Microsoft

ハイブリッド ワーク時代の デバイス マネジメント

新しい時代の働き方に
最適な管理ツールとデバイスとは？

INDEX

第 1 章

多様な働き方を推進する デバイス マネジメントとは?

近年リモート ワークが普及し、自宅や外出先から各種デバイスを使って会社の業務を行うなど、私たちのワーク スタイルは多様化しています。

そうした働き方に合わせて環境を整える会社も増えてきましたが、ルールや仕組みづくりが行き届かずに、

リスクを放置してしまっていたり、セキュリティ対策が古いままだったりする状況も多く見られます。

この ebook は、デバイス マネジメントの観点から、新時代の働き方を支援するための入門書です。

あなたの会社の成長のために、どうぞお役立てください。

業務用デバイス、どうやって管理していますか？

これまで、自社で使用する PC やスマートフォンなどの
デバイスはどのように管理していましたか？
管理担当者が 1 台ずつ設定して、更新やトラブルのたびに対応、
高度なセキュリティ対策や管理ルールはなし…
そんな会社も多いのではないでしょうか。

HINT!

使う側も管理する側も満足できる デバイス管理とは？

ハイブリッド ワークの時代には、デバイスの社外持ち出しや BYOD（個人デバイスの業務利用）の導入といった、新たなニーズに対応したルールや仕組みづくりが求められます。

利用者側の意見

- いつでもどこでもリモート ワークできる環境がほしい
- 会社の Windows 端末を社外でも使いたい
- 自分のスマートフォンを仕事でも使いたい

管理者側の意見

- どうやってリモートワーク用デバイスを管理すればいい？
- BYOD で社内の情報にアクセスするのはセキュリティが心配
- デバイスを社外に持ち出すのは心配。VPN のセッション数も足りない

POINT

ハイブリッド ワーク時代のモダンなデバイス管理へ

デバイスの選定と Microsoft Intune の活用により、管理者の負担を減らしながら、安心・簡単に社員へデバイスを展開することができます。費用対効果も高く、管理者はもちろん、利用する社員、ひいては会社全体の満足度が高まる管理方法へシフトしましょう。

自宅や外出先で快適に仕事できるようにするには？

自宅や外出先で安全かつ快適にデバイスを使うためには、
デバイスそのものとアカウントの保護が必要です。
社内のデバイスを統合的に管理する「クラウド サービス」を利用すれば、
手間をかけずに更新管理やデバイスの自動構成、アプリの自動割り当てなど、
デバイス管理に必要な作業の一元管理が可能となります。

HINT!

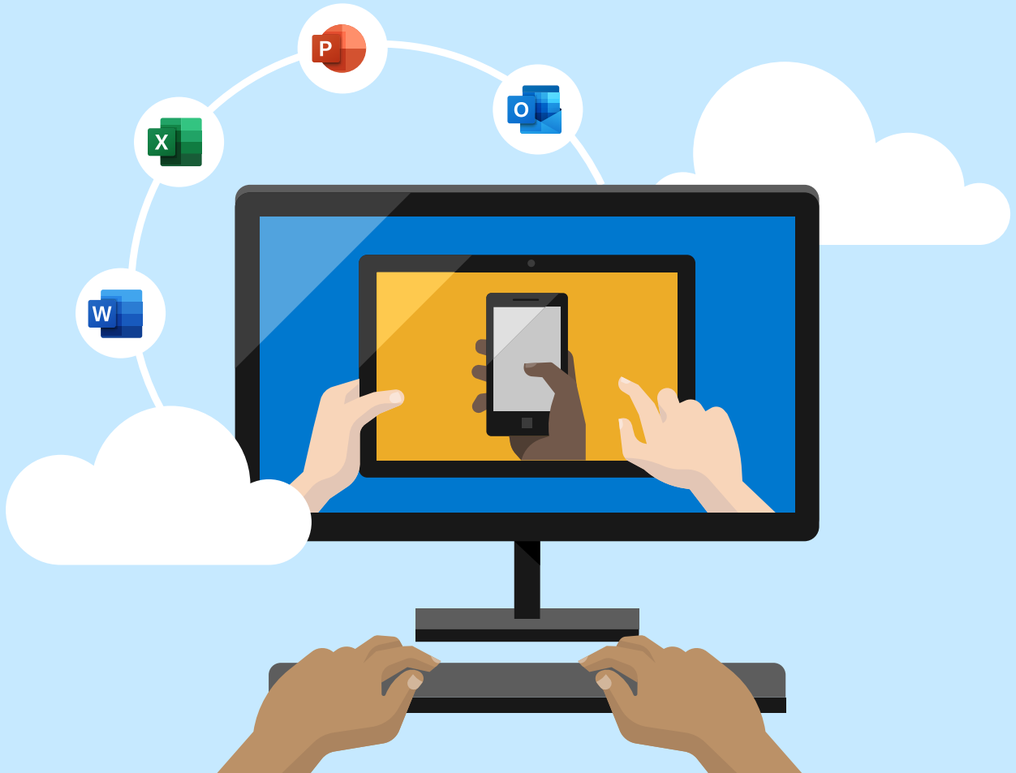
クラウド ベースの端末管理がもたらすメリットに注目！

クラウド サービスであれば、インターネットにつながっているすべてのデバイスで利用できます。もちろん PC に限らず、タブレットやスマートフォンでもアクセス可能です。また、クラウド サービスはサーバーを用意する必要がないので、運用管理費やウイルス対策のコストを削減でき、初期費用も抑えられるため、スモール スタートが可能です。将来的に管理するデバイスが増えた場合でも、同じ UI で対応できるので、管理者の負担を減らせます。

