# Messaging, Malware and Mobile Anti-Abuse Working Group

# M³AAWG ヘルプ！ スパムトラップに引っかかってしまった！

**2023年 2月**

この文書へのURL: https://www.m3aawg.org/help-i-hit-a-spam-trap

## 序論

このドキュメントは、電子メールサービスプロバイダー（ESP）がスパムトラップに引っかかった際の影響を軽減するための手助けとなります。また、顧客のメール送信運用を改善し、将来のスパムトラップによる影響を最小限に抑えることができるようなスパムトラップのフィードバックの活用方法も提案しています。このドキュメントでは、「顧客」とは、ESPを使用して電子メールを送信する組織を意味しています。

ほとんどの電子メール送信者は、ある時点でスパムトラップにメールを送信してしまった（「スパムトラップヒット」）ことによる影響を受けます。その影響の大きさは、トラップヒットの数、どのような種類のトラップにヒットしたか、誰がトラップを運用しているか、その他の変数によって大きく異なり、顧客はこれらの要因に気づいていない恐れがあります。ESPはトラップヒットの発生を監視し、発生した場合に顧客に通知する責任があります。ESPは、トラップヒットのさらなる発生を防ぎ、これらのヒットによる配信への影響を軽減したいと考えます。対応の遅れは、ESPの送信インフラストラクチャ全体でより深刻な結果につながる可能性があります。

特定の送信元からのスパムトラップヒット率が高い場合は、悪意がある送信者、あるいはベストプラクティス（M3AAWGが推奨する基準はM3AAWG Sender Best Common Practices に記載されています）を一貫して実施していない送信者である可能性があります。受信ドメインは、利用者にとって最適と判断した場合、その送信元からのメールを拒否するか、あるいは配信の優先度を引き下げる対応を行うことがあります。極端な状況ではESP自身がブロックリストに掲載され、スパムトラップを作成した特定のISPなどだけでなく、インターネット上の広範囲でメールが拒否される可能性があります。

スパムトラップにヒットすることは決して望ましいことではありませんが、スパムトラップヒットは、ESPが悪意のある顧客を検出し利用停止するだけでなく、正当な顧客の不適切な送信方法を特定し、修正するきっかけにすることができます。このドキュメントの後半では、スパムトラップに関する軽減策と顧客との話し合いのポイントについて説明します。

## スパムトラップとは？

スパムトラップとは、スパムやその他の迷惑メール、不正なメールを収集、記録、監視するために使用されるメールアドレスです。スパムトラップは、他のメールアドレスと区別がつかないように設計されて

おり、企業ドメインや「フリーメール」ドメインなど、あらゆる種類のネットワークで見つけることができます。

トラップにはさまざまな種類がありますが、共通しているのは、メールを送信したり、メーリングリストやニュースレターに登録したりしないことです。トラップの運用者は、これらのアドレスに送信された電子メールを監視し、そのデータを使用して、IPアドレスとドメイン名のレピュテーションを分析、電子メールの内容を評価します。

これらのデータは、DNSブロックリスト（DNSBL）やその他のレピュテーションシステムを通じて頻繁に使用および再配布され、それらを利用する受信側のブロック判断を支援します。

## スパムトラップの分類

一般的なトラップの種類には、以下のようなものがあります:

リサイクルトラップ

> 過去に個人が実際に使用していた可能性のあるアドレスまたはドメインが、その後一定期間の非アクティブ状態を経て廃止され、スパムトラップとして再利用されたものです。非アクティブ期間の長さは運用者によって大きく異なりますが、M3AAWGは最低12か月を推奨しています。この種のトラップヒットは、リスト管理が不十分である（または古いリストを使用している）、正常なバウンス処理に不備がある、またはその両方であることを示しています。

プリスティンまたはピュアトラップ

> 過去に一度も使用されていないアドレスであり、スパムトラップのために生成されたものです。プリスティントラップへ引っかかることは、多くの場合、ウェブハーベスティング、アドレス空間プロービング、または辞書攻撃が実施されたことを示します。またプリスティントラップへのヒットは、リストが購入された事実を示す強力な指標ともなります。

