

次世代レピュテーションテクノロジー



Proofpoint Dynamic
Reputation and netMLX >

ほとんどの組織にとって、インバウンドメッセージ量（主にスパム電子メールからなる）は2006年を通して劇的に増加し、この傾向は2007年も続いています。電子メール量のこのような継続的増加は組織にとって新たな課題になっています。どのようにすれば組織はこのように増大したメッセージ量をもっとも効果的に管理し、大きな出費をすることなく巨大なスパムの嵐による影響を減少させることができるでしょうか？

レピュテーションサービスはコネクションレベルで大量のメールトラフィックを削減できるので、あらゆる電子メールセキュリティソリューションの当然のコンポーネントになっています。

良い電子メールセキュリティソリューションであれば99%以上のスパム検知率と、コネクションレベルで80%のボリューム削減を達成できることが望めます。このレベルのスパム精度は強力なスパム対策テクノロジーによって達成でき、一方、このレベルの削減率は信頼できるレピュテーションサービスによって達成が可能です。

目次

課題	1
コネクションマネジメントによる回線容量利用の改善	1
レピュテーションサービス	3
正しいレピュテーション	4
全体像	7
その他の情報	8
Proofpoint, Inc. について	8

課題

ほとんどの組織にとって、インバウンドメッセージ量（主にスパム電子メールからなる）は 2006 年を通して劇的に増加し、この傾向は 2007 年も続いています。電子メール量のこのような継続的増加は組織にとって新たな課題になっています。どのようにすれば組織はこのように増大したメッセージ量をもっとも効果的に管理し、大きな出費をすることなく巨大なスパムの嵐による影響を減少させることができるでしょうか？増大するスパム量と闘う上で、エンタープライズには 3 つの選択肢があります。

コンピューティング・キャパシティの向上

スパムが増加するにつれて、コンピューティング・キャパシティを追加することは効果的な 1 つの選択肢です。より多くのサーバをスパムフィルタクラスタに追加すれば、組織はパワーを高めることができます。たとえば、スパム量が 2 倍になっても、1 つか 2 つのサーバを追加することで容量を簡単に 2 倍にできます。これよりも的確で強力なソリューションは、仮想化を通じて更にキャパシティの追加をする方法です。より多くの仮想サーバをスパムフィルタクラスタに追加すれば、容量を劇的に増加することができます。これは「ダイナミックキャパシティプランニング」と呼ばれています。その重要な付加的利点は、これによって組織がスパムの嵐の場合のような、スパム量の膨大な増加に経済的に対処できるという点にあります。

帯域幅利用の改善

メールボリュームの増加を適切に処理する上での 2 番目のソリューションは、回線容量利用を改善することです。これには 2 つの方法があります。一つの方法はネットワーク上、つまり自社ネットワーク外でスパムフィルタリングを行うことです。このアプローチの欠点は、組織の IT 部門が電子メールに対するあらゆる種類のコントロールを失ってしまうという点にあります。もう一つの方法はコネクションマネジメントソリューションを活用することです。コネクションマネジメントは電子メールインフラのコントロールを維持しながら、同じ結果、すなわち、回線容量利用の改善を達成する方法です。この方法については次の節で詳細に説明しますが、電子メールレピュテーションサービスが注目のソリューションになった理由はこの方法にあります。

コンビネーションアプローチ

現在と将来にわたってあらゆる種類のスパム量増加に対処できる究極的に拡張性のあるソリューションは、上記の拡張性についての両方の方法を組み合わせたものです。これによって、スパム量の膨大な増加に対してエンタープライズのインフラを拡張するための経済的なロードマップがエンタープライズにもたらされます。この方法はエンタープライズの拡張性に対する「ベストプラクティス」として進化してきました。Proofpoint は組み合わせアプローチを採用し、カスタマにはすべてのオプションを提供しています。

コネクションマネジメントによる帯域幅利用の改善

コネクションマネジメントはスパム量を管理するための効果的な技法です。コネクションマネジメントとは、コネクションレベルで着信電子メールメッセージに対してシステムが決定を下すことができる技法群のことを指します。

まず、コネクションの意味について説明しましょう。SMTP プロトコルを介して送信された電子メールは、エンベロープ、ヘッダー、メッセージの本文という 3 つの構成要素からなります。電子メールが送信されると、送信元 SMTP サーバはエンベロープ、ヘッダー、本文の送信を開始する前に、受信サーバへのコネクションを開通します。コネクションフェーズの間、交換される唯一の情報は送信元サーバの IP アドレス（その他のセットアップ情報と共に）です。受信サーバが送信元 IP アドレスを受信確認すると、コネクションが確立され、送信元サーバは実際の電子メールメッセージを送信することができます。2 つ以上のメッセージを単一のコネクションで送信することができるという点に留意してください。たとえば、連続して 5 つのメッセージを送信することになるコネクションを確立することもできます。

