pwc

新しい世界、新しいルール：不確実性の時代におけるサイバーセキュリティ

「Global Digital Trust Insights 2026」：
CxOプレイブックおよび調査結果

www.pwc.com/jp

60%

地政学的な不安定化を受けてサイバーセキュリティ投資を増額する組織は全体の60%

6%のみ

調査対象に含まれる全てのデータリスク対策を完全に実行しているのは6%のみ

Top 2

サイバーディフェンスにAIを実装する際の課題のトップ2は、ノウハウとスキルのギャップ

サイバーセキュリティは未知の領域に踏み出そうとしています。ここ数年におけるテクノロジーの飛躍的な進化を受けて、世界秩序と脅威環境が急速に変化する中、サイバーセキュリティ戦略の真価が問われています。

組織はポストグローバリゼーション時代の新常態に直面しています。それを特徴付けるのは、同盟関係の亀裂、国際機関の弱体化、関税の大幅な引き上げ、サプライチェーンの混乱です。私たちは今日、前例のない技術発展がもたらすアタックサーフェスの拡大や、サイバーセキュリティに関する新たな脅威の登場を目の当たりにしています。これらの多くは国家の支援を受けたものです。

このように不確実性が増大する中で、企業のリーダーは、自社の能力、人材、技術の再評価を避けて通ることはできません。すなわち、サイバーセキュリティ戦略の根本的な再検討を迫られているのです。その中には、活動拠点をどこに置くか、誰を相手に事業を行うかも含まれます。

世界72カ国のビジネスリーダーおよびテクノロジーリーダー計3,887名を対象にPwCが実施した年次調査「Global Digital Trust Insights 2026」では、企業のリーダーが、この不確実な時代にどのように対処しているのか、対応が不十分なのはどの分野か、そして、課題にもっと効果的に対処するには何を変えていけば良いのかを明らかにしています。主な調査結果は以下のとおりです。

- **地政学的リスクが戦略の立案に影響：**ビジネスリーダーとテクノロジーリーダーの60%が、地政学的な不確実性の増大を受けて、重点戦略の上位3項目の1つにサイバーセキュリティリスクへの投資を位置付けています。
- **レジリエンス強化の取り組みはいまだ道半ば：**リーダーの約半数は、現在の地政学的情勢に鑑みれば、組織における特定の脆弱性をターゲットにしたサイバー攻撃に対して、自社組織は「ある程度耐性がある」と回答しています。調査において、組織の脆弱性に関連する全調査項目について自信があると回答したのは、全体の6%に過ぎません。
- **トラブルへの備え：**未然防止策（モニタリング、アセスメント、テスト、セキュリティ管理策など）への支出が事後対応策（インシデント対応、罰金、復旧）への支出を大幅に上回っている組織は、全体の24%にとどまります。支出割合としては、前者が後者を上回ることが理想ですが、大半の企業（全体の67%）では、両者がほぼ拮抗しています。理想的な支出割合と比べて、結果的によりコストやリスクが増大する可能性があります。
- **サイバーディフェンスに自律型AIを活用：**自律型AIは、今後12カ月間において、各組織が最も重視するセキュリティにおけるAI活用の1つです。優先項目の中でも、特にクラウドセキュリティ、データ保護、サイバーディフェンスとその運用を目的とする自律型AIの導入計画が進められています。

- **刻々と迫る量子コンピューティングの実現：**量子コンピューティングは、組織的な対応態勢が整っていない脅威のトップ5に入っています。しかし、優先的に予算を配分している組織は全体の10%を下回り、調査対象とした主要な量子耐性対策が全て実行されている組織は全体の3%に過ぎません。
- **深刻化するサイバーセキュリティ人材不足への対応策の再検討：**サイバーセキュリティ対策を進めるにあたり、依然として、スキルの不足が障害の1つとなっています。半数を超える（53%）組織が、能力のギャップを埋める手段として、AIを重視しています。また、専門的なマネージドサービスが専門性と規模を確保するための戦略的なアクセラレーターとなりつつあります。

現状に対応するには、緊急性について再認識するとともに、創造性を高め、従前とは異なるアプローチを取る必要があります。漫然と事業を継続すれば良いとの意識は改めていかねばなりません。PwCが取りまとめた2025年版のCxOプレイブックでは、調査結果を実践的な手順として提示することにより、主要なステークホルダーのサイバーセキュリティプラクティスの基盤強化が進展すること、そして、この新しい環境に適合する未来志向の対策が促進されることを目指しています。

目次

01

リスクと脅威の状況

地政学的情勢の変化に伴うサイバーセキュリティの脆弱性の変容

60%

不安定化する地政学的情勢を受けてサイバーセキュリティ投資を増額する組織は全体の60%

6%のみ

現在の地政学的情勢を踏まえた上で、調査対象の全ての脆弱性について、それらを狙ったサイバー攻撃に「十分対処できる」組織は6%のみ

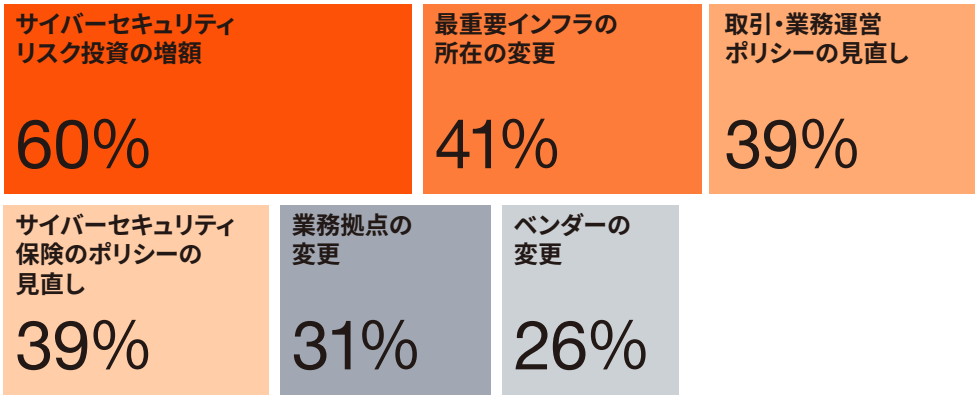
Top 2

組織において最も対策が遅れているサイバーセキュリティ上の2大脅威は、クラウドとコネクテッド製品への攻撃

現在の地政学的情勢は、サイバーセキュリティリスクの形成に対し、破壊的なテクノロジーに劣らぬくらいの影響を及ぼしています。新時代を迎えた現在の戦略的競争関係においては、同盟関係の崩壊、通商摩擦、国際機関の弱体化など、安定を阻害するさまざまな要因が新たな脅威環境を形作っているため、これまでのビジネスの在り方を変化させることが必要になりつつあります。

このような地政学的情勢を受けて、ビジネスリーダーとテクノロジーリーダーの60%が、今後12カ月間における優先項目のトップ3の1つとして、サイバーセキュリティリスク投資の増額を挙げています。それ以外にも、優先的に見直しを進める事項として、重要インフラの所在（41%）、取引や業務運営ポリシー（39%）、サイバーセキュリティ保険のポリシー（39%）を挙げています。破壊的な脅威が日常化した今日、レジリエンスを確保する方策として、サイバーセキュリティ戦略の強化は避けて通ることができません。

現在の地政学的情勢に応じたサイバーセキュリティ戦略の優先項目
（トップ3に挙げたリーダーの割合）

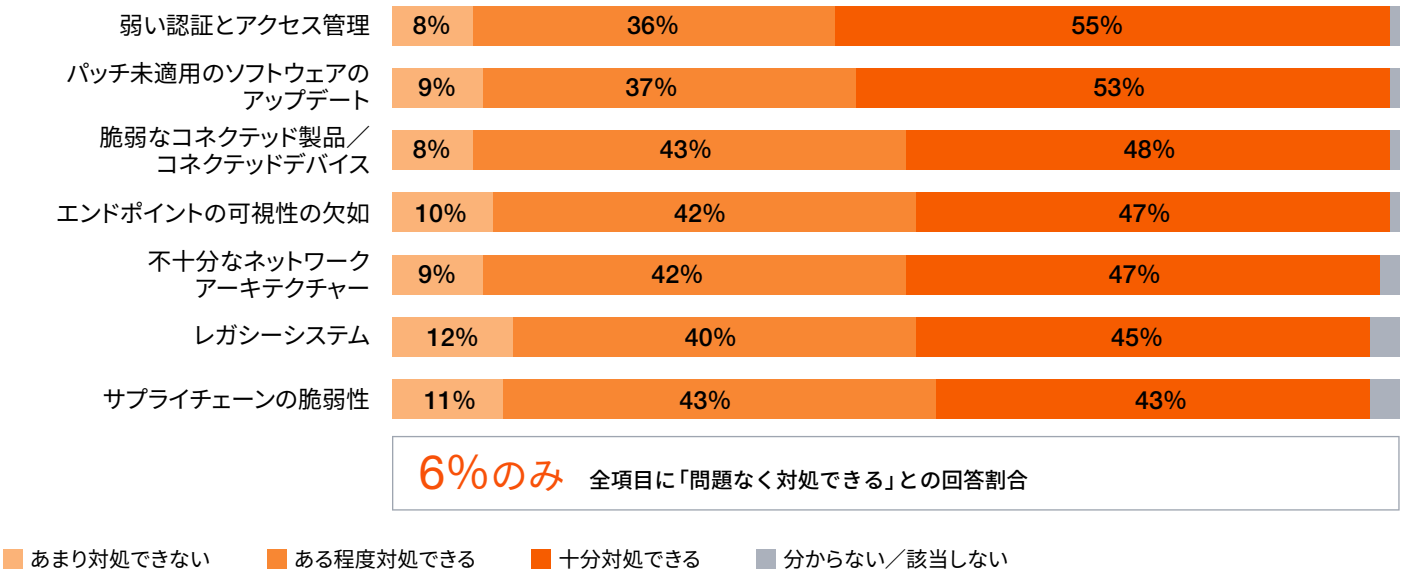


質問2　現在の地政学的情勢を踏まえて、今後12カ月間に、あなたの組織でサイバーセキュリティ戦略の見直しを行う分野を以下から選択してください。 調査ベース：全回答者（3,887）
出所：PwC「Global Digital Trust Insights 2026」

