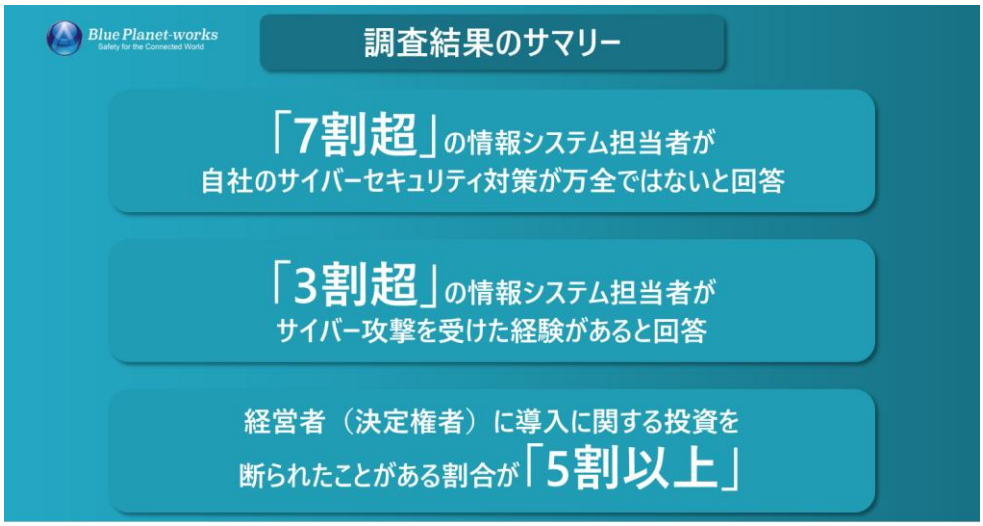
NEWS RELEASE
報道関係者各位

2025年3月11日
Blue Planet-worksPR事務局

【情報システム担当500名に聞いた「サイバーセキュリティ実態調査」】3割以上が被害経験、7割が対策に不安を抱える実態が明らかに 経営者（決定権者）のセキュリティ投資判断に課題

ゼロトラスト型エンドポイントセキュリティ「AppGuard」を提供する、株式会社Blue Planet-works（東京都品川区、代表取締役社長：坂尻浩孝、以下当社）は、各企業の情報システム担当者500名に対して、「サイバーセキュリティに関する実態調査」を行い、調査結果を発表します。

7割超（70.8%）の情報システム担当者が自社のサイバーセキュリティ対策が万全ではないと回答しており、サイバー攻撃を受けた経験があると回答した割合は3割超（33.0%）となりました。自社のセキュリティ対策が万全ではない、サイバー攻撃に対して事前の対策が必要であると考える情報システム担当者が多い中、経営者（決定権者）に導入に関する投資を断られたことがある割合が5割以上（52.4%）と半数を超える状況が判明しました。



■調査実施の背景

昨今の急速なテクノロジーの進化により、ランサムウェアは依然として企業にとって大きな脅威として立ちはだかっています。ランサムウェアを含むマルウェア感染以外にも、フィッシングメールや偽サイトを悪用するソーシャルエンジニアリングの手法も巧妙化しており、多くの組織がセキュリティ対策を見直す必要が生じています。

そこで、情報セキュリティ業務に従事している500名の情報システム担当者に対して、「サイバーセキュリティに関する実態調査」を実施し、結果を公開します。

調査内容の詳細は本記事でご覧いただけます。

■調査概要

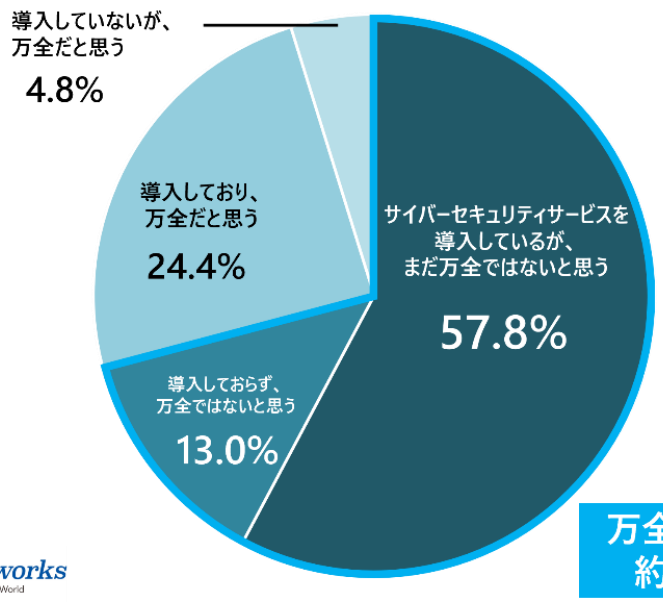
-調査概要　　：サイバーセキュリティに関する実態調査
-調査方法　　：インターネット調査
-調査主体　　：Blue Planet-works
-調査期間　　：2024年11月8日～11月12日
-調査対象　　：企業の情報システム部門担当者
-調査対象地域：全国
-回答数　　：500サンプル

