McAfee Enterprise Products Lineup

マカフィー エンタープライズ
プロダクト ラインアップ

intel Security

脅威対策ライフサイクルとは

脅威対策ライフサイクルとは、組織のセキュリティを３つのプロセスからなる枠組み（Protect･Detect･Correct）として捉え、その仕組みを積極的に組織に取り入れて、自動化や改善をする（Adapt）ことで、セキュリティ全般の効率化を図る考え方です。
従来のセキュリティソリューションは、脅威を**「防御（Protect）」**することを大きな目的としてきました。
しかし、企業や組織に対する攻撃が加速度的に高度化・巧妙化しつづけている現状では、いくら「防御（Protect）」を強固にしても、100％確実な防御は不可能です。そのため、攻撃を受けてしてしまった場合でも、脅威の兆候や侵入を素早く**「検知（Detect）」**して、被害を速やかに**「復旧（Correct）」**することが重要となります。
さらには、そのプロセスで得られた知見を組織全体にフィードバックして、状況の変化に**「適応（Adapt）」**させていくことが、これからのセキュリティには求められます。

ライフサイクルを通して自動化を促進し、運用負担を軽減

Protect 防御

脅威情報の素早い共有で
高い障壁を構築

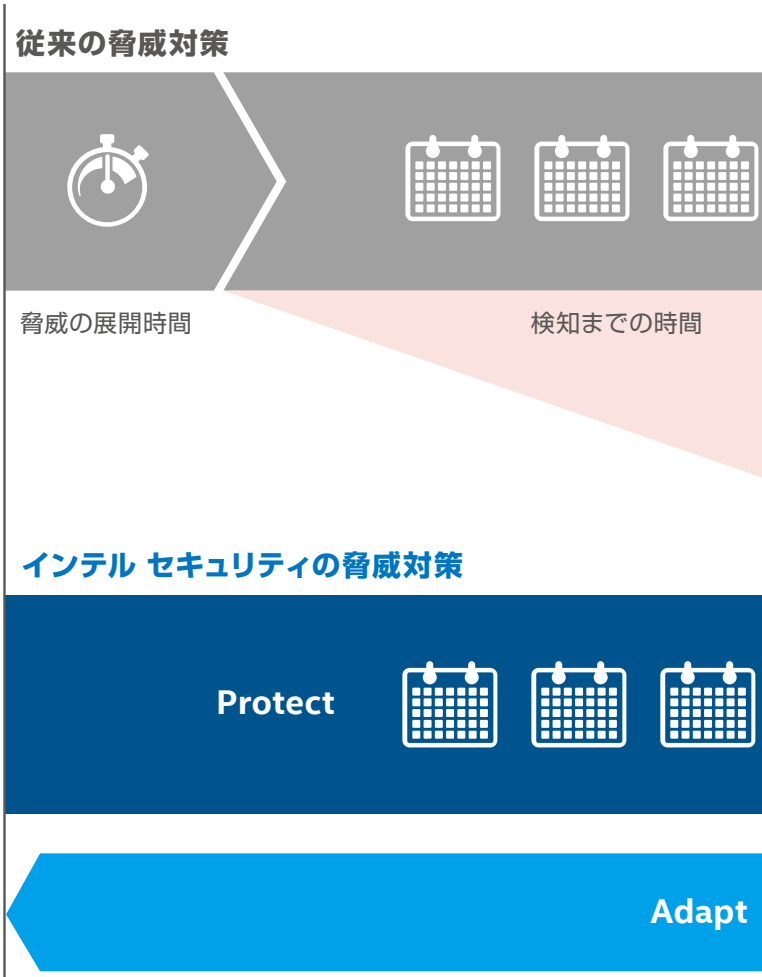
組織内のセキュリティシステムが脅威情報を瞬時に共有する基盤と、未知の脅威に有効な高性能解析システムが連携して強力な防御を提供します。

