SOPHOS

中小企業におけるサイバーセキュリティスキル不足の解消

本書では、サイバーセキュリティのスキル不足が中小企業に現在与えている影響と、リソースと予算の制約がある中でこれらの課題に対処する方法を解説します。

ソフォス ホワイトペーパー 2024 年 10 月

はじめに

サイバーセキュリティに関連するスキルを有する人材が世界的に不足していることは周知の事実であり、多くのメディアでも取り上げられています。この人材不足はすぐに解消されることはないため、中堅・中小企業はこの問題への対策を講じなければなりません。

この課題を理解することが、解決のための第一歩となります。本レポートでは、世界各国の第一線で活躍しているセキュリティの担当者を対象とした独自の調査結果についてお伝えし、サイバーセキュリティのスキル不足が中小企業の日常業務にどのような影響を及ぼしているかを明らかにします。また、調査から得られた知見に基づいて、企業が現在抱えているリソースと予算の制約の中で、これらの課題に取り組むための実践的な指針を示します。また、小規模な企業であっても優れたサイバーセキュリティ対策を実現できるソフォスのソリューションについても紹介します。

調査について

ソフォスは 14 か国 5,000 名の最前線で働く IT / サイバーセキュリティプロフェッショナルを対象とした、調査を独立した第三者機関に委託しました。1,402 人の回答者は、従業員数 100 ～ 500 人の組織に属しています。この報告書では、この規模の組織を中堅・中小企業 (SMB) として定義しています。本調査は 2024 年第 1 四半期に実施されました。

小規模な組織ほどスキル不足の影響を大きく受けている

中堅・中小企業は、スキル不足の問題の影響を特に大きく受けています。この調査で、**従業員数が 500 人未満の組織では、社内のサイバーセキュリティのスキルや専門知識の不足が、ゼロデイ脅威を上回る 2 番目に大きなサイバーセキュリティのリスク**であると認識されていることが明らかになりました。対照的に、従業員 500 人以上の企業ではスキル不足の課題は 7 位となっています。

企業のサイバーセキュリティリスクにおける「社内のサイバーセキュリティスキル / 専門知識の不足」の相対的なランク

SMB (回答数 =1,402)	大規模な組織 (回答数 =3,598)	
従業員数 100 ～ 500 人	従業員数 501 ～ 1000 人	従業員数 1001 ～ 5000 人
2 位	7 位	7 位

自社のサイバーセキュリティリスクのトップ 3 は何ですか？回答の中で第 1 位となった「社内のサイバーセキュリティスキル / 専門知識の不足」の相対的な位置付け (回答数は図内に記載)

あらゆる規模の組織がスキル不足の影響を受けていますが、中でも中小企業がその影響を最も強く感じていることが明らかになりました。サイバーセキュリティツールの不足 (従業員数 501 ～ 1,000 人の企業が回答したリスクの第 2 位) や、アクセスデータや認証情報の窃取 (従業員数 1,001 ～ 5,000 人の企業が回答したリスクの第 2 位) などのリスクは大企業で上位にランクされていますが、中小企業では優先順位が低い懸念事項となっています。これは、中小企業がこれまで投資してきたセキュリティソリューションを運用するための人材を確保するという基本的な課題に悩まされているためです。

