Messaging, Malware and Mobile Anti-Abuse Working Group

ヘルプ — ブロックリストに登録された

2018 年 2 月版 バージョン 1.0.1（2014 年 6 月）

このドキュメントの短縮 URL： www.m3aawg.org/BlocklistHelp

目次

このバージョンの更新内容 1
エグゼクティブサマリー 1
序論 2
ブロックリストとは 2
ブロックリストポリシー 3
リスティングへの対応 4
ステップ 1：発見 6
ステップ 2：ブロック影響評価 7
ステップ 3：行動を取る（または行動を取らないことを選択する） 9
ステップ 4：取った行動 / 解決を伝える 10
結論 11
付録 A - 一般的なブロックリストのリスティングポリシー 12
スパムトラフィック 12
マルウェアトラフィック 12
オープンプロキシ / オープンメールリレー 12
組織的 / ROKSO リスティング 12

このバージョンの更新内容

明快さを改善し文書を更新するために 2018 年 2 月版で軽微な変更を行った。

エグゼクティブサマリー

ほとんど全ての電子メールシステムは、ブロックリストに送信 IP またはドメインが含まれていると、ある時点で配信の問題が発生します。これには、電子メールサービスプロバイダとネットワーク事業者が含まれます。メールがどこでブロックされたかによって、これらのリスティングはブロックされた会社内で広範なパニックを引き起こす可能性があります。ブロックに緊急度を付けて対応する方法を知ることで、タイムリーな解決を保証することができます。この文書では、送信者の IP アドレスまたはドメインに対して能動的なブロックが適用されるため、特に配信エラーに対処します。

ブロックリストに含まれている IP またはドメインを修復するためには、いくつかの手順を実行する必要があります。

1. ブロックリストに登録されていることを確認する。
    a. メールが失敗した理由とそれがリスティングに起因する理由を特定する。
    b. リスティングに責任を負う組織を特定する。
    c. デリスティング(リストからの削除) に必要な手順を特定する。
2. リスティングの影響を評価する。
    a. リスティングの結果、どのくらいのメールが届かないかを特定する。
    b. 修復のコストを定量化する。
    c. コストが影響を上回るかどうかを判断する。
3. 行動を取る。
    a. 修復計画を実行するか、
    b. 何もしないことを決定する。
4. （もしあれば）取った行動を伝える。
    a. ブロックリストの所有者へ連絡する。
    b. ブロックリストの所有者へ実行された修復手順を通知する。
    c. ブロックリストからの削除を要求する。

早期発見、確立された緊急手続き、災害対応計画の実施、効果的な社内外のコミュニケーションにより、組織はブロックのビジネスへの影響を最小限に抑えることができます。これらの行動を取ることで、問題を迅速に解決し、デリスティングに向かうことができます。この文書は、ブロックリストの最も一般的な機能、IP やドメインのリスト化の仕組み、所有者が問題を修復し電子メールを配信する能力を回復する方法を記載します。

序論

電子メールを送信したり SMTP サービスを提供しているほとんどすべての組織は、それらがブロックリストに登録されていると、ある時点でメールの配信に失敗します。ESP やネットワーク事業者など、電子メールを送信することに頼っている組織にとっては、ブロックリストへの登録は、実行可能な長期的ソリューションの合理的な議論を妨げる非常事態となり得ます。この文書は、リスティングを検知する方法を説明することによって組織がこれらの状況を計画するのに役立ち、修復の手順を概説します。

多くの組織では、電子メールブロックを経験する際にオプションがあることを認識していません。メール配信の復旧に集中しているため、問題を解決するために必要な最も適切な手順を検討しないことがよくあります。適切な行動方針は、リスティングの事業への影響とブロックリストの要件を満たすことの困難さに左右されます。ブロックリストの基本を理解することで、能動的なリスティングの制約下でも、意思決定と解決の道筋が明確になります。利用可能なオプションを知り、危機に先立って計画を立てることで、問題を解決し、それについてより効果的に伝えることができます。

電子メールがブロックされる理由はたくさんあります。ブロックリストに IP アドレスまたはドメイン名が登録されるのはその 1 つだけです。この文書では、特にブロックリストに登録されることによってブロックされた電子メールを特定し、その影響を判断し、該当するブロックリストの削除プロセスを調査し、適切な場所や時期に削除される一般的なプロセスに焦点を当てています。

ブロックリストとは

一般に、ブロックリストとは、最も単純な形式で、スパム、ウィルスやマルウェアを含む電子メール、不要な SSH 接続など、何らかの形の悪質なトラフィックを発する疑いがある IP アドレスまたはドメイン名のリストです。ブロックリストは、悪意のあるトラフィックや望ましくないトラフィックが意図された受信者に届かないようにするアクセス制御として使用でき、望ましくないトラフィックに見られる IP アドレス、IP

