## Messaging, Malware and Mobile Anti-Abuse Working Group

# M³AAWG 送信者のベストコモンプラクティス

**第 3.0 版**

2015 年 2 月更新

**注意:**本文書は、メールアドレス収集とデータの透明化の両プロセスに重点を置いて、2011 年 10 月に発行されたバージョン 2.0 を大幅に改定したものです。本文書は、前バージョンに含まれる MAAWG Sender Best Communications Practices および Executive Summary の両文書を置き換えるものです。いずれの文書も、バージョン 3.0 に組み込まれます。

**要約**

本文書は、運用上の技術および実践的なポリシーの側面に焦点を当てながら、商用の電子メッセージの送信に関する現行のベストコモンプラクティスの概要を説明します。本文書は、ESP（電子メールサービスプロバイダー）および大規模な送信者で働く配信やコンプライアンスの専門家から、本文書に記載するプラクティスの承認および展開に関わるマーケティングや管理者までを対象読者としています。本文書は、電子メッセージの送信者による受信者メールアドレスの収集、利用および削除に関するプラクティスを取り扱っています。必要に応じて、本文書は所定のテーマに関して、詳細な情報を提供する他の文書へリンクをしています。

本文書の内容は、電子メール通信に限定されてはいますが、M³AAWG Senders Committee は、テキストメッセージ（つまり、SMS）、インスタントメッセージ（IM）、ソーシャルネットワークに基づくメッセージなどの他の形式の電子メッセージ通信や、他のプラットフォームにも順次拡張していく予定です。ただし、本文書に含まれる多くのプラクティスは、他の種類のメッセージングに対しても直接適用することが可能です。

目次

## 1. 序論

M³AAWG Senders Committee は、メッセージの不正使用を減らすという M³AAWG の使命を支援するために、電子メッセージ通信に関するベストコモンプラクティスを開発しました。これらのプラクティスの目標は、正規のメッセージングを維持する送信者の透明化を推進かつ強化し、個別の受信者とメールボックスプロバイダーが正規のメッセージングと不正のメッセージングをさらに簡単に区別することができるようにすることです。これにより、メッセージングの不正使用に対抗するに当たり、メールボックスプロバイダーが、手持ちのリソースをさらに効率的に利用し、エンドユーザーをさらに保護することが可能となります。

M³AAWG は、オプトイン加入者が明確にはっきりとした検証可能な情報に基づいて同意することが、メッセージ送信を許可するベストプラクティスであると、断言します。本文書では、オプトイン加入者の同意と、他のベストプラクティスの要点を述べます。ただし、許容されるメッセージング交換のベストプラクティスは、メッセージングおよびメールボックスプロバイダーの利用目的に関する要件（AUP）や、適用される国家政府および地方政府の法令および規制の各要件（付録 B を参照）に少なくとも準拠したものでなければなりません。送信者は、業界規制措置を回避し、新しい規制措置の必要性が生じるリスクを回避するために、それらの要件には準拠しなければなりません。また、送信者は関連する業界団体への参加や、他の事業者団体や電子メール認定プロバイダーが規定したような関連自主規制のイニシアチブの支持などを検討するべきです。

本文書は、業界のベストコモンプラクティス（BCP）の要点を述べています。受信側ネットワークや電子メッセージの送信者の一部は、ネットワークインフラの複雑性、公共政策への配慮、あるいはネットワークプラットフォームのスケーラビリティーの理由から、本文書に記載するプラクティスのすべてを完全に実装することはできない場合もありますが、本文書に記載したプロセスは業界内では基本的な合意を表しています。

## 2. メールアドレス収集の意図の透明化

次節では、バルク／商用メッセージングおよび取引メッセージングの電子メールアドレスの収集および利用を取り巻くベストプラクティスについて要点を述べます。ここでは、送信者ブランドと電子メールサービスプロバイダーの双方は、メッセージの最終受信者に対して透明でなければならないという義務に重点を置いています。本節では、受信者の登録（つまり、オプトイン）、配信解除の方法および個人データの取り扱いを取り巻くプラクティスに関して記載します。

### 2.1 オプトイン、登録、電子メールアドレス収集

電子メールや他の電子メッセージ、具体的に言えばバルクメッセージやマーケティング関連メッセージの送信に関する基本的なルールは、送信者は、電子メールアドレスをメッセージ送信する前、あるいは継続して繰り返される通信に受信者を追加する前に、受信者の明確な同意を得なければないということです。受信者は、メッセージに対して積極的にサインアップした場合、そのメッセージが迷惑または不正であると報告する可能性は低くなります。

オプトイン登録には３つのレベルが存在します。各レベルは、下位のレベルが前提となり、レベルが上がるごとに、送信者がオプトイン登録したアドレスにメッセージを送信するのに受信者の明確な同意を得ていることが保証される点で効果が高まります。

1. シングルオプトイン

a. エンドユーザーは電子メールアドレスを送信者に提供します。

b. エンドユーザーは、オプトイン登録に関して指定の電子メッセージの受信を開始します。

c. 登録完了の通知は送信しません。

d. 同意の確認は行いません。

**2. 通知付きシングルオプトイン（良）**

a. エンドユーザーは電子メールアドレスを送信者に提供します。

b. 通知メッセージやウェルカムメッセージが受信者に送信され、受信者がメッセージを受信することができるようになったことを通知します。（詳細は以下のレベル 2 参照のこと。）

c. 同意の確認は行いません。

**3. 確認済みオプトイン（最良）**

a. エンドユーザーは電子メールアドレスを送信者に提供します。

b. 確認メッセージが受信者に送信され、登録を完了するためには、リンクのクリックや電子メールへの返信などの操作を行わなければならないことが通知されます。（詳細は以下のレベル 3 参照のこと。）

c. 受信者は、登録メッセージが送信される前に、リンクをクリックするか、あるいは電子メールに返信するなどの指定された操作を行い、以降のメッセージ受信に同意することを確認しなければなりません。

以下に示す内容は、上記の各レベルについてさらに詳細に記載したものです。これらのガイドラインは、オンラインとオフラインの両方のメールアドレス収集の手法に適用することが可能です。各レベルは、下位レベルが前提となります。例えば、レベル 1 に含まれる手順はすべて、上位のレベル 2 にも含まれますが、ここでは重複したステップの記載は省略します。

## *レベル 1 - シングルオプトイン*

シングルオプトインは、細心の注意を払って利用するべきです。それは、未確認のアドレスがメーリングリストに追加されることが可能であるからです。つまり、誤字や明白な偽造が検査されずに追加されてしまう可能性があり、苦情を受けたり、宛先不明のメッセージが戻ってきたり、最終的には送信者のレピュテーションが下がることになります。

