Digital Security
Progress. Protected.

ESET SMB サイバーセキュリティレポート 2024 年版

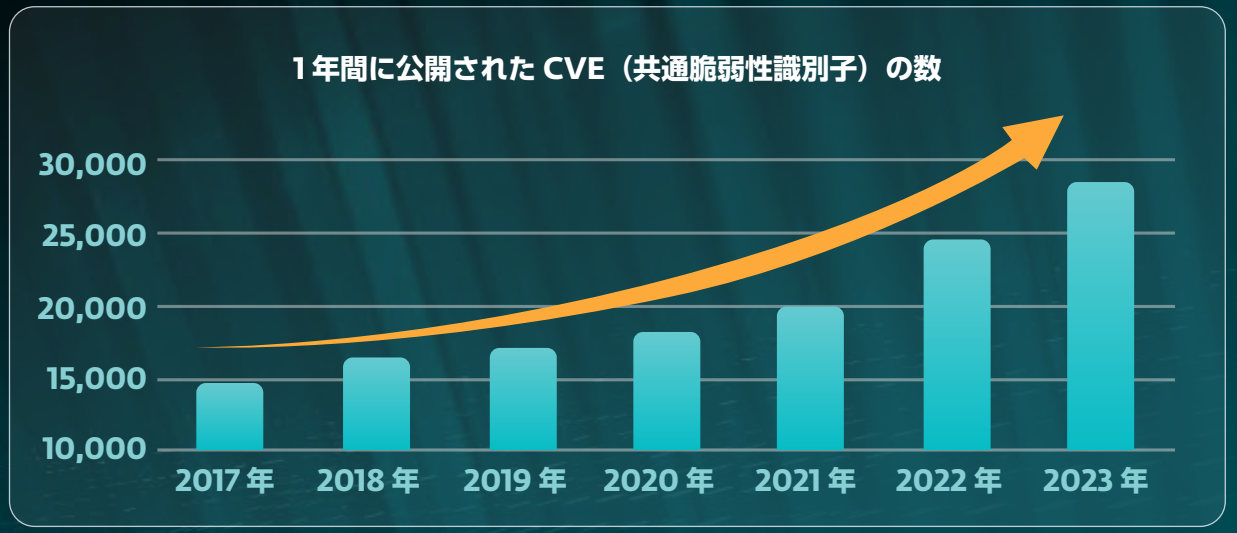
CYBERSECURITY™
MADE IN EUROPE

2023 年
新たなマルウェアとソフトウェア脆弱性が記録的に急増

データ侵害とサイバー攻撃が今後さらに広がることを示す**2 つの重要な指標**があります。

最初の指標はマルウェアの数です。**サイバー犯罪者は記録的な数の新しいマルウェアを展開**しています。ESET は 1 日あたり平均 50 万件以上のユニークマルウェアを検出しています。

次の指標は、**オペレーティングシステムを含むソフトウェアの脆弱性**です。これらの脆弱性は**昨年 7 年連続で過去最高を記録**し、1 日平均 80 件の脆弱性が新たに見つかっています。



50 万件

毎日検出される新しいユニークマルウェアの数。

基本知識

エクスプロイトは、ソフトウェアの脆弱性を攻撃してコンピュータシステムを侵害する方法であり、通常は悪意のある目的で使用されます。エクスプロイトによる攻撃には、ランサムウェアやスパイウェアなどのマルウェアのインストールや機密データの窃取など、有害な行為が含まれます。

序文

「サイバー犯罪者は、かつてないほど精度の高い巧妙な攻撃を仕掛けています。**中堅・中小企業（SMB）もこれらの脅威の標的**になっています。実際、攻撃者は SMB の防御が脆弱であることを理解しており、重要な標的にしていることも多くあります。

しかし、このレポートでは恐怖を煽るのではなく、実用的な対策について説明します。**シンガポールサイバーセキュリティ庁が提供している Cyber Essentials マークやオーストラリアのサイバーセキュリティセンターが公開している Essential Eight** など、効果的なサイバーセキュリティモデルは、SMB にとっても有用なフレームワークとなります。これらのモデルやその他のツールを活用することで、SMB は防御力を強化し、逆境に立ち向かうことができます。

