耐量子コンピュータの安全な未来への備え: APAC 調査

委託元: デジサート

独自実施: Ponemon Institute LLC

発行日: 2023 年 11 月

digicert

Ponemon INSTITUTE

耐量子コンピュータの安全な未来への備え:
APAC 調査

Ponemon Institute 作成、2023 年 11 月

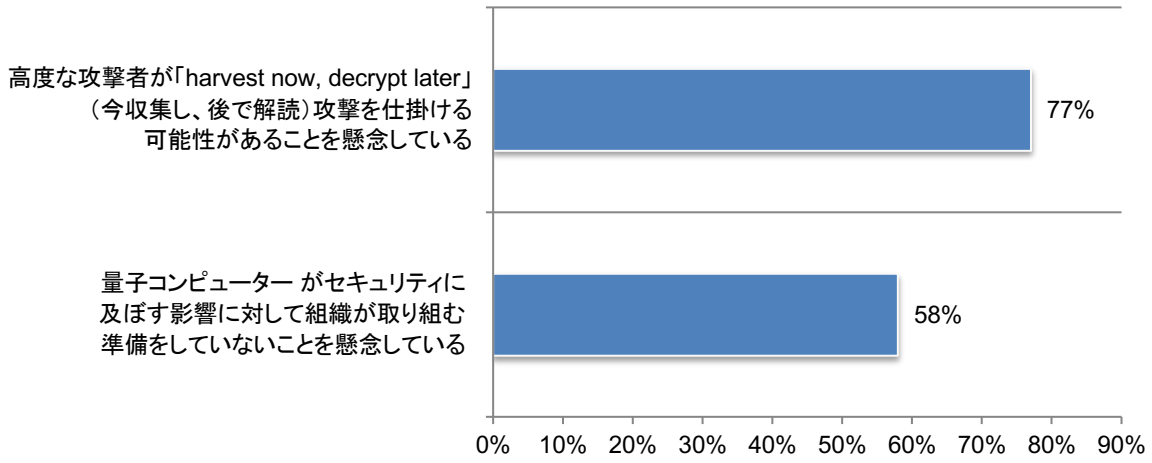
パート 1. イントロダクション

デジサートからの委託を受けて実施されたこの調査の目的は、組織が耐量子コンピュータの脅威にどのように取り組んでいるか、また、耐量子コンピュータの安全な未来に向けた備えはどのような状況かを理解することです。Ponemon Institute は、耐量子コンピューター暗号への組織のアプローチについて知っている APAC の IT 管理者および IT セキュリティ管理者 393 人を対象に調査を実施しました。

量子コンピュータは、量子力学の法則を活用し、従来のコンピュータには複雑すぎて解けない問題を解くことができます。しかし、量子コンピュータによって、暗号解読がはるかに簡単に行えるようになるため、データセキュリティに巨大な脅威がもたらされます。

そのため、図 1 に示すとおり、回答者の 57 パーセントが、こうしたセキュリティへの影響に取り組む準備ができていないことについて、非常に心配であると答えています。また、高度な攻撃者が「harvest now, decrypt later」攻撃を仕掛け、データを将来、復号することを目的として、暗号化されたデータを今、収集して蓄積する可能性があることも、重大な脅威となっています（回答者の 77 パーセント）。こうした懸念にもかかわらず、量子コンピュータがセキュリティに及ぼす影響に取り組むための戦略を組織が立てていると答えた回答者は、19 パーセントにとどまっています。

図 1. 量子コンピュータが引き起こすリスクについて深刻な懸念がある
1 =「懸念していない」から、10 =「非常に懸念している」までの 10 段階評価。評価 7 以上の回答を表示



以下の調査結果は、耐量子コンピュータの安全な未来に向けて備えるなかで、組織が直面している課題を示しています。

セキュリティチームは、組織を標的にしたサイバー攻撃の常に先を行きながら、耐量子コンピュータの未来に向けて備えるというプレッシャーに対処する必要があります。組織が企業全体でのリスク、脆弱性、攻撃の軽減について非常に効果を発揮していると答えた回答者は、50 パーセントにとどまりました。効果が不足している理由として、ほぼすべての回答者が、サイバー攻撃の巧妙化、標的の明確化、深刻化を挙げています。この調査の対象組織が受けたことがあるサイバー攻撃の上位 2 つは、ランサムウェアとアカウント乗っ取りです。

PQC への備えは時間との闘いです。回答者の 39 パーセントが、組織が備えを固めるための猶予期間は 5 年未満と答えています。最大の課題は、時間と資金が十分でないこと、そして成功させるための明確なオーナーシップが欠如していることです。現在、組織が PQC への備えに予算を割り当てていると答えた回答者は、32 パーセントにとどまっています。必要なサポートが得られていない理由の 1 つとして考えられるのは、量子コンピュータがセキュリティに及ぼす影響について、組織の幹部はある程度しか認識していない（30 パーセント）、またはまったく認識していない（19 パーセント）ためであると、回答者の半数近く（49 パーセント）が答えています。また、回答者の 51 パーセントは、PQC の影響がよくわからないと答えています。

組織が耐量子コンピュータの安全な未来に向けて備えるのに役立つリソースが用意されています。ここ数年の間に、ANSI X9 の Quantum Risk Study Group や米国商務省標準化技術研究所（NIST）の耐量子暗号プロ

ジェクトなどの業界団体は、組織が PQC に備えるための支援を開始しました。回答者の 55 パーセントが、これらの団体についてよく知っていると答えています。そのうちの 32 パーセントが、ANSI X9 の Quantum Risk Study Group について詳しく知っていると回答しています。米国科学アカデミーの「Quantum Computing: Progress and Prospects」レポートについて詳しく知っていると答えた回答者は 31 パーセント、米国商務省標準化技術研究所（NIST）の耐量子コンピューター暗号プロジェクトについてよく知っていると答えた回答者は 27 パーセントでした。

多くの組織は暗号鍵の特徴と場所を把握していない状況です。回答者の 51 パーセントが、組織は現在、使用している暗号鍵の種類と特徴のインベントリ作成を行っていると答えています。データ保持要件を理解することは PQC に備えるための重要なステップであると答えた回答者は 44 パーセントにとどまっています。暗号化資産のインベントリ作成と優先順位付けを行っている組織は、37 パーセントにとどまっています。

企業全体に一貫して適用される、完全に一元的な暗号管理戦略を立てている組織はほとんどありません。回答者の 40 パーセントが、自分の組織には特定のアプリケーションやユースケースに適用される限定的な暗号管理戦略しかないと答えています。また 23 パーセントが、組織には一元的な暗号管理戦略がないと答えています。

企業規模の暗号管理戦略を立てていない組織は、量子コンピュータ手法を利用したものを含め、セキュリティ脅威に対して脆弱です。自分の組織が暗号アルゴリズム、パラメータ、プロセス、テクノロジーのタイムリーな更新を非常に効率的に行っていると答えた回答者は、27 パーセントにすぎません。自分の組織が重要な情報を量子コンピュータの脅威から保護するのに必要な暗号技術を持つと確信している回答者は、23 パーセントにとどまっています。

暗号鍵の正確なインベントリは暗号管理戦略の重要な要素ですが、組織が鍵の使用の増加に常に対処するのは大仕事です。回答者の 48 パーセントが、自分の組織が実装する暗号鍵と電子証明書は増加していると答えています。回答者の 60 パーセントが、結果として、チームにかかる運用の負担は増えていると答えています。回答者の 63 パーセントが、自分の組織は所有している鍵と証明書の正確な数を把握していないと答えています。

鍵と証明書の設定ミスと、暗号変更への適応能力の不足は、暗号管理プログラムが効果を発揮する妨げとなります。回答者の 60 パーセントが、アルゴリズム廃止や耐量子コンピュータ暗号といった暗号変更への適応能力について懸念していると答えています。61 パーセントが、鍵と証明書の設定ミスについて懸念しています。55 パーセントが、SSL/TLS 証明書の有効期間の短縮によって生じるワークロードと機能停止のリスクの増加について懸念しています。

情報資産と IT インフラを保護するために、組織は暗号化ソリューションおよび手法を効率的に実装する能力を向上させる必要があります。ほとんどの回答者が、自分の組織は企業規模のベストプラクティスとポリシーの推進、証明書や鍵の不正使用の検知と対応、アルゴリズムや侵害の修復、および計画外の証明書の防止に必要な高い能力を備えていないと答えています。

Crypto Centers of Excellence（CCOE）は、量子コンピュータの安全な未来に向けた組織の取り組みをサポートできます。CCOE は、暗号化の運用プロセスの改善と、組織のトラスト環境の拡大を支援できます。組織は、セキュアな運用を維持し、適用される規制に準拠するために、高度なテクノロジーと暗号の専門知識を必要としています。この調査の対象組織のほとんどは、CCOE の設置を予定しています。ただし、現時点で、暗号に関する指導、調査、実装戦略、オーナーシップ、ベストプラクティスを提供する成熟した CCOE を組織に設置していると答えた回答者は、26 パーセントにとどまっています。さらに、回答者の 28 パーセントが、組織に CCOE は設置されているが、まだ発展途上であると答えています。

デジタルセキュリティの戦略上の最重要事項は、有能な人材の採用と定着への投資です（回答者の 56 パーセント）。これに続いて、暗号移行の俊敏性（回答者の 53 パーセント）、デジタルセキュリティの状況を強化するテクノロジーへの投資（回答の 47 パーセント）となっています。

日本とオーストラリアは 393 人の回答者から成るアジア太平洋のクラスターに含まれています。日本とオーストラリアはアジア太平洋のクラスターに含まれているため、これらの国の回答者について個別に分析することはできません。ただし、日本とオーストラリアの回答者について興味深い発見がありました。日本については、以下の点が挙げられます。

- サイバー攻撃の標的が明確化していると考える可能性は低い一方で、サイバー攻撃は深刻化していると考える可能性は高くなっている
- 日本の組織が耐量子コンピュータ暗号への備えに予算を割り当てる可能性は高まっている
- 暗号鍵のインベントリ作成を実施し、所有している暗号鍵と証明書の数を正確に把握する可能性は高まっている

オーストラリアについては、以下の点が挙げられます。

- オーストラリアの組織が量子コンピュータへの備えに必要なリソースを持っている可能性は低くなっている
- オーストラリアの組織が Crypto Center of Excellence を設置する可能性は高くなっている
- 量子コンピュータがセキュリティに及ぼす影響を上層部が認識している可能性は高くなっている

