We bring security to life.

報道関係各位

2022/11/8
Trellix

Trellix（トレリックス）、セキュリティ担当者の業務におけるモチベーションと経営層のセキュリティ意識に関する実態調査結果（2022 年 10 月版）を発表

セキュリティ担当者の 61.7%が業務にフラストレーションの経験があり、
68.0%が別のキャリアへ進むことを検討

XDR（eXtended Detection and Response）の未来を提供するサイバーセキュリティ企業である、Trellix（トレリックス）は、日本国内の企業・団体の経営層、および情報システム部門など組織のセキュリティに関与するビジネスパーソンを対象に、経営層とセキュリティ担当者の情報セキュリティに関する意識調査を、Web アンケート方式で実施（2022 年 10 月）し、調査結果を発表しました。

ニュースハイライト
・セキュリティ業務への満足度：セキュリティ担当者の 59.0%が満足していると回答。セキュリティを担う仕事の価値は「従業員の円滑な業務遂行を支えている」「経営に対して貢献している」「組織の情報セキュリティ目標の立案、達成に向けた運用をしている」が上位 3 項目。
・業務におけるフラストレーション：セキュリティ担当者の 61.7%が経験があると回答。一方で経営層はセキュリティ担当者のフラストレーションを感じた経験について 43%があると見ていると回答。
・フラストレーションの要因：セキュリティ担当者が、フラストレーションを感じた場面として「スキル向上に対するサポート不足」が最多で、「従業員のプライバシーなど、センシティブな情報の取り扱い」は 51.2%が経験したと回答。
・業界キャリアの継続意向：セキュリティ担当者の 32.0%が今後もサイバーセキュリティ業界に留まるとし、68.0%は別のキャリアを考えていると回答。

今回の調査を通じて、セキュリティ担当者のキャリア形成の経緯と現状、業務上さまざまな場面でセキュリティ業務特有のフラストレーションが存在すること、今後もセキュリティ業界に留まるかどうかなど、彼らの意識実態を明らかにしています。また、経営側からのセキュリティ担当者への評価やセキュリティ担当者とのフラストレーションに関する認識のギャップについても触れ、事業進捗との関係などについても言及しています。

顕著な結果として、業務の影響で発生する疲労感や嫌悪感、フラストレーションの有無については、担当者は 61.7%が「経験がある」、経営層は 43.0%が、現場は「経験がある」（と見ている）と回答し、セキュリティ担当者の実感と経営側の認識に 20%近くのギャップが存在することがわかりました。一方で、セキュリティ担当者は自身の業務に満足感を持っており、特に従業員および組織への貢献に 70.0%が価値、やりがいを感じています。なお、集計にあたっては、勤務先または自身の顧客企業・団体の従業員数 500 名以上の経営層、セキュリティ担当者・専門家を対象としています。なお、2021 年 11 月に日本で実施した企業・団体のセキュリティ対策に関する調査結果、および 2022 年 6 月に米国で発表したセキュリティ人材の意識に関する調査結果を一部引用し比較しています（以降、「前回調査、2022 年 6 月 米国で発表した調査結果」と表記）。

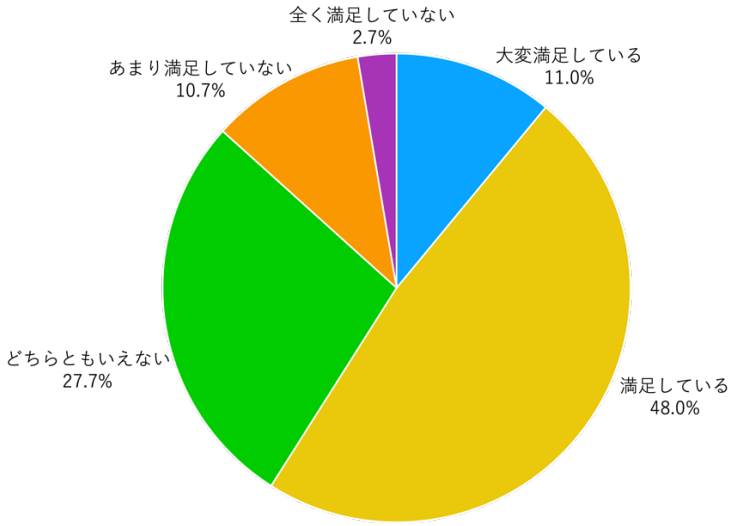
Media@Trellix.com

セキュリティ業務への満足度

・自身の現在の業務全般に対する満足度

セキュリティ担当者の 11%は「大変満足している」、48%は「満足している」と回答し、過半数以上が業務に対してポジティブな評価をしていることがうかがえます。（図 1）

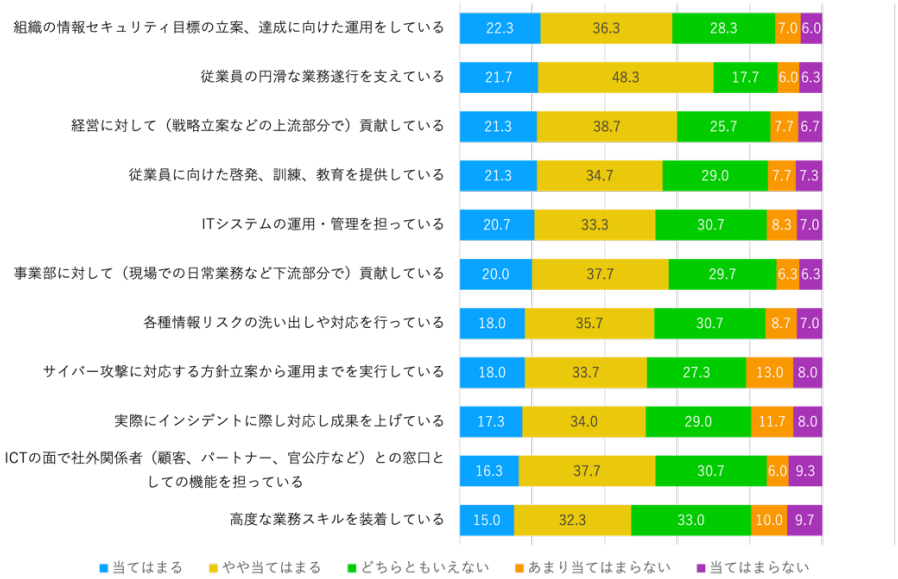
図 1. 業務全般に対する満足度（単一回答,n=300）



・企業や団体のセキュリティを担う業務の価値

セキュリティ担当者が思う自身の仕事の価値としては、「従業員の円滑な業務遂行を支えている」「経営に対して（戦略立案などの上流部分で）貢献している」「組織の情報セキュリティ目標の立案、達成に向けた運用をしている」が上位 3 項目に挙げられました。（図 2）

