Gmail送信者ガイドライン変更
対策セミナー

株式会社ラクス

配配メール事業部

楽!ラクス 配配メール

はじめに

いつも配配メールをご利用いただきありがとうございます。

2023年10月Google社よりGmailに関するガイドライン変更の発表がされました。
多くの方に影響のある内容でありながら、詳細が不明瞭な点や、急な記載内容の追記、
また専門的な知識が必要な部分もあり、解読が難しい点も多いかと思います。

そこで、本件の概要および弊社の見解も踏まえて、配配メールユーザの皆様向けに
セミナーを開催させていただくことで、少しでも皆様のご理解が深まり、
その対策に向けて具体的な準備を進めていただくご支援ができればと考えております。

AGENDA

1. Gmail送信者ガイドラインの概要
2. 配信担当者が対応すべきこととは？
3. 配配メールサービスへの影響について
4. まとめ

1. Gmail送信者ガイドラインの概要

Gmail送信者ガイドラインについて

2023年10月にGoogle社が下記を発表しました。

> **重要:** Gmail では 2024 年 2 月以降、Gmail アカウントに 1 日あたり 5,000 件以上のメールを送信する送信者に対し、1. 送信メールを認証すること、2. 未承諾のメールまたは迷惑メールを送信しないようにすること、3. 受信者がメールの配信登録を容易に解除できるようにすること、の 3 つが義務付けられます。詳しくは、1 日あたり 5,000 件以上のメールを送信する場合の要件をご覧ください。

▼原文（Google社）
https://support.google.com/mail/answer/81126?hl=ja

Gmail送信者ガイドラインについて

2024 年 2 月以降、
Gmail アカウントに 1 日あたり **5,000 件以上のメールを送信する送信者**に対し、

①送信メールを認証すること
②未承諾のメールまたは迷惑メールを送信しないようにすること
③受信者がメールの配信登録を容易に解除できるようにすること

の 3 つが義務付けられます

1 日あたり 5,000 件以上のメールを送信する送信者　とは？

・5,000件のカウントは自社ドメイン(@xxx.co.jp)単位

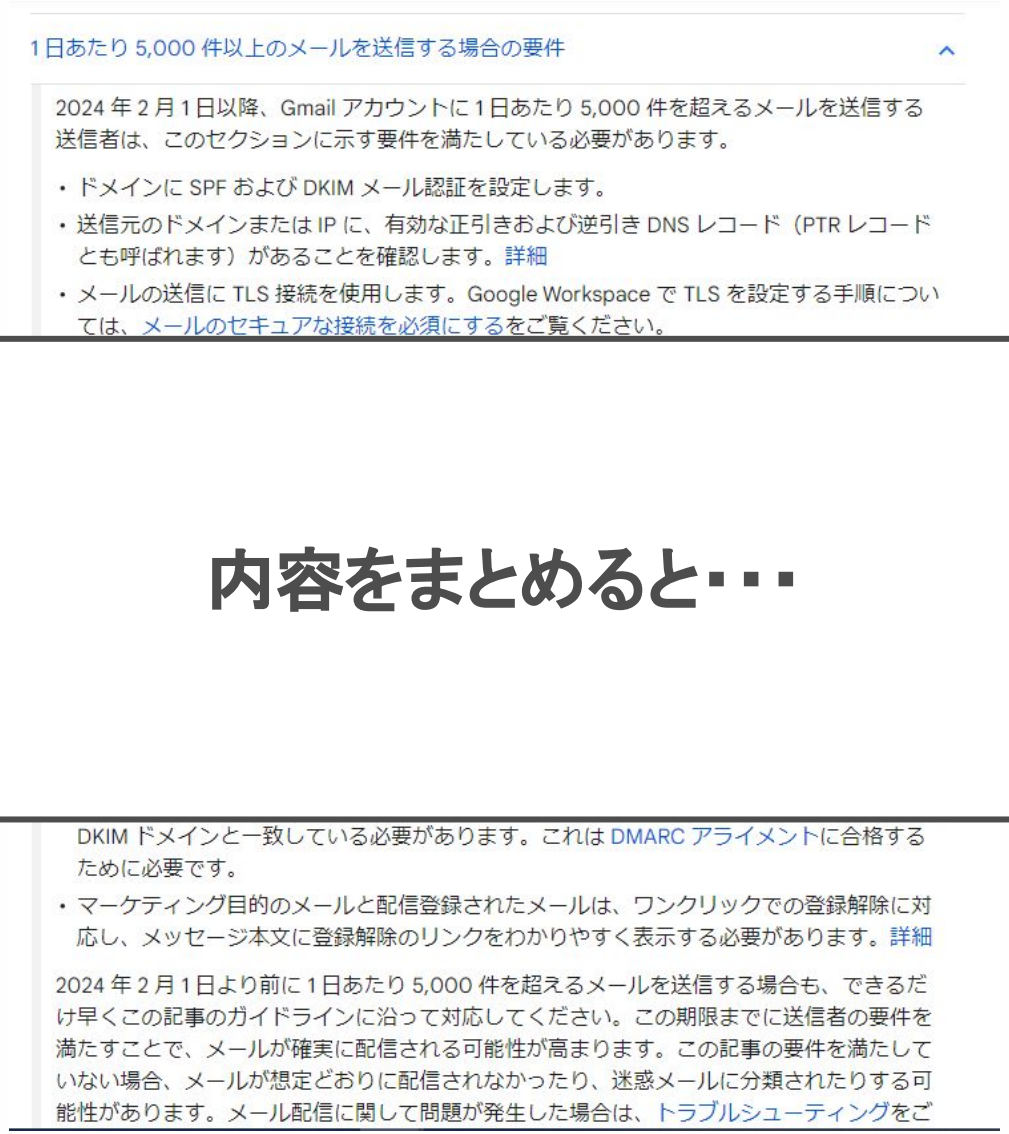
・社内外問わず、xxx@gmail.com宛に送るメールすべてが対象
　送信回数（一括配信）や、社内向け、顧客向け問わず1日5000件以上

