ビジネスと顧客に関するデータをサイバー犯罪者から保護する方法

中小・中堅企業に向けた8つのサイバーセキュリティ戦略

このeガイドについて

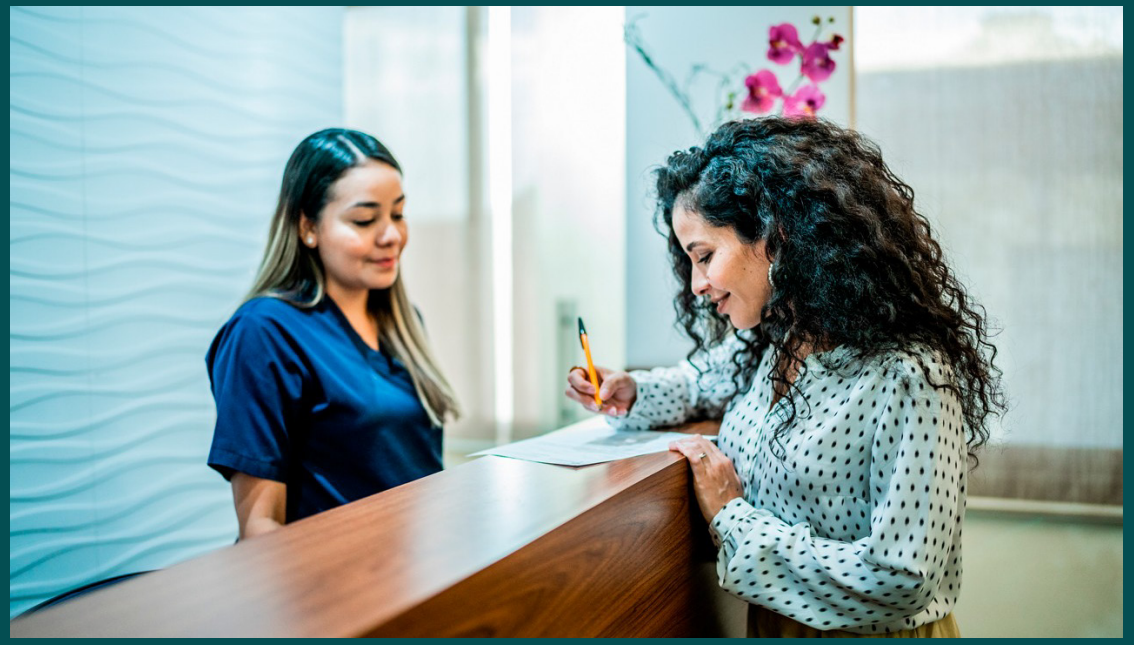
デル・テクノロジーズは、ITとセキュリティのパートナーとしてあらゆる規模の企業から信頼されており、中小・中堅企業(SMB)が日常的に直面するサイバーセキュリティの課題を理解しています。このeガイドでは、サイバー脅威からビジネスと顧客に関するデータを保護するための8つのスマートな戦略について説明します。

目次

概要

サイバー攻撃の発生頻度が増加し、あらゆる規模の企業が攻撃を受けているというニュースを、よく目にします。中小・中堅企業(SMB)にとって、サイバーセキュリティは「あると便利」ではなく、なくてはならないものです。サイバー犯罪者は、SMBなら侵害しやすいと考え、SMBを標的にすることがよくあります。一般に、大企業にはITとセキュリティが専門のチームやリソースがありますが、SMBにはない可能性があるからです。実際、調査によると、世界中の小規模組織の35%が、自社のサイバーレジリエンスが不十分であると考えています。2022年以降、この数値は7倍に増加しています。パソコンに最新のセキュリティ パッチを適用していない、機密情報を保護していない、フィッシングEメールと知らずにクリックするなど、1つのミスがサイバー犯罪を許し、金銭面の損害、データの消失、お客様からの信頼喪失など、さまざまな問題を招き入れてしまいます。

幸いなことに、いくつかのプロアクティブな手順を実行すると、大きな効果が得られます。ビジネスと顧客に関するデータを保護することで、自信を持ち、競争力を維持し、将来に備えることができます。▸