究極的には、**プロアクティブで予防を中心とした防御が最善のサイバーセキュリティ戦略**となります。」

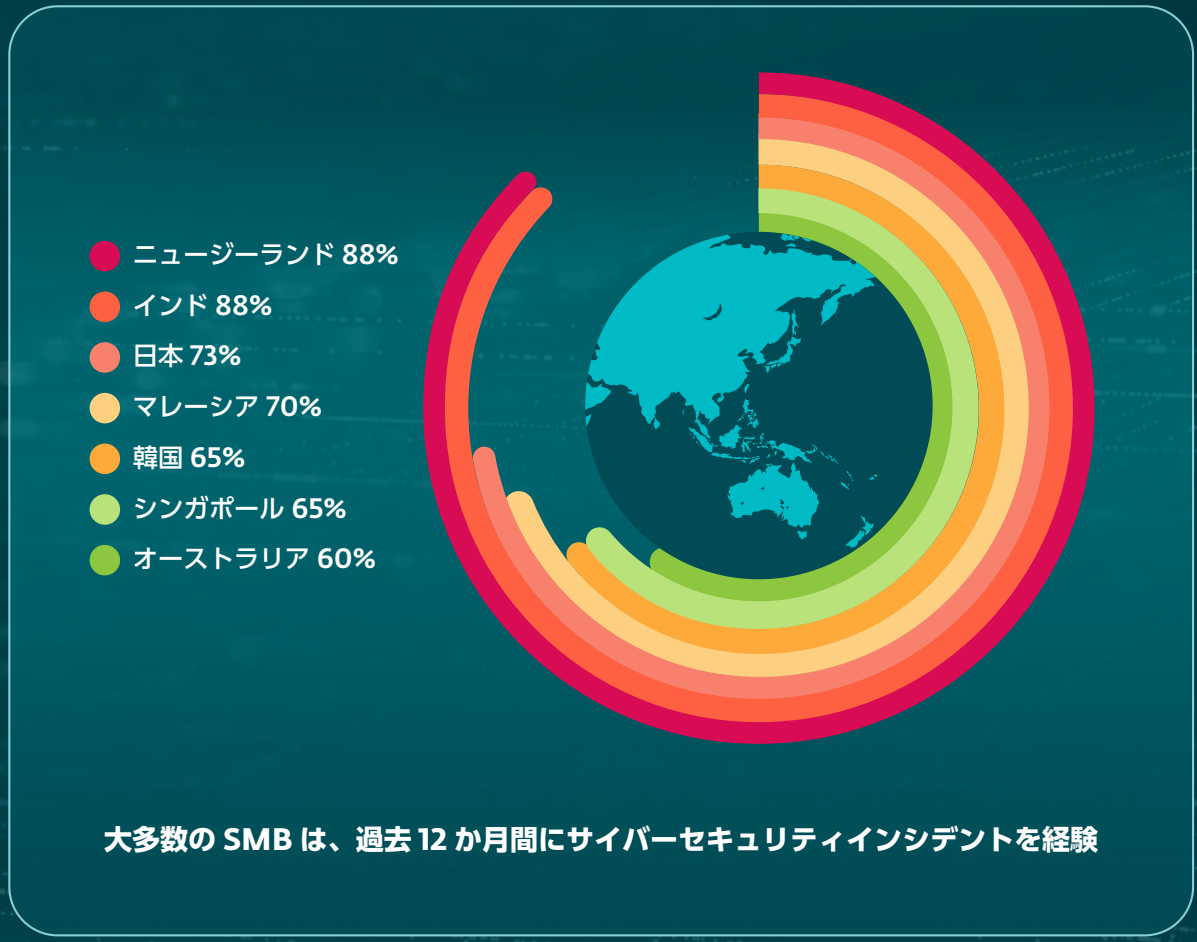
PARVINDER WALIA（パービンダー・ワリア）
アジア太平洋地域および日本担当プレジデント、ESET

SMB でのサイバーセキュリティインシデントは驚くほど多い

10 社に 7 社

調査対象となった APAC 全域の組織の **10 社中 7 社が、過去 1 年間にサイバーセキュリティ侵害を経験したか、データセキュリティインシデントが発生したことを示す確度の高い兆候に基づいて対応を講じていました。**

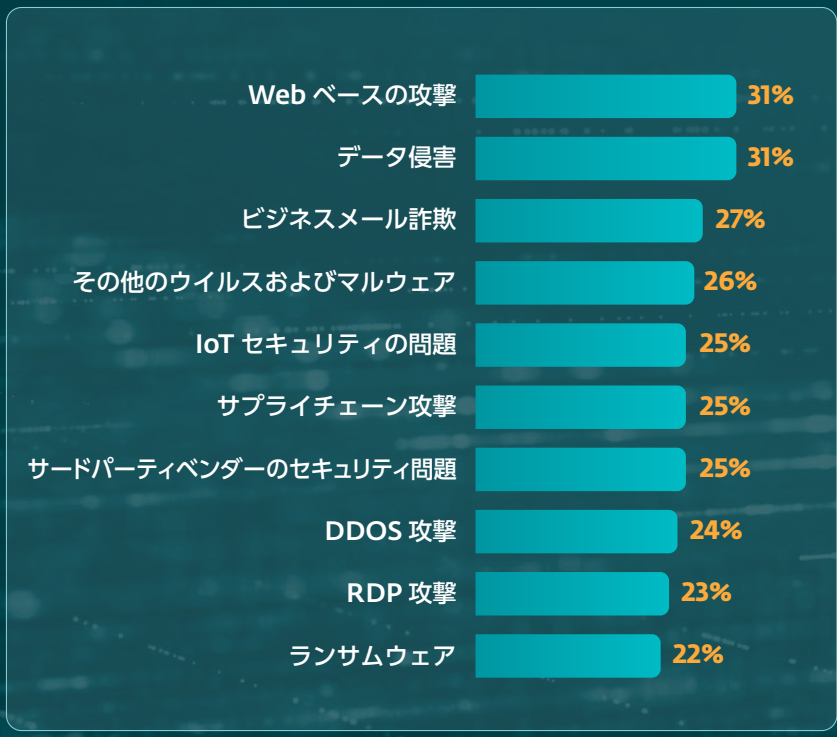
インドとニュージーランドの組織でインシデントが発生した割合は 88% であり、非常に高くなっています。



