SOPHOS
Cybersecurity evolved.

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 2 版

「ソフォスの委託による TRA のレポート」

目次

はじめに

2019 年にソフォスと TRA が共同で、「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」レポートの第 1 版を発表しました。

このレポートでは、日本およびアジア太平洋地域の組織が教育、企業文化、スキル、予算編成、運用管理の分野でサイバーセキュリティのさまざまな課題に直面していることが明らかになりました。レポートの第 1 版における重要なテーマは、新しいサイバーセキュリティツールやソリューションをより効率的な方法で導入・使用し、セキュリティの脅威や問題に対する教育と意識向上を図ることでした。

2019 年のレポートと比べて何が変わったのでしょうか。

激変とは言えませんが、変化が見られています。新型コロナウイルスの感染拡大を契機とする 2020 年のテレワークへの大規模な移行で、企業の IT 部門やサイバーセキュリティ部門は大きなプレッシャーを受けました。簡潔に言えば、働く場所が大きく変わり、デジタルトランスフォーメーションが加速しましたが、2019 年にすでに表面化していたセキュリティの成熟度、教育、人材確保といった課題は解消されていません。

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 900 の企業の IT およびセキュリティの意思決定者を対象とした調査から、以下の状況が明らかになりました。

- 新型コロナウイルスの感染拡大がサイバーセキュリティにはプラスに作用し、今回の調査対象となった 69% の企業が、*「新型コロナウイルスの感染拡大が過去 12 か月間にサイバーセキュリティの戦略やツールをアップグレードする最大のきっかけになった」*と回答しました。
- 売上に占めるサイバーセキュリティ予算の割合は 2019 年から 2021 年ではほぼ横ばいでしたが、管理や監視の一元化を進める企業が多く見られました。64% の企業がサイバーセキュリティ予算を自社の IT 部門に組み込んでおり、2019 年と比較して 14% 増加しました。
- サイバーセキュリティが置かれている現状は誰もが知るところです。つまり、脅威や入手可能なソリューションを市場が熟知しているということです。新たな脅威パターンに対応したり、新しいツールを導入したりする側面もありますが、ほとんどの場合、文化、教育、およびテクノロジーを最適化することでオペレーショナルエクセレンスを向上することに重点が置かれています。
- アジア太平洋地域の企業からはサイバーセキュリティが成熟しつつあると回答も多くありましたが、一方で今も多くの攻撃を受けています。攻撃を受けた企業の割合が 2019 年に 32% だったのに対し、2021 年には 56% に上昇しました。
- スキル、予算、組織におけるサイバーセキュリティへの関心の低さが上位の課題として挙げられ、ほとんどの回答者が最新のセキュリティソリューションの開発ペースに追いていないと回答しました。2019 年と 2021 年のデータを比較すると、スキル不足、クラウド移行、脅威・攻撃の増加に伴う労力を軽減する手段としてマネージドサービスプロバイダーを活用する企業が増加したことがわかります。

第 1 版と同様、本レポートも、調査結果、各国の分析、サイバーセキュリティ戦略の評価 / 実装にあたって検討すべき手順のリスト、そして本レポートのスポンサーであるソフォスの見解という 4 つのセクションで構成されています。

> **コメントの紹介 :**2020 年までは、従業員がオフィスの外部からアクセスする手段はありませんでした。2020 年に 400 のブランチオフィスから LAN を使用しない 3,000 の「ホームブランチ」へと移行し、従来とは異なる方法でエンドユーザーを制御し、Wi-Fi を制限するようにしました。ゼロトラストセキュリティとセキュアエッジ戦略がなければ、この移行は成功しませんでした。」
>
> Angel Broking Ltd. (インド)

調査結果

調査結果を 3 つのサブセクション (成熟度と戦略、スキルの課題、インシデントと将来の展望) に分けて提示し、各サブセクションでは重要なデータと調査結果を中心に説明します。

成熟度と戦略

2019 年のレポートでは、*「回答者が自己評価するセキュリティ成熟度は低いままである」*ことを指摘しました。当時の調査で最上位の評価である「最適化された」成熟度レベルであると自己評価した企業は調査対象のわずか 2% でした。

今回の調査では、この割合が 18% に増加しました (図 1 を参照)。2 年前と比べて大幅に改善されたことから、多くの組織がセキュリティ体制の強化に向けて大きく前進したことは間違いありません (分類方法の詳細については、本レポート末尾の「回答者の内訳、定義、および調査方法」を参照してください)。

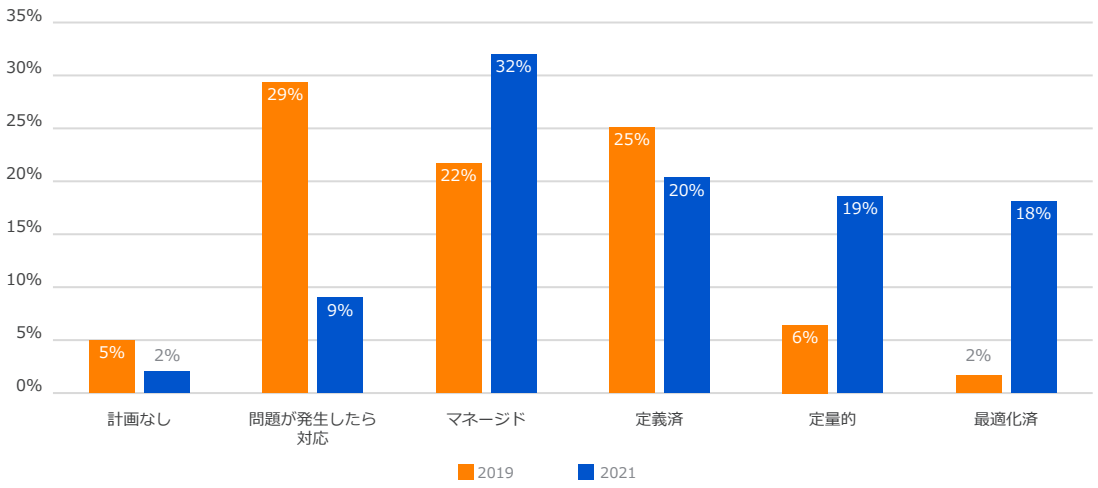


図 1:「自社のサイバーセキュリティ成熟度はどれに該当しますか？」

> **コメントの紹介：**「毎年の戦略の見直しで重要なのは、ビジネス目標を理解し、同じことを毎年繰り返すのではなく、何に投資すべきかを毎年判断することです。すべてを実行することは不可能であることはわかっていましたので、最も価値あるものを保護することの重要性を経営幹部に理解してもらう必要がありました」
>
> 国営の高齢者介護事業者 (オーストラリア)

