メール到達率向上ガイドライン

目次

1. はじめに

「あんなに苦労して作成したメールなのに、受信先で迷惑メール判定されてしまった・・・」

どんなに時間をかけて作成したメールでも、迷惑メール判定され、受信者に届かなくなってしまうと、意味がありません。

「迷惑メールじゃないのになぜ？」

メール配信を担当される方なら、このような思いを一度は抱くことがあるのではないでしょうか。悪意のないメールでも、1 対 1 のメールとは違い、メールマガジンのように一度にたくさんのメールを送る場合、メールが届かないことがよく起きます。

迷惑メールフィルタとしては、受信者を守るために悪質なメール配信者を排除しようとしているだけなのですが、迷惑メールフィルタが、受信者に届く大量のメールをチェックする中で、正当なメールも迷惑メールと勘違いしてしまうケースは珍しくありません。

それでは、迷惑メールフィルタから勘違いされることなく、「このメールは信頼できるメールだ！」と認めてもらうためにはどうしたらいいのでしょうか。

『メール到達率向上ガイドライン』では、正当なメールが正当なメールとしてきちんと受信者に届くことを目指し、メール到達率向上のための対策までを一つずつ解説していきます。

2. まずは特定電子メール法に違反しない内容を！

特定電子メール法とは、広告・宣伝メールを規制対象とした、メール配信についての法律です。特定電子メール法のポイントとなる以下 3 点を守らない広告・宣伝メールは、当然ながら受信者が求めていないコンテンツに直結しますので、受信拒否を受ける可能性も高くなります。

- **オプトインの取得**
- **オプトアウトの運用**
- **送信者情報の記載**

最悪の場合「1 年以下の懲役又は 100 万円以下の罰金（法人は 3000 万円以下の罰金）」が課せられることもありますのでご注意ください。

では、それぞれのポイントについて具体的にみていきましょう。

● オプトインの取得

オプトインとは、「メール配信をする際はあらかじめ相手の同意を得ましょう」という意味を表します。特定電子メール法では、具体的に以下の 2 つが必要となります。

・あらかじめ、広告・宣伝メールの送信が行われることを認識してもらうこと

・それについて賛成の意思を表示してもらうこと

オプトインの取得方法はいくつかありますが、例えばお客様からお問い合せをいただく登録フォームに下記のような設問項目を設けることでオプトインを取得することが出来ます。

- **オプトアウトの運用**

オプトアウトとは「受信者がメールの受け取り拒否を出来るようにしましょう」という意味を指します。

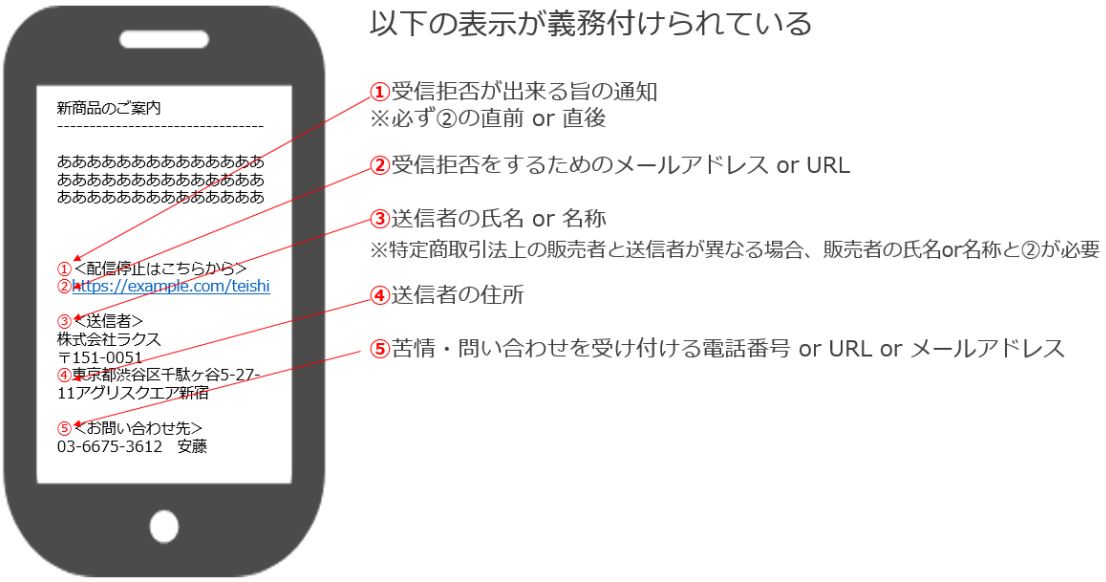
具体的な方法としては、本文に受信拒否の依頼先メールアドレスを記載するなどが挙げられますが、最近ではより簡単にオプトアウトの方法を提供することが推奨されています。