従来の端末管理		クラウド ベースの端末管理
遅い	展開時間	速い　MERIT さまざまなデバイスからアクセス可能！
高コスト	費用対効果	低コスト　MERIT コストを削減でスモール スタートが可能！
増	管理者の作業量	減　MERIT 管理するデバイスが増えても管理者の負担は増えません！

クラウド ベースの デバイス & アプリ管理ツール Microsoft Intune

Microsoft Intune は、マイクロソフトが提供する法人向けクラウド サービス
Microsoft 365 E3 に含まれるデバイス管理機能です。
会社管理の PC、スマートフォンや BYOD デバイスの、
デバイス情報の管理、状況確認、制御・ポリシー、さらにアプリの配信・制御まで、
すべてクラウドベースで行うことができます。



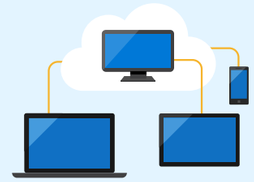
HINT!

個人スマホでも安心！ Microsoft Intune 4 つのメリット

MERIT 1

クラウド サービスである

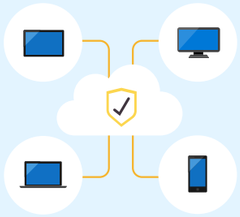
インターネットにつながっているすべての端末で利用できるため、社外にアクセスポイントを設置するなどの対応が不要です。また、従来の管理方法と比べて、セキュリティのリスクを減らすことができます。



MERIT 2

Azure AD との連携

Microsoft Intune は、マイクロソフトが提供する IDaaS（Identity as a Service）である「Azure AD」と連携可能です。あらゆるデバイスを一元管理する Microsoft Intune とアクセス制御機能を備えた Azure AD を連携させれば、クラウド利用の安全性を高められます。



MERIT 3

マルチデバイス対応

Windows OS だけでなく、Mac OS、Android、iOS など、幅広い環境に対応・サポートしているので、PC、タブレット、スマートフォンなど、デバイスに縛られずに一元管理することができます。

MERIT 4

同一デバイス上でのデータ切り分け

BYOD の場合でも、個人デバイス内のプライベート データやアプリとは完全に切り離され、業務用のファイルやデータには Microsoft Intune のポータルサイトやアプリにログインしないとアクセスできないため、安全に利用することができます。

第 2 章

デバイス マネジメント 実践編

Microsoft Intune でハイブリッド ワークをサポート

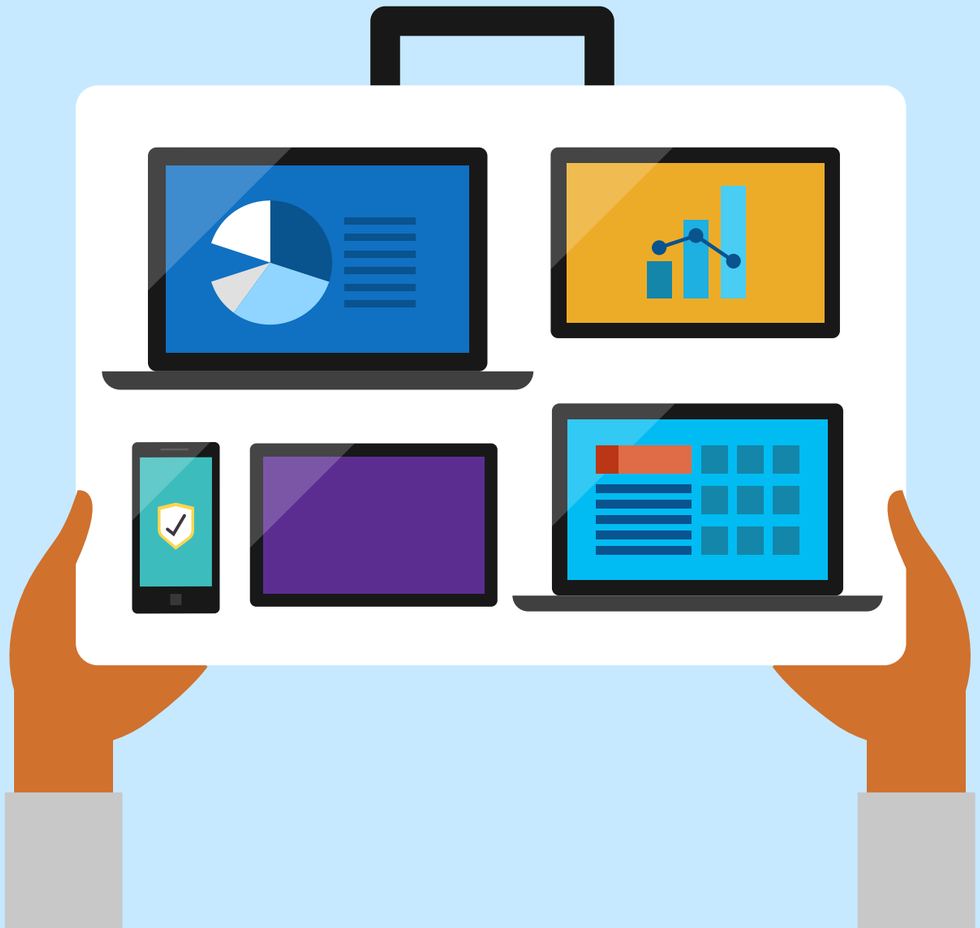
Microsoft Intune は、ハイブリッド ワーク時代の多様な働き方を支援するデバイスやアプリの管理ツールです。

