# 【Microsoft Defender for Endpoint】サービス概要

2025年6月30日

# 改訂履歴

| 版数 | 発行日 | 改訂内容 |
| --- | --- | --- |
| 第1版 | 2025年6月30日 | 初版発行 |

本資料の内容は 2025/6/30 時点のものです。製品のアップデートにより変更となる場合がございます旨ご了承ください。

# Agenda

1. 前提情報
    1. 用語集
    2. 資料の構成と目的
2. Microsoft Defender for Endpoint とは
    1. Microsoft Defender とは
    2. Microsoft Defender for Endpoint とは
    3. 他製品との比較
    4. 導入直後の自動防御とその後の運用フェーズの違い
3. Microsoft Defender for Endpoint の主な機能
    1. Microsoft Defender for Endpoint の主な機能
    2. 自動攻撃かく乱
    3. セキュリティ運用支援AI
    4. おとり資産の自動展開
    5. 優先度付きセキュリティ態勢の推奨事項
    6. 柔軟なエンタープライズ コントロール
    7. ネットワークの検出と応答
    8. シンプルなエンドポイント管理
4. Microsoft Defender for Endpoint プラン比較
    1. Microsoft Defender for Endpoint プラン比較
    2. Microsoft Defender for Endpoint の各プランを含む Microsoft 365 ライセンス比較
    3. Microsoft Microsoft Defender for Business で利用できる機能
    4. Defender for Endpoint P1 で利用できる機能
    5. Microsoft Defender for Endpoint P2 で利用できる機能
    6. プラン選択のポイント

# 1. 前提情報

# 1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

| No. | 用語 | 説明 |
|---|---|---|
| 1 | EDR（Endpoint Detection and Response） | エンドポイント（PCやサーバーなど）を監視し、不審な挙動を検知・調査・対処するセキュリティ製品。攻撃後の調査や事後対応に強みを持つ。 |
| 2 | XDR（Extended Detection and Response） | EDRの対象範囲を拡張し、ネットワーク、クラウド、メールなど複数のセキュリティデータを統合して脅威を検出・対応する仕組み。 |
| 4 | C2通信（Command and Control） | 攻撃者が侵入後にマルウェアと通信し、命令を送ったり情報を取得したりする通信。早期検出が重要。 |
| 5 | デコイ（Decoy） | 攻撃者を誘い込む偽物のシステムやデータ。攻撃の動きを監視・分析するために設置される。 |
| 6 | ルアー（Lure） | デコイに誘導するための罠となるデータやファイル。攻撃者の行動を促すために配置される。 |
| 7 | CVE（Common Vulnerabilities and Exposures） | 公開された脆弱性情報の識別番号。<br>中でも「既知の悪用脆弱性（Exploited CVE）」は、実際に攻撃に使われているリスクの高い脆弱性。 |

# 1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

| No. | 用語 | 説明 |
|---|---|---|
| 8 | ロールベースアクセス制御（RBAC） | ユーザーの役割（ロール）に応じて、アクセス権限を管理する方法。最小権限の原則を実現しやすい。 |
| 9 | 攻撃面縮小（ASRルール） | マクロ、スクリプトなど悪用されやすい機能を制限し、攻撃の足がかりを減らすセキュリティ機能。 |
| 10 | Kerberos | ネットワーク認証プロトコル。チケットを使って安全な通信を実現し、ユーザーの身元を確認する。 |
| 11 | LDAP（Lightweight Directory Access Protocol） | ディレクトリサービスにアクセスするためのプロトコル。ユーザー情報やグループ情報の管理に使用され、検索や認証を行う。 |
| 12 | SMB（Server Message Block） | Windows環境でよく使われるファイル共有・プリンタ共有の通信プロトコル。過去に多くの攻撃対象にもなっている。 |

# 1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

| No. | 用語 | 説明 |
|---|---|---|
| 13 | RDP<br>（Remote Desktop Protocol） | リモートでPCやサーバーに接続するためのWindows標準の通信プロトコル。ブルートフォースや脆弱性攻撃の対象になりやすい。 |
| 14 | Large Language Model<br>（LLM：大規模言語モデル） | 膨大なテキストデータを学習し、人間の言語を理解・生成できるAIモデルのこと。<br>自然な文章の生成、質問への回答、要約、翻訳、コード作成などに活用される。<br>Microsoft Security  Copilotはセキュリティ分野に特化した代表的なLLMの応用例。 |
| 15 | Machine Learning<br>（ML：機械学習） | 人が明示的にルールを教えなくても、データからパターンを学習し、判断や予測ができるAI技術の一分野。<br>不正アクセスの検知、商品のレコメンド、音声認識など、様々な分野に使われている。 |
| 16 | 脆弱性 | システムやソフトウェアの設計・実装上の欠陥や弱点のこと。<br>攻撃者が侵入の起点として狙う箇所になる。 |
| 17 | ランサムウェア暗号化 | 攻撃者がマルウェアを使ってPCやファイルの中身を勝手に暗号化し、利用者が使えない状態にする攻撃手法。 |

# 1.2. 資料の構成と目的

**■ エンドポイントのセキュリティを強化**

エンドポイント（PCやサーバーなど）を狙った攻撃が急増する中、 企業はマルウェア感染や情報漏えいを未然に防ぎ、インシデント発生時も迅速に対応できる体制を整えることが求められています。
Microsoft Defender for Endpoint は、エンドポイントを監視・防御・検知・対応するための高度な機能を提供し、組織の情報資産を保護します。