コネクションを説明するのに役立つかもしれない比喩を以下に述べます。オークランド港に入港する 2 隻の大型貨物船を考えてください。最初の船の原産地は北朝鮮です。2 番目の船の原産地は英国です。各貨物船は商品が詰まった多くのコンテナを積んでいます。この船をコネクションと考え、コンテナを電子メールメッセージと考えてください。さて、オークランドの税関職員は北朝鮮からの最初の船を迎えます。税関職員は原産地を見ます。北朝鮮となっています。税関職員は、その原産地は米国の「禁止」リストに記載されているので、米国への入港を拒否します。税関職員は禁制品や不法品がないか各コンテナを調査・探索することで貴重なリソースを浪費したりはしません。税関職員は次に 2 番目の船を迎えます。原産地を見て、税関職員は米国の通商相手である英国だとわかります。次に税関職員は各コンテナの内容物を調査し、その中に悪意のある商品が含まれていないことを確認します。

この例はコネクションマネージメントのパワーを説明しています。最初のケースでは、税関のリソースの使用をできるだけ少なくして北朝鮮の船を拒否しました。早く決定を下すために十分な情報がありました。このことはコネクションマネージメントの危険も説明しています。税関職員が自分の決定を下す上で誤った情報を持っていたとしたら、すなわち、中国またはその他の有効な米国の通商相手の船を拒否したとしたら、外交上の危機にいたる可能性があります（極端なケースでは）。要するに、コネクションマネージメントでは、情報の正確さが何に増しても重要だということです。

このアナロジーは電子メールの世界におけるコネクションマネージメントにも応用できます。スパムフィルタが単に差出人情報に基づいてコネクションを拒否できるならば、多くのメッセージを一度に受信拒否できるので、各メッセージと添付ファイルをスキャンするために貴重なサーバリソースを消費する必要がありません。（特にスパマーからのコネクションの場合には、1つのコネクションで複数のメッセージを運ぶことができるということを思い出してください）。拒否の正当性は差出人 IP アドレスのレピュテーションを計算するために使用する情報に依存しています。

レピュテーションサービス

電子メールレピュテーションサービスはある種のコネクションマネージメントツールです。レピュテーションサービスは過去数年の間に出現し、スパム量の増加のために過去 12 ヶ月のうちに特に注目を浴びるようになってきました。

レピュテーションサービスはコネクションレベルで大量のメールトラフィックを削減できるので、電子メールセキュリティソリューションの当然の構成要素となっています。

良い電子メールセキュリティソリューションは 99% 以上のスパム対策の検知率とコネクションレベルにおける 80% の量削減率を達成できることが望まれます。このレベルのスパム精度は強力なスパム対策テクノロジーによって達成でき、一方、このレベルの削減率は信頼できるレピュテーションサービスによって達成が可能です。

レピュテーションサービスはどのように機能するか？

レピュテーションサービスは送信元 IP アドレスを特定し、その IP の「レピュテーション」について決定を下し、そのコネクションに対する処置を講じます。代表的な処置には以下が含まれます。

- **許可**：送信する電子メールメッセージのさらなる処理のための IP アドレス。
- **抑制**：当該 IP からのメッセージ量を減少させるための IP アドレスですが、すべてのメッセージを受信拒否するわけではありません。
- **受信拒否／拒否**：当該 IP アドレスからのすべてのメッセージを受信拒否する IP アドレス。

レピュテーションサービスには次の 3 つの一般的なクラスがあります。すなわち、ローカルサーバレベルで動作するもの、中核的かつグローバルに動作するもの、そして両タイプの組み合わせです。

ローカルレピュテーションサービス

ローカルレピュテーションサービスは、すべての IP アドレス送信元メッセージから所定組織のメールクラスタまでのトラフィックパターンならびに挙動を分析することができます。この種の分析は、強力なコンテンツ分析テクノロジーを原動力とし、非常に微妙で「捕捉できない」ボットネット攻撃でさえ特定することができます。（こういった種類の攻撃は短時間に少ない量のトラフィックだけを送信します。）IP レピュテーションスコアのダイナミックデータベースはローカルに格納されます。着信コネクションが悪意ある IP アドレスから見えた場合は、さらなる処置（たとえば、受信拒否や抑制）を講じることができます。ほとんどのスパム対策ベンダはローカルな挙動分析を活用していません。しかしながら、多くの侵入予防システム (IPS) はこのアプローチを用いていることを留意すべきです。

ローカルレピュテーションサービスの主な強みは、ローカルに観察された IP 挙動に基づいて処置を講じるということですが、これは同時に弱点の源にもなります。ローカルレピュテーションサービスは、ローカルサーバにすでにコネクションされている IP アドレスに対してだけインテリジェントな処置を講じることができます。

