SOPHOS
Cybersecurity evolved.

IT セキュリティチームの現状：2021年以降の展望

30ヶ国 5,400 人の IT 管理者を対象とした調査結果

ソフォス ホワイトペーパー2021年6月

IT チームは、ほとんどすべての組織でパンデミック対応の最前線に立たされています。COVID-19 による制約や制限にも関わらず、組織が業務を継続できるようにするために、IT 部門は直接的かつ重要な役割を果たしてきました。世界中の献身的で情熱的な IT チームによる大きな貢献のおかげで、多くの組織がパンデミック中も業務を続けることができるようになりました。教育機関では、オンライン学習、小売業では、オンライン取引への切り替えを IT チームが支援し、また、公共機関では必要なサービスをオンラインで継続的に提供できるようにしました。

このレポートは、30ヶ国 5,400 人の IT 管理者からの直接のフィードバックを基に、過去 12 か月に IT チームが直面した現実に焦点を当てています。2020 年に IT チームが経験した変化、特にサイバーセキュリティに注目し、その変化が IT チームのメンバーに与える影響を明らかにしています。また、このレポートでは、IT セキュリティチームの将来についても考察し、今後 5 年間の IT への期待を明らかにし、組織が将来の IT チームの構築を開始できるように支援します。

主な調査結果

2020 年の IT チームの経験の変化

- **IT とサイバーセキュリティの仕事量の増加:** 63%がセキュリティ以外の仕事量が増加し、69%が IT セキュリティの仕事量が増加した。
- **さらに蔓延するサイバー攻撃:** 61% が、組織に対するサイバー攻撃の増加を報告
- **サイバーセキュリティ機能を強化した IT チーム:** IT チームの 70% が、この期間中にサイバーセキュリティのスキルと知識をさらに向上させたと回答
- **逆境によりチームが一つに:** 52% が、この 1年間でチームの士気が向上したと回答し、ランサムウェアの被害者は、攻撃を受けなかった組織よりもチームの士気が向上した可能性がかなり高いと回答 (60% 対 47%)

現状

- **複雑な攻撃に対処するための支援が必要な IT チーム:** 回答者の 54%が、現在、サイバー攻撃は、組織内の IT チームが単独で対処するには高度すぎると回答
- **目の前の課題に十分な準備が出来ていると感じる IT チーム:** 82% は、完全に疑わしいアクティビティを調査するためのツールと知識を持っていると考えている

未来の IT チーム

- **IT セキュリティ チームの規模は拡大する見通し**
  - 68% は、2023 年までに社内の IT セキュリティスタッフが増加し、2026 年までに 76% 増加すると予測
  - 56% は、アウトソーシングをする IT セキュリティスタッフが 2023 年までに増加し、2026 年までに 64% 増加すると予測
- **AI 技術は、将来のセキュリティ戦略における重要なツール**
  - 92% が、AI により脅威の増加や複雑さに対応できると予測

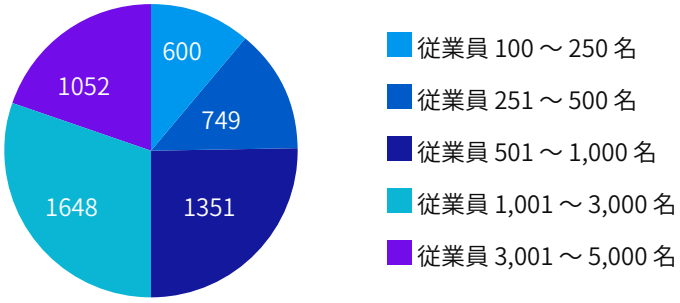
調査方法について

ソフォスは、独立系の調査会社 Vanson Bourne 社に委託して、30 か国にわたる 5,400 人の IT 意思決定者に調査しました。この調査は、2021年 1月と 2月に実施されました。

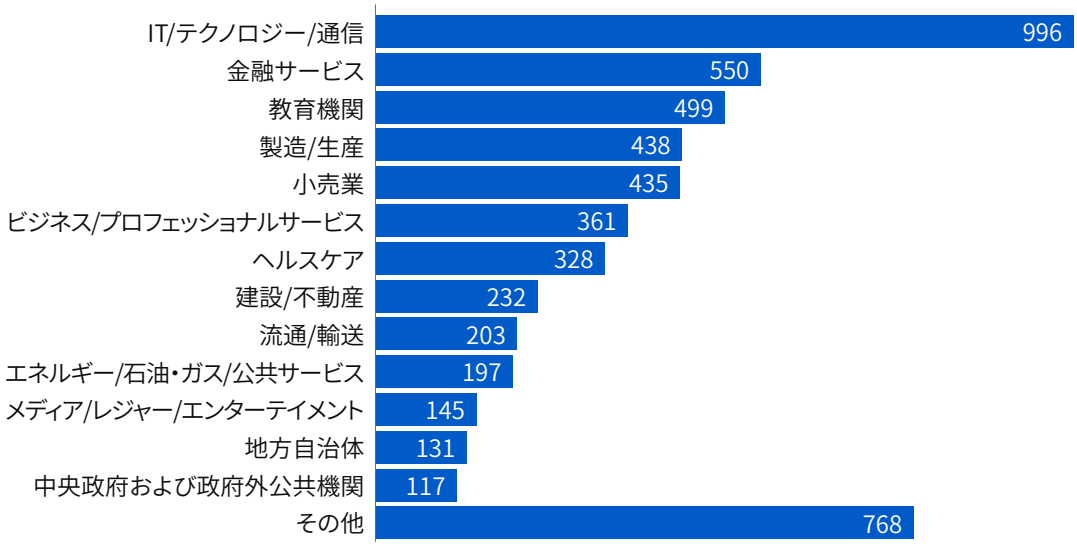
国	回答者数	国	回答者数	国	回答者数
オーストラリア	250	インド	300	サウジアラビア	100
オーストリア	100	イスラエル	100	シンガポール	150
ベルギー	100	イタリア	200	南アフリカ	200
ブラジル	200	日本	300	スペイン	150
カナダ	200	マレーシア	150	スウェーデン	100
チリ	200	メキシコ	200	スイス	100
コロンビア	200	オランダ	150	トルコ	100
チェコ共和国	100	ナイジェリア	100	アラブ首長国連邦 (UAE)	100
フランス	200	フィリピン	150	英国	300
ドイツ	300	ポーランド	100	米国	500