範囲、ドメイン名、URL、その他の特性に基づいています。リストにはさまざまなタイプの情報（IP アドレス、ドメイン名、ASN など）を含めることができますが、この文書では用語を簡潔にするために、以下の説明では「IP アドレス」に言及します。ドメイン名、URL、その他の情報が含まれているリストを扱う場合、読み手はその情報タイプを知的に「IP アドレス」と置き換えるべきです。電子メールのコンテキストでは、ブロックリストは、迷惑メール、ウィルス、またはフィッシングメールがエンドユーザに届かないように、受信メールシステムによって使用されるデータを識別する集まりです。リスト化された IP アドレスまたはドメイン名からの着信電子メールの接続を拒否することによって保護されます。

リストの多様性、リスティングポリシー、デリスティング要件などにより、さまざまなブロックリストポリシーの詳細を記述することはできません。「典型的な」リストはありません。この文書では、ブロックリストによって引き起こされた電子メールの停止を特定し、原因を調査し、必要な削除手順を特定し、リストから削除される一般的なプロセスに焦点を当てています。

ブロックリストには 2 つの主要な種類がある：内部（プライベート）と外部（サードパーティ）のブロックリスト：

- 内部ブロックリストは、メールを受信するグループまたはメールボックスプロバイダによって直接管理されるリストです。内部リストからブロックを解決するには、リスト者[1]は自分のメールをブロックしているエンティティと直接連絡する必要がある。内部リストの管理者は、自分のネットワークを保護する責任があり、彼らは雇用主とエンドユーザを満足させようとします。
- 外部リストは、サードパーティによって管理されています。デリスティングは、リストを使用しているメールボックスプロバイダではなく、リストを作成しているエンティティと連絡する必要があります。外部ブロックリストには、さまざまな運用者や管理スタイルがあります。一部は有給職員と商用で、他の人はボランティア、またはおそらく単一のボランティア/愛好家を雇っています。外部リスト管理者は、リストを使用してメールボックスプロバイダを満足させようとします。また、公開されているポリシーページもあり、その多くは IP アドレスをデリスティングするための方法を提供しています。

送信行為に関係しない特別な種類のリストが 1 つあります。これらの「情報」リストは、「悪い」送信者をブロックするためには使用されません；代わりに、送信者の動作に基づかないローカルポリシーを適用するために使用されます。情報リストには、ロケーションベースのリスト、「ダイナミック」または「レジデンシャルクラス」IP アドレスのリスト、正しく設定された RFC-2142[2]ロールアカウントを持たないドメイン名のリスト、または ASN[3]ルーティングリストが含まれます。情報リストの場合、デリスティングはめったな選択肢ではありません。リスト内のエンティティが誤って分類されている場合のみ、デリスティングが行われます。

ブロックリストポリシー

各ブロックリストには、IP アドレスの追加または削除のための独自の基準があります。多くのリストは、自分のウェブサイト上にリスティングの基準を記載しています。しかし、一般的には、「リスト者」はリストに登録された理由を正確に知るためにブロックリストを運営している人に頼ることはできません。「リスト者」は一般的に利用可能な情報を使用して、特定の情報のためにリストの担当者に頼ることなく、リスティングの問題を解決することが期待されます。リスト運営者からのサポートの欠如は、トラブルシューティングに重要なリスティングの背後にある方法と理由を理解することになります。

多くのブロックリストは受動的な検出技術に依存しています。これらのブロックリストは、リスト化する IP アドレスを探すためにネットワークを積極的にスキャンしません。むしろ、リスティングは、受信側のネットワークで見られる電子メール送信者の行動の結果です；

[1] 「リスト者」という用語は、ブロックリストにある IP またはその他のエントリを管理する権限を持つ人物またはエンティティを指します。
[2] IETF RFC2142, Mailbox Names for Common Services, Roles and Functions, https://www.rfc-editor.org/rfc/rfc2142.txt
[3] ASN (Autonomous system), https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

すなわち、受信ネットワークの禁止された動作のポリシー内にあるようにみえるエンティティによって制御される着信 IP アドレスまたはドメイン。内部リストの場合、その組織に送信されたトラフィックはブロックリストを更新する基準として使用されます。外部リストの場合、情報はブロックリストのネットワークから、またユーザのネットワークから提供される共有情報から収集されます。受動型検出技術は、通常、メールを要求しなかった受信者に送信されるメールに適用されます。多くの場合、これらの「受信者」は実際には自動化されたスパムトラップです。しかし、場合によっては、メールを要求しなかった個人に直接送信されたメールがリスティングのきっかけになることがあります。リスト化する IP を見つけるための能動型検出方法に依存するブロックリストがいくつかあります。これらの手法には、オープンリレーやオープンプロキシスキャン、ユーザの推薦、新たに利用開始された IP を探す ASN モニタリングなどがあります。他の種類のリストは、新たに登録されたドメイン名および新しいドメインに関する報告を監視します。位置または特性に基づくリストは、通常は能動的な検出技術に依存します。例えば、動的に割り当てられた IP アドレスをターゲットとするリストは、特定の単語または DNS 逆引きの形式を含むすべての IP 空間をリスト化することができます。リストはあらかじめ作成されているか、または、その場で決定し作成されることに留意すべきです。送信者の運用への影響は、通常、リストの作成方法に依存しません。

IP が一般に公開されているリストに掲載されているという理由だけで、特定の電子メールの障害がそのリストに関連しているわけではないことを理解することが重要です。グローバル規模で使用される公開リストはほとんどありません。

