SOPHOS

日本およびアジア太平洋地域におけるサイバーセキュリティの展望 第 5 版

ソフォスの委託による Tech Research Asia のインサイトレポート

ソフォス ホワイトペーパー 2025 年 8 月

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 5 版をご覧いただきありがとうございます。

2020 年の初版以来、ソフォスは組織における「サイバーセキュリティ運用」に影響を与える主要な問題に焦点を当て、技術的な詳細に深く踏み込むことは避けてきました。第 5 版では、サイバーセキュリティチームの構成、予算、典型的な「サイバーフラストレーション」などの分野に関する動向の最新データを引き続き紹介しています。

今回も、昨年の研究に引き続き、サイバーセキュリティの燃え尽き症候群やセキュリティ疲れに関する調査を重視しています。この問題は日本とアジア太平洋地域 (APJ) のほぼすべての組織に影響を与えており、今年のデータは 2024 年からほぼ改善が見られていないことを示しています。興味深いことに、ストレスや燃え尽き症候群に関するデータの中で、AI を活用したサイバーセキュリティツールの導入が明るい兆しとして浮かび上がりました。これらの AI ツールは、複数のシステムやツールを手動で切り替えることによって生じる精神的疲労や業務効率の低下を軽減し、脅威の迅速な特定にも寄与しています。

人工知能 (AI) が多くの企業の課題において重要な位置を占める中、ソフォスは AI を活用したビジネスソリューション (エージェント AI やコパイロットなど) が組織のサイバーセキュリティポスチャに与える影響を把握するために、最新版のレポートに新たにこのテーマを追加しました。

主な調査結果

サイバーセキュリティのストレスと燃え尽き症候群：

- ストレスレベルは依然として高く、86% の企業が従業員やサイバーセキュリティの運用に関する問題を抱えています。
- これらのストレスは、従業員のサイバーセキュリティ業務のパフォーマンス、運用のレジリエンス、インシデント対応時間が低下する要因となっています。
- この問題は生産性の低下にも影響を及ぼしており、組織では平均して週あたり 4.6 時間の損失が発生しています。これは 2024 年の平均値である 4.1 時間から 12% 増加しています。

ビジネス AI ツールの利用とサイバーセキュリティへの影響：

- シャドー AI やシャドー IT が再登場。見えにくい利用実態。すべての企業の約 85% が何らかのビジネス AI ツールを利用しており、72% の企業が正式な AI 戦略と利用ポリシーを導入しています。しかし、46% の企業は従業員が承認されていない AI ツールを使用することを防止できていません。
- このような状況により、導入されている AI ツールの特定、アクセスされているデータの内容、ツールの利用状況 (誰が、どのツールを使用しているか) についての可視性が低下しており、さらに AI ツール自体に内在する脆弱性が新たなリスク要因として浮上しています。

サイバーセキュリティの運用：

- 企業の 74% (2024 年は 75%) が専任のサイバーセキュリティチームを持ち、21% は IT 従業員にサイバーセキュリティの責任を課し、4% はすべての業務を社外のベンダーに委託しています。
- 取締役会および経営幹部チームのサイバーセキュリティに対する理解度は、2024 年のデータと比較して 5% 改善しました。
- 法規制が厳格化したことで、サイバーセキュリティ業務も一層複雑化しています。平均して 83% の企業が、サイバーセキュリティに関する法規制の枠組みを遵守する必要があると回答しています。これは、サイバーセキュリティにおけるストレスや燃え尽き症候群の軽減にはつながっていません。
- サイバーセキュリティ関連の予算は堅調であり、85% の企業が来年度の予算を増額する予定です。そのうち 24% は、10%以上の増加を見込んでいます。

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

以下の 3 つのセクションに分けて調査結果を示します。

1. サイバーセキュリティの燃え尽き症候群
2. ビジネス AI ツールの利用とサイバーセキュリティへの影響
3. サイバーセキュリティの運用

サイバーセキュリティの燃え尽き症候群

燃え尽き症候群の広がり

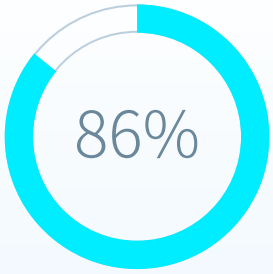
2 年連続でサイバーセキュリティの専門家は、高いレベルの燃え尽き症候群を経験していることが明らかになりました。

2024 年にサイバーセキュリティ疲労や燃え尽き症候群を経験した、または経験していると回答した組織は 85% でしたが、今年は 1% 増加して、86% に達しました。

燃え尽き症候群やサイバーセキュリティ疲れのレベルも増加しています。「頻繁に経験している」と回答した組織は、2024 年は 23% でしたが、2025 年には 29% となり、6% 増加しました。その「理由」については後ほど説明します。従業員がサイバーセキュリティ疲れを「頻繁に経験している」と回答した割合の増加傾向を見ると、シンガポールとインドの企業で特に顕著であり、それぞれ 26% および 10% の増加が見られました。

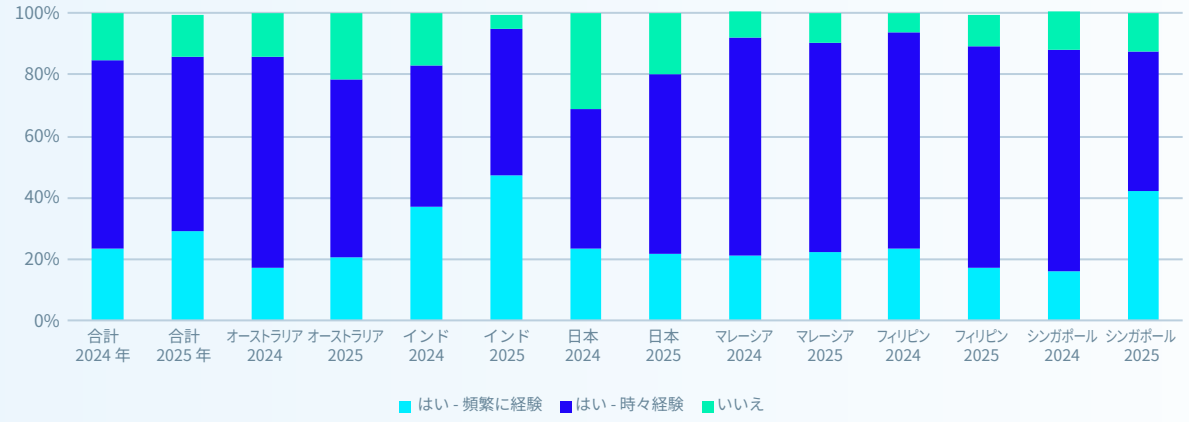
オーストラリアと日本 (20%) は、「サイバーセキュリティのストレスや燃え尽き症候群がない」と回答した企業の割合が最も高い国です。オーストラリアでは 22% の企業が問題を経験しておらず (2024 年の 14% から増加)、2025 年にこの問題を経験していない日本の組織は 20% でした。注意が必要なのは、これは見かけ上の改善に過ぎない可能性があることです。というのも、2024 年には日本の組織の 31% がこの問題を経験していなと回答していたからです。

問題を経験した企業のうち、95% が過去 12 か月間にストレスや燃え尽き症候群の増加を報告しており、その内訳は「顕著な増加」（最高レベル）が 28%、続いて「中程度の増加」が 49%、そして「わずかな増加」が 19% となっています。