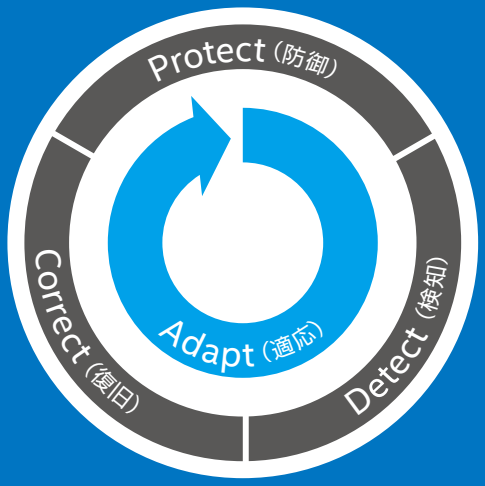
Adapt 適応

知見と洞察を素早く反映し
継続的に強化

グローバル脅威情報や、日々の活動で得た知見や洞察を素早くライフサイクルに反映できるため、防御力・運用効率を継続的に向上できます。

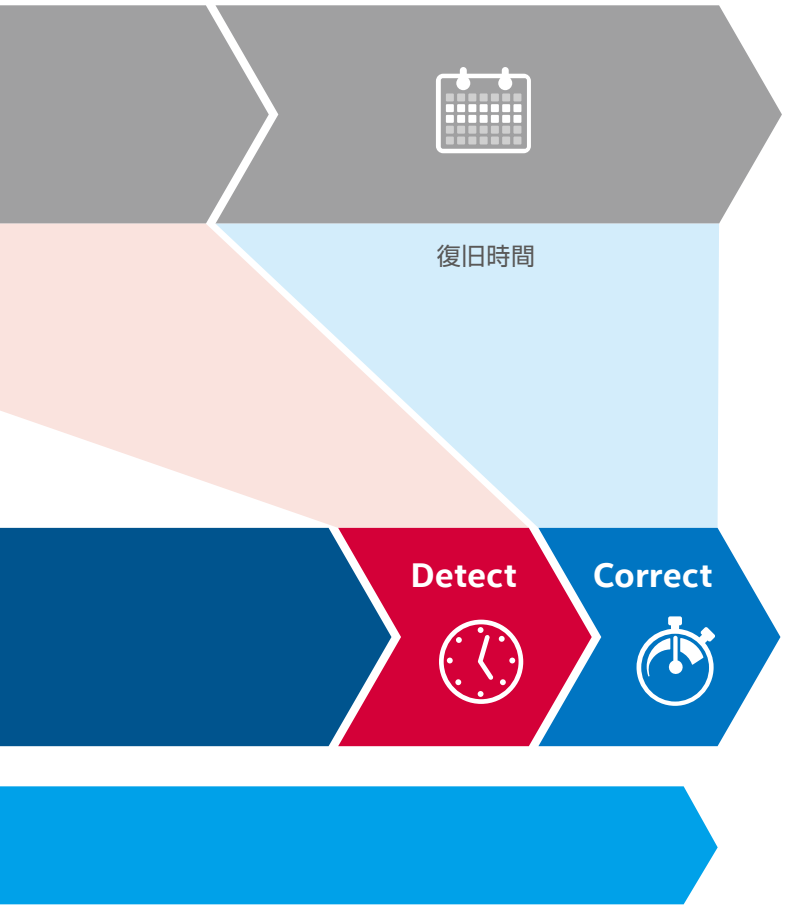
■ 従来の脅威対策とインテル セキュリティの脅威対





INDEX

策の比較



Detect 検知

集約した情報を活用し脅威を素早く検知

セキュリティシステム、OS、ミドルウェアなどから得られるログやイベント情報を集約し、脅威の検知力向上と運用負担の軽減を実現します。

Correct 復旧

一次対応の自動化を促進し被害を最小化

脅威の検出から調査、状況把握、一次対応まで負担の大きな運用プロセスを自動化することで、迅速な一次対応を実現し被害を最小化します。

最新の脅威に徹底対抗

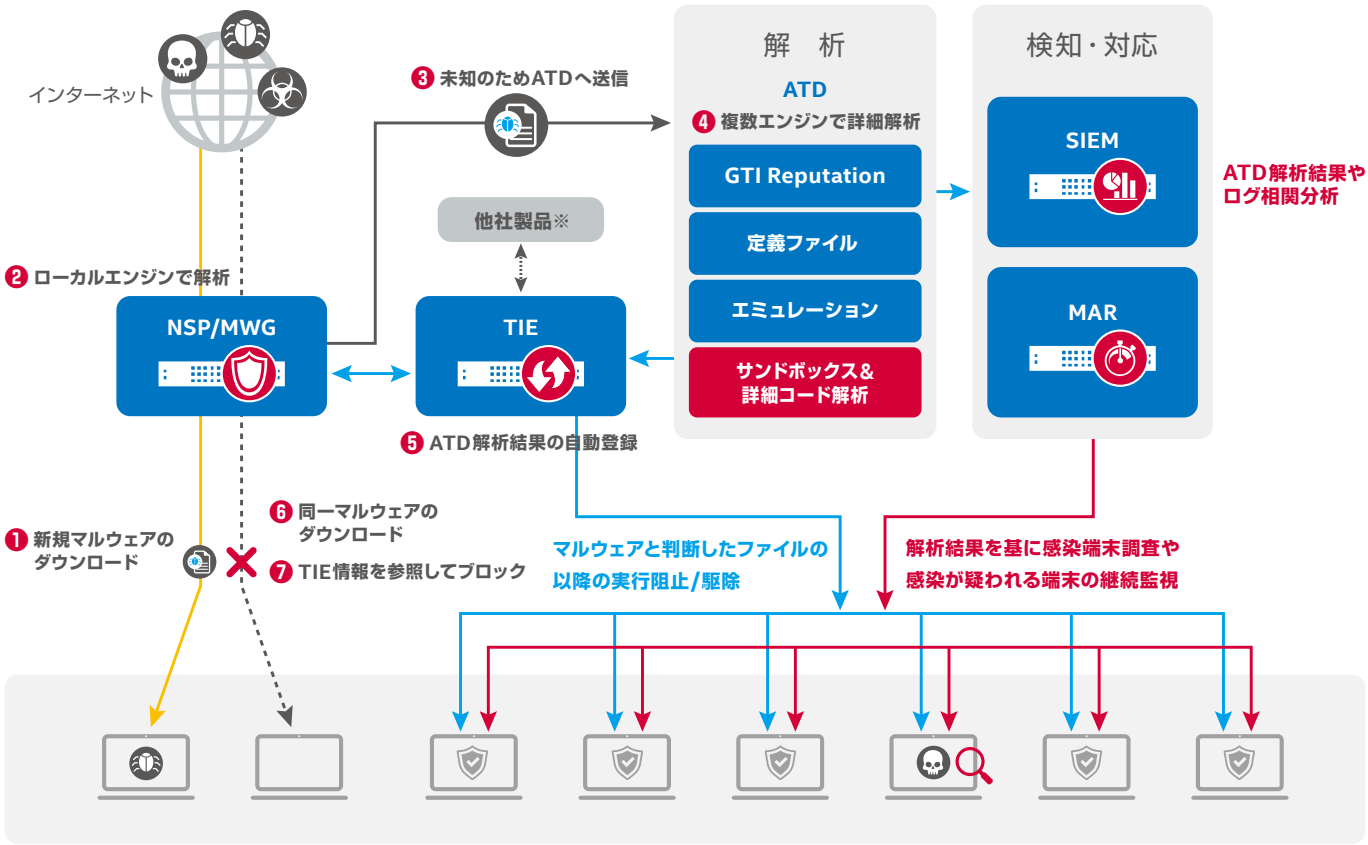
エンドポイント向けのマルウェア対策、脆弱性保護、Webセキュリティ、デスクトップファイアウォールなどのモジュールを統合したプラットフォームで、高い保護機能を提供しながら、セキュリティ管理の複雑さを軽減し、昨今のセキュリティ人材不足の課題を解決します。また、ローカルおよびグローバルで収集された脅威情報の共有と活用により、未知の脅威に対する高い保護機能を提供します。脅威情報の検知から復旧までを前提とした包括的なアプローチをとりいれることで、戦略的なセキュリティ対策を実現することができます。

最新の脅威情報を組織内で瞬時に共有し防御に活用

管理性と拡張性に優れた統合プラットフォーム

高度なシステム連携で単一製品では得られない強力なセキュリティ

脅威情報の共有による強力なセキュリティ



※他社製品の解析結果（脅威情報）の登録も可能。

- NSP.....Network Security Platform（ネットワークIPS） P.8
- MWG.....McAfee Web Gateway（Webセキュリティアプライアンス） P.7
- SIEM.....Security Information and Event Management（セキュリティ情報/イベント管理） P.11
- MAR.....McAfee Active Response（インシデントレスポンスを効率化する検出、監視、対応） P.11

エンドポイントの情報漏えい対策を包括的に実現するスイート

McAfee® Threat Intelligence Exchange（TIE）

主な特長

- グローバルの脅威情報やローカルのセキュリティ製品が検出・解析した脅威情報をリアルタイムに統合し、未知の攻撃を検出・防御
- 統合された脅威情報をネットワークやエンドポイントに配置されたセキュリティ製品にリアルタイムに共有し、先行的な防御を実現
- 従来、数日、数週間、数か月必要だった高度な脅威の検出から抑制を数ミリ秒に短縮

