

SpamKiller白書

バージョン2.4

1. はじめに.....	3
2. スпам対策テクノロジー.....	3
2.1 コンテンツフィルタリング.....	3
2.1.1 誤検出と見逃し.....	4
2.2 ブラックホールリスト.....	4
3. 現在のビジネスの要件.....	4
3.1 McAfee のスパム対策ソリューション.....	5
3.2 SpamKiller 製品シリーズ.....	6
4. SpamKiller 製品の仕組み.....	7
4.1 各ルールにデフォルトスコアを割り当てる方法.....	7
4.2 SpamAssassin のルール.....	8
4.3 スコアによりメッセージをスパムメールと判断した場合の処理.....	10
4.4 ルールとスコアの編集.....	13
4.5 SpamKiller のアップデート.....	14

1. はじめに

現在、電子メールは、ビジネスにおける最も重要なコミュニケーションツールとして認識されています。META Group が最近実施した調査によると、ユーザの80パーセントが、主なビジネス コミュニケーション ツールとして電話ではなく電子メールを利用しています。その理由として、複数の相手とすばやく通信できることと、インタラクショ

ンの記録を生成できることが挙げられます。

当然のことながら、ユーザは毎日受信する大量の電子メールに悩まされています。中には、1日に 200 通以上の電子メールを受信するユーザもいます。この場合、電子メールの管理に数時間を費やすことにもなりかねません。

IDC が作成した最近の報告書によると、2002 年には1日 200 億通もの電子メールが送信されており、2006 年までにはこの数が 600 億通に増加する見込みです。さらに、電子メールの利用度の増加も見込まれているため、管理者とユーザは電子メール管理を合理化するための手段を求めています。

このような状況の中で、スパムメールが注目を浴びています。業界では、スパムメールを UCE (Unsolicited Commercial Email: 迷惑な商用メール) と UBE (Unsolicited Bulk Email: 迷惑な大量メール) の2種類に分類しています。スパムメールは、ユーザに一方的に送りつけられる迷惑メールとして定義されます。

電子メールは、職場と家庭の両方で一般的なコミュニケーション手段として定着しています。マーケティング会社は、この機会を利用して、電子メールでさまざまなメッセージを送信しています。

金銭的な面では、電子メールによるマーケティングは非常に経済的です。電子メールアドレスを無作為に集めた配信リストは、最低 10 ドルで利用できます。また、的を絞った上質な顧客データの利用コストは 500 ドルから 1,000 ドルほどです。連絡用の電子メールアドレスを一旦入手すれば、電子メールマーケティングは最低限のコストで展開できます。これに対し、マーケティングメッセージを郵送する場合は、書類代と郵送料がかかります。

初期のスパムメール事件のひとつに、1994 年4月の Canter & Siegel (C&S) 社のものがあります。同社の2人の弁護士が、わずか 90 分の間に、Usenet ディスカッションフォーラムの 6,000 以上のグループにスパムメールを送信しました。その内容は、「米国グリーンカード抽選 - 外国人に米国労働許可証があたる絶好のチャンス」という広告でした。C&S は、一人あたり95ドル、夫婦の場合は145ドルで申請書記入を代行すると宣伝しました(ただし、グリーンカード申請書が無料配布されていることは伝えませんでした)。その結果、同社とその ISP である Internet direct に、世界中から苦情が殺到しました。この ISP は C&S のアカウントを閉鎖しましたが、2人の弁護士はアカウントを再開しないと25万ドルの損害賠償訴訟を起こすと脅しました。結局アカウントは再開されませんでした。この弁護士たちはその後、インターネット商法でもうけるためのアドバイスをまとめた『How to make a fortune on the Information superhighway』(情報スーパーハイウェイで大もうけする方法)という本を出版しました。

この事件以来、多くの組織が、迷惑メールをブロックするための既存および新テクノロジーの導入を開始しました。

2. スпам対策テクノロジー

2.1 コンテンツフィルタリング

第一世代のスパムブロッカーの多くは、既存のコンテンツフィルタリングを利用して、迷惑メールに関連した既知のキーワードやフレーズをもとに電子メールメッセージを検出し、排除するものでした。この方法は、現在の多数のソリューションの基本的な要素となっています。

たとえば、「Viagra」(バイアグラ)という言葉を含むメールは広告である可能性が高いため、スパムメールと見なされ、排除されます。ここでの問題は、このルールが適さない場合もあるということです。たとえば、製薬産業では、バイアグラという言葉は正規の電子メールで日常的に使われています。

スパム対策ベンダーには、「chicken breast」のような話もつきものです。性的な内容の電子メールをブロックする一般的なルールは、「breast」(胸)という言葉をもとにフィルタリングを実行します。しかし、このルールを設定すると、「chicken breast」(鶏の胸肉)という言葉を含む正規メールもブロックされてしまいます。

2.1.1 誤検出と見逃し

誤検出 (False positive)

