SOPHOS

サイバーセキュリティの現状 2023 年版：サイバー攻撃者が防御側のビジネスに及ぼす影響

14 か国の IT/ サイバーセキュリティリーダー 3,000 人を対象として
2023 年 1 ～ 2 月に実施された独立調査から得られた知見。

調査の方法

ソフォスは、2023 年にサイバーセキュリティが実際のビジネスに及ぼす影響を探るため、14 か国の IT/ サイバーセキュリティを担うリーダー 3,000 人を対象とする調査を独立系調査会社に委託しました。すべての回答者は、従業員数が 100 ～ 5,000 名の組織に所属しています。調査は、Vanson Bourne 社が 2023 年 1 ～ 2 月に実施しました。

3000
回答者数

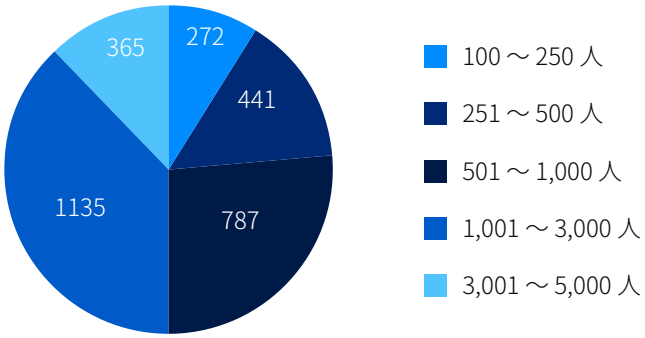
100 ～ 5,000 名
従業員

14
か国

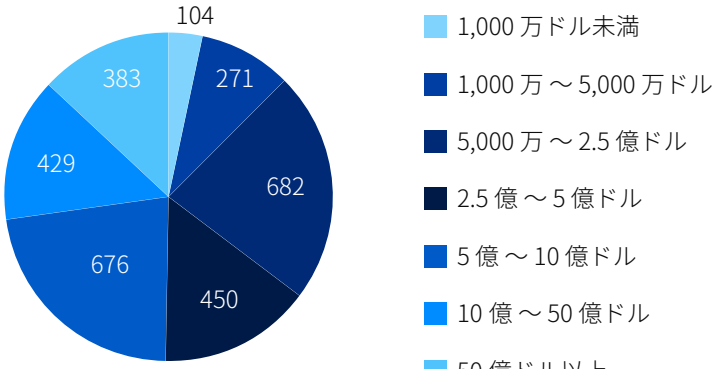
1,000 万ドル未満から 50 億ドル超まで
年間収益

23 年 1 ～ 2 月
調査の実施期間

組織規模 (従業員数) 別の回答者数



組織規模 (年間売上高) 別の回答者数



国別の回答者数

国名	回答者数	国名	回答者数
米国	500	英国	200
ドイツ	300	南アフリカ	200
インド	300	フランス	150
日本	300	スペイン	150
オーストラリア	200	オーストリア	100
ブラジル	200	シンガポール	100
イタリア	200	スイス	100

エグゼクティブサマリー

現状：攻撃の頻度やペースが増大する中で、防御側が守勢に回っている。

この調査では、サイバーセキュリティの戦いにおいて攻撃者と防御側のスピードが異なっていることが明らかになりました。攻攻撃者は、自動化、サイバー犯罪をサービスとして展開するモデル 、巧妙な「なりすまし」、標的の環境への適応によって活動を加速させており、高度な攻撃を幅広く大規模に実行できるようになっています。94% の組織は、過去 1 年間に何らかのサイバー攻撃を経験しています。したがって、2023 年には規模や売上高にかかわらず、すべての企業が標的になると想定すべきです。

専門知識の不足、膨大なアラート、長時間におよぶインシデント対応により、攻撃者の遅れをとっています。ほとんどの組織にとって、脅威の検出と対応の業務を運用することのハードルは高く、93% の回答者がセキュリティオペレーションに不可欠なタスクを実施することが困難だと感じています。

セキュリティアラートの調査は、多くの組織の懸案事項となっています。悪意のあるアクティビティの兆候を調査して判断する対象となっているアラートの割合は、平均して半数にも満たず (48%)、多くの組織が調査すべきアラート / イベントの特定 (71%) と優先順位付け (71%) に苦労しています。調査を必要とするアラートについて、検出から調査、対応までのプロセス全体に要する時間は、従業員数 100 ～ 3,000 名の組織では平均 9 時間、3,001 ～ 5,000 人の組織では 15 時間に達しています。

運用面では、防御側が自社のプロセスに自信を持てない状況にあり、2023 年にセキュリティリスクとして「セキュリティツールの設定ミス」が最も多く挙げられています。 IT プロフェショナルの半数以上 (52%) が、サイバー脅威が高度化し、自社で対処することが困難になっている回答しており、従業員数が 100 ～ 250 名の小規模な企業ではその回答率が 64% に上ります。

ビジネスへの影響：財務、オペレーション、リソースなど多方面で組織に悪影響を及ぼす

このような状況が、組織全体に大きな影響を与えています。サイバーセキュリティインシデントがもたらす直接的な金銭的影響は甚大であることは周知の事実であり、中小規模の組織がランサムウェア攻撃を修復するためにかかる平均コストは 140 万ドルに上ります。[1] しかし、インシデントを修復するための費用は、全体のほんの一部に過ぎません。

第一に、IT プロジェクトを実施・提供する能力が低下します。回答者の 55% が、サイバー脅威への対応が IT チームによる他のプロジェクトへの取り組みに悪影響を与えていることを報告しています。サイバーセキュリティへの対応は、緊急を要することが多く、予測が困難であることから、コアビジネスに特化したプロジェクトを推進する妨げにもなっています。回答者の 64% が IT チームがビジネス戦略に関する問題により多くの時間を費やし、セキュリティ問題の修正にかける時間を削減することを望んでいます。

セキュリティアラートの検出、調査、修正に費やす時間が長くなると、人員の確保について財務面にも大きな影響を与えます。

また、従業員の心身にも大きな負担を強いる状況となっています。IT プロフェッショナルの 57% がサイバー攻撃を受けることを心配し、不眠になる場合があると述べています。従業員数が 3,001 ～ 5,000 名の組織の回答者では、この割合は 65% に高まります。サイバーセキュリティのスタッフを採用し、訓練し、維持するコストが高いことを踏まえると、こうした影響は企業のコストを増大させ、さらに深刻な課題を生み出します。

1『ランサムウェアの状況 (2022 年版)』(ソフォス)

推奨される対策：防御側の変化を加速させ、攻撃者に先んじる

2023 年のサイバーセキュリティ競争において、防御側が攻撃者より先んじるためには、包括的でありながら、わかりやすいアプローチが必要となります。まず、攻撃対象領域や注意が必要なアラートの数を最小限に抑え、専門的なサービスを活用して対応にかかる時間を短縮できるような、インシデント対応のプロセスを構築する必要があります。

