



McAfee SaaS Web Protection

ネットワークを保護するクラウド ベースのWebセキュリティ

主な特長

- 連続した更新でオフネットワークを含むすべてのユーザーを変化の激しいゼロデイのマルウェア攻撃から保護します。
- インターネット使用ポリシーを施行し、ユーザーまたはグループのWeb使用状況を確認できます。
- 100以上のコンテンツ カテゴリで柔軟なコンテンツ制御が可能です。法的責任からビジネスを保護します。
- 数百のオンライン メディアとアプリケーション (ソーシャルメディア サイトを含む) を制御し、生産性を維持できます。
- プロアクティブでシームレスに拡張可能なサブスクリプション サービスです。オンプレミスで機器に投資する必要も、スタッフを用意する必要もありません。
- 実績豊富な保護対策 – McAfee SaaS Web Protection は世界中の多くの顧客とユーザーが利用しています。

Webはビジネスにとって無限の可能性を秘めています。しかし、これはサイバー犯罪者にとっても同様です。Webを介してマルウェアに感染したり、不正な侵入を受ける可能性があります。McAfee® SaaS Web Protectionは、使いやすい様々なセキュリティ機能とMcAfee Global Threat Intelligenceの最新の脅威データにより、変化の激しいWebベースの攻撃を阻止します。McAfee SaaS Web Protectionは、マカフィーのWeb/クラウド セキュリティの専門家が常時管理し、業界のベストプラクティスを実施します。脅威や不要なインターネット アクセスを効率的かつ経済的に制御できます。

Webの動的なコンテンツと対話性により、従来のセキュリティ対策では検出されない巧妙な脅威が増えています。従業員、顧客、ネットワーク、知的財産を保護するには、プロアクティブなWebセキュリティを導入する必要があります。既知の不正なURLをブロックするだけでは不十分です。未知の攻撃や痕跡を隠す攻撃、複合型の攻撃、スパイウェアも阻止できるソリューションが必要です。McAfee SaaS Web ProtectionはWebコンテンツの動作とコンテキストを識別し、McAfee Gateway Anti-Malware Engineを使用して攻撃の意図を予測します。これにより、他のセキュリティソリューションでは見逃してしまう脅威を防ぎ、ネットワークを保護します。

Webへのアクセスを制限なく許可すると、ユーザーが私的に利用したり、法的な問題が発生する可能性があります。しかし、インターネット アクセスを監視して適切な利用状況を維持するために、多くのリソースが必要になる場合があります。マカフィーのクラウド ベースのコンソールを使用すると、ポリシー ルールを簡単に設定し、オンライン コンテン

ツ、メディア タイプ、アプリケーションをきめ細かく制御できます。また、特定のWebサービスに対するアクセス時間も制限できます。

ハードウェアやソフトウェアを新たに用意する必要はありません。McAfee SaaS Web Protectionは、信頼性が高く、コスト効率に優れたソリューションで、包括的なWebセキュリティを提供します。このグローバルなサービスは実績豊富なSaaS (Software-as-a-Service) プラットフォームを利用しているので、ほとんど遅延がなく、業界最高の稼働時間とエンタープライズ クラスの拡張性を実現しています。広範囲に分散している環境や要件の厳しい環境でも十分に耐え得るパフォーマンスを提供します。オンプレミスのWebフィルタリングを使用している環境でも、弊社のリスクの少ない低価格のソリューションを利用すると、高度なマルウェア対策でセキュリティを強化するだけでなく、支店やモバイル ユーザーも簡単に保護することができます。

主な要因

- 既存のWebセキュリティ技術のメンテナンス コストを抑えたい
- マルウェアの問題が増加している
- リモート ユーザーやモバイル ユーザーにもエンタープライズ クラスのセキュリティが必要