スキル不足が引き起こす 2 つの課題

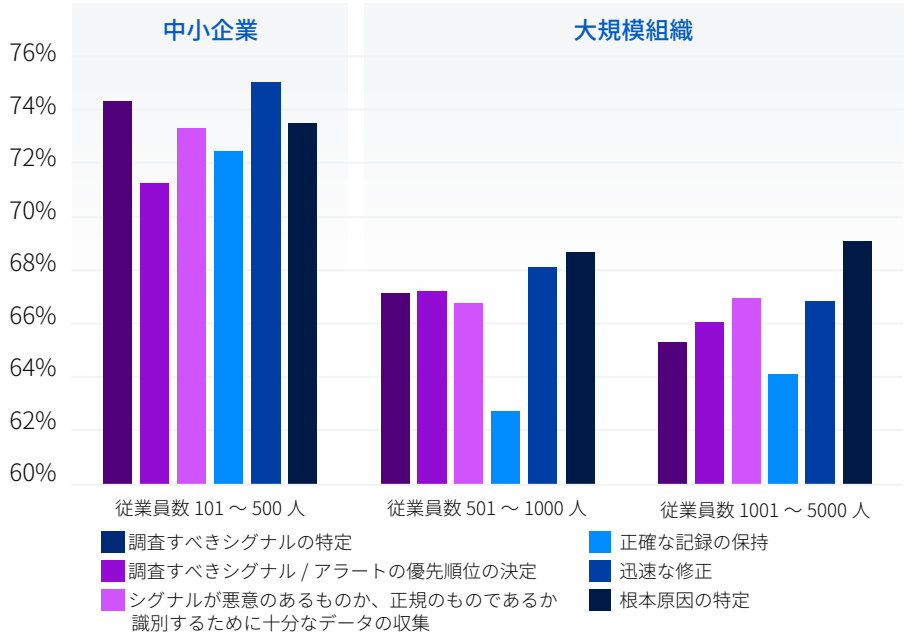
サイバーセキュリティのスキル不足が挙げられているのは、経験豊富なサイバーセキュリティプロフェッショナルが不足していることが原因です。この問題は、中小企業に 2 つの影響を与えています。

専門知識の欠如

サイバー脅威とセキュリティテクノロジーは複雑になっています。自社のサイバーセキュリティの能力を高めるためには、高度な専門知識とスキルが求められ、これらの要件を満たす人材を確保するハードルはますます高くなっています。サイバー攻撃が複雑になるにつれ、攻撃を阻止するために、より高度な専門知識も必要となっています。

今回の調査では、**中小企業の 96% が、セキュリティアラートの調査における少なくとも 1 つの領域について困難と感じている**ことが明らかになりました。大企業もセキュリティの運用について困難と感じることが多くありますが、中小企業ではこの課題が最も深刻になっています。

セキュリティ運用のタスクが困難だと感じている組織の割合



セキュリティアラートを社内で調査している場合、攻撃を示している可能性があるアラートの調査における以下の領域は、あなたの組織にとってどの程度困難なものですか？「非常に困難」および「ある程度困難」（回答数は図内に記載）

サイバーセキュリティの専門知識を習得することは、中小企業で働いている従業員にとって現実的には困難です。IT やセキュリティチームの人員が数名の場合、定期的に時間を確保して、継続的に教育することは容易ではありません。さらに、同僚が少なければ、各人がピアツーピア学習の恩恵を受ける機会も少なくなります。

能力の不足

サイバー攻撃者は午前 9 時から午後 5 時まで決まった時間に働いているわけではないため、24 時間体制でサイバーセキュリティを運用しなければなりません。攻撃者は検出されずに組織に侵入するため、実際、ランサムウェア攻撃の 91% が通常の営業時間外に開始されています[1]。

最前線で働くセキュリティオペレーターは、24 時間 365 日体制でサイバーセキュリティを運用するには、スタッフの休日や病気、週末対応を考慮して、最低でも 4、5 人の常勤スタッフが必要となると述べています。多くの中小企業は、社内のリソースだけでこのような体制を構築することはできません。

これを裏付けるように、今回の調査では、**3 分の 1 (33%) の中小企業は、アラートを積極的に監視および調査し、特定された脅威に対応しているスタッフを置いていないことが明らかになりました**。積極的に対応するスタッフがいなければ、中小企業は攻撃に広くさらされることになります。

33%
セキュリティアラートを監視・調査する担当者がいない中小企業の割合

直近 1 年間で (夜間、週末、休日を含む) に、組織でセキュリティアラートを監視・調査を担当する人が勤務中となっていた時間は全体 (1 年間) の何 % ぐらいでしたか？回答者 = 1,402 社 (従業員数 100 ～ 500 人)

1 アクティブアドバーサリーの阻止：最前線のサイバー防御からの教訓 – ソフォス

サイバーセキュリティのスキルギャップが中小企業に与える影響

スキル不足は中小企業にさまざまな形で影響を与えています。中小企業は、ランサムウェア攻撃でデータが暗号化される可能性が最も高いセグメントであり、インシデントの 74% でデータが暗号化されています。これは、ランサムウェアが最終的に実行される前に攻撃を検出して、阻止する能力が低いことを反映していると考えられます。

