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 28 年 12 月

総 務 省 総 合 通 信 基 盤 局
電気通信事業部消費者行政第二課

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、その後の迷惑メール送信の悪質化、巧妙化に鑑み、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宛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。

さらに、2008 年（平成 20 年）の第二次改正では、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強化のための改正、国際連携強化のための改正が行われた。

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。)における新たな迷惑メール対策技術の導入がなされてきた。

その対策の一つである Outbound Port 25 Blocking 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 での導入が進んでいる。

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、調査を行ったところ報告する。

―――――― 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

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

(1) 契約後の期間限定型制御

契約後の一定期間は、一度（１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、同一の送信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で状況に応じて、適宜定められる。実際の適用に当たっては、常に同じ基準を全ての送信者に適用するのではなく、臨機応変にきめ細かい対応が望ましい。

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。

(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]。

---

[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番ﾎﾟｰﾄ）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。

(2) SMTP AUTH (SMTP Authentication：SMTP 認証)

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。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ーに対しても、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。

3　送信者アドレス照合

送信者アドレスは比較的簡単に変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、ISP が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。一致しない場合は、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不正な手段で送信者認証に使う ID／パスワードを入手し、送信者認証を成功させることが多い。これを防止するため、一定回数以上認証に失敗した場合に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に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ため、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は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) 転送アドレス書き換え

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。これにより、転送者自身が宛先不明による転送失敗やエラーメールの管理ができ、混乱を防ぐことができる。

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、安価で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とから、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が、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 番ポートの使用ができないメールソフトを用いている場合には、それができるメールソフトへの変更が必要となる。

(2) 導入状況

当初、米国の一部 ISP で採用された OP25B は、我が国では 2005 年（平成 17 年）１月に初めて携帯電話向け送信に導入された。2006 年（平成 18 年）６月頃から ISP での導入が始まり、2014 年（平成 26 年）12 月では、導入 ISP は 148 社となっている（図 1-1）。

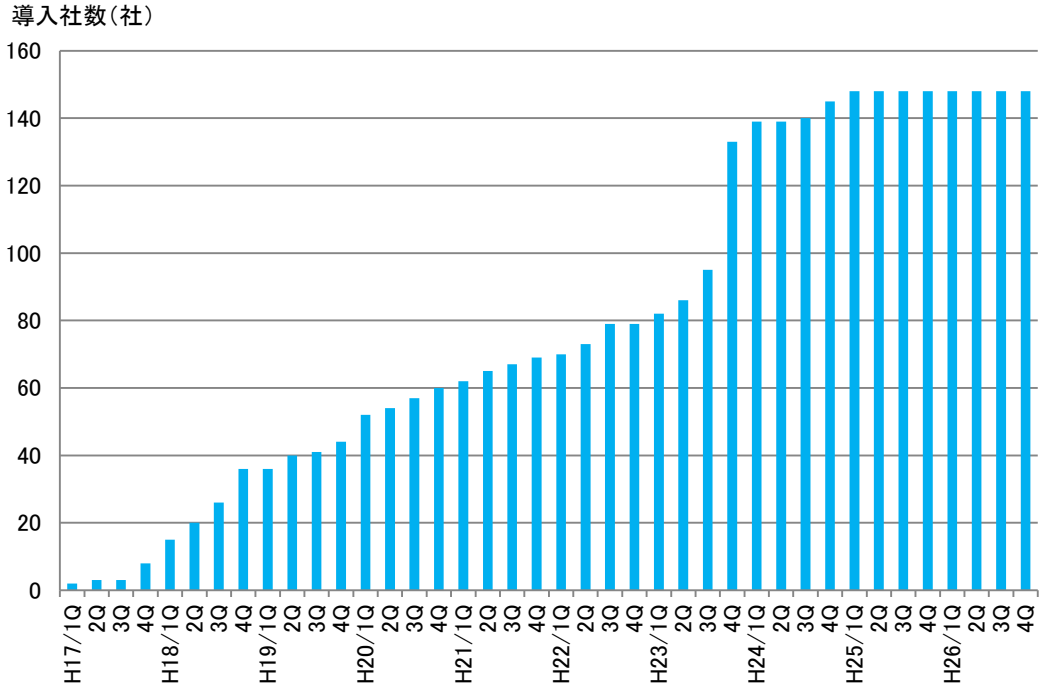

図1-1　国内ISPのOP25B導入推移

(3) OP25B の導入効果

OP25B の導入初期において、ISP による OP25B の導入増に伴い、迷惑メール送信国ランキング（ソフォス株式会社調べ）の日本の順位が下がっている。しかし、2012 年（平成 24 年）2Q 以降に順位が上昇し始め、OP25B のみで迷惑メールを防ぐのは難しくなっている。（図 1-2）

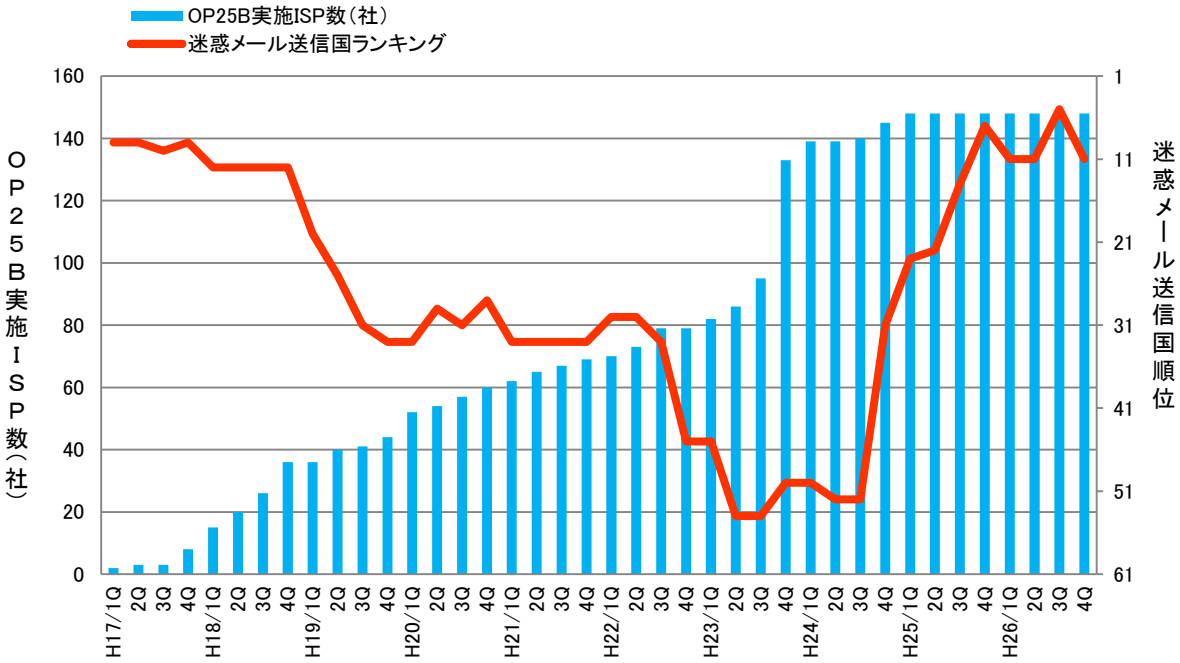

図1-2　国内のOP25B導入状況と日本の迷惑メール送信国順位

（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株式会社資料より作成）

また、OP25Bの導入初期には、迷惑メール送信者がOP25Bを導入しているISPから導入していないISPへと移動している状況が見られた（図1-3）。

例えば、ISP A のOP25B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か月でほぼ０のレベルとなっている。一方、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、しばらくすると、ISP Bから送信される迷惑メール比率も減少に転じ、代わってISP Cの比率が増加している。

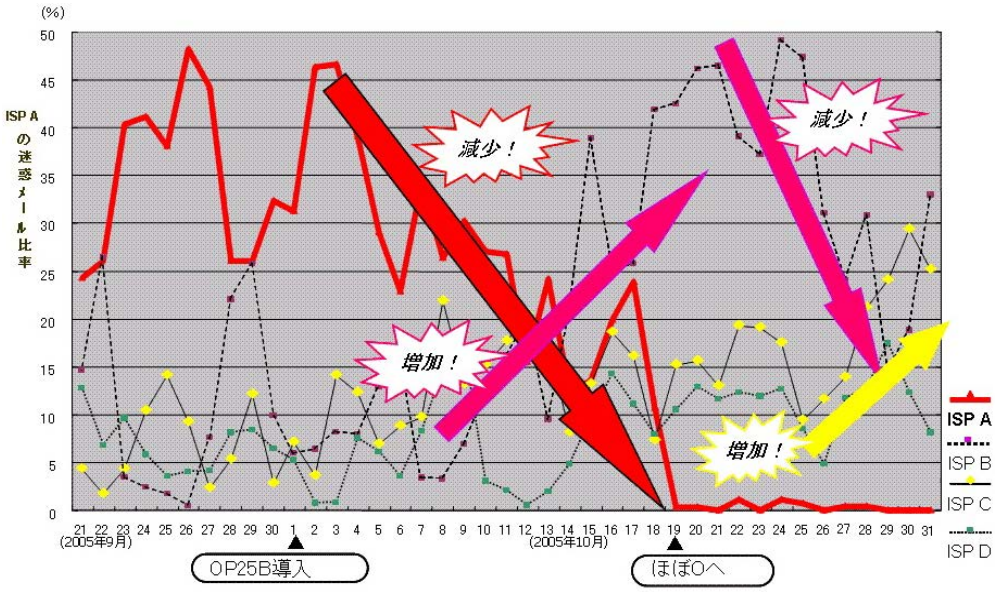

図1-3　OP25B導入効果

(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。

ア　未導入 ISP の早期導入

イ　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圧倒的に多い現状であることから、海外ISPでの早期導入やそのための国際連携の強化が必要である。

