タダで手に入る強力ソフトウェア登場

最終兵器 POPFileで スパムメールをやっつけろ

illust.: 関根まさみち

毎日、英語、中国語、韓国語など、さまざまな国からさまざまな言語でスパムメールがどんどん押し寄せる。頼みもしていないのに自動的に送られてくるこの迷惑なメールは、必要なメールを埋もれさせるほどの量に達してきた。これまで、メールソフトのフィルター機能を使ってゴミ箱に振り分ける設定作業にどれほどの時間を費やしてきただろうか。今後もそれが続くかと思うとうんざりさせられる。そんなある日、POPFileに出会った。管理画面からユーザーが教えていくにつれて、みるみる学習して分類効率を上げるという。導入して3日もたたないうちに、まるで浄水器をとりつけたようにスパムメールがゴミ箱に放り込まれるようになる！

筆者紹介

岡田良太郎（おかだ・りょうたろう）riotaro@techstyle.jp
株式会社テックスタイルにて、情報セキュリティーやオープンソース技術に関するリサーチ・コンサルティングに従事。「blog」での検索結果の上位を占める「Okdt BLOG」では、本業のかたわら執筆する日常のコラムの中にPOPFileの解説を掲載し、POPFile日本語化ページなどからも参照されている。

URL http://okdt.org/blog/

POPFile関連情報はここでゲット！
URL http://popfile.sourceforge.net/
URL http://popfile.sourceforge.jp/

準備編

インストーラーの入手とインストールから始めよう

ウィンドウズだったら簡単インストール

POPFileのソフトウェア本体、ウィンドウズ用バイナリー、ならびにドキュメントは公式サイトで公開されている(日本語ページあり)。POPFileはPerl5で記述されているため、インストール時に最小バージョンのPerlもインストールされる。

すべてのコンポーネントをインストールしても、必要なディスクスペースは11MB強となる。実際の稼働では、メールの分類に必要なコーパス(corpus)という単語データベースが蓄積されていくため、もう少し余裕が必要だ。20MBもあれば十分だろう。

インストール終了後に、ブラウザーでPOPFileの設定インターフェイス「POPFileコントロールセンター」が表示されればひとまずインストールは一段落だ。

01

POPFileの入手先(POPFile Download Page)

URL http://sourceforge.net/project/showfiles.php?group_id=63137

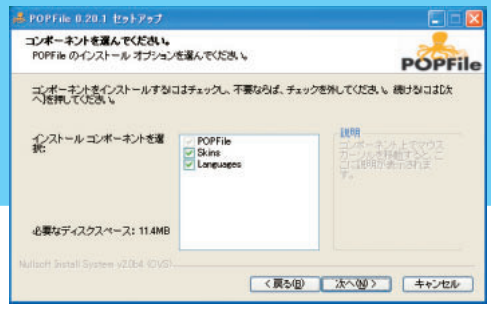
ここからPOPFileの最新版のウィンドウズ用バイナリー「popfile-0.20.1a-windows.zip」(執筆時点)をダウンロードする。

02

*01*でダウンロードしたファイルを解凍するとsetup.exeファイルができるのでこれを起動する。インストールの最初のポップアップ画面で「Japanese」を選択すると、その後の手順が日本語で表示される。

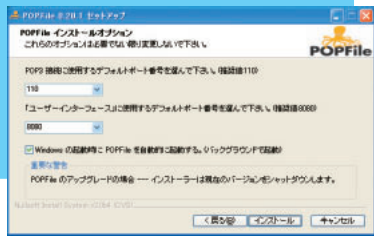
03

インストーラーに従って「次へ」ボタンを押しながらインストールを進める。インストールコンポーネントの全サイズは11MB強。すべてインストールしておこう。

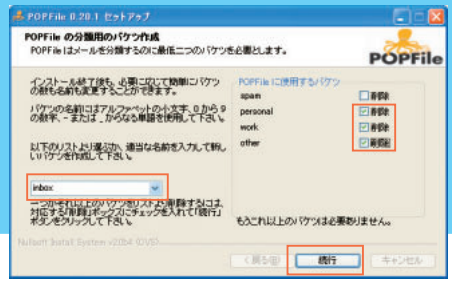


04

使用するポート番号の選択などが表示されるが、インストールオプションは必要がない限り変更しない。「ウィンドウズの起動時に自動的に起動する」は選択しておく。

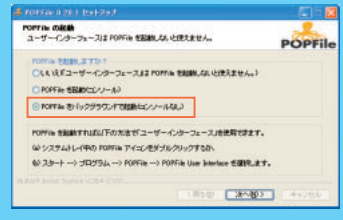


05



この画面では、当初用意されているバケツの「personal」「work」「other」の「削除」にチェックを入れ、左下のプルダウンメニューから「inbox」を選んで、「続行」ボタンを押す(バケツについては次ページ参照)。すると新たなウィンドウが現れるので「はい」を押す。

