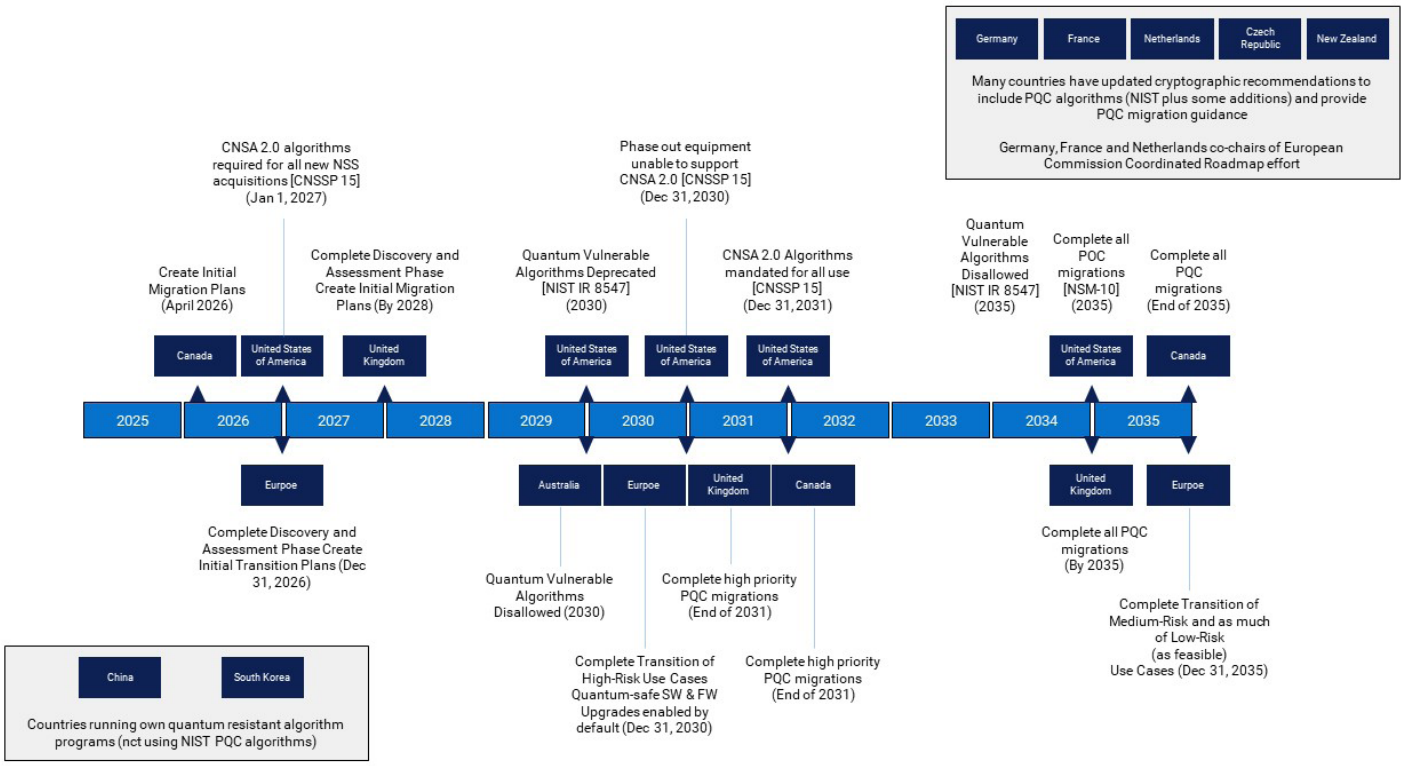
NIST IR 8547
Provides guidance on transition, outlining NIST'S expected approach to PQC digital signatures and key-establishment schemes

OMB Memorandum 23-02 (OMB M-23-02)
Provides detalied guidelines for federal agencies to how to comply with NSM-10

2022年9月にNSAによって発表されたCNSA 2.0では、ポスト量子暗号アルゴリズムに関する最初の推奨事項が導入されています。CNSA 2.0は、国家安全保障システム(NSS)全体で量子耐性アルゴリズムを採用するための明確な期限を設定しており、独自の移行を準備している企業にとって強力な指標となります。



