

メール到達率向上ガイドライン



目次

1.	はじめに	}
2.	まずは特定電子メール法に違反しない内容を!	ŧ
•	オプトインの取得4	F
•	オプトアウトの運用	5
•	送信者情報の記載	;
3.	各種ガイドラインが推奨する設定	7
•	リストのクリーニング	3
•	受信指定の設定依頼)
•	SPF の設定)
•	DKIM 署名の設定	F
•	DMARCの設定	5
•	STARTTLS 対応	7
4.	各種チェックサイトのご案内19)
•	Gmail Postmaster Tools)
•	Mail tester	2



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 オ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。



 電話番号 必須 例) 03-1234-5678 都道府県 必須 - 選択してください− マ 満入予定時期 一 選択してください− ● ご次のを受け取る ● 案内を受け取る 	例)info@rakus.co.jp		
 例) 03-1234-5678 ☞道府県 ☎3 -選択してください- * 記以ールをお知りになったきっかけ Google * Google * 第内を受け取る ※ 案内を受け取る ※ 案内を受け取る ※ 案内を受け取る ※ 案内を受け取らない * (資間などございましたら、お気軽にご記入下さいませ。 	電話番号 () 颜角		
 第道府県 必須 一選択してくださいー 「第入予定時期 一選択してくださいー 「夏択してくださいー 「回 案内を受け取る 「案内を受け取る 「案内を受け取る 「案内を受け取る 「案内を受け取る 「案内を受け取る 「案内を受け取らない ご検討の背景、ご質問などございましたら、お気軽にご記入下さいませ。 	例)03-1234-5678		
 - 選択してくださいー * 記記メールをお知りになったきっかけ - 選択してくださいー * 配記メールをお知りになったきっかけ Google * Google * 案内を受け取る * 案内を受け取る * 案内を受け取る * 案内を受け取らない * ご検討の背景/ご質問 * ご検討の背景、ご質問などございましたら、お気軽にご記入下さいませ。 	郡道府県 <mark>必須</mark>		
ご導入予定時期 配配メールをお知りになったきっかけ - 選択してください- Google キャンペーン・新製品などのご案内 2011 第 ● 案内を受け取る 案内を受け取らない ご検討の背景/ご質問などございましたら、お気軽にご記入下さいませ。 ご入力頂いた個人情報は、「個人情報の取扱いについて」の記載に基づいて適切に管理します。	- 選択してください-		
 - 選択してください - 選択してください - 選択してください - 愛内を受け取る 	二導入予定時期	配配メールをお知りになったきっかけ	
キャンペーン・新製品などのご案内	- 選択してください-	Google	۳
 ・ 案内を受け取る ・ 案内を受け取らない ご検討の背景/ご質問 ご検討の背景、ご質問などございましたら、お気軽にご記入下さいませ。 ご入力頂いた個人情報は、「個人情報の取扱いについて」の記載に基づいて適切に管理します。 	キャンペーン・新製品などのご案内 🜌		
ご検討の背景/ご質問 ご検討の背景、ご質問などございましたら、お気軽にご記入下さいませ。 ご入力頂いた個人情報は、「個人情報の取扱いについて」の記載に基づいて適切に管理します。	● 案内を受け取る	🔵 案内を受け取らない	
ご検討の背景、ご質問などございましたら、お気軽にご記入下さいませ。 こ入力頂いた個人情報は、「個人情報の取扱いについて」の記載に基づいて適切に管理します。	ご検討の背景/ご質問		
ご入力頂いた個人情報は、「個人情報の取扱いについて」の記載に基づいて適切に管理します。	ご検討の背景、ご質問などございました。	ら、お気軽にご記入下さいませ。	
ご入力頂いた個人情報は、「個人情報の取扱いについて」の記載に基づいて適切に管理します。			
	ご入力頂いた個人情報は、「個人情報の取扱いについて」の	記載に基づいて適切に管理します。	
「個人情報の取扱いについて」に同意の上、入力情報を送信して下さい。	「個人情報の取扱いについて」に同意の上、入力情報を送信	して下さい。	