・自動送信メールなども対象
　システム入力後に自動でメールが飛ぶ設定がある場合なども注意

・メール施策を行う企業（特にB2C）はほぼ必須

配配メールユーザのみならず、多くの企業に影響のある内容になります

Gmail送信者ガイドラインの概要



1日あたり 5,000 件以上のメールを送信する場合の要件

2024 年 2 月 1 日以降、Gmail アカウントに 1 日あたり 5,000 件を超えるメールを送信する送信者は、このセクションに示す要件を満たしている必要があります。

- ドメインに SPF および DKIM メール認証を設定します。
- 送信元のドメインまたは IP に、有効な正引きおよび逆引き DNS レコード（PTR レコードとも呼ばれます）があることを確認します。詳細
- メールの送信に TLS 接続を使用します。Google Workspace で TLS を設定する手順については、メールのセキュアな接続を必須にするをご覧ください。

DKIM ドメインと一致している必要があります。これは DMARC アライメントに合格するために必要です。

- マーケティング目的のメールと配信登録されたメールは、ワンクリックでの登録解除に対応し、メッセージ本文に登録解除のリンクをわかりやすく表示する必要があります。詳細

2024 年 2 月 1 日より前に 1 日あたり 5,000 件を超えるメールを送信する場合も、できるだけ早くこの記事のガイドラインに沿って対応してください。この期限までに送信者の要件を満たすことで、メールが確実に配信される可能性が高まります。この記事の要件を満たしていない場合、メールが想定どおりに配信されなかったり、迷惑メールに分類されたりする可能性があります。メール配信に関して問題が発生した場合は、トラブルシューティングをご

内容をまとめると・・・

Gmail送信者ガイドラインの概要

【送信担当者側】
① 電子メール認証（SPF・DKIM・DMARC）の必須化
② メール送信にTLS接続を使用する
③ 迷惑メール率を0.3%以下にする
④ 受信者がメールの配信登録を容易に解除できるようにする
⑤ メールサービスプロバイダを利用する

【配信システム側】
⑥ ワンクリックでの登録解除を有効にする
⑦ メールの形式はRFC5322に準拠する
⑧ PTRレコード設定の必須化
⑨ ARCヘッダー設定の必須化

Gmail送信者ガイドラインの概要

【送信担当者側】
① 電子メール認証（SPF・DKIM・DMARC）の必須化
② メール送信にTLS接続を使用する
③ 迷惑メール率を0.3%以下にする
④ 受信者がメールの配信登録を容易に解除できるようにする
⑤ メールサービスプロバイダを利用する

【配信システム側】
⑥ ワンク
⑦ メール
⑧ PTRレ
⑨ ARCヘ

弊社側で対応

Gmail送信者ガイドラインの解説

① 電子メール認証（SPF・DKIM・DMARC）の必須化

メール送信認証である3つ（SPF・DKIM・DMARC）の設定が義務付けています。

※SPF認証とは
電子メールの**送信元ドメインが詐称されていないこと**を確認する仕組み

※DKIM認証とは
メールを送信する際に送信元が電子署名を付け、受信者がそれを検証することで、
送信者のなりすましやメールの改ざんを検知できるようにする仕組み

※DMARC認証とは
SPF・DKIMのうち片方でも認証が通らないケースに対し、
受信者に拒否させる設定などをすることで
送信者自ら第三者のなりすましを防ぎ、メールの信頼性を高める仕組み

Gmail送信者ガイドラインの解説

② メール送信にTLS接続を使用する

暗号化通信であるTLS通信の利用を要求しています。

※TLS通信とは
インターネット上のウェブブラウザとウェブサーバ間でのデータの通信を暗号化し、
安全に送受信させる仕組み

※SSL通信という同様の通信技術と一緒に記載されることも
ありますが、**TLSはSSLの進化バージョン**にあたる一般的なセキュリティ対策です

※配配メールでは**「STARTTLS」オプション（月額3,000円）**で提供しています

Gmail送信者ガイドラインの解説

③ 迷惑メール率を0.3%以下にする

迷惑メールに対する言及は、下記についても開示されています。

▼関連部分を抜粋
・Postmaster Tools* でドメインの迷惑メール率を定期的に監視する
・迷惑メール率を 0.1%未満に維持し、決して 0.3%以上にならないようにする
・迷惑メール率を低く維持すれば、一時的に急上昇してもメールがシステムによって
迷惑メールとしてマークされる可能性が低くなる
・迷惑メール率が高い状態が続くと、迷惑メールへの分類が増加する
・メールの認証確認するために、Gmail アカウントに送信されたメールのチェックを行う
・メールの受け取りを承諾しているユーザーにのみメールを送信するようにする