各国の回答者は、従業員数 100 ～ 1,000 名の組織が 50%、1,001～5,000 名の組織が 50%になっています。また、回答者の業種も多岐にわたります。

グローバルな従業員数[5,400]



組織の業種[5,400]



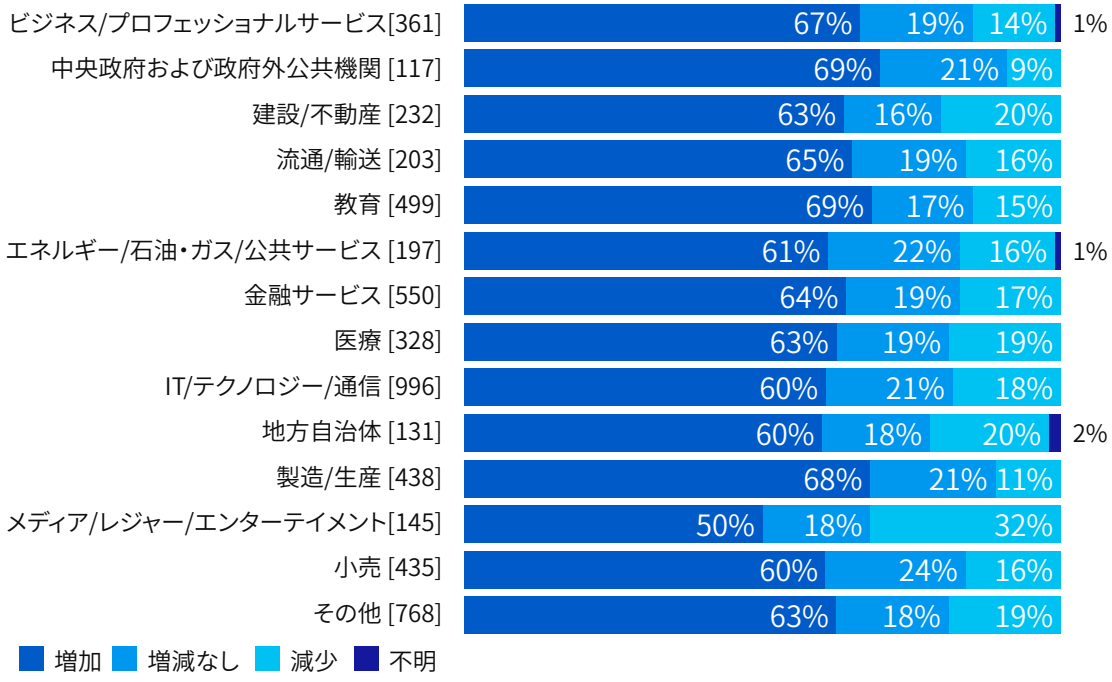
2020年: 変化の年

2020 年は他に類を見ない変化の年でした。IT チームは、パンデミックに対応し、組織の運用を適応させるために最前線にいました。当然ながら、これは仕事量に大きな影響を与えました。

セキュリティ以外の IT に関する仕事量の増加

IT チームに多くの新たな作業をもたらした 2020年: IT 管理者の 63%、セキュリティ以外の仕事量が 2020 年に比べて増加し、減少したと回答したのがわずか 17% でした。トルコ (84%)、オーストリア (81%)、米国 (75%) の回答者は、仕事量の増加を報告する可能性が最も高いと回答しました。

IT の仕事量 (セキュリティ以外) が 2020 年にどのように変化したか



2020年では、ITの仕事量（セキュリティ以外）は、業界ごとに分割され減少 / 増加 / 増減なし [グラフ内の基本サイズ] があります。

業界ごとにデータを見ると、**中央政府/政府外公共機関**および**教育機関**の IT 部門が最も影響を受けていることが分かります。回答者の 69% が、パンデミックに対応するために政府と教育機関の両方が対応において中心的な役割を果たしたために、仕事量が 1年で増加したと報告しています。それとは逆に、**メディア/レジャー/エンターテインメント**は回答者の 32% が減少したと回答し、最も高い割合でした。おそらくこの原因の 1つは、パンデミックのために多くの施設でサービスを制限しなければならなかったことが考えられます。

