

# McAfee Web Gateway

## パフォーマンスに優れたインテリジェンスなセキュリティ

以前に比べるとWebでできることが増えています。現在では、動的なコンテンツをリアルタイムに扱うことができます。しかし、Webでは毎日巧妙な攻撃が発生し、以前に比べると危険な領域となっています。McAfee® Web Gatewayは、進化するマルウェアの脅威を最前線で阻止し、組織を保護します。ローカルの強力な意図分析とMcAfee Labsのクラウド ベースの保護対策を統合した最先端のセキュリティ アプローチにより、インターネット アクセスによるリスクを大幅に軽減できます。

インターネットが様々な分野・形態で利用されている現在、高度なWebセキュリティは欠かせない存在です。安全に見えるサイトでもマルウェアの拡散に利用される可能性があります。既知のウイルスや不正なサイトをブロックするだけでは十分な対応とは言えません。シグネチャ ベースのウイルス対策や、カテゴリのみのURLフィルタリングなど、これまでの対策も重要です。しかし、これらのアプローチでクラウド アプリケーションへのアクセスを保護し、高度なエクスプロイトを阻止することはできません。

従来のソリューションは既知のコンテンツや不正なオブジェクト/実行ファイルには有効ですが、無害に見えるHTTP/HTTPSトラフィックに不正なコードが潜んでいる高度な脅威や、新たに発生する未知の脅威は阻止できません。クラウド アプリケーションへのアクセスを柔軟に制御しながら、既知の脅威だけでなく、未知の脅威も阻止する必要があります。

### 包括的なセキュリティでインバウンドとアウトバウンドの両方向を保護

McAfee Web Gatewayは、Webトラフィックに対する包括的なセキュリティを提供する高性能なアプライアンス ソフトウェアです。ユーザーが送信したWeb要求に対して、McAfee Web Gatewayは組織のインターネット使用ポリシーを施行します。許可されたトラフィックであれば、ローカルの保護対策とグローバルの評価情報を利用しながら、要求されたWebページを介してネットワークに侵入を試みるコンテンツとアクティブ コードの特性、意図を分析します。これにより、マルウェアやトラフィックに潜む脅威を阻止します。一般的なパケット調査技術と異なり、McAfee Web GatewayではSSL (Secure Sockets Layer) トラフィックを調査し、暗号化で自身の存在を隠す不正なコードやアプリケーションを阻止します。

### McAfee Web Gateway

- 複数のハードウェア モデルで使用可能。VMwareとMicrosoft Hyper-Vの仮想マシンにも対応。
- McAfee Endpoint Security、McAfee Advanced Threat DefenseなどのMcAfee Threat Intelligence Exchangeソリューションとの統合
- Common criteria EAL2+とFIPS 140-2 Level 2に準拠
- Gemalto SafeNet Hardware Security Module (HSM)、Thales nShield HSM、Thales PCIeカードなど、複数の暗号化キー保存オプションに対応
- Webゲートウェイのマルウェア対策として業界最高の評価 (AV-TEST)

McAfeeとつながる



## データシート

また、インバウンド保護により、外部からのデータや文書のアップロードを許可しているWebサイトのリスクを回避できます。McAfee Web Gatewayをリバース プロキシ モードで使用すると、アップロード前にすべてのコンテンツがスキャンされるので、サーバーとコンテンツの両方を保護できます。

アウトバウンド トラフィックを保護するため、McAfee Web Gatewayは業界最先端のデータ損失防止技術を使用し、HTTP、HTTPS、FTPなど、主要なすべてのWebトラフィックのコンテンツをスキャンします。また、重要な情報や機密情報、規制対象の情報も保護します。ソーシャル ネットワーク サイト、ブログ、Wikisだけでなく、Webメール、予定表、カレンダーなどのオンライン ツールからの漏えいも防ぎます。McAfee Web Gatewayは、ボットに感染したコンピューターによる不正なデータ送信を阻止します。故意かどうかにかかわらず、ユーザーが重要なデータを社外に転送しないように監視します。

### 業界最高のセキュリティを提供する McAfee Web Gateway

マルウェア対策を含むWebセキュリティで業界最高の評価<sup>1</sup>を得ているMcAfee Web GatewayのMcAfee Gateway Anti-Malware Engineは、特許取得済みのアプローチ (シグネチャ レスの意図解析) でマルウェアを検出します。プロアクティブな意図解析により、Webトラフィックから未知あるいはゼロデイ攻撃の不正なコンテンツをリアルタイムで排除します。McAfee Web Gatewayは、Webページのアクティブコンテンツをスキャンし、その挙動を詳細に分析して意図を予測することで、ゼロデイ マルウェアによる攻撃からエンドポイントを保護します。これにより、システムのクリーンアップや修復にかかるコストが劇的に削減されます。

