

「@niftyメール」でDDoS攻撃や スパム対策にIronPort X1000を採用

ニフティは、メールサービス「@niftyメール」の大幅リニューアルを行い、同時に無料メールサービスを開始した。

そこでメールセキュリティとして採用されたのがIronPortの製品だった。ニフティ株式会社 パーソナルサービス部 チーフエンジニアの工藤隆久氏に、採用の理由と背景について聞いた。



@nifty



ニフティ株式会社
パーソナルサービス部 チーフエンジニア
工藤 隆久氏

「サービスプロバイダが求める
かなりの処理量に対しても、
安心して任せられると
感じています」

無料メールサービスでのセキュリティに IronPortを採用

— IronPortは、ニフティのどのサービスに 使われているのでしょうか。

今回、6月4日からメールサービス「@niftyメール」をリニューアルするに伴い、まず新たに開始した無料メールサービスでIronPortの製品を利用しています。具体的には、外部からのメールを受信するフロントエンドのMTAとして複数台のIronPort X1000を導入し、また、スパムメールのフィルタリングなどメールセキュリティにも利用しています。

ボットネットからの保護と高精度の スパムフィルタリング

— IronPort導入の目的は、どのようなもの だったのでしょうか。

@niftyメールの大改造と同時に、これまでの課題を解決していきたいと考えていました。そこで選んだのがIronPortです。

主な課題は、以下の2点でした。

1. サーバ群を守る

これまで、MTAには多数の汎用IAサーバを用いてきました。そのサーバを攻撃から守るために、いろいろな仕組みを設けていましたが、最近増えてきたボットネットによるDDoS攻撃などでは、ソースIPの範囲を特定することもできないなど、防御が難しくなっていました。しかも、防御のためのレピュテーション基準としては社内のデータを使っていたため、初回の攻撃は防ぐことができなかったのです。サービスプロバイダとしては、メール不達などはサービス品質の上で許されるものではないので、大胆な対策もできませんでした。

特に多かったのは、セッションを張ったまま黙り込む

ケースで、これが大きな問題となっていました。一度に数千本ものコネクションを取られたこともあったほどです。しかし、これまでMTAとして使っていた汎用IAサーバはオープンソースで構築しており、1台あたりの同時コネクション数に限りがあります。我々としても、お客様に影響が出ないような仕掛けを作って対処していましたが、それでも遅延などの影響を避けることが困難でした。

この点で、IronPortの独自OS (AsyncOS)が可能とする同時コネクション数は、送受信10,000と汎用OSの数十倍もあるので、IronPortは我々のニーズにちょうど合うものでした。

2. スパムの振り分け

メールサービスを開始するにあたり、無料とはいえスパム対策が施されているのは当たり前前の時代、サービスプロバイダとして誤検知というのはあってはならないものです。IronPortのスパムフィルタリングの精度の高さはIronPortを採用する上での大きな要因の一つとなりました。IronPortが独自に展開するSenderBaseネットワークというレピュテーションネットワークは収集している情報が膨大であるがゆえ、精度の高いスパムフィルタリングを実現でき、以前からの@niftyサービスの評判を下げず、同等以上のサービスを無料の「@niftyメール」でも提供できると確信しました。実は、品質の高いサービスをお客様に提供すると共に、内部のリソース消費を削減するという意味でもIronPortは大きく貢献しています。無料メールサービスというのは無料ゆえに明確な「解約」が行われず、使われなまま放置されたメールボックスが、いつまでも残ってしまう可能性があります。そこで、「迷惑メールフォルダー」の機能をデフォルトでONにすることにしました。こうする事により、スパムを振り分け削除し(短期間保有)、リソース消費を削減する事が可能となりました。精度の高さを保持するためには、情報収集は欠かせないものです。世界のプロバイダ/企業/大学/研究機関をまたがるIronPortの情報収集は我々にはできない部分ですから、高く評価

