特集2

スパムメールと闘う

迷惑メールを排除して効率的に仕事をしよう

インターネットが、ノイズの海に呑み込まれようとしている。ネットの黎明期からわれわれを悩ませ続けてきたスパム――日本語で言ういわゆる「迷惑メール」が、昨年から今年にかけて猛威をふるい、ついに臨界点を突破した。多数のスパムのために、仕事などで本当に必要なメールを探すのがわずらわしかったり、1件1件削除するのはもちろんのことフィルタリングをかけて排除するのも手間がかかったりする。このように、スパムによって効率的な作業がしにくくなったり、ストレスを感じたりしてはいないだろうか。いったいスパムとは何なのか。最新の状況を取り上げるほか、具体的な対処や対策の方法も説明しよう。

Text：【P95～P97】佐々木俊尚（Press Archives）、【P98～P99】四家正紀（株式会社カレン）、【P100～P108】山崎誠也、【P109】編集部
Illust：金子ナンペイ

次々に送信されてくるのはなぜ？

1.スパムメールの正体と取り締まりの現状

社会現象としても取りざたされた携帯電話の「迷惑メール」は、鳴りを潜めた。しかし、PCで受け取るスパムメールは以前にも増して猛威をふるっている。どうしてスパムメールは送られてくるのだろうか。法律で規制しても、いっこうに状況が改善されないのはどうしてだろう。

暴走するスパムの影響は絶望的

対策費用は１兆円強

昨年から今年にかけて、世界中で見られたスパムメールの暴走ぶりは、明らかに度を越している。たとえば昨年、大手調査会社の米ガートナーによれば、スパムメール（以下スパム）は一般企業が受信する総メール数の約半数に到達したという。また、サンフランシスコの調査会社フェリス・リサーチは、今年のスパム対策費用は全米で100億ドル（約1兆2,000億円）に達すると予測している。天文学的な数字ではないか。スパムの根本的な問題は「スパムを相手にする人が減るにつれ、スパムの絶対量はどんどん増えていく」というジレンマだ。果たしてわれわれはこの絶望的な戦いに、勝利を収めることができるのだろうか。

技術と低コストを武器に増加

「反応するユーザーが少なければ、送る量を増やせばいい。いずれは返事をくれる誰かに到達するはず」。ある迷惑メール関係者はこう話した。10万人に送ろうと、100万人に送ろうと、スパマー（スパムの送り手）側のコストはほとんど変わらない。送付数が多くなろうとも、マウスを1回クリックしてデータがすべて流れ終わるまでに数十分かかっていたのが、数時間に変わる程度のことでしかない、つまり手間は同じというわけだ。一方、この膨大なトラフィックの増加によってインターネット全体が被る金銭的な被害は、等比級数的に増えていく。おまけにスパマーの技術も加速度的に進んでいる。

1994年にニュースグループのUSENETで行われた「米グリーンカード抽選手続き代行」の宣伝が、スパムの先駆けと言われている。この時代、メールアドレスはUSENETの書き込みやウェブサイトから集められていた。しかし、今はそうした牧歌的な手法はあまり使われない。主力はDHA（Directory Harvest Attack）だ。「アドレス刈り取り攻撃」とでも訳せるだろうか。たとえば「example.jp」というドメインの企業があれば「suzuki@example.jp」や「ichiro.suzuki@example.jp」など、それらしいアドレスのメールを送りつけ、エラーが返ってきたアドレスは取り除き、反応がなかったアドレスだけをデータベースに登録していく仕組みだ。まるでサイバーテロのDoS攻撃のようなアグレッシブかつシンプルな手口だが、これに対抗するのはきわめて難しい。対症療法以上の対策は、今のところ誰も思いついていない。

広がる「スパム」の定義

そもそもスパムは「求めていないのに送りつけられる大量のメール」と定義されていた。米ガートナーによれば、その分類は下表のとおりだ。同社は、このうち退治すべきスパムは「純然たるゴミ」と「チェーンメール」だけだという。しかしスパムの嵐に辟易するユーザーは、最近真っ当な企業が送ってくる広告メールからウェブのポップアップ広告（確かにこれはうんざりする存在だが）まで、すべてをスパムとして敵視しはじめている。ネットで目に入る気にくわないものはすべてスパムというわけだ。実際、日本の広告業界関係者によると「携帯メール広告はスパムと混同されやすいため、広告主から敬遠される傾向にある」と言う。せっかく立ち上がりつつあるネット広告業界も、スパムの海へと呑み込まれていこうとしているのだ。影響は決して小さくないだろう。

■米調査会社ガートナーによるスパムの分類

分類	内容
純然たるゴミであるスパム（Pure-Trash Spam）	アダルトサイトの宣伝や売春の斡旋、金融、オンラインカジノなどの広告。勝手に収集されたメールアドレスに大量に送りつけられてくるスパムの王道。
チェーンメール（Chain Mail）	根拠のない都市伝説や、「この人が困っています。メールを送って励ましてあげて」といったヘルプを求める詐欺の類。あるいは「リストの名前の人に各者5,000円を振り込み、ほかの人に広げよう」というネズミ講まがいの無差別メール。
ジャンクメール（Junk Mail）	以前に商品を購入したり、サービスを利用したことのある企業などから送られてくる広告メール。ユーザーの側がメールアドレスを登録し、広告を受け取ることに承諾していることから「正当なスパム」とも呼ばれる。しかし、実際には読まずに捨てられる率はふつうのスパムとあまり変わらない。
企業内スパム（Occupational Spam）	会社の中で、同僚や上司から届くどうでもいい内容のメール。

片手間でもできるスパムメールの商売と手口

携帯電話から流れ込む

昨年夏ごろから、あるスパム業者の登場が業界で話題になっている。Mと名乗るそのスパマーは、下品なチャイルドポルノを皮切りに出会い系から大麻の種まで、ありとあらゆるスパム広告メールを大量に繰り返し送信している。独自に収集した膨大な数のメールアドレスに対し、1つのアドレスに1日数十通を送りつけるその圧倒的な物量作戦は、過去に例がないレベル。おまけにアンチスパム運動の個人サイト掲示板などで“荒らし行為”までをも繰り広げたことから“スパム退治人”たちの間で一躍悪名を轟かせる結果となった。

スパム退治人の1人A氏が語る。「Mが現れたのは昨年の8～9月ごろだった。それまでは携帯電話の“ワン切り”を専門にやっていたらしいが、規制が厳しくなってインターネットのスパムに流れてきた。携帯電話の迷惑メールやワン切りは、携帯電話会社が監視を厳しくした結果、ほぼ全滅状態になっており、民族大移動のようにネットスパムに業者が流れ込んできているという背景がある」。

メールアドレスの刈り取り方

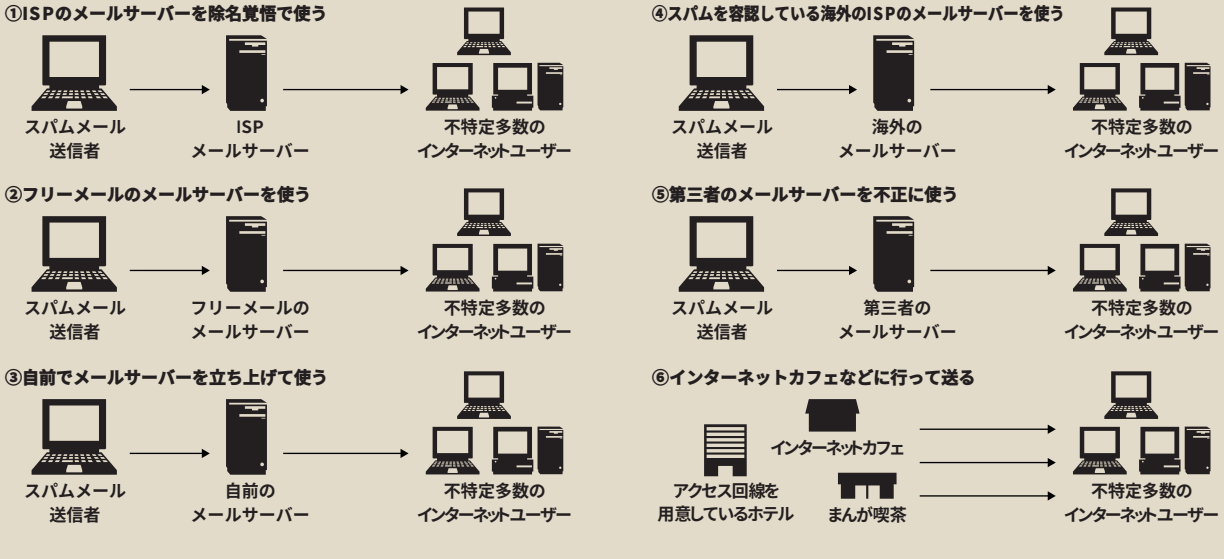
それにしても、スパマーたちはどのようにしてスパムを発信しているのだろうか。まず、その仕組みを考えてみよう。