*Postmaster ToolsはGoogle社が無償提供するGmailアカウント迷惑メール率監視ツール

Gmail送信者ガイドラインの解説

④ 受信者がメールの配信登録を容易に解除できるようにする

受信者がメールの配信解除を簡単にできることを要求しています。
また、マーケティング目的のメールを送信する場合には、
メッセージ本文に登録解除のリンクをわかりやすく表示する必要があります。

※営利目的の広告宣伝メールへの オプトアウト＝解除フォーム設置 は以前より
特定電子メール法で定められています。

※Google基準での”マーケティング目的”の定義やその判別方法は不明

Gmail送信者ガイドラインの解説

⑤ ドメインプロバイダ（独自ドメイン）を利用する

Gmail(xxx@gmail.com)を送信元として配信すると迷惑メール判定や破棄されます。
独自ドメインで配信しましょう。

※独自ドメイン未取得の場合、ドメインの取得をご検討ください。
下記の主要ドメイン取得会社5社については配配メールサポートサイトにも
SPF設定方法を掲載しております。
（お名前.com、さくらインターネット、XSERVER、ムームードメイン、バリュードメイン）

ガイドラインに準拠しなかった場合のリスク

ガイドラインに準拠しなかった場合、以下のようなリスクが発生します

・迷惑メールに分類される可能性が高くなり、**到達率や開封率が低くなる**

・共有IPアドレスを使用する（配配メールなどのメール配信システムを使う）場合、
送信者のアクティビティが使用する他の送信者全体の評価に影響する

・ブラックリストに登録された場合、一斉配信のみならず
すべてのメールが正常に送信できなくなり
Webサイトなどにも影響が出る可能性がある。
（解除申請をしても解除までに数日～数週間以上が必要になる場合が多い）

※ブラックリストについてはセミナー内後半で詳しくお伝えさせていただきます

2. 配信担当者が対応すべきこととは？

Gmail送信者ガイドラインの概要

【送信担当者側】
① 電子メール認証（SPF・DKIM・DMARC）の必須化
② メール送信にTLS接続を使用する
③ 迷惑メール率を0.3%以下にする
④ 受信者がメールの配信登録を容易に解除できるようにする
⑤ メールサービスプロバイダを利用する

【配信システム側】
⑥ ワンク
⑦ メール
⑧ PTRレ
⑨ ARCヘ

弊社側で対応

配信担当者が対応すべきこと

① SPF・DKIM・DMARC の設定を行う

すべての設定を行うことにより迷惑メールに振り分けられる可能性を大幅に減らすことができます。必ず設定をお願いいたします。

SPF　：DNSサーバでの作業
DNSサーバにて配配メールから提供されるSPFレコード情報を記述する。

DKIM　：配配メールでの作業 & DNSサーバでの作業
配配管理画面上にてDKIM署名および鍵を設定する。
DKIMには2つの種類がありますが、原則「作成者署名」の設定が必要です。

DMARC：DNSサーバでの作業
DNSサーバにてDMARCレコード（TXTレコード）を登録する。

それぞれの詳しい説明と設定方法はサポートサイトをご確認ください。

▸サポートサイトはこちら

配信担当者が対応すべきこと

① SPF・DKIM・DMARC の設定を行う

すべての設定を行うことにより迷惑メールに振り分けられる可能性を
大幅に減らすことができます。必ず設定をお願いいたします。

順序としては下記がおすすめです

①配配メールのサポートサイトからSPFの設定情報を取得する
②配配メール管理画面にてDKIM設定を行い設定情報を取得する
③DNSサーバーにてSPFの記載、DKIMの記載とDMARC設定を行う

それぞれの詳しい説明と設定方法はサポートサイトをご確認ください。

▸サポートサイトは[こちら]

配信担当者が対応すべきこと

② メール送信にTLS接続を使用する

TLS接続は配配メールでは STARTTLSオプション（有償）として提供しています。
- **既にご契約中のお客様は追加の対応は不要です**
- **STARTTLSオプション未契約のお客様はオプションの契約をご検討ください**