パート 2. 主な調査結果

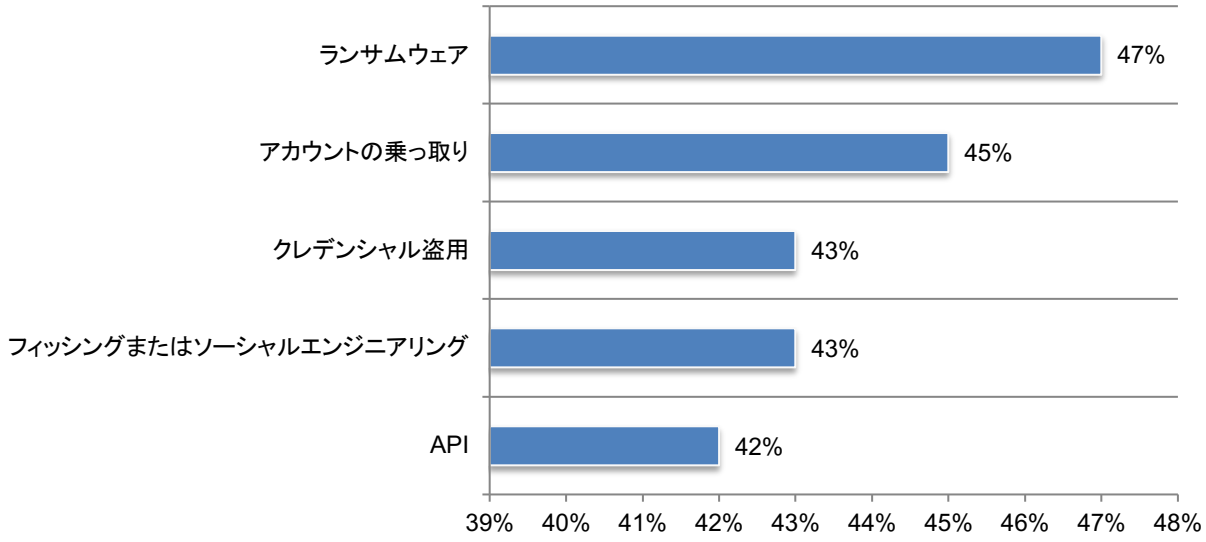
このセクションでは、APAC の調査について分析します。完全な調査結果は、このレポートの付録に記載されています。このレポートは次のトピックに従って構成されています。

- PQC（耐量子コンピューター暗号）への備えは不安定な状況
- 暗号管理の課題

PQC（耐量子コンピューター暗号）への備えは不安定な状況

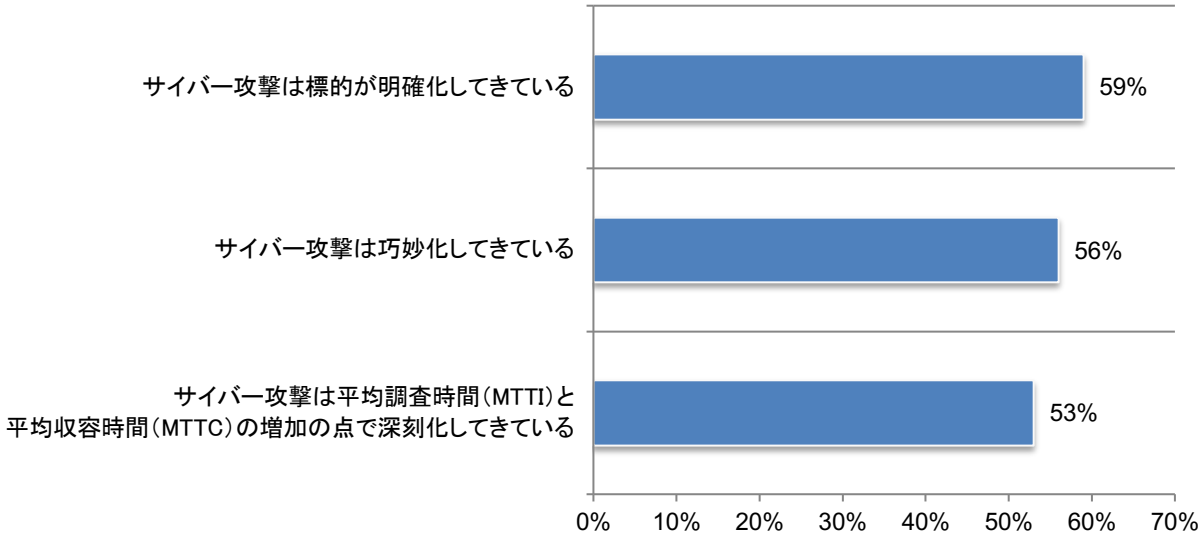
PQC への備えを進めるとともに、ランサムウェアやクレデンシャル盗用などのサイバー攻撃にも対処しなければなりません。回答者の 50 パーセントは、組織が企業全体でのリスク、脆弱性、攻撃の軽減について、あまり効果を発揮していないと答えています。結果として、過去 1 年で組織は少なくとも 1 件のサイバー攻撃を受けたことがあると、回答者の 47 パーセントが答えています。8 パーセントは、わからないと答えています。図 2 は攻撃の種類の上位 5 つを示しています。ご覧のとおり、ランサムウェア（回答者の 47 パーセント）とアカウントの乗っ取り（回答者の 45 パーセント）の 2 つが上位にランクされています。

図 2. 受けたことのあるサイバー攻撃
複数回答可



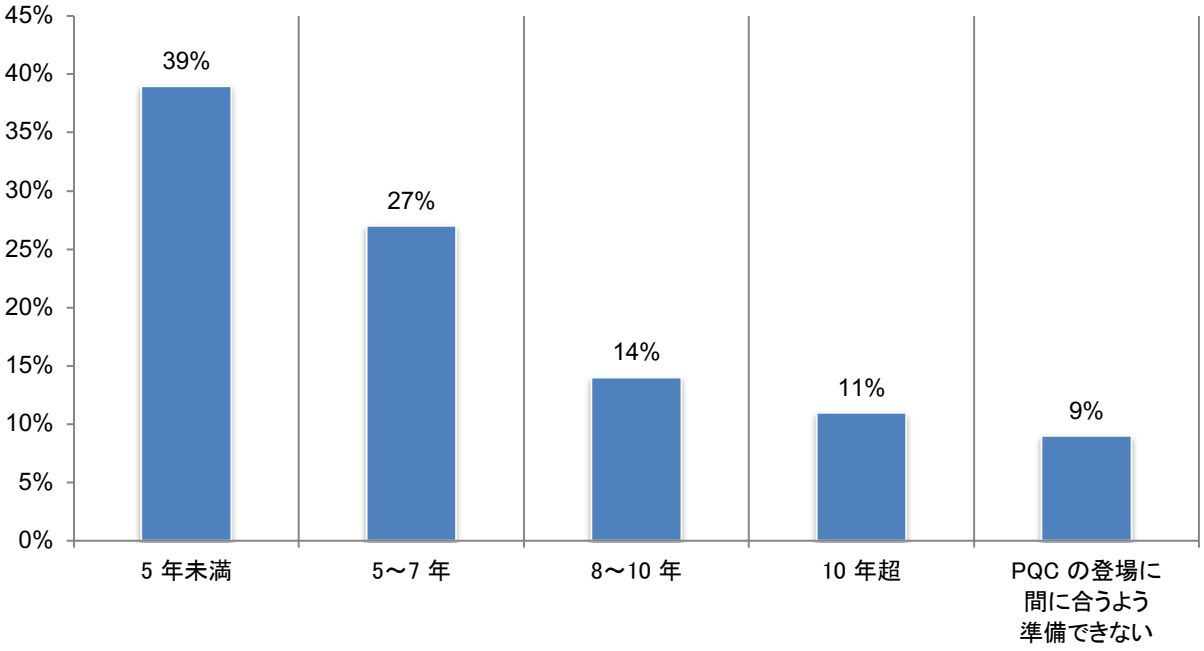
サイバー攻撃の深刻化と巧妙化は、組織のセキュリティ態勢に影響を及ぼしています。図 3 に示すとおり、回答者の 59 パーセントが、サイバー攻撃の標的がより明確化されてきていると答えています。サイバー攻撃は平均調査時間（MTTI）と平均収容時間（MTTC）の増加の点で深刻化していると答えた回答者は 53 パーセント、また、サイバー攻撃は巧妙化していると答えた回答者は 56 パーセントとなっています。

図 3. サイバー攻撃の巧妙化、標的の明確化、深刻化が進んでいる
「強くそう思う」と「そう思う」の回答の合計



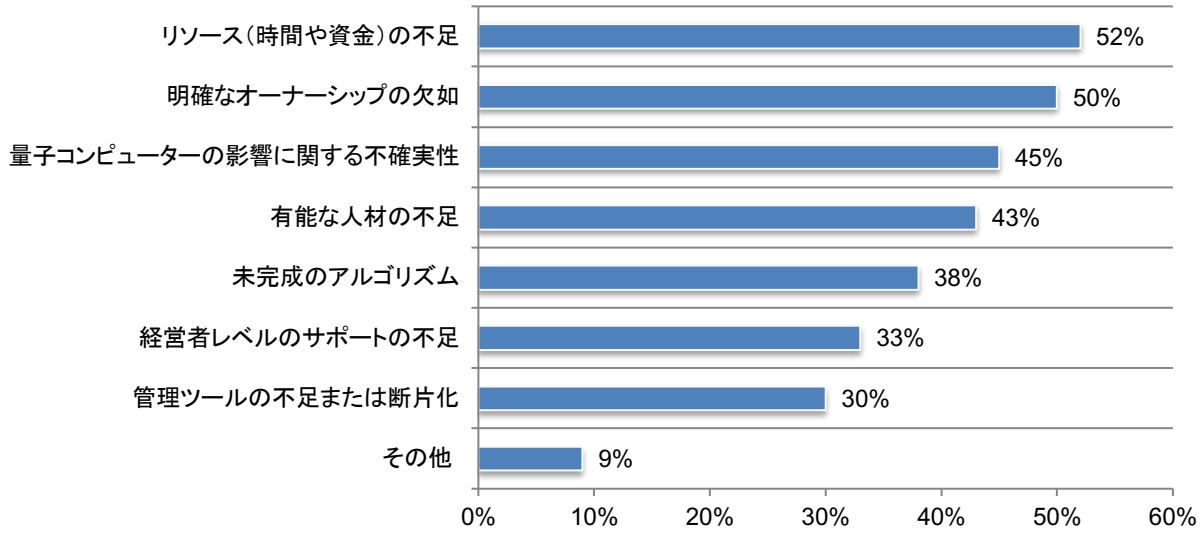
PQC への備えは時間との闘いです。組織が PQC への準備を整えるのにどれぐらいの猶予期間があるか、回答者に質問しました。図 4 に示すとおり、5 年未満と答えた回答者は 39 パーセントでした。組織が備えを固めるための猶予期間は 8 年以上、または 10 年超と考えている回答者は、合計 25 パーセントにとどまっています。

