HOME type-M※に送信ドメイン認証（DKIM/DMARC)機能を追加しました ※Canonetメールサービスを含む

2025年7月7日（月）から、マイデスクよりDKIM/DMARCの設定ができるようになりました。
このPDFでは、 DKIM/DMARCのご利用法と注意事項、送信ドメイン認証についてご案内します。
DKIM/DMARCを有効にするためには、お客様ドメイン毎に設定が必要です。

ユーザーズマニュアル（管理者編）より“5.6 DKIM/DMARCを設定する”をご参照いただき
お客様のDKIM/DMARCの有効化とDNSの設定変更をしてください。

https://app.canonet.ne.jp/manual/admin/05_mail_manual/50_set_dkim_dmarc.html

注意事項
・DNSに同一のTXTレコードがある場合は上書きされます。
・インターネットの仕組み上、DNSへ設定したDKIM・DMARCの伝播には時間がかかります。
受信者側がこのDNS設定を引けるまでの間は、受信者側で認証が失敗する可能性があります。

お問い合わせ先
キヤノンマーケティングジャパン株式会社
HOMEコンタクトセンター　ホスティングサポート
E-Mail　：home-support@canon-mj.co.jp
TEL　　：03-6632-9519
受付時間：平日 09:00～18:00※土日・祝日、その他当社指定の休日を除く

送信ドメイン認証はなぜ必要なのか

メールの差出人をなりすますのは簡単

インターネットのメールの仕組みを「郵便」にたとえると・・・
たとえば、誰かが手紙を送るとき、封筒の差出人と便せんに書かれた名前が違うことがあります。
メールも同じで、実際にメールを送った人（封筒の差出人）は「エンベロープFrom」、
メールの画面に表示される送り主（便せんの名前）は「ヘッダーFrom」と呼ばれます。
この「ヘッダーFrom」は簡単に偽装できてしまうため、悪意のある人が本物の会社や人を装って迷惑メールを送ることができてしまいます。
Outlookなどのメールアプリでは、この「ヘッダーFrom」が差出人として表示されるため、
受け取った人は本物だと勘違いしてしまうことがあります。
そこで、こうした偽装を防ぐために「送信ドメイン認証」という仕組みが使われるようになりました。

メールの差出人には2種類あります。

- “ヘッダーFrom”は**便せんの差出人**にあたるもので、outlookなどのメーラに差出人として表示されます。

  書換え（偽装）が容易。

- “エンベロープFrom”は**封筒の差出人**にあたるもので、メールが届かなかった際の返送先となります。

  書換え（偽装）の難易度は高い。

送信ドメイン認証の代表的な３つの技術

これらを使うことで、迷惑メールやなりすましメールを減らすことができます。

技術名	役割・目的	機能(動作）の概要	濃い青文字はHOME type-Mで対応している機能
SPF	送信元の正当性確認	送信側の動作	ドメインのDNSに、TXTレコードとしてSPF情報を登録する。
		受信側の動作	送信元IPが、DNSのSPFレコードに記載されたIPやホストに含まれているかを確認し、検証する。
DKIM	メールの改ざん防止	送信側の動作	秘密鍵で暗号化した電子署名（DKIM署名）をメールに付加する。DNSに公開鍵を登録し公開する。
		受信側の動作	DNSを参照し、公開鍵を使ってDKIM署名を復号し、正当な送信者からの改ざんされていないメールかどうか判断する。
DMARC	SPF・DKIMの検証とポリシーの適用	送信側の動作	DMARCポリシーをDNSに設定し、受信側にどう処理してほしいかを公開する。
		受信側の動作	SPFまたはDKIMが成功し、かつFromヘッダーと一致しているかを基準に、受信したメールをどう処理するか（受け入れ・拒否・隔離など）を決定し処理する。 DMARCレコードに指定されたメールアドレスに、検証結果のレポート（Aggregate Report）を送信。

SPF（Sender Policy Framework）認証について

SPFはメールの送信元が本物かどうかを見分けるための仕組み

インターネットのメールとSPFの仕組みを「郵便」にたとえると…
たとえば、誰かが手紙を送るとき、「この住所から送っていますよ」と郵便局に届け出ておくようなものです。
SPFでは、メールを送る人（送信者）が、自分のDNSサーバーに「このサーバーからメールを送ります」という情報（SPFレコード）を登録しておきます。
メールを受け取る側（受信者）は、封筒に書かれた差出人（エンベロープFrom）を見て、そのドメインのDNSにアクセスし、「このメールは本当に許可されたサーバーから送られているか？」をチェックします。
この仕組みによって、悪意のある人が勝手に他人の名前を使ってメールを送ることを防ぐことができます。
SPFは、あるIPアドレスが特定のドメインのメールを送信する権限を持っているかどうかを検証する仕組みとも言えます。