ランサムウェア攻撃によってデータが暗号化された割合

SMB (回答数 =1,402)	大規模な組織 (回答数 =3,598)	
従業員数 100 ～ 500 人	従業員数 501 ～ 1000 人	従業員数 1001 ～ 5000 人
74%	72%	66%

出典 : ランサムウェアの現状 2024, 年版、ソフォスランサムウェア攻撃でデータは暗号化されましたか？はい。回答数を図内に記載。

さらに、サイバーセキュリティ業務の負荷を分担できるスタッフが少ないため、燃え尽き症候群に陥る可能性も高くなっています。ソフォスが委託しアジア太平洋地域と日本で実施した別の調査では、**85% の組織がサイバーセキュリティと IT の専門家で「セキュリティ疲れ」と「燃え尽き症候群」を経験していると回答しており**、約 4 人に 1 人 (23%) が「頻繁に経験」し、62% が「時々経験」していると述べています。厄介なことに、90% の企業が過去 1 年間に燃え尽き症候群やセキュリティ疲れが増加したと回答しており、そのうち 30% は「大幅に増加した」と回答しています。

85%

サイバーセキュリティや IT プロフェッショナルの
セキュリティ疲れや燃え尽き症候群を報告した組織の割合

中小企業のスキルギャップを解決する方法

多くの中小企業にとって、雇用を増やすことは現実的な選択肢ではありません。サイバーセキュリティのスタッフを増員するためには、多くの予算が必要となります。大規模な組織と比較すると、小規模な組織では増員の予算によって受ける影響が大きくなります。同時に、企業は少ない人材を奪い合う競争にさらされています。引く手あまたのスキルを有する人材は働く企業を自由に選ぶことができ、多くの場合、ピアツーピア学習によって能力や技能を高めることができる機会が多い、大規模な組織を選ぶ傾向があります。セキュリティの専門知識とスキル不足の問題への解決策は、サードパーティのセキュリティ専門家と連携し、中小企業のために設計されたサイバーセキュリティソリューションを活用することです。

サードパーティのセキュリティの専門家との連携

サードパーティのサイバーセキュリティの専門家を外部リソースとして活用することは、専門知識と能力を強化する最も簡単で費用対効果の高い方法となることが多くあります。最も一般的な 2 つのアプローチには、MDR (Managed Detection and Response) サービスと MSP (マネージドサービスプロバイダ) の利用があります。

MDR サービスは通常、お客様の環境全体にわたって、専門家主導による脅威の調査、検出、および対応を 24 時間 365 日提供します。アナリストがお客様の組織を監視し、攻撃が疑われる活動を特定して対応し、ビジネスに影響が及ぶ前に攻撃を無効化します。

脅威の検出と対応を完全にアウトソーシングするのか、プロバイダーのアナリストと分業・連携するのかなど、自社のニーズや自社に最適な連携方法を提供しているプロバイダーを見つけてください。また、常に予算に制限があるため、既に導入しているセキュリティテクノロジーを活用できるサービスを利用し、不要なコストやテクノロジーの総入れ替えによる混乱を避けることが重要です。

MDR サービスを利用することで、サイバー保険会社に支払う保険金を削減することができ、その費用を MDR サービスの資金に充てることができます。MDR サービスを利用している企業は、保険金を請求するリスクが低いため、多くの保険会社はこれらの顧客に有利な等級を設定しています。保険会社は通常、MDR サービスを利用する企業に大幅な割引を提供しており、削減できる保険料を MDR サービスの資金に割り当てることが可能になります。

ソフォスの顧客事例 : 従業員 350 人の非営利団体

米国ノースカロライナ州にある従業員 350 名の非営利団体は、Sophos MDR サービスを利用していたため、サイバー保険料を 8,000 ドル削減できました。Sophos MDR の年間サブスクリプションは 8,467 ドルでしたが、保険料が削減されたことにより、わずか 467 ドルの追加費用で、セキュリティの専門家による脅威の検出と対応を 24 時間 365 日利用できるようになりました。

MSP は、長年にわたって IT とサイバーセキュリティのサポートを社内チームのように中小企業に提供してきました。サイバー脅威が複雑になる中で、社内リソースを補完するために MSP との協業を選択する中堅企業が増えています。

