+abmail — 迷惑メール対策サービス
～ 迷惑メール判定プログラム「abmail」の導入について ～

株式会社あいはら 研究開発チーム

2007/2/23 初版 2007/3/5 改訂 2007/6/25 改訂

はじめに

弊社で大量の迷惑メールが届くようになったのは２００４年中頃、当時、メールサーバの負荷を考えるとコストの掛かるスパム判定法を行うわけにもいかず、なるべく単純な検査項目の積み重ねでスパム自動振り分け等の対処を行ってきました。しかし、いくつかの検査項目は安定して有効なものの、特にメール本文に関する検査項目は、敵も手を変え品を変え送りつけてくるので、もはやイタチごっこになるのは必至に思えました。そこで、既存の迷惑メール対策を検討しましたが、現状、それらの手法を惑わし擦り抜けるスパムが絶えず出現しているという有様です。

そこで、スパマーがメールを送る際に自由にならない項目のみから、迷惑メールであることを判定することは出来ないかと、かつての検査項目を見直し且つ洗練させ、単純で軽量な独自の迷惑メール判定プログラム「abmail」を書き起こしました。２００６年、弊社ではそのプログラムにより再び迷惑メールに患わされない、かつての平穏な日々を取り戻すことが出来たのです。

１．迷惑メール判定プログラム「abmail」とは

このサービスの中核をなす迷惑メール判定プログラム「abmail」は、以下の特徴を持ちます。

1. メール本文をいっさい走査せず、ヘッダ情報のみから迷惑メールであることを判定します。スパマーやボットは大量のメールを送信する都合上、なんらかの偽装や特異な痕跡を残すので、それを検知しています。
2. 併せて、外部アカウントからの意図した転送にも対応するために、メールサーバへの正当なメール到達経路情報を設定することによって、他の正当なMTA経由の迷惑メールを判定することが出来ます。
3. 軽量なアルゴリズムをプログラミング言語Cでセキュアコーディングされており、極めて安全かつ高速に動作します。よって、メールサーバへの負荷が少なく済みます。
4. 正当なMTAから返されるバウンスメールについて、真にユーザが宛先を間違えてしまったのか、差出人が詐称された故の偽のバウンスなのかを判定することが出来ます。この場合も、バウンスメールに添付される元メールのヘッダ情報から判定します。
5. 稀ですが誤判定があり得ます。運用形態によっては、偽陽性の誤判定に関してはホワイトリスト管理が肝要となります。
6. それでも擦り抜けてくる迷惑メールについては、RBLを併用してスパム判定することも可能です。

このabmailはあくまで判定結果を返すだけですので、運用形態に合った導入が必要となります。

２．+abmail — 迷惑メール対策サービスとは

迷惑メール対策サービスとして、abmailの導入支援を電子メール運用形態に併せて行うものが「+abmail」サービスです。

- 例えば、メールサーバ管理者もしくはＩＴ担当者が居り、この迷惑メール判定技術さえあれば、具体的な導入作業からすべて自前でしたい場合には、サーバ環境、クライアント運

用環境と abmail の特性に合った総合的ソリューションのご提案と abmail 及びそれに係る技術提供を行います。

- また、具体的な管理・運用は自前で、但し、既存のメールサーバへの導入作業までは委託したい場合には、上記に加えて abmail 導入作業を行います。
- また、既存のメールサーバ環境に手を加えられない、もしくは、加えたくないという場合には、メールサーバとクライアントとの間に迷惑メール対策用サーバ機が必要となるでしょう。この場合は、上記に加えて、対策用サーバ機の構築と導入を行います。

以上、個別のユーザアカウント管理について、メールサーバ管理者もしくはＩＴ担当者が行う場合には、このサービスにおいて、ユーザアカウント数に係る制限は設けません。よって、既存のユーザアカウント数に依らない費用で導入頂けます。

- 但し、サーバの処理能力に対してユーザアカウント数が多い場合には、メールサーバと迷惑メール対策に特化した処理の高効率化が推奨されます。こうした技術の導入支援についても柔軟に対応します。

一方、迷惑メール対策に伴う個別のユーザアカウント管理やサポート体制を必要とされる場合には、ユーザアカウント数に係る保守費用が掛かります。

また、メールサーバ環境にも手を加えず、対策用サーバ機も運用形態に適さないという場合には、クライアント側であるパソコンそれぞれに対策技術の導入・管理・運用が必要になります。