今回の調査結果から、企業が直面するサイバーセキュリティ問題の重要性に対する認識が高まっている背景として、次のような要因が推測されます。

- 法規制の要件、特に個人特定可能情報 (PII) 保護や侵害報告の義務化に関する法律の整備が継続して進んでいること。
- 新型コロナウイルスの感染拡大によって、2020 年通年でデジタルトランスフォーメーションが加速し、テレワークやリモートでの業務への移行が進んだこと。今回の調査でも 53% の企業が、*「新型コロナウイルスの感染拡大によって突如として生まれたテレワークの保護に伴うセキュリティ要件にすぐに対応できなかった」*と回答しました。
- Infrastructure-as-a-Service (IaaS) や Software-as-a-Service (SaaS) などのクラウドベースのテクノロジーの採用が進んでいること。

調査対象企業の中で、オーストラリア、インド、フィリピンの企業が回答した成熟度は全体の平均を上回ったのに対し、日本、マレーシア、シンガポールでは「限定的な」アプローチとなっている企業の割合が多くなっています。

ただし、企業の自己評価の結果は、自己満足や過大評価であることもあり、調査データから判断すると、実際の成熟度との間には若干の乖離があると考えられます。

サイバーセキュリティ戦略の継続的な見直しについては、次のようなことがわかりました。

2019 年の調査では、51% の企業が最後に戦略を見直したのは 12 か月以上前と回答しました。2021 年に成熟度が大幅に上昇したため、多くの企業がサイバーセキュリティ戦略を継続的に改善するアプローチに移行したと予想していました。

しかし、それは間違いでした。

2021 年のデータから、わずか 3% の増加ではあるものの、全体の 54% の企業が過去 12 か月間にサイバーセキュリティ戦略を見直さなかったことがわかりました。これは、デジタル化やテレワークの取り組みが急速に進む中での数字です。

2019 年のレポートで、*「適切に定量化され、定期的にテストされない限り、成熟度レベルは非常に主観的なものになり得る」*と結論づけましたが、その考えは今も変わっていません。今回の調査では、スキル、予算、テクノロジー導入に関連する調査項目で、成熟度と能力の問題を明らかにしようと試みましたが、多くの場合、2019 年と 2021 年の間で大きな改善はほとんど確認されませんでした。

例えば、2021 年に企業がサイバーセキュリティで経験している不満のトップ 3 は以下の通りでした。

1. *「経営幹部は、サイバーセキュリティは容易に実現できるもので、サイバーセキュリティの脅威や問題が誇張されていると考えている」*(2019 年の調査で第 3 位)
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」*(2019 年の調査で第 2 位)
3. *「サイバーセキュリティのプロフェッショナル（人材）を十分に雇用できない」*(2019 年の調査で第 1 位)

以上の不満は、順位は若干異なるものの、2019 年の調査と変わっていません。

> **コメントの紹介：**「ユーザーを管理し、リスクを周知することは、重要な課題の 1 つです。経営幹部には、製品購入の目的は、1 つの問題ではなく、より複雑な問題を解決するためであることを理解してもらう必要があります。経営幹部の理解が得られたことは、幸運なことでした。」
>
> 国営の電気工学企業 (オーストラリア)

脅威を適切に検出、調査、対応できるサイバーセキュリティチームが自社に配置されているかという質問に対し、2019 年には 50% の組織が「いいえ」と回答し、2021 年には 52% に増加しました。

セキュリティを常に重視して、最新の対策を維持するのは困難と考える企業が多いのが現状です。文化、能力、熱意、教育などの企業における他の取り組みと同様、すべてが常に変化します。「不変の状態」は存在せず、企業の状況は曲線を描き、時には上昇し、時には下降します。

> **コメントの紹介：**「多くの企業がサイバーセキュリティ対策のテクノロジーをアップグレードし、成熟度を上げようとしていますが、ハッカーはそれを上回る速さで攻撃を高度化させています。ハッカーに狙われるのは、テクノロジーより、むしろ人間の弱点です。」
>
> Tanglin Trust School (シンガポール)

最新のサイバーセキュリティ対策の導入に関する課題があるかという質問では、「ある」という回答が 2019 年に 72% だったのに対し、2021 年には緩やかながら 5% の改善が見られ、67% になりました (図 2 を参照)。

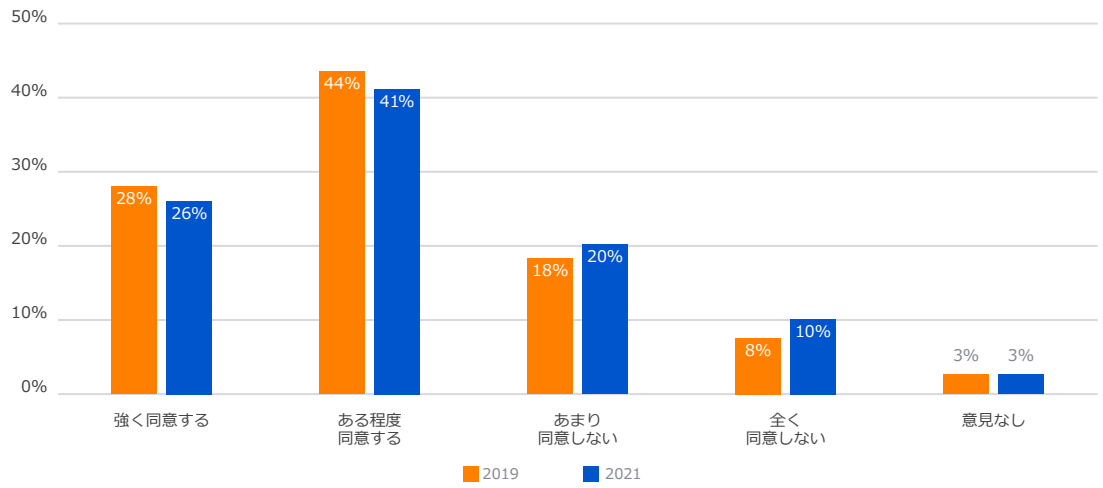


図 2:「サイバーセキュリティテクノロジーを常に最新の状態に保つことが組織の課題」

全体として改善が見られているものの、その歩みの速度は十分とは言えません。サイバーセキュリティに終わりは決してなく、技術的および文化的な両方の視点から常に注意を払っていく必要があります。

