Amazon Simple Email Service
E メール送信のベストプラクティス

2012 年 7 月

（本ペーパーの最新版については、http://aws.amazon.com/whitepapers/をご覧ください）

目次

要約

自分が送信する E メールをターゲットの受信トレイに入れることは、簡単ではないこともあります。
多数のさまざまな要因、例えば E メールの内容、送信者が保有するリストの質、
送信者とターゲットの受信者の間にあるインフラストラクチャが、E
メール配信に影響を及ぼす可能性があります。
このホワイトペーパーでは、このような要因について解説するとともに、E
メールがターゲットに到達する確率を高めるためのベストプラクティスと推奨事項を紹介します。

序論

E メールが送信される理由はさまざまです。例えば、顧客との間に築いた関係の強化、
新製品のマーケティング、同じ事項に関心を持つグループへの情報提供、顧客へのイベントの通知です。
具体的には、次のようなものがあります。

- ニュースレター（例: 食材宅配会員向けのレシピ）
- 受領通知（例: 購入の確認）
- 旅行の案内（例: 航空券）
- アカウント関連の通知（例: パスワードのリセット）
- 法的通告（例: プライバシーポリシーの変更）

E メール送信者が受信者との間の電子コミュニケーションを管理する方法を、送信者の *E メールプログラム*と呼ぶこともできます。

E メールプログラムを適切に運営するには、E メールの配信に影響を及ぼし、
最終的には受信者にも影響を及ぼす可能性がある、いくつかのトピックについて認識していることが必要です。このホワイトペーパーでは初めに、送信された E メールの価値を、受信者や、
受信者の受信トレイを保護する責任を持つインターネットサービスプロバイダ
（ISP）がどのように考えるかについて説明します。次に、E メール送信のプロセスがどのようなものであり、誰が関係するかを、それぞれの役割とともに説明します。最後に、AWS
がこれまでに集めたベストプラクティスに基づいて価値を最適化し拡大する方法を紹介します。

このホワイトペーパーを読み終えると、E
メールプログラムを成功に導くための多数の手法を理解しているはずです。

E メールはどのように配信されるのか

E メールがどのようにして、そしてなぜ配信されるかを考えたことはありますか? *配信到達性*とは、送信した E メールメッセージが、意図した宛先に実際に到達する可能性を指す言葉です。E メールは、
意図した受信者の受信トレイに必ず到達するとは限りません。*ジャンクフォルダ*（*スパムフォルダ*という名称

のこともあります）に配信されたり、受信者のメールインフラストラクチャによって拒否されたり（通常はバウンスの形を取ります）、完全に消えてしまったり（例えば、受信側のシステムによってメッセージが破棄されたが、送信者にも受信者にも通知されない）することがあります。ISP の中には、ユーザーの利用度合いに応じて、受信メッセージを整理しやすいようにデフォルトのフォルダを作成しているところもあり、E メールは受信トレイではなくそのフォルダに配信されます。

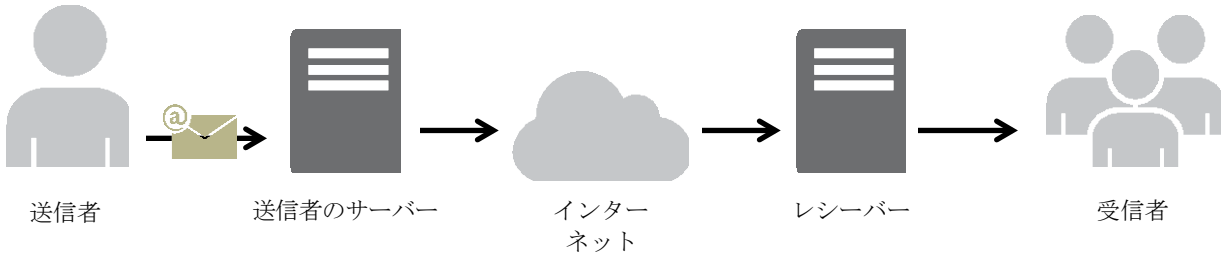
E メールの送信者としては、できる限り多くのメッセージが相手の受信トレイに届いてほしいと思うものです。配信率を高める最善の方法は、質の高いメール、つまり受信者にとって価値のあるメールを送信することです。E メールの受信者がメールを受け取りたいと思うのは、メッセージから価値を引き出せる場合に限られます。この価値は、さまざまな形を取ります。例えば、お得な情報、注文の確認、懸賞の通知、さらにはソーシャルネットワークでのコミュニケーションなどがあります。言うまでもなく、「価値」は含みのある言葉です。何が E メールメッセージの価値となるかは、人によって異なるからです。