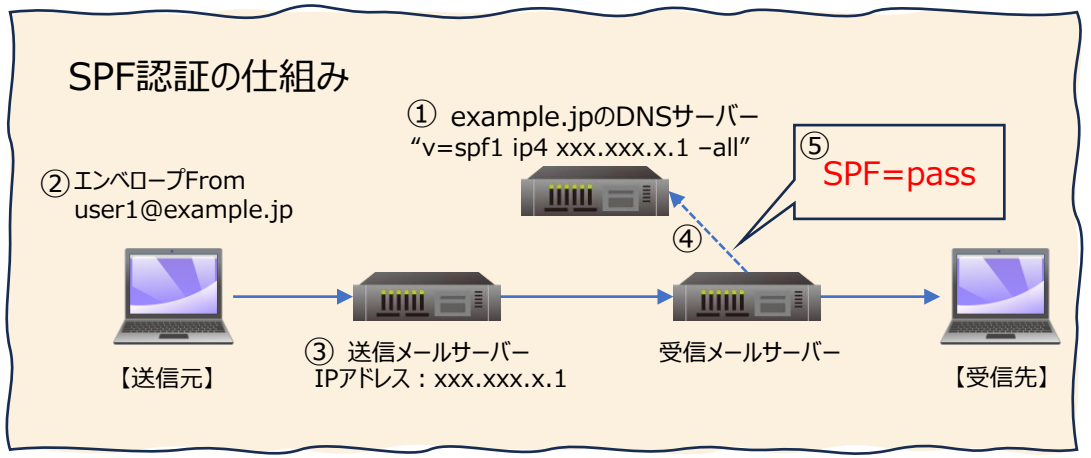
SPFは多くの企業やサービスで導入されており、たとえば国内のJPドメインでは2023年時点で82.9%※と高い普及率です。
そのため、多くの企業やインターネットサービスプロバイダー（ISP）のメールサーバーでSPF認証が使われています。

※総務省　令和6年版　情報通信白書の概要　送信ドメイン認証技術のJPドメイン導入状況より

SPFの注意点とは

SPFは、封筒の差出人（エンベロープFrom）しか確認しないので、便せんに書かれた名前（ヘッダーFrom）が偽装されていても、SPFではチェックできません。
悪意のある送信者がヘッダーFromのドメインを、自分の自由になるDNSのSPFレコードに登録してSPF認証に合格させることが可能です。

SPFだけではヘッダーFromの正当性を確認できないため、5ページで紹介するDMARCではエンベロープFromとヘッダーFromが同一であるかをチェックする仕組みとなっています。
この仕組みをドメインの整合性（アライメント）を取ると言います。
メール配信サービスを利用していて、ヘッダーFromが自社ドメイン、エンベロープFromがそのサービスのドメインと両社が異なる場合は、いわば”意図した正規のなりすまし”のような状態ですが、送信サーバーのIPアドレスを、自社のドメインのSPFレコードに明示的に登録しておかないと、 SPF認証には合格しても、DMARCは不合格となるので注意してください。



①DNS（例: example.jp）のSPFレコードに、
　送信メールサーバーのIPアドレス（ 例xxx.xxx.x.1 ）を登録
②送信元からメールを送信（例:エンベロープFromがuser1@example.jp）
③送信メールサーバーがメールを配送（例:IPアドアレス xxx.xxx.x.1）
④受信メールサーバが、DNSに対してこのIPアドレス（例:xxx.xxx.x.1)が
　メールを送信する権限を持っているかを照会
⑤結果、合格ならSPF=passとしてメールを配信