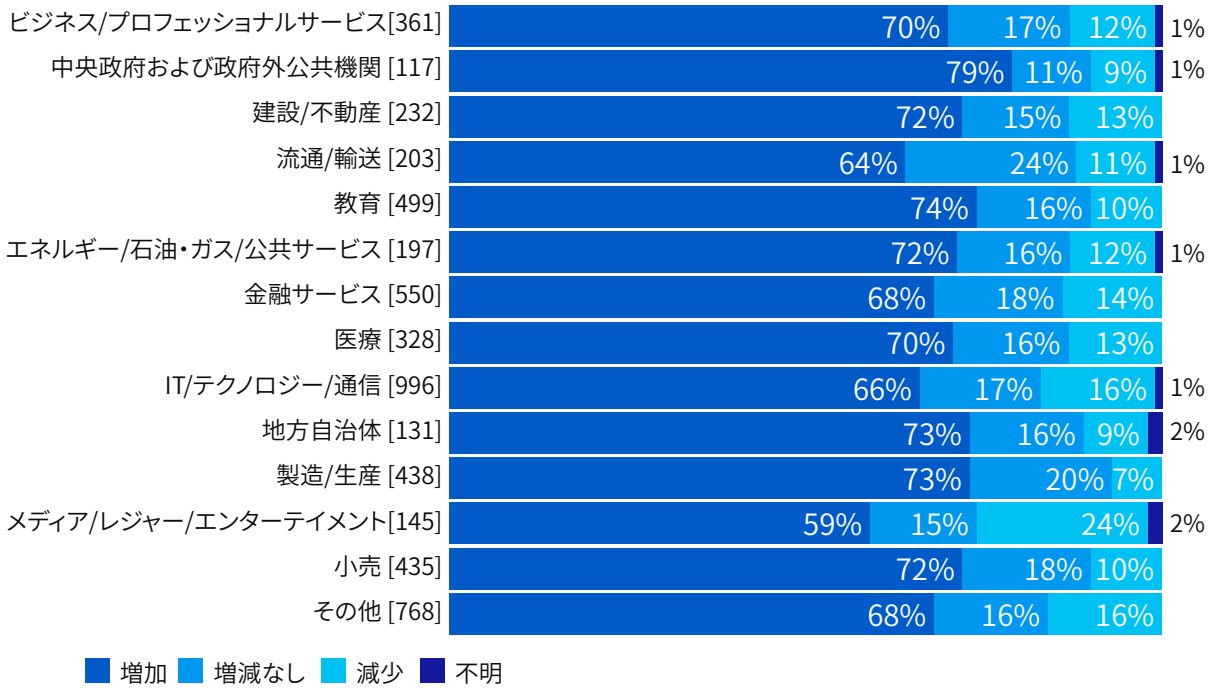
サイバーセキュリティの仕事量がさらに増加

サイバーセキュリティが 2020 年にどのように変化したか

「不明」を除くと、2020年では、サイバーセキュリティの仕事量は減少 / 増加 / 増減なし [5,400人] があります

回答者の 69% がサイバーセキュリティの仕事量は前年よりも増加、13% が減少、17% が仕事量は増減なしと回答しました。トルコ（82%）が再び最高レベルの増加を報告し、スウェーデン（80%）、イスラエル、ブラジル（共に78%）がそれに続きました。それとは対照に、アラブ首長国連邦の回答者はサイバーセキュリティ仕事量の減少を報告する割合が最も高く（26%）、その後にスイス（22%）、ナイジェリア、フィリピン（共に 19%）が続きました。

サイバーセキュリティが 2020 年にどのように変化したか



2020 年では、サイバーセキュリティの仕事量 は、業界ごとに減少 / 増加 / 増減なし [グラフ内の基本サイズ] があります。

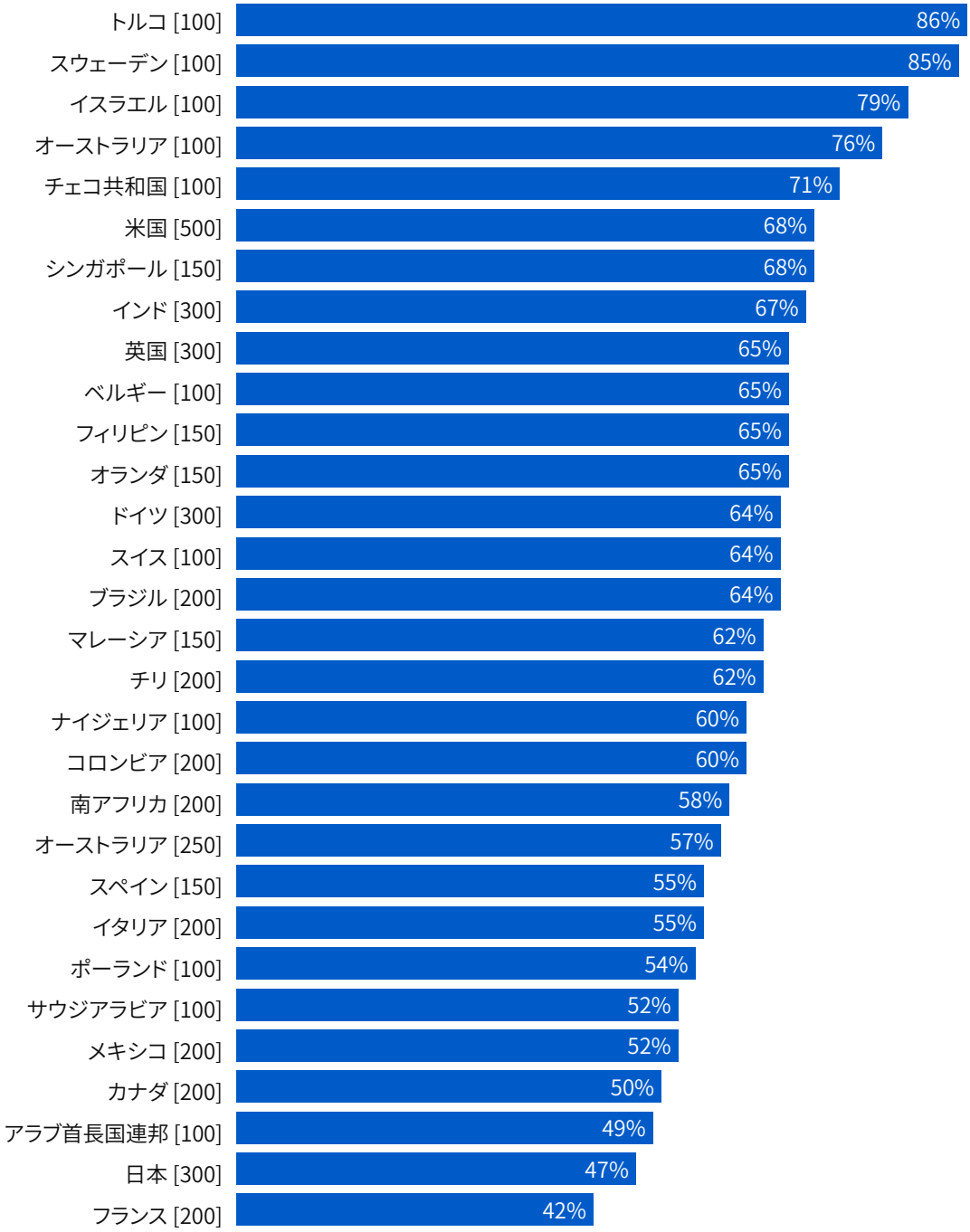
今まで見た業界の傾向をみても、**中央政府/政府外公共機関** (79%) および **教育機関** (74%) の IT 管理職は、サイバーセキュリティの仕事量が前年よりも増加すると報告し、**メディア/レジャー/エンターテイメント**の IT 管理者は減少 (24%) すると報告する可能性が最も高かったです。繰り返しになりますが、このような業界は、非常に異なる方法ではありますが、パンデミックの影響を最も受けていることが原因である可能性が高いと考えられます。

増加したサイバー攻撃の頻度

2020年にサイバーセキュリティの仕事量が増加した背景は、サイバー攻撃の増加が一因となっています。昨年の回答者の10 人中 6 人（61%）が組織に対する攻撃の増加を報告しています。減少を報告したのはわずか 19% でした。

この増加はすべての業界で発生し、最大 **(中央政府/政府外公共機関)** と最小 **(IT/テクノロジー/通信、**および**メディア/レジャー/エンターテイメント)** の増加を経験した業界間の差異はわずか 16 パーセント (74% 対 58%) でした。

