

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24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)の第一次改正では、特定電子メールへの範囲への企業や事業を営む個人が利用している事業用メールアドレス宛ての広告宣伝メールの追加、送信者情報の偽装禁止、罰則の強化等が行われた。

さらに、2008年(平成20年)には、特定電子メール法の第二次改正が行われ、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。

このような法改正や、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導入も拡大されてきた。

その対策の一つである Outbound Port 25 Blocking に関しては、国内の主要な ISP で導入されており、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、なりすまし対策として有効な送信ドメイン認証技術に関しても、国内の主要な ISP での導入が徐々に進んできており、総務省の調査によれば、2011年(平成23年)11月現在、ISP 約90社において導入されている。

技術的な対策は、迷惑メールを一定程度抑制できるものであることから、その取組に対する期待が大きい。

こうした状況等を踏まえ、昨年に引き続き、迷惑メール対策関連技術及び ISP による技術的対策の導入状況等について、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	4
第 1 節 迷惑メール送信防止のための技術動向	4
第 2 節 迷惑メール受信防止のための技術動向	9
第 2 章 迷惑メールに関する移動系 ISP の対策導入状況	18
第 1 節 迷惑メール送信防止対策の導入状況	18
第 2 節 迷惑メール受信防止対策の提供状況	21
第 3 節 SMS を利用した迷惑メール送信防止対策の提供状況	39
第 4 節 SMS を利用した迷惑メール受信対策の提供状況	40
第 3 章 迷惑メールに関する固定系 ISP の対策提供状況	43
第 1 節 迷惑メール送信防止対策の提供状況	43
第 2 節 迷惑メール受信防止対策の提供状況	52

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

ISPにおいては、自社ネットワークからの迷惑メール送信が行われないうような様々な対策を行っている。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

迷惑メール送信の特徴である「大量のメール一括送信」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) 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、対策が不十分な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。

(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。

2 送信者認証

他人になりすました送信者が迷惑メールを送信するのを防止するため、送信者側のISPで自社メールサーバから送信しようとする送信者を確認する方法である。

・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が必須である。

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等により、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。

(参考) 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。

3 送信者アドレス照合

送信者アドレスは比較的簡単に換えられる場合が多いので、送信者認証をパスしても送信者アドレスを変えて迷惑メールを送信することが多い。これを阻止するため、送信時の送信者アドレスを送信者認証したIDに対応する送信者アドレスと照合するもの。一致しない場合、送信しない、本来の送信アドレスに書き換えて送信する等の対策が取られる。

4 送信認証情報漏えいに対する対策

迷惑メール送信者は、送信者認証に使うID/パスワードを推測し、送信者認証を成功させることがある。これを防止するため、一定回数以上認証に失敗した場合、送信させない対策である。

(1) アカウントロック

送信者認証時、あらかじめ登録していた回数以上パスワード入力を誤ると一時的に利用停止となるもの。この際、警報を出力することでシステム管理者が不正アクセスを検知できる場合もある。

(2) IPアドレスブロック

同一のIPアドレスからの送信者認証が一定回数以上失敗した場合、そのIPアドレスからの接続を拒否するもの。アカウントロックを回避するため1ID当たりのアクセス回数を少なくし、IDを次々に変えてアクセスしてくる迷惑メール送信者に有効である。

5 転送機能の利用制限

メールサーバの多くは、受信者があらかじめ設定した宛先へ受信メールを自動転送する機能を備えている。この機能を利用している場合、受信者に迷惑メールが届くと同時に設定したアドレスに迷惑メールが配信されてしまう。転送先が、転送しているメールサーバを迷惑メール送信サーバとみなし、受信を拒否する場合もある。これを防止するため以下のような対策が考えられている。

(1) フィルタリング転送

転送する前に迷惑メールフィルタ等で迷惑メールを除去し、その後、転送するもの。

(2) 転送設定解除

受信者が転送設定の最新化を忘れている場合、存在しない宛先へ転送し続けるのを避けるため、一定回数以上転送を失敗した場合転送を解除するもの。

転送しているメールサーバが、宛先不明メール送信サーバとして受信側に拒否されたり、宛先不明に伴うエラーメールが転送者ではなく元のメール送信者に返り混乱するのを防ぐことができる。

(3) 転送アドレス書換え

転送する場合の送信者アドレスを、元の送信者のアドレスではなく転送者のアドレスに書き換えるもの。

6 OP25B (Outbound Port 25 Blocking)

迷惑メール送信者は、ISPの迷惑メール対策を回避するため、契約先のISPのメールサーバを使わず、自前で設置するメールサーバやボットネットを利用して直接メール送信を行うことが多い。

この際、使用されるIPアドレスは、使用者を特定しにくい動的IPアドレスであることが多い。このため、ISPのメールサーバを使用せず、動的IPアドレスを割り振られたサーバから直接メール送信するのを阻止するのが、OP25B である。

(1) 仕組み

メール送信は受信側メールサーバの 25 番ポートに向けて行われる。OP25B は、ISP のメールサーバ以外の動的 IP アドレスを持つ機器から 25 番ポート向けに発信される通信を遮断する。

ISP が OP25B を実施すると、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。

これに対処するため、多くの ISP では、メール配信用ポート 25 番とは別に、メール投稿用ポート 587 番を認証機能 (SMTP AUTH) 必須として提供している。

なお、この際、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。

(2) 導入状況

OP25B は、我が国では平成 17 年 (2005 年) 1 月に初めて携帯電話向け送信に導入された。平成 18 年 (2006 年) 6 月頃から ISP での導入が進展し、平成 23 年 (2011 年) 6 月には 91 社にまで拡大した。(図 1-1)

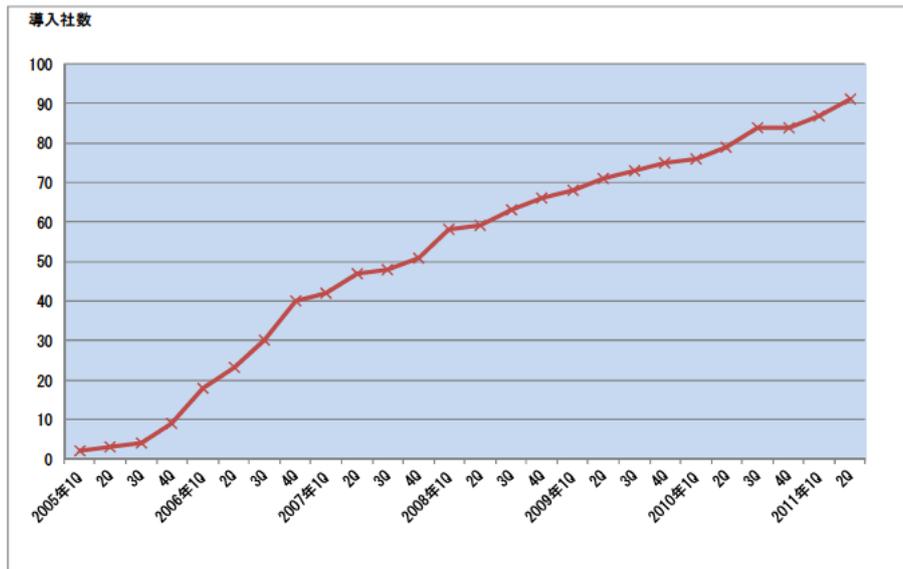


図1-1 国内ISPのOP25B導入推移

(3) OP25B の導入効果

図1-2は、OP25Bの導入状況と日本のスパム送信国ランキングである。ISPにおけるOP25Bの導入が進むにつれて、日本の迷惑メール送信国ランキングが下がっている状況がうかがえる。

