SOPHOS

アジア太平洋地域のサイバーセキュリティの展望

第 4 版、2024 年 2 月
ソフォスの委託による TRA Report

本レポートでは、アジア太平洋地域と日本におけるサイバーセキュリティの燃え尽き症候群とセキュリティ疲れ、そしてこれらが従業員と組織に与える影響について主に解説します。

A Sophos Whitepaper. February 2024

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 4 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、日本、オーストラリア、インド、マレーシア、フィリピン、シンガポールの企業が直面するサイバーセキュリティの問題を調査した結果をお伝えしてきました。

前回のレポートでは、企業におけるサイバーセキュリティの成熟度、取締役会レベルのサイバーセキュリティに対する理解、サイバーセキュリティプログラムの成功を妨げる一般的な要因、サイバーセキュリティ環境を管理するその他の実践的な取り組みなどについて主に取り上げました。

今回のレポートの内容は大きく異なり、サイバーセキュリティ燃え尽き症候群やセキュリティ疲れ、そして、これらの問題が従業員と企業に与える影響を調査した結果に主にお伝えします。

ソフォスが実施した調査によると、サイバーセキュリティチームや IT プロフェショナルが強力なセキュリティ対策を継続的に実行する能力を低下させる要因として、攻撃の頻度、アラート疲れ、教育やトレーニングに対する社内での苦悩や葛藤、さらに取締役会や管理職からの要求の高まりがあることが明らかになりました。

サイバーセキュリティにおけるさまざまな運用業務に携わる従業員が燃え尽き症候群に陥っており、その割合も増加傾向にあります。30% の組織が、燃え尽き症候群について過去 1 年間に「著しく」増加したと回答し、41% のプロフェショナルが、燃え尽き症候群がサイバーセキュリティの職務を遂行する「気力と能力を減退させている」と回答しています。

その他の重要な調査結果を以下に示します。

- 回答した企業の 75% がサイバーセキュリティを専門とするチームを有しており、5% の企業がサイバーセキュリティ業務をサードパーティー企業に完全にアウトソーシングしている。
- サイバーセキュリティと IT のプロフェショナルは、取締役会とシニアリーダーシップチーム (SLT) がサイバーセキュリティに関する理解が十分ではないと感じている (取締役会の理解が不十分という回答は 49%、SLT の理解が不十分という回答は 46%)。
- ただし、これらのグループの 95% が、規制やその他の法的要件の厳格化により、サイバーセキュリティ対策を強化している。
- 取締役会の 60% と半数の SLT がサイバーセキュリティに関する最新情報を定期的に得ていない。
- サイバーセキュリティと IT プロフェショナルの 81% が、他社のサービスを利用しているときに個人のデータが漏えいした経験がある。
- 個人のデータが侵害された経験から、現在働いている会社でもデータ侵害が必然的に発生するのではないかなどの懸念が高まり、ストレスが増大するなど、直接的な影響を受けている。
- 継続的にトレーニングや教育キャンペーンを受けているにもかかわらず、SLT の 41%、従業員の 38%、取締役会の 28% が、サイバーセキュリティ対策で基本的なミスを繰り返し犯している。
- 84% の企業がインシデント対応計画とセキュリティ侵害時のコミュニケーション計画を策定しているが、その有効性については懐疑的である。29% の企業が、攻撃や侵入を受けた場合の対応が「乱雑」と回答し、26% の企業は「プロフェッショナルとして優れた対応を行っている」と回答している。
- これらの計画の 75% は、セキュリティ侵害の発生後や攻撃を受けた後に策定された。

データ調査の詳細については、付録の「アンケート回答者の内訳と調査方法」を参照してください。

調査結果

この調査結果は以下の 5 つのセクションに分かれています。

1. サイバーセキュリティ燃え尽き症候群
2. 取締役会および経営幹部とサイバーセキュリティの関係
3. 全般的なサイバーセキュリティの環境
4. インシデント対応と復旧
5. サイバーセキュリティと IT プロフェッショナルが懸念およびフラストレーションを抱えている領域

サイバーセキュリティ燃え尽き症候群

燃え尽き症候群の広がり

85% の企業が、サイバーセキュリティと IT プロフェショナルはセキュリティ疲れと燃え尽き症候群を経験していると回答しており、ほぼ 4 人に 1 人 (23%) がこの問題を「頻繁に」経験し、62% が「時々」経験していると回答しています。

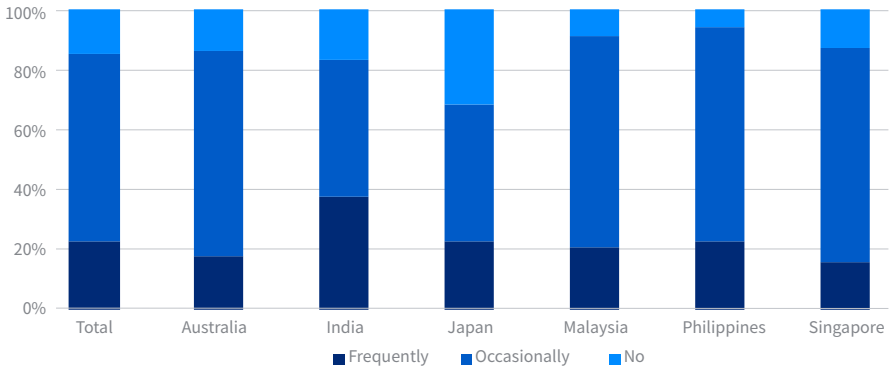
日本では燃え尽き症候群とセキュリティ疲れを経験する割合は 69% と低くなっており、調査対象国の平均を下回りました。日本のデータを除くと、オーストラリア、インド、マレーシア、フィリピン、シンガポールでは燃え尽き症候群を経験する割合は全組織の 80% 以上と高くなっています。

インドの組織の 37% が、燃え尽き症候群やセキュリティ疲れを「頻繁に経験している」と回答しており、平均 (23%) よりも大幅に高くなっています。フィリピン (94%) とマレーシア (91%) では 90% 以上の企業が燃え尽き症候群やセキュリティ疲れの影響を受けています。

燃え尽き症候群やセキュリティ疲れは増加傾向にあります。厄介なことに、90% の企業が過去 1 年間に燃え尽き症候群やセキュリティ疲れが増加したと回答しており、そのうち 30% は「大幅に増加した」と回答しています。

インド企業 (48%) と日本企業 (38%) は、過去 12 か月間に燃え尽き症候群とセキュリティ疲れが「大幅に増加した」割合が最も高く、フィリピン企業 (21%) とシンガポール企業 (18%) は、「大幅に増加した」割合が平均よりも低くなりました。

あなたやあなたの同僚 (サイバーセキュリティや IT 部門) は、サイバーセキュリティ疲れや燃え尽き症候群を経験したことがありますか？



サイバーセキュリティ燃え尽き症候群とセキュリティ疲れの影響

これらの影響は従業員と企業の両方に及びます。この調査では、サイバーセキュリティと IT の従業員、およびサイバーセキュリティ部門の管理者や監督者の両方から回答を得ており、両方のグループの状況を把握するようにしています。

最初に従業員の結果から見ていきましょう。

燃え尽き症候群とセキュリティ疲れが従業員に与える影響

アジア太平洋地域全体を見ると、サイバーセキュリティと IT に携わる従業員の約 90% が、燃え尽き症候群やセキュリティ疲れによる悪影響を受けています。自分の業務のパフォーマンスへの影響を感じていないと回答した従業員はわずか 10% でした。

90% の従業員がこれらの問題があると感じている結果は、深刻です。

多くの企業が、サイバーセキュリティのスキル不足と複雑化する脅威に苦しんでいる中で、従業員が安定して働くことができ、優れたパフォーマンスを挙げることは極めて重要です。燃え尽き症候群とセキュリティ疲れが、従業員の雇用の維持とパフォーマンスを阻害する要因になっています。今回のデータから、以下の状況が明らかになりました。

- 41% の従業員が、努力を継続できなくなっており、十分なパフォーマンスを発揮していないと感じている。
- 34% の従業員が、侵害や攻撃があった場合、不安が高まると感じている。
- 31% の従業員が、サイバーセキュリティ対策やその責務に対して、懐疑的、無関心、無気力のような感情を抱いている。
- 30% の従業員が、退職または転職したいと考えるようになったと回答している (調査対象者全体の 23% が、この問題によって実際に退職している)。
- 10% の従業員が、サイバーセキュリティ活動を支えるために自分が多くの役割を果たすことができないことに罪の意識を感じている。

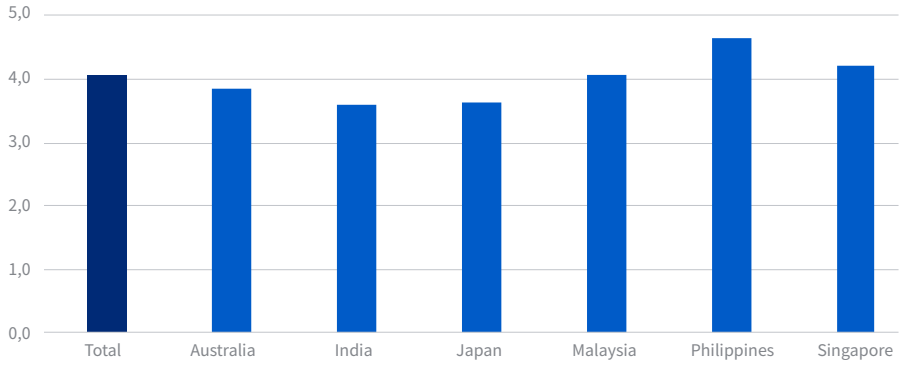
現在のセキュリティ環境を考えれば、従業員が罪の意識や不安を感じたり、無気力や無関心になったり、苦心したりして、業務に影響が出ることは決して不思議ではありません。