最初に必要なのは、ウェブや掲示板からメールアドレスを収集するためのアドレス収集ソフト。検索エンジンにかければ数千円～1万円程度のシェアウェアが簡単に手に入る。ウェブサイトのソースをダウンロードし、そこからメールアドレスを抽出しているだけの簡単なソフトだ。先のMの場合は常時5～6台のアドレス収集専用サーバーそれぞれでアドレス収集ソフトを走らせ、数日間もかけて大量のメールアドレスを集めていると推測されている。実際、1台のパソコンで試しにこの種のソフトを走らせてみたら、わずか数時間で1000以上のメールアドレスを簡単に集めることができた。M並みの規模で収集すれば、膨大な数のメールアドレスが入手できるだろう。

ただこの手のソフトの場合、ウェブの管理者や掲示板利用者のアドレスは調べられるが、圧倒的多数を占める普通のユーザーのアドレスを集めるのは難しい。そこで登場してきたのが、DHA（Directory Harvest Attack）と呼ばれる手口だ。これは企業など特定のターゲットを定めたら、いかにもありそうなメールアドレスを想定して数万種類のメールをそのドメイン宛てに送りつける。エラーが返ってきたら、そのメールアドレスは不達だとわかる。逆にエラーが返ってこなかったら、メールアドレス存在の逆証明になる。これで企業内の個人ユーザーの貴重なメールアドレスを大量に入手することができ、米国で主流になりつつあるという。しかし、大量のエラーが生じると、スパマーの利用しているISPにはDoS（サービス拒否）攻撃に近い集中的なパケットが返ってくる。ネットのトラフィックに与える影響は少なくない。

しかし日本では、DHAを使っている業者もさほど多くなく、現状ではメールアドレス収集ソフトを使っているケースがほとん

■図1　スパムはこうして送られている



どだと言われる。しかし、これからどうなるか。「日本のスパマーは現在は技術的レベルもさほど高くない。米国並みになるのはまだこれからでしょう」（A氏）というのは不吉な予言ではないか。

ADSLの普及がスパマーを生み出す

さて、こうしてメールアドレスが集まれば、あとはそのアドレス宛てに広告メールを送りつけるだけだ。スパム退治の専門家は「上り速度1MbpsのADSL回線が1本あれば、1日数十万通のメールを送り出すことができる」と言う。実際には、スパマー向けのベンダーがアドレス収集ソフトと同時送信ソフトをセットにしてパッケージで販売している。そうしたソフトを買えば、ボタン一発でメールアドレスを大量に収集し、そうして集めたアドレスに再びボタン一発でメールを送ってくれる。あとはひたすらパソコンが作業をこなすのを待っていればよい。

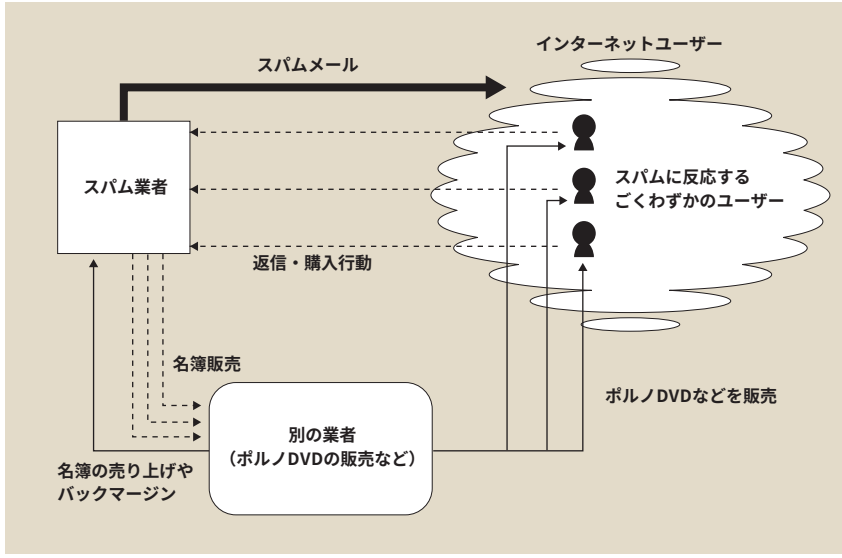
もちろん、スパムを送信する際には“ISPの規約”という大きなハードルがある。これをどうクリアするかが、スパマーたちの独自ノウハウにもなっている。前出のスパム退治の専門家によれば、その方法は6種類に大別できる（図1）。

悪名高いMは、比較的高度な③の方法を採っているとされるが、しかし日本国内でもっとも多いのは、実は原始的な①のケース。「日本はまだ技術的に幼稚なスパマーが多いうえ、日本のISPの中にはスパムを事実上容認していて大量のメール発信が行われても看過しているところがある。スパマーの連中は、そうしたISPを利用している」（A氏）と言うわけだ。いずれにせよ、適当なADSL回線とそれにつながったパソコンを持っていれば、後は1万数千円程度のソフト代があればスパマーを開業できてしまうということなのだ。

スパムビジネスは儲かるのか

さて、ここまで読んでピンと来なかっただろうか。スパム業というのは、実はとんでもない低コストで運営できてしまうのである。「大量のスパムを送信しても、反応があるのは0.001パーセント程度。百万通送って、数十件から数件の返事がある程度。『そんなレベルでビジネスとして成り立つのか』と誰もが思うでしょう。でも10人ぐらいから反応があり、そこからいくばくかの収入が上がれば、それでビジネスとして成立してしまう」とA氏は語る。

■図2　低コストで儲けるスパムメールのビジネス



営業コストがきわめて低いということは、利益が出やすいということだ。ADSLの回線費用が月額3,000円程度だとすれば、単純に考えると月額3,000円の売り上げで損益分岐点は超えてしまう。人件費もゼロに近い。「昨年ぐらいから急激にスパムが増えています。これはケータイの迷惑メールが難しくなったのと同時に、ADSLの低価格化で大量のスパムメール送信が簡単にできるようになったことが大きい。個人がサイドビジネスとして片手間にできてしまう」（A氏）。

さらに、ビジネスモデルとして興味深いのは、スパムは二重に売り上げを得られる仕組みになっていることだ。たとえば冒頭に挙げたチャイルドポルノの広告を発信しているMの場合。まずスパムを見て返信してきた人に非合法のチャイルドポルノDVD-ROMを販売し、同時に、そうやって購入した人の名簿をまとめてポルノ業者に売りつけるのだ。Mは「一度チャイルドポルノを買った客の名簿だからね、そりゃ高く確実に売れるわけだよ」とうそぶいているという。

撤退と参入の繰り返し

とはいえ、その儲けが営利事業として成り立つほどかと言えば、案外そうでもないようだ。さまざまな業者や個人がスパムビジネスに参入する。しかし利幅が思ったほど大きくはないためにすぐに撤退する。そしてまた別の業者が参入してくる。スパム業界はそうした繰り返しを続けているようだ。「本当に儲かってるのは、スパマーにソフトやシステムを売りつけているベンダーだけかもしれませんね」（A氏）。なんだかまるで、ネットバブル華やかなりしころのネットベンチャー企業とシステムインテグレーターの関係のようだ、と言ったら不謹慎だろうか。

それにしても、インターネットのモラルなどにはまったく興味のないそうした人たちが、雪崩を打ってスパム業界に参入してきているということなのだろう。寒気のするような光景ではある。

期待された法律の規制もいまだ効果なし

きっかけは携帯電話のメール

日本におけるスパムメールに対する法規制のきっかけとなったのは、主にiモードなど電子メール機能付きの携帯電話において多発した「迷惑メール」問題である。「出会い系」や「アダルトコンテンツ」などのスパムがインターネット経由で携帯電話端末に大量に送信され、携帯電話利用者の通信コスト（パケット代金）負担の増加と、インフラの障害によるメール送信遅延などの被害が出た。また、未成年者の利用も多い携帯電話に対して大量の有害情報が送りつけられる危険性も指摘され、こうしたスパムに対する規制を望む声が強くなった。

まず、総務省が2001年秋に「迷惑メールへの対応の在り方に関する研究会」を開催したが、当時はまだ憲法などに定められている「表現の自由」「通信の秘密」などを理由に、法規制について消極的な姿勢が見られた。この一方でNTT出身の参院議員である世耕弘成氏（自民党）を中心に、議員立法による「迷惑メール対策法案」が年末までにまとめられ、国会に提出されることになっていた。

しかし、実際には2002年1月に経済産業省の省令による「特定商取引法施行規則の一部改正」がスパムに対する日本初の法規制となった。その内容は、①通信販売事業者などの電子メールアドレスを表示、②メールの件名欄に「！広告！」と表示するとともにメールの本文にも広告である旨を表示（ただし消費者から広告の送付を求めたり、送付を承諾したりした場合は表示義務なし）、③消費者がメールの受け取りを希望しない場合に、その連絡を行う方法を表示（ただし連絡方法を設定しない場合には件名欄に「！連絡方法無！」と表示するとともにメールの本文にも連絡方法がない旨を明確に表示）という、営業手段としてのメール配信における表示義務を追加したものである。そして「件名のフィルタリングによる受信者側でのスパムの削除」と「受け取り拒否の連絡（オプトアウト）」を可能にするというものだった。だが、この省令には数々の問題点があったのだ。