図 4. 組織が PQC への備えを固めるための猶予期間はどれぐらいだと思いますか？



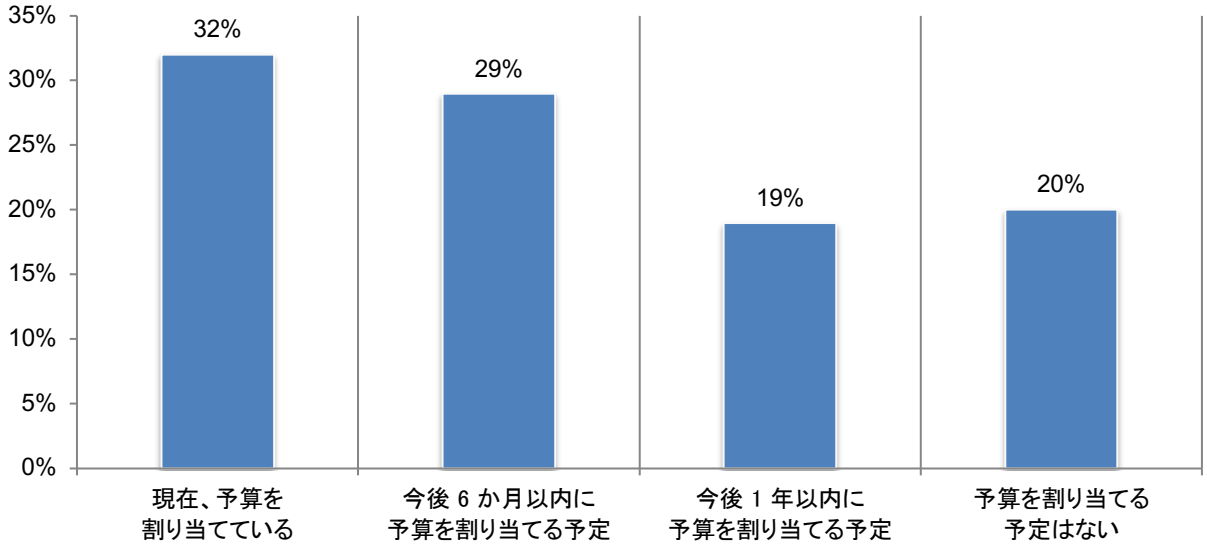
PQC への備えを固めるのは難しい状況です。リソース（時間または資金）が不十分で、明確なオーナーシップが欠如しているからです。図 5 に示すとおり、リソースの割り当てが不十分であることは、耐量子コンピュータ暗号によって安全な未来への備えを固める能力に影響を及ぼしています（回答者の 52 パーセント）。これに続いて、「明確なオーナーシップの欠如」（回答者の 50 パーセント）、「PQC の影響に関する不確実性」（回答者の 45 パーセント）となっています。

図 5. PQC への備えで主な課題となるのは何ですか？
3 つ選択可



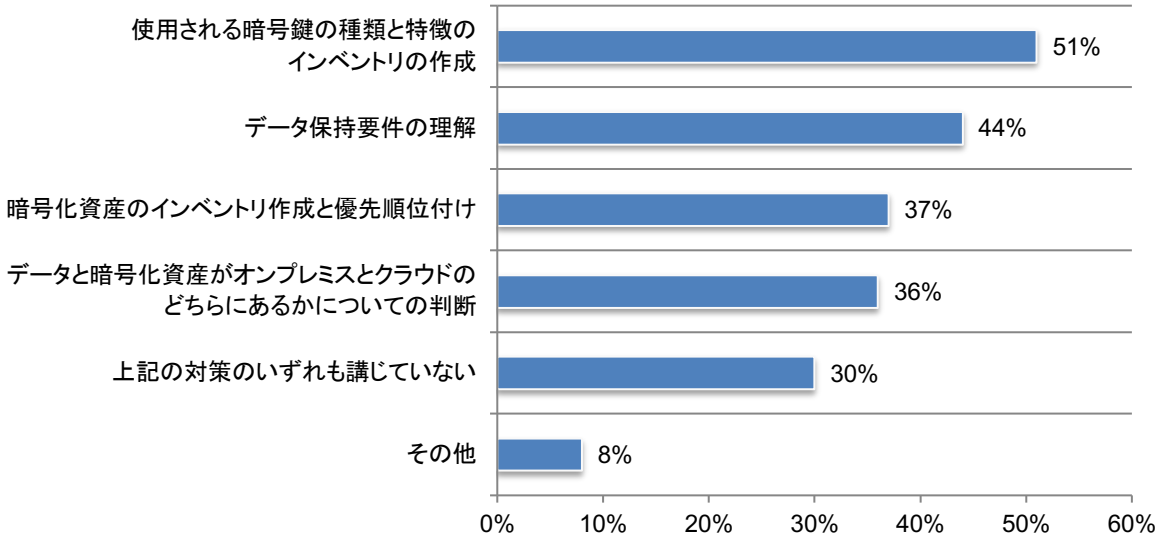
前述のとおり、資金不足は PQC への準備の妨げとなります。図 6 に示すとおり、組織が耐量子コンピュータ暗号への備えに「何らかの」予算を割り当てていると答えた回答者は 32 パーセントにとどまっています。組織が資金を提供する予定はないと答えた回答者は、20 パーセントに達しています。

図 6. 組織は耐量子コンピュータに「何らかの」予算を割り当てていますか？



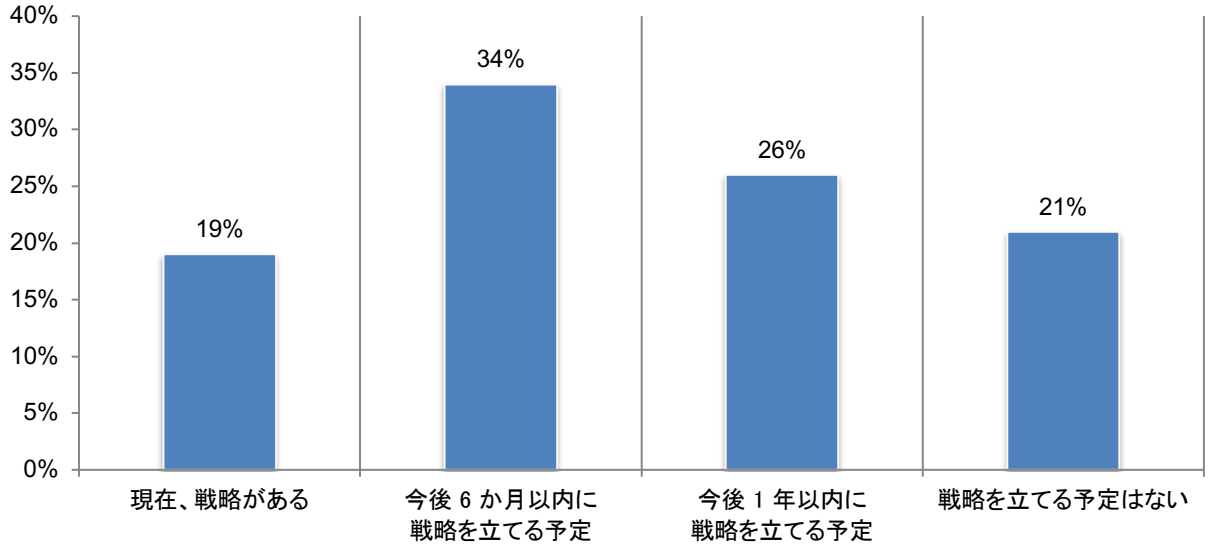
多くの組織は暗号鍵の特徴と場所を把握していない状況です。自分の組織が暗号鍵の種類と特徴のインベントリ作成を行っていると答えた回答者は、半数（51 パーセント）にとどまっています。これに続いて、「データ保持要件を理解するための対策を講じている」と答えた回答者は、44 パーセントとなっています。 図 7 に示すとおり、「暗号化資産のインベントリ作成と優先順位付け」と答えた回答者は、37 パーセントにとどまっています。

図 7. 耐量子コンピュータ暗号に備えるために、組織はどのような対策を講じていますか？
複数回答可



PQC の登場に間に合うよう備えを固めるために、組織は戦略とスケジュールを策定する必要があります。しかし、図 8 に示すとおり、組織に戦略があると答えた回答者は、19 パーセントにとどまっています。一方、今後 6 か月以内（34 パーセント）または来年までに（26 パーセント）戦略を立てる予定はないと答えた回答者は、60 パーセントとなっています。組織が戦略を立てる予定がないまま動いているという答えた回答者は、21 パーセントとなっています。

図 8. あなたの組織は量子コンピュータがセキュリティに及ぼす影響に取り組むための戦略を立てていますか？

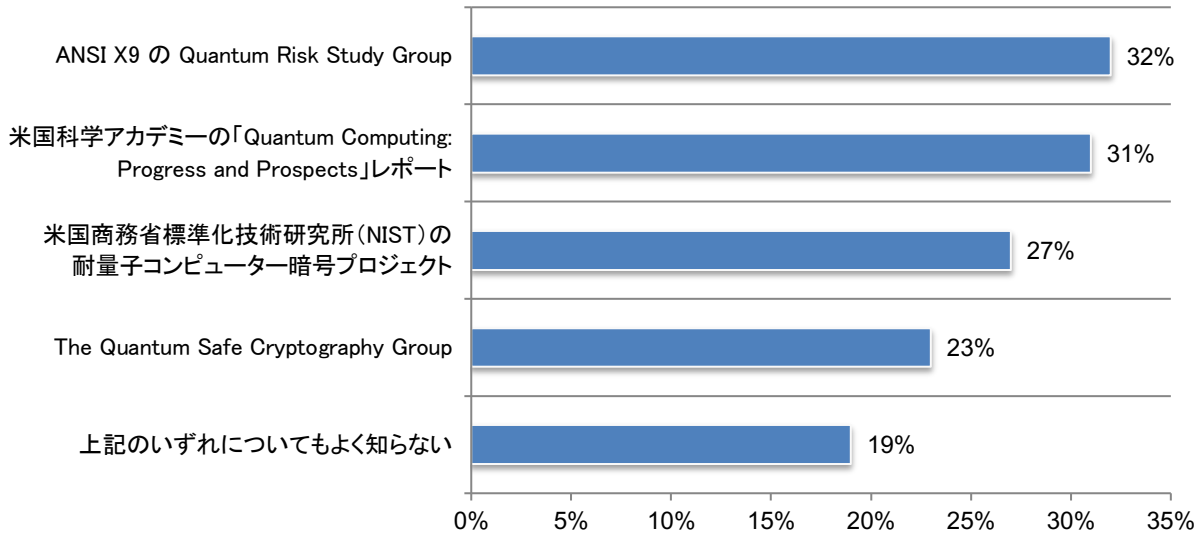


組織が耐量子コンピュータの安全な未来に向けて備えるのに役立つリソースが用意されています。耐量子の未来に備えるために業界標準化団体が実施している取り組みについて「よく知っている」または「知っている」と答えた回答者は、51 パーセントでした。

