SOPHOS

日本およびアジア太平洋地域のパートナー向けのサイバーセキュリティプレイブック

ソフォスの委託による Tech Research Asia レポート
2024 年 9 月

はじめに

本レポートは、日本、オーストラリア、インド、マレーシア、シンガポール、フィリピンを含む日本およびアジア太平洋 (APJ) 市場におけるサイバーセキュリティのマネージドセキュリティパートナー (MSP) のビジネス機会を中心に説明したレポートの第 2 弾です。

第 1 弾のレポートでは以下について説明しました。

1. サイバーセキュリティの構造とチーム、レポートライン、責任の概要
2. MSP が取締役会や経営幹部チームに伝えるべき重要なメッセージ
3. 中堅企業が業務で直面するサイバーセキュリティ戦略における主な痛点。
4. 効果的なサイバーセキュリティ運用の障害となる、隠れたサイバーセキュリティの問題
5. MSP が企業にセキュリティソリューションを販売するときに陥りやすい間違い

第 1 弾のレポートで説明したパートナーにとって重要な情報：

1. MSP は企業のサイバーセキュリティ計画と運用に不可欠と考えられている
2. すべての企業にとって最適な万能のソリューションはない。企業がサイバーセキュリティグループを構成し、リーダーを割り当て、経営幹部が監督する方法には共通点がある。
3. 取締役会や経営幹部は、主な関心分野に関するガイダンスを求めている。これらの分野を重視して、知見を提供できるようにすることが重要
4. テクノロジーよりも、カルチャー、燃え尽き症候群、教育を重視する必要がある

本レポートの第 2 弾では、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におけるサイバーセキュリティニーズについて 2024 年 7 月に調査し、そのデータを分析した以下の結果をお伝えしています。

1. ビジネス目標とサイバーセキュリティ投資との重要な関連性
2. サイバーセキュリティ予算とパートナーにとってのビジネス機会がある分野の特定
3. パートナーにとっての AI サイバーセキュリティソリューションの可能性とビジネス上の懸念
4. 企業がサイバーセキュリティパートナーに求めている能力
5. 調査レポートのスポンサーであるソフォスから見た課題とパートナーのビジネス機会
6. 国別の調査データ

Tech Research Asia によるこのプレイブックのデータと解説が、パートナーの皆様の市場開拓と継続的なビジネスの成功に役立つことを願っています。

よろしくお願いいたします。

Tech Research Asia

サイバーセキュリティのビジネスニーズ

多くのアナリストが執筆しているプレイブックは、翌年のビジネス戦略や目標の概要から始まりますが、本書の構成は異なります。

来年のビジネス戦略や目標ではなく、企業の事業運営のどのような部門でサイバーセキュリティが切実に必要となっているのかを把握することから着手しました。サイバーセキュリティが不可欠であると企業が考えているのは、営業でしょうか？マーケティング、研究開発、物流、それともその他の部門でしょうか？

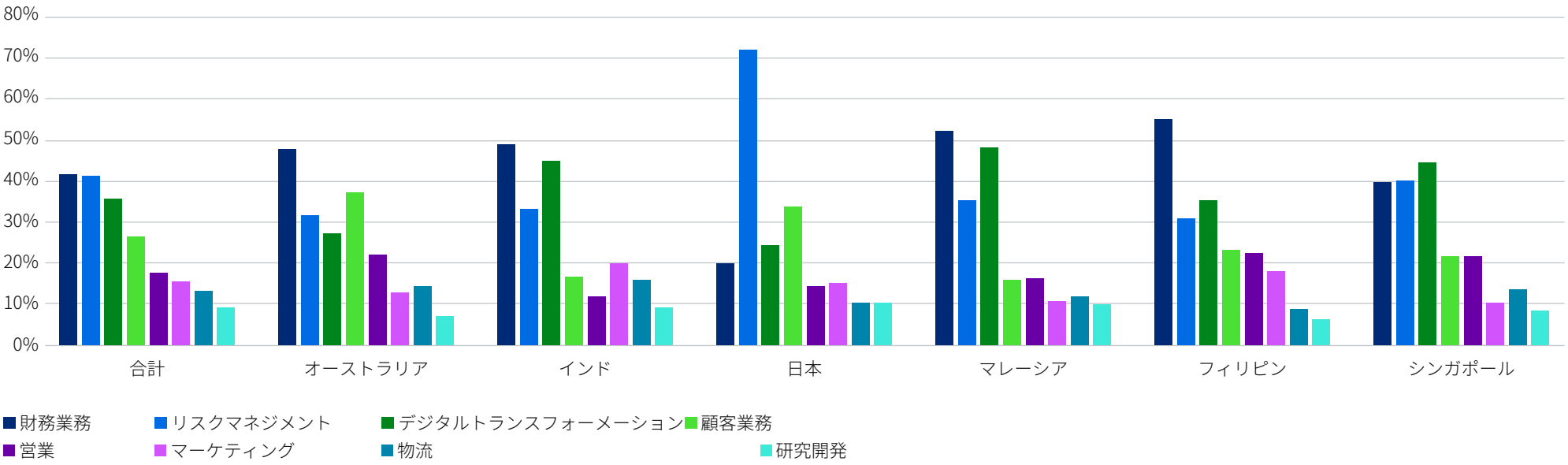
APJ 全体では、サイバーセキュリティが重要な部門とサイバーセキュリティ能力の上位 3 つには以下が挙げられています。

1. **財務関連**業務におけるサイバーセキュリティ体制の強化
2. **リスク管理の能力**の向上とリスクエクスポージャーの削減
3. 堅牢なサイバーセキュリティプラットフォームの導入と、**デジタルトランスフォーメーションプログラムのサポート**

その他の重要な分野を以下に示します。

- 顧客と顧客データの保護の強化、フィッシング攻撃の軽減、顧客とのコミュニケーションと認証の改善
- 事業運営、特に営業とカスタマーサポート部門におけるサイバーレジリエンスの向上
- サイバーインシデントや混乱からの物流とサプライチェーンの保護、およびインシデント発生時における必要な業務データとシステムへのアクセスの確保
- 企業の知的財産や研究開発データの紛失や漏えいの防止

サイバーセキュリティ対策が必要な最も重要なビジネス分野のトップ 3 は？



パートナーにとってのサイバーセキュリティに関するビジネス機会のヒートマップ

企業が優先すべき投資先と考えているサイバーセキュリティソリューションは何でしょうか？

その答えは、ソフォスの「パートナーにとってのサイバーセキュリティに関するビジネス機会のヒートマップ」にあります。このヒートマップは、投資先として優先度が高いソリューションと、これらのソリューションが企業や組織のサイバーセキュリティ体制にどの程度の影響を与えるかを示しています。右上に位置するほど投資先として重視されているソリューションになります。

パートナーのビジネス機会のトップ 5 を以下に示します。

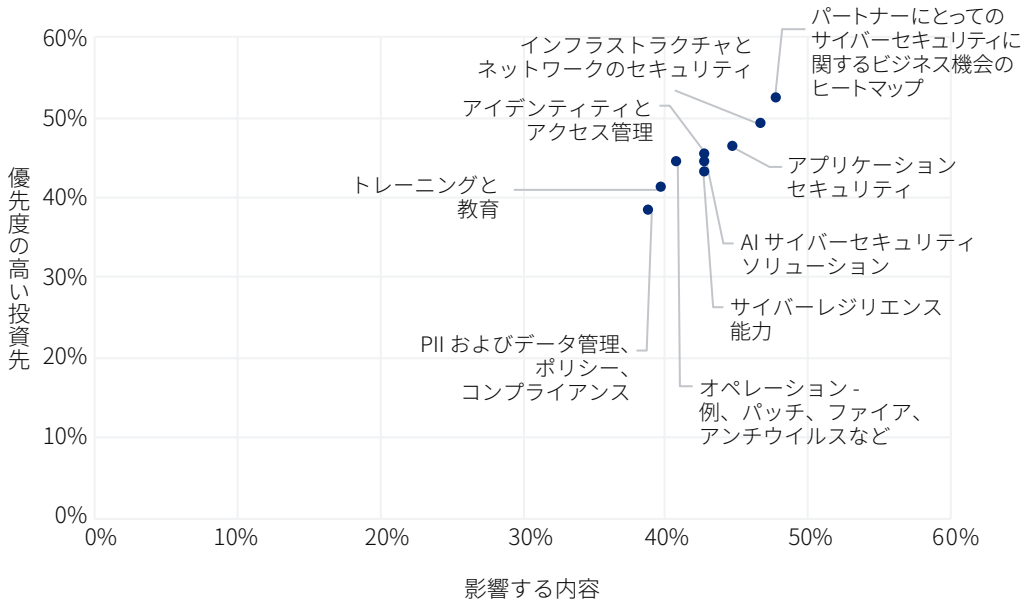
- 脅威の検出と対応
- インフラストラクチャとネットワークのセキュリティ
- アプリケーションセキュリティ
- アイデンティティとアクセス管理
- AI サイバーセキュリティとサイバーレジリエンス (同率 5 位)