■調査結果の詳細

■7割超の情報システム担当者が自社のサイバーセキュリティ対策が万全ではないと回答
■セキュリティ対策において期待している効果は「社内のセキュリティ意識強化」、「事業継続の担保」が多い結果に

自社のセキュリティ対策に関して、70.8%の情報システム担当者が「万全ではないと思う」と回答しました。
セキュリティ対策において期待している効果は「社内のセキュリティ意識強化(45.4%)」、「対策を講じることによる、事業継続の担保(44.6%)」の回答が多い結果となっています。

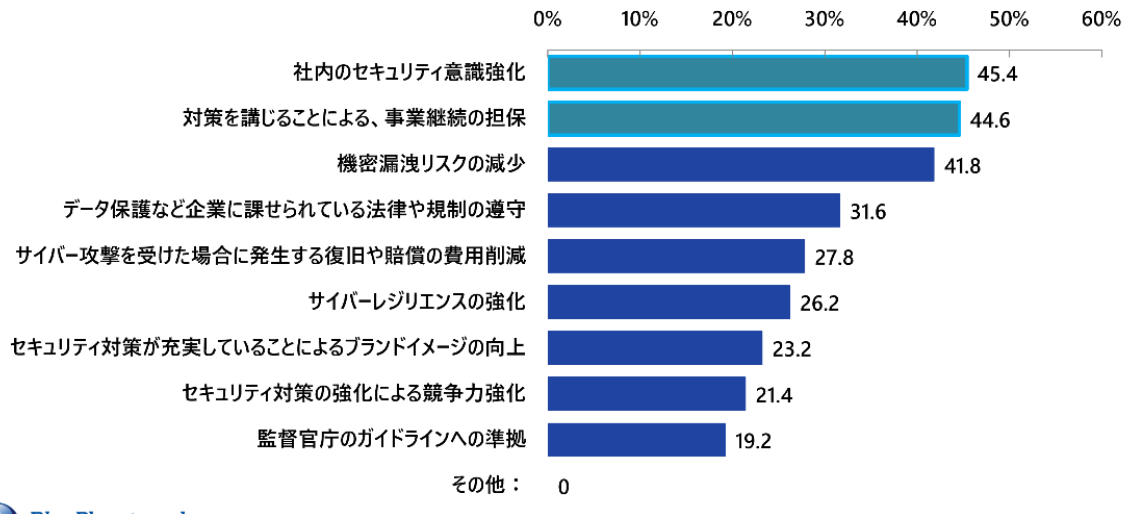
Q1 近年、大手企業を中心にサイバー攻撃が多発していますが、現在の自社のセキュリティ対策について、どのように考えていますか。
（n=500「企業の情報システム部門担当者」／単一回答）



Blue Planet-works
Safety for the Connected World

万全ではないと思う：約7割（70.8%）

Q2 自社のセキュリティ対策は、どのような効果を期待して行なっていますか。
※自社のセキュリティ対策について、セキュリティサービス未導入、または万全ではないと感じている方も、セキュリティ対策をする場合に期待する効果についてお答えください。
（n=500「企業の情報システム部門担当者」／複数回答）