３．迷惑メール対策サービスの導入［サーバ編］

迷惑メールに困っている方で、迷惑メール対策の導入を検討したい方は、まず、迷惑メールの検体をひとつ添付し、その旨のメールを弊社宛にお送り下さい。そのヘッダ情報とご要望から総合的ソリューションをご提案致します。

加えて、メールサーバ管理者もしくはＩＴ担当者の方の場合は、

1. 全アカウントに対して一括して対策を施すか、それとも、個別に施すか
2. 迷惑メールと判定されたメールは削除、隔離、情報付加のどれを施すか
3. メールサーバのディスク容量、サーバ機のスペック
4. メールサーバの運用形態（POP3、IMAP4、WebMail、ネームサービス、認証方式など）

他、ご要望などをお知らせ下さい。

４．迷惑メール対策サービスの保守［サーバ編］

まず、特に運用当初において偽陽性の誤判定が少なからずあり得ることをご承知下さい。そのため、ホワイトリスト管理が必要になります。

そのホワイトリスト管理に掛かる人的コストは、アカウント数、迷惑メールと判定されたメールの取り扱い方法、メールサーバの運用形態などに依存します。それに応じた誤判定の補正処置の枠組みを整備し、迷惑メール対策を実施しつつ対外的な支障が生じないような総合的ソリューションをご提案したいと考えております。

また、迷惑メールと判定されたメールに対して、情報付加するだけであれば、多少の偽陽性の誤判定はそれほど支障が無い、という場合もあり得ると思います。というもの、例えば、一日に三十通以上もの迷惑メールを受信しているような方で、それらを削除しつつ正当なメールを見分けるといった作業を行うよりは、迷惑メールと判定されたメールが退避されるフォルダの中から、偽陽性の誤判定となってしまった正当なメールを見つけることの方が極めて容易いからです。そして、時間的にゆとりのある場合に、その誤判定の補正処置を設定に反映してもよいでしょう。

５．abmail のソースコードについて

このサービスの中核をなす迷惑メール判定プログラム「abmail」は公益性の高いものと考えられるので、そのソースコードは将来的にオープンソースとして公開する予定です。しかしそれが、利用者の利益を損なわないかを正確に見極めるために、現時点では、しばらくはスパマーの動向を見守りつつ、同時に、適切なオープンソースライセンスの選定・策定を検討して参ります。よって、当初はこの点についてのご意見ご要望も承りたいと考えております。

6．迷惑メール対策サービスの利用法［クライアント編］

メールサーバ側で迷惑メール対策を施した場合、そのやり方によってはクライアント側であるメーラ等にも設定を施す必要、もしくは、それを利用者に周知する必要があります。

例えば、迷惑メールと判定されたメールに情報付加という運用方法を採用した場合、迷惑メールであれば、メールに「`X-Abmail-Flag: Yes`」というヘッダ情報が付加されます。ちなみに、正当なメールであれば、そういったヘッダ情報は付加しません。

このヘッダ情報を利用者がどのように活用するかは利用者次第ではありますが、ひとつの方法として、利用者が使っているメーラの自動振り分け機能で「`X-Abmail-Flag: Yes`」ヘッダ情報の付いたメールを「`Abmail`」フォルダに自動的に振り分けるといった運用方法が考えられます。そして、誤判定が無いかどうか定期的にそのフォルダを確認する必要性を利用者に周知する必要があるでしょう。

一方で、クライアント側であるメーラになんら設定を施す必要がない運用方法もあります。例えば、迷惑メールと判定されたメールを隔離という運用方法を採用した場合、メーラ等にはなんら必要な設定はありません。しかしそれでも、隔離されたメールに誤判定が無いかどうかを利用者が確認する必要性だけでなく、そういったことが出来る枠組みが必要となります。そういった枠組みを用意しやすいかどうかは、メールサーバの運用形態（IMAP4、WebMail）に依ります。

7．abmail のスパムに対する基本姿勢と誤判定について

スパムは日々変容しているので、メール本文検査型の迷惑メール対策では、パターンファイル等の更新やマッチング等の学習だけでなく、新手のスパムに対する新たな判定手法を導入し続けないと、いずれ正当なメールの数をスパムが凌駕していきます。

一方で本手法は、メールヘッダにおいて偽装が明らかな箇所や詐称が行い難い箇所から迷惑メールであることを判定するので、比較的イタチごっこになり難い特徴を持っています。