2020 年にサイバー攻撃の増加を経験した組織の割合

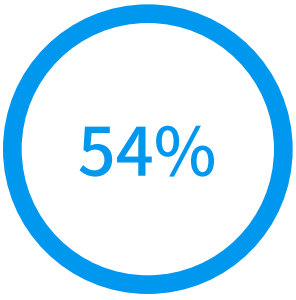


2020年の間、サイバー攻撃は増加 [グラフ内の基本サイズ] しており、一部の回答オプションを省略し、国ごとに分割

しかし、国別のデータを見ると、トルコではフランスの2倍以上(86% 対 42%)の回答者が攻撃の増加を報告しており、攻撃の経験に大きな差があることが分かります。また、スウェーデン（85%）、イスラエル（79%）、オーストリア（76%）の回答者も非常に高い割合で、2020年に組織へのサイバー攻撃が増加したと報告しました。逆に、フランス、日本、アラブ首長国連邦では、増加の報告は半分以下でした。

阻止が困難になってきた攻撃

高度なサイバー攻撃は複雑かつ複数の段階を踏んで実行され、攻撃者はインシデントの過程で無数の戦術、テクニック、手順（TTP）を使用します。これらの攻撃への対処は困難で、回答者の半数以上 (54%) が、IT チームが自分達で対処するには攻撃が高度すぎると考えています。

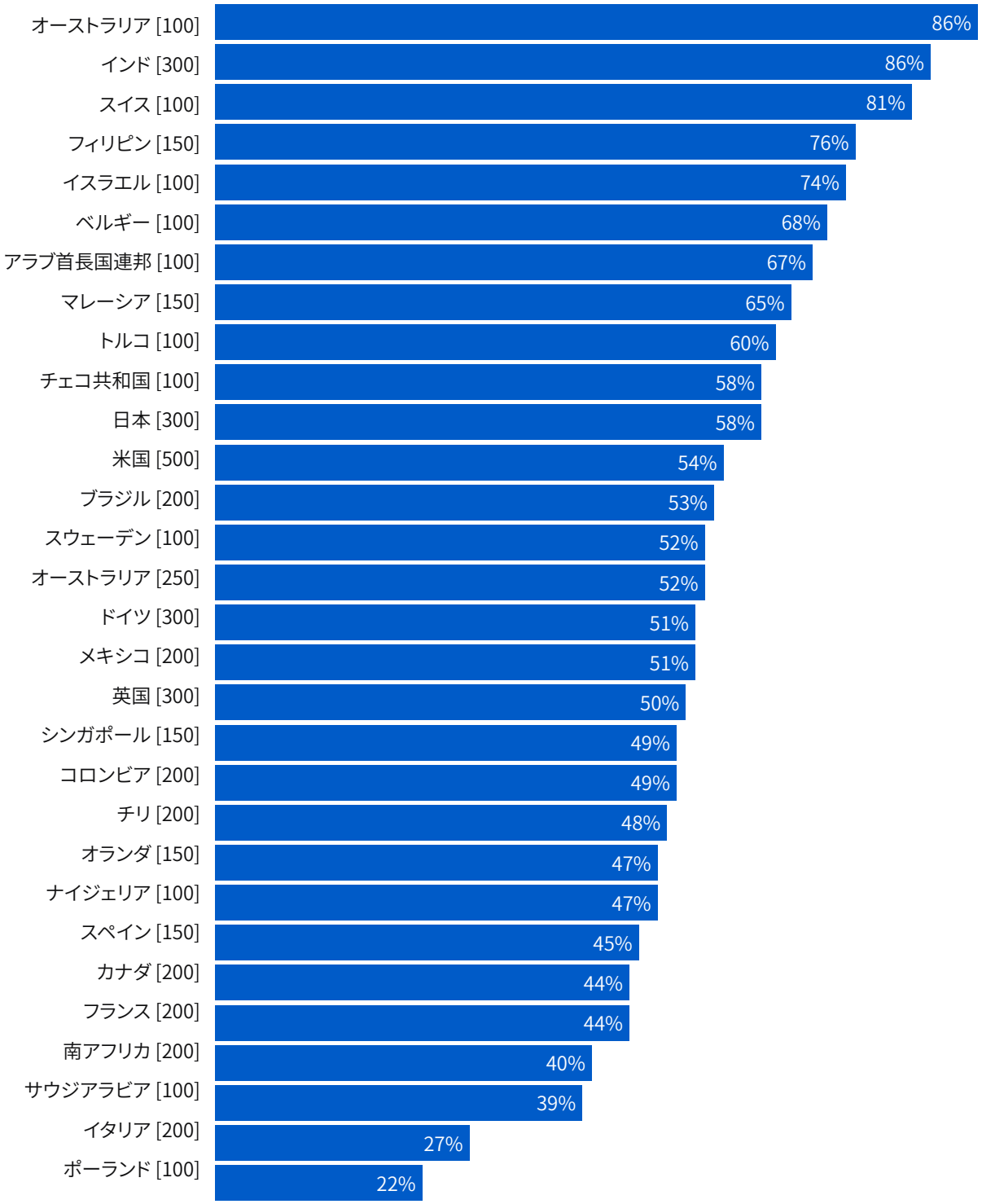


現在、組織内の IT チームが単独で対処するには攻撃は高度すぎると回答

この課題は、**ビジネスおよび専門サービス**部門で最も深刻です。回答者の 63% が、自分達でサイバー攻撃に対処する能力がなくなったと考えており、そのあとに続き**中央政府/政府外公共機関** (62%) および **医療機関** (60%)) が同じように考えています。逆に、**建設/不動産業界**、および**地方自治体**が同じように考える可能性は低い結果でした (47%)。ランサムウェアの現状 2021 年版で報告されているように、地方自治体の場合、これは驚くべき発見です。この業界はランサムウェア攻撃でデータを暗号化される可能性が最も高いためです。

調査対象国の中で、複雑な攻撃への対処における自信レベルにかなりのばらつきが見られます。

現在のサイバー攻撃は、組織内の IT チームが単独で対処するには高度すぎると考える回答者



サイバー攻撃は、現在の組織の IT チームが単独で対処するには高度すぎると同意する回答者[グラフ内の基本サイズ]一部の回答の選択肢を省略し、国ごとに分割

オーストリアとインドを拠点とする企業は、攻撃への対応に対する自信が最も低いと回答しています。86% が、現在 IT チームが単独で対処するには複雑すぎると回答し、その後に、スイス（81%）、フィリピン（76%）、イスラエル（74%）が続いて回答しています。