06



次に「POPFileをバックグラウンドで起動(コンソールなし)」を選び「次へ」を押す。あとは画面にしたがって進めばインストールは完了だ。

注意

POPFile 0.20シリーズがリリースされた時点では、それ以前のバージョンに必要だった日本語用の特別なパッチは必要ないとアナウンスされていた。しかし、昨年11月、日本語の処理に不具合が発見されたため、0.20.0ないしは0.20.1(執筆時点の最新版)を利用している場合には、1つのファイル(インストールしたディレクトリーのClassifier/Bayes.pm)を差し替える必要があることが知らされた。この差し替えファイルは日本語化パッチ0.20.1.1としてPOPFile日本語化サイトから入手できる。なお、この問題は近いうちにリリースされる次バージョン(0.20.2)で修正される予定とのことだ。

◎POPFile日本語化サイト

URL http://popfile.sourceforge.jp/

［基礎知識編］

プロキシーとして機能するからどんなメールソフトにも対応

メールの中身を見てヘッダーに付加情報をつけるのがポイント

次に分類用の「バケツ」を用意しなければならない。基本的に、POPFileは自動でメールをスキャンして分類するツールだということを覚えておいてほしい。ひとたびセットアップして訓練すると、やってきたすべてのメールをスキャンし、そして各バケツに分類するのだ。

まず、ユーザーが必要なメールとそうでないものを分類してみせることにより、POPFileはその各々のメールの特徴を分析する。そうして推定したルールに基づき、新たに取得するメールを次々に分類していく。それは、あたかも釣ってきた魚を種類ごとにバケツに分類する様子に例えられる。それで、分類先を「バケツ」と呼んでいるのだ。

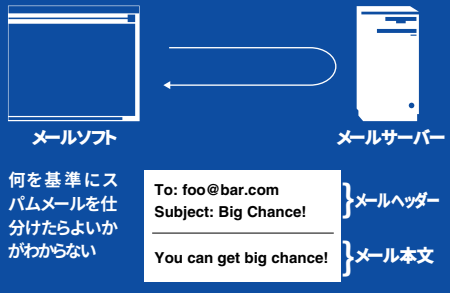
通常、Outlook Expressを代表とするメールソフトは、POP3プロトコルでメールサーバーにアクセスしてメールを取得する。POPFileはその間に入り、プロキシー（代理）サーバーとして動作する。メールソフトからリクエストを受けると、POPFile はメールソフトの代理でメールサーバーに接続する。

POPFileはメールをスキャンして分類先のバケツを判断すると、それを次のいずれかの方法で識別できるようにメールそのものに記録する。

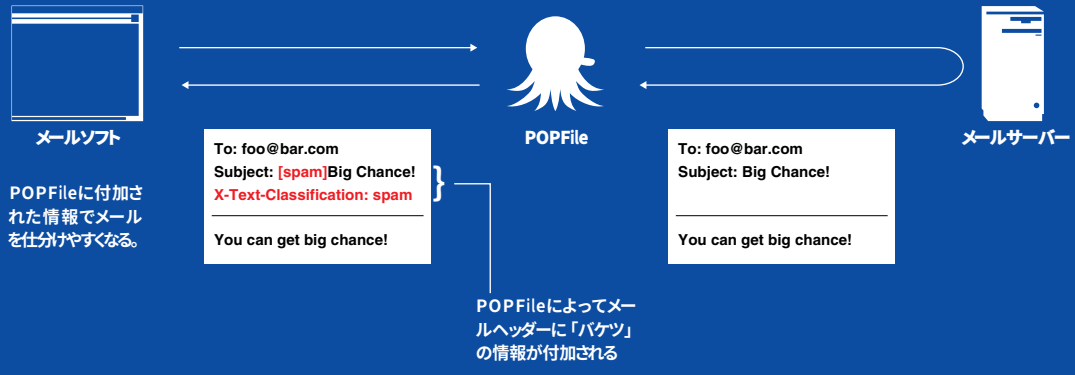
1つはメールのサブジェクト（件名）に「[spam]」のようにバケツ名を挿入する方法だ。これは、Outlook Expressのフィルター機能でメールを振り分けるのに使える。もう1つは、「X-Text-Classification: spam」のように拡張ヘッダーとしてバケツ名を追加する方法だ。これはヘッダーを自由に参照してフィルタリングできるメールソフトにとってありがたい。