燃え尽き症候群とセキュリティ疲れがビジネスオペレーションに与える影響

燃え尽き症候群とセキュリティ疲れがビジネスオペレーションに影響を及ぼす主な分野には、以下の 4 つがあります。

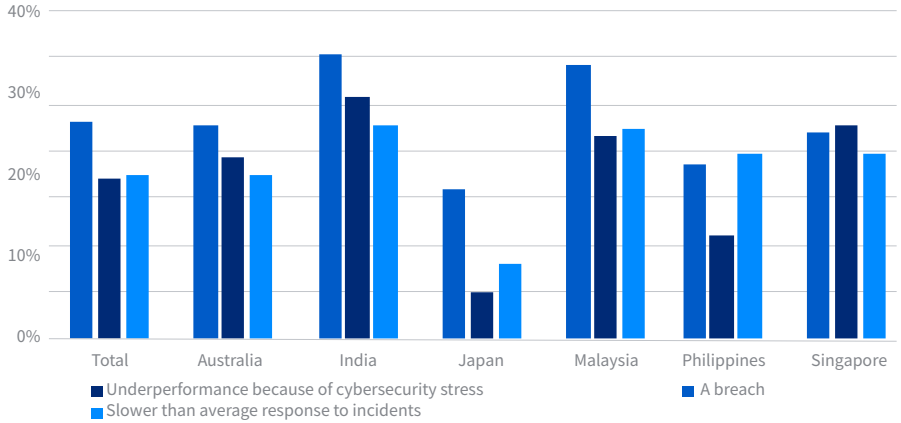
1. 生産性の低下：サイバーセキュリティと IT プロフェショナルの燃え尽き症候群とセキュリティ疲れによって、企業は平均して週に 4.1 時間の生産性の低下を経験しています。最も大きな影響を受けているのはフィリピン (4.6 時間 / 週) とシンガポール (4.2 時間 / 週) の企業であり、最も影響が少なかったのはインドと日本 (共に 3.6 時間 / 週) でした。

あなたや IT/ サイバーセキュリティチームの他のメンバーは、サイバーセキュリティ疲れによる生産性の低下を経験したことがありますか？「はい」と回答した場合、1 週間に何時間生産性が低下したかを回答してください。(平均)



2. セキュリティ侵害に対する直接的な影響：平均で 17% の組織が、燃え尽き症候群やセキュリティ疲れがサイバーセキュリティ侵害の原因の一部あるいは直接の原因になっていると認識していました。平均より高かった国は、インド (25%)、シンガポール (23%)、マレーシア (21%)、オーストラリア (19%) であり、日本 (5%) とフィリピン (11%) は平均よりも低くなっていました。

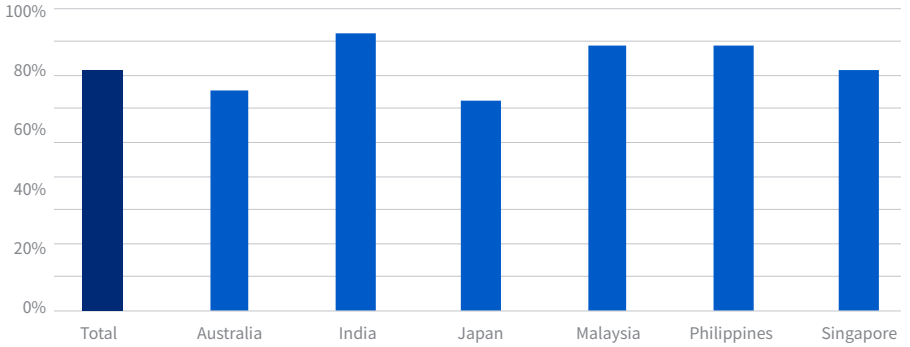
サイバーセキュリティ疲れや燃え尽き症候群は、次のいずれかの問題に関連しているか、直接の原因となっていますか？



3. サイバーセキュリティインシデントへの対応の遅れ：17% の企業が平均と比較して対応が遅れたことを経験しています。インドとマレーシアの企業は、対応が遅れたと回答した割合が最も高く (共に 22%)、シンガポール (20%)、フィリピン (19%)、オーストラリア (17%) が続いていました。対応が遅れたと報告した日本企業は 8% であり、平均を大幅に下回りました。
4. 従業員の退職と異動：23% の企業で、ストレスと燃え尽き症候群がサイバーセキュリティと IT プロフェッショナルの退職の直接の原因となっています。しかし、この数字は国によって大きな差異があり、たとえば、シンガポール (38%) やインド (31%) では退職の原因を占める割合が大幅に高くなっています。また、平均で 11% の企業が、ストレスや燃え尽き症候群による影響により、サイバーセキュリティや IT の従業員を「異動」させたことがあると回答しています。このような異動が最多となったのはマレーシアとシンガポールであり、それぞれ 28% と 15% の企業で異動がありました。

企業も燃え尽き症候群やセキュリティ疲れを経験している従業員を支援する必要性を理解しており、全ての国の平均で 71% の企業がサイバーセキュリティと IT のプロフェッショナルにストレス軽減に関するカウンセリング支援を実施しています。

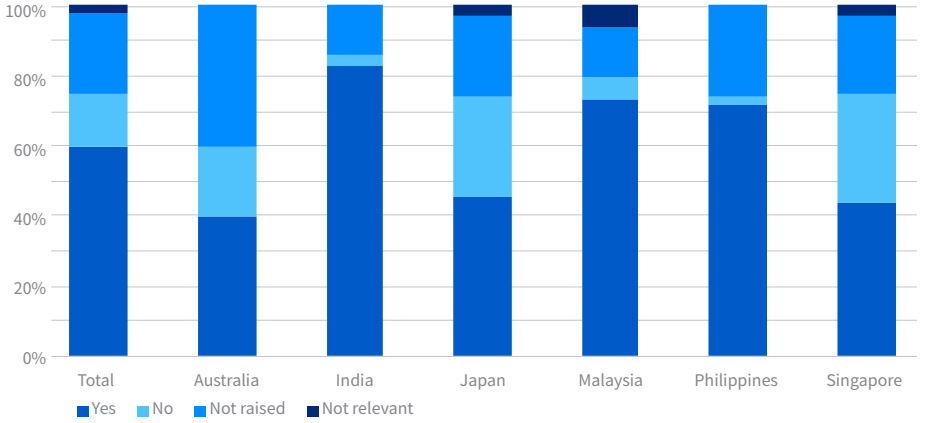
あなたの組織は、IT/ サイバーセキュリティの従業員に対してサイバーセキュリティによるストレスを軽減するためのカウンセリングを提供していますか？「はい」



心の健康の問題を、業務と関連付けて捉えることの重要性が認知されつつあります。いくつかの国で、従業員がセキュリティ疲れや燃え尽き症候群への懸念を訴えた場合に、企業が問題を軽減または解消しようとしていることは歓迎すべきです。

これらの問題の解消に向けた支援があると回答した従業員が多かったのはインド (83%)、マレーシア (74%)、フィリピン (71%) であり、いずれも平均 (60%) を上回りましたが、オーストラリア (40%)、シンガポール (44%)、日本 (46%) は平均を下回っています。

サイバーセキュリティ疲れの懸念を組織に訴えた場合、支援するという肯定的な回答がありましたか？

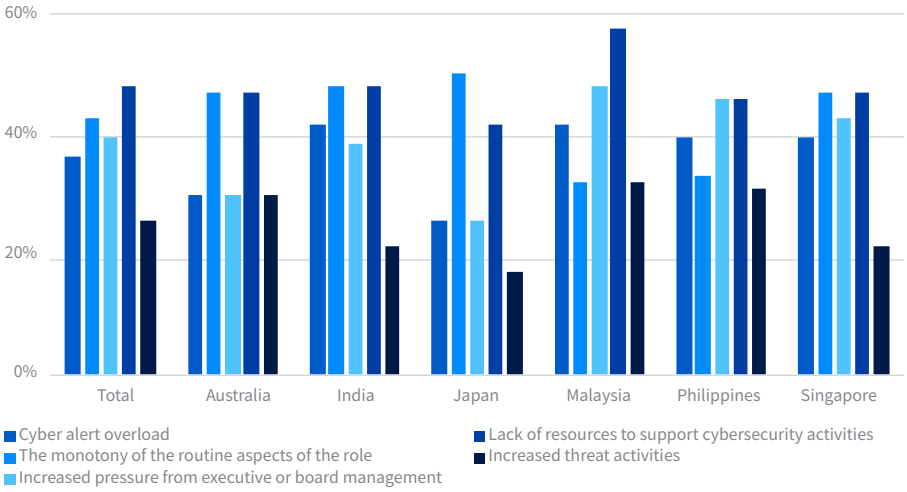


燃え尽き症候群とセキュリティ疲れの原因

主な原因の上位 5 位には、割り当てられたロール (役割) の問題、リソース不足、経営幹部などからのプレッシャーが挙げられています。各原因を詳細に見てきましょう。