サイバーセキュリティのストレスと燃え尽き症候群を報告した組織の割合。

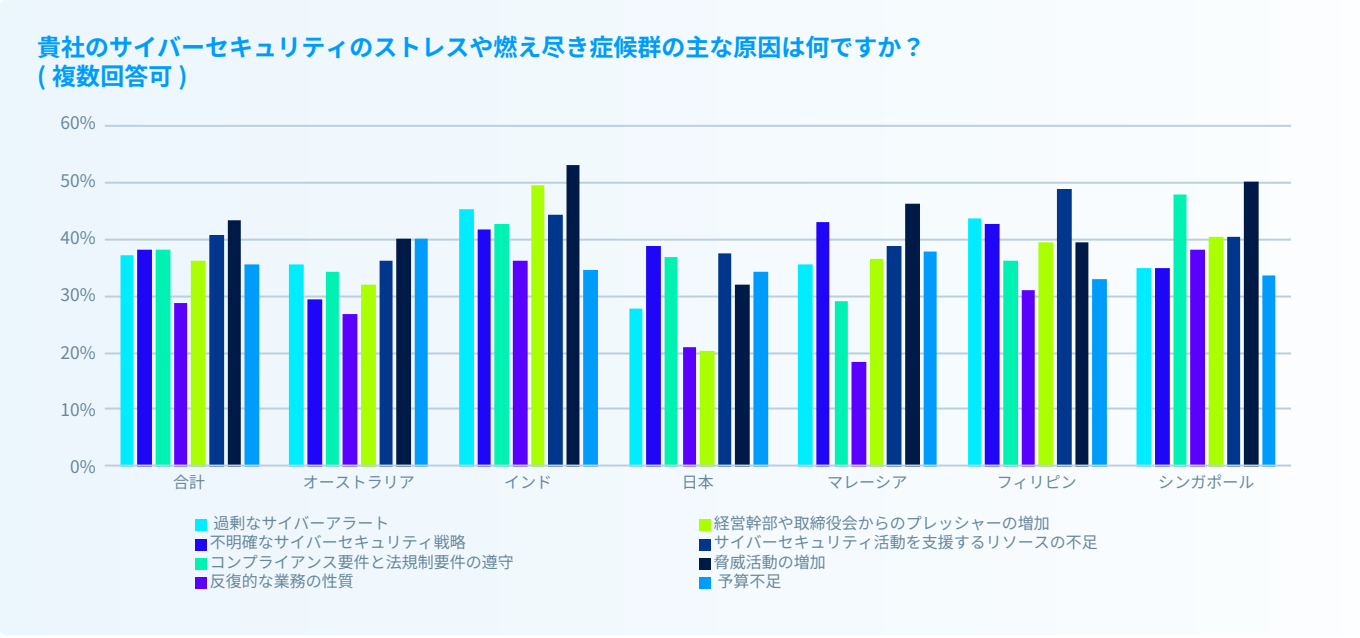
貴社の従業員は、サイバーセキュリティに関するストレスや燃え尽き症候群を経験していますか、または過去に経験したことがありますか？ 2024 年および 2025 年



ストレスと燃え尽き症候群の原因

2024 年の初回調査では、この問題の主な 5 つの要因には、役割の不明確さ、リソースの不足、経営幹部からのプレッシャーが複合的に影響していることを明らかにしました。

大まかには、今年も同様の傾向が見られますが、注目すべき例外があります。2025 年では、脅威の活動増加がストレスと燃え尽き症候群の主な原因として 1 位に浮上したことです。これは 2024 年の 5 位から 4 ランクも上昇したことになります。



上位 3 つの原因は次の通りです。

1. 脅威活動の増加
2. リソースの不足
3. コンプライアンス要件の遵守 / 不明確なサイバーセキュリティ戦略

注目すべき例外として、オーストラリアでは、「サイバーセキュリティの予算不足」と「脅威の活動増加」がストレスや燃え尽き症候群の要因として同程度挙げられています。日本の組織では、不明確なサイバーセキュリティ戦略が主な原因となっており、フィリピンではリソース不足が重要な問題となっていました。

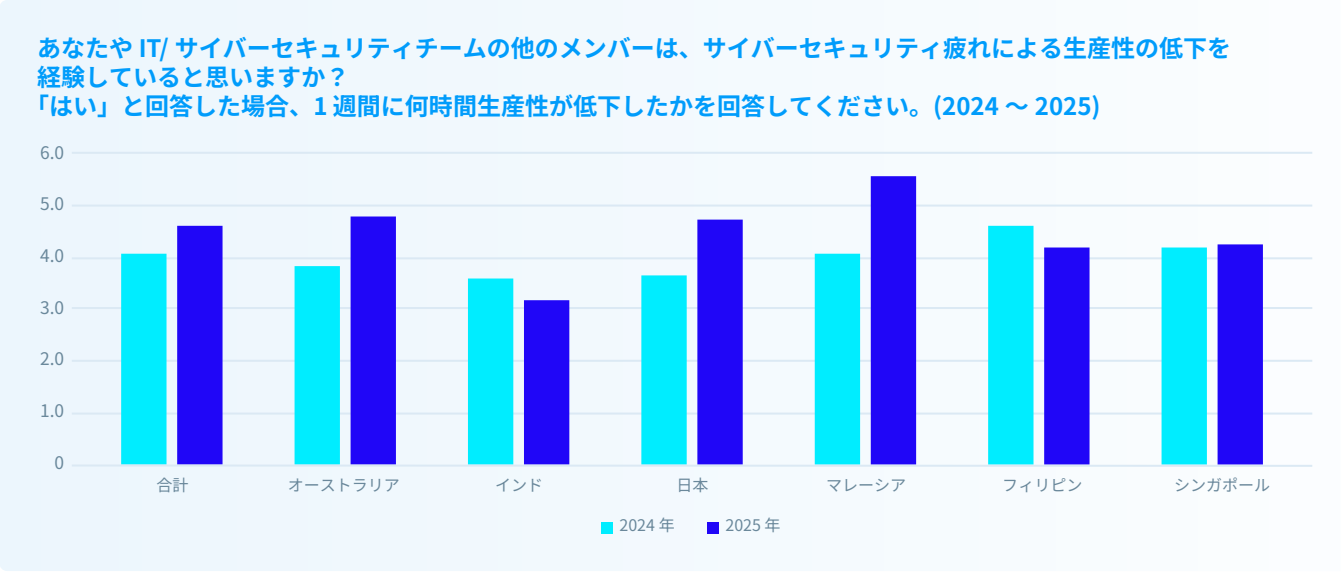
影響

サイバーセキュリティ疲れと燃え尽き症候群の影響は、業務運営の以下の 3 つの主要な領域に現れています。

1. 従業員の生産性
2. サイバーセキュリティ体制の劣化
3. 業務運営

従業員の生産性

平均して、企業はサイバーセキュリティ疲れと燃え尽き症候群によって毎週 4.6 時間の生産性低下を招いています。これは 2024 年の 4.1 時間から 12% 増加しています。



フィリピンとインドの企業では、生産性がそれぞれ 0.5 時間および 0.4 時間減少したが、他のすべての国では増加しました。

- マレーシア：毎週 1.5 時間
- 日本：毎週 1.1 時間
- オーストラリア：毎週 1.0 時間
- シンガポール：毎週 0.1 時間

日本とオーストラリアのデータを、ストレスと燃え尽き症候群のレベルと対比させると重要な洞察を得ることができます。両国はいずれも、従業員がストレスや燃え尽き症候群を経験していない企業の割合が最も高くなっています。これは、これらの国において強固かつ成熟したサイバーセキュリティ対策が実践されていることを示しており、燃え尽き症候群の少ない企業と、いまだ成熟度を高める過程にある企業との間でギャップが拡大している現状が浮き彫りになっています。

サイバーセキュリティ体制の劣化

サイバーセキュリティのストレスや燃え尽き症候群が与えている影響がないと報告したのは、僅か 5% の企業のみでした。残りの 95% の企業は、従業員のパフォーマンスの低下から、セキュリティ侵害に至るまでさまざまな影響を受けています。

