SOPHOS
Cybersecurity delivered.

アジア太平洋地域と日本のサイバーセキュリティの展望

第 3 版、2022年 4月

ソフォスの委託による TRA レポート

目次

はじめに

「アジア太平洋地域と日本のサイバーセキュリティの展望」の第 3 版をご覧いただきありがとうございます。本レポートは 2019 年に初めて発行されて以来、これらの地域における企業が直面しているサイバーセキュリティに関連する課題を調査・検証して報告してきました。

TRA が発行しているレポートは、攻撃手法や脆弱性情報、そして、サイバーセキュリティのテクノロジーにとどまらず、成熟度、予算、意識、教育とトレーニングなど、企業がサイバーセキュリティ環境をどのように管理するかという実践的な要素も取り入れています。

本年度のレポートでは、前年度と同様に次の 3 つの重要課題に対する企業の取り組みや検討状況について紹介しています。

- サイバーセキュリティの戦略と実行
- 教育とスキル
- 脅威からの保護

また、今年は調査対象項目を拡充しており、以下の関連項目についても取り上げています。

- 経営幹部の教育
- サイバーセキュリティのスキル不足と最も需要の高い分野
- TRA の調査グループが経験した最も頻度の高い攻撃手法
- 企業の防御戦略における脅威ハンティングの重要性

この調査は、オーストラリア、インド、日本、マレーシア、フィリピン、シンガポールの IT およびサイバーセキュリティの意思決定者 900 人を対象に行われました。調査によっていくつかもの重要な知見が得られました。

サイバーセキュリティ戦略と実行

- **支出は増加。**平均して、サイバーセキュリティへの支出は、2022 年のテクノロジー予算の 11% を占めており、前年度より増加しました。
- **成熟度の上昇は、能力の向上を必ずしも意味しない。**サイバーセキュリティの成熟度は上昇を続けていますが、組織は毎年同じ問題に悩まされ続けています。自己評価した成熟度が楽観的すぎるか、対処できていない深刻な体系的の問題があると考えられます。
- **サイバーセキュリティは、パートタイムのスタッフが担うべき業務ではない。** 企業は、現在社内にいる IT プロフェッショナルにそのままセキュリティ業務を割り当てるのではなく、専門のセキュリティスペシャリストを任命する傾向が明らかになっています。

教育とスキル

- **サイバーセキュリティのスキル不足は今後も継続する。**73% の企業が、今後 2 年間にサイバーセキュリティ関連の従業員を採用することは困難になると予想しています。
- **経営幹部レベルの教育が重要。**取締役会がサイバーセキュリティを本当に理解していると考えている企業はわずか 40% に過ぎません。サイバーセキュリティプロフェッショナルが経験する最大のフラストレーションは、経営幹部や役員が、自分の会社は絶対に攻撃されないと思い込んでいることです。
- **ベンダーは、経営幹部を啓蒙・教育する役割を担っている。**回答者の 60% は、サイバーセキュリティベンダーが、経営幹部の啓蒙と教育に役立つ適切な情報を十分に提供していると思っていません。
- **アウトソーシングか社内リソースの活用か？**このアプローチはどのようなニーズがあるかによって異なります。戦略策定、データ管理、コンプライアンス、個人情報管理は、ほぼ社内のリソースが使用されています。脅威ハンティング、修復、インシデント対応、侵入テストなどの業務は、通常、アウトソーシングされるか、インハウスのリソース (DIY) とアウトソーシングのブレンド (混在) になります。

脅威からの保護：

- 防御で重要な鍵を握るのは脅威ハンティング。 回答者の 90% は、組織を保護する手段として脅威ハンティングを利用しています。現在のユーザーの 85% が、サイバーセキュリティの能力を高めるために脅威ハンティングが「重要」または「不可欠」と評価しています。
- 現在の主要な攻撃手法は、 フィッシング、認証情報の窃取、サプライチェーンの脆弱性、パッチが適用されていない脆弱性、悪意のある従業員です。
- 今後の攻撃手法の上位は、現在とほぼ変わらないと予測される。 フィッシング、マルウェア、システム構成の不備、企業スパイ、国家的な攻撃が主流となるでしょう。

本レポートは、調査結果、主要なデータポイントと考察を含む各国の分析、レポートのスポンサーであるソフォスの見解の 3 つのセクションから構成されています。

本レポートのデータと解説が、貴社のサイバーセキュリティの能力と環境を向上するために役立つことを心から願っています。

調査結果

調査結果は 3 つのサブセクションに分けられています。各サブセクションでは以下の重要なデータや知見を説明しています。

1. サイバーセキュリティの成熟度、戦略、実行

2. 教育とスキル

3. 防御の強化

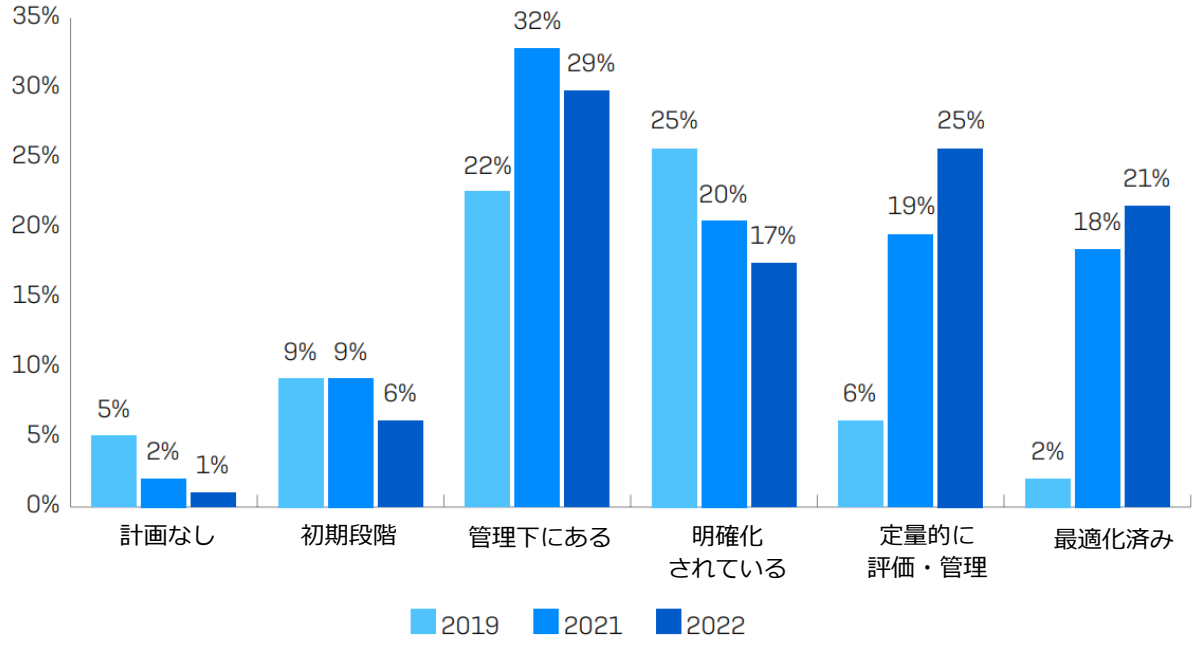
サイバーセキュリティの成熟度、戦略、実行

成熟度

2019 年以降、回答者にサイバーセキュリティの成熟度を自己評価してもらっていますが (評価基準の定義は付録で確認できます)、成熟度、能力、サイバーセキュリティ環境の理解度については継続的に向上していることが報告されています。

実際、2022 年のデータでは、調査対象の企業の 21% が、自社が成熟度の最上位レベル (「最適化済み」) にあると考えており、最高レベルにあると考えていたのがわずか 2% だった 2019 年の第1版と比較して大幅に増加しています。

サイバーセキュリティの成熟度レベル 2019～2022 年 (自己評価)

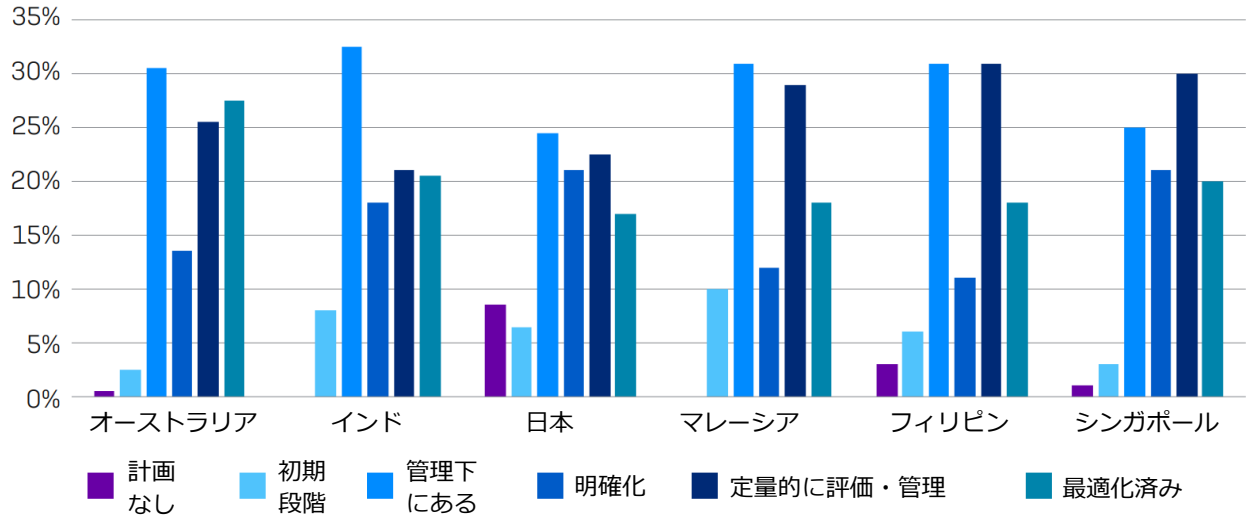


このグラフを見ると時間の経過とともに、成熟度が右肩上がりになっていることが分かりますが、各国の回答から次のような状況を伺うことができます。

- オーストラリアのプロファイルでは、成熟していると考えている組織の割合が最も高い (28%) 一方で、セキュリティ能力を開発中の組織の割合も比較的高い (31%が「管理下にある」) 。

- インドは、オーストラリアと同様に「最適化済み」と「管理下にある」と評価する組織が多いが、「管理下にある」の方が多く、成熟度が向上しています。
- 日本では、9% の企業がセキュリティ能力開発における「計画なし」であり、7% が「初期段階」にあります。
- インドと同様に、マレーシアでも 31% の企業が「管理下にある」レベルにあります。「初期段階」の割合は 10% で、これはすべての国の中で最も高くなっています。
- フィリピンでは、「定量的に評価・管理」の段階にある組織の割合が 31% と最も高く、来年も「最適化済み」に向けて順調に歩んでいることが示されています。
- シンガポールは、全回答者の 50% が「定量的に評価・管理」または「最適化済み」と回答しており、成熟度ではオーストラリアに次いで第 2 位です。

国別のサイバーセキュリティ成熟度 2019～2022年 (自己評価)



成熟度が継続的に向上していることは喜ばしいことです。一方で、企業の自己評価が楽観的すぎるという懸念もあり、それを裏付ける 2 つの客観的なデータもあります。

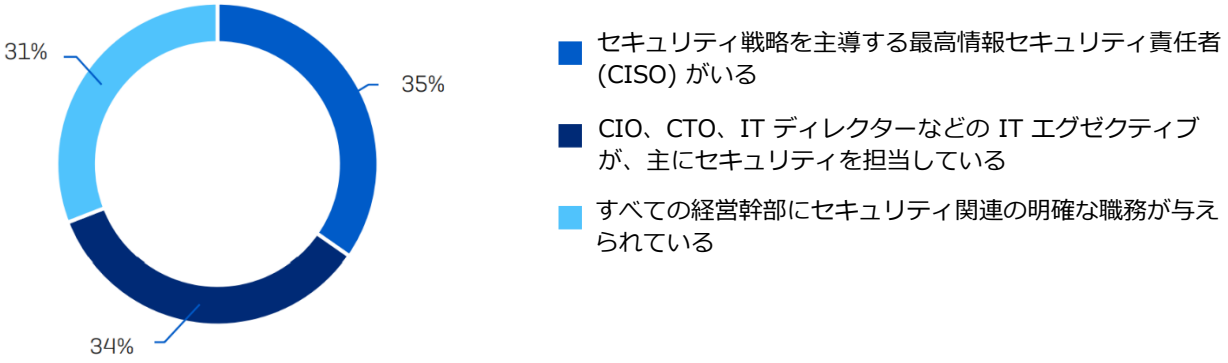
1. まず、次のセクションで紹介するように、一部の回答者は、セキュリティ侵害や攻撃を受けた結果、サイバーセキュリティ戦略を変更している傾向があります。そのために、攻撃と戦略の変更を延々と繰り返すスパイラルが発生している場合があります。
2. 第 2 に、成熟度を向上しているにもかかわらず、サイバーセキュリティプロフェッショナルが経験している共通の不満があります。それは、テクノロジーソリューションではなく、
脅威環境についての誤った想定や誤解です。これは、教育や意識向上に関する問題です。

もちろん、サイバーセキュリティ戦略や教育は「一度実施したら終わり」であると言っているのではありません。成熟度が向上していると主観的に思い込み、自社の能力について根拠のない楽観論を展開するようになると、不利益を被る恐れがあります。

戦略と実行

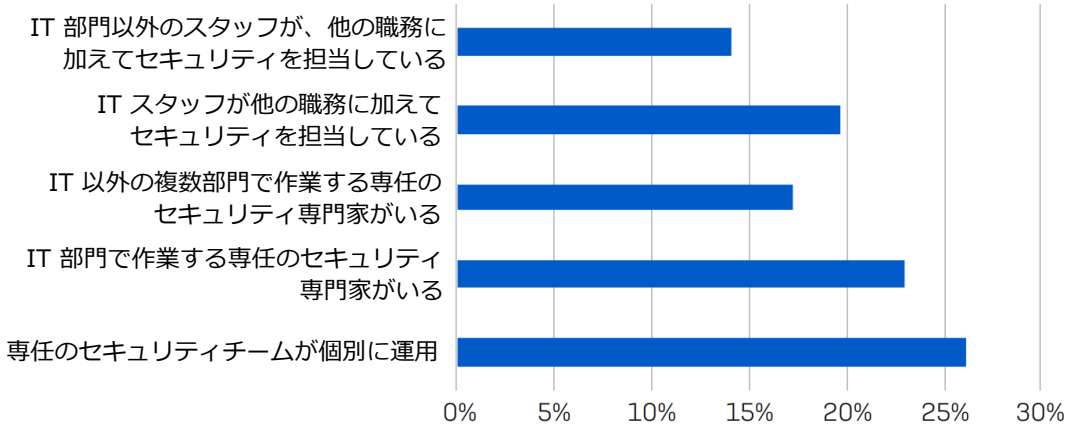
35% の組織では、最高情報セキュリティ責任者 (CISO) が戦略を主導しており、さらに 34% の回答者は IT 経営幹部 (CIO、CTO) が責任を負うと述べています。31% の企業は、経営幹部や管理職グループ間で責任を分散させる混合モデルを採用しています。これの傾向は、2019 年に発行した最初のレポート以降、あまり変化していません。