次に、状況に応じて自動的に調整される柔軟な防御の仕組みを導入する必要があります。これにより、攻撃者の動きを鈍らせて、防御側が対応する時間を稼ぐことが可能になります。

さらに、テクノロジーと人の専門知識を組み合わせて防御を強化し、スピード、効率性、そして成果を向上させる好循環を作り出す必要があります。これらの要素を包括的に取り入れて防御側の対策強化を加速させることで、攻撃者よりも優位な状況にすることができます。

このアプローチを成功させる上で要となるのは、サードパーティのスペシャリストの活用です。幸いなことに、このようなアプローチはすでに一般的になっており、サイバーセキュリティ対策において、94% の企業は何らかの形で外部の専門家と連携し、オペレーションを拡張させています。攻撃が活発化している中、セキュリティオペレーションに特化した専門家との連携は、ますます不可欠なものとなっています。

主な調査結果

94% の組織が、過去 1 年間に何らかのサイバー攻撃を経験した

2023 年のセキュリティの最大の懸念は**データの流出**である

93% が、セキュリティ対策に不可欠なタスクを実行することが困難だと感じている

調査対象となっておりセキュリティアラートの割合は **48%** にとどまる

アラートの検出、調査、対応にかかる平均時間は、従業員数 3,001 ～ 5,000 名の組織では **15** 時間に達する

2023 年に懸念されるセキュリティリスクとして **セキュリティツールの設定ミス**が最も多く挙げられている

52% は、現在、サイバー攻撃が高度になりすぎており、自社で対処することができないと回答している

55% は、サイバー脅威への対応が、IT チームの他のプロジェクトに悪影響を与えていると報告している

64% が IT チームがビジネス戦略に関する問題により多くの時間を費やし、セキュリティ問題の修正にかける時間を削減することを望んでいる

IT プロフェッショナルの **57%** は、サイバー攻撃を受けることを心配して不眠になることがあると報告している

2023 年のサイバー脅威：防衛の最前線の現実

2023 年に最も懸念されるサイバー攻撃の脅威

IT プロフェッショナルの 99% が、2023 年に自社がサイバーセキュリティの脅威を受けることを懸念しています。 IT プロフェッショナルが自社に対するサイバー脅威として最も多く挙げたのがデータの流出 (外部の攻撃者によるデータの窃取) であり、次いでフィッシング (スピアフィッシングを含む) となっています。また、ランサムウェアが第 3 位にランクインしています。

これら 3 つの脅威が連動していること多いことを把握しておくことが重要です。つまり、フィッシングメールがきっかけとなり、データの流出やランサムウェアにつながる攻撃が多く発生しています。

サイバー脅威	最も重要な懸念とした回答者の割合
データの流出 (外部の攻撃者による窃取)	41%
フィッシング (標的型攻撃を含む)	40%
ランサムウェア	35%
サイバー恐喝	33%
サービス拒否 (DDoS)	32%
ビジネスメール詐欺 (BEC)	31%
アクティブアドバーサリ (手動でキーボードを操作する攻撃者)	30%
モバイルマルウェア	30%
クリプトマイナー	22%
ワイパー型マルウェア	16%
その他	0%
2023 年にサイバー脅威が自社に影響を与えることを心配していない	1%
不明	0%

2023 年にどのようなサイバー脅威が自社に影響することを最も懸念していますか？ (回答者数 =3,000)

膨大な数の攻撃を大規模に実行している攻撃者

IT プロフェッショナルの懸念は、防衛の最前線で起こっている現実を反映しています。94% の組織は、過去 1 年間に少なくとも 1 回のサイバー攻撃を経験しています。ランサムウェアは最も多く報告された攻撃でしたが、攻撃者は多様な攻撃を大規模に実行しています。このように幅広く深い攻撃は、防御側にとって深刻な課題となっています。

こうした数字の背景には、サービスとしてのアクセス、サービスとしてのフィッシング、サービスとしての詐欺といった「XaaS」モデルの成長をはじめとして、サイバー犯罪の経済において専業化が進んでいる状況があります。このようにサイバー犯罪の運用形態が進化しているため、誰でも簡単にサイバー犯罪者に手を染めることが可能になっています。(詳細は、「ソフォス脅威レポート 2023 年版」をご覧ください。)

ランサムウェア以外のサイバー攻撃を経験し、報告した組織の割合

27%	27%	26%
悪意のあるメール	フィッシング (標的型攻撃を含む)	データの外部への流出 (攻撃者による)
24%	24%	21%
オンライン恐喝	ビジネスメール詐欺 (BEC)	モバイルマルウェア
18%	24%	14%
クリプトマイナー	サービス拒否 (DDoS)	ワイパー型マルウェア

アクティブアドバーサリによる攻撃が一般的に

23%
過去 1 年間にアクティブアドバーサリが関連する攻撃を経験した組織の割合

30%
2023 年のサイバー脅威の懸念として、アクティブアドバーサリを挙げた組織の割合

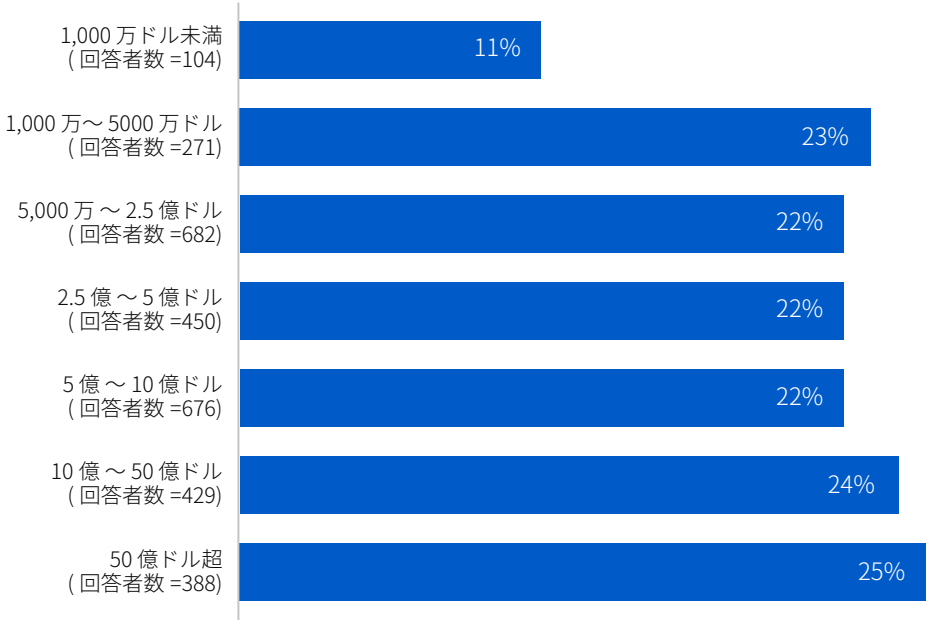
アクティブアドバーサリとは、、セキュリティテクノロジーや防御側の対策に応じて、リアルタイムにキーボードを操作して、攻撃対象の環境に合った戦術、手法、手順 (TTP) を適用して、検出を回避しながら攻撃を実行するサイバー攻撃者を意味します。アクティブアドバーサリによる攻撃により、壊滅的なランサムウェアやデータ侵害のインシデントにつながることも多く、防止することも最も困難な攻撃の 1 つです。

