特定電子メール等による電子メールの送受信上の支障の防止に資する技術の研究開発及び電子メールに係る役務を提供する電気通信事業者によるその導入の状況

平 成 ２ ２ 年 ３ 月

総 務 省 総 合 通 信 基 盤 局
電気通信事業部消費者行政課

はじめに

迷惑メールの送信に対処するために、2002 年(平成 14 年)に、特定電子メールの送信の適正化等に関する法律(平成 14 年法律第 26 号。以下「特定電子メール法」という。)が制定された。2005 年(平成 17 年)の第 1 次改正では、その後の迷惑メール送信の悪質化、巧妙化にかんがみ、特定電子メールの範囲の拡大や架空電子メールアドレスあての送信禁止範囲の拡大、送信者情報を偽って送信することの禁止及びこれに違反した者に対する刑事罰の導入が行われた。このような法律の改正や、新たな迷惑メール対策技術に対する総務省の法令解釈を踏まえ、インターネット接続事業者(以下「ISP」という)における迷惑メール対策技術の適用も拡大されてきた。

さらに、2008 年(平成 20 年)には、特定電子メール法の第 2 次改正が行われ、オプトイン方式の導入のほか、罰則の強化等の法の実効性の強化、国際連携の強化が行われた。

民間では、移動系・固定系の主要な ISP 及びソフトウェア・ハードウェアメーカーなど約 30 社は、2005 年(平成 17 年)3 月に、迷惑メール対策グループ JEAG(Japan E-mail Anti-abuse Group。以下「JEAG」という。)設立した。JEAG では、2006 年(平成 18 年)2 月に、迷惑メール撲滅に有効な技術の導入方法、運用情報などを取りまとめたリコメンデーション(提言書)を策定し、迷惑メール撲滅に向けた具体的な対策を連携して行うことを促している。その対策の一つである Outbound Port 25 Blocking(以下「OP25B」という)に関しては、すでに国内の主要な ISP では導入されており、我が国発の迷惑メール送信比率の低下に大きく貢献している。

また、2008 年(平成 20 年)11 月に、迷惑メール対策に関する関係者が幅広く集まり、関係者間の緊密な連絡の確保、最新の情報共有、対応方策の検討、対外的な情報提供などを行うことを目的とした「迷惑メール対策推進協議会」(座長：新美育文明治大学教授) が設立された。同協議会では、第１回会合で、迷惑メールの追放に向けた決意と具体的に講ずるべき措置等をまとめた「迷惑メール追放宣言」を採択し活動を開始している。

これらの状況や迷惑メールを取り巻く環境なども踏まえ、迷惑メール対策関連技術及びこれらを活かしたサービス並びにそれらのサービスの強化、向上について、昨年に引き続き調査を行ったのでここに報告する。

―――――― 目　　次 ――――――

第１章　迷惑メール対策の技術動向に関する調査

迷惑メール防止に関する技術は、ISP が自社ネットワークから迷惑メールを送信させないようにするための技術(第１節)と、ISP や受信者側で迷惑メールを受信しないための技術(第２節)に大別される。

第１節　迷惑メール送信防止のための技術動向

各 ISP では、自社ネットワークからの迷惑メール送信が行われないよう種々の対策を行っている。本節では、その主な取組や技術について解説する。

１　送信トラフィック制御

大量のメールの一括送信を阻止するために、同一アカウントからの送信量を制御する方法である。

１．１　入会後の期間限定型制御

入会後の一定期間は、一度(一日等)に送信できる通数を制限するもの。

迷惑メール送信者は、ISP を渡り歩いて送信することが一般的なので、このような制御も一定の抑止効果が得られる。

１．２　連続メール送信制御

一定期間内に送信されるメールの通数を制御するもの。

制限に達するまでは自由に送信できるが、その後、当該アカウントからのメール送信を制限する。その制限期間及び制限する通数は、各 ISP で状況に応じ適宜定められる。実際の適用に当たっては、常に同じ基準をすべての送信者に適用するのではなく、臨機応変できめ細かい対応が望ましい。

２　送信者認証

一般的なメール送信プロトコル(SMTP: Simple Mail Transfer Protocol)では、送信者の認証が行われないため、送信側の ISP で、自社メールサーバから送信しようとする送信者に対して認証を行う方法である。

２．１　POP before SMTP

メール受信時に行われる POP(Post Office Protocol)の認証を利用し、その認証が行われた IP アドレスからの送信を一定時間許容するもの。

サーバ上で新たな技術を要しないので導入が簡単であるが、認証された一定時間以内に別の利用者に同一 IP アドレスが割り当てられたり、認証された同一 IP アドレスを共有し、ローカルアドレスで動作する LAN の別の PC 等から送信したりする場合であっても、認証されたものとして送信ができてしまうというセキュリティ上の弱点があり、本方式を廃止する ISP も出ている[1]。

２．２　SMTP AUTH (SMTP Authentication)

既存の SMTP プロトコルを拡張して、認証機能を追加したもの。サーバ側及びクライアント側の対応が必要となる。

後述する OP25B に関連して、Submission Port(投稿ポート)587 番を利用するが、この提供に際しては、SMTP AUTH を必須である。なお、587 番ポートで SMTP AUTH を使用する際、暗号化処理のできないメールソフトもあり、この場合インターネット上に、ID とパスワードが平文で流れてしまうことに注意する必要がある。

OP25B に伴い、ISP のメールサーバを使った迷惑メール送信の可能性が出てきたことや、セキュリティ上の問題もあり、自社サーバ利用のユーザに対しても、最初のメール設定時点で SMTP AUTH 機能を利用するよう誘導する ISP も多い。

---

[1] JEAG ではこの方式を推奨しておらず、JEAG Recommendation ~OP25B について~(p.16)では「MSA の Submission Port (587 番ポート)では、SMTP AUTH の代用として POP before SMTP を提供してはならない。」としている。

３　OP25B（outbound Port 25 Blocking）

迷惑メール送信者は、契約先の ISP のメールサーバを経由させずに、動的 IP アドレスを割り当てられた自前で設置するメールサーバから直接メール送信を行うことが多い。このため、ISP のメールサーバを経由しない動的 IP アドレスからのメール送信を行わせないようにするのが、OP25B である。

この場合、当該 ISP の正当な利用者であっても、他の ISP アカウントや会社・学校等のアカウントでメールを送信することができなくなってしまうこととなり、これが、本技術導入を進めていく上での大きな課題であった。

これに対処するためには、OP25B を実施する ISP ではなく、利用者が利用したい先の(他の ISP や会社の)メールサーバにおいて、メール配信用ポート 25 番に替わる 587 番ポートを認証機能(SMTP AUTH)必須として利用可能とするとともに、利用者の使用しているメールソフトの設定変更、さらに、587 番ポートの使用が不可能なメールソフトを用いている場合にはそれが可能なメールソフトへの変更が必要となる。

このため、すべての通信に適用する前に、前記のような問題の生じにくい携帯電話向けのメールに対する OP25B が進められた。また、PC 向けメールの OP25B 導入を進めていく前提として、他社の導入時に自社ユーザが影響されることのないよう Submission Port 587 + SMTP AUTH の導入を多くの ISP やレンタルサーバ提供会社が進めてきた。

このような状況の中で、2006 年(平成 18 年)を境に OP25B の導入が進み、現在までの導入状況は、図 1-1 に示すとおりとなっている。

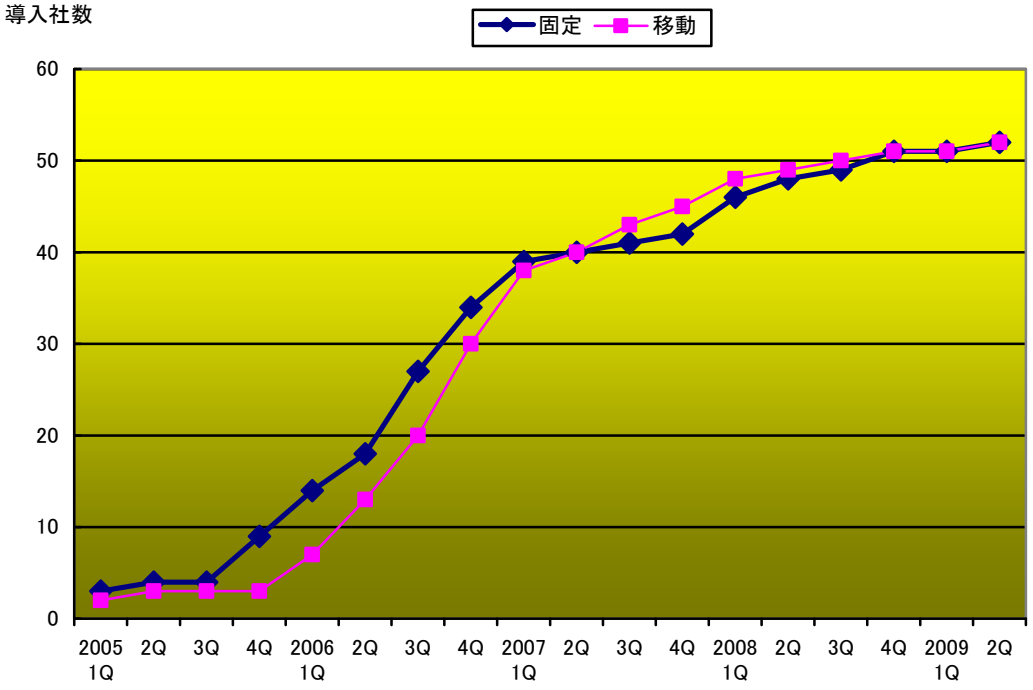

図１－１　国内 ISP の OP25B 導入推移

３．１　OP25B の導入効果

OP25B の導入効果について、(財)日本データ通信協会では、情報提供された携帯電話あての違反メールを分析することで検証している。

図１－２は､迷惑メール送信国における日本の順位である｡これをみると、日本の順位が低下していること、その傾向が、前掲の図１－１の増加傾向とほぼ逆相関関係にあることが分かる。これは、OP25B による対策で、国内からの迷惑メール送信が困難となってきたものとも考えられる。

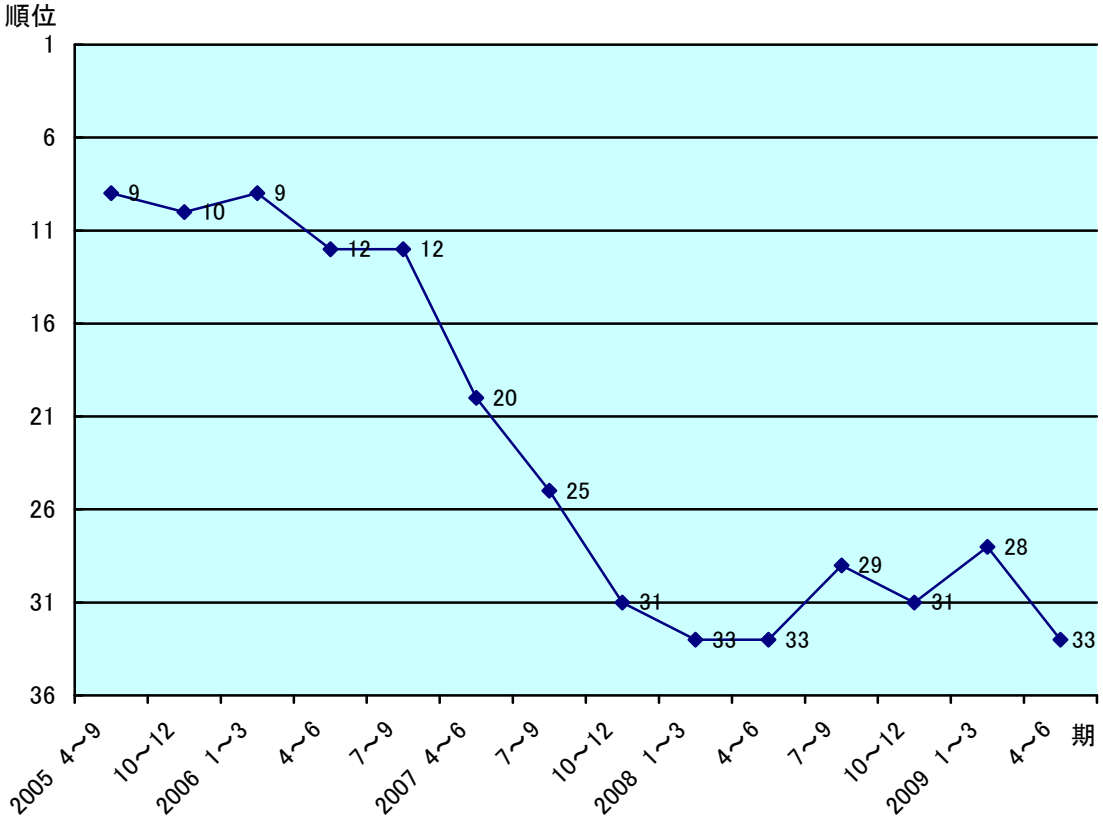

図１－２　スパム送信国における日本の順位

また、ある ISP での OP25B の導入に伴い、迷惑メール送信者が OP25B を導入していない他の ISP へと移動している状況が見られた(図１－３)。

ISP A の OP25B の導入とともに、ISP A から送信される迷惑メール比率が減少し、１ヶ月でほぼ０のレベルとなっている。一方で、ISP A から送信される迷惑メール比率が減少するのに呼応して ISP B の比率が増加している。暫くすると ISP B から送信される迷惑メール比率も減少に転じ、今度は ISP C の比率が増加している。

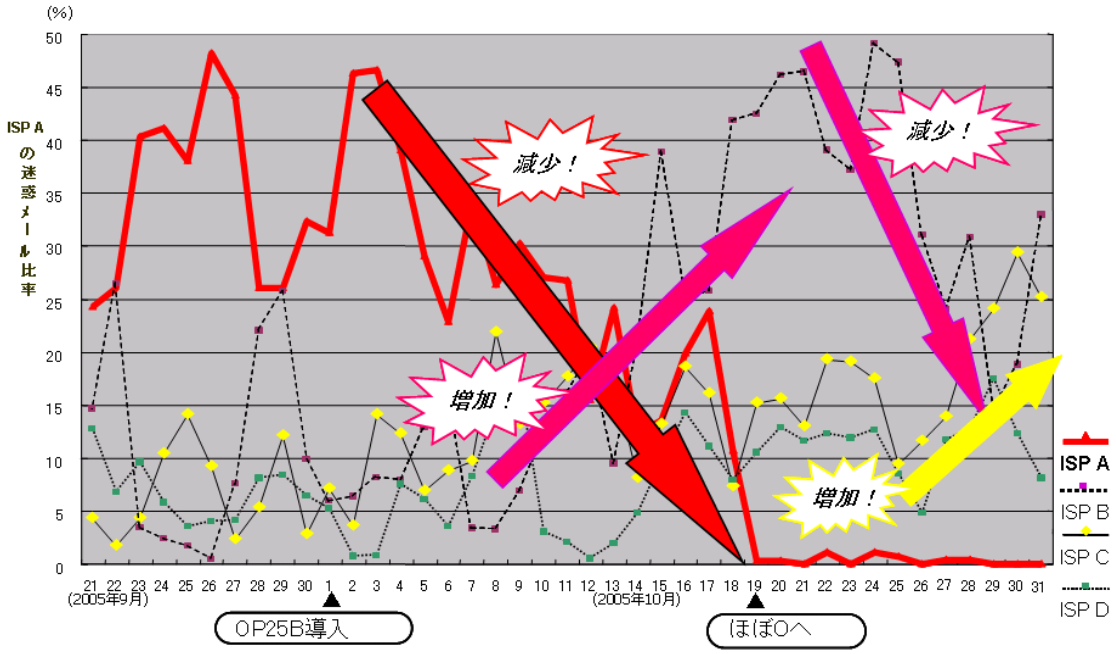

図１－３　OP25B 導入効果

第２節　迷惑メール受信防止のための技術動向

１　迷惑メール判定技術の概要

受信するメールを迷惑メールと判定する技術については、比較的容易に行うことができ、一定の効果のある判定技術として、以下の 3 つがある。

(1)メール容量制限

受信メールの容量(サイズ)により判定するもの。画像情報等大容量の情報を含むメールを受信しないよう上限値を超える容量のメールや、下限値に満たない少ない容量のメールを受信しないようするものである。