どちらの方法を用いるかは、POPFile UIの「設定」メニューで指定できる（2つを同時に用いることもできる）。

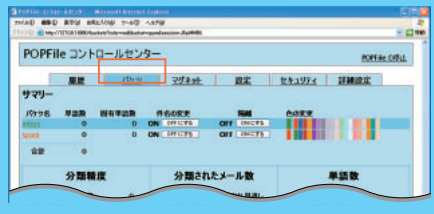
●通常のメールの受信（POP）



●POPFileを使ったメールの受信



01



バケツの状態はPOPFileコントロールセンターで確認できる。まず、上の画面のようにシステムトレイにあるPOPFileのアイコンをクリックして「POPFile UI」を選ぶ。ブラウザーが立ち上がりPOPFileコントロールセンターが表示されるので、「バケツ」をクリックすると、バケツの状態が表示される。画面のように前ページで用意した「inbox」「spam」の2つのバケツがあることがわかる。

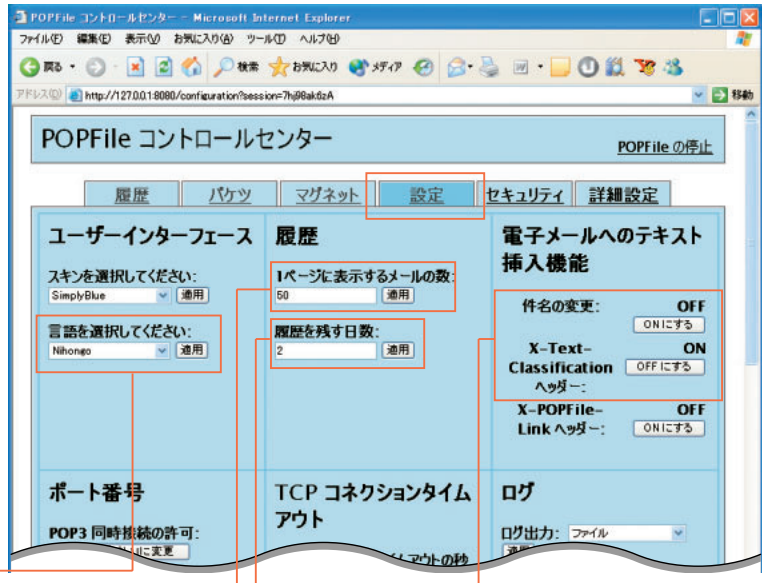
［設定編①］

POPFileに必要な設定はたったこれだけで簡単

件名の変更かそれとも拡張ヘッダーを使うかがポイント

今回はバケツはspamとinboxの2つを用意したが、必要であればもっと増やせる。しかし、バケツの数だけ後述するPOPFileのトレーニングの時間が長くかかる。また、バケツへの分類ルールが不明確だと、POPFileの精度に影響するので2つのバケツで十分だろう。

さて、ここで、POPFileがバケツの分類をどうやって表現するかを設定しよう。それには2つの方法があることは述べたが、1つ注意したい点がある。それは、件名に「[バケツ名]」という文字を追加する方法を選択した場合だ。このとき件名に[spam]と挿入されたメールに返信しなければならない場合に、うっかり[spam]という文字を消さずに返信してしまうかもしれない。そのメールを受け取った人は決して快く思わないだろう。したがって件名の変更機能を利用するかどうかは慎重に判断すること。



01

ユーザーインターフェイスの言語は「Nihongo」か「Japanese」を選択。「履歴」画面の表示にも影響するので、英語が好みでも、日本語メールを扱う以上は日本語表示を使うように。

02

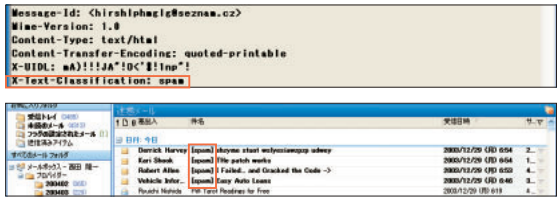
履歴メニューで1ページに表示するメールの数を50にする。一覧にざっと出るため、十分多いほうが扱いやすい。

