Microsoft Security

Microsoft Defender for Business

Windows を知り尽くした セキュリティ ツール

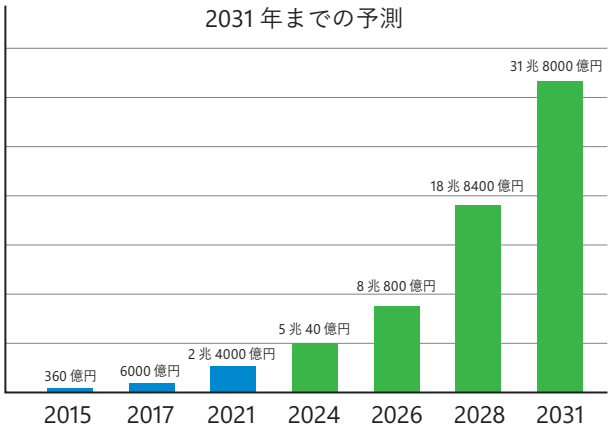
サイバー脅威のもたらす被害が深刻化

社会全体の ICT 化が進むにつれて、サイバー脅威のもたらす被害が深刻化しています。
そのような状況下において多くの組織が何らかの対策を講じています。
しかしサイバー脅威の被害にあった組織をみると 90% 以上の企業で対策を行っているにもかかわらず 80% 近くの組織では攻撃の検出ができなかったという状況になっています※1。

ランサムウェアの被害総額は年々増加しています※3

2015 年には世界で 3 億ドル (約 360 億円) だったランサムウェアの被害総額ですが、2021 年には 200 億ドル (約 2 兆 4,000 億円) まで拡大しており、2031 年には 2,650 億ドル (約 31 兆 8,000 億円) にまで拡大する見込みです。
最近では Emotet などランサムウェアを拡大させるためのウイルスも流行しており、被害拡大の土壌が生成されています。
ランサムウェア自身のふるまいも変化し、データ暗号化による身代金要求から拒否後のデータ公開に至る二重脅迫といったケースも増え、被害総額が増加する傾向にあります。
2022 年はサプライ チェーン攻撃やオープンソース ターゲットの商品化が進み、1 か所の脆弱性をねらった犯罪収益の最大化が問題視されています。

ランサムウェアによる被害総額
2031 年までの予測



※ $1=120 円換算

個人情報漏洩に対して企業が負う責務が増大しています

2022 年 4 月 1 日より改正個人情報保護法が施行され、個人情報漏洩時の報告が義務となりました。侵害された本人への通知が必要となるため、データの保護だけではなくデータの内容や漏洩時の状況などを早期に把握するための手段を準備しておく必要があります。

※1 警視庁 令和 3 年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/news/release/2021/20210915001.html

※2 IPA「中小企業向けサイバー セキュリティ事後対応支援実証事業成果報告書」
https://www.ipa.go.jp/security/fy2020/reports/sme/otasuketai_houkoku.html

※3 cybersecurity ventures Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 (レート￥120 / $1)
https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Microsoft Defender for Business

従来のウイルス対策は対策ソフトに依存し、マルウェアがデバイス内に入ったときにのみ対策を講じていました。その対策もマルウェアの隔離にとどまり、抜本的な侵入阻止には消極的な対応が主だった方針でした。しかしこれからのウイルス対策では、侵入後のマルウェアの隔離はもちろんのこと、クラウド利用を前提に侵入に対する防御を第一に考えた対策が必要です。また、「侵入は行われるものである」ことを前提に、問題発生時の監査やリカバリーに重点をおく必要があります。

これまでのセキュリティ対応		これからのセキュリティ対応
ウイルス対策ソフトの管理 (定義ファイルの更新管理)		潜在するリスク全体の管理 (定義ファイルの更新管理、ウイルス対策の状態、OS やアプリの脆弱性、セキュリティ設定・構成)
ファイルやプログラム単位のチェック		膨大なデータによるチェック (一連の行動に基づくふるまい分析、AI / 機械学習による検知)
社内ネットワーク & 異常検知時のみ	VS	場所を選ばず常時監視、常時対応
人に依存したオペレーション		自動アップデート、自動対応
オンプレミス環境前提のアプローチ		クラウド環境に最適なアプローチ (ゼロ トラスト モデルによるアプローチ)

Windows を知り尽くしたセキュリティ ツールが新登場

中小企業のサイバー セキュリティのために生まれた、**Microsoft Defender for Business**
大企業向けのセキュリティ対策と同等の機能を使うことができるクラウド型のセキュリティ サービスで、すぐに導入することができます。
Microsoft のセキュリティ製品だから、普段お使いの Windows との相性は完璧です。
Microsoft Defender for Business で、あなたのビジネスとセキュリティを Win-Win の関係に。

