CompTIA

RESEARCH REPORT

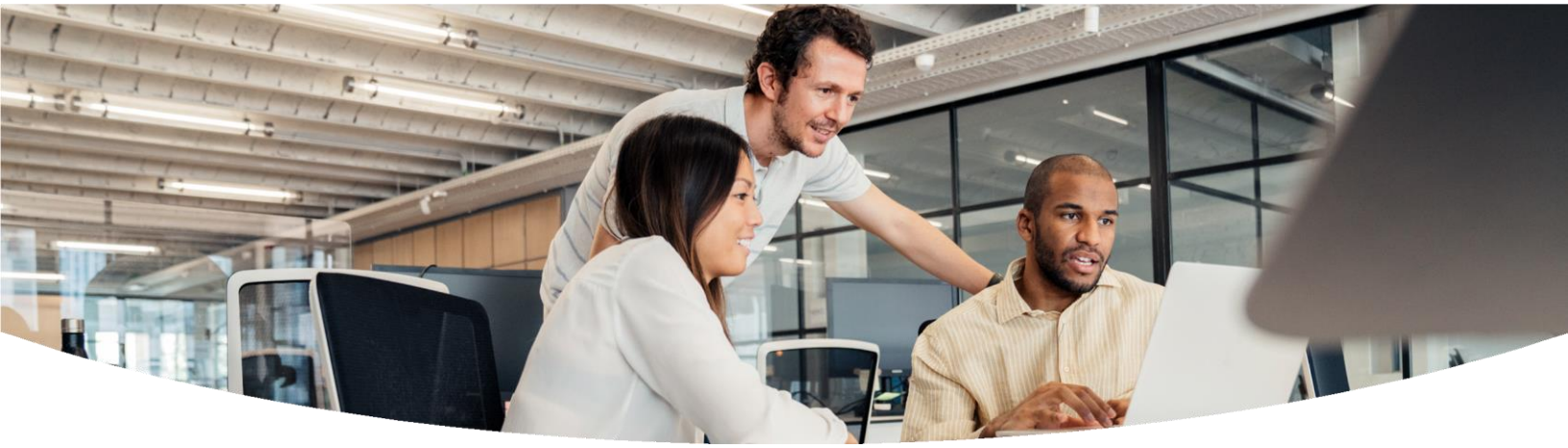
2021 State of Cybersecurity

～サイバーセキュリティの現状～

September 2021

Introduction

今のデジタル時代における特徴のひとつは、変化のペースの速さです。コアテクノロジーのコンポーネントを安価に入手できること、そして世界中の人とつながることができること、これらがイノベーションの力を飛躍的に加速させました。それと同時に、企業がひっきりなしに、無関係なことに直面したり適合したりする必要に迫られている感があります。



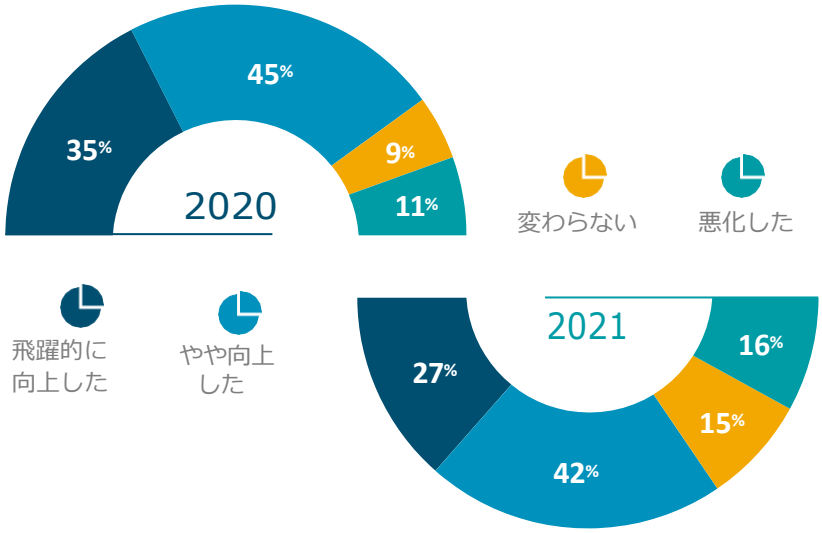
このようにテクノロジーが乱れ飛ぶ状況のなかで、企業の機能が変化するスピードの遅さは見逃されがちです。つまり、イノベーションの力が適応力を追い越しているのです。新たなテクノロジーは世界を変えることができます…でもこれは理論上の話です。実際には、これらすべての新しい玩具を利用できるようになるまでには、ビジネスプロセスや学ぶ姿勢の変化に何十年もかかります。

このことが突出して顕著なのがサイバーセキュリティ分野です。CompTIAの2020 State of Cybersecurityレポートには、サイバーセキュリティがいかにしてビジネスの必須事項になってきたか、財務や法務の実務と同じくらい組織の長期的成功に重要なものになってきたか、について述べられています。このような高い優先順位を考えると、素早い対応が必要だと納得できます。それなのに、企業は立ち止まっているようなのです。

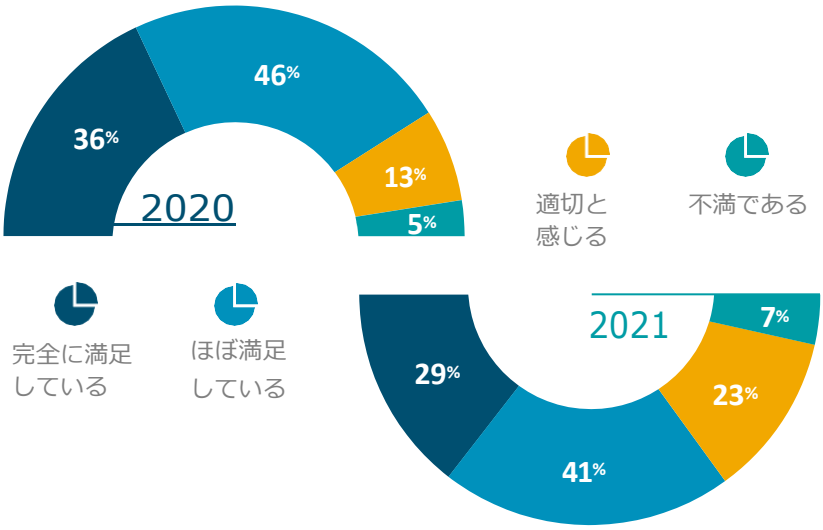
この問題の俯瞰的様相を２つのデータから見ることができます。まず人々は、経済における全般的なサイバーセキュリティは悪化していると感じています。2020年、CompTIAの調査対象者の80%が、サイバーセキュリティ状況は向上していると感じていました。2021年、同様に感じている人は69%しかいませんでした。長引く新型コロナ感染拡大の不確実性、主要インフラに対するランサムウェア攻撃、そしてビジネス環境を引き裂くサプライチェーン攻撃、といったすべてが、より悲観的な感情を生み出していると考えられます。

同時に、企業戦略への満足度も下がっています。2020年、従業員の80%が、自社のサイバーセキュリティへの取り組みに満足していました。2021年には、その数値が70%に下がっています。世界状況を考えると、以前は十分だと思われていた実践事項が、もはや効果的ではなくなっているのです。

サイバーセキュリティの状況



会社のサイバーセキュリティに対する満足度



サイバーセキュリティが複雑な問題であることは疑うべくもありません。ですから、会社が複雑なソリューションの構築に四苦八苦しているということにも驚きはありません。最も複雑な事項の一つは、ITが戦略的意義を担い、クラウドコンピューティングが従来の安全な境界（セキュアペリメーター）に対する認識を打ち消している状況の中、現代のセキュリティには、これまでと全く異なる考え方が求められるということです。CompTIAの2021 State of Cybersecurityレポートでは、サイバーセキュリティ戦略の包括的な様相と、サイバーセキュリティ実践を一気に加速させるために必要な戦術の概要を提示しています。

注目すべき動向

2021

1 ポリシー

ゼロトラストがサイバーセキュリティの指針となる

2 プロセス

サイバーセキュリティが深耕・拡大の両方向に進む

3 人材

会社は大規模なサイバーセキュリティ・チームを構築する

4 製品

サイバーセキュリティのツールボックスは戦術に合わせ整備される

市場概況

サイバーセキュリティ脅威統計

424万ドル
データ侵害にかかる平均コスト[1]

287
データ侵害を検出し封じ込めるまでの平均日数[2]

350K
一日に発見される新たなマルウェアプログラム数[3]

18,000
サプライチェーン侵害に影響を受けるSolarWinds顧客[4]

185万ドル
ランサムウェア攻撃を修復するための平均コスト[5]

74%
2020年にフィッシング攻撃を受けたアメリカ企業の数[6]

なぜサイバーセキュリティが、企業の最優先事項になってきたのでしょうか。数字を見れば一目瞭然です。まず、脅威環境は、日々起こる攻撃量やサイバー犯罪者が用いる方法の多様性という点において、伸長を続けています。攻撃は猛烈なペースでやってきますし、たった一つの侵害によって、会社は、膨大な時間と何百万ドルものコストを費やさなければなりません。もちろん、最大の脅威は企業の評判が損なわれるということで、この先何年にもわたる事業見通しに被害を及ぼします。

マルウェアやウイルスが懸念事項であることに変わりはありませんが、新たな攻撃が防御戦略の別の抜け穴を探っています。2020年末のSolarwinds、そして最近ではKaseyaの事件が知れ渡ったことで、サプライチェーン攻撃は今や、サイバーセキュリティ用語集に必ず載っているものとなりました。これらの攻撃は、顧客の手元に届く前の初期の段階で、ハッカーが悪意あるコードをソフトウェアに挿入するというものでした。これらの攻撃における問題点は、ソフトウェアが信頼できるソースから来るために攻撃の検知が難しいということだけでなく、ソフトウェアへのアクセスが顧客のさらに顧客にまで許可されるために急激に広がる、ということにあります。

