STATE OF CYBERSECURITY 2024

Introduction

サイバーセキュリティは常に「バランス」が求められ、長年に渡り、そこにはセキュリティ vs. 利便性の争いがあります。ビジネス環境においても消費者市場においても、セキュリティ管理の強化は、利便性の低下を意味しており、ほとんどのエンドユーザーが躊躇するトレードオフとなります。組織は、テクノロジーとポリシーを使ってこの問題を強制することができますが、それにより、リスキーな回避策への扉が開かれてしまう可能性があります。

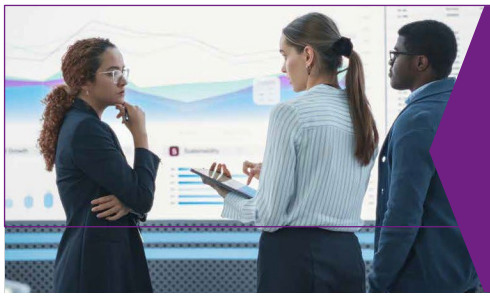
今日、新たな課題が浮上しています。情報セキュリティー最高責任者（CISO）や最高情報責任者（CIO）など、企業のセキュリティ維持に携わる者にとって、そのような葛藤は対「利便性」ではなく、対「進歩」だといいます。組織がDXを進め、テクノロジーの取り組みをビジネスの成功に強く結びつけるにつれ、過剰なサイバーセキュリティ対策が全体的な進歩を妨げる可能性があります。もちろん、緩すぎる対策は深刻なインシデントにつながる可能性もあり、結果として進歩にさらなる影響を与えることもあるのです。

本レポート「State of Cybersecurity ～セキュリティの現状～」レポートでは、サイバーセキュリティの方程式の「バランス」を取る上で考慮すべき、多くの変数を探ります。サイバーセキュリティがビジネスに不可欠なものとなるにつれ、あらゆるプロセスで潜在的な脆弱性がないか精査する必要があります。そして、このリスク分析をすることで、ワークフロー、スキル構築、テクノロジー導入に関する意思決定が促されます。テクノロジーの動向が進化し、攻撃パターンが変化する中、真の均衡に達することは困難であり、こうしたバランス取りはフルタイムの仕事なのです。