「安全と感じる」か、「安全である」か

現在の地政学的情勢を念頭に置いた場合、サイバー面での備えに対する自信の在り方は二分されています。回答者の約半数は、今回の調査対象の脆弱性を狙ったサイバー攻撃を受けた場合でも、自社組織が「十分な耐性を備えている」としています。他方で、同程度の割合の組織がこのような準備が整っていないと回答しています。さらには、調査対象の全ての脆弱性について問題なく対処できると回答した組織はわずか6%しかありません。レガシーシステムやサプライチェーンの脆弱性は最たる弱点の1つで、重要インフラの混乱を目論む国家のアクターによる頻繁な攻撃にさらされ続けています。

組織の脆弱性を狙った主なサイバー攻撃への耐性



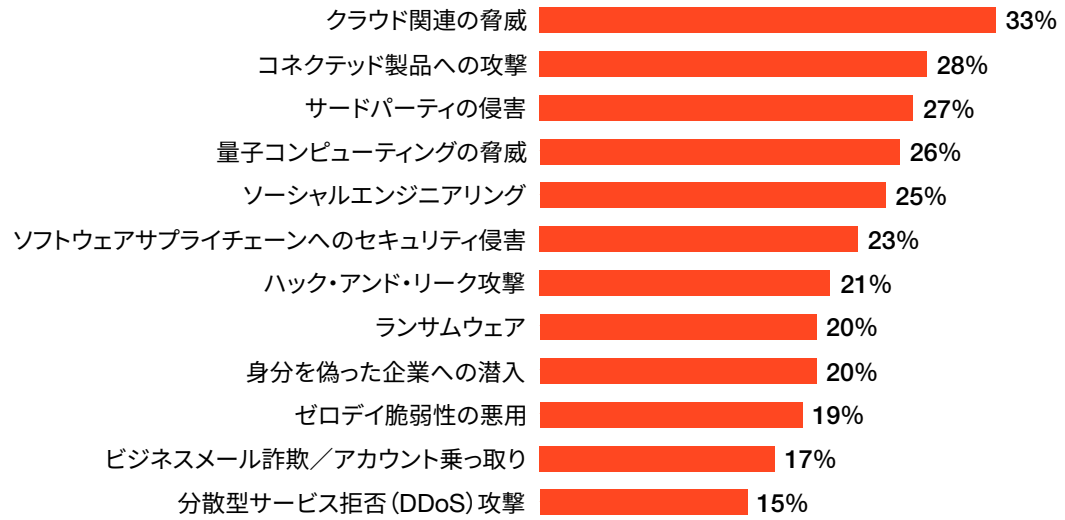
質問3　現在の地政学的情勢を踏まえた上で、次のような脆弱性を狙って大規模サイバー攻撃を受けた場合、あなたの組織にはどの程度の耐性がありますか。
調査ベース：セキュリティリーダー、COO、事業運営担当役員（1,971）
出所：PwC「Global Digital Trust Insights 2026」

埋まらないギャップ、増大するリスク

上記の脆弱性以外にも、特定のタイプの脅威に対する備えについて、組織のリーダーは懸念を持っています。前回の調査と同様に、最大の懸念事項はクラウドとコネクテッド製品への攻撃で、リーダーのおよそ3分の1が、この2つを自社組織で最も準備が遅れているサイバーセキュリティ脅威のトップ3に挙げています。

このようなリスクは目新しいものではありません。しかし、AIを活用する攻撃者が攻撃の限界を押し広げていることもあり、ガバナンス、管理、可視性における根本的なギャップを解消する上でこれらのリスクは依然として課題となっています。技術やエコシステムが一層複雑化するにつれて、多くの組織は、特にサードパーティやサプライチェーンへの依存関係全般で後れを取らぬよう懸命に努力しています。

組織において最も準備が遅れているサイバーセキュリティ脅威
（脅威の上位3項目のパーセンテージ）



質問1　今後12カ月間において、あなたの組織で最も対応準備が遅れているサイバーセキュリティ脅威はどのようなものですか？
調査ベース：セキュリティリーダー（1,740）
出所：PwC「Global Digital Trust Insights 2026」

失敗を通じて学習

CxOの4分の1以上が、過去36カ月間で最も甚大な被害をもたらしたデータ漏洩のコストは100万米ドルを下らなかったと言っています。最も被害を受けた企業は、売上高50億米ドル以上の企業（41%）、米国を拠点とする企業（37%）、そして、テクノロジー・メディア・情報通信業界の企業（33%）です。このような企業は、規模が大きく事業内容が複雑なことから、インシデントのコストが高額化しがちです。

過去に重大な攻撃を経験した組織は、大きな出費を通じて学び取った経験を行動に活かしています。このような組織は、他と比べて、より高い割合で（88%、全体では78%）サイバーセキュリティ予算の増額に取り組んでいます。また、重大なスキルの不足を補うためにマネージドサービスを採用する組織の割合も他を上回っています（48%、同39%）。さらに、このような組織には、サイバーセキュリティ保険契約の見直しを行う傾向（49%、同39%）がより強くみられますが、保険料の上昇や保険引受条件の厳格化も背景にあるのかもしれません。こうした組織の多くは、データ最小化の実践を組織全体に根付かせる取り組みを進めています。

02

サイバーセキュリティ戦略と運用

投資と効果の調和を図る

24%のみ

サイバーセキュリティ対策において、未然防止目的の支出額が事後対応目的を大幅に上回る組織は24%のみ

78%

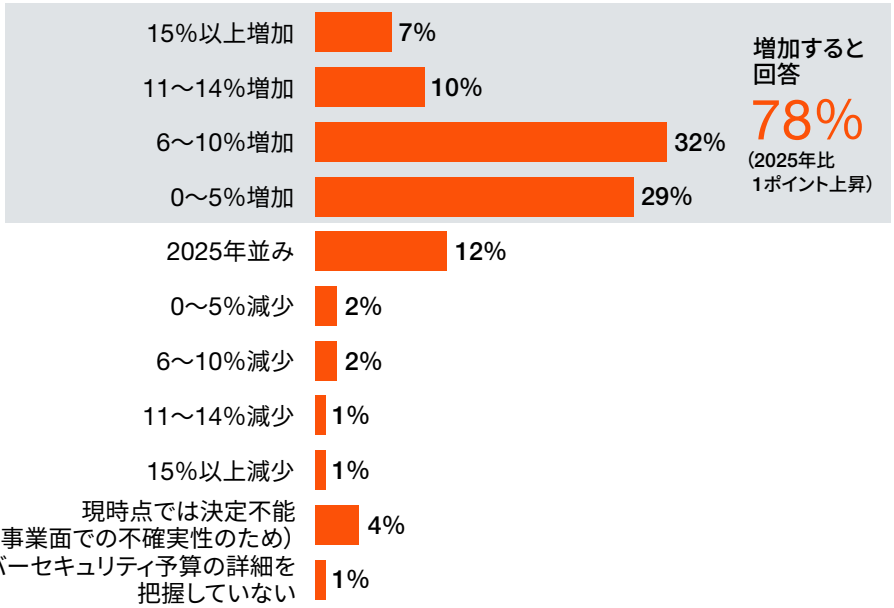
2026年のサイバーセキュリティ予算の増額を見込む組織は78%

わずか16%

サイバーセキュリティリスクがもたらす財務上の影響について、相当程度の見積りができている組織は全体のわずか16%

各組織におけるサイバーセキュリティ予算は、時流に沿った内容になっているでしょうか。回答者のおよそ8割（78%）が、2026年にはサイバーセキュリティ予算を増額するとしています。しかし、実際のところ、この数字は2025年（77%）からほとんど変化していません。回答者は、現在の地政学的情勢を受けて、サイバーセキュリティリスク投資を増額するとしていますが、そのためには、他の重要な支出項目の削減が必要になるかもしれません。

2026年におけるサイバーセキュリティ予算の対2025年比較



質問8　あなたの組織の2026年のサイバーセキュリティ予算は、2025年比でどうなりますか？
調査ベース：セキュリティリーダー、CFO、財務担当役員（2,027）
出所：PwC「Global Digital Trust Insights 2026」

