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通信役務を提供する電気通信事業者によるその導入の状況

令和２年４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

―――――― 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ための送信側の技術（第１節）と、ISPや受信者が迷惑メールを受信しないための受信側の技術（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

送信側では、迷惑メール送信防止のため、以下の方法でメールの送信量を制限する、送信者認証を行う等の対策を講じている。

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、ISP が契約者の同一アカウントからのメール送信量を制限する方法である。

(1) 契約後の期間限定型制御

ISP との契約後の一定期間、１日当たり等に送信できるメール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、このような制御は一定の抑止効果が得られる。

(2) 連続メール送信制御

一定期間内に送信でき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、制限に達した後は、同一のアカウントからのメール送信を制御する。制限する通数及び制限期間は、各 ISP が状況に応じて、適宜定めている。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をすることが望ましい。

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ことを防止するため、送信者側の ISP が自社の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。

この方法はサーバ上で新たな技術を要しないため導入が簡単であるが、送信が許容されている時間内に別の利用者が同一 IP アドレスを割り当てられたり、認証された IP アドレスを共有し、ローカルアドレスで動作する LAN では、認証された利用者とは別の利用者が別の PC 等から送信した場合でも、認証されたものとして送信ができてしまうセキュリティ上の弱点がある。

(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。この方法は、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 では、Submission Port(投稿ポート)587 番（又は、465 番）を利用するが、これを利用する場合は、SMTP AUTH が必須である。なお、587 番ポートで SMTP AUTH を使用する際、暗号化処理ができないメールソフトがあり、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。

３　送信者アドレス照合

送信者アドレスは送信者認証をパスした後でも比較的簡単に変えられることが多いため、迷惑メール送信者は、送信者認証をパスした後に、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に、ISP が送信時の送信者アドレスと送信者認証した ID に対応する送信者アドレスとを照合し、一致しない場合は、送信しない、又は本来の送信者アドレスに書き換えて送信する等の方法である。

４　送信者認証情報の漏えい防止

迷惑メール送信者は送信者認証に使う ID/パスワードを不正な手段で入手し、送信者認証を成功させることが多い。これを阻止するため、一定回数以上認証に失敗した場合に送信させない方法である。

(1) アカウントロック

送信者認証時、一定回数以上のパスワード入力誤りがあ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に１ID 当たりのアクセス回数を少なくし､同一の IP アドレスから 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転送元サーバは設定した宛先に迷惑メールを配信してしまう。そのため、転送先は、転送元の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がある。これを防止するための方法である。

(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、迷惑メー

ルでないものだけを転送するもの。

(2) 転送設定解除

受信者が転送設定の最新化をしていない場合、存在しない宛先へ転送され続けることになる。これを避けるため、一定回数以上転送に失敗した場合、転送設定を解除するもの。これにより、転送しているメールサーバが、宛先不明メールの送信サーバとして転送先から拒否されることや宛先不明に伴うエラーメールが転送設定している者ではなく元のメールの送信者に届くことによる混乱を防ぐことができる。

(3) 転送アドレス書換え

転送設定をしている場合に送信者アドレスを、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、転送設定をしている者自身が、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を送信することが多い。このとき使用される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。このような、ISPのメールサーバを使用せず、動的IPアドレスが割り振られたサーバから直接メールを送信をすることを阻止する方法が、OP25B である。

(1) 仕組み

メール送信は送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そのISP のネットワーク外の 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（又は、465 番）を認証機能（SMTP AUTH）必須として提供している。なお、これを利用するには利用者の使用しているメールソフトの設定変更が必要であり、587 番（又は 465 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) OP25B の課題

OP25B の導入は迷惑メール送信防止に大きな効果を上げてきたが、OP25B を未導入の ISP からは未だに迷惑メールが送信されている実態が

あり、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　未導入の ISP での早期の OP25B の導入

イ　海外への普及

サービス制限に対する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ことから、海外のISPでの早期のOP25B導入やそのための国際連携の強化が必要である。

ウ　ISP内のメールへの対策の導入

OP25Bを導入しても、そのISP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、ISP内のメールへの対策の導入が望まれる。

エ　利用者への周知

OP25Bの導入に伴う587番（または465番）ポート利用のためには利用者の設定が必要になり、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、迷惑メール受信防止のため、以下の方法で迷惑メールをブロックする又は受信を制御する等の対策を講じている。

１　迷惑メールの特徴を踏まえた制御

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されることが多いため、特定の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、受信を制御するもの。

ただし、数分～数時間単位で常時接続回線のセッションを一旦切断し、再接続して、別の動的IPアドレスを取得することで、特定のIPアドレスからの受信数を減らすケースやボットネットを利用して１台当たりの送信数を減らすケースがある。このようなケースにはこの手法では対応が困難である。このため、メールアドレスやドメイン単位で送信元の同一性を判断し、受信制御する手法も使われている。

(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制御する方法である。宛先不明メールを受信した際に、そのIPアドレスから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にはそのIPアドレスからのメールの受信を行わないようにするもの。

２　受信メールの内容による制御

迷惑メールの外形的な内容（メール容量（サイズ）、URL の有無等）により、受信を制御する方法である。

(1) メール容量による制御

受信メールの容量（サイズ）により制御するもの。画像情報等の大容量の情報を含むために上限値を超える容量のメールや、逆に下限値に満た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制御

添付ファイルの有無により制御するもの。添付ファイルに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 の有無による制御

サイトへ接続ができる URL の有無により制御するもの。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、大容量のメールを受信する必要があるとき、添付ファイルが必要なとき、URL が必要なときが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）による制御

