CISCO
SECURE

CISCO The bridge to possible

中堅中小企業向けサイバーセキュリティ：アジア太平洋地域の企業のためのサイバーインシデント対策

2021 年 9 月

目次

序文

デジタルニューノーマルを支えるサイバーセキュリティ

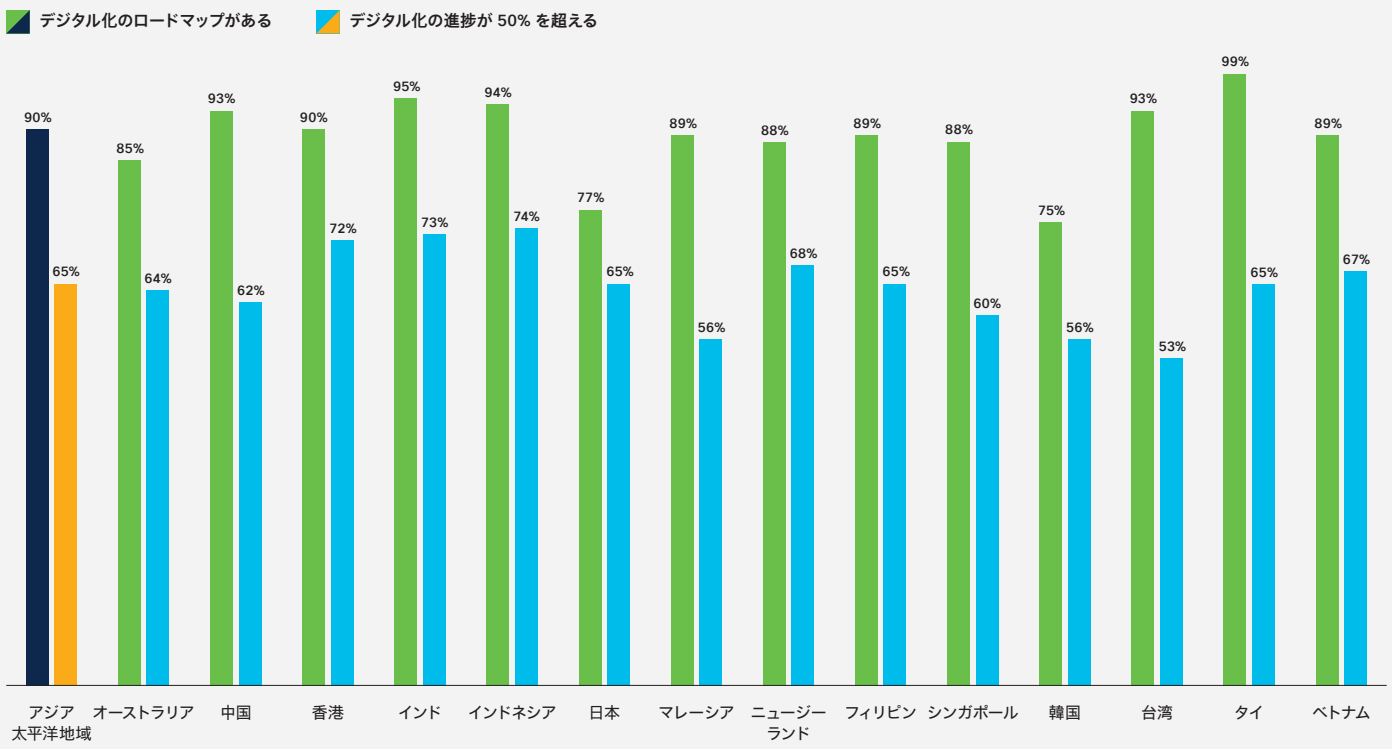
コロナ禍の影響により、あらゆる規模の組織が、テクノロジーソリューションや機能に投資する必要性を強く感じることとなりました。パンデミック当初、企業がテクノロジーを重視したのは生き残るためでした。もし大規模な都市封鎖により従業員の大半がテレワークに移行しても、テクノロジーを活用できれば業務を停止することなく、顧客にサービスを提供し続けられるからです。しかし、テクノロジーには「生き残ること」以上の効果がありました。今や各国が段階的な経済再開を試みる中、その効果を実感したあらゆる組織が積極的にテクノロジーを活用し、このニューノーマルの時代で成功することを目指しているのです。

その意識がとりわけ高いのは、アジア太平洋地域の中堅中小企業です。シスコは中堅中小企業を対象に、テクノロジーの中でも特にサイバーセキュリティに関する傾向を把握するため、独自の調査を実施しました。

その結果、アジア太平洋地域の中堅中小企業のうち、94% が何らかのテクノロジーを活用していることがわかりました。さらに注目すべきは、90% という非常に多くの企業が、デジタル化のロードマップを持っていたことです。中でも、タイの 99%、インドの 95% という結果は特に際立っていました。一方で、日本や韓国など経済が成熟した国々では数値がやや低く、デジタル化のロードマップまたは戦略があると答えた割合は、日本では 77%、韓国では 75% に留まりました。

導入においては、中堅中小企業全体の 65% がデジタル化への道を順調に歩んでおり、工程の 50% 以上が完了していると回答しています。インドネシア、インド、香港の中堅中小企業は道のりの半分を超え、台湾、マレーシア、韓国ではまだ先が長いと言えるでしょう。

市場別に見るアジア太平洋地域中堅中小企業のデジタル化の進捗



この地域の 中堅中小企業 は、デジタル化のペースを上げるにつれて、サイバーセキュリティにもより注目するようになっています。その最たる理由は、デジタル化が進むのと同時にハッカーや悪意のある攻撃者が攻撃できる対象領域も広がっているからです。「サイバーセキュリティへの懸念は 1 年前より今の方が高い」と 4 分の 3 の中堅中小企業が答えているのも驚くことではありません。懸念はかなり増加した一方で、サイバーリスクに対する中堅中小企業の認識の高まりが見られるという事実には希望が持てます。

中堅中小企業の不安には根拠があります。シスコの調査では、この地域の 中堅中小企業 の半数以上（56%）が過去 1 年間でサイバーインシデントを経験しています。その多くはサイバー犯罪で、85% がマルウェア攻撃の被害者です。こうしたインシデントの結果、悪意のある攻撃者が盗んだ貴重なデータは、顧客情報（75%）から社内電子メール（62%）、従業員データ（61%）、知的財産（61%）、財務情報（61%）にまで及びます。

サイバーインシデントにより業務が中断した企業が 62%、収益の損失につながった企業が 61% に上ることからも、中堅中小企業への影響は明らかです。

さらに、57% が顧客の信頼を失い、66% が企業の評判が低下したと回答しています。信頼の喪失や評判の低下は数値化できませんが、これらもあらゆるビジネスに壊滅的な影響を与え得ると言えるでしょう。

とは言え、中堅中小企業はこの課題をしっかり認識しています。多くの企業が自社のセキュリティ態勢を理解、改善するための戦略的イニシアチブを設定し、計画的なアプローチで対抗しようとしています。シスコの調査では、過去 12 か月で 81% の 中堅中小企業 が、潜在的なサイバーセキュリティ インシデントを想定したシナリオ策定やシミュレーションを実施しています。大半(81%)が対応計画を立て、82% は必要に応じてロールアウトできるリカバリ計画を策定しています。今後のセキュリティ成果調査では、この分野ではどのような頻度で実行するとセキュリティにプラスの効果をもたらすかを、より詳細に調査する予定です。

アジア太平洋地域の中堅中小企業が直面しているサイバーセキュリティの課題に関して、このレポートが有益な情報を提供できることを願っています。地域全体の中堅中小企業が、テレワークとオフィスワークを組み合わせたハイブリッドワークに備えて準備を進めています。これによりサイバーセキュリティ対策にはまた別の複雑さが加わりますが、このレポートに記載したサイバー対策とレジリエンス向上への実践的な提案を活用いただけると幸いです。