**■資料の構成**

本資料では、第2章で Microsoft Defender for Endpoint の概要について説明します。

第3章では、Microsoft Defender for Endpoint の主要機能について機能概要、利用時のポイントを解説します。

最後に、Microsoft Defender for Endpoint 各プランと機能を比較し、組織に最適なプランを選択するための情報を提供します。

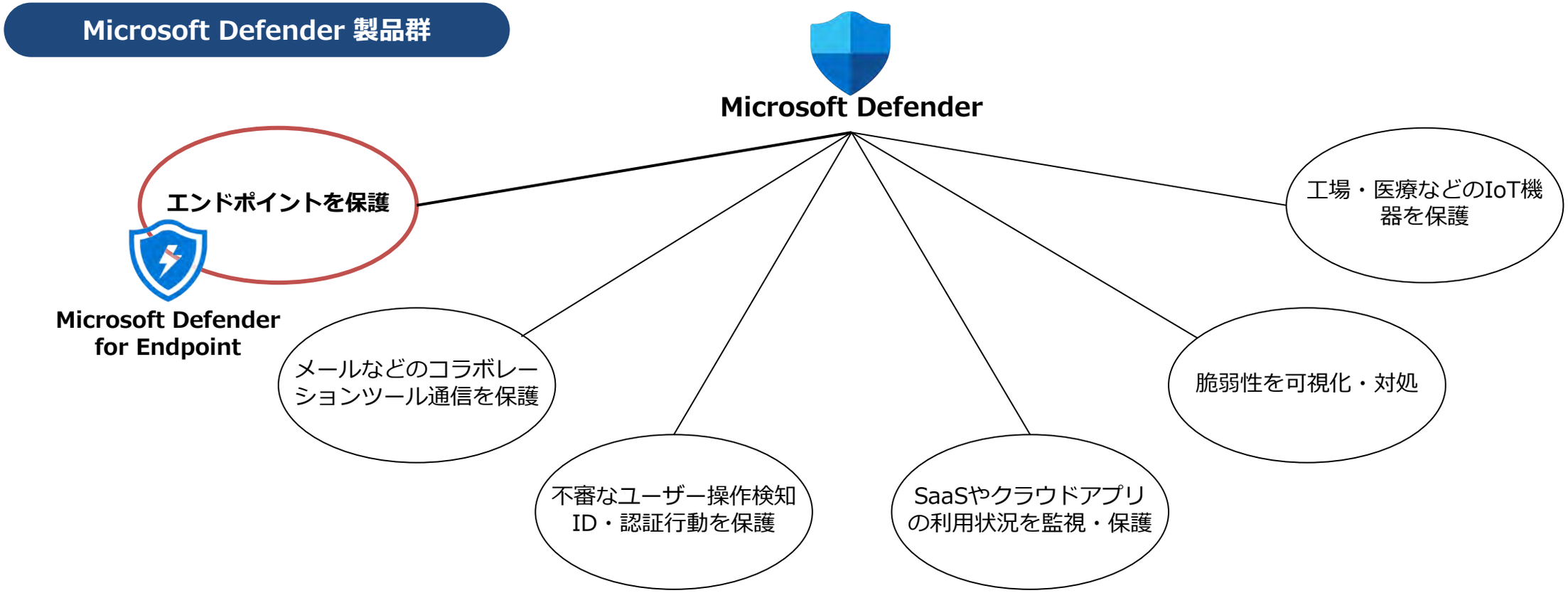
**■資料の目的**

Microsoft Defender for Endpoint の導入に際して、Microsoft Defender for Endpoint の機能や利用時のポイントをまとめたナレッジを提供し、ライセンス選定や組織の運用設計を支援します。

# 2. Microsoft Defender for Endpoint とは

# 2.1. Microsoft Defender とは

Microsoft Defender とは、Microsoftが提供する、多様な環境を保護するためのセキュリティ製品群です。
エンドポイント（PCやスマートフォンなどの端末）からクラウド環境まで、幅広い領域のセキュリティを強化する複数のサービスが含まれています。
本資料では、この中でもエンドポイントを対象に脅威の検出・対応を行う Microsoft Defender for Endpoint についてご紹介します。



# 2.2. Microsoft Defender for Endpoint とは

Microsoft Defender for Endpoint は、Microsoft 社が提供するセキュリティ製品群「Microsoft Defender」シリーズの一つで、エンドポイント（PCやスマートフォンなどの端末）を保護するためのセキュリティサービスです。
マルウェア対策に加え、脆弱性の管理や攻撃経路の削減、AIを活用した攻撃検知と自動対応（EDR）、Microsoftが保有する最新の脅威情報活用などの保護機能を提供し、巧妙化するサイバー攻撃に対して多層的なエンドポイント防御を実現できます。

## Microsoft Defender for Endpoint の利用目的

**■エンドポイント保護の強化**
防御AIとグローバル脅威インテリジェンスを活用し、未知の攻撃手法を含めた様々なサイバー攻撃をリアルタイムで検知・防御します。
感染リスクを低減し、常にエンドポイントの安全性を維持できます。

**■インシデントの可視化と迅速な初動対応**
検知された脅威情報はDefenderセキュリティポータルに集約され、攻撃の全体像や影響範囲を可視化できます。
自動調査と修復機能により、迅速な初動対応と被害拡大防止を実現します。

**■脆弱性の把握と事前対策**
エンドポイントの脆弱性情報を常時収集・分析し、優先順位を付けた修正提案を提示します。
これにより重要な脆弱性から優先的に対処でき、攻撃を受ける前に予防的なセキュリティ対策を実施できます。

**■セキュリティの一元管理**
Microsoft Intune などと連携し、端末の管理・セキュリティ対策・アクセス制御を統合管理できます。
Microsoft 365ライセンスに含まれるため、追加ツールの導入コストを抑えながら、管理負荷の少ない運用が可能です。

# 2.3. 他製品との比較

Microsoft Defender for Endpoint のようなエンドポイント向けのセキュリティサービスは、EDR (Endpoint Detection and Response)、および XDR (Extended Detection and Response) と呼ばれるカテゴリに分類されます。
従来のウイルス対策製品はマルウェア検知が主な目的でしたが、EDR/XDR では「不審な侵入検知」「攻撃の被害範囲特定」「自動で感染端末隔離・修復」などの機能が提供されます。

各製品によって提供機能や連携の柔軟性が異なるため、組織のセキュリティ方針や運用体制に合わせた製品選定が重要です。

■製品を選ぶ基準の例

・マルウェア検知だけでなく、侵入後の封じ込めや修復まで対応できるか
・運用負荷を軽減する自動化、可視化機能が充実しているか
・ゼロトラストや最新のセキュリティ要件に対応しているか
・Microsoft 365や他の既存環境と統合できるか

代表的な EDR/XDR 製品を比較すると以下のようになります。

| 項目 | Microsoft Defender for Endpoint | CrowdStrike | SentinelOne | Trend Micro Vision One |
|---|---|---|---|---|
| **運用負荷軽減**<br>（管理ポータルの統合度・操作性） | 高い | 中程度 | 中程度 | 中程度 |
| **自動対応力**<br>（検知後の自動隔離・修復） | 非常に高い | 高い | 高い | 中程度 |
| **ゼロトラスト適合性** | 高い | 中程度 | 中程度 | 中程度 |
| **Microsoft 製品との連携** | 非常に高い | 中程度 | 中程度 | 中程度 |