攻撃の複雑さを認識し、外部の専門知識がいつ必要かを特定することが、今日の高度なサイバー攻撃から防御する重要なステップとなります。SophosLabs と Sophos Managed Threat Response (MTR)チームは、自動化と実践的なライブハッキングを組み合わせて、組織の防御を回避しようとする攻撃が着実に増加していることを確認しています。これらの巧妙な攻撃を阻止するには、熟練した専門家が必要です。組織はこれらのスキルを外部に委託する必要があることを認識するのが賢明です。

一方、ポーランドは社内でサイバー攻撃に対処する際の課題が最も少ないと報告しており、IT チームが攻撃を処理するには高度すぎると答えた回答者は 22% のみです。イタリア（27%）はそれ直後に続いています。攻撃の増加に直面しても自身を持っているのは、攻撃者の先を行くことができる熟練した専門家を採用し、育成への投資によるものかもしれません。しかし、今日の高度な攻撃に直面した際に誤った自信を反映している可能性もあります。攻撃者は常にアプローチを進化させているため、彼らを阻止するために必要な専門知識レベルについて現実的に考えることが重要となります。

対応時間の減少

2020 年では、仕事量が大幅に増加していることと、パンデミックに適応するための課題があること考えると、回答者の大多数（61%）がこの期間に IT に関する問い合わせへの対応時間の増加を報告していることは驚くべきことではありません。この期間中に対応時間が減少したと 20% は答えましたが、19% は増減なしでした。

2020 年の IT に関する問い合わせへの対応時間の変化

「不明」を除くと、2020年では、IT に関する問い合わせの対応時間の減少 / 増加 / 増減なしがあります [5,400人]

回答者の 65% が増加したと回答した**教育分野**では、対応時間の増加が最も多く見られました。ほとんどの国の教育機関は 2020年にオンライン学習に転換する必要があったため、ITチームにはかなりの負担がかかり、問い合わせへの迅速な対応にも影響が出ています。

メディア/レジャー/エンターテインメントの応対時間が最も減少し、約 3分の 1（32%）が問い合わせ対してより迅速に対応ができたと回答しています。ここでも、パンデミックがこの変化の主な要因であると考えられます。組織の生産量が減ることで、ITチームの時間が確保され、より迅速な対応が可能になります。

IT チームに与える 2020 年の影響

悪い話ばかりではありません。IT チームの状況について、勇気づけられるニュースもたくさんあります。IT 管理者の 70% は、2020年までにサイバーセキュリティのスキルと知識をさらに発展させる能力が向上したと回答し、わずか 12% が減少したと回答しています。

2020 年にサイバーセキュリティのスキルと知識をさらに発展させる能力の変化

2020年に、サイバーセキュリティの知識とスキルをさらに発展させる能力は「不明」を除いて、減少 / 増加 / 増減なし [5,400人] があります。四捨五入のため、結果の合計は 100% にはなりません。

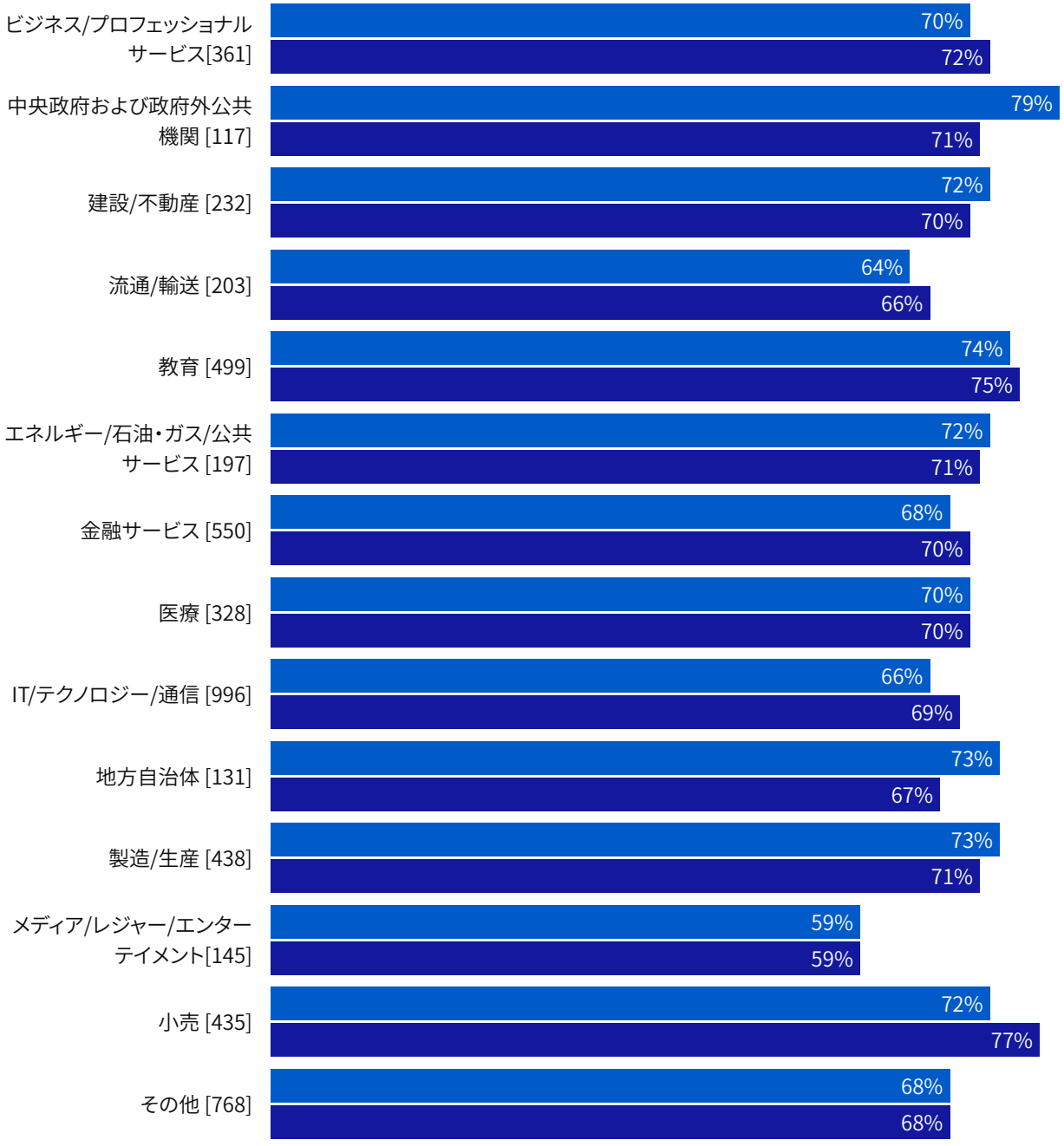
興味深いことに、特にパンデミックの影響を受けたいくつかの業界は、対照的な経験を報告しています。