Blue Planet-works
Safety for the Connected World

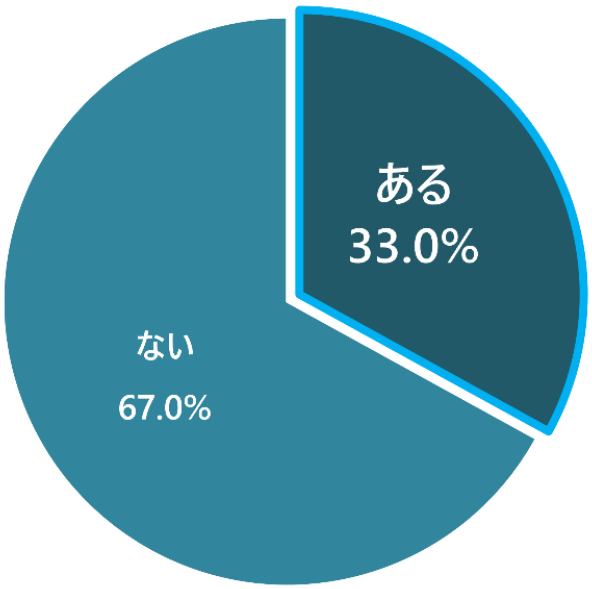
■調査結果の詳細

■3割超の情報システム担当者がサイバー攻撃を受けた経験があると回答

■被害の影響として「業務の中断・遅延」と回答した割合が4割と最多

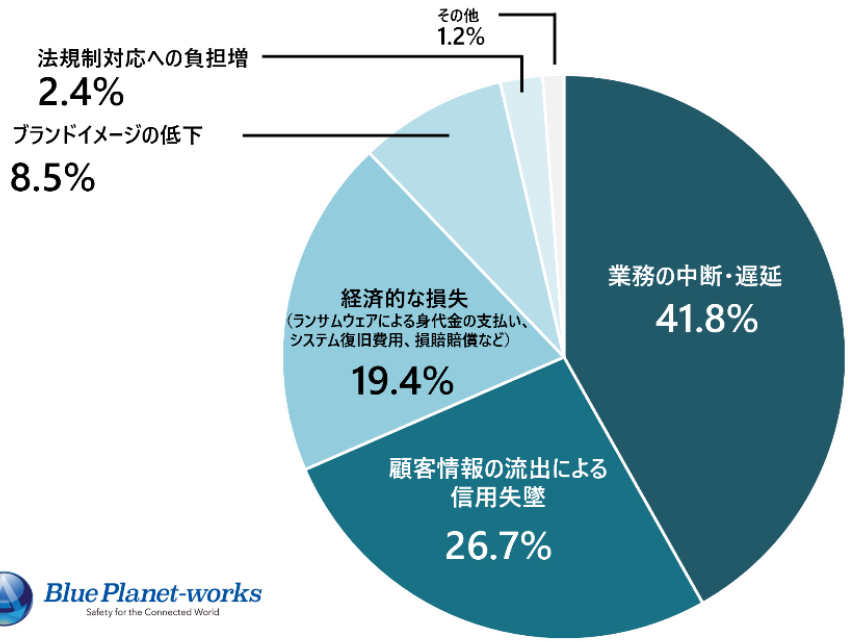
33.0%の情報システム担当者が、今まで自社においてサイバー攻撃を受け、何らかの被害や影響が生じた経験があると回答。被害により一番影響を受けた内容として、最も多かったのは「業務の中断・遅延」で約41.8%。続いて「顧客情報の流出による信用失墜(26.7%)」、「経済的な損失《ランサムウェアによる身代金の支払い、システム復旧費用、損賠賠償など》(19.4%)」と、企業において深刻な影響が発生していることがわかりました。

