IronPort 導入事例

大東文化大学

→ 大東文化大学が、スパムメール対策に
IronPortを選んだ理由は3点。具体的には・・・

「『誤検知率の低さ』、『スパム検知されたメールの隔離と復活の容易さ』、『ライセンス形態』、この3点を基準に製品選定を行ないました」

大東文化大学 学園総合情報センター事務室　波多江 哲也氏、吉澤 潤氏

大東文化大学　学園総合情報センター（以下、情報センター）事務室の、波多江哲也氏、吉澤潤氏に、大学という環境ならではのスパムメール対策の課題と、IronPortへの評価について詳しく聞いた。

DAITO BUNKA UNIVERSITY

もくじ

大東文化大学ではIronPortをどう活用しているか

― 大東文化大学ではIronPortをどのように活用していますか。

大東文化大学では、事務職員及び教育職員など約300人（300メールアカウント）の、スパムメール対策システムとしてIronPortを活用しています。

スパムメール対策における「大学ならではの難しさ」

― スパムメール対策における、「大学ならではの、難しさ」があれば、お聞かせください。

「大学ならではの難しさ」は2つあります。一つは「大学という組織の運営理念から生じる、難しさ」、もう一つは、「海外との交流が非常に多いことから生じる、難しさ」です。

＊導入製品：IronPort

IronPort 導入事例

大東文化大学

組織の運営理念から生じる、スパム対策の難しさ

― 「大学という組織の運営理念から生じる、難しさ」とは具体的には。

一般企業と対比して考えれば、分かりやすいと思います。一般企業とは、形式定義の上では、社長をトップとする利益追求集団です。企業は、業務時間中は社員を「管理」することができます。一方、大学は、学問研究を自由に行う場所です。「管理」、「統制」という概念は、なじみません。

このことを、スパムメール対策に当てはめて考えてみます。企業であれば、スパムメールとは「業務と関係ないメール」であり、一律に排除して問題はありません。しかし、大学の場合は、社会学の教育職員などが研究対象としてスパムメールを収集することも、理論上はありえます。一律に排除できません。

海外との交流が非常に多いことから生じる、スパム対策の難しさ

― 「海外との交流が非常に多いことから生じる、難しさ」とは具体的には。

大学とは研究機関ですから、必然的に海外との交流が多くなります。したがって、英文やその他の言語のメールが、世界中から来ます。そのように世界とつながっている場所には、スパムメールも、世界中から大量に届きます。

日本人一般のスパム選り分け基準として、「英語の題名の、変なメールが来たら捨てる」というやり方があります。しかし、大学は、もともと英文メールが多く来る場所なので、その基準は使えません。

また、「件名がカラのメールは、変なメール」と見なすやり方も使えません。大学の場合は、学生が携帯電話からメールをしてくる時に、不注意で件名がカラになることがよくあるからです。

夏休み中に1万通のスパムメール

― 大東文化大学が、スパムメール対策に本格的に取り組むようになった経緯を教えてください。

2004年になって、スパムメールが大量に来襲するようになりました。特に海外とのやりとりが頻繁な国際交流センターのメールボックスでは、届くメールの95%がスパムでした。担当職員は、いちいちメールを開いて、読んで、要不要を判断して、捨てて、そんな作業だけで一日に数十分を使わねばなりませんでした。

「スパム検知レポートの自動生成機能は便利です。」

あるメールアカウントを、40日ぶりに開いてみた時も、ひどかった。スパムメールを含む10,000通の受信メールが溜まっていました。その10,000通のメールの中に、まともなメールがほんの数通まぎれこんでいるわけです。本当の気持ちとしては、全部まとめて削除してしまいたかったのですが、業務となれば、そうもいかない。あの時は、まいりました。

スパムメールによる事務効率の低下は、見過ごせないレベルに達していました。平成17年度の予算編成の際に、スパムメール対策の導入を、予算項目に入れることが決まりました。