Microsoft Defender for Business

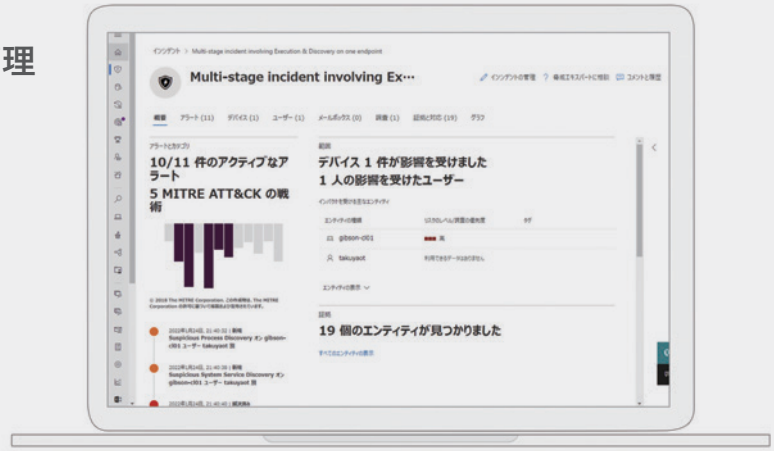
クラウド サービスを活用したセキュリティの監視と保護

■ 脅威の可視化と自動対処
■ Microsoft 製品連携/ウイルス対策も管理
■ クロス プラットフォーム対応※

ランサムウェアなどによるサイバー攻撃が多様化している今、Windows OS 標準搭載のウイルス対策機能に **Microsoft Defender for Business** をプラスして、最高レベルのセキュリティ対策を実現します。

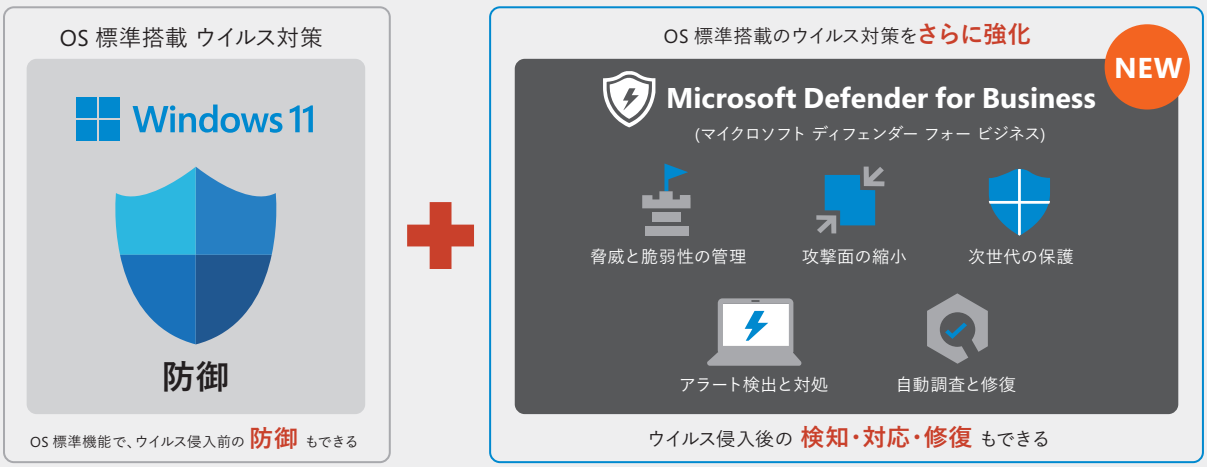
301 人以上の組織を想定して開発された
エンタープライズ クラスのエンドポイント保護なら
Microsoft Defender for Endpoint

※iOS, macOS, Android, iPadOS での利用には、Microsoft Intune のライセンスが必要になります。



ウイルス対策機能では防げない脅威に対する防御、検知、修復対応

ウイルス侵入前の防御を目的としたウイルス対策ソフトでは最近増加しているランサムウェアをはじめとした未知のウイルスを防ぐことは難しいと言われています。最新のウイルスは、ウイルス対策ソフトをすり抜けて侵入するものも増えています。そのため、クラウドから監視を行う Microsoft Defender for Business にて検知し、対応、修復を行うことが重要です。こういった検知や対応、修復を行う製品を Endpoint Detection and Response と呼び、ウイルス対策ソフトを補完しています。



Windows 10/11 と最高レベルの親和性

Windows 10/11 を利用している場合、簡単なオンボーディング作業のみで利用が開始できます。面倒なソフトウェアの最新化などは Windows Update に任せることができ、メンテナンス フリーで利用者にわずらわしさを感じさせません。