1. 受信者は、メールアドレスの収集時に意識して同意しなければなりません。
2. 同意は、明確にはっきりとしている必要があります。受信者の電子メールアドレスへメッセージを送信する意図を示す通知は、フォントを小さくしたり、理解しにくい法律用語を使用したり、別のページに表示するなどして受信者の目から隠すべきではありません。
3. サインアップ通知は、受信者が属するリストの特定のタイプを明確に提示するべきです。可能であれば、送信者は、受信者が登録したいリストや、登録をしたくないリストを指定できるようにするべきです。（例えば、エンドユーザーは、関連製品ではなく、購入製品に関する更新通知の受信を望むかもしれません。）受信者が、受信メッセージを抑制すればするほど、これらのメッセージが不正であると報告する可能性は低くなります。
4. 送信者は、受信者に対して配信頻度の見込みや、配信の種類を通知し、受信者がこれらの各設定に関して選択できるようにするべきです。メッセージの配信頻度が予期せずに増加すれば、多くの場合、不正使用の苦情が増えることになります。
5. 電子メールアドレスは、サインアップ時に受信者に開示した目的についてのみ利用するべきです。メールアドレス収集後に、内容が異なるニュースレターを追加するなどの第２の目的が作成された場合、受信者には、この第２の目的に対してオプトインとするか否かを選択する機会を与えられるべきです。第２の目的に対しては、デフォルトでオプトインとしてはならなりません。メッ

セージが第２の目的に該当するか否かの判断は、受信者の視点から考慮されるべきです。受信者は、許可を与えたと思わなければ、第２の目的のメッセージは不要であるか、あるいは不正であると報告する可能性が増えます。さらに、第１の目的の範囲を超えてさらに通信を送信する前に、この種類の許可を得ることが法的に求められる場合もあります。

6. 送信者は、受信する電子メールの視覚的例を含めても構いません。電子メールメッセージが受信者の電子メールボックスに到着した際に、受信者は、視覚的例により要求した通信の電子メールメッセージであると認識できるようになり、メッセージングの不正使用であると報告する可能性は低くなります。

7. メールアドレス収集にあたり、送信者は、IP アドレス、メールアドレス収集日および収集を行ったウェブサイトやイベントなどのサインアップに関して、他にどのような種類のデータを保持するか検討するべきです。大企業は、当初どの部署がどのような方法でメールアドレス収集を行ったかに関しても、記録していくべきです。この情報は、個人、ISP（インターネットサービスプロバイダー）、RBL（リアルタイムブラックホールリスト）のオペレータおよび規制者との同意を示す必要が生じた場合に、簡単にアクセスできるようにするべきです。送信者は、個人識別情報(PII)データの保存を取り巻く法令についても考慮しなければなりません。

*レベル 2 – 通知付きシングルオプトイン（良）*

8. エンドユーザーが自身のアドレスをリストに提出後すぐに、もしくはできるだけすぐ（２４時間以内）に、確認メッセージを送信するべきです（上記 2.1、2 参照）。確認メッセージは、可能な限り、以下のガイドラインに準拠するべきです。

   a. 確認メッセージは、リストに提出されたアドレスやエンドユーザーが提供したその他の情報を含むべきです。

   b. 確認メッセージは、メール送信の頻度や内容の種類についての通知を含むべきです。

   c. 確認メッセージは、受信者が、必要に応じて自分のアドレス帳やホワイトリストに追加できるように、登録後に受信するメッセージと同じ「from」アドレスを利用するべきです。

   d. 可能であれば、確認メッセージを送信するサーバーは、通常のバルク送信 IP とは別のセグメントに配置するべきです。

*レベル 3 - 確認済みオプトイン（最良）*

9. 確認済みオプトイン（「ダブルオプトイン」や「閉ループ登録」とも呼ばれる）は、最高水準のオプトインベストプラクティスです。確認メッセージの受信者は、リストに追加されるためには、積極的に行動を取る必要があります。これによって、誤字や悪意をもって提出されたアドレスが、運用中のメーリングリストに追加されないようにすることができます。可能な場合には、以下のガイドラインに従うべきです。

   a. アドレス提出時に、電子メールをチェックして、確認メッセージに対して行動を取る必要があることを、エンドユーザーに通知します。

   b. 確認メールには、メッセージングの不正使用として識別されたり、フィルターされたりしないように、広告が入らない簡単なものにするべきです。

### 2.2 暗黙の同意

暗黙の同意は、ある個人が組織とやりとりすることによって許可が得られたと推測される場合に収集されます。電子メールメッセージングにおける暗黙の同意の一般的な例は、顧客が販売時に電子メールアドレスを提供した結果として、継続するメール配信に追加されることをユーザーに通知しない場合です。この場合、業者は、顧客がマーケティングリストに追加されることを求めていると推測します。これは多くの場合、リストを増やす方法としては認められますが、すべての送信者には有効ではなく、不正使用の苦情の原因となる可能性があり、ベストプラクティスとは言えません。送信者がこの手法を利用している場合、顧客の苦情に注意深く耳を傾け、リストの該当部分を開いてクリックし、変更をする必要があるか否かを

判断させるべきです。選択肢としては、メールアドレス収集時に明確な同意を得るためにチェックボックスを目立つ場所に追加することであり、この方法は上に記載したようにベストプラクティスとして推奨されます。送信者が暗黙の同意によってアドレスを収集することを選択した場合は、さらにマーケティングメッセージを送信する前に「許可パス」または「確認」をキャンペーンすることにより明確な同意を得るように努力することがベストプラクティスです。

留意すべきは、どの登録方法、あるいはどの登録方法を組み合わせて利用するにしろ、個別のアドレスがそれぞれどのようにしてリストに追加されるようになったか記録していくことが重要です。この記録には、発信元 IP やサインアップ時の IP の捕捉、タイムスタンプ、開示言語のスクリーンキャプチャーおよび登録時に実施されるすべての関連プライバシーポリシーを含みます。これは将来、リストの特定の部分に発生した問題の解決に有用となります。

### 2.3 Email Append（M³AAWG の意見表明）

Email appending のプラクティスとは、e-pending としても知られていますが、送信者が、有効な顧客レコードを電子メールアドレスと照合しようと試みるデータ照合を実施することを言います。電子メールアドレスの所有者は、明確にアドレスを提供しておらず、このアドレスで送信者からメッセージを受信することにも同意していません。