デジタル化がますます進む世界において、本レポートでは、すべての中堅中小企業がサイバーセキュリティの障壁に立ち向かって乗り越えるためには、時間とリソースの投入がいかに重要であるかに着目しています。この取り組みが、レジリエンスを備え将来の変化にも対応できる、最終的に成功するビジネスの構築につながると、シスコは考えています。

Kerry Singleton

シスコ アジア太平洋地域、
日本、中国、サイバーセキュリティ部門
マネージングディレクタ

鎌田道子

シスコ アジア太平洋地域、
日本、中国、小規模企業
成長戦略オフィス部門長

Bidhan Roy

シスコ アジア太平洋地域、
日本、中国、民間企業および
中規模企業セグメント部門
マネージングディレクタ

はじめに

本レポートは、アジア太平洋地域における 3,700 社以上の中堅中小企業を対象として、サイバーセキュリティの責任を担うビジネスリーダーおよび IT リーダーに調査を実施した結果を分析および紹介しています。調査は 2021 年 4 月から 7 月にかけて実施されました。

目的は、サイバー脅威が変化する中で、地域の中堅中小企業がどのようなセキュリティの課題に直面し、各リーダーがどのような対策に取り組んでいるか、また、推奨される改善策についても理解を深めてもらうことにあります。

回答者はオーストラリア、中国、香港、インド、インドネシア、日本、ニュージーランド、マレーシア、シンガポール、韓国、台湾、タイ、フィリピン、ベトナムを含む、アジア太平洋地域の 14 の市場の中堅中小企業です。

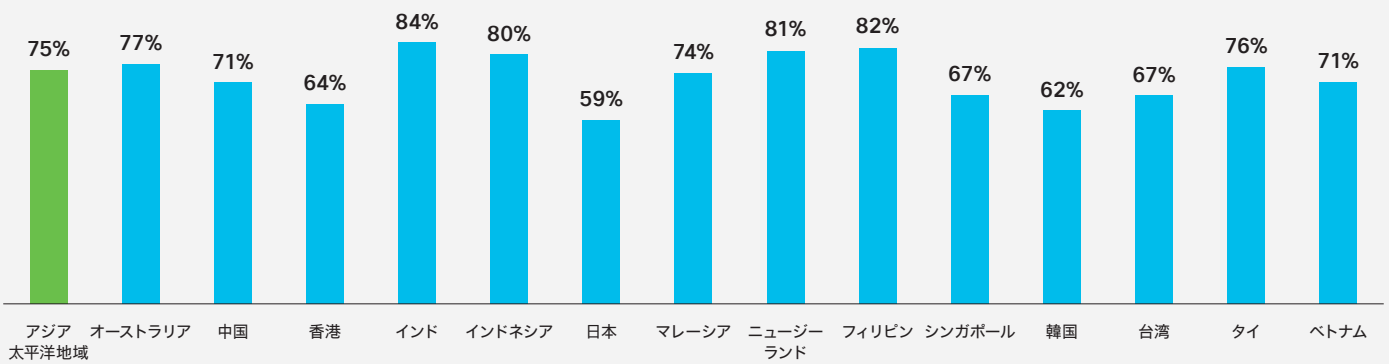
対象の業種は、ビジネスサービス、建設、教育、エンジニアリング、建築設計、金融サービス、食品 / 飲料、医療機関、製造、メディア / 通信、天然資源、パーソナルケアサービス、プロフェッショナル サービス、不動産、小売、テクノロジーサービス、旅行、運輸、卸売など多岐にわたります。

セキュリティへの高まる懸念

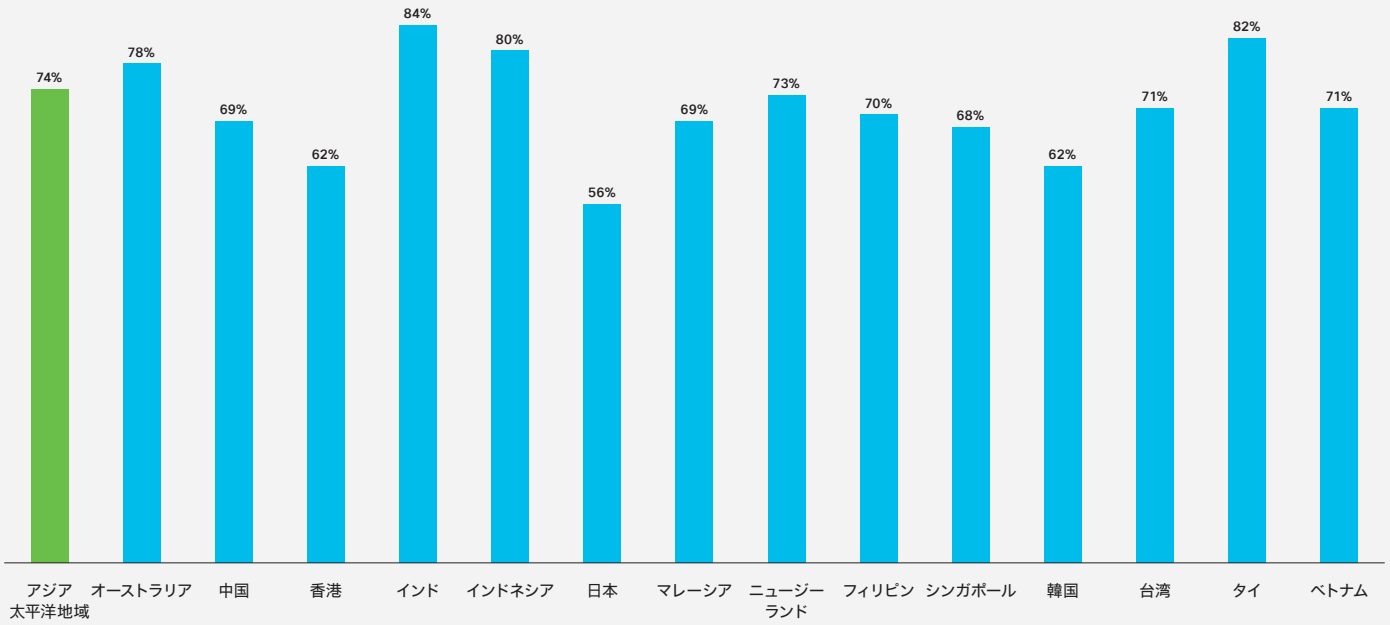
ビジネス環境の急速な進化にともない、サイバー脅威の状況もこの 1 年間で大きく変化しました。これにより、地域全体の中堅中小企業にもサイバーセキュリティリスクへの懸念が広がっています。地域の中堅中小企業の 4 分の 3（75%）が「1 年前よりサイバーセキュリティに対する懸念が高まった」と回答し、中でもインド（84%）、フィリピン（82%）、ニュージーランド（81%）、インドネシア（80%）、オーストラリア（77%）が高い懸念を抱いていることがわかります。

その背景の一部には、重大なインシデントがビジネスに与え得る影響について、中堅中小企業が理解を深めていることが挙げられます。回答した中堅中小企業のリーダーの 4 分の 3（74%）は、重大なサイバーインシデントは組織を破綻させる恐れがあると考えています。