サイバーセキュリティ戦略を主導しているのは誰か？



また、調査データから、通常の IT スタッフや他の従業員に、彼らの従来の業務に加えてセキュリティ業務を割り当てるよりも、サイバーセキュリティ業務を専任にするスタッフを任命することが望ましいことが明らかになりました。

あなたの組織は、サイバーセキュリティの運用にどのように取り組んでいますか？



社内リソース、アウトソーシング、またはその組み合わせなど、企業におけるセキュリティ運用の責任分担の方法は、必要となっている業務によって大きく異なります。データから見えてくるのは、「社内リリース」だけが圧倒的に選択されている要件はなく、多くの場合、アウトソーシングと社内リソースを組み合わせた「協力型」のアプローチが進められています。

戦略策定、教育とデータ管理、コンプライアンスなどは、僅差で社内リソースを使用するケースが多くなっています。2021年には同じレポートで「組織の大半は今でもほぼすべての機能を社内、で管理しており、ペネトレーションテストやトレーニングなどのいくつかの分野についてのみアウトソーシングしているのが一般的です。」と報告していましたが、この社内リソースを利用する傾向は、2022年には減少しています。

攻撃の防御と影響の復旧に関連する分野 (侵入テスト、インシデント対応、脅威ハンティング、修復など) では、直接アウトソーシングする方法とブレンド (社内リソースとアウトソーシングの両方) の方法のいずれかが採用されることが多くなっています。

戦略の変更

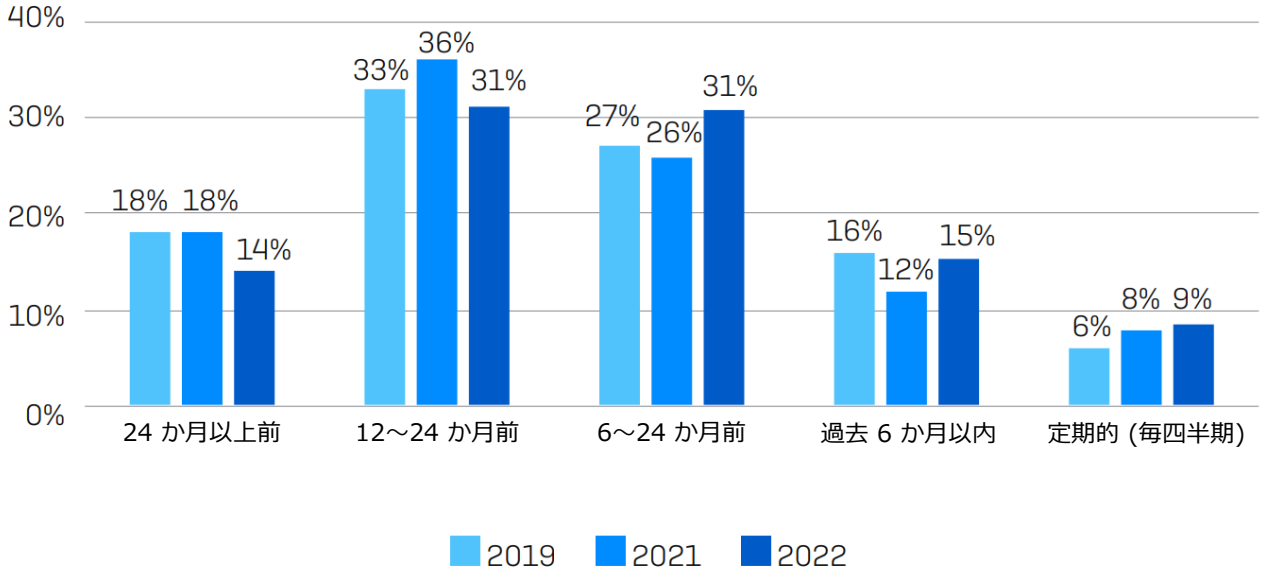
このセクションでは、サイバーセキュリティ戦略を変更する理由とその頻度について得られた知見について説明します。最後に戦略を大きく変更したのはいつか、また変更した理由について尋ねました。

2019 年と 2021 年のデータとは対照的に、2022年には、組織が短いスパンでより多くの戦略を変更していたことが浮き彫りになっています。

- 31% が過去 7～12 か月間に変更を行った
- 15% が過去 3～6 か月間に変更を行った
- 9% が四半期ごとに頻繁に変更している

最後に情報セキュリティやサイバーセキュリティのアプローチに大きな変更を加えたのはいつですか？

2019 年～2022 年



また、次に戦略を見直し、変更する可能性があるのはいつですか、という質問に対しては、次のような回答がありました。16% の回答者が四半期ごとに変更していると答え、33% が今後 4～6 か月間に変更すると答えました。なぜ? 攻撃を経験したことが変更した理由です。

攻撃の経験という要因は、これまでのすべての調査でトップを維持しています。一方で、全体的なテクノロジー戦略の変更、新しいテクノロジーソリューションの採用、予算の問題、デジタルトランスフォーメーションプログラム、規制の変更の影響など、他の事項はすべて重要性が変動しています。

攻撃を多く受けるほど、その対策が必要となります。このスパイラルに陥っている企業が多くなっている可能性があります。

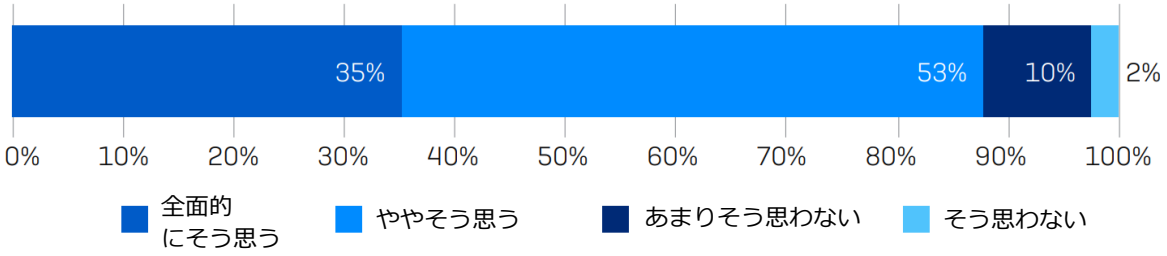
サイバーセキュリティのプロフェッショナル以外のスタッフや経営幹部がサイバーセキュリティの実態を十分に理解していないことが、このセキュリティの負のスパイラルを悪化させている事例も見られています。この問題を解決するためには、教育とスキルセットの向上が必要となります。これらの課題については、次のセクションで詳しく見ていきます。

教育とスキル

「教育とスキル」に対する意識を把握するために、「今後 24 か月のセキュリティに関する最大の課題は、従業員とリーダーの意識向上と教育である」という記述について、調査参加者がどの程度同意するか評価してもらいました。

- 35% の企業が「非常にそう思う」と回答
- 53% の企業が「ややそう思う」と回答
- 12% の企業が「そう思わない」と回答

次の文章について、どの程度同意しますか。今後 24 か月のセキュリティに関する最大の課題は、従業員とリーダーの意識向上と教育である。



サイバーセキュリティのプロフェッショナルが自分の業務で多く体験するフラストレーションに、この問題が含まれているのは不思議ではありません。

戦略と運用で多く感じるフラストレーション

過去のレポートでも、サイバーセキュリティのプロフェッショナルに、自社について、また、セキュリティ業務で最もフラストレーションを感じることは何かを質問してきました。

今年の上位 5 つの要因の内の 4 つが大きく上昇していました。これらの要因の大半は、セキュリティに関する意識、認識、メッセージ、教育に関するフラストレーションです。

1. 希望的観測か、幸せな無知か。「経営幹部は自社が攻撃されることは決してないと考えている」希望的観測や幸せな無知かは分かりませんが、フラストレーションの第 1 位は、「自社は絶対に攻撃を受けない」という楽観的な見方です。しかし、一度でも攻撃を受けると、通常、戦略の変更を余儀なくされ、大きな混乱を引き起こすことになります。
2. 高度なスキルを有するセキュリティプロフェッショナルの不足。「スキルを持ったセキュリティプロフェッショナルを十分に雇用できない。」スペシャリストを採用するためには多額の費用が必要ですが、採用したスペシャリストを維持することも非常に大変です。しかし、企業は、自社のセキュリティ業務を支えるための一般の従業員の教育やトレーニングに十分な費用と時間を投資していません (表の 6 番目の項目を参照)。
3. 誰もが攻撃される運命にある (i)。「恐怖と疑念を与えるメッセージ多すぎるため、サイバーセキュリティについて議論することが難しい。」昨年に続き、FUD (恐怖、不安、疑念) のメッセージが多く悪用されており、再び注目されるようになりました。実在しない脅威をしきりに探している状況では、適切な啓蒙と教育を行うことは困難です。
4. 誰もが攻撃される運命にある (ii)。「経営陣は今後自社が攻撃されると予想しているが、攻撃を阻止する方法はないと考えている」。悲観的な考えに陥り、適切な対策を迅速に講じようとしないケースがあります。
5. 余りにも動きが速すぎる。「セキュリティ脅威のスピードに追いつけない。」起こりうることのすべてに対応することはできないため、できることをするしかありません。そして、何事もないことを期待します。

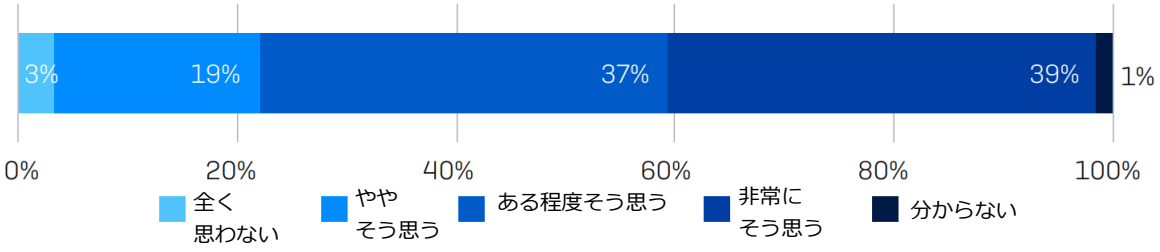
フラストレーションの原因となる主な問題	2019	2021	2022
1.経営陣は自社が攻撃されることは決してないと考えている	7	7	1
2.スキルを持ったセキュリティ専門家を十分に雇用できない	5	3	2
3.「恐怖と疑念」を与えるメッセージが多すぎるため、サイバーセキュリティについて正確に議論することが難しい	4	11	3
4.経営陣は今後自社が攻撃されると予想しているが、攻撃を阻止する方法はないと考えている	10	8	4
5.セキュリティ脅威のスピードに追いつけない	8	9	5
6.IT 以外のスタッフのトレーニングに十分な投資も時間もかけられていない	6	6	6
7.サイバーセキュリティに十分な予算が確保されていない	2	2	7
8.経営陣は口先ではサイバーセキュリティ対策について賛同しているが、本当に信じているわけではない	9	5	8
9.セキュリティに関して雑音が多すぎる	11	10	9
10.経営陣は、サイバーセキュリティは簡単に実現できるもので、私を含む他のサイバーセキュリティ関係者が脅威や問題を誇張していると考えている	3	1	10
11.サイバーセキュリティの優先順位を下げられることが多い	1	4	11

スキルの高いセキュリティスペシャリストの不足 (前の表の第 2 位) を除くと、他の上位 5 つの課題については、経営幹部や役員から組織の他の従業員まで、全社的な教育や意識向上プログラムによって対応することが可能です。

このアプローチには 1 つだけ問題があります。それは、TRA の調査データではサイバーセキュリティのプロフェッショナルが、会社の経営幹部のセキュリティに対する理解度が低いと感じていることです。

経営幹部がサイバーセキュリティを本当に理解していると考えているサイバーセキュリティのプロフェッショナルは約 4 割に留まっています。回答した企業の 22% しか毎月または毎四半期にサイバーセキュリティに関する最新情報を聞き取る取締役会を設置していない調査データもあり、この課題がさらに深刻であることが分かります (この数値は、2024 年には 26% に増加すると予測されています)。

自社の経営幹部は、サイバーセキュリティについて本当に理解していると思いますか。

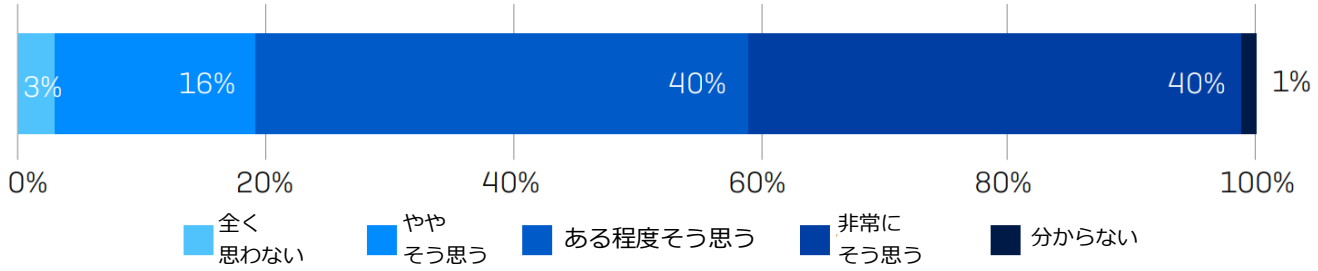


経営幹部が、本当にサイバーセキュリティの問題を理解しているのか、それとも、問題を十分に理解せずに提示されたチェック項目に盲目的に従っているのかは不明です。

しかし、教育に関するニーズが存在していることは間違いありません。多くの場合、企業は特にセキュリティ戦略、意識向上、トレーニングなどの分野で、ベンダー、あるいは社内リソースとベンダーの両方に支援を求めています。

今回のデータでは、ベンダーの意図は評価できる一方で、期待通りの結果が得られていないことを示唆しています。サイバーセキュリティベンダーが、サイバーセキュリティに関する経営幹部の啓蒙や教育に役立つ適切な情報を提供していると感じている企業は、わずか 40% に過ぎません。

サイバーセキュリティベンダーは、経営幹部がサイバーセキュリティについて理解を深めるために役立つ適切な情報を提供していると思いますか。



もちろん、これはベンダーにすべての責任を押し付けるべき単純な問題ではありません。古くから、IT 担当者が新しいテクノロジーを導入すると、ビジネス部門のユーザーは「これは何に使うの？」と質問してくるように、ビジネス部門とテクノロジー部門の両方の経営幹部が明確かつ緊密にコミュニケーションを取ることに苦労するという大きな問題を引きずっています。

