IronPort 導入事例

アイテック阪神

→ スパム対策製品を選定するにあたり、4社の製品を比較した。なぜ、IronPortが採用されたのか？

プロバイダ事業に注力するアイテック阪神は、ユーザー向けのスパム対策とウィルス対策に注力している。今回、なぜIronPortがセキュリティ・アプライアンスとして選定されたのか、ネットワーク技術グループの森健一氏（写真右）、南村達哉氏（写真中央）、石井孝志氏（写真左）に聞いた。キーワードは、「サーバ集約」「LDAP完全連携」、そして「ユーザーへのON/OFF選択権の提供」・・・

耐久テストに最後まで耐え抜く

― アイテック阪神にとってのIronPortの最大の魅力は何でしょうか。

速さと堅牢さです。処理速度が驚くほど速い。あまりに速くメールを吐き出すので、それを受ける次のシステムがスピードに追いつけません。今は、そのシステムが追いつけるよう、IronPortをわざわざ遅く設定しているほどです。

また、導入前の耐久試験（拷問テスト）で分かった堅牢さも印象的でした。

― どのような耐久試験を行ったのでしょうか。

以下のような試験です。

1. 疑似環境を組んで、その中にIronPortを組み入れる。
2. そこに、毎秒何十通かのスピードでメールを10分間流し続けた。
3. 毎秒10通　→　IronPort問題なし。
4. 毎秒50通　→　問題なし。
5. 毎秒80通　→　問題なし。
6. 毎秒100通（10分で6万通）　→　IronPort依然として問題なし。もういい分かったということでテスト終了

結局IronPortは最後まで音を上げませんでした。

IronPortは、プロバイダ契約者向けのメールセキュリティ対策サービス

― 現在、アイテック阪神では、IronPortをどのように使っているのでしょうか。


「サーバ集約が果たせたことは大きなプラスです」

アイテック阪神では、阪神電鉄グループの情報システムの構築・保守の他に、一般のお客様向けのISP事業も行っています。IronPortは、そのISP事業における、「会員向けスパム対策サービスおよびウイルス対策サービス」として活用しています。また、会員一人一人を管理するための、既存LDAPシステムとも完全に連携させています。

導入台数は4台です。ISP事業における、これまでのメール流量のピーク量を元に積算すると、IronPort2台でも処理可能でした。とはいうものの、将来のメール流量増加を見越して、もう一台。さらにトラブル時のスタンバイ機としてもう一台。つまり「2台＋将来を見越してもう1台＋予備としてもう一台」の、２＋１＋１構成です。

ウイルス対策とスパム対策を、4台のアプライアンスに集約できることは、システム肥大化の防止、保守コストの削減の面から言って、大きなプラスです。

＊導入製品：IronPort

IronPort 導入事例

アイテック阪神

なぜスパム対策が必要になったか

― アイテック阪神がスパム対策に本格的に取り組むようになったのは、どういう経緯から。

2004年になって、スパムの量や頻度が無視できないほどに増えてきました。この事で、以下２つの側面から問題が生じてきました。

1.【 システム可用性、信頼性の問題 】
外部から大量のスパムメールを送りつけられると、メール流量が無意味に増大し、そのため正規メールの送受信が滞る事態が生じてきました。またスパム大量受信が、疑似DOS攻撃の働きをして、システムが一時的にダウンすることさえありました。

2.【 顧客満足度の問題 】
単純な話として、スパムがたくさん届く状況は、お客様にとって不快です。対策を提供することは、プロバイダの責務であると思われました。

こうした問題を解決するために、スパム対策システムの導入を決めました。

スパム対策システムに求める4要件

― アイテック阪神として、スパム対策製品に求めた要件はどのような。

以下4つの要件を求めました。

1.【 大量のメールの中からスパムメールを確実に選別できること 】

2.【 スパム対策サービスをONにするかOFFにするかをユーザーが選択できること 】

3.【 既存のLDAPシステムと完全に連携できること 】

4.【 大量のメール処理に耐えうる堅牢な設計であること 】

― 2つ目の要件「スパム対策サービスをONにするかOFFにするかをユーザーが選択できること」とは具体的には。

無料スパム対策のような便利なサービスは、全ユーザーに一律にONに設定してもよいという考えもあります。しかし、弊社では、スパム対策をONにするかOFFにするかは、ユーザーの選択にゆだねることにしました。理由は以下の二つです。