DKIM（DomainKeys Identified Mail）認証について

DKIMはメールが本当にその人から送られたもので、途中で改ざんされていないかを確認するための仕組み

インターネットのメールとDKIMの仕組みを「郵便」にたとえると…
たとえば、手紙の中に「この手紙は私が書きました」という印鑑が押されているようなものです。
DKIMでは、メールを送る人（送信者）が、メールの内容（ヘッダーや本文）にデジタル署名をつけて送ります。
この署名は、送信者だけが持っている「秘密鍵」で作られていて、受け取った人は、送信者のDNSサーバーにある「公開鍵」を使って、その署名が正しいかどうかを確認します。
これによって、「このメールは途中で書き換えられていない」「本物の送信者から送られた」ということが証明できるのです。

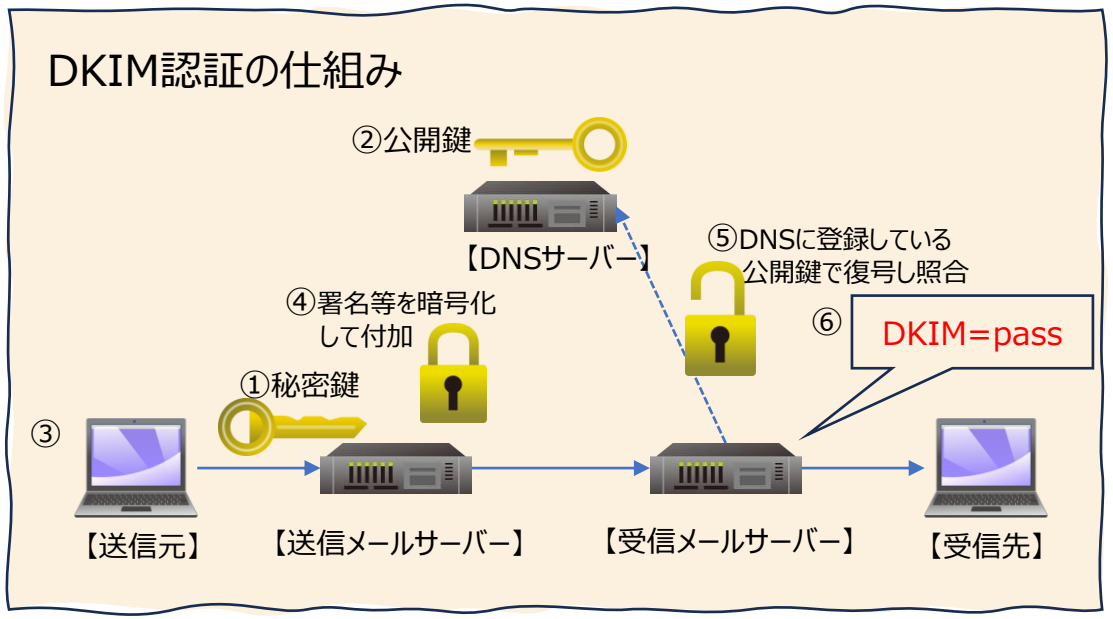
秘密鍵を持っている人しか、正しい署名を作ることができません。
悪意のある人が送信者を装っても、正しい署名が作れないため、なりすましを防ぐことができます。

DKIMの導入率が低かったため、企業やインターネットサービスプロバイダー（ISP）ではあまり使われていませんでしたが、2024年にGmailなどのフリーメールサービスが、大量にメールを送る送信元のドメインに対してDKIMを必須化してから普及が進んでいます。

DKIMの注意点とは

転送時のヘッダー変更などで、メールの内容が途中で少しでも変更されると、署名が一致しなくなり、正しいメールでも「改ざんされた」と判断されてしまうことがあります。
また、署名を行ったドメインとDNSに登録された公開鍵が一致してさえいれば合格するので、これらを別途用意すれば偽装することが可能です。

そこで、DMARCでは、DKIMに署名をしたドメインと「ヘッダーFromのドメイン」が完全一致するかサブドメイン関係にあれば合格として、偽装を見破れるようにしています。
これをドメインの整合性（アライメント）を取ると言います。



①送信メールサーバーに秘密鍵を登録
②DNSサーバーのTXTレコードに公開鍵を登録
} マイデスクから鍵の作成と登録が可能
③送信元からメールを送信
④送信メールサーバが秘密鍵を使って暗号化したデジタル署名を付与してメール送信
⑤受信メールサーバが、DNSに公開鍵を照会し、署名を復号し照合
⑥結果、合格ならdkim=passとしてメールを配信