広く使用されているリストのほとんどは、良好で一貫して適用されるポリシーと明確なデリスティング基準を持つ傾向があります。合理的なポリシーを持たないリスト、またはそれらの説明が不十分なリストは、あまり頻繁に使用されない傾向があり、したがって、通常、「リスト者」との関連性は低いと考えられます。ある種の疑わしいリストは、ローカルの「人気」や、リストの所有者や管理者に何らかの形で関係するメールアプライアンスへ含めるために、地域ベースで採用されるかもしれません。リスティングの重大度については、ステップ 2：ブロック影響評価で詳しく説明します。

内部リストは、特定の受信者のポリシーを実装します。場合によっては、これらのポリシーが送信者に過度に重い負担に見えることがあります。受信システムは、受信ドメインが受け入れたくない電子メールを受け入れるよう強制されないなど、送信ルールを決定する立場にあります。送信者は基本的なロジックを理解できないかもしれないが、リストは受信者に価値を提供していると考えられるべきです。

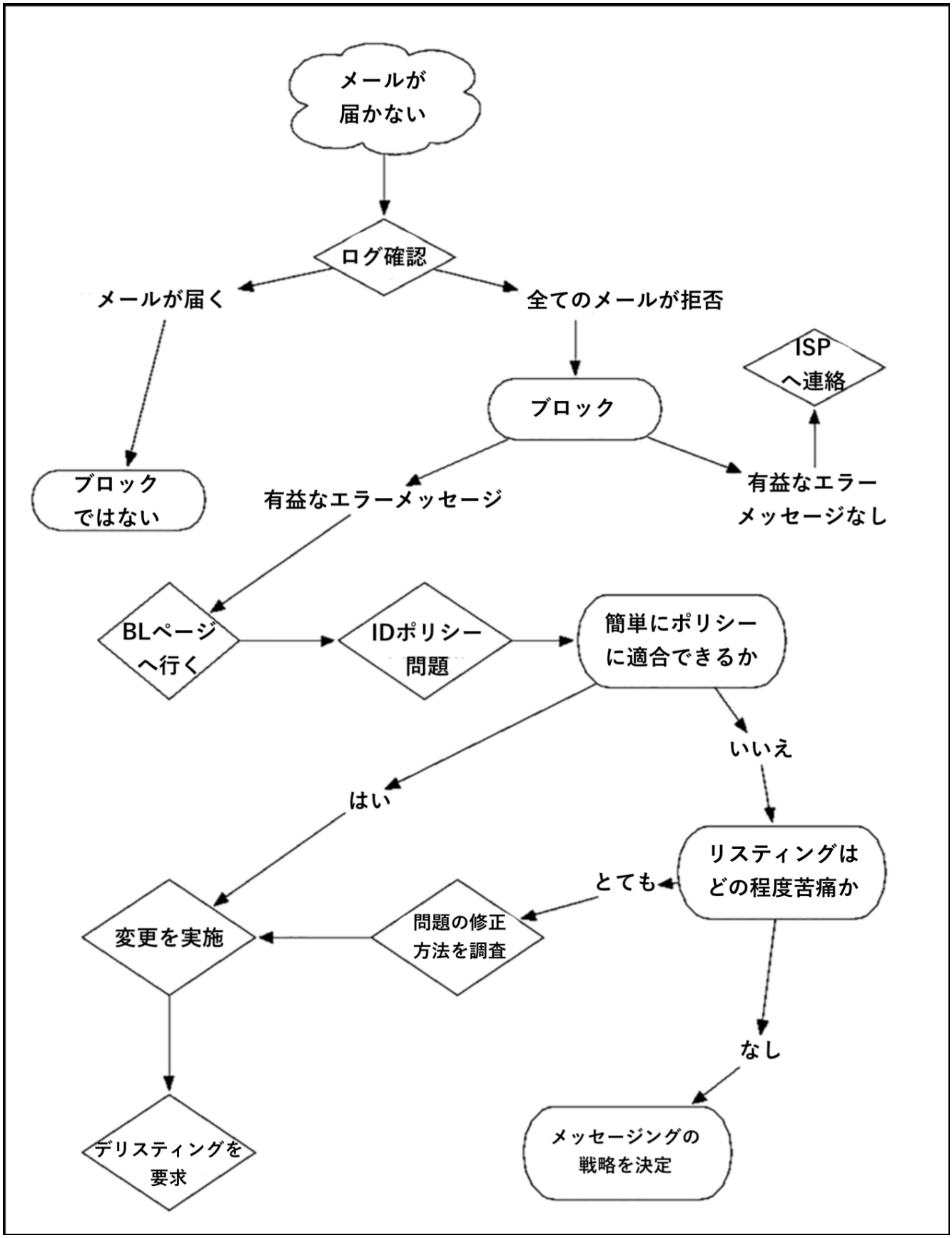
各ブロックリストのポリシーは特有だが、最も一般的なブロックリストポリシーは、付録 A - 一般的なブロックリストのリストポリシーにリスト化されています。