ウ　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できるため、OP25Bの導入が望まれる。

エ　利用者への周知

OP25B導入に伴う587番ポート利用では利用者の設定が必要になり、広く周知する必要がある。

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する、又は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「大量送信」や宛先不明を検出し、受信を制御する方法である。

(1) 連続メール受信数

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する、又はボ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

特定の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、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（メール内容（サイズ）、URLの有無等）により、受信を制御する方法である。

(1) メール容量による判定

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) 添付ファイル有無による判定

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ため、その感染の防止を目的としている。

(3) URL の有無による判定

サイトへ接続ができる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。

(4) キーワード（ブラックワード）による判定

メールのヘッダー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、他の判定技術や後述する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、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と、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[2]ため、複数の設定条件を組み合わせて判定できるようにしておくと効果的である。

なお、ヘッダー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ヘッダー
・拡張ヘッダー（テキスト形式、文字コード、使用メールソフト　等）

(5) 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。

ア　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従い、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できる。

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る。

[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。

イ　ヒューリスティックフィルタ(Heuristic Filter)

メールヘッダー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（中継できる）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。

ウ　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[3])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。

本方式の課題として、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が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ー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できるようにするなど、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。

[3] 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

(6) 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[4]の予防にもつながる。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、迷惑メールと判断できる場合に受信制限するもの。

(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。

本方式は、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、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できるようになり、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がある。

[4] フィッシング（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) 送信ドメイン認証

迷惑メール送信者は、受信者にメールを開いてもらうために有名なサイトに見せかけるなど送信者を特定しづらくするため、自前のサーバ等から直接迷惑メールを送信する際にドメイン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と送信者が作成する電子署名を利用するものがある。

ア　ネットワークベースの送信ドメイン認証技術（SPF／Sender ID）

受信したメールの送信者メールアドレスのドメイン名と送信元 IP アドレスが、送信側メールサーバ管理者が設定したものと一致するかどうかを検証する技術である。

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。SPF レコードには、送信元ホスト名や IP アドレス、これらに該当した場合の認証結果が記号で示される。また、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、送信元 IP アドレスが SPF レコードに一致するかどうかを検証する。

また、ネットワークベースの送信ドメイン認証技術には、SPF の上位互換に当たる Sender ID がある。

本方式は、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できることから、比較的導入が容易であり、主要 ISP では、送信側はおおむね実施されている。

本方式の課題として、メール転送時など配送経路が変わった場合に送信元情報が変更され、認証できなくなる点があるが、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、転送元のメールアドレスをホワイトリストに入れて送信ドメイン認証をしない又はその結果を利用しないで受信するという２つの方法がある。

イ　電子署名ベースの送信ドメイン認証技術

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、DKIM（Domainkeys Identified Mail）といわれる。

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ーに付加して送信する。

受信側では、メールヘッダー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、メール本文とヘッダーから作成したハッシュデータと比較・検証する。

DKIM は、メール転送時の配送経路変更に対しても電子署名が崩れない限り、正しく認証でき、加えてメール本文の改ざんも検知できるなどの利点があるが、

導入に当たっては、送信側で秘密鍵の作成管理、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導入コストが大きいといわれている。

ウ　送信側での設定状況

WIDE Project[5]のAntispam Working Groupが行ったjpドメインにおけるドメイン認証の普及率調査によると、2012年（平成24年）5月時点のSPFの普及率は43.89%、DKIMの普及率は0.50%である[6]

また、総務省が行なっている電気通信事業者における全電子メール数の送信ドメイン認証結果調査によると、2016年（平成28年）6月時点でのSPFの普及率は93.14%と高い普及率を保っており、DKIMの普及率は45.79%と徐々に普及率が増加している。

エ　認証後のメール処理の標準化

認証できなかったメールは配信しないことになるが、現在の送信ドメイン認証システムでは、「認証できたもの＝正規メール」、「認証できなかったもの＝詐称メール」とは必ずしも言えない場合がある。

認証方式によって認証対象が異なるため、メール受信者が直接確認できる「メール作成者アドレス(from)」のドメインが詐称されていても認証がパスしてしまう場合や、転送されたメールやメーリングリスト宛に送られたメールは、認証に必要な情報が伝送中に破損されることがあるため正規のメールであっても認証に失敗する場合がある。

また、送信側で設定等に誤りがあれば当然認証失敗となるが、受信側で認証失敗と判断した理由などの情報を送信側へフィードバックする仕組みがないため、送信側で認証失敗の原因を修正し、速やかに正規の運用にすることができないなどの問題がある。これを解決するため、

（ア）　認証できなかったメールの取扱いを送信側で規定し公表する
（イ）　受信側は公表された規定に基づいて処理し、認証できないと判断した情報等を送信側へ送る

といった機能を盛込み、認証対象の基本をメール作成者アドレス(from)のドメインとして、SPF 及び DKIM の認証結果を利用して統一的に処理する認証処理の標準規格：DMARC（Domain-based Message Authentication, Reporting & Conformance）の策定が進んでいる。

DMARC は、Google、Facebook、Microsoft、Yahoo 等 15 社が 2012 年（平成 24 年）１月に発表した DMARC.org[7]で原案が作成され、2015 年（平成 27 年）３月に IETF から Informational というカテゴリで RFC7489 として仕様が公表されている。これにより送信ドメイン認証の信頼性が大きく向上することが期待される。

[5] http://www.wide.ad.jp/index-j.html
[6] http://member.wide.ad.jp/wg/antispam/stats/index.html.ja
[7] http://dmarc.org/news/press_release_20120130.html

(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を格付けする。

(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対策。OP25B は、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、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。

したがって、当該 ISP の利用者は、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。

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。

ア　迷惑メールを正当なメールと誤判定する（false negative）
イ　正当なメールを迷惑メールと誤判定する（false positive）

アとイは相反するものであり、迷惑メール判定が緩めだとアが増加し、迷惑メール判定を厳しく行うとイが増加する。

このうち、実際上問題となるのはイの場合が多いと思われるが、イの問題については、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）

一般的に「ホワイトリスト」は警戒する必要のない対象の一覧表で、ここでは、送信者アドレス又は送信者のドメインを登録するもの。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。

(2) ホワイトリスト（ヘッダー、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。

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つの方法がある。

(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はなく、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ーに含ませるもの。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、拡張ヘッダーラベリングの場合、メールソフト側で拡張ヘッダーを処理でき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できるようになり、より使いやすいものとなる。

（参考１）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」に該当すると考えられる。

(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、実施できると考えられる。

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、
ア 送信ドメインの認証
イ 認証結果のラベリング
ウ 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。ウについては、当事者（受信者）の同意が必要である。

(3) ア、イの行為についても、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、ア、イの

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、送信ドメイン認証は、目的の必要性、行為の正当性が認められる。

(5) また、ア、イ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、ア、イの行為は、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、実施できると考えられる。

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」に該当すると考えられる。

(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）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、実施できると考えられる。

（参考２）送信ドメイン認証技術普及に向けた活動

迷惑メール対策推進協議会（座長:新美育文明治大学法学部教授）は、迷惑メール撲滅に向けた有力手段が送信ドメイン認証であるとみて、普及活動を展開している。

迷惑メールでは、送信者情報詐称が多い。これを検出するには送信ドメイン認証が有効であるが、できるだけ多くのメールサーバで足並みを揃えて導入することが重要である。このため、導入までの工程を示した「なりすましメール撲滅プログラム」を作成している。加えて導入に当たっては、技術の詳細や、メールの利用環境・利用局面に応じて考慮すべきことなど、具体的な導入手順や内容について理解する必要があるため、「送信ドメイン認証技術導入マニュアル」を作成し 2010 年（平成 22 年）7 月 23 日に公表した。その後、2011 年（平成 23 年）8 月 4 日に、より分かりやすい解説にするとともにデータ等を最新化し改訂している。

2010 年（平成 22 年）9 月より、協議会を構成する企業が所属する団体等への説明会が開始されており、2010 年（平成 22 年）11 月からは、協議会構成企業以外の団体へも拡大されている。