1 年前よりサイバーセキュリティへの懸念が高まったと回答した中堅中小企業の割合



重大なサイバーインシデントが組織を破綻させる恐れがあると回答した中堅中小企業の割合

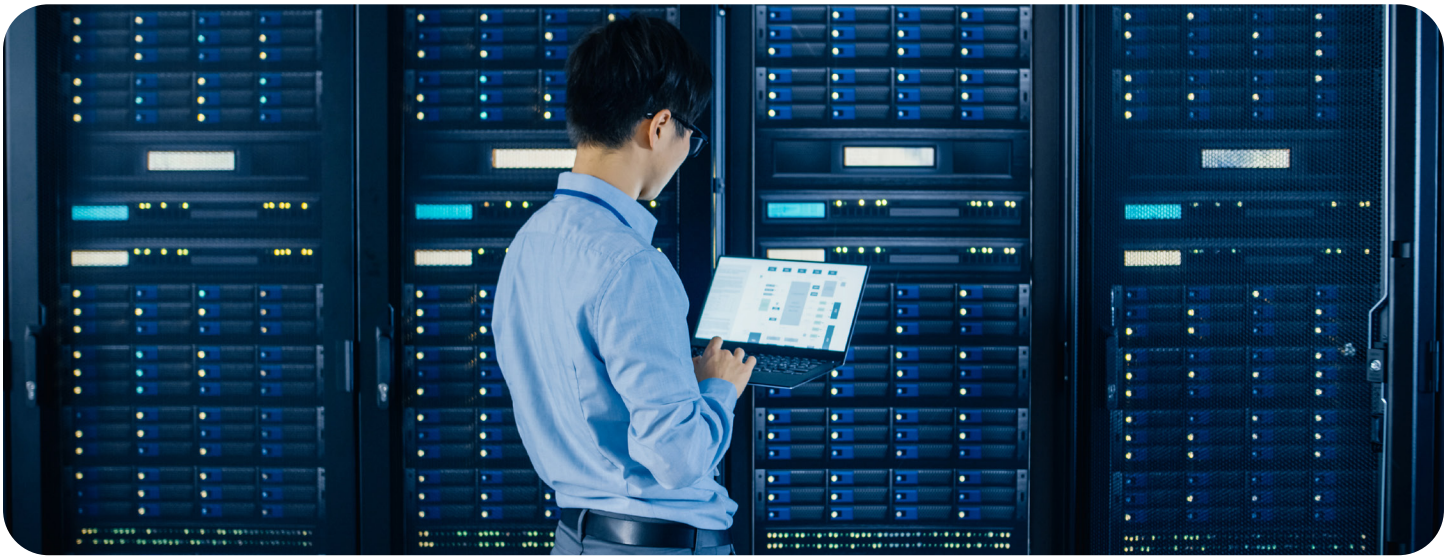


また 中堅中小企業 は、最大の脅威の発生源をこれまで以上に認識するようになっています。最大の脅威はフィッシングだと答えた中堅中小企業が地域全体で 43% と最も多く、フィッシングが最も危惧されていることが本調査でわかりました。フィッシングとは、ハッカーが信頼できる組織になりすまして電子メール、ハイパーリンク、インスタントメッセージといった特定のデジタル通信を送りつけ、ユーザに開かせようとする手口です。使い古された手口ではあるものの、簡単で効果もあるため、今も大量に出回っています。

同時に、コロナ禍をきっかけとした急速な環境の進化は、中堅中小企業の業務体系にも大きな変化をもたらしました。テレワークへの大規模な移行により、かなりの割合の従業員が社外から企業のネットワークに接続して情報にアクセスするようになりました。その大多数は接続の際に個人デバイスを使用しています。そのため、中堅中小企業のセキュリティ全体における最大の脅威は何かという質問の回答には、セキュリティ対策が施されていないラップトップ（20%）、悪意のある攻撃者による標的型攻撃（19%）、個人デバイス（12%）が挙げられました。

自社にとってサイバー攻撃の最大のリスクと思われるのは次のどれですか。

セキュリティ脅威と攻撃

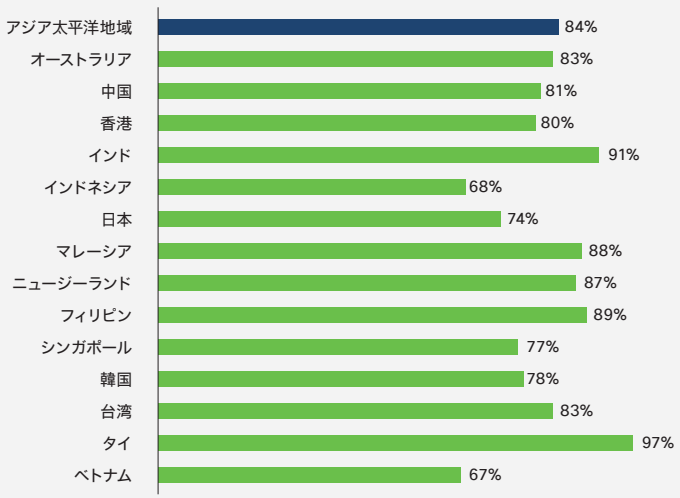


中堅中小企業が感じている不安には根拠があります。調査の結果、サイバー脅威に「さらされていると感じる」という回答が 5 分の 4（84%）を超え、「非常にさらされていると感じる」という回答が 3 分 の 1 に上りました。その大きな理由は、中堅中小企業の多くが実際にサイバーインシデントを経験しているからです。シスコの調査によれば、この 1 年間で地域の中堅中小企業の 56% がサイバーインシデントに見舞われています。

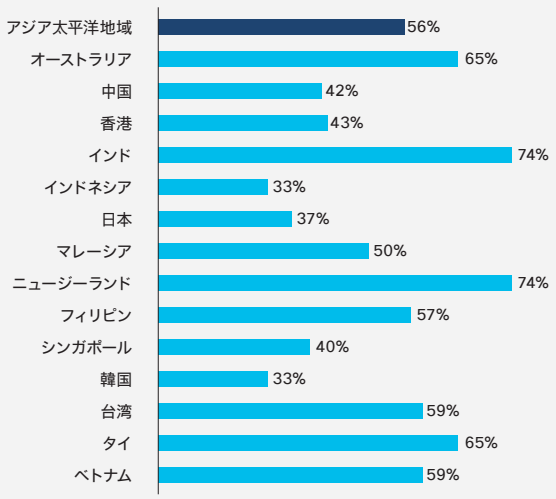
ただしこれには地域差があり、インドとニュージーランドでは 74% の中堅中小企業がインシデントを経験しているのに対し、インドネシアと韓国ではわずか 33%、日本では 37% です。

加えて、中堅中小企業の半分近くはコロナ禍の間にサイバーインシデントの被害が増加したと回答しています。増加率はインド（70%）とニュージーランド（61%）が最大で、フィリピン（53%）、ベトナム（53%）、オーストラリア（50%）がこれに続きます。

サイバー脅威にさらされていると感じる中堅中小企業の割合



過去 1 年の間にサイバーインシデントに見舞われた中堅中小企業の割合

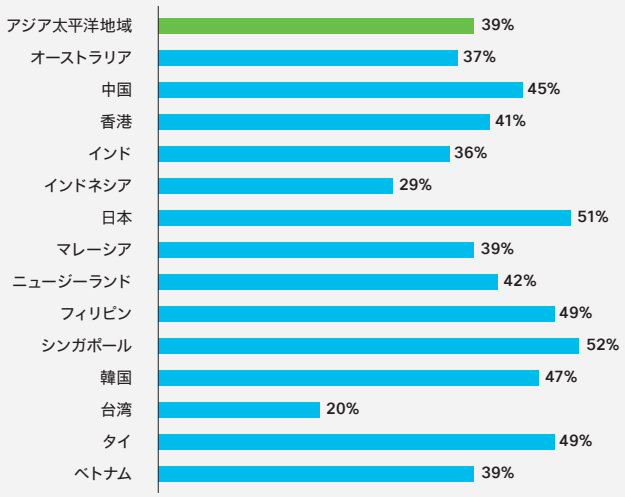


被害を受けた中堅中小企業の 3 分の 1（33%）は、その最大の要因はサイバーセキュリティ ソリューションを導入していなかったことだと考えています。しかし、さらに多くの中堅中小企業(39%) が、最大要因は「導入していたサイバーセキュリティ ソリューションが攻撃を検知して防御するには不十分だった」と回答しました。これは注目に値します。強力なセキュリティ態勢を整えるには、適切なテクノロジーが欠かせないという事実を明らかにしたためです。このことは、中堅中小企業セクターの傾向を掘り下げたシスコの『セキュリティ成果調査』における重要な発見でもありました。

インシデントを経験した中堅中小企業は、攻撃者がシステムに侵入しようと試みる手口は無数にあることに気付きました。最も多かった攻撃手法は、85% の中堅中小企業が経験したというマルウェア攻撃です（下の図を参照）。