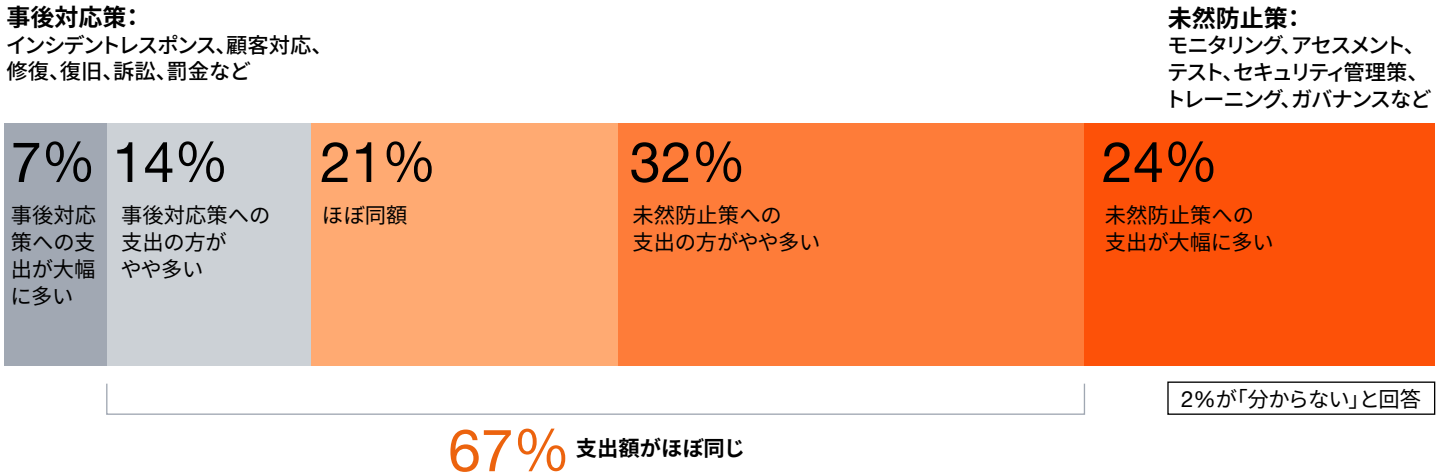
未然防止のコストと事後対応のコスト

サイバーセキュリティにおいて重要なのは、準備です。すなわち、危機に直面する**前に**先手を打って計画を立て、モニタリング、アセスメント、テスト、セキュリティ管理策、トレーニングといった未然防止策への投資を行うことです。これに代わる主な手段は事後対応策（例：インシデントレスポンス、顧客対応、修復、復旧、訴訟、罰金）ですが、未然防止策よりコストとリスクが増し、持続可能ではありません。

今回調査した組織の3分の2（67%）は、未然防止策と事後対応策に投じるコスト比率がほぼ同程度であると回答しています。すなわち、サイバーセキュリティ対策として、未然防止と事後対応への支出がほぼ同水準であるか、いずれかが若干多い程度ということです。最適な投資（事後対応目的よりも未然防止策への投資割合が著しく高い）を実行している組織はあまり多いとは言えません（全体の24%）。こうしたデータでは、事後対応に付随するコストが過小評価されている可能性があります。未然防止を目的とする支出はセキュリティリーダーの予算の範疇にあり、容易に追跡することができます。他方、事後対応に伴うコストは、法務、広報、営業、IT、製品、マーケティング、政府対応など組織全体に及び、さらには機会損失や企業イメージの悪化など、定量化が困難なコストも含まれます。

なお、未然防止策の実効性は、適切なリスクに照準を定め、状況の変化に機敏に追随できて初めて担保されるものです。強固な準備のためには、リスクや脅威の状況について深く理解する必要があり、その理解により得られた情報が、当該企業のサイバーセキュリティ戦略、雇用する従業員、企業が採用するプロセス、システム、ツールに活かされます。

事後対応策と未然防止策に係る支出



質問13　あなたの組織のサイバーセキュリティ対策では、事後対応策と未然防止策のどちらにより多くのリソースを充当していますか？ 調査ベース：全回答者（3,887）
出所：PwC「Global Digital Trust Insights 2026」

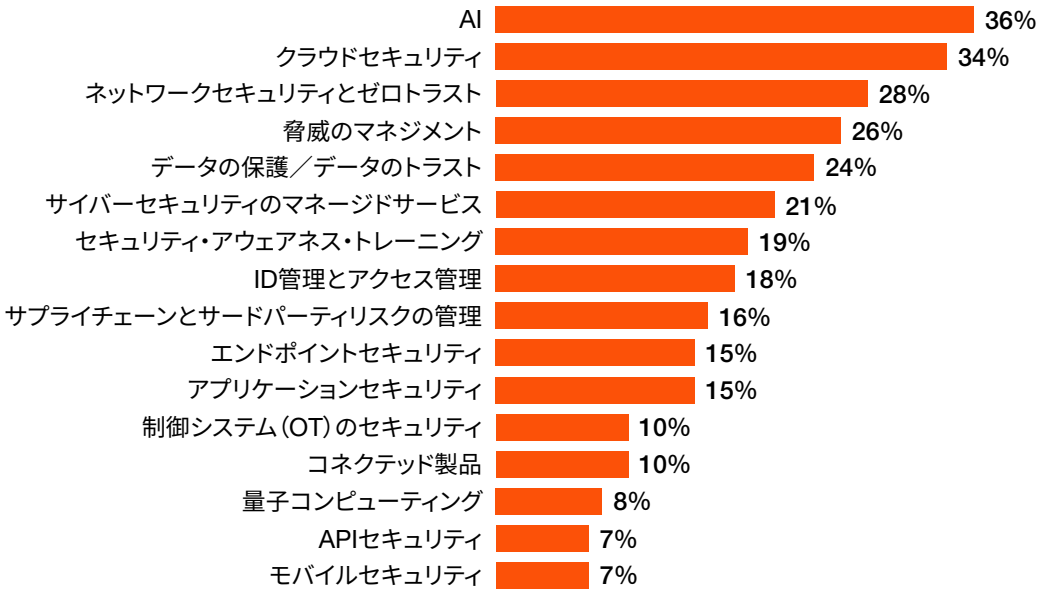
準備志向の優先投資項目の計画

AIとクラウドのセキュリティ確保は、2026年のサイバーセキュリティ予算における2大優先項目です。これは驚くにはあたりません。前述のとおり、クラウドは準備の遅れをリーダーが実感している脅威の最上位に位置しています。リスクと準備状況の間に存在するギャップに関する認識は広まってきており、これに応じた投資もなされるようになっています。

それでも、全体として十分な現状認識がなされているとは言えません。クラウドの次に各組織で準備の遅れを実感している分野としてコネクテッド製品への攻撃がありますが、この対応に予算を配分している組織ははるかに少ないのです。このようなミスマッチの存在から、脅威の火種がいまだ飛び交っている状態であることがうかがえます。

サイバーセキュリティのマネージドサービスにも、多くの組織が優先的に資金を振り分けています。例えば、高成長を遂げている企業では、さらなる成長手段としてマネージドサービスを活用しており、こうした企業の30%が優先投資対象の上位3項目にマネージドサービスを挙げています。このことは、外部の専門ノウハウを活用して、サイバーセキュリティへの準備状況における重大なギャップを解消しようとする戦略的な動きを反映するものです。

サイバーセキュリティ予算の配分にあたり、各組織で優先的に投資する分野
（上位3項目に挙げた組織の割合）

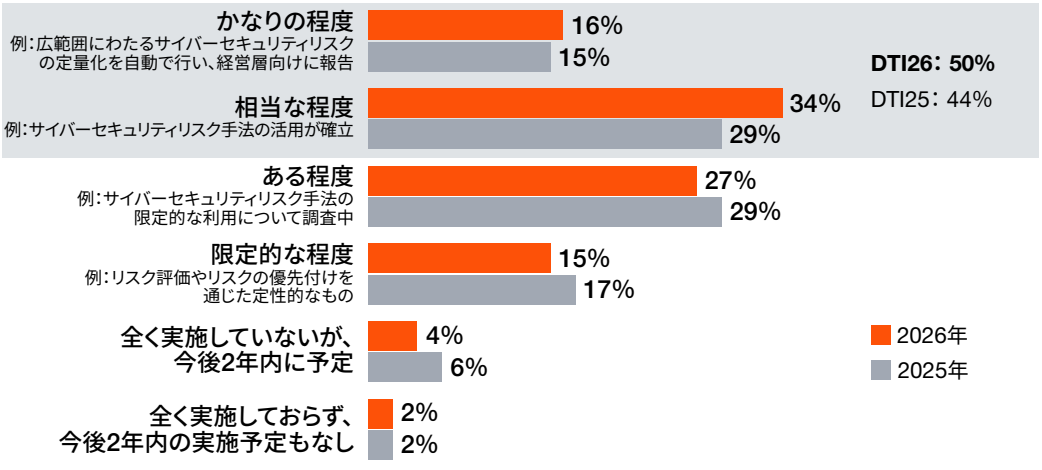


質問9　あなたの組織で今後12カ月間に実施するサイバーセキュリティ予算において、優先配分する投資分野を以下から挙げてください。 調査ベース：セキュリティリーダー（1,740）
出所：PwC「Global Digital Trust Insights 2026」

サイバーセキュリティリスクを定量化する

より多くの組織でリスクの定量化が進められています。今回の調査では、サイバーセキュリティリスクを定量化して、財務上の影響をかなりの程度（または相当な程度）まで計測していると回答した組織が全体の半数に上り、2025年の44%から増加しています。しかし、もう少し掘り下げてみると、「かなりの程度」計測している組織は16%にとどまります。ビジネスリーダーが必要としているものは、信頼性が高く、行動につなげられるような**サイバーセキュリティリスク報告から得られる知見**です。すなわち、それらに基づいて、組織が直面する脅威を評価し、最善の対処法を判断できるものです。

サイバーセキュリティリスクによる財務上の影響に関する計測



質問12　あなたの組織では、サイバーセキュリティリスクが及ぼす可能性のある財務上の影響について、現時点でどの程度まで計測（すなわち、リスクの定量化）していますか？ 調査ベース：セキュリティリーダー、CFO、CEO、CRO、取締役（2,673）。2025年調査：セキュリティリーダー、CFO、CEO、CRO、取締役（2,570）
出所：PwC「Global Digital Trust Insights 2026」