例えば、配配メールでも、広告・宣伝を目的としたメールの本文に、メール受信者が簡単にオプトアウトを行える配信停止 URL を設置することが出来ます。

※配配メールでの解除フォーム設定手順詳細は、ユーザ操作マニュアルをご参照ください。

● 送信者情報の記載

メールを送信する際には、以下のようにオプトアウトの方法以外にも、必ず送信元の所在を明らかにする必要があります。



これらの内容は、広告・宣伝メールでは毎回必ず挿入する必要が出てきますので、予めテンプレート登録すると便利です。

※配配メールでのテンプレートの設定手順はユーザ操作マニュアルをご参照ください。

3. 各種ガイドラインが推奨する設定

迷惑メールと判定を受ける理由は、もし公開してしまうと、その内容をもとに、さらに悪質な迷惑メールが送られてしまう危険性があることから、そのメールが例え本来は正しいメールであっても、明確な理由を知ることはなかなか難しいのが現状です。

しかしながら、どのような条件であれば迷惑メールと誤判定が受けにくくなるのか、各社もガイドラインやポリシーを公開しております。

・Gmail 一括送信ガイドライン

https://support.google.com/mail/answer/81126?hl=ja

・Apple　iCloud メール

メールを一括配信する場合のベストプラクティス

https://support.apple.com/ja-jp/HT204137

・Yahoo!メールガイドライン