Q3｜ 自社においてサイバー攻撃を受けたことで何らかの被害や影響が生じた経験はありますか。
（n=500「企業の情報システム部門担当者」／単一回答）



Blue Planet-works
Safety for the Connected World

Q4｜ 被害を受けたことで一番影響を受けたことは何ですか？最もあてはまるものをお選びください。
（n=165「サイバー攻撃を受けたことのある方」／単一回答）



Blue Planet-works
Safety for the Connected World

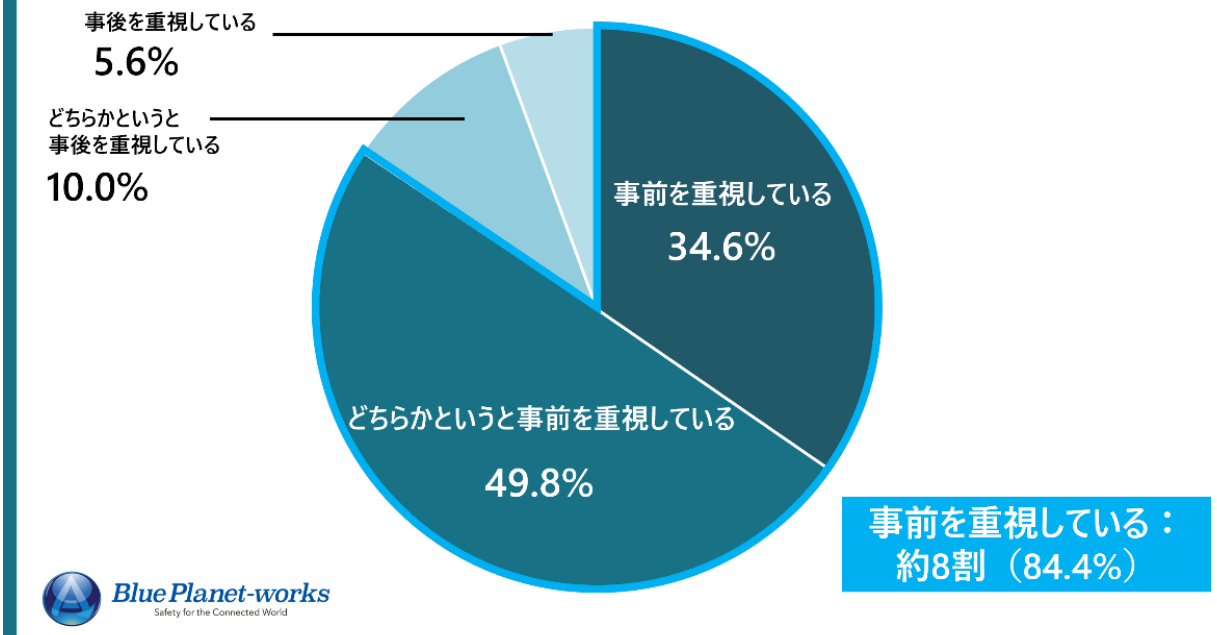
■調査結果の詳細

■セキュリティ対策をする場合、「事前」の対策を重視すると回答した割合が約8割に

■危機感を感じているセキュリティリスクは「システムのロックダウン」がトップ

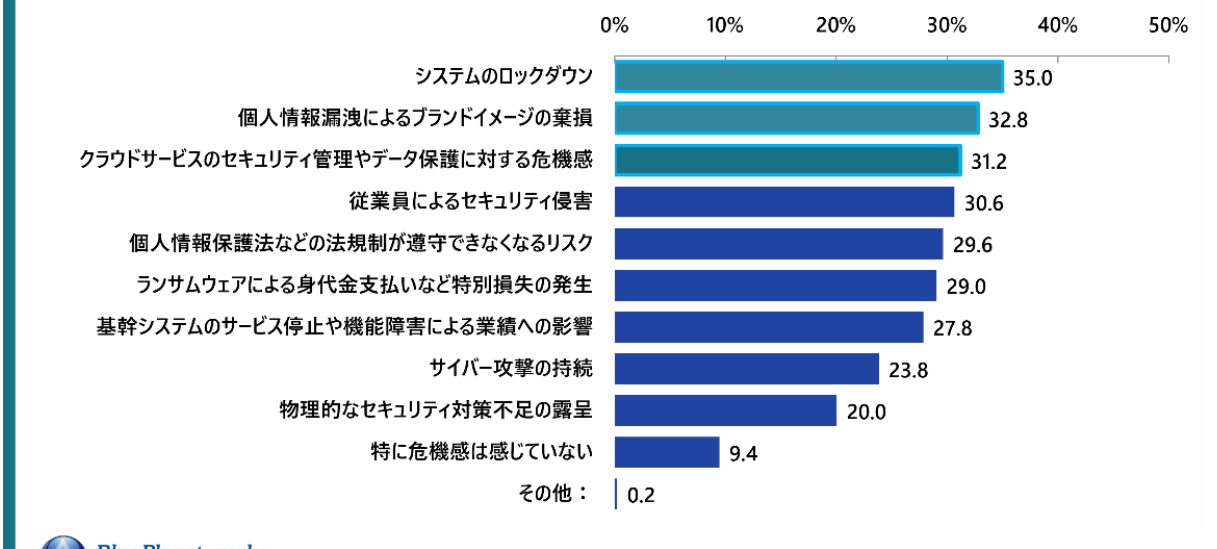
サイバーセキュリティ対策に関して、サイバー攻撃に備える「事前」の対策、サイバー攻撃を受けたあとの「事後」の対処法、どちらを重視しているか調査したところ、事前を重視していると回答した割合が84.4%という結果に。
また、自社の事業を展開する上でのセキュリティリスクについて、危機感を感じているTOP 3 は「システムのロックダウン（35.0%）」「個人情報漏洩によるブランドイメージの棄損（32.8%）」「クラウドサービスのセキュリティ管理やデータ保護に対する危機感（31.2）」となりました。