03

サイバーセキュリティにおけるAIの活用

「期待」が「優先」に変わるまで

AIへの投資

セキュリティリーダーが最優先で取り組むサイバーセキュリティ投資はAI

脅威ハンティング

AIを活用したセキュリティ機能のうち、セキュリティリーダーが最も重視するのは脅威ハンティング

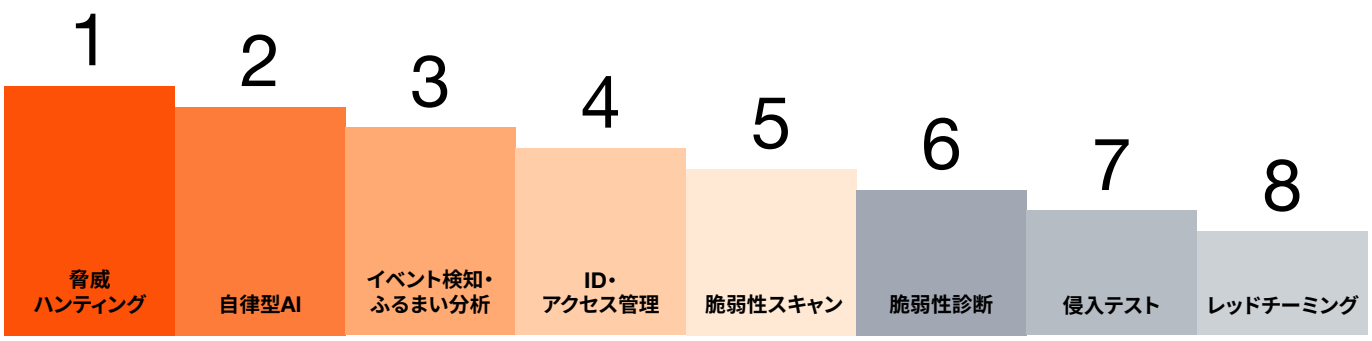
Top 3

自律型AI活用3大優先分野は、クラウドセキュリティ、データ保護、サイバーディフェンス

AIがサイバーセキュリティ機能を大幅に変革する可能性を有していることは誰の目にも明らかで、その影響は広範囲に及びます。PwCが実施した調査において、いくつかのカテゴリでAIが最上位に挙げられているのは、このような背景があるからです。マネージド・サイバーセキュリティ・サービスの活用や、サイバーセキュリティ人材のギャップへの対処を通じて、サイバーセキュリティの主要機能をAIによって強化することは、この分野の予算配分における最優先項目です。

AIを活用したサイバーセキュリティ機能の強化に向けて、セキュリティリーダーが今後12カ月間で取り組む最優先項目に挙げるのは脅威ハンティングです。また、自律型ソリューション、イベント検知・ふるまい分析、ID・アクセス管理、脆弱性スキャンや脆弱性診断などの機能向上も進められています。

自律型AIは、AIによるセキュリティ機能に関する最優先項目の1つ
（最優先項目に位置付けた回答数に基づく順位）



質問18　AIのセキュリティ機能のうち、あなたの組織が今後12カ月間で優先的に取り組むものを、以下の項目から挙げてください。調査ベース：セキュリティリーダー（1,740）
出所：PwC「Global Digital Trust Insights 2026」

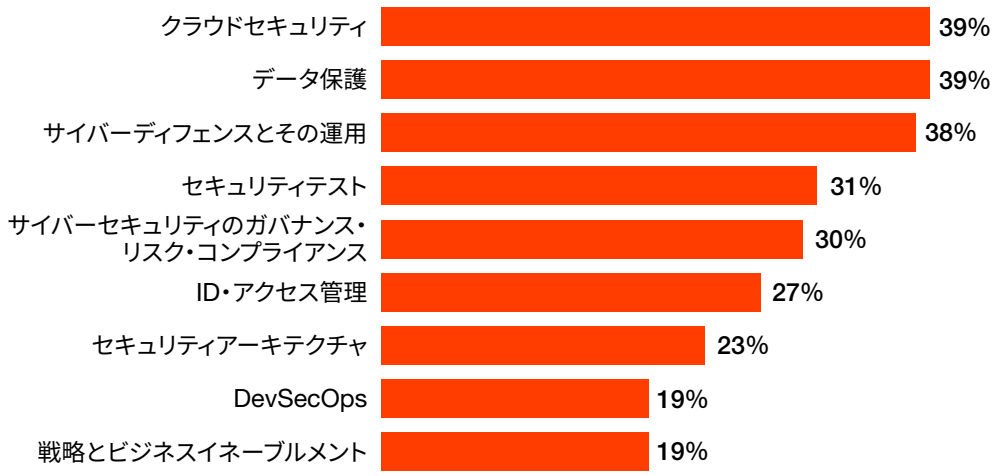
サイバーディフェンスを変革する自律型AI

自律型AIは、人間が限定的に介入するだけでタスクを実行できる自律型かつ目標達成型のシステムです。ビジネス界は、この自律型AIが各社のサイバーセキュリティ計画を変革する途方もないポテンシャルを秘めていることに気付き始めています。もはや分析に役立つツールの域を超えて、このようなAIシステムは、デジタルアシスタントとして自律的に動作し、人間のチームと協働し、さらにはセキュリティ対応を開始できるまでに進化を遂げ、効率と生産性の改善に貢献しています。

このような事情もあって、セキュリティリーダーは、AIによるセキュリティ機能に関して今後12カ月間に組織として最優先で取り組む項目の1つに、自律型AIを挙げているのです。

セキュリティリーダーは、このような自律型ソリューションをどのような場面に導入しようとしているのでしょうか。自律型AIにおいて、クラウドセキュリティ、データ保護、サイバーディフェンスとその運用は、2026年のセキュリティの最優先分野とされています。これ以外の優先分野としては、セキュリティテスト、サイバーセキュリティのガバナンス・リスク・コンプライアンス（GRC）、ID・アクセス管理などがあります。

効率と生産性の改善を目的とする自律型AIの優先項目
（上位3項目に挙げた組織の割合）



質問19　あなたの組織が、効率と生産性の改善を図るにあたって、自律型AIを活用して今後12カ月間で優先的に取り組む分野を以下の項目から挙げてください。調査ベース：セキュリティリーダー（1,740）
出所：PwC「Global Digital Trust Insights 2026」

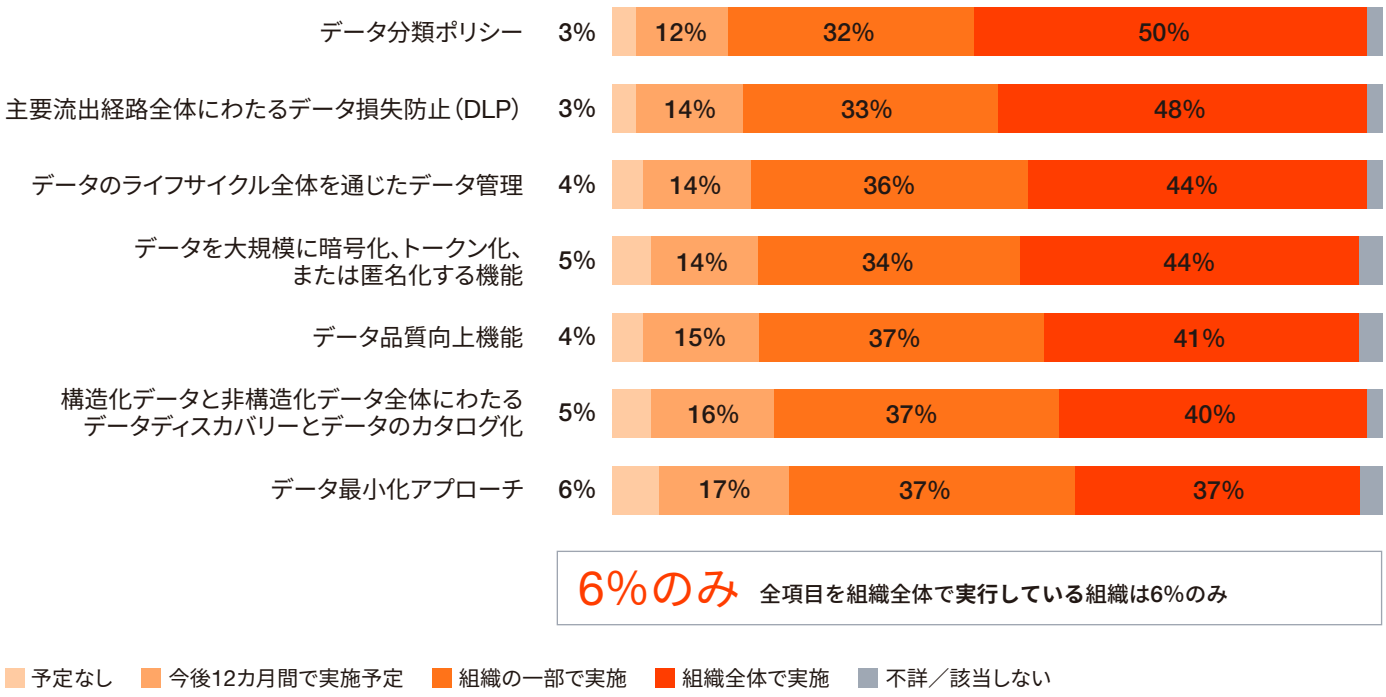
AIデータリスク管理

AIの導入と活用で実効を上げるには、**データリスク**管理を確実に実践することが必要です。なぜなら、AIソリューションを効果的に活用するポイントは、質が高く厳選されたデータセットの利用可否にあるからです。さらには、全社的かつ強力なガバナンスとセキュリティによって、このようなデータセットが適切な文脈で使用されるようにしなければなりません。