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。 以下に、さまざまな国の要件の一部を示します。



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。

業界における協同体制

Dellは、NISTやNSAだけでなく、相互運用性と採用を推進している業界コンソーシアムや標準グループに積極的に影響を与え、またこれらに参加しています。Trusted Computing Groupは、PQCをTrusted Platform Module (TPM)標準に統合しています。IETFは、TLS、X.509証明書などの業界プロトコルへのPQCアルゴリズムの多くの統合を推進しています。OASIS Key Management Interoperability Protocol (KMIP)委員会は、キー管理フレームワークのPQCを有効にしています。FIDOアライアンスは、PQCの認証とデバイスオンボーディング標準への影響を研究しています。一方、SAFECodeのような組織は、移行準備に向けて業界を教育する活動を行っています。

NIST National Cyber Security Center of Excellence (NCCoE)は、NISTが分野に重点を置いたプロジェクトを通じて、業界、学界、政府機関と連携できるよう組織化されたものです。次のような多くの事項に重点を置いています。

- 暗号化検出 – 移行が必要な暗号資産を特定し、移行の優先順位をどのように設定すべきかを判断します。
- 相互運用性 – 一般的な暗号化機能とプロトコルに新しいPQCアルゴリズムが組み込まれており、さまざまなベンダーの実装が相互運用されていることを確認します。
- 暗号俊敏性 – システムのインフラストラクチャに大きな変更を加えることなく、新しい暗号化プリミティブとアルゴリズムの迅速な適応を促進する情報システムの開発に重点を置いています（暗号化の俊敏性とも呼ばれる）。

これらのプロジェクトは、作成するガイダンスや標準に関する情報提供や開発を支援し、提供した標準やガイダンスに対する業界ソリューションの例を確実に提供するうえで役立ちます。 Dellは、NCCoE Migration to PQCプロジェクトの開始当初からこれに参加しています。

現在、PQCは単なる研究トピックではなく、具体的なアルゴリズム、タイムライン、導入経路を備えた開発基準となっています。今から準備を始める組織は、直前の混乱によるコスト、中断、リスクを回避できます。この移行は、単なるコンプライアンスの問題ではなく、量子コンピューティングがデジタル環境を再構築する中で、信頼性、機密性、整合性が損なわれないことを保証するものです。

なぜ今こそ行動すべき時なのか

脅威の即時性

量子コンピューティングを遠い将来のリスクと見なし、このテクノロジーが完全に実現してから対処すればよいと考える方もいるかもしれません。実際には、時計はすでに動き始めています。機密情報（金融取引、医療記録、知的財産、政府の通信）は、現在は安全に暗号化されているかもしれませんが、量子マシンがRSAやECCを破る領域に達すると、データが遡及的に公開される可能性があります。その結果、過去のコミュニケーションと記録のバックログ全体が突然リスクにさらされる可能性があります。

テクノロジー サイクルの長さ

最新のITエコシステムは、簡単にも迅速にも変革されません。これまで、SHA-1からSHA-2への移行やDES/3DESからAESへの移行など、単一のアルゴリズムの置き換えは完了までに10年以上かかっています。これらのアルゴリズムは、オペレーティング システム、アプリケーション、ネットワーク デバイス、ハードウェアに深く組み込まれています。これらを置き換えるには、データセンターからクラウド プラットフォーム、エッジ デバイスに至るまで、環境全体で再設計、検証、テスト、導入を行う必要があります。多くの組織において、これには何年もかかるでしょう。量子コンピューティングが現実世界に脅威をもたらすようになるまでの残り時間よりも、はるかに長い時間を要します。そのため、規制当局、標準化団体、セキュリティ リーダーは、即時の準備を訴えています。CRQCが広く利用できるようになるまで待てば、秩序ある移行のための時間がなくなります。