企業がコンピュータ、タブレット、スマートフォンといったデバイスを導入して使う頻度が増えたため、攻撃者はこうしたデバイスにマルウェアを展開させようとしています。悪意のあるソ

サイバーインシデントに見舞われた最大の要因は、自社のサイバーセキュリティ ソリューションが攻撃を検知して防御するのに不十分だったと回答した中堅中小企業の割合



フトウェアを展開し、対象となるデバイスへの妨害、損害、不正アクセスを企む攻撃者は、とりわけ中堅中小企業を標的にしています。

中堅中小企業が格好の標的となる理由には、いくつか重要な点があります。1 点目は、ハッキングコミュニティの中堅中小企業に対する認識です。大規模な組織と比べて、中堅中小企業はサイバーセキュリティ分野が比較的脆弱であると考えられているため、魅力的な標的となっているのです。2 点目は、中堅中小企業と大企業の協働がさまざまな形で進んでいることです。ハッカーの狙いは、大企業のネットワークにアクセスすることです。もし中堅中小企業のネットワークに侵入できれば、そこを踏み台にして、その中堅中小企業がデジタルトランザクションやデジタル通信を行っている相手先の大企業のネットワークにアクセスできます。

回答者によれば、マルウェア攻撃の後にフィッシングがあり、70% がこの手口で攻撃されたと答えています。これ以外の主な攻撃形態には、DNS トンネリング（68%）、Denial of Service（DoS）（64%）、SQL インジェクション（62%）、中間者攻撃（61%）、ゼロデイエクスプロイト（60%）などがありました。

定義

Denial of Service（DoS）攻撃：マシンやネットワークを機能停止に追い込み、意図したユーザ（多くは銀行、メディア企業、政府機関の Web サーバ）からのアクセスを妨害する攻撃

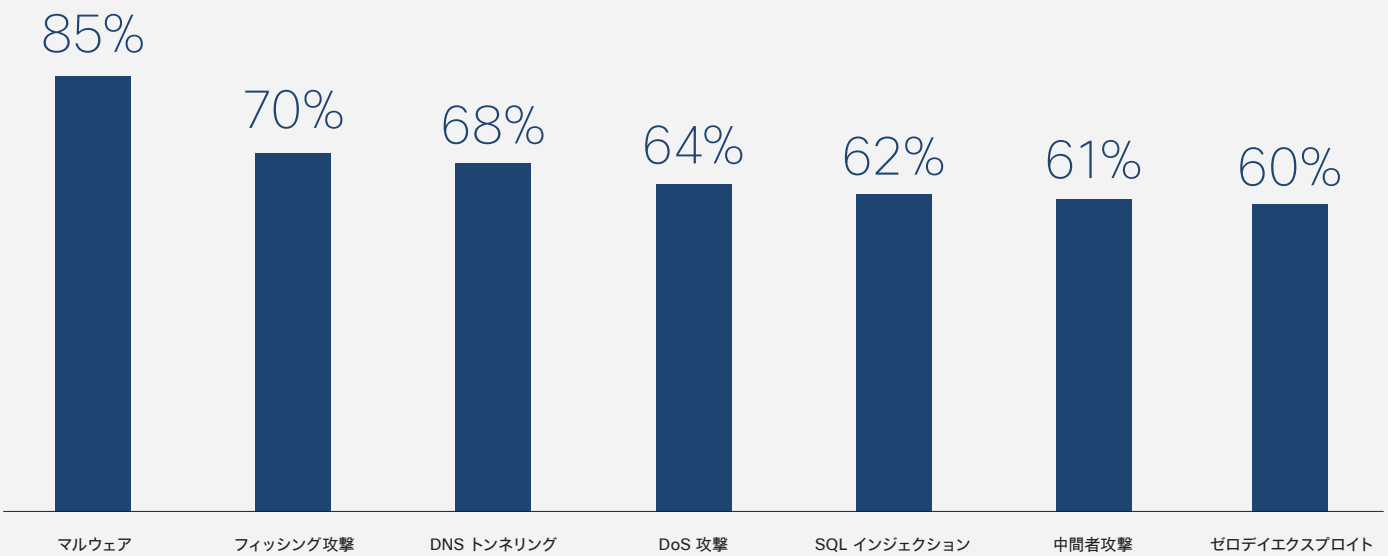
DNS トンネリング：DNS クエリと応答を利用して他のプログラムやプロトコルのデータをエンコードする攻撃

SQL インジェクション：悪意のある SQL ステートメントを入力フィールドに埋め込んで実行する、データ駆動型アプリケーションに使われる攻撃（例：攻撃者にデータベースの内容をダンプする）

中間者攻撃：攻撃者がユーザとアプリケーション間の通信に割り込み、情報交換が正常に行われているように見せかけて個人情報を盗もうとする攻撃

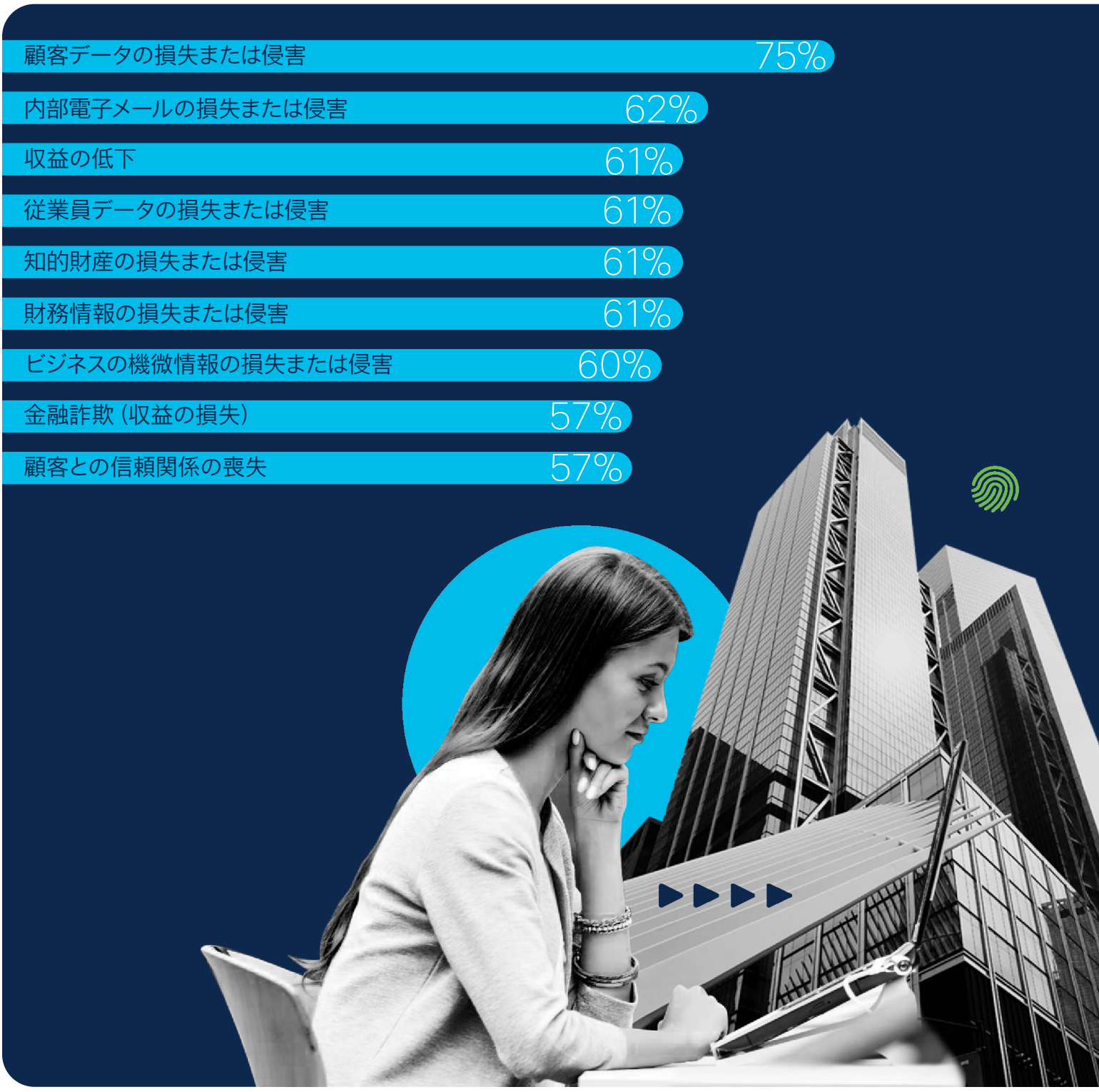
ゼロデイエクスプロイト：新しく発見されたソフトウェアの脆弱性を悪用してデータを盗んだり損害を与えようとしたりする攻撃