メールのヘッダーまたは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し、制御するもの。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く、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はなく、メールの内容に応じた振分けのための機能であるが、きめ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により、迷惑メール判定技術としても十分機能するものとなる。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、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、ホワイトリストを併用した判定を行うことが効果的である。

なお、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、ブラックワードではないと誤判断させる[1]ことがある。このため、ブラックワードだけで迷惑メールを判定するのではなく、複数の条件を組み合わせて判定す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）
・日時（date）
・Receivedフィールド
・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）

[1] 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。

(5) 迷惑メールフィルタ

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

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定するもの。“迷惑メールである”、“迷惑メールではない”と判定した基準に従い、以後のメールを自動的に解析・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、利用者の利用状況に合わせた効果的な判定ができる。

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を解析し、そこから得られた迷惑メールの特徴などをルールに従い点数化し、集計点数が基準値を超える場合に迷惑メールと判定するもの。

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ものを迷惑メールであると判定する”といったルールを作ることもできる。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。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定する。

この方法の欠点は、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である。

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[2]）を抽出しておき、受信したメールのものと比較を行うことで、迷惑メールであるかを判定するもの。シグネチャーは、実際の迷惑メールから作成されるため同一のメールを確実に識別できるのは当然であるが、亜種の識別にも適用できるよう工夫されている。

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による検出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

[22] 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

惑メールかどうかを判定する方式となっている。メッセージの全体を視覚的に判定しないため、フィルタリング速度は速く、メールシステムの管理者による負担も少なく、高いシステムパフォーマンスを発揮する。

この方法の課題は、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シグネチャーデータベースの構築には、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を常に行い有効性の低下を防ぐ必要がある点である。

ベンダーが提供する対策製品に重要なことはその正確性であり、誤認識を低減し、利用者が受信すべきメッセージが失われ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、技術をバランス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、迷惑メールと判定するスコアを利用者が設定できるようにするなどにより、絶えず判定性能を改善するよう、総合的な迷惑メール分析手法の技術を向上させていくことが求められる。

(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、迷惑メールの特徴となる宣伝等の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、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 を隠したりしていたとしても、メッセージに埋め込まれた URL を正確に抽出し、実際に使われることになるリンクで確認するため、フィッシング[33]の防止にもつながる。一般的に、迷惑メールには URL が記述されたものが多いため、判定方式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かく、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　送信元情報による制御

メールの送信元情報を参照し、受信制御するもの。

(1) ブラックリスト（RBL：Realtime Black List）

迷惑メールの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含まれる IP アドレスからのメールを、迷惑メールと判定するもの。

外部機関が数多くの RBL を提供しており、これらを利用するのが一般的である。送信元の IP アドレスが、利用する RBL に含まれている場合に、

---

[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。

該当するメールを迷惑メールと判定する。

送信元のIPアドレスは受信メールサーバのメール受信処理の最初の段階で判明することから、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、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には、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

受信メールサーバがメールを受信した際に、既知の送信メールサーバからの場合には正常に配信を行い、未確認のメールサーバからの場合には配信を一時的に拒否するもの。本来なら送信側のメールサーバは、拒否応答を適切に扱い、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、再試行しないことが多いため、迷惑メールをブロックできる。

このグレーリストの欠点は、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、受信が数時間遅延してしまうという点である。

(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かせるために送信者を有名なブランドに見せかけるなど、送信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。送信ドメイン認証結果によって、詐称と判定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で認証する技術である。

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。登録された情報を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アドレスおよび、送信元がこれらに一致した場合の認証結果を記号で示す。一方、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レコード中のものに一致するかどうか

を検証し、認証の判定を行う。また、SPF の上位互換に当たる技術には Sender ID がある。

この方法は、送信側の 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、電子署名を利用するものに比べ、比較的導入が容易である。

この方法の問題点は、メール転送などで配送経路が変わった場合に送信元 IP アドレスが変わり、認証できなくなる点であるが、解決策としては２つの方法がある。

１つは転送元で送信者情報を書き換える方法である。転送時に、送信者情報を転送元のメールアドレスやドメインに書き換えて送信すれば、受信側では転送元のドメインを認証することになるので、転送元のドメインがネットワークベースの送信ドメイン認証技術に対応していれば認証ができる。この場合、送信者情報を単純に書き換えてしまうと、転送先で宛先不明になったエラーメールが転送元と転送先でループしてしまう可能性がある。そのため、転送時に書き換えるメールアドレスのローカルパート部分を受信時の（転送設定された）メールアドレスとは別のものにして、そのメールアドレス宛にエラーメールとして戻ってきた場合は転送しないといった方法を取ることが必要となる。

もう１つは、転送先で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、またはその結果を利用しないで受信するという方法である。

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技術を用いて送信ドメインの認証を行うものであり、DKIM（Domain keys Identified Mail）という。

送信側では、あらかじめ自ドメインに対する公開鍵を DNS サーバに登録する。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電子署名と関連情報を取り出し、DNS サーバから公開鍵を取得する。取得した公開鍵を使って、関連情報に従って電子署名を検証する。

DKIMは、メール転送による配送経路変更があっ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、送受信側で鍵を用いた「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　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。

認証方式が利用する認証対象によっては、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成功してしまう場合や、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が、認証に必要な情報が伝送中に書き換えられ、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認証に失敗することがあるが、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速やかに修正し、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、2 つの機能

・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
・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

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として DMARC（Domain-based Message Authentication, Reporting, and Conformance）が策定された。