03

履歴を残す日数については、ユーザーが受け取るメールの数によるが、あまり多くの日数を残していても役に立たない。分類ミスをチェックする無理のない量が確保されていれば十分だ。

04

Becky!やOutlookなど拡張ヘッダーの項目をメールの振り分けに使えるソフトの場合は、「X-Text-Classification ヘッダー」だけを「ON」にする。Outlook Expressのような複雑な振り分け機能がないソフトの場合は、「件名の変更」を「ON」にする。実際には下の画面のように表示される。



05

「設定」メニューで件名の変更をONにしている場合に限り、「バケツ」メニューでは件名の変更をバケツごとに無効にできる。この例では、スパムではないメールに[inbox]とは挿入せず、スパムメールと分類したものだけに[spam]と挿入する設定を示している。

［設定編②］

メールソフトを設定してスパムを振り分けよう

受信設定は簡単だが振り分けにはちょっと高度な設定が必要

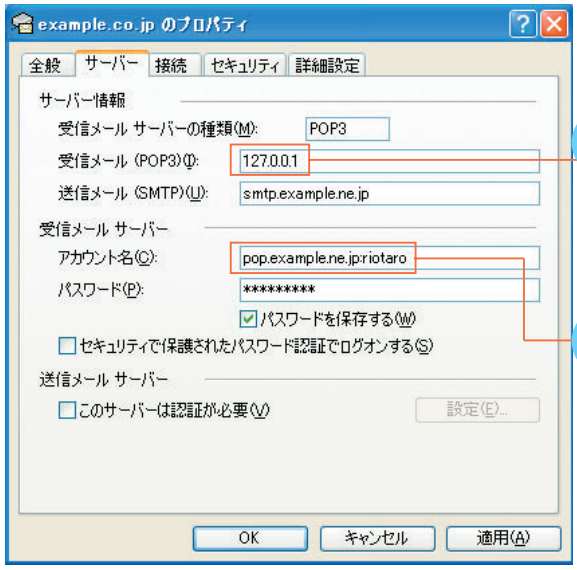
次に、メールソフトとPOPFileを連携させることにしよう。メールソフトの設定変更はそれほど難しくない。変更箇所はメールを受信するための設定の部分のみで、わずか二箇所だ。念のため、元の設定は必ず控えておくこと。まず、現在設定しているPOP3サーバー名を控えておき、そこを「127.0.0.1」に変更する。次に、POP3ユーザー名を「控えておいたPOP3サーバードレス:ユーザー名」に変更する。送信メール用のSMTPサーバーやパスワードの項目はそのままでいい。

読者はPOPFile自身にメールサーバーに関する一切の設定をしないことを意外に思うかもしれない。しかし、これにより、POPFileは複数のメールサーバーとの通信を同時に扱うことができ、複数のメールアドレスを持つゆえに複数のメールサーバーにアクセスする必要のあるユーザーに対応できるようになっているのだ。

こうしてメールソフトを設定すると、さっそくメールを受信して、POPFileを経由しても同じようにメールを取得できることを確認してみるように。この時点でメールの特別な仕分けは発生しないが、受信は可能となっているはずだ。

実際に受信できることが確認できたら、メールのフィルターも設定しておこう。前ページで設定したとおり、POPFileはメールを分類した結果、そのバケツ名を件名あるいはX-Text-Classificationヘッダーに記載する。あとは、メールプログラムでメールを受け取った際に、適切なフォルダーに仕分けするように設定するだけだ。スパムメールを「ごみ箱」に自動で振り分けられるようにする設定が1つの設定で完了するのは感涙モノだろう。