*E メールの質*とは、E メールの受信者にとっての価値です。主観的なものであるにもかかわらず、ISP は E メールの質をできるかぎり正確に予測しようとしています。そのために、さまざまなメトリックスを使用して、メッセージが求められている（価値がある）ものか、求められていない（スパムとみなされる）ものかを判断しています。このメトリックスとは、例えばアンチスパムテクノロジーに基づいて内部的に計算された数値や、受信者から受け取った情報を ISP が数値化したものです。

送信者は、質の高い E メールを送信することによって、*レシーバー*（宛先アドレスの背後にいる人または物）との間に時間とともに信頼を確立していきます。この信頼を、専門用語では*レピュテーション*（評判）といいます。レシーバーは、メトリックスを使用して送信者の E メールの価値を評定します。このようなメトリックスは多くの場合、いくつかが組み合わされてスコアとして使用されます。また、このメトリックスが一般的に送信者のレピュテーションと呼ばれます。

E メールのフロー

次の図は、E メールの送信と受信に関与する実体を表したものです。



E メールのレシーバーと E メール配信

E メールのレシーバーは、送信されたメールを配信するかどうかを判断します。E メール配信を管理するネットワークシステム、ソフトウェア、ポリシーが一体となって、レシーバーを構成します。E メールのレシーバーにはさまざまな種類がありますが、送信者の E メールプログラムの配信到達性を最適化するには、送信先のレシーバーの種類を知っておくことが必要です。

インターネットサービスプロバイダ

インターネットサービスプロバイダ（ISP）は一般的に、加入者向けに E メールサービスをホスティングしています。一般的に、B2C（Business to Consumer）の E メールの送信先は、ISP においてホスティングされるアドレスです。Yahoo!、Gmail、Comcast などのサイトが、このカテゴリに該当します。このような大手プロバイダは、数百万ものメールボックスを対象に、送られてきたメールがスパムかどうかを判断しますが、その判断の元になるのは、多くの受信者からのフィードバックです。

このフィードバックの形として最も多いのは苦情（受信者が各自のメールクライアントで、メッセージがスパムであると報告）ですが、受信者が E メールを開いたりクリックしたりしたかどうかも、フィードバックに含まれます。ISP がレピュテーション計算に自由に使用できる受信者フィードバックの量は膨大ですが、ISP が実装するレピュテーションシステムは「万人向け」の傾向があります。すべてのメールボックスに容易にロールアウトできるからです。

コーポレートシステム

コーポレートシステムとは一般に、従業員、学生、政府機関、非営利組織などによって使用される、独立してホスティングされている E メールシステムです。このシステムは一般に、B2B（Business to Business）システムと呼ばれます。ISP がインバウンドの E メールシステムを運用するための、ホステッド型の E メールサービスもコーポレートシステムに含まれることがあります。多くの場合は、スパム防止のためのルールが組織内の IT（情報技術）部門によって設定されていますが、E メールを受信する MTA（Mail Transfer Agent）ソリューション、例えば Microsoft Exchange のデフォルトのルールが使用されることもあります。

個人製システム

メールボックスは、ISP や IT 部門によって管理されるもの以外にも、クラウド内または個人所有のサーバー上で運用されているものが考えられます。個人製システムの場合は、標準的ではないルールを、サーバーの所有者が*随時*設定できることに注意する必要があります。このような個人所有の E メールサーバーの背後にいる人にメールが届くようにするには、その所有者が独自に定める高品質メールの定義に従う必要があります。

以上の種類のレシーバーはいずれも、求められていない E メールに対する防御の手段を多数採用しています。Amazon Simple Email Service（Amazon SES）は、このような防御のほとんどを、送信者に代わってインフラストラクチャ層で処理しています（例: E メール DNS セットアップ、送信レート、スロットリング、自動再試行など）。しかしそれでも、送信先のレシーバーの種類を知っておくことは、そのレシーバーのルールに従い、メッセージを受信者の受信トレイまで到達させるために必要です。