Email Appending は、M³AAWG の本質的価値に対して明らかに違反しています。Email Appending が不正使用され、スパムの苦情やメッセージの拒否が大量に発生することになるのには、多くの理由が存在します。Email Appending によって、苦情以外にも、個人情報保護やスパム対策の法令に違反する重大なリスクが生じます。Email Appending に対する M³AAWG の立場については、その全文が下記 URL にて公開されています。http://www.maawg.org/sites/maawg/files/news/MAAWG_Epending_Position_2011-09.pdf

### 2.4 登録削除

1. 送信者は、登録削除処理をある程度可能な限り簡単かつ明確に利用できるようにしなければなりません。
2. 送信者は、適用される法令すべてを継続的に順守するために、さらには受信者に尊敬の念の表すように、すべての登録削除要求を遅滞することなく処理しなければなりません。
3. 送信者は、登録削除処理時に自身が登録削除要求を処理する実際のタイムフレームや、登録削除する受信者のリストや通信の種類について詳細を明らかにし、期待を設定するべきです。受信者をリストから削除するタイムフレームが長くなると、ユーザーは継続して送信される電子メールを不正であると考え、苦情となる可能性が高くなることに留意してください。
4. 送信者は、アウトバウンド電子メールに含まれる From アドレスおよび Reply-to アドレスから、電子メールベースの登録削除要求を処理する機能を備えるべきです。
5. 登録削除のリンクは、リストからの登録削除が成功するために必要な情報をすべて含むべきです。この情報には、以下の項目が含まれます。
    a. 加入者 ID
    b. 複数リストのオプションがある場合は登録削除の対象となるリスト
    c. サードパーティーが悪意をもってユーザーの誰かを登録削除することを防ぐ必要がある場合は、ユーザー単位認証トークン。
6. 送信者は、RFC 2369 に記載されるように各メッセージのヘッダ内の List-Unsubscribe 機能を採用するべきです。
    a. 「Mailto」による List-unsubscribe は、特定の受信者にのみ一致するアウトバンドメッセージに含まれる暗号化された電子メールアドレスを参照します。その特殊な電子メールアドレスで

受信した電子メールメッセージは、登録したアドレス以外からメッセージが送信されたとしても、その受信者の代わりに提出された登録削除要求とすることができます。

b. 「URL」による List-unsubscribe によって、送信側プラットフォームが既に提供している登録削除機能へのリンクを提供することもできます。このリンクは、ほとんどのバルクメールメッセージに通常含まれる登録削除のリンクと同じにしても構いません。登録削除機能の悪意ある不正使用を防止し、消費者が登録削除要求を最大限使いやすくするために、実際に使用中の登録削除のリンクに必要な個人情報を暗号化することを推奨します。

7. 送信者は、具体的なリストオプションがあるプリファレンスセンターを表示できない場合、登録削除の処理のポリシーを決めるべきです。これは、業務の種類によって違いはあるが、登録削除が有効であるのはすべてのメールなのか、あるいは個々のリストなのかを決めることが重要です。すべてのメールから受信者を削除することをデフォルトにすることが、ベストプラクティスです。

8. 送信者は、ワンクリックでオンライン登録削除ウェブページを表示するハイパーリンクには、画像ではなく読みやすいテキスト文を併記するべきです。

9. 送信者は、また、郵送先に登録削除要求を送付する機能や、登録削除の電話を受けるなどの登録削除メカニズムがオフラインで利用できるように検討するべきです。そのようなプロセスは、個人が負担する費用が安いか、あるいは無料であることを確実にするために、ローカルな（国内）住所や、フリーダイヤルを利用するべきです。

10. 複数の登録オプションを含むハイパーリンクを付けてオンライン登録のプリファレンスセンターを加入者に表示する場合、デフォルトの登録削除オプションは、ユーザーが現在登録しているリストが予め選択されているべきです。

11. プロバイダーが提供された新規登録を利用可能にした場合、その新規の選択項目はデフォルトではチェックが外した状態で加入者に表示するべきです。

12. 加入者は、プリファレンスセンターにログインすることなく、さらにはいかなる形でもセキュリティの情報を求められることなく、登録削除が可能でなければなりません。プリファレンスセンターのエクスペリエンスを提供することを希望する送信者は、加入者にログインフォームを提供して、他の登録を管理することができるようにしてもよいです。ただし、受信者は、セキュリティエリアの外側からでも特定のリストに対して登録削除が可能でなければなりません。

13. 送信者は、受信者の電子メールアドレスをメッセージ本文に含めて、受信者が特定のリストの登録に利用した電子メールアドレスを思い出せるようにすることを**強く推奨**します。これは、一つの集約アカウントや集約メールボックスに転送される複数の電子メールアドレスを利用する受信者にとっては、特に有用です。

### 2.5 データセキュリティ

加入者の電子メールアドレスや他の個人情報（(PII）に関するデータの保存と管理に従事するESPおよび他の送信者は、自身の環境およびアプリケーションの安全性を実現するために、業界標準のベストプラクティスを活用する包括的なセキュリティプログラムを継続することを強く推奨します。推奨に関する詳細は、本文書の範囲外ですが、さらに詳しく知りたい場合の出発点として、オープンウェブアプリケーションセキュリティプロジェクト（OWASP - https://www.owasp.org）や SANS（https://www.sans.org）サイバーセキュリティやデータセキュリティのリスクおよび勧告に関する豊富な情報が提供されています。オンライントラストアライアンス（OTA -https://otalliance.org）業界団体は、興味のある読者に対して「Data Protection and Breach Readiness Guide」を公開しています。さらに、業界やアプリケーションによっては、包括的なセキュリティプログラムに適した基礎としてAccess Control, Communications and Operations Management, and Information Security Incident Management codeに含まれるISO/IEC 27002:2013 code（http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54533）の推奨に準拠することが参考になるかもしれません。

M³AAWGは、データの収集および保存に関するプロセスを開発する場合、セキュリティを第一に考慮する

ことを**強く推奨**します。犯罪者が銀行強盗を働くのは「そこに現金があるから」であって、サイバー犯罪者が、電子メールサービスプロバイダーや他のPIIおよび機密データのオンライン管理者を、不正使用の目的で電子メールアドレスデータを盗む標的とみなすことはないと思い込むことは、考えが甘いと言わざるをえません。同じように、送信者は、サービスやソフトウェアアプリケーションは電子メールアドレスのみを保存するので、サイバー犯罪者の標的になりそうにないと思い込むべきではありません。保存されたデータは、所有者(つまり、加入者)と犯罪者の双方にとって価値があるのです。メッセージングエコシステムのすべてのメンバーが、データは適正に保管されており、犯罪者の手に落ちないことを保証することが最も重要です。さらに米国の連邦取引委員会は、消費者を保護するためのベストプラクティスに関して詳細な報告書を発行しています。（http://ftc.gov/opa/2012/03/privacyframework.shtma）.

