レポート

2026 年におけるサイバーセキュリティの信頼の実態

独立した調査会社が実施した IT およびセキュリティのリーダー 5,000 人を対象とした調査から得られた知見

SOPHOS

はじめに

組織がサイバーセキュリティベンダーを選定する際には、人材、データ、収益といった重要な運用面のレジリエンスを、ベンダーに委ねることになります。

しかし、ソフォスの最新調査によると、このように高い依存関係にあるにもかかわらず、多くの組織が、セキュリティ確保のために依存しているベンダーに十分な信頼を寄せていない実態が明らかになっています。

ソフォスは、サイバーセキュリティベンダーに対する信頼の実態を把握するため、独立した調査会社に委託し、17 か国 5,000 人の IT およびセキュリティ意思決定者を対象としたグローバル調査を実施しました。本調査は、サイバーセキュリティ分野に特化した調査会社である Vanson Bourne によって実施され、サイバーセキュリティの購入者とベンダー間における信頼がどのように構築され、またどのように損なわれているのかについて、統計的に有意かつ実務に即した示唆を提供しています。

5,000

独立した調査会社が実施したグローバルな調査に参加した 17 か国の IT およびセキュリティのリーダーの数

主な調査結果

信頼の欠如：自分と自社の両方がサイバーセキュリティベンダーを全面的に信頼していると回答した IT リーダーは、わずか 5% にとどまっています。

信頼は、裏付けとなる実証データによって築かれる：IT 部門および経営幹部は、検証可能なサイバーセキュリティ成熟度の証跡こそが、信頼性を示す最も重要な指標であるという点で一致しています。

ベンダーの信頼性を評価することは依然として困難：79% の組織が、新規のサイバーセキュリティベンダーの信頼性を評価することは難しいと感じており、さらに 62% の組織が既存ベンダーについても同様に難しいと感じています。回答者は、ベンダーへの信頼を低下させる要因としていくつかの点を挙げており、その中でも特に多かったのが、ベンダーが提供する情報が事実に基づいていない、あるいは十分に詳細でないという点でした。

この信頼の欠如がもたらす結果：回答者の 51% は、信頼の欠如により、自社が重大なサイバーインシデントに見舞われる可能性が高まるのではないかという不安につながっていると回答しています。

実務担当者と経営幹部の間では見解が一致していないことが多い：回答者の 78% が、自社のサイバーセキュリティベンダーの信頼性について、IT 部門と経営幹部や取締役会の間で見解が異なると回答しています。ソフォスの調査に回答した企業の 3 分の 1 近くが、この意見の相違は「頻繁」と回答しています。

信頼性を評価することは困難

自分と自社の両方がサイバーセキュリティベンダーを全面的に信頼していると回答した IT リーダーは、わずか 5%にとどまっています。

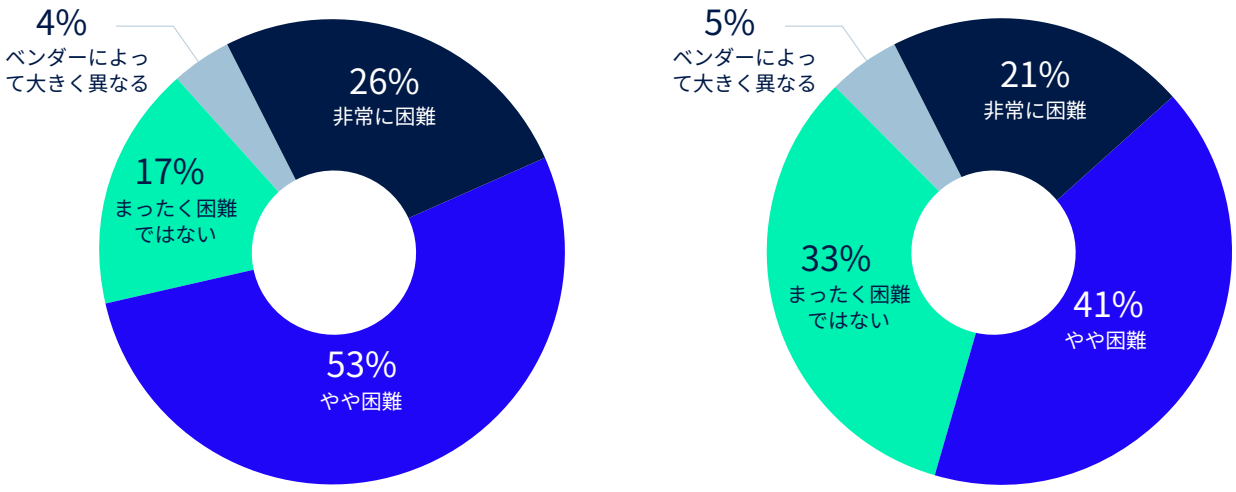
サイバーセキュリティベンダーにネットワークの保護と業務継続性を委ねる上で、信頼は極めて重要な要素です。サイバーセキュリティベンダーは、夜間や週末、IT 部門のスタッフの休暇中でも、24 時間体制でお客様のビジネスを保護します。中小企業では、専任の IT スタッフさえいない場合があり、導入しているサイバーセキュリティ製品やサービスが、自社の一員のような役割を担うこともあります。

