中小企業のための サイバーセキュリティ

マカフィーのリソース ガイド

目次

お客様のビジネスは準備できていますか？中小企業のためのサイバーセキュリティ ガイド

ニュース報道でサイバー犯罪は、目立つランサムウェアやデータ侵害攻撃の標的となる大企業の懸念事項として描かれることが多いものです。しかし、実際にこの脅威は**中小企業**の世界にも存在します。

「既製品」のハッキング ツールが入手しやすくなり、悪意ある個人の参入障壁が低くなったため、サイバー犯罪者は、年間売上高が50万ドル以下の企業に対して攻撃を仕掛けるケースが増えています。

大企業にとって、サイバー犯罪はビジネスを行う上でのコストとして織り込まれている場合が多いのです。しかし、**中小企業**の経営者にとっては、強固なサイバーセキュリティが乏しく、脆弱なまま放置されているため、こうした攻撃は壊滅的な打撃を与えかねません。平均して、通常、標的型フィッシングやその他のアカウント ハッキングによって行われるビジネス メール攻撃は、125,611 ドルの資金を吸い上げます。ランサムウェア攻撃者は平均 14,403 ドルで企業データを人質に取り、データ侵害は平均 164,336 ドルの損失を企業に与えています。

700 名の企業経営者と IT 専門家を対象としたグローバル調査に基づき、McAfee は、**中小企業**（従業員数 100 名未満の組織）のプロフェッショナルにこの増えつつある脅威を伝え、従業員、顧客、ビジネスの安全を守るためのツールを提供するべく、このガイドを作成しました。

サイバー犯罪者の脅威が高まり、中小企業は懸念しています

サイバー犯罪によってハッキングされ、業務に支障をきたしたり、顧客からの信頼を失ったりする脅威は、**中小企業経営者**の心に重くのしかかっています。

サイバーセキュリティは、調査対象となった組織の73%が最大のリスクまたは脆弱性の1つとして挙げており、調査対象となった企業経営者およびIT専門家の24%が、サイバー攻撃について日々心配していると回答しています。

こういった懸念ももっともなことなのです。データによると、調査対象となった**中小企業**の 44% がサイバー攻撃を経験しており、17% はサイバー攻撃を複数回経験しています。サイバー攻撃を経験した組織の 67% において、その攻撃は過去 2 年間に発生しており、サイバー犯罪の脅威がより拡大していることを示しています。

中小企業にとっては、たった一度のサイバー インシデントでさえ、壊滅的な打撃を与えかねません。サイバー攻撃を受けた小規模企業の 61% が、攻撃への対応で 1 万ドル以上を失っています。調査対象となった企業経営者や IT 専門家の多く (60%) は、事業に対するサイバー攻撃によって、自分自身やスタッフ、同僚が身体的・精神的な打撃を受けたと回答しています。58% のケースで、企業は攻撃で発生した IT 問題に対処することに、貴重なビジネス時間を 1 週間以上失っています。

データが中小企業を標的に

- 中小企業の関係性が増えデジタル化が進むにつれ、ハッカーにとって魅力的なデータが蓄積されていきます。
- 調査対象となった企業経営者 /IT 専門家のほぼ半数 (46%) が、データの紛失を最大の懸念事項として挙げています。
- サイバー攻撃を受けた企業では、ほとんどの場合、顧客データ (38%)、パスワード (34%)、その他のファイル (34%) を失いました。

中小企業経営者は、サイバー犯罪の脅威について知識があると感じています…

ほとんどの企業経営者は、サイバー犯罪が業務にもたらすリスクを理解しています。当社の調査によると、調査対象となった企業経営者や IT 専門家の 69% が、自身のビジネスにおけるサイバーセキュリティの決断を下す上で十分な知識があると感じています。