1. 人員不足、予算やサードパーティーによるサポートの制限など、サイバーセキュリティ活動に利用できるリソースが不足している。
2. セキュリティ業務がルーチン化しており、単調で退屈であり、やりがいを感じる瞬間が少ない。
3. サイバーセキュリティに関する規制や法的義務の変化に伴い、取締役会や経営幹部からのサイバーセキュリティと IT チームへのプレッシャーが高まっている。
4. アラートが多すぎる。継続的かつ膨大なアラートがツールやシステムから発行されており、サイバーセキュリティと IT プロフェショナルはその対応に直面しており、誤報も多く含まれるこれらのすべてのアラートに優先順位を付けて対応しなければならない。
5. 脅威が増加し、新しいテクノロジーが採用される中で、これまで以上に複雑な対応が常に求められている。

燃え尽き症候群とセキュリティ疲れの原因トップ 5



企業の方向性、テクノロジー、サイバーセキュリティに関連する戦略を推進するときに、取締役会や経営幹部は重要な役割を果たしています。経営幹部からのプレッシャーが大きくなる場合、燃え尽き症候群やセキュリティ疲れを助長する恐れがあることに注意する必要があります。

ここでは、取締役会および経営幹部のサイバーセキュリティに対する理解度が、前回のレポートからどのように変化したのか、また、規制や法改正が経営幹部によるサイバーセキュリティへの理解や対応にどのような影響を及ぼしているのかを見ていきます。

取締役会および経営幹部とサイバーセキュリティの関係

このレポートの第 3 版では、経営幹部がサイバーセキュリティを十分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 割に留まっていたことをお伝えしました。

今年はこのデータが 51% に増加しており、経営幹部の理解が進んでいることを示しています。

前のレポートでは、取締役会レベルのデータには、シニアリーダーシップチーム (SLT) のデータを組み込んではいませんでしたが、今年のレポートには追加しています。

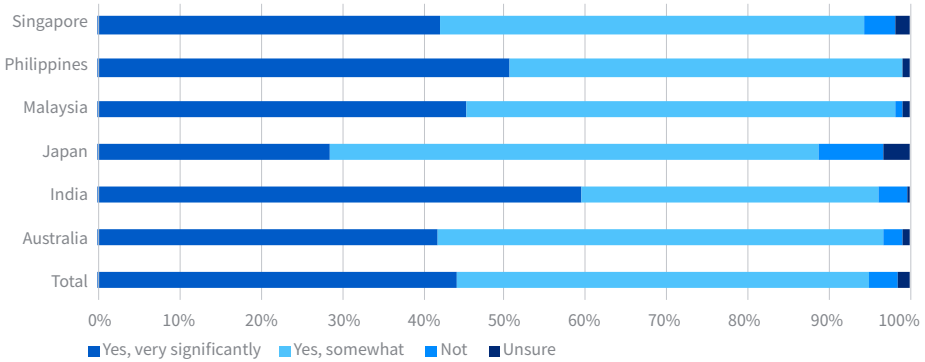
SLT がサイバーセキュリティを理解していると回答した割合は 54% となっており、取締役会が理解していると回答した割合 (51%) よりもわずかに高くなっています。これは、企業の優先課題トップ 10 の中でサイバーセキュリティの重要性が高まっていることが一因です。サイバーセキュリティは現在 2 位であり、5 年前の 9 位から着実に順位を上げています。

アジア太平洋地域の多くの国では、サイバーセキュリティ攻撃を受けてセキュリティが侵害された場合に情報を開示するように企業や組織に義務付ける法律が既に導入されているか、導入される計画が進んでいます。取締役会や SLT に求められる善良な管理者としての注意義務は、最終的にサイバーセキュリティ侵害にも拡大される可能性があると考える法律の専門家も存在します。

セキュリティ侵害が発生すると、最終的に取締役会の責任が問われる恐れがあります。SLT は、自社のセキュリティを維持し、保護するためにあらゆる努力を行っていることを確認しなければなりません。

今回の調査データは、このような規制の変更がすでに取締役会と SLT によるサイバーセキュリティに対する考え方に反映されていることを示しています。平均では回答者の 44% が、サイバーセキュリティ対策の義務化によって、その優先順位が「非常に高くなった」と回答し、さらに 51% が「ある程度高くなった」と感じています。

法律や規制が変更され、サイバーセキュリティの取締役会レベルの関与と責任が義務付けられるようになったことで、企業の取締役会やディレクターレベルにおけるサイバーセキュリティ対策の優先順位は高まりましたか？



このような状況の中で、取締役会や SLT は、サイバーセキュリティ環境を積極的に管理する必要に迫られています。半数の SLT がサイバーセキュリティを理解していない中で、従業員は「サイバーセキュリティ対策で成果を挙げるように経営幹部から期待されていると感じている」と述べています。これは最悪の結末を招く恐れがあります。

適切な支援がなければ、燃え尽き症候群やセキュリティ疲れを経験する従業員の割合が増加することになります。

調査データから、企業は直面している問題を理解し始めており、正しい方向に支援が進んでいると考えることができます。今回の調査データから、企業の支援が変化した恩恵を受けている 5 つの分野がわかりました。

1. 調査対象の 44% が、組織内の全従業員に対するサイバーセキュリティ教育とトレーニングのための資金を増やしていると回答している。
2. 42% が、サイバーセキュリティテクノロジーソリューションの新規導入やアップグレードのための資金を増やしている。
3. 41% が、サイバーセキュリティと IT 関連の従業員のための教育とトレーニングに投資を進めている。
4. 36% が、サイバーセキュリティの人員を新規に採用して増員している。
5. 31% が、サイバーセキュリティのサードパーティパートナーへの投資を増やしている。

燃え尽き症候群とセキュリティ疲れは、企業と従業員のさまざまなレベルで影響を及ぼす重大な問題です。攻撃の頻度の増加、企業とサイバー攻撃者の双方が導入する新しいテクノロジー、そして、経営幹部からの期待とプレッシャーの高まりによって、多くの企業でサイバーセキュリティに対応する能力が低下しており、業務が停止する事態を招くリスクが高まっています。

このような状況を念頭に置いて、前回のレポートで分析したサイバーセキュリティに関する他の実務的な問題について見てきましょう。

企業におけるサイバーセキュリティの構造と担当者のロールと責務に関する「全般的なサイバーセキュリティ環境」から見てきましょう。

全般的なサイバーセキュリティの環境：責任、レポートライン、報告の頻度

サイバーセキュリティに対するリーダーシップチームの構成は、業界間や業界内で見ても非常に多様ですが、IT マネージャーや IT ディレクターがリーダーとなることが一般的です (シンガポールでは 36%、マレーシアでは 21%)。日本 (28%) 、マレーシア (21%)、フィリピン (33%) では、サイバーセキュリティの役員がリーダーになるケースが多くなっています。オーストラリアでは 21% の組織が CISO (最高情報セキュリティ責任者) を指名しています。

興味深いことに、9% の組織が、リーダーシップチームを構成するときに、サイバーセキュリティを担当するリーダーは 1 名ではなく、複数ロールのリーダーで責任を分担していると回答していました。このような複数ロールによるアプローチはマレーシア (13%) とシンガポール (11%) で最も高く、インド (5%) で最も低くなっています。

サイバーセキュリティのリーダーが CEO に直接レポートしているケースは 39% であり、オーストラリア (51%) が最も高く、日本 (23%) が最も低くなっています。日本の 26% の組織は、サイバーセキュリティのリーダーがデジタルトランスフォーメーション部門の責任者に報告していると回答しています。3 番目に多いレポートラインが CIO/CTO でした。

75% の企業がサイバーセキュリティの専門チームを設置しており、39% の企業が IT 部門内にチームを設置していると回答しています。日本は、IT スタッフがサイバーセキュリティ業務も担っている組織の割合が最も高くなっています (25%)。アジア太平洋地域全体では、5% の組織がサイバーセキュリティを 100% アウトソーシングしていると回答しています (日本では 8%、シンガポールでは 7%)。

今年の調査では、サイバーセキュリティのリーダーが社内の関係者や顧客、パートナー、政府機関などの社外グループに対して行う説明会の頻度について新たに注目しました。

取締役会や SLT の間でサイバーセキュリティへの関心が高まっていますが、主要な関係者への最新情報の提供については今後積極的に取り組まなければならないことが多くあります。

- サイバーセキュリティに関する最新情報の提供を定期的に受けているのは、取締役会の 41% と SLT の 51% に過ぎない (平均値)。
- このデータセットでは、更新頻度は良好な結果になっており、37% の取締役会と 27% の SLT が毎週更新を受けており、さらに 36% の取締役会と 39% の SLT が毎月更新を受けている。
- 取締役会の 60% と半数の SLT はサイバーセキュリティの最新情報を定期的に得ていない。

	Total	Australia	India	Japan	Malaysia	Philippines	Singapore
The board	41%	49%	46%	21%	49%	52%	38%
The executive committee	51%	46%	53%	38%	65%	60%	58%
Company-wide	45%	47%	48%	36%	56%	41%	51%
3rd party vendors and suppliers	22%	21%	27%	13%	29%	25%	25%
Government officials	19%	18%	26%	4%	33%	11%	29%
Customers	16%	12%	21%	12%	20%	13%	24%
Informal updates only	2%	1%	0%	5%	1%	4%	3%
No	1%	1%	0%	1%	0%	1%	0%