これは、スパム対策テクノロジーの最も重要な要素に関連しています。迷惑メールの受信を防止する一方で、正規メールの削除、フィルタリングによる除去や遅延を防ぐ必要があります。正規メールが影響を受けた結果、多大なコストが発生する可能性があります。たとえば、入札時に顧客に送った見積りがスパムメールとして誤検出されたために、競争相手に契約の機会を奪われてしまうケースなどが考えられます。これが、正規メッセージがスパムメールとして検出される誤検出の概念です。

見逃し (False negative)

一般的に、スパム対策製品は、検出するスパムメールの数を基準に評価します。迷惑メールの検出に失敗することを、見逃しと呼びます。

実際のビジネスの世界では、誤検出によって発生するコストが見逃しによるコストを大幅に上回る可能性があります。

2.2 ブラックホールリスト

2003年4月、AOL Time Warner社が大手スパムメール送信企業5社を相手に訴訟を起こしました。米国最大のインターネットサービスプロバイダであるAOLによれば、スパムメール送信企業がAOLメンバーに約10億通のスパムメールを送信した結果、800万件以上の苦情が発生しています。スパムメールの内容は、ポルノ、美容関連詐欺、ダイエット用品や金融関係の勧誘でした。この訴訟は、合計1,000万ドルの損害賠償とスパムメール活動の停止を5社に求めるものでした(うち2社の社名は公表されていますが、残り3社の社名は非公認です)。

この訴訟は、既知の多数のスパムメール送信者の存在を浮き彫りにしています。また、2番目に普及度の高いスパム防止策であるRBL (Realtime Blackhole List) が現在も使われています。このスパム対策は、一般的に契約ベースで提供されています。

RBLの目的は、メールホストサイトまたはメールアカウントを基準に電子メールをブロックすることです。このアプローチの利点は、コンテンツフィルタリングなどのテクニックを使ったメッセージの有効性確認が不要であることです。RBL上にあるサイトやユーザからのすべてのメールが、スパムメールと見なされます。

コンテンツフィルタリングと同様に、RBLも完璧な問題解決手段とはいえません。RBLは動的で、その多くが特定の送信元に焦点をあてたものです。また、特定のスパムメール送信者を確定するまでは、スパムメールの送信元として識別したホストサイトがブロックされます。

正規メールへの潜伏は、検出を回避するためにスパムメール送信者が頻繁に使う手段です。そのため、RBLプロバイダがスパムメールの送信元を特定するまでは、正規メールの送信者がスパムメール送信者と混同される可能性があります。

3. 現在のビジネスの要件

1980年代以来、迷惑メールを正規メールとして隠蔽する方法が激増したため、このようなメールを検出してブロックするための対策が実施されています。

Ferris Researchの調査では、現在スパムメールにより発生しているコストは、米国企業で89億ドル、ヨーロッパの企業で25億ドル、さらに米国とヨーロッパのサービスプロバイダで5億ドルに上ります。

同社によれば、米国に拠点を置く ISP の着信電子メールの 30 パーセント、米国に拠点を置く企業の着信電子メールの 15 パーセントから 20 パーセントをスパムメールが占めています。この差は、企業電子メールの一部が社内に限定されているために生じます。

英国の BT Openworld の発表によると、2003 年 3 月に電子メールを 1 週間モニターした結果、英国ユーザあての電子メールの 40 パーセント以上がスパムメールでした。一方、ウイルスに感染した電子メールの割合は、220 通に 1 通でした。

ユーザによる正規メールの送受信をさまたげずに、フィルタリングによって迷惑メールを除去する機能が、今日の効果的なスパム対策ソリューションの条件となっています。

3.1 McAfee のスパム対策ソリューション

McAfee ソリューションには、2001 年の WebShield e500 Appliance のリリース以来、スパム対策機能が組み込まれています。



ゲートウェイ上に設置されるこのアプライアンスは、一般的なインターネットプロトコル (SMTP、HTTP、FTP と POP3) をモニターし、悪性コードを検出します。さらに、迷惑メールの一般的なフィルタリング機能を含む、ウェブおよび電子メールのセキュリティ管理機能を提供します。

以下に、具体的な機能の例を紹介します。

- ・SMTP トラフィックのコンテンツフィルタリングにより、迷惑メールに含まれるキーワードと語句を検出します。
- ・スパム対策オプション：
 - (1) 迷惑メールを送信する既知の電子メールアドレスとドメインのリスト (ブラック ホール リスト) を契約ベースで利用できます。
 - (2) 電子メールアドレスを基準に、電子メールのフィルタリングを実行します。

現在 McAfee では、要件に合わせたさまざまなハードウェア仕様でこのアプライアンスを提供しています。いずれの仕様でも、共通のソフトウェアを利用します。

GroupShield 製品にもスパムフィルタリング機能が搭載されており、件名と本文のフィルタリングが可能です。この機能を利用して、キーワードと語句をもとに迷惑メールを除去できます。