回答者の 23% が、昨年、自社がアクティブアドバーサリが関連する攻撃を経験したことを報告しています。攻撃を受ける確率は組織の規模に関係なく一定になっており、すべての組織規模をセグメントに分割しても 2 ポイントの差異しかありません。

興味深いのは、年間収益が 1,000 万ドル未満の組織では、アクティブアドバーサリによる攻撃の報告率が 11% にまで低下しています。これは攻撃者が意図的に収益の多い企業を標的にしていることを示唆しています。アクティブアドバーサリを検出するためには高度なスキルが必要であることから、検出されていないケースも多くあり、実際のインシデントの発生率はさらに高いと考えられます。

これらの攻撃による影響が破壊的であることから、回答者の 30% が、アクティブアドバーサリが 2023 年のサイバー脅威の最大の懸念事項の 1 つと回答しています。

アクティブアドバーサリによる攻撃を経験した割合 (年間収益別)

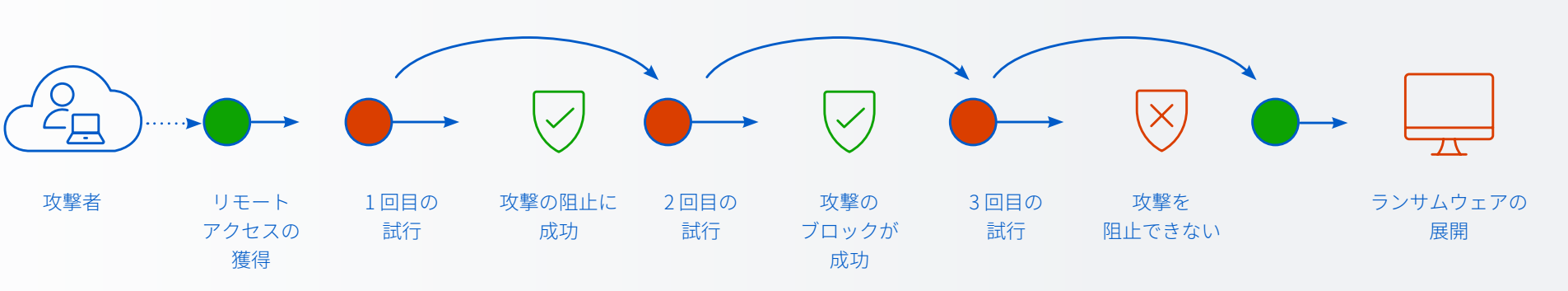


過去 1 年間にサイバー攻撃を受けたことがありますか？という質問に、「はい。アクティブアドバーサリ (手動でキーボードを操作する攻撃者) による攻撃を受けた」と回答した組織の割合

アクティブアドバーサリとは？

防御側が直面している課題を正しく認識するには、アクティブアドバーサリをブロックするだけでは攻撃全体を阻止するために不十分であることをまず理解する必要があります。アクティブアドバーサリは、持続的攻撃を実行する練度の高いサイバー犯罪者であり、目標を達成するために、以下のような複数の戦術、手法、手順 (TTP) を展開します。

- 認窃取した認証情報、パッチが適用されていない脆弱性、セキュリティツールの設定ミスなどを悪用し、セキュリティの弱点を突いて組織に侵入して、ネットワーク内を水平方向に移動する。
- 防御側が使用する正規の IT ツールを悪用し、検出を回避する。
- セキュリティ管理に応じてリアルタイムに攻撃を変化させ、目的を達成する方法を見つけるまで、何度も新たな手法で攻撃を継続する



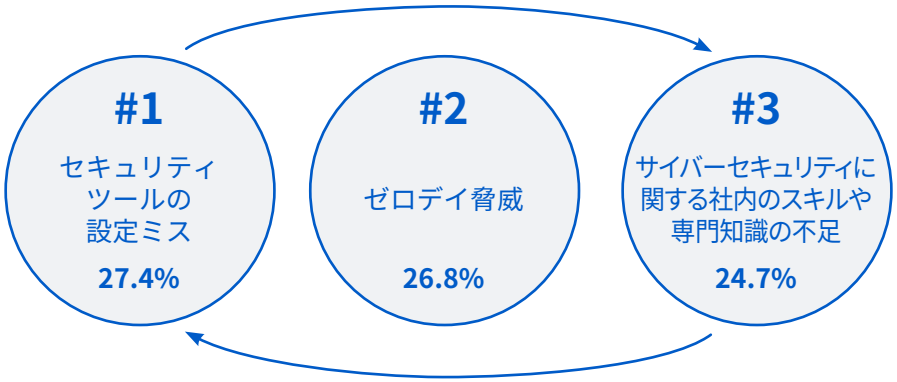
2023 年のサイバーセキュリティ：防御側の現状

サイバーリスクに関する懸念トップ 3

セキュリティ管理の設定ミス (エンドポイントやファイアウォールソリューションの設定ミスなど) は、最も懸念されているセキュリティリスクであり、回答者の 27.4% がサイバーリスクのトップ 3 に挙げています。このランキングから、セキュリティコントロールを正しく設定および展開し続けることが IT チームの課題となっている一方で、攻撃者が首尾良く防御の隙を突いて攻撃を仕掛けている状況が伺われます。

ゼロデイ攻撃 (未知のセキュリティ脆弱性やソフトウェアの欠陥を利用する攻撃) は 26.8% で、懸念されるセキュリティリスクの第 2 位になっています。サイバーセキュリティに関する社内のスキル / 専門知識の不足は第 3 位となり、回答者の 25% がセキュリティリスクのトップ 3 に挙げています。

スキル不足とセキュリティツールの設定ミスは、直接関係します。セキュリティコントロールを適切に設定するには時間、知識、経験が必要であり、これらが不足していると防御にギャップが生じます。



サイバーセキュリティのリスク	回答者がトップ 3 の懸念に挙げた割合
セキュリティコントロールの設定ミス (エンドポイントやファイアウォールソリューションなど)	27%
ゼロデイ脅威 (公開されていない手法を攻撃する脅威)	27%
サイバーセキュリティに関する社内のスキルや専門知識の不足	25%
アクセスデータや認証情報の窃取	24%
保護されていないデバイス (認識されていないデバイスを含む)	24%
サイバーセキュリティツールの不足	23%
未修正の脆弱性	22%
リモートユーザーへのアクセスの有効化	20%
安全でないワイヤレスネットワーク	20%
社内ユーザーの脅威 (偶発的に発生する問題)	18%
パートナー / サプライチェーン	18%
リモートアクセスツール	18%
内部ユーザー (意図的に行われる攻撃)	17%
IoT デバイス	17%
その他	0%
いずれも自社にとってリスクとなるサイバーセキュリティの問題ではない	0%
不明	0%