アジア太平洋地域の中堅中小企業が過去 1 年間で経験したサイバーインシデントの種類



脅威による損失

インシデントに見舞われた中堅中小企業の大半は、何らかの損失を受けています。
インシデントを経験した中堅中小企業のうち、実に 75% が顧客データを損失し、60% が収益に悪影響が及んだと述べています。



ダウンタイムがビジネスに及ぼす深刻な影響

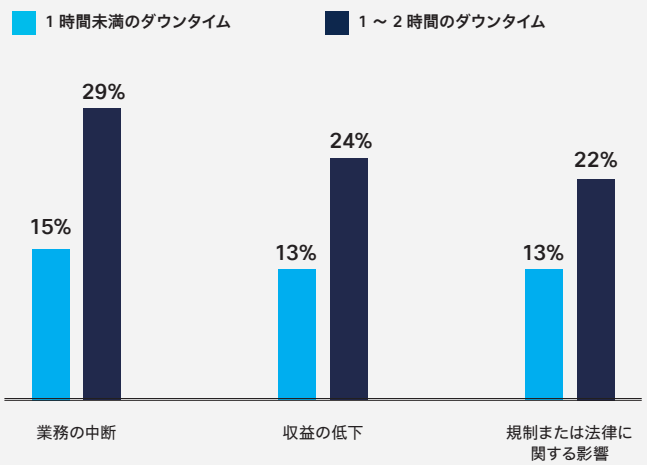
サイバーセキュリティはいわば確率のゲームです。しかしその確率は、悪意のある攻撃者に有利となっているのが現実です。彼らは常に標的を攻撃しています。攻撃されているユーザは全勝しなければならない一方で、攻撃者は一度だけ防御を通過すれば勝てるからです。

さらに、企業がサイバーインシデントを検知し、調査と修復を終えるまでには時間がかかるという現実が加わります。そのため、悪意のある攻撃者は、何らかの形で企業に先駆けて行動し、被害を拡大させられるというわけです。

世界がハイパーコネクテッドなデジタルファーストの世界に移行している現在、顧客は瞬時に満足感を得ることを求めています。これが中堅中小企業が直面している課題です。つまり、サイバーセキュリティインシデントで業務を中断させる余地は、ほとんどないに等しい状況です。そのため、サイバーインシデントの検知から調査、ブロック、修復までを、一刻も早く行う必要に迫られています。

この調査で印象的だったのは、アジア太平洋地域の中堅中小企業の 15% が 1 時間未満のダウンタイムでも業務が中断すると回答しているのに対し、29% は 1 ～ 2 時間のダウンタイムで業務が中断すると回答していることです。回答者の 13% が 1 時間未満のダウンタイムが収益に深刻な影響を与えると回答しているのに対して、24% は 1 ～ 2 時間のダウンタイムが同じ影響を与える可能性があると回答していることから、影響は数値化できます。

ダウンタイムの長さによる影響の増加 *



* 各メトリックの市場全体の内訳については、付録 A のチャートを参照してください

最も顕著なのは、中堅中小企業の 10 社に 1 社が、1 日のダウンタイムが組織の閉鎖につながると回答していることです。

同時に、各国でサイバーセキュリティに関するガイドラインや規制が導入されて施行が始まると、サイバーインシデントによるダウンタイムが法的な影響を及ぼすことにもなります。この傾向はすでに表面化しつつあり、中堅中小企業の 13% が、1 時間未満のダウンタイムにより法的な影響を受けると回答しているのに対し、22% は 1 ～ 2 時間のダウンタイムで同じ状況が発生すると回答しています。

一方で、1 時間以内にサイバーインシデントを検知できると答えた回答者は 15% しかいません。この課題が中堅中小企業にとっていかに重要であるかが浮き彫りになりました。1 時間以内にインシデントを修復できると回答した中堅中小企業は、さらに少ない 10% でした。

インシデントの検出と修復にかかった時間と中堅中小企業の割合 (%)

	アジア太平洋地域	オーストラリア	中国	香港	インド	インドネシア	日本	マレーシア	ニュージーランド	フィリピン	シンガポール	韓国	台湾	タイ	ベトナム
インシデントの検知にかかった平均時間															
1 時間未満	15%	8%	13%	11%	17%	17%	16%	17%	24%	9%	8%	11%	25%	13%	8%
1 ～ 2 時間	30%	28%	36%	28%	34%	31%	18%	32%	28%	28%	16%	34%	16%	33%	33%
組織がインシデントを修復するのにかかった平均時間															
1 時間未満	10%	6%	8%	3%	12%	12%	9%	12%	11%	9%	5%	4%	16%	7%	3%
1 ～ 2 時間	23%	20%	31%	26%	23%	27%	13%	21%	17%	22%	21%	18%	21%	26%	24%

インシデントへの対応の遅れがビジネスにいかに致命的かを考えれば、迅速な対応が鍵であることは明らかです。

中堅中小企業にとっての課題は、収益の低下だけではありません。サイバーインシデントはまた、コスト全体に影響を及ぼします。この地域で過去 1 年間にサイバーインシデントに見舞われた中堅中小企業のうち、インシデント対応に 50 万米ドル以上のコストがかかった企業が半数以上 (51%)、100 万米ドルを超えた企業は 13% に上ります。

実際に、インシデントに見舞われた企業の大半が財務的な影響を受けています。全体では 83% が、インシデントにより 10 万米ドル以上のコストを被ったと回答しました。

これには無形のコストも含まれます。過去 1 年間でインシデントに見舞われた中堅中小企業のうち、57% が顧客との信頼関係の喪失、66% が評判の低下につながったと述べています。信頼の喪失や評判の低下は数値化できませんが、これらもあらゆるビジネスに壊滅的な影響を与え得ると言えるでしょう。

過去 1 年間 (US ドル) におけるサイバーインシデントの財務的影響

	アジア太平洋地域	オーストラリア	中国	香港	インド	インドネシア	日本	マレーシア	ニュージーランド	フィリピン	シンガポール	韓国	台湾	タイ	ベトナム
50 万米ドル以上	51%	64%	41%	39%	62%	43%	49%	32%	62%	28%	51%	58%	27%	47%	30%
100 万米ドル以上	13%	33%	3%	10%	13%	12%	6%	6%	18%	10%	11%	10%	2%	28%	4%

不安を乗り越えるための対策

地域全体の中堅中小企業は、サイバーインシデントへの不安や具体的な影響があってもなお、戦う姿勢を見せています。計画策定とトレーニングから着手し、回答者の 81% がすでにシナリオ策定やシミュレーションを完了しています。

現実的なシナリオ策定とシミュレーションは、サイバー攻撃に備えた重要な対策事項です。対策によって自らセキュリティ態勢の脆弱性を発見し、攻撃者によるエクスプロイトを防げるためです。シミュレーションを実施した中堅中小企業の 85% が、これによりサイバー対策の脆弱な点や問題点が把握できたと述べています。