(2)添付ファイル制限

添付ファイルの有無により判定するもの。添付ファイルとしてウイルスなどが添付されている場合があるので、その感染の防止を目的としている。

(3)URL 有無制限

サイトへ接続可能な URL の有無により判定するもの。URL をクリックすること等による不本意なサイトへの接続の防止を目的としている。

しかし、大きな容量のファイルを受信する必要がある場合や、添付ファイルが必要な場合、URL 情報が必要な場合も日常的にあることから、これらの方法による対応では、日常のメールの使用に不便を来すこともある。

本節では、迷惑メール判定技術のうち、よりきめの細かい高度な技術で、ISP のメールサーバや、受信者の PC 内部で行われるものを取り上げる。

迷惑メールの判定処理は概ね次の手順を踏むことが多いので、その順に解説する。最後に前述の OP25B と対照をなす Inbound Port 25 Blocking(以下「IP25B」という)について概説する。

(1)迷惑メールであることの判定技術

(2)誤判定防止のための判定除外

(3)判定後の処理

２　迷惑メールであることの判定技術

２．１　キーワード(ブラックワード)判定

メールのヘッダ及び本文中の特定のキーワードに合致するものを迷惑メールと判定するもの。迷惑メールの判定に当たり、外部データベースを利用する必要がないため、受信者の PC 上で動作するメールソフトで使用されることが多い。

キーワード判定は、本来、迷惑メールを判定するためのものでなく、メールの内容に応じた振分けのための機能であるが、きめ細かい設定により、また、他の判定技術やホワイトリストと組み合わせることで、迷惑メール判定技術としても十分機能するものとなる。このため、メール本文で判定する場合には、正当なメールを迷惑メールと誤判定しないようにするため、複数のキーワードでの判定、その他の条件(URL の有無等)と組み合わせた判定、後述するホワイトリストとの併用が効果的である。

ブラックワードだけで迷惑メールを判定しようとすると、悪意ある送信者は人間には判読できるが PC ソフトでは判読できない文字列を使用して、ブラックワードではないと誤判断させてしまうことも起きるため、複数の設定条件を組み合わせて判定できるようにすることが効果的である[2]。

ただし、大部分の ISP 及び PC のメールソフトが提供している機能では、判定するための項目が不十分であったり判定条件の設定数が少なすぎたりするので、迷惑メール対策としては実用的でない場合も多い。

なお、ヘッダ上で指定する対象としては、一般的に、以下のような項目がある。

- 送信者(from)アドレス、送信者ドメイン
- 件名(subject)
- あて先(to)、写し送付先(cc)
- 時刻(date)
- Received ヘッダ
- 拡張ヘッダ(テキスト形式、文字コード、使用メールソフト　等)

２．２　送信元情報参照による判定

メールの送信元情報を参照し、迷惑メールであるかを判定するもの。

２．２．１　ブラックリスト(RBL：Realtime Black List)による判定

迷惑メール送信元として知られる IP アドレスをまとめたリストからのメールを、迷惑メールと判定するもの。

---

[2] replica を“r_e_p_l_i_c_@”とすることで replica とは判断できずにパスさせてしまうことなど。

このリストとして外部機関の提供するRBLの利用が一般的であり、数多くのRBLが存在している。これにより、送信元のIPアドレスがRBLに含まれているかどうかを確認し、該当するメールを迷惑メールと判定する。

受信メールサーバ側において、メール受信処理の最初の段階で送信元のIP アドレスが判明することから、本方式の場合、メール本文を受信せずに速やかに迷惑メール判定を行うことが可能となり、受信メールサーバ側の処理負荷が少ないことが特徴である。しかし、ブラックリストへの登録は、誤登録の可能性が残ることや、動的IPアドレスが登録されてしまうと、その後、そのIPアドレスを割り当てられた無関係な利用者からのメールも迷惑メールと判定されてしまうこと等の課題もあり、ブラックリストのみでの迷惑メール判定は行うべきではなく、他の判定技術や後述するホワイトリストとの併用が必須である。

２．２．２　グレーリストによる判定フィルタ

受信メールサーバでメールを受信する際に、既知の送信メールサーバからの場合は正常に配信を行い、未確認のメールサーバに対してのみ配信を一時的に拒否するもの。送信側のメールサーバでは、本来ならこの応答を適切に扱い、少し後に配送を再試行するが、不正なメールサーバの場合再配送しないことが多いため、迷惑メールをブロックできる。

このグレーリストの欠点としては、正当なメールであっても、過去にメールを受け取ったことのない人からのメールが、受信に当たって数時間遅延してしまうという点にある。

２．２．３　送信ドメイン認証

自社のメールドメインから発信されるメールに対して、メールドメインの認証を付与することで、メール受信側のサーバに対して、自社サーバから送付されたメールであることを保証できるようにするもの。受信メールサーバ側は、送信ドメインが認証されたメールを受信した場合、当該ドメインからの送信であることを確認できる。

一般に、迷惑メール送信者は送信元を詐称するため、このようなISPのドメインを騙ったメールであれば、受信側のサーバで送信元が詐称されたメールであると判定できる。

本技術の導入により、直ちに、迷惑メール送信が行われないようになるものではないが、大多数のサーバが導入する状況となった時には、送信認証すらしない“怪しげな”サーバの識別が可能となるとともに、送信認証してまで迷惑メールを送信してくる送信者に対して、その“認証された”身元となるドメインを識別可能とすることが可能となる。

送信ドメイン認証には、主に２つの方式がある。それぞれ長所短所があることから、両方式の特徴を踏まえた相互補完的な利用が望ましい。

２．２．３．１　SPF(Sender Policy Framework)

送信メールサーバをその IP アドレスから認証するものである。

送信メールサーバは、自ドメインに対する IP アドレスを DNS サーバの SPF レコードに記述する。受信メールサーバでは、メールが配送されてくる送信側の IP アドレスと、メールに含まれるドメイン情報により DNS 検索した IP アドレスとを比較することで、そのメールのドメインの認証を行うことが可能となる。

本方式は、送信側における DNS への SPF レコードの追加作業と受信側における DNS の検索作業で実現可能であり、次に説明する DKIM に比べ、相対的に導入が容易である。

特に、送信側は DNS への登録だけで済むので、積極的な登録が望ましい。この SPF 登録については、まず、ISP から導入が進んでおり、現在では、主要 ISP では概ね実施されている。

一方で、受信側では、相対的に容易ではあるものの、メールフィルタ(認証ソフト)の導入が必要であり、まだ、受信側での対応は進んでいないのが現状である[3]。

本方式の課題として、メール転送時には送信元情報が変更される場合もあるため、認証できなくなる点がある。

２．２．３．２　DKIM (Domainkeys Identified Mail)

送受信メールサーバ間で公開鍵暗号化技術を用いて送信ドメインの認証を行うものである。

送信メールサーバは、あらかじめ自ドメインに対する公開鍵を DNS に登録するとともに、メールを送る際に、秘密鍵でデジタル署名を付加する。受信メールサーバでは、デジタル署名されたメールが配送された時点で、その送信ドメインから DNS 検索を行い、公開鍵を取得し、その署名内容を検証することで、そのメールのドメイン認証を行うことが可能となる。

本方式は、秘密鍵の作成管理を行う送信側に負担がかかるほか、送受信側で鍵の「署名」「検証」処理機能を追加する必要があり、SPF に比べると、相対的に経費負担が大きい。

本方式の課題として、メーリングリスト利用時に署名情報が改変されるため認証ができなくなる点がある。

２．２．３．３　送信側での設定状況

WIDE Project[4]の Anti-spam Working Group では jp ドメインにおける送信ドメイン認証への対応状況を毎月報告している。それによると SPF の 2010 年１月現在の普及率は 37.7%となっており[5]、上昇傾向が続いている。この普及率の上昇傾向はセカンドレベルドメインの全ての型に共通しており、各団

---

[3] 2008 年(平成 20 年)8 月、国内の大手 ISP(D社)が、自社で設計・開発した、商用環境でも安定的に稼働するメールフィルタプログラムを無償で提供することを発表している。

[4] http://www.wide.ad.jp/index-j.html

[5] http://member.wide.ad.jp/wg/antispam/stats/index.html.ja

体へ意識が浸透してきていることが窺える。特に登録数の大きい co ドメインと or ドメインの上昇が大きく全体の上昇牽引力となっていることが分かる。今後ともこの傾向が続くことが望まれるが、関係者の一層の啓蒙活動が重要である。[6]。

２．３　レピュテーション (Reputation)

実際の迷惑メールの情報を基に構築した「信用度(レピュテーション)データ」を用いて、IP アドレス又はメールが経由してきたサーバの情報から、迷惑メール判定を行うもの。数十万件のメール発信元のサーバについて、過去の送信履歴から迷惑メールを送ったかどうかを判断し、そのサーバのメール送信パターン、オープン・プロキシやセキュアでないメールサーバの存在、メッセージの送信量及び苦情などのデータなどからレピュテーションの格付けをする。

２．４　内容参照による判定

主にメールの内容を検査し、流通する迷惑メールから分析した情報に基づいて迷惑メールかどうかを判定するもの。

２．４．１　ベイジアンフィルタ (Bayesian Filter)

メール受信者が迷惑と判定したメールを基に迷惑メールの判断基準を自己学習し、迷惑メールであるかどうかを統計学的に判断するもの。“迷惑メールである”“迷惑メールではない”と判断された基準にしたがい、以後のメールにおいて自動的に解析・分類していく。使用し続けることで、迷惑メール判定の精度が高まり、ユーザの利用状況に合わせた効果的な判定が可能となる。

しかし、昨今の迷惑メールにおいては、文章を画像化したり、問題となりそうな単語を人間であれば読み取れる程度の誤字で表現したり、関係のない長い文章を後方部分に載せるなどしてベイジアンフィルタを撹乱するものもあり、フィルタ側でも対応を図っているが、それでも、さらに攪乱させるようなものも出てきている。

２．４．２　ヒューリスティックフィルタ (Heuristic Filter)

メールヘッダや本文からメッセージを解析し、そこから得られた迷惑メールの特徴などをスコア化し、スコアが一定以上の基準値を超える場合に迷惑メールとして判断するもの。

例えば、メールの送られてきた“道筋”が記録されている「Received フィールド」を確認し、“メールが届けられる過程でオープンリレー(中継可能な)メールサーバを経由している場合は、迷惑メールである確率が高い”といったルールを作ることができる。また、“メール本文において、URL が多用されている場合や HTML メールでかつ画像だけのケースを迷惑メールと

[6] http://member.wide.ad.jp/wg/antispam/stats/index.html.ja

する”といったルールを多数用意し、これらのルールと受信メールを比較し、迷惑メールらしさ(likelihood)を点数として表現する。こうして、それぞれのメールに対してこの点数を集計し、ある点数以上となったものを迷惑メールと判断する。

本方式の課題として、管理上の負担が非常に大きくなる点や、正しく判別するよう適切に処理をしないと、受け取るべきメールを誤って迷惑メールと誤認識するケースが多発しかねないという点がある。

２．４．３　シグネチャーフィルタ(Signature Filter)

多数の迷惑メールから、あらかじめ迷惑メール特有の「指紋」(シグネチャー[7])を抽出しておき、受信したメールと比較を行うことで、迷惑メールの判定を行うもの。シグネチャーは、実際の迷惑メールから作成されるため正確さが保持され、亜種の識別にも適用できる。

最新のシグネチャーフィルタは、メッセージのランダム化や、迷惑メール送信者がフィルタを逃れるために挿入するHTML形式の「ノイズ」(コメント、定数、不良タグ)に対抗できるように、まずメッセージからノイズ(コメント、定数、不良タグ)を除去してスケルトン化し、短い文字配列を抽出してその内容とシグネチャーデータベースを比較することにより、迷惑メールかどうかを判断させる方式となっている。メッセージの全体を視覚的に判定しないため、フィルタリング速度は速く、メールシステムの管理者による負担も少なく、高いシステムパフォーマンスを発揮する。

この方式の課題として、日々進化していく最新の迷惑メールに対しても適切な判断ができるように、シグネチャーデータベースについて、グローバルレベルでの収集体制が必要であり、また迅速かつ継続的な更新が常に行われていなければ有効性は低くなってしまう点がある。

また、ベンダーの提供する一連の対策製品に重要なことはその正確性であり、誤認識の低減又はユーザが受信すべきメッセージを失わない回避策や防護手段を備えることが必要である。そのため、技術バランスをよく組み合わせて過度に攻撃的なフィルタリングを避ける、スコア制の場合には、迷惑メールと判断するスコアを利用者が設定可能とするなど、絶えず判定性能を改善し、総合的な迷惑メール分析手法の技術を向上していくことが求められる。

２．４．４　URLコンテンツカテゴリ

メール本文中に含まれるURLでリンクされたサイトの内容を評価し、迷惑メールの宣伝対象となる特定のコンテンツを含む場合、迷惑メールと判定するもの。

判定は、URLフィルタ情報提供ベンダーが提供するURLブラックリストと受信メールの中に含まれるURLとを比較する。送信者が意図的に不要な文字を入れて難読化したり、見かけ上のアドレスに不正なURLを隠したりしてい

[7] 迷惑メールを数学的手法で分析し抽出した文字列や数値列の部分的な並びなどの特徴データとのこと

ないかを、メッセージに埋め込まれたアドレスのリンクから確認するため、フィッシング[8]の予防にも繋がる。一般的に、迷惑メールは URL が記述されたメールが多いため、判定基準としては有効である。しかし、このような不正なサイトのライフサイクルは短命で、URL がすぐに変化してしまうため、迅速な対応と継続的なデータベースの更新が必須である。

２．５　受信トラフィック制御

迷惑メールと判断されるメール受信のトラフィック量を制御するもの。

２．５．１　連続メール受信制御

迷惑メールは大量に送信してくることが多いため、特定 IP アドレスから一定期間内に送信されるメールの受信数を制御するもの。

ただし、最近の迷惑メール送信者の中には、数分～数時間単位で常時接続回線のセッション切断、再接続を行うことで、別な動的 IP アドレスを取得し、当該 ISP からみた特定 IP アドレスからの受信数を増やさない工夫をしている者もある。

２．５．２　エラーメール受信制御

特定の IP アドレスから、あて先不明なメールを受信した際に、次の受信を受け付ける時間を延ばしたり、あて先不明メールが多い場合は受信を行わないようにしたり制御するもの。

最近の携帯電話では、比較的簡単なアドレスとしても、迷惑メールが来ることはほとんど無くなったが、これは、各携帯電話事業者において、適切なエラーメール受信制御が行われていることも一因と考えられる。

ただし、非常に多数の適当なアドレスを送付して、エラーとならない有効なアドレスを収集する方法もある。

---

[8] phishing: 「釣り」を意味する fishing と詐欺の手口が「洗練された」という意味の（sophisticated）を合わせた造語。

３　誤判定防止のための判定除外

迷惑メールを判定する際には、以下のとおり、誤判定が必ず発生する。

(1)迷惑メールを正当なメールと誤判定する(false negative)

(2)正当なメールを迷惑メールと誤判定する(false positive)

(1)と(2)は相反するものであり、迷惑メール判定を緩く行うと(1)が増加し、迷惑メール判定を厳しく行うと(2)が増加する。

このうち、実際上大きな問題となるのは、(2)の場合が多いと思われる。(2)の問題については、個々のメール受信者特有の情報を元に、受信者にとっては迷惑メールとはならない要素をあらかじめリストアップしておき、この要素を含むメールを受信した場合に、それを無条件で正当なものとして迷惑メール判定処理を除外することで回避することができる。この受信者個々にあらかじめ用意した要素群をホワイトリストという。