図 9 は、業界標準化団体を示しています。最もよく知られているのは ANSI X9 の Quantum risk Study Group です。この Study Group は 2018 年に設立されました。設立の目的は、量子コンピュータの状況を検討し、暗号に関連する量子コンピュータが金融業界に及ぼすリスクを判断し、このような量子コンピュータが登場する可能性が最も高い時期を判断することでした。

「Quantum Computing: Progress and Prospects」レポートを発行した米国科学アカデミーの取り組みについて知っている回答者は 31 パーセント、また、米国商務省標準化技術研究所（NIST）の耐量子コンピューター暗号化プロジェクトについて知っている回答者は 27 パーセントでした。

図 9. あなたの組織は、耐量子コンピューター暗号の未来に備えるための業界標準化団体の取り組みについて知っていますか？
複数回答可



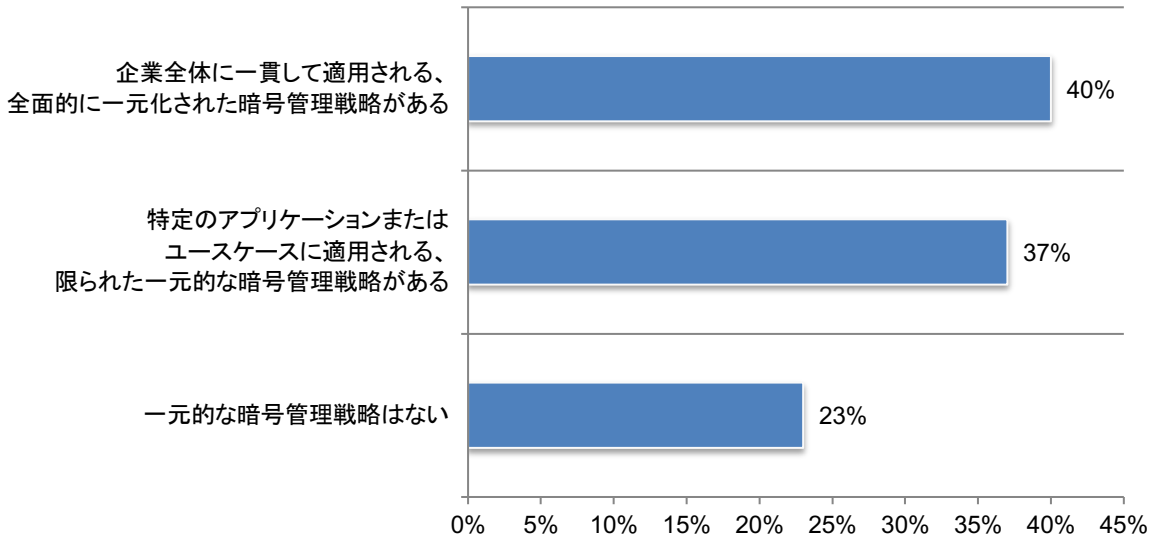
暗号管理の課題

この調査で明らかになったとおり、暗号は、意図しない受取人が理解できない形式に情報を変換することにより、情報を保護する手段です。暗号化アルゴリズムは、メッセージとデータをデジタルエンコードして通信とトランザクションの機密性、完全性、否認防止、真正性を確保するために使用されます。

企業全体に一貫して適用される一元的な暗号管理戦略を立てている組織はほとんどありません。多くの組織に耐量子コンピュータ戦略がないのと同様ですが、図 10 に示すとおり、自分の組織には特定のアプリケーションやユースケースに適用される「限定的な暗号管理戦略がある」（37 パーセント）、または「一元的な戦略はない」（23 パーセント）と答えた回答者は、60 パーセントとなっています。

このような戦略には、暗号鍵のインベントリ作成、暗号鍵の特性の理解、脆弱な暗号の修正、ベストプラクティスへの準拠、および暗号を制御し要件を遵守するポリシーの適用を目的とした継続的監視を含めることをお勧めします。

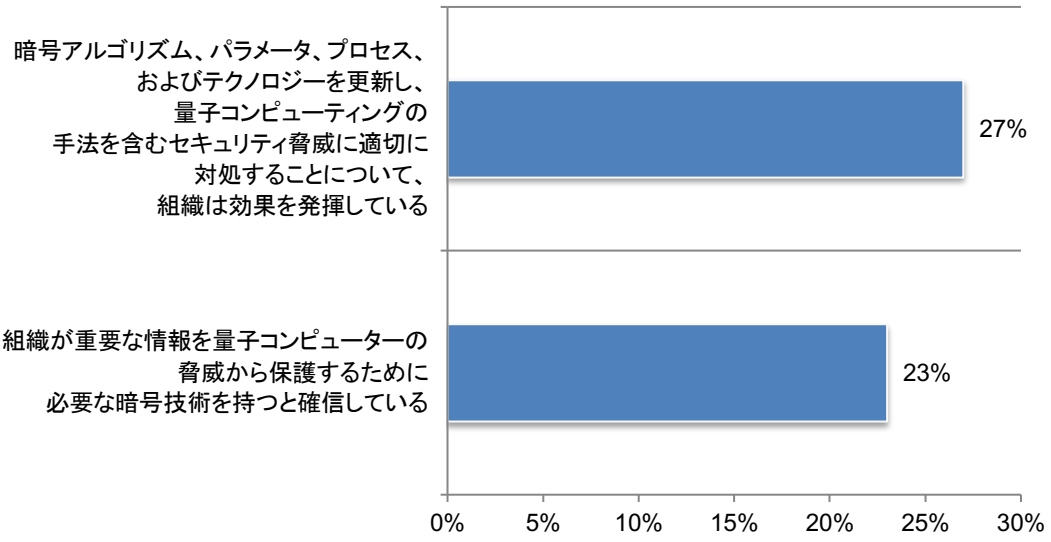
図 10. あなたの組織には、一元的な全社規模の暗号管理戦略がありますか？



企業規模の暗号管理戦略を立てずに、暗号アルゴリズムのタイムリーな更新を効率的に行っている企業は、ほとんどありません。組織が暗号アルゴリズム、パラメータ、プロセス、およびテクノロジーの更新について、どの程度、効果を発揮しているかについて、回答者に評価を依頼しました。1 =「効果を発揮していない」から、10 =「非常に効果を発揮している」までの 10 段階評価です。また、組織が重要な情報を量子コンピュータの脅威から保護するために必要な暗号技術を持つことを、どの程度確信しているかについても、評価を依頼しました。1 =「確信していない」から、10 =「強く確信している」までの 10 段階評価です。図 11 は、「非常に効果を発揮している」、および「強く確信している」という回答（10 段階の評価 7 以上）を示しています。

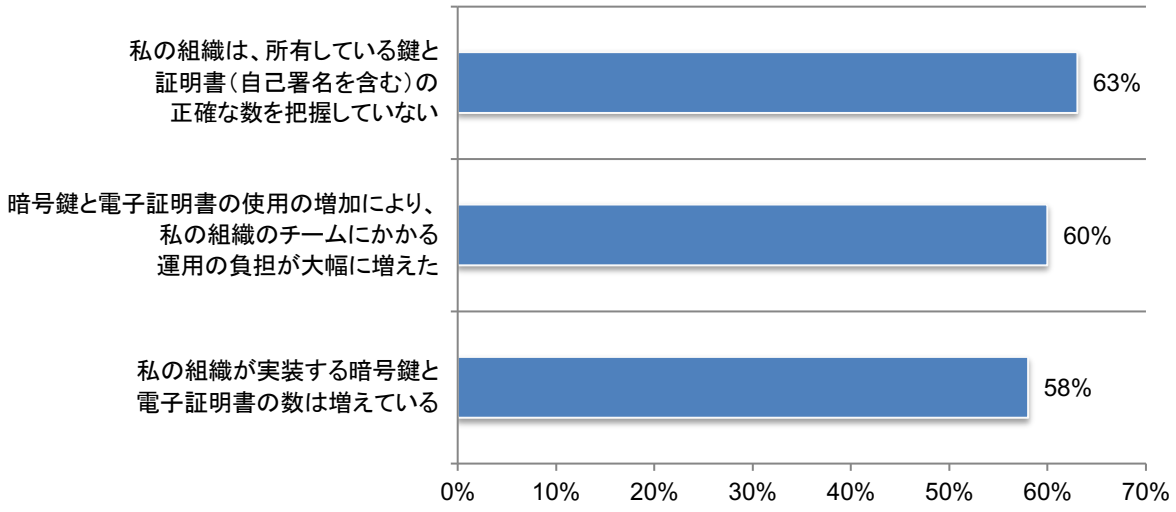
ご覧のとおり、暗号アルゴリズム、パラメータ、プロセス、およびテクノロジーのタイムリーな更新について、非常に効果を発揮していると答えた回答者は、27 パーセントにとどまっています。組織が重要な情報を量子コンピュータによる脅威から保護するために必要な暗号技術を持つと確信している回答者は、23 パーセントにとどまっています。

図 11. 暗号アルゴリズム、パラメータ、プロセス、およびテクノロジーの更新について効果を発揮しているか、また、重要な情報を量子コンピュータの脅威から保護するために必要な暗号技術を持つと確信しているか
1 =「効果を発揮している」/「確信していない」から、10 =「非常に効果を発揮している」/「強く確信している」までの 10 段階評価。評価 7 以上の回答を表示



暗号鍵の正確なインベントリは暗号管理戦略の重要な要素ですが、組織は所有している鍵と証明書の正確な数を把握していません。図 12 に示すとおり、63 パーセントの回答者が、組織は所有している鍵と証明書の数を把握していないと答えています。回答者の 48 パーセントが、自分の組織が実装する暗号鍵と電子証明書は増加していると答えています。結果として、回答者の 60 パーセントが、暗号鍵とデジタル証明書の使用の増加により、チームにかかる運用の負担が増えたと答えています。