最初の 4 つのソリューションはすでに確立されているテクノロジーであり、パートナーがこれらの分野で強力な資格を持っていなければならないことは明らかです。さらに重要なのは、パートナーは、5 位であった AI サイバーセキュリティとサイバーレジリエンスにおける能力を開発し、強化し続ける必要があることです。

現在、企業の 44% がサイバーセキュリティのための AI 投資戦略を策定しています。AI を活用したサイバーセキュリティは今後必須となり (詳細は後述)、多くのサイバーセキュリティ活動の支柱となると考えられます。パートナーはこの分野に投資し、スキルを開発し、力強いメッセージを発信し、市場開拓 (GTM) 活動を推進し、信用を得なければなりません。このような努力を怠ると、競合にビジネス機会を奪われることになるでしょう。

サイバーレジリエンスの重要性を伝えるメッセージ (サイバーインシデント発生時や復旧時に通常通り事業を継続すること) は、多くのベンダーが重要視しており、あらゆる場所で発信しています。多くの組織はセキュリティ侵害を避けられないものと考えており、パートナーは自社のレジリエンス能力について明確に伝えることができなければなりません。この能力には、レジリエンス戦略の策定、取締役会および経営幹部に対する教育、復旧計画の策定など、企業に対する支援も含まれます。

パートナーにとってのサイバーセキュリティに関するビジネス機会のヒートマップ



ヒートマップの注：

回答者には、各テクノロジーソリューションの優先度と影響度を 0 (非常に低い) から 10 (非常に高い) の 10 段階で評価してもらいました。

このヒートマップは、10 段階で 8、9、10 の優先度を選択したすべての国の回答者の割合を示しています。

サイバーセキュリティの現状と成熟度

パートナーが企業のサイバーセキュリティ能力と成熟度を高めるのを支援するビジネス機会は、製品 / ソリューションレベルと戦略 / フレームワークの両方に明確に存在します。

下図のデータは、国別および全体レベルで、セキュリティ対策の各能力と戦略を確立している企業の割合を示しています。これらの能力を確立している割合が低ければ低いほど、その国におけるパートナーの潜在的なビジネス機会は大きくなります。

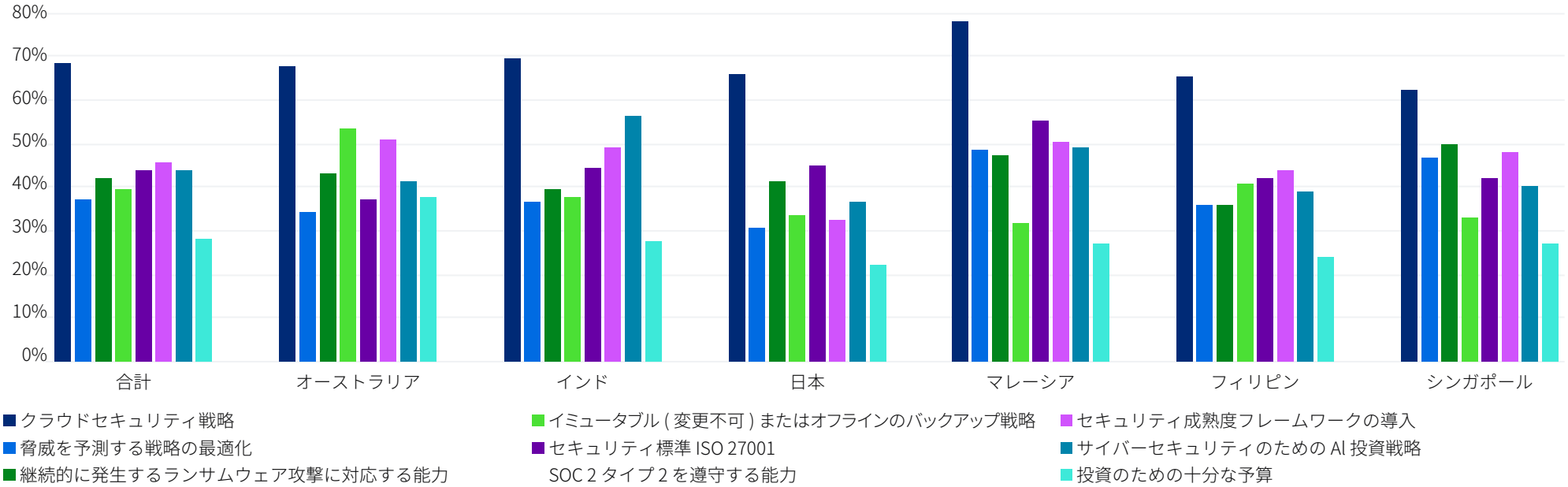
多くの組織にとって、予算は明らかに大きな課題です。この予算の問題については後続のページで詳しく説明します。

予算の問題も重要ですが、パートナーは顧客に製品ソリューションに付加価値を付けて提供していく必要があります。

パートナーは、以下のような多くの戦略とフレームワークのニーズをサポートしなければなりません。

1. サイバーセキュリティ戦略の最適化、ランサムウェアやその他の攻撃に対応できるようにする支援、および成熟度の強化
2. セキュリティ成熟度フレームワークを確立して導入するための知見と教育の提供
3. 複数のセキュリティ標準認証を取得および維持するための支援
4. ゼロトラストサイバーセキュリティ戦略を策定し、その運用の仕組みを確立して維持するための支援

貴社が重要であると考えているセキュリティ能力のうち、現在導入しているものはどれですか？



予算配分と予算を費やす分野

企業のセキュリティ予算については、パートナーに朗報があります。

アジア太平洋地域の企業の平均 72% は、現在サイバーセキュリティに十分な予算が割り当てられていないと回答しており、これらの企業の 83% は、今後 1 年間でサイバーセキュリティ予算が増加すると予測しています。

サイバーセキュリティへの支出を増加させると回答した企業の 21% が 10% 以上の増加を見込んでいます。

ヒートマップに示した優先度の高い分野に関する先ほどの解説と関連付けると、多くの予算が配分される製品 / ソリューション分野の上位は以下のようになります。

1. インフラストラクチャとネットワークセキュリティ (62% が予算を増加)
2. 脅威の検出と対応 / データ保護とプライバシー (61% が予算を増加)
3. アプリケーションセキュリティ (56% が予算を増加)
4. アイデンティティアクセス管理 (53% が予算を増加)
5. インシデント対応と復旧 (50% が予算を増加)

予算の大幅な増加が見込まれるその他分野は以下の通りです。

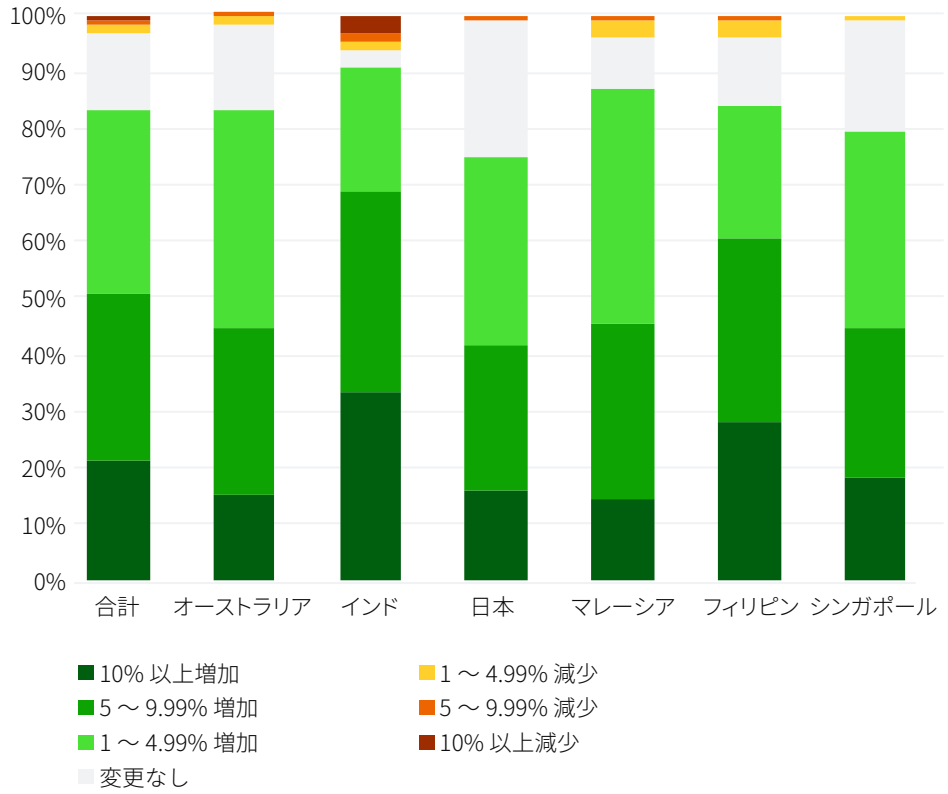
1. データ保護とプライバシーのポリシーと戦略 (62% が予算を増加)
2. トレーニングおよび教育プログラム (56% が予算を増加)
3. サイバーセキュリティ戦略、人材、ガバナンス、リスク、コンプライアンス (55% が予算を増加)
4. 保険 (48% が予算を増加)