不作為のリスク

移行を遅らせることによる影響は、技術的なリスクに留まりません。

- データ セキュリティのリスク：病歴、財務記録、防衛情報などの長期保存データは、量子コンピューターが成熟すると、遡及的に侵害される可能性があります。
- ソフトウェアの信頼性と整合性リスク：ソフトウェアの信頼性と整合性は、現行の署名方式で署名され今でも使用されている場合、量子コンピューターが成熟した時点で、悪意のあるコードによって侵害される可能性があります。
- 運用リスク：公益事業、輸送ネットワーク、緊急サービスなどの重要なインフラストラクチャ システムは、アップグレードの難しさでよく知られています。今すぐ計画しないと、将来的に運用が中断する可能性があります。
- 規制およびコンプライアンスのリスク：**CNSA 2.0**などのフレームワークでは、コンプライアンスのための明確なタイムラインが確立されています。準備を怠った組織は、リスクにさらされるだけでなく、政府や業界の期待に応えられなくなるリスクもあります。
- 評判の悪化および財務上のリスク：暗号形式の脆弱性に未対処であることに起因する侵害は、ブランドの信頼に永続的な損害を与え、重大な財務的損失を招く可能性があります。

積極的な行動の必要性

積極的な準備は、防御体制の構築にとどまらず、長期的なレジリエンスを強化する機会でもあります。暗号化インベントリーの実施、対称キー長のアップグレード、PQC対応ソリューションの試験運用、量子耐性を備えた製品を提供するベンダーとの連携により、組織は信頼の継続性を確保できます。早期導入企業は、将来を見据えた運用、コンプライアンスの維持、お客様、パートナー、規制当局に対するリーダーシップの発揮において、優位に立つことができます。

ポスト量子暗号化に対するDellのアプローチ

Dellは、テクノロジーが人類の進歩を促進すると考えており、セキュリティがその進歩の基盤であると考えています。デル・テクノロジーズは企業として、自社のポートフォリオ、ITインフラストラクチャ、ライフサイクル サポート システムが、量子耐性アルゴリズムへの移行に十分に準備された状態であるよう徹底しています。移行の準備に向けた手順は次のとおりです。

- 製品、サービス、ITインフラストラクチャ、サポート システムで暗号化が採用されている具体的な領域と目的を特定し、包括的な移行計画を策定する。
- PQCアルゴリズムへのスムーズな移行を促進するために、暗号の俊敏性に関連する実装面と設計原則を考慮して、Post Quantum Cryptography (PQC)アルゴリズムに関する社内知識を強化する。
- デル・テクノロジーズの多様なポートフォリオに関連するさまざまなユース ケースにおけるPQCアルゴリズムのパフォーマンス、適用可能性、適合性を評価する。

PQC移行の複雑な性質を考慮すると、暗号化ユース ケースのアップグレードがデル・テクノロジーズ製品に段階的に組み込まれる可能性があります。たとえば、データの観点から見ると、転送中や保存中のデータの暗号化など、「今すぐ収集、後で復号化」攻撃に対して脆弱になる可能性のあるユース ケースは、移行の優先度が高くなります。

テクノロジー プラットフォームを考慮すると、暗号化ユース ケースの移行には、製品の完全な更新/交換または製品のアップグレードが含まれる可能性があります。 これは、対象の製品と、その製品および周辺システムにおける、暗号化の領域や実装の方法によって異なります。

今後5年以上は、量子耐性を備えた製品の提供に注力し、政府や業界団体が公表している2027年から2035年までのPQC移行スケジュールに顧客が対応できるよう支援します。

お客様は、Dellアカウント チームと協力して、製品固有の詳細 (リリース ロードマップやタイムラインなど) を取得し、移行計画に組み込む必要があります。Dellは、今後数か月以内に、PQCを自社製品ラインと製品に統合する具体的なスケジュールを発表する予定ですので、ご期待ください。