グローバルレピュテーションサービス

グローバルレピュテーションサービスはさらに一般的です。IP アドレスの中央データベースが保守され、このデータベースには各 IP アドレスとその対応するレピュテーションスコアがリストされています。レピュテーションスコアは定期的に更新されます（異なるグローバルレピュテーションサービスのリフレッシュレートは大きく変わることがあります）。各 IP アドレスに関する判断はさまざまな特性の分析に基づいています。データはさまざまな方法を通じて中央データベースに入力されます。

グローバルレピュテーションの潜在的な弱点としては以下が挙げられます。

- **不正なレピュテーションデータ**：中央データベースに含まれるレピュテーションデータが不正であれば、着信コネクションに対して誤った処置が講じられることとなります。つまり、有効なコネクションが拒否され、許可されるべきだったメッセージが拒否される結果になる（すなわち、偽陽性）ことがあります。偽陽性のリスクをできるだけ少なくするために、グローバルレピュテーションサービスは各 IP アドレスに対して決定を導いてくれる正確なデータとインテリジェントなアルゴリズムを備える必要があります。「ゴミを入れればゴミしか出てこない」という古い格言は、この状況にぴったり当てはまります。
- **システム管理者による個別対応の必要性**：偽陽性が生じた場合、通常はカスタマが直面しているホワイトリストインタフェースを通じて、この状況を即時是正する方法が必要になります。
- **ボットネットに対する低い感度**：現在のほとんどのレピュテーションサービスは「静的」であり、ボットネットの動的な性質に欺かれることがあります。現在のほとんどのスパムは、スパマーの代わりにスパムを送信する危機にさらされたマシンからなるボットネットから送信されます。単一のスパム活動が何百あるいは何千ものボットネットノード（ゾンビとも呼ばれます）から送信される場合もあります。どういった結果になるかという、単一の IP アドレスがスパム量全体の一部を受け持つだけになります。多くのレピュテーションサービスは、こういった短活動で低量の攻撃を特定する上で十分な迅速さに欠けます。そのため、攻撃が検出されずに通過し、偽陰性（すなわち、悪意のあるコネクションが拒否されるのではなく、許可されてしまう）や検知率の低下を招いてしまいます。

ハイブリッドレピュテーションシステム

ハイブリッドレピュテーションシステムはローカルレピュテーションシステムとグローバルレピュテーションシステムを 1 つのサービスに結合して、より正確な対策を求めるものです。本書であとからさらに説明するように、Proofpoint のレピュテーションソリューションである Proofpoint Dynamic Reputation はこのような能力を提供する上で独自のものです。

正しいレピュテーション

Proofpoint Dynamic Reputation は、ローカルで予測的な挙動データとグローバル的に観察されたレピュテーションの組み合わせを強力なマシンラーニングアルゴリズムで分析したものを使用して、悪意のある IP アドレスからのコネクションを拒否する唯一の電子メールレピュテーションサービスです。このシステムは、スパム、実質的な帯域幅の節約を実現しながら、ディレクトリハーベスト攻撃、DoS 攻撃、その他電子メールが媒介する脅威に対する正確で最前線の防御を Proofpoint カスタマに提供します。

Proofpoint Dynamic Reputation の各能力を十分に語るために、さまざまなレイヤーを以下に説明します。

Proofpoint MLX —スパム対策コンテンツスキャンレイヤー

下の図 1 が示しているのは、着信メッセージを分析し、スパム（着信拒否されるか、または検疫を受ける場合があります）と有効なメール（エンドユーザーに配信されます）に分類する Proofpoint Spam Detection モジュールならびに Proofpoint MLX スパム対策エンジンの全体像です。

MLX は成熟したマシンラーニングベースのテクノロジーであり、あらゆる種類のスパムに対して 99% の検知率を誇ります。MLX はマシンラーニングアルゴリズムを用いてメッセージのコンテンツを分析し、スパムと有効なメールを区別する 30 万を超える属性を調べます。図の右側には、時間の関数としてのコネクション量のグラフがあります。Proofpoint の MLX エンジンによって実際にすべてのスパムが阻止されるとしても、サーバに対する負荷は急上昇します。なぜなら、システムはすべてのコネクションを許可し、すべてのメッセージをスキャンするからです。