MDR と MSP は、両方同時に利用することもできます。Sophos の別の調査 によると、多くの MSP (81%) が MDR サービスを提供しており [2]、単一のプロバイダーから両方のサービスの利点を受けることができます。自社の MDR サービスのみを提供している MSP もありますが、MDR 専門のサードパーティプロバイダーを活用する MSP もあります。

中堅・中小企業のために設計されたソリューションの選択

多くのサイバーセキュリティソリューションは、大規模な組織向けに設計・構築されており、これらのソリューションを展開および管理するためには相応のチームが必要となります。大規模企業向けのソリューションを利用することに魅力を感じるかもしれませんが、小規模な組織では、これらのソリューションを効果的に利用することが難しく、セキュリティを向上する効果や投資収益率 (ROI) に関する利点を得るのに苦労することが多くあります。

2 MSP のビジネス展望 2024 年版 - ソフォス

大規模企業向けのソリューションではなく、高度なテクノロジーを組み込みながら、多忙な IT チームが実際に使いやすいように設計されているセキュリティツールを見つけることが重要です。これらの利点に焦点を当てて、ソリューションを選ぶ場合でもコストは増加することはないはずです。さらに、テクノロジーと管理にかかる費用の両方を削減できる可能性もあります。セキュリティソリューションを評価するときには、プラットフォームと製品機能の両方を考慮してください。

プラットフォーム

- サイバーセキュリティプラットフォームとは、エンドポイント保護 / アンチウイルス、メールセキュリティ、ファイアウォールなどの複数のサイバーセキュリティソリューショを一元的に導入、監視、管理するためのツールです。
- これらのサイバーセキュリティソリューションを共通のプラットフォームに統合すれば、発生している脅威を確認して対応するためにコンソールを切り替える必要がなくなり、日々の運用管理の負担を大幅に削減できます。利用するプロバイダー数を減らすことで、ベンダーを管理する負担も軽減できます。
- また、効果的なプラットフォームであれば、セキュリティソリューションを連携させ、テレメトリ、知見、ユーザーベースのポリシーなどを共有し、自社のサイバー攻撃への防御を強化できます。

製品機能

- ベンダーの Web サイトには、自社製品の機能や能力が長々と掲載されています。導入するソリューションを評価するときには、自社で必要な機能と不要な機能を明確に理解し、自社にメリットのないテクノロジーに支出することは避けてください。
- サイバーセキュリティへの投資から最大限の効果を得るためには、セキュリティソリューションを効果的に展開して使用できなければなりません。展開したその日から推奨される設定を自動的に利用できるソリューションを選択すれば、時間がかかり、誤設定のリスクのある手動設定が不要になります。また、実際の使用環境に合っており、直感的な操作が可能で、使いやすいソリューションを探してください。
- セキュリティツールの設定ミスは、SMB にとって最大のリスクになっています。セキュリティツールを運用するときには、適切な設定を維持することが重要であり、ツールの運用が最適化されていない場合、迅速に修正するサポート機能を提供しているなど、運用環境を明確に可視化できるソリューションを選択することが重要です。
- 中小企業の場合、社内のチームがサイバーセキュリティの問題だけに集中できるわけではありません。このため、自社のチームが介入できるようになるまで必要なアクションを実行でき、攻撃に自動的に対応できるソリューションを選ぶことが特に重要となります。

ソフォスが提供する支援

ソフォスには、高度なサイバー脅威から中堅中小企業を保護してきた豊富な経験があり、中堅中小企業のニーズに特化した多くの製品やサービスを提供しています。

サードパーティのセキュリティの専門家

MDR

ソフォスは、世界で最も信頼されている MDR サービスを提供しており、他のどのプロバイダーよりも多くの中小企業を保護しています。ソフォスは、中小企業に対する攻撃に対する幅広い知見を有しており、顧客ベース全体から収集しているテレメトリを活用して、あらゆる企業の強力に保護しています。