図 2. 企業や団体のセキュリティを担う業務の価値（単一回答,n=300）



Media@Trellix.com

セキュリティ業務におけるフラストレーション

・セキュリティ担当者の業務におけるフラストレーションの有無

セキュリティ担当者のうちフラストレーションを感じたことが「よくある」「時々ある」「ごくまれにある」の合計は 85.3%（図 3）で、頻度はさまざまなものの、ほとんどのセキュリティ担当者は業務中に疲労感や嫌悪感を感じていることが明らかになりました。一方で、経営層の担当者のフラストレーションに対する認識は同 3 つの項目について合計 68.0%（図 4）と、経営層とセキュリティ担当者に 17.3 ポイントの認識ギャップがあり、経営層の認識以上に現場がフラストレーションを感じていることがわかりました。

図 3. セキュリティ担当者特有の業務の影響で疲労感や嫌悪感、フラストレーションを感じた経験（単一回答,n=300）

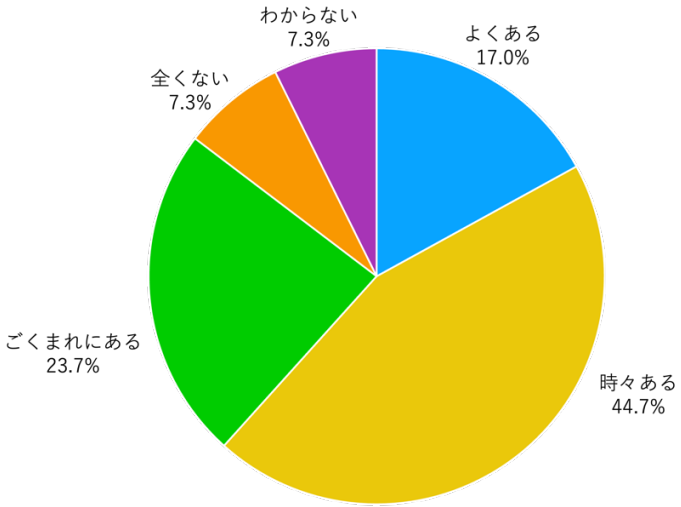
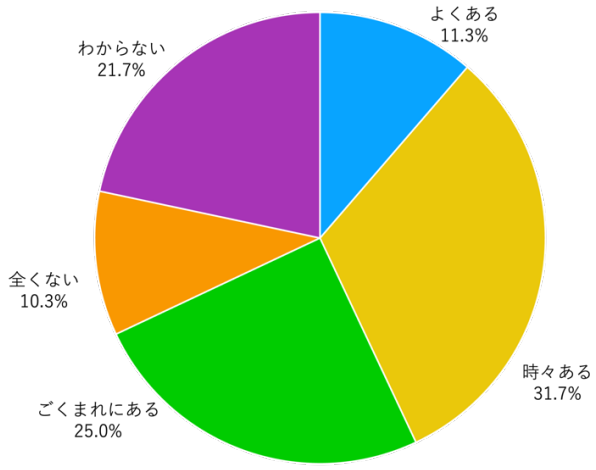


図 4. 自身の企業・団体のセキュリティ担当者の業務中の疲労感や嫌悪感、フラストレーションの経験の認識（単一回答, n=300）



・フラストレーションを感じた具体的な場面

具体的にセキュリティ担当者がフラストレーションを感じた場面は、「スキル向上に対するサポート不足」「組織的にも社会的にも意義のある業務の割に十分に評価されない」「関係部門の協力が得られない」が上位 3 項目で、セキュリティ担当者、経営層とも、同様の結果となりました。（図 5）（図 6）

上位に、第三者からの評価や理解・協力が挙げられていることから、「認められていない」と感じることがフラストレーションに繋がっている可能性がうかがえます。また、「従業員のプライバシーなどセンシティブな情報の取り扱い」に過半数のセキュリティ担当者がフラストレーションを感じるなど、セキュリティ業務ならではの避けることが難しい課題があることが明らかになりました。（図 5）
この質問については、2022 年 6 月に米国で発表した調査結果でも、「スキル向上に対する限定的なサポート」「社会貢献していることへの認識不足」が上位に挙げられており、世界共通で同様の場面でフラストレーションを感じることが多いことがうかがえます。

図 5. 疲労感や嫌悪感、フラストレーションを感じた具体的な場面（それぞれひとつずつ回答,n=300）

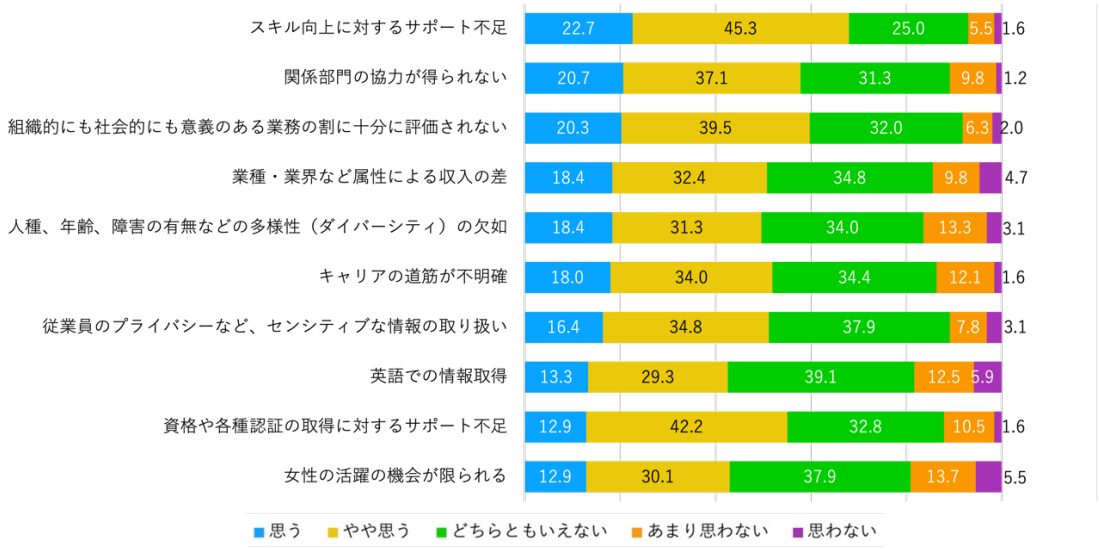
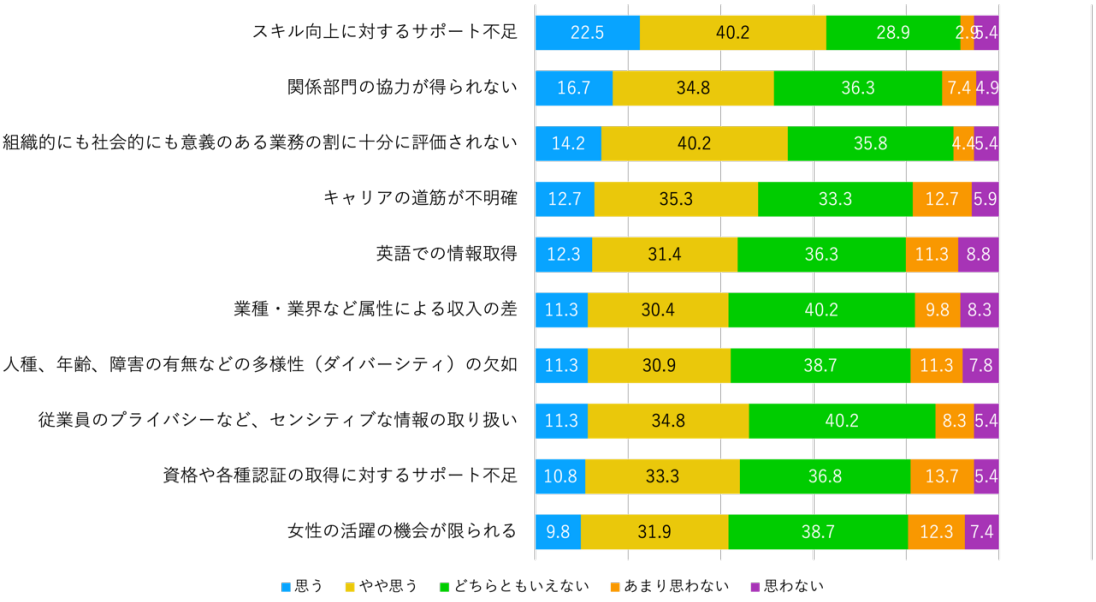


