



IronPortはここがすごい!

日本語スパムメールも正確に検知!

スパム判定の正確性は、スパム対策の最重要項目です。検知率が低ければスパム対策の導入の意味がなくなりませんが、一方で、正規のメールをスパムと判断してしまう誤検知の発生は生産性の大幅な低下を招きます。誤検知を回避しつつ高いレベルの検知率を維持することが求められているのです。IronPort Cシリーズは、革新的なテクノロジーを駆使して、日本語スパムはもちろんの事、世界中に氾濫しているスパムメールを確実に検知します。

▶ E-mailレピュテーション(送信元IPアドレスの格付け)

送信元IPアドレスによるスパム対策としては、ブラックリストの利用が広く普及しています。しかし、ブラックリストでは、「黒」、「それ以外」という情報提供しかされず、リストへの登録基準も運営団体によって異なります。このため、取引先のサーバが突然ブラックリストに登録されて必要なメールの受信ができなくなった、という例が後を絶ちません。

こうした中、ブラックリストの情報を生かしつつ、より正確かつ柔軟な運用を実現する目的で考案されたのがE-Mailレピュテーションです。レピュテーションは、日本語では「評価」と訳されます。各種ブラックリストへの登録の有無のほか、メールの総送信数、所有者の企業情報など、様々なパラメータを元に、メールの送信元IPアドレスの総合的な評価、格付けをおこないます。数多くのパラメータを参照するため、特定のブラックリストのみに登録されたような場合、格付けへの影響は限定的です。また、「黒」と「それ以外」という二者択一ではないため、いわゆるグレーゾーンに対する受信数制限等の対策も可能になります。

このように、E-Mailレピュテーションは非常に有効なサービスですが、その品質の維持に欠かせないのが、格付けの判断材料となる情報の種類とサンプル数です。IronPortが運営するレピュテーションサービス「SenderBase」は世界最大の規模を誇り、2,000万以上のIPアドレスに関して、110を超えるパラメータを常に監視しています。統計の対象となるメールの総量は1日あたり50億通を超え、これは、インターネットを流れるメールの総量の25%以上にあたると言われてしています。

IronPort SenderBase NetWork



巧妙化を続けるスパムメールへの対策は極めて難易度の高い命題です。IronPortでは、これら多数の優れたテクノロジーを駆使し、多角的な分析をおこなうことで、スパムメールの正確な検知を実現しているのです。また、スパム判定されたメールの隔離、件名へのタグ付け、ヘッダの挿入など、検知後に必要な機能も、すべて、完備しています。

▶ Webレピュテーション

多彩な情報を集計、分析するSenderBaseは、E-mailレピュテーションに加えて、もうひとつ、貴重な情報を提供しています。それが、Webレピュテーションです。

ほとんどのスパムメールではURLが本文に記載されています。これは、スパムを送信する目的が、受信者をURLに誘導ことにあるため、フィッシングはその代表例となります。スパムメールに含まれるURLの情報はSenderBaseが収集するパラメータのひとつとなっており、集められた情報はリアルタイムでデータベース化されます。IronPort Cシリーズは、10 - 15分という極めて短い間隔でデータベースの更新をおこない、新手のフィッシングやスパムメールに対しても正確な検知をおこなっています。

▶ チューニング不要

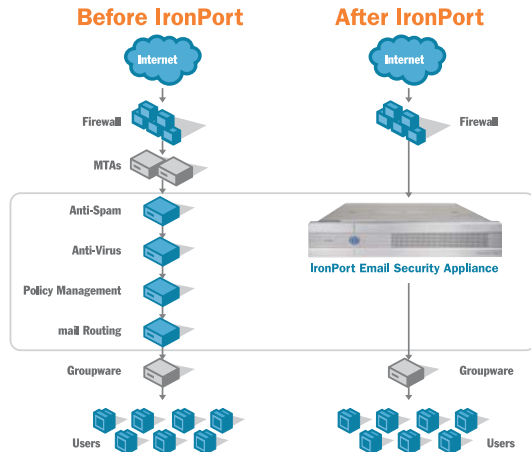
スパム対策について語るとき、「チューニングをすれば精度は向上します」というフレーズが頻繁に使用されます。しかし、チューニングという作業は決して簡単なものではありません。メールに関する専門知識が必要になるだけでなく、継続的な作業が要求されます。IronPortのスパム対策ソリューションは、日々のチューニング作業をメーカー側で実施することで、お客様への運用負荷を軽減しつつ、高い検知精度を維持しています。