企業はまた、社内の従業員への投資を増やすことを計画しており、50% の企業が従業員の昇給を計画しています。

当然のことながら、給与が上昇するようになると、費用対効果の高い代替案を検討する必要が生じてきます。このような背景から、50% の企業が、サードパーティのマネージドセキュリティサービスへの投資を増加することを検討しています。

サードパーティのサービスへの支出を増加させることを検討している企業の 20% は予算を 10% 以上、残りの 80% は 1 ～ 10% 増加させることを予定しています。

貴社のサイバーセキュリティ予算は、今後 12 か月間で増加しますか、それとも減少しますか？



パートナーとのエンゲージメントに対する需要は強い

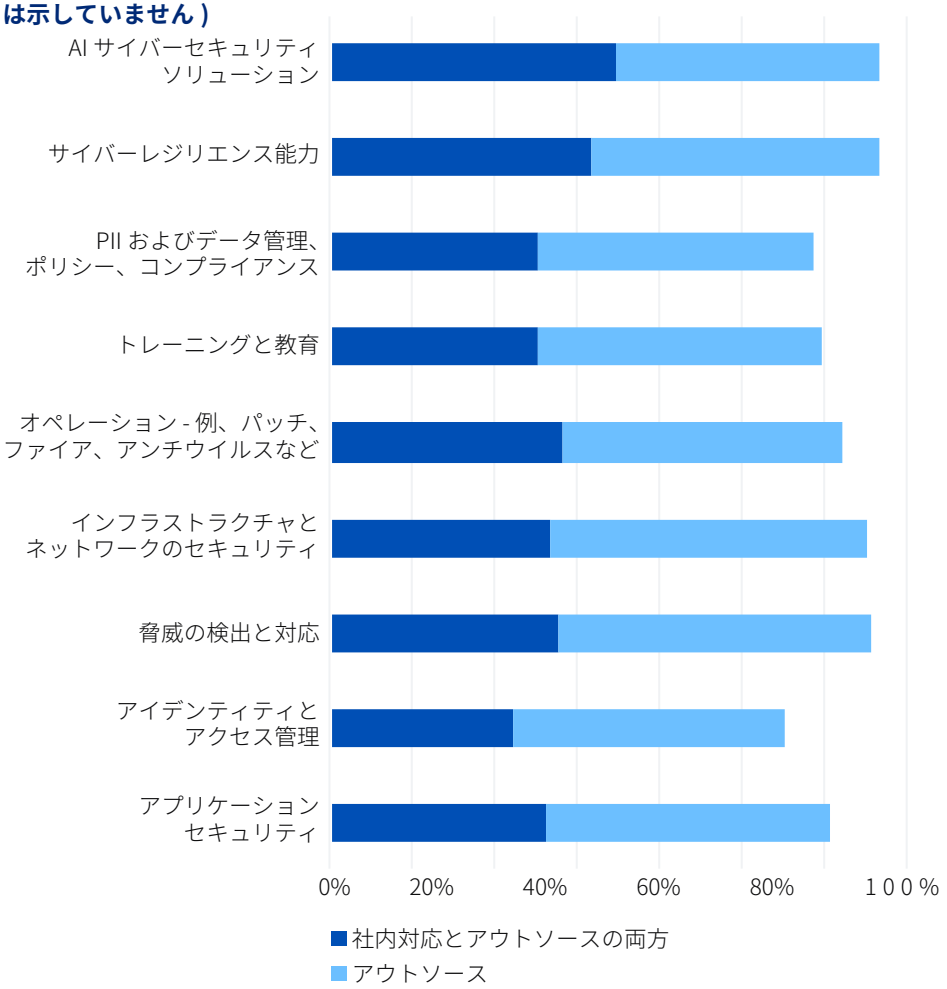
このデータは、企業が以下のような多くのメリットを認識しており、パートナーから支援を受けることに意欲的になっていることを示しています。

- 複数のインフラ、エンドポイント環境、ツールセットの統合と管理
- セキュリティ機能を強化し、社内の従業員への影響や負荷を軽減するマネージド SOC サービス
- 社内のスキル不足の解消
- 認証情報管理、パッチ適用などの基本的なセキュリティ対策が最新であることの確認
- 高コストの社内従業員を割り当てるのではなく、費用対効果の高いサードパーティサービスによる予算の問題解決
- ガバナンス、リスク、コンプライアンスに関する監査、評価、管理を通じた、リスクの削減・軽減への重点的な取り組み

右のグラフは、各サイバーセキュリティ分野におけるサードパーティベンダーによる支援 (アウトソーシング) または社内対応とアウトソーシングの両方の組み合わせに対する現在の需要を示しています。このグラフは、パートナーに対する需要が旺盛であること明確に示しています。

今後 2 年間の予測でも、アウトソーシングする意向は強く、比較的一定しています。アウトソーシングの需要が増加しているのは、「アプリケーションセキュリティ」と「PII およびデータ管理、ポリシー、コンプライアンスサービス」の 2 つの分野です。

以下のサイバーセキュリティ要件で、自社で対応している、アウトソースしているもの、あるいは両方を組み合わせているものはどれですか？ (注:このグラフは「自社での対応」は示していません)



懸念される脅威：AI を悪用するサイバー攻撃がトップに

ほぼすべてのビジネステクノロジーに AI が深く関わるようになり、重要なトピックになっています。オーストラリアを除くすべての市場において、AI を悪用するサイバーセキュリティ攻撃が最も懸念されるサイバー脅威として考えられています。

パートナーは、AI を悪用するサイバー攻撃の現状、パートナーベンダーが確立している AI 戦略と能力について明確なメッセージで伝え、「サイバーセキュリティ分野での AI 利用は何から着手すべきか」を伝える市場開拓 (GTM) のメッセージングとキャンペーンを実施しなければなりません。AI とサイバーセキュリティの関係は、製品だけに限りません。AI ポリシー、倫理的な利用、許可される使用方法、ユーザーアクセスと管理にも及びます。

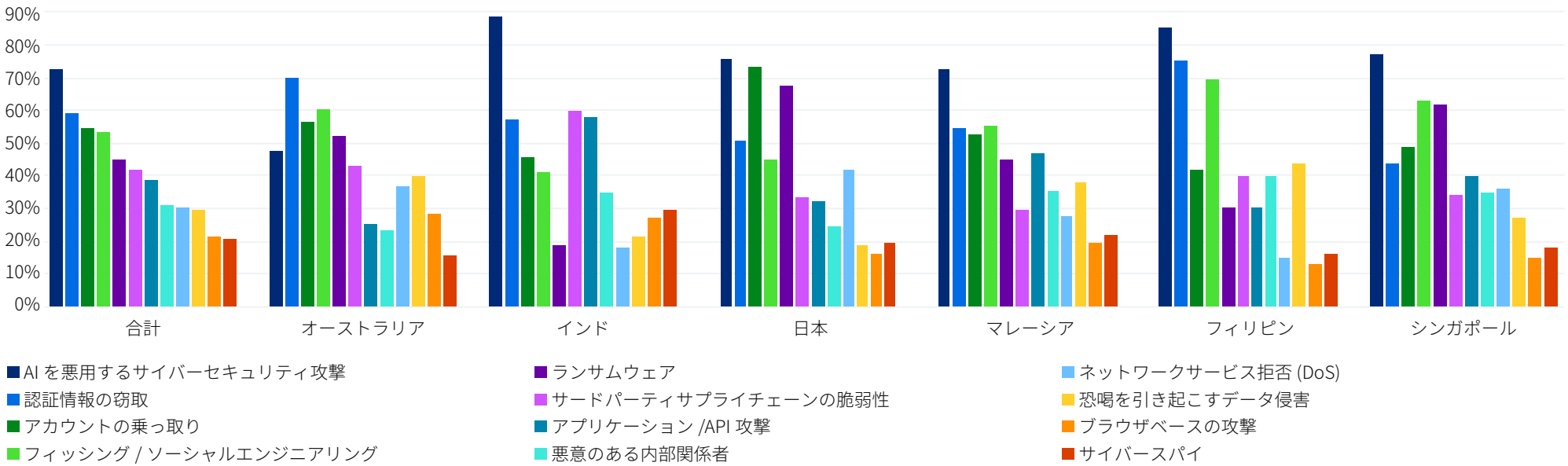
AI に関する FUD (恐怖、不安、疑念) を利用した営業手法は効果を失っています。