すべてを決めるのは、**受信者のルールです。**E メールは誰でも送信できますが、E メールを受信トレイまで届けることができるのは、受信者のことをどのように尊重するかをよく知っている送信者だけです。

送信者の成功を決定づけるメトリックス

以下に列挙するメトリックスがすべてではありません。これは単に、E
メールプログラムに伴う問題となりうる領域を示すものです。これらの問題領域におけるメトリックスを管理するだけで、配信が保証されるとは考えないでください。すでに述べたように、送信者は顧客のことをよく知る必要があります。

バウンス率

バウンスは、配信を試みて失敗したことを示します。これは、レシーバーから送信者に報告される有益な情報です。

レシーバーでは、ハードバウンスとソフトバウンスの両方が生成されます。*ハードバウンス*が恒久的な配信失敗（例えば「メールボックスが存在しない」）であるのに対し、*ソフトバウンス*は一時的な配信失敗（例えば「メールボックスの容量超過」）です。バウンスには、同期型と非同期型があります。*同期型*のバウンスは、E メールサーバーどうしが通信しているときに通知されます。*非同期型*のバウンスとは、
メッセージが配信の対象としてレシーバーで正常に受け付けられた後で送信されるバウンスのことです。
Amazon SES では、成功を示す応答（「250 OK」）が送信者に返されることはありません。Amazon SES
はソフトバウンスを自動的に処理するようになっており、送信先のドメインに応じた最適な設定で再試行が行われます。ハードバウンスは、同期型と非同期型のどちらであっても、自動的に送信者に渡されます。詳細については、『*Amazon Simple Email Service Developer Guide*』の「Bounce and Complaint Notifications」
をご覧ください。

**ハードバウンス率が高いときは、E
メールレシーバーは送信者が受信者のことをあまりよく知っていないと判断します。**したがって、ハードバウンス率の高さは、送信者の配達可能性にマイナスの影響を及ぼす可能性があります。ハードバウンスを減らす方法のヒントを後ほど紹介します。

苦情率

E メールの受信者が、メッセージがスパムであることを示すために Web
メールクライアントの「スパムとして報告」ボタンをクリックすると、ISP
はこのことを苦情として記録します。このような苦情が多すぎる場合は、送信者がスパムを送信していると ISP が判断する可能性が高くなります。ISP の中には、受信者の対応を送信者にある程度知らせるために、*フィードバックループ*を設けているところもあります。これは、あるメッセージについて受信者が苦情を申し立てたことを ISP から送信者に知らせる仕組みです。Amazon SES では、フィードバックループを採用している ISP からの苦情は自動的に送信者に転送されます。詳細については、『*Amazon Simple Email Service Developer Guide*』の「How Amazon SES Handles Email」をご覧ください。

想像できると思いますが、苦情が多すぎると、配信到達性が低下する可能性があります。**苦情率が高いときは、E メールレシーバーは受信者が望まないメールを送信者が送信していると判断します。**
苦情率を下げるためのヒントを後ほど紹介します。

コンテンツの問題

E メールのコンテンツは、伝えたい内容やメッセージです。E メールレシーバーは、スパム送信者からの悪意のある通信（例えば、フィッシング、マルウェア、ウイルス拡散、詐欺）を防ぐために、堅牢な*コンテンツフィルタ*を実装しています。このコンテンツフィルタによって、メールのコンテンツに対するレビューが自動的に実行されて、迷惑メールが検出されます。技術に詳しいユーザーの間では、オープンソースのコンテンツフィルタ（例えば Apache Spam Assassin）が利用されています。大企業では、Google の Postini や Symantec の BrightMail のようなコンテンツフィルタが利用される傾向があります。Amazon SES で使用されているコンテンツフィルタリングテクノロジーは、ウイルスやマルウェアが含まれるメッセージを検出してブロックし、これらが送信されるのを未然に防ぎます。

レシーバーのコンテンツフィルタによって、コンテンツの特性がスパムに似ていると判定された場合は、おそらくそのコンテンツは印が付けられて、受信者の受信トレイとは別のところに配信されます。送信する E メールのコンテンツがフィルタで阻止されるのを防ぐ方法のヒントを後ほど紹介します。