このような分析機能とMcAfeeのウイルス対策、McAfee Labsのグローバルレピュテーション技術を統合することで、既知のマルウェアと不正なサイトを迅速にブロックします。McAfee Web Gatewayは1つのプラットフォームで複数の技術を提供するので、最適な保護対策で組織のセキュリティを強化できます。また、多くの組織が必要とする多層型のセキュリティ アプローチを実現します。

- **McAfeeのウイルス対策とリアルタイムのMcAfee Global Threat Intelligence (McAfee GTI) ファイル レピュテーション:** クラウドベースのMcAfee GTIファイル レピュテーションを利用することで、システムの更新を待たずにウイルスを検出し、阻止できます。
- **McAfee GTI WebレピュテーションとWebカテゴリーライゼーション:** McAfee Web Gatewayは、レピュテーションとカテゴリによるフィルタリング機能により、高度なWebフィルタリングを行います。McAfee GTIは、McAfee Labsが世界中から収集したデータの属性に基づき、インターネット上のすべてのエンティティ (Webサイト、メール、IPアドレス) にプロファイルを作成します。さらに、セキュリティ リスクに基づいてレピュテーション スコアを割り当てるので、管理者は、許可または禁止対象に対して柔軟なルールを適用できます。
- **位置情報:** McAfee Web Gatewayは、位置情報を使用してWebトラフィックとユーザー トラフィックの発信元を特定し、トラフィックの可視化とポリシー管理を実現しています。

WebカテゴリーライゼーションとWebレピュテーションにより、オンプレミス、クラウドまたはその両方で情報を参照できます。クラウド参照により、システムの更新を待たずに検出/変更を検出し、豊富なマルウェア情報を利用して保護を行うことができます。

## データシート

### 高度脅威分析の統合

高度なマルウェア検出技術であるMcAfee Advanced Threat DefenseとMcAfee Web Gatewayの統合により、カスタマイズ可能なサンドボックスと詳細な静的コード分析を利用することができます。McAfee Web GatewayのGateway Anti-Malware Engineが提供するインライン スキャン機能とMcAfee Advanced Threat Defenseにより、インターネットで発生する脅威を最高の保護ソリューションで阻止することができます。クラウドベースのサンドボックスであるMcAfee Cloud Threat Detectionと他の脅威分析層を統合すると、コストを削減し、高度脅威分析を簡単に行うことができます。

### 脅威情報の共有

現在、多くのセキュリティ ツールが存在しますが、それぞれが個別に機能し、脅威情報を共有できる状態ではありません。しかし、重要な情報はエンドポイント、ネットワーク、SIEM (セキュリティ情報/イベント管理)、ゲートウェイなど、様々な場所に存在します。これらの情報を共有することで、脅威対策とデータ侵害の識別を強化できます。感染したシステムを効率的に修復できるので、インシデント対応を改善することができます。McAfee Web GatewayなどのMcAfee ソリューションは、McAfee Threat Intelligence Exchange によってソリューション間で脅威情報を共有し、このような問題を解決しています。McAfee Web Gatewayは、Gateway Anti-Malware Engineが検出したゼロデイ マルウェアのファイル レピュテーションを作成し、他のソリューションと共有します。これにより、新しいDATファイルがリリースされる前にエンドポイント デバイスを保護できます。McAfee Threat Intelligence Exchangeから提供される脅威情報を利用することで、より多くの脅威をMcAfee Web Gatewayで阻止することができます。

### 暗号化されたトラフィックの分析と保護

サイバー犯罪者は、企業のセキュリティ対策を破るためSSLトラフィック (HTTPS、HTTP/2) を悪用しています。皮肉なことに、セキュリティを強化するために開発されたプロトコルが攻撃に利用されるようになっていきます。McAfee Web Gatewayには、マルウェア検出、SSLインスペクション、証明書検証が統合されているので、暗号化されたトラフィックに総合的な分析を行うことができます。

SSLスキャン用にハードウェアを追加する必要はありません。McAfee Web Gatewayは、1つのハードウェアまたは仮想アプライアンス アーキテクチャですべての機能を実行します。McAfee Web Gatewayは、すべてのSSLトラフィックを直接スキャンし、暗号化されたトランザクションのセキュリティ、整合性、プライバシーを保護します。

SSLトラフィックの詳細分析を優先したい場合には、McAfee Web GatewayのSSLタップを使用します。これにより、暗号化されていないトラフィックのストリームを全体または個別にオフロードできます。ソフトウェアで有効にできる機能を使用することで、復号したSSLトラフィックの全体または一部を侵入防止システム (IPS) やネットワークベースのデータ損失防止 (DLP) などの別のセキュリティ ソリューションに送信できます。