- **小売業**は、サイバーセキュリティのスキルと知識を最も向上させることができた業界でした（77%）。ロックダウン中にオンライン販売に大きな変化が生じ、この業界の IT チームに新たな課題と機会がもたらされた可能性があります。
- **教育業界**は、サイバーセキュリティのスキルと知識が 2番目に向上しました（75%）。これは昨年の大きな変化を経験したもう一つの業界であり、オンライン授業やオンライン学習への移行は IT チームにとって間違いなく大きな課題ではありましたが、同時に大きな学習機会も生み出しました。
- **メディア/レジャー/エンターテインメント** が最も低い増加率（59%）を報告しました。この業界は、セキュリティ以外とサイバーセキュリティの両方の仕事量の最大の減少にも注目しており、アクティビティの減少により開発機会が制限される可能性があります。

仕事量の増加により、知識とスキルが向上

全体的に、データでは、すべての業界においてサイバーセキュリティの仕事量の増加と、サイバーセキュリティの知識とスキルを開発する能力の向上との間に明確な相関関係があることが明らかになりました。

サイバーセキュリティの仕事量の増加とサイバーセキュリティに関する知識とスキルの開発能力の向上



業界ごとに表示された 2020年のサイバーセキュリティの仕事量の増加 / 2020年のサイバーセキュリティの知識とスキルを向上させる能力の増加 [グラフ内の基本サイズ]

2020年のサイバーセキュリティの仕事量が増加すると回答したうち、84% はサイバーセキュリティのスキルと知識を開発能力で向上したと回答しています。同様に、組織に対するサイバー攻撃の増加を報告した 10 人中 8 人（82%）も、サイバーセキュリティのスキルと知識を開発する能力が向上したと述べています。これは、当然のことです。仕事量やサイバー攻撃の増加はプレッシャーを与える一方で、新しいスキルを開発する機会も提供します。

チームの士気の向上

調査した IT 管理者の半数以上（52%）が、2020年ではチームの士気が高まったと回答しています。26% が減少したと回答し、22% が増減なしであると回答しました。

2020 年のチームの士気の変化

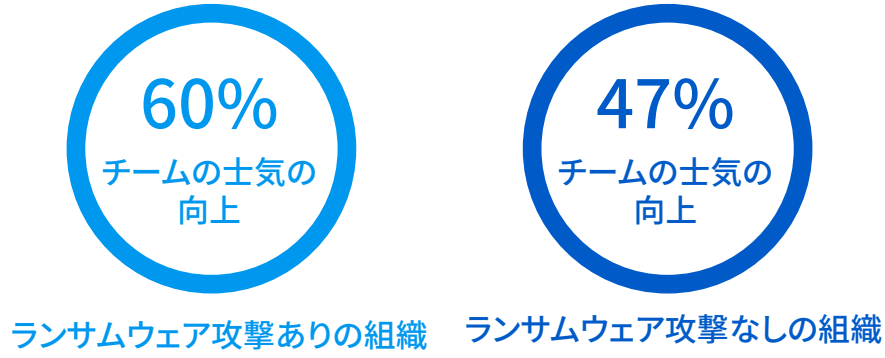
「不明」を除くと、2020年では、チームの士気は減少 / 増加 / 増減なし [5,400人] があります

地理的には、最大の士気の増加は、トルコ（75%）、オーストリア（71%）、インドと南アフリカ（両方とも 69%）と報告されています。一方、イスラエル（26%）、フランス（31%）、イタリア（33%）、ポーランド（36%）の IT チームは、チームの士気の向上を報告する割合が最も低くかったようです。

ここで名前に挙がったいくつの国は、前のセクションでも言及されていたことに気づいたかもしれません。チームの士気が向上した回答した人の割合が最も高かったトルコとオーストリアは、サイバー攻撃が増加した上位 4か国の 1つでした。同様に、フランスは調査したすべての国の中で士気の向上やサイバー攻撃の増加を報告した回答者の割合が 2番目に低い結果となりました。サイバー攻撃の経験とチームの士気との相関関係は、調査で最も印象的な調査結果の 1つです。

この点をさらに裏付けたのは、過去 12か月間に組織がランサムウェア攻撃を受けたと回答した 60% は、攻撃を受けなかったと回答した 47% と比較して、チームの士気が向上したと報告しました。

2020 年のチームの士気の変化

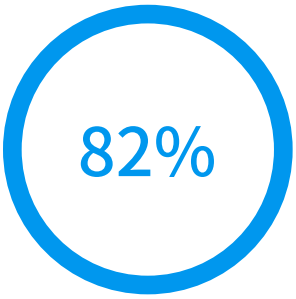


2020年の間、いくつかの回答の選択肢を除き、チームの士気は、減少 / 増加 / 増減なし [5,400人] があります。昨年のランサムウェアの攻撃を受けた回答者ごとに分類

この相関関係の背景には、いくつかの要因が考えられます。逆境 (ここではサイバー攻撃) は、多くの場合、仲間が集まり、チームとして共通の目標に一丸となって作業をする機会を提供し、士気を高めます。さらに、増加する攻撃に直面している組織をサポートできることは、ある満足感をもたらします。士気の最大の上昇は、パンデミックの影響を大きく受けた 2つの業界によって報告され、**教育業界** は最高の改善 (58%) を経験し、**医療業界** (57%) がそのすぐ後に続きます。

同時に、IT チームがパンデミックに直面してビジネスの継続性を実現する上で極めて重要な役割は、自分たちの貢献に対する認識や評価を高め、士気を高めることにもつながっていると考えられます。もし IT チームが十分に認識、評価されていない場合は、今がそのタイミングです。

目の前の課題に十分準備が出来ていると感じる IT チーム



完全に疑わしいアクティビティを調査するためのツールと知識を持っていると考えている割合

組織内で疑わしいアクティビティを検出した場合、完全に調査するために必要なツールや知識を持っていると思うと回答した人 [5,400]。いくつかの回答の選択肢を除く。

