ポスト量子暗号に備えるための 4 つの重要なステップ

量子コンピューティングの進展により、早ければ 2029 年にも暗号標準の安全性が低下することが予想されています。[1] つまり、量子コンピューティングを活用した復号に耐えられる暗号化が、まもなくあらゆるビジネスにとって必要なものになります。この差し迫った脅威と、すでに脅威となっている「Harvest now, decrypt later (今収集し、後で解読する)」攻撃に対処するため、組織は次の 4 つの重要なステップを考慮して、ポスト量子暗号に備える必要があります。

1 組織の機密データと既存の暗号化プロトコルを評価する

ポスト量子暗号への準備を開始するには、組織が保護する必要があるデータの現在の脆弱性を評価する必要があります。

これを行うには、多面的なチーム (ビジネス運用、法務およびコンプライアンス、IT、その他の関連部門の代表者を含む) を結集して、データへのすべてのアクセスパスを特定し、追跡するのが最善です。チームはこれらの調査結果をもとに、現在、近い将来、あるいは遠い将来、機密性があると見なされるデータの分類を開始できます。

次に、組織に現在導入されている暗号化プロトコルのインベントリーを取得し、どのプロトコルが更新の緊急性が最も高く、どれが変更可能で、どれがハードウェアやソフトウェアの制限のために同じままにする必要があるかを評価することが重要です。

2 優先すべき資産を特定する

チームは組織の機密データについて明確に把握できたら、直ちに保護する必要がある資産の優先順位を付けることができます。

さまざまな資産のセキュリティに一度に対処することは実用的ではなく、現実的でもありません。そのため、チームがすでに行った準備作業から得られた知見を利用して、計画において実用的なアプローチを採用し、直ちに対処すべき資産とシステムはどれで、後で対処すればよい資産とシステムはどれかを慎重に検討することが重要です。

1 Horvath, Mark、「Begin Transitioning to Post-Quantum Cryptography Now」、Gartner、2024 年 9 月 30 日。

3　自社の環境で新しい耐量子アルゴリズムのテストを開始する

ほとんどのコンプライアンス組織は、米国国立標準技術研究所 (NIST) が 2024 年 8 月にリリースした最初の確定された標準[2] などの新しい量子暗号プロトコルとアルゴリズムへの移行をできるだけ早く開始するよう組織に推奨しています。

チームがアルゴリズムのテストと、組織のアルゴリズムへの移行の成功を妨げる可能性のある問題の対処を早期に開始すれば、まもなく必須となるコンプライアンス要件に対する準備を整え、「今収集し、後で解読する」攻撃のリスクをより適切に軽減できます。

組織が新しい耐量子アルゴリズムのテストを開始しやすくするために、Red Hat® Enterprise Linux® 10 の導入またはアップグレードをご検討ください。このオペレーティングシステム (OS) には、耐量子アルゴリズムの最初のバージョンが含まれており、OpenSSL、ML-KEM (FIPS 203)、ML-DSA (FIPS 204) など、鍵交換、暗号化、署名を提供します。後続のリリースでは、追加機能が予定されています。

4　全面的な移行を開始してプロダクションへの移行に着手する

新しい耐量子アルゴリズムの実装はこのプロセスの最後のステップですが、プロセスの中で最も広範で複雑な部分です。

このステップには、すぐに結果を得ようとするのではなく、長期的なメリットを目標とする継続的な取り組みとして取り組む必要があります。

環境全体のすべての暗号化アルゴリズムのアップデートは即座に完了できるものではありませんが、準備段階で得られた知見と特定した優先事項により、組織が持続可能な成功を収められる態勢が整います。

暗号化プロトコルに変更を適用して耐量子アルゴリズムをプロダクションに組み込むにあたっては、意図しない結果やダウンタイムを軽減するために、テスト段階で特定された相互依存関係に特別な注意を払う必要があります。

ポスト量子暗号の準備を今すぐ始める

このページでは、組織がポスト量子暗号の時代に備えるのに役立つ耐量子アルゴリズムが Red Hat Enterprise Linux 10 にどのように組み込まれているかについて、詳しく説明しています。

2　「NIST Releases First 3 Finalized Post-Quantum Encryption Standards」、米国国立標準技術研究所、2024 年 8 月 13 日。