Sophos MDR サービスは、顧客やアナリスト企業からも高い評価を受けています。最近の受賞の一部を以下に紹介します。

- Gartner® Peer Insights ™ Customers' Choice では過去 2 年間、647 件のレビューで 4.8/5 の評価を獲得 (2024 年 9 月 17 日現在)
- G2 の MDR 部門でリーダーに選出 (中堅企業顧客から第 1 位の評価を受けた MDR ソリューション)
- IDC MarketScape が実施した Worldwide Managed Detection and Response (MDR) 2024 Vendor Assessment (MDR ベンダーのグローバルな調査 2024 年版) でリーダーに選出

「セキュリティに関する深い専門知識に基づき、インシデントの発生から解決まで一貫した人間主導のサービスを提供してくれるような MDR プロバイダーを求めている組織にとって、ソフォスは魅力的な選択肢である」
Richard Thurston 氏 (IDC、European Security Services、リサーチマネージャ)

MSP

ソフォスには、大規模で今も急速に成長している MSP パートナーのエコシステムがあり、Sophos MDR などのソフォスの製品とサービスを世界中の中小企業に提供することができます。

中堅中小企業向けに設計されたソリューション

プラットフォーム

Sophos Central は、業界で最大かつ最もスケーラブルなクラウドネイティブ AI プラットフォームです。Sophos Endpoint、Sophos Firewall、Sophos XDR、Sophos MDR、Sophos Email、Sophos ZTNA など、すべてのソフォスの次世代サイバーセキュリティソリューションを管理するときに、Sophos Central を使用できます。ソフォス以外の Microsoft や Google などの幅広いテクノロジーを統合することができ、顧客は既存のセキュリティ投資から最大限の価値を得ることができます。