推奨ベストプラクティス

受信者にとって何が最善かを送信者が念頭に置いていても、理想的な印象を与えるようにプログラムを微調整するのは簡単ではありません。ここでは、受信者にとって、そして ISP にとって最善のことを実施するのに役立つヒントを集めました。

全般的な推奨事項

- 受信者になったつもりで考えます。自問してみてください。「これは、*自分の*受信トレイに届いてほしいだろうか」。はっきり「はい」と言えないのであれば、おそらく、そのメッセージは送信すべきではありません。
- 常に警戒します。残念なことに、いくつかの業種は、質の低いメールを送ってくるという評判が確立しています。実に単純です。送信者が次に示す業種に属しているのであれば、自らのレピュテーションメトリックスをよく監視して、問題がある場合はすぐに改善してください。
    - 住宅担保ローン
    - クレジット
    - 医薬品
    - たばこ
    - アルコール
    - アダルト向けエンターテインメント
    - ギャンブル
    - 在宅就業プログラム

ドメインと「差出人（From）」アドレスに関する考慮事項

- 送信するメールの差出人アドレスについて、よく考えてください。差出人（From）アドレスは、受信者のメールクライアントに表示される（プレビュー領域にも）だけでなく、ISP によってはレピュテーションの収集にも使用されます。差出人は、件名行とともに、受信者に対するそのメールの第一印象を作り出します。
- メールの送信元アドレスのドメインについて、よく考えてください。その理由は次の 2 つです。
    - ISP はレピュテーション情報を、あるドメインから送信されたすべての E メールから収集します。送信がどのように分割されているかは関係ありません。
    - 受信者が送信者のドメインを認識できることが必要です。例えば、*www.example-foo.com* でホスティングされている Web フォームで入力された E メールアドレスに対して、*sender@example-bar.com* というアドレスからメールを送信してはなりません。送信者を認識できないので、受信者は「スパムとして報告」ボタンをクリックしてしまいます。
- 大量のメールを送信する場合は、ISP ベースのメールアドレス（例えば *sender@hotmail.com*）から送信しないでください。例えば、*sender@hotmail.com* から大量のメッセージが届いていることに Yahoo! が気付いた場合は、Yahoo! がそのメールを扱う方法は、適切なアウトバウンドのメール送信ドメイン（送信者が所有しているドメイン）からのメールとは異なります。
- 自身のドメインの正しい WHOIS 情報を追加してください。送信元ドメイン所有者の詳細情報をレシーバーが検索できるようにするためです。WHOIS レコードのセットアップ方法については、ドメインレジストラの指示に従ってください。レシーバーは、実績があって素性が明確であり、インターネットレジストリに情報が登録されているドメインを、そうでないドメインよりも信頼します。

認証

- 送信者のドメインが、**Sender Policy Framework（SPF）** と **SenderID** によって認証されていることを確認します。これらの方法で認証を行うと、送信者のドメインの信頼性が増加します。E メールが実際にそのドメインから送信されたものであることが、メール受信者に対して保証されるからです。詳細については、『*Amazon Simple Email Service Developer Guide*』の「Authenticating Your Email Address」を参照してください。認証設定をテストするには、自分が所有する ISP アカウントの受信トレイ（例えば Gmail のアカウント）にメールを送信して、メッセージのソースのヘッダーを見ます。ヘッダーを見ると、認証に成功したかどうかがわかります。
- さらに、**DomainKeys** または **DomainKeys Identified Mail（DKIM）** を使用して発信 E メールに署名してください。

Amazon SES での SPF と SenderID

Amazon SES をお申し込みいただくと、すぐに使用できる構成済みの DNS レコードが用意されます。さらに、SPF もセットアップ済みです。amazonses.com から送信する IP アドレスはすべて、SPF 経由で認証されます。ただし、SenderID による認証も行うことをお勧めします。このようにするには、Amazon SES のドメインへのポインタを送信者の TXT レコードに追加してください。

この認証ステップによって、送信する E メールの信頼性が増加します。
コンテンツが送信者からレシーバーまで送られる間に変更されていないことが、受信者に対して保証されるからです。SPF と DKIM の違いについては、Wikipedia の記事「Email authentication」に簡単な説明があります。認証設定をテストするには、自分が所有する ISP アカウントの受信トレイ（例えば Gmail のアカウント）にメールを送信して、メッセージのソースのヘッダーを見ます。ヘッダーを見ると、認証に成功したかどうかがわかります。