この章では、Microsoft Intune の機能を活用したデバイス マネジメントについて、

具体的にどのようなことができるのかをご案内します。

モバイル ワークや BYOD も簡単に導入できるの？

Microsoft Intune を利用すれば、会社によるデバイスの一括購入・
一括管理の場合も BYOD の場合も、簡単に導入でき、
安全に利用を開始することができます。



HINT!

会社支給デバイスでも 個人所有デバイスでも簡単に導入可能！

デバイス一括購入の場合

デバイスを会社で一括購入する場合、各 OS の購入プログラム経由で購入した段階で会社のデバイスとして設定され、利用者が組織 ID を入力すれば、すぐに管理者が設定したポリシーに基づいて利用することができます。

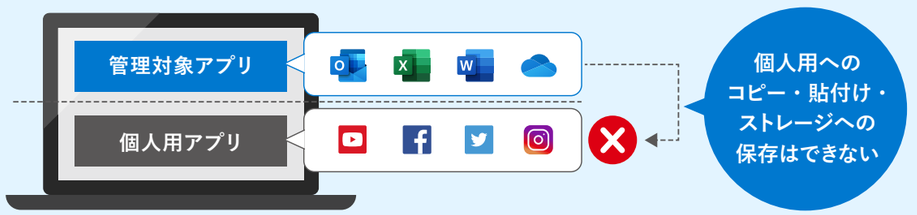
BYOD の場合

個人デバイスの場合も、Microsoft Intune のポータル アプリをインストールして登録すれば、すぐに管理者が設定したポリシーに基づいて利用を始められ、管理者は個人のデータやアプリに触れずにデバイスを管理できるようになります。

