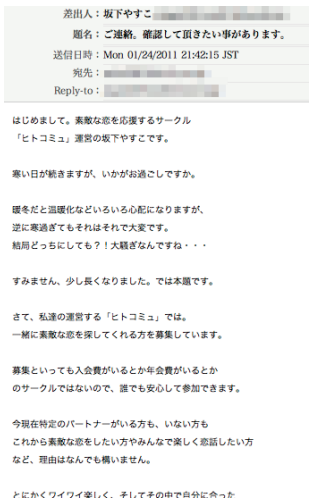
スパム対策システムについて

総合情報基盤センター杉谷キャンパス　業務主任　笹野　一洋

１．スパムとは

スパムとは，米国の Hormel Foods 社が製造する肉の缶詰（ランチョンミート）の一種である。もともと Spiced Ham という商品名であったが，後日 SPAM と改名した。日本では，沖縄県においてよく食されているとのことであり，チャンプルーなどには欠かせない材料となっている。

一方，**スパム（メール）**とは，「宣伝や詐欺などを目的として，受信者の同意無く一方的に送りつけられるメール」，つまり一言で言えば「迷惑メール」のことである。多くは，医薬品（特に，性機能改善剤），低金利融資，海賊版ソフトなどの広告や，出会い系サイトなどへの勧誘を目的としたものであるが，最近では，コンピューターウイルスに直接的／間接的に感染させることを目的としたものも多くなっている。



このような迷惑メールがスパムと呼ばれるようになった理由には諸説紛々あるが，もともとスパムがあまり上品な食品ではないと認識されていたことに加え，英国 BBC の番組「モンティーパイソン」において放映された『大勢の海賊がレストランに押しかけ，全員が SPAM を注文し，Spam! Spam! Spam!と叫んで大騒ぎする』という迷惑行為を描いたコントがその命名の根源であるという説が有力である。

迷惑メールそれ自体は，スパムという名前で呼ばれる以前から存在していたのではあるが，10 年ほど前から無視できないほど大量に発信されるようになってきた。最近の調査では，全世界のメールの総数のうち７～８割以上がスパムメールであるという報告もある。さらに最近では，掲示版に執拗に書き散らされる記事や，ブログのコメントやトラックバックを利用した迷惑メッセージ，チャットやインスタントメッセージを利用した迷惑行為など，より広い意味にもスパムという言葉が用いられるようになってきている。

今後，本稿では，数多あるスパムの中でも，スパムメールに限定して論を進めることにする。

２．スパムメールを受け取った場合の対処

不幸にしてスパムメールを受け取ってしまった場合には，迂闊に開かないことが肝要である。（開いただけでウイルスに感染してしまったり，開いたことが相手に伝わってしまう場合もある。）また，受け取ったメールを徹底して無視することが大切である。

もしも記載されているリンクをクリックしたり，返事を出したり，あるいはスパムメールを送り付けてきたことに憤慨して抗議のメールを送ったりしただけでも，そのメールアドレスが実際に使われている（生きている）アドレスであることが相手に伝わってしまい，そのメールアドレスがブラックマーケットにおいてスパム業者間で売買され，

その結果さらに多くのスパム業者からスパムが届くということになってしまう。

よって，非常に受動的な方法ではあるが，**開かずに徹底的に無視する**こと以外に対処の方法はない。

３．スパムメールの防止策

幸福にもまだ一通もスパムメールを受け取ったことがないという人であれば，そのメールアドレスはまだブラックマーケットに流通していないと思われるため，次のようにしてメールアドレスの漏洩の防止に努めるべきである。

先ずは，メールアドレスを公開の場（ホームページや掲示版など）に公表しないことである。やむを得ず公表せざるを得ない場合にも，例えば，somebody@fff.u-toyama.ac.jp と記述するのではなく， somebody (at) fff (dot) u-toyama (dot) ac (dot) jp のような記述にしたり，あるいは文字を画像に変換して貼り付けたりして，機械的にメールアドレスだと判断できないような形にしておくことが大切である。このような配慮により，クローラー（web page に網羅的にアクセスしてメールアドレスとみられる文字列などを漁っていくようなプログラム）によって自分のアドレスが機械的に収集されてしまうことを避けることができる。

また，メールアドレスを信頼できない他人に教えないようにすることも重要である。特に，懸賞への応募やアンケートへの回答に迂闊にメールアドレスを書き込まないように十分に注意する必要がある。最近では多くの企業が効率的な広告手段としてメールアドレスを知りたがるが，メールアドレスを教えることによるメリット／デメリットと安全性についてよく考えた上で行動して頂きたい。

