



# McAfee Complete Endpoint Protection—Business

## 集中管理機能を搭載したインテリジェントな統合セキュリティ

### 主な特長

- インテリジェントなエンドポイント保護、デスクトップとノートPCの侵入防止/ファイアウォール、デバイス制御、暗号化などの技術を搭載し、最も包括的な多層防御を提供します。
- 実行前に封じ込めるので、システムに感染する前にランサムウェアや高度な脅威を隔離できます。機械学習や動作分類との組み合わせで、検出能力を向上しています。ゼロデイマルウェアも検出できます。
- PC、Mac、Linuxなど、すべてのエンドポイントを一元的に管理できます。
- 分かりやすいフォレンジック情報を利用し、高度脅威に迅速に対応できます。
- すべてのデバイス、リムーバブルメディア、クラウドストレージの機密データを保護し、ファイルを安全に共有できます。

オールインワンソリューションのMcAfee® Complete Endpoint Protection—Businessを使用すると、エンドポイント デバイスを手頃な価格で保護できます。このソリューションには複数の脅威対策が統合され、グローバルの脅威情報を利用して高度脅威を阻止します。また、暗号化によってデータを保護し、アプリケーションの動的隔離と機械学習によりゼロデイ エクスプロイトからデスクトップとノートPCを保護します。さらに、メールとWebを保護するエンドポイント保護機能により、フィッシング詐欺や多段階の攻撃をブロックします。Webベースの集中コンソールで管理作業を行うので、ITスタッフの負担が軽減され、脅威発生時に迅速な対応が可能になります。

McAfee Complete Endpoint Protection—Businessを使用すると、組織に最適なセキュリティをすぐに実装し、脅威に対して迅速な対応を行うことができます。1つの統合ソリューションで、PC、Mac、Linuxなどのシステムを保護できます。ルートキット、Webとメールを利用した標的型攻撃、持続型攻撃からエンドポイントを保護しながら、管理作業を簡素化し、コストを抑えることができます。このような強力で効率的なセキュリティ管理を提供しているのは、エンドポイント セキュリティをリードするMcAfeeだけです。

### 高度な脅威対策

1つのシステムが感染しただけで、ビジネスが持続不能になることもあります。ウイルス対策だけでは、現在の高度な脅威を阻止することはできません。このような脅威を阻止するには、McAfee Complete Endpoint Protection—Businessが最適です。このエンドポイント フレームワークでは、保護対策が相互に連携して分析を行い、新たに

発生する脅威に対してアクションを実行します。また、フォレンジック データをリアルタイムで共有します。

McAfeeは、高度脅威を阻止するインテリジェントな保護機能、デスクトップとノートPC用のアプリケーションの動的隔離と機械学習、デバイス制御、暗号化など、多層型の保護対策でマルウェアを迅速に検出し、問題を修復します。

McAfeeは多層型の保護対策を提供しています。高度な暗号化により、PC、Mac、ラップトップ、仮想マシン、リムーバブル メディアの機密情報を自動的に保護し、不正なアクセスを阻止します。Box、DropBox、Google Drive、Microsoft OneDriveなどのクラウド ストレージも保護します。また、システムのパフォーマンスを低下させることなく、重要な資産を保護します。Webベースの集中管理プラットフォームであるMcAfee® ePolicy Orchestrator® (McAfee ePO™)により、ポリシーの施行と管理を簡単に行うことができます。

クラウドベースのMcAfee Global Threat Intelligenceにより、ファイル、Web、メッセージ、ネットワーク経由で発生する新たな脅威をリアルタイムで検出し、組織を保護します。弊社は、120か国以上に1億台を超える脅威センサーを配備し、1日に450億以上のクエリーを処理しています。1日に150万個以上のファイルと100万個のURLを分析し、業界で最も優れたグローバル脅威情報を提供しています。

用できる状態になります。管理作業も簡単です。McAfee ePOで全体のセキュリティ状況を確認し、すべてのデバイスのポリシーを一元的に管理できます。

## 優れたパフォーマンス

弊社の拡張性に優れたエンドポイントフレームワークを利用すると、無駄を排除し、ITをより効率的に運用できます。スキャンパフォーマンスも最適化されています。アイドル時間にスキャンを実行するだけでなく、自己学習機能を搭載し、ファイルとプロセスの動作に基づいた適応型のスキャンを実行します。より多くの処理能力が必要になった場合でも、最適なパフォーマンスを維持できます。