リスティングへの対応

このセクションでは、リスティングの発見、リスティングへの対応方法、連絡方法について説明します。

1. 発見
2. ブロック影響評価
3. 行動を取る（または行動を取らないことを選択する）
4. 取った行動または解決を伝える

次の図は、ブロックリストの検出、応答、修復プロセスを示します。



ステップ 1：発見

ブロックリストに送信 IP やドメインが登録されていることを発見して特定する方法は数多くあります。– これらには、事前検知手法と事後対応方法の両方が含まれます。早期検出監視は、重要な配信の問題を引き起こす前のブロックについて送信者に警告します。場合によっては、送信者はメールが配信されていないことを顧客が気付く前に問題に対処することができます。

早期の警告方法には、「ブロックされた」、「迷惑メール」、その他の識別用語を含む、ブロックリストに共通する用語のメールログを監視することが含まれます。ブロックリストへの包含を事前に特定する別の方法は、リストを直接監視することです。ブロックリストへの登録を事前に特定する別の方法は、リストを直接監視することです。これは外部リストではうまく機能しますが、組織やドメインの外部にはほとんど公開されていない内部リストに対しては不可能またはサポートされない可能性があります。

ほとんどのリストは、リスティングが発生する前に電子メール通知やその他の警告を提供しません。したがって、ブロックリストがネットワークの問題を識別したかどうかを判断するには、効果的なモニタリングを実施することが重要です。組織が提供するインターネットアクセスのタイプに応じて、効果的な監視が必要です。例えば、ネットワークサービスを提供する ISP は、しばしば SMTP キューやログにアクセスすることはできませんが、外部のブロックリストで IP 空間を見つけることができます。他の ISP は SMTP サービスを提供し、キューとメールログを監視できるが、クリックと受信トレイの配置データにはアクセスできません。

ESP プロバイダであれ、メールボックスプロバイダであれ、公開ブロックリストと内部ログ監視の仕組みを定期的にチェックして、ブロッキングやメール配信の問題を特定することを推奨します。これらのチェックには、次のいずれかを含みます：

- 送信メールの返送に関する顧客からの不満
- 外部リストを監視するスクリプトからの通知
- メールを受信しないという顧客/エンドユーザからの苦情
- 配信されなかった電子メールの割合/数
- メールキューがいっぱいで、配送されていない
- その他の集計チェック（開封率/クリック率/顧客転換率）
- 低い受信箱の配置率
- メール配信ログに記録された配信の失敗または遅延の理由に関する具体的詳細
- フィードバックループによるスパムレポート

最良の早期警告監視でさえ、いくつかのリスティングが欠落することがあります。このようなケースでは、電子メールの配信に大きな影響が出るまで、リスティングが検出されないことがあります。
別のウェブサイトは、多くの異なるブロックリストを横断して IP アドレスをチェックする機能を提供します。これらのサイトは、チェックしたリストの品質に関するチェックの量を評価します。すべてのリスティングが重要な配信問題を引き起こすわけではありません。ISP とネットワークの所有者は、公開リストの評判を調べてから、リスティングに責任を負う顧客をどのように扱うかを決定する必要があります。ESP はログファイルを調べて、特定のリストがメール障害の原因であるかどうかを判断する必要があります。

いくつかの配信またはブランド監視会社は、組織の IP とドメインを既知のブロックリストから監視するための商用サービスを提供する場合があります。ブロックリストの中には、信頼できるユーザに直接通知するサービスを提供するものがあります。これはリスト、組織、ユーザによって異なると考えてください。

重要なブロックリストデータフィードを購読することは、登録をチェックする別の方法です。これは、一般に、データベースにリストをロードし、それをネットワーク空間（DNS と IP の両方）と比較することを必要とします。通常、このプロセスは、毎日または時間ごとに自動的に実行するようにスケジュールできます。

このような戦略に投資する前に、メールトラフィックの配信に実際に重要なリストを特定する必要があります。

ステップ 2：ブロック影響評価

ブロックリストに登録されることは必ずしもネットワークや配信の失敗を説明するものではありません。ネットワークの場合、IP ベースのブロックは広範な顧客ベースに影響を与えないため、ネットワークの所有者は個々の顧客に対処することを決定する可能性があります。一方、一部のネットワークブロックは、複数の顧客に影響を与える広範なルーティング障害を引き起こします。このような場合、ネットワークの所有者がブロックに対処しなければならない可能性があり、影響の重大性のために問題の顧客を切断する可能性があります。

ESP の場合、ブロックの影響は別々に測定されます。ブロッキングは、メールの配信にどれだけ影響を与えているかということです。IP がブロックリストに記載されているからといって、すべての配信失敗がそのブロックリストに起因するわけではありません。一部のブロックリストのリスティングと内部的に維持されているリストの間にはかなりの重複部分があります。リスティングが配信に影響を与えるかどうかを判断する最善の方法は、受信したバウンスメッセージと送信サーバによって収集されたログを調べることです。関連するリスティングに関するほとんどの情報が含まれます。一部のバウンスは、どのブロックリストがバウンスを引き起こしたかを示すが、これは必ずしも完全に正確ではありません。

