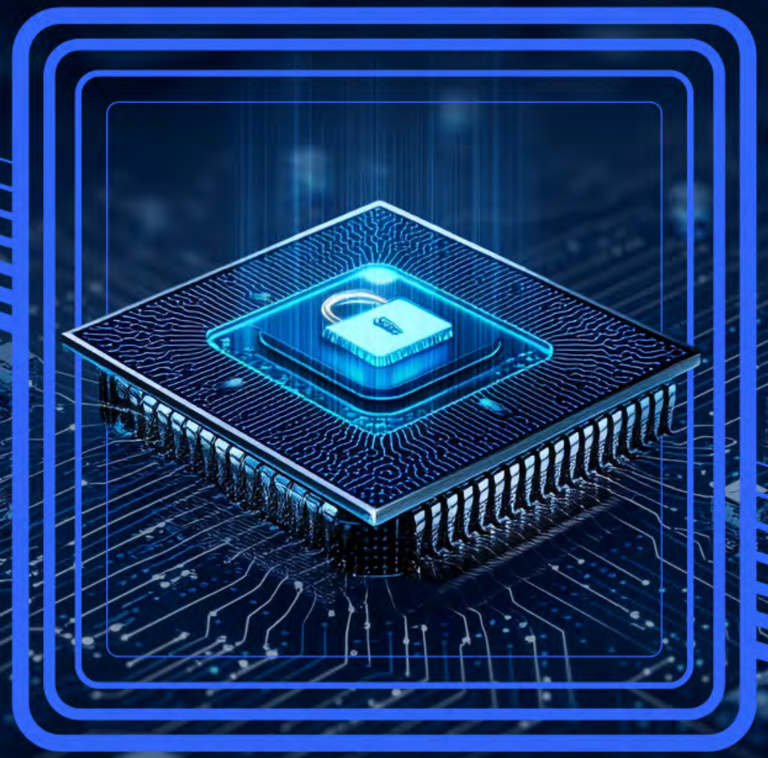
ホワイトペーパー



量子の転換点

抜本的な改革なしで行うポスト量子時代への備えに向けた経営幹部向けガイダンス

Zscalerチーフ サイエンティスト、インターネット アーキテクチャ委員会(IAB)委員、Yaroslav Rosomakho著

開始

zscaler

THE RESILIENCE FACTOR

はじめに

組織の計画において、将来にわたるリスクは十分に理解されています。リスクは脅威として認識されているものの、依然として遠い将来であるため、組織には影響が及ぶ前に準備する時間があります。しかし、このように余裕を持って対応できる状況は、量子を悪用したセキュリティ脅威には当てはまりません。実際に脅威が顕在化するよりはるか前に、準備のための時間がなくなりつつあります。

量子コンピューティングは、現代の暗号システムにとって将来的な課題となりますが、今すぐ対応を始める必要があります。現在の量子システムでは、現代の公開鍵暗号を大規模に破ることはできません。しかし、**暗号に関連する量子コンピューター (CRQC) のしきい値、いわゆる「Q デイ」を迎える時期は、早ければ 2030 年になる可能性があります**。その時期がいつになるかは不確かですが、それに備えて行動するために必要な準備期間は明らかです。

準備段階の攻撃はすでに始まっており、特に大量のネットワーク通信データにアクセスできる国家支援型の攻撃者による活動が目立っています。こうした攻撃者は、十分な性能を備えた量子技術が実現した際に復号することを見越して今のうちから暗号化されたデータを収集しています。

組織は脅威が現実のものとなる前に、ポスト量子時代への備え (PQR) を整えた状態に移行できるのでしょうか。早期に基盤を整備しておかなければ、組織はリスクにさらされ続けることになるでしょう。

ポスト量子時代への備え(PQR):

ポスト量子時代への備えとは、組織が依存している暗号技術のうち、将来の量子攻撃に対して脆弱なものを特定し、それらを量子耐性を備えた代替手段に、管理された段階的な手順で移行できる能力です。現状を把握し、移行に向けた計画を策定することは、ビジネス上の重要な課題です。