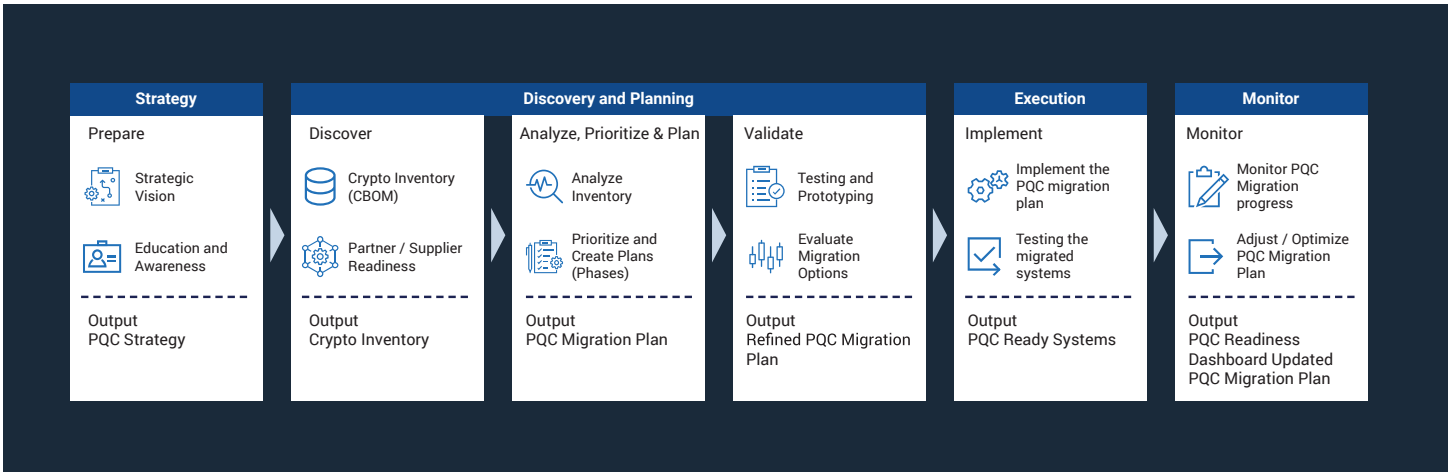
量子耐性のイノベーションに向けた準備

Dellの目標は、お客様が新たな標準に準拠できるよう支援するだけでなく、量子時代において安全にイノベーションを実現できるよう支援することです。AIワークロードの導入、ハイブリッドクラウド環境の管理、エッジ インフラストラクチャのモダナイズなど、お客様はDellのソリューションがレジリエンスを念頭に置いて設計されていることで、安心感を得ることができます。セキュリティは後付けの機能ではなく、Dellのポートフォリオのあらゆる層に組み込まれているため、組織は自信を持って確実に、ポスト量子暗号への移行を進めることができます。

移行への準備

ポスト量子暗号への移行は、数十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。



今日のセキュリティ体制の準備

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、Groverのアルゴリズムによってもたらされるマージンの減少に対抗するために、対称暗号化をより長いキー長（AES-256およびSHA-384以上）にアップグレード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、アーカイブデータが含まれます。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最も脆弱であるため、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

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

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、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。量子・古典のハイブリッドなラボを使用することで、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耐障害性を確保できます。

コラボレーションと知識の共有

最後に、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。

PQCへの準備は短距離走ではなく、マラソンのようなものです。現在の防御の強化、暗号資産の監査、PQCの試験運用、ハイブリッド戦略の採用、完全な移行の実行など、段階的なアプローチを採用することで、組織は確実に量子レジリエンスに移行できます。Dellとのパートナーシップにより、この取り組みは達成可能であるだけでなく、信頼を強化し、将来に向けてイノベーションを実現する機会となるでしょう。

実社会での応用とメリット

ポスト量子暗号への移行は、コンプライアンスの取り組みとして重要なだけではありません。信頼、レジリエンス、長期的な競争力に直接影響を与えるビジネス上の必須事項です。通信プロバイダー、金融機関、医療機関、政府機関の場合、量子耐性アルゴリズムを採用することで、重要なデジタル インフラストラクチャを現在と将来の両方の脅威に対して安全に保つことができます。

通信

通信ネットワークは、グローバルなデジタル化のバックボーンです。緊急時のサービスやIoT接続から、お客様との通信の安全性確保まで、あらゆる場面を支えています。この分野で量子侵害が発生すると、SIMプロビジョニング、eSIMオンボーディング、4Gや5Gの基盤となる認証プロセスが侵害される可能性があります。ハイブリッドで量子安全な暗号化を今すぐ導入することで、オペレーターはお客様の信頼を維持し、データプライバシーを保護して、世代間のモバイル テクノロジー全体でサービスのシームレスな継続性を確保できます。

金融サービス

金融業界はサイバー攻撃の標的となっており、トランザクションの整合性は暗号化に依存しています。ポスト量子対応は、量子技術を利用した不正行為からデジタル決済、オンライン バンキング、銀行間送金を保護します。早期に導入することで、規制当局やお客様に、組織が資産の保護と体系的な安定性の維持に取り組んでいるという安心感を与えることができます。この分野では将来を見据えた暗号化により、規制上のリスクと評判悪化のリスクの両方が軽減されます。