McAfee では、迷惑メールの世界的な増加に対応するため、2002 年初めに Deersoft SpamAssassin スキャンテクノロジーを取得しました。現在、このテクノロジーは、企業向け製品である McAfee SpamKiller の中核となっています。

これらの製品は、独立した製品として利用することも、GroupShield ウイルス対策製品および WebShield アプライアンスと統合して、電子メール管理機能を拡張することもできます。

McAfee が提供する製品とサポート可能なプラットフォームについては、以下の McAfee ウェブサイトを参照してください。

<http://www.nai.com/japan/products/>

3.2 SpamKiller 製品シリーズ

このドキュメントでは、McAfee 製品に使用するスキャンテクノロジーである SpamAssassin エンジンに言及します。

SpamKiller は、McAfee がこのエンジンを活用して開発した製品ブランドです。McAfee は、2003 年中に、さまざまなプラットフォーム用の SpamKiller をリリースする予定です。その目的は、ネットワークを柔軟かつ完全にカバーすることです。

SpamKiller 2.0 for Microsoft Exchange Small Business

(2003 年 6 月リリース) Microsoft Exchange 2000 上で最大 500 個のメールボックスをスキャンするこの製品は、ユーザの受信ボックスに新規メッセージを書き込む OnSyncSave API を監視します。SpamKiller は、この API を利用してメッセージを傍受し、検査を実行する SpamAssassin エンジンに引き渡します。

この製品は Exchange 2000 環境で動作するため、このプラットフォーム用の特殊なオプションを利用できます。以下はその例です。

- ・ スпамメールをユーザ受信ボックスのジャンクフォルダ、または共用フォルダに転送します。この製品は Exchange 環境に統合されるため、ユーザの受信ボックスにジャンクフォルダを作成し、このフォルダにメッセージを転送することが可能です。
- ・ ユーザ個人の連絡先リストを、各ユーザのホワイトリスト(信頼性の高い電子メール送信者のリスト)に追加します。ユーザは、この製品のウェブインターフェースを利用して、各自のブラックリストとホワイトリストを編集できます。
- ・ Microsoft 2000 環境を基盤とする Small Business パージョンは、すべてのメールボックスのスキャンと、ユーザ受信ボックスの特定の Active Directory グループのスキャンをサポートします。

SpamKiller 2.0 for WebShield Appliance 2.7

(2003 年 9 月リリース) SpamKiller for WebShield Appliances は、アプライアンスの既存フィルタを利用して SMTP トラフィックを傍受し、ウイルス対策とコンテンツフィルタリングを実行します。このフィルタがキャッチした SMTP メッセージは SpamAssassin エンジンに引き渡され、スキャン実行後にウイルス対策エンジンに転送されます。

WebShield Appliance パージョン 2.7 には、SpamKiller の 30 日間の試用バージョンが含まれています。

30 日の試用期間終了後に SpamKiller を使用するためには、ネットワークアソシエイツからライセンスを購入する必要があります。続いて、トライアルライセンスを購入したライセンスに切り替えるためのアップグレード CD が送付されます。

注: この場合、WebShield Appliance ソフトウェアを再インストールする必要はありません。

WebShield Appliance では、コンテンツフィルタリング、専用ブラックリストおよびホワイトリストの作成やリアルタイム リストの自動配布などの、基本的なスパムオプションを利用できます。SpamAssassin テクノロジーの追加により、WebShield Appliance を完全なウイルス対策およびスパム対策ソリューションとして活用できます。

SpamKiller 2.1 for Microsoft Exchange

この製品には、(2003 年 12 月リリース予定) GroupShield ウイルス対策と統合された製品と、独立した製品の 2 種類があります。また、GroupShield コンソールにインストールする方法と、スタンドアロン製品としてインストールする方法があります。

機能的には、従来 Small Business Edition とよく似ていますが、スキャンが可能なメールボックスの数の制限がありません。また、Microsoft Exchange 2000 および 2003 をサポートする予定です。

SpamKiller 2.1 for Lotus Domino

前出の(2003年12月リリース予定)Microsoft Exchangeバージョンと同様の機能を備え、Dominoバージョン5.0および6.0もサポートする予定です。

上記バージョンの詳細な情報は、製品リリースに合わせてMcAfeeウェブサイトで公開する予定です。

ローカライゼーションのサポート

現在のSpamAssassinエンジンは、英語のテキストコンテンツを含むスパムメールのみを検出します。

ここで、ヘッダールールの例を紹介します。ヘッダールールは、言語に関係なく、メッセージのルーティング履歴を調べます。件名に含まれるキーワードを検出するヘッダールールは、英語のメッセージを対象としたものです。ただし、「teen」などのキーワードは、スパムメールで使われる多数の語句と同様に、一般的に認識されているものです。「Viagra」(パイアグラ)なども、ほとんどの言語で共通のブランド名です。

今後は、テキストコンテンツルールをローカライズする可能性があります。ただし、これまでの経験から、世界中で現在送信されているスパムメールの多くがアメリカ英語で書かれていることがわかっています。