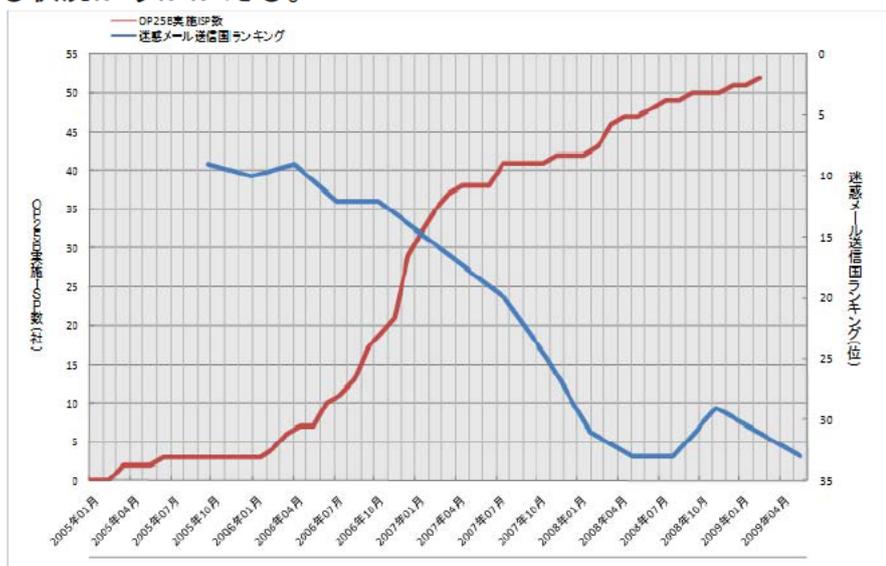


図1-2 国内のOP25B導入状況と日本の迷惑メール送信国ランキング
(出典：日本データ通信協会迷惑メール相談センター及びソフォス社資料より作成)

(4) OP25B の今後の課題

OP25Bの導入は迷惑メール送信抑止に大きな効果を上げてきたが、迷惑メール撲滅に向け以下のような課題が挙げられる。

① OP25B未導入ISPにおける早期導入

② 海外への普及

サービス制限の考え方の違いなどから海外ではあまり普及していない。海外発の迷惑メールが多い現状を見ても、海外ISPでの早期導入が望まれる。

③ ISP内のメールに対する導入

ISP内のメールにOP25Bを導入しているところは少ないが、契約者である迷惑メール送信者が、ISPの受信メールサーバへ容易に迷惑メールを送ることが可能であることからOP25Bの導入が望まれる。

第2節 迷惑メール受信防止のための技術動向

受信側では、以下の方法で迷惑メールであることを判定し、迷惑メールをブロックしたり、受信を制限する等の対策を講じている。

1 受信メールの特徴判定

迷惑メールの特徴である「大量受信」や宛先不明を検出し、受信を制御する方法。

(1) 連続メール受信

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が基準を超えた場合、受信を制限するもの。

ただし、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たり、ポットネットを利用し1台当たりの送信数を抑えているようなケースには対応が困難である。

このため、送信元が同じである場合には、該当するメールアドレスやドメイン単位で受信制限する手法も行われている。

(2) エラーメール受信

特定IPアドレスから、宛先不明なメールを多数受信するかどうかで判断する。宛先不明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、宛先不明メールが多い場合は受信を行わないようにするもの。

2 受信メールの内容判定

迷惑メールの外形的な内容（メールサイズ、URLの有無等）から、受信を制御する方法。

(1) メール容量

受信メールの容量(サイズ)により判定するもの。迷惑メールに多い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にする。

(2) URL 有無

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。

(3) キーワード（ブラックワード）

メールのヘッダ及び本文中に特定のキーワードが存在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り分けのための機能であるが、きめの細かい設定により、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。

しかし、ブラックワードだけで迷惑メールを判定しようとする、悪意ある送信者は、人間には判読できるがPCの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ることで判定できるようにしておくことが効果的である¹。

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）
- ・宛先（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）

(4) 迷惑メールフィルタ

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。

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、ユーザー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攪乱するものも出現しており、フィルタ側で更なる対応を図っている。

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、迷惑メールと判断してするもの。

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

¹ replica を”r_e_p_l_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。

やHTMLメールでかつ画像だけのケースを迷惑メールとする”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」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。

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²⁾)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、また、メールシステムの管理者による負担も少ないと言われている。

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いう点がある。

(5) 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とを比較して行う。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³⁾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。

3 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、迷惑メールと判断された場合に受信制限する方法。

² 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。

³ 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。

(1) ブラックリスト (RBL : Realtime Black List)

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ブラックリストにある IP アドレスからのメールを、迷惑メールと判定するもの。

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問題もあり、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) グレーリスト

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。

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は、受信に当たって数時間遅延してしまうという点にある。

(3) 送信ドメイン認証技術

迷惑メール送信者は送信者を特定しづらくするため、迷惑メールを送信する際、有名なサイトのドメイン等を詐称して送信することが多い。受信側でこの詐称を検出できるようにするのが送信ドメイン認証技術である。送信ドメイン認証技術の導入により、認証結果を踏まえて、詐称と判断されたメールは受信しない等の対策がとれるようになる。

送信ドメイン認証技術には、送信元の IP アドレスを利用するネットワークベースのもの (SPF/Sender ID) と送信者が作成する電子署名を利用するもの (DKIM) がある。

① ネットワークベースの送信ドメイン認証技術 (SPF/Sender ID)

送信メールサーバをその IP アドレスを用いて認証を行うものである。

送信側では、メールアドレスのドメイン名とこのメールを送信するサーバの IP アドレス等の送信元情報を DNS サーバに登録する。これを SPF (Sender Policy Framework) レコードという。

受信側では、メール受信時に、送信者情報から抽出したドメイン名で DNS から SPF レコードを取得し、SPF レコードに記載されている IP アドレスと、SMTP で接続した先の送信メールサーバの IP アドレスが一致するかどうかを検証する。

この方式は、送信側 DNS への SPF レコード追加と受信側における受信メールの

送信者情報検証で実現可能であり、特に送信側では、コスト負担も少なく、導入が容易であるといわれている。

この方式の課題として、メール転送時など配送経路が変わった場合に、認証に失敗する場合があるという点が指摘されている。この課題の解決策としては、転送アドレスを書き換える方法がある。転送時に、転送元のドメインに送信者情報を書き換えて送信すれば、受信側では転送元のドメインで認証することとなり、認証が可能となる。また、受信者において、転送元のメールアドレスをホワイトリストに入れておき、送信ドメイン認証技術の結果を利用しないで受信するという方法もある。

② 電子署名ベースの送信ドメイン認証技術 (DKIM)

送信メールサーバを公開鍵暗号化技術を用いて認証を行うものである。

送信側では、あらかじめ自ドメインに対する公開鍵を DNS に登録する。送信メールサーバは、メール送信時に、1 通ずつ秘密鍵で電子署名を作成し、関連情報とともにメールヘッダに付加して送信する。

受信側では、メールヘッダからこの付加情報を取り出し DNS から公開鍵を取得する。取得した公開鍵を使って電子署名を復号し、検証する。

DKIM は、メール転送時の配送経路変更に対しても正しく認証でき、また、メール本文の改竄も検知できる。

ただし、導入に際し、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といわれている。

③ 送信側での設定状況

WIDE Project⁴の Anti-spam Working Group では jp ドメインにおける送信ドメイン認証技術への対応状況を年 2 回報告している。それによると SPF/Sender ID の 2011 年 (平成 23 年) 11 月現在の普及率は 43.5% となっており、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、各団体へ意識が浸透してきていることがうかがえる。また、DKIM については、普及率は約 0.5% となっている。

また、総務省では実際に流通している電子メールにおける送信ドメイン認証技術への対応状況を調査している。それによると、2011 年 (平成 23 年) 11 月現在、約 9 割のメールが SPF/Sender ID に対応しており、約 2 割のメールが DKIM に対応している。