タイポトラップ

> 主にアドレスのドメイン部分において意図的かつ一般的と思われる誤植が含まれるトラップで、user@gmial.com, user@notmail.comなどの例があります。この種のヒットは、多くの場合、顧客が受信者のアドレスを確認できなかったことを示しており、送信者がメールアドレスを収集したときの転記ミス、またはスキャンエラーが原因である可能性があります。厳密にはプリスティントラップですが、送信者は正当な収集方法で取得した可能性があるため、多くの運用者はこれらを区別して分類しています。

M3AAWGの、Best Current Practices For Building and Operating a Spamtrap では、スパムトラップの種類とその使用方法についてより詳細に分類されており、追加情報として参照できます。このドキュメントでは、主に、レピュテーション監視を目的としたセンサートラップネットワークではなく、メールを実際にブロックして配信に直接影響を与えるトラップについて言及しています。

## スパムトラップに引っかかったとわかるのは…

スパムトラップは、一般的に他のメールアドレスと区別がつかないように設計されているため、特定のメッセージがスパムトラップに送信されたかどうかを知ることは困難です。トラップヒットしたことを示す指標としては、ドメインまたはIPがブロックリストに掲載されたり、拒否されるメールが増加したりすることが挙げられます。ブロックリストやレピュテーションを監視するツールは、スパムトラップ自体を公開すること

なく（または無効化することなく）、スパムトラップヒットに関する指標を提供できます。

まれに、受信側のドメインがスパムトラップの存在を発表することがあります。これは、DNSでのMXサーバーのホスト名（例：spamtrap.domain.com）、またはアドレスがスパムトラップであることを示すSMTP応答のテキストによって行われる場合があります。

スパムトラップの情報を提供する商用サービスもあります。これらのサービスは、配信モニタリング会社によって提供され、独自のスパムトラップネットワークを持っています。ネットワークはブロックには使用されず、配信モニタリング会社の顧客が自分のメールがこれらのトラップにどれだけ送信されているかを確認できるようにするために使用されます。

## 意図しないトラップの公開

トラップ運用者は、一般的にトラップを公開しようとはしません。有用なデータを生成できるトラップを作成し維持するには、多大な投資が必要です。運用者は、一度公開されると、トラップの存在に関する知識が急速に広まり、トラップの有効性が低下すると想定しなければなりません。

調査と修復の過程で、ESPまたはその担当者が、スパムトラップのIPアドレス、ドメイン、またはネットワークのIDを誤って発見することがあります。必要な隠密作戦を維持するために、ESPは、このデータの機密性を維持するためにあらゆる適切な措置を講じる必要があります。

顧客とのコミュニケーションでは、トラップやネットワークを特定できる情報の明示的または暗示的な開示をしてはならず、**ESP**による当該データの取り扱いは「知る必要がある人」に限定して行うべきです。

トラップまたはネットワークに関する識別データが開示され、トラップ運用者の身元がわかっている場合は、トラップ運用者に通知するのが賢明な場合があります。運用者にトラップが侵害された可能性があることを知らせることで、運用者はネットワークの有効性を維持するために必要な措置を講じることができます。トラップ運用者に通知することで、ESPがネットワーク所有者との良好な関係を確立または維持するのにも役立つ場合があります。

## 問題への対処

### 顧客への通知

ESPは、トラップヒットしたという証拠がある場合は、顧客に通知する責任があります。顧客に通知する際の考慮事項をいくつか紹介します。

### 取得監査

スパムトラップの配信に関する問題では、通常、スパムトラップアドレスが送信者のデータベースに含まれることを許した取得手順の監査が必要です。このような監査は、必然的に、M3AAAWG Vetting Best Common Practicesドキュメントに詳述されているリスト審査手順に似ています。ただし、監査のいくつか

の側面では、よりきめ細かいアプローチが必要となり、以下のような考慮事項が含まれます:

- 連絡先リストがどのように作成されたのか - 取得プロセスの監査では、主に各連絡先リスト内の受信者を取得および検証するために使用された方法に焦点を当てる必要があります。
- 送信者がスパムトラップに初めて送信した時期はいつか、またその事象を特定の配信や配信リストと関連付け、レビュー対象とすることは可能か
- IPまたはドメインがブロックリストに掲載されたのがトラップイベントの結果なのか、またそこからどのような種類のトラップが関係しているかを推測することは可能か
- 問題となっているセグメントの中で、特定のドメインが不自然に多く、リストポイズニングやハーベスティングの傾向を示していないか