この意味で、量子コンピューティングは、「**意思決定の期限が迫る脅威**」として捉える方が適切かもしれません。決断をもって行動できる期間が短くなり、脅威そのものが現実化する前から新たなリスクが生じるためです。2026 年は、組織がこの脅威に戦略的に対処するうえで極めて重要な年となります。**実際、私たちは 2026 年を量子の転換点と捉えるべきだと考えています。**

3つすべての量子リスクの把握

データの機密性に影響を及ぼす「収集しておいて後で復号する」(HNDL) 攻撃モデルは、脅威が差し迫っていると同時に将来にわたるものであることを示す、広く知られた例です。Zscaler の最新の調査レポートである**波及効果：レジリエンスに優れたサイバーセキュリティの証**のデータは、この点を示しています。14 か国で 1,750 人の IT リーダーを対象に実施した調査の結果、ビジネス リーダーの 10 人に 6 人が、現在盗まれたデータが CRQC の登場によって悪用可能になった時点で、将来に重大なリスクを招く恐れがあると考えていることが明らかになりました。

しかし、HNDL は課題の 1 つにすぎません。より大きなビジネス上のリスクは、信頼です。現代のシステムにおける認証、認可、証明を支えるデジタル署名は、将来の CRQC に耐えられるよう設計されていません。署名が機能しなくなれば、何年も後ではなくリアルタイムで信頼が失われます。ポスト量子デジタル署名への移行は非常に複雑であり、複数のタイムラインが関係します。その計画は、今から始める必要があります。

最後に、規制環境も変化しています。脅威そのものが現実化する前に新たなコンプライアンス要件や規制要件が導入される可能性があり、組織が対応を後回しにすれば、評判、財務、法務の面で損害を被るリスクがあります。さらに状況を複雑にし、緊急性を高めているのが、どの攻撃者も暗号に関連する量子コンピューティング能力を獲得したかどうか、またいつ獲得したのかをを明らかにすることはないという現実です。組織のリスクを定量化し、戦略的な優先順位を設定する際、組織は長期間にわたってこの不確実性に悩まされることになるでしょう。**かなりの部分について、手探りで対応することになるのです。**

量子の脅威が緊急の課題となっているのは、単にその脅威が急速に迫っているからではありません。予防的な軽減策を講じるための時間が急速に失われつつあるからこそ緊急の課題なのです。

現実の運用では、備えよりも認識の高まりの方が速いペースで進んでいます。その大きな理由は、ほとんどの組織がプロトコル、環境、ベンダーにわたる暗号化のエクスポージャーを依然として定量化できていないことにあります。波及効果のレポートでは、52% の組織が、自社のセキュリティ システムでは現在の高度な脅威に対して防御できず、ましてや新たな脅威には対応できないことを認めています。そのため、明確な計画がないまま長期的な取り組みに優先順位を付けることは、より困難になっています。

洞察の共有

“本書では、こうした量子の脅威を、PQRに向けた経営幹部向けの計画に落とし込むことを目指します。これにより、リーダーはあらゆるリスクをより適切に理解し、エクスポージャーを定量化するとともに、移行中の影響範囲を縮小し、規格の進化に応じて適応できる俊敏性を構築できるようになります。

PQRは、Qデイがいつ到来するかを正確に予測することではありません。重要なレベルの機密性、信頼、全体的なセキュリティを保護しながら、対応の自由度を確保し、選択肢が狭まる前に管理された段階的な方法で移行できるようにすることです。

この計画的な移行に効果的に優先順位を付けるために、リーダーは以下の3つの主要なリスク領域に注目する必要があります。

機密性：現在転送中のデータが傍受され、将来的に復号される可能性

信頼：現在の認証システムが将来的に破られる可能性

コンプライアンス：今後の規制要件により、コンプライアンス違反となるリスク”