## データシート

### データ損失対策

McAfee Web Gatewayは、SSLを含む主要なWebプロトコル経由で外部に送信されるコンテンツをスキャンし、機密情報の漏えいなどの内部からの脅威を防ぎます。コンプライアンスの状況を文書化し、漏えい発生時のフォレンジック データを提供するため、知的財産の漏えい防止に最適なツールです。McAfee Data Loss Prevention (McAfee DLP) を利用するMcAfee Web Gatewayは事前定義のDLPディクショナリに対応しています。キーワード比較や正規表現を使用してカスタム ディクショナリを作成することもできます。

組み込みのファイル暗号化機能により、クラウド ベースのストレージを利用する組織は、ファイル共有/コラボレーションサイトにアップロードされたデータを不正アクセスから保護できます。McAfee Web Gateway経由でなければ、データを取得して表示することはできません。

### モバイル環境のユーザーを保護

職場の分散化やモバイル環境への移行が進む現在では、このような環境にもWebフィルタリングとWeb保護をシームレスに展開する必要があります。不正防止を行うクライアントエージェントのMcAfee Client Proxyを利用すると、ローミングユーザーがシームレスに認証され、DMZにあるオンプレミスのMcAfee Web GatewayまたはMcAfee Web Gateway Cloud Serviceにリダイレクトされます。ローミングユーザーやリモートユーザーがコーヒESHOP、ホテル、Wi-Fiホットスポットなどのパブリック ポータルからアクセスしている場合でも、これらのユーザーにインターネット アクセス ポリシーを施行し、完全なセキュリティ スキャンを実行できます。

また、WebトラフィックをMcAfee Web Gatewayに転送することで、自社のセキュリティ ポリシーをモバイル デバイスに展開することもできます。モバイルデバイス管理プロバイダーのAirWatch、MobileIronとMcAfee Web Gatewayにより、高度なマルウェア対策と会社のWebフィルタリング ポリシーでApple iOSデバイスやGoogle Androidデバイスを保護できます。

### McAfee Web Gatewayによる柔軟な管理

McAfee Web Gatewayは、強力なルール ベースのエンジンを搭載しているため、きめ細かいポリシー管理を行うことができます。ポリシーを簡単に作成できるように、McAfee Web Gatewayでは広範なルール ライブラリと共通のポリシー アクションが用意されています。これらのルールを修正して独自のルールを作成し、オンライン コミュニティで共有できます。コンテキスト ベースのルール条件と共有リストを統合することで高度な管理を行い、問題解決とWebセキュリティを最適化できます。対話モードでルールを追跡できるので、ルールのデバッグも簡単です。

McAfee Web Gatewayは、ポリシーによる管理でWebアプリケーションの使用方法をきめ細かく制御します。この機能はクラウド アプリケーションにも利用できます。このプラットフォームは、数千以上のクラウド アプリケーションに対応しています。必要に応じて特定の機能を有効または無効にして、Webアプリケーションの利用者と使用方法を制限できます。たとえば、Dropboxへのアクセスを許可し、アップロードを禁止できます。

## データシート

ユーザー認証とアクセスも柔軟に制御できます。McAfee Web Gatewayは、NTLM (NT LAN Manager)、RADIUS (Remote Authentication Dial in User Service)、Active Directory (AD) /LDAP (Lightweight Directory Access Protocol)、eDirectory、Cookie認証、Kerberos、ローカル ユーザー データベースなど、様々な認証方法に対応しています。McAfee Web Gatewayの認証エンジンでは、柔軟なルールを実装できます。たとえば、McAfee Web Gatewayがユーザーを透過的に認証し、その結果に基づいてユーザーに認証情報を要求したり、別の認証方法を使用したりします。また、制限付きのポリシーを適用したり、アクセスを拒否することもできます。

オプションのアドオンであるMcAfee Web Gateway Identityは、人気のある多くのクラウド アプリケーションに対応したシングル サインオン (SSO) コネクタです。McAfee Web Gateway Identityにより、セキュリティを強化するだけでなく、パスワードに関連するヘルプ デスクへの問い合わせを減らすことができます。SSOランチャパッドを使用すると、1回のマウス クリックで承認済みのクラウド アプリケーションにアクセスできます。HTTP POST (Power-on Self-test) と SAML (Security Assertion Markup Language) コネクタの両方に対応しているため、様々なアプリケーションで利用できます。また、コネクタを用意することで、特定の SaaS (Software-as-a-Service) アプリケーションのユーザー アカウントを管理できます。

McAfee Web Gatewayはネイティブ ストリーミング プロキシに対応しているため、ストリーミング コンテンツのアクセス制御を行い、帯域幅の節約と待機時間の短縮を実現します。トラフィックのクラス別に最小、最大、優先値を設定して帯域幅を管理できるので、帯域幅の利用を最適化することができます。