スキルに関する課題

2021 年の調査で 67% の企業が「サイバーセキュリティテクノロジーを常に最新の状態に保つことが組織の課題」と回答しており、組織がこの問題に取り組む上では、社内のスキルが重要事項になります。残念ながら、59% の企業がサイバーセキュリティのスキルを持つ人材の不足が組織にとって課題であると回答しており、2019 年の 62% からわずか 3% しか改善していません。

社内のスキルを向上させようとする企業は、適切な人材の不足と予算の制約という 2 つの障害に直面します。

- 2019 年に 67% の企業が必要なサイバーセキュリティのスキルを持つ人材の採用に苦労していると回答しましたが、2021 年にはこれがわずかに改善され、5% 減少して 62% になりました。
- 需要と供給の法則から、適切な人材の相対的な不足が続く現状で、採用側の企業に予算の増額が迫られています。2021 年も 59% の企業が、サイバーセキュリティの予算は本来必要な金額を下回っていると考えていました。これは 2019 年と同じ割合です (図 3 を参照)。

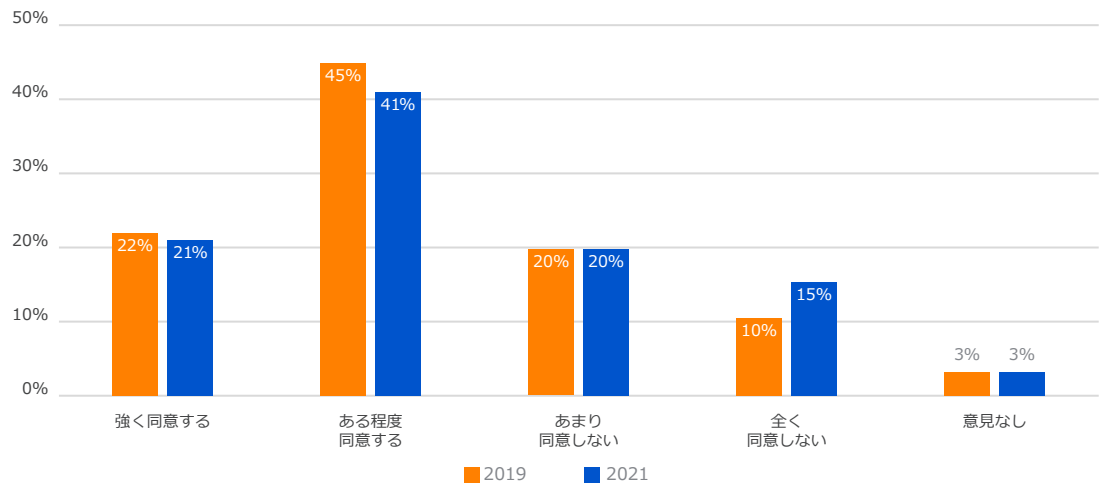


図 3:「組織に必要なサイバーセキュリティのスキルを持つ人材の採用に苦労している」

この問題をさらに掘り下げてみると、常態化した傾向が明らかになります。

多くの企業がスキル不足を解消する手段としてサードパーティの活用を検討しています。2019 年の調査では、半数以上の企業がサイバーセキュリティの戦略と管理のほとんどを社内で賄っていましたが、今回の調査データによると、全面的な外部委託または併用 (社内とサードパーティの混合) モデルへと移行する傾向が続いていることがわかりました。この傾向は、2019 年と 2021 年の比較だけでなく、回答者の 2023 年に向けての計画にもはっきり現れています。

サイバーセキュリティ戦略の策定と維持や全従業員へのトレーニングなどの活動では、外部委託や併用のアプローチがわずかな増加にとどまりましたが、サイバーセキュリティの運用やプロセスが複雑な業務では、社内を減らし、サードパーティへの委託を増やす方向に大きく動いていることがわかりました。

> **コメントの紹介 :**「必要な人材の確保が見込めない現状では、今後はパートナーに頼らざるを得ません。」
>
> Melanoma Institute (オーストラリア)

例えば、データ管理とコンプライアンスの活動では、2019 年と 2023 年の比較で、外部委託 / 併用モデルを採用する企業が 43% から 50% に増加する見込みであることがわかりました。

サイバーセキュリティのレポート作成、テスト、インシデント対応、調査、修正などのその他の機能についても、次表に示すように、2019 年と 2023 年の比較で外部委託の活用が大幅に増加しています。

表 1：2019 年の外部委託 / 併用の割合と 2023 年の予測

アクティビティ	2019 年の外部委託 / 併用の割合	2023 年の外部委託 / 併用の割合
レポート作成	46%	57%
テスト	54%	61%
インシデント対応	50%	62%
インシデント調査	56%	61%
インシデント修正	56%	61%

> **コメントの紹介：**「パートナーを活用することは合理的な選択ではありますが、パートナーが知ることができない複雑な問題が企業には存在するため、理想は、パートナーと社内の両方の人材でチームを編成することです」
>
> 国営の高齢者介護事業者 (オーストラリア)

サードパーティの活用が強化される傾向にあっても、社内の教育やトレーニングが重要であることに変わりなく、企業が直面するより重大な課題の 1 つとなっています。2019 年の調査で、60% の企業が従業員への効果的なサイバーセキュリティ教育が困難だと考えていることがわかりました。