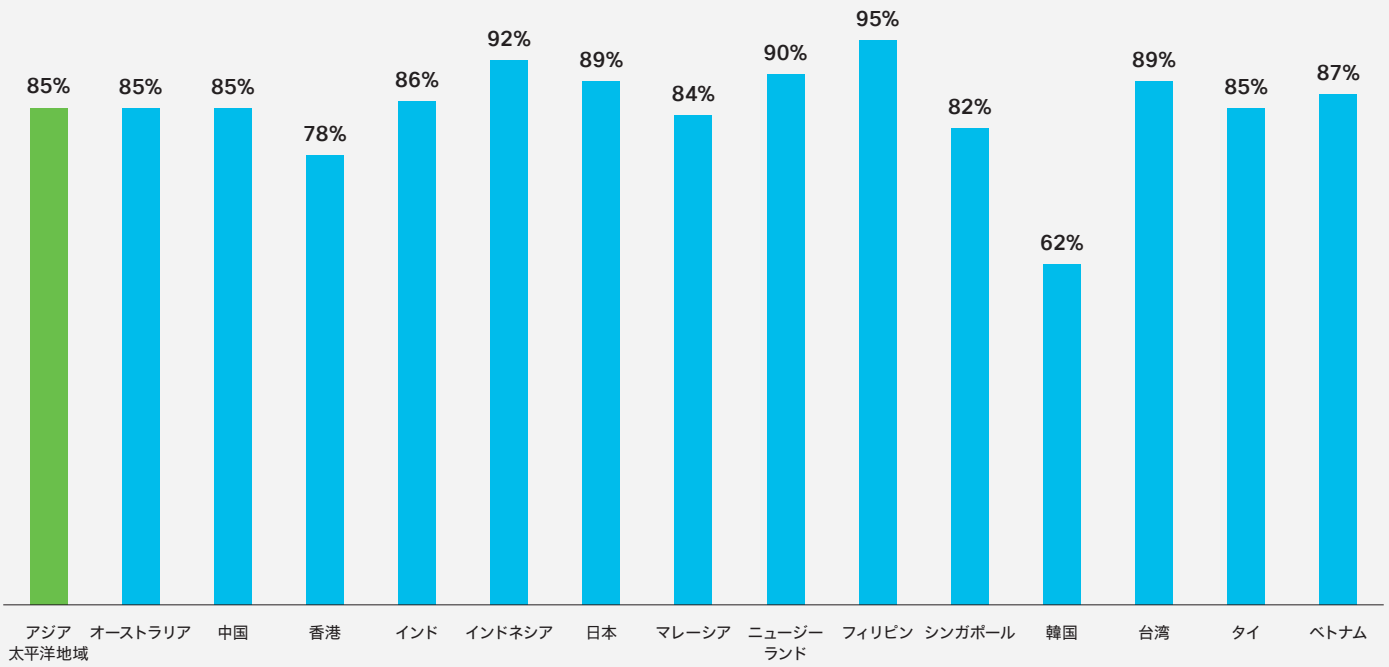
問題点を特定できた中堅中小企業の 95% は、対策を行ったことにより、サイバー攻撃や脅威を検知できる適切なテクノロジーソリューションを導入していないという、新たな問題に気が付いたと言います。また、同じく 95% が多くのテクノロジーを導入し過ぎて統合が課題だと理解し、96% が、攻撃をブロックするための適切なテクノロジーソリューションをまだ導入していないことを認識しています。

サイバー攻撃への対応プロセスが不明であるとした企業も 94% と、高い割合に上りました。一方で 95% の企業が、適切なテクノロジーを導入しているものの、それを活用できるだけのスキルを持つ従業員が不足しているという課題を挙げました。

約半分の中堅中小企業が、シナリオ策定から特定したギャップや問題点に、2 週間以内に対処できたことは心強い結果でした。唯一の例外は、攻撃や脅威を検出するための適切なテクノロジーをまだ導入していなかった中堅中小企業です。その大半は対処するまでに 2 週間を超える時間が必要でした。

中堅中小企業は全体として、シナリオ策定を通して適切な対策を講じ、サイバーセキュリティ分野におけるレジリエンスを強化しています。しかし、対処すべきエリアはまだ残っています。最も優先度が高いのは、関係者全員の教育です。中堅中小企業の 5 社に 1 社近く（17%）が、自社の幹部が現地のサイバーセキュリティの法的要件や規制要件について、限られた知識しか持っていないと述べています。このナレッジギャップはニュージーランド（30%）、香港（29%）、日本（28%）、韓国（27%）でかなり顕著です。

サイバーセキュリティのシナリオ策定またはシミュレーションを通して、サイバー対策の脆弱点を発見したと答えた企業の割合



投資先の調整とその重要性

中堅中小企業は、対策プランを確実にサポートするため投資しています。地域の中堅中小企業全体で見ても、サイバーセキュリティへの投資の比率は高いことが、この調査で明らかになりました。

この地域の中堅中小企業の 3 分の 2（63%）が年間収益の平均 4% 以上をサイバーセキュリティに費やし、30% が収益の 6% 以上、9% は 10% 超の投資をしていました。

実際、この地域の中堅中小企業の約 4 分の 3 はコロナ禍の発生以降、サイバーセキュリティへの投資額を増やしています。5% 以上増額した企業の割合も、およそ 5 分の 2 に上ります。

特筆すべきなのは、投資の増額が重要なエリアに等しく分配されていることです。これは、サイバー対策への備えを強化するには、多面的かつ総合的なアプローチが必要であることを、中堅中小企業 が十分に理解しているためと考えられます。

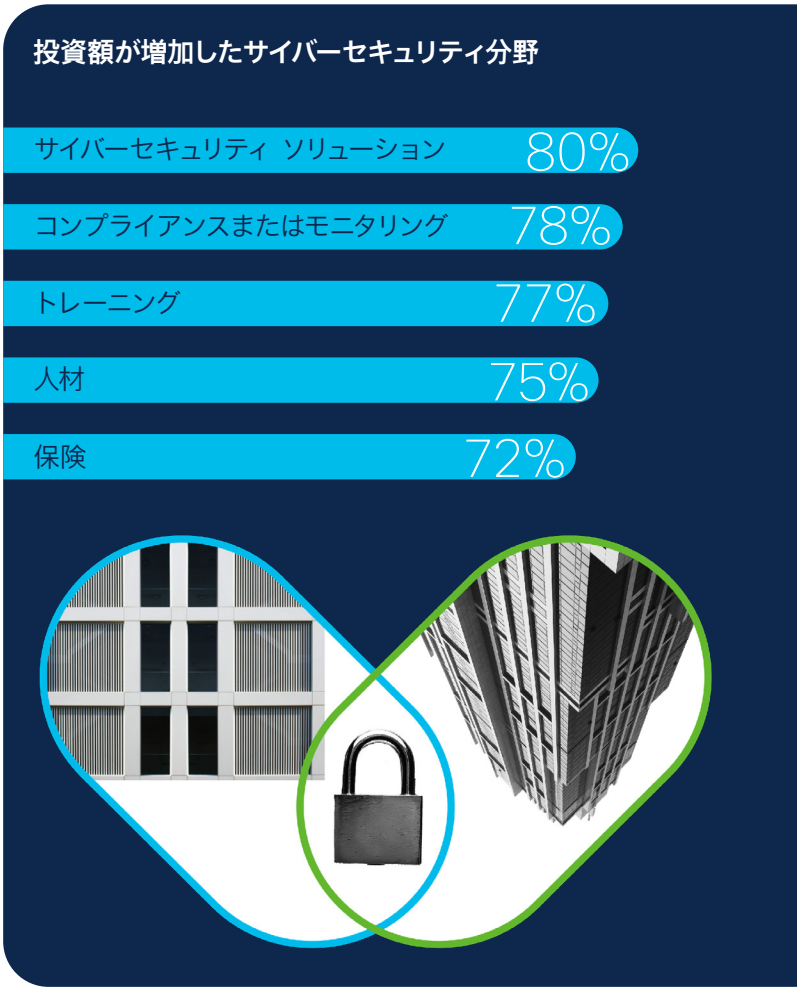
中堅中小企業の年間収益に対するサイバーセキュリティへの投資比率（%）

	アジア太平洋地域	オーストラリア	中国	香港	インド	インドネシア	日本	マレーシア	ニュージーランド	フィリピン	シンガポール	韓国	台湾	タイ	ベトナム
なし	1%	1%	0%	2%	1%	1%	8%	0%	0%	1%	2%	3%	0%	1%	0%
1% 未満	8%	11%	4%	7%	6%	5%	18%	13%	17%	7%	9%	15%	13%	6%	2%
1 ～ 3%	27%	27%	30%	38%	20%	14%	33%	28%	26%	32%	29%	37%	42%	19%	18%
4 ～ 5%	33%	34%	45%	40%	30%	37%	29%	23%	24%	32%	36%	28%	24%	32%	53%
6 ～ 10%	21%	15%	15%	9%	30%	34%	9%	24%	21%	14%	17%	15%	17%	27%	16%
10% 超	9%	11%	6%	3%	13%	9%	3%	12%	11%	15%	7%	2%	4%	15%	11%

