

●この技術がわかれば、10歩差が付く！

ネットワークマニアックス

第21回 スпам対策とメール保存が要となる現代の電子メールセキュリティ

業務を支えるビジネスインフラとして定着したネットワーク。そのバックエンドで活躍する、ルータ、スイッチ、サーバやアプライアンスなどのネットワーク機器には、日々複雑化するビジネスニーズに対応したさまざまな機能が搭載されている。本連載は、そうした機能の中でも特にユニークなものに焦点を当て、どのような仕組みで実現しているのか、技術面と絡めながら解説する。 Lynx

安全な電子メール基盤には 内部統制への対応も不可欠

企業活動における電子メールの重要性は、それが登場した当初よりもずっと増している。今や受発注の処理や財務関係書類のやり取りなどでも、頻繁に電子メールが利用されるようになってきた。これに伴い、電子メールに対するセキュリティ対策の実施がこれまで以上に重要になっている。

また、電子メールがビジネス上重要な書類として認知され始めた中で、その確実な保存が法律で義務化される動きが見られ始めている。米国ではすでに2002年にSOX (Sarbanes-Oxley) 法という内部統制のための法律が施行されており、違反した際の罰則はかなり重いものとなっている。日本でも、新会社法および日本版SOX法による内部統制の義務化が予定されている。

このようにメールシステムの基盤としては、ウイルス/スパムなどに対する耐性だけでなく、これらの法規を遵守するためにメールデータの保存システムとの関係が重要となってきている。

ミラポイントは、電子メールを中心としたメッセージング基盤に特化したベンダーで、こうした電子メールのセキュリティおよび内部統制への対応を目指したソリューションを展開している。

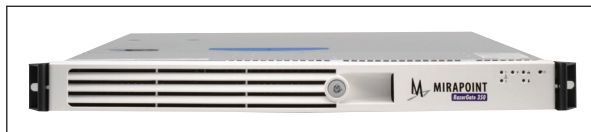


写真1● ミラポイントのRazorGateシリーズは「MailHurdle」技術により、主に外部からの攻撃に対する電子メールのセキュリティを確保する

まず電子メールのセキュリティ確保であるが、同社では「MailHurdle」という独自技術を展開している。

最大80パーセントのスパムを SMTPレベルで排除するMailHurdle

セキュアなメッセージングシステムの構築のためには、昨今、企業で問題視されているスパムメールへの対策を無視するわけにはいかない。ミラポイントではメールセキュリティについて、「MailHurdle」を活用したスパム対策やコンテンツフィルタリング、ポリシー管理を行うゲートウェイサーバ「RazorGateシリーズ (RZシリーズ)」(写真1)を展開している。ネットワークのDMZに配置することにより、インバウンドおよびアウトバウンドの両方に対してフィルタリングやポリシーの実施も可能だ。

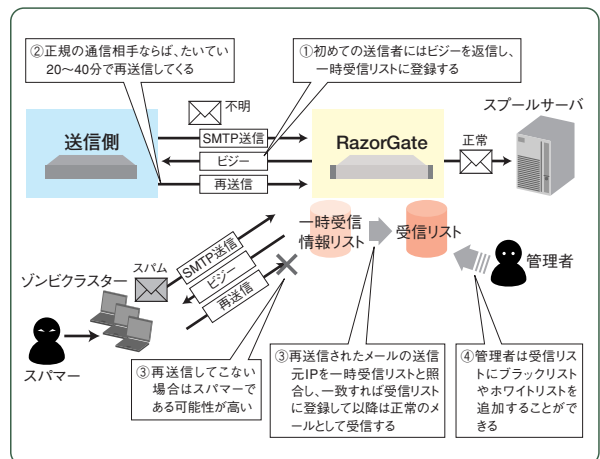


図1●RazorGateのMailHurdleにより、SMTPレイヤで60~80%のスパムを排除できる

スパム対策の古典的な手法は、コンテンツベースによるものだ。すなわち、ウイルス対策の仕組みと同様にシグネチャを用いたものや、スパムメールのメッセージの特徴を評価し、一定のしきい値を超えた場合スパムと判定するヒューリスティック、ユーザーがスパムメールを特定し、それをフィルタに学習させるベイジアンフィルタといったものなどだ。