なお、会社等においては、関連する送信者が共有できることから、利用者個々でなくそのサーバ単位でホワイトリストを設定することもある。

３．１　ホワイトリスト(送信者アドレス・ドメイン)

一般的に「ホワイトリスト」といわれているもので、送信者アドレス又は送信者のドメインを登録するもの。

登録する対象として、正当ではあるが迷惑メールと判定されそうな内容を送付してくる送信先とする必要がある。事前にリストアップすることは困難であるため、誤判定(false positive)されたら順次ホワイトリストに追加していく、という使い方が一般的である。

なお、PC 上のメールソフトでは、アドレス帳で管理している送信先メールアドレスを自動的にホワイトリストに登録できるものもある。

３．２　ホワイトリスト(ヘッダ、本文)

件名や本文中のキーワードを登録するもの。

メールマガジン等の送信者で、送信者アドレス・ドメインを複数使用しているものもあり、そのような場合は、件名や本文中のそのメールマガジン等固有のキーワードをリストアップすることで、対処が容易となる。

４　判定後の処理

迷惑メール判定後の処理として、以下の 3 方法がある。

(1)削除

　迷惑メールと判定されたメールを削除するもの。判定が確実であればよいが、誤判定(false positive)を考慮するとリスクが大きい。

(2)特定フォルダへ移動

　通常メールが受信されるメールフォルダでなく、別のフォルダに移動するもの。

　誤判定(false positive)を考慮したものであるが、ISP の提供する迷惑メール対策で提供されていて、PC 上でのメールソフトを使用している利用者の場合、適宜、ISP の当該フォルダにアクセスしてチェックする必要がある。

(3)ラベリング

　ISP が迷惑メール判定結果を、メールの件名又は拡張ヘッダに含ませるもの。例えば、件名の場合、件名の最初に[MEIWAKU]等の文字を付加する形式となる。

　この方法は、受信者自身又は PC 上のメールソフトでの振り分け処理を前提としたものである。なお、件名ラベリングは、サーバ上で判定を行う ISP のサービスだけでなく、PC 上のセキュリティソフトの迷惑メール機能でも採用されており、これは、多くのメールソフトで件名による振り分け設定が可能であることを前提としている。

　また、拡張ヘッダラベリングの場合、メールソフト側で拡張ヘッダを処理可能であることが前提となるが、メール一覧画面等で迷惑メールと判定されたメールに特有のマークを表示することや、誤判定の場合そのマークを消す等の処理が可能となり、より使いやすいものとなる。

５　IP25B（Inbound Port 25 Blocking）

ISPにおいて、OP25Bが、自ネットワークから、自社メールサーバを経由しない動的 IP アドレスからのメール送信を行わせないようにするものに対し、IP25Bは、その逆に、他ネットワークの動的 IP アドレスから送信されたメールを受信しない、というものである。

従って、当該 ISP の利用者が、他の ISP ネットワークや、会社・学校等からそのISPのアカウントでメールを送信することができなくなってしまうが、OP25Bの場合と異なり、当該ISPが、投稿用ポート587番(Submission Port 587)に認証機能を必須として提供すれば、利用者側の問題は生じない。

ただし、ブロックする他のISP等の動的IPアドレス情報は、個別に各社から取得する必要があるので、海外発信を含めて完全に実施することは困難である。

(参考)各種施策の法律上の見解

１　OP25B の実施に伴う法律上の見解

(1)　特定の通信に関する送信元 IP アドレス及びポート番号という通信の秘密を知得し、かつ、当該通信の秘密を、当該メールの接続拒否という送信者の意思に反して利用していることから、当事者の同意を得ない限り、「通信の秘密を侵す行為」に該当する。
(2)　受信側の ISP が自ら提供するメールサーバを適正に管理することによる大量送信の防止措置のみではネットワークの維持管理に不十分であれば、ネットワークを適正に維持管理してメールサービスを運営するために、自ら提供するメールサーバを経由しない動的 IP アドレスからの送信について送信制御を行う正当性、必要性が認められる。
(3)　侵害することとなる通信の秘密は、送信元(及びあて先)IP アドレスとポート番号であり、目的達成のために必要な限度にとどまるものであり、手段の相当性も認められる。
(4)　従って、OP25B は通信の秘密侵害行為に該当するものの、正当業務行為(違法性阻却事由あり)と解釈できるので、当事者の同意の有無に関わりなく、実施可能と考えられる。

２　ドメイン認証を受信側で実施することに伴う法律上の見解

(1)　送信ドメイン認証は、法律的に見れば「電子メールの受信メールサーバにおいて、電子メールの送信ドメインを認証(チェック)し、認証できない場合は一定の措置を講ずる行為」と解される。

(2)　送信ドメイン認証された電子メールの受信側での処理は、

ｉ　送信ドメインの認証

ii　認証結果のラベリング

iii ラベリングの結果等に基づくフィルタリング

の３段階に分けて考えることができる。iii については、当事者(受信者)の同意が必要である。

(3)　i、ii の行為についても、通信の当事者の同意を得ない限り、「通信の秘密」を「侵す行為」に該当する。

(4)　しかし、送信元を偽装した電子メールの大半が迷惑メールであること、及び、迷惑メールのほとんどが送信元を偽装していること等から、送信ドメインを偽装している電子メールは一時に多数のものに送信されていると推定できるので、i、ii の行為は、大量送信される迷惑メールにより生じるサービスの遅延等のメール送受信上の支障の恐れを減少させるための行為と認められ、送信ドメイン認証は、目的の必要性、行為の正当性が認められる。

(5)　また、i、ii の行為により侵害することとなる通信の秘密は、送信ドメインという通信の経路情報であり、ISP としての目的達成のために必要な限度を超えるものでないこと、及びその他の迷惑メール対策技術では対応できない場合があることから、手段の相当性も認められる。

(6)　したがって、i、ii の行為は、通信の秘密侵害行為に該当するが、正当業務行為(違法性阻却事由あり)と解釈できるので、当事者の同意の有無に関わりなく、実施可能と考えられる。

３　IP25B の実施に伴う法律上の見解

(1)　特定の通信に関する送信元 IP アドレス及びポート番号という通信の秘密を知得し、かつ、当該通信の秘密を、当該メールの接続拒否という送信者の意志に反して利用していることから、当事者の同意を得ない限り、「通信の秘密」を「侵す行為」に該当する。

(2)　受信側の ISP が自ら提供するメールサーバを適正に管理することによる大量送信の防止措置のみではネットワークの維持管理に不十分であれば、ネットワークを適正に維持管理してメールサービスを運営するために、他ネットワークの動的 IP アドレスからの受信について受信制御を行う正当性、必要性が認められる。

(3)　侵害することとなる通信の秘密は、送信元(及びあて先)IP アドレスとポート番号であり、目的達成のために必要な限度にとどまるといえ、手段の相当性も認められる。

(4)　したがって、IP25B は、通信の秘密侵害行為に該当するものの、正当業務行為(違法性阻却事由あり)と解釈できるので、当事者の同意の有無に関わりなく、実施可能と考えられる。

第２章　迷惑メールに関する移動系 ISP の対策導入状況

第１節　迷惑メール送信防止対策の導入状況

移動系 ISP 側で設定する迷惑メールに対する規制措置は、次のとおりである。なお、措置の発動基準や実績等は明確にしていない場合もある。

１　あて先不明メールの受信ブロック

移動系 ISP5 社は、あて先に実在しない大量のメールアドレスを含むメールは、事業者側の設備で受信拒否している。

２　送信通数規制

２．１　Ａ社

1 日 1 台当たりの送信を 1,000 通未満に制限している。これを超える送信については、送信者に対して「送信できませんでした。」等のメッセージが表示される。

２．２　Ｂ社

2G 方式では、3 時間以内に 120 件以上のあて先に送信した場合、以後 21 時間送信を規制している。3G 方式では、24 時間以内に 1,000 件以上のあて先に送信した場合、その後 24 時間送信を規制するとしていたが、2008 年(平成 20 年)3 月 27 日から送信できるあて先数を 500 件としている。

２．３　Ｃ社

1 日当たり 1,000 件以上のメールの送信が確認された契約回線について規制措置を実施していたが、措置の実施までの間にも大量送信が可能であることから、2004 年(平成 16 年)8 月からは、1 日当たりの送信件数の上限を一律に 1,000 件までとしている。

また、1 回の送信処理で同時に複数のあて先に配信できる機能について、迷惑メールの大量送信手段として利用されていることから、2003 年(平成 15 年)9 月から、それまで約 30 件だった同報送信あて先数を、5 件までに制限した。その後、メールフィルタの強化により迷惑メールが減少したとの考えから、2008 年(平成 20 年)1 月 16 日より、同報送信あて先数を 30 件に戻している。

２．４　Ｔ社

30 分当たり 100 件を超えるメールが送信された場合に利用停止などの措置を行っている。また、2004 年(平成 16 年)8 月から、1 日当たり 1,000 件

を超えるメールが送信された場合について利用停止などの措置を行っている。

３　メールアドレスの初期設定の変更

移動系 ISP の多くは、当初、契約時におけるメールアドレスの初期設定が、推測されやすい「電話番号@×××.ne.jp」であったが、現在では、5 社とも推測されにくい「複数のランダムな英数字@×××.ne.jp」としている。

４　自動転送先設定回数の制限

Ｃ社では、自動転送先設定機能を悪用した迷惑メールが送信されていたことから、転送先を設定(変更)できる回数を、2006 年(平成 16 年)6 月から 1 日 3 回までに制限している(機種により、最大 6 メールアドレスまで設定(変更)が可能)。

５　送信ドメイン認証の導入(送信側)

移動系 ISP5 社では、迷惑メール対策の一つとして送信ドメイン認証技術の導入を進めており、迷惑メール送信防止の対策の一つとして自社ドメインについて、DNS サーバへの SPF レコードの既述を実施している。

５．１　Ａ社

2005 年(平成 17 年)12 月より、DNS サーバへ「SPF レコード」の記述を実施。

５．２　Ｂ社

2006 年(平成 18 年)3 月より､DNS サーバへ｢SPF レコード｣の記述を実施。

５．３　Ｃ社

2005 年(平成 17 年)12 月より、DNS サーバへ「SPF レコード」の記述を実施。

５．４　Ｔ社

2006 年(平成 18 年)3 月より､DNS サーバへ｢SPF レコード｣の記述を実施。

５．５　Ｕ社

2008 年(平成 20 年)3 月より、DNS サーバへ「SPF レコード」の記述を実施

６　OP25B の実施

６．１　Ａ社

Ａ社では、2005 年(平成 17 年)6 月より、一部のインターネット接続サービスから移動系 ISP、固定系 ISP あてに送信されるメールについて、OP25B を実施している。さらに、2007 年(平成 19 年)1 月からは、公衆無線 LAN サービスから送信されるメールについても、OP25B を実施している。

また、2008 年(平成 20 年)7 月から、あるインターネット接続サービス(別途申込みが必要)を利用し 3G 方式からアクセスポイント接続経由で 25 番ポートを利用して送信されるメールについて、現行の 384kbps/回線交換 64kbps から概ね 10kbps 程度へ速度制限を開始している。

６．２　Ｂ社

Ｂ社では、2007 年(平成 19 年)12 月より、インターネット接続サービスから携帯電話あてに送信されるメールについて、OP25B を実施している。2008 年(平成 20 年)3 月からは、固定系 ISP あてのメールの送信についても、OP25B を実施している。

６．３　Ｃ社

Ｃ社では、2006 年(平成 18 年)6 月より、インターネット接続サービスから携帯電話(Ａ社、Ｂ社及びＣ社)あてに送信されるメールについて、OP25B を実施している。2008 年(平成 20 年)6 月からは、Ｔ社あてに送信されるメールについて、2008 年(平成 20 年)9 月下旬からは、固定系 ISP あてのメールについても、OP25B を実施している。

６．４　Ｔ社

Ｔ社では、2006 年(平成 18 年)5 月より、インターネット接続サービスから携帯電話あてに送信されるメールについて、OP25B を実施している。2008 年(平成 20 年)6 月からは、固定系 ISP あてのメールの送信についても、OP25B を実施している。

６．５　Ｕ社

携帯事業者向けには 2008 年(平成 20 年)3 月より OP25B を適用している。その他は 2009 年（平成 21 年）5 月より順次開始している。

第２節　迷惑メール受信防止対策の提供状況

移動系 ISP は、前節で紹介した自らが行う規制措置に加えて、迷惑メールのパターンや受信状況に応じた防止措置や、本来必要となるメールと迷惑メールの取捨選択(フィルタリング)を可能とするようなサービスを、従来から利用者に対し提供しており、ISP 自らが行う規制措置と併せて、利用者に迷惑メールを送信させない、受信させないための対策を進めている。

各移動系 ISP が提供するサービスの詳細は次のとおりである。

１　指定受信／拒否設定

１．１　Ａ社

携帯電話及び PHS、インターネット(携帯電話及び PHS 以外からのすべて)のメールを事業者ごとに選択可能な「一括指定」と、任意のメールアドレス又はドメインを受信／拒否リストへ個別に指定する方法がある。個別の拒否設定では、従来はメールアドレスのみ指定可能であったが、2007 年(平成 19 年)11 月より、ドメインを指定しての拒否機能も追加された。

設定件数は、受信設定では最大 40 件、拒否設定では、ドメイン拒否・メールアドレス拒否において、それぞれ最大 40 件設定できる。「受信設定」と「拒否設定」は併用することが可能である。

これらの設定は、インターネットからのメールを受信するように設定してあると、携帯電話及び PHS のメールアドレスになりすましたメールを拒否するフィルタを使用するかどうかの選択もできる。

１．２　Ｂ社

すべての電話番号又はメールアドレスを許可・拒否する「一括設定」と、任意のアドレス・ドメイン・電話番号と合わせて最大 20 件を受信拒否又は受信許可する「アドレス指定設定」がある。「受信拒否」と「受信許可」は併用することはできない。

2007 年(平成 19 年)9 月より、ネットワークサーバ上にあるアドレス帳に登録されたメールアドレスからのメールを優先受信するサービスが追加されている。この機能では、(1)アドレス帳に登録されたメールアドレスからのメールのみ受信する、(2)アドレス帳に登録されたメールアドレスからのメールを優先受信する、(3)利用しない、の中から選択できる。(1)を設定すると、アドレス帳に登録してあるメールアドレス以外のメールを受信拒否することができる。(2)を選択した場合、アドレス帳に登録してあるメールアドレスからのメールは優先的に受信するが、それ以外のメールは設定した迷惑メール対策機能に応じてフィルタリングしながら受信することが可能となる。なお、この機能は有料サービス(月額 105 円)で、申込みが必要となる。

１．３　Ｃ社

Ａ社と同様に、携帯電話及び PHS、インターネット(携帯電話及び PHS 以外からのすべて)のメールを事業者ごとに選択可能な「一括指定受信」と、任意のメールアドレス又はドメインを受信／拒否リストそれぞれ最大 100 件を個別に指定する「指定受信リスト設定」／「指定拒否リスト設定」がある。「受信設定」と「拒否設定」は併用することが可能である。

これらの設定が重複した場合、その優先順位は、(1)指定拒否リスト設定、(2)指定受信リスト設定、(3)一括指定受信となる。

具体的な指定受信の設定例としては、移動系 ISP5 社からのメールはすべて受信し、インターネット発のメールについては特定のメールマガジンや勤務先からの電子メールのみを受信したい場合は、一括指定で移動系 ISP5 社を指定(インターネット及び PHS からのメールは一括指定から外す)した上で、メールマガジンの送信元及び勤務先のドメイン名を個別に「指定受信リスト設定」に登録する。

