IronPort 導入事例

沖縄国際大学

→ スパム対策のみを期待してIronPortを導入したが、その他の良さも分かってきた。具体的には・・・

学生、教職員6,300人をすべてLDAP管理するなど、先進的なネットワーク体制を整えている沖縄国際大学は、悪質化し続けるスパムメールへの対策として、IronPortを導入した。導入の経緯、選定の理由などにつき、情報センターの玉手氏に詳しく聞いた。

沖縄国際大学にとってのIronPortの良さ

― 沖縄国際大学にとってのIronPortの魅力は何でしょうか。

「サーバ集約力」です。最近のセキュリティ製品は、多すぎるし、ややこしすぎます。スパム対策サーバ、ウイルス対策サーバ、何とか対策サーバをリレー、リレーで数珠繋ぎにする構成では、管理が難しい。IronPortは、様々なセキュリティ製品を、一個のアプライアンスに集約しうる「器」として、良いと思います。

しかし、「複数のセキュリティ製品を一個のアプライアンスに収める」というコンセプトだけなら、IronPort以外にも製品はあります。では、そういう製品とIronPortとの違いは何かということになると、それは高速性、堅牢性だと思います。機能をたくさん詰め込みすぎて、スループットが低下するのでは意味がない。従って、セキュリティ・アプライアンスでは、丈夫で速いこと、少々のことではビクともしないことが重要です。IronPortが優れているのはその点です。

なぜスパム対策に本格的に取り組むようになったか

― 沖縄国際大学では、現在、IronPortをどのようにお使いでしょうか。

学内ネットワークでのスパム対策に活用しています。ネットワーク使用者（メール使用者）の内訳は、教職員が約200人、非常勤が約300人、学生が約5,800人。合計で約6,300人を対象としたスパム対策です。

― 沖縄国際大学がスパム対策に本格的に取り組むようになったのは、どのような経緯で。

2005年になって、スパムの受信量が見過ごせないほど増え、内容も悪質になってきたこと。これが理由です。スパムも最初の頃は他愛ない内容でした。メール件名も、いかにもスパムと分かる扇情的な文字で、かえって選り分けやすかった。しかし、最近は「先日の件について」、「失礼いたしました」、「支払いの件」など通常のメールと見分けにくい件名になりました。学内でもスパムの手口にひっかかる学生が現れ、また先生方からも「あのスパムとやらは何とかならないか。これでは研究にならないのだが」と苦情が来るようになり、これはもう本格的に対策するしかないと判断。スパム対策製品を導入することにしました。

導入前に、どんな事前試験をしたか

― 製品選定はどのような基準で。

誤検知がないこと。高速、堅牢であることを求めました。SI会社に、そうした製品はないかと聞いたところ、IronPortが推薦されてきました。本当に誤検知が少ないのか、本当に高速なのかということは、実際にテストして判断するのが一番早い。ソリトンに実機を借りて、学内ネットワーク環境でテストすることにしました。

― どのようなテストを行ったのでしょうか。

以下のような手順でテストしました。

1.実際のメール送受信環境の中にIronPortを組み込む。

2.外からメールが来た場合の受け口が一時的にIronPortになるように、DNSを書き換える。もし試験中にトラブルが起きた場合は、ただちにDNSを書き戻し、元の設定に戻す。

3.教職員10人ほどにテストユーザーになってもらい、スパムの誤検知が発生しないかどうか見てもらった。

― 全6,300人のネットワーク参加者のうち、教職員10人だけをスパム対策の対象にできたのは、どのように。

IronPortでは、アドレス毎に個別ポリシーを定義できるという柔軟な設定が可能で、その機能により、特定の10人だけをスパム対策オンにしました。

― テストの結果はいかがでしたか。

すばらしい結果でした。スパムが、バシバシ引っかかって選り分けられていくのは、見ていて爽快でした。メール処理能力の点でも問題はなく、こちらの要件を満たしていると分かったので、IronPortの購入を決定しました。

＊導入製品：IronPort

IronPort 導入事例

沖縄国際大学

→ スパム対策のみを期待してIronPortを導入したが、その他の良さも分かってきた。具体的には・・・

使ってみて分かったIronPortの良さ3点

― 現在IronPortを使ってのご感想はいかがでしょうか。

スパム対策のみを期待して導入しましたが、その他の良さも分かってきました。具体的には以下の三点です。

1. バウンスメールによるネットワーク帯域内の性能劣化(目詰まり)が防げるという効果。
2. SenderBaseのスパム対策の有効性。
3. ネットワーク統計の現況把握ができること。