製品の特長

1 大企業同等のセキュリティ

大企業向け製品と同等のセキュリティ機能が、中堅・中小企業向けに最適化、1 ユーザーから購入可能

2 攻撃への耐性

万が一サイバー攻撃を受けてもプログラムやサービス停止など影響は最小限

3 メンテナンス フリー

Windows にプレインストール済 Windows Update の適用で更新手間いらず

4 高パフォーマンス

パソコンへの負荷が非常に低く、通信データも 1 台あたり **1 日 5 MB 程度**

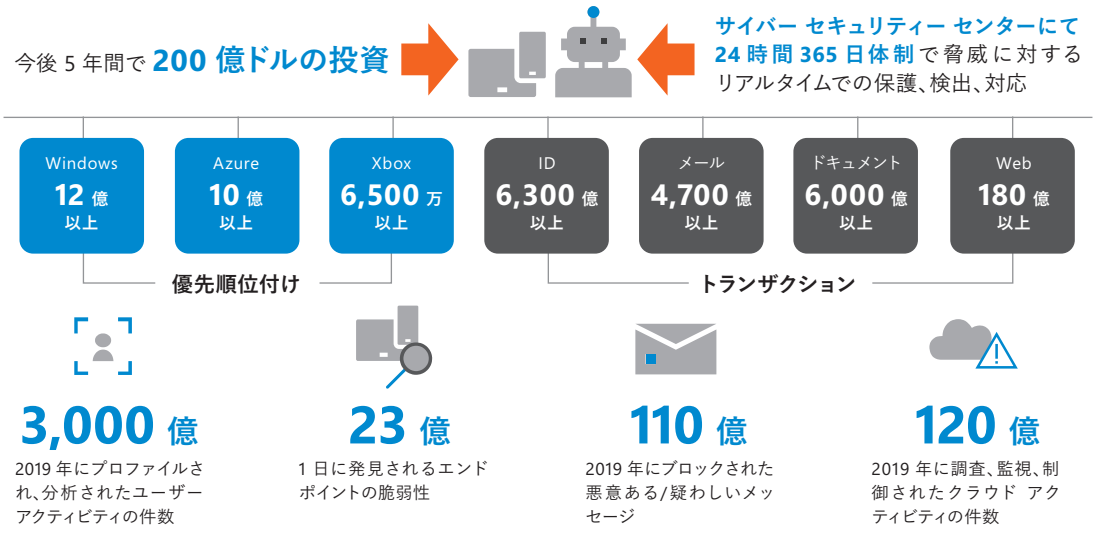
5 さまざまな製品と連携

Microsoft 365 はもちろんさまざまな製品と連携できるマルチ OS 対応※も

※ iOS, macOS, Android, iPadOS での利用には、Microsoft Intune のライセンスが必要になります。

世界随一のサイバー攻撃への防御力を誇る Microsoft のセキュリティ知見を提供

Microsoft は、米国国防総省に次いで世界で 2 番目に多くのサイバー攻撃を受けている組織と言われています。
世界中でご利用いただいている Microsoft 製品を通してサイバー攻撃を地球規模で監視、24 時間 365 日体制で、AI + セキュリティ専門家による対応を通じ世界最高水準のセキュリティを提供します。



3,000 億
2019 年にプロファイルされ、分析されたユーザー アクティビティの件数

23 億
1 日に発見されるエンドポイントの脆弱性

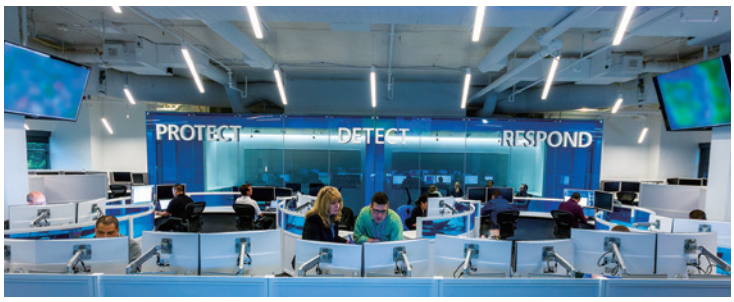
110 億
2019 年にブロックされた悪意ある/疑わしいメッセージ

120 億
2019 年に調査、監視、制御されたクラウド アクティビティの件数

第三者機関によるセキュリティ評価は最高ランク

ガートナー マジック クアドラントの 5 部門で「リーダー」の評価を獲得※1

IDC MarketScape「Modern Endpoint Security for Enterprise and Small and Midsize Businesses」部門で「リーダー」の評価を獲得※2



Microsoft サイバー防御オペレーション センター (CDOC)

サイバー防御オペレーション センターでは Microsoft 全社からセキュリティ対応の専門家を募り、脅威に対するリアルタイムでの保護、検出、対応に取り組んでいます。このセンターは 24 時間 365 日体制の専任チームを擁しており、セキュリティの脅威に対する迅速な対応と解決を実現するために、Microsoft 全体の何千ものセキュリティ専門家、データ サイエンティスト、製品エンジニアと共に脅威にリアルタイムで対抗しています。

※1 下記の 5 部門に相当
Gartner「Magic Quadrant for Access Management」、Henrique Teixeira、Abhyuday Data、Michael Kelley、2021 年 11 月
Gartner「Magic Quadrant for Cloud Access Security Brokers」、Craig Lawson、Steve Riley、2020 年 10 月
Gartner「Magic Quadrant for Enterprise Information Archiving」、Michael Hoech、Jeff Vogel、2020 年 10 月
Gartner「Magic Quadrant for Endpoint Protection Platforms」、Paul Webber、Rob Smith、Prateek Bhajanka、Mark Harris、Peter Firstbrook、2021 年 5 月
Gartner「Magic Quadrant for Unified Endpoint Management」、Dan Wilson、Chris Silva、Tom Cipolla、2021 年 8 月
※2 Microsoft、IDC MarketScape の「Modern Endpoint Security for Enterprise and Small and Midsize Businesses」部門で「リーダー」の評価を獲得 - Microsoft Security ブログ (英語)

Microsoft Defender for Business

6 つの機能

脅威と脆弱性の管理

Microsoft Defender for Business では専用のサイトを通じて、世界の脅威トレンド情報や Microsoft 以外のメーカーが作成したソフトウェアの脆弱性を管理する機能などが提供されます。一元管理することで脆弱性管理の問題が一気に解決されるのです。