スパムメール対策会社に質問状を送る

― 製品のリストアップや選定はどのように行ったのですか。

まず展示会に出向いて、スパムメール対策製品の情報を集めました。その後、各社に、こちらで作成した質問状を送付しました。質問状の内容は以下の通りです。

1.「個人管理画面はありますか」
2.「以下の個人管理画面のユーザー認証方法はありますか。1): POP3、2): IMAP4、3): Windows Server 2003のActiveDirectoryを含むLDAPサーバー、4): スパムフィルターにメールアドレス、パスワードを登録する個別認証」
3.「スパムフィルターで個別認証が可能な場合、パスワード忘れに自動で対応する機能はありますか？(例えば、秘密の質問などを設定し、回答が一致した場合はパスワードを該当するメールアドレスに送るなどの方法)」
4.「複数ドメインの管理ができて、かつドメイン単位で認証方法を変えることはできますか(AドメインはActiveDirectory、BドメインはPOP3など)」
5.「1日1回サマリーメールを利用者にHTML形式以外にテキスト形式で送付することはできますか。また、スパムの検出がなかった場合はサマリーメールを送信しないことも可能ですか」
6.「管理者が個人のブラックリスト・ホワイトリスト、スパム誤検出メールの再送信などの作業を行うことはできますか。」
7.「スパムの検出率は？」
8.「スパムの誤検出率は？」
9.「スパムフィルターに実際には3ドメイン合計の数万ユーザーのメールが経由して1次MTAに送られますが、実際に使用するユーザー数は、(xxx).daito.ac.jpドメインの350ユーザーです。ただし、(xxx).daito.ac.jpドメインから実質スパムフィルターに登録するのは320ユーザーで、残りの30ユーザーについては先着順で(yyy).daito.ac.jpドメインから希望者を募りたいと考えています。この場合、何ライセンスの購入が必要ですか。」
10.「HTML形式のサマリーメールの件名等をクリックしたときに個人管理画面の認証を経由せず、本文を閲覧することは可能ですか」
11.「スパムパターンファイルの更新は一日平均何回ですか？(リアルタイムで更新する場合はその旨ご回答ください)」

＊導入製品：IronPort

12.「1次MTAから2次MTAにリレーするメールについても、スパムフィルターをかけることとかけないことと両方が可能ですか？つまりinfo@(yyy).daito.ac.jpというメーリングリストのメールアドレスが存在し、そのメンバーがa@(xxx).daito.ac.jp、b@(xxx).daito.ac.jpで、スパムフィルターにはinfo@(yyy).daito.ac.jpのユーザー登録をしなかった場合。」
13.「ソフトまたはハードの故障又は停止が発生した場合、スパムフィルター機能は停止してもメールの送受信を止めないことは可能ですか。(故障時にバイパス機能のようなものはありますか？)」
14.「件名にスパム判定結果をスタンプする機能はありますか」
15.「メールヘッダーにスパム判定結果を追加(例えばX-Spam…など)する機能はありますか」
16.「icドメインは1200ユーザーですが、メーリングリストのアドレス200が含まれています。実質的なユーザー登録数は1000ユーザーです。この場合に必要なライセンス数は？」
17.「350ユーザーが使用可能な環境での費用(初年度)」
18.「次年度以降のソフトウエア、ハードウエア保守経費」
19.「保守内容」
20.「その他経費(本学で実施するのであれば不要)」

