BtoB デジマトレンド
by DM Card Japan

大量にメール配信をする企業は要チェック!

Gmailポリシー変更

2024年2月

Gmailのメール送信者ガイドラインが アップデートされました

Gmailアカウントにメルマガや通知メールなどを配信している企業は要チェックです！
「変更内容は？」「何を対応すればいい？」とお悩みの方へ、要件を解説します。

【Gmail】メール送信者のガイドライン

2024年2月、Googleの発表により、Gmailのポリシーが変更され、以下のように義務付けられました。

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、

（同じドメインから）

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**

引用元：Google Workspace 管理者 ヘルプ　https://support.google.com/a/answer/81126

目的

悪意のあるなりすましメールをブロックして、
フィッシング詐欺や個人情報の流出などから、ユーザーを守る

- Gmailアカウントとは … 末尾が「@gmail.com」または「@googlemail.com」の個人用アカウント

※Google Workspaceの企業アカウントなどは対象外

どのような対応をすれば良いか？

Gmailポリシーの変更によって、メール送信者は具体的にどのような対応が必要になるでしょうか？

1. 送信メールを認証すること

SPF、DKIM、DMARCの設定をする。 4ページへ

これらは、メールの送信元を認証する仕組みで、メールのなりすましを防止するために必要です。

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

迷惑メール率を定期的に監視する。 11ページへ

Gmailでは迷惑メール率を0.1%未満に維持し、0.3%以上にならないよう要求しています。

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

かんたんに登録解除できるフォームを設置する。 12ページへ

受信者が望まないメールの配信登録をワンクリックで解除できる仕組みを提供する必要があります。

※米国Yahoo！社も、同様にメール送信元に対して義務付けをすることを発表しています。

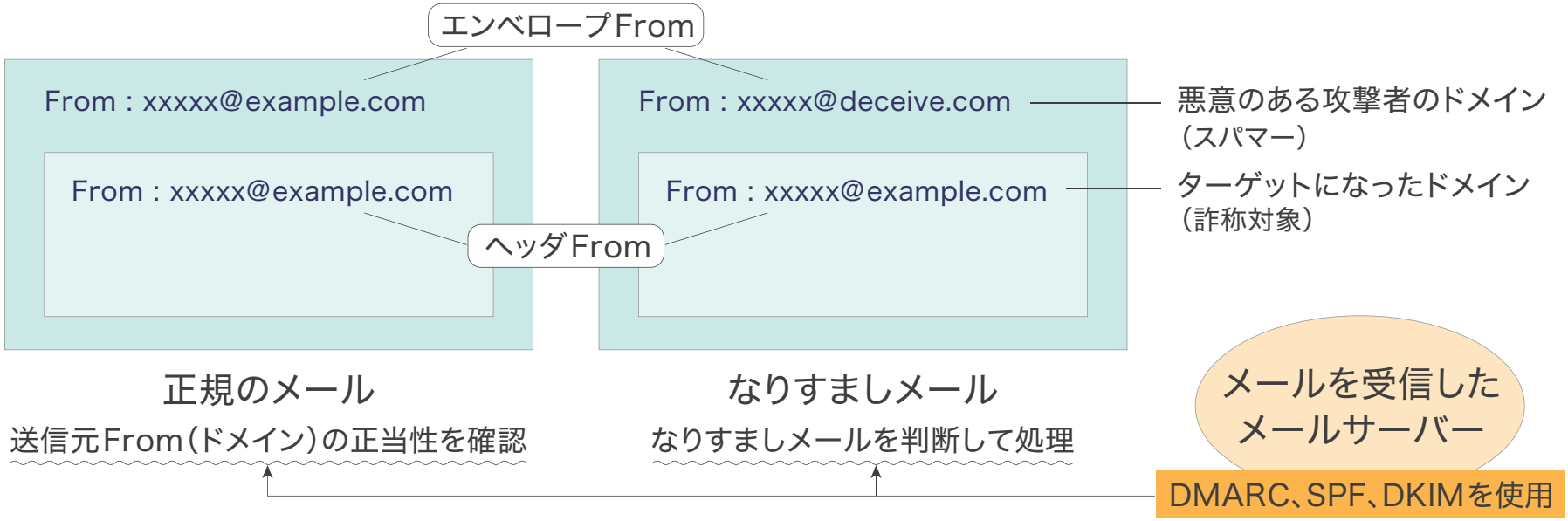
Yahoo！：More Secure, Less Spam: Enforcing Email Standards for a Better Experience（英文）
https://blog.postmaster.yahooinc.com/post/7301721674944839 68/more-secure-less-spam