自社のサイバーセキュリティリスクのトップ 3 は何だと思いますか？ 1 位、2 位、3 位の回答の合計 (回答者数 =3,000)。

アラートの調査に対するさまざまなアプローチ

悪意ある活動の兆候かどうかを特定するための調査対象となる
セキュリティアラートは 48% にとどまる

防御側にとって課題の 1 つは、調査すべきアラートを見極め、限られたリソースを効果的に活用する方法を判断することです。

悪意ある活動の兆候かどうかを特定するための調査対象となるセキュリティアラートの割合は、平均して半分にも満たず (48%)、従業員数 3,001 ～ 5,000 名の組織でも 54% です。しかし、調査方法は大きく異なっています。16% の組織がアラートの 4 分の 3 以上を調査 (しかも、5% はすべてのアラートを調査) している一方で、4 分の 1 以下しか調査していない組織も 18% に上ります。

業界別に見ると、中央 / 連邦政府機関でアラート調査率が最も低く (39%、回答者数 =89)、エネルギー / 石油・ガス / 公共事業で最も高く (55%、回答者数 =69) なっています。

検出、調査、対応にかかる負荷

セキュリティアラートの検出、調査、対応に要する時間の中央値は、従業員数 100 ～ 3,000 名の組織で 9 時間、3,001 ～ 5,000 名の組織で 15 時間となっており、運用環境が複雑になるほど長くなっています。

この調査では、業種によって大きな差があることが明らかになりました。製造 / 生産 (15 時間) とエネルギー / 石油・ガス / 公共事業 (18 時間) は、IT/ 技術 / 通信 (6.75 時間) の 2 倍以上の時間をかけています。

注意すべきは、アラートの大半が対応の段階には至らないという点です。多くの攻撃はセキュリティテクノロジーによりプロアクティブしてブロックされ、アラートの一部はトリアージされて調査対象になります。また、対応アクションも、ユーザーの受信トレイからのフィッシングメール削除から、サーバーファーム全体の再構築まで、修復を必要とするイベントの特性に応じて大きく異なります。

アラートの検出、調査、対応に要する時間の中央値

活動	従業員数 100 ～ 3,000 名 (回答者数 =2,460)	従業員数 3,001 ～ 5,000 名 (回答者数 =350)	IT/ 技術 / 通信 (回答者数 =98)	製造 / 生産 (回答者数 =331)	エネルギー / 石油・ガス / 公共事業 (回答者数 =69)
検出	3 時間	3 時間	1.5 時間	3 時間	6 時間
調査	3 時間	6 時間	2.25 時間	6 時間	6 時間
対応	3 時間	6 時間	3 時間	6 時間	6 時間
合計	**9 時間**	**15 時間**	**6.75 時間**	**15 時間**	**18 時間**

あなたの組織は、潜在的なインシデントを検出および調査、必要に応じて修復するまでにどれくらいの時間を要しますか？
(回答者数 =2,812、社内でアラートを調査している回答者)

セキュリティ運用に必要なスキルが不足している組織

前述のとおり、IT プロフェッショナルは、サイバーセキュリティに関する社内のスキル / 専門知識の不足が 2023 年の主要なセキュリティリスクであると考えています。さらに詳しく見ていくと、大多数の組織がセキュリティオペレーションで不可欠なタスクを日常的に実行することに苦労していることがわかります。93% が、以下の活動のうち少なくとも 1 つを「困難」であると答えています。

- ノイズの中からシグナルを選り分ける (71% が困難と感じている)
- 調査すべきシグナル / アラートに優先順位を決定する (71% が困難と感じている)
- シグナルが悪意のあるものか、正規のものであるか識別するために十分なデータを収集する (71% が困難と感じている)
- アラートの脅威やインシデントをタイムリーに修復する (71% が困難と感じている)
- インシデントの根本原因を特定する (75% が困難と感じている)
- 正確な調査記録を維持する (68% が困難と感じている)

インシデントの根本原因を特定することは、最も多くの組織が課題と考えており、75% が困難であると回答しています。

セキュリティオペレーションのタスクを困難と感じる割合が最も高いのは、年間収益が最も小さい組織 (1,000 万ドル未満) であり、これに売上高が最も大きい組織 (50 億ドル以上) が続いています。組織が直面する障害は、売上高の規模によって異なります。特に、大規模組織では、組織やシステムが複雑であることが影響していると思われます。