Question

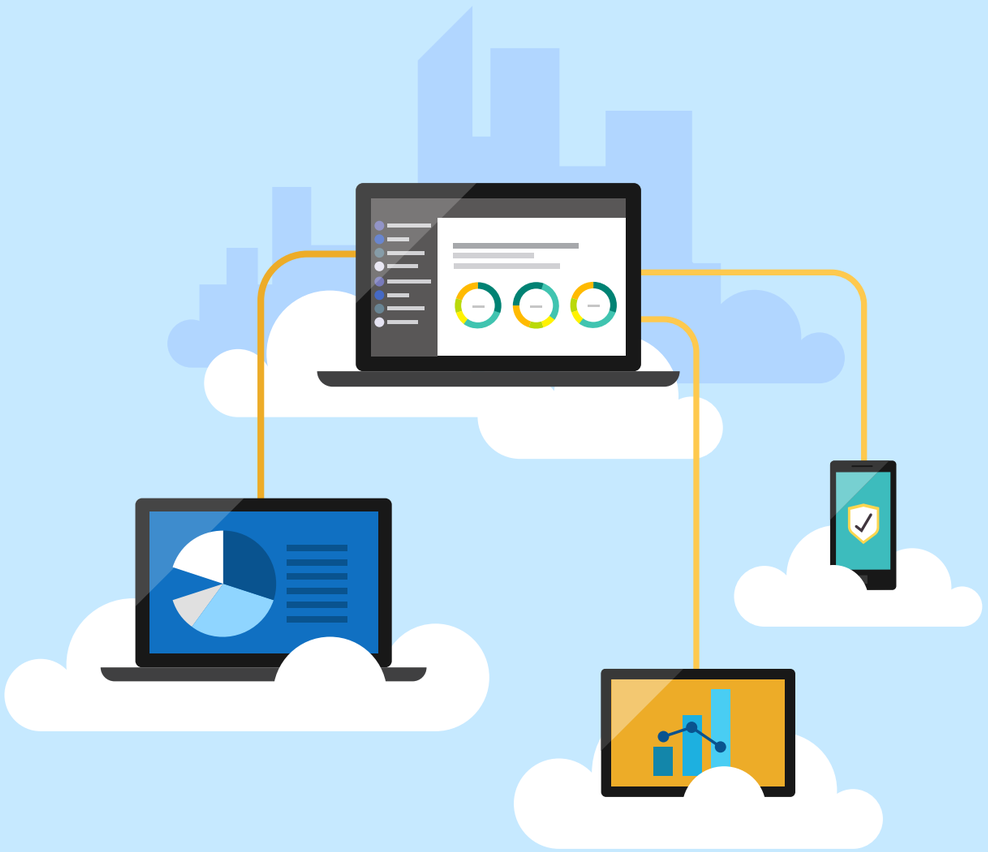
業務データの不正利用や漏洩の心配は？

Microsoft Intune を利用してアプリの管理を行うことで、Word、Excel、Outlook などのネイティブ アプリを安全な状態で利用できるようになります。BYOD の場合も、業務データの個人用アプリへの貼り付けや個人用ストレージへの保存はできませんし、管理者が指定したデータやアプリは個人デバイス内のプライベートなデータやアプリとは完全に切り離され、業務データは複製・受け渡しできない状態で社内情報にアクセスすることになるため、安全に作業できます。



リモートワークでも安全に使えるの？

Microsoft Intune を利用すれば、リモート ワーク時のデバイス管理も安全・簡単です。
デバイスを紛失したり盗難にあったりした場合も、クラウド上でデバイスを制御し、
データの漏洩や破損を防ぐことができます。



HINT!

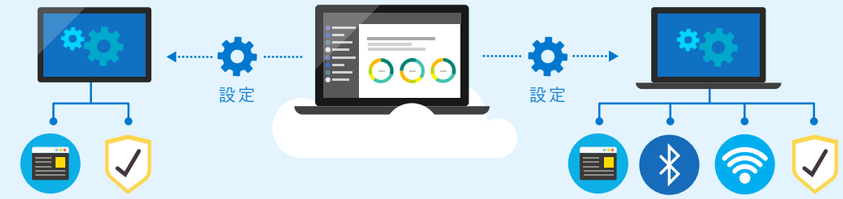
クラウド上のデバイス制御で リモート ワーク時の不安を解消！

Microsoft Intune によるデバイス管理

- 接続デバイスの確認
- デバイスのインベントリ取得
- デバイスの自動構成・自動設定
- レポート表示
- 更新管理
- リモートワイプ

プラットフォームに応じてポリシーを設定可能

会社支給のデバイスと個人所有のデバイス、どちらについても、OS やデバイスの種類に応じて、さまざまなポリシーを作成・設定することができます。



設定項目例

- ブラウザーの設定
- Bluetooth やカメラの利用許可 / 不許可
- Wi-Fi の設定（SSID / Password）
- Microsoft Defender ウイルス対策の設定
- 更新プログラムのダウンロード / 適用時間設定

万が一の紛失や盗難への備えは？

デバイスの紛失や盗難などのトラブル時には、クラウド上で対象デバイスのデータやアプリを制御・削除することができます。

遠隔操作による紛失・盗難時対応

- デバイスを製造元の既定設定にリセット
- 会社関連データとビジネス アプリケーションを削除（BYOD の場合、プライベート データは削除されません）

アプリの管理や更新はどうすればいい？

Microsoft Intune を利用すれば、配信したいアプリを選択して、
登録されているデバイスへの配信方法やインストール方法など、
さまざまな管理をリモートで行うことができます。
プラットフォームに応じたポリシーの設定も可能です。

HINT!

アプリのインストールから削除まで、リモートで管理・制御可能！

Microsoft Intune によるアプリ管理

アプリの割り当て	アプリの構成	アプリの更新
使用レポート作成	更新管理	アプリ内の組織データのみを選択してワイプ

プラットフォームに応じてポリシーを設定可能

会社支給のデバイスと個人所有のデバイス、どちらについても、OS やデバイスの種類に応じて、さまざまなポリシーを作成・設定することができます。

インストールの種類を選択可能

強制的なインストール、利用者が選択できる任意のインストール、管理者による削除など、管理者がインストールの種類を選択できます。またアプリ構成ポリシーを設定することで、対応しているアプリに対して規定値を展開させることができるため、管理者が個別に設定を行わなくても、アプリケーションの設定を行うことが可能です。