サプライチェーン攻撃がホットな新しいアイテムである一方、ランサムウェアは強力なサイバー兵器として活動を続けています。Colonial PipelineとJBS Foodsに対するランサムウェア攻撃によって、国家間の攻撃的戦術がもはや航空機や戦車によるものに留まらないという認識が強くなりました。主要インフラのITシステムを狙えば、効果的に被害を与えることができるので、ハッカーは同じ手口を使って、企業から金銭を脅し取ろうとするわけです。

最後に、サイバーセキュリティにおける最も弱いリンクが人であることに変わりはありません。企業に押し入る方法として、ハッカーは純粋に技術的な手法を使う代わりに、フィッシングなどのソーシャルエンジニアリング戦術を用いて、それと気づかない従業員から情報を得るのです。これらの攻撃は人間心理の弱点を突いてきます。そして、世界的パンデミックのような出来事によって、そのような弱点がより表れてきます。

サイバーセキュリティの範囲や規模を示す数値として、支出に関するデータが挙げられます。2020年について、Gartner社は当初、対象となる一連のトピック全体におけるサイバーセキュリティ支出は、年末までに1,240億ドル近くに達すると予想していました。これは2019年と比較して2.4%の増加です。実際には、サイバーセキュリティ支出はそこから1億3300万ドル超過し、10.6%の増加となりました。2021年に関して、Gartner社はこの勢いは継続するという明らかな予測を立てています。

サイバーセキュリティ支出推定[7]

市場	2020	2021	増加率
アプリケーションセキュリティ	3,333	3,738	12.2%
クラウドセキュリティ	595	841	41.2%
データセキュリティ	2,981	3,505	17.5%
アイデンティティアクセス管理	12,036	13,917	15.6%
インフラ保護	20,462	23,903	16.8%
統合的リスク管理	4,859	5,473	12.6%
ネットワークセキュリティ機器	15,626	17,020	8.9%
その他のセキュリティソフトウェア	2,306	2,527	9.6%
セキュリティサービス	65,070	72,497	11.4%
顧客セキュリティソフトウェア	6,507	6,990	7.4%
Total	**133,776**	**150,409**	**12.4%**

支出の増加は、ポストコロナの現実をある程度反映しています。劇的な増加の多くは、クラウドセキュリティのエリアに見られます。これは一部には、クラウドセキュリティが2020年ベースの支出で最も少なかったことにも起因しています。また、会社がITアーキテクチャにおいて、クラウドファーストの考え方に移行している印でもあります。

しかしながら、支出状況に関して、新型コロナのパンデミックによる派生効果というだけで片付けられない、それ以上の背景があります。支出は全体的に著しく高くなっています。その中には、ネットワークセキュリティ機器も入っていますが、これに関してはリモートワークへの移行はその背景説明にはなりません。セキュリティサービスやインフラ保護といったエリアは、2020年ベースの支出額では最大でしたが、これらも2桁成長が見込まれているのです。

サイバーセキュリティ推進要因となる主要な問題点

会社が脅威環境への自社の対応や行う投資について考える際、様々な問題点を考察しています。攻撃の量や種類の多さをまず考えます。次に、自社顧客のプライバシーを守ることを懸念します。そこから、ビジネスオペレーションにおいて増大するデータ依存や、投資を正当化するためのサイバーセキュリティ取り組みの定量化、そして成功するために必要なさまざまな種類のスキルについて、対応を進めていきます。実際、会社はこれらの問題点の多くを過小評価しているかもしれません ― 規制遵守は特に前進していく際の大きな課題になる可能性があります。

サイバーセキュリティ市場全体を流れる共通テーマは、複雑性です。その大半は、ITシステムがさらに複雑化していることによるものです。基本的コンピューティングプラットフォームの安定化が、無数のソリューションを発生させました。その多くは新興技術を取り込み始めています。ITアーキテクチャを超えて、サイバーセキュリティは今や、リスク管理やユーザ教育といった、多くの側面を持つものになりました。

複雑な問題には系統的なソリューションが必要です。会社がサイバーセキュリティをITオペレーション全体から切り離して考える際、4つの要素に関する取り組みを構造化させることで成功を収めることができます：サイバーセキュリティの決定を導く方針、強い姿勢を維持するために必要なプロセス、サイバーセキュリティ結果を担当する人材、そしてデジタル資産を守る製品、です。

1 ポリシー

広義で考えるとサイバーセキュリティ方針は、将来の決定や投資に資する全体的な戦略に照らしたものです。多くの会社では、この方針の要素が組織としての文書に落とし込まれているかもしれません。しかし、組織としての文言に留まらず、方針はそもそも文化的な考え方なのです。この考え方が、現在のビジネス環境に対する理解に影響を与え、組織を守るための最適な方法に関して、認識や行動を推進するもととなります。

会社の歴史においてほとんどの場合、2つの概念がこの考え方の中心になっています。1つ目は、防御的取り組みです。脅威は外からやってきて検知可能であるという想定に基づき、会社は防御的姿勢をとりました。これによって悪いものが入ってくるのを防ごうとしたのです。2つ目の概念は、セキュアペリメーターです。脅威は会社の外で生み出されるという想定から、セキュアペリメーターの概念はロジスティック面のインフラに根差しています。何年もの間、会社は特定の物理的場所からこのオペレーションをしていました。その場所にはコンピュータ機器が設置され、そこで行われる業務はほぼその場所内で完結していました。

最初に崩れた概念はセキュアペリメーターでした。時が経つにつれ、会社などの組織では生産性を上げるため、職員にPCはその他のモバイルデバイスを持たせるようになりました。クラウドコンピューティングがセキュアペリメーターの崩壊を加速させました。会社が、公共インフラ上の安全なアプリケーションやデータを必要とするようになったからです。

防御から未然防止策への移行は遅々として進んでいません。企業にとって、サイバーセキュリティ脅威の性質を完全に把握するのは難しい状況となっています。そこでは、悪者がさまざまなやり方で攻撃をしかけ、検知されることなく企業ネットワークを乗っ取る方法を見つけています。強力な防御を構築し、常にその防御の脆弱性を確認するというのは、2倍の仕事量に思えますし、実際その通りなのです。デジタルコンポーネントへの依存の増加は、安全なオペレーションにかかるコストが増加することを意味しています。

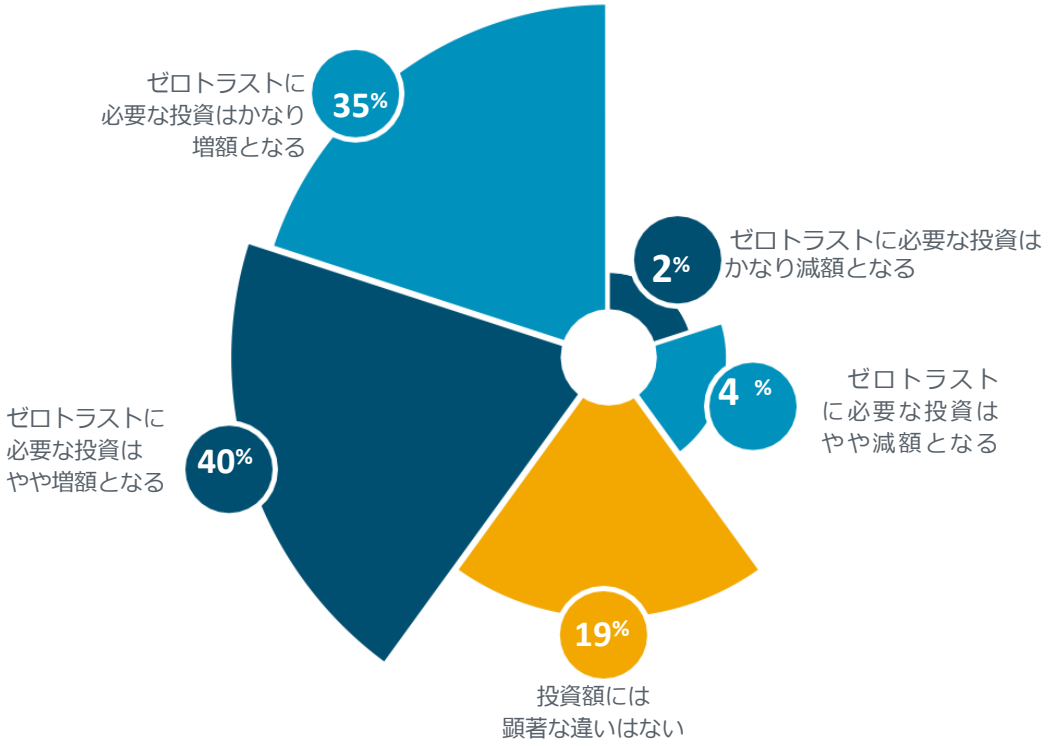
ゼロトラストは、デジタルトランスフォーメーションに対応して新たに生まれた考え方です。潜在的なソリューションを漠然と表現することの多いITトレンドの中にあって、ゼロトラストはそのものずばりを示す言葉です。ネットワークトラフィックやユーザーアクセスはその出所や認証情報があるから無害だと想定するのではなく、ひとつひとつのステップにおいてさらなる確認を求めるのです。

ゼロトラストのフレームワークにおける要素

ゼロトラストアーキテクチャに関するNIST文書に、ゼロトラストは「単一のアーキテクチャではなく、ワークフロー、システム設計およびオペレーションに関する一連の指針である」と記されています（NIST Special Publication 800-207）。組織はこれらの指針に従って、広く使われている手法のいくつかを取るようになっています。多要素認証によって、単一の認証情報だけに依存することが減っています。ネットワーク分析は明らかになっていない悪意ある行為を掘り出します。マイクロセグメンテーションによって、トラフィックが細かい粒度で管理され、対象となるセキュリティ方針が適用できるようになります。ゼロトラストについて、これらどれか一つだけで独立した最優良実践にはなりません。すべてを一緒に行うことで、堅牢な保護ができるのです。

未然防止的なセキュリティ対策への移行に伴い、ゼロトラスト方針はよりお金のかかる取り組みになる傾向があります。CompTIAの調査の中で、ゼロトラストアーキテクチャを追求している会社のうち4分の3が、以前の取り組みよりもゼロトラストに要する投資が大きいことがわかったと言っています。取り巻く状況が変化し続ける中、サイバーセキュリティへの適切な支出額に関しては、これという具体的な数値はありません。実際、サイバーセキュリティ支出を定量化するのは会社にとって非常に難しいのではないでしょうか。肝心なのは、適切な施策には慎重な投資が必要だということです ー 財務面だけではなく、社内資源と時間という観点においてもです。