お客様が抱える「脆弱性管理」に関する主な問題点

検出

- 定期チェックができていない
- 盲点がある
- 実際の状況との乖離
- 過去のある時点の情報

優先順位付け

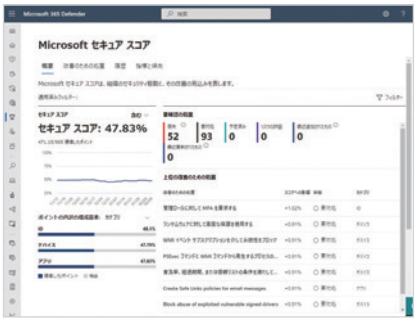
- 重要度に基づいていない
- 組織に基準がない
- 脅威に基づいていない
- 大雑把なレポート

補正

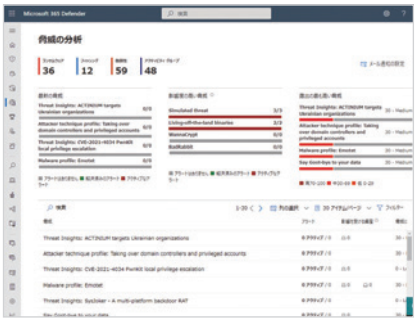
- パッチを待つのみ
- IT と セキュリティ部門の連携
- 手動処理
- 作業完了の確認

結果： 高い維持費にもかかわらず、組織は依然として高い脆弱性を抱えている

Microsoft Defender for Business で脆弱性を一元管理

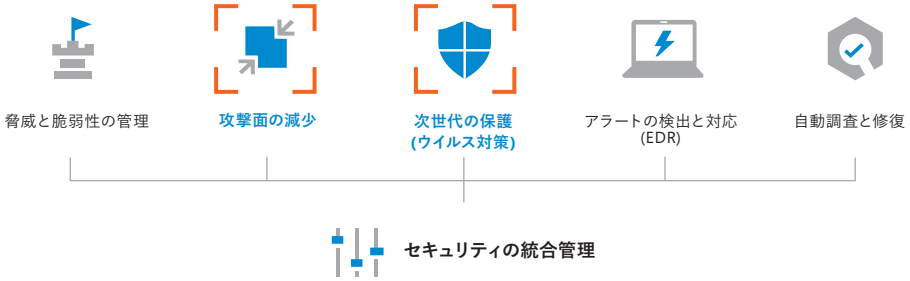


Microsoft セキュリティ スコア
組織のセキュリティ状況をスコア化
改善のための処置方法を提案



脅威の分析
世界で起こる最新の脅威情報確認
組織内への影響・対策も確認可能

脆弱性の管理
サードパーティ ソフトウェアを含む脆弱性への対応状況を確認可能



攻撃面の減少

増え続ける脅威への対抗策は攻撃される可能性を減らすことです。デバイス レベルで不要な機能をオフにすることで攻撃可能な範囲を極小化することができます。もちろんブロックした問題を一元管理できるので、攻撃状況も漏れなく把握可能です。

お客様が抱える「攻撃」に関する主な問題点

ゼロ デイ
ゼロ デイ攻撃が続くセキュリティ業界の現状

ネットワーク境界
境界線が侵食されているため、独自の防御ソリューションが必要

クロス プラットフォーム
異機種混在の環境では防御が難しい

結果： 企業は、積極的なセキュリティ対策に苦慮している

Microsoft Defender for Business で攻撃可能な範囲を極小化

攻撃面の縮小ルール
Windows OS の機能。悪用されることが多いプログラムやソフトウェア動作を 15 のルールを基にブロックすることが可能。

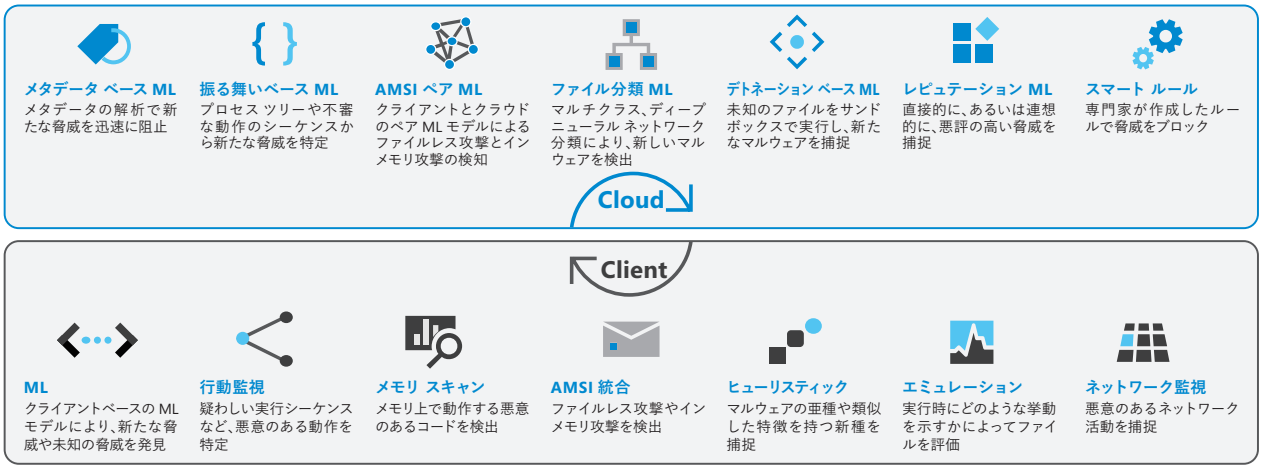
デバイス構成の確認
組織内での利用可能条件を満たしていないデバイスや、誤って構成されているデバイスを特定。