■メールアカウントの設定［例 Outlook Express］



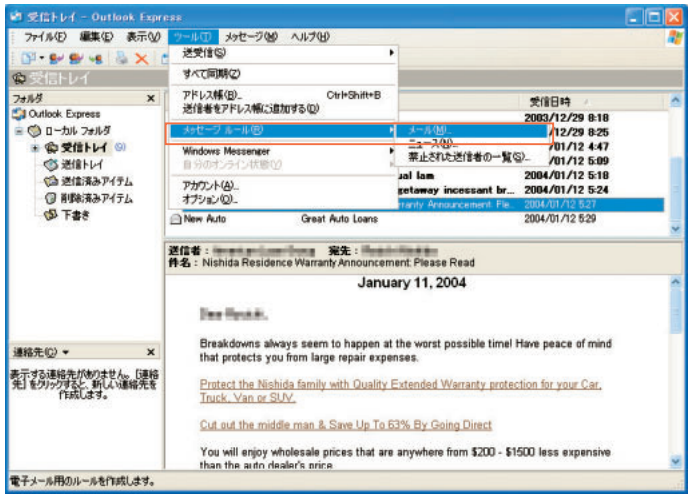
01 受信メール（POP3）サーバーの欄はいずれのメールソフトでもこのように127.0.0.1と記入する。

02 ユーザーアカウント名の部分では、［POPサーバー名］:［ユーザー名］とする。スペースなどが間に入らないように。

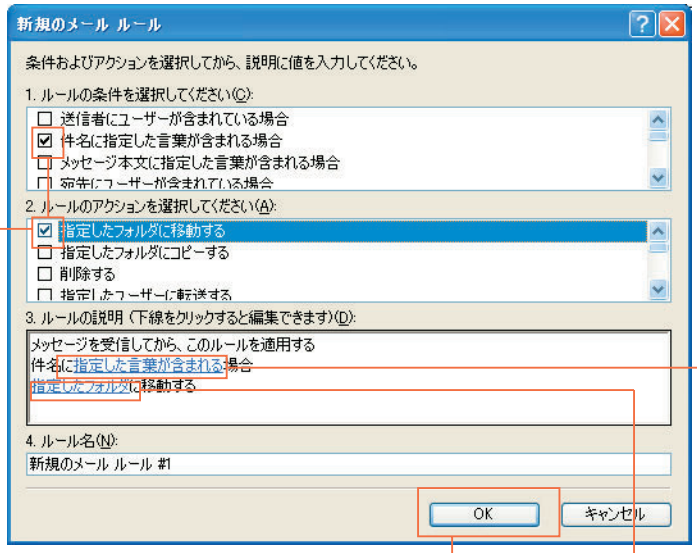
表　メールソフト設定変更例

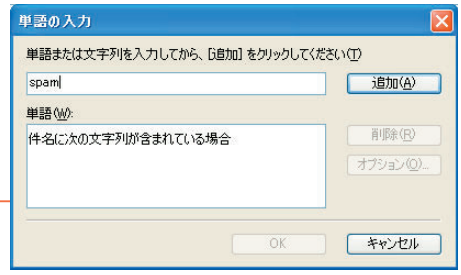
メールソフト設定項目	変更前	変更後
受信用POPサーバー	mail.example.ne.jp	127.0.0.1
ユーザーカウント名	riotaro	mail.example.ne.jp:riotaro
送信用SMTPサーバー	変更しない	
パスワード	変更しない	

■メールソフトのフィルター設定［Outlook Express編］



01 現状のOutlook Expressでは拡張ヘッダーをメールの仕分けの項目として扱えないが、POPFileの設定で「件名の変更機能」をオンにしておけば、件名を使ってメールを仕分けられる。仕分けの設定は、ツールメニューから「メッセージルール」を選び、「メール」を選ぶ。





02

「spam」を判定用の言葉として設定し、件名に「spam」を含むメールを別のフォルダに移動するために、「件名にした言葉が含まれる場合」「指定したフォルダに移動する」を選択する。

03

「指定した言葉」にはバケツで設定した「spam」を入力する。厳密にはバケツで分類されたメールの件名には「[spam]」と入力されるので、より正確さを求めるならばカッコ([ ])が付いたまま設定したほうがいい。