組織が誰を信頼すべきかを判断する以前に、さらに根本的な課題に直面しています。それは、そもそもベンダーの信頼性そのものを適切に評価することです。

調査によると、回答者の 79% が、新規のサイバーセキュリティベンダーやパートナーの信頼性を評価することは難しいと感じており、多くの組織が製品の比較、主張内容の検証、さらには候補となるベンダーが実際に自社を保護できるのかを見極めることに苦労している実態が明らかになっています。さらに回答者の 62% が、すでに取引のあるベンダーの信頼性を評価するのにも苦労していると回答しており、契約後も信頼の問題が解消されないことを示しています (図 1)。

79%

調査対象の企業のうち、新しいサイバーセキュリティベンダー / パートナーの信頼性を評価することが困難であると回答した企業の割合



新しいサイバーセキュリティベンダーとパートナーの評価

既存のサイバーセキュリティベンダーとパートナーの評価

図 1：一般的に、サイバーセキュリティベンダーやパートナーの信頼性を評価することは、どの程度困難ですか？

信頼を評価するときの障壁

回答者は、信頼を評価するときの障壁をいくつか指摘していますが、それらの多くは透明性に関係しています。多くの組織が、ベンダーの主張を正しく理解したり、技術的な詳細を評価したり、確信を持って意思決定を行うために必要な情報を見つけたりすることに苦労しています。

半数近く (47%) が、ベンダーが提供する情報が事実に基づかない、あるいは詳細ではないと回答し、45% が情報を解釈または理解することが困難だと感じています。さらに 43% が、ベンダーを効果的に評価するためのスキルや知識が不足していると認め、41% が矛盾する情報に遭遇し、38% が必要な情報を見つけるのに苦労しています (図 2)。

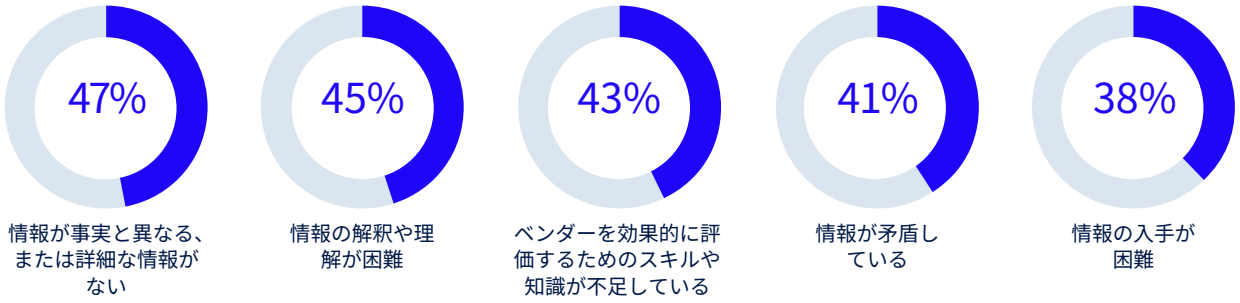


図 2：サイバーセキュリティベンダーの信頼性を評価するのが難しいと感じている理由は何ですか？回答者数 =4,483

従業員 250 名未満の中小企業と 1,000 名以上の大企業との間で最も大きな違いとして挙げられるのは、中小企業の方がベンダーの信頼性を適切に評価するために必要なスキルや知識が不足している傾向が強い点です。この課題を挙げた割合は、大企業の回答者と比べて中小企業の方が 8% 高くなっています (図 3)。