https://mail.yahoo.co.jp/info/guidelines/mail.html

-Yahoo!メール迷惑メール対策

https://mail.yahoo.co.jp/info/guidelines/about.html

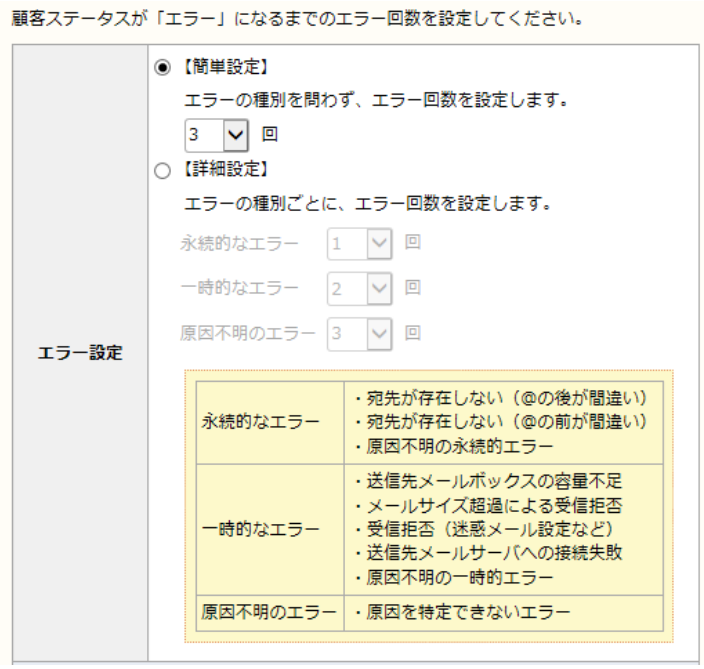
次のページからは、各社が推奨する運用・設定について、まとめて解説していきます。

● リストのクリーニング

配信したメールの宛先で、エラー判定されるメールアドレスが多いと「怪しい送信元」として迷惑メール判定されやすくなります。

そのためにも、配信リストは定期的にクリーニングを行いましょう。

配配メールでは、下図のように「エラー設定」で、過去に送ったメールの中で、累計何回エラーがでたら、ステータスを「エラー」にするか設定することができます。



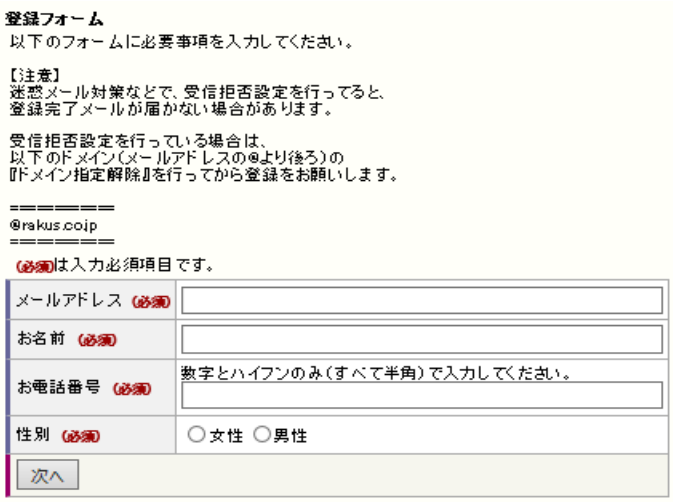
ステータスが「エラー」になったメールアドレスは、自動的に配信対象から外れるようになるので、簡単にリストのクリーニングを行うことができます。

※エラー設定詳細については[ユーザ操作マニュアル]をご参照ください。

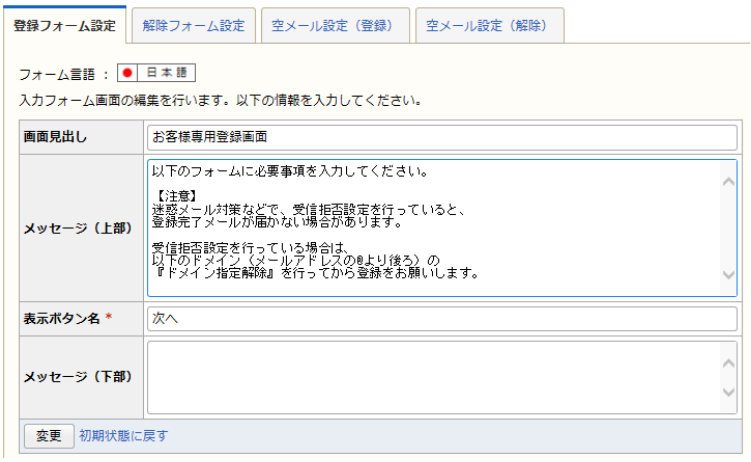
● 受信指定の設定依頼

受信者にメールマガジンの会員登録をしてもらう際、受信者登録用ページに、受信者宛に送るメールマガジンの差出人（From）アドレスのドメインを予め受信指定してもらえるようご案内しましょう。

«登録フォームイメージ»