セキュリティ統合管理ソリューション

McAfee ePolicy Orchestrator（ePO）

主な特長

- シングルエージェント、シングルコンソール、シングルサインオン
- Webベースのコンソールでブラウザがあればどこからでもアクセス可能
- ネットワークに負荷をかけないウイルス定義ファイル/エンジンの更新
- Microsoft Active Directoryとの同期
- レポートの自動作成

ゼロデイマルウェア解析

McAfee Advanced Threat Defense（ATD）

主な特長

- 既知のマルウェア、未知のマルウェアに有効な複数の検知エンジンを融合
- 詳細な静的コード解析とサンドボックス解析で未知の脅威も解析と検出を実現
- 製品連携で被害の最小化、事後対策支援までを効率的に実現

全ての端末を包括的で多層的に保護するエンドポイントセキュリティスイート

McAfee Complete Endpoint Protection

主な特長

- デスクトップ/ノートPC、サーバすべてのデバイスの一元統合管理が可能
- ウイルス対策に加えて、脆弱性対策、ホワイトリスト型ウイルス対策などの先進的な対策ソリューションを包含
- ディスク/ファイル/フォルダの暗号化や、Android向けウイルス対策も可能

関連製品

エンタープライズ規模の企業に対する
総合エンドポイントセキュリティ対策スイート
McAfee Complete Endpoint Protection - Enterprise

中小規模向け総合エンドポイントセキュリティ対策スイート
McAfee Complete Endpoint Protection - Business

多層的なマルウェア・プロテクションを実現するエンドポイントセキュリティスイート

McAfee Endpoint Protection

主な特長

- Windows/Mac/Linuxウイルス対策、スパイウェア対策、メールウイルス・スパム対策、デバイス制御、Webレピュテーション、Webフィルタリングを提供
- 多層的なプロテクションに追加して、ファイルレピュテーション、Webレピュテーションの活用によりプロアクティブな防御を実現

関連製品

すべてのエンドポイントに必要なセキュリティを統合したスイート
McAfee Endpoint Protection Suite

多層的なマルウェア・プロテクションとエンドポイントの
脆弱性管理を実現するスイート
McAfee Endpoint Protection - Advanced Suite

中小規模企業に最適化された低コスト・高パフォーマンスのエンドポイントセキュリティ対策スイート

McAfee Endpoint Protection for SMB

主な特長

- 利用環境に合わせて、オンプレミス管理またはクラウド管理を選択可能
  クラウド管理なら管理サーバ不要でコストも削減
- 新しいエンドポイントプラットフォームである「Endpoint Security」により、マルウェア対策、脆弱性対策、デスクトップファイアウォール、Web対策を統合、さらに従来よりもスキャン時のパフォーマンスを向上し、システムへの負荷を大幅に低減

関連製品

ベーシックな脅威対策を包含したセキュリティスイート
McAfee Endpoint Protection Essential for SMB

重要データの保護

組織で扱う重要なデータは、生き物です。重要なデータであるからこそ、複数の階層でデータが共有され更新されます。さらに、クラウドやモバイルデバイスの普及により、様々なデバイスで情報にアクセスできるようになったため、社内・社外の領域が不明確になり、重要データの管理や把握が難しくなっています。インテル セキュリティは、総合的なデータ保護ソリューションで対策強化を提案します。包括的かつ効果的に統合された機能を活用することで、ビジネス上のコラボレーションや生産性を維持しつつ、情報漏えいのリスクを抑え、規制やコンプライアンスを保つことができます。

総合的なデータ保護ソリューションを提供

情報保護規制やコンプライアンスに対応

重要データの可視化とコントロール強化を提供

幅広い対応が必要になる情報漏えい対策

データのタイプ	データ紛失の要素	該当ソリューション
送信データ	メール／インスタントメッセージ、ウェブへのポスト、ネットワークトラフィック、クラウド	DLP Prevent DLP Monitor
格納データ	ファイル共有、データベース、デスクトップPC／モバイルPC、クラウドストレージ	DLP Discover Drive Encryption
活用データ	リムーバブルデバイス、データベース、クラウド アプリ、ファイル&クリップボード	DLP Endpoint File and Removable Media Encryption Device Control