第 3 章

デバイス マネジメント セキュリティ編

Microsoft Intune で一元管理

リモートワークやクラウドサービスの普及に伴い、デバイスのセキュリティマネジメントが大きな課題となっています。

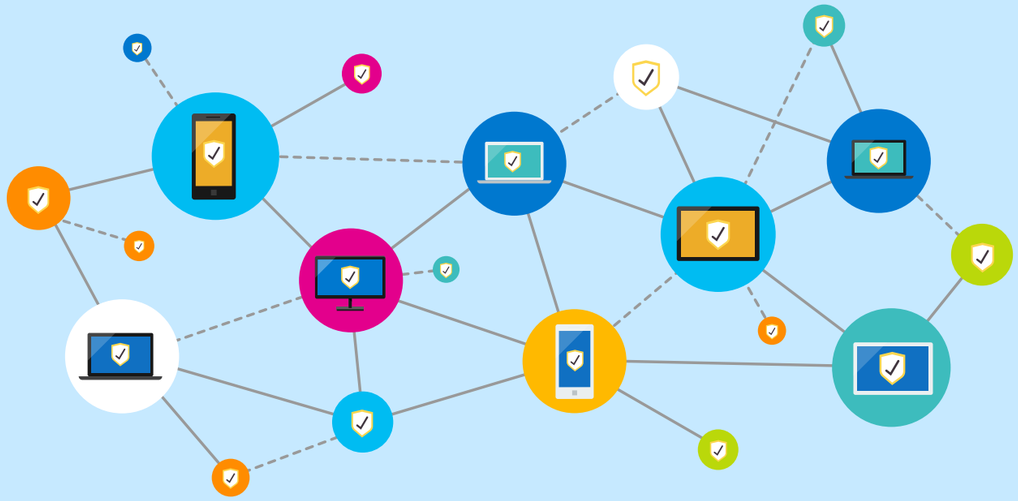
デバイスごとのセキュリティ対策や、社員がどんなクラウドサービスに接続し、

どんなアプリを使っているのかを把握して一元管理できる Microsoft Intune を使えば、

セキュリティ対策の強化と管理業務の手間・コストの削減を同時に実現することができます。

リモートでデバイスのセキュリティ管理ができるの？

これまではデバイスごとにセキュリティ対策ソフトで個別に管理する必要がありましたが、
Microsoft Intune には、登録デバイスのセキュリティを一元管理する機能が備えられています。
危険にさらされたデバイスを特定、修復し、安全な状態に復元します。
また、Windows のウイルス対策プログラム「Microsoft Defender ウィルス対策」の
基本設定を行う UI も用意されており、より高度なセキュリティ機能の追加も可能です。

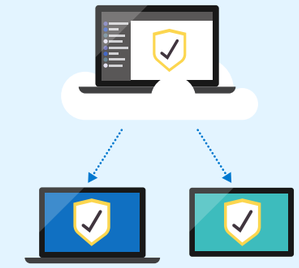


HINT!

さまざまな機能で確かなセキュリティ対策！

対策 1　エンドポイントのセキュリティ設定

遠隔操作でデバイスの安全を確保し、脅威から保護することができます。Windows デバイス用の Microsoft 推奨設定である「セキュリティ ベース ライン」や「Microsoft Defender ウイルス対策」などの各種セキュリティ設定が用意されています。



対策 2　「Microsoft Defender ウィルス対策」レポート

「Microsoft Defender ウィルス対策」の状況やウイルスの感染状況をレポートする機能を利用することができます。（ウイルス感染時のメール通知が必要な場合は、別途「Microsoft Defender for Endpoint」の含まれるライセンスが必要となります。）

対策 3　「Microsoft Defender for Endpoint」との連携

クラウド ベースのエンドポイント セキュリティ統合プラットフォーム サービスである Microsoft Defender for Endpoint と 連携すれば、各デバイスのリスクレベルに応じた条件付きアクセス、セキュリティタスクの管理、自動調査と修復といっ た、より高度なセキュリティ機能を利用できます

デバイスの安全を常に監視したい

デバイスは、24 時間 365 日セキュリティリスクにさらされています。
Microsoft Defender for Endpoint は、エンドポイントである
デバイスがサイバー攻撃を受けることを前提とした
EDR（Endpoint Detection and Response）製品。
セキュリティの脅威をいち早く検知・除去し、被害を最小限に抑えたうえで修復します。

HINT!

Microsoft Defender for Endpoint が常にデバイスを監視し、あらゆる脅威に対処！

対処 1

インフラ構築不要のクラウド サービス

クラウドベースの EDR ツールであり、インフラを構築する必要もサーバーを用意する必要もありません。遅延や更新プログラムの互換性の問題もなく、常に最新の状態を保ちます。

対処 2

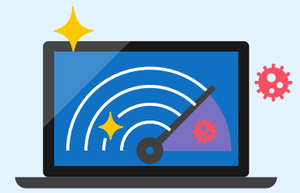
脅威の可視化と分析によるサポート

マイクロソフトが持つ莫大なデータとエンドポイントであるデバイスから収集したデータを組み合わせて分析することで、セキュリティ上の異常をいち早く検知し、適切に対処します。