# 2.4. 導入直後の自動防御とその後の運用フェーズの違い

Microsoft Defender for Endpoint は導入するだけで、多くのセキュリティ機能が自動で有効化され高い防御力を発揮します。
しかし、高度な防御や組織に最適化した運用を実現するためには、追加設定や外部連携などの管理者による運用が必要です。
本スライドでは、導入するだけ（Microsoft Defender for Endpointの監視対象として端末が認識されていて追加設定はしていない状態）で自動的に守られる範囲と、どこから人の管理・対応が必要になるのかを整理します。

**導入だけで自動で機能する領域**

### 攻撃侵入

**脅威の検出と初期判断**
・Microsoft Defender for Endpoint を導入したエンドポイントには、常駐エンジンと AI による脅威検出が適用される
・既知のマルウェアや不審な通信は自動で検出

### 感染・初期挙動

**自動検出と初期修復アクション**
・不審な動作やファイルを自動で検出・隔離

自動実行される修復アクションの例
・悪性ファイルの隔離
・不審プロセスの強制終了
・スクリプトやマクロの実行ブロック
・スケジュールされたタスクの削除

### 横展開・情報流出

**脆弱性の可視化と優先付け**
・エンドポイントの脆弱性情報を収集し、リスクの高い端末を可視化
・対応優先度の提案

### 修復対応・再発防止

**自動対応は一部に限定される**
※Defender は修復アクションを提案しますが、実行には管理者がポータル上で個別に操作する必要があります。
（複数端末への一括適用は Intune との連携が必要）

# 2.4. 導入直後の自動防御とその後の運用フェーズの違い

**管理者対応が必要な領域**

| 攻撃侵入 | 感染・初期挙動 | 横展開・情報流出 | 修復対応・再発防止 |
| --- | --- | --- | --- |
| **柔軟なセキュリティ設定**<br>組織の業務アプリ・運用に合わせて許可・ブロック動作を最適化 | **アラート検知ルール・対処方針の調整**<br>・誤検知対策<br>・優先度ルールの調整<br>・不審なファイル等を隔離後の手動確認や復旧判断 | **脆弱性対策の実施**<br>・パッチ適用や設定変更の適用<br>・他製品との連携設定（Intune・Entra IDなど）<br>・アラート相関分析、過去の影響調査、ログ調査など | **恒久対応と分析**<br>・再発防止のためのアラート振り返りや Defender による調査結果・分析レポートの確認<br>・Intuneポリシーの強化、対応プロセスの見直し、デバイス保有者や管理者への教育・訓練など |

# 2.4. 導入直後の自動防御とその後の運用フェーズの違い

## 導入だけで自動で機能する領域

Microsoft Defender for Endpoint を導入すると、既定のセキュリティベースラインに沿った防御機能が自動的に有効化されます。
これは Microsoft が推奨する構成をもとに設計されており、**初期状態でも高い防御力を発揮**できるようになっています。

マルウェアの検出や脆弱性の可視化など多くの防御アクションが導入後すぐに開始され、管理者が設定を調整しなくても、ある程度の攻撃は初動で自動的にブロックされます。

## 管理者対応が必要な領域

一方で、セキュリティ対策を組織の状況や業務ニーズに最適化するには、運用フェーズでの管理者対応が不可欠です。
アラート対応の基準策定、外部サービスとの連携構成など、判断が求められる場面が多く存在します。

アラートの傾向分析や恒久対策の検討、ユーザーへの影響評価など、より高度なセキュリティ運用を実現するには、継続的な管理体制が必要です。
Microsoft Defender for Endpoint はこうした**対応も支援しますが、最終的な意思決定と行動は人の介入が必要**な領域となります。

## 外部連携（Intune など）について

Microsoft Defender for Endpoint は、単体の導入・運用だけで、脅威の検出や隔離、一部の自動修復、管理者による手動対処といった十分なセキュリティ保護機能を提供します。
Intune などとの外部連携は、新たな防御機能を追加して**セキュリティ対策の範囲を広げるものではなく、運用効率や大規模運用への拡張性を高めるための手段**です。修復アクションの一括適用（Defender 単体では対象デバイスごとに手動実行）、ポリシーの自動展開（単体ではセキュリティ設定の設計から適用まで全て手作業）など、外部連携によって運用の大規模化・自動化を支援する機能が得られます。

# 3. Microsoft Defender for Endpoint の主な機能

# 3.1. Microsoft Defender for Endpoint の主な機能

Microsoft Defender for Endpoint で主要とする機能は以下のようなものがあります。各機能についての詳細は次のページから紹介します。

| 主な機能 | 機能概要 |
| --- | --- |
| 自動攻撃かく乱 | 攻撃の進行をリアルタイムで遮断し、被害拡大を防ぐ |
| セキュリティ運用支援AI | Microsoft Security Copilot：Large Language Model（LLM系）AI が脅威検知内容の要約・影響分析・対応策を自動提示し、専門知識がなくても迅速に対応できる<br>グローバル脅威インテリジェンス：Machine Learning（ML系）AI がMicrosoftが収集・分析する毎日45兆件以上の脅威シグナルをもとに、最新の攻撃手法にも自動で対応する |
| おとり資産の自動展開 | 攻撃者を欺く偽の資産を自動展開し、攻撃者の動きを監視・誘導して侵害を早期検出し攻撃パターンを把握する |
| 優先度付きセキュリティ態勢の推奨事項 | 端末の脆弱性情報を分析し、優先度を付けた修正提案を提示 |
| 柔軟なエンタープライズ コントロール | Intune等と連携し、ポリシー適用・端末制御・ゼロトラストによるアクセス制御を柔軟に管理できる |
| ネットワークの検出と応答 | エンドポイント内のネットワーク通信も監視対象とし、侵害拡大や外部通信も検知する |
| シンプルなエンドポイント管理 | Defender セキュリティポータルでインシデント・端末状態・脆弱性を一元管理 |

# 3.2. Microsoft Defender for Endpoint の主な機能
## 自動攻撃かく乱

自動攻撃かく乱は、攻撃の侵入後に行われる横展開やランサムウェアの暗号化などの挙動をAIでリアルタイムに監視し、攻撃の進行を自動でかく乱・遮断する仕組みです。
攻撃が拡大する前に封じ込め、被害を最小限に抑えます。

Microsoft Defender for Endpoint の自動攻撃かく乱は、以下のアクションを自動実行します。
・ネットワーク隔離：感染が疑われる端末をネットワークから切り離し、横展開やC2通信を遮断
・セッション切断　：攻撃者が侵害端末にリモート接続中の場合、強制的にセッションを切断
・プロセス強制終了：暗号化など悪質なプロセスを検出し、停止
・自動修復　　：悪性ファイルの削除、設定改変の修復などを実行