組織には、このような課題に立ち向かう力が備わっているでしょうか。さまざまなデータリスク対策の全社的な実施状況に関する質問に対して、完全に実行されているとの回答は、データ分類方針については50%、データの主要流出経路（egress channels）全体にわたるデータ損失防止については48%と、全回答の約半数で、その他の対策に関しては、さらに低い数値になっています。さらに言えば、調査対象の全ての対策が全社的に実行されている組織は、全体の6%に過ぎません。

このように、組織間での進捗状況の相違から、自社のデータをAIソリューション向けに有効活用していくために、各組織が今後どのような取り組みを進める必要があるかをうかがい知ることができます。透明性と責任ある安全なデータプラクティスを通じて、強固な**デジタルトラスト**を構築することが、AIを活用したイノベーションと成長を成功に導く鍵となるでしょう。

データリスク対応策の実行



質問5　あなたの組織では、以下に掲げるデータリスクに対処する全社的な方策がどの程度実施されていますか？（または、実施予定がありますか？）
調査ベース：セキュリティリーダー、CFO、財務担当役員、CDO、主任顧問／GC／CLO、CRO、リスク担当役員、CAE、社内監査役（2,395）
出所：PwC「Global Digital Trust Insights 2026」

04

量子コンピューティングへの備え

異次元の脅威に立ち向かう態勢の整備

Top 4

4大脅威の1つ量子コンピューティングは、組織の準備が現時点で最も遅れている4大脅威の1つ

49%

何らかの量子耐性セキュリティ対策について、検討していないか、まだ実施していない組織は49%

8%のみ

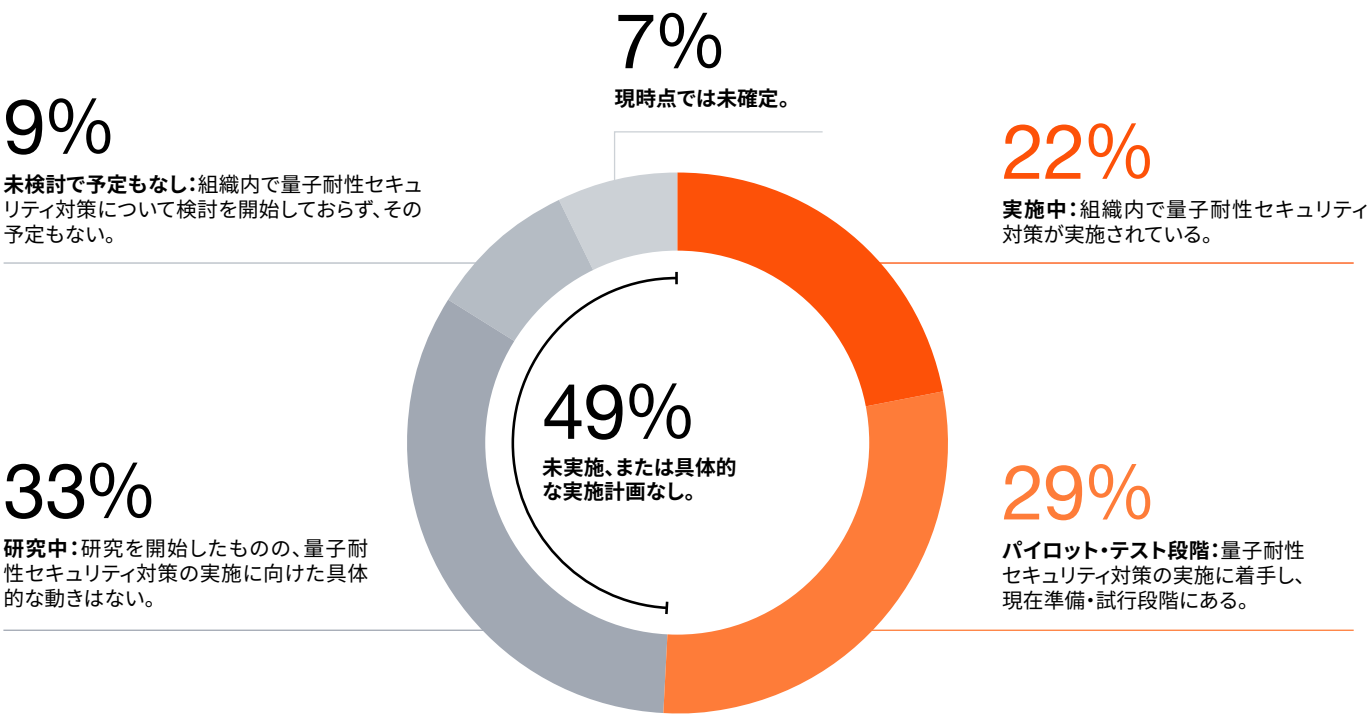
量子コンピューティングへの準備を、予算上の優先項目のトップ3に据えているセキュリティリーダーは全体の8%のみ

量子コンピューティングの実現は、秒読み段階に差し掛かっています。量子コンピューティングは、もはや理論の領域にとどまりません。既に実社会においても、財務モデリングやロジスティクスの最適化をはじめとする入り組んだ課題の解決に、新たな道筋を提示しています。しかし、その一方で、過去何十年にもわたるサイバーセキュリティの常識が覆ろうとしているのです。

量子コンピューティングは、サイバーセキュリティ上の差し迫った脅威というわけではありません。しかし、**耐量子暗号**への移行を急がなければ、組織の機微情報や認証サービス、暗号化システムが脅威にさらされることになるかもしれません。実現までのタイムラインは何年にも及びますが、量子耐性セキュリティの土台を築くためには、将来的に攻撃者の破壊行為を許さぬよう、早急に行動を起こす必要があります。

今後の進展に向けて第一歩を踏み出した組織もあります。全体の29%が既にパイロット導入段階やテスト段階にあります。ただし、パイロット導入段階を超えた先にいる組織は22%にとどまる上、半数近い（49%）組織は、量子耐性セキュリティ対策について検討していないか未実施です。このような組織が躊躇しているのはなぜなのでしょうか。組織内で量子コンピューティングの実用化がもたらすリスクについての理解が得られないことも多いことや、内部リソースが限られること、他の優先課題との競合がその理由です。

量子耐性セキュリティの進捗状況



質問21　あなたの組織の量子耐性セキュリティ対策はどの程度進捗していますか？　調査ベース：全回答者（3,887）
出所：PwC「Global Digital Trust Insights 2026」

量子コンピューティングへの懸念は増大、しかし準備は遅延

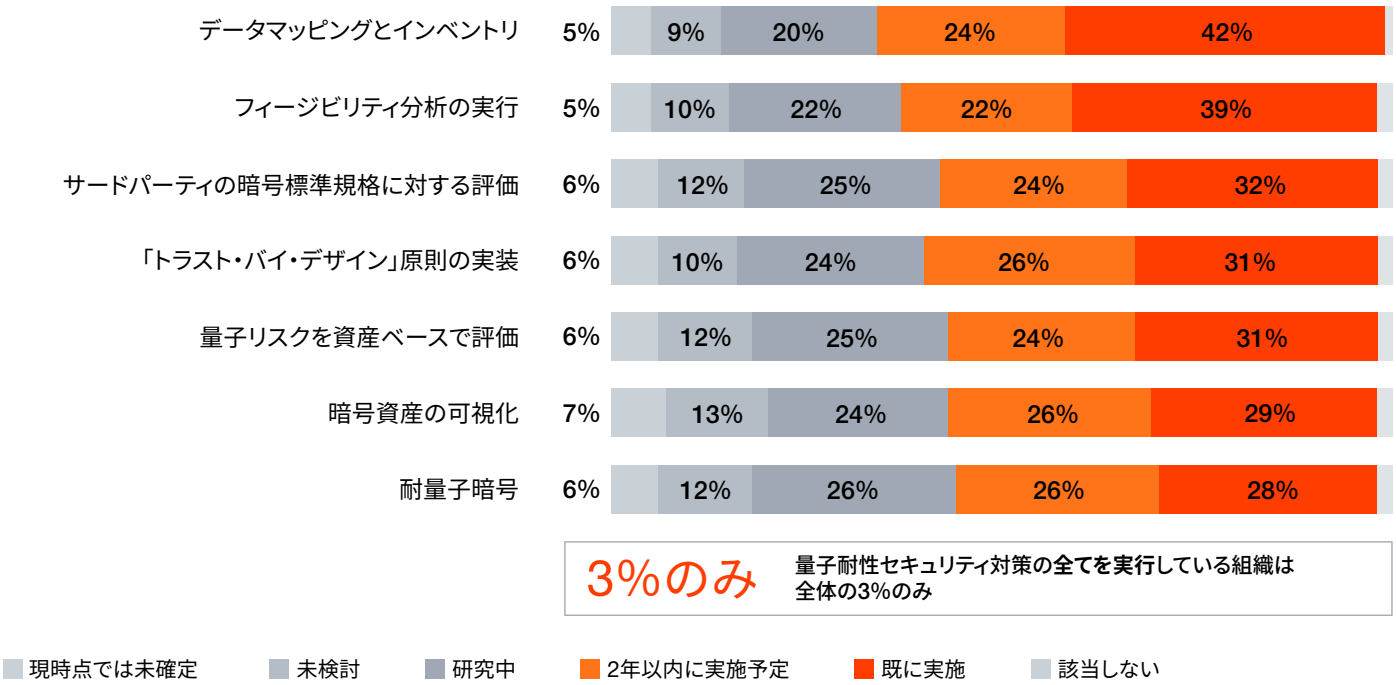
量子コンピューティングがもたらす脅威への認識は広まりつつあります。いまや量子コンピューティングは、組織が準備の遅れを実感している脅威の上位4項目に入っており、前回の調査から数ポイント順位を上げています。