図 6. 経営層から見た現場が疲労感や嫌悪感、フラストレーションを感じると思う場面（単一回答,n=300）



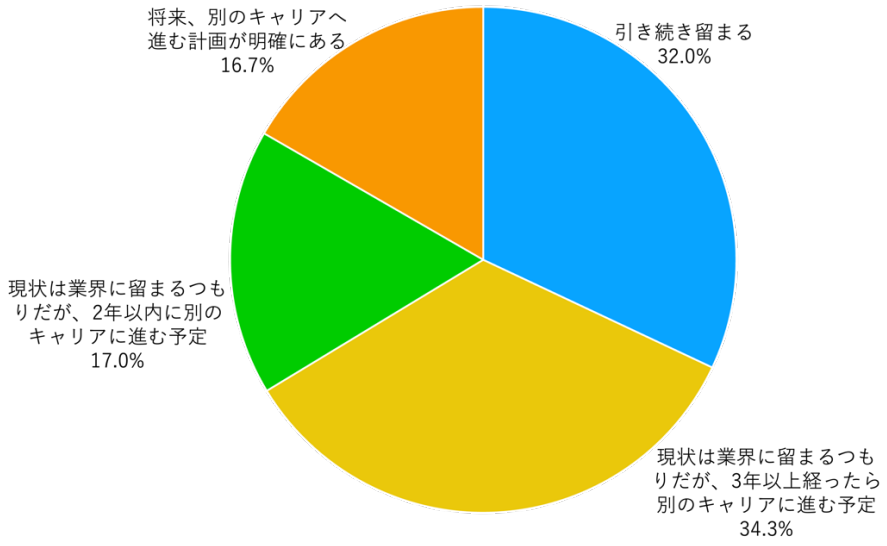
Media@Trellix.com

・サイバーセキュリティ業界に留まる意向

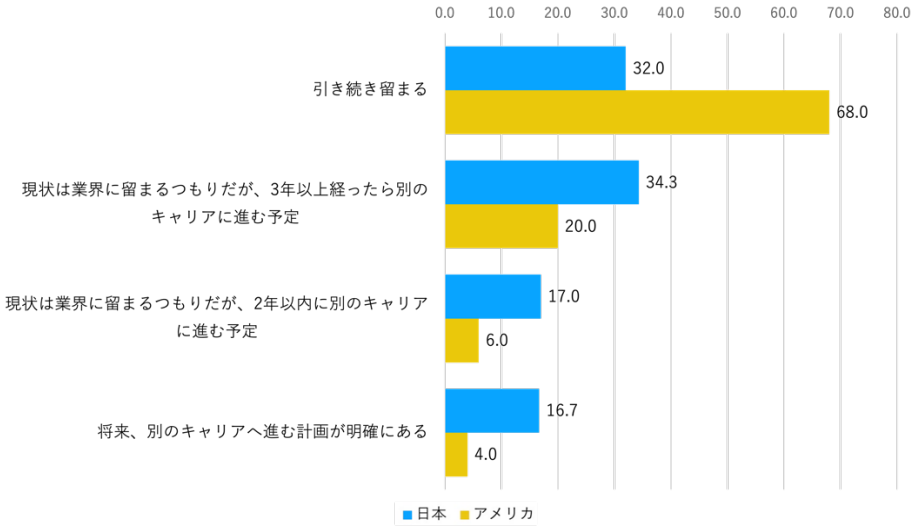
セキュリティ担当者の 32%が業界に引き続き留まると回答した一方で、別のキャリアに進むと合計 68%が回答。（図 7）

一方、2022 年 6 月の米国で発表した調査結果では、引き続き留まると回答した方は全体の 68.0%で、日本と大きく異なる結果でした。日本のセキュリティ人材不足を解消するためには、この高い離職傾向に目を向け、対策を講じることが不可欠であり、組織のセキュリティ体制を確保するための機会としても捉えられると考えられます。

図 7.　今後もサイバーセキュリティ業界に留まる意向（単一回答,n=300）



同、日本とグローバル調査の比較



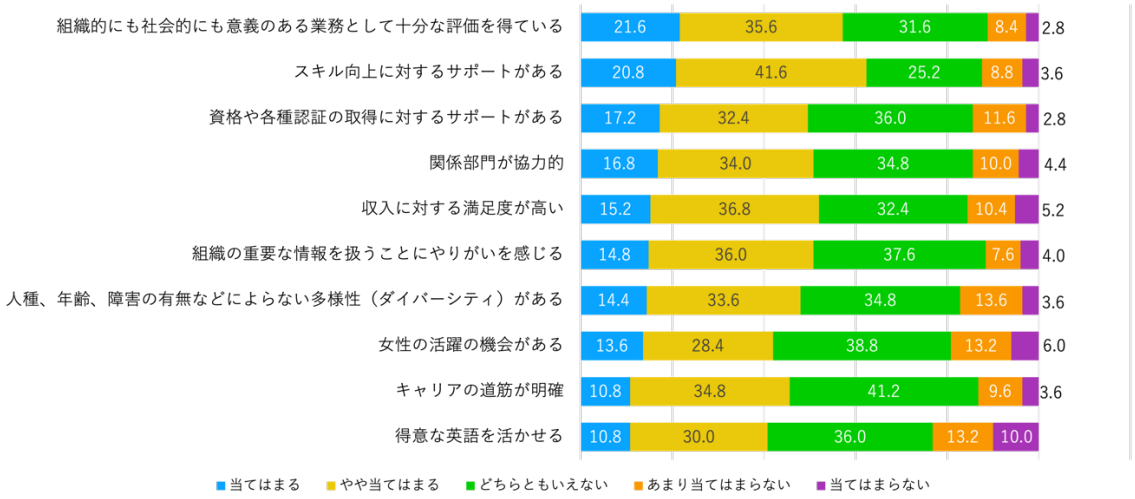
Media@Trellix.com

・サイバーセキュリティ業界に留まる理由

セキュリティ担当者が業界に留まる理由として、「スキル向上に対するサポートがある」「組織的にも社会的にも意義のある業務として十分な評価を得ている」「資格や各種認証の取得に対するサポートがある」が上位 3 項目に挙げられました。（図 8）