配配メールで登録フォームを作成する場合も、以下のように受信指定の設定を依頼するご案内文を挿入することができます。



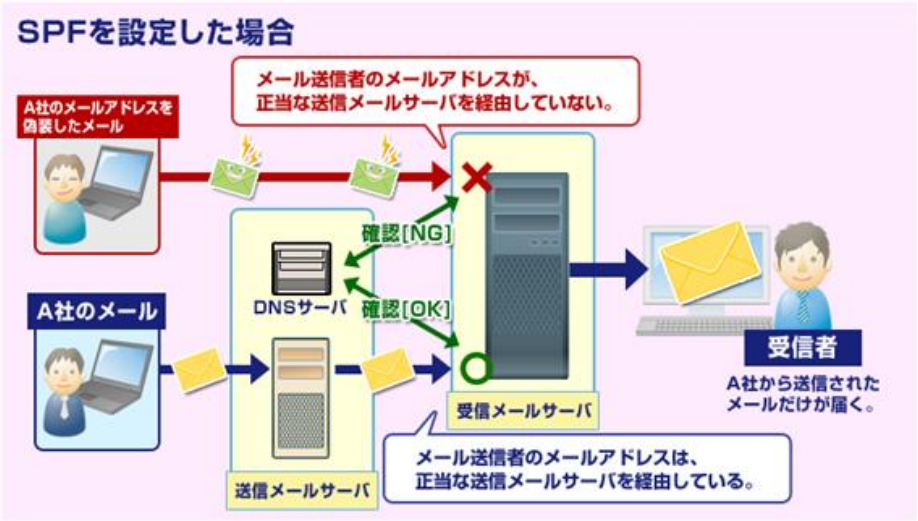
※登録フォームの設定手順詳細はユーザ操作マニュアルをご参照ください。

● SPF レコードの設定

SPF とは、「メールマガジンの From アドレスのドメイン（@マークの右側）に使用しているメールサーバはこれですよ」と DNS サーバ（※）で宣言し、なりすましメールと誤判定されることを防ぐ仕組みのことです。

※DNS サーバとは

インターネット上でのコンピュータの名前にあたる「ドメイン名」を、住所にあたる「IP アドレス」に変換するコンピュータのこと。



▼設定手順

1. SPF 設定が可能か確認

SPF レコードの設定はメールアドレスを運用（設定）しているサーバで設定をする必要があるため、独自ドメインのメールアドレスであれば設定が可能です。

※「差出人アドレス」がプロバイダーのメールアドレスや Yahoo!メール、Gmail 等のフリーメールのメールアドレスである場合には設定できません。

また、独自ドメインでも、サーバ会社によっては設定できないところも稀にあります。

そこでまずは、配配メールからメールを送信するときに「差出人(From)アドレス」に設定しているメールアドレスを確認し、そのメールアドレスを運用（設定）しているシステム担当者、もしくはサーバ会社（※）に SPF の設定ができるか確認しましょう。

（※）ムームードメイン、お名前.com、さくらインターネット　等

2.サーバへ SPF レコードを登録

SPFの設定が可能と分かった場合、設定可能なサーバに以下のSPFレコードを設定しましょう。

▼設定するレコード

TXT "v=spf1 ip4:送信メールサーバの IP アドレス include:spf.haihaimail.jp ~all"

※送信メールサーバの IP アドレスは、配配メールの「From（差出人）」に設定しているメールアドレスを管理しているシステム担当者もしくはサーバ会社に確認してください。

設定方法は、自分で設定する場合とサーバ会社側で設定してもらえる場合があります。まずはサーバ会社に上記レコードを設定したい旨を伝え、設定方法を確認しましょう。

設定例 ）サーバが「お名前.com」の場合

①下記 URL にアクセスしログインする

https://www.onamae.com/navi/domain.html

※「お名前.com」サイトへ移動します。

② 「ドメイン ＞ ドメイン設定 ＞ その他の機能ネームサーバーの設定 ＞ DNS 関連機能の設定」をクリック

③ 対象のドメイン名にチェックをし、「次へ進む」をクリック

④ 【DNS レコード設定を利用する】の「設定する」をクリック

⑤ 【入力】の箇所に以下情報を設定する

TYPE： TXT

VALUE(TARGET)：

v=spf1 ip4:送信メールサーバの IP アドレス include:spf.haihaimail.jp ~all

⑥ 「追加」をクリック

※各サーバー会社の設定例

・お名前.com

https://www.onamae.com/guide/details.php?g=18

・ムームードメイン

http://muumuu-domain.com/?mode=guide&state=muudns_setup

・さくらインターネット

http://support.sakura.ad.jp/manual/rs/domain/spf_record.html

・エックスサーバー

http://www.xserver.ne.jp/manual/man_domain_dns_setting.php

・バリュードメイン

http://www.value-domain.com/howto/?action=moddns

なお、SPF レコードの設定は、上記のようなサーバ会社が管理を行っているため、設定する上での不具合等については、ご自身のメールアドレスを運用（設定）しているサーバー会社にお問い合わせください。

