報道関係各位

2022 年 5 月 24 日

Trellix（トレリックス）、経営者とセキュリティ担当者の「情報セキュリティ」に関する意識調査結果（2022 年 5 月版）を発表

～情報漏洩は 68.8%、ランサムウェア攻撃は 45.5%が直近 1 年に経験～

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、Trellix（トレリックス）は、日本国内の企業・団体の経営層、また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（いずれも従業員数 500 人を超える組織）を対象に、組織の情報セキュリティに関する調査を、Web アンケート方式で実施（2022 年 4 月）し、調査結果を発表しました。

ニュースハイライト

- インシデントの実態：過去 1 年のクラウド上のデータ侵害（情報漏洩）は 68.8%が経験。侵害内容は「標的型攻撃」が最多。ランサムウェア攻撃は 45.5%が経験したと回答
- 情報セキュリティ予算：今年度（2022 年度）は昨年度対比で 3 割強の組織で増額。増加背景は「DX の推進」がすべての従業員帯でそれぞれ最多
- 情報セキュリティ運用課題：「社内の人員不足、専門知識や経験の不足」「セキュリティツールの使い分けの煩雑性」「システム全体像の複雑性」が上位 3 位
- 1 年以内に自組織で発生すると想定される脅威：「メール詐欺」がトップ。1 万人以上の組織では「ランサムウェア」「サイバーによる物理攻撃」が突出して高い

今回の調査を通じて、国内企業・団体のサイバーセキュリティに関する実状や、情報漏洩やランサムウェア攻撃といったサイバーインシデントの実態、セキュリティ予算の状況等を明らかにしました。また、今後起こりうる各種脅威に対する見立てや、具体的な対策といった意識実態についても言及しています。

顕著な結果として、直近 1 年以内に被害を受けたサイバーインシデントとして、情報漏洩は 68.8%、ランサムウェア攻撃は 45.5%と回答しており、多くの企業・団体が実際に何等かの対応を迫られたことがわかりました。もはやインシデントが他人事ではないことを物語っていると考えられます。その他、セキュリティ予算増加の背景に「デジタルトランスフォーメーション（DX）の推進」との回答が得られたこと、特に大企業でのランサムウェアへの備えへの意識の高まりなどは、昨年から今年にかけて国内外で頻発する規模の大きなサイバー攻撃による被害状況を通じ、より対策への切迫度が高まっていることの証左であると考えられます。なお、集計にあたっては従業員数 500 名以上の組織を対象とし、また、2021 年 11 月に実施した調査の結果を一部引用し比較しています（以降、「前回調査」と表記）。

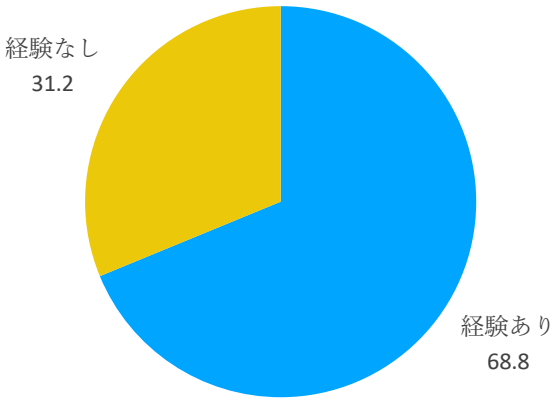
サイバーセキュリティ インシデントの発生状況

- **クラウド上のデータ侵害（情報漏洩）の最新実態**

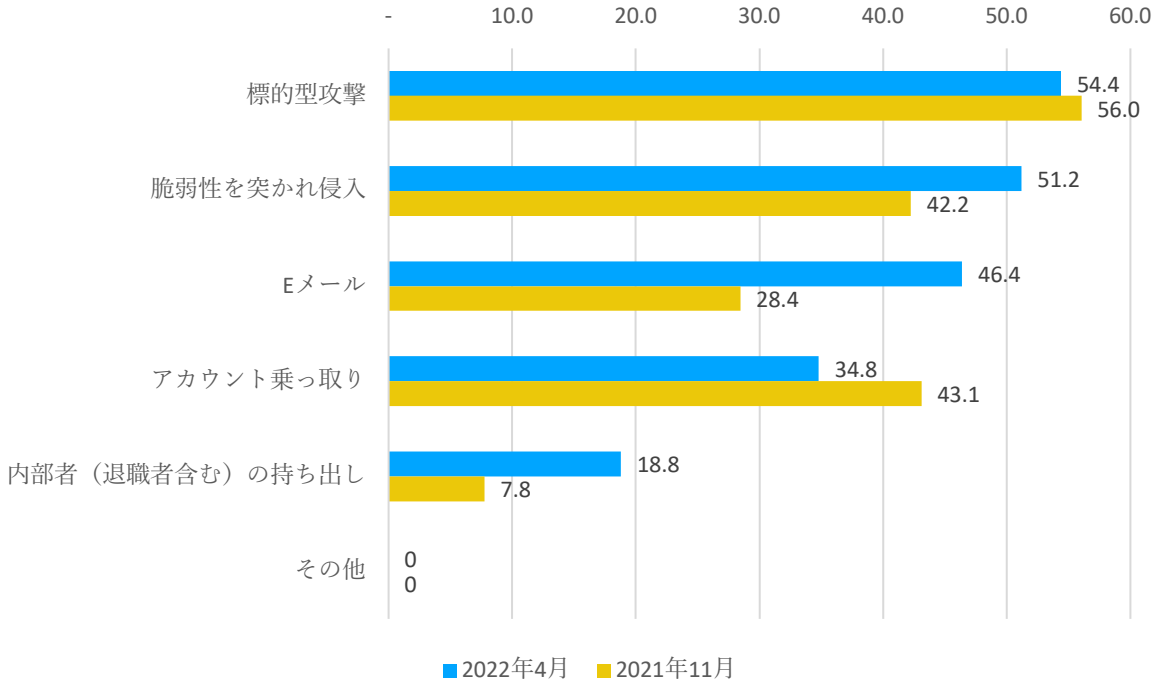
過去 1 年以内のインシデント、特にクラウド上のデータ侵害（情報漏洩）では、68.8%の組織が何らかのインシデントを経験していることがわかりました（図 1）。

データ侵害の原因については、「標的型攻撃（54.4%）」が最多。前回調査対比で増加が最も大きかったのは「E メール」で 18.0 ポイント増、「内部者（退職者含む）の持ち出し」が 11.0 ポイント、「脆弱性を突かれ侵入」が 9.0 ポイントとそれぞれ増加しました（図 2）。

【図 1　過去 1 年以内、クラウド上の格納データへの侵害（情報漏洩）経験有無（単一回答,n=378）】



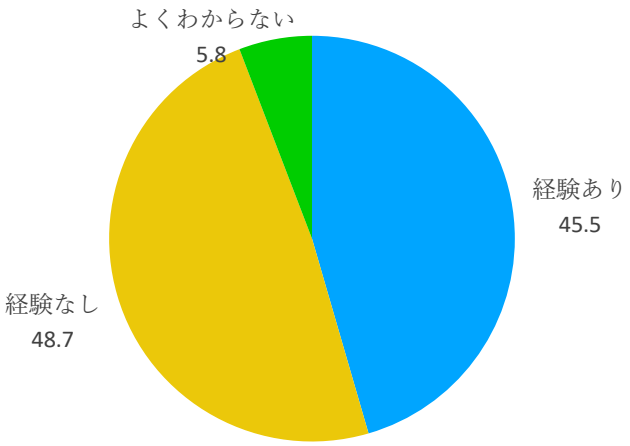
【図 2　過去 1 年以内、クラウド上格納データへの侵害（情報漏洩）の原因（複数回答,n=378）】