「なりすましメール撲滅プログラム～送信ドメイン認証技術普及工程表～」については、2012 年（平成 24 年）7 月及び 2013 年（平成 25 年）9 月に改訂を行い、進捗のモニタリングが行われている。

また、2014 年（平成 26 年）9 月には「送信ドメイン認証技術 WG」を発展的に解散し「技術 WG」を新設した。

今後の検討課題として、

・DMARC ＋ Reputation＋ Feedback
・メールサーバ踏み台問題への対応
・その他の技術的対策
－フィッシング対策の入り口としての迷惑メール対策(なりすまし EC サイト問題など)
－セキュリティ的に好ましくない古いシステムの刷新
－その他新たな脅威に対して迅速に対応するための情報共有などの体制

を掲げて議論を進めている。

（参考３）なりすましメール対策としてのDMARC普及に向けて

メールの送信者情報を詐称する、いわゆる「なりすましメール」による被害が続いている。なりすましメールの目的は、受信者に不正プログラム（マルウエェア）を実行してもらうことで、PCを制御できるようにし、情報搾取など様々な不正行為を行うことである。不正プログラムの侵入を防ぐため、検知技術の開発や様々な訓練が行われるようになってきたが、一箇所でも侵入を許してしまうと、それまでの対策全体が意味をなさなくなってしまうという難しさがある。

これまでメール配送上の仕組みでは、なりすましを防ぐために、送信ドメイン認証技術などが提案、導入されてきた。しかし、それぞれが特徴を持った複数の技術があることの分かりづらさや、なりすまされる立場のドメインを管理する側が、より強い対策を講じることが難しいなどの課題があった。こうした背景から、既に標準化され、普及が進んでいるSPFとDKIMを利用し、さらにドメインの管理側でドメイン認証ができるメールの送信割合や、認証が失敗した場合に受信側に期待する振る舞いを送信側のポリシーとして表明することができるDMARCが規格として提案された。DMARCの特徴には以下のものがある。

・SPFとDKIMの両方の認証結果を利用することで相互補完的に送信ドメインの認証を行える。
・メール受信者が確認することができるメールヘッダー上の送信ドメインを認証する技術。
・ドメイン管理者がドメイン認証の状況をレポートで受け取ることができる。
・ドメイン管理者が認証失敗したメールの処理方法を送信側としてポリシー表明できる。

ドメインの認証状況のレポートは、受信側から送信するものであるため、受信側で新しく導入が必要な機能となる。受信側の認証状況が、ドメイン管理側で認知できることで、正規のメールが予期せず認証失敗している配送パターンを把握し、メール送信側としての送信ドメイン認証技術の導入状況を改善できるようになる。また、受信時に認証が失敗する明確になりすましメールと考えられるメールの送信状況を知ることで、より強いポリシーを表明する動機付けにもなる。

受信側では、認証できるメールの割合が高まることで、認証されたドメインを利用したメールのふるい分けがしやすくなる。認証が失敗したドメインのメールについては、ドメイン管理側のポリシーを参照できることで、当該メールの処理方法に関して送信ドメイン側の意向を取り入れることができるようになる。

これまでのなりすましメール対策は、主としてメール受信側で検知できる対策技術として、SPFなどの送信ドメイン認証技術が推奨されてきた。DMARCでは、さらにメール送信側としてのドメイン管理者が、自らのドメインがなりすまされないようにポリシーの強弱の度合いを設定でき、受信側の認証結果をレポートとしてフィードバックしてもらえるなどの利点が得られるようになる。

（参考４）ISP を踏み台にした迷惑メール送信とその対策について

近年、利用者の送信者ID及びパスワードが何らかの方法で大量に不正取得され、それらを用いた迷惑メール送信が急激に増加している。言い換えれば、迷惑メールはISP各社の正規の送信サーバを踏み台にして大量に発信されている。そのため、ISPの送信サーバがブラックリストへ登録されやすく、利用者のメールが届きにくい状況が発生している。このようなISPを踏み台にした迷惑メールに対するいわゆる「銀の弾丸」は存在しないため、多層的な対策が必要となる。具体的には、不正取得の防止、大量送信の防止といった２層での対策が考えられる。

(1) 不正取得の防止

送信者ID及びパスワードの不正取得の方法の実態は明確になっていないが、いくつかの方法が考えられる。例えば、最近、急激に増加している、マルウェア感染サイトに誘導するメールによって利用者の端末を感染させて送信者ID又はパスワードを入手する方法、総当たり攻撃などのオンライン攻撃によって入手する方法である。さらに、暗号化を行わない状態で公衆無線LANサービスを利用した際に通信が盗聴される可能性があることも不正取得のリスクと言える。このような不正取得を未然に防止するためには、受信サーバでのセキュリティ対策強化だけではなく、利用者への啓発活動も重要となる。

(2) 大量送信の防止

不正取得された送信者IDを使ったメール送信を防止、あるいは軽減する方法はいくつかあり、実際にISPで運用されている。

ISPが運用している踏み台送信対策

対策	対策の概要
SMTP認証と送信通数制限	送信者ID当たりの送信数に制限を設ける方法。
送信IPアドレスの分離	送信メールの内容を元にしたレピュテーションを用いて、迷惑メールと判定したメールを別のIPアドレスから送信する方法。
接続元情報による制限	接続元のIPアドレスや地域情報を元にしたレピュテーションを用いて、迷惑メール発信元と判定した場合にはペナルティを与える方法。
マルチ要素認証	SMTP認証やパスワード認証以外の方法で本人認証を実施し、送信者IDの不正利用を防止する方法。
送信者詐称の制限	SMTP認証の結果と送信者情報の一致性を用いて、なりすましを見分ける方法。

送信IPアドレスの分離では、まず、送信メールのヘッダーや本文を分析して、迷惑メールかどうかを判定する。そして、迷惑メールではないと判定されたメールは、専用の送信サーバから送信する。これにより、専用の送信サーバのIPアドレスがブラックリスト登録されにくくなり、メールが届きやすくなる。なお、迷惑メールかどうかの判定を

実施するに当たっては、利用者（企業であれば管理者）の同意を得て実施する必要がある。

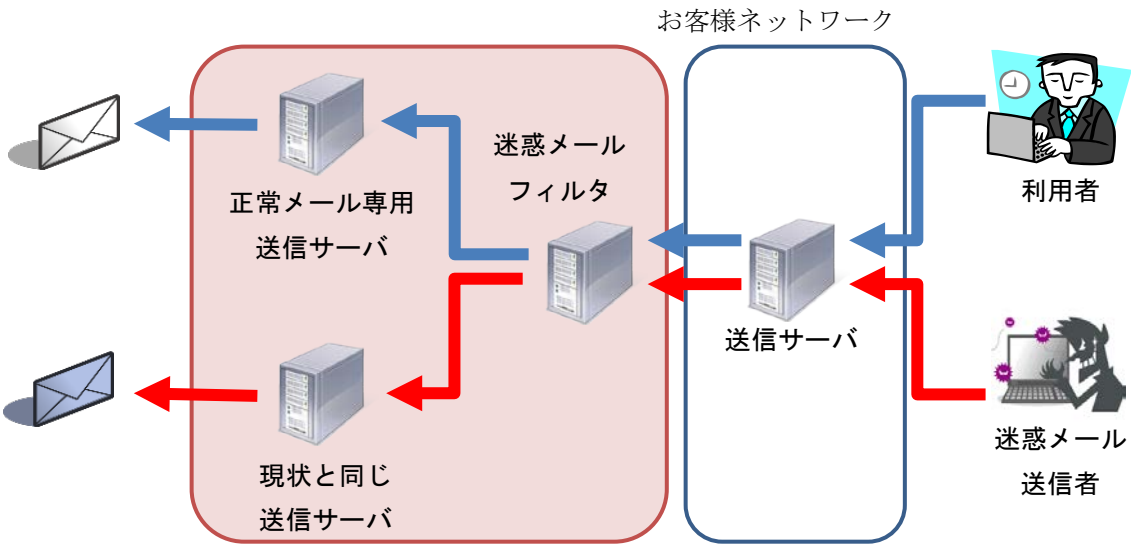

図1-5　送信IPアドレスの分離

送信者詐称の制限では、SMTP認証された送信者IDと送信者情報（エンベロープFromアドレスやヘッダーFromアドレス）を比較して、なりすましメールを判定する。これにより、なりすましメールはISPの送信サーバで拒否することができ、踏み台送信を防止することができる。