YAROSLAV ROSOMAKHO
Zscaler チーフ サイエンティスト、インターネット アーキテクチャ委員会 (IAB) 委員

なぜ今なのか：意思決定の期限が迫るリスク

マクロ経済や地政学的な変動が続く世界において、組織が直面する喫緊の課題は数多く、優先順位を付けることも困難です。

まだ現実のものとなっていないテクノロジー上の脅威が、比較的緊急性の低いものと考えられるのは無理もないことです。結局のところ、現在の暗号技術は、現時点で攻撃者が利用できるツールに対して概ね有効に機能しています。多くのセキュリティ部門は、迅速で大抵は事後対応型の防御策が求められる、AI による脆弱性の発見への対応に追われ、手一杯の状態です。さらに、規模を理由に自社は標的になる可能性が低いと考えている組織もあるでしょう。

しかし、将来の CRQC が招く脅威は、**その時が来たときに対応を切り替えるだけで軽減できるものではありません**。組織における将来のエクスポージャーを軽減するために必要な変革は、広範囲に及びます。このリスクは、すでに存在しています。

ポスト量子への移行には長い時間と複雑な対応が必要であり、周囲のあらゆる要素に左右されます。

長期的な計画サイクルは避けられず、ハードウェアとソフトウェアの両方について包括的なインベントリーを整備することが不可欠です。また、長期にわたる移行期間中は、従来の暗号とポスト量子暗号 (PQC) の環境を並行して稼働させる必要があります。移行の進捗は、ベンダー、規格、パートナー、そして更新サイクルに左右されます。

CRQC が存在することを示す証拠を待つという選択肢はありません。実際、このようなマシンが存在するかどうかについて、長期間にわたる不確実性が続くことは避けられません。なぜなら、**攻撃者がその能力を公表することはないためです**。幸い、今すぐ行動すれば、組織にはまだ準備に充てられる時間があります。

重要なポイント：

意思決定の期限が迫るリスクを誤って認識し、対応を先送りすると、脆弱性が高まり、ポスト量子暗号への移行を管理された状態かつ適切なタイミングで実施する能力が制限されます。

現在地から目標地点へ：現在の暗号技術とポスト量子時代への備え

暗号技術は、デジタル上の信頼を支える目に見えないインフラです。そのインフラがどこに存在し、どこで脆弱になる可能性があるのかを把握することが、量子の脅威に対する信頼性のある対応の基盤となります。

現代のデジタル システムは、暗号技術を次の 3 つの重要な機能に利用しています。**データの機密性を確保して交換する**こと、**アイデンティティーを認証する**こと、そして**オープン ネットワーク上で**データの完全性を維持することです。

幸いなことに、現代の暗号技術のすべてが量子の脅威に対して脆弱なわけではありません。現代の共通鍵暗号や広く利用されている暗号学的ハッシュ関数は、今後も堅牢性を維持すると予想されています。移行における主な優先対象は、**公開鍵暗号**、特に鍵交換とデジタル署名です。これらは置き換える必要があります。

鍵交換

鍵交換は、インターネットなどの信頼できない通信媒体を介して、二者が共有の「秘密」を確立するための仕組みです。この共有秘密は、その後、プロトコル固有の鍵スケジュールを使用して、他の鍵を導出するために使用されます。TLS、SSH、IPSec、WireGuard などの最新のプロトコルでは、CRQC によって解読される可能性のある数学的問題に基づく ECDHE などの鍵交換アルゴリズムが使用されています。鍵交換の脆弱性は、HNDL 攻撃に関連する主要なリスクです。