また、過半数が「組織の重要な情報を扱うことにやりがいを感じる」と回答し（図 6）、フラストレーションを感じつつも（図 3）、やりがいを持って業務に取り組んでいることがうかがえます。

図 8.　セキュリティ業界に留まる理由（それぞれひとつずつ回答,n=300）

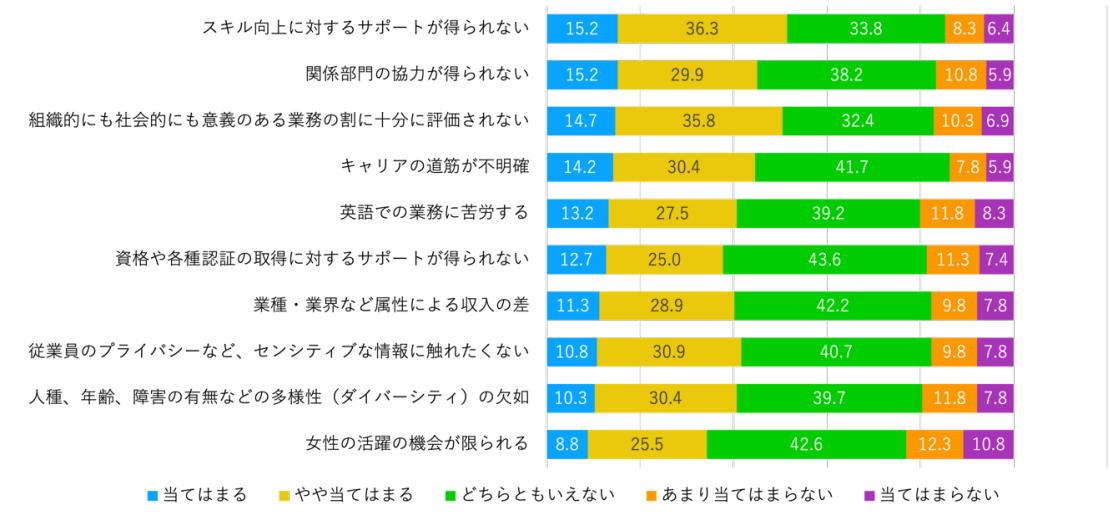


・サイバーセキュリティ業界に留まらない理由

一方で、セキュリティ業界に留まらない理由としては、「スキル向上に対するサポートが得られない」「組織的にも社会的にも意義のある業務の割に十分に評価されない」「関係部門の協力が得られない」が上位 3 項目に挙げられ（図 9）、手厚いサポートを受けている担当者と受けていない担当者で、業界に留まる意向が二分することがうかがえます。

また、フラストレーションの要因と合致する（図 3）ことから、担当者のフラストレーションをそのままにしておくと、人材流出に繋がることが明らかになりました。

図 9. 別のキャリアを考える理由 （それぞれひとつずつ回答,n=300）



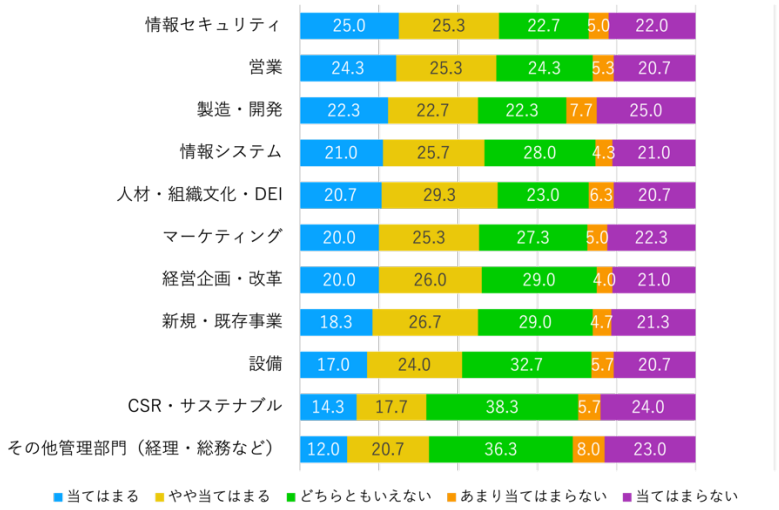
Media@Trellix.com

情報セキュリティと経営について

・経営層が 投資が必要と考える領域

経営層が 投資が必要と考える領域として、「情報セキュリティ」に 25.0%が「当てはまる」と回答し、経営層が最も注目している領域であることが明らかになりました。（図 10）

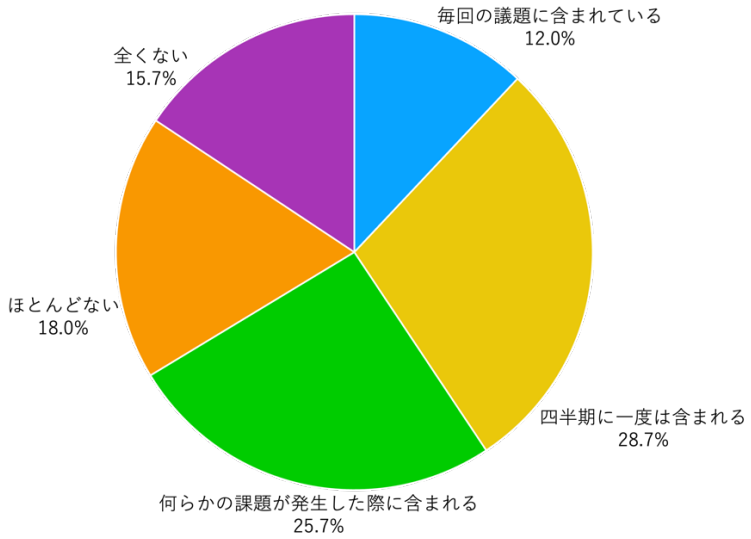
図 10. 投資が必要と考える領域（それぞれひとつずつ,n=300）



・サイバーセキュリティ関連のトピックを経営会議等の議題に含む頻度

経営層の 12.0%が経営会議等の定常的な議題の「毎回の議題に含まれている」、28.7%が「四半期に一度は含まれる」と回答し、合計 40.7%の経営層が定期的にサイバーセキュリティのトピックを扱っていることが明らかになりました。一方で、ほとんどない、全くないと回答した経営層が約 34%となり、管理対象が 500 名を超える企業や団体であっても、未だセキュリティの経営への影響に関する意識が低い組織がこれだけ存在していることが明らかになりました。（図 11）