送信メールを認証する

エンベロープFROMとヘッダFROM

メールに書かれている送信元From（ドメイン）は2種類あります。

エンベロープFrom 封筒の差出人に相当	メールソフト上で表示されない差出人 … 受信者には見えていない メールサーバ上で自動的に付加されるため、メール作成者は設定できない
ヘッダFrom 便箋の差出人に相当	メールソフト上で表示される差出人 … 受信者が見ている メール作成者は自由に変更できる → なりすましメールを送信できてしまう

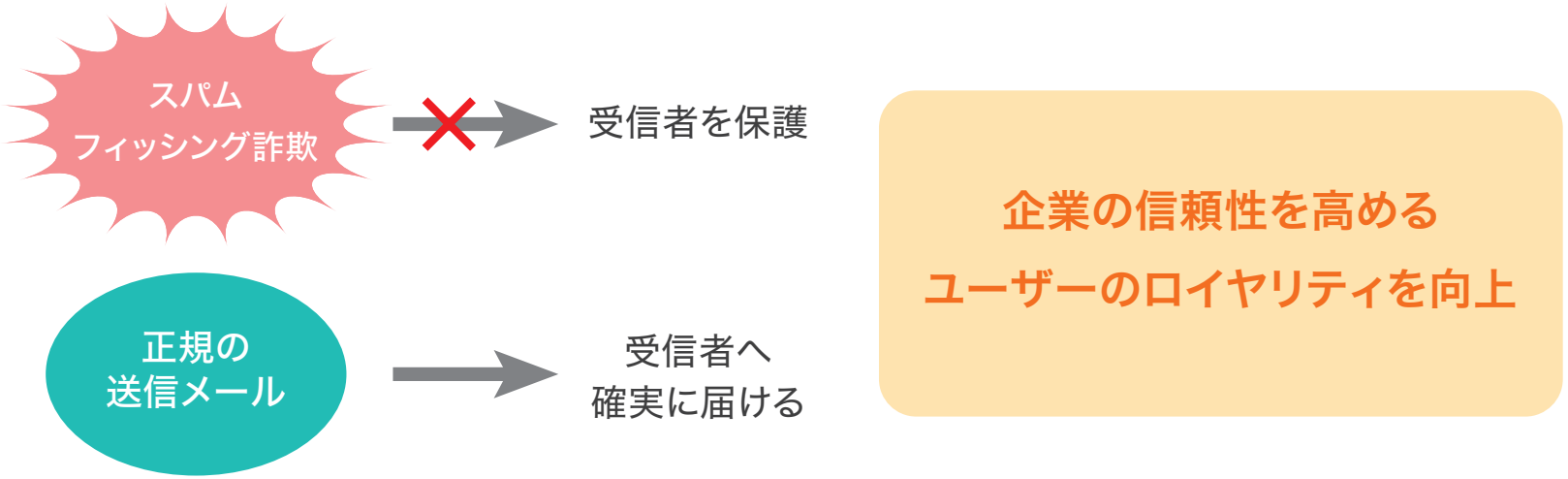


SPF、DKIM、DMARCとは

それぞれメールの送信元（ドメイン）を認証する仕組みで、メールのなりすましを防止するためには欠かせません。
正規の送信者から送られたメールであることを証明するため、すべて設定しましょう。
（Gmailアカウントに送信するメールが1日あたり5,000件に満たない場合もSPFとDKIM認証を設定しましょう。）