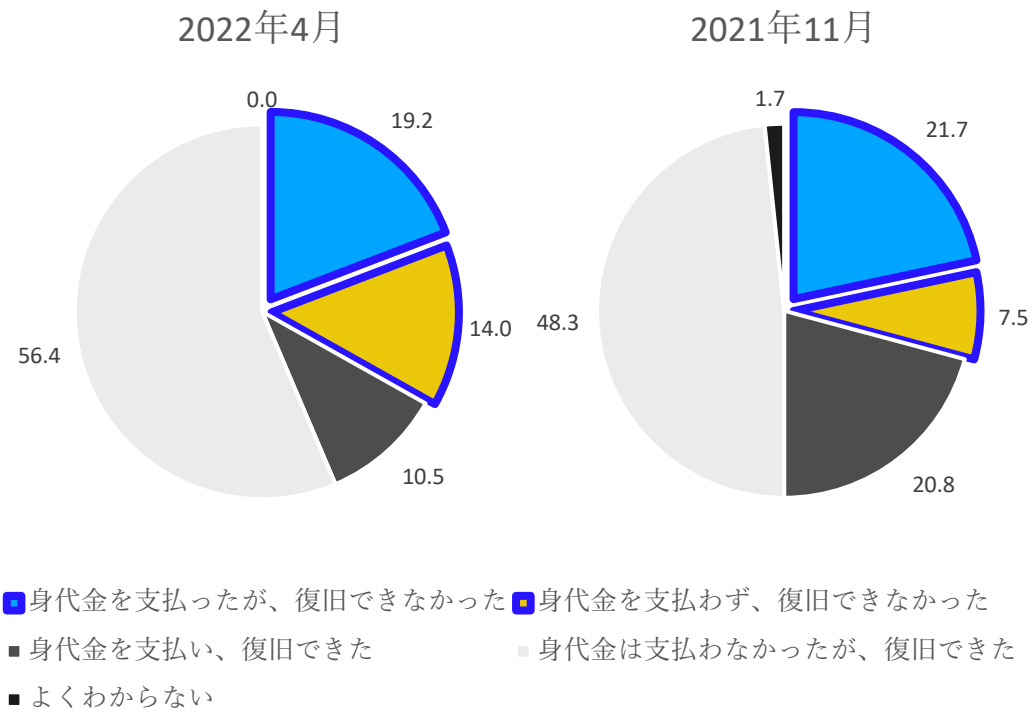
- **ランサムウェア攻撃の最新実態**

過去 1 年以内のランサムウェア攻撃においては、45.5%の組織が経験していると回答（図 3）、攻撃を受けた後の対応としては、身代金を「支払った」と 29.7%が回答、前回調査比 12.8 ポイント減少となり、身代金を支払わないようにという啓発が多少なりとも効奏していることが考えられます。しかし、「身代金は支払わなかったが、復旧できた」との回答が、前回比で 8.1 ポイント増加したものの、身代金の支払い如何によらず結果的に「復旧できなかった」が前回対比で 4.0 ポイント増の結果となり（図 4）、被害を受ける企業の拡大が見られ、より一層のセキュリティ対策の重要性の認識及び実際の運用が必要であることが伺えます。

【図 3　過去 1 年以内のランサムウェア攻撃の経験有無（単一回答,n=378）】



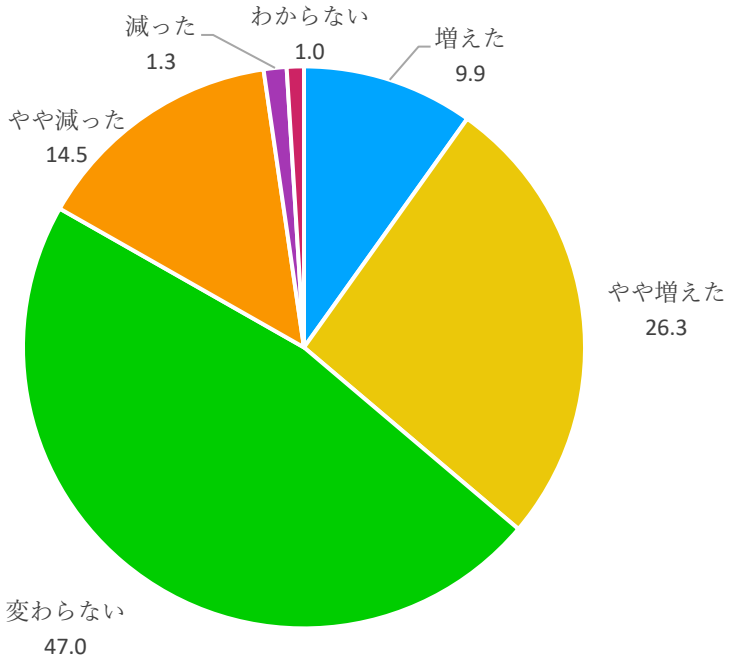
【図 4　過去 1 年以内のランサムウェア被攻撃後の対応　今回／前回調査（単一回答,n=378）】



セキュリティ関連予算の前年度との比較

今年度（2022 年度）予算額の前年度（2021 年度）対比の変化について、「増えた」「やや増えた」は計 37.2%、「減った」「やや減った」が計 15.8%、「変わらない」が 47.0%となり（図 5）、前年同等以上の投資を予定する企業・団体が 8 割以上と、未だ景気が低迷する中、セキュリティに対する投資への関心の高さを感じられる結果となりました。

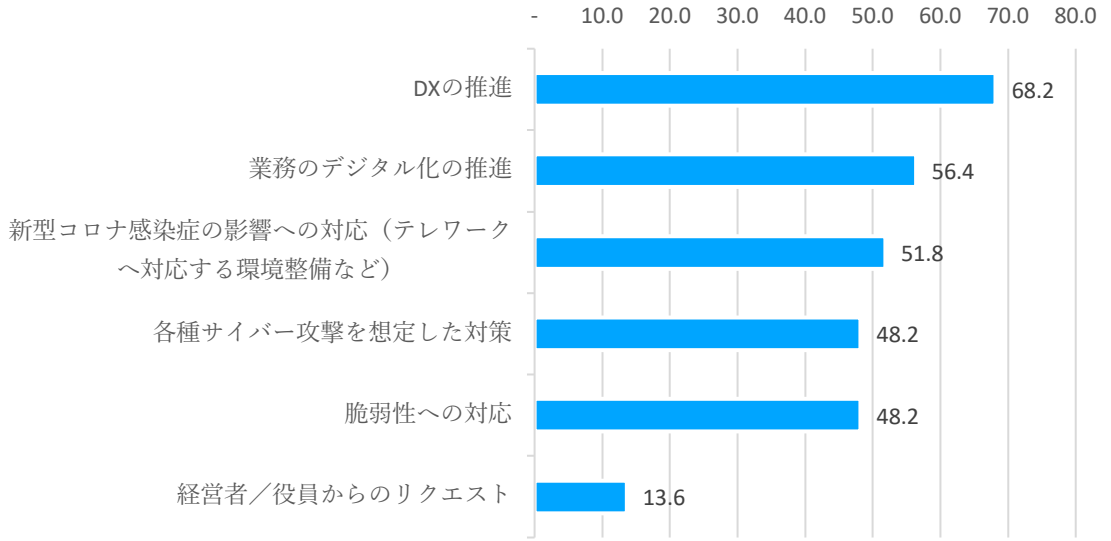
【図 5　2022 年度 セキュリティ対策関連予算額の前年度変化（単一回答,n=304）】



