RESEARCH REPORT

2022 State of Cybersecurity

～サイバーセキュリティの現状～

September 2022

CompTIA

Introduction

この1年間、世界中のビジネスはパンデミックの教訓に対応してきました。ワークフォースの観点では、企業は働き方への柔軟性と企業文化の均衡を保つため最良の方法を模索しています。テクノロジーの観点では、クラウドファーストアーキテクチャにある多く利点が、マルチクラウド環境における複雑性とコスト管理という課題と比較検討されています。パンデミック後の環境における均衡はどのようなものか、私たちが知るにはまだ数年はかかるでしょう。ですが、その初期変化は大きな再編成を示唆しているようです。

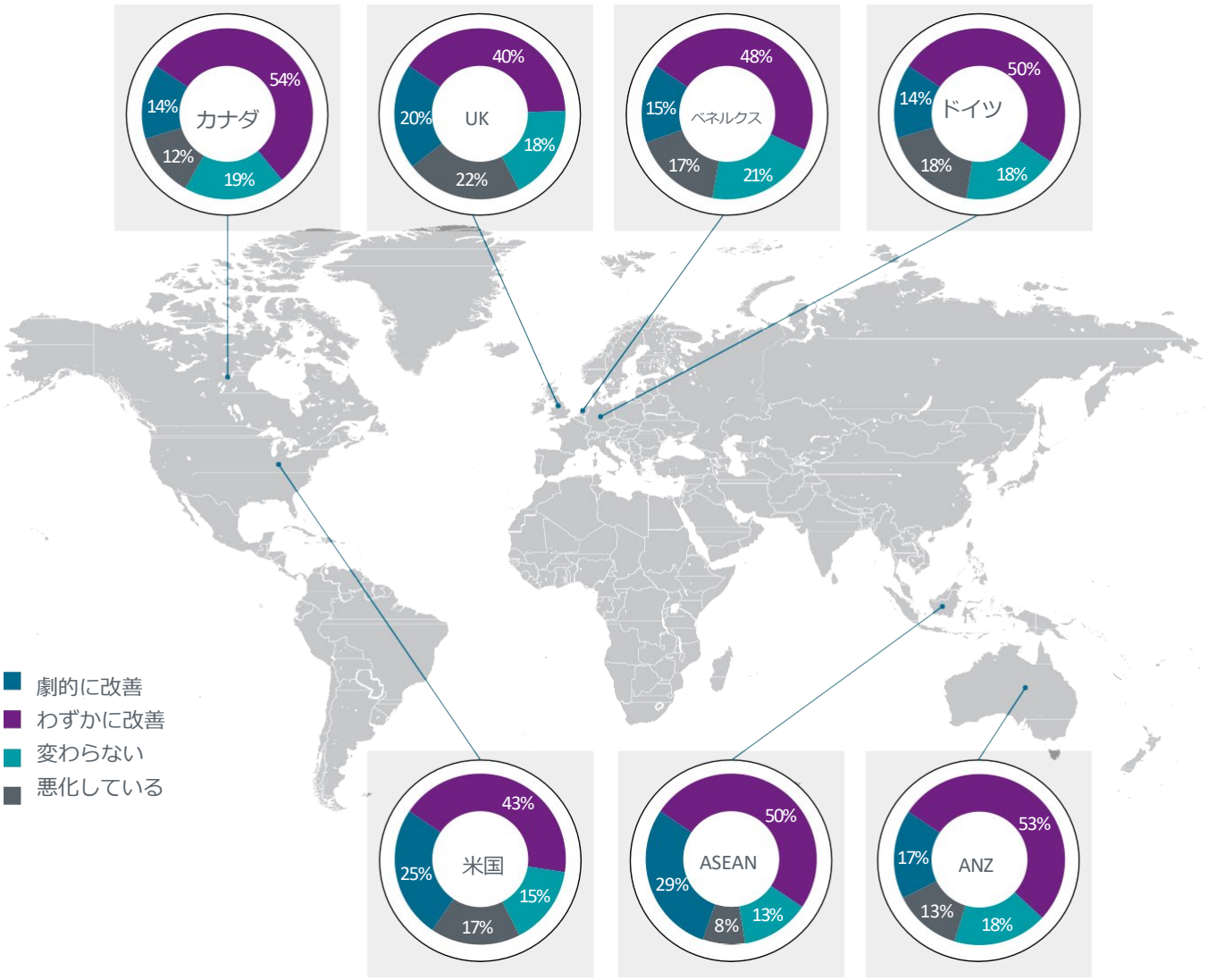
パンデミックから得た顕著な教訓の一つは、根本原因よりも、症状の方が診断や補正がしやすいケースが多いということです。それは、当然ながら企業戦略の枠を超えて影響を及ぼすものとなり、その概念の最たる例がサイバーセキュリティです。企業は、サイバーセキュリティが侵害された際、その脆弱性を痛感し、事後分析することで攻撃を防止または軽減できたであろうプロセスやツールを特定します。しかし、そのアクションが、将来の別のサイバーインシデントにつながるかもしれない潜在的問題に対処するとは限りません。

CompTIAの2022年版の「State of Cybersecurity ～サイバーセキュリティの現状～」レポートでは、根本原因と症状のディスコネクト（ずれ）について考察します。クラウドとモバイルの導入によるデジタルトランスフォーメーションにより、サイバーセキュリティに新しい戦略的アプローチが必要ですが、それらの完全に採用するには戦術面にも資金面にも大きな課題が伴います。サイバーセキュリティは、現代のビジネスにとって依然として差し迫った課題の1つですが、ITに対する古い見解や脅威に対する理解の低さといったハードルが、規定の「治療」を行うことを困難にしているのです。

サイバーセキュリティの情勢は、前進することの難しさをよく表します。本レポートには、経済的・技術的成熟度の異なる7つの地域が参加しています。サイバーセキュリティは、参加する全ての地域において、「一般的な懸念」および「企業のジレンマ」として、問題のある領域であるという明確な見解が示されています。