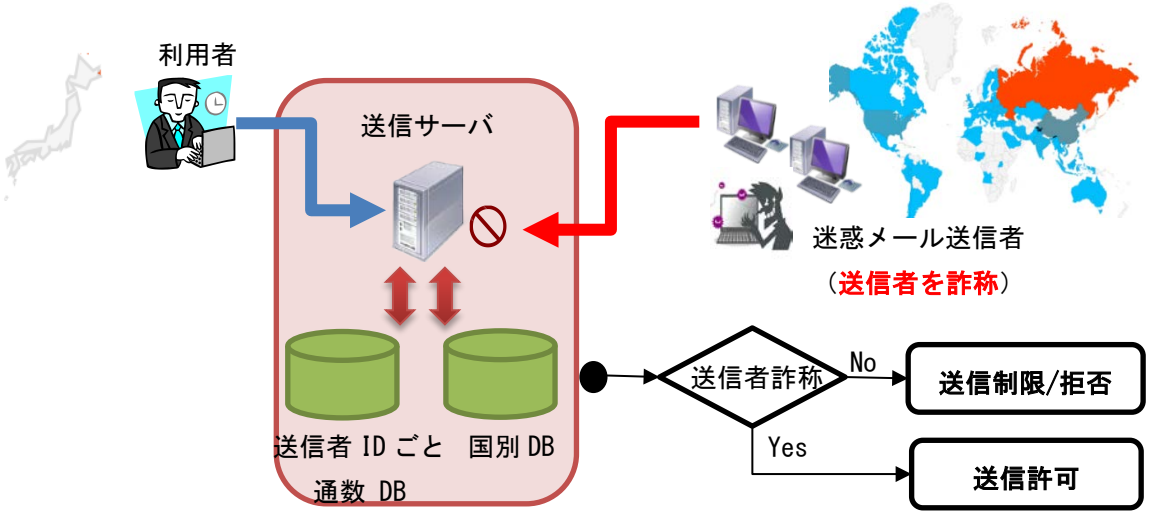

図1-6　送信者詐称の制限

これらの対策は、単独で実施するのではなく複数の対策を合わせて実施するべきである。というのも、迷惑メール送信側は、複数の対策を回避するためにより多くの送信コストが必要になることから、結果として、ISP は送信サーバを踏み台に使われることがなくなり、ひいては利用者のメール環境の改善につながることが期待できる。

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 ISP４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 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 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できたため 2004 年（平成 16 年）８月からは、１日当たりの送信数の上限を一律に 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、それまでは約 30 宛先だった同報送信宛先数を５宛先までに制限した。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して、同報送信宛先数を 30 宛先に変更している。

(4) Ｔ社

ア　サービス１

2004 年（平成 16 年）８月から、１日当たり 1,000 を超える宛先にメールが送信された場合、利用停止などの措置を行っている。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。

イ　サービス２

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

ウ　サービス３

１日１ユーザーあたり 1,000 通までに制限､同報送信宛先数を１通あたり 100 宛先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、Ａ社、Ｂ社、Ｃ社、Ｔ社（サービス２）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（サービス１、サービス３）は初期設定がなく、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恐れがあることから、転送先を設定（変更）できる回数を、2004 年（平成 16 年）６月から１日３回までに制限した（最大２メールアドレスまで設定（変更）ができる）。

５　送信ドメイン認証技術の導入（送信側）

移動系 ISP４社では、迷惑メール送信防止対策のひとつとして、送信ドメイン認証技術の導入を進めており、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 月から、DNS サーバへの「SPF レコード」の記述を実施。

(2) Ｂ社

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

(3) Ｃ社

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

(4) Ｔ社

ア　サービス１

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

イ　サービス２

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

ウ　サービス３

2014 年（平成 26 年）８月より、DNS サーバへの「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月から、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 宛に送信されるメールについて、OP25B を実施している。

(2) Ｂ社

Ｂ社では、2007 年（平成 19 年）12 月から、インターネット接続サービスから携帯電話宛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、2005 年（平成 17 年）11 月から、インターネット接続サービスから携帯電話宛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 宛のメールについても、OP25B を実施している。

(4) Ｔ社

ア　サービス１

2006 年（平成 18 年）５月から、インターネット接続サービスから携帯電話宛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 宛のメール送信についても、順次 OP25B を実施している。

イ　サービス２

携帯事業者向けには 2008 年（平成 20 年）３月から、OP25B を適用している。その他は 2009 年（平成 21 年）５月から順次開始し、同年７月に全適用が完了した。

ウ　サービス３

2014年（平成26年）８月から、ホワイトリスト管理で他社サーバへの25番ポート使用した接続を制限している。

※OP25Bを実施しているかどうかはキャリアのネットワーク側（FW等）の設定に依存しているためサービス２を基準にするのであれば実施済と言える。

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迷惑メールの送信防止対策に加えて、従来から、迷惑メールのパターンや受信状況に応じた防止措置や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利用者に対して提供しており、ISP 自らが行う迷惑メールの送信防止対策と併せて、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できる「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できたが、2007 年（平成 19 年）11 月から、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端末（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」は併用できる。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場合には、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。

(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できる。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できる。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月から、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おり、以下①～③の中から選択できる。

ア　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。
イ　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。
ウ　利用しない。

アを選択した場合は、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。また、イを選択した場合は、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できる。なお、この機能は有料サービス（月額使用料 300 円：税別）で、申込みが必要となる。

(3) Ｃ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できる「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個別に指定する「受信リスト設定」（最大220件）／「拒否リスト設定」（最大200件）があり、「受信設定」と「拒否設定」は併用することができる。

これらの設定が重複した場合、その優先順位は、以下のとおりとなる。

ア　受信リスト設定（必ず受信）
イ　拒否リスト設定
ウ　受信リスト設定
エ　一括指定受信

例えば、移動系ISP４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の受信を希望する場合は、一括指定で移動系ISP４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「受信リスト設定」に登録することとなる。

(4) Ｔ社

ア　サービス１

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、@のないアドレス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できる。なお、「指定受信」と「指定拒否」を併用することはできない。

イ　サービス２

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できる。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／拒否することもできる（登録可能件数：20件）。

ウ　サービス３

受信拒否設定については、最大で500件（ドメイン/アドレス）設定することができる。指定受信はサーバ側では行っていない。

２　送信元詐称対策

(1) Ａ社

ア　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。

イ　送信ドメイン認証技術

2007年（平成19年）11月から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おり、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） 存在しないドメインからは拒否する
（ウ） 全て拒否する

の中から選択することができる。このうち、イを設定した場合は、DNS サーバを参照して送信元のアドレス（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。ウを選択した場合は、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が、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についても、正当性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。

ウ ホワイトリスト

2008 年（平成 20 年）1 月 23 日から、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、「転送元・メーリングリストアドレスの登録機能」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

ア 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。

イ 送信ドメイン認証技術

2014 年（平成 26 年）11 月から、送信ドメイン認証技術を導入しており、迷惑メール判定の情報として利用している。

ウ 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 件までアドレスを登録することにより、当該アドレスのメールについては、フィルタリングされずに受信することができる。

(3) C社

ア なりすまし拒否

個別設定できる「なりすまし規制」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。

イ 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、「なりすまし規制」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 ともい

う)）及びヘッダーFrom を偽ったメールを拒否することができる。本機能は、なりすまし設定（高）及び（中）で利用でき、なりすまし設定（高）ではドメイン認証に成功したメールのみを受信し、なりすまし設定（中）では認証に失敗したメールを拒否することができる。

ウ　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、「受信リスト設定（必ず受信）」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「受信リスト設定」と合計で最大 220 件まで登録することができる。

(4) Ｔ社（サービス２）

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 月から、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。

ア　「低年齢層向けフィルタリング」（高）

指定受信/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）、特定 URL 付きメール拒否設定

イ　「受信拒否　強」（高）

指定受信/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）、特定 URL 付きメール拒否設定

ウ　「受信拒否　弱」（低）

指定受信/拒否設定（なりすましメール拒否、存在しないドメインからは拒否する）、特定 URL 付きメール拒否設定

(2) Ｂ社

2008 年（平成 20 年）３月 27 日から、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。設定レベルは以下の①～③のとおりであり、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。

ア　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

イ　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。

ウ　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
2005 年（平成 17 年）11 月から、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が、2010 年（平成 22 年）12 月から、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。また、2011 年（平成 23 年）２月から、迷惑メール自動規制が設定に追加された。

①　オススメ設定
　「携帯」「PHS」「PC メール」を受信、なりすましメール規制（高）、迷惑メール自動規制、拒否通知可否設定

②　携帯／PHS メールのみ受信設定（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、迷惑メール自動規制、拒否通知可否設定

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）。

(2) Ｂ社
宛先、件名及び本文の一部を受信し、全文の受信を希望しない電子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。

(3) Ｃ社
加入者は、はじめからメールの全文を受信する、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[1]、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、のいずれかを設定をすることができる（機種依存の機能）。

[1] 一部機種は未対応

(4) Ｔ社

ア　サービス１

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。

イ　サービス２

件名のみ受信した後、受信を希望する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）。

- 全て受信許可
- URL 付きメールを全て受信拒否
- 特定 URL[2]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、「特定 URL 付きのメールのみ受信拒否」は、2011 年（平成 23 年）11 月に迷惑メールフィルタ設定に統合された。

(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) Ｔ社（サービス 2）

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できるようにした。

[2] 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

⑴ 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。

⑵ 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。

⑶ Ｃ社
Ｃ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。

７　メールアドレスの変更

⑴ Ａ社
１日３回かつ月 10 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。

⑵ 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回まで変更ができる。2006 年（平成 18 年）10 月から、メールアドレスの変更回数を、一つの電話番号について 99 回までの制限を設けている。