DMARC[4]は、SPF と DKIM の認証結果を利用して、総合的に送信ドメイン認証を行う技術である。DMARC では、認証に失敗した場合のメールの取扱いを送信側でポリシーとして宣言できる。これにより、なりすましが重大な問題となるメールに対しては、受け取らないといった強いポリシーを受信側に伝えることができる。さらに、送信側のドメイン管理者のポリシー設定の判断を助けるために、メール受信側は認証結果を、送信側が設定する宛先に送信できる。送信側での DMARC 導入は、既に SPF あるいは DKIM を導入していれば容易であるが、受信側での導入には処理機能の追加が必要になる。

エ　転送されるメールの送信ドメイン認証技術

これまでに説明した送信ドメイン認証技術は送信サーバから受信サーバに直接送信されたメールに対してはうまく働くが、転送などで中間に他のサーバが介在したメールに対しては正しく認証できない場合があった。

この問題を解決する技術として、ARC（The Authenticated Received Chain）が策定された。

ARC[5]を実装したメールサーバは、直前のメールサーバとの関係での認証結果と直前のメールサーバが行った ARC 認証の結果を使って自らの ARC 認証を行ない、その結果を ARC ヘッダセットとして累積的にヘッダーに付加し、電子署名する。これにより、転送経路に沿って信頼の連鎖

[4] IETF から RFC7489 として仕様が公開されている
[5] IETF から RFC8617 として仕様が公開されている

が形成され、最初の受信サーバが行った従来の認証結果を後続の受信サーバが信頼することができ、真正なメールの転送であれば、転送先でも送信ドメイン認証が成功する。

(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。

数十万件のメール送信元のサーバに対して、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、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行って、信用度（レピュテーション）データを作成する。

(5) IP25B（Inbound Port 25 Blocking）

迷惑メール送信者は、固定 IP アドレスを割り振られた、契約先 ISP のメールサーバを使わず、動的 IP アドレスからボットネット等を利用し直接メール送信を行うことがある。受信側の ISP が、これらの動的 IP アドレスからの送信をブロックするのが IP25B である。

OP25B は、ISP が自ネットワークから他のネットワークに、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 アドレスから自ネットワークに送信されたメールを受信しない、というものである。

ただし、ブロックすべき他の ISP の動的 IP アドレスに関する情報は、個別に各 ISP から取得する必要があるので、海外発信を含めて IP25B を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2通りの誤判定が発生し得る。

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）

アとイはトレードオフの関係にあり、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されるが、イの誤判定は、個々のメール受信者特有の情報を元に、その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あり、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。

正当ではあるが迷惑メールと判定されそうな内容を送付してくる送信者を登録する。事前にリストを完成させるのは容易ではないため、誤判定（false positive）のつど、ホワイトリストに順次追加していく方法が一般的である。

なお、PC 上のメールソフトには、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には、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、この方法を用いて、件名や本文中に含まれるそのメールマガジン等に固有のキーワードをリストアップすることが有効である。

５　判定後の処理

迷惑メール判定後の処理として、以下の４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

正当なメールを格納す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 が提供する迷惑メール対策で提供されているメールフォルダの利用者の場合、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、件名に含ませる場合、件名の最初に［MEIWAKU］等の文字を付加する。

この方法は、受信者自身又は PC 上のメールソフトでの振分け処理を前提としたものである。なお、件名へのラベリングは、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

対策機能でも採用されている。これは、多くのメールソフトで、件名による振分けが可能であることを前提としている。

また、拡張ヘッダーへのラベリングの場合、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、そのようなメールソフトでは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することで、より使いやすいものとなる。

(4) メールソフトへのブランド標識の表示

送信ドメイン認証に成功したメールやそれに対応していないメールには、認証結果（pass、none など）が拡張ヘッダーに設定されることはあっても、一般には、件名には表示されない。そのため、メール受信ユーザは受信メールが認証に成功しているのかどうか、さらに、成功しているとしたらどのドメインに対して成功したのかを容易に知ることはできない。この問題を解決する手段として、BIMI（Brand Indicators for Message Identification）の規格化が進められている。

BIMI[6]においては、送信側のドメインオーナは、認証に成功した場合に表示すべきブランド標識（アイコン、ロゴなど）の画像データを指す URI を DNS サーバに登録しておく。受信側サーバは DMARC または ARC の認証に成功し、かつ、ポリシー強度が規定以上の場合に、この画像データをメールに付加し、メールソフトに対し、その画像を表示すべきことを指示する。メールソフトがその画像を受信メールとともに表示することで、ユーザはそのメールがどのドメインで認証に成功したことを容易に知り、その後の扱いを判断することができようになる。

この技術の弱点は、DNS を利用する技術に共通した、DNS のセキュリティに関するもののほか、送信ドメイン認証技術に共通したホモグラフドメインやカズンドメイン[7]に関するものがある。つまり、有名ブランドのドメイン名に類似したドメイン名を定義して、送信ドメイン認証のための設定を行い、有名ブランドと同じ画像を登録した場合、メールユーザはこの偽装メールを真正なメールと誤認する可能性が非常に高いという問題である。この問題を解決するために、BIMI では身元、ドメインとブランド標識の権利の正当性が確認できた者にのみ発行される証明書（VMC（Verified Mark Certificates））を取得した送信側のドメインオーナが、画像データの所在とともにその証明書の所在を指定する仕組みが提案され、実用が始まっている。

6 IETF から Draft として仕様が公開されている

7 ドメイン名を誤認させるために、著名な企業のドメインによく似た名称や、見誤りやすい文字（例えば、「m」の代わりに「rn」、「a」（ラテン文字）の代わりに「ａ」（キリル文字）など）を利用したドメイン名。