● DKIM 署名の設定

DKIM とは、送信者側でメールに電子署名を付加し、受信者側でその電子署名を照合することで、送信者がなりすましでないかを確認することができる方法です。

DKIM と SPF はどちらも送信者のメールアドレスが正しいものであることを証明するための技術ですが、SPF は送信メールサーバの IP アドレス情報を使用し、正しいメールサーバからメールが送信されているのかをチェックするのに対し、DKIM はメールに付加された電子署名を使用して、メールの送信者情報が正しいのかをチェックします。

また、DKIM 署名には以下の 2 種類があります。

種類	内容	設定のポイント
第三者署名	受信者側はメールの改ざん検出が出来ます	配配メールの管理画面上だけで設定できます
作成者署名	受信者側は送信ドメインの認証と、メールの改ざん検出が出来ます	From に使用するドメインの DNS サーバの TXT レコードに公開鍵を設定する必要があります

「作成者署名」の方がセキュリティ強度は高いのですが若干技術的な難易度も高くなります。

配配メールでは、どちらの設定も可能ですので、まずは簡単な第三者署名を設定してみて、より到達率を改善する必要がある場合には、作成者署名に切り替えるといいでしょう。

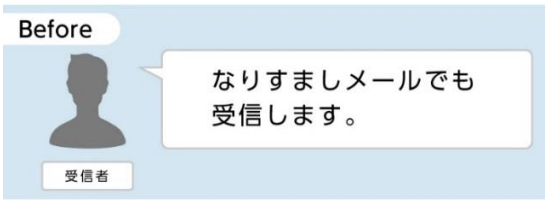
※DKIM 設定の手順詳細はユーザ操作マニュアルをご参照ください。

● DMARC の設定

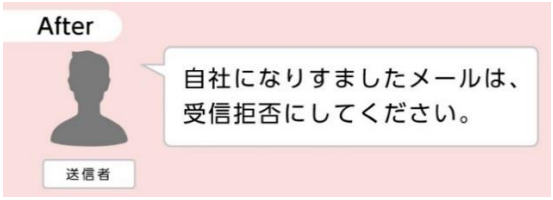
これまでは、送られたメールがなりすましメールだったとしても（SPF・DKIM の認証に失敗した場合でも)、受信側が「受信する」というポリシーだった場合、なりすましメールは受信者の意向に沿って、そのままユーザのメールボックスで受信されていました。

そこで “自社になりすまされたメールは、ユーザに受信させたくない”という要望を満たすために登場したのが、DMARC です。

«DMARC 対応前»



«DMARC 対応後»



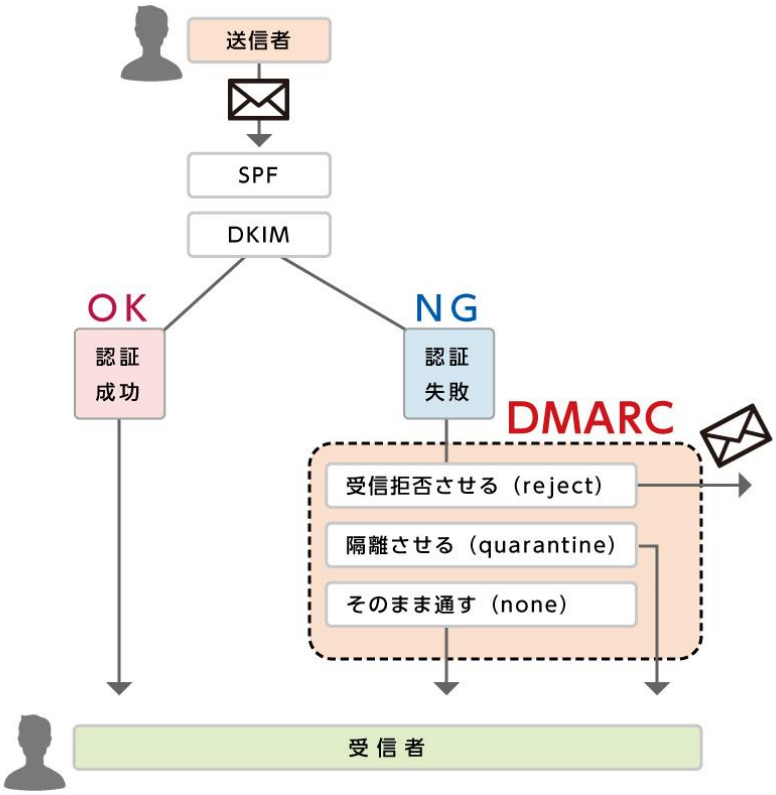
DMARC の設定を行うことで、自社になりすました可能性のあるメール配信が行われた場合に、送信者側の意思で、そのメールの制御を以下の３つのパターンのいずれかを選択することができるようになります。