デジタル署名

デジタル署名は、ユーザー、デバイス、サーバー、Web サイト、ワークロードのアイデンティティーと完全性を検証するための仕組みです。現在広く導入されている RSA、ECDSA、EdDSA などの署名方式は、組織がほぼすべてのデジタルのやり取りで利用している信頼と認証のフレームワークを支えています。これらは Web サイトの証明書だけでなく、ユーザー認証情報、署名付きトークン、ハードウェア セキュリティ デバイス、そして現代の組織全体で大規模に運用されている公開鍵基盤 (PKI) にも組み込まれています。デジタル署名に対する量子の脅威とは、CRQC が (いつ登場するかは不明である可能性がありますが) 実現した場合、あらゆる認証と信頼が無効になることです。

重要なポイント：

PQRは、すべてを一律に置き換える作業ではなく、移行の順序が重要となる課題です。まずは鍵交換に重点を置き、その後すぐにデジタル署名に取り組むことが当面の優先事項です。

3つの主要なリスク：移行が必要となる背景

量子コンピューティングは、組織にとって3つの主要なセキュリティ リスクを招きます。これらを理解することで、なぜ移行が緊急の課題なのかが明確になります。

1. **機密性：**HNDL 攻撃は、現在の鍵交換メカニズムの脆弱性を悪用します。ポスト量子鍵交換への移行が完了する前に傍受されたデータは、CRQC が登場すれば将来的に復号されるリスクがあります。移行が 1 日遅れるごとに、攻撃者が将来悪用できるデータの量が増えていきます。

2. **信頼：**デジタル署名は、暗号化されたトラフィックと同じ HNDL のエクスポージャーを生み出すわけではありませんが、別の信頼性継続の問題を引き起こします。CRQC によって、攻撃者は署名を偽造したり、証明書、ソフトウェア アップデート、ファームウェア、署名付きトークン、長期保存される記録など、既存の信頼チェーンへの信頼性を損なったりする可能性があります。これにより、ユーザー、デバイス、サーバー、ワークロードを安全に認証、認可、証明することができなくなります。

3. **コンプライアンス：**政府や規制当局はすでに、ポスト量子暗号への移行について明確な期限を設定しており、2030 ～ 2035 年までに量子に対して脆弱な暗号を廃止または禁止とする動きが進んでいます。これは、NIST が公開した IR 8547 ロードマップ (組織がいつ、どのように量子耐性暗号に移行すべきかを示すもの) や、政府システムに対して量子耐性暗号への移行を義務付ける、最近の米国大統領令 EO 14412 にも表れています。CRQC が利用可能になるのが 2050 年になったとしても、組織はそれより何年も前からコンプライアンス違反のリスクにさらされる可能性があります。

これらのリスクに加えて、CRQC の「確認された」存在が把握されない可能性もあります。そのため、**ポスト量子暗号への移行は、近い将来における戦略上の最優先課題です。**ただし、これら 3 つのリスク領域には、それぞれ固有の要因、要件、緊急性の度合いがあります。これらについては、次ページの表にまとめています。リーダーはこの知見を活用し、移行に向けた基盤を整備できます。



リスク プロファイル：移行計画への影響

	機密保持	Trust	コンプライアンス
移行要因	現在転送中のデータが将来復号されることを防止	ユーザー、デバイス、システムの認証能力を保持	外部から課せられた期限に先立ち、コンプライアンスを維持
脅威の期間 / トリガー	現在収集されているデータ	CRQC が存在するようになった時点で発生	規制上の期限。技術的な期限とは無関係
緊急度	現在すでにデータが収集されていることを考えると、緊急性は極めて高い	複雑性と準備期間を考えると、緊急性が高い。現在進行中の攻撃によるものではない	規制当局の要件に依存
移行範囲	限定的：対象となる鍵交換プロトコルが明確に定義されている	広範：証明書、認証情報、ハードウェア、PKI 階層全体に組み込まれている	脆弱な暗号すべてに適用
移行アプローチ	段階的：ライブラリーや構成を段階的にアップグレード可能	保護を実現するには、PKI の信頼チェーン全体をエンドツーエンドでポスト量子対応にする必要がある	規制ガイダンスと期限によって決まる
ハードウェアの課題	低：主にソフトウェアと構成に関する課題	高：セキュリティ キー、TPM、HSM、セキュア エンクレーブの交換が必要	変数
並列稼働が必要？	移行期間中は、ハイブリッド モードやフォールバック モードが必要になる可能性がある	はい。移行期間中は、従来の PKI とポスト量子 PKI を同時に運用する必要が生じる可能性がある	規制要件による
移行の複雑性	中程度	高	変数