4. SpamKiller 製品の仕組み

ネットワークアソシエイツのSpamAssassinエンジンは、すべての一般的なスパム検知テクニック(650以上のルール)を利用し、それぞれのルールに加重スコアを割り当てることによって、スキャン対象の電子メールを累積的に評価します。

SpamAssassinエンジンは、この方法により、有効な電子メールと迷惑メールを総合的に評価します。

一般的に、メッセージをスパムメールに分類するためには、3つ以上のルールが必要です。この方法は、単一のルールと一致したメッセージをスパムメールに分類する伝統的なアプローチよりもはるかに正確です。



SpamAssassinエンジンのそれぞれのルールには、スコアがあらかじめ割り当てられています。総合的なスコアが5を超えたメッセージは、SpamAssassinによって自動的にスパムメールに分類されます。

ルールの中には、負のスコアを持つものもあります。このようなルールは、誤検出(スパムメールに似た正規メッセージをスパムメールとして検出すること)を防ぐためのものです。

4.1 各ルールにデフォルトスコアを割り当てる方法

ネットワークアソシエイツには、30万以上のメッセージを集めたデータベースがあります。それぞれのメッセージは、人間の手によって、スパムメール、正規メール、またはこの2つの範囲の中間のメールに分類されています。

ネットワークアソシエイツの開発チームは、人工知能(AI)の一種である遺伝的アルゴリズムを利用します。

遺伝的アルゴリズムに関する非常に科学的な説明は、インターネットで参照できます。このアルゴリズムを最も簡単に説明すると、進化する人間行動をもとに開発された、コンピュータベースの学習モデルということになります。

たとえば、遺伝的アルゴリズムは、生成と反復を行うたびに、前回の経験から学習して適応します。

SpamAssassin は、このテクニックを利用して、各ルールの加重スコアを最適化します。SpamAssassin エンジンのルールは、人間が作成した各ルールのスコアを基準に、30 万件の既知の電子メールと照らし合わせてテストされます。

続いて、AI テクノロジーが、現在のルールスコアをもとに、予測される結果と照合してスパムフィルタリングの効果を調べます(すべてのテストメッセージは、人間の手によって分類されています)。

さらに、検出率の向上と誤検出の低減を図るため、スコアを調整します。ルールのスコア変更とテストの再実行を、生成サイクルとして考えることができます。

遺伝的アルゴリズムは、膨大な数の生成サイクルを実行し、既知の結果と照らし合わせることによって、定義されたルールセットに最適なスコアの組み合わせを定義します。

4.2 SpamAssassin のルール

McAfee SpamKiller 製品で利用する SpamAssassin エンジンには、電子メールのメッセージをテストして迷惑メールを検出するための、650 種以上のデフォルトルールが含まれています。

管理者は、SpamKiller インターフェースを利用して既存のルールを有効化または無効化し、標準と異なる企業独自の要件に適合させることができます。たとえば、製薬会社の場合、「Viagra」(バイアグラ)という言葉を含む電子メールの受信が必要かもしれません。一方、銀行などの金融機関にとっては、このメールが迷惑メールである可能性があります。SpamKiller は、環境に合わせてテクノロジーをカスタマイズするための柔軟性を提供します。カスタマイズについては、のちほど詳しく説明します。

つぎに、SpamKiller 製品を使ったスパムメールの検出に SpamAssassin エンジンが利用する主なルールの種類と、その仕組みを紹介します。

ヘッダールール

電子メールのヘッダーには、以下のような情報が含まれます。

- ・宛先
- ・差出人
- ・件名
- ・送信日
- ・受信ヘッダー(電子メールをルーティングする各リレーポイントで、ヘッダーに追加されるリレー情報)
- ・アプリケーションヘッダー(Exchange や AOL の電子メール クライアント ヘッダー)
- ・Xヘッダー

以下は、スパムメッセージを判別するための電子メールのヘッダーの検査に利用するルールの例です。

- ・コンテンツルール - スパムメールの件名で一般的に使われる語句を検出します。代表的なものに、「\$\$\$」や「FOR FREE」(無料)があります。
- ・メールの信頼性 - AOL アカウントを偽装した電子メールでも、アプリケーションヘッダーを検査すると、AOL 電子メール クライアント ヘッダーが含まれていないことがわかります。
- ・日付の妥当性検査 - 送信日を先の日付に変更する方法は、スパムメール送信者が頻繁に使う手段です。電子メールプログラムの多くは、受信日をもとに電子メールを分類するようにデフォルト設定されています。そのため、この方法を使って、電子メールを常に受信ボックスの最上部に表示できます。
- ・ルーティング情報 - メールホストが「差出人」の電子メールアドレスを変更できる場合もありますが、受信メールのヘッダー情報は、宛先に届く前に通過するリレーポイントで作成されます。このエントリは電子メールの送信後に書き込まれるため、メールの履歴を偽造することは不可能です。この情報を利用して、電子メールの出所が RBL(リアル タイム ブラック リスト)に登録された送信元かどうかを確認できます。