１.そのまま受信させる（none）

２.隔離させる（quarantine）

３.受信を拒否する（reject）

«DMARC の仕組み»



このように、受信者側ではなく送信者側がそのメールの挙動を管理できるようになる仕組みが、DMARC です。

送信者が DMARC に対応するには、まずは SPF の設定と、DKIM の設定がされていることが前提となります。SPF、DKIM の設定が完了した後、ドメインを管理する DNS サーバーに、DMARC レコードを記載していきます。

具体的な記述方法は以下のサイトを参考にしてください。

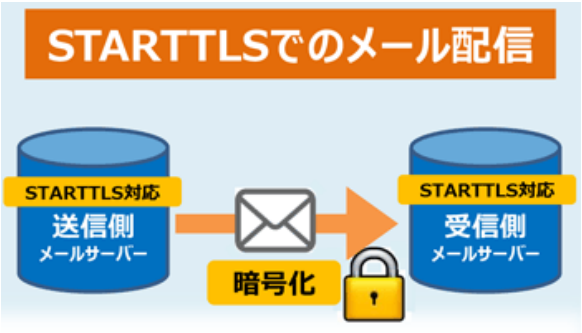
【参考】https://support.google.com/a/answer/2466563?hl=ja

尚、DMARC が機能するためには、メール送信側だけでなく、受信側も DMARC をサポートする必要があります。現状全ての受信サーバーが DMARC に対応しているわけではありませんが、Gmail をはじめ、多くのメールサービスプロバイダが DMARC のサポートを開始しており、Google のガイドラインでも DMARK ポリシーの公開は推奨されています。

- **STARTTLS 対応**

「STARTTLS」とは、メール送信時に SSL/TLS による暗号化を行う方式のことです。
受信側のサーバーが STARTTLS に対応していれば、 メール送信するための通信を自動的に暗号化（SSL/TLS 暗号化） して送信し、よりセキュアなメール送信を行うことができます。

メールソフト大手 Gmail では STARTTLS 対応を積極的に推奨しており、今後、STARTTLS 未対応の場合にメールの到達率に影響してくる可能性があります。



配配メールでは、オプション機能として、STARTTLS 対応にすることが可能です。

ご利用をご希望の場合は、以下よりお申し込みが可能です。

■機能追加オプション：STARTTLS 対応（月額税抜 3,000 円）

https://support.haihaimail.jp/option/index.php

[注意]

- ・STARTTLS に対応するサーバー（Gmail など）へのメール配信は、通常のメール配信より、配信速度が若干低下する場合があります。
- ・添付ファイル付きのメール配信は、STARTTLS ではなく、平文での配信となります。
- ・配信するメールに応じて、STARTTLS の対応有無を選択することはできません。本オプションにお申込みいただきますと、添付ファイル送信を除く、すべてのメール配信は STARTTLS での配信を試みます。
- ・STARTTLS 対応オプションをお申込みいただく場合は、 併せて SPF、DKIM（作成者署名）の設定を推奨します。