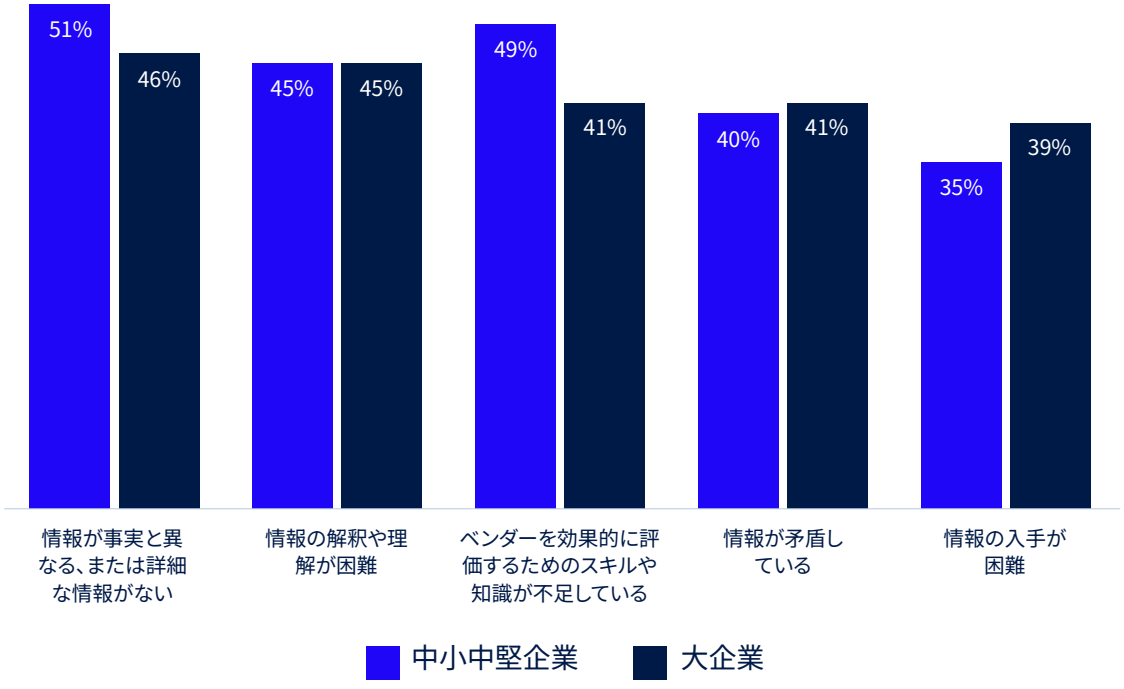


図 3：サイバーセキュリティベンダーの信頼性を評価するのが難しいと感じている理由は何ですか？回答者数 =504 (中小中堅企業)、2,260 (大企業)。

信頼の欠如がもたらす結果

本調査は、セキュリティベンダーと顧客の間における信頼の欠如が、さまざまな側面において重大な影響を及ぼす課題であることを定量的に示しています。サイバーセキュリティベンダーを全面的に信頼できない影響について質問したところ、回答者は感情的な影響と業務面での影響が混在していると指摘しました。

- **51%** が、重大なサイバーインシデントが発生する懸念が高まると回答しています。
- **45%** が、結果としてベンダーの切り替えを検討する可能性が高まる回答しています。これは多くの組織にとってコストがかかり、業務にも大きな影響を及ぼすプロセスです。
- **42%** が、監視要件が増大すると認識しています。
- **41%** が、サイバーセキュリティポスチャに関する安心感が低下したと報告しています。
- **38%** が、自分または自社が誤ったベンダーを選択したのではないかと懸念しています。

これらの影響は、すでに IT およびサイバーセキュリティ部門に課されている運用負荷をさらに増大させる要因となっています。

IT 部門と経営幹部の評価の食い違い

もう一つの重要な課題は、日常的にサイバーセキュリティツールを利用する現場担当者と、契約の最終承認を行う意思決定者との間に生じる認識のズレです。回答者の 78% が、サイバーセキュリティベンダーの信頼性について、IT 部門と経営幹部または取締役会の間で意見が異なると回答し、ほぼ 3 分の 1 が、これらの意見の相違は「頻繁に発生する」と回答しています (図 4)。

回答者は、上級管理職が購入の決定に依然として強く関与していると回答しています。取締役会や経営幹部がサイバーセキュリティ製品の購入決定に関与していないと回答した組織はわずか 1% でした。