ゼロトラストのフレームワークに必要な投資



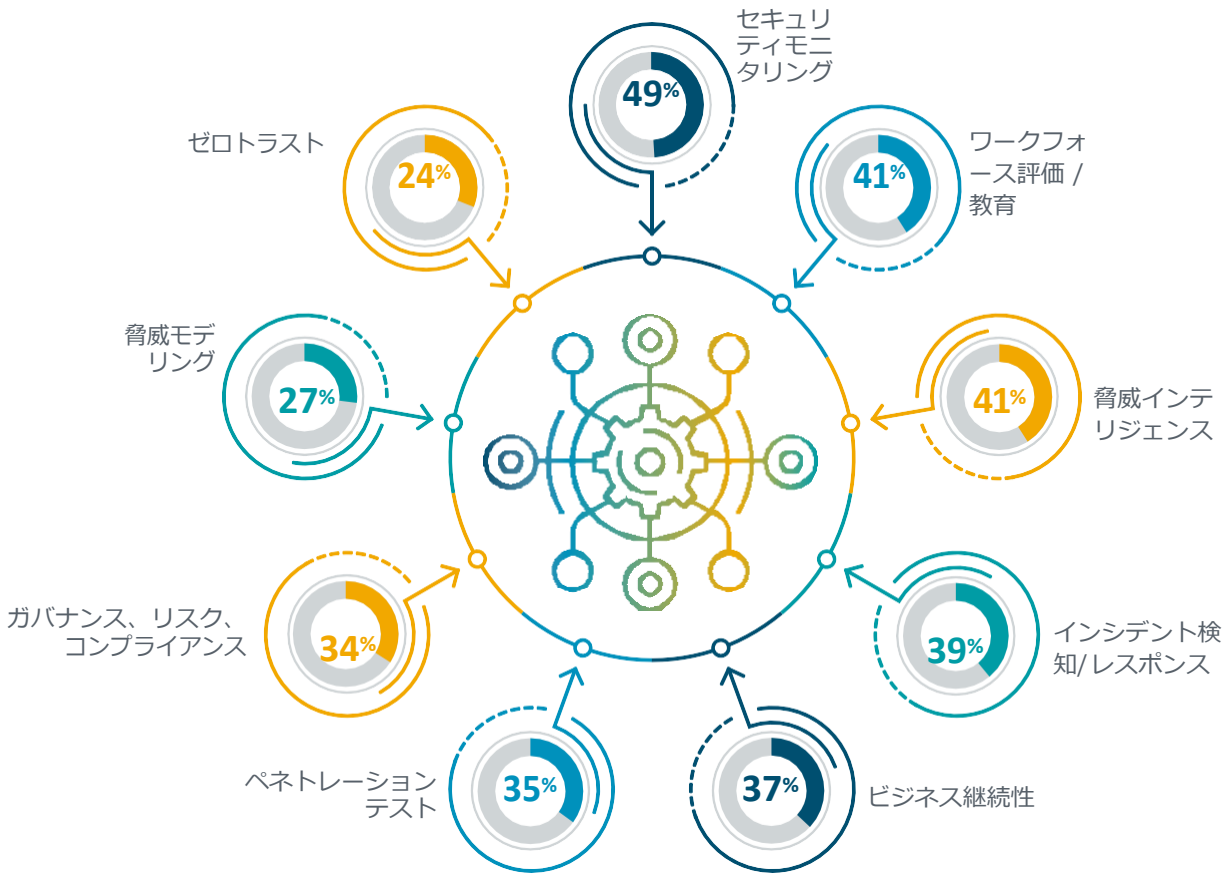
ゼロトラスト以上に、現在のサイバーセキュリティ方針で新たに出現した要素があります。エッジコンピューティングは、アプリケーションアーキテクチャにおいて、クラウドシステムに代わるものだという見方がもっとも多いのです。エッジシステムはソースにより近いところでデータを保存したり、計算を実行したりできます。これにより、周波数帯の需要やレイテンシ（遅延時間）が削減されます。サイバーセキュリティの観点では、エッジコンピューティングはやや異なる意味合いを含んでいます。

ITシステムの複雑性が増すにつれ、会社はそのアーキテクチャ的ニーズに対応するために多種多様の外部企業を使っています。これはクラウドプロバイダーから始まり、コンテンツ配信やオーバーレイネットワーキングのようなサービスを提供している会社（CloudFlareやNetFoundryもその中に入ります）にまで至っています。これらのエッジ企業を自社のアーキテクチャ構成の一部として活用することで、組織/会社は提供物に織り込み済みのサイバーセキュリティ上の利点を得ることもできるのです。例えばDDos低減やマイクロセグメンテーションなどがそれにあたります。会社が外部企業を使う第一の理由は、サイバーセキュリティの利点ではないかもしれません。しかし結局、それが全体のソリューションの一部を成すことになるのです。

2 プロセス

サイバーセキュリティのプロセスはタイヤと道路との接点のようなものです。方針への理解が行き届いたら、次に組織がすべきは、その方針の実行方法を決めることです。現在、サイバーセキュリティはビジネスにおける非常に多くのエリアに関わっているので、この実行フェーズには、個々の実践が数えきれないくらい入ることになります。

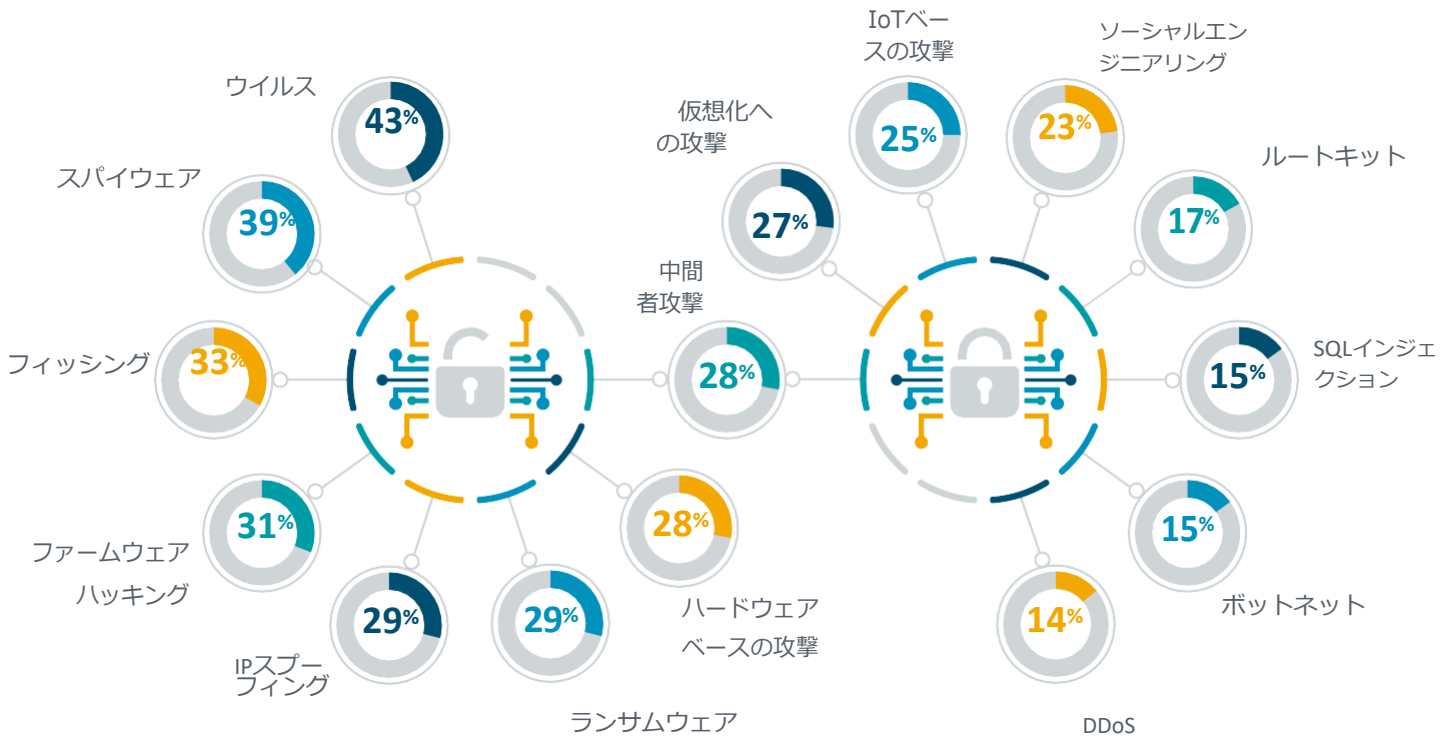
サイバーセキュリティ対策の実践



最も一般的なサイバーセキュリティ実践は、サイバーセキュリティインシデントのモニタリングです。これが何かの説明は不要でしょう。しかしながら、この実践にはネットワークトラフィックへの攻撃パターンの分析も含まれており、この点が興味深いところです。単にインシデントをモニタリングするのは静的な行為です。モニタリングツールが既知の攻撃タイプに対応して構成され、これらの攻撃が検知された場合に通知を送るようプログラミングされているのです。分析はより進んだ、未然防止的な取り組みです。これには典型的なネットワーク行動への理解と、攻撃方法論への理解が必要となります。それにより、いかなる異常も感染可能性のあるものとして調査することができるのです。

ワークフォース評価と教育は、この数年でさらに浸透してきました。この実践を後押ししたのは、ワークフォース全体にデジタルツールが偏在するようになったことです。以前は、PCやスマートフォンといったツールは特定の職種のワークフォースのみが使用するものでした。デジタルトランスフォーメーションが扉を開いたことで、ほとんどの従業員が企業システムや業務に特化したアプリケーションにアクセスできるようになりました。さらに、平均的従業員が日々の個人生活でテクノロジーを使用していますが、消費者レベルの行動はエンタープライズレベルの行動に比べて、セキュリティへの認識が低いというのが通例です。評価によって、企業の安全性に最も影響を及ぼすエリアを特定し、その状況を改善するのに役立つ、的を絞った教育パッケージとメトリックを設定することができます。