１．４　Ｔ社

特定の(1)アドレス、(2)ドメイン、(3)サブドメイン、(4)すべてのアドレス、(5)すべての@を含むアドレス、(6)@のないメールなど返信できないメールアドレスなどを最大 20 件指定して指定受信又は指定拒否することが可能である。Ｂ社と同様に、「指定受信」と「指定拒否」は併用できない。

１．５　Ｕ社

携帯電話事業者及びＰＨＳ事業者ごとに受信可否を一括で選択することが可能である。また、指定した文字列が、送信者のメールアドレス（メールアドレス、アカウント又はドメイン）に部分的に含まれる場合、その電子メールを受信／拒否することも可能としている。(登録可能件数：20 件)

２　送信元詐称対策

２．１　Ａ社

(1)なりすまし拒否

拒否設定において、携帯電話及びPHSドメインになりすましたメールを拒否することができる。

(2)送信ドメイン認証

2007年(平成19年)11月より、送信ドメイン認証を導入し、一般のドメインになりすましたメールについても対応を開始している。送信元情報を詐称したメールについて拒否することができる。

この機能では、(1)「拒否しない」、(2)「存在するドメインからのみ受信する」、(3)「すべて拒否する」の中から選択することができる。(2)を設定した場合はDNSサーバを参照し、送信元のアドレス(Header From)のドメインが存在することを確認し、確認できなかった場合は受信しない。(3)を選択すると、送信ドメイン認証を行い、送信元のアドレス(Header From)のIPアドレスの正当性が確認できた場合にのみ受信することができる。(3)を選択した場合には、サーバにSPF登録を行っていないISPや企業などからのメールも正当確認の認証ができないため受信することができなくなる。

(3)ホワイトリスト

2008年(平成20年)1月23日より、メーリングリストや転送メールなどがなりすましメールと判定される問題に対応し、「あて先指定受信機能」の提供している。この機能では、救済するメールアドレスを10件まで指定できる。

２．２　Ｂ社

(1)なりすまし拒否

拒否設定において、携帯電話及びPHSドメインになりすましたメールを拒否することができる。

(2)送信ドメイン認証

携帯電話及びPHS以外の一般のドメインのなりすましに対する送信ドメイン認証を導入することによる対応については、今後、提供予定としている。

(3)ホワイトリスト

メーリングリストや転送メールなどがなりすましメールと判定される問題に対応し、救済リストとして、最大3件まで救済するアドレスを登録

し、フィルタリングされずに受信可能としている。

２．３　Ｃ社

⑴なりすまし拒否

個別設定できる「基本設定」において、携帯電話及びPHSドメインになりすましたメールを拒否することができる。

⑵送信ドメイン認証

送信ドメイン認証を導入しており、「ドメイン認証規制」を利用することで、一般のドメインから送られてくる送信元を偽ったメールを拒否することが可能となっている。

ただし、DNSサーバにSPF登録（SPF、Sender IDの記述）を実施しているISPや企業等のドメインを詐称した場合に限られる。このため、サーバにSPF登録を行っていないISPや企業などからのメールは認証できないため拒否対象とはならない。

⑶ホワイトリスト

メーリングリストや転送メールなどがなりすましメールと判定される問題に対応し、「あて先指定受信機能」を提供している。この機能では、携帯自動転送元のメールアドレスを最大5件まで登録することができる。

２．４　Ｕ社

⑴なりすまし拒否

拒否設定において、PCから携帯電話及びPHSドメインになりすましたメールを拒否することができる（初期値はOFFに設定されている。）。

⑵送信ドメイン認証

送信元のIPアドレスがメールアドレスのドメインに対応するSPFレコードと不合致の場合に当該メールを拒否することができる（初期値はOFFに設定されている。）

。

３　簡易設定

３．１　Ａ社

2007 年(平成 19 年)11 月より、迷惑メール対策機能の充実に伴い、設定方法が複雑かつ多岐にわたるため、初心者や低年齢層向けの補助機能を提供している。

インターネットからのメールと特定の URL リンク付きメールを拒否する「低年齢層向けフィルタリング」・「受信拒否(強)」、インターネットからのメールを受信するが、送信元アドレスが実在しないドメインからのメール及び特定の URL リンク付きメールを拒否する「受信拒否(弱)」の 3 つの中から選択して、より簡単に設定を行うことができる。

・「低年齢層向けフィルタリング」(高)
　受信/拒否設定(携帯・PHS のみ、なりすましメール拒否)、URL 付きメール拒否設定
・「受信拒否　強」(高)
　受信/拒否設定(携帯・PHS のみ、なりすましメール拒否)、URL 付きメール拒否設定
・「受信拒否　弱」(低)
　受信/拒否設定(なりすましメール拒否、存在するドメインからのみ受信)、URL 付きメール拒否設定

３．２　Ｂ社

2008 年(平成 20 年)3 月 27 日より、各種迷惑メール対策機能を、3 つの設定レベルから 1 つ選択するだけで一括設定できる簡易な設定サービスを開始している。3 つの設定レベルには、(1)推奨設定(標準レベル)、(2)ケータイ／PHS 設定(中レベル)、(3)低年齢層向けフィルタリング設定(強レベル)があり、設定レベルごとに各種迷惑メール対策機能を、従来よりも簡単に設定することができる。

また、2008 年(平成 20 年)6 月より、6 つある迷惑メールブロック機能を、パスワード入力不要の 2 クリックで一括して設定できるサービスの提供を開始した。設定は「初めての設定」(なりすましたメールを拒否・特定 URL を含むメールを拒否の 2 つをデフォルト設定)と、「さらに強めたい」(「初めての設定」の設定に加えて、発信元を携帯・PHS のみとメールアドレスのドメインに「.jp」がつくメールに限定)の 2 つから選択して設定することができる。

・低年齢層向けフィルタリング設定(高)
　なりすましメール拒否、優先受信、未承諾広告拒否、URL 付きメール拒否設定(URL を含むメールをすべて受信しない)、受信許可・拒否設定(携帯・PHS のみ)、海外からの電話番号拒否設定。
・ケータイ／PHS 設定(高)

なりすましメール拒否、優先受信、未承諾広告拒否、URL 付きメール拒否設定(特定 URL を含むメールのみ受信しない)、受信許可・拒否設定(携帯・PHS のみ)。

・推奨設定(標準レベル)(低)

なりすましメール拒否、優先受信、未承諾広告拒否、URL 付きメール拒否設定(特定 URL を含むメールのみ受信しない)。

３．３　Ｃ社

2006 年(平成 17 年)11 月より、簡易な設定サービスが追加され、受信者が質問に答えるだけでフィルタを設定できる機能と、フィルタのレベル設定機能を提供している。フィルタのレベル設定では、希望のレベルに合わせて 3 段階から選んで、設定することができる。

・「フィルタレベル」(高)

未承諾広告、なりすましメール拒否、指定拒否、ドメイン指定受信(携帯・PHS のみ)

・「フィルタレベル」(中)

未承諾広告、なりすましメール拒否、指定拒否

・「フィルタレベル」(低)

未承諾広告、なりすましメール拒否

４　選択受信

４．１　Ａ社

Ａ社の携帯電話からの電子メールについて、件名等を確認し、電子メールごとに受信・削除・保留を選択することができる。（機種依存の機能となる）

４．２　Ｂ社

あて先、件名及び本文の一部を受信し、読みたくない電子メールは全文を受信せずにメールサーバで削除することができる。

４．３　Ｃ社

加入者は、はじめから電子メールの全文を受信するのか、「送信者」及び「件名」のみを受信して確認した後、本文を受信するか否かを決定するのか、の設定をすることができる。

４．４　Ｔ社

PC から送られてきた電子メールや、自宅や会社から転送している電子メールに添付されているファイルをメールサーバで削除することができる。

４．５　Ｕ社

件名のみ受信した後、受信したい電子メールの本文及び添付ファイルを受信することができる。

５　URL 付きメール受信拒否

インターネットから送られてくる電子メールを対象に、URL 付きメールを受信拒否できる。ユーザは URL 付きメールの扱いについて、次の分類から選択できる(初期設定は、すべて受信許可)。

(1)すべて受信許可

(2)URL 付きメールをすべて受信拒否

(3)特定 URL[9]付きのメールのみ受信拒否

迷惑メールのほぼすべてに宣伝サイトへ誘引する URL が含まれること、宣伝サイトのほとんどが出会い系／アダルト系であることから、(3)の機能はかなり有効となる。

５．１　Ａ社

2007 年(平成 19 年)4 月から提供しており、(1)すべて受信許可、(3)特定 URL 付きのメールのみ受信拒否の中から選択して設定することができる。

５．２　Ｂ社

2000 年(平成 12 年)11 月より提供を開始しており、(1)すべて受信許可、(2)URL 付きメールをすべて受信拒否、(3)特定 URL 付きのメールのみ受信拒否の中から選択して設定することができる。

なお、Ｂ社では 2008 年(平成 20 年)8 月より、新規契約者及び URL 付きメール拒否設定を利用したことがない契約変更・買い増し・機種変更した利用者について、迷惑メールブロックの申込みがあったものとし、「特定 URL を含むメールのみ受け取らない」設定を５営業日以内に実施することとしている。設定は各利用者で任意に変更できる。

５．３　Ｃ社

2007 年(平成 19 年)3 月より提供を開始しており、(1)すべて受信許可、(2)URL 付きメールをすべて受信拒否の中から選択して設定することができる。

５．４　Ｕ社

E メールについて、(1)すべて受信許可、(2)URL 付きメールをすべて受信拒否の中から選択して設定することができる。

---

[9]特定 URL＝外部データベースに登録された「出会い系サイト」や「アダルトサイト」等の特定カテゴリーに分類されたＵＲＬ

６　ブラウザからの設定

受信／拒否登録件数の拡張に伴い、携帯事業者ではユーザビリティに配慮し、PC から大画面で見やすく迷惑メール対策機能を設定することを可能とした。

６．１　Ａ社

Ａ社の HP から ID／パスワードを入力してログインする。

６．２　Ｂ社

携帯上でワンタイムパスワードを取得し、Ｂ社の HP からログインする。

６．３　Ｃ社

携帯上でワンタイムパスワードを取得し、Ｃ社の HP からログインする。

７　メールアドレスの変更

７．１　Ａ社

1 日 3 回以内で、半角英数字等で 3 字以上 30 字以下の任意のメールアドレスに変更できる。

７．２　Ｂ社

半角英数字等で 3 字以上 30 字以下の任意のメールアドレスに変更でき、変更後、24 時間は再変更できない。2006 年(平成 18 年)10 月より、メールアドレスの変更回数を、一つの電話番号に対して 99 回までの制限を設けている。

７．３　Ｃ社

1 日 3 回以内で、半角英数字で 30 字以下の任意のメールアドレスに変更できる。

７．４　Ｔ社

英字で始まる半角英数字等で 4 字以上 20 字以下の任意のメールアドレスに変更できる。ただし、変更後、48 時間は再変更できない。

７．５　Ｕ社

半角英数字 3 字以上 30 字以下の任意のメールアドレスに変更できる。

８　メールヘッダ情報の提供

移動系 ISP5 社は、受信者が一定の手続や携帯電話による機能の設定を行った場合に、インターネット経由で送信されたメールの送信元アドレス、時間、経由サーバ等の詳細が分かるヘッダ情報を受信者に提供している。取得したヘッダ情報は、当該 ISP、迷惑メール相談センター等への迷惑メールに関する情報提供、送信元 ISP への問合せ等に利用することができる。

８．１　Ａ社

インターネットから送られたメールのヘッダ情報を、携帯電話に受信するメール本文末尾に付加して携帯電話画面上で確認できる。Ａ社携帯電話間のメールのヘッダ情報は提供されない。ヘッダ情報を付加したメールを携帯画面上から転送することができ、これによりヘッダ情報付きの迷惑メールの情報提供を行うことが可能となる。

８．２　Ｂ社

携帯電話が受信したメールのヘッダ情報は、PC を利用して閲覧することができる。加入者は、PC からＢ社のサイトにアクセスし、あらかじめ同社のコールセンターへ電話して取得したヘッダ情報閲覧用のパスワードでログインすることで、ヘッダ情報を閲覧できる。パスワードの有効期限は 10 日間で、閲覧できるのは過去 2 日間に受信したヘッダ情報に限られ、Ｂ社携帯電話間の、ヘッダ情報は提供されない。

８．３　Ｃ社

携帯電話に着信し、メールサーバに保存されているメールの詳細ヘッダ情報を、携帯電話画面上で確認できる(30 日前までに受信したメールで、最大直近の 500 件まで)。さらに、ヘッダ情報の付加されたメールを携帯電話の画面上から転送することができ、たとえば転送先をＣ社の迷惑メール専用窓口にすることで、迷惑メールの情報提供を行うことが可能となる。

なお、受信したメールについて、あらかじめ任意のアドレスへ転送設定を行うことが可能であり、PC で受信するようにしておけば、ヘッダ付きのメールとして確認可能となる。

８．４　Ｔ社

WEB 上より、自動転送設定であらかじめ任意のアドレスを指定して転送を行うことが可能であり、受信したメールについて、PC で受信するようにしておけば、ヘッダ付きのメールとして確認可能となる。

８．５　Ｕ社

メール設定サイトへアクセスすることでメールヘッダの閲覧をすること

ができる。

９　未承諾広告メールの受信拒否

2002 年(平成 14 年)7 月に特定電子メール法が施行され、特定電子メールは件名に「未承諾広告※」と表示することが定められた(表示義務)。これに併せて、携帯電話事業者も、早期から、件名欄に「未承諾広告※」が表示されているメールを破棄する未承諾広告メール受信拒否機能の提供を開始した。

なお、特定電子メール法の 2008 年(平成 20 年)改正によるオプトイン方式の規制の導入に伴い、「未承諾広告※」の表示義務は廃止されたが、移動系 ISP5 社では、未承諾広告メール受信拒否機能の提供は継続している。

９．１　Ａ社及びＢ社

件名欄に「未承諾広告※」と記載されて送られてきた電子メールを受信又は受信拒否するよう利用者が設定できる。初期設定は、特定電子メールを「受信しない」に設定されている。

９．２　Ｃ社

件名欄に「未承諾広告※」と記載されて送られてきた電子メールを受信又は受信拒否するよう利用者が設定できる。初期設定は、特定電子メールを「受信する」に設定されている。

９．３　Ｔ社

件名欄に「！広告！」または「未承諾広告※」と記載されて送られてきた電子メールを受信又は受信拒否するよう利用者が設定できる。初期設定は、「受信する」に設定されている。

９．４　Ｕ社

件名欄中に「未承諾広告※」の記載された電子メールを受信又は受信拒否できるよう利用者が設定できる。初期設定は「受信する」に設定されている。

１０　その他各社が提供するサービス

１０．１　Ａ社

１０．１．１　Ａ社携帯電話から大量送信されたメールの受信制限

1台のＡ社携帯電話から大量の送信があった時、500通目以降のメールを受信者の設定により受信拒否できる(送信先アドレス1件を1通とカウントする。また、毎日、午前0時で送信通数は「0」にリセットされる。)。499通目まではこの機能の設定の有無(「受信拒否する」、「受信拒否しない」)にかかわらず送信され、500通目以降のメールは「受信拒否する」とした受信者には送信されないが、「受信拒否しない」とした受信者には送信される。１．１のドメイン指定受信で、携帯電話及びPHSからのメールを受信するとしている利用者も500通目以降の受信の可否を設定できる。

なお、受信拒否されて送信できなかった500通目以降のメールについては、送信者に「送信できません。あて先を確認してください。」とのメッセージが表示される。

2007年(平成19年)11月より、一般利用者のメール送信機会の増加や、対策機能の充実などの理由により、受信制限条件を変更し従来1日200通だった通数を1日500 通に緩和している。