こうしたスキル不足はドミノ効果を生み、アラートの調査に要する時間が長くなった結果、チームの能力が低下してリスクが増大するという状況が起こっています。

93%

セキュリティの運用が困難だと感じている組織の割合

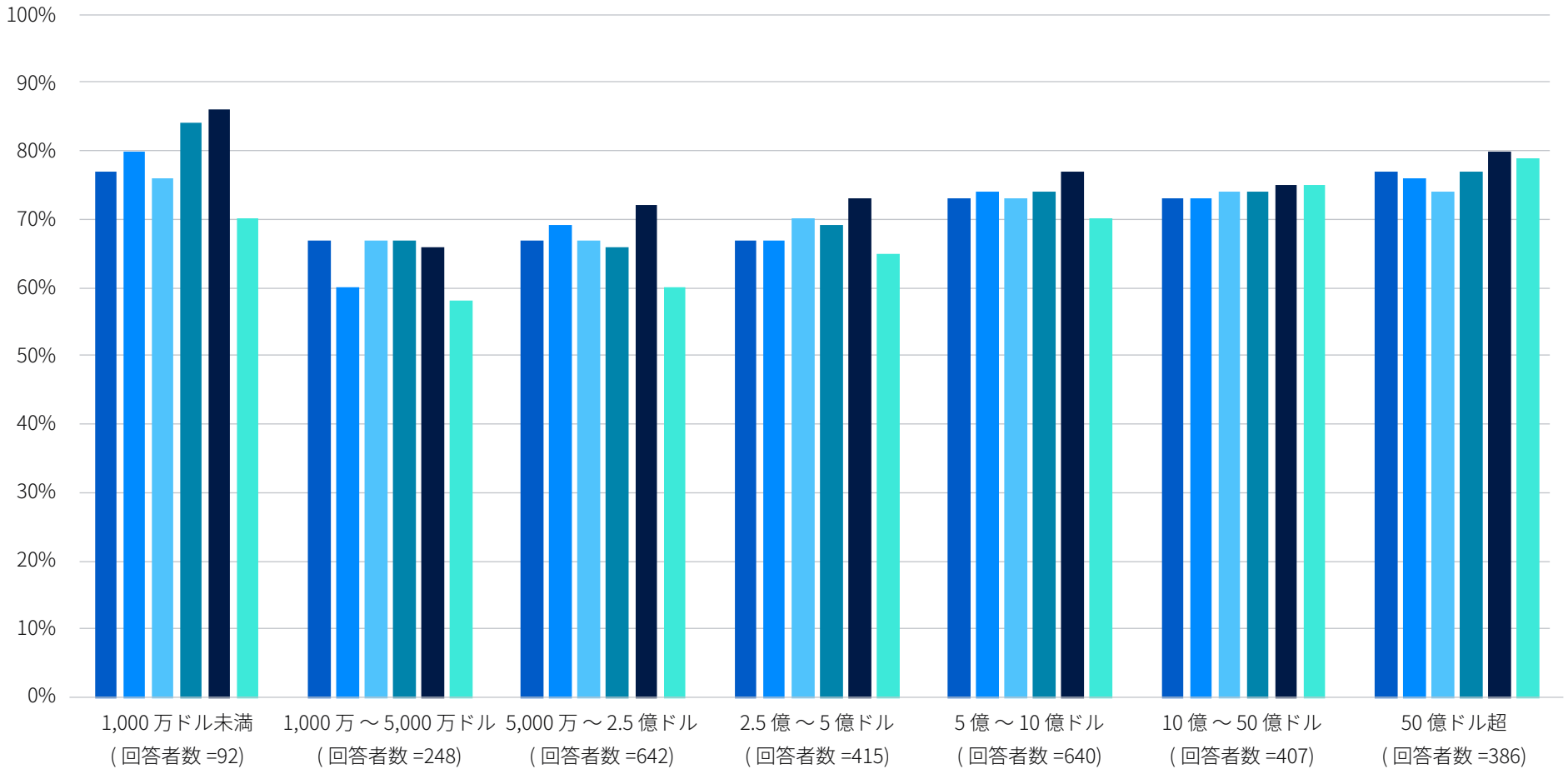
75%

インシデントの根本原因を特定することが難しいと感じている組織の割合

71%

調査対象のアラートの特定に苦労している組織の割合

セキュリティオペレーションのタスクが「困難」だと感じている組織 (収益別)



攻撃が疑われるアラートを調査するときに、組織のセキュリティオペレーションが「非常に困難」または「やや困難」と感じる回答者 (回答者数 =2,812、自社でセキュリティアラートを調査している回答者)

- ノイズの中から本当の脅威のシグナルを識別する (調査が必要なシグナル / アラートを特定すること)
- 調査すべきシグナル / アラートの優先順位を決定する
- シグナルが悪意のあるものか、正規のものであるか識別するために十分なデータを収集する
- インシデントの根本原因、つまりサイバー攻撃者が組織に侵入した方法を特定する
- アラートの脅威やインシデントをタイムリーに修復する
- 調査の正確な記録を保持する

攻撃者が防御側よりも優位な状態にある

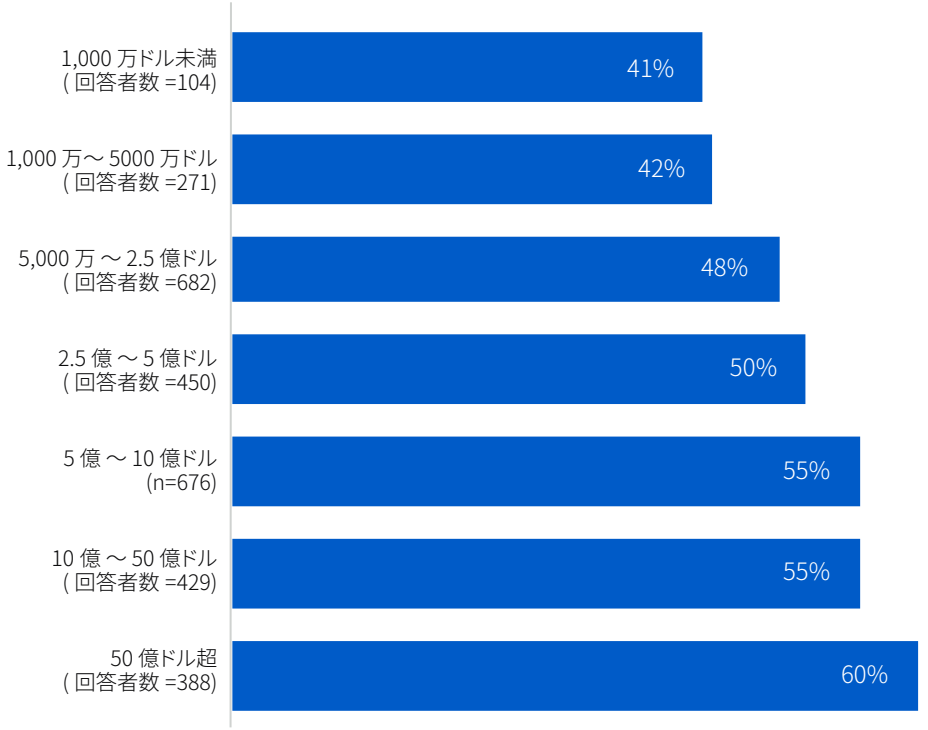
52%

現在、サイバー攻撃が高度になりすぎており、
自社で対処することができない回答した組織の割合

IT プロフェショナルの半数以上 (52%) が、サイバー脅威が高度化し、自社で対処することが困難になっている回答しており、従業員数が 100 ～ 250 名の小規模な企業ではその回答率が 64% に上ります。

組織の収益が増加すると、社内チームが追いつかなくなる可能性が高くなります。これは、収益規模が大きい組織では、社内のサイバーセキュリティ環境が複雑化しており、専門のセキュリティサービスを利用する傾向が強いことを反映している可能性があります。また、脅威環境や高度な脅威に対する防御の課題に対して、理解が深まっていることを反映している可能性もあります。

現在、サイバー攻撃が高度になりすぎており、自社で対処することができない



「現在、サイバー攻撃が高度になりすぎており、自社で対処することができないという意見に、どの程度賛成または反対しますか？」という質問に、「強くそう思う」「ややそう思う」を選択した回答者 (表中に回答数を表示)