対処 3

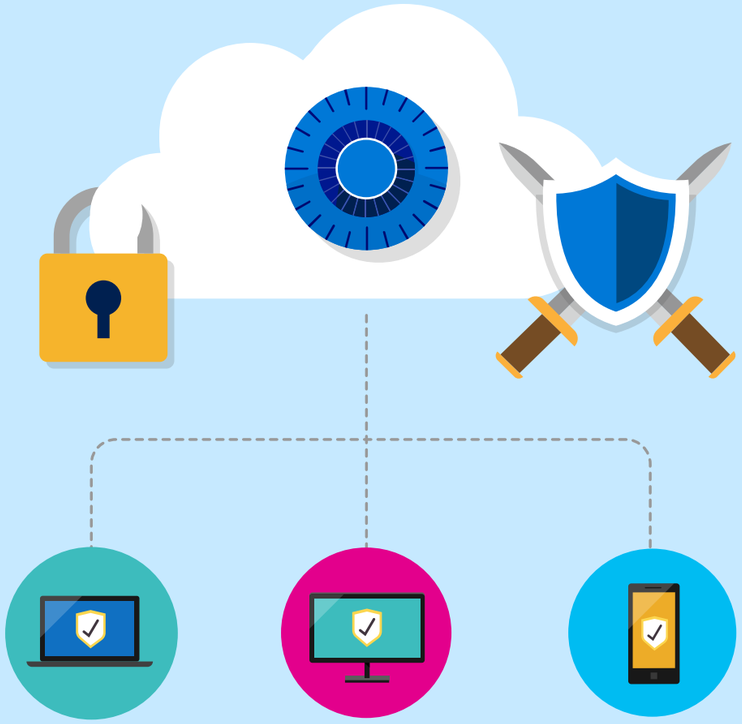
自動で脅威を検知・迅速な修復対応

脅威を検知すると、アラートから修復までわずか数分で対応。高度な行動分析と機械学習を用いて、未知の脅威や複雑な脅威であっても対処可能。攻撃の予兆まで認識することができます。



脅威への備えを万全にしたい

社内と社外の境界線があいまいなハイブリッド ワーク時代を迎えた今、
脅威に備える方法として「ゼロトラスト アプローチ」が注目されています。
ゼロトラストとは、脅威が侵入してくることを前提に、ユーザーに最小権限のアクセスを与え、
あらゆるアクセスを明示的に常に確認するという考え方です。
Microsoft Defender for Endpoint は、ゼロトラスト アプローチに基づいて、
セキュリティ対策のために必要な情報を提供します。



HINT!

Microsoft Defender for Endpoint が管理者が知りたい情報を確実にご提供!