## McAfee: 業界のリーダー

- Forrester Wave™が2016年第4四半期のエンドポイントセキュリティ製品の評価でリーダーと評価しました<sup>1</sup>。
- NSS LabsがMcAfee Endpoint Securityを推奨しています<sup>2</sup>。

## 配備が簡単な集中管理

大半の企業は自社のオフィスにセキュリティ専門家を常駐させていません。これも簡単なセキュリティを提供する理由の一つです。このセキュリティ対策は数回のクリックでインストールが完了し、使

## McAfee Complete Endpoint Protection—Businessのハイライト

### マルウェア対策 (PC、Mac、Linux、仮想マシン)

#### McAfee Endpoint Security

複数のエンドポイント保護技術とリアルタイムで通信を行い、新しい高度脅威を迅速に阻止し、システムやユーザーへの影響を未然に防ぎます。

#### アプリケーションの動的隔離

セキュリティを侵害することなく、グレーウェア、ランサムウェア、新種の脅威などの動作を分析し、隔離します。クラウドへの接続は不要です。

#### Real Protect

- リアルタイムの動作分析と機械学習で高度なゼロデイ脅威を検出し、阻止します。実行前の特徴を抽出し、実行後の動作とメモリを分析することで脅威を特定します。
- サンドボックスを回避するマルウェアを阻止します。不正な動作の実行を許可してリアルタイムで分析を行い、マルウェアがシステムに感染する前にアプリケーションの動的隔離が不正なアクションをブロックします。

#### Application Control

システムパフォーマンス、ユーザー、管理者に対する影響を最小限に抑えながら、不要なアプリケーションとマルウェアのインストールと実行を阻止します。

#### デスクトップを保護する侵入防止とファイアウォール

- 未知のゼロデイの脅威と新しい脆弱性に対する攻撃を阻止します。
- 緊急パッチの回数が少なくなります。

#### Global Threat Intelligence

- 世界各地に配備された数百万台のセンサーからリアルタイムで脅威情報を収集します。攻撃経路に関係なく、新たに発生する脅威を阻止します。
- エクスプロイト、メモリに対する攻撃、特権昇格を狙う脅威などを阻止するため、セキュリティ統制をカスタマイズできます。

### Webとメールの保護

#### URLフィルタリングと安全検索機能を搭載したWeb管理

- ユーザーが閲覧する前にWebサイトの危険性を通知します。リスクを軽減し、コンプライアンスを維持できます。
- Web閲覧ポリシーを施行し、Webアクセスを承認または阻止します。

#### メールサーバー用のマルウェア対策とスパム対策

- メールサーバーへのマルウェアの侵入を阻止し、ユーザーのメールボックスを保護します。
- McAfee Security for Email Serversにより、Microsoft Exchange ServerとLotus Dominoサーバーのマルウェアを検出、駆除、ブロックします。

### データ保護

#### デバイスコントロール

リムーバブルメディアの使用を制限し、重要なデータの漏えいを防ぎます。

#### ディスク全体、ファイル、フォルダー、リムーバブルメディア、クラウドストレージの暗号化

PC、Mac、ノートPC、ネットワークサーバー、リムーバブルメディア、クラウドストレージサービスの機密データを保護します。

### 管理

#### McAfee ePO

- 一元管理された単一のコンソールでポリシー、コンプライアンス、レポートを管理します。
- クロスプラットフォームポリシーにより、異なるOSが混在する環境でも簡単に管理できます。

### 脅威対策のライフサイクル全体を網羅

McAfee Complete Endpoint Protection–Businessスイートを使用すると、保護状態を維持し、セキュリティ問題に迅速に対応できます。統合されたセキュリティフレームワークにより、エンドポイントセキュリティ環境の複雑さを排除し、保護対策のパフォーマンスとユーザーの生産性を向上できます。また、高度脅威に対する可視性を実現し、検出と対応を迅速に行うことができます。クラウドベースのグローバル脅威情報を利用し、新しい高度脅威を迅速に検出し、効果的な対応とフォレンジック

が可能になります。Webベースの集中管理コンソールで、Intel® Securityと他社の製品を一元管理できます。複数のソリューションを利用していても、脅威対策の状況を迅速に把握し、管理作業をより簡単に行うことができます。詳細については、下記のサイトをご覧ください。