リストの作成と保守

- E
メールアドレスを収集する方法について、注意が必要です。オンラインフォームなどで申し込みを受け付けるときに、実在しない E メールアドレスが入力されることはよくあります。
そのアドレスに E メールを送信しようとすると、ハードバウンスが発生するため、
ISP からは無責任な送信のように見えてしまいます。
- フォームで収集したアドレスへの初回 E
メール送信時にハードバウンスとなることが続いた場合は、受信者が入力するアドレスを確認できる仕組みを用意してください。アドレスを表示して確認を求める、E メールアドレスを 2 つのフィールドに入力させて内容が一致していることを確認する、という方法があります。可能であれば、クライアント側の自動入力機能をオフにします。
- *ダブルオプトイン*（E メール送信先のアドレスの所有者が確認リンクをクリック済みの場合にのみ、そのアドレスにメールを送信する）を利用すると、実在しないアドレスに何度もメールを送信することはなくなります。
- サードパーティベンダーのサービスを利用して、E
メールアドレスが実在するものかどうかを確認してからそのアドレスに送信します。
- E メールアドレスの構文を調べて、ある程度は正しいことを確認します。
例えば、アドレスがローカル部分と @ 記号で正しく構成されているか、
アドレスを解決するとドメインと MX レコードが得られるか、といったことを調べます。
- ユーザー定義の入力を未チェックのまま Amazon SES や ISP
に渡すことを許可するかどうかを十分に検討してください。フォーラムやフォームからの送信には、特に注意が必要です。コンテンツが完全にユーザー生成されたものである（したがってスパム送信者がフォームのフィールドに自分のコンテンツを入力できる）こともありますが、E
メールのレシーバーにはそのことはわかりません。E
メールで質の高いコンテンツしか送信しないことを保証するのは、送信者の責任です。
- E メールを受け取るアドレスとして、標準的なエイリアス（postmaster@、abuse@、noc@ など）
が意図的に指定されることはほとんどないはずです。E
メールアドレスをどのように入手するかについて、送信者がコントロールできることが必要です。また、そのアドレスが実在する人物のものであり、その人物がメール受信を望んでいる場合にのみ、メールを送信してください。これが特に当てはまるのは、ロールアカウント（通常は E
メール監視用に予約されています）です。ロールアカウントは、悪意のある者によって送信者のリストに追加されることがありますが、この目的は送信者のインターネット活動を妨害することです。収集したアドレスのリストに、ロールアカウントのエイリアスがないことを確認してください。監視が必要なすべてのロールアカウントの一覧については、「Mailbox Names for Common Services, Roles and Functions」をご覧ください。

- サードパーティのリスト（自身の権限の及ばないところから購入、レンタルなどの方法で集めたもの）に E メールを送信しないでください。E メールをサードパーティのリストに送信するときは、出所が不明な E メールアドレスに送信するというリスクを取ることになります。そのリストに*スパムトラップ*（迷惑メール監視の目的で ISP がセットアップした特別なアドレス）や、バウンスするアドレス、または苦情を申し立てている受信者が含まれている場合は、ISP による規制を受けることがあります。サードパーティリストに含まれている E メールアドレスが正当なものであっても、受信者が本当にメール受信を望んでいるかどうか、つまり送ったメールがスパムと見なされるかどうかが不明であることに変わりはありません。E メールアドレスの収集は自分自身で、受信者から直接行ってください。

コンプライアンス

- E メールの送信先である受信者が米国在住かどうかにかかわらず、E メール送信者は E メール送信に適用される法規制に従う必要があります。このガイドでは、このようなコンプライアンスの事項については取り上げないので、適用法を理解して従ってください。