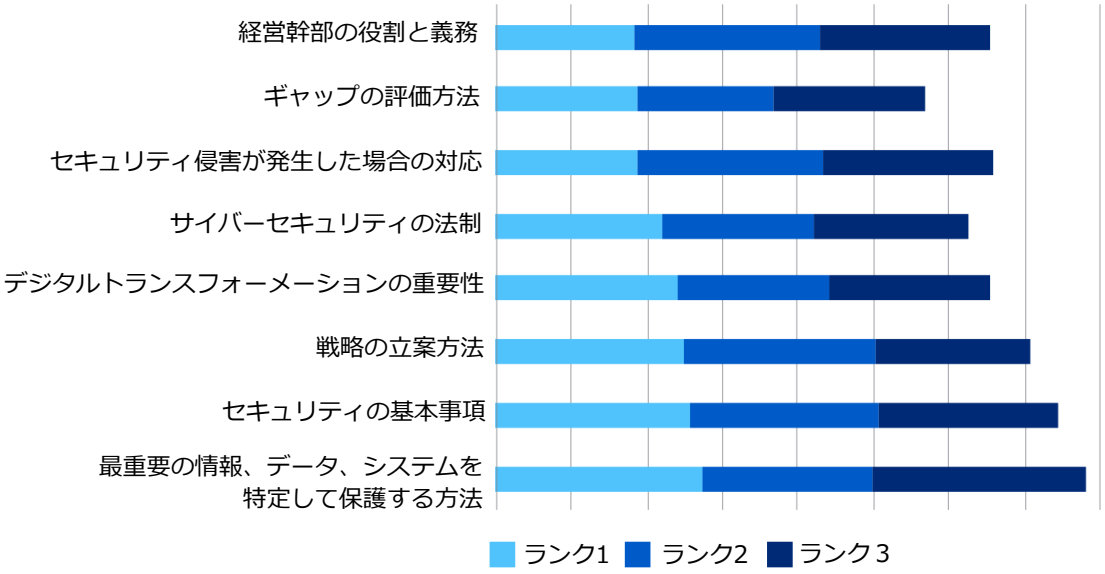
では、重点的に教育する必要がある分野は何でしょうか。

経営幹部を教育する上で重要なサイバーセキュリティの課題 (簡易版)

これは、いくつもの階層から構成されるアプローチであり、教育について検討している組織に何から着手するべきかを示すリストです。

1. **最も重要なシステムとデータを最初に特定する。**最初に、すべてを保護することは不可能であり、保護すべき最も重要な情報、データ、システムを特定することに注力することがより効果的であることを、経営幹部に理解してもらうことが先決事項です。
2. **保護しなければならないことは理解した場合に、何から着手するべきか？**サイバーセキュリティの基本について教育します。サイバーセキュリティの基本原則、攻撃の真偽性、攻撃手法、脅威となる攻撃者、また、サイバーセキュリティの専門家にとっては第 2の言語となっていますが、専門外のユーザーには分かりにくい専門用語について教育します。
3. **デジタルトランスフォーメーションプログラムにおける戦略と意味。**基本について明確に伝えることができたら、セキュリティ戦略を策定し、その戦略とデジタルトランスフォーメーションプログラムと統合することを検討することが重要です。
4. **実質的な対策。**ステップ 1～3 を明確にしたら、適用される法規制、セキュリティ侵害が発生した場合の対応、身代金の支払い方針、ギャップの評価、将来の役割と義務など、実務的な内容について決定していきます。
5. **コンプライアンス。**多くの問題に適切に対処するためには、コンプライアンス、自社の運営環境に関わる法規制、規制に違反した場合に法的に求められる措置、データセキュリティと管理に関する適切なコントロールについて明確に把握しなければなりません。

会社の経営幹部について理解してほしい情報は何ですか？



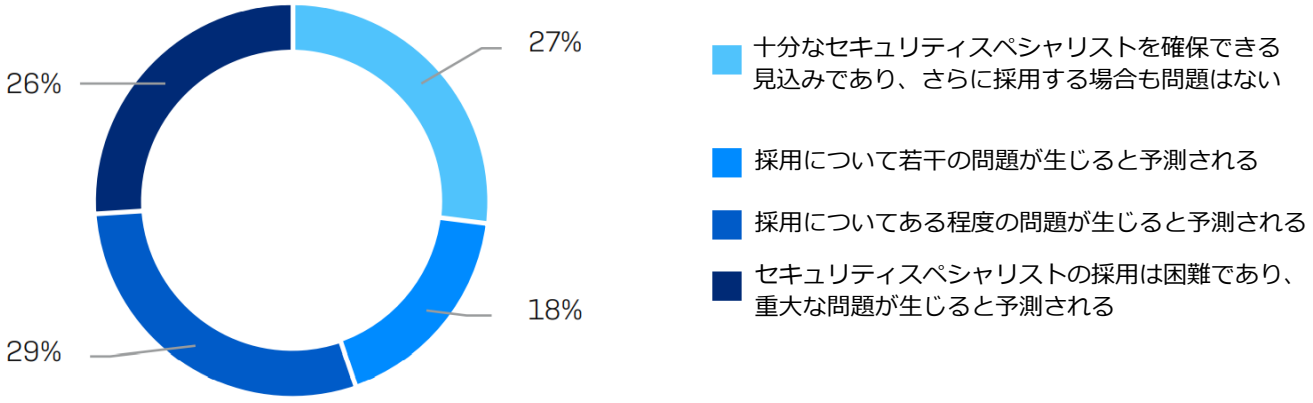
経営幹部の教育の問題を解決したら、フラストレーションのトップ 5 にあった残り 1 つの問題、スキル不足について検討しましょう。

サイバーセキュリティのスキル

調査対象となった組織ではスキル不足の問題が明確となっていることから、本レポートの新たな調査対象分野にしています。この問題の重要性を考慮し、今後発行されるレポートには詳細な分析を追加する予定です。

平均して 73% の企業が、今後 24 か月にサイバーセキュリティの従業員の確保に問題が生じると予想しています (26% は大きな課題、29% はある程度の問題、18% が若干の問題と考えています)。

自社組織でスキルを有するセキュリティ人材の今後 24 か月間の採用について、どのように考えていますか。



求められるスキルと能力

当然ながら、この問題は国によって大きく異なっています。日本 (35%)、フィリピン（31%)、インド (29%) の組織は、今後 24 か月間に採用について大きな困難を経験すると予測しています。

フィリピンの 38% の組織が、この 24 か月に採用について問題は発生しないと予想していることは注目に値します。また、オーストラリア (31%) とマレーシア (30 %) が、フィリピンを合わせて、採用に問題がないと考えている上位 3 カ国を占めています。

人材の確保が不安視される中で、企業は、以下の分野について社内のセキュリティスペシャリストのスキルと能力を向上させる必要があると考えています。

1. クラウドセキュリティのポリシーとアーキテクチャ
2. 「トレーナーを育成」できる従業員と経営幹部のサイバーセキュリティスキルトレーニング
3. ソフトウェア脆弱性テスト
4. 最新の脅威情報を常に取り入れること
5. ポリシーの遵守と報告
6. 脅威ハンティングを含むセキュリティ防御機能
7. インシデント処理の自動化
8. フォレンジック分析
9. エッジコンピューティングのセキュリティ

次の表には、各国におけるスキルの優先順位の上位 3 つを示します。

	優先して向上すべき スキル 1	優先して向上 すべきスキル 2	優先して向上すべき スキル 3
オーストラリア	クラウドセキュリティポリシー/ アーキテクチャの知識	最新の脅威情報を常に取り入れ ること	従業員と経営幹部のトレーニング
インド	クラウドセキュリティポリシー/ アーキテクチャの知識	ソフトウェア脆弱性テスト	従業員と経営幹部のトレーニング
日本	従業員と経営幹部のトレーニング	ソフトウェア脆弱性テスト	最新の脅威情報を常に取り入れる こと
マレーシア	最新の脅威情報を常に取り入れること	ポリシーの遵守と報告	従業員と経営幹部のトレーニング
フィリピン	クラウドセキュリティポリシー/ アーキテクチャの知識	ソフトウェア脆弱性テスト	最新の脅威情報を常に取 り入れること
シンガポール	クラウドセキュリティポリシー/ アーキテクチャの知識	ソフトウェア脆弱性テスト	最新の脅威情報を常に取り入れる こと

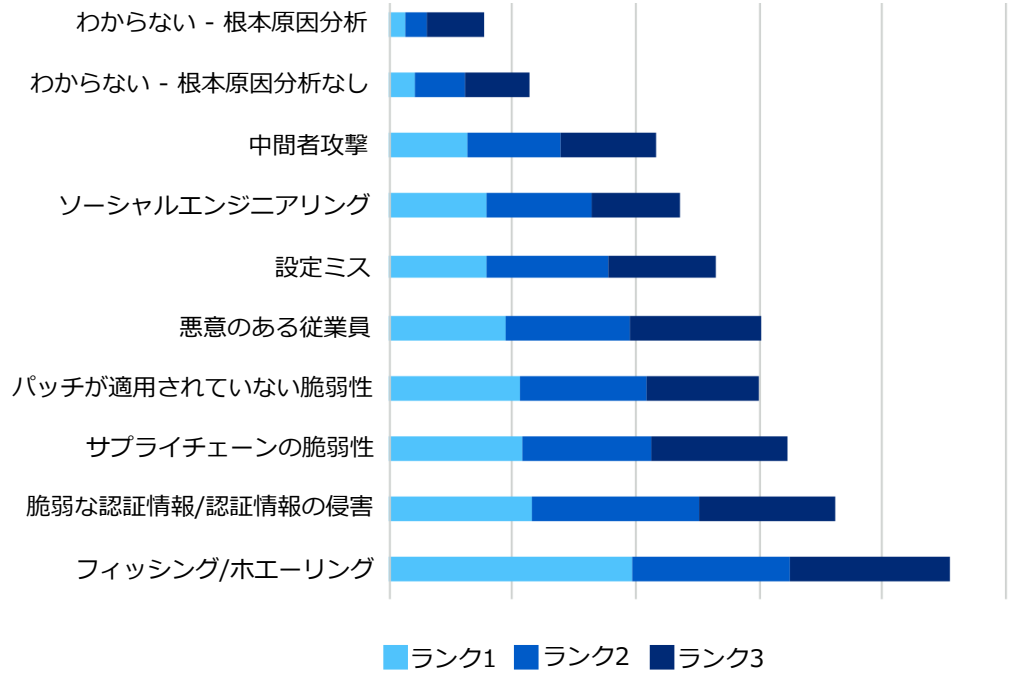
防御の強化

一般的な攻撃手法

また、2022 年版のレポートでは新しい質問として、自社が最も多く体験したセキュリティ攻撃の手法について尋ね、関連するテーマとして、現在および 24 か月後に最も重要だと考える脅威は何かも尋ねました。

次の最初の 2 つの手法は、教育と意識向上キャンペーンを継続的に実施することで部分的に対応できます。フィッシングとホエーリング (攻撃者が経営幹部や役員を標的とする攻撃)、および保護が脆弱な従業員の認証情報とこれらの認証情報の漏洩。

自社が最も多く受けているセキュリティ攻撃の手法は何ですか？



国別に見ても、攻撃手法に大きな違いはなく、6 か国すべての企業がフィッシング/ホエーリングを最も多い攻撃として認識しています。

	攻撃方法 1	攻撃方法 2	攻撃方法 3
オーストラリア	フィッシング/ホエーリング	脆弱な認証情報/認証情報の侵害	サプライチェーンの脆弱性
インド	フィッシング/ホエーリング	脆弱な認証情報/認証情報の侵害	ソーシャルエンジニアリング
日本	フィッシング/ホエーリング	未修正の脆弱性	サプライチェーンの脆弱性
マレーシア	フィッシング/ホエーリング	悪意のある従業員	サプライチェーンの脆弱性
フィリピン	フィッシング/ホエーリング	脆弱な認証情報/認証情報の侵害	悪意のある従業員
シンガポール	フィッシング/ホエーリング	構成ミス	中間者攻撃

脅威の環境のランキング

例年通り、回答者には、自分の組織にとって最も深刻だと思う脅威を評価してもらいました。

攻撃手法に関する調査結果と同様に、フィッシングがトップで、マルウェアが第 2 位でした。どちらの脅威も以前の調査で深刻な脅威の第 1 位と第 2 位にランクインしており、2022 年も同じ結果になったことに驚きはありません。

注目すべきは、2021 年に 13 位であった「脆弱なシステム」が第 3 位に上昇したことです。この結果は、APJ の多くの組織が採用しているセキュリティ・バイ・デザイン (情報セキュリティを企画・設計段階から確保するための方策) の有効性に疑問を投げかけるものとなっています (本レポートの前のセクションで説明したサイバーセキュリティ成熟度評価にもこれは若干の影響を及ぼしています)。

2022 年の注目すべきランキングの変動を以下に示します。

1. 悪意のある従業員が、2021 年の第 11 位から 2022 年に第 7 位に上昇
2. 2021 年に第 4 位であったソーシャルエンジニアリングが第 9 位に下落
3. 2021 年に第 5 位であった分散型サービス拒否 (DDoS) 攻撃は 2022 年に 12 位へ下落
4. 2021 年に第 8 位であったゼロデイの脆弱性は 2022 年に 13 位へ下落

脅威ランキング	2019	2021	2022
フィッシングとホエーリング	1	2	1
マルウェア	2	1	2
脆弱なシステム	13	13	3
企業スパイ	6	6	4
国家による攻撃	5	3	5
暗号化バックドア	4	7	6
悪意のある従業員	7	11	7
AI/ML 攻撃	10	12	8
ソーシャルエンジニアリング	3	4	9
サードパーティによるミス	8	10	10
従業員によるミス	9	9	11
DDoS 攻撃	12	5	12
ゼロデイ脆弱性	11	8	13

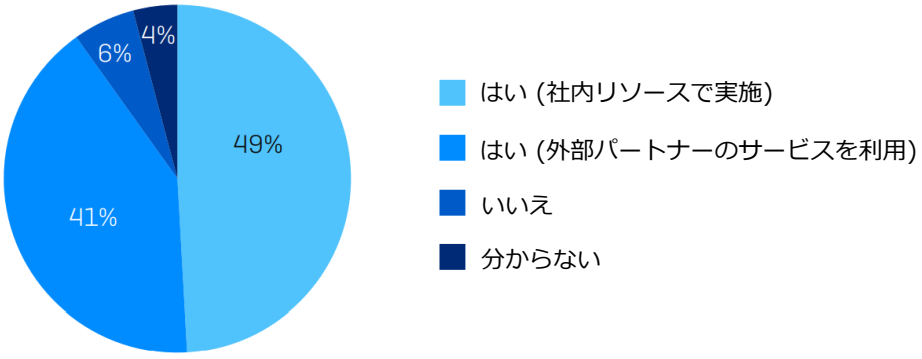
脅威ハンティングの導入と重要性

今年の調査では、サイバーセキュリティの防御を強化するための重要な検討事項として、最新のセキュリティツールを常に利用することと並んで、脅威ハンティングを積極的に行うことも挙げられていました。

今回の調査では平均して 90% の組織が、サイバーセキュリティの能力を強化するために脅威ハンティングを実施していると回答しています。

この状況は、アジア太平洋地域全体で脅威ハンティングの価値が肯定的に捉えられていることを示しています。脅威ハンティングを実施している組織の 85% は、このアプローチが自社のサイバーセキュリティ能力を底上げするために極めて重要である (21%) または重要である (64%) と回答しています。