2020年にサイバー攻撃の仕事量と頻度が増加する中、IT 管理者の 82%が、組織内で完全に疑わしいアクティビティが検出された場合には、それらを調査するのに必要なツールや知識を持っていると述べたことは心強いことです。2020年のスキルと知識を開発する機会は、今後の課題に対応するためにチームを適切に配備することにあります。IT チームがサイバー攻撃の継続的な進化に対応できるようにするためには、ツールとトレーニングへの投資を継続することが不可欠です。

しかし、分野別にこの質問の回答を見ると、**中央政府/政府外公共機関** (67%) および **地方 自治体** (64%) という 2つの明らかな異常値があります。世界各地で、政府部門はパンデミックの影響を大きく受けています。市民と組織の両方に追加のサポートを提供しつつ、長期にわたる混乱の中で重要なサービスの継続性を確保する必要があります。同時に、公共機関の資金調達は多くの国で継続的な課題であり、利用可能なリソースが制限される可能性があります。ランサムウェアの攻撃者は政府機関に重点を置いているため、疑わしいアクティビティを効果的に調査するために必要なリソースとスキルを持っていることが不可欠です。

未来の IT セキュリティチーム

私達が見たように、昨年は多くの IT 業界にとって困難な年でした。しかし、IT チームは昨年の課題に見事に立ち向かい、その結果、スキルと士気の両方が向上しました。これらの経験は、柔軟な作業の拡大やクラウドの使用など、IT 環境の幅広い変化とともに、今後の IT セキュリティチームに直接的な影響を与えます。

IT セキュリティ チームは迅速に拡大する見通し

IT チームに対する需要の高まりに対応するために、回答者は、社内やアウトソーシングされた IT セキュリティスタッフの規模が、大幅に拡大すると予想しています。特に今後 2年間では、次のようになることが予測されます。

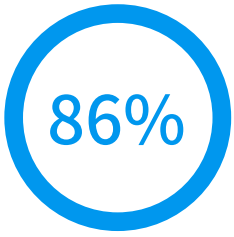
- 68% は、今後 2年間で社内スタッフが増加、76% は今後 5年間で増加すると予測
- 56% は、アウトソーシングされた IT スタッフが今後 2年間で増加、64% は今後 5年間で増加すると予測
- わずか 8% が、社内スタッフの人数が 5年以内に減少すると予想

IT セキュリティのリソース	予測される変化	2023 年までに	2026 年までに
社内の IT セキュリティスタッフ	増加	68%	76%
	減少	11%	8%
アウトソーシングした IT セキュリティスタッフ	増加	56%	64%
	減少	14%	10%

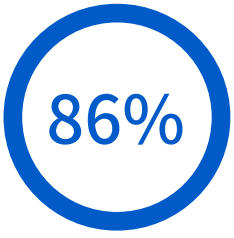
2023年と 2026年までに、組織の IT セキュリティチームの規模はどのように変化すると思いますか？[5,400人] いくつかの回答オプションを除く興味深いことに、アウトソーシングされた IT スタッフの増加により社内チームが減らされることはありません。回答者の半数近く (46%) は、社内およびアウトソーシングされた IT セキュリティスタッフの両方が 2023年までに増加し、2026年までには 55% に増加すると予測しています。

全体として、回答者の 77% は、今後 2年間で少なくとも 1つのリソースエリア (社内またはアウトソーシング)の成長を予測しており、2026年までに 85% に増加しています。

AI が ”鍵” となる



増加する攻撃数への対処に AI が役立つと回答する割合



ますます巧妙化する攻撃への対処に AI が役立つと回答する割合

AI テクノロジーが攻撃の増加に対処するのに役立つと考える回答者、および AI テクノロジーが攻撃の巧妙化の増加に対処するのに役立つと考える回答者 [5,400人] いくつかの回答の選択肢を除く。

ほぼ例外なく、IT チームは、サイバー脅威の増加に対処するために AI テクノロジーを求めています。86% は、AI テクノロジーが攻撃の増加の対処に役立つと考えていると同時に AI テクノロジーが巧妙化する攻撃の増加に対処するのに役立つと期待しています。92% がこれらの選択肢の最低 1つを選択しています。

今すぐ未来の IT セキュリティチームを構築

未来の IT チームを構築するには、今すぐ始めてください。組織は、これらの洞察を直接最前線から活用して、2030年以降のサイバーセキュリティの成功に向けた準備を支援する必要があります。このレポートからの学習に基づき、ソフォスは次の 5つの推奨事項を提供しています。

1.IT セキュリティ管理者の作業負荷を軽減するツールとアプローチを実装

昨年のセキュリティ以外の仕事量とセキュリティ仕事量の両方の増加は非常に明白です。組織は、IT セキュリティの仕事量を削減し、他のアクティビティにチームを解放するためのツールとアプローチを実装する必要があります。

- **自動化。**自動化を活用することで、IT担当者の貴重な時間とエネルギーを奪い、戦略プロジェクトから逸脱させるような日々のタスクの負担を軽減することができます。機械は常に人間のオペレーターよりも迅速に反応できるため、対応時間が短縮され、脅威にさらされるリスクを減らします。
- **統合整理。**単一の統合コンソールを介してすべてのサイバーセキュリティのソリューションを管理することにより日常の管理を簡素化します。すべてを 1か所にまとめることで、コンソールからコンソールに移動してセキュリティを管理したり、異なるシステム間でデータを相互に関連付ける必要がなくなり、IT チームの貴重な時間や労力を節約できます。IT セキュリティを統合することで、ベンダー管理の負担も軽減されます。
- **統合連携。**統合され、連携するように設計されたソリューションを選択してください。これにより、タスクを自動化しながら、製品間の調査を容易に実行する機能と、セキュリティ体制に関するより深い洞察を提供する機能の両方が向上します。

2.IT チームが成長したスキルを活かせるようなツールやトレーニングに投資

過去 1年間で、IT チームのスキルと知識が大幅に向上しました。組織は、これらの新しいスキルを活用できるようにするツールとトレーニングに投資し、学習を継続できるようにすることをお勧めします。これらのリソースは、チームに新しい人材を採用するのにも役立ちます。