まず「！広告！」という表記は「！」について、2バイトなのか1バイトなのか（つまり全角と半角）の規定がなく、1つのフィルタリング設定では対応できない。またオプトアウトにより、架空ではなくて実際に使われている「生きたメールアドレス」であることが確認されてしまうために、新たなスパムを誘発する危険性が考慮されていない。さらに、「！広告！」「！連絡方法無！」などの表示義務を守ればスパムを配信してもかまわないという「お墨付き」を国が与えたとの批判も強かった。

そして、結局は通報を受けても行政側でメールの発信元である業者を特定することが難しく、この省令による行政処分は1件もなかった。

2つの法律施行後も行政処分ゼロ

経済産業省による「特定商取引法の施行規則の一部改正」は、総務省と与党サイドの動きとが完全には連動しなかったため、その後に改めて関係者による内容の調整が行われた。そして、2002年4月に参議院自民党案を元にした「特定電子メールの送信の適正化等に関する法律」（特定電子メール法）と、「特定商取引法の改正案」がほぼ同時に成立した。

法律の主な内容については下にまとめてあるので参照してほしいが、スパムを「商売」と「通信」の両方から挟み撃ちに規制するかたちになっている。2002年1月の省令改正では不十分だった「受信拒否者に対する再送信の禁止」が規定されるなど、規制は強化されており、その効果が期待されていた。

ところが、実際には施行後半年以上が経過し、市民より相当数の通報が寄せられているにもかかわらず、行政処分はいまだゼロだ。総務省がわずか1件の措置命令を出したのみである（右ページ上の囲み記事）。業者はスパムの配信技術を高度化させるうえに、取り締まりを逃れるために法人格や住所を頻繁に移転するため、

■ 法律施行までの道のり

2001年12月14日	自民党の世耕弘成議員が「迷惑メール対策法案」を議員立法で提出することの党内承認を得る。
2001年12月18日	経済産業省が研究会を発足して「特定商取引に関する法律施行規則の一部改正」に関してパブリックコメントを実施。
2002年1月10日	経済産業省「特定商取引に関する法律施行規則の一部を改正する省令」を公布。
2002年1月16日	広告主要7団体が経済産業省を訪問。
2002年1月24日	総務省「研究会」の中間とりまとめを公表。“技術的対策よりも制度的対策を優先 〝継続的見直しが必要 ”という内容。
2002年1月25日	広告主要7団体が経済産業省に対して要望書を提出。「！広告！」の見直しを要望。
2002年2月1日	経済産業省が「特定商取引に関する法律施行規則の一部を改正する省令」を施行。
2002年2月21日	経済産業省と参議院与党三党（議員立法）から提出された二法、規制対象を分けることで同時成立を目指すことになる。
2002年4月11日	世耕弘成議員案→総務省「特定電子メールの送信の適正化等に関する法律」が成立。
2002年4月12日	経済産業省「特定商取引に関する法律の改正案」成立
2002年5月17日	広告主要7団体が“「未承諾広告※」から広告の文字を抜くように ”と再度要望書を提出。
2002年5月21日	経済産業省がパブリックコメントを募集。
2002年6月11日	社団法人日本広告主協会Web広告研究会独自の調査にもとづく意見書を経済産業省に提出。
2002年6月21日	DDIポケットが「未承諾広告※」のフィルタリング機能を実装。これ以降、各社が追随。
2002年7月1日	二法施行

スパムを送りつけてくる業者や送信者の所在を特定することが難しい。当初期待されていた件名の「未承諾広告※」表記によるフィルタリングは携帯電話事業者がサービスとして提供しているが、行政処分が難しいことを見越した「未承諾広告＊」「未承諾広告※」といった表示義務違反が後を絶たないためになかなか機能しない。

さらに海外からの配信は野放しである。韓国や中国、台湾などのアジアをはじめとする世界各国からのスパムに手を焼く読者も多いと思われるが、これに対する規制はまったくない。

この一方で、法規制に対する過剰反応から正当なメールマーケティングが阻害されるケースも出てきている。悪質なスパムを取り締まれずに、正当な商行為が萎縮してしまってはまったくの本末転倒である。「！広告！」「未承諾広告※」といった表示義務は「広告＝迷惑メール＝削除すべきもの」との認識を広げるとして、広告業界からの反発を招いている。

いまのところ、2つの法律におけるスパム抑止力は残念ながらまだ低い。しかし、今後取り締まりが強化されて行政処分が執行されれば、少なくとも国内の業者に対する一罰百戒の効果により、スパムが減少に転じる可能性もある。また、スパムをもっとも多用する「出会い系サイト」の未成年利用に対する法規制が、警察庁を中心に現在検討されている。これがスパムに対する新たな抑止力として機能するかもしれない。

一般的に法律というものは、施行されてすぐにはなかなかその効力が発揮できない。法律に示された考え方のもとに、運用における詳細が詰められて初めて機能するようになる。欧米においてもスパム規制はまだ決して効果的に機能しているとは言いがたい状況である。スパムという新しい社会問題に対して、法規制がその抑止効果を挙げていくためには、従来の行政の枠を超えた省庁間と官民、国際間の協調によるに努力がまだまだ必要になるだろう。

法律施行で初の摘発者！

総務省は、昨年12月25日に東京都内の電子メール配信業者に対して、法律を守るように求める措置命令を出した。これは、特定電子メール法と改正特定商取引法というスパムを規制する法律が昨年7月に施行されて以来、初の処分になる。本文にあるとおり、特定電子メール法では受信者の同意を得ていない広告メールを送る業者は、表題部分に「未承諾広告※」と明示することが義務付けられたほか、受信を拒否した人への再送信を禁じている。この業者はこれらの規則に違反したメール配信を行い、総務省から警告を受けたが、これに従わなかった。今後、措置命令にも従わない場合は、行政処分として50万円以下の罰金が科される可能性もある。

「特定商取引法」と「特定電子メール法」

「特定商取引法」は、もともと「訪問販売法」として施行された法律を、通信販売などさまざまな商取引に規制範囲を拡大したものだ。ほかの法律に規定がない特定の商取引について「消費者（購入者）保護と取引の公正性の確保」という視点で規制している。多くのECサイトの「利用案内」などのページに「特定商取引法に基づく表示」が記載されていることからも分かるように、規制対象となるのは特定商取引に該当する事業を行う「事業者」である。所管官庁は経済産業省となる。

これに対して「特定電子メール法」の所轄官庁は総務省。こちらは通信行政の立場から電子メールの利用についての良好な環境の整備のために昨年7月から新たに設けられた法律で、大量の「特定電子メール」（広告宣伝目的でオプトインのないメール）を配信する行為を規制する（たとえばスパムのせいでiモードが遅延するようなことを防ぐ）ための法律であると言える。そのため規制の対象は「発信者」、つまり発信代行業者も含めたスパムを送信する業者である。

2つの法律はその規制の基準において矛盾しないように調整されており、規制の主な内容としては、

①規制対象となるメールの件名の最前部に「未承諾広告※」と表示
②送信者あるいは事業者の連絡先（氏名または名称、住所、送信に用いたメールアドレス）を表示
③受信拒否者に対する再送信の禁止。受信拒否ができることを表記し、メールアドレスなどそのための連絡方法を表示

などがある。

さらに特定商取引法では事業者に対して「事業者の住所や電話番号、価格、商品の支払い方法、返品特約など、商品やサービスの取引条件に関する情報を広告内に表示」「消費者の請求などに基づいて送信される広告メールには、オプトアウトの通知を受ける方法を広告内に表示」という規制があり、特定電子メール法では送信者に対して「架空電子メールアドレスに宛てた電子メールの送信禁止」を規定している。

罰則は、特定商取引法については「個人:300万円以下の罰金もしくは2年以下の懲役、法人:3億円以下の罰金」、特定電子メール法では「50万円以下の罰金」となっている。また、どちらの法律についても通報先は警察ではなく、所轄官庁の外郭団体となる。特定商取引法については財団法人日本産業協会URL01、特定電子メール法については財団法人日本データ通信協会URL02だが、特に個別応答してくれるわけではない。提供された情報については分析や検討を行い、迷惑メール問題に関する行政対応に十分に活用される。

URL01 http://www.nissankyo.or.jp/
URL02 http://www.dekyo.or.jp/

もうこれ以上貴重な時間を奪われない

2.スパムメール予防・対策実践テクニック

スパムメールとはどういうものかがわかっても、スパムがなくなるわけではない。貴重な時間をスパムの処理に費やさなくてもすむように、スパム対策のテクニックを知り、実践することが大切だ。今すぐ実行できるスパム対策テクニックをここで紹介する。

どうすりゃいいんだこのスパム　スパム対策の大原則

現段階では、日々増え続けるスパムメールを根本的に解決する方法はなく、対症療法的に解決せざるをえない。スパム対策の大原則は2つだ。1つは、これ以上スパムが届かないようにすること。もう1つは、スパムが届いても目にしないように工夫することだ。