提供 1

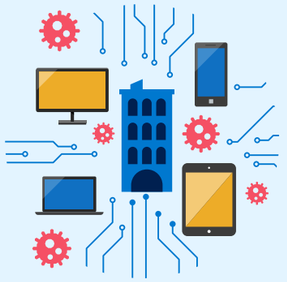
世の中の脅威情報を把握したい

- 流行している脅威の一覧
- それぞれの脅威の概要
- アナリストの詳細レポート
- 自組織での対策状況

提供 2

組織に脆弱性がないか確認したい

- 自組織の全体的なスコア
- セキュリティの推奨事項
- 脆弱性への対応状況
- 対応の指示と管理



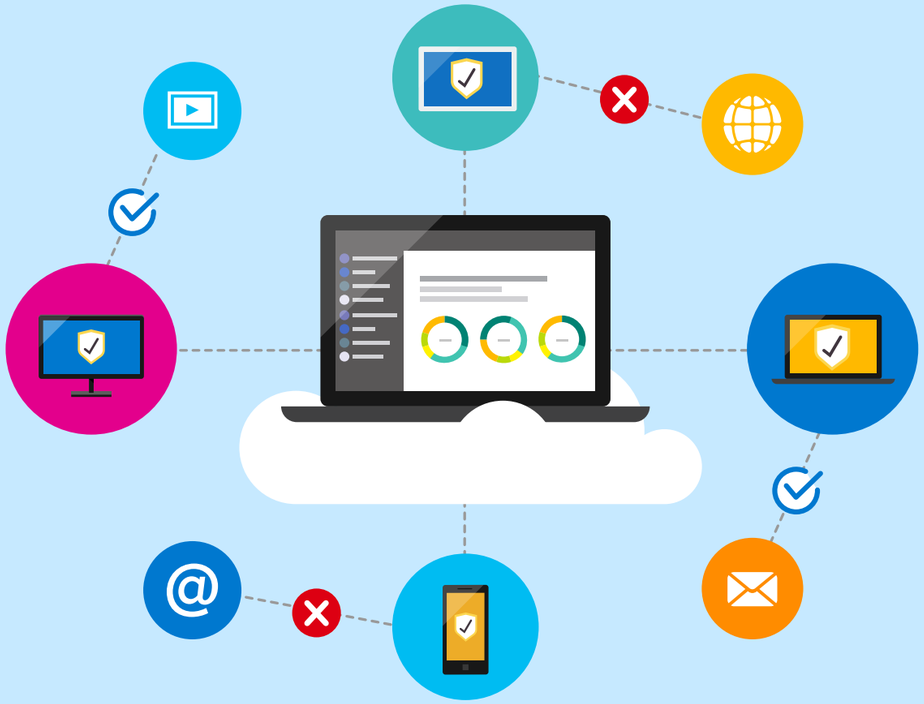
提供 3

組織の健全性を確認したい

- 脅威の発生・保護の状況
- デバイスの健全性
- Web アクセスの保護状況
- カスタムレポートの作成

社外ネットワーク利用時のリスクを減らしたい

リモートワーク時には、セキュリティに不安のある外部ネットワークからも、
業務データにアクセスする可能性があります。
また、社内で使用が許可されていない外部サービスや、
個人で所有しているデバイスを業務で無断使用するシャドウ IT 対策も課題となっています。
Microsoft Defender for Endpoint では、
デバイスのセキュリティ対策の状況やクラウドアプリの利用状況を、
クラウド上で一元管理できます。



HINT!

Microsoft Defender for Endpoint が非信頼ゾーンでもエンドポイントで制御！

制御 1

Web フィルタリング機能

Web サイトの閲覧許可や閲覧禁止を簡単に登録でき、カテゴリでフィルタリングして、有害サイトへのアクセスをブロックすることもできます。この機能により、情報漏洩やウィルス感染などのリスクを低減することができます。

制御 2

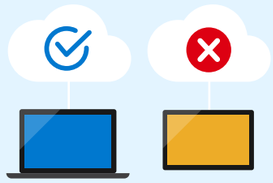
セキュリティ ベースライン設定

マイクロソフトのセキュリティ推奨設定のテンプレートを使って、ウィルス対策やファイアウォールの構成、悪意ある Web サイトからの保護など、ポリシーに即して各端末へのセキュリティを設定できます。

制御 3

Cloud App Security でシャドウ IT を検出・制御

Microsoft Defender for Endpoint と Cloud App Security を連携させることで、登録デバイスからアクセスされているクラウド サービスを検出、利用の可否を制御できます。未承認アプリについても、使用時にアラートを出すなどして制御することが可能です。



第 4 章

ハイブリッド ワーク時代の デバイス選び編

オフィスとそれ以外の場所とでワークスタイルを柔軟に切り替えるハイブリッドワークの時代においては、

多様な働き方に対応可能かつ安心して快適に使えるデバイスを選ぶことが重要です。

この章では、コミュニケーションの質と業務のパフォーマンスを高めるデバイス選びに役立つポイントをまとめました。

ハイブリッド ワークを快適にこなすためのノート PC 選び

これからのノート PC には、持ち運んだり、いろいろなスペースで作業したりと、
これまでの社内デスクだけで使う場合とは異なる使い方に合わせた機能が求められます。
PC としてのスペックはもちろん、機動性や安全性、リモートワークへの対応力など、
快適なハイブリッドワークのための機能や特徴を備えたノート PC を選びましょう。

HINT!

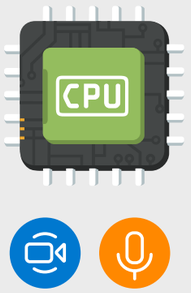
ハイブリッド ワークに合わせたノート PC 選びのポイント

POINT 1　安心・安全に使えること

- マルウェアなどの侵入からリアルタイムで保護
- 常に最新のセキュリティ対策が可能な Windows 10 Pro 搭載
- 起動時のパスワードに加え、顔認証などの多要素認証に対応

POINT 2　生産性を高められる機能があること

- ビジネスユースを最優先にデザインされた Windows 10 Pro 搭載
- Web 会議に対応するカメラやマイクがついていること
- 処理速度の速いストレージ
- CPU は Core i5、メモリは 8 GB 以上



POINT 3　持ち運びしやすいこと

- 薄くて軽いボディ
- 衝撃や振動に強い堅牢性
- 長持ちするバッテリー

ハイブリッド ワーク対応の Surface シリーズ

Microsoft Surface

Surface Go 3

最もポータブルなタッチスクリーンの 2-in-1
スマートで軽快な働き方を求める人へ。

SPEC

CPU	第 10 世代 Intel® Core™ i5-1035G1
メモリ	4 ～ 8 GB
SSD（eMMC）	64 ～ 128 GB
画面サイズ	10.5 インチ PixelSense™タッチスクリーン ディスプレイ
バッテリー持続時間	最大約 11 時間
重量（最軽量）	約 544 g～