- リストの所有者はリストを再構築し、受信者から新たに許可を取得する意思と能力があるか
- 過去の送信によるブロックリストへの掲載履歴があるか、またある場合はどのように解決されたか
- リスト所有者は、問題のあるデータのソースを特定し、そのソースを通じて取得したすべてのデータを削除することができるか
- メッセージの送信に使用されたESPは、スパムトラップネットワークの所有者から追加データを取得できるか

顧客の最初の審査と同様に、監査の過程で調査すべき重要な領域には、アドレスの収集、検証、およびクリーニングが含まれます。

## リストクリーニング

M3AAWGのSender Best Common Practicesで概説されているように、ESPは、受信者アドレスが正しく処理され、必要に応じて削除されていることを確実にするため、すべてのフィードバックループ、バウンス、および購読解除処理を確認する必要があります。

ESPはスパムトラップにメールを送信するリスクを軽減するために、顧客のリストの品質管理方法を確認する必要があります。送信者ベストコモンプラクティスを遵守することで、スパムトラップヒットの減少につなげることができます。遵守すべき事項は以下のとおりです:

- 特定のドメイン内にて受信者による活動またはエンゲージメントが平均よりも低い場合は、スパムトラップネットワークを示している可能性があります。そのドメインを使っているアドレスの取得を特定の配信リスト、または取得方法と関連付けることができる場合は、これらのリストを改善の候補とし、現状の方法での取得は中止する必要があります。

- 送信者は、長期間にわたってメールを開封しない、あるいは配信できない受信者への送信を抑制するポリシーの導入を検討すべきです。これにより、これらのアドレスがリサイクルトラップに変換された場合に、将来のトラップヒットの可能性を最小限に抑えることができます。トラップヒットの発生率が現在のレベルで続く場合は、送信者は既存のポリシーを調整して、より積極的なものにすることを検討できます。

- 配信リストのセグメンテーションに用いる条件や、配信停止リストの管理方法を変更した場合、スパムトラップヒット率の増加を招く可能性があり、常に綿密に監視する必要があります。変更の結

果、長期間送信されていなかった一部の受信者にメールが送信される場合、その間にアドレスが廃止され、スパムトラップとして再利用されている可能性があるため、特に注意が必要です。

いずれにしても、スパムトラップヒットが多い顧客またはリストは、徹底的な再審査の候補とするべきです。顧客またはリストがすでに厳格な審査プロセスを経ている場合は、以下のような変更がスパムトラップ活動の活発化に関与している可能性があります:

- 顧客の組織で人事異動はありましたか？
- 新しいAPIの実装、または既存のAPIの仕様変更により、APIが悪用された可能性はありますか？
- 顧客のアドレス収集箇所に変更があり、悪用可能なウェブフォームやリストポイズニングを示唆している可能性はありますか？
- 合併や買収活動、ビジネスモデルの変更など、顧客の徹底的な再審査の必要性がある広範な組織変更はありましたか？

**ESP**は時折、改善を拒否するクライアントを抱えることがあります。そのような場合、改善を拒否する顧客との契約を終了することが強く推奨されており、加えて、その顧客に対しては本来提供される可能性のある情報を制限することも検討すべきです。

## 将来のインシデントを最小限に抑える

### アドレス収集方法

ESPは懸念すべき点を特定するために、顧客のアドレス収集手段を確認する必要があります。収集方法によっては、利用者本人のメールアドレスであることを確認する仕組みなしに共有するよう促す場合があります。これらの方法は多くの場合、リストにスパムトラップをもたらします。リスクの高い収集方法には、以下のようなものがあります:

- 報酬付きのサインアップ
- ソーシャルメディアのサインアップ
- 友達紹介フォーム
- 懸賞

これらの方法を用いた場合、収集されたアドレスは「質より量」を優先するため、結果として質の低いリストにつながります。

また、スパムトラップは他にも次のような方法でリストに載ることがあります:

- 販売時点での入力ミスによる誤字脱字
- （自動または手動にかかわらず）Webサイトから収集されたアドレス
- 購入、レンタル、またはアペンディングされたリスト
- 展示会参加者リスト
- シングルオプトインのサインアップフォーム

アドレス収集方法の調査中に、ESPは顧客に特定のオプトインデータを要求すべきです。 一般的な調査手法は、リストにないアドレスを含め、複数のアドレスを顧客に提供することです。 顧客は、以下のオプトインデータを提供するよう求められます:

- サインアップの日時
- （サインアップがオンラインで行われた場合）使用されたフォームのURLと接続IP
- （対面でアドレスが収集された場合）取引の場所

顧客はWebフォームのURLを含めた特定のオプトインデータを提供できる必要があります。スパムトラップは、自動フォーム送信によってリストに追加されることがあるため、顧客とESPはWebサイトのトラフィックの分析を実施する必要があります。従来とは異なるトラフィックや不自然な配信量の増加は、ボットによって標的にされたフォームを示している可能性があり、リスト上のスパムトラップの増加につながります。

ESPはまた、オプトインプロセスが意図したとおりに機能しているかどうかを確認することもできます。監査時にリスト所有者から提供されたURLでのサインアップにより、検証可能な購読が行われますか？そうでない場合は、提供されたURLがリスト所有者のものではない、またはそのページからのサインアップが多数の間で共有されている可能性を検討してください。確認する仕組みが存在し、意図したとおりに機能しているかどうかを検証します。

## 収集時点での検証

データ収集プロセスをより優れたものにする対策の一環として、メールアドレスの検証があげられます。このような検証はESPでの内部レビュー、またはアドレス収集時もしくは要求に応じて検証を提供する多数のサービスのいずれかによって実施できます。ベストプラクティスは、メールアドレスが入力されたときに検証し、検証に失敗した場合は購読者にアドレスの再入力を促すことです。

リスト所有者が独自で検証を行う場合、ESPがリストを確認する際に、対策が不十分または存在しないことを示唆することがいくつかあります。M3AAWG Vetting Best Common Practicesは、これらの対策の包括的な概要を提供します。

## 追加の防止対策

将来的な課題を減らすために検討すべき追加の対応としては、顧客の宛先リスト導入方法を制限することが挙げられます。例えば、ESPが提供するフォームスクリプトを通じてのみ追加を許可する、あるいはその他の特定のプロセスを経由させるといった方法です。

他にも、エンゲージメントのある宛先へのみ送信ができるようにする、送信者にエンゲージメントの履歴がほとんどない宛先を削除や抑制するよう要求したりすることも挙げられます。また、送信者は許可のない宛先を破棄する必要がありますが、許可の再取得を試みることは許容される場合があります。

クライアントが共有環境内でプロビジョニングされている場合は、同じ共有環境を使用している他の送信者のレピュテーションの悪化の可能性を最小限に抑えるために、そのクライアントを専用環境に分離する必要がある場合があります。

## 結論

システムがスパムトラップに引っかかった際に、考慮すべきことはたくさんあります。ESPは自社の配信システムやインフラを保護する必要がありますが、それらのトラップに引っかかってしまった顧客を評価する必要もあります。結局のところ、スパムトラップ自体は問題ではなく、顧客のアドレス取得と検証に根本的な問題があることを示す兆候なのです。スパムトラップは、不適切なアドレス収集手法を特定する方法です。トラップ自体は、リスト上にメール受信の承諾を得ていないアドレスがあることを示すマー

カーです。多くの場合、これらの承諾を得ていないアドレスは、現在スパムを受信している実際のユーザーのものです。スパムトラップにつながる収集プロセスを修正することで、実在の人々に影響を与えているスパムにも対処できます。最も重視すべきは、何よりもまずスパムを受け取っている受信者です。効果的な対策はたくさんありますが、このドキュメントは問題解決の出発点となります。

## 参考情報

- M3AAWGのウェブサイトで『Documents for Senders and ESPs | 送信者およびESP向けのドキュメント』を参照してください。
  https://www.m3aawg.org/documents-for-senders-and-esps
  特に以下の3文書をご確認ください。
- M³AAWG Sender Best Common Practices, version 3.0, updated February 2015
  https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf
- M³AAWG Best Current Practices for Building and Operating a Spam Trap, version 1.2.0, updated August 2016
  https://www.m3aawg.org/documents/en/m3aawg-best-current-practices-for-building-and-operating-a-spamtrap-ver-120
- Vetting Best Common Practices (BCP), November 2011
  https://www.m3aawg.org/sites/default/files/document/MAAWG_Vetting_BCP_2011-11.pdf

M3AAWGが公開する全ての文書と同様に、アップデートに関してはM3AAWGのウェブサイト（www.m3aawg.org）を確認してください。

© 2023 Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) M3AAWG-141