⁴ <http://www.wide.ad.jp/index-j.html>

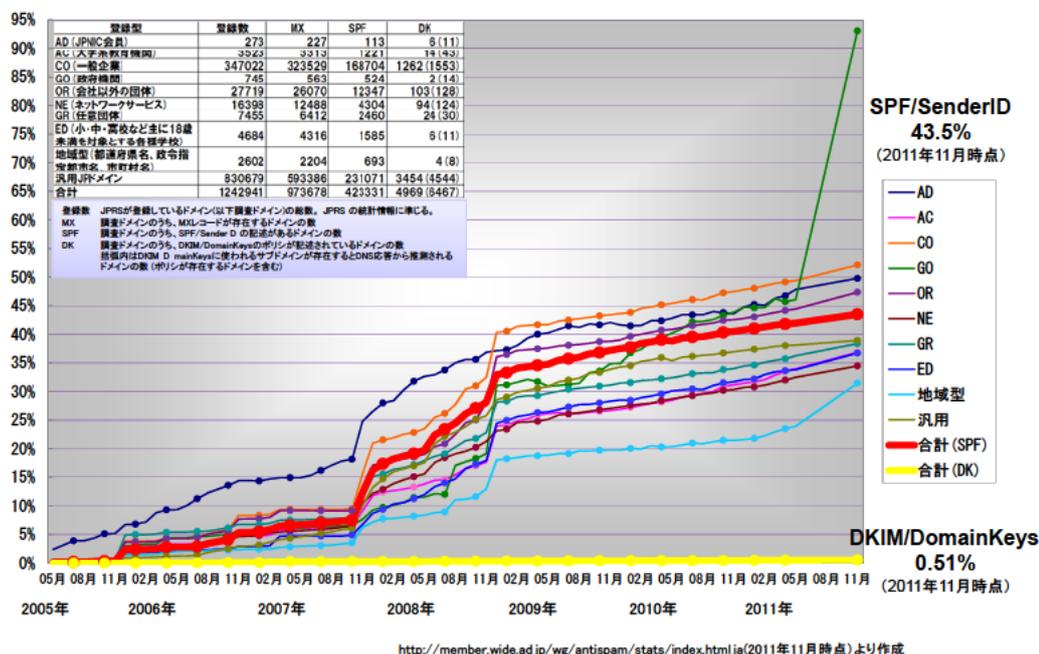


図1-3 送信ドメイン認証技術の導入状況

(4) 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からレピュテーションの格付けをする。

(5) IP25B (Inbound Port 25 Blocking)

迷惑メール送信者が、ISPの迷惑メール対策を回避するため、ISPのメールサーバを使わず直接送信してくる迷惑メールを受信しないようにするもの。

OP25Bが、ISP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であるのに対し、IP25Bは、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のネットワークや、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。

4 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、迷惑メール判定が緩めだと①が増加し、迷惑メール判定を厳しく行くと②が増加する。

このうち、實際上問題となるのは、②の場合が多い。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、利用者個々ではなくサーバ単位でホワイトリストを設定することもある。

(1) ホワイトリスト（送信者アドレス・ドメイン）

正当な送信者としてメールを受け取ることが必要な送信者アドレス又は送信者のドメインを登録するもの。

(2) ホワイトリスト（ヘッダ、本文）

正当なメールの内容として、メールを受け取ることが必要な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。

5 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、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。

この方式は、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。

(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（及び宛先）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) したがって、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 送信ドメイン認証技術を受信側で実施することに伴う法律上の見解

- (1) 送信ドメイン認証技術は、法的に見れば「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電子メール送受信上の支障のおそれを減少させるための行為と認められ、送信ドメイン認証技術は、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。

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（及び宛先）と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、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送信防止対策の状況は、次のとおりである。なお、事業者によっては措置の発動基準等を明確にしていない場合もある。

1 宛先不明メールの受信拒否

移動系 ISP5 社は、宛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

(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) B社

24時間以内に1,000件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としていたが、2008年(平成20年)3月27日から送信できる宛先数を500件としている。

(3) C社

1日当たり1,000宛先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宛先までとしている。

また、1回の送信処理で同時に複数の宛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件だった同報送信宛先数を、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、同報送信宛先数を30件に変更している。

(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なっている。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も利用停止などの措置を行なっている。その際、注意喚起を行ったにもかかわらず、迷惑メール送信行為を継続した場合には、契約を解除している。

(5) U社

1日1台当たりの送信を1,000回未満に、同報送信宛先数を1回当たり10件までに制限している。

3 メールアドレスの初期設定の変更

当初は、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」を用いる移動系 ISP もあったが、現在では、T社を除く4社は推測されにくい「複数のランダムな英数字@×××.ne.jp」とし、T社は初期設定はなく、必ずユーザー指定としている。

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るおそれがあることから、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回までに制限した（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 送信ドメイン認証技術の導入（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 レコードの記述を実施している。

(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。

(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。

(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。

(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) 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

(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 宛てに送信されるメールについて、OP25Bを実施している。

また、2008年（平成20年）7月から、インターネット接続サービス（別途申込が必要）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。

(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宛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 宛てのメールの送信についても、OP25B を実施している。

(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宛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社宛てに送信されるメールについて、2008年(平成20年)9月からは固定系 ISP 宛てのメールについても、OP25B を実施している。

(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宛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 宛てのメール送信についても、順次 OP25B を実施している。

(5) U社

携帯電話事業者向けには、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月より順次開始し同年7月に全適用が完了した。

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、本来必要となる電子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) A社

携帯電話及び PHS、インターネット（携帯電話及び PHS 以外からの全て）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。

また、2009年（平成21年）11月以降に販売開始した携帯電話機（一部除く）については、受信したメール表示画面から直接、受信／拒否設定を簡易に設定する機能が追加された。

設定件数は、受信では最大120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120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ーを使用するかどうかの選択もできる。

(2) B社

全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、任意のメールアドレス・電話番号を受信許可・受信拒否する「アドレス指定設定」がある。メールの受信許可・受信拒否は、それぞれ最大300件。また携帯電話事業者及び PHS 事業者からのみ受信を選択可能。受信許可、受信拒否、携帯電話事業者及び PHS 事業者からのみ受信は併用可能。電話番号メールは、許可・拒否いずれか選択で最大150件。

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、以下①～③の中から選択できる。

- 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。

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、申し込みが必要となる。

(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 以外からの全て）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 200 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、以下となる。

- 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

具体的な指定受信の設定例としては、移動系 ISP5 社からの電子メールは全て受信し、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 からの電子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。

(4) T社

特定のアドレス、ドメイン、サブドメイン、全てのアドレス、全ての@を含むアドレス、@のないメールなど返信できないメールアドレスを最大 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。

(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

(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 送信ドメイン認証技術

2007 年(平成 19 年)11 月より送信ドメイン認証技術を導入し、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、

- ア 拒否しない
- イ 存在するドメインからのみ受信する
- ウ 全て拒否する

の中から選択することができる。イを設定した場合は 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。ウを選択すると、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。ウ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、「宛先指定受信機能」の提供をしている。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) 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 送信ドメイン認証技術

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技術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 20 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。

(3) C 社

① 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。

② 送信ドメイン認証技術

送信ドメイン認証技術を導入しており、「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 (リバースパス (Envelope From とも呼ぶ))、及びヘッダ From (PRA) を偽ったメールを拒否することが可能となっている。

本機能はなりすまし設定 (高) 及び (中) で利用可能となっており、(高) ではドメイン認証に成功したメールのみを受信、(中) では認証に失敗したメールを拒否することができる。

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、「指定受信 (なりすまし、転送メール許可)」を提供している。この機能では、From、To、Cc のいずれかに含まれるアドレスの文字列を最大 20 件まで

登録することができる。

(4) U社

- ・ 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。）。

3 簡易設定

(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つの段階から選択して、より簡単に設定を行うことができる。

① 「低年齢層向けフィルタリング」（高）

受信/拒否設定（携帯・PHSのみ受信、インターネットからのメール拒否）、URL 付きメール拒否設定

② 「受信拒否 強」（高）

受信/拒否設定（携帯・PHSのみ受信、インターネットからのメール拒否）、URL 付きメール拒否設定

③ 「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

(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。設定レベルは以下①～③で、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。

① 推奨ブロック設定（標準レベル）

なりすましメール拒否、優先受信、迷惑メールフィルタ

② ケータイ / PHS 設定（中レベル）

なりすましメール拒否、優先受信、受信許可・拒否設定（携帯・PHSのみ）、迷惑メールフィルタ

③ 低年齢層向けフィルタリング設定（強レベル）

なりすましメール拒否、優先受信、URL 付メール拒否設定（URL を含むメールを全て受信しない）、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、迷惑メールフィルタ

(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た。

2010年（平成22年）12月より、設定レベルを見直して、以下の2段階から選んで設定することができる。2012年（平成23年）2月より、迷惑メールおまかせ規制が設定に追加された。

- ① 「携帯」「PHS」「PCメール」を受信
「携帯」「PHS」「PCメール」を受信、なりすましメール規制（高）、迷惑メールおまかせ規制、拒否通知メール返信設定
- ② 「携帯」「PHS」を受信（ジュニアおすすめ）
「携帯」「PHS」を受信、なりすましメール規制（高）、インターネット拒否、迷惑メールおまかせ規制、拒否通知メール返信設定