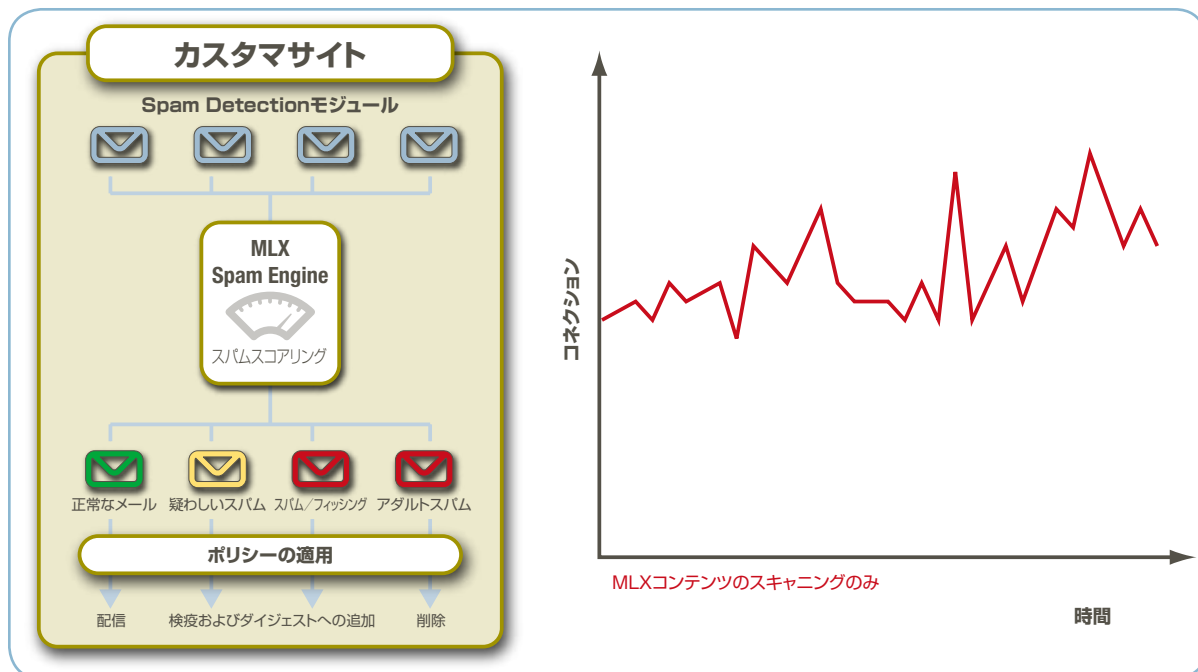


図 1：コネクションマネジメント機能を追加する前でも、Proofpoint MLX スпам検出そのものは 99% を超えて有効ですが、コネクションおよび電子メールメッセージをそのつど処理しなければならないので、コネクション量と処理が「急上昇」します。

Proofpoint Dynamic Reputation — ローカルレピュテーション分析

ローカルレピュテーションサービスはコネクションピークの影響を減少させることができます。このサービスはコネクション量を「平滑」にして、結果として、ダウンストリームのスパム対策コンテンツ分析エンジンに対する負荷を減少させます。Proofpoint Dynamic Reputation には図 2 に示すローカル分析コンポーネントが含まれます。

ほぼ同じ量のスパムが受信拒否されますが、グラフ上の茶色の線によってわかるように、MLX エンジンへの総メッセージ量は減少します（現実世界のアプリケーションでは、約 30-50% の減少となります）。ローカルレピュテーションの採用によって、当社はコアサーバに対する負荷を減少させました。

Proofpoint のローカルレピュテーションコンポーネントは挙動を計算する上で数多くのベクトルを使用しています。

- **Proofpoint Spam Detection で使用されている MLX エンジン**：どの IP アドレスがスパムを送信しているかを特定するために使用され、この結果を Proofpoint Dynamic Reputation エンジンに報告します。
- **Proofpoint Virus Protection で使用されているウィルス対策エンジン**：どの IP アドレスがウィルスを送信しているかを特定するために使用され、この結果を Proofpoint Dynamic Reputation エンジンに報告します。
- **宛先確認エンジン（図には示されていません）**：無効宛先になっている（ディレクトリハーベスト攻撃の主要な指標です）数多くのメッセージを送信している IP アドレスを特定するために使用され、この結果を Proofpoint Dynamic Reputation エンジンに報告します。

次に、これらのベクトルとその他のインテリジェンスベクトルを使用して、着信 IP アドレスごとに動的レピュテーションスコアを計算します。この計算は各 IP アドレスが継続的に分析されるにつれてリアルタイムで行われます。

結果として、ボットネットは迅速に特定され、すぐに受信拒否されます。Proofpoint アプライアンス、仮想アプライアンス、ソフトウェア導入はいずれもローカル IP トラフィックの予測的挙動分析を取り入れています。この分析はリアルタイムで反応し、電子メールトラフィックスパイクを除去し、悪意のあるコネクション（ボットネットからの新しいスパム攻撃など）を受信拒否または抑制します。