ISP やネットワーク事業者がリスティングの重要性を判断するために求めなければならないいくつかの一般的な質問は次のとおりです：

- 自ネットワークはどこにリスト化されているか？
- このリスティングは、1 人の顧客または複数の顧客に影響を及ぼしているか？
- このリストには、ネットワーク悪用者が他のネットワークから切断されていることが示されているか？
- このリストは、自ネットワーク上の何かがボットやトロイの木馬に感染していることを示しているか？
- このリストには、自ネットワーク上の何かがボットネットのコマンド&コントロール（C&C）サービスを提供していることが示されているか？

感染とトロイの木馬の流行、およびユーザと広範なインターネットへのそれらの重大な影響を考慮すると、ネットワーク上の感染または C&C の存在を示すリストは、すべてのケースで調査および軽減する必要があります。

ESP がリスティングの重要性を判断するために求めなければならないいくつかの一般的な質問は次のとおりです：

- このリスティングは、受信者のかなりの割合のメールをブロックしているか？
- 小規模なドメインだが、送信者と受信者の間に強い関係があるため、1 つの電子メールアドレスに影響を与えるブロックさえも解決するのに十分重要か？
- 解決は可能か？

場合によっては、バウンスはブロックリストやその他の情報源を引用してメールの受信拒否に関する情報を確認することがあるが、誰かが調査するまで情報は存在しません。他のバウンスは、どのブロックリストが関係しているのかを示していない可能性があります。このため、ブロックの調査方法を知ることが重要です。リスト上の特定のエントリの存続期間は変わる可能性があるため、ブロックは時間が経過するだけで消滅し、能動的な介入は必要ありません。リスティングが調査の各段階でまだ有効であることを確認することは賢明です。

リスティングの影響を評価するためのバウンスデータの分析は、複数の方法で行うことができます：

1. 特定のブロックリストが、受信ドメインに関係なく、指定された時間枠内に受信されたすべてのバウンスからなる、指定されたデータセット内の他のブロックリストよりも多く引用されているかどうかを調べる。

2. 関心のあるドメインのみにデータセットを制限する。
3. データセットを特定のリスティングを引用するものに限定して、幅と影響を判断する。

他にも問題の範囲を決める数多くの方法がある；いくつかは、メールを送信するシステムや組織の特有の構造に関連する。

バウンスデータの分析で、あるブロックリストが配信失敗の原因と考えられるが、特定のブロックリストが引用されていない場合、参照ブロックリストと同じ期間内で他のバウンスを探し、引用されたものが明らかになっていない原因と同じであるかどうかを判断することができます。しかし、ブロックリストを引用する 1 つのバウンスタイプと、ブロックリストが非公開のままである別のバウンスタイプとの単なる相関関係は、両方のバウンスタイプが同じリストによるものであることを必ずしも意味しません。

多くの場合、指定されたブロックリストは、リスト者が問題を識別するために使用できるデータを提供します。このデータを取得する手段は数多くあります。以下はその例です：

- 特定のブロックリストには、影響を受けるリスト者へ自動的に通知する正式な通知手順が用意されています。これは、WHOIS で利用可能な連絡先情報、以前に確立されたチャネル、または IP 所有者の不正利用アドレス宛の電子メールの形式でもよい。この通知には、リスト化の理由に関する情報が含まれることがあります。多くの場合、この情報は実用的です。[また、ステップ 3：行動を取る（または行動を取らないことを選択する）のメール管理者と不正利用連絡先については以下を参照してください。]
- 多くのブロックリストは、このデータをウェブサイトで直接利用できるようにしています。ネットワークプロバイダと ESP は、この情報を使用して問題のある顧客を特定することができます。
- リストに登録された当事者は、サイト上のウェブフォームを使用してブロックリストから直接リストデータを要求したり、ブロックリスト運用者が連絡先の電子メールアドレスを提供している場合には、電子メールでリストデータを要求することができます。ブロックリスト運用者と連絡するときは、要求されているものに関してできるだけ簡潔かつ明確にすることが重要です。デリスティングを求める前に実用的なデータを要求することは可能だが、多くのブロックリストは実用的なデータを提供していません。
- 問題のブロックリストに関して、ブロックリストを運用している人員と直接対話することは不可能であり、ブロックリストのすべてのやり取りは自動化された手段で行われます。このような場合、リスト化の基準を理解するためにブロックリストのウェブ情報を徹底的に見直すことが重要です。場合によっては、リストに登録された当事者がリスティングの問題に対処するための適切な方向へ動くのに十分なデータです。

ESP の影響評価では、ブロックリストに具体的に挙げられているブロックされたメールの量を調べることが不可欠です。ブロックされたメールが、特定の IP アドレスが登録されているブロックリストに関連していない場合があります。そのブロックリストから IP アドレスを削除しても、基本的な電子メールの配信問題は修正されません。さらに、ある組織の電子メール配信に重要な特定の受信者サイト以外ではほとんど使用されないリストがあります。