### メリット

**■被害拡大の防止**
・攻撃の兆候を即座に検知し、自動で攻撃経路を遮断できる

**■運用負荷の軽減**
・管理者の対応前に自動で攻撃をかく乱、遮断する

**■迅速な初動対応による復旧時間の短縮**
・初期の侵害段階で遮断できるため、復旧に要する時間やコストを低減

### 注意点

**■適切なポリシー設定が必要**
・AIによる自動判定の精度を高めるため、環境に合わせた適切な初期設定が重要（アラート設計、承認済みソフトウェア登録など）

**■高度な攻撃に対する限界**
・一部の高度な標的型攻撃では100%の遮断が難しいケースもある

# 3.3. Microsoft Defender for Endpoint の主な機能
# セキュリティ運用支援AI

従来のセキュリティ運用では、大量のアラート対応や手動調査が管理者の負担となっていました。
Microsoft Defender for Endpoint では、AIを活用することで調査・分析を自動化して支援し、対応の効率化・高度化を実現します。

## 主な機能

### Microsoft Security Copilot

・管理者の分析・対応を支援する会話型AIアシスタント
・検知されたインシデントの要約や影響範囲の分析、推奨される対処方法を提示し、専門的な知識がなくても迅速な対応を可能にする

### グローバル脅威インテリジェンス

・全Defender製品の防御精度を支える情報基盤
・Microsoftが世界中から収集する毎日45兆件以上の脅威情報を、機械学習AI により継続的に分析・学習する

## メリット

**■インシデント対応の迅速化**
・攻撃内容の要約、影響範囲の特定、対応策を即時提示により、調査時間を短縮
・クラウドベースで常に最新の脅威情報が反映され、進化する攻撃への適応力を維持（未知の攻撃にも自動で防御可能）

**■セキュリティ人材不足への対応**
・自然言語による対話が可能なため、専門知識が浅い管理者でも高度な分析・調査を実施できる

## 注意点

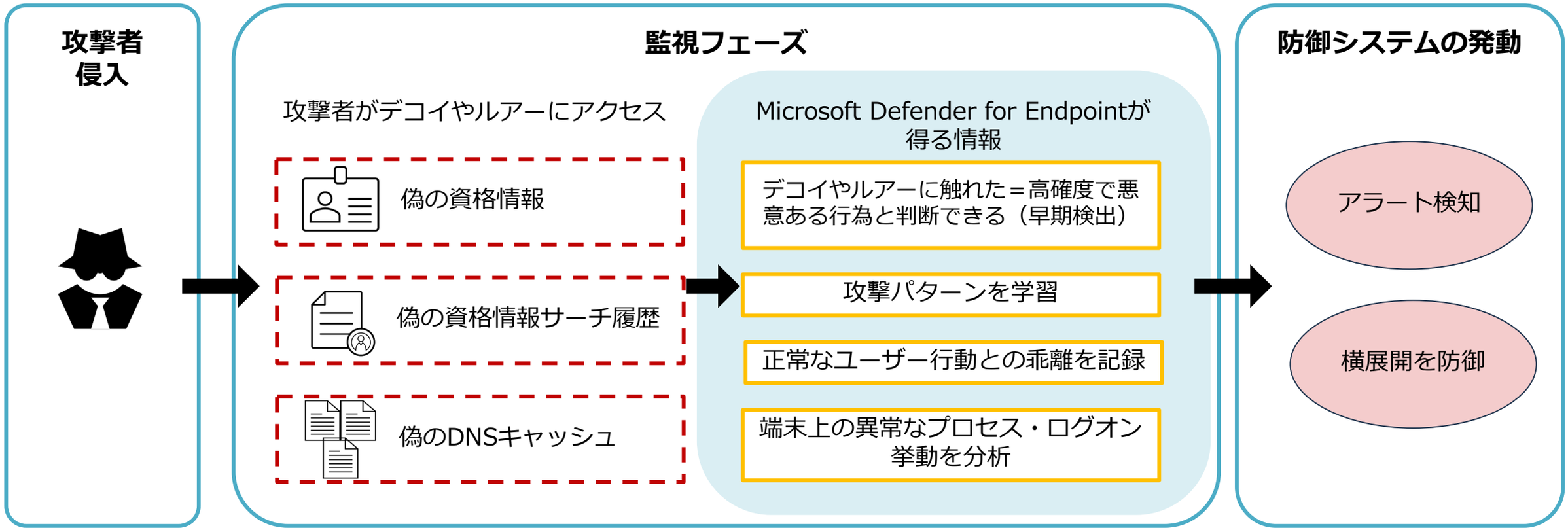
**■AIの提案に対する最終判断**
・AIの出力内容は学習データに基づくため、常に正確とは限らず、最終的な判断は管理者レビューが必要

**■機密データの取扱い注意**
・質問する際の入力内容はMicrosoftのAIモデルに送信・処理されるため、機密情報などの含有には注意が必要
※送信データはAIの学習には利用されませんが、組織の情報管理ルールに従った運用が求められます。

# 3.4. Microsoft Defender for Endpoint の主な機能
# おとり資産の自動展開

おとり資産の自動展開は、攻撃者を欺くための罠となる偽の資産を自動で展開し、攻撃を誘導・監視する仕組みです。
偽のアカウントIDや端末情報（デコイ）、偽の資格情報やファイル（ルアー）が展開されます。
これにより、攻撃の早期検出や手法分析が可能となり、防御体制の強化に繋がります。

## おとり資産の自動展開の機能イメージ



# 3.4. Microsoft Defender for Endpoint の主な機能
## おとり資産の自動展開

### メリット

**■早期検知の実現**
・攻撃者が偽の資産にアクセスした時点で検知できる
・本物の資産へのアクセスを遅らせ、アクセスされる前に検出・遮断できる

**■誤検知リスクが低い**
・正常なユーザーは偽の資産にアクセスする可能性が低いため、アラート検知の信頼性が高い

**■攻撃パターンの学習**
・攻撃手法や経路を分析し、新しい脅威情報の収集に役立てる

### 注意点

**■導入設計の検討が必要**
・業務影響を考慮したスコープ設計が重要

**■見破られる可能性**
・デコイやルアーは攻撃者を欺くよう設計されているが、高度な攻撃者には見抜かれ回避される可能性もある

**■運用における定期的なレビュー**
・環境変化や攻撃手法の進化に対応するため、展開範囲の定期的な見直しが必要（手動対応）

### 偽の資産のスコープ設定

攻撃者の行動を効果的に検知・分析するには、偽の資産（デコイ・ルアー）をどの端末やユーザーに展開するかの設計が重要です。

スコープ設定におけるポイント

・管理者権限を持つ端末や攻撃対象頻度の高い端末に重点的に展開することで、効果的な監視と検知が可能

・通常業務で誤ってアクセス・編集されにくい場所に配置することで、誤検知をさらに減らす設計が可能

# 3.5. Microsoft Defender for Endpoint の主な機能
# 優先度付きセキュリティ態勢の推奨事項

優先度付きセキュリティ態勢の推奨事項は、Microsoft Defender for Endpointがエンドポイントをスキャンし、脆弱性の検出・評価・修復支援までを包括的に行う機能です。