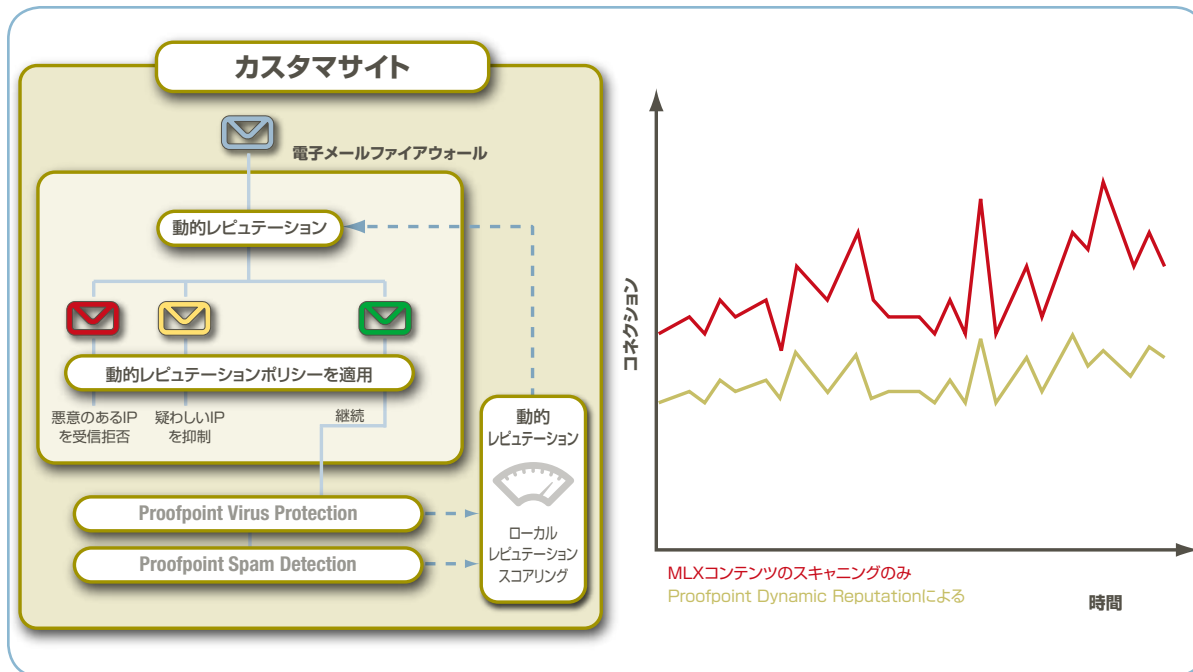


図 2 : Proofpoint の MLX コンテンツスキャンの前に、観察されたローカルコネクション挙動に基づくコネクションマネージメントを行う Proofpoint Dynamic Reputation を追加すると、着信コネクション負荷が 25% を超えて削減され、コネクションスパイクが減少し、トラフィックが「平滑化」され、コンテンツについてスキャンしなければならない電子メールメッセージの数が減ります。

Proofpoint Dynamic Reputation — netMLX グローバルレピュテーション分析

Proofpoint のグローバルレピュテーションコンポーネントである netMLX はトラフィックをさらに削減します。このグローバルレピュテーションコンポーネントを追加することは、大量のインバウンドコネクションを受信するサイトにとって特に有効です。

Proofpoint Dynamic Reputation はローカルな予測的挙動データとグローバル的に観察されたレピュテーション (Proofpoint MLX から配信されます) の組み合わせを用いて、悪意のある IP アドレスからの着信コネクションを受信拒否し、性能、精度、レスポンスタイムの最適バランスを達成します。他のレピュテーションサービスと違って、Proofpoint Dynamic Reputation には次のような特徴があります。

- ローカルなレピュテーションソースとグローバルなレピュテーションソースの両方を用いて、最大量の負荷を削減し、悪意のある新しい IP アドレスに対して非常に迅速に反応します。インバウンドコネクションの 80% 以上をも拒否することができ、誤検知率は 100 万分の 1 未満です。
- 特許出願中のマシンラーニング技法 (netMLX) を使用して、IP 関連の何百もの属性を継続的に分析し、もっとも正確なレピュテーションスコアを出します。
- そういったレピュテーションスコアを分単位で更新し、新しい脅威に対する最速の応答を確保しています。

Proofpoint Dynamic Reputation と netMLX の効果は図 3 に見ることができます。グラフ上の青線は MLX スпам対策エンジンによって処理しなければならないコネクションおよびメッセージの数の劇的な減少を示しています。(現実世界のアプリケーションでは、メッセージ量の 80% 超をこの技法によって削減することができます。) 他のすべてのトラフィックは Proofpoint Dynamic Reputation によってコネクションレベルで着信拒否されてきましたが、これにはローカルレピュテーションデータとグローバルレピュテーションデータの組み合わせが利用されました。数多くのコネクションが着信拒否されると、Proofpoint Spam Detection エンジン (コネクションレベルでの助けがなくても、99% の精度を誇ります) の性能も少し上昇します。