検出された侵害アクティビティ
攻撃面の減少ルールによって検出された侵害アクティビティを確認。

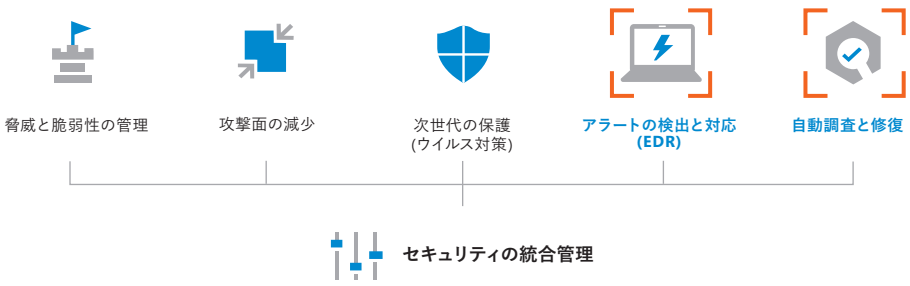
Web 保護
Web の脅威からコンピューターを保護することができ、不要なコンテンツを規制することが可能。
またその状況をアラートやレポートで確認。

次世代の保護 (ウイルス対策)

Windows 10/11 に標準搭載された Microsoft Defender ウイルス対策は Microsoft Defender for Business を利用することで、Windows 単体では実現できないスキャン実施状況やウイルス対策状態も統合管理できます。もちろん標準搭載されたウイルス対策も業界内テストでトップ スコア※を取得し続ける安全性の高い機能を有しています。



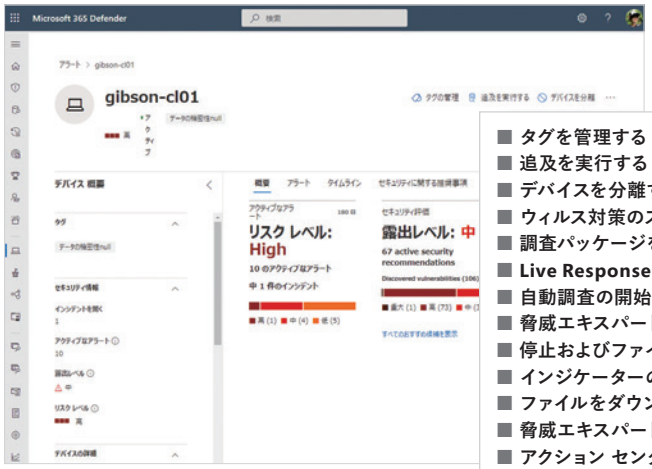
※AV-TEST 調べ 。2021 年を通じて保護スコアは 6.0/6.0 となっている。



アラートの検知と対応 (EDR)

脅威が組織内部に入り込んだ場合、一般にそれを検出することは困難を伴います。
Microsoft Defender for Business を利用すればデバイスとファイルの脅威の発生を自動的に検知し、アラートをメール送信することが可能です。
解析された状況と共にアラートを受け取ったら、デバイスに対する操作を選ぶだけで適切な対処が行えます。
問題が複雑で調査が難しければ自動調査に委ねましょう。

- 感染したシステムの 46% にマルウェアが存在しなかった
- ネットワークやさまざまなセンサーを経由した高度な攻撃を追跡することは困難
- 1 台の感染端末からでも、証拠やアラートを収集することは、長い時間のかかる作業となる
- Living off the land (LOTL) – 攻撃者は回避技術を駆使する



- タグを管理する
- 追及を実行する
- デバイスを分離する
- ウィルス対策のスキャンを実行する
- 調査パッケージを収集
- Live Response セッションを開始する
- 自動調査の開始
- 脅威エキスパートに相談
- 停止およびファイルの検疫
- インジケーターの追加
- ファイルをダウンロード
- 脅威エキスパートに相談
- アクション センター

自動調査と修復

脅威に遭遇した時、影響が本当にあったのか確認するのは管理者の役割です。しかし規模の小さい組織ほど、この役割にかけられるコストが小さいことは明白です。Microsoft Defender for Business は AI を活用した自動対処の機能を備えています。

自動調査

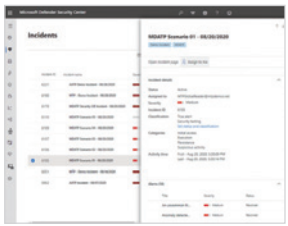
アラートを自動的に調査し、複雑な脅威を数分で修正

- **アナリストが実行する理想的な手順を模倣**
- **ファイルまたはメモリ ベースの攻撃に有効**
- **無制限のキャパシティで 24 時間 365 日動作**