※代理店経由でご契約のユーザは担当代理店へご連絡をお願いします

TLSの詳しい説明と申込方法はサポートサイトをご確認ください。

▸サポートサイトは**こちら**

配信担当者が対応すべきこと

③ 迷惑メール率を0.3%以下にする

●**特定電子メール法に準拠する**

【ポイント】

・オプトインが取れているリストに送る
・オプトアウト＝解除フォーム を必ず設定する
・送信者表示（送信者情報・連絡先）を入れる

●**その他の有効な方法**

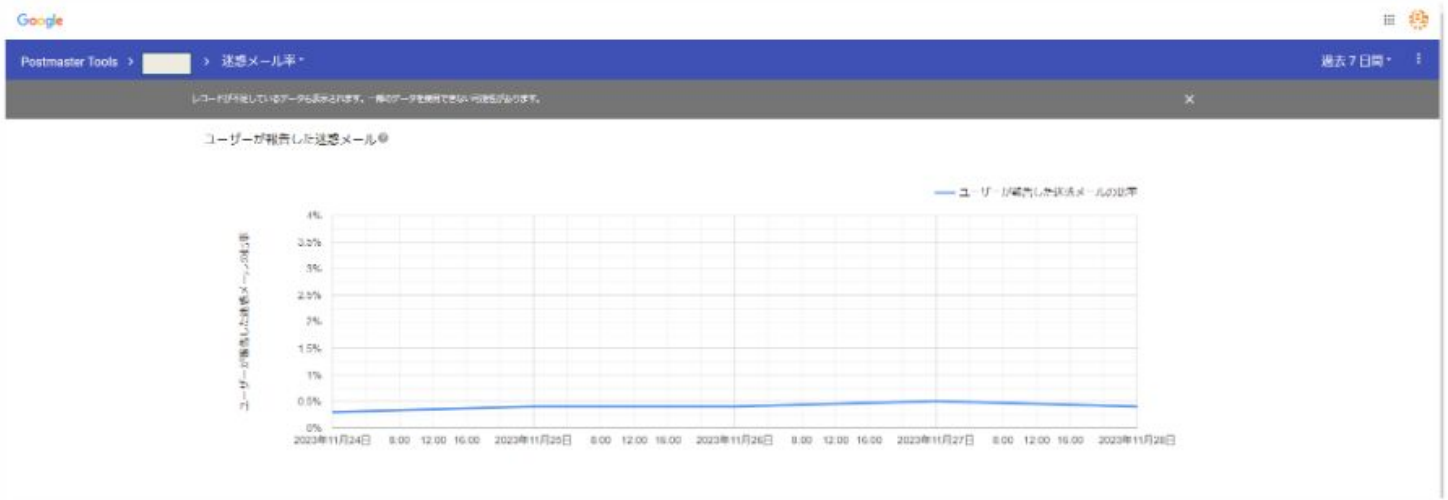
・**リスト内にトラップアドレスがないかチェック**する
　※2024年中に「アドレスクリーニング機能」搭載予定
・リストクリーニングを定期的（目安は月1回）に行う
・古いリストや購入リストは別グループで配信をしながらリストを育てていく

●**Postmastertoolsで定期的に監視する**

▶**参考サイト（配配メールお役立ちコラム：特定電子メール法って何？適用範囲と4つのポイントとは）**

Postmaster Toolsの活用

Google社の ”Postmaster Tools “ を使用すると、送信メールのデータを追跡し
送信ドメインに関するデータを確認することができます。
ダッシュボードで配信エラー、スパムレポート、フィードバック ループなどの詳細がわかります。



ダッシュボード数値の解釈方法はGoogleのページ内に説明があります。

▼Google説明
https://support.google.com/mail/answer/9981691?sjid=16252998857736451022-AP

配信担当者が対応すべきこと

④ 受信者がメールの配信登録を容易に解除できるようにする

営利目的の**広告宣伝メールには解除フォームを必ず設定**しましょう。

※配配メールの**「解除フォーム」機能**をご活用ください
※配配メール以外でオプトアウト管理をしている場合は
リンクなどの解除導線を設置してください
※「ワンクリック登録解除」機能は1月実装予定です

解除フォームの詳しい説明と設定方法はサポートサイトをご確認ください。

▸サポートサイトは**こちら**

配信担当者が対応すべきこと

⑤ メールサービスプロバイダを利用する

ほとんどのユーザ様は既に独自ドメイン利用した配信をして頂いておりますが、
稀にGmail(xxx@gmail.com)を送信元としている方がいらっしゃいます。

Googleや他の大手フリーメーラーについても基本的に送信元として設定することを
推奨していません。**独自ドメインでの配信をお願いします**。

※ドメインとは「support@haihaimail.com」の「haihaimail.com」を指します
※読者からの返信先としてFromアドレスとは別のアドレスを指定したい場合には、
「reply to」設定をご活用ください。

▶サポートサイトは**こちら**

配信担当者が対応すべきこと

その他

・送信ガイドラインとしておすすめの送信方法、避けるべき送信方法についても
Googleのページ内に記載がありますのでご参考ください。

▼原文（Google社）
https://support.google.com/mail/answer/81126?hl=ja

3. 配配メールサービスへの影響について

配配メールサービスへの影響について

本件における、システムへの影響（弊社側での対応）について

【弊社側での対応について】
⑥ ワンクリックでの登録解除を有効にする
⑦ メールの形式はRFC5322に準拠する
⑧ PTRレコード設定の必須化
⑨ ARCヘッダー設定の必須化

➡これらはシステムへの実装が必要なため、**弊社側にて対応**いたします。

1月にリリース予定となっており、これらの詳しい情報は
リリース1週間前までにはマニュアルも含め、
サポートサイトにて公開させていただきますので、
必ずご確認の上ご利用をお願いします。