ボディルール

電子メールのボディは、ユーザがメールクライアントで電子メールを開いた時に表示される内容です。ボディは一般的に、件名と本文で構成されています。

スパムメール送信者は、電子メールにコードを追加してローメッセージの内容を偽装する方法を頻繁に利用します。

たとえば、HTML ベースの電子メールに HTML コードを追加すると、ユーザに対して表示されるテキストを変更せずに、スパムメールスキャナを妨害するためのノイズをコードレベルで発生させることができます。

下の図の電子メールには、つぎの HTML コードが含まれています。

```
<FONT face=Arial size=2>This message is s<U></U>pa<STRONG></STRONG>m</FONT>
```

このメッセージには、フォントを定義し、<U> (下線) と (太字テキスト) の有効・無効を切り替える HTML コードが含まれています。しかし、オプションの切り替えが同時実行されて効果が無効になるため、ユーザには下線のオプションも太字テキストのオプションも表示されません。



この場合、「spam」というキーワードを含む HTML ローメッセージを検査するコンテンツルールを利用して、HTML コードがキーワードをカムフラージュします。SpamAssassin エンジン、受信者のメールクライアントと同様のメッセージ翻訳テクノロジーを備えているため、ユーザに表示された形式のメッセージボディをスキャンできます。

SpamAssassin エンジン、ボディルールを使ったスキャンの実行時に、特殊なテクノロジーを使ってスキャン速度を最適化します。その結果、高度なボディ ルール スキャンを高速実行した上で、高レベルなパスでトリガーされたルールを使った再スキャンを実行できます。

以下は、ボディルールの例です。

- ・ 「Make money fast」 (短期間で金もうけ) などの語句の検出
- ・ 電子メールに含まれるわいせつな言葉のパーセンテージの確認
- ・ ナイジェリア詐欺に関連したさまざまな電子メールの検出

SpamKiller 製品は、特定のキーワードではなく電子メールのパターンをチェックして、既存のテーマに基づいているスパムの新しい亜種を検出することができます。

ロー ボディ ルール

ロー ボディ ルールは、ボディルールとは対照的に、ローフォーマットのままで電子メールを検査します。この方法により、スパムメール作成者がスパムメールのカモフラージュ (隠蔽) のために利用するテクニック (ノイズを追加してコンテンツルールによるキーワードや語句の検出を妨害する方法) を検出します。

ロー ボディ ルールは、追加データの中の真のメッセージを隠蔽しようとするため、正規のメッセージかどうか疑わしいことを示すフラグを検出します。

隠蔽には、以下を含むさまざまなテクニックが使われます。

- ・ HTML – ボディルールの例のように、HTML コードを語中に追加します。
- ・ テキストの符号化 – SMTP メールを使った送信が可能なフォーマットに添付ファイルを変換する、Base64 符号化などがあります。テキスト送信には符号化は必要ありませんが、スパムメール送信者が符号化を利用してテキストのフォーマットを変更すると、ローコンテンツルールによる検出ができなくなります。つまり、スパムメールそのものが符号化されることとなります。ユーザが電子メールを開くと、メールクライアントが自動的にテキストを復号化するため、ユーザにはスパムメッセージが表示されます。

SpamAssassin エンジンを利用して、Base64 などの一般的な標準を復号化できます。そのため、ボディルールによる真のスパムコンテンツの検出が可能になります。ただし、ローボディルールも、コンテンツの隠蔽試行という事実をもとに、潜在的なスパムメールとしてメッセージを識別します。

ボディルールとローボディルールの組み合わせにより、単一のテクニックに依存する場合よりも確実にスパムメッセージを検出できます。

- ・ ホワイトテキスト – HTML ベースのスパムメールの中には、背景色と同じ色の正規テキストをメッセージに追加したものもあります。この場合、エンドユーザは正規テキストを見ることができません。これは、迷惑メールの要素よりも正規メールの要素を多くすることにより、ベイズ定理とコンテンツルールによる検出を回避するための手段です。これは一般的な動作ではないため、SpamAssassin エンジンはこれを潜在的スパムとして処理し、迷惑メールとしての識別に重点を置きます。

フルボディルール

符号化されていない電子メールメッセージを1つの単位として見なします。この方法は、既知のスパム属性を検査するもので、従来のウイルス対策製品によく似ています。一般的には、ハッシュテクニック (DCC や Pysor が作成したものなど) を使って、メッセージのハッシュチェックサムをもとに既知のスパムメールのデータベースを構築します。

URI ルール

URI ルールは、ハイパーリンクや URL (Universal Resource Locator) などの、メッセージボディに埋め込まれた URI (Universal Resource Identifier) を検出する特殊なボディルールです。SpamAssassin は、URI を検出するために、以下の要素を探します。