1.誤検知のリスクに備える
正規メールがスパムと勘違いされて削除されることを恐れました。現在は、IronPortがスパムと認定したメールでも、すぐに削除したりせず、「これはスパムメールです」という印をつけてユーザーに送信しています。ユーザーはメーラーの振り分け設定により、スパムと正規メールとを選り分けることができます。

なお、その選り分けが面倒というお客様向けには、「弊社のメールサーバ側でスパムを削除する（お客様にはスパムは届かない）」というオプションも用意しています。これももちろんお客様にON・OFFの選択権があります。

2.「通信の秘密」を尊重する
スパム対策を一律ONにした場合、「プロバイダがメールを検閲している」というイメージにつながりかねません。厳密に言えば「通信の秘密」に抵触します。弊社では、「スパム対策をしてもよい」とお客様から明示的な許可が出たときのみ、スパムチェックをすることにしました。

なぜLDAPが必須か

― 3つ目の要件「既存のLDAPシステムと完全に連携できること」については。

LDAPとの連携は必須でした。その理由は以下の通りです。

1.弊社は、ユーザー一人一人にスパムチェックのON・OFFの選択権を与えることにした。

2.これは、会員一人一人のスパム対策のON・OFF記録を弊社側で厳密に管理できねばならないことを意味する。

3.会員A様はスパム対策ON、B様はOFF。C様は昨日までONだったが今日からはOFF…といった管理が、確実、厳密にできねばならない。

4.アイテック阪神では、LDAPによるユーザー管理システムが既に存在していた。スパム対策やウイルス対策のON・OFF管理も、この既存システムで行いたい。

5.従って、新たなスパム対策システムは既存LDAPに完全に連携できねばならない。

ちなみに現状のON・OFFの種別は、スパム対策[ON/OFF]、ウイルス対策[ON/OFF]、スパムのサーバでの自動削除の[ON/OFF]の3通りになります。この場合、順列組み合わせで8通りのパターンが存在します。これをユーザー一人一人につき、確実に管理できねばなりません。


「LDAP連携は、必須でした」

各製品をどのように比較したか

― 今回、スパム対策製品を選定するにあたり、色々と比較検討もなさったと思います。どのような製品と比較なさいましたか。

まず「ユーザー毎のON・OFFが可能なLDAP対応スパム対策システム」という基準で調査したところ、以下4社の製品が候補にあがりました。

1.A社

2.B社

3.IronPort

4.既存のウイルス対策システムの継承・拡張

このうちA社については、よく調べると、ユーザー毎の[ON/OFF]は実際は不可能でした。ユーザー全員の一律ON、一律OFFしか実はできませんでした。

B社の製品は、ユーザー毎のON・OFFはできました。しかしONをOFFに戻すことができなかった。きめ細かさに難がありました。

― 3つめの選択肢、「既存のウイルス対策システムの継承・拡張」については。

実は、この選択肢が当初は最も有力でした。

その頃の弊社では、あるウイルス対策企業(C社)から購入したウイルス検出エンジンを、自前で構築したシステムに組み込んで、

＊導入製品：IronPort

ユーザー向けウイルス対策サービスを行っていました。

このC社からスパム対策エンジンの供給を受け、それを既存サーバに組み込むことを検討していました。こうすれば、「目新しい、不慣れなシステムを導入する」のではなく「今日動いているシステムを、明日も使う」ことができます。

― その「有力な選択肢」をなぜ選ばなかったのでしょうか。

理由は二つあります。一つは、その時点でC社のスパム対策エンジンが、ロードマップ上には計画されてはいたものの、製品としてはまだ発売されていなかったこと。「今から作ります」であって「今あります」ではなかったこと。もう一つの理由はサーバ台数の問題です。