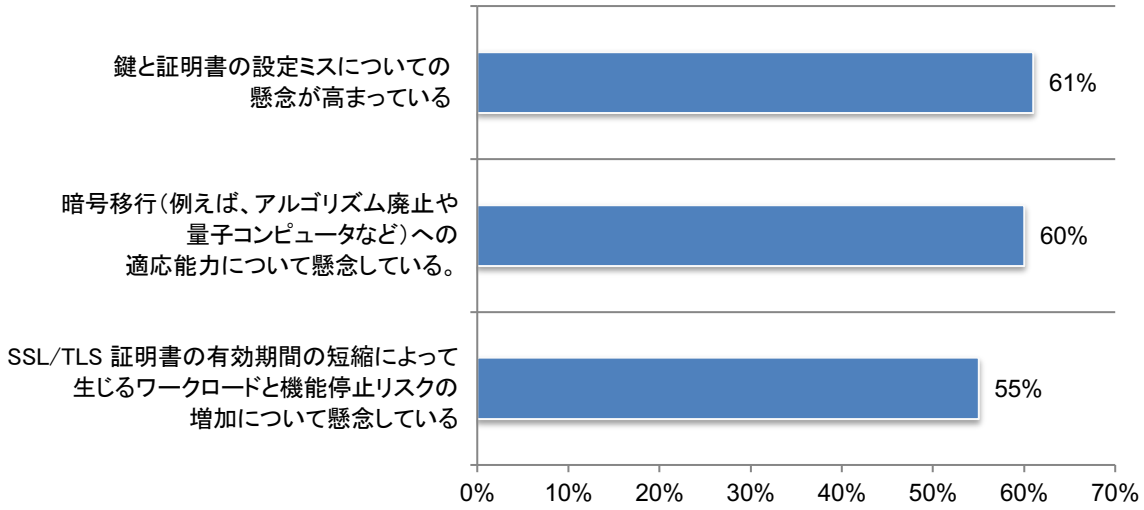
図 12. 実装する暗号鍵とデジタル証明書の増加は負担となっており、組織が所有している鍵と証明書の数が把握しにくくなっている
「強くそう思う」と「そう思う」の回答の合計



鍵と証明書の設定ミスと、暗号移行への適応能力の不足は、暗号管理プログラムが効果を発揮する妨げとなります。暗号管理プログラムの成功には重大な課題があります。図 13 に示すとおり、ほとんどの回答者は鍵と証明書の設定ミス（61 パーセント）、暗号移行への適応能力（61 パーセント）、および SSL/TLS 証明書の有効期間の短縮によって生じるワークロードと機能停止リスクの増加（55 パーセント）について懸念しています。

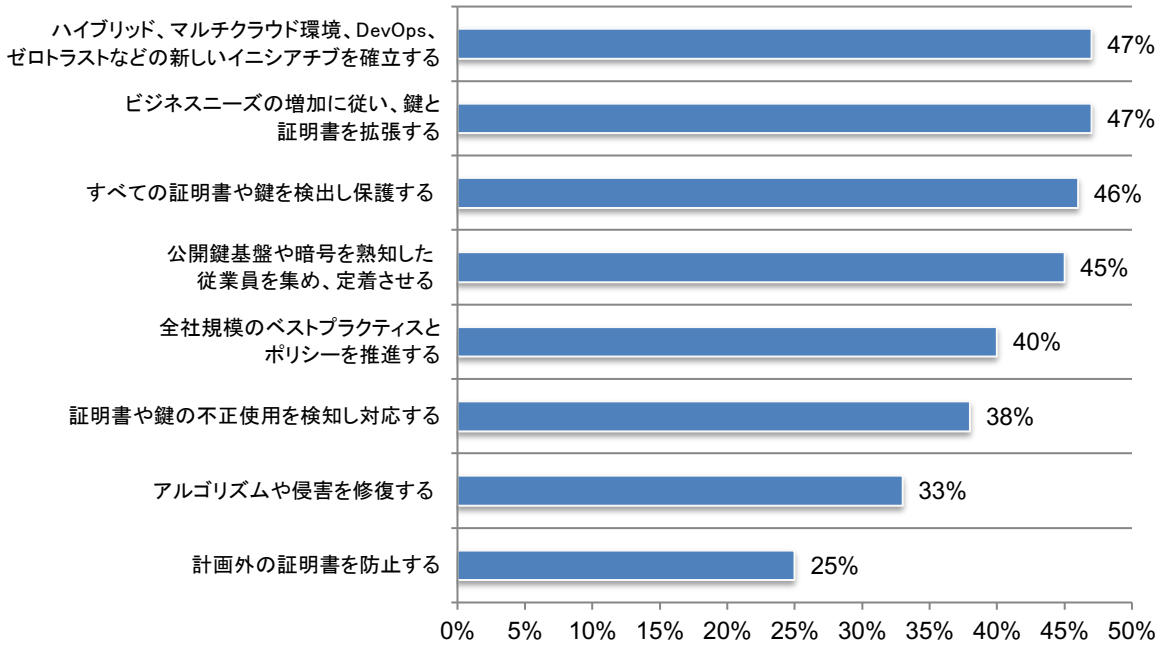
図 13. は SSL/TLS 証明書の有効期間の短縮、鍵と証明書の設定ミス、暗号移行への適応能力について懸念している

「強くそう思う」と「そう思う」の回答の合計



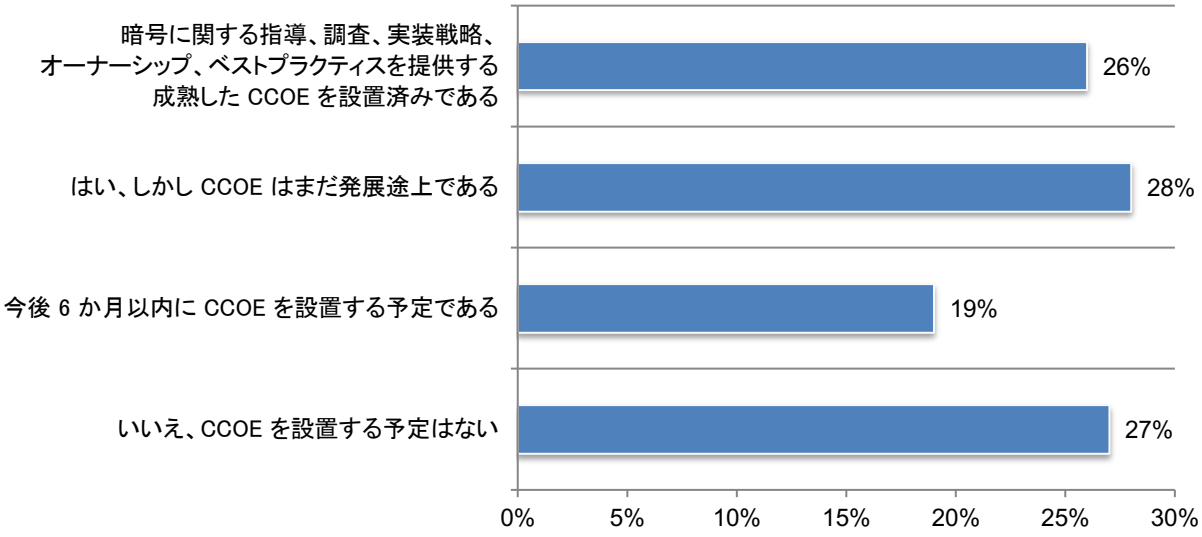
暗号ソリューションおよび手法の実装を効率的に行うことができないために、重要な情報がリスクにさらされます。情報資産と IT インフラを保護する能力について、回答者に質問しました。1 =「能力が低い」から、10 =「能力が高い」までの 10 段階評価です。図 14 は、「能力が高い」と回答された項目（10 段階の評価 7 以上）を示しています。ご覧のとおり、能力が高いと評価した回答者は半数未満です。ハイブリッド、マルチクラウド環境、DevOps、ゼロトラストなどの新しいイニシアチブを確立する能力が高いと答えた回答者は、47 パーセントにとどまっています。ビジネスニーズの増加に従って鍵と証明書を拡張する能力が高いと答えた回答者も、47 パーセントとなっています。組織が証明書や鍵をすべて検出して保護する能力が高いと答えた回答者は、半数未満（46 パーセント）でした。

図 14. 資産と IT インフラを保護するために暗号化ソリューションおよび手法を効果的に実装する能力
1 =「能力が低い」から、10 =「能力が高い」までの 10 段階評価。評価 7 以上の回答を表示



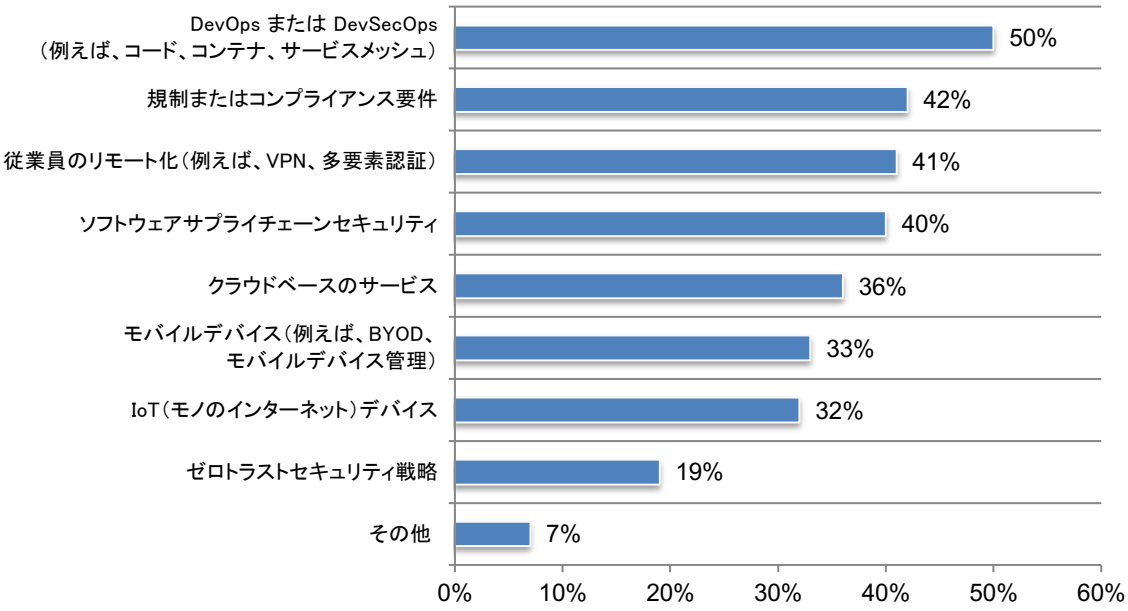
Crypto Centers of Excellence（CCOE）は、量子コンピュータの安全な未来に向けた組織の取り組みをサポートできます。CCOE は、暗号の運用プロセスの改善と、組織のトラスト環境への信頼の向上をサポートできます。CCOE は、セキュアな運用を維持し、適用される規制に準拠するために、高度なテクノロジーと使用される暗号の専門知識を必要としています。ただし、ご覧のとおり、組織に成熟した CCOE が設置されていると答えた回答者は 26 パーセントにすぎません。組織に CCOE は設置されているものの、まだ発展途上であると答えた回答者は、28 パーセントとなっています。