図 11. サイバーセキュリティ関連のトピックを経営会議等の議題にする頻度（単一回答,n=300）



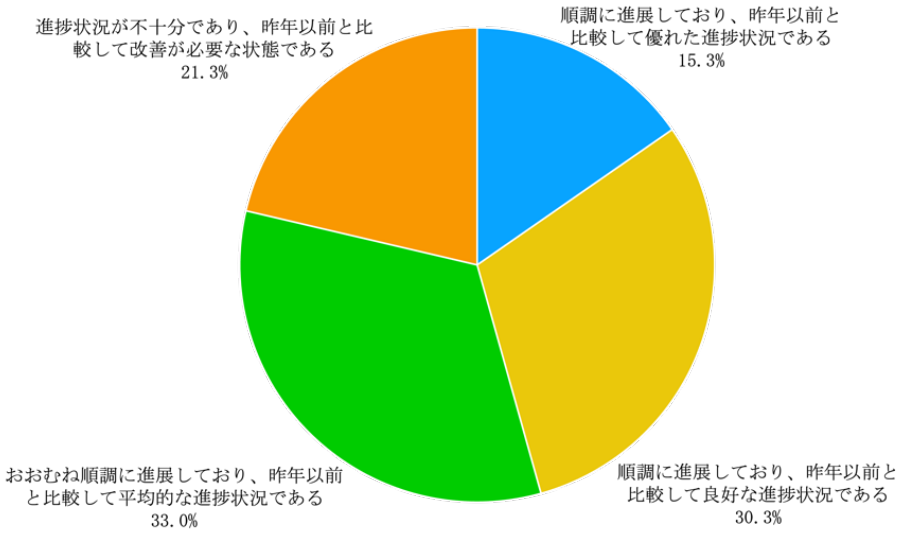
Media@Trellix.com

・今年度の事業の状況

経営層の 15.3%が「順調に進展しており、昨年以前と比較して優れた進捗状況である」、30.3%が「順調に進展しており、昨年以前と比較して良好な進捗状況である」と回答し、45.7%の経営層が昨年以前よりも順調な事業進捗であることが明らかになりました。（図 12）

また、サイバーセキュリティのトピックを「毎回の議題に含まれている」と回答したうちの 72.2%が事業の状況を昨年以前と比較して「優れた」「良好」と回答していることから、サイバーセキュリティを経営課題としてとらえる経営層が所属する組織は事業進捗が良いことがうかがえる結果となりました。

図 12. 企業・団体での今年度の事業の状況 （単一回答,n=300）



まとめ・考察

今回の調査では、セキュリティ担当者の業務を通じて経験するフラストレーションの存在と、今後セキュリティ業界に留まり続ける、事業進捗とセキュリティ対策との関連性などが特にハイライトとなりました。

現在、セキュリティ業界で働く人々の多くはフラストレーションを抱えています。
中でもスキル向上に対するサポートが不足していることや、組織的にも社会的にも意義のある業務の割に評価されていないと感じている方が多く、業界課題となっているセキュリティ人材不足、採用難への影響も考えられ、すでにセキュリティ業界で従事している方々に向けた課題解消が急がれます。また、セキュリティ担当者の今後のキャリアについても、7 割近くがいずれ業界を離れると回答し、今年 6 月に行われたグローバル調査と比べても、依然として離職意志が高い傾向にあります。
しかし、結果について悲観するばかりではありません。それはセキュリティ担当者の約 6 割が自身の職務内容について満足していると回答し、その理由の中でも 7 割の回答者が従業員や組織の円滑な業務遂行を支えていると感じ、経営に対して貢献しているところに仕事の価値を感じている点からも明らかです。この点については経営層のセキュリティ担当者への評価回答からも同様の認識を持っていることがわかります。
つまり、セキュリティ担当者は情熱を持って目の前の仕事に取り組み、組織や社会に対して貢献している実感を得ているのです。

こうした中、経営層は情報セキュリティに対する投資が必要だと考えつつも、具体的なアクションとして定期的に経営会議等の議題に上げていると回答したのは 4 割に留まりました。一方、事業進捗が順調で優れた状況である企業は同様の議題を定期的に社内で検討していることもわかりました。このことから、特に経営層において、自社のセキュリティについて、全社的な取り組み、さらに言えば経営課題として認識し、本調査で明らかになったような課題への対策や担当者へのケアを含む、包括的なサポートを実施することが今後さらに重要であり、そのような対応を進めることがさまざまなポジティブな効果をもたらす「機会」になると考えられます。

今回の調査結果について、サイバーセキュリティの人材育成に長く携わられ、その動向について研究されており、多くの知見を有する奈良先端科学技術大学院大学 サイバーレジリエンス構成学研究室 門林 雄基 教授は、次のように述べています。「今回の調査結果は、主にパーセンテージで示されていますが、レポート後半に示された結果からもみてとれるように、サイバーセキュリティへの取り組みが進んでいる企業とそうでない企業には大きな格差があります。このようなセキュリティ取り組み格差がセキュリティ専門家の離職率や、ひいては事業の成否にまで影響を与えているのではないでしょうか。一般的に、売り上げ上位の営業成績は評価をして気前よくインセンティブをはずむ一方で、企業の守護神たるセキュリティ専門家には十分な評価やサポートができていません。今回明らかになった厳しい数字は、経営層や管理職に今すぐ対処すべき、と伝えているのではないでしょうか。」

Trellix では、こうした社会的意義や組織への貢献といった実感を持ちながら職務遂行するセキュリティ担当者をソウルフルワーカーと呼び、これまで過小評価されてきたコミュニティへのインクルージョンを促進するために設計された、情熱的な仕事（Soulful Work）に対するプログラムに多数取り組んでいます。
具体的な施策のひとつとして 2022 年 9 月、サイバーセキュリティ業界に入ろうと考える人材へ専門家向けの業界知識を提供し、採用情報を掲載する SoulfulWork.co を公開しました。
そのほかにも、サイバーセキュリティの仕事を、有意義でやりがいのあるキャリアパスとして奨励したり、採用するための包括的な指導・教育プログラムであるアクセラレータープログラムを用意したり、学生向けには、実践的なトレーニングや専門的な能力開発の機会、スキルアップをサポートする無料の e ラーニングを提供しています。また、セキュリティ業界において意欲的で影響力のある女性リーダーを集めて、多様性を阻む課題について議論を進める Xpand Women in Cyber Changemaker Forum なども行いました。

【調査概要】

調査名	業務における満足度とフラストレーション
調査対象	日本国内に在住する企業経営者、企業に勤務する情報システム担当者、一般従業員など 22 歳以上の男女 600 人。
調査方法	インターネットによるアンケート調査
調査期間	2022 年 9 月 30 日（金）から 10 月 4 日（火）
調査主体	Trellix（株式会社アスマークに委託）

Trellix について
Trellix は、サイバーセキュリティの未来を再定義するグローバル企業です。オープンかつネイティブな Trellix の XDR（Extended Detection and Response）プラットフォームは、現在最も高度な脅威に直面するお客様が業務の保護や回復に確信を持って対応するための支えとなります。Trellix のセキュリティ専門家は、広範なパートナーエコシステムとともに、データサイエンスと自動化によりテクノロジーイノベーションを加速させ、4 万を超える企業や政府機関のお客様の力となっています。