送信元（ドメイン）認証の重要性

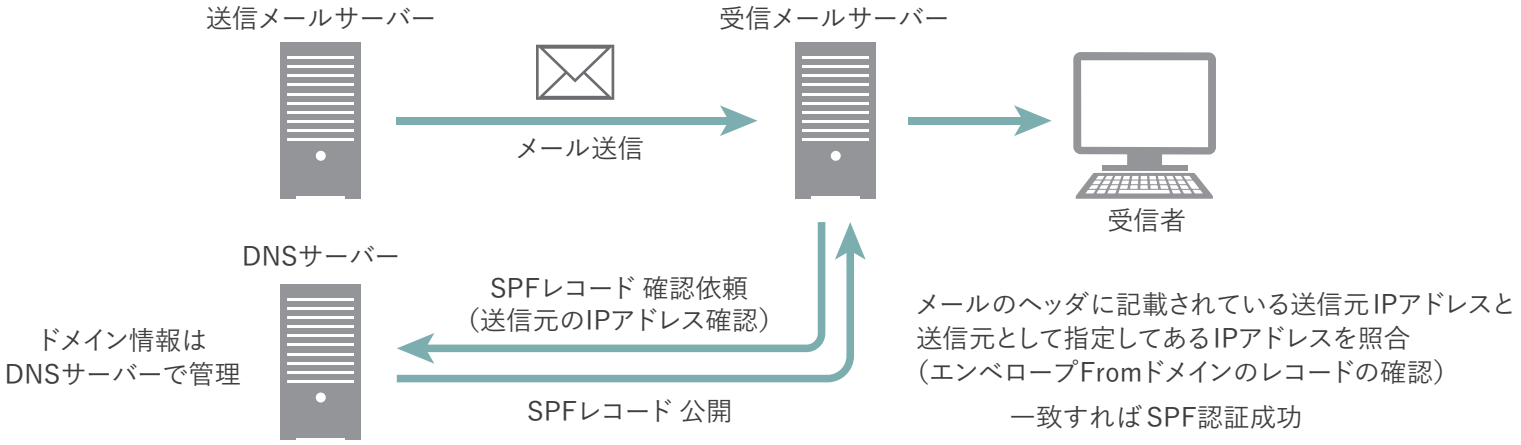
送信元（ドメイン）認証（SPF、DKIM、DMARC）は、電子メールのセキュリティと信頼性を向上させるための重要な手段です。
これらの技術を組み合わせることで、受信者や送信者が安全にメールのやり取りを行える環境を提供します。



SPFの設定

SPF（Sender Policy Framework）とは

メールの送信元IPアドレスにより、メール送信元のドメインが公式であること（詐称されていないか）を認証するための仕組みです。
送信元ドメインがSPFを設定している場合、メールサーバーはそのドメインから送信されるメールを許可（拒否）するかを判断します。



SPFレコードの設定方法

SPFは、ドメインの（送信元となるメールアドレスを運用している）DNSサーバーにSPFレコードを追加することで設定します。

SPFレコードの記述例 ： ドメイン名. IN TXT "v=spf1 include:_spf.example.com ~all"