大原則1 メールアドレスの流出を防ぐ

これ以上スパムが届かないようにするには、なによりもスパム業者にメールアドレスが渡らないようにすること。スパム業者はさまざまな方法を使って、メールアドレスを集めている。たとえば、メールアドレス収集ソフトでインターネットを巡回させている。このソフトは、ホームページからメールアドレスを効率よく抽出する。また、懸賞などに応募することによって、アドレスが流出する可能性もある。

メールアドレスが流出しないための最低限の自衛策を「一般常識スパム予防テクニック」で紹介する。

大原則2 届いたスパムは読まない

ネガティブな対策だが、要はスパムが届いても目にしなければいいのだ。メールを受信する前にメールサーバーからスパムを削除する方法や、メールソフトの振り分け（フィルター）の機能を使ってスパムを隔離する方法が有効だ。メールの件名や本文に特定のキーワード（具体的な例を各ページ下の **はみだしスパムチェック** に示しておいた）がある場合や、送信者がスパム送信者のブラックリストにある場合にスパムと判断するのだ。ただし、振り分け機能が万能というわけではない。誤動作して大切なメールをスパム隔離用メールボックスに入れてしまったり削除したりすることもあるので、注意する必要がある。

ホワイトリストという考え方もある。文字どおりブラックリストの逆で、ビジネスパートナーや知人のアドレスをリストに登録し、登録者のメールを優先的に読む方法だ。メールソフトに付属しているアドレス帳を利用して、スパムの可能性が低いメールを特定のフォルダーに振り分けておけば、すぐに重要なメールが見つかる。

これらの具体的な方法は、「自分でできるスパム対策テクニック」で紹介する。

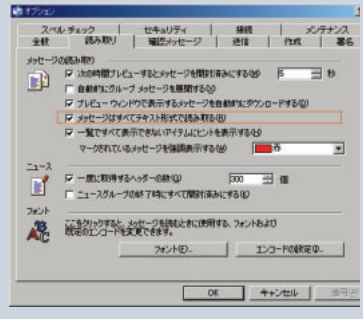
自分からスパムを呼び込んでない？一般常識スパム予防テクニック

1 知らない人からの怪しいメールは開かない

難易度：★☆☆☆☆
費　用：\0

ウイルス対策の基本と同じで、非常に基本的なことだが、怪しいと思ったら手をつけないのがいい。HTMLメールのインタラクティブ性を悪用して、メールアドレスを収集する方法がある。たとえば、HTMLによる開封確認などだ。うっかりメールを開いてしまうと、ウェブサイトにアクセスしてしまい、そのメールアドレスが有効なものだとスパム業者に知らせていることになる。知らない人からのメールは、うかつに開かないようにしよう。

HTMLメールは読まないか、テキスト形式で表示するようにしておくといい。



Outlook Express 6ではメニューから「ツール」→「オプション」を選び、「読み取り」タブの「メッセージはすべてテキスト形式で読み取る」を選んでおく。

はみだしスパムチェック1「未承諾広告」（件名）：今は当然のキーワード。

2 スパムには絶対に返信しない

難易度：★☆☆☆☆
費　用：\0

スパムメールに記載されている受信拒否のための連絡先に返信するのも考えものだ。かえって、そのメールアドレスが有効であることを知らせ、さらにメールアドレスが他の業者に転売される可能性もある。現状では、スパムは、放置するのが得策だ。

また、スパム対策ソフトのなかには、差出人に「UserUnknown」のエラーメールを送るものがある。つまり「メールを送っても、そのアドレスは存在しないから無駄ですよ」と通知する試みだ。これは得策のように思えるが、少々危ない点もある。というのも、メールのヘッダーから偽装がバレてしまうのだ。さらに、海外からのスパムは差出人のメールアドレスを詐称していることも多い。この場合、差出人宛てに返信すると、まったく関係のない人に迷惑がかかってしまうこともある。このようなソフトを利用するときは、以上の点に留意しよう。

3 掲示板や懸賞でむやみにアドレスを晒さない

難易度：★★☆☆☆
費　用：\0

掲示板などでのメールアドレスの公開はスパム業者にとって恰好の餌食だ。なにしろアドレス収集ソフトを巡回させるだけで、生きたメールアドレスが自動的に入手できるからだ。このような収集ソフトへの対策を施した掲示板もあるが、その数はまだ少ない。いまのところ掲示板でのメールアドレスの公開は気をつけるべきだ。ふだん使用するものとは別に、投稿専用のメールアドレスを取得しておくのもいいだろう。

インターネットでのアンケートや懸賞にも注意が必要だ。これらを悪用してアドレスを収集している業者もいる。また、そのような業者でなくとも、登録情報の管理体制が甘いため、プライバシー情報が流出することもありうる。昨年続発した企業サイトからのプライバシー情報漏洩事件などが、この例だ。どうしても応募するなら、いくらかスパムの襲来を覚悟しておくべきだ。

4 ウェブページに出すメールアドレスはエンコードする

難易度：★★★★☆
費　用：\0

自分のウェブページに連絡先として出すメールアドレスも、アドレス収集ソフトの餌食になってしまう。とはいえ、ウェブサイトの管理者ならば、連絡先としてメールアドレスを掲載しておかないわけにはいかない。アドレス収集ソフトは、HTMLソースの「mailto:」に続く文字列や「@」記号の前後を目安にしてアドレスを収集している。この対策として、メールアドレスのアルファベットや数字をHTMLエンティティーにエンコードしてしまう方法が有用だ。

HTMLエンティティーとは、ひらたく言えば、ある文字を別の特別な文字列で表現したものだ。「&」を「&」で書く方法だと言えば、HTMLを書いたことがある人ならわかるだろう。このHTMLエンティティーは特殊文字だけでなく、アルファベットや数字などどんな文字にでも使える。たとえば、小文字の「a」は「a」で表現できる。ウェブページに書くメールアドレスをHTMLエンティティーにエンコードしておけば、アドレス収集ソフトの目から逃れられる可能性が高くなるということだ。もちろん、この方法に対応しているアドレス収集ソフトからは逃れられないが、現状ではかなり有効な措置だと言えるだろう。

```
<A HREF="mailto:
&amp;#105;&amp;#109;&amp;#45;&amp;#105;&amp;#110;&amp;
#102;&amp;#111;&amp;#64;&amp;#105;&amp;#109;&amp;#112;
&amp;#114;&amp;#101;&amp;#115;&amp;#115;&amp;#46;&amp;
#99;&amp;#111;&amp;#46;&amp;#106;&amp;#112;">
&#105;&#109;&#45;&#105;&#110;&#102;&#111;&#64;&#105;&#
109;&#112;&#114;&#101;&#115;&#115;&#46;&#99;&#111;&#46
;&#106;&#112;</a>
```

メールアドレスをHTMLエンティティーに変換するソフトとしては、ウィンドウズ用なら「HTMLエンティティ生成」URL01、Mac用なら「SpamStopper」URL02などがある。また、メールアドレスを入力すれば、適切なHTMLエンティティに変換したHTMLコードを出力してくれるウェブページURL03もある。

URL01 http://ab.jpn.ph/
URL02 http://www.railheaddesign.com/
URL03 http://spam.h1r.org/spambot/

メールアドレスを上の図のようにHTMLエンティティーにエンコードしておけば、HTMLソースを見てもメールアドレスだとはわからない。もちろん、これをブラウザーで表示すると、下の図のようにちゃんと見える。

はみだしスパムチェック2「未承認広告」「未承諾広告」（件名）：微妙な違いに注意。

スパムなんて見たくもない！ 自分でできるスパム対策テクニック

5 Norton Internet Security 2003でスパムチェック

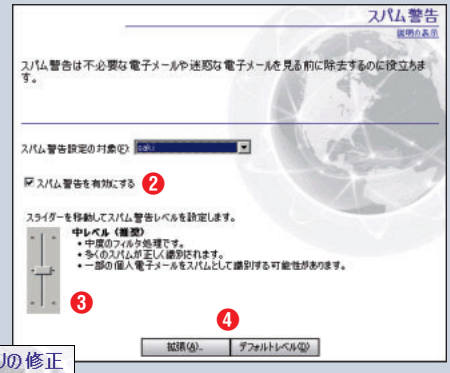
難易度：★★★★☆
費　用：\7,800

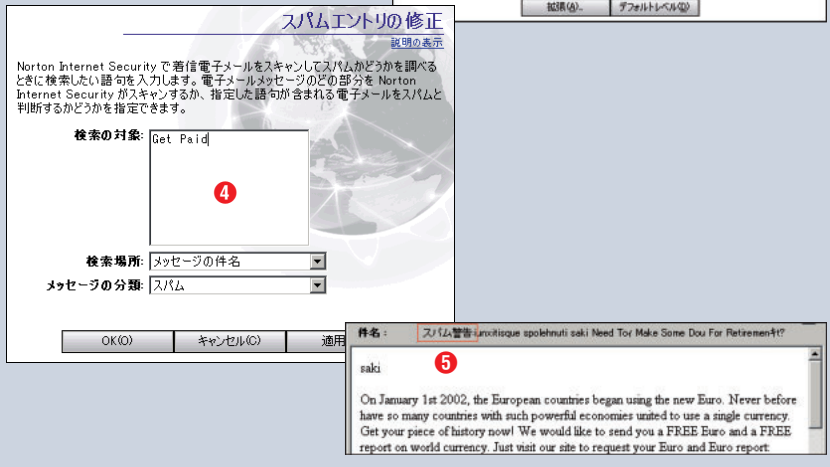
【ウィンドウズ】【メールソフトを問わない】

ウィンドウズでしか使えないが、シマンテックのインターネット総合セキュリティーソフト「Norton Internet Security 2003」は、「スパム警告機能」を搭載している。サーバーとメールソフトの間で動作するので、いつものメールソフトを使える。インストールしてサーバーやメールアドレスの情報を登録すれば、あとは簡単な操作でスパムをチェックできる。