バウンスを防ぐ

- 基本的に、バウンス率は 5% 以下に維持してください。これは、送信者のリストがクリーンである（受信者のアドレスの状態を送信者が知っている）ことを ISP に対して証明する方法の一つとなります。この比率は業種の傾向に伴って変化することがあり、すべての ISP に普遍的なものではありませんが、目安としては妥当です。
- 送信者が所有しているリストが古く、しばらく E メールを送信していなかった場合は、アドレスの状態の確認（自分のサイトでログインアクティビティを調べる、履歴を購入するなど）が完了するまでは、バウンス率を制限している ISP（Amazon SES も含まれます）経由でそのリストに E メールを送信しないでください。リストのクリーニングが完了する前に送信すると、使用されていない古い E メールアドレスからの大量のバウンスが発生する可能性があり、ISP と Amazon SES の両方からブロックされるというリスクがあります。
- 重要な情報（例えばパスワードのリセット）を顧客に送信しようとしている場合は、E メールアドレスのバウンスに備えて、E メールに代わる通信手段を用意しておいてください。代替手段として考えられるものには、ブラウザ内での秘密の質問、郵便、SMS などがあります。また、メールを送信する予定の送信先アドレスを表示し、その E メールアドレスが実際には正しくなかった場合の別のワークフロー（例えば SMS）を受信者が選択できるようにしてください。

バウンスの取り扱い

- ハードバウンスの原因が恒久的な配信失敗の場合は、その E メールアドレスに送信しないでください。その配信失敗が本当に恒久的なものである場合は、送信を繰り返し試してもメッセージは配信されず、代わりにバウンスの数が増えるだけであり、ISP から見た送信者のレピュテーションが低下します。
- バウンスを受け取るアドレスのメールボックスそのものが、バウンスするものであってはなりません。そのメールボックスで受信できることを確認してください。さらに、インバウンド E メールシステムを ISP にアウトソーシングしている（組織自身の内部サーバーを通して E

メールを受信するのではない）場合は、殺到するバウンスがスパムフォルダに振り分けられたり、完全にドロップされたりする可能性があることに留意してください。バウンスの受信にはホステッド型の E メールアドレスを使用しないのが理想的です。
使用しなければならない場合は、スパムフォルダを頻繁にチェックしてください。
また、バウンスメッセージをスパムとして報告しないでください。Amazon SES では、バウンスを受信する方法として、Amazon Simple Notification Service（Amazon SNS） と E メールの一方または両方を指定できます。詳細については、 *『Amazon Simple Email Service Developer Guide』* の「Bounce and Complaint Notifications」をご覧ください。

- 通常は、バウンスには配信を拒否されたメールボックスのアドレスが記載されています。ただし、受信者のアドレスを特定の E メールキャンペーンにマッピングするために、
より細分化されたデータが必要な場合は、自社のトラッキングシステムまでさかのぼることのできる値を X-header で指定してください。詳細については、 *『Amazon Simple Email Service Developer Guide』* の「Header Fields Appendix」を参照してください。

苦情を防ぐ

- 基本的に、苦情率は 0.1% 未満に維持してください。これは、送信者が価値のある E メールを送信していることを ISP に対して証明する方法の一つとなります。
この比率は業種の傾向に伴って変化することがあり、すべての ISP に普遍的なものではありませんが、目安としては妥当です。
- 苦情の元になったものと同じタイプの E メールをその受信者に送り続けないでください。例えば、マーケティングの E メールについてある受信者から苦情を受けた場合は、それ以降その人にマーケティングの E メールを送信してはなりませんが、その人がサイトで何かを購入したときに、手続きに関する E メールをそのアドレスに送信するのは問題ありません。同じタイプの E メールを再送信しても苦情が増えるだけであり、これが時とともに積み重なると、送信者の苦情率が増加してしまいます。そのアドレスを、該当するリストから除外すればよいのです。
- バウンスと同様に、リストに登録されているアドレスにしばらくメールを送信していなかった場合は（例えば、送信者が Amazon SES を使い始めたばかりの場合）、なぜ E メールが送られてきたかを受信者が理解できるようにしてください。「ようこそ」メッセージなどの手段を使用して、受信者に、送信者が誰であるかを改めて知らせることを強くお勧めします。ISP と Amazon SES の両方に苦情が持ち込まれるのを防ぐためです。

苦情の取り扱い

- バウンスと同様に、苦情を受け取るアドレスのメールボックスそのものがバウンスするものであってはなりません。そのメールボックスで受信できることを確認してください。さらに、インバウンド E メールシステムを ISP にアウトソーシングしている（組織自身の内部サーバーを通して E メールを受信するのではない）場合は、殺到するバウンスがスパムフォルダに振り分けられたり、完全にドロップされたりする可能性があることに留意してください。苦情の受信にはホステッド型の E メールアドレスを使用しないことをお勧めします。使用しなければならない場合は、スパムフォルダを頻繁にチェックしてください。また、苦情メッセージをスパムとして報告しないでください。
Amazon SES を使用するときは、バウンスを受信する方法として、Amazon Simple Notification