１０．１．２　シークレットコードの提供

電話番号のメールアドレスの後に 4 桁の暗証番号(シークレットコード)を設定することで、暗証番号を知らない相手からのメールを拒否することができる。

１０．２　Ｃ社

１０．２．１　拒否通知メール返信設定

フィルタでブロックされたメールに対し、拒否通知の返信可否を設定できる。初期設定は「返信しない」に設定されている。拒否通知を設定しない場合は、送信側にはメールを拒否されたかどうかは分からない。

１０．２．２　HTMLメール規制

2007年(平成19年)3月より、HTMLメールの受信を拒否することが可能となっている。

１０．３　Ｕ社

１０．３．１　拒否通知メール返信設定

フィルタでブロックされたメールに対し、拒否通知の返信可否を設定できる。初期設定は「返信しない」に設定されている。

第３節　SMSを利用した迷惑メール受信防止のための移動系ISPによる規制措置

移動系ISP側で設定する迷惑メールに対する規制措置は次のとおりである。

１　大量迷惑メールの送信制限

１．１　Ａ社

2005年(平成17年)8月より、SMSにおけるメール送信可能通数の上限を設定し、1日当たり200通未満とする対策を実施している。

１．２　Ｂ社

2005年(平成17年)5月より、1日に500件以上のSMSを送信した場合、その後20日間の送信規制を行っている。

１．３　Ｃ社

2004年(平成16年)11月より、月間の送信数を加入3ヶ月以内の利用者とプリペイド会員については、3,000件、その他については6,000件に制限している。

１．４　Ｔ社

送信制限実施せず。

１．５　Ｕ社

１日に送信できるSMSを300通に制限している。

２　同報送信メールの送信制限

同報送信メールサービスは、現在、全社において提供されていない。

第４節　SMS の利用者が任意に条件を設定して迷惑メールの受信を防止するサービス

１　迷惑メール防止のための受信拒否機能

１．１　Ａ社

SMS 一括拒否機能では、ユーザが SMS を利用しない場合、すべての SMS の受信を拒否することができる。非通知 SMS 拒否機能は、発信者番号が非通知で発信されたメッセージを拒否することができる。

１．２　Ｂ社

受信者の携帯電話に「PIN コード」を設定し、SMS を送ってくる相手に、あらかじめ設定した PIN コードの付いていないメールの受信を拒否することができる。

(1)「PIN コードフィルタ」機能

不特定多数から送信される SMS などの短い迷惑メールを受信拒否する方法として、PIN コード設定がある。家族や友人などの特定の人に PIN コード設定をする事で、PIN コードが一致したメールのみ受信し、それ以外のメールは受信拒否することができる。

(2)「アドレスフィルタ」機能

20 件まで、特定アドレスの受信拒否を設定がすることができる。

１．３　Ｃ社

(1)ブロック機能

2005 年(平成 17 年)3 月より、メッセージ本文内に接続先 URL(http://**, https://**)や電話番号が含まれるメールを受信拒否する機能を実施している。

(2)「SMS 受信フィルタ機能」

SMS を受信した時点で、一切受信したことを意識しないように、メール通知表示、通知音(バイブ含む)鳴動などを起こさず、自動的に受信メールを破棄する。

次の 4 種類のフィルタをそれぞれ設定可能。

ｉ　指定番号
　　指定番号一覧に登録された電話番号から届いた SMS を破棄。

ii　非通知
　　電話番号通知のない SMS を破棄。

iii　Ｅメールお知らせ拒否
　　Ｅメールお知らせで届いた SMS を破棄。

iv　アドレス帳登録外(一部機種に限る)

アドレス帳に登録されていない電話番号から届いたSMSを破棄。

(3)利用制限

意図しないSMSを受信したくない場合、SMS等の利用を停止することができる。

１．４　Ｔ社

指定した電話番号、電話番号非通知のSMSを拒否設定が可能である。

(別表１)移動系 ISP が提供する迷惑メール送信対策一覧

１　迷惑メールの送信防止に関するサービス

記載節番号 サービス名	内　容				
	Ａ社	Ｂ社	Ｃ社	Ｔ社	Ｕ社
1-1 あて先不明メール	あて先に実在しない大量のアドレスを含むメールは、事業者側の設備で受信拒否する。				
提供開始時期	平成 13 年 1 月	平成 14 年 1 月	平成 17 年 4 月	平成 18 年 12 月	平成 20 年 3 月
1-2 送信通数規制	1 日 1 台当たりの送信を 1,000 回未満に制限する。平成 16 年 3 月から、3G 方式についてのみ、送信回数ではなく、同報通信を含む 1,000 通未満に送信を制限することに変更した。	2G 方式で、3 時間で 120 件以上のメールを送信した場合、その後 21 時間送信を規制する。 平成 17 年 2 月から、3G 方式において、24 時間以内に 1,000 以上の宛先に送信した場合、その後 24 時間送信を規制することとした。	平成 15 年より従来の 30 件から一度に送信できるメールのあて先数を 5 件までとしたが、迷惑メール機能拡充による迷惑メールの減少により、平成 20 年 1 月より元の 30 件に拡大された。また、平成 16 年 8 月(同社別サービスについては平成 18 年 9 月)より、1 日当たりの送信数の上限を一律 1,000 件までとした。	30 分当たり 100 件を超えるメールが送信された場合に利用停止とする等の措置を行なっていたが、平成 16 年 8 月より 1 日当たり 1,000 通を超えるメールを送信した場合も迷惑メールとみなして利用停止などの処置を行う。	
提供開始時期	平成 15 年 10 月	平成 15 年 12 月	平成 15 年 9 月	平成 16 年 8 月	
1-2 同報送信あて先数の制限			1 回当たり 30 件までに制限		
提供開始時期			平成 20 年 1 月		
1-3 メールアドレスの初期設定の変更	契約時における初期設定は「複数のランダムな英数字@xxx.ne.jp」				
提供開始時期	平成 13 年 7 月	平成 15 年 1 月	平成 11 年 4 月	平成 10 年 12 月	平成 20 年 3 月
1-4 自動転送先設定回数の制限			転送先を設定（変更）できる回数を 1 日 3 回までに制限した。		
提供開始時期			平成 16 年 6 月		

記載節番号 サービス名	内　容					
	Ａ社		Ｂ社	Ｃ社	Ｔ社	Ｕ社
1-5 送信ドメイン認証	DNS サーバへ SPF レコードの記述					
提供開始時期	平成 17 年 12 月		平成 18 年 3 月	平成 17 年 12 月	平成 18 年 3 月	平成 20 年 3 月
1-6 OP25B	平成 17 年 6 月よりインターネット接続サービスにて規制を実施。	平成 20 年 7 月、インターネット接続サービスを利用し、3G 方式からアクセスポイント接続経由で 25 番ポートを利用して送信されるメールに対し、速度制限を開始した。	平成 19 年 12 月よりインターネット接続サービスから携帯電話宛ての OP25B を実施、平成 20 年 3 月からは固定系 ISP 宛てのメール送信についても、実施。	平成 18 年 6 月よりインターネット接続サービスから携帯電話宛ての OP25B を実施、平成 20 年 9 月下旬からは固定系 ISP 宛てのメール送信についても、実施。	平成 18 年 5 月よりインターネット接続サービスから携帯電話宛ての OP25B を実施、平成 20 年 6 月からは、固定系 ISP 宛てのメール送信についても、実施。	携帯事業者向けは平成 20 年 3 月より OP25B を適用している。その他は平成 21 年 5 月より順次開始している。
提供開始時期	平成 17 年 6 月	平成 20 年 7 月	平成 20 年 3 月	平成 20 年 10 月	平成 20 年 6 月	平成 20 年 3 月

２　迷惑メールの受信防止に関するサービス

記載節番号 サービス名	内　容				
	Ａ社	Ｂ社	Ｃ社	Ｔ社	Ｕ社
2-1 指定受信／拒否	指定したドメイン、アドレスから送信されたメールを受信／拒否する。移動系ISP ごとに受信可否を一括で選択可能。 平成19年11月より、個別の拒否設定において、メールアドレスに加えドメイン単位での設定も可能。	指定したドメイン、アドレスから送信されたメールを受信／拒否する。移動系ISP ごとに受信可否を一括で選択可能。 平成19年9月より、ネットワーク上のアドレス帳に登録されたメールアドレスからのメールを優先受信するサービス（有料）の提供を開始。	指定したドメイン、アドレス、アドレスの「@」の前の文字列などから送信されたメールを受信／拒否する。移動系ISP ごとに受信可否を一括で選択可能。これらの設定が重複した場合、その優先順位は、(1)指定拒否リスト設定、(2)指定受信リスト設定、(3)一括指定受信。	指定した(1)アドレス、(2)ドメイン、(3)サブドメイン、(4)すべてのアドレス、(5)すべての@を含むアドレス、(6)@のないメールなどから送信されたメールを受信／拒否。	携帯電話事業者及びＰＨＳ事業者ごとに受信可否を一括で選択することが可能である。また、指定した文字列が、送信者のメールアドレス（メールアドレス、アカウント又はドメイン）に部分的に含まれる場合、その電子メールを受信／拒否することも可能としている。
設定内容	受信40件 アドレス、ドメイン拒否各40件	許可／拒否 いずれか20件	受信100件 拒否100件	許可／拒否 いずれか20件	受信20件 拒否20件
指定受信／許可の併用	可能	不可	可能	不可	不可
提供開始時期	平成16年5月に設定件数が20件から40件に拡大。平成18年3月よりメールアドレス指定拒否、平成19年11月よりドメイン指定拒否との併用が可能。	平成13年12月に10件から20件に拡大。平成19年9月より、ネットワーク上のアドレス帳優先受信機能を拡充。	平成14年4月より提供。指定拒否との併用は平成15年5月、17年11月の2度に渡って拡充。 平成19年3月には、設定数が20件から100件に拡大。	平成14年6月より提供している。	平成20年3月より。

記載節番号 サービス名	内　容				
	Ａ社	Ｂ社	Ｃ社	Ｔ社	Ｕ社
2-2-(1) 送信元詐称対策 なりすまし拒否	受信・拒否設定において、携帯電話及び PHS(一部除く）のドメインになりすましたメールを受信拒否する。				
提供開始時期	平成 18 年 3 月	平成 17 年 3 月	平成 14 年 7 月	平成 18 年 5 月	平成 20 年 3 月
2-2-(2) 送信元詐称対策 送信ドメイン認証	送信元情報を詐称したメールを受信拒否。 送信元の IP アドレスと、DNS サーバに登録された送信用メールサーバの IP アドレスとを比較し、合致した場合にのみメール受信し、不一致の場合や、当該 IP アドレスが DNS サーバに存在しないなど、整合性がとれない場合には受信しない。		送信元情報を詐称したメールを受信拒否。 ただし、DNS サーバに SPF 登録(SPF/Sender ID の記述）を実施している ISP や企業等を詐称したドメインに限られる。このため、サーバに SPF 登録を行っていない ISP 事業者や企業などからのメールは認証できないため規制対象とはならない。		拒否設定において、PC から携帯電話及び PHS ドメインになりすましたメールを拒否することができる。(初期値は OFF に設定されている。)送信元の IP アドレスがメールアドレスのドメインに対応する SPF レコードと不合致の場合に当該メールを拒否することができる。(初期値は OFF に設定されている。)
提供開始時期	平成 19 年 11 月		平成 19 年 3 月		
2-3 送信元詐称対策 ホワイトリスト	最大 10 件まで自動転送元のメールアドレスを設定できる。	最大 3 件まで自動転送元のメールアドレスを設定できる。	最大 5 件まで自動転送元のメールアドレスを設定できる。		
提供開始時期	平成 19 年 1 月	平成 18 年 10 月	平成 19 年 3 月		
2-3 簡易設定	メールフィルタを「低年齢層向け」「受信拒否（強)」「受信拒否（弱)」から選ぶことで従来よりも簡単に設定可能。	メールフィルタを「推奨設定(標準)」「ケータイ／PHS 設定（中)」「低年齢層向け（強)」から選ぶことで従来よりも簡単に設定可能。 平成 20 年 6 月より、パスワード入力で一括して設定できるサービス提供を開始した。	メールフィルタを「受信者が質問に答えるだけでフィルタを設定できるサポート設定機能」「メールフィルタを 3 段階のレベルから選んで、設定する機能」から選ぶことで従来よりも簡単に設定可能。		
提供開始時期	平成 19 年 11 月	平成 20 年 3 月	平成 20 年 3 月		

記載節番号 サービス名	内　容				
	Ａ社	Ｂ社	Ｃ社	Ｔ社	Ｕ社
2-4 選択受信	件名のみ受信した後、受信したいメールの本文及び添付ファイルを受信する。	あて先、件名及び本文の一部を受信し、読みたくないメールは全文を受信せずにサーバで削除する。	件名のみ受信した後、受信したいメールの本文及び添付ファイルを受信する。	PC から送られてきたメールや、自宅や会社から転送しているメールに添付されているファイルをサーバで削除する。	件名のみ受信した後、受信したい電子メールの本文及び添付ファイルを受信する。
提供開始時期	平成 13 年 5 月（3G 方式のみ） 平成 15 年 5 月（2G の一部の端末可）	平成 11 年 12 月	平成 11 年 12 月	平成 16 年 3 月	平成 20 年 3 月
2-5 URL 付きメール受信拒否	E メールについて(1)すべて受信許可(2)特定 URL 付きのメールのみ受信拒否から選択。	E メールについて(1)すべて受信許可(2)URL 付きメールをすべて受信拒否(3)特定 URL 付きのメールのみ受信拒否の中から選択。	E メールについて(1)すべて受信許可(2)ＵＲＬ付きメールをすべて受信拒否から選択。		E メールについて(1)すべて受信許可(2)ＵＲＬ付きメールをすべて受信拒否から選択。
提供開始時期	平成 19 年 4 月	平成 12 年 11 月	平成 19 年 3 月		平成 20 年 3 月
2-6 ブラウザからの設定	PC からＡ社 HP で ID／パスワードを入力する。	携帯電話上でワンタイムパスワードを取得し、Ｂ社 HP にログインする。	携帯電話上でワンタイムパスワードを取得し、Ｃ社 HP にログインする。		
提供開始時期	平成 14 年 10 月	平成 15 年 5 月	平成 16 年 6 月		
2-7 メールアドレスの変更	半角英数字 3 字以上 30 字以下の任意のメールアドレスに変更できる。	半角英数字 3 字以上 30 字以下の任意のメールアドレスに変更できる。変更回数を 99 回まで制限。	半角英数字 30 字以下の任意のメールアドレスに変更できる。	半角英数字 4 字以上 20 字以下の任意のメールアドレスに変更できる。	半角英数字 3 字以上 30 字以下の任意のメールアドレスに変更できる。
	1 日 3 回まで	24 時間で 3 回まで	1 日 3 回まで	48 時間以内に 1 回	1 日 3 回まで
提供開始時期	平成 11 年 7 月	平成 14 年 1 月	平成 13 年 12 月	平成 16 年 9 月	平成 20 年 3 月

記載節番号 サービス名	内　容				
	Ａ社	Ｂ社	Ｃ社	Ｔ社	Ｕ社
2-8 メールヘッダ情報の提供	A 社以外から送信された電子メールのヘッダ情報を受信メール本文に付加して携帯電話画面上で確認できる。Ａ社携帯電話間のヘッダ情報は提供されない。	受信したＥメールのヘッダ情報は、PC を利用して閲覧する。閲覧時のパスワードの有効期限は 10 日間。2 日前までに受信したメールに限られる。Ｂ社携帯電話間のヘッダ情報は提供されない。	携帯電話に受信し、メールサーバに保存されているメールの詳細ヘッダ情報を、携帯電話画面上で確認できる。(30 日前までに受信したメールで、最大直近の 500 件まで)	メール転送機能を利用し、指定先アドレスへ転送したメールから確認する。	メール設定サイトへアクセスすることでメールヘッダの閲覧をすることができる。
提供開始時期	平成 14 年 10 月	平成 15 年 5 月	平成 16 年 6 月	平成 10 年 12 月	平成 20 年 3 月
2-9 未承諾広告メールの受信拒否	件名欄の最前部に「未承諾広告※」と記載されて送られてきた電子メールを受信又は受信拒否する。		件名欄の最前部に「未承諾広告※」と記載されて送られてきた電子メールを受信又は受信拒否する。	件名欄中に「！広告！」又は「未承諾広告※」と記載されて送られてきた電子メールを受信又は受信拒否する。	件名欄中に「未承諾広告※」の記載された電子メールを受信又は受信拒否する。初期設定は「受信する」。
初期設定	受信しない		受信する		
提供開始時期	平成 14 年 10 月	平成 14 年 8 月	平成 14 年 11 月	平成 14 年 6 月	平成 20 年 3 月

