



McAfee Web Gateway

脅威情報を共有する高性能なセキュリティ

以前に比べるとWebで実現できることが増えています。動的なコンテンツをリアルタイムで扱うことも可能になりました。しかし、危険度も増しています。Webでは毎日のように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 アクセスに伴うリスクを大幅に軽減します。

McAfee Web Gateway

- EAL2+とFIPS 140-2 Level 2に準拠
- 複数のハードウェア モデルで使用可能。VMwareおよびMicrosoft Hyper-Vの仮想マシンにも対応。
- McAfee Advanced Threat DefenseやMcAfee Threat Intelligence ExchangeなどのIntel® Securityソリューションとの統合により、機能を補完
- 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)

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。既知の脅威と未知の脅威を阻止するだけでなく、クラウド アプリケーションに対するアクセスを柔軟に制御しなければなりません。

インバウンドとアウトバウンドの両方向を保護する包括的なセキュリティ

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 アーキテクチャです。McAfee Web Gatewayは、ユーザーが送信したWeb要求に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て、Webページを介して侵入を試みるコンテンツやアクティブ コードの特性・意図を分析し、トラフィックに潜む脅威やマルウェアを阻止します。一般的なパケット検査技術と異なり、McAfee Web GatewayはSSLトラフィックを検査し、暗号化で存在を隠す不正なコードとアプリケーションをブロックします。

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サイトにはリスクが存在します。McAfee Web Gatewayはインバウンド保護機能でこのような脅威を阻止します。リバース プロキシモードで使用すると、アップロードの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。

McAfee Web Gatewayは、業界最先端のIntel® Security Data Loss Protection技術によってHTTP、HTTPS、FTPなど、主要なWebトラフィックで送信されるコンテンツをスキャンし、アウトバウンドトラフィックを保護します。ソーシャル ネットワーク サイト、ブログ、Wikisからの流出だけでなく、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、重要な情報や機密情報、規制対象の情報を保護します。また、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も阻止します。McAfee Web Gatewayは、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

Webセキュリティのマルウェア対策で業界最高の評価¹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します。これにより、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、システムのクリーンアップや修復にかかるコストを大幅に削減することができます。

このような分析機能とIntel Security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できます。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 アプローチを実現できます。

- **マカフィー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、管理者は許可対象または禁止対象に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行います。

Webカテゴリゼーションと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することができます。

Advanced Threat Defenseの統合

Intel Securityの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実行できます。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。

脅威情報の共有

現在、多くの組織のセキュリティアーキテクチャは脅威情報を共有できる体制になっていません。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、脅威対策が強化されます。データ侵害を早期に識別し、感染したシステムを効率的に修復することが可能になります。McAfee Web Gatewayを含むIntel Securityのソリューションはすでに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、このような課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で阻止できます。

暗号化されたトラフィックの保護

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)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のプロトコルが攻撃に利用されています。McAfee Web Gatewayは、業界で初めてマルウェア検出、SSLインスペクション、証明書検証を統合したセキュリティ製品です。暗号化トラフィックを別の機器に送信し、SSLを調査する必要はありません。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。

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(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。

クラウドベースのストレージを利用する組織は、組み込みのファイル暗号化機能により、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。Web Gateway経由でなければ、ユーザーはデータを取得して表示することができません。

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。Web Gatewayの標準のデバイス管理とセキュリティ統制により、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を実施し、モバイルデバイスを保護できます。イントラネット、Wiki、Microsoft SharePointサーバーなど、社内サーバー上のコンテンツに対するモバイルデバイスのアクセスも制御できます。これらの情報は通常、セキュリティ上の理由から特定のモバイルデバイスでの使用が許可されていません。McAfee Web Gatewayをリバースプロキシとして配備することで、社内リソースに対する保護と管理を行うことができます。

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。McAfee Web Gatewayでは、ポリシーを簡単に作成できるように、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。同じ機能をクラウドアプリケーションにも使用できます。このプラットフォームは、1,600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。

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、RADIUS、AD/LDAP、eDirectory、Cookie認証、Kerberos、ローカルの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ルールを柔軟に実装できます。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することができます。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ランチャードを使用すると、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できます。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、仮想マシンもサポートします。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が存在する環境にも簡単に対応できます。

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サービスにリダイレクトすることで、MPLS回線またはVPN経由でのバックホールトラフィックのコストを削減できます。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るため、ネットワークアーキテクチャに合わせて実装できます。

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 (Socket Secure) 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。

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、セキュリティ機能と
インフラでトラフィックを保護できるように、内部
のIPv4ネットワークと外部のIPv6ネットワークの
ギャップを解消します。

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一元的に管理で
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、未知または不正なシャドウITア
プリケーションの識別、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
の負荷が増加す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

Intel Security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**とし
て提供しています。McAfee Web Protectionは、
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、Intel
Security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。



McAfee. Part of Intel Security.

マカフィー株式会社

東京本社 〒150-0043 東京都渋谷区道玄坂 1-12-1
渋谷マークシティエスト 20F
TEL 03-5428-1100 (代) FAX 03-5428-1480
〒530-0003 大阪府大阪市北区堂島 2-2-2
西日本支店
近鉄堂島ビル 18F
TEL 06-6344-1151 (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
アーク博多 5F
TEL 092-287-9674 (代)
www.intelsecurity.com

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して、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%です。— McAfee Web Gateway Security Appliance Test (McAfee Web Gateway Securityアプライアンスのテスト)、AV-TEST GmbH.

Intel、Intelのロゴ、McAfeeのロゴ、ePolicy Orchestrator、McAfee ePOは、米国法人Intel CorporationまたはMcAfee, Inc.もしくは米国またはその他の国の関係会社における商標です。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 © 2016 Intel Corporation. 1758_0916
2016年9月