重要なポイント：

機密性、信頼、コンプライアンスはそれぞれ異なる要因から対応を迫りますが、いずれも同じ結論に行き着きます。ポスト量子への移行は、もはや選択肢ではありません。唯一の現実的な選択は、移行を段階的かつ管理された方法で進めるのか、それとも制約がますます増えるなかで進めるのかです。

PQRに関するプレイブック：把握、封じ込め、維持

量子の脅威には既知の要素も未知の要素も含めてさまざまな側面がありますが、組織には自らを守り、備えるための**明確な機会**があります。今すぐ断固として行動することで、ビジネス リーダーは将来直面するリスクを軽減できます。

ポスト量子時代への備えを実現するには、多くの組織がまだ備えていない専門的なスキルを組み合わせる必要があります。こうした作業 (資産のインベントリー化、リスクの優先順位付け、プログラム ガバナンスなど) は、社内で主導できる場合が多い一方、暗号技術の解読、プロトコルの修復、アーキテクチャーの再設計などより複雑な作業には外部の専門知識が必要になる可能性があります。実際には、ほとんどの組織がハイブリッド モデルを採用することになるでしょう。戦略的な管理は社内で維持しながら、専門パートナーの支援を得て複雑性の高い領域での実行を加速させるモデルです。重要なのは、早い段階から社内で理解を深め、主体性を確立することです。そうすることで、PQR を一度限りの変革ではなく、継続的に維持できる能力として定着させることができます。

以降では、ビジネスにおける移行を導くためのアクション プランを紹介します。意思決定者向けに策定されたこのプランは、組織が量子の脅威に伴う**業務の中断、エクスポージャー、信頼の喪失を最小限に抑える**ことを支援します。

重要なのは、対応を慎重に順序立てて進めることです。

ポスト量子時代への備えの進化：戦略的アプローチ

把握
新たな量子の脅威へのエクスポージャーを特定し定量化することで、効果的な優先順位付けを実現

封じ込め
PQRへの段階的移行中に、エクスポージャーを軽減するためのガードレールを導入

維持
基準や技術進歩の変化に迅速に対応できる能力を構築

PQRに関するプレイブック：移行の順序

移行プロセスを順序立てて進めることで、**早期に焦って対応することによるリスクと、対応が遅れてパニックに陥った状態で対応することによるリスクの双方を**排除するための枠組みを構築できます。これにより、組織の取り組みを、適切な順序で容易に管理できる**達成可能なステップ**に分割できます。地政学的、マクロ経済的、その他のテクノロジー上の既存の課題があるなかでも、対応を進めることが可能です。

今すぐこのプロセスを開始することで、数年後に解決が極めて困難になる可能性のある課題に取り組まなければならない事態を避けることができます。

洞察：認識から行動までのギャップ

Zscalerによる波及効果の調査では、多くの組織がすでに量子を信頼できる将来的な脅威として認識していることが明らかになっています。しかし、暗号化のエクスポージャーを明確に把握することが依然として難しいため、その認識が具体的な計画につながっていません。

この可視性のギャップが、認識を行動の停滞へと変えてしまいます。リーダーが、どのシステム、プロトコル、信頼チェーンが最も大きなエクスポージャーであるのかを把握できなければ、投資の必要性を説得力をもって示すことも、段階的な移行計画を策定することもできません。調査結果はまさにこの乖離を示しています。量子リスクが重大だと認識しているにもかかわらず、**55%の組織が自社のエクスポージャーを定量化することに苦慮しており**、さらに**57%はポスト量子暗号をまだ**サイバーセキュリティ戦略に組み込んでいません。