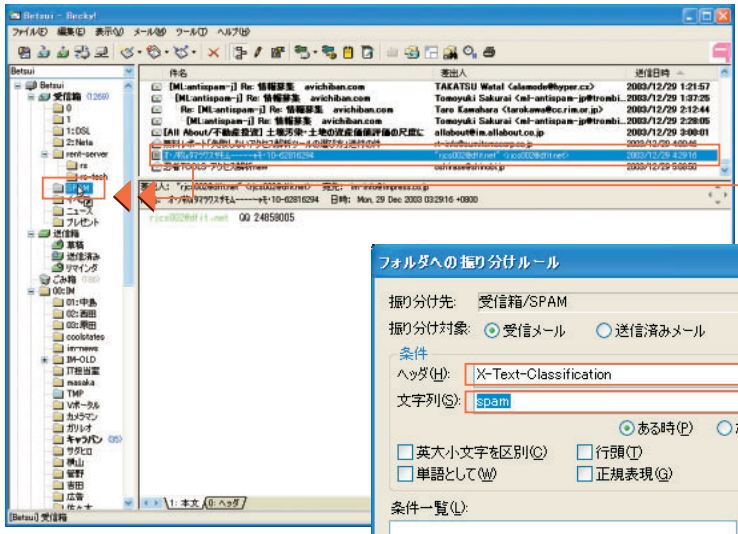
04

スパムとして仕分けされたメールは「spam」に移動するように設定する。「spam」フォルダーの代わりに「削除済みアイテム」フォルダーを指定してもいい。

05

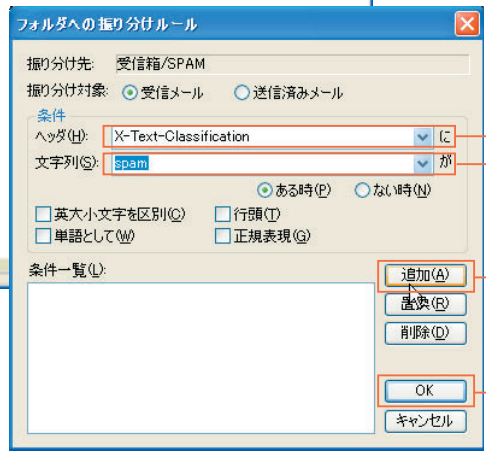
最後にこのOKボタンを押せば完了だ。

■メールソフトのフィルター設定[Becky!編]



01

Becky!やOutlook、Datulaのようなソフトはメールの特定のヘッダーをフィルターの項目に使用できるため、「X-Text-Classification:」ヘッダーで仕分けを設定できる。Beky!の場合、仕分けを設定するのは簡単で、仕分けのルールを適用したいメールを画面のように選択し、ALTキーを押しながら、仕分け先のフォルダーに移動する。



02

すると画面のようなウィンドウがあらわれるので、「ヘッダ」から「X-Text-Classification」を選ぶ。

03

文字列に「spam」と入力する。

04

「追加」ボタンを押し、最後に「OK」を押せば完了だ。これで「X-text-Classfication:spam」というヘッダーを持つ(つまり、spamのバケツに分類された)メールが目的のフォルダーに仕分けされる。

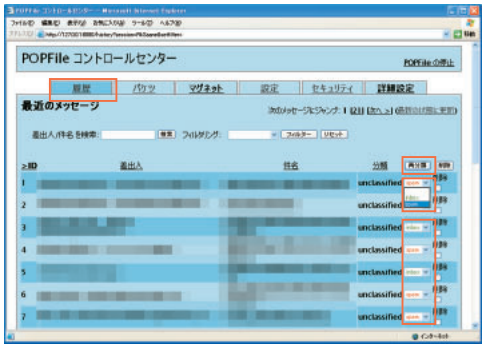
［活用編］

鍛えることで自分好みのフィルターにしよう

どのメールがスパムなのかを教えることが大事！

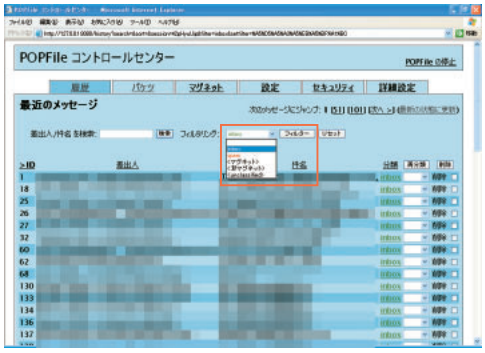
最初のメールの受信が成功し、フィルターを設定したところで、POPFile UIの「履歴」メニューを見てほしい。分類が<unclassified>となっているだろう。これは、POPFileに分類するだけの情報を持ち合わせていないため、トレーニングが必要であることを意味している。そこで、メール1通1通に対し、分類すべきバケツを指定して「再分類」することで、受信したメールがスパムか否かをPOPFileに教えていくのだ。