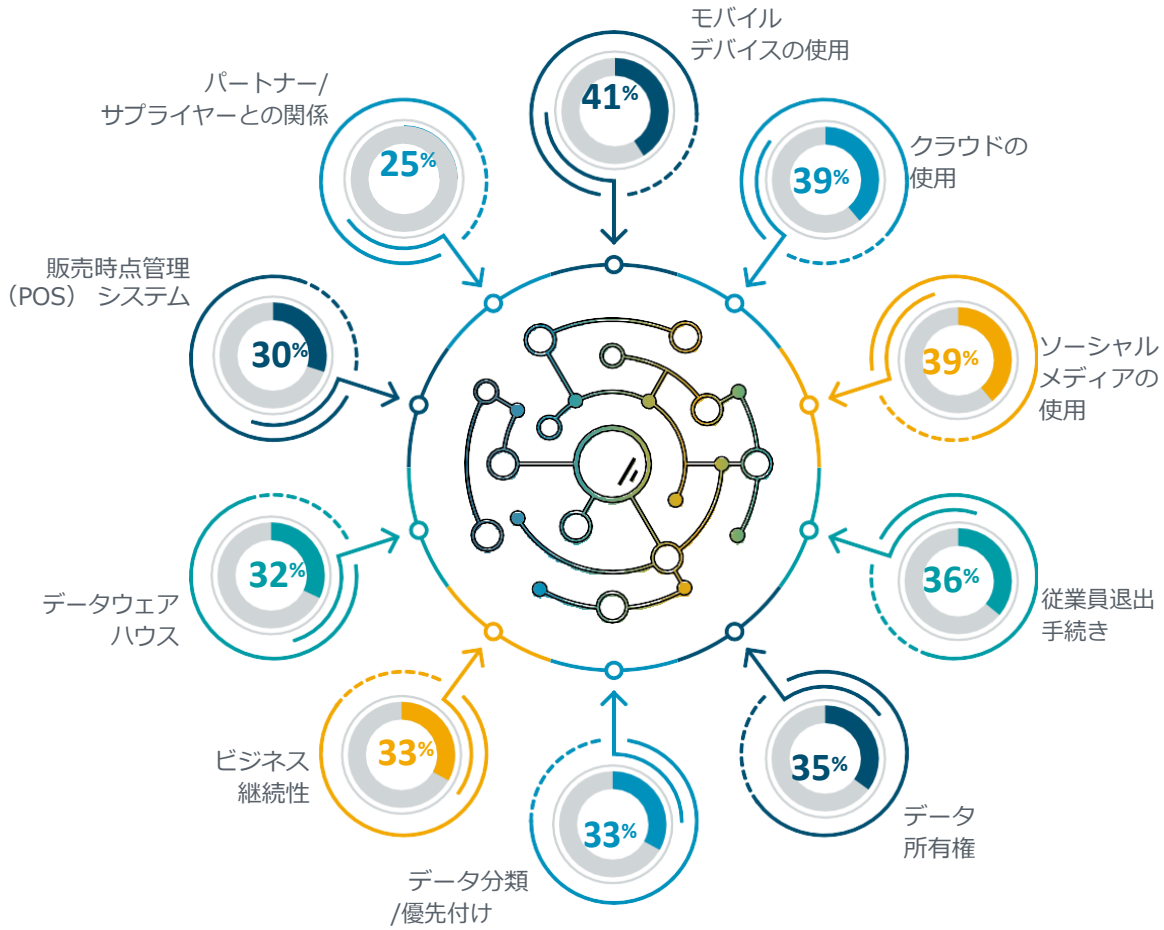
脅威への理解が必要な項目



脅威インテリジェンスは通常、企業システムに発生する攻撃へのインサイトを提供するデータ主導の実践を指します。セキュリティモニタリングと同様、脅威インテリジェンスでは、ビジネス環境全体で発生している攻撃の種類に関する基本的知識に始まり、さらに多くの層（レイヤー）が考えられます。デジタルビジネス実践が進化するにつれ、ビジネスフローを破壊し、その破壊を収益化するさまざまな方法の爆発が起こってきました。ほとんどの会社はまだ昔ながらの脅威に目を向けがちで、ウイルスやマルウェアに関する知識を高めたいと思っています。これらの攻撃の新たな変異種は確実に潜在的脆弱性を利用できますが、その一方で、その他の攻撃は、IT実践における変化に狙いを定めています。IT実践の中には、比較的古いけれども使用が拡大しているもの（仮想化のように）や、新興技術を採用しているもの（モノのインターネットIoTのように）があります。

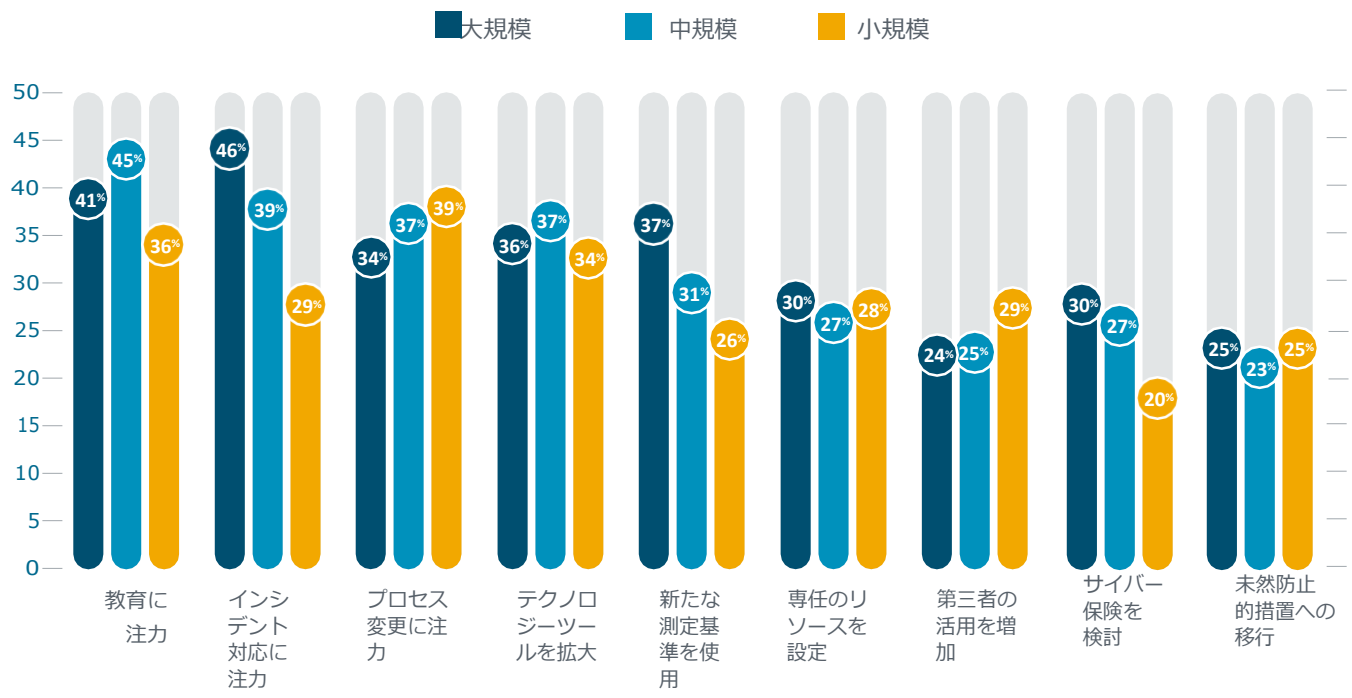
多種多様な攻撃についての幅広い知識に留まらず、脅威インテリジェンスは複雑性を管理するための正式なプロセス構築の必要性を示す、代表的な例です。脅威インテリジェンスのプロセスは、データ収集から始まります ー 社内ネットワークのデータと外部ソースからのデータの両方です。このデータはすべて、他のビジネスデータフローと同様の処理をする必要があります。組織化されたスキームに情報を取り込み、冗長、あるいは不要な情報をふるいにかけて取り除いていきます。自動化やデータ分析技術の助けで、処理済みデータの内容を確認し、その後、緩和計画とフィードバックループによって次に取るべき行動が示されることになります。

リスク管理の要素



近年さらに組織化されてきたプロセスのもう一つの例が、リスク管理です。多くの会社がリスク管理と規制意識を組み合わせて、チームを立ち上げたり、ガバナンス・リスク・コンプライアンス（GRC）の専門家を集めたりしています。このような組織的仕組みを構築していない会社でも、リスク管理に対するしっかりした取り組みをすべきです。多くの場合、リスク分析によって、利便性とセキュリティの間の妥協点が検討されます。たとえば、モバイルデバイスとクラウドコンピューティングは生産性を目覚ましく向上させますが、同時に新たな脆弱性を生み出すことにもなります。完璧なセキュリティは達成できないし、手ごろな価格で手に入るものでもない、というのがふつうです。ですから、ビジネス上の決定がまだなされていない段階で、リスクのレベルを評価しなければなりません。

サイバーセキュリティ取り組みの変化



考えられる実践はさまざま数多くありますが、すべてのエリアを深堀して構築するのは困難です。特に小規模企業（従業員100人未満）にとっては。小規模企業が中・大規模企業に後れを取っている主要エリアは4つです。小規模企業では教育すべき対象の従業員数は少ないのですが、教育への注力が低くなっています。さらに注力が低いのがインシデント対応で、これは小規模企業には資産が少ないので、サイバーセキュリティの懸念も低いと信じられていた時代の名残なのでしょう。小規模会社はサイバーセキュリティ状況に測定基準を適用することが少なく、これがサイバーセキュリティの効果を理解する上での問題となっています。最後に、サイバー保険を検討している小規模会社の数はほんのわずかです。

