

マカフィー スпамキラー フォー マイクロソフト エクステンジ スモール ビジネス

McAfee SpamKiller 2.0 for WebShield Appliance 2.7

スパムメール対策ソリューション (McAfee SpamAssassin™搭載)

McAfee® SpamKiller™ for WebShield® Appliance は、SMTP メールに対してルールベースの業界屈指のスパムメール保護機能を提供します。最適なパフォーマンスチューニングが施されて、McAfee SpamKiller は WebShield Appliance の追加オプションとして、95%の正確な検出により、スパム対策機能を提供します。McAfee SpamKiller for WebShield Appliance は、外部からの電子メールが社内ネットワークに到着する前にスキャンすることで、増加傾向にあるスパム対策コストを劇的に削減することが可能です。

スパムメールとは

増加するスパムメールの定義

スパムメールにはさまざまなとらえ方があり、あるユーザにとってはスパムメールでも、別のユーザにとっては有益な情報である場合があります。McAfee では、スパムメールの定義を明確化するために、スパムメールを「**悪性スパム**」、「**広告スパム**」、「**フレンドリースパム**」の3つのカテゴリーに分類しています。「悪性スパム」は、不適切なコンテンツやセキュリティの脅威などを伴う電子メールです。「広告スパム」は、製品やサービスを販売する企業が送信するPRを目的とした電子メールです。「フレンドリースパム」は、ジョーク、チェンレターやユーモラスな URL リンクを含む電子メールです。

また昨今のさまざまな調査結果から、スパムメールが大幅に増加していることが分かっています。組織が受信する電子メールの **25 パーセント** から **50 パーセント** をスパムメールが占めるという予測も多数あります。

単なる迷惑メールを超えたスパムメール

甚大な被害

2003年には、米国企業が迷惑メールによって10億ドルの損害を被ると予想されています。また、欧州が最近実施した調査によると、スパムメールがインターネットユーザに与える被害は**年間100億ユーロ(日本円で約1.38兆円)**にのぼっています。

スパムメールによる企業の金銭的損失は、以下の3種類に分けられます。

生産性損失 不要なメールを読んで処理するためにユーザが費やす時間。ユーザの生産性損失は、企業のスパムメール関連コストの中でも最高額を占めると予測されています。

不適当なコンテンツ 相手に不快感を与える電子メールで、人権侵害にもつながります。この種のメッセージは個人やグループをターゲットにしたもので、アダルトコンテンツなどを一方的に送信します。

ITリソースの消費 ネットワークに侵入したスパムメールにより、ネットワーク帯域幅が占領されます。

McAfee Spamkiller テクノロジ

Powered by McAfee SpamAssassin

McAfee SpamKiller for WebShield Appliance の中核となるテクノロジーは、**McAfee SpamAssassin™ エンジン**です。SpamAssassin エンジンは、一連のテストを基準に電子メールの質を評価する「**スコアシステム**」機能を持っています。この高度なスコアシステム機能が全スパムメールのうち**95 パーセント**を自動検出し、誤検出率を非常に低い**0.05 パーセント未満**におさえます。製品に組み込まれたデフォルトルールを McAfee が管理するため、ルールの設定も必要ありません。McAfee SpamKiller for WebShield Appliance は、インストール終了と同時に、すぐれたスパム検出効果を発揮します。

スコアシステム機能

電子メールを正確に識別

SpamAssassin エンジンは、「**スコアシステム**」機能を利用して、特定の電子メールがスパムメールであるかどうかを確定します。まずそれぞれの電子メールは、プラス(+)またはマイナス(-)のスコアを持つ数百種類のルールと照合されます。マイナスのスコアルールは正規メール、プラスのスコアルールはスパムメールの属性です。このスコアを合計することにより、各電子メールの「総合スパム評価」を算出します。過去から蓄積された膨大な数のスパムメールと正規メールの情報を、遺伝アルゴリズム^{注1}によって最適化し、各ルールのスコアを決定します。そして SpamKiller ESB は、サーバまたはユーザ専用のジャンクメールフォルダにスパムメールを移動します。電子メールがビジネスインフラストラクチャに欠かせない構成要素となっている現在、スパムメール対策ベンダーにとって誤検出を最小限に抑えることは非常に重要な課題です。スパムメール識別のあいまいな部分を明確化する「**スコアシステム**」機能は、スパム対策に欠かせない機能です。

【注1】 遺伝アルゴリズム

生物界では、任意の生物種は移行行く環境変化への適応の善し悪しで何世代もかけて自然淘汰されています。結果として環境により良く適合した遺伝子を持った多数の個体からなる生物種が生き残ることになります。この生物種の進化過程をほとんどそのまま真似る形で、スパム認識の適用を逐次改良する解析方法。

マルチレベルのスパムプロテクション

5段階の徹底的な検出

McAfee SpamKiller for WebShield Appliance は、基本のデフォルトルールセットプロセスを利用して、受信した各電子メールメッセージを検査します。McAfee SpamKiller for WebShield Appliance は、5種類の検出方法を備えています。