- ・ スパムメール送信者が悪用する機能 (ウェブページのオープンや、不正な許可の付与など)。
- ・ メッセージがスパムメールであることを示唆する、埋め込み URI に含まれるキーワードと語句。たとえば、URI に含まれる「sex」や「teen」などのキーワード (画像やウェブサイトへのリンクの可能性のあるもの) を検出します。
- ・ ホストネームではなく、IP アドレスを含む URL。IP アドレスの使用は、電子メールで宣伝するウェブサイトの名前を隠すための一般的なテクニックです。
- ・ プレーンテキストのメッセージも、URI をサポートしません。しかし、メールクライアントによっては (Outlook など)、フォーマットをもとに、メッセージ内のテキストを URI として解釈するものもあります。たとえば、「http://www.nai.com」というテキストを含むプレーンテキストのメールを受信すると、多くのメールクライアントはこれをハイパーリンクとして動的に処理します。そのため、プレーンテキストのメールがハイパーリンクではないにもかかわらず、これをクリックするとウェブブラウザが起動して URL が表示されます。右の例を参照してください。



以上の例の多くは、正規の電子メールにも含まれる可能性があります。そのため、SpamAssassin テクノロジーは、単一のルールに依存してスパムメッセージを識別するのではなく、メッセージを累積的に評価します。

メタルール

複数のルールの組み合わせがトリガーされた場合、それぞれのルールのスコアを加算して評価した場合よりも、メッセージが実際にスパムメールである可能性は高くなります。

メタルールを利用して、論理演算のルールの組み合わせをもとに、特定のスコアを定義できます (たとえば、ルールの番号が 12 と 17 の場合はスパムメールの可能性が非常に高いため、当該メッセージの全体的なスコアにポイントを加算します)。メタルールは、正と負のスパムスコアルールを含む組み合わせを検出します。

4.3 スコアによりメッセージをスパムメールと判断した場合の処理

SpamKiller は、スコアが 5 以上のメッセージを迷惑メールと判断するようにデフォルト設定されています。

すべての SpamKiller 製品(メールサーバとゲートウェイ)のフィルタリングオプションは共通ですが、その実装方法は製品のインストール環境によってわずかに異なります。

メールサーバとゲートウェイに共通のフィルタリングオプション

・ 件名の接頭語を追加

件名にテキスト(デフォルト設定は「Spam」)を追加する機能です。この機能は、メールサーバまたはメールクライアントを使って潜在的なスパムメールを管理する場合に特に便利です。

1. 管理者またはエンドユーザは、メールの件名に共通の接頭語を追加して、指定された中央またはローカルユーザのフォルダかデータベースに潜在的なスパムメールを振り分けるメールルールを作成できます。その結果、スパムメールの疑いのあるメッセージがユーザの受信ボックスにたまることを防ぐと同時に、メッセージの内容を検証する機会を提供できます。
2. ほとんどのメールサーバまたはメールクライアントのメール処理ルールを利用して、ユーザがメッセージにアクセスして内容を確認した後に、スパムの疑いのあるメールの削除を管理できます。一般的なスパム管理として、メッセージを数日間保存(ユーザの受信箱以外の場所に保存)した後に削除する方法が挙げられます。たとえば、メッセージの古さと件名タグを調べるメールルールを設定して、定義した保存期間を過ぎたスパムメールを削除することができます。

・ メッセージにスパムスコアを追加

SpamKiller for Exchange SMB 製品では、このオプションを「Spam Level header」(スパム レベル ヘッダー)と呼んでいます。このオプションは、メッセージに割り当てられたスパムスコアを識別します。前述のとおり、メールサーバまたはクライアントのルールを利用して、スコアに応じてスパムメッセージを個別のフォルダやデータベースに振り分けることができます。

・ トリガーされたスパムルールのリストを電子メールの X ヘッダーに追加

SpamKiller for Exchange SMB 製品では、このオプションを「Spam Report」(スパムレポート)と呼んでいます。このオプションは、スパムメッセージを検出したルールのリストを提供します。この機能を利用してそれぞれのメッセージがトリガーしたルールを確認できるため、各環境でのスパム検出の最適化に不可欠なオプションです。

SpamKiller for WebShield Appliance 独自のオプション

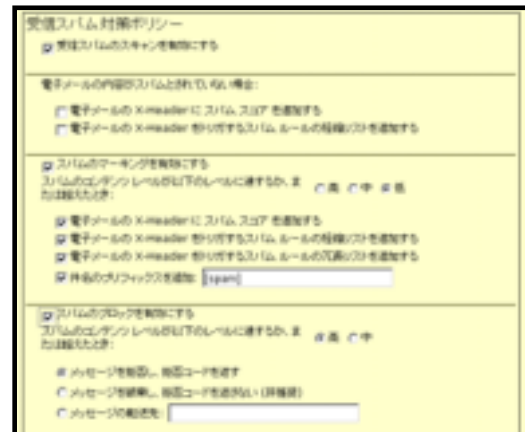
右の図のゲートウェイソリューション(WebShield Appliance のプラグインコンポーネント)は、2段階のアプローチにもとづくインバウンドとアウトバウンドのスパムフィルタリング機能を提供します。