大多数の SMB は、過去 12 か月間にサイバーセキュリティインシデントを経験

Web ベースの攻撃とデータ侵害が最も多い

最も多く発生しているセキュリティ侵害またはセキュリティインシデントは、Web ベースの攻撃とデータ侵害であり、これらの発生率は 31%でした。

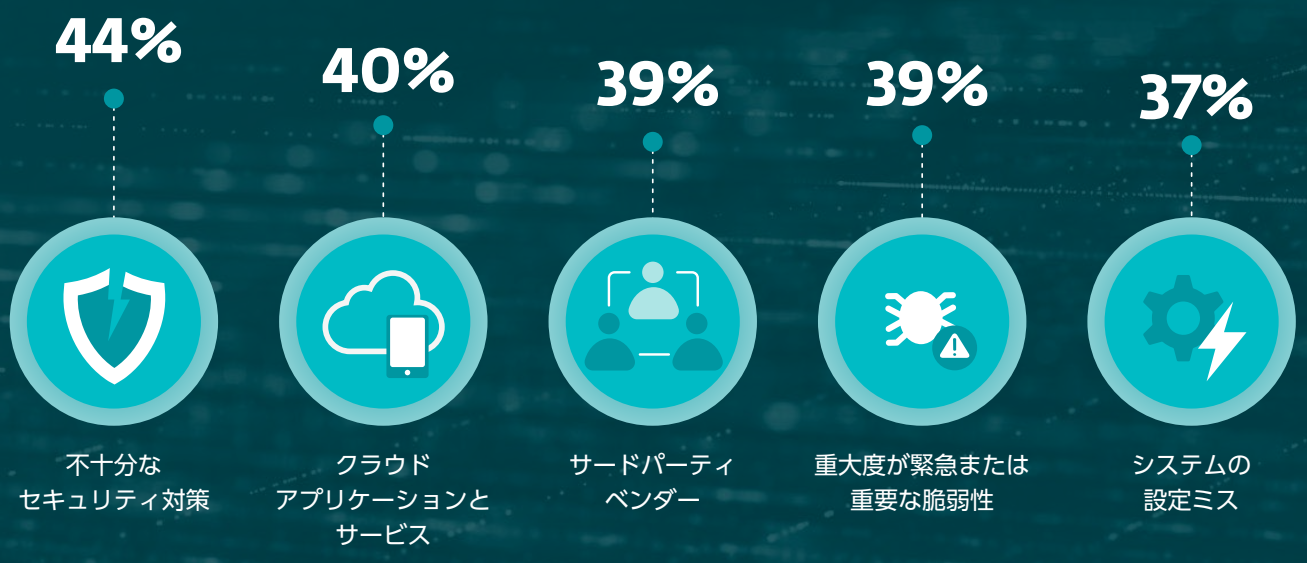


インドは他の国と比較して **Web ベースの攻撃が 42% と大幅に高くなっています**。

シンガポールではビジネスメール詐欺が 34% であり、他国よりも**多く発生しています**。ランサムウェア攻撃はマレーシアが 31%と他国よりも多くなっています。

セキュリティ侵害やインシデントを引き起こす主要な要因

SMB の 44% は十分な防御策を講ずることができていないと述べており、対策の欠如がサイバー攻撃によるセキュリティ侵害やインシデントを引き起こす原因となっています。サードパーティベンダーや、重大度が緊急または重大な脆弱性もリスクを増加させる原因になっています。



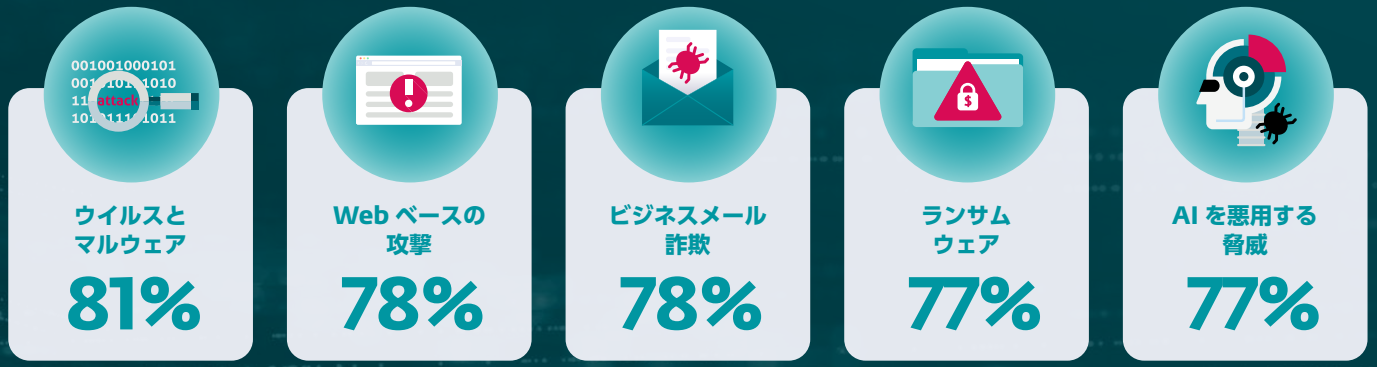
サイバーセキュリティインシデントを引き起こす主な原因

基本知識

SMB で一般的に使用されているクラウドベースのメール、コラボレーション、ストレージアプリケーションも、ランサムウェアなどの脅威の影響を受けることが多くあります。
このようなクラウドアプリケーションに保護機能を適用し、ネットワーク内のサイバー攻撃を防ぐことが極めて重要です。

一般的なサイバーセキュリティの脅威

ウイルスやマルウェア、Web ベースの攻撃、ビジネスメール詐欺、ランサムウェア、サイバー攻撃での AI の悪用が、SMB にとって今後 12 か月間の最大の懸念事項となっています。



APAC で最も懸念されているサイバーセキュリティ脅威トップ 5

基本知識

メールは、マルウェアや有害なスクリプトの配信やフィッシング詐欺に簡単に利用できるため、最も多くの脅威で利用されています。

ビジネスメール詐欺（BEC）の一般的な目的は、標的となったユーザーに正当で承認されている商取引であると信じ込ませ、攻撃者に送金させることです。BEC では通常、なりすましが行われ、被害者がよく知っており正規のように見えるメールアドレスや電話番号が使用されます。