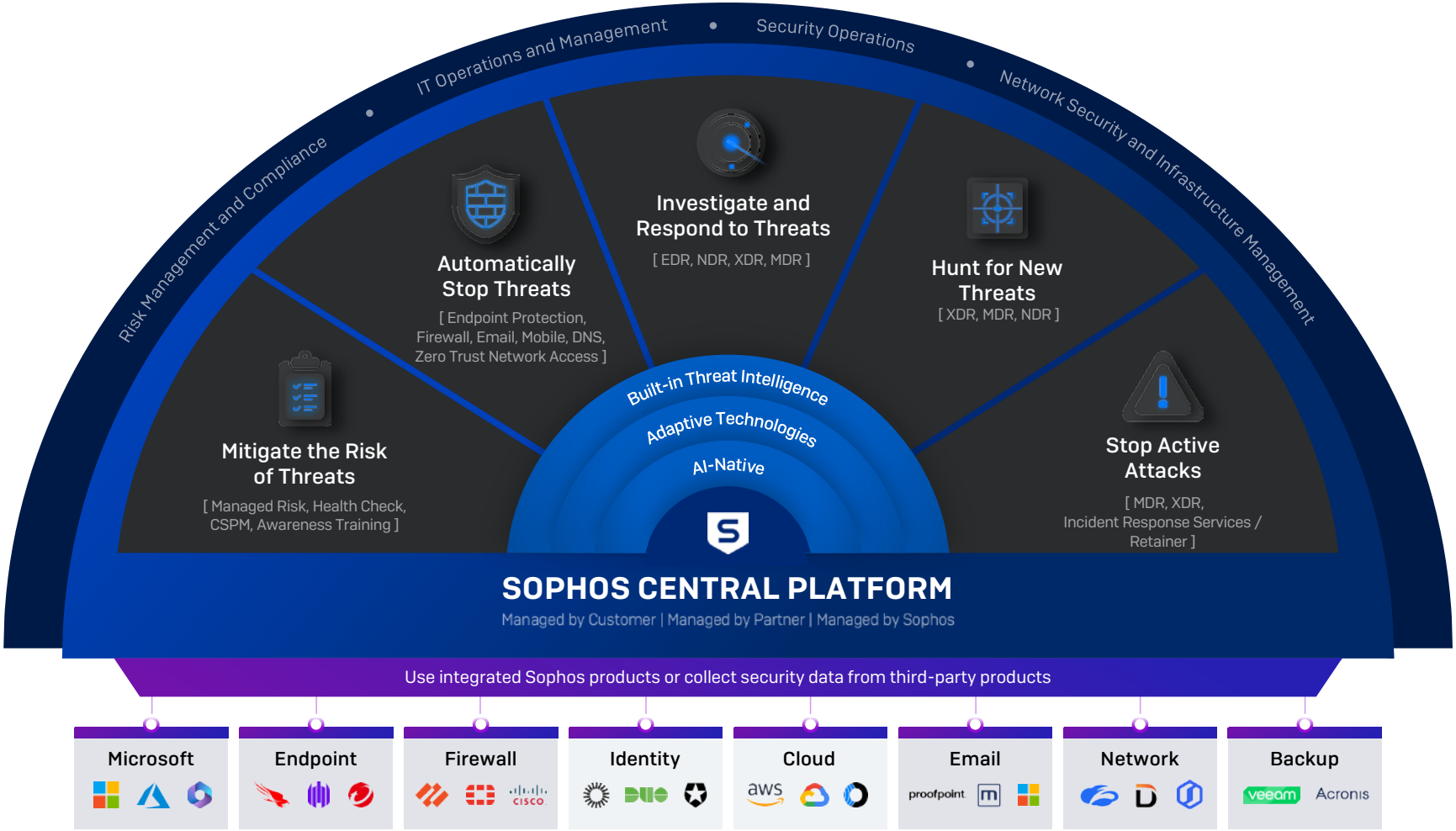
製品機能

ソフォスのソリューションは非常に洗練されており、サイバー脅威を阻止してきた数十年にわたる経験が活かされています。また、利便性を重視した設計になっており、あらゆる規模やリソースレベルの組織が、市場をリードする防御機能の恩恵を受けることができます。

以下のようなソフォスのソリューションを利用できます。

- **Sophos Endpoint** には、市場をリードするランサムウェア対策とエクスプロイト対策機能が含まれ、推奨される設定が有効になった状態で自動的に導入されるため、手動での調整が不要です。
- **Sophos Firewall** の一元管理およびレポート機能で、複数のファイアウォールを一か所から管理できます。この機能は、特に複数の拠点がある企業で役立ちます。
- **Sophos Endpoint** には、自社環境に存在する攻撃者を検出して自動的に対応する適応型防御機能が搭載されており、防御体制を強化し、対応するための貴重な時間を確保できるようにします。
- **Sophos Endpoint** に組み込まれているアカウントの状態チェック機能によって、セキュリティポスチャを明確かつリアルタイムに可視化でき、ワンクリックで推奨設定に戻すことができる [自動修正] オプションも利用できます。
- **Sophos Firewall** はソフォスのプラットフォームと統合され、進行中の脅威を自動的にブロックし、エンドポイントや ZTNA、さらにスイッチやワイヤレスアクセスポイントのすべてにわたって対応を調整し、ラテラルムーブメントを防止します。

ソフォスのサイバーセキュリティプラットフォーム



結論

今回の調査では、サイバーセキュリティのスキル不足が中小企業にとって重大な課題になっていることが明らかになりました。スキルや能力が不足していると、企業が攻撃を防ぐ能力に重大な影響を及ぼします。スキル不足の解消に終わりが見えない中、中小企業はサードパーティの専門家と協業し、自社のビジネスに最適なソリューションを選択することで、スキル不足による影響を緩和する手段を取り入れる必要があります。

中堅中小企業向けのソフォスソリューションの詳細については、ソフォスの担当者またはパートナーにお問い合わせいただくか、www.sophos.com をご覧ください。

Gartner および Peer Insights™は、Gartner, Inc. および/またはその関連会社の商標です。All rights reserved.
Gartner Peer Insights のコンテンツは、独自の経験に基づいた個々のエンドユーザーの意見で構成されており、事実を示すものではありません。また、Gartner やその関連会社の見解を表すものでもありません。

Gartnerは、Gartner Peer Insightsに掲載された特定のベンダー、製品またはサービスを推奨するものではありません。
Gartnerは、商品性または特定目的への適合性の保証を含む、その正確性または完全性について、本コンテンツの内容に関する一切の責任を、明示または黙示を問わず負うものではありません。

© Copyright 2024.Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK.
Sophos は、Sophos Ltd. の登録商標です。本書に記載されている製品や企業名はすべて、各所有者の商標または登録商標です。

2024-10-08 JA-WP (PC)

SOPHOS