（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者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ものであり、手段の相当性も認められる。

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

４　DMARC導入に関する法的な留意点

（１）　DMARCを導入した場合、ドメイン管理者は当該ドメイン名義で送信される電子メールに関して、受信時のドメイン認証が失敗した場合の取り扱い方針を宣言するとともに、認証結果に関するレポートの送付先メールアドレスを

公開し、受信サーバから当該レポートを受領する。

（２）電子メールの受信サーバにおいてドメイン認証を行い、認証できない場合には一定の措置を講じ、認証できない通信に関する情報を、ドメイン管理者又はその指定する者に報告する行為と解釈されることから、「通信の秘密」を「侵す行為」に該当すると考えられる。

（３）約款等による事前の包括的合意によって通信の秘密の利益を放棄させることは、①約款の性質になじまないこと、②同意の対象が不明確であることから、原則として許されず、有効な同意とは解されない。

（４）ただし、以下の条件を満たす場合には、約款等による包括同意に基づいて提供する場合であっても、利用者の有効な同意を取得したものと考えることができる。

ア　利用者が、随時、任意に設定変更できること
イ　同意の有無に関わらず、その他の提供条件が同一であること
ウ　同意の対象・範囲が明確にされていること
エ　ドメイン認証の結果に係るレポートを送付する場合、レポートの内容に電子メールの本文及び件名が含まれないこと
オ　DMARCの内容について、事前の十分な説明を行うこと（電気通信事業法第26条に規定する重要事項説明に準じた手続きによること）

（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[8]（座長:新美育文明治大学名誉教授）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。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。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た第 2 版を公表した。2020 年度末現在、世界的な技術導入動向を踏まえ、DMARC を含めるなどの改定に向け作業中である。

2010 年（平成 22 年）９月から、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た。

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。

2016 年（平成 28 年）11 月には「送信ドメイン認証技術とフィードバックループの推進」と「電気通信事業者による迷惑メールの踏み台送信対策の状況（概要）」を取りまとめ、これらを公表した。

また、2018 年（平成 30 年）からは、それまで発行していた「迷惑メール対策ハンドブック」の内容を見直し、迷惑メールの現状や迷惑メールへの様々な対策を総合的にまとめた「迷惑メール白書」を年次で発行しており、2020 年（令和 2 年）9 月に「迷惑メール白書 2020」を発行した。

[5]https://www.dekyo.or.jp/soudan/contents/anti_spam/

（参考３）
「政府機関等の情報セキュリティ対策のための統一基準群
（平成 30 年度版）」について

サイバーセキュリティ戦略本部は、平成 30 年 7 月 25 日、「政府機関等の情報セキュリティ対策のための統一基準群」（以下「統一基準群」という。）を決定した。
（https://www.nisc.go.jp/active/general/kijun30.html）
サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 25 条第１項第２号において、国の行政機関等のサイバーセキュリティに関する対策の基準を作成することとされおり、今回の決定は、これに基づいたものである。

「統一基準群」のうちの「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」（以下「統一基準」という。）の電子メールの項目（7.2.1）には、電子メールの送受信に関して、不適切な利用による情報漏えいなど機密性に対するリスクの他、悪意のある第三者によるなりすまし等で、不正な行為の被害に職員等が巻きこまれるリスクもあるため、適切な電子メールサーバの管理が必要であるとの趣旨が述べられている。

そして、電子メールの導入時の対策として、情報システムセキュリティ責任者への遵守事項を以下としている。
(a)電子メールサーバが電子メールの不正な中継を行わないように設定すること。
(b)電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。
(c)電子メールのなりすましの防止策を講ずること。
(d)インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講ずること。

上記「統一基準」の対策を具現化するため、「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」には、送信ドメイン認証技術に関する以下のような内容が記載された。

「統一基準群」7.2.1 電子メールの遵守事項(1)(c)関連の基本対策事項として、

「7.2.1(1)-2　情報システムセキュリティ責任者は、以下を例とする電子メールのなりすましの防止策を講ずること。

a)SPF、DKIM、DMARC 等の送信ドメイン認証技術による送信側の対策を行う。
b)SPF、DKIM、DMARC 等の送信ドメイン認証技術による受信側の対策を行う。
（後略）　　」

また、「送信ドメイン認証技術」の導入に当たっては、迷惑メール対策推進協議による「送信ドメイン認証技術導入マニュアル」を参考にすると良い旨が記載されている。

（参考：https://www.dekyo.or.jp/soudan/aspc/report.html#dam）

第２章　迷惑メールに関する移動系ISPの対策状況

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。

B 社サービス２、サービス３については旧仕様を記述しているが、2017 年度より順次 B 社サービス１の仕様に移行している。

１　宛先不明メールの受信拒否

移動系 ISP３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

ア サービス１

24 時間以内に 1,000 通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 通としている。

イ サービス２

2004 年（平成 16 年）8 月から、１日当たり 1,000 通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。

ウ サービス３

１日１ユーザー当たり 1,000 通までに制限、同報送信宛先数を１通当たり 100 宛先までに制限している。

エ サービス４

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。

(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、2008 年（平成 20 年）1 月 16 日から、同報送信宛先数を 30 宛先に変更している。

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社は推測されにくい「複数のランダムな英数字@×××.ne.jp」としている。

４　自動転送先設定回数の制限

Ｃ社では、自動転送先設定機能を悪用した迷惑メールが送信され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、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 ISP３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、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 月から、DNS サーバへ「SPF レコード」の記述を実施。