今回の調査ではこれが 22% 増加し、82% になりました。

複雑な環境を管理するためにサードパーティを活用するケースが増加していることに加えて、自動化、機械学習、人工知能を活用したより効率的なテクノロジーソリューションを企業は求めています。それを裏付けるように、AI/ML を活用したソリューションとパブリッククラウドへの活用の両方が、企業のサイバーセキュリティに対する能力に最も大きく影響する技術的アプローチとして挙げられました (AI/ML はサイバーセキュリティの対策にも最も大きく影響することになるでしょう)。

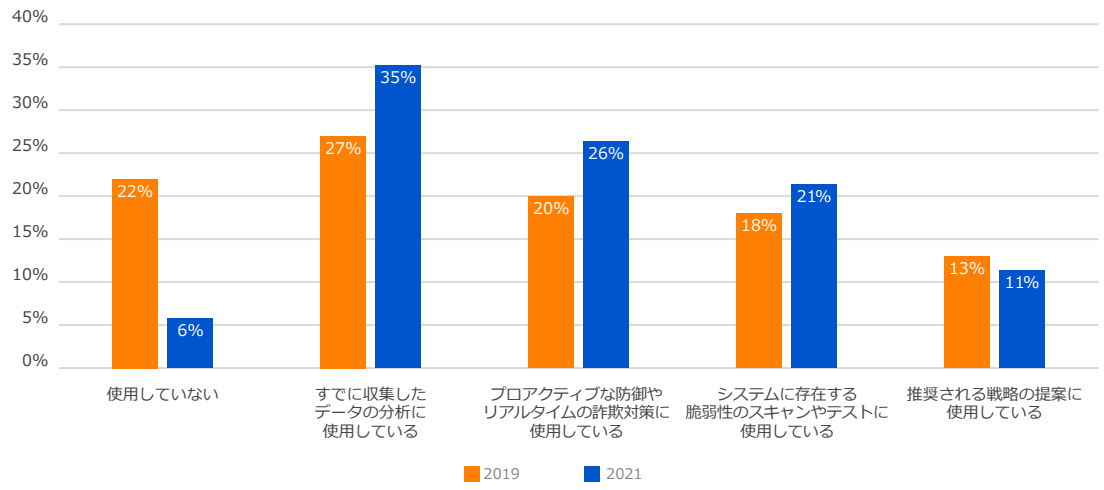


図 4:「組織の今日のセキュリティアプローチにおける AI と機械学習の役割は何ですか」

コメントの紹介：「サイバーセキュリティのスキルの需要は非常に大きいため、人材の確保は常に困難です。そのため、自動化への移行を積極的に進めて脅威の影響を軽減することを選択しました。」

フィリピン政府機関の CISO (フィリピン)

インシデントと今後の展望

2021 年に攻撃を経験した企業は多く存在します。

その攻撃が成功し、データの損失を経験した企業も多く存在します。

決して一握りではありません。

2021 年に調査対象となった企業の 68% が、何らかの形のサイバー攻撃の被害を受けたと回答しました。32% の企業が攻撃の被害を受けたと回答した 2019 年のデータと比較すると、36% と大幅に増加しました。

これらの被害を受けた企業の 55% が、データの損失を「非常に深刻」(24%) または「深刻」(31%) と回答しました (図 5 を参照)。2019 年の調査にこの質問はありませんでしたが、2021 年の攻撃の頻度から判断すると、17% の企業が週に 50 件以上の攻撃を経験し、今後はさらに活動が活発になると予想されます。

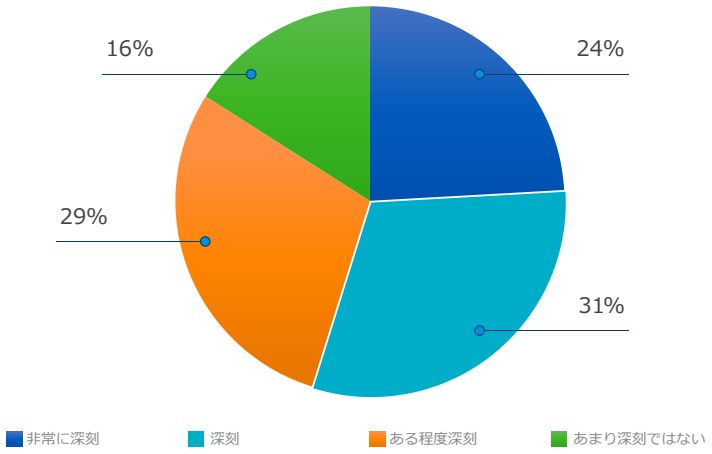


図 5:「サイバーセキュリティ侵害の損失の深刻度はどれ位でしたか」

また、調査データから、従業員数が 500 人以上の大企業が攻撃される可能性はわずかに高いものの、僅差であることがわかります。このことは、中小中堅企業も「エンタープライズクラス」のセキュリティレベルを検討する必要があることを示しており、製造業、テクノロジー、銀行および金融サービス、プロフェッショナルサービス、医療、公的機関などが最も多く標的になっています。

> **コメントの紹介：**「本校では、厳格なインシデント対応が必要とされています。ハードコピーとソフトコピーの 2 種類のインシデント対応マニュアルを用意し、問題が発生した場合にチームがマニュアルに沿って対応できるようにしています。テストを頻繁に実行して学習し、プロセスの継続的な改善に取り組んでいます。重要なのは、自分の役割と責任を全員が理解することです。」
>
> ニューカッスル大学 (オーストラリア)

脅威環境は進化し続けています。

2021 年に向けてのセキュリティ脅威として前回の回答者が挙げたトップ 3 は、以下のとおりです。

1. ランサムウェア
2. マルウェア
3. フィッシング

2023 年に向けてのセキュリティ脅威については、前回と同じ点も変わった点もあります。サプライチェーンの脆弱性 (セキュリティベンダーなどのテクノロジープロバイダーがセキュリティ侵害に気付かず、その下流の顧客が標的になること) を考慮して 2023 年の脅威のトップ 3 を予測すると、次のようになります。

1. フィッシング
2. マルウェア
3. 設計に問題がある / 脆弱なサプライヤーのシステム

テクノロジーツールが企業のサイバーセキュリティ体制に直接影響するのは明らかであり、2019 年の調査でも、人工知能と機械学習、デジタルトランスフォーメーションのプログラム、IT と OT の融合、クラウドコンピューティングへの移行が、組織のセキュリティに最も影響する要素として挙がりました。