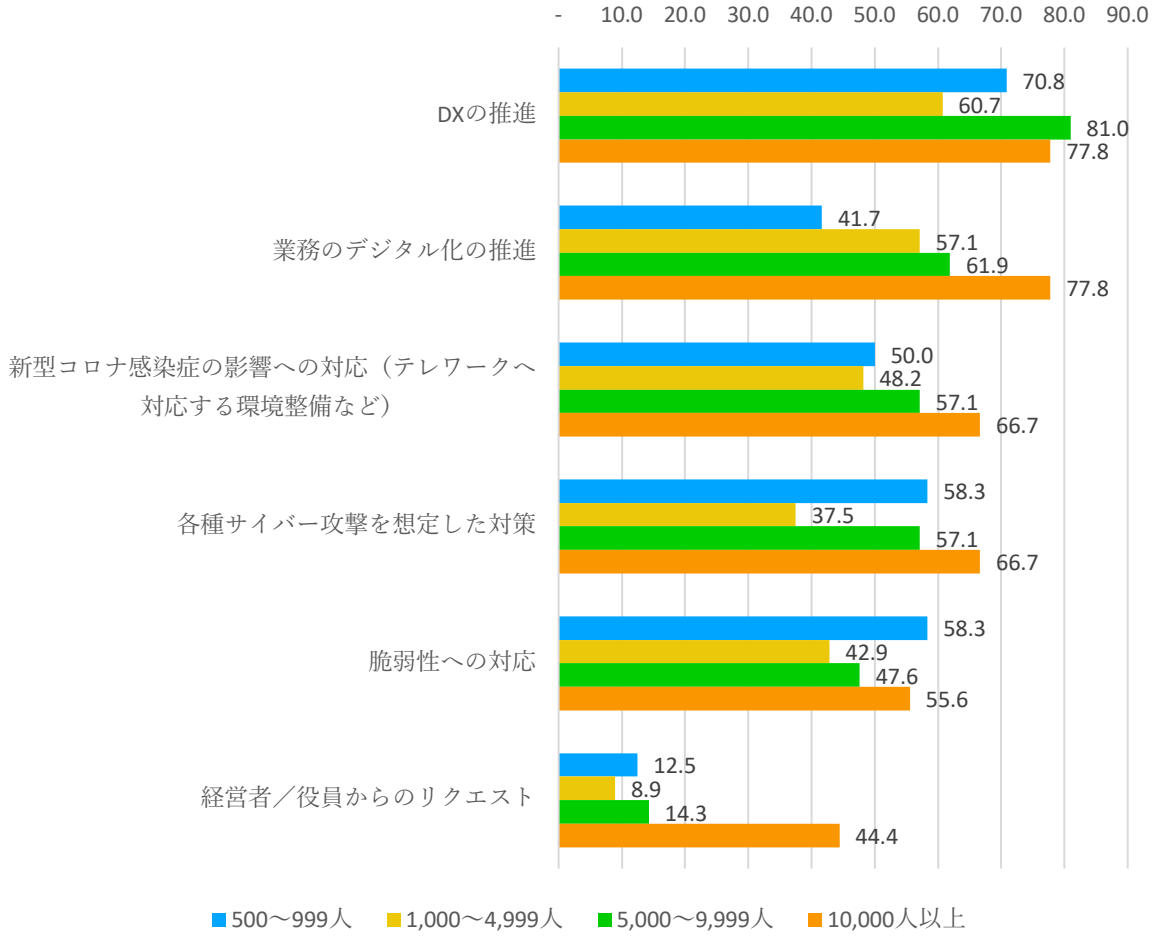
「増えた」「やや増えた」とする背景や理由については、「DX の推進」が 62.8%で最多となり、事業のデジタル化が続き（図 6）、組織規模別でみた場合も「DX」は最多となりました（図 7）。DX は新型コロナ禍を通し、直近数年のもっとも大きなビジネストレンドとなりましたが、今回の結果から DX や業務のデジタル化を推進する中で、セキュリティ対策の重要性が、多くの企業・団体で広まりつつあることを示していると考えられます。

また、組織規模別の特徴として、1 万人以上の組織で各選択肢に対し、軒並み高い回答が得られました。特に「経営者・役員からのリクエスト」が顕著であり、大企業の経営層にセキュリティを管轄する役割が増えていることやセキュリティ対策の重要性の認識の増大がうかがえる結果となりました。昨今の報道状況や実際にサイバーインシデントが増加傾向にある中、社会的インパクトや所有する資産の大きな企業・団体にとって、より優先課題とされている状況がうかがえます。