42% がサイバーセキュリティおよび IT 担当者のパフォーマンス低下を経験

41% がサイバーセキュリティのレジリエンスの低下を経験

39% がインシデント対応の時間が遅くなったと回答

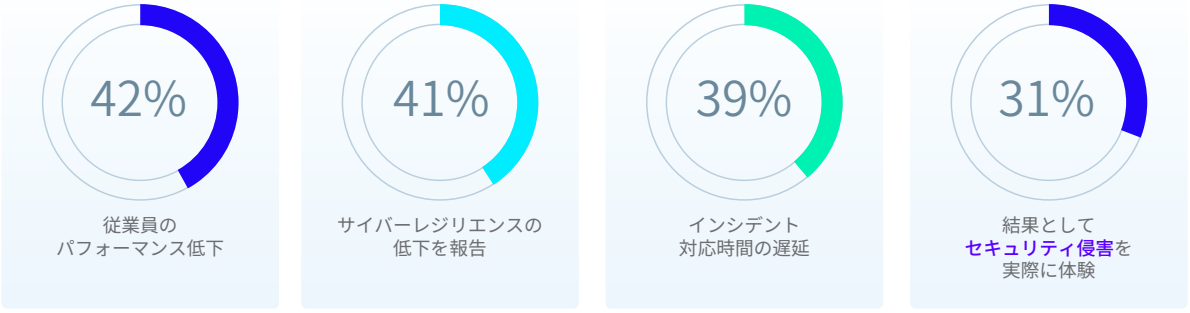
34% がサイバーセキュリティの責任に対して、懐疑的、無関心、無気力のような感情を従業員が抱いていると指摘

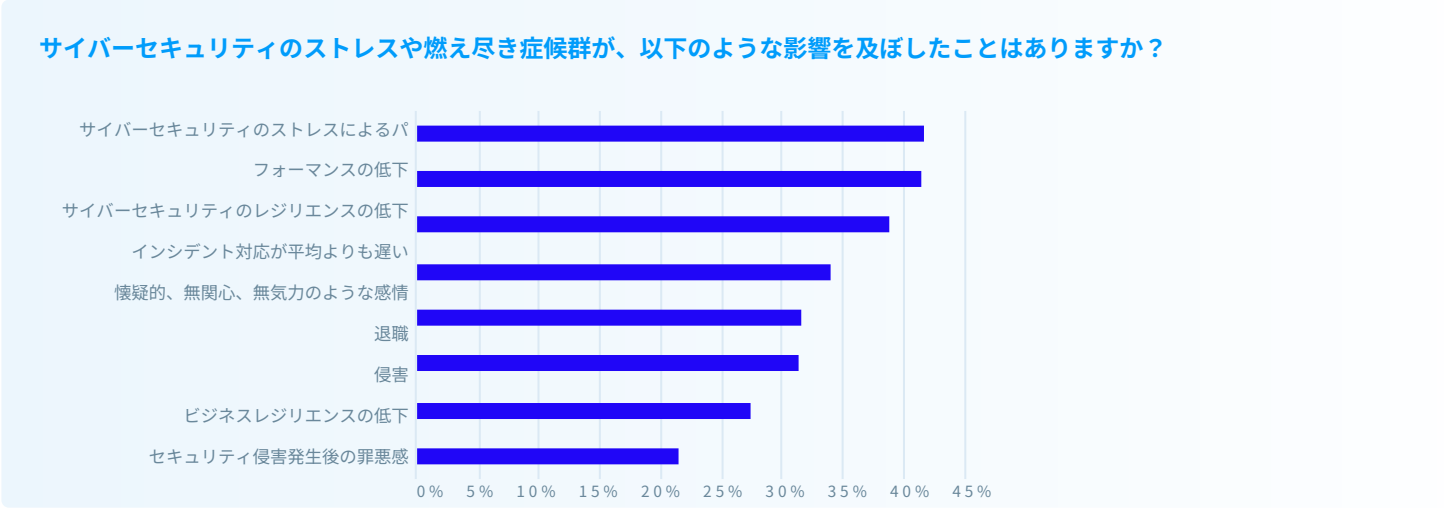
32% が従業員の退職を経験

31% がセキュリティ侵害を経験

燃え尽き症候群による測定可能な影響

ストレスと燃え尽き症候群を経験している企業の 95% が、組織に直接的な影響があったことを報告しています。





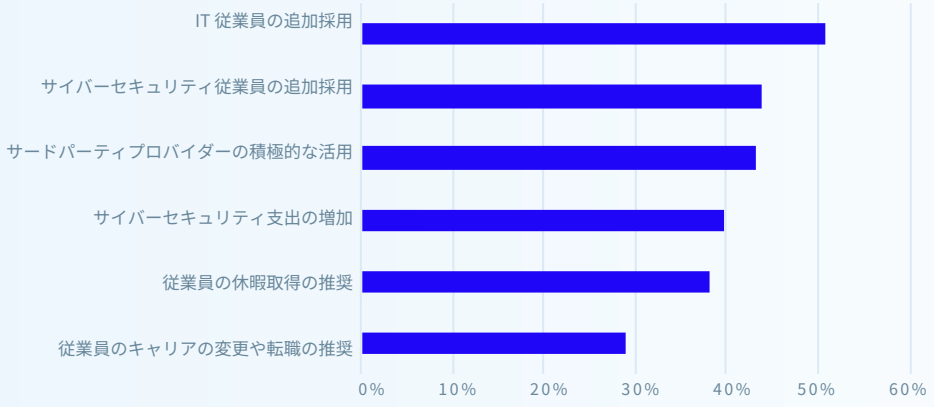
国別にデータを見ていくと、いくつかの違いが見られます。たとえば、シンガポールでは 50%、インドでは 44% の企業が、従業員が懐疑的あるいは無気力といった感情を抱えていると回答しています。これに対し、全体の平均は 34% です。ただし、パフォーマンスの低下、レジリエンスの低下、対応時間の遅延といった主要な 3 つの影響については、すべての国の企業でほぼ同じ割合で報告されています。

業務運営

ストレスと燃え尽き症候群の影響を受ける 3 位の分野は、組織の業務運営です。

- サイバーセキュリティソリューションの予算増加への圧力：40% の企業が、ストレスと燃え尽き症候群を軽減するためにサイバーセキュリティツールへの支出を増加させています。
- スキルの高いサイバーセキュリティ人材の採用と定着：51% が IT 人材を追加で採用し、44% がサイバーセキュリティ人材を追加で採用しており、29% は従業員にキャリアの変更や転職を促しています。
- 業務を強化するために、マネージドセキュリティサービスプロバイダー (MSSP など) などのサードパーティパートナーの利用を増加：43% が、業務を強化するためにパートナーのより積極的に活用しています。

サイバーセキュリティに関するストレスや燃え尽き症候群が原因で、以下のいずれかの対応を取ったことはありますか？



IT やサイバーセキュリティプロフェッショナルの採用はほぼすべての国で最優先課題となっており、最も大きな問題として挙げられています (マレーシアは例外であり、業務を強化するためにパートナーを積極的に活用しています)。

フィリピン (59%)、オーストラリア (51%)、日本 (45%) では IT 従業員の採用が最優先課題であり、シンガポール (62%) やインド (58%) ではサイバーセキュリティ従業員の採用が最優先課題となっています。

多くの国でスキル不足が深刻な課題となっており、組織は即戦力となる人材の迅速な採用を望んでいます。しかし実際には、採用には時間がかかるうえ、高額なコストも伴うため、ストレスや燃え尽き症候群といった課題に対する即効性のある解決策とはなりにくいのが現状です。

プレッシャーが継続する中でも、ストレスや燃え尽きの軽減につながる前向きな兆候も見られました。AI を活用したサイバーセキュリティツールを導入している組織では、以下の 2 つの分野で迅速な効果が表れています。

1. 56% の企業が、セキュリティインシデントの兆候を特定し、エスカレーションの精度を向上することで、ストレスと燃え尽き症候群の減少を報告
2. 40% が、AI によって人間のオペレーターによるセキュリティインシデントのトリアージにおけるスピードと正確性が高まったと指摘

ビジネス AI ツールの利用とサイバーセキュリティへの影響

AI に関する調査を続け、ビジネス AI ソリューションが組織のサイバーセキュリティにどのような影響を与えているのかを把握することにしました。

ソフォスのデータによれば、2024 年に AI ツールの利用がほぼ主流となってきた頃から、各組織では導入や展開の取り組みが徐々に成熟し始めていることが分かります。