ただし，上記のような典型的なスパムメールを１通でも受け取ったことがある人であれば，そのメールアドレスは既に流出していると考えた方が良いであろう。その場合には，次のように，コンピューターによって迷惑メールをフィルターするという方策をとることにより，被害を少なくすることが可能である。

４．コンピューターによるスパムメールの防止策

一度スパムメールが届き始めると，その数は次第に増えていき，やがては一日に百通を超えるような事態になってしまうことも珍しくない。そうなってしまうと，人の眼によってすべてのメールをチェックすることは難しくなり，必然的にコンピューターによって自動的にスパムメールをフィルターすることが必要となってくる。

コンピューターによるフィルタリングには大きく分けて２つの方法がある。

一つは，メーラーのフィルタリング機能の利用である。Thunderbird や Apple Mail などのまともなメーラーが備えているフィルタリング機能はかなり高機能であり，よく訓練すればかなりの正確度でスパムメールをフィルターしてくれる。しかしこの方法は，あくまでもメールが端末に届いてから処理する方法であり，膨大な数のメールがメールサーバーから端末へと流入するという問題点を回避できない。

そこでもう一つの方法，つまり，メールがメールサーバーに届く前にフィルタリングしてしまうという方法が有用となる。この処理をするのが，表題にあげたスパム対策システムである。

これからスパム対策システムについて解説していくが，その前に，メーラー／スパム対策システムを問わず，フィルタリング機能が必然的に持つ問題点と，それを使用する際に気をつけておきたい注意点について解説しておきたい。

５．フィルタリング機能の問題点・注意点

そもそも特定のメールがスパムであるか否かという判断は，メールの受信者の主観的な基準によってなされるものである。極端な例をあげると，スパムメールの動向を調査している研究者にとっては，スパムメールは貴重な研究材料であり，決して迷惑なものではない。このような極端な例は別にしても，一般的に言って，メールの受信者の主観的な判断基準をコンピューターが的確に忖度して正確なフィルタリングをしてくれることを期待すること自体が間違っていると言えよう。よって，フィルタリングには必然的に何らかエラーが生ずることを前提として利用するべきである。

フィルタリングのエラーは次の２種類に分類することができる。一つは「スパムメールをスパムでないと判断してしまうエラー（偽陰性）」であり，もう一つは「スパムでないメールをスパムだと判断してしまうエラー（偽陽性）」である。

このうち前者のエラーは実は大きな問題ではない。たとえスパムがフィルターをすり抜けたとしても，最終的には「受信者の眼」というフィルターによって選別されるからである。

一方，後者のエラーは極めて大きな問題を引き起こす。重要なメールがフィルターによってブロックされてしまい，受信者に届かないという危険性があるからである。

よって，フィルタリング機能を利用する場合には，後者のエラーが起こった場合に備えて，細心の注意を払う必要がある。具体的には，フィルタリング機能によってスパムと判断されたメールを直ちに削除するのではなく，一時的に隔離しておき，後刻，隔離されたメールの中に重要なメールが含まれていないかを送信者や件名などから判断し，削除あるいは配送をするという行動をとる必要がある。

ユーザー各位には，このような特性を十分に理解した上でフィルタリング機能を利用して頂きたい。

６．スパム対策システム Barracuda

杉谷キャンパスでは，旧・医薬大の頃から，Barracuda networks 社の Barracuda Spam & Virus Firewall（以下，Barracuda と言う）というスパム対策システムを導入して運用してきた。今回の新システムにおいては，Barracuda を全教職員（正確には，ems 以外のメールサーバのユーザー）が使用できるように，より処理能力の高い機種へと更新した。