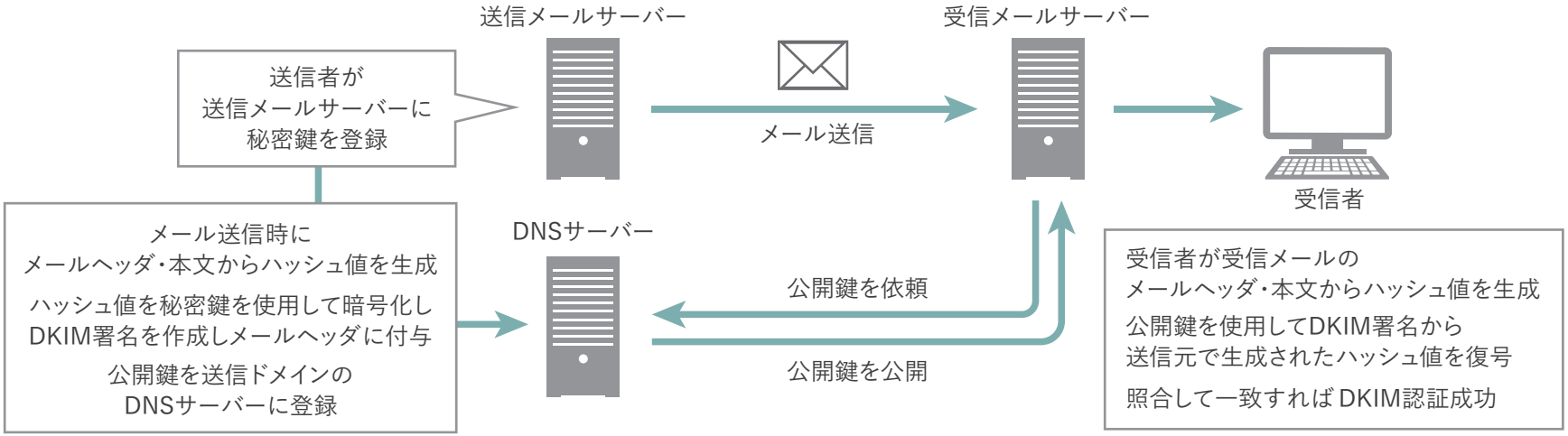
メール配信システムの運営会社からSPFレコードを教えてもらい、自社ドメインの管理画面にログインをして、SPFレコードを記入します。
ドメイン管理について、外部に委託をしている場合は、SPFレコードを委託先に提供し、設定を依頼しましょう。

※DNS（Domain Name System）とは、インターネット上の場所を示す「ドメイン」と割り振られた識別番号である「IPアドレス」の関係を結びつけるシステムのこと。

DKIMの設定

DKIM(DomainKeys Identified Mail)とは

送信メールに対して電子署名を作成し、受信者がメールの検証することで、送信元の認証をする仕組みです。
送信元ドメインのDNS上に公開されている公開鍵を使用し、受信メールのヘッダに記載されたDKIM署名の正当性を検証します。



DKIM署名の設定方法

DKIMの設定には、送信ドメインのメールサーバーでの設定が必要です。

送信メールサーバーにDKIM署名用のソフトウェアをインストールします。
送信元ドメインのDNSレコードに、メールサーバーで生成された公開鍵を含むDKIMレコードを追加します。
ドメイン管理について、外部に委託をしている場合は、DKIMレコードを委託先に提供し、設定を依頼しましょう。

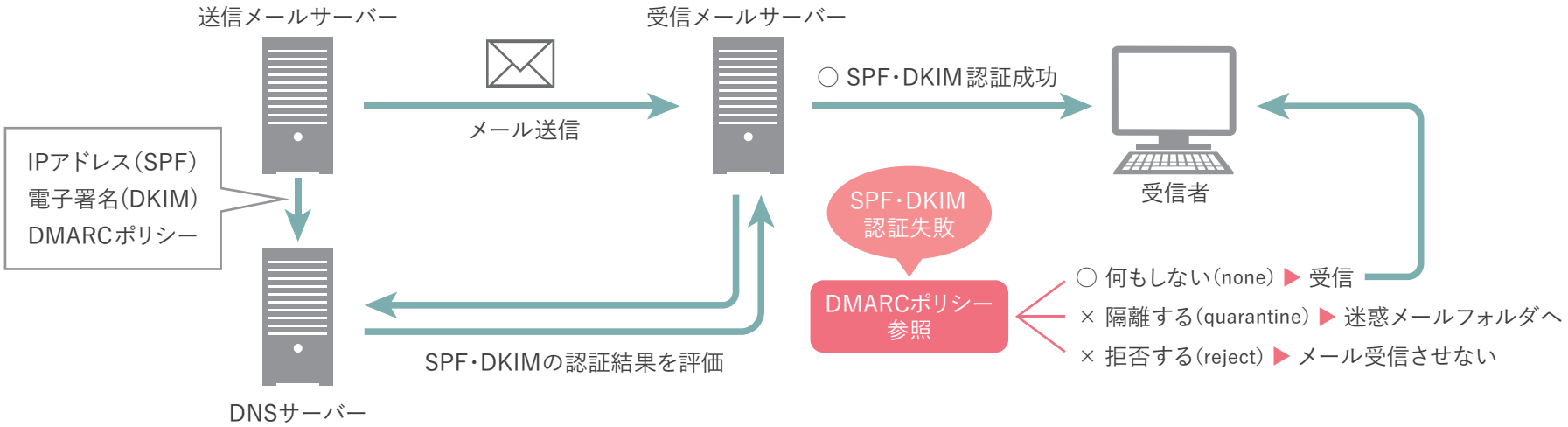
※ハッシュ値とは、データをハッシュ関数という計算方法で変換し、固定長(固定の桁数)の数値に置き換えたもの。