配配メールサービスへの影響について

本件における、お客様への影響について

①ブラックリストへの影響について

今回のガイドライン変更により、多くの範囲に影響が生じます。
しかしながらGoogleがどの程度の違反措置を実施してくるかは全く読めません。

違反措置として一番可能性が高いのが、**ブラックリスト登録** です。

ブラックリストは一度登録されてしまうと、下記の影響がございます。
- メールを送信しても、**正常に送信ができない**（すべてのメールが全く届かない）
- **Webサイト**などが正常に動作しなくなる
- 解除申請をしても時間がかかったり、本国との時差や言語により**交渉が難航**する
- 以降、**ブラックリスト登録されやすくなる**（監視のマークがより強くなる）
- 自社のみならず、配配メールの他ユーザ様へも直接的に影響を及ぼす

配配メールサービスへの影響について

ブラックリストの影響について

配配メールでは今年8月に大規模なブラックリスト登録が発生しました。
特定のユーザによって特定電子メール法違反の配信を大量に行ったことで、
外部機関のブラックリストに登録され、多くのユーザに影響を及ぼしました。

これらは強度な監視や対策を行っていても、違反者からの一時的な大量配信により、ブロックされることがございます。

また、外部機関各社の基準は非公開のため、どのタイミングで閾値が変更されるかが
わからないまま運用をしなくてはなりません。

そのため、日頃から対策を行い、ブラックリスト登録されない運用を
皆様にもご協力いただく必要がございます。

配配メールサービスへの影響について

②監視強化と是正フォローについて

本件およびブラックリスト対策の一環として、
弊社側での監視強化と是正フォロー強化を行って参ります。

・迷惑メール対策関連の設定強化
SPF、DKIM、DMARC未設定の場合、設定依頼およびフォローを実施

・高エラー配信への対応
一定値の配信エラー率、エラー数を確認した場合、確認および是正を依頼

・コンテンツチェック
メール件名、本文のコンテンツ・URLチェック（システムでの自動判定）

4. まとめ

Gmail送信者ガイドラインの概要

【送信担当者側】
① 電子メール認証（SPF・DKIM・DMARC）の必須化
② メール送信にTLS接続を使用する
③ 迷惑メール率を0.3%以下にする
④ 受信者がメールの配信登録を容易に解除できるようにする
⑤ メールサービスプロバイダを利用する

【配信システム側】
⑥ ワンク
⑦ メール
⑧ PTRレ
⑨ ARCヘ

弊社側で対応

やるべきことチェックリスト

ガイドライン施行前

- □ SPF・DKIM・DMARCを設定する
- □ 配信リストのチェック（オプトインが取れているリスト）
- □ Postmaster Toolsの準備
- □ TLS通信を準備する　※TLS未契約の場合のみ
- □ 独自ドメインを準備する　※独自ドメイン未取得の場合のみ

ガイドライン施行後

- □ 独自ドメイン・TLS通信で配信する
- □ 広告宣伝目的のメールにはワンクリック解除フォームを入れる
- □ 定期的にリストクリーニングをする（タイポ/無効アドレスの除外）
- □ 定期的にPostmaster Toolsで監視する

付録（ご参考資料）

迷惑メールとされる5つの要因

- コンテンツチェック
- 高エラー配信
- 大量配信
- ブラックリスト
- なりすましメール

コンテンツチェック

コンテンツチェックとは？

もっとも初期から行われる迷惑メール判定方法
メールの件名・内容をチェックして、迷惑メールではないかを区分けする

公序良俗に反すると思われる単語

いわゆる

・アダルト系の単語
・暴力的な単語、犯罪に関わる単語
・投資、ギャンブル、お金儲け系の単語

などが含まれていると高確率で迷惑メールと判定されます。

それ以外にも

「無料」「稼げます」「いまだけ」

など一般用語でも、「多くのスパムメールが使っている単語」が入っていると
迷惑メールとして判定されやすくなります。

過剰なテキスト装飾

┌ 見出し ┐
└──────────┘

■■ 見出し　■■■■■■■■■■■■■■■■
_/_/ 見出し　_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/

■□□□□□□□□□□□□□□□□□□□□□□□□□□□□■
http://URL/
■□□□□□□□□□□□□□□□□□□□□□□□□□□□□■

↓↓──────────────────────────────↓↓
http://URL/
↑↑──────────────────────────────↑↑