【図 6　昨年度（2021 年度）対比の予算増加背景（複数回答,n=110）】



【図 7　組織規模別　昨年度（2021 年度）対比の予算増加背景（複数回答,n=110）】

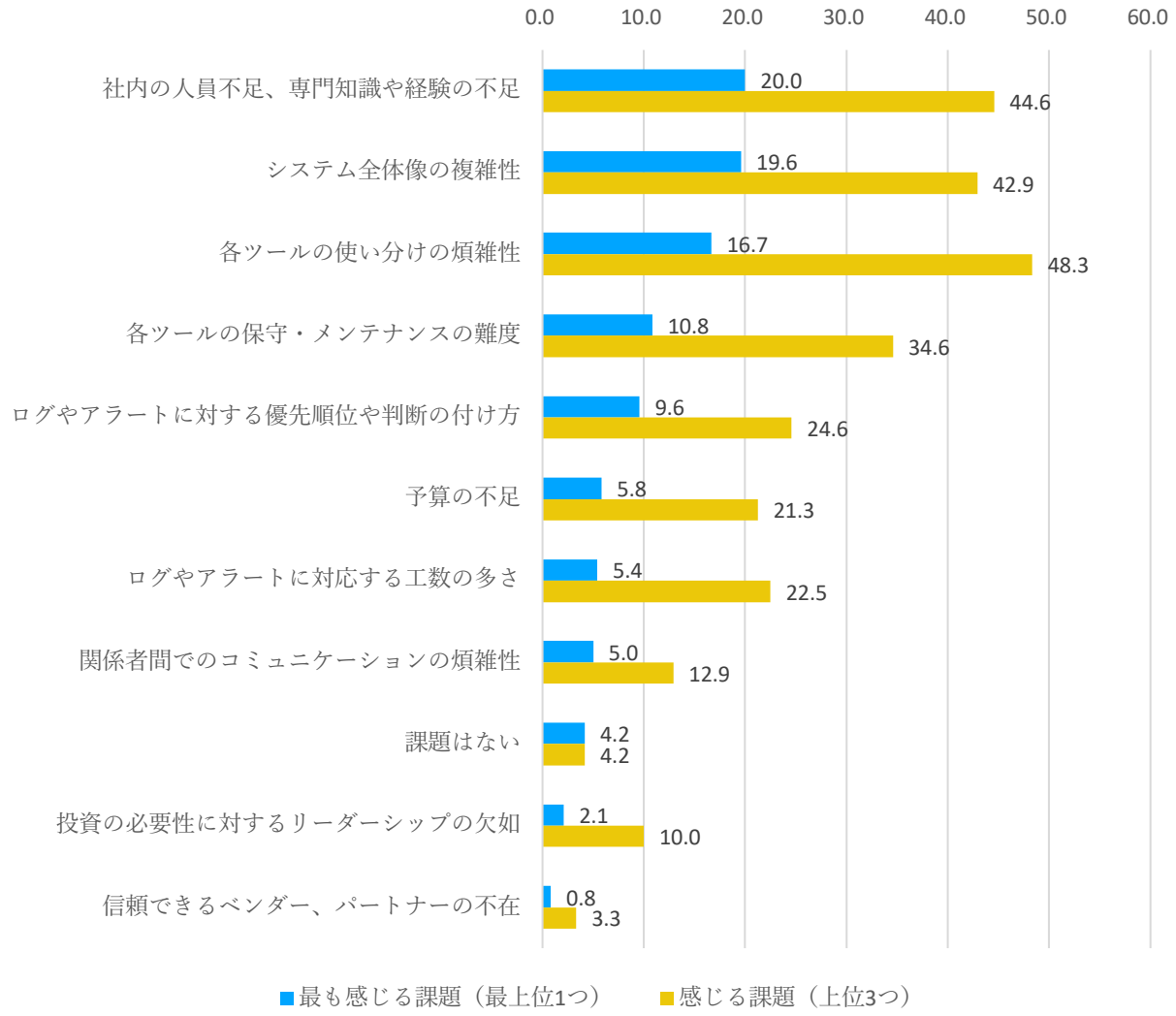


セキュリティ運用の課題

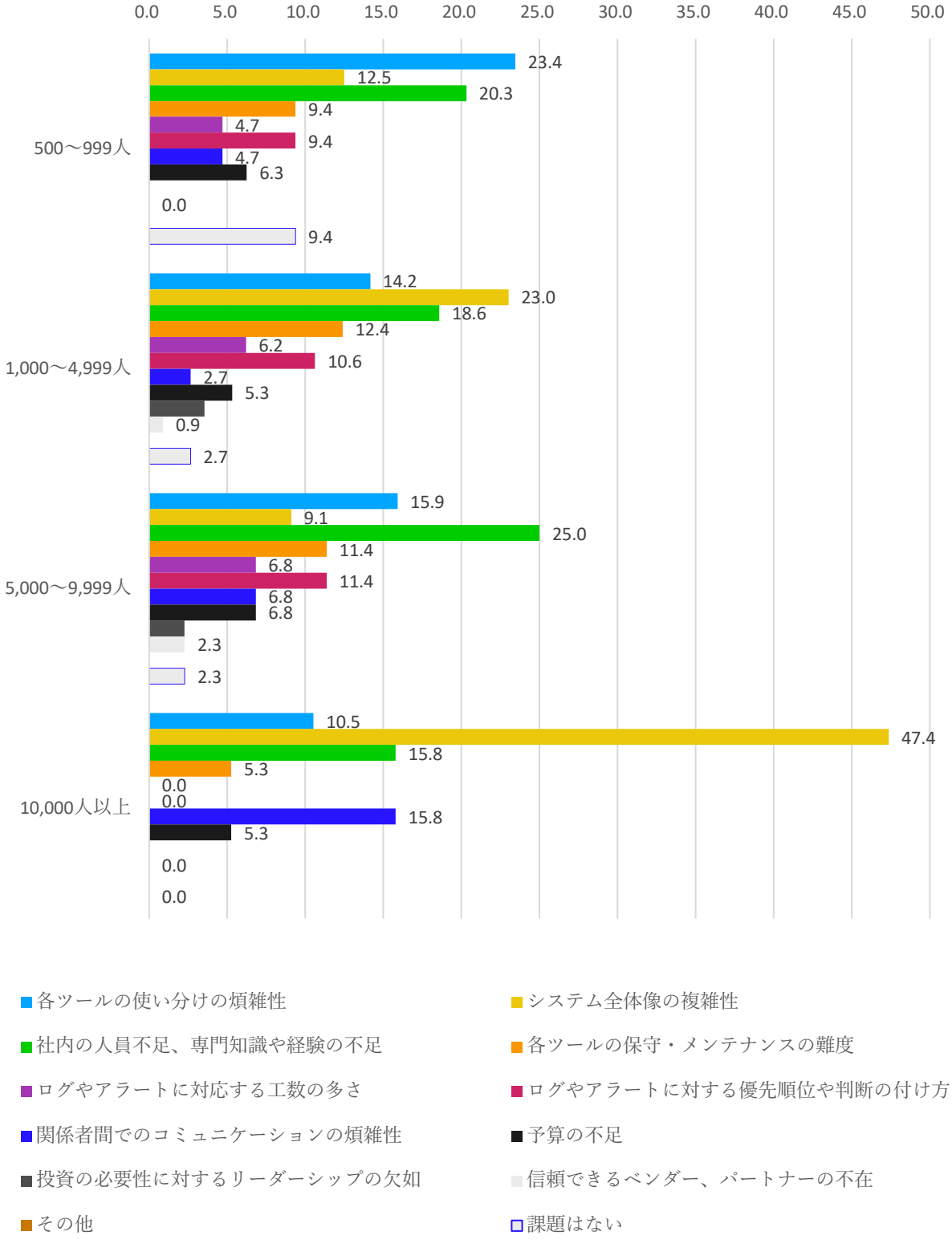
運用上の課題として、「各ツールの使い分けの煩雑性（複数回答 48.3%／単一回答 16.7%）」「社内の人員不足、専門知識や経験の不足（複数回答 44.6%／単一回答 20.0%）」「システム全体像の複雑性（複数回答 42.9%／単一回答 19.6%）」と、複数回答・単一回答いずれも上位 3 位は同十悔過となり（図 8）、共通の課題として明らかと言える結果となりました。

組織規模別でも、この傾向に変わりはないものの、特徴的な人数帯別のポイントとしては、1 万人以上の組織で「システム全体像の複雑性（47.4%）」が突出して多く、他の人数帯も 500～999 人と 5,000～9,999 人では「使い分けの煩雑性」「人員、知識、経験不足」が相対的に高く、1,000～4,999 人では「システムの複雑性」「人員、知識、経験不足」が同様に高い結果となりました。大組織ほど最新のソリューションを早期に導入し、多重防御で脅威に備えることが可能ですが、パッチワーク的にシステムの追加がなされてきたことで、結果として運用負荷が増大している様子が見えます。また、日本のみならず世界的に、サイバーセキュリティ人材が不足していますが、今回の調査からも、そうした人材の不足、知識や経験の不足、といった状況が明らかになりました。