Q5｜ 自社では、サイバーセキュリティ対策に関して、サイバー攻撃に備える「事前」の対策、サイバー攻撃を受けたあとの「事後」の対処法、どちらを重視して対策していますか。
（n=500「企業の情報システム部門担当者」／単一回答）



Blue Planet-works
Safety for the Connected World

Q6｜ 自社の事業を展開していく上でのセキュリティリスクについて、危機感を感じている事はありますか。当てはまるものをすべてお知らせください。
（n=500「企業の情報システム部門担当者」／複数回答）



Blue Planet-works
Safety for the Connected World

■調査結果の詳細

■サイバー攻撃によって自社の業務システムがストップした際の備えとして「サーバやパソコン、プリンターなどIT機器のソフトウェアの脆弱性対策」が31.8%で最多

業務システムがストップする場合の備えに関して、最も多い回答が「サーバやパソコン、プリンターなどIT機器のソフトウェアの脆弱性対策(31.8%)」となり、続いて「セキュリティ情報収集体制の確認（27.8%）」、「従業員に対するインシデント確認時の報告窓口や連絡体制、対応時の注意事項などの確認（25.6%）」が多い状況です。

Q7 | サイバー攻撃によって自社の業務システムが（部分的、または全面的に）ストップした際に備えて、どのような対策をしていますか。
（n=500「企業の情報システム部門担当者」／複数回答）

1. サーバやパソコン、プリンターなどIT機器のソフトウェアの脆弱性対策（31.8%）
2. セキュリティ情報収集体制の確認（27.8%）
3. 従業員に対するインシデント確認時の報告窓口や連絡体制、対応時の注意事項等の確認（25.6%）
4. 感染が確認された時の連絡先やルート、相談先の確認（24.8%）
5. 緊急度、重要度の高いセキュリティ情報を受け取った時の社内体制の確認（24.2%）

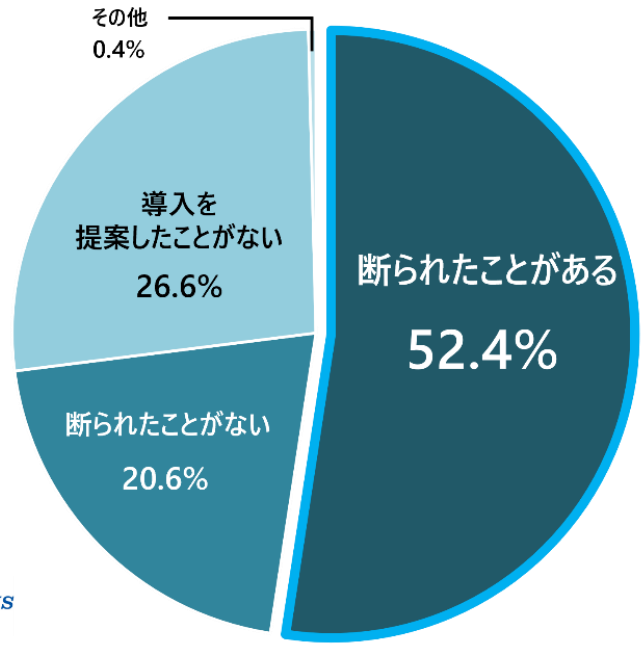
Blue Planet-works
Safety for the Connected World

■調査結果の詳細

■5割以上の情報システム担当者が
経営者（決定権者）に導入に関する投資を断られたことがあると回答

自社のセキュリティ対策が万全ではない、サイバー攻撃に対して事前の対策が必要であると考える情報システム担当者が多い中、経営者（決定権者）に導入に関する投資を断られたことがある割合が52.4％と半数を超える結果となりました。理由として最も多かったものは「優先順位が低いとされ断られたことがある（20.6%）」となり、続いて「効果や必要性を理解してもらえず断られたことがある（16.8%）」、「予算が確保できず断られたことがある(15%)」でした。