図 15. あなたの組織は CCOE を設置済みですか？



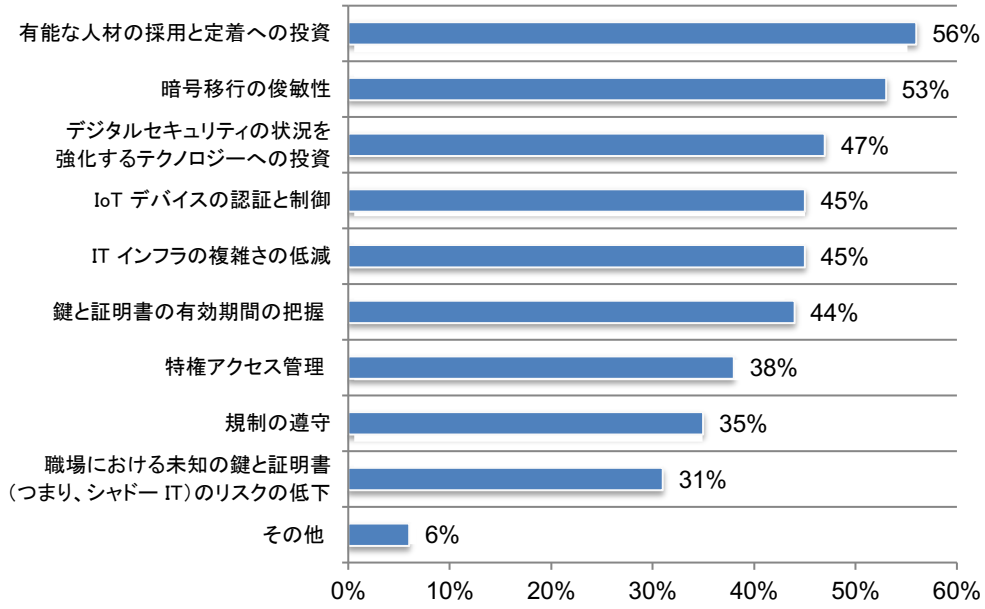
DevOps や DevSecOps は、公開鍵基盤、鍵、証明書、その他のシークレットの実装を促進する主要要因です（回答者の 50 パーセント）。図 16 に示すとおり、その他の主要要因には、規制またはコンプライアンス要件（42 パーセント）、およびリモート従業員（41 パーセント）などがあります。

図 16. 公開鍵基盤、鍵、証明書、その他のシークレットの実装を推進する主要なトレンドの上位 3 つは何ですか？
回答の上位 3 つを表示



有能な人材の採用と定着への投資は、デジタルセキュリティの重要事項です。図 17 に示すとおり、有能な人材の採用と定着への投資はデジタルセキュリティの戦略上の最重要事項であると答えた回答者は、56 パーセントでした。暗号移行の俊敏性は戦略上の優先事項であると答えた回答者は、53 パーセントでした。デジタルセキュリティの状況を強化するテクノロジーに投資することも、戦略上の重要事項であると答えた回答者は、47 パーセントでした。

図 17. デジタルセキュリティの戦略上の最優先事項は何ですか？
複数回答可



まとめ

PQC に備えるために、組織は次のステップを組み込む戦略を立てる必要があります。

- 上層部は、量子コンピュータによって引き起こされるデータセキュリティへの脅威を理解する必要があります。調査が示すとおり、組織は PQC への備えを優先事項にしていません。結果として、リソース、時間、オーナーシップの欠如が PQC への備えの妨げになっていると、回答者は答えています。
- 組織は、使用される暗号鍵の種類と特徴のインベントリを作成する必要があります。組織が暗号化資産の優先順位付けを行っていると答えた回答者は、37 パーセントにとどまっています。暗号化資産がオンプレミスとクラウドのどちらかにあるか、組織が把握していると答えた回答者は、36 パーセントとなっています。
- 組織は、企業全体に一貫して適用される一元的な暗号管理戦略を立て、その成功のための説明責任とオーナーシップを持つ必要があります。
- 暗号アルゴリズム、パラメータ、プロセス、およびテクノロジーをタイムリーに更新することと、重要な情報を量子コンピュータの脅威から保護するのに必要な暗号技術を持つことを、優先事項にする必要があります。
- 組織は暗号移行への適応能力を向上する必要があります。このような変更の背景には、アルゴリズム廃止や量子コンピュータなどがあります。有能な人材の不足は、新しいプロトコル、基準や、量子コンピュータの手法を含むセキュリティ脅威に対応するための妨げとなります。

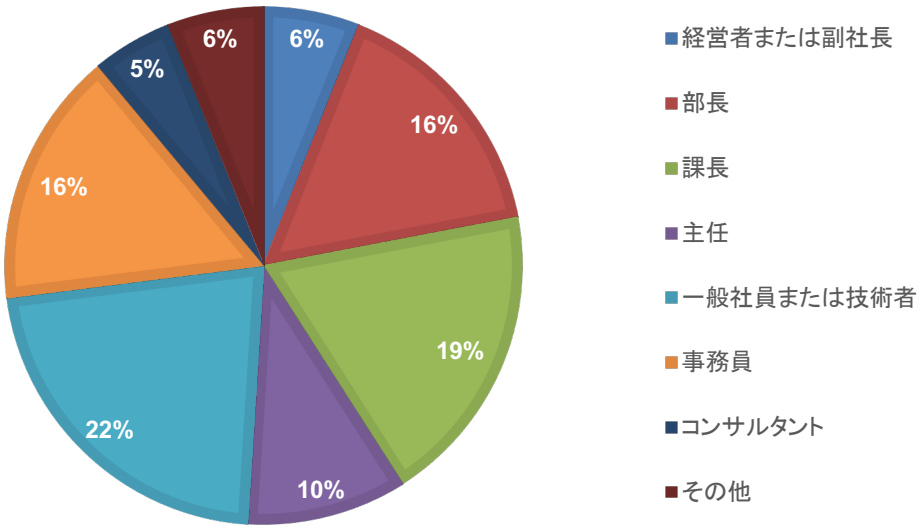
パート 3. 手法

この調査の参加者として、耐量子暗号に対する組織のアプローチについて知っている APAC の IT 管理者および IT セキュリティ管理者 12,565 人のサンプリング枠が選出されました。表 1 は、回答合計が 432 件であることを示しています。信頼性チェックにおいて、39 件の調査回答を取り除く必要がありました。最終的なサンプルは 393 件の調査回答で構成されました。回答率は 3.1 パーセントです。

表 1. サンプル回答	APAC
サンプリング枠	12,565
回答合計	432
却下またはスクリーニングされた調査回答	39
最終サンプル	393
回答率	3.1%

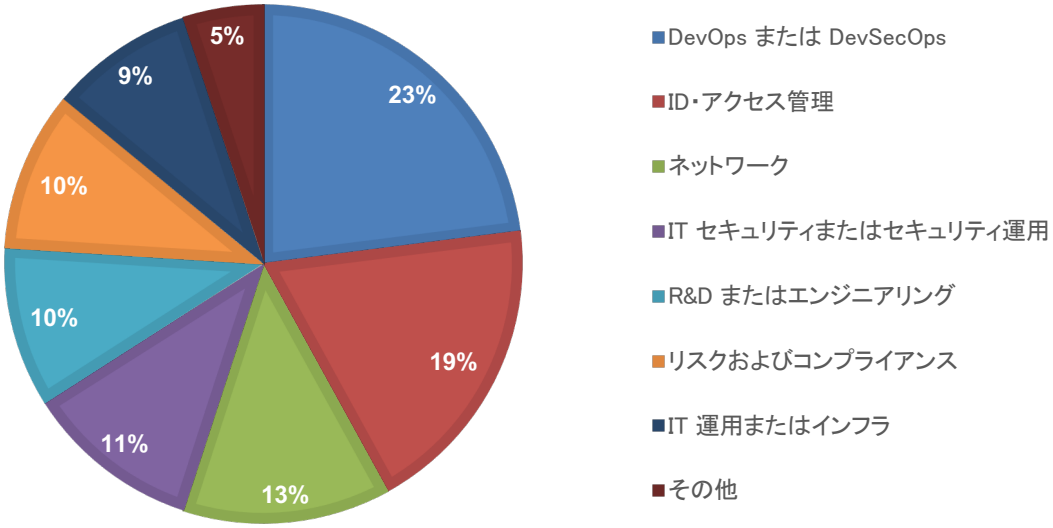
円グラフ 1 は、参加組織内の回答者の組織階層を示しています。意図的に、回答者の半数（51 パーセント）が管理層以上になっています。

円グラフ 1. 組織内での現在の役職



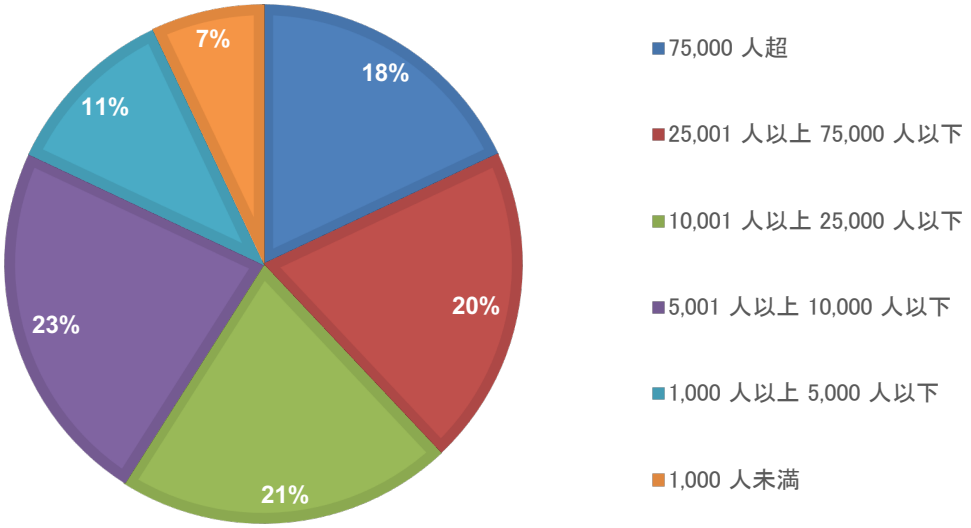
円グラフ 2 は、回答者が所属する部署またはチームを表しています。回答者の 23 パーセントが DevOps または DevSecOps に所属しています。これに続き、ID およびアクセス管理（回答者の 19 パーセント）、ネットワーク（回答者の 13 パーセント）、IT セキュリティまたはセキュリティ運用（回答者の 11 パーセント）、R&D またはエンジニアリング（回答者の 10 パーセント）、リスクおよびコンプライアンス（回答者の 10 パーセント）となっています。