3.社内とアウトソースのITチームの専門性の融合

サイバー脅威は、IT 管理者の半数以上が単独で対処するにはすでに複雑になりすぎており、今後もさらに複雑になっていきます。セキュリティチームに社内の専門家と外部の専門家の両方を組み合わせることで、脅威や組織に関する深い知識を持った専門家を確保することができます。この組み合わせにより、変化への適応や対応が容易になり、それぞれの状況に最適な人材を活用できます。組織は、社内では利用できないスキルと能力を備えた IT チームを拡張すると同時に、希望する運用モデルに柔軟に適応できるセキュリティパートナーを探す必要があります。

4.グローバルな最高の人材を獲得するための準備

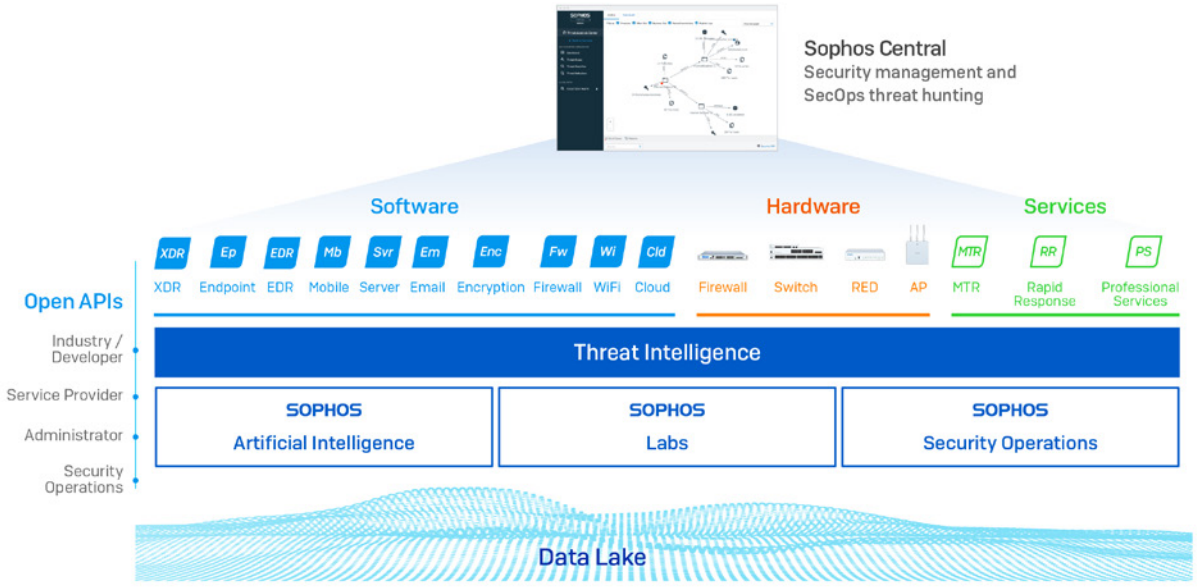
大多数の組織が IT チームの拡大を検討しているため、最高の人材を獲得するための競争は激化しています。どこからでも管理できる革新的なテクノロジーを採用することで、タレントプールを増やすことができます。パンデミックは、ほぼすべての IT の役割を必要に応じてリモートで実行できることを教えてくれました。さらに、質の高いツールを提供することで、最も有能な候補者へアピールすることができます。

5.社内 IT セキュリティチームのパイプラインを構築

IT セキュリティの人材はすでに不足しています。タレントプールを拡大するとともに、組織は、見習いトレーニングや職務中のトレーニングなど、IT チームパイプラインを育成および構築するための社内プログラムにも目を向ける必要があります。フード付きの服を着た若者が寝室でコンピュータに向かっているというイメージはステレオタイプですが、多くの人々が従来のキャリアパスの外で高度なサイバースキルを身につけていることも忘れてはなりません。

ソフォスが提供する支援

ソフォスは、50 万以上の組織と 150 か国の IT チームがサイバー脅威から自分達の組織を保護できるようサポートをしています。



Sophos Adaptive Cybersecurity Ecosystem (ACE)

- AI を活用した**次世代型テクノロジー**の完全なポートフォリオを提供しています。ソフォスの製品は、連携して動作するように設計されており、手動タスクを自動化し、脅威にさらされるリスクを減らします。これを Synchronized Security と呼びます。ソフォスのエンドポイントやファイアウォールの保護を利用しているお客様は、日常的な管理作業を 50% 以上削減し、セキュリティインシデントが減少したと一貫して報告しています。
- **Sophos Extended Detection and Response (XDR)** および **Sophos Endpoint Detection and Response (EDR)** を使用することで、IT チームに脅威および IT の予防策問題を迅速に特定して、修復するのに必要なツールを提供します。Sophos EDR は、セキュリティアナリストと IT 管理者の両方を対象に設計された初の EDR であり、IT チームは人員を追加することなく専門知識を開発できます。
- ソフォスのすべての次世代型テクノロジーは、**Sophos Central** セキュリティプラットフォームを通じて管理されています。これは、場所に関係なく最高のセキュリティ人材を採用できる Web ベースのツールです。
- **Sophos Managed Threat Response (MTR)** および **Sophos Rapid Response** チームは、高度な脅威ハンティングとインシデント対応の専門知識を提供して、フルマネージド型サービスとして社内チームをサポートします。潜在的なインシデントをエスカレートする方法とタイミング、そしてお客様に代わってどのような対応（ある場合）をソフォスに望むかを制御します。
- ソフォスのすべての保護は、**SophosLabs**、**Sophos Security Operations**、**Sophos AI** チーム、および **Sophos Data Lake**の総合的な脅威インテリジェンスによって支えられています。
- **オープン API** を使用すると、すべてのお客様は世界中のパートナーの知見やテレメトリからメリットを得ることができます。

ソフォスが提供している内容やお客様が直面している課題については、ソフォスの Web サイト にアクセスするか、ソフォスの営業担当者へお問い合わせください。

ソフォスが提供している内容やお客様が直面している課題については、当社のWebサイトにアクセスするか、ソフォスの営業担当者へお問い合わせください。

ソフォスは、業界をリードするサイバーセキュリティソリューションをあらゆる規模の企業に提供し、マルウェア、ランサムウェア、フィッシングなどの高度な脅威をリアルタイムで保護します。実績のある次世代機能により、AI と機械学習を駆使した製品でビジネスデータを効率的に保護できます。

2021-05-20 (WP-NP)

SOPHOS