整合性の分析 (Integrity analysis) – McAfee SpamKiller for WebShield Appliance は、各電子メールのヘッダー、レイアウトと構成を検査し、スパムメール特有の特徴を持っているかどうかを分析します。メール受信時の一連の検査過程の中で、最先端のパターン照合エンジンが膨大な数の情報と受信したメールを照らし合わせ、スパムメールであるかどうかを確定します。これは非常に正確な方法であり、スパムメッセージを確実に検出することが可能となります。

ヒューリスティック検出 (Heuristic detection) – これはスパムメールの疑いがある電子メールを検出する機能です。さまざまな内部テストを実行し、電子メールがスパムメールであるかどうかを決定します。また、各テストのスコアを利用して、誤検出を低減させます。McAfee SpamKiller for WebShield Appliance は、パワフルなヒューリスティック検出機能を活用してスパムメールをプロアクティブに処理し、ユーザ環境をスパムメールから保護します。

コンテンツフィルタリング (Content filtering) – この機能を利用して、電子メールに含まれるスパムメール特有のキーワードやフレーズを検索します。管理者またはユーザがデータベース上に特定の語句や文章を追加することで、不適切なコンテンツを定義することができます (サーバ用ソフトウェアを使用する場合は管理者、クライアント用ソフトウェアを使用する場合はユーザが語句を追加します)。

ブラックリスト^{注2}とホワイトリスト^{注3} (Black and white lists) – 管理者は、「ブラックリスト」および「ホワイトリスト」設定機能を利用してサーバレベルで基準を設定し、組織内の全ユーザのスパムメールを定義することができます。さらに、各ユーザが独自の「ブラックリスト」と「ホワイトリスト」定義して、デスクトップでルールを補足することも可能です。ユーザが「ブラックリスト」と「ホワイトリスト」をカスタマイズし、ユーザが各自のリストを表示したり、編集することができます。このパワフルな機能を利用して、スパムメールの最終的な定義をエンドユーザに任せられるため、システム管理者は時間を有効活用できるようになります。

RBL のサポート – スパムメール送信者として知られている送信元をリスト化している RBL (Real-time Blockhole List) を元に、検索し、ブロックすることができます。

スパムメールのマーキング

誤検出の低減

電子メールをスキャンし、低いスパムスコアであった場合、メッセージは「潜在的なスパム」としてマークされます。管理者は、メッセージ件名にマークを追加して送信、またはヘッダ内の「X-フィールド」にスパムスコア、スパムと該当した短縮リスト、広範なスパム検出結果を追加するなど選択が可能です。この機能により、ユーザは自分のメールボックス内でスパムメールか否かの可能性に応じて、自動的にメール振り分けを行えます。

メッセージの取扱

自社内のスパムコントロール

電子メールをスキャンし、中程度あるいは高いスパムスコアであった場合、管理者はそのメッセージをブロック、許可、破棄、または WebShield Appliance 内のメールボックスストアに転送する選択が可能です。他のメールボックスに隔離メールとして転送することにより、管理者は隔離されたスパム隔離ファイルを自社メール環境内のほかのツールを使い管理することが可能です。

詳細なレポートの作成

ePolicy Orchestrator™ と統合することで、WebShield Appliance、はゲートウェイ上のスパムメール アクティビティをグラフィカル レポートで表示することが可能です。詳細なレポートについては、「トリガーとされたスパムルール」、「トップ スパム送信者」、「トップ スパム受信者」、「破棄されたメッセージ数」、「マークされた、あるいはブロックされたメッセージ パーセンテージ」など McAfee SpamKiller for WebShield Appliance のあらゆるログから抽出されます。さらにレポートに加え、ゲートウェイ上のスパム アクティビティの時系列ビューにより傾向分析をすることが可能です。

システム要件		
・ WebShield e250 Appliance, WebShield e500 Appliance, および WebShield e1000 Appliance 上で動作		
・ アプライアンスの追加ソフトウェア コンポーネントとしてインストール		
電子メール パフォーマンス		
各アプライアンスにより、また使用するスキャン処理によりパフォーマンスが異なります。		
e250	e500	e1000
スパムフィルタリングのみ		
30,000 /h	55,000 /h	80,000 /h
スパムフィルタリングおよびコンテンツフィルタリング		
25,000 /h	40,000 /h	60,000 /h
スパムフィルタリング・コンテンツフィルタリング・ウイルススキャン		
20,000 /h	35,000 /h	50,000 /h

[注2] ブラックリスト - スパムメールの差出人リスト

[注3] ホワイトリスト - 正規 (スパムメールではない) メール差出人リスト



日本ネットワークアソシエイツ株式会社 www.nai.com/japan/

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

名古屋営業所 〒460-0002 愛知県名古屋市中区丸の内 2-20-25 丸の内 ST ビル 8F
TEL: 052-203-8421(代) FAX: 052-203-8422

西日本営業所 〒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

福岡営業所 〒812-0013 福岡県福岡市博多区博多駅東 1-10-27 アステリア博多ビル 8F
TEL: 092-452-3511(代) FAX: 092-452-3515