あなたの組織は、サイバーセキュリティの防御を強化するために、脅威ハンティングを実行していますか。



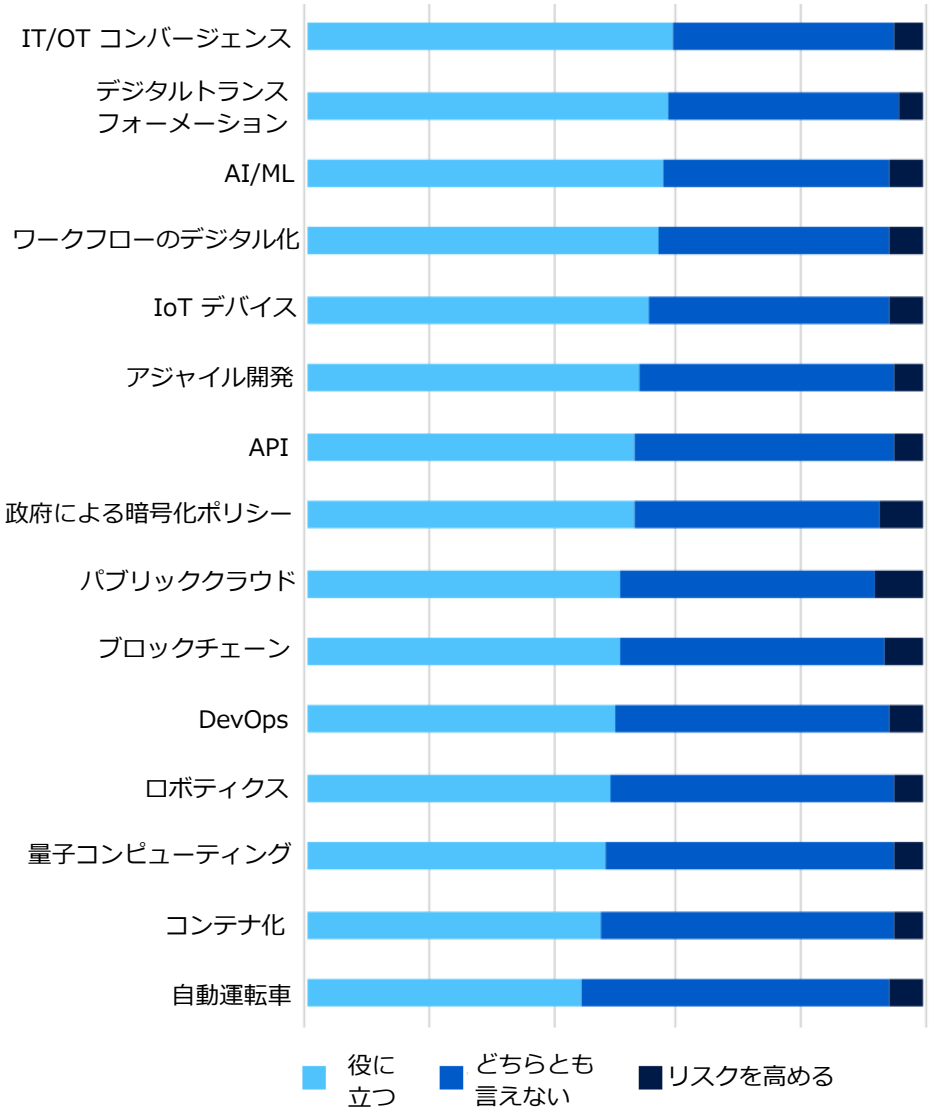
データが示すこの盛り上がりには若干の注意が必要です。定量的な検証は行っていませんが、ログ解析、インシデント応答、デジタルフォレンジック、侵入テスト、脆弱性評価などを脅威ハンティングの例としている組織もいるために、脅威ハンティングの導入数が過剰に増加している可能性もあります。

サイバーセキュリティの防御環境に影響を与えるテクノロジーと問題

この調査では毎年、回答者に対して、今後 24 か月間に組織のサイバーセキュリティに影響を与えると思われるテクノロジーや問題について尋ねています。

テクノロジーに関して回答者は、今後 24 か月で社内のセキュリティに最も影響を与えるテクノロジーは、IT と OT コンバージェンス)、デジタルトランスフォーメーション、AI (人工知能) と機械学習、ワークフローのデジタル化と IoT デバイスであると回答しています。

今後 24 か月の間に貴社のセキュリティに影響を与えると思われるテクノロジーや問題はどれですか。

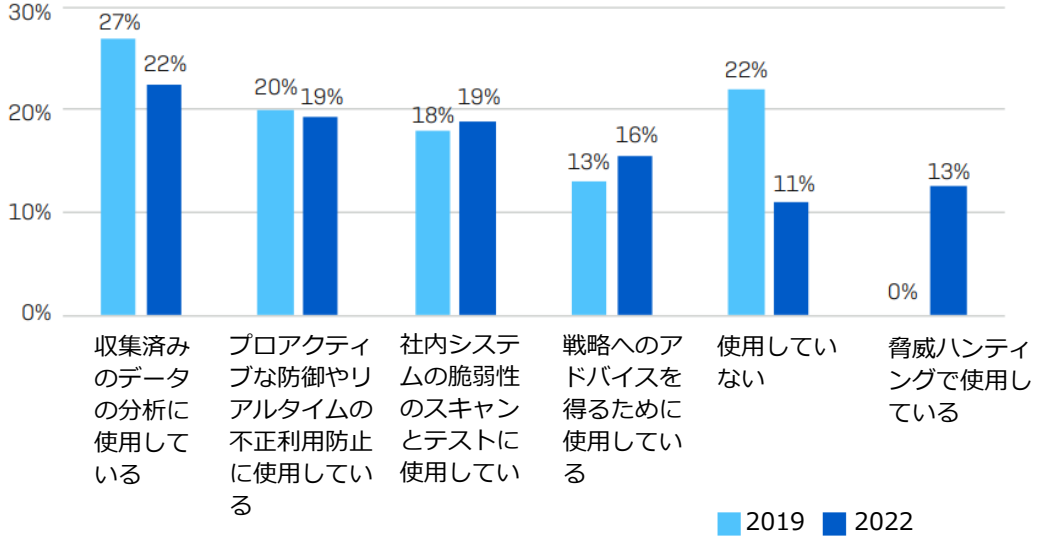


コンテナ化 (ソフトウェアコードをカプセル化し、インフラストラクチャに関わらず一貫性のある方法で実行できるようにする方法) が問題として非常に低い順位となったことには少し驚かされました。多くの組織がクラウドインフラストラクチャにおけるコンテナのスプロール化に悩まされており、これらの環境を効果的に管理するために Kubernetes のようなソリューションが必要となっています。コンポーネントの新しく追加されることで、攻撃対象領域が拡大する恐れもあります。今後、さらに多くの大企業や政府機関がコンテナ化の導入を進める中で、コンテナ化が問題として認識される順位が上がっていくことが予測されます。

2021 年のレポートでは、「*AI* と *ML* に関しては市場で過剰な期待と多くの混乱が発生していますが、調査の結果、これらのテクノロジーが将来どのように役立つかについて相当な関心と欲求があることが分かった」と報告しました。最新のデータからデータ分析および詐欺防止への AI の利用が変動していることが読み取れます。テクノロジーの進化と AI の進化に伴い、前年同期比での増加は今後も継続すると予想されます。

他のユースケースでも AI や ML の採用が進んでいる傾向は明らかであり、今後、あらゆるセキュリティプラットフォームにさらに深く組み込まれることが予想されます。注目すべき点は、2019 年には AI と機械学習を利用していないと回答した企業は 22% でしたが、2022年に利用していないと回答した企業は 12% となり、全体的に減少していることです。

現在、組織のセキュリティ対策において、AI と機械学習はどのような役割を担っていますか？



まとめ

現在の問題はテクノロジーではなく、教育です。

サイバーセキュリティへの支出 (人員、マネージドセキュリティプロバイダー、テクノロジーなど) を単に増やしても、サイバー攻撃が企業の存続、業務継続の能力、その顧客にもたらす本質的な脅威を組織の経営幹部から従業員までが理解していない限り、最適な効果を生み出すことはありません。

サイバーセキュリティの実際の成熟度を正面から正直に評価することによって、組織は一度立ち止まって、自社の本当の能力を見直すことができる場合があります。同様に、サイバーセキュリティの問題に対する経営幹部の理解を深め、サイバーセキュリティのプロフェッショナルが経験している大きなフラストレーションの一つを取り除くためには、経営幹部や役員に対して教育キャンペーンを継続的に実施して参加してもらうことが重要です。

昨年のレポートのまとめでも、「スキルのある専門家とパートナーによって強化されたサイバーセキュリティへの堅牢なプラットフォームアプローチに加えて、オペレーション面と文化面を改善することによって、企業ができない将来的に成功のする可能性が向上する」」と述べましたが、これは今年も有効なままです。

この後のセクションでは、調査対象の 6 か国の関連データについて示します。

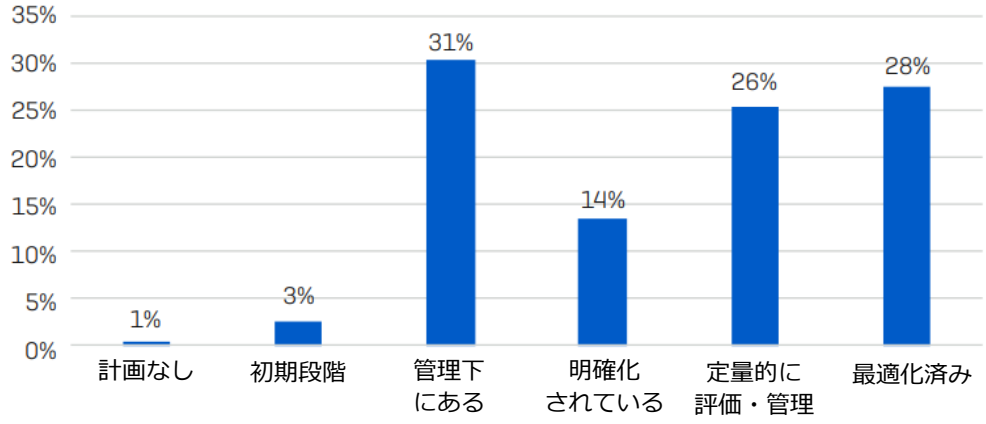
1. オーストラリア
2. インド
3. 日本
4. マレーシア
5. フィリピン
6. シンガポール

オーストラリアにおけるサイバーセキュリティ

テクノロジー予算全体に占めるサイバーセキュリティの支出の割合：11 .8%

サイバーセキュリティ成熟度のプロファイル

サイバーセキュリティ成熟度評価 – オーストラリア



サイバーセキュリティ戦略を主導しているのは誰か？

CISO：38%、CIO/CTO：32%、グループで責任を共有/その他: 29%

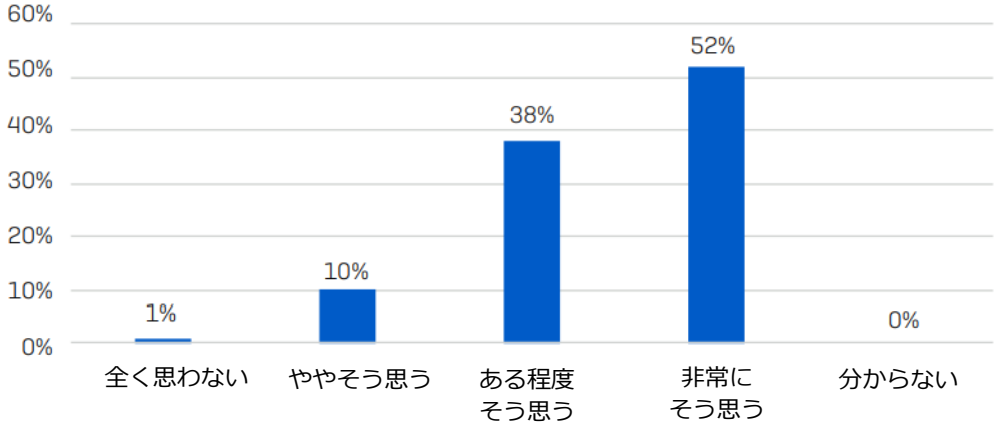
サイバーセキュリティプロフェッショナルの上位のフラストレーション

1. サイバーセキュリティの優先順位を下げられることが多い
2. サイバーセキュリティに十分な予算が確保されていない
3. 経営陣は、サイバーセキュリティは簡単に実現できるもので、私を含む他のサイバーセキュリティ関係者が脅威や問題を誇張していると考えている