これにより、重要な脆弱性から優先的に対処でき、予防的なセキュリティ対策が実現します。

**主な機能**

### 脆弱性の検出

すべてのエンドポイントに対して、脆弱性や不適切な構成を継続的に監視し検出します。

検出対象はアプリケーション、ブラウザ拡張、証明書など多岐にわたります。

検出結果はMicrosoftの脅威インテリジェンスと照合され、既知の悪用脆弱性（CVE）も識別可能です。

### リスクの優先順位付け

検出されたリスクにはスコアが付与され、対応の優先順位が自動的に決まります。

3要素に基づきスコアが付与されます。
・脅威：実際の攻撃で悪用された、または現在進行中の攻撃で悪用されているか
・侵害の可能性：脆弱性が攻撃者にとって悪用しやすい状態か（パッチ未適用、ポート開放など）
・ビジネス価値：リスクにさらされているデバイスやユーザーの組織上の重要度合

### 修復アクションの支援

優先度の高いリスクに対して、修復アクションを推奨します。

Microsoft Intune と連携することで修復アクションを組織全体に自動展開可能です。管理者は推奨内容を確認し、実行を承認するだけで対処が進みます。

修復アクションの例
・特定のソフトウェアのアンインストール
・アプリ更新
・設定構成変更

# 3.5. Microsoft Defender for Endpoint の主な機能
# 優先度付きセキュリティ態勢の推奨事項

## メリット

**■スコア付与による優先順位付け**
・脆弱性が可視化され優先順位付けされるため、攻撃を受けるリスクの高いものから順に対応できる
・スコアの変化を見れば、何を直せば安全になるかが分かりやすい

**■予防的な対応**
・セキュリティ推奨事項が提示され、攻撃を受ける前に対策を講じることができる

**■管理者向けのレポート提供**
・リスクの高いユーザーやサインインのレポートにより、対策の意思決定を支援

## 注意点

**■スコアの理解が必要**
・リスクに付与されるスコアの意味を正しく理解しないと、過剰対応や見落としにつながる可能性がある

**■統合利用を前提とした機能**
・修復アクションの自動展開にはMicrosoft Intuneとの連携が必要
・未連携の場合、一部機能は利用できない

## セキュリティ推奨事項 とは

Microsoft Defender for Endpointは検出された脆弱性に対して「セキュリティ推奨事項」を提示します。
これにより、修正対象・優先順位・対応方法が明確になり、具体的な修復アクションにつなげやすくなります。
推奨事項には、影響を受けるデバイス数や脅威・悪用の有無なども含まれており、単なるスコアではなく、対応の優先度を判断する実用的な材料として活用できます。

# 3.6. Microsoft Defender for Endpoint の主な機能
# 柔軟なエンタープライズ コントロール

柔軟なエンタープライズ コントロールは、組織の運用体制に応じた柔軟な制御・細かなセキュリティ管理を実現する機能です。
さらに、Microsoft Intune などと連携することで、デバイス管理やセキュリティポリシーの適用を一元化し、ゼロトラストの考え方と統合された高度な運用も可能になります。

**主な機能**

### ロールベースアクセス制御（RBAC）による権限管理

・管理者や閲覧者などの役割を設定できる
・アラート対応、ポリシー編集、閲覧のみなど、役割ごとに操作範囲を細かく制限可能
・Microsoft Defender ポータル上での不必要な操作を防止

### デバイスグループによる柔軟なポリシー制御

・部署や地域、チームごとにデバイスをグループ分けできる
・グループ単位で異なるセキュリティポリシーを設定可能
・運用状況や利用環境に合わせた柔軟な管理ができる
・特定グループだけルールを緩和・強化することも可能

### 柔軟なセキュリティ設定

・マルウェア防止や、攻撃の入り口となる攻撃面縮小（ASRルール）などを細かく設定可能
・警告のみのモニターモードと強制実行モードを切り替え可能
・組織のリスク許容度に合わせた段階的な運用ができる
・新しいルールを段階的に展開することもサポート

### 外部連携による一元管理とゼロトラスト対応

・Microsoft Intuneと連携し、ポリシーの一元管理が可能
・デバイスの準拠状況をリアルタイムで確認できる
・条件付きアクセスによりゼロトラストセキュリティを強化
・PCやスマホなど多様なデバイスを統合的に管理

# 3.6. Microsoft Defender for Endpoint の主な機能
## 柔軟なエンタープライズ コントロール

### メリット

**■柔軟なポリシー適用**

・デバイス状態やユーザー属性に合わせて、細かくセキュリティルールを設定できる

**■ゼロトラスト対応**

・信頼できる状態の端末だけがアクセスできるようにすることで、ゼロトラスト セキュリティを実現できる

### 注意点

**■設計の複雑さ**

・多様な条件や管理ポリシーの設定が必要なため、要件によっては設計が複雑になる可能性がある

・定期的なレビューやポリシーの更新など、運用に伴う負担が増える可能性がある

**■技術的な学習コスト**

・専門的な知識やスキルが必要になるため、管理者の学習に時間とコストがかかる

### ゼロトラスト セキュリティとは

従来の「社内は安全だが、外部は危険」という「境界型防御」に代わる新しいセキュリティアプローチ。

**ネットワーク内外のすべてのアクセスを信頼せず、常に検証する**ことが基本となる。

特にクラウドサービスやテレワークの普及により、従来のセキュリティ方法では不十分とされ、ゼロトラストが注目されている。

Microsoft Entra ID では、条件付きアクセスを使用して、ゼロトラストの概念を実現し、アクセスを動的に制御する。

# 3.6. Microsoft Defender for Endpoint の主な機能
# 柔軟なエンタープライズ コントロール

Microsoft Defender for Endpoint の外部連携例として Microsoft Intune との統合運用をご紹介します。

**概要**

Microsoft Defender for Endpoint と Microsoft Intune を連携することで、
エンドポイントの脅威検出とコンプライアンス評価を統合し、組織内のセキュリティ体制を強化する。