ビジネスへの影響

プロジェクトの実行への影響

64%
IT チームがビジネス戦略に関する問題により多くの時間を費やし、セキュリティ問題の修正にかける時間を削減することを望んでいる組織の割合

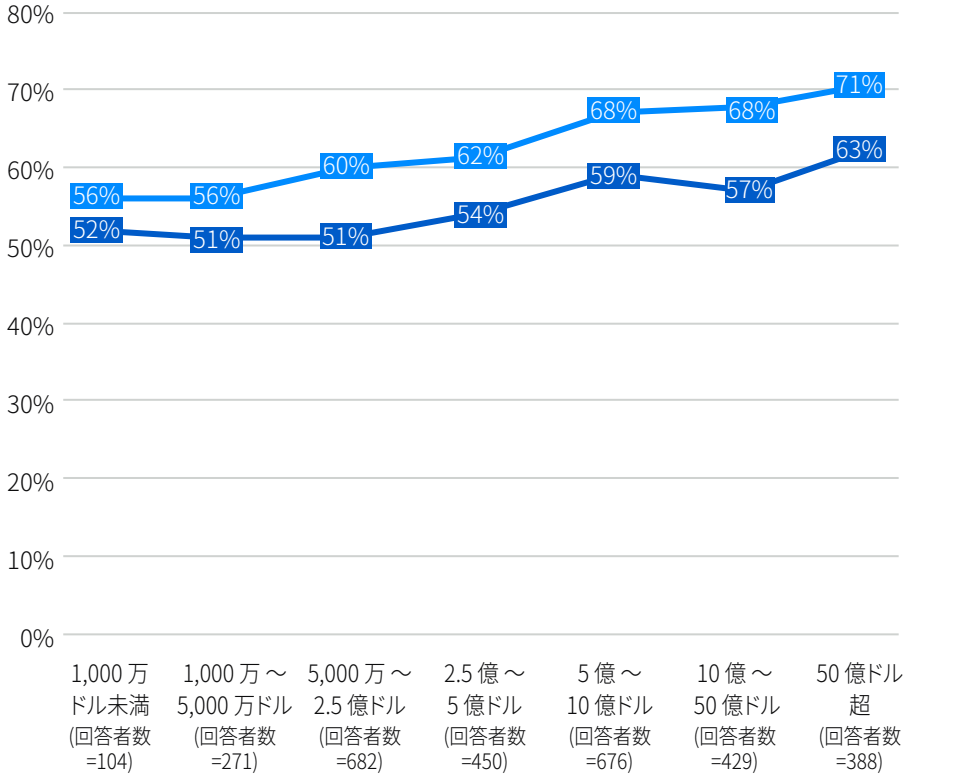
55%
サイバー脅威への対応が、IT チームの他のプロジェクトに悪影響を与えていると回答した組織の割合

60% の組織は、サイバーセキュリティとさまざまな IT 機能が非常に緊密に連携していると考えています。52% は IT チーム内にサイバーセキュリティチームがあり、8% は IT チームがサイバーセキュリティを兼任しています。残りの 40% の組織では、サイバーセキュリティチームと IT チームが別々にあります。サイバーセキュリティに必要な時間と労力は、IT 組織に多大な影響を与えています。

過半数 (55%) の組織は、サイバー脅威への対処のために、IT チームの他のプロジェクトに支障が生じたと報告しています。中でも、収益が最も大きな組織が最も大きな影響を受けています。

また、サイバーセキュリティは緊急性が高く予測不可能であることから、ビジネスに集中した取り組みに支障を与えます。平均して 64% の組織が、IT チームがビジネス戦略に関する問題により多くの時間を費やし、セキュリティ問題の修正にかける時間を削減することを望んでいます。ここでも、収益が大きい組織ほど、広範なプロジェクトの実行に影響が及んでいます。

サイバーセキュリティへの対応が IT チームの他のプロジェクトに悪影響を及ぼしている



「サイバーセキュリティインシデントへの対応が、IT チームの他のプロジェクトに悪影響を与えている。IT チームがビジネス戦略に関する問題により多くの時間を費やし、セキュリティ問題の修正にかける時間を削減してほしいと思うか」という質問に、「強くそう思う」「ややそう思う」を選択した回答者 (回答者数はグラフ内の数値を参照)

財務への影響

サイバーセキュリティ環境が厳しいため、組織は財務面でもいくつかの点で影響を受けています。単独で最も大きなコストが発生するのは、大規模なサイバーインシデントが発生したときです。ソフォスのレポート「ランサムウェアの現状 2022 年版」で報告しているとおり、ランサムウェアの修復にかかるコストは平均で 140 万ドルに上ります。

しかし、サイバー攻撃への対応による財務的影響は、インシデントを修正するためにかかるコストだけではありません。米国における IT セキュリティスペシャリストの平均給与は現在、年間 10 万ドル弱であり [2]、各セキュリティアラートの調査にかかるリソースの時間あたりのコストも増大しています。給与は地域ごとの状況によって異なりますが、インシデント調査プロセスは長期にわたり、その財務的影響は著しく大きくなります。

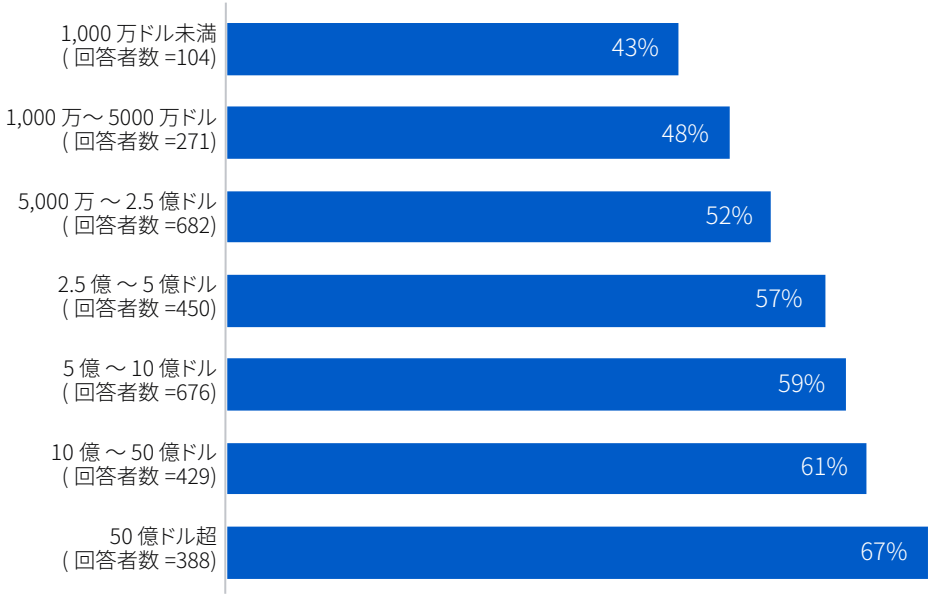
チームへの影響

回答者の 57% は、がサイバー攻撃を受けることを心配し、不眠になる場合があると述べています。サイバーセキュリティを担うスタッフを採用し、維持するコストが高い点を踏まえると、これは福利厚生とコストの両面で懸念をもたらします。さらに、防御側がセキュリティツールに全幅の信頼を寄せていないことも示唆されます。

サイバーセキュリティの分野では、燃え尽き症候群が大きな問題になっています。アラートの数や、やるべき作業が多すぎて、従業員にかなりのストレスがかかっています。過度な緊張を強いられると、チームは重要なシグナルを見逃す可能性が高くなり、悪循環に陥るケースもあります。最終的に、体調不良など心身に支障をきたす場合もあります。

サイバーセキュリティを心配する余り、不眠に陥る傾向は、組織の収益が大きくなるにつれて増加する傾向にあり、年間収益が 1000 万ドル未満の組織では 43% ですが、50 億ドル以上の組織では 67% に上ります。

サイバー攻撃を受けることを心配し、不眠になる場合があると答えた回答者の割合



「組織がサイバー攻撃を受けることが心配になり、不眠になる場合があるか」という質問について、「強くそう思う」「ややそう思う」を選択した回答者 (表中に回答数を表示)

2 2023 年 3 月時点における IT セキュリティスペシャリストの平均給与に基づく
https://www.indeed.com/career/it-security-specialist/salaries