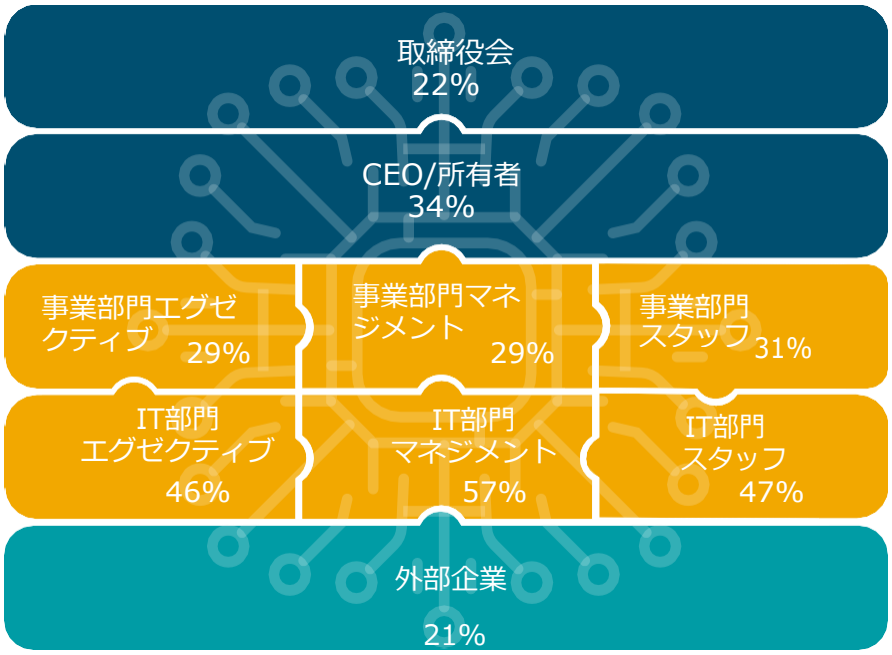
大規模会社であっても、サイバーセキュリティのプロセスを広く深く保つのは、主要課題となっています。静的なセキュアペリメーターという昔ながらの方法は比較的、維持が単純なもので、通常のIT機能のわきにある要素として扱われることもしばしばでした。今日のプロセスには、技術系ワークフォースの専門性と、ワークフォース全体におけるセキュリティファーストの考え方が必要です。組織全体で受け入れて取り組まなければ、セキュリティのプロセスは壊れ、ビジネスが露出されてしまいます。

3 人材

サイバーセキュリティの人材についての認識は、その実行プロセスに伴って拡大してきました。プロセスがかつては単純なセキュアペリメーターだったのが、今では組織のあらゆる点に関わってきているのと同様、サイバーセキュリティの責任は別個のスキルであったものから会社全体の認識そのものへと広がってきました。もちろん、組織内の従業員全員が深い専門知識を持つ必要はありません。しかし、多くの集団が関わるものなので、考えるべき主要ポイントはいくつかあります。

.

サイバーセキュリティチェーンに関わるグループ

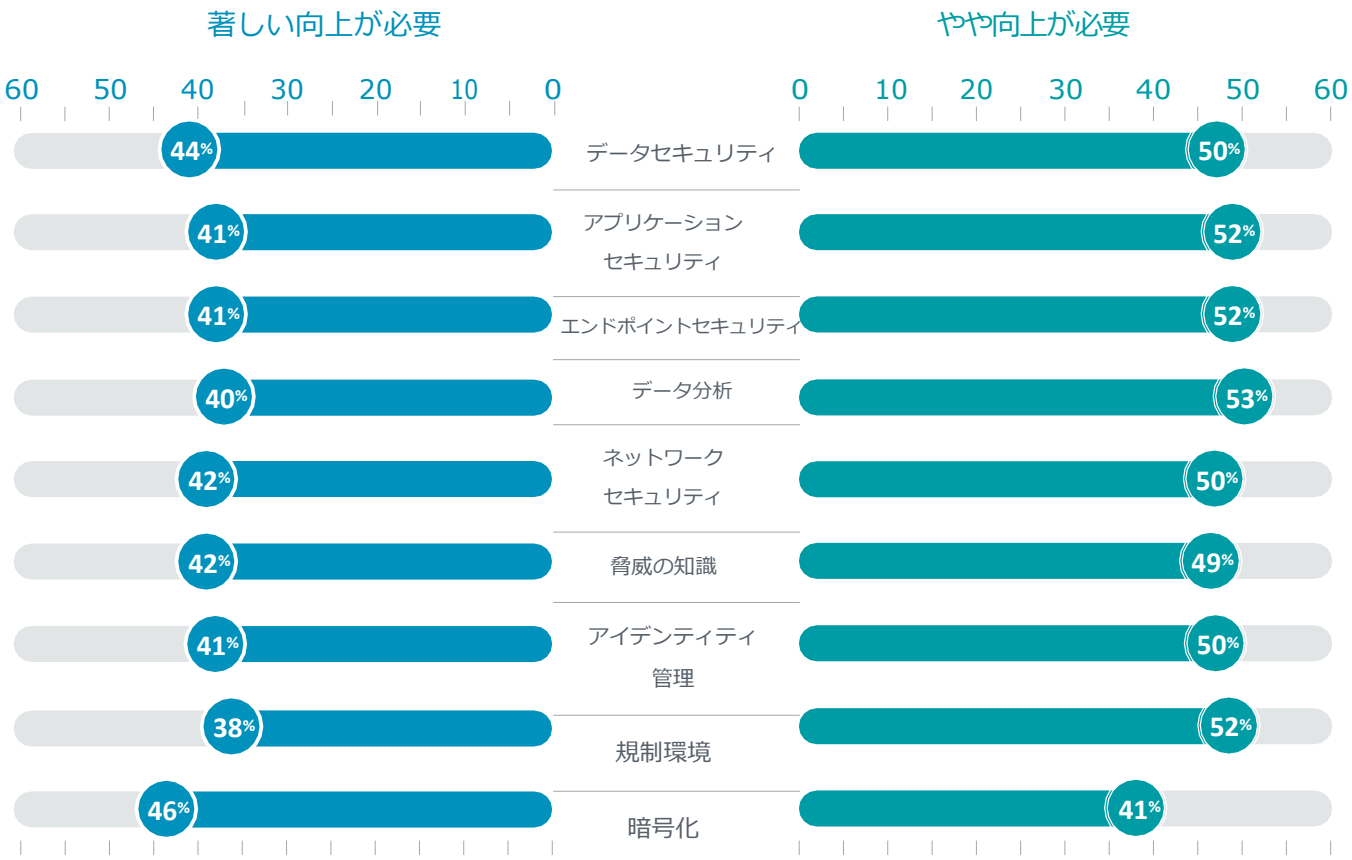


まず、議論の内容は聞く相手にとって適切でなければなりません。取締役会は通常、IT部門スタッフの日々の戦術には関心を持ちません。日々の活動と全体的な戦略の間に翻訳が必要です。そして、上層部と管理職がビジネスの利害に即した測定基準を定義し、そこからまた翻訳をするのです。2つ目に、すべての議論をつなぐ共通の糸がなくてはなりません。社内データセンターのセキュリティを向上させることで、リスク削減に役立つかもしれませんが、この話では、柔軟性を向上されられる外部のプロバイダが視野に入っていないかもしれないのです。

サイバーセキュリティのビジョンを管理するのは、セキュリティ・オペレーション・センター（SOC）の役割です。サイバーセキュリティのビジョンは組織の目標と成功に非常に緊密に結びついているので、圧倒的多数の会社はそのSOCを社内に置くことを選んでいます。形態としてはIT部門の中に置く場合もあれば、別建てで設定する場合もあります。社外にSOCを置いている会社は11%しかありませんが、その数は増加していくかもしれません。2020年、社外にSOCを置いていると答えた会社はわずか7%でした。この数が増え続けるのか、それとも同じレベルに留まるのか、追跡していく価値はあるでしょう。

サイバーセキュリティのリソース配分がどのようになされるかに関わらず、会社としては、自社のスキルを常に時機に合ったものに保つ必要性を強く認識しています。まずはスキル評価です。セキュリティ関連の他の測定基準と同様、スキルレベルの評価は歴史が浅く、様々な解釈が可能なものです。ITプロフェッショナルは個人的な強みと弱みがどのエリアにあるのか認識していることは多いのですが、それはビジネスの目標や方針に照らした重要なスキルとは、関係がないかもしれません。CompTIAのデータには、スキル間の差別化がほとんど見られません。これは実際のスキルレベルに関する知識が欠如していることを表していると考えられます。

サイバーセキュリティスキル向上の必要性



向上させるべきスキルの特定についても、同じような話になります。全体のうち、著しい向上が必要だと感じている会社は約10社に4社です。現在のスキルレベル評価をより効果的に行う方法に加えて、IT構想の持つ性質そのものが、正しいスキルに的を絞る助けになるかもしれません。

- **データセキュリティ**は、組織的なデータ戦略を構築している会社において、重要度がより高くなるようです。以前のCompTIA調査では、ほとんどの会社が自社データに対して組織的な取り組みをしていませんでした。ですから、取り組みがより厳然としたものにならない限り、データセキュリティへの適切な投資は難しいでしょう。
- **アプリケーションセキュリティ**は、クラウド移行と連動しています。特に、カスタムアプリケーションが公共クラウドインフラをホストとしている場合には。これらのアプリケーションは以前、セキュアペリメーターで守られていましたが、クラウドインフラプロバイダーが自社提供物しか保護しなくなり、そこに付加されたものはすべてクライアントの責任となってしまったために、脆弱性が増しています。
- **エンドポイントセキュリティ**は、コロナ後にワークフォースがより柔軟性を求めていることに伴い、見直されているようです。従業員がフルタイムのリモートワークを選ぶのか、それとも何日か出社するというハイブリッド型を選ぶのかに関わらず、彼らの機器はリフレッシュして再構成をする必要があります。そしてセキュリティのスキームをワークスタイルに合ったものにしなければなりません。
- **アイデンティティ管理**も、リモートで働く人のいるクラウドファーストの環境では必須事項です。最小特権アクセスの粒度が、アプリケーションやデータセットに対する強力なセキュリティを提供し、中央管理スキームによって、ワークフォース全体の柔軟性を上げるとともに、間接費も削減できます。
- **規制環境**の専門知識は、ヘルスケアや金融といった規制の厳しい業界では長いこと求められていたものです。しかし、今やどのような形態、どのような規模の会社にも重要なものとなりました。デジタルプライバシーへの精査が厳しくなり、州や国ごとに指針が異なっていることから、これらのスキルに対する需要が増しているのです。