多くの SMB がランサムウェアで要求される身代金の支払いを検討

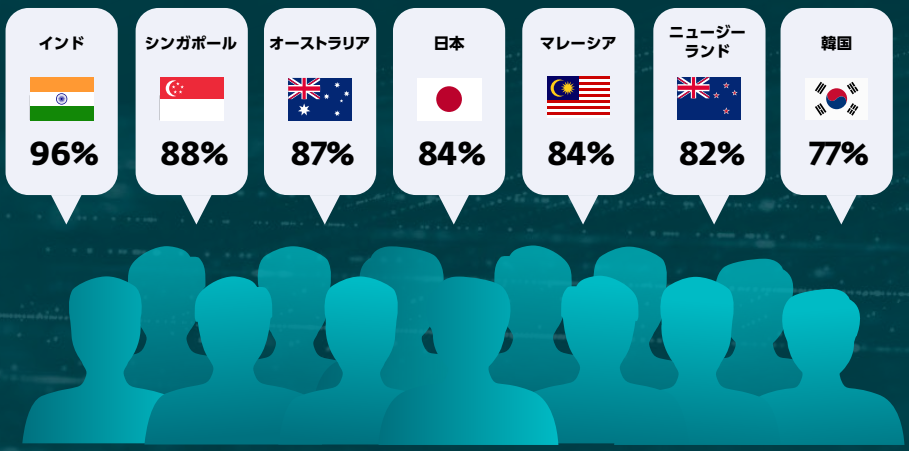
86%

SMB の 86% が、ランサムウェア攻撃の被害にあった場合に、**サイバー犯罪者に身代金を支払うことを検討**します。

被害を受けた企業が復号鍵を受け取れる保証も、窃取されたデータが公開されない保証もないことから、世界の多くの司法機関や警察は身代金を支払うことを推奨していないにもかかわらず、これだけ多くの企業が身代金を支払うことを検討しています。

回答者の 22%は、過去 12 か月間にランサムウェアに関連するサイバーセキュリティインシデントを経験しています。

ランサムウェア攻撃の被害にあった場合、サイバー犯罪者に身代金を支払うことを検討する SMB の割合



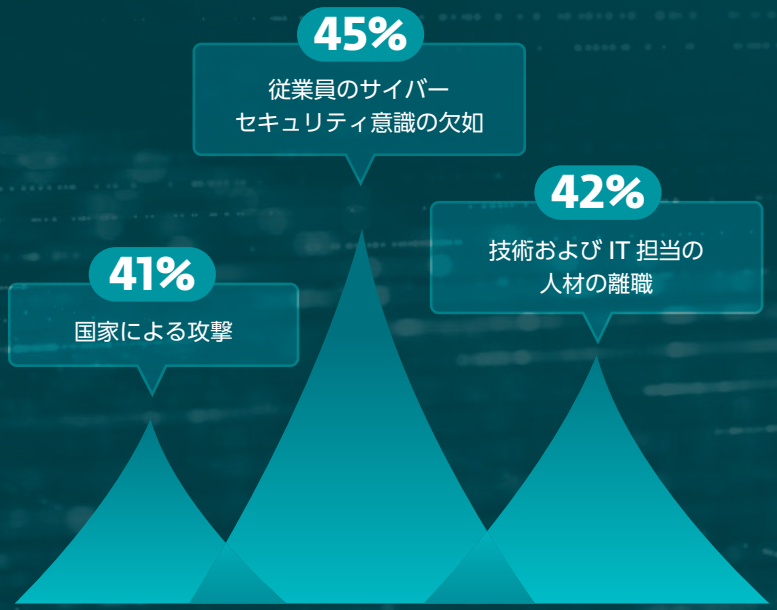
基本知識

最近の報告書によると、ランサムウェア攻撃の被害者は 2023 年に総額で 11 億米ドルが恐喝されています [1]。ランサムウェアは、他のサイバー犯罪グループにサービスとしてランサムウェア（RaaS）を提供するほど儲かるビジネスモデルとなっており、ランサムウェア攻撃の増加にさらに拍車をかけています。

[1] 出典：*https://www.businesstimes.com.sg/companies-markets/banking-finance/crypto-ransom-attack-payments-hit-record-us1-billion-2023*

SMB はサイバーセキュリティの意識向上に優先的に取り組む必要がある

従業員のサイバーセキュリティ意識の欠如は、調査の回答者が今後 1 年間にサイバー攻撃のリスクに影響を与えると考える要因の上位に挙げられています。



サイバー攻撃のリスクに影響する要因トップ 3

リスクが存在する領域の多様化

今後１年間にサイバーセキュリティに最も影響を与える要因（国別の回答者の割合）

サイバー攻撃のリスクに影響する重要な要因

	全体	日本	オーストラリア	インド	シンガポール	マレーシア	韓国	ニュージーランド
従業員のサイバーセキュリティ意識の欠如	**45%**	34%	50%	50%	49%	51%	37%	44%
IT 担当の人材の離職	**42%**	35%	36%	45%	46%	44%	38%	50%
国家による攻撃	**41%**	41%	39%	50%	40%	46%	35%	41%
サプライヤーエコシステムにおける脆弱性	**39%**	36%	39%	39%	36%	49%	26%	46%
従業員が使用するアプリケーションの増加	**38%**	35%	38%	44%	48%	41%	30%	38%
リモートデスクトッププロトコルの使用	**36%**	33%	35%	41%	43%	36%	31%	35%
生成 AI	**36%**	28%	33%	40%	43%	44%	28%	38%
クラウド型の生産性向上ソフトウェアの利用拡大	**35%**	32%	37%	38%	36%	34%	29%	37%
ハイブリッド勤務や在宅勤務の継続	**34%**	34%	35%	39%	33%	34%	23%	41%

SMB のサイバーセキュリティの最大の課題

回答者は、全体的に見ると、**サイバーセキュリティの専門チームの不足、アラート疲れ、最新の脅威に対応する能力**を上位 3 つの課題として挙げています。

詳しく見てみると、サイバーセキュリティ専門のチームの不足（27%）とアラート疲れ（26%）が、上位 2 つの課題となっており、他の課題を大きく引き離しています。

日本、オーストラリア、マレーシア、韓国、ニュージーランドでは、サイバーセキュリティの専門チームの不足が最大の課題となっています。一方で、インドとシンガポールの SMB はアラート疲れを最大の課題に挙げています。