Barracuda によるスパムメールのフィルタリングは以下のように行われる：

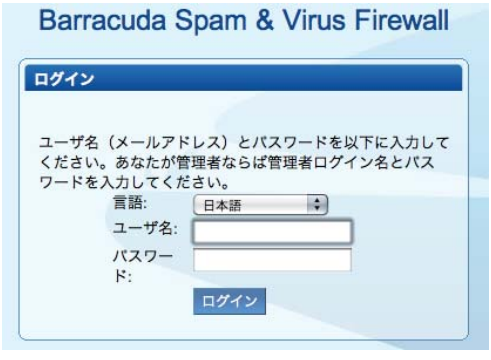
Step 1. 一般に公開されているブラックリストおよび Barracuda 社独自のブラックリストに登録された IP address からのメールを拒否する。
Step 2. それ以外のメールについて，種々のルールに基づいて，スパムであるか否かを評価し，点数化（0 点～10 点）する。
Step 3. その点数に基づいて，各ユーザーが設定した基準に応じて，以下のいずれかを行う：
  a. スパムではないと判断し，ユーザーに配送する。
  b. 件名に「Spam」のようなタグを付けてユーザーに配送する。
  c. メールを隔離する。
  d. メールを拒否する。
Step 4. メールを隔離した場合，適当な間隔（各ユーザが設定可能）で，各ユーザに隔離通知をメールする。
Step 5. 隔離通知を受け取った各ユーザーは，送信者や件名などに基づいて，そのメールの取り扱い（配送／削除など）を決定する。

以下，具体的な画面を示しつつ，Barracuda の機能について説明していくことにする。なお，画面は一部旧 Barracuda のものを使用しているが，新 Barracuda でも大きな違いはない。

Barracuda の設定

最初に，上記 Step 3. で使用する基準値の設定を行う。（設定を行わない場合，センターがあらかじめ全ユーザーに対して行った初期設定に基づいて動作する。）

先ず，`https://spamfw.u-toyama.ac.jp` にアクセスして，Barracuda にログインする。



ログイン時に使用するユーザー名はメールアドレス（u-toyama.ac.jp まで入力），パスワードはメールを利用する時に使うパスワードと同じである。

ログイン後表示される画面で，「プリファレン

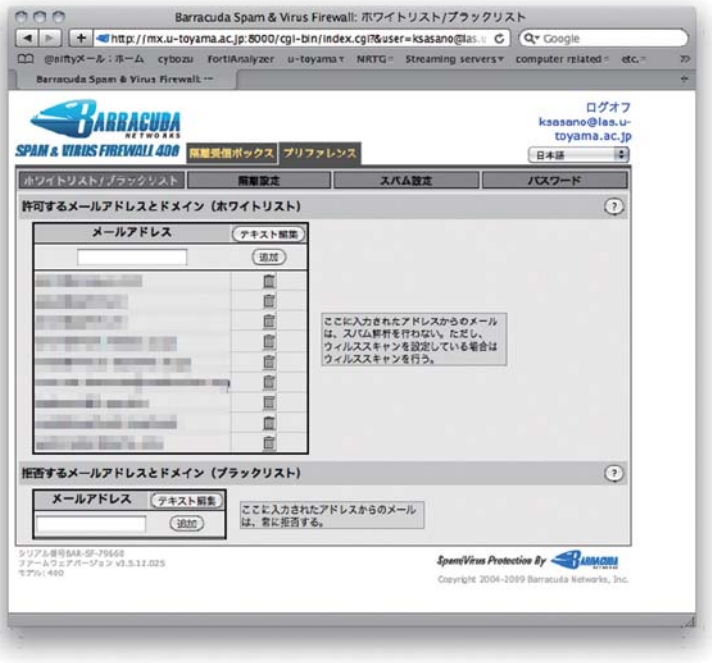
ス」タブをクリックし，さらに「スパム設定」タブをクリックすると，左上のような画面になる。

この画面において，スパムフィルタリングを有効にするか否かや，タグ付け／隔離／拒否の基準となる点数を設定する。基準点を低く設定しておけば，ほんの少しだけ怪しいと判断されたメールでも引っかかることになる。また，高く設定すれば，かなり確実にスパムであろうと判断されたメールのみを引っかけることになる。「システムデフォルトを使用する」を「いいえ」にし，「タグ」の点数は低めに，また「隔離」の点数はかなり高く設定しておくことを推奨する。なお，「拒否」してしまうと，隔離もせずに完全に削除されてしまうので，「拒否」はしないように設定しておくのが良いであろう。

なお，初期設定（システムデフォルト）は，3.5 点以上でタグ付けを行い，隔離と拒否はしないようになっているので，この設定のままで良いと思うユーザーは特に設定する必要はない。

次に「隔離設定」タブをクリックすると，右下のような画面になる。この画面において，「隔離有効」を「はい」にすることにより，メールの隔離が行われるようになる。「いいえ」にすると，隔離は行わず当該メールの件名に「QUARANTINE」というタグを付けたメールがユーザーに配送される。