サイバー攻撃者に関する基礎知識

自衛の*方法*を学ぶ前に、攻撃者自身の考え方を知ることが重要です。攻撃者は戦略に沿い、パッチが適用されていないパソコン、脆弱なパスワード、セキュリティで保護されていないネットワークなど、侵入しやすい入口を探します。多くの場合、攻撃者はユーザーの行動や標的のIDを調査し、見逃されている脆弱性を巧みに利用します。攻撃者の戦術を知っておくことで、防御の優先順位を決定し、疑わしいアクティビティを早期に発見して、事後対応ではなくプロアクティブなセキュリティ戦略を構築できます。▸

攻撃者は何者か？

攻撃者は、一般的な犯罪者（悪意のあるハッカー）から国家まで多岐にわたります。Eメールやテキスト メッセージの下手な文章から簡単に見抜ける攻撃者もいれば、資金力があり、そうとわからないように非常に巧妙に仕掛けてくる攻撃者もいます。

攻撃する理由は？

主な動機は金銭です。世界のサイバー犯罪は毎年増加し続けており、専門家は2025年に年間コストが10.5兆米ドルに達すると予測しています。言うまでもなく、1回の攻撃が成功した場合に発生し得る利益の大きさは無視できません。

攻撃方法は？

サイバー犯罪者は容赦しません。AIを自在に操り、巧妙さを増しています。よく使われている攻撃方法をいくつか紹介します。

- パソコンなどの「エンドポイント」への攻撃は、ますます大きな問題となっています。Forrester Research, Inc.の『Endpoint Security Market Insights』（2025年3月）では、「過去12か月間で侵害を受けた企業において、エンドポイントは、外部からの攻撃の主な標的の1つとなっている」と説明されています。
- ID攻撃も急増しています。フィッシングは依然として最大の脅威です。一貫して主要な攻撃方法の1つであり、多くの場合は認証情報を盗みマルウェアを配信するために使用されています。
- ランサムウェアなどのネットワーク攻撃は、大損害を与え続けています。最近の調査結果によると、小規模企業は大企業よりも大きな被害を受けており、侵害の88%がランサムウェアに関連しています。

要するに、サイバー攻撃は金になるのです。ランサムウェア攻撃を成功させたサイバー犯罪者は、平均200万ドルを手にしています。このように、攻撃者にとっては執拗な攻撃が戦略の一部なのですから、攻撃される側は保護を戦略の一部にしなければなりません。

SMBにとっての主要なサイバーセキュリティ リスク

デバイスの侵害

IDの侵害

ネットワークの侵害

1 守るべきものを知る

攻撃者は顧客と従業員に関する機密データを狙いますが、攻撃を受ける側は、狙われるものについて把握していなければ、保護することはできません。会社のすべてのIT資産とデータについて、一覧表を作ってみましょう。データの保管場所、アクセス権限を持っている人、ネットワークで使用しているデバイス、こういった情報を揃えてから、行動を起こします。保管されているデータをセキュリティで保護し、機密情報へのアクセスを制限しましょう。自社のデータについて把握しておくことは、データを保護するための重要な第一歩です。▸

2 セキュアなサプライヤーと連携する

トロイの木馬の話を考えてみてください。ギリシャ人は兵士を一見無害な贈り物の中に隠し、トロイ人はそれを城塞都市の中に運び入れました。城の内側に入った攻撃者は、攻撃を開始しました。今日のサイバー犯罪者は同様の戦術を使用し、信頼できるベンダー、ソフトウェアアップデート、ハードウェアを介して忍び込みます。SMBは多数のサプライヤーに依存していることが多く、そのうちの1社が侵害された場合、脆弱性が生じます。そのため、ベンダーの審査、ソフトウェアの整合性の監視、出荷の詳細の可視化などは、強力なサイバーセキュリティ戦略に不可欠です。▸