<https://www.mcafee.com/jp/products/complete-endpoint-protection-business.aspx>

### 高度脅威を阻止するセキュリティ対策の連携

技術	機能	処理
<b>McAfee Endpoint Security 10</b>	複数の脅威対策間の通信を可能にします。無関係に見えるイベントを関連付け、標的型攻撃を検出します。	<ul style="list-style-type: none"> <li>• 複数の脅威対策が情報を交換し、新たに発生する脅威を検出します。</li> <li>• 適応型のインテリジェントなスキャン機能が複数の情報源から取得した監視結果を使用し、新たに発生する攻撃をリアルタイムに検出します。</li> <li>• 脅威対策でグローバルとローカルの脅威情報を使用します。</li> <li>• 不審なアプリケーションやプロセスを検出すると自動的にアクションを実行します。迅速にエスカレーションを行うだけでなく、他の脅威対策やグローバルコミュニティに情報を提供します。</li> </ul>
<b>McAfee Threat Intelligence Exchange*</b>	グローバルなデータソースとサードパーティから収集した情報を提供します。ローカルでリアルタイムに発生しているイベントとその履歴から脅威情報を収集します。	<ul style="list-style-type: none"> <li>• セキュリティ コンポーネントが、エンドポイント、ゲートウェイ、他のセキュリティ コンポーネントによって検出された情報を利用し、グローバル ネットワーク上の組織を狙った脅威を分析します。</li> <li>• マルウェア対策から収集した脅威情報を McAfee Data Exchange Layer 経由ですべてのエンドポイントに瞬時に配信し、脅威を未然に防ぎます。</li> <li>• 組織の要件に応じて、発行者の証明書リスト、ファイル ハッシュ、リスク許容度をカスタマイズできます。</li> </ul>
<b>McAfee Active Response*</b>	実行中の調査結果をリアルタイムで使用し、インシデント対応能力を強化します。	<ul style="list-style-type: none"> <li>• コンテキストとシステムの状態変化を自動的に監視して、攻撃の兆候 (IoA) や攻撃コンポーネントの潜伏を検出し、分析、運用、フォレンジックの各チームに脅威情報を提供します。</li> <li>• 攻撃方法、データの自動収集、アラート、対応方法を調整できます。また、カスタム ワークフローを提供します。</li> <li>• 攻撃イベントの検出時に管理者とシステムに攻撃を警告します。</li> </ul>
<b>McAfee Application Control</b>	社内のデスクトップと専用デバイスでの不正なアプリケーションやコードの実行を防ぎます。	<ul style="list-style-type: none"> <li>• 信用モデルと革新的なセキュリティ機能で高度な持続型脅威を阻止します。シグネチャの更新も手間のかかるリスト管理も不要です。</li> <li>• McAfee Global Threat Intelligenceとの統合により、承認されたアプリケーションとコードのみを実行し、既知または未知の不正コードの実行を阻止します。</li> <li>• McAfee Threat Intelligence Exchangeと一緒に配備することで、ローカルの脅威情報を使用してホワイトリストを強化し、未知の標的型のマルウェアを迅速に阻止できます。McAfee Threat Intelligence ExchangeはMcAfee Advanced Threat Defenseと連携し、サンドボックスで未知のアプリケーションの動作を動的に分析します。すべてのエンドポイントを新たに検出されたマルウェアから自動的に保護します。</li> </ul>

\* McAfee Threat Intelligence Exchange、McAfee Active Response、McAfee Advanced Threat DefenseはMcAfee Complete Endpoint Protectionのオプション機能で、別売りになります。

1. Forrester Wave™が実施したエンドポイント セキュリティの評価: 2016年第4四半期のエンドポイント セキュリティ製品  
<https://www.mcafee.com/resources/reports/rp-endpoint-security-advantage-forrester.pdf>
2. NSS Labs高度なエンドポイント保護 (AEP) グループのテスト (2017年)  
<https://www.mcafee.com/jp/resources/reviews/nss-labs-aep-endpoint-security.pdf>

#### マカフィー株式会社

〒150-0043  
東京都渋谷区道玄坂 1-12-1  
渋谷マークシティWEST 20F  
TEL 03-5428-1100 (代)  
[www.mcafee.com/jp](http://www.mcafee.com/jp)

McAfee、McAfeeのロゴ、ePolicy Orchestrator、McAfee ePOは、米国法人McAfee LLCまたは米国またはその他の国の関係会社における登録商標または商標です。その他すべての登録商標および商標はそれぞれの所有者に帰属します。Copyright © 2017 McAfee LLC. 2814\_0417  
2017年4月