特に注目したのは、「誤検知率の低さ」、「スパム検知されたメールの隔離と復活の容易さ」、「ライセンス形態」の3点でした。

各社の質問状への精査した結果、IronPortが最も優れていました。書類審査は合格です。続いて、実機を試験導入して実地検査を行いました。

実地検査で重点を置いた検査項目3点

— 実地検査で重点を置いた検査項目は何ですか。

「誤検知の少なさ」、「スパム検知されたメールの隔離と復活の容易さ」、「特殊なネットワーク環境への対応」の3点でした。

検査項目1:「誤検知の少なさ」

— 順々にお聞きします。検査項目1:「誤検知の少なさ」とは具体的には。

本来のメールがスパムとして誤検知されることは極力避けなければなりません。IronPortは、カタログによれば、誤検知はメール100万通に1通とのことでした。良い性能だと思いますが、鵜呑みにはできないので、実地に検査を行いました。検査対象にしたメールアドレスは普段からスパムメールに悩まされている2つのメーリングリストのメールアドレスです。

2週間ほど検査を行なったところ、結果として誤検知はゼロでした。「誤検知ゼロ」の定義は、「スパムメールがチェックされずにメールボックスに届いた例は、数通ある。しかし、正しいメールをスパムと勘違いして隔離してしまった例はゼロ」ということです。

良い成績だと思いました。合格です。

検査項目2:「スパム検知されたメールの隔離と復活の容易さ」

— 検査項目その2:「スパム検知されたメールの隔離と復活の容易さ」とは。

仮にスパム対策システムが「スパム」と判定した場合でも、ユーザー判断により、「それはスパムではない。受信させるように」と指示したい場合があります。大学のような研究機関では、特にそれがありえます。

そのような「ユーザー判断によるスパム・非スパムの仕分け」を容易に行える仕組みが必要でした。

IronPortにおいては、その仕組みは、「サマリーメール」という形で実装されていました。

スパム認定が不服の場合は、左の「スパムではない」をクリックすれば、正規メールとして配送される。

この内容、この文面なら、ユーザーでも自主管理が可能です。ユーザーが自主管理してくれれば、情報センターの運用負荷が減ります。ユーザーと我々の双方にとって良い仕様だと思いました。

検査項目3:「特殊なネットワーク環境への対応」

— 検査項目その3:「特殊なネットワーク環境への対応」とは。

大東文化大学では、事務職員が使う事務系ネットワークと、教育職員が使う教育研究系ネットワークが、別系統になっています。しかしスパムメール対策は、IronPort1台で、両方のネットワークに施したい。IronPortは、LANカード二本差しにより、それが可能だとのことで、実験時にその構成を試みました。問題なく稼働しました。

以上、期待通りの結果を得たので、IronPortを実導入することを決定しました。本稼動したのは平成19年3月からです。

＊導入製品:IronPort

導入後の学内での評判

― 導入後の、学内でのIronPortの評判はいかがですか。

良い評判を得ています。情報センター所長は、「一日500～600通は来ていたスパムメールがほとんど無くなった」と感動していました。サマリーメールによる、スパム・非スパムの自主選り分けも順調に進んでいます。情報センターに、使い方の問い合わせが来ることもほとんどありません。

「学内ユーザーからも高い評価を受けています」

― 実際につきあってみて分かったソリトンの良さなどあればお聞かせください。

ソリトンは、エンジニアのみなさんの対応力が優れています。何か質問すると、必ず、的確な応えがあります。

技術的に難しい質問、製品に対する厳しい要求に対し、メーカーの技術者が、堂々と回答してくれるようでないと、そのメーカーを推している我々は困ります。

ソリトン以外の数社に技術的な質問をしたところ、曖昧な回答が返ってくることが多かったです。唯一、ソリトンのエンジニアだけが、常に的確な回答をしてくれました。聞けば、IronPortにはソリトン社内でも、トップクラスのエンジニアが充てられているとのこと。心強いですね。

今後の期待

― ソリトンやIronPortへの今後の期待をお聞かせください。

今回のスパムメール対策システムの導入は、期待通りの成果を納めることができた、成功プロジェクトとなりました。ご協力有り難うございます。今後もソリトンには、今の技術力の高さ、対応力の高さを今後も継続提供していただき、大東文化大学のセキュリティ向上を支えていただけるようお願いします。期待しています。

― お忙しい中、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®