表 1「質問：以下のいずれかのグループに対して、サイバーセキュリティに関する定期的な最新情報や説明会を提供していますか？

インシデント対応と復旧

今年は、セキュリティ侵害の発生率に関するデータを提供するのではなく (このデータについては次回のレポートで説明します)、インシデント対応と復旧に関連する以下の要因について考察します。

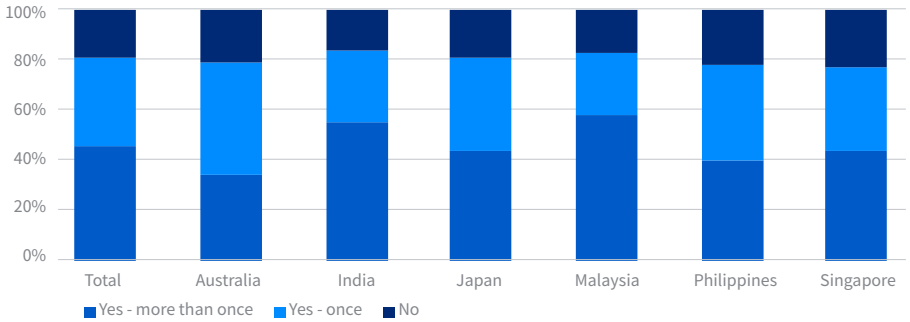
- サイバーセキュリティと IT に携わる従業員が、雇用されている会社以外の場所で、個人的に経験したセキュリティ侵害の影響と、そのような経験が自社のサイバーセキュリティ活動に対する考え方に与えた影響。
- どれだけの組織が正式なインシデント対応計画を策定しているか、また計画を策定するに至った要因。
- サイバーセキュリティ対策で過去にミスを犯した担当者は、そのミスから教訓を得ているか？
- サイバーセキュリティのインシデント対応への準備状況を自社で評価する方法。

個人が経験したセキュリティ侵害の影響

サイバーセキュリティや IT プロフェショナルが個人として経験したセキュリティ侵害[1]が、自社のサイバーセキュリティに対する考え方にどのような影響を与えているのかを調査しました。

回答者の 81% が個人としてセキュリティ侵害を経験しています。多くの読者の方がこの数値は過去に見たことがあるかもしれません。他の質問の結果は国によってばらつきがありますが、この質問については各国の違いは比較的小さく、すべての国である程度似通った結果になっています。

個人的に他社の製品やサービスを利用しているときに、その会社のセキュリティが侵害され自分の個人情報が窃取あるいは漏洩した経験がありますか？またはそのような通知を受けたことがありますか？ (四捨五入が合計に影響する場合があります)



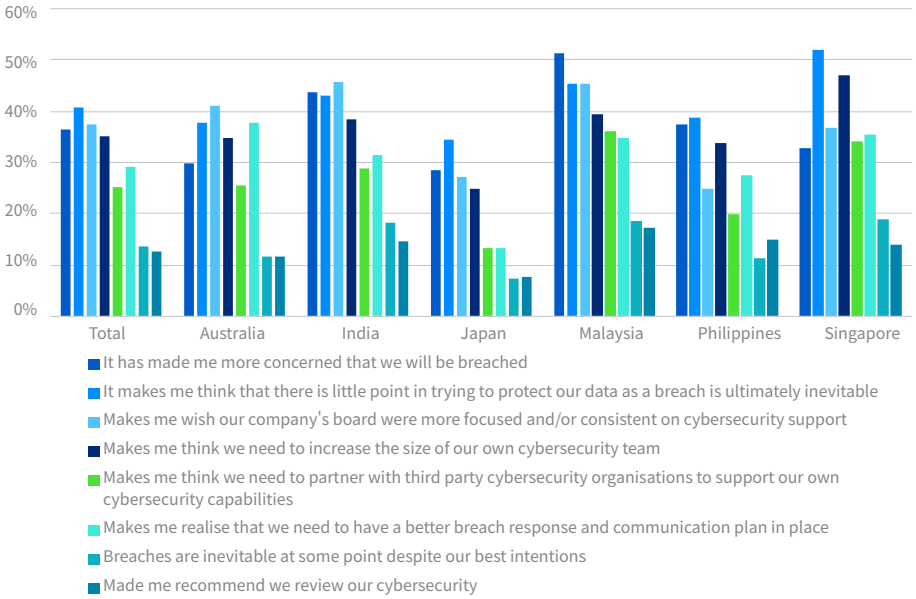
1 個人として経験したセキュリティ侵害とは、サイバーセキュリティや IT プロフェショナルが、他の企業の製品やサービスを個人的に利用しているときに、自分の個人データが窃取された経験を意味します。

個人として経験したセキュリティ侵害が、プロフェショナルとしての自分の考え方を変えましたか？

国によっては、大きく変わったという回答が多くありました。セキュリティ疲れと燃え尽き症候群、社内業務、サードパーティーのマネージドセキュリティサービスプロバイダーへの影響があったという回答が得られています。上位 5 位の影響は以下の通りです。

1. 41% のプロフェショナルは、企業データの漏洩は最終的に避けられないものであり、企業データを保護する取り組みにはあまり意味がないと考えるようになった。
2. 37% は、自社の取締役会がサイバーセキュリティの問題により重視して、一貫性のある対応を行うことを望むようになった。
3. 36% は、自社のセキュリティ侵害をより懸念するようになった。
4. 35% は、社内のサイバーセキュリティチームを強化する必要があると感じるようになった。
5. 29% は、セキュリティ侵害への対応とコミュニケーション計画を改善する必要があると考えるようになった。

個人としてデータの漏洩や窃取を経験したことで、自社におけるセキュリティ業務に対する考え方は変わりましたか？



主な影響に対する各国の回答は、多少のばらつきがあります。また、マレーシアとシンガポールは、グループ全体と比較して、多くのカテゴリで変わったと回答した割合が高くなりました。

- オーストラリアでは、取締役会の問題、インシデント対応とコミュニケーション計画、そしてセキュリティ侵害の必然性に対する考え方が多く変化しています。
- インドは、取締役会の問題、懸念の高まり、セキュリティ侵害の必然性に対する考え方が多く変化しています。
- 日本は全体的な影響が小さくなっていますが、主に、セキュリティ侵害の必然性、懸念の高まり、取締役会の問題に対する変化がありました。
- マレーシアでは、セキュリティ侵害の必然性、セキュリティ侵害の必然性、取締役会の問題に対する変化がありました。
- フィリピンでは、セキュリティ侵害の必然性、懸念の高まり、社内のサイバーセキュリティチームの規模を拡大する必要性に対する変化がありました。
- 最後に、シンガポールでは、セキュリティ侵害の必然性、懸念の高まり、取締役会の問題に対する変化がありました。

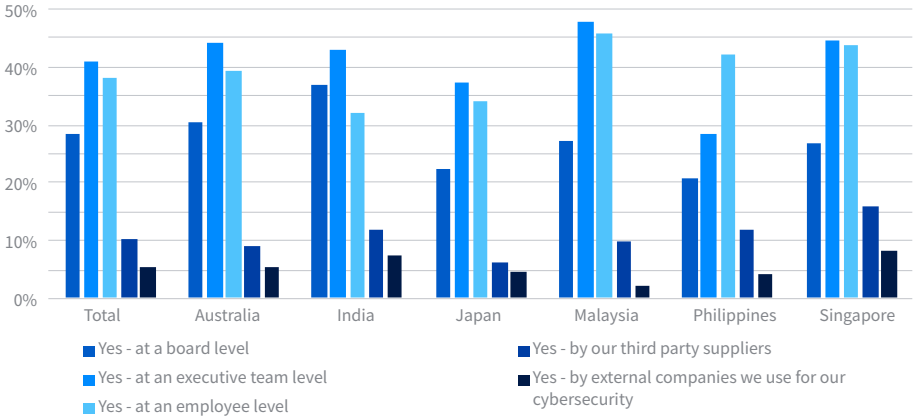
セキュリティ対策のミスの繰り返しと教育とトレーニングの効果

これまでも、人為的ミスがセキュリティ侵害やインシデントの最も一般的な要因になっていることを説明する多くの記事が公開されています。企業、サードパーティーサプライヤー、マネージドセキュリティプロバイダーがサプライチェーンの脆弱性の影響を受ける事案が増えていることから、最近では、取締役会、SLT、従業員などに教育やトレーニングに広範な投資を行う企業も増えています。

しかし、企業は教育やトレーニングプログラムを実施しているにもかかわらず、セキュリティ対策における常習犯が存在していることも明らかになっています。トレーニングや教育を受けているにもかかわらず、同じ間違いを犯している割合をユーザーのカテゴリ別に以下に示します。

- SLT の 41%
- 従業員の 38%
- 経営幹部の 28%
- サードパーティーサプライヤーの 10%
- サードパーティーのマネージドサイバーセキュリティプロバイダーの 5%