ソフォスの提言

このような状況に対処するためには、3 つのステップを確実に取り入れる必要があります。まず、拡張性の高いインシデント対応プロセスを導入し、対応にかかる時間を短縮します。次に、適応型の防御を活用して攻撃者の動きを止めます。最後に、セキュリティ保護の強化とコストの低減という好循環を生み出します。

いわゆる「盾」を強化することが重要です。高度で持続的な攻撃者を阻止するには、防御 (つまり、盾) の有効性を最適化する必要があります。コンテキストに合わせてテクノロジーを使用することも重要であり、状況に応じて保護レベルを高めることができます。また、防御により時間を稼ぎ、人間の専門知識を駆使して根本原因を解決することも重要です。

強力な防御策が不可欠

サイバーセキュリティテクノロジーの品質は極めて重要となり、以下のようなセキュリティコントロールが必要になります。

- **予防を最適化し、**攻撃チェーンの早期の段階で可能な限り多くの脅威を自動的に検出および防止します。これにより、組織のリスクを軽減し、防御の担当者が取り組むべきインシデント数を減らすことができます。
- 投資したセキュリティテクノロジーが正しく展開されていることを簡単に確認できるようにし、設定ミスの問題を避けることで、**リスクを軽減できます。**
- **攻撃を妨害します。**攻撃を自動的に検出して妨害するテクノロジーは、攻撃を失敗させて、インシデントを無力化するための時間を稼ぐことができます。

予防の最適化

可能な限り早期に攻撃を止め、影響を最小限に抑える

リスクの低減

攻撃者がセキュリティのギャップや弱点を突く機会を最小化する

攻撃の妨害

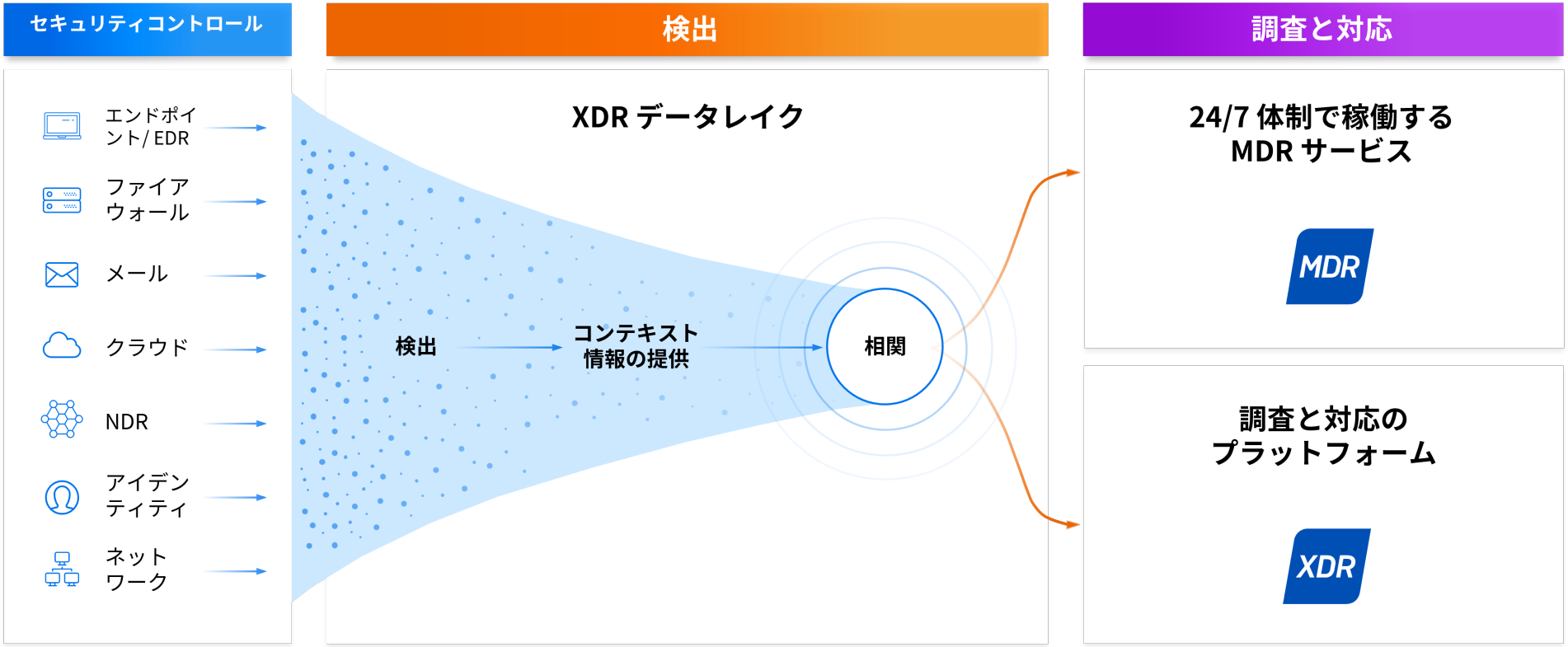
人間が主導する高度な攻撃を受けた場合に、防御側が対応するための時間を確保する

人とテクノロジーによって根本原因を解決する

盾を強化することで、防御側は攻撃を調査して対応するための貴重な時間を稼ぐことができます。しかし、完璧な予防を保証するものではありません。だからこそ、根本原因の修復を迅速に、十分な情報に基づき、適切に実施することが不可欠です。

攻撃手法は常に変化することが調査から明らかになっています。セキュリティ環境全体から収集したテレメトリを活用し、すでに導入しているセキュリティコントロールを利用することで、組織は脅威を迅速に特定して対応し、既存の投資を効果的に活用できます。

膨大なアラートの中から悪意のある活動を見つけることは、干し草の中から針を探すようなものです。コンテキストを踏まえた知見を追加し、関連するアラートを相関する XDR プラットフォームで、このシグナルを処理すれば、防御を担当している社内の担当者は本当に重要な脅威に迅速に対応できます。社内チームが XDR プラットフォームを使用して調査や対応することができます。また、検出、調査、対応の業務を MDR サービスのスペシャリストにアウトソーシングすることもできます。



防御側の対策を加速させる

防御策を迅速化することができれば、その流れを継続することは決して困難ではありません。効率化した防御策を、さらに強化していくことも可能です。組織は、セキュリティテクノロジーと人間の専門知識を組み合わせることで、サイバーセキュリティの強化を加速させることができます。セキュリティ管理を強化することができれば、対処しなければならないアラート数を軽減し、攻撃を無効化しながら、セキュリティ態勢の強化に集中できます。その結果、自社のセキュリティ管理の効果が高まり、好循環を生み出すことができます。

必要なセキュリティコントロールとサービスの導入を多くの組織が計画している

今回の調査から、多くの組織が、今後 1 年以内に脅威を検出して対応するためのソリューションを自社のセキュリティスタックに追加することを計画していることがわかりました。4 分の 3 以上 (78%) は、今後 1 年間で EDR (Endpoint Detection and Response) や XDR (Extended Detection and Response) ツールを導入する予定です。