【図 8　情報セキュリティ運用上の課題（上位 3 つまで複数回答／単一回答,n=240）】



【図 9　情報セキュリティ運用上の最も大きな課題（単一回答,n=240）】

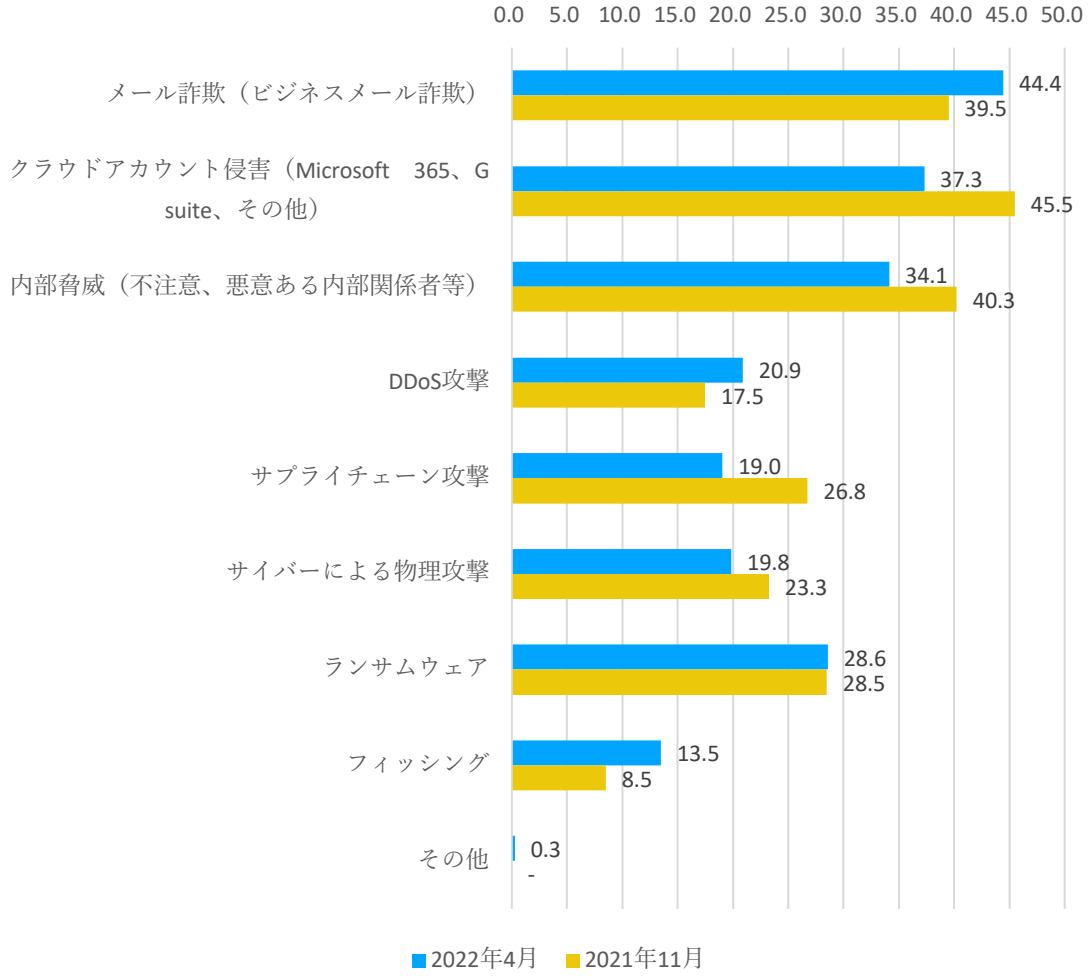


今後自組織で発生すると考えられるサイバー脅威

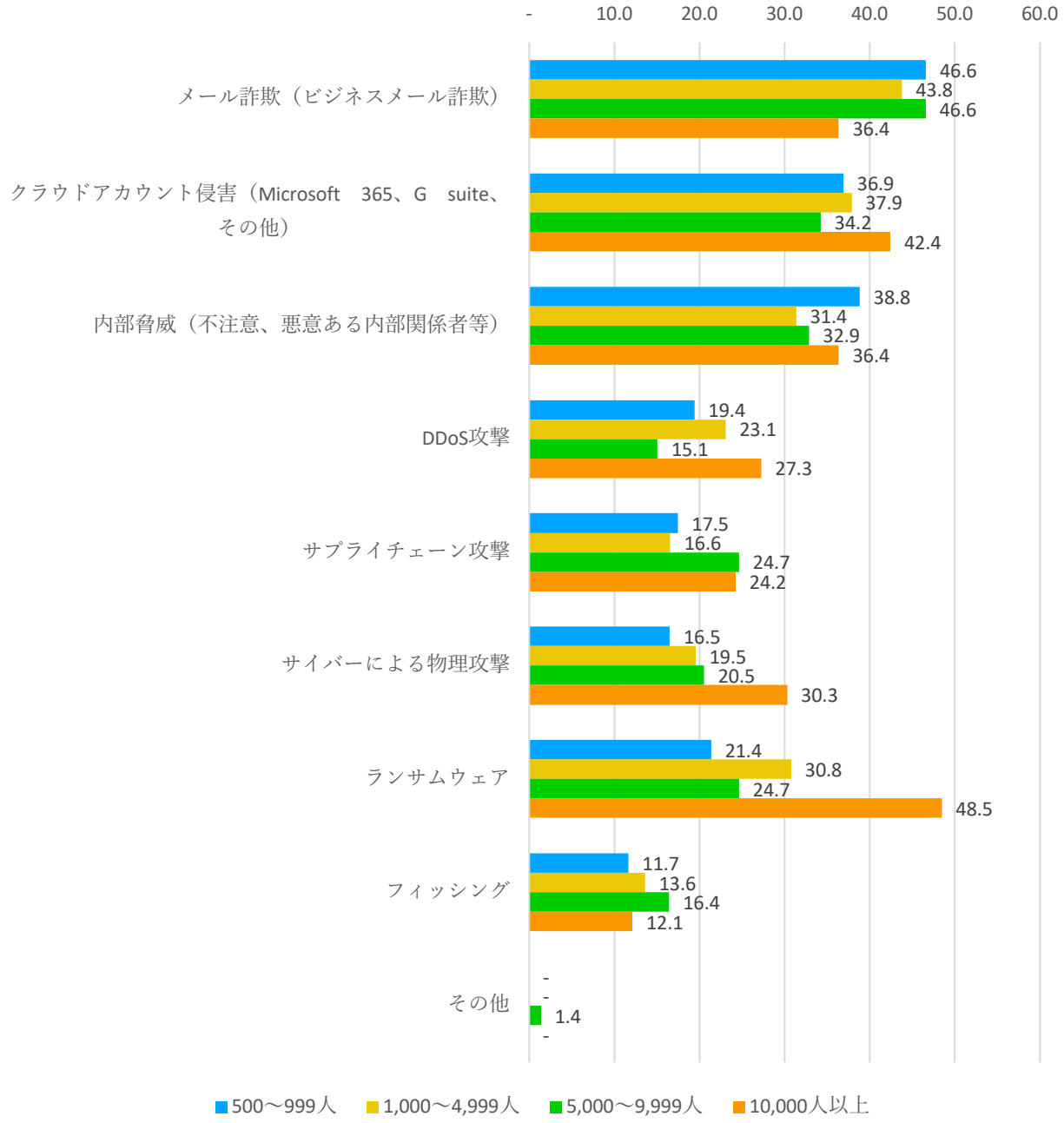
回答者が向こう 1 年間に自組織で発生すると考えるインシデントは、「メール詐欺（ビジネスメール詐欺）（44.4%）」が最多で、次に「クラウドアカウント侵害（Microsoft365、Gsuite、その他）（37.3%）」、続いて「内部脅威（不注意、悪意ある内部関係者等）（34.1%）」となり、前回調査同様の結果でした（図 10）。