## McAfee Web Gatewayでアジャイルなインフラを実現

McAfee Web Gatewayは、高性能なエンタープライズ クラスのプロキシで、拡張性の高いアプライアンス モデルとして適用されます。高可用性を備え、仮想化もサポートします。また、McAfee Web Gateway Cloud Serviceによりハイブリッドな配備環境のサポートを提供します。McAfee Web Gatewayには柔軟な配備オプションが用意されているため、非常に多くのユーザーを抱える環境にも対応できます。

配備オプションを組み合わせることも可能です。たとえば、ネットワーク上のユーザーの場合には、すべてのWebトラフィックをオンプレミスのアプライアンスにルーティングし、モバイル環境のユーザーの場合にはクラウドにリダイレクトすることで、MPLS (Multiprotocol Label Switching) 回線またはVPN (Virtual Private Network) 経由でのバックホール トラフィックのコストを劇的に削減できます。オンプレミスとクラウドの両方に配備しても、ポリシーの同期とレポートが自動的に実行され、一貫したポリシーが施行されます。レポート、追跡、調査も簡単に実行できます。

McAfee Web Gatewayには、明示的プロキシ、透過型ブリッジ、ルーター モードなど、様々な実装オプションが用意されています。ネットワーク アーキテクチャに合わせて実装することができます。

McAfee Web Gatewayは、ユーザー固有の環境でも動作するように、複数の統合基準に対応しています。McAfee Web Gatewayは、WCCP (Web cache communication protocol)、ICAP/ICAPS (Internet content adaptation protocol)、WebSocketプロトコル、SOCKS (Socketsecure) プロトコルを使用して他のネットワーク機器やセキュリティ アプライアンスと効率的に通信を行います。



## データシート

McAfee Web GatewayはIPv6にも対応しているので、大企業や政府機関の規制対応にも役立ちます。McAfee Web Gatewayは、内部のIPv4ネットワークと外部のIPv6ネットワークのギャップを埋め、使用可能なすべてのセキュリティ機能とインフラをトラフィックに適用します。

### 将来のニーズにも対応できる統合プラットフォーム

McAfee Web Gatewayには、複数のスタンドアロン製品で提供される保護対策が1つに統合されています。URLフィルタリング、ウイルス対策、ゼロデイ マルウェア対策、SSL (スキャン、データ損失防止、集中管理などの機能が1つのアプライアンス ソフトウェア アーキテクチャに統合されています。ファームファクターに関わらず配備を一元管理できます。1つのポリシーをオンプレミスのアプライアンス、アプライアンス クラスター、仮想アプライアンス、クラウド サービスに使用し、1つの管理コンソールで管理できます。

### セキュリティ リスク管理とレポート

McAfee Web Gatewayは、洗練されたセキュリティ管理技術であるMcAfee ePolicy Orchestrator® (McAfee ePO™) に対応しています。これにより、すべてのセキュリティ レポートを管理できます。

McAfee ePOでは、McAfee Content Security Reporter拡張ファイルにより詳細なWebセキュリティ レポートを作成できます。McAfee Content Security Reporterは、組織のWeb利用状況の把握に必要な情報とフォレンジック ツールを提供します。これにより、コンプライアンス対応、傾向の識別、問題の隔離などを行います。また、フィルタリングの設定を調整してWebセキュリティ ポリシーを施行できます。McAfee Content Security Reporterは、リソースを集中的に使用する処理を外部の独立したレポート サーバーで実行し、データを保存するため、既存のMcAfee ePOサーバーに負荷をかけることはありません。世界中でビジネスを展開する企業でも、レポート要件に合わせて拡張することができます。

### ライセンス

McAfeeでは、非常に柔軟な配備を可能にし、将来の投資を保護するため、McAfee Web GatewayとMcAfee Web Gateway Cloud Serviceのすべての機能を**McAfee Web Protection**という1つのスイート製品として提供しています。オンプレミス、クラウドまたはその両方に配備できます。必要に応じて配備オプションを選択し、高可用性を実現できます。いずれの場合も、McAfeeが提供する業界最高のマルウェア対策と包括的なWebフィルタリングを利用できます。

McAfee Web Gatewayハードウェアは別売りです。

1. AV-TESTが実施したテストで、McAfee Web Gatewayは94.5%のゼロデイ マルウェアを検出。不正なWindows 32 PEファイルの検出率は99.8%、PE以外の不正なファイルは98.63%。「McAfee Web Gateway Security Appliance Test」(McAfee Web Gatewayセキュリティ アプライアンスのテスト)、AV-TEST GmbH。



〒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 (代表)  
[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 © 2018 McAfee, LLC. 4174\_1118  
2018年11月