注目すべき動向 2024

ポリシー

リスク管理はサイバーセキュリティの原動力である

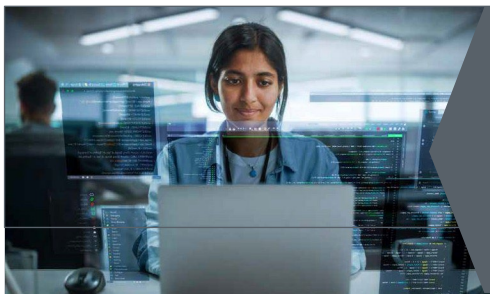


プロセス

サイバーセキュリティプロセスがさまざまな意思決定を促す

人材

企業がスキルのレジリエンスを高めることで、人材のパイプラインが強化される



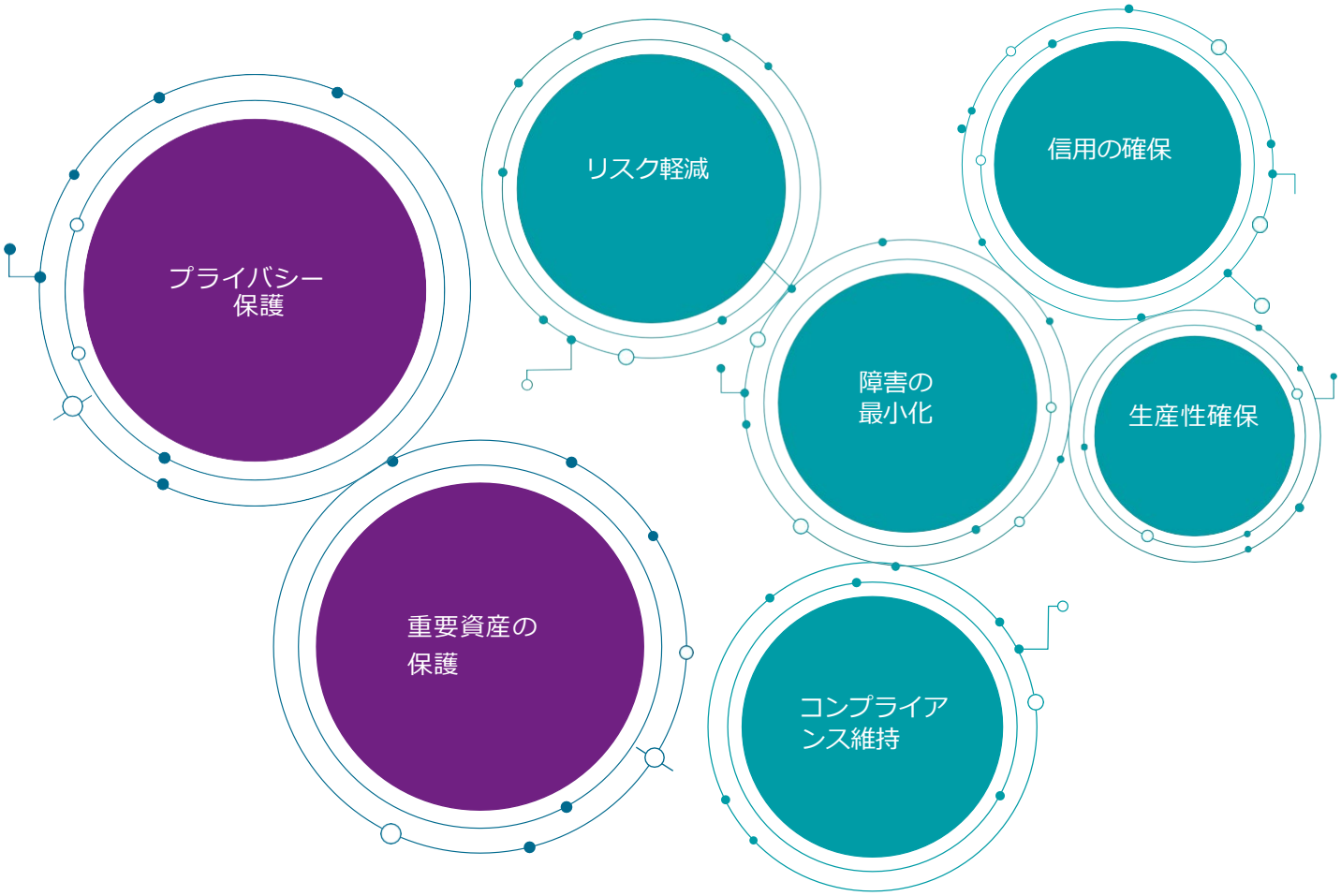
製品

AIがサイバーセキュリティ製品を新たな高みへと押し上げる

市場概要

適切な「バランス」を見つけることがいかに難しいかは、組織のサイバーセキュリティ戦略の背景にある目的を見ればわかります。本レポートの調査には、6つの異なる地域が参加し、さまざまな経済的かつ技術的成熟度を表しています。6つの地域すべてにおいて、サイバーセキュリティ戦略の最優先事項には、「重要な企業資産の保護」や「顧客データのプライバシー保護」など、「保護」という従来の目的が含まれています。

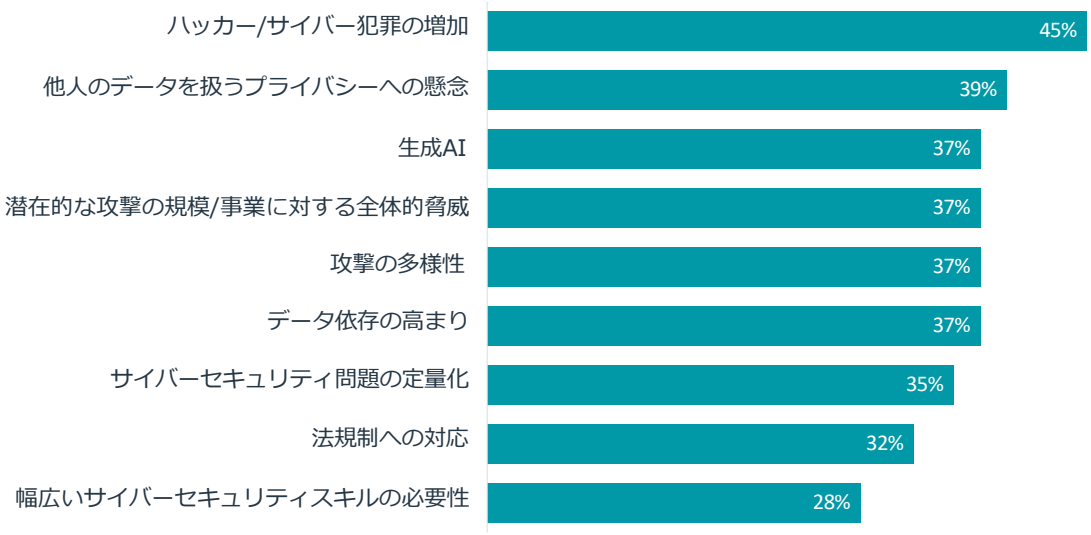
サイバーセキュリティの目的



Source: CompTIA 2024 State of Cybersecurity | n=1156 technical and business professionals

しかし、「保護」はパズルの1 ピースにすぎません。業務のデジタル化が進むにつれ、業務の障害を最小限に抑え、増える規制へのコンプライアンスを維持し、企業ブランドの一部としての信頼を確立するには、強固なサイバーセキュリティのアプローチが必要になります。これらを達成するには、外部からの脅威を防ぐだけでは不十分であることから、健全な内部プロセスに対する積極的なマインドセットが必要なのです。

サイバーセキュリティ懸念を駆り立てる多くの問題

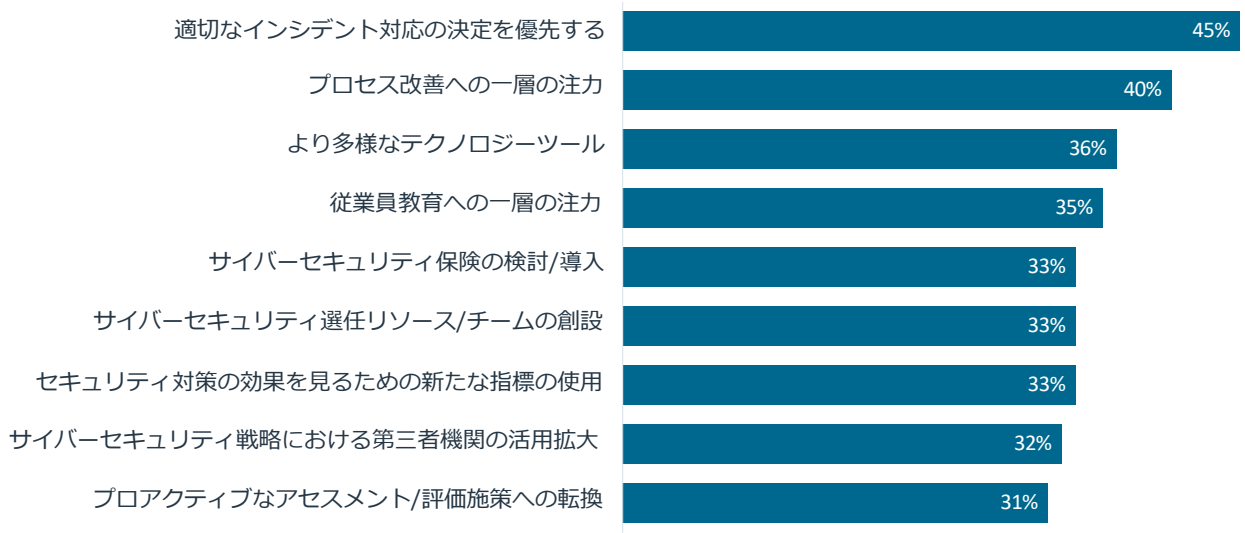


Source: CompTIA 2024 State of Cybersecurity | n=511 U.S. technical and business professionals