組織規模別にみると、全体的に大きな違いが無いなか、突出して高いのが、1 万人以上の組織の「ランサムウェア（48.5%）」で、他の組織規模と比較し約 20 ポイント高。同様に「サイバーによる物理攻撃（30.3%）」も、他と比べ約 10 ポイント高い結果となりました（図 11）。これらの背景には、2022 年 2 月に発生したトヨタ自動車取引先へのランサムウェア攻撃被害や、2022 年 3 月の関係 4 省庁（経済産業省、総務省、警察庁、内閣官房内閣サイバーセキュリティセンター）からのサイバーセキュリティ対策強化への注意喚起等も影響しているものと考えられます。直近の攻撃の傾向として、大企業やインフラ企業をはじめ、重要性が高く且つ攻撃による社会的インパクトが高い組織が顕著に狙われています。攻撃に対する、大企業の危機感が現れた結果といえるでしょう。

【図 10　今後 1 年間に自組織で発生を懸念するサイバー脅威（上位 3 つまで複数回答,n=378）】



【図 11　組織規模別：今後 1 年間に自組織で発生を懸念するサイバー脅威（上位 3 つまで複数回答,n=378）】



まとめ・考察

今回の調査では、サイバーインシデントの発生状況、それに対応する企業・団体のセキュリティ予算の状況やセキュリティ運用上の課題、今後懸念される脅威について、特にハイライトすべき結果となりました。

国内外で急増する被害事例からも明らかなように、多くの組織にとってもはやセキュリティは、部門や担当者レベルの問題ではなく、経営課題として優先度を上げて取り組むべき課題です。今回の調査からは、特に大企業で、そうした認識が高まりつつあることがうかがえる結果となりました。

一方、現場では、人員不足、専門知識や経験の不足といった「人」にまつわる問題、システムの複雑性や使い分けの煩雑性といった「仕組み」の問題、という大きく 2 つの問題が根強く存在することも、調査結果のとおり事実です。これらの課題に対しては、今後どのような組織でも、いっそう優先順位を上げて取り組むこととなると推察します。そのためには、人や仕組みの問題を、テクノロジーを有効に活用することで解決していく発想、アプローチが必要となるでしょう。

また、昨今のサンラムウェア攻撃をはじめ各種インシデントから明らかなように、攻撃は年々複雑化、巧妙化しています。これらの攻撃による被害を未然に防ぐこと、また発生時に効率よく対処するには、単一の技術ではもはや対応は不可能です。そこで大切な考え方は、さまざまなセンサー群で脅威を検知するフロントエンド、そうしたセンサーからのログを解析、保存、相関的分析からリスクへの回答や復旧支援を行うバックエンドを、統合的に管理・運用していくことです。

こうした課題や考え方を実現するソリューションとして、XDR（eXtended Detection and Response）へ高い期待が寄せられています。次世代のセキュリティ対策のスタンダードといわれる XDR の普及と進化において、当社 Trellix は今後も国内外で一層大きな役割を担うべく、尽力してまいります。

【調査概要】

調査名	サイバーセキュリティについての調査
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 1000 人。集計にあたり、従業員数 500 名以上の組織に所属する回答者を抽出（n=378）
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 4 月 14 日（木）から 4 月 18 日（月）
調査主体	Trellix（株式会社アスマークに委託）

Trellix について

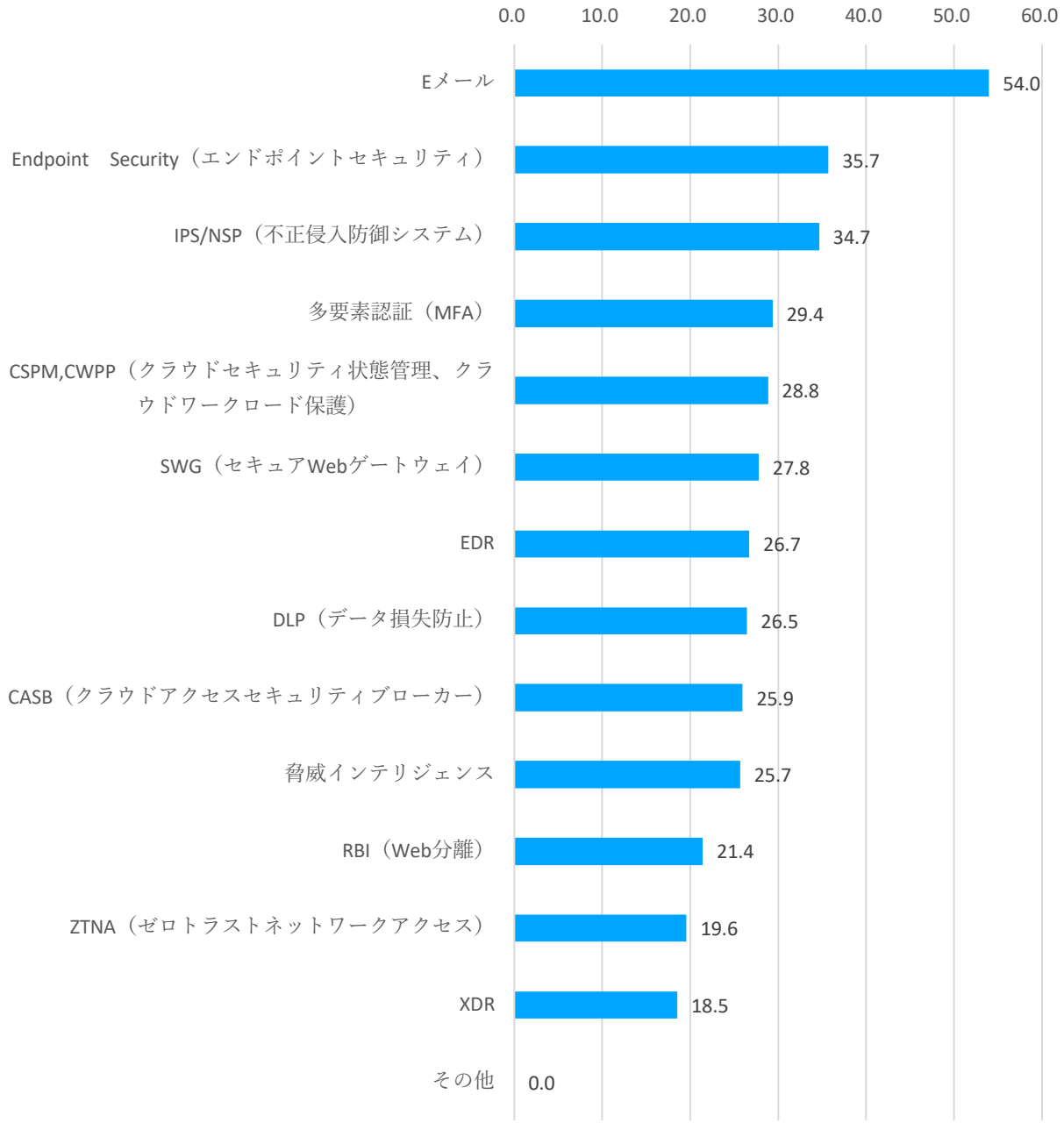
Trellix は、サイバーセキュリティの未来を再定義するグローバル企業です。オープンかつネイティブな Trellix の XDR（Extended Detection and Response）プラットフォームは、現在最も高度な脅威に直面するお客様が業務の保護や回復に確信を持って対応するための支えとなります。Trellix のセキュリティ専門家は、広範なパートナーエコシステムとともに、データサイエンスと自動化によりテクノロジーイノベーションを加速させ、4 万を超える企業や政府機関のお客様の力となっています。