⑶ 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。

⑷ Ｔ社

ア　サービス１
１日３回以内で、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。

イ　サービス２
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。

ウ　サービス３
24 時間に１回の変更ができる(過去 24 時間以内に変更履歴がある場合不可)。半角英数字で３字以上 29 字以内の任意のメールアドレスに変更できる。

８　メールヘッダー情報の提供

移動系 ISP４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ー情報を受信者に提供している。取得したヘッダー情報は、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。

⑴ Ａ社
インターネットから送られたメールのヘッダー情報を、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ー情報は提供されないが、ヘッダー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る。また、Ａ社が提供する ISP サービスのメールアプリではヘッダー情報は提供されないが、当該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、ヘッダー情報を見ることができる。

(2) Ｂ社

携帯電話が受信したメールのヘッダー情報は、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、ヘッダー情報を閲覧できる。ただし、閲覧できるのは過去２日間に受信したメールのヘッダー情報に限られ、Ｂ社携帯電話間のヘッダー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ー情報を、携帯電話(スマートフォンを除く)の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、ヘッダー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、例えば、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できる。また、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でき、PC で受信するようにしておけば、ヘッダー付きのメールとして確認できる。

(4) Ｔ社

ア　サービス１

携帯電話の画面より、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でき、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、ヘッダー付きのメールとして確認できる。

イ　サービス２

メール設定サイトへアクセスすることでメールヘッダーを閲覧することができる（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)。

ウ　サービス３

ブラウザ版で確認できる。

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、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。

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、Ｂ社とＴ社（サービス１、サービス２）は未承諾広告メール受信拒否機能の提供を継続している。

(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｣に設定されていたが、2008 年（平成 20 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、2014 年（平成 26 年）に機能を廃止した。

(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」に設定されていたが、2008 年（平成 20 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月に機能を廃止した。

(4) Ｔ社

ア　サービス１

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。

イ　サービス２

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

ア　迷惑メール自動ブロック

迷惑メールの疑いのあるメールを自動で判定し、ブロックすることができる。ブロックしたメールを後から確認することもできる。

イ　メールウイルスチェック

メールを通して感染するウィルスから、スマートフォンを保護することができる。メールの送受信時にチェックを行い、ウィルスを検知した場合は即座に駆除（削除）される。

ウ　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場合、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。

さらに、2007年（平成19年）11月から、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。

エ　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。

(1) Ｂ社

ア　迷惑メールフィルタ設定

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。

イ　Ｅメールのウィルスチェック

2008年（平成20年）７月から、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。ウィルス駆除ができない場合、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。

(2) Ｃ社

ア　迷惑メール自動規制

2012年（平成24年）１月から、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仕組みを実施。また、利用者は、迷惑メール自動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。

イ　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月から、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検知ができる。

ウ　HTML メール規制

2007年（平成19年）３月から、HTMLメールの受信を拒否することができる。

エ　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」に設定されており、拒否通知を設定しない場合には、送信側はメールを拒否されたかどうか分からない。

(3) Ｔ社

ア　サービス１

・迷惑メールフィルタ設定

受信メールの内容を、迷惑メールデータベースを元に機械的に判定し、迷惑メールと判断された場合は受信を拒否することができる。

イ　サービス２

・拒否通知可否設定

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。

ウ　サービス３

・迷惑メールフィルタ設定

受信メールの内容を、迷惑メールデータベースを元に機械的に判定し、迷惑メールと判断された場合は「迷惑メールフォルダ」に振り分けることができる。

（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		
				サービス１	サービス２	サービス３
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 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 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 とした。	平成 15 年から従来の約 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月から 30 に拡大された。また、平成 16 年８月から、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。	平成 16 年８月から１日当たり 1,000 を超える宛先にメールを送信した場合、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 通未満に制限している。	１日１ユーザー当たり 1000 通までに制限している。
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	平成 26 年８月
1-2 同報送信宛先数の制限			１回当たり 30 宛先までに制限		１回当たり 10 宛先までに制限	１回当たり 100 宛先までに制限している。
提供開始時期			平成 20 年１月		平成 20 年３月	平成 26 年８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」	初期設定なし。
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	平成 26 年８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		
				サービス１	サービス２	サービス３
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	平成 26 年８月
1-6 OP25B	平成17年６月から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月からインターネット接続サービスから携帯電話宛のメールに対しOP25Bを開始、平成20年３月からは固定系ISP宛のメールについても、規制した。	平成17年11月からインターネット接続サービスから携帯電話宛のメールに対しOP25Bを開始。平成20年９月下旬からは固定系ISP宛のメールについても、規制を開始した。	平成18年５月からインターネット接続サービスから携帯電話宛のメールに対しOP25Bを開始、平成20年６月からは、固定系ISP宛のメールについても、順次、規制を開始した。	携帯電話事業者向けは平成20年３月からOP25Bを開始。その他は平成21年５月から順次開始し、同年７月に全適用が完了した。	平成26年８月からホワイトリスト管理で他社サーバへの25番ポート使用した接続を制限している。
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17年11月	平成18年５月	平成20年３月	平成26年８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		
				サービス１	サービス２	サービス３
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電子メールを受信／拒否する。 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できる。 平成19年11月から、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できる。	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。携帯電話事業者及びPHS事業者からのみ受信を選択できる。 平成19年9月から、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。	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。 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できる。これらの設定が重複した場合、その優先順位は、①受信リスト設定（必ず受信）②拒否リスト設定③受信リスト設定　④一括指定受信となる。	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@のないアドレスなどから送信されたメールを受信／拒否する。	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できる。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／拒否することもできる。	受信拒否設定については、拒否は最大で500件（ドメイン／アドレス）で設定できる。
設定内容	受信120件 アドレス、ドメイン拒否各120件	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/拒否いずれか：150件	受信220件 拒否200件	許可／拒否 いずれか20件	受信20件 拒否20件	受信500件
指定受信／許可の併用	可能	Eメールは併用可。電話番号メールは許可／拒否いずれか選択	可能	不可	不可	不可
提供開始時期	平成12年11月 アドレス指定拒否 平成15年12月 事業者ごと一括指定 平成19年11月 ドメイン指定拒否 平成22年3月 設定件数拡大 40 件→120件	平成11年12月 事業者ごと一括設定（設定件数10件） 平成13年12月 設定件数拡大 10件→20件 平成19年9月 ネットワークアドレス帳優先受信機能追加 平成22年11月 設定件数増、併用可	平成14年４月 開始 平成15年５月及び17年11月 指定拒否との併用拡充 平成19年３月 設定件数拡大 20件→100件 平成22年12月 設定件数拡大 100件→200件 平成27年６月 「指定受信（なりすまし、転送メール許可）」を「受信リスト設定（必ず受信）」と改めて、登録できる最大件数を「受信リスト設定」と「受信リスト設定（必ず受信）」の合計で220件とした。	平成10年12月 開始 平成14年６月 設定件数拡大 10件→20件	平成20年3月 開始	平成26年８月 開始

記載節番号 サービス名	内　容					
	A社	B社	C社	T社		
				サービス１	サービス２	サービス３
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。	対策として送信ドメイン認証技術で詐称したと判定したものを拒否している
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20年３月	平成26年８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。	送信ドメイン認証技術を導入しており、迷惑メール判定の情報として利用している。	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できる。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26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	「転送元・メーリングリストアドレスの登録」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。	「受信リスト設定（必ず受信）」で、From、To、Ccのいずれかに含まれるアドレスの文字列を「受信リスト設定」と合計で最大で220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		
				サービス１	サービス２	サービス３
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できる。	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できる。	メールフィルタを希望のレベルに合わせて、『オススメ設定』『「携帯」「PHS」を受信』の２段階から選ぶことで、簡単に設定できる。また、平成 23 年より、迷惑メー自動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、受信を希望する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、全文の受信を希望し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、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、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、受信を希望する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		
				サービス１	サービス２	サービス３
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 付きメールをすべ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 付きメールをすべ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 付きメールをすべ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。	Ｃ社 HP で ID／パスワードを入力する。			マルチデバイスメールであるため、ブラウザ上から利用できる。
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 26 年８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 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。	半角英数字で３字以上 29 字以内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 (※平成 18 年 10 月から１つの携帯電話番号で最大 99 回まで制限)	１日３回まで	１日３回まで (平成 25 年７月より)	１日３回まで	24 時間で１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	平成 26 年８月