- (1) 前述の共通オプションを利用して、メッセージをスパムメールとしてマークします。
- (2) メッセージをブロックまたは転送します。スパムスキャンをゲートウェイで実行し、スパムメッセージのネットワーク侵入を防ぐことにより、ネットワーク帯域幅を節約できます。

下の表に示したように、SpamAssassin エンジンのスコアに対応した高、中、低の3段階評価により、コントロールを簡素化できます。

評価	スコア
低	5 – 9.99
中	10 – 14.99
高	15 +

デフォルト設定では、スコア範囲を GUI で変更することはできません。ただし管理者は、必要に応じてスコアを変更できます。そのためには、WebShield XML システム設定ファイルの値を変更します。詳細については、テクニカルサポートに問い合わせてください。



SpamKiller for WebShield Appliance を使ったスパムのルーティング

以下は、SpamKiller for WebShield Appliance のルーティング設定の例です。

- (1) 迷惑メールと正規メールの判別がつきにくい(スパム評価が低い)メッセージは、ユーザに送信し、最終的な検査をユーザに任せます。

電子メールをスパムメールとしてマークすることにより、ユーザはこのメールをとりあえず無視し、正規メールの処理に専念できます。前述のように、メール クライアント ルールを利用して、スパムとマークされたメッセージを他のローカル メール フォルダまたはデータベースに移動できます。

必要なメッセージが届かない場合は、ユーザがスパムメールの疑いのあるメッセージを検査します(スパムフィルタリングによって必要なメッセージが誤って除去されていないことを確認します)。

時間的な余裕があれば、潜在的なスパムメールとしてマークされたすべてのメッセージを調べることもできます。

- (2) メッセージが確かにスパムメールである場合(スパム評価が中または高の場合)は、メッセージを拒否するか、定義されたロケーションに転送します。

SpamKiller for Exchange Small Business 独自のオプション

ゲートウェイソリューションと同様に、2つのフィルタリングレベルがあります。

ただし、SpamKiller 製品はメールシステムの内部で直接動作するため、メールサーバ環境でメールをフォルダまたはデータベースに転送する許可を利用できます。

つまり、中央のフォルダまたはデータベースか、指定されたジャンクメールフォルダ(SpamKiller 製品が各ユーザの受信ボックスに作成

するもの)に電子メールをルーティングできます。スパムメールとして最初にフィルタリングされたメッセージは、特定のユーザのジャンクメールフォルダにルーティングされます。



SpamKiller Small Business Edition for Exchange 2000 製品(右の図)には、全ユーザの受信ボックスまたは特定のアクティブ ディレクトリ グループの着信スパムメールをスキャンおよびフィルタするオプションがあります。このグループは、製品のインストール時に作成されます。

ルーティングは、SpamAssassin エンジンが割り当てるスコアをもとに決定します。このスコアは、アクション設定インターフェース(右の図)を利用してカスタマイズできます。

SpamKiller for Microsoft Exchange Small Business を使ったスパムルーティング

以下は、SpamKiller for Exchange 2000 Small Business のルーティング設定の例です。

- (1) メッセージのスコアが5以上の場合、正規メールと迷惑メールの判別が難しいため、メッセージをフィルタしてユーザのジャンク メール フォルダに転送します。その結果、ユーザの受信箱には重要なメールのみが送信されます。ユーザは、必要に応じてジャンク メール フォルダを調べ、メッセージがスパムメールであることを確認できます。
- (2) メッセージのスコアが 15 以上の場合、スパムメールと断定します。デフォルト設定では、中央のシステムフォルダにスパムメールがルーティングされます。管理者は、ユーザがメールの内容確認を希望する場合に備えて、何日でもメッセージを保存できます。

4.4 ルールとスコアの編集

すべての SpamKiller 製品のルールは、一般ユーザが最適なスパム検出を利用できるよう事前設定されています。ただし、個人の要件に合わせてルールセットをカスタマイズできます。

ルールをカスタマイズする理由には、つぎのがあります。

- (1) メインルールセットに含まれていない、スパムメールとして処理する必要のある特定のメッセージを検出して、見逃しを防止します。
- (2) 通常はスパムメールとして処理するメッセージをそのまま通過させ、誤検出を防止します。たとえば、製薬会社では、「Viagra」(パイアグラ)という言葉を含むメッセージの送受信が必要となる場合とあります。

SpamKiller 製品で SpamAssassin ルールセットを設定する場合、遺伝的アルゴリズムにもとづくスコアがあらかじめルールに割り当てられていることに注意する必要があります。スコアの変更やルールの無効化を行うと、ほかのすべてのルールが連鎖反応的な影響を受けます。

SpamKiller によるスパムメール検出を変更する場合は、最初にブラックリストとホワイトリストのオプションを利用します。このオプションを利用すると、ルールセットを変更せずに、メッセージを暗黙的にブロックまたは通過させることができます。リストに追加できるエントリの種類は、使用する SpamKiller ソリューションが定義します。