一般的に、調査対象となった中小企業の 84% は現在、何らかのオンライン セキュリティ対策を実施しており、60% はサイバー攻撃が発生した場合の行動計画を立てていると回答していることから、サイバー脅威に対する計画が必要で、数を減らすには投資が必要だと皆理解しています。

… しかし、多くの企業は、複雑化し、頻度を増すこういった脅威に対処するためのリソースが不足しています

企業経営者は、サイバーセキュリティが問題であることを知ってはいても、この増大する脅威に対応するためのスタッフやリソースを持ち合わせていないことが多いのです。

広く認識されているにもかかわらず、企業経営者 /IT 専門家の約半数 (48%) しか、サイバー攻撃を防ぐ自社の能力に十分な自信を持っていません。ほとんどの中小企業 (76%) は、社外の第三者の助けを借りずにサイバーセキュリティを管理しています。

- 17% では、主な業務は異なっても、デバイスや IT 関連の管理も行う従業員を抱えています。
- 調査対象となった小規模企業のうち、サイバーセキュリティ製品の購入や導入を指導するために外部コンサルタントを雇っているのはわずか 8% に過ぎません。

他の業務に加え、サイバーセキュリティを自身で処理する経営者が多すぎるのです。これはサイバーセキュリティだけではありません：調査対象となった企業経営者の 45% が、IT 全般の問題に週 7 時間以上取り組んでいると回答しています。

ハッカーの侵入経路

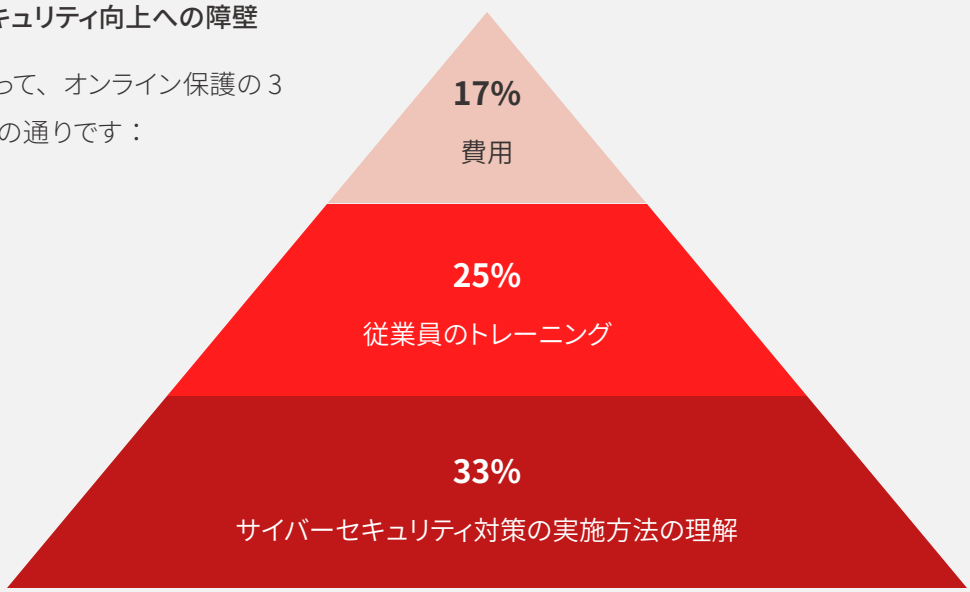
サイバー犯罪者が**中小企業**を妨害する方法はたくさんありますが、特に好む傾向がある方法がいくつかあります。警戒を怠らず、この種の攻撃とその防止策について従業員を教育することで、企業経営者の時間とコストを節約することができます。

当社の調査によると、ほとんどの攻撃(43%は、従業員が誤ってフィッシングリンクをクリックしたり、悪意のある添付ファイルを開いたりし、マルウェアをダウンロードしたことが原因でした。これらのケースの36%では、ログイン認証情報がフィッシングサイトに誤って入力されたこと、そして35%の攻撃は、ユーザーアカウントでハッキングされた弱いパスワードが原因でした。