❶Norton Internet Securityを開き、「スパム警告」をクリックする。続いて「設定」ボタンをクリックする。
❷「スパム警告を有効にする」にチェックを入れると、メールソフトでスパム警告機能を利用できるようになる。
❸警告レベルを「高」にすると一般のメールもスパムと認識する確率が高くなり、「低」ではスパムの認識率が低くなる。
❹「拡張スパム警告」を使えば、スパムメールの定義をカスタマイズできる。ただし、件名や名前には日本語が利用できないので注意が必要だ。
❺スパム警告機能を利用すると、メールの件名に「スパム警告:」の文字列が付加される。後はメールソフトの振り分け（フィルター）機能を使って、スパムを排除できる（メールソフトの振り分け機能についてはテクニック9以降を参照）。

URL http://www.symantec.co.jp/





6 スパム対策メールサービスを利用する

難易度：★★☆☆☆
費　用：サービスによる

【OSを問わない】【メールソフトを問わない】

スパムメールを拒否できるサービスや、メールの振り分け機能を利用できるメールサービスを利用するのも1つの方法だ。メールアカウントを変更しなくても、今使っているアドレスに来たメールはすべてこれらのサービスへ自動的に転送するようにして使えばいい。メールの転送方法については各プロバイダーに問い合わせてほしい。

スパム対策のできるメールサービス

IIJmio／セーフティメールサービス	http://www.iijmio.jp/guide/outline/mm/
BIGLOBE／メール受信拒否サービス	http://email.biglobe.ne.jp/reject/
@nifty／スパムメールブロック	http://www.nifty.com/mail/reject.htm
So-net／着信拒否サービス	http://www.so-net.ne.jp/rejct/
OCN／Mail ON	http://www.ocn.ne.jp/
ぷらら／メールリジェクト	http://www.plala.or.jp/access/community/mailplus/reject/
スペースタウン／パワーメール	http://www.spacetown.ne.jp/

はみだしスパムチェック3 「ADV:」（件名）：未承諾広告の海外版。

7 Mail Check It!でサーバーからスパムを削除

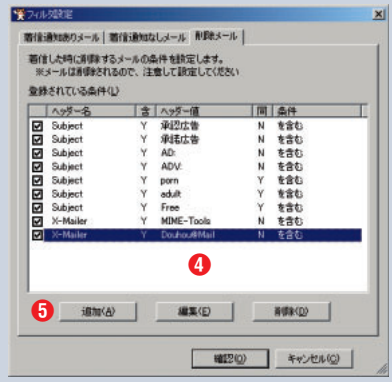
難易度：★★★☆☆
費　用：\1,575

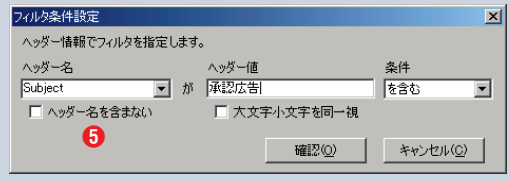
【ウィンドウズ】【メールソフトを問わない】

Mail Check It!は、タスクトレイに常駐して定期的にメールサーバーをチェックして、新しいメールがあれば教えてくれるシェアウェアだ。フィルター機能があり、メールチェック時にヘッダーや本文に指定したキーワードがあるメールをスパムとしてサーバー上で削除できる。このため、Mail Check It!を起動しておけば、いつものメールソフトでメールを受信してもスパムは届かない。複数のメールアカウントにも対応している。

❶起動するとタスクトレイに常駐するので、右クリックして「設定」を選ぶ。
❷チェックの時間間隔や使うメールソフトを設定する。
❸「アカウント設定」でメールアカウントを設定する。
❹アカウント情報の「オプション設定」タブで「フィルタ設定」ボタンをクリックする。「フィルタ設定」ウィンドウの、「削除メール」タブにスパムのフィルターを設定していく。
❺「追加」ボタンを押すと設定ウィンドウが開くので、フィルターの条件をメニューから選び、キーワードを入力していく。

URL http://www.skyarts.com/japan/





8 Spam Mail Killerでスパムに柔軟に対応

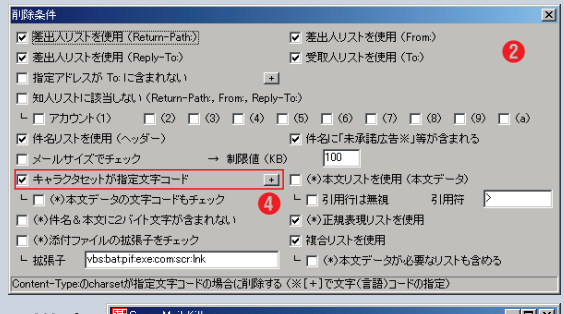
難易度：★★★★★
費　用：\0

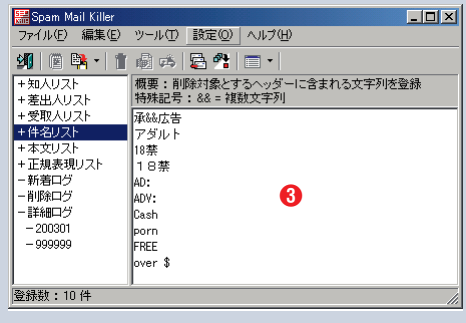
【ウィンドウズ】【メールソフトを問わない】

Spam Mail Killerは、Mail Check It!と同様なメールチェッカーだ。フリーソフトだがスパム削除の条件を非常に細かく設定でき、正規表現が使えるので詳しい人なら絶えず変化するスパムメールにも柔軟に対応できる。Spam Mail Killerは非常に多機能なので、ここではそのすべてを紹介しきれない。使いこなせば非常に心強いスパム対策ツールとなるだろう。

❶「設定」→「動作環境の設定」→「アカウントの登録」メニューでメールアカウントを、「設定」→「動作環境の設定」→「基本設定」メニューでチェック間隔などを設定する。
❷メニューの「設定」→「動作環境の設定」→「削除条件」で削除の全体的な条件を指定する。ここでは、差出人をチェックするのか、件名をチェックするのかといった、チェックの対象となる項目(場所)を指定する。
❸あとは、メインウィンドウの左側で項目を選び、それぞれの項目に対する削除条件を、右側に1行に1条件ずつ記述していく。
❹削除条件ダイアログの文字コードによる判別機能を利用すれば、韓国や中国経由のスパムメールを簡単に削除できる。

URL http://homepage1.nifty.com/eimei/





はみだしスパムチェック4「us-ascii」「iso-8859-1」(Content-Typeヘッダー)：英語のメールに用がない人向け。

※Outlook Expressはウィンドウズに付属するメールソフト

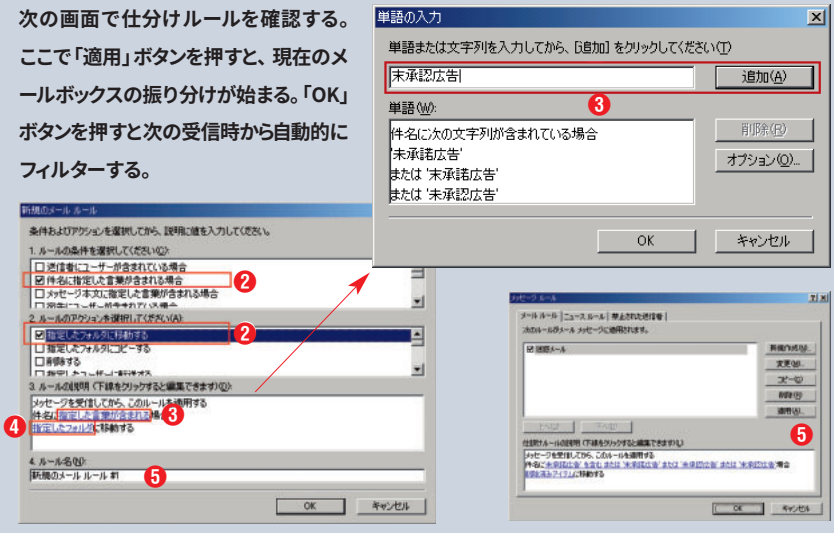
9 Outlook Express 6でキーワードを使って振り分ける

難易度：★★★☆☆
費　用：\0

【ウィンドウズ】【Outlook Express】

❶「ツール」メニューから「メッセージルール」→「メール」の順に選ぶ。
❷「新規作成」ボタンをクリックし、「1.ルールの条件…」に「件名に指定した言葉が含まれる場合」を、「2.ルールのアクション…」に「指定したフォルダに移動する」を選ぶ。
❸「3.ルールの説明」で青い「指定した言葉が…」をクリックする。「単語の入力」ダイアログが表示されるのでキーワードを入力して「追加」していく。
❹同様に「3.ルールの説明」で青い「指定したフォルダ」をクリックし、迷惑メールを振り分けるフォルダーを指定する。
❺「4.ルール名」をつけて「OK」ボタンを押す。