サイバーセキュリティスキルの向上計画

スキルを向上させるため、会社はさまざまな選択肢に目を向けています。社内リソースに関しては、新規採用をいう選択肢が明らかに存在します。しかしながら、採用を試みている会社は労働市場の制約に直面しており、供給/需要問題は今後さらに悪化すると予測されています。さらに、新たな人材を迎え入れるたびに、企業文化に馴染んでもらえるようにするという負担が生じます。サイバーセキュリティ方針の決定をまさにしようとしている会社にとっては、これは複雑性を追加することになります。現在の従業員をトレーニングするというのはより実現可能な選択肢です。そして、社内での育成に認定を加えることは、これまでにも会社と従業員双方に利点があると証明されています。

社内リソースとは別に、会社は新たな提携の選択肢を検討しています。この中には、現在の外部企業との提携内容を拡大することや、新たな専門家を探すことも含まれます。第三者エコシステムには、従来型マネージドサービスプロバイダーに始まり、マネージドセキュリティサービスプロバイダー、クラウドプロバイダー、そしてエッジコンピューティングのカテゴリに含まれるその他の企業に至るまで、多くの異なった選択肢が存在します。

外部企業の選択に当たり、会社はいくつかの異なった基準を検討します。従来のMSP型により近いような既存の提携先については、提供されるサービスの中核となる部分が優れていれば、セキュリティは適切に扱われるだろうと考えられます。それぞれの組織は、サイバーセキュリティの特定の側面を対象としているため、その対象エリアにおける専門性を当然極めていくからです。最後に、会社はサイバーセキュリティをビジネスの利害に結び付けることに注力し始めています。これは、ROIを理解するための費用便益分析であったり、意思決定を向上させるための脅威インテリジェンス活用であったりします。

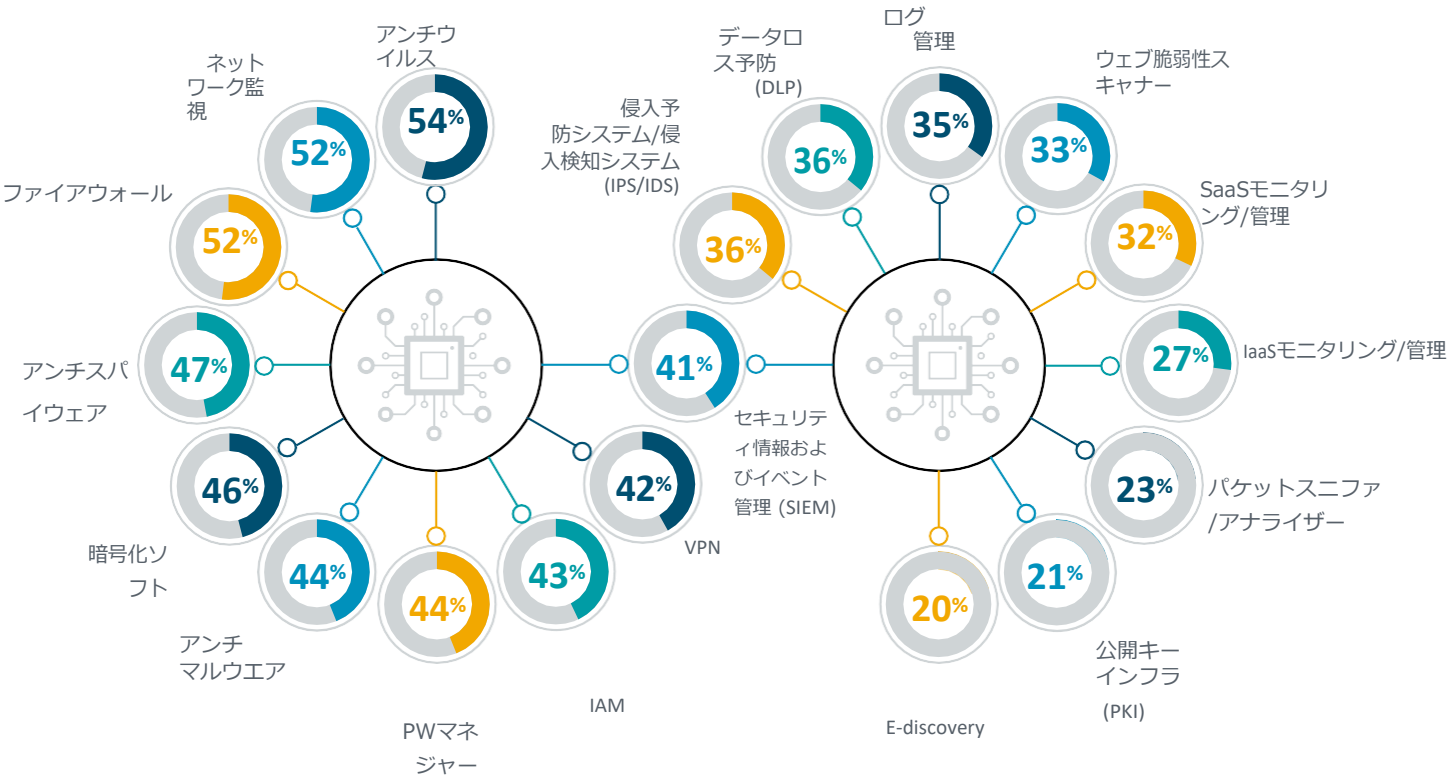
第三者サイバーセキュリティ企業の重要基準

4 製品

サイバーセキュリティパズルの最後のピースは、従来から最前部にありました。サイバーセキュリティが、主にITオペレーションの副産物とみなされていたころ、防御的テクノロジーは安全体制の主要な要素でした。多くの会社にとって、これは2つの製品に集約されます：ファイアウォールとアンチウイルスで、これらが当時、企業の考え方を支配していたセキュアペリメ―ターを形成していたのです。

今日、様相ははるかに複雑で微妙なものになっています。ツールボックスにツールがはるかに増えている、というだけではなく、それらのツールが自己完結型製品として独立していることは、ほとんどありません。その代わりに、ツールはサイバーセキュリティ戦略を構成している包括的な方針や特定のプロセスの中で機能しているのです。スキル評価と同様、CompTIAの調査で見られるツール使用数は全体に低めになっています。これは、自社のITアーキテクチャにあまり馴染みがない企業回答者が、調査に含まれているためです。それでも、データからはどのツールが十分確立されていて、どのツールがもっと検討されるべきなのかが明確にわかります。

使用しているサイバーセキュリティ製品



アンチウイルスとファイアウォールはリスト上位の位置をキープしていますが、単に過去の栄光の名残というわけではありません。アンチウイルスソフトウェアは確かに、新たに生み出される悪意あるコードの新種に対応すべく変化し続けていますが、それだけでなく、ITオペレーションの変化に適合するよう進化してきました。その中には、データセンターからクラウドへのシフト、使用されるPCのさまざまな組み合わせ、そしてスマートフォンやタブレットへの対応などがあります。同じ流れで、ファイアウォールはさらに能力を上げてきました。単純なパケットフィルタリングツールからステートフルファイアウォールへ、さらには一元的な脅威管理へと成長したのです。

最大の脆弱性のひとつは脆弱なパスワードなので、多くの会社はパスワードマネジャーを実行しています。エンドユーザー向けには、まだ試行錯誤があるようですが、これらのツールは複数サイトをカバーして強力なパスワード維持能力を提供すると同時に、中央管理もできるようになっています。パスワードマネジャーを検討している会社は、データベース接続確認情報がどこに保存されているか、そしてアカウントはどうすればリカバリーできるかに精通していなければなりません。

データロス予防（DLP）ツールは、決して新しいものではありません。しかし、まだ大量採用には至っていません。クラウドファーストアーキテクチャの基本的属性のひとつは、データそのものに保護が必要だということです。主要なストレージの選択肢としては１つの場所かもしれませんが、データはアプリケーションで使われる、あるいはモバイルデバイスに保存される可能性もある、流動的なものです。DLPソリューションによって、静止状態の時、動いている時、使用されている時のデータをモニターできるので、何か不整合があれば、セキュリティープロフェッショナルが気づくようになっています。

その他の多くのツールは、クラウドモニタリングからネットワーク分析に至るまで、特定のオペレーション上の実践を対象としています。企業が集めるツールはますます多くなっているので、すべての情報を集約して消化できるようにする必要性が、以前よりはるかに増してきています。セキュリティ情報とイベント管理（SIEM）ツールは、セキュリティチームが複雑な環境をモニタリングするためのダッシュボード機能を提供します。これらのツールにおける課題は構成です。イベントが適切にフラッグ立てされ、分析できるようにデータが収集されることを担保しなければなりません。そうすれば、大量の情報を観察し、起こりうる脅威に迅速に対応できる、簡素化された方法が手に入るのです。

さまざまなツールがあることが、サイバーセキュリティへの統制のとれた取り組みの重要性を物語っています。単にテクノロジーにプラグインしさえすれば、最上の結果が得られるなどということはまずありません。現代の戦略はまず最上層部から始まります。すべてのステークホルダーが企業方針を確実に理解するのです。その後で、プロセスを実行し、適切な人材を投入することで日々の任務が推進され、必要な製品への投資が防御と攻撃両方の手段を与えることになります。会社はサイバーセキュリティに関して迅速に動く必要があります。そして新たな世界秩序における問題を全面的に理解することが、前進するための最速の方法なのです。

Methodology 手法

この定量的調査は2021年第3四半期に、ワークフォース・プロフェッショナルを対象としたオンライン調査を基にしています。アメリカ合衆国で活動する全400名のプロフェッショナルが参加し、信頼区間95%における標本誤差代理変数の全体的マージンは+/−5.0パーセントポイントとなりました。標本誤差はデータのサブグループでより大きくなっています。