## 3. データの透明性

次節では、送信者が、受信側サーバーに対してさらに透明性を高めるために、業務に組み込むべきさまざまなプラクティスの概要を述べます。透明性は、電子メール業界において、信頼を確立するための基本原則であり、送信側サーバーの IP およびドメインの双方に対して、さらには、メッセージ本文に含まれるすべてのリンク対しても適用されます。すべての情報が公になっている場合、送信者は、顧客の良い行いと悪い行いの両方に対して責任を負うことができます。後述するメカニズムを通して送信者が自己紹介をする場合、受信者はさらに親身になって、送信者との間で問題のある顧客についてやりとりすることができます。透明性によって、送信者は信頼を築くことができ、また、所望する電子メールを受信箱に配信する一方でスパムを締め出す能力を備えることができます。

### 3.1 WHOIS 情報

WHOIS プロトコルは、システム管理者が IP アドレス割当てやドメイン名の管理者に関する連絡先情報を取得するための方法です。大量の電子メールに対する責任を主張するドメインの正確な WHOIS 情報は、重要な透明性の要素です。

送信者は、不正使用に関する問題の改善を支援するために、正確な問い合わせ先を受信者などに提供するために、正確かつ最新の WHOIS レコードを維持しなければなりません。本文書は、WHOIS あるいは rWHOIS に基づいて実施する必要があります。WHOIS／rWHOIS に加え、他の形式による同等の情報も許容されます。サブネットマスクが、IPv4 の場合は/29 以上、IPv6 の場合は/56 以上のサブブロックを IP アドレスに割り当てる場合、ARIN（American Registry for Internet Numbers）や他の RIR（地域インターネットレジストリ）ポリシーを順守して、正確かつ完全に記録しなければなりません。例えば、次の情報を参照してください。https://www.arin.net/resources/request/reassignments.html

特に、秘匿ドメインおよびプロキシドメインの登録 WHOIS データを公開することによって、上記のプロセスが不要となり、透明性の根本原理が簡略化されます。ただし、メッセージングネットワークを不正使用しようとしないエンティティが、曖昧あるいは不正確な WHOIS データを意図的に利用することに関しては、説得力のあるビジネス上の適用例は存在しません。

### 3.2 電子メール認証

認証は、メッセージの送信者を特定することにより透明化を支援しますが、一方でなりすましやアドレス偽造の削減や排除にも貢献します。送信者を簡単かつ正確に識別することができれば、受信者は、メール送受信履歴や認証済みのドメインのレピュテーションに基づいて判断することができます。認証はまた、メールを認証する受信側ドメインが偽装を検出することになるので、ブランドの保護を強化することになります。送信者は、インフラやメール設定に基づいて、以下の認証メカニズムの一部または全部を採用する選択をすることもできます。

認証には、以下の４つの形式があります。

1. SPF（Sender Policy Framework）は、return-path（マシン名）および HELO ドメインに対して送信側 IP を認証します。
2. Sender ID は、「責任を持つはずのアドレス（purported responsible address）」、つまり PRA（ただし、この技法は現在あまり利用されていない）に対して送信側 IP を認証します。
3. DKIM（DomainKeys Identified Mail）は、デジタル暗号化署名を利用して、ヘッダ内の特定ドメインに対して認証を行います。
4. DMARC（Domain-based Message Authentication, Reporting & Conformance）は、受信者が未認証の電子メールをどのように取り扱って欲しいかに関するコントロールを電子メールの送信者に与えます。DMARC は、送信者に対して、「From」行に送信者のドメインを含む認証済みおよび未認証の電子メールの送信元について可視性を提供し、また SPF および DKIM の認証に失敗するメッセージに対するポリシーを設定する機能を提供します。受信側 ISP は、DMARC ポリシーを利用して、なりすましメールやフィッシングメールを効率よく処理することができます。

認証の背景についての詳細については、以下のリンクから 2015 年 2 月に更新された M3AAWG 文書「Trust in Email Begins with Authentication」を参照することができます。
https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Email_Authentication_Update-2015.pdf

M³AAWG DMARC トレーニングシリーズのビデオは、DMARC 専門家メンバーによって作成されており、このビデオは DMARC 技術の利用に関する広い範囲をカバーする講座を提供しています。
http://www.maawg.org/activities/training/dmarc-training-series

### 3.3 IP の技術的詳細

下記のIPの技術的詳細は、もっぱらIPv4について記述したものです。IPv6に関する追加情報は、基準が明確に確立してから、追加される予定です。

下記ガイドラインの目的は、オーナーシップを透明化し、レピュテーション／フィルタリングを判断するシステムに対する送信側メールサーバーの責任を明確にすることです。これらのガイドラインは、苦情や問題を調査するシステム管理者にも有益な環境を提供します。

1. フォワード DNS
   a. ドメイン名には、責任のある当事者のドメインを明確に識別する名前を選択しなければなりません。IPアドレスが共有される場合はプロバイダー／ESPであり、専有IPの場合は通常、顧客／広告主です。

      ドメイン名が顧客／広告主に属する後者の場合、フォワードDNSの実装は、顧客／広告主のドメイン管理者の責任であることに注意してください。

   b. また、ドメイン名はマシンがサーバーであって、汎用のプールスペースではないことを明確に示すものでなければなりません。

      例：「server03.espname.com」であって、「pool-dhcp-456.espname.com」ではありません。

   c. 共有IPの場合は特に、同一のIPアドレスを指すドメイン名が複数存在する可能がありますが、上記（1a）で選択された名前が「プライマリ名」であるとみなされなければなりません。

   d. 専有IPの場合を除き、エンドユーザーへの電子メール送信を目的としたESP／広告主に属するすべてのメールサーバーは、同じドメイン名あるいは「ドメイン登録レベル」の少数のドメイン名を利用しなければならず、さらに必要に応じて、区別するためにサブドメインを使用しなければなりません。目標は、一つのエンティティまたは主なエンティティの配下の複数のサブエンティティとして、ドメイン名を明確に特定できる状態にしておくことです。

例：espname01.comやespname02.comは使用しません。その代わりに、server1.espname.comやserver2.espname.com等を使用します。

2. 逆引き DNS
   a. 送信側サーバーのIPアドレスは、逆引きDNS（PTRあるいはIN-ADDRとも呼ばれる）が設定されている必要があります。
   b. IPアドレス毎に、一つの逆引きDNS名のみが設定されていなければなりません。
   c. 逆引きDNS名は、上記（1a）により選択したプライマリ名に一致しなければなりません。