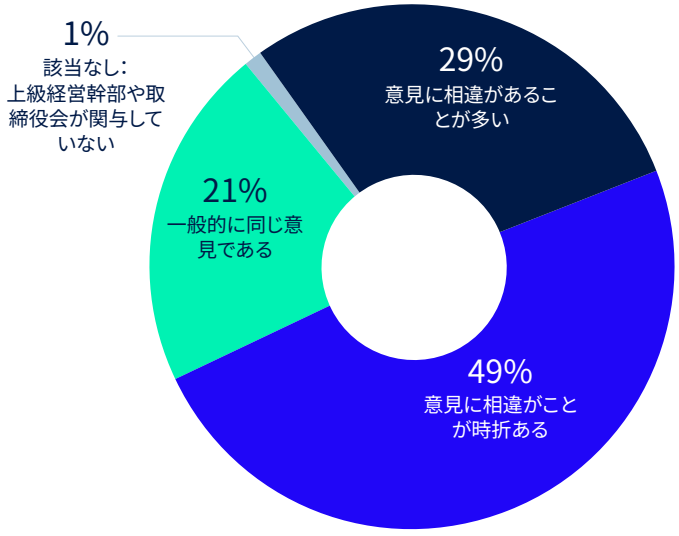


図 4：自社のサイバーセキュリティベンダーの信頼性について、IT 部門と経営幹部や取締役会の間で見解が異なる場合はありますか？回答者数 =5,000。

1%

上級経営幹部がサイバーセキュリティ製品の購入決定に関与していないと回答した組織の割合

サイバーセキュリティの信頼を構築する方法

回答者は、透明性が高く、根拠に基づいたセキュリティの取り組みこそが、信頼構築のために重要であることを示しています。組織は、透明性、明確さ、根拠に基づくセキュリティの対策を通じて信頼を築くことができるベンダーを求めています。

経営幹部と IT 部門の両方ともに、「サイバーセキュリティ成熟度を示す検証可能な証跡」が、サイバーセキュリティベンダーへの信頼を左右する最も重要な要因としてあげています。これらの検証可能な証跡のタイプには、バグ報奨金プログラム、公開しているトラストセンター、自社製品の脆弱性とその対応方法を詳述したアドバイザリ、第三者評価、各種認証などが含まれます。

「インシデント発生時および情報開示時における透明性と迅速なコミュニケーション」も、経営幹部にとっては第 2 位、IT 部門にとっては第 3 位の重要な要因として位置付けられました。

サイバーセキュリティベンダーに対する信頼を左右する要因

要因	上級経営幹部 / 取締役会	IT / サイバーセキュリティ部門	影響を与える要因
第一の要因	1 位	1 位	サイバーセキュリティの成熟度を示す検証可能な証跡 (例、バグ報奨金プログラム、トラストセンター、アドバイザリ、第三者評価、各種認証)
	2 位	3 位	インシデントや開示時の透明性と迅速なコミュニケーション
	3 位	4 位	大規模なサイバーインシデント発生後の専門家による解説 (例、報道機関やテレビでのコメント)
	4 位	2 位	高品質のサイバーセキュリティサービスと製品の一貫とした提供
	5 位	5 位	アナリストレポートでの実績 (Gartner Magic Quadrant など)
第二の要因	6 位	9 位	内部のセキュリティ手順の透明性
	7 位	7 位	MITRE、SE Labs などの独立したテストでの実績
	8 位	6 位	迅速で信頼されるサポート
	9 位	8 位	リセラー / サイバーセキュリティパートナーからの推奨
第三の要因	10 位	13 位	脅威調査レポートの品質
	11 位	12 位	金融 / ビジネス分野のメディアにおける掲載状況
	12 位	11 位	他社 (同業者 / 顧客) の経験
	13 位	10 位	個人的な経験

経営幹部 / 取締役会のサイバーセキュリティベンダーに対する信頼レベルに最も影響を与える要因は何ですか？1位の回答から順に表示
IT / サイバーセキュリティ部門のサイバーベンダーに対する信頼レベルに最も影響を与える要因は何ですか？1位の回答から順に表示

お客様とパートナーの信頼に応えるソフォスの取り組み

信頼とは押し付けるものではなく、築き上げるものだとソフォスは考えています。だからこそ、日々、透明性と誠実性を重視しながら、セキュリティやプライバシーの保護に取り組んでいます。

ソフォスの取り組みの中心にあるのは、Sophos Trust Center です。ここでは、セキュリティアドバイザリの公開、製品の脆弱性とその対応方法の明示、コンプライアンス体制の説明、お客様データの保護方法についての情報を提供しています。

この透明性は、Sophos X-Ops による Pacific Rim の調査にも表れており、中国を拠点とするサイバー攻撃グループによる 5 年間にわたる活動を公表するとともに、戦術、手法、手順 (TTP)、侵害の痕跡 (IOC)、組織全体のレジリエンス強化に役立つ防御ガイダンスを詳細に共有しています。

高度な国家支援型の攻撃活動を明らかにし、政府機関や他ベンダーと連携しつつ、自社の強みだけでなく弱みについても率直に開示することで、ソフォスは、信頼とは誠実さ、説明責任、デジタルエコシステム全体を守るという継続的な取り組みによって日々築かれるものであることを示しています。

詳細情報

信頼の確立に向けたソフォスの取り組みや、ソフォスの信頼性評価に役立つ各種リソースの詳細については、Trust Center にアクセスするか、ソフォスのパートナーまたはソフォス営業部までお問い合わせください。

詳細については、トラストセンターにアクセスするか、ソフォスのパートナーまたは担当者にお問い合わせください。

ソフォス株式会社営業部
Email: sales@sophos.co.jp