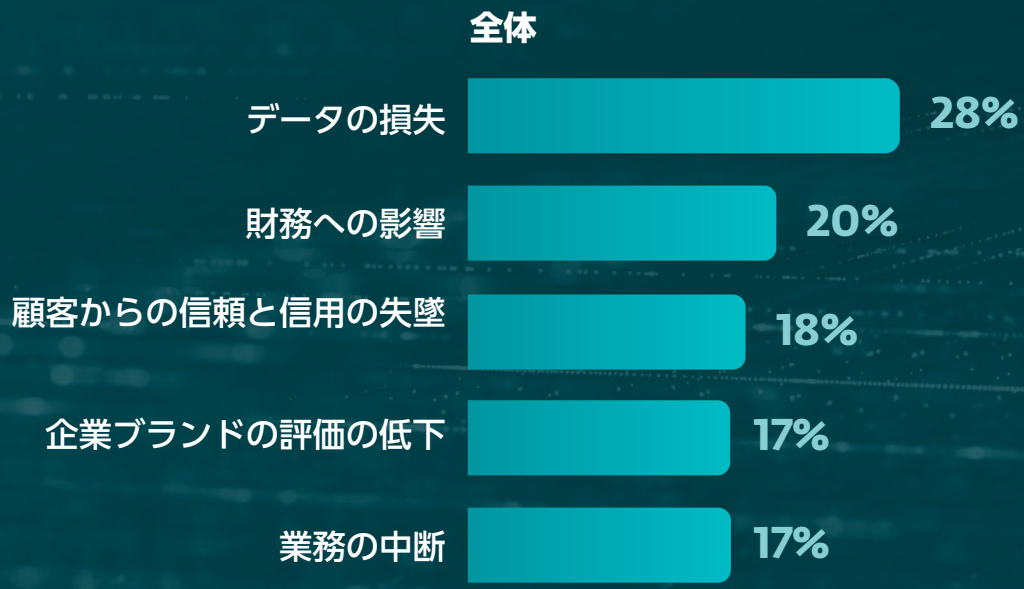
SMB が直面しているサイバーセキュリティの最大の課題

	全体	日本	オーストラリア	インド	シンガポール	マレーシア	韓国	ニュージーランド
サイバーセキュリティの専門チームの不足	27%	30%	29%	23%	23%	25%	32%	29%
アラート疲れ	26%	26%	26%	36%	31%	24%	23%	20%
最新の脅威に対応する能力	14%	8%	13%	15%	16%	17%	13%	17%
IT チームのスタッフ不足や負担の増大	14%	14%	13%	9%	17%	13%	17%	15%
経営幹部からの協力が得られない	8%	12%	12%	7%	5%	8%	7%	8%
最新テクノロジーの導入と管理	7%	7%	6%	10%	5%	8%	6%	10%
予算の制約	3%	4%	3%	2%	5%	7%	4%	2%

基本知識

誤検知が多い、あるいは、セキュリティソリューションの設定が不十分である場合、膨大な数のセキュリティアラートが発生し、IT 管理者はそれらの確認と対応に追われ、負担が増大します。その結果、業務に対して散漫になり、本当の脅威を見逃す恐れがあります。

サイバー犯罪者の成功＝SMB の損失



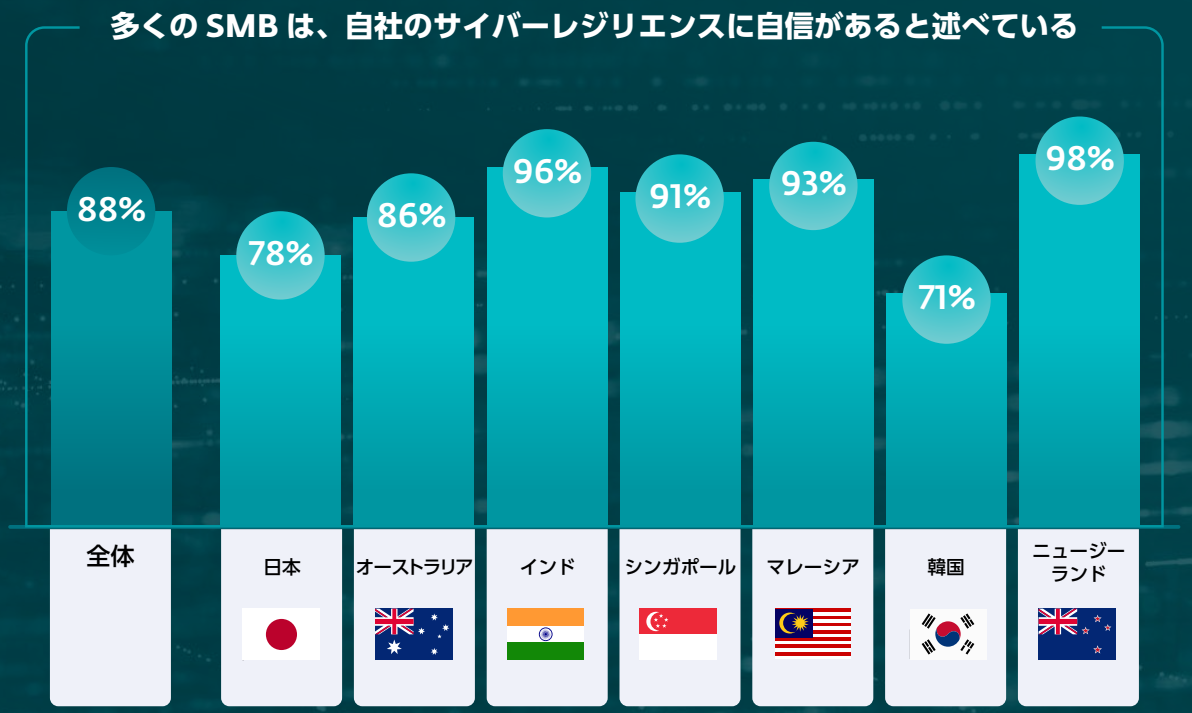
サイバー攻撃が成功した場合に
SMB が最も懸念するビジネスへの影響

今後のサイバーセキュリティ対策について自信を持っている企業は多い。しかし、その自信は本物か?