DMARC（Domain-based Message Authentication, Reporting & Conformance）について

DMARCは、SPFやDKIMの結果をもとに、「このメールをどう扱うか？」を決めるための仕組み

インターネットのメールとDMARCの仕組みを「郵便」にたとえると…
たとえば、郵便局が封筒の住所や印鑑の情報と、便せんの名前が一致しているかどうかをチェックして、
この手紙は怪しいから「怪しい郵便として区別しよう」とか「配達しないで返送しよう」と判断するようなものです。

DMARCでは、送信者が「SPFやDKIMの認証に失敗したら、メールを拒否してほしい」「迷惑メールフォルダに入れてほしい」などのポリシーをDNSに登録しておきます。
メールを受け取る側（受信者）は、SPFやDKIMの結果を見て、そのポリシーに従ってメールを処理します。

DMARCでは、SPFやDKIMの認証結果だけでなく、送信者のドメインが一致しているかどうかもチェックします。
これを「アライメント（整合性）」と呼びます。
たとえば、便せんに書かれた名前（ヘッダーFrom）が「example.com」なのに、SPFやDKIMで認証されたドメインが「mailer.example.net」だった場合、ドメインが一致していないと判断されます。
SPFやDKIMだけでは、「認証に失敗したメールをどうするか？」は受信者任せでしたが、DMARCを使えば、送信者があらかじめルールを決めておけるので、なりすましメールをより確実にブロックできます。

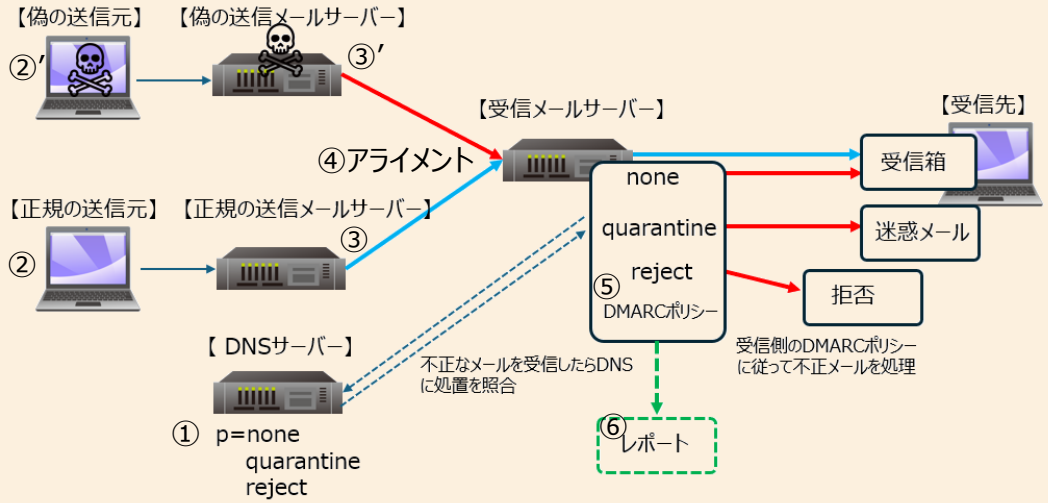
2023年時点での導入率はJPドメインで約10.2%※と低かったのですが、最近では企業でも導入が進んでいます。
送信ドメイン認証は送信側、受信側ともに広く普及しないと導入に踏み切りにくいものですが、今後さらに普及が期待されています。

※総務省　令和6年版　情報通信白書の概要　送信ドメイン認証技術のJPドメイン導入状況より

DMARCの注意点

DMARCは、SPFまたはDKIMが正しく設定されていることが前提です。
どちらかがうまく機能していないと、正当なメールでも「認証失敗」と判断されてしまうことがあります。
また、DMARCのポリシーを「拒否（reject）」にすると、一部の正当なメールが届かなくなるリスクもあります。
特に、メールの転送や外部サービスを使っている場合は、慎重な設定が必要です。

DMARCの仕組み



送信側（HOME type-Mは送信側のDMARCに対応しています）
①DNSサーバのTXTレコードにDMARCレコードを登録　←マイデスクから登録可能
②、②′メールを送信
③、③′送信メールサーバーがメールを配送

受信側
④受信サーバーがSPFやDKIMの整合性（アライメント）を取り認証
⑤受信メールサーバ側のDMARCポリシーに従いメールを配送
　noneは何もしない、quarantineは隔離し迷惑メールへ、rejectは受信拒否
⑥レポートを作成して指定されたメールアドレスに送信