課題については、絶えず進化するテクノロジーとセキュリティ要件に対応すること（77%）、絶えず変化するサイバー脅威に対応すること（76%）、従業員に責任をもって取り組んでもらうのが難しいこと（75%）、業界が複雑すぎること（75%）、人材確保（73%）がそれぞれ、サイバーセキュリティに対するレジリエンスを高める上で最大の障壁になると答えています。

右の図で示したように、ソリューション、コンプライアンス、人材、トレーニングといった分野への投資を厚くするという対策は、地域全体の中堅中小企業がサイバーセキュリティに適切に備えるのに妥当な第一歩です。

サイバーセキュリティに対する中堅中小企業の理解が成熟していることは、中堅中小企業が総合的な視点で対策を検討しているという事実におそらく最もよく表れています。しかし、たとえソリューション、人材、トレーニングなどに投資をしても、サイバー攻撃を受けることはあります。結局、それは業界の避けられない現実なのです。サイバーインシデントがビジネスに与える潜在的な影響、増大する法的意味への理解を深めた中堅中小企業は、別の重要な投資分野として、サイバーセキュリティ保険に関心を寄せるようになっています。サイバーセキュリティ保険はこうしたインシデントをカバーし、ビジネスに与え得る経済的影響を緩和してくれるからです。



サイバーセキュリティのレジリエンスを高める障壁と見なされる項目とその割合

	アジア太平洋地域	オーストラリア	中国	香港	インド	インドネシア	日本	マレーシア	ニュージーランド	フィリピン	シンガポール	韓国	台湾	タイ	ベトナム
進化し続けるテクノロジーとセキュリティ要件への対応	77%	82%	63%	73%	87%	53%	69%	84%	83%	89%	79%	75%	72%	71%	80%
変化し続けるサイバー脅威への対応	76%	80%	59%	71%	87%	50%	66%	87%	81%	88%	82%	74%	74%	77%	81%
従業員に責任をもって取り組んでもらうのが難しい	75%	76%	61%	65%	86%	55%	70%	81%	82%	81%	75%	67%	68%	73%	81%
複雑すぎる業界	75%	77%	61%	63%	85%	57%	65%	80%	87%	82%	82%	69%	65%	74%	79%

セキュアな中堅中小企業が実践している 5 つの習慣

サイバーセキュリティを取り巻く状況は、絶えず変化しています。本レポートでは、中堅中小企業がそうした状況に取り組む中で直面する共通の課題を説明してきました。このセクションでは、あらゆる規模の中堅中小企業が実践できる、サイバーセキュリティ態勢の改善に向けた 5 つの習慣を説明します。

1 **定期的なミーティング：**サイバーセキュリティを取り巻く環境は進化し続けているため、その脅威と組織への潜在的な影響を、常に把握しておく必要があります。シニアリーダーとすべての関係者が集まる定例ミーティングを頻繁に開催することで、ビジネス計画の策定に脅威の状況を組み込むことができます。サイバーセキュリティ イベントへの対応能力を備えた中堅中小企業は、高い頻度でこの話題を共有しています。90% 以上が脅威状況とリスクについて毎週話し合い、3 分の 2 以上（68%）は毎日話し合うと答えています。一方、脅威に対抗する体制が整っていない中堅中小企業の場合、こうしたミーティングが月に 1 回以下と答えた企業が約 3 分の 1（31%）であり、話し合いの頻度が低いことがわかっています。

2 **シンプルさが鍵：**サイバーセキュリティに対する従来のアプローチは、ポイントセキュリティ製品やポイントセキュリティ ソリューションを購入し、その時点における特定の懸念に対処することでした。こうして中堅中小企業の多くが、自社のインフラストラクチャに無数の製品とソリューションを導入しました。しかしたいていの場合、それぞれが統合されないまま運用だけが複雑になり、イベントが発生した場合に不要な遅延が発生するという結果に陥っています。重要なのは、サイバーセキュリティ スタックを構成するさまざまなソリューションがどのように連携するかを評価することです。これにより、攻撃に対処する速さとその結果が大きく左右されるためです。まったく異なる製品やソリューションの連携には、セキュリティ インフラストラクチャ全体を明確に可視化し、実際の環境でシステムをテストしてシームレスに機能することを確認できる、統合プラットフォームのアプローチが必要です。

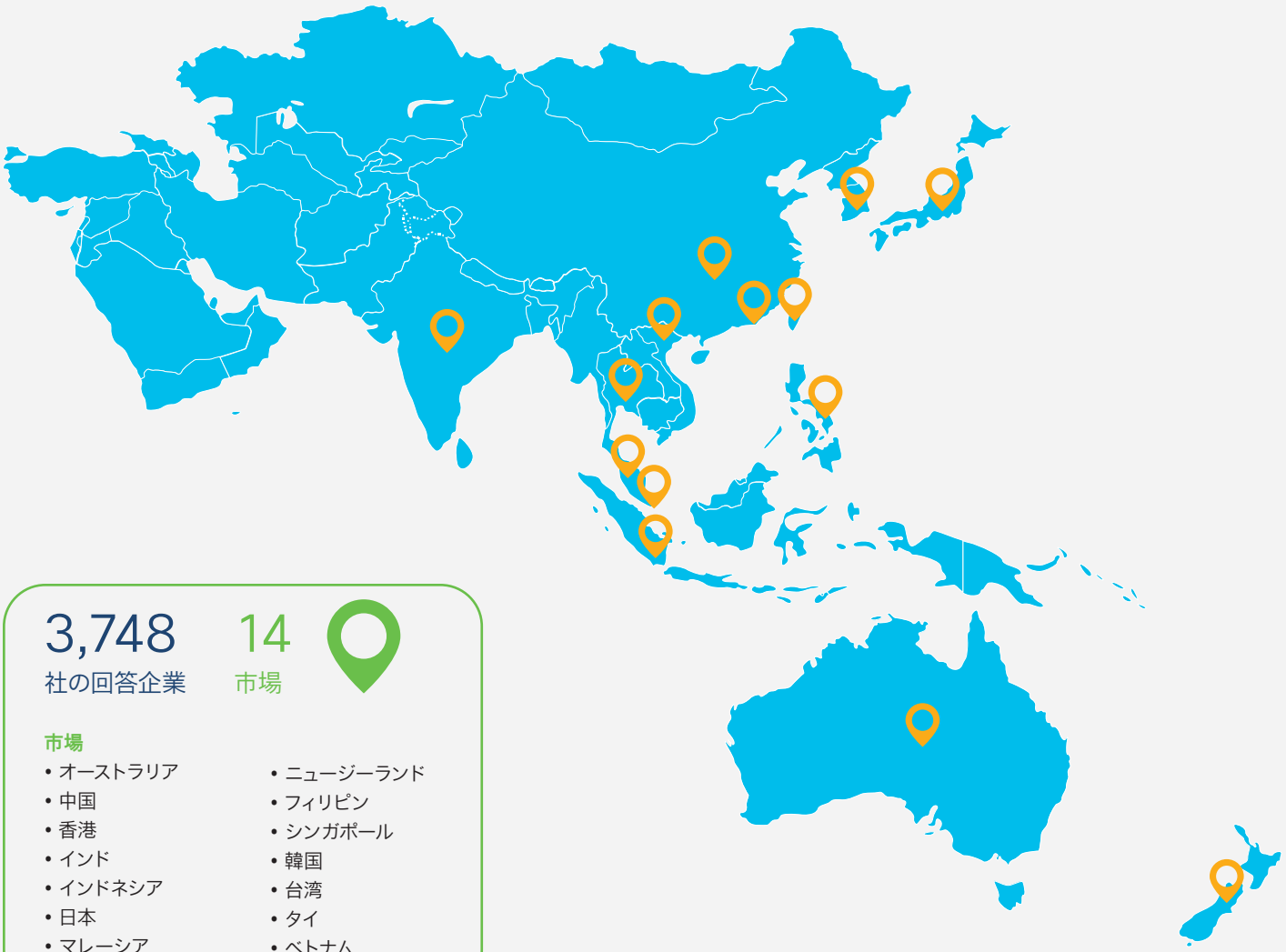
3 **準備段階で失敗し、本番に備える：**現実世界のインシデントに確実に備えるには、より管理された環境下で状況とその結果をシミュレートするのも一つの方法です。こうして脆弱性が存在する可能性がある場所を実際のシステムで特定し、その脆弱性に対処する機会が得られるため、シナリオが現実となった場合の備えが強化しやすくなるからです。シスコの調査でも、準備態勢の整った中堅中小企業の実に 98% が、過去 1 年以内にシナリオ策定やシミュレーションを実施していました。そしてそのすべてに近い 96% の中堅中小企業が、可能な限り迅速かつ効率的に業務を復旧させるためのリカバリプランを作成しています。一方で、効果的なプランを作成していない中堅中小企業では半数以上（58%）がシナリオ策定を行っておらず、3 分の 2 近く（63%）がリカバリプランを作成していませんでした。