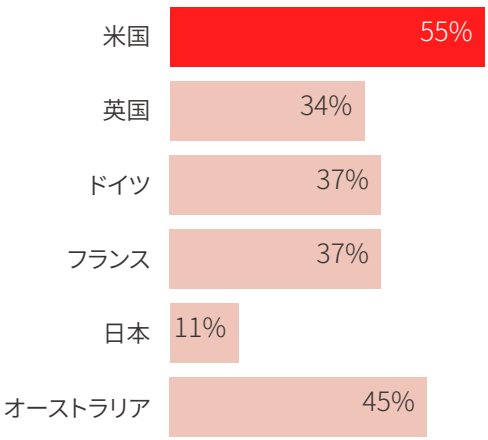
また、企業へのサイバー攻撃を防ぐだけではありません。時には企業名や知名度が犯罪者のツールとして利用されることもあります。調査回答者の17%が、自社の企業情報が他者を標的にしたフィッシング攻撃に利用されたと回答しました。

オンライン セキュリティ向上への障壁

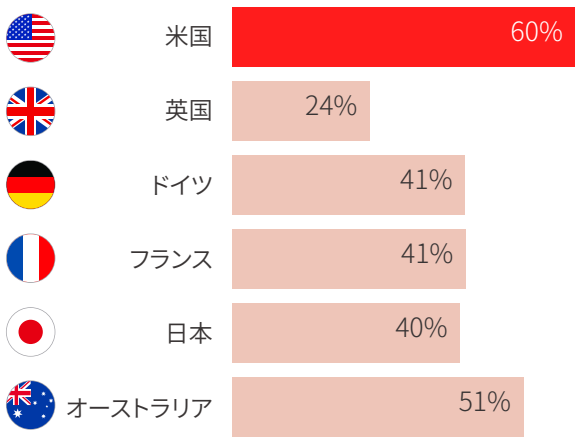
中小企業にとって、オンライン保護の 3 大障壁は以下の通りです：



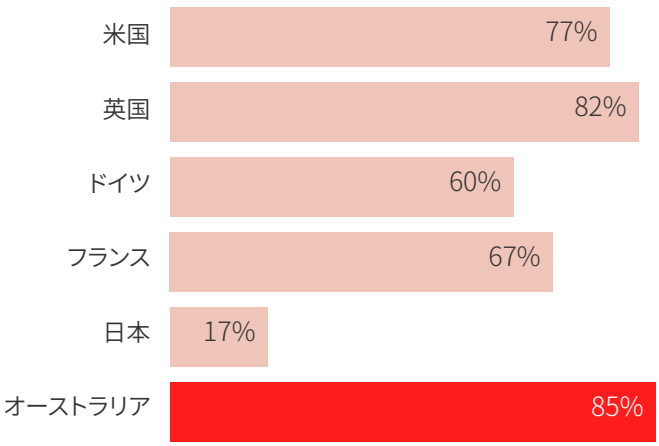
サイバーセキュリティへの AI 導入率が最も高いのは米国の中小企業…



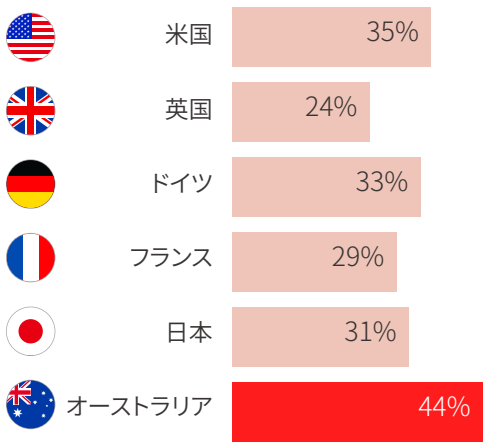
… しかし、AI の普及に伴うサイバーセキュリティを最も懸念している。



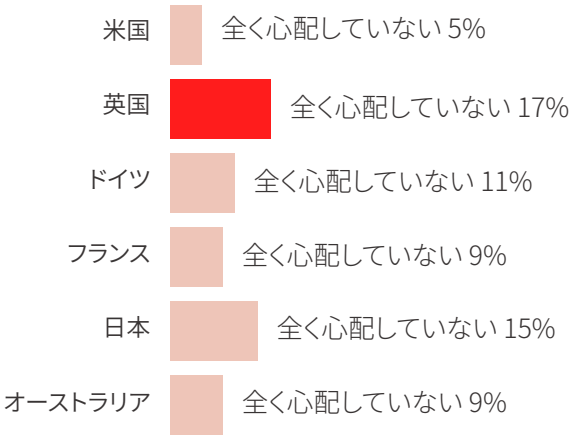
従業員が詐欺の見破り方を知っていると最も自信を持っているのは、オーストラリアの中小企業…



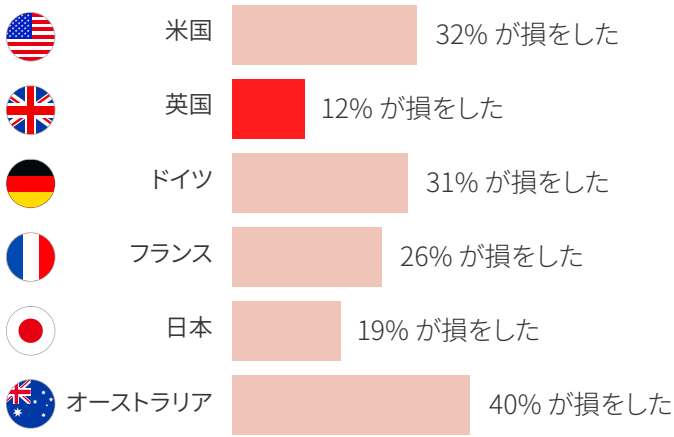
… にもかかわらず、オンライン保護における最大の障壁は、サイバーセキュリティ対策の実施方法を理解することであると回答する割合が高い。



サイバー攻撃を最も懸念していないのは英国の中小企業…



… そして、ハッキングで損をする可能性が最も低い。