Service（Amazon SNS）と E メールの一方または両方を指定できます。詳細については、*『Amazon Simple Email Service Developer Guide』*の「Bounce and Complaint Notifications」をご覧ください。

- 苦情メッセージには一般的に、その E メールの内容が含まれています（対照的に、バウンスメッセージの場合は一般的にヘッダーのみです）。ただし、苦情元のアドレスの部分を、ISP がプライバシーを考慮して編集していることもあります。独自の X-header を使う、またはコンテンツに値を埋め込むといった方法で、苦情と苦情元の E メールアドレスとをマッピングできるようにしておくのは、送信者の責任です。

質の高いコンテンツを作る

- 今日のコンテンツフィルタのほとんどは包括的です。厳格な規則に従うのではなく、コンテンツのフィンガープリントに注目するようになっています。数年前は、英文の E メールの件名に句読点が含まれていたり、すべて大文字であったりすると、その E メールはかなりの確率でスパムフォルダに振り分けられていました。現在では、さまざまなコンテンツ特性の組み合わせが重視されており、その組み合わせがスパムによく見られるものかどうかに重点が置かれています。Spam Assassin や、サードパーティのレピュテーションサービス（Return Path など）は、コンテンツの問題の特定に役立ちます。
- 送信する E メールの中で使用している URL がブラックリストにあるかどうかを調べることは、非常に有益です。ISP の中には、ブラックリスト登録済みのリンクが含まれている E メールをブロックしているところがあるからです。URIBL.com と SURBL.org の 2 つのサイトは、リンクがリストに登録されているかどうかを調べるのに非常に便利です。なお、第三者から提供されたリンクや、短縮リンクは必ずチェックしてください。このようなリンクは最終的なドメインをわかりにくくするものであるため、危険性が増加しつつあるからです。
- リンク切れの URL を E メールで送信してはなりません。リンク先のページが実際に存在することを確認してください。配信中止用のリンクがある場合は、そのリンクが機能することを確認してください。E メールプログラムを新たに構築しているときや、既存の E メールテンプレートを変更しているときは、リンクを一つ一つテストすることを忘れがちです。
- 自サイトのプライバシーや利用規約のページが機能していることを確認してください。標準的な規約のページがサイトで見つからない場合は、受信者は E メールを信頼しないことがあります。その結果、送信者のメールの価値と配信到達性が低下します。
- 送信頻度の高いコンテンツ（例えば毎日）については、そのコンテンツが実際に毎日違うものであることを確認してください。次々とコンテンツを送る場合は、タイミングが適切で意義深いコンテンツであることを保証するという責任が伴います。

まとめ

E メールの送信者とターゲットである受信者との間にある、さまざまなシステムを通過することの難しさにもかかわらず、E メールはコミュニケーションのメカニズムとして多大なる効果を挙げる可能性がありますが、そのためには正

しく使うことが必要です。このホワイトペーパーでは、送信した E
メールがターゲットの受信トレイに到達するかどうかを左右する要因にはどのようなものがあり、送信者の E
メールプログラムをより良いものにするにはどうすればよいかを説明しました。

前述のリストは、E メールの質の向上（および、その結果の配信到達性向上）
に役立つことすべてを網羅しているわけではありませんが、スタート地点として参考にしてください。
E メールプログラムを構築するときは、次の 2 つを常に忘れないでください。