3. HELO名（電子メール送信時に、HELO／EHLOコマンド内でサーバーが提供する名前。RFC5321を参照）。これらは多くの場合、メールサーバーのフルホスト名に一致します。

   **注意：**HELOがSPF認証に関与することを、本節を通じて考慮しなければなりません。

   a. HELOは解決可能なホスト名でなければなりません。括弧（[ ]）で括ったIPアドレス文字は許容されません。
   b. 専有（非共有) IP環境においては、HELOはプライマリフォワードDNS名に一致しなければなりません。
   c. 共有IP環境で、あるいはIPが複数のサーバーにNATされる場合、発行されるHELO名は、少なくともプライマリフォワードDNS名の「ドメイン登録レベル」のプライマリ名に一致しなければなりません。HELO名は、全体の名前に完全一致しても構いません。

      **注意：**HELO名は、NATに関する電子メールの問題を診断する（つまり、LAN上の責任のあるサーバーを識別する）のに有用な場合があり、「NAT」の背後に配置された共有環境の各メールシステムや顧客は、ドメイン登録レベル名のサブドメインである自身のHELO名を有することが推奨されます。

      **例：**いずれか適切な方です。

      「server01.espname.com」、「server02.espname.com」、...
      「server01.brand1.espname.com」、「server01.brand2.espname.com」、 ...

### 3.4 共有 IP と専有 IP

ESP や同様のサービスを利用して、ある程度の量のメールを頻繁に送信する組織は、アウトバウンドのメールに関して、共有 IP または専有 IP の環境にアカウントを設定または選択をすることができます。この両環境には、重要な利点と欠点があります。ESP とその顧客は、どちらの環境が最も適しているか、さらには設定をどうすべきかを判断する場合に、多くの要因を評価するべきです。

***IP 環境の定義***

専有 IP 環境は、特定のエンティティが独占的に利用し、その環境を通過するアウトバンドメールに関して責任がある環境です。専有環境は、1 つ以上の IP から構成されていてもよいが、その利用に関しては、ただ一つのエンティティが責任を負うことができます。

共有 IP 環境では、1 つ以上のエンティティが、任意の IP 環境に割り当てられます。共有環境は、環境内部に設定したエンティティ間で共有される単一の IP または IP のプールから構成されます。

*「エンティティ」に関する一言*

IP 環境を設定するために、さまざまな性質により独自のエンティティを定義することができます。エンティティは、一企業、企業内の一ブランド、あるいは電子メールサービスプロバイダーの一顧客の場合もあ

ります。一般に、「エンティティ」は、メッセージ送信に責任がある当事者として定義することができます。

## *正しい設定を決める*

エンティティの電子メールを送信するための環境を設定する際には、多くのさまざまな要素を考慮する必要があります。考慮すべきいくつかの重要な点については以下で記載し、一般的なガイドラインとして提供しています。

### *専有環境*

送信者や ESP が、少なくとも一時的に、専有環境の内部にエンティティを設定することを希望する特定の状況が数多く存在します。

例えば、エンティティのメールやリストの品質が未知であるか平均未満であるかもしれません。この場合、送信者や ESP は、他のエンティティからのメールを分離して、メールが引き起こす可能性のある悪評の影響から守り、メールの品質を確立し、あるいは品質の変更を追跡できるようにしたいと考えるかもしれません。

反対に、エンティティのメールやリストの品質は、標準の品質よりも優れているものだといわれているかも知れません。この場合、送信者や ESP は、他のエンティティからのメールによって引き起こされる悪評の影響の可能性からエンティティを分離したいと願うかもしれません。

さらに、送信者や ESP は、送信側 IP から発信されるメールの流量に対して統制力を発揮したいと願うかも知れません。1 つ以上のエンティティからの取引用とマーケティング用の電子メールやメールを組み合わせることは、トラフィック量にムラを生み出す可能性があります。トラフィック量が一貫していることは、その量の多寡に関係なく、IP レピュテーションの判定や、配信可能量の結果に対して不可欠な部分です。これは、大規模なプロバイダーを利用してメールをホスティングする無料のメールボックスプロバイダー、大規模なドメインおよび小規模なビジネスにメールを送信する場合に、特にあてはまります。留意すべきは、トラフィック量が一定であることは、自動化した配信判定を行うセルフホスティングの小規模なビジネスに関しては通常、有用な測定基準ではないということです。

エンティティは、メールに対して完全に責任を負い、さらにはレピュテーションや認証の理由に関して、ESP で特定されず、ESP の責任にしないことを願うかもしれません。エンティティはまた共有環境に実装したものとは異なる特有のアウトバウンド MTA 設定を必要とする可能性があります。

最後に、エンティティはさらに、承認、ホワイトリストや他の拡張配信サービスを、これらのサービスの前提条件として専有環境を必要とするサードパーティーに依頼する場合もあります。

### *共有環境*

共有環境への設定が適切となる状況は多数存在します。上に記載の通り、IP レピュテーションは、送信量の変化に敏感です。1 つ以上のエンティティからのメール量は、共有環境ではこれを統合して、共有環境からの一貫した全体の平均送信量を持続し、IP レピュテーションを確立して維持することができます。

1 つ以上のエンティティ間で環境を共有するということは、IP に関するレピュテーションもまた共有されるということを意味します。1 つの共有環境内に数多くのエンティティを設定することによって、環境内の任意の単独の送信者により行われた失敗が、全体のレピュテーションに悪い影響を与える可能性があります。

最終的には、共有環境は通常、顧客にとっては専有環境よりも安価であり、極めて小規模のビジネスに関するメールの送受信は経済的に採算が合います。

*共有環境の設定に関して考慮すべき点*

可能な限り、共有環境内のエンティティは、苦情や返送の割合などの内容と測定基準が類似しているべきです。ただしその場合でも、共有環境内に審査エンティティに対する適性評価を追加して設定することを推奨します。それは、送信およびリスト構築のプラクティスが不十分な 1 つのエンティティによって、環境が「毒され」、環境内に設定された他のエンティティが影響を受ける可能性が高くなるからです。

共有環境内の各エンティティからのメールは DKIM を利用して、固有のドメインやサブドメインにより、メールに関する責任を主張するエンティティとして認証することを推奨します。自動化した配信量を判定する場合に、共有環境から発信されるさまざまなメールの流れに対して責任がある個々のエンティティを識別する機会を ISP や受信者ドメインに提供します。これはまた、共有環境に設定した個々のエンティティが、DMARC を適用することを許容します。最終的に、DKIM は、エンティティが、以前の環境で獲得した肯定的な送信のレピュテーションから継続して利益を受け、さらには将来的に再度設定が必要になった場合も、そのレピュテーションを持ち越すことができることを可能にします。