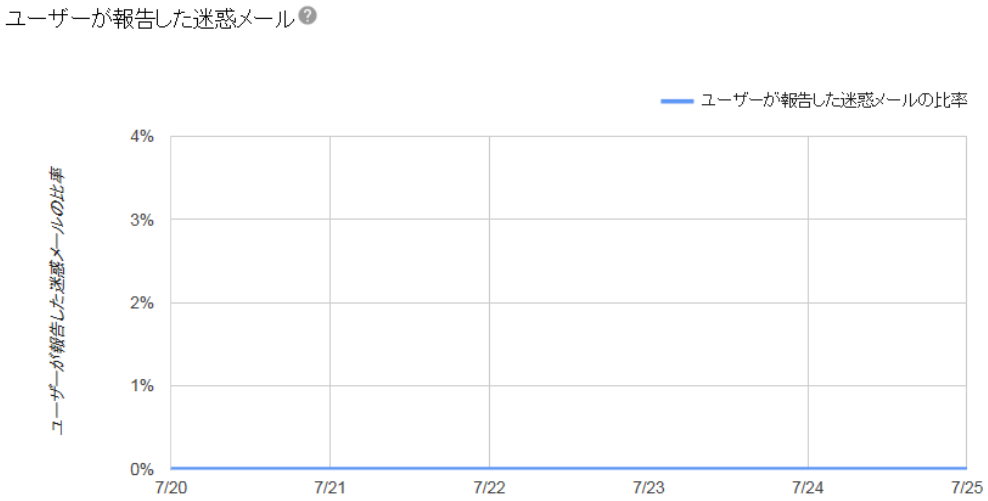
4. 各種チェックサイトのご案内

ここでは、配信したメールがどの程度迷惑メールと判定される可能性がありそうか、簡単に確認出来るチェックサイトを 2 つご紹介します。

● Gmail Postmaster Tools

Gmail Postmaster Tools では、Gmail 宛に配信したメールについて、迷惑メール通報された比率や、配信エラー率等を確認することができます。

迷惑メール率画面見本

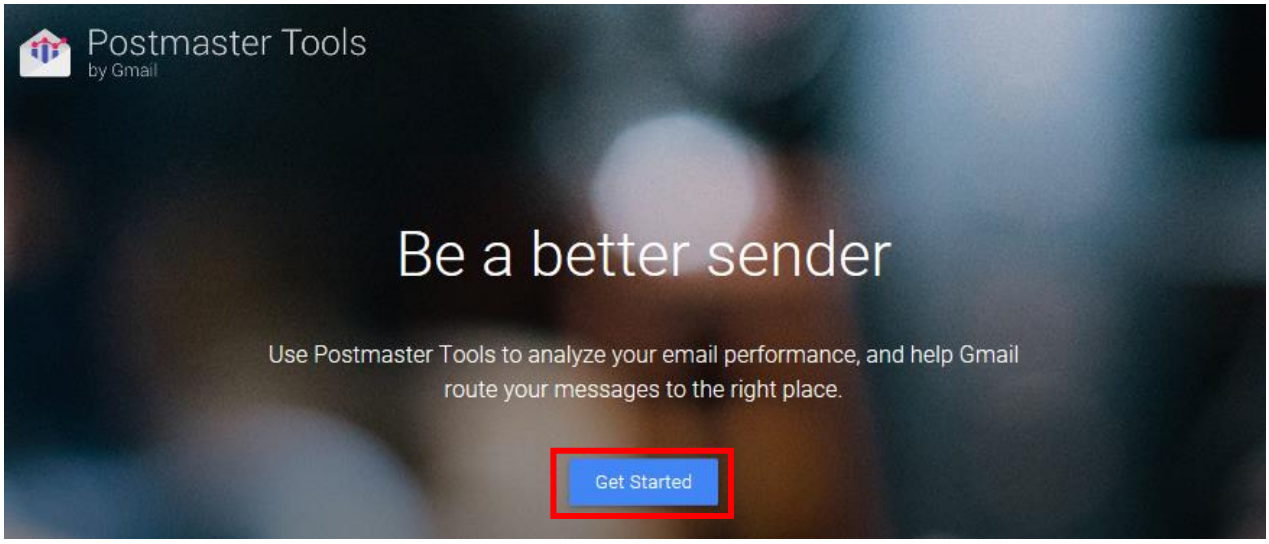


※Postmaster Tools を利用するには、Google アカウントが必要です。

Google アカウントが無い方は、先にアカウントを作成してください。

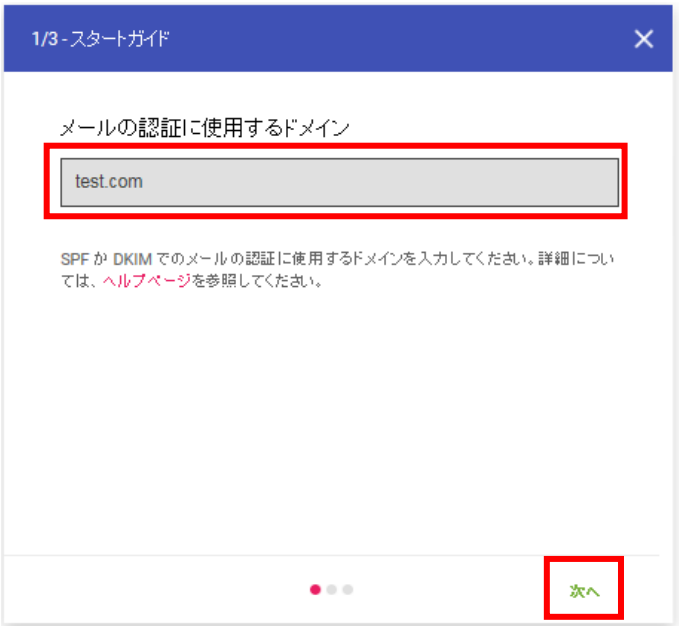
▼設定手順

1.Postmaster Tools のページから「Get Started」をクリック



2.ログイン情報を入力し、「次へ」をクリック

3.登録するドメインを入力し、「次へ」をクリック



4.「google-site-verification=xxxxxxxxxxx」の部分を設定を行うドメインの DNS 設定の TXT レコードへ追加する。