インシデント対応の流れ

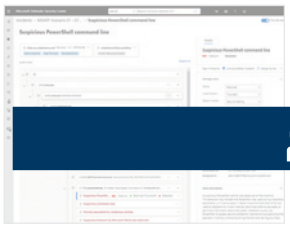
自動調査・対応の場合

❶ インシデント ページで アラート確認



- ダッシュボード
- インシデント

❷ アラートをドリルダウンして詳細確認

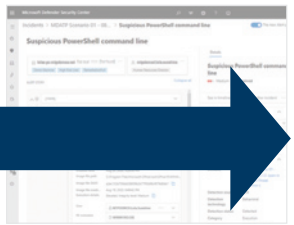


- アラート
- アラートの詳細ページ
- ファイルページ
- デバイス ページ

❸ デバイスやファイルにアクションを実施

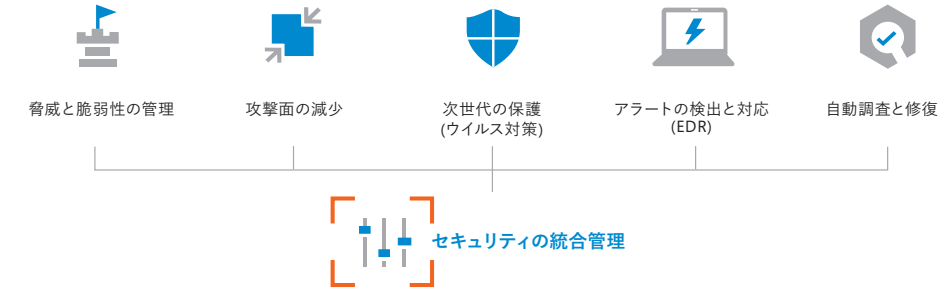
- ファイル ページ
- デバイス ページ
- アクション センター

❹ インシデント/アラートのクローズ



- インシデント

❷ ～ ❹を自動対応



セキュリティ統合管理

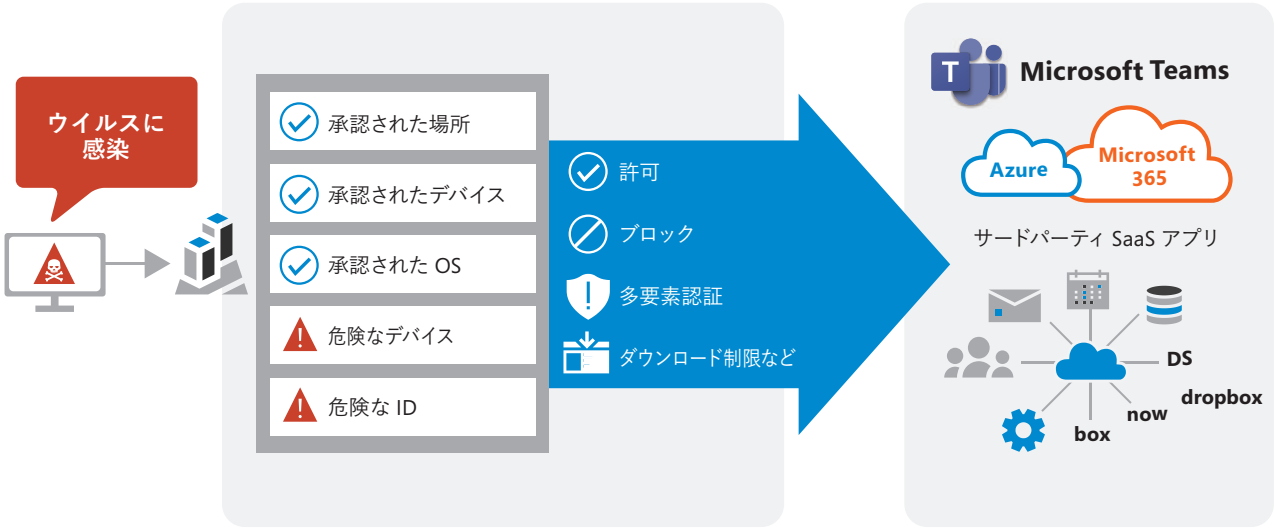
サイバー脅威はデバイス、ネットワーク、ID など多方面からやってきます。これらを統合的にチェックすることで脅威の見落としを防ぐことができます。
これを実現できるのは Microsoft 365 や、サードパーティの脅威を統合管理できる Microsoft Defender for Business です。
Azure AD P1 および Intune が含まれる Microsoft 365 Business Premium を利用すればゼロ トラスト セキュリティも容易に実現可能です。