*共有環境の設定に関するベストプラクティス*

- ESP のドメインと個々のエンティティを同時に認証する。明らかに、これは簡単に取り組むことのできる展開ではなく、この目標を達成するためには、重要なインフラを整備しなければなりません。
- 共有環境と専有環境の両方を提供する ESP は、共有環境から専有環境へのエンティティの移行に先立って、基準を確立したいと考えるかもしれません。ESP は、これらの基準を達成するために、エンティティからのメールを監視するべきです。

*専有環境の設定に関するベストプラクティス*

- 各専有 IP に関する逆引き DNS は、ESP 固有ではなく、エンティティ固有であるべきです。例えば、entity.cust.esp.com などとなります。RDNS を参照することによってエンティティが誰であるかをかなり理解しやすくするべきです。
- ESP は、専有環境に IP ウォーミングを導入するために明確に定義されたプロセスを保有するべきであり、また一貫してそれに従うべきです。
- ESP は、ホワイトリストが利用できる場合には、専有環境に設定したエンティティが、そのホワイトリストに IP を登録することを支援するべきです。
- ESP は、送信のレピュテーションを達成可能な最高点まで高め、これを維持するために、一貫して平均的な送信量を維持することを支援するべきです。

### 3.5 審査（Vetting）

顧客の代わりに大量の電子メールを送信する ESP は、最悪の顧客の最悪のプラクティスのなすがままです。すべての ESP は、顧客がメールを送信する前に、悪意のある送信者を積極的に識別する何らかの送信前審査プロセスを保有しなければならず、さらには顧客がメールを送信した後、顧客を監視する送信後審査プロセスも保有しなければなりません。優れた審査プロセスは、ESP が本当に悪意のあるスパマーから、リストの衛生についてガイダンスを単に必要とする顧客を見分けるのに有用です。顧客の審査は、良いレピュテーションを維持し、メッセージングの不正使用を抑えるのに不可欠です。顧客の審査に関する詳細なガイドについては、MAAWG Vetting Best Common Practices （BCP）文書を参照してください。

### 3.6 不正使用／フィードバックループ（FBL）の処理

ESP は、大量メールの送信者として、多くの場合、そのメールに関する苦情の受信者ともなります。通常、データ送信者が受信する苦情の最大の情報源は、メールボックスプロバイダーによって設定された自動化

されたフィードバックループ（FBL）からですが、ESP は、受信者からの苦情を不正使用に関するメールボックスに直接受信します。ESP は、FBL メッセージおよび直接送られた苦情メッセージの両方を取り扱うシステムと、これらのメッセージをどうするかを決定するプロセスを保有するべきです。苦情は、顧客が送信者の契約条件に違反しているのか、あるいは単に行儀が悪いのかを決定するための鍵となる要素の 1 つです。詳細に関しては、M³AAWG Feedback Reporting Recommendation を参照してください。不正使用の苦情の取り扱いに関して新たなベストプラクティス文書が近い将来に公開され、M³AAWG ウェブサイトから利用できるようになる予定です。

### 3.7 転送サービス

ESP は、小規模の顧客に対して、メッセージのヘッダ内に利用するために ESP の送信側ドメインに基づくアドレスを設定することを選択するかもしれません。ESP は、返信や他の応答を、顧客に転送して戻す必要があるかもしれません。この場合、ESP は、メール転送サービスを設定するべきです。メール転送サービスに関する詳細なベストプラクティスは、M³AAWG Email Forwarding Best Practices の文書内に記載されています。（http://www.maawg.org/system/files/news/MAAWG_Email_Forwarding_BP.pdf）

### 3.8 コネクション／NDR （配信不能レポート）の処理

電子メールアドレスが正しくても、送信された電子メールが、宛先の受信者に配信されるという保証はありません。電子メールが宛先に配信されない理由は数多くあり、これらの失敗が発生するメカニズムも複数存在します。多くの場合、これは宛先の受信者の関知しないところで発生します。受信側の電子メールシステムは、電子メールを拒否して、送信側システムに返送する可能性があるので、送信側システムは、これらの返送を、送信時と同じ容量と速度で受信し、処理することができなければなりません。すべての送信者は、SMTP トラフィックの送信および受信の両方のために、十分なリソースを所有していることを確認しなければなりません。

受信側が電子メールを送信者に返送する場合、通常は同期的に返送されるか、送信者が開始した SMTP のやり取りの最中に「拒否」されます。それほど頻繁ではありませんが、電子メールは、送信者の return-path アドレス（「返送」）宛てに送信された電子メールによって、非同期的に戻ってくる可能性もあります。これは、数時間後、あるいは数日後でも発生する可能があります。実際には、すべての返送の約 95%は、同期的に発生します。送信者は、返送されたメールを正しく処理するために、メールを受け取って、返送されたアドレスを識別することができなければなりません。

チャネル（同期あるいは非同期）に関わらず、電子メールは、通常は理由付きで返送されます。この理由は、数値の「ステータスコード」と「説明メッセージ」で構成されます。RFC 5321 は基本的な SMTP 応答（NDR）を規定し、RFC 3463 は拡張ステータスコードおよびそれらの意味を規定します。多くの MTA ソフトウェア、ISP およびメールボックスプロバイダーは、RFC 仕様書に準拠する正直かつ正確な「ステータスコード」を提供します。ただし、「説明メッセージ」は受信側の要求を満足するようにカスタマイズされている可能性があり、受信側によって大きく異なる可能性があります。結果として、MTA ソフトウェア、ISP およびメールボックスプロバイダーは RFC に大まかに準拠するにすぎないということになります。これは重要な点です。なぜなら、送信者は、返送された電子メールの「ステータスコード」と「説明メッセージ」の両方に基づいて、これらの返送された電子メールを処理して分類し、多くの場合報告することが求められるからです。多数の受信側が返送するメッセージを理解し、調整することは、電子メールが受け入れられて、送信者の良いレピュテーションを維持するための秘訣です。

ステータスコードには、コード内の最初の数字によって区別される 3 つの主なクラスが存在します。ここに記載した SMTP 応答コードや他のコードの詳細に関しては、上で引用する RFC を参照してください。

以下に例を示します。

2xx - 成功、メッセージは受け取られました。
4xx - 一時的なエラー、メッセージは受け取られませんでした

5xx - 恒久的なエラー、メッセージは受け取られませんでした

上に示した最初のクラスは、実際には成功であり、細かく説明するまでもありません。メッセージが受け取られたことを意味します。受信側が、ただちに電子メールを受け取ることができない場合、あるいは受信者にただちに配信することができない場合、一時的なエラーコードまたは恒久的なエラーコードが返信されます。一時的なエラーは、送信者はメッセージを再度送信キューに入れて、後で再送を試みるべきであることを一般的に意味します。恒久的なエラーは、送信者は再度送信キューに入れるべきではないことを一般的に意味します。