McAfee Global Threat Intelligenceが世界中の脅威データを収集

Web脅威と不正なコンテンツは世界中に存在しています。マカフィーでは、このような脅威を調査するため、McAfee Global Threat Intelligence ネットワークを構築しています。このネットワークは120を超える国に配備されている1億台以上のセンサーから脅威情報をリアルタイムで収集して分析し、結果を配布しています。

- 北米では、スパムURLがWeb脅威の41%を占めています。これに不正なサイト、疑わしいサイトが続いています。
- ヨーロッパ/中東/アフリカでは、スパムURLとフィッシング詐欺URLがそれぞれ全体の31%を占め、不正なサイトが29%を占めています。
- ラテンアメリカでは、不正なURLの36%にスパムに関連し、30%がフィッシング詐欺に関連しています。それ以外の不正サイトに関連しているURLが全体の25%を占めています。
- アジア/太平洋地域では、全体の31%が不審なサイトで、これらのサーバーは厳重な監視が必要なサイトとして登録されています。これに続くのがスパムURLで、全体の29%を占め、不正なサイトは24%です。

(情報ソース: McAfee Labs)

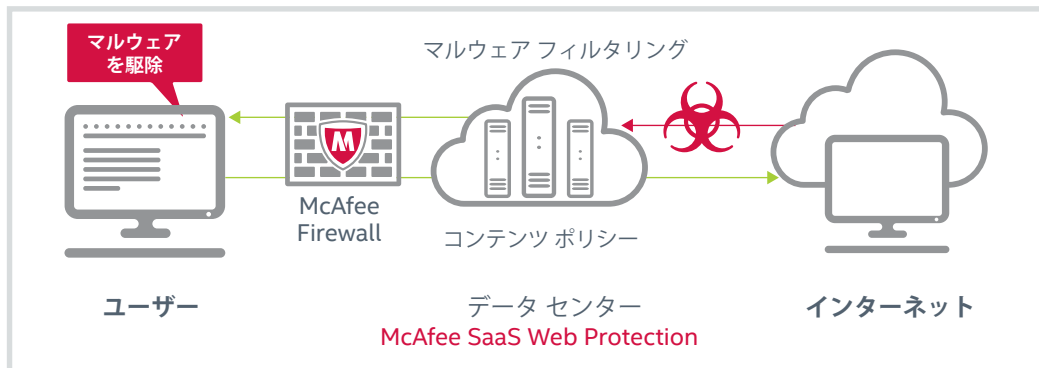


図 1. McAfee SaaS Web ProtectionでのWeb要求のフロー

完全なWeb保護

McAfee SaaS Web Protectionは、送受信されるすべてのWebトラフィックを保護します。ポリシーで制限されたWebトラフィックにアクセス ルールを自動的に適用し、組織のインターネット利用ポリシーを施行します。ポリシーに違反するトラフィックはネットワークに入る前にブロックされます。McAfee SaaS Web Protectionは、高度なマルウェア対策エンジン、ウイルス対策、グローバル脅威レピュテーション フィルターなどの洗練された技術を使用して、要求されたWebページのコンテンツとアクティブ コードを分析し、その性質と意図を特定します。不正なページをブロックし、脅威となる要素を除去して安全なコンテンツを配信することでマルウェア、ウイルス、エクスプロイトを阻止します。ユーザーはそのまま作業を続けることができます。

コンテンツ分析で、変化するマルウェアを検出

知らないうちにWebサイトのマルウェアがダウンロードされ、知的財産や顧客情報が流出する可能性があります。実績豊富なMcAfee Gateway Anti-Malware Engineを使用してWebページのアクティブ コンテンツをスキャンして、その意図や動作を分析することで、情報を盗み出すゼロデイ マルウェア、複合型脅威、フィッシング詐欺サイト、標的型攻撃からプロアクティブに保護します。