次の画面で仕分けルールを確認する。ここで「適用」ボタンを押すと、現在のメールボックスの振り分けが始まる。「OK」ボタンを押すと次の受信時から自動的にフィルターする。



10 11 Outlook Express 6で ブラックリスト／ホワイトリストを使って振り分ける

難易度：★★☆☆☆
費　用：\0

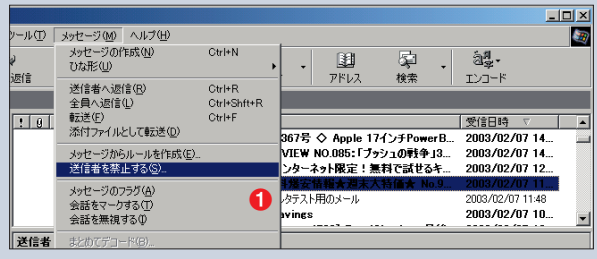
【ウィンドウズ】【Outlook Express】

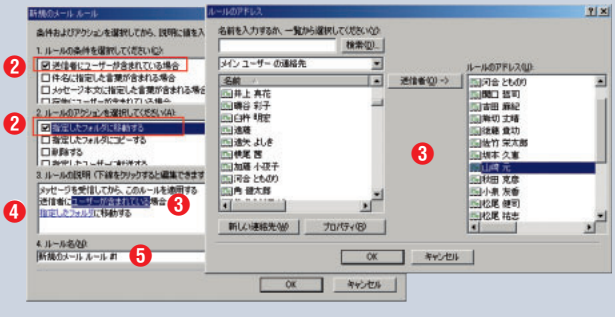
ブラックリストを使って振り分ける

❶ブラックリストに掲載するメールを選択し、「メッセージ」メニューから「送信者を禁止する」を選ぶ（図上）。

ホワイトリストを使って振り分ける

❶「ツール」メニューから「メッセージルール」→「メール」の順に選ぶ。
❷「新規作成」ボタンをクリックし、「1.ルールの条件…」に「送信者にユーザーが含まれている場合」を、「2.ルールのアクション…」に「指定したフォルダに移動する」を選ぶ（図下）。
❸「3.ルールの説明」で青い「ユーザーが含まれている場合」をクリックし、「ユーザーの選択」画面で「アドレス帳」ボタンをクリックする。アドレス帳で知人のメールアドレスをすべて選択して「送信者」を押し、リストに追加する（図下）。
❹同様に「3.ルールの説明」で青い「指定したフォルダ」をクリックし、ホワイトリスト登録者からのメールを優先して振り分けるフォルダーを指定し、「OK」ボタンを押してダイアログを閉じる。
❺「4.ルール名」を「ホワイトリスト」にして「OK」ボタンを押す。後はキーワードでの振り分けのときと同様だが、ホワイトリストのユーザーからのメールは優先して見るようにする。





はみだしスパムチェック5「euc-kr」「iso-2022-kr」（Content-Typeヘッダー）：韓国語のメールに用がない人向け。

※Outlook 2002はオフィスXPに含まれるメールソフト

12 Outlook 2002の迷惑メール振り分け機能を使う

難易度：★☆☆☆☆
費　用：\0

【ウィンドウズ】【Outlook 2002】

Outlook 2002には迷惑メール自動振り分け機能が内蔵されているが、標準では動作していないので、次のようにして有効にする。

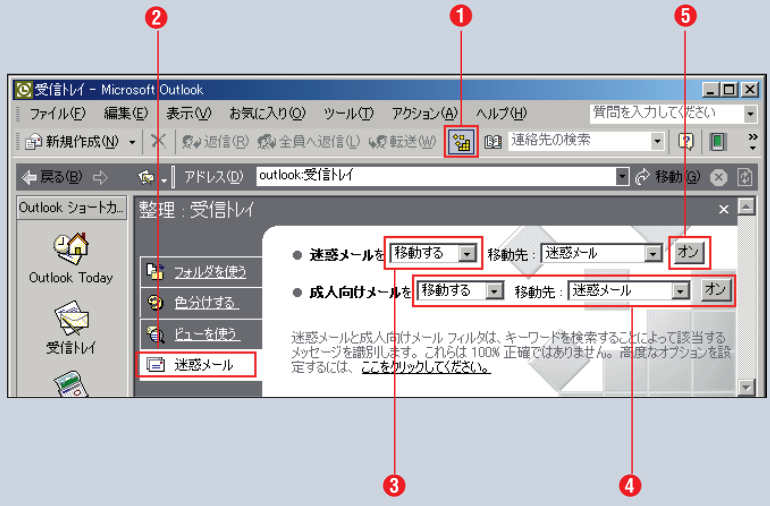
❶ツールバーの「整理」ボタンを押す。

❷整理設定が開くので「迷惑メール」を選ぶ。

❸迷惑メールに「移動する」を、移動先に「迷惑メール」を選ぶ。

❹「オン」を押すと振り分けフォルダー作成のダイアログが開く。そのまま「OK」を押すと「迷惑メール」というフォルダーができて振り分け先に指定される。

❺同様の手順を「成人向けメール」にも行う。



13 Outlook 2002でキーワードを使って振り分ける

難易度：★★★☆☆
費　用：\0

【ウィンドウズ】【Outlook 2002】

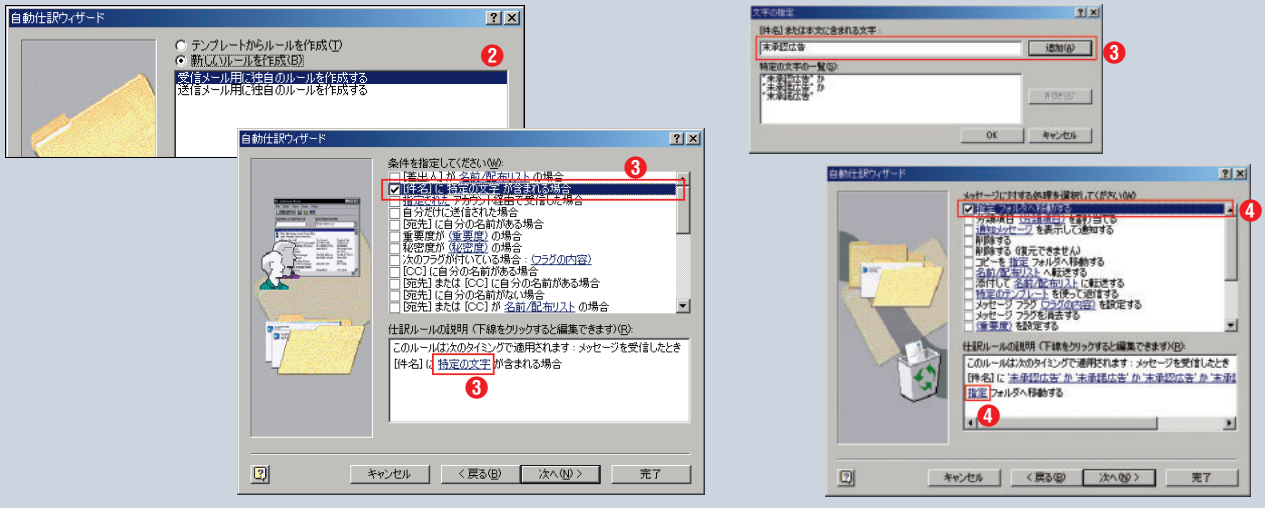
❶メニューから「ツール」→「自動仕訳ウィザード」を選んでウィザードを起動し、「新規作成」ボタンを押す。