**要件**

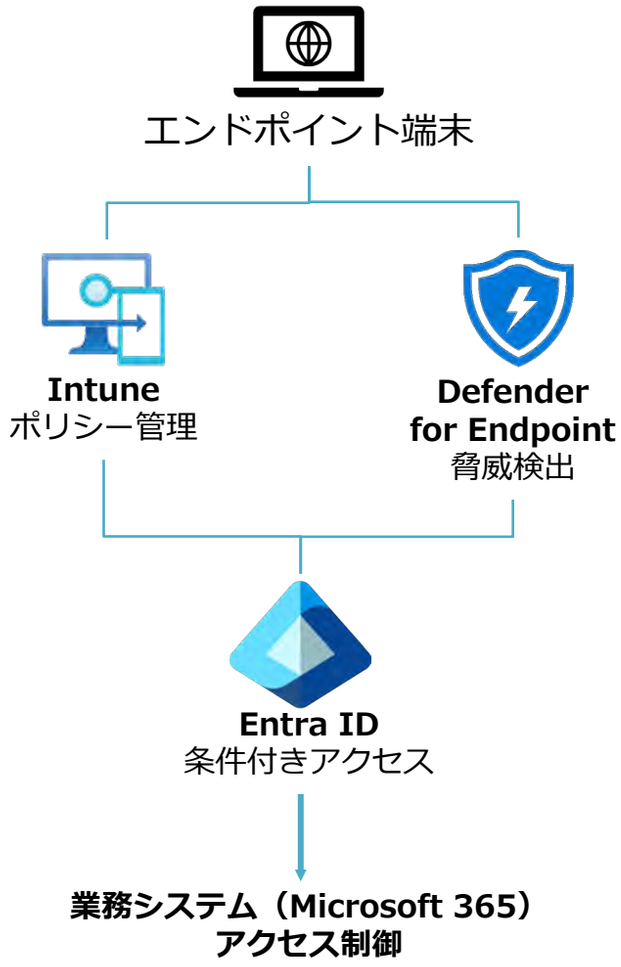
・端末のセキュリティ状態や社内基準に基づき、ポリシー適用やアクセス制御を行いたい
・Defender for Endpoint が提示する修復アクションを、組織内の複数デバイスに対して一括で実行したい

**活用方法**

・Defender for Endpoint がマルウェア検出 ⇒ Intune が該当デバイスに非準拠フラグ ⇒ Entra ID の条件付きアクセスで**業務システムへのアクセスを遮断**
**◆製品の関与：Defender（検知）→ Intune（準拠判断）→ Entra ID（遮断）**

・複数デバイスで同時に脅威を検知 ⇒ Defender for Endpoint が修復アクションを提示 ⇒ Intune が対象デバイスに**修復アクションを一括配信・適用** ⇒ 組織全体で迅速に対処
**◆製品の関与：Defender（修復アクション提案）→ Intune（実行）→ 組織全体に適用される**

・Intune がデバイスの準拠状態をチェック ⇒ Defender for Endpoint のリスク評価（脅威の有無、脆弱性など）を参照 ⇒ Intune がその評価を準拠状態に反映 ⇒ Entra ID の条件付きアクセスでアクセス制御に反映 ⇒ デバイス隔離・リスク再評価・アクセス再許可をリアルタイムに自動化
**◆製品の関与：Intune（準拠状態チェック）↔ Defender（評価）→ Entra ID（アクセス制御）**



# 3.7. Microsoft Defender for Endpoint の主な機能
## ネットワークの検出と応答

Microsoft Defender for Endpointは、エンドポイントだけでなくネットワーク通信も監視対象に含め、侵害拡大や外部通信による情報漏洩などを検出します。ネットワーク上の不審な動きを可視化でき、より包括的な防御が可能になります。

Microsoft Defender for Endpoint が検知できるネットワーク通信は以下の通りです。

| 通信の種類 | 概要 |
| --- | --- |
| **横展開通信** | 社内の他のPCやサーバーに攻撃を広げるためのSMB通信やRDP通信を検知。 |
| **C2通信（攻撃者との通信）** | マルウェアが外部の攻撃者とやり取りする不審な通信を検知。 |
| **異常なプロトコル通信** | 通常とは異なる使われ方をしているLDAP通信やKerberos通信を監視。 |
| **通信とエンドポイント動作の相関** | 通信内容とPC動作を関連付けて分析し、怪しい動作を特定。 |
| **自動対応トリガーとなる通信検知** | 危険な通信を検出した際に、自動でネットワーク遮断やアラート通知を実行。 |