(2) Ｂ社

ア サービス１

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

イ サービス２

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

ウ サービス３

2014 年（平成 26 年）8 月から DNS サーバへ「SPF レコード」の記述を実施。

エ サービス４

2008 年（平成 20 年）3 月から 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 月から 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

ア　サービス１

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。

イ サービス２

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。

ウ サービス３

2014 年（平成 26 年）8 月から他社サーバへの 25 番ポート使用した接続を制限している。

エ サービス４

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。

(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Ｂ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。

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）ができるようなサービスを、従来から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。

また、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

ア サービス１

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（ア）～（ウ）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、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。

イ サービス２

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。「指定受信」と「指定拒否」を併用することはできない。

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。

エ サービス４

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）。

(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 ISP３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 ISP３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。

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 のメールアドレス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、パソコンなどのメールアドレス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。

⑵Ｂ社

（サービス１）

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。

（サービス３）

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。

（サービス４）

ア 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）。

⑶Ｃ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 という））、及び送信元のアドレス(Header From)を偽っ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最大 220 件まで登録することができる。

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（サービス１）

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ア～ウのとおりであり、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

2017 年（平成 29 年）6 月 13 日から、PC・スマートフォン向け各種迷惑メール対策の変更画面を改善した。

(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。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。

ア　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

イ　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
ア　サービス１
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。

イ　サービス２
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。

ウ　サービス４
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。

(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）。

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、すべて受信許可）。

ア 全て受信許可

イ URL 付きメールを全て受信拒否

ウ 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、③特定 URL 付きのメールのみ受信拒否の中から選択して設定することができる。

(2) Ｂ社

ア サービス１

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。

イ サービス４

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。

(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。

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。

(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。

---

1 一部機種は未対応

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

⑵ Ｂ社

ア　サービス１

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。

イ　サービス３

マルチデバイスメールであるため、ブラウザ上から利用可能。

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

ア サービス１

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。

イ サービス２

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。

ウ サービス３

24 時間に１回の変更できる（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 文字以上 29 文字以内の任意のメールアドレスに変更できる。

エ サービス４

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。

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。

８　メールヘッダー情報の提供

移動系 ISP３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。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。

⑵ Ｂ社

ア　サービス１

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。閲覧できるのは過去 48 時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。

イ　サービス２

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。

ウ　サービス３

ブラウザ版で確認できる。

エ　サービス４

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）。

⑶ Ｃ社

携帯電話が受信したメールのヘッダー情報は、Web メールを利用して閲覧することができる。

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。

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（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。

⑴ 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。

⑵ Ｂ社

ア　サービス１

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。

イ　サービス２

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

ウ　サービス４

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。

⑶ 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）に機能を廃止した。

１０　その他各社が提供するサービス

⑴ Ａ社

ア　詐欺/ウイルスメール拒否

フィッシング詐欺などの危険なメールの送信元情報の一覧と、送信されたメールの送信元情報を比較し、一致した場合はメールを拒否できる。危険なサイトにつながる URL の一覧と、メール内に含まれる URL を比較し、一致した場合はメールを拒否できる。また、メールの受送信時にウイルスを検知した場合、駆除（削除）できる。

イ　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。

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）。

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。

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。

⑵ Ｂ社

ア　サービス１

（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　サービス２

（ア）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。

ウ　サービス３

（ア）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。

エ　サービス４

（ア）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。

⑶ 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受信する（１日１回）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。

（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
		サービス１	サービス２	サービス３	サービス４	
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 18 年 12 月	平成 20 年３月	平成 20 年３月	平成 17 年４月
1-2 送信通数規制	１日１台当たりの送信を 1,000 通未満に制限する。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。	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。平成 29 年度より順サービス１の仕様に移行中。	１日１ユーザー当たり 1,000 通までに制限している。 平成 29 年度より順次サービス１の仕様に移行中。	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。
提供開始時期	平成 15 年 10 月	平成 15 年 12 月	平成 16 年８月	平成 20 年８月	平成 20 年３月	平成 15 年９月
1-2 同報送信宛先数の制限				１通当たり 100 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 30 件までに制限
提供開始時期				平成 26 年 8 月	平成 20 年３月	平成 20 年１月
1-3 メールアドレスの初期設定の変更	契約時における初期設定は「複数のランダムな英数字@xxx.ne.jp」					
提供開始時期	平成 13 年７月	平成 15 年１月	平成 10 年 12 月	平成 20 年３月	平成 26 年８月	平成 11 年４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
		サービス１	サービス２	サービス３	サービス４	
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 18 年３月	平成 26 年８月	平成 20 年３月	平成 17 年 12 月
1-6 OP25B	平成 17 年６月から一部の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。	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 を実施、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 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。	平成26年８月から他社サーバへの25番ポート使用した接続を制限している。	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月からより順次開始し、同年７月に全適用が完了した。	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。
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５月	平成 26 年８月	平成 20 年３月	平成 17 年 11 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
		サービス１	サービス２	サービス３	サービス４	
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。	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。「指定受信」と「指定拒否」を併用することはできない。 平成 29 年度より順次サービス１の仕様に移行中。	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。 平成 29 年度より順次サービス１の仕様に移行中。	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。	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。
設定内容	受信 120 件 ｱﾄﾞﾚｽ、ﾄﾞﾒｲﾝ拒否各 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	許可/拒否いずれか 20 件	受信 500 件	受信 20 件 拒否 20 件	受信 220 件 拒否 200 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	不可	不可	不可	可能
提供時期	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 10 年 12 月開始 平成 14 年６月設定件数拡大 10 件→20 件	平成 26 年８月から開始	平成 20 年３月から開始	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。