4 選択受信

(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、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。）。

(2) B社

宛先、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メールサーバで削除することができる。

(3) C社

加入者は、はじめからメールの全文を受信するのか、指定したアドレスのみ全受信し、それ以外は「送信者」及び「件名」のみを受信確認した後、本文を受信するか否かを決定するのか⁵、又は、「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、のいずれかを設定をすることができる（機種依存の機能となる。）。

(4) T社

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ことができる。

(5) U社

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メールを対象にURL付きメールを受信拒否できる。ユーザーは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、全て受信許可。）。

⁵ 一部機種は未対応

- ① 全て受信許可
- ② URL 付きメールを全て受信拒否
- ③ 特定 URL⁶付きのメールのみ受信拒否

(1) A社

2007年(平成19年)4月から提供を開始しており、①全て受信許可、②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。

(2) B社

2000年(平成12年)11月から提供を開始しており、①全て受信許可、②URL 付きメールを全て受信拒否、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たが、2011年(平成23年)11月に「特定 URL 付きのメールのみ受信拒否」は、迷惑メールフィルター設定に統合された。

(3) C社

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

(4) U社

2008年(平成20年)3月から提供を開始しており、①全て受信許可、②URL 付きメールを全て受信拒否の中から選択して設定することができる。

6 ブラウザからの設定

受信／拒否登録件数の拡張に伴い、携帯電話事業者ではユーザービリティに配慮し、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。

(1) A社

A社のホームページからID／パスワードを入力してログインする。

(2) B社

携帯電話上でパスワードを取得し、B社のホームページからログインする。

(3) C社

携帯電話上でワンタイムパスワードを取得し、C社のホームページからログインする。

7 メールアドレスの変更

(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。

⁶ 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

(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、24時間で3回まで変更が可能。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。

(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。

(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。

(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き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電子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。

(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。

なお、スマートフォン向けプロバイダメールの場合、スマートフォン向けプロバイダメールアプリではヘッダ情報は提供されない。ただし、スマートフォン向けプロバイダメールアプリの機能として、選択したメールをSDカードにeml形式でエクスポートする機能があり、エクスポートされたメールをPC等にインポートすることによりヘッダ情報を見ることが可能となる。

(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、ヘッダ情報を閲覧できる。閲覧できるのは過去2日間に受信したメールの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。

(3) C社

携帯電話で受信し、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)。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。

(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。

(5) U社

メール設定サイトへアクセスすることでヘッダの閲覧をすることができる（過去30日間に受信したメールを250件まで確認できる。規定容量に依存するためあくまで目安）。

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、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、C社を除く移動系ISP4社は、未承諾広告メール受信拒否機能の提供は継続している。

(1) A社

件名欄に「未承諾広告※」と記載されて送られてきた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、「受信しない」に設定されている。

(2) B社

件名欄に「未承諾広告※」と記載されて送られてきたメールを受信又は受信拒否するよう利用者が設定できたが、2010年（平成22年）11月に未承諾広告メールの受信拒否は、迷惑メールフィルター設定に統合された。

(3) C社

件名欄に「未承諾広告※」と記載されて送信されてきた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」に設定されていたが、2008年の特定電子メール法の改正に伴い、オプトイン方式が導入されたことから、2010年（平成22年）6月に機能廃止を実施。

(4) T社

件名欄に「! 広告!」又は「未承諾広告※」と記載されて送られてきた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。

(5) U社

件名欄中に「未承諾広告※」の記載されたメールを受信又は受信拒否できるように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

(1) A社

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。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。宛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1日200通だった通数を1日500通に緩和している。

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電子メールを拒否することができる。

(2) B社

① 迷惑メールフィルター設定

蓄積されたスパム(迷惑メール)データベースをもとに、メールの内容を機械的に判断し、迷惑メールと判断されたメールの受信を拒否することができる。

② Eメールのウィルスチェック

2008年(平成20年)7月より、一部のスマートフォンでは、メール内容を変更することなく、ウィルスだけ取り除いてメールを受信することができる。ウィルス駆除が不可能な場合、ウィルスに感染した部分を本文から削除し、ウィルスを駆除したことを通知するメッセージを本文に挿入する。

(3) C社

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「返信する」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。

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。

③ 迷惑メールおまかせ規制

2012年(平成24年)1月より、受信したPCメールの中で、迷惑メールの疑いのあるメールを検知し、拒否することができる「迷惑メールおまかせ規制」を実施。また、利用者は、迷惑メールおまかせ規制で迷惑メールと判定され規制されたメールの受信日時やFromアドレス等の情報を1日1回、受信するか否かを選択できる。

④ スマートフォン向け「ウィルスメール規制」

2012年(平成24年)1月より、メール送受信に伴うウィルス感染及び拡散を防ぐため、スマートフォン向けにウィルスメール規制を提供し、ウィルスメールの受信拒否及び送信メールのウィルスを検知できる。

(3) U社

・ 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。

(別表1) 移動系 ISP が提供する迷惑メール送受信対策一覧

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 宛先不明メールの受信拒否	宛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している。				
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。	24時間以内に1,000件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が、平成20年3月から送信できる宛先数を500件とした。	平成15年より従来の約30件から一度に送信できるメールの宛先数を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30件に拡大された。また、平成16年8月より、1日当たりの送信宛先数の上限を一律1,000宛先までとした。	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措置を行う。その際、注意喚起を行ったにもかかわらず、迷惑メール送信行為を継続した場合には、契約を解除する。	1日1台当たりの送信を1,000回未満に制限している。
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	平成20年3月
1-2 同報送信宛先数の制限			1回当たり30件までに制限		1回当たり10件までに制限
提供開始時期			平成20年1月		平成20年3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」			初期設定なし。必ずユーザーが指定	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 認証技術	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。 また、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でのメールに対し OP25B を開始、平成 20 年 3 月からは固定系 ISP 宛でのメール送信についても、規制した。	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でのメールに対し OP25B を開始。 平成 20 年 9 月下旬からは固定系 ISP 宛でのメール送信についても、規制を開始した。	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でのメールに対し、OP25B を開始、平成 20 年 6 月からは、固定系 ISP 宛でのメール送信についても、順次、規制を開始した。	携帯事業者向けは平成 20 年 3 月より OP25B を開始。その他は平成 21 年 5 月より順次開始し、同年 7 月に全適用が完了した。
提供開始時期	(前段) 平成 17 年 6 月 (後段) 平成 20 年 7 月	平成 19 年 12 月	平成 18 年 6 月	平成 18 年 5 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	<p>指定したドメイン、アドレスから送信された電子メールを受信／拒否する。</p> <p>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可能。</p> <p>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となった。</p>	<p>指定したドメイン、アドレスから送信された電子メールを受信／拒否する。</p> <p>携帯電話事業者及びPHS事業者からのみ受信を選択可能。</p> <p>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有料サービスを開始した。</p>	<p>メールアドレスに指定した文字列を含むドメイン、アドレスなどから送信された電子メールを受信／拒否する。</p> <p>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 ③一括指定受信となる。</p>	<p>指定した①アドレス、②ドメイン、③サブドメイン、④全てのアドレス、⑤全ての@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／拒否する。</p>	<p>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。</p>
設定内容	<p>受信120件 アドレス拒否、 ドメイン拒否各 120件</p>	<p>Eメール許可：300 件 Eメール拒否：300 件 電話番号メール 許可/拒否いづれ か：150件</p>	<p>受信200件 アドレス拒否、 ドメイン拒否各 200件</p>	<p>許可／拒否 いずれか20件</p>	<p>受信20件 拒否20件</p>
指定受信／許可 の併用	<p>可能</p>	<p>Eメールは併用可 能。電話番号メー ルは許可/拒否い づれか選択</p>	<p>可能</p>	<p>不可</p>	<p>不可</p>
提供開始時期	<p>平成12年11月 アドレス指定 拒否</p> <p>平成15年12月 事業者每一括 指定</p> <p>平成19年11月 ドメイン指定 拒否</p> <p>平成22年3月 設定件数拡大 40件→120件</p>	<p>平成11年12月 事業者每一括 設定（設定件数 10件）</p> <p>平成13年12月 設定件数拡大 10件→20件</p> <p>平成19年9月 ネットワークド メイン帳 優先受信機能 追加</p> <p>平成22年11月 設定件数増、併 用可</p>	<p>平成14年4月 開始</p> <p>平成15年5月及 び17年11月 指定拒否との 併用拡充</p> <p>平成19年3月 設定件数拡大 20件→100件</p> <p>平成22年12月 設定件数拡大 100件→200件</p>	<p>平成10年12月 開始</p> <p>平成14年6月 設定件数拡大 10件→20件</p>	<p>平成20年3月 より開始</p>