＜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

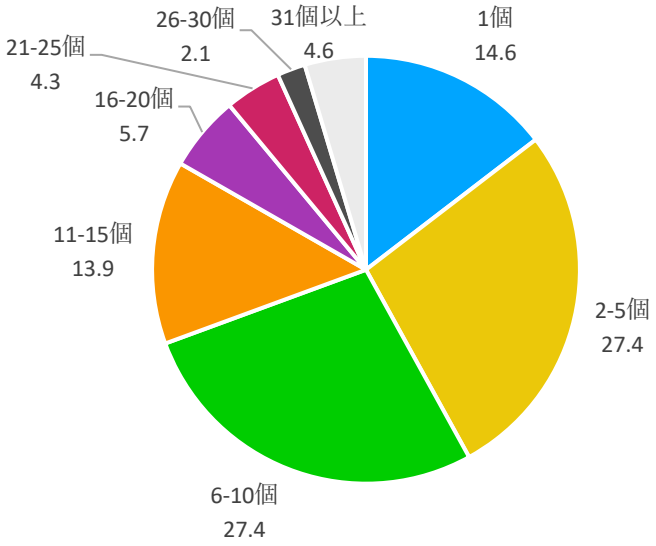
Trellix（McAfee Enterprise）広報担当
LaCreta 担当：野澤 / 近藤
Tel: 050-4560-2425　trellixjpn@lacreta.jp

別紙：その他の調査結果

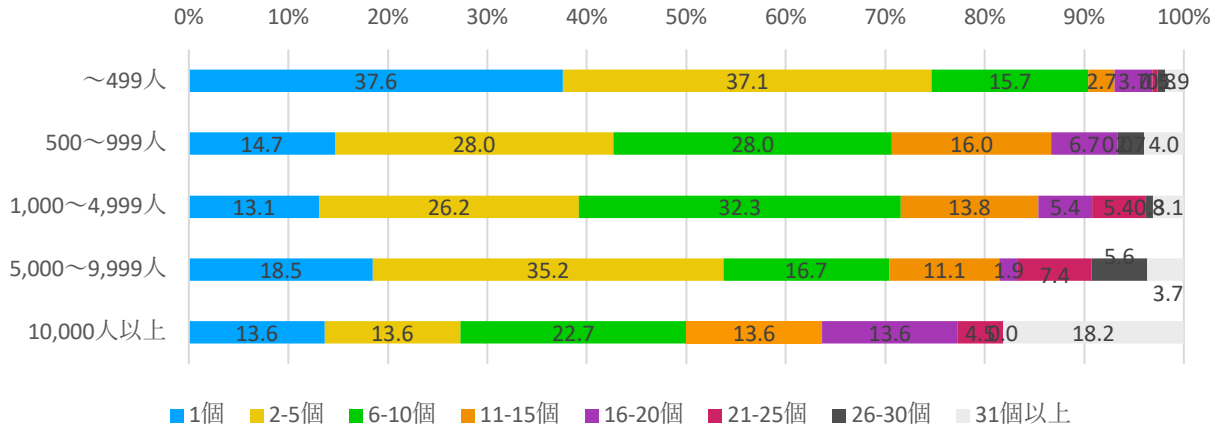
【図 12　導入中／導入済の製品分野（複数回答,n=378）】



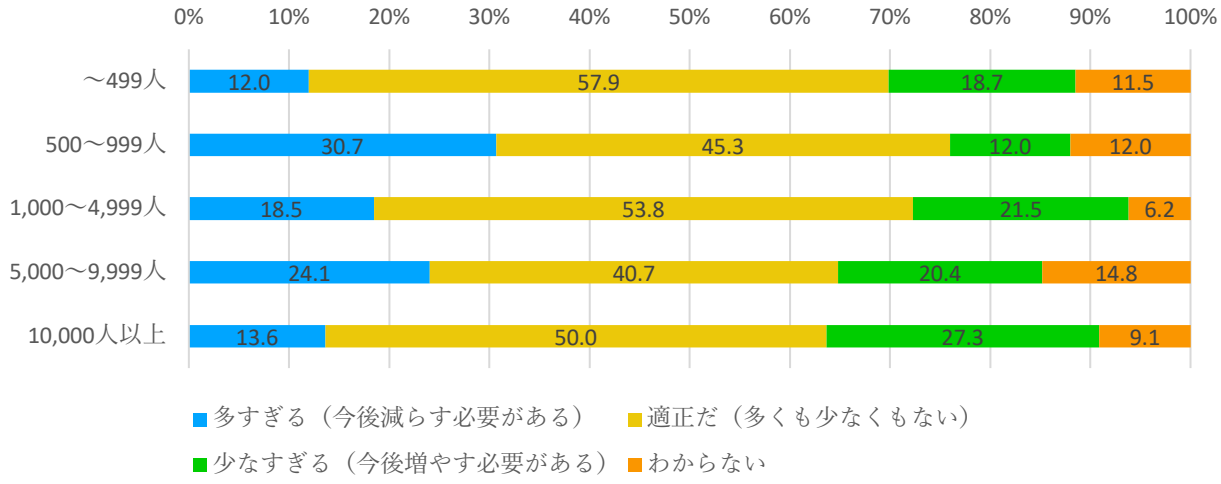
【図 13　導入中／導入済のセキュリティ製品・サービスの導入数（単一回答,n=281）】



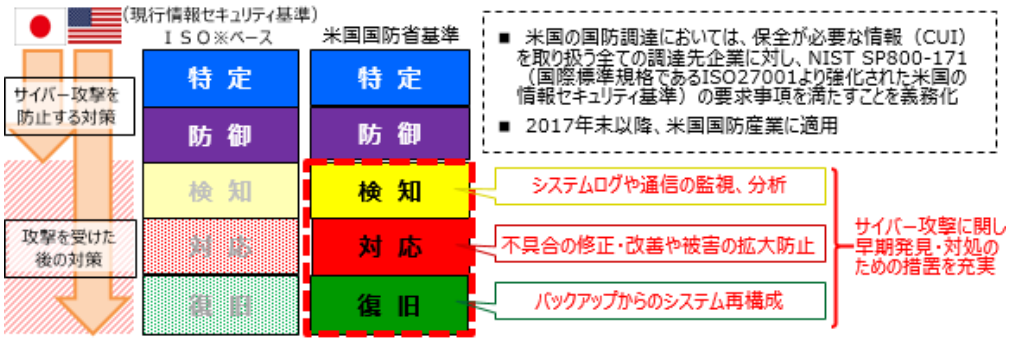
【図 14　企業規模別　導入中／導入済のセキュリティ製品・サービスの導入数（単一回答,n=281）】