Media@Trellix.com

参考情報
・Trellix ブログ：Trellix、サイバー人材不足に関する調査結果を発表（2022 年 6 月）

別紙：その他の調査結果

図 13.【セキュリティ担当者】サイバーセキュリティに業務として取り組むことになったきっかけ（単一回答,n=300）

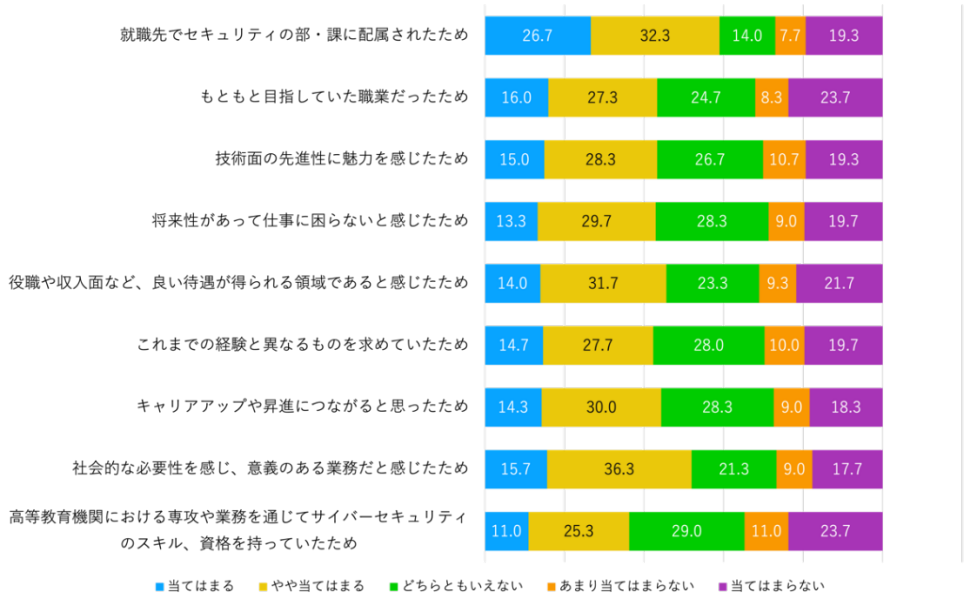
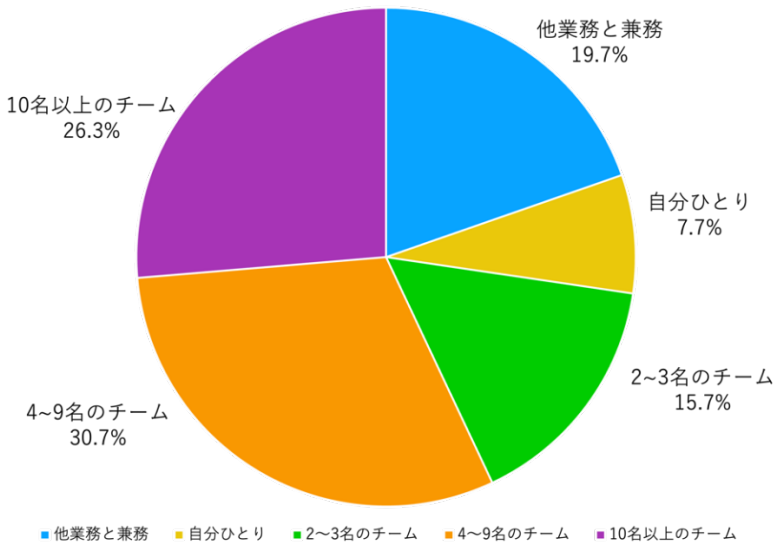