Q8｜ サイバーセキュリティサービスを導入したほうがいいと判断したが、
経営者（決定権者）に導入に関する投資を断られたことがありますか。
※あなたご自身の経験のほか、あなたのチームや社内システム関連の部署としての経験まで含めてお知らせください。
（n=500「企業の情報システム部門担当者」／単一回答）



Blue Planet-works
Safety for the Connected World

Q8｜ 経営者（決定権者）に導入に関する投資を断られた主な理由

1 優先順位が低いとされ断られたことがある（20.6%）

2 効果や必要性を理解してもらえず断られたことがある（16.8%）

3 予算が確保できず断られたことがある（15.0%）

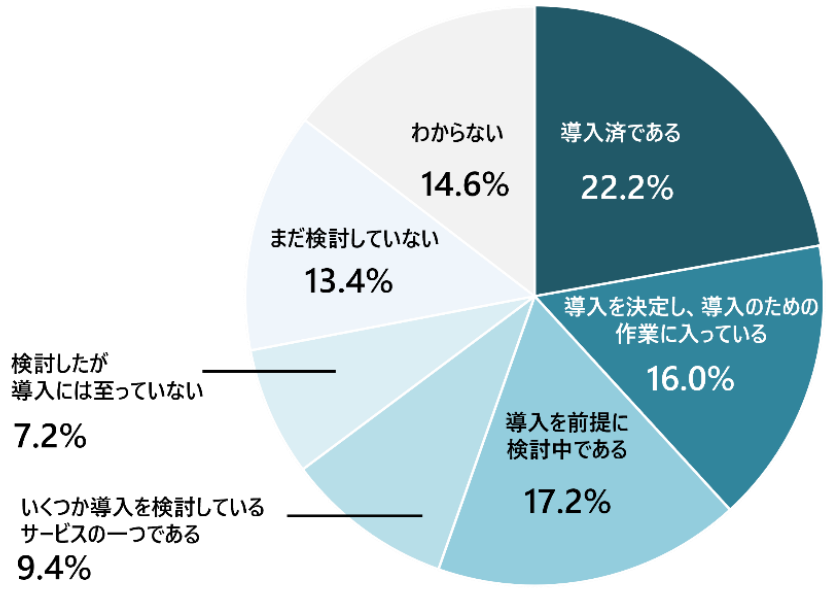
Blue Planet-works
Safety for the Connected World

■調査結果の詳細

■EDR（Endpoint Detection and Response）に関して、
導入済であると回答した割合が約2割、導入予定＋導入を前提に検討中が約3割
■約6割がEDRを導入すれば自社のセキュリティ対策は万全だと考えている状況

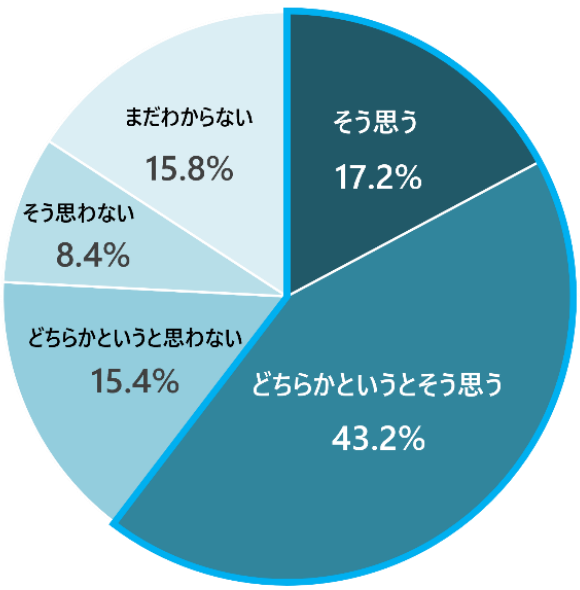
既にEDRを導入していると22.2%が回答。導入を決定、導入を前提に検討していると回答した割合は33.2%となっています。併せて、EDRによる対策の信頼性を調査したところ、60.4%がEDRを導入すれば自社のセキュリティ対策は万全だと考えている状況です。