最初は、メールを受信するたびに「履歴」メニューで教えていく。スパムメールも多様化しているので、繰り返し教えてやる必要があるが、一貫性のある分類をしていけば、早い段階で高い精度でメールが分類されるのを実感できる。そのうち、鬱陶しく感じたスパムメールが、POPFileを育てるためのエサになっているのに気がつくだろう。



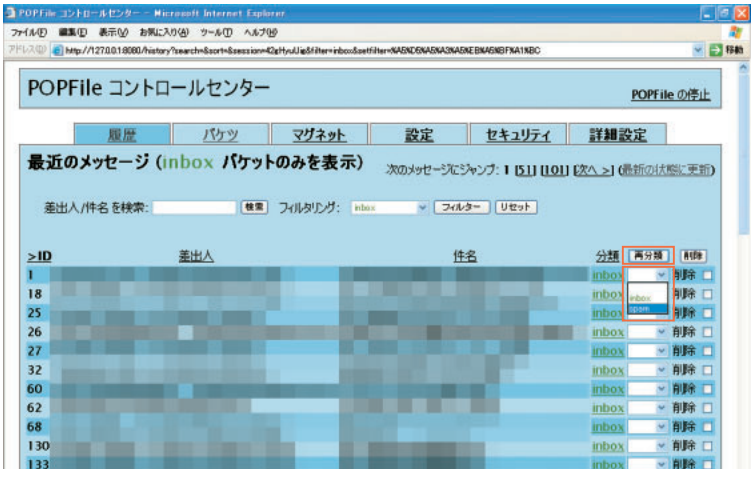
01

まず「履歴」メニューを開くと分類が「<unclassified>」となっているので、「inbox」に分類したいものを「inbox」にし、「spam」に分類したいものを「spam」にして「再分類」を押す。これで最初は様子を見よう。



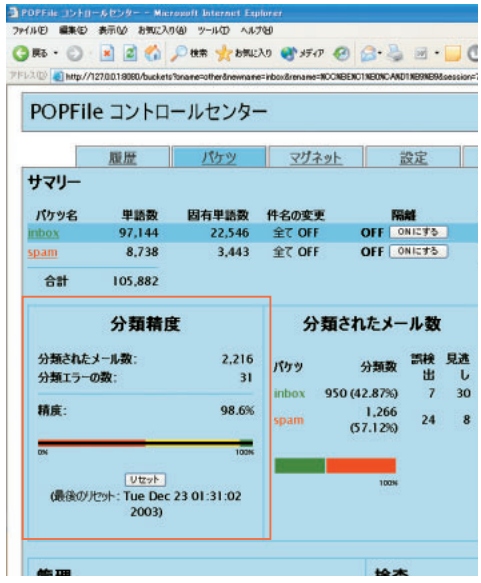
02

POPFileを使い続けながら、POPFileを鍛えなければならない。そこで、間違ったメールを再分類していく。「履歴」メニューでは、バケツごとにフィルタリングする機能があるので、画面のように「inbox」を選んで「フィルター」を押して、受信したメールをinboxでフィルタリングする。



03

02でフィルタリングしたinboxのメールの中から「spam」に分類してほしかったメールを見つけ、「spam」にして「再分類」を押す。これにより、POPFileはすでに知っているルールを変更し、さらに厳密に学習する。



04

今度は02と同様に「spam」でフィルタリングして、03と同様に「spam」の中から「inbox」に分類してほしかったメールを再分類する。また、時折、<unclassified>でフィルタリングをして、同様の作業を行う。これを繰り返すことで、POPFileの精度が高まっていくのだ。

05

POPFileを使い続けて、「バケツ」メニューの「分類精度」を確認してみよう。トレーニング後に分類されたメールの数や、正しく分類するその高い精度に拍手を送りたくなることだろう。時折、分類精度をリセットしてみてPOPFileの成長ぶりを観察するのもいいだろう。

—スパムを判断するためのメカニズムに迫る—

POPFileの決め手になる「ベイズ理論」って何だ？

POPFileはいったいどのようにしてこれほどの高い精度でメールを正しく分類できるのだろうか？　その秘密はベイジアンフィルターにある。POPFileはベイジアンフィルターというものを採用してメールを解析しているのだ。

ベイジアンフィルターの基礎となっているベイズ理論とは、古く18世紀の牧師であり数学者であったトーマス・ベイズという英国人によって考え出された原理だ。ベイズは、「物事を判断する確率は、その物事の観察者にとっての不確かさである」と説き、神の存在でさえ数学的に示すことができると述べたそうだ。つまり、新たなできごとを予測する際には、すでに起きている事実と、観察者自身の経験を考慮に入れることにより、かなり正確に推測できる、という考え方である。