図 14.【セキュリティ担当者】サイバーセキュリティに業務を行うチーム体制（単一回答,n=300）



Media@Trellix.com

図 15.【セキュリティ担当者】サイバーセキュリティに業務に従事している年数（単一回答,n=300）

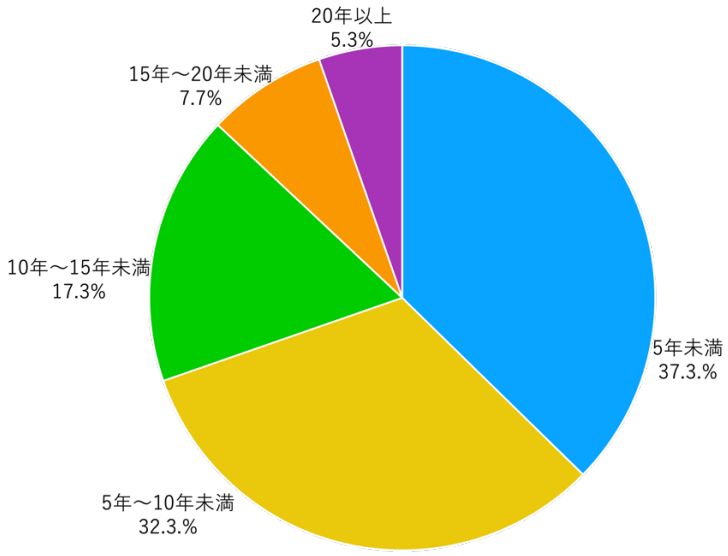


図 16.【セキュリティ担当者】フラストレーションが与える影響（単一回答,n=300）

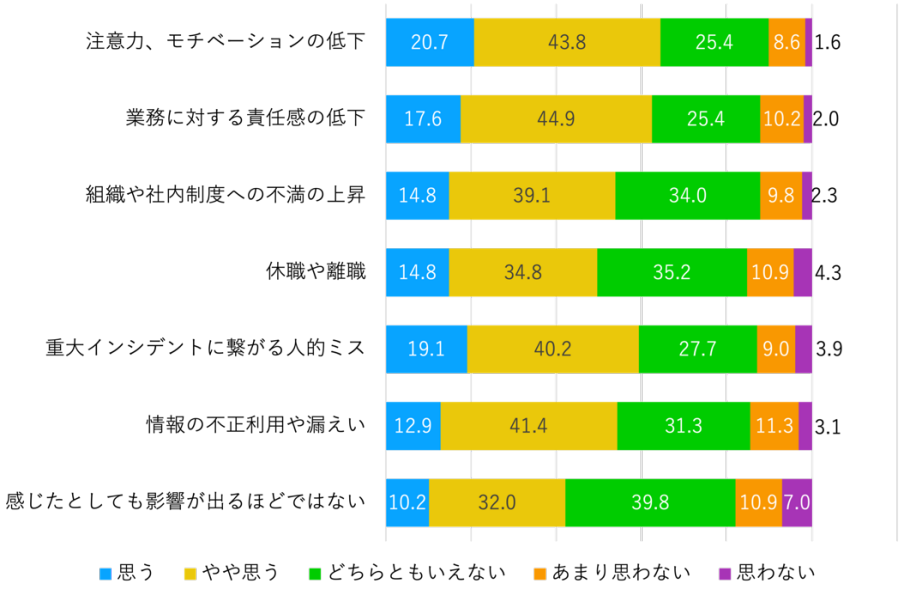


図 17.【セキュリティ担当者】今年度の事業の状況（単一回答,n=300）

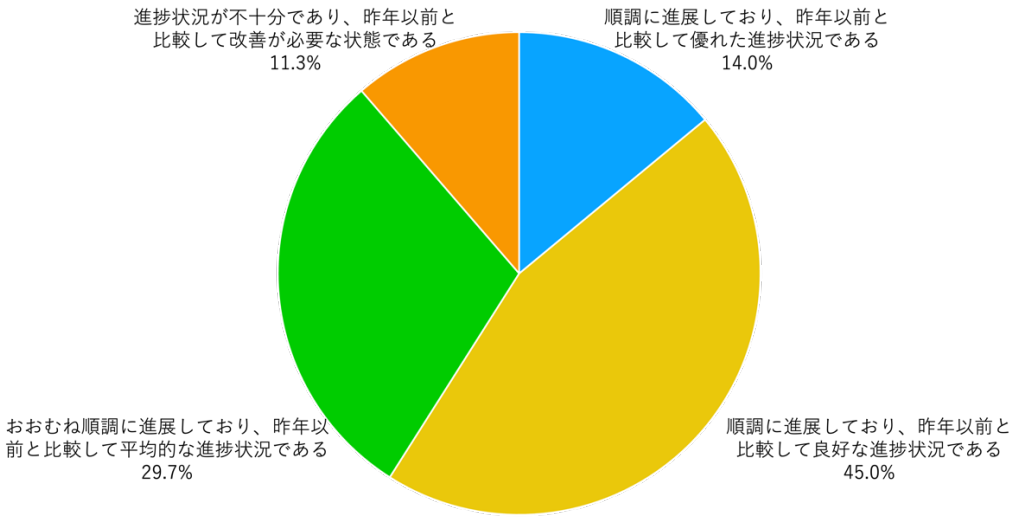


図 18.【経営層】サイバーセキュリティの需要や必要性（単一回答,n=300）

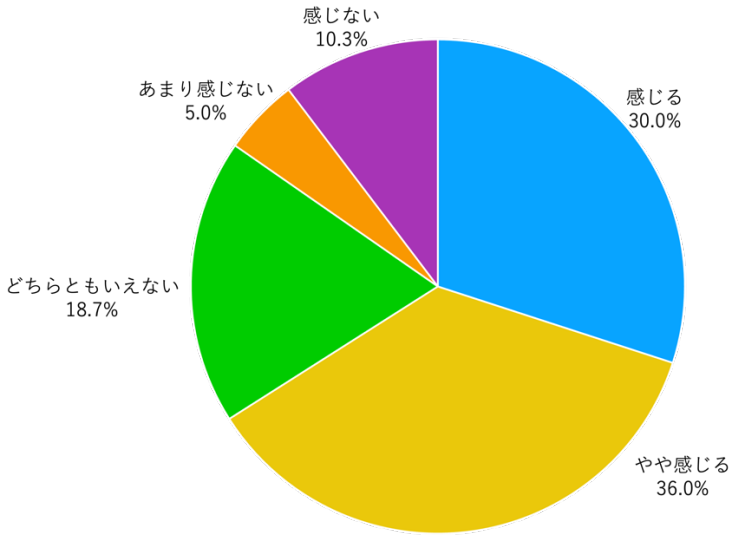


図 19.【経営層】セキュリティ担当者の業務に関する認識（単一回答,n=300）

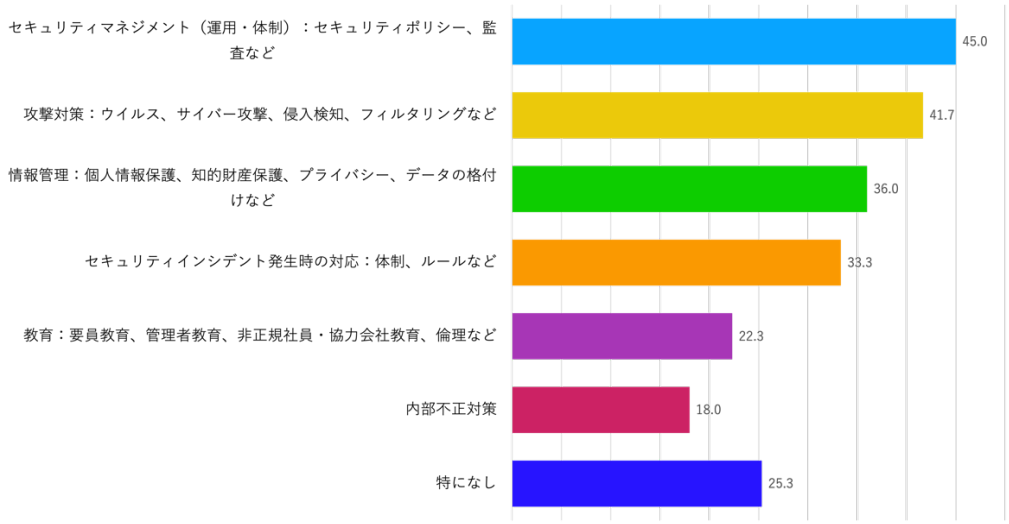
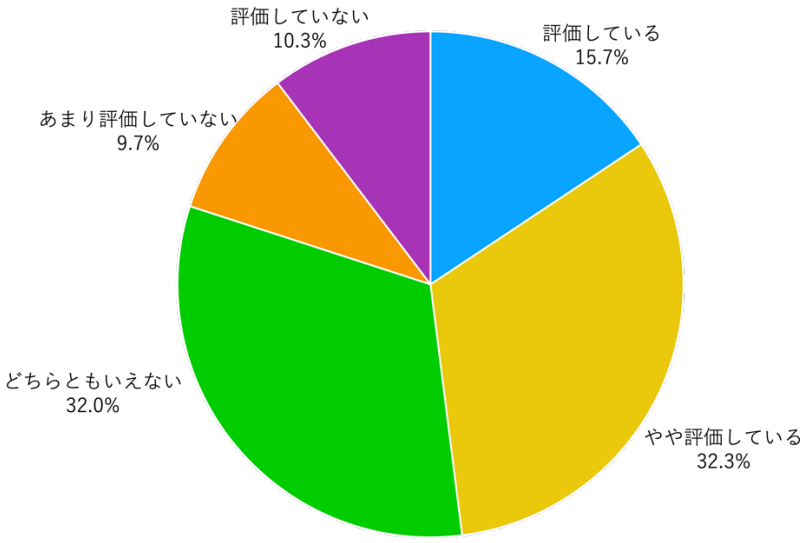