***一時的なエラー***

すでに記載したように、一時的なエラーは、送信側サーバーがメッセージを再度送信キューに入れて、再送を行うべきであることを示します。よくある一時的なエラーは、受信側サーバーが他の受信電子メールの処理で忙しすぎるため、問題となっている単数または複数のメッセージを受け取るのに十分なリソースがないというケースです。別の理由としては、受信側がある IP アドレスから異常なメールの特徴を検出したので、その IP アドレスからの電子メールの受け取りを一定期間停止することを決めるケースです。

異なる受信者から上記の２つのケースでの返送メッセージは、ステータスコードは同じでも、説明メッセージが違っている可能性があります。いずれの場合も、送信者はコネクションを切断後、新規のコネクションを設定するべきです。ほとんどの商用のメーリングシステムには、複雑なアルゴリズム、再送タイミングを特定する待ち行列技術および再送回数ならびに再送を中断するタイミングなどを指定するための設定が存在します。大量の電子メールを処理する受信側には、送信側サーバーはリアルタイムでこれらの調整を行うことができ、大規模なプロセスとして、同じ IP アドレスによって受信側に送信されるすべての電子メールに対しても調整を行うことができるという期待があります。送信者が一時的なエラーを正しく取り扱い、恒久エラーとして扱わないことがきわめて重要です。その理由は、スパムの発信者は、RFC には従わないことが多いので、送信者が正しく RFC に従っているか否かを確認するために、受信側で最初のメッセージを「一時的に失敗させる」場合があるからです。

***恒久的なエラー***

恒久的なエラーは、メッセージを再送してはならないことを意味します。もっとも一般的な恒久的なエラーは、「user unknown」です。さらに、5xx 番コードの多くは、説明文によればポリシー違反を示します。説明文の内容に関わらず、これらの種類のエラーは、送信側サーバーにこのメッセージを再送してはならないことを常に示します。

***NDR の処理***

数値のステータスコード 4xx および 5xx は、送信側メールサーバーが行うべきことを記載しています。これらの数値コードは、マーケターや他のバルクメールの送信者を考慮して設計されておらず、そのアドレスをメーリングリストから削除すべきか否かを明確に規定していません。宛先不明のメッセージを受信した送信者は、メッセージ内の説明文を注意深く読んで、メーリングリストに含まれる特定のアドレスをどのように扱うかを決定しなければなりません。説明文が、送信側インフラやメールの内容に関する問題を診断するのに有用となる場合があるかもしれません。さらに、送信者の IP はブラックリストに掲載されており、メールがそのドメインに届く前に削除しなければならないことを示しているかも知れません。メールの送信者は、説明文に基づいて、有効であるとされるアドレスに対して配信の問題を診断し、解決するように努力しなければなりません。

NDR を取り扱うためのプロセスを備えることは、大量のメールを送信する組織には必須です。受信側が、恒久的なエラーで返送されてしまうメッセージが多すぎるという理由で、送信側 IP にペナルティーを科すことがよくあります。受信側が、送信者に対して、その電子メールアドレスに該当するユーザーは存在しないと連絡する場合、このメッセージを再送しないことがきわめて重要で、当該電子メールアドレスにはそれ以降送信しないようにしなければなりません。恒久的なエラーの量は、受信側が、送信者に関するレピュテーションを確立するために、さらにはその送信者から送られてくる電子メールをどのように処理す

べきかの判断をくだすために使用する指標の 1 つです。大量のハードバウンスは、大抵は、登録処理が十分に管理されていないか、メーリングリストが古いか、あるいはメーリングリストの不正使用を示しています。これは、IP のレピュテーションスコアから減点され、さらなる配信の問題を引き起こします。

推奨するベストプラクティスは、複数回連続したキャンペーンにわたって、失敗コードや説明文が連続して返送された場合、そのアドレスはリストから削除することです。キャンペーンの回数やその期間は、個々の送信者によりますが、一般的には、少なくとも 2 週間以上にわたって 2 回連続して返送された場合、そのアドレスをリストから削除することがベストプラクティスであると考えられます。これは、誤った返送の原因となった可能性のある受信サイドのサーバーの問題として説明されるべきです。

## 4. 結論

メールの送信者が本文書から読み取るべき最も重要な点は、エンドユーザーおよびエンドユーザーの期待が最優先されるべきだということです。送信者が法的に許されている行為や、個人情報保護方針（プライバシーポリシー）に基づいて権限が与えられている行為は重要ではありません。重要なことは、受信者、受信者のプリファレンスおよび受信者の期待に配慮することです。もちろん、送信者は、本文書で説明したすべての推奨に準拠することができたものの、それでもなお配信の問題や不満に思う受信者が存在するかもしれません。しかし、本文書に記載したベストプラクティスに厳密に従うことによって、最も重大かつ深刻な問題に対処するべきです。すべての送信者は、本文書に従って選択したすべての点に関して、必要とするすべての法令に順守していることを確実にするために、法務部門に助言を求めるべきです。

## 付録 A - 便利なツール

### データプライバシー

データプライバシーツールおよびベストプラクティスの詳細な情報に関するリソースを以下に示します。

- OWASP (Open Web Application Security Project), https://www.owasp.org)
- SANS Institute, https://www.sans.org
- OTA (Online Trust Alliance) "Data Protection and Breach Readiness Guide," https://otalliance.org
- ISO/IEC 27002:2013 from the Access Control, Communications and Operations Management, and Information Security Incident Management, http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54533
- U.S. Federal Trade Commission report "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers," http://ftc.gov/opa/2012/03/privacyframework.shtm

### 認証

- "Trust in Email Begins with Authentication," by Dave Cocker and edited by Terry Zink, February 2015, https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Email_Authentication_Update-2015.pdf
- M³AAWG DMARC Training Series videos, Michael Adkins and Paul Midgen, DMARC.org: http://www.maawg.org/activities/training/dmarc-training-series

### 関連する RFC

- RFC 2369: The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields, http://tools.ietf.org/html/rfc2369
- RFC 3463: Enhanced Mail System Status Codes, http://tools.ietf.org/html/rfc3463
- RFC 5321: Simple Mail Transfer Protocol, http://tools.ietf.org/html/rfc5321
- RFC 5598: Internet Mail Architecture, https://tools.ietf.org/html/rfc5598