調査対象の 85% が、何らかのビジネス AI ツールを導入しており、一般的にはコパイロットや大規模言語モデル (LLM) をサポートするソリューションが使われています。これらの多くは、ビジネスプロセスの自動化や、従業員の生産性向上、営業、マーケティング、コンテンツ制作のニーズを満たすことを目的としています。

他のテクノロジーと同様に、AI ソリューションも既存のプラットフォームやデータセットとの統合が不可欠であり、通常は堅牢なデータガバナンス、ユーザーガバナンス、サイバーセキュリティの監視体制が求められます。AI ツールは、その特性上、ビジネスやテクノロジープラットフォームのさまざまな側面に深く統合されるため、運用は一層複雑になります。

多くの企業にとって、データの品質とガバナンスは依然として大きな障壁となっており、未成熟なデータインフラや、各国で厳格化が進むプライバシー規制への対応に苦慮しています。さらに、知的財産や顧客データの誤用に伴うリスクも高まりつつあります。

本調査で対象とした 6 か国すべての政府が、透明性、説明責任、倫理基準に焦点を当てて、責任ある AI 利用を目指して国家的な枠組みを確立するため、AI に関する法整備を進めていますが、その重点を置いている分野には国によって異なります。

今回の調査では、72% の企業が「誰が、どのような AI を、どのように活用するか」を明確に定めた正式な戦略を策定していることが明らかとなっており、これは非常に好ましい傾向と言えます。

AI ツールは導入やセキュリティの確保が複雑であり、業務に深く統合されることもあるため、次のような追加の懸念事項も挙げられています。

- 承認された AI ツールと並行して使用されている、非公式なシャドー AI ツールの利用
- どの AI 環境にどのデータが存在しているのか、どのツールやユーザーがそのデータにアクセスできるのか、これら環境を適切にガバナンスする方法についての可視性。

勢いを増すシャドー AI

シャドー AI がすでに APJ の企業で利用されているという結果は、予想通りでした。

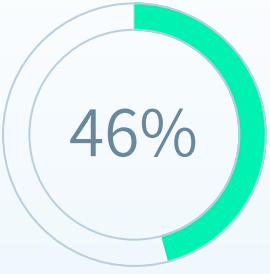
- 46% の企業では、従業員が承認されていない AI ツールを使用しており、さらに 12% の企業は、シャドー AI アプリが自社に存在するかどうかを把握していませんでした。
- シャドー AI を最も多く利用していたのは、インド (62% の企業)、シンガポール (60%)、日本 (47%) の企業でした。

AI ポリシーやガイドラインを整備していても、シャドー AI を確実に防ぐことができるわけではありません。AI ポリシーとフレームワークを設定している 72% の企業のうちの 54% がシャドー AI に関する問題を経験しています。

また、ソフォスの以下の分析結果から、組織は特にツール、ユーザー、データについて AI 環境の可視性を強化する必要があることが明らかになっています。

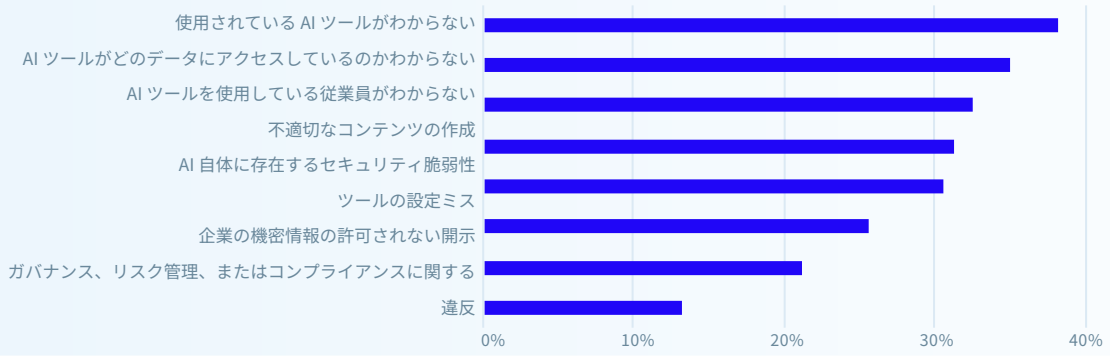
- 38% の企業は使用されている AI ツールについて十分に可視化できていない (インドが最も高く 47%、マレーシアは 41%)。
- 35% の企業は AI ツールがアクセスしているデータを把握していない (フィリピン 43%、シンガポール 41%)。
- 33% の企業は AI ツールを使用して従業員を特定できていない (インド 39%、シンガポール 38%)。
- 31% の企業は、AI ツール自体に組織のリスクを高める恐れのある脆弱性を特定している (インド 44%、マレーシア 35%)。
- 26% の企業は AI ツールの設定ミスを経験している (フィリピン 42%、インド 31%)。

シャドー AI が蔓延している



すでに従業員が無許可の AI ツールを使用している組織の割合

従業員が AI ツールを使用するときに、以下のいずれかの問題を経験したことがありますか？



サイバーセキュリティの運用

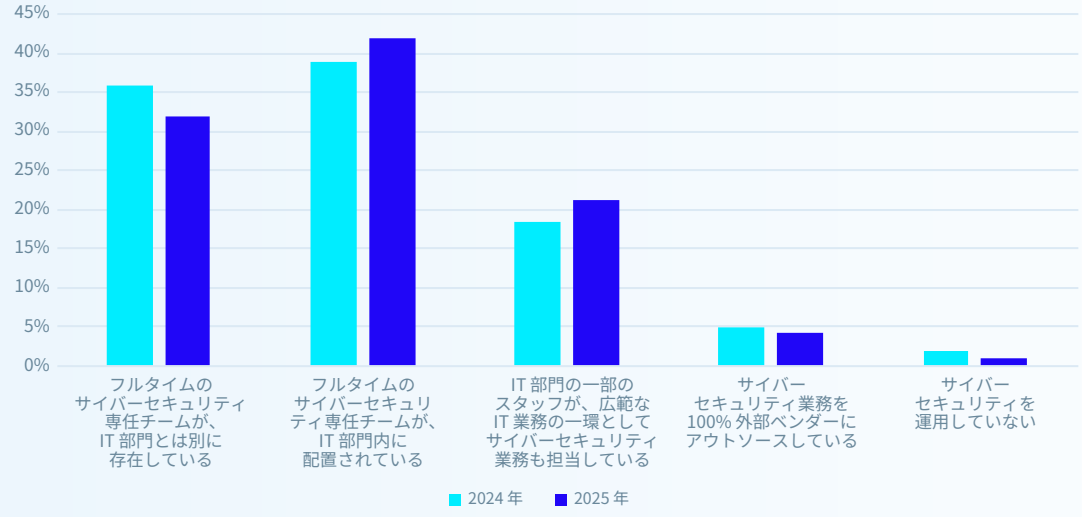
最後に、組織がどのようにサイバーセキュリティの運用体制を構築しているか、どの役職がサイバーセキュリティに責任を持ち、誰に報告しているのか、今後 12 か月の予算がどのように変化するかを調査しました。

運用体制

2024 年以降のデータを追跡したところ、IT 部門とは別に編成されたチームではなく、IT 部門内に専任のフルタイムのサイバーセキュリティチームを配置する企業が、わずかに増加している傾向が見られます。

- 2024 年には、39% のサイバーセキュリティチームが IT 部門内で運営されていましたが、2025 年には 3% 増加しました。一方で、IT 部門に属さずに活動するチームは、36% から 32% へと 4% 減少しました。
- マレーシア (51%) とオーストラリア (48%) は、サイバーセキュリティチームが IT 部門に属している割合が最も高く、シンガポール (47%) とインド (43%) は、IT 部門から独立して活動しているサイバーセキュリティチームの割合が最も高くなっています。
- サイバーセキュリティ人材の確保が難しい現状を反映してか、サイバーセキュリティ業務を IT 担当者に兼任させ、IT とセキュリティの両方を担わせる企業が 3% 増加しました。
- サイバーセキュリティ業務を 100% アウトソースしている企業は、5% から 4% に減少しましたが、日本とフィリピンは 6% と平均を上回っていました。