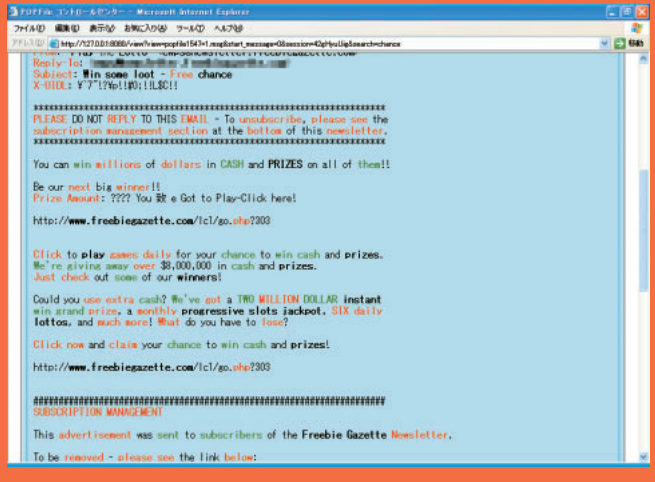
たとえば、あなたに届いた宅配便の小包が、うれしいプレゼントか、そうでないかを予測するとしよう。単純に確率を述べるなら、いちかばちか、50パーセントという確率も悪いとはいえない。しかし、実際には、その小包の大きさ、重さ、差出人、内容に関する記載事項などという「事実」と、過去の「経験」に基づく確率、つまりプレゼントだと思ったらそうでなかったという確率、あるいは期待どおりだった確率を考え合わせることにより、実際の結果にかなり近い予測をすることができる。

この考え方で正しい分類を予測するために、POPFileはユーザーのトレーニングを受けると、それらのメールから、添付ファイルやHTMLのタグやコメントを取り除き、残されたヘッダーと本文をコーパス(corpus)と呼ばれる単語に分解する。そして、分類されるメールの共通点を知るために、出現頻度の高いものを重み付けし、こうしてメールにおける各単語の出現と各バケツに分類された確率を計算できるようにコーパスデータベースを構築する。

そして、新たなメールを受け取ると、そのコーパスデータベースに基づいて、各バケツへの分類に影響を及ぼす単語を抽出し、その単語の有無や出現回数などから計算して、いずれのバケツに分類するかを決定する。その作業の結果、POPFileはさらにセルフトレーニングを行うため、間違わない限り、精度の高いコーパスデータベースができあがっていく。ユーザーの再分類によって訂正される場合、そのデータベースを訂正することにより、POPFileは「観察者の判断」を学習し、観察者にとっての精度を上げることができるのだ。

ためしに、POPFile UIの「履歴」メニューから、spamに指定されたメールの「件名」をクリックしてみてほしい。すると、メールヘッダと本文のあちこちがバケツと同じ色で表示されている。さらに、ページの下のほうから「単語の頻度を表示」「単語の確率を表示」というリンクをたどると、各メールの分類に大きな影響を及ぼした単語が順に表示されており、大変興味深い。

POPFileのデータベースにスパムで使われる単語が十分蓄積されていくにつれ、業者はスパムらしからぬ単語を使ってメールを送らない限り、その判定をすり抜けることは難しくなっていく一方だ。しかし、そのようなメールでは、スパム業者の目的を達することはできないだろう。スパムのフィルタリングの技術が向上するにつれ、彼らのビジネス上の目的が立ち行かなくなり、ついにはスパムメールという手段をあきらめてくれるようになればよいのだが。



「履歴」メニューから件名をクリックするとメールの全文が表示される（画面）。どの言葉がどのバケツに対応しているかが、色分けして表示される。

ニフティがベイズ理論を採用した迷惑メール対策サービスを開始！

大手ISPのニフティが@niftyの会員向けサービスとして、ベイズ理論を応用した迷惑メール対策フィルターの提供を1月14日から開始した。このサービスは、フィルターをユーザーが学習させることによって迷惑メールの判断基準の精度をあげていく、つまり、今回紹介したPOPFileと同じようなものだ。今後はこのような機能がメールサーバー側で提供されるようになっていくだろう。

URL https://www.nifty.com/mail/webmail/spam_folder.htm

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp