

# Proofpoint Spam Detection モジュール



Proofpoint Messaging Security Gateway™と Proofpoint Protection Server®のコンポーネントである Proofpoint Spam Detection モジュールは、スパムの検出と除去に対する最強の手法を提供します。その無類の精度を誇る鍵を握っているものが特許出願中の Proofpoint MLX™マシンラーニングテクノロジーであり、これは Proofpoint Attack Response Center の科学者や技術者が開発したシステムです。Proofpoint はもっとも効果的な従来のスパムフィルタリング方法を画期的なマシンラーニングテクノロジーと組み合わせて、業界で最高の検知率ともっとも低い偽陽性率を誇るシステムを提供します。

## 特徴

### 最大の検知率を実現する多層式スパム防止

Proofpoint Spam Detection は、もっとも効果的な複数のスパム除去テクノロジーを管理が簡単な単一の統合型システムに組み込むことにより、スパムに対して強固でありながら管理がシンプルな対策を実現します。Proofpoint の多層式スパム防御では、コネクション分析、ローカルおよびグローバルな評価、そして先進的なコンテンツ分析の統計的手法を組み合わせています。Proofpoint Spam Detection は着信電子メールメッセージにおける何十万もの属性、すなわち、差出人 IP アドレス、メッセージエンベロープヘッダー、構造、画像属性、差出人評価データ、そしてメッセージ本文の非構造的コンテンツなどを検査して、非常に高い信頼度でスパムを正確に分類します。

Proofpoint Spam Detection は、スパム攻撃によって引き起こされたトラフィック・スパイクを除去し、かつエンドユーザのメールボックスにスパムが入り込まないようにするために、多層全体にわたって対策を実現しています。

#### ○ コネクションレベルの分析

Proofpoint Email Firewall™は、DNS、MX レコード確認、SPF、宛先確認、Proofpoint Dynamic Reputation 情報、および任意の netMLX データなど、数多くのコネクションレベルデータポイントを評価することにより、スパムや悪意のあるコネクションからステータフルな最前線の防御を行います。Proofpoint Dynamic Reputation テクノロジーは IP アドレスレベルでの SMTP コネクションをたえず監視し、疑わしい活動や悪意のある活動を探索します。このような分析に基づき、SMTP 率制御を用いて悪意のあるコネクションを自動的に拒否または抑制して、インバウンドコネクション負荷の 30% から 80% 以上を削減しながら、ディレクトリ獲得攻撃やサービス拒絶攻撃に対して抜群の対策を実現します。

#### ○ コンテキスト上、語彙上、そして画像ベースの分析

Proofpoint MLX テクノロジーは、構造試験、英語および外国語検査、ポルノグラフィ検出、悪意のある（スパイウェア／フィッシング／ファームウェア）URL 検出、フィッシング攻撃を検出するための目標規則、画像分析、評価分析、そしてユーザが定義したカスタムポリシーを用いて、メッセージのコンテンツとコンテキストを検査します。Proofpoint のマシンラーニングテクノロジーは多くの言語にわたってスパムの認識とフィルタリングを行うのに最高に適しています。Proofpoint MLX は 2 バイト言語にも完全対応し、検出困難な日本語をはじめとするアジア系言語のスパムに対してさえ卓越した対策を実現します。Proofpoint MLX に含まれる独自の画像分析テクニックでは、他のソリューションが捕捉できない画像ベースのスパムを識別します。

#### ○ エンドユーザによるコンフィギュレーション

有効な差出人と無効な差出人を区別するために個人のセーフおよび受信拒否リストをチェックします。

#### ○ 管理者によるカスタマイズ

グローバルセーフおよび受信拒否リストとカスタム式に作成したスパムルールをチェックします。グローバルリストはエンドユーザリストに優先します。

着信電子メール内で検出されたすべての属性は、メッセージがスパムである確率を表すスパムスコアを最終的に割り当てるために MLX Engine によって使用されます。進化するスパム戦術に先を越されないよう、MLX Engine は Proofpoint Dynamic Update Service™によってたえず自動的に最新の状態に維持されます。



## メリット

- 未体験の攻撃を正確に予想し、阻止するのを助けるために、スパムテクニックとともに自動的に進化します。
- MLX はベイジアンフィルタなどの単純な統計的テクニックよりもはるかに優れており、スパマーによって簡単に破られるシグネチャやフィンガープリントテクニックに頼っていません。
- 管理に煩わされる必要はありません。
- あらゆるメールにおける構造上、コンテキスト上、評価上の何十万という属性を検査して、スパムを阻止します。
- 個別の検疫や個人的なセーフおよび受信拒否リストにより個人が自分宛の疑わしい電子メールを管理することができます。
- 先進的なフィッシング対策法で scam、詐欺、ID 盗用、悪意のあるコードからエンドユーザを守ります。
- スパムスコアとは別にアダルトコンテンツスコアにより、ポルノグラフィスパムに対するゼロトレランスポリシーを強化することができます。
- 偽陽性の発生数を最小限に抑え、長期間にわたって効果的です。
- ポリシーはグローバルレベル、グループレベル、ユーザレベルでカスタマイズことができ、LDAP または Active Directory への完全な統合が可能です。
- 「hush-busting」やランダム化されたスパム攻撃から組織を守ります。
- 信頼性のあるスパムスコアリングにより、スパムに対して決定的な処置を講じることができます。
- カスタムポリシーを簡単に構成できます。

# Proofpoint Spam Detection モジュール

## MLX テクノロジー

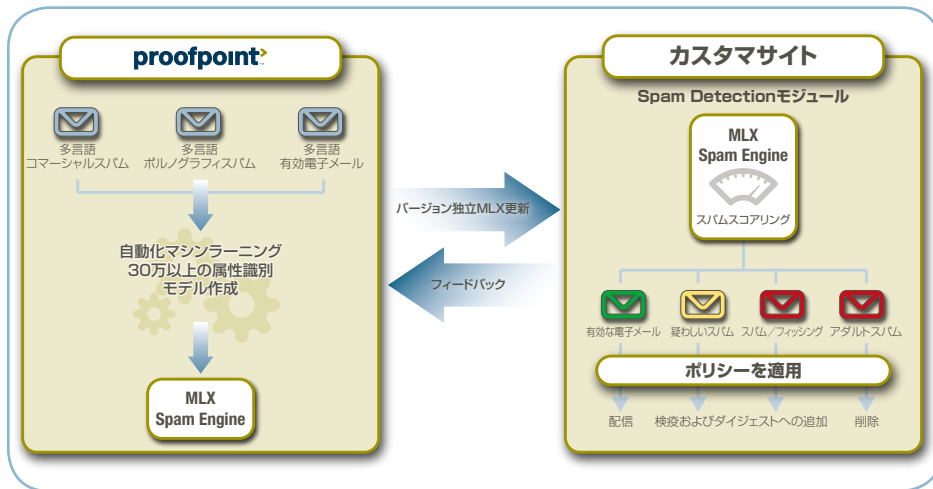
### Proofpoint MLX はスパマーに打ち勝つ上で完全な自信を与えてくれます。

Proofpoint MLX テクノロジーは競合するスパム対策ソリューションの能力をはるかに超えています。MLX はベイジアンフィルタなどの単純な統計的手法よりもはるかに優れており、スパマーによって簡単に破られるシグネチャやフィンガープリントテクニックに頼っていません。MLX はロジスティック回帰や情報獲得分析などの先進的マシンラーニングテクノロジーにより従来のテクニックを強化しています。その結果として業界で最高のスパム検出率を達成しています。

### MLX のスパム検出方法

- プロセスは Proofpoint Attack Response Center から始まります。ここでは Proofpoint の科学者や技術者によって開発されたツールが何百万ものスパムメッセージを分析し、それから何十万ものスパム属性を抽出し、現在および将来のスパムについて基礎となる特性や新興技術を明らかにします。
- これらの属性はロジスティック回帰や情報獲得分析などの高度なマシンラーニングアルゴリズムに投入されます。投入された属性は、最終的なメッセージ分類プロセス中に特定の属性がどれだけ重要かをシステムが理解できるように、動的にバランスがとられます。
- この情報は次に Proofpoint MLX Engine の形でパッケージ化され、自動的に Proofpoint ユーザーに届けられます。
- ローカル面では、Spam Detection モジュールは複数の構造層やコンテンツ層を調べ、各着信電子メールから属性を抽出します。次に、先進的マシンラーニングアルゴリズムは最終的なスパムスコアを計算し、これによってどんな処置をとるかが決まります。
- Proofpoint の Attack Response Center は新たな攻撃や導入済 Proofpoint システムからのフィードバックに基づいて MLX Engine を継続的にトレーニングし、最大限の精度が達成されるようたえず再微調整を行います。

Proofpoint MLX テクノロジーは、Proofpoint の netMLX グローバルレピュテーションデータベースを備えた先進的コネクションマネージメント機能で強化することも可能です。詳細については、<http://www.proofpoint.com/downloads/DS-Proofpoint-Dynamic-Reputation.pdf> を参照してください。



MLX 検出プロセスは Proofpoint Attach Response Center から始まります。ここでは科学者や技術者がインターネットスパムを代表する数学モデルの構築および精製に携わっています。これらのモデルは頻りにユーザーに届けられ、たえず更新されて、ユーザーが最新のスパム攻撃に負けないようにしています。Proofpoint は着信メッセージのあらゆる面、すなわち、差出人の IP アドレスからメッセージエンベロープ、ヘッダ、構造までを調べ、最終的にメッセージ自体のコンテンツとフォーマットを調べます。全部で、20 の分析層と何十万の属性（コンテンツと構造コンポーネントの両方を表している）が分析されます。典型的なメッセージで 300 を超える MLX 属性が起動することがあります。

### エンタープライズスパム検出

大規模エンタープライズのお客様の独自のニーズを対象にしているのは、Proofpoint の Spam Detection モジュールだけです。再度目的が与えられるホストソリューションやカスタムソリューション、あるいは管理が難しいクライアントサイドのソフトウェア導入と違って、Proofpoint のソリューションは次のような特徴をもっています。

- ゲートウェイでスパムを除去します。
- 自由度が高く、企業特性や業界用語に適応性があります。
- エンタープライズのメッセージング戦略およびスケールアップの要件を満足します。
- 組織内のさまざまな電子メールユーザの独自のニーズに応えるために、グローバルスパムポリシー、グループスパムポリシー、個別スパムポリシーを簡単に管理し、実施することができます。
- 非常に低い偽陽性率を確保し、幅広いエンドユーザーコントロールによりミッションクリティカルなビジネスコミュニケーションがつねに利用可能できるようにします。
- 継続的かつ自動的に更新され、画像ベースや外国語のスパムなど、もっとも検出しがたい最新形のスパムに対してさえ最大限の対策を実現します。

### 抜群のエンドユーザーコントロール

Proofpoint は、以下の特徴を通じて、個人的なスパム対策上の好みに対する簡単な「セルフサービス」コントロールをエンドユーザーに提供します。

- 個別の検疫と検疫ダイジェストレポート
- 個別のセーフおよび受信拒否リスト
- ウェブベースの検疫とプロファイル管理
- さまざまなスパムポリシーのオプトインおよびオプトアウト（管理者が構成可能な設定により許可する）を行うことができます。

### Proofpoint MLX について更に詳しく知りたい方のために

Proofpoint の特許出願中マシンラーニングテクニックがスパムに対して抜群の対策をどのように実現するかについての詳しい情報は、以下のサイトから Proofpoint MLX に関する無料ホワイトペーパーをダウンロードしてください。

<http://www.proofpoint.com/mlxwp>

©2007 Proofpoint, Inc. Proofpoint Protection Server は米国およびその他の国々における Proofpoint, Inc. の登録商標です。Proofpoint, Proofpoint MLX, MLX Engine, Proofpoint Messaging Security Gateway, Proofpoint Spam Detection, Proofpoint Email Firewall, MLX Anti-Spam Engine, MLX Dynamic Reputation, Proofpoint Dynamic Update Service は米国およびその他の国々における Proofpoint, Inc. の商標です。ここに含まれる他のすべての商標はそれぞれの所有者の所有物です。05/07