自社において、教育やトレーニングを受けているにもかかわらず、従業員が定期的に同じミスを犯しており、サイバーセキュリティ対策に失敗しているケースはありませんか？



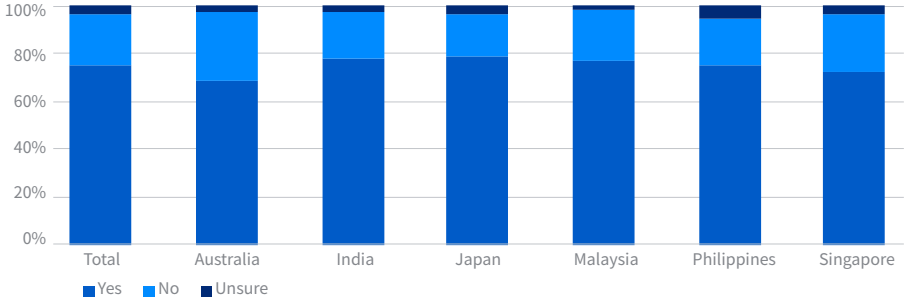
経営幹部、従業員、パートナーのすべてがヒューマンエラーを起こすことのないサイバーセキュリティ環境を実現して維持できると考えるのは非現実的です。

このデータは、効果的なインシデント対応計画とコミュニケーション計画を策定してテストすることの重要性を示しています。次のセクションでは、これらの計画の策定と準備の状況について見てきましょう。

インシデント対応計画と準備

84% の組織が、正式なサイバーセキュリティインシデントへの対応計画およびコミュニケーション計画を策定しています。マレーシア (92%) とインド (91%) が、計画を実施している企業の割合が最も高く、日本 (73%) とオーストラリア (83%) は最も低くなっています。

自社で正式なサイバーセキュリティ対策、インシデント対応計画、コミュニケーション計画を策定していますか？

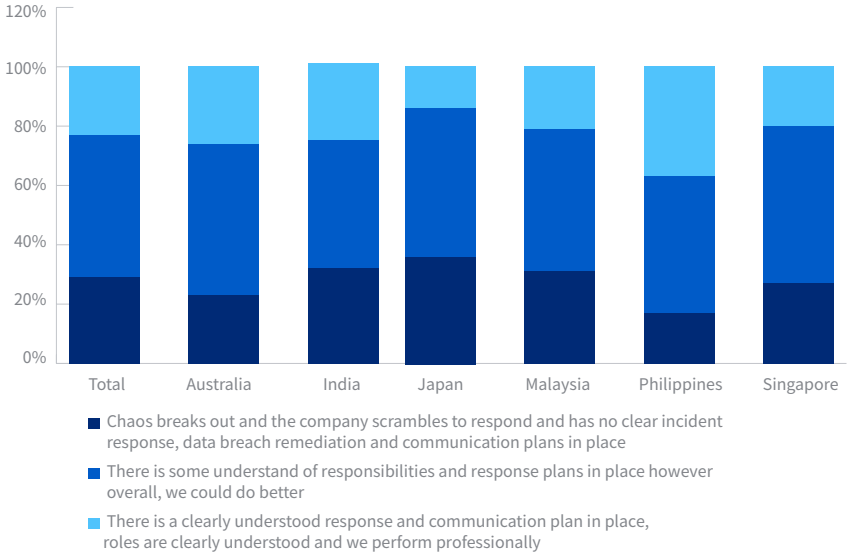


計画を立てておくことと、効果的に計画を実施することは異なります。

75% の組織が、自社でセキュリティ侵害を経験した後に、計画の策定に着手したと回答しています。また、サイバー攻撃やセキュリティ侵害に対する自社の対応を自己評価してもらったところ、「インシデント対応計画やコミュニケーション計画が明確に理解されており、役割分担が明確化されており、プロフェッショナルな対応ができている」と考えている企業はわずか 23% にとどまっているのも、このような事後的な対応になっていることが原因でしょう。

逆に、29% の回答者は「セキュリティ侵害によって混乱が生じ、対応に追われることになるが、明確なインシデント対応計画、セキュリティ侵害による影響の修復計画やコミュニケーション計画が策定されていない」と感じています。

サイバー攻撃やセキュリティ侵害への自社の対策の説明として最も適切なのは、次のどれですか？



日本 (36%) とインド (32%) は、「混乱が生じている」と回答した割合が最も高く、フィリピン (37%)、オーストラリア (26%)、インド (26%) は、策定した計画を「プロフェッショナルな方法で実行している」と回答した割合が最も高くなっています。

今回の調査データからは、定期的にテストが行われていないか、行われていたとしても、そのテストで得られた結果が必ずしも計画の改善に役立っていないことが示されています。

このデータは、企業が全社的に強固なセキュリティカルチャーを構築することに苦労していることを示していると考えられます。組織がサイバーセキュリティに対して抱いているフラストレーションのリストのトップに、セキュリティカルチャーの問題が挙げられることは予想外の結果でした。

サイバーセキュリティと IT プロフェッショナルの懸念と不満の領域

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、自社とセキュリティ業務に対して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。

今年の調査データでは、組織が感じているフラストレーションのランキングにいくつかの変化が見られ、セキュリティ環境がいかに動的であるかを示しています。

フラストレーションのトップ 5：

1. 今年は、全社的に強固なサイバーセキュリティカルチャーを確立することが、経験した最も大きなフラストレーションに挙げられています。例年であれば、この問題はトップ 10 圏外にランクされていました。
2. 「サイバーセキュリティ対策は容易であり、懸念が誇張されすぎていると経営幹部が考えている」いう 2 番目のフラストレーションは、昨年の 10 位から今年は 2 位へと大幅に上昇しました。
3. 「経営幹部が自社は攻撃を受けないと考えている」というフラストレーションは今年 1 位から 3 位に落ちており、セキュリティ問題に関する意識が高まっていることを示しています。
4. 経済の落ち込みが多くの組織に影響を及ぼしており、予算に関する懸念は 7 位から 4 位に上昇しています。この問題は 2024 年もトップ 5 に入ることが予想されます。
5. 「SLT は、口先ではサイバーセキュリティ対策に賛同しているが、真剣ではない」というフラストレーションは、8 位から 5 位に上昇しました。

フラストレーションの原因となる主な問題	2019 年	2021 年	2022 年	2023 年
強力で効果的なサイバーセキュリティカルチャーを全社的に構築することに苦労している	トップ 10 圏外	トップ 10 圏外	トップ 10 圏外	1
サイバーセキュリティ対策は容易であり、懸念が誇張されすぎていると経営幹部が考えている	3	1	10	2
経営幹部が自社は攻撃を受けないと考えている	7	7	1	3
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	4
経営幹部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、真剣ではない	9	5	8	5
経営幹部は、自社が攻撃されることを予想しているが、攻撃を阻止する方法はないと考えている	10	8	4	6
セキュリティ脅威のスピードに追いつけない	8	9	5	7
サイバーセキュリティのプロフェショナルを十分に雇用できない	5	3	2	8
サイバーセキュリティが常に優先事項になっていない	トップ 10 圏外	トップ 10 圏外	トップ 10 圏外	9
規制や法律への対応が後手に回っており、サイバーセキュリティの管理が複雑になっている。	トップ 10 圏外	トップ 10 圏外	トップ 10 圏外	10

フラストレーションのトップ 5 は、技術的な問題でもなければ、規制や法律の問題でもありません。効果的なコミュニケーションに関する問題です。サイバーセキュリティと IT プロフェショナルが、大規模な組織でサイバーセキュリティの問題を分かりやすく伝えることができておらず、以下のような問題が組織で発生しています。

- 取締役会と SLT にサイバーセキュリティの専門用語を簡明に説明できていない。
- 企業にとって最重要であり、絶対に保護しなければならない資産の優先順位を決定できていない。
- セキュリティ侵害が発生したときの実践的な手順を決定できるように支援できていない。

まとめ

サイバーセキュリティ疲れと燃え尽き症候群は、従業員と企業の双方がサイバーセキュリティ対策を遂行していく能力に悪影響を及ぼす重大な問題です。リソースの不足、経営幹部や取締役会からのプレッシャーの増加、サイバーセキュリティ業務が反復的でルーチンであることなどの要因によって、業務に対する集中力が低下し、脆弱な環境を見過ごす割合が上昇しています。また、サイバーセキュリティ担当者や IT 担当者の離職率が上昇していることは、多くの組織が直面している現実の問題です。自動化機能の向上や、人工知能 (AI) を活用したサイバーセキュリティソリューションによって、燃え尽き症候群の原因の一端は軽減できます。さらに重要なのは、全社的な強固なサイバーセキュリティカルチャーを構築し、サイバーセキュリティの問題が複雑であることについて取締役会と SLT が十分に理解できるように努め、「サイバーセキュリティ対策でミスを繰り返している従業員」がパフォーマンスを向上できるようにコーチングと教育を確実に受けられるように注力すれば、サイバーセキュリティ燃え尽き症候群とセキュリティ疲れの原因である一般的なフラストレーションの多くを軽減できるでしょう。

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

国別のプロファイル

オーストラリア

サイバーセキュリティと IT プロフェショナルがサイバーセキュリティ燃え尽き症候群を経験している割合：

- 頻繁に経験している：17% (平均 - 23%)
- 時折経験している：69% (平均 - 62%)

過去 12 か月の間に、サイバーセキュリティ燃え尽き症候群は増加しましたか？

- 大幅に増加した：30% (平均 - 30%)
- 若干増加した：63% (平均 - 60%)