企業のサイバーセキュリティに対する危機感と、そのポリシーを策定する上での課題を簡単に表すなら、規模の劇的な拡大です。脅威の観点から見ると、サイバー犯罪件数が急増し、その組織的能力が高まっていることがわかります。同時に、攻撃による潜在的な被害は壊滅的なものになりかねません。データの観点から見ると、膨大なデータが収集され、顧客のプライバシーへの影響と、社内ワークフローの運用リスクが存在します。製品の観点から見ると、生成AIの能力が加速しており、組織のスキル格差はさらに広がっています。

米国において、その規模が過小評価されているであろうものに、サイバーセキュリティに対する外部要因の台頭があります。その最たる例が、政府の規制です。どの国においても、サイバーセキュリティのガイドラインはますます複雑化しており、医療や金融といった一般に規制の厳しい業界を超えています。グローバルに事業を展開する組織にとって、それぞれの国の規制に対応することはさらに困難といえます。また、その他の外部要因には、関係を結ぶ企業間の契約要件や、サイバー保険に付随する規定などがあります。

過去1年間のサイバーセキュリティの変化



Source: CompTIA 2024 State of Cybersecurity | n=511 U.S. technical and business professionals

サイバーセキュリティという大きな問題に対処するには、多面的なアプローチが必要です。組織全体のプロセス、特にインシデント対応に関するプロセスが改善されなければなりません。さらに、スキルギャップに対処しなければなりません。そのためには、広範な人材教育、専任のサイバーセキュリティリソース、外部パートナーの協力が必要となります。特定のアクティビティに対応するターゲットテクノロジーと、すべてをまとめるダッシュボードとともに、ツールボックスをアップデートする必要があります。

ゆっくりですが確実に、こうしたアプローチの変化は効果を発揮しているようです。経済におけるサイバーセキュリティの全体的な状況に関しては、調査回答者の67%が「改善している」と感じていて、そのうち27%は「劇的に改善している」としています。後者の「劇的に改善している」に関しては、2022年の時点では25%でした。組織の観点から見ると、回答者の76%が「自社のサイバーセキュリティ対応は十分である」と感じており、その中には「完全に満足している」とする回答が28%も含まれています。2022年には、後者の「完全に満足している」は24%のみでした。

興味深いことに、組織全体を通してエグゼクティブ（経営層）と他の従業員の間で満足度に大きな差があることがわかりました。10人中4人以上のエグゼクティブが、自社のサイバーセキュリティ対応に「完全に満足している」と報告していますが、ITスタッフでは25%、事業スタッフでは21%です。この背景には、エグゼクティブは、テクノロジーに関してより多くの裁量が与えられていて、他の従業員よりも利便性が高いということがあるかもしれません。一方、一般スタッフは、エグゼクティブには見えないサイバーセキュリティ導入の詳細について頭を悩ませているかもしれません。いずれにせよ、こうした意識のギャップは、このトピックに関するコミュニケーションが改善されるべきであることを示唆しています。

満足度がわずかに向上したとしても、改善の余地はたくさんあります。近年、企業はサイバーセキュリティをテクノロジーと密接に関連したクリティカルな機能と捉え始めていますが、成功に関連する指標は独立しています。 次の段階では、この独立したユニットの運用を確立し、洗練させ、さらに戦略的なポリシーとプロセスを用いることで、人材と製品に関する戦術的なアクションを推進することです。

インシデントと影響

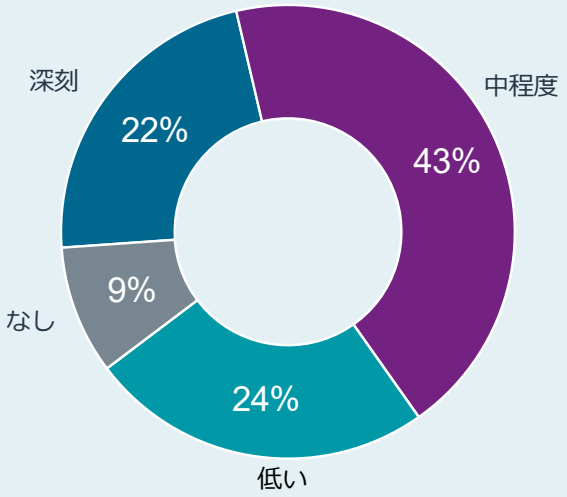
サイバーセキュリティに関しておそらく最も一般的な質問は、サイバーセキュリティインシデントのコストについてでしょう。この質問に答えるには、エンドユーザーから2つの情報が必要になります。まず、侵害が発生したという認識についてです。次に、被害低減に要する総コストを把握しているかです。どちらの情報も収集は簡単ではありません。

サイバーセキュリティインシデントを認識するには、システムに対する十分な可視性と、インシデントの構成要素に関する合意の両方が必要です。Palo Alto Networksの調査What's Next in Cyber Reportによると、96%の組織が2022年に少なくとも1件の侵害を経験したと報告しています。これと比較して、Splunkの調査State of Security 2023では、52%組織が最近のデータ侵害を報告している一方、87%がランサムウェアの標的となったと報告しています。これら回答は、インシデントに関する不確実性を示すもので、ネットワーク侵入が何か月も検出されなかったという報告によってさらに悪化した可能性があります。