記載節番号 サービス名	内　容					
	Ａ社	Ｂ社	Ｃ社	Ｔ社		
				サービス１	サービス２	サービス３
2-8 メールヘッダー情報の提供	Ａ社以外から送信されたメールのヘッダー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ー情報は提供されない。	受信したメールのヘッダー情報は、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ー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ー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ー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）。	ブラウザ版で確認できる。
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	平成 26 年８月
2-9 未承諾広告メールの受信拒否	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」に設定されていたが、平成 20 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、平成 26 年に機能を廃止した。	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	受信する		
提供開始時期	平成 15 年 10 月（平成26年２月廃止）	平成 15 年 12 月	平成 15 年 9 月（平成 22 年６月廃止）	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 迷惑メール自動ブロック	迷惑メールの疑いのあるメールを自動で判定し、ブロックすることができる。ブロックしたメールを後から確認することもできる。
提供開始時期	平成 25 年 12 月
2-10 メールウイルスチェック	メールを通して感染するウィルスから、スマートフォンを保護することができる。メールの送受信時にチェックを行い、ウィルスを検知した場合は即座に駆除（削除）される。
提供開始時期	平成 22 年９月
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 日から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桁の暗証番号(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
2-10	Ｂ社
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 メールのウィルスチェック	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。ウィルス駆除ができない場合、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 迷惑メール自動規制	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「迷惑メール自動規制」を実施。また、利用者は、迷惑メール自動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検知ができる。
提供開始時期	平成 24 年１月
2-10 HTML メール規制	HTML 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 19 年３月
2-10 拒否通知可否設定	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
	Ｔ社（サービス１）
2-10 迷惑メールフィルタ	受信メールの内容を、迷惑メールデータベースを元に機械的に判定し、迷惑メールと判断された場合は受信を拒否することができる。
提供開始時期	平成 25 年２月
	Ｔ社（サービス２）
2-10 拒否通知可否設定	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」になっている。
提供開始時期	平成 20 年３月
	Ｔ社（サービス３）
2-10 迷惑メールフィルタ	受信メールの内容を、迷惑メールデータベースを元に機械的に判定し、迷惑　メールと判断された場合は「迷惑メールフォルダ」に振り分けることができる。
提供開始時期	平成 26 年８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月から、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行っている。

(2) Ｂ社

2005 年(平成 17 年)５月から、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月から、１日に 200 件以上送信した場合、その後 24 時間規制するように変更した。

(3) Ｃ社

2004年（平成16年）11月から、月間の送信数を加入３ヶ月以内の利用者は3,000件/月、プリペイド会員は3,000件/月、その他は6,000件/月に制限していたが、2011年（平成23年）７月から、送信数を200件/日又は6,000件/月（契約後３ヶ月未満は3,000件/月）に制限するよう変更した（日または月の制限に達したお客様がSMSを送信した場合エラーとなり、各制限は24:00にリセットされる)。

(4) Ｔ社

ア　メール１

2014年（平成26年）10月より、１日に送信可能なSMSを200通に制限している。

イ　メール２

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

ア　SMS一括拒否

全てのSMSを拒否することができる。

イ　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。

ウ　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。

エ　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。

オ　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）。

カ　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月から、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 月から、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

以下３つの機能を提供中。

ア　ブロック機能（NW側機能・全加入者利用可能）

2012年（平成24年）10月から、国内他事業者からのSMSを一括拒否する機能と、海外事業者からのSMSを一括拒否する機能を提供開始。

2005年（平成17年）３月から開始した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は2015年（平成27年）11月に廃止。

イ　SMS受信フィルタ機能（端末側機能（一部端末のみ））

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できる。

（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。

ウ　SMS利用制限（NW側機能・全加入者利用可能）

SMSを利用したくない場合、SMSの利用を停止することができる。

(4) Ｔ社（メール１）

指定した電話番号リスト（最大 150 件）からの SMS 受信拒否/許可設定、

または全ての SMS 受信拒否設定可能な受信フィルタ機能を提供している。

２　事業者を跨いで送信された迷惑 SMS への対応

移動系 ISP においては、2011 年（平成 23 年）７月から、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、事業者をまた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図２のような対応を行っている。

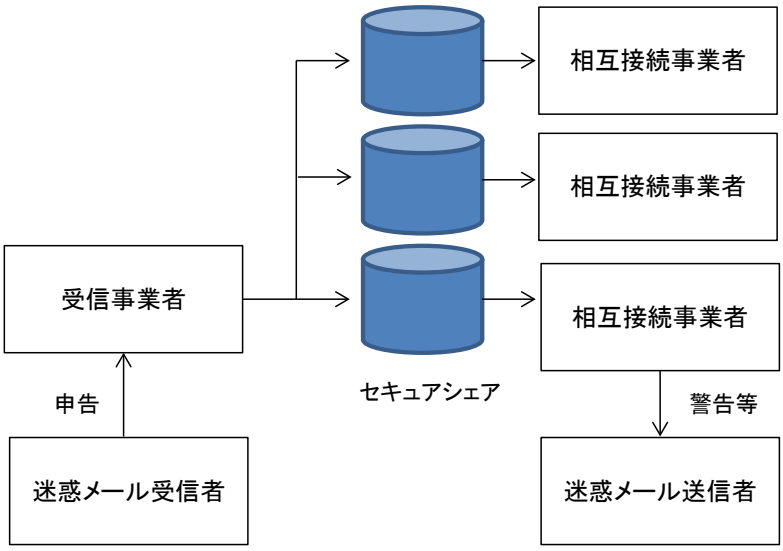

図２　申告情報の伝達ルート

(1) 申告受信事業者の対応

ア　電話、ウェブ等で申告を受け付ける。

イ　申告者から取得する情報は、SMS 本文、送信電話番号等。

ウ　取得した情報を他移動系 ISP に提供する場合がある旨、申告者本人の同意を取得する。

エ　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。

オ　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

ア　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。

イ　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。

（参考５）迷惑 SMS 対策について

宛先に電話番号を指定するのみでテキスト交換できることがSMSの最大の利点であるが、過去、国内では独自規格によるSMSが乱立し、国内の他事業者のユーザー同士でのメッセージの交換ができず、積極的に利用されなくなった。一方、携帯電話事業者がISPとなり、いわゆるキャリアメールと呼ばれるメールサービスが先行して普及したが、2011年（平成23年）７月23日に事業者間の相互接続が実現され、事業者間を跨いだメッセージの送受信ができるようになった。

メールサービスが先行したこともあり、インターネットから携帯電話宛の迷惑メールが多く、過去、受信するメールの約７割が迷惑メールという状況もあったが、その後、送信ドメイン認証技術やOP25Bによる対策が進み、迷惑メールの割合は約５割まで減少した。また、受信側におけるフィルタリングサービスの機能向上と普及により、迷惑メールはユーザーへ届かないようになったが、2014年（平成26年）10月頃より迷惑SMSに関する相談件数は増加傾向にある。

一般的にSMSは宛先に電話番号を指定してメッセージを送信するため、差出人は電話番号と思われがちだが、技術的には数字以外に英字、および一部の記号を用いることができる。

メール、MMS、SMSの違い

	メール	MMS	SMS
差出人 （使用可能文字）	あり （英数字、@、記号）	あり （英数字、@、記号）	あり （英数字、一部記号）
件名	あり	あり	なし
本文 （長さ制限）	あり （なし）	あり （なし）	あり （最大255連結）
添付ファイル	可能	可能	一部可能

（出典：メール（RFC5322）、MMS（Multimedia Messaging Service）（3GPP TS23.140、OMA MMS V1.3）、SMS（3GPP TS23.038、TS23.040））

迷惑SMSの送信元を調べると、その多くが海外事業者から国際網を経由して国内事業者へ送信されていることが判明している。当初、送信国はスウェーデン、デンマークのみであったが、その後、カンボジア、マルタ、アフガニスタン、セネガル等、送信元は拡大傾向にある。SMSの送信単価（米国のあるサービス事業者のケースで平均送信単価は$0.046／通）はメールと比較して高額のためトラフィックの総量は少ないが、携帯端末へ直接届くためユーザーの目に届く機会は高

いことが想定される。2016年（平成28年）１月では、ユーザーが講じられる対策として携帯電話事業者が提供している迷惑SMS対策機能を利用する手段がある。

国内の携帯電話事業者が提供する迷惑SMS対策機能一覧

機能	(株)NTTドコモ	KDDI(株)	ソフトバンク(株)
SMS一括拒否	○		○
非通知SMS拒否	○		
国際SMS拒否	○	○	○
国内他事業者SMS拒否	○	○	
個別番号拒否	○		○
個別番号受信	○		○

（出典：(株)NTTドコモ、KDDI(株)、ソフトバンク(株)）

迷惑SMSの多くが海外事業者から送信されている状況において、国際SMS拒否設定を適用することが有効な対策となる。ただし、初期設定ではこうした機能が無効となっている場合や当該拒否設定をした場合に、正規の国際SMSが利用できなくなる点には留意が必要である。

ネットワーク側（国際網や事業者網）での対策としては、IWSで選択的にSMSCとの接続を許可することや事業者間で積極的に連携して問題解決を図ることが考えられる。また、国内携帯電話事業者の取組として、2011年（平成23年）７月13日に迷惑SMSに関する申告情報の取扱いについて接続先事業者の加入者が送信した迷惑SMSの本文、送信電話番号、受信日時などを相互に提供し、約款に基づくことが行われている。