サイバーセキュリティと IT プロフェショナルがサイバーセキュリティ燃え尽き症候群が原因で退職した従業員いる企業の割合：

- 22% (平均 - 23%)

サイバーセキュリティ燃え尽き症候群によりパフォーマンスの問題が発生し、従業員を「異動」したことはありますか？

- はい：16% (平均 - 20%)

サイバーセキュリティ燃え尽き症候群によって発生している 1 週間あたりの平均損失時間：

- 3.8 時間 / 週 (平均 4.1 時間 / 週)

サイバーセキュリティ戦略を主導しているのは誰ですか？

- IT ディレクター
- CISO
- サイバーセキュリティ部門のディレクターまたはマネージャー

サイバーセキュリティプロフェッショナルのフラストレーションのトップ 3

1. 全社的に強固なサイバーセキュリティカルチャーを構築することに苦労している。
2. サイバーセキュリティ対策は容易であり、懸念が誇張されすぎていると経営幹部が考えている。
3. 予算が不足している。

サイバーセキュリティに関する経営幹部と SLT の理解 :

オーストラリア	全く理解していない	あまり理解していない	十分に理解している	分からない
経営幹部レベル	4%	41%	51%	4%
平均	7%	37%	51%	5%
SLT レベル	3%	39%	57%	1%
平均	6%	36%	54%	4%

法規制が変更されたことで、取締役会および SLT レベルでのサイバーセキュリティに対する重点的な取り組みが必要となっている：

- 非常のそう思う：42% (平均 - 44%)
- ある程度そう思う：55% (平均 - 51%)

このような重点的な取り組みによって大きな影響を受ける分野のトップ 3：

1. トレーニングと教育の拡充
2. サイバーセキュリティテクノロジーの新規導入やアップグレードへの投資
3. サイバーセキュリティの人員の増加または人員増加の承認

定期的にサイバーセキュリティに関する説明会を実施していますか？

はい	取締役会	SLT	会社全体	サードパーティー サプライヤー	政府機関	顧客	非公式な アップデート	いいえ
オーストラリア	49%	46%	47%	21%	18%	12%	1%	1%
平均	41%	51%	45%	22%	19%	16%	2%	1%

正式なインシデント対応計画の策定：

- 83% (平均 - 84%)

攻撃を受けた後に計画を策定した：

- 68% (平均 - 75%)

インシデントへの対応の準備状況：

- 混乱が生じている：23% (平均 - 29%)
- 準備をしているが、十分ではない：51% (平均 - 48%)
- 役割分担が明確化されており、プロフェッショナルな対応ができている 26% (平均 - 23%)

トレーニングおよび教育の効果 - セキュリティ対策の常習犯の割合：

- 取締役会：30% (平均 - 28%)
- SLT：44% (平均 - 41%)
- 従業員：39% (平均 - 38%)

インド

サイバーセキュリティと IT プロフェショナルがサイバーセキュリティ燃え尽き症候群を経験している割合：

- 頻繁に経験している：37% (平均 - 23%)
- 時折経験している：46% (平均 - 62%)

過去 12 か月の間に、サイバーセキュリティ燃え尽き症候群は増加しましたか？

- 大幅に増加した：48% (平均 - 30%)
- 若干増加した：45% (平均 - 60%)

サイバーセキュリティと IT プロフェショナルがサイバーセキュリティ燃え尽き症候群が原因で退職した従業員いる企業の割合：

- 31% (平均 - 23%)

サイバーセキュリティ燃え尽き症候群によりパフォーマンスの問題が発生し、従業員を「異動」したことはありますか？

- はい：31% (平均 - 20%)

サイバーセキュリティ燃え尽き症候群によって発生している 1 週間あたりの平均損失時間：

- 3.6 時間 / 週 (平均 4.1 時間 / 週)

サイバーセキュリティ戦略を主導しているのは誰ですか？

- IT ディレクターまたはマネージャー
- サイバーセキュリティ部門のディレクターまたはマネージャー
- CIO/CTO

サイバーセキュリティプロフェッショナルのフラストレーションのトップ 3

1. サイバーセキュリティ対策は容易であり、懸念が誇張されすぎていると経営幹部が考えている。
2. 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。
3. 強力なサイバーセキュリティカルチャーを全社的に構築することに苦労している。

サイバーセキュリティに関する経営幹部と SLT の理解 :

インド	全く理解していない	あまり理解していない	十分に理解している	分からない
経営幹部レベル	4%	31%	58%	6%
平均	7%	37%	51%	5%
SLT レベル	4%	26%	66%	4%
平均	6%	36%	54%	4%

法規制が変更されたことで、取締役会および SLT レベルでのサイバーセキュリティに対する重点的な取り組みが必要となっている：

- 非常にそう思う：59% (平均 - 44%)
- ある程度そう思う：37% (平均 - 51%)

このような重点的な取り組みによって大きな影響を受ける分野のトップ 3：

1. IT/ サイバーセキュリティ従業員のみを対象としたトレーニングと教育を強化する。
2. 全従業員に対するトレーニングと教育を強化する。
3. サイバーセキュリティの人員の増加または新規採用の承認。

定期的にサイバーセキュリティに関する説明会を実施していますか？

はい	取締役会	SLT	会社全体	サードパーティー サプライヤー	政府機関	顧客	非公式な アップデート	いいえ
インド	46%	53%	48%	27%	26%	21%	0%	0%
平均	41%	51%	45%	22%	19%	16%	2%	1%

正式なインシデント対応計画の策定：

- 91% (平均 - 84%)

攻撃を受けた後に計画を策定した：

- 78% (平均 - 75%)

インシデントへの対応の準備状況：

- 混乱が生じている：32% (平均 - 29%)
- 準備をしているが、十分ではない：43% (平均 - 48%)
- 役割分担が明確化されており、プロフェッショナルな対応ができている 26% (平均 - 23%)

トレーニングおよび教育の効果 - セキュリティ対策の常習犯の割合：

- 取締役会：37% (平均 - 28%)
- SLT：43% (平均 - 41%)
- 従業員：32% (平均 - 38%)

日本

サイバーセキュリティと IT プロフェショナルがサイバーセキュリティ燃え尽き症候群を経験している割合：

- 頻繁に経験している：23% (平均 - 23%)
- 時折経験している：46% (平均 - 62%)

過去 12 か月の間に、サイバーセキュリティ燃え尽き症候群は増加しましたか？

- 大幅に増加した：38% (平均 - 30%)
- 若干増加した：58% (平均 - 60%)

サイバーセキュリティと IT プロフェショナルがサイバーセキュリティ燃え尽き症候群が原因で退職した従業員いる企業の割合：

- 13% (平均 - 23%)

サイバーセキュリティ燃え尽き症候群によりパフォーマンスの問題が発生し、従業員を「異動」したことはありますか？

- はい：12% (平均 - 20%)

サイバーセキュリティ燃え尽き症候群によって発生している 1 週間あたりの平均損失時間：

- 3.6 時間 / 週 (平均 4.1 時間 / 週)

サイバーセキュリティ戦略を主導しているのは誰ですか？

- サイバーセキュリティ部門のディレクターまたはマネージャー
- CISO
- CIO/CTO

サイバーセキュリティプロフェッショナルのフラストレーションのトップ 3

1. 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、真剣ではない。
2. 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。
3. 強力なサイバーセキュリティカルチャーを全社的に構築することに苦労している。

サイバーセキュリティに関する経営幹部と SLT の理解 :

日本	全く理解していない	あまり理解していない	十分に理解している	分からない
経営幹部レベル	18%	36%	38%	8%
平均	7%	37%	51%	5%
SLT レベル	14%	47%	32%	6%
平均	6%	36%	54%	4%

法規制が変更されたことで、取締役会および SLT レベルでのサイバーセキュリティに対する重点的な取り組みが必要となっている：

- 大幅に増加した：28% (平均 - 44%)
- ある程度そう思う：60% (平均 - 51%)

このような重点的な取り組みによって大きな影響を受ける分野のトップ 3：

1. 全従業員に対するトレーニングと教育を強化する。
2. サイバーセキュリティテクノロジーの新規導入やアップグレードへの投資。
3. IT/ サイバーセキュリティ従業員のみを対象としたトレーニングと教育を強化する。

定期的にサイバーセキュリティに関する説明会を実施していますか？

はい	取締役会	SLT	会社全体	サードパーティー サプライヤー	政府機関	顧客	非公式な アップデート	いいえ
日本	21%	38%	36%	13%	4%	12%	5%	1%
平均	41%	51%	45%	22%	19%	16%	2%	1%

正式なインシデント対応計画の策定：

- 73% (平均 - 84%)

攻撃を受けた後に計画を策定した：

- 79% (平均 - 75%)

インシデントへの対応の準備状況：

- 混乱が生じている：36% (平均 - 29%)
- 準備をしているが、十分ではない：50% (平均 - 48%)
- 役割分担が明確化されており、プロフェッショナルな対応ができている 14% (平均 - 23%)

トレーニングおよび教育の効果 - セキュリティ対策の常習犯の割合：

- 取締役会：22% (平均 - 28%)
- SLT：37% (平均 - 41%)
- 従業員：34% (平均 - 38%)