ここでは、以下の営業スキル、コンピテンシー、能力が求められます。現在、AI による攻撃の脅威に対処するために必要なスキルをすべて備えていると考えている APJ の企業は半数以下です。

APJ 地域全体では、45% の企業が AI の脅威に対応できるスキルがあると考えています。これは、マネージドセキュリティサービスとトレーニングや教育サービスの分野で、パートナーが企業と関わり、支援できることを明確に示しています。

AI を悪用する脅威を除けば、懸念される脅威は国によって大きく異なっています。そのため、パートナーにとってターゲット市場で重要となっている脅威を把握することが重要です。複数の国を対象に営業をしている場合は、特にこれは重要となります。

最も懸念されるサイバー脅威は、次のうちのどれですか？



AI サイバーセキュリティのビジネス機会が広がる

適切な方法でアプローチすれば、パートナーは、AI サイバーセキュリティソリューションを導入および展開する企業を支援し、大きな収益機会を得ることができます。

戦略の立案から開始する。現在、全社的に包括的な AI および自動化戦略を導入していると回答した企業はわずか 22% に過ぎません。企業が AI 生成コンテンツがもたらす詐欺などのサイバー攻撃と混乱を防止するための支援が必要となっているとは明らかです。

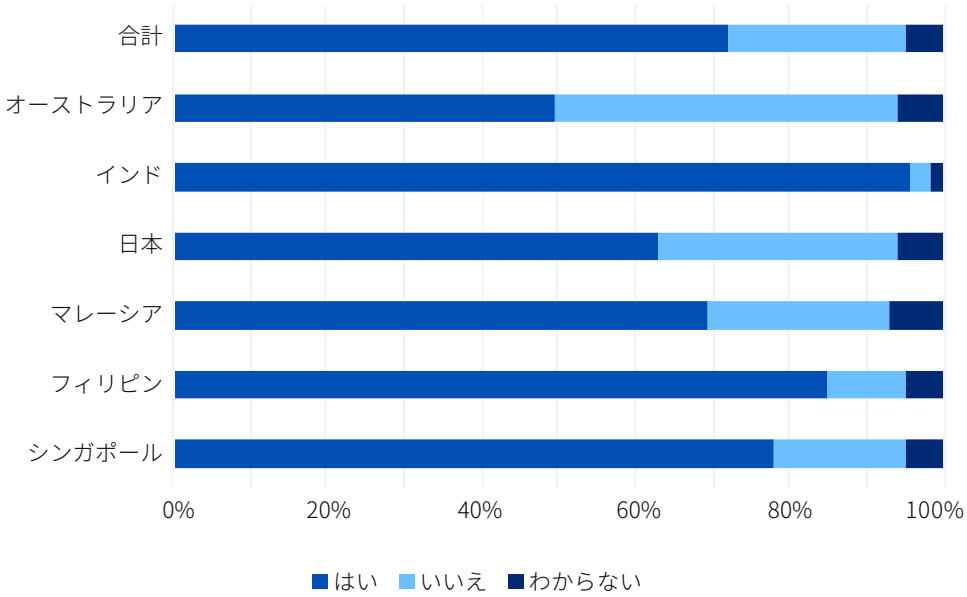
迅速に行動する。企業はすでに AI サイバーセキュリティ戦略立案に向けた取り組みを進めています。

- 回答者の 72% が AI 戦略と取り組みを主導する担当者を任命したと述べています。このようなリーダーの全員が技術者ではありません。実際、これらのリーダーの 4 分の 3 は一般的にビジネス部門 (営業、マーケティング、財務など) の経営幹部になっています。
- 75% の回答者が AI 関連のサイバーセキュリティについて既存のパートナーとすでに打ち合わせを行っています。ただし、既存のパートナーの AI サイバーセキュリティのスキルと知識について 5 点満点を採点した回答者は 26% に留まっています。
- そのため、これらの回答者の 8% がすでに別のパートナーを利用するようになっています。

企業における AI スキルの不足は、パートナーにとって大きなビジネス機会になります。AI スキルの不足に対応するため、回答者の 45% はパートナーに支援をアウトソースすると述べています。49% は社内でトレーニングや能力開発を実施すると回答しており、この分野でもパートナーのサポートによるトレーニングや教育のニーズが存在しています。

組織が抱えている AI サイバーセキュリティのニーズを支援する。TRA の調査によると、企業は戦略、新しいアイデアの創出、導入と実行という 3 つの異なる段階を経て AI サイバーセキュリティを強化しています。3 つ目のフェーズである「導入と運用」を最適化するために、企業はネットワーク、ストレージ、エンドポイント、GRC、セキュリティ、データ資産を監査し、AI セキュリティへの対応状況を評価しなければなりません。パートナーは、この分野で明確な役割を果たすことができます。

貴社では、AI 戦略と取り組みを主導する担当者を任命していますか？



企業がパートナーに求めている能力

プレイブックのこのパートでは、サイバーセキュリティのニーズと運用を支援するためにサードパーティの利用を企業が決定するときに影響を与えるいくつかの要因について説明します。

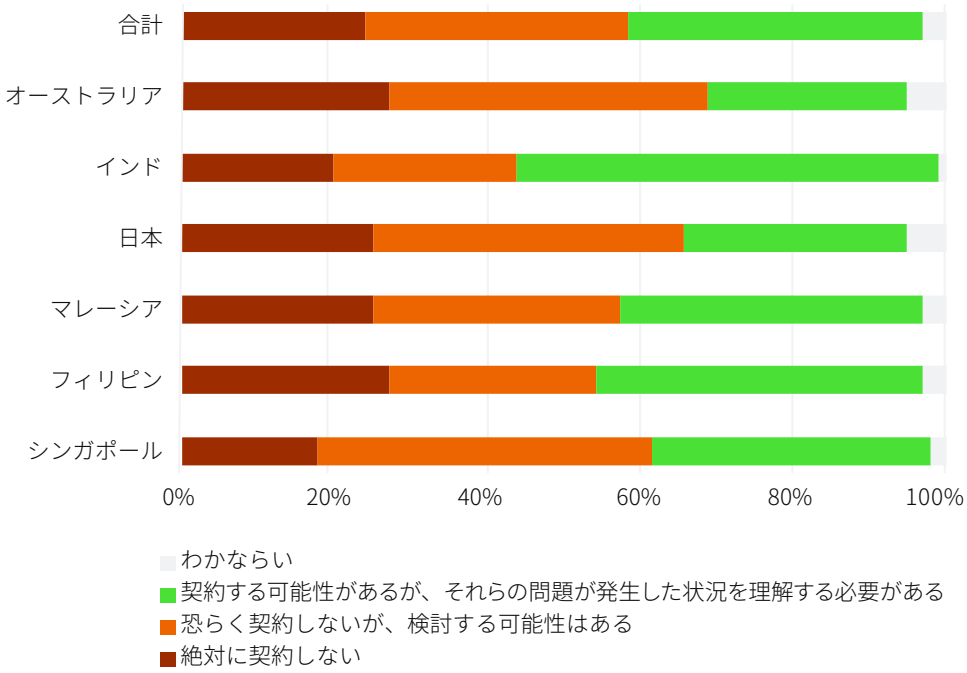
これらの要因を説明する前に、パートナーが押さえておくべき基本的な事項がいくつかあります。

- 業界をリードする信頼できるベンダーと契約して実績を作る
- 統合のスキル
- プロアクティブな脅威検出能力
- サイバーレジリエンスの能力と専門知識
- AI によって強化したサイバーセキュリティソリューションの活用と支援
- 顧客のニーズに合わせてソリューションを提供する能力
- 教育とトレーニングの支援

強力なセキュリティスキルは、パートナーにとって欠かすことができません。これは当然のことかもしれませんが、調査データからもその重要性が裏付けられています。59% の組織は、情報漏えいやセキュリティインシデントを経験しているパートナーとは「絶対に」あるいは「恐らく」契約を結ばないと回答しています。

セキュリティ侵害を経験しているパートナーとの契約を検討する企業の 81% は、これらのパートナーに特別なパフォーマンス条項や特定のサービスレベル契約を含める可能性があると述べています。

貴社は、過去 12 か月間にサイバーセキュリティインシデント、セキュリティ侵害、またはデータ漏えいを経験したサードパーティと契約する可能性はありますか？



企業は複数のパートナーを利用している。

マルチベンダー環境は一般的になっています。

平均すると、サイバーセキュリティニーズに対してベンダー 1 社しか利用していない組織は 20% です。29% の組織が 2 社、23% は 3 社、10% は 5 社以上のベンダーのソリューションを利用しています。