記載節番号 サービス名	内　容
	Ａ社
2-10-1-1 Ａ社携帯電話から大量送信されたメールの受信制限	大量の送信があった携帯電話から、同一日に送信された 500 通目以降のメールを受信するか、しないかを受信者が選択できる。平成 19 年 11 月 20 日より一般利用者のメール送信数増加や対策機能の充実等により、規制数を 200 から 500 通へと緩和。
提供開始時期	平成 16 年 1 月
2-10-1-2 シークレットコード	電話番号で構成されたメールアドレスの後に 4 けたの暗証番号(シークレットコード）を設定し、この暗証番号を付していないメールの受信を拒否する。
提供開始時期	平成 11 年 7 月
	Ｃ社
2-10-2-1 拒否通知返信設定	メールフィルタでブロックされたメールに対し、拒否通知の返信可否を設定。初期設定は「返信しない」になっている。
提供開始時期	平成 17 年 11 月
2-10-2-2 HTML メール規制	HTML メールの受信を拒否する。
提供開始時期	平成 19 年 3 月
	Ｕ社
2-10-3-1 拒否通知メール返信設定	メールフィルタでブロックされたメールに対し、拒否通知の返信可否を設定。初期設定は「返信しない」になっている。
提供開始時期	平成 20 年 3 月

第３章　迷惑メールに関する固定系 ISP の対策導入状況

第１節　迷惑メール送信防止対策の提供状況

１　Ｄ社

１．１　送信ドメイン認証

・SPF 登録

2005 年(平成 17 年)12 月より実施。

・DKIM

法人向けサービスにおいて 2005 年(平成 17 年)3 月より実施。

１．２　OP25B

・携帯あて

2005 年(平成 17 年)10 月より実施。

・PC あて

2006 年(平成 18 年)11 月より実施。

・Submission Port(587 番)

2005 年(平成 17 年)10 月より提供。

１．３　送信通数規制

2007 年(平成 19 年)2 月より、Ｄ社のメールサーバを経由して送信される迷惑メールへの対策として、基本メールアドレス、追加メールアドレスともに、1 日当たりのメール送信数を 1,000 通に制限した。また、短時間に大量のメールを送信した場合は、メールの送信効率を下げる制御を一定時間行う。

２　Ｅ社

２．１　OP25B

・携帯あて
　2005 年(平成 17 年)10 月より実施。
・PC あて
　2006 年(平成 18 年)6 月より実施。
・Submission Port(587 番)
　2006 年(平成 18 年)6 月より提供。

３　Ｆ社

３．１　送信ドメイン認証

・SPF 登録

2007 年(平成 19 年)2 月より実施。

３．２　OP25B

・携帯あて

2005 年(平成 17 年)11 月より実施。

・PC あて

2007 年(平成 19 年)7 月より実施。

・Submission Port(587 番)

2005 年(平成 17 年)11 月より提供。

４　Ｇ社

４．１　送信者確認

送信者アドレス(From:)を改変したメールの SMTP 接続を拒否。

４．２　送信ドメイン認証

・SPF 登録

2007 年(平成 19 年)5 月より実施。

４．３　OP25B

・携帯あて

2006 年(平成 18 年)6 月より実施。

・PC あて

2006 年(平成 18 年)10 月より実施。

・Submission Port(587 番)

2006 年(平成 18 年)6 月より提供。

５　Ｈ社

５．１　送信ドメイン認証

・SPF 登録

2006 年(平成 18 年)2 月より実施。

５．２　OP25B

・携帯あて

2006 年(平成 18 年)2 月より実施。

・PC あて

2006 年(平成 18 年)12 月より実施。

・Submission Port(587 番)

2006 年(平成 18 年)2 月より提供。

５．３　送信元 IP アドレス検証による送信規制

2007 年(平成 19 年)8 月より、不正な送信元 IP アドレスによる通信を遮断するための送信元 IP アドレスの検証を実施した。

通常、正規ユーザはインターネット接続やメールの送信の際は、同社が割り当てる IP アドレスを利用するが、ウイルスに感染しボット化してしまった場合、同社が割り当てる IP アドレスではなく、偽装された IP アドレスが利用されることがある。この点に着目し、送信されるメールの IP アドレスについて uRPF(unicast Reverse Path Forwarding)と ACL(Access Control List)によるパケットフィルタの仕組みを利用した検証を行い、IP アドレスが偽装されている場合は通信を規制する。

※　uRPF(unicast Reverse Path Forwarding)

ダイナミック(動的)な経路情報を利用したフィルタリング手法。インターネット関連技術の標準化団体である IETF(Internet Engineering Task Force)から推奨されており、今後広く普及することが期待されている技術。

ⅰ　Loose Mode：パケットの送信元 IP アドレスがルーティングテーブルに存在するかどうかのみを確認し、ルーティングテーブルに存在する場合には通過、存在しない場合には遮断される。

ⅱ　Strict Mode：パケットの送信元 IP アドレスがルーティングテーブルに存在し、かつそのパケットが適切に転送されるべきインターフェースからのパケットの場合は通過させ、異なるインターフェースからのパケットの場合は遮断される。

６　Ｉ社

６．１　送信ドメイン認証

・SPF 登録

2006 年(平成 18 年)11 月より実施。

６．２　OP25B

・携帯あて

2005 年(平成 17 年)3 月より実施。

・PC あて

2005 年(平成 17 年)3 月より実施。

他社等のメールアカウント送信用の代替送信メールサーバ有り。

・Submission Port(587 番)

2005 年(平成 17 年)3 月より提供。

７　Ｊ社

７．１　送信ドメイン認証

・SPF 登録

2006 年(平成 18 年)3 月より実施。

７．２　OP25B

・携帯あて

2005 年(平成 17 年)12 月より実施。

・PC あて

2006 年(平成 18 年)3 月より実施。

他社等のメールアカウント送信用の代替送信メールサーバ有り。

・Submission Port(587 番)

2005 年(平成 17 年)11 月より提供。

８　Ｋ社

８．１　送信ドメイン認証

・SPF 登録

2006 年(平成 18 年)4 月より実施。

８．２　OP25B

・携帯あて

2006 年(平成 18 年)6 月より実施。

・PC あて

2006 年(平成 18 年)6 月より実施。

他社等のメールアカウント送信用の代替送信メールサーバ有り。

・Submission Port(587 番)

2006 年(平成 18 年)3 月より提供。

８．３　送信通数規制

Ｋ社では、一定時間に送信できるメールの通数に制限を設けている。メール通数の制限は、Port25 を設定しメールを送信する場合は回線単位、サブミッションポート（Port587）を設定しメールを送信する場合はメールアドレス単位で行う。

９　Ｌ社

９．１　送信ドメイン認証

・SPF 登録

2005 年(平成 17 年)12 月より実施。

９．２　OP25B

・携帯あて

2006 年(平成 18 年)3 月より実施。

・PC あて

2006 年(平成 18 年)12 月より実施。

他社等のメールアカウント送信用の代替送信メールサーバ有り。

・Submission Port(587 番)

2006 年(平成 18 年)8 月より提供。

１０　M社

１０．１　送信ドメイン認証

・SPF 登録
　2005 年(平成 17 年)5 月より実施。
・DKIM
　2005 年(平成 17 年)5 月より実施。

１０．２　OP25B

・携帯あて
　2006 年(平成 18 年)2 月より実施。
・PC あて
　2006 年(平成 18 年)2 月より実施。
　他社等のメールアカウント送信用の代替送信メールサーバ有り。
・Submission Port(587 番)
　2005 年(平成 17 年)10 月より提供。

１１　Ｎ社

１１．１　送信ドメイン認証

・SPF 登録
　2006 年(平成 18 年)5 月より実施。
・SPF 認証
　受信時のチェックの導入を検討中。(導入時期未定)

１１．２　OP25B

・携帯あて
　2005 年(平成 17 年)9 月より実施。
・PC あて
　2006 年(平成 18 年)12 月より実施。
・Submission Port(587 番)
　2006 年(平成 18 年)2 月より提供。

１２　Ｏ社

１２．１　送信トラフィック制御

・入会直後の仮パスワード期間の送信通数制限
・連続メール送信制限
・同一 IP アドレスからの同時大量送信対策
・差出人アドレスのチェックの強化
・DNS に登録されていないドメインからのメールを受信拒否の対象
・ボット対策

2006 年(平成 18 年)5 月より、ボット感染により自覚なく迷惑メールの送信元になっている利用者向けのサポートを開始した。カスタマーサポートは、ボット感染の可能性があること、感染の確認方法及び駆除の方法等について郵送とメールにて案内した後、利用者のセキュリティ対策状況を確認し、対策が完了するまでをサポートする。

・メール送信数制御

個人会員について、1 日当たりに送信可能なメールあて先数を制御。これにより、同社メールサーバを経由した大量送信による迷惑メールを削減。

１２．２　送信ドメイン認証

・SPF 登録

2005 年(平成 17 年)11 月より実施。

・DKIM

2007 年(平成 19 年)9 月より実施。

１２．３　OP25B

・携帯あて

2006 年(平成 18 年)7 月下旬より実施。

・PC あて

2006 年(平成 18 年)9 月下旬より実施。
他社等のメールアカウント送信用の代替送信メールサーバ有り。

・Submission Port(587 番)

2005 年(平成 17 年)7 月より提供。

１３　Ｐ社

１３．１　送信トラフィック制御

大量のメール送信を検知した場合は、送信者を特定し、それ以降の送信を規制。迷惑メールに分類されるメールの大量送信が始まってから全体の 1%程度の送信が行われた段階で検知し、残りの 99%を破棄することが可能。

１３．２　送信ドメイン認証

・SPF 登録

2006 年(平成 18 年)11 月より実施。

１３．３　OP25B

・携帯あて

2005 年(平成 17 年)1 月より実施。

・PC あて

2006 年(平成 18 年)7 月より実施。

他社等のメールアカウント送信用の代替送信メールサーバ有り。

・Submission Port(587 番)

2006 年(平成 18 年)6 月より、標準・無料サービスとして提供（それ以前はオプションサービスとして提供)。

１４　Ｑ社

１４．１　送信ドメイン認証

・SPF 登録
　2006 年(平成 18 年)12 月より実施。
・DKIM
　2005 年(平成 17 年)7 月より実施。

１４．２　OP25B

・携帯あて
　2006 年(平成 18 年)6 月より実施。
・PC あて
　2007 年(平成 19 年)1 月より実施。
・Submission Port(587 番)
　2006 年(平成 18 年)6 月より提供。

１５　Ｒ社

１５．１　送信ドメイン認証

・SPF 登録
　2006 年(平成 18 年)10 月より実施。

１５．２　OP25B

・携帯あて
　2005 年(平成 17 年)3 月より実施。
・PC あて
　2005 年(平成 17 年)3 月より実施。
　他社等のメールアカウント送信用の代替送信メールサーバ有り。
・Submission Port(587 番)
　2005 年(平成 17 年)3 月より提供。

１６　Ｓ社

１６．１　送信トラフィック制御

Ｓ社のメールサーバが同一の送信者から短期間に大量のメールを受信したときに、一時的に、もしくは一定の期間、その送信者からのメールの受信を拒否する。

１６．２　送信ドメイン認証

・SPF 登録

2007 年(平成 19 年)11 月より実施。

１６．３　OP25B

・携帯あて

2006 年(平成 18 年)11 月より実施。

・PC あて

2006 年(平成 18 年)11 月より実施。「一部未実施のサービスあり」

・Submission Port(587 番)

2006 年(平成 18 年)6 月より提供。

（別表２）主要な固定系 ISP が提供する迷惑メール送信対策一覧

	送信ドメイン認証		OP25B 関連			
	SPF	DKIM (Domainkeys)	携帯あて	PC あて	代替送信サーバ	port 587
D社	H17/12	H21/02 (企業向け)	H17/10	H18/11	－	H17/10
E社	－	－	H17/10	H18/06	有	H18/03
F社	H19/02	－	H17/11	H19/07	－	H17/11
G社	H19/05	－	H18/06	H18/10	－	H18/06
H社	H18/02	－	H18/02	H18/12	－	H17/02
I社	○	－	H17/03	H17/03	有	H17/03
J社	H18/03	－	H17/12	H18/03	有	H17/12
K社	H18/04	－	H18/06	H18/06	有	H18/03
L社	H17/12	－	H18/03	H18/12	メールサーバ用 有	H18/08
M社	H17/05	H17/05	H18/02	H18/02	有	H17/10
N社	H18/05	－	H17/09	H18/12	H20/6(25 番ポートでの SMTP 接続を自社接続のみに制限)	H18/02
O社	H17/11	H19/09	H18/07	H18/09	有	H17/07
P社	H18/11	－	H17/01	H18/07	メールサーバ用 有	H18/06
Q社	H18/12	H17/07	H18/08	H19/01	－	H18/06
R社	H18/10	－	H17/03	H17/03	有	H17/03
S社	H19/11	－	H18/11	H18/11	無	H18/06

第２節　迷惑メール受信防止対策の提供状況

１　Ｄ社

Ｄ社の提供する迷惑メール対策サービスには、複数のフィルタ機能を持つサービスがある。

１．１　迷惑メールの判定

１．１．１　キーワード判定

・ブラックワード

送信者アドレス(From:)、あて先アドレス(To:)、写しあて先アドレス(Cc:)、件名(Subject:)、Content-Type:、メールソフト名(X-mailer:):、Received:、Return-Path:、Date:、全ヘッダの各項目にキーワードを、単独又は組み合わせで合計 100 パターンまでの受信拒否条件の設定ができる。指定できる条件としてワイルドカードの設定も可能。

・メール容量

20Ｋバイト、50Ｋバイト、100Ｋバイト、500Ｋバイト、1Ｍバイト、3Ｍバイト以上のいずれかのレベルを選択すると、その容量(ヘッダ情報を含む)を超えるメールを受信しないよう設定できる。

・添付ファイル

添付ファイルつきのメールをごみ箱に入れる。

・メールソフト名(X-mailer:)

メールソフト名(X-mailer:)の記載がないメールをごみ箱に入れる。

１．１．２　送信元情報参照による判定(送信ドメイン認証)

送信元メールアドレス(From:)のドメインと SPF を利用した認証結果(スコア)を選択し、フィルタの条件として設定する。対象ドメインにを設定する際には、”*”を用いたワイルドカードも指定可能。

１．１．３　内容参照による判定(ヒューリスティックフィルタ)

2004 年(平成 16 年)10 月より提供。受信メールのヘッダや本文の情報から迷惑メールの特徴等をスコア化し、スコアが一定以上の基準値を超える場合に迷惑メールとして判定し、振り分け作業を行う。迷惑メールである可能性が高いメールは、一旦自動的に隔離され、それらを一括で削除することも可能。判定後は、ヘッダ部分に判定結果が付与され、ユーザの使用しているメールソフトで振り分けることができる。

なお、判定スコアはユーザが任意に変更可能。

１．２　ホワイトリスト

受け取りたい相手のメールアドレスを最大 1,000 件登録することができる。

１．３　迷惑メール判定後の処理

受信拒否条件に該当するメールは、ごみ箱フォルダに保存され（件数及び容量は無制限）、利用者はごみ箱フォルダに保存されたメールの送信者名、件名等の閲覧が可能であるが、メールサーバへの到着後 4 週間で自動的に削除される。