マレーシア

サイバーセキュリティと IT プロフェショナルがサイバーセキュリティ燃え尽き症候群を経験している割合：

- 頻繁に経験している：21% (平均 - 23%)
- 時折経験している：71% (平均 - 62%)

過去 12 か月の間に、サイバーセキュリティ燃え尽き症候群は増加しましたか？

- 大幅に増加した：29% (平均 - 30%)
- 若干増加した：61% (平均 - 60%)

サイバーセキュリティと IT プロフェショナルがサイバーセキュリティ燃え尽き症候群が原因で退職した従業員いる企業の割合：

- 25% (平均 - 23%)

サイバーセキュリティ燃え尽き症候群によりパフォーマンスの問題が発生し、従業員を「異動」したことはありますか？

- はい：23% (平均 - 20%)

サイバーセキュリティ燃え尽き症候群によって発生している 1 週間あたりの平均損失時間：

- 4.1 時間 / 週 (平均 4.1 時間 / 週)

サイバーセキュリティ戦略を主導しているのは誰ですか？

- サイバーセキュリティ部門のディレクターまたはマネージャー
- IT ディレクターまたはマネージャー
- CISO

サイバーセキュリティプロフェッショナルのフラストレーションのトップ 3

1. 強力なサイバーセキュリティカルチャーを全社的に構築することに苦労している。
2. サイバーセキュリティ対策は容易であり、懸念が誇張されすぎていると経営幹部が考えている。
3. サイバーセキュリティの脅威のスピードに追いつくことは困難になっている。

サイバーセキュリティに関する経営幹部と SLT の理解 :

マレーシア	全く理解していない	あまり理解していない	十分に理解している	分からない
経営幹部レベル	3%	42%	52%	3%
平均	7%	37%	51%	5%
SLT レベル	2%	35%	60%	4%
平均	6%	36%	54%	4%

法規制が変更されたことで、取締役会および SLT レベルでのサイバーセキュリティに対する重点的な取り組みが必要となっている：

- 非常にそう思う：45% (平均 - 44%)
- ある程度そう思う：53% (平均 - 51%)

このような重点的な取り組みによって大きな影響を受ける分野のトップ 3：

1. 全社的に強力なサイバーセキュリティカルチャーを作り上げるのに苦労している。
2. 経営幹部がサイバーセキュリティは簡単な問題であり、懸念が誇張されていると考えている。
3. サイバーセキュリティの脅威のペースに自社の対応を合わせるのが難しい。

定期的にサイバーセキュリティに関する説明会を実施していますか？

はい	取締役会	SLT	会社全体	サードパーティー サプライヤー	政府機関	顧客	非公式な アップデート	いいえ
マレーシア	49%	65%	56%	29%	33%	20%	1%	0%
平均	41%	51%	45%	22%	19%	16%	2%	1%

正式なインシデント対応計画の策定：

- 92% (平均 - 84%)

攻撃を受けた後に計画を策定した：

- 77% (平均 - 75%)

インシデントへの対応の準備状況：

- 混乱が生じている：31% (平均 - 29%)
- 準備をしているが、十分ではない：48% (平均 - 48%)
- 役割分担が明確化されており、プロフェッショナルな対応ができている 21% (平均 - 23%)

トレーニングおよび教育の効果 - セキュリティ対策の常習犯の割合：

- 取締役会：27% (平均 - 28%)
- SLT：47% (平均 - 41%)
- 従業員：45% (平均 - 38%)

フィリピン

サイバーセキュリティと IT プロフェショナルがサイバーセキュリティ燃え尽き症候群を経験している割合：

- 頻繁に経験している：23% (平均 - 23%)
- 時折経験している：71% (平均 - 62%)

過去 12 か月の間に、サイバーセキュリティ燃え尽き症候群は増加しましたか？

- 大幅に増加した：21% (平均 - 30%)
- 若干増加した：67% (平均 - 60%)

サイバーセキュリティと IT プロフェショナルがサイバーセキュリティ燃え尽き症候群が原因で退職した従業員いる企業の割合：

- 17% (平均 - 23%)

サイバーセキュリティ燃え尽き症候群によりパフォーマンスの問題が発生し、従業員を「異動」したことはありますか？

- はい：13% (平均 - 20%)

サイバーセキュリティ燃え尽き症候群によって発生している 1 週間あたりの平均損失時間：

- 4.6 時間 / 週 (平均 4.1 時間 / 週)

サイバーセキュリティ戦略を主導しているのは誰ですか？

- サイバーセキュリティ部門のディレクターまたはマネージャー
- IT ディレクターまたはマネージャー
- CIO/CTO

サイバーセキュリティプロフェッショナルのフラストレーションのトップ 3

1. 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。
2. サイバーセキュリティ対策は容易であり、懸念が誇張されすぎていると経営幹部が考えている。
3. 強力なサイバーセキュリティカルチャーを全社的に構築することに苦労している。

サイバーセキュリティに関する経営幹部と SLT の理解 :

フィリピン	全く理解していない	あまり理解していない	十分に理解している	分からない
経営幹部レベル	3%	40%	56%	1%
平均	7%	37%	51%	5%
SLT レベル	4%	34%	59%	3%
平均	6%	36%	54%	4%

法規制が変更されたことで、取締役会および SLT レベルでのサイバーセキュリティに対する重点的な取り組みが必要となっている：

- 非常にそう思う：50% (平均 - 44%)
- ある程度そう思う：49% (平均 - 51%)

このような重点的な取り組みによって大きな影響を受ける分野のトップ 3：

1. 全従業員に対するトレーニングと教育を強化する。
2. IT およびサイバーセキュリティの従業員に対するトレーニングと教育を強化する。
3. サイバーセキュリティテクノロジーの新規導入やアップグレードへの投資。

定期的にサイバーセキュリティに関する説明会を実施していますか？

はい	取締役会	SLT	会社全体	サードパーティー サプライヤー	政府機関	顧客	非公式な アップデート	いいえ
フィリピン	52%	60%	41%	25%	11%	13%	4%	1%
平均	41%	51%	45%	22%	19%	16%	2%	1%

正式なインシデント対応計画の策定：

- 88% (平均 - 84%)

攻撃を受けた後に計画を策定した：

- 75% (平均 - 75%)

インシデントへの対応の準備状況：

- 混乱が生じている：17% (平均 - 29%)
- 準備をしているが、十分ではない：46% (平均 - 48%)
- 役割分担が明確化されており、プロフェッショナルな対応ができている 37% (平均 - 23%)

トレーニングおよび教育の効果 - セキュリティ対策の常習犯の割合：

- 取締役会：20% (平均 - 28%)
- SLT：28% (平均 - 41%)
- 従業員：42% (平均 - 38%)

シンガポール

サイバーセキュリティと IT プロフェショナルがサイバーセキュリティ燃え尽き症候群を経験している割合：

- 頻繁に経験している：16% (平均 - 23%)
- 時折経験している：72% (平均 - 62%)

過去 12 か月の間に、サイバーセキュリティ燃え尽き症候群は増加しましたか？

- 大幅に増加した：18% (平均 - 30%)
- 若干増加した：64% (平均 - 60%)

サイバーセキュリティと IT プロフェショナルがサイバーセキュリティ燃え尽き症候群が原因で退職した従業員いる企業の割合：

- 38% (平均 - 23%)

サイバーセキュリティ燃え尽き症候群によりパフォーマンスの問題が発生し、従業員を「異動」したことはありますか？

- はい：26% (平均 - 20%)

サイバーセキュリティ燃え尽き症候群によって発生している 1 週間あたりの平均損失時間：

- 4.2 時間 / 週 (平均 4.1 時間 / 週)

サイバーセキュリティ戦略を主導しているのは誰ですか？

- IT ディレクターまたはマネージャー
- サイバーセキュリティ部門のディレクターまたはマネージャー
- CIO/CTO

サイバーセキュリティプロフェッショナルのフラストレーションのトップ 3

1. 強力なサイバーセキュリティカルチャーを全社的に構築することに苦労している。
2. サイバーセキュリティ対策は容易であり、懸念が誇張されすぎていると経営幹部が考えている。
3. サイバーセキュリティのスピードに追いつくことは困難になっている。

サイバーセキュリティに関する経営幹部と SLT の理解 :

シンガポール	全く理解していない	あまり理解していない	十分に理解している	分からない
経営幹部レベル	7%	33%	57%	3%
平均	7%	37%	51%	5%
SLT レベル	5%	32%	58%	5%
平均	6%	36%	54%	4%

法規制が変更されたことで、取締役会および SLT レベルでのサイバーセキュリティに対する重点的な取り組みが必要となっている：

- 非常にそう思う：42% (平均 - 44%)
- ある程度そう思う：52% (平均 - 51%)

このような重点的な取り組みによって大きな影響を受ける分野のトップ 3：

1. サイバーセキュリティテクノロジーの新規導入やアップグレードへの投資。
2. 全従業員に対するトレーニングと教育を強化する。
3. IT およびサイバーセキュリティの従業員に対するトレーニングと教育を強化する。

定期的にサイバーセキュリティに関する説明会を実施していますか？

はい	取締役会	SLT	会社全体	サードパーティー サプライヤー	政府機関	顧客	非公式な アップデート	いいえ
シンガポール	38%	58%	51%	25%	29%	24%	3%	0%
平均	41%	51%	45%	22%	19%	16%	2%	1%