また、SMS はユーザー同士によるメッセージ交換（双方向通信）の利用だけでなく、ユーザーへの到達可能性の高さからアプリケーションサービスの通知や認証コードの送付（一方向通信）にも利用されるようになった。また、ユーザーインタフェースやデザインの変化によりメールと SMS の区別を意識することなく利用されるようになり、今後はメールだけでなく SMS の迷惑メール対策も求められるようになっている。

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

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国内からの送信の場合1,000通、海外からの送信の場合100通に制限している。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

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。

(3) Ｉ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。

(4) Ｊ社

2009年（平成21年）７月から、Ｊ社のメール送信用サーバに一定回数の送信失敗（大量送信）を検出する仕組みを実装した。検出された送信元端末については、必要に応じて送信停止処置を行う。

(5) 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。

(6) Ｎ社

2008年（平成20年）４月から、SMTP認証(SMTP Auth)を使用している場合には、基本メールアドレス、追加メールアドレスともに、１日あたりのメール送信数を1,000通に制限している。短時間に大量のメールを送信した場合には、上記とは別にメールの送信効率を下げる制御を一定時間行う。

(7) Ｏ社

連続メール送信の制限、同一IPアドレスからの同時大量送信への対策及び１契約者が１日に送信できるメール宛先数を制御する。

(8) 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する。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%を破棄することができる。

(9) Ｑ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。

(10) Ｒ社

１日に送信できるメールの通数に制限を設けている。

(11) 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時、一時的に、又は一定の期間、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

ア　Ｇ社

送信者アドレス(FROM:)を改変したメールの SMTP 接続を拒否する。

イ　Ｉ社

2012 年（平成 24 年）５月から、Submission Port（587 番）を利用するメール送信について SMTP-AUTH による送信者認証を実施しているが、2012 年（平成 24 年）９月から、全てのメール送信に対して SMTP-AUTH 必須化を開始した。対象を全ユーザーに拡大し、未対応の場合は送信不可とする。

ウ　Ｊ社

2004 年（平成 16 年）４月から、送信者認証を行うメール送信サービスを開始し、2007 年（平成 19 年）11 月から、新規利用ユーザーへは当該サービスの利用を案内する。

送信者確認を行った送信者が、一定時間内に一定数のメール送信を行った場合に規制する。

エ　Ｎ社

2008 年（平成 20 年）５月から、Submission Port（587 番）を利用するメール送信について SMTP-AUTH による送信者認証を実施する。

オ　Ｏ社

差出人アドレスのチェックを強化。

カ　Q社

差出人アドレス（From:）が送信者のものと確認できなかった場合、送信不可とすることがある。

(2) 送信元 IP アドレス検証

ア　H社

2007 年（平成 19 年）８月から、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 と ACL 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実現しやすい。

イ　J社

2012 年（平成 24 年）６月から、認証付き送信サーバにて、送信元 IP アドレスを元に送信元の国を判別し、複数国からの同時接続に対して規制する仕組みを導入している。

(3) 送信ドメイン認証

ア　Ｄ社

・SPF 登録：2005 年（平成 17 年）12 月から実施。

・DKIM：法人向けサービスにおいて 2005 年（平成 17 年）３月から、個人向けサービスにおいて 2010 年（平成 22 年）６月から実施。

イ　Ｅ社

・SPF 登録：2008 年（平成 20 年）１月から実施。

・DKIM：2014 年（平成 26 年）12 月から実施。

ウ　Ｆ社

・SPF 登録：2007 年（平成 19 年）２月から実施。

エ　Ｇ社

・SPF 登録：2007 年（平成 19 年）５月から実施。

オ　Ｈ社

・SPF 登録：2006 年（平成 18 年）２月から実施。

カ　Ｉ社

・SPF 登録：2006 年（平成 18 年）11 月から実施。

キ　Ｊ社

・SPF 登録：2006 年（平成 18 年）３月から実施。

ク　Ｋ社

・SPF 登録：2011 年（平成 23 年）10 月から実施。

・DKIM：2011 年（平成 23 年）９月から実施。

ケ　Ｌ社

・SPF 登録：2005 年（平成 17 年）12 月から実施。

コ　Ｍ社

・SPF 登録：2005 年（平成 17 年）５月から実施。

・DKIM：2005 年（平成 17 年）５月から実施。

サ　Ｎ社

・SPF 登録：2006 年（平成 18 年）５月から実施。

シ　Ｏ社

・SPF 登録：2005 年（平成 17 年）11 月から実施。

・DKIM：2007 年（平成 19 年）９月から実施。

ス　Ｐ社

・SPF 登録：2006 年（平成 18 年）11 月から実施。

セ　Ｑ社

・SPF 登録：2006 年（平成 18 年）12 月から実施。

・DKIM：2005 年（平成 17 年）７月から実施。

ソ　Ｒ社

・SPF 登録：2006 年（平成 18 年）10 月から実施。

タ　Ｓ社

・SPF 登録：2007 年（平成 19 年）11 月から実施。

３　OP25B

(1) Ｄ社

・携帯宛：2005 年（平成 17 年）10 月から実施。

・PC 宛：2006 年（平成 18 年）11 月から実施。

・Submission Port（587 番）：2005 年（平成 17 年）４月から提供。

(2) Ｅ社

・携帯宛：2005 年（平成 17 年）10 月から実施。

・PC 宛：2006 年（平成 18 年）６月から実施。

・Submission Port（587 番）：2006 年（平成 18 年）３月から提供。

(3) Ｆ社

・携帯宛：2005 年（平成 17 年）11 月から実施。

・PC 宛：2007 年（平成 19 年）７月から実施。

・Submission Port（587 番）：2005 年（平成 17 年）11 月から提供。

(4) Ｇ社

・携帯宛：2006 年（平成 18 年）６月から実施。

・PC 宛：2006 年（平成 18 年）10 月から実施。

・Submission Port（587 番）：2006 年（平成 18 年）６月から提供。

(5) Ｈ社
- 携帯宛：2006 年（平成 18 年）２月から実施。
- PC 宛：2006 年（平成 18 年）12 月から実施。
- Submission Port（587 番）：2006 年（平成 18 年）２月から提供。

(6) Ｉ社
- 携帯宛：2005 年（平成 17 年）３月から実施。
- PC 宛：2005 年（平成 17 年）３月から実施。
- Submission Port（587 番）：2005 年（平成 17 年）３月から提供。

(7) Ｊ社
- 携帯宛：2005 年（平成 17 年）12 月から実施。
- PC 宛：2006 年（平成 18 年）３月から実施。
- Submission Port（587 番）：2005 年（平成 17 年）11 月から提供。

(8) Ｋ社
- 携帯宛：2006 年（平成 18 年）６月から実施。
- PC 宛：2006 年（平成 18 年）６月から実施。
- Submission Port（587 番）：2006 年（平成 18 年）３月から提供。

(9) Ｌ社
- 携帯宛：2006 年（平成 18 年）３月から実施。
- PC 宛：2006 年（平成 18 年）12 月から実施。
- Submission Port（587 番）：2006 年（平成 18 年）８月から提供。

(10) Ｍ社
- 携帯宛：2006 年（平成 18 年）２月から実施。
- PC 宛：2006 年（平成 18 年）２月から実施。
- Submission Port（587 番）：2005 年（平成 17 年）10 月から提供。

(11) Ｎ社
- 携帯宛：2005 年（平成 17 年）９月から実施。
- PC 宛：2006 年（平成 18 年）12 月から実施。
- Submission Port（587 番）：2006 年（平成 18 年）２月から提供。

(12) Ｏ社
- 携帯宛：2006 年（平成 18 年）７月から実施。
- PC 宛：2006 年（平成 18 年）９月から実施。
- Submission Port（587 番）：2005 年（平成 17 年）７月から提供。

(13) Ｐ社

・携帯宛：2005 年（平成 17 年）１月から実施。
・PC 宛：2006 年（平成 18 年）７月から実施。
・Submission Port（587 番）：2006 年（平成 18 年）６月から、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月から実施。
・PC 宛：2007 年（平成 19 年）１月から実施。
・Submission Port（587 番）：2006 年（平成 18 年）６月から提供。

(15) Ｒ社

・携帯宛：2005 年（平成 17 年）３月から実施。
・PC 宛：2005 年（平成 17 年）３月から実施。
・Submission Port（587 番）：2005 年（平成 17 年）３月から提供。

(16) Ｓ社

・携帯宛：2006 年（平成 18 年）11 月から実施。
・PC 宛：2006 年（平成 18 年）11 月から一部を実施。
・Submission Port（587 番）：2006 年（平成 18 年）６月から提供。

４　その他（ボット対策）

Ｏ社

2006 年（平成 18 年）５月から、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) H22/06(個人向)	H17/10	H18/11	H17/04
E社	H20/01	H26/12	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を利用した判定

ア　Ｄ社

従来の SPF、DKIM に加え、2014 年（平成 26 年）8 月より DMARC の認証結果も検証し、結果をメールヘッダに付与している。また、SPF、DKIM の認証結果を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 月から提供しており、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)」ことができる。