今回のデータでも、下表に示すように、トップ 5 にほとんど変化はありません。

表 2：組織のセキュリティに最も影響を及ぼすテクノロジー

テクノロジーのトップ 5	2019 年	2021 年
1	人工知能と機械学習	人工知能と機械学習
2	デジタルトランスフォーメーション	デジタルトランスフォーメーション
3	ワークフローの自動化	ワークフローの自動化
4	IT と OT の融合	IoT デバイス
5	クラウドコンピューティング	アジャイル開発

TRA のデータは、サイバーセキュリティ業務における AI と ML の採用が 2019 ～ 2021 年に大幅に増加したことを示しています (図 6 を参照)。セキュリティアプローチ、特にデータ分析、プロアクティブな防御と不正利用防止、およびスキャンシステムにおいて、AI と ML の採用が進んでいることは明らかです。

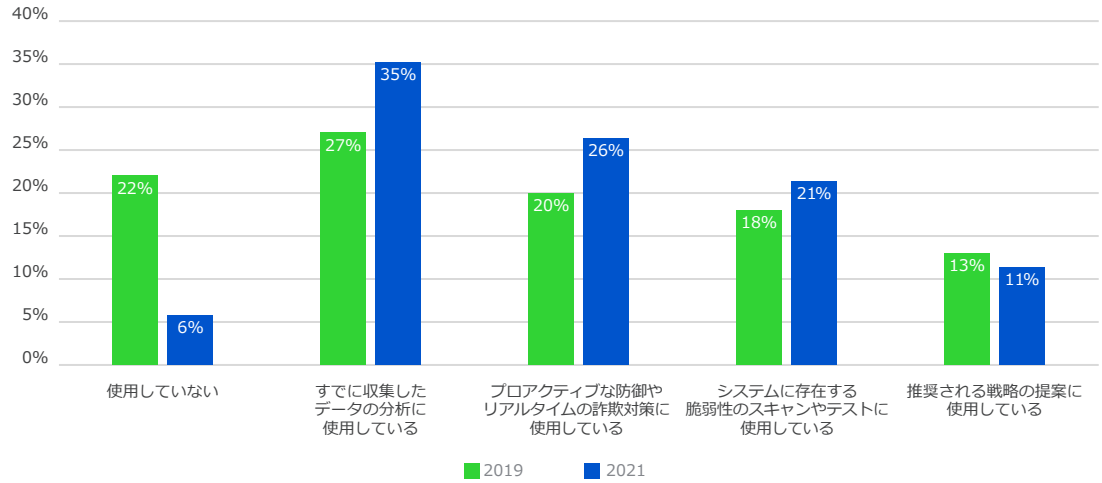


図 6:「組織の現在のセキュリティアプローチにおける AI と機械学習の役割は何ですか」

> **コメントの紹介：**「毎日 15,000 回以上の攻撃を受けているため、注目を集めた最近の攻撃をきっかけに、ゼロトラストのアプローチの強化に取り組みました」
>
> フィリピン政府機関の CISO (フィリピン)

結論

2019 年の第 1 版のレポートから何が変わったのでしょうか？

サイバーセキュリティの変化が加速しました。

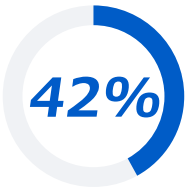
調査データによると、攻撃の頻度も脅威の方法も増え、成功率も高くなりました。新型コロナウイルスにより、企業はサイバーセキュリティ戦略の刷新を迫られましたが、テレワークへの移行に伴い、新たな弱点も露呈しています。企業は、ワークプレイス環境を変革し、デジタルトランスフォーメーションを加速させてきましたが、経営幹部の無関心、低予算、熟練したサイバーセキュリティ専門家の不足など、2 年前にすでに明らかになっていたサイバーセキュリティの構造的な課題が未だに解決されていません。

大きく飛躍するために羽を休めている可能もあります。業界をあげての取り組み、サイバーセキュリティのエキスパートとの連携によるリスクの低減、新しいテクノロジー、特に人工知能や機械学習の積極的な活用などの進展の兆しもあり、組織も、これらの機能を強化しつつ、教育と意識向上にも引き続き取り組んでいます。

2019 年のレポートと同様、以降のページでは、国ごとの詳細なデータと分析、サイバーセキュリティ戦略の策定にあたって検討すべき手順のチェックリストを提示します。さらには、本レポートのスポンサーで、この地域におけるプレミアサイバーセキュリティソリューションのプロバイダーでもあるソフォスの見解も紹介します。

日本におけるサイバーセキュリティ

「セキュリティ侵害を経験しましたか」という質問に対する回答は、以下のとおりです。



日本の企業の 42% が
過去 12 か月間に
サイバーセキュリティ攻撃の
被害者になったと回答

38% がセキュリティ侵害を
「深刻」または
「非常に深刻」と回答

38% が「セキュリティ
侵害の修正に 1 週間以上
かかった」と回答

日本の企業の 18% が、サイバーセキュリティに関して「計画なし」または「限定的」と回答し、「最高の成熟度」であると回答したのは 7% でした。

最高情報セキュリティ責任者 (CISO) が自社の戦略を率いることを計画している組織の数が、今後 24 か月間で現在の 13% から 17% に増加すると予測されます。

60% が「組織に必要なサイバーセキュリティのスキルを持つ人材の採用に苦労している」と回答しました。

わずか 4% が「活用する外部のセキュリティパートナーの数が今後 12 か月間に大幅に増加する」と回答しました。

セキュリティ関連のプロバイダーがセールスで犯しがちな主な間違いは何ですか？という問いに、72% が「自社の問題を理解していない」と回答しました。

テクノロジー関連予算に占めるサイバーセキュリティの割合の中央値は、現在の 5% から今後 24 か月間に 9% へと増加する見込みです。

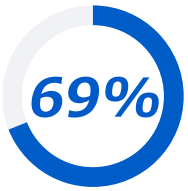
日本の企業が今後 24 か月間に自社のセキュリティに影響すると考える上位のテクノロジーや問題は以下の通りです。