エンドポイントの情報漏えい対策を包括的に実現するスイート

McAfee Complete Data Protection

エンタープライズ クラスの強力なドライブ暗号化機能により、エンドポイントの重要なデータを保護します。この暗号化スイートでは、リムーバブル メディア、クラウド ストレージ サービスのデータを保護するだけでなく、MacとWindowsのネイティブ暗号化機能も管理が可能。管理コンソール（ePO）で、データ保護ポリシーの施行だけでなく、データセキュリティを一元管理できます。

主な特長

■ ハードディスク暗号化（Drive Encryption）
- ハードディスク全体の暗号化による紛失・盗難などへの保護対策
- FIPS140-2やEAL 2+に対応した高度な暗号化技術に対応
- インテル®AES-NIに対応し、暗号化処理の高速化が可能

■ ファイル／フォルダ／リムーバブルメディア暗号化（File and Removable Media Encryption）
- 特定のファイル・フォルダやUSBメモリーなどのリムーバブルメディアの暗号化で、社外への持ち出しデータを保護
- FIPS140-2やEAL 2+に対応した高度な暗号化技術に対応
- McAfee DLP Endpointとの連携で重要データの自動暗号化が可能

■ デバイス制御・管理対策
- 設定されたポリシーに違反するデバイスの使用やデータ転送をブロック
- リムーバブルストレージへの転送行為を詳細にログ収集し、監査にも的確に対応
- ePOによる一元管理で管理作業、管理時間、トレーニングを効率化

■ ホスト型情報漏えい防止（McAfee DLP Endpoint）
- 重要データのメール／Web経由での送信、クラウドファイルストレージへの保存、印刷などの監視・ブロック

関連製品

暗号化による情報漏えい対策スイート
McAfee Complete Data Protection

暗号化とホストDLP/デバイス制御を包含した統合情報漏えい対策スイート
McAfee Complete Data Protection – Advanced

低コストで暗号化を実現する情報漏えい対策スイート
McAfee Complete Data Protection – Essential

デバイス制御・管理対策
McAfee Device Control

包括的な情報漏えい防止対策（DLP）ソリューション

McAfee Total Protection for Data Loss Prevention

オンプレミス、クラウド、エンドポイントなど、データの場所に関わらず知的財産を保護し、法令を遵守します。
管理コンソール（ePO）で配備、管理、更新、レポートを簡単に行うことができます。

主な特長

■ ホスト型情報漏えい防止対策

- 知的財産や企業秘密などの重要な非構造化データを保護
- ポリシーとインシデントをePOで簡単に管理
- ユーザの重要データをリアルタイムに監視し、リスクを可視化
- ユーザの日々の操作で発生する違反を解決、データセキュリティを維持

■ ネットワーク型情報漏えい防止対策

- 専用の管理マネージャによるフレキシブルな集中管理
- 簡単なポリシー管理
- Webやメール などによる情報漏えいをブロック
- ユーザの環境内に存在する未分類の重要データを検出・分類

関連製品

包括的な情報漏えい防止対策スイート
McAfee Total Protection for Data Loss Prevention

ホスト型情報漏えい防止対策
McAfee DLP Endpoint

ネットワーク型情報漏えい防止対策

ネットワークを流れる重要データを監視、記録、通知する
McAfee DLP Monitor

ネットワーク上のデータをスキャンし、重要データを発見、分類する
McAfee DLP Discover

ネットワーク通信を監視し、重要データの流出のブロック・暗号化を行う
McAfee DLP Prevent

Webセキュリティ

McAfee Web Gateway

主な特長

- アプライアンス※、仮想環境、SaaSで利用可能なWebセキュリティを提供
- 意図分析、レピュテーションを活用したマルウェア対策やURLフィルタなど強力なWebセキュリティを提供

※ アプライアンスを使用する場合は専用ハードウェアが必要になります。

関連製品

McAfee Web Protection
McAfee Web Security, Gateway Edition Software
McAfee Web Anti-Malware, Gateway Edition Software
McAfee SaaS Web Protection

SaaSとオンプレミスを統合したWebセキュリティ

McAfee SaaS Web Protection

主な特長

- McAfee Global Threat Intelligence（GTI）によるリアルタイムレピュテーションやコンテンツ解析により、Webベースの動的なマルウェアを防御
- 100を超えるカテゴリーにより、アクセス先を細かく制御できるURLフィルタ
- ユーザグループを作成でき、その単位でポリシー設定が可能

データセンター／クラウドの要塞化

データセンターにおける仮想化テクノロジーやクラウドサービスの活用が進んでいます。また、既存のオンプレミスと新しいテクノロジーのハイブリッドな利用形態も増えてきました。インテル セキュリティは、様々な環境でセキュリティの可視性、防御、運用性を高めるソリューションを用意しています。またIoTで利用される組み込み型デバイス等のセキュリティでも高い実績を誇っています。