# 3.7. Microsoft Defender for Endpoint の主な機能
## ネットワークの検出と応答

### メリット

**■広域な監視体制**

・エンドポイントだけでなくネットワーク経路の攻撃も可視化するため、広範な監視体制が実現する

・横展開や外部通信による情報漏えいの兆候を早期に検出できる

**■攻撃範囲の可視化**

・ネットワーク上の攻撃拡大状況を把握でき、対応範囲の判断がしやすくなる

### 注意点

**■センサー設置の必要やライセンス考慮**

・対象となるネットワーク機器や範囲には制限がある

・一部機能は追加ライセンスや専用センサーの導入が必要な場合がある

**■ネットワーク負荷に配慮した設計**

・大規模ネットワークでは、通信量に応じた監視設計を行う必要がある

### 導入におけるポイント

監視対象の範囲と機器を事前に整理

・どこまでの通信を可視化したいか、対象とするネットワーク機器を明確化

既存の運用ポリシーと整合性をとる

・管理者の承認が必要な操作や通信の監視に対応できるよう、社内の運用ルールと合わせて検討

段階的に導入・検証を進める

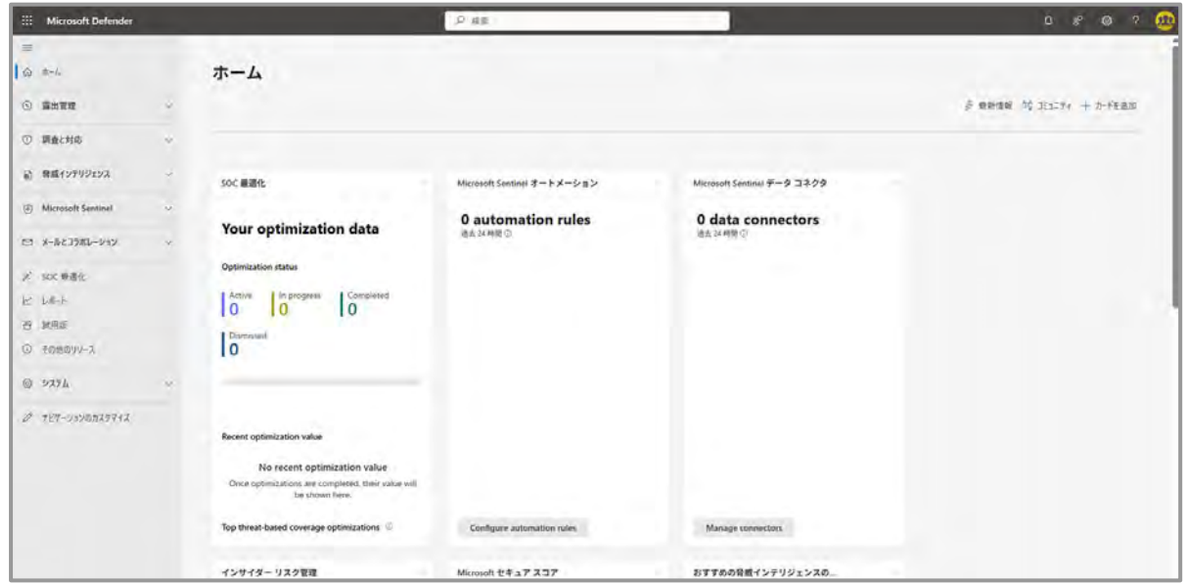
・まずは重要領域からスタートし、効果と負荷を見ながら段階的に展開

# 3.8. Microsoft Defender for Endpoint の主な機能
## シンプルなエンドポイント管理

Microsoft Defender for Endpoint を含む、「Microsoft Defender」製品群の機能を管理できる Web ベースのインタフェースが用意されており、それが **Microsoft Defender ポータル** です。組織の管理責任者、または特権ロールを持つユーザーは Microsoft Defender ポータルにて、エンドポイントのセキュリティ状態監視、脅威のリアルタイム検出、インシデント対応、脆弱性管理などを行います。

### Microsoft Defender ポータルで利用できる機能

・エンドポイントの脅威検出、アラートの監視と管理
・インシデントの調査と対応
・脆弱性スキャンとリスク評価によるセキュリティ強化
・セキュリティポリシーの作成・適用管理
・セキュリティ状況の可視化とレポート作成、その他 新機能のリリース など



# 4. Microsoft Defender for Endpoint プラン比較

# 4.1. Microsoft Defender for Endpoint プラン比較

Microsoft Defender for Endpointの各プランには、基本的なウイルス対策や怪しい動きを監視して自動的に防ぐ機能（改ざん防止やWebコンテンツフィルタリング、ランサムウェア対策など）が共通して備わっています。

上記に加えた他機能については、プランによって利用できる機能が異なります。本章では、Microsoft Defenderのプランについて比較します。

| 機能/Microsoft Defenderプラン | Microsoft Defender for Business | Microsoft Defender for Endpoint Plan 1 | Microsoft Defender for Endpoint Plan 2 |
|---|---|---|---|
| 自動攻撃かく乱 | △ ※1 | △ ※1 | ○ |
| Microsoft Security Copilot | × ※2 | × ※2 | × ※2 |
| グローバル脅威インテリジェンス | ○ | ○ | ○ |
| おとり資産の自動展開 | × | × | ○ |
| 優先度付きセキュリティ態勢の推奨事項 | × | × | ○ |
| 柔軟なエンタープライズコントロール | × | ○ | ○ |
| ネットワークの検出と応答 | × | × | ○ |
| シンプルなエンドポイント管理 | ○ | ○ | ○ |

最新情報は Microsoft公式ページをご確認ください。

※1 エンドポイント単体での攻撃遮断は可能ですが、複数サービス（ID・メール・アプリ・デバイスなど）をまたいだ一括遮断は不可です。フル機能を利用したい場合、基本的にプラン全体のアップグレードが必要となります。
※2 Microsoft Security Copilot は各プランに標準搭載されておらず、利用には別途専用ライセンスが必要です。

# 4.2. Microsoft Defender for Endpoint の各プランを含む Microsoft 365 ライセンス比較

Microsoft Defender for Endpoint の各プランは、Microsoft 365 のライセンスに組み込まれており、ライセンスごとにその内容は異なります。
Microsoft Defender for Endpoint のプランがそれぞれどの Microsoft 365 ライセンスに含まれるかを比較します。

| **Microsoft 365 ライセンス/ Microsoft Defender for Endpoint プラン** | Microsoft Defender for Business | Microsoft Defender for Endpoint Plan 1 | Microsoft Defender for Endpoint Plan 2 |
|---|---|---|---|
| Business Basic | × | × | × |
| Business Standard | × | × | × |
| Business Premium | ○ | × | × |
| Microsoft 365 E3 | × | ○ | × |
| Microsoft 365 E5 | × | ○ | ○ |

最新情報は Microsoft公式ページをご確認ください。

・Defender for Endpoint の各プランは、アドオンとして追加購入が可能です。
・複数のDefender for Endpointライセンス（例: P1とP2、またはDefender for Business）がテナント内で混在する場合、適用される機能や管理方法に複雑性が生じる可能性があります。

# 4.3. Microsoft Defender for Business で利用できる機能

Microsoft Defender for Business は中小企業向けに最適化されたプランであり、Microsoft Defender for Endpoint Plan 1 の簡易版ではなく別コンセプトの並行プランのような位置付けです。
一部ではMicrosoft Defender for Endpoint Plan 2 に近い機能も含まれていますが、利用できる機能や管理の自由度には制限があります。
Microsoft Defender for Business で提供される主な機能とその制限について、以下に一部抜粋しました。

## 提供される機能

**■基本的な脅威検出と防御**

・未知の脅威や、従来のウイルスパターンでは検出が難しい高度な攻撃もリアルタイムで検出
・Microsoft のグローバル脅威インテリジェンスを活用し、エンドポイント単位で攻撃を遮断
制限：調査・分析機能は個別のインシデントに限定され、環境全体を横断的に調べるような高度な手動調査機能は利用不可。
　　攻撃の遮断対象はエンドポイント単位に限定される。

**■脆弱性管理とセキュリティ構成**

・影響を受けるエンドポイントに対してセキュリティ推奨事項を提示し、対応を支援
・専門知識がなくても導入しやすいよう、Microsoft が推奨する既定のセキュリティポリシーを適用
制限：脆弱性の優先順位付けや高度な分析機能は利用不可。