― 「サーバ台数の問題」とは。

当時、C社のウイルス対策エンジンをサーバ5台で稼働させていました。C社に問い合わせたところ、これにスパム対策エンジンを加えるとなると、そのエンジン用にサーバ3台が別途必要。さらにウイルス対策サーバ群と、スパム対策サーバ群をつなぐためのサーバが別途1台必要という試算でした。さらに構築にあたってはOSの入れ替えも必要。エンジン以外のシステム部分は一から作り直しが必要とのことでした。

このやり方の場合、以下の問題が生じます。

1.ハードウエアとしてのサーバを合計9台揃えねばならない。その購入コスト。

2.サーバ9台を、保守管理せねばならない。その人的コスト。

3.OSの入れ替え、システム作り直しという開発コスト。

4.既存システムを拡張、継続使用した場合、ウイルス対策サーバ群、スパム対策サーバ群、メールスプールサーバ群の三段構成になる。そうなると、メール配送状況をチェックする際に三カ所を調査しなければならず、面倒。

これらの問題を一文で述べると、「システムが肥大化し、シンプルさが失われ、管理コストも増大し、現状把握は困難になる」ということです。これらデメリットの方が、既存システム継続使用のメリットよりも大きいと判断できました。ここにおいて既存システムの継続使用という選択肢は消滅しました。

― そうしてIronPortのみが残ったと。

はい、そうです。IronPortは、LDAP連携もユーザー毎ON・OFFを正しくきめ細かく行えました。また堅牢性、高速性も、冒頭に述べたとおり全く問題ありませんでした。さらにスパム対策、ウイルス対策、メールシステムが4台のアプライアンスに集約できるなど、システムのシンプル化の点で優れていました。こうしてIronPortの採用が決定いたしました。

IronPortの使用感

― IronPortの現状の使用感はいかがですか。

堅牢性など性能面は申し分ありません。また外部からのスパムはほぼ皆無となりました。高速性も、冒頭に申し上げたとおり、スプーラが追いつかないほど。速すぎるほどに速い状況です。

― IronPortと既存LDAPとの連携にあたり既存LDAPシステムを、どのぐらい変更したのでしょうか。

きわめて軽微な変更だけですみました。IronPort用のフラグを一つ増やしただけでした。

ソリトンの付加価値

― IronPortの導入における、ソリトンの付加価値につき、ご評価ください。

「ソリトンのネットワーク構築ノウハウに期待しています」

ソリトンの付加価値は大変大きかったと思います。今回のIronPort導入にあたり、既存のLDAPと連携させながら、実際のISPシステムの中に、手際よく組み込んでいくことができました。万事がさりげなく手際よく進行しましたが、これはソリトンのネットワークに対する理解の深さ、IronPortに対する理解の深さに負うところが大きかったと思います。「単なる販売店」から購入していたとしたら、LDAP連携もこれほどスムーズには進まなかったでしょう。

ソリトンでは、IronPortを販売する前に、自社のシステムに組み入れて自分で使ったとのことでした。人に売る物はまず自分で使うという、誠実な姿勢だと思います。こちらの質問に常に的確にお答えいただけるのも、その経験の裏打ちあってのことでしょう。

― 今後ソリトンに期待することなどあればお聞かせください。

弊社のプロバイダ事業は、おかげさまで順調に会員数を伸ばし続けており、今は、小規模プロバイダから中規模プロバイダに成長しようとする段階です。システムや設備については、これまで手作りを中心にコツコツと取り組んできましたが、それらのシステムも処理能力が中途半端になってきました。今後、この先5年10年を見すえたネットワーク設備をくみ上げたいと思っています。その際にはスパム対策のみならず、ネットワーク構築のさまざまな局面で、技術支援をいただければと思います。

― 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。

過酷な試験に耐え抜いたIronPort

＊導入製品：IronPort

MAKING THE INTERNET SAFE.™

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®