記載節番号	内　容					
サービス名	Ａ社	Ｂ社				Ｃ社
		サービス１	サービス２	サービス３	サービス４	
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。			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。	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 26 年８月	平成 20 年３月	平成 14 年７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。		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。	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。	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 26 年 8 月	平成 20 年 3 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 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
		サービス１	サービス２	サービス３	サービス４	
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 メールのみ受信設定』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	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)。	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。	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。	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。
提供開始時期	平成 13 年５月 (3G 方式のみ) 平成 15 年５月 (2G の一部端末可)	平成 11 年 12 月	平成 16 年３月		平成 20 年３月	平成 12 年 11 月

記載節番号 サービス名	内　容					
	Ａ社	Ｂ社				Ｃ社
		サービス１	サービス２	サービス３	サービス４	
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③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 20 年３月	平成 19 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。		マルチデバイスメールであるため、ブエウザ上から利用可能。		Ｃ社 HP で ID/パスワードを入力する。
提供開始時期	平成 14 年 10 月	平成 15 年５月		平成 26 年８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 29 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 30 字以下の任意のメールアドレスに変更できる。
	１日３回までかつ月 10 回以内	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 （平成 25 年 7 月から）	24 時間で 1 回まで	１日３回まで	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 16 年９月	平成 26 年８月	平成 20 年３月	平成 13 年 12 月

記載節番号 サービス名	内　容					
	Ａ社	Ｂ社				Ｃ社
		サービス１	サービス２	サービス３	サービス４	
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。48 時間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。	ブラウザ版で確認できる。	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。規定要領に依存するためあくまで目安）。	携帯電話が受信したメールのヘッダー情報は、Web メールを利用して閲覧することができる。 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。
提供開始時期	平成 14 年 10 月	平成 15 年５月	平成 10 年 12 月	平成 26 年８月	平成 20 年３月	平成 16 年６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。	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。		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。	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。
初期設定	受信しない	受信しない	受信する		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 14 年６月		平成 20 年３月	平成 15 年９月 （平成 22 年６月廃止）

記載節番号 サービス名	内　容 提供開始時期
	Ａ社
2-10 詐欺/ウイルスメール拒否	フィッシング詐欺などの危険なメールのチェックを行い、危険を検知した場合、拒否することができる。また、メールの受送信時にウイルスを検知した場合、駆除（削除）できる。 令和２年１月
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。 平成 25 年 12 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。2007 年（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。 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。 平成 11 年７月
	Ｂ社（サービス１）
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。 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。 平成 20 年７月
	Ｂ社（サービス２）
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。 平成 25 年２月
	Ｂ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。 平成 26 年８月
	Ｂ社（サービス４）
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。 平成 20 年３月
	Ｃ社
2-10 迷惑メール自動規制	受信したメールの中で、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受信する（１日１回）か、否かを選択できる。 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。 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。 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。 平成 17 年 11 月

第３節　SMSを利用した迷惑メール送信防止対策の導入状況

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実施している。

(2) Ｂ社

ア サービス１

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。

イ サービス２

2014年（平成26年）10月から、1日に送信できるSMSを200通に制限している。

ウ サービス３

１日に送信できる SMS を 200 通に制限している。

(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/日または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）。

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防止対策の提供状況

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

すべての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

個別に指定した電話番号からの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

ア　サービス１

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。

イ　サービス２

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。

(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月に、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月に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月に廃止した。

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 5 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。

（オ） サードアプリ連携

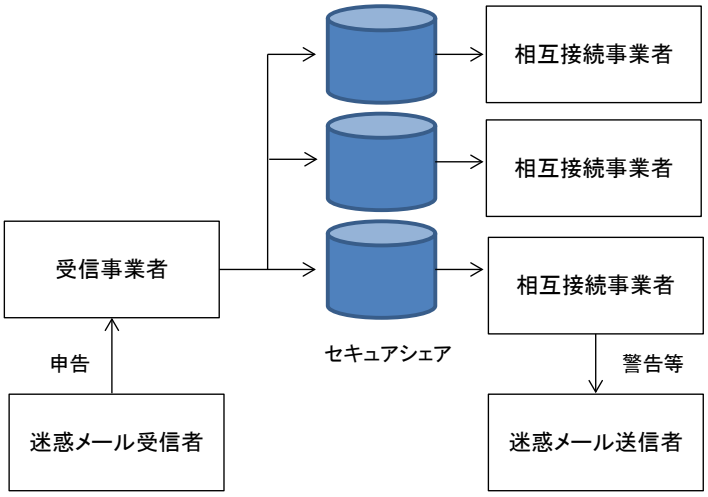
フィルタリング会社により迷惑メール判定された SMS を警告表示もしくは迷惑フォルダに自動振り分け。

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。

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。

図表 3-1　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。

第５節　RCS(＋メッセージ)を利用した迷惑メール受信防止対策の提供状況

移動系ISP3社（A社、B社、C社）は、携帯電話番号だけでメッセージがやり取りできるSMS（ショートメッセージサービス）の機能を進化させた新サービス「＋メッセージ（プラスメッセージ）」を、2018年5月に開始した。現在、3社のスマートフォン、タブレットで利用できる。