### 他の M³AAWG 関連ベストプラクティス

- Messaging Anti-Abuse Working Group Position on Email Appending, https://www.maawg.org/sites/maawg/files/news/MAAWG_Epending_Position_2011-09.pdf
- M³AAWG Email Forwarding Best Practices, http://www.maawg.org/system/files/news/MAAWG_Email_Forwarding_BP.pdf
- MAAWG Vetting Best Common Practices (BCP), https://www.m3aawg.org/sites/maawg/files/news/MAAWG_Vetting_BCP_2011-11.pdf

## 付録 B - 法令順守リンク集

電子メール業界に適用される法令はさまざまです。法律の専門家に相談して、地域のすべての法令を順守していることを確認する責任は、各企業にあります。以下のリストには、世界中から集めた法令のリポジトリが含まれています。

- CAUCE-Cornell Spam Law Inbox Project: http://www.inboxproject.org
  スパム対策法関連資料集

- 欧州： http://europa.eu/legislation_summaries/internal_market/single_market_services/l24120_en.htm 電子通信セクターにおける EU データ保護法の概要

- US：連邦通信委員会、 Can-Spam:
  http://www.fcc.gov/encyclopedia/can-spam

- カナダのスパム対策法（CASL）：http://fightspam.gc.ca

- CAUCE カナダのスパム対策法に関する公文書集 http://www.cauce.org/2014/06/official-documents-related-to-canadas-anti-spam-law-casl.html

## 付録 C - 標準用語集

用語は、可能な限り RFC 5598 から取得しています。

**アクセスプロバイダー** - エンドユーザーにインターネットへのアクセスを提供する企業や組織。エンドユーザーがメールボックスプロバイダーとして利用するエンティティとは異なる場合もあります。

**バルク／マーケティングメッセージング** - 宣伝あるいはブランド／企業とメッセージの受信者の間で信頼関係を築く目的で送信されるメッセージであり、商用取引を目的としていません。（取引メッセージングと比較してください。）

**確認メッセージ** - 新規の加入者あるいは受信者が、電子メールアドレスを送信者に提供した際に、新規の加入者あるいは受信者に向けて送信される電子メール。通常、今後受信者の電子メールアドレスで送信者からのメッセージを受信することになり、また、受信者が電子メールアドレスを確かに提供しており、メッセージの受信を希望することに対して確認が必要であることを受信者に通知します。メッセージ内のリンクをクリックするか、メッセージに返信することによって確認が行われます。

**専有 IP** - 送信者、企業やブランドを代表して電子メールを送信するためにのみ利用される静的な IP アドレスであって、送信者、企業やブランドは、その IP から送信されるすべてのメッセージの内容に責任があります。IP は通常、rDNS （逆引き DNS）において、そのブランドと関連していることを宣言します。（共有 IP と比較した場合）

**ダーティな（手入れされていない）メーリングリスト** - アドレスの一部あるいはすべてが、不十分なメールアドレス収集とオプトインプラクティスを利用して取得した、および／または、アドレスの一部あるいはすべてが、徐々に最新の状態が保たれなくなった電子メールアドレスのリスト。これは、例えばハードバウンスや登録削除要求への対処が不十分であった場合、および／または、当該アドレスに１年あるいはそれ以上の期間メールされていない場合の結果である可能性もあります。

**エンドユーザー** - メールボックスプロバイダーの顧客。

**ESP（電子メールサービスプロバイダー）** - 顧客のために一定量のメールを送信するサービスを提供する企業。「送信者」と呼ばれることもあります。

**FBL（フィードバックループ）** - メールボックスプロバイダーが利用するシステムであって、資格を有する正規の送信者に、送信者に所属する IP アドレスから送信され、メールボックスプロバイダーのエンドユーザーがスパムであると報告したメッセージの写し（複写）を提供します。本システムは、送信者が苦情の原因となる問題を識別、対処することができるように提供されます。

**ハードバウンス** - 受信側 MTA は、電子メールアドレスが存在しなくなった、または元々存在しない、あるいはドメインが存在しなくなった、または元々存在しない等の恒久的なエラーが原因で電子メールが受信者に配信できないことを通知します。

**メールボックスプロバイダー** - エンドユーザーに電子メールボックスを提供する企業。エンドユーザーにインターネットへのアクセスを提供していなくてもよい。

**メッセージングの不正使用の苦情／報告** - メッセージングの不正使用の苦情や報告は、メッセージの受信者が、メッセージは不正であると苦情を述べたり、報告したりする時に発生します。このメカニズムとして最も多いのは、ウェブインターフェースや MUA（メールユーザーエージェント）のスパムボタンがクリックされることです。なお、メールボックスプロバイダーのサポート問い合わせ窓口や、不正使用に関する問い合わせ窓口へのサポートチケットのオープン、あるいは、メールボックスプロバイダーのサポート問い合わせ窓口、不正使用に関する問い合わせ窓口、またはメッセージの送信者への苦情メールの送信が

含まれる場合があります。また、メールボックスプロバイダーのサポート問い合わせ窓口、不正使用に関する問い合わせ窓口、またはメッセージの送信者に対して、メッセージが送信されたことに関して苦情を述べる目的で電話をかけることが含まれる場合もあります。

**オプトイン** - 送信者からのメッセージの受信を希望することを通知する受信者側の手順。

**オプトアウト** - 送信者からのメッセージの受信を希望しないことを通知する受信者側の手順。

**受信側 MTA** - メールボックスプロバイダーがメールメッセージの受信に利用するメール転送エージェント。

**送信者** - 電子メールメッセージの送信者。メッセージの送信に利用される送信側 MTA を管理する ESP や、メッセージの内容に責任のあるブランドや企業の双方を示す可能性があります。

**送信側 MTA** - 送信者がメールメッセージの送信に利用するメール転送エージェント。

**共有 IP** - 全員が、通常、そこから同時にメールを送信する多くの異なる送信者／ブランド／ESP 顧客が共有する IP アドレス。通常は、その IP からメールを送信するブランドの一つとしてではなく、IP を所有する ESP と同一視されます。共有 IP は、小規模な顧客にサービスを提供する大規模なアウトバウンド ISP メールサーバーを含む場合もあります。

**ソフトバウンス** - 受信側 MTA は、メールボックスの容量不足、接続の問題、メールボックスプロバイダーの技術的な問題、あるいは、配信される電子メールの配信速度を低く抑えるためにメールボックスプロバイダーが接続中の IP に制限を掛けるなどの一時的なエラーにより、受信者に対して電子メールが配信できないことを通知します。

**取引メッセージング** - 電子メールの送信者と受信者との間の商用取引を確認する目的や、送信者と受信者の関係の状況について個別に情報を提供する目的で送信されるメッセージ。例えば、これは、銀行口座通知やパスワード変更のお知らせなどです。（バルク／マーケティングメッセージングと比較してください。）