2-2 送信元詐称対策 なりすまし拒否	拒否設定において、携帯電話及びPHSのドメインになりす ましたメールを受信拒否する。			拒否設定にお いて、携帯電話 及びPHS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 12 年 11 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 送信元詐称対策 送信ドメイン認 証技術	一般のドメイン になりすましたメ ール（送信元情報 を詐称したメー ル）を拒否する。 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（リバ ースパス： Envelope fromと もいう。）を偽っ たメールを拒否 することが可能。 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 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。		
提供開始時期	平成 19 年 11 月		平成 19 年 3 月		
2-2 送信元詐称対策 ホワイトリスト	「宛先指定受 信」機能で最大 10 件まで自動転送元 のメールアドレス を設定できる。	「救済リスト設 定」で最大 20 件ま で自動転送元のメ ールアドレスを設 定できる。	「指定受信 （なりすまし、 転送メール許 可）」で、From、 To、Cc のいずれ かに含まれるアド レスの文字列を最大 20 件まで 設定できる。		
提供開始時期	平成 20 年 1 月	平成 18 年 10 月	平成 19 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
2-3 簡易設定	メールフィルタを「低年齢層向けフィルタリング」「受信拒否（強）」「受信拒否（弱）」の3種類から選ぶことで簡単に設定可能。	メールフィルタを「推奨ブロック設定（標準レベル）」「ケータイ／PHS 設定（中レベル）」「低年齢層向けフィルタリング設定（強レベル）」の3種類から選ぶことで簡単に設定可能。	メールフィルタを希望のレベルに合わせて、『「携帯」「PHS」「PC メール」を受信』『「携帯」「PHS」を受信』の2段階から選ぶことで、簡単に設定可能。また、平成23年より、迷惑メールおまかせ規制が設定に追加された。		
提供開始時期	平成19年11月	平成20年3月	平成22年12月		
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ことができる。	宛先、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ことができる。	はじめからメールの全文を受信するのか、指定したアドレスのみ全受信し、それ以外は「送信者」及び「件名」のみを受信確認した後、本文を受信するか否かを決定するのか、又は、「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、のいずれかを設定できる。なお、これらの機能は、移動機の種類によって異なる。	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ことができる。	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ことができる。
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12年11月	平成16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
2-5 URL 付きメール 受信拒否	Eメールについて①全て受信許可②特定 URL 付きのメールのみ受信拒否から選択して設定。	Eメールについて①全て受信許可②URL 付きメールを全て受信拒否の中から選択して設定。	Eメールについて、①全て受信許可②URL 付きメールを全て受信拒否から選択して設定。		Eメールについて、①全て受信許可②URL 付きメールを全て受信拒否から選択して設定。
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	A社 HP で ID /パスワードを入力する。	携帯電話上でパスワードを取得し、B社 HP からログインする。	携帯電話上でワンタイムパスワードを取得し、C社 HP からログインする。		
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	半角英数字等 3 字以上 30 字以下の任意のメールアドレスに変更可能。		半角英数字 30 字以下の任意のメールアドレスに変更可能。	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可能。	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可能。
	1 日 3 回まで	24 時間で 3 回まで (※平成 18 年 10 月より一つの携帯電話番号で最大 99 回まで制限)	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。なお、スマートフォン向けプロバイダメールの場合、スマートフォン向けプロバイダメールアプリではヘッダ情報は提供されない。	受信したメールのヘッダ情報は、PCを利用して閲覧できる。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。	携帯電話で受信し、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、PCの指定先アドレスへ転送したメールで確認できる。	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(過去30日間に受信したメールを250件まで確認できる。規定容量に依存するためあくまで目安)。
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メールを受信又は受信拒否する。初期設定は「受信しない」。	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メールを受信又は受信拒否するよう利用者が設定できたが、平成22年11月に未承諾広告メールの受信拒否は、迷惑メールフィルター設定に統合された。	特電法改正により、広告メールがオプトイン規制に変わったことから廃止。	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メールを受信又は受信拒否する。	件名欄中に「未承諾広告※」と記載されたメールを受信又は受信拒否する。
初期設定	受信しない	受信しない		受信する	
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22年6月廃止	平成16年8月	平成20年3月

記載節番号 サービス名	内 容
	A 社
2-10 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 通から 500 通へと緩和。
提供開始時期	平成 16 年 1 月
2-10 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、暗証番号を知らない相手からのメールの受信を拒否することができる。
提供開始時期	平成 11 年 7 月
	B 社
2-10 迷惑メールフィルタ	蓄積されたスパム(迷惑メール)データベースをもとに、メールの内容を機械的に判断し、迷惑メールと判断されたメールの受信を拒否することができる。
提供開始時期	平成 22 年 9 月
2-10 E メールウィルス チェック	一部のスマートフォンでは、メール内容を変更することなく、ウィルスだけ取り除いてメールを受信することができる。ウィルス駆除が不可能な場合、ウィルスに感染した部分を本文から削除し、ウィルスを駆除したことを通知するメッセージを本文に挿入する。
提供開始時期	平成 20 年 7 月
	C 社
2-10 拒否通知返信設定	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。平成 22 年 12 月のフィルタ機能拡張により、初期設定は「返信する」に設定されている。
提供開始時期	平成 17 年 11 月
2-10 HTML メール規制	HTML メールを受信を拒否することができる。
提供開始時期	平成 19 年 3 月
2-10 迷惑メールおまかせ規制	受信した PC メールの中で、迷惑メールの疑いのあるメールを検知し、拒否することができる「迷惑メールおまかせ規制」を実施。また、利用者は、迷惑メールおまかせ規制で迷惑メールと判定され規制されたメールの受信日時や From アドレス等の情報を 1 日 1 回、受信するか否かを選択できる。
提供開始時期	平成 24 年 1 月
2-10 スマートフォン向け「ウィルスメール規制」	メール送受信に伴うウィルス感染及び拡散を防ぐため、スマートフォン向けにウィルスメール規制を提供し、ウィルスメールの受信拒否及び送信メールのウィルスを検知できる。
提供開始時期	平成 24 年 1 月
	U 社
2-10 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。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節 SMS を利用した迷惑メール送信防止対策の提供状況

1 大量迷惑メールの送信制限

(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。

(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たが、2011年(平成23年)7月より、1日に200件以上送信した場合、その後24時間送信規制するように変更した。

(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。

(4) T社

送信制限実施せず。

(5) U社

1日に送信できるSMSを200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 を利用した迷惑メール受信対策の提供状況

1 迷惑メール防止のための受信拒否機能

(1) A社

① SMS 一括拒否

全ての SMS を拒否することができる。

② 非通知 SMS 拒否

ショートメールを SMS として受信する場合に、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。

③ 国際 SMS 拒否

海外事業者の利用者から送信された SMS を拒否することができる。

④ 国内他事業者 SMS

A社以外の事業者からの SMS を拒否することができる。

⑤ 個別番号拒否

個別に指定した電話番号からの SMS を拒否することができる（最大 30 件登録可）。

⑥ 個別番号受信

個別に指定した番号からの SMS のみを受信することができる（最大 30 件登録可）。

■ 受信拒否機能併用可否表

	SMS一括 拒否	非通知 SMS拒否	国際SMS 拒否	国内事業者 SMS拒否	個別番号 拒否	個別番号 受信
SMS一括 拒否		×	×	×	×	×
非通知 SMS拒否	×		○	○	○	×
国際SMS 拒否	×	○		○	○	×
国内事業者 SMS拒否	×	○	○		○	×
個別番号 拒否	×	○	○	○		×
個別番号 受信	×	×	×	×	×	