柔軟で包括的な制御

ビジネス環境でのWebの利用は諸刃の剣です。生産性や利便性の点では欠かせないものですが、不正な活動の温床となる場合もあります。ユーザーをマルウェアから保護することは重要ですが、他にもやるべきことがあります。データ漏えいを防ぎながら従業員の生産性を維持できれば、コストを削減し、法的責任を回避できます。

約100のサイト カテゴリ、数百のメディア タイプ、1,000以上のオンライン アプリケーション、暗号化されたSSLトラフィックに対応しているWebフィルタリング オプションにより、攻撃や生産性を阻害する活動からWebアクセスを保護できます。ユーザーも遅延なくWebを利用することができます。また、次の機能も利用できます。

- 特定のWebアプリケーションにドリルダウンし、ソーシャル メディア サイトへのアクセスを許可する時間を設定できます。
- オンライン ファイル共有サイトへのアップロード機能を無効にしたり、アップロード前にファイルの暗号化を施行してデータの流出を防ぐことができます。また、外部の協力者が作成したファイルのダウンロードを許可できます。
- エンタープライズ クラスのセキュリティを施行しながら、リモートまたはモバイル環境の従業員が自分の判断でWebにアクセスできるようにします。

ブロックするインターネット アクセスを柔軟に設定できるので、セキュリティを維持しながら生産性を向上させることができます。

透過型の認証とオフネットワークでの保護

McAfee SaaS Web Protectionでは、従業員のWebトラフィックを簡単にルーティングできます。ブラウザのプロキシ設定やプロキシ自動設定 (PAC) などの標準的なルーティング技術を使用することも、McAfee Client Proxyを利用することもできます。この無料のクライアントソフトウェアを使用すると、認証とリダイレクトをシームレスに実装できます。ブラウザ プラグインやCookieを管理する必要はありません。中央のハブへのバックホールトラフィックやPACファイルの作成も不要です。不正防止機能のあるMcAfee Client Proxyでは、Web保護ポリシーとWebセキュリティをオフネットワークのローミング ユーザーにも適用できます。コーヒーショップ、ホテル、Wi-Fiホットスポットなどのパブリック ポータルを介してインターネット アクセスが提供されている場合でも適用できます。

便利な管理機能とレポート

カスタマイズ可能なダッシュボードにより、管理者は傾向を監視し、組織のWeb/電子メール リソースの使用状況を把握できます。ブラウザで問題を隔離し、不適切なアクティビティを記録してコンプライアンス対応を行うことができます。また、フィルタリングの設定を調整し、Web利用ポリシーを施行できます。ポリシー違反やブロックされたWebコンテンツをユーザーに通知したり、管理アラートで重要なセキュリティ イベントをすぐに確認できます。

詳細

マカフィーのクラウドベースのセキュリティ サービスを利用すると、ビジネスを簡単に、手頃な価格で保護できます。**McAfee SaaS Web Protection**と一緒に**McAfee SaaS Endpoint Protection**、**McAfee SaaS Email Protection**、**McAfee SaaS Email Archiving**サービスを使用すると、すべてのデジタル脅威と脆弱性に対応できます。

マカフィーでは、SaaS型のサービス以外にも、柔軟なソリューションを必要とするユーザー向けにアプライアンス、仮想、SaaSを含むオールインワンのソリューションを用意しています。

詳細については、www.mcafee.com/saasまたはwww.mcafee.com/webprotectionをご覧ください。



McAfee. Part of Intel Security.

東京本社 〒150-0043 東京都渋谷区道玄坂 1-12-1
渋谷マークシティ東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 13 階
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)
www.intelsecurity.com

IntelおよびIntelのロゴは、米国法人Intel Corporation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。McAfeeおよびMcAfeeのロゴは米国法人McAfee, Inc.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。本資料は情報提供を目的としています。ここに記載されている製品計画、仕様、説明は予告なしに変更される場合があります。本資料の内容について弊社はいかなる保証も行いません。Copyright © 2014 McAfee, Inc. 61131ds_saas-web-protection_0514B