Microsoft 365 製品との連携

Microsoft 365 製品間でデータを連携することにより、統合された保護と、製品をまたいだ知識と機能の新しいレイヤーを提供

- **統合されたダッシュボードでの管理**
- **リスク レベルに応じたアクセス制御 (Azure AD P1 + Intune※)**

※Azure AD P1 および Intune が含まれる Microsoft 365 Business Premium で利用可能。



Microsoft Defender for Business を使いたい場合は

セキュリティ強化の度合いや現在利用中のクラウド環境における対策状況によって 2 つのプランから選択できます。

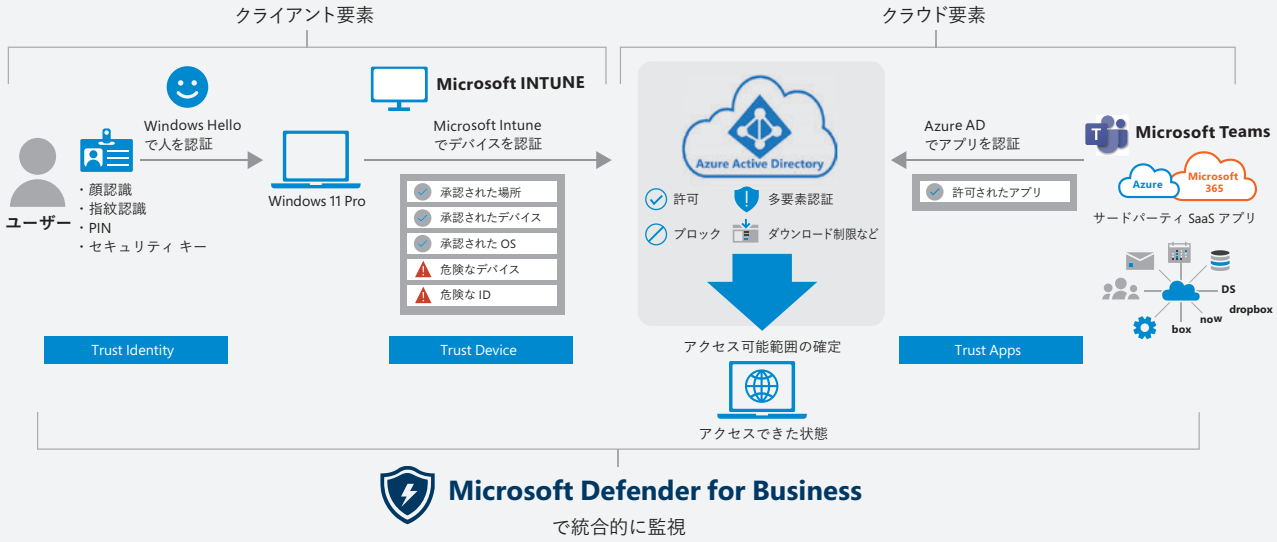
Microsoft 365 Business Premium で ゼロ トラスト型セキュリティ対策が実現可能

Microsoft 365 の機能と Azure AD P1/Intune が提供されます。Office アプリとパワフルなクラウド サービスに包括的なセキュリティを組み合わせたプランです。ビジネスを高度なサイバー脅威から守るのに役立ちます。

Microsoft Defender for Business で 端末セキュリティのみ切り出して対応可能

Microsoft Defender for Business 単独での購入もおすすめです。Windows OS 標準のセキュリティ対策ソフトを強化して、さらに EDR 機能を追加したい場合にはこちらを選択しましょう。

アクセスが可能となるまでチェックの行われない要素がない状態。これがゼロ トラスト セキュリティ。



課題解決にクラウドの Microsoft 365

Microsoft 365 は、Office アプリケーションを含む Microsoft のクラウド ソリューションを利用できるサービスです

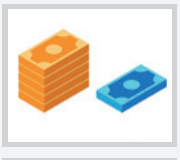
Microsoft 365 を利用すると、常に最新の Office アプリケーションを利用することはもちろん、場所やデバイスに関係なく効率的に作業することができます。
Exchange Online によるメール/スケジュール/連絡先管理、SharePoint Online による情報/ドキュメント共有、Microsoft Teams によるチャットや Web 会議も可能。大容量 1 TB のオンライン ストレージである OneDrive も標準で提供。
エンタープライズ レベルのセキュリティで企業を守ります。