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。

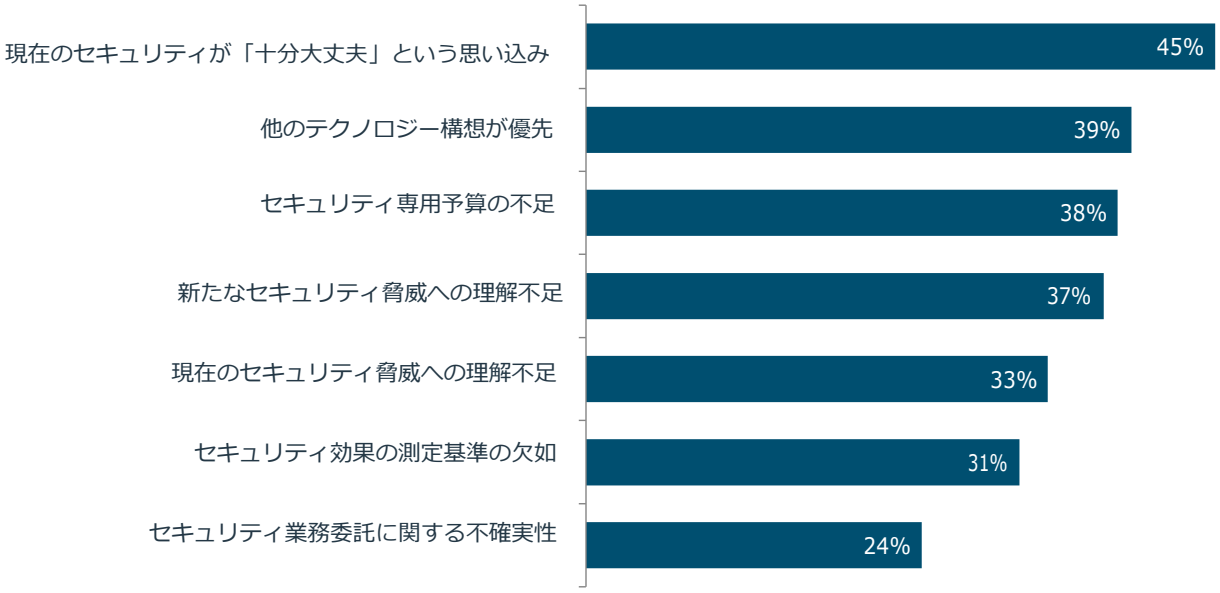
CompTIAについて

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。

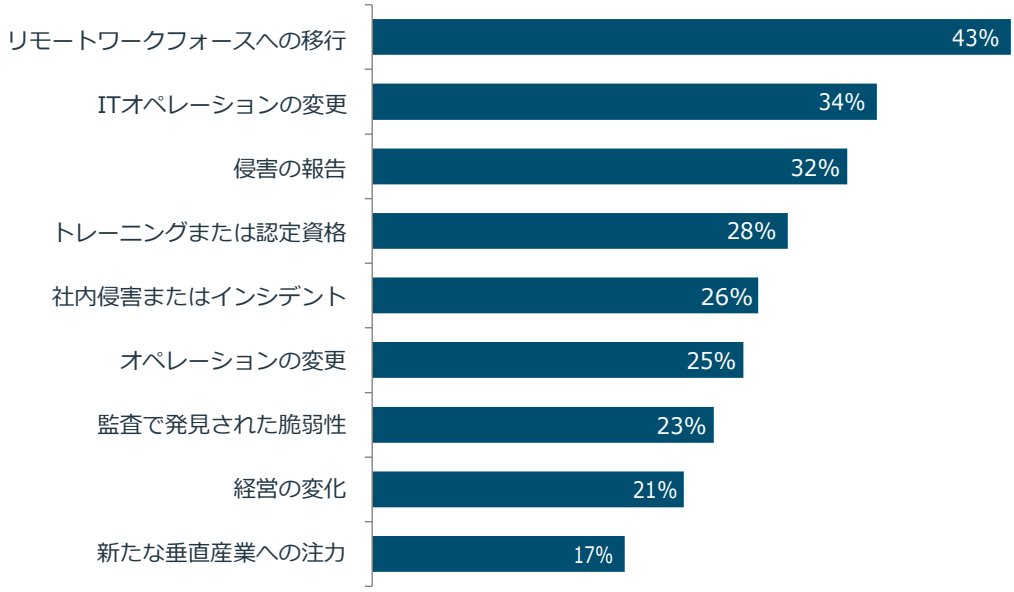
CompTIAは世界有数のベンダーニュートラルなIT認定団体であり、提供されるパフォーマンスベースの試験による認定者数は280万以上にのぼります。CompTIAはエントリーレベルからエキスパートレベルのプロフェッショナルまで、テクノロジー分野におけるキャリアのあらゆるステージでの成功に欠かせない業務能力を評価します。また、慈善活動として、CompTIAは革新的なオンランプ（入口）およびキャリアパスを開発しました。これは、従来、ITワークフォースとして活躍することの少なかった人々に対する機会を拡大するものです。