**■自動対応と運用のしやすさ**

・一部の攻撃に対し、感染拡大を防ぐ自動隔離や攻撃かく乱を実行
・中小企業向けに最適化されており、複雑な設定をせずに導入・運用が可能
制限：管理は最大300ユーザーまでであり、細かなロール制御（RBAC）や大規模環境向けの拡張性には制限あり。

# 4.4. Microsoft Defender for Endpoint P1 で利用できる機能

Microsoft  Defender for Endpoint P1 で提供される主な機能とその制限について、以下に一部抜粋しました。

## 提供される機能

**■包括的な脅威検出と防御**

・未知の脅威を含めた幅広い高度な脅威をリアルタイムで検出
・Microsoft のグローバル脅威インテリジェンスを活用し、複数デバイスやネットワーク全体を通じた攻撃も検知可能
制限：調査・分析機能は個別のインシデントに限定され、環境全体を横断的に調べるような高度な手動調査機能は利用不可。
　　攻撃の遮断対象はエンドポイント単位に限定される。

**■脆弱性管理とセキュリティ構成の強化**

・影響を受けるエンドポイントの構成ミスや既知の脆弱性に対してセキュリティ推奨事項を提示し、対応を支援
・専門知識がなくても導入しやすいよう、Microsoft が推奨する既定のセキュリティポリシーを適用
制限：脆弱性の優先順位付けや高度な分析機能は利用不可。

**■自動対応とスケーラブルな運用管理**

・検出された脅威に対して、自動で隔離や実行ブロックなどの対処を実行
・セキュリティ運用を簡素化する基本的な自動修復支援に対応
・Microsoft Defender セキュリティポータルから一元管理
制限：管理できるユーザーに制限は無いがロールベースアクセス制御（RBAC）で定義できる役割の種類はP2に比べて限定的。

# 4.5. Microsoft Defender for Endpoint P2 で利用できる機能

Microsoft Defender for Endpoint P2 は、Microsoft Defender for Endpoint P1 の機能に加え、より高度なセキュリティ機能を提供しています。
Microsoft Defender for Endpoint P1 では提供されていない機能を以下に一部抜粋しました。
以下の機能が利用要件に含まれている場合は、Microsoft Defender for Endpoint P2 の利用を検討する必要があります。

## エンドポイントの検出・対応

**■機能概要**

ネットワークの挙動データを収集・分析し、脅威を継続的に監視・検出。
侵害の兆候を自動で発見し、カスタム検出ルールを作成。

**■P2 で提供される機能**

脅威の検出、インシデント対応、脆弱性管理, データ収集と分析、セキュリティポリシーの適用、隔離と修復、プロアクティブな脅威ハンティングなど

## 活用シナリオ

・未知のマルウェアがシステムに侵入した際、異常な挙動を特定し検知。
・過去のログデータを検索し、既存のセキュリティツールで見逃された攻撃の痕跡や内部不正を発見。
・従業員が許可されていないアプリケーションを実行しようとした際、起動を自動ブロックする。

## 自動調査と修復

**■機能概要**

大量に発生するセキュリティアラートに対して自動調査を行い、脅威の範囲や影響を特定。確認された脅威に対して、自動隔離、ブロック、クリーンアップなどの修復アクションを実行。

**■P2 で提供される機能**

アラートトリガー、自動調査、脅威の自動修復、修復アクションの承認/拒否など

## 活用シナリオ

・不審なPowerShellスクリプトの実行を検知すると、自動調査を開始。
・脅威の自動修復機能により検出されたマルウェアファイルを自動的に検疫し、関連する悪意のあるプロセスを終了させる。
・特定した脅威に対する推奨修復アクションは管理者が確認し、承認または拒否。

# 4.5. Microsoft Defender for Endpoint P2 で利用できる機能

## 脅威と脆弱性の管理

**■機能概要**

エンドポイントに存在する脆弱性やセキュリティ設定のミスを継続的に検出・評価し、リスクに基づいて優先順位を付け、修復を支援。

**■P2 で提供される機能**

リスクベースの条件付きアクセス、アクセスレビューなど

## 活用シナリオ

・異常なサインインや疑わしいデバイスからのアクセスに対し、アクセス拒否を自動で行う。

・特権ロールは普段非アクティブにし、必要な時だけ一時的に有効化して悪用リスクを低減。

・定期的にアクセス権限を見直し、不要な権限がないか確認・整理。

## 次世代の保護

**■機能概要**

未知の脅威や、従来のウイルスパターンに基づく検出が難しい高度な攻撃からエンドポイントを守ります。

リアルタイム監視やAI・機械学習、行動分析を組み合わせて、新たな脅威を検出します。

**■P2 で提供される機能**

基本的なウイルス・スパイウェア対策、機械学習など

## 活用シナリオ

・ランサムウェアの不正な暗号化試行など、初期段階の特徴的な挙動をリアルタイムで検知し、攻撃を自動的に阻止して資産を守る。

・ディスクに痕跡を残さないファイルレス攻撃に対しても、プロセスの異常な動作を監視することで正確に検知し、感染を防止。

・正常なユーザーが誤って悪意のあるスクリプトを実行しようとした場合、実行を停止させ侵害や情報漏洩を阻止する。

# 4.6. プラン選択のポイント

前述したように、Microsoft Defender for Endpointのプランによって利用できる機能に違いがあります。
これらの違いを理解し、ビジネスの規模やニーズに応じて最適なプランを選択することが重要です。

## 小規模・個人向けプラン

**Microsoft Defender for Business**

300ユーザー以下の組織で、IT担当者やセキュリティリソースが限られる中小企業に最適。簡単なセットアップ、推奨設定、Microsoft 365との統合管理により、使いやすさと運用効率を重視したセキュリティを提供します。特に、Microsoft 365 Business Basic や Business Standard ライセンスを利用している組織にとって、アドオンとしての導入に最適です。

## 中規模向けプラン

**Microsoft Defender for Endpoint Plan 1**

エンドポイント数が多く、基本的な保護を超えたセキュリティを求める中規模組織に最適。
次世代の保護や攻撃面の縮小などの機能により、一般的な脅威に対して効果的な保護を提供します。

## 大規模向けプラン

**Microsoft Defender for Endpoint Plan 2**

多数のエンドポイントと広範な攻撃対象領域を持つ大規模組織に最適。
高度な脅威検出と対応（EDR）、脅威インテリジェンス、脆弱性管理といった包括的な機能で、複雑なセキュリティ要件に対応できます。