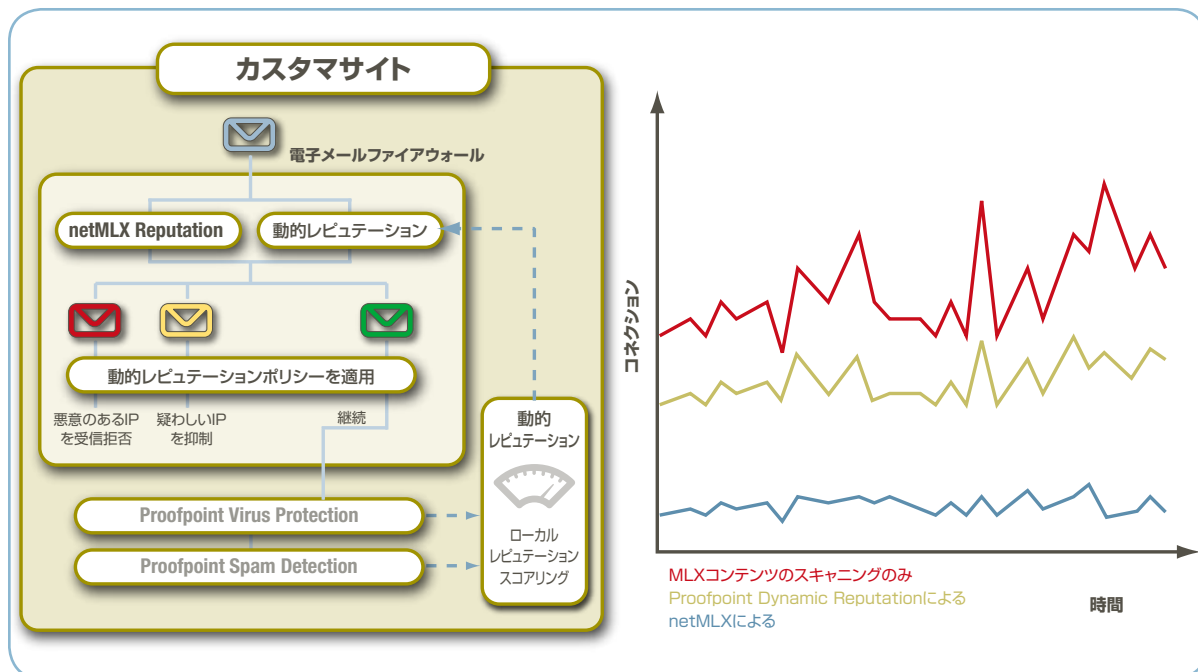


図 3 : ローカルおよびグローバルネットワークベース IP レピュテーション (netMLX) の両方を追加すると、インバウンドコネクション量が 80% も減少し、コネクションスパイクが劇的に平滑化されます。

Proofpoint netMLX はインターネット全体にわたって電子メールを送信する IP アドレスに対するレピュテーションに関する業界でもっとも正確で最新のデータベースを作成し、これによって各カスタマサイトはグローバル差出人挙動に関する Proofpoint のリアルタイムなマシンラーニング分析によって達成されるネットワーク効果から利益を得ることができます。Proofpoint netMLX は悪意のある IP アドレスと有効な IP アドレスに関するグローバルデータを連結し、カスタマサイトにおけるローカル MLX 分析からの測定データと外部ソースからの観察データの両方を処理し、陽性が陰性かを問わず、差出人のレピュテーションを表すスコアを出します。

毎分、すべての IP アドレスのための何百というデータポイントが先進的マシンラーニングアルゴリズムによって構文解析され、非常にタイムリーで正確なネットワークレピュテーションスコアを生成します。多様なレピュテーション関連の属性が分析されますが、その中には以下が含まれます。

- SPF
- 各 IP に関連するスパム、ウィルス、フィッシング、無効宛先の割合
- URL とドメイン受信拒否のリスト
- DHCP アドレス (ゾンビ、ボットネット)
- 画像履歴 (ファジーマッチング)
- 宛先リストサイズ
- その他数百の属性

次に、Proofpoint Dynamic Reputation は、これらのスコアを用いて、ローカルな挙動データと組み合わせ、着信電子メールコネクションの許可、抑制、または拒否についてインテリジェントな決定をします。

Proofpoint Dynamic Reputation は、レピュテーションサービスの 3 つの重要な属性を独自に調和させたレピュテーションサービスをカスタマに提供します。

- **迅速なレスポンスタイム** : ローカル挙動分析を組み合わせた Proofpoint netMLX グローバルマシンラーニング分析によって達成される 1 分というリフレッシュレートはリアルタイムに近い反応を約束します。Proofpoint Dynamic Reputation はボットネットなどの新しいスパムソースに対して、競合する静的レピュテーションソリューションよりも 1 桁速い程度にまで反応します。
- **最高のスパム対策およびコネクションマネージメント精度** : グローバルレベルでレピュテーション関連の何百もの属性を処理する Proofpoint netMLX は、Proofpoint Dynamic Reputation が IP ア

ドレスレピュテーションに関するもっとも広範で正確な査定につねにアクセスできるようにします。

- **性能および効率の向上**：80%を超えるコネクションレベル受信拒否は、カスタマが電子メール量を劇的に減少させたり、追加ハードウェアを導入する必要もなく絶えず増加するスパム量に対応したりするのに役立っています。