中小企業の **10 社中 9 社が今後 12 か月間の自社のサイバーレジリエンス（サイバー攻撃への防御体制）に自信を持っている**と述べています。一方で、インド、マレーシア、ニュージーランドの回答者の 44% が、サイバーセキュリティインシデントの影響を受けた主な要因にセキュリティ対策不足を挙げています。

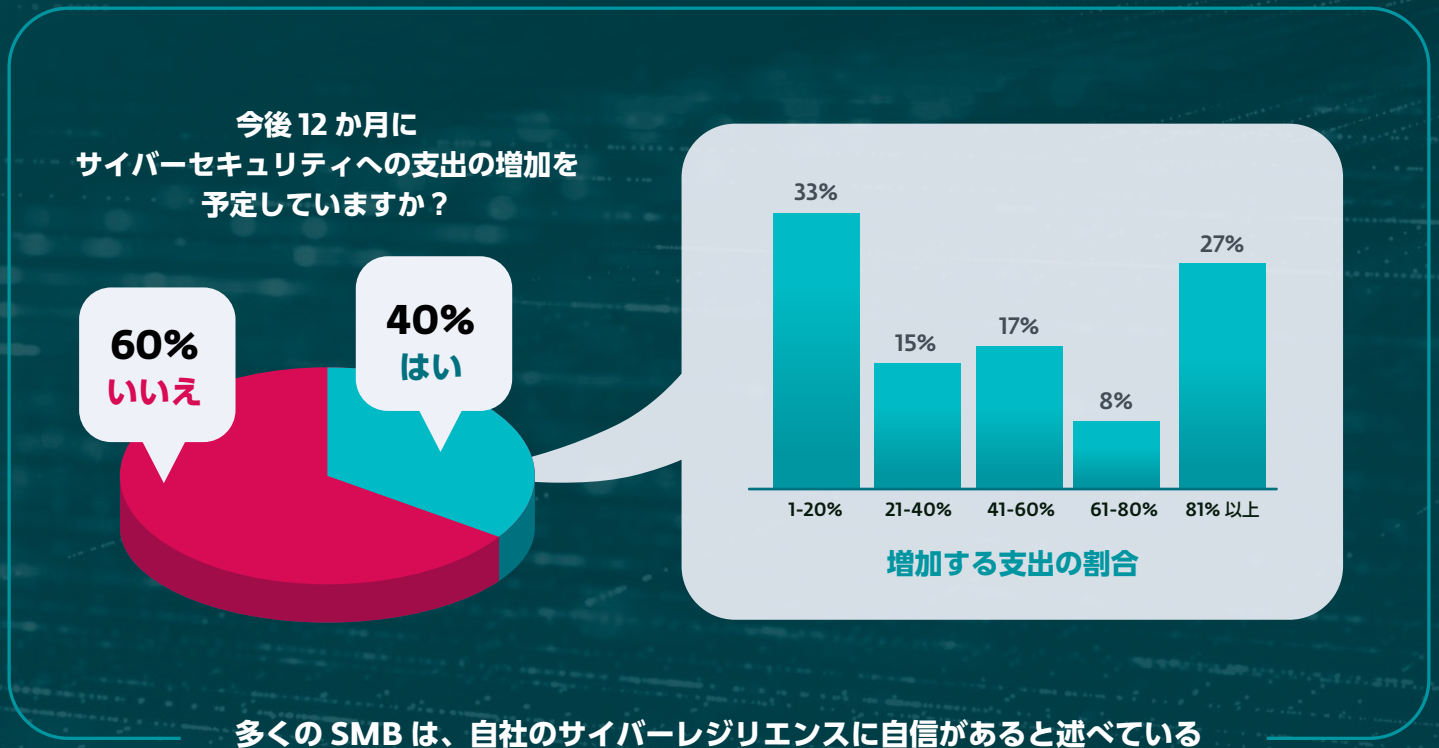
82%

大規模企業と比較して SMB はサイバー攻撃に対してより脆弱であると考えている回答者の割合



SMB はサイバーセキュリティへの支出を増加している

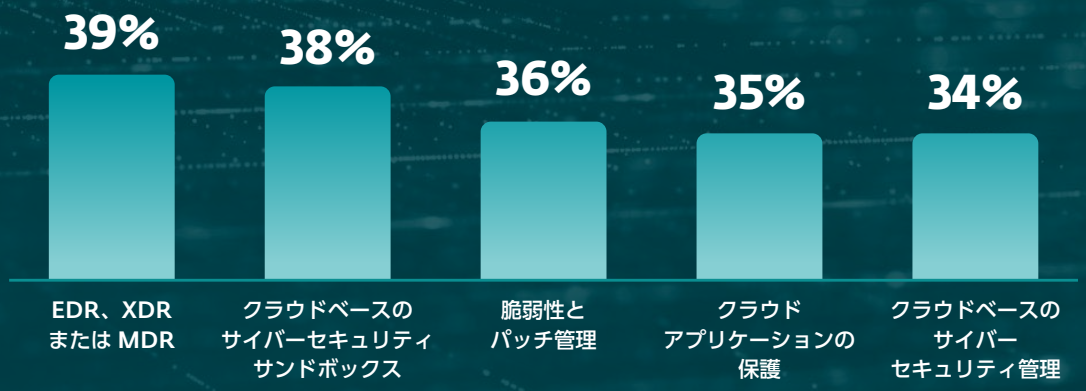
レジリエンスと保護対策を強化するため、回答者の **10 社の 4 社が今後 1 年間にサイバーセキュリティへの支出を増やすことを計画**しており、これらの回答者の 35% 以上が支出を大幅に増加（60% 以上）させると述べています。



多くの SMB は、自社のサイバーレジリエンスに自信があると述べている

サイバーレジリエンスを向上させるために、SMB が導入している保護機能

SMB は、EDR/XDR/MDR、クラウドベースのサイバーセキュリティ管理、脆弱性とパッチの管理、クラウドベースのサンドボックスなど、これまで使用していないソリューションを取り入れてサイバーレジリエンスを向上しています。