多くの広く使われているブロックリストには合理的なポリシーがあります。しかし、リストが広く使用されていないが、配信に大きな影響を与えている状況では、リスト者にはいくつかのオプションがあります。1 つはリストの基準に合致することだが、どれほど困難であってもリストから削除されます。もう 1 つはリストを使用して組織に直接話し、これらのポリシーが不合理に思える理由と送信者がそれらに従うことができない理由を説明することです。受信側の組織にとってメールが欲しい、または有益な場合、ほとんどの受信者はブロックリストの例外にすることができます。

全体として、特定のリスティングの影響を評価するには、配信失敗の数を分析し、配信失敗が組織のビジネスに与える影響を判断する必要があります。すべての組織やあらゆる状況に合った正しい決断はありません；普遍的に問題になるブロックリストや決して問題にならないブロックリストといったものは存在しないのと同様に。

ステップ 3：行動を取る（または行動を取らないことを選択する）

リスト者がリスティングの原因や働きを認識すると、不正なトラフィックを止めるために多くの行動が取られます。一部の企業は他の企業よりはるかに積極的ですが、最低限、問題のリスト者は、リスティングの全体的な影響、財務的影響、評判の影響と、行動を取らないことの影響を比較する必要があります。

デリスティングと解決の手順はブロックリストごとに異なります；以下のリストは、ブロックリストへの登録を解決するために使用される一連のコモンプラクティスです。（**注**：これらの手順の中には、問題の原因を**正確に**把握する必要があり、実際、それを引き起こした独立したインシデントがあった場合です。）正確な原因がわからない場合、解決することが非常に困難になる可能性があります。

管理者に連絡する際には、丁寧でプロフェッショナルな論調が非常に役立ちます。メッセージには、送信 IP アドレス、時間と日付（該当するタイムゾーンを含む）、配信ログや配信不能メール通知からの情報、不適切な行動を特定するのに役立つ情報の要求が含まれている必要があります。

スパムトラップベースのブロックリストから削除される非常に効果的でないアプローチの 1 つは、スパムトラップアドレスを「メーリングリストから削除する」ことを求めることです。ほとんどのブロックリストは、スパムトラップを根本的なリスト問題の兆候として扱います。リストにスパムトラップアドレスが存在することは、そのリストに送信者からメールを受信することを選択しなかった他のアドレスがあることを示します。単にトラップアドレスを削除しても、選択していない他の受信者アドレスへのメールは停止されません。スパムトラップアドレスを要求すると、実際にはリスティングが長くなることがあります。これは、根本的なリスト問題を解決することに抵抗があり、ブロックリストの動作原理を理解していないことを示しているからです。より良いアプローチは、定期的にクリック開封数やその他の関与指標（エンゲージメントメトリクス）のリストを確認することです。スパムトラップはメッセージを開きません。

ESP や ISP のようなネットワークプロバイダは、問題となる顧客を解約させ、メールインフラをさらに使用されることを防ぐだけで、リスティングに対処することができます。顧客に代わって問題のトラブルシューティングを行う ESP にとって、この状況はより一般的な場合があります。この行動をブロックリスト運営者に明確に伝えることで、リスト化された当事者が問題を重く受け止めて、状況を解決するための迅速な対応がとられたことを知らせることができます。何らかの理由でネットワークプロバイダが顧客を単に解約させることを選択しなかった場合、顧客が再びメールを送信可能にする前に、顧客に要求できるいくつかのことがあります。

最も一般的な解決策の 1 つは、顧客にデータベースの全部または一部を確認させることです。完全な再確認とは、受信者が送信者からの電子メールを引き続き受信するかどうかを尋ねる電子メールをデータベースのすべてのメンバーに送信することを意味します。受信者が肯定的に応答する場合、アドレスは将来の電子メールを送信するのに適したものとしてデータベースに保持されます。受信者が肯定的に応答しない場合は、そのアドレス宛へ再度メールをしないでください。部分的な再確認では、送信者は再確認プロセスからセグメントを除外できます。これらのセグメントは、その送信者からの電子メールに最近関与したことが示されている受信者に限定する必要があります。たとえば、メッセージをクリックして短期間（60〜90 日間）に購入した受信者は、再確認から除外することができます。

リスティングを解決する別の戦略は、メーリングリストの特定のセグメントを削除することです。これは通常、送信者がクリーンメールの履歴を持っていても、特定のソースから一連のアドレスをインポートした場合に実行されます。ブロックリストがそのセグメントにトラッキングできる場合は、そのセグメントを完全に削除すると問題が解決する可能性があります。

ウィルスやマルウェア感染によるリスティングの場合、問題を解決する適切な方法は、感染したマシンを実際に修復することです。リスト化された IP が NAT（ネットワークアドレス変換）である場合、これは単一の外部 IP アドレスを使用して複数のマシンをスキャンする際に重要な作業です。許可されたマシンが SMTP 経由、ポート 25 経由、または代替メールポート経由での送信のみを許可するように NAT を設定することは、

リスト化の問題を潜在的に解決する可能性があります。ただし、企業や家庭内のファイアウォール内の感染したマシンの根本的なセキュリティ問題を修正するものではありません。