RGシリーズでは、これらのコンテンツベースのスパム対策技術に加えて、MailHurdleによるアンチスパムを実現している。

MailHurdleは、スパムメールやウイルスをSMTPレイヤーで阻止するため、コンテンツベースのフィルタリングやメールプールに必要なネットワークおよびプロセッサリソースを大幅に削減することができる。

具体的な動作を例に挙げると、「スパマーはスパムメールを再送しない」という特徴を元に、正規の通信者かどうかを振り分ける(図1)。SMTP通信を受け取ったRGは、それが初めての通信相手であった場合に「ビジョー応答」を返信する。そして、その通信先のIPアドレスは、一時受信リストに登録される。その後ビジョー応答に対して、同一のIPアドレスから電子メールが再送信されてきたら正規の受信リストに登録して、電子メールを受け取る。この受信リストには、管理者がホワイトリストやブラックリストに登録できるので、これによりフィルタリングの精度はさらに高めることができる。ある大規模ユーザーではこの機能により16万通の電子メールを8万通に削減しているという。

そのほか、コンテンツの発生パターンに基づく検知や、過去の行動に対する評価を蓄積し、参照するレピュテーションによるフィルタリングも行う。

さまざまな技術との関係で さらに安全な電子メール基盤を構築

「メッセージゲートウェイサーバアプライアンス」であるRGシリーズは「メッセージプールサーバアプライアンス」との関係によって、よりセキュアなメッセージングシステムも構築できる(図2)。

プールサーバであるMirapoint Message Server「Mシリーズ」(写真2)は、電子メール専用の独自OS(MOS)を採用しており、セキュリティホールを狙った攻撃などにも強い耐性を持つ。また、ハイエンド機

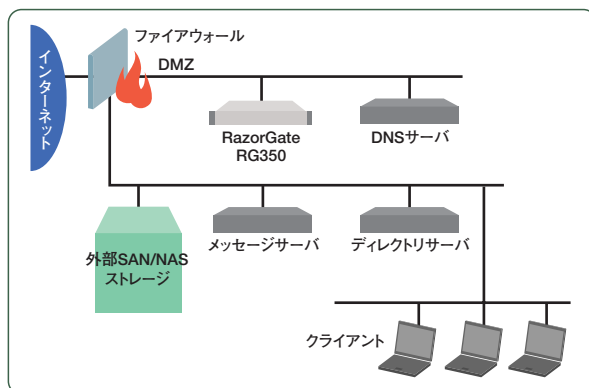


図2● RGで危険なメールを削除し、さらにメッセージサーバが外部ストレージに電子メールを保存することで万全な環境を構築する



写真2● 「Mシリーズ」は、電子メール専用の独自OSを搭載したメッセージサーバである

種の「M5000S」では、日立製作所、ヒューレットパッカード、IBM、ネットアップなどのベンダーのSANシステムに対応。ストレージとの関係による柔軟なバックアップシステムを構築可能としている。

電子メールの流通量は大きく増えているが、1通当たりのメッセージサイズも増大している。以前の電子メールは、テキストメッセージが主なものだったが、最近ではHTMLメールベースになったり画像が含まれていたりするためだ。法規制により電子メールのすべてをきちんと保存することが必要になった場合、巨大なデータストレージが必要であり、そのバックアップのためにメールサーバを止めることはできない。そのような観点からも、信頼性の高いSANとの関係は今後、重要となっていこう。

さらにミラポイントでは、さまざまなセキュリティ機能との統合も進めている。例えば、「インスタントメッセージング機能」ではテクノロジーパートナーであるフェイスタイムとのコラボレーションとして、無許可のP2Pトラフィックの遮断や、スパイウェアなどに対するプロテクションを提供している。このほか、ウイルス対策としてはFセキュアやソフォスとの関係で、1つのシステム内で複数のアンチウイルスエンジンを利用できるようになっている。今後、ミラポイントでは内部統制などを目的としたメールデータのアーカイブについても、製品の展開を予定しているという。