Appendix 別表

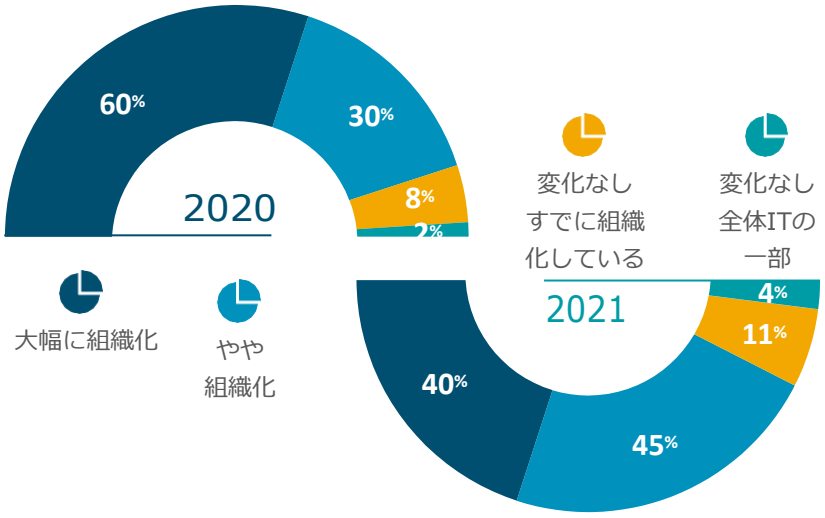
サイバーセキュリティ取り組みを変える際の障害



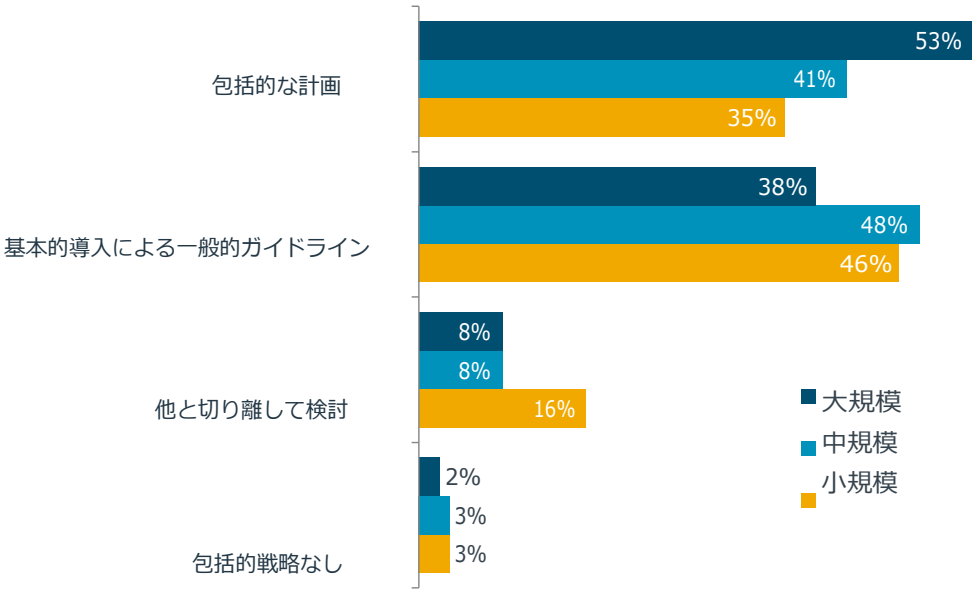
サイバーセキュリティ取り組みを変えるきっかけ



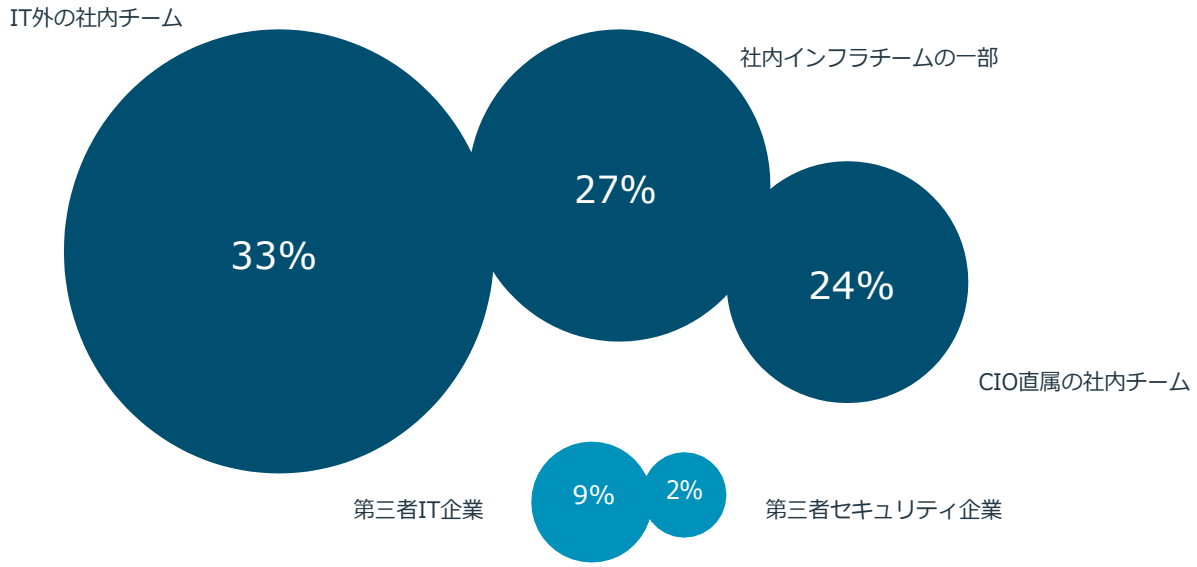
サイバーセキュリティ実践への取り組み



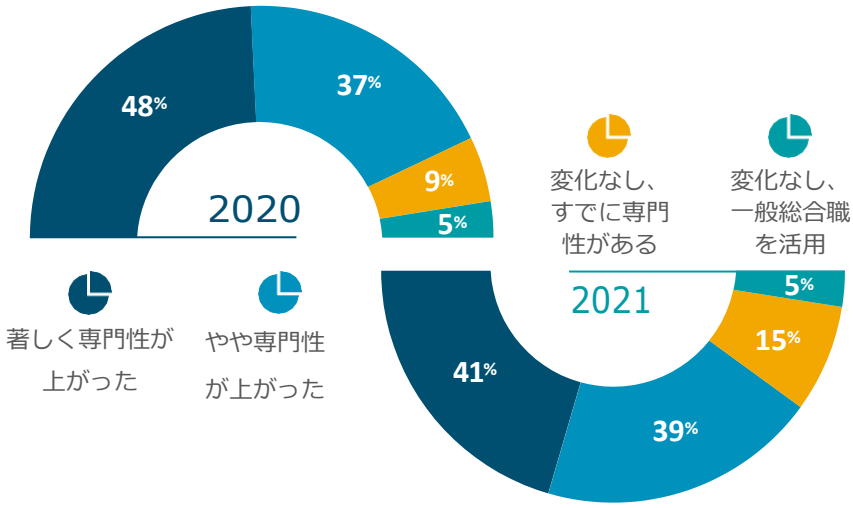
サイバーセキュリティチェーンにおける検討内容の特性



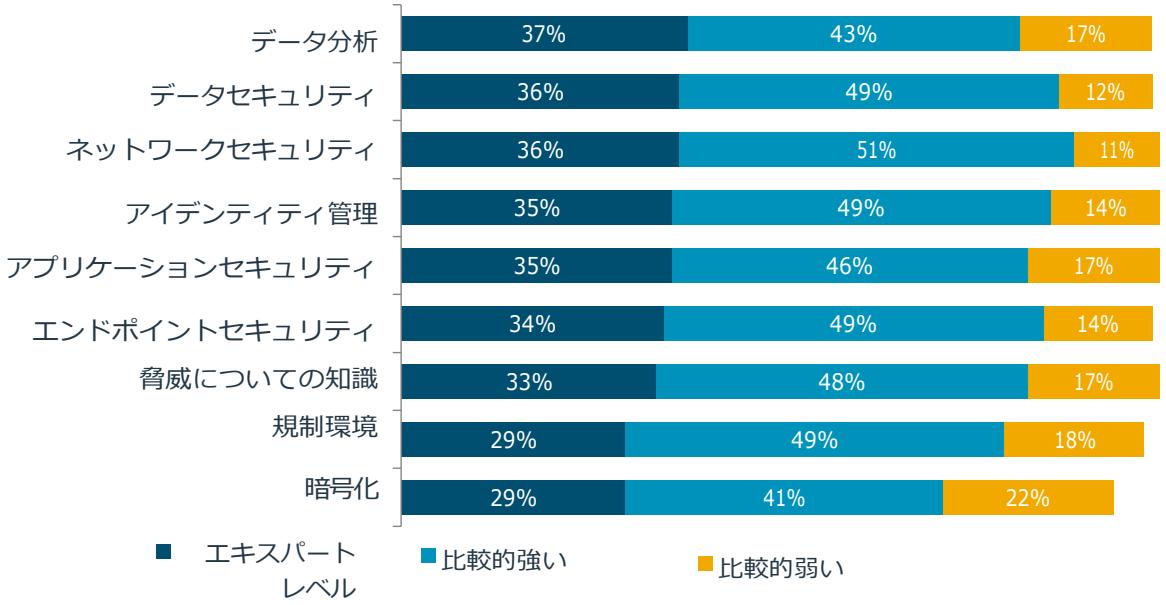
セキュリティオペレーションセンターの場所



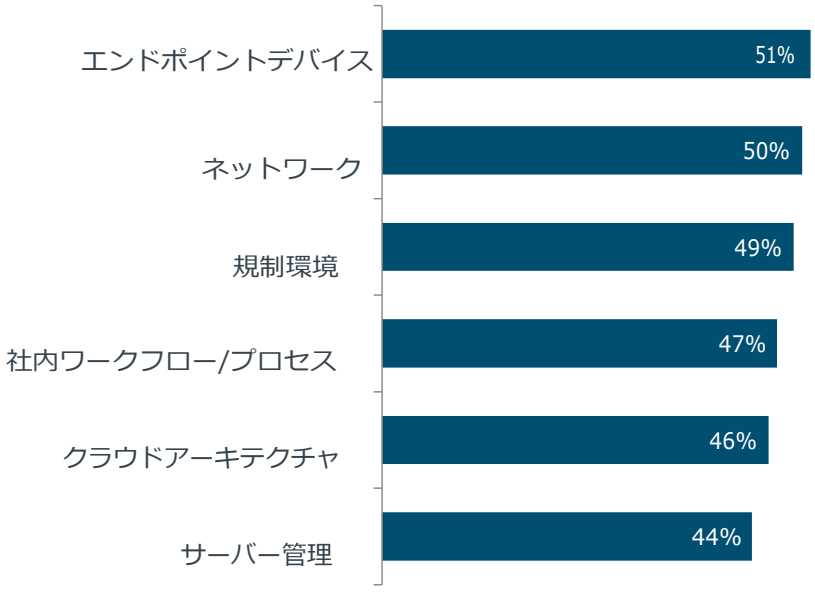
サイバーセキュリティ人材への取り組み



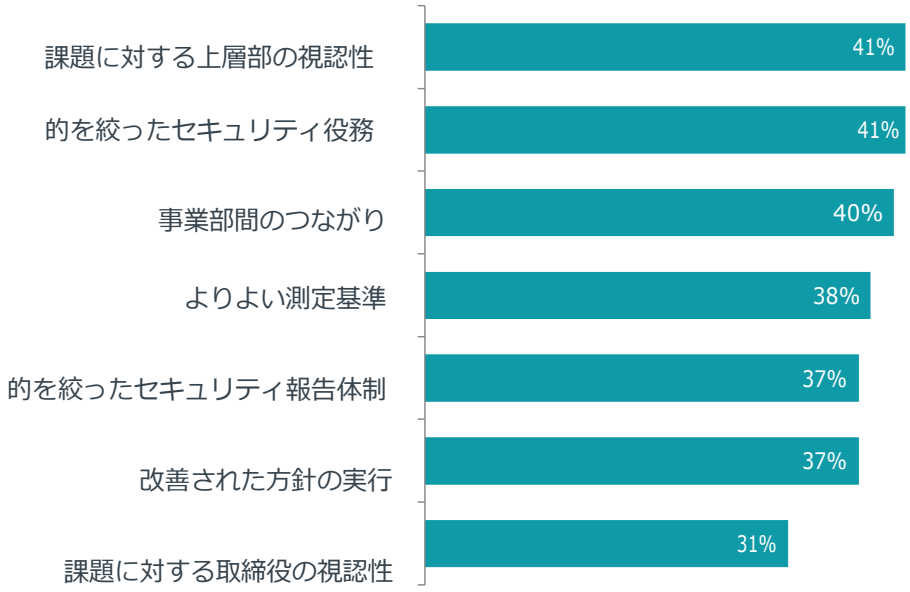
サイバーキュリティスキルの評価



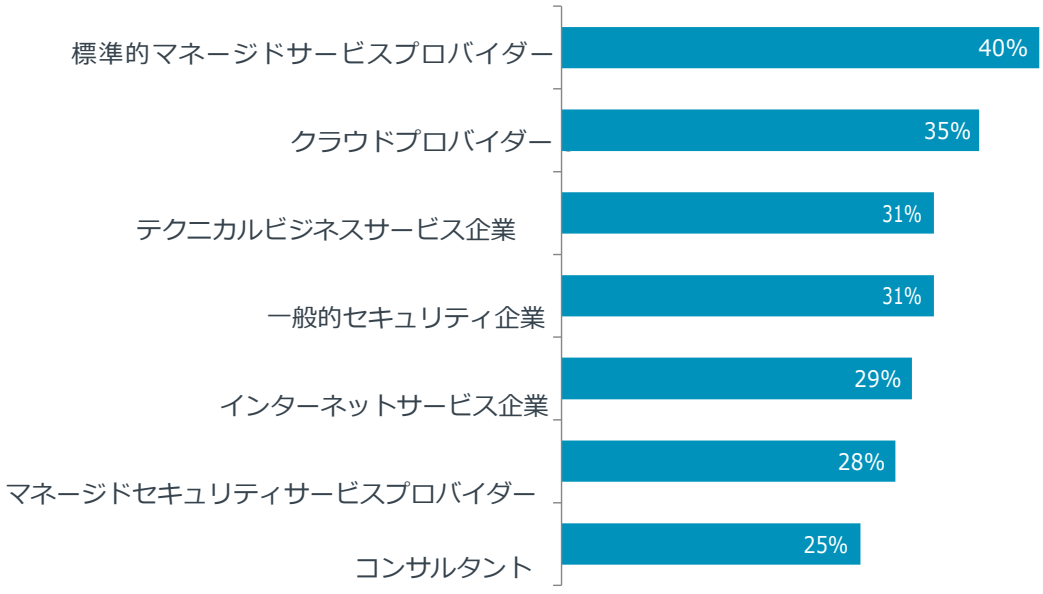
サイバーセキュリティ役職の前提となる知識



セキュリティリソースの効率向上に向けての行動



サイバーセキュリティに関わる第三者企業のタイプ



Sources

1 IBM/Ponemon Cost of a Data Breach Report 2021

2 IBM/Ponemon Cost of a Data Breach Report 2021

3 AV-TEST Institute

4 U.S. SEC filing, 12/14/20

5 Sophos State of Ransomware 2021 report

6 Proofpoint 2021 State of the Phish Report

7 Gartner | Spending amounts shown in millions of U.S. dollars

8 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

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.