たとえば、SpamKiller for Exchange 2000 SMB ソリューションでは、電子メールの SMTP アドレスをもとに、ブラックリストとホワイトリストにエントリを追加できます。また、ワイルドカードをサポートするため、メールアドレス全体のブロックも可能です。

このソリューションは Exchange 環境で動作するため、個人のブラックリストとホワイトリストを各ユーザの電子メールアカウントにリンクさせることもできます。デフォルト設定では、このオプションを使って、ユーザの連絡先リストをホワイトリストに追加できます。

SpamKiller for WebShield Appliance をゲートウェイで使用すると、ブラックリストとホワイトリストの用途が拡張されます。その結果、Exchange SMB ソリューションがメッセージオブジェクトのみを検査するのに対し、WebShield Appliance による SMTP トラフィックの検査が可能になります。

この場合、電子メールアドレスやドメイン、ネットワークのアドレス、範囲を、ブラックリストとホワイトリストを使ってサポートすることができます。

さらに細かいカスタマイズが必要な場合は、すべての SpamKiller 製品で既存のルールを有効化または無効化する機能を利用できます。ただし、スコアの変更はできません。

これは、ひとつのルールを変更すると、ほかのルールが連鎖反応的な影響を受けるためです。遺伝的アルゴリズムは、ルールの相互作用をもとに、それぞれのルールのスコアを最適化します。

ルールの変更が不可欠な場合は、つぎの方法を推奨します。

1. SpamKiller オプションを使って、スコアと、すべてのメールメッセージがトリガーしたルールのリストを表示します。この方法で、メッセージがトリガーしたルールと、メッセージに割り当てられたスコアを確認できます。

右の例には、SpamKiller 2.7 for WebShield Appliance でスキャンした電子メールの X ヘッダー、スコア、トリガーされたルールが表示



されています。

2. スпамメールを正確に検出していないルールを探します。たとえば、名物のチキンパイのレシピを含むおばあさんからの電子メールがスパムメールとして検出された場合を想定します。材料リストに「chicken breast」(鶏の胸肉)が含まれているため、「breast」(胸)という言葉によってコンテンツフィルタがトリガーされます。これを防ぐためには、このルールを無効化します。

注: スпамルールのリストを更新する場合、無効化したルールは無効化されたままの状態です。

SpamAssassin テクノロジーを利用して、ルールをさらに細かくカスタマイズできます。たとえば、新規ルールの作成や新規ルールのスコア変更などが可能です。

既存ルールのバランスを維持しながらルールをカスタマイズするためには、ルールセットを完全に理解する必要があります。そのため、SpamKiller 製品のユーザインターフェースでルール変更機能にアクセスすることはできません。

ルールセットは Perl スクリプトで記述されており、経験豊富なエキスパートによるマニュアル編集が必要です。ルールの作成や編集が必要な場合は、ネットワークアソシエイツ社 Expert Services 部門のコンサルティングチームが必要な専門技術を提供しています。

4.5 SpamKiller のアップデート

すべての SpamKiller ソリューションには、FTP アップデートサイトを利用してルールセットとスパム スキャン エンジンを更新する機能があります。

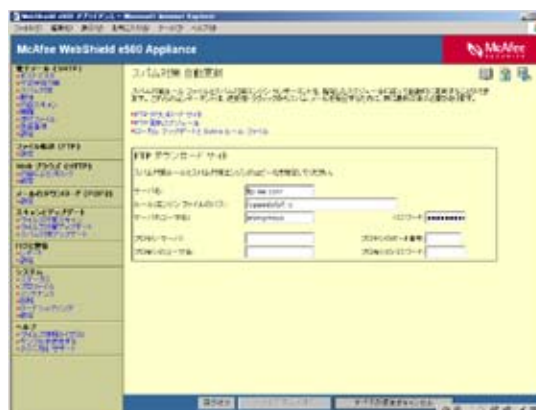
効果的なスパム検出のためには、アップデートが不可欠です。

現在のところ、アップデートは数ヶ月に1回で十分ですが、この頻度はスパム作成者の技術の変化に応じて変わる可能性があります。

SpamKiller 製品のアップデートテクノロジーに含まれるスケジューラは、1日1回新規アップデートを確認するようデフォルト設定されています。この機能により、常に最新のプロテクションを配備できます。

アップデートを実行すると、SPAMUPD.INI ファイルをプルダウンし、FTP サイトで利用可能なスパムルールとスキャンエンジンのバージョンを調べます。その後、必要に応じて最新のルールとスキャンエンジンをダウンロードし、適用します。最近のルールとエンジンのアップデートのサイズは、300KB 未満です。

SpamKiller 製品では、作成したカスタムルールがアップデート実行中に上書きされるのを防ぐために、作成したルールの保存のエキストラ ルール ファイルを使用します。





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

製品、サービスに関するお問い合わせは下記へ