CompTIA

State of Cybersecurity 2025

Developing strategy using enterprise architecture

STATE OF CYBERSECURITY 2025

Introduction

2020年代の大部分において、テクノロジー業界は圧倒的な勢いを誇っています。パンデミックの間、テクノロジーに関連した製品や職業は、リモートワークとオンラインコマースへの転換を可能にする主要な原動力としてあげられました。パンデミック明けには、企業はテクノロジー投資と雇用を倍増させ、失われた勢いの取り戻しを図ります。そして、特に生成AIの導入により、テクノロジーは将来の成長への展望を提供し続けています。

2024年半ば、市場の現実に衝突します。企業が金利上昇とデジタル変革の複雑さに苦慮するなか、技術職の雇用における減速が生じました。AIへの期待が高まる一方、コストと有効性に関する疑問が浮上し、7月のCrowdStrikeのインシデントは高度にインテグレートされたテクノロジースタックの脆弱性、さらにはテクノロジー問題が起きた場合の人の介入が必要であることを浮き彫りにしました。

すべての市場サイクルがそうであるように、減速は一時的なものとなるでしょう。ここでの問題は、企業がこのような状況から何を教訓として学ぶかということです。初期段階に見られたデジタル疲れやフラストレーションは、組織が戦略的テクノロジーを活用したワークフローの課題に関する考え方と文化を完全に受け入れていないことの表れでもあります。

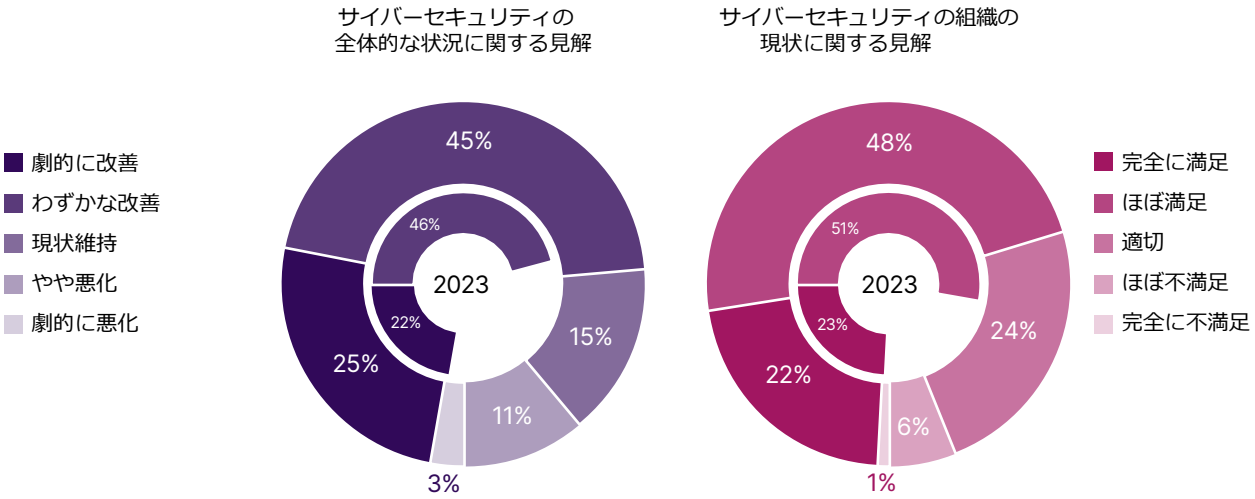
CompTIAのState of Cybersecurityのレポートにおいて、一貫して取り上げられているテーマの1つは、サイバーセキュリティ分野の劇的な変化です。単にどの製品が優れた防御を提供できるかではなく、サイバーセキュリティは今や、デジタル資産の保護やデータのプライバシー、規制への準拠、業務の信頼性を確保するプロアクティブなプロセスでなければなりません。

従来の市場指標は、サイバーセキュリティの将来について明るい見通しを示しています。IDCは、サイバーセキュリティ製品の世界的収益が2022年から2023年にかけて、15.6%増加したと報告しています（Gartnerの推定ではIT支出全体の増加率は3.3%）。IDCは、2023年以降の5年間、サイバーセキュリティ市場が2桁ペースで成長を続け、2028年には2,000億ドルに達すると予想しています。

雇用の観点から見ると、CompTIAのCyberseekツールでは2023年5月から2024年4月の間に、サイバーセキュリティ関連のスキルを求める米国ベースの求人が約47万件あること示しており、さまざまな職種にわたりサイバーセキュリティスキルに対する幅広い需要があることがわかっています。サイバーセキュリティ専門職については、CompTIAのState of the Tech Workforce 2024によると米国のサイバーセキュリティ雇用は成長率267%を上回る成長が見込まれています。

しかし、計画された投資とその結果の間には依然として乖離があります。本リサーチで調査対象となる6地域全体では、セイバーセキュリティの全体的な方向性が劇的に改善していると感じている人はわずか25%で、所属する組織のサイバーセキュリティの取り組みが完全に満足のいくものであると評価する人はわずか22%でした。

肯定的意見の進展がスローなのは、異なるアプローチの必要性を示している

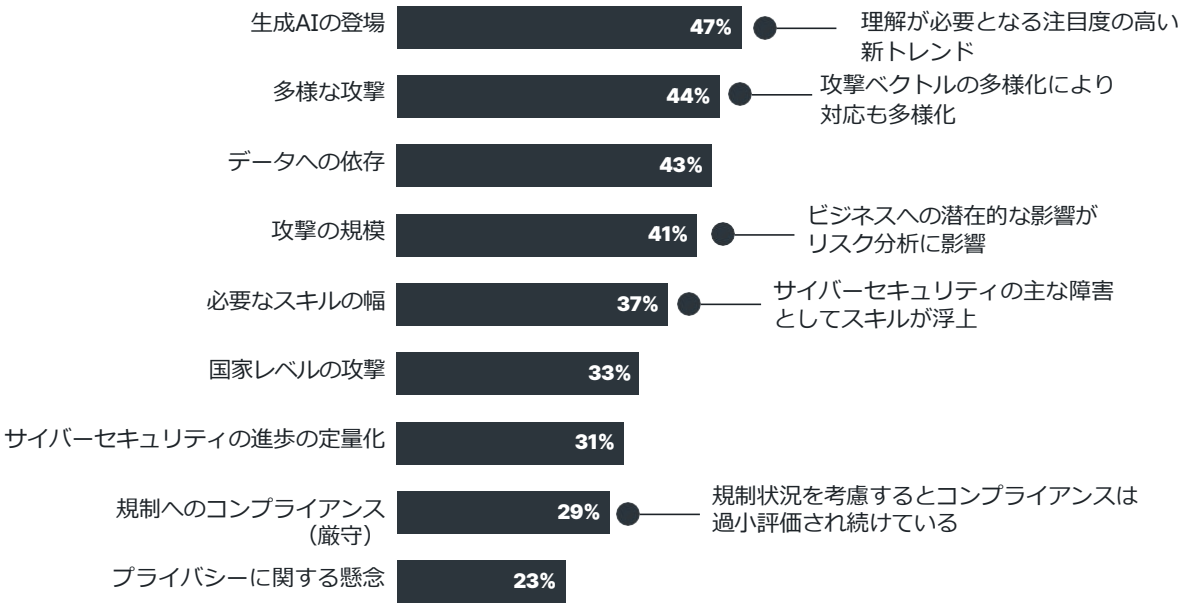


Source: CompTIA State of Cybersecurity 2025 | n=1,181 | 2023 n=1,167

これらのデータ結果はここ数年、中立的な状態が続いています。「わずかな改善」や「ほぼ満足」といった意見は大幅に増えていますが、サイバーセキュリティの重要性を考えると最も良いレベルを目指すのは当然のことです。組織が取っているアプローチ、あるいは理想的なサイバーセキュリティはどうあるべきか？という期待において、何かが欠けています。