詐称が行い難い箇所とは、主に IP アドレスやその逆引きであるドメイン名ですが、エンドユーザ空間であれば通常ある範囲の動的アドレスであるので、そういったアドレス空間には正当な MTA が設置されていることは稀で、むしろ、ウイルスでボットと化したパソコン、スパマーとの相関が極めて高いことが判っています。こうした点に注目して MTA コネクションで対策を施す手法が既に提案されています。エンドユーザ空間であることをドメイン名から推定して、そこからのメールを拒否応答してしまうのが S25R(Selective Port 25 Rejection)、正当な MTA か否かを判定すべく、再送要求するのが Rgrey(S25R & greylisting)、応答遅延するのが Startpit(S25R & tarpitting)、応答遅延と再送要求するのが taRgrey(tarpitting, S25R & greylisting)という対策方式です。

この S25R 派生の方式は、スパム排除に効果的であることが知られていますが、正当な MTA であることを判定するための資源を正当な MTA に託す、いささか他者に迷惑な方式であることが問題視されています。その意味でも、ホワイトリストの管理を適切に行っていく必要がありますが、さしせまった必要性が生じ難いことから、管理側のその動機付けが低くなりがちで、それによる弊害も報告されています。また、正当な MTA と同等な応答の実装を、もしスパマーが実現した暁には破綻してしまうことは明らかで、現にそういったウイルスが出現しています。こうした敵に気

付かれる手法では、スパマーに次の手を考える余地をすぐさま与えてしまうので、有効性の寿命は短いと言わざるを得ません。

一方、本手法はそういったスパムと相関の高いエンドユーザ空間からのメールであっても、正当なメールと同様に受信します。設定によってはそのまま棄ててしまうことも可能ですが、スパムである可能性が極めて高いメールを振り分けてしまうという方式を採っていますので、スパマーは徐々に収益が低下していくことしか知り得ないでしょう。

その代わり、本手法はスパムと判定されたメールが蓄積されるフォルダに偽陽性の誤判定、つまり正当なメールが無いか確認する必要があります。しかし、スパムが集まるメール一覧から正当なメールを見出すのは意外にも容易いことに気付かれるはずです。そして、これは当人に合った頻度で行えばよいことであり、誤判定を設定にフィードバックすれば、その後の精度が向上します。

併せて、スパムと判定されたメールが蓄積されるストレージ容量と、誤判定の確認頻度との兼ね合いで、定期的に古いメールから自動的に消去するのもひとつの方法です。

その他にも S25R 系の方式には、逆引き不能の正当な MTA に関する問題や、偽のバウンスメールには効力がないという問題があります。その点本手法は、逆引き不能な MTA に関する誤判定を救済する機構も用意できますし、偽のバウンスメールを迷惑メール判定する機能が備わっています

つまり、偽陽性の誤判定は稀にも起こりうるものですから、メールサーバに導入したとしても迷惑メールを大して受信しておらず、特に困っていないユーザのアカウントについては、メールサーバレベルでの自動振り分け等の機能を無効にしておくことをお奨めします。その場合、メールサーバでは判定結果の情報付加のみを行い、対策が必要なユーザが使うメーラで適宜、その付加情報を利用したメールフォルダでの自動振り分け、といった運用方法が考えられます。

8．abmailsreport による隔離メール報告と再送について

スパムと判定されたメールを隔離する場合、同梱される abmailsreport の運用により、利用者に隔離メール一覧をメールで報告することが可能です。加えて、この隔離メール報告に対して利用者が、メールで所望の隔離メールの再送を要求することにより、稀に起こるかもしれない偽陽性の誤判定メールを救済することが IMAP4 や WebMail なしで可能となります。

9．導入費用

メールサーバ管理者が居り、迷惑メール判定プログラムのソースコードとそれに係る技術情報があれば十分である、といった方には以下の費用でご活用頂けます。

- 単一の MTA 向け
  - メールサーバ管理技術者優待価格　　￥500,000（税抜き）
  - 同上、教育研究機関向け価格　　￥200,000（税抜き）
- 複数の MTA 向け（組織内においては無制限）
  - メールサーバ管理技術者優待価格　￥1,750,000（税抜き）
  - 同上、教育研究機関向け価格　　￥700,000（税抜き）

その他の導入作業、運用管理に係る費用については別途お見積もり致します。

【お問い合わせ先】

〒273-0012 千葉県船橋市浜町 2-16-8

株式会社あいはら 研究開発チーム

E-Mail: rdteam@aihara.co.jp

TEL: 047-437-1151 FAX: 047-437-1160