サイバー犯罪を防ぐには準備が鍵

効果的なサイバーセキュリティの鍵は、準備することです。攻撃を未然に防ぐことは、その余波に対処するよりもはるかに簡単で、ビジネスにとってコストもかかりません。ここでいくつか紹介するのは、中小企業向けの優れたサイバーセキュリティ対策に重要な要素です：

#1：従業員のトレーニング

当社が調査した中小企業のうち、72%　が従業員にサイバーセキュリティ　トレーニングを実施しています。しかし、従業員や同僚がデバイスや　IP　を保護するために、必要な手順を取る能力に自身を持つ企業経営者や　IT　専門家は半数以下 (46%) しかいません。

サイバーセキュリティトレーニングは、オンボーディング時のビデオ以上の内容であるべきです。従業員一人ひとりが、攻撃を防ぐために何ができるのか、攻撃が起こった場合の企業の計画、データセキュリティや報告などの面でどのような責任があるのかを知っておく必要があります。

#2：リスク アセスメントの実施

リスクアセスメントを実施することで、脆弱性を特定し、ビジネスが大規模な攻撃のリスクにさらされていないことを確認し、政府の規則や規制へのコンプライアンスを確保することができます。

#3：ウイルス対策ソフトウェアの導入

ウイルス対策ソフトウェアは、ウイルス、スパイウェア、ランサムウェアやフィッシング詐欺など、さまざまな脅威からデバイスを保護します。優れたソフトウェアは、デバイスをクリーンアップ、リセットするツールだけでなく、最初からデバイスを保護するツールも提供しています。