- 人工知能と機械学習
- パブリッククラウドコンピューティング
- IoT デバイス

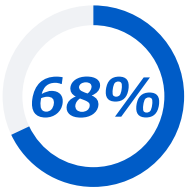
オーストラリアにおけるサイバーセキュリティ

「セキュリティ侵害を経験しましたか」という質問に対する回答は、以下のとおりです。

オーストラリアの企業の 52% が過去 12 か月間にサイバーセキュリティ攻撃の被害者になったと回答



69% がセキュリティ侵害を「深刻」または「非常に深刻」と回答



68% が「セキュリティ侵害の修正に 1 週間以上かかった」と回答

オーストラリアの企業の 61% が、プロアクティブなまたはさらに高度なセキュリティ機能を導入していると回答しましたが、10% は、「計画なし」または「限定的」と回答しました。

最高情報セキュリティ責任者 (CISO) が自社の戦略を率いることを計画している組織の数が、今後 24 か月間で現在の 37% から 43% に増加すると予測されます。

63% が「組織に必要なサイバーセキュリティのスキルを持つ人材の採用に苦労している」と回答しました。

28% が「活用する外部のセキュリティパートナーの数が今後 12 か月間に大幅に増加する」と回答しました。

セキュリティ関連のプロバイダーがセールスで犯しがちな主な間違いは何ですか？という問いに、70% が「自社の問題を理解していない」と回答しました。

テクノロジー関連予算に占めるサイバーセキュリティの割合の中央値は、現在の 6% から今後 24 か月間に 9% へと増加する見込みです。

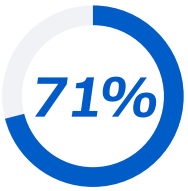
オーストラリアの企業が今後 24 か月間に自社のセキュリティに影響すると考える上位のテクノロジーや問題は以下の通りです。

- 人工知能と機械学習
- パブリッククラウドコンピューティング
- IT と OT の融合

インドにおけるサイバーセキュリティ

「セキュリティ侵害を経験しましたか」という質問に対する回答は、以下のとおりです。

インドの企業の 52% が
過去 12 か月間に
サイバーセキュリティ攻撃の
被害者になったと回答



71% がセキュリティ侵害を
「深刻」または
「非常に深刻」と回答

65% が「セキュリティ
侵害の修正に 1 週間以上
かかった」と回答

インドの企業の 3 分の 2 が、サイバーセキュリティに少なくともプロアクティブな機能を持たせていると回答しましたが、これは今回の調査対象国の中で最大の割合でした。

最高情報セキュリティ責任者 (CISO) が自社の戦略を率いることを計画している組織の数が、今後 24 か月間で現在の 33% から 40% に増加すると予測されます。

60% が「組織に必要なサイバーセキュリティのスキルを持つ人材の採用に苦労している」と回答しました。

27% が「活用する外部セキュリティパートナーの数が今後 12 か月間に大幅に増加する」と回答しました。

セキュリティ関連のプロバイダーがセールスで犯しがちな主な間違いは何ですか？という問いに、75% が「自社の問題を理解していない」と回答しました。

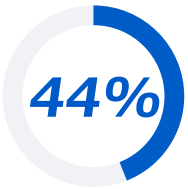
テクノロジー関連予算に占めるサイバーセキュリティの割合の中央値は、現在の 9% から今後 24 か月間に 10% へと増加する見込みです。

インドの企業が今後 24 か月間に自社のセキュリティに影響すると考える上位のテクノロジーや問題は以下の通りです。

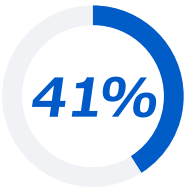
- 人工知能と機械学習
- IT と OT の融合
- IoT デバイスとブロックチェーン

マレーシアにおけるサイバーセキュリティ

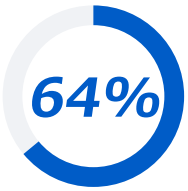
「セキュリティ侵害を経験しましたか」という質問に対する回答は、以下のとおりです。



マレーシアの企業の 44% が過去 12 か月間にサイバーセキュリティ攻撃の被害者になったと回答



41% がセキュリティ侵害を「深刻」または「非常に深刻」と回答



64% が「セキュリティ侵害の修正に 1 週間以上かかった」と回答

マレーシアの企業の 10 社に 1 社が、サイバーセキュリティに関して、「計画なし」または「限定的」と回答し、33% が基本的な計画しか策定していないと回答しました。

最高情報セキュリティ責任者 (CISO) が自社の戦略を率いることを計画している組織の数が、今後 24 か月間で現在の 41% から 43% に増加すると予測されます。

54% が「組織に必要なサイバーセキュリティのスキルを持つ人材の採用に苦労している」と回答しました。

14% が「活用する外部セキュリティパートナーの数が今後 12 か月間に大幅に増加する」と回答しました。

セキュリティ関連のプロバイダーがセールスで犯しがちな主な間違いは何ですか？という問いに、75% が「自社の問題を理解していない」と回答しました。

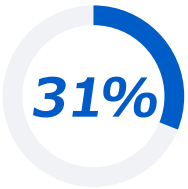
テクノロジー関連予算に占めるサイバーセキュリティの割合の中央値は、現在の 7% から今後 24 か月間に 10% へと増加する見込みです。

マレーシアの企業が今後 24 か月間に自社のセキュリティに影響すると考える上位のテクノロジーや問題は以下の通りです。

- 人工知能と機械学習
- パブリッククラウドコンピューティング
- IoT デバイス

フィリピンにおけるサイバーセキュリティ

「セキュリティ侵害を経験しましたか」という質問に対する回答は、以下のとおりです。



フィリピンの企業の 31% が過去 12 か月間にサイバーセキュリティ攻撃の被害者になったと回答

39% がセキュリティ侵害を「深刻」または「非常に深刻」と回答

55% が「セキュリティ侵害の修正に 1 週間以上かかった」と回答

フィリピンは、サイバーセキュリティの成熟度が最高レベルであると回答した企業の割合が今回の調査対象国の中で最も高くなりました (30%)。

最高情報セキュリティ責任者 (CISO) が自社の戦略を率いることを計画している組織の数が、今後 24 か月間で現在の 37% から 38% に増加すると予測されます。