現在の貴社におけるサイバーセキュリティ体制として最も当てはまるものは次のどれですか？

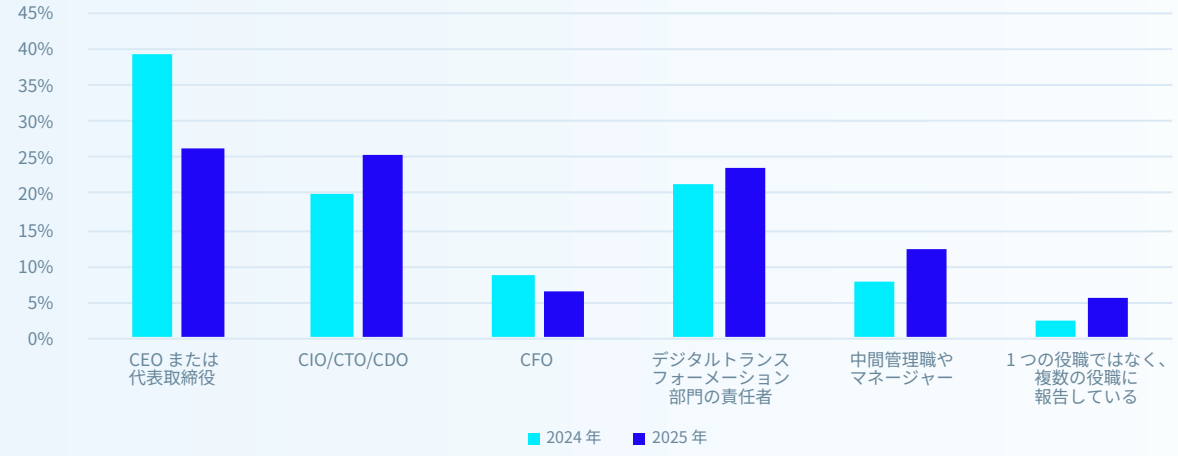


報告の仕組み

2025 年のサイバーセキュリティの問題を報告する仕組みは、2024 年から大きく変化しました。

- 注目すべき点として、サイバーセキュリティの責任者が CEO や代表取締役に直接報告するケースは、2024 年から 2025 年の間で 13% 減少しました。
- 一方で、2024 年から 2025 年にかけて IT リーダー (CIO、CTO、CDO) に報告するケースが 5% 増加し、デジタルトランスフォーメーションプログラムを担当するリーダーに報告するケースも 3% 増加しました。

現在の貴社ではサイバーセキュリティの問題をどの役職に報告していますか？



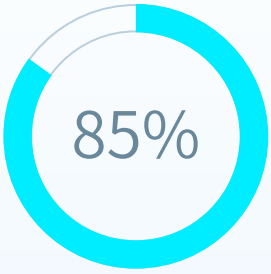
サイバーセキュリティ予算

サイバーセキュリティの予算は、通常、CIO (35%) や CISO (26%) が決定していますが、データによると、CEO や代表取締役が決定しているケースも 14%、CFO が決定しているケースが 9% あります。また、7% の企業は経営幹部全体で予算に関する責任を共有していると回答しています。

セキュリティ予算は 2024 年から引き続き増加しており、85% の組織が今後 12 か月間で予算が増加すると回答しました。これは前年の 83% から 2% の増加です。

- 24% の組織が 10% 以上増加すると予測
- 34% の組織が 5 ～ 10% 増加すると予測
- 27% の組織が 1 ～ 4.99% 増加すると予測
- 13% の組織は予算が変わらないと予測
- 2% の組織が、予算が減少すると予測

サイバーセキュリティ予算が拡大している



サイバーセキュリティ予算を増やすことを予定している組織の割合。24% の組織は 10% 以上の増加を予測しています。

一般的なフラストレーション

調査の締めくくりとして、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、上位 5 つのフラストレーションの要因の 3 つが大きく順位を上げました。これらの要因はいずれも脅威活動の増加、規制の強化、セキュリティ文化や理解の不足に関連していました。

以下の表に、これらのフラストレーションと 5 年間の順位を示します。

問題と順位	2019	2021	2022	2023	2025
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が困難になっている。	8	9	5	7	**1**
法規制への対応が受け身になっており、サイバーセキュリティの管理がより困難になっている	トップ 10 圏外	トップ 10 圏外	トップ 10 圏外	10	**2**
企業全体で強固なサイバーセキュリティ文化を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	**3**
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	**4**
恐怖と疑念を煽るメッセージによって、サイバーセキュリティについて正しい議論することが難しくなっている	トップ 10 圏外	トップ 10 圏外	トップ 10 圏外	トップ 10 圏外	**5**
スキルの高い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	**6**
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	7	7	1	3	**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	4	**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、真剣ではない	9	5	8	5	**9**
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	3	1	4	6	**10**
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	**トップ 10 圏外**

脅威活動の増加 (1 位のフラストレーション) と規制の複雑化 (2 位) は、依然として困難な課題となっています。AI を悪用した脅威は、新たな攻撃を生み出すスピードを高めるだけでなく、一部のサイバーセキュリティ防御ツールやソリューションの効果を低下させています。

ソフォスの調査によると、規制強化に関するフラストレーションは以下の 4 つの領域に関連しています。

- 47% が法規制を遵守するためにサイバーセキュリティのコストが増加すると回答
- 36% が法規制はストレスや燃え尽き症候群のレベルを高める直接的な原因になっていると回答
- 36% がビジネスの推進よりも規制対応を優先せざるを得なくなったと回答
- 34% がビジネスの推進よりもコンプライアンス要件への対応のためにリソースが割かれたと回答

最後は前向きな話で締めくくりますが、法規制やコンプライアンス要件の厳格化による影響について尋ねたところ、以下のような回答がありました。

- 56% が、コンプライアンス要件の遵守やサイバーセキュリティフレームワークの導入などが、サイバーセキュリティとビジネスレジリエンスの両方に良い影響を与えたと回答
- また、51% が、法規制は戦略的な指針や改善に役立つだけでなく、戦術面と運用面を強化し、より強固なサイバーセキュリティ体制の構築につながっていると回答

まとめ

燃え尽き症候群は、依然として多くの組織にとって重要な課題となっています。サイバーセキュリティに起因するストレスや燃え尽き症候群は 86% の企業が経験し、従業員のパフォーマンス、オペレーショナルレジリエンス、インシデント対応、生産性を低下させています。また、週あたり平均で 4.6 時間の労働損失を引き起こしています。これは 2024 年と比較して 12% 増加しています。 AI を活用したサイバーセキュリティツールは、インシデントの検知精度を高め、トリアージの迅速化を実現することで、こうしたストレス要因の一部を緩和する助けとなります。

昨年と比較すると、燃え尽き症候群の原因が変化しており、脅威活動の増加が最大のストレス要因となっており、リソース不足と不明確なサイバーセキュリティ戦略が続いています。多くの組織は、このような課題に対応するため、サイバーセキュリティへの支出を増やし、人員を増強し、外部パートナーとの連携を強化するなどの対応を取っていますが、人材採用は依然として困難な状況です。

85% の企業がすでにビジネス AI ツールを導入しており、72% が正式な AI 戦略を策定していますが、一方で 46% の企業が、従業員が未承認の AI ツールを使用していることを報告しています。この「シャドー AI」は、ツールの可視化やデータガバナンスの課題を引き起こしており、潜在的なリスクをもたらしています。明確な戦略なしに AI ビジネスツールを導入し、適切に管理しなければ、サイバーセキュリティ環境が複雑化する恐れがあります。多くの企業がすでに複雑なサイバーセキュリティの課題に直面している中で、これは好ましくありません。

全体の 74% の組織が専任のサイバーセキュリティチームを設置していますが、IT 業務とサイバーセキュリティの両方を兼任するチーム体制を取っている組織もあります。法規制の強化は、83% の組織に影響を与えており、業務の複雑化やストレスの増加を招いているものの、戦略的な観点からは一定の利点も見られます。セキュリティ予算は依然として堅調であり、85% の組織が予算増加を予定しており、そのうち 24% は 10% 以上の増加を見込んでいます。