仮想環境に最適なセキュリティ

ハイブリッドクラウド環境でも優れた可視性と管理性

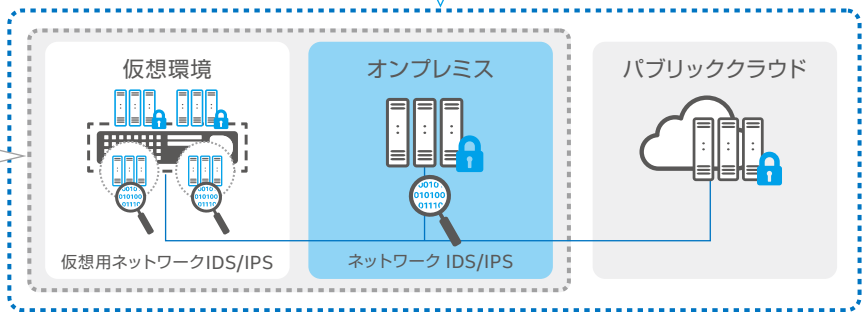
高速ネットワーク環境、及び仮想環境対応ハイパフォーマンスIPS

ePolicy Orchestrator (ePO)
オンプレミスに加えて、クラウドや仮想環境上の重要サーバーも管理コンソールで一元管理

Data Center Connector for vSphere / for OpenStack / for Amazon Web Service (AWS) / for Microsoft Azure

Network Security Platform (NSP)
物理ネットワーク環境でも仮想ネットワーク環境でも次世代IPSで強固なネットワークセキュリティを実現

Intel® Security Controller
仮想基盤（VMware NSX）と連動してダイナミックな仮想ネットワーク環境でも高い管理性を提供



仮想デスクトップ / サーバ向けウイルス対策最適化ソリューション

McAfee MOVE AntiVirus

主な特長

- 主要仮想環境に対応し、各ゲストOSのスキャン処理リソース負荷を抑制
- デスクトップ対策にはホストIPSやWeb対策も利用可能
- ホワイトリストを活用したスキャン効率化、定期的なスキャン時に負荷を考慮
- Data Center Connector for vSphereによりVMware環境で高い管理性を提供

関連製品

仮想環境に最適化されたVDI用セキュリティ対策
McAfee MOVE AntiVirus for Virtual Desktops

仮想環境に最適されたサーバ用セキュリティ対策
McAfee MOVE AntiVirus for Virtual Servers

パブリック クラウドに最適化されたサーバセキュリティスイート

McAfee Public Cloud Server Security Suite

主な特長

- クラウド上のインスタンスの可視性、脅威に対する包括的な保護を提供
- パブリッククラウド上での使用時間をベースにした課金体系を採用
- Data Center Connector（OpenStack、AWS、Microsoft Azure用）による高い管理性を提供

ネットワークIDS/IPS

McAfee Network Security Platform (NSP)

主な特長

- 標的型攻撃対策にも最適な先進のテクノロジーを活用した入口と出口対策
- 複数の高度な検知テクノロジーによるマルウェア検知とボットネット遮断
- 最大320Gbpsまで対応し、1,500を超えるアプリケーションの可視化と制御

関連製品

次世代IPSの仮想アプライアンス
McAfee Network Security Virtual Software

仮想基盤と連動して優れた管理性を実現
Intel Security Controller

物理 / 仮想化 / クラウドのあらゆる環境を保護するサーバセキュリティスイート

McAfee Server Security Suite

主な特長

- 従来型のマルウェア対策に加え、仮想環境に最適化されたマルウェア対策やホワイトリスト型マルウェア対策によるレガシーOSの保護を提供
- Webサーバやファイルサーバに対する不正変更や改ざんの防止機能を提供
- Data Center Connector（VMware vSphere、OpenStack、AWS、Microsoft Azure用）による高い管理性を提供

関連製品

物理 / 仮想 / クラウド環境のサーバ向けセキュリティスイート
McAfee Server Security Suite Essentials

物理 / 仮想 / クラウド環境のサーバ向けの先進的かつ高度なセキュリティスイート
McAfee Server Security Suite Advanced

ホワイトリスティング技術によるアプリケーション実行制御

McAfee Application Control

主な特長

- システム環境からダイナミックにホワイトリスティングを生成
- ホワイトリストで許可しないアプリケーション、マルウェアの実行を禁止
- シグネチャベースのマルウェア対策ソフトの導入が難しいシステムを保護