基本知識

クラウドベースのサイバーセキュリティサンドボックスは、過去に検出や分析されたことのない未知のランサムウェアなどの脅威を分析できる重要なツールの1つです。

隔離された強力なテスト環境で不審なプログラムを実行し、そのプログラムの挙動を数分以内に自動化された方法で観察、分析、報告できます。

SMB は、インシデント発生後に利用するサイバーセキュリティ機能を多く取り入れているが、ベストプラクティスは予防ファーストの戦略である

調査対象となった SMB の半数以上が、サイバー攻撃によるセキュリティ侵害やインシデントの発生後に、サイバーセキュリティ体制を強化するためリスク監査を実施し、サイバーセキュリティトレーニングの強化に投資しています。

	全体	日本	オーストラリア	インド	シンガポール	マレーシア	韓国	ニュージーランド
サイバーセキュリティリスク監査の実施	51%	37%	43%	55%	56%	52%	54%	55%
サイバーセキュリティトレーニングの強化への投資	50%	41%	47%	57%	51%	59%	42%	50%
新しいサイバーセキュリティツールへの投資	49%	40%	44%	57%	51%	58%	42%	49%

効果的なサイバーセキュリティ戦略によってデータ侵害を防止する

SMB は、限られたリソースの中で、少ない労力で多くの成果を達成しなければなりません。そのため、予防を重視するセキュリティ機能への投資を優先し、脅威が深刻な問題に発展する前にサイバーリスクを効果的に軽減することが極めて重要です。

人工知能（AI）、アナリストの専門知識、クラウドベースのサンドボックスを取り入れた**多層防御型のエンドポイントセキュリティソフトウェアを活用**すれば、ランサムウェアだけでなく、過去に検出されていない新たな脅威などの高度な脅威からも自社を防御できます。

データ漏洩を防止するため、すべてのエンドポイントが暗号化されていることを確認します。パスワードでデバイスをロックするだけでは不十分です。犯罪者はハードディスクを取り外してデータにアクセスすることができます。

多要素認証（MFA）を導入して、定期的にパスワードを更新します。データ漏洩の一般的な原因は、ユーザー名とパスワードの窃取です。

脆弱性とパッチ管理ソリューションを使用して、ソフトウェア脆弱性のパッチを速やかに適用します。アップデートが適用されていないソフトウェアやオペレーティングシステムは、サイバー犯罪者に簡単に攻撃されます。このような脆弱性が攻撃されると、マルウェアへの感染、デバイスの乗っ取り、またデータの窃取が行われる恐れがあります。

従業員へサイバーセキュリティトレーニングを提供します。各従業員がフィッシングを見分け、オンライン詐欺を避けなければなりません。インターネットを利用するときのベストプラクティスを従業員に遵守させることは、セキュリティ侵害を防ぐ極めて重要な保護層になります。

本調査について

調査対象国

日本　オーストラリア　インド　シンガポール

マレーシア　韓国　ニュージーランド

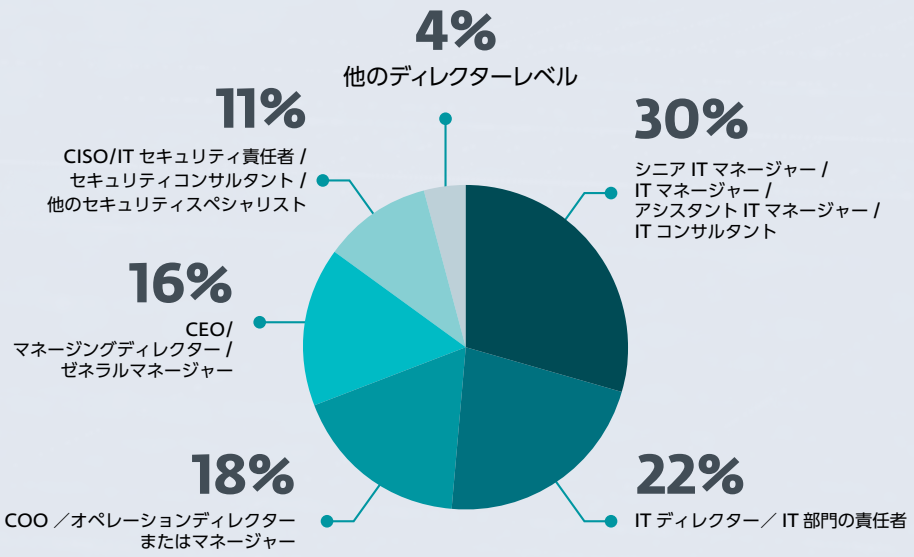
調査規模

合計 1,400 人の回答者

回答者のプロフィール：

従業員数 25 ～ 200 名のさまざまな業界の組織の IT 意思決定者。

回答者の役職：



本調査は、Blackbox Research の協力のもとで行われました。

ESET は、SMB がコンプライアンス要件を満たすことができるように支援します

SMB は、限られたリソースの中で、少ない労力で多くの成果を達成しなければなりません。そのため、予防を重視するセキュリティ機能への投資を優先し、脅威が深刻な問題に発展する前にサイバーリスクを効果的に軽減することが極めて重要です。

規制 / 標準	アンチウィルスおよびマルウェア対策の保護機能	暗号化	多要素認証	一元管理	メールセキュリティ	脆弱性診断	ソフトウェアパッチの管理	バックアップ *
Essential Eight のレベル 1（オーストラリア）	✓	✓	✓	✓	✓	✓	✓	✓
Cyber Essentials（シンガポール）	✓	✓	✓	✓	✓	✓	✓	✓
SMB 向けの NIST CFS 2.0（米国）	✓	✓	✓	✓	✓	✓	✓	✓
EU 一般データ保護規則（EU）	✓	✓	✓	✓	✓	✓	✓	✓