円グラフ 2. あなたの部署またはチームを最も的確に表しているものはどれですか？



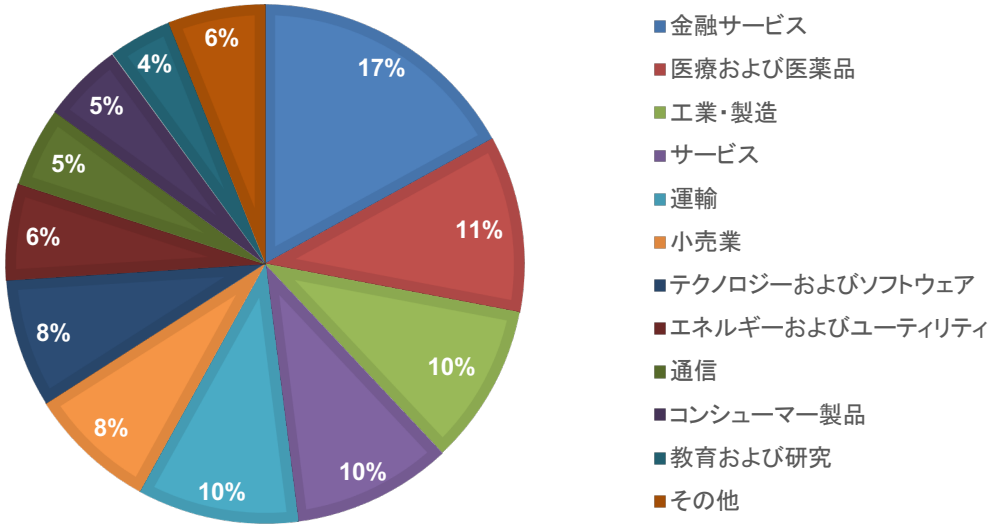
円グラフ 3 に示すように、回答者の 59 パーセントは、全世界の従業員数が 10,000 人を超える組織に所属しています。

円グラフ 3. 全世界のフルタイム従業員



円グラフ 4 は、回答者の組織の業種を示しています。このグラフでは、金融サービス（17 パーセント）が最多業種となっています。金融サービスには、銀行、投資管理、保険、証券、決済、クレジットカードが含まれます。これに続いて、医療および医薬品（回答者の 11 パーセント）、製造（回答者の 10 パーセント）、サービス（回答者の 10 パーセント）、運輸（回答者の 10 パーセント）、小売（回答者の 8 パーセント）となっています。

円グラフ 4. 主な業種



パート 4. この調査の注意事項

調査結果から推論を引き出す前に、調査に固有の制限事項について、慎重に考慮する必要があります。次の項目は、Web ベースのほとんどの調査と密接に関連する固有の制限事項です。

- 無回答バイアス：現在の調査結果は、調査回答のサンプルに基づいています。当社は、個人の代表サンプルに調査を送付し、有効な回答を多数得ました。無回答のテストを経たにもかかわらず、調査に回答しなかった個人は、調査に回答した個人とは基本的信条の点で本質的に異なっている可能性が常にあります。

- サンプリング枠バイアス：精度は、連絡先情報と、サンプルが耐量子暗号への自分の組織のアプローチについて知っている個人をどの程度代表しているかに基づきます。また、調査結果には、マスコミ報道など外部イベントのバイアスがかかる可能性があることも認めます。最後に、当社は Web ベースの回収方法を採用したため、郵送または電話による Web 以外の回答方法であれば、調査結果のパターンが異なっていた可能性もあります。

- 自己申告による結果：調査研究の品質は、対象者から受け取る機密の回答の完全性に基づきます。調査プロセスに一定の抑制と均衡が組み込まれることがありますが、対象者が正確な回答を提供しない可能性は常にあります。

パート 5. APAC の調査結果のまとめを含む付録

以下の表は、この調査に含まれるすべての調査質問への回答の度数、または度数のパーセンテージを示しています。すべての調査回答は 2023 年 8 月に収集されました。

耐量子コンピュータと耐量子暗号の状況

調査回答	APAC
サンプリング枠の合計	12,565
調査回答合計	432
調査回答の却下	39
最終サンプル	393
回答率	3.1%

S1. 耐量子暗号について、どの程度知っていますか？	APAC
よく知っている	44%
知っている	38%
少し知っている	18%
知らない（中止）	0%
合計	100%

S2. 耐量子暗号に対する組織のアプローチについて、あなたがどの程度、詳しいかを最も的確に表しているものはどれですか？	APAC
非常に詳しい	40%
詳しい	28%
少し詳しい	32%
詳しくない（中止）	0%
合計	100%

S3. 組織でのあなたの役職を最も的確に表しているものはどれですか？	APAC
最高情報セキュリティ責任者（CISO）	16%
最高情報責任者（CIO）	15%
IT セキュリティ担当副社長	18%
IT セキュリティ部長または課長	27%
セキュリティアーキテクト	9%
PKI（公開鍵基盤）エンジニア	8%
プロダクトマネージャー	7%
上記のいずれでもない（中止）	0%
合計	100%

パート 1. セキュリティ態勢の背景

Q1. あなたの組織の IT セキュリティ体制についてお伺いします。企業全体でのリスク、脆弱性、攻撃の軽減について、あなたの組織はどの程度、効果を発揮していると評価しますか？1 =「効果を発揮していない」から、10 =「非常に効果を発揮している」までの 10 段階で評価してください。	APAC
1 または 2	12%
3 または 4	18%
5 または 6	20%
7 または 8	32%
9 または 10	18%
合計	100%

Q2. あなたの組織は過去 12 か月以内にサイバー攻撃を 1 回以上受けたことがありますか？	APAC
はい	47%
いいえ	45%
わからない	8%
合計	100%

Q3.「はい」の場合、組織が受けた攻撃の種類を最も的確に表したものはどれですか？当てはまるものをすべて選択してください。	APAC
高度なマルウェアまたはゼロデイ攻撃	38%
API	42%
フィッシングまたはソーシャルエンジニアリング	43%
サービス拒否攻撃	35%
アカウントの乗っ取り	45%
クレデンシャル盗用	43%
ランサムウェア	47%
Web アプリケーション攻撃	23%
Web 媒介型攻撃	38%
デバイスの危殆化または窃盗	31%
悪意あるインサイダー	28%
高度なマルウェア	32%
その他（具体的に記述ください）	11%
合計	456%

Q4. 次の文に当てはまる評価を、以下の「強くそう思う」から「まったくそう思わない」までの項目の中から選択してください。	
Q4a.過去 12 か月で、私の組織が受けたサイバー攻撃は**標的がより明確化**されてきている。	APAC
強くそう思う	26%
そう思う	33%
わからない	18%
そう思わない	15%
まったくそう思わない	8%
合計	100%

Q4b. 過去 12 か月で、私の組織が受けたサイバー攻撃は**巧妙化**してきている。	APAC
強くそう思う	31%
そう思う	25%
わからない	21%
そう思わない	16%
まったくそう思わない	7%
合計	100%

Q4c. 過去 12 か月で、私の組織が受けたサイバー攻撃は、平均調査時間（MTTI）と平均収容時間（MTTC）の増加の点で**深刻化**してきている。	APAC
強くそう思う	30%
そう思う	23%
わからない	23%
そう思わない	15%
まったくそう思わない	9%
合計	100%

パート 2. 耐量子コンピュータ（PQC）への備えの状況

Q5. 組織が PQC への備えを固めるための猶予期間はどれぐらいだと思いますか？	APAC
5 年未満	39%
5 ～ 7 年	27%
8 ～ 10 年	14%
10 年超	11%
PQC の登場に間に合うように備えを固めるつもりはない	9%
合計	100%

Q6. PQC がセキュリティに及ぼす影響に対して組織が取り組む準備をしていないことを、あなたはどの程度、懸念していますか？1 =「懸念していない」から、10 =「非常に懸念している」までの 10 段階で評価してください。	APAC
1 または 2	7%
3 または 4	9%
5 または 6	26%
7 または 8	22%
9 または 10	36%
合計	100%

Q7. 高度な攻撃者が「harvest now, decrypt later」（今収集し、後で解読）攻撃を仕掛ける可能性があることについて、どの程度、懸念していますか？1 =「懸念していない」から、10 =「非常に懸念している」までの 10 段階で評価してください。	APAC
1 または 2	6%
3 または 4	5%
5 または 6	12%
7 または 8	32%
9 または 10	45%
合計	100%

Q8. 暗号アルゴリズム、パラメータ、プロセス、およびテクノロジーを更新し、量子コンピュータの手法を含むセキュリティ脅威に適切に対処することについて、あなたの組織はどの程度、効果を発揮していますか？1 =「効果を発揮していない」から、10 =「非常に効果を発揮している」までの 10 段階で評価してください。	APAC
1 または 2	15%
3 または 4	33%
5 または 6	25%
7 または 8	13%
9 または 10	14%
合計	100%
Q9. 重要な情報を量子コンピュータの脅威から保護するために必要な暗号技術をあなたの組織が持つことを、どの程度確信していますか？1 =「確信していない」から、10 =「強く確信している」までの 10 段階で評価してください。	APAC
1 または 2	19%
3 または 4	35%
5 または 6	23%
7 または 8	13%
9 または 10	10%
合計	100%

Q10. あなたの組織は量子コンピュータがセキュリティに及ぼす影響に取り組むための戦略を立てていますか？	APAC
はい、現時点で戦略がある	19%
今後 6 か月以内に戦略を立てる予定	34%
今後 1 年以内に戦略を立てる予定	26%
戦略を立てる予定はない	21%
合計	100%

Q11. あなたの組織の幹部は量子コンピュータがセキュリティに及ぼす影響について、どの程度認識していますか？	APAC
十分に認識している	16%
認識している	35%
少し認識している	30%
認識していない	19%
合計	100%

Q12. 耐量子の未来に備えるために業界標準化団体が実施している取り組みについて、あなたの組織はどの程度、知っていますか？	APAC
よく知っている	23%
知っている	32%
少し知っている	36%
知らない（Q14 に進んでください）	9%
合計	100%