5.DNS の変更が反映された後、「確認」をクリック

※設定を行う DNS によっては、反映までにお時間がかかる可能性があります。

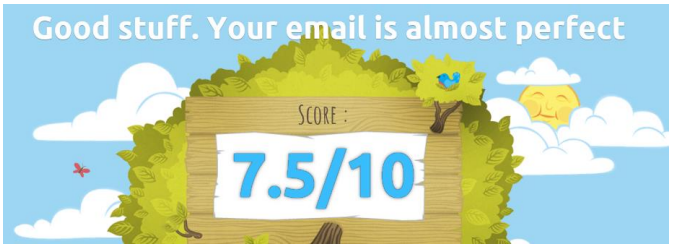
→「Postmaster Tools からドメインの所有権が確認されました。」と表示されます。

完了をクリックし、設定したドメインの箇所をクリックすると、データを確認することができます。

● Mail tester

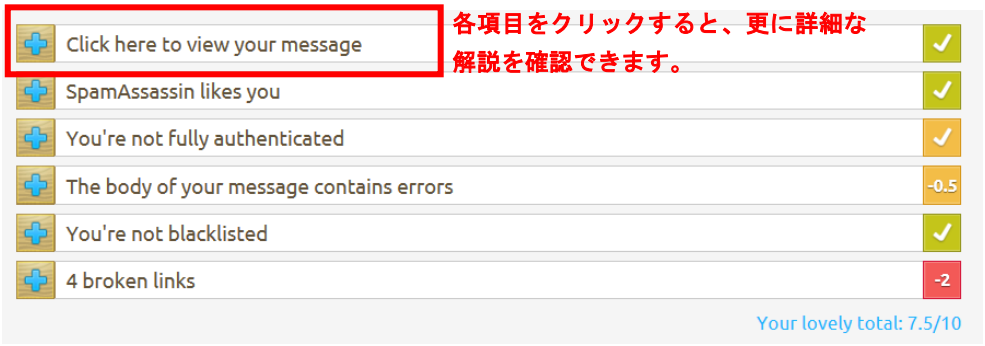
Mail tester とは配信したメールを様々な要素から 10 点満点で評価するサービスです。

※無料版の場合、一日 3 回まで利用できます。



海外のサービスであるため、英語表記とはなりますが、評価項目毎に採点理由が表示されるので、

到達率を上げるためにどの部分を改善すればいいのか、具体的な対策が考えやすくなります。



▼手順

1. Mail tester のページからチェック用の宛先アドレス（下図赤枠内）を確認

2. 上で確認したチェック用の宛先アドレスに、確認したいメールを送信

3. メール送信後、「THEN CHECK YOUR SCORE」をクリック

→採点結果が表示されます。