❷「新しいルールを作成」で「受信メール用に独自のルールを作成する」を選んで「次へ」をクリックする。

❸「件名に特定の文字が含まれる場合」を選び、青い「特定の文字」をクリックし、続いてキーワードを「追加」していく。

❹ウィザードの次のページで「指定フォルダへ移動する」を選び、青い「指定」をクリックして「迷惑メール」フォルダーを選択する

❺「例外条件」はスキップし、「受信トレイ内のメッセージにルールを適用する」と「この仕訳ルールを有効にする」を選んで「完了」ボタンをクリックする。



はみだしスパムチェック6「gb2312」「big5」（Content-Typeヘッダー）：中国語のメールに用がない人向け。

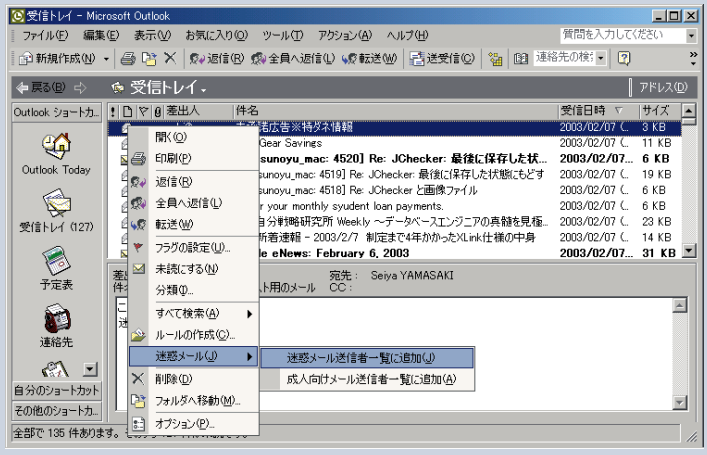
※Outlook 2002はオフィスXPに含まれるメールソフト

14 Outlook 2002でブラックリストを使って振り分ける

難易度：★☆☆☆☆
費　用：\0

【ウィンドウズ】【Outlook 2002】

❶受信トレイに来た迷惑メールを選択して右クリックする。
❷メニューから「迷惑メール」→「迷惑メール送信者一覧に追加」を選ぶ。
❸そのメールの受信者がブラックリストに追加され、次に同じ送信者から出されたメールは自動的に迷惑メールとして扱われる。
❹迷惑メール送信者一覧を確認するには、「ツール」→「自動仕訳ウィザード」メニューを選び、「迷惑メールのルール」を選んでルールの説明のボックスで「迷惑メール送信者」をクリックする。

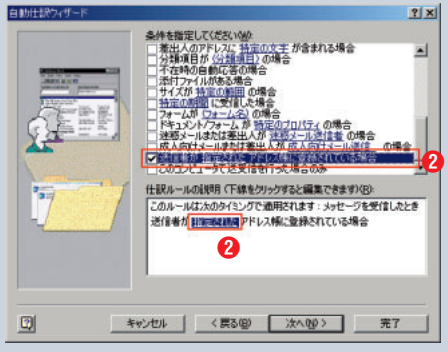


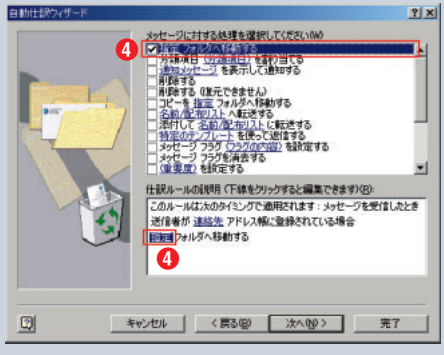
15 Outlook 2002でホワイトリストを使って振り分ける

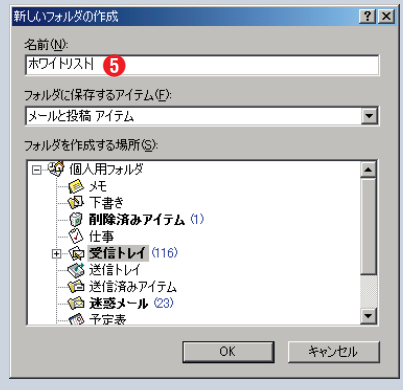
難易度：★★☆☆☆
費　用：\0

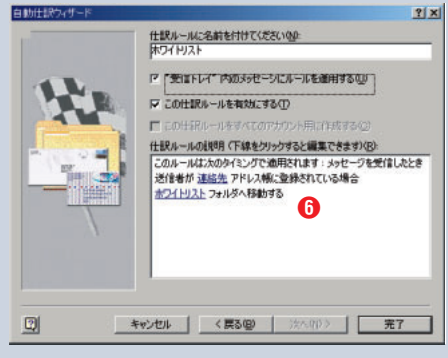
【ウィンドウズ】【Outlook 2002】

❶テクニック13の手順1と2と同様にして自動仕訳ウィザードを進める。
❷条件として「送信者が指定されたアドレス帳に登録されている場合」を指定し、仕訳ルールの説明で青い「指定された」をクリックする。
❸「アドレス一覧の追加」画面が表示されるので、「連絡先」もしくは「Outlookアドレス帳」を選び「次へ」ボタンを押す。
❹メッセージに対する処理として「指定フォルダへ移動する」を選び、仕訳ルールの説明で青い「指定」をクリックする。
❺振り分け先の画面が表示されるので「新規作成」を選び、「ホワイトリスト」フォルダを作る。「次へ」ボタンをクリックする。
❻「例外条件」はスキップし、仕訳ルールに「ホワイトリスト」と命名する。「完了」ボタンを押して終了する。









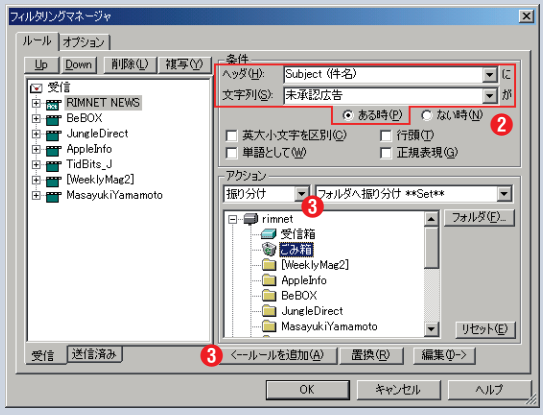
はみだしスパムチェック7「自宅で高収入」(件名／本文)：おいしい話には罠がある。

※Becky! 2はシェアウェアのメールソフト（URL http://www.rimarts.co.jp/index-j.html）

16 Becky! 2でキーワードを使って振り分ける

難易度：★★★☆☆
費　用：\0

【ウィンドウズ】【Becky! 2】

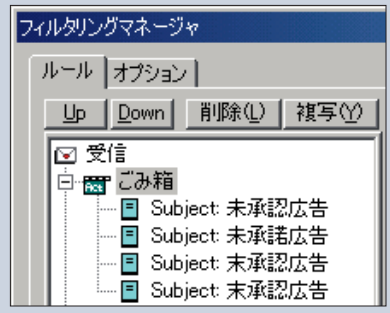


❶「ツール」メニューから「フィルタリングマネージャ」を選ぶ。

❷メールの件名で振り分けをする場合は、「ヘッダ」で「Subject」を選び、「文字列」にキーワードを指定してから、すぐ下の「ある時」にチェックをする。

❸同じ画面のアクション欄で「振り分け」で「フォルダへ振り分け」を選択し、「ごみ箱」を選んでから「<--ルールを追加」ボタンをクリックする。

❹同様にしてルールを追加していく。正規表現も使えるので、詳しい人ならかなり凝ったフィルターも作れるはずだ。追加したルールは左側に表示され、後から編集することもできる。



17 Becky! 2でホワイトリストを使って振り分ける

難易度：★★☆☆☆
費　用：\0

【ウィンドウズ】【Becky! 2】

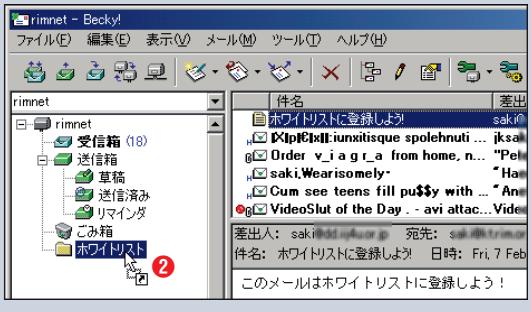
Becky!ではアドレス帳を振り分けに利用できないので、フィルタリングマネージャーで1つ1つ設定しなければならない。しかし、ALTキーを押しながらメールをドロップすると、簡単にメールアドレスを振り分け条件に追加できる。

❶「ファイル」メニューから「フォルダ」→「新規作成」を選び、「ホワイトリスト」というフォルダーを作成する。

❷「受信箱」でホワイトリストに登録するメールを選び、キーボードのALTキーを押したまま「ホワイトリスト」フォルダーにドラッグする。

❸「フォルダへの振り分けルール」画面が表示されるので、ヘッダーで「From」を選べばあとは自動的に補完してくれる。

❹2～3を繰り返して、複数のメールアドレスを登録していく。



18 Becky! 2のAntiSpamプラグインでスパム防止

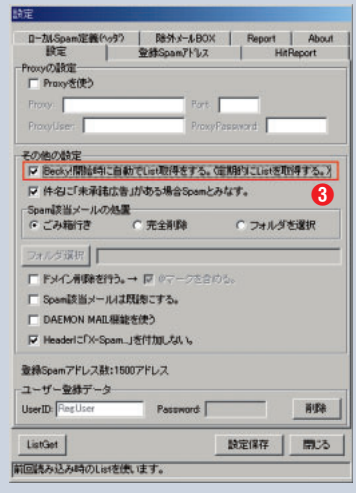
難易度：★☆☆☆☆
費　用：\0

【ウィンドウズ】【Becky! 2】

❶「AntiSpam」プラグインをダウンロードしてインストールする。

❷Becky! 2の「ツール」メニューから「プラグインの設定」→「Anti Spam Plug-in」を選ぶ。

❸インストールするだけで機能するが、「設定」タブで「List取得」を選んでおくと新しい種類のスパムにも対応できる。また、Spam該当メールをごみ箱以外に入れるときは、ここでフォルダーを選択できる。あとは普通にBecky! 2を使えばいい。