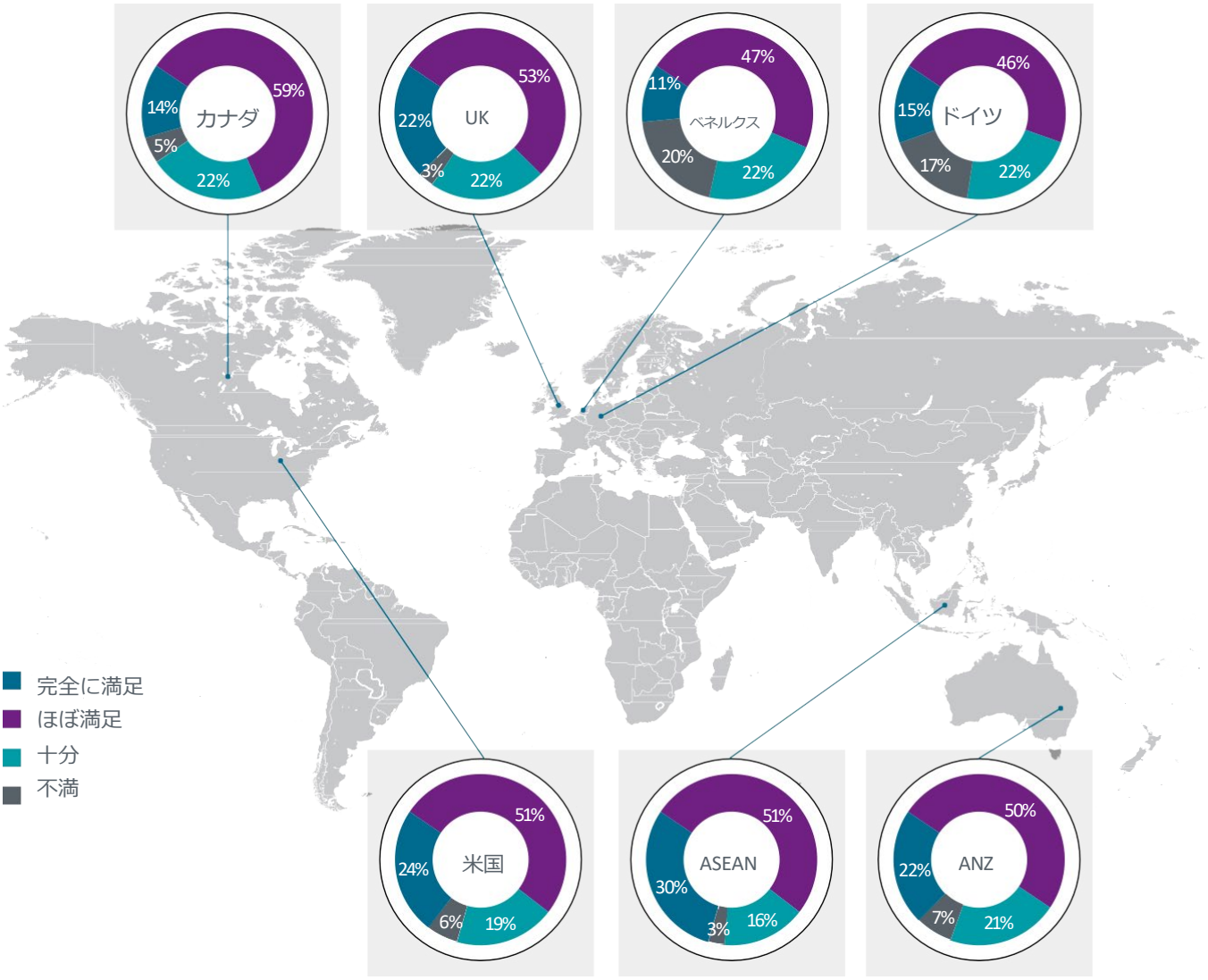
まず、サイバーセキュリティの全体的現状 - サイバー犯罪者の組織、政府の対応または、利用できるサイバーディフェンスメカニズムの機能などに関して - は、比較的ゆっくりとした改善を見せています。先進地域においては、劇的な改善があると考える人はほとんどいません。多くの場合、ほぼ同じ割合の人が、状況は悪化していると考えます。米国以外では前年比データはないものの、回復傾向にありません。米国の回答者のうち、サイバーセキュリティの状況に改善が見られると答えた割合は、69%から68%と、わずかに減少しています。

グローバルのサイバーセキュリティの状況



さらに、個々の企業レベルでも状況はあまり良くないのが現状です。どの地域でも、回答者の大多数が自社のサイバーセキュリティは「ほぼ満足」と回答しますが、「完全に満足」とする回答者は少数です。ほぼ全ての調査参加者が「改善の余地がある」と感じており、より深刻とするケースもあります。また、前年比の傾向を見ると、あるシグナルも示されています。米国では、「満足度（net）」は70%から75%に上昇しているものの、「完全に満足」は29%から24%に低下しています。本レポートは、米国内のデータに焦点をあてており、海外地域のデータについては、別途調査概要を掲載しています。

企業におけるサイバーセキュリティの満足度



パンデミックという歴史的な混乱に適応するため、企業は技術導入のペースを加速させました。これにより、柔軟性の向上と長期的な効率化への扉が開かれます。しかし同時に、従来のサイバーセキュリティの考え方やツールキットでは不十分である状況に陥ったのです。企業は、活動ごとの取り組みではなく、業務の全領域にサイバーセキュリティの決定を行き渡らせる新しいパラダイムを採用する必要があります。

注目すべき動向

2022

ポリシー

サイバーセキュリティは事業とより一体化する

1

2

プロセス

ゼロトラスト戦術が目立った変化をもたらす

人材

組織は、専門性とイネーブルメント（仕組化）を重視

3

4

製品

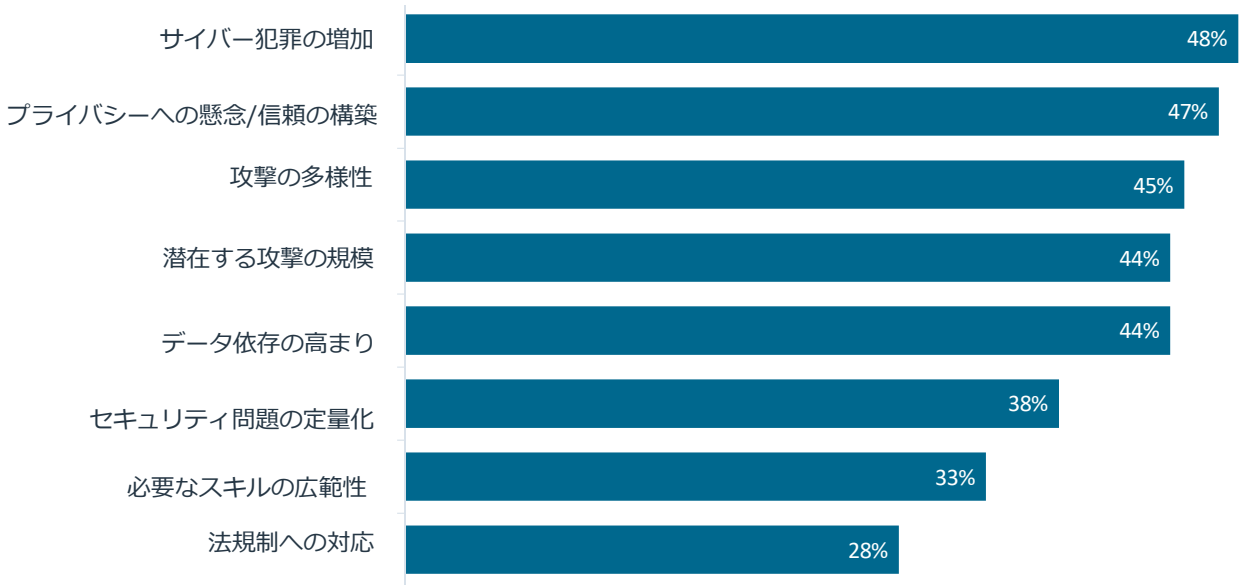
自動化は複雑性を軽減するも、新たな課題も

市場概要

サイバーセキュリティは、企業ITの進化に対する「反応」です。つまり、サイバーセキュリティの必要性は、テクノロジーが導入された後にのみ生じます。近年このような傾向が強まっており、企業が積極的にテクノロジーを追求するにつれ、サイバーセキュリティは二の次にされています。

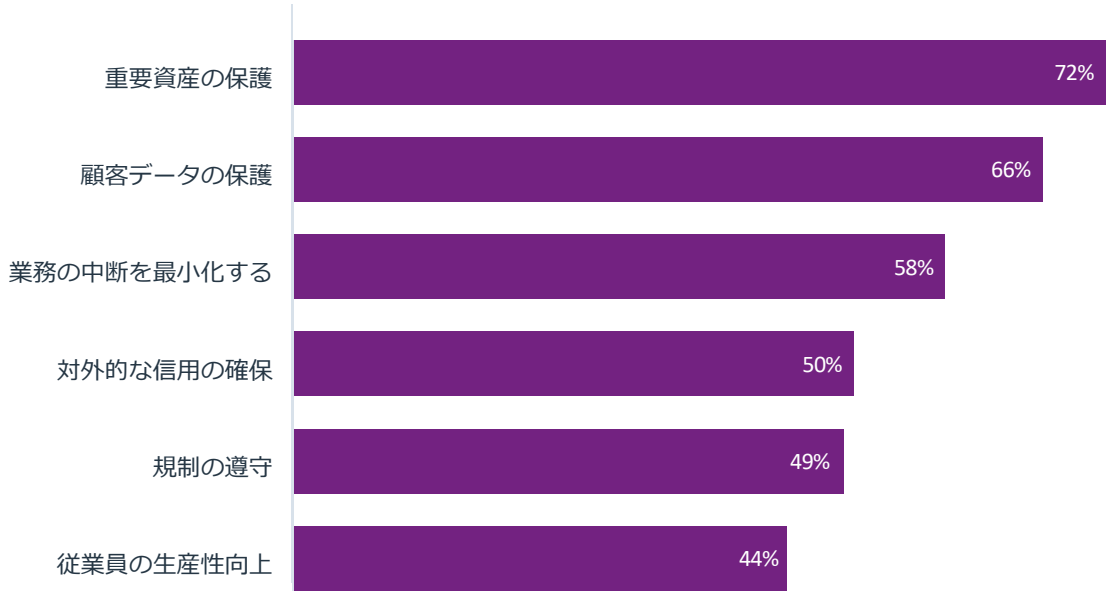
サイバーセキュリティの在り方がITに追随する限り、現代のサイバーセキュリティの特徴は「複雑」そのものです。IT運用と戦略がクラウドやモバイルシステムの導入により複雑性を増したように、サイバーセキュリティの管理も、脅威の拡大に対応するため、さまざまな側面を持つようになりました。CompTIAの調査では、サイバーセキュリティを推進する要因の上位トップ3のうち2つに、サイバー犯罪件数の増加とサイバー攻撃の種類の増加が挙がりました。

サイバーセキュリティの推進要因



「複雑」なものには、明確性が求められます。サイバーセキュリティの取り組みに影響を与える要因には、DX、政府規制、顧客の認識など複数あることから、サイバーセキュリティを単なる「保護コーティング」と捉えるだけではもはや十分ではありません。組織は、サイバーセキュリティ戦略を進める目的を慎重に検討する必要があり、そうすることで明確な疑問が浮き彫りになります。サイバーセキュリティは、どのようにビジネス上の利益を促進するのか？サイバーセキュリティの成功はどのように測定されるべきか？適切な投資はどう決定されるのか？などです。

サイバーセキュリティ戦略の目的



これらの疑問、特に最後の疑問の答えを導き出すことが、独立した分野としてのサイバーセキュリティにこれまで以上に取り組むことになります。サイバー犯罪が財務および業務上のマイナス材料として劇的に増しているのであれば、専念することが深刻な結果を回避する上での処方箋となります。

これら3つのデータは、サイバーセキュリティの爆発的普及を表しているかのようです。Cybersecurity Venturesのレポートでは、2021年のサイバー犯罪による世界の金銭的被害額は、6兆1,000億ドルに上るといいます。この数字は、前年比15%増に。さらに、2025年には10.5兆ドルに達すると予想されています。サイバーセキュリティインシデントのコストは、盗まれたデータの回収や、ランサムウェア攻撃による支払いに止まりません。イメージの悪化は、顧客離れによるビジネスの損失、パートナーやサプライヤーの信頼を失ったことによる新規契約の交渉に要する時間など、大きな波及効果をもたらす可能性があります。

サイバー関連記事の見出しに載らないよう、企業はサイバーセキュリティの予算を増やしています。ガートナー社は、世界のサイバーセキュリティへの支出は、2021年の1,500億ドルから2022年には1,725億ドルに増加し、最終的に2026年には2,673億ドルに拡大すると予測しています。これらの成長は、企業がクラウドファーストのアーキテクチャアプローチへの移行が進めていることから、クラウドセキュリティへの支出によるものと考えられます。また、特に、企業がブロックチェーンに対応したアイデンティティソリューションや、メタバースアプリケーションに対して意味するところを慎重に考察する際には、セキュアなアイデンティティも大きな話題となるでしょう。

そして、サイバーセキュリティのスキルに関する需要は非常に高くなっています。CompTIA、労働分析の会社であるLightcast、National Initiative for Cybersecurity Education（NICE）の共同プロジェクトCyberSeekによると、サイバーセキュリティ関連のスキルを必要とする求人件数が米国には714,500件以上あることが分かっています。これら求人の多くは、サイバーセキュリティアナリストやペネトレーションテスターといった、サイバーセキュリティに特化した職種の募集となります。CompTIAのState of the Tech Workforceレポートでは、これらの分野の需要は引き続き高く、2022年には4%の成長が見込まれ、今後10年間で国の成長率を上回る253%と予測されています。Lightcastによると、米国の労働市場全体では、2022年に1%、今後10年間で7.8%の成長が見込まれているとしています。

サイバーセキュリティ問題の規模と範囲は計り知れず、破壊的な攻撃を免れる組織はもはや存在しません。重要なインフラを守る政府機関から、顧客データを保護する個人事業主まで、デジタル時代のあらゆる機関は、サイバーセキュリティに最大限の注意を払わなければなりません。古い慣行が多くの企業の足かせとなっている可能性はありますが、可能な限り堅固なサイバーセキュリティ体制を作るために、ポリシーの策定、プロセスの構築、人材教育、製品の導入を支援するリソースはこれまで以上に充実しています。

サイバーセキュリティのトレンドを把握するために組織が活用できるリソースの1つが、情報共有分析機関（ISAO）です。CompTIA ISAOは、そのような機関であり、特にテクノロジー業界の企業に影響を与えるサイバーセキュリティのトレンドに重点を置いています。トップベンダーや政府機関から提供される脅威インテリジェンスや脅威フィードに加え、マネージドサービスプロバイダーやテクノロジーベンダーにネットワーキングのための機会を提供し、サイバーセキュリティソリューションの導入や顧客ニーズの管理に関するベストプラクティスを共有することができます。

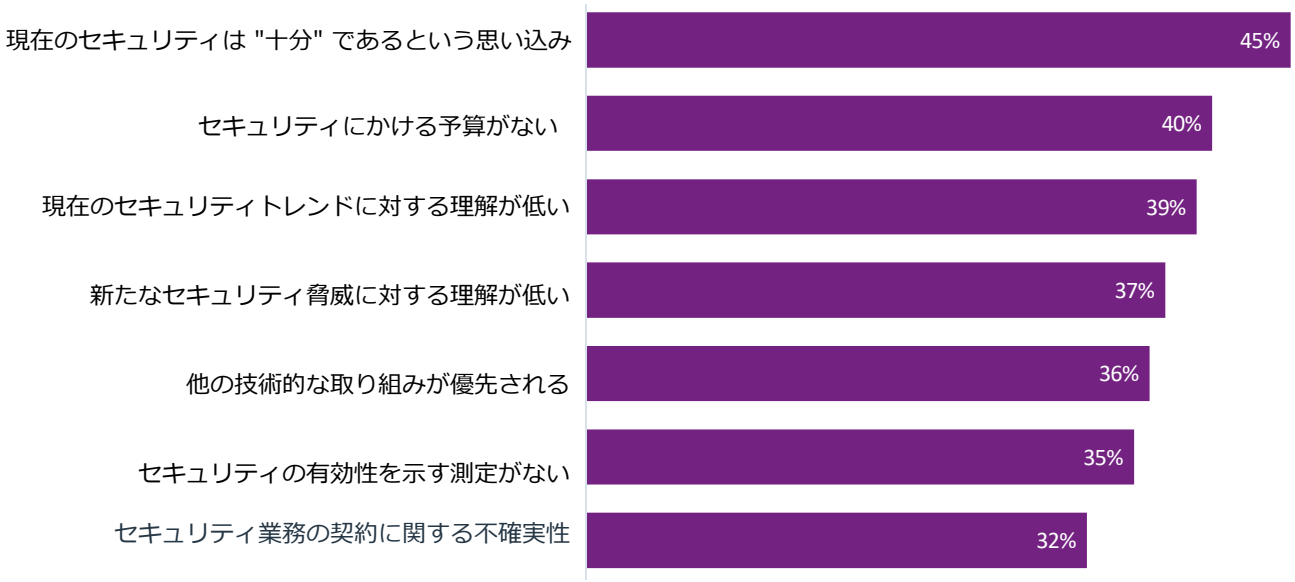
1. ポリシー

サイバーセキュリティが企業ITの進化を反映している点の一つは、両者いずれもより戦略的になっていることです。ITに関して言えば、成長期の困難はあるものの、組織はより戦略的なアプローチへの移行を受け入れています。一方サイバーセキュリティは、戦略的なマインドセットを実践する上で難航しています。

戦略的マインドセットの最も重要な点の1つは、「サイバーセキュリティは、もはや外部的事象を主な対象としていない」という認識です。上述のサイバーセキュリティを推進する要因では、上位に挙げられている問題のほとんどが外部に向けたものであることがわかります。攻撃の数、種類、規模は、ビジネスの外側で起きていることへの着目です。プライバシーに関する懸念も、外部からの期待に関する懸念です。つまり、データ依存の高まりや、変化する規制へのコンプライアンスの維持など、内部業務の変化にサイバーセキュリティが付随しているという認識が低いことがうかがえます。

来年にかけて、サイバーセキュリティを事業運営と統合する動きが進むでしょう。サイバーセキュリティをDXの重要な要素として受け入れることで、組織全体に新たな課題や取り組みがもたらされます。同時に、全体的視点を採用することで、サイバーセキュリティへの取り組みを変える際の数あるハードルを取り除くことができます。

サイバーセキュリティへの取り組みを変える上でのハードル



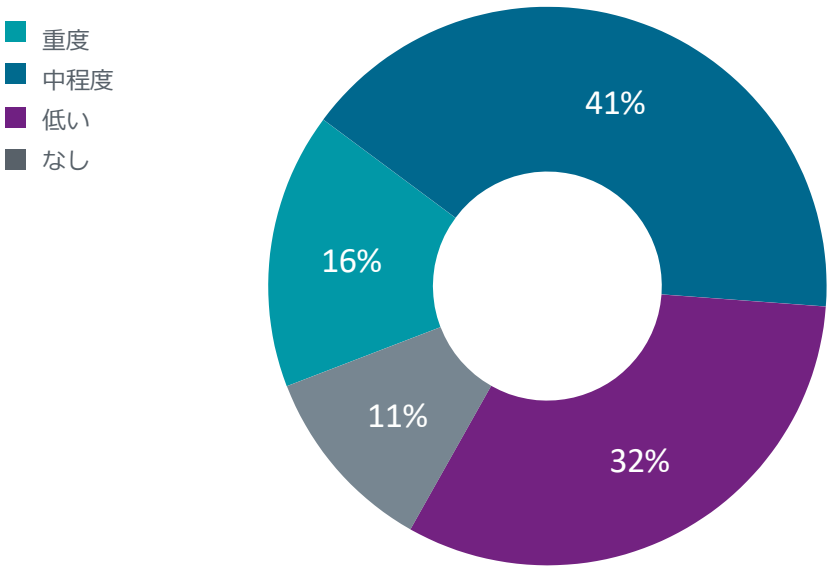
企業が挙げた第一のハードルは、現在のサイバーセキュリティ体制が「十分である」という考えです。これには、2つの異なる「思い込み」が考えられます。まず、「十分である」ということは、サイバーセキュリティの取り組みを測定するための具体的な指標がないことを示します。CompTIA の調査では、数年前から、より適切で対象を絞ったサイバーセキュリティのメトリクスを確立する必要があることが一貫して示されています。

第二に、「十分である」と認識することは、データ侵害発生の有無が主となっていることが一般的な背景としてあります。企業は、メトリクスを定義するだけでなく、サイバーセキュリティに関する具体的かつ戦略的な目標を設定する必要があります。

2つ目のハードルは、テクノロジーが戦術的でなくなることで起こる、ITの全領域に共通するものです。予算は横ばいではなく、むしろテクノロジー投資は増やす必要があることが認識されています。もちろん、ここにも新たなメトリクスが必要です。ROI（投資収益率）を計算することは、全てのテクノロジー分野にとって新たな課題です。プラスの成果があまり定義されていないサイバーセキュリティにとっては、さらに大きな挑戦となります。

次のハードルは、サイバーセキュリティの専門知識に関するものです。ビジネス上の意思決定を左右する一般的なサイバーセキュリティのトレンドの知識であれ、防御強化が必要となる特定のサイバーセキュリティ脅威であれ、組織はサイバーセキュリティに関する知識を向上させる必要があります。これは、ビジネスの領域で異なるでしょう。本レポートの「人材」のセクションでは、サイバーセキュリティチェーンのさまざまな部分のニーズについて詳しく見ていきます。

サイバーセキュリティインシデントの影響



サイバーセキュリティインシデントだけでは、サイバーセキュリティ体制を十分に測ることはできませんが、それでも戦略的思考の必要性を示すものとなり得ます。過去1年間にサイバーセキュリティインシデントの発生を認識している企業のうち、57%が（インシデントは）組織に「重度」または「中程度」の影響を与えたと回答し、「重度」としたのは16%です。インシデントに対処するための新たなソフトウェアやハードウェアの購入は別として、緩和策となった最大要素は、問題を解決するために技術スタッフが費やした「時間」です。

インシデント対応に費やす時間には、明らかに機会損失が発生します。DX時代では、組織は彼らの技術的目標に必要となるスキルの習得と導入に苦労しています。予防できる危機に対応するために、革新的な事業から資金を引き離すという余裕は多くの企業にはありません。サイバーセキュリティの取り組みに対し、よりプロアクティブなアプローチを取ることで、「火災」に費やす時間を最小限に抑えることができます。

また、緊急のサイバーセキュリティの問題に費やす時間が増えることで、モチベーションの低下にもつながります。セキュリティスペシャリストが残業を強いられることで、戦略的ITへの移行や、スタッフの入れ替わり、ここ数年のパンデミックなどですでに存在している可能性のある精神的緊張に拍車をかけることになるのです。ワーカーが新たな機会を求めている環境において、ストレスを増やすことは企業にとって得策とは言えません。

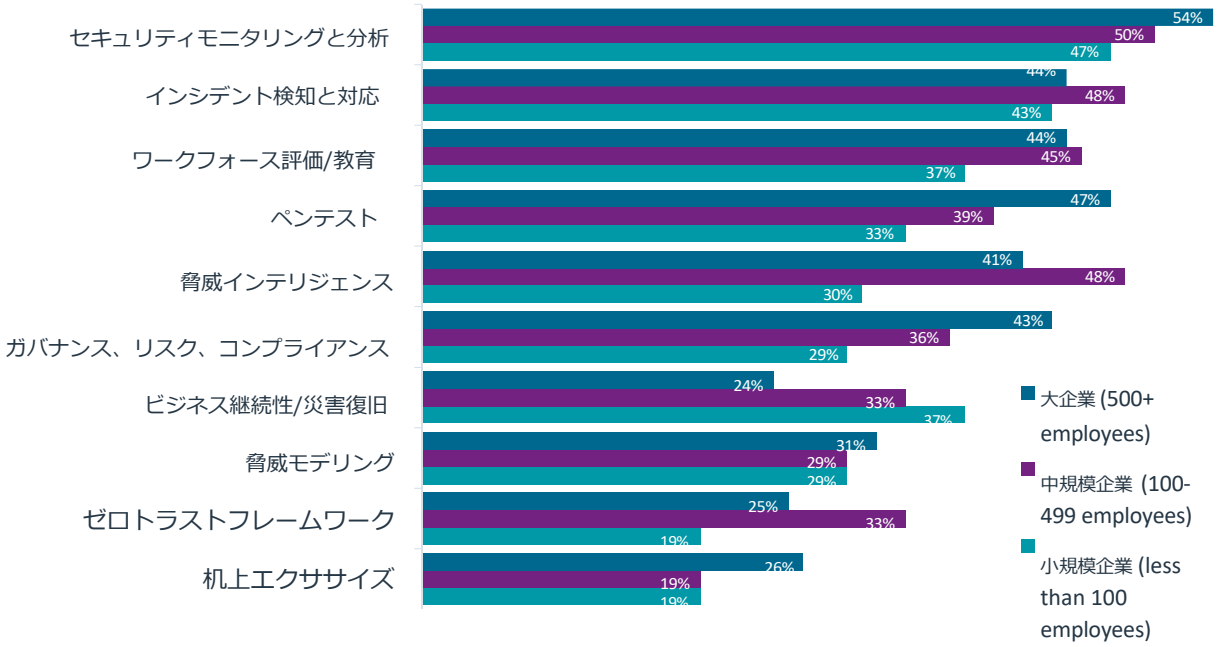
最終的には、サイバーセキュリティを事業運営とより強固に組み込まれることで、企業が直面する多くの革新的問題に対処することができます。サイバーセキュリティを組織の文化に組み込むことでより良いプロセスが生まれ、不注意なエラーの少ない知識豊富な従業員が確保され、最新のITアーキテクチャをサポートする包括的な製品セットを実現することができます。こうした変化が、より高い満足度という達成困難な目標へとつながります。

2. プロセス

昨年のState of Cybersecurityレポートでは、現代のサイバーセキュリティの指針となるポリシーとして、ゼロトラストを挙げていました。クラウドコンピューティングとモバイルデバイスの登場は、数十年に渡り主要なマインドセットであったセキュアペリメーターという視点を大きく変えました。このパラダイムシフトに取り組むにあたって、組織が困難としていたのは、サイバーセキュリティに関するさまざまな決定に資する包括的なアプローチの定義でした。このジレンマの答えとして登場したのが、ゼロトラストです。

今年、ゼロトラストは、広範なポリシーから戦術的なプロセスへと移行し始めています。ゼロトラストの採用は一夜にして実現するものではありません。何よりもまず、ゼロトラストは、サイバーセキュリティに対する考え方が大幅に変わることを意味します。企業は、サイバーセキュリティを IT部門の数あるコンポーネントの 1つとして捉え、単にハードウェアやソフトウェアに投資するのではなく、サイバーセキュリティを組織の必須事項として捉えなければなりません。テクノロジー製品にとどまらず、ワークフローや人材に関する決定にまで拡大しなければなりません。

サイバーセキュリティ対策の実践

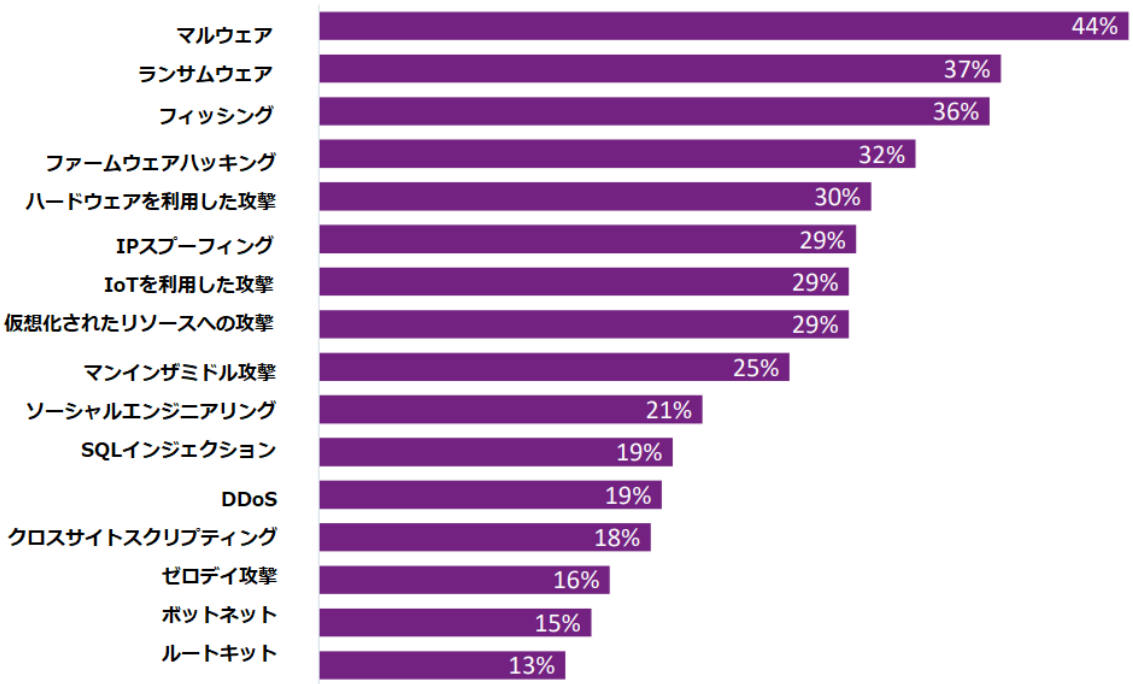


ゼロトラストに関する組織の意識を高めることは、困難な作業となります。ゼロトラストは、組織のサイバーセキュリティ対策としてかなり低い位置にありますが、これは従業員の領域によってサイバーセキュリティ戦略に対する精通度が異なることが一因です。その一例に、大企業のわずか24%を含めても、ビジネス継続性と災害復旧（BCDR）に関する実践（プラクティス）が組織にあると回答した人の割合は比較的低いものでした。BCDR計画の発生率ははるかに高いと思われますが、事業部内の人たちはその計画に関して理解する必要はないのかもしれません。

さらに、ゼロトラストは単一の製品や行動ではなく、多くの個々のツールや実践がゼロトラストアプローチの一部となることがあります。ゼロトラストの傘下にある構成要素を見ると、個々のパーツとして認識している組織が多いようです。多要素認証は、信頼できるアイデンティティを検証するための最良ツールの1つであり、46%の組織で導入されています。クラウドワークロードガバナンス - クラウドのリソースが計画通りに使用されていることを確認するプロセス - は、41%の組織で導入されています。他の要素、ソフトウェア定義のマイクロセグメンテーション（38%）や、最小権限のアクセス権（26%）などの採用率は低いものの、ゼロトラストポリシーに対する幅広い認識に比べるとわずかに先行しているようです。

ゼロトラストは、課題と意思決定に役立つサイバーセキュリティに関する哲学であるということです。ゼロトラストを採用する最善方法は、一連の成功基準を定義することではなく、組織の状況に応じて最適な手順を特定するロードマップを構築することです。そのような手順には、データとワークフローのフル監査、アイデンティティおよびアクセス管理（IAM）ソフトウェアなどの製品の導入、継続教育プログラムの作成などが含まれるでしょう。各手順においては、明確な課題に対処し、測定可能な成果が含まれる必要があります。