コストについては、サイバーセキュリティインシデントによる経済的影響に関する多くの推計報告があります。注目すべきはIBMのCost of a Data Breachの調査で、2023年のデータ侵害のグローバルな平均コストは445万ドルとされています。さまざまな数値や、低減の取り組みを定量化しようとした動きがありますが、最終的な数値は大企業に偏るもので、企業がそうした取り組みを詳細に示すには至っていません。

過去1年間のインシデントのリスク低減について

インシデントに伴う推定影響



一般的な低減措置

1. テクニカルスタッフを時間外業務から外す
2. 新しいソフトウェアの購入
3. テクニカルスタッフをルーチン業務から外す
4. 従業員の懲戒処分/解雇
5. 新しいハードウェアの購入
6. 事業スタッフをワークフローから外す
7. 外部へのコミュニケーション計画の見直し

Source: CompTIA 2024 State of Cybersecurity | n=511 U.S. technical and business professionals

CompTIAのアプローチは、回答者にインシデントの影響を評価するよう求めるもので、企業サイズに関係なく正規化したものです。（100万ドルの軽減措置は小規模企業にとっては深刻な影響かもしれませんが、巨大企業にとっては低いものかもしれません。）次に、インシデントに対処するために取られた典型的な手順について求めました。これには、時間や労力を伴うものの、必ずしも直接的コストではないものが含まれます。例えば、上記にあるインシデントに関与した従業員の懲戒処分/解雇で、サイバーセキュリティ問題における人的ミスや不正行為の脅威を強調しています。

1 ポリシー：リスク管理はサイバーセキュリティの原動力である

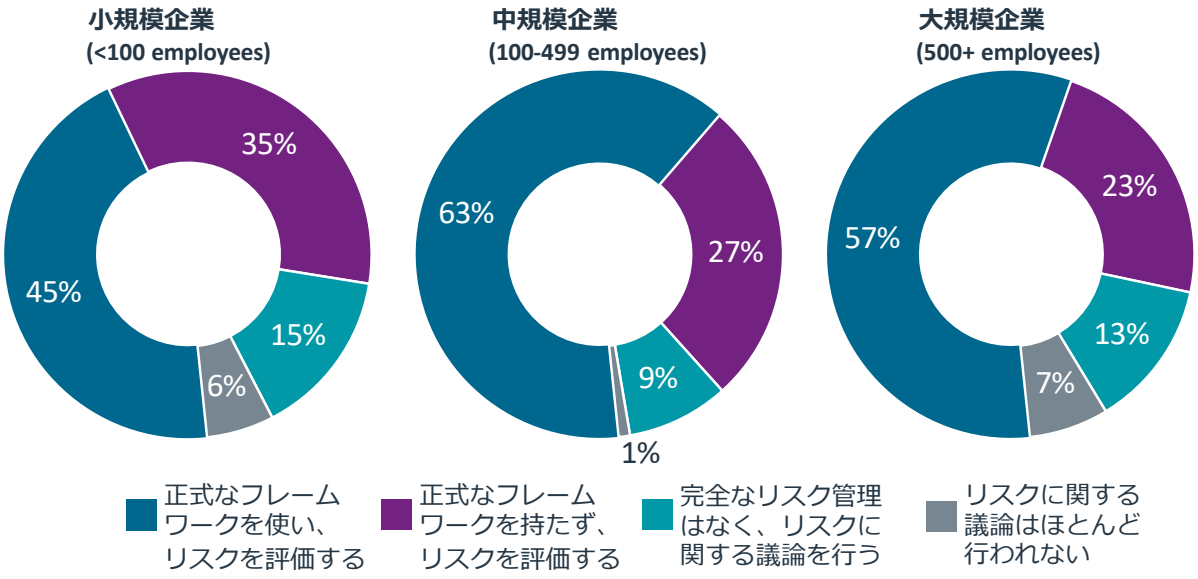
リスク管理は、現代のサイバーセキュリティにおける大きな課題の1つを解決する主要な手法になりつつあります。その理由は、サイバーセキュリティの取り組みと業務運用の関係性です。

サイバーセキュリティプロフェッショナルが以下を行うと、サイバーセキュリティ対策への支出と望ましい成果との関係性はより強くなります。

1. さまざまなリスクの特定
2. サイバーインシデントの確率の割り当て
3. 潜在的コストの特定
4. インシデントレスポンス計画の提案

正式なリスク管理フレームワークが必要ですか？ 回答者の取り組みを見てみましょう

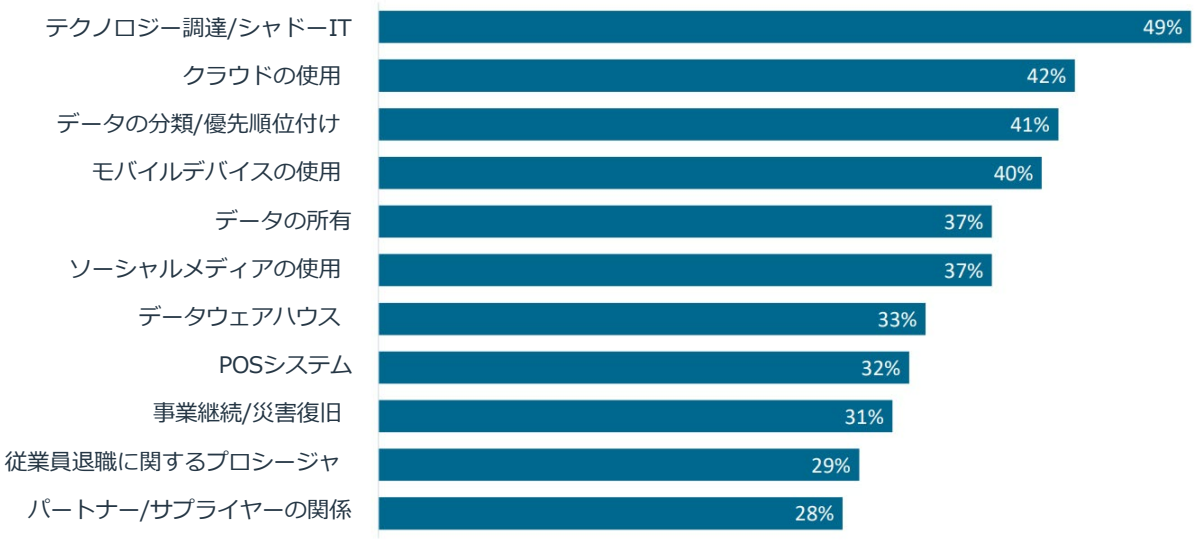
リスク管理への組織的アプローチ



Source: CompTIA 2024 State of Cybersecurity | n=511 U.S. technical and business professionals