DMARCの設定

DMARC（Domain-based Message Authentication, Reporting and Conformance）とは

DMARCは、SPF・DKIMの認証結果と組み合わせて、送信元ドメインを認証する仕組みです。

DMARCは、送信メールがSPFレコードまたはDKIM署名での認証に失敗した場合に、メールに表示される送信者ドメイン（ヘッダFrom）とSPF・DKIMで認証したドメインが一致するかの検証を行い、処理方法を受信サーバーに指示します。



DMARCの設定方法

DMARCは、ドメインの（送信元となるメールアドレスを運用している）DNSサーバーにDMARCレコードを追加することで設定します。

設定は、各サービスプロバイダーやドメイン管理者の設定画面を使用して行うことができます。

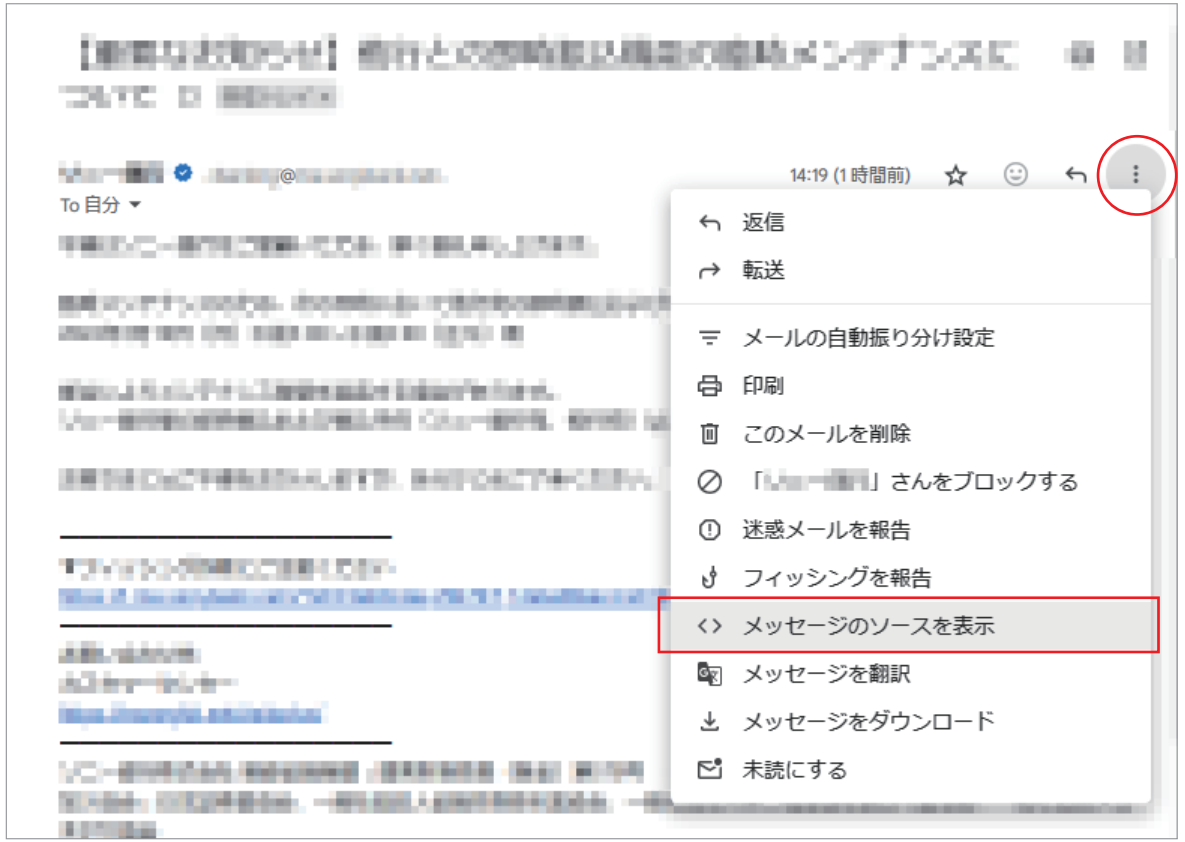
ドメイン管理について、外部に委託をしている場合は、DMARCレコードを委託先に提供し、設定を依頼しましょう。