把握：
エクスポージャーを定量化しましょう。

把握できていないものに優先順位を付けることはできないため、可視性を対応の基盤にする必要があります。そのためには、資産とエクスポージャーの包括的なインベントリーを整備し、必要な対応を把握するとともに、優先的な投資の必要性を説明できるようにしなければなりません。推測や思い込みに頼らないでください。

鍵交換とデジタル署名の両方の環境におけるリスクを把握します。鍵交換のインベントリーは、TLS、SSH、IPSec、WireGuard など、明確に定義された特定のプロトコルに限定されます。デジタル署名のインベントリーは、より難しい課題です。証明書、ユーザーとワークロードの認証情報、ハードウェア依存関係にまで及ぶためです。

静的なインベントリーではなく、実際のトラフィックに基づいて、どの暗号アルゴリズムが実際に使用されているのかを可視化できるプラットフォームを活用することで、担当部門は**「認識」を測定可能なエクスポージャーへ**と変えることができます。Zscaler は、この変化を支援するために、このようなポスト量子暗号の可視性を提供しています。

可視化の転換：
リスク認識から、測定可能なエクスポージャーへ。

封じ込め：
移行中の影響範囲を縮小します。

量子耐性を備えたシステムへの移行は普遍的な必須事項ですが、露出しているすべてのシステムで同時に実施することは**できません**。組織は、従来のシステムとPQCシステムの両方を運用する、長期にわたる並行稼働に備える必要があります。

このフェーズで最初に行うべき重要なステップは、アップグレードに最も多くの時間と労力を要する従来のシステムやアプライアンスを特定し、それらが処理するデータを保護するための対策を講じることです。

ここでは、2つの選択肢があります。

- **データ機密性を低減**
  ビジネス リスクにつながる可能性のあるデータが、従来のチャネルを通じて送信されないようにします。現在収集されるリスクのあるデータは、Qデイまでに関係のないものにしておく必要があります。
- **従来のトラフィックをPQCトンネル内にカプセル化**
  送信元システムの能力にかかわらず、宛先との間に新たなPQC接続を確立し、まだアップグレードできないシステムにもポスト量子保護を実質的に拡張します。

この移行フェーズでは、一部のシステムを迅速にアップグレードできない場合があります。そのため、**ブローカー レイヤー**を活用することで、従来のトラフィックをカプセル化し、先の宛先との間に新たな接続を確立することで、エンドポイントがまだポスト量子対応でなくてもエクスポージャーを低減できます。**Zscaler Zero Trust Exchange**は、これを実現する実用的な方法を提供します。

封じ込めの転換：
従来のシステムが持ちこたえる期待から、安全な移行を実現するための設計へ。



維持：
クリプト アジリティーによるレジリエンスの構築

量子コンピューティングによって、これまで比較的安定していた暗号技術の世界に、新たなレベルの不安定性がもたらされます。レジリエンスは、現在のシステムがどれほど強固であるかではなく、絶えず変化する環境において迅速に対応できるよう、**十分な適応性**を維持できることによって定義されるようになります。

実際のところ、量子とAIを活用した暗号解析が進化するにつれて、ポスト量子暗号そのものが脆弱になる可能性もあります。**暗号プリミティブを変更できる能力**として、鍵交換アルゴリズム、共通鍵暗号、ハッシュ、デジタル署名方式を計画外の切り替えに伴う混乱を招くことなく、迅速かつ意図的に変更できることが不可欠になるでしょう。このモデルでは、これらのプリミティブをシステムやインフラにハードコードしません。状況に応じて、比較的短期間で切り替えられるようにします。

ポスト量子暗号への移行は、一度アップグレードすれば状況が落ち着くというような一回限りの対応にはならないでしょう。現在は予測できない、その他の破壊的な技術の進展によって、将来的にさらなる迅速な移行が必要になる可能性があります。**こうした適応可能な暗号インフラへの移行**によって、組織は危機的な状況に陥ることなく、この不確実性に対応できるようになります。目標は、暗号技術の変更を例外的かつ混乱を伴うイベントではなく、繰り返し実行可能な運用能力にすることです。