正式なフレームワークを使用すべき理由の1つは、従来のITシステムアーキテクチャから外れた領域を特定しやすくするためです。

リスク分析に含まれるトピック



Source: CompTIA 2024 State of Cybersecurity | n=488 U.S. technical and business professionals

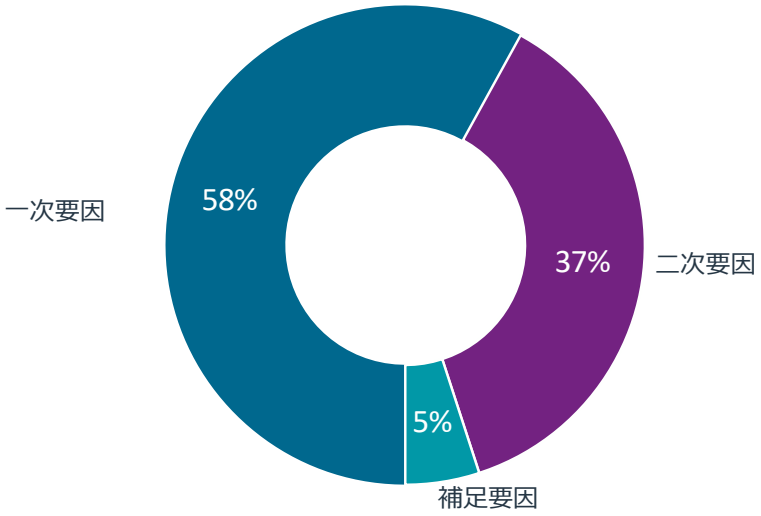
徹底したリスク分析では、技術的なトピックにとどまらず、IT チームとはあまり関係のないポリシーやプロセスも調査します。

2 プロセス：サイバーセキュリティプロセスがさまざまな意思決定を促す

包括的なリスク管理の規律に従い、サイバーセキュリティプロセスを構築し、サイバーセキュリティを事業ワークフローに組み込むことで、多くの機能的な決定を促します。

1．サイバーセキュリティは、テクノロジーを評価する際の第一要因になりつつある

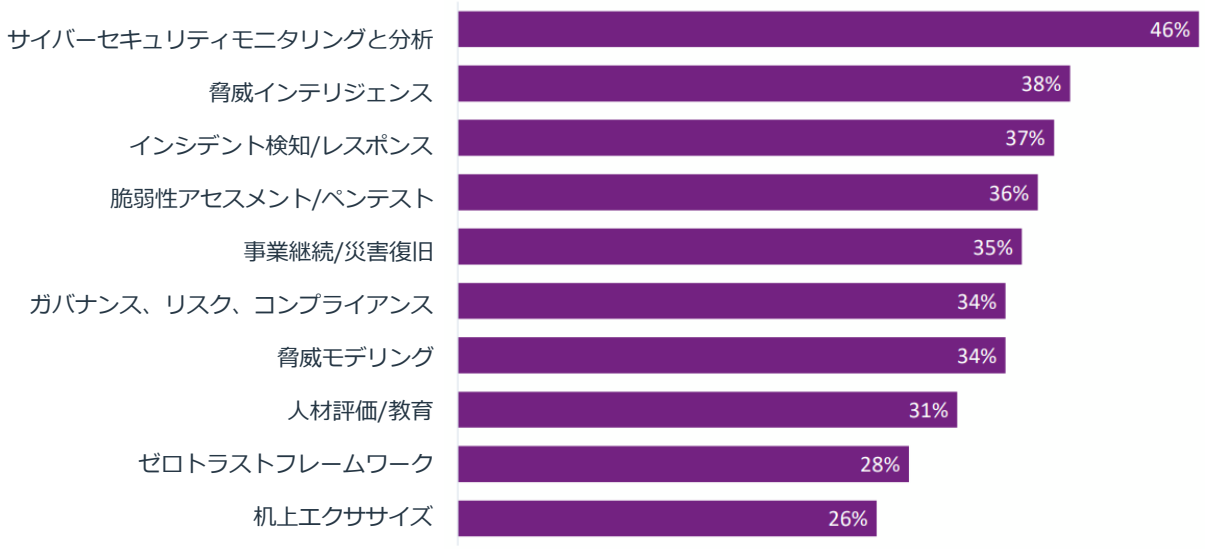
テクノロジー評価におけるサイバーセキュリティの役割



Source: CompTIA 2024 State of Cybersecurity | n=511 U.S. technical and business professionals

58%の企業が、新しい取り組み（イニシアチブ）を評価する際にサイバーセキュリティを主な考慮事項とみなしていますが、サイバーセキュリティを依然として二次的要因、あるいは後回しにしている企業が多いことも事実です。従来のIT部門の監視が少なくなった中でテクノロジー導入が進んでいることから、組織は、新しいシステムを議論する際にサイバーセキュリティが最前線かつ中心にあることを確認する必要があります。