「＋メッセージ」は、GSMAで世界的に標準化されているRCS（Rich Communication Services）に準拠したサービスで、3社間であれば、文字数（最大全角2,730文字）を気にすることなく、携帯電話番号宛てにチャット形式でメッセージや写真、動画を送受信可能。また、コミュニケーションを豊かにする専用スタンプや、複数人で同時にメッセージをやり取りできるグループメッセージを楽しむこともできる。

本サービスの受信対策として、以下の機能を提供中。
（３社同一仕様のため、A社、B社、C社共通）

(1) ブロック機能

指定した連絡先からのメッセージを迷惑メッセージボックスで受信し、通知表示、通知音（バイブ含む）鳴動などを起こさず、メッセージ一覧にも表示しないことができる。

(2) 未登録連絡先フィルタ機能

電話帳登録済みと未登録の連絡先でメッセージを振り分けて表示することができる。未登録の連絡先からのメッセージは、通知表示、通知音（バイブ含む）鳴動などを起こさずに受信する。

(3) 迷惑メッセージ申告機能

迷惑メッセージを本サービス提供事業者に申告することができる。

ア　申告受信事業者の対応

（ア）　アプリの機能により申告を受け付ける。（申告者から取得する情報は、受信した本文、送信電話番号等）

（イ）　同一の電話番号から送信された迷惑メッセージについて、一定期間内に複数の受信者から申告があった場合、自網から送信されたメッセージに関する申告情報を判別する。

（ウ）　自網から送信されたメッセージに関する申告情報であると判定されなかったものを、本サービスを提供する他事業者に提供する。

イ　情報提供を受けたサービス提供事業者の対応

（ア）　申告受信事業者から提供された申告情報（受信した本文、送信電話番号等）について、自網から送信されたメッセージに関する申告情報を判別する。

（イ）　自網から送信されたメッセージに関する申告件数や内容に応じて、当該メッセージ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の対策状況

第１節　迷惑メール送信防止対策の導入状況

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、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は国別で異なっており、最も厳しい規制が適用されている国で 33 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) Ｆ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。

(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%を破棄することが可能。

(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　Ｆ社

すべてのメール送信について、SMTP(S)-AUTH による送信者認証を実施する。

イ　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。

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（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）から推奨されている技術。

※　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。

ウ　Ｑ社

2016 年（平成 28 年）７月から、短時間に大量のアカウントでのアクセスが確認された IP に対して、送信サーバの利用を一時規制する仕組みを導入している。

なお、誤判定を考慮し、規制対象外とする送信元 IP/ホストのリスト運用も併せて実施している。

(3) 送信ドメイン認証登録等

ア　Ｄ社

・SPF 登録

2005 年（平成 17 年）12 月から実施。

・DKIM 署名

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。

・DMARC 登録

法人向けサービスにおいて 2014 年（平成 26 年）8 月から、
個人向けサービスにおいて 2014 年（平成 26 年）11 月から実施。

イ　Ｅ社

・SPF 登録

2008 年（平成 20 年）１月から実施。

・DKIM 署名

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。

・DMARC 登録
2014 年（平成 26 年）7 月から実施。

カ　Ｊ社
・SPF 登録
2006 年（平成 18 年）3 月から実施。

キ　Ｋ社
・SPF 登録
2011 年（平成 23 年）10 月から実施。

・DKIM 署名
2011 年（平成 23 年）9 月から実施。

・DMARC 登録
2014 年（平成 26 年）10 月から実施。

ク　Ｌ社
・SPF 登録
2005 年（平成 17 年）12 月から実施。

ケ　Ｍ社
・SPF 登録
2005 年（平成 17 年）5 月から実施。

・DKIM 署名
2005 年（平成 17 年）5 月から実施。

・DMARC 登録
2014 年（平成 26 年）8 月から実施。

コ　Ｎ社
・SPF 登録
2006 年（平成 18 年）5 月から実施。

サ　Ｏ社

・SPF 登録

2005 年（平成 17 年）11 月から実施。

・DKIM 署名

2007 年（平成 19 年）9 月から実施。

・DMARC 登録

2015 年（平成 27 年）9 月から実施

シ　Ｐ社

・SPF 登録

2006 年（平成 18 年）11 月から実施。

ス　Ｑ社

・SPF 登録

2006 年（平成 18 年）12 月から実施。

・DKIM 署名

2005 年（平成 17 年）7 月から実施。

・DMARC 登録

2019 年（平成 31 年）3 月から実施。

セ　Ｒ社

・SPF 登録

2006 年（平成 18 年）10 月から実施。

ソ　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。

・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。

(6) 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。

(7) 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。

(8) 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。

(9) 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。

(10) 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。

(11) 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。

(12) 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）7 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）。

(13) 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。

(14) 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。

(15) 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
(1) 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	DMARC	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）	H26/08（企業向） H26/11（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	-	H26/07	H18/02	H18/12	H18/02
J社	H18/03	-	-	H17/12	H18/03	H17/11
K社	H23/10	H23/09	H26/10	H18/06	H18/06	H18/03
L社	H17/12	-	-	H18/03	H18/12	H18/08
M社	H17/05	H17/05	H26/08	H18/02	H18/02	H17/10
N社	H18/05	-	-	H17/09	H18/12	H18/02
O社	H17/11	H19/09	H27/09	H18/07	H18/09	H17/07
P社	H18/11	-	-	H17/01	H18/07	H18/06
Q社	H18/12	H17/07	H31/03	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制御

(1) 送信ドメイン認証技術を利用した判定

ア　Ｄ社

SPF、DKIM、DMARC 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、SPF、DKIM の認証結果を利用したフィルタを、2010 年（平成 22 年）12 月から、DMARC の認証結果を利用したフィルタを 2018 年(平成 30 年)4 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」「隔離する」「DMARC ポリシーに従う」などの動作を設定することができる。