Q9 自社におけるEDR（Endpoint Detection and Response）の導入状況をお知らせください。
（n=500「企業の情報システム部門担当者」／単一回答）



Blue Planet-works
Safety for the Connected World

Q10 EDR（Endpoint Detection and Response）を導入すれば自社のセキュリティ対策は万全だと考えていますか。
（n=500「企業の情報システム部門担当者」／単一回答）



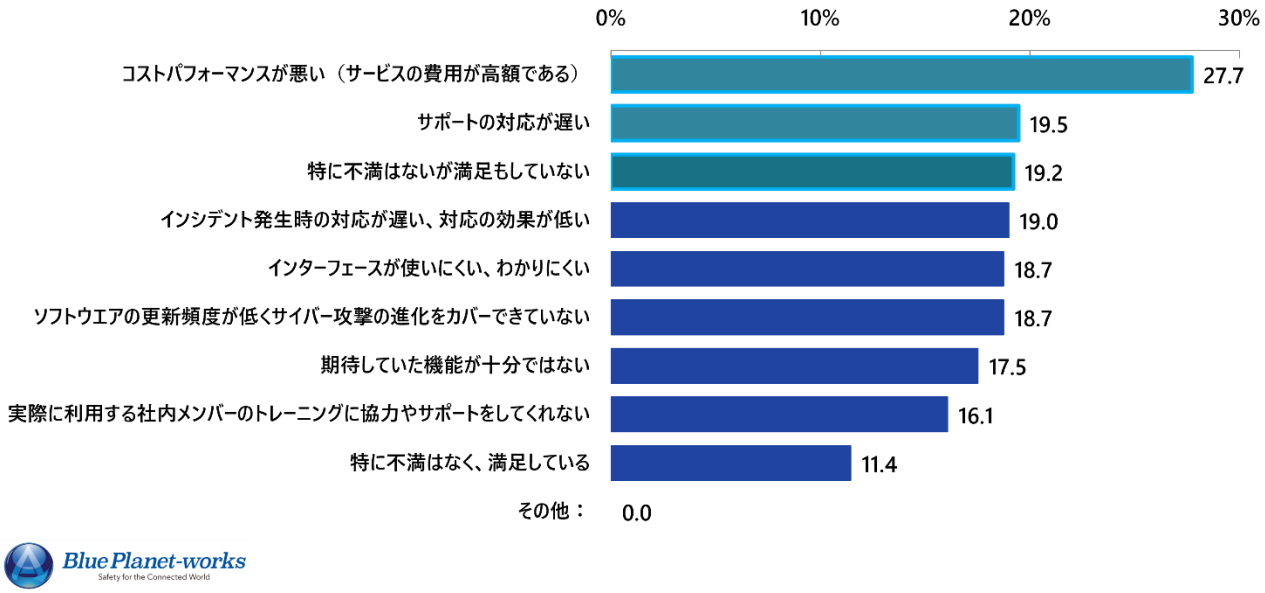
Blue Planet-works
Safety for the Connected World

■調査結果の詳細

■導入済のサイバーセキュリティサービスに対する不満点に関して、「コストパフォーマンスが悪い《サービスの費用が高額》」が約3割と一番多い回答に

既にサイバーセキュリティサービスを導入している担当者（n=411）に、サービスに対する不満点を調査したところ、「コストパフォーマンスが悪い《サービスの費用が高額である》（27.7%）」と一番多い回答に。次に「サポートの対応が遅い（19.5%）」、「インシデント発生時の対応が遅い、対応の効果が低い（19.0%）」という結果となりました。

Q11 サイバーセキュリティサービスを導入している方にお聞きします。
導入しているサービスに対する不満点はありますか。当てはまるものをいくつでもお知らせください。
（n=411「既にサイバーセキュリティサービスを導入している担当者」／複数回答）