Microsoft 365 Business Premium のメリット

どこからでも安心して仕事ができる

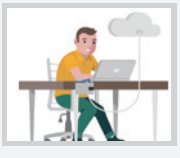
包括的で使いやすい

- 1 つのソリューションで生産性とセキュリティを両立
- クラウド プラットフォームであるため、導入が簡単
- すぐに利用できる



コスト削減

- 複数のポイント ソリューションにかかるコストを廃止
- ヘルプ デスクのコストを削減
- ライセンスの複雑さを解消



エンタープライズ レベルのテクノロジー

- 多くのエンタープライズが信頼する高度なセキュリティ
- AI を活用した脅威インテリジェンス
- 評価の高いセキュリティ

ゼロトラスト型セキュリティ対策を実現する場合
Microsoft 365 Business Premium がおすすめです。

あなたのビジネスに最適なプランをお選びいただけます※1 最適なプランの詳細はこちらをご覧ください	Remote Work Starter Plan リモートワーク スターター プラン	Microsoft 365 Business Basic (旧 Office 365 Business Essentials)	Microsoft 365 Business Standard (旧 Office 365 Business Premium)	Microsoft 365 Business Premium (旧 Microsoft 365 Business)
	リモートワークの第一歩、今すぐ Web 会議をはじめよう	包括的なチームワークとコラボレーションを実現	業務効率化とコミュニケーションを最大化	管理の効率化と最新セキュリティを提供
価格プラン	販売パートナー様、もしくはマイクロソフト公式サイトでご確認ください	販売パートナー様、もしくはマイクロソフト公式サイトでご確認ください	販売パートナー様、もしくはマイクロソフト公式サイトでご確認ください	販売パートナー様、もしくはマイクロソフト公式サイトでご確認ください
含まれる Office アプリ	(Web 版とモバイル版のみ)	(Web 版とモバイル版のみ)	Outlook, Word, Excel, PowerPoint, Access, Publisher (Access, Publisher は Windows PC のみ)	Outlook, Word, Excel, PowerPoint, Access, Publisher (Access, Publisher は Windows PC のみ)
含まれる サービス	Teams, OneDrive	Teams, OneDrive, SharePoint, Exchange	Teams, OneDrive, SharePoint, Exchange	Teams, OneDrive, SharePoint, Exchange, Intune, Azure AD Premium P1, Azure Information Protection, Microsoft Defender for Business
最大ユーザー数	300 人	300 人	300 人	300 人
Web とモバイル版の Office アプリ				
Word、Excel、PowerPoint、Outlook、OneNote (Web とモバイル版)	✓ (モバイル版一部機能制限有)※3	✓	✓	✓
(最大 5 台のスマートフォンと 5 台のタブレット)※2	(Web 版のみ)	✓	✓	✓
リアルタイム共同編集	✓	✓	✓	✓
メールとタスク管理				
メールのホスティングと 50 GB のメールボックス	(2 GB のメールボックスのみ)	✓	✓	✓
Microsoft Planner タスクやスケジュール、進捗の管理	–	✓	✓	✓
ファイル ストレージと共有				
OneDrive 1 TB クラウド ストレージ	✓	✓	✓	✓
SharePoint ファイル共有やイントラネット サイト構築	✓	✓	✓	✓
チームワークとコミュニケーション				
Microsoft Teams コミュニケーション アプリ	✓	✓	✓	✓
最大 300 人での Web 会議	✓	✓	✓	✓
会議のスケジューリングと開催	✓	✓	✓	✓
チームやチャネル内でのファイル共有	✓	✓	✓	✓
チャット、会議、アプリなどすべてまとめて Teams からアクセス	✓	✓	✓	✓
デスクトップ版の Office アプリ				
常に最新版の Office アプリを Windows または Mac にインストールして使用できます (Access と Publisher は Windows PC のみ)	–	–	✓	✓
Office アプリをユーザー 1 人あたり最大 5 台の Windows PC または Mac にインストールできます	–	–	✓	✓
セキュリティとコンプライアンス				
高度なセキュリティ対策	–	–	–	✓
EDR 機能	–	–	–	✓

EDR の強化に Microsoft Defender for Business の購入をおすすめします。

サポートと展開				
電話または Web でのサポート	(クラウド ソリューション プロバイダー にて提供)	✓	✓	✓
法人向けライセンス	✓	✓	✓	✓

※1. 中堅・中小企業向け Microsoft 365 プランの詳細はこちらをご覧ください。Remote Work Starter Planの詳細はこちらをご覧ください。
※2. Windows 10 以降に対応しています。Windows PC と Mac の全要件については、システム要件をご覧ください。
※3. モバイル版の機能制限の詳細についてはこちらをご覧ください。

Microsoft Defender for Business の最小要件

ライセンス (以下のいずれか)

- Microsoft 365 Business Premium
- Microsoft Defender for Business のライセンス

ネットワーク接続

- 各 PC からサービス URL にアクセスできること

※最新の情報をご確認ください。
※その他 Microsoft Defender for Business の要件はこちらをご覧ください。

サポート OS

- Windows 10/11 (Business, Pro, Enterprise)
- macOS※
- Android、iOS / iPadOS※

※ 最新の 3 つのリリースがサポートされています。
※ iOS、macOS、Android、iPadOS での利用には、Microsoft Intune のライセンスが必要になります。

ブラウザー要件

- Microsoft Edge
- Google Chrome

Microsoft Defender for Business - FAQ

Q. ウイルス対策ソフトとの違いはなんでしょう?

A. ウイルス対策ソフトは侵入や実行防止を目的としていますが、Microsoft Defender for Business は脅威発生後のいち早い検知と対処、セキュリティ統合管理を目的としています。ウイルス対策ソフトを包含し、管理する機能も提供するものとなります。

Q. 他社製のウイルス対策ソフトも使用できますか?

A. 組み合わせることが可能です。ただし一部機能 (ファイルの実行防止) などが使用できません。Defender ウイルス対策が推奨とはなりますが、他社製のウイルス対策ソフトとの組み合わせも可能です。

Q. Microsoft Defender for Endpoint の必要要件を教えてください。

A. Defender for Endpoint のライセンスおよび、対応 OS、インターネット接続 (80/443) が必要です。各クライアントからお客様テナントにリアルタイムにデータが送信されます。(1 日平均 5 MB/台程度)

Q. Microsoft Defender for Business を試してみることはできますか?

A. 可能です。
https://aka.ms/MDBJP よりお申込みいただくことで、無料トライアルが可能です。

ソリューションの詳細は各パートナーの公式サイトをご参照いただくか、または各パートナーにお問い合わせください。
Microsoft Security に関する最新情報はこちらをご覧ください。**https://aka.ms/JPMDB**

製品に関するお問い合わせは、次のインフォメーションをご利用ください。

■ インターネット ホームページ　https://www.microsoft.com/ja-jp/
■ マイクロソフト購入相談 窓口　0120-167-400 (9:00 ～ 17:30 土日祝日、弊社指定休業日を除きます)

※ 電話番号のおかけ間違いにご注意ください。

Microsoft
日本マイクロソフト株式会社
〒108-0075 東京都港区港南 2-16-3 品川グランドセントラルタワー