イ　Ｅ社

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

また、有償オプションにて、SPF、DKIM 認証結果に応じたメールの配送制御を行うことが可能。

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 の認証を実施し、結果を、Received-SPF 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 の認証を実施し、結果を Authentication-Results ヘッダに付与している。2014 年（平成 26 年）10 月からは DMARC の検証結果の付与を開始した。

カ　Ｌ社

SFP、SenderID の認証を実施し、結果を Authentication-Results ヘッダに付与している。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　Ｎ社

自社ドメイン宛てに届いたメールについて SPF、DKIM、DMARC の認証結果をメールのヘッダ部分に挿入して配送する。

ケ　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。

コ　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。

2020 年（令和 2 年）3 月からは DMARC の検証結果の付与を開始した。

(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　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。

エ　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。

オ　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

（ア）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。

（イ）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。

（ウ）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

（ア）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。

（イ）海外の IP アドレスからの POP / SMTP / IMAP の利用を禁止するオプションを、2017 年（平成 29 年）1 月より提供。

（海外からのメールソフトの利用を制限）

（ウ）POP / SMTP / IMAP の利用を無効にするオプションを、2018 年（平成 30 年）8 月より提供。

（環境に関係なくメールソフトの利用を制限）

(4) IP25B を利用した判定

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

メールヘッダおよびメール本文中に指定した任意のキーワードが含まれるメール、また、指定した差出人、宛先アドレス/ドメインのメールに対して「拒否する」「隔離する」などの動作を設定することができる。キーワードは 200 件、差出人、宛先はそれぞれ 1,000 件登録できる

（イ）メール容量

100M バイトまでの指定した容量以上のメールに対して「受け取る」「隔離する」などの動作を設定することができる。

（ウ）添付ファイル

添付ファイルの形式、ファイル名、ファイル数などを条件として、合致したメールに対して「隔離する」「添付ファイルを削除する」などの動作を設定することができる。

イ　Ｅ社

（ア）ブラックワード

受信許可メールアドレス/ドメイン/IP アドレス及び受信拒否メールアドレス/ドメイン/IP アドレスとしてそれぞれ最大 300 件登録できる。また、管理者用と利用者用それぞれ登録することができる。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/IP 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）で指定ができる。件名（Subject:）は部分一致（～を含む）により指定ができる。

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

（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:）、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。

カ　Ｊ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:）、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。

キ　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。

ク　Ｌ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:）について最大 500 件登録できる。

ケ　Ｍ社

（ア）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。

コ　Ｎ社

（ア）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 100 件、任意のキーワードを設定できる。

サ　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。

シ　Ｐ社

（ア）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。

ス　Ｑ社

（ア）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 件設定できる。

セ　Ｒ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:）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。

ソ　Ｓ社

（ア）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

ア　Ｄ社

ヒューリスティックフィルタ、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する。また、迷惑メール判定の内容により迷惑メール度高/中の二種類に分類され、それぞれ「拒否する」「隔離する」「件名の先頭に指定した文字列を付与する」などの動作が設定できる。

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。また、件名の先頭に[spam]といった文字を付記することもできる。

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]を付記する事も可能。

（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。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。

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

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。

サ　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メールから申告できる方法が提供されている。

（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。

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フィルタ、及びシグネチャ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。

ソ　Ｓ社

ヒューリスティックフィルタ、及び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/ドメインを最大 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/ドメイン/IP アドレスを最大 300 件登録できる。また、管理者用と利用者用それぞれ登録することができる。

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可能。受信拒否と併せて最大 300 件まで設定できる。

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　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。

キ　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。

ク　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。

ケ　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。

コ　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。

サ　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。

シ　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。

ス　Ｒ社

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。

セ　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

送信ドメイン認証、迷惑メール、添付ファイル、キーワードなど各種フィルタ条件に合致したメールに対して、フィルタ毎に動作を設定することができる。動作には「受け取る」「拒否する」「隔離する」「破棄する」があり、「受け取る」「隔離する」場合は、任意のヘッダ情報を付加する、件名の先頭に任意の文字列を付加する、添付ファイルを削除といった処理を設定することもできる。

隔離されたメールは14日間保存され、利用者から閲覧ができる。

(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]の識別子を付記することができる。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) 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。

(7) 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、アとイのどちらかを選択可能。

（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）。

(8) 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。または、案内のメールを送信してメールを破棄する。(案内メールには、元のメールの送信者アドレス(From;)、及び件名 (Subject:)、受信日時(Date:)が記載される)

ア 破棄したメールの送信者アドレス (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 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。

(9) 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。

(10) Ｎ社

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、迷惑メールフォルダに隔離される。

(11) 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。

(12) 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。

(13) 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。

(14) 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。

(15) 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）主要な固定系 ISP が提供する迷惑メール受信対策一覧(1/2)

	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							
		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	ポリシーに基づく処理の設定	レポートの送信設定
D社	○	○	○	○	○	○	○	○	
E社	○	○	○	○	○				
F社		○							
G社									
H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(2/2)

	②送信元情報参照による受信制限			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
	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	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				○				○		○
J社	○			○				○		○
K社			○	○	○				○	○
L社				○					○	○
M社		○	○	○	○			○	○	○
N社				○					○	
O社		○		○	○		○	○		○
P社	○			○	○			○	○	○
Q社	○	○	○	○			○	○	○	○
R社				○				○	○	○
S社				○				○	○	○