IronPortでは、経験豊富な技術者が24時間365日の体制でルールセットの作成、更新作業に従事しています。日本語を含めた32の言語のスパムメールを専門的な視点から分析し、コンテンツやメールの構造など、スパムメールの特徴をルールセットとして構築します。

ルールセットは、IronPort AntiSpamスキャンエンジンによって使用され、E-Mail / Webレピュテーションの情報と合わせて、総合的なスパム判定が実施されます。

1台の統合型E-Mailセキュリティアプライアンス！

E-Mailが直面する脅威は、スパムメールの流入だけではありません。今日、E-Mailは日々の生活や企業活動に欠くことのできないコミュニケーションインフラへと成長し、その継続的な安定性を維持することが求められています。IronPort Cシリーズは、スパムメール対策だけでなく、E-Mailに関連したセキュリティ機能を包括的に提供する統合アプライアンス製品です。



▶ ウィルス対策

E-Mailの添付ファイルはウィルス感染拡大の主要な感染経路となっており、ウィルスへの対策はE-Mailシステムの必須要件となっています。IronPort Cシリーズは、法人、教育、政府ユーザ向けのウィルス対策として定評のあるSophos社のウィルス対策エンジンを内蔵しており、ウィルスへの対処を外部サーバなしにおこなうことが可能です。

また、SenderBaseが提供するレピュテーション情報を活用し、新種のウィルスの隔離、拡散防止を実現する独自ソリューション、VOF (Virus Outbreak Filter)も提供しています。

基本機能、基本性能も実はすごいです！

スパムメールの増加は社会問題にもなっていますが、その背後では、スパムではない正規のメールの数も大幅に増え続けています。また、E-Mailを介してやり取りされる情報の中身にも変化が現れてきています。今日では、重要性の高い情報もE-Mailを介して交換されており、迅速かつ確実な配信が求められているのです。

IronPortでは、パフォーマンスと安定性、信頼性の向上をE-Mailシステムの重要課題と位置づけ、様々な取り組みをおこなっています。

▶ パフォーマンス、スケーラビリティ

IronPort Cシリーズは、自社開発のAsyncOSで動作します。AsyncOSは、TCP/IPプロトコルスタックのSMTPへの最適化、ハードディスクの直接制御など多彩なテクノロジーを実装し、汎用UNIXベースのシステムに比べて飛躍的に向上したパフォーマンスとスケーラビリティを実現しています。また、宛先ドメインごとに独立した個別の送信キューを使用することで、遅延の短縮と確実な配信が可能になります。

▶ 情報漏えい対策とコンプライアンスの確保

E-mailは、社内外を問わずに、メールアドレスを持つ誰でもコミュニケーションできる非常に便利なツールです。しかし、E-Mailの利便性は一方で、個人情報や機密情報の漏えいといったリスクも持ち込んでいます。企業の情報管理の重要性が叫ばれる現在、E-Mailの運用を適切なポリシーに基づいてコントロールすることが求められています。

IronPort Cシリーズでは、添付ファイルを含めたメールのスキヤニングに対応し、特定のキーワードやメール送信先、添付ファイルの種類等によって、メールの隔離や管理者への転送等を設定することが可能です。

▶ スパム発信者にならない、疑われないための対策

スパムメールの急増を受け、近年、流入するスパムメールへの対策が脚光をあびています。反面、スパム発信者にならないための対策は、軽視されることが多いのが実情です。

また、実際にスパムを送信していなくても、スパム発信者に利用される可能性があるという理由からメールの受信を拒否されるケースも少なくありません。

IronPort Cシリーズでは、SMTP Auth、DomainKeys、送信メールの流量制御、不達通知の配信制御など多彩な機能を実装し、スパム発信者による悪用をあらゆる角度から防いでいます。

▶ 管理機能

IronPortのCシリーズの管理、監視は、GUI、CLI、SNMPなど、様々な方法でおこなうことができます。設定画面のGUIは日本語化されており、システム全般の設定のほか、トラフィック状況等の監視やレポートの生成等がおこなえます。導入時の初期設定には、セットアップウィザードの利用が便利です。画面上に表示される質問に回答することで、基本的な設定が完了します。導入後の設定変更やバージョンアップも簡単な操作でおこなえるため、運用コストの削減にも大きく貢献します。



アイアンポート システムズ株式会社

〒107-0052 東京都港区赤坂2-10-12 フォーシズ溜池山王ビル8F
phone: 03-5573-8160 fax: 03-5573-8159

http://www.ironport.com/jp/
email: Sales_Japan@ironport.com