(2) B社

2011年（平成23年）6月より、国内SMS向けに電話番号メール許可拒否リスト（最大150件）を提供している。また、2011年（平成23年）10月より、国際SMS向けに海外からの電話番号メール一括拒否機能を提供している。

(3) C社

① ブロック機能

2005年（平成17年）3月に、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。

ア 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。

イ 非通知

電話番号通知のないSMSを破棄。

ウ 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。

エ 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の利用を停止することができる。

(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。

2 事業者を跨いで送信された迷惑SMSへの対応

移動系ISPIにおいては、2011年（平成23年）7月より、第3世代携帯電話におけるSMSの事業者間接続を開始しているが、事業者を跨いで送信された迷惑メールについて、送信元事業者から迷惑メール送信者に対して以下のような対応を行っている。

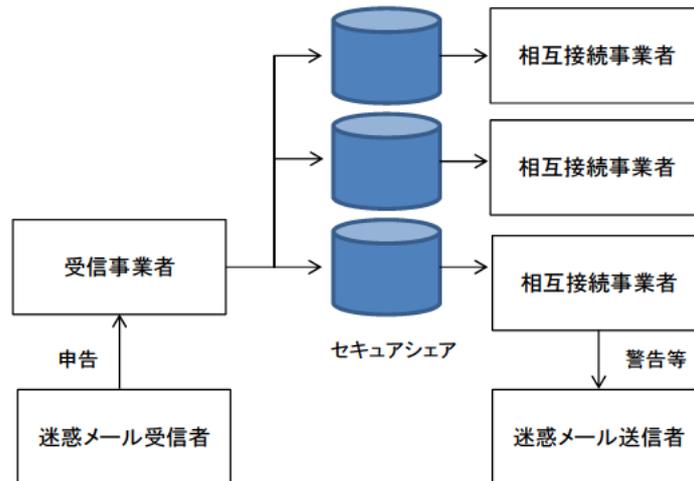


図2-1 申告情報の伝達ルート

(1) 申告受信事業者の対応

- ① 電話、ウェブ等で申告を受け付ける。
- ② 申告者から取得する情報は、SMS本文、送信電話番号等
- ③ 取得した情報を他移動系ISPIに提供する場合がある旨、申告者本人の同意を取得する。
- ④ 同一の電話番号から送信された迷惑SMSについて、一定期間内に複数の受信者から申告があった場合、申告情報と顧客情報との照合を行い、自網から送信されたSMSに関する申告情報を判別する。
- ⑤ 自網から送信されたSMSに関する申告情報であると判定されなかったものを相互接続事業者に提供する。

(2) 情報提供を受けた相互接続事業者の対応

- ① 申告受信事業者から提供された申告情報（送信電話番号、受信日）と顧客情報との照合を行い、自網から送信されたSMSに関する申告情報を判別する。
- ② 自網から送信されたSMSに関する申告件数や内容に応じて、当該SMS送信回線契約者に対して警告等を行う。

第3章 迷惑メールに関する固定系ISPの対策提供状況

第1節 迷惑メール送信防止対策の提供状況

1 送信通数規制

(1) D社

2007年(平成19年)2月より、D社のメールサーバを經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) K社

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。

(3) O社

- ・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
- ・1会員当たりのメール送信数制御

個人会員について、1日当たりに送信可能なメール宛先数を制御。

(4) P社

大量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。

(5) S社

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。

2 送信元情報確認による送信制限

(1) 送信者確認

① G社

送信者アドレス (FROM :) を改変したメールの SMTP 接続を拒否。

② O社

差出人アドレスのチェックを強化。

(2) 送信元 IP アドレス検証

・ H社

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ている。

通常、正規ユーザー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、ウィ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。

ア 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。

イ 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。

※ ACL (Access Control List)

パケットの送信元・受信先 IP アドレスや送信元・受信先インターフェースなどスタティック (静的) な情報を利用したフィルタリング手法。

フィルタ条件を人手で管理する必要がある代わりに、ハードウェアによる高性能な処理を比較的实现しやすい。

(3) 送信ドメイン認証技術

- ① D社
 - ・ 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。

- ② E社
 - ・ SPF 登録
2008 年（平成 20 年）1 月より実施。

- ③ F社
 - ・ SPF 登録
2007 年（平成 19 年）2 月より実施。

- ④ G社
 - ・ SPF 登録
2007 年（平成 19 年）5 月より実施。

- ⑤ H社
 - ・ SPF 登録
2006 年（平成 18 年）2 月より実施。

- ⑥ I社
 - ・ SPF 登録
2006 年（平成 18 年）11 月より実施。

- ⑦ J社
 - ・ SPF 登録
2006 年（平成 18 年）3 月より実施。

- ⑧ K社
 - ・ SPF 登録
2011 年（平成 23 年）10 月より実施
 - ・ DKIM
2011 年（平成 23 年）9 月より実施

- ⑨ L社
 - ・ SPF 登録
 - 2005 年（平成 17 年）12 月より実施。

- ⑩ M社
 - ・ SPF 登録
 - 2005 年（平成 17 年）5 月より実施。
 - ・ DKIM (Domainkeys)
 - 2005 年（平成 17 年）5 月より実施。

- ⑪ N社
 - ・ SPF 登録
 - 2006 年（平成 18 年）5 月より実施。

- ⑫ O社
 - ・ 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。

- ⑬ P社
 - ・ SPF 登録
 - 2006 年（平成 18 年）11 月より実施。

- ⑭ Q社
 - ・ 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。

- ⑮ R社
 - ・ SPF 登録
 - 2006 年（平成 18 年）10 月より実施。

- ⑯ S社
 - ・ SPF 登録
 - 2007 年（平成 19 年）11 月より実施

3 OP25B

(1) D社

- ・携帯宛
2005年（平成17年）10月より実施。
- ・PC宛
2006年（平成18年）11月より実施。
- ・メール投稿用ポート 587番
2005年（平成17年）4月より提供。

(2) E社

- ・携帯宛
2005年（平成17年）10月より実施。
- ・PC宛
2006年（平成18年）6月より実施。
- ・メール投稿用ポート（587番）
2006年（平成18年）3月より提供。

(3) F社

- ・携帯宛
2005年（平成17年）11月より実施。
- ・PC宛
2007年（平成19年）7月より実施。
- ・メール投稿用ポート 587番
2005年（平成17年）11月より提供。

(4) G社

- ・携帯宛
2006年（平成18年）6月より実施。
- ・PC宛
2006年（平成18年）10月より実施。
- ・メール投稿用ポート 587番
2006年（平成18年）6月より提供。

(5) H社

- ・携帯宛
2006年（平成18年）2月より実施。
- ・PC宛
2006年（平成18年）12月より実施。
- ・メール投稿用ポート 587番

2006年（平成18年）2月より提供。

(6) I社

・携帯宛

2005年（平成17年）3月より実施。

・PC宛

2005年（平成17年）3月より実施。

・メール投稿用ポート 587番

2005年（平成17年）3月より提供。

(7) J社

・携帯宛

2005年（平成17年）12月より実施。

・PC宛

2006年（平成18年）3月より実施。

・メール投稿用ポート 587番

2005年（平成17年）11月より提供。

(8) K社

・携帯宛

2006年（平成18年）6月より実施。

・PC宛

2006年（平成18年）6月より実施。

・メール投稿用ポート 587番

2006年（平成18年）3月より提供。

(9) L社

・携帯宛

2006年（平成18年）3月より実施。

・PC宛

2006年（平成18年）12月より実施。

・メール投稿用ポート 587番

2006年（平成18年）8月より提供。

(10) M社

・携帯宛

2006年（平成18年）2月より実施。

・PC宛

2006年（平成18年）2月より実施。

- ・メール投稿用ポート 587 番
2005 年（平成 17 年）10 月より提供。

(11) N 社

- ・携帯宛
2005 年（平成 17 年）9 月より実施。
- ・PC 宛
2006 年（平成 18 年）12 月より実施。
- ・メール投稿用ポート 587 番
2006 年（平成 18 年）2 月より提供。

(12) O 社

- ・携帯宛
2006 年（平成 18 年）7 月より実施。
- ・PC 宛
2006 年（平成 18 年）9 月より実施。
- ・メール投稿用ポート 587 番
2005 年（平成 17 年）7 月より提供。