システム変更作業に対する監査と制御

McAfee Change Control

主な特長

- リアルタイムでの変更検知、および、ポリシーによるシステム変更の許可・禁止
- 変更範囲をコントロールすることで、誤った変更作業に起因するシステム障害を回避
- 変更監査ログにより、PCI DSSやSOXで求められるシステム整合性の証明

データベースセキュリティソリューション

McAfee Data Center Security Suite for Databases

主な特長

- メモリー監視型のモニターにより詳細な監査と脆弱性予防を実現
- 監査、脆弱性管理と予防がシームレスに連動
- 豊富で詳細な脆弱性検査が可能

※ 本製品の提供方法についての詳細は、事前にご確認ください。

含まれる製品

McAfee Database Activity Monitoring
McAfee Virtual Patching for Databases
McAfee Vulnerability Manager for Databases

組込み機器システム向けのアプリケーション実行制御

McAfee Embedded Control

主な特長

- ホワイトリスト上で許可されていないアプリケーション、マルウェアの実行を禁止
- シグネチャベースのマルウェア対策ソフトの導入が難しいシステムを保護
- リアルタイムでの変更検知、および、ポリシーによるシステム変更の許可・禁止
- 変更範囲をコントロールすることで、誤った変更作業に起因するシステム障害を回避
- 変更監査ログにより、PCI DSSやSOXで求められるシステム整合性の証明