場合によっては、リスト者はリスティングに対して何の行動も取らないと決めるかもしれません。これを決める理由はいくつかあります。1つは、リスト自体が情報リストであり、IPアドレスまたはドメイン名がリスティングの基準を満たしているということです。組織がリスティングを解決しないことを決定するもう一つの理由は、リスティングが広く使用されていないため、リスティング自体が深刻な配信問題を引き起こしていないことです。最後に、一部の組織は、ブロックリストのデリスティングの条件を遵守するにはあまりにも面倒で問題があると判断します。

ステップ4：取った行動 / 解決を伝える

リスティングの原因が特定され解決されたら、問題のブロックリストに解決策を報告する必要があります。これらの行動をブロックリスト運営者に伝える際には、正直で率直なことが重要です。リスト化された当事者は、行動が通知されても、実際には行動が取られていない場合、一時的なブロックリストが永続的なブロックリストに変わる可能性があることに留意する必要があります。

各ブロックリストには、デリスティングのための独自の推奨通知方法があります。ブロックリストのウェブサイトをチェックし、指示に従ってください。指示に従わなかった場合は、デリスティングが遅れる可能性があります；間違ったデリスティング依頼は放棄されたり、ブロックリストによって処理されることはありません。

ブロックリストが削除要求を受け入れる一般的な方法の1つは、影響を受ける当事者がブロックリストの特定のアドレスに電子メールを送信することです。ほとんどの主要なブロックリストには、内部と外部の両方で、リスト者との対話を訓練された人員による電子メールアドレスが配備されています。これらの電子メールは、十分な関連情報を含め、簡潔にする必要があります。関連情報には以下が含まれます：

- リスト化されているIPアドレスまたはドメイン名
- 問題を解決するために取られた措置の概要
- 変更が完了するまでのタイムライン（完了していない場合）

いくつかのブロックリストは電子メールアドレスの代わりにウェブフォームを提供します。この場合、要求されるすべての情報を記入してください。この場合も、リスト化されているIPアドレスまたはドメイン名を含めることが非常に重要です。ウェブフォームを使用するほとんどのグループは、IPアドレスを含まないデリスティング要求を拒否するために入念に構築していますが、この重要な情報が欠けている提出を受け入れるかもしれません。

特定のブロックリストは、デリスティングの要求を受け入れません。これらのリストが送信者に多くの影響を与えることはほとんどありませんが、送信者はその存在を認識している必要があります。場合によっては、これらのブロックリストには自動有効期限ポリシーがあります。；リスト化の原因となった動作を停止するIPアドレスまたはドメイン名は、一定期間後に自動的に削除されます。他のリストは削除されず、運用者は修正はないと信じています。繰り返しになりますが、これらのリストは、配信に大きな影響を与えるような形では使用されない可能性が高いです。

また、デリスティングに支払いを期待するブロックリストもあります。M³AAWGは、ブロックリスト運営者が任意の形式でデリスティング費用を請求することを強く推奨しません；私たちは、いくつかの緊急の状況下では、リストに登録された当事者が係る費用を支払うことを選択する可能性があることを認識しています。たとえば、デリスティング費用の支払いは、根本的な問題をすばやく特定し、解決し、係る費用を支払うことがない送信者にとって実行可能な選択肢であるかもしれません。しかし、この問題を特定して解決できない場合、送信者は将来のリスティング、そして、将来のデリスティング費用が設定されます。さらに、支払いは繰り返される問題や異なる問題による将来のリスティングを妨げるものではありません。

結論

リスト化を特定する方法を知ることやそれを解決する方法を理解することは、事態を効果的に管理する上で不可欠です。問題の緊急性は、影響を受けるビジネスへの影響と必要な要件を満たす柔軟性によって決まります。ビジネスへの影響は、ブロックリストごとに異なる場合があります。

一貫して適用される合理的なポリシーを持つブロックリストは、最も広く使用される傾向があります。多くの場合、これらのリスト化する当事者はリスティングの基準を公開し、内部調査および対応計画の役に立つリスト化の要因に関する情報を提供することがあります。

リスト化は、スパムトラフィック、マルウェアトラフィック、オープンプロキシ/オープンメールリレー、より主観的にはプロフェッショナルでない送信行為など、さまざまな理由が要因になります。スパムトラフィックは、受信者の苦情（メールの受信を要求していないアドレスに配信されたメール）と無効なアドレスの両方で観測されます。プロフェッショナルでない送信行為には、IP の変更や異なるレンジの多くの IP でのメール拡散、ブロックリストプロバイダに対するあからさまな脅威など、悪用を示す送信パターンが含まれます。

ブロックリスト化に対応するためのビジネス手段を講ずることで、メールが届かないことに伴うストレスの合理的な管理が可能になります。電子メールを送信することをビジネスとする組織にとって、ブロックリストに登録されることは緊急事態となります。あらかじめ定義された発見、分析、行動方針に従って、合理的な議論と実行可能な長期的解決策が提供されます。