Q13. 知っている場合、次の団体について詳しく知っていますか？当てはまるものをすべて選択してください。	APAC
米国商務省標準化技術研究所（NIST）の耐量子暗号プロジェクト	27%
米国科学アカデミーの「Quantum Computing: Progress and Prospects」レポート	31%
ANSI X9 の Quantum Risk Study Group	32%
The Quantum Safe Cryptography Group	23%
上記のいずれについてもよく知らない	19%
合計	132%

Q14. PQC への備えで主な課題となるのは何ですか？上位 **3 つ**を選択してください。	APAC
明確なオーナーシップの欠如	50%
未完成のアルゴリズム	38%
有能な人材の不足	43%
リソース（時間や資金）の不足	52%
管理ツールの不足または断片化	30%
PQC の影響に関する不確実性	45%
経営者レベルのサポートの不足	33%
その他（具体的に記述ください）	9%
合計	300%

Q15. 耐量子コンピュータに備えるために、組織はどのような対策を講じていますか？当てはまるものをすべて選択してください。	APAC
暗号化資産のインベントリ作成と優先順位付け	37%
データ保持要件の理解	44%
データと暗号化資産がオンプレミスとクラウドのどちらにあるかについての判断	36%
使用される暗号鍵の種類と特徴のインベントリの作成	51%
その他（具体的に記述ください）	8%
上記の対策のいずれも講じていない	30%
合計	206%

Q16. あなたの組織は CCOE を設置済みですか？	APAC
はい、暗号に関する指導、調査、実装戦略、オーナーシップ、ベストプラクティスを提供する成熟した CCOE を設置済みである	26%
はい、しかし CCOE はまだ発展途上である	28%
いいえ、しかし今後 6 か月以内に CCOE を設置する予定である	19%
いいえ、CCOE を設置する予定はない	27%
合計	100%

パート 3. 暗号化に備える能力

Q17. あなたの組織には、一元的な全社規模の暗号管理戦略がありますか？	APAC
企業全体に一貫して適用される、全面的に一元化された暗号管理戦略がある	40%
特定のアプリケーションまたはユースケースに適用される、限られた一元的な暗号管理戦略がある	37%
一元的な暗号管理戦略はない	23%
合計	100%

Q18. 公開鍵基盤、鍵、証明書、その他のシークレットの実装を推進する最も重要なトレンドは上位 3 つは何だと思いますか？**回答を 3 つ**だけ選択してください。	APAC
規制またはコンプライアンス要件	42%
モバイルデバイス（例：BYOD、モバイルデバイス管理）	33%
リモート従業員（例：VPN、多要素認証）	41%
IoT（モノのインターネット）デバイス	32%
ソフトウェアサプライチェーンセキュリティ	40%
DevOps または DevSecOps（例：コード、コンテナ、サービスメッシュ）	50%
クラウドベースのサービス	36%
ゼロトラストセキュリティ戦略	19%
その他（具体的に記述ください）	7%
合計	300%

Q19. あなたの組織内でデジタルセキュリティの戦略上の**最重要**事項は何ですか？**回答を 4 つ**だけ選択してください。	APAC
暗号移行の俊敏性	53%
特権アクセス管理（PAM）	38%
規制の遵守	35%
職場における未知の鍵と証明書（つまり、シャドー IT）のリスクの低下	31%
鍵と証明書の有効期間の把握	44%
デジタルセキュリティの状況を強化するテクノロジーへの投資	47%
有能な人材の採用と定着への投資	56%
IT インフラの複雑さの低減	45%
IoT デバイスの認証と制御	45%
その他（具体的に記述ください）	6%
合計	400%

次の文に当てはまる評価を、以下の「強くそう思う」から「まったくそう思わない」までの項目の中から選択してください。	
Q20. 私の組織が実装する暗号鍵と電子証明書の数は増えている。	APAC
強くそう思う	33%
そう思う	25%
わからない	22%
そう思わない	16%
まったくそう思わない	4%
合計	100%

Q21. 暗号鍵と電子証明書の使用の増加により、私の組織のチームにかかる運用の負担が大幅に増えた。	APAC
強くそう思う	34%
そう思う	26%
わからない	21%
そう思わない	14%
まったくそう思わない	5%
合計	100%

Q22. 私の組織は、所有している鍵と証明書（自己署名を含む）の正確な数を把握していない。	APAC
強くそう思う	29%
そう思う	34%
わからない	20%
そう思わない	11%
まったくそう思わない	6%
合計	100%

Q23. 私の組織は、SSL/TLS 証明書の有効期間の短縮によって生じるワークロードと機能停止リスクの増加について懸念している。	APAC
強くそう思う	23%
そう思う	32%
わからない	21%
そう思わない	8%
まったくそう思わない	16%
合計	100%

Q24. 私の組織では、鍵と証明書の設定ミスについての懸念が高まっている。	APAC
強くそう思う	29%
そう思う	32%
わからない	15%
そう思わない	15%
まったくそう思わない	9%
合計	100%

Q25. 私の組織は、暗号変更（例えば、アルゴリズム廃止や量子コンピュータなど）への適応能力について懸念している。	APAC
強くそう思う	28%
そう思う	32%
わからない	15%
そう思わない	14%
まったくそう思わない	11%
合計	100%

以下は、組織が情報資産と IT インフラを保護するために暗号化ソリューションおよび手法を効果的に実装することに関連する固有の能力です。次の 10 段階の評価基準を使用して、組織の能力を評価してください。1 =「能力が低い」、10 =「能力が高い」です。

Q26a. すべての証明書や鍵を検出し保護する能力	APAC
1 または 2	20%
3 または 4	15%
5 または 6	19%
7 または 8	35%
9 または 10	11%
合計	100%

Q26b. 計画外の証明書を防止する能力	APAC
1 または 2	23%
3 または 4	21%
5 または 6	31%
7 または 8	12%
9 または 10	13%
合計	100%

Q26c.アルゴリズムや侵害を修復する能力	APAC
1 または 2	19%
3 または 4	23%
5 または 6	25%
7 または 8	20%
9 または 10	13%
合計	100%

Q26d.証明書や鍵の不正使用を検知し対応する能力	APAC
1 または 2	23%
3 または 4	23%
5 または 6	16%
7 または 8	22%
9 または 10	16%
合計	100%

Q26e.ビジネスニーズの増加による鍵と証明書をスケーリングする能力	APAC
1 または 2	17%
3 または 4	16%
5 または 6	20%
7 または 8	33%
9 または 10	14%
合計	100%

Q26f.全社規模のベストプラクティスとポリシーを推進する能力	APAC
1 または 2	21%
3 または 4	16%
5 または 6	23%
7 または 8	26%
9 または 10	14%
合計	100%

Q26g.公開鍵基盤と暗号に熟練した従業員を引きつけ、定着させる能力	APAC
1 または 2	18%
3 または 4	17%
5 または 6	20%
7 または 8	28%
9 または 10	17%
合計	100%

Q26h.ハイブリッド、マルチクラウド環境、DevOps、ゼロトラストなどの新しいイニシアチブを確立する能力	APAC
1 または 2	19%
3 または 4	18%
5 または 6	16%
7 または 8	28%
9 または 10	19%
合計	100%

パート 4. 予算

Q27. 2023 年の IT セキュリティの予算総額は？	APAC
100 万ドル未満	0%
100 万ドル ～ 500 万ドル	8%
600 万ドル ～ 1,000 万ドル	13%
1,100 万ドル ～ 1,500 万ドル	12%
1,600 万ドル ～ 2,000 万ドル	23%
2,100 万ドル ～ 2,500 万ドル	21%
2,600 万ドル ～ 5,000 万ドル	14%
5,100 万ドル ～ 1 億ドル	9%
1 億ドル超	0%
合計	100%
挿入値	23.93 ドル

Q28. 暗号管理に割り当てられる予算は、IT セキュリティの総予算の何パーセントですか？	APAC
1% ～10%	31%
11% ～ 25%	34%
25% 超	35%
合計	100%

Q29. 証明書の管理と保護に割り当てられる予算は、何パーセントですか？	APAC
1% ～10%	31%
11% ～ 25%	42%
25% 超	27%
合計	100%

Q30. あなたの組織は、耐量子コンピュータに備えるために、何らかの予算を割り当てていますか？	APAC
はい、現在、予算を割り当てている	32%
はい、今後 6 か月以内に予算を割り当てる予定	29%
はい、今後 1 年以内に予算を割り当てる予定	19%
いいえ、予算を割り当てる予定はない	20%
合計	100%

パート 5. 組織と回答者の人口統計

D1. 組織内でのあなたの職位を最も的確に表しているものはどれですか？	APAC
経営者または副社長	6%
部長	16%
課長	19%
主任	10%
一般社員または技術者	22%
事務員	16%
コンサルタント	5%
その他（具体的に記述ください）	6%
合計	100%

D2. あなたの部署またはチームを最も的確に表しているものはどれですか？	APAC
IT セキュリティまたはセキュリティ運用	11%
IT 運用またはインフラ	9%
ID およびアクセス管理（IAM）	19%
R&D またはエンジニアリング	10%
ネットワーク	13%
リスクおよびコンプライアンス	10%
DevOps または DevSecOps	23%
その他（具体的に記述ください）	5%
合計	100%

D3. あなたの組織の全世界のフルタイム従業員の人数に当てはまるものはどれですか？	APAC
1,000 人未満	7%
1,000 人以上 5,000 人以下	11%
5,001 人以上 10,000 人以下	23%
10,001 人以上 25,000 人以下	21%
25,001 人以上 75,000 人以下	20%
75,000 人超	18%
合計	100%
挿入値	31,065

D4. あなたの組織の主な業種を最も的確に表しているものはどれですか？	APAC
農業・外食産業	0%
通信	5%
コンシューマー製品	5%
教育および研究	4%
エネルギーおよびユーティリティ	6%
金融サービス	17%
医療および医薬品	11%
工業・製造	10%
小売業	8%
サービス	10%
テクノロジーおよびソフトウェア	8%
運輸	10%
その他（具体的に記述ください）	6%
合計	100%

この調査の詳細については、research@ponemon.org まで E メールで、または 1.800.887.3118 までお電話でお問い合わせください。

Ponemon Institute

責任ある情報管理の推進

Ponemon Institute 社は、企業と政府機関内で責任ある情報およびプライバシー管理の慣行を推進する独立した調査と教育に力を尽くしています。当社の使命は、人と組織に関する機密情報の管理とセキュリティに影響を及ぼす重要な問題について、高品質の実証的調査を実施することです。

当社は、厳格なデータの機密性、プライバシー、および調査の倫理基準を遵守します。当社は、個人から、本人を識別できる情報（または当社のビジネス調査で会社を識別できる情報）は一切収集していません。さらに、当社は厳格な品質管理基準を定めており、基準外、無関係、または不適切な質問を対象者に尋ねることはありません。