しかし、このような懸念は実際の行動に結びついているのでしょうか。今回調査を行った量子耐性セキュリティ対策について、おおむね全組織の3分の1で何らかの対策が実施されていますが、調査対象7項目の全てを実施している組織は全体のわずか3%に過ぎません。今回の調査では、全て対策が網羅されているわけではありませんが、この7項目は、今後数年を見据えて直ちに対処すべき最優先の課題です。今後についてみると、2026年の予算において、量子耐性を優先項目のトップ3に含めているセキュリティリーダーは、全体の8%にとどまります。

売上高が50億米ドルを上回る組織では、他と比較すると、上記の対策が既に実施されている傾向が認められます。対策の具体例としては、「Harvest Now, Decrypt Later（HNDL）攻撃」（「今収集し、後で解読する」攻撃）のリスクを緩和するデータインベントリ、脆弱な暗号資産の特定を目的とした暗号資産の可視化、耐量子暗号のテストと実装、フィージビリティ分析と量子リスクアセスメントなどが挙げられます。同様に、より急成長を遂げている企業も、量子コンピューティングが投げかけるサイバーセキュリティ上の課題を認識し、それに応じた準備を進めています。

ただし、このような組織は依然として例外的な存在です。技術が進歩する中で耐量子暗号を迅速に採用できるか否かが、企業の能力を決定付ける要因になることは確実です。

量子耐性セキュリティ対策の実施状況



質問22　あなたの組織において、以下に示す量子耐性セキュリティ対策はどの程度進捗していますか？ 調査ベース：セキュリティリーダー（1,740）
出所：PwC「Global Digital Trust Insights 2026」

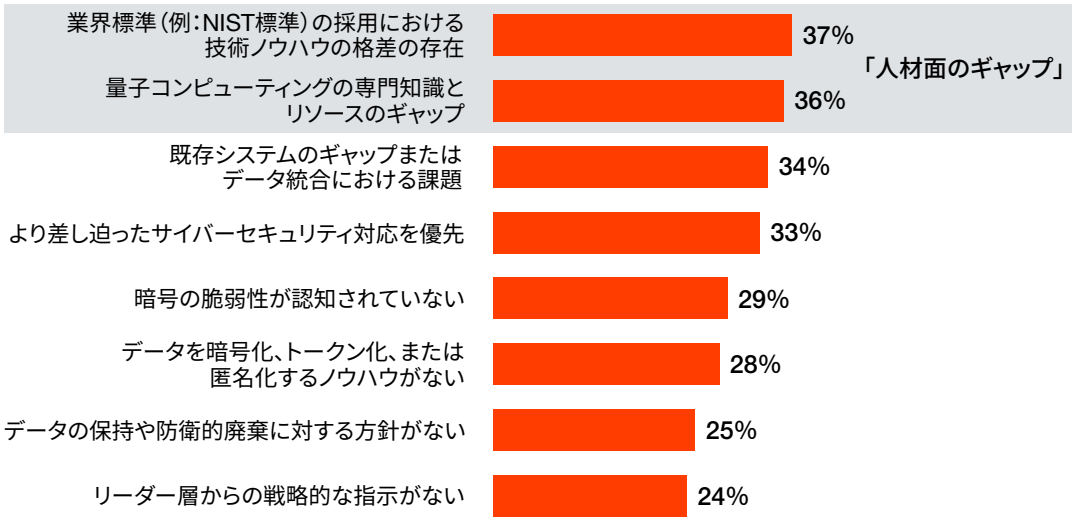
耐量子暗号化が困難な理由

量子コンピューティングへの備えとは、単なる技術力強化の枠を超えて、将来を見据えてセキュリティプラクティスを根本的かつ戦略的に転換することを意味します。では、組織内で何が最大の障害になっているのでしょうか。例えば、組織内の技術ノウハウや知識の不足といった人材面のギャップの他、硬直化したレガシーシステムが挙げられます。

耐量子暗号への移行の手始めとして組織が暗号インベントリを作成する際には、組織のテクノロジースタック全体に存在する脆弱なアルゴリズムを特定すべきです。公開鍵暗号が「今収集し、後で解読する」攻撃を想定した場合に脆弱であることは広く認識されていますが、認証やデジタル署名に欠かせない技術にも同程度に脆弱な暗号アルゴリズムが使われていることをセキュリティリーダーは認識すべきです。

このようなハードルからある事実が浮かび上がってきます。それは、たとえ優先的に取り組む場合であっても、暗号インベントリの作成に着手してから耐量子暗号を実装するまでには時間がかかるということです。しかし、時間的な余裕はありません。米国立標準技術研究所（NIST）などによる業界をリードする暗号化標準では、脅威アクターが量子コンピューティング能力を獲得する前に脆弱なアルゴリズムを廃止することを推奨しています。それゆえに、企業は知識のギャップを解消し、自組織における暗号依存関係を評価し、将来に備えるためのロードマップを作成することが極めて重要なのです。

耐量子暗号化までの課題
（課題の上位3項目に挙げた組織の割合）



質問23　今後12カ月間で耐量子暗号化を実現するにあたって、あなたの組織が抱える最大の課題はどのようなものですか？
調査ベース：セキュリティリーダー（1,740）
出所：PwC「Global Digital Trust Insights 2026」

05

サイバーセキュリティ人材とスキル

マネージドサービスが最前線に

Top 2

サイバーディフェンスにAIを実装する際の課題のトップ2は、ノウハウとスキルのギャップ

53%

サイバーセキュリティ人材のギャップに対処するために、今後12カ月間で優先的に取り組む項目のトップ3にAIを挙げたのは全回答者の53%

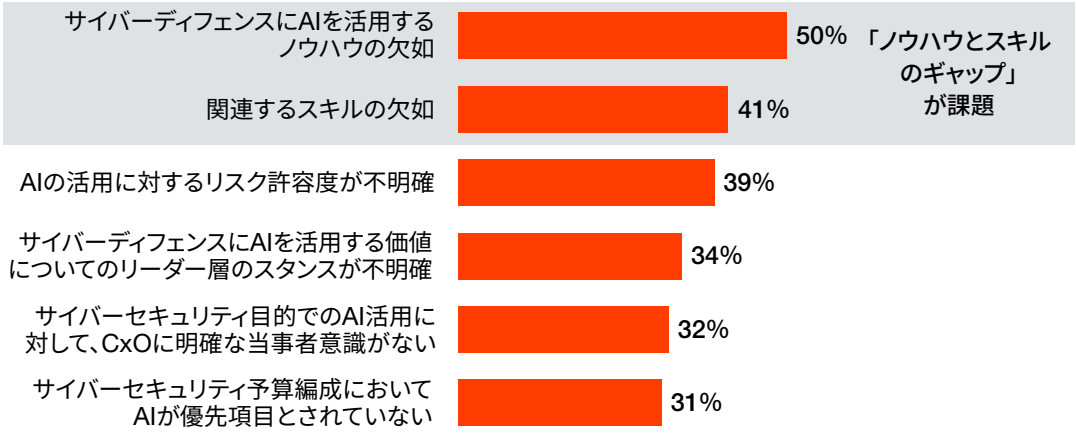
48%のみ

重大な攻撃を受けたことがある組織の48%が、サイバーセキュリティ人材のギャップを埋める手段としてマネージドサービスを重視

各組織においては、AIの運用を可能にし、複雑な環境の安全を確保し、次世代の脅威に対する準備を整えるための取り組みが進められています。しかしながら、サイバーセキュリティを担う人材不足が続き、思うように進捗していないのが実情です。

ノウハウとスキルのギャップは、過去12カ月間において、サイバーディフェンスへのAIの実装を阻害する2大要因とされており、各組織は具体的な方策の再検討を迫られていました。各組織は、今後12カ月間で優先的に取り組む項目として、AIツール（53%）、セキュリティ自動化ツール（48%）、サイバーセキュリティツールの整理統合（47%）、スキルアップやリスキリング（47%）などを挙げており、AIの実装に向けて新たな可能性を探る取り組みが進められています。また、過去に重大な攻撃を受けたことがある組織（全体の48%）を中心に、専門化したマネージドサービスが重視されています。

サイバーディフェンスのためのAIの実装における課題
（課題の上位3項目に挙げた組織の割合）

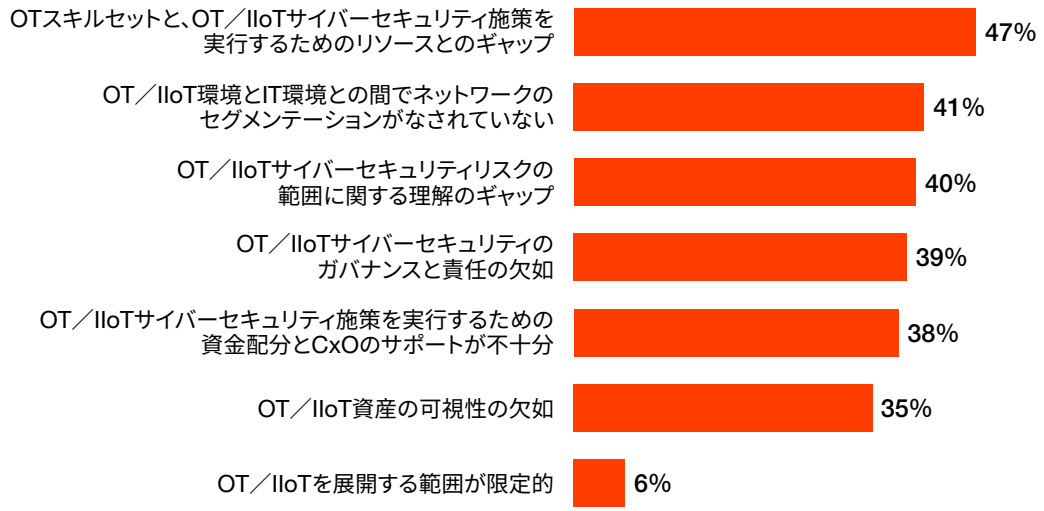


質問20　サイバーディフェンスにAIを実装するにあたり、過去12カ月間において、あなたの組織が抱える最大の課題はどのようなものでしたか？ 調査ベース：セキュリティリーダー、CEO、CFO、財務担当役員、COO、事業運営担当役員（2,764）
出所：PwC「Global Digital Trust Insights 2026」

