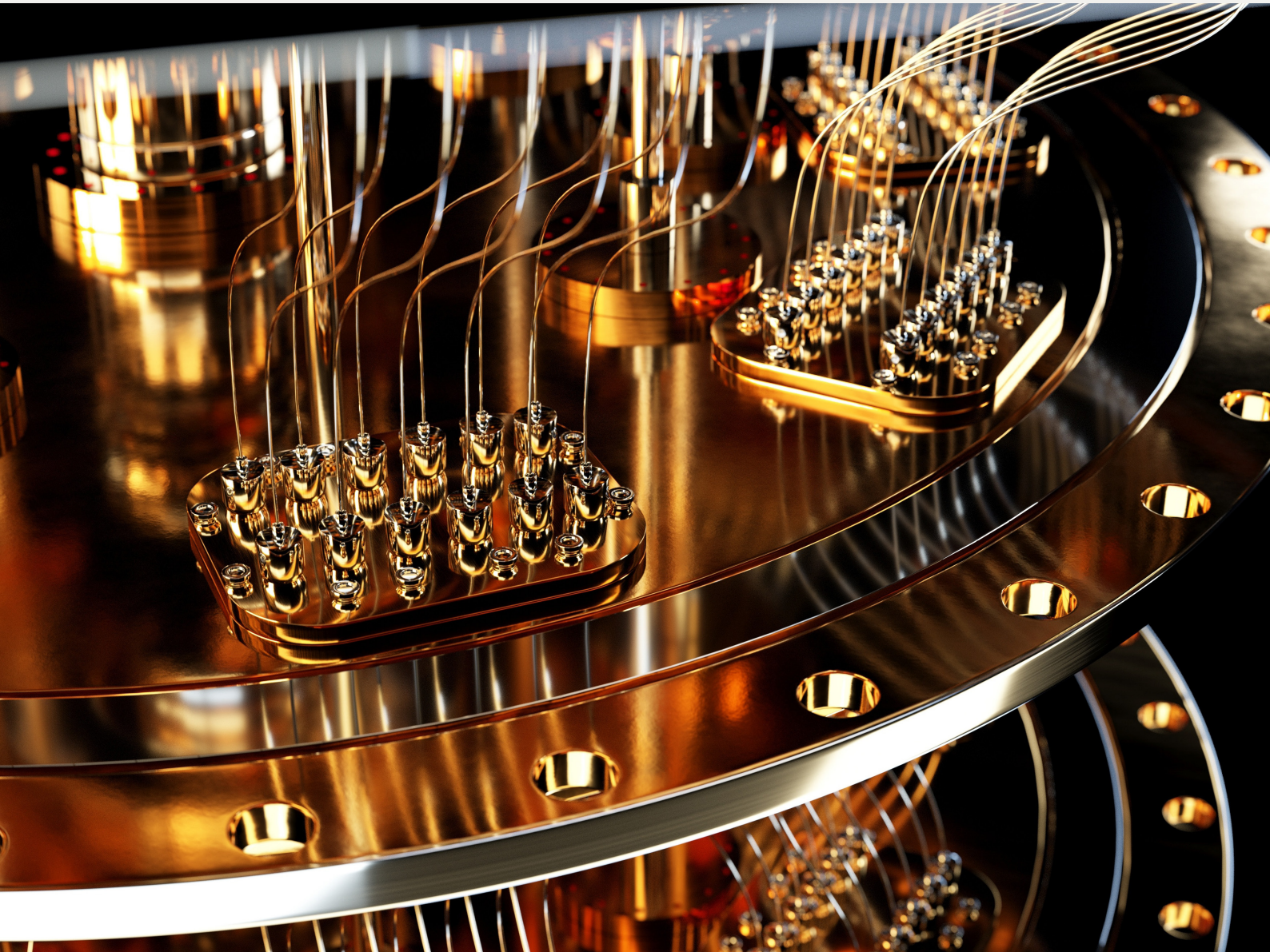
kyndryl

CIOのための量子コンピューターによる脅威ガイド

最も安全なデータにも有効期限があるか

クリス・ラブジョイ
キンドリル セキュリティ&レジリエンシー グローバルプラクティスリーダー



はじめに

長年にわたり、サイバーセキュリティはレジリエンスの追求によって定義されてきました。つまり、単に攻撃を防御するのではなく、それに耐えられるシステムを構築することが求められてきたのです。しかし、耐障害性を備えた量子コンピューティングの登場は、これまでにない脅威をもたらし、世界のデジタル経済を支える暗号基盤を崩壊させる可能性があります。