正式なインシデント対応計画の策定：

- 85% (平均 - 84%)

攻撃を受けた後に計画を策定した：

- 72% (平均 - 75%)

インシデントへの対応の準備状況：

- 混乱が生じている：27% (平均 - 29%)
- 準備をしているが、十分ではない：53% (平均 - 48%)
- 役割分担が明確化されており、プロフェッショナルな対応ができている 20% (平均 - 23%)

トレーニングおよび教育の効果 - セキュリティ対策の常習犯の割合：

- 取締役会：26% (平均 - 28%)
- SLT：44% (平均 - 41%)
- 従業員：43% (平均 - 38%)

ソフォスの見解

「遊ぶことなく仕事ばかりしていると、
空虚な人生が待っている」

Aaron Bugal、フィールド CTO、アジア太平洋および日本

サイバーセキュリティ業界は急速な成長を続けており、多くの求人が発生しています。

しかし、その業務内容を詳しく理解しないまま、応募される方も多く存在しています。

「サイバーセキュリティの仕事にチャレンジしたい」
という動機を聞くことが多くあります。

これは素晴らしいことですが、効果的なサイバーセキュリティ対策を遂行するためには、マルウェアの分析、フォレンジックデータの復元、システムの強化、ポリシーの策定、チームのリーダーシップなどの多くの業務が必要となります。ここで挙げたのは、サイバーセキュリティ業界で求められる業務の一部であり、これらすべての業務に対応できるジェネラリストになるように従業員に期待すると、すぐに大きな負担がのしかかることになります。

そして、亀裂が生じ始めることになります。

しかし、これは従業員の責任ではありません。多くの企業がサイバー犯罪者による攻撃から自社を守るために奔走している中で、人材不足が深刻になっており、「サイバーセキュリティの業務に携わりたい」と考えている求職者を大量に採用しようとする傾向が生まれています。

このような状況で新しく採用されたプロフェショナルの多くは、効果的なサイバーセキュリティ対策を推進するための技術的な役割や技術面以外の役割や、求められる多くの専門分野に習熟していない場合もあります。

組織のサイバーセキュリティカルチャーが成熟するのが遅い、あるいは進歩しなければ、組織で不足している能力を埋めるための適切なスキルを得られないことも多くあります。経営幹部だけがこのような問題の責任を負っているわけではありませんが、経営幹部は以下の状況を理解し、適切に支援できるように取り組まなければなりません。

脅威環境やサイバーセキュリティに関する問題が、ここ数年間で飛躍的に増大しています。企業の経営者や意思決定を推進する経営幹部は、サイバー攻撃の被害に遭った場合に、不十分な対応が招いた結果や不作為の責任を受け入れなければならなくなっています。

本レポートでは、サイバーセキュリティに関して組織が抱えているストレスについて調査した結果をお伝えしましたが、調査から、組織に変革が求められていることが明らかになっています。単純な解決策は存在しません。しかし、サイバーセキュリティへの耐性が高い企業へと進化するために求められる能力を適切に把握するためには、経営幹部は現状を把握して、方針を転換しなければならないでしょう。取締役会や経営幹部は積極的な変化を求め、責任者としての立場を明確して、サイバーセキュリティのアプローチに対するガバナンスを改善する必要があります。そのときには、計画を策定して維持する説明が経営幹部にあることを明確に示す必要があります。サイバーセキュリティは全社的な取り組みになりますが、決定する責任があり、問題が発生したときに責任を取らなければならいのも取締役会や経営幹部です。

付録

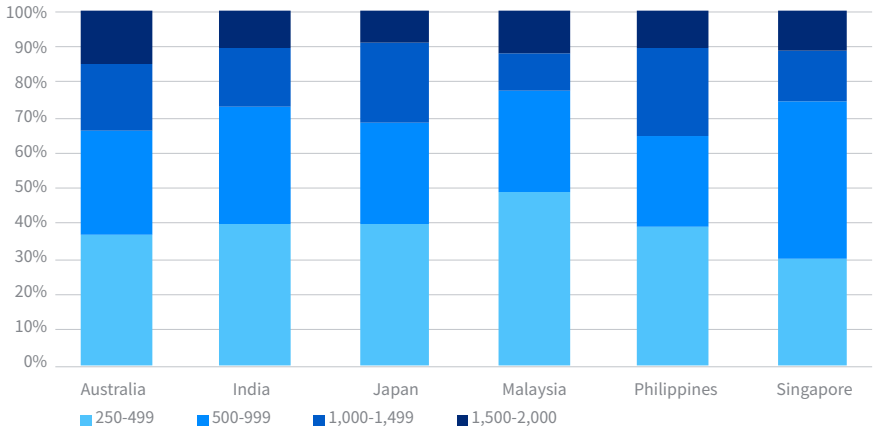
アンケート回答者の内訳と調査方法

ソフォスは 2023 年 9 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。オーストラリア (204 社)、インド (202 社)、日本 (204 社)、マレーシア (104 社)、フィリピン (103 社)、シンガポール (102 社) から合計 919 件の回答を得ました。

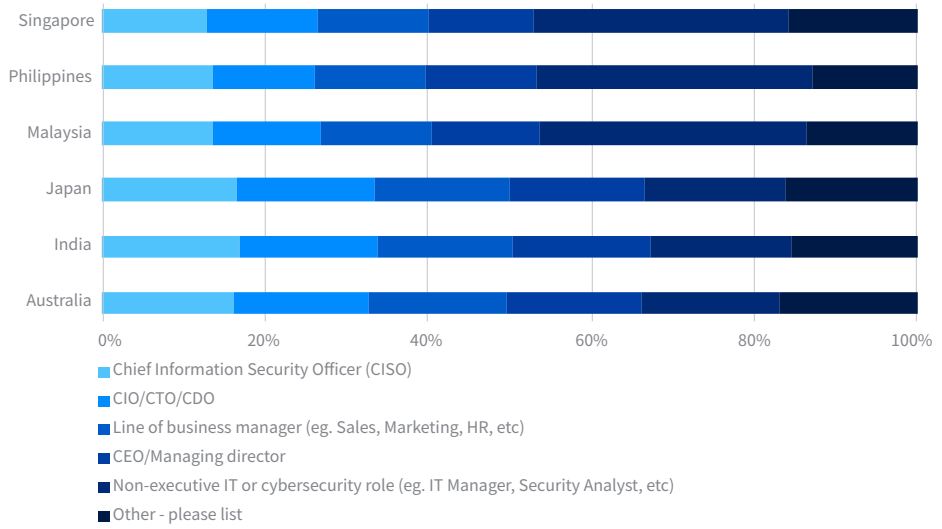
これらの企業は、オンラインアンケートに匿名で回答しています。この調査は、サイバーセキュリティと IT 部門の従業員の回答を統合し、サイバーセキュリティ燃え尽き症候群に関する個人への影響に関するデータを提供しています。

以下のグラフに、企業の規模、回答者の役割、業種についての詳細を示します。

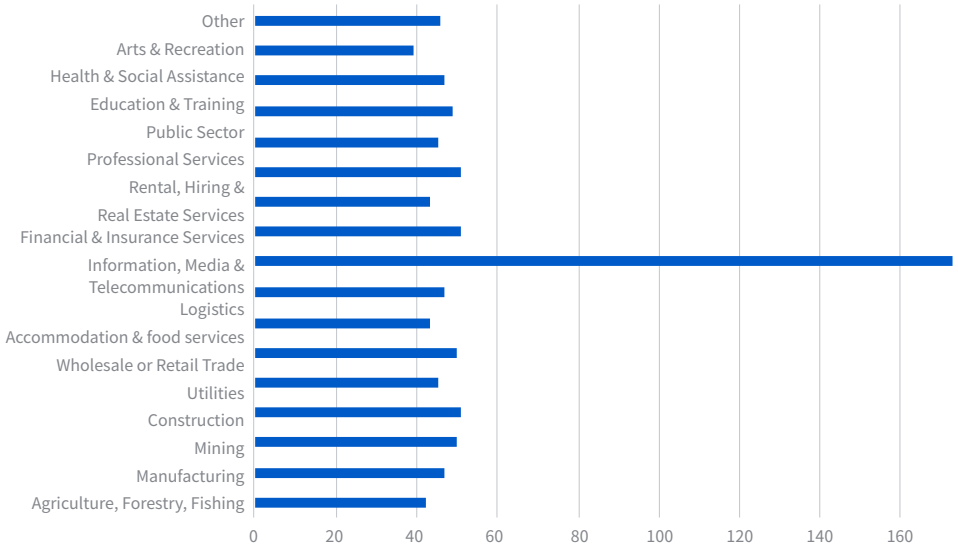
貴社の従業員数は何名ですか？



役割と国別の回答者数



業界別の回答者数



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 カ国以上の 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

Tech Research Asia (TRA) は、アジア太平洋全域の企業を対象として、テクノロジーリサーチ、コンサルティング、アドバイザリーサービスを提供しており、テクノロジートレンドとビジネスバリューへの影響の分析を専門としています。Tech Research Asia は、これらの地域のあらゆる組織、テクノロジーベンダー、チャネルパートナーが、市場の状況を詳細に読み解き、業績を向上できるように支援しています。

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。

www.techresearch.asia

2024-02-01 (WP-NP)

SOPHOS