44% が「組織に必要なサイバーセキュリティのスキルを持つ人材の採用に苦労している」と回答しました。

28% が「活用する外部セキュリティパートナーの数が今後 12 か月間に大幅に増加する」と回答しました。

セキュリティ関連のプロバイダーがセールスで犯しがちな主な間違いは何ですか？という問いに、86% が「自社の問題を理解していない」と回答しました。

テクノロジー関連予算に占めるサイバーセキュリティの割合の中央値は、現在の 10% から今後 24 か月間に増加しない見込みです。

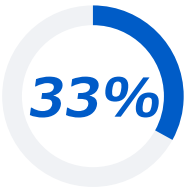
フィリピンの企業が今後 24 か月間に自社のセキュリティに影響すると考える上位のテクノロジーや問題は以下の通りです。

- 人工知能と機械学習
- IT と OT の融合
- デジタルトランスフォーメーションのプログラム

シンガポールにおけるサイバーセキュリティ

「セキュリティ侵害を経験しましたか」という質問に対する回答は、以下のとおりです。

シンガポールの企業の 28% が過去 12 か月間にサイバーセキュリティ攻撃の被害者になったと回答



33% がセキュリティ侵害を「深刻」または「非常に深刻」と回答

75% が「セキュリティ侵害の修正に 1 週間以上かかった」と回答

シンガポールの企業の 53% が、限定的または基本レベルのセキュリティ戦略しか策定していないと回答しました。

最高情報セキュリティ責任者 (CISO) が自社の戦略を率いることを計画している組織の数が、今後 24 か月間で現在の 25% から 38% に増加すると予測されます。

61% が「組織に必要なサイバーセキュリティのスキルを持つ人材の採用に苦労している」と回答しました。

10% が「活用する外部セキュリティパートナーの数が今後 12 か月間に大幅に増加する」と回答しました。

セキュリティ関連のプロバイダーがセールスで犯しがちな主な間違いは何ですか？という問いに、73% が「自社の問題を理解していない」と回答しました。

テクノロジー関連予算に占めるサイバーセキュリティの割合の中央値は、現在の 7% から今後 24 か月間に 8% へと増加する見込みです。

シンガポールの企業が今後 24 か月間に自社のセキュリティに影響すると考える上位のテクノロジーや問題は以下の通りです。

- 人工知能と機械学習
- ブロックチェーン
- パブリッククラウドコンピューティング

サイバーセキュリティのチェックリスト

TRA が提案する以下の質問を手掛かりに、組織におけるサイバーセキュリティの現状を判断してみてください。これは出発点として意図されたものであり、デューデリジェンスに取って代わるものではありません。

人と文化

- **顧客、従業員、パートナーのセキュリティに関する体験がどのようなものかを評価したことがありますか？** 顧客と従業員の体験を正しく把握しなければ、正しいセキュリティ文化を定着させるのは困難です。
- **セキュリティの脆弱性、プライバシー、倫理に関する最新知識を得ていますか？** すべてのリーダーと従業員がこの分野の最新情報の習得に努めていると断言できますか？
- **全従業員に対し、トレーニングやセキュリティスキルを「ジャストインタイム」かつ継続的に提供していますか？**
- **セキュリティを担当する適切なリーダーとチームがいますか？** そのチームの支援を全事業部門が受けられますか？また、そのチームがどのように運用され、その方法がなぜ採用されたのかを理解していますか？
- **従業員が最良のセキュリティ認定を取得するための投資を行っていますか？** これには、正規のベンダーや認証機関による外部のトレーニングが含まれます。

ポリシー、プロセス、実践

- **プロセスを監査し、組織を結び付けるものが何かの理解に役立つ、サービスの計画図や工程表を作成してくれる、信頼できるパートナーがいますか？** これは、知識の共有に役立ち、環境の管理にあたっての出発点になります。
- **各プロセスでの従業員の実際の手順を、時間をかけて観察したことがありますか？** その手順は想定や期待と一致していて、セキュリティリスクにつながらないものですか？
- **アジャイルでスプリントごとの計画図を採用して、プロセスの改善、デジタル化、自動化を進めていますか？** 状況の変化に応じた計画図の修正に備え、早期に成果を出すことで関係者の熱意を維持することが重要です。
- **セキュリティのエキスパート（社内および外部のパートナー）が、プロセスの改善や変更、新しいプロセスの構築などの初期段階に関わっていますか？** 設計済みのプロセスにセキュリティを後付けするべきではありません。
- **アジャイル開発やチームコラボレーションのための同様のアジャイルアプローチをすでにサポートしていますか？あるいは、その方向に向かっていますか？** いずれかに該当する場合、セキュリティとスピードを両立できるワークフローを実現するための他社の取り組みも調査することをお勧めします。
- **監査、ペネトレーションテスト、コンプライアンスチェックの強固なプロセスが確立されていますか？**

配置と場所

- **職場がどのように設計されていて、どのようなフロアプラン作成することでセキュリティを強化できるか、理解していますか？**
- **データや文書の漏洩が発生する可能性が高い物理的な場所を特定し、リスクを軽減するための対策を講じていますか？**データセンターから始めますが、テレワークの場所や自宅など、検討すべき場所はたくさんあります。
- **従業員の安全衛生の取り組みのアジャイル化やデジタル化はどの程度進んでいますか？**
- **融合に向けて、どのような長期計画を策定していますか？**物理的なセキュリティのデジタル化や情報セキュリティとの融合が進んでいます。つまり、画像認識などの機械学習アルゴリズムを CCTV カメラと組み合わせて利用する方法です。

データとテクノロジー

- **オンプレミス環境からマルチクラウドサービスまでの「エッジからクラウドまで」の環境を想定したセキュリティを計画していますか？**
- **どのデータやドキュメントが重要で最高レベルのセキュリティ対策が必要か把握していますか？**仮説を立てて実際に検証し、厳格に判断する必要があります。
- **現在のセキュリティ成熟度はどれ位ですか？**利用可能なさまざまなセキュリティ成熟度フレームワークだけにとらわれることなく、現状を評価します。
- **セキュリティとプライバシー（倫理）に関するフレームワークがありますか？**データや文書に関する法的および倫理的な義務をすべて満たしていることを確認します。これは、会社だけでなく、個人のキャリアをも左右する恐れがあります。