これはもはや理論上の話ではありません。サイバー犯罪による世界的な損失は2030年までに数兆ドル規模に達すると予測されており、量子コンピューターによる脅威はその大きな加速要因となるでしょう。CIOにとって、これは単なる技術的なリスクではなく、経営レベルで早急な対応を要する戦略的課題です。ポスト量子暗号（PQC）時代を理解し準備することは、真の長期的な企業レジリエンスを構築するうえで新たな必須条件となっています。

暗号の時限爆弾：「ハーヴェスト・ナウ、ディクリプト・レイター（今すぐ収集、後で解読）」

量子脅威の最も深刻な側面は、被害は既に始まっているということです。国家レベルの敵対勢力や高度な犯罪組織は、「ハーヴェスト・ナウ、ディクリプト・レイター（Harvest now, decrypt later）」攻撃を積極的に行っています。彼らは長期間にわたる財務記録、知的財産、顧客の個人識別情報、戦略計画など、最も機密性の高い暗号化データを大量に盗み出し、保管しています。このようなデータは現在、RSAやECCといった業界標準の暗号化技術によって保護され安全が確保されていますが、その保護に関しては、不確定ながらも「有効期限」があることが分かっています。

暗号解読に適した量子コンピューターが稼働した瞬間に、これらの暗号は破られ解読できるようになるでしょう。今日収集されたすべてのデータは、将来的なリスクとなります。このことはCIOにとって数十年安全だと思われていたはずのデータが突然漏えいし、前例のない規制、財務、そして風評のリスクに直面する可能性があることを意味します。

Y2Qグローバル期限

このような脅威について世界各国政府も軽視しているわけではありません。米国政府の国家安全保障覚書10号は、連邦機関が量子耐性暗号規格へと移行する厳格な期限を2035年と定めており、Y2Q（Years to Quantum）という世界的な移行の取り組みの開始を事実上宣言しました。2035年という期限は規制当局、サプライチェーン、顧客の期待に波及し、民間企業にも影響を与えます。

この世界的な移行は、Y2K問題の規模をはるかに上回るものになるでしょう。組織は、企業全体にわたるレガシーなソフトウェア、ハードウェア、デジタル証明書に深く埋め込まれた暗号プロトコルを特定し、置き換える必要があります。量子脅威が完全に現実化するのを待つという選択肢はありません。現時点で準備を怠る組織は、データセキュリティにおいて新たなレベルの脆弱性に直面することになります。

CIOのための実践ガイド：3つの必須事項

この移行を乗り切るには、問題認識の段階から実際の行動へと踏み出す必要があります。CIOの戦略は、次の3つの必須事項に集約されます。

01 暗号アジリティ（俊敏性）を確保：タスクフォースを設立

暗号アルゴリズムを容易に置き換え・更新できるシステム設計が必要です。その第一歩は、経営レベルでスポンサーされた「ポスト量子準備タスクフォース」を設置することです。これはIT部門の副業ではなく、戦略的イニシアチブとして認識されるべきです。

02 暗号資産調査：リスクを把握

タスクフォースの最初の使命は、暗号資産を調査して、企業全体の公開鍵暗号をすべて棚卸しすることです。脆弱な暗号を使用しているアプリケーション、システム、ベンダーを特定し、移行計画の基盤となる青写真を作成します。見えないリスクは管理ができないため、予算を確保して優先的に対応する必要があります。

03 移行計画と予算を策定：正式な取り組みとして位置付ける

棚卸し結果に基づき、米国国立標準技術研究所（NIST）が承認したPQCアルゴリズムへの移行に向けて、優先順位を付けたロードマップを策定します。最も重要なのは、今後のテクノロジーとセキュリティ予算として、移行を正式な予算項目に組み込むことです。移行は組織の長期的なレジリエンスにとって不可欠であり、複数年にわたる戦略的プログラムとなります。移行を単なるITアップグレードとして扱ってしまうと、失敗を招くことになります。