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。なお、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 件登録できるが、ワイルドカードは設定できない。

イ　Ｅ社

SPF 及び DKIM による送信ドメイン認証を実施し、結果をメールヘッダに付与している。

ウ　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。

エ　Ｊ社

2012 年（平成 24 年）12 月から、SPF、SenderID、DKIM の認証を実施し、結果を、SPF と SenderID については Received-SPF ヘッダに、DKIM については Authentication-Results ヘッダに付与している。

また、自社メールドメインを送信元としたメールについては、SPF と SenderID の認証結果を利用して振り分けることができるサービスを開始した。

オ　Ｋ社

2011 年（平成 23 年）10 月から 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。

カ　Ｌ社

SFP、SenderID の認証を実施し、結果を Authentication-Results ヘッダに追記している。また、なりすましと判断したメールを迷惑メールとして扱うことができるフィルタを提供している。

キ　Ｍ社

2010 年（平成 22 年）６月から 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（Authentication-Results)。

また、2011 年（平成 23 年）５月から 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た。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。

ク　Ｏ社

SPF 及び DKIM による送信ドメイン認証を実施し、認証結果をメールヘッダに付与している。2015 年（平成 27 年）9 月から DMARC の認証結果も検証し、認証結果をメールヘッダに付与している。SPF 及び DKIM 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の実現をできるよ

うにしている。

ケ　Q社

DKIM 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を希望しない場合は救済リストとして最大 100 件設定できる。

(2) IP アドレスを利用した判定

ア　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。

イ　G社

2008 年（平成 20 年）10 月から、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。

ウ　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オンになっている。

エ　J社

2010 年（平成 22 年）３月から、迷惑メールを大量に送信する IP アドレスをシステムで自動的に判別し、迷惑メールの送信元以外から送信されるメールを優先的に取り扱う仕組みを導入した。

オ　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。

カ　Q社

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。

(3) 送信者情報を利用した判定

ア　M社

・未登録のアドレスから送信されるメールのブロック
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。

・海外 IP アドレスからのメール送信のブロック
M社のユーザーに対して、海外 IP アドレスからの POP/SMTP を禁止するオプションを、2014 年（平成 26 年）10 月から提供。

・SMTP 認証と From アドレスに基づくメール送信のブロック
M社のユーザーによるメール送信に対して、SMTP 認証の ID とヘッダ From アドレスの一致性に基づき、なりすましメールの大量送信を停止することができる。

イ　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。

ウ　Q社

送信者アドレス（From:)が存在しないメールは迷惑メールと判定し、送信元へ Reject 応答を返し受信しない。

(4) IP25B を利用した判定

①ア　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。

イ　K社

ISP 等のメールサーバを経由せず、動的 IP アドレスから直接送信されるメールをブロック。

ウ　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。

エ　M社

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　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

ア　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、単独又は組合せて、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できる。

（イ）　メール容量

20Ｋバイト、50Ｋバイト、100Ｋバイト、500Ｋバイト、１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。

イ　E社

・　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最大 300 件登録できる。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。

ウ　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できる。

エ　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）で指定できる。件名（Subject:）は部分一致（～を含む)により指定できる。設定項目は、それぞれ ON、OFF を切替でき、受信拒否と受信許可を含めて最大 300 件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できる。

オ　Ｈ社

・　ブラックワード

受け取りを希望し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、条件に当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、受信許可も含めて任意の順番で最大 30 件指定することができる。

カ　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。

キ　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できる（最大 20 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）の受信拒否設定ができる。

ク　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。設定できる条件数は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できる。

（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できる。

ケ　L社

・　ブラックワード

送信者アドレス（From:）、宛先アドレス（To:）、写し宛先アドレス（Cc:）について最大 500 件登録できる。

コ　M社

・　ブラックワード/メール容量

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:）及びメールの容量（メール容量については数値）の５項目について、単独又は組合せで合計 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でき、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。

サ　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できる。

シ　O社

（ア）　ブラックワード

受け取りを希望し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。設定できる条件数は、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。

また、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、拒否を希望するメールのヘッダを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できる。

（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。

ス　P社

・　ブラックワード/メール容量

送信者アドレス（Frpm:）（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合せ受信拒否の条件を最大99件設定できる。

セ　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最大500件設定。

ソ　R社

・　ブラックワード

受け取りを希望し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できる。２ペアで許可設定も含めて最大100件登録することができる。

タ　Ｓ社

・　ブラックワード

拒否を希望するメールアドレス、ドメイン名を指定して受信拒否設定ができる。最大50件設定できる。

(2) フィルタによる判定

ア　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月から提供。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。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できる。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できる。

イ　Ｅ社

2006年（平成18年）12月から、ヒューリスティックフィルタやシグネチャ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。

ウ　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できる。

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]を付記することもできる。

（イ）　シグネチャフィルタ

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。

エ　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。

オ　Ｈ社

ヒューリスティックフィルタを使い、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。その後、件名に[meiwaku]を付記し、メールサーバ上の迷惑メールフォルダへ振り分ける。

カ　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。

キ　Ｋ社

シグネチャ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段階まで設定できる。判定後に、その結果をヘッダに付記する。

ク　Ｌ社

シグネチャ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。

ケ　M社

（ア）　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。

（イ）　シグネチャフィルタ

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か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。

コ　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。

サ　O社

・　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て申告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（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。

シ　P社

送信者評価、ヒューリスティックフィルタ、シグニチャフィルタ、URL評価等を使い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。

ス　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）　シグネチャフィルタ

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。

（エ）　URL評価

メール本文に記載されたURLを評価し、悪質なサイトへの誘導と判断されたメールは迷惑メールフォルダへ振り分ける。またフィッシングURLなど通常より悪質と判断できたものは受信を拒否する。

セ　R社

ヒューリスティック及びシグネチャ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。

ソ　S社

ヒューリスティックフィルタ、シグネチャ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

ア　D社

受け取りを希望する相手のメールアドレスを最大1,000件登録できる。

イ　E社

受け取りを希望する相手のメールアドレスを最大300件登録できる。

ウ　F社

送信者アドレス（From:）、宛先アドレス（To:）、件名（Subject:）のそれぞれについて各100件、合計300件を設定できる。

エ　G社

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

オ　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、任意の順番で最大30件指定することができる。

カ　I社

受け取りを希望する相手のメールアドレスを設定することができる。

キ　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できる。
また、設定条件に合致するメールのみを受信することもできる。

ク　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できる。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できる。

ケ　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:)について最大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。

コ　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、単独又は組合せで受信許可条件として設定できる。設定できる条件の数は、受信拒否の条件と合わせて最大100件。

サ　Ｏ社

受け取りを希望する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。

シ　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て受信拒否の条件を最大99件設定できる。

ス　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。

セ　Ｒ社

受け取りを希望し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できる。２ペアでの拒否設定も含めて最大100件登録することができる。

ソ　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できる。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、件名等の閲覧ができるが、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、１日～30日の間で設定できる（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]の識別子を付記できる。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（設定のオンオフはユーザーにて任意で設定できる)。

(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

ユーザーの設定により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ついて、以下の対応を実施。

・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(7 日後に削除)。

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メールは、全て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、ア又はイのいずれかを選択できる。

（ア）　ラベリング

判定メールに対して件名に[meiwaku]が付記される。

（イ）　メールサーバ上のフォルダへの振り分け

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できる（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できる。）。

(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。また、以下の判定結果に応じて、各案内のメールが送信される（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)。

ア　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、送信者アドレス（From:）をホワイトリストに登録を案内するメールを送信。

イ　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。

ウ　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。

エ　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／破棄することができる。さらに、ユーザーの設定によって、[meiwaku]の文字を挿入しない等の設定もできる。

(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ない。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。また、特定の銀行や金融機関を騙ったメールに対して、ヘッダ From ドメインと表示名情報の一致性が確認できなかった場合、迷惑メールフォルダに振り分けられる。

(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　受け取りを希望し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（付記しない設定もできる）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できる。

また、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判定度合いに応じて、迷惑メールフォルダへの振り分け、送信元へ Reject 応答を返し受信しない、といった処理が行われる。また、受信拒否設定により判定されたメールは破棄される。

(15) R社

迷惑メールと判定されたメールは、メールサーバ上での隔離（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、配送又は迷惑メールフォルダに保管のいずれかを選択できる。迷惑メールフォルダに振り分け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３－１）主要な固定系 ISP が提供する迷惑メール受信対策一覧

	①大量受信制限	②送信元情報参照による受信制限								
		送信ドメイン認証技術						IPｱﾄﾞﾚｽを利用した判定	送信者ｱﾄﾞﾚｽを利用した判定	IP25B
		SPF		DKIM		DMARC				
		ラベリング	フィルタリング	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３－２）主要な固定系 ISP が提供する迷惑メール受信対策一覧

	③指定条件一致による受信制限			④迷惑メールフィルタ			⑤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	ベイジアン	ﾋｭｰﾘｽﾃｨｯｸ	シグネチャ	
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	○				○	○	○