脅威インテリジェンスに関する改善点

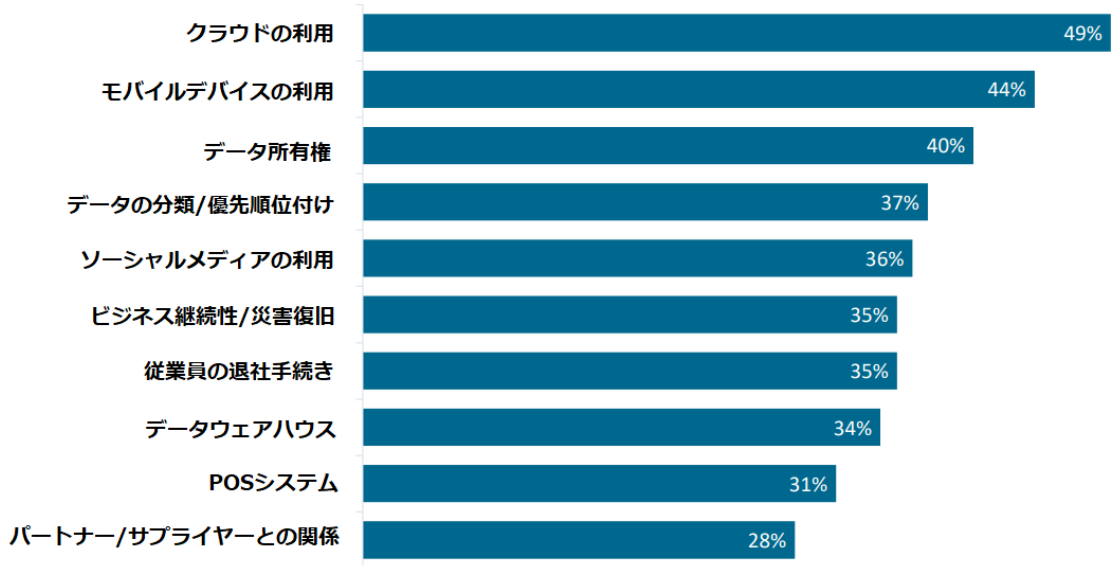


ゼロトラストアプローチの影響を受けるサイバーセキュリティ業務の中で、特に注目すべき分野が2つあります。1つ目の「脅威インテリジェンス」は、サイバーセキュリティの従来の機能を自然に発展させたものです。あらゆる攻撃の侵入を防ぎたいのであれば、企業はそれら攻撃の性質を理解する必要があります。

サイバーセキュリティチームは、脅威の状況を幅広く理解するとともに、最も厄介な攻撃がどのように実行されるのかについて深い知識を持つ必要があります。サイバー脅威モニタリングは、厳密さとスケジューリングを必要とする作業ですが、ゼロデイ攻撃やサプライチェーン攻撃などの深刻な問題に迅速に行動できる能力も必要となります。脅威インテリジェンスは、一貫性と防御を重視する旧来のサイバーセキュリティの領域と、柔軟性とプロアクティブな対応が重要となる新しい領域の両方に足を踏み入れています。

企業が理解を深めたいとする脅威リストは、問題の深刻さを表します。マルウェアは最も長い歴史を持つ脅威ですが、常に進化しているため、継続して注意を払う必要があり、依然1位にランクしています。ランサムウェアとフィッシングは、デジタル運用が増加し、人的ミスがより大きな損失をもたらすことが証明されたことから、たちまち主要な懸念事項となりました。全企業の少なくとも4分の1が懸念を抱いている脅威は9種類あります。ハッカーにとって有益であることがわかれば、リスト下位にある脅威は直ちに差し迫った課題となる可能性があります。今後、脅威のインテリジェンスを向上させるには、強い取り組みとピアネットワークやISAOへの幅広い参加が必要となります。

リスク管理の要素



2つ目の領域は、「リスク管理」です。ガバナンス、リスク、コンプライアンス（GRC）は、わずか35%の企業が実践していると回答しています。（デジタル業務に関する規制は急速に変化しているにもかかわらず）規制的な側面からGRCを軽視する企業もあるようですが、リスクの側面については軽視すべきではありません。

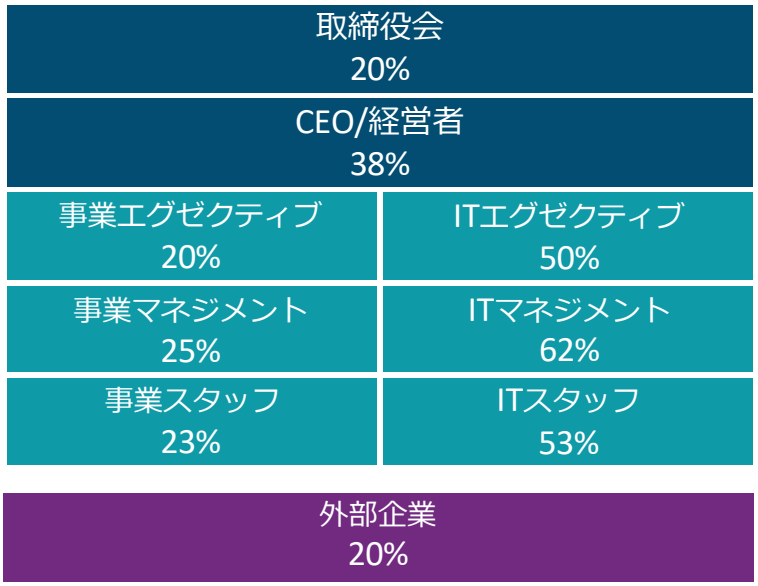
正式なリスク分析には、技術的な側面と業務的な側面の双方に踏む込むことが必要です。セキュアペリメーターの時代は、サイバーリスクに対して言わば無頓着なアプローチが取られ、重要とされる情報はファイアウォールの背後に置かれるだけでした。今日においては、重要データにセキュリティを施し過ぎることはないものの、予算やユーザビリティ（有用性）の面で限界があり、すべてのデータに最高レベルのセキュリティを施すことは現実的ではありません。リスク管理は、特にゼロトラストの時代には、企業資産とビジネスの両方を徹底して理解することから始まります。

そこから、リスク管理は一連のトレードオフとなります。クラウドシステムをセキュアにするためのコスト vs. レジリエントクラウドアーキテクチャのメリットとは？企業データを漏洩させることなく、モバイルデバイスで柔軟な働き方を実現するにはどうすればよいか？市場分析に最も重要な顧客データは何か、また収集すべきではないデータは何か？といった具合です。これらの質問を検討するには、事業部門とIT部門の双方からの情報が必要であり、さらにビジネス目標の変化や技術の進歩に伴い、そのプロセスは反復されることになります。

3. 人材

企業がセキュリティ上の欠陥の根本原因を解決しようとするとき、問題には複数の「層」があることに気付かされます。技術的な層があることは明らかで、これは何年も前から焦点となっていることであり、サイバーセキュリティソリューションの重要な部分であることに変わりません。また、人材の層もあり、多くの企業が改善のため、サイバーセキュリティの意識向上に向けた教育を行っています。しかし、事業運営や企業経営に関わる層は、近年あまり注目されていないようです。