サイバーセキュリティに関する経営幹部レベルの理解

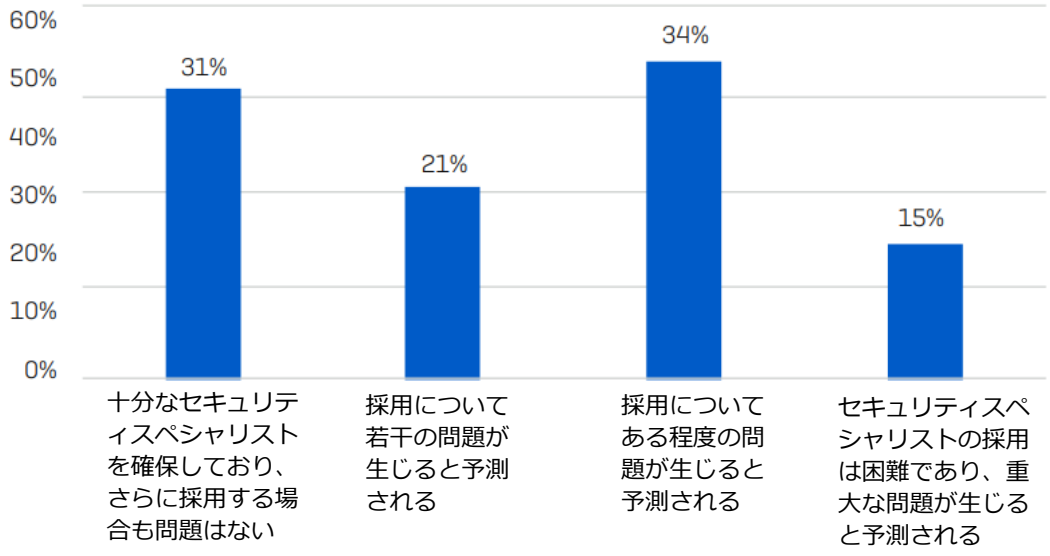
セキュリティについての経営幹部の理解度 – オーストラリア

あなたの会社の経営幹部は、サイバーセキュリティの問題をどの程度理解していると思いますか？



サイバーセキュリティプロフェッショナルの採用の難易度

自社組織でスキルを有するセキュリティ人材の今後 24 か月間の採用について、どのように考えていますか。オーストラリア



需要の高い上位スキル：

1. クラウドセキュリティポリシー/アーキテクチャの知識
2. 最新の脅威情報を常に取り入れること
3. 従業員と経営幹部のトレーニング

最も多い攻撃手法：

1. フィッシングとホエーリング
2. 脆弱な認証情報または認証情報の侵害
3. サプライチェーンの脆弱性

2022 年の重大な脅威：

1. 設計に問題があるシステム
2. マルウェア
3. フィッシングとホエーリング
4. 国家による攻撃
5. 企業スパイ

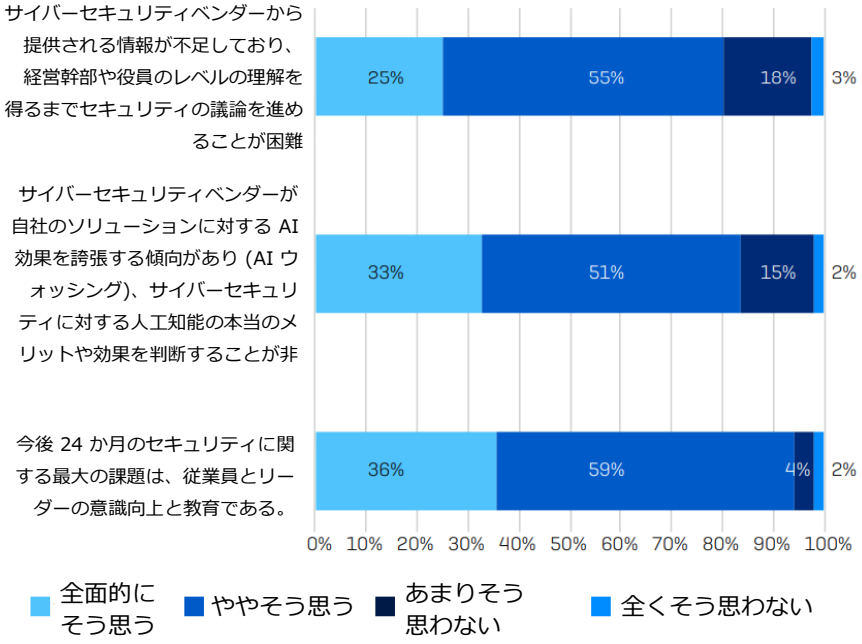
重大な脅威 2021～2022 年

2021	2022
マルウェア	設計に問題があるシステム
フィッシングとホエーリング	マルウェア
ランサムウェア	フィッシングとホエーリング
国家による攻撃	国家による攻撃
バックドア	企業スパイ
DDoS	暗号化バックドア
企業スパイ	ランサムウェア
従業員によるミス	DDoS
設計に問題があるシステム	ソーシャルエンジニアリング
AI/ML 攻撃	従業員によるミス
パートナー/サードパーティによるミス	悪意のある従業員
悪意のある従業員	AI/ML 攻撃
ゼロデイ脆弱性	ゼロデイ脆弱性
ソーシャルエンジニアリング	サードパーティによるミス

脅威ハンティングの導入

66% の企業が自社で脅威ハンティングを実施し、31% が外部パートナーのサービスを利用、3% は実施していない/わからない

次の文章について、どの程度同意しますか – オーストラリア

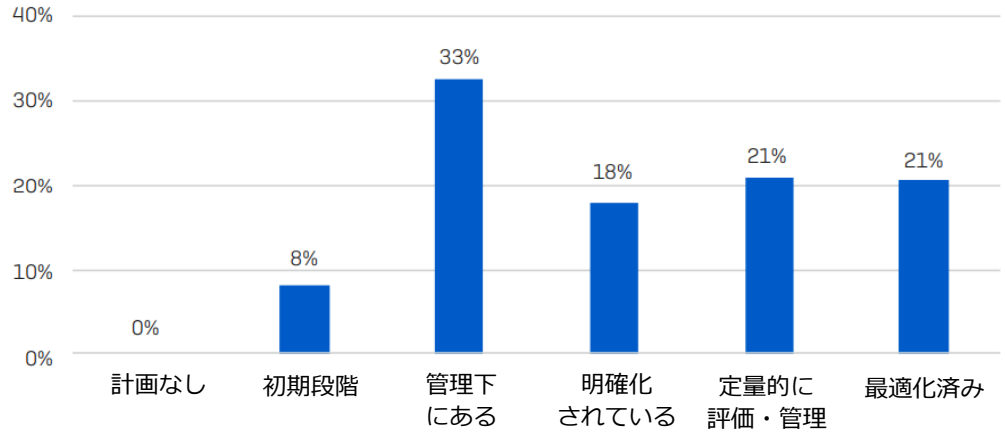


インドにおけるサイバーセキュリティ

テクノロジー予算全体に占めるサイバーセキュリティの支出の割合：10 .7%

サイバーセキュリティ成熟度のプロファイル

サイバーセキュリティ成熟度評価 – インド



サイバーセキュリティ戦略を主導しているのは誰か？

CISO：34%、CIO/CTO：34%、グループで責任を共有／その他：32%

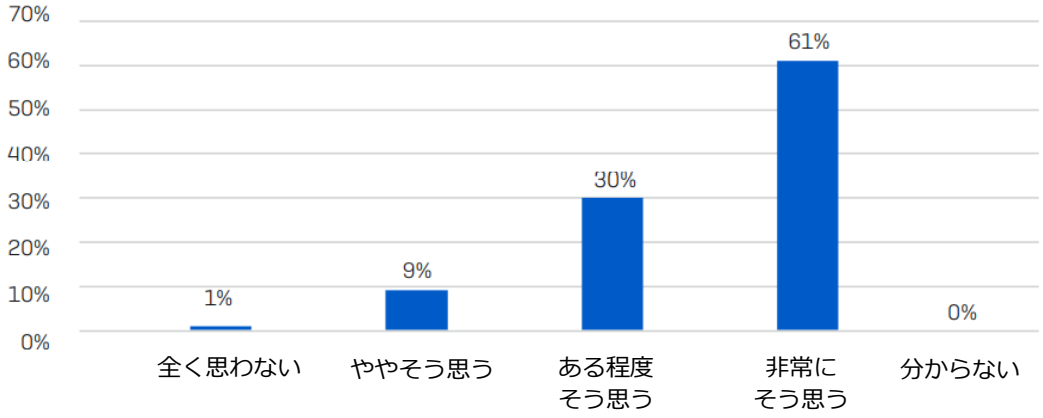
サイバーセキュリティプロフェッショナルの上位のフラストレーション

1. 経営陣は、サイバーセキュリティは簡単に実現できるもので、私を含む他のサイバーセキュリティ関係者が脅威や問題を誇張していると考えている
2. 「恐怖と疑念」を与えるメッセージが多すぎるため、サイバーセキュリティについて正確に議論することが難しい
3. サイバーセキュリティの優先順位を下げられることが多い

サイバーセキュリティに関する経営幹部レベルの理解

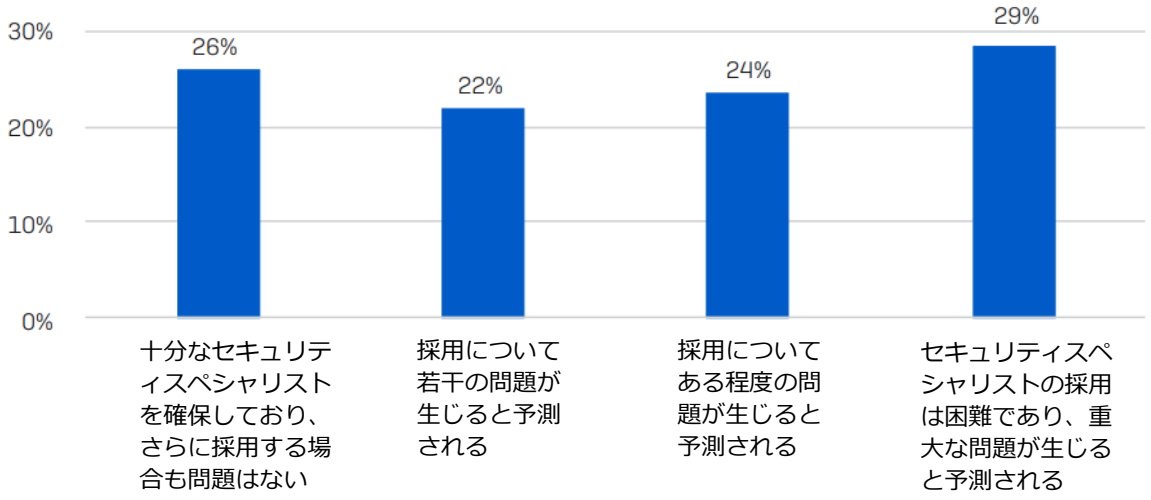
セキュリティについての経営幹部の理解度 – インド

あなたの会社の経営幹部は、サイバーセキュリティの問題をどの程度理解していると思いますか？



サイバーセキュリティプロフェッショナルの採用の難易度

自社組織でスキルを有するセキュリティ人材の今後 24 か月間の採用について、どのように考えていますか。インド



需要の高い上位スキル：

1. クラウドセキュリティポリシー/アーキテクチャの知識
2. ソフトウェア脆弱性テスト
3. 従業員と経営幹部のトレーニング

最も多い攻撃手法：

1. フィッシングとホエーリング
2. 脆弱な認証情報または認証情報の侵害
3. ソーシャルエンジニアリング

2022 年の重大な脅威：

1. マルウェア
2. 悪意のある従業員
3. サードパーティによるミス
4. 設計に問題があるシステム
5. フィッシングとホエーリング

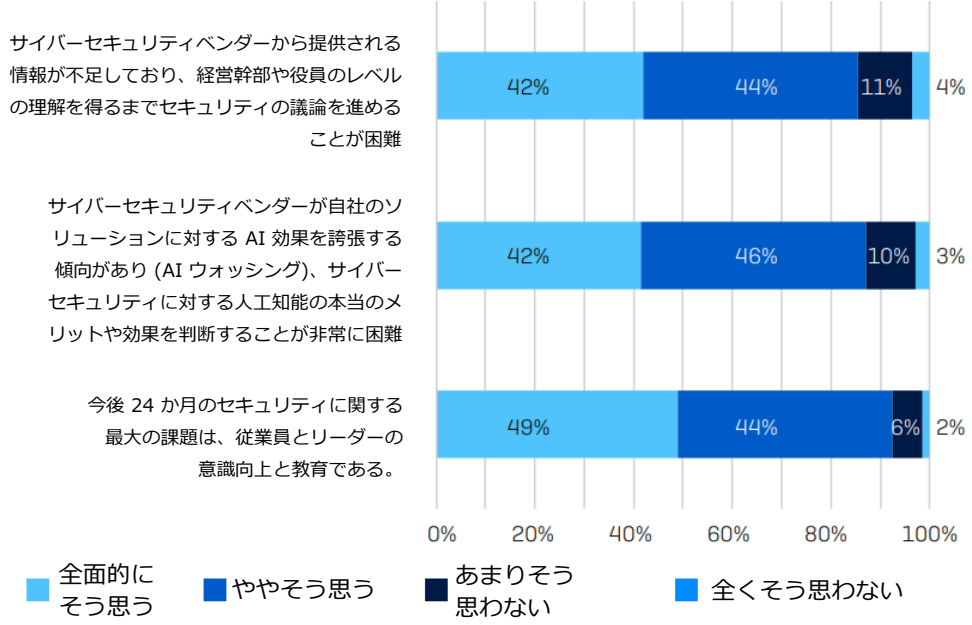
重大な脅威 2021～2022 年

2021	2022
マルウェア	マルウェア
フィッシングとホエーリング	悪意のある従業員
バックドア	サードパーティによるミス
AI/ML 攻撃	設計に問題があるシステム
ランサムウェア	フィッシングとホエーリング
国家による攻撃	暗号化バックドア
設計に問題があるシステム	ソーシャルエンジニアリング
悪意のある従業員	企業スパイ
ゼロデイ脆弱性	AI/ML 攻撃
ソーシャルエンジニアリング	ゼロデイ脆弱性
企業スパイ	従業員によるミス
従業員によるミス	国家による攻撃
パートナー/サードパーティによるミス	DDoS
DDoS	ランサムウェア

脅威ハンティングの導入：

54% の企業が自社で脅威ハンティングを実施し、41% が外部パートナーのサービスを利用、6% は実施していない/わからない

次の文章について、どの程度同意しますか – インド

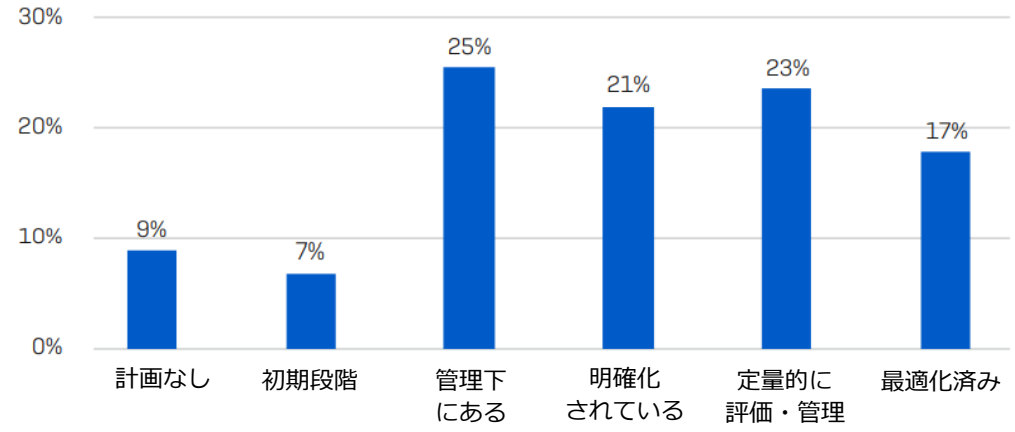


日本におけるサイバーセキュリティ

テクノロジー予算全体に占めるサイバーセキュリティの支出の割合：12 .3%

サイバーセキュリティ成熟度のプロファイル

サイバーセキュリティ成熟度評価 – 日本



サイバーセキュリティ戦略を主導しているのは誰か？

CISO：32%、CIO/CTO：33%、グループで責任を共有／その他：35%

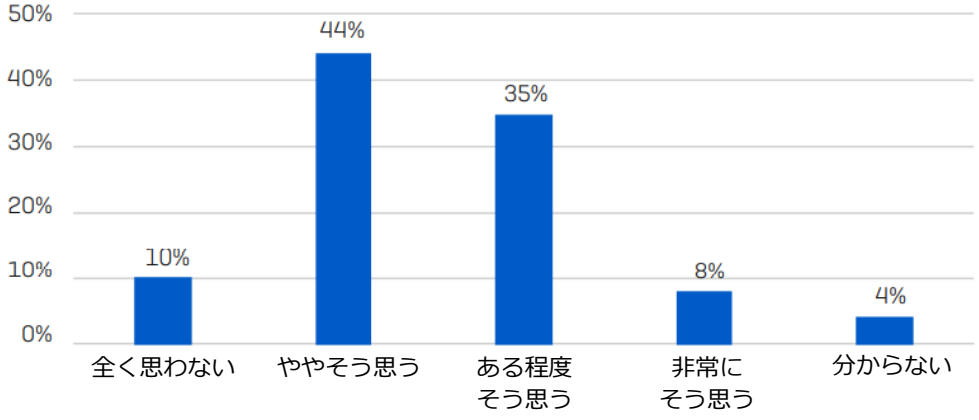
サイバーセキュリティプロフェッショナルの上位のフラストレーション

1. スキルを持ったセキュリティプロフェッショナルを十分に雇用できない
2. セキュリティ脅威のスピードに追いつけない
3. 「恐怖と疑念」を与えるメッセージが多すぎるため、サイバーセキュリティについて正確に議論することが難しい