全体的に、サイバーセキュリティ疲れと燃え尽き症候群は依然として高い水準にありますが、AI ツールと法規制の枠組みによる軽減効果も見られています。サイバーセキュリティ予算は APJ の組織が抱えている課題に対応するために増加している傾向にあります。

ソフォスの見解

重要なのは、過去の実績ではなく、これからの成果。

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に関する最新レポートは、これらの地域の多様な業種におけるサイバーレジリエンスの現状について、鋭い洞察を提供しています。今回のレポートタイトルには明確な意図が込められています。私たちは「情報の時代」から「生成 AI の時代」へと移行しています。

目まぐるしいほどの勢いで、あらゆる業務フロー、プロセス、プラットフォームに AI が組み込まれつつあります。AI の利点を否定するつもりはありません。AI は、適切に活用すれば、サイバーセキュリティチームの能力を飛躍的に向上させる強力なツールとなり得ます。しかし、現実は理想とは程遠いところにあります。

シャドー IT 2.0 と呼ばれる現象が起こっています。これまでにも両刃の剣と評価されるさまざまな事象を見てきましたが、生成 AI はその頂点に立っています。この両刃の剣の一方の刃は、慎重に導入すれば非常に役立ちます。サイバーセキュリティチームに好ましい成果をもたらし、特に AI がチームの対応力を実質的に拡大し、オペレーターの時間を解放する点で、その効果は顕著です。

しかし、両刃の剣のもう一方の刃として、AI によって発生する課題があり、チームに対して直接および間接的なプレッシャーをかけています。特定のタイミングで世界規模の変化を正確に把握するのは難しいのですが、AI が業務レベルで活用されているかどうか、自社のチームや事業部門の声に耳を傾けて直接確認してみる価値があります。否定的な意見やよくわからないという回答が返ってくるかもしれませんが、「わからないけど、AI アプリは詳しく質問に答えてくれる」という多くの声が聞かれるはずです。

再び諸刃の剣の話に戻りますが、多くの組織では、現場レベルの生産性を高めるために AI ツールの活用が大幅に増えています。これは、シャドー IT が今もなお存在していることの明確な証拠と言えるでしょう。そもそも、シャドー IT がなくなった時期など本当にあったのでしょうか。シャドー IT が再び広がりを見せている背景には、増大する業務負荷への対応が求められている現状があります。この負荷はストレスの原因となり得ます。今年の「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」レポートでは、ストレス、そして最終的に燃え尽き症候群を引き起こす主な要因として、脅威活動の増加、リソース不足、コンプライアンス要件の遵守の 3 つが挙げられています。これはまさに「三重苦」とも言える状況であり、現場で働く従業員には過酷なプレッシャーがのしかかっています。

私は AI そのものに反対しているわけではありません。問題なのは、規制、監視、評価がないまま AI を導入・活用しようとする無秩序なアプローチです。

すべての企業が、AI 活用に関する自社独自の明確なガバナンス体制を整備すべきです。AI とは何か、そしてどのようなものなのか、特にその成果について明確に説明することは、エンドユーザーが接している情報処理ツールが自社によって所有・運用されていない可能性があることを理解する助けになります。この「所有・運用されていない」という事実自体が、リスク管理ガイドラインを確立して適用すべきことを強く示しています。

少なくとも、セキュリティ意識向上プログラムやトレーニングでは、受信トレイに届く脅威を特定することだけに焦点を当てるべきではありません。情報をどのように取り扱うのか、サードパーティサービスにどのように提供すべきかなどを含めながら、プログラムを進化させていく必要があります。例えば、機密の財務レポートをお気に入りの対話型 AI サービスにアップロードして要約させることは、危険な行為です。

安易な解決策に頼ることで一時的には楽をできるかもしれませんが、多面的な AI 機能を性急に導入したり、企業の支援 (管理) なしで展開したりすると、リスクとなります。間接的なプレッシャーについて先に述べましたが、AI の導入によるパフォーマンス向上が見えにくい形で進むため、人員削減の口実に使われる可能性があります。これは、一部の企業にとってはメリットとなる一方、他の企業にとってはリスク要因となる可能性もあります。

組織は、新しい AI ツールを導入・展開する際に、強力なガバナンス機能、および評価と監視を伴う手法を通じて、共生関係を築く必要があります。これにより、どこに成果が見込めるのか、そしてそれがどれほど経済的かつ持続可能かが明確になります。優れた解決策のはずですが、現実はそうなっていません。

特に AI 利用に責任を持つチームのメンバー、あるいはその責任をあなたが任せた方々に、どれほど AI に依存しているかを尋ねてみてください。AI が突然使えなくなった場合、どのように対処するのか、その行動方針を聞いてみてください。長い間、不安そうな沈黙が続くようであれば、それは解決すべき問題が存在している証拠です。そのチームの業務負荷が、自社で把握しているかどうか分からないプラットフォームに依存している可能性があります。速やかに話し合いを始めましょう。

Aaron Bugal、APJ 地域、最高情報セキュリティ責任者

国別のプロファイル

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。

オーストラリア

サイバーセキュリティのストレスと燃え尽き症候群

- 頻繁に経験している：20% (2024 年は 17%)
- 時々経験している：58% (2024 年は 69%)

原因のトップ 3：

- 予算不足 / 脅威活動の増加
- リソース不足 / 過剰なサイバーアラート
- コンプライアンス要件と法規制要件の遵守

影響のトップ 3：

- サイバーセキュリティ体制の弱体化
- インシデント対応時間の遅延 / パフォーマンスの低下
- セキュリティ侵害

リソースへの影響のトップ 3：

- IT 人材の追加採用の必要性
- サイバーセキュリティ疲れや燃え尽き症候群を抱える従業員への休暇取得の推奨
- サイバーセキュリティ人材の追加採用の必要性

ストレスや燃え尽き症候群による生産性の低下：

- 毎週 4.8 時間 (2024 年は毎週 3.8 時間)

ストレスや燃え尽き症候群を抱える従業員に対して、カウンセリングを行っていますか？

- はい、69% (2024 年は 68%)

サイバーセキュリティにおける AI の影響

ChatGPT、エージェント AI、コパイロットなどのビジネス AI ツールを使用している組織の割合：

- 70% の組織が正式な AI 戦略を策定
- 53% の組織が許可されていない AI ツールを使用 (シャドー AI)
- そのうち 32% が無許可の使用を認識しており、13% は状況を認識していない

経験した問題のトップ 3：

- 使用されている AI ツールがわからない
- AI ツールがどのデータにアクセスしているのかわからない
- AI ツールを使用している従業員がわからない

AI をサイバーセキュリティに活用する最大の利点：

セキュリティインシデントを正確にトリアージし、調査のために人間のオペレーターへエスカレーションすること

サイバーセキュリティの運用

一般的なサイバーセキュリティのフラストレーションのトップ 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が困難になっている
- 法規制への対応が受け身になっており、結果としてサイバーセキュリティの管理がより困難になっている
- 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

運用体制：

- IT 部門とは独立したフルタイムのサイバーセキュリティ専門チームを設置：27%
- IT 部門内にフルタイムのサイバーセキュリティ専門チームを設置：48%
- IT 部門の従業員がサイバーセキュリティの業務を兼任：20%
- 100% アウトソース：4%

サイバーセキュリティに最も責任を持つ役職 / 報告先：

CIO/IT ディレクター、CEO/ 代表取締役に報告

予算

	合計予算	オーストラリア
10% 以上増加	24%	15%
5 ～ 9.99% 増加	34%	34%
1 ～ 4.99% 増加	27%	31%
増減なし	13%	19%
1 ～ 4.99% 減少	1%	1%
5 ～ 9.99% 減少	1%	0%
10% 以上減少	0%	0%

インド

サイバーセキュリティのストレスと燃え尽き症候群

- 頻繁に経験している：47% (2024 年は 37%)
- 時々経験している：48% (2024 年は 46%)