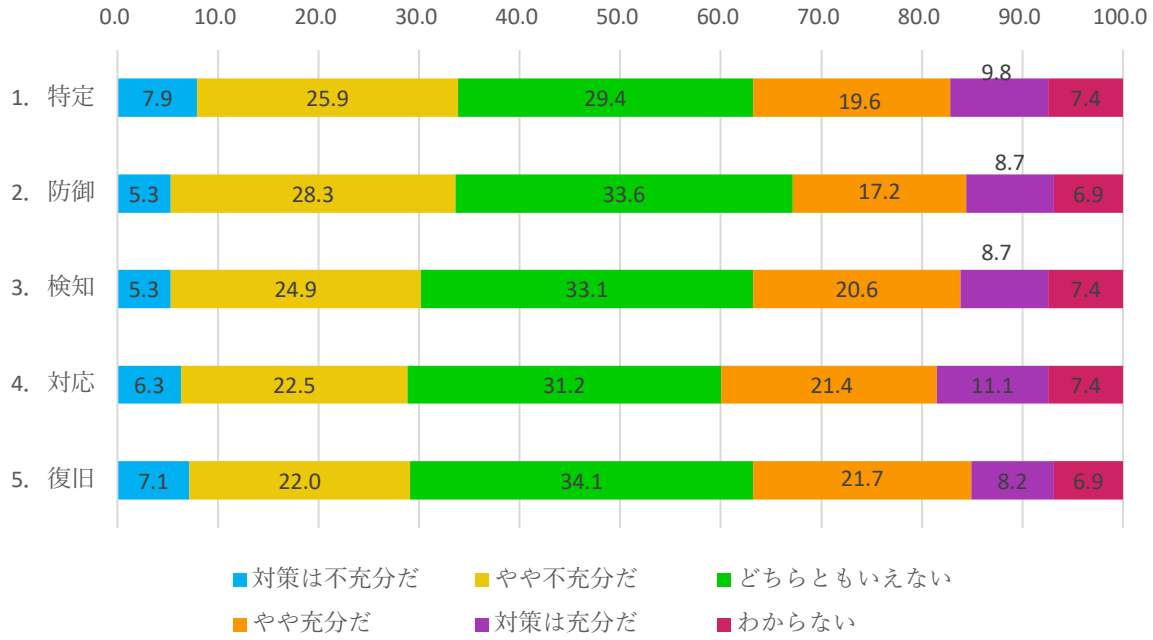
【図 15　セキュリティ製品・サービスの導入数に対する適正性の認識（単一回答,n=281）】



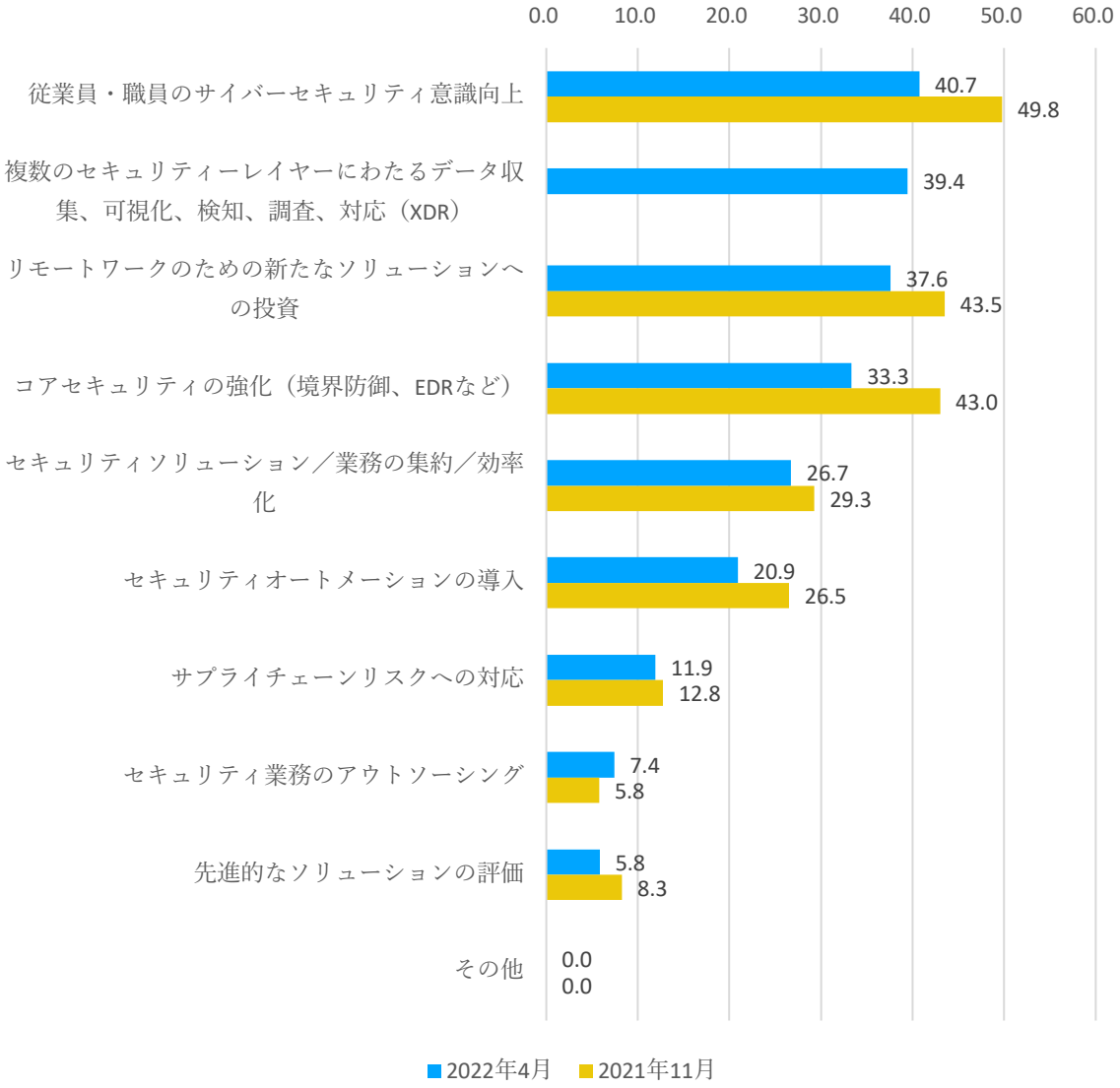
【図 16　米国国防省基準に照らした、自組織のセキュリティ対策認識（単一回答,n=378）】



出典：防衛装備庁ウェブサイト　https://www.mod.go.jp/atla/cybersecurity.html



【図 17　自組織の情報セキュリティで、今後優先すべき事項（上位 3 つまで複数回答,n=378）】



※選択肢「複数のセキュリティレイヤーにわたるデータ収集、可視化、検知、調査、対応（XDR）」は新設のため前回分データなし