パートナーが提供するソリューションやサービスは、顧客のニーズに合わせて柔軟に対応できることが不可欠です。

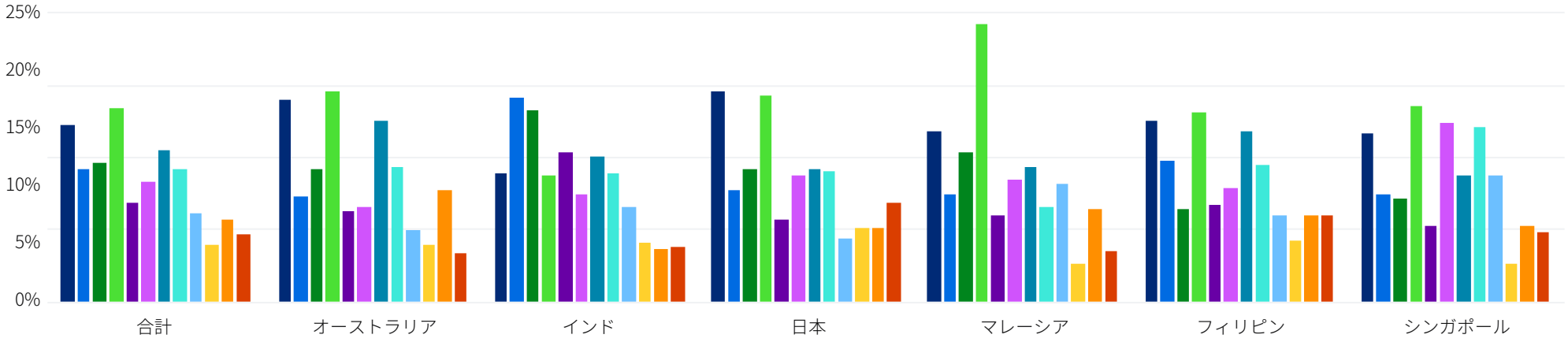
- 54% の組織が、今後 24 か月間の契約の一部に成果ベースの条件を追加すると述べています。
- 48% が消費ベースと固定契約を組み合わせた価格設定を希望し、31% が固定契約を希望、17% が消費ベースの価格設定のみを希望している。

サイバーセキュリティベンダーや戦略の変更を企業が検討する理由のトップ 3 を以下に示します。

1. ソリューションのパフォーマンスが不十分
2. セキュリティ侵害や大規模な障害がサードパーティで発生し、データやシステムにアクセスされた
3. 予算の変更

厳しい予算と業務コストの最適化に対する需要は、製品やサービスを柔軟に利用できることを実証し、統合型のプラットフォームやツールセットを提供して管理労力や教育のためのコストを簡素化削減できることを実証できるパートナーにとってビジネス機会となります。

価格を除き、サイバーセキュリティベンダーや戦略の変更を検討する要因は何ですか？



- セキュリティ侵害や大規模な障害の発生
- ベンダーサプライチェーンの問題 (納期の遅れなど)
- 侵入テストの結果
- 現在のソリューションのパフォーマンスが不十分
- サイバーセキュリティベンダーまたはパートナーの担当者の変更
- 法規制の改正
- 予算の変更
- サイバーセキュリティテクノロジープラットフォームの管理が複雑
- 社内で必要とされるサイバーセキュリティスキルの変更
- カスタマーサポートが不十分
- テクニカルサポートが不十分
- より優れたイノベーションが必要

マーケットプレイスとの競合

APJ のチャネル組織やディストリビューターとの対話や調査結果から、マーケットプレイスは多くのパートナーにとって問題となる可能性があることが分かっています。マージンは非常に低く、既存の商流を保護することが難しくなっています。

また、企業や組織が、サイバーセキュリティソリューションを購入して利用するためにマーケットプレイスを今後も利用する意向であることも分かっています。

顧客のビジネスを獲得するためにマーケットプレイスと価格面で直接競合するパートナーは、通常は負けます。クラウドビジネス、特にクラウドクレジットがコミットされている場合は、単純に案件を獲得するのは困難です。

しかし、パートナーは価値提案と契約内容に、以下のようないくつかの要素を組み込むことで、マーケットプレイスに関する不安を緩和できます。

- **リスク管理 1** マーケットプレイスは、シンプルで DIY 型であり、スタンドアロンの展開には適していますが、サイバーセキュリティ業務の多くは複雑であり、統合やマルチプラットフォームのサポートが必要であることを強調します。リスクの管理と軽減を、重要なビジネスニーズの一つとして重視している企業は、強固なリスクポスチャとサイバーセキュリティ能力を確保するためにパートナーの支援を必要としています。
- **リスク管理 2** 製品のパフォーマンスや能力について徹底的に調査せずに、マーケットプレイスで DIY 型の製品を購入するとリスクが高まります。組織がソリューションの一部を導入し、その他の部分をパートナーが導入した場合、サイバーインシデントが発生した場合に責任問題に発展する恐れがあります。
- **プロフェッショナルサービスのアドオン**は、マーケットプレイスでの調達に付加価値を与え、顧客との関係性を強化する強力なオプションです。これらのサービスは、投資価値を迅速に実現するためにも役立ちます。投資価値の早期の実現は、コスト重視の現在の環境において重要な考慮事項になっています。

まとめ

マネージドセキュリティパートナーの支援に対する需要は高い

企業の 83% が、今後 12 か月間にサイバーセキュリティ予算が増加すると回答し、50% が同期間に MSP への支出を増やすと回答しています。

企業はサイバーセキュリティを向上するために、サイバーレジリエンスを提供できるパートナーを求めるケースが増えています。つまり、MSP は、顧客のビジネス目標や業務を明確に理解するだけでなく、サイバーセキュリティの強力な技術的スキルを提供できなければなりません。

脅威の検出と対応、インフラとネットワークセキュリティ、アプリケーションセキュリティ、IAM、サイバーレジリエンス、攻撃者が AI を悪用する方法を理解し、防御にも AI を活用するサイバーセキュリティのスキルが、技術的な需要が明確に存在する分野になっています。

カスタマーエンゲージメントの深化と強化を促進するために、パートナーはこれらの技術的スキルを顧客データ (および企業の評判) の保護、財務業務、営業、マーケティング、デジタルトランスフォーメーションなどの取り組みに明確に関連付ける必要があります。

AI サイバーセキュリティを運用することの重要性、さらに、業務や IT の運用に生成 AI などの AI ツールを採用することが組織のサイバーセキュリティやリスクプロファイルに与える影響について、明確かつ説明でき、実践的な対策を提示することが求められています。

FUD (恐怖、不安、疑念) を利用した営業手法を排除し、ビジネスを勝ち取るために信頼性、スキル、実行力を高めることに集中する

無数のサイバーセキュリティツールは、完全な保護を約束する過大な宣伝を企業に行っていますが、このような戦略は意味を失っています。FUD (恐怖、不安、疑念) を煽る手法は効果的ではありません。

自社の信頼性、ベンダーとの緊密な連携、統合スキル、実行能力と価値の証明、従業員の教育とトレーニングを向上することに集中することが重要です。これらのメッセージは、テクノロジーチームとビジネスチーム (およびバイヤー) の双方に対する訴求力が高いことを多くの企業が認めています。

最後に、調査した 6 か国の企業の具体的なデータを提供するため、国別の調査結果データを以下のセクションに示します。

ソフォスの見解

顧客と長期的な関係性を築いている MSP が成功を収めている

企業が積極的にサービスをアウトソースしていることはデータからも明確に裏付けられています。しかし、多くの企業は社内リソースとアウトソーシングサービスの両方を利用するハイブリッドモデルを求めています。このため、成功を収めているパートナーは、サービスを提供するだけでなく、顧客との長期的な関係性を構築して維持するための投資を行っています。顧客との関係性を強化するには、社内スタッフの業務を置き換えるのではなく、社内スタッフと協力・連携して業務を進めることに重点を置きます。

TRA のこの調査では、市場から貴重な知見とデータを直接引き出しており、顧客にとって最も重要なビジネス分野を浮き彫りにしています。MSP は、TRA が提供しているこれらの知見と戦略的な要点を活用し、不断の努力と効果的なメッセージを伝えることに注力することを強く推奨します。50% の企業がサードパーティのマネージドセキュリティサービスに投資することを検討しています。MSP には顧客や見込み客にサイバーセキュリティをサービスとして提供する方法を検討する絶好の機会があります。

MSP は、企業の規模にかかわらず、絶えず進化する脅威環境に対する最良の防御策を提供できます。MSP は、この第 2 弾と第 1 弾のレポートを参考に、オーバーヘッドとリスクを最小限に抑えながら、この絶好な機会を活かし、収益性を高めるために、広範なサービスを提供しているベンダーとの提携を検討する必要があります。