原因のトップ 3：

- 脅威活動の増加
- 取締役会や経営幹部からの圧力の増加
- 過剰なサイバーアラート

影響のトップ 3：

- IT およびサイバーセキュリティチームのパフォーマンス低下 / サイバーセキュリティレジリエンス体制の弱体化
- インシデント対応時間の遅延
- サイバーセキュリティ業務や責任に対して、懐疑的、無関心、無気力のような感情を抱いている。

リソースへの影響のトップ 3：

- サイバーセキュリティ従業員の追加採用の必要性
- サイバーセキュリティツールやソリューションへの支出の増加
- IT 従業員の追加採用の必要性

ストレスや燃え尽き症候群による生産性の低下：

- 毎週 3.2 時間 (2024 年は毎週 3.6 時間)

ストレスや燃え尽き症候群を抱える従業員に対して、カウンセリングを行っていますか？

- はい、87% (2024 年は 74%)

サイバーセキュリティにおける AI の影響

ChatGPT、エージェント AI、コパイロットなどのビジネス AI ツールを使用している組織の割合：

- 97% の組織が正式な AI 戦略を策定
- 92% の組織が許可されていない AI ツールを使用 (シャドー AI)
- そのうち 62% が無許可の使用を認識しており、31% は状況を認識していない

経験した問題のトップ 3：

- 使用されている AI ツールがわからない
- AI ツール自体に存在する脆弱性が、組織を危険にさらす可能性がある
- AI ツールがどのデータにアクセスしているのかわからない

AI をサイバーセキュリティに活用する最大の利点：

セキュリティインシデントを正確にトリアージし、調査のために人間のオペレーターへエスカレーションすること

サイバーセキュリティの運用

一般的なサイバーセキュリティのフラストレーションのトップ 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が困難になっている
- 法規制への対応が受け身になっており、結果としてサイバーセキュリティの管理がより困難になっている
- 企業全体で強固なサイバーセキュリティ文化を構築することに苦労している

運用体制：

- IT 部門とは独立したフルタイムのサイバーセキュリティ専門チームを設置：43%
- IT 部門内にフルタイムのサイバーセキュリティ専門チームを設置：34%
- IT 部門の従業員がサイバーセキュリティの業務を兼任：19%
- 100% アウトソース：3%

サイバーセキュリティに最も責任を持つ役職 / 報告先：

CEO/ 代表取締役、CIO、デジタルトランスフォーメーション部門の責任者

予算

	合計予算	インド
10% 以上増加	24%	30%
5 ～ 9.99% 増加	34%	41%
1 ～ 4.99% 増加	27%	21%
増減なし	13%	4%
1 ～ 4.99% 減少	1%	2%
5 ～ 9.99% 減少	1%	3%
10% 以上減少	0%	0%

日本

サイバーセキュリティのストレスと燃え尽き症候群

- 頻繁に経験している：21% (2024 年は 23%)
- 時々経験している：59% (2024 年は 46%)

原因のトップ 3：

- 不明確なサイバーセキュリティ戦略
- リソースの不足
- コンプライアンス要件と法規制要件の遵守

影響のトップ 3：

- IT およびサイバーセキュリティチームのパフォーマンス低下
- サイバーセキュリティ体制の弱体化
- 退職

リソースへの影響のトップ 3：

- IT 人材の追加採用の必要性
- サイバーセキュリティ運用を効率化するためにサードパーティのパートナーを利用
- サイバーセキュリティ人材の追加採用の必要性

ストレスや燃え尽き症候群による生産性の低下：

- 毎週 4.7 時間 (2024 年は毎週 3.6 時間)

ストレスや燃え尽き症候群を抱える従業員に対して、カウンセリングを行っていますか？

- はい、75% (2024 年は 66%)

サイバーセキュリティにおける AI の影響

ChatGPT、エージェント AI、コパイロットなどのビジネス AI ツールを使用している組織の割合：

- 80% の組織が正式な AI 戦略を策定
- 63% の組織が許可されていない AI ツールを使用 (シャドー AI)
- そのうち 47% が無許可の使用を認識しており、12% は状況を認識していない

経験した問題のトップ 3：

- AI ツールを使用している従業員がわからない
- 使用されている AI ツールがわからない
- AI ツールがどのデータにアクセスしているのかわからない

AI をサイバーセキュリティに活用する最大の利点：

- セキュリティインシデントを正確にトリアージし、調査のために人間のオペレーターへエスカレーションすること

サイバーセキュリティの運用

一般的なサイバーセキュリティのフラストレーションのトップ 3：

- 予算が不足している
- 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が困難になっている
- スキルの高い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

運用体制：

- IT 部門とは独立したフルタイムのサイバーセキュリティ専門チームを設置：22%
- IT 部門内にフルタイムのサイバーセキュリティ専門チームを設置：39%
- IT 部門の従業員がサイバーセキュリティの業務を兼任：31%
- 100% アウトソース：6%

サイバーセキュリティに最も責任を持つ役職 / 報告先：

中間管理職やマネージャー、
デジタルトランスフォーメーション部門の責任者、CIO

予算

	合計予算	日本
10% 以上増加	24%	21%
5 ～ 9.99% 増加	34%	28%
1 ～ 4.99% 増加	27%	27%
増減なし	13%	19%
1 ～ 4.99% 減少	1%	3%
5 ～ 9.99% 減少	1%	1%
10% 以上減少	0%	1%

マレーシア

サイバーセキュリティのストレスと燃え尽き症候群

- 頻繁に経験している：22% (2024 年は 21%)
- 時々経験している：68% (2024 年は 71%)

原因のトップ 3：

- 脅威活動の増加
- 不明確なサイバーセキュリティ戦略
- リソースの不足

影響のトップ 3：

- サイバーセキュリティ体制の弱体化
- IT およびサイバーセキュリティチームのパフォーマンス低下
- インシデント対応時間の遅延

リソースへの影響のトップ 3：

- サイバーセキュリティ運用を効率化するためにサードパーティのパートナーを積極的に活用
- IT 人材の追加採用の必要性
- サイバーセキュリティツールやソリューションへの支出の増加

ストレスや燃え尽き症候群による生産性の低下：

- 毎週 5.6 時間 (2024 年は毎週 4.1 時間)

ストレスや燃え尽き症候群を抱える従業員に対して、カウンセリングを行っていますか？

- はい、73% (2024 年は 72%)

サイバーセキュリティにおける AI の影響

ChatGPT、エージェント AI、コパイロットなどのビジネス AI ツールを使用している組織の割合：

- 91% の組織が正式な AI 戦略を策定
- 78% の組織が許可されていない AI ツールを使用 (シャドー AI)
- そのうち 36% が無許可の使用を認識しており、13% は状況を認識していない

経験した問題のトップ 3：

- 使用されている AI ツールがわからない
- AI ツール自体に存在する脆弱性が、組織を危険にさらす可能性がある
- AI ツールを使用している従業員がわからない

AI をサイバーセキュリティに活用する最大の利点：

セキュリティインシデントを正確にトリアージし、調査のために人間のオペレーターへエスカレーションすること

サイバーセキュリティの運用

一般的なサイバーセキュリティのフラストレーションのトップ 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が困難になっている
- 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
- 組織全体で強固なサイバーセキュリティ文化を構築することに苦労している

運用体制：

- IT 部門とは独立したフルタイムのサイバーセキュリティ専門チームを設置：25%
- IT 部門内にフルタイムのサイバーセキュリティ専門チームを設置：51%
- IT 部門の従業員がサイバーセキュリティの業務を兼任：20%
- 100% アウトソース：3%

サイバーセキュリティに最も責任を持つ役職 / 報告先：

CIO/IT ディレクター、CEO/ 代表取締役、デジタルトランスフォーメーション部門の責任者

予算

	合計予算	マレーシア
10% 以上増加	24%	27%
5 ～ 9.99% 増加	34%	33%
1 ～ 4.99% 増加	27%	33%
増減なし	13%	5%
1 ～ 4.99% 減少	1%	1%
5 ～ 9.99% 減少	1%	0%
10% 以上減少	0%	0%

フィリピン

サイバーセキュリティのストレスと燃え尽き症候群

- 頻繁に経験している：17% (2024 年は 23%)
- 時々経験している：71% (2024 年は 72%)