4 **トレーニングの強化：**中堅中小企業が導入できるテクノロジーとソリューション全体のうち、人間が最大の「脆弱性」となることも多々あると認識しておくことも重要です。サイバーセキュリティがあらゆる面で進化しているにもかかわらず、フィッシングが依然として脅威媒体の第 1 位であるという事実が、それを物語っています。その手口の多くは、送信した相手にデジタル通信内のリンクをクリックするよう誘導するというものです。中堅中小企業 が取るべき対策は、役割に関係なく全従業員に必ずサイバーセキュリティの基本的な知識を身に付けさせ、ビジネスの安全性を確保するために果たせる役割についても基本的な理解をしてもらうことです。

この分野の調査データから、興味深い事実がわかります。サイバーセキュリティ事情にうまく対処している中堅中小企業のうち、「従業員は基本的なサイバーセキュリティを理解している」という質問には 96% が、「潜在的な攻撃の重大性と自身の役割を理解している」という質問には 95% が、「そう思う」あるいは「強くそう思う」と答えています。一方、イベントへの備えが不十分な中堅中小企業では、「従業員がサイバーセキュリティを理解している」という回答はわずか 15% で、従業員への信頼度が非常に低いことが明らかになりました。

5 **適切なパートナー：**サイバーセキュリティ分野全体で目標を達成するには、適切なテクノロジーパートナーとの連携が不可欠です。適切なパートナーにはいくつか重要な条件があります。まず、中堅中小企業のビジネス全体にエンドツーエンドの保護を提供できる必要があります。多くの場合、さまざまな製品やソリューションを 1 つのプラットフォームに統合し、インフラストラクチャ全体でシンプルさと可視性を実現する必要が生じるからです。次に、ビジネスの規模に関係なく運用を保護できることです。中堅中小企業 がデジタル化に着手すれば、ビジネスは最終的に成長し、業務を拡大することになるからです。最後に、中堅中小企業 がテクノロジーをどのように導入するかについて、さまざまな消費モデルを提供できる能力が求められます。

この調査について



3,748 社の回答企業

14 市場

市場

- オーストラリア
- 中国
- 香港
- インド
- インドネシア
- 日本
- マレーシア
- ニュージーランド
- フィリピン
- シンガポール
- 韓国
- 台湾
- タイ
- ベトナム

対象者

サイバーセキュリティの責任を担う IT/ビジネスリーダー

対象企業規模：

- 小規模（従業員 1 ～ 249 人）
- 中規模(従業員 250 ～ 999 人）

業界

- 広告または市場調査
- ビジネスサービス（会計、コンサルティングなど）
- 建設
- 教育
- エンジニアリング、設計、アーキテクチャ
- 金融サービス
- 医療機関
- 製造業
- メディア / コミュニケーション
- 天然資源（石油、鉱業、林業など）
- パーソナルケア / サービス
- プロフェッショナル サービス
- 不動産
- レストランサービス
- 小売
- テクノロジーサービス
- 運輸
- 旅行サービス
- 卸売
- その他

付録 A

ダウンタイムの長さによる影響の増加

	アジア太平洋地域	オーストラリア	中国	香港	インド	インドネシア	日本	マレーシア	ニュージーランド	フィリピン	シンガポール	韓国	台湾	タイ	ベトナム
組織の運用に重大な影響が及ぶダウンタイムの長さ															
1 時間未満	15%	10%	21%	11%	17%	18%	10%	13%	17%	16%	7%	10%	21%	18%	8%
1 ～ 2 時間	29%	25%	28%	21%	32%	35%	18%	32%	39%	28%	23%	29%	28%	31%	30%
収益に重大な影響が及ぶダウンタイムの長さ															
1 時間未満	13%	8%	16%	12%	12%	25%	7%	16%	9%	15%	10%	14%	14%	14%	9%
1 ～ 2 時間	24%	20%	26%	21%	24%	27%	17%	23%	19%	27%	20%	19%	34%	28%	20%
規制上または法的な影響が出るダウンタイムの長さ															
1 時間未満	13%	7%	16%	14%	13%	19%	6%	17%	8%	13%	11%	13%	18%	14%	12%
1 ～ 2 時間	22%	19%	24%	18%	24%	32%	15%	23%	20%	19%	24%	21%	25%	22%	17%

Cisco Secure について

シスコは長年にわたりネットワーク分野のリーダーとしての地位を守り続け、総合的かつオープンなサイバーセキュリティ ソリューションのポートフォリオを構築してきました。セキュリティソリューションは連携して機能するように設計すべきというのがシスコの基本的な考え方です。

セキュリティソリューションとは本来、相互に連携して情報を取り入れ、協調的なユニットとして対応するものであるべきです。それが実現すれば、セキュリティはより体系的かつ効果的なものとなります。シスコは IT インフラとネットワーキングサービスにおける世界最大のプロバイダーとして、また B2B サイバーセキュリティ事業を手掛ける世界最大手として、長年の信頼と実績があります。

Cisco Secure は、最高水準のセキュリティを目指して開発されています。導入、管理、使用が簡単な、顧客中心の合理化されたアプローチを通じてセキュリティを確保できるだけでなく、すべての要素が連携して機能します。シスコは人とお客様を第一に考えて活動しています。また、複雑さとノイズを取り除き、自社のセキュリティに対する自信を高めたいというお客様の声にしっかり向き合い、成果に焦点を当てて開発に取り組んでいます。そのためには極度な単純化を避けつつシンプル化を推し進める必要があります。この目標に向けた大きな布石が、シスコのクラウドネイティブなプラットフォームです。

シスコは Cisco SecureX プラットフォームを通じて、現在および将来の脅威に対する安心感と信頼性をセキュリティのコミュニティに提供しています。現在、すべてのフォーチュン 100 企業が、世界で最も包括的なシスコの統合型サイバーセキュリティ プラットフォームにより現在と将来の脅威から守られています。シスコのソリューションがエクスペリエンスをどのようにシンプル化し、成功を加速させ、未来を保護するかについては、www.cisco.com/c/ja_jp/products/security/index.html をご覧ください。

シスコセキュリティ成果調査

詳細については、『2021 年度 セキュリティ成果調査 - 中堅中小企業版』をご覧ください。また、Cisco Secure ソートリーダーシップのコンテンツについては、専用ページをご覧ください。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp


CISCO