(13) P 社

- ・携帯宛
2005 年（平成 17 年）1 月より実施。
- ・PC 宛
2006 年（平成 18 年）7 月より実施。
- ・メール投稿用ポート 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

- ・携帯宛
2006 年（平成 18 年）6 月より実施。
- ・PC 宛
2007 年（平成 19 年）1 月より実施。
- ・メール投稿用ポート 587 番
2006 年（平成 18 年）6 月より提供。

(15) R 社

- ・携帯宛
2005 年（平成 17 年）3 月より実施。

- ・ PC 宛
2005 年（平成 17 年）3 月より実施。
- ・ メール投稿用ポート 587 番
2005 年（平成 17 年）3 月より提供。

(16) S 社

- ・ 携帯宛
2006 年（平成 18 年）11 月より実施。
- ・ PC 宛
2006 年（平成 18 年）11 月より一部を実施。
- ・ メール投稿用ポート 587 番
2006 年（平成 18 年）6 月より提供。

4 その他（ボット対策）

- ・ O 社
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などについて郵送とメールで案内後、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。

(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

	送信ドメイン認証技術		Outbound Port 25 Blocking 関連		
	SPF	DKIM	携帯宛	PC宛	メール投稿用 ポート 587 番
D社	H17/12	H17/03 (企業向け)	H17/10	H18/11	H17/04
E社	H20/01	-	H17/10	H18/06	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	H18/02
I社	H18/11	-	H17/03	H17/03	H17/03
J社	H18/03	-	H17/12	H18/03	H17/11
K社	H23/10	H23/09	H18/06	H18/06	H18/03
L社	H17/12	-	H18/03	H18/12	H18/08
M社	H17/05	H17/05	H18/02	H18/02	H17/10
N社	H18/05	-	H17/09	H18/12	H18/02
O社	H17/11	H19/09	H18/07	H18/09	H17/07
P社	H18/11	-	H17/01	H18/07	H18/06
Q社	H18/12	H17/07	H18/06	H19/01	H18/06
R社	H18/10	-	H17/03	H17/03	H17/03
S社	H19/11	-	H18/11	H18/11	H18/06

第2節 迷惑メール受信防止対策の提供状況

1 大量受信制限

(1) M社

M社に向けて大量の架空アドレス宛メールを送信する発信元からの受信を拒否する対策が実施されている。M社メールサーバが宛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、その発信元のIPアドレスからの受信を拒否する。

(2) Q社

一定時間内に特定のユーザー宛に大量送信を行なうサーバや、大量の宛先不明のメールの送信を行なうサーバに対し、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～数十時間の遅延措置が取られる。

2 送信元情報による判定

(1) 送信ドメイン認証技術

① D社

従来のSPFに加えDKIMも利用した迷惑メールフィルタリングサービスを、2010年(平成22年)12月より提供。送信ドメイン認証の結果に基づき「受け取る」又は「捨てる(ごみ箱に入れる)」ことが可能。

指定したドメイン名を差出人とするメールについて送信ドメイン認証の検証結果、正当なメールと判断できた場合は以降のフィルタでは判定せず受け取る。なりすましと判断したメールはごみ箱に入れるが、例外ドメインを指定することができ、ドメイン名を差出人とするメールについては、なりすましメールと判断できた場合でも以降のフィルタでは判定せず受け取る。

利用者は、「指定ドメイン」(必須)と「例外ドメイン」(任意)を設定するだけでよい。いずれも最大1,000件まで登録できるが、ワイルドカードは設定できない。

② F社

自社が受信したメールについて、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加して配送する。

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 K社

2011年(平成23年)10月より、SPF、DKIMの認証結果を検証し、結

果をメールヘッダに付与している。

④ L社

認証結果を、RFC4408 に準拠した判定結果のフォーマットにしたがい、メールヘッダに付与している。

⑤ M社

2010年（平成22年）6月より SPF、DKIM の認証結果を検証し、結果をメールヘッダに付与している。

また、2011年（平成23年）5月より Webmail 上の一覧画面において、なりすましされていないメールのマーク表示を開始している。あらかじめ登録しているメールアドレスからのメールについて実施しており、なりすまされたメールについては 警告表示をしている。

⑥ O社

SPF 方式及び DKIM 方式による送信ドメイン認証技術を実施している。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技術の実現を可能としている。

⑦ Q社

DKIM (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。

(2) IP アドレスを利用した判定

① F社

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。

② G社

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。

③ I社

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。

④ P社

動的IPアドレスのメールサーバからのメール送信に対しては、再送要求を発信する。再送要求に応え、再送を行ったもののみを受信する。

適正に管理されていない迷惑メール送信サーバは、メールの再送信を行わないという特性を利用し、迷惑メール受信数の削減を図っている。

⑤ Q社

IPアドレスなどの評判情報（レピュテーション）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

(3) 送信者情報を利用した判定

① M社

未登録のアドレスから送信されるメールをブロックする。

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、全て迷惑メールフォルダに振り分けられる。

② O社

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を実施。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。

(4) IP25B

① F社

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。

② M社

F社からのメールに対して、ISPのサーバを経由せず、動的IPアドレスから直接送信されるメールをブロック。

③ Q社

大手 ISP からの依頼により実施。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。

3 メールの内容による判定

(1) キーワード/メール容量/添付ファイルによる判定

① D社

ア ブラックワード

送信者アドレス (From:)、宛先アドレス (To:) 写し宛先アドレス (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て合計 100 パターンまでの着信拒否条件の設定ができる。指定できる条件には、ワイルドカードの設定も可能。

イ 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）以上のメールを受信しないよう設定できる。

ウ 添付ファイル

添付ファイル付きのメールをごみ箱に入れることができる。

エ 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ことができる。

② E社

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、拒否アドレスとして登録することはできない。

③ F社

ア セキュリティ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セキュリティソフトをインストールし、当該セキュリティソフトに含まれる迷惑メールフィルタ機能を利用することができる。迷惑メールへの対応は、インストールしたソフトに基づき行う。

イ メールの自動削除サービス

フィルタ設定を利用しメールの自動削除を行う。送信者アドレス (From:)、宛先アドレス (To:)、件名 (Subject:) 等に加え、ユーザーがメールのヘッダ情報に応じて細かく指定することが可能。

④ G社

ア ブラックワード

送信者メールアドレス (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 の切替が可能で、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、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。

イ メール容量

受信メールのサイズによる受信拒否設定が可能。

⑤ H社

・ 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:)、件名 (Subject:) などのヘッダ項目の条件を設定し、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。

⑥ I社

・ 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。

⑦ J社

・ ブラックワード

送信者アドレス (From:)、宛先アドレス (To:)、写し宛先アドレス (Cc:)、件名 (Subject:)、本文、Return-path: に任意のキーワードを設定可能 (最大 20 件のパターン)。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。

⑧ K社

ア ブラックワード

送信者アドレス (From:)、宛先アドレス (To:)、件名 (Subject:) について、単独又は 2 つまでの組合せで受信拒否条件を設定できる。設定可能な条件数は 2 つまでの組合せを 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。また、ユーザーが明らかに迷

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することも可能。

イ メール容量

指定した容量を超えるメールを受信拒否条件とする設定も可能。

⑨ L社

・ ブラックワード

送信者アドレス (From:)、宛先アドレス (To:)、写し宛先 (Cc:)
について 500 件まで登録可能。

⑩ M社

・ ブラックワード/メール容量

From アドレス (From:)、宛先アドレス (To:)、写し宛先 (Cc:)、
件名 (Subject:) 及びメールの容量の 5 項目について (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。

⑪ N社

・ ブラックワード

送信者アドレス (From:)、件名 (Subject:) について、それぞれ
30 件、任意のキーワードを設定可能。

⑫ O社

ア 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:)、宛先アドレス
(To:)、写し宛先アドレス (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、宛先アドレス (To:)
100 件まで、写し宛先アドレス (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:)、宛先アドレス (To:)、写し宛先アド
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。

イ メール容量

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。

⑬ P社

・ ブラックワード/メール容量

送信者アドレス (From:) (最大 5 個)、宛先アドレス (to:) 又は写し宛先アドレス (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。