原因のトップ 3：
- リソースの不足
- 過剰なサイバーアラート
- 不明確なサイバーセキュリティ戦略

影響のトップ 3：
- サイバーセキュリティ体制の弱体化
- IT およびサイバーセキュリティチームのパフォーマンス低下
- インシデント対応時間の遅延

リソースへの影響のトップ 3：
- IT 人材の追加採用の必要性
- サイバーセキュリティツールやソリューションへの支出の増加
- サイバーセキュリティ運用を効率化するためにサードパーティのパートナーを利用

ストレスや燃え尽き症候群による生産性の低下：
- 毎週 4.2 時間 (2024 年は毎週 4.6 時間)

ストレスや燃え尽き症候群を抱える従業員に対して、カウンセリングを行っていますか？
- はい、77% (2024 年は 75%)

サイバーセキュリティにおける AI の影響

ChatGPT、エージェント AI、コパイロットなどのビジネス AI ツールを使用している組織の割合：

- 89% の組織が正式な AI 戦略を策定
- 79% の組織が許可されていない AI ツールを使用 (シャドー AI)
- そのうち 33% が無許可の使用を認識しており、19% は状況を認識していない

経験した問題のトップ 3：
- AI ツールがどのデータにアクセスしているのかわからない
- ツールの設定ミス
- 使用されている AI ツールがわからない

AI をサイバーセキュリティに活用する最大の利点：
セキュリティインシデントを正確にトリアージし、調査のために人間のオペレーターへエスカレーションすること

サイバーセキュリティの運用

一般的なサイバーセキュリティのフラストレーションのトップ 3：
- 恐怖と疑念を煽るメッセージによって、サイバーセキュリティについて正しい議論することが難しくなっている
- 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が困難になっている
- 法規制への対応が受け身になっており、結果としてサイバーセキュリティの管理がより困難になっている

運用体制：
- IT 部門とは独立したフルタイムのサイバーセキュリティ専門チームを設置：30%
- IT 部門内にフルタイムのサイバーセキュリティ専門チームを設置：43%
- IT 部門の従業員がサイバーセキュリティの業務を兼任：21%
- 100% アウトソース：6%

サイバーセキュリティに最も責任を持つ役職 / 報告先：
CEO/ 代表取締役、
デジタルトランスフォーメーション部門の責任者

予算

	合計予算	フィリピン
10% 以上増加	24%	30%
5 ～ 9.99% 増加	34%	33%
1 ～ 4.99% 増加	27%	23%
増減なし	13%	14%
1 ～ 4.99% 減少	1%	0%
5 ～ 9.99% 減少	1%	0%
10% 以上減少	0%	0%

シンガポール

サイバーセキュリティのストレスと燃え尽き症候群

- 頻繁に経験している：42% (2024 年は 16%)
- 時々経験している：46% (2024 年は 72%)

原因のトップ 3：

- 脅威活動の増加
- コンプライアンス要件と法規制要件の遵守
- リソースの不足

影響のトップ 3：

- サイバーセキュリティ業務や責任に対して、懐疑的、無関心、無気力のような感情を抱いている。
- IT およびサイバーセキュリティチームのパフォーマンス低下
- サイバーセキュリティ体制の弱体化

リソースへの影響のトップ 3：

- サイバーセキュリティ人材の追加採用の必要性
- サイバーセキュリティ運用を効率化するためにサードパーティのパートナーを利用
- IT 人材の追加採用の必要性

ストレスや燃え尽き症候群による生産性の低下：

- 毎週 4.3 時間 (2024 年は毎週 4.2 時間)

ストレスや燃え尽き症候群を抱える従業員に対して、カウンセリングを行っていますか？

- はい、79% (2024 年は 68%)

サイバーセキュリティにおける AI の影響

ChatGPT、エージェント AI、コパイロットなどのビジネス AI ツールを使用している組織の割合：

- 88% の組織が正式な AI 戦略を策定
- 79% の組織が許可されていない AI ツールを使用 (シャドー AI)
- そのうち 60% が無許可の使用を認識しており、14% は状況を認識していない

経験した問題のトップ 3：

- AI ツールがどのデータにアクセスしているのかわからない
- AI ツールを使用している従業員がわからない
- 使用されている AI ツールがわからない

AI をサイバーセキュリティに活用する最大の利点：

セキュリティインシデントを正確にトリアージし、調査のために人間のオペレーターへエスカレーションすること

サイバーセキュリティの運用

一般的なサイバーセキュリティのフラストレーションのトップ 3：

- 法規制への対応が受け身になっており、結果としてサイバーセキュリティの管理がより困難になっている
- 恐怖と疑念を煽るメッセージによって、サイバーセキュリティについて正しい議論することが難しくなっている
- 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

運用体制：

- IT 部門とは独立したフルタイムのサイバーセキュリティ専門チームを設置：47%
- IT 部門内にフルタイムのサイバーセキュリティ専門チームを設置：40%
- IT 部門の従業員がサイバーセキュリティの業務を兼任：10%
- 100% アウトソース：3%

サイバーセキュリティに最も責任を持つ役職 / 報告先：

デジタルトランスフォーメーション部門の責任者、CIO/IT ディレクター、CEO/ 代表取締役

予算

	合計予算	シンガポール
10% 以上増加	24%	26%
5 ～ 9.99% 増加	34%	35%
1 ～ 4.99% 増加	27%	27%
増減なし	13%	12%
1 ～ 4.99% 減少	1%	0%
5 ～ 9.99% 減少	1%	0%
10% 以上減少	0%	0%

付録：アンケート回答者の内訳と調査方法

ソフォスは 2025 年 6 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 (205 社)、インド (203 社)、日本 (205 社)、マレーシア (103 社)、フィリピン (105 社)、シンガポール (105 社) から合計 926 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。本調査には、サイバーセキュリティおよび IT 部門の従業員および経営幹部からの回答が含まれます。

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。

本書について

ソフォスについて

ソフォスは、サイバーセキュリティ業界のリーダー企業として、AI を駆使したプラットフォームや精鋭スタッフによるサービスを世界中の 600,000 社以上のお客様にご利用いただいています。セキュリティの成熟度にかかわらず、あらゆるお客様のご要望にお応えし、サイバー攻撃を撃退すべくお客様とともに成長を続けています。機械学習や、自動化、リアルタイムの脅威インテリジェンスに、Sophos X-Ops の最前線スタッフから得た専門知識を組み合わせて、高度な脅威監視、検出、対応を 24 時間 365 日体制で行っています。ソフォスは、業界最先端の MDR (managed detection and response) を提供しているのに加えて、エンドポイントをはじめ、ネットワーク、メール、クラウドセキュリティ、XDR (extended detection and response)、ITDR (identity threat detection and response)、次世代の SIEM まで、サイバーセキュリティテクノロジーのあらゆるラインナップを取り揃えています。さらに、専門家によるアドバイザリーサービスも提供しており、組織はこれらを組み合わせて利用することで、リスクをあらかじめ減らし、迅速な対応をとれるようになるだけでなく、進化し続ける脅威の一歩先をいくために必要な可視性および拡張性を確保することが可能となります。ソフォスは、グローバルに広がるパートナーエコシステムを通じて市場展開しており、お客様は、MSP (Managed Service Provider)、MSSP (Managed Security Service Provider) や、リセラー、ディストリビューターのほか、マーケットプレイスにおける統合、ソフォスのサイバーリスクパートナーまで、信頼できる関係性を自由にお選びいただけます。ソフォス本社は英国の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) (現在は Omdia 傘下) 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、最新のテクノロジーを活用することを検討している経営幹部などのリーダー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。

ソフォス製品がお客様の企業の防御にどのように役立つかをご覧ください。

ソフォスは、業界をリードするサイバーセキュリティソリューションをあらゆる規模の企業に提供し、マルウェア、ランサムウェア、フィッシングなどの高度な脅威をリアルタイムで保護します。実績のある次世代機能により、AI と機械学習を駆使した製品でビジネスデータを効率的に保護できます。

2025-08-20 WP (NP)