メールが隔離された場合，上記 Step 4. で述べたように，隔離されたメールがあることを通知するメールが Barracuda から各ユーザー宛に送られるが，その間隔を毎日一度にするのか毎週一度にするの



か，あるいは通知しないのかを「通知間隔」で設定する。ここは「毎日」を選択しておくことを推奨する。さらに，隔離通知メールを対象となっているメールアドレス以外のアドレスに送るようにも指定できるが，特に理由がない限り何も指定する必要はないであろう。

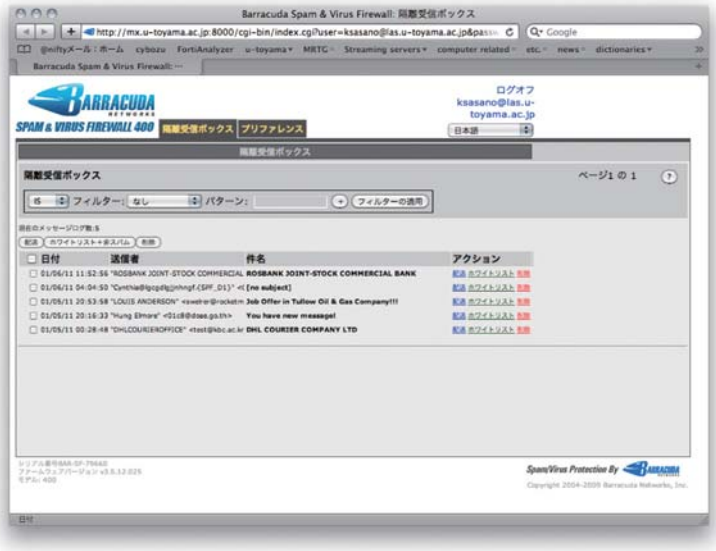
さらに「ホワイトリスト／ブラックリスト」タブをクリックして表示される画面（左上）において，ホワイトリスト（このリストに登録されたメールアドレスから届いたメールは，スパム解析を行わず，常に配送される）やブラックリスト（常に拒否するメールアドレスのリスト）を指定できる。例えば，会議の開催通知や学会からの連絡のように多くのアドレスに同時に送られるメールや，Bcc で送られてくるメールなどはスパムだと誤認されてしまう可能性が高くなるので，そのようなメールを送ってくる送信者のメールアドレスをホワイトリストに登録しておくことを推奨する。なお，スパムメールの送信メールアドレスは常に変化し続けているので，ブラックリストを積極的に使用することは少ないと思われる。

Barracuda からの隔離通知メール

上記 Step 4. で述べたように，メールが隔離された場合，一定の期間ごとに，右下のような隔離通知メールが Barracuda から送られてくる。

そこにリストされたメールが，隔離されているメールである。送信者名や件名からスパムであるか否かの判断が可能な場合には，「アクション」欄の「配送／ホワイトリスト／削除」をクリックすることによって，個々のメールをそれぞれ「配送する／送信者をホワイトリストに登録する／削除する」ことができる。

もしもリストされているメールの数が多く，一括して処理したいような場合には，右下に表示されている「ここをクリック」をクリックすると，ブラウザが起動して自動的に Barracuda にログインし，「隔離受信ボックス」が表示される（次頁左上）。この画面において，該当するすべてのメールの左のボックスをチェックしてから，「配送」，「ホワイトリスト＋非スパム」，「削除」



ボタンをクリックすることにより，チェックしたメールを一括して処理することができる。なお，「日付」欄の左のボックスをチェックすれば，すべてのメールがチェックされる。

７．杉谷キャンパスにおけるスパムメールの状況

最後に，実際にどのくらいの量のスパムメールが送られてきているかを示す。下のグラフは，2010 年 12 月から 2011 年 1 月にかけて杉谷キャンパスに送られてきたメールの総数とその内訳を日毎に示したものである。これをみれば，日によっては全メールのうち半数以上がスパムであると判断されていることがわかるであろう。全体でこの比率であるということから，ユーザーによっては，受け取ったメールのほとんどがスパムであるという状況が起こっているであろうことが容易に推測される。このようなユーザーにとっては，Barracuda は非常に有用なシステムであると言えるであろう。

８．結語

以上述べてきたように，Barracuda は非常に有用なシステムであると言えよう。そして新システムにおいてはそれを全教職員が利用できるようになった訳である。ユーザー各位が，上述のように「偽陽性」メールに十分注意しつつ，Barracuda を活用して頂ければ幸いである。