組織がどの暗号プリミティブをネゴシエートするかを一元的に設定し、更新できるようになり、コンテキストに応じてきめ細かく制御できるようになって、クリプト アジリティーは現実のものとなります。**Zscalerは、暗号プロファイルの開発を進めています**。これにより、規格や脅威の進化に応じて、以下のような制御をお客様に提供できるようになります。

- PQCを最善の努力として試みるだけでなく、PQCを確実に施行する機能
- 機密性の非常に高いデータに対して、より強固な(より計算負荷の高い)アルゴリズムを施行する機能
- クライアントとサーバーごとに暗号方式の優先順位をきめ細かく制御する機能
- 業界や地域によって相反する可能性のある、さまざまな規制要件への準拠

維持の転換：
一度限りのアップグレードから、長期的なレジリエンス能力へ。

PQRプレイブック：概要

	課題	教訓	アクション
可視化	エクスポージャーについてはよく理解されていない	優先順位付けと投資には可視性が不可欠	使用中のシステムの包括的なインベントリーを作成
封じ込め	従来のシステムごとに移行プロファイルが異なる	移行は不均一であり、従来のシステムと PQC の並行運用を伴う	移行中にエクスポージャーを軽減するためのガードレールを導入
維持	ポスト量子アルゴリズムは新しく、それ自体がさらなる移行を必要とする可能性がある	俊敏性が業務上の新たな必須事項	暗号技術の変更を、繰り返し実行可能な運用能力にする

重要なポイント：

PQRは、適切な作業を適切な順序で進めることが重要です。まずエクスポージャーを可視化し、次に移行中の影響範囲を縮小し、その後、規格や脅威の進化に合わせて継続的に適応できる俊敏性を構築します。

量子レジリエンス：備えの転換点

量子の脅威は、明確な兆候を示さずに現れる可能性があります。Qデイはまだ数年先になるとしても、脅威の証拠が確認されるまで待っていては、管理された移行を行う時間がなくなってしまいます。ポスト量子時代への備えを整えられる組織とは、意思決定の期限こそが実質的な締め切りであることを早期に認識している組織です。

進むべき道は明らかです。

把握：優先順位付けを可能にする可視性とインベントリーを構築します。

封じ込め：移行を進めながらエクスポージャーを軽減するガードレールを導入します。

維持：クリプト アジリティーを一度限りのプロジェクトではなく、恒久的な運用能力にします。

レジリエンスは、混乱が起きてから築くものではなく、混乱する前に備えておくものです。転換点はすでに到来しており、今こそ行動を起こすときです。

準備は万全ですか？

PQRのリトマス試験：リーダーとして、以下に挙げる質問を自問してください。いずれか1つでも「いいえ」と答える場合、組織は現在も将来も量子の脅威に対して脆弱です。

すべてのリーダーが自問すべき3つの質問は、以下のとおりです。

1. 自社の機密データがどのようにどこで露出する可能性があるかを把握していますか？
2. すべての暗号システムとプロトコルについて、最新の情報をリアルタイムで把握したインベントリーを整備していますか？
3. 暗号システムとプロトコルに対するガードレールを整備していますか？

備えの開始

ポスト量子暗号への移行は、すべてを一度に変える必要はありません。Zscaler Zero Trust Exchange は、検出から長期的な管理まで暗号リスクをリアルタイムで可視化、軽減、管理できるよう組織を支援します。

ZSCALER ZERO TRUST EXCHANGE の詳細はこちら

Zscaler について
Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™ は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 160 拠点以上のデータ センターに分散された SASE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細はこちら：www.zscaler.com/jp

Zscaler, Inc. (Worldwide HQ), 120 Holger Way, San Jose, CA 95134, United States