制御システム（OT）人材不足

今日、セキュリティ環境の核心にあるのは、OTと産業用IoT（IIoT）です。組織が抱える課題の上位3項目で、有能な人材の欠如を挙げるリーダーは、全体の半数近く（47%）に上ります。また、リーダーの39%は、明確なガバナンスと当事者意識がないことを指摘しています。このように、求められる人材とスキルの間に横たわるギャップから、より深刻な課題が浮かび上がってきます。それは、インターネットへのOTの接続が加速する中で、自信を持ってOTを管理するための仕組みと専門知識を備えていない組織が依然として多いということです。

OTとIIoTシステムの安全を確保する上での障害
（課題の上位3項目に挙げた組織の割合）



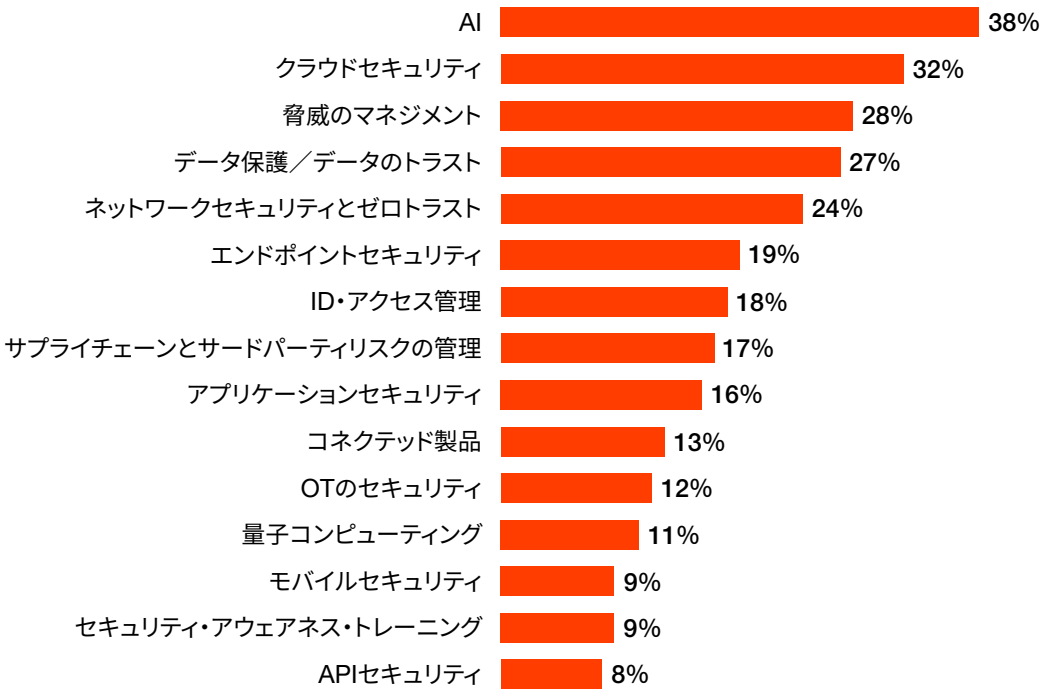
質問4　制御システム（OT）または産業用IoT（IIoT）システムの安全を確保するにあたり、あなたの組織が直面している課題の上位3項目を挙げてください。調査ベース：セキュリティリーダー（1,740）
出所：PwC「Global Digital Trust Insights 2026」

戦略的アクセラレーターとしてのマネージドサービス

AIとクラウドは、サイバーセキュリティ投資において最優先される投資対象であるのみでなく、専門的なマネージド・セキュリティ・サービスにおいて最も活用されているものでもあります。組織では、専門能力のアウトソーシングの域を超えて、マネージドサービスが活用されています。また、プロバイダーと連携して、重要なシステムの提供方法の近代化を進めています。

マネージドサービスは戦略的アクセラレーターになりつつあり、スキルの不足を補うとともに、速度の向上と規模の拡大、専門知識の強化を促進する役割を担っています。日々複雑化する脅威環境の中で、マネージドサービスは、イノベーションと成長から軸足をずらすことなく、サイバーセキュリティを刷新する上での手助けになります。

マネージドサービスを活用する際、サイバーセキュリティ面で重視する項目
（上位3項目に挙げた組織の割合）



質問15　あなたの組織のサイバーセキュリティ計画において、以下の各分野のうち、マネージドサービスの優先的な活用を今後12カ月間で予定しているものがあれば挙げてください。 調査ベース：セキュリティリーダー（1,740）
出所：PwC「Global Digital Trust Insights 2026」

CxOプレイブック

不確実な状況から行動へ

いまリーダーにできることは？

今回の調査において、最も先見性のある組織では、サイバーセキュリティと事業戦略との整合が図られており、事後対応よりも事前準備が重視されていることが明らかになりました。

多くの組織は、サイバーセキュリティリスクの管理を目的とした基礎的な取り組みを既に実行しています。具体的には、主要なサイバーセキュリティ体制に合わせてガバナンスの仕組みを強化すること、サイバーセキュリティリスク管理を全社的に徹底すること、リスク診断と報告を優先的に行うことが挙げられます。

しかし、現状を維持するだけでは、将来への備えとして十分とは言えません。必要とされるのは、予測が困難な状況に立ち向かうこと、情報に即して果敢な意思決定を下すこと、素早く戦略を策定することなのです。

CISO／CSO

CISO／CSOに求められる能力は、複雑なサイバーセキュリティリスクをビジネスリスクの視点に置き換えて解釈できることだけではありません。CxOが協調してサイバーセキュリティの責任を果たしていくための方策について、効果的に伝達する能力も不可欠です。これらを通じてCxOの賛同と協力を確保していくのです。このような理解を共有することは、ガバナンス、レジリエンス、法令遵守、レスポンスの基盤となる取り組みを促進するために有益です。今後は、セキュア・バイ・デザインの意識を高めることによって新たなリスクに先手を打って対処するとともに、サイバーセキュリティ投資において、データを活用して最優先すべき項目を評価し説明することが求められます。

基盤

重要インフラ、海外事業展開、業界特有の混乱と連動したメトリクスを活用して地政学的リスク環境を定量化し、その結果をCxOと共有します。

ハイリスク地域、サイバー攻撃活動、データ恐喝の傾向に関する最新のインテリジェンスと整合した動的脅威モデリングを実装します。

AIの導入にあたっては、「**責任あるAI**」の原則を貫徹させ、機密性、重要度、露出度に基づいてAIシステム（モデル、エージェントとその識別情報、アプリケーションとトレーニングデータを含む）を分類します。

現行のセキュリティ管理を拡大して、AIシステムも管理対象に含まれるようにします。また、対処するために新たなノウハウを必要とするギャップ（AIガードレールやLLMゲートウェイなど）を特定して、AIの安全を確保します。

AIや量子コンピューティングなど、テクノロジーの急速な進歩がもたらすリスクを織り込めるよう、日常的にサイバーセキュリティリスク管理モデルの再検討とアップデートを行います。

実行可能なKPIを通じてガバナンスを強化し、サードパーティ、サプライチェーン、レガシーシステムのリスクや、クラウドベースのリスクの管理に係るパフォーマンスを追跡します。

机上演習とシミュレーションにより、意思決定のストレステストを行い、エスカレーション経路を決定し、復旧ステップを検証します。

将来への備え

新興の脅威や攻撃者の能力に関して、脅威インテリジェンスの知見やCxOクラス向けのサマリーから得られる情報に加え、ガバナンスに関する協議の成果を取り入れることで、サイバーセキュリティはCxOと取締役の共同責任であるとの認識を確立します。

可視化、分類、危険度のマッピング、継続的モニタリング（攻撃者のシミュレーションを含む）を行うことによって、自律型AIによる監視とガバナンスを運用できるようにします。

特定時点におけるベンダーの評価から、継続的に行う第三者リスクの監視へと移行します。

暗号依存システムを診断し、必要に応じて耐量子暗号標準を採用します。

投資収益率（ROI）ベースでマネージドサービス計画を策定して、必要な技術、スキル、リソースを割り振ります。それを基に、組織がマネージドサービスを有効活用すべきか否かを判断します。