サイバーセキュリティに関する経営幹部レベルの理解

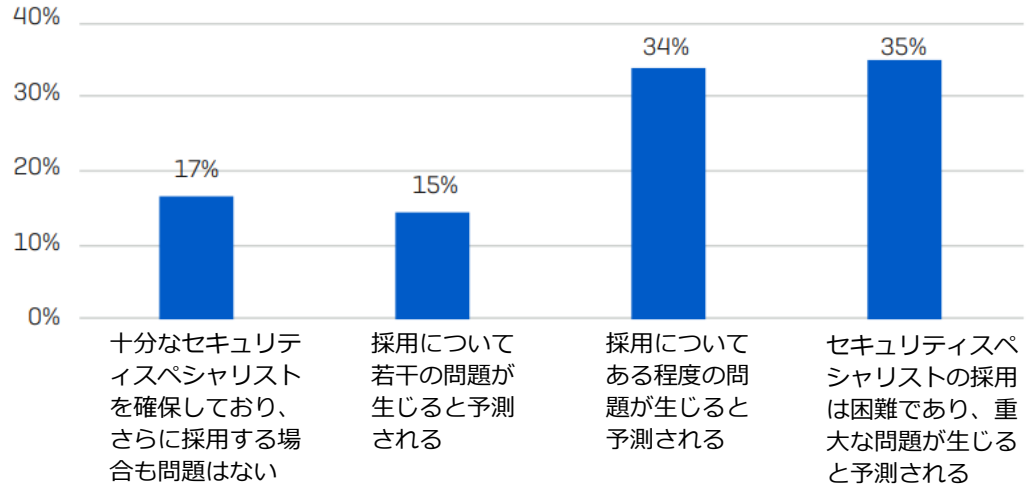
セキュリティについての経営幹部の理解度 – 日本

あなたの会社の経営幹部は、サイバーセキュリティの問題をどの程度理解していると思いますか？



サイバーセキュリティプロフェッショナルの採用の難易度

自社組織でスキルを有するセキュリティ人材の今後 24 か月間の採用について、どのように考えていますか。日本



需要の高い上位スキル：

1. 従業員と経営幹部のトレーニング
2. ソフトウェア脆弱性テスト
3. 最新の脅威情報を常に取り入れること

最も多い攻撃手法：

1. フィッシングとホエーリング
2. 未修正の脆弱性
3. サプライチェーンの脆弱性

2022 年の重大な脅威：

1. フィッシングとホエーリング
2. 悪意のある従業員
3. 従業員によるミス
4. ランサムウェア
5. 企業スパイ

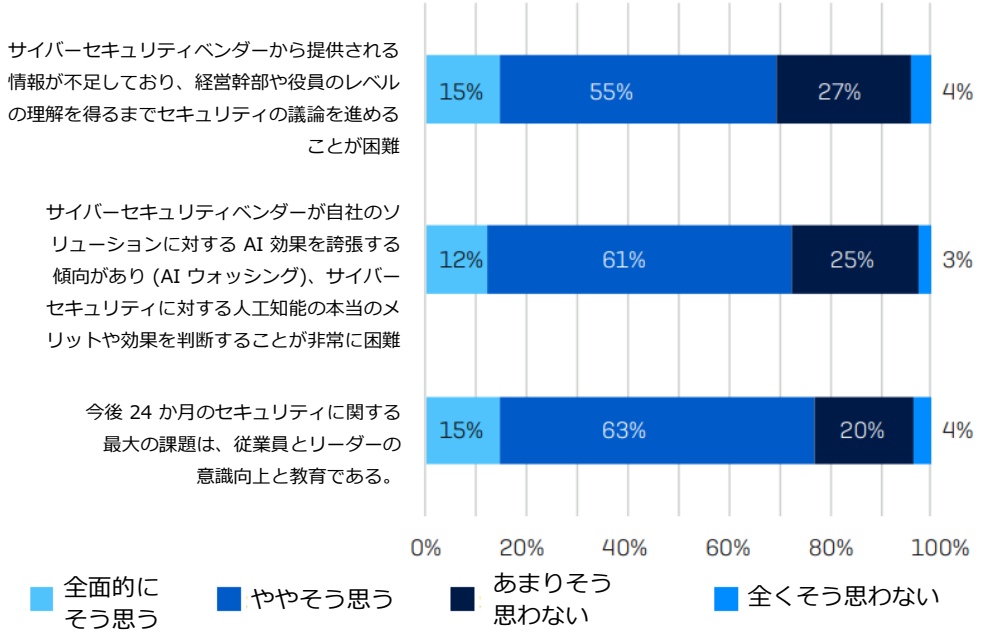
重大な脅威 2021～2022 年

2021	2022
従業員によるミス	フィッシングとホエーリング
悪意のある従業員	悪意のある従業員
設計に問題があるシステム	従業員によるミス
ランサムウェア	ランサムウェア
マルウェア	企業スパイ
フィッシングとホエーリング	マルウェア
DDoS	設計に問題があるシステム
バックドア	AI/ML 攻撃
パートナー/サードパーティによるミス	ゼロデイ脆弱性
国家による攻撃	国家による攻撃
企業スパイ	サードパーティによるミス
ゼロデイ脆弱性	暗号化バックドア
AI/ML 攻撃	DDoS
ソーシャルエンジニアリング	ソーシャルエンジニアリング

脅威ハンティングの導入：

27% の企業が自社で脅威ハンティングを実施し、52% が外部パートナーのサービスを利用、23% は実施していない/わからない

次の文章について、どの程度同意しますか – 日本

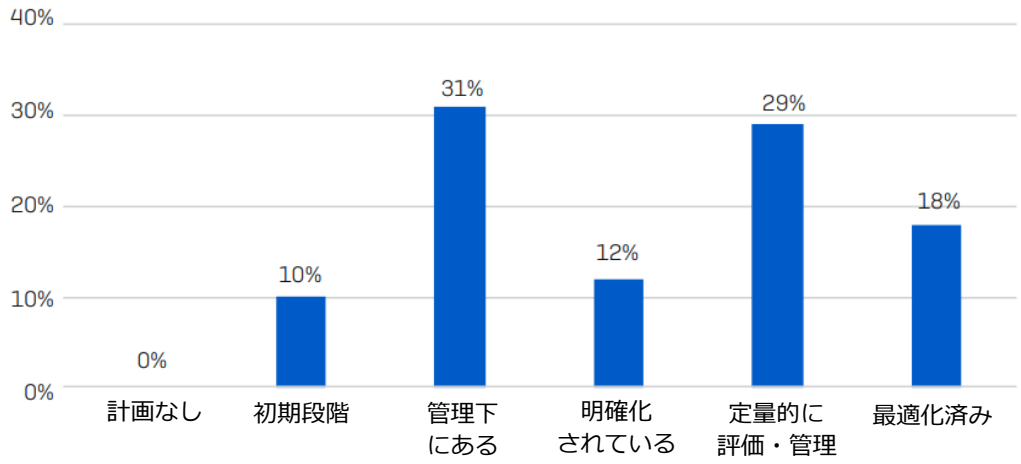


マレーシアのサイバーセキュリティ

テクノロジー予算全体に占めるサイバーセキュリティの支出の割合：8 .6%

サイバーセキュリティ成熟度のプロファイル

サイバーセキュリティ成熟度評価 – マレーシア



サイバーセキュリティ戦略を主導しているのは誰か？

CISO：35%、CIO/CTO：38%、グループで責任を共有／その他：27%

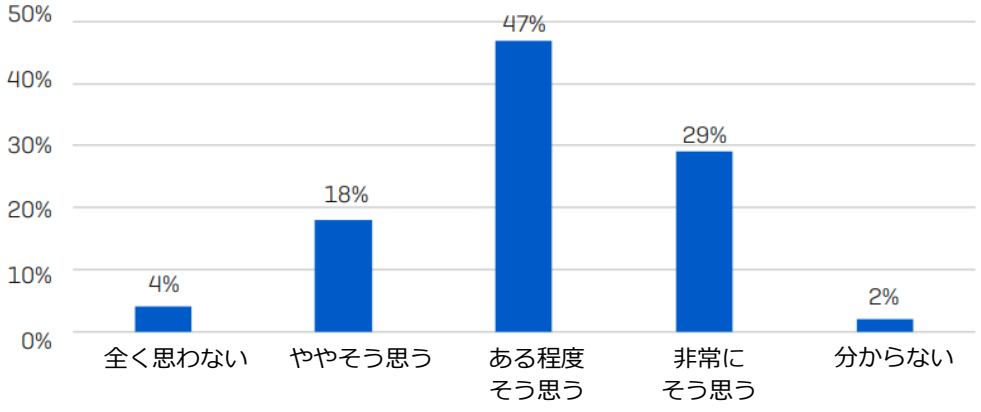
サイバーセキュリティプロフェッショナルの上位のフラストレーション

1. セキュリティ脅威のスピードに追いつけない
2. スキルを持ったセキュリティ専門家を十分に雇用できない
3. IT 以外のスタッフのトレーニングに十分な投資も時間もかけられていない

サイバーセキュリティに関する経営幹部レベルの理解

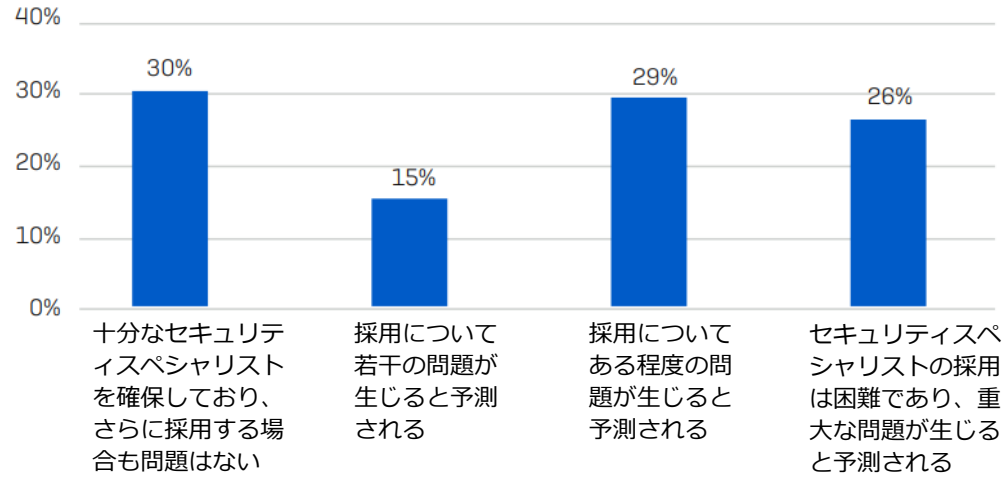
セキュリティについての経営幹部の理解度 – マレーシア

「あなたの会社の経営幹部は、サイバーセキュリティの問題をどの程度理解していると思いますか？」



サイバーセキュリティプロフェッショナルの採用の難易度

自社組織でスキルを有するセキュリティ人材の今後 24 か月間の採用について、どのように考えていますか。マレーシア



需要の高い上位スキル：

1. 最新の脅威情報を常に取り入れること
2. ポリシーの遵守と報告
3. 従業員と経営幹部のトレーニング

最も多い攻撃手法

1. フィッシングとホエーリング
2. 悪意のある従業員
3. サプライチェーンの脆弱性

2022 年の重大な脅威：

1. マルウェア
2. 悪意のある従業員
3. 従業員によるミス
4. ランサムウェア
5. 企業スパイ

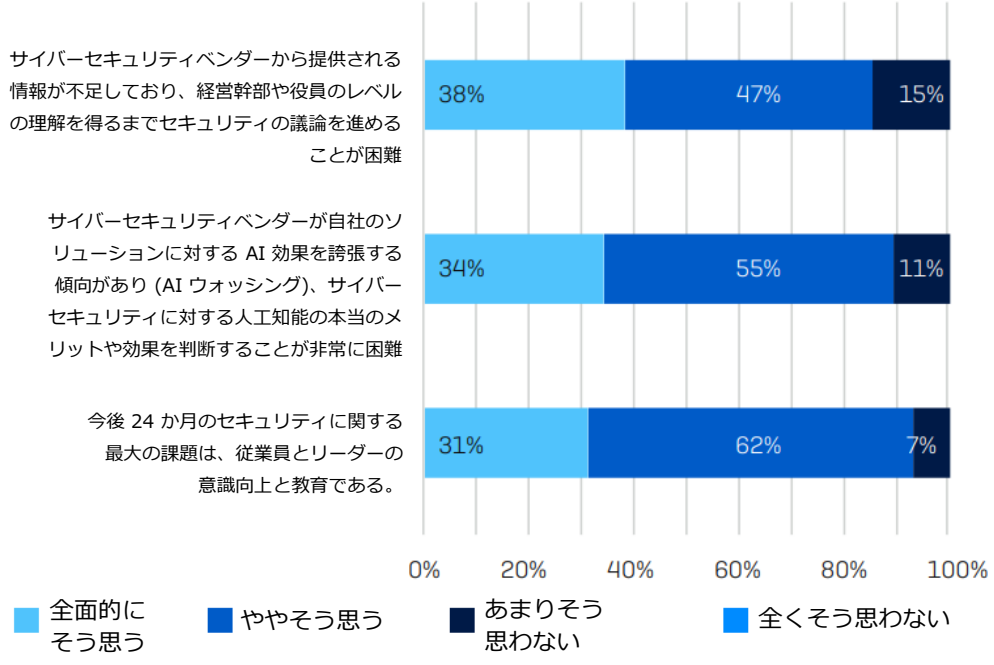
重大な脅威 2021～2022 年

2021	2022
フィッシングとホエーリング	マルウェア
ランサムウェア	悪意のある従業員
マルウェア	従業員によるミス
悪意のある従業員	ランサムウェア
AI/ML 攻撃	企業スパイ
ソーシャルエンジニアリング	暗号化バックドア
DDoS	フィッシングとホエーリング
バックドア	AI/ML 攻撃
設計に問題があるシステム	ゼロデイ脆弱性
ゼロデイ脆弱性	設計に問題があるシステム
企業スパイ	サードパーティによるミス
従業員によるミス	国家による攻撃
パートナー/サードパーティによるミス	DDoS
国家による攻撃	ソーシャルエンジニアリング