付録 A - 一般的なブロックリストのリスティングポリシー

スパムトラフィック

多くの場合、IP アドレス、サーバ、または ISP は、ブロックリストプロバイダによって監視された IP 空間からエンドポイントにスパムを渡した結果としてリスト化されます。最も広く使用されているブロックリストは、迷惑な商業メールまたは迷惑なバルクメール（UCE または UBE）の定義を使用します。一部の ISP は、ユーザが特定の種類のメールや特定のソースからどれくらいのメールを受信するかの判断に基づいてブロックします。これらのブロックは通常動的であり、このドキュメントの範囲外です。

ブロックリストプロバイダは、さまざまな方法を使用してスパムトラフィックを検出します。これらの技術の多くは、決してメールの受信を要求していないアドレス（スパムトラップまたはハニーポットとも呼ばれる）でメールを受信することに依存しています。一部のブロックリストでは、苦情や個々のブロックデータなどの購読者からのデータを使用して、どのアドレスをリストに追加するかを決定します。

マルウェアトラフィック

IP アドレスは、ブロックリストの検出器にウィルスを送信した場合、またはキャプティブ・スパイウェア・プロトコルの活動を分析した結果として表示されます。さらに、ブロックリストは、ブロックリストで操作するファイアウォールに配信されるデータを活用します。

一般的に、知られていないスパムサーバとして使用されている、ゾンビとも呼ばれるウィルスに感染したユーザが含まれ、ホストがハッキングまたは悪用されている疑いがある場合はいつでもリスト化されます。これは、感染したホストがブロックリストに属するテストサーバに接続し、既知のワームコードを悪用しようとした場合に発生します。このように、NAT を利用してネットワークを介してスパムを送信する単一の感染マシンは、LAN 全体からの電子メールをブロックする可能性があります。マルウェアが定期的に発信されると、リスティングがエスカレートします。

URL やその他の文字列がスパムやウィルス攻撃の一部として表示されている可能性に基づいて、リスト化されることもあります。言い換えれば、受信システムは、メールメッセージに見られる様々なトークンを解析し、以前のトラフィックで見られたものに基づいてブロックリストを調整することができます。

オープンプロキシ / オープンメールリレー

一部のブロックリストには、オープンプロキシまたはオープンメールリレーが登録されています。これらのマシンは、送信者に匿名接続を提供します。多くの場合、オープンリレーとオープンプロキシは実際にはウィルスに感染したマシンです。オープンリレーやプロキシが検出される方法はいくつかあります。一般に、オープンリレーとオープンプロキシリストは、オープンリレーまたはオープンプロキシとして登録する前にマシンをテストします。

組織的 / ROKSO[4]リスティング

特定の組織の管理下にあるシステムがリストに登録されている場合は、そのマシンから直接またはそのマシンに直接誘導されるトラフィックに基づく IP アドレスとホスト名のリストが表示されます。これらのリストには、組織の管理下にあるシステムからの悪意あるトラフィックの履歴と、悪質なトラフィックを阻止する永続的かつ効果的な対策を講じていないことが記載されています。組織リストに加えて、ブロックリストの中には、卑劣な詐欺に隣り合わせの長期的な迷惑メール送信の疑いのある人物を非難することに焦点を合わせたものがあります。これらのリスティングは、メールの世界で FBI の「最重要指名手配」に似ており、修復の対象にはなりません。

組織のリスティングは、悪意のあるトラフィックのソースとは完全に別の IP レンジとホスト名に影響する可能性があります。組織リストの 1 つのタイプはエスカレートされたリスティングです。エスカレートされたリスティングを採用しているブロックリストでは、リスティングにリスト者の注目を集めさせるために企業のメールサーバなどの追加の IP をリストに追加することがあります。エスカレートされたリスティングは、プロバイダからプロバイダに乗り移る組織を監視することがあります。

[4] Register of Known Spam Operations http://www.spamhaus.org/rokso 「The Register of Known Spam Operations（ROKSO）は、スパム送信者およびスパムサービスの登録簿であり、スパム送信またはスパムサービスの提供に関して 3 回以上インターネットサービスプロバイダから解除されており、したがって再犯者である。。。ROKSO データベースは、各スパム行為に関する情報とエビデンスを照合して、ISP の不正利用申告窓口と法執行機関を支援しています。」スパムハウスのウェブサイトより。

組織のリスティングには、次のような要因があります：

- リスティング後の迷惑メールの繰り返し
- 迷惑行為の苦情に対する適切な対応の欠如（または苦情への返信の欠如）
- 問題を警告された後、スパマーと知りながらかくまっている。例えば：
  - スパマーの活動にサポートサービスを提供する
  - ある IP レンジから別の IP レンジにユーザを移動してリスティングを回避するプロバイダ
  - 長期間重度の迷惑行為を無視したり、顧客をリスティングから回避するのを支援する意図を積極的に表明しているプロバイダ
  - あるレンジ（通常は 1 つの/24 またはそれ以上）の過剰な IP からスパムが送信された場合
  - 単一の IP アドレスのリストが効果を持たないように見える場合

M³AAWG が公開している全ての文書と同様、この文書の更新については M³AAWG ウェブサイト (www.m3aawg.org) をチェックして下さい。

M3AAWG080

この文書はインターネット協会 (Internet Association Japan) によって産業界への貢献を目的として翻訳されたものです。
http://www.iajapan.org/