POINT

第 10 世代 Intel® Core® i3 プロセッサを搭載した、
544 グラムのポータブル デバイス。

3 つのモードで限りない柔軟性を実現する、調整可能なキックスタンド。

鮮明な 10.5 インチ タッチスクリーン ディスプレイで作業が容易に。

最大 11 時間のバッテリーにより、1 日中生産性を維持。
LTE Advanced 接続モデルもご用意。

Surface Pro 8

場所や時間を気にせず、
オフィス同様の環境で仕事をしたい人へ。

SPEC

CPU	第 11 世代 Intel® Core™ プロセッサ
メモリ	8 ～ 32GB
SSD（eMMC）	128 ～ 1 TB
画面サイズ	13 インチの PixelSense™ Flow タッチスクリーン ディスプレイ
バッテリー持続時間	最大約 16 時間
重量（最軽量）	約 899 g～

POINT

アクティブ冷却機能搭載の第 11 世代 Intel® Core™ プロセッサ

ペンがさらに使いやすく - Signature キーボードに
Surface スリム ペンを収納して充電可能

ノート PC のようなパフォーマンスを実現する、
スタイリッシュでコンパクトな Surface Pro Signature キーボード

最大 120Hz のリフレッシュ レートで、ペンの応答性が高まり、
滑らかな操作に。

Surface Laptop Go

よりコンパクトなノート PC で、
フレキシブルな働き方をする人へ。

SPEC

CPU	第 10 世代 Intel® Core™ i5-1035G1
メモリ	4 ～ 16 GB
SSD（eMMC）	64 ～ 256 GB
画面サイズ	12.4 インチ PixelSense™タッチスクリーン ディスプレイ
バッテリー持続時間	最大約 13 時間
重量（最軽量）	約 1,110 g

POINT

わずか 1,110g の Surface Laptop Go なら、
どこにでも持ち歩きが可能。

最大 13 時間の長時間バッテリーと急速充電機能 により、
複数のミーティングが続く日も、1 日中安心。

高音質の Omnisonic スピーカー、Dual far-field スタジオマイク、
720p HD のフロントカメラを搭載し、リアルなオンライン会議を実現。

Windows Hello と One Touch サインインで、瞬時にファイルやデータへ
セキュアにアクセス可能です。さらに指紋認証対応。

Surface Laptop 4

会議も集中も。すべての仕事で
パフォーマンスを発揮したい人へ。

SPEC

CPU	AMD Ryzen™ 5 4680U Microsoft Surface® Edition AMD Ryzen™ 7 4980U Microsoft Surface® Edition 第 11 世代 Intel® Core™ i5-1145G7 第 11 世代 Intel® Core™ i7-1185G7
メモリ	8 ～ 32 GB
SSD（eMMC）	256 GB ～ 1 TB
画面サイズ	13.5 / 15 インチ PixelSense™タッチスクリーン ディスプレイ
バッテリー持続時間	最大約 13 時間
重量（最軽量）	約 1,265 g ～ 1,542 g

POINT

高いマルチタスク処理能力と最大 70% の
高速化を実現した CPU を搭載。

指 1 本で開閉できる革新的なデザイン、薄くて軽 いエレガントなボディ。

暗い場所でも高画質のビデオ通話が可能な f 値 2.0 の明るい
720 HD フロントカメラと、立体音響の Dolby Atmos® を搭載。

Instant On 機能によりディスプレイを開くだけですばやく作業に復帰。
パスワード不要の Windows Hello なら、安全にサインインが可能。

製品の詳細は Surface.com をご覧ください。

高度なセキュリティ機能をオールインワンで提供

Microsoft 365 E5 では、新時代のビジネス環境に必要な
「ID 保護」「脅威対策」「情報保護」「クラウドセキュリティ」の
4 つのセキュリティ機能がまとめて提供されます。
あとから機能を追加しなくても、Azure AD をはじめとする
さまざまなセキュリティ機能を提供するサービスを常に最新の状態で利用できるため、
各機能を連携させて包括的に組織全体を守ることができます。
同時に、自動化によって管理者の負担も軽減できます。

	Microsoft 365 E3	Microsoft 365 E5
ユーザー / 月	詳しくは、販売パートナー様へお問合せください	
含まれる Office アプリ	Outlook, Word, Excel, PowerPoint, Access, Publisher（Access、Publisher は Windows PC のみ）	
含まれるクラウドサービス	Exchange, OneDrive, SharePoint, Teams, Bookings, Sway, Lists, Yammer, Stream, Power Apps, Power Automate, Planner, ToDo, MyAnalytics	
1 ライセンスでのインストール	最大 5 台の Windows PC / Mac （Web・モバイル版と合わせて最大 15 台のデバイス）	
デバイスとアプリの管理	○	○
アイデンティティとアクセスの管理	△ ※	○
脅威対策	△ ※	○
情報保護	△ ※	○
セキュリティ管理	○	○
コンプライアンス管理	△ ※	○

※詳しくはこちらをご確認ください。https://www.microsoft.com/ja-jp/microsoft-365/compare-microsoft-365-enterprise-plans

Microsoft

ご購入前のご相談は「セキュア リモートワーク相談窓口」

0120-167-400

（営業時間：9:00 ～17:30 土日祝日、弊社指定休業日を除く）

詳しくはこちらから

https://www.microsoft.com/ja-jp/microsoft-365

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