詳細は、www.sophos.com を参照してください。

国別データ - オーストラリア

サイバーセキュリティのサポートが必要な上位のビジネス分野：

1. 金融サービス
2. カスタマーサービス
3. リスク管理
4. デジタルトランスフォーメーション
5. マーケティングサービス

使用しているサイバーセキュリティベンダーの数：

1: 29%
2: 25%
3: 23%
4: 3%
5 社以上：2%
分からない：18%

包括的な AI 導入戦略を実施：

10%

AI 担当のリーダーを任命

50%

必要な AI スキルが社内にありますか？

「はい」28%

契約している、あるいは契約を検討しているパートナーの AI 関連の知識をどのように評価しますか？

5 点満点の 5：15%
5 点満点の 4：47%

サイバーインシデントを経験したパートナーを利用しますか？

「絶対に利用しない」27%
「恐らく利用しない」41%

セキュリティ侵害が発生したパートナーに、より厳格なパフォーマンス要件および SLA を課す可能性がありますか？

「はい」60%

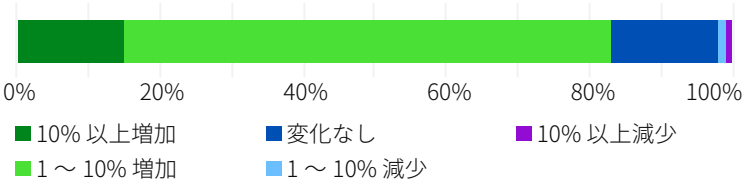
サイバーセキュリティベンダーを変更する要因には何かがありますか？

1. ソリューションのパフォーマンスが不十分
2. 自社のセキュリティが侵害された
3. 管理が複雑すぎる
4. 侵入テストの結果が不十分
5. テクニカルサポートが不十分

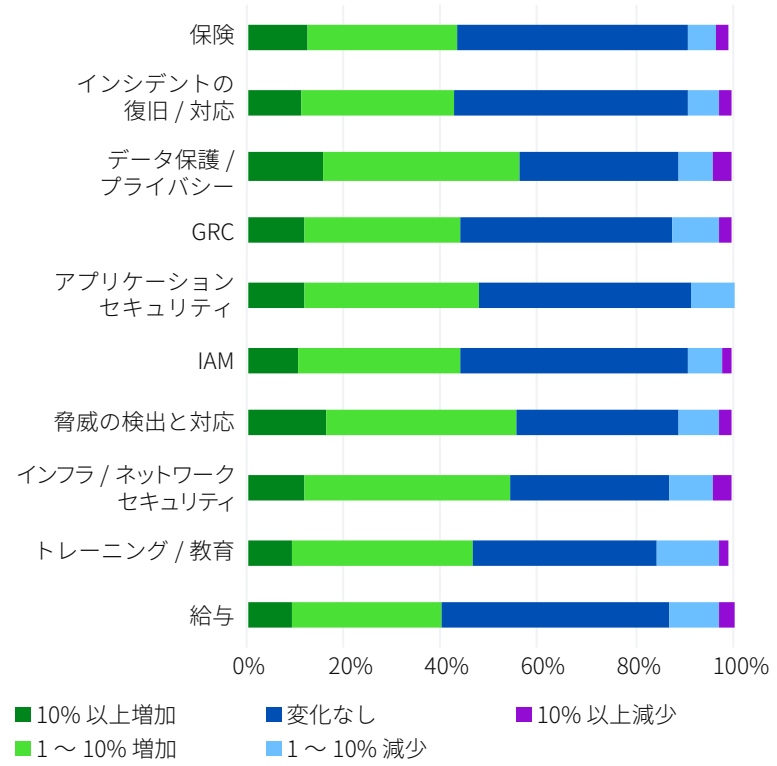
関連するフレームワーク

- オーストラリア信号局 (ASD) 情報セキュリティマニュアル (ISM)
- Australian Cybersecurity Centre Essential 8
- 米国国立標準技術研究所 (NIST) サイバーセキュリティフレームワーク
- ISO 27001 および ISO 27002
- Cloud Security Alliance (CSA) Cloud Control Matrix (CCM)

予算の変化の見通し：



予算項目の変更予測：



国別データ - インド

サイバーセキュリティのサポートが必要な上位のビジネス分野：

1. 金融サービス
2. デジタルトランスフォーメーション
3. リスク管理
4. マーケティング業務
5. カスタマーサービス

使用しているサイバーセキュリティベンダーの数：

1: 5%
2: 25%
3: 24%
4: 21%
5 社以上：26%
分からない：1%

包括的な AI 導入戦略を実施：

38%

AI 担当のリーダーを任命

96%

必要な AI スキルが社内にありますか？

「はい」72%

契約している、あるいは契約を検討しているパートナーの AI 関連の知識をどのように評価しますか？

5 点満点の 5：49%
5 点満点の 4：44%

サイバーインシデントを経験したパートナーを利用しますか？

「絶対に利用しない」20%
「恐らく利用しない」24%

セキュリティ侵害が発生したパートナーに、より厳格なパフォーマンス要件および SLA を課す可能性がありますか？

「はい」98%

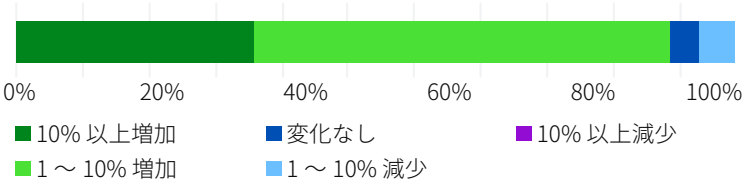
サイバーセキュリティベンダーを変更する要因には何かがありますか？

1. ベンダーサプライチェーンの問題
2. ソリューションのパフォーマンスが不十分
3. ベンダーによるスタッフ / 担当者の変更
4. 予算の変更
5. 管理が複雑すぎる

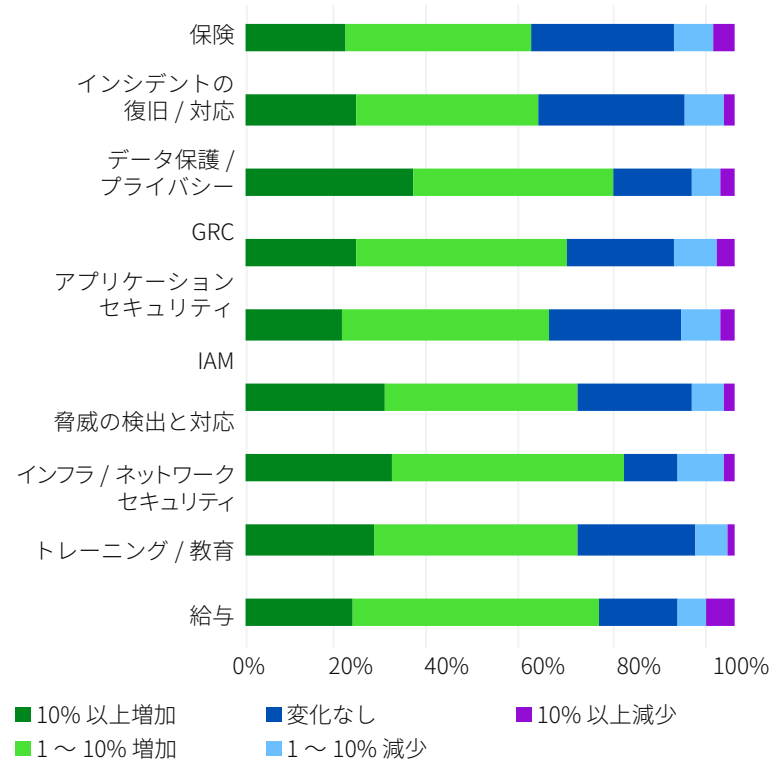
関連するフレームワーク

- Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules、2013 年
- Information Technology (Information Security Practices and Procedures for Protected System) Rules、2018 年
- The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code Rules、2021 年)
- 米国国立標準技術研究所 (NIST) サイバーセキュリティフレームワーク
- ISO 27001 および ISO 27002
- Cloud Security Alliance (CSA) Cloud Control Matrix (CCM)