#4：ソフトウェアの更新

より有害なマルウェア攻撃の多くは、オペレーティング システム、ブラウザ、その他中小企業が使用する主要なプログラムなど、一般的なアプリケーションのソフトウェアの脆弱性を悪用しています。

実際、サイバー攻撃を経験した中小企業の 30% が、古いソフトウェアや、パッチが適用されていないソフトウェアの脆弱性が侵害されたために攻撃が発生したと報告しています。

ソフトウェアの更新には、セキュリティホールに対する重要なパッチが含まれていることが多く、保護を提供する上で最も優れ、最も簡単な対策法の1つとなっています。

#5：定期的なファイルのバックアップ

サイバー攻撃はしばしばデータ障害を引き起こします。そのため、ファイルを定期的にバックアップし、必要に応じてデータを取り出せるようにすることが不可欠となります。

#6：重要情報の暗号化

暗号化によって、Webサイト所有者のような技術提供者は、クレジットカード番号、パスワード、その他の財務情報などの機密情報を、サイバー犯罪者に読み取られないコードに変換することができます。マカフィー ®ビジネスプロテクション™には、銀行レベルのWi-Fi暗号化により、データのプライバシーと安全性を維持する安全なVPNが含まれています。

#7：機密データへのアクセスの制限

サイバー攻撃は必ずしもハイテクとは限りません。ハッカーは多くの場合ソーシャルエンジニアリングによってデータにアクセスします。サイバーセキュリティ計画を作成する際、企業は人的要素も考慮する必要があります。

重要なデータにアクセスできる人数が減れば、企業はデータ漏洩の影響を最小限に抑え、疑いを抱くことのない従業員にデータへのアクセス権限を与えてしまう可能性を減らすことができます。どの個人がさまざまなレベルの情報にアクセスできるかをまとめた計画を作成することで、役割と責任を明確にすることができます。

#8：Wi-Fi 接続の保護

無線ネットワークは電波を使ってデータを送信するので、サイバー攻撃に対して特に脆弱なため、Wi-Fi 接続を保護することが、データ保護の上で必須なのです。

マカフィーの Wi-Fi スキャンは、安全でない Wi-Fi ネットワークに接続しようとすると自動的にスキャンして警告を表示するので、VPN をオンにするか、別のネットワークを選択することができます。機密データを共有する前に、接続が安全であることを確認してください。

#9：強固なパスワードポリシーの徹底

アカウントをハッキングから効果的に守るには、作成するアカウントごとに強力なパスワードを設定することが重要です。

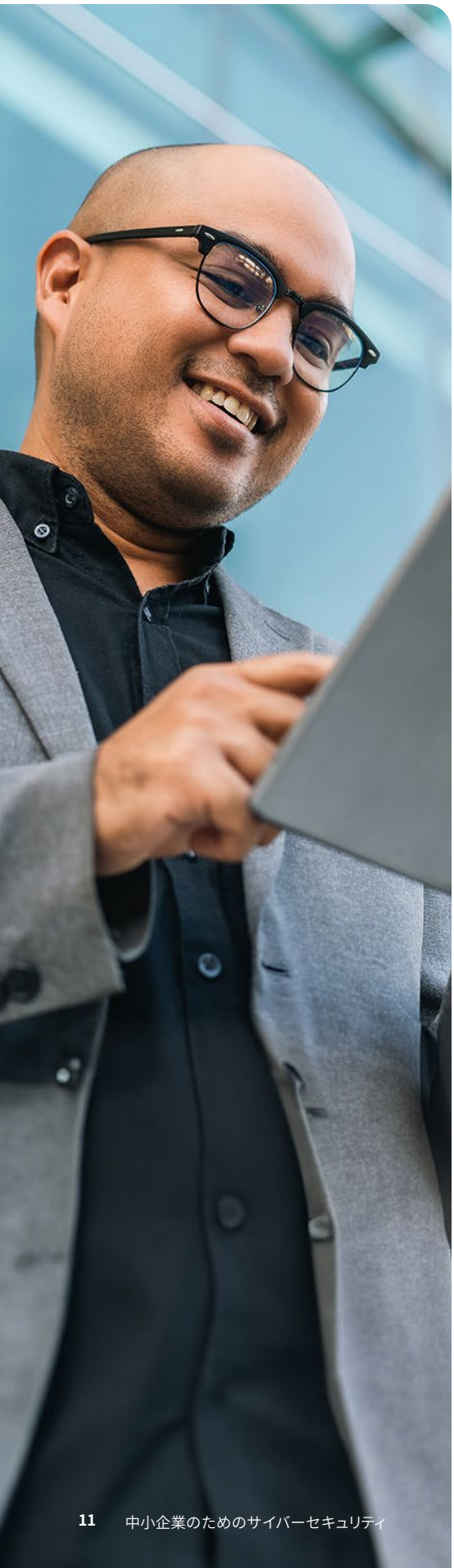
強力なパスワードは、少なくとも 7 ～ 8 文字の長さで、数字、記号、大文字と小文字の両方を組み合わせて使用する必要があります。その他の重要な対策として、パスワードを毎日変更すること、アカウントごとに異なるパスワードを使用すること、そしてパスワードを決して書き留めないことが挙げられます。