２　Ｅ社

Ｅ社の提供する迷惑メール対策サービスには、メール全般に関するオプションサービスがある。これは、標準サービスであり、Web メール(携帯電話版 Web メールつき)、メール転送、迷惑メールフィルタ、メール自動振り分けの４つの機能からなる。これらの機能のうち、迷惑メール対策機能は、迷惑メールフィルタ及びメール自動振り分けである。

２．１　迷惑メールの判定

２．１．１　キーワード判定(ブラックワード)

受信許可アドレス及び受信拒否アドレスとしてそれぞれ 100 件のメールアドレスを登録可能。既に受信許可アドレスとして登録されているメールアドレスを、受信拒否アドレスとして登録することはできない。

２．１．２　内容参照による判定(ヒューリスティックフィルタ)

2006 年(平成 18 年)12 月より、迷惑メール判定エンジンを使用してメールサーバ上で一括して迷惑メールか否かの判定を行い、迷惑メールと判定されたメールを迷惑メールフォルダに移動してユーザの受信トレイに配信されないようにしている。

２．２　ホワイトリスト

受け取りたい相手のメールアドレスを件数に制限なく登録できる。

２．３　迷惑メール判定後の処理

Ｅ社のメールサーバ上で一括して迷惑メールを識別し、迷惑メールと判定されたメールには、メールサーバ上にある迷惑メールフォルダへ隔離し、ユーザが受信することがないように設定できる。迷惑メールフォルダの保存期間の初期設定は 7 日間であり、最大で 28 日まで設定可能（超過したものから自動的に削除される)。初期設定では、件名に[spam]を付記する設定になっている。また、迷惑メールフォルダへ配信された場合、ユーザへ通知する機能もある(初期設定はオフに設定されている)。

３　Ｆ社

Ｆ社の迷惑メール対策サービスは、迷惑メールフィルタソフトをインストールして使用するサービスと、Ｆ社が行う迷惑メールのブロックサービス、迷惑メールの自動判定サービス及びメールの自動削除サービスがある。

３．１　迷惑メールの判定

３．１．１　キーワード判定

・迷惑メールフィルタソフトの月額版を使用するサービス

月額の使用料を支払うことにより、迷惑メールフィルタソフトのインストールができる。迷惑メールへの対応は、インストールしたフィルターソフトに基づき行う。

・メールの自動削除サービス

⑴シンプルバージョン

送信者アドレス(From:)、あて先アドレス(To:)、件名(Subject:)に条件を設定し、その条件に当てはまるメールのみ受信を拒否し、自動的に削除する。

⑵プロバージョン

自動削除の条件をヘッダ情報に応じて細かく指定できる。

⑶アドレス指定バージョン

送信者アドレス(From:)を指定し、そのメールアドレスから送信されるメールの受信を拒否し、自動的に削除する。最大 50 アドレスの登録が可能。

⑷条件指定バージョン

自動削除の条件をさらに細かく指定できる。アドレス指定バージョンと組み合わせて利用すると合計で最大 100 パターンの登録が可能。

３．１．２　内容参照による判定

・ヒューリスティックフィルタ

⑴迷惑メールのブロックサービス

迷惑メールコミュニティから申告される情報を元に迷惑メールを自動判定し、迷惑メールやフィッシングメールをＦ社メールサーバ上に隔離して、利用者の受信トレイに配信されないようにする。件名の先頭に[meiwaku]を付記して配信することも可能。

⑵迷惑メールの自動判定サービス

迷惑メール判定エンジンでスコア付けし、その結果をヘッダに付与する。ユーザが設定するスコア以上のメールの件名に[meiwaku]を付記する事も可能。

・シグネチャーフィルタ（セキュリティソフトの月額版を使用するサービスにおいて提供）

メールソフトにアドインするタイプの迷惑メール判定エンジンを採用。

参照データベースは、ネットワークで結ばれたメンバーから、毎日大量に迷惑メールの報告を受け取っている。この情報により、素早く迷惑メールを識別し、遮断可能としている。

３．２　ホワイトリスト

・迷惑メールのブロックサービス

送信者アドレス(From:)、あて先アドレス(To:)、件名(Subject:)のそれぞれについて 100 件、計 300 件を設定することができる。

３．３　迷惑メール判定後の処理

・セキュリティソフトの月額版を使用するサービス

迷惑メール判定エンジンでスコア付けし、その結果をヘッダに付与し、ユーザが設定するスコア以上のメールをフィルタリングする。

・迷惑メールのブロックサービス

メールサーバ上で迷惑メールと判定されたメールに対して、スコアがヘッダに付与される。その後、件名に[meiwaku]を付記する、メールサーバ上の迷惑メールフォルダに隔離する、迷惑メールフォルダに隔離されたメールを通知する、の 3 つの設定を任意に選択できる。

迷惑メールフォルダに隔離されたメールは 14 日間保存され、ユーザが必要に応じて内容の確認を行うことができる。

・迷惑メールの自動判定サービス

迷惑メール判定エンジンでスコア付けし、その結果をヘッダに付与し、件名に [meiwaku] がオプションで付記される。

・メールの自動削除サービス

削除の設定に基づいて、条件に該当するメールをメールサーバ上で削除する。

３．４　送信元情報参照による判定(送信ドメイン認証)

自社から送信されるメールについて、送信元の IP アドレスを調査し、その結果をメールヘッダへ付与して配送する。

他ドメインから送信されたメールに対しても、メールサーバで送信元の認証を行い、その結果をメールヘッダへ付与して配送する。

３．５　IP25B

Ｆ社のメールサーバに対して、自社を含む ISP のメールサーバ等を経由せず、動的 IP アドレスから直接送信されるメールを規制。また、ボットも規制の対象となる。

３．６　その他

不正な通信を遮断するために送信元 IP アドレスの正当性を検証する uRPF を使用。

４　Ｇ社

Ｇ社の提供する迷惑メール対策サービスは、メール全般に関するオプションサービスとして、無料のサービス 1 種類と有料のサービスが 2 種類ある。迷惑メール対策サービスは、これらの種類によって利用できるものが異なり、「未承諾広告※」の表示があるメールを受信拒否するサービスは無料のサービスにおいても設定可能だが、迷惑メールのブロック及び条件設定による受信拒否の各サービスは有料のサービスにおいて提供される。

４．１　迷惑メールの判定

４．１．１　キーワード判定

・未承諾広告の受信拒否サービス

件名に「未承諾広告※」が含まれるメールの受信拒否ができる

・条件設定による受信拒否サービス

送信者アドレス(From:)の完全一致、前方一致(～で始まる)、後方一致(～で終わる)で指定が可能。件名(Subject:)は部分一致（～を含む）により指定が可能。

設定項目はそれぞれ ON、OFF の切り替えが可能で、受信拒否と受信許可を含めて最大 300 件まで登録することができる。

また、受信メールのサイズによる拒否設定も可能。

４．１．２　内容参照による判定(ヒューリスティックフィルタ)

・迷惑メールのブロックサービス

迷惑メール判定エンジンにより、メールサーバ上で一括して迷惑メールを判定し、迷惑メールと判定されたメールには、メールの件名に[spam]を付記する、あるいはメールサーバ上にある迷惑メールフォルダへ隔離し、ユーザが受信することがないようにも設定できる。初期設定は、メールの件名に[spam]を付記する設定になっている。

迷惑メールフォルダに隔離されたメールは 14 日間保存される。

４．２　ホワイトリスト

着信許可設定を行うことにより設定可能。受信拒否と併せて最大 300 件まで設定できる。

４．３　迷惑メール判定後の処理

着信拒否条件に該当しメールサーバ上にある迷惑メールフォルダへ隔離されたメールは保存期間経過後、メールサーバ上で削除され、復元することが出来ない。

４．４　送信元情報参照による判定(送信元 IP アドレス)

2008 年(平成 20 年)10 月より、迷惑メールを大量に送信する送信元 IP ア

ドレスをシステムにより自動判定し、迷惑メールの送信元以外から受信するメールを優先的に扱う、新たな迷惑メール対策システムを導入した。迷惑メールの送信元と判定された場合は、メールが届きにくくなるが破棄されることはない。

５　Ｈ社

Ｈ社の提供する迷惑メール対策サービスは、迷惑メールのブロックと判定のサービスがあり、ユーザの設定した条件にしたがって処理する。

５．１　迷惑メールの判定

５．１．１　キーワード判定

受け取りたくない相手の送信者アドレス(From:)や件名(Subject:)などのヘッダ情報に条件を設定し、条件にあてはまるメールを自動的に破棄することができる。条件は、受信許可も含めて最大 30 件まで任意の順番で指定することができる。

また、条件の設定に「指定したサイズ以下」、「指定したサイズを超える」も選択できる。

５．１．２　内容参照による判定(ヒューリスティックフィルタ)

メールサーバ上で迷惑メールと判定されたメールに対して、判定結果がヘッダに付記される。その後、件名に[meiwaku]を付記する。

５．２　ホワイトリスト

キーワード判定と同様に、ヘッダ情報に条件を設定し、条件に合致した場合に受信する。設定条件は、受信拒否とする条件と合わせて最大 30 件まで任意の順番で指定することができる。

５．３　迷惑メール判定後の処理

「受信」、「削除」、「本文を破棄しヘッダのみ受信」及び「識別ヘッダを付記」から選択できる。

６　Ｉ社

Ｉ社の提供する迷惑メール対策サービスは、特定のメールについて、メールフォルダに入る前に受信を拒否し、削除する。

６．１　迷惑メールの判定

６．１．１　キーワード判定(ブラックワード)

受信時の動作をメールアドレス及びドメイン名に応じて個別に指定することができる。

６．１．２　送信元情報参照による判定(ブラックリスト)

リアルタイムブラックリストデータベースを参照して迷惑メール受信数の軽減を図っている。データベースは、過去に迷惑メールの送信や不正中継の履歴があり十分な対策が施されていないメールサーバの IP アドレスが随時登録されているものである。初期設定では、このデータベースを利用した判定が ON になっている。

６．２　ホワイトリスト

メールアドレスを設定することができる。

６．３　迷惑メール判定後の処理

迷惑メールと判定されたメールへの動作には以下がある。

・受信
・削除
・Reject メッセージを送信者に返信
・User unknown メッセージを送信者に返信

７　Ｊ社

Ｊ社の提供する迷惑メール対策サービスには、迷惑メールと判定したメールをブロックする設定及び迷惑メールと判定したメールに表示を付加する設定がある。

７．１　迷惑メールの判定

７．１．１　キーワード判定(ブラックワード)

送信者アドレス(From:)、あて先アドレス(To:)、件名(Subject:)に任意のキーワードを設定可能（最大100件のパターン設定が可能)。この他、「未承諾広告※」の表示があるメール、Bcc で送信されてくるメール、件名(Subject:)・本文共に英文又は空白のメール(日本語などの2バイト文字を含まないメール)の受信拒否設定が可能。

７．１．２　内容参照による判定(ヒューリスティックフィルタ)

予め設定した基準にどの程度該当するかを判定し、一定の基準を超えた場合、規定文字列の[spam]を該当メールのメールヘッダー（メール件名）に自動的に付与する。

７．２　ホワイトリスト

送信者アドレス(From:)、あて先アドレス(To:)、写しあて先アドレス(Cc:)、件名(Subject:)、本文に任意のキーワードを設定し、該当するメールを受信することが可能。

また、設定した条件に合致するメールのみを受信することも可能。

７．３　迷惑メール判定後の処理

迷惑メールと判定されたメールに対して、件名に [spam] の表示が付記される。メールサーバでブロックする設定の場合には、メールサーバ上で自動的に削除される。

８　Ｋ社

Ｋ社の提供する迷惑メール対策サービスには、迷惑メールと判定されたメールの受信拒否サービス及び振り分けサービスがある。

８．１　迷惑メールの判定

８．１．１　キーワード判定

送信者アドレス(From:)、あて先アドレス(To:)、件名(Subject:)について、単独又は２つまでの組み合わせで受信拒否条件を設定できる。設定可能な条件の数は２つまでの組み合わせを１ペアとして 100 ペア、合計 200 件まで登録することができる。

指定した容量を越えるメールを受信拒否とする設定も可能。

８．１．２　内容参照による判定(シグネチャーフィルタ)

迷惑メール判定度として、最高／高／中／低の 4 段階まで設定可能。判定後に、その結果をヘッダに付記する。

また、ブラックリストにユーザが明らかに迷惑と考えるメールの条件を設定することにより、必ず迷惑メールと判定される。

８．２　ホワイトリスト

送信者アドレス(From:)、あて先アドレス(To:)、件名(Subject:)について、任意のキーワードを設定可能。パスリスト（最大 100 件）に設定された特定のアドレスからのメールに対して、迷惑メール判定を行わないようにすることも可能。

８．３　迷惑メール判定後の処理

・受信拒否サービス

設定条件に合致するすべてのメールはメールサーバ上で削除される。

・振り分けサービス

判定後の処理は、(1)と(2)のどちらかを選択可能。

(1)ラベリング

判定メールに対して、件名に[meiwaku] が付記される。

(2)メールサーバ上のフォルダに振り分け

件名に[meiwaku]と付記したメールを、メールサーバ上の専用フォルダに振り分ける。これにより、迷惑メールと判定されたメールを一切ダウンロードしないことが可能（専用フォルダへ振り分けられたメールの閲覧はメールサーバ上で行うことが可能)。

９　Ｌ社

Ｌ社の提供する迷惑メール対策サービスは、メールサーバ上で迷惑メールを自動判定し、迷惑メールの件名に[meiwaku]を付記する。

９．１　迷惑メールの判定

９．１．１　キーワード判定(ブラックリスト)

送信者アドレス(From:)、あて先アドレス(To:)、写しあて先アドレス(CC:)について 500 件まで登録可能。

９．１．２　内容参照による判定(シグネチャーフィルタ)

迷惑メール判定エンジン（1 日当たり 100 万件近くにのぼる迷惑メール攻撃に関する情報を収集・分析した情報を元に迷惑メールの判定を行うもの）を使用し、メールサーバ上で迷惑メールの判定を行う。

９．２　ホワイトリスト

送信者アドレス(From:)、あて先アドレス(To:)、写しあて先アドレス(CC:)について 500 件登録することができる。受信したメールが迷惑メールであるか否かによらずに迷惑メール判定の対象外とすることができる。

９．３　迷惑メール判定後の処理

迷惑メール判定エンジンを使用し、メールサーバ上で一括して迷惑メールの判定を行い、判定されたメールは件名（Subject:）に [meiwaku] を付記する。以下の判定結果によって各案内のメールが送付される（元のメールは添付される。案内のメールの送信者アドレス(From:)及び件名（Subject:）は元のメールと同様。）。

(1)送信者アドレス(From:)がメールアドレスとして正しい場合
　誤判定の可能性があるため、クリックするだけで、自動的に送信者アドレス(From:)をホワイトリストに登録できる URL を案内するメールを送信。

(2)送信者アドレス(From:)がない又は空欄の場合
　送信者アドレス(From:)がない又は空欄の場合のメールの受信拒否機能を案内するメールを送信。

(3)送信者アドレス(From:)がメールアドレスとして正しくない場合
　迷惑メール判定を案内するメールを送信。

なお、Web メール利用者は、迷惑メールと判定されたメールを迷惑メールフォルダに振り分ける事が可能。さらに、ユーザの設定によって、[meiwaku]の文字を挿入しない、上記文言を挿入しない等の設定も可能。

加えて、Web メールで表示されているアドレスをワンタッチでブラックリストやホワイトリストに登録が可能となっている。

１０　Ｍ社

Ｍ社の提供する迷惑メール対策サービスには、未登録のアドレスから送信されるメール又は迷惑メールと判定されるメールをブロックするサービスや自動的に振り分けるサービス等がある。