図 20.【経営層】セキュリティ担当者への評価（単一回答,n=300）



Media@Trellix.com

図 21.【経営層】セキュリティ担当者を評価している理由（単一回答,n=300）

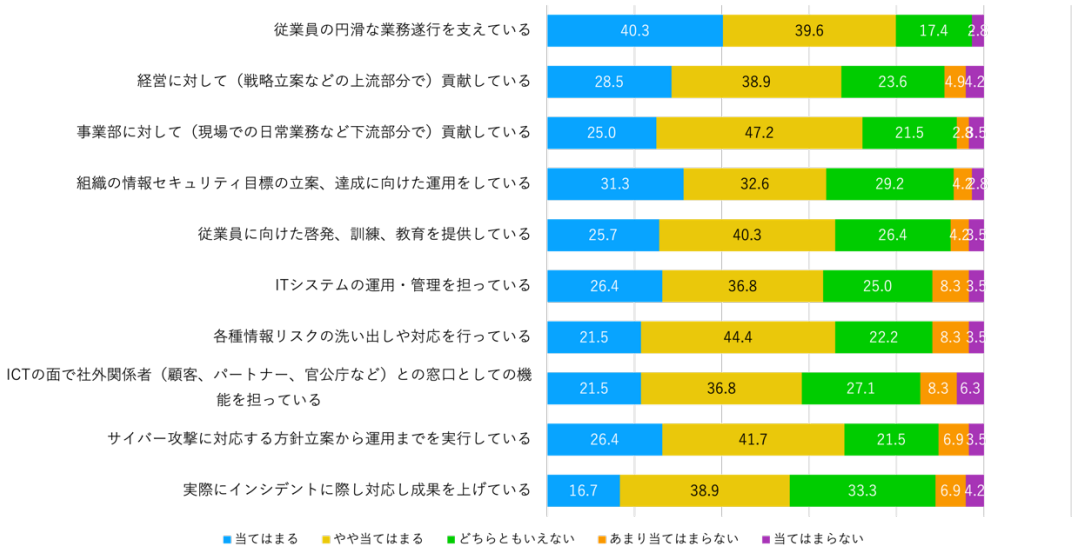
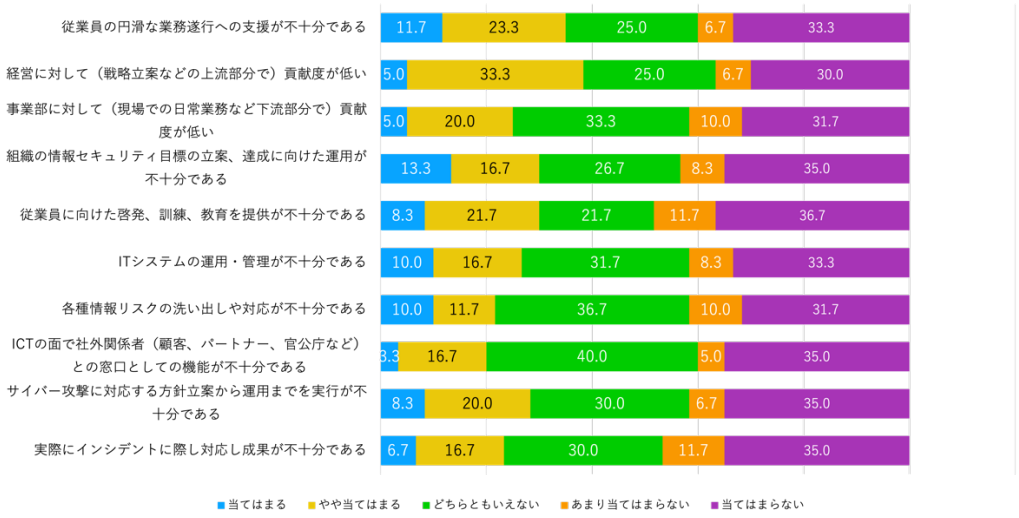


図 22.【経営層】セキュリティ担当者を評価していない理由（単一回答,n=300）



Media@Trellix.com

図 23.【経営層】セキュリティ担当者のフラストレーションの改善方法（単一回答,n=300）

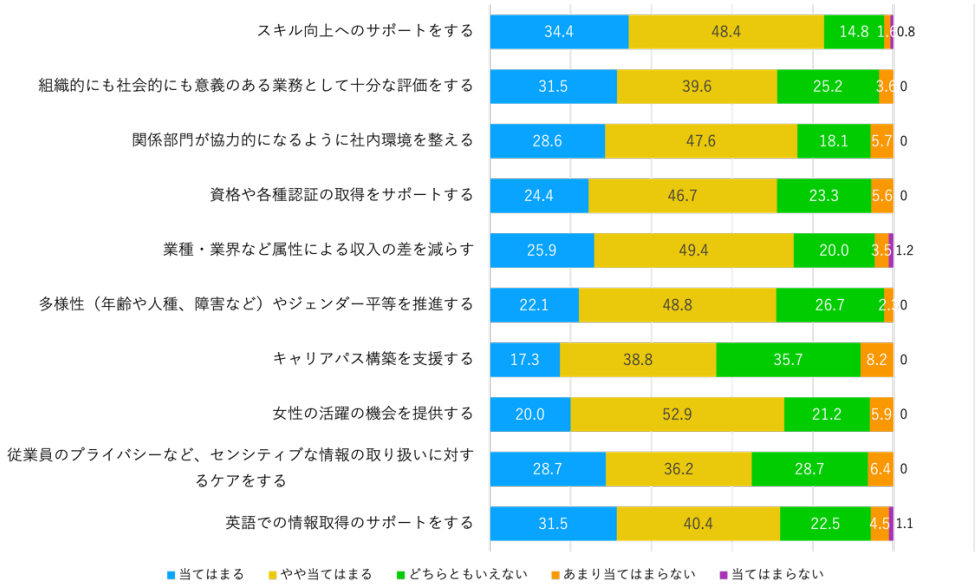
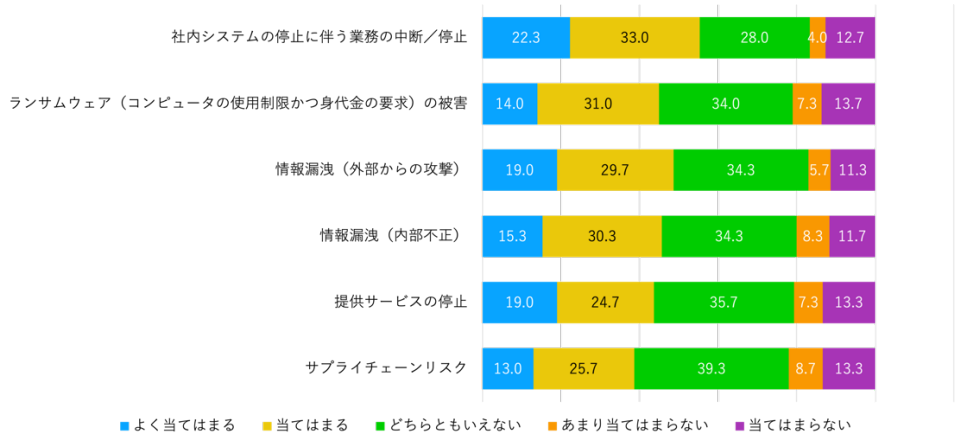


図 24.【経営層】サイバーセキュリティ関連で恐れている被害（単一回答,n=300）



＜本情報のお問い合わせ＞
Trellix（McAfee Enterprise）
広報担当 戸田
Tel: 070-2680-0731
hiromi.toda@trellix.com

Trellix（McAfee Enterprise）広報担当
LaCreta 担当：野澤 / 近藤
Tel: 050-4560-2425
trellixjpn@lacreta.jp