⑭ Q社

・ 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。

⑮ R社

・ 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:)、宛先アドレス (To:)、写し宛先アドレス (Cc:)、件名 (Subject:) にキーワードを、単独又は組合せで設定可能。2 ペアで許可設定も含めて 100 件登録することができる。

⑯ S社

・ 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。

(2) フィルタによる判定

① D社

ヒューリスティック及びシグネチャフィルタを、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定し、振り分け作業を行うことができる。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る。

なお、判定スコアはユーザーが任意に変更可能。

② E社

2006年（平成18年）12月より、ヒューリスティックフィルタやシグネチャーフィルタを用いた迷惑メール判定エンジンを利用して、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ーの受信トレイに配信されないようにすることができる。

③ F社

ア ヒューリスティックフィルタ

(a) 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。

(b) 迷惑メールの自動判定サービス

迷惑メール自動判別エンジンでスコア付けし、その結果をヘッダに付与することができる。ユーザーが設定する一定のスコア以上のメールの件名に[meiwaku]を付記する事も可能。

イ 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。

④ G社

ヒューリスティックフィルタ利用の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、ユーザー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。

⑤ H社

シグネチャーフィルタを使い、メールサーバ上で迷惑メールと判断されたメールに対して、判定結果をヘッダに付記することができる。その後、件名に[meiwaku]を付記する。

⑥ J社

ヒューリスティックフィルタを利用し、あらかじめ設定した基準に

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（メール件名）に自動的に付与し、メールサーバ上の迷惑メールフォルダへ振り分けることができる。

⑦ K社

シグネチャーフィルタを利用しており、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。

⑧ L社

シグネチャーフィルタによる迷惑メール判定エンジン（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ことができる。

⑨ M社

ア 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ことができる。

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。

イ 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ることができる。ホワイトリストの設定もできる。

ウ 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ト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ことができる。

⑩ N社

・ 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、ユーザー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、以降の判定に用いることができる。フィルタを継続使用することで判定精度が向上する。

⑪ O社

ア 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することができる。

また、ユーザー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 OutlookExpress 及び Windows メール用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）。

イ 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（90%で固定）を超える場合に迷惑メールとして判定することができる。

⑫ P社

送信者評価、ヒューリスティックフィルタ、シグネチャーフィルタ、URL 評価等を使い迷惑メールを判定することができる。

送信者信頼度、IP アドレス信頼度で選別後、メッセージの内容、メッセージの構成、送信者、コンテンツに記載された URL などといったメッセージの構成要素を包括的に検査し、迷惑メール度をスコア化する。スコアが基準値を超えた場合に迷惑メールと判定する。基準値は、受信者の利用形態に合わせ 4 レベルから選択できる。

⑬ Q社

ア 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、ユーザー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ことができる。

イ 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ことができる。

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。

ウ 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、該当項目数の一定値以上を超えると迷惑メールフォルダへ振り分けることができる。

⑭ R社

ヒューリスティックフィルタ、シグネチャーフィルタによる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の判定を行うことができる。迷惑メールと判定したメールについては、件名に [spam] を付記する。また、メールサーバ上に隔離することもできる。

⑮ S社

ヒューリスティックフィルタ、シグネチャーフィルタにより迷惑メールと判断したメールを拒否することができる。

(3) ホワイトリスト

① D社

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。

② E社

受け取りたい相手のメールアドレスを 100 件まで登録できる。

③ F社

送信者アドレス (From:)、宛先 (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。

④ G社

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。

⑤ H社

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。条件設定は、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。

- ⑥ I 社
メールアドレスを設定することができる。
- ⑦ J 社
送信者アドレス (From:)、宛先アドレス (To:)、写し宛先アドレス (Cc:)、件名 (Subject:)、本文、Return-path: に任意のキーワードを設定(最大 20 件)し、該当するメールを受信することが可能。
また、設定条件に合致するメールのみを受信することも可能。
- ⑧ K 社
送信者アドレス (From:)、宛先アドレス (To:) や件名 (Subject:) について任意のキーワードを設定可能。パズリスト (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。
- ⑨ L 社
送信者アドレス (From:)、宛先アドレス (To:)、写し宛先アドレス (Cc:) について 500 件登録できる。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。
- ⑩ M 社
送信者アドレス (From:)、宛先アドレス (To:)、宛先アドレス (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、受信拒否の条件を合わせて 100 件。
- ⑪ O 社
受け取りたい相手の送信者アドレス (From:)、宛先アドレス (To:)、写し宛先アドレス (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 P 社
送信者アドレス (From:) (最大 5 個)、宛先アドレス (To:) 又は写し宛先アドレス (Cc:) (最大 5 個)、件名 (Subject:) (最大 5 個)、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 Q社

送信者アドレス (From :)、宛先アドレス (To :)、写し宛先アドレス (Cc :)、件名 (Subject :)、本文に任意の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 R社

受け取りたくない相手の送信者アドレス (From :)、宛先アドレス (To :)、写し宛先アドレス (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 ペアで拒否設定も含めて 100 件登録することができる。

⑮ S社

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。

4 判定後の処理

(1) D社

着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

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、ユーザー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、ユーザーへ通知する機能もある(初期設定はオフ設定されている。)

(3) F社

ア 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、ユーザーが設定するスコア以上のメールをフィルタリングする。

イ 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、ユーザーは必要に応じて内容の確認を行うことができる。

ウ 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、こ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。

エ メール自動削除サービス

削除の設定に基づいて、条件に該当するメールをサーバ上で削除する。

(4) G社

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、サーバ側で、削除され、復元することができない。

(5) H社

「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

迷惑メールと判定されたメールに対する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

迷惑メールと判定されたメールに対して、件名に[spam]の表示が付記されメールサーバ上の迷惑メールフォルダに隔離される(4週間後に削除)。

キーワード判定による受信拒否設定の場合には、メールサーバ上で自動的に削除される。

(8) K社

ア 受信拒否サービス

設定条件に合致する全てのメールはメールサーバ上で削除される。

イ 振り分けサービス

判定後の処理は、(a)と(b)のどちらかを選択可能。

(a) ラベリング

判定メールに対して件名に[meiwaku]が付記される。

(b) 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、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

迷惑メール判定エンジンで迷惑メールと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）

(a) 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。

(b) 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。

(c) 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、ユーザーの設定によって、[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

ア 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、全て迷惑メールフォルダに振り分けられる。

イ 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」、「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ず、受信拒否したメール

は破棄される。

ウ 自動振り分けサービス

あらかじめ定めた基準に基づいて迷惑メールを判別し、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。

(11) N社

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

ア 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。

イ 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（90%で固定）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、ユーザー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、ユーザーには件数、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。迷惑メールフォルダのメールの保存期間は10日間で、経過後は自動的に削除される。

(13) P社

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

(14) Q社

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。

(15) R社

迷惑メールと判定されたメールは、メールサーバ上で隔離（7日間保存）や、削除・受信を行うことができる。

(16) S社

迷惑メールと判定したメールは、ヘッダに特定の文字列を付加し、配

送するか又は迷惑メールフォルダに保管するかのいずれかを選択できる。
迷惑メール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

	大量受信 制限	送信元情報による判定						
		送信ドメイン認証技術				IPアドレスを 利用した判 定	送信者情 報を利用 した判定	IP25B
		SPF		DKIM				
		ラベリン グ	フィルタ リング	ラベリ ング	フィルタ リング			
D社		○	○	○	○			
E社								
F社		○				○		○
G社						○		
H社								
I社						○		
J社								
K社		○		○				
L社		○						
M社	○	○		○			○	○
N社								
O社		○		○			○	
P社						○		
Q社	○	○	○	○	○	○		○
R社								
S社								

(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

	メールの内容による判定						ホワイト リスト
	ブラック ワード	メール 容量	添付 ファイル	迷惑メールフィルタ			
				ベイジアン	ヒューリスティック	シグネチャー	
D社	○	○	○		○	○	○
E社	○				○	○	○
F社	○				○	○	○
G社	○	○			○		○
H社	○					○	○
I社	○						○
J社	○				○		○
K社	○	○				○	○
L社	○					○	○
M社	○	○		○	○	○	○
N社	○			○			
O社	○	○		○	○		○
P社	○	○			○	○	○
Q社	○			○	○	○	○
R社	○				○	○	○
S社	○				○	○	○