1. 価値を届ける。
2. その E メールを望んでいる人だけに送信する。

このペーパーで紹介したヒントに従って、上記の 2 点を常に心がけていれば、E
メールプログラムの成功につながるでしょう。

用語集

- **非同期バウンス** -
メッセージが配信の対象としてレシーバーで正常に受け付けられた後で送信されるバウンス。
- **バウンス** - 配信を試みて失敗したことを示すメッセージ。
- **苦情** - 受信者が、メッセージがスパムであることを示すために E
メールクライアントの「スパムとして報告」ボタンをクリックしたときに生成されるメッセージ。
- **コンテンツフィルタ** - E メールのコンテンツを自動的にレビューして迷惑メールを検出する機能。
- **配信到達性** – 送信された E メールメッセージが、意図した宛先（通常は受信者の受信トレイ）
に実際に到達する可能性。
- **ダブルオプトイン** –
サービスを利用したい人が利用開始を申し込んだ後で、その人にメールを送信し、その中の確認リンクがクリックされたら利用手続き完了とする仕組み。
- **E メールプログラム** - E メール送信者が受信者との間の電子コミュニケーションを管理する方法。
- E メールの質 - E メールが受信者にとって価値があると見なされるかどうか。
- **フィードバックループ** - メッセージについて受信者が苦情を申し立てたことを ISP
から送信者に知らせる仕組み。
- **ハードバウンス** – 恒久的な配信失敗（例えば「メールボックスが存在しない」）を示すメッセージ。
- **インターネットサービスプロバイダ（ISP）** - インターネットへのアクセスサービスを提供する組織。
- **ジャンクフォルダ** - 「スパムフォルダ」または「バルクフォルダ」とも呼ばれる。
各種フィルタによって価値が低いと判定された E メールメッセージを集めるフォルダ。
そのようなメッセージは受信者の受信トレイには配信されませんが、受信者がアクセスできます。
- **レシーバー** - 受信者の E メールインフラストラクチャをサポートするシステム。E
メール送信先アドレスの背後にいる人または物。
- **受信者** - E メールメッセージを受け取る人または実体。受信者は、メッセージの To、Cc、または Bcc
のフィールドで指定されます。
- **レピュテーション** - E メール送信者が、質の高い E
メールを送信することによって時間とともに確立する信頼。
通常は、さまざまな要因の影響を受けます。
- **送信者** - E メールメッセージを送信する人または実体。
- **ソフトバウンス** - 一時的な送信失敗（例えば「メールボックスの容量超過」）を示すメッセージ。
- **スパムトラップ** - 迷惑メール監視の目的で ISP がセットアップした特殊なアドレス。
- **同期バウンス** - E メールの送信者とレシーバーの E メールサーバーとがアクティブに E
メールメッセージを送受信しているときに通知されるバウンス。

その他のリソース

本ホワイトペーパーで紹介した推奨事項に関する詳細情報

- 米国における E メール関連の規制の詳細については、FTC のサイトをご覧ください。http://business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business
- Amazon SES のソリューションプロバイダの詳細については、Amazon SES リソースのページをご覧ください。http://aws.amazon.com/ses/resources/
- E メール認証設定をテストする方法の詳細については、ESPC のサイトをご覧ください。http://www.espcoalition.org/senderid/

Amazon SES の詳細情報

- 概要 – http://aws.amazon.com/ses/
- 開発者向けドキュメント – http://aws.amazon.com/documentation/ses/
- コミュニティフォーラム – https://forums.aws.amazon.com/forum.jspa?forumID=90
- AWS Support – https://aws.amazon.com/support

Amazon SES ソリューションプロバイダ

- 配信到達性: Return Path – http://aws.amazon.com/solution-providers/si/return-path
- プレビューレンダリングと分析: Litmus – http://aws.amazon.com/solution-providers/si/litmus/
- フルサービスとストラテジー: Zeta Interactive – http://aws.amazon.com/solution-providers/si/zeta-interactive-1320423244
- ストラテジー: Synchronicity Marketing – http://aws.amazon.com/solution-providers/si/synchronicity-marketing
- テクノロジーインテグレーション: Cambridge Technology Enterprises – http://aws.amazon.com/solution-providers/si/cambridge-technology-enterprises

ISP ポストマスターのページ

- AOL – http://postmaster.info.aol.com/
- ATT – http://www.att.com/esupport/postmaster/
- BellSouth – http://www.att.com/esupport/postmaster/
- Charter – http://www.charter.com/customers/support.aspx?supportarticleid=1953
- Comcast – http://postmaster.comcast.net/
- Cox – http://postmaster.cox.net/confluence/display/postmaster/Postmaster+Home
- Facebook – http://postmaster.facebook.com/
- Frontier – http://postmaster.frontier.net/
- Gmail – https://mail.google.com/support/bin/answer.py?answer=81126&topic=12838

- Hotmail – http://postmaster.msn.com/
- RoadRunner – http://postmaster.rr.com/
- United Online – http://unitedonline.net/postmaster/
- USA.NET – http://postmaster.usa.net/
- Yahoo! – http://postmaster.yahoo.com/