予算の変化の見通し：



予算項目の変更予測：



国別データ - 日本

サイバーセキュリティのサポートが必要な上位のビジネス分野：

1. リスク管理
2. カスタマーサービス
3. デジタルトランスフォーメーション
4. 財務業務
5. セールス

使用しているサイバーセキュリティベンダーの数：

1: 23%
2: 31%
3: 24%
4: 2%
5 社以上：4%
分からない：14%

包括的な AI 導入戦略を実施：

15%

AI 担当者を任命

63%

必要な AI スキルが社内にありますか？

「はい」30%

契約している、あるいは契約を検討しているパートナーの AI 関連の知識をどのように評価しますか？

5 点満点の 5：9%
5 点満点の 4：54%

サイバーインシデントを経験したパートナーを利用しますか？

「絶対に利用しない」25%
「恐らく利用しない」41%

セキュリティ侵害が発生したパートナーに、より厳格なパフォーマンス要件および SLA を課す可能性がありますか？

「はい」74%

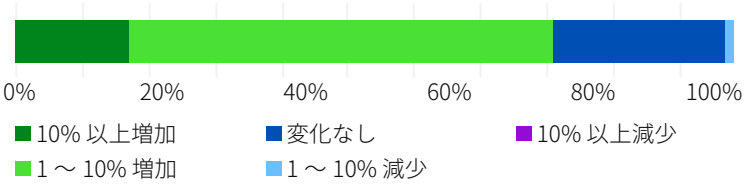
サイバーセキュリティベンダーを変更する要因には何かがありますか？

1. 自社のセキュリティが侵害された
2. パフォーマンスが不十分
3. 管理が複雑すぎる
4. 侵入テストの結果が不十分
5. テクニカルサポートが不十分

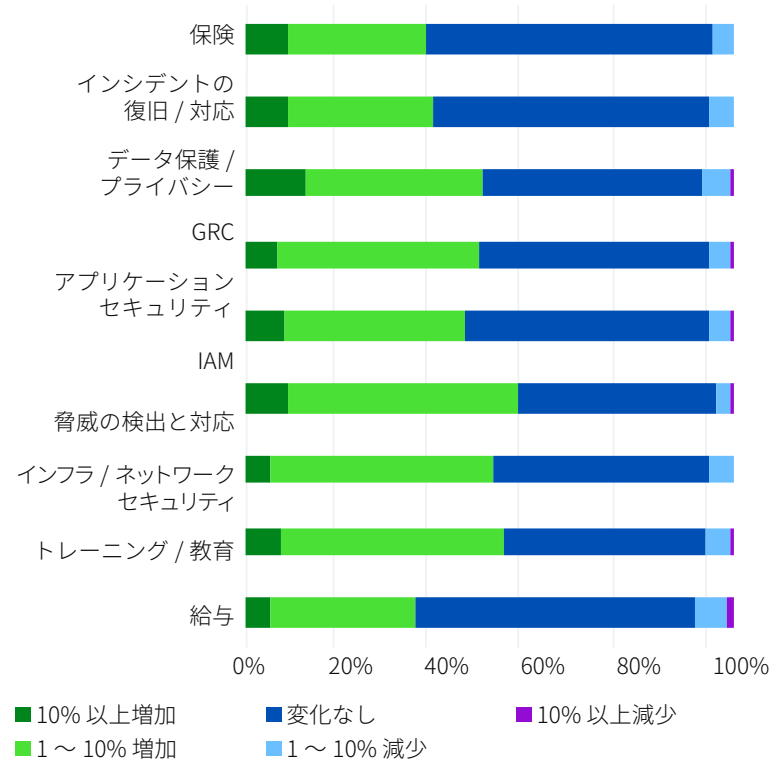
関連するフレームワーク

- 内閣サイバーセキュリティセンター (NISC) - 政府機関等のサイバーセキュリティ対策のための統一基準群
- 地方公共団体における情報セキュリティポリシーに関するガイドライン 2021 年版
- 米国国立標準技術研究所 (NIST) サイバーセキュリティフレームワーク
- ISO 27001 および ISO 27002
- Cloud Security Alliance (CSA) Cloud Control Matrix (CCM)

予算の変化の見通し：



予算項目の変更予測：



国別データ - マレーシア

サイバーセキュリティのサポートが必要な上位のビジネス分野：

1. 金融サービス
2. デジタルトランスフォーメーション
3. リスク管理
4. カスタマーサービス
5. セールス

使用しているサイバーセキュリティベンダーの数：

1: 25%
2: 29%
3: 25%
4: 12%
5: 5%
分からない：4%

包括的な AI 導入戦略を実施：

15%

AI 担当のリーダーを任命

46%

必要な AI スキルが社内にありますか？

「はい」46%

契約している、あるいは契約を検討しているパートナーの AI 関連の知識をどのように評価しますか？

5 点満点の 5：20%
5 点満点の 4：56%

サイバーインシデントを経験したパートナーを利用しますか？

「絶対に利用しない」25%
「恐らく利用しない」32%

セキュリティ侵害が発生したパートナーに、より厳格なパフォーマンス要件および SLA を課す可能性がありますか？

「はい」86%

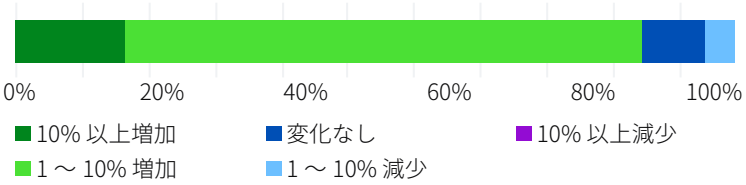
サイバーセキュリティベンダーを変更する要因には何かがありますか？

1. ソリューションのパフォーマンスが不十分
2. 自社のセキュリティが侵害された
3. 侵入テストの結果が不十分
4. 予算の変更
5. 管理が複雑すぎる

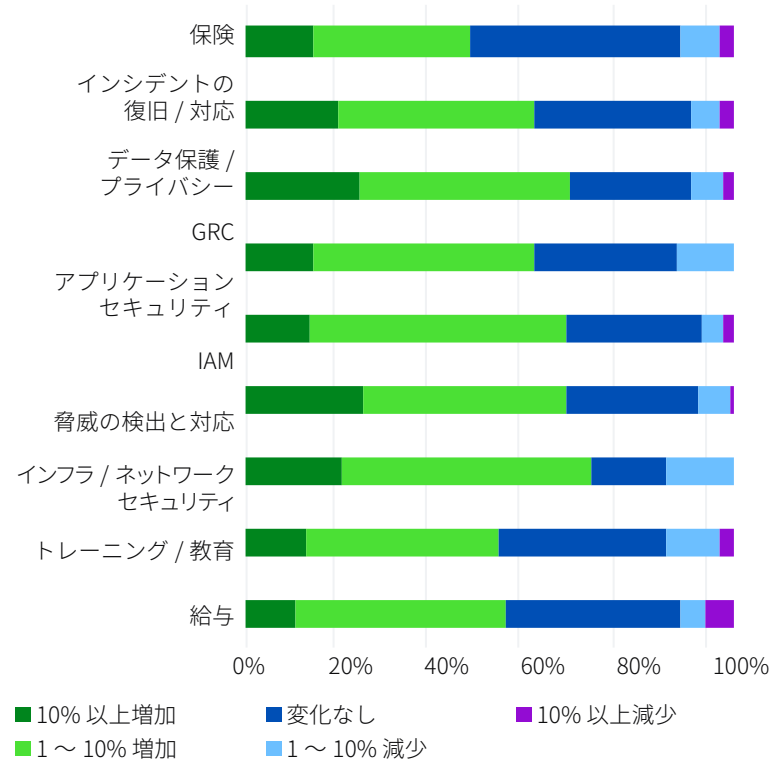
関連するフレームワーク

- Malaysian Government Cyber Security Bill 2024
- Malaysian Cyber Security Framework For Public Sector (RAKKSSA)
- 米国国立標準技術研究所 (NIST) サイバーセキュリティフレームワーク
- ISO 27001 および ISO 27002
- Cloud Security Alliance (CSA) Cloud Control Matrix (CCM)

予算の変化の見通し：



予算項目の変更予測：



国別データ - フィリピン

サイバーセキュリティのサポートが必要な上位のビジネス分野：

1. 金融サービス
2. カスタマーサービス
3. リスク管理
4. デジタルトランスフォーメーション
5. マーケティングサービス

使用しているサイバーセキュリティベンダーの数：

1: 20%
2: 27%
3: 21%
4: 10%
5: 17%
分からない：6%

包括的な AI 導入戦略を実施：

36%

AI 担当のリーダーを任命

85%

必要な AI スキルが社内にありますか？

「はい」59%

契約している、あるいは契約を検討しているパートナーの AI 関連の知識をどのように評価しますか？

5 点満点の 5：41%
5 点満点の 4：48%

サイバーインシデントを経験したパートナーを利用しますか？

「絶対に利用しない」28%

「恐らく利用しない」27%

セキュリティ侵害が発生したパートナーに、より厳格なパフォーマンス要件および SLA を課す可能性がありますか？

「はい」93%

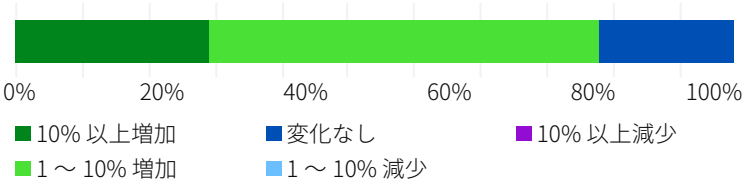
サイバーセキュリティベンダーを変更する要因には何かがありますか？

1. ソリューションのパフォーマンスが不十分
2. 自社のセキュリティが侵害された
3. 予算の変更
4. ベンダーサプライチェーンの問題
5. 侵入テストの結果