SPF・DKIM・DMARCの確認方法

SPF・DKIM・DMARCを簡単にチェックするには

・Gmail宛にメールを送信

・Gmail上で「メッセージのソースを表示」から
受信メールのヘッダ情報を確認します。



＞ 次のページへ

・SPF・DKIM・DMARCの認証結果が表示されます。

「PASS」→ 認証成功　　「FAIL」→ 認証失敗

設定されていない場合は認証結果が表示されません。

ブラウザ上でSPF、DKIM、DMARCの各レコードが確認できるWEBサイトもあります。

・SKYSNAG

https://www.skysnag.com/spf-checker-2/
https://www.skysnag.com/dkim-checker-2/
https://www.skysnag.com/dmarc-checker-2/

・POWERDRAMARC

https://powerdmarc.com/ja/spf-record-lookup/
https://powerdmarc.com/ja/dkim-record-lookup/
https://powerdmarc.com/ja/dmarc-record-checker/

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

迷惑メール率を0.3%以下にする

迷惑メール率とは、メール受信者によって迷惑メールとして分類された割合です。
Googleが提供する「Postmaster Tools」でドメインの迷惑メール率を確認することができます。

> Postmaster Toolsでユーザーから報告される迷惑メール率を0.1%未満に保ち、
> **迷惑メール率が決して0.3%以上にならないようにします。**

Postmaster Toolsで、迷惑メール率を定期的に監視するようにしましょう。

- 迷惑メール率は毎日計算されます。
- 迷惑メール率を低く維持することで、一時的に上昇しても、迷惑メールとしてマークされる可能性が低くなります。
- 迷惑メール率が高い状態が続くと、迷惑メールの分類が増加します。

Postmaster Toolsを使用すると
「迷惑メール率」の他に、IPのレピュテーション（IPアドレスの評価）、ドメインのレピュテーション（ドメインの評価）、
SPF・DKIM・DMARCの認証の割合、配信エラー率などのデータを確認できます。

- Postmaster Toolsを利用するには、ドメインの所有権を証明する必要があります。
- ドメインの所有権を証明することにより、そのドメインが Googleサービスで不正使用されるのを防ぐことができます。

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

かんたんに登録解除できるフォームを設置する

オプトインとオプトアウト

オプトインとは、広告や宣伝目的でメールを配信する前に、受信者からメール配信の承諾を得ることです。
オプトインによるメール配信は「特定電子メール法」で義務付けられており、承諾を得ずにメール配信を行うことは違法行為と見なされます。
メール送信者は、WEBサイト上で個人情報の取り扱いについて記載し、メール配信に「同意する」ボタンを設置するなどの案内をしましょう。

オプトアウトとは、承諾を得ずにメール配信を行い、受信者からメール配信登録の解除をしてもらうことです。※この方法は違法です。
メール送信者は、解除の通知を受けるサーバーを設置し、配信メール内に「配信停止希望はこちら」といったリンクを設定するなどの対策が必要です。

メール送信者は、受信者が望まないメールの配信登録を
ワンクリックでかんたんに解除できる仕組みを提供する必要があります。

配信登録解除機能の重要性

受信者がかんたんにメール配信登録の解除できるようにすれば、迷惑メール率の低下にもつながり、IPのレピュテーションが改善されると、開封率、クリック率を上げることができます。