などテキストによる飾り罫なども好まれないといわれています。

メール内の画像サイズが極端に大きい

過去、テキスト配信が迷惑メール配信の主流でしたが、
テキストフィルタリングを避けるため**メッセージを画像化**
して送信する手法が増えました。

そのため、**テキスト量に比べて画像の比率が極端に高い場合は、**
迷惑メールと見なされる可能性があります。

画像の方が訴求しやすく、ブランディングにも向いていますが、
伝えたいことはテキストでも記載しましょう。

コンテンツチェックを回避するための注意点

・テキストと画像のバランスを取る

画像

テキスト

画像

テキスト

画像

画像

画像

テキスト

○

画像だけではなく適宜テキストも添える

×

コンテンツのほとんどが画像
文章を画像化（キャプチャ）して
添付する…など

その他

●本文内のURL

セキュリティレベルの低いサイト（非暗号化のhttpなど）や、
危険な広告だらけのサイトへのリンクを記載すると迷惑メール
と見なされやすくなります。

また、フリーの**短縮URLも**迷惑メール業者に多く使われ、
迷惑メールと同じドメインURLが載っている＝同様のメールと
見なされてしまいます。

●ファイル添付

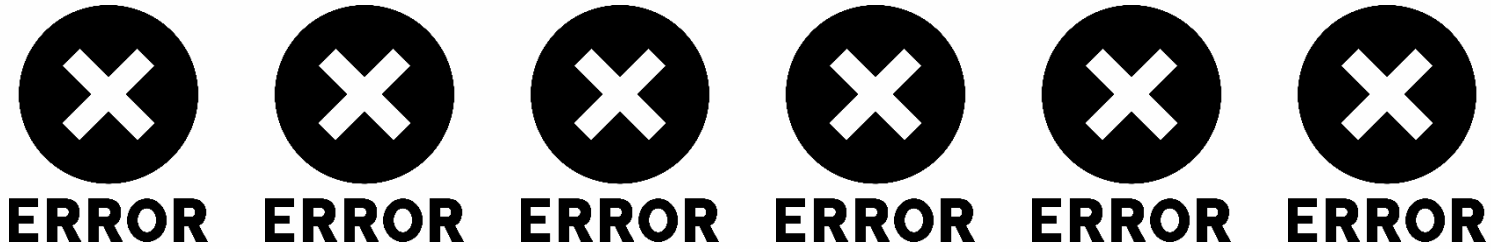
ファイル添付はウィルスメールに多用されるため、誤判定確率が高い。
特にexeファイルは高確率で迷惑メールと見なされます。

コンテンツチェックを回避するための注意点

- 使う単語に注意
- 同じ単語を何回も繰り返し使わない
- 過剰な装飾（飾り罫など）をしない
- テキストと画像のバランスを取る
- http（非暗号化）のURLは載せない
- フリーの短縮URLは使わない

高エラー配信

迷惑メール業者は、大量にかき集めたアドレスを精査せずに配信しています。
そのため、迷惑メール配信は大量のエラーを発生させます。



つまり、受信側では　**迷惑メール≒高エラー**　と捉えられます。
宛先不明や間違いアドレスなどが多く含まれる配信は迷惑メール送信とみなされ、
一律にブロックされます。
この時、本来届くはずのメールも含めてブロックされてしまいます。

エラーアドレスの管理

配配メールでは、エラー回数フラグにより、エラーアドレスの管理を行います。
一定回数エラーが発生したアドレスを宛先から自動的に除外します。
また10%を超える配信エラーが発生した場合は、アラートメールを通知します。