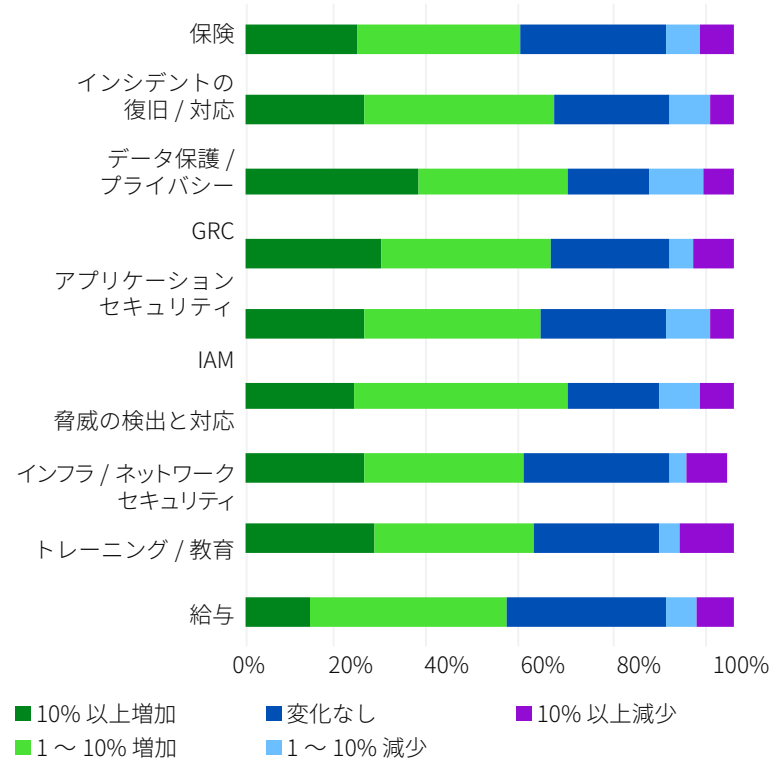
関連するフレームワーク

- フィリピン情報通信技術省 (DICT)
  国家サイバーセキュリティ計画 (NCSP) 2023-2028
- 米国国立標準技術研究所 (NIST)
  サイバーセキュリティフレームワーク
- ISO 27001 および ISO 27002
- Cloud Security Alliance (CSA)
  Cloud Control Matrix (CCM)

予算の変化の見通し：



予算項目の変更予測：



国別データ - シンガポール

サイバーセキュリティのサポートが必要な上位のビジネス分野：

1. デジタルトランスフォーメーション
2. 金融サービス
3. リスク管理
4. セールス
5. カスタマーサービス

使用しているサイバーセキュリティベンダーの数：

1: 24%
2: 40%
3: 18%
4: 8%
5: 7%
分からない：4%

包括的な AI 導入戦略を実施：

24%

AI 担当のリーダーを任命

43%

必要な AI スキルが社内にありますか？

「はい」28%

契約している、あるいは契約を検討しているパートナーの AI 関連の知識をどのように評価しますか？

5 点満点の 5：20%
5 点満点の 4：55%

サイバーインシデントを経験したパートナーを利用しますか？

「絶対に利用しない」18%
「恐らく利用しない」44%

セキュリティ侵害が発生したパートナーに、より厳格なパフォーマンス要件および SLA を課す可能性がありますか？

「はい」83%

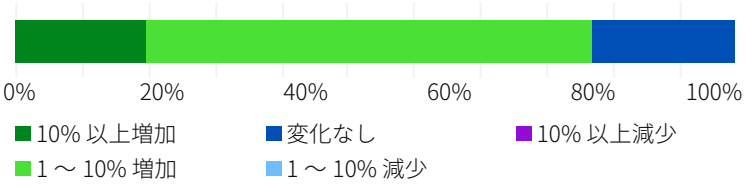
サイバーセキュリティベンダーを変更する要因には何かがありますか？

1. ソリューションのパフォーマンスが不十分
2. 自社のセキュリティが侵害された
3. 法規制の変更
4. ソリューションのパフォーマンスが不十分
5. 管理が複雑すぎる

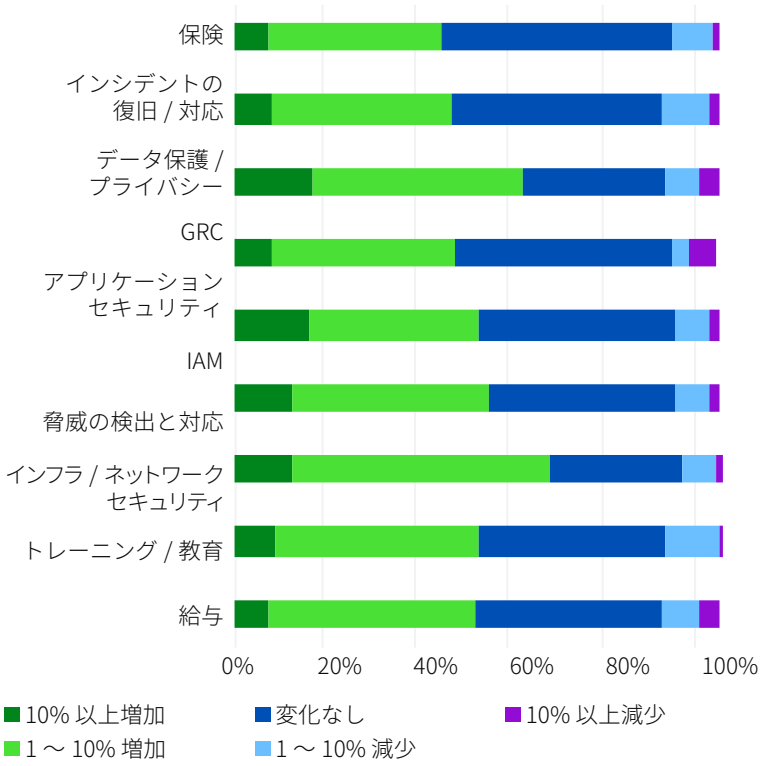
関連するフレームワーク

- シンガポールのコンピューター緊急対応チーム (SINGCert) サイバーセキュリティ法
- SINGCert Cyber Essentials
- 米国国立標準技術研究所 (NIST) サイバーセキュリティフレームワーク
- ISO 27001 および ISO 27002
- Cloud Security Alliance (CSA) Cloud Control Matrix (CCM)

予算の変化の見通し：



予算項目の変更予測：



本書について

本レポートで参照しているデータは、TRA がソフォスからの委託を受けて 2024 年 7 月にオーストラリア、インド、日本、マレーシア、フィリピン、シンガポールの 900 社を対象に実施した調査から得られています。

ソフォスについてソフォスは、MDR (Managed Detection and Response) サービス、インシデント対応サービス、およびエンドポイント、ネットワーク、メール、クラウド セキュリティテクノロジーの幅広いポートフォリオなど、サイバー攻撃を阻止する高度なセキュリティソリューションを提供する世界的なリーダーであり、革新的な企業です。ソフォスは、最大手のサイバーセキュリティ専門プロバイダーの 1 つであり、全世界で 60 万以上の組織と 1 億人以上のユーザーを、アクティブな攻撃者、ランサムウェア、フィッシング、マルウェアなどから保護しています。ソフォスのサービスと製品は、Sophos Central 管理コンソールを介して接続され、企業のクロスドメイン脅威インテリジェンスユニットである Sophos X-Ops を利用しています。Sophos X-Ops のインテリジェンスは、Sophos ACE (Adaptive Cybersecurity Ecosystem) 全体を最適化します。このエコシステムには、お客様、パートナー、開発者、その他のサイバーセキュリティおよび情報技術ベンダーが利用できる豊富なオープン API セットを活用する一元化されたデータレイクが含まれます。ソフォスは、フルマネージド型のソリューションを必要とする組織に、Cybersecurity-as-a-Service を提供します。お客様は、ソフォスのセキュリティ運用プラットフォームを使用してサイバーセキュリティを直接管理することも、脅威ハンティングや修復などソフォスのサービスを使用して社内チームを補完するハイブリッドアプローチを採用することもできます。ソフォスは、リセラーパートナー、MSP (マネージド サービス プロバイダー) を通じて販売しています。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 (TRA) 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。

www.techresearch.asia

2024-09-06 (WP-NP)