登録解除リンクが見つけにくかったり、会員ページにログインをしないと登録解除できない仕様など、かんたんに解除することができない場合は、今回のガイドラインを遵守していないと見なされます。
また、特定電子メール法にも触れるおそれがありますので、ワンクリックで登録解除ができるフォームを用意しましょう。

ワンクリックで登録解除できる方法

List-Unsubscribeとは

List-Unsubscribeとは、メールのヘッダに拡張される情報のひとつで、受信者が望まないメールの配信登録をワンクリックでかんたんに解除できるようにするためのものです。

メール本文内に配信停止リンクを用意せずに登録解除ができるため、受信者がフィッシングではないかとリンクを警戒する場合にも有効です。

例）Adobeから送信されたメールのGmail画面

メールの暗号化を行う

メール暗号化の重要性

メール送信に利用される仕組みであるSMTP（Simple Mail Transfer Protocol）は、標準では通信の暗号化に対応していません。

そのままでは情報漏洩などの危険性があるため、メール通信の安全性を確保することは重要です。

TLS（Transport Layer Security）接続とは

インターネット上の通信におけるセキュリティとプライバシーを確保するための仕組みです。

ブラウザとサーバーとの通信データを暗号化し、送受信者の認証、個人情報や機密情報などのデータを保護します。

※今回のGoogleが示すガイドラインの送信者要件にも、「メールの送信にTLS接続を使用する」ことが盛り込まれています。

STARTTLSとは

TLSを使用して暗号化通信を取り入れる技術のことです。メールサーバー上で設定を行います。

メール形式はRFC5322に準拠する

RFC5322（Internet Message Format）とは

メールの形式に関する標準を規定した仕様のことで、メッセージ構造やヘッダー情報、本文のコンテンツ内容など、メールのフォーマットについてルールを定めています。

RFC5322に準拠することで、メール送受信システム間での互換性を保ち、セキュリティ上のリスクが軽減され、メッセージの信頼性が向上します。

まとめ

期日までに対応できなかったらどうなる？

2024年2月以降、新しいGmailポリシーに準拠できない場合、Gmailのアドレスへメールを送信できない可能性があります。
1日あたり5,000件以上の大量送信を行っている企業は早期に適切な対応が求められます。

- メール送信者がガイドラインに沿った対応をしない場合は
  送信したメールがGmailによって
  - エラーとして拒否され、送信者に届かない（受信拒否）
  - 迷惑メールフォルダに振り分けられる

Gmail以外のメールにも影響はある？

Gmailのポリシー変更のため、現状でGmail以外への影響はありません。
ただし、他のメールクライアントでもDMARC設定の推奨など、なりすまし対策の強化をしているため、同様の対処を行いましょう。

まとめ

以上、Gmailのポリシー変更について、まとめました。
1日あたりの配信数を問わず、すべてのメール送信者はここで紹介した対応をしておくことが得策と言えるでしょう。
現状で対策が実施できているかどうか、あらためて見直しを行ってみてください。

会社概要

1988年創業の製造業、建築業など業界に特化した自社独自のデータベースを駆使し、
合理的なダイレクトマーケティングサービスを展開する企業です。

■会社概要

名　　称	DMカードジャパン株式会社
本社所在地	〒112-0014 東京都文京区関口1-10-2
創　　業	1988年9月5日
資 本 金	20,000,000円
代表取締役	佐藤 義弘

■業務

情報誌の発行・Webマーケティングサービス
製造業向け情報誌 インダストリアルカード
建築業向け情報誌 アークカード
DMS ダイレクトマーケティングサービス
Webマーケティング支援サイト PRISMの運営
Webコンサルティング（SEM）
SEO施工
リスティング広告の運用管理・提案
Webサイト制作

■本書に関して

本書に記載のURL等は予告なく変更される事があります。本書の作成にあたり可能な限り正確な情報を掲載するよう努めておりますが、コンテンツの特性上、必ずしも最新の情報を保証するものではないことをご了承ください。本書に掲載された内容で生じた損害等の一切の責任を負いかねますのでご了承ください。

デジタルマーケティングの最新情報公開中
https://dmcj.jp/