レピュテーションシステムをスパム対策ソリューションの中心部分として利用し、結果として、レピュテーションコンポーネントを取り外したときにスパム対策性能の低下に悩む他のベンダとは違って、Proofpoint はレピュテーションから得られるコネクションマネジメント上の利益に焦点を合わせています。Proofpoint MLX テクノロジーに支えられた Proofpoint Spam Detection モジュールは、ローカルレピュテーションコンポーネントを使用するのか、それともグローバルレピュテーションコンポーネントを使用するかにかかわらず、99%以上の検知率を誇ります。Proofpoint Dynamic Reputation の目的は、追加ハードウェアを必要とせずに、コネクションレベルでメッセージ量を減少させ、ダウンストリームメールシステムのスループットを効果的に増加させることです。

全体像

Proofpoint Dynamic Reputation は全体的な Proofpoint Protection Server プラットフォームのコンポーネントとして機能します。レピュテーションサーバは自由にできる利用可能なすべてのデータを使用して、コネクションレベルにおける最高の対策を実施し、それによって悪意のある偽りの大量トラフィックを迅速かつ効率的に除去します。図4は、Proofpoint Dynamic Reputation、netMLX データベース、Proofpoint のスパムおよびウィルス防御モジュールがどのように協同してコネクション量を減少させ、スパム、フィッシング、ウィルス感染メッセージから守るのかを示しています。

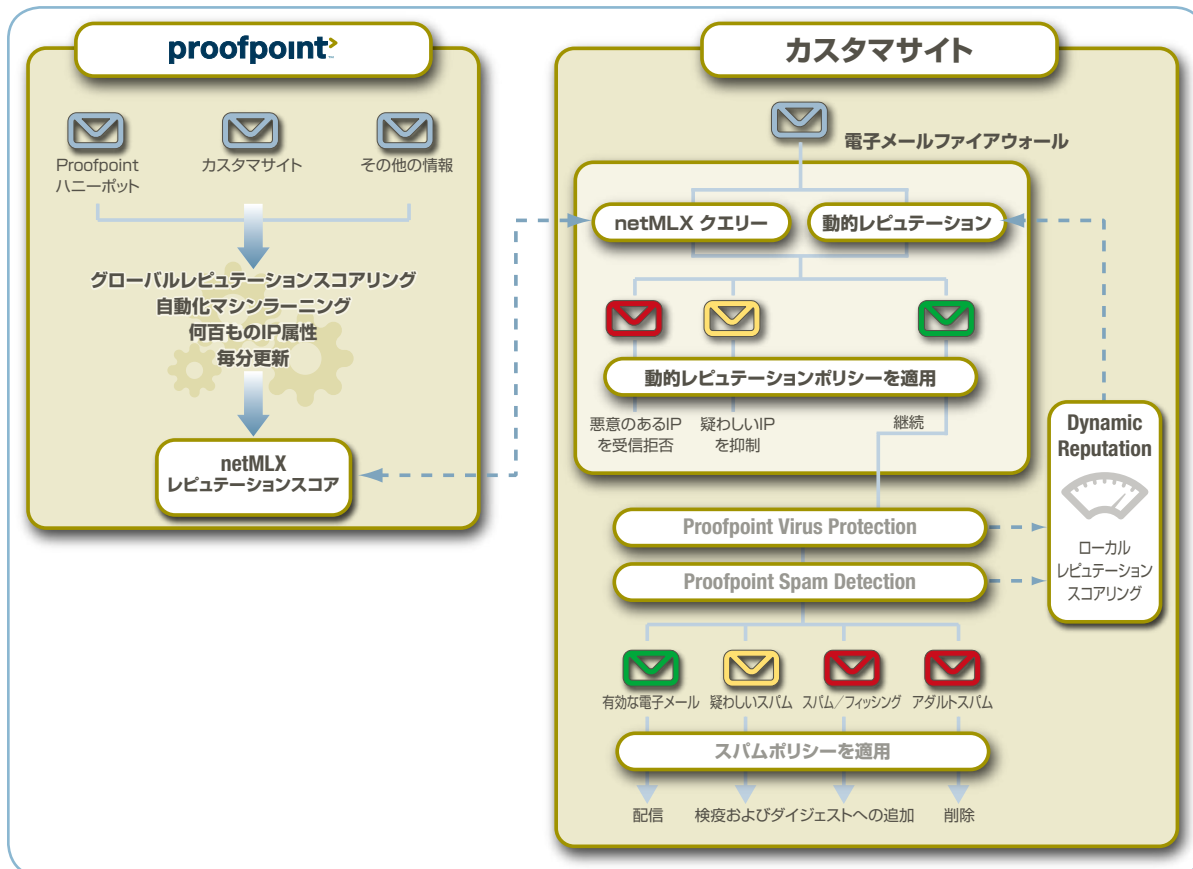


図4: コネクションマネジメントに対する Proofpoint の革新的アプローチでは、ローカル分析とネットワークベース分析を組み合わせています。

ローカル分析とネットワークベース分析の独特な組み合わせは、Proofpoint カスタマがインバウンドコネクション負荷を減少させ、電子メールトラフィックスパイクを防御するのに役立っています。netMLX 検出プロセスは Proofpoint Attack Response Center から始まり、ここでは何百万もの IP アドレス