導入事例：ニフティ株式会社

していると共に更なる向上を期待しています。

— 構築に際し、パフォーマンスなどについては、どのような評価をされたのでしょうか。

サービスインの1年ほど前に評価機を借り、2カ月半ほどMTAとしての評価を行いました。まず評価の段階で今後のトラフィックの増大を想定し、IronPort X1000はどこまで耐えられるかというテストを行いました。その結果、IronPortは、かなりの負荷がかかっても問題ないという事がわかり、安心して導入台数を抑える事ができました。

なお、スパム対策面の評価に使うサンプル収集に時間がかかったりしましたが、それを除けば評価も導入も、ほとんどスムーズに進みましたね。

技術的なサポートも重要な要件

— 選定に際し、他にどのような条件を考慮したのでしょうか。

やはり技術的なサポートですね。我々はサービスプロバイダとして、一瞬のサービス停止も許されません。サービスプロバイダのトラフィックは膨大なので、5分ほどの遅延でも溜まったデータの後処理には相当の時間を要し、完全復旧までに数十時間かかってしまうような可能性もあるのです。

IronPort製品のようなアプライアンスは、オープンソースプロダクトのように、インターネットで検索すればノウハウが出てくるというものではないので、細かなノウハウの部分までサポートしてもらえることが重要です。

一般的に、海外ベンダーは日本語でのサポートに不安がありますが、IronPortは非常に手厚いサポートをしてくれます。特に、既存のアーキテクチャに対してどのような工夫をすれば良いか、というコアなアドバイスをIronPort自身から受けられたのが良かったですね。

またIronPortと共に技術サポートに加わってくれましたIronPortの販売パートナーさんの技術力も高く、信頼できるサポート体制に大変満足しました。

「利活用促進」という戦略を支えるIronPort

— @niftyメールのリニューアル、無料サービス開始において、IronPortは大きな役割を果たしたと言えますそうですね。

当社サイトのIP情報などを見ていただければ分かるかと思いますが、代表取締役社長の和田一也が「利活用分野への積極的な投資による新サービスの早期立ち上げ」を重要な事業戦略のひとつとして語っているように、インターネット上で楽しむ、インターネットを活用するといった、接続サービス以外のサービス分野にも力を入れています。無料メールサービスは、まさにその各種サービスへの入り口となるものです。もちろん、そこには高いサービスレベルが要求されていますし、その一方できちんとした収益性も求められます。こういった我々の要求に対して、IronPortはメールセキュリティといった観点での製品力のみならず、導入から運用にいたるまで総合的に十分ペイできるソリューションであると思いますね。



「@niftyメール」Web MAIL画面(2007年8月時点)



(左) 工藤チーフエンジニアと会談する(右) アイアンポートシステムズ株式会社 代表取締役社長原田英昭

「一瞬のサービス停止も許されないプロバイダですから、IronPortの技術的なサポートの厚さは信頼できます」



アイアンポートシステムズ株式会社

<アイアンポートシステムズはシスコシステムズの事業部門です>

〒107-0052 東京都港区赤坂2-10-12フォーシーズン溜池山王ビル8F
TEL. 03-5573-8160 FAX. 03-5573-8159
email: jp-info@ironport.com

www.ironport.com/jp

*本ケーススタディに記載された情報は初掲載時及び更新時のものであり、閲覧される時点では変更されている可能性があることをご了承ください。

*本ケーススタディは情報提供のみを目的としています。明示的または暗示的を問わず、いかなる保証も与えるものではありません。

*IronPort, IronPort logo, SenderBase, IronPort製品名はCisco Systems, Inc.の登録商標です。本カタログに記載されているその他の会社名、製品名はそれぞれ各社の商標または登録商標です。

Copyright © 2000-2007 Cisco Systems, Inc. All rights reserved. IronPort, the IronPort logo and SenderBase are registered trademarks of Cisco Systems, Inc. All other trademarks are the property of Cisco Systems, Inc. or their respective owners. While every effort is made to ensure the information given is accurate, Cisco does not accept liability for any errors or omissions which may arise. Specifications and other information in this document may be subject to change without notice. P/N CSJP-3 07/08

IronPort is now
part of Cisco.

