

耐量子暗号導入の スタートアップガイド



2024 年

NIST による、耐量子暗号標準の公開



2030 ~ 2035 年

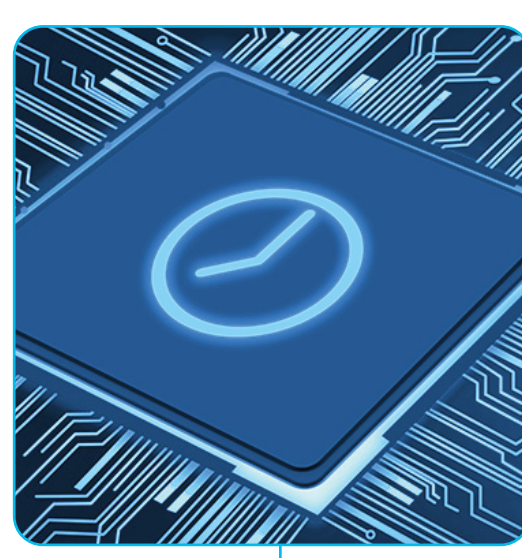
暗号上きわめて重要な量子コンピュータの出現



2024 ~ 2030 年

NIST 耐量子暗号標準への移行

NIST が耐量子暗号標準を公開しました。耐量子の世界の脅威を防御して、重要なデータのセキュリティを維持しなければならない時期が正式に始まったのです。このインフォグラフィックでは、耐量子暗号への移行に備えるためのヒントをご紹介します。



標準化団体との連携を強化

標準化を推進する組織と積極的に連携するとともに、必要なアルゴリズムやプロトコルの変更について、最新の開発状況を常に把握します。



重要なデータ資産をカタログ化

現在リスクにさらされている可能性があり、暗号関連の量子コンピュータが利用可能になれば復号されかねない重要なデータを特定し、カタログ化します。これにより、将来のリスクを評価します。



暗号技術を監査

暗号技術を使用する全システムを対象とした包括的なインベントリを実施します。これにより、耐量子暗号への移行をスムーズに進められます。



量子コンピューティングに脆弱な公開鍵システムを特定

インベントリリストから、公開鍵暗号が使用されている場所や目的を特定し、それらを量子コンピューティングに脆弱なシステムとしてマークします。



組織内の標準を更新

調達、サイバーセキュリティ、データセキュリティのそれぞれに使用されている標準を特定して更新し、耐量子の要件をそれらに反映させます。



調達



サイバーセキュリティ



データセキュリティ



リスクを評価し、システムアップグレードの優先順位を判断

組織の機能、目標、ニーズに基づいて、暗号技術を移行するシステムに優先順位を付けます。量子コンピューティングに脆弱なシステムをリスク評価する際には、次の点を考慮しましょう。



① 組織のリスク評価基準に従って高価値資産と見なされているか。



② どのような種類のデータをそのシステムによって保護しているか（鍵ストア、パスワード、ルート鍵、署名鍵、個人を特定できる情報、個人を特定できる機密情報など）。



③ どれくらいの期間、データ保護が必要か。



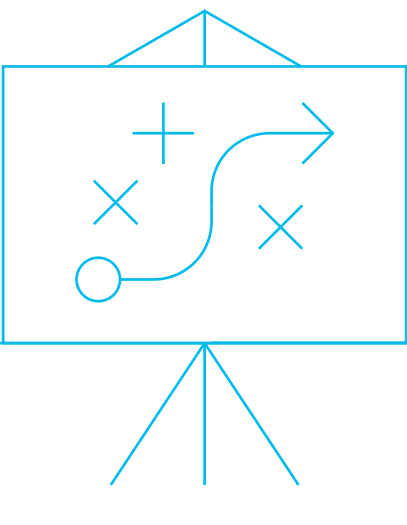
④ 他のどのシステムと通信しているか、情報が別の関係者に漏洩した場合にどのようなリスクがあるか。

- ・ 政府機関との間でどれほどの量の情報を共有しているか。
- ・ 外部組織との間でどれほどの量の情報を共有しているか。
- ・ 重要なインフラ部門に不可欠なシステムか。



移行戦略を策定

インベントリと優先順位付けの情報に基づいて、システムの移行計画を立てます。計画には、暗号技術上のアジリティ確保を組み入れ、将来の調整への対応や、予想しない変化への柔軟な対応を行えるようにします。



今すぐ始めましょう

- ・ 耐量子技術への安全な移行を定義するのに非常に良いタイミングです。
- ・ PQC を実装するうえでの明確な所有権を割り当てる必要があります。
- ・ データを保護するには、暗号技術への投資が不可欠です。



詳細については、www.cisco.com/go/pqc をご覧ください