それぞれ対策サービスは、以下の順に適用される。

1.受信拒否アドレスリストの判定
2.受信拒否条件の判定
3.未登録アドレスブロックの判定、
4.学習型フィルタセーフリストの判定
5.学習型フィルタのスパム判定

※「未登録アドレスブロック」と「学習型フィルタ」の併用は出来ない。

１０．１　迷惑メールの判定

１０．１．１　キーワード判定

・未登録のアドレスから送信されるメールのブロックサービス

アドレスブックや許可リストに登録してあるアドレス以外は、すべて迷惑メールフォルダに振り分けられる。

・迷惑メールと判定されるメールのブロックサービス

送信者アドレス(From:)、あて先アドレス(To:)、写しあて先アドレス(CC:)、件名(Subject:)及びメールの容量の 5 項目について、キーワード（メール容量については数値)を、単独又は組み合わせで合計 100 パターンまで受信拒否条件として設定することができる。

ワイルドカードを使った受信拒否条件の設定も可能。また、送信者アドレス(From:)、件名(Subject:)等のヘッダに空欄を含むメールを一括拒否することもできる。

１０．１．２　内容参照による判定

・ベイジアンフィルタ

ベイズ理論を応用した迷惑メール判定エンジンを用いたフィルタであり、振り分けた迷惑メールの特徴をフィルタが自ら学習し、メールアドレスを変えた同内容の迷惑メール等にも自動的に対応する。

なお、学習型フィルタをすり抜けてきた迷惑メールを手動でフィルタに学習させることや、フィルタの学習度(精度)を表示することも可能である。

迷惑メール判定エンジンは、受信メールをスコア付けし、その結果をヘッダに付記する。迷惑メールと判定されたメールは、件名に[SPAM]が付記され、メールサーバ上で内容を WEB ブラウザから確認できる。ホワイトリストの設定や、自動削除の設定もできる。

・ヒューリスティックフィルタ

迷惑メール判定エンジンを使用し、メールサーバ上で迷惑メールを判定し、Ｍ社の基準で迷惑メールと判定されたメールは、自動で迷惑メールフ

ォルダに振り分けられる。
　ホワイトリストの設定もできる。
・シグネチャーフィルタ
　迷惑メール判定エンジン（多数の迷惑メール特有の情報を抽出しておき、受信したメールと比較を行うもの。迷惑メール特有の情報は、世界 20 カ国以上のハニーポッドから収集した情報を活用し、精度の向上が図られている）を使用し、迷惑メールの判定を行う。

１０．１．４　受信トラフィック制御
　Ｍ社に向けて大量の架空アドレスあてメールを送信する送信元からの受信を拒否する対策が実施されている。Ｍ社メールサーバがあて先不明のメールを大量に受信したことを検知した時点で、その送信元の IP アドレスからの受信を拒否する。

１０．２　ホワイトリスト
　送信者アドレス(From:)、あて先アドレス(To:)、写しあて先アドレス(CC:)、件名(Subject:)及びメールの容量の 5 項目について、任意のキーワード（メール容量については数値)を、単独又は組み合わせで受信許可条件として設定できる。設定可能な条件の数は、受信拒否の条件と合わせて合計 100 件。

１０．３　迷惑メール判定後の処理
・未登録のアドレスから送信されるメールのブロックサービス
　アドレス帳や許可リストに登録してあるアドレス以外は、すべて迷惑メールフォルダに振り分けられる。
・迷惑メールと判定されるメールのブロックサービス
　「受信拒否」、「ごみ箱に移動」、「迷惑メールフォルダに移動」の中から動作を設定する。「ごみ箱に移動」と「迷惑メールフォルダに移動」については、メールソフトへの転送は行われない。受信拒否したメールは、破棄される。
・自動振り分けサービス
　Ｍ社があらかじめ定めた基準に基づいて迷惑メールを判定し、メールボックスに受信した時点で迷惑メールフォルダに自動的に振り分けられる。

１０．４　IP25B
　Ｆ社のメールサーバに対して、ISP のメールサーバ等を経由せず、動的 IP アドレスから直接送信されるメールをブロック。

１１　Ｎ社

Ｎ社の提供する迷惑メール対策サービスには、学習型迷惑メールフィルタ、特定のメールを受信拒否するサービスがある。

１１．１　迷惑メールの判定

１１．１．１　キーワード判定(ブラックワード)

送信者アドレス(From:)、件名(Subject:)について設定件数はそれぞれ 5 件任意のキーワードを設定可能

１１．１．２　内容参照による判定(ベイジアンフィルタ)

受信者ごとに用意される学習型フィルタを通じ、ユーザが受信メールの中から迷惑メールを指定すれば、そのメールの特徴をフィルタが学習し、以降の判定に用いられる。フィルタを継続使用することで判定精度が向上する。

１１．２　迷惑メール判定後の処理

学習型迷惑メールフィルタで迷惑メールと判定されたメールは、件名に「meiwaku」が付記される。

また、受信拒否の設定をしたメールは、サーバ上で削除される。

１２　Ｏ社

Ｏ社の提供する迷惑メール対策サービスには、迷惑メールの自動判定、受け取りたくないメールの受信拒否サービスがある。両方のサービスを同時に利用することが可能であるが、いずれかのサービスの拒否条件に合致したメールは、メールボックスに届かず削除される。

１２．１　迷惑メールの判定

１２．１．１　キーワード判定

受け取りたくない相手の送信者アドレス(From:)、あて先アドレス(To:)、写しあて先アドレス(CC:)、件名(Subject:)などのヘッダ情報に対して任意のキーワードを設定できる。設定可能な条件数は、送信者アドレス(From:)1000 件まで、あて先アドレス(To:)100 件まで、写しあて先アドレス(CC:)100 件まで、件名(Subject:)500 件まで、その他任意のヘッダ(1～3 種類)合計 300 件までとなる。送信者アドレス(From:)、あて先アドレス(To:)、写しあて先アドレス(CC:)、件名(Subject:)の他にも、Received(経由したサーバ)、メールソフト名(X-mailer:)など、拒否したいメールのヘッダを 3 種類まで自由に設定できる。

さらに、件名(Subject:)がない、送信者アドレス(From:)がない、未承諾広告※の表示があるなども受信拒否条件として設定可能。

また、受信するメールのデータ容量の上限を、最大 5Mバイトまで１バイト単位で設定できる。

１２．１．２　送信元情報参照による判定

SPF 方式及び DKIM 方式による送信ドメイン認証を実施している。認証結果は、ヘッダに付加し、受信者側で送信者アドレス(From:)の偽装の判定が可能となる。

SPF 方式及び DKIM 方式双方の方式を導入することにより、より精度の高い送信ドメイン認証の実現が可能としている。

１２．１．３　内容参照による判定

・ベイジアンフィルタ

迷惑メールコミュニティから収集されるサンプルに基づき、迷惑メールを自動判定している。

また、ユーザ自身が迷惑メールを申告しやすいように Web メールからの申告と Outlook Express 用のアドインを利用し申告ができる方法が提供されている。(2008 年(平成 20 年)7 月提供開始)

・ヒューリスティックフィルタ

受信メールのヘッダや本文の情報から迷惑メールの特徴などをスコア化し、スコアが基準値(ユーザが任意に設定できる)を超える場合に迷惑メールとして判定する。

１２．１．４　受信トラフィック制御(送信者アドレス)

送信者アドレス(From:)が存在しない偽装メールアドレスからのメールの受信拒否が実施されている。迷惑メールは、送信者アドレス(From:)を詐称している場合が多いため、送信者アドレス(From:)が存在しないメールを迷惑メールと判定し、Ｏ社メールサーバ上で受信拒否する。

１２．２　ホワイトリスト

受け取りたい相手の送信者アドレス(From:)、あて先アドレス(To:)、写しあて先アドレス(CC:)、件名(Subject:)にキーワードを、単独又は組み合わせて設定し、合計 2,000 件登録することができる。設定されたアドレスからのメールに対しては、迷惑メール判定を行わないようにすることができる。

１２．３　迷惑メール判定後の処理

・受け取りたくないメールの受信拒否サービス

条件に該当したメールをサーバ上で削除する。送信者に自動的にメッセージを返信することもでき、返信メールのタイトルとメッセージ内容、該当したメールを添付する場合の形式が指定可能。該当メールの条件(ヘッダ条件、サイズ、時間)により返信するメッセージを変えることも可能。

・迷惑メールの自動判定サービス

受信メールのヘッダや本文の情報から迷惑メールの特徴などをスコア化し、スコアが基準値(ユーザが任意に設定できる)を超える場合に迷惑メールとして判定する。判定後は、ヘッダ部分に判定結果が付与され、件名に[spam]が付記される(付記しない設定も可能)ので、ユーザの使用しているメールソフトで振り分けることが可能となる。

有料オプションとして迷惑メールと判定されたメールをサーバ上の迷惑メールフォルダに保存し、ユーザには件数及びヘッダ、送信者アドレス(From:)、件名(Subject:)を翌日にメール配信するサービスがある(配信しない設定も可能)。迷惑メールフォルダの保存期間は初期設定では 10 日で、ユーザが 1～31 日の範囲で指定できる。

１３　Ｐ社

Ｐ社の提供する迷惑メール対策サービスには、迷惑メール自動振り分けサービスがある。

１３．１　迷惑メールの判定

１３．１．１　キーワード判定

送信者アドレス(From:)(最大 5 個)、あて先アドレス(To:)又は写しあて先アドレス(CC:)(最大 5 個)、件名(Subject:)(最大 5 個)、その他任意のヘッダ、メール容量(最大 5 個)、メールソフト名(X-mailer:)(最大 5 個)の条件を複合的に組み合わせ受信拒否の条件を最大 99 件まで設定できる。

１３．１．２　内容参照による判定

迷惑メールの判定レベル及び迷惑メールと判定されたメールの取り扱いについて、受信者の利用形態に合わせ 4 つのレベルから選択可能。

１３．２　ホワイトリスト

送信者アドレス(From:)(最大 5 個)、あて先アドレス(To:)又は写しあて先アドレス(CC:)(最大 5 個)、件名(Subject:)(最大 5 個)、その他任意のヘッダ (最大 5 個)、メールソフト名(X-mailer:)(最大 5 個)の条件を複合的に組み合わせ受信拒否の条件を最大 99 件まで設定できる。

１３．３　迷惑メール判定後の処理

迷惑メールと判定されたメールの扱いとして、「P 社の迷惑メールフォルダに振り分け」、「件名に[meiwaku]を付記」、「削除」の 3 つから、選択できる。

１４　Ｑ社

Ｑ社の提供する迷惑メール対策サービスには、迷惑メールの振り分け、学習型の迷惑メールフィルタなどがある。

１４．１　迷惑メールの判定

１４．１．１　キーワード判定(ブラックワード)

メールアドレス又はドメイン名を受信拒否条件として 500 件まで設定可能。

１４．１．２　送信元情報参照による判定

・レピュテーション

IP アドレスなどの評判情報を蓄積し、その情報をもとに迷惑メールの度合いを判定する

・なりすましメール拒否

Domainkeys と SPF の認証結果を用いて、差出人が詐称されている場合に該当のメールを受信拒否する。また特定のメールアドレス・ドメインについて拒否したくない場合は救済リストとして 100 件まで設定可能。

１４．１．３　内容参照による判定

・ベイジアンフィルタ

自社の迷惑メール判定エンジンを使用した受信者ごとに用意される学習型フィルタを通じ、ユーザが受信メールの中から迷惑メールを指定すれば、そのメールの特徴をフィルタが学習し、以降の受信メールから迷惑メールを判定する。フィルタを継続使用することで判定精度が向上する。

・シグネチャーフィルタ

自社の迷惑メール判定エンジンを使用し、多数の迷惑メール特有の情報を抽出し、自動的に迷惑メールフォルダへ振り分ける。

迷惑メールと判定する条件は、Ｑ社の迷惑メール報告の機能によって寄せられた情報を、蓄積・分析した結果を参考にして設定している。

・ヒューリスティックフィルタ

自社の迷惑メール判定エンジンを使用し、迷惑メールに使われやすい特徴、単語や色、フォントなどを登録しておき、該当項目数の一定以上を超えると迷惑メールフォルダへ振り分ける。

１４．２　ホワイトリスト

送信者アドレス(From:)、あて先アドレス(To:)、写しあて先アドレス(CC:)、件名(Subject:)、本文にキーワードを、設定できる。特定のアドレスからのメールに対して、迷惑メール判定を行わないようにすることもできる。

１４．３　受信トラフィックによる判定

一定時間内に特定のユーザあてに大量送信を行うサーバや、大量のあて先

不明のメールの送信を行うサーバに対し、応答を一時的に遅延させる仕組みを導入。流量に応じて、数時間～数十時間の遅延処置がとられる

１４．４　迷惑メール判定後の処理

迷惑メールと判定されたメールは、メールサーバ上の迷惑メールフォルダへ自動的に移動される。

１４．５　IP25B

大手 ISP からの依頼により実施。Q社のメールサーバに対して、ISP のメールサーバ等を経由せず、動的 IP アドレスから直接送信されるメールをブロック。

１５　Ｒ社

Ｒ社の提供する迷惑メール対策サービスには、設定した条件に合致するメールの受信を拒否し、サーバから削除するサービスがある。

21年度中または22年度早期に自動でスパム判定を行なうシステムを導入予定。

１５．１　迷惑メールの判定

１５．１．１　キーワード判定(ブラックワード)

受け取りたくない相手の送信者アドレス(From:)、あて先アドレス(To:)、写しあて先アドレス(CC:)、件名(Subject:)にキーワードを、単独又は組み合わせで設定可能。2 ペアで許可設定も含めて合計 20 件登録することができる。

１５．２　ホワイトリスト

受け取りたい相手の送信者アドレス(From:)、あて先アドレス(To:)、写しあて先アドレス(CC:)、件名(Subject:)にキーワードを、単独又は組み合わせて設定可能。2ペアで拒否設定も含めて合計20件登録することができる。

１５．３　迷惑メール判定後の処理

迷惑メールと判定されたメールは、メールサーバ上で削除される。

１６　Ｓ社

Ｓ社の提供する迷惑メール対策サービスには、迷惑メールと判定したメールを拒否する、ユーザが設定した条件でメールを拒否するサービスがある

１６．１　迷惑メールの判定

１６．１．１　キーワード判定(ブラックワード)

拒否したいメールアドレス、ドメイン名を指定して受信拒否設定が可能。最大 50 件設定できる。

１６．１．２　内容参照による判定

Ｓ社が迷惑メールと判定したメールを拒否する。

１６．２　ホワイトリスト

メールアドレス、ドメインを指定して受信許可条件設定が可能。最大 50 件設定できる。

１６．３　迷惑メール判定後の処理

迷惑メールと判定したメールの処理として、ヘッダに特定の文字列を付加又は迷惑メールフォルダに割り振りのいずれかを選択できる。迷惑メールフォルダに割り振られたメールの保存期間は 7 日間で、保存期間経過後は自動的に削除される。

（別表３）主要な固定系 ISP が提供する迷惑メール受信対策一覧

	(1)キーワード			(2)送信元情報参照	(3)内容参照			(4)受信トラフィック	(5)ホワイトリスト	(6)IP 25B
	ブラックワード	容量	添付		ベイジアン	ヒューリスティック	シグネチャー			
D社	○	○	○	送信ドメイン認証		○			○	
E社	○					○			○	
F社	○			送信ドメイン認証		○	○		○	○
G社	○	○		IP アドレス		○			○	
H社	○	○							○	
I 社	○			ブラックリスト (RBL)					○	
J社	○					○			○	
K社	○	○					○		○	
L社	○						○		○	
M社	○	○			○	○	○	○	○	○
N社	○				○					
O社	○	○		送信ドメイン認証	○	○		○	○	
P社	○	○		○		○	○	○	○	
Q社	○				○	○	○	○	○	○
R社	○								○	
S社	○		○			○	○	○	○	