脅威ハンティングの導入：

20% の企業が自社で脅威ハンティングを実施し、60% が外部パートナーのサービスを利用、20% は実施していない/わからない

次の文章について、どの程度同意しますか – マレーシア

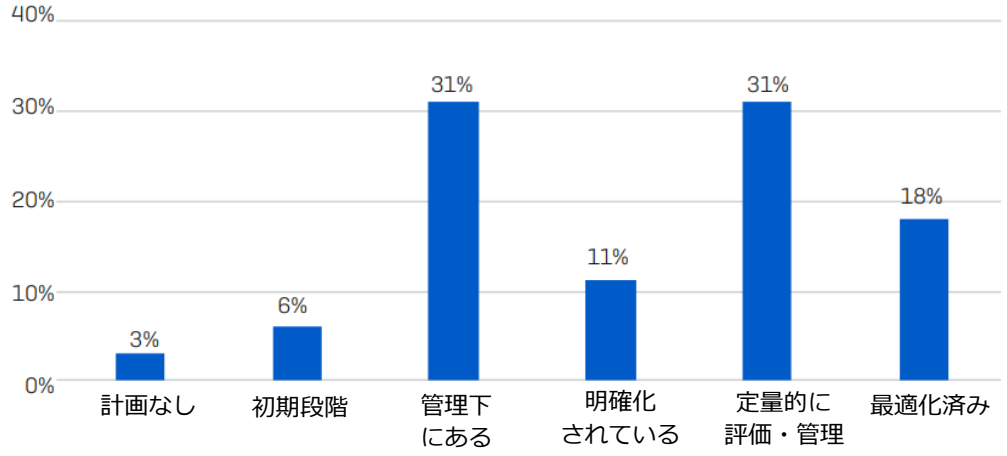


フィリピンのサイバーセキュリティ

テクノロジー予算全体に占めるサイバーセキュリティの支出の割合：13 .3%

サイバーセキュリティ成熟度のプロファイル

サイバーセキュリティ成熟度評価 – フィリピン



サイバーセキュリティ戦略を主導しているのは誰か？

CISO：33%、CIO/CTO：36%、グループで責任を共有／その他：31%

サイバーセキュリティプロフェッショナルの上位のフラストレーション

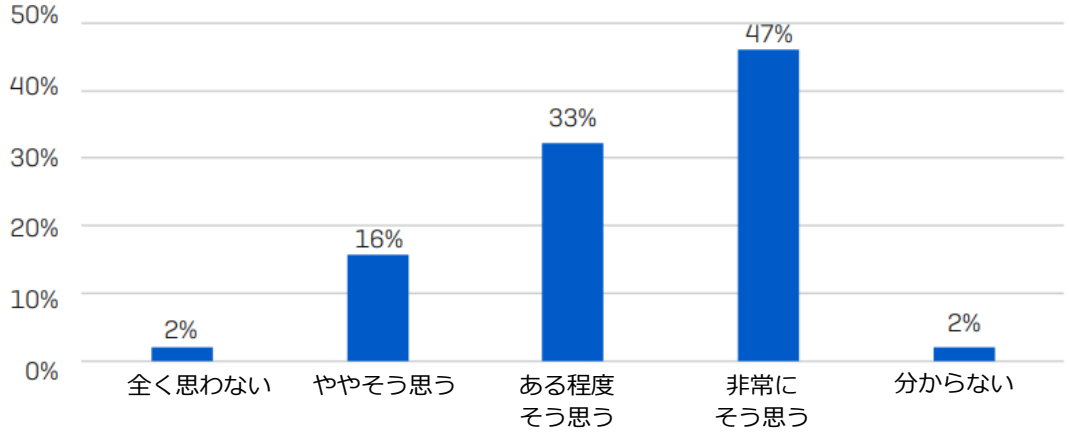
1. サイバーセキュリティの優先順位を下げられることが多い
2. 経営陣は、サイバーセキュリティは簡単に実現できるもので、私を含む他のサイバーセキュリティ関係者が脅威や問題を誇張していると考えている

3 .経営陣は自社が攻撃されることは決してないと考えている

サイバーセキュリティに関する経営幹部レベルの理解

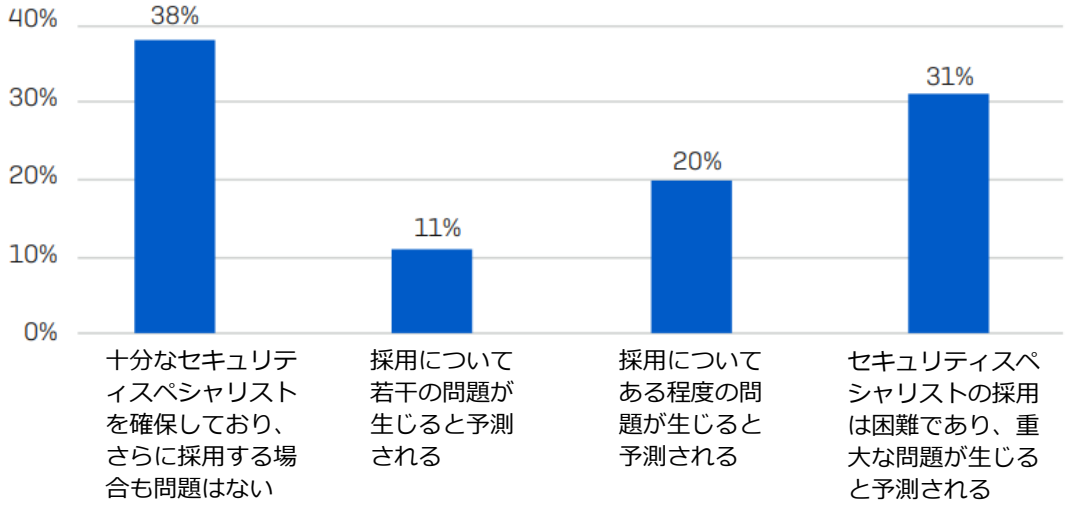
セキュリティについての経営幹部の理解度 – フィリピン

あなたの会社の経営幹部は、サイバーセキュリティの問題をどの程度理解していると思いますか？



サイバーセキュリティプロフェッショナルの採用の難易度

自社組織でスキルを有するセキュリティ人材の今後 24 か月間の採用について、どのように考えていますか。フィリピン



需要の高い上位スキル：

1. クラウドセキュリティポリシー/アーキテクチャの知識
2. ソフトウェア脆弱性テスト
3. 最新の脅威情報を常に取り入れること

最も多い攻撃手法：

1. フィッシングとホエーリング
2. 脆弱な認証情報または認証情報の侵害
3. 悪意のある従業員

2022 年の重大な脅威：

1. フィッシング
2. 設計に問題があるシステム
3. マルウェア
4. 暗号化バックドア
5. AI/ML 攻撃

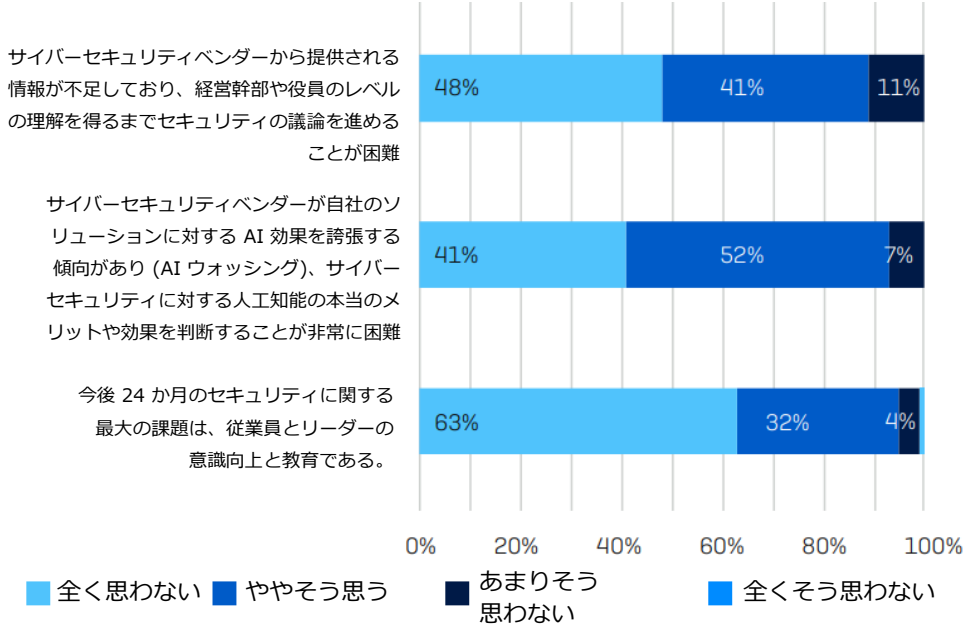
重大な脅威 2021～2022 年

2021	2022
フィッシングとホエーリング	フィッシングとホエーリング
マルウェア	設計に問題があるシステム
ランサムウェア	マルウェア
企業スパイ	暗号化バックドア
悪意のある従業員	AI/ML 攻撃
AI/ML 攻撃	企業スパイ
脆弱なシステム	悪意のある従業員
従業員によるミス	従業員によるミス
パートナー/サードパーティによるミス	国家による攻撃
ゼロデイ脆弱性	DDoS
バックドア	ソーシャルエンジニアリング
ソーシャルエンジニアリング	ゼロデイ脆弱性
国家による攻撃	サードパーティによるミス
DDoS	ランサムウェア

脅威ハンティングの導入：

24% の企業が自社で脅威ハンティングを実施し、69% が外部パートナーのサービスを利用、8% は実施していない/わからない

次の文章について、どの程度同意しますか – フィリピン

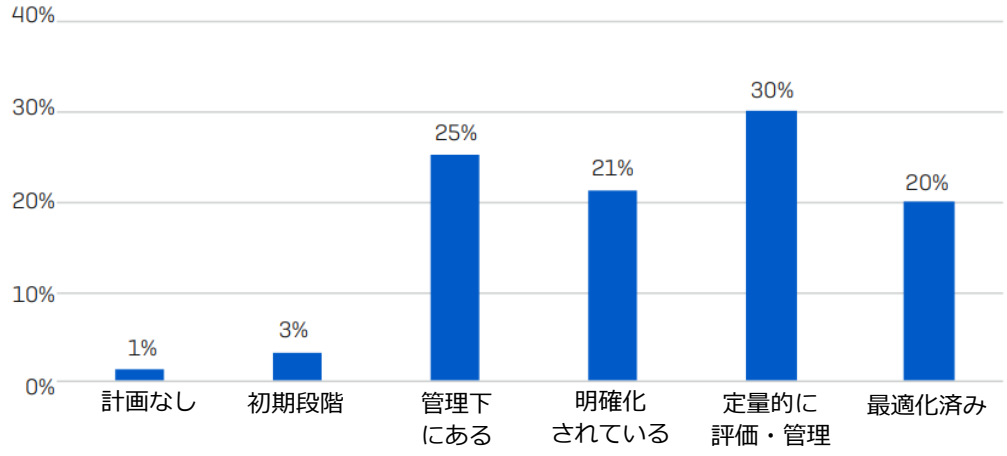


シンガポールにおけるサイバーセキュリティ

テクノロジー予算全体に占めるサイバーセキュリティの支出の割合：11 .23%

サイバーセキュリティ成熟度のプロファイル

サイバーセキュリティ成熟度評価 – シンガポール



サイバーセキュリティ戦略を主導しているのは誰か？

CISO：33%、CIO/CTO：36%、グループで責任を共有／その他：31%

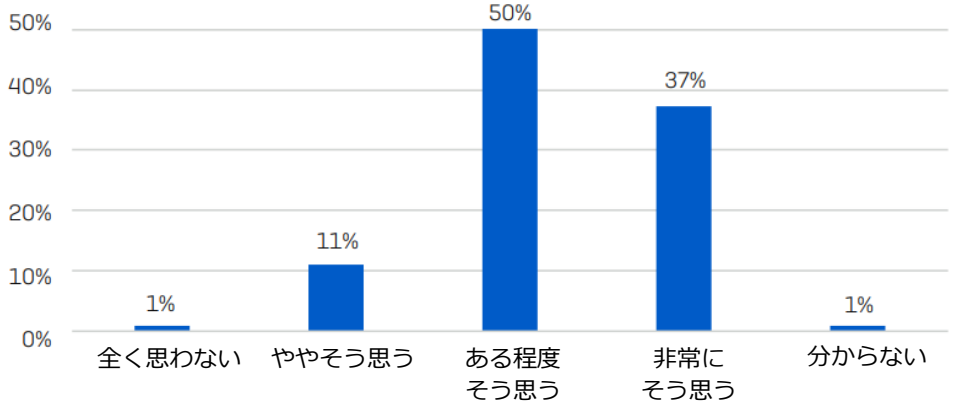
サイバーセキュリティプロフェッショナルの上位のフラストレーション

1. 経営陣は、サイバーセキュリティは簡単に実現できるもので、私を含む他のサイバーセキュリティ関係者が脅威や問題を誇張していると考えている
2. 「恐怖と疑念」を与えるメッセージが多すぎるため、サイバーセキュリティについて正確に議論することが難しい
3. サイバーセキュリティの優先順位を下げられることが多い