サイバーセキュリティチェーンに関わるグループ

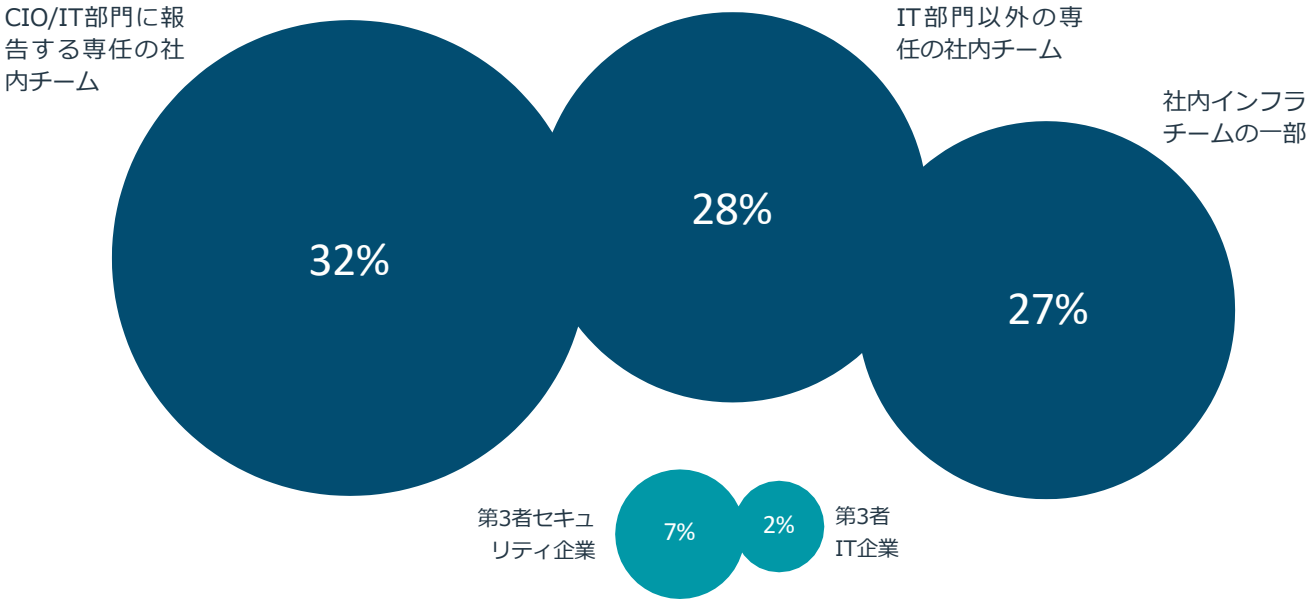


上で見られる参加率は、どの層があまり重視されていないかを示しています。サイバーセキュリティチェーンとは、サイバーセキュリティの議論に関わる全ての関係者のことであり、そうした議論を包括的な戦略に結びつけることを目的としています。予想の通り、ほとんどの企業でIT 部門の参加率が高くなっています。この数字は、専任のITスタッフを持たない小規模な企業によって若干引き下げられますが、ほとんどの企業では、サイバーセキュリティソリューションの一部として技術スタッフがいることは明らかなようです。同時に、ITスタッフをサイバーセキュリティチェーンの一部として認識していない組織は、組織全体でより広範な議論を行うべきであるとすら認識していないケースもあります。

議論が認識されているところであっても、事業部門の参加率は低いようです。中小企業では、経営者が積極的に関与する傾向があります - 小規模企業の47%はCEOまたは経営者がサイバーセキュリティチェーンの一員であるのに対し、中規模企業では37%、大規模企業では27%にとどまる。しかし、ビジネスに不可欠な機能であるにもかかわらず、全体的な事業スタッフの参加率が低すぎるのです。

参加率が全体的に低いだけでなく、変化もないのが現状です。取締役会から事業スタッフ、ITスペシャリスト、外部企業に至るまで、今年の調査における参加率は、昨年の調査とほぼ同じです。組織は、戦術的な取り組みと戦略的なビジョンを結びつけるサイバーセキュリティの議論を高めるのに苦労しています。

セキュリティオペレーションセンターの所在地

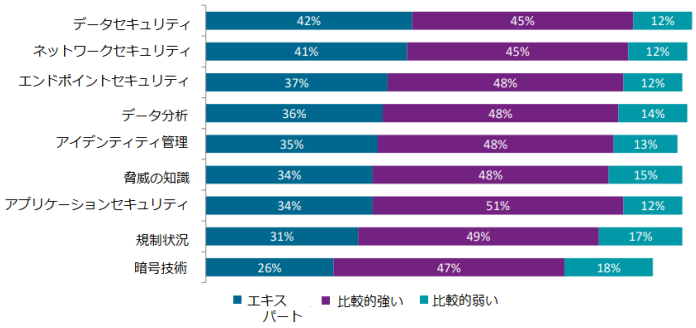


サイバーセキュリティチェーンを促進させることは、セキュリティオペレーションセンター（SOC）の役割の1つです。SOCは通常、サイバーセキュリティの戦術を実行するグループと考えられ、大半の組織では、内部機能として位置づけられています。SOCの一部として専任のチームを作ろうとする傾向が顕著になってきていて、IT部門の外に移す企業が増えていることは早くから指摘されています。所在地に関係なく、SOCリーダーは、あらゆる層でサイバーセキュリティを業務上の議論に組み込むことをもっと検討する必要があります。

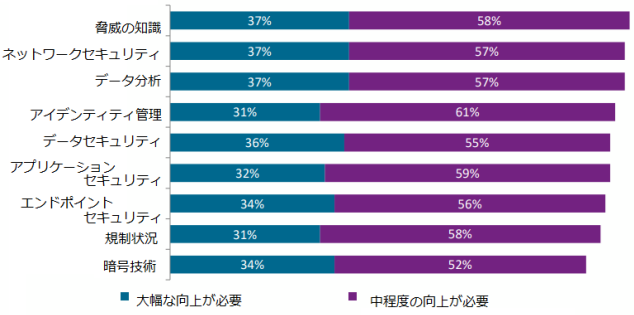
そのような担当者を特定するためには、SOCを正式に定義する必要があるとする企業もあるでしょう。大企業では、最高情報セキュリティ責任者（CISO）がサイバーセキュリティの取り組みを主導することが多いですが、小規模企業では、サイバーセキュリティエンジニア1名や、サイバーセキュリティを担うITジェネラリスト数名でSOCを構成する場合もあります。SOCを具体的に構築し、役割と責任を明確にすることで、議論を進め、取り組むべき他の戦略的ギャップを特定することができます。

企業におけるSOCの定義にかかわらず、技術スペシャリストは常に重要な要素です。サイバーセキュリティのスキルに関する需要と供給のバランスは崩れており、この状況は近い将来に改善される兆しはほとんど見られません。サイバーセキュリティ関連のスキルを要求している求人件数は714,500件以上もあることに加え、CyberSeekは、2021年5月から2022年4月の12ヶ月間、情報セキュリティアナリストの募集が18万件であったのに対し、現在その職務に就いているのは14万1千人に過ぎないこと報告しています。企業は、成長が追いつかない人材プールで争っているのです。

サイバーセキュリティスキルのアセスメント



サイバーセキュリティスキルの必要性



組織化されたスキルと知識を向上させるために、企業はまずサイバーセキュリティ人材の現状を把握する必要があります。CompTIAの調査データは、現在のスキルの概算に過ぎませんが - 事業スタッフやIT管理層でさえ、日常業務から切り離されている場合もありますし - たとえ概算であっても議論の出発点としては十分です。企業は次のステップに進み、スキル向上を検討する際、より詳細なアセスメント（評価）を行うための方法を開発する必要があります。

「サイバーセキュリティスキルの必要性」にあるリストは、スキルアセスメントが概算であることをさらに証明するものです。リストの上位に挙げられているいくつかは、「サイバーセキュリティスキルのアセスメント」でも高い専門性を持つ分野と捉えられているからです。しかし、「サイバーセキュリティスキルの必要性」は、より正確な状況を示しているのかもしれません。ネットワークセキュリティは、長きに渡って行われてきた作業であることから深い専門性があるように見えるかもしれませんが、実際にはIT環境の変化により、常に改善が求められています。脅威に関する知識、データ分析、アイデンティティ管理などの分野は、サイバーセキュリティのより最近の傾向を表わすことから、スキルアップの対象となります。