3 セキュリティが組み込まれたパソコンを調達する

すべてのパソコンは、サイバー攻撃者の入口となる可能性があります。ハードウェア保護、セキュア ブート、ID保護などのセキュリティ機能が組み込まれていると、パソコンを購入したその日から脅威を防御できます。セキュアなパソコンはIT管理をシンプルにし、マルウェア、フィッシング、不正アクセスに対する防御を強化します。また、攻撃者が遠くから攻撃するとは限らないことにも注意してください。公共スペースや共有スペースにあるパソコンは、誰でも触れるため、スタッフや保守担当者に偽装した人物から侵害される可能性があります。人手不足で物理的リスクもデジタル リスクも増大している今、組み込み型のセキュリティは必須機能です。▸

4 パソコンは常に最新の状態に

サイバー犯罪者は、多くの場合、鍵のかかっていないドアから忍び込むように、古いシステムの既知の欠陥を悪用します。パソコンのアラートを無視してアップデートを延期していると、攻撃に対して脆弱になります。ソフトウェアのアップデートとパッチは、ドアに鍵をかけることと同じです。攻撃者が使用する可能性のあるバグやセキュリティ ホールを修正します。定期的なパッチ適用とアップデートは、脆弱性を修正し、ビジネスと顧客のデータ保護に役立ちます。SMBにとっては、シンプルな手順で大きな問題を防ぐことができます。▸

5 問題を見つけて迅速に修正する

パソコンにセキュリティ対策を施し、常に最新の状態に維持しているからといって、サイバー犯罪者が攻撃しないというわけではありません。攻撃者は、1台のデバイスに対して何十回も攻撃を試みたり、Eメールやテキスト メッセージで多数のフィッシングを送りつけたりします。こうすると、侵入して機密データにアクセスできる確率が高まるからです。そのため、仕事で使用するすべてのビジネス パソコン、ネットワーク、クラウド環境を可視化することが重要です。これにはソフトウェアのレイヤーが役立ちます。すべてを可視化し、不審なアクティビティを発見したらすぐに対処できるようになります。▸

6 強力なパスワードを使用し、MFAを有効にする

「123456」や「password」などのパスワードを使用している人はまだまだ多いですが、これは危険です。認証情報が盗まれると、多くの侵害が発生します。強力なパスワードは防御の第一段階として必須です。とは言え、執拗な攻撃者は近くの抜け穴を探します。多要素認証(MFA)が重要なのは、このためです。2番目のレイヤーが追加され、ハッキングされる可能性が99%低下します。

ですから、まずは強力なパスワードを設定してください。

次に、IDを検証する2番目の方法（指紋認証リーダー、スマート カード、NFCなど）と組み合わせます。さらに保護を強化する場合は、ユーザー認証情報を盗もうとするマルウェアの手の届かない安全なハードウェアに、それを保存します。▸

7 従業員をトレーニングして、スキルをテストする

セキュリティの強さは、最も弱い部分の強度で決まります。残念ながら、人為的ミスは依然として侵害の主な原因です。パソコンの重要なアップデートを先送りする、機密データを誤って公開する、パスワードを再利用する、などがこれに該当します。サイバー攻撃者は標的の陣地に足場を作るため、人為的ミスや不注意な行動を期待しています。こういった理由から、サイバー セキュリティのトレーニングは重要です。従業員は脅威を認識し、セキュリティ慣行にならって行動できるようになります。トレーニングを定期的に実施して、従業員のスキルをテストしましょう。フィッシングを見つけられるか、適切に対処しているか、その理由についても考えます。学習内容を強化し、手遅れになる前にギャップを発見しましょう。知識という力を与えられた従業員は、強力な防御の最前線になります。▸

8 侵害が発生した場合の計画を策定する

常に最悪のシナリオを想定しましょう。非常に多くのものが危険にさらされています。侵害を受けたら、対処のスピードが非常に重要です。インシデント対応計画を策定しておくと、チームは問題発生時に何をすればよいかを明確に知ることができます。侵害の検出から損害の封じ込め、安全なリカバリーまで、対応戦略があれば、ダウンタイムが短縮され、ビジネスの再開が迅速になります。強力なサイバーセキュリティとは、プロアクティブに行動し、何が起こっても対処できるよう準備しておくことです。▸