1配信あたりのエラー率を下げることで受信ブロックを防ぎます。

単一IPからの大量配信

迷惑メールの特徴は**大量配信**です。
無秩序に収集したリストに精査せず一斉に配信します。

メールの配信場所は、IPアドレスにより把握されます。
そのため、1か所（1つのIP）から大量に配信されると、迷惑メール配信と見なされ、
ブロックされます。

また**迷惑メール配信は再配信（Retry）を行わない**特徴があるため、
受信側は一旦ブロックして様子を見ることがあります。

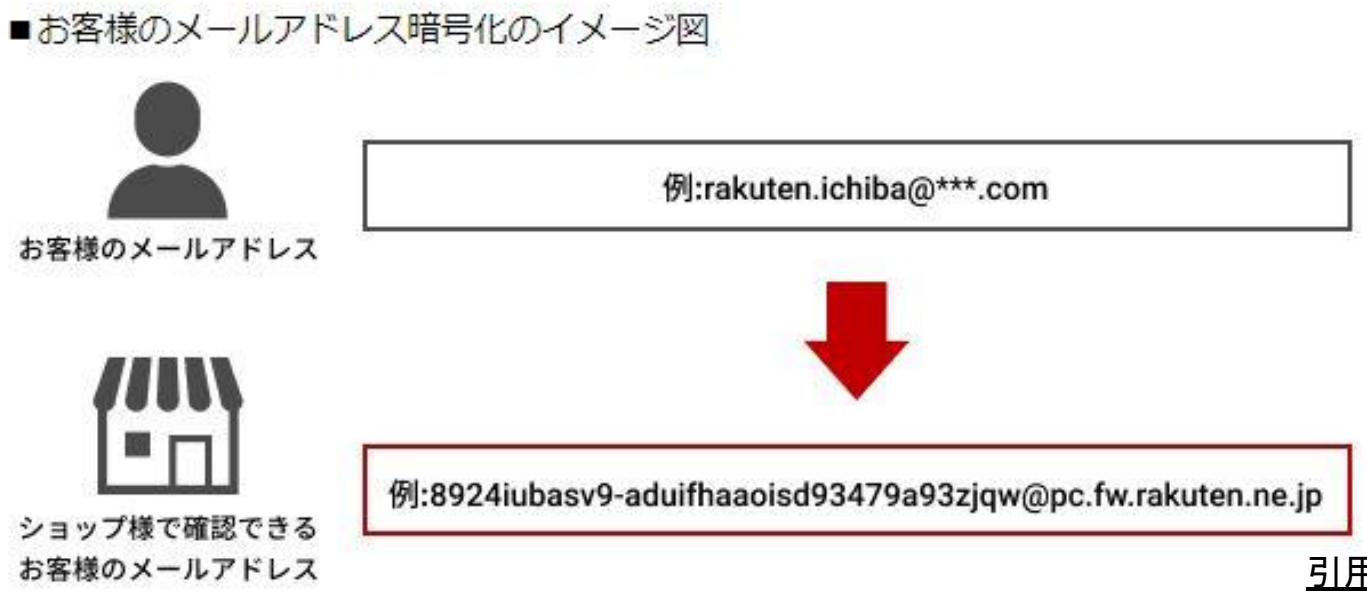
分散配信とブロック回避

配配メールでは**複数IPアドレスによる分散配信**の仕組みを実装し、
受信ブロックを回避します。

また単一IPからの配信量もエンジニアがコントロールし、ブロック回避に努めます。

万一ブロックが生じた際も他のIPに配信を迂回させたり、
再送配信を実施し、受け渡しを試みます。

要注意：マスクアドレスへの配信



引用：楽天あんしんメルアドサービス

マスクアドレスとは
ECサイトなどでショップとエンドユーザーの**メールアドレスを暗号化＝マスク化したもの**を指します。

これにより、エンドユーザーは自分のアドレスをショップに開示せずに購入等を行えます。

要注意：マスクアドレスへの配信

例：Amazonマスクアドレス,au PAYマーケットアドレスなど

マスクアドレスは、一般的なメールアドレスと異なります。
送信元として利用できるサーバに指定があったり、専用のメールサーバを通さなければメール送信ができなかったりと制限があります。

また**ユーザ様と各ショップとの個別やり取り用途のみを想定しています。**
そのため、**大量配信を行うと、サーバに配信を拒否されます**

ブラックリストの影響

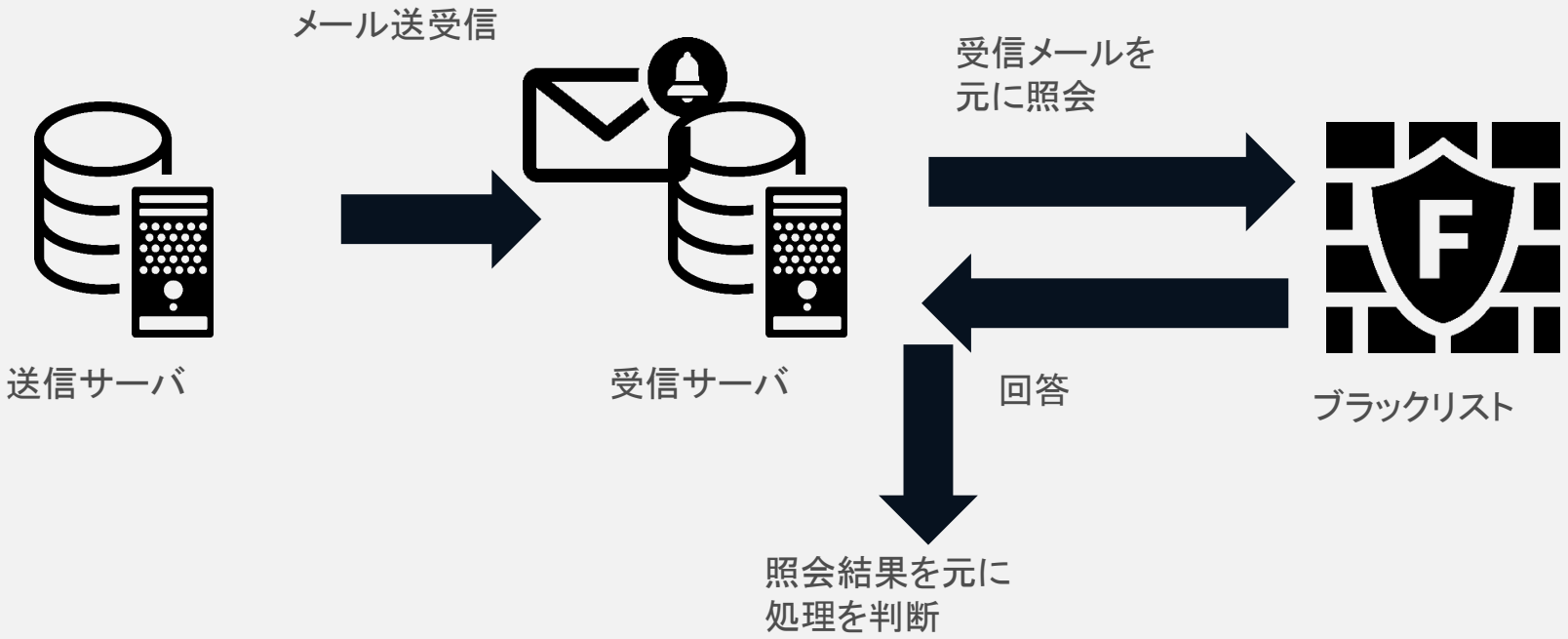
ブラックリストとは

不正なメールを送信しているIPアドレスやドメインの一覧のことを指します。
ブラックリストはセキュリティ団体などの第三者団体によって管理され、
世界中に複数存在します。