マカフィー ビジネスプロテクションには、社内のデバイスがパスワードで保護されていない場合にアラートを送信する「パスワード保護ステータス」が含まれます。

#10：パスワード マネージャーの使用

各デバイスやアカウントごとに強力な一意のパスワードを作成すると、それぞれのパスワードを覚えておくのが難しくなります。パスワード マネージャーはパスワードを保存し、アカウントごとに正しいユーザー名とパスワードを自動的に生成します。

マカフィー ® True Key は、長くて強力な一意のパスワードを作成するように設計されており、ローカル データの暗号化、様々なブラウザのサポート、Windows、Mac、iOS、Android デバイス間での同期機能や様々なサインイン方法を備えています。



#11：ファイアウォールの使用

ファイアウォールは、ハードウェアとソフトウェアの両方を保護し、ネットワークへのウイルスの侵入を防止または阻止することができます。ファイアウォールを導入すれば、事業のネットワーク トラフィックを保護し、特定の Web サイトをブロックすることでハッカーによるネットワーク攻撃を阻止することができます。

#12：仮想プライベート ネットワーク (VPN) の使用

VPN はデータがインターネットを通過する際、他のユーザーによるデータの読み取りを阻止することで、データを保護します。デバイスの IP アドレスを別の IP アドレスに置き換えることで、VPN はお客様の現在地を隠し、さらにプライバシーを守ります。VPN の暗号化はまた、ネットワーク トラフィックも匿名化するため、顧客の行動をターゲットにした広告やユーザーの行動に基づいて広告を配信する広告主は、従来の方法で閲覧パターンや検索パターンを特定できなくなります。

#13：物理的な盗難から身を守る

ハードウェアを保護することは、ソフトウェアを保護することと同様に極めて重要です。権限のない個人がデバイスにアクセスできないようにすること、物理的にデバイスを保護すること、紛失したデバイスを復元するためのトラッカーを追加することなどが、盗難に備えるために企業経営者が取ることのできる手順です。また、リモート ワイプ機能を設定することで、紛失や盗難にあったデバイスのデータを保護することもできます。

#14：モバイル デバイスを見落とさないこと

モバイル デバイスがビジネス目的で使用される機会が増えているため、サイバーセキュリティ計画ではモバイル デバイスを考慮することが不可欠です。従業員にモバイル デバイスのパスワード保護、セキュリティ アプリのインストールやデータの暗号化を求めることが、モバイル デバイスが公共ネットワーク上にある間に犯罪者が情報を盗むのを防ぐ上で、重要です。