サイバーセキュリティに関する経営幹部レベルの理解

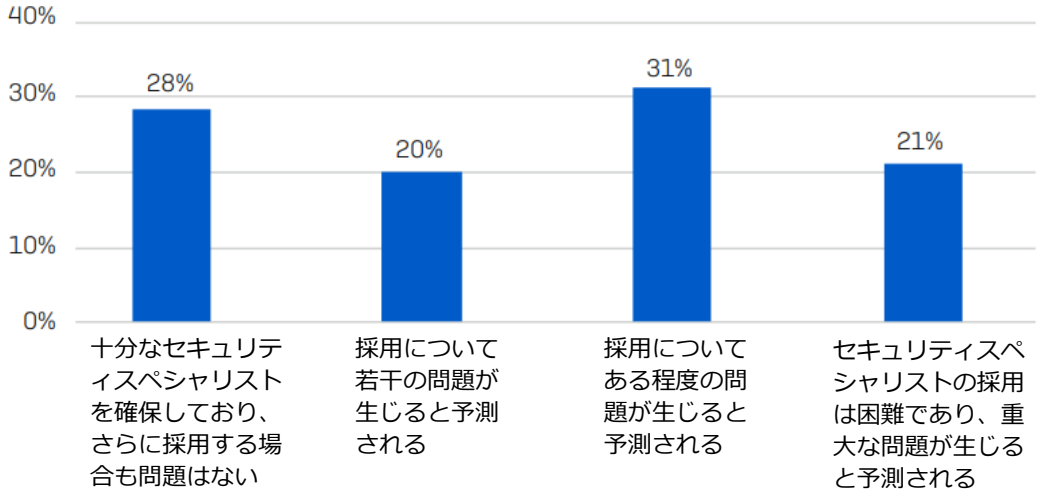
セキュリティについての経営幹部の理解度 – シンガポール

あなたの会社の経営幹部は、サイバーセキュリティの問題をどの程度理解していると思いますか？



サイバーセキュリティプロフェッショナルの採用の難易度

自社組織でスキルを有するセキュリティ人材の今後 24 か月間の採用について、どのように考えていますか。シンガポール



需要の高い上位スキル

1. クラウドセキュリティポリシー/アーキテクチャの知識
2. ソフトウェア脆弱性テスト
3. 最新の脅威情報を常に取り入れること

最も多い攻撃手法：

1. フィッシングとホエーリング
2. 構成ミス
3. 中間者攻撃

最も重大な脅威

1. マルウェア
2. フィッシング
3. DDoS
4. ソーシャルエンジニアリング
5. ランサムウェア

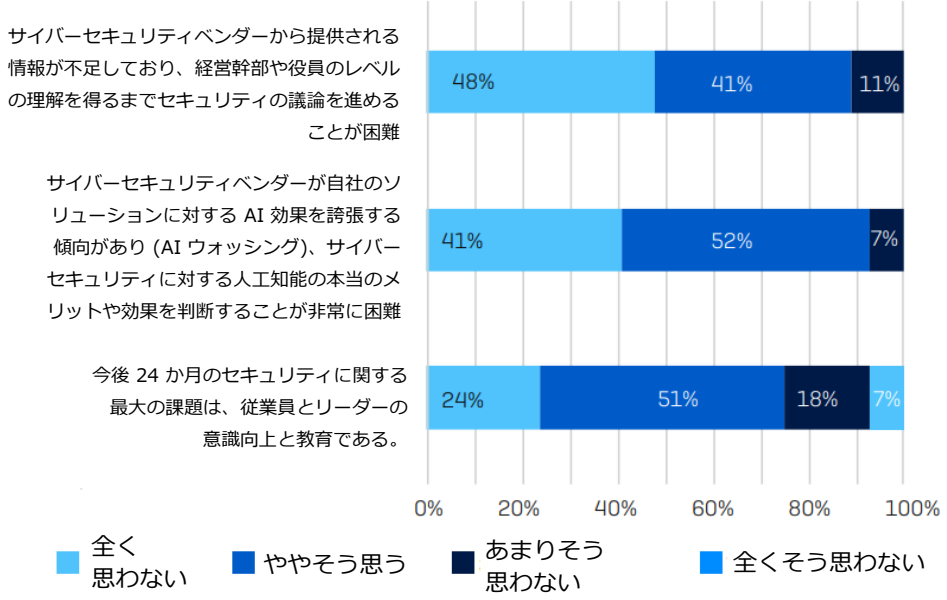
重大な脅威 2021～2022 年

2021	2022
ランサムウェア	マルウェア
悪意のある従業員	フィッシングとホエーリング
AI/ML 攻撃	DDoS
マルウェア	ソーシャルエンジニアリング
バックドア	ランサムウェア
フィッシングとホエーリング	国家による攻撃
国家による攻撃	企業スパイ
ゼロデイ脆弱性	従業員によるミス
企業スパイ	サードパーティによるミス
設計に問題があるシステム	悪意のある従業員
DDoS	設計に問題があるシステム
従業員によるミス	暗号化バックドア
パートナー/サードパーティによるミス	ゼロデイ脆弱性
ソーシャルエンジニアリング	AI/ML 攻撃

脅威ハンティングの導入：

23% の企業が自社で脅威ハンティングを実施し、61% が外部パートナーのサービスを利用、16% は実施していない/わからない

次の文章について、どの程度同意しますか - シンガポール



ソフォスの見解

TRA が発表した最新の調査結果は、今年になって潮目が変わり、APJ の組織が以前よりもサイバーセキュリティを真剣に受け止めていることを示しています。この考え方が今後の「ニューノーマル」になることが望まれます。

「サイバーセキュリティに真剣に取り組んでいない」と考える外部の人間を一蹴したくなるかもしれませんが、歴史的にはそれが現実でした。そして、多くの組織がサイバーセキュリティ成熟度チャートのランキングを上げるようになったことから、改善が切実に求められていたこと、そして実際に改善の余地があったことは明らかです。

しかし、その自己評価の成熟度は、説明のつかない問題が発生した場合の対応準備にどれだけつながるでしょうか。

評価や自己評価はともかく、実際のセキュリティインシデントに直面したときに、自社のサイバーレジリエンスを実践し、検証している組織はごくわずかです。

「誰にでも作戦 (計画) はある、鼻にパンチを食らうまでは。」

TRA の調査結果から、計画を持っている組織であっても、深刻な攻撃シナリオに対するテストを十分に行っていない可能性があることがわかります。実際にインシデントが発生した際に、計画や対応がその場しのぎになってしまったケースもあります。また、ランサムウェア攻撃を受けたデスクトップやサーバー上に保存されていたために、計画書を回収できないこともあります。

このようなサイバーレジリエンスの課題の多くは、脅威に対する理解不足、および組織内のサイバーセキュリティの役割と責任の多様化に起因しています。アジア太平洋地域の企業がサイバーインシデントに備えて適切な計画を立てることができない主な理由は、サイバー問題がどれほどの利益の損失をもたらすのかを経営幹部が理解していないことにあります。

ドアを開けたままにしないでください。高い確率で攻撃者に悪用されてしまいます。

ProxyShell や Log4J などを悪用し、企業データを盗み出したり恐喝の手口を用いたりすることで、攻撃者が深刻な影響を及ぼす脆弱性が大々的に悪用したり、あらゆる業種・規模の企業に大打撃を与えるのを私達は目撃してきました。
しかし、私たちが回避すべきなのは、大きなゼロデイ脆弱性だけではありません。基本的なサイバーセキュリティを維持することは、今なお多くの組織にとって困難です。なぜなら、アプリケーションやオペレーティングシステムにパッチが適用されていないため、攻撃が容易に展開され、サイバー犯罪グループは単純なフィッシングや認証情報収集を実行するだけで広範にアクセスできてしまうからです。

こうした非常に複雑で根深い問題を解決してくれるソリューションは、一夜にして見つけられるものではありません。また、1 つのソフトウェアやポリシーコントロールがすべての問題を解決してくれるわけではありません。フィッシングやユーザーとのやり取りなど、人的要素が絡むと、攻撃者は正面から堂々と侵入しやすくなります。毎日のように直面する脅威とその対処法を理解することは、あなたが経営幹部であるか郵便仕分け担当者であるかにかかわらず、組織を守る上で不可欠です。つまり、社内への侵入を試みる犯罪者を発見して対処する方法について、誰もが同じレベルの見識を身につけ、トレーニングを受ける必要がある、というのが結論です。

サイバーセキュリティの役割と責任の多様化という点について言うと、セキュリティコントロールは建前上は自律的であっても、実際は技術的なものです。このような極めて技術的なコントロールを理解し、重要項目を実行するためには、専門知識が必要です。だからこそ、さまざまなスキルを持つ多様なチームがサイバーレジリエンスを担当することで、インシデント発生時の対応が強化されます。

理解力と多様性の向上に取り組むことで、あなた自身、従業員、会社、そして最も大切にしている情報に侵入してくる前に攻撃を検出・対処できるようになります。

付録

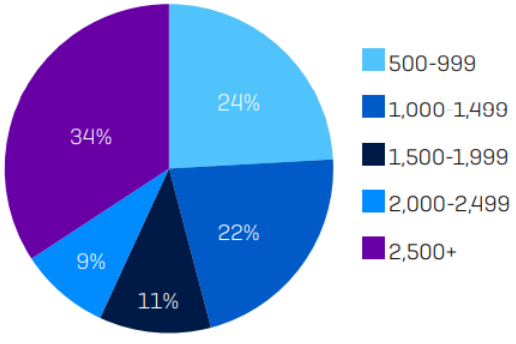
サイバーセキュリティ成熟度モデルの定義:

- 計画なし (No plan): 文字通り、サイバーセキュリティの機能を導入していない。
- アドホック (Ad-hoc): 特定のプロジェクトやイニシアティブにはリアクティブ (事後) に対応するが、活動を管理するための全体的な戦略はない。
- 実環境ではテストしていない (Untested in real life): 組織、グループ、または部門内にまだ導入されていない理論上の計画。
- 管理下にある (Managed): プロジェクトと活動が計画的に実施され、進捗を追跡するための基本的なパフォーマンス、測定、およびコントロールが行われることを保証する基本レベルの戦略。
- 明確化されている (Defined): リアクティブではなくプロアクティブで、かつ組織全体を対象とする機能。調和のとれたプログラムの中のプロジェクトと活動に対して適切な助言が与えられる。
- 定量的: 機能、パフォーマンス、およびアセスメントは評価基準ベースで、企業のサイバーセキュリティ戦略と目標に合わせて定量化された目標が設定されている。
- 最適化済み (Optimised): 変化に適応する実証済みの機能を備えた継続的な改善サイクルに焦点を当てている。

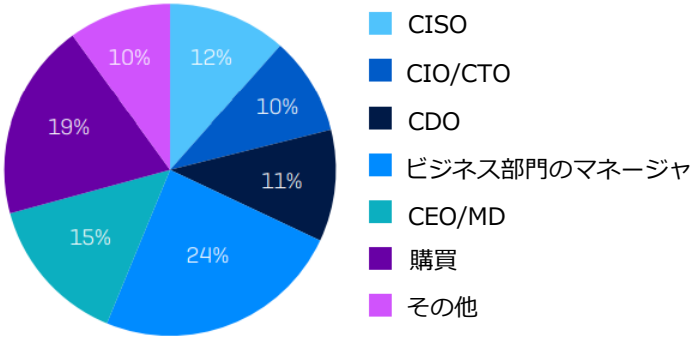
回答者の内訳と調査方法

ソフォスは 2022 年　1 月に Tech Research Asia (TRA) に委託して、アジア太平洋および日本のサイバーセキュリティ環境に関する調査を実施しました。これには、マレーシア、フィリピン、シンガポールでそれぞれ 100 社、オーストラリア、インド、日本でそれぞれ 200 社の合計 900 社からの回答を収集した大規模な定量調査が含まれます。

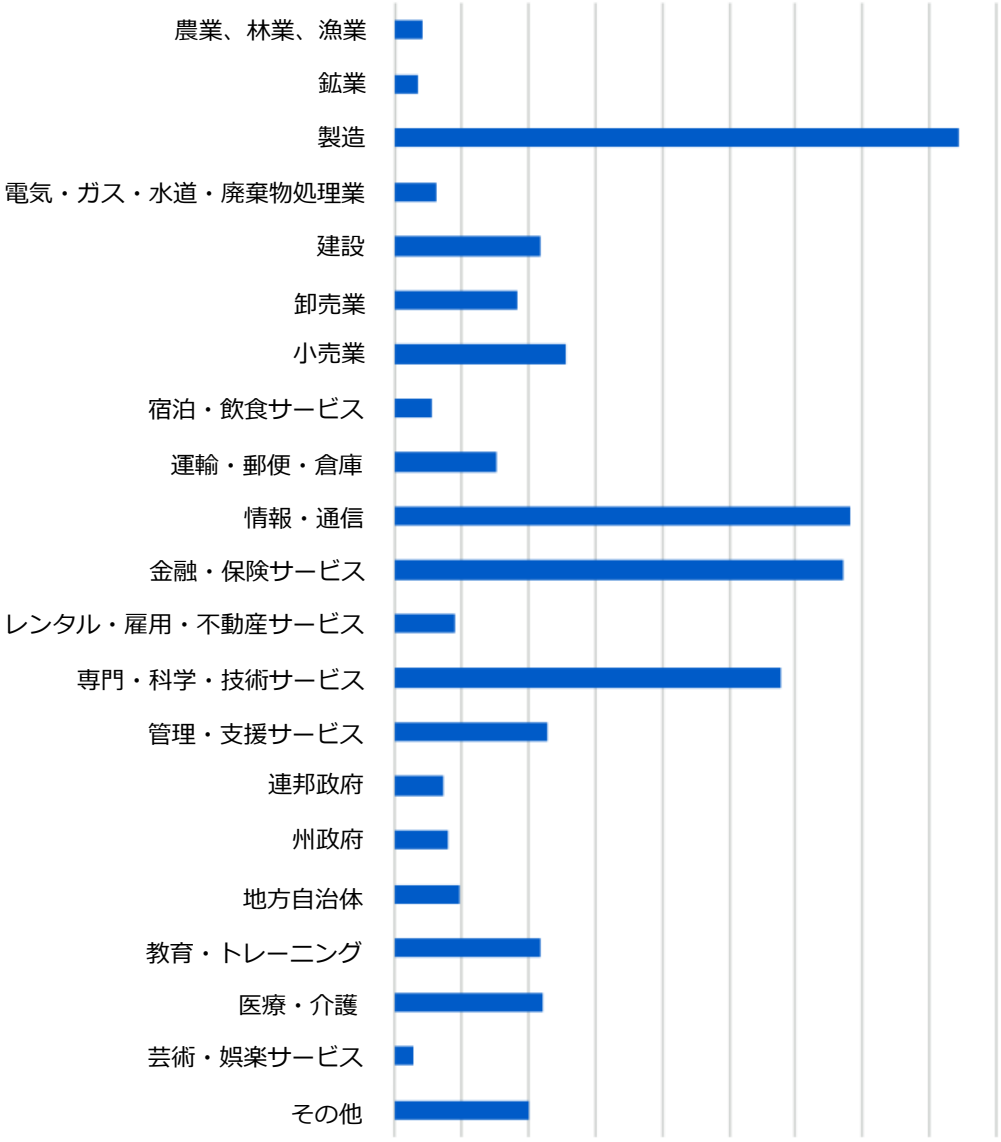
従業員数



役職



業界



ソフォスについて

ソフォスは、次世代エンドポイントおよびネットワークセキュリティのリーダー企業であり、現在の最も高度なサイバー攻撃の脅威から 150 か国以上の 50 万の組織と 1 億人を超えるユーザーを保護しています。SophosLabs と SophosAI の脅威インテリジェンス、AI、機械学習を活用し、ランサムウェア、マルウェア、エクスプロイト、フィッシング、その他のさまざまなサイバー攻撃からユーザー、ネットワーク、エンドポイントを保護するための高度な製品およびサービスの幅広いポートフォリオを提供しています。ソフォスは、クラウドベースの統合型管理コンソールである Sophos Central を提供しています。Sophos Central は、適応型サイバーセキュリティエコシステムの中核となっており、一元的なデータレイクを提供しています。顧客、パートナー、開発者、他のサイバーセキュリティベンダーは豊富なオープン API セットを活用して、このデータレイクを利用できます。ソフォスは、世界各国のリセラーパートナーや MSP (マネージドサービスプロバイダー) から製品およびサービスを販売しています。ソフォスの本社は英国オックスフォードにあります。詳細については、www .sophos .comをご覧ください。

Tech Research Asia について

TRA は、シドニー、メルボルン、シンガポール、クアラルンプール、香港、東京に経験豊富で多様なチームを有し、急成長を続ける IT アナリスト、リサーチ、コンサルティングの企業です。アジア太平洋地域でエグゼクティブレベルのテクノロジーの買い手とサプライヤーにアドバイスを提供します。TRA のアプローチは厳格で、事実に基づき、オープンで、透明です。リサーチ、コンサルティング、エンゲージメント、アドバイザリーの各種サービスを提供します。また、
最新のテクノロジーを活用したいと考えるエグゼクティブなどのリーダーたちにとって重要な課題、トレンド、および戦略に関する TRA 独自のリサーチも実施しています。TRA はまた、オープンなオンラインジャーナル 『TQ』を発行しています。

www.techresearch.asia

2022-03-31 (WP-NP)