*ESET のテクノロジーアライアンスパートナーから提供

✓ 必須　✓ 推奨　✓ 不要

ESET PROTECT Advanced

イーセットプロテクトアドバンスト

ランサムウェア攻撃からエンドポイントとデータを保護

ESET PROTECT Advanced は、ランサムウェアやゼロデイ脅威に対するクラス最高のエンドポイント保護製品です。クラウド型やオンプレミス型のセキュリティ管理ツール、サーバーのセキュリティ対策、高度な脅威に対抗する防御機能、フルディスク暗号化を実装するクロスプラットフォームソリューションです。

★★★★★

**「ESET 製品は堅牢で高い効果を発揮します。
カスタマーサービスと製品サポートも優れています。」**

Arun DeSouza 氏、CISO 兼 CPO、Nexteer Automotive Corporation

ESET PROTECT Advanced に搭載されるモジュール

統合プラットフォーム

サーバーセキュリティ

最新のエンドポイント保護機能

モバイル脅威の防御

組織のすべての Android および iOS モバイルデバイスに堅牢なセキュリティ機能を提供します。マルウェア対策、データ窃取対策、MDM 機能によって企業が提供しているモバイルデバイスのセキュリティを向上します。

- モバイルの脅威からの保護
- ラテラルムーブメントの防止
- スマートフォンやタブレットなどのデバイスにある企業データの保護
- 不要なアプリのブロック
- iOS および iPad OS 対応の MDM

高度な脅威への対応

標的型攻撃や、ランサムウェアなどの過去に検出されていない新しい脅威に対して、クラウドベースのプロアクティブな防御機能を、自律的な修復機能と合わせて提供します。

- 高度な解読およびスキャン
- 最先端の機械学習
- クラウドベースのサンドボックス
- 詳細な振る舞い分析
- 自動および手動のファイル提出
- 比類のない分析速度

フルディスク暗号化

接続されている Windows と Mac エンドポイントにワンクリックで導入し、データを暗号化します。自社のデータセキュリティを大幅に向上させ、データ保護規制の要件を満たすことが可能です。

- Windows および macOS マシンの暗号化を管理
- システムディスク、パーティション、またはドライブ全体を暗号化
- 一回の操作で展開および有効化して、デバイスを暗号化

新たな脅威に対する AI ネイティブの予防策

予防ファーストのアプローチによって新たな脅威に対抗

ESET独自のテクノロジー「ESET LiveSense」は、いくつもの保護レイヤーを実装しています。ESET LiveSenseは、ESET LiveGridと連携して機能します。ESET LiveGridは、クラウド型の脅威ハンティングテクノロジーであり、膨大な数の不審な検体を収集して分析しています。ESET のセキュリティソリューションは、AI とアナリストの専門知識を組み合わせることで、進化し続けるサイバー脅威から企業をリアルタイムで保護します。

ESET LiveGrid®

ランサムウェアなどのゼロデイの脅威を発見すると、ファイルは ESET のクラウドベースマルウェアプロテクションシステムである ESET LiveGrid® に送信され、ファイルを実行したときの振る舞いが監視されます。このシステムによる分析結果は、ユーザーが更新しなくても、数分以内に全世界のすべてのエンドポイントに取り込まれます。

人工知能

ニューラルネットワークと厳選したアルゴリズムの力を結集し、受信した検体を「正規」、「潜在的に望ましくないもの」、「悪意があるもの」として正しくラベル付けします。最高の検出率と誤検出を最小化するため、ESET の機械学習エンジンである ESET Augur は、DNA、サンドボックス、メモリ分析などの他の保護テクノロジーと連携し、振る舞いの特徴を抽出するように高度な調整が行われています。

アナリストの専門知識

テクノロジーですべてを解決できるわけではありません。ESETは、教育とトレーニングを受け高度な知識と経験を有する優れた人材を確保できるよう、人材に多額の投資を行っています。世界最高クラスのセキュリティ研究者が知識を共有し、24 時間体制で最高のグローバル脅威インテリジェンスを提供します。

ESET について

プロアクティブな防御と予防重視のアプローチでリスクを最小限に抑える

AI と人間の専門知識の両方を活用した予防ファーストのアプローチで、既知および未知のサイバー脅威の一歩先を行くことが可能になります。業界最高クラスの ESET の保護機能をぜひ体験してください。ESET のグローバルな脅威インテリジェンスは、業界で高く評価されている研究者が率いる広範な研究開発ネットワークから生まれ、30 年以上にわたって磨き上げられています。

ESET はお客様のビジネスを保護し、テクノロジーの可能性を最大限に引き出します。

ESET の顧客

MITSUBISHI MOTORS
Drive your Ambition

2017 年から 9,000 台以上の
エンドポイントを保護

Allianz Suisse

2016 年から 4,000 以上の
メールボックスを保護

Canon
Canon Marketing Japan Group

2016 年から 32,000 台以上の
エンドポイントを保護

2008 年から
ISP セキュリティパートナーとなり、
200 万の顧客基盤を保護

セキュリティ認定

ISO セキュリティ認定

ESET は、情報セキュリティの実践・管理において国際的に認められているセキュリティ標準である ISO/IEC 27001:2013 を取得しています。

OPSWAT 認定

ESET は、エンドポイントセキュリティアプリケーションで Platinum OPSWAT アクセスコントロール認定を取得しています。

Cybersecurity Made In Europe

ESET は、欧州サイバーセキュリティ機構（ECSO）から「Cybersecurity Made In Europe」認定を最初に受けた IT セキュリティ企業の 1 社です。

数値で見る ESET

10 億人以上
保護している
インターネットユーザー

40 万社以上
法人顧客

195
国と地域

13
世界各国にある
研究開発拠点

Digital Security
Progress. Protected.

詳細については、https://www.eset.com/jp/ をご覧ください。