サイバーセキュリティの懸念を引き起こしている問題のリストは、企業が導入戦略の弱点に対処する際に直面する課題をさらに浮き彫りにしています。サイバーセキュリティの改善が単に最新のテクノロジーを購入するだけの作業だった時代は終わったのです。今日のサイバーセキュリティの問題に対処するには、企業は、サイバーセキュリティのテクノロジースタックだけではなく、資産保護を確実にするプロセスや最先端の専門知識を提供する組織構造においても議論する必要があります。

サイバーセキュリティの推進要因は、さまざまな潜在的行動を示す



Source: CompTIA State of Cybersecurity 2025 | n=1170

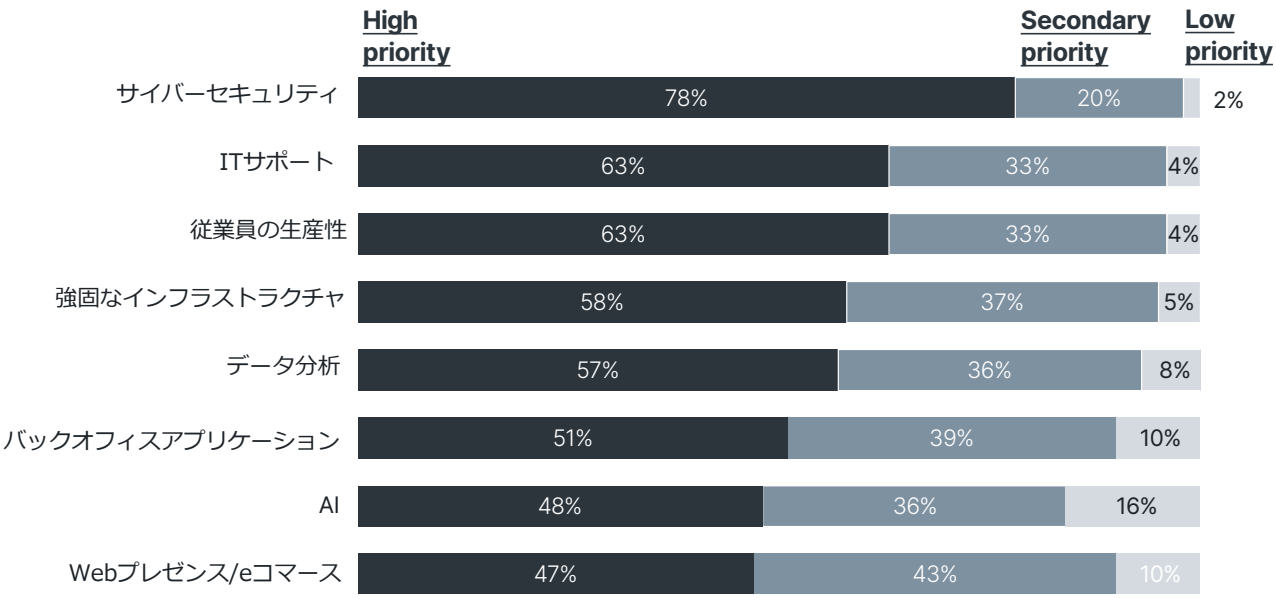
エンタープライズアーキテクチャフレームワーク全体におけるサイバーセキュリティの必須事項

戦略的なテクノロジーの考え方と、強固なサイバーセキュリティアプローチのジレンマは、密接に絡み合っています。サイバーセキュリティの取り組みは、テクノロジー運用の変化に対応するだけでなく、これまで以上に意思決定プロセスに大きく影響する必要があります。組織がこの両方を解決するとき、エンタープライズアーキテクチャモデルの4つのレイヤーは、意思決定を行うための構造を提供することができます。広範なビジネスの視点から出発し、アプリケーション、データ、テクノロジーを掘り下げていくことで、企業が効果的なサイバーセキュリティに向かう際の優先順位を設定し、トレードオフを特定することができます。

1 ビジネス アーキテクチャ

ほとんどの場合、エンタープライズアーキテクチャモデルを全体的なテクノロジーの取り組みに適用することで、4つの主要テクノロジー領域（インフラストラクチャ、ソフトウェア、データ、サイバーセキュリティ）すべてにまたがる問題に着目することができます。しかしサイバーセキュリティは、事業存続により直接的な影響を与えるという点で、これら領域の中でも特殊です。それゆえ、サイバーセキュリティは、スタッフ、マネージメント、経営幹部、統治機関など組織のあらゆるレベルにとって考慮すべきビジネス上の必須事項となっています。こうした重要性から、エンタープライズアーキテクチャモデルは、より広範なテクノロジー戦略とともに、サイバーセキュリティの取り組みに直接適用することができます。

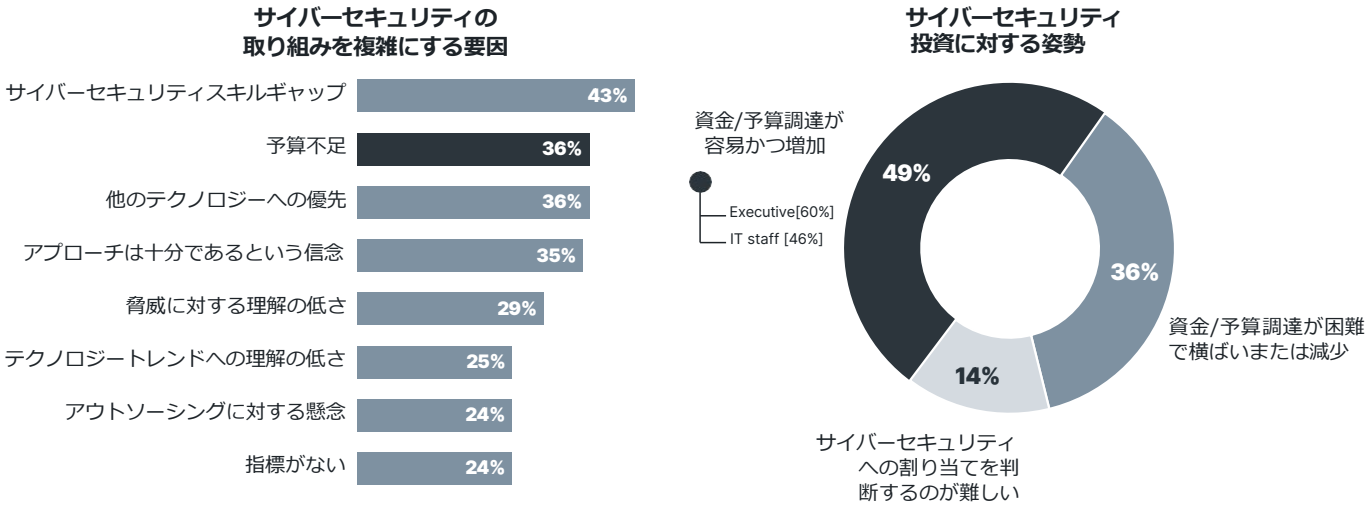
サイバーセキュリティが組織の優先順位のトップに



Source: CompTIA State of Cybersecurity 2025 | n=525

ビジネスアーキテクチャレベルでは、解決すべき主な問題は、組織内の優先順位に基づいたサイバーセキュリティに関する継続的な運用プロセスです。最初の投げかけは、企業がサイバーセキュリティにどのような優先順位を置いているか？です。サイバーセキュリティにフォーカスした調査データには多少の偏りがあるかもしれませんが、サイバーセキュリティがさまざまなテクノロジイニシアティブの中で最優先事項としてランク付けされていることは驚くことではありません。サイバーセキュリティインシデントは注目度が高く、影響も広範囲に及ぶため、組織が優先順位を高く設定するのは当然のことです。