重要なポイント

生成AIを使った生産性の向上や従業員エクスペリエンスの強化を検討している企業にとって、職場のモダナイズは最優先事項です。最近の調査によると、AI/生成AIがビジネス戦略の重要な要素であると回答したSMBは77%にのぼる一方、半数以上が新しいイノベーションによる攻撃対象領域の拡大を懸念しています。このような心配は当然です。

AI PCの普及とWindows 10のサポート終了に伴い、**アップグレードの絶好のタイミングが訪れています。**最新のAI PCを導入し、パフォーマンスとセキュリティのメリットを最大限に活用しましょう。▸

8つのベスト プラクティスとDellが提供できる支援の概要

1 **守るべきものを知る。**
Dell Servicesは、貴社のIT資産、ネットワーク、データの一覧表作成をお手伝いできます。

2 **セキュアなサプライヤーと連携する。**
Dellのサプライ チェーン管理により、改ざんのリスクを軽減します。セキュアなパソコン設計が、脆弱性のリスクを最小限に抑えます。

3 **セキュリティが組み込まれたパソコンを調達する。**
Dell製パソコンにはセキュリティ機能が組み込まれており、追加の費用は必要ありません。

4 **パソコンは常に最新の状態に。**
Dellはタイムリーなパッチでパソコンを安全な状態に保ちます。お問合せ先Dell Security Servicesで脆弱性評価をお試しください。

5 **問題を見つけて迅速に修正する。**
Dellパートナー ソフトウェア上にレイヤーを配置し、パソコン、ネットワーク、クラウドにわたって不審なアクティビティを監視します。

6 **強力なパスワードを使用し、MFAを有効にする。**
ハードウェアベースの認証情報ストレージにDell SafeIDを使用して、セキュリティをさらに強化します。

7 **従業員をトレーニングして、スキルをテストする。**
従業員のセキュリティ意識向上トレーニングはDell Servicesにお任せください。

8 **侵害が発生した場合の計画を策定する。**
Dellのインシデント対応とリカバリー サービスがお役に立ちます。

更新の準備はお済みですか？お客様の組織に最適なパソコンをお選びください

貴社のセキュリティ目標を満たすAI PCを探してください。Dellは複数のオプションを提供しています。

安全なAI PCでデバイス、ID、ネットワークの攻撃に対抗し、安心して日常業務に注力しましょう。▸

利用可能なセキュリティ機能[1]	Dellと Dell Plus	Dell Pro Essential	最も安全[2] Dell Proと Pro Max
サプライ チェーン保証	●	●	●
サプライ チェーン保証の強化			●
プライバシー シャッター	●	●	●
ロックスロット	●	●	●
指紋認証リーダー	●	●	●
TPM 2.0	●	●	●
認証情報の保護[3]			●
認証情報保護の強化[4]			●
パソコンのセキュリティ アラート			●
ソフトウェア アップデートとパッチ	●	●	●
PC管理			●
AI向けに最適化されたシリコン	●	●	●
セキュリティ向けに最適化されたシリコン			●
次世代アンチウイルス(NGAV)ソフトウェア[5]	●	●	●
NGAV + PC、ネットワーク、クラウドの脅威検出ソフトウェア[5]			●
パソコンの自己修復、ジオロケーション、レジリエンス ソフトウェア			●
高度なパソコン サポート	●	●	●

--

1 あるパソコン機能が、ある製品ラインの中で利用できることはありますが、すべてのプラットフォームでその機能が利用できることを保証するものではありません。

2「最も安全なビジネス向けAI PC」:Dellの社内分析（2025年3月）に基づきます。AMDプロセッサー搭載のパソコンに適用されます。一部のパソコンでは利用できない機能があります。一部の機能については追加購入が必要です。