■【ご参考】調査結果に関する見解

株式会社Blue Planet-works 取締役 鳴原祐輔

現代において、サイバー攻撃は規模や知名度に関わらず、あらゆる組織にとって避けられない脅威となっています。経営層は、セキュリティ対策を単なる「コスト」ではなく、事業継続に不可欠な「投資」と捉え、その認識を改める必要があります。しかし、今回のアンケート結果から、日本の経営者はセキュリティ対策を事業成長への貢献が不明確なコストと捉えがちで、情報システム部門は、経営者からの合意を得るのに苦労するケースが多いようです。確かにセキュリティ対策が直接的な利益や生産性向上に結びつきにくいという構造的な問題から、経営層の理解と投資を得ることが難しいという現状も理解できます。しかし、サイバー攻撃による事業停止や信用失墜は、短期的利益を遥かに超える損失をもたらし、企業の存続を脅かす可能性もあることを、経営者にも理解してもらわなければなりません。

また、セキュリティ対策への取り組みとして国内の多くの組織が矛盾した行動をとっている状況が浮き彫りになりました。セキュリティ対策の目的として「業務の継続性」を掲げ、さらに「事前対策」の重要性を理解しているにもかかわらず、実際には「攻撃を検知すること」に注力し、セキュリティ対策として「EDR」に過度な期待を寄せています。多くの組織が「EDR」を導入すればセキュリティ対策は万全だと考えているようですが、それは大きな誤解です。「EDR」は、例えるならば「監視カメラ」のようなものです。確かに、異常を検知し、記録することはできます。しかし、監視カメラがあるだけでは犯罪を防げないように、EDRも導入しただけで安心できるわけではありません。重要なのは、検知した情報を分析し、適切に対処できる体制と具体的な対処策を整備することです。セキュリティ対策において有事の対策も必要ではありますが、平時のセキュリティ対策こそが、根本的な解決策であり、被害を最小限に抑えるための最良の手段です。病気が発症してから慌てるのではなく、日頃から免疫力を高めることが重要であるのと同様です。

2025年も2024年と同様に、従来のセキュリティ対策では対処しきれない高度な攻撃がさらに拡大すると予想されます。マルウェアはますます検知が困難な構造になり、正規の認証情報やツールを悪用して侵入してくるでしょう。もはや、ユーザーの操作なのか、それとも攻撃なのかを区別し続けることには限界があると考えられます。このように絶えず変化する脅威に対抗するため、私たちも防御のアプローチを抜本的に見直す時期に来ているのかもしれません。

■株式会社Blue Planet-worksについて

株式会社Blue Planet-worksは、「サイバー攻撃は完全に防ぐことができるという、新しい常識をつくる。」をミッションに掲げ、革新的な「AppGuard」テクノロジーをベースとしたサイバーセキュリティ製品及びサービスを提供する日本発のグローバル・サイバーセキュリティ・カンパニーです。

■会社名	：株式会社Blue Planet-works
■所在地	：〒141-0032　東京都品川区大崎4-1-2 ウィン第 2 五反田ビル3F
■設立	：2017年4月
■代表取締役社長	：坂尻浩孝
■グループ子会社	：AppGuard Inc.、株式会社ITガード
■事業内容	：「AppGuard」の技術を応用したサイバーセキュリティプロダクトの開発・販売及び付帯サービスの提供
■公式Webサイト	：https://www.blueplanet-works.com/

■「ゼロトラスト型」エンドポイントセキュリティ製品「AppGuard」について

ゼロトラスト型エンドポイントセキュリティ製品「AppGuard」は、過去の脅威情報に頼ることなくシステムの安全性を保つという発想の転換を独自の特許技術で実現し「もう、セキュリティで悩まない。」世界を提供します。
AppGuardは、未知・既知を問わず、高度なサイバー攻撃によるエンドポイントの侵害を未然に防止するセキュリティソリューションです。
この技術は2000年代にアメリカ国内で開発が進められましたが、2017年にBlue Planet-worksがその特許技術、知財を含むAppGuard事業を買収し、当初の米国チームから日本国内の開発チームが引き継いで製品の開発、改善を行っています。海外では米政府関連機関にも導入されており、日本国内は2018年より販売が開始され、大手航空会社や大手旅行会社、大手監査法人等において導入が進み、累計で20,000社(※)を超える企業に採用されてきました。
2025年2月現在、大手企業向けAppGuard Enterprise、中小・中堅企業向けAppGuard Small Business Edition、スタンドアローン版AppGuard Solo、サーバー向けAppGuard Server、産業システム向けAppGuard Industrial、公共機関向けAppGuard Government、医療機関向けAppGuard Medical、個人向けAppGuard Home Editionのシリーズを展開しています。

(※) 2025年2月時点での国内における導入社数（累計）