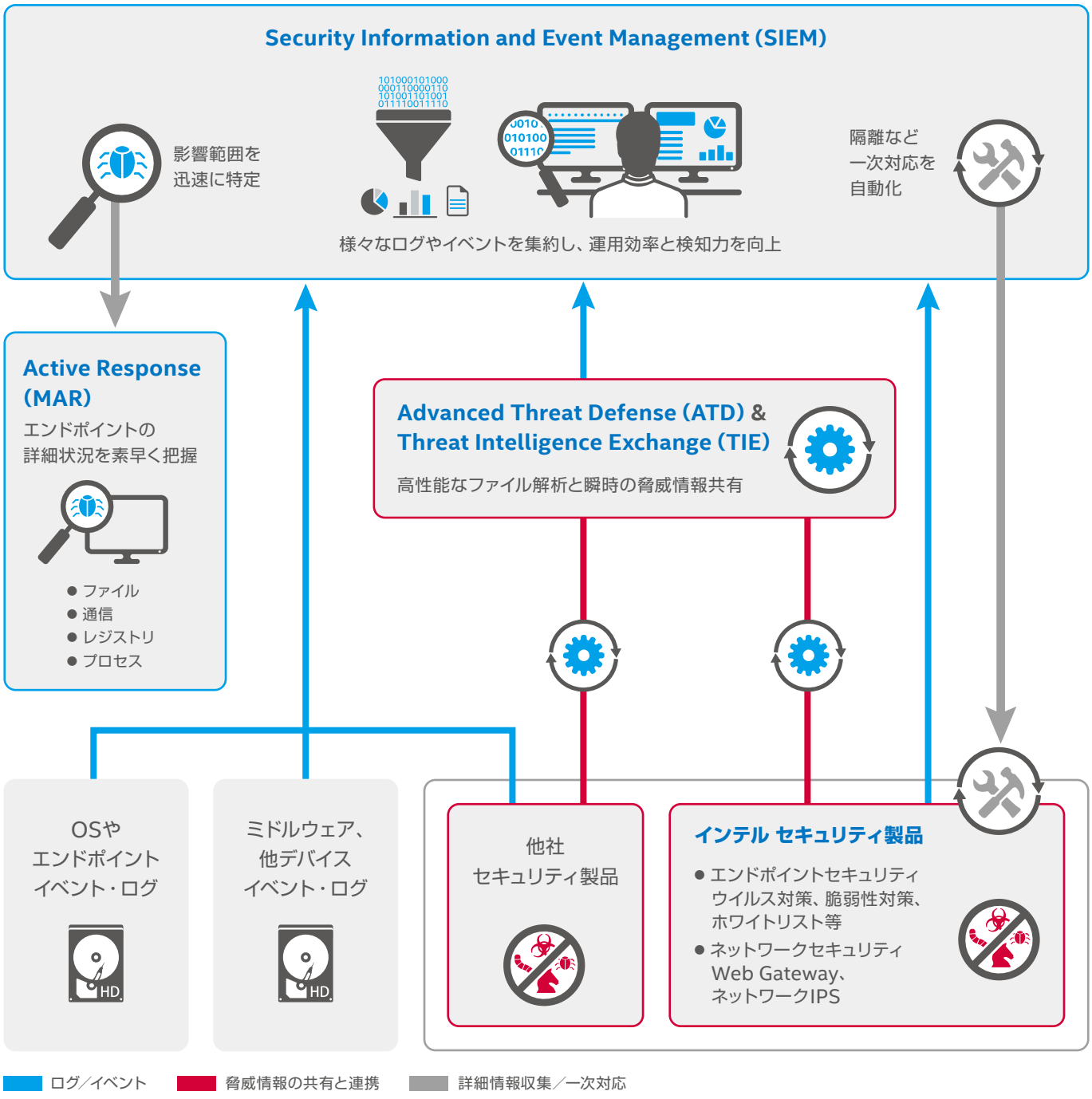
セキュリティの運用改革

インテル セキュリティが推進する脅威対策ライフサイクルの効率化が、セキュリティ運用に改革をもたらします。自動化を促進し限られた運用リソースでも、防御、検知、復旧に代表されるサイクルの継続的な効率化を実現します。さらに、脅威対策の様々な活動で得たセキュリティに関する知見や洞察を素早く適応することで、組織におけるセキュリティレベルの向上も同時に推進することができます。

素早い検知と迅速な状況把握による運用負担軽減

全体を俯瞰し重要イベントを優先して対応

一次対応を自動化して被害を最小化



検知力向上と運用負担軽減を実現するセキュリティ運用

McAfee Security Information and Event Management (SIEM)

主な特長

- 様々なデバイスのアラートやログ管理を一元化してセキュリティの可視化を促進
- 複数のセキュリティ機器やOSなどの情報対象に、高度な分析や迅速な調査を支援
- 専用DBにより高いパフォーマンスとスケーラビリティを提供

関連製品

セキュリティイベント管理とログ管理の統合
McAfee Enterprise Security Manager (ESM)
McAfee Enterprise Log Manager (ELM)

大量ログデータの収集
McAfee Event Receiver (ERC)

長期大量データの関連付けとリスク分析
McAfee Advanced Correlation Engine (ACE)

アプリケーションの可視化
McAfee Application Data Monitor (ADM)

運用効率の向上
McAfee Global Threat Intelligence (GTI) for ESM

インシデントレスポンスを効率化する検出・監視・対応

McAfee Active Response (MAR)

主な特長

- 簡単にファイル、レジストリ、通信、プロセスの情報を検索
- 重大なイベントやシステム変更を継続的に監視
- 監視条件(トリガー)検出時に一次対応を自動実行

セキュリティ戦略から運用支援まで

プロフェッショナルサービスとトレーニング

お客様が抱える課題に対して専門的なアプローチを展開し、戦略から製品導入、運用支援まで、幅広くかつ一貫したサービスを提供します。担当するセキュリティコンサルタントは、主にコンサルティングファーム、セキュリティベンダー、SIベンダーなど、多様なバックグラウンドの出身者で構成され、中央省庁や大手通信キャリアのような、日本社会におけるセキュリティの中核・最先端と言える極めてシビアな現場で活躍しています。


上流コンサルティングサービス


設計支援 / 製品導入


診断 / 監査


教育 / トレーニング


運用支援 / 緊急対応

サービス詳細はプロフェッショナルサービスブローシャをご覧ください

http://www.mcafee.com/jp/resources/brochures/br-professional-services.pdf

製品情報はこちらをご覧ください　http://www.mcafee.com/jp/products-solutions.aspx

マカフィー株式会社　www.mcafee.com/jp

東京本社　〒150-0043 東京都渋谷区道玄坂1-12-1 渋谷マークシティウエスト20F
TEL：03-5428-1100（代） FAX：03-5428-1480

西日本支店　〒530-0003 大阪府大阪市北区堂島2-2-2 近鉄堂島ビル18F
TEL：06-6344-1511（代） FAX：06-6344-1517

名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅4-6-17 名古屋ビルディング13F
TEL：052-551-6233（代） FAX：052-551-6236

福岡営業所　〒810-0801 福岡県福岡市博多区中洲5-3-8 アクア博多5F
TEL：092-287-9674（代）

● 製品、サービスに関するお問い合わせは下記へ

MCABR-PL-1604-GRP