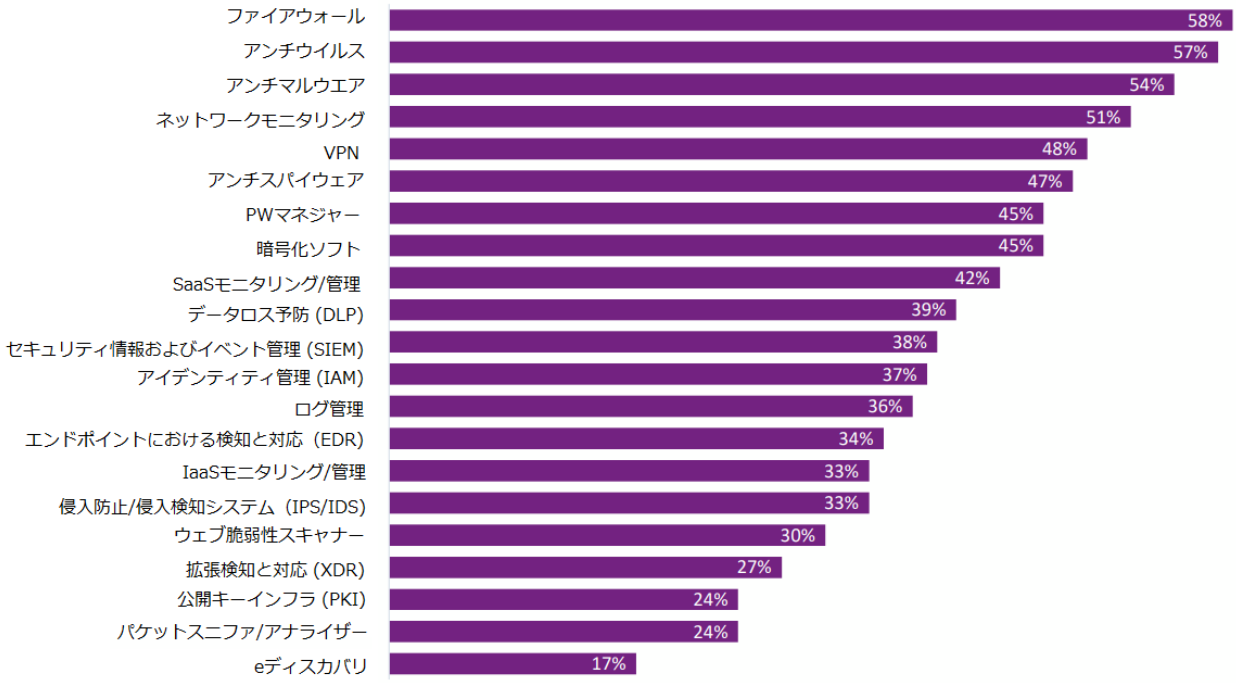
企業は、人材不足を補うために採用だけに頼るわけにはいきません。自由市場において適任者を見つけることは難しく、費用もかさみます。トレーニングは、もっと活用されるべきオプションです。既存の従業員に対するトレーニングは、特定のスキルに焦点を当てることができ、より迅速に結果を出し、従業員のロイヤリティを高めることができます。サイバーセキュリティが複雑化するにつれ、パートナー連携の拡大も検討する価値があります。

残念ながら、適切なスキル人材を獲得 or 構築することは、道半ばに過ぎません。特に需要の高い環境では、リテンションは大きな課題です。ISACAのState of Cybersecurity 2022レポートによると、2021年には60%の企業がサイバーセキュリティプロフェッショナルを保持することが困難であったとし、2020年から7ポイントの上昇です。明るいニュースは、多くのリテンション活動が、サイバーセキュリティの戦略的視野の開発にうまく合致していることです。CompTIAの調査では、回答者の半数がサイバーセキュリティの人材管理における最大の課題として、「スタッフが能力を発揮できるツールやサポートの提供」を挙げています。これは、財務的な投資（2番目に挙がった課題「相場賃金の支払い」と同様）を意味する場合もありますが、構造的な変化や新しいプロセスによって達成することも可能です。3番目に挙がった課題は、財務的な投資を必要としませんが、政策目標に立ち戻ることができます。「サイバーセキュリティをビジネスの取り組みと統合する」は、サイバーセキュリティプロフェッショナルが組織から切り離されていると感じる症状に対処することができます。

4. 製品

サイバーセキュリティ製品のツールボックスが小さくなることはありません。ポリシーやプロセスは、企業がサイバーセキュリティの体制を向上させるために使うことができる最大のレバー（手段）ですが、ソフトウェアとハードウェアは依然としてソリューションに欠かせない要素です。

使用しているサイバーセキュリティ製品



サイバーセキュリティ製品のリストは、長い間存在していたものから始まります。ファイアウォール、アンチウイルス、アンチマルウェアは、セキュアペリメーターの重要性が低下した今でも、その機能を果たしています。これらのツールは至るところに存在しますが、あまりにも一般的なため、多くのエンドユーザー（おそらくITスタッフでさえも）製品セットの一部とは考えていないかもしれません。

ネットワークモニタリングも長い歴史を持ち、時代に合わせて進化しているツールの一つです。SolarWinds Network Performance Monitor、Datadog Network Monitoring、Auvikなどのツールは、ネットワークアーキテクチャ全体を監視し分析する広範な機能を提供します。ネットワークモニタリングの近年の機能には、ネットワークのクラウドコンポーネントの可視化や、データフローをより理解するための分析ツールが含まれます。

クラウドに関しては、SaaSモニタリングや管理ツールの普及率は、2021年の32%から2022年には42%へと大幅に跳ね上がりました。クラウド導入の加速は、パンデミック時のIT運用における最大の変化の1つであり、現在企業は、その副次的な影響に対応しています。サイバーセキュリティの問題とともに、クラウドシステムにはその利用やコストに関する懸念事項があり、クラウドアーキテクチャを適切に管理し、構成し、セキュアにするための新しい管理ソフトウェアが必要とされています。

一方で、採用率は低いものの、近く採用が検討されるべきツールもあります。クラウドの導入はSaaSが主流ですが、IaaSもまた広く普及されており、適切なモニタリングと管理には（IaaSの方が）より重要かもしれません。全体像の把握には、包括的なネットワークモニタリングツールが不可欠ですが、パケットスニッファーやLANアナライザーは、発見しにくい問題を一掃することができます。

これほど多くのツールが存在し、サイバーセキュリティ人員には多くの制約があるため、次なるステップは「自動化」であることは明らかです。自動化をテーマとしたCompTIAのリサーチでは、自動化のサイバーセキュリティ戦略への関わりについて、いくつかの点を明らかにしています。2021年第2四半期に397人のビジネスプロフェッショナルを対象に実施したこの調査では、潜在するサイバーセキュリティインシデントを検出することが、現在企業が行っている自動化の取り組みのトップ例であることがわかりました。ですが、自動化の他の取り組みにも見られるように、2つの側面あります。1つの側面は、自動化は現代のサイバーセキュリティの取り組みに存在する高度な複雑性を激減させるものという考えです。この理由から、多くの企業は自動化について、人員的な制約を直接解決できるものとして早くから捉えています。自動化とセルフサービスによって、Tier1のヘルプデスクサポートの需要が減ることを期待したように、企業は自動化によってSOCのTier1作業の需要を減らせることを期待しているのです。

しかし、もう一方の側面も考慮しなければなりません。自動化そのものは、複雑な取り組みです。自動化に関する調査で挙げられた課題の上位2つは、ITシステムとの連携とスキルギャップの解消です。現代のITアーキテクチャの規模と領域から、自動化は必要とされていますが、その実装や機能面でのモニタリングなど、リソース（人）の点ではまだ手一杯なのが現状です。

Tier1の需要が減るという想定も誤りです。DXにより、組織全体で使用されるテクノロジーの量、日々の業務におけるデータの活用、そしてパフォーマンスを阻害したり脆弱性を生み出す問題は大幅に増加しています。自動化は、Tier1の需要を取り除くのではなく、問い合わせの内容を変えるだけです。パスワードのリセットやソフトウェアのパッチといった単純な問題は自動化によって処理されるかもしれませんが、以前にこのような問い合わせを対応していた人は、今ではより大きな問題を解決することを任されているのです。

自動化がリソース問題を完全に解決しなくても、状況をより管理しやすくすることができます。サイバーセキュリティと事業運営を統合することで、サイバーセキュリティはこれまで以上にクリティカルになり、ゼロトラストを導入することで、新しいプロセスにつながります。特化した組織構造と適切なツールセットは、この新たな複雑性に取り組む上でのファーストステップです。自動化に対してバランスの取れたアプローチを取ることで、組織は根本的な問題に対処し、健全なサイバーセキュリティの展望に向かうことができます。

Methodology 手法

この定量的調査は2022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500名が調査に参加し、95%の信頼性でのサンプル誤差は+/−4.5%ポイントでした。海外地域（ANZ、ASEAN、ベネルクス、カナダ、ドイツ、イギリス）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.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.