ソフォスの見解

サイバーレジリエンスの重要性は、どれほど強調しても十分ではありません。最新のコンピューティングプラットフォーム、高速のインターネット回線、従業員の分散化、クラウドベースのテクノロジーの採用が急速に進んでいることで、誰もが大きな負担を強いられています。テクノロジーの管理者には導入したツールを理解することが、ユーザーにはその使い方を学ぶことが求められますが、サイバーセキュリティインシデントのリスクを軽減するには、全員が協力してこれらの重要システムを安全な状態に維持する必要があります。

TRA による今回の調査で浮き彫りになったのは、サイバーセキュリティインシデントは誇張されていると考えている経営幹部の誤った姿勢です。これは、サイバーセキュリティを担当する IT リーダーが直面する最大のハードルです。2020 年末に、グローバルなサプライチェーン攻撃によって大きな影響を受けた組織が多くあったにもかかわらず、このような姿勢が蔓延していることに困惑しています。さらに、多くの組織で利用されている Microsoft Exchange Server プラットフォームで最近特定されたゼロデイの脆弱性が攻撃されるインシデントも多発しており、サイバーレジリエンスへの一体的な対応が強く求められています。あらゆる組織がそれぞれの役割を果たす必要があり、役割を果たすためには、全員がリスクを適切に理解しなければなりません。

フィッシング攻撃のシミュレーションやハッキングを想定した机上演習による従業員へのリスク教育の成果で、ほとんどの組織で意識が高まりつつありますが、サイバーセキュリティ成熟度とリスク許容度の差は解消されていません。

サイバーセキュリティリスクを大げさに考えすぎだと主張する役員や経営幹部を説得するには、高度なスキルと知識を持つ人材が必要であるだけでなく、信頼を得ることが極めて重要です。しかしながら、信頼はすぐに得られるものではありません。サイバーセキュリティ成熟度や必要な対策について議論して積極的に採用し、トップダウンで推進できるようになるまでには、時間がかかります。サイバーセキュリティのプロフェッショナルが組織にとってのプロバイダーとして働くことで、影響力を発揮し、サイバーセキュリティ成熟度を常に評価して対策を必要なレベルに引き上げることができます。

多くの組織が、自らの対策に対する支援を求めたり、少なくとも、現在の対策が正しいかどうかについての助言を求めたりしています。「人手が多ければ仕事は楽になる」という諺もあり、検出と対応を専門にするサイバーセキュリティプロバイダーに外部委託する組織もありますが、これらのサービスが過剰と考える組織もあります。サイバーセキュリティのプロフェッショナルとして、このような考えを変えるよう説得し、座して「それほど深刻ではない」と考えるのは組織の大きなリスクであると粘り強く説明してください。あまりにも多くの組織が有名な脅迫やデータ窃取の被害に遭い、たとえ復旧できたとしても長い時間と多額の費用がかかっています。

回答者の内訳、定義、および調査方法

本レポートの作成にあたっては、サイバーセキュリティの問題を総体的に理解するため、定量的な調査と各社の部門の最高責任者による定性的なラウンドテーブルを組み合わせた手法を採用しました。

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、シンガポールからサンプリングされた 900 社の IT およびサイバーセキュリティの部門のエグゼクティブや意思決定者を対象に、2020 年 12 月～2021 年 1 月に実施されました。調査対象はいずれも、従業員数が 150 人以上の企業です。

オーストラリア、インド、日本、シンガポール (ASEAN を代表) で実施した仮想のラウンドテーブルには、金融サービス、公共サービス、製造、医療、プロフェッショナルサービス、小売などの分野の企業の上級管理職が参加しました。

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。
- 限定的 (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。
- 実環境でテストされていない (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
- 管理されている (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。
- 定量化されている (Quantitative): 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。
- 最適化されている (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。

ソフォスについて

ソフォスは、次世代サイバーセキュリティの世界的リーダーとして、150 か国以上のあらゆる規模の 400,000 社以上の企業を今日の最も高度なサイバー脅威から保護しています。SophosLabs のグローバルな脅威インテリジェンスおよびデータサイエンスチームにより、ソフォスのクラウドネイティブで AI によって機能拡張されたソリューションは、ランサムウェア、マルウェア、エクスプロイト、データ流出、自動化されたアクティブな攻撃、フィッシングなど進化するサイバー犯罪技術からエンドポイント (ラップトップ、サーバー、モバイルデバイス) とネットワークを保護します。クラウドネイティブな管理プラットフォームである Sophos Central は、Intercept X エンドポイントソリューションや XG 次世代ファイアウォールなど、ソフォスの次世代製品ポートフォリオ全体を、API のセットを介してアクセス可能な単一の同期セキュリティ (Synchronized Security) システムに統合します。ソフォスは、クラウド、機械学習、API、自動化、MTR (Managed Threat Response) などの高度な機能を活用して、あらゆる規模の企業にエンタープライズレベルの保護を提供し、次世代サイバーセキュリティへの移行を推進しています。ソフォスは、53,000 社以上のパートナーおよびマネージドサービスプロバイダー (MSP) からなるグローバルチャネルを通じて製品を販売しています。ソフォスはまた、革新的な商用テクノロジーを Sophos Home 経由で消費者に提供しています。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 (日本語サイト : https://www.sophos.com/ja-jp.aspx) をご覧ください。

Tech Research Asia について

TRA は、優れた IT アナリストを有し、リサーチおよびコンサルティングの分野で急成長を続ける企業です。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、東京を拠点とし、経験豊富で多様なチームを擁しています。TRA は、アジア太平洋地域のエグゼクティブテクノロジーバイヤーやサプライヤーに助言を行っています。リサーチ、コンサルティング、エンゲージメント、アドバイザリサービスを提供し、厳格で、ファクトベースのオープンかつ透明性のある知見を提供しています。また、最新テクノロジーを活用することを検討しているエグゼクティブやその他の経営幹部にとって重要となる課題、トレンド、戦略について、独自の調査を行っています。TRA は、オンラインジャーナル「TQ」も発行して公開しています。

www.techresearch.asia

ソフォス株式会社営業部
sales@sophos.co.jp

2021-03-26 EN (PC)

SOPHOS