組織のサイバーセキュリティ戦略の要素

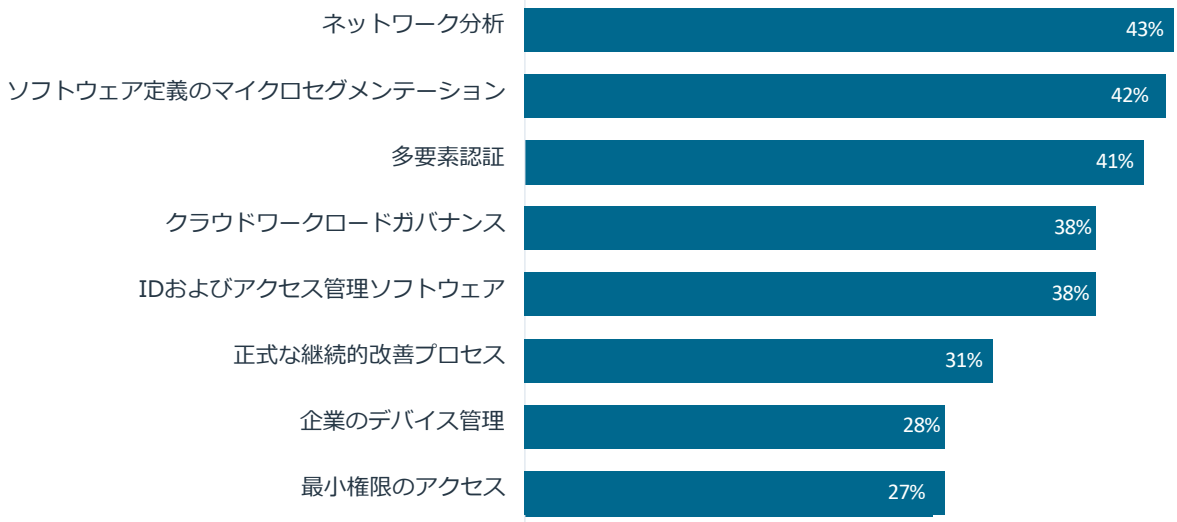


Source: CompTIA 2024 State of Cybersecurity | n=511 U.S. technical and business professionals

2. サイバーセキュリティは他のビジネス活動に影響を与えている

・**脅威インテリジェンス**には現在、ソーシャルエンジニアリングやランサムウェア攻撃などテクノロジーと現実が交差する新しいタイプのサイバー脅威が含まれています。
・**規制問題**やデジタルビジネスを監督する政府機関により、組織はビジネスの進め方をより認識するようになっています。
・リモートやハイブリッドワークが続く中、**従業員教育**によるセキュアプラクティスを維持する各従業員の責任はかつてないほど高まっています。

サイバーセキュリティ戦略に含まれるプラクティス



Source: CompTIA 2024 State of Cybersecurity | n=511 U.S. technical and business professionals

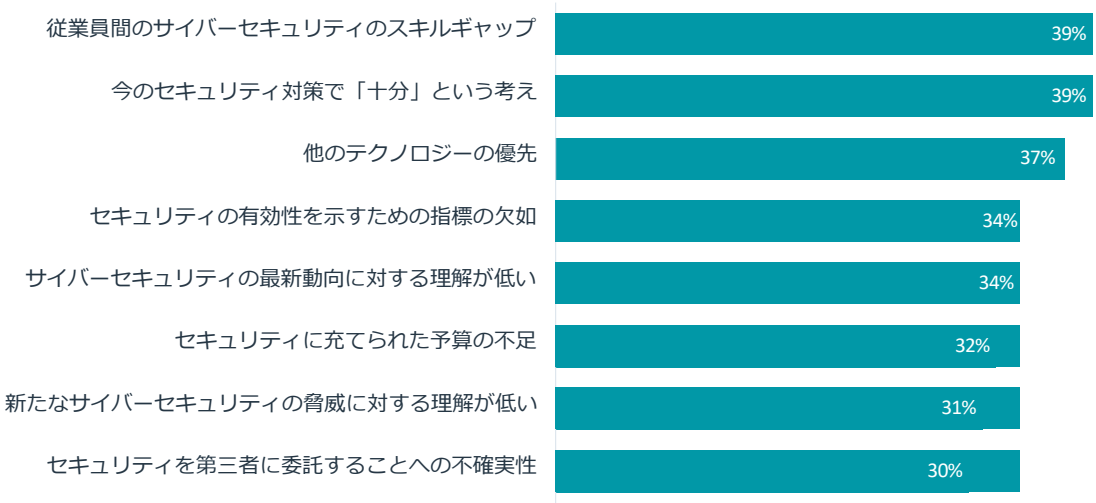
ゼロトラストフレームワークをサイバーセキュリティ戦略の一部として捉えている企業は28%に止まりますが、一般にゼロトラストのアプローチに含まれる個別のプラクティスを取り入れる企業は増加しています。

3 人材：企業がスキルのレジリエンスを高めることで、人材のパイプラインが強化される

組織は、従業員全体のサイバーセキュリティスキルの重要性を明確に認識しています。CompTIAのCyberseekツールによると、2022年5月から2023年4月までに米国では66万件以上のサイバーセキュリティ関連の求人があり、パンデミック下の2020年の同時期と比べて28%増加しました。

サイバーセキュリティの最大の課題は何ですか？ 回答者の課題を見てみましょう

サイバーセキュリティの取り組みにおける課題

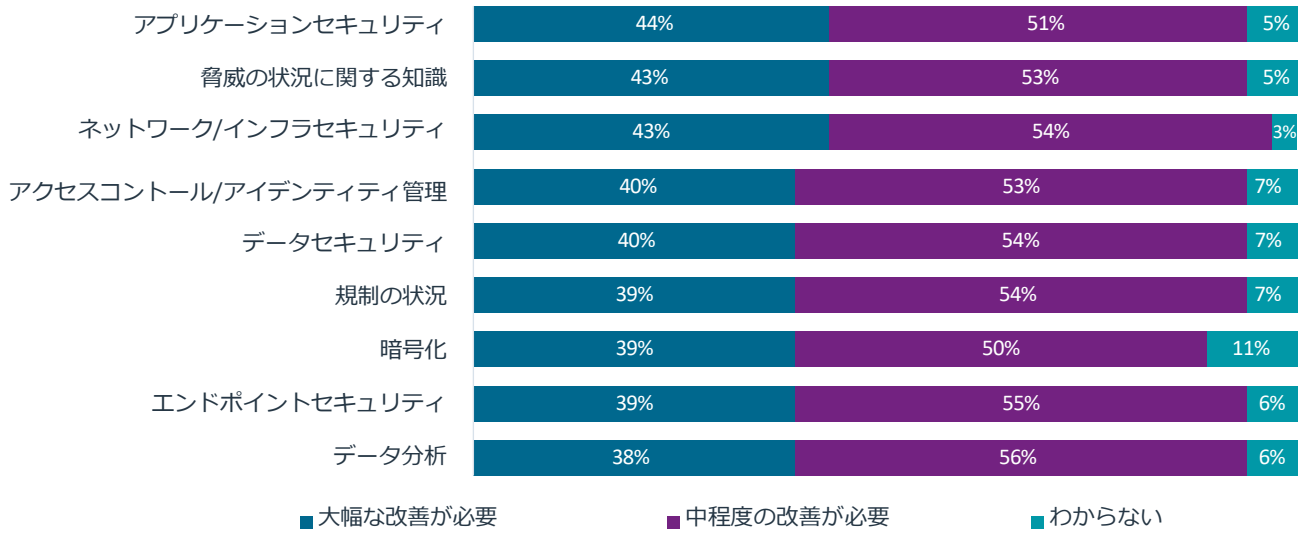


Source: CompTIA 2024 State of Cybersecurity | n=511 U.S. technical and business professionals

サイバーセキュリティの取り組みを推進する上での最大の課題は、サイバーセキュリティのスキルギャップです。ギャップを埋めるための有効な選択肢の1つは、経験の浅いサイバーセキュリティプロフェッショナルを迎え入れ、企業文化や目標を理解しながらスキルを高めてもらうことです。

採用のルートに関わらず、新しい人材が組織に加わる時や、社内の従業員がサイバーセキュリティに異動する時には、何らかのスキルギャップが存在します。

サイバーセキュリティ担当の要改善エリア

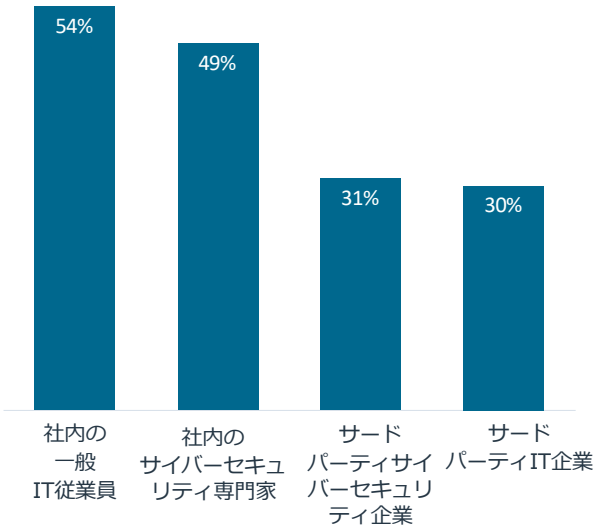


Source: CompTIA 2024 State of Cybersecurity | n=511 U.S. technical and business professionals

業界の専門知識とベストプラクティスに基づいた定期的なスキル評価を計画することは、スキルギャップの正確な性質を理解するための重要なステップとなります。

サードパーティの利用については？ 回答者の状況を見てみましょう

サイバーセキュリティの取り組みに携わるグループ



利用するサードパーティの種類

1. 主要IT製品を提供するマネージドサービスプロバイダー
2. サイバーセキュリティに特化したマネージドサービスプロバイダー
3. サイバー/物理セキュリティを提供する総合セキュリティ企業
4. 技術ビジネスサービスを提供する企業
5. セキュリティを製品に組み込むクラウドプロバイダー

Source: CompTIA 2024 State of Cybersecurity | n=511 U.S. technical and business professionals
n=314 U.S. technical and business professionals using third parties for cybersecurity strategy

今日、組織はベンダーやパートナーを選ぶ際、より包括的なアプローチを取っています。何よりもまず、エンドユーザーは、現代の脅威の状況を理解し、脅威インテリジェンスにアクセスできる企業を探しています。

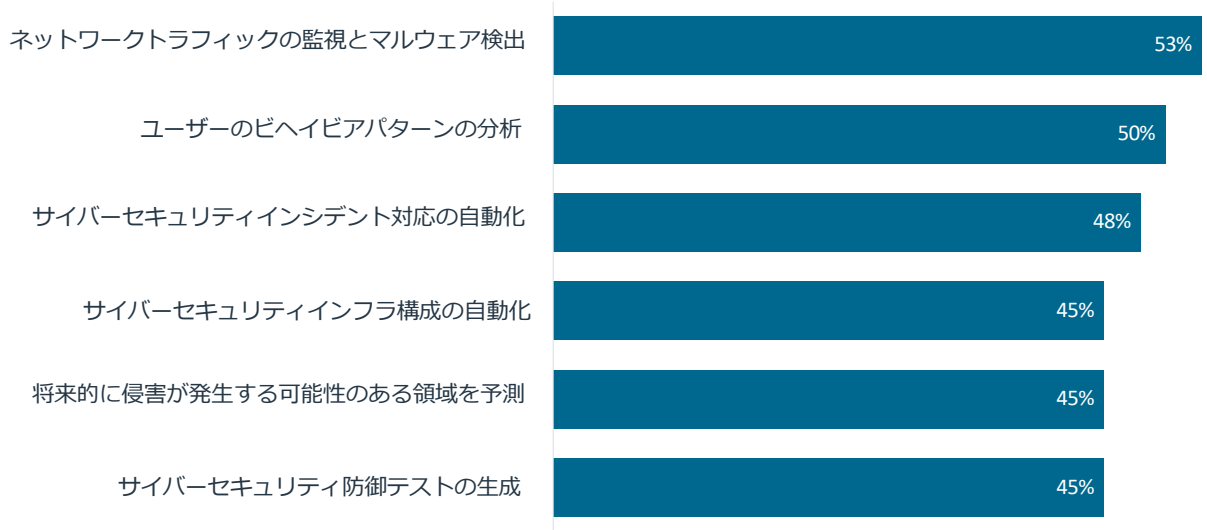
4 製品：AIがサイバーセキュリティ製品を新たな高みへと押し上げる

生成人工知能（AI）が話題になっています。多くの人は、このAIの新たな波は、ここ数十年で最大のテクノロジーパラダイムシフトであるといいますが、多くの企業は以前からAIを使用しているのです。

回答者の56%は、すでにAIと機械学習 (ML) を使用していると回答しています。
36%は、使用していないが、可能性を模索しているといいます。

サイバーセキュリティにおけるAIの可能性とは？ 回答者の見解を見てみましょう

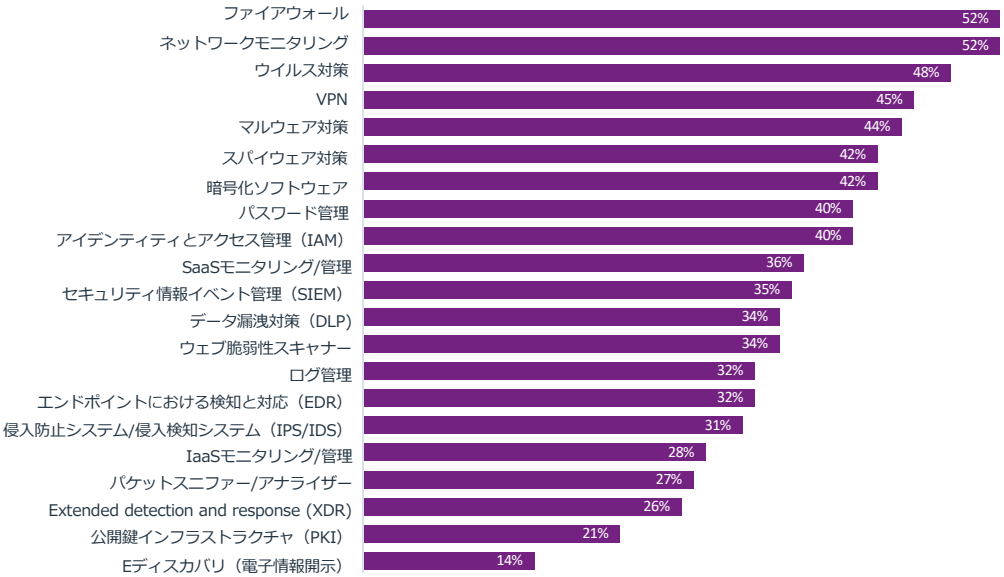
サイバーセキュリティにおけるAIの潜在的な用途



Source: CompTIA 2024 State of Cybersecurity | n=511 U.S. technical and business professionals

もちろん、AIも他の新興テクノロジーと同じで、それ自体はスタンドアローン製品ではなく、他の製品の組み込まれるコンポーネントです。

使用されているサイバーセキュリティ製品



Source: CompTIA 2024 State of Cybersecurity | n=511 U.S. technical and business professionals

サイバーセキュリティリソースはここ数年で着実に拡大しており、さまざまなサイバーセキュリティツールを管理するという課題は、それぞれにAI機能が組み込まれていることでさらに複雑になっています。

Methodology 手法

この定量的調査は2023年第3四半期に、サイバーセキュリティに関わるビジネスおよびITプロフェッショナルを対象としたオンライン調査から構成されています。米国で活動する511名が調査に参加し、95%の信頼性でのサンプル誤差は+/−4.4%ポイントでした。海外地域（ANZ、ASEAN、ベネルクス、DACH、イギリス/アイルランド）については、各地域で合計125名のプロフェッショナルが調査に参加し、95%の信頼性における全体のサンプリング誤差は±8.9%ポイントとなりました。サンプリングエラーは、データのサブグループほど大きくなります。

どの調査でもそうであるように、標本誤差は起こり得る誤差の原因の一つにすぎません。非標本誤差を正確に計算することはできないため、その影響を最小限におさえるために調査設計、データ収集と処理のあらゆるフェーズで予防的ステップがとられました。

CompTIAはすべての内容および分析に責任を負います。当調査に係るいかなる質問も、CompTIA Research and Market Intelligenceのスタッフが対応します。メールアドレスはresearch@comptia.org です。

CompTIAは市場調査業界のInsights Associationの一員であり、世界的に尊重されているその標準および倫理規定を順守しています。

CompTIAについて

CompTIA（the Computing Technology Industry Association）は、ITエコシステム、そして5兆ドル規模の世界的の動力であるテクノロジーを設計、管理、保守している約7,500万の業界やITプロフェッショナルを代表する、業界団体です。教育、トレーニング、認定資格、政策支援、慈善活動や市場調査を通し、CompTIAはIT業界とそのワークフォースが進歩するためのハブとなっています。

CompTIAは世界有数のベンダーニュートラルなIT認定団体であり、提供されるパフォーマンスベースの試験による認定者数は300万以上にのぼります。CompTIAはエントリーレベルからエキスパートレベルのプロフェッショナルまで、テクノロジー分野におけるキャリアのあらゆるステージでの成功に欠かせない業務能力を評価します。また、慈善活動として、CompTIAは革新的なオンランプ（入口）およびキャリアパスを開発しました。これは、従来、ITワークフォースとして活躍することの少なかった人々に対する機会を拡大するものです。

CompTIA

CompTIA.org

CompTIA is responsible for all content and analysis. Any questions regarding the report should be directed to CompTIA Research and Market Intelligence staff at research@comptia.org.