AntiSpamプラグイン（フリーソフト）

URL http://homepage1.nifty.com/redwing/

はみだしスパムチェック8「make money」「money-back guarantee」（本文）：英語のメールに用がない人ならなおさら。

※MailはMac OS X付属のメールソフト

19 Mac OS XのMailで迷惑メール防止機能を使う

難易度:★★☆☆☆
費　用：\0

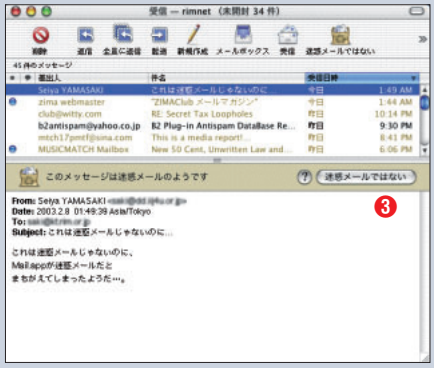
【Mac OS X】【Mail】

❶Mac OS Xの付属メールソフト「Mail」は、内蔵の迷惑メール防止機能が標準状態で稼働している。最初のうちは、この機能をトレーニングしていく。

❷スパムなのに迷惑メールと判断されなかった場合には、メニューから「メッセージ」→「迷惑メールにする」をクリックする。

❸ふつうのメールなのに迷惑メールと判断された場合には、メールに表示されている「迷惑メールではない」をクリックする。

❹迷惑メール判断の精度が高くなったら、「Mail」メニューから「迷惑メール」→「自動」を選んで自動モードに移行しよう。



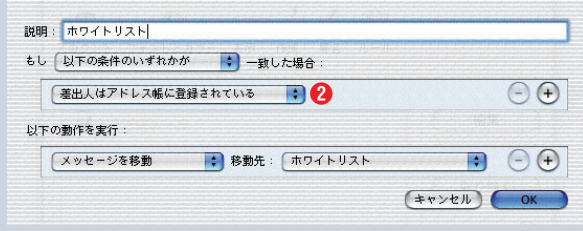
21 Mac OS XのMailでホワイトリストを使って振り分ける

難易度:★★☆☆☆
費　用：\0

【Mac OS X】【Mail】

❶テクニック20のブラックリスト作成の手順1〜2と同様にして、ルール作成画面を呼び出す。

❷「差出人はアドレス帳に登録されている」を条件にして、移動先を指定する。



「差出人はアドレス帳に登録されていない」をルールに使うと、ホワイトリスト登録者をメインのメールボックスへ、それ以外のメールを特定のメールボックスへトラップさせることも可能だ。

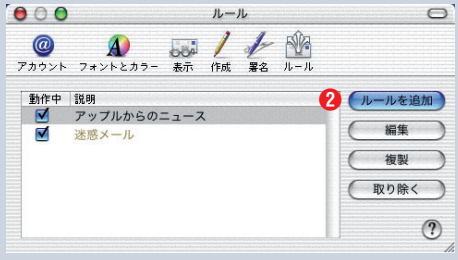
20 Mac OS XのMailでブラックリストを使って振り分ける

難易度:★★★☆☆
費　用：\0

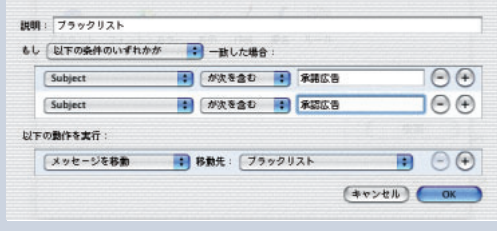
【Mac OS X】【Mail】

Mailでは、Outlook Expressなどのように手軽に「送信者を禁止する」機能がないので、振り分け機能を使う。ブラックリストに登録するメールアドレスやキーワードを振り分けルールに設定していく。

❶「Mail」メニューから「環境設定」を選ぶ。



❷「ルール」アイコンをクリックして画面を切り替えて、「ルールを追加」ボタンをクリックする。



❸条件を入力し、移動先を指定する。

❹2〜3を繰り返して、複数のメールアドレスを登録していく。

はみだしスパムチェック9「adults only」「100% satisfied」(本文)：成人向けの内容を避けたい人向け。

番外編　サーバー側でできるスパム対策

22 メールサーバーの常識：第三者中継の拒否

難易度：★★★★★
費　用：\0

【OSを問わない】【メールサーバーを問わない】

インターネット上でメールを目的のサーバーまで届けるために使われるSMTPでは、本来はパスワードなどの認証は必要ない。
つまり、スパム送信業者は自分のメールサーバーを使わずに、どこか適当なメールサーバー(MTA)を利用して大量のスパムを送信できる。これを「第三者中継」や「踏み台」と呼ぶ。踏み台にされたメールサーバー側では、関係のないスパム送信業者によって送信される。場合によっては数百万件ものメールの送信処理にネットワーク資源を使われて通常のメール配信に影響が出る。スパムが送信者情報を詐称していた場合、スパムを受け取ったユーザーからの苦情が来る。スパム送信を許しているサーバーとしてブラックリストに登録され、他のサーバーにメールを送れなくなるかもしれない。
スパムに荷担してしまわないように、メールサーバーを管理する場合は第三者中継、つまり正式な利用者以外がメールサーバーを悪用することを拒否するようにサーバーを設定しなければいけない。設定方法についてはメールサーバーによって異なる。

23 SurfControlでメールフィルター

難易度：★★☆☆☆
費　用：\400,000〜

【ウィンドウズNT／2000】【メールサーバーを問わない】

アスキーソリューションズによるプロキシー型のメールフィルター。送受信されるメールはすべてSurfControlがフィルターする。スパム対策だけでなく情報漏洩や添付ファイルのチェックなどにも対応している。GUIで設定でき、レポートなどがグラフィカルに表示できるのが特徴。ただしスパム対策機能はRiskfilterオプションが必要。初年度50ユーザー40万円から。

URL http://www.filtering.jp/email/

24 MailShieldでメールフィルター

難易度：★★★☆☆
費　用：\650,000程度

【各種OSに対応】【メールサーバーを問わない】

ウィンドウズ、Solaris、Linux、FreeBSDなどに対応したメールプロキシーサーバー。ヘッダー偽造やアドレス詐称などのチェック、RBLなどのブラックリストを使ってスパムを検知して受け取りを拒否したり、Subjectにラベルを付けたりできる。米Lyris Technologies URL01 の製品で、日本語版はSynaptive Technologies URL02 が開発／販売、Activewave Technologies URL03 が販売をしている。1サーバーあたり約65万円、試用版あり。

URL01 http://www.lyris.com/
URL02 http://www.awavetech.com/mailshield/
URL03 http://www.synaptive.net/jp/mailshield/

25 TMDAで「確認後配送」を使う

難易度：★★★★★
費　用：\0

【Unix系OS／Solaris】【各種メールサーバーに対応】

Jason R. Mastaler氏によるフリーソフトで、ブラックリスト、ホワイトリストを使ったメールのフィルターを持つ。TMDAとはTagged Mail Delivery Agentを表し、どちらのリストにもない人から送信されたメールをいったん保留して送信者に確認のメールを自動的に送り、送信者がそのメールに返事をすると、送信者の確認がとれたものとしてメールを配信する仕組み。その際送信者がホワイトリストに自動的に追加される。送信者が必ず1回は確認の処理をしなければいけないが、スパム対策としてはすぐれた手法だ。qmail、Postfix、Exim、Courier、SendmailなどのMTAに対応。

URL http://tmda.net/

これらのサーバー用のテクニックは、エンドユーザーが自分ですることではないので詳細な解説は省略した。もし自分でメールサーバーを管理していて、エンドユーザーがスパムに煩わされないようにしたいならばどれも有効な手段なので、詳細を検討してみてほしい。誌面の都合上紹介しきれなかったが、トレンドマイクロのInterScan Messaging Security Suite URL01 （ウィンドウズ用プロキシー、5,930円/ユーザーから、最低ユーザー数25人）や、各種メールサーバーに対応したフリーのスパム対策フィルターのSpamAssasin URL02 など、優れたツールはほかにもある。

URL01 http://www.trendmicro.com/jp/products/gateway/imss/
URL02 http://spamassassin.org/

はみだしスパムチェック10 「Viagra」「inkjet cartridges」「printer cartridges」（件名）：よく来るスパムのキーワードをうまく見つけよう。

［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