予算の問題は、組織がサイバーセキュリティを解決するのが依然難しいことを示している



Source: CompTIA State of Cybersecurity 2025 | n=525

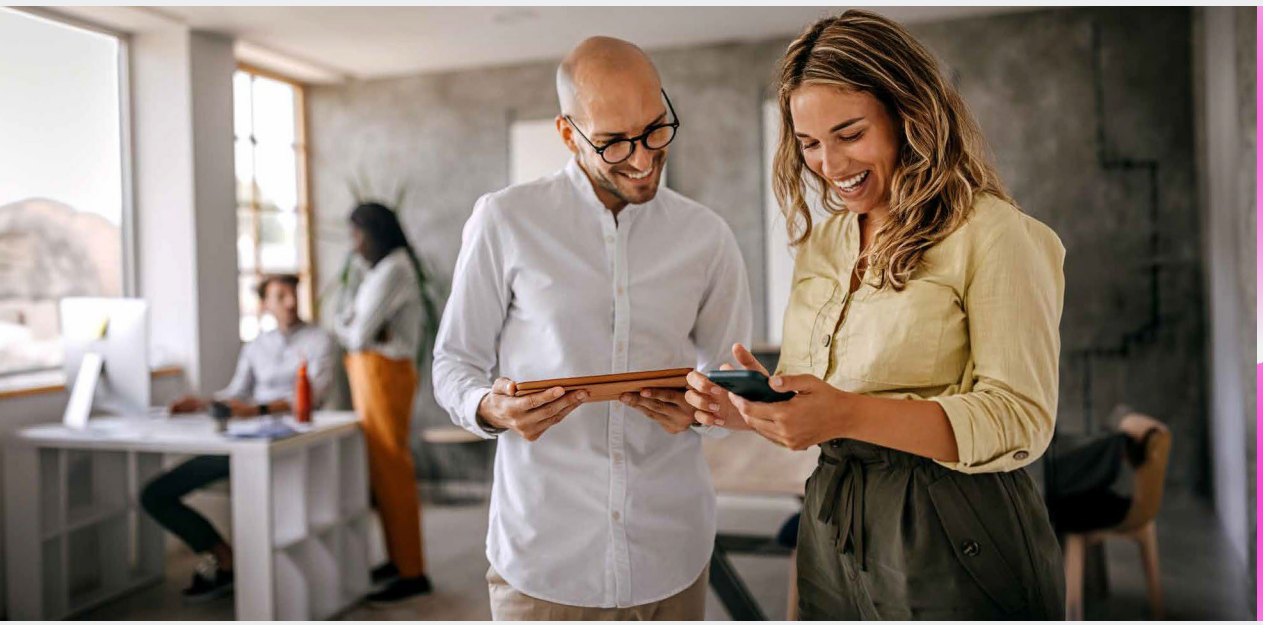
しかし、実際の行動と照らし合わせると、食い違いが明らかになります。まず表面化するのは、予算の割り当てです。数年にわたるCompTIAの調査では、サイバーセキュリティイニシアチブを推進する上での主な難しさは、組織の考え方の克服であることがわかっています。昨年は、スキルギャップが主な障害としてトップを占めました。今年は、予算不足と他のテクノロジーイニシアチブへの優先が、スキル問題に加わり、大きな課題となっています。

サイバーセキュリティが他の活動に織り込まれているため、サイバーセキュリティの予算額を割り出すのは非常に困難です。クラウドインフラストラクチャプロバイダーの選択やコンプライアンス監査の実施は、他部門が主導する場合がありますが、サイバーセキュリティチームが大きな役割を果たしていることは明らかです。とは言え、サイバーセキュリティの資金調達に関する姿勢においても、食い違いが見られます。回答者の78%がサイバーセキュリティは自社の優先事項であると述べる一方、サイバーセキュリティ活動のための資金調達は比較的容易または増加していると感じているのは49%にすぎません。60%の経営幹部がサイバーセキュリティの資金は比較的容易に調達できると答えているのに対し、ITスタッフではわずか46%です。

優先順位に沿ったプロセスにおいて合意を得るには共同作業が必要です。
ビジネスリーダーにとっては、企業構造の検討、つまりサイバーセキュリティチームの構成やガバナンス慣行におけるサイバーセキュリティの関与を伴う場合があります。サイバーセキュリティリーダーは、サイバーセキュリティが事業存続に与える影響についてより深い理解が必要になります。このような高いレベルの影響を判断するには、エンタープライズアーキテクチャモデルの下位レイヤーにサイバーセキュリティの原則を組み込むことが重要です。

ガバナンスの二つの側面

サイバーセキュリティの議論では、「ガバナンス」と聞くと一般に、規制へのコンプライアに関する問題を思い浮べます。この点は、医療や金融など規制の厳しい業界や地域において特に当てはまります。コンプライアンスの必要性は現実であり、高まりを増していますが、企業が考慮すべきガバナンスにはより広い視点があります。サイバーセキュリティとデータの分野は、数十年にわたる経験から文書化されたフレームワークとベストプラクティスがあるインフラストラクチャとソフトウェア開発の分野ほど確立されていません。サイバーセキュリティでは、リスク分析やインシデント対応などの特定のトピックに関するベストプラクティスが生まれており、これらの個々の要素が全体的なフレームワークとなりつつありますが、そのフレームワークは企業戦略にさらに統合される必要があります。サイバーセキュリティのプロフェッショナルにとって、ガバナンスの両側面のバランスを保つことは、長期計画を定義する上で重要となります。

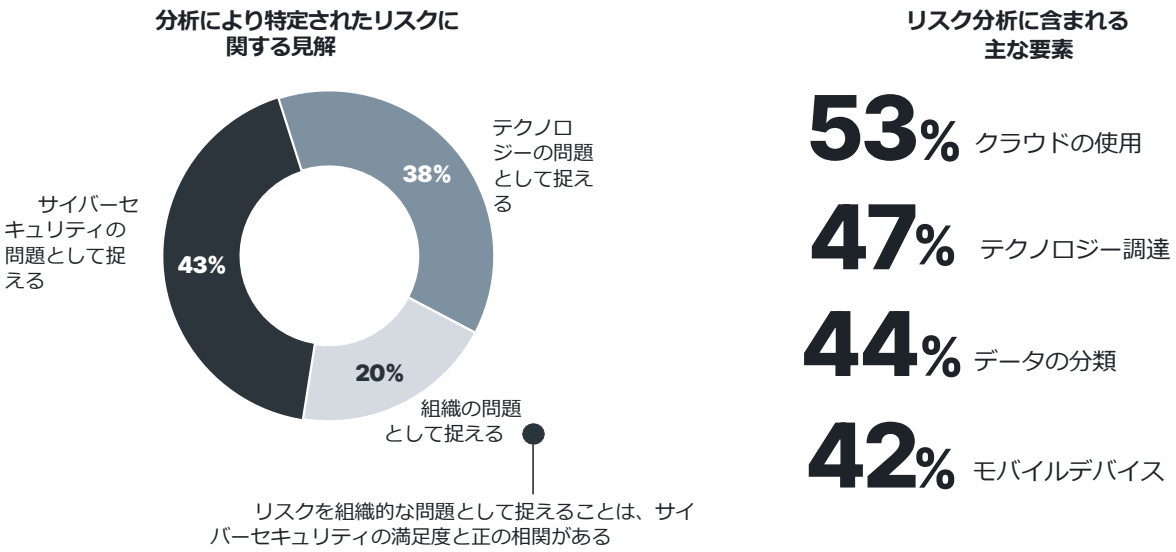


2 アプリケーション アーキテクチャ

アーキテクチャモデルにある、次の2つレイヤーの順序については、見解が分かれています。ある視点から見れば、データレイヤーは社内業務に使用される個々のアプリケーションよりも基礎的なものとされます。一方で、アプリケーションは全体的なワークフローに統合され、そのワークフローを定義することは技術的な意思決定に影響を与えます。本レポートではアプリケーションアーキテクチャのより包括的な視点を見解を採用します。

リスク分析は、ワークフローを定義する重要な要素であり、サイバーセキュリティの取り組みの指標にもなっています。リスク分析の具体的な実践方法は組織により多少異なりますが、CompTIAのデータでは、公式または非公式のリスク分析手順が比較的多く採用されていることがわかっています。予想通り、NST Risk Management FrameworkやIRGC Risk Governance Frameworkなどの公式なフレームワークの使用は、大企業でより一般的となっています。しかし、非公式のリスク分析を行う中小企業の割合が高いため、リスク管理はほとんどの企業にとって身近な概念となっています。

リスク分析と低減は組織全体のプロセスであるべき



Source: CompTIA State of Cybersecurity 2025 | n=511

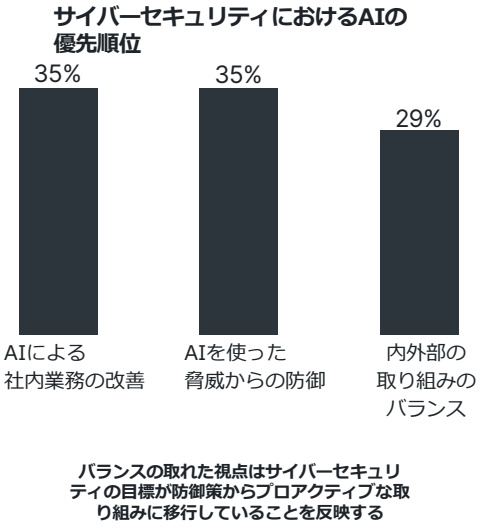
しかし、ここでも細部が重要です。最も重要な点は、リスク分析のアウトプットが組織の幅広い懸念事項として考慮されないことが多いということです。大多数の企業は、リスク分析をテクノロジー部門に限定された活動と捉えていて、さらに10社中4 社以上が、リスク分析はサイバーセキュリティプロフェッショナルに特化したものであると回答しています。

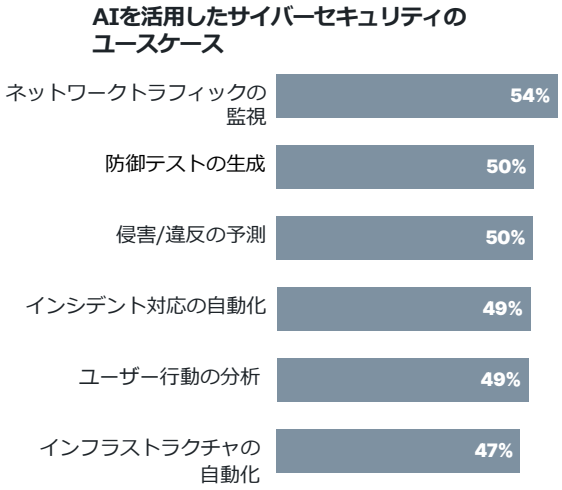
確かに、分析で最も多く確認されたリスクは、テクノロジー要素を中心にしたものでした。クラウドの使用、テクノロジー調達、データの分類、モバイルデバイスの実装といったコアコンポーネントはすべてテクノロジーに関連しています。しかし、分析はこれらコンポーネントごとのセキュリティ対策に限定されるべきではありません。セキュリティ選択のコストとトレードオフは、組織の目標に照らして評価されなければなりません。

今日、企業の願望とサイバーセキュリティ分析の両方で取り上げられている最も顕著なテクノロジーコンポーネントは、人工知能です。AIは数年前から新興テクノロジーの議論の一部でしたが、生成AIの登場により、新たなハイプサイクルが始まりました。当然のことながら、企業はこの新しいトレンドからできるだけ多くの価値を得たいと考えています。それが可能かどうかは、進化するテクノロジースタックにAI がどのように適合するかをしっかりと理解しているかどうかにかかっています。

あらゆるハイプサイクルと同様に、初期の興奮は実装という障害にぶつかっています。標準的な4段階の導入曲線では、企業の41%が教育/パイロットプログラムを実施していると回答し、36%が優先度の低い実装を行っていると回答しています。つまり、大半の企業がAIジャーニーの始まりにいることを意味します。これは新しいテクノロジーではよくあることですが、メディアや最先端のエンタープライズ企業が抱く期待とは逆かもしれません。歴史が物語るように、内外の要因によって進歩が妨げられ、「優先度の高い実装」とする企業が16%、「ワークフローの全面的な変革」とする企業が7%と、進展が見られないことがわかります。

AIはサイバーセキュリティの取り組みを自動化し加速させる可能性を秘めている





Source: CompTIA State of Cybersecurity 2025 | n=525

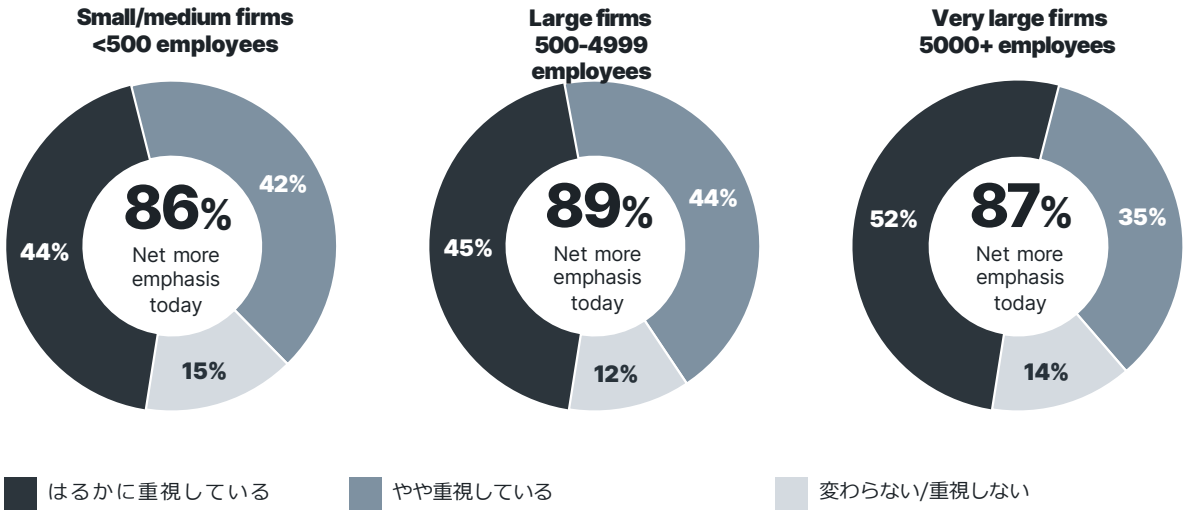
サイバーセキュリティの観点から見ると、AIは両方の側面で役割を果たしています。企業は、AIを社内で活用して防御力を高めることに重点を置くか、AIを使った新しい攻撃形式について学習することに重点を置くかで意見が半々に分かれています。いずれのアプローチも、AIが現代のサイバーセキュリティをさらに複雑化していることを示しています。予想されるユースケースには、自動化やデータ分析など、企業がすでに苦労しているさまざまな活動が含まれます。

3 データアーキテクチャ

データアーキテクチャは、意思決定の観点からはアプリケーションアーキテクチャに続きますが、優先順位の観点からではありません。全体として、企業の46%が、2年前と比較して現在では、データをはるかに重視していると回答しています。非常に大規模な企業が、データ管理と分析に投入できるリソースを武器に、この取り組みをリードしています。データ分析と視覚化によってデータドリブンの意思決定が強化されたため、経営幹部もこの考え方を推進しています。

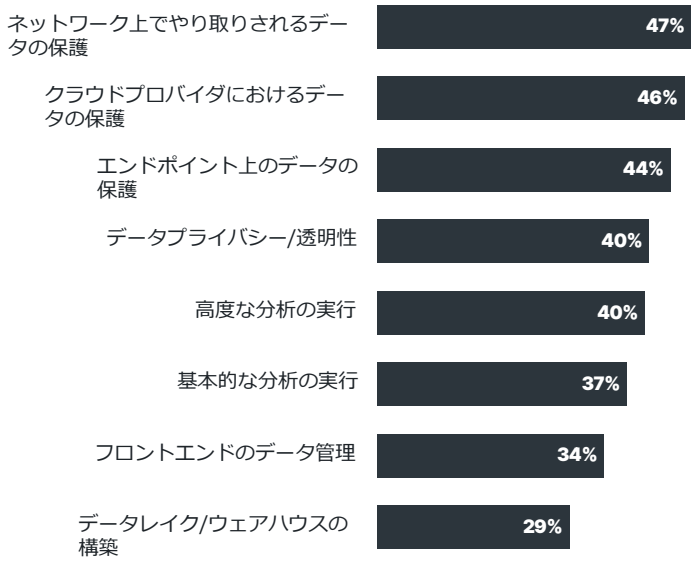
データの重要性が高まった理由はいくつかありますが、データとサイバーセキュリティの分野には大きな重なりがあります。コンピューティングリソースが企業間である程度コモディティ化されるにつれて（特にクラウドの導入により）、データは差別化を図る上で重要な領域になりました。最近では、AIへの関心が高まり、AIアルゴリズムのトレーニングに適したデータを生成する堅牢な手法の必要性が高まっています。

2年前と比較して現在では、データははるかに重視されている



Source: CompTIA State of Cybersecurity 2025 | n=525 | Smaller n for subsegments

データ分野の重点分野はサイバーセキュリティと強い相関関係がある



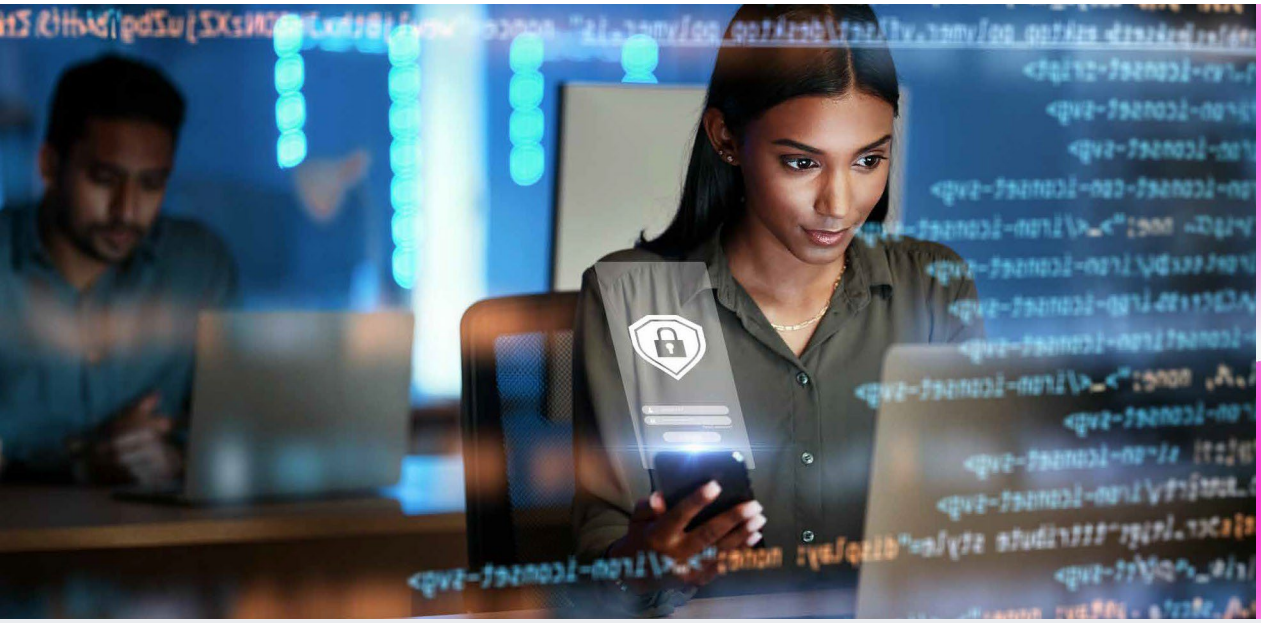
組織は、保存中、移動中、使用中のデータを保護するとともに、高度なテクニックを可能にする基礎的なデータ管理手法の構築に取り組んでいます。AIの台頭により、AIアルゴリズムを適切にトレーニングするための堅牢なデータ手法の必要性が加速。企業が競争上の差別化を模索する中で、データサイエンスの需要は引き続き高まっています。

Source: CompTIA State of Cybersecurity 2025 | n=525

このようなデータへの依存は、サイバーセキュリティと重なる最初の点です。データ管理と分析のさまざまな要素の中でも、データのセキュリティ保護は明らかに最優先事項です。クラウド運用のセキュアペリメーターが排除されたことで、データとアプリケーションの両方に重点を置いたセキュリティが実現し、サイバーセキュリティチームは、使用の各段階でデータを保護するための方法を今も構築中です。データの保護はおそらく、ゼロトラストフレームワークの主要な考えでしょう。検証されていない破損データは、データに依存する運用に壊滅的な影響を与えかねないからです。

データとサイバーセキュリティにおける2つ目の重なりは、サイバーセキュリティプロフェッショナルが脅威を監視しインシデントに対応しながら独自のデータ分析を行うことで発生します。デジタル化の加速とリソースの制約により、サイバーセキュリティプロフェッショナルが処理しなければならない膨大な量の情報が生成されるため、状況を把握するには自動化とあわせて高度なデータ分析手法が不可欠です。

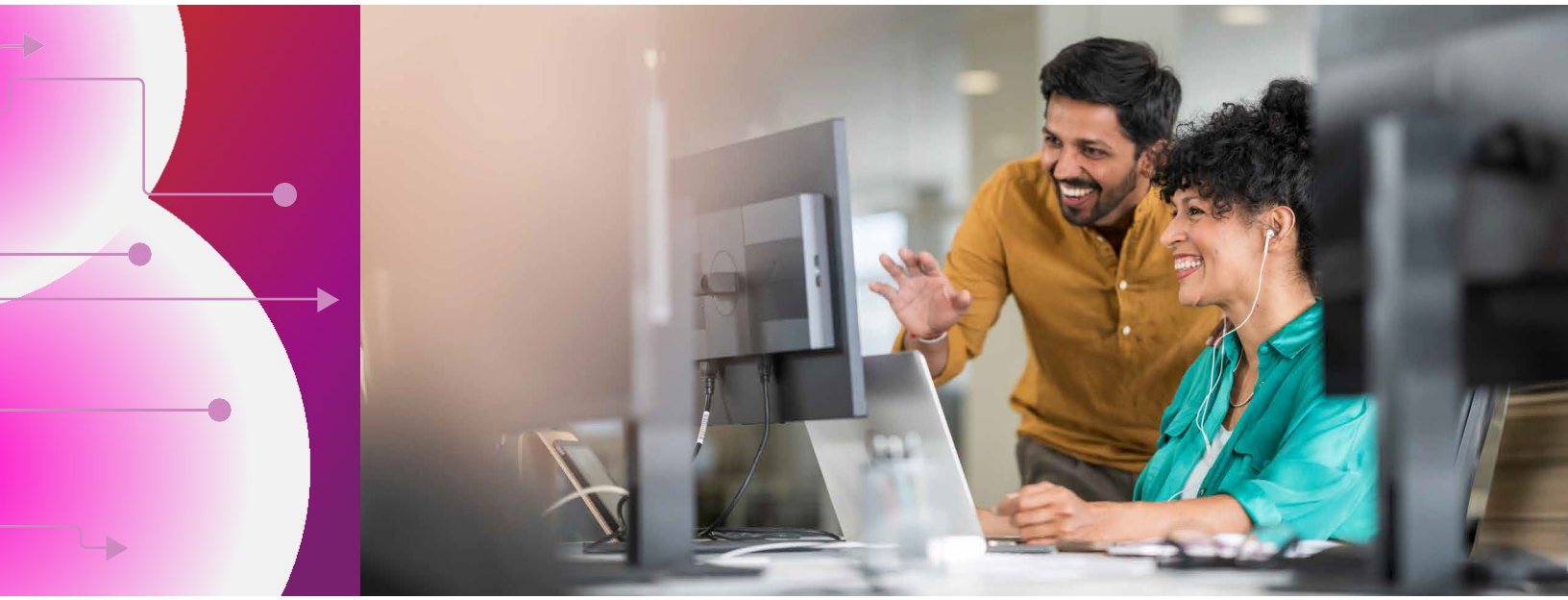
データは、組織がサイバーセキュリティ戦略の成功や進捗を定義するために使用している新しい指標を支える役割を果たします。過去1年間に新しいサイバーセキュリティ指標の使用を開始したと回答した企業はわずか29%ですが、経営幹部の38%が新しい指標を重要なプロセス改革として認識しています。これは、ビジネスの健全性に関する議論の一部としてサイバーセキュリティを組み込む必要があることを示しています。この必要性は、企業がテクノロジーで目標を推進するにつれて高まる一方です。



ゼロトラストの価値

過去5年間にわたり、「ゼロトラスト」はサイバーセキュリティに関する新しい考え方の有力候補になりました。古い考えを「セキュアペリメーター」とするのであれば、ゼロトラストは現代のデジタル環境におけるデータ、アプリケーション、ユーザービヘイビアに関する考え方の指標を提供します。ただし、この用語は混乱を招く可能性もあります。サイバーセキュリティの製品中心の歴史と、サイバーセキュリティチームとビジネスリーダー間の現在の協業を考えると、どの製品またはイニシアチブがゼロトラストに分類されるかといった疑問が生じます。ゼロトラストの成功を証明する指標がないため、状況はさらに複雑になっています。多くの行動がゼロトラストフレームワークに貢献しているため、サイバーセキュリティプロフェッショナルは、経営幹部のステークホルダーに対してゼロトラストを強調するのではなく、これらの要素（例えばアイデンティティアクセス管理や多要素認証など）に焦点を当てる必要があります。そうすることで、投資と成功の定義がより明確になり、ゼロトラストはサイバーセキュリティ チームが社内で使用する指針として残ることができます。

4 テクノロジーアーキテクチャ



エンタープライズアーキテクチャモデルの最下位レイヤーでは、戦術に焦点が当てられます。ここでは、攻撃から保護しリスクを減らす包括的ソリューションに統合されたテクノロジー製品という、従来のセイバーセキュリティの考え方に最も近い状況があります。

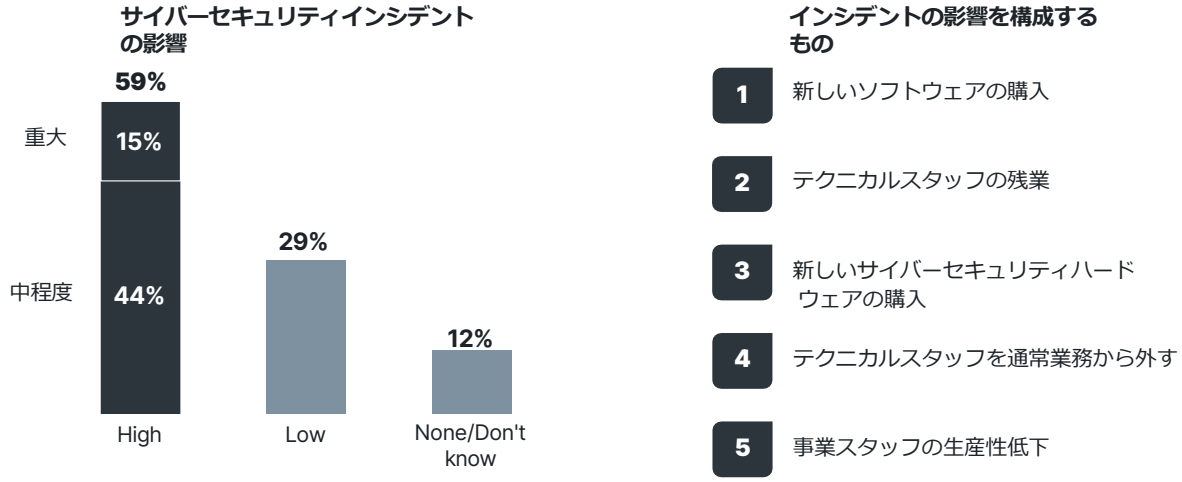
脅威の状況は変化しており、サイバーセキュリティプロフェッショナルにとって最初の戦術的な課題となっています。まず、脆弱な組織を狙うサイバー犯罪者がいることで長年の脅威が今も蔓延しています。マルウェアは数十年にわたって進化してきましたが、多くのコアプリンシプルは変わっていません。一般的な防御策も同様です。それでも、マルウェアは、組織が理解を深めたいとしている懸念事項のトップ3に挙げられています。

他の2つは、ランサムウェアとフィッシングです。これらは最近出現した攻撃ベクトルであり、サイバー犯罪者にとって非常に強力であることがわかっています。これら脅威に関する興味深い点は、予防と低減においてテクノロジーの果たす役割が小さいことです。代わりに、明確に定義されたプロセスと効果的なエンドユーザートレーニングがダメージを回避するための重要な要素となります。

これら3つの脅威だけでも、監視と低減に多大な時間と労力を要しますが、その他にも考慮しなければならない脅威は多岐にわたります。サプライチェーン攻撃は、自動化されたソフトウェア更新プロセスと複雑なテクノロジースタックを悪用します。データポイズニングは、多くの企業が構築の初期段階にあるデータ管理プロセスを歪め悪影響を与えます。サイバー恐喝はランサムウェアの一種で、攻撃者は単にデータを使えなくするのではなく、データを公開すると脅します。

もちろん、外部要因は組織にとって唯一、あるいは最大の懸念事項とも限りません。内部の人的エラーは、サイバーセキュリティ事象において依然として重要な役割を果たしています。フィッシングやソーシャルエンジニアリングは、エンドユーザーのミスを悪用し、その攻撃は極めて巧妙になっています。加えて、企業が挙げるサイバーセキュリティインシデントで最も多いのは昔からあるデバイスの紛失です。

サイバーセキュリティインシデントは多大な混乱をもたらす

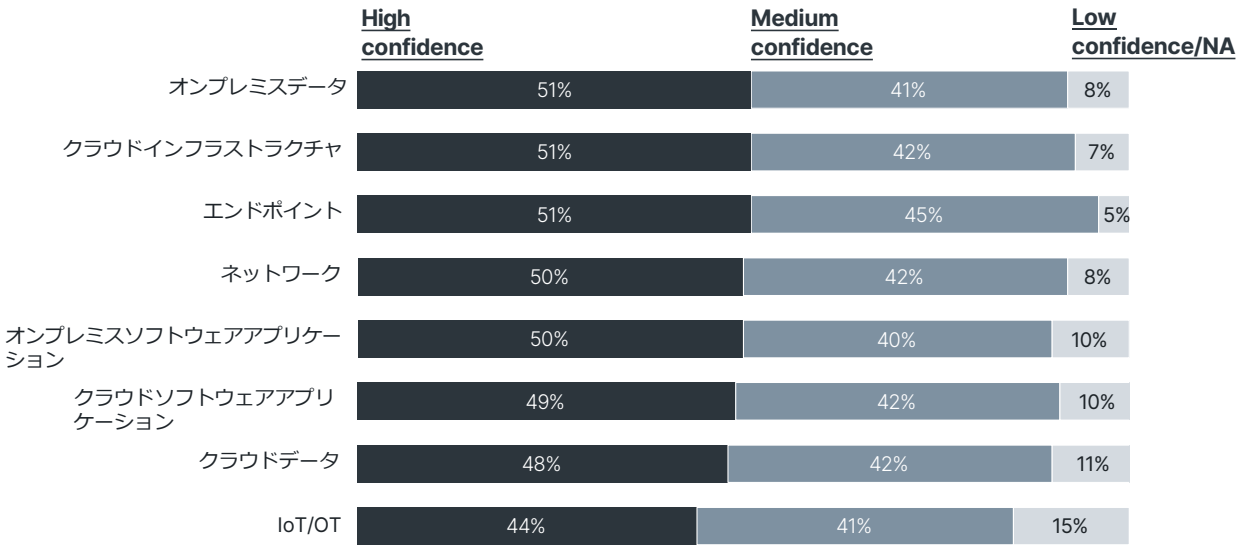


Source: CompTIA State of Cybersecurity 2025 | n=525

サイバーセキュリティインシデントの影響を見れば、ほとんどの企業にとって依然として重要な問題である理由は明確です。10社中6社近くが、過去1年間のサイバーセキュリティインシデントの影響は「中程度」～「重大」で、財務と生産性の両面に明らかな悪影響があったと回答しています。サイバーセキュリティが依然として優先課題であるのは、問題解決されていないからだと言うのは単純化しすぎですが、多くの組織が十分に理解できずにいる分野であることには変わりありません。

このような状況は、サイバーセキュリティチームが対処を求められる複雑さが爆発的に増大したことに起因するところが大きいでしょう。企業の60%が、エンドポイント、クラウドシステム、運用テクノロジー（OT）など、1,000を超える資産が管理対象であると回答しています。特にOTは、この複雑な環境の良い例と言えます。サイバーセキュリティプロフェッショナルは、デジタル化されネットワーク接続されたビルのユーティリティシステムや製造設備といった物理的なインフラストラクチャコンポーネントを理解する必要があるからです。

各資産カテゴリにおけるサイバーセキュリティの適用範囲に対する信頼度



Source: CompTIA State of Cybersecurity 2025 | n=525

すべての資産カテゴリにおいて、可視化と制御のレベルに対する信頼度が相対的に低いという厳しい現実があります。サイバーセキュリティの機能について最も知識があるとされるITスタッフは、一貫して信頼度が最も低いグループにいます。サイバーセキュリティが扱う脅威数が少なく、攻撃対象領域が小さいのであれば、この仕事はインフラ全体の責任の一部として処理することができます。しかし今日の環境では、異なるアプローチと高度なスキルが求められます。

5 サイバーセキュリティスキルの構築

組織がサイバーセキュリティ戦略において多層防御を考慮する必要があるのと同様に、サイバーセキュリティの専門知識においても多層的に構築する必要性が高まっています。サイバーセキュリティの責任をテクノロジージェネラリストに委ねる慣習は急速に消えつつあります。あらゆるテクノロジー分野のプロフェッショナルは、自身の分野に関連したサイバーセキュリティの洞察力をある程度備える必要があり、サイバーセキュリティチーム内では、高度に専門化された役割が数多く検討されています。

企業はサイバーセキュリティ対策の基盤として引き続き、社内リソースを重視しています。企業の半数以上が、人材戦略の一環としていずれも社内の専任セイバーセキュリティプロフェッショナルまたは、テクノロジープロフェッショナルを活用していると回答しています。2023年と比較すると専任スタッフを配置する企業数はわずかながら増加しています。

多くの企業にとって、サードパーティの活用は依然として、リソースの方程式の重要な一部であり、約3分の1の企業が専門のサイバーセキュリティプロバイダーまたはさまざまなテクノロジーサービスを提供するパートナーを活用しています。大企業は、小企業よりも専門プロバイダーやコンサルタントを利用する傾向にあります。これは小規模の顧客にサービスを提供するテクノロジー企業が、サイバーセキュリティに焦点を当てたサービスをポートフォリオに追加する機会を示しています。

スキルレベルと改善の必要性に関するデータは、詳細なスキル認識の欠如を示唆する

スキルドメイン	スキルレベル				改善の必要性		
	エキスパート	比較的高い	比較的低い	No experience	かなりの必要性	中程度の必要性	Don't know
ネットワーク/インフラセキュリティ	43%	44%	11%	2%	34%	59%	7%
脅威状況に関する知識	37%	48%	12%	3%	37%	58%	5%
アプリケーションセキュリテ	39%	53%	8%	1%	35%	58%	7%
データセキュリティ	45%	46%	7%	2%	37%	58%	5%
エンドポイントセキュリ	39%	48%	11%	1%	34%	59%	7%
ティ	40%	48%	11%	2%	35%	59%	7%
アイデンティティ管理	44%	44%	12%	1%	36%	58%	6%
データデータ分析	33%	50%	16%	2%	33%	58%	9%
規制の状況	29%	43%	23%	5%	49%	43%	8%
自動化/AI							

Source: CompTIA State of Cybersecurity 2025 | n=525

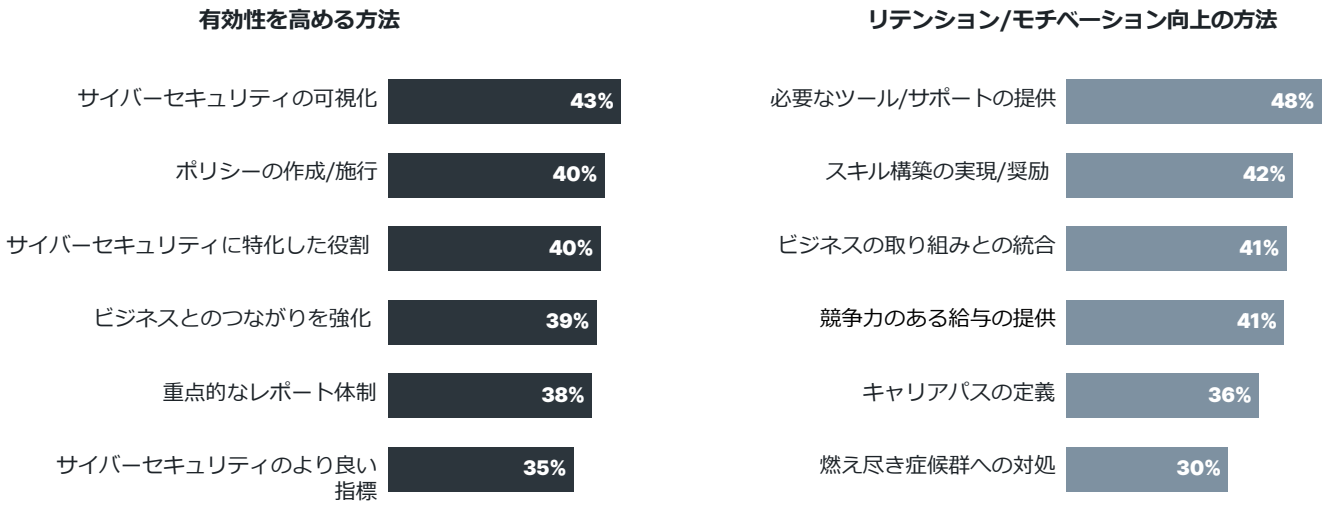
内部/外部リソースの両方に渡り、組織はサイバーセキュリティスキルの階層を構築しています。サイバーセキュリティが独立した分野として台頭した際、多くの企業にとっての最初のステップは、確立されたインフラのプロフェッショナルからサイバーセキュリティの専門家を育成することでした。サイバーセキュリティの実践が成熟化し、その範囲が拡大するにつれ、先進的な企業はしっかりとしたキャリアパスを備えた専門チームを構築しています。

サイバーセキュリティスキルの評価と需要が、このチーム構築アプローチの原動力となっています。以前のCompTIAリサーチもそうであったように、組織はスキルが比較的高いとされる分野でも改善の必要性を訴えています。ネットワークセキュリティは新しいトピックではありませんが、企業は、アイデンティティ管理やペネトレーションテストに関連した専門的スキルを開発するためにも、この基本的な領域における進化に注力できるチームを必要としています。

サイバーセキュリティスキルに対する階層的なアプローチは、トレーニングと認定資格の需要を物語っています。サイバーセキュリティキャリアの初期におけるポジションでも、テクノロジーシステムとサイバーセキュリティの手法に関する多少の知識は必要で、さまざまな教育課程を通じて知識を証明することができます。その時点から、組織はキャリア開発と企業の健全性のため、スキル構築の選択肢を提供し続ける必要があります。

サイバーセキュリティのための採用意欲は依然として高く、企業の53%が新規採用を選択肢として検討しています。しかし、そのような採用意欲は外部要因によって妨げられることがあり、限られた専門知識をめぐって企業が争奪戦を繰り広げることから容易ではありません。さらに多くの企業（56%）がサイバーセキュリティ人材のトレーニングを計画しており、42%は、チーム内で主要概念を確立し、新たな分野へのスキルセットを拡大するため、サイバーセキュリティ認定資格を提供する予定としています。

効果を最大化し、長期的な成功を確実にするためには、集中的な取り組みが必要



Source: CompTIA State of Cybersecurity 2025 | n=429

スキルの開発は、企業が効率性を向上させるために取るべき最も重要な行動ですが、他にも選択肢はあります。経営幹部の間で認知を高め意識を向上させることは、アーキテクチャアプローチの原点に立ち返えることを表します。また、組織の必須事項と指標を確立することで、サイバーセキュリティチームは将来の成果に対してより大きな関心を持つようになります。そこから従業員の行動を促すポリシーを構築することで、余計な緊張感を持たず業務を遂行できるといったサイバーセキュリティの文化が作られます。

最後に、企業はサイバーセキュリティプロフェッショナルの長期的な見通しに注目する必要があります。他のテクノロジーの職務と同様に、離職や燃え尽き症候群といった要因により、戦略的ビジョンの実現が困難になることがあります。スキル構築に加えて、容易なツール調達、ビジネスイニシアチブとの密接な統合により、エンゲージメントとキャリア成長のために必要なサポートを提供することが可能です。

デジタルの取り組みが新たな境界を押し広げるなか、セイバーセキュリティの取り組みを、一連のテクノロジー製品で比較的信頼性の高い防御が実現できる・・といった単純化した見方にも戻したくなるかもしれません。しかしこうした見方は、テクノロジー統合の複雑さと、デジタル運用の重要性を過小評価することになります。企業は、サイバーセキュリティをビジネスの必須事項として構造化し、企業の健全性と成功に欠かせないスキルを構築するという課題を受け入れるべきなのです。

Methodology

この定量的調査は2024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525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。この調査は、ANZ、ASEAN、ベネルクス、DACH、イギリス/アイルランドでも実施されました。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。 research@comptia.org

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。

International region	Sample size
ANZ	134
ASEAN	134
Benelux	128
DACH	128
UK/Ireland	132

About CompTIA

CompTIA（the Computing Technology Industry Association）は、世界をリードするIT認定資格およびトレーニング業界団体です。CompTIAは、テクノロジー分野でのキャリアをスタートまたは前進させようとしているすべての学生、キャリアチェンジャー、プロフェッショナルの可能性を引き出すことをミッションとしています。

CompTIA Learning and Training CompTIA

Solutions Catalog CompTIA Career Explorer

CompTIA Job Posting Optimizer CompTIA IT

Salary Calculator

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.