高度なサイバー脅威の調査と対応には専門的なスキルが必要であり、24 時間 365 日体制で対応するには、最低でも 5 ～ 6 人の人材を配置しなければなりません。2023 年に懸念されるサイバーリスクのトップ 3 の 1 つに、社内のサイバーセキュリティスキル / 専門知識の不足が挙げられており、多くの組織が外部の専門家にサポートを求めることを検討しています。今後 12 か月以内に MDR (Managed Detection and Response) プロバイダーとの連携を開始することを予定している組織は、44% に上ります。

今後 12 か月以内に検出 / 対応ソリューションの導入を予定している組織の割合

78%	44%
EDR/XDR	MDR

ソフォスのソリューション

ソフォスは、防御側の組織がセキュリティの強化を加速させ、攻撃者よりも先んじることを可能にするサービスとテクノロジーを提供します。ソフォスは、最先端の脅威から 55 万以上の組織を保護しており、Sophos MDR は世界で最も信頼されている MDR サービスです。

最強の保護対策を基盤とする

ソフォスのエンドポイント /EDR、ファイアウォール、メール、ネットワーク、クラウドの各ソリューションは、攻撃者の動きを鈍らせ、防御側が対応するために必要な時間と知見を与える、最強の盾となります。

- **予防を最適化する：**ソフォスは、脅威の 99.98% を自動的にブロックして、リスクを最小限に抑え、防衛側の担当者は人が介入しなければならないインシデントに集中できます。
- **リスクを軽減する：**導入した当日から最適な保護設定が自動的に展開され、セキュリティギャップを解消できます。セキュリティ状態のチェック機能が組み込まれており、回避できるはずの感染を招いてしまうソフトウェアの欠落や構成ミスを特定します。
- **攻撃を妨害する：**手動の操作によるエンドポイントへの侵入を検知すると、アクティブアドバーサリの攻撃を保護する機能によって、直ちに防御が強化され、攻撃者を防止し、防御側が対応できる時間を確保します。

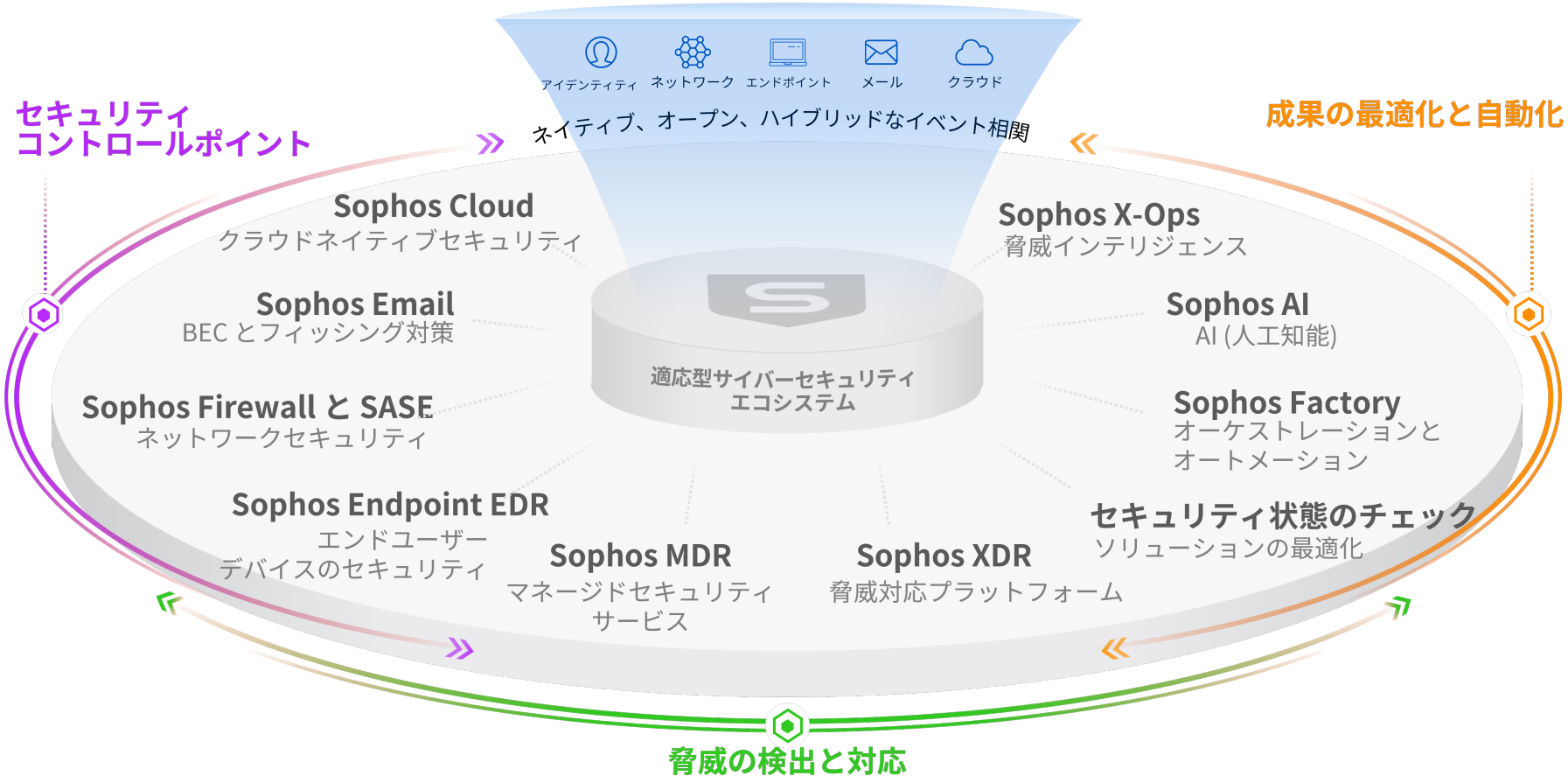
検出、調査、対応を最適化する

防御側が確認できる情報が多いほど、迅速な行動が可能になります。ソフォスとサードパーティーのセキュリティ製品の両方のテレメトリを統合し、セキュリティ環境全体で特定された情報を活用し、検出と対応を加速させ、既存のセキュリティ製品への投資をさらに活用できるようにします。

Sophos MDR サービスは、500 人以上の専門家から構成されており、24 時間 365 日、お客様に代わってアクティブアドバーサリによる攻撃などをハンティング、調査、対応するサービスです。Sophos MDR が脅威を解決するまでの平均時間は 38 分であり、社内チームの平均時間を大幅に上回るスピードで対応できます。また、EDR のすべての機能を搭載する Sophos XDR プラットフォームを使用して、攻撃を自社で調査して対応することも、Sophos MDR チームと連携して対応することもできます。

現在のセキュリティ環境や、将来どのようなレベルの対策を目標とするのかは、組織ごとに異なります。しかし、ソフォスの支援を活用することで、どのような組織も防御対策を加速させ、今日の高度な攻撃者に先んじることができるようになります。詳しくは、www.sophos.com にアクセスするか、セキュリティアドバイザーにご相談ください。

ソフォスでサイバーセキュリティの最適な成果を実現する



2023-03-29 (WP-NP)

SOPHOS