ネットワーク帯域内の性能劣化が防げる

― 最初のポイント「バウンスメールによるネットワーク帯域内の性能劣化が防げる」とは具体的には。

スパムを一般のMTAと通常のスパムフィルタの組み合わせで処理しようとした場合、以下のような流れにより、結局、ネットワークが目詰まりを起こすことがありえます。

1. スパムが、大量にMTAに送りつけられる。ただしそのスパムの発信元は偽装アドレスである。
2. 一般のMTAの場合、そのアドレスが実在するかどうかを区別できない。だからそのままメールサーバからは、発信元宛のエラーメールが返ってくる。
3. スパムは次々やってくる。メールサーバはエラーメールを次々送り返す。その結果、MTAの送信キューに、エラー通知メールが次々にたまる。
4. こうしてMTAのリソースが浸食される。最悪の場合、高負荷に耐えきれず、停止してしまうことも。

しかし、IronPortの場合は、「LDAPと組み合わせれば、実在しないユーザー宛のメールは破棄できる。またLDAP連携を行わない場合でも、大量メール受信の際は、メール送受信量制御機能による学内メールシステムの負荷軽減が可能」とソリトンから説明があり、納得しました。

SenderBase方式の有効性

― SenderBaseのスパム対策の有効性については。

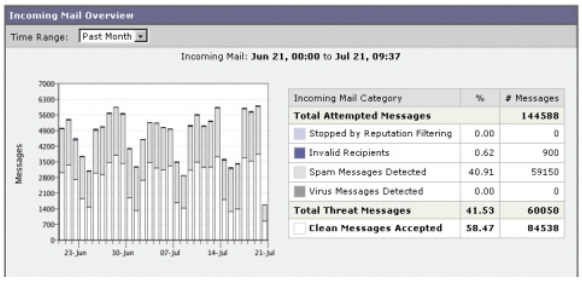
SenderBaseのスパム検知機能とは、要するにメールの発信元(Sender)について、信用度を-9.9から+9.9までの多段階でスコア付けをして、そのスコアが低い怪しい発信元からのメールはスパムと見なして受けないようにするという考え方でした。

最初は、少し不安でした。正規の送信者を、怪しいと決めつけて誤検知をしたらどうしようと恐れました。しかし、ソリトンによれば、「単純な話、何十回もスパムを送りつけているような発信元は、とうていまともとはいえない。そういう発信元は、当然SenderBaseでも低いスコアを持つこととなる。スパム送信者と決めつけて99.99%間違いない」との説明で、これにも納得しました。

ネットワークの濫用率の把握

― 「ネットワークの状況が把握できる」は具体的には。

IronPortの場合、以下のようなレポートが見られます。これにより、全メール流量におけるスパムの割合が把握できます。つまり、「全メール流量のうち何割が正規使用で、何割がスパムによる濫用なのか」がすぐに分かります。シンプルなデータですが、意外に重宝します。



※この図により、メール総量(Total Attempted Messages)は144588通で、うちスパムなど不正メール(Total Threat Messages)は60050通 41.53%で、正規メール(Clean Messages Accepted)は84538通 58.47%だと分かる。

プロスタッフへの評価

― 今回、導入に関わったSI会社、プロスタッフへの評価につきお聞かせください。

プロスタッフには、学内のパソコン教室のネットワーク構築などで、お手伝いいただいています。他の業者が、面倒くさがってサポートしたがらない所、あるいは技術が追いつかなくてサポートできないところでも、丁寧に確実にサポートしてくださいます。プロスタッフのネットワーク知識と仕事に対する姿勢には、強い信頼感を持っています。IronPortについても、「プロスタッフが推薦してきた製品なら間違いはない」と最初に思ったことが、採用理由の一つです。

ソリトンへの評価と期待

― 今回のIronPort導入におけるソリトンへの評価はいかがでしょうか。

担当SEの方の技術力とコンサルティング力は評価に値します。今回、IronPortを実際のネットワークに組み込むにあたり、我々としては、色々戸惑う点も多く、様々な既存機器との組み合わせの中で、この場合はどうなるのだろう、ここの設定をもしこう変えたらどうなるのかと、いろいろ湧き上がる疑問を、逐一SEの方にぶつけるのですが、常に原理原則に基づいた、的確な回答が返ってきました。

またSEのみならず、担当の営業の方も、この人、営業なのにどうしてこんなに詳しいのだろうというぐらい技術に明るい点も驚きました。

― 今後、ソリトンに期待することがあればお聞かせください。

今後も、沖縄国際大学では、無線LANの本格導入をはじめ、さまざまなネットワーク拡充を予定しています。そうして利便性を上げていけば、当然、セキュリティ上の課題も複雑化するでしょう。ソリトンには、そうした課題の解決をご支援いただきたいと思います。最新情報や最新技術、あるいは今となっては最新ではないが実は有用な技術など、様々な技術要素を上手くミックスさせた提案をお願いいたします。

― 承りました。今日は貴重なお話をありがとうございました。

お問合せ先
株式会社ソリトンシステムズ 〒160-0022 東京都新宿区新宿 2-4-3
TEL. 03-5360-3811 FAX. 03-5360-3880 MAIL. netsales@soliton.co.jp www.soliton.co.jp

Soliton