に関する情報が継続的にコンパイルされ、独自のマシンラーニングシステムを用いて分析されています。レピュテーションスコアは毎分更新されます。

電子メールコネクションがカスタマサイトから受信されると、各 IP アドレスの最新レピュテーションスコアがないか netMLX に照会することができます。このスコアに基づいて、コネクションは受信拒否されるか、抑制されるか、あるいは追加処理のために許可されます。ローカル的には、Proofpoint Dynamic Reputation は許可されたすべてのコネクションの挙動を追跡し、スパム、ウィルス、無効宛先のそれぞれの割合といったような挙動を監視します。このローカル分析に基づいて、コネクションはまた受信拒否されるか、もしくは抑制されることがあります（すべての Proofpoint 導入に含まれている機能）。

許可されたメッセージのコンテンツは、最終的な処理が決定される前に、Proofpoint Virus Protection と Proofpoint Spam Detection を含む他の防御によって続いて処理されます。

その他の情報

Proofpoint Dynamic Reputation、Proofpoint MLX テクノロジー、Proofpoint のメッセージングセキュリティソリューションについて詳しくお知りになりたい場合は、以下のオンラインリソースをご参照ください。

Proofpoint Dynamic Reputation および netMLX データシート

この簡単なデータシートでは、Proofpoint Dynamic Reputation と netMLX の主要な特徴について説明しています。以下のサイトにて、コピーを入手してください。

<http://www.proofpoint.com/downloads/DS-Proofpoint-Dynamic-Reputation.pdf>

Proofpoint MLX テクノロジーホワイトペーパー

Proofpoint のソリューションの原動力であり、もっとも困難な種類のスパム（ボットネット配信の画像ベーススパムを含む）に対してさえ 99% を超える検知率を誇るマシンラーニングテクノロジーについて詳細をご確認ください。以下のサイトにて、ご登録後にこの文書のコピーをダウンロードしてください。

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

Proofpoint Virtual Appliance の無料試用版

Proofpoint MLX のパワーをご自分で体験してみてください。Proofpoint Messaging Security Gateway Virtual Edition を 45 日間無料でご利用ください。当社の仮想アプライアンスは VMware の無料仮想化プラットフォーム上に簡単に導入できます。このアプライアンスにはインバウンド電子メール対策モジュールの完全な一式、すなわち、Proofpoint Spam Detection、Proofpoint Virus Protection、Proofpoint Zero-Hour Anti-Virus に加えて、Proofpoint の電子メールファイアウォールと許容使用ポリシー実施機能が含まれます。ご希望の方は Proofpoint 正規販売代理店までお問い合わせください。

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

Proofpoint, Inc. について

Proofpoint は大規模エンタープライズのためにメッセージングセキュリティソリューションを提供して、スパムの阻止、電子メールウィルスの対策、企業ポリシーおよび規定への確実なコンプライアンス、電子メールやその他のメッセージストリームを介しての機密情報ならびに独占情報の漏洩に対する防衛を行います。Proofpoint のフラッグシップ製品である Proofpoint Messaging Security Gateway™ および Proofpoint Protection Server® は、Proofpoint の科学者や技術者が開発した先進的マシンラーニングシステムである Proofpoint MLX™ テクノロジーを用いた将来も安心なメッセージングセキュリティを提供します。

©2007 Proofpoint, Inc. すべての権利は留保されています。Proofpoint、Proofpoint Protection Server、Proofpoint Spam Detection、Proofpoint Virus Protection、Proofpoint Zero-Hour Anti-Virus、Proofpoint Secure Messaging、Proofpoint Network Content Sentry、Proofpoint Messaging Security Gateway、Proofpoint MLX、Proofpoint Content Compliance、Proofpoint Regulatory Compliance、Proofpoint Digital Asset Security は米国およびその他の国々における Proofpoint, Inc. の商標または登録商標です。

この文書はその本来の目的以外に複製または使用してはなりません。

ここに記載された情報は Proofpoint の創出物かつ所有物であり、書面の同意により明示的に授与された権利を除いて、当該情報は全部または一部を問わず開示または流布してはなりません。Proofpoint はすべての特許権、所有権、設計権、使用权、販売権、製造権および生産権を留保します。バージョン 04/07、改訂 A

For More Information

Proofpoint, Inc. US

日本ブルーポイント株式会社

E info@proofpoint.com
www.proofpoint.com

E sales-japan@proofpoint.com
www.proofpoint.co.jp