医療

患者の記録、ゲノム データ、接続された医療機器はすべて、「今すぐ収集、後で復号化」攻撃のリスクにさらされています。医療業界では、機密性の高い医療データに求められる長期的な保管という、さらなる課題に直面しています。病院や医療機関がすぐにPQCへの移行を開始することで、医療記録のプライバシーは現在だけでなく、数十年先まで確実に守られます。これは、進化するデータ保護規制に対応しながら、患者の信頼を維持するために不可欠です。

政府および重要なインフラストラクチャ

防衛通信からエネルギー分配システムまで、政府やインフラストラクチャ事業者は、運用の継続性と国家安全保障のために暗号化に依存しています。ポスト量子暗号は、攻撃者から短期的に防御するだけでなく、将来的な悪用を目的とした暗号化通信の戦略的な収集からも保護します。CNSA 2.0などのフレームワークと連携することで、量子時代において政府システムの相互運用性、安全性、信頼性を維持できます。

幅広いビジネス上のメリット

PQCの技術的な必要性は明らかですが、ビジネス上のメリットも同様に強力なものになります。

- 信頼とブランドの評判：お客様とパートナーのデータ保護におけるリーダーシップを示します。
- 法令遵守：NIST標準とCNSA 2.0などの政府の義務に準拠します。
- 運用上のレジリエンス：暗号化の突破による致命的なアウテージのリスクを軽減します。
- 競争上の差別化：組織を事後対応型のフォロワーではなく、プロアクティブなイノベーターとして位置付けます。

今行動を起こすことのメリットは、技術的なレジリエンスだけにとどまりません。PQCを早期に採用している組織は、リスクを軽減するだけでなく、信頼性に依存するデジタル経済において、イノベーション、コンプライアンス、競争力を強化することができます。

次のステップへ

量子コンピューティングの到来は、世代を超えた機会であると同時に、前例のないセキュリティ上の課題をもたらします。暗号学的に有用な量子コンピューターの正確な実現時期は不透明ですが、確実なのは準備には労力が求められるということです。ポスト量子暗号化への移行には、何年にもわたる計画、投資、実行の調整が必要です。量子コンピューターが運用可能になるまで待つことは、現実的な選択肢ではありません。

あらゆる組織にとっての最初のステップは、環境全体で暗号化がどこでどのように使用されているかを理解することです。そこから、企業は量子安全ソリューションのインベントリー、優先順位付け、試験運用のプロセスを開始する必要があります。従来のアルゴリズムとポスト量子アルゴリズムを組み合わせたハイブリッド暗号化は、標準が進化し続ける中で、レジリエンス強化の即効性のある手法となります。NISTのPQC標準やCNSA 2.0タイムラインなどのグローバル フレームワークに合わせて社内ロードマップを調整することで、組織はコンプライアンスと相互運用性に向けて自信を持って進むことができます。

デル・テクノロジーズは、お客様がこの移行に対応できるよう支援することに尽力しています。当社はこのアプローチを通じて、サプライ チェーンの整合性、ハードウェア組み込み型の保護、ソフトウェア対応の適応性の基盤を提供しています。業界をリードするセキュリティ プロバイダーとのパートナーシップと業界標準団体での積極的な役割により、Dellのソリューションは最新の要件に適合するだけでなく、実際のパフォーマンスと相互運用性についてもテスト済みの状態です。

今すぐ準備を始めましょう。検出とリスク分析から始め、信頼できるベンダーと連携し、量子安全テクノロジーを試験的に導入します。今実行するあらゆるステップで、将来の混乱のリスクが軽減されます。早期に行動する組織は、データやシステムを保護できるだけでなく、デジタルの信頼が最優先される時代において、顧客、規制当局、パートナーからの信頼も得られます。

デル・テクノロジーズについて

デル・テクノロジーズは、高度なテクノロジーを誰もが利用しやすく、信頼できるものにし、支援することに取り組んでいます。私たちは、個人や組織が安全にイノベーションを活用できるよう支援し、より安全かつインクルーシブで、つながりのある未来への道を切り開きます。

DELL Technologies