3 TPMに安全に保存された認証情報を使用して、指紋認証リーダーを介して認証します。

4 Dell独自のControlVaultに安全に保存された認証情報を使用して、指紋認証リーダー、スマート カード、またはNFCを介して認証します。

5 一部のサービスは数量が多い場合のみ利用でき、最低限の数のライセンスが必要です。FedRAMP認証を受けたオプションを利用できます。

次のステップへ

パソコンの更新

Windows 10のサポートは10月に終了し、多くのSMBが古いサポート対象外のパソコンを使用

AMD Ryzen AI PROプロセッサーを搭載したセキュアなDell AI PCにアップグレードする

ソフトウェアのレイヤー

多層防御で攻撃者を阻止

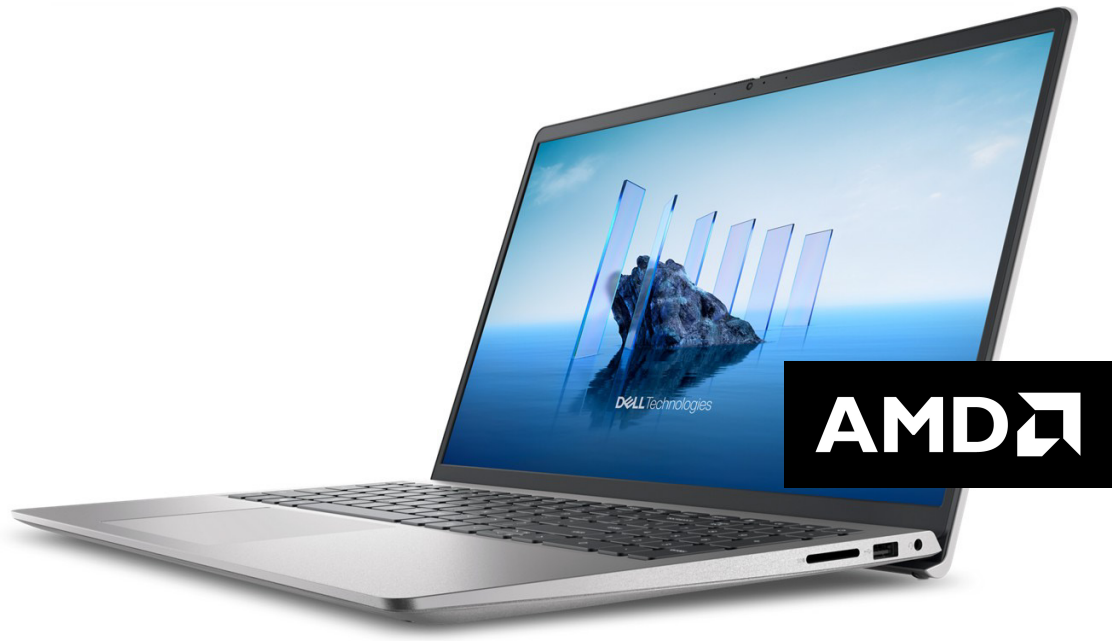
新規および既存のパソコンにソフトウェア保護を追加する

セキュリティ管理のサポートが必要な場合

Dellのサイバーセキュリティ エキスパートが、必要なセキュリティ運用を実行

マネージド セキュリティ サービスの詳細を見る

AMD Ryzen AI PROプロセッサーを搭載した最新のDell AI PCにアップグレードしましょう



詳細はこちら：

お問い合わせ先： Global.Security.Sales@Dell.com

ソリューションの詳細： Dell.com/Endpoint-Security

Dellをフォロー： LinkedIn @DellTechnologies | X @DellTech

デル・テクノロジーズとは

SMBは、人手不足の中でもビジネス情報と顧客データをプロアクティブに保護する必要があります。サイバーセキュリティへの投資は、ビジネス継続性の確保、評判の保護、顧客の信頼の構築に役立ち、現代のビジネス運営に必要とされるスマートな要素です。

Dellは、ランサムウェア攻撃のリスクの軽減から、疑わしいアクティビティの検出、リアルタイムの脅威への対応まで、お客様が現在および将来の組織のニーズに合わせてセキュリティ戦略を策定し、セキュリティ ソリューションを実装できるよう支援します。