ブラックリストの影響

ブラックリストは多くの受信サーバやセキュリティソフトなどにより利用されます。

受信サーバは受信した**メールの送信元情報をブラックリストと照会**し、
照会結果を元に、受信サーバはメールをどう処理するかを決定します。

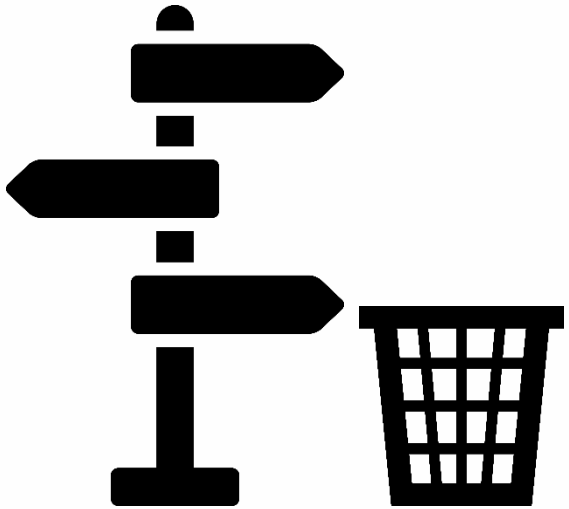


ブラックリストの影響

ブラックリスト登録されてしまった場合
多くの受信サーバにてメール受信を拒否する可能性が生じます。

ブラックリストの影響

単にエラー情報を返す以外にも送信者には**正常応答を返した上で、**
迷惑メールフォルダに振り分けたり**メールを破棄したりする場合もあります。**
（受信側がどんな振る舞いをするかは、送信側ではわかりません）



また、ブラックリスト管理団体は多数あり、
サーバによって参照しているブラックリストは異なります。

したがって、ある宛先には正常に届くが、別の宛先にはメールが
届かないというケースもありえます。

ブラックリストの影響

受信サーバ側がブラックリストを参照して、受信拒否する場合、
配信側（読者自身含む）が行える回避策はありません。

ブラックリスト登録は団体が違反と見なすアドレスへの配信や
通報の蓄積により、登録されます。

避けてほしい配信アドレス

迷惑メール送信者を識別するためにブラックリスト管理団体は
使われていないメールアドレスやドメインを所有し、
そこに送信されるメールを**迷惑メール送信元とする判断に利用**しています。

これを　**トラップアドレス**　と呼びます。

トラップアドレスの種類

■利用されていないドメイン （プリスティン・トラップ / Pristine Trap）

使用していないメールアドレスまたはドメインをインターネットに掲載し、
ネット上から無秩序にメールを収集する者や、そういった者からのリスト購入者を
特定します。

■入力間違いアドレス （Typos Trap）

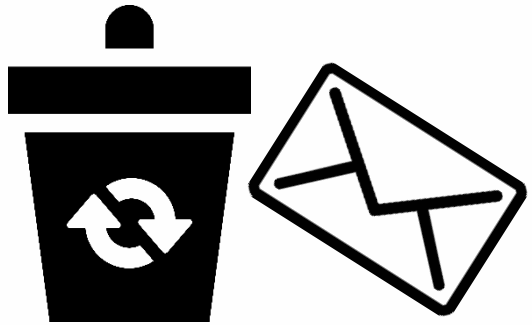
大手メーラのドメインのタイプミスなどもスパム・トラップとして使用されます。
※正：gmail.com　誤：gmai.com、　正：icloud.com　誤：iclud.com など

■過去に利用されていたアドレス （リサイクル・トラップ / Recycled Spam Trap）

過去に使われていたドメインやメールアドレスをスパム・トラップ用に再利用し、
迷惑メール送信者かどうかを判断します。
※会社に在籍していない従業員のアドレスやロールアドレスなど

リストのクリーニングにご協力ください

特に注意してほしいものが、
■過去に利用されていたアドレス（リサイクル・トラップ / Recycled Spam Trap）
です。



**正当に入手したアドレスでも時間経過により無効となり、
トラップアドレスになっている可能性があります。**

一般的に休眠状態が3ヵ月続いているメールアドレスはメールプロバイダー等で
無効と見なされるため、開封クリック等反応のないアドレスは削除や除外などを
検討ください。

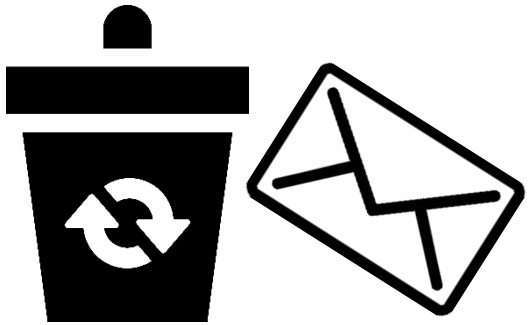
リストのクリーニングにご協力ください

クリーニング頻度目安

週1-2回、配信を実施している場合は月1程度
長くとも3か月に1回

間違いやすいスペルミス例

正：gmail.com　誤：gmai.com
正：yahoo.com　誤：yahaba.com
正：outlook.com　誤：outlooc.com
正：icloud.com　誤：iclud.com
など



さいごに

セミナーにご参加いただき、誠にありがとうございました。

本日の内容につきましては是非積極的にお取組みいただけますと幸いです。

今後も皆様が快適にサービスをご利用いただけますよう、品質向上に取り組んで
参りますので末永く配配メールをご利用いただけますと幸いです。