「個人情報の取り扱いについて」に同意して送信

• 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。

顧客ステータスか「エラー」になるまでのエラー回数を設定してください。					
	 【簡単設定】 エラーの種別を問わ 3 <> 回 【詳細設定】 	ず、エラー回数を設定します。			
	エラーの種別ごとに	、エラー回数を設定します。			
	永続的なエラー 1	1 🔽 🛛			
	一時的なエラー 2	2 🗸 🔲			
エラー設定	原因不明のエラー	3 💙 🛛			
	永続的なエラー	 ・宛先が存在しない(@の後が間違い) ・宛先が存在しない(@の前が間違い) ・原因不明の永続的エラー 			
	一時的なエラー	 ・送信先メールボックスの容量不足 ・メールサイズ超過による受信拒否 ・受信拒否(迷惑メール設定など) ・送信先メールサーバへの接続失敗 ・原因不明の一時的エラー 			
	原因不明のエラー	・原因を特定できないエラー			
	1				

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»

登録フォーム						
以下のフォームに必要事項を入力してください。						
【注意】 迷惑メール対策などで、 登録完了メールが届か	【注意】 迷惑メール対策などで、受信拒否設定を行ってると、 登録完了メールが届かない場合があります。					
受信拒否設定を行って 以下のドメイン(メール) IFメイン指定解除』を行	受信拒否設定を行っている場合は、 以下のドメイン(メールアドレスの@より後ろ)の 『ドメイン指定解除』を行ってから登録をお願いします。					
@rakus.cojp = 						
◎●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●						
メールアドレス 🚱 🌆						
お名前 🐼 🏾						
	数字とハイフンのみ(すべて半角)で入力してください。					
お電話番号 (必須)						
性別(必須)	○女性 ○男性					
次へ						

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。

登録フォーム設定	解除フォーム設定	空メール設定(登録)	空メール設定	(解除)	
フォーム言語 : ● 入力フォーム画面の編	日本語 議を行います。以下	の情報を入力してください	۱.,		
画面見出し	お客様専用登録画の	面			
メッセージ(上部)	以下のフォームには 【注意】 迷惑メール対策など 登録完了メール対策など 受信拒否設定を行っ 以下のドメイン公 『ドメイン指定解释	必要事項を入力してくださ どで、受信拒否設定を行っ 面かない場合があります。 っている場合は、 メールアドレスの0より後ろ 余』を行ってから登録をお。	い。 ていると、 う)の 頼いします。		< >
表示ボタン名*	次へ				
メッセージ(下部)					\sim
変更初期状態に	戻す				

※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	
第二老罢夕	受信者側はメールの改ざん検出が出		
- 第二有者石	来ます		
作式老田女	受信者側は送信ドメインの認証と、メ	From に使用するドメインの DNS サーバの TXT レコ	
1F成有者名	ールの改ざん検出が出来ます	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 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

ユーザーが報告した迷惑メール



※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

1/3 -スタートガイド		×
メールの認証に使用するドメイン		
test.com		
SPF か DKIM でのメールの認証に使用する ては、ヘ <mark>ルブページ</mark> を参照してください。	ドメインを入力してください。詳細	細につい
•••		次へ

4. 「google-site-verification=xxxxxxxxx」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。



2/3-ドメイン確認	×
test.comの所有権の確認 1. test.comの <mark>DNS設定にTXT レコードを追加します。</mark>	
TXT レコード: google-site-verification=.	
 2. [確認] センリックしょす。 追加した DNS レコードが認識されると、ドメインの所有権が確認されます。確認 済みの状態を維持するには、確認が完了した後も DNS レコードを削除しないでく たさい(DNS の変更には時間がかかることがあります。また、レコードがすぐに検 出されない場合がありますが、定期的に確認が行われます)。 問題が発生した場合は、CNAME レコードを追加してみてください。 注:確認が完了すると、ご利用のアカウントで Google Search Console のドメイン データにもアクセスできるようになります。 	
戻る ●●● 後で行う 確認	

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。

Click here to view your message	各項目をクリックすると、更に詳細な 解説を確認できます。	/
SpamAssassin likes you		/
You're not fully authenticated		/
The body of your message contains erro	rs	0.5
You're not blacklisted		/
4 broken links		-2
	Your lovely total: 7.5/	/10

▼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。