暗号化アルゴリズムのセキュリティ比較（従来型 と量子型）

ポスト量子暗号（PQC）戦略において重要なことは、どの暗号システムが脆弱で、どの程度脆弱であるか、そしてその脆弱性がいつ悪用される可能性があるかを理解することです。共通鍵暗号と公開鍵暗号では、脅威の性質が大きく異なります。

以下は、一般的なアルゴリズムと、それらを従来型コンピューターおよび量子コンピューターで解読するために必要な推定時間とリソースです。

アルゴリズム	種類	主な用途／暗号化対象	解読に要する時間（従来型コンピューター）	解読に要する時間（量子コンピューター）	必要な量子リソース
共通鍵暗号（単一の共有鍵）					
AES-256	共通鍵	**保存データと転送中データ** ファイル、データベース、ネットワークトラフィックの暗号化における最新のグローバル標準	**非現実的** 非常に長い時間（宇宙の年数の数十億倍）	**非現実的** 依然として数千年、あるいはそれ以上	**数百万の安定した物理量子ビット** 量子耐性があると見なされる
3DES / TDEA	共通鍵	**レガシーの金融システムや決済システム** ATM取引や旧式金融アプリケーションで使用。	**現実的** 専用ハードウェアで数カ月以内に解読可能	**数分から数時間**	数千量子ビット。従来型の脅威の方がより差し迫っている
DES	共通鍵	**時代遅れのシステム** 初期のメインフレーム暗号化標準	**非常に短い** 入手可能なリソースで数時間から数日以内で解読できる	**数秒**	最小限の量子コンピューター。非常に危険
公開鍵暗号（公開鍵と秘密鍵のペア）					
RSA-2048	公開鍵	**デジタル署名と鍵交換** ウェブトラフィックの保護（HTTPS）とソフトウェア / 文書の信頼性の検証	**非現実的** 数兆年	**数時間**	**約 2000 万物理量子ビット**（または約 4000 の安定した論理量子ビット）
ECC	公開鍵	**デジタル署名と鍵交換** モバイルや IoT で一般的な、RSA に代わる現代的で効率的な代替手段	**非現実的** 数兆年	**数時間**	**約 30 万物理量子ビット**（または約 2,500 の安定した論理量子ビット）
Diffie-Hellman	公開鍵	**鍵合意** TLS や VPN などのプロトコルで共有秘密鍵を確立	**非現実的** 数兆年	**数時間**	鍵サイズに応じた、RSA/ECC と同等のリソース

重要なポイント：公開鍵暗号が差し迫った脅威にさらされています。RSA や ECC のような公開鍵暗号は、数時間でアルゴリズムを解読されるようになり、保護されているすべてのデータが脆弱になり、「ハーヴェスト・ナウ、ディクリプト・レイター」攻撃が活発になります。

その一方で、共通鍵暗号は従来型の脅威にさらされています。メインフレームでよく使用される DES や3DES といったアルゴリズムにとって最も重大なリスクは、現在の従来型コンピューターに起因するものです。これらは既に解読されているか非推奨と見なされており、量子脅威の有無にかかわらず早急に対処すべきセキュリティの脆弱性となっています。

新しい共通鍵暗号のニーズには、量子耐性標準として AES-256が推奨されています。グローバーのアルゴリズムは、暗号解読時間を短縮する量子アルゴリズムで、理論上は AES-256を弱体化させるものの、AES-256の解読要件が膨大であるため、既知のあらゆる量子攻撃や従来型の攻撃に対して安全であり続けます。

暗号技術を解決済みの問題とみなす時代は完全に終わりました。CIO の役割は、組織の基盤を揺るがす新たなリスクに対応を拡大させることです。今こそ断固たる行動を取り、歴史的転換点においても組織を導いてください。新たなデジタルの現実において、リーダーは防御だけにとどまらず、レジリエントで、適応力があり、インテリジェンスである必要があるのです。

kyndryl