組織のデータを診断し、現時点において耐量子化を行うべき項目を決定します。次に、組織内のデータ管理チームと連携して、耐量子化の受け入れに向けた準備を進めます。

CTO／CIO

基本的な使命は、**セキュリティを確保しながら技術規模を拡大**し、人材とトレーニングのギャップに先回りして対処するよう注力することです。それによって、組織のサイバーセキュリティ体制の整備に不可欠な支援を行うことができます。技術の受け入れ全体にわたるリスクの管理とガバナンスを根付かせるには、セキュリティリーダーとの緊密な協力関係を持続する必要があります。将来的には、AIや量子コンピューティングのような新興の技術を準備し、ビルトインセキュリティと統合する取り組みを先導するとともに、将来のサイバーセキュリティリスクを想定して、これを緩和するイノベーションを推進します。

基盤
セキュリティを確保しながら、AIなどの新興技術の規模を拡大します。最重要な予防型セキュリティ対策に予算を配分し、根づかせます。
CISOやCROとの緊密な協力関係の下、リスク管理やコンプライアンスの要件を充足しつつ、技術の導入を進めます。
AI実装計画の立ち上げ時から、ガバナンスとサイバーセキュリティリスクの管理を着実に行うことにより、AIの安全を確保し、セキュア・バイ・デザインの原則に即したものにします。
サードパーティのプラットフォーム、API、インテグレーション全体にわたって、一貫したID、アクセス、ポリシーの管理を実施します。
組織のアーキテクチャ戦略において、堅牢なIIoTとOTガバナンスを適用することにより、エンドツーエンドで、分散環境全体をカバーする可視化と管理を可能にします。

将来への備え
CISOやデータ管理者と連携して、トレーニングに供される機微情報の安全を確保し、AIモデルの入力／出力のガバナンスを強化します。
セキュリティリーダーと協力して、耐量子化の受け入れと準備に向けた取り組みと、全社的な量子耐性セキュリティ戦略との整合を図ります。
AIを活用した自動リスク検知・対応ツールの採用を進め、運用効率の向上とレジリエンスの強化を実現します。
コネクテッド製品の運用ライフサイクル全体にわたるセキュア・バイ・デザインのフレームワークを採用します。

CRO

リスクを抱える企業や新興リスクを特定し、それとサイバーセキュリティとの相互依存関係を究明するという、組織の安全確保に不可欠な役割を担っています。脆弱性の増大に見合うよう継続的にコントロールを調整しつつ、リスクフレームワークを最新の状態に維持する必要があります。今後も、AIや量子コンピューティング、地政学的な脅威にさらされる環境を、組織のアジリティとレジリエンスを支える適応性と先進性を備えたリスク管理戦略に統合していく役割を引き続き担っていくことになるでしょう。

基盤

既知の地政学的リスク要因を最優先に、脅威ベースのシナリオをリスク登録簿とストレステストサイクルに組み入れます。

脅威に対処するために現在実行されている管理を査定し、必要に応じて、現行の緩和戦略を調整します。

デジタルによる業務自動化を優先項目として、ビジネスインパクト分析を調整してAIリスクと量子リスクを定量化します。

規制の要件に適合するようサイバーセキュリティ脅威の管理をマッピングし、法令遵守の取り組みをサポートします。

将来への備え

ベンダー環境における量子耐性と攻撃者によるAIの悪用に対するレジリエンスを考慮に入れて、サードパーティリスク管理モデルを拡張します。

AIを活用して、サイバーセキュリティリスクの定量化から診断・報告に至るまで、サイバーセキュリティリスクに関する大規模な診断を継続的に実施します。

脅威インテリジェンス統合型リスク管理フレームワーク（IIRF）を開発して、組織のリスクスコアリングに、戦略的な脅威インテリジェンスに関するさまざまな視点を取り入れます。

予測型脅威モデリングツールの先行テストを通じて、新興リスクのシミュレーションを行うとともに、今後12カ月から36カ月の間に事業が受ける可能性がある影響度を定量化します。

CFO

戦略的取り組みと技術の実装において、予防型サイバーセキュリティ対策に適切な予算を配分するという、組織のレジリエンスに不可欠な基盤的役割を果たします。非効率な領域の特定を継続して行い、大きな影響を持つサイバーセキュリティイニシアティブに見合った予算を編成します。将来的には、今後の必要性を見越した予算の割り当てや**投資収益率（ROI）重視型の資金配分モデル**を推進し、新興リスクへの備えを構築します。それによって、組織として、安全を確保するための技術とスキルに合理的に投資できるようにします。

基盤
レジリエンス、競争上の優位性、法令遵守体制の整備を長期的視点から推進する戦略的投資をサポートします。
セキュリティインシデントへの事後的対応と、予防的投資（サイバーディフェンス、マネージドサービス、保険、法令遵守など）との長期的なコスト比較を行います。
インシデントの未然防止、規制違反に伴う課徴金の回避、対応所要時間の短縮によって削減できた費用を織り込めるように、サイバーセキュリティに係るROI指標を再調整します。
CISO、CTO、CIOと連携して、サイバーセキュリティ関連のスキル開発や技能訓練に、効果的に予算を割り当てます。
日常的な運用費と戦略的なサイバーセキュリティ投資とのバランスが図られるような、サステナブルな資金配分モデルをサポートします。

将来への備え
取締役クラスが想定する業績目標に見合うレベルに投資水準を設定し、必須のビジネス機能としてサイバーセキュリティを主導します。
ゼロデイ攻撃への対応能力の向上や量子耐性の強化などを「レジリエンスの達成手段」と位置付けて、これに資本を割り振ることを目的とする積立金を創設します。
マネージド・セキュリティ・サービスを目的とするROI重視型のビジネスケースを作成します。
ツールの冗長性などの非効率を特定し、効率の向上を図り、可能な場合は集約します。

CEO

サイバーセキュリティを事業における優先項目として確実に位置付けることは、CEOの役割として今後とも不可欠です。取締役とCxO全体の連携強化に注意を払いながら、事業活動とサイバーセキュリティリスク管理戦略とを整合させる取り組みを続けていくことが必要です。将来的な役割としては、影響力のある提携関係を構築すること、そして、サイバーセキュリティの世界における新興リスクの荒波を組織が乗り越えていくための投資を主導していくことが求められます。

基盤
エグゼクティブを対象とするオフサイトミーティングにおいて、部門特有の混乱やハイブリッド型の脅威作戦を模したサイバーセキュリティシナリオへの参加を義務付けます。
サイバーセキュリティレジリエンスと、収益手段（デジタルプラットフォームの安全確保、顧客データのトラスト、国際的な成長など）とを結び付けます。
AIと量子耐性プロジェクトにおいては、当初から倫理的なセキュリティガードレールを組み入れるようにし、責任あるイノベーションを主導します。
サイバーセキュリティ予算のどこにトレードオフを設けるか、また、このようなトレードオフとリスク許容度との折り合いがつくか否かを理解します。
取締役からバックオフィスに至るまで、あらゆるレベルでサイバーセキュリティの責任を共有するようにします。
戦略的なサイバーセキュリティ計画上の優先項目に関して取締役と理解を共有し、計画のニーズに関する検討への関与を求めます。

将来への備え
耐量子標準への準備、共同でのサイバーディフェンス態勢の構築、脅威インテリジェンスの交換に向けた複数業界間の連携を主導します。
当初から安全の維持を織り込んで、新興技術（AI、量子コンピューティング）への投資を主導します。
量子技術や地政学的情勢に関する未来予測レビューを、戦略計画サイクルや取締役会のリスク憲章として制度化します。
地政学的・技術的混乱に備えて、ストレステストに積極的に参画します。

本調査について

「Global Digital Trust Insights 2026」は、世界のビジネスリーダーおよびテクノロジーリーダー3,887名を対象に、その見解を調査することを目的として、2025年5月から7月にかけて実施したものです。

回答者の3分の1（33%）は売上高50億米ドル以上の大企業のCxOです。回答企業の業種は、金融サービス（21%）、製造・自動車（21%）、テクノロジー・メディア・通信（19%）、小売・消費財（16%）、ヘルスケア（10%）、エネルギー・ユーティリティ・資源（9%）、政府・公共サービス（4%）と多岐にわたっています。

回答企業は72カ国に拠点を置いており、その地域別分布は、西欧（32%）、北米（27%）、アジア太平洋（18%）、中南米（11%）、中・東欧（6%）、アフリカ（4%）、中東（3%）となっています。

「Global Digital Trust Insights」調査は、以前は「グローバル情報セキュリティ調査（GSISS）」として知られていたものです。今回で28年目を迎える本調査は、サイバーセキュリティの動向に関する年次調査として最も長い歴史を有しています。また、サイバーセキュリティ業界で最大規模の調査でもあり、セキュリティリーダーやテクノロジーリーダーだけでなく、シニアビジネスリーダーの参画を得ている調査としても他に類を見ないものです。

本調査は、PwCグローバルネットワークで世界の市場調査とインサイト提供を担当するCentre of Excellenceである**PwCリサーチ**が実施しました。

お問い合わせ先

PwC Japanグループ

https://www.pwc.com/jp/ja/contact.html

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびブローダーアシュアランスサービス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約13,500人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。PwCは、クライアントが複雑性を競争優位性へと転換できるよう、信頼の構築と変革を支援します。私たちは、テクノロジーを駆使し、人材を重視したネットワークとして、世界137の国と地域に364,000人以上のスタッフを擁しています。監査・保証、税務・法務、アドバイザリーサービスなど、多岐にわたる分野で、クライアントが変革の推進力を生み出し、加速し、維持できるよう支援します。

本報告書は、PwCメンバーファームが2025年10月に発行した『2026 Global Digital Trust Insights: C-suite playbook and findings』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。オリジナル（英語版）はこちらからダウンロードできます。
https://www.pwc.com/gr/en/advisory/technology/global-digital-trust-insights.html

日本語版発刊年月：2026年3月　　管理番号：I202512-08