#15：協働する第三者も安全であることを確認すること。

システムにアクセスする必要があるビジネス パートナーやサプライヤーと協働する場合、アクセス権を共有する前に、強力なサイバーセキュリティ慣習に従っていることを確認します。

マカフィー ビジネスプロテクションのご紹介

サイバー犯罪が**中小企業**を標的にするケースが増えています。しかし、適切なツールとサポートがあれば、企業経営者は業務を安全に保ち、従業員と顧客を保護することができます。

マカフィー ® ビジネスプロテクション™ を Dell の**中小企業**のお客様専用のソリューションとして提供できることを嬉しく思います。マカフィー ビジネスプロテクションは、**中小企業**を念頭に置いて構築されています。ビジネスを、ハッカー、マルウェア、ウイルスなどから 1 つのソリューションで保護します。

オールインワン：データ、デバイス、オンライン接続など、ビジネス環境を 1 つのソリューションで包括的に保護することができます。

シンプルでガイド付き：自動化された保護とタイムリーなアラートによるシンプルなセットアップにより、ビジネスの安全確保が容易になります。すべてセキュリティ コンソールから行うことができます。タイムリーなアラートで、外出先でも注意が必要なことをお知らせします。

あなたとともに成長します：ビジネスの成長とともに成長する保護機能です。経営者は、各従業員とそのデバイスに簡単に保護を拡大することができます。

サービスの主な特徴は以下の通りです：

- **セキュリティ コンソール：**社内のセキュリティ対策の状況を簡単に確認し、保護機能の設定に関する社員宛ての通知の管理など、必要な作業をすべて 1 か所で行うことができます。モバイル デバイスでも作業できます。
- **次世代型の脅威ブロック製品：**実績豊富なセキュリティ対策に付属している、デバイスの処理速度を低下させない超高速スキャンで、マルウェア、ランサムウェア、ウイルスなど、既知および未知の脅威からビジネス用デバイス (台数無制限)[1] を保護します。
- **ユーザー管理型のセキュリティ対策：**各従業員は、経営者から保護対策を設定するための招待を受け取ると、自身のログインの作成、データとデバイスの保護の設定、必要なセキュリティ対策の実施をすべて 1 つのビジネス契約下で行うことができます。
- **セキュア VPN：**銀行レベルの Wi-Fi 暗号化により、どこでもデータのプライバシーを確保し、かつ安全に保護します。保護されていないネットワークにアクセスすると、自動的に VPN に接続されます。
- **セキュリティレポート：**ステータスや未解決の項目を強調表示し、ビジネス、デバイス、社員のセキュリティ環境を改善します。
- **年中無休の専用サポート：**マカフィーの専任のサポート チームが、24 時間 365 日体制でテクニカル サポート サービスを提供します。電話やチャットを使用して、保護機能の設定などをサポートいたします。

1. 無制限は、典型的な中小企業の合理的かつ予見可能な範囲を対象としています。

方法論 / 本研究について

- 2023 年 9 月、McAfee は以下 6 か国の**中小企業**を対象にオンライン セキュリティに関する調査を実施しました：アメリカ、イギリス、ドイツ、フランス、日本、オーストラリア。
- 回答者は、従業員数 250 人未満の組織で働いている **[　企業経営者および IT 専門家]** のいずれかです。
- この調査は 2023 年 8 月 24 日から 9 月 5 日にかけて、MSI-ACI が世界 6 か国の企業経営者と IT 専門家 700 人を対象として、オンライン アンケートで実施したものです。

マカフィーについて

McAfee は、オンライン保護の分野で世界をリードする企業です。私たちが保護するものは、デバイスではなくお客様です。当社のソリューションはお客様のニーズに対応し、統合された使いやすいソリューションを通じて、お客様が自信を持ってオンライン生活を体験できるよう支援します。

www.mcafee.com

詳細については、
mcafee.com をご覧ください。

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com

gd-cybersecurity-for-small-businesses_0124 JANUARY 2024